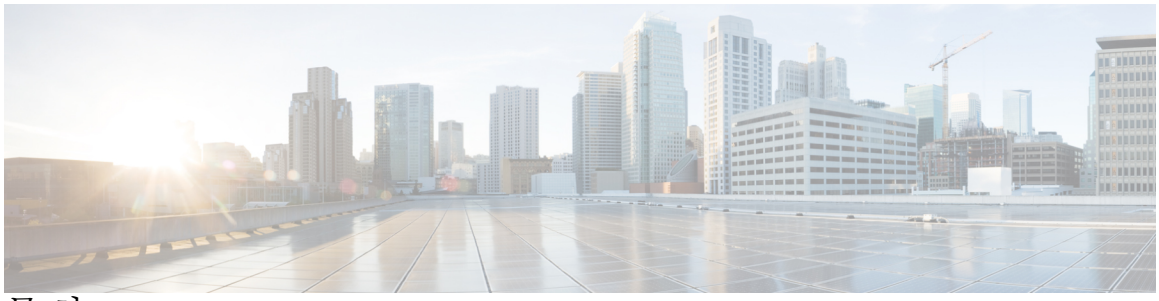
ASDM Book 3: Cisco ASA Series VPN ASDM 구성 가이드, 7.8

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



목 차

가이드 정보

다음 주제에서는 이 가이드를 사용하는 방법을 설명합니다.

문서 목적

이 설명서는 웹 기반 GUI 애플리케이션인 ASDM(Adaptive Security Device Manager)을 사용하여 ASA(Adaptive Security Appliance)에서 VPN을 구성하는 작업을 지원하기 위해 제공됩니다. 여기서는 모든 기능을 다루기보다는 가장 대표적인 구성 시나리오에 대해서만 설명합니다.

이 설명서는 Cisco ASA 시리즈에 적용됩니다. 이 가이드에서 "ASA"라는 용어는 별도로 지정하지 않는 한, 일반적으로 지원되는 모델에 적용됩니다.

관련 문서

자세한 내용은 http://www.cisco.com/go/asadocs에서 *Navigating the Cisco ASA Series Documentation(Cisco ASA Series* 설명서 찾기*)*을 참조하십시오.

문서 표기 규칙

이 문서는 다음의 텍스트, 표시 및 알림 표기 규칙을 따릅니다.

텍스트 표기 규칙

표기 규칙	표시
boldface	명령, 키워드, 버튼 레이블, 필드 이름 및 사용자 입력 텍스트는 **boldface**에 나타납니다. 메뉴 기반 명령의 경우, 명령에 대한 전체 경로가 표시됩니다.

가이드 정보

표기 규칙	표시
기울임꼴	제공하는 값에 대한 변수는 기울임꼴 서체로 표시됩니다. 기울임꼴 유형은 문서 제목 및 일반적인 강조 시에도 사용됩니다.
monospace	시스템에 표시되는 터미널 세션 및 정보는 monospace 유형으로 표시됩니다.
{x | y | z}	필수 대체 키워드는 중괄호로 묶어 세로 선으로 구분합니다.
[ ]	대괄호로 묶인 요소는 선택적 요소입니다.
[x | y | z]	선택적 대체 키워드는 대괄호로 묶어 세로 선으로 구분합니다.
[ ]	시스템 프롬프트에 대한 기본 응답은 대괄호 안에도 표시됩니다.
< >	비밀번호와 같이 인쇄할 수 없는 문자는 꺾쇠괄호 안에 표시됩니다.
!, #	코드 라인 시작 부분에 있는 느낌표(!) 또는 숫자 기호(#)는 코멘트 행을 나타냅니다.

독자 알림

이 문서에서는 독자에게 알리기 위해 다음 사항을 사용합니다.

참고 독자가 주목해야 하는 내용을 의미합니다. 참고에는 유용한 제안이나 해당 설명서에서 다루지 않는 자료에 대한 참조 정보가 포함됩니다.

팁 다음 정보가 문제를 해결하는 데 도움이 된다는 것을 의미합니다.

주의 독자가 유의해야 하는 내용임을 의미합니다. 장비 손상이나 데이터 손실이 발생할 수 있으므로 주의해야 한다는 내용이 포함됩니다.

간편한 방법 설명한 작업이 시간을 절약함을 의미합니다. 단락에서 설명한 작업을 수행함으로써 시간을 절약할 수 있습니다.

경고! 독자에게 경고하는 내용을 의미합니다. 이러한 상황에서는 신체 상해로 이어질 수 있는 작업을 수행해야 할 수 있습니다.

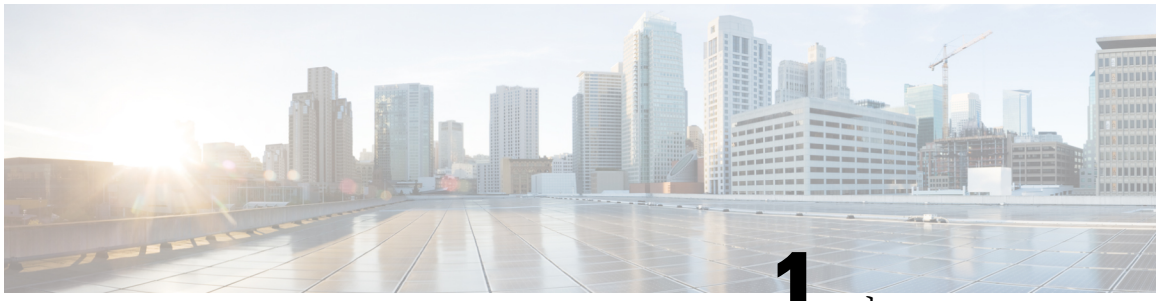
문서 가져오기 및 서비스 요청 제출

문서 가져오기, Cisco BST(Bug Search Tool) 사용, 서비스 요청 제출, 추가 정보 수집에 대한 자세한 내용은 Cisco 제품 설명서의 새로운 사항을 참조하십시오.

신규 및 수정된 Cisco 기술 콘텐츠를 데스크톱에서 곧바로 받으려면 Cisco 제품 설명서의 새로운 사항 RSS 피드를 구독하십시오. RSS 피드는 무료 서비스입니다.

I 부

Site-to-Site 및 클라이언트 VPN



1 장

VPN 마법사

VPN 개요

ASA에서는 사용자에게 비공개 연결로 표시되는 TCP/IP 네트워크(예를 들어 인터넷)를 통해 보안 연결을 생성하여 VPN(Virtual Private Network)을 생성합니다. 단일 사용자-LAN(single-user-to-LAN) 연결 및 LAN-to-LAN 연결을 만들 수 있습니다.

보안 연결을 터널이라고 하며, ASA에서는 터널링 프로토콜을 사용하여 보안 파라미터를 협상하고, 터널을 생성하고 관리하며, 패킷을 캡슐화하고, 터널을 통해 패킷을 전송하거나 수신하고, 패킷의 캡슐화를 해제합니다. ASA에서는 양방향 터널 엔드포인트로서의 기능을 수행합니다. 플레인 패킷을 수신하고, 이를 캡슐화한 다음, 해당 패킷의 캡슐화가 해제되고 최종 대상으로 전송되는 터널의 다른 쪽 끝에 패킷을 전송합니다. ASA에서는 캡슐화된 패킷을 수신하고 해당 패킷의 캡슐화를 해제한 후 이를 최종 대상으로 전송할 수도 있습니다.

VPN 마법사에서는 기본 LAN-to-LAN 및 원격 액세스 VPN 연결을 구성하고, 인증을 위해 사전 공유된 키 또는 디지털 인증서를 할당할 수 있습니다. 고급 기능을 수정하고 구성하려면 ASDM을 사용해 주십시오.

이 섹션에서 설명하는 네 가지 VPN 마법사는 다음과 같습니다.

- Clientless SSL VPN Wizard(클라이언트리스 SSL VPN 마법사), 2 페이지

  ASA 클라이언트리스 SSL VPN은 웹 브라우저와 해당 네이티브 SSL 암호화만 사용하여 인터넷이 지원되는 거의 모든 곳에서 SSL(Secure Socket Layer) 원격 액세스 연결을 제공합니다. 이 브라우저 기반 VPN을 통해 사용자는 ASA(Adaptive Security Appliance)에 대한 보안 원격 액세스 VPN 터널을 설정할 수 있습니다. 사용자는 인증 후 포털 페이지에 액세스하여 지원되는 특정 내부 리소스에 액세스할 수 있습니다. 네트워크 관리자는 사용자 그룹별로 리소스에 대한 액세스를 제공합니다. 사용자는 내부 네트워크의 리소스에 직접 액세스할 수 없습니다.

- AnyConnect VPN Wizard(AnyConnect VPN 마법사), 3 페이지

Cisco AnyConnect VPN 클라이언트는 기업 리소스에 대한 전체 VPN 터널링을 통해 원격 사용자에게 ASA에 대한 SSL 또는 IPsec(IKEv2) 연결을 제공합니다. 이전에 설치된 클라이언트가 없는 경우 원격 사용자는 SSL 또는 클라이언트리스 VPN 연결을 허용하도록 구성된 인터페이스의 브라우저에 IP 주소를 입력합니다. ASA는 원격 컴퓨터의 운영 체제와 일치하는 클라이언트를 다운로드합니다. 다운로드 후에는 클라이언트가 자동으로 설치 및 구성되어 보안 연결을 설정하며, 연결이 종료되면 ASA 구성에 따라 그대로 유지되거나 자동으로 제거됩니다. 클라이언트가 이전에 설치된 경우 사용자가 인증을 통과하면 ASA에서 클라이언트의 개정 내역을 확인하고 필요에 따라 클라이언트를 업그레이드합니다.

- IPsec IKEv2 Remote Access Wizard(IPsec IKEv2 원격 액세스 마법사), 11 페이지

  IKEv2는 다른 공급업체의 VPN 클라이언트에서 ASA에 연결할 수 있도록 해줍니다. 이러한 기능은 보안을 향상시키며, 정부 및 공공 부문의 규정에 정의된 IPsec 원격 액세스 요건을 준수합니다.

- IPsec IKEv1 Remote Access Wizard(IPsec IKEv1 원격 액세스 마법사), 6 페이지
- IPsec Site-to-Site VPN Wizard(IPsec 사이트 대 사이트 VPN 마법사), 14 페이지

  IPv4 및 IPv6 주소 지정을 둘 다 사용하는 LAN-to-LAN 연결의 경우 ASA는 두 피어(peer) 모두 ASA이고, 두 내부 네트워크의 주소 지정 체계가 일치(둘 다 IPv4이거나 둘 다 IPv6)하는 경우 VPN 터널을 지원합니다. 이는 피어 내부 네트워크와 외부 네트워크가 둘 다 IPv6인 경우에도 적용됩니다.

Clientless SSL VPN Wizard(클라이언트리스 SSL VPN 마법사)

이 마법사는 포털 페이지를 통해, 지원되는 특정 내부 리소스에 대한 클라이언트리스 브라우저 기반 연결을 지원합니다.

SSL VPN Interface(SSL VPN 인터페이스)

SSL VPN 사용자가 연결할 연결 프로파일 및 인터페이스를 제공합니다.

- Connection Profile Name(연결 프로파일 이름) - 연결 프로파일 이름을 지정합니다.
- SSL VPN Interface(SSL VPN 인터페이스) - 사용자가 SSL VPN 연결을 위해 액세스하는 인터페이스입니다.
- Digital Certificate(디지털 인증서) - ASA에서 ASA를 인증하기 위해 원격 웹 브라우저로 전송하는 항목을 지정합니다.
  - Certificate(인증서) - 드롭다운 목록에서 선택합니다.
- Accessing the Connection Profile(연결 프로파일 액세스)
  - Connection Group Alias/URL(연결 그룹 별칭/URL) - 그룹 별칭은 로그인하는 동안 Group(그룹) 드롭다운 목록에서 선택됩니다. 이 URL이 웹 브라우저에 입력됩니다.

- Display Group Alias list at the login page(로그인 페이지에 그룹 별칭 목록 표시) - 로그인 페이지에 그룹 별칭 목록을 표시하려면 선택합니다.

사용자 인증

이 창에서 인증 정보를 지정합니다.

- Authenticate using a AAA server group(AAA 서버 그룹을 사용하여 인증) - ASA에서 사용자를 인증하기 위해 원격 AAA 서버 그룹에 연결할 수 있도록 지원합니다.
  - AAA Server Group Name(AAA 서버 그룹 이름) - 미리 구성된 그룹 목록에서 AAA 서버 그룹을 선택하거나, **New(**새로 만들기**)**를 클릭하여 새 그룹을 만듭니다.
- Authenticate using the local user database(로컬 사용자 데이터베이스를 사용하여 인증) - ASA에 저장된 로컬 데이터베이스에 새 사용자를 추가합니다.
  - Username(사용자 이름) - 사용자의 사용자 이름을 만듭니다.
  - Password(비밀번호) - 사용자의 비밀번호를 만듭니다.
  - Confirm Password(비밀번호 확인) - 확인을 위해 동일한 비밀번호를 다시 입력합니다.
  - Add/Delete(추가/삭제) - 로컬 데이터베이스에서 사용자를 추가하거나 삭제합니다.

그룹 정책

그룹 정책은 사용자 그룹에 대한 공통 특성을 구성합니다. 새 그룹 정책을 만들거나 수정할 기존 그룹 정책을 선택합니다.

- Create new group policy(새 그룹 정책 만들기) - 새 그룹 정책을 만들 수 있습니다. 새 정책의 이름을 제공합니다.
- Modify existing group policy(기존 그룹 정책 수정) - 수정할 기존 그룹 정책을 선택합니다.

Bookmark List(책갈피 목록**)**

포털 페이지에 링크로 표시되는 그룹 인트라넷 웹사이트의 목록을 구성합니다. 예를 들면 https://intranet.acme.com, rdp://10.120.1.2, vnc://100.1.1.1 등이 있습니다.

- Bookmark List(책갈피 목록) - 드롭다운 목록에서 선택합니다.
- Manage(관리) - Configure GUI Customization Object(GUI 사용자 지정 개체 구성) 대화 상자를 열려면 클릭합니다.

AnyConnect VPN Wizard(AnyConnect VPN 마법사)

이 마법사를 사용하여 AnyConnect VPN 클라이언트의 VPN 연결을 허용하도록 ASA를 구성할 수 있습니다. 이 마법사는 전체 네트워크 액세스에 대해 IPsec(IKEv2) 또는 SSL VPN 프로토콜을 구성합니

다. ASA는 VPN 연결이 설정된 경우 엔드 유저의 디바이스로 AnyConnect VPN 클라이언트를 자동으로 업로드합니다.

Connection Profile Identification(연결 프로파일 식별)

연결 프로파일 식별은 원격 액세스 사용자에게 ASA를 알려주는 데 사용됩니다.

- Connection Profile Name(연결 프로파일 이름) - 원격 액세스 사용자가 VPN 연결을 위해 액세스할 이름을 제공합니다.
- VPN Access Interface(VPN 액세스 인터페이스) - 원격 액세스 사용자가 VPN 연결을 위해 액세스할 인터페이스를 선택합니다.

VPN Protocols(VPN 프로토콜)

이 연결 프로파일에 연결되는 VPN 프로토콜을 지정합니다.

AnyConnect 클라이언트는 기본적으로 SSL로 설정됩니다. IPsec을 연결 프로파일의 VPN 터널 프로토콜로 설정한 경우에는 ASDM에서 프로파일 편집기를 사용하여 IPsec을 지원하는 클라이언트 프로파일을 만들고 구축해야 합니다.

AnyConnect 클라이언트를 웹 실행하는 대신 사전 구축하는 경우에는 첫 번째 클라이언트 연결에서 SSL을 사용하며 세션 중에 ASA에서 클라이언트 프로필을 받습니다. 이후의 연결에서는 클라이언트에서 프로파일에 지정된 프로토콜(SSL 또는 IPsec)을 사용합니다. 클라이언트에 지정된 IPsec을 사용하여 프로파일을 구축하는 경우에는 첫 번째 클라이언트 연결에서 IPsec을 사용합니다. IPsec을 지원하는 클라이언트 프로파일 사전 구축에 대한 자세한 내용은 *AnyConnect Secure Mobility Client* 관리자 가이드를 참조해 주십시오.

- SSL
- IPsec(IKE v2)
- Device Certificate(디바이스 인증서) - 원격 액세스 클라이언트에 ASA를 알려줍니다. 일부 AnyConnect 기능(예: always on, IPsec/IKEv2)에는 ASA의 유효한 디바이스 인증서가 필요합니다.
- Manage(관리) - **Manage(**관리**)**를 선택하면 Manage Identity Certificates(ID 인증서 관리) 창이 열립니다.
  - Add(추가) - ID 인증서와 해당 세부사항을 추가하려면 **Add(**추가**)**를 선택합니다.
  - Show Details(세부사항 표시) - 특정 인증서를 선택하고 **Show Details(**세부사항 표시**)**를 클릭하면 인증서 발행 기관 및 발행 대상을 비롯하여 인증서의 일련 번호, 사용 현황, 연계된 신뢰 지점, 유효한 시간 범위 등이 표시된 Certificate Details(인증서 세부사항) 창이 나타납니다.
  - Delete(삭제) - 제거할 인증서를 강조 표시하고 **Delete(**삭제**)**를 클릭합니다.
  - Export(내보내기) - 인증서를 강조 표시하고 **Export(**내보내기**)**를 클릭하여 인증서를 파일로 내보냅니다(암호화에 사용되는 암호를 포함하거나 포함하지 않음).
  - Enroll ASA SSL VPN with Entrust(Entrust에 ASA SSL VPN 등록) - Entrust의 SSL Advantage 디지털 인증서로 Cisco ASA SSL VPN 어플라이언스를 신속하게 가동 및 실행합니다.

Client Images(클라이언트 이미지**)**

ASA는 엔터프라이즈 네트워크에 액세스할 때 최신 AnyConnect 패키지를 클라이언트 디바이스로 자동으로 업로드할 수 있습니다. 관리자는 정규식을 사용하여 브라우저의 사용자 에이전트를 이미지와 일치시킬 수 있습니다. 또한 가장 일반적으로 사용되는 운영 체제를 목록의 맨 위로 이동하여 연결 설정 시간을 최소화할 수 있습니다.

인증 방법

이 화면에서는 인증 정보를 지정합니다.

- AAA server group(AAA 서버 그룹) - ASA에서 사용자를 인증하기 위해 원격 AAA 서버 그룹에 연결할 수 있도록 지원합니다. 미리 구성된 그룹 목록에서 AAA 서버 그룹을 지정하거나, **New(**새로 만들기**)**를 클릭하여 새 그룹을 만듭니다.
- Local User Database Details(로컬 사용자 데이터베이스 세부사항) - ASA에 저장된 로컬 데이터베이스에 새 사용자를 추가합니다.
  - Username(사용자 이름) - 사용자의 사용자 이름을 만듭니다.
  - Password(비밀번호) - 사용자의 비밀번호를 만듭니다.
  - Confirm Password(비밀번호 확인) - 확인을 위해 동일한 비밀번호를 다시 입력합니다.
  - Add/Delete(추가/삭제) - 로컬 데이터베이스에서 사용자를 추가하거나 삭제합니다.

Client Address Assignment(클라이언트 주소 할당**)**

원격 AnyConnect 사용자에게 IP 주소 범위를 제공합니다.

- IPv4 Address Pools(IPv4 주소 풀) - SSL VPN 클라이언트가 ASA에 연결하면 새 IP 주소가 제공됩니다. 클라이언트리스 연결에는 새 IP 주소가 필요하지 않습니다. 주소 풀은 원격 클라이언트에 제공할 수 있는 주소 범위를 정의합니다. 기존 IP 주소 풀을 선택하거나 **New(**새로 만들기**)**를 클릭하여 새 풀을 만듭니다.

  New(새로 만들기**)**를 선택한 경우 시작 및 끝 IP 주소와 서브넷 마스크를 제공해야 합니다.

- IPv6 Address Pool(IPv6 주소 풀) - 기존 IP 주소 풀을 선택하거나 **New(**새로 만들기**)**를 클릭하여 새 풀을 만듭니다.

참고 IKEv2 연결 프로파일에는 IPv6 주소 풀을 만들 수 없습니다.

Network Name Resolution Servers(네트워크 이름 확인 서버**)**

원격 사용자가 내부 네트워크에 액세스할 때 확인할 도메인 이름을 지정합니다.

- DNS Servers(DNS 서버) - DNS 서버의 IP 주소를 입력합니다.
- WINS Servers(WINS 서버) - WINS 서버의 IP 주소를 입력합니다.

- Domain Name(도메인 이름) - 기본 도메인 이름을 입력합니다.

NAT 제외

ASA에서 네트워크 변환을 활성화하는 경우 VPN 트래픽은 이 변환에서 제외해야 합니다.

AnyConnect Client Deployment(AnyConnect 클라이언트 구축**)**

다음 방법 중 하나를 사용하여 클라이언트 디바이스에 AnyConnect 클라이언트 프로그램을 설치할 수 있습니다.

- Web launch(웹 실행) - 웹 브라우저를 사용하여 ASA에 액세스하는 경우 AnyConnect 클라이언트 패키지가 자동으로 설치됩니다.

  참고 웹 실행은 다중 상황 모드에서 지원되지 않습니다.

- Pre-deployment(사전 구축) - AnyConnect 클라이언트 패키지를 수동으로 설치합니다.

Allow Web Launch(웹 실행 허용)는 모든 연결에 영향을 주는 전역 설정입니다. 이 확인란을 선택하지 않으면(disallowed(허용 안 함)) AnyConnect SSL 연결 및 클라이언트리스 SSL 연결이 작동하지 않습니다.

사전 구축의 경우 disk0:/test2_client_profile.xml 프로파일 번들에 .msi 파일이 포함되어 있으므로 IPsec 연결이 정상적으로 작동하도록 ASA의 이 클라이언트 프로파일을 AnyConnect 패키지에 포함해야 합니다.

IPsec 마법사

관련 항목

IPsec IKEv1 Remote Access Wizard(IPsec IKEv1 원격 액세스 마법사), 6 페이지
IPsec IKEv2 Remote Access Wizard(IPsec IKEv2 원격 액세스 마법사), 11 페이지

IPsec IKEv1 Remote Access Wizard(IPsec IKEv1 원격 액세스 마법사)

참고 Cisco VPN Client는 단종되고 지원이 중단되었습니다. AnyConnect Secure Mobility Client로 업그레이드해야 합니다.

IKEv1 Remote Access Wizard(IKEv1 원격 액세스 마법사)를 사용하여 모바일 사용자와 같은 VPN 클라이언트에 대한 보안 원격 액세스를 구성하고, 원격 IPsec 피어에 연결하는 인터페이스를 식별할 수 있습니다.

- VPN Tunnel Interface(VPN 터널 인터페이스) - 원격 액세스 클라이언트에 사용할 인터페이스를 선택합니다. ASA에 여러 인터페이스가 있는 경우 지금 중지하고 ASA에서 인터페이스를 구성한 후 이 마법사를 실행해 주십시오.
- Enable inbound IPsec sessions to bypass interface access lists(인바운드 IPsec 세션을 활성화하여 인터페이스 액세스 목록 우회) - 항상 ASA를 통과할 수 있도록(즉, 인터페이스 액세스 목록을 확인하지 않음) IPsec 인증된 인바운드 세션을 활성화합니다. 인바운드 세션은 인터페이스 ACL만 우회합니다. 구성된 그룹 정책, 사용자 및 다운로드한 ACL은 여전히 적용됩니다.

원격 액세스 클라이언트

다양한 유형의 원격 액세스 사용자가 이 ASA에 대한 VPN 터널을 열 수 있습니다. 이 터널의 VPN 클라이언트 유형을 선택합니다.

- VPN 클라이언트 유형
  - Easy VPN Remote 제품
  - L2TP over IPsec을 사용하는 Microsoft Windows 클라이언트 - PPP 인증 프로토콜을 지정합니다. PAP, CHAP, MS-CHAP-V1, MS-CHAP-V2 및 EAP-PROXY 중에서 선택할 수 있습니다.

    PAP - 인증하는 동안 일반 텍스트 사용자 이름 및 비밀번호를 전달하므로 안전하지 않습니다.

    CHAP - 서버 챌린지에 대한 응답으로 클라이언트에서 일반 텍스트 사용자 이름 및 비밀번호와 함께 암호화된 챌린지를 반환합니다. 이 프로토콜은 PAP보다 안전하지만 데이터를 암호화하지 않습니다.

    MS-CHAP, 버전 1 - CHAP와 유사하지만 일반 텍스트 비밀번호를 사용하는 CHAP와 달리 서버에서 암호화된 비밀번호만 저장하고 비교한다는 점에서 보다 안전합니다.

    MS-CHAP, 버전 2 - MS-CHAP, 버전 1보다 보안 기능이 향상되었습니다.

    EAP-Proxy - ASA에서 외부 RADIUS 인증 서버에 대한 PPP 인증 프로세스에 프록시를 사용하도록 허용하는 EAP를 활성화합니다.

    원격 클라이언트에 프로토콜이 지정되지 않은 경우에는 이 유형을 지정하지 마십시오.
  - 클라이언트에서 터널 그룹 이름을 username@tunnelgroup으로 전송할지 지정합니다.

VPN Client Authentication Method and Tunnel Group Name(VPN 클라이언트 인증 방법 및 터널 그룹 이름)

VPN Client Authentication Method and Name(VPN 클라이언트 인증 방법 및 이름) 창을 사용하여 인증 방법을 구성하고 연결 정책(터널 그룹)을 만들 수 있습니다.

- Authentication Method(인증 방법) - 원격 사이트 피어에서 사전 공유 키 또는 인증서를 사용하여 인증합니다.
  - Pre-shared Key(사전 공유 키) - 로컬 ASA와 원격 IPsec 피어 간의 인증에 사전 공유 키를 사용하려면 클릭합니다.

사전 공유 키를 사용하면 제한된 수의 원격 피어와의 통신 및 안정적인 네트워크를 빠르고 쉽게 설정할 수 있습니다. 하지만 각 IPsec 피어에 보안 연결을 설정하는 각 피어에 대한 구성 정보가 필요하므로 대규모 네트워크에서 확장성 문제가 발생할 수 있습니다.

보안 터널을 설정하려면 각 IPsec 피어 쌍이 사전 공유 키를 교환해야 합니다. 안전한 방법을 사용하여 원격 사이트의 관리자와 사전 공유 키를 교환해 주십시오.

- Pre-shared Key(사전 공유 키) - 1~128자의 영숫자 문자열을 입력합니다.
- Certificate(인증서) - 로컬 ASA와 원격 IPsec 피어 간의 인증에 인증서를 사용하려면 클릭합니다. 이 화면을 완료하려면 이전에 CA에 등록하고 하나 이상의 인증서를 ASA로 다운로드해야 합니다.

  디지털 인증서를 사용하여 IPsec 터널을 설정하는 데 사용되는 보안 키를 효율적으로 관리할 수 있습니다. 디지털 인증서에는 이름, 일련 번호, 회사, 부서, IP 주소 등 사용자 또는 디바이스를 식별하는 정보가 포함되어 있습니다. 또한 공개 키 사본도 포함되어 있습니다.

  디지털 인증서를 사용하려면 각 피어가 디지털 인증서를 발급하는 CA(Certification Authority)에 등록해야 합니다. CA는 신뢰할 수 있는 공급업체이거나 조직 내에서 만든 비공개 CA일 수 있습니다.

  두 피어가 통신하려면 인증서를 교환하고 데이터를 디지털로 서명하여 서로 인증해야 합니다. 네트워크에 새 피어를 추가한 경우 해당 피어가 CA에 등록하므로 다른 피어에는 추가 구성이 필요 없습니다.

  Certificate Signing Algorithm(인증서 서명 알고리즘) - 디지털 인증서 서명 알고리즘(RSA의 경우 rsa-sig)을 표시합니다.

- Tunnel Group Name(터널 그룹 이름) - 이 IPsec 연결에 대한 터널 연결 정책을 포함하는 레코드를 만들 이름을 입력합니다. 연결 정책에서는 인증, 권한 부여 및 어카운트 관리 서버, 기본 그룹 정책, IKE 특성 등을 지정할 수 있습니다. 이 VPN 마법사를 사용하여 구성한 연결 정책에서는 인증 방법을 지정하며, ASA 기본 그룹 정책을 사용합니다.

클라이언트 인증

Client Authentication(클라이언트 인증) 창을 사용하여 ASA에서 원격 사용자를 인증하는 방법을 선택할 수 있습니다. 다음 옵션 중 하나를 선택합니다.

- Authenticate using the local user database(로컬 사용자 데이터베이스를 사용하여 인증) - ASA 내부 인증을 사용하려면 클릭합니다. 안정적인 소수의 사용자가 있는 환경에 이 방법을 사용합니다. 다음 창에서는 ASA에서 개별 사용자에 대한 어카운트를 생성할 수 있습니다.
- Authenticate using an AAA server group(AAA 서버 그룹을 사용하여 인증) - 원격 사용자 인증에 외부 서버 그룹을 사용하려면 클릭합니다.
  - AAA Server Group Name(AAA 서버 그룹 이름) - 이전에 구성한 AAA 서버 그룹을 선택합니다.
  - New...(새로 만들기...) - 새 AAA 서버 그룹을 구성하려면 클릭합니다.

사용자 계정

User Accounts(사용자 어카운트) 창을 사용하여 인증을 위해 ASA 내부 사용자 데이터베이스에 새 사용자를 추가할 수 있습니다.

주소 풀

Address Pool(주소 풀) 창을 사용하여 ASA에서 원격 VPN 클라이언트에 할당하는 로컬 IP 주소 풀을 구성할 수 있습니다.

- Tunnel Group Name(터널 그룹 이름) - 이 주소 풀이 적용되는 연결 프로파일(터널 그룹)의 이름을 표시합니다. VPN Client and Authentication Method(VPN 클라이언트 및 인증 방법) 창에서 이 이름을 설정합니다(3단계).
- Pool Name(풀 이름) - 주소 풀을 설명하는 식별자를 선택합니다.
- New...(새로 만들기...) - 새 주소 풀을 구성하려면 클릭합니다.
- Range Start Address(범위 시작 주소) - 주소 풀의 시작 IP 주소를 입력합니다.
- Range End Address(범위 끝 주소) - 주소 풀의 끝 IP 주소를 입력합니다.
- Subnet Mask(서브넷 마스크) - (선택 사항) 이러한 IP 주소의 서브넷 마스크를 선택합니다.

Attributes Pushed to Client (Optional)(클라이언트에 푸시되는 특성(선택 사항))

Attributes Pushed to Client (Optional)(클라이언트에 푸시되는 속성(선택 사항)) 창을 사용하여 ASA에서 DNS 및 WINS 서버에 대한 정보와 기본 도메인 이름을 원격 액세스 클라이언트로 전달하도록 할 수 있습니다.

- Tunnel Group(터널 그룹) - 주소 풀이 적용되는 연결 정책의 이름을 표시합니다. VPN Client Name and Authentication Method(VPN 클라이언트 이름 및 인증 방법) 창에서 이 이름을 설정합니다.
- Primary DNS Server(기본 DNS 서버) - 기본 DNS 서버의 IP 주소를 입력합니다.
- Secondary DNS Server(보조 DNS 서버) - 보조 DNS 서버의 IP 주소를 입력합니다.
- Primary WINS Server(기본 WINS 서버) - 기본 WINS 서버의 IP 주소를 입력합니다.
- Secondary WINS Server(보조 WINS 서버) - 보조 WINS 서버의 IP 주소를 입력합니다.
- Default Domain Name(기본 도메인 이름) - 기본 도메인 이름을 입력합니다.

IKE 정책

ISAKMP(Internet Security Association and Key Management Protocol)라고도 하는 IKE는 두 개의 호스트가 IPsec 보안 연계를 구축하는 방법에 동의할 수 있도록 해주는 협상 프로토콜입니다. 각 IKE 협상은 Phase1과 Phase 2라는 두 개의 섹션으로 나누어집니다. 1단계에서는 최신 IKE 협상 메시지를 보호하는 첫 번째 터널을 생성합니다. 2단계에서는 데이터를 보호하는 터널을 생성합니다.

IKE Policy(IKE 정책) 창을 사용하여 데이터 및 개인 정보를 보호할 암호화 방법, 피어의 ID를 확인할 인증 방법, 암호화 키 결정 알고리즘의 장점을 확립할 Diffie-Hellman 그룹을 포함하는 Phase 1 IKE 협상 조건을 설정할 수 있습니다. ASA는 이 알고리즘을 사용하여 암호화 및 해시 키를 파생합니다.

- Encryption(암호화) - ASA에서 Phase 2 협상을 보호하는 Phase 1 SA를 설정하는 데 사용할 대칭 암호화 알고리즘을 선택합니다. ASA에서 지원하는 암호화 알고리즘은 다음과 같습니다.

알고리즘	설명
DES	Data Encryption Standard(데이터 암호화 표준)의 약어입니다. 56비트 키를 사용합니다.
3DES	삼중 DES입니다. 56비트 키를 사용하여 암호화를 세 번 수행합니다.
AES-128	Advanced Encryption Standard(고급 표준 암호화)의 약어입니다. 128비트 키를 사용합니다.
AES-192	192비트 키를 사용하는 AES입니다.
AES-256	256비트 키를 사용하는 AES입니다.

  기본값인 3DES는 DES보다 안전하지만 암호화 및 암호 해독을 위한 추가 처리가 필요합니다. 이와 마찬가지로 AES 옵션도 향상된 보안을 제공하지만 더 많은 처리가 필요합니다.

- Authentication(인증) - 인증 및 데이터 무결성 보장에 사용되는 해시 알고리즘을 선택합니다. 기본값은 SHA입니다. MD5의 다이제스트가 더 작으며, 속도는 SHA보다 약간 더 빠른 것으로 간주됩니다. MD5 공격은 매우 어렵지만 성공한 사례가 있습니다. 하지만 ASA에서 사용하는 HMAC(Keyed-Hash Message Authentication Code) 버전은 이 공격을 방지합니다.
- Diffie-Hellman Group(Diffie-Hellman 그룹) - 서로 전달하지 않고 공유 비밀을 파생하기 위해 두 IPsec 피어가 사용하는 Diffie-Hellman 그룹의 식별자를 선택합니다. 기본값인 Group 2(1024비트 Diffie-Hellman)는 CPU 실행 시간이 짧지만 Group 5(1536비트)보다 안전하지 않습니다.

IPsec Settings (Optional)(IPsec 설정(선택 사항))

IPsec Settings (Optional)(IPsec 설정(선택 사항)) 창을 사용하여 주소 변환이 필요 없는 로컬 호스트/네트워크를 식별할 수 있습니다. 기본적으로 ASA는 동적 또는 정적 NAT(Network Address Translation)를 사용하여 내부 호스트 및 네트워크의 실제 IP 주소를 외부 호스트로부터 숨깁니다. NAT는 신뢰할 수 없는 외부 호스트에 의한 공격의 위험을 최소화하지만 VPN에 의해 인증 및 보호된 외부 호스트에는 적절하지 않을 수 있습니다.

예를 들어 동적 NAT를 사용하는 내부 호스트는 풀에서 무작위로 선택된 주소와 일치시켜 해당 IP 주소를 변환합니다. 이 변환된 주소만 외부에 표시됩니다. 따라서 실제 IP 주소로 데이터를 보내 이러한 호스트에 연결하려는 원격 VPN 클라이언트는 NAT 제외 규칙을 구성하지 않으면 이러한 호스트에 연결할 수 없습니다.

참고 모든 호스트와 네트워크를 NAT에서 제외하려면 이 창에서 아무 것도 구성하지 마십시오. 하나의 항목만 구성해도 다른 모든 호스트와 네트워크에 NAT가 적용됩니다.

- Interface(인터페이스) - 선택한 호스트 또는 네트워크에 연결하는 인터페이스의 이름을 선택합니다.
- Exempt Networks(제외 네트워크) - 선택한 인터페이스 네트워크에서 제외할 호스트 또는 네트워크의 IP 주소를 선택합니다.
- Enable split tunneling(스플릿 터널링 활성화) - 공개 인터넷으로 전송되는 원격 액세스 클라이언트의 트래픽을 암호화되지 않은 상태로 전송하려면 선택합니다. 스플릿 터널링을 사용하면 보호된 네트워크의 트래픽은 암호화되는 반면, 보호되지 않은 네트워크의 트래픽은 암호화되지 않습니다. 스플릿 터널링을 활성화하면 ASA에서 인증 후 원격 VPN 클라이언트로 IP 주소 목록을 푸시합니다. 원격 VPN 클라이언트는 ASA 뒤에 있는 IP 주소로 전송되는 트래픽을 암호화합니다. 다른 모든 트래픽은 ASA를 거치지 않고 인터넷으로 직접 암호화되지 않은 상태로 전송됩니다.
- Enable Perfect Forwarding Secrecy (PFS)(PFS(Perfect Forwarding Secrecy) 활성화) - Phase 2 IPsec 키 생성 시 Perfect Forward Secrecy를 사용할지 여부 및 사용할 숫자 크기를 지정합니다. PFS는 각각의 새로운 키가 이전 키와 무관한 암호화 개념입니다. PFS가 활성화되지 않은 경우 IPsec 협상에서 Phase 2 키는 Phase 1 키를 기반으로 합니다. PFS는 Diffie-Hellman 기술을 사용하여 키를 생성합니다.

  PFS는 비공개 키 중 하나가 이후에 손상된 경우에도 장기 공개 및 비공개 키 집합에서 파생된 세션 키가 손상되지 않도록 합니다.

  연결의 양쪽 모두에서 PFS를 활성화해야 합니다.

  - Diffie-Hellman Group(Diffie-Hellman 그룹) - 서로 전달하지 않고 공유 비밀을 파생하기 위해 두 IPsec 피어가 사용하는 Diffie-Hellman 그룹의 식별자를 선택합니다. 기본값인 Group 2(1024비트 Diffie-Hellman)는 CPU 실행 시간이 짧지만 Group 5(1536비트)보다 안전하지 않습니다.

Summary(요약**)**

구성에 만족하는 경우 **Finish(**마침**)**를 클릭합니다. 그러면 ASA에서 LAN-to-LAN 구성을 저장합니다. **Finish(**마침**)**를 클릭한 후에는 더 이상 VPN 마법사를 사용하여 이 구성을 변경할 수 없습니다. 고급 기능을 수정하고 구성하려면 ASDM을 사용해 주십시오.

IPsec IKEv2 Remote Access Wizard(IPsec IKEv2 원격 액세스 마법사)

IKEv2 Remote Access Wizard(IKEv2 원격 액세스 마법사)를 사용하여 모바일 사용자와 같은 VPN 클라이언트에 대한 보안 원격 액세스를 구성하고, 원격 IPsec 피어에 연결하는 인터페이스를 식별할 수 있습니다.

Connection Profile Identification(연결 프로파일 식별**)**

Connection Profile Name(연결 프로파일 이름**)**을 입력하고 IPsec IKEv2 원격 액세스에 사용할 **VPN Access Interface(VPN** 액세스 인터페이스**)**를 선택합니다.

- Connection Profile Name(연결 프로파일 이름) - 이 IPsec 연결에 대한 터널 연결 정책을 포함하는 레코드를 만들 이름을 입력합니다. 연결 정책에서는 인증, 권한 부여 및 어카운트 관리 서버, 기본 그룹 정책, IKE 특성 등을 지정할 수 있습니다. 이 VPN 마법사를 사용하여 구성한 연결 정책에서는 인증 방법을 지정하며, ASA 기본 그룹 정책을 사용합니다.
- VPN Access Interface(VPN 액세스 인터페이스) - 원격 IPsec 피어와의 보안 터널을 설정하는 인터페이스를 선택합니다. ASA에 여러 인터페이스가 있는 경우 이 마법사를 실행하기 전에 먼저 VPN 구성을 계획하여 보안 연결을 설정하려는 각 원격 IPsec 피어에 사용할 인터페이스를 식별해야 합니다.

표준 기반 **IPSec(IKEv2)** 인증 페이지

IKE Peer Authentication(IKE 피어 인증) - 원격 사이트 피어는 사전 공유 키로 인증하거나 EAP를 사용한 인증서 또는 피어 인증으로 인증합니다.

- Pre-shared Key(사전 공유 키) - 1~128자의 영숫자 문자열을 입력합니다.

  사전 공유 키를 사용하면 제한된 수의 원격 피어와의 통신 및 안정적인 네트워크를 빠르고 쉽게 설정할 수 있습니다. 하지만 각 IPsec 피어에 보안 연결을 설정하는 각 피어에 대한 구성 정보가 필요하므로 대규모 네트워크에서 확장성 문제가 발생할 수 있습니다.

  보안 터널을 설정하려면 각 IPsec 피어 쌍이 사전 공유 키를 교환해야 합니다. 안전한 방법을 사용하여 원격 사이트의 관리자와 사전 공유 키를 교환해 주십시오.

- Enable Certificate Authentication(인증서 인증 활성화) - 선택한 경우 인증서를 사용하여 인증할 수 있습니다.
- Enable peer authentication using EAP(EAP를 사용한 피어 인증 활성화) - 선택한 경우 EAP를 사용하여 인증할 수 있습니다. 이 확인란을 선택한 경우 로컬 인증에 인증서를 사용해야 합니다.
- Send an EAP identity request to the client(클라이언트로 EAP ID 요청 전송) - 인증을 위한 EAP 요청을 원격 액세스 VPN 클라이언트로 전송할 수 있습니다.

Mobike RRC

- Enable Return Routability Check for mobike(Mobike에 대한 반환 라우팅 가능성 확인 활성화) — mobike가 활성화되어 있는 IKE/IPSEC 보안 연결에서 동적 IP 주소 변경 사항에 대한 반환 라우팅 가능성 확인을 활성화합니다.

IKE Local Authentication(IKE 로컬 인증)

- 로컬 인증을 활성화하고, 사전 공유 키 또는 인증서를 선택합니다.
  - Preshared Key(사전 공유 키) - 1~128자의 영숫자 문자열을 입력합니다.

- Certificate(인증서) - 로컬 ASA와 원격 IPsec 피어 간의 인증에 인증서를 사용하려면 클릭합니다. 이 화면을 완료하려면 이전에 CA에 등록하고 하나 이상의 인증서를 ASA로 다운로드해야 합니다.

  디지털 인증서를 사용하여 IPsec 터널을 설정하는 데 사용되는 보안 키를 효율적으로 관리할 수 있습니다. 디지털 인증서에는 이름, 일련 번호, 회사, 부서, IP 주소 등 사용자 또는 디바이스를 식별하는 정보가 포함되어 있습니다. 또한 공개 키 사본도 포함되어 있습니다.

  디지털 인증서를 사용하려면 각 피어가 디지털 인증서를 발급하는 CA(Certification Authority)에 등록해야 합니다. CA는 신뢰할 수 있는 공급업체이거나 조직 내에서 만든 비공개 CA일 수 있습니다.

  두 피어가 통신하려면 인증서를 교환하고 데이터를 디지털로 서명하여 서로 인증해야 합니다. 네트워크에 새 피어를 추가한 경우 해당 피어가 CA에 등록하므로 다른 피어에는 추가 구성이 필요 없습니다.

인증 방법

IPsec IKEv2 원격 액세스에는 Radius 인증만 지원됩니다.

- AAA Server Group(AAA 서버 그룹) - 이전에 구성한 AAA 서버 그룹을 선택합니다.
- New(새로 만들기) - 새 AAA 서버 그룹을 구성하려면 클릭합니다.
- AAA Server Group Details(AAA 서버 그룹 세부사항) - 필요한 경우 이 영역을 사용하여 AAA 서버 그룹을 수정합니다.

Client Address Assignment(클라이언트 주소 할당**)**

IPv4 및 IPv6 주소 풀을 만들거나 선택하십시오. 그러면 원격 액세스 클라이언트에 IPv4 또는 IPv6 주소 풀의 주소가 할당됩니다. 둘 다 구성된 경우 IPv4 주소가 우선적으로 적용됩니다. 자세한 내용은 로컬 *IP* 주소 풀 구성을 참조하십시오.

Network Name Resolution Servers(네트워크 이름 확인 서버**)**

원격 사용자가 내부 네트워크에 액세스할 때 도메인 이름을 확인하는 방법을 지정합니다.

- DNS Servers(DNS 서버) - DNS 서버의 IP 주소를 입력합니다.
- WINS Servers(DNS 서버) - WINS 서버의 IP 주소를 입력합니다.
- Default Domain Name(기본 도메인 이름) - 기본 도메인 이름을 입력합니다.

NAT 제외

- Exempt VPN traffic from Network Address Translation(Network Address Translation에서 VPN 트래픽 제외) - ASA에서 NAT가 활성화된 경우 이 옵션을 선택해야 합니다.

IPsec Site-to-Site VPN Wizard(IPsec 사이트 대 사이트 VPN 마법사)

두 ASA 디바이스 간의 터널을 사이트 대 사이트 터널이라고 하며, 이는 양방향입니다. 사이트 대 사이트 VPN 터널은 IPsec 프로토콜을 사용하여 데이터를 보호합니다.

Peer Device Identification(피어 디바이스 식별)

- Peer IP Address(피어 IP 주소) - 다른 사이트(피어 디바이스)의 IP 주소를 구성합니다.
- VPN Access Interface(VPN 액세스 인터페이스) - 사이트 대 사이트 터널에 사용할 인터페이스를 선택합니다.
- Crypto Map Type(암호화 맵 유형) — 이 피어에 사용할 맵의 유형(정적 또는 동적)을 지정합니다.

Traffic to Protects(보호할 트래픽)

이 단계에서는 로컬 네트워크와 원격 네트워크를 식별할 수 있습니다. 이러한 네트워크는 IPsec 암호화를 사용하여 트래픽을 보호합니다.

- Local Networks(로컬 네트워크) - IPsec 터널에서 사용되는 호스트를 식별합니다.
- Remote Networks(원격 네트워크) - IPsec 터널에서 사용되는 네트워크를 식별합니다.

보안

이 단계에서는 피어 디바이스 인증 방법을 구성할 수 있습니다. 간단한 구성을 선택하고 사전 공유 키를 제공할 수 있습니다. 또는 다음과 같은 고급 옵션을 제공하는 Customized Configuration(사용자 정의 구성)을 선택할 수 있습니다.

- IKE Version(IKE 버전) - 사용할 버전에 따라 IKEv1 또는 IKEv2 확인란을 선택합니다.
- IKE version 1 Authentication Methods(IKE 버전 2 인증 방법)
  - Pre-shared Key(사전 공유 키) - 사전 공유 키를 사용하면 제한된 수의 원격 피어와의 통신 및 안정적인 네트워크를 빠르고 쉽게 설정할 수 있습니다. 하지만 각 IPsec 피어에 보안 연결을 설정하는 각 피어에 대한 구성 정보가 필요하므로 대규모 네트워크에서 확장성 문제가 발생할 수 있습니다.

    보안 터널을 설정하려면 각 IPsec 피어 쌍이 사전 공유 키를 교환해야 합니다. 안전한 방법을 사용하여 원격 사이트의 관리자와 사전 공유 키를 교환해 주십시오.
  - Device Certificate(디바이스 인증서) - 로컬 ASA와 원격 IPsec 피어 간의 인증에 인증서를 사용하려면 클릭합니다.

    디지털 인증서를 사용하여 IPsec 터널을 설정하는 데 사용되는 보안 키를 효율적으로 관리할 수 있습니다. 디지털 인증서에는 이름, 일련 번호, 회사, 부서, IP 주소 등 사용자 또는 디바이스를 식별하는 정보가 포함되어 있습니다. 또한 공개 키 사본도 포함되어 있습니다.

    두 피어가 통신하려면 인증서를 교환하고 데이터를 디지털로 서명하여 서로 인증해야 합니다. 네트워크에 새 피어를 추가한 경우 해당 피어가 CA에 등록하므로 다른 피어에는 추가 구성이 필요 없습니다.

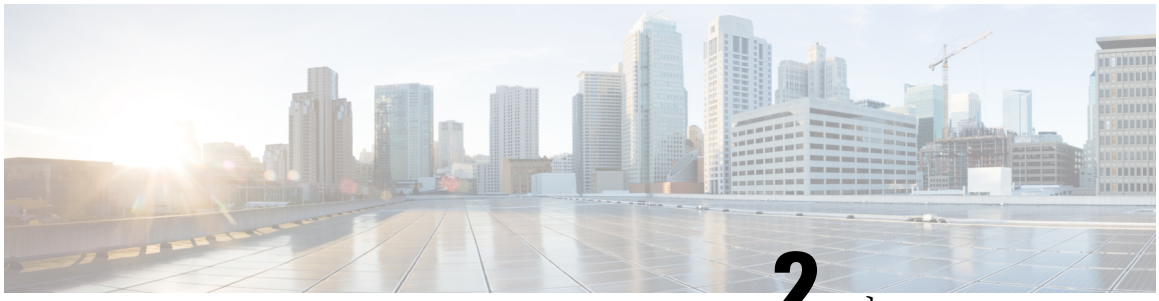
- IKE version 2 Authentication Methods(IKE 버전 2 인증 방법)
  - Local Pre-shared Key(로컬 사전 공유 키) - IPsec IKEv2 인증 방법 및 암호화 알고리즘을 지정합니다.
  - Local Device Certificate(로컬 디바이스 인증서) - 보안 어플라이언스를 통해 VPN 액세스를 인증합니다.
  - Remote Peer Pre-shared Key(원격 피어 사전 공유 키) - 로컬 ASA와 원격 IPsec 피어 간의 인증에 사전 공유 키를 사용하려면 클릭합니다.
  - Remote Peer Certificate Authentication(원격 피어 인증서 인증) - 이 옵션을 선택하면 피어 디바이스에서 인증서를 사용하여 이 디바이스에 자동으로 인증할 수 있습니다.
- Encryption Algorithms(암호화 알고리즘) - 이 탭에서는 데이터를 보호하는 데 사용되는 암호화 알고리즘 유형을 선택할 수 있습니다.
  - IKE Policy(IKE 정책) - IKEv1/IKEv2 인증 방법을 지정합니다.
  - IPsec Proposal(IPsec 제안서) - IPsec 암호화 알고리즘을 지정합니다.
- Perfect Forward Secrecy
  - Enable Perfect Forwarding Secrecy (PFS)(PFS(Perfect Forwarding Secrecy) 활성화) - Phase 2 IPsec 키 생성 시 Perfect Forward Secrecy를 사용할지 여부 및 사용할 숫자 크기를 지정합니다. PFS는 각각의 새로운 키가 이전 키와 무관한 암호화 개념입니다. PFS가 활성화되지 않은 경우 IPsec 협상에서 Phase 2 키는 Phase 1 키를 기반으로 합니다. PFS는 Diffie-Hellman 기술을 사용하여 키를 생성합니다.

    PFS는 비공개 키 중 하나가 이후에 손상된 경우에도 장기 공개 및 비공개 키 집합에서 파생된 세션 키가 손상되지 않도록 합니다.

    연결의 양쪽 모두에서 PFS를 활성화해야 합니다.
  - Diffie-Hellman Group(Diffie-Hellman 그룹) - 서로 전달하지 않고 공유 비밀을 파생하기 위해 두 IPsec 피어가 사용하는 Diffie-Hellman 그룹의 식별자를 선택합니다. 기본값인 Group 2(1024비트 Diffie-Hellman)는 CPU 실행 시간이 짧지만 Group 5(1536비트)보다 안전하지 않습니다.

NAT 제외

- Exempt ASA side host/network from address translation(주소 변환에서 ASA 쪽 호스트/네트워크 제외) - 드롭다운 목록을 사용하여 주소 변환에서 제외할 호스트 또는 네트워크를 선택합니다.



2 장

IKE

IKE 구성

ISAKMP라고도 하는 IKE는 두 개의 호스트가 IPsec 보안 연계를 구축하는 방법에 동의할 수 있도록 해주는 협상 프로토콜입니다. VPN(Virtual Private Network)에 대한 ASA를 구성하려면 전체 시스템에서 적용되는 전역 IKE 파라미터를 설정하고, VPN 연결을 설정하기 위해 피어가 협상하는 IKE 정책을 만들어야 합니다.

프로시저

단계 **1** IKE 활성화, 17 페이지.

단계 **2** 사이트 대 사이트 VPN에 대한 IKE 매개변수, 18 페이지를 설정합니다.

단계 **3** IKE 정책, 21 페이지을 구성합니다.

IKE 활성화

프로시저

단계 **1** VPN 연결에 대해 IKE를 활성화하려면 다음을 수행하십시오.

a) ASDM에서 **Configuration(**구성**) > Remote Access VPN(**원격 액세스 **VPN) > Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**) > AnyConnect Connection Profiles(AnyConnect** 연결 프로파일**)**를 선택합니다.

b) Access Interfaces(액세스 인터페이스) 영역에서 IKE를 사용할 인터페이스에 대해 IPsec (IKEv2) Access(IPsec(IKEv2) 액세스) 아래의 **Allow Access(**액세스 허용**)**를 선택합니다.

단계 **2** 사이트 대 사이트 VPN에 대해 IKE를 활성화하려면 다음을 수행하십시오.

a) ASDM에서 **Configuration(**구성**) > Site-to-Site VPN(**사이트 대 사이트 **VPN) > Connection Profiles(**연결 프로파일**)**를 선택합니다.
b) IKEv1 및 IKEv2를 사용할 인터페이스를 선택합니다.

사이트 대 사이트 **VPN**에 대한 **IKE** 매개변수

ASDM에서 **Configuration(**구성**) > Site-to-Site VPN(**사이트 대 사이트 **VPN) > Advanced(**고급**) > IKE Parameters(IKE** 파라미터**)**를 선택합니다.

NAT 투명성

- IPsec over NAT-T 활성화

  IPsec over NAT-T는 IPsec 피어가 NAT 디바이스를 통해 원격 액세스 및 LAN-to-LAN 연결을 모두 설정할 수 있도록 해줍니다. 이는 NAT 디바이스에 포트 정보를 제공하는 포트 4500을 사용하여 UDP 데이터그램 내의 IPsec 트래픽을 캡슐화하는 방법으로 수행됩니다. NAT-T는 모든 NAT 디바이스를 자동으로 탐지하며, 필요한 경우 IPsec 트래픽만 캡슐화합니다. 이 기능은 기본적으로 활성화되어 있습니다.

  - ASA는 데이터를 교환 중인 클라이언트에 따라 표준 IPsec, TCP를 통한 IPsec, NAT-T 및 UDP를 통한 IPsec을 동시에 지원할 수 있습니다.
  - NAT-T와 IPsec over UDP가 둘 다 활성화된 경우 NAT-T가 우선적으로 적용됩니다.
  - 이 기능을 활성화하면 IPsec over TCP가 다른 모든 연결 방법보다 우선적으로 적용됩니다.

  NAT-T의 ASA 구현은 다음과 같은 단일 NAT/PAT 디바이스 뒤의 IPsec 피어를 지원합니다.

  - 단일 LAN-to-LAN 연결.
  - LAN-to-LAN 연결 또는 여러 원격 액세스 클라이언트(둘 중 하나만 지원).

  NAT-T를 사용하려면 다음을 수행해 주십시오.

  - 포트 4500을 여는 데 사용할 인터페이스에 대한 ACL을 만듭니다(Configuration(구성) > Firewall(방화벽) > Access Rules(액세스 규칙)).
  - 이 창에서 IPsec over NAT-T를 활성화합니다.
  - Configuration(구성) > Site-to-Site VPN(사이트 대 사이트 VPN) > Advanced(고급) > IPsec Prefragmentation Policies(IPsec 사전 조각화 정책) 창의 Fragmentation Policy(조각화 정책) 매개변수에서 IPsec 사전 조각화를 활성화하는 데 사용할 인터페이스를 수정합니다. 이 구성을 완료한 경우 IP 조각화를 지원하지 않는 NAT 디바이스를 통해서도 여전히 트래픽을 전달할 수 있습니다. 이러한 NAT 디바이스는 IP 조각화를 지원하는 NAT 디바이스의 작업을 방해하지 않습니다.

- IPsec over TCP 활성화

IPsec over TCP는 Cisco VPN 클라이언트가 표준 ESP 또는 IKE가 작동할 수 없거나 기존 방화벽 규칙의 변경을 통해서만 작동할 수 있는 환경에서 작동할 수 있게 합니다. IPsec over TCP는 TCP와 같은 패킷 내에서 IKE 및 IPsec 프로토콜을 캡슐화하여 NAT 및 PAT 디바이스와 방화벽을 통해 안전한 터널링을 활성화합니다. 이 기능은 기본적으로 비활성화되어 있습니다.

참고 이 기능은 프록시 기반 방화벽에서 작동하지 않습니다.

IPsec over TCP는 원격 액세스 클라이언트에서 작동합니다. 모든 물리적 및 VLAN 인터페이스에서 작동합니다. ASA 기능에만 적용되는 클라이언트이며, LAN-to-LAN 연결에서 작동하지 않습니다.

- ASA는 데이터를 교환 중인 클라이언트에 따라 표준 IPsec, TCP를 통한 IPsec, NAT-Traversal 및 UDP를 통한 IPsec을 동시에 지원할 수 있습니다.
- 이 기능을 활성화하면 IPsec over TCP가 다른 모든 연결 방법보다 우선적으로 적용됩니다.

연결하는 ASA 및 클라이언트에서 TCP를 통한 IPsec을 활성화합니다.

사용자가 지정하는 최대 10개의 포트에 대해 TCP를 통한 IPsec을 활성화할 수 있습니다. 잘 알려진 포트(예: 포트 80(HTTP) 또는 포트 443(HTTPS))를 입력하면 해당 포트와 연계된 프로토콜이 더 이상 작동하지 않음을 알리는 경고가 표시됩니다. 결과적으로 IKE 지원 인터페이스를 통해 ASA를 관리하는 데 더 이상 브라우저를 사용할 수 없습니다. 이 문제를 해결하려면 HTTP/HTTPS 관리를 다른 포트로 재설정하십시오.

ASA뿐만 아니라 클라이언트에서도 TCP 포트를 구성해야 합니다. 클라이언트 구성은 ASA를 위해 설정한 포트를 최소 1개 이상 포함해야 합니다.

Identity Sent to Peer(피어로 전송되는 ID)

IKE 협상 중에 피어가 자신을 식별하는 데 사용할 **Identity(ID)**를 선택합니다.

Address	ISAKMP ID 정보를 교환하는 호스트의 IP 주소를 사용합니다.
Hostname	ISAKMP ID 정보(기본값)를 교환하는 호스트의 정규화된 도메인 이름을 사용합니다. 이 이름은 호스트 이름 및 도메인 이름으로 구성됩니다.
Key ID	원격 피어에서 지정한 **Key Id String(**키 **ID** 문자열**)**을 사용하여 사전 공유 키를 조회합니다.
Automatic	연결 유형별 IKE 협상을 결정합니다. • 사전 공유 키의 IP 주소 • 인증서 인증의 경우 Cert DN

Session Control(세션 제어**)**

- 인바운드 적극적인 모드 연결 비활성화

  Phase 1 IKE 협상에서는 Main(기본) 모드 또는 Aggressive(적극적인) 모드를 사용할 수 있습니다. 두 모드 모두 동일한 서비스를 제공하지만 Aggressive(적극적인) 모드에서는 피어 간에 세 번이 아니라 두 번의 교환만 필요합니다. 적극적인 모드가 조금 더 빠르지만 통신 당사자의 ID를 보호하지 않습니다. 따라서 정보를 암호화할 보안 SA를 설정하기 전에 식별 정보를 교환해야 합니다. 이 기능은 기본적으로 비활성화되어 있습니다.

- 연결 해제 전 피어에 알림
  - 클라이언트 또는 LAN-to-LAN 세션은 ASA 종료 또는 재부팅, 세션 유휴 시간 제한, 최대 연결 시간 초과, 관리자의 연결 차단 등 여러 가지 이유로 끊어질 수 있습니다.
  - ASA에서는 적격 피어(LAN-to-LAN 구성에서), VPN 클라이언트 및 VPN 3002 하드웨어 클라이언트에 연결이 해제되는 세션과 그 이유를 알려줄 수 있습니다. 알림을 받은 피어나 클라이언트는 원인을 디코딩하여 이벤트 로그 또는 팝업 창에 표시합니다. 이 기능은 기본적으로 비활성화되어 있습니다.
  - 이 창에서는 ASA에서 이러한 알림과 연결 해제 이유를 보낼 수 있도록 이 기능을 활성화할 수 있습니다.

  적격 클라이언트 및 피어에는 다음이 포함되어 있습니다.
  - 알림이 활성화된 보안 어플라이언스
  - 4.0 이상의 소프트웨어를 실행하는 VPN 클라이언트(구성 필요 없음)

- 재부팅하기 전에 모든 액티브 세션이 자발적으로 종료할 때까지 대기

  모든 활성 세션이 자발적으로 종료한 경우에만 ASA를 리부팅하도록 예약할 수 있습니다. 이 기능은 기본적으로 비활성화되어 있습니다.

- IKEv1 협상에서 허용되는 SA 수

  언제든지 협상에 참여할 수 있는 최대 SA 수를 제한합니다.

IKE v2 관련 설정

IKE v2에는 열려 있는 SA 수를 제한하는 추가 세션 제어를 사용할 수 있습니다. 기본적으로 ASA에서는 열려 있는 SA 수를 제한하지 않습니다.

- Cookie Challenge(쿠키 챌린지) - ASA에서 SA 초기화 패킷에 대한 응답으로 쿠키 챌린지를 피어 디바이스로 보낼 수 있도록 합니다.
  - % threshold before incoming SAs are cookie challenged(들어오는 SA에 쿠키 챌린지가 적용되기 전의 임계값(%)) - ASA에 대해 협상에서 허용되는 총 SA의 백분율이며, 이 백분율에 도달하면 이후의 모든 SA 협상에 대해 쿠키 챌린지가 트리거됩니다. 범위는 0~100%이고, 기본값은 50%입니다.

- Number of Allowed SAs in Negotiation(협상에서 허용되는 SA 수) - 언제든지 협상에 참여할 수 있는 최대 SA 수를 제한합니다. Cookie Challenge(쿠키 챌린지)와 함께 사용하는 경우 효과적인 교차 확인을 위해 쿠키 챌린지 임계값을 이 제한보다 낮은 값으로 구성합니다.
- Maximum Number of SAs Allowed(허용되는 최대 SA 수) - ASA에서 허용되는 IKEv2 연결 수를 제한합니다. 기본적으로 라이센스에 따라 지정된 최대 연결 수로 제한됩니다.
- Notify Invalid Selector(유효하지 않은 선택기 알림) - 관리자는 SA에서 해당 SA에 대한 트래픽 선택기와 일치하지 않는 인바운드 패킷을 수신하는 경우 피어에 대한 IKE 알림 전송을 활성화하거나 비활성화할 수 있습니다. 이 알림의 전송은 기본적으로 비활성화되어 있습니다.

IKE v2 관련 설정으로 **DoS** 공격 방지

들어오는 SA(Security Association)의 ID를 묻는 Cookie Challenge(쿠키 챌린지)를 구성하거나 열려 있는 SA 수를 제한하여 IPsec IKEv2 연결에 대한 DoS(Denial-of-Service) 공격을 방지할 수 있습니다. 기본적으로 ASA에서는 열려 있는 SA 수를 제한하지 않으며, SA에 대해 쿠키 챌린지를 실행하지 않습니다. 허용되는 SA 수를 제한할 수도 있습니다. 이렇게 하면 추가 연결의 협상이 중지되므로 쿠키 챌린지 기능으로 방지할 수 없는 메모리 및/또는 CPU 공격을 방지하고 현재 연결을 보호할 수 있습니다.

DoS 공격을 통해 공격자는 피어 디바이스에서 SA 초기화 패킷을 보내고 ASA에서 해당 응답을 보냈지만 피어 디바이스가 이후에 응답하지 않은 경우에 공격을 시작합니다. 피어 디바이스가 이 작업을 계속할 경우 ASA에서 가능한 전체 SA 요청 한도가 소진되어야 응답이 중단됩니다.

쿠키 챌린지에 대한 임계값 백분율을 활성화하면 열려 있는 SA 협상 수가 제한됩니다. 예를 들어 기본 설정인 50%를 사용하면 허용된 SA의 50%가 협상 중인(열려 있는) 경우 ASA에서 추가로 도착하는 모든 SA 초기화 패킷에 대해 쿠키 챌린지를 실행합니다. 허용되는 IKEv2 SA가 10,000개인 Cisco ASA 5585-X의 경우 5,000개의 SA가 열리면 추가로 들어오는 모든 SA에 쿠키 챌린지가 적용됩니다.

Number of SAs Allowed in Negotiation 또는 Maximum Number of SAs Allowed(허용되는 최대 SA 수)와 함께 사용하는 경우 효과적인 교차 확인을 위해 쿠키 챌린지 임계값을 이 제한보다 낮은 값으로 구성합니다.

또한 Configuration(구성) > Site-to-Site VPN(사이트 대 사이트 VPN) > Advanced(고급) > System Options(시스템 옵션)를 선택하여 IPsec 수준에서 모든 SA의 수명을 제한할 수 있습니다.

IKE 정책

Configuration(구성) > Site-to-Site VPN(사이트 대 사이트 VPN) > Advanced(고급) > IKE Policies(IKE 정책)

이 창을 사용하여 IKEv1 및 IKEv2 정책을 추가, 수정하거나 삭제할 수 있습니다.

IKE 협상 조건을 설정하려면 다음을 포함하는 IKE 정책을 하나 이상 만듭니다.

- 고유한 우선순위(1~65,543, 1이 우선순위가 가장 높음).
- 피어의 ID를 확인할 인증 방법
- 데이터 및 개인정보를 보호할 암호화 방법

- 보낸 사람의 ID를 확인하고 메시지가 전송 중에 수정되지 않았는지 확인할 HMAC 방법.
- 암호 키 결정 알고리즘의 장점을 확립할 Diffie-Hellman 그룹. ASA는 이 알고리즘을 사용하여 암호화 및 해시 키를 파생합니다.
- ASA에서 암호 키를 교체하지 않고 계속 사용할 수 있는 기간에 대한 제한

각 IKE 협상은 Phase1과 Phase 2라는 두 개의 섹션으로 나누어집니다. 1단계에서는 최신 IKE 협상 메시지를 보호하는 첫 번째 터널을 생성합니다. 2단계에서는 데이터를 보호하는 터널을 생성합니다.

IKEv1의 경우 각 매개변수에 대해 하나의 설정만 활성화할 수 있습니다. IKEv2의 경우 각 제안에 암호화, D-H 그룹, 무결성 해시(Integrity Hash) 및 PRF 해시에 대한 여러 설정이 있을 수 있습니다.

IKE 정책을 구성하지 않으면 ASA에서 항상 최하위 우선순위로 설정되고 각 파라미터를 기본값을 포함하는 기본 정책을 사용합니다. 특정 매개변수의 값을 지정하지 않으면 기본값이 적용됩니다.

IKE 협상이 시작되면 협상을 시작한 피어가 모든 정책을 원격 피어로 보내고 원격 피어는 우선순위대로 자신의 정책과 일치하는 정책을 검색합니다.

암호화, 해시, 인증 및 Diffie-Hellman 값이 동일하고 SA 수명이 전송된 정책의 수명보다 작거나 같으면 IKE 정책 간에 일치하는 항목이 존재하는 것으로 간주됩니다. 수명이 동일하지 않은 경우에는 원격 피어 정책의 더 짧은 수명이 적용됩니다. 일치하는 항목이 존재하지 않을 경우 IKE는 협상을 거부하고 IKE SA가 설정되지 않습니다.

필드

- IKEv1 Policies(IKEv1 정책) - 구성된 각 IKE 정책에 대한 매개변수 설정을 표시합니다.
  - Priority #(우선순위 번호) - 정책의 우선순위를 표시합니다.
  - Encryption(암호화) - 암호화 방법을 표시합니다.
  - Hash(해시) - 해시 알고리즘을 표시합니다.
  - D-H Group(D-H 그룹) - Diffie-Hellman 그룹을 표시합니다.
  - Authentication(인증) - 인증 방법을 표시합니다.
  - Lifetime (secs)(수명(초)) - SA 수명(초)을 표시합니다.
- IKEv2 Policies(IKEv2 정책) - 구성된 각 IKEv2 정책에 대한 매개변수 설정을 표시합니다.
  - Priority #(우선순위 번호) - 정책의 우선순위를 표시합니다.
  - Encryption(암호화) - 암호화 방법을 표시합니다.
  - Integrity Hash(무결성 해시) - 해시 알고리즘을 표시합니다.
  - PRF Hash(PRF 해시) - PRF(Pseudo Random Function) 해시 알고리즘을 표시합니다.
  - D-H Group(D-H 그룹) - Diffie-Hellman 그룹을 표시합니다.
  - Lifetime (secs)(수명(초)) - SA 수명(초)을 표시합니다.

IKEv1 정책 추가 또는 수정

Configuration(구성) > Site-to-Site VPN(사이트 대 사이트 VPN) > Advanced(고급) > IKE Policies(IKE 정책) > Add/Edit IKE Policy(IKE 정책 추가/수정)

Priority #(우선순위 번호) - IKE 정책에 대한 우선순위를 설정할 번호를 입력합니다. 범위는 1~65,535이며, 1이 우선순위가 가장 높습니다.

Encryption(암호화) - 암호화 방법을 선택합니다. 두 IPsec 피어 간에 전송되는 데이터를 보호하는 대칭 암호화 방법이며, 선택 항목은 다음과 같습니다.

des	56비트 DES-CBC. 다른 방법보다 안전하지 않지만 더 빠름. 기본값.
3des	168비트 삼중 DES.
aes	128비트 AES.
aes-192	192비트 AES.
aes-256	256비트 AES.

Hash(해시) - 데이터 무결성을 보장하는 해시 알고리즘을 선택합니다. 패킷이 표시된 원하는 위치에서 제대로 시작하는지, 전송 중 변경되지 않았는지 확인합니다.

sha	SHA-1	기본값은 SHA-1입니다. MD5의 다이제스트가 더 작으며, 속도는 SHA-1보다 약간 더 빠른 것으로 간주됩니다. 그러나 MD5에 대한 공격(매우 어려움)이 발생하는 경우 IKE가 사용하는 HMAC 변형이 이 공격을 방지합니다.
md5	MD5	

Authentication(인증) - 각 IPsec 피어의 ID를 설정하기 위해 ASA가 사용하는 인증 방법을 지정합니다. 사전 공유 키는 증가하는 네트워크와 잘 비례하지 않지만 소규모 네트워크에서 설치하기 쉽습니다. 선택 사항은 다음과 같습니다.

pre-share	사전 공유 키.
rsa-sig	RSA 서명 알고리즘에서 생성한 키를 사용하는 디지털 인증서.

D-H Group(D-H 그룹) - 서로 전달하지 않고 공유 비밀을 파생하기 위해 두 IPsec 피어가 사용하는 Diffie-Hellman 그룹의 식별자를 지정합니다.

1	그룹 1(768비트)	기본값인 Group 2(1024비트 Diffie-Hellman)는 CPU 실행 시간이 짧지만 Group 1 또는 5보다 안전하지 않습니다.

2	그룹 2(1024비트)	
5	그룹 5(1536비트)	

Lifetime (secs)(수명(초)) - Unlimited(무제한)를 선택하거나 SA 수명에 대한 정수를 입력합니다. 기본값은 86,400초 또는 24시간입니다. 수명이 더 길면 ASA에서 향후 IPsec 보안 연계를 설정하는 시간이 더 오래 걸립니다. 암호화 강도는 몇 분마다 한 번씩 매우 빠른 리키(rekey) 시간을 사용하지 않고도 보안을 보장할 만큼 충분히 강력합니다. 기본값을 적용하는 것이 좋습니다.

Time Measure(시간 단위) - 시간 단위를 선택합니다. ASA에서 허용되는 값은 다음과 같습니다.

120~86,400초
2~1,440분
1~24시간
1일

IKEv2 정책 추가 또는 수정

Configuration(구성) > Site-to-Site VPN(사이트 대 사이트 VPN) > Advanced(고급) > IKE Policies(IKE 정책) > Add/Edit IKEv2 Policy(IKEv2 정책 추가/수정)

Priority #(우선순위 번호) - IKEv2 정책에 대한 우선순위를 설정할 번호를 입력합니다. 범위는 1~65,535이며, 1이 우선순위가 가장 높습니다.

Encryption(암호화) - 암호화 방법을 선택합니다. 두 IPsec 피어 간에 전송되는 데이터를 보호하는 대칭 암호화 방법이며, 선택 항목은 다음과 같습니다.

des	ESP에 대해 56비트 DES-CBC 암호화를 지정합니다.
3des	(기본값) ESP에 대해 Triple DES 암호화 알고리즘을 지정합니다.
aes	ESP에 대해 128비트 키 암호화 포함 AES를 지정합니다.
aes-192	ESP에 대해 192비트 키 암호화 포함 AES를 지정합니다.
aes-256	ESP에 대해 256비트 키 암호화 포함 AES를 지정합니다.
aes-gcm	대칭 암호화 및 무결성을 위해 AES-GCM/GMAC 128비트 지원을 지정합니다.
aes-gcm-192	대칭 암호화 및 무결성을 위해 AES-GCM/GMAC 192비트 지원을 지정합니다.

aes-gcm-256	대칭 암호화 및 무결성을 위해 AES-GCM/GMAC 256비트 지원을 지정합니다.
NULL	암호화가 없음을 나타냅니다.

D-H Group(D-H 그룹) - 서로 전달하지 않고 공유 비밀을 파생하기 위해 두 IPsec 피어가 사용하는 Diffie-Hellman 그룹의 식별자를 지정합니다.

1	그룹 1(768비트)	기본값인 Group 2(1,024비트 Diffie-Hellman)는 CPU 실행 시간이 짧지만 Group 2 또는 5보다 안전하지 않습니다.
2	그룹 2(1024비트)	
5	그룹 5(1536비트)	
14	그룹 14	
19	그룹 19	
20	그룹 20	
21	그룹 21	
24	그룹 24	

Integrity Hash(무결성 해시) - ESP 프로토콜에 대한 데이터 무결성을 보장하는 해시 알고리즘을 선택합니다. 패킷이 표시된 원하는 위치에서 제대로 시작하는지, 전송 중 변경되지 않았는지 확인합니다.

sha	SHA 1	기본값은 SHA 1입니다. MD5의 다이제스트가 더 작으며, 속도는 SHA 1보다 약간 더 빠른 것으로 간주됩니다. 그러나 MD5에 대한 공격(매우 어려움)이 발생하는 경우 IKE가 사용하는 HMAC 변형이 이 공격을 방지합니다.
md5	MD5	
sha256	SHA 2, 256비트 다이제스트	256비트 다이제스트로 Secure Hash Algorithm SHA 2를 지정합니다.
sha384	**SHA 2, 384-bit digest**	384비트 다이제스트로 Secure Hash Algorithm SHA 2를 지정합니다.
sha512	**SHA 2, 512-bit digest**	512비트 다이제스트로 Secure Hash Algorithm SHA 2를 지정합니다.

null		AES-GCM 또는 AES-GMAC가 암호화 알고리즘으로 구성되었음을 나타냅니다. AES-GCM이 암호화 알고리즘으로 구성된 경우 null 무결성 알고리즘을 선택해야 합니다.

Pseudo-Random Function (PRF)(PRF(Pseudo Random Function)) - SA에서 사용되는 모든 암호화 알고리즘에 대한 키 관련 자료를 작성하는 데 사용되는 PRF를 지정합니다.

sha	SHA-1	기본값은 SHA-1입니다. MD5의 다이제스트가 더 작으며, 속도는 SHA-1보다 약간 더 빠른 것으로 간주됩니다. 그러나 MD5에 대한 공격(매우 어려움)이 발생하는 경우 IKE가 사용하는 HMAC 변형이 이 공격을 방지합니다.
md5	MD5	
sha256	SHA 2, 256비트 다이제스트	256비트 다이제스트로 Secure Hash Algorithm SHA 2를 지정합니다.
sha384	SHA 2, 384비트 다이제스트	384비트 다이제스트로 Secure Hash Algorithm SHA 2를 지정합니다.
sha512	SHA 2, 512비트 다이제스트	512비트 다이제스트로 Secure Hash Algorithm SHA 2를 지정합니다.

Lifetime (secs)(수명(초)) - Unlimited(무제한)를 선택하거나 SA 수명에 대한 정수를 입력합니다. 기본값은 86,400초 또는 24시간입니다. 수명이 더 길면 ASA에서 향후 IPsec 보안 연계를 설정하는 시간이 보다 단축됩니다. 암호화 강도는 몇 분마다 한 번씩 매우 빠른 리키(rekey) 시간을 사용하지 않고도 보안을 보장할 만큼 충분히 강력합니다. 기본값을 적용하는 것이 좋습니다.

ASA에서 허용되는 값은 다음과 같습니다.

120~86,400초
2~1,440분
1~24시간
1일

IPsec 구성

ASA는 LAN-to-LAN VPN 연결을 위해 IPsec을 사용하고 client-to-LAN VPN 연결을 위해 IPsec을 사용하는 옵션을 제공합니다. IPsec이라는 용어에서 "peer"는 원격 액세스 클라이언트 또는 다른 보안 게이트웨이입니다. ASA는 Cisco 피어(IPv4 또는 IPv6) 및 모든 관련 표준을 준수하는 타사 피어와의 LAN-to-LAN IPsec 연결을 지원합니다.

터널을 구성하는 동안 2개의 피어가 인증, 암호화, 캡슐화 및 키 관리를 제어하는 보안 연계를 협상합니다. 이 협상은 2단계로 이루어집니다. 첫 번째 단계에서는 터널(IKE SA)을 구성하고 두 번째 단계에서는 터널(IPsec SA) 내에서 트래픽을 제어합니다.

LAN-to-LAN VPN은 다양한 위치에 있는 네트워크를 연결합니다. IPsec LAN-to-LAN 연결에서 ASA가 초기자 또는 응답자로 작동할 수 있습니다. IPsec client-to-LAN 연결에서는 ASA가 응답자로만 작동합니다. 초기자는 SA를 제안하는 반면 응답자는 구성된 SA 매개변수에 따라 카운터 제안을 수락, 거절 또는 생성합니다. 연결을 설정하려면 두 엔터티가 모두 SA에 동의해야 합니다.

ASA는 다음과 같은 IPsec 속성을 지원합니다.

- 인증에 디지털 인증서를 사용할 때 1단계 ISAKMP 보안 연계를 협상하는 기본 모드
- 인증에 사전 공유 키를 사용할 때 1단계 ISAKMP SA(Security Association)를 협상하는 적극적인 모드
- 인증 알고리즘:
  - ESP-MD5-HMAC-128
  - ESP-SHA1-HMAC-160
- 인증 모드:
  - 사전 공유 키
  - X.509 디지털 인증서
- Diffie-Hellman Group 1, 2, 5
- 암호화 알고리즘:
  - AES-128, -192, -256
  - 3DES-168
  - DES-56
  - ESP-NULL
- 확장된 인증(XAuth)
- 모드 구성(ISAKMP 구성 방법이라고도 함)
- 터널 캡슐화 모드

- LZS를 사용한 IP 압축(IPCOMP)

프로시저

단계 **1** 암호화 맵, 28 페이지을 구성합니다.
단계 **2** IPsec 사전 조각화 정책, 37 페이지을 구성합니다.
단계 **3** IPsec 제안서(변형 집합), 39 페이지을 구성합니다.

암호화 맵

Configuration(구성) > Site-to-Site VPN(사이트 대 사이트 VPN) > Advanced(고급) > Crypto Maps(암호화 맵)

이 창에는 IPsec 규칙에 정의되어 있는 현재 구성된 암호화 맵이 표시됩니다. 여기에서 IPsec 규칙을 추가, 수정 및 삭제하고 위 또는 아래로 이동하고, 잘라내기, 복사 및 붙여넣기를 수행할 수 있습니다.

참고 암시적 규칙은 수정, 삭제 또는 복사할 수 없습니다. ASA에서는 동적 터널 정책으로 구성된 경우 원격 클라이언트의 트래픽 선택 제안을 암시적으로 허용합니다. 특정 트래픽 선택을 제공하여 이를 재정의할 수 있습니다.

또한 Interface(인터페이스), Source(소스), Destination(대상), Destination Service(대상 서비스) 또는 Rule Query(규칙 쿼리)를 선택하고, is(일치) 또는 contains(포함)를 선택한 다음, 필터 매개변수를 입력하여 규칙을 **Find(찾기)**할 수 있습니다(표시 필터링). 줄임표(...)를 클릭하여 선택할 수 있는 모든 기존 항목이 표시된 Browse(찾아보기) 대화 상자를 실행합니다. **Diagram(다이어그램)**을 사용하여 규칙을 그림처럼 표시합니다.

IPsec 규칙은 다음과 같이 지정합니다.

- Type: Priority(유형: 우선순위) - 규칙의 유형(정적 또는 동적) 및 해당 우선순위를 표시합니다.
- Traffic Selection(트래픽 선택)
  - # - 규칙 번호를 나타냅니다.
  - Source(소스) - Remote Side Host/Network(원격 측 호스트/네트워크) 열에 나열된 IP 주소로 트래픽이 전송된 경우 이 규칙이 적용되는 IP 주소를 나타냅니다. 세부 정보 모드(Show Detail(세부 정보 표시) 버튼 참조)에서는 주소 열에 any라는 단어가 포함된 인터페이스 이름이 표시될 수 있습니다(예: inside:any). any는 규칙에 의해 영향을 받는 내부 인터페이스의 모든 호스트를 의미합니다.
  - Destination(대상) - Security Appliance Side Host/Network(보안 어플라이언스 측 호스트/네트워크) 열에 나열된 IP 주소로 트래픽이 전송된 경우 이 규칙이 적용되는 IP 주소를 나열합니다. 세부 정보 모드(Show Detail(세부 정보 표시) 버튼 참조)에서는 주소 열에 any라는 단어가 포함된 인터페이스 이름이 표시될 수 있습니다(예: outside:any). any는 규칙에 의해 영향

을 받는 외부 인터페이스의 모든 호스트를 의미합니다. 또한 세부 정보 모드에서는 주소 열에 대괄호로 묶인 IP 주소가 표시될 수 있습니다(예: [209.165.201.1-209.165.201.30]). 이러한 주소는 변환된 주소입니다. 내부 호스트가 외부 호스트에 연결하는 경우 ASA는 내부 호스트의 주소를 풀의 주소에 매핑합니다. 호스트가 아웃바운드 연결을 생성한 후에는 ASA에서 이 주소 매핑을 유지 관리합니다. xlate라고 하는 이 주소 매핑 구조는 일정 기간 동안 메모리에서 유지됩니다.

- Service(서비스) - 규칙에 의해 지정된 서비스 및 프로토콜(TCP, UDP, ICMP 또는 IP)을 지정합니다.
- Action(작업) - IPsec 규칙의 유형(보호 또는 보호 안 함)을 지정합니다.

- Transform Set(변형 집합) - 규칙의 변형 집합을 표시합니다.
- Peer(피어) - IPsec 피어를 식별합니다.
- PFS - 규칙에 대한 PFS(Perfect Forwarding Secrecy) 설정을 표시합니다.
- NAT-T Enabled(NAT-T 활성화) - 정책에 대해 NAT 통과가 활성화되었는지 여부를 나타냅니다.
- Reverse Route Enabled(역방향 라우팅 활성화) - 정책에 대해 역방향 라우팅 주입(RRI)이 활성화되었는지 여부를 나타냅니다. RRI는 구성 시 수행되며 정적이라고 간주되어 구성이 변경될 때까지 그대로 남아 있거나 제거됩니다. ASA에서는 라우팅 테이블에 고정 경로를 자동으로 추가하고, OSPF를 사용하여 사설 네트워크 또는 경계선 라우터에 이 경로를 알립니다.
  - Dynamic(동적) — Dynamic(동적)이 지정된 경우, RRI는 IPsec 보안 연계(SA)를 성공적으로 설정할 경우 생성되며 IPsec SA가 삭제된 후에 삭제됩니다.

  참고 동적 RRI는 IKEv2 기반 정적 암호화 맵에만 적용됩니다.

- Connection Type(연결 유형) - (정적 터널 정책에만 적용.) 이 정책의 연결 유형(양방향, 시작 전용 또는 응답 전용)을 식별합니다.
- SA Lifetime(SA 수명) - 규칙의 SA 수명을 표시합니다.
- CA Certificate(CA 인증서) - 규칙의 CA 인증서를 표시합니다. 이는 정적 연결에만 적용됩니다.
- IKE Negotiation Mode(IKE 협상 모드) - IKE 협상에서 기본 모드를 사용하는지 또는 적극적인 모드를 사용하는지 표시합니다.
- Description(설명) - (선택 사항) 이 규칙에 대한 간략한 설명을 지정합니다. 기존 규칙의 경우 규칙을 추가할 때 입력한 설명입니다. 암시적 규칙에는 "Implicit rule"이라는 설명이 포함됩니다. 암시적 규칙 이외의 다른 규칙에 대한 설명을 수정하려면 이 열을 마우스 오른쪽 버튼으로 클릭하고 Edit Description(설명 수정)을 선택하거나 열을 두 번 클릭합니다.
- Enable Anti-replay window size(재전송 방지 창 크기 활성화) - 재전송 방지 창 크기를 64의 배수 단위로 64~1,028의 범위에서 설정합니다. 트래픽 셰이핑을 사용하는 계층적 QoS 정책("Rule Actions(규칙 작업) > QoS 탭" 참조)에서 우선순위 큐의 한 가지 파생 작업은 패킷 순서 변경입니다. IPsec 패킷의 경우 재전송 방지 창 내에 없는 비순차적 패킷에서는 경고 시스템 로그 메시지

를 생성합니다. 이러한 경고는 우선순위 큐의 경우 잘못된 경보가 됩니다. 재전송 방지 창 크기를 구성하면 잘못된 경보를 방지하는 데 도움이 됩니다.

- Enable IPsec Inner Routing Lookup(IPsec 내부 라우팅 조회 활성화) — 기본적으로 조회는 IPsec 터널을 통해 전송된 패킷에 대해 수행되지 않으며 패킷별 인접성 조회는 외부 ESP 패킷에 대해서만 수행됩니다. 일부 네트워크 토폴로지에서 라우팅 업데이트가 내부 패킷의 경로를 변경했지만 로컬 IPsec 터널이 계속해서 작동 중인 경우, 터널을 통과하는 패킷은 올바르게 라우팅되지 않으며 목적지에 연결하는 데 실패합니다. 이를 방지하려면 IPsec 내부 패킷에 대한 패킷별 라우팅 조회를 활성화하십시오.

IPsec 규칙 터널 정책 만들기 또는 수정(암호화 맵) - Basic(기본) 탭

이 창을 사용하여 IPsec 규칙에 대한 새 터널 정책을 정의할 수 있습니다. 여기에서 정의한 값은 **OK(**확인**)**를 클릭한 후 IPsec Rules(IPsec 규칙) 테이블에 표시됩니다. 모든 규칙은 IPsec Rules(IPsec 규칙) 테이블에 표시되는 즉시 기본적으로 활성화됩니다.

Tunnel Policy(터널 정책) 창에서는 IPsec(Phase 2) SA(security association)를 협상하는 데 사용되는 터널 정책을 정의할 수 있습니다. ASDM에서는 구성 수정 사항을 캡처하지만 **Apply(**적용**)**를 클릭할 때까지 실행 중인 구성에 저장하지 않습니다.

모든 터널 정책에서 변형 집합을 지정하고 적용되는 보안 어플라이언스 인터페이스를 식별해야 합니다. 변형 집합은 IPsec 암호화 및 암호 해독 작업을 수행하는 암호화 및 해시 알고리즘을 식별합니다. 모든 IPsec 피어가 동일한 알고리즘을 지원하는 것은 아니므로 여러 정책을 지정하고 각각에 대한 우선순위를 할당할 수도 있습니다. 그러면 보안 어플라이언스가 원격 IPsec 피어와 협상하여 두 피어 모두 지원하는 변형 집합에 동의합니다.

터널 정책은 *static(*정적*)* 또는 *dynamic(*동적*)*일 수 있습니다. 정적 터널 정책은 보안 어플라이언스에서 IPsec 연결을 허용하는 하나 이상의 원격 IPsec 피어 또는 서브네트워크를 식별합니다. 정적 정책은 보안 어플라이언스가 연결을 시작하든 원격 호스트로부터 연결 요청을 받든 상관없이 사용할 수 있습니다. 정적 정책을 사용하려면 허용된 호스트 또는 네트워크를 식별하는 데 필요한 정보를 입력해야 합니다.

동적 터널 정책은 보안 어플라이언스와의 연결을 시작하도록 허용된 원격 호스트에 대한 정보를 제공할 수 없거나 제공하지 않으려는 경우에 사용됩니다. 보안 어플라이언스를 원격 VPN 중앙 사이트 디바이스와 관련된 VPN 클라이언트로만 사용할 경우에는 동적 터널 정책을 설정할 필요가 없습니다. 동적 터널 정책은 원격 액세스 클라이언트가 VPN 중앙 사이트 디바이스 역할을 하는 보안 어플라이언스를 통해 네트워크 연결을 시작하도록 허용하려는 경우에 가장 유용합니다. 동적 터널 정책은 원격 액세스 클라이언트에 동적으로 할당된 IP 주소가 있는 경우 또는 많은 원격 액세스 클라이언트에 대해 별도의 정책을 구성하지 않으려는 경우에 유용합니다.

Configuration(구성**) > Site-to-Site VPN(**사이트 대 사이트 **VPN) > Advanced(**고급**) > Crypto Maps(**암호화 맵**) > Create / Edit IPsec Rule(IPsec** 규칙 만들기/수정**) > Tunnel Policy (Crypto Map)(**터널 정책**(**암호화 맵**)) - Basic(**기본**)**

- Interface(인터페이스) - 이 정책을 적용할 인터페이스 이름을 선택합니다.
- Policy Type(정책 유형) - 이 터널 정책의 유형(정적 또는 동적)을 선택합니다.
- Priority(우선순위) - 정책의 우선순위를 입력합니다.

- IKE Proposals (Transform Sets)(IKE 제안(변형 집합)) - IKEv1 및 IKEv2 IPsec 제안을 지정합니다.
  - IKEv1 IPsec Proposal(IKEv1 IPsec 제안) - 정책에 대한 제안(변형 집합)을 선택하고 **Add(**추가**)**를 클릭하여 액티브 변형 집합 목록으로 이동합니다. **Move Up(**위로 이동**)** 또는 **Move Down(**아래로 이동**)**을 클릭하여 목록 상자에서 제안 순서를 다시 정렬합니다. 최대 11개의 제안을 암호화 맵 항목 또는 동적 암호화 맵 항목에 추가할 수 있습니다.
  - IKEv2 IPsec Proposal(IKEv2 IPsec 제안) - 정책에 대한 제안(변형 집합)을 선택하고 **Add(**추가**)**를 클릭하여 액티브 변형 집합 목록으로 이동합니다. **Move Up(**위로 이동**)** 또는 **Move Down(**아래로 이동**)**을 클릭하여 목록 상자에서 제안 순서를 다시 정렬합니다. 최대 11개의 제안을 암호화 맵 항목 또는 동적 암호화 맵 항목에 추가할 수 있습니다.
- Peer Settings(피어 설정) - (동적 암호화 맵 항목에 대한 선택 사항) 정책에 대한 피어 설정을 구성합니다.
  - Connection Type(연결 유형) - (정적 터널 정책에만 적용.) 양방향, 시작 전용 또는 응답 전용을 선택하여 이 정책의 연결 유형을 지정합니다. LAN-to-LAN 연결의 경우 양방향 또는 응답 전용을 선택합니다(시작 전용은 제외). LAN-to-LAN 이중화에는 응답 전용을 선택합니다. Originate Only(시작 전용)를 선택한 경우 최대 10개의 중복 피어를 지정할 수 있습니다. 단방향의 경우 시작 전용 또는 응답 전용을 지정할 수 있으며, 둘 다 기본적으로 비활성화되어 있습니다.
  - IP Address of Peer to Be Added(추가할 피어의 IP 주소) - 추가할 IPsec 피어의 IP 주소를 입력합니다.
- Enable Perfect Forwarding Secrecy(PFS(Perfect Forwarding Secrecy) 활성화) - 정책에 대해 PFS(Perfect Forwarding Secrecy)를 활성화하려면 선택합니다. PFS는 각각의 새로운 키가 이전 키와 무관한 암호화 개념입니다. PFS를 지정하지 않은 경우 IPsec 협상에서 Phase 2 키는 Phase 1 키를 기반으로 합니다.
- Diffie-Hellman Group(Diffie-Hellman 그룹) - PFS를 활성화한 경우 ASA에서 세션 키를 생성하는 데 사용할 Diffie-Hellman 그룹도 선택해야 합니다. 선택 항목은 다음과 같습니다.
  - Group 1(768비트) = PFS(Perfect Forwarding Secrecy)를 사용하며, Diffie-Hellman Group 1을 사용하여 IPsec 세션 키를 생성합니다. 이때 프라임 및 생성기 번호는 768비트입니다. 이 옵션은 보다 안전하지만 더 많은 처리 오버헤드가 필요합니다.
  - Group 2(1024비트) = PFS(Perfect Forwarding Secrecy)를 사용하며, Diffie-Hellman Group 2를 사용하여 IPsec 세션 키를 생성합니다. 이때 프라임 및 생성기 번호는 1024비트입니다. 이 옵션은 Group 1보다 안전하지만 더 많은 처리 오버헤드가 필요합니다.
  - Group 5(1,536비트) = PFS(Perfect Forwarding Secrecy)를 사용하며, Diffie-Hellman Group 5를 사용하여 IPsec 세션 키를 생성합니다. 이때 프라임 및 생성기 번호는 1,536비트입니다. 이 옵션은 Group 2보다 안전하지만 더 많은 처리 오버헤드가 필요합니다.
  - Group 14 = PFS(Perfect Forwarding Secrecy)를 사용하며, IKEv2에 Diffie-Hellman Group 14를 사용합니다.
  - Group 19 = PFS(Perfect Forwarding Secrecy)를 사용하며, ECDH를 지원하기 위해 IKEv2에 Diffie-Hellman Group 19를 사용합니다.

- Group 20 = PFS(Perfect Forwarding Secrecy)를 사용하며, ECDH를 지원하기 위해 IKEv2에 Diffie-Hellman Group 20을 사용합니다.
- Group 21 = PFS(Perfect Forwarding Secrecy)를 사용하며, ECDH를 지원하기 위해 IKEv2에 Diffie-Hellman Group 21을 사용합니다.
- Group 24 = PFS(Perfect Forwarding Secrecy)를 사용하며, IKEv2에 Diffie-Hellman Group 24를 사용합니다.

IPsec 규칙 만들기/터널 정책(암호화 맵) - Advanced(고급) 탭

Configuration(구성) > Site-to-Site VPN(사이트 대 사이트 VPN) > Advanced(고급) > Crypto Maps(암호화 맵) > Create / Edit IPsec Rule(IPsec 규칙 만들기/수정) > Tunnel Policy (Crypto Map)(터널 정책(암호화 맵)) - Advanced(고급)

- Enable NAT-T(NAT-T 활성화) - 이 정책에 대해 NAT-T(NAT Traversal)를 활성화합니다.
- Enable Reverse Route Injection(역방향 라우팅 주입 활성화) - 이 정책에 대해 역방향 라우팅 주입을 활성화합니다. RRI(Reverse Route Injection)는 원격 VPN 클라이언트 또는 LAN to LAN 세션에서 ASA 또는 RIP(Routing Information Protocol)를 실행하는 경우 OSPF(Open Shortest Path First), EIGRP(Enhanced Interior Gateway Routing Protocol)와 같은 동적 라우팅 프로토콜을 실행하는 내부 라우터의 라우팅 테이블을 채우는 데 사용됩니다. RRI는 구성 시 수행되며 정적이라고 간주되어 구성이 변경될 때까지 그대로 남아 있거나 제거됩니다. ASA에서는 라우팅 테이블에 고정 경로를 자동으로 추가하고, OSPF를 사용하여 사설 네트워크 또는 경계선 라우터에 이 경로를 알립니다.
  - Dynamic(동적) — Dynamic(동적)이 지정된 경우, RRI는 IPsec 보안 연계(SA)를 성공적으로 설정할 경우 생성되며 IPsec SA가 삭제된 후에 삭제됩니다. 일반적으로 RRI 경로는 경로가 없고 트래픽을 암호화해야 하는 경우 터널을 시작하는 데 사용됩니다. 동적 RRI가 지원되는 경우, 터널을 가져오기 전에 경로가 없습니다. 따라서, 동적 RRI가 구성된 ASA는 일반적으로 응답자로 작동합니다.

  참고 동적 RRI는 IKEv2 기반 정적 암호화 맵에만 적용됩니다.

- Security Association Lifetime Settings(보안 연계 수명 설정) - SA(Security Association) 기간을 구성합니다. 이 매개변수는 IPsec SA 키의 수명(IPsec SA가 만료되어 새 키로 재협상해야 할 때까지 지속되는 기간)을 측정하는 방법을 지정합니다.
  - Time(시간) - SA 수명을 시(hh), 분(mm), 초(ss) 단위로 지정합니다.
  - Traffic Volume(트래픽 양) - SA 수명을 트래픽 양(KB)으로 정의합니다. IPsec SA가 만료되는 페이로드 데이터의 킬로바이트 수를 입력합니다. 최소값은 100KB이고, 기본값은 10,000KB이며, 최대값은 2,147,483,647KB입니다.
- Static Type Only Settings(정적 유형 전용 설정) - 정적 터널 정책의 매개변수를 지정합니다.

- Device Certificate(디바이스 인증서) - 사용할 인증서를 선택합니다. 기본값인 None(없음) 이외의 값(Use Preshared Keys(사전 공유 키 사용))을 선택한 경우에 적용됩니다. None(없음) 이외의 값을 선택하면 Send CA certificate chain(CA 인증서 체인 보내기) 확인란이 활성화됩니다.
- Send CA certificate chain(CA 인증서 체인 보내기) - 전체 신뢰 지점 체인 전송이 활성화됩니다.
- IKE Negotiation Mode(IKE 협상 모드) - IKE 협상 모드(Main(주요) 또는 Aggressive(적극적인))를 선택합니다. 이 매개변수는 키 정보를 교환하고 SA를 설정할 모드를 설정합니다. 또한 협상 초기자가 사용하는 모드를 설정합니다. 응답자는 자동으로 협상됩니다. Aggressive Mode(적극적인 모드)는 사용하는 패킷 및 교환이 적으므로 더 빠르지만 통신 당사자의 ID를 보호하지 않습니다. Main Mode(기본 모드)는 사용하는 패킷과 교환이 많으므로 더 느리지만 통신 당사자의 ID를 보호합니다. 이 모드가 더 안전하고 기본적으로 선택됩니다. Aggressive(적극적인)를 선택하면 Diffie-Hellman Group(Diffie-Hellman 그룹) 목록이 활성화됩니다.
- Diffie-Hellman Group(Diffie-Hellman 그룹) - 적용할 Diffie-Hellman 그룹을 선택합니다. Group 1(768비트), Group 2(1,024비트) 또는 Group 5(1,536-비트)를 선택할 수 있습니다.

- ESP v3 - 들어오는 ICMP 오류 메시지가 암호화 및 동적 암호화 맵에 대해 검증되는지 여부를 지정하거나, 보안 연계별 정책을 설정하거나, 트래픽 흐름 패킷을 활성화합니다.
  - Validate incoming ICMP error messages(들어오는 ICMP 오류 메시지 검증) - IPsec 터널을 통해 수신되고 비공개 네트워크의 내부 호스트로 전달되는 이러한 ICMP 오류 메시지를 검증할지 여부를 선택합니다.
  - Enable Do Not Fragment (DF) policy(DF(조각화 금지) 정책 활성화) - IPsec 하위 시스템에서 IP 헤더에 DF(Do Not Fragment) 비트가 설정된 대용량 패킷을 처리하는 방법을 정의합니다. 다음 중 하나를 선택합니다.

    Clear DF bit(DF 비트 지우기**)** - DF 비트를 무시합니다.

    Copy DF bit(DF 비트 복사**)** - DF 비트를 유지합니다.

    Set DF bit(DF 비트 설정**)** - DF 비트를 설정하고 사용합니다.
  - Enable Traffic Flow Confidentiality (TFC) packets(TFC(Traffic Flow Confidentiality) 패킷 활성화) - 터널을 우회하는 트래픽 프로파일을 마스킹하는 더미 TFC 패킷을 활성화합니다.

    참고 TFC를 활성화하기 전에 터널 정책(암호화 맵) Basic(기본) 탭에서 IKE v2 IPsec 제안을 설정해야 합니다.

    Burst(버스트), Payload Size(페이로드 크기) 및 Timeout(시간 제한) 매개변수를 사용하여 지정된 SA에서 무작위 간격으로 임의 길이의 패킷을 생성할 수 있습니다.

IPsec 규칙 만들기 또는 수정 트래픽 선택 탭

Configuration(구성**) > Site-to-Site VPN(**사이트 대 사이트 **VPN) > Advanced(**고급**) > Crypto Maps(**암호화 맵**) > Create / Edit IPsec Rule(IPsec** 규칙 만들기/수정**) > Traffic Selection(**트래픽 선택**)**

이 창에서는 보호하거나(허용) 보호하지 않을(거부) 트래픽을 정의할 수 있습니다.

- Action(작업) - 이 규칙에서 수행할 작업을 지정합니다. 보호 또는 보호 안 함을 선택할 수 있습니다.
- Source(소스) - 소스 호스트 또는 네트워크의 IP 주소, 네트워크 개체 그룹 또는 인터페이스 IP 주소를 지정합니다. 규칙에서는 동일한 주소를 소스와 대상 둘 다로 사용할 수 없습니다. 줄임표(...)를 클릭하여 다음 필드가 포함된 Browse Source(소스 찾아보기) 대화 상자를 실행합니다.
  - Add/Edit(추가/수정) - 추가 소스 주소 또는 그룹을 추가할 IP 주소 또는 네트워크 개체 그룹을 선택합니다.
  - Delete(삭제) - 항목을 삭제하려면 클릭합니다.
  - Filter(필터) - 표시되는 결과를 필터링할 IP 주소를 입력합니다.
  - Name(이름) - 뒤에 오는 매개변수가 소스 호스트 또는 네트워크의 이름으로 지정됩니다.
  - IP Address(IP 주소) - 뒤에 오는 매개변수가 소스 호스트 또는 네트워크의 인터페이스, IP 주소 및 서브넷 마스크로 지정됩니다.
  - Netmask(넷마스크) - IP 주소에 적용할 표준 서브넷 마스크를 선택합니다. 이 매개변수는 IP Address(IP 주소) 옵션 버튼을 선택한 경우에 표시됩니다.
  - Description(설명) - 설명을 입력합니다.
  - Selected Source(선택한 소스) - **Source(**소스**)**를 클릭하여 선택한 항목을 소스로 포함합니다.
- Destination(대상) - 대상 호스트 또는 네트워크의 IP 주소, 네트워크 개체 그룹 또는 인터페이스 IP 주소를 지정합니다. 규칙에서는 동일한 주소를 소스와 대상 둘 다로 사용할 수 없습니다. 줄임표(...)를 클릭하여 다음 필드가 포함된 Browse Destination(대상 찾아보기) 대화 상자를 실행합니다.
  - Add/Edit(추가/수정) - 추가 대상 주소 또는 그룹을 추가할 IP 주소 또는 네트워크 개체 그룹을 선택합니다.
  - Delete(삭제) - 항목을 삭제하려면 클릭합니다.
  - Filter(필터) - 표시되는 결과를 필터링할 IP 주소를 입력합니다.
  - Name(이름) - 뒤에 오는 매개변수가 대상 호스트 또는 네트워크의 이름으로 지정됩니다.
  - IP Address(IP 주소) - 뒤에 오는 매개변수가 대상 호스트 또는 네트워크의 인터페이스, IP 주소 및 서브넷 마스크로 지정됩니다.
  - Netmask(넷마스크) - IP 주소에 적용할 표준 서브넷 마스크를 선택합니다. 이 매개변수는 IP Address(IP 주소) 옵션 버튼을 선택한 경우에 표시됩니다.
  - Description(설명) - 설명을 입력합니다.

  - Selected Destination(선택한 대상) - **Destination(**대상**)**을 클릭하여 선택한 항목을 대상으로 포함합니다.

- Service(서비스) - 서비스를 입력하거나 줄임표(...)를 클릭하여 서비스 목록에서 선택할 수 있는 Browse Service(서비스 찾아보기) 대화 상자를 실행합니다.
- Description(설명) - 트래픽 선택 항목에 대한 설명을 입력합니다.
- 추가 옵션
  - Enable Rule(규칙 활성화) - 이 규칙을 활성화하려면 클릭합니다.
  - Source Service(소스 서비스) - 서비스를 입력하거나 줄임표(**...**)를 클릭하여 서비스 목록에서 선택할 수 있는 Browse Service(서비스 찾아보기) 대화 상자를 실행합니다.
  - Time Range(시간 범위) - 이 규칙이 적용되는 시간 범위를 정의합니다.
  - Group(그룹) - 뒤에 오는 매개변수가 소스 호스트 또는 네트워크의 인터페이스 및 그룹 이름으로 지정됩니다.
  - Interface(인터페이스) - IP 주소의 인터페이스 이름을 선택합니다. 이 매개변수는 IP Address(IP 주소) 옵션 버튼을 선택한 경우에 표시됩니다.
  - IP Address(IP 주소) - 이 정책이 적용되는 인터페이스의 IP 주소를 지정합니다. 이 매개변수는 IP Address(IP 주소) 옵션 버튼을 선택한 경우에 표시됩니다.
  - Destination(대상) - 소스나 대상 호스트 또는 네트워크의 IP 주소, 네트워크 개체 그룹 또는 인터페이스 IP 주소를 지정합니다. 규칙에서는 동일한 주소를 소스와 대상 둘 다로 사용할 수 없습니다. 이러한 필드 중 하나에 대한 줄임표(**...**)를 클릭하여 다음 필드가 포함된 Browse(찾아보기) 대화 상자를 실행합니다.
  - Name(이름) - 소스 또는 대상 호스트나 네트워크로 사용할 인터페이스 이름을 선택합니다. 이 매개변수는 Name(이름) 옵션 버튼을 선택한 경우에 표시됩니다. 이 매개변수만 이 옵션과 연계되어 있습니다.
  - Interface(인터페이스) - IP 주소의 인터페이스 이름을 선택합니다. Group(그룹) 옵션 버튼을 클릭하면 이 매개변수가 표시됩니다.
  - Group(그룹) - 소스 또는 대상 호스트나 네트워크의 지정된 인터페이스에서 그룹 이름을 선택합니다. 목록에 포함된 항목이 없는 경우 기존 그룹의 이름을 입력할 수 있습니다. Group(그룹) 옵션 버튼을 클릭하면 이 매개변수가 표시됩니다.
- **Protocol and Service(**프로토콜 및 서비스**)** - 이 규칙과 관련된 프로토콜 및 서비스 매개변수를 지정합니다.

참고 "Any - any" IPsec 규칙은 허용되지 않습니다. 이 규칙 유형은 디바이스와 해당 피어가 여러 LAN-to-LAN 터널을 지원하지 못하도록 합니다.

- TCP - 이 규칙이 TCP 연결에 적용되도록 지정합니다. 이 항목을 선택하면 Source Port(소스 포트) 및 Destination Port(대상 포트) 그룹 상자도 표시됩니다.
- UDP - 이 규칙이 UDP 연결에 적용되도록 지정합니다. 이 항목을 선택하면 Source Port(소스 포트) 및 Destination Port(대상 포트) 그룹 상자도 표시됩니다.
- ICMP - 이 규칙이 ICMP 연결에 적용되도록 지정합니다. 이 항목을 선택하면 ICMP Type(ICMP 유형) 그룹 상자도 표시됩니다.
- IP - 이 규칙이 IP 연결에 적용되도록 지정합니다. 이 항목을 선택하면 IP Protocol(IP 프로토콜) 그룹 상자도 표시됩니다.
- Manage Service Groups(서비스 그룹 관리) - Manage Service Groups(서비스 그룹 관리) 창을 표시합니다. 이 창에서 TCP/UDP 서비스/포트 그룹을 추가, 수정 또는 삭제할 수 있습니다.
- Source Port and Destination Port(소스 포트 및 대상 포트) - Protocol and Service(프로토콜 및 서비스) 그룹 상자에서 선택한 옵션 버튼에 따라 TCP 또는 UDP 포트 매개변수를 포함합니다.
- Service(서비스) - 개별 서비스에 대한 매개변수를 지정합니다. 필터를 적용할 때 사용할 서비스 및 부울 연산자의 이름을 지정합니다.
- Boolean operator (unlabeled)(부울 연산자(레이블 없음)) - 서비스 상자에 지정된 서비스와 일치하는지 확인하는 데 사용할 부울 조건(같음, 같지 않음, 보다 큼, 보다 작음 또는 범위)을 나열합니다.
- Service (unlabeled)(서비스(레이블 없음)) - 일치하는지 확인해야 하는 서비스(예: https, kerberos 또는 any)를 식별합니다. 범위 서비스 연산자를 지정한 경우 이 매개변수는 범위의 시작 및 끝을 입력할 수 있는 두 개의 상자로 제공됩니다.
- … - Service(서비스) 상자에 표시할 서비스를 선택할 수 있는 서비스 목록을 표시합니다.
- Service Group(서비스 그룹) - 소스 포트에 대한 서비스 그룹의 이름을 지정합니다.
- Service (unlabeled)(서비스(레이블 없음)) - 사용할 서비스 그룹을 선택합니다.
- ICMP Type(ICMP 유형) - 사용할 ICMP 유형을 지정합니다. 기본값은 any입니다. 줄임표(**...**) 버튼을 클릭하면 사용 가능한 유형 목록이 표시됩니다.

• 옵션

- Time Range(시간 범위) - 기존 시간 범위의 이름을 지정하거나 새 범위를 만듭니다.
- … - 새 시간 범위를 정의할 수 있는 Add Time Range(시간 범위 추가) 창을 표시합니다.
- Please enter the description below (optional)(아래에 설명을 입력하십시오(선택 사항).) - 규칙에 대한 간략한 설명을 입력할 수 있는 공간을 제공합니다.

IPsec 사전 조각화 정책

Configuration(구성) > Site-to-Site VPN(사이트 대 사이트 VPN) > Advanced(고급) > IKE Prefragmentation Policies(IKE 조각화 정책)

IPsec 사전 조각화 정책에서는 공개 인터페이스를 통해 트래픽을 터널링할 때 MTU(Maximum Transmission Unit) 설정을 초과하는 패킷을 처리하는 방법을 지정합니다. 이 기능을 사용하면 ASA와 클라이언트 사이의 라우터 또는 NAT 디바이스가 IP 조각화를 거부하거나 무시하는 경우를 처리할 수 있습니다. 예를 들어 클라이언트가 ASA 뒤에 있는 FTP 서버에서 FTP를 가져오는 경우를 가정해 보겠습니다. FTP 서버가 캡슐화된 경우 공개 인터페이스에서 ASA의 MTU 크기를 초과할 수 있는 패킷을 전송합니다. 선택한 옵션에 따라 ASA에서 이러한 패킷을 처리하는 방법이 결정됩니다. 사전 조각화 정책은 ASA 공개 인터페이스 외부로 전달되는 모든 트래픽에 적용됩니다.

ASA에서는 터널링된 모든 패킷을 캡슐화합니다. 캡슐화 후 ASA에서는 MTU 설정을 초과하는 패킷을 조각화한 후 공유 인터페이스를 통해 전송합니다. 이것이 기본 정책입니다. 이 옵션은 조각화된 패킷이 방해 없이 터널을 통과하도록 허용되는 경우에 적용됩니다. FTP 예의 경우 대용량 패킷은 캡슐화된 다음 IP 계층에서 조각화됩니다. 중간 디바이스는 조각화를 무시하거나 단순히 비순차적으로 처리할 수도 있습니다. 로드 밸런싱 디바이스는 비순차적 조각화를 발생시킬 수 있습니다.

사전 조각화를 활성화한 경우 ASA에서는 MTU 설정을 초과하는 터널링된 패킷을 조각화한 다음 캡슐화합니다. 이러한 패킷에 대해 DF 비트가 설정된 경우에는 ASA에서 DF 비트를 제거하고 패킷을 조각화한 다음 캡슐화합니다. 이 작업은 공개 인터페이스 외부로 전달되는 조각화되지 않은 두 개의 독립된 IP 패킷을 만들며, 조각화를 피어 사이트에서 다시 어셈블할 완전한 패킷으로 전환하여 이러한 패킷을 피어 사이트로 전송합니다. 위 예의 경우 ASA에서는 MTU를 재정의하고, DF 비트를 제거하여 조각화를 허용합니다.

참고 임의의 인터페이스에서 MTU 또는 사전 조각화 옵션을 변경하면 모든 기존 연결이 해제됩니다. 예를 들어 액티브 터널 100개가 공개 인터페이스에서 종료되는 경우 외부 인터페이스에서 MTU 또는 사전 조각화 옵션을 변경하면 공개 인터페이스의 모든 액티브 터널이 무시됩니다.

이 창을 사용하여 상위 창에서 선택한 인터페이스에 대한 기존 IPsec 사전 조각화 정책 및 DF(Do Not Fragment) 비트 정책을 보거나 **Edit(수정)**할 수 있습니다.

필드

- Interface(인터페이스) - 선택한 인터페이스를 식별합니다. 이 대화 상자를 사용하여 이 매개변수를 변경할 수 없습니다.
- Enable IPsec pre-fragmentation(IPsec 사전 조각화 수정) - IPsec 사전 조각화를 활성화하거나 비활성화합니다. ASA에서는 MTU 설정을 초과하는 터널링된 패킷을 조각화한 다음 캡슐화합니다. 이러한 패킷에 대해 DF 비트가 설정된 경우에는 ASA에서 DF 비트를 제거하고 패킷을 조각화한 다음 캡슐화합니다. 이 작업은 공개 인터페이스 외부로 전달되는 조각화되지 않은 두 개의 독립된 IP 패킷을 만들며, 조각화를 피어 사이트에서 다시 어셈블할 완전한 패킷으로 전환하여 이러한 패킷을 피어 사이트로 전송합니다.
- DF Bit Setting Policy(DF 비트 설정 정책) - 조각화 금지 비트 정책(Copy(복사), Clear(지우기) 또는 Set(설정)).

IKEv2 조각화 옵션 구성

ASA에서 IKEv2 조각화를 활성화하거나 비활성화할 수 있고, IKEv2 패킷을 조각화할 때 사용되는 MTU(Maximum Transmission Unit)를 지정할 수 있으며, 관리자가 다음 화면에서 기본 조각화 메소드를 구성할 수 있습니다.

Configuration(구성**)** > **Site-to-Site VPN(**사이트 대 사이트 **VPN)** > **Advanced(**고급**)** > **IKE Parameters(IKE** 파라미터**)**를 선택합니다.

기본적으로 IKEv2 조각화의 모든 메소드가 활성화되면 MTU는 IPv4의 경우 576, IPv6의 경우 1280이고, 메소드는 IETF 표준 RFC-7383를 사용하는 것이 좋습니다.

다음 사항을 고려하여 MTU를 지정합니다.

- 사용되는 MTU 값에는 IP(IPv4/IPv6) 헤더 + UDP 헤더 크기를 포함해야 합니다.
- 관리자가 지정하지 않은 경우 기본 MTU는 IPv4의 경우 576, IPv6의 경우 1280입니다.
- 지정한 경우에는 IPv4와 IPv6 모두에 대해 동일한 MTU가 사용됩니다.
- 유효한 범위는 68-1500입니다.

지원되는 다음 조각화 메소드 중 하나를 IKEv2에 대한 기본 조각화 메소드로 구성할 수 있습니다.

- IETF RFC-7383 표준 기반 IKEv2 조각화.
  - 협상 중에 두 피어 모두 지원 및 기본 설정을 지정하는 경우 이 메소드를 사용됩니다.
  - 이 메소드를 사용하면 각 IKEv2 Fragment(IKEv2 조각화) 메시지에 대한 개별 보호를 제공하는 조각화 후에 암호화가 수행됩니다.
- Cisco의 독점 조각화입니다.
  - 이 메소드가 AnyConnect 클라이언트와 같은 피어가 제공하는 유일한 메소드이거나 두 피어 모두 협상 중에 지원 및 기본 설정을 지정하는 경우 이 메소드가 사용됩니다.
  - 이 메소드를 사용하면 암호화 후에 조각화가 수행됩니다. 모든 조각화를 수신할 때까지 수신 피어가 암호를 해독하거나 메시지를 인증할 수 없습니다.
  - 이 방법은 Cisco 이외의 피어와 상호 운용될 수 없습니다.

시작하기 전에

- 경로 MTU 검색은 지원되지 않으므로, MTU를 네트워크의 요구 사항에 맞게 수동으로 구성해야 합니다.
- 이 구성은 전역으로, 구성을 적용한 후에 설정되는 향후의 SA에 영향을 줍니다. 이전 SA에는 영향을 주지 않습니다. 조각화가 비활성화되면 동일한 동작이 일어납니다.
- 최대 100개의 프래그멘트를 수신할 수 있습니다.

프로시저

단계 1 ASDM에서 **Configuration(**구성**)** > **Site-to-Site VPN(**사이트 대 사이트 **VPN)** > **Advanced(**고급**)** > **IKE Parameters(IKE** 파라미터**)**를 선택합니다.

단계 2 **Enable fragmentation(**조각화 활성화**)** 필드를 선택하거나 선택을 취소합니다.

단계 3 **Fragmentation MTU(**조각화 **MTU)** 크기를 지정합니다.

단계 4 **Preferred fragmentation method(**기본 조각화 메소드**)**를 지정합니다.

IPsec 제안서(변형 집합)

Configuration(구성**) > Site-to-Site VPN(**사이트 대 사이트 **VPN) > Advanced(**고급**) > IPsec Proposals (Transform Sets)(IPsec** 제안서**)(**변형 집합**))**

변형은 데이터 인증, 데이터 기밀성 및 데이터 압축을 제공하기 위해 데이터 흐름에서 수행되는 작업 집합입니다. 예를 들어 한 가지 변형은 3DES 암호화 및 HMAC-MD5 인증 알고리즘을 갖춘 ESP 프로토콜(ESP-3DES-MD5)입니다.

이 창을 사용하여 아래에 설명된 IKEv1 및 IKEv2 변형 집합을 보고, **Add(**추가**)**, **Edit(**수정**)** 또는 **Delete(**삭제**)**할 수 있습니다. 각 테이블에는 구성된 변형 집합의 이름 및 세부사항이 표시됩니다.

IPsec IKEv1 제안서(변형 집합)

- **Mode(**모드**)** - ESP 암호화 및 인증을 적용하기 위한 모드입니다. 이는 원래 IP 패킷의 어느 부분에 ESP가 적용되어 있는지 결정합니다.
  - **Tunnel(**터널**)** 모드 - (기본값) 전체 원래 IP 패킷(IP 헤드 및 데이터)에 ESP 암호화 및 인증을 적용하여 최종 소스 및 대상 주소를 숨깁니다. 원래 IP 데이터그램 전체가 암호화되어 있으며 새 IP 패킷에서 페이로드가 됩니다. 이 모드에서는 라우터와 같은 네트워크 디바이스가 IPsec 프록시 역할을 합니다. 즉, 라우터는 호스트를 대신하여 암호화를 수행합니다. 소스 라우터는 패킷을 암호화하고 IPsec 터널을 따라 패킷을 전달합니다. 대상 라우터는 원래 IP 데이터그램을 암호 해독하고 대상 시스템으로 전달합니다. 터널 모드의 주요 장점은 IPsec이 보장하는 이점을 위해 최종 시스템을 수정할 필요가 없다는 점입니다. 터널 모드는 또한 트래픽 분석으로부터 보호 기능을 제공하므로 터널 모드를 통해 공격자는 터널 엔드포인트만 판단할 수 있으며 터널링된 패킷이 터널 엔드포인트와 동일하더라도 해당 소스 및 대상은 판단할 수 없습니다.
  - **Transport(**전송**)** 모드 - IP 페이로드만 암호화되며 원래 IP 헤더는 그대로 유지됩니다. 이 모드는 적은 바이트만 각각의 패킷에 추가하고 공용 네트워크에서 디바이스가 패킷의 최종 소스 및 대상을 확인할 수 있다는 이점이 있습니다. 전송 모드를 사용하면 IP 헤더의 정보에 기반하여 중간 네트워크에서 특수 처리(예: QoS)를 활성화할 수 있습니다. 그러나 패킷 검사를 제한하는 계층 4 헤더가 암호화되었습니다.
- **ESP Encryption(ESP** 암호화**)** - 변형 집합에 대한 ESP(Encapsulating Security Protocol) 암호화 알고리즘입니다. ESP는 데이터 프라이버시 서비스, 선택적 데이터 인증 및 재전송 방지 서비스를 제공하며, 보호할 데이터를 캡슐화합니다.

- **ESP Authentication(ESP** 인증**)** - 변형 집합에 대한 ESP 인증 알고리즘입니다.

IPsec IKEv2 제안서

- **Mode(**모드**)** - ESP 암호화 및 인증을 적용하기 위한 모드입니다. 이는 원래 IP 패킷의 어느 부분에 ESP가 적용되어 있는지 결정합니다.
  - **Tunnel(**터널**)** 모드 - (기본값) 캡슐화 모드가 터널 모드가 됩니다. Tunnel(터널) 모드는 전체 원래 IP 패킷(IP 헤드 및 데이터)에 ESP 암호화 및 인증을 적용하여 최종 소스 및 대상 주소를 숨깁니다. 원래 IP 데이터그램 전체가 암호화되어 있으며 새 IP 패킷에서 페이로드가 됩니다.

    이 모드에서는 라우터와 같은 네트워크 디바이스가 IPsec 프록시 역할을 합니다. 즉, 라우터는 호스트를 대신하여 암호화를 수행합니다. 소스 라우터는 패킷을 암호화하고 IPsec 터널을 따라 패킷을 전달합니다. 대상 라우터는 원래 IP 데이터그램을 암호 해독하고 대상 시스템으로 전달합니다.

    터널 모드의 주요 장점은 IPsec이 보장하는 이점을 위해 최종 시스템을 수정할 필요가 없다는 점입니다. 터널 모드는 또한 트래픽 분석으로부터 보호 기능을 제공하므로 터널 모드를 통해 공격자는 터널 엔드포인트만 판단할 수 있으며 터널링된 패킷이 터널 엔드포인트와 동일하더라도 해당 소스 및 대상은 판단할 수 없습니다.
  - **Transport(**전송**)** 모드 - 피어가 지원하지 않는 경우 캡슐화 모드는 터널 모드에 대한 폴백 옵션을 사용하는 전송 모드가 됩니다. Transport(전송) 모드에서는 IP 페이로드만 암호화되며 원래 IP 헤더는 그대로 유지됩니다.

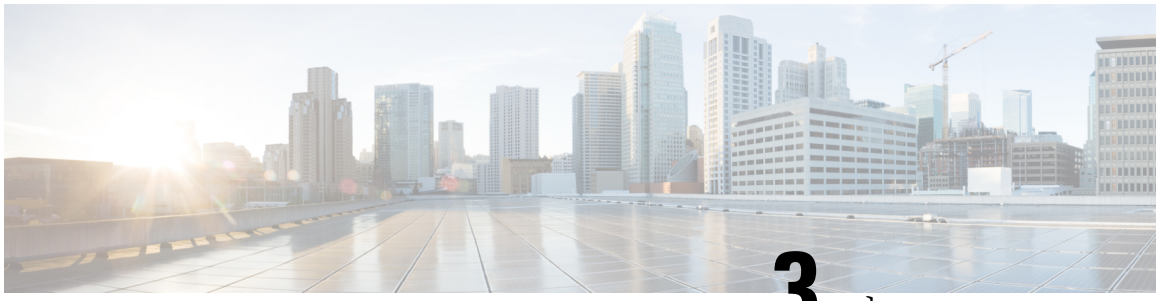
    이 모드는 적은 바이트만 각각의 패킷에 추가하고 공용 네트워크에서 디바이스가 패킷의 최종 소스 및 대상을 확인할 수 있다는 이점이 있습니다. 전송 모드를 사용하면 IP 헤더의 정보에 기반하여 중간 네트워크에서 특수 처리(예: QoS)를 활성화할 수 있습니다. 그러나 패킷 검사를 제한하는 레이어 4 헤더가 암호화됩니다.
  - 전송 필요 - 캡슐화 모드가 전송 모드만 되며, 터널 모드의 폴백이 허용되지 않습니다.

참고 원격 액세스 VPN에는 전송 모드가 권장되지 않습니다.

캡슐화 모드의 협상의 예는 다음과 같습니다.

- 이니시에이터가 전송 모드를 제안하고 응답자가 터널 모드를 사용하여 응답하는 경우 이니시에이터가 터널 모드로 폴백됩니다.
- 이니시에이터가 터널 모드를 제안하고 응답자가 전송 모드를 사용하여 응답하는 경우 응답자가 터널 모드로 폴백됩니다.
- 이니시에이터가 터널 모드를 제안하고 응답자가 전송-필수 모드에 있는 경우 선택한 제안이 응답자에 의해 전송되지 않습니다.
- 마찬가지로 이니시에이터가 전송-필수 모드에 있고 응답자가 터널 모드에 있는 경우 선택한 제안이 응답자에 의해 전송되지 않습니다.

- **Encryption(**암호화**)** - IKEv2 IPsec 제안에 대한 ESP(Encapsulating Security Protocol) 암호화 알고리즘을 표시합니다. ESP는 데이터 프라이버시 서비스, 선택적 데이터 인증 및 재전송 방지 서비스를 제공하며, 보호할 데이터를 캡슐화합니다.
- **Integrity Hash(**무결성 해시**)** - ESP 프로토콜에 대한 데이터 무결성을 보장하는 해시 알고리즘을 표시합니다. 패킷이 예상한 대상으로부터 들어오고 전송 중에 수정되지 않았는지 확인합니다. 패킷이 예상한 대상으로부터 들어오고 전송 중에 수정되지 않았는지 확인합니다. AES-GCM/GMAC가 암호화 알고리즘으로 구성된 경우 null 무결성 알고리즘을 선택해야 합니다.



3 장

고가용성 옵션

고가용성 옵션

로드 밸런싱과 장애 조치는 고가용성 기능이지만 서로 다르게 작동하고 요건도 다릅니다. 경우에 따라 구축 시 여러 기능을 사용할 수 있습니다. 다음 섹션에서는 이러한 기능에 대해 설명합니다. 장애 조치에 대한 자세한 내용 ASA 일반 운영 ASDM 구성 가이드의 적절한 릴리스를 참조하십시오. 로드 밸런싱에 대한 자세한 내용은 여기에 포함되어 있습니다.

부하 균형

부하 균형은 가상 클러스터의 디바이스 간에 원격 액세스 VPN 트래픽을 균등하게 분산시키는 메커니즘입니다. 처리량이나 기타 요인을 고려하지 않고 트래픽의 단순한 분산을 기반으로 합니다. 부하 균형 클러스터는 둘 이상의 디바이스로 구성되며, 그 중 하나는 가상 마스터이고 나머지는 백업입니다. 이러한 디바이스는 정확히 동일한 유형이거나 동일한 소프트웨어 버전 또는 구성일 필요가 없습니다.

가상 클러스터의 모든 활성 디바이스는 세션 부하를 수반합니다. 부하 균형은 클러스터에서 부하가 가장 적은 디바이스로 트래픽을 디렉션하여 모든 디바이스 간에 부하를 분산시킵니다. 따라서 시스템 리소스가 효율적으로 사용되며, 성능 및 고가용성이 증가합니다.

페일오버

장애 조치 구성에는 전용 장애 조치 링크 및 선택적 상태 저장 장애 조치 링크를 통해 서로 연결된 두 개의 동일한 ASA가 필요합니다. 액티브 인터페이스 및 유닛의 상태를 모니터링하여 특정 장애 조치 조건이 충족되는 시점을 확인합니다. 이러한 조건이 충족되면 장애 조치가 발생합니다. 장애 조치에서는 VPN 구성과 방화벽 구성을 둘 다 지원합니다.

ASA에서는 두 가지 장애 조치 구성, 즉 액티브/액티브 장애 조치와 액티브/스탠바이 장애 조치를 지원합니다.

활성/활성 장애 조치의 경우 두 장치 모두 네트워크 트래픽을 전달할 수 있습니다. 하지만 부하 균형에서는 같은 효과가 있는 것처럼 보일 수 있지만 실제로 두 디바이스 모두 네트워크 트래픽을 전달할 수 있는 것은 아닙니다. 장애 조치가 발생하면 남은 활성 장치가 구성된 매개변수를 기반으로 결합된 트래픽을 전달하는 역할을 합니다. 따라서 액티브/액티브 장애 조치를 구성할 때는 두 유닛의 결합된 트래픽이 각 유닛의 용량 내에 있는지 확인해야 합니다.

액티브/스탠바이 장애 조치에서는 하나의 유닛만 트래픽을 전달하며 다른 유닛은 트래픽을 전달하지 않고 스탠바이 상태로 대기합니다. 액티브/스탠바이 장애 조치에서는 두 번째 ASA가 장애가 발생한 유닛의 역할을 수행할 수 있습니다. 액티브 유닛에서 장애가 발생한 경우 이 유닛은 스탠바이 상태로 변경되며, 스탠바이 유닛이 액티브 상태로 변경됩니다. 활성 상태로 변경된 장치는 장애가 발생한 장치의 IP 주소(또는 투명 방화벽을 위해 관리 IP 주소) 및 MAC 주소를 인수하여 트래픽 전달을 시작합니다. 스탠바이 상태가 된 유닛은 액티브 유닛의 스탠바이 IP 주소를 인수합니다. 액티브 유닛에서 장애가 발생한 경우 스탠바이 유닛은 클라이언트 VPN 터널의 중단 없이 액티브 유닛의 역할을 수행합니다.

부하 균형

로드 밸런싱 정보

동일한 네트워크에 연결된 둘 이상의 ASA를 사용하여 원격 세션을 처리하는 원격-클라이언트 구성의 경우 이러한 디바이스에서 해당 세션 로드를 공유하도록 구성할 수 있습니다. 이 기능을 로드 밸런싱이라고 합니다. 로드 밸런싱은 로드가 가장 적은 디바이스로 세션 트래픽을 전달하여 모든 디바이스 간에 로드를 분산시킵니다. 따라서 시스템 리소스가 효율적으로 사용되며, 성능 및 가용성이 증가합니다.

로드 밸런싱을 구현하려면 동일한 비공개 LAN-to-LAN 네트워크에 있는 둘 이상의 디바이스를 가상 클러스터로 논리적으로 그룹화합니다.

가상 클러스터의 모든 디바이스는 세션 로드를 수반합니다. 가상 클러스터에 있는 하나의 디바이스인 가상 클러스터 마스터는 수신 연결 요청을 백업 디바이스라는 나머지 디바이스로 디렉션합니다. 가상 클러스터 마스터는 클러스터의 모든 디바이스를 모니터링하고 각각의 사용량을 추적하며 그에 따라 세션 로드를 분산시킵니다. 가상 클러스터 마스터 역할은 물리적 디바이스와 연관이 없으며, 디바이스 간에 전환될 수 있습니다. 예를 들어 현재 가상 클러스터 마스터에서 장애가 발생한 경우 클러스터의 백업 디바이스 중 하나가 해당 역할을 맡아 즉시 새로운 가상 클러스터 마스터가 됩니다.

가상 클러스터는 단일 가상 클러스터 *IP* 주소로 외부 클라이언트에 표시됩니다. 이 IP 주소는 특정 물리적 디바이스에 연결되지 않으며, 현재 가상 클러스터 마스터에 속하므로 가상 주소입니다. 연결을 설정하려는 VPN 클라이언트는 먼저 이 가상 클러스터 IP 주소에 연결합니다. 그러면 가상 클러스터 마스터가 클러스터에서 사용 가능한 호스트 중 로드가 가장 적은 호스트의 공개 IP 주소를 클라이언트로 다시 전송합니다. 두 번째 트랜잭션(사용자에게 투명함)에서 클라이언트는 해당 호스트에 직접 연결합니다. 가상 클러스터 마스터는 이러한 방식으로 리소스 간에 트래픽을 균등하고 효율적으로 디렉션합니다.

클러스터의 시스템에서 장애가 발생한 경우 종료된 세션이 가상 클러스터 IP 주소에 즉시 다시 연결될 수 있습니다. 그러면 가상 클러스터 마스터가 이러한 연결을 클러스터의 다른 액티브 디바이스로 디렉션합니다. 가상 클러스터 마스터 자체에서 장애가 발생한 경우에는 클러스터의 백업 디바이스

가 즉시 자동으로 새로운 가상 세션 마스터의 역할을 합니다. 클러스터의 여러 디바이스에서 장애가 발생한 경우에도 클러스터에 실행되고 사용 가능한 디바이스가 남아 있는 한 사용자는 클러스터에 계속 연결할 수 있습니다.

VPN 부하 균형 알고리즘

마스터 디바이스는 IP 주소가 오름차순으로 정렬된 백업 클러스터 요소의 목록을 유지 관리합니다. 각 백업 클러스터 요소의 부하는 정수 백분율(활성 세션의 수)로 계산됩니다. AnyConnect 비활성화 세션은 부하 균형에 대한 SSL VPN 부하에 포함되지 않습니다. 마스터 디바이스는 나머지보다 1% 더 높을 때까지 가장 부하가 낮은 디바이스로 IPsec 및 SSL VPN 터널을 리디렉션합니다. 모든 백업 클러스터 요소가 마스터보다 1% 높은 경우 마스터 디바이스가 자체적으로 리디렉션합니다.

예를 들어 마스터 1개와 백업 클러스터 요소 2개가 있는 경우 다음 주기가 적용됩니다.

참고 모든 노드가 0%로 시작하고 모든 백분율이 반올림됩니다.

1. 모든 요소에 마스터보다 1% 더 높은 로드가 있는 경우 마스터 디바이스가 연결을 수행합니다.
2. 마스터 디바이스가 연결을 수행하지 않은 경우 부하 백분율이 가장 작은 백업 디바이스가 세션을 수행합니다.
3. 모든 요소에 같은 백분율 부하가 있는 경우 세션 수가 가장 작은 백업 디바이스가 해당 세션을 가져옵니다.
4. 모든 요소에 같은 백분율 부하가 있고 세션 수가 같은 경우 IP 주소가 가장 작은 디바이스가 해당 세션을 가져옵니다.

VPN 부하 균형 클러스터 구성

로드 밸런싱 클러스터는 다음 제한 사항에 따라 동일한 릴리스 또는 혼합된 릴리스의 ASA로 구성될 수 있습니다.

- 동일한 릴리스의 ASA로 구성된 로드 밸런싱 클러스터는 IPsec, AnyConnect 및 클라이언트리스 SSL VPN 클라이언트와 클라이언트리스 세션이 혼합된 세션에 대해 로드 밸런싱을 실행할 수 있습니다.
- 혼합된 릴리스의 ASA 또는 동일한 릴리스의 ASA가 포함된 로드 밸런싱 클러스터는 IPsec 세션만 지원할 수 있습니다. 그러나 이러한 구성에서는 ASA가 전체 IPsec 용량에 도달하지 않을 수도 있습니다.

7.1(1) 릴리스부터 클러스터의 각 디바이스에 수반되는 로드를 결정할 때 IPsec 세션과 SSL VPN 세션을 동일하게 계산하거나 가중치를 부여합니다. 이는 ASA 릴리스 7.0(x) 소프트웨어에 대한 로드 밸런싱 계산과 다르다는 것을 의미합니다. 즉, 이 플랫폼에서는 일부 하드웨어 플랫폼에서 SSL VPN 세션 로드를 IPsec 세션 로드와 다르게 계산하는 가중치 알고리즘을 사용합니다.

클러스터의 가상 마스터는 클러스터의 요소에 세션 요청을 할당합니다. ASA에서는 모든 세션, SSL VPN 또는 IPsec을 동일하게 간주하여 그에 따라 세션 요청을 할당합니다. 구성 및 라이센스에서 허용하는 최대 범위 내에서 허용할 IPsec 및 SSL VPN 세션 수를 구성할 수 있습니다.

Cisco에서는 하나의 로드 밸런싱 클러스터에서 최대 10개의 노드를 테스트했습니다. 더 큰 클러스터도 작동할 수 있지만 공식적으로는 이러한 토폴로지를 지원하지 않습니다.

일반적인 혼합 클러스터 시나리오의 예

혼합 구성을 사용하는 경우, 즉 로드 밸런싱 클러스터에 ASA 소프트웨어 릴리스의 혼합을 실행 중인 디바이스가 포함된 경우, 초기 클러스터 마스터에 장애가 발생하여 다른 디바이스가 마스터 역할을 하면 가중치 알고리즘의 차이로 인해 문제가 발생합니다.

다음 시나리오는 ASA 릴리스 7.1(1) 및 ASA 릴리즈 7.0(x) 소프트웨어가 실행 중인 ASA가 혼합으로 구성된 클러스터에서 VPN 로드 밸런싱의 사용을 보여줍니다.

시나리오 **1: SSL VPN** 연결을 하지 않는 혼합 클러스터

이 시나리오에서 클러스터는 ASA의 혼합으로 구성됩니다. ASA 클러스터 피어의 일부는 ASA 릴리스 7.0(x)을 실행하고 일부는 Release 7.1(1)을 실행합니다. 7.1(1) 이전 피어에는 SSL VPN 연결이 없으며 7.1(1) 클러스터 피어에는 두 개의 SSL VPN 세션을 허용하지만 SSL VPN 연결이 없는 기본 SSL VPN 라이선스만 있습니다. 이러한 경우 모든 연결이 IPsec이며 부하 균형이 올바르게 작동합니다.

시나리오 **2: SSL VPN** 연결을 처리하는 혼합 클러스터

예를 들어 ASA Release 7.1(1) 소프트웨어를 실행 중인 ASA가 초기 클러스터 마스터이고 해당 디바이스에 장애가 발생한다고 가정해 보십시오. 클러스터의 다른 디바이스가 자동으로 마스터의 역할을 수행하고 클러스터 내에서 프로세서 부하를 결정하기 위해 자체 부하 균형 알고리즘을 적용합니다. ASA Release 7.1(1) 소프트웨어에서 실행 중인 클러스터 마스터는 해당 소프트웨어가 제공하는 부분 이외에는 어떤 방식으로도 세션 로드에 가중치를 부여할 수 없습니다. 따라서 IPsec 및 SSL VPN 세션 부하의 혼합을 이전 버전을 실행 중인 ASA 디바이스에 적절히 할당할 수 없습니다. 다음 시나리오는 이러한 딜레마를 보여줍니다.

이 시나리오는 클러스터가 ASA의 혼합으로 구성되었다는 점에서 이전 시나리오와 유사합니다. ASA 클러스터 피어의 일부는 ASA 릴리스 7.0(x)을 실행하고 일부는 Release 7.1(1)을 실행합니다. 그러나 이 경우 클러스터는 SSL VPN 연결뿐만 아니라 IPsec 연결을 처리합니다.

ASA 릴리스 7.1(1) 이전 버전의 소프트웨어를 실행 중인 디바이스가 클러스터 마스터인 경우 이 마스터는 릴리스 7.1(1) 이전의 프로토콜과 로직을 적용합니다. 즉, 세션이 세션 제한을 초과한 부하 균형 피어에게 디렉션될 수 있습니다. 이 경우 사용자는 액세스가 거부됩니다.

클러스터 마스터가 ASA 릴리스 7.0(x) 소프트웨어를 실행 중인 디바이스인 경우 기존 세션 가중치 알고리즘이 클러스터의 7.1(1) 이전 피어에만 적용됩니다. 이 경우에 액세스가 거부되지 않습니다. 7.1(1) 이전 피어는 세션 가중치 알고리즘을 사용하기 때문에 좀 더 가볍게 로드됩니다.

그러나 7.1(1) 피어가 항상 클러스터 마스터가 된다고 보장할 수 없기 때문에 문제가 발생합니다. 클러스터 마스터에 장애가 발생하는 경우 다른 피어가 마스터의 역할을 수행합니다. 새 마스터는 자격을 갖춘 피어 중 하나일 수 있습니다. 결과를 예측할 수 없으므로 해당 유형의 클러스터는 구성하지 않는 것이 좋습니다.

부하 균형에 대한 자주 묻는 질문(FAQ)

- 멀티 컨텍스트 모드

멀티 컨텍스트 모드

Q. 다중 상황 모드에서 로드 밸런싱이 지원됩니까?

A. 로드 밸런싱 또는 스테이트풀 장애 조치는 다중 상황 모드에서 지원되지 않습니다.

IP 주소 풀 소모

Q. ASA에서는 VPN 로드 밸런싱 방법의 일환으로 IP 주소 풀 소모를 고려합니까?

A. 아니요. 원격 액세스 VPN 세션이 소모된 IP 주소 풀이 있는 디바이스로 디렉션되는 경우 세션이 설정되지 않습니다. 부하 균형 알고리즘은 부하를 기반으로 하며 각 백업 클러스터 요소가 제공하는 정수 백분율(활성 세션 및 최대 세션의 수)로 계산됩니다.

고유한 IP 주소 풀

Q. VPN 로드 밸런싱을 구현하려면 다른 ASA의 AnyConnect 클라이언트 또는 IPsec 클라이언트에 대한 IP 주소 풀이 고유해야 합니까?

A. 예. IP 주소 풀은 디바이스별로 고유해야 합니다.

같은 디바이스에서 부하 균형 및 장애 조치 사용

Q. 하나의 디바이스에서 부하 균형과 장애 조치를 모두 사용할 수 있습니까?

A. 예. 이 구성에서는 클라이언트가 클러스터의 IP 주소에 연결되고 클러스터에서 부하가 가장 적은 ASA로 리디렉션됩니다. 해당 디바이스에서 장애가 발생하면 대기 장치가 즉시 해당 역할을 맡아 VPN 터널에 아무런 영향을 미치지 않습니다.

여러 인터페이스의 부하 균형

Q. 여러 인터페이스에서 SSL VPN을 활성화한 경우 모든 인터페이스에서 부하 균형을 구현할 수 있습니까?

A. 1개의 인터페이스만 공유 인터페이스로 클러스터에 참여하도록 정의할 수 있습니다. 이는 CPU 부하의 균형을 유지하기 위한 것입니다. 여러 인터페이스가 같은 CPU에서 통합되므로 여러 인터페이스에서 부하 균형의 개념은 의미가 없습니다.

부하 균형 클러스터에 대한 최대 동시 세션 수

Q. 각각 100개의 사용자 SSL VPN 라이센스를 사용하는 2개의 ASA 5525-X을 배포한다는 점을 고려하십시오. 부하 균형 클러스터에서 최대 전체 사용자 수는 200개의 동시 세션을 허용합니까

아니면 100개만 허용합니까? 100개의 사용자 라이센스를 사용하는 제3의 디바이스를 추가하는 경우 300개의 동시 세션을 지원할 수 있습니까?

A. VPN 부하 균형을 사용하면 모든 디바이스가 활성화되므로 사용자가 클러스터에서 지원할 수 있는 최대 세션 수는 클러스터의 각 디바이스에 대한 세션 수의 총합과 같습니다. 이 경우에서는 300개의 세션을 지원합니다.

로드 밸런싱에 대한 라이센싱

VPN 로드 밸런싱을 사용하려면 Security Plus 라이센스가 있는 ASA 모델 5512-X 또는 ASA 모델 5515-X 이상이 있어야 합니다. VPN 로드 밸런싱에도 활성 3DES/AES 라이센스가 필요합니다. 보안 어플라이언스는 로드 밸런싱을 활성화하기 전에 이러한 암호화 라이센스가 있는지 확인합니다. 활성 3DES 또는 AES 라이센스가 탐지되지 않는 경우 보안 어플라이언스가 로드 밸런싱의 활성화를 방지하며 라이센스에서 허용할 때까지 로드 밸런싱을 통한 3DES의 내부 구성을 방지합니다.

VPN 로드 밸런싱에 대한 지침 및 제한 사항

또한 로드 밸런싱을 위한 사전 요구 사항, 50 페이지의 내용을 참조하십시오.

적격 플랫폼

로드 밸런싱 클러스터에는 Security Plus 라이선스가 포함된 ASA 모델 ASA 5512-X 및 모델 5515-X 이상이 포함될 수 있습니다. 혼합된 구성을 사용할 수 있는 경우 일반적으로 클러스터의 종류가 같으면 관리가 더 간단합니다.

적격 클라이언트

로드 밸런싱은 다음 클라이언트에서 시작되는 원격 세션에만 적용됩니다.

- Cisco AnyConnect Secure Mobility Client(릴리스 3.0 이상)
- Cisco ASA 5505 Security Appliance(Easy VPN 클라이언트 역할을 하는 경우)
- IKE 리디렉션을 지원하는 Cisco IOS EZVPN 클라이언트 디바이스(IOS 831/871)
- 클라이언트리스 SSL VPN(클라이언트가 아님)

클라이언트 고려 사항

로드 밸런싱은 IPsec 클라이언트와 SSL VPN 클라이언트 및 클라이언트리스 세션에서 작동합니다. LAN-to-LAN을 비롯한 다른 모든 VPN 연결 유형(L2TP, PPTP, L2TP/IPsec)은 로드 밸런싱이 활성화된 ASA에 연결할 수 있지만 로드 밸런싱에 참여할 수는 없습니다.

로드 밸런싱을 위해 여러 개의 ASA 노드가 클러스터링된 경우, AnyConnect 클라이언트 연결에 대해 그룹 URL을 사용하는 것이 바람직한 경우, 개별 ASA 노드는 다음을 수행해야 합니다.

- 각 로드 밸런싱 가상 클러스터 주소(IPv4 및 IPv6)에 대한 그룹 URL을 사용하여 각 원격 액세스 연결 프로필을 구성합니다.

- 이 노드의 VPN 로드 밸런싱 공용 주소에 대해 그룹 URL을 구성합니다.

상황 모드

다중 상황 모드에서 VPN 로드 밸런싱은 지원되지 않습니다.

인증서 확인

AnyConnect에서의 로드 밸런싱을 위해 인증서 확인을 수행할 때 연결이 IP 주소를 통해 리디렉션되는 경우 클라이언트는 이 IP 주소를 통해 모든 이름 확인을 수행합니다. 리디렉션 IP 주소가 인증서 공통 이름 또는 주체 대체 이름에 나열되어 있는지 확인합니다. IP 주소가 이러한 필드에 없으면 인증서가 신뢰할 수 없는 것으로 간주됩니다.

주체 대체 이름이 인증서에 포함된 경우에는 RFC 2818에 정의된 지침에 따라 이름 확인에 주체 대체 이름만 사용하며, 공통 이름은 무시합니다. 인증서를 제시하는 서버의 IP 주소가 인증서의 주체 대체 이름에 정의되어 있는지 확인합니다.

독립형 ASA의 경우 IP 주소는 해당 ASA의 IP입니다. 클러스터링 상황에서는 인증서 구성에 따라 달라집니다. 클러스터에서 하나의 인증서를 사용하는 경우 해당 인증서에는 클러스터 IP 주소와 클러스터 FQDN에 대한 SAN 확장명이 있어야 하며 각 ASA의 IP와 FQDN이 있는 주체 대체 이름 확장명이 포함되어야 합니다. 클러스터에서 여러 인증서를 사용하는 경우 각 ASA에 대한 인증서에는 클러스터 IP, 클러스터 FQDN, 개별 ASA의 IP 주소 및 FQDN에 대한 SAN 확장명이 있어야 합니다.

지리적 로드 밸런싱

DNS 확인이 정기적으로 변경되는 로드 밸런싱 환경에서는 TTL(Time to Live) 값을 설정하는 방법을 신중하게 고려해야 합니다. AnyConnect에서 DNS 로드 밸런싱 구성이 제대로 작동하려면 ASA를 선택한 시점부터 터널이 완전히 설정될 때까지 ASA 이름-주소 매핑이 동일하게 유지되어야 합니다. 자격 증명을 입력하기 전에 너무 많은 시간이 경과한 경우에는 조회가 다시 시작되고 다른 IP 주소가 확인된 주소가 될 수도 있습니다. 자격 증명을 입력하기 전에 DNS 매핑이 다른 ASA로 변경되면 VPN 터널이 실패합니다.

VPN에 대한 지리적 로드 밸런싱에서는 Cisco GSS(Global Site Selector)를 사용하는 경우가 많습니다. GSS는 로드 밸런싱에 DNS를 사용하며, DNS 확인에 대한 TTL(Time to Live) 값이 기본적으로 20초로 설정됩니다. GSS에서 TTL 값을 늘리면 연결에 실패할 가능성을 크게 낮출 수 있습니다. 훨씬 더 높은 값으로 늘리면 인증 단계에서 사용자가 자격 증명을 입력하고 터널을 설정할 수 있는 충분한 시간이 허용됩니다.

자격 증명 입력 시간을 늘리기 위해 Connect on Start Up(시작 시 연결)을 비활성화할 수도 있습니다.

부하 균형 구성

동일한 네트워크에 연결된 둘 이상의 ASA를 사용하여 원격 세션을 처리하는 원격-클라이언트 구성의 경우 이러한 디바이스에서 해당 세션 로드를 공유하도록 구성할 수 있습니다. 로드 밸런싱이라고 하는 이 기능은 로드가 가장 적은 디바이스로 세션 트래픽을 전달하여 모든 디바이스 간에 로드를 분산시킵니다. 로드 밸런싱은 시스템 리소스의 효율적 사용을 지원하며, 성능 및 고가용성을 증가시킵니다.

로드 밸런싱을 사용하려면 클러스터의 각 디바이스에서 다음을 수행하십시오.

- 공통 VPN 로드 밸런싱 클러스터 속성을 설정하여 로드 밸런싱 클러스터를 구성합니다. 이 클러스터에는 가상 클러스터 IP 주소, UDP 포트(필요한 경우) 및 클러스터의 IPsec 공유 암호가 포함됩니다. 클러스터의 모든 참여자는 클러스터 내에서 디바이스 우선순위를 제외하고 클러스터 구성이 같아야 합니다.
- 디바이스에서 로드 밸런싱을 활성화하고 디바이스별 속성(공용 주소 및 사설 주소)을 정의하여 참여하는 디바이스를 구성합니다. 이러한 값은 디바이스마다 다릅니다.

로드 밸런싱을 위한 사전 요구 사항

또한 VPN 로드 밸런싱에 대한 지침 및 제한 사항, 48 페이지의 내용을 참조하십시오.

- 부하 균형은 기본적으로 비활성화되어 있습니다. 명시적으로 부하 균형을 활성화해야 합니다.
- 먼저 공용(외부) 및 사설(내부) 인터페이스를 구성해야 합니다. 이 섹션의 후속 참조는 내부 및 외부의 이름을 사용합니다.

  이 작업을 수행하려면 **Configuration(**구성**) > Device Setup(**디바이스 설정**) > Interface Settings(**인터페이스 설정**) > Interfaces(**인터페이스**)**로 이동합니다.
- 가상 클러스터 IP 주소가 참조하는 인터페이스를 미리 구성해 두어야 합니다. 공통 가상 클러스터 IP 주소, UDP 포트(필요한 경우) 및 클러스터의 IPsec 공유 암호를 설정합니다.
- 클러스터에 참여하는 모든 디바이스는 클러스터 특정 값(IP 주소, 암호화 설정, 암호 키 및 포트)이 같아야 합니다.
- 암호화를 사용하는 경우 로드 밸런싱 내부 인터페이스를 구성해야 합니다. 이 인터페이스가 로드 밸런싱 내부 인터페이스에서 활성화되지 않은 경우에는 클러스터 암호화를 구성하려고 할 때 오류 메시지가 나타납니다.
- 활성/활성 상태 저장 장애 조치 또는 VPN 부하 균형을 사용하는 경우 로컬 CA 기능이 지원되지 않습니다. 로컬 CA는 다른 CA에 종속될 수 없고 루트 CA의 역할만 수행할 수 있습니다.

고가용성 및 확장성 마법사를 사용하여 **VPN** 로드 밸런싱 구성

프로시저

단계 **1** **Wizards(**마법사**)** > **High Availability and Scalability(**고가용성 및 확장성**)**를 선택합니다.

단계 **2** Configuration Type(구성 유형) 화면에서 **Configure VPN Cluster Load Balancing(VPN** 클러스터 로드 밸런싱 구성**)**을 클릭하고 **Next(**다음**)**를 클릭합니다.

단계 **3** 전체 가상 클러스터를 나타내는 단일 IP 주소를 선택합니다. 가상 클러스터의 모든 ASA에서 공유하는 공개 서브넷 주소 범위 내에 있는 IP 주소를 지정합니다.

단계 **4** 해당 디바이스가 참여하는 가상 클러스터의 UDP 포트를 지정합니다. 기본값은 9023입니다. 다른 애플리케이션에서 이 포트를 사용하는 경우 로드 밸런싱에 사용할 UDP 대상 포트 번호를 입력합니다.

단계 **5** IPsec 암호화를 활성화하고 디바이스 간에 전달되는 모든 로드 밸런싱 정보를 암호화하려면 **Enable IPsec Encryption(IPsec** 암호화 활성화**)** 확인란을 선택합니다.

또한 공유 암호를 지정하고 확인해야 합니다. 가상 클러스터의 ASA는 IPsec을 사용하여 LAN-to-LAN 터널을 통해 통신합니다. IPsec 암호화를 비활성화하려면 **Enable IPsec Encryption(IPsec** 암호화 활성화**)** 확인란의 선택을 취소합니다.

참고 암호화를 사용하는 경우 로드 밸런싱 내부 인터페이스를 구성해야 합니다. 이 인터페이스가 로드 밸런싱 내부 인터페이스에서 활성화되지 않은 경우에는 클러스터 암호화를 구성하려고 할 때 오류 메시지가 나타납니다.

단계 **6** IPsec 암호화를 활성화한 경우 IPsec 피어 간의 공유 암호를 지정합니다. 여기에서 입력하는 값은 연속된 별표(*) 문자로 표시됩니다.

단계 **7** 클러스터 내에서 이 디바이스에 할당할 우선순위를 지정합니다. 범위는 1에서 10까지입니다. 우선순위는 시작 시 또는 기존 마스터에서 장애가 발생한 경우 해당 디바이스가 가상 클러스터 마스터가 될 가능성을 나타납니다. 우선순위가 높을수록(예: 10) 이 디바이스가 가상 클러스터 마스터가 될 가능성이 더 높습니다.

참고 가상 클러스터 내 디바이스의 전원이 켜지는 시점이 서로 다른 경우에는 가장 먼저 전원이 켜지는 디바이스가 가상 클러스터 마스터 역할을 수행합니다. 모든 가상 클러스터에는 마스터가 필요하기 때문에 가상 클러스터의 각 디바이스는 전원이 켜지는 시점을 확인하여 클러스터에 가상 마스터가 있는지 확인합니다. 가상 마스터가 없으면 해당 디바이스가 그 역할을 수행합니다. 나중에 전원이 켜지고 클러스터에 추가된 디바이스는 보조 디바이스가 됩니다. 가상 클러스터의 모든 디바이스가 동시에 전원이 켜지는 경우에는 우선순위 설정이 가장 높은 디바이스가 가상 클러스터 마스터가 됩니다. 가상 클러스터에서 둘 이상의 디바이스가 동시에 전원이 켜지고 둘 다 우선순위 설정이 가장 높은 경우에는 IP 주소가 가장 낮은 디바이스가 가상 클러스터 마스터가 됩니다.

단계 **8** 이 디바이스에 대한 공개 인터페이스의 이름 또는 IP 주소를 지정합니다.

단계 **9** 이 디바이스에 대한 비공개 인터페이스의 이름 또는 IP 주소를 지정합니다.

단계 **10** VPN 클라이언트 연결을 클러스터 디바이스로 리디렉션할 때 VPN 클러스터 마스터가 외부 IP 주소 대신 해당 클러스터 디바이스의 호스트 및 도메인 이름을 사용하여 정규화된 도메인 이름을 전송하도록 **Send FQDN to client instead of an IP address when redirecting(**리디렉션할 때 **IP** 주소 대신 **FQDN** 을 클라이언트로 보내기**)** 확인란을 선택합니다.

단계 **11** 다음을 클릭합니다. Summary(요약) 화면의 구성을 검토합니다.

단계 **12** 마침을 클릭합니다.

VPN 클러스터 로드 밸런싱 구성이 ASA로 전송됩니다.

다음에 수행할 작업

로드 밸런싱을 위해 여러 개의 ASA 노드가 클러스터링된 경우, AnyConnect 클라이언트 연결에 대해 그룹 URL을 사용하는 것이 바람직한 경우, 개별 ASA 노드는 다음을 수행해야 합니다.

- 각 로드 밸런싱 가상 클러스터 주소(IPv4 및 IPv6)에 대한 그룹 URL을 사용하여 각 원격 액세스 연결 프로필을 구성합니다.
- 이 노드의 VPN 로드 밸런싱 공용 주소에 대해 그룹 URL을 구성합니다.

Configuration(구성**) > Remote Access VPN(**원격 액세스 **VPN) > Network (Client) Access(**네트워크(클라이언트**)** 액세스**) > AnyConnect Connection Profiles(AnyConnect** 연결 프로필**)** *connection profile name(*연결 프로필 이름*)* > **Add or Edit(**추가 또는 수정**) >Advanced(**고급**) > Group Alias/Group URL(**그룹 별칭/그룹 **URL)** 창에서 그룹 URL이 구성됩니다.

VPN 로드 밸런싱 구성(마법사를 사용하지 않음)

프로시저

단계 **1** **Configuration(**구성**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **Load Balancing(**로드 밸런싱**)**을 선택합니다**.**

단계 **2** **Participate in Load Balancing(**로드 밸런싱에 참여**)**을 선택하여 이 ASA가 로드 밸런싱 클러스터의 참여자임을 나타냅니다.

로드 밸런싱에 참여하는 모든 ASA에서 이 방식으로 로드 밸런싱을 활성화해야 합니다.

단계 **3** **VPN Cluster Configuration(VPN** 클러스터 구성**)** 영역에서 다음 필드를 구성합니다. 이러한 값은 전체 가상 클러스터에 대해 동일해야 합니다. 클러스터의 모든 서버가 동일한 클러스터 구성으로 설정되어야 합니다.

- **Cluster IPv4 Address(**클러스터 **IPv4** 주소**)** - 전체 IPv4 가상 클러스터를 나타내는 단일 IPv4 주소를 지정합니다. 가상 클러스터의 모든 ASA에서 공유하는 공용 서브넷 주소 범위 내에 있는 IP 주소를 선택합니다.
  - **UDP Port(UDP** 포트**)** - 이 명령은 해당 디바이스가 참여하는 가상 클러스터의 UDP 포트를 지정합니다. 기본값은 9023입니다. 다른 애플리케이션에서 이 포트를 사용하는 경우 로드 밸런싱에 사용할 UDP 대상 포트 번호를 입력합니다.
- **Cluster IPv6 Address(**클러스터 **IPv6** 주소**)** - 전체 IPv6 가상 클러스터를 나타내는 단일 IPv6 주소를 지정합니다. 가상 클러스터의 모든 ASA에서 공유하는 공용 서브넷 주소 범위 내에 있는 IP 주소를 선택합니다. IPv6 주소를 사용하는 클라이언트는 ASA 클러스터의 공개 IPv6 주소 또는 GSS 서버를 통해 AnyConnect 연결을 설정할 수 있습니다. 마찬가지로 IPv6 주소를 사용하는 클라이언트는 ASA 클러스터의 공개 IPv4 주소 또는 GSS 서버를 통해 AnyConnect 연결을 설정할 수 있습니다. ASA 클러스터 내에서 이 두 가지 연결 유형 중 하나에 로드 밸런싱을 적용할 수 있습니다.

  참고 하나 이상의 DNS 서버로 구성된 DNS 서버 그룹이 있고 ASA 인터페이스 중 하나에서 DNS 조회가 활성화된 경우 Cluster IPv4 Address(클러스터 IPv4 주소) 및 Cluster IPv6 Address(클러스터 IPv6 주소) 필드에서 가상 클러스터의 정규화된 도메인 이름을 지정할 수도 있습니다.

- **Enable IPsec Encryption(IPsec** 암호화 활성화**)** - IPsec 암호화를 활성화하거나 비활성화합니다. 이 상자를 선택한 경우 공유 암호를 지정하고 확인해야 합니다. 가상 클러스터의 ASA는 IPsec을 사용하여 LAN-to-LAN 터널을 통해 통신합니다. 디바이스 간에 전달되는 모든 로드 밸런싱 정보를 암호화하려면 이 특성을 활성화하십시오.
- **IPsec Shared Secret(IPsec** 공유 암호**)** - IPsec 암호화를 활성화한 경우 IPsec 피어 간의 공유 암호를 지정합니다. 이 상자에 입력하는 값은 연속된 별표(*) 문자로 표시됩니다.
- **Verify Secret(**암호 확인**)** - 공유 암호를 다시 입력합니다. IPsec Shared Secret(IPsec 공유 암호) 상자에 입력한 공유 암호 값을 확인합니다.

단계 **4** 특정 ASA에 대해 **VPN Server Configuration(VPN** 서버 구성**)** 영역의 필드를 구성합니다.

- **Public Interface(**공개 인터페이스**)** - 이 디바이스에 대한 공개 인터페이스의 이름 또는 IP 주소를 지정합니다.
- **Private Interface(**비공개 인터페이스**)** - 이 디바이스에 대한 비공개 인터페이스의 이름 또는 IP 주소를 지정합니다.
- **Priority(**우선순위**)** - 클러스터 내에서 이 디바이스에 할당할 우선순위를 지정합니다. 범위는 1에서 10까지입니다. 우선순위는 시작 시 또는 기존 마스터에서 장애가 발생한 경우 이 디바이스가 가상 클러스터 마스터가 될 가능성을 나타냅니다. 우선순위가 높을수록(예: 10) 이 디바이스가 가상 클러스터 마스터가 될 가능성이 더 높습니다.

  참고 가상 클러스터 내 디바이스의 전원이 켜지는 시점이 서로 다른 경우에는 가장 먼저 전원이 켜지는 디바이스가 가상 클러스터 마스터 역할을 수행합니다. 모든 가상 클러스터에는 마스터가 필요하기 때문에 가상 클러스터의 각 디바이스는 전원이 켜지는 시점을 확인하여 클러스터에 가상 마스터가 있는지 확인합니다. 가상 마스터가 없으면 해당 디바이스가 그 역할을 수행합니다. 나중에 전원이 켜지고 클러스터에 추가된 디바이스는 백업 디바이스가 됩니다. 가상 클러스터의 모든 디바이스가 동시에 전원이 켜지는 경우에는 우선순위 설정이 가장 높은 디바이스가 가상 클러스터 마스터가 됩니다. 가상 클러스터에서 둘 이상의 디바이스가 동시에 전원이 켜지고 둘 다 우선순위 설정이 가장 높은 경우에는 IP 주소가 가장 낮은 디바이스가 가상 클러스터 마스터가 됩니다.

- **NAT Assigned IPv4 Address(NAT** 할당 **IPv4** 주소**)** - 이 디바이스의 IP 주소가 NAT에 의해 변환되는 IP 주소를 지정합니다. NAT를 사용하지 않거나 디바이스가 NAT를 사용하는 방화벽 뒤에 있는 경우에는 이 필드를 비워 둡니다.
- NAT Assigned IPv6 Address(NAT 할당 IPv6 주소) - 이 디바이스의 IP 주소가 NAT에 의해 변환되는 IP 주소를 지정합니다. NAT를 사용하지 않거나 디바이스가 NAT를 사용하는 방화벽 뒤에 있는 경우에는 이 필드를 비워 둡니다.
- **Send FQDN to client(**클라이언트로 **FQDN** 보내기**)** - VPN 클라이언트 연결을 클러스터 디바이스로 리디렉션할 때 VPN 클러스터 마스터가 외부 IP 주소 대신 해당 클러스터 디바이스의 호스트 및 도메인 이름을 사용하여 정규화된 도메인 이름을 전송하도록 하려면 이 확인란을 선택합니다.

기본적으로 ASA는 로드 밸런싱 리디렉션에서 IP 주소만 클라이언트로 전송합니다. DNS 이름을 기반으로 하는 인증서를 사용 중인 경우 백업 디바이스로 리디렉션할 때는 인증서가 유효하지 않습니다.

VPN 클러스터 마스터로서 이 ASA는 VPN 클라이언트 연결을 클러스터 디바이스(클러스터의 다른 ASA)로 리디렉션할 때 역방향 DNS 조회를 사용하여 외부 IP 주소 대신 해당 클러스터 디바이스의 FQDN(Fully Qualified Domain Name: 정규화된 도메인 이름)을 전송할 수 있습니다.

클러스터 내 로드 밸런싱 디바이스의 모든 외부 및 내부 네트워크 인터페이스는 동일한 IP 네트워크에 있어야 합니다.

참고 IPv6을 사용하고 FQDN을 클라이언트로 전송할 때는 ASA에서 DNS를 통해 이러한 이름을 확인할 수 있어야 합니다.

자세한 내용은 FQDN을 사용하여 클라이언트리스 SSL VPN 로드 밸런싱 활성화, 54 페이지을/를 참조하십시오.

다음에 수행할 작업

로드 밸런싱을 위해 여러 개의 ASA 노드가 클러스터링된 경우, AnyConnect 클라이언트 연결에 대해 그룹 URL을 사용하는 것이 바람직한 경우, 개별 ASA 노드는 다음을 수행해야 합니다.

- 각 로드 밸런싱 가상 클러스터 주소(IPv4 및 IPv6)에 대한 그룹 URL을 사용하여 각 원격 액세스 연결 프로필을 구성합니다.
- 이 노드의 VPN 로드 밸런싱 공용 주소에 대해 그룹 URL을 구성합니다.

Configuration(구성) > **Remote Access VPN**(원격 액세스 **VPN**) > **Network (Client) Access**(네트워크(클라이언트) 액세스) > **AnyConnect Connection Profiles**(**AnyConnect** 연결 프로필) *connection profile name*(연결 프로필 이름) > **Add or Edit**(추가 또는 수정) > **Advanced**(고급) > **Group Alias/Group URL**(그룹 별칭/그룹 **URL**) 창에서 그룹 URL이 구성됩니다.

FQDN을 사용하여 클라이언트리스 SSL VPN 로드 밸런싱 활성화

프로시저

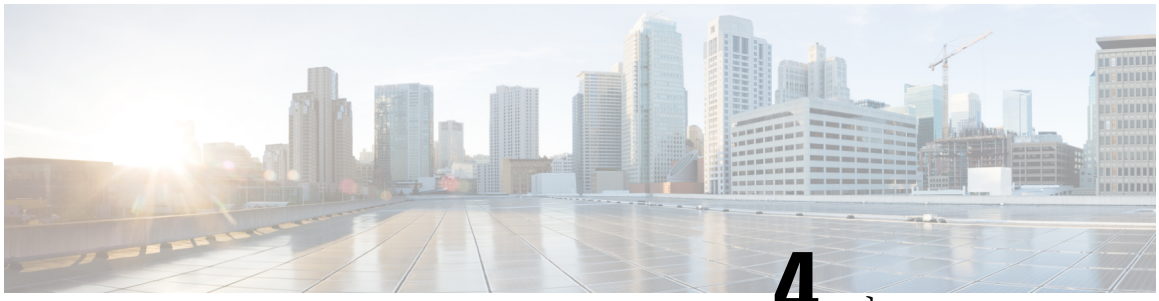
단계 **1** **Send FQDN to client instead of an IP address when redirecting**(리디렉션할 때 **IP** 주소 대신 **FQDN**을 클라이언트로 보내기) 확인란을 선택하여 로드 밸런싱에 FQDN을 사용하는 기능을 활성화합니다.

단계 **2** 해당 항목이 없는 경우 각 ASA 외부 인터페이스의 항목을 DNS 서버에 추가하십시오. 각 ASA 외부 IP 주소에는 조회를 위한 관련 DNS 항목이 있어야 합니다. 또한 역방향 조회에 대해 이러한 DNS 항목을 활성화해야 합니다.

단계 **3** DNS 서버로 라우팅하는 모든 인터페이스에 대해 **Configuration**(구성) > **Device Management**(디바이스 관리) > **DNS** > **DNS Client**(**DNS** 클라이언트) 대화 상자에서 ASA의 DNS 조회를 활성화합니다.

단계 **4** ASA에서 DNS 서버 IP 주소를 정의합니다. 이 작업을 수행하려면 이 대화 상자에서 **Add(**추가**)**를 클릭합니다. 그러면 Add DNS Server Group(DNS 서버 그룹 추가) 대화 상자가 열립니다. 추가할 DNS 서버의 IPv4 또는 IPv6 주소(예: 192.168.1.1 또는 2001:DB8:2000::1)를 입력합니다.

단계 **5** **OK(**확인**)** 및 **Apply(**적용**)**를 클릭합니다.



4 장

일반 VPN 설정

시스템 옵션

Configuration(구성**) > Remote Access VPN(**원격 액세스 **VPN) > Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**) > Advanced(**고급**) > IPsec > System Options(**시스템 옵션**)** 창(또는 **Configuration(**구성**) > Site-to-Site VPN(**사이트 대 사이트 **VPN) > Advanced(**고급**) > System Options(**시스템 옵션**)**를 사용하여 이동**)**을 사용하면 ASA의 IPsec 및 VPN 세션별로 기능을 구성할 수 있습니다.

- Limit the maximum number of active IPsec VPN sessions(최대 활성 IPsec VPN 세션 수 제한) - 최대 활성 IPsec VPN 세션 수 제한을 활성화하거나 비활성화합니다. 범위는 하드웨어 플랫폼 및 소프트웨어 라이센스에 따라 달라집니다.
  - Maximum IPsec Sessions(최대 IPsec 세션 수) - 허용되는 최대 활성 IPsec VPN 세션 수를 지정합니다. 이 필드는 최대 활성 IPsec VPN 세션 수를 제한하는 이전 확인란을 선택한 경우에만 활성화됩니다.
- L2TP Tunnel Keep-alive Timeout(L2TP 터널 킵얼라이브 시간 제한) - 킵얼라이브 메시지의 빈도(초)를 지정합니다. 범위는 10초부터 300초까지입니다. 기본값은 60초입니다. 이는 네트워크(클라이언트) 액세스에만 적용되는 고급 시스템 옵션입니다.
- Reclassify existing flows when VPN tunnels establish(VPN 터널이 설정된 경우 기존 흐름 다시 분류)
- Preserve stateful VPN flows when the tunnel drops(터널 연결이 끊어진 경우 상태 저장 VPN 흐름 유지) - NEM(Network-Extension Mode)에서 IPsec 터널링된 흐름 유지를 활성화하거나 비활성화합니다. 영구 IPsec 터널링된 흐름 기능이 활성화된 경우 터널이 시간 제한 대화 상자 내에서 다시 생성되는 한, 데이터 흐름이 정상적으로 지속됩니다. 이는 보안 어플라이언스에서 상태 정보에 대한 액세스 권한을 계속 유지하기 때문입니다. 이 옵션은 기본적으로 비활성화되어 있습니다.

  참고 터널링 TCP 흐름은 삭제되지 않으므로 정리를 위해 TCP 시간 제한을 사용합니다. 그러나 특정 터널링 흐름의 시간 제한을 비활성화한 경우 해당 흐름은 수동으로 또는 피어의 TCP RST와 같이 다른 수단을 통해 삭제될 때까지 시스템에 남아 있습니다.

- IPsec Security Association Lifetime(IPsec 보안 연계 수명) - SA(Security Association) 기간을 구성합니다. 이 매개변수는 IPsec SA 키의 수명(IPsec SA가 만료되어 새 키로 재협상해야 할 때까지 지속되는 기간)을 측정하는 방법을 지정합니다.
  - **Time(**시간**)** - SA 수명을 시(hh), 분(mm), 초(ss) 단위로 지정합니다.
  - **Traffic Volume(**트래픽 양**)** - SA 수명을 트래픽 양(KB)으로 정의합니다. IPsec SA가 만료되는 페이로드 데이터의 킬로바이트 수를 입력하거나 제한 없음을 선택합니다. 최소값은 100KB이고, 기본값은 10,000KB이며, 최대값은 2,147,483,647KB입니다.

- Enable PMTU (Path Maximum Transmission Unit) Aging(PMTU(Path Maximum Transmission Unit) 에이징 활성화) - 관리자가 PMTU 에이징을 활성화할 수 있습니다.
  - Interval to Reset PMTU of an SA (Security Association)(SA(Security Association)의 PMTU 재설정 간격) - PMTU 값이 원래 값으로 다시 설정되는 시간(초)을 입력합니다.

- Enable inbound IPsec sessions to bypass interface access-lists(인바운드 IPsec 세션을 활성화하여 인터페이스 액세스 목록 우회). Group policy and per-user authorization ACLs still apply to the traffic(그룹 정책 및 사용자별 권한 부여 ACL을 트래픽에 계속 적용) - 기본적으로 ASA에서는 VPN 트래픽이 ASA 인터페이스에서 종료되도록 허용합니다. 액세스 규칙에서 IKE 또는 ESP(또는 다른 유형의 VPN 패킷)를 허용할 필요가 없습니다. 이 옵션을 선택하면 암호 해독된 VPN 패킷의 로컬 IP 주소에 대한 액세스 규칙이 필요 없습니다. VPN 터널이 VPN 보안 메커니즘을 통해 성공적으로 종료되므로 이 기능은 보안 위험 없이 구성을 간소화하고 ASA 성능을 극대화합니다. (그룹 정책 및 사용자별 권한 부여 ACL이 트래픽에 계속 적용됩니다.)

  이 옵션의 선택을 취소하여 로컬 IP 주소에 적용할 액세스 규칙을 요구할 수 있습니다. 액세스 규칙은 로컬 IP 주소에 적용되며, VPN 패킷이 암호 해독되기 전에 사용된 원래 클라이언트 IP 주소에는 적용되지 않습니다.

- Permit communication between VPN peers connected to the same interface(동일한 인터페이스에 연결된 VPN 피어 간의 통신 허용) - 이 기능을 활성화하거나 비활성화합니다.

  또한 암호화 여부에 상관없이 동일한 인터페이스를 통해 들어오는 클라이언트 VPN 트래픽을 외부로 다시 리디렉션할 수 있습니다. 암호화되지 않은 동일한 인터페이스를 통해 VPN 트래픽을 다시 외부로 전송할 경우 공개적으로 라우팅 가능한 주소가 비공개 IP 주소를 대체하도록(로컬 IP 주소 풀에서 이미 공개 IP 주소를 사용하지 않는 경우) 인터페이스에 대해 NAT를 활성화해야 합니다.

- Compression Settings(압축 설정) - 압축을 활성화할 기능(WebVPN 및 SSL VPN 클라이언트)을 지정합니다. 압축은 기본적으로 활성화되어 있습니다.

최대 VPN 세션 수 구성

허용되는 최대 VPN 세션 수 또는 AnyConnect 클라이언트 VPN 세션 수를 지정하려면 다음 단계를 수행합니다.

프로시저

단계 1 **Configuration**(구성) > **Remote Access VPN**(원격 액세스 **VPN**) > **Advanced**(고급) > **Maximum VPN Sessions**(최대 **VPN** 세션 수)를 선택합니다.

단계 2 **Maximum AnyConnect Sessions**(최대 **AnyConnect** 세션 수) 필드에 허용되는 최대 세션 수를 입력합니다.

유효한 값의 범위는 1부터 라이센스에서 허용하는 최대 세션 수까지입니다.

단계 **3** **Maximum Other VPN Sessions(**최대 다른 **VPN** 세션 수**)** 필드에 허용되는 최대 VPN 세션(Cisco VPN 클라이언트(IPsec IKEv1) 및 LAN-to-LAN VPN 세션 포함) 수를 입력합니다.

유효한 값의 범위는 1부터 라이센스에서 허용하는 최대 세션 수까지입니다.

단계 **4** **Apply(**적용**)**를 클릭합니다.

DTLS 구성

DTLS(Datagram Transport Layer Security: 데이터그램 전송 계층 보안)를 사용하면 SSL VPN 연결을 설정하는 AnyConnect 클라이언트가 동시에 2개의 터널(SSL 터널 및 DTLS 터널)을 사용할 수 있습니다. DTLS를 사용하면 SSL 연결과 연계된 대기 시간 및 대역폭 문제를 방지하고 패킷 지연에 민감한 실시간 애플리케이션의 성능을 개선할 수 있습니다.

시작하기 전에

이 헤드엔드에서 DTLS 및 사용되는 DTLS 버전을 구성하려면 SSL 설정, 237 페이지의 내용을 참조하십시오.

DTLS가 TLS 연결을 대체하려면 DPD(Dead Peer Detection: 데드 피어 감지)를 활성화해야 합니다. DPD를 활성화하지 않은 경우, DTLS 연결에 문제가 발생하고 TLS로 대체되는 대신 연결이 종료됩니다. DPD에 대한 자세한 내용은 내부 그룹 정책, AnyConnect 클라이언트, 데드 피어 감지, 89 페이지를 참조하십시오.

프로시저

단계 **1** AnyConnect VPN 연결에 대한 DTLS 옵션을 지정합니다.

a) **Configuration(**구성**) > Remote Access VPN(**원격 액세스 **VPN) > Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**) > AnyConnect Connection Profiles(AnyConnect** 연결 프로파일**), Access Interfaces(**액세스 인터페이스**)** 섹션으로 이동합니다.

b) **Interface(**인터페이스**)** 테이블에서, AnyConnect 연결을 구성하려는 인터페이스 행에서, 인터페이스에서 활성화할 프로토콜을 선택합니다.

- **SSL Access/Allow Access(SSL** 액세스**/**액세스 허용**)**를 선택하거나 활성화하면, **Enable DTLS(DTLS** 활성화**)**가 기본적으로 선택되거나 활성화됩니다.
- DTLS를 비활성화하려면 **Enable DTLS(DTLS** 활성화**)**의 선택을 취소합니다. SSL VPN 연결은 SSL VPN 터널에만 연결됩니다.

c) **Port Settings(**포트 설정**)**를 선택하여 **SSL Ports(SSL** 포트**)**를 구성합니다.

- **HTTPS Port(HTTPS** 포트**)** - HTTPS(브라우저 기반) SSL 연결에 대해 활성화할 포트입니다. 범위는 1부터 65535까지입니다. 기본값은 포트 443입니다.
- **DTLS Port(DTLS** 포트**)** - DTLS 연결에 대해 활성화할 UDP 포트입니다. 범위는 1부터 65535까지입니다. 기본값은 포트 443입니다.

단계 2 특정 그룹 정책에 대한 DTLS 옵션을 지정합니다.

a) **Configuration(**구성**) > Remote Access VPN(**원격 액세스 **VPN) > Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**) > Group Policies(**그룹 정책**)**으로 이동한 다음, **Add/Edit(**추가/편집**) > Advanced(**고급**) > AnyConnect Client(AnyConnect** 클라이언트**)**로 이동합니다.

b) Inherit(기본값)를 선택하고, **DTLS(Datagram Transport Layer Security)**에 대해 활성화하거나 비활성화합니다.

c) Inherit(기본값)를 선택하고, DTLS에 대한 압축을 구성하는 **DTLS Compression(DTLS** 압축**)**에 대해 활성화하거나 비활성화합니다.

DNS 서버 그룹 구성

Configuration(구성**) > Remote Access VPN(**원격 액세스 **VPN) > DNS** 대화 상자의 테이블에는 서버 그룹 이름, 서버, 시간 제한(초), 허용되는 재시도 횟수, 도메인 이름 등의 구성된 DNS 서버가 표시됩니다. 이 대화 상자에서 DNS 서버 그룹을 추가, 수정 또는 삭제할 수 있습니다.

- Add or Edit(추가 또는 수정) - Add or Edit DNS Server Group(DNS 서버 그룹 추가 또는 수정) 대화 상자를 엽니다. 다른 곳에 존재하는 항목에 대한 도움말
- Delete(삭제) - 테이블에서 선택한 행을 제거합니다. 확인 또는 실행 취소가 없습니다.
- DNS Server Group(DNS 서버 그룹) - 이 연결에 대한 DNS 서버 그룹으로 사용할 서버를 선택합니다. 기본값은 DefaultDNS입니다.
- Manage(관리) - Configure DNS Server Groups(DNS 서버 그룹 구성) 대화 상자를 엽니다.

암호화 코어 풀 구성

SMP(Symmetric Multi-Processing: 대칭적 다중 처리) 플랫폼에서 암호화 코어의 할당을 변경하여 AnyConnect TLS/DTLS 트래픽의 처리량을 늘릴 수 있습니다. 변경을 통해 SSL VPN 데이터 경로를 가속화하고 AnyConnect, 스마트 터널 및 포트 전달에서 눈에 띄는 성능 향상을 제공할 수 있습니다. 다음 단계에서는 단일 또는 다중 상황 모드에서 암호화 코어의 풀 구성을 설명합니다.

다음 플랫폼에서 암호화 코어 균형 다시 맞추기 작업을 할 수 있습니다.

- 5585-X
- 5545-X
- 5555-X
- ASASM

프로시저

단계 **1** **Configuration(**구성**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **Advanced(**고급**)** > **Crypto Engine(**암호화 엔진**)**을 선택하십시오.

단계 **2** Accelerator Bias(바이어스 가속화) 드롭다운 메뉴에서 암호화 가속화 프로세서를 할당하는 방법을 지정합니다.

참고 이 필드는 ASA에서 기능을 사용할 수 있는 경우에만 표시됩니다.

- **balanced** — 암호화 하드웨어 리소스(Admin/SSL 및 IPsec 코어)를 동등하게 배포합니다.
- **ipsec** — IPsec을 지원하도록 암호화 하드웨어 리소스를 할당합니다(SRTP 암호화된 음성 트래픽 포함).
- **ssl** — Admin/SSL을 지원하도록 암호화 하드웨어 리소스를 할당합니다.

단계 **3** **Apply(**적용**)**를 클릭합니다.

SSL VPN 연결에 대한 클라이언트 주소 지정

이 대화 상자를 사용하여 전역 클라이언트 주소 할당 정책을 지정하고, 인터페이스별 주소 풀을 구성할 수 있습니다. 또한 이 대화 상자를 사용하여 인터페이스별 주소 풀을 추가, 수정 또는 삭제할 수 있습니다. 대화 상자의 아래쪽에 있는 테이블에는 구성된 인터페이스별 주소 풀이 나열됩니다.

- Global Client Address Assignment Policy(전역 클라이언트 주소 할당 정책) - 모든 IPsec 및 SSL VPN 클라이언트 연결(AnyConnect 클라이언트 연결 포함)에 영향을 주는 정책을 구성합니다. ASA에서는 주소를 찾을 때까지 선택된 소스를 순서대로 사용합니다.
  - Use authentication server(인증 서버 사용) - ASA에서 인증 서버를 클라이언트 주소의 소스로 사용해야 하도록 지정합니다.
  - Use DHCP(DHCP 사용) - ASA에서 DHCP를 클라이언트 주소의 소스로 사용해야 하도록 지정합니다.
  - Use address pool(주소 풀 사용) - ASA에서 주소 풀을 클라이언트 주소의 소스로 사용해야 하도록 지정합니다.
- Interface-Specific IPv4 Address Pools(인터페이스별 IPv4 주소 풀) - 구성된 인터페이스별 주소 풀을 나열합니다.
- Interface-Specific IPv6 Address Pools(인터페이스별 IPv6 주소 풀) - 구성된 인터페이스별 주소 풀을 나열합니다.
- Add(추가) - 인터페이스를 선택하고 할당할 주소 풀을 선택할 수 있는 Assign Address Pools to Interface(인터페이스에 주소 풀 할당) 대화 상자를 엽니다.

- Edit(수정) - 인터페이스 및 주소 풀 필드가 채워진 Assign Address Pools to Interface(인터페이스에 주소 풀 할당) 대화 상자를 엽니다.
- Delete(삭제) - 선택한 인터페이스별 주소 풀을 삭제합니다. 확인 또는 실행 취소가 없습니다.

인터페이스에 주소 풀 할당

이 대화 상자를 사용하여 인터페이스를 선택하고 해당 인터페이스에 하나 이상의 주소 풀을 할당할 수 있습니다.

- Interface(인터페이스) - 주소 풀을 할당할 인터페이스를 선택합니다. 기본값은 DMZ입니다.
- Address Pools(주소 풀) - 지정된 인터페이스에 할당할 주소 풀을 지정합니다.
- Select(선택) - 이 인터페이스에 할당할 주소 풀을 하나 이상 선택할 수 있는 Select Address Pools(주소 풀 선택) 대화 상자가 열립니다. 선택한 주소 풀이 Assign Address Pools to Interface(인터페이스에 주소 풀 할당) 대화 상자의 Address Pools(주소 풀)에 표시됩니다.

주소 풀 선택

Select Address Pools(주소 풀 선택) 대화 상자에는 풀 이름, 시작 및 끝 주소, 클라이언트 주소 할당에 사용 가능한 주소 풀의 서브넷 마스크가 표시되며, 목록에서 항목을 추가, 수정 또는 삭제할 수 있습니다.

- Add(추가) - 새 IP 주소 풀을 구성할 수 있는 Add IP Pool(IP 풀 추가) 대화 상자가 열립니다.
- Edit(수정) - 선택한 IP 주소 풀을 수정할 수 있는 Edit IP Pool(IP 풀 수정) 대화 상자가 열립니다.
- Delete(삭제) - 선택한 주소 풀을 제거합니다. 확인 또는 실행 취소가 없습니다.
- Assign(할당) - 해당 인터페이스에 할당된 채로 남아 있는 주소 풀 이름이 표시됩니다. 할당되지 않은 풀 중에 인터페이스에 추가할 각 풀을 두 번 클릭합니다. Assign(할당) 필드의 풀 할당 목록이 업데이트됩니다.

IP 주소 풀 추가 또는 수정

IP 주소 풀을 구성하거나 수정합니다.

- Name(이름) - IP 주소 풀에 할당된 이름을 지정합니다.
- Starting IP Address(시작 IP 주소) - 풀의 첫 번째 IP 주소를 지정합니다.
- Ending IP Address(종료 IP 주소) - 풀의 마지막 번째 IP 주소를 지정합니다.
- Subnet Mask(서브넷 마스크) - 풀의 주소에 적용할 서브넷 마스크를 선택합니다.

그룹 정책

그룹 정책은 사용자 중심 특성/값 쌍의 모음으로, 내부의 ASA 또는 외부의 RADIUS 또는 LDAP 서버에 저장됩니다. VPN 연결이 설정되면 그룹 정책에서는 클라이언트에 특성을 할당합니다. 기본적으로 VPN 사용자는 그룹 정책 연계가 없습니다. 그룹 정책 정보는 VPN 연결 프로파일(터널 그룹) 및 사용자 어카운트에서 사용됩니다.

ASA는 이름이 DfltGrpPolicy인 기본 그룹 정책을 제공합니다. 기본 그룹 정책 매개변수는 모든 그룹 및 사용자에게 가장 공통적인 것으로, 구성 작업을 간소화할 수 있게 도와줍니다. 새 그룹은 이 기본 그룹에서 매개변수를 "상속"할 수 있으며, 사용자는 그룹 또는 기본 그룹에서 매개변수를 "상속"할 수 있습니다. 그룹 및 사용자를 구성할 때 이러한 매개변수를 재정의할 수 있습니다.

내부 및 외부 그룹 정책을 구성할 수 있습니다. 내부 그룹 정책은 로컬에 저장되고, 외부 그룹 정책은 외부에서 RADIUS 또는 LDAP 서버에 저장됩니다.

Group Policy(그룹 정책) 대화 상자에서 다음 매개변수를 구성합니다.

- 일반 특성: 이름, 배너, 주소 풀, 프로토콜, 필터링, 연결 설정.
- 서버: DNS 및 WINS 서버, DHCP 범위, 기본 도메인 이름.
- 고급 특성: 스플릿 터널링, IE 브라우저 프록시, AnyConnect 클라이언트, IPsec 클라이언트.

이러한 매개변수를 구성하기 전에 다음을 먼저 구성해야 합니다.

- 액세스 시간(General(일반) | More Options(추가 옵션) | Access Hours(액세스 시간)).
- 필터(General(일반)| More Options(추가 옵션) | Filters(필터)).
- IPsec 보안 연계(Configuration(구성) | Policy Management(정책 관리) | Traffic Management(트래픽 관리) | Security Associations(보안 연계)).
- 필터링 및 스플릿 터널링에 대한 네트워크 목록(Configuration(구성) | Policy Management(정책 관리) | Traffic Management(트래픽 관리) | Network Lists(네트워크 목록)).
- 사용자 인증 서버 및 내부 인증 서버(Configuration(구성) | System(시스템) | Servers(서버) | Authentication(인증)).

다음과 같은 유형의 그룹 정책을 구성할 수 있습니다.

- 외부 그룹 정책, 65 페이지 - 외부 그룹 정책은 ASA를 RADIUS 또는 LDAP로 안내하여 대부분의 정책 정보를 검색하며, 그렇지 않을 경우 이러한 정책 정보는 내부 그룹 정책에서 구성됩니다. 외부 그룹 정책은 네트워크(클라이언트) 액세스 VPN 연결, 클라이언트리스 SSL VPN 연결 및 사이트 대 사이트 VPN 연결에 대해 같은 방식으로 구성됩니다.
- 내부 그룹 정책, 68 페이지 - 이러한 연결은 엔드포인트에 설치된 VPN 클라이언트를 통해 시작됩니다. VPN 클라이언트의 예로는 AnyConnect Secure Mobility Client 및 Cisco VPN IPsec 클라이언트가 있습니다. VPN 클라이언트가 인증된 후 원격 사용자는 마치 현장에 있는 것처럼 기업 네트워크 또는 애플리케이션에 액세스할 수 있습니다. 원격 사용자와 기업 네트워크 간의 데이터 트래픽은 인터넷을 통과할 때 암호화되어 보호됩니다.

- AnyConnect 클라이언트 내부 그룹 정책, 74 페이지
- 클라이언트리스 SSL VPN 내부 그룹 정책 구성, 99 페이지 - 이를 브라우저 기반 VPN 액세스라고도 합니다. 원격 사용자는 ASA 포털 페이지에 로그인하는 즉시 웹 페이지의 링크를 사용하여 기업 네트워크 및 애플리케이션에 액세스할 수 있습니다. 원격 사용자와 기업 네트워크 간의 데이터 트래픽은 SSL 터널을 통과하여 보호됩니다.
- 사이트 대 사이트 내부 그룹 정책, 104 페이지

Group Policy(그룹 정책) 창 필드

ASDM의 Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > Network (Client) Access(네트워크(클라이언트) 액세스) > Group Policies(그룹 정책) 창에는 최근 구성된 그룹 정책이 나열됩니다. 아래 설명된 것처럼 Add(추가), Edit(수정), Delete(삭제) 버튼을 사용하여 VPN 그룹 정책을 관리할 수 있습니다.

- Add(추가) - 내부 또는 외부 그룹 정책을 추가할 것인지 여부를 선택할 수 있는 드롭다운 목록을 제공합니다. Add(추가)를 클릭하면 기본적으로 내부 그룹 정책이 생성됩니다. Add(추가)를 클릭하면 목록에 새 그룹 정책을 추가할 수 있는 Add Internal Group Policy(내부 그룹 정책 추가) 대화 상자 또는 Add External Group Policy(외부 그룹 정책 추가) 대화 상자가 열립니다. 이 대화 상자는 다음과 같은 3개 메뉴 섹션으로 구성되어 있습니다. 각 메뉴 항목을 클릭하면 매개변수가 표시됩니다. 한 항목에서 다른 항목으로 이동하면 ASDM에서 설정을 유지합니다. 모든 메뉴 섹션에서 매개변수 설정을 마친 후 **Apply(적용)** 또는 **Cancel(취소)**을 클릭합니다.
- Edit(수정) - 기존 그룹 정책을 수정할 수 있는 Edit Group Policy(그룹 정책 수정) 대화 상자가 표시됩니다.
- Delete(삭제) - 목록에서 AAA 그룹 정책을 제거할 수 있습니다. 확인 또는 실행 취소가 없습니다.
- Assign(할당) - 하나 이상의 연결 프로파일에 그룹 정책을 할당할 수 있습니다.
- Name(이름) - 현재 구성된 그룹 정책 이름을 나열합니다.
- Type(유형) - 현재 구성된 각 그룹 정책의 유형을 나열합니다.
- Tunneling Protocol(터널링 프로토콜) - 현재 구성된 각 그룹 정책에서 사용하는 터널링 프로토콜을 나열합니다.
- Connection Profiles/Users Assigned to(이 그룹 정책에 할당된 연결 프로파일/사용자) - ASA에서 바로 구성되어 이 그룹 정책과 연결된 연결 프로파일 및 사용자를 나열합니다.

외부 그룹 정책

외부 그룹 정책은 외부 서버에서 특성 값 권한 부여 및 인증을 검색합니다. 그룹 정책은 ASA에서 특성에 대해 쿼리할 수 있는 RADIUS 또는 LDAP 서버를 식별하고, 이러한 특성을 검색할 때 사용할 비밀번호를 지정합니다.

ASA에 있는 외부 그룹 이름은 RADIUS 서버의 사용자 이름을 나타냅니다. 즉 외부 그룹 X를 ASA에 구성하는 경우, RADIUS 서버는 쿼리를 사용자 X에 대한 인증 요청으로 간주합니다. 따라서 외부 그

룹은 ASA에 특별한 의미가 있는 RADIUS 서버의 사용자 어카운트입니다. 외부 그룹 특성이 인증하려는 사용자와 동일한 RADIUS 서버에 존재하는 경우, 이 둘 간에 이름이 중복되지 않아야 합니다.

외부 서버를 사용하도록 ASA를 구성하려면 먼저 올바른 ASA 권한 부여 속성을 사용하여 해당 서버를 구성해야 하며 이러한 속성의 하위 집합에서 특정한 권한을 개별 사용자에게 할당해야 합니다. "권한 부여 및 인증용 외부 서버"의 지침에 따라 외부 서버를 구성하십시오.

이러한 RADIUS 구성에는 로컬 인증을 사용하는 RADIUS, Active Directory/Kerberos Windows DC를 사용하는 RADIUS, NT/4.0 도메인을 사용하는 RADIUS, LDAP를 사용하는 RADIUS가 포함됩니다.

External Group Policy(외부 그룹 정책**)** 필드

- Name(이름) - 추가 또는 변경할 그룹 정책을 식별합니다. Edit External Group Policy(외부 그룹 정책 수정) 대화 상자의 경우 이 필드는 표시만 됩니다.
- Server Group(서버 그룹) - 이 정책을 적용할 수 있는 서버 그룹을 나열합니다.
- New(새로 만들기) - 새 RADIUS 서버 그룹 또는 새 LDAP 서버 그룹을 만들지 여부를 선택할 수 있는 대화 상자가 열립니다. 이러한 옵션을 선택하면 Add AAA Server Group(AAA 서버 그룹 추가) 대화 상자가 열립니다.
- Password(비밀번호) - 이 서버 그룹 정책의 비밀번호를 지정합니다.

AAA 서버 만들기 및 구성에 대한 내용은 *Cisco ASA Series* 일반적인 작업 *ASDM* 구성 가이드에서 *AAA* 서버 및 로컬 데이터베이스 장을 참조해 주십시오.

AAA 서버로 비밀번호 관리

ASA는 RADIUS 및 LDAP 프로토콜에 대한 비밀번호 관리를 지원합니다. ASA는 LDAP에만 "“password-expire-in-days" 옵션을 지원합니다. 나머지 매개변수는 알림을 지원하는 AAA 서버, 다시 말해서 RADIUS, NT 서버가 포함된 RADIUS, LDAP 서버에 유효합니다. RADIUS 또는 LDAP 인증이 구성되어 있지 않으면 ASA는 이 명령을 무시합니다.

참고 MS-CHAP를 지원하는 일부 RADIUS 서버는 현재 MS-CHAPv2를 지원하지 않습니다. 이 기능에는 MS-CHAPv2가 필요하므로 공급업체에 확인해 주십시오.

ASA에서는 일반적으로 MS-CHAPv2를 지원하는 LDAP 또는 RADIUS 구성을 통해 인증할 때 다음 연결 유형에 대한 비밀번호 관리를 지원합니다.

- AnyConnect VPN 클라이언트
- IPsec VPN 클라이언트
- IPsec IKEv2 클라이언트
- 클라이언트리스 SSL VPN

Kerberos/Active Directory(Windows 비밀번호) 또는 NT 4.0 도메인에 대해서는 비밀번호 관리가 지원되지 않습니다. 예를 들어 Cisco ACS 같은 일부 RADIUS 서버는 인증 요청을 또 다른 인증 서버로 프

록시할 수 있습니다. 그러나 ASA의 관점에서 보면 RADIUS 서버에 대해서만 통신을 수행하는 것입니다.

참고 LDAP의 경우 시중에 출시된 여러 LDAP 서버 전용의 비밀번호 변경 방법이 있습니다. 현재 ASA에서는 Microsoft Active Directory 및 Sun LDAP 서버에만 사용할 수 있는 독점적 비밀번호 관리 로직을 구축하고 있습니다.

기본 LDAP에는 SSL 연결이 필요합니다. LDAP에 대한 비밀번호 관리를 시도하기 전에 LDAP over SSL을 활성화해야 합니다. 기본적으로 LDAP는 포트 636을 사용합니다.

AnyConnect로 비밀번호 지원

ASA는 AnyConnect에 대해 다음과 같은 비밀번호 관리 기능을 지원합니다.

- 사용자가 연결을 시도할 때 비밀번호 만료 알림
- 비밀번호가 만료되기 전에 비밀번호 만료 알림
- 비밀번호 만료 재정의. ASA는 AAA 서버의 비밀번호 만료 알림을 무시하고 사용자의 연결을 인증합니다.

비밀번호 관리가 구성되어 있으면 ASA에서는 원격 사용자가 로그인을 시도할 때 현재 비밀번호가 만료되었음을 또는 곧 만료될 예정임을 알립니다. 그런 다음 ASA에서는 사용자에게 비밀번호를 변경할 기회를 제공합니다. 현재 비밀번호가 아직 만료되지 않은 경우 사용자는 여전히 기존 비밀번호로 로그인할 수 있으며 나중에 비밀번호를 변경할 수 있습니다.

AnyConnect 클라이언트는 비밀번호 변경을 시작할 수는 없고, ASA를 통해 전달되는 AAA 서버의 변경 요청에 응답할 수만 있습니다. AAA 서버는 AD 또는 LDAP 서버로 프록시하는 RADIUS 서버여야 합니다.

ASA는 다음 조건 하에서는 비밀번호 관리를 지원하지 않습니다.

- 로컬(내부) 인증을 사용하는 경우
- LDAP 권한 부여를 사용하는 경우
- RADIUS 인증만 사용하고, 사용자가 RADIUS 서버 데이터베이스에 있는 경우

비밀번호 만료 재정의를 설정하면 ASA는 AAA 서버의 어카운트 비활성화 알림을 무시합니다. 이로 인해 보안 위험이 발생할 수 있습니다. 그 예로, 관리자 비밀번호를 변경할 생각이 없는 경우를 들 수 있습니다.

비밀번호 관리를 활성화하면 ASA에서 AAA 서버로 MS-CHAPv2 인증 요청을 보내게 됩니다.

내부 그룹 정책

내부 그룹 정책, 일반 특성

Configuration(구성**) > Remote Access VPN(**원격 액세스 **VPN) > Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**) > Group Policies(**그룹 정책**)** 창에서 Add or Edit Group Policy(그룹 정책 추가 또는 수정) 대화 상자를 사용하면 추가하거나 수정할 그룹 정책에 대해 터널링 프로토콜, 필터, 연결 설정, 서버를 지정할 수 있습니다. 이 대화 상자의 각 필드에 대해 Inherit(상속) 확인란을 선택하면 해당 설정에 기본 그룹 정책의 값을 적용할 수 있습니다. Inherit(상속)는 이 대화 상자의 모든 특성에 대한 기본값입니다.

Configuration(구성**) > Remote Access VPN(**원격 액세스 **VPN) > Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**) > Group Policies(**그룹 정책**) > Add/Edit(**추가/수정**) > General(**일반**)**을 선택하여 ASDM에서 내부 그룹 정책의 일반 속성을 구성할 수 있습니다. 다음 속성은 SSL VPN 및 IPsec 세션에 적용됩니다. 예를 들어 일부 특성이 한 세션 유형에 대해서는 최신 상태이지만 다른 세션 유형에 대해서는 그렇지 않은 경우가 있습니다.

- **Name(**이름**)** - 이 그룹 정책의 이름을 지정합니다. 최대 64자까지 가능하며 공백을 사용할 수 있습니다. Edit(수정) 기능이 따로 있기 때문에 이 필드는 읽기 전용입니다.
- **Banner(**배너**)** - 로그인 시 사용자에게 표시되는 배너 텍스트를 지정합니다. 길이는 최대~4000자가 될 수 있습니다. 기본값은 없습니다.

  IPsec VPN 클라이언트는 배너에 대해 전체 HTML을 지원합니다. 그러나 클라이언트리스 포털 및 AnyConnect 클라이언트는 부분 HTML을 지원합니다. 원격 사용자에게 배너를 올바르게 표시하려면 다음 지침을 따르십시오.

  - IPsec 클라이언트 사용자를 위해서는 /n 태그를 사용합니다.
  - AnyConnect 클라이언트 사용자의 경우
 태그를 사용합니다.

- **SCEP forwarding URL(SCEP** 전달 **URL)** - CA 주소이며 클라이언트 프로필에 SCEP 프록시가 구성된 경우에 필요합니다.
- **Address Pools(**주소 풀**)** - 이 그룹 정책에 사용할 하나 또는 여러 IPv4 주소의 이름을 지정합니다. Inherit(상속) 확인란을 선택하면 그룹 정책에서는 Default Group Policy(기본 그룹 정책)에 지정된 IPv4 주소 풀을 사용합니다. IPv4 주소 풀 추가 또는 수정에 대한 내용을 참조해 주십시오.

  참고 내부 그룹 정책에 대해 IPv4 및 IPv6 주소 풀을 모두 지정할 수 있습니다.

  Select(선택**)** - 이 버튼을 활성화하려면 Inherit(상속) 확인란의 선택을 취소합니다. **Select(**선택**)**를 클릭하면 Address Pools(주소 풀) 대화 상자가 열립니다. 이 대화 상자에는 풀 이름, 시작 및 끝 주소, 클라이언트 주소 할당에 사용 가능한 주소 풀의 서브넷 마스크가 표시되며 해당 목록의 항목을 추가, 수정, 삭제 및 할당할 수 있습니다.

- **IPv6 Address Pools(IPv6** 주소 풀**)** - 이 그룹 정책에 사용할 하나 또는 여러 IPv6 주소 풀의 이름을 지정합니다.

Select(선택) - 이 버튼을 활성화하려면 Inherit(상속) 확인란의 선택을 취소합니다. **Select(**선택**)**를 클릭하면 앞에서 설명한 Select Address Pools(주소 풀 선택) 대화 상자가 열립니다. IPv6 주소 풀 추가 또는 수정에 대한 내용은 을 참조해 주십시오.

- **More Options(**추가 옵션**)** - 필드 오른쪽의 아래로 화살표를 클릭하여 이 그룹 정책에 대해 구성 가능한 추가 옵션을 표시합니다.
- **Tunneling Protocols(**터널링 프로토콜**)** - 이 그룹에서 사용할 수 있는 터널링 프로토콜을 지정합니다. 사용자는 선택된 프로토콜만 사용할 수 있습니다. 선택 항목은 다음과 같습니다.
  - **Clientless SSL VPN(**클라이언트리스 **SSL VPN)** - SSL/TLS를 통해 VPN을 사용하도록 지정합니다. 이 프로토콜을 선택하면 웹 브라우저를 사용하여 ASA에 안전한 원격 액세스 터널이 설정됩니다. 소프트웨어나 하드웨어 클라이언트가 필요 없습니다. 클라이언트리스 SSL VPN을 사용하면 HTTPS 인터넷 사이트에 연결할 수 있는 거의 모든 컴퓨터에서 기업 웹사이트, 웹 지원 애플리케이션, NT/AD 파일 공유(웹 지원), 이메일 및 기타 TCP 기반 애플리케이션 등의 광범위한 엔터프라이즈 리소스에 손쉽게 액세스할 수 있습니다.
  - **SSL VPN Client(SSL VPN** 클라이언트**)** - Cisco AnyConnect VPN 클라이언트 또는 기존 SSL VPN 클라이언트를 사용하도록 지정합니다. AnyConnect 클라이언트를 사용 중인 경우 MUS(Mobile User Security)를 지원하려면 이 프로토콜을 선택해야 합니다.
  - **IPsec IKEv1** - IP 보안 프로토콜입니다. 가장 안전한 프로토콜로 간주되는 IPsec은 VPN 터널에 가장 완벽한 아키텍처를 제공합니다. 사이트 대 사이트(피어 대 피어(peer-to-peer)) 연결과 Cisco VPN client-to-LAN 연결 모두에 IPsec IKEv1을 사용할 수 있습니다.
  - **IPsec IKEv2** - AnyConnect Secure Mobility Client에서 지원합니다. IPsec과 IKEv2를 사용하는 AnyConnect 연결은 소프트웨어 업데이트, 클라이언트 프로파일, GUI 현지화(번역) 및 사용자 지정, Cisco Secure Desktop, SCEP 프록시 등의 고급 기능을 제공합니다.
  - **L2TP over IPsec** - 여러 공용 PC 및 모바일 PC 운영 체제와 함께 제공되는 VPN 클라이언트를 사용하는 원격 사용자가 공용 IP 네트워크를 통해 보안 어플라이언스 및 사설 기업 네트워크에 대한 보안 연결을 설정할 수 있도록 해줍니다. L2TP는 데이터를 터널링하기 위해 UDP(포트 1701)를 통한 PPP를 사용합니다. IPsec 전송 모드에 대해 보안 어플라이언스를 구성해야 합니다.
- **Filter(**필터**)** - IPv4 또는 IPv6 연결에 어떤 액세스 제어 목록을 사용할 것인지, 또는 그룹 정책의 값을 상속할 것인지 여부를 지정합니다. 필터는 소스 주소, 대상 주소 및 프로토콜 등의 기준에 따라 ASA를 통해 수신하는 터널링된 데이터 패킷의 허용 또는 거부 여부를 결정하는 규칙으로 구성됩니다. 필터 및 규칙을 구성하려면 **Manage(**관리**)**를 클릭합니다.
- **NAC Policy(NAC** 정책**)** - 이 그룹 정책에 적용할 NAC(Network Admission Control) 정책의 이름을 선택합니다. 선택적인 NAC 정책을 각 그룹 정책에 할당할 수 있습니다. 기본값은 --None(없음)--입니다.
- **Manage(**관리**)** - Configure NAC Policy(NAC 정책 구성) 대화 상자를 엽니다. 하나 이상의 NAC 정책을 구성하면 NAC 정책 이름이 NAC Policy(NAC 정책) 특성 옆에 있는 드롭다운 목록에 옵션으로 표시됩니다.

- **Access Hours(**액세스 시간**)** - 이 사용자에게 적용되는 기존 액세스 시간 정책의 이름을 선택하거나(있는 경우) 새 액세스 시간 정책을 만듭니다. 기본값은 Inherit(상속)이며 Inherit(상속) 확인란을 선택하지 않을 경우 기본값은 Unrestricted(제한 없음)입니다. **Manage(**관리**)**를 클릭하면 시간 범위를 추가, 수정 또는 삭제할 수 있는 Browse Time Range(시간 범위 찾아보기) 대화 상자가 열립니다.
- **Simultaneous Logins(**동시 로그인 수**)** - 이 사용자에게 허용되는 최대 동시 로그인 수를 지정합니다. 기본값은 3입니다. 최소값은 0이며, 이 경우 로그인이 비활성화되고 사용자 액세스가 차단됩니다.

  참고 최대 한도는 없지만 여러 동시 연결을 허용하면 보안이 취약해지고 성능이 저하될 수 있습니다.

- **Restrict Access to VLAN(VLAN**에 대한 액세스 제한**)** - (선택 사항) "VLAN 매핑"이라고도 부르는 이 파라미터는 이 그룹 정책이 적용되는 세션의 이그레스(egress) VLAN 인터페이스를 지정합니다. ASA에서는 이 그룹의 모든 트래픽을 선택된 VLAN으로 전달합니다. 이 특성을 사용하여 그룹 정책에 VLAN을 할당하면 액세스 제어를 간소화할 수 있습니다. ACL을 사용하여 세션의 트래픽을 필터링하는 방법 대신 이 특성에 값을 할당하는 방법도 가능합니다. 기본값(Unrestricted(제한 없음)) 이외에는 이 ASA에 구성된 VLAN만 드롭다운 목록에 표시됩니다.

  참고 이 기능은 HTTP 연결에 사용할 수 있지만 FTP 및 CIFS에는 사용할 수 없습니다.

- **Connection Profile (Tunnel Group) Lock(**연결 프로필**(**터널 그룹**)** 잠금**)** - 이 파라미터는 선택된 연결 프로필(터널 그룹)을 이용한 원격 VPN 액세스만 허용하고 다른 연결 프로필을 이용한 액세스를 차단합니다. 기본 상속 값은 None(없음)입니다.
- **Maximum Connect Time(**최대 연결 시간**) - Inherit(**상속**)** 체크 박스를 선택하지 않은 경우 이 파라미터는 최대 사용자 연결 시간(분)을 설정합니다.

  이 시간이 경과하면 연결이 자동으로 종료됩니다. 최소값은 1분이고 최대값은 35,791,394분(4,000년 이상)입니다. 무제한 연결 시간을 허용하려면 **Unlimited(**무제한**)**(기본값)를 선택합니다.
- **Idle Timeout(**유휴 시간 제한**) - Inherit(**상속**)** 체크 박스를 선택하지 않은 경우 이 파라미터는 유휴 시간 제한(분)을 지정합니다.

  이 기간 동안 연결을 통한 통신 활동이 없는 경우 시스템은 연결을 종료합니다. 최소 시간은 1분, 최대 시간은 10080분, 기본값은 30분입니다. 무제한 연결 시간을 허용하려면 **Unlimited(**무제한**)**를 선택합니다.
- **SGT(Security Group Tag)** - 이 그룹 정책을 사용하여 연결하는 VPN 사용자에게 할당될 SGT 태그의 숫자 값을 입력합니다.
- **On smart card removal(**스마트 카드 제거 시**)** - 기본값인 Disconnect(연결 해제)를 선택할 경우 인증에 사용되는 스마트 카드가 제거되면 클라이언트에서 연결을 해제합니다. 사용자가 연결 시

간 내내 스마트 카드를 컴퓨터에 연결하지 않아도 되도록 설정하려면 **Keep the connection(**연결 유지**)**을 클릭합니다.

스마트 카드 제거 구성은 RSA 스마트 카드를 사용하는 Microsoft Windows에서만 작동합니다.

- **Maximum Connection Time Alert Interval(**최대 연결 시간 알림 간격**)** - 최대 연결 시간에 도달하여 사용자에게 메시지가 표시되기 전까지의 시간 간격입니다.

  Inherit(상속**)** 확인란의 선택을 취소하면 **Default(**기본값**)** 확인란이 자동으로 선택됩니다. 이 경우 세션 알림 간격이 30분으로 설정됩니다. 새 값을 지정하려면 **Default(**기본값**)**의 선택을 취소하고 세션 알림 간격을 1분에서 30분 사이로 지정합니다.

- **Periodic Authentication Interval(**주기적 인증 간격**)** - 인증서 인증을 주기적으로 다시 수행하기 전까지의 시간 간격(시간)입니다.

  Inherit(상속**)** 체크 박스가 선택되지 않은 경우 주기적인 인증서 확인을 수행할 간격을 설정할 수 있습니다. 범위는 1~168시간이며 기본값은 비활성화되어 있습니다. 무제한 확인을 허용하려면 Unlimited(무제한)를 선택합니다.

내부 그룹 정책, 서버 특성 구성

Group Policy(그룹 정책) > Servers(서버) 창에서 DNS 서버, WINS 서버 및 DHCP 범위를 구성합니다. DNS 및 WINS 서버는 전체 터널 클라이언트(IPsec, AnyConnect, SVC 및 L2TP/IPsec)에만 적용되고 이름 확인에 사용됩니다. DHCP 범위는 DHCP 주소 할당이 정상적인 경우에 사용됩니다.

프로시저

단계 **1** **Configuration(**구성**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**)** > **Group Policies(**그룹 정책**)** > **Add/Edit(**추가/수정**)** > **Servers(**서버**)**를 선택하십시오.

단계 **2** DefaultGroupPolicy를 수정하지 않을 경우 DNS Servers **Inherit(**상속**)** 확인란의 선택을 취소합니다.

단계 **3** DNS Servers(DNS 서버) 필드에서, 이 그룹이 사용할 DNS 서버의 IPv4 또는 IPv6 주소를 추가합니다. 두 개의 IPv4 주소와 두 개의 IPv6 주소를 지정할 수 있습니다.

DNS 서버를 두 개 이상 지정할 경우 원격 액세스 클라이언트는 이 필드에 지정된 순서대로 DNS 서버를 사용합니다.

여기서 수행하는 변경 작업은 이 그룹 정책을 사용하는 클라이언트에 대해 ASDM의 **Configuration(**구성**) > Remote Access VPN(**원격 액세스 **VPN) > DNS** 창에서 구성한 DNS 설정을 재정의합니다.

단계 **4** WINS Servers **Inherit(**상속**)** 확인란의 선택을 취소합니다.

wins-server value {**ip_address** [*ip_address*] | **none**}

단계 **5** WINS Servers(WINS 서버) 필드에서 기본 및 보조 WINS 서버의 IP 주소를 입력합니다. 첫 번째 지정하는 IP 주소는 기본 WINS 서버의 IP 주소입니다. 두 번째(선택 사항) 지정하는 IP 주소는 보조 WINS 서버의 IP 주소입니다.

wins-server 명령을 입력할 때마다 기존 설정이 덮어쓰기됩니다. 예를 들어 WINS 서버 x.x.x.x를 구성한 후 WINS 서버 y.y.y.y를 구성하는 경우 두 번째 명령이 첫 번째 명령을 덮어쓰고, y.y.y.y가 유일한

WINS 서버가 됩니다. 여러 서버의 경우에도 마찬가지입니다. 이전에 구성한 서버를 덮어쓰지 않고 WINS 서버를 추가하려면 이 명령을 입력할 때 모든 WINS 서버의 IP 주소를 포함하십시오.

예제:

다음 예에서는 이름이 CLI에서 FirstGroup인 그룹 정책에 대해 IP 주소 10.10.10.15 및 10.10.10.30을 사용하여 WINS 서버를 구성하는 방법을 보여줍니다.

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# wins-server value 10.10.10.15 10.10.10.30
hostname(config-group-policy)#
```

단계 **6** More Options(추가 옵션) 막대의 이중 아래로 화살표를 클릭하여 **More Options(**추가 옵션**)** 영역을 확장합니다.

단계 **7** **Configuration(**구성**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **DNS** 창에 지정된 기본 도메인이 없을 경우 **Default Domain(**기본 도메인**)** 필드에서 기본 도메인을 지정해야 합니다. 예를 들어 example.com과 같은 도메인 이름과 최상위 도메인을 사용하십시오.

단계 **8** **OK(**확인**)**를 클릭합니다.

단계 **9** **Apply(**적용**)**를 클릭합니다.

내부 그룹 정책, 브라우저 프록시

Configuration(구성**) > Remote Access VPN(**원격 액세스 **VPN) > Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**) > Group Policies(**그룹 정책**) > Add/Edit(**추가/수정**) > Advanced(**고급**) > Browser Proxy(**브라우저 프록시**)**

이 대화 상자는 클라이언트에 푸시다운되는 특성을 구성하여 Microsoft Internet Explorer 설정을 재구성합니다.

- Proxy Server Policy(프록시 서버 정책) - 클라이언트 PC에 대해 Microsoft Internet Explorer 브라우저 프록시 작업("메서드")을 구성합니다.
  - Do not modify client proxy settings(클라이언트 프록시 설정 수정 안 함) - 이 클라이언트 PC에 대해 Internet Explorer의 HTTP 브라우저 프록시 서버 설정을 변경하지 않습니다.
  - Do not use proxy(프록시 사용 안 함) - 클라이언트 PC에 대해 Internet Explorer의 HTTP 프록시 설정을 비활성화합니다.
  - Select proxy server settings from the following(다음 중에서 프록시 서버 설정 선택) - Auto detect proxy(프록시 자동 탐지), Use proxy server settings given below(아래 제공된 프록시 서버 설정 사용), Use proxy auto configuration (PAC) given below(아래 제공된 프록시 자동 구성(PAC) 사용)의 확인란을 활성화합니다.
  - Auto detect proxy(프록시 자동 탐지) - 클라이언트 PC에 대해 Internet Explorer의 자동 프록시 서버 탐지 사용을 활성화합니다.
  - Use proxy server settings specified below(아래 제공된 프록시 서버 설정 사용) - Proxy Server Name or IP Address(프록시 서버 이름 또는 IP 주소) 필드에 구성된 값을 사용하도록 Internet Explorer에서 HTTP 프록시 서버 설정을 구성합니다.

- Use proxy auto configuration (PAC) given below(아래 제공된 프록시 자동 구성(PAC) 사용) - 프록시 자동 구성(PAC) 필드에 지정된 파일을 자동 구성 특성의 소스로 사용하도록 지정합니다.

- Proxy Server Settings(프록시 서버 설정) - Microsoft Internet Explorer를 사용하는 Microsoft 클라이언트의 프록시 서버 매개변수를 구성합니다.
  - Server Address and Port(서버 주소 및 포트) - 이 클라이언트 PC에 적용되는 Microsoft Internet Explorer 서버의 IP 주소 또는 이름과 포트를 지정합니다.
  - Bypass Proxy Server for Local Addresses(로컬 주소에 프록시 서버 사용 안 함) - 클라이언트 PC에 대해 Microsoft Internet Explorer 브라우저 프록시 로컬-우회 설정을 구성합니다. 로컬 우회를 활성화하려면 **Yes(**예**)**, 비활성화하려면 **No(**아니요**)**를 클릭합니다.
  - Exception List(예외 목록) - 프록시 서버 액세스에서 제외할 서버 이름 및 IP 주소를 나열합니다. 프록시 서버를 통해 액세스하지 못하게 하려는 주소 목록을 입력합니다. 이 목록은 Internet Explorer 프록시 설정 대화 상자의 예외 목록에 해당합니다.

- Proxy Auto Configuration Settings(프록시 자동 구성 설정) - PAC URL은 자동 구성 파일의 URL을 지정합니다. 이 파일은 프록시 정보를 검색할 위치를 브라우저에 알려줍니다. 프록시 자동 구성(PAC) 기능을 사용하려면 원격 사용자가 Cisco AnyConnect VPN 클라이언트를 사용해야 합니다.

  많은 네트워크 환경에서 웹 브라우저를 특별한 네트워크 리소스에 연결하는 HTTP 프록시를 정의합니다. 브라우저에 프록시가 지정되어 있고 클라이언트가 HTTP 트래픽을 프록시로 전달하는 경우에만 HTTP 트래픽이 네트워크 리소스에 도달할 수 있습니다. 엔터프라이즈 네트워크로 터널링할 때 필요한 프록시는 광대역 연결을 통해 인터넷에 연결할 때 또는 서드파티 네트워크에 있을 때 필요한 프록시와 다를 수 있기 때문에 SSLVPN 터널은 HTTP 프록시의 정의를 복잡하게 만듭니다.

  또한 대규모 네트워크를 보유한 회사는 프록시 서버를 둘 이상 구성하고, 상황에 따라 사용자에게 선택권을 제공해야 할 수 있습니다. .pac 파일을 통해 관리자는 엔터프라이즈 전체에서 모든 클라이언트 컴퓨터가 여러 프록시 중 어떤 것을 사용해야 할지 결정하는 단일 스크립트 파일을 작성할 수 있습니다.

  다음은 PAC 파일을 사용하는 방법을 보여주는 몇 가지 예입니다.

  - 로드 밸런싱 목록에서 무작위로 프록시 선택
  - 서버 유지 관리 일정에 맞게 시간별 또는 요일별로 돌아가며 프록시 사용
  - 기본 프록시에 장애가 발생하는 경우 사용할 백업 프록시 서버 지정
  - 로컬 서브넷을 기반으로 사용자 로밍을 위한 가장 가까운 프록시 지정

  텍스트 편집기를 사용하여 브라우저용 프록시 자동 구성(.pac) 파일을 만들 수 있습니다. .pac 파일은 URL의 내용에 따라 하나 이상의 사용할 프록시 서버를 지정하는 논리가 포함된 JavaScript 파일입니다. PAC URL 필드를 사용하여 .pac 파일을 검색할 URL을 지정해 주십시오. 그러면 브라우저에서 .pac 파일을 사용하여 프록시 설정을 확인합니다.

- 프록시 잠금

- Allow Proxy Lockdown for Client System(클라이언트 시스템에 대해 프록시 잠금 허용) - 이 기능을 활성화하면 AnyConnect VPN 세션 동안 Microsoft Internet Explorer의 연결 탭이 숨겨집니다. 이 기능을 비활성화하면 연결 탭 디스플레이가 그대로 유지됩니다. 사용자 레지스트리 설정에 따라 탭의 기본 설정이 표시될 수도 있고 숨겨질 수도 있습니다.

AnyConnect 클라이언트 내부 그룹 정책

Internal Group Policy(내부 그룹 정책) > Advanced(고급) > AnyConnect Client(AnyConnect 클라이언트)

- Keep Installer on Client System(클라이언트 시스템에서 설치 프로그램 유지) - 원격 컴퓨터에 영구 클라이언트를 설치할 수 있도록 하려면 활성화합니다. 이렇게 구성하면 클라이언트 자동 제거 기능이 비활성화됩니다. 원격 사용자의 연결 시간을 줄일 수 있도록 후속 연결을 위해 원격 컴퓨터에 클라이언트가 설치된 상태로 있습니다.
- Compression(압축) - 압축하면 전송되는 패킷 크기가 작아져서 보안 어플라이언스와 클라이언트 간의 통신 성능이 향상됩니다.
- Datagram TLS - DTLS는 일부 SSL 연결과 관련된 레이턴시 및 대역폭 문제를 방지하고 패킷 지연에 민감한 실시간 애플리케이션의 성능을 향상시킵니다.
- Ignore Don't Defrag (DF) Bit(조각 모음 안 함(DF) 비트 무시) - 이 기능은 DF 비트가 설정된 패킷의 강제 조각화를 허용하여 터널을 통과할 수 있게 해줍니다. 예를 들면, 네트워크에서 TCP MSS 협상에 제대로 응답하지 않는 서버에 사용할 수 있습니다.
- Client Bypass Protocol(클라이언트 우회 프로토콜) - Client Protocol Bypass(클라이언트 프로토콜 우회) 기능을 사용하면 IPv6 트래픽만 예상될 때 ASA에서 IPv4 트래픽을 관리하는 방식 또는 IPv4 트래픽만 예상될 때 ASA에서 IPv6 트래픽을 관리하는 방식을 구성할 수 있습니다.

  AnyConnect 클라이언트가 ASA와의 VPN 연결을 수행할 때 ASA는 IPv4, IPv6 주소를 또는 IPv4 및 IPv6 주소 모두 지정할 수 있습니다. ASA가 AnyConnect 연결에 IPv4 주소만 또는 IPv6 주소만 지정할 경우, ASA에서 IP 주소를 지정하지 않은 네트워크 트래픽을 삭제하거나 이 트래픽이 ASA를 우회하여 암호화되지 않은 "일반 텍스트" 형태로 클라이언트에서 전송되는 것을 허용하도록 클라이언트 우회 프로토콜을 구성할 수 있습니다.

  예를 들어, ASA에서 AnyConnect 연결에 IPv4 주소만 지정하고 엔드포인트가 이중 스택이라고 가정합니다. 엔드포인트가 IPv6 주소에 연결하려고 시도할 때 클라이언트 우회 프로토콜이 비활성화된 경우 IPv6 트래픽이 끊기지만 클라이언트 우회 프로토콜이 활성화된 경우, IPv6 트래픽은 클라이언트에서 암호화되지 않은 상태로 전송됩니다.
- FQDN of This Device(이 디바이스의 FQDN) - 네트워크 로밍 이후에 VPN 세션 재설정에 사용되는 ASA IP 주소를 확인하기 위해 클라이언트에서 이 정보를 사용합니다. 이 설정은 IP 프로토콜이 서로 다른 네트워크 간(예: IPv4에서 IPv6로)에 로밍을 지원하는 핵심 설정입니다.

참고 AnyConnect 프로파일에 있는 ASA FQDN을 사용하여 로밍 후에 ASA IP 주소를 얻을 수 없습니다. 주소가 부하 균형 시나리오에 있는 올바른 디바이스(터널이 설정된 디바이스)와 일치하지 않을 수 있습니다.

FQDN 디바이스가 클라이언트에 푸시되지 않은 경우, 클라이언트는 터널에서 이전에 설정한 모든 IP 주소에 재연결하려고 시도합니다. 서로 다른 IP 프로토콜로 구성된 네트워크 사이의 로밍(예: IPv4에서 IPv6로)을 지원하려면 터널 재설정에 사용할 ASA 주소를 확인할 수 있도록 로밍 후에 AnyConnect에서 디바이스 FQDN의 이름 확인 작업을 수행해야 합니다. 클라이언트는 초기 연결 동안 프로파일에 있는 ASA FQDN을 사용합니다. 후속 세션 재연결 동안 사용 가능한 경우 ASA에서 푸시하고 그룹 정책에서 관리자가 구성한 디바이스 FQDN을 항상 사용합니다. FQDN이 구성되지 않은 경우, ASA는 Device Setup(디바이스 설정) > Device Name/Password and Domain Name(디바이스 이름/비밀번호 및 도메인 이름) 아래 설정에서 디바이스 FQDN을 파생시키고 이를 클라이언트에 전송합니다.

디바이스 FQDN이 ASA에서 푸시되지 않은 경우, 클라이언트는 여러 IP 프로토콜의 네트워크 간 로밍 후에 VPN 세션을 재설정할 수 없습니다.

- MTU - SSL 연결의 MTU 크기를 조정합니다. 256~1410바이트 사이의 값을 입력합니다. 기본적으로 MTU 크기는 연결 시 사용하는 인터페이스의 MTU에 기초하여 IP/UDP/DTLS 오버헤드를 뺀 값으로 자동으로 조정됩니다.
- Keepalive Messages(킵얼라이브 메시지) - 디바이스에서 연결에 허용되는 유휴 시간을 제한하더라도 프록시, 방화벽 또는 NAT 디바이스를 통한 연결이 계속 열려 있도록 Interval(간격) 필드에 15~600 사이의 숫자(초)를 입력하여 킵얼라이브 메시지를 활성화하고 간격을 조정합니다. 또한 이 간격을 조정함으로써 원격 사용자가 소켓 기반 애플리케이션(예: Microsoft Outlook, Microsoft Internet Explorer)을 능동적으로 실행하고 있지 않을 때 클라이언트의 연결이 끊겼다가 다시 연결되는 현상을 방지할 수 있습니다.
- **Optional Client Modules to Download(**다운로드할 선택적 클라이언트 모듈**)** - 다운로드 시간을 최소화하기 위해 AnyConnect 클라이언트는 지원하는 각 기능에 꼭 필요한 모듈의 다운로드만 ASA에서 요청합니다. 다른 기능을 활성화하는 모듈의 이름을 지정해야 합니다. AnyConnect 클라이언트에는 다음 모듈이 포함되어 있습니다(일부 이전 버전은 모듈 수가 더 적음).
  - AnyConnect DART - DART(Diagnostic AnyConnect Reporting Tool)는 시스템 로그 및 기타 진단 정보를 캡처하여 데스크톱에 .zip 파일을 만듭니다. 따라서 편리하게 Cisco TAC로 문제 해결 정보를 보낼 수 있습니다.
  - AnyConnect Network Access Manager - 이전에 Cisco Secure Services Client로 불리던 이 모듈은 802.1X(계층 2)와 유선 및 무선 네트워크에 액세스하기 위한 디바이스 인증을 제공합니다.
  - AnyConnect SBL - SBL(Start Before Logon:로그온 전 시작 사용)은 Windows 로그인 대화 상자가 나타나기 전에 AnyConnect를 시작하여 Windows에 로그온하기 전에 VPN 연결을 통하여 사용자를 엔터프라이즈 인프라에 연결시킵니다.
  - AnyConnect Web Security Module - 이전에 ScanSafe Hostscan으로 불리던 이 모듈은 AnyConnect로 통합되었습니다. 이 모듈은 각 요소를 동시에 분석하기 위해 웹 페이지의 요소를 해체합

니다. 그런 다음 정의된 보안 정책에 따라 적합한 콘텐츠를 허용하고 악의적이거나 적합하지 않은 콘텐츠는 차단할 수 있습니다.

- AnyConnect Telemetry Module - 악성 콘텐츠 출처에 대한 정보를 Cisco IronPort WSA(Web Security Appliance)의 웹 필터링 인프라로 보냅니다. WSA에서는 이 데이터를 사용하여 향상된 URL 필터링 규칙을 제공합니다.

  참고 AnyConnect 버전 4.0에서는 Telemetry 모듈이 지원되지 않습니다.

- ASA Posture Module - 이전에 Cisco Secure Desktop HostScan 기능이라고 한 상태 모듈은 AnyConnect로 통합되었으며, ASA에 대한 원격 액세스 연결을 만들기 전에 상태 평가에 필요한 크리덴셜을 수집하는 기능을 AnyConnect에 제공합니다.
- ISE Posture — OPSWAT v3 라이브러리를 사용하여 엔드포인트의 컴플라이언스를 평가하기 위한 상태 확인을 수행합니다. 그런 다음 엔드포인트가 규정을 준수할 때까지 네트워크 액세스를 제한하거나 로컬 사용자 권한을 상승시킬 수 있습니다.
- AMP Enabler — 엔드포인트용 AMP(Advanced Malware Protection)를 구축하기 위한 매체로 사용됩니다. AMP Enabler는 엔터프라이즈 내의 로컬로 호스팅되는 서버에서 엔드포인트 하위 집합으로 엔드포인트용 AMP 소프트웨어를 푸시하고 기존 사용자 기반에 대해 AMP 서비스를 설치합니다.
- 네트워크 가시성 모듈 — 용량 및 서비스 계획, 감사, 컴플라이언스 및 보안 분석을 수행하기 위한 엔터프라이즈 관리자의 역량을 개선합니다. NVM은 엔드포인트 텔레메트리를 수집하고 syslog에서 플로우 데이터와 파일 평판을 로그하고 파일 분석을 수행하고 UI 인터페이스를 제공하는 컬렉터(서드파티 벤더)로 플로우 레코드를 내보냅니다.
- Umbrella 로밍 보안 모듈 — 활성 VPN이 없을 때 DNS 레이어 보안을 제공합니다. 이 모듈은 Cisco Umbrella 로밍 서비스 또는 OpenDNS Umbrella 서비스에 서브스크립션을 제공하고 지능형 프록시 및 IP 레이어 시행 기능을 추가로 제공합니다. Umbrella 보안 로밍 프로필은 각 구축을 해당하는 서비스와 연결하며 해당하는 보호 레벨(콘텐츠 필터링, 여러 정책, 강력한 보고, Active Directory 통합 또는 기본 DNS 레이어 보안)을 자동으로 활성화합니다.

- Always-On VPN - AnyConnect 서비스 프로파일의 Always-On VPN 플래그 설정이 비활성화되었는지 또는 AnyConnect 서비스 프로파일 설정을 사용해야 하는지 확인합니다. Always-On VPN 기능은 사용자가 컴퓨터에 로그온한 후 AnyConnnect에서 자동으로 VPN 세션을 설정할 수 있게 해줍니다. VPN 세션은 사용자가 컴퓨터에서 로그오프할 때까지 유지됩니다. 물리적 연결이 해제될 경우 세션이 유지되고, AnyConnect는 ASA를 통해 물리적 연결을 다시 설정하여 VPN 세션을 재개하려고 계속 시도합니다.

  Always-On VPN은 기업 정책을 시행하여 보안 위협으로부터 디바이스를 보호하는 것을 허용합니다. 이 기능을 사용하면 엔드포인트가 신뢰할 수 있는 네트워크에 있지 않을 때마다 AnyConnect에서 VPN 세션을 설정하게 할 수 있습니다. 활성화하면 연결이 없을 때 네트워크 연결을 어떻게 관리할 것인지를 결정하는 정책이 구성됩니다.

참고 Always-On VPN을 사용하려면 AnyConnect Secure Mobility 기능을 지원하는 AnyConnect 버전이 필요합니다.

-
-
- Client Profiles to Download(다운로드할 클라이언트 프로필) - 프로필은 AnyConnect 클라이언트에서 VPN, 네트워크 액세스 관리자, 웹 보안, ISE Posture, AMP Enabler, 네트워크 가시성 모듈 및 Umbrella 로밍 보안 모듈 설정을 구성하는 데 사용하는 구성 파라미터 그룹입니다. **Add(**추가**)**를 클릭하여 Select AnyConnect Client Profiles(AnyConnect 클라이언트 프로필 선택) 창을 실행하고 이 그룹 정책에 대해 이전에 만든 프로필을 지정할 수 있습니다.

AnyConnect 트래픽에 대한 스플릿 터널링 구성

스플릿 터널링은 일부 AnyConnect 네트워크 트래픽(암호화됨)을 VPN 터널을 통해 보내고 기타 네트워크 트래픽(암호화되지 않은 "일반 텍스트")을 VPN 터널 외부로 보냅니다.

스플릿 터널링은 스플릿 터널링 정책을 생성하고, 이 정책에 대해 액세스 제어 목록을 구성하며 그룹 정책에 스플릿 터널 정책을 추가하는 방법으로 구성됩니다. 그룹 정책이 클라이언트에 전송되는 경우 이 클라이언트는 스플릿 터널링 정책에서 ACL을 사용하여 네트워크 트래픽을 어디로 보낼지 결정합니다.

참고 스플릿 터널링은 보안 기능이 아니라 트래픽 관리 기능입니다. 최상의 보안을 위해 스플릿 터널링을 활성화하지 않는 것이 좋습니다.

Windows 클라이언트의 경우 ASA의 방화벽 규칙을 먼저 평가한 후 클라이언트의 방화벽 규칙을 평가합니다. Mac OS X의 경우 클라이언트의 방화벽 및 필터 규칙이 사용되지 않습니다. Linux 시스템의 경우 AnyConnect 버전 3.1.05149부터 그룹 프로파일에 사용자 지정 특성 circumvent-host-filtering을 추가하고 true로 설정하여 클라이언트의 방화벽 및 필터 규칙을 평가하도록 AnyConnect를 구성할 수 있습니다.

액세스 목록을 생성할 경우,

- 액세스 제어 목록에서 IPv4와 IPv6 주소 두 개를 모두 지정할 수 있습니다.
- 표준 ACL을 사용하는 경우 한 개의 주소 또는 네트워크만 사용됩니다.
- 확장 ACL을 사용하는 경우, 소스 네트워크는 스플릿 터널링 네트워크입니다. 대상 네트워크는 무시됩니다.
- any(모두) 또는 split-include(스플릿-포함) 또는 split-exclude(스플릿-제외)로 0.0.0.0/0.0.0.0 또는 ::/0을 구성한 액세스 목록은 클라이언트로 전송되지 않습니다. 모든 트래픽을 터널을 통해 보내려면 스플릿 터널 **Policy**에 대해 **Tunnel All Networks**를 선택합니다.

- 스플릿 터널 정책이 **Exclude Network List Below**인 경우 주소 0.0.0.0/255.255.255.255 또는 ::/128은 클라이언트로만 전송됩니다. 이 구성은 클라이언트에 모든 로컬 서브넷으로 오는 트래픽을 터널링하지 않도록 알려줍니다.
- AnyConnect는 스플릿 터널링 정책에 지정된 모든 사이트 및 ASA에서 할당한 IP 주소와 동일한 서브넷에 포함되는 모든 사이트에 트래픽을 전달합니다. 예를 들어 ASA에서 할당한 IP 주소가 255.0.0.0 마스크가 있는 10.1.1.1인 경우, 엔드포인트 디바이스는 스플릿 터널링 정책에 관계 없이 10.0.0.0/8로 오는 모든 트래픽을 전달합니다. 따라서 예상 로컬 서브넷을 적절하게 참조하는 할당된 IP 주소에 대해 넷마스크를 사용하십시오.

시작하기 전에

- 적절한 ACE를 사용하여 액세스 목록을 만들어야 합니다.
- IPv4 네트워크에 대해 스플릿 터널 정책을 생성하고 IPv6 네트워크에 대해 다른 스플릿 터널 정책을 생성하는 경우, 지정한 네트워크 목록이 두 가지 프로토콜 모두에 사용됩니다. 따라서 네트워크 목록은 IPv4 및 IPv6 트래픽에 대한 ACE(Access Control Entries: 액세스 제어 항목)를 포함해야 합니다. 이러한 ACL을 생성하지 않은 경우, 일반 운영 구성 가이드를 참고하십시오.

다음 절차에서 필드 옆에 Inherit(상속) 확인란이 있는 모든 경우에 Inherit(상속) 확인란을 선택한 상태로 두면 구성하는 그룹 정책에서 해당 필드에 기본 그룹 정책과 같은 값을 사용한다는 뜻입니다. Inherit(상속) 확인란의 선택을 취소하면 해당 그룹 정책에 새 값을 지정할 수 있습니다.

프로시저

단계 **1** ASDM을 사용하여 ASA에 연결하고 **Configuration(**구성**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**)** > **Group Policies(**그룹 정책**)**로 이동합니다.

단계 **2** **Add(**추가**)**를 클릭하여 새 그룹 정책을 추가하거나 기존 그룹 정책을 선택하고 **Edit(**수정**)**를 클릭합니다.

단계 **3** **Advanced(**고급**)** > **Split Tunneling(**스플릿 터널링**)**을 선택합니다.

단계 **4** **DNS Names(DNS** 이름**)** 필드에서, AnyConnect에서 터널을 통해 확인할 도메인 이름을 입력합니다. 이 이름은 비공개 네트워크의 호스트에 해당합니다. split-include(스플릿-포함) 터널링이 구성되면 네트워크 목록이 지정된 DNS 서버를 포함해야 합니다. 필드에 정규화된 도메인 이름 IPv4 또는 IPv6 주소를 입력할 수 있습니다.

단계 **5** 스플릿 터널링을 비활성화하려면 **Yes(**예**)**를 클릭하여 **Send All DNS Lookups Through Tunnel(**터널을 통해 모든 **DNS** 조회 전송**)**을 활성화합니다. 이 옵션을 사용하면 DNS 트래픽이 물리적 어댑터로 유출되지 않습니다. 이 옵션은 암호화되지 않은 트래픽을 허용하지 않습니다. DNS 확인이 실패하면 주소가 미확인 상태로 남아 있고 AnyConnect 클라이언트는 VPN 외부의 주소를 확인하지 않습니다.

스플릿 터널링을 활성화하려면 기본값인 **No(**아니요**)**를 선택합니다. 이렇게 설정하면 클라이언트에서는 스플릿 터널 정책에 따라 터널을 통해 DNS 쿼리를 보냅니다.

단계 **6** 스플릿 터널링을 구성하려면 **Inherit(**상속**)** 확인란의 선택을 취소하고 스플릿 터널링 정책을 선택합니다. **Inherit(**상속**)** 확인란의 선택을 취소하지 않으면 그룹 정책에서는 기본 그룹 정책인 **DfltGrpPolicy**

에 정의된 스플릿 터널링 설정을 사용합니다. 기본 그룹 정책의 기본 스플릿 터널링 정책 설정은 Tunnel All Networks(모든 네트워크 터널링)입니다.

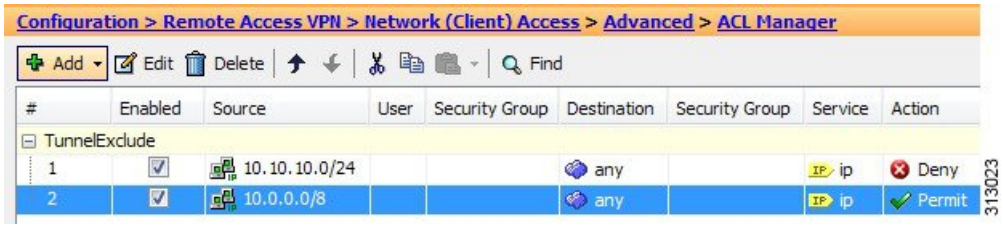
스플릿 터널링 정책을 정의하려면 드롭다운 목록에서 **Policy(**정책**)** 그리고 **IPv6 Policy(IPv6** 정책**)**를 선택합니다. Policy(정책) 필드에서는 IPv4 네트워크 트래픽에 대한 스플릿 터널링 정책을 정의합니다. IPv6 Policy(IPv6 정책) 필드에서는 IPv6 네트워크 트래픽에 대한 스플릿 터널링 정책을 선택합니다. 이러한 차이점이 있는 반면 같은 목적도 있습니다.

Inherit(상속**)** 확인란의 선택을 취소하면 다음 정책 옵션 중 하나를 선택할 수 있습니다.

- **Exclude Network List Below(**아래 네트워크 목록 제외**)** - 암호화되지 않은 트래픽을 전송할 네트워크 목록을 정의합니다. 이 기능은 터널을 통해 기업 네트워크에 연결하는 원격 사용자가 로컬 네트워크의 디바이스(예: 프린터)에 액세스하려는 경우 유용합니다.
- **Tunnel Network List Below(**아래 네트워크 목록 터널링**)** - Network List(네트워크 목록)에 지정된 네트워크와 주고받는 모든 트래픽을 터널링합니다. 포함 네트워크 목록의 주소로 보내는 트래픽은 터널링됩니다. 기타 모든 주소에 대한 데이터는 암호화되지 않고 이동하며 원격 사용자의 인터넷 서비스 공급자를 통해 라우팅됩니다.

  ASA 9.1.4 이상 버전의 경우 포함 목록을 지정할 때 포함 범위 내에 있는 서브넷에 대해 제외 목록을 지정할 수 있습니다. 제외된 서브넷은 터널링되지 않으며, 포함 목록 네트워크의 나머지는 터널링됩니다. 포함 목록의 하위 집합이 아닌 제외 목록에 있는 네트워크는 클라이언트에서 무시됩니다. Linux의 경우 제외된 서브넷을 지원하려면 그룹 정책에 사용자 지정 특성을 추가해야 합니다.

  예를 들면 다음과 같습니다.



  참고 스플릿-포함 네트워크는 로컬 서브넷(예: 192.168.1.0/24)과 정확히 일치하며, 해당 트래픽이 터널링됩니다. 스플릿-포함 네트워크가 로컬 서브넷의 부분 집합(예: 192.168.0.0/16)인 경우 로컬 서브넷 트래픽을 제외하고 해당 트래픽이 터널링됩니다. 로컬 서브넷 트래픽도 터널링하려면 일치하는 스플릿-포함 네트워크를 추가해야 합니다(192.168.1.0/24 및 192.168.0.0/16 모두 스플릿-포함 네트워크로 지정).

  스플릿-포함 네트워크가 유효하지 않은 경우(예: 0.0.0.0/0.0.0.0) 스플릿 터널링이 비활성화됩니다(모두 터널링됨).

- **Tunnel All Networks(**모든 네트워크 터널링**)** - 이 정책은 모든 트래픽을 터널링하도록 지정합니다. 이것은 사실상 스플릿 터널링을 비활성화하는 것입니다. 원격 사용자는 기업 네트워크를 통해 인터넷 네트워크에 연결하며, 로컬 네트워크에 액세스할 권한은 없습니다. 이것이 기본 옵션입니다.

단계 **7** **Network List(**네트워크 목록**)** 필드에서 스플릿-터널링 정책에 대한 액세스 제어 목록을 선택합니다. Inherit(상속)를 선택한 경우 그룹 정책에서는 기본 그룹 정책에 지정된 네트워크 목록을 사용합니다.

Manage(관리) 명령 버튼을 선택하여 ACL Manager(ACL 관리자) 대화 상자를 엽니다. 이 대화 상자에서 네트워크 목록으로 사용할 액세스 제어 목록을 구성할 수 있습니다. 네트워크 목록을 만들거나 수정하는 방법에 대한 자세한 내용은 일반적인 작업 구성 가이드를 참조해 주십시오.

확장된 ACL 목록은 IPv4 및 IPv6 주소를 모두 포함할 수 있습니다.

단계 **8** **Intercept DHCP Configuration Message from Microsoft Clients(Microsoft** 클라이언트의 **DHCP** 가로채기 구성 메시지)를 보면 DHCP Intercept 고유의 추가 매개변수를 알 수 있습니다. DHCP 가로채기를 통해 Microsoft XP 클라이언트가 ASA에서 스플릿 터널링을 사용할 수 있습니다.

- Intercept(가로채기) - DHCP 가로채기가 발생하도록 허용할 것인지 여부를 지정합니다. Inherit(상속)를 선택하지 않을 경우 기본 설정은 No(아니요)입니다.
- Subnet Mask(서브넷 마스크) - 사용할 서브넷 마스크를 선택합니다.

단계 **9** **OK(**확인**)**를 클릭합니다.

동적 스플릿 터널링 구성

동적 스플릿 터널링을 사용할 때는 호스트 DNS 도메인 이름을 기준으로 하여 터널 설정 후 스플릿 제외 터널링을 동적으로 프로비저닝할 수 있습니다. 맞춤형 속성을 생성한 다음 그룹 정책에 추가하는 방식으로 동적 스플릿 터널링을 구성합니다.

시작하기 전에

이 기능을 사용하려면 AnyConnect 릴리스 4.5 이상이 있어야 합니다. 자세한 내용을 보려면 동적 스플릿 터널링 정보를 참조하십시오.

프로시저

단계 **1** **Configuration(**구성**) > Remote Access VPN(**원격 액세스 **VPN) > Network (Client) Access(**네트워크(클라이언트) 액세스**) > Advanced(**고급**) > AnyConnect Custom Attributes(AnyConnect** 맞춤형 속성**)** 화면으로 이동합니다.

단계 **2** **Add(**추가**)**를 클릭하고 속성 유형으로 `dynamic-split-exclude-domains`를 입력한 후 설명을 입력합니다.

단계 **3** 이 새 속성을 적용하도록 클릭한 후에 UI 화면의 상단에 있는 **AnyConnect custom attribute names(AnyConnect** 맞춤형 속성 이름**)** 링크를 클릭합니다.

단계 **4** VPN 터널 외부의 클라이언트가 액세스해야 하는 각 클라우드/웹 서비스에 대해 해당하는 맞춤형 속성 이름을 추가합니다. 예를 들어 Google 웹 서비스와 관련된 DNS 도메인 이름 목록을 표시하려면 Google_domains를 추가합니다. 도메인을 쉼표 문자로 구분하는 CSV(쉼표로 구분된 값) 형식을 사용하여 AnyConnect Custom Attribute Names(AnyConnect 맞춤형 속성 이름) 화면의 값 부분에서 이러한 도메인을 정의합니다. AnyConnect는 구분자 문자(약 300개의 일반적인 크기의 도메인 이름)를 제외하고 첫 번째 5000자를 고려합니다. 해당 한도를 초과하는 도메인 이름은 무시됩니다.

맞춤형 속성은 421자를 초과할 수 없습니다. 더 큰 값을 입력한 경우, ASDM은 421자로 제한된 여러 값으로 나누어집니다. 특정한 속성 유형 및 이름에 대한 모든 값은 클라이언트에 구성이 푸시될 때 ASA에 의해 연결됩니다.

단계 **5** **Configuration(**구성**) > Remote Access VPN(**원격 액세스 **VPN) > Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**) > Group Policies(**그룹 정책**)**로 이동하여 동적 스플릿 제외 터널링 속성을 특정 그룹 정책에 연결합니다.

단계 **6** 새 그룹 정책을 생성하거나 기존 그룹 정책을 관리하기 위해 **Edit(**수정**)**을 클릭할 수 있습니다.

다음에 수행할 작업

스플릿 포함 터널링이 구성된 경우, 동적 스플릿 제외는 DNS 응답 IP 주소 중 하나 이상이 스플릿 포함 네트워크의 일부인 경우에만 적용됩니다. 모든 DNS 응답 IP 주소 및 스플릿 포함 네트워크 간에 중복되는 부분이 없는 경우, 모든 DNS 응답 IP 주소와 일치하는 트래픽이 터널링에서 이미 제외되었으므로 동적 스플릿 제외를 적용할 필요가 없습니다.

확장된 서브넷을 지원하도록 **Linux** 구성

스플릿 터널링에 대해 **Exclude Network List Below(**아래 네트워크 목록 제외**)**가 구성된 경우 제외된 서브넷을 지원하려면 Linux를 추가로 구성해야 합니다. circumvent-host-filtering라는 사용자 지정 특성을 만들어서 true로 설정하고, 스플릿 터널링에 대해 구성된 그룹 정책에 연결해야 합니다.

프로시저

단계 **1** ASDM에 연결하고 **Configuration(**구성**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**)** > **Advanced(**고급**)** > **AnyConnect Custom Attributes(AnyConnect** 맞춤형 속성**)**로 이동합니다**.**

단계 **2** **Add(**추가**)**를 클릭하고, **circumvent-host-filtering**이라는 사용자 지정 특성을 만들고, 값을 **true**로 설정합니다.

단계 **3** 클라이언트 방화벽에 사용할 그룹 정책을 수정하고 **Advanced(**고급**)** > **AnyConnect Client(AnyConnect** 클라이언트**)** > **Custom Attributes(**맞춤형 속성**)**로 이동합니다.

단계 **4** 만든 사용자 지정 특성 **circumvent-host-filtering**을 스플릿 터널링에 사용할 그룹 정책에 추가합니다.

내부 그룹 정책**, AnyConnect** 클라이언트 특성

Configuration(구성**) > Remote Access VPN(**원격 액세스 **VPN) > Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**) > Group Policies(**그룹 정책**) > Add/Edit(**추가/수정**) > Advanced(**고급**) > AnyConnect Client(AnyConnect** 클라이언트**)**로 이동하면 이 그룹 정책에서 AnyConnect 클라이언트에 대해 구성할 수 있는 특성이 있습니다.

- Keep Installer on Client System(클라이언트 시스템에서 설치 프로그램 유지) - 원격 컴퓨터에 영구 클라이언트를 설치할 수 있습니다. 이렇게 구성하면 클라이언트 자동 제거 기능이 비활성화

됩니다. 원격 사용자의 연결 시간을 줄일 수 있도록 후속 연결을 위해 원격 컴퓨터에 클라이언트가 설치된 상태로 있습니다.

참고 AnyConnect 클라이언트 2.5 이후 버전에서는 Keep Installer on Client System(클라이언트 시스템에서 설치 프로그램 유지)이 지원되지 않습니다.

- DTLS(Datagram Transport Layer Security) - 일부 SSL 연결과 관련된 레이턴시 및 대역폭 문제를 방지하고 패킷 지연에 민감한 실시간 애플리케이션의 성능을 향상시킵니다.
- DTLS Compression(DTLS 압축) - DTLS에 대해 압축을 구성합니다.
- SSL Compression(SSL 압축) - SSL/TLS에 대해 압축을 구성합니다.
- Ignore Don't Defrag (DF) Bit(조각 모음 안 함(DF) 비트 무시) - 이 기능은 DF 비트가 설정된 패킷의 강제 조각화를 허용하여 터널을 통과할 수 있게 해줍니다. 예를 들면, 네트워크에서 TCP MSS 협상에 제대로 응답하지 않는 서버에 사용할 수 있습니다.
- Client Bypass Protocol(클라이언트 우회 프로토콜) - Client Protocol Bypass(클라이언트 프로토콜 우회)는 IPv6 트래픽만 예상될 때 ASA에서 IPv4 트래픽을 관리하는 방식 또는 IPv4 트래픽만 예상될 때 ASA에서 IPv6 트래픽을 관리하는 방식을 구성합니다.

  AnyConnect 클라이언트가 ASA와의 VPN 연결을 수행할 때 ASA는 IPv4, IPv6 주소를 또는 IPv4 및 IPv6 주소 모두 지정할 수 있습니다. Client Bypass Protocol(클라이언트 우회 프로토콜)은 ASA에서 IP 주소를 할당하지 않은 트래픽을 끊을 것인지 아니면 해당 트래픽이 ASA를 우회하여 클라이언트에서 암호화되지 않은 "일반 텍스트" 상태로 전송되도록 허용할 것인지를 결정합니다.

  예를 들어, ASA에서 AnyConnect 연결에 IPv4 주소만 지정하고 엔드포인트가 이중 스택이라고 가정합니다. 엔드포인트가 IPv6 주소에 연결하려고 시도할 때 클라이언트 우회 프로토콜이 비활성화된 경우 IPv6 트래픽이 끊기지만 클라이언트 우회 프로토콜이 활성화된 경우, IPv6 트래픽은 클라이언트에서 암호화되지 않은 상태로 전송됩니다.

- FQDN of This Device(이 디바이스의 FQDN) - 네트워크 로밍 이후에 VPN 세션 재설정에 사용되는 ASA IP 주소를 확인하기 위해 클라이언트에서 이 정보를 사용합니다. 이 설정은 IP 프로토콜이 서로 다른 네트워크 간(예: IPv4에서 IPv6로)에 로밍을 지원하는 핵심 설정입니다.

  참고 AnyConnect 프로파일에 있는 ASA FQDN을 사용하여 로밍 후에 ASA IP 주소를 얻을 수 없습니다. 주소가 부하 균형 시나리오에 있는 올바른 디바이스(터널이 설정된 디바이스)와 일치하지 않을 수 있습니다.

  FQDN 디바이스가 클라이언트에 푸시되지 않은 경우, 클라이언트는 터널에서 이전에 설정한 모든 IP 주소에 재연결하려고 시도합니다. 서로 다른 IP 프로토콜로 구성된 네트워크 사이의 로밍(예: IPv4에서 IPv6로)을 지원하려면 터널 재설정에 사용할 ASA 주소를 확인할 수 있도록 로밍 후에 AnyConnect에서 디바이스 FQDN의 이름 확인 작업을 수행해야 합니다. 클라이언트는 초기 연결 동안 프로파일에 있는 ASA FQDN을 사용합니다. 후속 세션 재연결 동안 사용 가능한 경우 ASA에서 푸시하고 그룹 정책에서 관리자가 구성한 디바이스 FQDN을 항상 사용합니다. FQDN

이 구성되지 않은 경우, ASA는 Device Setup(디바이스 설정) > Device Name/Password and Domain Name(디바이스 이름/비밀번호 및 도메인 이름) 아래 설정에서 디바이스 FQDN을 파생시키고 이를 클라이언트에 전송합니다.

디바이스 FQDN이 ASA에서 푸시되지 않은 경우, 클라이언트는 여러 IP 프로토콜의 네트워크 간 로밍 후에 VPN 세션을 재설정할 수 없습니다.

- MTU - SSL 연결의 MTU 크기를 조정합니다. 256~1410바이트 사이의 값을 입력합니다. 기본적으로 MTU 크기는 연결 시 사용하는 인터페이스의 MTU에 기초하여 IP/UDP/DTLS 오버헤드를 뺀 값으로 자동으로 조정됩니다.
- Keepalive Messages(킵얼라이브 메시지) - 디바이스에서 연결에 허용되는 유휴 시간을 제한하더라도 프록시, 방화벽 또는 NAT 디바이스를 통한 연결이 계속 열려 있도록 Interval(간격) 필드에 15~600 사이의 숫자(초)를 입력하여 킵얼라이브 메시지를 활성화하고 간격을 조정합니다. 또한 이 간격을 조정함으로써 원격 사용자가 소켓 기반 애플리케이션(예: Microsoft Outlook, Microsoft Internet Explorer)을 능동적으로 실행하고 있지 않을 때 클라이언트의 연결이 끊겼다가 다시 연결되는 현상을 방지할 수 있습니다.
- Optional Client Modules to Download(다운로드할 선택적 클라이언트 모듈) - 다운로드 시간을 최소화하기 위해 AnyConnect 클라이언트는 지원하는 각 기능에 꼭 필요한 모듈의 다운로드만 ASA에서 요청합니다. 다른 기능을 활성화하는 모듈의 이름을 지정해야 합니다. AnyConnect 클라이언트 4.0 버전에는 다음 모듈이 포함되어 있습니다(이전 버전은 모듈 수가 더 적음).
  - AnyConnect DART - DART(Diagnostic AnyConnect Reporting Tool)는 시스템 로그 및 기타 진단 정보를 캡처하여 데스크톱에 .zip 파일을 만듭니다. 따라서 편리하게 Cisco TAC로 문제 해결 정보를 보낼 수 있습니다.
  - AnyConnect Network Access Manager - 이전에 Cisco Secure Services Client로 불리던 이 모듈은 802.1X(계층 2)와 유선 및 무선 네트워크에 액세스하기 위한 디바이스 인증을 제공합니다.
  - AnyConnect SBL - SBL(Start Before Logon:로그온 전 시작 사용)은 Windows 로그인 대화 상자가 나타나기 전에 AnyConnect를 시작하여 Windows에 로그온하기 전에 VPN 연결을 통하여 사용자를 엔터프라이즈 인프라에 연결시킵니다.
  - AnyConnect Web Security Module - 이전에 ScanSafe Hostscan으로 불리던 이 모듈은 AnyConnect로 통합되었습니다. 이 모듈은 각 요소를 동시에 분석하기 위해 웹 페이지의 요소를 해체합니다. 그런 다음 정의된 보안 정책에 따라 적합한 콘텐츠를 허용하고 악의적이거나 적합하지 않은 콘텐츠는 차단할 수 있습니다.
  - AnyConnect Telemetry Module - 악성 콘텐츠 출처에 대한 정보를 Cisco IronPort WSA(Web Security Appliance)의 웹 필터링 인프라로 보냅니다. WSA에서는 이 데이터를 사용하여 향상된 URL 필터링 규칙을 제공합니다.

참고 AnyConnect 4.0에서는 Telemetry가 지원되지 않습니다.

- ASA Posture Module - 이전에 Cisco Secure Desktop HostScan 기능이라고 한 상태 모듈은 AnyConnect로 통합되었으며, ASA에 대한 원격 액세스 연결을 만들기 전에 상태 평가에 필요한 크리덴셜을 수집하는 기능을 AnyConnect에 제공합니다.
- ISE Posture — OPSWAT v3 라이브러리를 사용하여 엔드포인트의 컴플라이언스를 평가하기 위한 상태 확인을 수행합니다. 그런 다음 엔드포인트가 규정을 준수할 때까지 네트워크 액세스를 제한하거나 로컬 사용자 권한을 상승시킬 수 있습니다.
- AMP Enabler — 엔드포인트용 AMP(Advanced Malware Protection)를 구축하기 위한 매체로 사용됩니다. AMP Enabler는 엔터프라이즈 내의 로컬로 호스팅되는 서버에서 엔드포인트 하위 집합으로 엔드포인트용 AMP 소프트웨어를 푸시하고 기존 사용자 기반에 대해 AMP 서비스를 설치합니다.
- 네트워크 가시성 모듈 — 용량 및 서비스 계획, 감사, 컴플라이언스 및 보안 분석을 수행하기 위한 엔터프라이즈 관리자의 역량을 개선합니다. NVM은 엔드포인트 텔레메트리를 수집하고 syslog에서 플로우 데이터와 파일 평판을 로그하고 파일 분석을 수행하고 UI 인터페이스를 제공하는 컬렉터(서드파티 벤더)로 플로우 레코드를 내보냅니다.
- Umbrella 로밍 보안 모듈 — 활성 VPN이 없을 때 DNS 레이어 보안을 제공합니다. 이 모듈은 Cisco Umbrella 로밍 서비스 또는 OpenDNS Umbrella 서비스에 서브스크립션을 제공하고 지능형 프록시 및 IP 레이어 시행 기능을 추가로 제공합니다. Umbrella 보안 로밍 프로필은 각 구축을 해당하는 서비스와 연결하며 해당하는 보호 레벨(콘텐츠 필터링, 여러 정책, 강력한 보고, Active Directory 통합 또는 기본 DNS 레이어 보안)을 자동으로 활성화합니다.

- Always-On VPN - AnyConnect 서비스 프로파일의 Always-On VPN 플래그 설정이 비활성화되었는지 또는 AnyConnect 서비스 프로파일 설정을 사용해야 하는지 확인합니다. Always-On VPN 기능은 사용자가 컴퓨터에 로그온한 후 AnyConnnect에서 자동으로 VPN 세션을 설정할 수 있게 해줍니다. VPN 세션은 사용자가 컴퓨터에서 로그오프할 때까지 유지됩니다. 물리적 연결이 해제될 경우 세션이 유지되고, AnyConnect는 ASA를 통해 물리적 연결을 다시 설정하여 VPN 세션을 재개하려고 계속 시도합니다.

  Always-On VPN은 기업 정책을 시행하여 보안 위협으로부터 디바이스를 보호하는 것을 허용합니다. 이 기능을 사용하면 엔드포인트가 신뢰할 수 있는 네트워크에 있지 않을 때마다 AnyConnect에서 VPN 세션을 설정하게 할 수 있습니다. 활성화하면 연결이 없을 때 네트워크 연결을 어떻게 관리할 것인지를 결정하는 정책이 구성됩니다.

  참고 Always-On VPN을 사용하려면 AnyConnect Secure Mobility 기능을 지원하는 AnyConnect 버전이 필요합니다.

- Client Profiles to Download(다운로드할 클라이언트 프로필) - 프로필은 AnyConnect 클라이언트에서 VPN, 네트워크 액세스 관리자, 웹 보안, ISE Posture, AMP Enabler, 네트워크 가시성 모듈 및 Umbrella 로밍 보안 모듈 설정을 구성하는 데 사용하는 구성 파라미터 그룹입니다. **Add(**추가**)**를 클릭하여 Select AnyConnect Client Profiles(AnyConnect 클라이언트 프로파일 선택) 창을 실행하고 이 그룹 정책에 대해 이전에 만든 프로파일을 지정할 수 있습니다.

내부 그룹 정책, AnyConnect 로그인 설정

Internal Group Policy(내부 그룹 정책)의 **Advanced > AnyConnect Client > Login Setting** 창에서, 원격 사용자에게 AnyConnect 클라이언트를 다운로드하라는 프롬프트를 표시하거나 클라이언트리스 SSL VPN 포털 페이지로 이동되도록 ASA를 설정할 수 있습니다.

- Post Login Setting(사후 로그인 설정) - 사용자에게 프롬프트를 표시하고 기본 사후 로그인 선택을 수행할 시간 제한을 설정하려면 선택합니다.
- Default Post Login Selection(기본 사후 로그인 선택) - 로그인 후 수행할 작업을 선택합니다.

클라이언트 방화벽을 사용하여 VPN에 대해 로컬 디바이스 지원 활성화

Internal Group Policy(내부 그룹 정책)의 **Advanced(고급) > AnyConnect Client(AnyConnect 클라이언트) > Client Firewall(클라이언트 방화벽)** 창에서, 네트워크 클라이언트 시스템의 방화벽으로 보낼 규칙을 구성할 수 있으며 이는 클라이언트가 공개 및 비공개 네트워크를 처리하는 방식에 영향을 미칩니다.

원격 사용자가 ASA에 연결하면 모든 트래픽이 VPN 연결을 통해 터널링되므로 사용자가 로컬 네트워크의 리소스에 액세스할 수 없습니다. 로컬 컴퓨터와 동기화되는 프린터, 카메라, Windows Mobile 디바이스(테더링된 디바이스)가 이에 포함됩니다. 클라이언트 프로파일에서 로컬 LAN 액세스를 활성화하면 이 문제가 해결됩니다. 하지만 로컬 네트워크에 대한 액세스 제한이 사라지기 때문에 일부 엔터프라이즈의 경우 보안 또는 정책 위험이 발생할 수 있습니다. 프린터 및 테더링된 디바이스와 같이 특정 유형의 로컬 리소스에 대한 액세스를 제한하는 엔드포인트 OS 방화벽 규칙을 구축하도록 ASA를 구성할 수 있습니다.

이렇게 하려면 인쇄용 특정 포트에 대해 클라이언트 방화벽 규칙을 활성화하십시오. 클라이언트는 인바운드 규칙과 아웃바운드 규칙을 구분합니다. 인쇄 기능의 경우 클라이언트는 아웃바운드 연결에 필요한 포트를 열고 들어오는 트래픽을 모두 차단합니다.

참고 관리자로 로그인하는 사용자는 ASA에서 클라이언트에 구축한 방화벽 규칙을 수정할 권한이 있습니다. 권한이 제한된 사용자는 규칙을 수정할 수 없습니다. 연결이 종료되면 사용자에 관계없이 클라이언트에서 방화벽 규칙을 다시 적용합니다.

관리자가 클라이언트 방화벽을 구성하고 사용자가 AD(Active Directory) 서버에 인증하면 클라이언트는 여전히 ASA의 방화벽 정책을 적용합니다. 그러나 AD 그룹 정책에 정의된 규칙이 클라이언트 방화벽의 규칙보다 우선적으로 적용됩니다.

다음 섹션에서는 이 작업을 수행하는 절차에 대해 설명합니다.

- 로컬 프린터를 지원하기 위한 클라이언트 방화벽 구축, 86 페이지
- VPN에 대해 테더링된 디바이스 지원 구성, 88 페이지

방화벽 동작에 대한 사용 참고 사항

다음 참고 사항은 AnyConnect 클라이언트에서 방화벽을 사용하는 방식을 설명합니다.

- 소스 IP는 방화벽 규칙에 사용되지 않습니다. 클라이언트는 ASA에서 보낸 방화벽 규칙에서 소스 IP 정보를 무시합니다. 클라이언트는 그 규칙이 공개인지 아니면 비공개인지에 따라 소스 IP를 결정합니다. 공개 규칙은 클라이언트의 모든 인터페이스에 적용됩니다. 비공개 규칙은 가상 어댑터에 적용됩니다.
- ASA는 ACL 규칙을 위해 여러 프로토콜을 지원합니다. 그러나 AnyConnect 방화벽 기능은 TCP, UDP, ICMP, IP만 지원합니다. 클라이언트가 다른 프로토콜의 규칙을 수신할 경우 이를 잘못된 방화벽 규칙으로 간주한 다음 보안을 위해 스플릿 터널링을 비활성화하고 완전한 터널링을 사용합니다.
- ASA 9.0부터 공개 네트워크 규칙 및 비공개 네트워크 규칙에서 통합 액세스 제어 목록이 지원됩니다. 이러한 액세스 제어 목록을 사용하여 같은 규칙에 IPv4 및 IPv6 트래픽을 정의할 수 있습니다.

운영 체제에 따라 다음과 같이 다르게 동작하므로 주의하십시오.

- Windows 컴퓨터는 Windows 방화벽에서 거부 규칙이 허용 규칙에 우선합니다. ASA가 AnyConnect 클라이언트에 허용 규칙을 푸시하지만 사용자가 이미 사용자 지정 거부 규칙을 만들었다면 AnyConnect 규칙은 적용되지 않습니다.
- Windows Vista의 경우 방화벽 규칙이 생성되면 Vista에서는 포트 번호 범위를 쉼표로 구분된 문자열로 받습니다. 포트 범위는 최대 300개입니다. 예를 들어 1-300 또는 5000-5300입니다. 300개를 초과하는 범위를 지정할 경우 처음 300개 포트에만 방화벽 규칙이 적용됩니다.
- 방화벽 서비스가 시스템에서 자동으로 시작되는 것이 아니라 AnyConnect 클라이언트에서 시작해야 하는 Windows 사용자의 경우 VPN 연결 설정에 걸리는 시간이 현저하게 늘어날 수 있습니다.
- Mac 컴퓨터의 경우 AnyConnect 클라이언트는 ASA의 규칙 적용 순서와 같은 순서로 규칙을 순차적으로 적용합니다. 전역 규칙은 항상 마지막에 와야 합니다.
- 서드파티 방화벽의 경우, AnyConnect 클라이언트 방화벽과 서드파티 방화벽 모두 해당 트래픽 유형을 허용해야 트래픽이 전달됩니다. AnyConnect 클라이언트에서 허용되는 특정 트래픽 유형을 서드파티 방화벽에서 차단할 경우 클라이언트에서 트래픽을 차단합니다.

로컬 프린터를 지원하기 위한 클라이언트 방화벽 구축

ASA는 ASA 버전 8.3(1) 이상 그리고 ASDM 버전 6.3(1) 이상에서 AnyConnect 클라이언트 방화벽 기능을 지원합니다. 이 섹션에서는 로컬 프린터에 대한 액세스를 허용하도록 클라이언트 방화벽을 구성하는 방법과 VPN 연결 실패 시 방화벽을 사용하도록 클라이언트 프로파일을 구성하는 방법에 대해 설명합니다.

클라이언트 방화벽의 한계 및 제한 사항

클라이언트 방화벽을 사용하여 로컬 LAN 액세스를 제한할 경우 다음과 같은 제한 사항이 적용됩니다.

- OS의 제한으로 인해 Windows XP를 실행하는 컴퓨터의 클라이언트 방화벽 정책이 인바운드 트래픽에만 적용됩니다. 아웃바운드 규칙 및 양방향 규칙은 무시됩니다. 여기에는 'permit ip any any' 같은 방화벽 규칙이 포함됩니다.

- 호스트 스캔 및 일부 서드파티 방화벽이 방화벽에 간섭할 수 있습니다.

다음은 소스 및 대상 포트 설정의 영향을 받는 트래픽 방향을 정리한 표입니다.

Source Port(소스 포트)	**Destination Port**(목적지 포트)	영향을 받는 트래픽 방향
특정 포트 번호	특정 포트 번호	인바운드 및 아웃바운드
범위 또는 '모두'(값 0)	범위 또는 '모두'(값 0)	인바운드 및 아웃바운드
특정 포트 번호	범위 또는 '모두'(값 0)	인바운드만
범위 또는 '모두'(값 0)	특정 포트 번호	아웃바운드만

로컬 인쇄에 대한 **ACL** 규칙의 예

간편하게 클라이언트 방화벽을 구성할 수 있도록 ACL AnyConnect_Client_Local_Print에 ASDM이 제공됩니다. 그룹 정책의 Client Firewall(클라이언트 방화벽) 창에서 Public Network Rule(공개 네트워크 규칙)에 대해 ACL을 선택할 경우 해당 목록에 다음 ACE가 포함됩니다.

.

표 ***1: AnyConnect_Client_Local_Print***의 ***ACL*** 규칙

설명	권한	인터페이스	프로토콜	소스 포트	대상 주소	대상 포트
모두 거부	Deny	공개	모든	기본	모든	기본
LPD	허용	공개	TCP	기본	모든	515
IPP	허용	공개	TCP	기본	모든	631
프린터	허용	공개	TCP	기본	모든	9100
mDNS	허용	공개	UDP	기본	224.0.0.251	5353
LLMNR	허용	공개	UDP	기본	224.0.0.252	5355
NetBios	허용	공개	TCP	기본	모든	137
NetBios	허용	공개	UDP	기본	모든	137
참고 기본 포트 범위는 1~65535입니다.						

참고 로컬 인쇄를 활성화하려면 ACL 규칙 allow Any Any를 통해 정의된 클라이언트 프로파일에서 Local LAN Access(로컬 LAN 액세스) 기능을 활성화해야 합니다.

VPN에 대해 로컬 인쇄 지원 구성

엔드 유저가 로컬 프린터로 인쇄할 수 있게 설정하려면 그룹 정책에 표준 ACL을 만듭니다. ASA에서는 해당 ACL을 VPN 클라이언트로 보내고, VPN 클라이언트에서는 클라이언트의 방화벽 구성을 수정합니다.

프로시저

단계 **1** 그룹 정책에서 AnyConnect 클라이언트 방화벽을 활성화하십시오. **Configuration(**구성**) > Remote Access VPN(**원격 액세스 **VPN) > Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**) > Group Policies(**그룹 정책**)**로 이동합니다.

단계 **2** 그룹 정책을 선택하고 **Edit(**수정**)**를 클릭합니다.

단계 **3** **Advanced(**고급**) > AnyConnect Client(AnyConnect** 클라이언트**) > Client Firewall(**클라이언트 방화벽**)**을 선택합니다. Private Network Rule(비공개 네트워크 규칙)에 대해 **Manage(**관리**)**를 클릭합니다.

단계 **4** 위에서 설명한 ACE가 포함된 ACL을 만듭니다. 이 ACL을 Private Network Rule(비공개 네트워크 규칙)로 추가합니다.

단계 **5** 자동 VPN 정책 Always-On을 활성화하고 닫힌 정책을 지정한 경우 VPN 장애 발생 시 사용자가 로컬 리소스에 액세스할 수 없습니다. 프로필 편집기의 **Preferences (Cont)(**환경 설정**(**계속**))**로 이동하여 **Apply last local VPN resource rules(**마지막 로컬 **VPN** 리소스 규칙 적용**)**를 선택하여 이 시나리오의 방화벽 규칙을 적용할 수 있습니다.

VPN에 대해 테더링된 디바이스 지원 구성

테더링된 디바이스를 지원하고 기업 네트워크를 보호하려면 그룹 정책에서 표준 ACL을 만들고, 테더링된 디바이스에서 사용하는 범위 내에서 대상 주소를 지정합니다. 그런 다음 터널링된 VPN 트래픽에서 제외할 네트워크 목록으로 스플릿 터널링에 대한 ACL을 지정합니다. 또한 VPN 장애 시 마지막 VPN 로컬 리소스 규칙을 사용하도록 클라이언트 프로파일을 구성해야 합니다.

참고 AnyConnect에서 실행되는 컴퓨터와 동기화가 필요한 Windows Mobile 디바이스의 경우 ACL에서 IPv4 대상 주소를 169.254.0.0으로 지정하거나 IPv6 대상 주소 fe80::/64를 지정합니다.

프로시저

단계 **1** ASDM에서 **Group Policy(**그룹 정책**) > Advanced(**고급**) > Split Tunneling(**스플릿 터널링**)**으로 이동합니다.

단계 **2** Network List(네트워크 목록) 필드 옆에 있는 **Inherit(**상속**)**의 선택을 취소하고 Manage(관리)를 클릭합니다.

단계 **3** **Extended ACL(**확장된 **ACL)** 탭을 클릭합니다.

단계 **4** **Add(**추가**) > Add ACL(ACL** 추가**)**을 클릭합니다. 새 ACL의 이름을 지정합니다.

단계 **5** 테이블에서 새 ACL을 선택하고 **Add(**추가**)**를 클릭한 후 **Add ACE(ACE** 추가**)**를 클릭합니다.

단계 6 **Action(**작업**)**에서는 **Permit(**허용**)** 라디오 버튼을 선택합니다.

단계 7 대상 기준 영역에서 IPv4 대상 주소로 169.254.0.0 또는 IPv6 대상 주소 fe80::/64를 지정합니다.

단계 8 **Service(**서비스**)**에서는 IP를 선택합니다.

단계 9 확인을 클릭합니다.

단계 10 **OK(**확인**)**를 클릭하여 ACL을 저장합니다.

단계 11 7단계에서 지정한 IP 주소에 따라 내부 그룹 정책에 대한 Split Tunneling(스플릿 터널링) 창에서 Policy(정책) 또는 IPv6 Policy(IPv6 정책)에 대한 Inherit(상속) 확인란의 선택을 취소하고 **Exclude Network List Below(**아래 네트워크 목록 제외**)**를 선택합니다. Network List(네트워크 목록)에서는 이전에 만든 ACL을 선택합니다.

단계 12 **OK(**확인**)**를 클릭합니다.

단계 13 **Apply(**적용**)**를 클릭합니다.

내부 그룹 정책, AnyConnect 클라이언트 키 다시 생성

ASA와 클라이언트에서 키 재설정을 수행하고 암호화 키 및 초기화 벡터를 재협상하면 키 재설정 협상이 발생하고, 결과적으로 연결 보안이 강화됩니다.

Internal Group Policy(내부 그룹 정책)의 **Advanced(**고급**) > AnyConnect Client(AnyConnect** 클라이언트**) > Key Regeneration(**키 다시 생성**)** 창에서 키 재설정에 대한 매개변수를 구성합니다.

- Renegotiation Interval(재협상 간격) - 세션 시작부터 키 재설정이 발생할 때까지의 시간을 1~10080분(일주일) 사이에서 설정하려면 **Unlimited(**무제한**)** 확인란의 선택을 취소합니다.
- Renegotiation Method(재협상 방법) - 기본 그룹 정책과 다른 재협상 방법을 지정하려면 Inherit(상속) 확인란의 선택을 취소합니다. **None(**없음**)** 라디오 버튼을 선택하여 키 재설정을 비활성화하고, **SSL** 또는 **New Tunnel(**새 터널**)** 라디오 버튼을 선택하여 키 재설정 동안 새 터널을 설정합니다.

참고 rekey 방식을 **ssl** 또는 **new-tunnel**로 구성하면 rekey 과정에서 SSL 재협상이 일어나지 않고 클라이언트가 새 터널을 설정합니다. **anyconnect ssl rekey** 명령 기록은 명령 참조를 참고하십시오.

내부 그룹 정책, AnyConnect 클라이언트, 데드 피어 감지

DPD(Dead Peer Detection: 데드 피어 감지)를 통해 ASA(게이트웨이) 또는 클라이언트는 피어가 응답하지 않으며 연결이 실패했음을 신속하게 감지합니다. DPD(Dead Peer Detection: 데드 피어 감지)를 활성화하고 AnyConnect 클라이언트 또는 ASA 게이트웨이가 DPD를 수행하는 빈도를 설정하려면 다음을 수행합니다.

시작하기 전에

- 이 기능은 ASA 게이트웨이 및 AnyConnect SSL VPN 클라이언트 간의 연결에만 적용됩니다. 이 기능은 IPsec과 함께 작동하지 않습니다. DPD는 패딩을 허용하지 않는 표준 구현을 기반으로 하기 때문입니다. 클라이언트리스 SSL VPN은 지원되지 않습니다.
- DTLS를 활성화하면 DPD(Dead Peer Detection: 데드 피어 감지)도 활성화됩니다. DPD는 실패한 DTLS 연결을 활성화하여 TLS로 대체합니다. 그렇지 않으면 연결이 종료됩니다.
- ASA에서 DPD가 활성화되면 OMTU(Optimal MTU) 기능을 사용하여 클라이언트가 DTLS 패킷을 전달할 수 있는 최대 엔드포인트 MTU를 찾을 수 있습니다. 패딩된 DPD 패킷을 최대 MTU로 보내 OMTU를 구현하십시오. 헤드 엔드에서 올바른 페이로드 에코가 수신되면 해당 MTU 크기가 수락됩니다. 그렇지 않을 경우 MTU 크기가 줄어들고, 프로토콜에 허용되는 최소 MTU 크기에 도달할 때까지 프로브가 다시 전송됩니다.

프로시저

단계 **1** 원하는 그룹 정책으로 이동합니다.

- **Configuration**(구성) **> Remote Access VPN**(원격 액세스 **VPN**) **> Network (Client) Access**(네트워크(클라이언트) 액세스) **> Group Policies**(그룹 정책)으로 이동한 다음, 원하는 그룹 정책을 **Add**(추가) 또는 **Edit**(수정)한 다음 **Advanced**(고급) **> AnyConnect Client**(**AnyConnect** 클라이언트) **> Dead Peer Detection**(데드 피어 감지)을 엽니다.
- 또는, 특정 사용자 정책에 도달하려면, 이동 또는 **Configuration**(구성) **> Device Management**(디바이스 관리) **> Users/AAA**(사용자/**AAA**) **> User Accounts**(사용자 어카운트)로 이동하여, 원하는 사용자 어카운트를 추가하거나 수정한 다음, **VPN Policy**(**VPN** 정책) **> AnyConnectClient**(**AnyConnect** 클라이언트) **> Dead Peer Detection**(데드 피어 감지) 창을 엽니다.

단계 **2** 게이트웨이 측 탐지를 설정합니다.

보안 어플라이언스(게이트웨이)에서 DPD를 수행하도록 지정하려면 **Disable**(비활성화) 확인란의 선택을 취소합니다. 보안 어플라이언스가 DPD를 수행하는 간격을 30(기본값)~3600초 사이로 입력합니다. 값을 300으로 지정하는 것이 좋습니다.

단계 **3** 클라이언트 측 탐지를 설정합니다.

클라이언트에서 DPD를 수행하도록 지정하려면 **Disable**(비활성화) 확인란의 선택을 취소합니다. 그런 다음 클라이언트가 DPD를 수행하는 간격을 30(기본값)~3600초 사이로 입력합니다. 값을 300으로 지정하는 것이 좋습니다.

내부 그룹 정책, 클라이언트리스 포털의 AnyConnect 사용자 지정

Internal Group Policy(내부 그룹 정책)의 **Advanced(**고급**) > AnyConnect Client(AnyConnect** 클라이언트**) > Customization(**사용자 지정**)** 창에서 그룹 정책에 대한 클라이언트리스 포털 로그온 페이지를 사용자 지정할 수 있습니다.

- Portal Customization(포털 사용자 지정) - AnyConnect 클라이언트/SSL VPN 포털 페이지에 적용할 사용자 지정을 선택합니다. 사전 구성된 포털 사용자 지정 개체를 선택하거나 기본 그룹 정책에 제공된 사용자 지정을 수락할 수 있습니다. 기본값은 DfltCustomization입니다.
  - Manage(관리) - 사용자 지정 개체를 추가, 수정, 삭제하고 가져오거나 내보낼 수 있는 Configure GUI Customization objects(GUI 사용자 지정 개체 구성) 대화 상자가 열립니다.
- Homepage URL(홈 페이지 URL)(선택 사항) - 그룹 정책과 완결된 사용자에 대해 클라이언트리스 포털에 표시할 홈 페이지 URL을 지정합니다. 문자열은 http:// 또는 https://로 시작해야 합니다. 클라이언트리스 사용자는 인증에 성공하면 즉시 이 페이지로 연결됩니다. AnyConnect는 VPN 연결이 성공적으로 설정되면 이 URL로 기본 웹 브라우저를 시작합니다.

  참고 AnyConnect는 현재 Linux 플랫폼, Android 모바일 디바이스, Apple iOS 모바일 디바이스에서 이 필드를 지원하지 않습니다. 설정하더라도 AnyConnect 클라이언트에서 무시합니다.
- Use Smart Tunnel for Homepage(홈 페이지에 스마트 터널 사용) - 포트 전달을 사용하는 대신 스마트 터널을 만들어 포털에 연결합니다.
- Access Deny Message(액세스 거부 메시지) - 액세스가 거부된 사용자에게 표시할 메시지를 작성하려면 이 필드에 메시지를 입력합니다.

내부 그룹 정책의 AnyConnect 클라이언트 사용자 지정 특성 구성

Internal Group Policy(내부 그룹 정책)의 **Advanced(**고급**) > AnyConnect Client(AnyConnect** 클라이언트**) > Custom Attributes(**사용자 지정 특성**)** 창에는 현재 이 정책에 할당된 사용자 지정 특성이 나열됩니다. 이 대화 상자에서는 이전에 정의된 사용자 지정 특성을 이 정책에 연계하거나, 사용자 지정 특성을 정의한 다음 이를 이 정책과 연계할 수 있습니다.

사용자 지정 특성은 AnyConnect 클라이언트로 전송되어 Deferred Upgrade(지연된 업그레이드)와 같은 기능을 구성하는 데 사용됩니다. 사용자 지정 특성에는 유형 및 명명된 값이 있습니다. 먼저 특성의 유형을 정의한 다음 이 유형의 명명된 값을 하나 이상 정의할 수 있습니다. 기능에 대해 구성할 특정 사용자 지정 특성에 대한 자세한 내용은 사용 중인 AnyConnect 릴리스에 대한 *Cisco AnyConnect Secure Mobility Client* 관리자 설명서를 참조해 주십시오.

사용자 지정 특성은 **Configuration(**구성**) > Remote Access VPN(**원격 액세스 **VPN) > Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**) > Advanced(**고급**) > AnyConnect Custom Attributes(AnyConnect** 사용자 지정 특성**)** 및 **AnyConnect Custom Attribute Names(AnyConnect** 사용자 지정 특성 이름**)**에서도 사전 정의할 수 있습니다. 사전 정의된 사용자 지정 특성은 동적 액세스 정책과 그룹 정책 모두에서 사용됩니다.

사용자 지정 특성을 추가 또는 수정하려면 이 절차를 사용합니다. 구성된 사용자 지정 특성을 삭제할 수도 있으나, 사용자 지정 특성이 또 다른 그룹 정책에도 연결되어 있으면 수정 또는 삭제할 수 없습니다.

프로시저

단계 **1** **Configuration**(구성) > **Remote Access VPN**(원격 액세스 **VPN**) > **Network (Client) Access**(네트워크(클라이언트) 액세스) > **Group Policies**(그룹 정책) > **Add/Edit**(추가/수정) > **Advanced**(고급) > **AnyConnect Client**(**AnyConnect** 클라이언트) > **Custom Attributes**(맞춤형 속성)로 이동합니다.

단계 **2** **Add**(추가)를 클릭하여 **Create Custom Attribute**(사용자 지정 특성 만들기) 창을 엽니다.

단계 **3** 드롭다운 목록에서 사전 정의된 **Attribute type**(특성 유형)을 선택하거나 다음을 수행하여 특성 유형을 구성합니다.

a) **Manage**(관리)를 클릭하고 **Configure Custom Attribute Types**(맞춤형 속성 유형 구성) 창에서 **Add**(추가)를 클릭합니다.

b) **Create Custom Attribute Type**(사용자 지정 특성 만들기) 창에서 새로운 특성 **Type**(유형) 및 **Description**(설명)을 입력합니다. 두 필드 모두 필수입니다.

c) **OK**(확인)를 클릭하여 이 창을 닫은 후 **OK**(확인)를 다시 클릭하여 새로 정의된 사용자 지정 특성 유형을 선택합니다.

단계 **4** **Select Value**(값 선택)를 선택합니다.

단계 **5** **Select value**(값 선택) 드롭다운 목록에서 사전 정의된 명명된 값을 선택하거나 다음을 수행하여 새 명명된 값을 구성합니다.

a) **Manage**(관리)를 클릭하고 Configure Custom Attributes(사용자 지정 특성 구성) 창에서 **Add**(추가)를 클릭합니다.

b) **Create Custom Attribute Name**(사용자 지정 특성 이름 만들기) 창에서 이전에 선택 또는 구성한 특성 **Type**(유형)을 선택하거나 새로운 필드 **Name**(이름) 및 **Value**(값)를 입력합니다. 두 필드 모두 필수입니다.

값을 추가하려면 **Add**(추가)를 클릭하고, 값을 입력하고, **OK**(확인)를 클릭합니다. 값은 420자를 초과할 수 없습니다. 값이 이 길이를 초과할 경우 추가 값 콘텐츠에 대한 여러 값을 추가하십시오. 구성된 값은 연결된 후 AnyConnect 클라이언트로 전송됩니다.

c) **OK**(확인)를 클릭하여 이 창을 닫은 후 **OK**(확인)를 다시 클릭하여 이 특성의 새로 정의된 명명된 값을 선택합니다.

단계 **6** **Create Custom Attribute**(사용자 지정 특성 만들기) 창에서 **OK**(확인)를 클릭합니다.

IPsec(IKEv1) 클라이언트 내부 그룹 정책

내부 그룹 정책, IPsec(IKEv1) 클라이언트에 대한 일반 특성

Configuration(구성) > **Remote Access**(원격 액세스) > **Network (Client) Access**(네트워크(클라이언트) 액세스) > **Group Policies**(그룹 정책) > **Advanced**(고급) > **IPsec (IKEv1) Client**(**IPsec (IKEv1)** 클라이

언트) Add or Edit Group Policy(그룹 정책 추가 또는 수정) > IPsec 대화 상자를 사용하면 추가하거나 수정할 그룹 정책에 대해 터널링 프로토콜, 필터, 연결 설정, 서버를 지정할 수 있습니다.

- Re-Authentication on IKE Re-key(IKE 키 재설정 시 다시 인증) - Inherit(상속) 확인란을 선택하지 않은 경우 IKE 키 재설정 발생 시 다시 인증을 활성화 또는 비활성화합니다. 자격 증명을 입력할 시간으로 30초가 제공되며, 약 2분이 되어 SA가 만료되고 터널이 종료되기까지 최대 세 번 재시도할 수 있습니다.
- Allow entry of authentication credentials until SA expires(SA가 만료될 때까지 인증 자격 증명 입력 허용) - 구성된 SA의 최대 수명이 다할 때까지 사용자가 인증 자격 증명을 다시 입력할 수 있도록 허용합니다.
- IP Compression(IP 압축) - Inherit(상속) 확인란을 선택하지 않은 경우 IP 압축을 활성화 또는 비활성화합니다.
- Perfect Forward Secrecy - Inherit(상속) 확인란을 선택하지 않은 경우 PFS(Perfect Forwarding Secrecy)를 활성화 또는 비활성화합니다. PFS는 특정 IPsec SA의 키가 다른 비밀 키에서 파생되지 않도록 합니다. 즉, 누군가가 키를 파괴한 경우 PFS는 공격자가 다른 키를 파생할 수 없게 합니다. PFS가 활성화되지 않으면 누군가가 IKE SA 비밀 키를 가상으로 파괴하고, IPsec으로 보호되는 모든 데이터를 복사한 후 IKE SA 비밀 키 정보를 사용하여 이 IKE SA로 IPsec SA 설정을 손상시킬 수 있습니다. PFS를 사용하면 IKE를 파괴해도 공격자가 IPsec에 즉시 액세스할 수 없습니다. 공격자는 각 IPsec SA를 개별적으로 파괴해야 합니다.
- Store Password on Client System(클라이언트 시스템에 비밀번호 저장) - 클라이언트 시스템에 비밀번호를 저장하도록 활성화하거나 비활성화합니다.

  참고 클라이언트 시스템에 비밀번호를 저장하면 잠재적 보안 위험이 증가할 수 있습니다.

- IPsec over UDP - IPsec over UDP 사용을 활성화 또는 비활성화합니다.
- IPsec over UDP Port(IPsec over UDP 포트) - IPsec over UDP에 사용할 UDP 포트를 지정합니다.
- Tunnel Group Lock(터널 그룹 잠금) - Inherit(상속) 확인란 또는 값 None(없음)을 선택하지 않은 경우 선택한 터널 그룹을 잠급니다.
- IPsec Backup Servers(IPsec 백업 서버) - Server Configuration(서버 구성) 및 Server IP Addresses(서버 IP 주소) 필드를 활성화합니다. 활성화하면 이러한 값이 상속되지 않을 경우에 사용할 UDP 백업 서버를 지정할 수 있습니다.
  - Server Configuration(서버 구성) - IPsec 백업 서버로 사용할 서버 구성 옵션을 나열합니다. 사용 가능한 옵션은 기본값인 Keep Client Configuration(클라이언트 구성 유지), Use the Backup Servers Below(아래의 백업 서버 사용) 및 Clear Client Configuration(클라이언트 구성 지우기)입니다.
  - Server Addresses (space delimited)(서버 주소(공백으로 구분)) - IPsec 백업 서버의 IP 주소를 지정합니다. 이 필드는 Server Configuration(서버 구성)의 값으로 Use the Backup Servers Below(아래의 백업 서버 사용)를 선택하는 경우에만 사용할 수 있습니다.

내부 그룹 정책의 IPsec(IKEv1) 클라이언트에 대한 액세스 규칙 정보

이 대화 상자의 Client Access Rules(클라이언트 액세스 규칙) 테이블에서 최대 25개의 클라이언트 액세스 규칙을 볼 수 있습니다. 클라이언트 액세스 규칙을 추가할 때 다음 필드를 구성하십시오.

- Priority(우선순위) - 이 규칙의 우선순위를 선택합니다.
- Action(작업) - 이 규칙을 기반으로 액세스를 허용 또는 거부합니다.
- VPN Client Type(VPN 클라이언트 유형) - 이 규칙이 적용되는 VPN 클라이언트 유형, 소프트웨어 또는 하드웨어, 그리고 소프트웨어 클라이언트의 경우 모든 Windows 클라이언트 또는 자유 형식 텍스트의 하위 집합을 지정합니다.
- VPN Client Version(VPN 클라이언트 버전) - 이 규칙이 적용되는 VPN 클라이언트 버전을 지정합니다. 이 열에는 이 클라이언트에 적합한 쉼표로 구분된 소프트웨어 또는 펌웨어 이미지 목록이 포함되어 있습니다. 항목은 자유 형식 텍스트이며 *는 모든 버전과 일치합니다.

클라이언트 액세스 규칙 정의

- 어떤 규칙도 정의하지 않은 경우, ASA는 모든 연결 유형을 허용합니다. 하지만 사용자는 여전히 기본 그룹 정책에 있는 모든 규칙을 상속합니다.
- 클라이언트가 어떤 규칙과도 일치하지 않는 경우, ASA는 연결을 거부합니다. 거부 규칙을 정의하는 경우, 최소한 하나의 허용 규칙을 정의해야 하며 그렇지 않은 경우, ASA는 모든 연결을 거부합니다.
- * 문자는 각 규칙에서 여러 번 입력할 수 있는 와일드카드입니다.
- 전체 규칙 집합의 문자 수는 255자로 제한됩니다.
- 클라이언트 유형 및/또는 버전을 전송하지 않는 클라이언트에 대해 **n/a**를 입력할 수 있습니다.

내부 그룹 정책, IPsec(IKEv1) 클라이언트에 대한 클라이언트 방화벽

Add or Edit Group Policy Client Firewall(그룹 정책 클라이언트 방화벽 추가 또는 수정) 대화 상자에서, 추가 또는 수정 중인 VPN 클라이언트에 대한 방화벽 설정을 구성할 수 있습니다. Microsoft Windows에서 실행 중인 VPN 클라이언트만 이러한 방화벽 기능을 사용할 수 있습니다. 이 기능은 하드웨어 클라이언트 또는 기타(Windows 이외) 소프트웨어 클라이언트에서는 현재 사용할 수 없습니다.

VPN 클라이언트를 사용하여 ASA에 연결하는 원격 사용자는 적절한 방화벽 옵션을 선택할 수 있습니다.

첫 번째 시나리오에서 원격 사용자의 PC에 개인 방화벽이 설치되어 있습니다. VPN 클라이언트는 로컬 방화벽에 정의된 방화벽 정책을 적용하고 방화벽이 실행 중인지 확인하기 위해 이를 모니터링합니다. 방화벽 실행이 중지되는 경우, VPN 클라이언트는 ASA에 대한 연결을 삭제합니다. (이 방화벽 적용 메커니즘은 VPN 클라이언트가 정기적으로 “are you there?”라는 메시지를 전송하여 방화벽을 모니터링하고 응답이 오지 않으면 방화벽이 다운된 것으로 알고 ASA에 대한 연결을 종료하므로 Are You There(AYT)라고 합니다.) 네트워크 관리자는 이러한 PC 방화벽을 초기 설정대로 구성할 수 있지만 이 접근 방식을 통해 각 사용자가 고유한 구성을 사용자 지정할 수 있습니다.

두 번째 시나리오에서는 VPN 클라이언트 PC의 개인 방화벽에 중앙 집중식 방화벽 정책을 적용하려고 합니다. 일반적인 예는 스플릿 터널링을 사용하여 그룹에 있는 원격 PC에 인터넷 트래픽을 차단하는 것입니다. 이러한 접근 방식은 터널을 설정하는 동안 인터넷을 통한 침입으로부터 PC와 중앙 사이트를 보호합니다. 이 방화벽 시나리오는 푸시 정책 또는 CPP(Central Protection Policy:중앙 보호 정책)라고 합니다. ASA에서 VPN 클라이언트에 적용할 트래픽 관리 규칙 집합을 만들어서 필터와 연결하고, 해당 필터를 방화벽 정책으로 지정합니다. ASA는 이 정책을 VPN 클라이언트에 푸시다운합니다. 그런 다음 VPN 클라이언트가 이 정책을 적용하는 로컬 방화벽에 차례대로 전달합니다.

Configuration(구성**) > Remote Access(**원격 액세스**) > Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**) > Group Policies(**그룹 정책**) > Advanced(**고급**) > IPsec (IKEv1) Client(IPsec(IKEv1)** 클라이언트**) > Client Firewall(**클라이언트 방화벽**)**

필드

- **Inherit(**상속**)** - 그룹 정책이 기본 그룹 정책에서 클라이언트 방화벽 설정을 가져오게 할 것인지 결정합니다. 이 옵션은 기본 설정입니다. 설정할 경우 이 대화 상자의 나머지 특성이 재정의되고 이름이 어둡게 표시됩니다.
- **Client Firewall Attributes(**클라이언트 방화벽 속성**)** - 방화벽이 있는 경우 어떤 방화벽 유형을 구현할 것인지, 또 해당 방화벽에 어떤 방화벽 정책을 적용할 것인지를 포함하여 클라이언트 방화벽 속성을 지정합니다.
- **Firewall Setting(**방화벽 설정**)** - 방화벽이 있는지, 만약 있다면 필수인지 아니면 선택 사항인지를 나열합니다. 기본값인 No Firewall(방화벽 없음)을 선택하면 이 대화 상자의 나머지 필드는 모두 비활성화됩니다. 이 그룹의 사용자를 방화벽으로 보호하려면 Firewall Required(방화벽 필수) 또는 Firewall Optional(방화벽 선택 사항) 설정을 선택합니다.

  Firewall Required(방화벽 필수**)**를 선택하면 이 그룹의 모든 사용자는 지정된 방화벽을 사용해야 합니다. ASA에서는 설치되어 작동 중인 지정된 지원 방화벽 없이 연결을 시도하는 모든 세션을 차단합니다. 이 경우 ASA에서는 방화벽 구성이 일치하지 않는다고 VPN 클라이언트에 알립니다.

  참고 그룹에 방화벽이 필요할 경우 그룹에 Windows VPN 클라이언트 이외의 다른 클라이언트가 포함되지 않게 하십시오. 클라이언트 모드의 ASA 5505를 비롯하여 그룹에 포함된 모든 기타 클라이언트는 연결이 불가능합니다.

  아직 방화벽 용량이 없는 원격 사용자가 이 그룹에 포함되어 있는 경우 **Firewall Optional(**방화벽 선택 사항**)**을 선택합니다. Firewall Optional(방화벽 선택 사항) 설정은 그룹의 모든 사용자가 연결할 수 있도록 허용합니다. 방화벽이 있는 사용자는 해당 방화벽을 사용할 수 있습니다. 방화벽 없이 연결하는 사용자는 경고 메시지를 받습니다. 일부 사용자는 방화벽 지원을 받고 일부 사용자는 받지 않는 그룹을 만들 때 이 설정이 매우 유용합니다. 구성원 중 일부는 방화벽 용량을 구성했고 일부는 아직 구성하지 않은 경우처럼 점진적으로 변하고 있는 그룹을 예로 들 수 있습니다.

- **Firewall Type(**방화벽 유형**)** - Cisco를 포함하여 여러 공급업체의 방화벽을 나열합니다. Custom Firewall(사용자 지정 방화벽)을 선택할 경우 Custom Firewall(사용자 지정 방화벽) 아래의 필드가

활성화됩니다. 지정하는 방화벽이 사용 가능한 방화벽 정책과 상관 관계가 있어야 합니다. 구성하는 특정 방화벽에 따라 지원되는 방화벽 정책 옵션이 결정됩니다.

- **Custom Firewall(**맞춤형 방화벽**)** - 맞춤형 방화벽의 공급업체 ID, 제품 ID, 설명을 지정합니다.
  - **Vendor ID(**공급업체 **ID)** - 이 그룹 정책의 맞춤형 방화벽 공급업체를 지정합니다.
  - **Product ID(**제품 **ID)** - 이 그룹 정책에 대해 구성된 맞춤형 방화벽의 제품 또는 모델 이름을 지정합니다.
  - **Description(**설명**)** - (선택 사항) 맞춤형 방화벽에 대해 설명합니다.
- **Firewall Policy(**방화벽 정책**)** - 맞춤형 방화벽 정책의 유형 및 소스를 지정합니다.
  - **Policy defined by remote firewall (AYT)(**원격 방화벽**(AYT)**에서 정책 정의**)** - 원격 방화벽(Are You There)에 의해 방화벽 정책이 정의되도록 지정합니다. 원격 방화벽(AYT)에서 정책을 정의한다는 것은 이 그룹의 원격 사용자가 본인 PC에 방화벽을 갖고 있다는 뜻입니다. 로컬 방화벽은 VPN 클라이언트에 방화벽 정책을 적용합니다. ASA에서는 이 그룹의 VPN 클라이언트에 지정된 방화벽이 설치되어 실행 중인 경우에만 연결을 허용합니다. 지정된 방화벽이 실행되지 않으면 연결이 실패합니다. 연결이 설정되면 VPN 클라이언트에서는 30초마다 방화벽을 폴링하여 방화벽이 실행 중인지 확인합니다. 방화벽이 중지되면 VPN 클라이언트에서는 세션을 종료합니다.
  - **Policy pushed (CPP)(**정책 푸시**(CPP))** - 정책이 피어에서 푸시되도록 지정합니다. 이 옵션을 선택하면 Inbound Traffic Policy(인바운드 트래픽 정책) 및 Outbound Traffic Policy(아웃바운드 트래픽 정책)와 Manage(관리) 버튼이 활성화됩니다. ASA에서는 Policy pushed (CPP)(정책 푸시(CPP)) 드롭다운 목록에서 선택한 필터에 의해 정의된 트래픽 관리 규칙을 이 그룹의 VPN 클라이언트에 적용합니다. 메뉴의 선택 항목은 기본 필터를 포함하여 이 ASA에 정의된 필터입니다. ASA는 이러한 규칙을 VPN 클라이언트로 푸시하므로 ASA가 아니라 VPN 클라이언트에 대해 이러한 규칙을 만들고 정의해야 합니다. 예를 들어 “in” 및 “out”은 VPN 클라이언트로 들어오는 트래픽 또는 VPN 클라이언트로 나가는 트래픽을 말합니다. VPN 클라이언트에도 로컬 방화벽이 있을 경우 ASA에서 푸시된 정책이 로컬 방화벽의 정책과 함께 작동합니다. 두 방화벽 중 하나의 규칙에 의해 차단되는 모든 패킷이 끊어집니다.
  - **Inbound Traffic Policy(**인바운드 트래픽 정책**)** - 인바운드 트래픽에 사용할 수 있는 푸시 정책을 나열합니다.
  - **Outbound Traffic Policy(**아웃바운드 트래픽 정책**)** - 아웃바운드 트래픽에 사용할 수 있는 푸시 정책을 나열합니다.
  - **Manage(**관리**)** - ACL(Access Control List)을 구성할 수 있는 ACL 관리자 대화 상자를 표시합니다.

내부 그룹 정책, IPsec(IKEv1)에 대한 하드웨어 클라이언트 특성

Configuration(구성**) > Remote Access(**원격 액세스**) > Network (Client) Access(**네트워크(클라이언트) 액세스**) > Group Policies(**그룹 정책**) > Advanced(**고급**) > IPsec (IKEv1) Client(IPsec(IKEv1)** 클라이언트**) > Hardware Client(**하드웨어 클라이언트**)** 대화 상자는 Easy VPN 원격 클라이언트에 전송할 그

룹 정책 속성을 설정합니다. ASA의 Easy VPN 지원에 대한 모든 설명은 용이한 VPN, 243 페이지 장을 참조하십시오.

참고 VPN 3002 하드웨어 클라이언트는 단종되고 지원이 중단되었습니다.

- **Inherit(상속)** - (여러 인스턴스) 해당 설정이 이후에 명시적으로 지정한 설정이 아니라 기본 그룹 정책에서 값을 가져오는 것을 나타냅니다. 이것은 이 대화 상자의 모든 속성에 대한 기본값입니다.
- **Require Interactive Client Authentication(인터랙티브 클라이언트 인증 필요)** - 인터랙티브 클라이언트 인증 필수 사용을 활성화 또는 비활성화합니다. 이 매개변수는 기본적으로 비활성화되어 있습니다.

  비활성화하면, 하드웨어 클라이언트에 저장된 크리덴셜을 사용하여 인증합니다. 저장된 크리덴셜이 없으면 하드웨어 클라이언트에서 수동으로 인증합니다. 저장하거나 입력한 크리덴셜이 유효한 경우, 터널이 설정됩니다.

  이 옵션이 활성화되면 클라이언트에 사용자 이름과 비밀 번호가 저장되어 있는지 여부에 상관없이 터널을 시작할 때마다 하드웨어 클라이언트에서 사용자 이름과 비밀 번호를 사용하여 수동으로 인증하도록 하여 추가 보안을 제공합니다. 입력한 크리덴셜이 유효한 경우, 터널이 설정됩니다.

  보안 유닛 인증에서는 하드웨어 클라이언트가 사용하는 연결 프로필에 대해 인증 서버 그룹을 구성해야 합니다. 1차 ASA에서 보안 유닛 인증이 필요한 경우, 백업 서버에서도 이를 구성했는지 확인하십시오.

  참고 이 기능을 활성화한 경우 VPN 터널을 호출하려면 사용자가 사용자 이름 및 비밀번호를 입력해야 합니다.

- **Require Individual User Authentication(개별 사용자 인증 필요)** - 개별 사용자 인증 필수 사용을 활성화 또는 비활성화합니다. 개별 사용자 인증은 하드웨어 클라이언트의 프라이빗 네트워크에서 허가받지 않은 사용자가 중앙 사이트에 액세스하지 못하게 보호합니다. 이 매개변수는 기본적으로 비활성화되어 있습니다.

  개별 사용자 인증을 활성화하면 하드웨어 클라이언트를 통해 연결하는 각 사용자는 터널이 이미 존재하더라도 웹 브라우저를 열고 유효한 사용자 이름과 비밀번호를 수동으로 입력하여 ASA를 지원하는 네트워크에 액세스해야 합니다.

  사용자는 인증하기 위해 하드웨어 클라이언트의 프라이빗 인터페이스에 대한 IP 주소를 브라우저 Location(위치) 또는 Address(주소) 필드에 입력해야 합니다. 그러면 브라우저에서 하드웨어 클라이언트에 대한 로그인 대화 상자가 표시됩니다. 인증하려면 Connect/Login Status(연결/로그인 상태)를 클릭합니다. 기본 홈 페이지가 ASA를 지원하는 원격 네트워크에 있거나, ASA를 지원하는 원격 네트워크의 웹 사이트를 브라우저로 여는 경우, 하드웨어 클라이언트에서 사용자 로그인을 위한 적절한 페이지를 브라우저에 연결합니다. 성공적으로 로그인하면 브라우저에 원래 입력했던 페이지가 표시됩니다.

사용자 인증을 활성화하면 사용자가 명령줄 인터페이스를 사용하여 로그인할 수 없습니다. 브라우저를 사용해야 합니다. 웹에 기반하지 않는 ASA를 지원하는 네트워크의 리소스(예: 이메일)에 액세스하려고 할 경우, 브라우저를 사용하여 인증할 때까지 연결에 실패합니다.

배너를 표시하려면 개별 사용자 인증을 활성화해야 합니다. 한 사용자가 동시에 최대 4개의 세션에 로그인할 수 있습니다.

1차 ASA에서 사용자 인증이 필요한 경우, 모든 백업 서버에서도 이를 구성했는지 확인하십시오.

- **User Authentication Idle Timeout(**사용자 인증 유휴 시간 제한**)** - 사용자 시간 제한 기간을 구성합니다. 보안 어플라이언스는 이 기간 동안 사용자 트래픽을 수신하지 못하는 경우 연결을 종료합니다. 시간 제한 기간은 특정 시간(분) 또는 무제한으로 지정할 수 있습니다.
  - **Unlimited(**무제한**)** - 연결 시간 제한이 없도록 지정합니다. 이 옵션은 기본 또는 지정된 그룹 정책에서 값을 상속받는 것을 방지합니다.
  - **Minutes(**분**)** - 시간 제한 기간을 분 단위로 지정합니다. 1~35791394의 정수를 사용합니다. 기본값은 Unlimited(무제한)입니다.

  show uauth 명령에 대한 응답으로 표시되는 유휴 시간 제한은 항상 Cisco Easy VPN 원격 디바이스의 터널에 인증된 사용자의 유휴 시간 제한 값입니다.

- **Cisco IP Phone Bypass(Cisco IP Phone** 우회**)** - Cisco IP Phone이 인터랙티브 개별 사용자 인증 프로세스(활성화된 경우)를 우회하도록 합니다. Cisco IP Phone Bypass(Cisco IP Phone 우회)는 기본적으로 비활성화되어 있습니다.

  하드웨어 클라이언트에서 IP 전화 연결에 네트워크 확장 모드를 사용하도록 구성해야 합니다.

- **LEAP Bypass(LEAP** 우회**)— Require Individual User Authentication(**개별 사용자 인증 필요**)**이 활성화된 경우에만 적용됩니다. Cisco 무선 디바이스의 LEAP 패킷이 개별 사용자 인증 프로세스를 우회하도록 합니다. LEAP 우회는 기본적으로 비활성화되어 있습니다.

  하드웨어 클라이언트를 지원하는 LEAP 사용자에게는 상충하는 문제가 발생합니다. 터널을 통해 중앙 사이트 디바이스를 지원하는 RADIUS 서버로 크리덴셜을 전송할 수 없으므로 LEAP 인증을 협상할 수 없습니다. 터널을 통해 크리덴셜을 전송할 수 없는 이유는 무선 네트워크에서 인증되지 않았기 때문입니다. LEAP Bypass(LEAP 우회)는 이 문제를 해결하기 위해 LEAP 패킷이(LEAP 패킷만) 터널을 통과하도록 허용하여 개별 사용자 인증에 앞서 RADIUS 서버에 대한 무선 연결을 인증하도록 합니다. 그러면 사용자가 개별 사용자 인증을 진행할 수 있습니다.

  LEAP Bypass(LEAP 우회)는 다음 조건에서 제대로 작동합니다.

  - **Require Interactive Client Authentication(**인터랙티브 클라이언트 인증 필요**)**를 비활성화해야 합니다. 인터랙티브 유닛 인증이 활성화되면 비 LEAP(유선) 디바이스에서 하드웨어 클라이언트를 인증해야 LEAP 디바이스가 해당 터널을 사용하여 연결할 수 있습니다.
  - **Require Individual User Authentication(**개별 사용자 인증 필요**)**을 활성화해야 합니다. 그렇지 않으면, LEAP Bypass(LEAP 우회)가 적용되지 않습니다.
  - 무선 환경에서 액세스 포인트는 CDP(Cisco Discovery Protocol)를 실행하는 Cisco Aironet Access Point여야 합니다. PC용 무선 NIC 카드는 다른 브랜드여도 됩니다.

- **Allow Network Extension Mode(**네트워크 확장 모드 허용**)** - 이 그룹의 하드웨어 클라이언트에서 네트워크 확장 모드를 사용하도록 결정합니다. 이 매개변수는 기본적으로 비활성화되어 있습니다. Network Extension Mode(네트워크 확장 모드)를 비활성화하면 하드웨어 클라이언트가 Port Address Translation(포트 주소 변환) 모드에서 이 ASA에 연결해야 합니다.

  Call Manager는 실제 IP 주소와만 통신할 수 있으므로 하드웨어 클라이언트에서 IP 전화 연결을 지원하려면 Network Extension Mode(네트워크 확장 모드)를 사용해야 합니다.

  참고 마찬가지로 이 그룹의 하드웨어 클라이언트를 구성해야 합니다. 하드웨어 클라이언트에서 Network Extension Mode(네트워크 확장 모드)를 사용하도록 구성했고 그에 연결되는 ASA는 아닌 경우, 하드웨어 클라이언트에서 4초마다 연결을 시도하며 시도할 때마다 거부됩니다. 이 경우, 하드웨어 클라이언트가 연결되는 ASA에 불필요한 처리 로드를 줍니다. 이 방식으로 잘못 구성된 하드웨어 클라이언트 중 대다수는 서비스를 제공하는 보안 어플라이언스의 성능이 저하됩니다.

클라이언트리스 SSL VPN 내부 그룹 정책 구성

내부 그룹 정책, 클라이언트리스 SSL VPN 일반 특성

Configuration(구성**) > Remote Access VPN(**원격 액세스 **VPN) > Clientless SSL VPN Access(**클라이언트리스 **SSL VPN** 액세스**) > Group Policies(**그룹 정책**) > Add/Edit(**추가/수정**) > General(**일반**)**

Add or Edit Group Policy(그룹 정책 추가 또는 수정) 대화 상자에서 추가하거나 수정할 그룹 정책에 대한 주소 풀, 터널링 프로토콜, 필터, 연결 설정 및 서버를 지정할 수 있습니다. 이 대화 상자의 각 필드에 대해 Inherit(상속) 확인란을 선택하면 해당 설정에 기본 그룹 정책의 값을 적용할 수 있습니다. Inherit(상속)는 이 대화 상자의 모든 특성에 대한 기본값입니다.

다음 특성은 Add Internal Group Policy(내부 그룹 정책 추가) > General(일반) 대화 상자에 표시되며

- Name(이름) - 이 그룹 정책의 이름을 지정합니다. 최대 64자까지 가능하며 공백을 사용할 수 있습니다. Edit(수정) 기능이 따로 있기 때문에 이 필드는 읽기 전용입니다.
- Banner(배너) - 로그인 시 사용자에게 표시되는 배너 텍스트를 지정합니다. 전체 배너 길이는 최대 4000자까지 가능합니다. 기본값은 없습니다.

  클라이언트리스 포털 및 AnyConnect 클라이언트는 부분 HTML을 지원합니다. 원격 사용자에게 배너를 올바르게 표시하려면 다음 지침을 따르십시오.

  - 클라이언트리스 사용자의 경우
 태그를 사용합니다.

- Tunneling Protocols(터널링 프로토콜) - 이 그룹에서 사용할 수 있는 터널링 프로토콜을 지정합니다. 사용자는 선택된 프로토콜만 사용할 수 있습니다. 선택 항목은 다음과 같습니다.
  - Clientless SSL VPN(클라이언트리스 SSL VPN) - SSL/TLS를 통해 VPN을 사용하도록 지정합니다. 이 프로토콜을 선택하면 웹 브라우저를 사용하여 ASA에 안전한 원격 액세스 터널이

설정됩니다. 소프트웨어나 하드웨어 클라이언트가 필요 없습니다. 클라이언트리스 SSL VPN을 사용하면 HTTPS 인터넷 사이트에 연결할 수 있는 거의 모든 컴퓨터에서 기업 웹사이트, 웹 지원 애플리케이션, NT/AD 파일 공유(웹 지원), 이메일 및 기타 TCP 기반 애플리케이션 등의 광범위한 엔터프라이즈 리소스에 손쉽게 액세스할 수 있습니다.

- SSL VPN Client(SSL VPN 클라이언트) - Cisco AnyConnect VPN 클라이언트 또는 기존 SSL VPN 클라이언트를 사용하도록 지정합니다. AnyConnect 클라이언트를 사용 중인 경우 MUS를 지원하려면 이 프로토콜을 선택해야 합니다.
- IPsec IKEv1 — IP 보안 프로토콜입니다. 가장 안전한 프로토콜로 간주되는 IPsec은 VPN 터널에 가장 완벽한 아키텍처를 제공합니다. 사이트 대 사이트(피어 대 피어(peer-to-peer)) 연결과 Cisco VPN client-to-LAN 연결 모두에 IPsec IKEv1을 사용할 수 있습니다.
- IPsec IKEv2 — IPsec IKEv2는 AnyConnect Secure Mobility Client에서 지원합니다. IPsec과 IKEv2를 사용하는 AnyConnect 연결은 소프트웨어 업데이트, 클라이언트 프로파일, GUI 현지화(번역) 및 사용자 지정, Cisco Secure Desktop, SCEP 프록시 등의 고급 기능을 제공합니다.
- L2TP over IPsec - 여러 공용 PC 및 모바일 PC 운영 체제와 함께 제공되는 VPN 클라이언트를 사용하는 원격 사용자가 공용 IP 네트워크를 통해 보안 어플라이언스 및 사설 기업 네트워크에 대한 보안 연결을 설정할 수 있도록 해줍니다. L2TP는 데이터를 터널링하기 위해 UDP(포트 1701)를 통한 PPP를 사용합니다. IPsec 전송 모드에 대해 보안 어플라이언스를 구성해야 합니다.

- Web ACL(웹 ACL) - (클라이언트리스 SSL VPN만 해당) 트래픽을 필터링하려면 드롭다운 목록에서 ACL(Access Control List)을 선택합니다. 선택하기 전에 ACL을 보고, 수정하고, 추가하고, 제거하려면 목록 옆에 있는 **Manage(**관리**)**를 클릭합니다.
- Access Hours(액세스 시간) - 이 사용자에게 적용되는 기존 액세스 시간 정책의 이름을 선택하거나(있는 경우) 새 액세스 시간 정책을 만듭니다. 기본값은 Inherit(상속)이며 Inherit(상속) 확인란을 선택하지 않을 경우 기본값은 Unrestricted(제한 없음)입니다. 시간 범위 개체를 보거나 추가하려면 목록 옆에 있는 **Manage(**관리**)**를 클릭합니다.
- Simultaneous Logins(동시 로그인 수) - 이 사용자에게 허용되는 최대 동시 로그인 수를 지정합니다. 기본값은 3입니다. 최소값은 0이며, 이 경우 로그인이 비활성화되고 사용자 액세스가 차단됩니다.

  참고 최대 한도는 없지만 여러 동시 연결을 허용하면 보안이 취약해지고 성능이 저하될 수 있습니다.

- Restrict Access to VLAN(VLAN에 대한 액세스 제한) - (선택 사항) "VLAN 매핑"이라고도 부르는 이 매개변수는 이 그룹 정책이 적용되는 세션의 이그레스(egress) VLAN 인터페이스를 지정합니다. ASA에서는 이 그룹의 모든 트래픽을 선택된 VLAN으로 전달합니다. 이 특성을 사용하여 그룹 정책에 VLAN을 할당하면 액세스 제어를 간소화할 수 있습니다. ACL을 사용하여 세션의 트래픽을 필터링하는 방법 대신 이 특성에 값을 할당하는 방법도 가능합니다. 기본값(Unrestricted(제한 없음)) 이외에는 이 ASA에 구성된 VLAN만 드롭다운 목록에 표시됩니다.

참고 이 기능은 HTTP 연결에 사용할 수 있지만 FTP 및 CIFS에는 사용할 수 없습니다.

- Connection Profile (Tunnel Group) Lock(연결 프로파일(터널 그룹) 잠금) - 이 매개변수는 선택된 연결 프로파일(터널 그룹)을 이용한 원격 VPN 액세스만 허용하고 다른 연결 프로파일을 이용한 액세스를 차단합니다. 기본 상속 값은 None(없음)입니다.
- **Maximum Connect Time(**최대 연결 시간**) - Inherit(**상속**)** 체크 박스를 선택하지 않은 경우 이 파라미터는 최대 사용자 연결 시간(분)을 설정합니다.

  이 시간이 경과하면 연결이 자동으로 종료됩니다. 최소값은 1분이고 최대값은 35,791,394분(4,000년 이상)입니다. 무제한 연결 시간을 허용하려면 **Unlimited(**무제한**)**(기본값)를 선택합니다.
- **Idle Timeout(**유휴 시간 제한**) - Inherit(**상속**)** 체크 박스를 선택하지 않은 경우 이 파라미터는 유휴 시간 제한(분)을 지정합니다.

  이 기간 동안 연결을 통한 통신 활동이 없는 경우 시스템은 연결을 종료합니다. 최소 시간은 1분, 최대 시간은 10080분, 기본값은 30분입니다. 무제한 연결 시간을 허용하려면 **Unlimited(**무제한**)**를 선택합니다.
- **Maximum Connection Time Alert Interval(**최대 연결 시간 알림 간격**)** - 최대 연결 시간에 도달하여 사용자에게 메시지가 표시되기 전까지의 시간 간격입니다.

  Inherit(상속**)** 확인란의 선택을 취소하면 **Default(**기본값**)** 확인란이 자동으로 선택됩니다. 이 경우 세션 알림 간격이 30분으로 설정됩니다. 새 값을 지정하려면 **Default(**기본값**)**의 선택을 취소하고 세션 알림 간격을 1분에서 30분 사이로 지정합니다.
- **Idle Timeout Alert Interval(**유휴 시간 제한 알림 간격**)** - 유휴 시간 제한에 도달하여 사용자에게 메시지가 표시되기 전까지의 시간 간격입니다.

  Inherit(상속**)** 확인란의 선택을 취소하면 **Default(**기본값**)** 확인란이 자동으로 선택됩니다. 이 경우 유휴 상태 알림 간격이 30분으로 설정됩니다. 새 값을 지정하려면 **Default(**기본값**)**의 선택을 취소하고 세션 알림 간격을 1분에서 30분 사이로 지정합니다.
- **Periodic Authentication Interval(**주기적 인증 간격**)** - 인증서 인증을 주기적으로 다시 수행하기 전까지의 시간 간격(시간)입니다.

  Inherit(상속**)** 체크 박스가 선택되지 않은 경우 주기적인 인증서 확인을 수행할 간격을 설정할 수 있습니다. 범위는 1~168시간이며 기본값은 비활성화되어 있습니다. 무제한 확인을 허용하려면 Unlimited(무제한)를 선택합니다.

내부 그룹 정책, 클라이언트리스 SSL VPN 액세스 포털

Portal(포털) 특성은 포털 페이지에서 클라이언트리스 SSL VPN 연결을 설정하는 이 그룹 정책의 구성원에게 표시할 항목을 결정합니다. 이 창에서 책갈피 목록 및 URL 입력, 파일 서버 액세스, 포트 전달 및 스마트 터널, ActiveX 릴레이, HTTP 설정을 활성화할 수 있습니다.

- Bookmark List(책갈피 목록) - 이전에 구성한 책갈피 목록을 선택하거나 **Manage(**관리**)**를 클릭하여 새 목록을 만듭니다. 책갈피는 링크로 표시되며, 사용자는 이 링크로 포털 페이지를 탐색할 수 있습니다.
- URL Entry(URL 입력) - 원격 사용자가 포털 URL 필드에 바로 URL을 입력할 수 있도록 허용하려면 활성화합니다.
- File Access Control(파일 액세스 제어) - CIFS(Common Internet File System) 파일에 대한 숨김 공유의 표시 여부를 제어합니다. 숨겨진 공유는 공유 이름의 끝에 달러 기호($)로 표시합니다. 예를 들어 드라이브 C는 C$의 형태로 공유됩니다. 숨겨진 공유에서 공유 폴더는 표시되지 않으며, 사용자는 이 숨겨진 리소스를 탐색하거나 액세스할 수 없습니다.
  - File Server Entry(파일 서버 항목) - 원격 사용자가 파일 서버 이름을 입력할 수 있도록 허용하려면 활성화합니다.
  - File Server Browsing(파일 서버 검색) - 원격 사용자가 사용 가능한 파일 서버를 검색할 수 있도록 허용하려면 활성화합니다.
  - Hidden Share Access(숨김 공유 액세스) - 공유 폴더를 숨기려면 활성화합니다.
- Port Forwarding Control(포트 전달 제어) - 사용자가 Java 애플릿을 통해 클라이언트리스 SSL VPN 연결로 TCP 기반 애플리케이션에 액세스할 수 있습니다.
  - Port Forwarding List(포트 전달 목록) - 이전에 구성한 목록 TCP 애플리케이션을 선택하여 이 그룹 정책과 연결합니다. 새 목록을 만들거나 기존 목록을 수정하려면 **Manage(**관리**)**를 클릭합니다.
  - Auto Applet Download(자동 애플릿 다운로드) - 사용자가 처음으로 로그인하면 자동으로 애플릿을 설치하여 시작합니다.
  - Applet Name(애플릿 이름) - Applet(애플릿) 대화 상자의 제목 표시줄 이름을 사용자가 지정하는 이름으로 변경합니다. 기본 이름은 Application Access입니다.
- Smart Tunnel(스마트 터널) - 클라이언트리스(브라우저 기반) SSL VPN 세션(ASA를 경로로, 보안 어플라이언스를 프록시 서버로 사용)을 사용하는 스마트 터널 옵션을 지정합니다.
  - Smart Tunnel Policy(스마트 터널 정책) - 네트워크 목록에서 선택하고 지정된 네트워크에 대해 스마트 터널 사용, 지정된 네트워크에 대해 스마트 터널 사용 안 함 또는 모든 네트워크 트래픽에 대해 터널 사용 터널 옵션 중 하나를 지정합니다. 그룹 정책 또는 사용자 이름에 스마트 터널 네트워크를 할당하면 세션이 해당 그룹 정책 또는 사용자 이름과 연결된 모든 사용자에 대해 스마트 터널 액세스가 가능하지만, 목록에 지정된 애플리케이션에 대한 스마트 터널 액세스는 제한됩니다. 스마트 터널 목록을 보고, 추가하고, 수정하고, 삭제하려면 **Manage(**관리**)**를 클릭합니다.
  - Smart Tunnel Application(스마트 터널 애플리케이션) - 드롭다운 목록에서 선택하여 최종 무선국에 설치된 TCP 기반 애플리케이션 Winsock 2를 인트라넷의 서버에 연결합니다. 스마트 터널 애플리케이션을 보고, 추가하고, 수정하고, 삭제하려면 **Manage(**관리**)**를 클릭합니다.

- Smart Tunnel all Applications(스마트 터널 모든 애플리케이션) - 모든 애플리케이션을 터널링하려면 이 확인란을 선택합니다. 네트워크 목록에서 선택하거나 엔드 유저가 외부 애플리케이션에 대해 어떤 실행 파일을 호출할지 몰라도 모든 애플리케이션이 터널링됩니다.
- Auto Start(자동 시작) - 사용자가 로그인 시 자동으로 스마트 터널 액세스를 시작하려면 이 확인란을 선택합니다. 사용자가 로그인 시 스마트 터널 액세스를 시작하는 이 옵션은 Windows에만 적용됩니다. 사용자가 로그인하는 즉시 스마트 터널 액세스를 활성화하지만 사용자가 클라이언트리스 SSL VPN 포털 페이지에서 Application Access(애플리케이션 액세스) > Start Smart Tunnels(스마트 터널 시작) 버튼을 사용하여 수동으로 스마트 터널 액세스를 시작하게 하려면 확인란의 선택을 취소합니다.
- Auto Sign-on Server List(자동 로그인 서버 목록) - 사용자가 서버에 대한 스마트 터널 연결을 구성할 때 사용자 자격 증명을 다시 발급하려면 드롭다운 목록에서 서버 이름을 선택합니다. 각 스마트 터널 자동 로그인 목록 항목은 사용자 자격 증명 제출을 자동화하는 서버를 식별합니다. 스마트 터널 자동 로그인 목록을 보고, 추가하고, 수정하거나 삭제하려면 **Manage(**관리**)**를 클릭합니다.
- Windows Domain Name(Windows 도메인 이름) - (선택 사항) 인증에 범용 명명 규칙(도메인\사용자 이름)이 필요한 경우 Windows 도메인을 지정하여 자동 로그인 동안 사용자 이름에 추가합니다. 예를 들어 사용자 이름 qu_team에 대해 인증할 때 CISCO를 입력하여 CISCO\qa_team을 지정합니다. 또한 자동 로그인 서버 목록에서 연결 항목을 구성할 때 "Use Windows domain name with user name(사용자 이름과 함께 Windows 도메인 이름 사용)" 확인란을 선택해야 합니다.

- ActiveX Relay(ActiveX 릴레이) - 클라이언트리스 사용자가 브라우저에서 Microsoft Office 애플리케이션을 실행할 수 있게 해줍니다. 이 애플리케이션은 이 세션을 사용하여 Microsoft Office 문서를 다운로드 및 업로드합니다. ActiveX Relay는 클라이언트리스 SSL VPN 세션이 종료될 때까지 그대로 실행됩니다.

추가 옵션:

- HTTP Proxy(HTTP 프록시) - HTTP 애플릿 프록시를 클라이언트로 전달하도록 활성화 또는 비활성화합니다. 프록시는 Java, ActiveX, Flash 등 적절한 콘텐츠 변환에 방해가 되는 기술에 유용합니다. 보안 어플라이언스의 지속적인 사용을 보장하면서 변조를 우회합니다. 전달된 프록시는 기존 브라우저 프록시 구성을 자동으로 수정하며, 모든 HTTP 및 HTTPS 요청을 새 프록시 구성으로 리디렉션합니다. HTML, CSS, JavaScript, VBScript, ActiveX, Java 등 모든 클라이언트 쪽 기술을 지원합니다. 유일하게 지원하는 브라우저는 Microsoft Internet Explorer입니다.
- Auto Start (HTTP Proxy)(자동 시작(HTTP 프록시)) - 사용자 로그인 시 HTTP 프록시를 자동으로 활성화하려면 선택합니다. 사용자 로그인 시 스마트 터널 액세스를 활성화하지만 사용자가 수동으로 스마트 터널 액세스를 시작하게 하려면 확인란의 선택을 취소합니다.
- HTTP Compression(HTTP 압축) - 클라이언트리스 SSL VPN 세션을 통해 HTTP 데이터를 압축할 수 있습니다.

내부 그룹 정책, 클라이언트리스 SSL VPN의 포털 사용자 지정 구성

그룹 정책에 대해 사용자 지정을 구성하려면 사전 정의된 포털 사용자 지정 개체를 선택하거나 기본 그룹 정책에 제공된 사용자 지정을 수락합니다. 또한 표시할 URL을 구성할 수 있습니다.

클라이언트리스 SSL VPN 액세스 연결에 대해 액세스 포털을 사용자 지정하는 절차는 네트워크 클라이언트 액세스 연결과 동일합니다. 내부 그룹 정책, 클라이언트리스 포털의 AnyConnect 사용자 지정, 91 페이지를 참고하십시오.

내부 그룹 정책, 클라이언트리스 SSL VPN의 로그인 설정

이 대화 상자에서 원격 사용자에게 AnyConnect 클라이언트를 다운로드하거나 클라이언트리스 SSL VPN 포털 페이지로 이동하라는 프롬프트를 표시하도록 ASA를 활성화할 수 있습니다. 내부 그룹 정책, AnyConnect 로그인 설정, 85 페이지를 참고하십시오.

내부 그룹 정책, 클라이언트리스 SSL VPN 액세스의 SSO(Single Sign On) 및 자동 로그인 서버

SSO(Single Sign On) 서버 및 자동 로그인 서버를 구성하는 방법은 내부 그룹 정책, 클라이언트리스 SSL VPN 액세스 포털, 101 페이지 섹션을 참고하십시오.

사이트 대 사이트 내부 그룹 정책

사이트 대 사이트 VPN 연결에 대한 그룹 정책은 터널링 프로토콜, 필터 및 연결 설정을 지정합니다. 이 대화 상자의 각 필드에 대해 Inherit(상속) 확인란을 선택하면 해당 설정에 기본 그룹 정책의 값을 적용할 수 있습니다. Inherit(상속)는 이 대화 상자의 모든 특성에 대한 기본값입니다.

필드

다음 특성은 Add Internal Group Policy(내부 그룹 정책 추가) > General(일반) 대화 상자에 표시되며 SSL VPN 및 IPsec 세션에 적용되거나 클라이언트리스 SSL VPN 세션에 적용됩니다. 예를 들어 일부는 한 세션 유형에 대해서는 최신 상태이지만 다른 세션 유형에 대해서는 그렇지 않은 경우가 있습니다.

- Name(이름) - 이 그룹 정책의 이름을 지정합니다. Edit(수정) 기능이 따로 있기 때문에 이 필드는 읽기 전용입니다.
- Tunneling Protocols(터널링 프로토콜) - 이 그룹에 허용되는 터널링 프로토콜을 지정합니다. 사용자는 선택된 프로토콜만 사용할 수 있습니다. 선택 항목은 다음과 같습니다.
  - Clientless SSL VPN(클라이언트리스 SSL VPN) - SSL/TLS를 통해 VPN을 사용하도록 지정합니다. 이 프로토콜을 선택하면 웹 브라우저를 사용하여 ASA에 안전한 원격 액세스 터널이 설정됩니다. 소프트웨어나 하드웨어 클라이언트가 필요 없습니다. 클라이언트리스 SSL VPN을 사용하면 HTTPS 인터넷 사이트에 연결할 수 있는 거의 모든 컴퓨터에서 기업 웹사이트, 웹 지원 애플리케이션, NT/AD 파일 공유(웹 지원), 이메일 및 기타 TCP 기반 애플리케이션 등의 광범위한 엔터프라이즈 리소스에 손쉽게 액세스할 수 있습니다.
  - SSL VPN Client(SSL VPN 클라이언트) - Cisco AnyConnect VPN 클라이언트 또는 기존 SSL VPN 클라이언트를 사용하도록 지정합니다. AnyConnect 클라이언트를 사용 중인 경우 MUS를 지원하려면 이 프로토콜을 선택해야 합니다.

- IPsec IKEv1 — IP 보안 프로토콜입니다. 가장 안전한 프로토콜로 간주되는 IPsec은 VPN 터널에 가장 완벽한 아키텍처를 제공합니다. 사이트 대 사이트(피어 대 피어(peer-to-peer)) 연결과 Cisco VPN client-to-LAN 연결 모두에 IPsec IKEv1을 사용할 수 있습니다.
- IPsec IKEv2 — IPsec IKEv2는 AnyConnect Secure Mobility Client에서 지원합니다. IPsec과 IKEv2를 사용하는 AnyConnect 연결은 소프트웨어 업데이트, 클라이언트 프로파일, GUI 현지화(번역) 및 사용자 지정, Cisco Secure Desktop, SCEP 프록시 등의 고급 기능을 제공합니다.
- L2TP over IPsec - 여러 공용 PC 및 모바일 PC 운영 체제와 함께 제공되는 VPN 클라이언트를 사용하는 원격 사용자가 공용 IP 네트워크를 통해 보안 어플라이언스 및 사설 기업 네트워크에 대한 보안 연결을 설정할 수 있도록 해줍니다. L2TP는 데이터를 터널링하기 위해 UDP(포트 1701)를 통한 PPP를 사용합니다. IPsec 전송 모드에 대해 보안 어플라이언스를 구성해야 합니다.

- Filter(필터) - (Network (Client) Access(네트워크(클라이언트) 액세스)만 해당) 어떤 액세스 제어 목록을 사용할 것인지 또는 그룹 정책의 값을 상속할지 여부를 지정합니다. 필터는 소스 주소, 대상 주소 및 프로토콜 등의 기준에 따라 ASA를 통해 수신하는 터널링된 데이터 패킷의 허용 또는 거부 여부를 결정하는 규칙으로 구성됩니다. 필터 및 규칙을 구성하려면 Group Policy(그룹 정책) 대화 상자를 참조하십시오. **Manage(**관리**)**를 클릭하여 ACL Manager(ACL 관리자)를 엽니다. 여기서 ACL을 보고 구성할 수 있습니다.
- **Idle Timeout(**유휴 시간 제한**) - Inherit(**상속**)** 체크 박스를 선택하지 않은 경우 이 파라미터는 유휴 시간 제한(분)을 지정합니다.

  이 기간 동안 연결을 통한 통신 활동이 없는 경우 시스템은 연결을 종료합니다. 최소 시간은 1분, 최대 시간은 10080분, 기본값은 30분입니다. 무제한 연결 시간을 허용하려면 **Unlimited(**무제한**)**를 선택합니다.
- **Maximum Connect Time(**최대 연결 시간**) - Inherit(**상속**)** 체크 박스를 선택하지 않은 경우 이 파라미터는 최대 사용자 연결 시간(분)을 설정합니다.

  이 시간이 경과하면 연결이 자동으로 종료됩니다. 최소값은 1분이고 최대값은 35,791,394분(4,000년 이상)입니다. 무제한 연결 시간을 허용하려면 **Unlimited(**무제한**)**(기본값)를 선택합니다.
- **Periodic Authentication Interval(**주기적 인증 간격**)** - 인증서 인증을 주기적으로 다시 수행하기 전까지의 시간 간격(시간)입니다.

  Inherit(상속**)** 체크 박스가 선택되지 않은 경우 주기적인 인증서 확인을 수행할 간격을 설정할 수 있습니다. 범위는 1~168시간이며 기본값은 비활성화되어 있습니다. 무제한 확인을 허용하려면 Unlimited(무제한)를 선택합니다.

로컬 사용자에 대해 VPN 정책 특성 구성

이 절차에서는 기존 사용자를 수정하는 방법에 대해 설명합니다. 사용자를 추가하려면 **Configuration(**구성**) > Remote Access VPN(**원격 액세스 **VPN) > AAA/Local Users(AAA/**로컬 사용자**) > Local Users(**로컬 사용자**)**를 선택하고 **Add(**추가**)**를 클릭합니다. 자세한 내용은 일반적인 작업 구성 가이드를 참조하십시오.

시작하기 전에

기본적으로 사용자 어카운트는 기본 그룹 정책인 DfltGrpPolicy에서 각 설정의 값을 상속받습니다. 각 설정을 재정의하려면 **Inherit(**상속**)** 확인란의 선택을 취소하고 새 값을 입력합니다.

프로시저

단계 **1** ASDM을 시작하고 **Configuration(**구성**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **AAA/Local Users(AAA/**로컬 사용자**)** > **Local Users(**로컬 사용자**)**를 선택합니다.

단계 **2** 구성할 사용자를 선택하고 **Edit(**수정**)**를 클릭합니다.

단계 **3** 왼쪽 창에서 **VPN Policy(VPN** 정책**)**를 클릭합니다.

단계 **4** 사용자에 대한 그룹 정책을 지정합니다. 사용자 정책이 이 그룹 정책의 특성을 상속받습니다. 이 화면의 다른 필드가 기본 그룹 정책에서 구성을 **Inherit(**상속**)**받도록 설정된 경우, 이 그룹 정책에 지정된 특성이 기본 그룹 정책의 특성보다 우선적으로 적용됩니다.

단계 **5** 사용자가 사용할 수 있는 터널링 프로토콜을 지정하거나 그룹 정책에서 값을 상속받을지 지정합니다.

원하는 **Tunneling Protocols(**터널링 프로토콜**)** 확인란을 선택하여 다음 터널링 프로토콜 중 하나를 선택합니다.

- 클라이언트리스 SSL VPN(SSL/TLS를 통한 VPN)에서는 웹 브라우저를 사용하여 VPN Concentrator에 대한 보안 원격 액세스 터널을 설정하며 소프트웨어나 하드웨어 클라이언트가 필요하지 않습니다. 클라이언트리스 SSL VPN을 사용하면 HTTPS 인터넷 사이트에 연결할 수 있는 거의 모든 컴퓨터에서 기업 웹사이트, 웹 지원 애플리케이션, NT/AD 파일 공유(웹 지원), 이메일 및 기타 TCP 기반 애플리케이션 등의 광범위한 엔터프라이즈 리소스에 손쉽게 액세스할 수 있습니다.
- SSL VPN 클라이언트는 사용자가 Cisco AnyConnect 클라이언트 애플리케이션을 다운로드한 후 연결할 수 있습니다. 사용자가 클라이언트리스 SSL VPN 연결을 사용하여 이 애플리케이션을 처음으로 다운로드합니다. 그러면 사용자가 연결할 때마다 필요한 클라이언트 업데이트가 자동으로 진행됩니다.
- IPsec IKEv1 — IP 보안 프로토콜입니다. 가장 안전한 프로토콜로 간주되는 IPsec은 VPN 터널에 가장 완벽한 아키텍처를 제공합니다. 사이트 대 사이트(피어 대 피어(peer-to-peer)) 연결과 Cisco VPN client-to-LAN 연결 모두에 IPsec IKEv1을 사용할 수 있습니다.
- IPsec IKEv2 — IPsec IKEv2는 AnyConnect Secure Mobility Client에서 지원합니다. IPsec과 IKEv2를 사용하는 AnyConnect 연결은 소프트웨어 업데이트, 클라이언트 프로파일, GUI 현지화(번역) 및 사용자 지정, Cisco Secure Desktop, SCEP 프록시 등의 고급 기능을 제공합니다.
- L2TP over IPsec은 여러 공용 PC 및 모바일 PC 운영 체제와 함께 제공되는 VPN 클라이언트를 사용하는 원격 사용자가 공용 IP 네트워크를 통해 ASA 및 프라이빗 기업 네트워크에 대한 보안 연결을 설정할 수 있도록 해줍니다.

  참고 프로토콜을 선택하지 않으면 오류 메시지가 나타납니다.

단계 **6** 사용할 필터(IPv4 또는 IPv6)를 지정하거나 그룹 정책에서 값을 상속 받을지 지정합니다.

필터는 소스 주소, 수신 주소 및 프로토콜 등의 기준에 따라 ASA를 통해 수신하는 터널링된 데이터 패킷의 허용 또는 거부 여부를 결정하는 규칙으로 구성됩니다.

a) 필터 및 규칙을 구성하려면 **Configuration(**구성**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**)** > **Group Policies(**그룹 정책**)** > **Add/Edit(**추가/수정**)** > **General(**일반**)** > **More Options(**추가 옵션**)** > **Filter(**필터**)**를 선택합니다.
b) ACL 및 ACE를 추가, 수정 및 삭제할 수 있는 ACL Manager(ACL 관리자) 창을 표시하려면 **Manage(**관리**)**를 클릭합니다.

단계 **7** 연결 프로파일(터널 그룹) 잠금을 상속받을지 또는 선택한 터널 그룹 잠금(있는 경우)을 사용할지 지정합니다.

특정 잠금을 선택하면 이 그룹을 통한 원격 액세스만 사용자에게 허용됩니다. Tunnel Group Lock(터널 그룹 잠금)은 VPN 클라이언트에 구성된 그룹이 사용자 할당 그룹과 동일한지 확인하여 사용자를 제한합니다. 동일하지 않으면 ASA에서 사용자의 연결을 차단합니다. Inherit(상속) 확인란이 선택되어 있지 않은 경우 기본값은 None(없음)입니다.

단계 **8** 그룹에서 Store Password on Client System(클라이언트 시스템에 비밀번호 저장) 설정을 상속 받을지 지정합니다.

Inherit(상속**)** 확인란의 선택을 취소하면 Yes(예) 및 No(아니요) 라디오 버튼이 활성화됩니다. 로그인 비밀번호를 클라이언트 시스템에 저장하려면 **Yes(**예**)**를 클릭합니다(잠재적으로 보안이 취약한 옵션). 사용자가 연결할 때마다 비밀번호를 입력하도록 하려면 기본값인 **No(**아니요**)**를 클릭합니다. 보안을 극대화하기 위해 비밀번호 저장을 허용하지 않는 것이 좋습니다.

단계 **9** 연결 설정을 구성합니다.

a) 이 사용자에게 적용할 액세스 시간 정책을 지정하거나, 사용자에 대한 새 액세스 시간 정책을 생성하거나, Inherit(상속) 상자를 선택된 상태로 둡니다. 기본값은 Inherit(상속)이며 Inherit(상속) 확인란을 선택하지 않을 경우 기본값은 Unrestricted(제한 없음)입니다.

   새 액세스 시간 집합을 지정할 수 있는 Add Time Range(시간 범위 추가) 대화 상자를 열려면 **Manage(**관리**)**를 클릭합니다.

b) 해당 사용자의 동시 로그인 수를 지정합니다. Simultaneous Logins(동시 로그인) 매개변수는 이 사용자에게 허용되는 최대 동시 로그인 수를 지정합니다. 기본값은 3입니다. 최소값은 0이며, 이 경우 로그인이 비활성화되고 사용자 액세스가 차단됩니다.

   참고 최대 한도는 없지만 여러 동시 연결을 허용하면 보안이 취약해지고 성능이 저하될 수 있습니다.

c) VPN 연결 시간에 대한 최대 연결 시간을 분 단위로 지정합니다. 이 시간이 경과하면 연결이 자동으로 종료됩니다.

   Inherit(상속**)** 확인란을 선택하지 않은 경우 이 파라미터는 최대 사용자 연결 시간(분)을 지정합니다. 최소값은 1분이고 최대값은 35,791,394분(4,000년 이상)입니다. 무제한 연결 시간을 허용하려면 **Unlimited(**무제한**)**(기본값)를 선택합니다.

d) VPN 연결 시간에 대한 유휴 시간 제한을 분 단위로 지정합니다. 이 기간 동안 연결을 통한 통신 활동이 없는 경우 시스템은 연결을 종료합니다.

Inherit(상속**)** 체크 박스를 선택하지 않은 경우 이 매개변수는 유휴 시간 제한을 분 단위로 지정합니다. 최소 시간은 1분, 최대 시간은 10080분이고 기본값은 30분입니다. 무제한 연결 시간을 허용하려면 **Unlimited(**무제한**)**를 선택합니다.

단계 **10** **Timeout Alerts(**시간 제한 알림**)**를 구성합니다.

a) **Maximum Connection Time Alert Interval(**최대 연결 시간 알림 간격**)**을 지정합니다.

Inherit(상속**)** 확인란의 선택을 취소하면 **Default(**기본값**)** 확인란이 자동으로 선택됩니다. 이 경우 최대 연결 알림 간격이 30분으로 설정됩니다. 새 값을 지정하려면 **Default(**기본값**)**의 선택을 취소하고 세션 알림 간격을 1분에서 30분 사이로 지정합니다.

b) **Idle Alert Interval(**유휴 상태 알림 간격**)**을 지정합니다.

Inherit(상속**)** 확인란의 선택을 취소하면 **Default(**기본값**)** 확인란이 자동으로 선택됩니다. 이 경우 유휴 상태 알림 간격이 30분으로 설정됩니다. 새 값을 지정하려면 **Default(**기본값**)**의 선택을 취소하고 세션 알림 간격을 1분에서 30분 사이로 지정합니다.

단계 **11** 이 사용자에 대한 전용 IPv4 주소를 설정하려면 **Dedicated IPv4 Address (Optional)(**전용 **IPv4** 주소**(**선택 사항**))** 영역에 IPv4 주소와 서브넷 마스크를 입력합니다.

단계 **12** 이 사용자에 대한 전용 IPv6 주소를 설정하려면 **Dedicated IPv6 Address (Optional)(**전용 **IPv6** 주소**(**선택 사항**))** 영역에 IPv6 접두사와 함께 IPv6 주소를 입력합니다. IPv6 접두사는 IPv6 주소가 상주하는 서브넷을 나타냅니다.

단계 **13** 왼쪽 창에서 이러한 옵션을 클릭하여 특정 **Clientless SSL VPN(**클라이언트리스 **SSL VPN)** 또는 **AnyConnect Client(AnyConnect** 클라이언트**)** 설정을 구성합니다. 각 설정을 재정의하려면 **Inherit(**상속**)** 확인란의 선택을 취소하고 새 값을 입력합니다.

단계 **14** **OK(**확인**)**를 클릭하여 실행 중인 구성에 변경 사항을 적용합니다.

연결 프로파일

터널 그룹이라고도 하는 연결 프로파일은 VPN 연결에 대한 연결 특성을 구성합니다. 이러한 특성은 Cisco AnyConnect VPN 클라이언트, 클라이언트리스 SSL VPN 연결, IKEv1 및 IKEv2 서드파티 VPN 클라이언트에 적용됩니다.

AnyConnect Connection Profile(AnyConnect 연결 프로파일), 기본 창

AnyConnect Connection Profile(AnyConnect 연결 프로파일)의 기본 창에서 인터페이스에 대한 클라이언트 액세스를 활성화하고 연결 프로파일을 추가, 편집, 삭제할 수 있습니다. 또한 사용자가 로그인 시 특정 연결을 선택하도록 허용할 것인지 여부를 지정할 수 있습니다.

- Access Interfaces(액세스 인터페이스) - 테이블에서 인터페이스를 선택할 수 있습니다. 이 인터페이스에서 액세스를 활성화합니다. 이 테이블의 필드에는 인터페이스 이름과 액세스 허용 여부를 지정하는 확인란이 포함되어 있습니다.

- Interface(인터페이스) 테이블에서, AnyConnect 연결을 구성하려는 인터페이스 행에서, 인터페이스에서 활성화할 프로토콜을 선택합니다. SSL 액세스, IPsec 액세스 또는 둘 모두를 허용할 수 있습니다.

  SSL을 선택하면 기본적으로 DTLS(Datagram Transport Layer Security)가 활성화됩니다. DTLS는 일부 SSL 연결에서 발생하는 레이턴시 및 대역폭 문제를 방지하고 패킷 지연에 민감한 실시간 애플리케이션의 성능을 높입니다.

  IPsec(IKEv2) 액세스를 선택하면 기본적으로 클라이언트 서비스가 활성화됩니다. 클라이언트 서비스는 소프트웨어 업데이트, 클라이언트 프로파일, GUI 현지화(변환) 및 사용자 지정, Cisco Secure Desktop, SCEP 프록시를 비롯한 향상된 Anyconnect 기능을 포함하고 있습니다. 클라이언트 서비스를 비활성화할 경우 AnyConnect 클라이언트는 계속 IKEv2와 기본 IPsec 연결을 설정합니다.

- Device Certificate(디바이스 인증서) - RSA 키 또는 ECDSA 키 인증을 위한 인증서를 지정할 수 있습니다. 디바이스 인증서 지정, 110 페이지를 참고하십시오.

- Port Setting(포트 설정) - HTTPS 및 DTLS(RA 클라이언트만 해당) 연결의 포트 번호를 구성합니다. 연결 프로파일, 포트 설정, 111 페이지를 참고하십시오.

- Bypass interface access lists for inbound VPN sessions(인바운드 VPN 세션에 대한 인터페이스 액세스 목록 우회) - Enable inbound VPN sessions to bypass interface ACLs(인바운드 VPN 세션이 인터페이스 ACL을 우회하도록 활성화)이 기본적으로 선택됩니다. 보안 어플라이언스는 인터페이스 ACL을 통해 모든 VPN 트래픽이 통과하도록 허용합니다. 예를 들어 외부 인터페이스 ACL에서 암호 해독된 트래픽이 통과하는 것을 허용하지 않을 경우 보안 어플라이언스는 원격 비공개 네트워크를 신뢰하고 암호 해독된 패킷이 통과하는 것을 허용합니다. 이 기본 동작을 변경할 수 있습니다. 인터페이스 ACL이 VPN으로 보호되는 트래픽을 검사하게 하려면 이 확인란의 선택을 취소하십시오.

- Login Page Setting(로그인 페이지 설정)
  - 로그인 페이지에서 사용자가 별칭으로 식별된 연결 프로파일을 선택할 수 있도록 허용합니다. 이 확인란을 선택하지 않을 경우 기본 연결 프로파일은 DefaultWebVPNGroup입니다.
  - Shutdown portal login page(포털 로그인 페이지 종료) - 로그인이 비활성화된 웹 페이지를 표시합니다.

- Connection Profiles(연결 프로파일) - 연결(터널 그룹)에 대한 프로토콜별 특성을 구성합니다.
  - Add/Edit(추가/수정) - 연결 프로파일(터널 그룹)을 추가 또는 수정하려면 클릭합니다.
  - Name(이름) - 연결 프로파일의 이름입니다.
  - Aliases(별칭) - 연결 프로파일을 식별하는 다른 이름입니다.
  - SSL VPN Client Protocol(SSL VPN 클라이언트 프로토콜) - SSL VPN 클라이언트의 액세스 권한 여부를 지정합니다.
  - Group Policy(그룹 정책) - 이 연결 프로파일의 기본 그룹 정책을 표시합니다.

- 로그인 페이지에서 사용자가 위의 테이블에 별칭으로 식별된 연결을 선택할 수 있도록 허용합니다. 로그인 페이지에서의 연결 프로파일(터널 그룹) 별칭 표시를 활성화하려면 선택합니다.

- 그룹 URL과 인증서 맵이 서로 다른 연결 프로파일과 일치하는 경우 그룹 URL을 우선 적용. 그렇지 않은 경우 인증서 맵과 일치하는 연결 프로파일 사용 - 이 옵션은 연결 프로파일 선택 프로세스에서 그룹 URL과 인증서 값의 상대적 선호도를 지정합니다. ASA는 선호하는 값과 일치하는 값을 찾지 못하면 다른 값과 일치하는 연결 프로파일을 선택합니다. 기존 ASA 소프트웨어 버전에서 사용되는 환경 설정을 사용하여 VPN 엔드포인트에서 지정한 그룹 URL을 동일한 그룹 URL을 지정하는 연결 프로파일과 일치시키려는 경우에만 이 옵션을 선택하십시오. 이 옵션은 기본적으로 선택되지 않습니다. 이 옵션을 선택하지 않으면 ASA에서는 연결 프로파일에 지정된 인증서 필드 값을 엔드포인트에서 연결 프로파일을 할당하는 데 사용하는 인증서 필드 값과 일치시킵니다.

디바이스 인증서 지정

Specify Device Certificate(디바이스 인증서 지정**)** 창에서는 ASA가 연결을 만들려고 할 때 클라이언트에 ASA를 식별하는 인증서를 지정할 수 있습니다. 이 화면은 AnyConnect 연결 프로파일 및 클라이언트리스 연결 프로파일에 적용됩니다. Always-on IPsec/IKEv2 같은 특정 AnyConnect 기능은 ASA에서 사용 가능한 유효하고 신뢰할 수 있는 디바이스 인증서가 필요합니다.

ASA Release 9.4.1부터는 SSL 연결(AnyConnect 클라이언트 및 클라이언트리스 SSL 모두에서)에 ECDSA 인증서를 사용할 수 있습니다. 이 릴리스 이전에는 ECDSA 인증서는 AnyConnect IPsec 연결에만 지원되고 구성되었습니다.

프로시저

단계 **1** (VPN 연결만 해당) **Certificate with RSA Key(RSA** 키를 사용하는 인증서**)** 영역에서 다음 작업 중 하나를 수행합니다.

- 한 인증서를 선택하여 두 프로토콜 중 하나를 사용하는 클라이언트를 인증하려면 **Use the same device certificate for SSL and IPsec IKEv2(SSL** 및 **IPsec IKEv2**에 같은 디바이스 인증서 사용**)** 확인란을 선택합니다. 목록 상자에 제공되는 인증서 중에 선택하거나 **Manage(**관리**)**를 클릭하여 사용할 ID 인증서를 만듭니다.
- SSL 연결 또는 IPsec 연결에 별도의 인증서를 지정하려면 **Use the same device certificate for SSL and IPsec IKEv2(SSL** 및 **IPsec IKEv2**에 같은 디바이스 인증서 사용**)** 확인란의 선택을 취소합니다.

단계 **2** **Device Certificate(**디바이스 인증서**)** 목록 상자에서 인증서를 선택합니다.

원하는 인증서가 보이지 않을 경우 **Manage(**관리**)** 버튼을 클릭하여 ASA의 ID 인증서를 관리합니다.

단계 **3** (VPN 연결만 해당) Certificate with ECDSA key(ECDSA 키를 사용하는 인증서) 필드에서 목록 상자의 ECDSA 인증서를 선택하거나 **Manage(**관리**)**를 클릭하여 ECDSA ID 인증서를 만듭니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

연결 프로파일, 포트 설정

ASDM의 Connection Profile(연결 프로파일) 창에서 SSL 및 DTLS 연결(원격 액세스만 해당)에 대한 포트 번호를 구성합니다.

Configuration(구성**) > Remote Access VPN(**원격 액세스 **VPN) > Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**) > AnyConnect Connection Profiles(AnyConnect** 연결 프로파일**)**

Configuration(구성**) > Remote Access VPN(**원격 액세스 **VPN) > Clientless SSL VPN Access(**클라이언트리스 **SSL VPN** 액세스**) > Connection Profiles(**연결 프로파일**)**

필드

- HTTPS Port(HTTPS 포트) - HTTPS(브라우저 기반) SSL 연결에 대해 활성화할 포트입니다. 범위는 1부터 65535까지입니다. 기본값은 포트 443입니다.
- DTLS Port(DTLS 포트) - DTLS 연결에 대해 활성화할 UDP 포트입니다. 범위는 1부터 65535까지입니다. 기본값은 포트 443입니다.

AnyConnect Connection Profile(AnyConnect 연결 프로파일), 기본 특성

AnyConnect VPN 연결에 대한 기본 특성을 설정하려면 Anyconnect Connection Profiles(AnyConnect 연결 프로파일) 섹션에서 Add(추가) 또는 Edit(수정)를 선택합니다. Add/Edit AnyConnect Connection Profile(AnyConnect 연결 프로파일 추가/수정) > Basic(기본) 대화 상자가 열립니다.

- Name(이름) - 특성을 추가하는 경우 추가하려는 연결 프로파일의 이름을 지정합니다. 특성을 수정하려는 경우 이 필드는 수정할 수 없습니다.
- Aliases(별칭) - (선택 사항) 연결의 대체 이름을 하나 이상 입력합니다. 공백 또는 문장 부호를 사용하여 이름을 구분할 수 있습니다.
- Authentication(인증) - 다음 중 연결을 인증할 방법을 선택하고 인증에서 사용할 AAA 서버 그룹을 지정합니다.
  - 방법 — 여러 인증서 인증을 위해 프로토콜 교환을 정의하고 두 가지 세션 유형에 활용하기 위해 인증 프로토콜이 확장되었습니다. AnyConnect SSL 및 IKEv2 클라이언트 프로토콜을 사용하여 세션당 여러 인증서를 검증할 수 있습니다. AAA, AAA 및 인증서, 인증서만, SAML, 여러 인증서 및 AAA 또는 여러 인증서 중에서 사용할 인증 유형을 선택합니다. 선택에 따라 연결하기 위해 인증서를 제공해야 할 수 있습니다.
  - AAA Server Group(AAA 서버 그룹) - 드롭다운 목록에서 AAA 서버 그룹을 선택하십시오. 기본 설정은 ASA에서 인증을 처리하도록 지정하는 LOCAL(로컬)입니다. 선택하기 전에 **Manage(**관리**)**를 클릭하여 이 대화 상자 위로 대화 상자를 열어서 AAA 서버 그룹의 ASA 구성을 살펴보거나 변경할 수 있습니다.

- LOCAL(로컬) 이외의 옵션을 선택하면 Use LOCAL if Server Group Fails(서버 그룹이 실패할 경우 로컬 사용) 확인란이 활성화됩니다.
- Use LOCAL if Server Group fails(서버 그룹이 실패할 경우 로컬 사용) - Authentication Server Group(인증 서버 그룹) 특성 필드에서 지정한 그룹이 실패할 경우 로컬 데이터베이스 사용을 활성화하려면 이 옵션을 선택합니다.

- Client Address Assignment(클라이언트 주소 할당) - DHCP 서버, 클라이언트 주소 풀 및 클라이언트 IPv6 주소 풀을 사용하도록 선택합니다.
  - DHCP Servers(DHCP 서버) - 사용할 DHCP 서버의 이름 또는 IP 주소를 입력합니다.
  - Client Address Pools(클라이언트 주소 풀) - 클라이언트 주소 할당에 사용할 이미 구성된 IPv4 주소 풀의 풀 이름을 입력합니다. 선택하기 전에 **Select(**선택**)**를 클릭하여 이 대화 상자 위로 대화 상자를 열어서 주소 풀을 살펴보거나 변경할 수 있습니다. IPv4 주소 풀 추가 또는 수정에 대한 자세한 내용은 을 참조하십시오.
  - Client Address Pools(클라이언트 주소 풀) - 클라이언트 주소 할당에 사용할 이미 구성된 IPv6 주소 풀의 풀 이름을 입력합니다. 선택하기 전에 **Select(**선택**)**를 클릭하여 이 대화 상자 위로 대화 상자를 열어서 주소 풀을 살펴보거나 변경할 수 있습니다. IPv6 주소 풀 추가 또는 수정에 대한 자세한 내용은 을 참조하십시오.

- Default Group Policy(기본 그룹 정책) - 사용할 그룹 정책을 선택합니다.
  - Group Policy(그룹 정책) - 이 연결의 기본 그룹 정책으로 할당할 VPN 그룹 정책을 선택합니다. VPN 그룹 정책은 사용자 중심 특성/값 쌍의 모음으로, 내부 디바이스에 또는 외부의 RADIUS 서버에 저장할 수 있습니다. 기본값은 DfltGrpPolicy입니다. **Manage(**관리**)**를 클릭하여 이 대화 상자 위로 대화 상자를 열어서 그룹 정책 구성을 수정할 수 있습니다.
  - Enable SSL VPN client protocol(SSL VPN 클라이언트 프로토콜 활성화) - 이 VPN 연결에 대해 SSL을 활성화하려면 선택합니다.
  - Enable IPsec (IKEv2) client protocol(IPsec(IKEv2) 클라이언트 프로토콜 활성화) - 이 연결에 대해 IKEv2를 사용하는 IPsec을 활성화하려면 선택합니다.
  - DNS Servers(DNS 서버) - 이 정책에 대한 DNS 서버의 IP 주소를 입력합니다.
  - WINS Servers(WINS 서버) - 이 정책에 대한 WINS 서버의 IP 주소를 입력합니다.
  - Domain Name(도메인 이름) - 기본 도메인 이름을 입력합니다.

- Find(찾기) - 검색 문자열로 사용할 GUI 레이블 또는 CLI 명령을 입력한 후 **Next(**다음**)** 또는 **Previous(**이전**)**를 클릭하여 검색을 시작합니다.

연결 프로파일, 고급 특성

Advanced(고급) 메뉴 항목 및 해당 대화 상자에서 이 연결에 대해 다음 특징을 구성할 수 있습니다.

- 일반 특성

- 클라이언트 주소 지정 특성
- 인증 특성
- 권한 부여 특성
- 어카운트 관리 특성
- 이름 서버 특성
- 클라이언트리스 SSL VPN 특성

참고 SSL VPN 및 보조 인증 특성은 SSL VPN 연결 프로파일에만 적용됩니다.

AnyConnect Connection Profile(AnyConnect 연결 프로파일), 일반 특성

- Enable Simple Certificate Enrollment (SCEP) for this Connection Profile(이 연결 프로파일에 대해 SCEP(Simple Certificate Enrollment) 활성화)
- AAA 서버로 전달하기 전에 사용자 이름에서 영역 제거
- AAA 서버로 전달하기 전에 사용자 이름에서 그룹 제거
- 그룹 구분 기호
- Enable Password Management(비밀번호 관리 활성화) - 사용자에게 비밀번호 만료에 대해 알리는 것과 관련된 파라미터를 구성할 수 있습니다.
  - Notify user __ days prior to password expiration(비밀번호 만료 __일 전에 사용자에게 알림) - 사용자 로그인 시 비밀번호 만료까지 남은 일 수를 알리도록 지정합니다. 비밀번호 만료 14일 전부터 알리기 시작하여 사용자가 비밀번호를 변경할 때까지 날마다 알리는 것이 기본값입니다. 범위는 1~180일입니다.
  - Notify user on the day password expires(비밀번호 만료 당일에 사용자에게 알림) - 비밀번호가 만료되는 당일에만 사용자에게 알립니다.

    어떤 옵션을 선택하든 사용자가 비밀번호를 변경하지 않고 비밀번호가 만료되면 ASA에서는 사용자에게 비밀번호를 변경할 수 있는 기회를 줍니다. 현재 비밀번호가 만료되지 않은 경우, 사용자는 이 비밀번호를 사용하여 계속 로그인할 수 있습니다.

    비밀번호 만료까지 남은 일 수를 변경하는 옵션이 아니라 알림을 활성화하는 옵션입니다. 이 옵션을 선택할 경우 일 수도 지정해야 합니다.
- Translate Assigned IP Address to Public IP Address(공개 IP 주소에 할당된 IP 주소 변환) - 매우 드물기는 하지만, 할당된 로컬 IP 주소 대신 VPN 피어의 실제 IP 주소를 내부 네트워크에 사용하려는 경우가 있습니다. 일반적으로 VPN에서는 내부 네트워크에 액세스할 수 있도록, 할당된 로컬 IP 주소를 피어에 제공합니다. 그러나 예를 들어 내부 서버 및 네트워크 보안이 피어의 실제 IP 주소를 기반으로 하는 경우, 로컬 IP 주소를 피어의 실제 공개 IP 주소로 다시 변환할 수 있습니다. 터널 그룹당 1개의 인터페이스에서 해당 기능을 활성화할 수 있습니다.

- Enable the address translation on interface(인터페이스에서 주소 변환 활성화) - 주소 변환이 활성화되고, 주소가 표시될 인터페이스를 사용자가 선택할 수 있습니다. *Outside*는 AnyConnect 클라이언트가 연결할 인터페이스이고 *inside*는 새로운 터널 인터페이스 그룹에 한정된 인터페이스입니다.

참고 라우팅 문제 및 기타 제한 때문에 꼭 필요한 경우가 아니면 이 기능을 사용하지 않는 것이 좋습니다.

- Find(찾기) - 검색 문자열로 사용할 GUI 레이블 또는 CLI 명령을 입력한 후 **Next(**다음**)** 또는 **Previous(**이전**)**를 클릭하여 검색을 시작합니다.

연결 프로파일, 클라이언트 주소 지정

연결 프로파일의 Client Addressing(클라이언트 주소 지정) 창에서는 이 연결 프로파일과 함께 사용할 IP 주소 풀을 특정 인터페이스에 할당합니다. Client Addressing(클라이언트 주소 지정) 창은 모든 클라이언트 연결 프로파일에 공통적으로 있으며, 다음 ASDM 경로에서 찾을 수 있습니다.

- **Configuration(**구성**) > Remote Access VPN(**원격 액세스 **VPN) > Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**) > AnyConnect Connection Profiles(AnyConnect** 연결 프로파일**)**
- **Configuration(**구성**) > Remote Access VPN(**원격 액세스 **VPN) > Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**) > IPsec (IKEv1) Connection Profiles(IPsec(IKEv1)** 연결 프로파일**)**
- **Configuration(**구성**) > Remote Access VPN(**원격 액세스 **VPN) > Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**) > IPsec (IKEv2) Connection Profiles(IPsec(IKEv1)** 연결 프로파일**)**

여기서 구성하는 주소 풀을 연결 프로파일의 Basic(기본) 창에서도 구성할 수 있습니다.

AnyConnect 연결 프로파일은 IPv4 주소 풀은 물론이고 IPv6까지 할당할 수 있습니다.

클라이언트 주소 지정을 구성하려면 원격 액세스 클라이언트 연결 프로파일(AnyConnect, IKEv1 또는 IKEv2)을 열고 **Advanced(**고급**)** > **Client Addressing(**클라이언트 주소 지정**)**을 선택합니다.

- 주소 풀 구성을 보거나 변경하려면 대화 상자에서 **Add(**추가**)** 또는 **Edit(**수정**)**를 클릭합니다. Assign Address Pools to Interface(인터페이스에 주소 풀 할당) 대화 상자가 열립니다. 이 대화 상자에서 ASA에 구성된 인터페이스에 IP 주소 풀을 할당할 수 있습니다. 선택을 클릭합니다. 이 대화 상자에서 주소 풀 구성을 살펴봅니다. 주소 풀 구성을 다음과 같이 변경할 수 있습니다.
  - ASA에 주소 풀을 추가하려면 **Add(**추가**)**를 클릭합니다. Add IP Pool(IP 풀 추가) 대화 상자가 열립니다.
  - ASA의 주소 풀 구성을 변경하려면 **Edit(**수정**)**를 클릭합니다. 주소 풀이 사용되지 않고 있으면 Edit IP Pool(IP 풀 수정) 대화 상자가 열립니다.

    주소 풀이 이미 사용되고 있으면 주소 풀을 수정할 수 없습니다. **Edit(**수정**)**를 클릭했는데 주소 풀이 이미 사용되고 있으면 ASDM에 오류 메시지가 표시되고 풀에서 해당 주소를 사용 중인 연결 이름 및 사용자 이름이 나열됩니다.

- ASA의 주소 풀을 제거하려면 테이블에서 해당 항목을 선택하고 **Delete(**삭제**)**를 클릭합니다.

  주소 풀이 이미 사용되고 있으면 주소 풀을 제거할 수 없습니다. **Delete(**삭제**)**를 클릭했는데 주소 풀이 이미 사용되고 있으면 ASDM에 오류 메시지가 표시되고 풀에서 해당 주소를 사용 중인 연결 이름 및 사용자 이름이 나열됩니다.

- 인터페이스에 주소 풀을 할당하려면 **Add(**추가**)**를 클릭합니다. Assign Address Pools to Interface(인터페이스에 주소 풀 할당) 대화 상자가 열립니다. 주소 풀을 할당할 인터페이스를 선택합니다. Address Pools(주소 풀) 필드 옆에 있는 **Select(**선택**)**를 클릭합니다. Select Address Pools(주소 풀 선택) 대화 상자가 열립니다. 할당되지 않은 풀 중에 인터페이스에 할당할 각 풀을 두 번 클릭하거나 할당되지 않은 각 풀을 선택하고 **Assign(**할당**)**을 클릭합니다. 인접한 필드에 풀 할당 목록이 표시됩니다. **OK(**확인**)**를 클릭하여 이러한 주소 풀 이름으로 Address Pools(주소 풀) 필드를 채운 후 **OK(**확인**)**를 다시 클릭하여 할당 구성을 완료합니다.
- 인터페이스에 할당된 주소 풀을 변경하려면 해당 인터페이스를 두 번 클릭하거나 인터페이스를 클릭하고 **Edit(**수정**)**를 클릭합니다. Assign Address Pools to Interface(인터페이스에 주소 풀 할당) 대화 상자가 열립니다. 주소 풀을 제거하려면 각 풀 이름을 두 번 클릭하고 키보드의 **Delete(**삭제**)** 버튼을 누릅니다. 인터페이스에 필드를 더 할당하려면 Address Pools(주소 풀) 옆에 있는 **Select(**선택**)**를 클릭합니다. Select Address Pools(주소 풀 선택) 대화 상자가 열립니다. Assign(할당) 필드에는 해당 인터페이스에 할당된 채로 남아 있는 주소 풀 이름이 표시됩니다. 할당되지 않은 풀 중에 인터페이스에 추가할 각 풀을 두 번 클릭합니다. Assign(할당) 필드의 풀 할당 목록이 업데이트됩니다. **OK(**확인**)**를 클릭하여 이러한 주소 풀 이름으로 Address Pools(주소 풀) 필드를 변경한 후 **OK(**확인**)**를 다시 클릭하여 할당 구성을 완료합니다.
- 항목을 제거하려면 해당 항목을 선택하고 **Delete(**삭제**)**를 클릭합니다.

관련 항목

연결 프로파일, 클라이언트 주소 지정, 추가 또는 수정, 115 페이지
연결 프로파일, 주소 풀, 116 페이지
연결 프로파일, 고급, IP 풀 추가 또는 수정, 116 페이지

연결 프로파일, 클라이언트 주소 지정, 추가 또는 수정

연결 프로파일에 주소 풀을 할당하려면 **Advanced(**고급**) > Client Addressing(**클라이언트 주소 지정**)**을 선택한 후 **Add(**추가**)** 또는 **Edit(**수정**)**를 선택합니다.

- Interface(인터페이스) - 주소 풀을 할당할 인터페이스를 선택합니다. 기본값은 DMZ입니다.
- Address Pools(주소 풀) - 지정된 인터페이스에 할당할 주소 풀을 지정합니다.
- Select(선택) - 이 인터페이스에 할당할 주소 풀을 하나 이상 선택할 수 있는 Select Address Pools(주소 풀 선택) 대화 상자가 열립니다. 선택한 주소 풀이 Assign Address Pools to Interface(인터페이스에 주소 풀 할당) 대화 상자의 Address Pools(주소 풀)에 표시됩니다.

연결 프로파일, 주소 풀

Connection Profile(연결 프로파일) > Advanced(고급)의 Select Address Pools(주소 풀 선택) 대화 상자에는 풀 이름, 시작 및 끝 주소, 클라이언트 주소 할당에 사용 가능한 주소 풀의 서브넷 마스크가 표시됩니다. 해당 목록에서 항목을 추가, 수정 또는 삭제할 수 있습니다.

- Add(추가) - 새 IP 주소 풀을 구성할 수 있는 Add IP Pool(IP 풀 추가) 대화 상자가 열립니다.
- Edit(수정) - 선택한 IP 주소 풀을 수정할 수 있는 Edit IP Pool(IP 풀 수정) 대화 상자가 열립니다.
- Delete(삭제) - 선택한 주소 풀을 제거합니다. 확인 또는 실행 취소가 없습니다.
- Assign(할당) - 해당 인터페이스에 할당된 채로 남아 있는 주소 풀 이름이 표시됩니다. 할당되지 않은 풀 중에 인터페이스에 추가할 각 풀을 두 번 클릭합니다. Assign(할당) 필드의 풀 할당 목록이 업데이트됩니다.

연결 프로파일, 고급, IP 풀 추가 또는 수정

Connection Profile(연결 프로파일) > Advanced(고급)의 Add or Edit IP Pool(IP 풀 추가 또는 수정) 대화 상자에서 클라이언트 주소 할당에 사용할 IP 주소 범위를 지정 또는 수정할 수 있습니다.

- Name(이름) - IP 주소 풀에 할당된 이름을 지정합니다.
- Starting IP Address(시작 IP 주소) - 풀의 첫 번째 IP 주소를 지정합니다.
- Ending IP Address(종료 IP 주소) - 풀의 마지막 번째 IP 주소를 지정합니다.
- Subnet Mask(서브넷 마스크) - 풀의 주소에 적용할 서브넷 마스크를 선택합니다.

AnyConnect Connection Profile(AnyConnect 연결 프로파일), 인증 특성

Connection Profile(연결 프로파일) > Advanced(고급) >Authentication(인증) 탭에서 다음 필드를 구성할 수 있습니다.

- Interface-specific Authentication Server Groups(인터페이스별 인증 서버 그룹) - 특정 인터페이스에 대한 인증 서버 그룹 할당을 관리합니다.
  - Add or Edit(추가 또는 수정) - Assign Authentication Server Group to Interface(인터페이스에 인증 서버 그룹 할당) 대화 상자가 열립니다. 이 대화 상자에서 인터페이스 및 서버 그룹을 지정하고, 선택한 서버 그룹에 장애 발생 시 로컬 데이터베이스로 대체하는 것을 허용할지 여부를 지정할 수 있습니다. 이 대화 상자의 Manage(관리) 버튼을 누르면 Configure AAA Server Groups(AAA 서버 그룹 구성) 대화 상자가 열립니다. 선택한 항목은 Interface/Server Group(인터페이스/서버 그룹) 테이블에 표시됩니다.
  - Delete(삭제) - 선택한 서버 그룹을 테이블에서 제거합니다. 확인 또는 실행 취소가 없습니다.
- Username Mapping from Certificate(인증서의 사용자 이름 매핑) - 사용자 이름을 추출할 디지털 인증서에서 방법 및 필드를 지정할 수 있습니다.

참고 이 기능은 다중 컨텍스트 모드에서 지원되지 않습니다.

- Pre-fill Username from Certificate(인증서의 사용자 이름 미리 채우기) - 이 창에 이어서 나오는 옵션에 따라, 지정된 인증서 필드의 사용자 이름을 추출하여 사용자 이름/비밀번호 인증 및 권한 부여에 사용합니다.
- Hide username from end user(엔드 유저에게 사용자 이름 숨김) - 추출한 사용자 이름이 엔드 유저에게 표시되지 않도록 지정합니다.
- Use script to choose username(스크립트를 사용하여 사용자 이름 선택) - 디지털 인증서에서 사용자 이름을 선택하는 데 사용할 스크립트 이름을 지정합니다. 기본값은 --None--(--없음--)입니다.
- Add or Edit(추가 또는 수정) - 인증서의 사용자 이름 매핑에 사용할 스크립트를 정의할 수 있는 Add or Edit Script Content(스크립트 콘텐츠 추가 또는 수정) 대화 상자가 열립니다.
- Delete(삭제) - 선택한 스크립트를 삭제합니다. 확인 또는 실행 취소가 없습니다.
- Use the entire DN as the username(사용자 이름으로 전체 DN 사용) - 인증서의 전체 DN(Distinguished Name) 필드를 사용자 이름으로 사용하도록 지정합니다.
- Specify the certificate fields to be used as the username(사용자 이름으로 사용할 인증서 필드 지정) - 결합하여 사용자 이름으로 사용할 필드를 하나 이상 지정합니다.

  기본 및 보조 특성에 사용할 수 있는 값은 다음과 같습니다.

특성	정의
C	Country(국가): 2자로 된 국가 약어입니다. 이러한 코드는 ISO 3166 국가 약어를 따릅니다.
CN	Common Name(공통 이름): 사람, 시스템 또는 기타 실체의 이름입니다. 보조 특성으로는 사용할 수 없습니다.
DNQ	Domain Name Qualifier(도메인 이름 한정자)입니다.
EA	E-mail address(이메일 주소)입니다.
GENQ	Generational Qualifier(세대 한정자)입니다.
GN	Given Name(이름)입니다.
I	Initials(이니셜)입니다.
L	Locality(구/군/시): 조직이 있는 구/군/시입니다.

특성	정의
아니요	Name(이름)입니다.
O	Organization(조직): 회사, 기관, 에이전시, 협회 또는 기타 실체의 이름입니다.
OU	Organizational Unit(조직 단위): 조직(O) 내의 하위 그룹입니다.
SER	Serial Number(일련 번호)입니다.
SN	Surname(성)입니다.
SP	State/Province(주/도): 조직이 있는 주/도입니다.
T	Title(직함)입니다.
UID	User Identifier(사용자 ID)입니다.
UPN	User Principal Name(사용자 어카운트 이름)입니다.

- Primary Field(기본 필드) - 인증서에서 사용자 이름에 사용할 첫 번째 필드를 선택합니다. 이 값이 있을 경우 보조 필드는 무시됩니다.
- Secondary Field(보조 필드) - 기본 필드가 없는 경우에 사용할 필드를 선택합니다.

- Find(찾기) - 검색 문자열로 사용할 GUI 레이블 또는 CLI 명령을 입력한 후 **Next(**다음**)** 또는 **Previous(**이전**)**를 클릭하여 검색을 시작합니다.

연결 프로파일, 보조 인증 특성

Connection Profile(연결 프로파일) > Advanced(고급) 아래의 Secondary Authentication(보조 인증)을 사용하면 이중 인증이라고도 하는 보조 인증을 구성할 수 있습니다. 보조 인증이 활성화되면 엔드 유저는 유효한 인증 자격 증명 두 세트를 제공해야 로그온할 수 있습니다. 인증서에서 사용자 이름 미리 채우기와 함께 보조 인증을 사용할 수 있습니다. 이 대화 상자의 필드는 기본 인증에 대해 구성하는 필드와 유사하지만 이러한 필드는 보조 인증과만 관련이 있습니다.

이중 인증이 활성화된 경우 이러한 특성은 인증서에 있는 하나 이상의 필드를 선택하여 사용자 이름으로 사용합니다. 인증서 특성에서 보조 사용자 이름을 구성하면 보안 어플라이언스가 지정된 인증서 필드를 두 번째 사용자 이름/비밀번호 인증을 위한 두 번째 사용자 이름으로 사용합니다.

참고 인증서의 보조 사용자 이름과 함께 보조 인증 서버 그룹을 지정한 경우에는 기본 사용자 이름만 인증에 사용됩니다.

- Secondary Authorization Server Group(보조 권한 부여 서버 그룹) - 보조 자격 증명을 추출할 권한 부여 서버 그룹을 지정합니다.
  - Server Group(서버 그룹) - 보조 서버 AAA 그룹으로 사용할 권한 부여 서버 그룹을 선택합니다. 기본값은 none(없음)입니다. 보조 서버 그룹은 SDI 서버 그룹을 지정할 수 없습니다.
  - Manage(관리) - Configure AAA Server Groups(DNS 서버 그룹 구성) 대화 상자를 엽니다.
  - Use LOCAL if Server Group fails(서버 그룹이 실패한 경우 로컬 사용) - 지정된 서버 그룹이 실패한 경우 로컬 데이터베이스로 대체하도록 지정합니다.
  - Use primary username(기본 사용자 이름 사용) - 로그인 대화 상자에서 하나의 사용자 이름만 요청해야 하도록 지정합니다.
  - Attributes Server(특성 서버) - 이 서버가 기본 특성 서버인지 또는 보조 특성 서버인지 선택합니다.

    참고 이 연결 프로필에 대해 권한 부여 서버도 지정한 경우 권한 부여 서버 설정이 우선적으로 적용됩니다. ASA에서는 이 보조 인증 서버를 무시합니다.

  - Session Username Server(세션 사용자 이름 서버) - 이 서버가 기본 세션 사용자 이름 서버인지 보조 세션 사용자 이름 서버인지 선택합니다.
- Interface-Specific Authorization Server Groups(인터페이스별 권한 부여 서버 그룹) - 특정 인터페이스에 대한 권한 부여 서버 그룹 할당을 관리합니다.
  - Add or Edit(추가 또는 수정) - Assign Authentication Server Group to Interface(인터페이스에 인증 서버 그룹 할당) 대화 상자가 열립니다. 이 대화 상자에서 인터페이스 및 서버 그룹을 지정하고, 선택한 서버 그룹에 장애 발생 시 로컬 데이터베이스로 대체하는 것을 허용할지 여부를 지정할 수 있습니다. 이 대화 상자의 Manage(관리) 버튼을 누르면 Configure AAA Server Groups(AAA 서버 그룹 구성) 대화 상자가 열립니다. 선택한 항목은 Interface/Server Group(인터페이스/서버 그룹) 테이블에 표시됩니다.
  - Delete(삭제) - 선택한 서버 그룹을 테이블에서 제거합니다. 확인 또는 실행 취소가 없습니다.
- Username Mapping from Certificate(인증서에서 사용자 이름 매핑) - 사용자 이름을 추출할 디지털 인증서의 필드를 지정합니다.
- Pre-fill Username from Certificate(인증서에서 사용자 이름 미리 채우기) - 이 패널에 지정된 기본 및 보조 필드에서 보조 인증에 사용할 이름을 추출하려면 선택합니다. 이 특성을 선택하기 전에 AAA와 인증서 모두에 대한 인증 방법을 구성해야 합니다. 이렇게 하려면 같은 창에서 Basic(기본) 패널로 돌아가 Method(방법) 옆에서 **Both(**둘 다**)**를 선택합니다.
- Hide username from end user(엔드 유저에게 사용자 이름 숨기기) - VPN 사용자에게 보조 인증에 사용할 사용자 이름을 숨기려면 선택합니다.
- Fallback when a certificate is unavailable(인증서를 사용할 수 없는 경우 대체) - 이 특성은 "Hide username from end user(엔드 유저에게 사용자 이름 숨기기)"를 선택한 경우에만 구성할 수 있습

니다. 인증서를 사용할 수 없는 경우 Cisco Secure Desktop Host Scan 데이터를 사용하여 보조 인증용 사용자 이름을 미리 채웁니다.

- Password(비밀번호) - 다음 방법 중 하나를 선택하여 보조 인증에 사용할 비밀번호를 검색합니다.
  - Prompt(매번 확인) - 사용자에게 비밀번호를 묻는 프롬프트를 표시합니다.
  - Use Primary(기본 사용) - 모든 보조 인증에 기본 인증 비밀번호를 다시 사용합니다.
  - Use(사용) - 모든 보조 인증에 일반적인 보조 비밀번호를 입력합니다.
- Specify the certificate fields to be used as the username(사용자 이름으로 사용할 인증서 필드 지정) - 사용자 이름으로 일치할 사용할 필드를 하나 이상 지정합니다. 인증서에서 사용자 이름 미리 채우기에서 이 사용자 이름을 보조 사용자 이름/비밀번호 인증 또는 권한 부여로 사용하려면 사용자 이름 미리 채우기 및 보조 사용자 이름 미리 채우기도 구성해야 합니다.
  - Primary Field(기본 필드) - 인증서에서 사용자 이름에 사용할 첫 번째 필드를 선택합니다. 이 값이 있을 경우 보조 필드는 무시됩니다.
  - Secondary Field(보조 필드) - 기본 필드가 없는 경우에 사용할 필드를 선택합니다.

기본 및 보조 필드 특성의 옵션은 다음과 같습니다.

특성	정의
C	Country(국가): 2자로 된 국가 약어입니다. 이러한 코드는 ISO 3166 국가 약어를 따릅니다.
CN	Common Name(공통 이름): 사람, 시스템 또는 기타 실체의 이름입니다. 보조 특성으로는 사용할 수 없습니다.
DNQ	Domain Name Qualifier(도메인 이름 한정자)입니다.
EA	E-mail address(이메일 주소)입니다.
GENQ	Generational Qualifier(세대 한정자)입니다.
GN	Given Name(이름)입니다.
I	Initials(이니셜)입니다.
L	Locality(구/군/시): 조직이 있는 구/군/시입니다.
아니요	Name(이름)입니다.
O	Organization(조직): 회사, 기관, 에이전시, 협회 또는 기타 실체의 이름입니다.

특성	정의
OU	Organizational Unit(조직 단위): 조직(O) 내의 하위 그룹입니다.
SER	Serial Number(일련 번호)입니다.
SN	Surname(성)입니다.
SP	State/Province(주/도): 조직이 있는 주/도입니다.
T	Title(직함)입니다.
UID	User Identifier(사용자 ID)입니다.
UPN	User Principal Name(사용자 어카운트 이름)입니다.

- Use the entire DN as the username(전체 DN을 사용자 이름으로 사용) - 전체 주체 DN(RFC1779)을 사용하여 디지털 인증서에서 권한 부여 쿼리 이름을 파생시킵니다.
- Use script to select username(스크립트를 사용하여 사용자 이름 선택) - 디지털 인증서에서 사용자 이름을 추출할 스크립트의 이름을 지정합니다. 기본값은 --None--(--없음--)입니다.
  - Add or Edit(추가 또는 수정) - 인증서의 사용자 이름 매핑에 사용할 스크립트를 정의할 수 있는 Add or Edit Script Content(스크립트 콘텐츠 추가 또는 수정) 대화 상자가 열립니다.
  - Delete(삭제) - 선택한 스크립트를 삭제합니다. 확인 또는 실행 취소가 없습니다.

AnyConnect Connection Profile(AnyConnect 연결 프로파일), 권한 부여 특성

AnyConnect Connection Profile(AnyConnect 연결 프로파일)의 Authorization(권한 부여) 대화 상자에서는 인터페이스별 권한 부여 서버 그룹을 확인, 추가, 수정 또는 삭제할 수 있습니다. 이 대화 상자의 각 테이블 행에는 하나의 인터페이스 관련 서버 그룹의 상태가 표시됩니다. 예를 들어 인터페이스 이름, 연계된 서버 그룹, 선택한 서버 그룹이 실패한 경우 로컬 데이터베이스로의 대체가 활성화되는지 여부 등이 표시됩니다.

이 창에 있는 필드는 AnyConnect, IKEv1 및 IKEv2, 클라이언트리스 SSL 연결 프로파일에 대해 동일합니다.

- Authorization Server Group(권한 부여 서버 그룹) - 권한 부여 매개변수를 가져올 권한 부여 서버 그룹 그룹을 지정합니다.
  - Server Group(서버 그룹) - 사용할 권한 부여 서버 그룹을 선택합니다. 기본값은 none(없음)입니다.

- Manage(관리) - Configure AAA Server Groups(DNS 서버 그룹 구성) 대화 상자를 엽니다. AAA 서버 구성에 대한 자세한 내용은 클라이언트리스 SSL VPN 연결 프로파일, 인증, 서버 그룹 추가, 130 페이지을 참조하십시오.
- Users must exist in the authorization database to connect(연결할 권한 부여 데이터베이스에 사용자가 존재해야 함) - 사용자가 이 조건을 충족하도록 하려면 이 확인란을 선택합니다.

- Interface-specific Authorization Server Groups(인터페이스별 권한 부여 서버 그룹) - 특정 인터페이스에 대한 권한 부여 서버 그룹 할당을 관리합니다.
  - Add or Edit(추가 또는 수정) - Assign Authentication Server Group to Interface(인터페이스에 인증 서버 그룹 할당) 대화 상자가 열립니다. 이 대화 상자에서 인터페이스 및 서버 그룹을 지정하고, 선택한 서버 그룹에 장애 발생 시 로컬 데이터베이스로 대체하는 것을 허용할지 여부를 지정할 수 있습니다. 이 대화 상자의 Manage(관리) 버튼을 누르면 Configure AAA Server Groups(AAA 서버 그룹 구성) 대화 상자가 열립니다. 선택한 항목은 Interface/Server Group(인터페이스/서버 그룹) 테이블에 표시됩니다.
  - Delete(삭제) - 선택한 서버 그룹을 테이블에서 제거합니다. 확인 또는 실행 취소가 없습니다.

- Username Mapping from Certificate(인증서에서 사용자 이름 매핑) - 사용자 이름을 추출할 디지털 인증서의 필드를 지정합니다.
  - Use script to select username(스크립트를 사용하여 사용자 이름 선택) - 디지털 인증서에서 사용자 이름을 선택하는 데 사용할 스크립트 이름을 지정합니다. 기본값은 --None--(--없음--)입니다. 인증서 필드에서 사용자 이름을 선택하는 스크립트를 만드는 방법에 대한 자세한 내용은 다음을 참조하십시오.
  - Add or Edit(추가 또는 수정) - 인증서의 사용자 이름 매핑에 사용할 스크립트를 정의할 수 있는 Add or Edit Script Content(스크립트 콘텐츠 추가 또는 수정) 대화 상자가 열립니다.
  - Delete(삭제) - 선택한 스크립트를 삭제합니다. 확인 또는 실행 취소가 없습니다.
  - Use the entire DN as the username(사용자 이름으로 전체 DN 사용) - 인증서의 전체 DN(Distinguished Name) 필드를 사용자 이름으로 사용하도록 지정합니다.
  - Specify the certificate fields to be used as the username(사용자 이름으로 사용할 인증서 필드 지정) - 결합하여 사용자 이름으로 사용할 필드를 하나 이상 지정합니다.
  - Primary Field(기본 필드) - 인증서의 사용자 이름에 사용할 첫 번째 필드를 선택합니다. 이 값이 있을 경우 보조 필드는 무시됩니다.
  - Secondary Field(보조 필드) - 기본 필드가 없는 경우에 사용할 필드를 선택합니다.

- Find(찾기) - 검색 문자열로 사용할 GUI 레이블 또는 CLI 명령을 입력한 후 Next(다음) 또는 Previous(이전)를 클릭하여 검색을 시작합니다.

AnyConnect Connection Profile(AnyConnect 연결 프로파일), 권한 부여, 스크립트 콘텐츠를 추가하여 사용자 이름 선택

AnyConnect Connection Profile(AnyConnect 연결 프로파일)의 Authorization(권한 부여) 창에서 **use a script to select username**(스크립트를 사용하여 사용자 이름 선택)을 선택하고 Add(추가) 또는 Edit(수정) 버튼을 클릭하면 다음과 같은 필드가 표시됩니다.

스크립트에서는 다른 매핑 옵션에 나열되지 않은 권한 부여를 위한 인증서 필드를 사용할 수 있습니다.

참고 스크립트를 사용하여 인증서에서 사용자 이름 미리 채우기 기능이 클라이언트 인증서에서 사용자 이름을 찾을 수 없는 경우에는 AnyConnect 클라이언트와 클라이언트리스 WebVPN 모두 사용자 이름 필드에 "Unknown(알 수 없음)"을 표시합니다.

- Script Name(스크립트 이름) - 스크립트의 이름을 지정합니다. 스크립트 이름은 권한 부여와 인증 모두에서 동일해야 합니다. 여기에서 스크립트를 정의하면 CLI에서 동일한 스크립트를 사용하여 이 기능을 수행합니다.
- Select script parameters(스크립트 매개변수 선택) - 스크립트의 특성 및 콘텐츠를 지정합니다.
- Value for Username(사용자 이름 값) - 표준 DN 특성의 드롭다운 목록에서 사용자 이름(주체 DN)으로 사용할 특성을 선택합니다.
- No Filtering(필터링 없음) - 지정된 전체 DN 이름을 사용하도록 지정합니다.
- Filter by substring(부분 문자열로 필터링) - 시작 인덱스(일치시킬 첫 번째 문자의 문자열 내 위치) 및 종료 인덱스(검색할 문자 수)를 지정합니다. 이 옵션을 선택한 경우 시작 인덱스를 비워 둘 수 없습니다. 종료 인덱스를 빈 상태로 둔 경우에는 기본적으로 -1로 설정됩니다. 이는 전체 문자열에서 일치하는 항목이 검색됨을 나타냅니다.

  예를 들어 호스트/사용자의 값이 포함된 DN 특성 Common Name(공통 이름) (CN)을 선택했다고 가정해 보겠습니다. 다음 표에는 다양한 반환 값을 얻기 위해 부분 문자열 옵션을 사용하여 이 값을 필터링할 수 있는 몇 가지 가능한 방법이 나와 있습니다. 반환 값은 실제로 사용자 이름으로 미리 채워집니다.

  표 ***2:*** 부분 문자열로 필터링

시작 인덱스	종료 인덱스	반환 값
1	5	host/
6	10	user
6	-1	user

  이 표의 세 번째 행으로 음수 인덱스를 사용하면 문자열의 끝에서 부분 문자열의 끝까지 역으로 계산하도록 지정됩니다(이 예의 경우 "user"의 "r").

부분 문자열로 필터링할 때는 찾으려는 부분 문자열의 길이를 알아야 합니다. 다음 예에서는 정규식 일치 또는 Lua 형식의 사용자 지정 스크립트를 사용합니다.

- 예 1: 정규식 일치 - Regular Expression(정규식) 필드에서 검색에 적용할 정규식을 입력합니다. 표준 정규식 연산자가 적용됩니다. 예를 들어 정규식을 사용하여 "EA(이메일 주소)" DN 값의 @ 기호까지 모든 문자를 필터링하려는 경우를 가정해 보겠습니다. 정규식 ^[^@]*는 이 작업을 수행하는 한 가지 방법입니다. 이 예에서 DN 값에 user1234@example.com 값이 포함된 경우 정규식 이후의 반환 값은 user1234가 됩니다.
- 예 2: LUA 형식의 맞춤형 스크립트 사용 - LUA 프로그래밍 언어로 작성된 맞춤형 스크립트를 지정하여 검색 필드를 구문 분석합니다. 이 옵션을 선택하면 맞춤형 LUA 스크립트를 입력할 수 있는 필드를 사용할 수 있습니다. 예를 들어 다음 스크립트를 입력할 수 있습니다.

```
return cert.subject.cn..'/'..cert.subject.l
```

이 스크립트는 두 개의 DN 필드, 즉 사용자 이름(cn)과 구/군/시(l)를 결합하여 단일 사용자 이름으로 사용하고 두 필드 사이에 슬래시(/) 문자를 삽입합니다.

다음 표에는 LUA 스크립트에서 사용할 수 있는 속성 이름 및 설명이 나와 있습니다.

참고 LUA는 대/소문자를 구분합니다.

표 ***3:*** 특성 이름 및 설명

특성 이름	설명
cert.subject.c	Country
cert.subject.cn	공용 이름
cert.subject.dnq	DN 한정자
cert.subject.ea	이메일 주소
cert.subject.genq	세대 한정자
cert.subject.gn	이름
cert.subject.i	이니셜
cert.subject.l	구/군/시
cert.subject.n	이름
cert.subject.o	조직
cert.subject.ou	조직 단위
cert.subject.ser	주체 일련 번호

cert.subject.sn	성
cert.subject.sp	주/도
cert.subject.t	직함
cert.subject.uid	사용자 ID
cert.issuer.c	Country
cert.issuer.cn	공용 이름
cert.issuer.dnq	DN 한정자
cert.issuer.ea	이메일 주소
cert.issuer.genq	세대 한정자
cert.issuer.gn	이름
cert.issuer.i	이니셜
cert.issuer.l	구/군/시
cert.issuer.n	이름
cert.issuer.o	조직
cert.issuer.ou	조직 단위
cert.issuer.ser	발급자 일련 번호
cert.issuer.sn	성
cert.issuer.sp	주/도
cert.issuer.t	직함
cert.issuer.uid	사용자 ID
cert.serialnumber	인증서 일련 번호
cert.subjectaltname.upn	사용자 어카운트 이름

터널 그룹 스크립트를 활성화하는 동안 오류가 발생하여 스크립트가 활성화되지 않은 경우에는 관리자의 콘솔에 오류 메시지가 표시됩니다.

클라이언트리스 SSL VPN 연결 프로파일, 인터페이스에 권한 부여 서버 그룹 할당

이 대화 상자에서는 인터페이스를 AAA 서버 그룹에 연계할 수 있습니다. 결과는 Authorization(권한 부여) 대화 상자의 테이블에 표시됩니다.

- Interface(인터페이스) - 인터페이스를 선택합니다. 기본값은 DMZ입니다.
- Server Group(서버 그룹) - 선택한 인터페이스에 할당할 서버 그룹을 선택합니다. 기본값은 LOCAL입니다.
- Manage(관리) - Configure AAA Server Groups(DNS 서버 그룹 구성) 대화 상자를 엽니다.

연결 프로파일, 어카운트 관리

Connection Profile(연결 프로필) > Advanced(고급)의 Accounting(어카운트 관리) 창은 ASA의 어카운트 관리 옵션을 전역적으로 설정합니다.

- Accounting Server Group(어카운트 관리 서버 그룹) - 어카운트 관리에 사용하기 위해 이전에 정의한 서버 그룹을 선택합니다.
- Manage(관리) - AAA 서버 그룹을 만들 수 있는 Configure AAA Server Groups(AAA 서버 그룹 구성) 대화 상자를 엽니다.

연결 프로파일, 그룹 별칭 및 그룹 URL

Connection Profile(연결 프로파일) > Advanced(고급)의 GroupAlias/Group URL(그룹 별칭/그룹 URL) 대화 상자에서는 로그인 시 원격 사용자에게 표시되는 항목에 영향을 주는 특성을 구성합니다.

이 대화 상자의 필드는 클라이언트리스 SSL VPN에 하나의 추가 필드가 있다는 점을 제외하고는 AnyConnect 클라이언트와 클라이언트리스 SSL VPN에 대해 동일합니다. 연결 프로파일에 있는 탭의 이름은 AnyConnect의 경우 Group URL/Group Alias(그룹 URL/그룹 별칭)이고, 클라이언트리스 SSL VPN의 경우 Clientless SSL VPN(클라이언트리스 SSL VPN)입니다.

- **Login and Logout (Portal) Page Customization(Clientless SSL VPN only)(**로그인 및 로그아웃**(**포털**)** 페이지 맞춤화**(**클라이언트리스 **SSL VPN**에만 해당**))** - 적용할 미리 구성된 맞춤형 속성을 지정하여 사용자 로그인 페이지의 디자인을 구성합니다. 기본값은 DfltCustomization입니다. 새 맞춤형 개체를 생성하려면 **Manage(**관리**)**를 클릭합니다.
- **Enable the display of Radius Reject-Message on the login screen(**로그인 화면에서 **Radius** 거부 메시지 표시 활성화**)** - 인증이 거부된 경우 로그인 대화 상자에 RADIUS 거부 메시지를 표시하려면 이 확인란을 선택합니다.
- **Enable the display of SecurId message on the login screen(**로그인 화면에서 **SecurId** 메시지 표시 활성화**)** - 로그인 대화 상자에 SecurId 메시지를 표시하려면 이 확인란을 선택합니다.
- **Connection Aliases(**연결 별칭**)** - 연결 별칭 및 상태입니다. 사용자가 로그인 시 특성 연결(터널 그룹)을 선택할 수 있도록 연결이 구성된 경우 사용자 로그인 페이지에 연결 별칭이 표시됩니다. 별칭을 추가 또는 삭제하려면 이 버튼을 클릭합니다. 별칭을 수정하려면 테이블의 별칭을 두 번 클릭하고 항목을 수정합니다. 활성화된 상태를 변경하려면 테이블에서 확인란을 선택하거나 선택 취소합니다.
- 그룹 **URL** - 그룹 URL과 그룹 URL의 상태입니다. 사용자가 로그인 시 특성 그룹을 선택할 수 있도록 연결이 구성된 경우 사용자 로그인 페이지에 그룹 URL이 표시됩니다. URL을 추가 또는 삭

제하려면 해당 버튼을 클릭합니다. URL을 수정하려면 테이블의 URL을 두 번 클릭하고 항목을 수정합니다. 활성화된 상태를 변경하려면 테이블에서 확인란을 선택하거나 선택 취소합니다.

- Do not run Cisco Secure Desktop (CSD) on client machine when using group URLs defined above to access the ASA(위에 정의된 그룹 URL을 사용하여 ASA에 액세스할 경우 클라이언트 컴퓨터에서 CSD(Cisco Secure Desktop)를 실행 안 함) (클라이언트가 연결 별칭을 사용하여 연결하는 경우, 이 설정은 무시됩니다.) - 그룹 URL에 연결하는 클라이언트에서 Cisco Secure Desktop의 Hostscan 애플리케이션을 실행할지 여부를 선택합니다. 이러한 옵션은 그룹 URL을 추가하는 경우에만 표시됩니다. 클라이언트를 면제하는 경우, 보안 어플라이언스가 이러한 사용자로부터 엔드포인트 조건을 수신하지 않으므로 사용자에게 VPN 액세스를 제공하도록 DAP 구성을 변경해야 할 수 있습니다. 다음과 같은 옵션이 있습니다.
  - Always run CSD(CSD 항상 실행) - 그룹 URL에 연결하는 모든 클라이언트에서 Hostscan을 실행합니다.
  - Disable CSD for both AnyConnect and clientless SSL VPN(AnyConnect 및 클라이언트리스 SSL VPN 모두에 대해 CSD 비활성화) - Hostscan 처리에서 그룹 URL에 연결하는 모든 클라이언트를 면제합니다.
  - Disable CSD for AnyConnect only(AnyConnect에 대해서만 CSD 비활성화) - Hostscan 처리에서 그룹 URL에 연결하는 AnyConnect 클라이언트를 면제하지만 클라이언트리스 연결에 대한 Hostscan을 사용합니다.

연결 프로파일, 클라이언트리스 SSL VPN

Configuration(구성**) > Remote Access VPN(**원격 액세스 **VPN) > Clientless SSL VPN Access(**클라이언트리스 **SSL VPN** 액세스**) > Connection Profiles(**연결 프로파일**)** 대화 상자에는 현재 정의된 클라이언트리스 SSL VPN 연결 프로파일과 전역 클라이언트 옵션 목록이 표시됩니다.

- Access Interfaces(액세스 인터페이스) - 액세스할 수 있도록 설정할 인터페이스를 선택할 수 있습니다. 이 테이블의 필드에는 인터페이스 이름과 액세스 허용 여부를 지정하는 확인란이 포함되어 있습니다.
  - Device Certificate(디바이스 인증서) - RSA 키 또는 ECDSA 키/신뢰 지점 인증을 위한 인증서를 지정할 수 있습니다. 두 개의 신뢰 지점을 구성할 수 있습니다. 클라이언트는 공급업체 ID 페이로드로 ECDSA 지원을 나타냅니다. ASA는 구성된 신뢰 지점 목록을 검사하고 클라이언트가 지원하는 첫 번째 신뢰 지점을 선택합니다. ECDSA를 선호할 경우 이 신뢰 지점을 RSA 신뢰 지점보다 먼저 구성해야 합니다.
  - Manage(관리) - 선택한 인증서에 대한 세부사항을 추가, 수정, 삭제, 내보내기 및 표시할 수 있는 Manage Identity Certificates(ID 인증서 관리) 대화 상자를 엽니다.
  - Port Setting(포트 설정) - 클라이언트리스 SSL 및 IPsec(IKEv2) 연결에 대한 포트 번호를 구성합니다. 범위는 1부터 65535까지입니다. 기본값은 포트 443입니다.
- Login Page Setting(로그인 페이지 설정)

- 로그인 페이지에서 사용자가 별칭으로 식별된 연결 프로파일을 선택할 수 있도록 허용합니다. 그렇지 않으면 DefaultWebVPN 그룹이 연결 프로파일이 됩니다. 사용자 로그인 페이지에서 사용자가 연결할 특정 터널 그룹을 선택할 수 있는 드롭다운 목록을 제공하도록 지정합니다.
- Allow user to enter internal password on the login page(사용자가 로그인 페이지에서 내부 비밀번호를 입력하도록 허용) - 내부 서버에 액세스할 때 다른 비밀번호를 입력할 수 있는 옵션을 추가합니다.
- Shutdown portal login page(포털 로그인 페이지 종료) - 로그인이 비활성화된 웹 페이지를 표시합니다.

- Connection Profiles(연결 프로파일) - 이 연결(터널 그룹)에 대한 연결 정책을 확인하는 레코드가 표시된 연결 테이블을 제공합니다. 각 레코드는 연결에 대한 기본 그룹 정책을 식별하며, 프로토콜별 연결 매개변수를 포함합니다.
  - Add(추가) - 선택한 연결에 대한 Add Clientless SSL VPN(클라이언트리스 SSL VPN 추가) 대화 상자를 엽니다.
  - Edit(추가) - 선택한 연결에 대한 Edit Clientless SSL VPN(클라이언트리스 SSL VPN 수정) 대화 상자를 엽니다.
  - Delete(삭제) - 테이블에서 선택한 연결을 제거합니다. 확인 또는 실행 취소가 없습니다.
  - Name(이름) - 연결 프로파일의 이름입니다.
  - Enabled(활성화됨) - 활성화된 경우 선택됩니다.
  - Aliases(별칭) - 연결 프로파일을 식별하는 다른 이름입니다.
  - Authentication Method(인증 방법) - 사용할 인증 방법을 지정합니다.
  - Group Policy(그룹 정책) - 이 연결 프로파일의 기본 그룹 정책을 표시합니다.

- 그룹 URL과 인증서 맵이 서로 다른 연결 프로파일과 일치하는 경우 그룹 URL을 우선 적용. 그렇지 않은 경우 인증서 맵과 일치하는 연결 프로파일 사용 - 이 옵션은 연결 프로파일 선택 프로세스에서 그룹 URL과 인증서 값의 상대적 선호도를 지정합니다. ASA는 엔드포인트에 지정된 기본 설정 값을 연결 프로파일에 지정된 값과 일치시키지 못한 경우 다른 값과 일치하는 연결 프로파일을 선택합니다. 기존 ASA 소프트웨어 버전에서 사용되는 환경 설정을 사용하여 VPN 엔드포인트에서 지정한 그룹 URL을 동일한 그룹 URL을 지정하는 연결 프로파일과 일치시키려는 경우에만 이 옵션을 선택하십시오. 이 옵션은 기본적으로 선택되지 않습니다. 이 옵션을 선택하지 않으면 ASA에서는 연결 프로파일에 지정된 인증서 필드 값을 엔드포인트에서 연결 프로파일을 할당하는 데 사용하는 인증서 필드 값과 일치시킵니다.

클라이언트리스 SSL VPN 연결 프로파일, 기본 특성

Clientless SSL VPN Connection Profile(클라이언트리스 SSL VPN 연결 프로파일) > Advanced(고급) > Basic(기본) 대화 상자에서는 기본 특성을 설정합니다.

- Name(이름) - 연결 이름을 지정합니다. Edit(수정) 기능이 따로 있기 때문에 이 필드는 읽기 전용입니다.
- Aliases(별칭) - (선택 사항) 이 연결에 대한 대체 이름을 하나 이상 지정합니다. 별칭은 Clientless SSL VPN Access Connections(클라이언트리스 SSL VPN 액세스 연결) 대화 상자에서 해당 옵션을 구성한 경우 로그인 페이지에 표시됩니다.
- Authentication(인증) - 인증 매개변수를 지정합니다.
  - Method(방법) - AAA 인증, 인증서 인증 또는 두 가지 방법 모두 중에서 이 연결에 사용할 방법을 지정합니다. 기본값은 AAA 인증입니다.
  - AAA server Group(AAA 서버 그룹) - 이 연결을 인증하는 데 사용할 AAA 서버 그룹을 선택합니다. 기본값은 LOCAL입니다.
  - Manage(관리) - Configure AAA Server Groups(DNS 서버 그룹 구성) 대화 상자를 엽니다.
- DNS Server Group(DNS 서버 그룹) - 이 연결에 대한 DNS 서버 그룹으로 사용할 서버를 선택합니다. 기본값은 DefaultDNS입니다.
- Default Group Policy(기본 그룹 정책) - 이 연결에 사용할 기본 그룹 정책 매개변수를 지정합니다.
  - Group Policy(그룹 정책) - 이 연결에 사용할 기본 그룹 정책을 선택합니다. 기본값은 DfltGrpPolicy입니다.
  - Clientless SSL VPN Protocol(클라이언트리스 SSL VPN 프로토콜) - 이 연결에 대해 클라이언트리스 SSL VPN 프로토콜을 활성화하거나 비활성화합니다.

클라이언트리스 SSL VPN 연결 프로파일, 일반 특성

Clientless SSL VPN Connection Profile(클라이언트리스 **SSL VPN** 연결 프로필**) > Advanced(**고급**) > General(**일반**)** 대화 상자를 사용하여 영역 및 그룹을 사용자 이름에서 제거한 후 AAA 서버로 전달할지 여부를 지정하고 비밀번호 관리 옵션을 지정할 수 있습니다.

- **Password Management(**비밀번호 관리**)** - AAA 서버의 어카운트 비활성화 표시를 재정의하고 사용자에게 비밀번호 만료에 대해 알리는 것과 관련된 파라미터를 구성할 수 있습니다.
  - **Enable notification password management(**알림 비밀번호 관리 활성화**)** - 이 확인란을 선택하면 다음 두 가지 파라미터를 사용할 수 있습니다. 로그인 시 사용자에게 비밀번호 만료 시까지 남은 기간(일)을 알릴지 또는 비밀번호가 만료되는 날에만 알림을 보낼지 결정합니다. 비밀번호 만료 14일 전부터 알리기 시작하여 사용자가 비밀번호를 변경할 때까지 날마다 알리는 것이 기본값입니다. 범위는 1~180일입니다.

참고 비밀번호 만료까지 남은 일 수를 변경하는 옵션이 아니라 알림을 활성화하는 옵션입니다. 이 옵션을 선택할 경우 일 수도 지정해야 합니다.

어떤 옵션을 선택하든 사용자가 비밀번호를 변경하지 않고 비밀번호가 만료되면 ASA에서는 사용자에게 비밀번호를 변경할 수 있는 기회를 줍니다. 현재 비밀번호가 아직 만료되지 않은 경우, 사용자는 이 비밀번호를 사용하여 계속 로그인할 수 있습니다.

이 매개변수는 알림을 지원하는 AAA 서버, 다시 말해서 RADIUS, NT 서버가 포함된 RADIUS, LDAP 서버에 유효합니다. RADIUS 또는 LDAP 인증이 구성되어 있지 않으면 ASA는 이 명령을 무시합니다.

클라이언트리스 SSL VPN 연결 프로파일, 인증

Clientless SSL VPN Connection Profile(클라이언트리스 SSL VPN 연결 프로파일) > Advanced(고급) > Authentication(인증) 대화 상자에서는 인터페이스별 인증 서버 그룹을 확인, 추가, 수정 또는 삭제할 수 있습니다. 이 대화 상자의 각 테이블 행에는 하나의 인터페이스 관련 서버 그룹의 상태가 표시됩니다. 예를 들어 인터페이스 이름, 연계된 서버 그룹, 선택한 서버 그룹이 실패한 경우 로컬 데이터베이스로의 대체가 활성화되는지 여부 등이 표시됩니다.

Authentication(인증) 창의 필드는 AnyConnect 인증에 대한 필드와 동일하며, AnyConnect Connection Profile(AnyConnect 연결 프로파일), 인증 특성, 116 페이지에 설명되어 있습니다.

클라이언트리스 SSL VPN 연결 프로파일, 인증, 서버 그룹 추가

Clientless SSL VPN Connection Profile(클라이언트리스 SSL VPN 연결 프로파일) > Advanced(고급) > Authentication(인증) 대화 상자의 Add(추가) 버튼을 클릭하면 인터페이스를 AAA 서버 그룹과 연계할 수 있습니다.

이 구성을 수행하는 필드는 클라이언트리스 SSL VPN 연결 프로파일, 인터페이스에 권한 부여 서버 그룹 할당, 125 페이지에 설명되어 있습니다.

클라이언트리스 SSL VPN 연결 프로파일, 보조 인증

클라이언트리스 SSL에 대한 보조 인증 구성 필드는 AnyConnect 클라이언트 액세스에 대한 필드와 동일하며, 연결 프로파일, 보조 인증 특성, 118 페이지에 설명되어 있습니다.

클라이언트리스 SSL VPN 연결 프로파일, 권한 부여

클라이언트리스 SSL에 대한 권한 부여 구성 필드는 AnyConnect, IKEv1 및 IKEv2와 동일합니다. 이러한 필드에 대한 자세한 내용은 AnyConnect Connection Profile(AnyConnect 연결 프로파일), 권한 부여 특성, 121 페이지을 참조하십시오.

클라이언트리스 SSL VPN 연결 프로파일, NetBIOS 서버

Advanced(고급) > NetBIOS Servers(NetBIOS 서버) 대화 상자의 Clientless SSL VPN Connection Profile(클라이언트리스 SSL VPN 연결 프로파일)은 현재 구성된 NetBIOS 서버의 특성을 표시합니다. 클라이언트리스 SSL VPN 액세스에 대한 Add or Edit Tunnel Group(터널 그룹 추가 또는 수정) 대화 상자 > NetBIOS 대화 상자에서는 터널 그룹에 대한 NetBIOS 특성을 구성할 수 있습니다. 클라이언트리스

SSL VPN에서는 NetBIOS 및 CIFS(Common Internet File System) 프로토콜을 사용하여 원격 시스템에 있는 파일에 액세스하거나 공유합니다. 해당 컴퓨터 이름을 사용하여 Windows 컴퓨터에 파일 공유 연결을 시도할 경우 지정하는 파일 서버가 네트워크에서 리소스를 식별하는 특정 NetBIOS 이름과 일치합니다.

ASA는 IP 주소에 NetBIOS 이름을 매핑하기 위해 NetBIOS 이름 서버를 쿼리합니다. 클라이언트리스 SSL VPN에는 원격 시스템에 있는 파일에 액세스하거나 이 파일을 공유하기 위해 NetBIOS가 필요합니다.

NBNS 기능이 작동하려면 최소한 하나 이상의 NetBIOS 서버(호스트)를 구성해야 합니다. 이중화를 위해 최대 3개까지 NBNS 서버를 구성할 수 있습니다. ASA는 NetBIOS/CIFS 이름 확인을 위해 목록에서 첫 번째 서버를 사용합니다. 쿼리가 실패할 경우 다음 서버를 사용합니다.

NetBIOS Servers(NetBIOS 서버) 창의 필드

- IP Address(IP 주소) - 구성된 NetBIOS 서버의 IP 주소를 표시합니다.
- Master Browser(마스터 브라우저) - 서버가 WINS 서버인지 아니면 CIFS 서버(즉, 마스터 브라우저)일 수도 있는지 표시합니다.
- Timeout (seconds)(시간 제한(초)) - 서버가 다음 서버로 쿼리를 보내기 전에 NBNS 쿼리에 대한 응답을 기다릴 초기 시간(초)을 표시합니다.
- Retries(재시도) - 구성된 서버로의 NBNS 쿼리 전송을 순서대로 재시도할 횟수를 표시합니다. 즉, 이는 오류를 반환하기 전에 서버 목록을 순차적으로 시도할 횟수입니다. 최소 재시도 횟수는 0이고, 기본 재시도 횟수는 2입니다. 최대 재시도 횟수는 10입니다.
- Add/Edit(추가/수정) - NetBIOS 서버를 추가하려면 클릭합니다. 그러면 Add or Edit NetBIOS Server(NetBIOS 서버 추가 또는 수정) 대화 상자가 열립니다.
- Delete(삭제) - 목록에서 강조 표시된 NetBIOS 행을 제거합니다.
- Move Up/Move Down(위로 이동/아래로 이동) - ASA에서 이 상자에 표시된 순서대로 NetBIOS 서버에 NBNS 쿼리를 보냅니다. 이 상자를 통해 목록에서 위 또는 아래로 이동하여 서버의 우선순위를 변경할 수 있습니다.

클라이언트리스 SSL VPN 연결 프로필, 클라이언트리스 SSL VPN

Clientless Connect Profile(클라이언트리스 연결 프로필)의 **Advanced(고급) > Clientless SSL VPN(클라이언트리스 SSL VPN)** 창에서는 로그인 시 원격 사용자에게 표시되는 항목에 영향을 주는 속성을 구성할 수 있습니다.

이 대화 상자의 필드와 AnyConnect 연결 프로필은 동일합니다. 자세한 내용은 연결 프로파일, 그룹 별칭 및 그룹 URL, 126 페이지 섹션을 참고하십시오.

IKEv1 연결 프로파일

IKEv1 연결 프로파일은 L2TP-IPsec을 비롯한 네이티브 및 서드파티 VPN 클라이언트에 대한 인증 정책을 정의합니다. IKEv1 연결 프로필은 **Configuration(**구성**) > Remote Access VPN(**원격 액세스 **VPN) > Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**) > IPsec (IKEv1) Connection Profiles(IPsec(IKEv1)** 연결 프로필**)** 창에서 구성되었습니다.

- **Access Interfaces(**액세스 인터페이스**)** - IPsec 액세스에 사용할 인터페이스를 선택합니다. 기본값은 액세스 안 함입니다.
- **Connection Profiles(**연결 프로필**)** - 기존 IPsec 연결에 대해 구성된 파라미터를 테이블 형식으로 표시합니다. Connections(연결) 테이블에는 연결 정책을 결정하는 레코드가 포함되어 있습니다. 레코드는 연결에 대한 기본 그룹 정책을 식별하며, 프로토콜별 연결 매개변수를 포함합니다. 이 테이블에 포함된 열은 다음과 같습니다.
  - **Name(**이름**)** - IPsec IKEv1 연결의 이름 또는 IP 주소를 지정합니다.
  - **IPsec Enabled(IPsec** 활성화**)** - IPsec 프로토콜이 활성화되었는지 여부를 나타냅니다. Add or Edit IPsec Remote Access Connection, Basic(IPsec 원격 액세스 연결 추가 또는 수정, 기본) 대화 상자에서 이 프로토콜을 활성화할 수 있습니다.
  - **L2TP/IPsec Enabled(L2TP/IPsec** 활성화**)** - L2TP/IPsec 프로토콜이 활성화되었는지 여부를 나타냅니다. Add or Edit IPsec Remote Access Connection, Basic(IPsec 원격 액세스 연결 추가 또는 수정, 기본) 대화 상자에서 이 프로토콜을 활성화할 수 있습니다.
  - **Authentication Server Group(**인증 서버 그룹**)** - 인증을 제공할 수 있는 서버 그룹의 이름입니다.
  - **Group Policy(**그룹 정책**)** - 이 IPsec 연결에 적용되는 그룹 정책의 이름을 나타냅니다.

참고 Delete(삭제) - 선택한 서버 그룹을 테이블에서 제거합니다. 확인 또는 실행 취소가 없습니다.

IPsec 원격 액세스 연결 프로파일, 기본 탭

Configuration(구성**) > Remote Access VPN(**원격 액세스 **VPN) > Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**) > IPsec (IKEv1) Connection Profiles(IPsec(IKEv1)** 연결 프로필**) > Add/Edit(**추가/수정**) > Basic(**기본**)**의 Add or Edit IPsec Remote Access Connection Profile Basic(IPsec 원격 액세스 연결 프로필 추가 또는 수정 기본) 대화 상자에서는 L2TP-IPsec을 포함하여 IPsec IKEv1 VPN 연결에 대한 일반적인 속성을 구성할 수 있습니다.

- **Name(**이름**)** - 이 연결 프로필의 이름입니다.
- **IKE Peer Authentication(IKE** 피어 인증**)** - IKE 피어를 구성합니다.
  - **Pre-shared key(**사전 공유 키**)** - 연결에 대한 사전 공유 키 값을 지정합니다. 사전 공유 키의 최대 길이는 128자입니다.

- **Identity Certificate(ID 인증서)** - ID가 구성되고 등록된 경우 ID 인증서의 이름을 선택합니다. **Manage(관리)**는 선택한 인증서에 대한 세부사항을 추가, 수정, 삭제, 내보내기 및 표시할 수 있는 **Manage Identity Certificates(ID 인증서 관리)** 대화 상자를 엽니다.

- **User Authentication(사용자 인증)** - 사용자 인증에 사용할 서버에 대한 정보를 지정합니다. 추가 인증 정보는 Advanced(고급) 섹션에서 구성할 수 있습니다.
  - **Server Group(서버 그룹)** - 사용자 인증에 사용할 서버 그룹을 선택합니다. 기본값은 LOCAL입니다. LOCAL 이외의 다른 값을 선택하면 Fallback(대체) 확인란이 활성화됩니다. 서버 그룹을 추가하려면 **Manage(관리)** 버튼을 클릭합니다.
  - **Fallback(대체)** - 지정한 서버 그룹이 실패한 경우 사용자 인증에 LOCAL을 사용할지 여부를 지정합니다.

- **Client Address Assignment(클라이언트 주소 할당)** - 클라이언트 속성 할당과 관련된 속성을 지정합니다.
  - **DHCP Servers(DHCP 서버)** - 사용할 DHCP 서버의 IP 주소를 지정합니다. 공백으로 구분하여 최대 10개의 서버를 추가할 수 있습니다.
  - **Client Address Pools(클라이언트 주소 풀)** - 최대 6개의 사전 정의된 주소 풀을 지정합니다. 주소 풀을 정의하려면 **Select(선택)** 버튼을 클릭합니다.

- **Default Group Policy(기본 그룹 정책)** - 기본 그룹 정책과 관련된 속성을 지정합니다.
  - **Group Policy(그룹 정책)** - 이 연결에 사용할 기본 그룹 정책을 선택합니다. 기본값은 DfltGrpPolicy입니다. 이 그룹 정책과 연결할 새 그룹 정책을 정의하려면 **Manage**를 클릭합니다.
  - **Enable IPsec Protocol(IPsec 프로토콜 활성화)** 및 **Enable L2TP over IPsec protocol(L2TP over IPsec 프로토콜 활성화)** - 이 연결에 사용할 프로토콜을 선택합니다.

원격 액세스 연결 추가/수정, 고급, 일반

이 대화 상자를 사용하여 영역 및 그룹을 사용자 이름에서 제거한 후 AAA 서버로 전달할지 여부를 지정하고 비밀번호 관리 매개변수를 지정할 수 있습니다.

- **Strip the realm from username before passing it on to the AAA server(사용자 이름에서 영역을 제거한 후 AAA 서버로 전달)** - 사용자 이름에서 영역(관리 도메인)을 제거한 후 AAA 서버로 전달하는 기능을 활성화하거나 비활성화합니다. 인증하는 동안 사용자 이름의 영역 한정자를 제거하려면 Strip Realm(영역 제거) 확인란을 선택합니다. AAA의 사용자 이름에 영역 이름(인증, 권한 부여 및 어카운트 관리)을 추가할 수 있습니다. 영역에 유효한 구분 기호는 @ 문자뿐입니다. 형식은 username@realm입니다(예: JaneDoe@example.com). 이 Strip Realm(영역 제거) 확인란을 선택한 경우 사용자 이름만을 기반으로 인증이 수행됩니다. 그렇지 않으면 전체 username@realm 문자열을 기반으로 인증이 수행됩니다. 서버에서 구분 기호를 구문 분석할 수 없는 경우 이 상자를 선택해야 합니다.

참고 영역과 그룹을 둘 다 사용자 이름에 추가할 수 있습니다. 이 경우 ASA에서는 그룹에 대해 구성된 파라미터 및 영역에 대해 구성된 파라미터를 모두 AAA 기능에 사용합니다. 이 옵션의 형식은 username[@realm]]<#or!>group] 입니다(예: JaneDoe@example.com#VPNGroup). 이 옵션을 선택하면 # 또는 !를 그룹 구분 기호로 사용해야 합니다. @ 문자가 영역 구분 기호로도 제공된 경우에는 ASA에서 @ 문자를 그룹 구분 기호로 해석할 수 없기 때문입니다.

Kerberos 영역은 특수한 경우입니다. Kerberos 영역의 명명 규칙에서는 Kerberos 영역의 호스트와 연계된 DNS 도메인 이름을 대문자로 표시합니다. 예를 들어 사용자가 example.com 도메인에 있는 경우 Kerberos 영역 EXAMPLE.COM을 호출할 수 있습니다.

ASA에서는 user@grouppolicy를 지원하지 않습니다. L2TP/IPsec 클라이언트는 user@tunnelgroup을 통한 터널 전환만 지원합니다.

- **Strip the group from the username before passing it on to the AAA server(**사용자 이름에서 그룹을 제거한 후 **AAA** 서버로 전달**)** - 사용자 이름에서 그룹 이름을 제거한 후 AAA 서버로 사용자 이름을 전달하는 기능을 활성화하거나 비활성화합니다. 인증하는 동안 사용자 이름에서 그룹 이름을 제거하려면 Strip Group(그룹 제거)을 선택합니다. 이 옵션은 Enable Group Lookup(그룹 조회 활성화) 확인란도 선택한 경우에만 유효합니다. 구분 기호를 사용하여 사용자 이름에 그룹 이름을 추가하고 그룹 조회를 활성화한 경우 ASA에서는 구분 기호 왼쪽에 있는 모든 문자를 사용자 이름으로 해석하고 오른쪽에 있는 모든 문자를 그룹 이름으로 해석합니다. 유효한 그룹 구분 기호는 @, #, ! 문자이며, 그룹 조회의 기본값은 @ 문자입니다. 사용자 이름에 그룹을 추가할 때는 username<delimiter>group 형식을 사용합니다(예: JaneDoe@VPNGroup, JaneDoe#VPNGroup, JaneDoe!VPNGroup).
- **Password Management(**비밀번호 관리**)** - AAA 서버의 어카운트 비활성화 표시를 재정의하고 사용자에게 비밀번호 만료에 대해 알리는 것과 관련된 파라미터를 구성할 수 있습니다.
  - **Enable notification upon password expiration to allow user to change password(**비밀번호 만료 시 사용자가 비밀번호를 변경할 수 있도록 알림 활성화**)** - 이 체크 박스를 선택하면 다음 두 파라미터를 사용할 수 있습니다. 로그인 시 사용자에게 비밀번호 만료 시까지 남은 기간(일)을 알릴지 또는 비밀번호가 만료되는 날에만 알림을 보낼지 결정할 수 있습니다. 비밀번호 만료 14일 전부터 알리기 시작하여 사용자가 비밀번호를 변경할 때까지 날마다 알리는 것이 기본값입니다. 범위는 1~180일입니다.

참고 비밀번호 만료까지 남은 일 수를 변경하는 옵션이 아니라 알림을 활성화하는 옵션입니다. 이 옵션을 선택할 경우 일 수도 지정해야 합니다.

어떤 옵션을 선택하든 사용자가 비밀번호를 변경하지 않고 비밀번호가 만료되면 ASA에서는 사용자에게 비밀번호를 변경할 수 있는 기회를 줍니다. 현재 비밀번호가 아직 만료되지 않은 경우, 사용자는 이 비밀번호를 사용하여 계속 로그인할 수 있습니다.

이 매개변수는 알림을 지원하는 AAA 서버, 다시 말해서 RADIUS, NT 서버가 포함된 RADIUS, LDAP 서버에 유효합니다. RADIUS 또는 LDAP 인증이 구성되어 있지 않으면 ASA는 이 명령을 무시합니다.

이 기능을 사용하려면 MS-CHAPv2를 사용해야 합니다.

IKEv1 클라이언트 주소 지정

클라이언트 주소 지정 구성은 클라이언트 연결 프로파일에 공통적으로 적용됩니다. 자세한 내용은 연결 프로파일, 클라이언트 주소 지정, 114 페이지를 참조하십시오.

IKEv1 연결 프로파일, 인증

이 대화 상자는 원격 액세스 및 사이트 대 사이트 터널 그룹의 IPsec에 사용할 수 있습니다. 이 대화 상자의 설정은 ASA의 이 연결 프로필(터널 그룹)에 전역적으로 적용됩니다. 인터페이스별 인증 서버 그룹 설정을 지정하려면 **Advanced(고급)**를 클릭합니다. 이 대화 상자를 사용하여 다음 특성을 구성할 수 있습니다.

- **Authentication Server Group(인증 서버 그룹)** - LOCAL 그룹(기본값)을 포함하여 사용 가능한 인증 서버 그룹을 나열합니다. None(없음)을 선택할 수도 있습니다. None(없음) 또는 Local(로컬) 이외의 옵션을 선택하면 Use Local if Server Group Fails(서버 그룹이 실패할 경우 로컬 사용) 확인란이 활성화됩니다.
- **Use LOCAL if Server Group Fails(서버 그룹이 실패할 경우 로컬 사용)** - 인증 서버 그룹 속성에 지정된 그룹이 실패한 경우 LOCAL 데이터베이스로의 대체를 활성화하거나 비활성화합니다.

  Enable Group Lookup(그룹 조회 활성화) 상자의 선택을 취소하여 사용자 이름만을 기반으로 하는 인증을 구성할 수 있습니다. Enable Group Lookup(그룹 조회 활성화) 상자와 Strip Group(그룹 제거)을 둘 다 선택하면 AAA 서버에 추가된 그룹 이름을 가진 사용자의 데이터베이스를 유지 관리하고, 이와 동시에 해당 사용자 이름만으로 사용자를 인증할 수 있습니다.

IKEv1 연결 프로파일, 권한 부여

권한 부여 구성은 클라이언트 연결 프로파일에 공통적으로 적용됩니다. 자세한 내용은 AnyConnect Connection Profile(AnyConnect 연결 프로파일), 인증 특성, 116 페이지를 참조하십시오.

IKEv1 연결 프로파일, 어카운트 관리

어카운트 관리 구성은 클라이언트 연결 프로파일에 공통적으로 적용됩니다. 자세한 내용은 연결 프로파일, 어카운트 관리, 126 페이지를 참조하십시오.

IPsec IKEv1 연결 프로파일, IPSec

Configuration(구성**) > Remote Access VPN(**원격 액세스 **VPN) > Network (Client) Access(**네트워크(클라이언트) 액세스**) > IPsec (IKEv1) Connection Profiles(IPsec(IKEv1)** 연결 프로필**) > Add/Edit(**추가/수정**) > Advanced(**고급**) > IPsec**

- **Send certificate chain(**인증서 체인 보내기**)** - 전체 인증서 체인 보내기를 활성화하거나 비활성화합니다. 이 작업은 전송 시 루트 인증서 및 하위 CA 인증서를 포함합니다.
- **IKE Peer ID Validation(IKE** 피어 **ID** 검증**)** - IKE 피어 ID 검증을 무시할지, 필수로 지정할지 또는 인증서에서 지원하는 경우에만 확인할지 선택합니다.
- **IKE Keep Alive(IKE** 킵얼라이브**)** - ISAKMP keep alive 모니터링을 활성화하고 구성합니다.
  - **Disable Keep Alives(keep alive** 비활성화**)** - ISAKMP keep alive를 활성화하거나 비활성화합니다.
  - **Monitor Keep Alives(keep alive** 모니터링**)** - ISAKMP keep alive 모니터링을 활성화하거나 비활성화합니다. 이 옵션을 선택하면 Confidence Interval(신뢰 구간) 및 Retry Interval(재시도 간격) 필드가 활성화됩니다.
  - **Confidence Interval(**신뢰 구간**)** - ISAKMP keep alive 신뢰 구간을 지정합니다. 이것은 ASA에서 keep alive 모니터링을 시작하기 전에 피어가 유휴 상태에 있도록 허용해야 하는 시간(초)입니다. 최소값은 10초이고, 최대값은 300초입니다. 원격 액세스 그룹의 기본값은 300초입니다.
  - **Retry Interval(**재시도 간격**)** - ISAKMP keep alive 재시도 간에 대기할 시간(초)을 지정합니다. 기본값은 2초입니다.
  - **Head end will never initiate keepalive monitoring(**헤드엔드에서 **keep alive** 모니터링을 시작하지 않음**)** - 중앙 사이트 ASA에서 keepalive 모니터링을 시작하지 않도록 지정합니다.

IKEv1 연결 프로필, IPsec, IKE 인증

Configuration(구성**) > Remote Access VPN(**원격 액세스 **VPN) > Network (Client) Access(**네트워크(클라이언트) 액세스**) > IPsec (IKEv1) Connection Profiles(IPsec(IKEv1)** 연결 프로필**) > Add/Edit(**추가/수정**) > Advanced(**고급**) > IPsec > IKE Authentication(IKE** 인증**)**

- **Default Mode(**기본 모드**)** - 기본 인증 모드(none(없음), xauth 또는 hybrid(하이브리드))를 위와 같이 선택할 수 있습니다.
- **Interface-Specific Authentication Mode(**인터페이스별 인증 모드**)** - 인터페이스별로 인증 모드를 지정합니다.
  - **Add/Edit/Delete(**추가/수정/삭제**)** - 선택한 인터페이스/인증 모드 쌍을 Interface/Authentication Mode(인터페이스/인증 모드) 테이블에서 추가/수정/삭제합니다.
  - **Interface(**인터페이스**)** - 명명된 인터페이스를 선택합니다. 기본 인터페이스는 내부와 외부이지만 다른 인터페이스 이름을 구성한 경우 해당 이름도 목록에 표시됩니다.

- **Authentication Mode(**인증 모드**)** - 인증 모드(none(없음), xauth 또는 hybrid(하이브리드))를 위와 같이 선택할 수 있습니다.

IKEv1 연결 프로필, IPsec, 클라이언트 소프트웨어 업데이트

Configuration(구성**) > Remote Access VPN(**원격 액세스 **VPN) > Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**) > IPsec (IKEv1) Connection Profiles(IPsec(IKEv1)** 연결 프로필**) > Add/Edit(**추가/수정**) > Advanced(**고급**) > IPsec > Client Software Update(**클라이언트 소프트웨어 업데이트**)**

Client VPN Software Update(클라이언트 **VPN** 소프트웨어 업데이트**)** 테이블 - 클라이언트 유형, VPN 클라이언트 수정 버전 및 설치된 각 클라이언트 VPN 소프트웨어 패키지의 이미지 URL를 나열합니다. 각 클라이언트 유형에 대해, 허용되는 클라이언트 소프트웨어 수정 버전과 필요한 경우 소프트웨어 업그레이드를 다운로드할 URL 또는 IP 주소를 지정할 수 있습니다. 클라이언트 업데이트 메커니즘(자세한 내용은 Client Update(클라이언트 업데이트) 대화 상자에 대한 설명 참조)에서는 이 정보를 사용하여 각 VPN 클라이언트에서 실행 중인 소프트웨어가 적절한 수준의 수정 버전인지 확인하고, 필요한 경우 오래된 소프트웨어를 실행하는 클라이언트에 알림 메시지 및 업데이트 메커니즘을 제공합니다.

- **Client Type(**클라이언트 유형**)** - VPN 클라이언트 유형을 식별합니다.
- **VPN Client Revisions(VPN** 클라이언트 수정 버전**)** - 허용되는 수준의 VPN 클라이언트 수정 버전을 지정합니다.
- **Location URL(**위치 **URL)** - 올바른 VPN 클라이언트 소프트웨어 이미지를 다운로드할 수 있는 URL 또는 IP 주소를 지정합니다. 대화 상자 기반 VPN 클라이언트의 경우 URL은 http:// 또는 https:// 형식이어야 합니다. 클라이언트 모드의 ASA 5505의 경우 URL은 tftp:// 형식이어야 합니다.

IKEv1 연결 프로파일, PPP

이 IKEv1 연결 프로필을 사용하여 PPP 연결에 허용되는 인증 프로토콜을 구성하려면 **Configuration(**구성**) > Remote Access VPN(**원격 액세스 **VPN) > Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**) > IPsec(IKEv1) Connection Profiles(IPsec(IKEv1)** 연결 프로필**) > Add/Edit(**추가/수정**) > Advanced(**고급**) > PPP**를 엽니다.

이 대화 상자는 IPsec IKEv1 원격 액세스 연결 프로파일에만 적용됩니다.

- **CHAP** - PPP 연결에 CHAP 프로토콜을 사용합니다.
- **MS-CHAP-V1** - PPP 연결에 MS-CHAP-V1 프로토콜을 사용합니다.
- **MS-CHAP-V2** - PPP 연결에 MS-CHAP-V2 프로토콜을 사용합니다.
- **PAP** - PPP 연결에 PAP 프로토콜을 사용합니다.
- **EAP-PROXY** - PPP 연결에 EAP-PROXY 프로토콜을 사용합니다. EAP는 확장 가능 인증 프로토콜(Extensible Authentication Protocol)을 의미합니다.

IKEv2 연결 프로파일

IKEv2 연결 프로파일은 AnyConnect VPN 클라이언트에 대한 EAP, 인증서 기반 및 사전 공유 키 기반 인증을 정의합니다. ASDM의 구성 패널은 **Configuration(**구성**) > Remote Access VPN(**원격 액세스 **VPN) > Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**) > IPsec(IKEv2) Connection Profiles(IPsec(IKEv2)** 연결 프로파일**)**입니다.

- Access Interfaces(액세스 인터페이스) - IPsec 액세스에 사용할 인터페이스를 선택합니다. 기본적으로 액세스 안 함이 선택되어 있습니다.
- Bypass interface access lists for inbound VPN sessions(인바운드 VPN 세션에 대한 인터페이스 액세스 목록 우회) - 인바운드 VPN 세션에 대한 인터페이스 액세스 목록을 우회하려면 이 확인란을 선택합니다. 그룹 정책 및 사용자 정책에 대한 액세스 목록은 항상 모든 트래픽에 적용됩니다.
- Connection Profiles(연결 프로파일) - 기존 IPsec 연결에 대해 구성된 매개변수를 테이블 형식으로 표시합니다. Connection Profiles(연결 프로파일) 테이블에는 연결 정책을 결정하는 레코드가 포함되어 있습니다. 레코드는 연결에 대한 기본 그룹 정책을 식별하며, 프로토콜별 연결 매개변수를 포함합니다. 이 테이블에 포함된 열은 다음과 같습니다.
  - Name(이름) - IPsec 연결의 이름 또는 IP 주소를 지정합니다.
  - IKEv2 Enabled(IKEv2 활성화) - 선택한 경우 IKEv2 프로토콜이 활성화되도록 지정합니다.
  - Authentication Server Group(인증 서버 그룹) - 인증에 사용되는 서버 그룹의 이름을 지정합니다.
  - Group Policy(그룹 정책) - 이 IPsec 연결에 적용되는 그룹 정책의 이름을 나타냅니다.

참고 Delete(삭제) - 선택한 서버 그룹을 테이블에서 제거합니다. 확인 또는 실행 취소가 없습니다.

IPsec IKEv2 연결 프로파일, 기본 탭

Add or Edit IPsec Remote Access Connection Profile Basic(IPsec 원격 액세스 연결 프로파일 추가 또는 수정 기본) 대화 상자에서는 IPsec IKEv2 연결의 일반적인 특성을 구성합니다.

- **Name(**이름**)** - 연결 이름을 식별합니다.
- **IKE Peer Authentication(IKE** 피어 인증**)** - IKE 피어를 구성합니다.
  - **Pre-shared key(**사전 공유 키**)** - 연결에 대한 사전 공유 키 값을 지정합니다. 사전 공유 키의 최대 길이는 128자입니다.
  - **Enable Certificate Authentication(**인증서 인증 활성화**)** - 선택한 경우 인증서를 사용하여 인증할 수 있습니다.

- **Enable peer authentication using EAP(EAP**를 사용한 피어 인증 활성화**)** - 선택한 경우 EAP를 사용하여 인증할 수 있습니다. 이 확인란을 선택한 경우 로컬 인증에 인증서를 사용해야 합니다.
- **Send an EAP identity request to the client(**클라이언트로 **EAP ID** 요청 전송**)** - 인증을 위한 EAP 요청을 원격 액세스 VPN 클라이언트로 전송할 수 있습니다.

- **Mobike RRC** - Mobike RRC를 활성화/비활성화합니다.
  - **Enable Return Routability Check for mobike(Mobike**에 대한 반환 라우팅 가능성 확인 활성화**)** — mobike가 활성화되어 있는 IKE/IPSEC 보안 연결에서 동적 IP 주소 변경 사항에 대한 반환 라우팅 가능성 확인을 활성화/비활성화합니다.

- **User Authentication(**사용자 인증**)** - 사용자 인증에 사용할 서버에 대한 정보를 지정합니다. 추가 인증 정보는 Advanced(고급) 섹션에서 구성할 수 있습니다.
  - **Server Group(**서버 그룹**)** - 사용자 인증에 사용할 서버 그룹을 선택합니다. 기본값은 LOCAL(로컬)입니다. LOCAL(로컬) 이외의 다른 값을 선택하면 Fallback(대체) 확인란이 활성화됩니다.
  - **Manage(**관리**)** - Configure AAA Server Groups(DNS 서버 그룹 구성) 대화 상자를 엽니다.
  - **Fallback(**대체**)** - 지정한 서버 그룹이 실패한 경우 사용자 인증에 LOCAL을 사용할지 여부를 지정합니다.

- **Client Address Assignment(**클라이언트 주소 할당**)** - 클라이언트 속성 할당과 관련된 속성을 지정합니다.
  - **DHCP Servers(DHCP** 서버**)** - 사용할 DHCP 서버의 IP 주소를 지정합니다. 공백으로 구분하여 최대 10개의 서버를 추가할 수 있습니다.
  - **Client Address Pools(**클라이언트 주소 풀**)** - 최대 6개의 사전 정의된 주소 풀을 지정합니다. Select(선택)를 클릭하여 Address Pools(주소 풀) 대화 상자를 엽니다.

- **Default Group Policy(**기본 그룹 정책**)** - 기본 그룹 정책과 관련된 속성을 지정합니다.
  - **Group Policy(**그룹 정책**)** - 이 연결에 사용할 기본 그룹 정책을 선택합니다. 기본값은 DfltGrpPolicy입니다.
  - **Manage(**관리**)** - 그룹 정책을 추가, 수정 또는 삭제할 수 있는 Configure Group Policies(그룹 정책 구성) 대화 상자를 엽니다.
  - **Client Protocols(**클라이언트 프로토콜**)** - 이 연결에 사용할 프로토콜을 선택합니다. 기본적으로 IPsec과 L2TP over IPsec이 둘 다 선택됩니다.
  - **Enable IKEv2 Protocol(IKEv2** 프로토콜 활성화**)** - 원격 액세스 연결 프로필에 사용할 IKEv2 프로토콜을 활성화합니다. 이는 방금 선택한 그룹 정책의 특성입니다.

IPsec Remote Access Connection Profile - Advanced(IPsec 원격 액세스 연결 프로파일 - 고급), IPsec 탭

IPsec (IKEv2) Connection Profiles(IPsec(IKEv2) 연결 프로파일)의 IPsec 테이블에는 다음과 같은 필드가 포함됩니다.

- Send certificate chain(인증서 체인 보내기) - 전체 인증서 체인 보내기를 활성화하거나 비활성화하려면 선택합니다. 이 작업은 전송 시 루트 인증서 및 하위 CA 인증서를 포함합니다.
- IKE Peer ID Validation(IKE 피어 ID 검증) - 드롭다운 목록에서 IKE 피어 ID 검증을 무시할지, 필수로 지정할지 또는 인증서에서 지원하는 경우에 확인할지 선택합니다.

IPsec 또는 SSL VPN 연결 프로파일에 인증서 매핑

ASA에서는 클라이언트 인증서 인증이 포함된 IPsec 연결 요청을 받은 경우 구성된 정책에 따라 해당 연결에 연결 프로필을 할당합니다. 이 정책에서는 구성된 규칙, 인증서 OU 필드, IKE ID(예: 호스트 이름, IP 주소, 키 ID), 피어 IP 주소 또는 기본 연결 프로파일을 사용할 수 있습니다. SSL 연결의 경우 ASA에서는 구성된 규칙만 사용합니다.

규칙을 사용하는 IPsec 또는 SSL 연결에 대해 ASA에서는 일치하는 항목을 찾을 때까지 규칙을 기준으로 인증서의 속성을 평가합니다. 일치하는 항목을 찾은 경우 일치하는 규칙과 연계된 연결 프로파일을 연결에 할당합니다. 일치하는 항목을 찾지 못한 경우 기본 연결 프로파일(IPsec의 경우 DefaultRAGroup, SSL VPN의 경우 DefaultWEBVPNGroup)을 연결에 할당하고, 사용자가 포털 페이지에 표시된 드롭다운 목록에서 연결 프로파일을 선택할 수 있도록 합니다(활성화된 경우). 이 연결 프로파일에서 한 번 시도한 연결의 결과는 인증서가 유효한지 여부 및 연결 프로파일의 인증 설정에 따라 결정됩니다.

인증서 그룹 일치 정책은 인증서 사용자의 권한 그룹을 식별하는 데 사용할 방법을 정의합니다.

Policy(정책) 창에서 일치하는 정책을 구성합니다. 구성한 규칙을 사용하도록 선택한 경우 Rules(규칙)로 이동하여 규칙을 지정합니다.

Certificate to Connection Profile Maps(인증서-연결 프로파일 맵), Policy(정책)

IPsec 연결의 경우 인증서 그룹 일치 정책은 인증서 사용자의 권한 그룹을 식별하는 데 사용할 방법을 정의합니다. 이러한 정책에 대한 설정은 **Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > Network (Client) Access(네트워크(클라이언트) 액세스) > Advanced(고급) > IPsec > Certificate to Connection Profile Maps(인증서-연결 프로필 맵) > Policy(정책)**에서 구성됩니다.

- **Use the configured rules to match a certificate to a group(구성된 규칙을 사용하여 그룹에 인증서 일치)** - Rules(규칙)에서 정의한 규칙을 사용할 수 있습니다.

- **Use the certificate OU field to determine the group(**인증서 **OU** 필드를 사용하여 그룹 결정**)** - 조직 구성 단위 필드를 사용하여 인증서와 일치시킬 그룹을 결정할 수 있습니다. 이 옵션은 기본적으로 선택되어 있습니다.
- **Use the IKE identity to determine the group(IKE ID**를 사용하여 그룹 결정**)** - 이전에 **Configuration(**구성**) > Remote Access VPN(**원격 액세스 **VPN) > Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**) > Advanced(**고급**) > IPsec > IKE Parameters(IKE** 파라미터**)**에서 정의한 ID를 사용할 수 있습니다. IKE ID는 호스트 이름, IP 주소, 키 ID 또는 자동일 수 있습니다.
- **Use the peer IP address to determine the group(**피어 **IP** 주소를 사용하여 그룹 결정**)** - 피어의 IP 주소를 사용할 수 있습니다. 이 옵션은 기본적으로 선택되어 있습니다.
- **Default to Connection Profile(**연결 프로필의 기본값**)** - 위 방법으로 일치하는 항목을 찾지 못한 경우에 사용할 기본 인증서 사용자 그룹을 선택할 수 있습니다. 이 옵션은 기본적으로 선택되어 있습니다. Default to group(기본 그룹 설정) 목록에서 기본 그룹을 클릭합니다. 해당 그룹이 구성에 이미 있어야 합니다. 그룹이 목록에 없는 경우에는 **Configuration(**구성**) > Remote Access VPN(**원격 액세스 **VPN) > Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**) > Group Policies(**그룹 정책**)**를 사용하여 정의해야 합니다.

Certificate to Connection Profile Maps(인증서-연결 프로파일 맵), Rules(규칙)

IPsec 연결의 경우 인증서 그룹 일치 정책은 인증서 사용자의 권한 그룹을 식별하는 데 사용할 방법을 정의합니다. 프로필 맵은 **Configuration(**구성**) > Remote Access VPN(**원격 액세스 **VPN) > Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**) > Advanced(**고급**) > IPsec > Certificate to Connection Profile Maps(**인증서-연결 프로필 맵**) > Rules(**규칙**)**에서 생성됩니다.

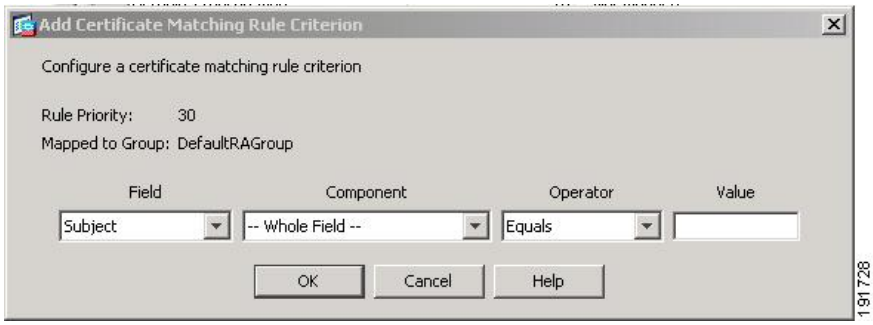
이 창에는 인증서-연결 프로파일 맵의 목록 및 매핑 조건이 포함됩니다.

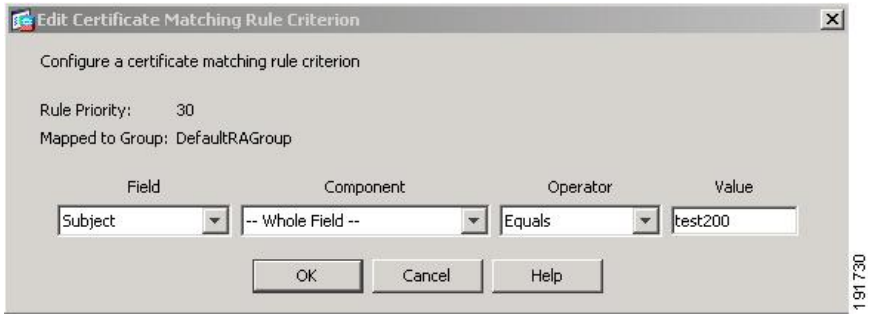
인증서-연결 프로파일 맵, 인증서 일치 규칙 조건 추가

연결 프로파일을 매핑 규칙에 매핑할 매핑 프로파일을 생성합니다.

- Map(맵) - 다음 중 하나를 선택합니다.
  - Existing(기존) - 규칙을 포함할 맵 이름을 선택합니다.
  - New(신규) - 규칙의 새 맵 이름을 입력합니다.
- Priority(우선순위) - ASA에서 연결 요청을 받은 경우 맵을 평가할 순서를 지정하는 숫자를 입력합니다. 정의된 첫 번째 규칙의 경우 기본 우선순위는 10입니다. ASA에서는 먼저 우선순위가 가장 낮은 맵에 대해 각 연결을 평가합니다.
- Mapped to Connection Profile(연결 프로파일에 매핑됨) - 이 규칙에 매핑할 연결 프로파일(이전의 "터널 그룹")을 선택합니다.

맵에 규칙 조건을 할당하지 않으면 다음 섹션에 설명된 대로 ASA에서 맵 항목을 무시합니다.





인증서 일치 규칙 조건 추가/수정

이 대화 상자를 사용하여 연결 프로파일에 매핑할 수 있는 인증서 일치 규칙 조건을 구성합니다.

- Rule Priority(규칙 우선순위) - (표시 전용) ASA에서 연결 요청을 받은 경우 맵을 평가할 순서입니다. ASA에서는 먼저 우선순위가 가장 낮은 맵에 대해 각 연결을 평가합니다.
- Mapped to Group(그룹에 매핑됨) - (표시 전용) 규칙을 할당할 연결 프로파일입니다.
- Field(필드) - 드롭다운 목록에서 평가할 인증서 부분을 선택합니다.
  - Subject(주체) - 인증서를 사용하는 사람 또는 시스템입니다. CA 루트 인증서의 경우 Subject(주체)와 Issuer(발급자)가 같습니다.
  - Alternative Subject(대체 주체) - 주체 대체 이름 확장을 통해 추가 ID를 인증서 주체에 바인딩할 수 있습니다.
  - Issuer(발급자) - 인증서를 발급한 CA 또는 기타 실체(관할권)입니다.
  - Extended Key Usage(확장 키 사용) - 일치시키도록 선택할 수 있는 추가 조건을 제공하는 클라이언트 인증서의 확장입니다.
- Component(구성 요소) - (Subject of Issuer(발급자 주체)를 선택한 경우에만 해당됩니다.) 규칙에 사용된 고유한 이름 구성 요소를 선택합니다.

DN 필드	정의
Whole Field(전체 필드**)**	전체 DN입니다.

DN 필드	정의
Country(국가) (C)	2자로 된 국가 약어입니다. 이러한 코드는 ISO 3166 국가 약어를 따릅니다.
Common Name(공통 이름) (CN)	사람, 시스템 또는 기타 실체의 이름입니다. 이는 식별 계층에서 최하위(가장 구체적) 수준에 속합니다.
DN Qualifier(DN 한정자) (DNQ)	특정 DN 특성입니다.
E-mail Address(이메일 주소) (EA)	인증서를 소유한 사람, 시스템 또는 실체의 이메일 주소입니다.
Generational Qualifier(세대 한정자) (GENQ)	Jr., Sr., III 등의 세대 한정자입니다.
Given Name(이름) (GN)	인증서 소유자의 성을 제외한 이름입니다.
Initials(이니셜) (I)	인증서 소유자의 이름 각 부분의 첫 글자입니다.
Locality(구/군/시) (L)	조직이 있는 구/군/시입니다.
Name(이름) (N)	인증서 소유자의 이름입니다.
Organization (O)(O(조직))	회사, 기관, 에이전시, 협회 또는 기타 실체의 이름입니다.
Organizational Unit (OU)(OU(조직 단위))	조직 내의 하위 그룹입니다.
Serial Number(일련 번호) (SER)	인증서의 일련 번호입니다.
Surname(성) (SN)	인증서 소유자의 성입니다.
State/Province(주/도) (S/P)	조직이 있는 주/도입니다.
Title(직함) (T)	인증서 소유자의 직함입니다(예: Dr.)
User ID(사용자 ID) (UID)	인증서 소유자의 식별 번호입니다.
Unstructured Name(구조화되지 않은 이름) (UNAME)	unstructuredName 특성 유형은 주체의 이름을 구조화되지 않은 ASCII 문자열로 지정합니다.
IP Address(IP 주소) (IP)	IP 주소 필드입니다.

- Operator(연산자) - 규칙에서 사용되는 연산자를 선택합니다.
  - Equals(같음) - 고유 이름 필드가 값과 정확히 일치해야 합니다.
  - Contains(포함) - 고유 이름 필드에 값이 포함되어야 합니다.
  - Does Not Equal(같지 않음) - 고유 이름 필드가 값과 일치하지 않아야 합니다.

- Does Not Contain(포함 안 함) - 고유 이름 필드에 값이 포함되지 않아야 합니다.

- Value(값) - 최대 255자를 입력하여 연산자 개체를 지정합니다. Extended Key Usage(확장 키 사용)의 경우 드롭다운 목록에서 사전 정의된 값 중 하나를 선택하고, 다른 확장의 경우 OID를 입력할 수 있습니다. 사전 정의된 값은 다음과 같습니다.

선택	키 사용 목적	**OID** 문자열
clientauth	클라이언트 인증	**1.3.6.1.5.5.7.3.2**
codesigning	코드 서명	1.3.6.1.5.5.7.3.3
emailProtection	보안 이메일 보호	1.3.6.1.5.5.7.3.4
ocspsigning	OCSP 서명	1.3.6.1.5.5.7.3.9
serverauth	서버 인증	1.3.6.1.5.5.7.3.1
timestamping	타임스탬프	1.3.6.1.5.5.7.3.8

사이트 대 사이트 연결 프로파일

Connection Profiles(연결 프로파일) 대화 상자에 현재 구성된 사이트 대 사이트 연결 프로파일(터널 그룹)이 표시되며, 연결 프로파일 이름을 구문 분석할 때 사용할 구분 기호를 선택하고, 연결 프로파일을 추가, 수정 또는 삭제할 수 있습니다.

ASA에서는 내부 및 외부 IP 헤더를 사용하는 네트워크 내부 및 외부 모두에서 IKEv1 또는 IKEv2를 사용하는 IPv4 또는 IPv6 대해 IPsec LAN-to-LAN VPN 연결을 지원합니다.

Site-to-Site Connection Profile(사이트 대 사이트 연결 프로파일**)** 창의 필드

- Access Interfaces(액세스 인터페이스) - 인터페이스의 원격 피어 디바이스에서 액세스하도록 설정할 수 있는 디바이스 인터페이스 테이블을 표시합니다.
  - Interface(인터페이스) - 액세스를 활성화하거나 비활성화할 디바이스 인터페이스입니다.
  - Allow IKEv1 Access(IKEv1 액세스 허용) - 피어 디바이스에서의 IPsec IKEv1 액세스를 활성화하려면 선택합니다.
  - Allow IKEv2 Access(IKEv2 액세스 허용) - 피어 디바이스에서의 IPsec IKEv2 액세스를 활성화하려면 선택합니다.

- Connection Profiles(연결 프로파일) - 프로파일을 추가, 수정 또는 삭제할 수 있는 연결 프로파일 테이블을 표시합니다.
  - Add(추가) - Add IPsec Site-to-Site connection profile(IPsec 사이트 대 사이트 연결 프로파일 추가) 대화 상자를 엽니다.

- Edit(추가) - Edit IPsec Site-to-Site connection profile(IPsec 사이트 대 사이트 연결 프로파일 수정) 대화 상자를 엽니다.
- Delete(삭제) - 선택한 연결 프로파일을 제거합니다. 확인 또는 실행 취소가 없습니다.
- Name(이름) - 연결 프로파일의 이름입니다.
- Interface(인터페이스) - 연결 프로파일이 활성화된 인터페이스입니다.
- Local Network(로컬 네트워크) - 로컬 네트워크의 IP 주소를 지정합니다.
- Remote Network(원격 네트워크) - 원격 네트워크의 IP 주소를 지정합니다.
- IKEv1 Enabled(IKEv1 활성화) - 연결 프로파일에 대해 활성화된 IKEv1을 표시합니다.
- IKEv2 Enabled(IKEv2 활성화) - 연결 프로파일에 대해 활성화된 IKEv2를 표시합니다.
- Group Policy(그룹 정책) - 연결 프로파일의 기본 그룹 정책을 표시합니다.

사이트 대 사이트 연결 프로필, 추가 또는 수정

Add or Edit IPsec Site-to-Site Connection(IPsec 사이트 대 사이트 연결 추가 또는 수정) 대화 상자에서는 IPsec 사이트 대 사이트 연결을 만들거나 수정할 수 있습니다. 이 대화 상자에서는 피어 IP 주소(IPv4 또는 IPv6)를 지정하고, 연결 이름을 지정하고, 인터페이스를 선택하고, IKEv1/IKEv2 피어 및 사용자 인증 매개변수를 지정하고, 보호된 네트워크를 지정하고, 암호화 알고리즘을 지정할 수 있습니다.

ASA는 두 개의 피어에 IPv4 내부 및 외부 네트워크(내부 및 외부 인터페이스의 IPv4 주소)가 있는 경우, Cisco 또는 서드파티 피어에 대한 LAN-to-LAN VPN 연결을 지원합니다.

IPv4 및 IPv6 혼합 주소 지정을 사용하거나 모두 IPv6 주소 지정을 사용하는 LAN-to-LAN 연결의 경우, 보안 어플라이언스는 두 피어 모두에 Cisco ASA 5500 시리즈 보안 어플라이언스가 있고 두 내부 네트워크 모두에 일치하는 주소 지정 체계(둘 다 IPv4 또는 IPv6)가 있는 경우 VPN 터널을 지원합니다.

특히 두 피어 모두 Cisco ASA 5500 시리즈인 경우 다음 토폴로지가 지원됩니다.

- ASA에 IPv4 내부 네트워크가 있으며 외부 네트워크는 IPv6입니다(내부 인터페이스의 IPv4 주소 및 외부 인터페이스의 IPv6 주소).
- ASA에 IPv6 내부 네트워크가 있으며 외부 네트워크는 IPv4입니다(내부 인터페이스의 IPv6 주소 및 외부 인터페이스의 IPv4 주소).
- ASA에 IPv6 내부 네트워크가 있으며 외부 네트워크는 IPv6입니다(내부 및 외부 인터페이스의 IPv6 주소).

Basic(기본**)** 패널의 필드

- 피어 IP 주소 - (IPv4 또는 IPv6) IP 주소 및 해당 주소가 고정인지 여부를 지정할 수 있습니다.
- Connection Name(연결 이름) - 이 연결 프로파일에 할당된 이름을 지정합니다. Edit(수정) 기능이 따로 있기 때문에 이 필드는 표시 전용입니다. 연결 이름이 Peer IP Address(피어 IP 주소) 필드에 지정된 IP 주소와 같도록 지정할 수 있습니다.

- Interface(인터페이스) - 이 연결에 사용할 인터페이스를 선택합니다.
- Protected Networks(보호된 네트워크) - 이 연결에 대해 보호되는 로컬 및 원격 네트워크를 선택하거나 지정합니다.
  - IP Address Type(IP 주소 유형) - IPv4 주소 또는 IPv6 주소를 지정합니다.
  - Local Network(로컬 네트워크) - 로컬 네트워크의 IP 주소를 지정합니다.
  - ... - 로컬 네트워크를 선택할 수 있는 Browse Local Network(로컬 네트워크 찾아보기) 대화 상자를 엽니다.
  - Remote Network(원격 네트워크) - 원격 네트워크의 IP 주소를 지정합니다.
- IPsec Enabling(IPsec 활성화) - 이 연결 프로파일에 대한 그룹 정책 및 해당 정책에 지정된 키 교환 프로토콜을 지정합니다.
  - Group Policy Name(그룹 정책 이름) - 이 연결 프로파일과 연계된 그룹 정책을 지정합니다.
  - Manage(관리) - 원격 네트워크를 선택할 수 있는 Browse Remote Network(원격 네트워크 찾아보기) 대화 상자를 엽니다.
  - Enable IKEv1(IKEv1 활성화) - 지정된 그룹 정책에서 키 교환 프로토콜 IKEv1을 활성화합니다.
  - Enable IKEv2(IKEv2 활성화) - 지정된 그룹 정책에서 키 교환 프로토콜 IKEv2를 활성화합니다.
- IKEv1 Settings(IKEv1 설정) 탭 - IKEv1에 대한 인증 및 암호화 설정을 지정합니다.
  - Pre-shared Key(사전 공유 키) - 터널 그룹에 대한 사전 공유 키 값을 지정합니다. 사전 공유 키의 최대 길이는 128자입니다.
  - Device Certificate(디바이스 인증서) - 사용 가능한 경우 인증에 사용할 ID 인증서의 이름을 지정합니다.
  - Manage(관리) - Manage Identity Certificates(ID 인증서 관리) 대화 상자를 엽니다. 이 대화 상자에서 이미 구성된 인증서를 확인하고, 새 인증서를 추가하고, 인증서 세부사항을 보고, 인증서를 수정하거나 삭제할 수 있습니다.
  - IKE Policy(IKE 정책) - IKE 제안에 사용할 하나 이상의 암호화 알고리즘을 지정합니다.
  - Manage(관리) - Configure IKEv1 Proposals(IKEv1 제안 구성) 대화 상자를 엽니다.
  - IPsec Proposal(IPsec 제안) - IPsec IKEv1 제안에 사용할 하나 이상의 암호화 알고리즘을 지정합니다.
- IKEv2 Settings(IKEv2 설정) 탭 - IKEv2에 대한 인증 및 암호화 설정을 지정합니다.
  - Local Pre-shared Key(로컬 사전 공유 키) - 터널 그룹에 대한 사전 공유 키 값을 지정합니다. 사전 공유 키의 최대 길이는 128자입니다.
  - Local Device Certificate(로컬 디바이스 인증서) - 사용 가능한 경우 인증에 사용할 ID 인증서의 이름을 지정합니다.

- Manage(관리) - Manage Identity Certificates(ID 인증서 관리) 대화 상자를 엽니다. 이 대화 상자에서 이미 구성된 인증서를 확인하고, 새 인증서를 추가하고, 인증서 세부사항을 보고, 인증서를 수정하거나 삭제할 수 있습니다.
- Remote Peer Pre-shared Key(원격 피어 사전 공유 키) - 터널 그룹에 대한 원격 피어 사전 공유 키 값을 지정합니다. 사전 공유 키의 최대 길이는 128자입니다.
- Remote Peer Certificate Authentication(원격 피어 인증서 인증) - 이 연결 프로파일의 IKEv2 연결에 대해 인증서 인증을 허용하려면 Allowed(허용됨)를 선택합니다.
- Manage(관리) - 인증서를 보고 새 인증서를 추가할 수 있는 Manage CA Certificates(CA 인증서 관리) 대화 상자를 엽니다.
- IKE Policy(IKE 정책) - IKE 제안에 사용할 하나 이상의 암호화 알고리즘을 지정합니다.
- Manage(관리) - Configure IKEv1 Proposals(IKEv1 제안 구성) 대화 상자를 엽니다.
- IPsec Proposal(IPsec 제안) - IPsec IKEv1 제안에 사용할 하나 이상의 암호화 알고리즘을 지정합니다.
- Select(선택) - IKEv2 연결의 연결 프로파일에 제안을 할당할 수 있는 Select IPsec Proposals (Transform Sets)(IPsec 제안(변형 집합) 선택) 대화 상자를 엽니다.
- 이 연결 프로파일에는 Advanced(고급) > Crypto Map Entry(암호화 맵 항목)도 있습니다.

사이트 대 사이트 터널 그룹

ASDM 창의 Configuration(구성) > Site-to-Site VPN (사이트 대 사이트 VPN) > Advanced(고급) > Tunnel Groups(터널 그룹)은 IPsec 사이트 대 사이트 연결 프로파일(터널 그룹)의 특성을 지정합니다. 또한 IKE 피어 및 사용자 인증 매개변수를 선택하고, IKE 킵얼라이브 모니터링을 구성하고, 기본 그룹 정책을 선택할 수 있습니다.

- Name(이름) - 이 터널 그룹에 할당된 이름을 지정합니다. Edit(수정) 기능이 따로 있기 때문에 이 필드는 표시 전용입니다.
- IKE Authentication(IKE 인증) - IKE 피어를 인증할 때 사용할 사전 공유 키 및 ID 인증서 매개변수를 지정합니다.
  - Pre-shared Key(사전 공유 키) - 터널 그룹에 대한 사전 공유 키 값을 지정합니다. 사전 공유 키의 최대 길이는 128자입니다.
  - Identity Certificate(ID 인증서) - 인증에 사용할 ID 인증서의 이름을 지정합니다(사용 가능한 경우).
  - Manage(관리) - Manage Identity Certificates(ID 인증서 관리) 대화 상자를 엽니다. 이 대화 상자에서 이미 구성된 인증서를 확인하고, 새 인증서를 추가하고, 인증서 세부사항을 보고, 인증서를 수정하거나 삭제할 수 있습니다.
  - IKE Peer ID Validation(IKE 피어 ID 검증) - IKE 피어 ID 검증을 선택할지 여부를 지정합니다. 기본값은 Required(필수)입니다.

- IPsec Enabling(IPsec 활성화) - 이 연결 프로파일에 대한 그룹 정책 및 해당 정책에 지정된 키 교환 프로토콜을 지정합니다.
  - Group Policy Name(그룹 정책 이름) - 이 연결 프로파일과 연계된 그룹 정책을 지정합니다.
  - Manage(관리) - 원격 네트워크를 선택할 수 있는 Browse Remote Network(원격 네트워크 찾아보기) 대화 상자를 엽니다.
  - Enable IKEv1(IKEv1 활성화) - 지정된 그룹 정책에서 키 교환 프로토콜 IKEv1을 활성화합니다.
  - Enable IKEv2(IKEv2 활성화) - 지정된 그룹 정책에서 키 교환 프로토콜 IKEv2를 활성화합니다.

- IKEv1 Settings(IKEv1 설정) 탭 - IKEv1에 대한 인증 및 암호화 설정을 지정합니다.
  - Pre-shared Key(사전 공유 키) - 터널 그룹에 대한 사전 공유 키 값을 지정합니다. 사전 공유 키의 최대 길이는 128자입니다.
  - Device Certificate(디바이스 인증서) - 사용 가능한 경우 인증에 사용할 ID 인증서의 이름을 지정합니다.

    참고 일부 프로필은 엔드포인트가 원격 액세스 또는 LAN to LAN인지를 확인할 수 없습니다. 터널 그룹을 결정할 수 없는 경우, 기본값은

    ```
    tunnel-group-map default-group <tunnel-group-name>
    ```

    *DefaultRAGroup*입니다.

  - Manage(관리) - Manage Identity Certificates(ID 인증서 관리) 대화 상자를 엽니다. 이 대화 상자에서 이미 구성된 인증서를 확인하고, 새 인증서를 추가하고, 인증서 세부사항을 보고, 인증서를 수정하거나 삭제할 수 있습니다.
  - IKE Policy(IKE 정책) - IKE 제안에 사용할 하나 이상의 암호화 알고리즘을 지정합니다.
  - Manage(관리) - Configure IKEv1 Proposals(IKEv1 제안 구성) 대화 상자를 엽니다.
  - IPsec Proposal(IPsec 제안) - IPsec IKEv1 제안에 사용할 하나 이상의 암호화 알고리즘을 지정합니다.

- IKEv2 Settings(IKEv2 설정) 탭 - IKEv2에 대한 인증 및 암호화 설정을 지정합니다.
  - Local Pre-shared Key(로컬 사전 공유 키) - 터널 그룹에 대한 사전 공유 키 값을 지정합니다. 사전 공유 키의 최대 길이는 128자입니다.
  - Local Device Certificate(로컬 디바이스 인증서) - 사용 가능한 경우 인증에 사용할 ID 인증서의 이름을 지정합니다.

- Manage(관리) - Manage Identity Certificates(ID 인증서 관리) 대화 상자를 엽니다. 이 대화 상자에서 이미 구성된 인증서를 확인하고, 새 인증서를 추가하고, 인증서 세부사항을 보고, 인증서를 수정하거나 삭제할 수 있습니다.
- Remote Peer Pre-shared Key(원격 피어 사전 공유 키) - 터널 그룹에 대한 원격 피어 사전 공유 키 값을 지정합니다. 사전 공유 키의 최대 길이는 128자입니다.
- Remote Peer Certificate Authentication(원격 피어 인증서 인증) - 이 연결 프로파일의 IKEv2 연결에 대해 인증서 인증을 허용하려면 Allowed(허용됨)를 선택합니다.
- Manage(관리) - 인증서를 보고 새 인증서를 추가할 수 있는 Manage CA Certificates(CA 인증서 관리) 대화 상자를 엽니다.
- IKE Policy(IKE 정책) - IKE 제안에 사용할 하나 이상의 암호화 알고리즘을 지정합니다.
- Manage(관리) - Configure IKEv1 Proposals(IKEv1 제안 구성) 대화 상자를 엽니다.
- IPsec Proposal(IPsec 제안) - IPsec IKEv1 제안에 사용할 하나 이상의 암호화 알고리즘을 지정합니다.
- Select(선택) - IKEv2 연결의 연결 프로파일에 제안을 할당할 수 있는 Select IPsec Proposals (Transform Sets)(IPsec 제안(변형 집합) 선택) 대화 상자를 엽니다.

- IKE Keepalive(IKE 킵얼라이브) - IKE 킵얼라이브 모니터링을 활성화하고 구성합니다. 다음 특성 중 하나만 선택할 수 있습니다.
  - Disable Keep Alives(킵얼라이브 비활성화) - IKE 킵얼라이브를 활성화하거나 비활성화합니다.
  - Monitor Keep Alives(킵얼라이브 모니터링) - IKE 킵얼라이브 모니터링을 활성화하거나 비활성화합니다. 이 옵션을 선택하면 Confidence Interval(신뢰 구간) 및 Retry Interval(재시도 간격) 필드가 활성화됩니다.
  - Confidence Interval(신뢰 구간) - IKE 킵얼라이브 신뢰 구간을 지정합니다. 이것은 ASA에서 킵얼라이브 모니터링을 시작하기 전에 피어가 유휴 상태에 있도록 허용해야 하는 시간(초)입니다. 최소값은 10초이고, 최대값은 300초입니다. 원격 액세스 그룹의 기본값은 10초입니다.
  - Retry Interval(재시도 간격) - IKE 킵얼라이브 재시도 간에 대기할 시간(초)을 지정합니다. 기본값은 2초입니다.
  - Head end will never initiate keepalive monitoring(헤드 엔드에서 킵얼라이브 모니터링을 시작하지 않음) - 중앙 사이트 ASA에서 킵얼라이브 모니터링을 시작하지 않도록 지정합니다.

사이트 대 사이트 연결 프로파일, 암호화 맵 항목

이 대화 상자에서는 현재 사이트 대 사이트 연결 프로파일에 대한 암호화 매개변수를 지정합니다.

- **Priority(**우선순위**)** - 고유한 우선순위(1~65,543, 1이 우선순위가 가장 높음)입니다. IKE 협상이 시작되면 협상을 시작한 피어가 모든 정책을 원격 피어로 보내고 원격 피어는 우선순위대로 자신의 정책과 일치하는 정책을 검색합니다.
- **Perfect Forward Secrecy** - 특정 IPsec SA의 키가 다른 비밀 키에서 파생되지 않도록 합니다. 누군가가 키를 파괴한 경우 PFS는 공격자가 다른 키를 파생할 수 없게 합니다. PFS를 활성화하면 Diffie-Hellman Group(Diffie-Hellman 그룹) 목록이 활성화됩니다.
  - **Diffie-Hellman Group(Diffie-Hellman** 그룹**)** - 두 IPsec 피어가 공유 암호를 서로 전송하지 않고 파생시키는 데 사용하는 그룹 식별자입니다. Group 1 (768-bits)(그룹 1(768비트)), Group 2 (1024-bits)(그룹 2(1024비트)) 및 Group 5 (1536-bits)(그룹 5(1536비트))를 선택할 수 있습니다.
- **Enable NAT-T(NAT-T** 활성화**)** - IPsec 피어가 NAT 디바이스를 통해 원격 액세스와 LAN-to-LAN 연결을 둘 다 설정할 수 있도록 이 정책에 대해 NAT-T(NAT Traversal)를 활성화합니다.
- **Enable Reverse Route Injection(**역방향 라우팅 주입 활성화**)** - 원격 터널 엔드포인트로 보호되는 네트워크 및 호스트에 대한 라우팅 프로세스에 정적 경로를 자동으로 삽입할 수 있는 기능을 제공합니다.
- **Security Association Lifetime(**보안 연계 수명**)** - SA(Security Association) 기간을 구성합니다. 이 매개변수는 IPsec SA 키의 수명(IPsec SA가 만료되어 새 키로 재협상해야 할 때까지 지속되는 기간)을 측정하는 방법을 지정합니다.
  - **Time(**시간**)** - SA 수명을 시(hh), 분(mm), 초(ss) 단위로 지정합니다.
  - **Traffic Volume(**트래픽 양**)** - SA 수명을 트래픽 양(KB)으로 정의합니다. IPsec SA가 만료되는 페이로드 데이터의 킬로바이트 수를 입력합니다. 최소값은 100KB이고, 기본값은 10,000KB이며, 최대값은 2,147,483,647KB입니다.
- Static Crypto Map Entry Parameters(고정 암호화 맵 항목 매개변수) - 피어 IP 주소가 고정으로 지정된 경우 다음 추가 매개변수를 구성합니다.
  - Connection Type(연결 유형) - 허용되는 협상을 양방향, 응답 전용 또는 시작 전용으로 지정합니다.
  - Send ID Cert. Chain(ID 인증서 체인 보내기) - 전체 인증서 체인에 대한 전송을 활성화합니다.
  - IKE Negotiation Mode(IKE 협상 모드) - SA, Main(기본) 또는 Aggressive(적극적인)를 설정하기 위해 키 정보를 교환하는 모드를 설정합니다. 또한 협상 초기자가 사용하는 모드를 설정합니다. 응답자는 자동으로 협상됩니다. Aggressive Mode(적극적인 모드)는 사용하는 패킷 및 교환이 적으므로 더 빠르지만 통신 당사자의 ID를 보호하지 않습니다. Main Mode(기본 모드)는 사용하는 패킷과 교환이 많으므로 더 느리지만 통신 당사자의 ID를 보호합니다. 이 모드가 더 안전하고 기본적으로 선택됩니다. Aggressive(적극적인)를 선택하면 Diffie-Hellman Group(Diffie-Hellman 그룹) 목록이 활성화됩니다.
  - Diffie-Hellman Group(Diffie-Hellman 그룹) - 두 IPsec 피어가 공유 암호를 서로 전송하지 않고 파생시키는 데 사용하는 그룹 식별자입니다. Group 1 (768-bits)(그룹 1(768비트)), Group

2 (1024-bits)(그룹 2(1024비트)) 및 Group 5 (1536-bits)(그룹 5(1536비트))를 선택할 수 있습니다.

CA 인증서 관리

CA 인증서 관리 작업은 다음과 같이 원격 액세스 및 사이트 대 사이트 VPN에 적용됩니다.

- Site-to_site(사이트 대 사이트)에서 IKE Peer Authentication(IKE 피어 인증) 아래에서 Manage(관리)를 클릭하면 Manage CA Certificates(CA 인증서 관리) 대화 상자가 열립니다.
- Remote Access VPN(원격 액세스 VPN)에서 **Certificate Management(**인증서 관리**)** > **CA Certificates(CA** 인증서**)**를 클릭합니다.

이 대화 상자를 사용하여 IKE 피어 인증에 사용할 수 있는 CA 인증서 목록의 항목을 확인, 추가, 수정 및 삭제할 수 있습니다. Manage CA Certificates(CA 인증서 관리) 대화 상자에는 인증서가 발급된 대상, 인증서를 발급한 주체, 인증서 만료 날짜 및 사용 현황 데이터를 포함하여 현재 구성된 인증서에 대한 정보가 나열됩니다.

- Add or Edit(추가 또는 수정) - 인증서에 대한 정보를 지정하고 인증서를 설치할 수 있는 Install Certificate(인증서 설치) 대화 상자 또는 Edit Certificate(인증서 수정) 대화 상자를 엽니다.
- Show Details(세부사항 표시) - 테이블에서 선택한 인증서에 대한 자세한 정보를 표시합니다.
- Delete(삭제) - 테이블에서 선택한 연결을 제거합니다. 확인 또는 실행 취소가 없습니다.

사이트 대 사이트 연결 프로파일, 인증서 설치

이 대화 상자에서는 새 CA 인증서를 설치할 수 있습니다. 다음 방법 중 하나를 사용하여 인증서를 가져올 수 있습니다.

- 인증서 파일을 검색하여 파일에서 설치합니다.
- 이전에 PEM 형식으로 가져온 인증서 텍스트를 이 대화 상자의 상자에 붙여넣습니다.
- Use SCEP(SCEP 사용) - Windows Server 2003 제품군에서 실행되는 인증서 서비스에 SCEP(Simple Certificate Enrollment Protocol) 에드온을 사용하도록 지정합니다. Cisco 라우터 및 다른 중간 네트워크 디바이스가 인증서를 가져올 수 있도록 SCEP 프로토콜을 지원합니다.
  - SCEP URL: http:// - SCEP 정보를 다운로드할 URL을 지정합니다.
  - Retry Period(재시도 기간) - SCEP 쿼리 간에 경과해야 하는 시간(분)을 지정합니다.
  - Retry Count(재시도 횟수) - 허용되는 최대 재시도 횟수를 지정합니다.
- More Options(추가 옵션) - Configure Options for CA Certificate(CA 인증서에 대한 옵션 구성) 대화 상자를 엽니다.

이 대화 상자에서는 이 IPsec 원격 액세스 연결의 CA 인증서 검색에 대한 세부사항을 지정할 수 있습니다. 이 대화 상자에는 Revocation Check(해지 확인), CRL Retrieval Policy(CRL 검색 정책), CRL

Retrieval Method(CRL 검색 방법), OCSP Rules(OCSP 규칙) 및 Advanced(고급) 대화 상자가 들어 있습니다.

Revocation Check(해지 확인) 대화 상자를 사용하여 CA 인증서 해지 확인에 대한 정보를 지정할 수 있습니다.

- 라디오 버튼은 인증서 해지 확인 여부를 지정합니다. **Do not check certificates for revocation(**인증서 해지를 확인하지 않음**)** 또는 Check Certificates for revocation(인증서 해지 확인)을 선택합니다.
- Revocation Methods(해지 방법) 영역 - 해지 확인에 사용할 방법(CRL 또는 OCSP) 및 이러한 방법을 사용할 순서를 지정할 수 있습니다. 두 방법 중 하나 또는 둘 다를 선택할 수 있습니다.

AnyConnect VPN 클라이언트 이미지

Configuration(구성**) > Remote Access VPN(**원격 액세스 **VPN) > Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**) > AnyConnect Client Software(AnyConnect** 클라이언트 소프트웨어**)** 창에는 ASDM에서 구성된 AnyConnect 클라이언트 이미지가 나열됩니다.

AnyConnect Client Images(AnyConnect 클라이언트 이미지) 테이블 - ASDM에 구성된 패키지 파일을 표시하며, ASA에서 원격 PC에 이미지를 다운로드할 순서를 설정할 수 있습니다.

- Add(추가) - Add AnyConnect Client Image(AnyConnect 클라이언트 이미지 추가) 대화 상자를 표시합니다. 여기에서 플래시 메모리의 파일을 클라이언트 이미지 파일로 지정하거나 플래시 메모리에서 클라이언트 이미지로 지정할 파일을 검색할 수 있습니다. 또한 로컬 컴퓨터에서 플래시 메모리로 파일을 업로드할 수 있습니다.
- Replace(바꾸기) - Replace AnyConnect Client Image(AnyConnect 클라이언트 이미지 바꾸기) 대화 상자를 표시합니다. 여기에서 플래시 메모리의 파일을 클라이언트 이미지 파일로 지정하여 SSL VPN Client Images(SSL VPN 클라이언트 이미지) 테이블에 강조 표시된 이미지를 바꿀 수 있습니다. 또한 로컬 컴퓨터에서 플래시 메모리로 파일을 업로드할 수 있습니다.
- Delete(삭제) - 테이블에서 이미지를 삭제합니다. 플래시에서 패키지 파일을 삭제하지는 않습니다.
- Move Up(위로 이동) 및 Move Down(아래로 이동) - 위쪽 및 아래쪽 화살표를 사용하여 ASA에서 원격 PC에 클라이언트 이미지를 다운로드할 순서를 변경할 수 있습니다. 테이블 맨 위에 있는 이미지가 가장 먼저 다운로드됩니다. 따라서 가장 자주 사용하는 운영 체제에서 사용되는 이미지를 맨 위로 이동해야 합니다.

AnyConnect VPN 클라이언트 이미지, 추가/교체

이 창에서는 ASA 플래시 메모리에서 AnyConnect 클라이언트 이미지로 추가하거나 테이블에 이미 나열된 이미지를 바꿀 파일의 파일 이름을 지정할 수 있습니다. 또한 플래시 메모리에서 식별할 파일을 찾아보거나, 로컬 컴퓨터에서 파일을 업로드할 수 있습니다.

- Flash SVC Image(플래시 SVC 이미지) - 플래시 메모리에서 SSL VPN 클라이언트 이미지로 식별할 파일을 지정합니다.

- Browse Flash(플래시 찾아보기) - 플래시 메모리에 있는 모든 파일을 볼 수 있는 Browse Flash(플래시 찾아보기) 대화 상자를 표시합니다.
- Upload(업로드) - 로컬 PC에서 클라이언트 이미지로 식별할 파일을 업로드할 수 있는 Upload Image(이미지 업로드) 대화 상자를 표시합니다.
- Regular expression to match user-agent(사용자 에이전트와 일치시킬 정규식) - ASA에서 브라우저로부터 전달된 사용자 에이전트 문자열과 일치시키는 데 사용할 문자열을 지정합니다. 모바일 사용자의 경우 이 기능을 사용하여 모바일 디바이스의 연결 시간을 줄일 수 있습니다. 브라우저는 ASA에 연결할 때 HTTP 헤더에 사용자 에이전트 문자열을 포함합니다. ASA가 문자열을 수신하고 그 문자열이 이미지에 대해 구성된 표현식과 일치될 경우, 나머지 클라이언트 이미지를 테스트하지 않고 즉시 그 이미지를 다운로드합니다.

AnyConnect VPN 클라이언트 이미지, 이미지 업로드

이 창에서는 AnyConnect 클라이언트 이미지로 식별할 로컬 컴퓨터의 파일 또는 보안 어플라이언스 플래시 메모리의 파일에 대한 경로를 지정할 수 있습니다. 또한 로컬 컴퓨터 또는 보안 어플라이언스의 플래시 메모리에서 식별할 파일을 찾아볼 수 있습니다.

- Local File Path(로컬 파일 경로) - 로컬 컴퓨터에서 SSL VPN 클라이언트 이미지로 식별할 파일의 파일 이름을 식별합니다.
- Browse Local Files(로컬 파일 찾아보기) - Select File Path(파일 경로 선택) 대화 상자를 표시합니다. 여기에서 로컬 컴퓨터의 모든 파일을 보고, 클라이언트 이미지로 식별할 파일을 선택할 수 있습니다.
- Flash File System Path(플래시 파일 시스템 경로) - 보안 어플라이언스의 플래시 메모리에서 SSL VPN 클라이언트 이미지로 식별할 파일의 파일 이름을 식별합니다.
- Browse Flash(플래시 찾아보기) - Browse Flash(플래시 찾아보기) 대화 상자를 표시합니다. 여기에서 보안 어플라이언스의 플래시 메모리에 있는 모든 파일을 보고, 클라이언트 이미지로 식별할 파일을 선택할 수 있습니다.
- Upload File(파일 업로드) - 파일 업로드를 시작합니다.

AnyConnect VPN 클라이언트 연결 구성

AnyConnect 클라이언트 프로파일 구성

모든 AnyConnect 사용자에게 전역으로 AnyConnect 클라이언트 프로필을 구축하도록 또는 그룹 정책에 따라 사용자에게 구축하도록 ASA를 구성할 수 있습니다. 일반적으로 사용자는 설치된 AnyConnect 모듈마다 클라이언트 프로파일을 하나씩 갖고 있습니다. 한 사용자에게 프로파일을 2개 이상 제공해야 하는 경우도 있습니다. 여러 위치에서 작업하는 사용자는 프로파일이 여러 개 필요할 수 있습니다. SBL 같은 일부 프로파일 설정은 전역 수준에서 연결 환경을 제어합니다. 기타 설정은 특정 호스트에 대해 고유하며 선택한 호스트에 따라 결정됩니다.

AnyConnect 클라이언트 프로파일을 만들고 클라이언트 기능을 제어하는 방법에 대한 내용은 AnyConnect VPN 클라이언트 관리자 가이드를 참조하십시오.

클라이언트 프로파일은 **Configuration(**구성**) > Remote Access VPN(**원격 액세스 **VPN) > Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**) > AnyConnect Client Profile(AnyConnect** 클라이언트 프로파일**)**에서 구성됩니다.

Add/Import(추가/가져오기) - Add AnyConnect Client Profiles(AnyConnect 클라이언트 프로파일 추가) 대화 상자를 표시합니다. 여기에서 플래시 메모리의 파일을 프로파일로 지정하거나 플래시 메모리에서 프로파일로 지정할 파일을 검색할 수 있습니다. 또한 로컬 컴퓨터에서 플래시 메모리로 파일을 업로드할 수 있습니다.

- Profile Name(프로파일 이름) - 이 그룹 정책에 대한 AnyConnect 클라이언트 프로파일을 지정합니다.
-
- Profile Usage(프로필 사용) - VPN, 네트워크 액세스 관리자, 웹 보안, ISE Posture, AMP Enabler 또는 네트워크 가시성 모듈 또는 Umbrella 로밍 보안이 처음 생성될 때 프로필에 할당된 용도를 표시합니다. XML 파일에 지정된 용도를 ASDM에서 인식하지 못할 경우 드롭다운 목록이 활성화되어 사용 유형을 수동으로 선택할 수 있습니다.
- Profile Location(프로필 위치) - ASA 플래시 메모리에서 프로필 파일의 경로를 지정합니다. 해당 파일이 없는 경우 ASA에서는 프로필 템플릿을 기반으로 새 프로필을 만듭니다.
- Group Policy(그룹 정책) - 이 프로파일에 대한 그룹 정책을 지정합니다. 프로파일은 AnyConnect 클라이언트와 함께 해당 그룹 정책에 소속된 사용자에게 다운로드됩니다.

Edit(수정) - AnyConnect 클라이언트 기능에 대한 프로파일에 포함된 설정을 변경할 수 있는 Edit SSL VPN Client Profile(SSL VPN 클라이언트 프로파일 수정) 창을 표시합니다.

내보내기

- Device Profile Path(디바이스 프로파일 경로) - 프로파일 파일의 경로 및 파일 이름을 표시합니다.
- Local Path(로컬 경로) - 프로파일 파일을 내보낼 경로 및 파일 이름을 지정합니다.
- Browse Local(로컬로 찾아보기) - 창을 실행하여 로컬 디바이스 파일 시스템을 검색하려면 클릭합니다.

Delete(삭제) - 테이블에서 프로파일을 삭제합니다. 플래시에서 XML 파일을 삭제하지는 않습니다.

AnyConnect Client Profiles Table(AnyConnect 클라이언트 프로파일 테이블) - AnyConnect 클라이언트 프로파일로 지정된 XML 파일을 표시합니다.

네트워크 주소 변환에서 **AnyConnect** 트래픽 제외

ASA에서 NAT(Network Address Translation)를 수행하도록 구성한 경우 AnyConnect 클라이언트, 내부 네트워크 및 DMZ의 기업 리소스가 서로 네트워크 연결을 설정할 수 있도록 원격 액세스 AnyConnect 클라이언트 트래픽을 제외하여 변환되지 않게 해주어야 합니다. AnyConnect 클라이언트 트래픽이

변환되지 않도록 제외하지 않으면 AnyConnect 클라이언트와 기타 기업 리소스가 통신할 수 없습니다.

"NAT 제외"라고도 하는 "ID NAT"는 주소가 자체적으로 변환되는 것을 허용하여 효과적으로 NAT를 우회합니다. 두 주소 풀 사이에, 한 주소 풀과 한 서브네트워크 사이에 또는 두 서브네트워크 사이에 ID NAT를 적용할 수 있습니다.

다음은 네트워크 토폴로지 예에서 가상 네트워크 개체인 Engineering VPN 주소 풀, Sales VPN 주소 풀, 내부 네트워크, DMZ 네트워크 및 인터넷 사이에 ID NAT를 구성하는 절차입니다. 각 ID NAT 구성에는 NAT 규칙이 하나 필요합니다.

표 ***4: VPN*** 클라이언트에 대해 ***ID NAT***를 구성하기 위한 네트워크 주소 지정

네트워크 또는 주소 풀	네트워크 또는 주소 풀 이름	주소 범위
내부 네트워크	inside-network	10.50.50.0 - 10.50.50.255
엔지니어링 VPN 주소 풀	Engineering-VPN	10.60.60.1 - 10.60.60.254
Sales VPN 주소 풀	Sales-VPN	10.70.70.1 - 10.70.70.254
DMZ 네트워크	DMZ-network	192.168.1.0 - 192.168.1.255

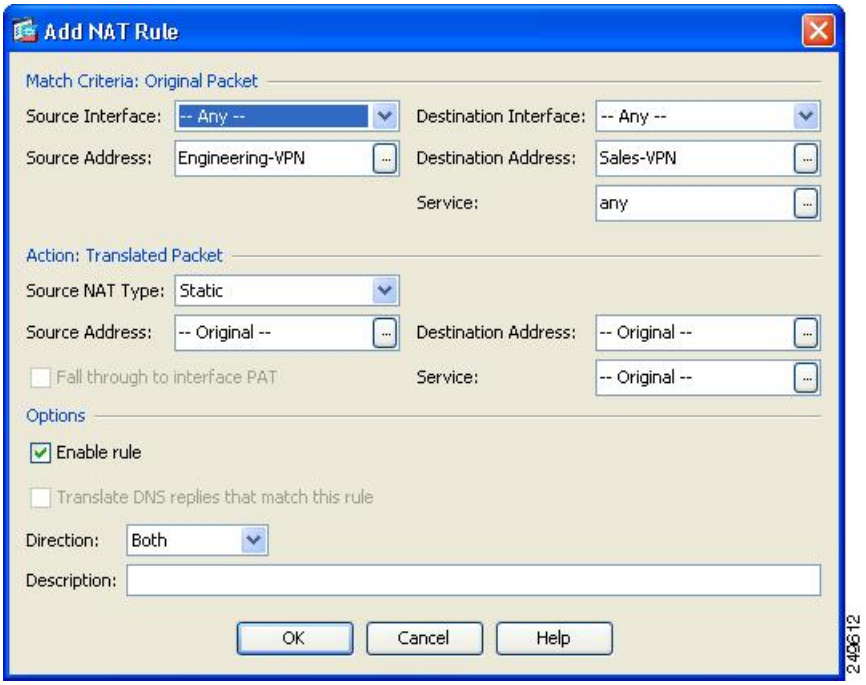
프로시저

단계 **1** ASDM에 로그인하여 **Configuration(**구성**) > Firewall(**방화벽**) > NAT Rules(NAT** 규칙**)**로 이동합니다.

단계 **2** Engineering VPN 주소 풀의 호스트가 Sales VPN 주소 풀의 호스트에 도달할 수 있도록 NAT 규칙을 만듭니다. ASA에서 통합 NAT 테이블의 다른 규칙보다 이 규칙을 먼저 평가하도록 NAT Rules(NAT 규칙) 창에서 **Add(**추가**) > Add NAT Rule** Before "Network Object" NAT rules("네트워크 개체" NAT 규칙보다 NAT 규칙 먼저 추가)로 이동합니다.

참고 NAT 규칙 평가는 위에서 아래로, 일치하는 순서대로 적용됩니다. ASA에서는 한 패킷을 특정 NAT 규칙과 일치시키면 더 이상 평가를 수행하지 않습니다. ASA에서 너무 일찍 광범위한 NAT 규칙과 일치시키는 일이 없도록 가장 구체적인 규칙을 통합 NAT 테이블 맨 위에 배치하는 것이 중요합니다.

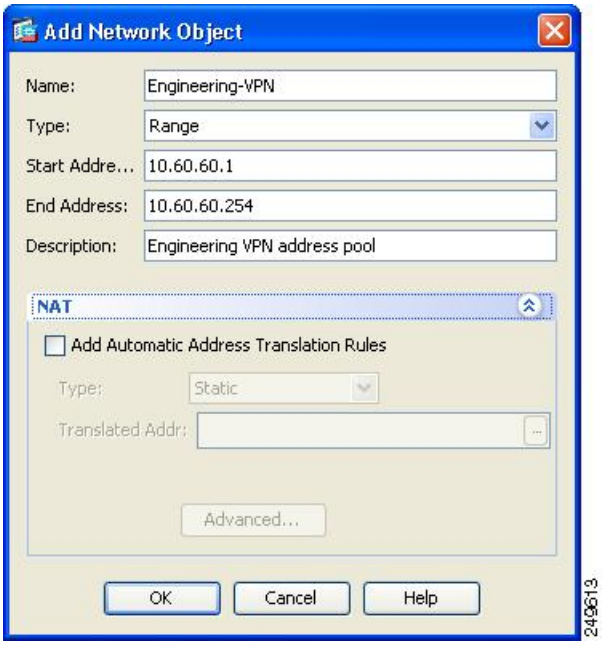
그림 *1: Add NAT rule(NAT* 규칙 추가*)* 대화 상자



a) Match criteria: Original Packet(일치 조건: 원래 패킷) 영역에서 다음 필드를 구성합니다.

- **Source Interface(**소스 인터페이스**)**: Any(모두)
- **Destination Interface(**대상 인터페이스**)**: Any(모두)
- **Source Address(**소스 주소**)**: Source Address browse(소스 주소 찾아보기) 버튼을 클릭하고 Engineering VPN 주소 풀을 나타내는 네트워크 개체를 만듭니다. 개체 유형을 주소의 Range(범위)로 정의합니다. 자동 주소 변환 규칙을 추가하지 마십시오.
- **Destination Address(**대상 주소**)**: Destination Address browse(대상 주소 찾아보기) 버튼을 클릭하고 Engineering VPN 주소 풀을 나타내는 네트워크 개체를 만듭니다. 개체 유형을 주소의 Range(범위)로 정의합니다. 자동 주소 변환 규칙을 추가하지 마십시오.

그림 2: VPN 주소 풀에 대한 네트워크 개체 만들기



b) **Action Translated Packet(**작업 변환된 패킷**)** 영역에서 다음 필드를 구성합니다.

- **Source NAT Type(**소스 **NAT** 유형**)**: Static(정적)
- **Source Address(**소스 주소**)**: Original(원본)
- **Destination Address(**대상 주소**)**: Original(원본)
- **Service(**서비스**)**: Original(원본)

c) Options(옵션) 영역에서 다음 필드를 구성합니다.

- **Enable rule(**규칙 활성화**)**을 선택합니다.
- **Translate DNS replies that match this rule(**이 규칙과 일치하는 **DNS** 응답 변환**)**의 선택을 취소하거나 빈 상태로 둡니다.
- **Direction(**방향**)**: Both(양쪽)
- **Description(**설명**)**: 이 규칙에 대한 설명을 추가합니다.

d) **OK(**확인**)**를 클릭합니다.

e) **Apply(**적용**)**을 클릭합니다.

CLI 예:

```
nat source static Engineering-VPN Engineering-VPN destination static Sales-VPN Sales-VPN
```

f) Send(보내기)를 클릭합니다.

단계 **3** ASA에서 NAT를 수행할 때 같은 VPN 풀의 두 호스트가 서로 연결되도록 또는 두 호스트가 VPN 터널을 통해 인터넷에 연결되도록 하려면 Enable traffic between two or more hosts connected to the same interface(같은 인터페이스에 연결된 2개 이상의 호스트 간 트래픽 활성화) 옵션을 활성화해야 합니다. 이렇게 하려면 ASDM에서 **Configuration(**구성**) > Device Setup(**디바이스 설정**) > Interface Settings(**인터페이스 설정**) > Interfaces(**인터페이스**)**를 선택합니다. Interface(인터페이스) 패널 하단에서 Enable traffic between two or more hosts connected to the same interface(같은 인터페이스에 연결된 2개 이상의 호스트 간 트래픽 활성화)를 선택하고 Apply(적용)를 클릭합니다.

CLI 예:

```
same-security-traffic permit inter-interface
```

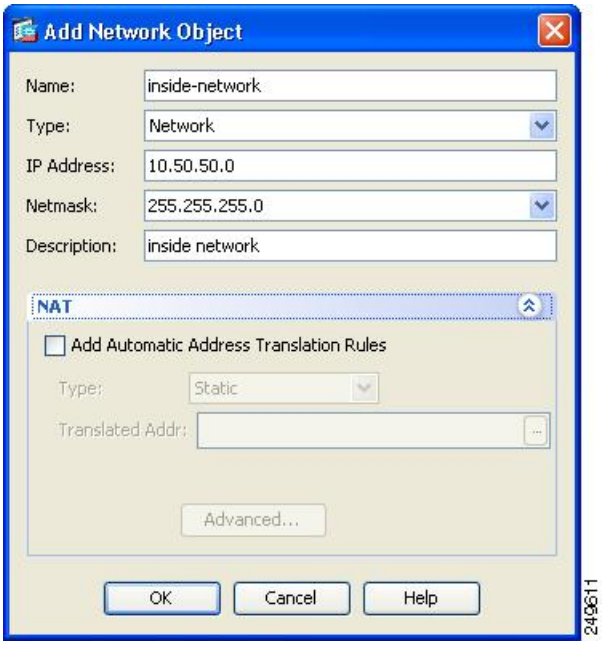
단계 **4** Engineering VPN 주소 풀의 호스트가 Engineering VPN 주소 풀의 호스트에 도달할 수 있도록 NAT 규칙을 만듭니다. 이전에 규칙을 만든 것처럼 이 규칙을 만들면 됩니다. 단, Match criteria: Original Packet(일치 조건: 원래 패킷) 영역에서 Engineering VPN 주소 풀을 소스 주소이자 대상 주소로 지정합니다.

단계 **5** Engineering VPN 원격 액세스 클라이언트가 "내부" 네트워크에 도달할 수 있도록 NAT 규칙을 만듭니다. 이 규칙이 다른 규칙보다 먼저 처리되도록 NAT Rules(NAT 규칙) 창에서 Add(추가) > Add NAT Rule Before "Network Object" NAT rules("네트워크 개체" NAT 규칙보다 NAT 규칙 먼저 추가)를 선택합니다.

a) Match criteria: Original Packet(일치 조건: 원래 패킷) 영역에서 다음 필드를 구성합니다.

- Source Interface(소스 인터페이스): Any(모두)
- Destination Interface(대상 인터페이스): Any(모두)
- Source Address(소스 주소): Source Address browse(소스 주소 찾아보기) 버튼을 클릭하고 내부 네트워크를 나타내는 네트워크 개체를 만듭니다. 개체 유형을 주소의 Network(네트워크)로 정의합니다. 자동 주소 변환 규칙을 추가하지 마십시오.
- Destination Address(대상 주소): Destination Address browse(대상 주소 찾아보기) 버튼을 클릭하고 Engineering VPN 주소 풀을 나타내는 네트워크 개체를 선택합니다.

그림 3: 내부 네트워크 개체 추가



b) Action: Translated Packet(작업: 변환된 패킷) 영역에서 다음 필드를 구성합니다.

- Source NAT Type(소스 NAT 유형): Static(정적)
- Source Address(소스 주소): Original(원본)
- Destination Address(대상 주소): Original(원본)
- Service(서비스): Original(원본)

c) **Options(옵션)** 영역에서 다음 필드를 구성합니다.

- **Enable rule(**규칙 활성화**)**을 선택합니다.
- **Translate DNS replies that match this rule(**이 규칙과 일치하는 **DNS** 응답 변환**)**의 선택을 취소하거나 빈 상태로 둡니다.
- Direction(방향): Both(양쪽)
- Description(설명): 이 규칙에 대한 설명을 추가합니다.

d) **OK(**확인**)**를 클릭합니다.

e) **Apply(**적용**)**을 클릭합니다.

CLI 예

```
nat source static inside-network inside-network destination static Engineering-VPN
Engineering-VPN
```

단계 **6** **5**단계의 방법에 따라 Engineering VPN 주소 풀과 DMZ 네트워크 간의 연결에 대해 ID NAT를 구성하는 새 규칙을 만듭니다. DMZ 네트워크를 소스 주소, Engineering VPN 주소 풀을 대상 주소로 사용합니다.

단계 **7** Engineering VPN 주소 풀이 터널을 통해 인터넷에 액세스할 수 있게 허용하는 새 NAT 규칙을 만듭니다. 이 경우에는 ID NAT를 사용하지 않습니다. 소스 주소를 비공개 주소에서 인터넷 라우팅 가능한 주소로 변경해야 하기 때문입니다. 이 규칙을 만들려면 다음 절차를 수행합니다.

a) 이 규칙이 다른 규칙보다 먼저 처리되도록 NAT Rules(NAT 규칙) 창에서 Add(추가) > Add NAT Rule Before "Network Object" NAT rules("네트워크 개체" NAT 규칙보다 NAT 규칙 먼저 추가)를 선택합니다.

b) Match criteria: Original Packet(일치 조건: 원래 패킷) 영역에서 다음 필드를 구성합니다.

- Source Interface(소스 인터페이스): Any(모두)
- Destination Interface(대상 인터페이스): Any(모두) Action: Translated Packet(작업: 변환된 패킷) 영역에서 Source Address(소스 주소)로 outside(외부)를 선택하면 이 필드가 자동으로 "outside(외부)"로 채워집니다.
- Source Address(소스 주소): Source Address browse(소스 주소 찾아보기) 버튼을 클릭하고 Engineering VPN 주소 풀을 나타내는 네트워크 개체를 선택합니다.
- Destination Address(대상 주소): Any(모두)

c) Action: Translated Packet(작업: 변환된 패킷) 영역에서 다음 필드를 구성합니다.

- Source NAT Type(소스 NAT 유형): Dynamic PAT (Hide)(동적 PAT(숨김))
- Source Address(소스 주소): Source Address browse(소스 주소 찾아보기) 버튼을 클릭하고 outside interface(인터페이스 외부)를 선택합니다.
- Destination Address(대상 주소): Original(원본)
- Service(서비스): Original(원본)

d) Options(옵션) 영역에서 다음 필드를 구성합니다.

- Enable rule(규칙 활성화)을 선택합니다.
- Translate DNS replies that match this rule(이 규칙과 일치하는 DNS 응답 변환)의 선택을 취소하거나 빈 상태로 둡니다.
- Direction(방향): Both(양쪽)
- Description(설명): 이 규칙에 대한 설명을 추가합니다.

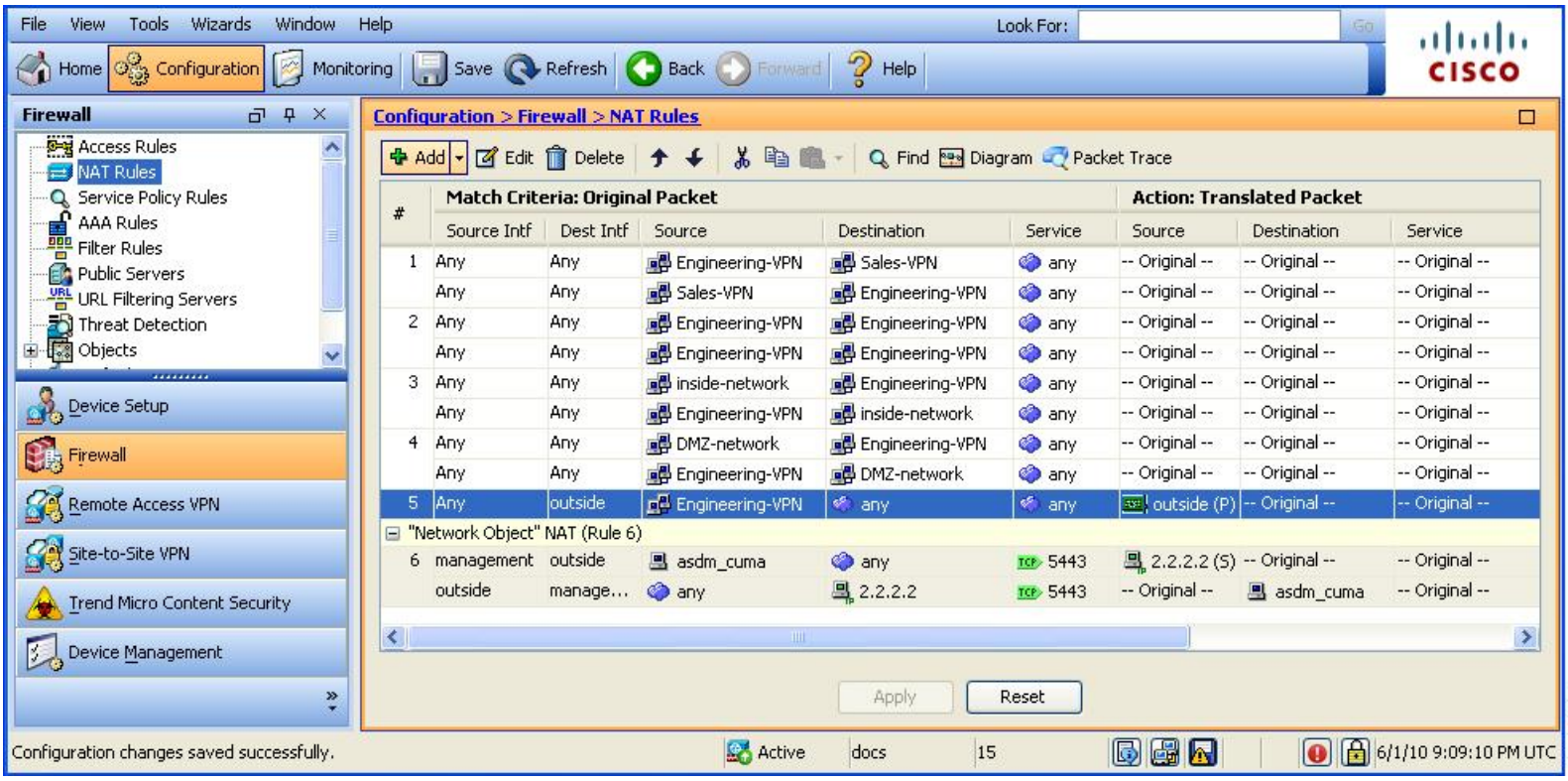
e) **OK(**확인**)**를 클릭합니다.

f) **Apply(**적용**)**을 클릭합니다.

CLI 예:

```
nat (any,outside) source dynamic Engineering-VPN interface
```

그림 *4:* 통합 ***NAT*** 테이블



단계 **8** Engineering VPN 주소 풀이 자신, Sales VPN 주소 풀, 내부 네트워크, DMZ 네트워크 및 인터넷에 연결되도록 구성한 후 Sales VPN 주소 풀에도 같은 프로세스를 반복해야 합니다. ID NAT를 사용하여 자신, 내부 네트워크, DMZ 네트워크, 인터넷 간에 기본 네트워크 주소 변환에서 Sales VPN 주소 풀 트래픽을 제외합니다.

단계 **9** ASA의 **File(**파일**)** 메뉴에서 **Save Running Configuration to Flash(**실행 중인 구성을 플래시에 저장**)**를 선택하여 ID NAT 규칙을 구현합니다.

AnyConnect HostScan

AnyConnect Posture 모듈은 호스트에 설치된 운영 체제, 안티바이러스, 안티스파이웨어, 및 방화벽 소프트웨어를 식별하는 기능을 AnyConnect Secure Mobility Client에 제공합니다. HostScan 애플리케이션은 이 정보를 수집합니다. 상태 진단의 경우 HostScan을 호스트에서 설치해야 합니다.

HostScan에 대한 사전 요구 사항

Posture 모듈이 있는 AnyConnect Secure Mobility Client는 다음과 같은 최소 ASA 구성 요소가 필요합니다.

- ASA 8.4

- ASDM 6.4

이러한 AnyConnect 기능을 사용하려면 Posture 모듈을 설치해야 합니다.

- SCEP 인증
- AnyConnect Telemetry 모듈

Posture 모듈은 다음 플랫폼 중 하나에 설치할 수 있습니다.

- Windows 7, 8, 8.1, 10, 10 RS1, RS2 및 RS3(x86(32비트) 및 x64(64비트)
- macOS 10.11, 10.12 및 10.13
- Linux Red Hat 6, 7 및 Ubuntu 14.04(LTS) 및 16.04(LTS)(64비트 전용)

AnyConnect Hostscan에 대한 라이선싱

다음은 Posture 모듈에 대한 AnyConnect 라이센싱 요건입니다.

- 기본 HostScan용 AnyConnect Apex입니다.
- 치료하려면 고급 엔드포인트 진단 라이선스가 필요합니다.

HostScan 패키징

HostScan 패키지를 다음과 같이 독립 실행형 패키지로 ASA에 로드할 수 있습니다. **hostscan-version.pkg** 이 파일에는 HostScan 소프트웨어뿐만 아니라 HostScan 라이브러리 및 지원 차트가 포함되어 있습니다.

HostScan 설치 또는 업그레이드

HostScan 패키지를 설치 또는 업그레이드하고 ASDM을 사용하여 이 패키지를 활성화하려면 다음 절차를 수행하십시오.

시작하기 전에

참고 HostScan 버전 4.3.x 이전 버전에서 HostScan 4.6.x 이상으로 업그레이드를 시도 중인 경우, 모든 기존 AV/AS/FW DAP 정책 및 이전에 설정한 LUA 스크립트가 HostScan 4.6.x 이상과 호환되지 않기 때문에 오류 메시지를 받게 됩니다.

구성에 맞게 수행해야 하는 일회성 마이그레이션 절차가 있습니다. 이 절차에서는 이 구성을 저장하기 전에 HostScan 4.4.x와 호환되도록 구성을 마이그레이션하기 위해 이 대화 상자를 그대로 둡니다. 자세한 내용을 보려면 이 절차를 중단하고 AnyConnect HostScan 4.3.x~4.6.x 마이그레이션 가이드를 참고하십시오. 간략하게 설명하자면, 마이그레이션에는 검토할 ASDM DAP 정책 페이지로 이동하고, 호환되지 않는 AV/AS/FW 속성을 수동으로 삭제한 다음 LUA 스크립트를 검토하고 재작성하는 작업이 포함됩니다.

프로시저

단계 **1** hostscan_version-k9.pkg 파일을 컴퓨터에 다운로드합니다.

단계 **2** ASDM을 열고 **Configuration(**구성**) > Remote Access VPN(**원격 액세스 **VPN) > Secure Desktop Manager(Secure Desktop** 관리자**) > Host Scan Image(Host Scan** 이미지**)** > 를 선택합니다.

단계 **3** **Upload(**업로드**)**를 클릭하여 사용자 컴퓨터에서 ASA의 드라이브로 HostScan 패키지 사본을 전송할 준비를 합니다.

단계 **4** Upload Image(이미지 업로드) 대화 상자에서 **Browse Local Files(**로컬 파일 찾아보기**)**를 클릭하여 로컬 컴퓨터에서 HostScan 패키지를 검색합니다.

단계 **5** 위에서 다운로드한 hostscan_*version*-k9.pkg 파일을 선택하고 **Select(**선택**)**를 클릭합니다. 선택한 파일의 경로는 Local File Path(로컬 파일 경로) 필드에 있으며, Flash File System Path(플래시 파일 시스템 경로) 필드는 HostScan 패키지의 대상 경로를 나타냅니다. ASA에 둘 이상의 플래시 드라이브가 있는 경우 Flash File System Path(플래시 파일 시스템 경로)를 수정하여 다른 플래시 드라이브를 지정할 수 있습니다.

단계 **6** **Upload File(**파일 업로드**)**을 클릭합니다. ASDM에서 파일의 사본을 플래시 카드로 전송합니다. 파일을 플래시에 성공적으로 업로드했음을 표시하는 Information(정보) 대화 상자가 표시됩니다.

단계 **7** **OK(**확인**)**를 클릭합니다.

단계 **8** Use Uploaded Image(업로드한 이미지 사용) 대화 상자에서 **OK(**확인**)**를 클릭하여 방금 현재 이미지로 업로드한 HostScan 패키지 파일을 사용합니다.

단계 **9** 아직 선택하지 않은 경우 **Enable HostScan(HostScan** 활성화**)**을 선택합니다.

단계 **10** **Apply(**적용**)**를 클릭합니다.

단계 **11** File(파일) 메뉴에서 **Save Running Configuration To Flash(**실행 중인 구성을 플래시에 저장**)**를 선택합니다.

HostScan 제거

HostScan 패키지를 제거하면 ASDM 인터페이스에 있는 보기에서 제거되며 HostScan이 활성화된 경우에도 ASA가 이를 배포하는 것이 방지됩니다. HostScan을 제거해도 플래시 드라이브에서 HostScan 패키지는 삭제되지 않습니다.

프로시저

단계 **1** ASDM에서 **Configuration(**구성**) > Remote Access VPN(**원격 액세스 **VPN) > Secure Desktop Manager(Secure Desktop** 관리자**) > Host Scan Image(Host Scan** 이미지**)** > 로 이동하여 HostScan을 제거합니다.

단계 **2** **Uninstall(**제거**)**을 클릭하고 **Yes(**예**)**를 클릭하여 확인합니다.

단계 **3** **Uninstall(**제거**)**을 클릭합니다.

그룹 정책에 AnyConnect 기능 모듈 할당

이 절차에서는 AnyConnect 기능 모듈을 그룹 정책과 연계합니다. VPN 사용자가 ASA에 연결하는 경우 ASA는 엔드포인트 컴퓨터에 이 AnyConnect 기능 모듈을 다운로드하여 설치합니다.

시작하기 전에

ASA에 로그온하고 전역 구성 모드를 시작합니다. 전역 구성 모드에서 ASA에 다음 확인 상자가 표시됩니다. hostname(config)#

프로시저

단계 **1** 네트워크 클라이언트 액세스를 위해 내부 그룹 정책을 추가합니다.

group-policy *name* **internal**

예제**:**

```
hostname(config)# group-policy PostureModuleGroup internal
```

단계 **2** 새 그룹 정책을 수정합니다. 명령을 입력한 다음 그룹 정책 구성 모드에 대해 확인 상자 hostname(config-group-policy)#를 받습니다.

group-policy *name* **attributes**

예제**:**

```
hostname(config)# group-policy PostureModuleGroup attributes
```

단계 **3** 그룹 정책 webvpn 구성 모드를 시작합니다. 명령을 입력하면 ASA가 다음 확인 상자를 반환합니다. hostname(config-group-webvpn)#

webvpn

단계 **4** 그룹의 모든 사용자에 대해 AnyConnect 기능 모듈을 다운로드하도록 그룹 정책을 구성합니다.

anyconnect modules value *AnyConnect Module Name*

anyconnect 모듈 명령 값은 다음 값 중 하나 이상을 포함할 수 있습니다. 두 개 이상의 모듈을 지정하는 경우 값을 쉼표로 구분합니다.

값	**AnyConnect** 모듈 이름
dart	AnyConnect DART(Diagnostics and Reporting Tool)
vpngina	AnyConnect SBL(Start Before Logon)
websecurity	AnyConnect Web Security Module
telemetry	AnyConnect Telemetry 모듈
posture	AnyConnect Posture 모듈
nam	Cisco AnyConnect Network Access Manager
none	그룹 정책에서 모든 AnyConnect 모듈을 제거하기 위해 자체에서 사용됩니다.

예제**:**

```
hostname(config-group-webvpn)# anyconnect modules value websecurity,telemetry,posture
```

모듈 중 하나를 제거하려면 유지하려는 모듈 값만 지정하는 명령을 다시 전송합니다. 예를 들어 다음 명령은 WebSecurity 모듈을 제거합니다.

```
hostname(config-group-webvpn)# anyconnect modules value telemetry,posture
```

단계 **5** 실행 중인 구성을 플래시에 저장합니다.

플래시 메모리에 새 구성을 성공적으로 저장한 이후에 [OK] 메시지를 받으며 ASA는 다음 확인 상자를 반환합니다. hostname(config-group-webvpn)#

write memory

HostScan 관련 문서

HostScan이 엔드포인트 컴퓨터에서 상태 크리덴셜을 수집하면 해당 정보를 활용하기 위해 동적 액세스 정책 구성 및 LUA 표현식 사용과 같은 주제를 이해해야 합니다.

이 주제에 대해서는 다음 문서에서 자세히 다룹니다.

- Cisco Secure Desktop 구성 가이드
- Cisco Adaptive Security Device Manager 구성 가이드

HostScan이 AnyConnect 클라이언트에서 작동하는 방식에 대한 자세한 내용은 Cisco *AnyConnect Secure Mobility Client* 관리자 가이드를 참고하십시오.

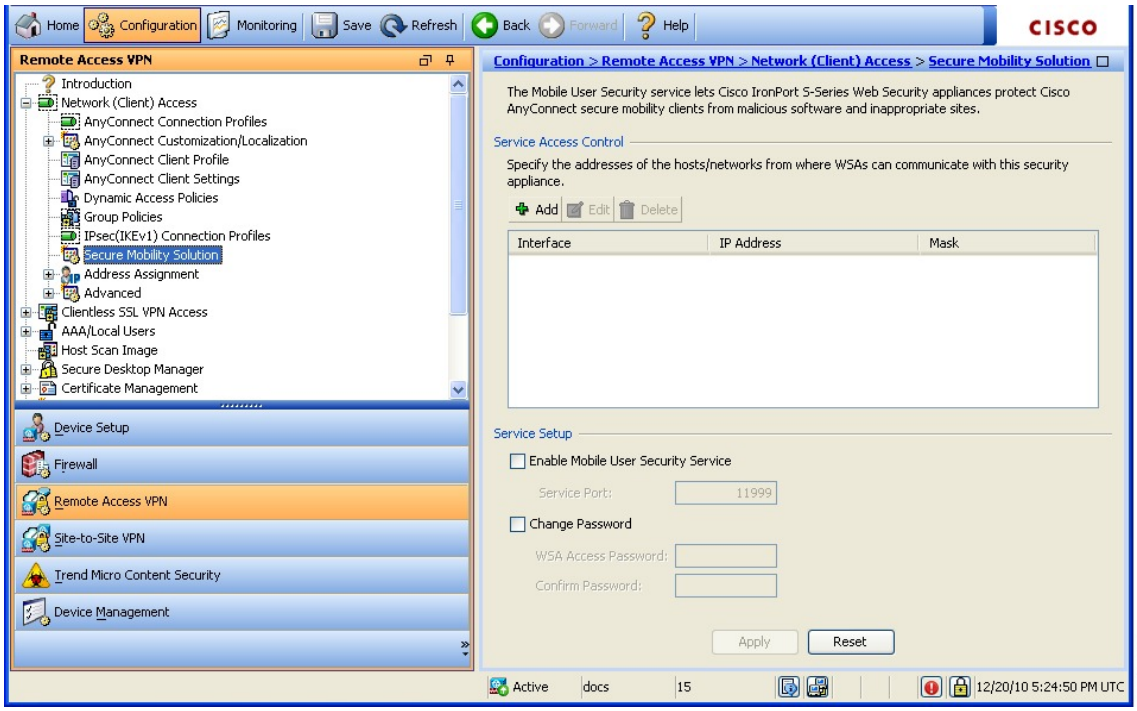
AnyConnect Secure Mobility Solution

AnyConnect Secure Mobility는 직원이 이동 중일 때 인터넷 위협으로부터 기업의 이익과 자산을 보호합니다. AnyConnect Secure Mobility는 Cisco IronPort S-Series Web Security Appliance에서 Cisco AnyConnect Secure Mobility Client를 검사하여 악성 소프트웨어 및/또는 부적절한 사이트로부터 클라이언트를 보호합니다. 클라이언트는 Cisco IronPort S-Series Web Security Appliances 보호가 활성화되어 있는지 정기적으로 확인합니다.

참고 이 기능에는 Cisco AnyConnect Secure Mobility Client에 대한 AnyConnect Secure Mobility 라이센싱 지원을 제공하는 Cisco IronPort Web Security Appliance 릴리스가 필요합니다. 또한 AnyConnect Secure Mobility 기능을 지원하는 AnyConnect 릴리스가 필요합니다. AnyConnect 3.1 이상에서는 이 기능을 지원하지 않습니다.

보안 모바일 솔루션을 구성하려면 **Configuration(**구성**) > Remote Access VPN(**원격 액세스 **VPN) > Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**) > Secure Mobility Solution(**보안 모빌리티 솔루션**)**을 선택합니다.

그림 ***5: Mobile User Security(***모바일 사용자 보안***)*** 창



- Service Access Control(서비스 액세스 제어) - WSA에서 통신할 수 있는 호스트 또는 네트워크 주소를 지정합니다.
  - Add(추가) - 선택한 연결에 대한 Add MUS Access Control Configuration(MUS 액세스 제어 구성 추가) 대화 상자를 엽니다.
  - Edit(수정) - 선택한 연결에 대한 Edit MUS Access Control Configuration(MUS 액세스 제어 구성 수정) 대화 상자를 엽니다.
  - Delete(삭제) - 테이블에서 선택한 연결을 제거합니다. 확인 또는 실행 취소가 없습니다.
- Enable Mobile User Security Service(모바일 사용자 보안 서비스 활성화) - VPN을 통해 클라이언트와의 연결을 시작합니다. 활성화된 경우 ASA에 연결할 때 WSA에서 사용하는 비밀번호를 입력해야 합니다. WSA가 없는 경우에는 상태가 비활성화됩니다.
- Service Port(서비스 포트) - 서비스를 활성화하려는 경우 사용할 서비스의 포트 번호를 지정합니다. 포트 번호는 1~65535이며, 관리 시스템을 통해 WSA에 프로비저닝된 해당 값과 일치해야 합니다. 기본값은 11999입니다.
- Change Password(비밀번호 변경) - WSA 액세스 비밀번호를 변경할 수 있습니다.
- WSA Access Password(WSA 액세스 비밀번호) - ASA와 WSA 간의 인증에 필요한 공유 비밀번호를 지정합니다. 이 비밀번호는 관리 시스템을 통해 WSA에 프로비저닝된 해당 값과 일치해야 합니다.
- Confirm Password(비밀번호 확인) - 지정한 비밀번호를 다시 입력합니다.

- Show WSA Sessions(WSA 세션 표시) - ASA에 연결된 WSA의 세션 정보를 볼 수 있습니다. 연결할(또는 연결된) WSA의 호스트 IP 주소 및 연결 기간이 대화 상자에 반환됩니다.

MUS 액세스 제어 추가 또는 수정

Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > Network (Client) Access(네트워크(클라이언트) 액세스) > Secure Mobility Solution(보안 모빌리티 솔루션) 아래의 Add or Edit MUS Access Control(MUS 액세스 제어 추가 또는 수정) 대화 상자에서는 AnyConnect 클라이언트에 대한 MUS(Mobile User Security) 액세스를 구성합니다.

- Interface Name(인터페이스 이름) - 드롭다운 목록을 사용하여 추가하거나 수정할 인터페이스 이름을 선택합니다.
- IP Address(IP 주소) - IPv4 또는 IPv6 주소를 입력합니다.
- Mask(마스크) - 드롭다운 목록을 사용하여 적절한 마스크를 선택합니다.

AnyConnect 사용자 지정 및 현지화

AnyConnect VPN 클라이언트를 사용자 지정하여 원격 사용자에게 기업 고유의 이미지를 표시할 수 있습니다. AnyConnect Customization/Localization(AnyConnect 사용자 지정/현지화) 아래에 있는 다음 필드에서 다음과 같은 유형의 사용자 지정 파일을 가져올 수 있습니다.

- **Resources**- AnyConnect 클라이언트에 대해 수정된 GUI 아이콘.
- **Binary**- AnyConnect 설치 프로그램을 바꾸는 실행 파일. 여기에는 GUI 파일뿐 아니라 VPN 클라이언트 프로파일, 스크립트 및 기타 클라이언트 파일이 포함됩니다.
- **Script**- AnyConnect에서 VPN 연결을 설정하기 전 또는 후에 실행될 스크립트.
- **GUI Text and Messages**- AnyConnect 클라이언트에서 사용하는 제목 및 메시지.
- **Customized Installer**- 클라이언트 설치 프로그램을 수정하는 변형.
- **Localized Installer**- 클라이언트에서 사용하는 언어를 변경하는 변형.

각 대화 상자에서는 다음 작업을 제공합니다.

- **Import(**가져오기**)**는 Import AnyConnect Customization Objects(AnyConnect 사용자 지정 개체 가져오기) 대화 상자를 실행합니다. 이 대화 상자에서 개체로 가져올 파일을 지정할 수 있습니다.
- **Export(**내보내기**)**는 Export AnyConnect Customization Objects(AnyConnect 사용자 지정 개체 내보내기) 대화 상자를 실행합니다. 이 대화 상자에서 개체로 가져올 파일을 지정할 수 있습니다.
- **Delete(**삭제**)**는 선택된 개체를 제거합니다.

참고 이 기능은 다중 상황 모드에서 지원되지 않습니다.

AnyConnect 사용자 지정 및 현지화, 리소스

가져오는 사용자 지정 구성 요소의 파일 이름은 AnyConnect GUI에서 사용되는 파일 이름과 일치해야 합니다. 이 파일 이름은 운영 체제마다 다르며 Mac과 Linux에서는 대/소문자를 구분합니다. 예를 들어 Windows 클라이언트의 기업 로고를 교체하려는 경우 company_logo.png로 기업 로고를 가져와야 합니다. 다른 파일 이름으로 가져오는 경우 AnyConnect 설치 프로그램이 구성 요소를 변경하지 않습니다. 그러나 GUI를 사용자 지정하기 위해 고유한 실행 파일을 구축할 경우 실행 파일이 어떤 파일 이름으로든 리소스 파일을 호출할 수 있습니다.

리소스 파일(예: company_logo.bmp)로 이미지를 가져오는 경우, 가져온 이미지는 같은 파일 이름을 사용하여 다른 이미지를 다시 가져올 때까지 AnyConnect를 사용자 지정합니다. 예를 들어 company_logo.bmp를 사용자 지정 이미지로 교체하고 해당 이미지를 삭제할 경우, 클라이언트는 같은 파일 이름을 사용하여 새 이미지(또는 원래 Cisco 로고 이미지)를 가져올 때까지 계속해서 사용자 지정 이미지를 표시합니다.

AnyConnect 사용자 지정 및 현지화, 이진 및 스크립트

AnyConnect 맞춤화/현지화, 이진

Windows, Linux 또는 Mac(PowerPC 또는 Intel 기반) 컴퓨터의 경우 AnyConnect 클라이언트 API를 사용하는 고유의 클라이언트를 구축할 수 있습니다. 클라이언트 이진 파일을 대체하여 AnyConnect GUI 및 AnyConnect CLI를 대체합니다.

Import 대화 상자의 필드:

- **Name** 대체하는 AnyConnect 파일의 이름을 입력합니다.
- **Platform** 파일이 실행되는 OS 플랫폼을 선택합니다.
- **Select a file** 파일 이름이 가져온 파일 이름과 같을 필요는 없습니다.

AnyConnect 맞춤화/현지화, 스크립트

스크립트 구축에 대한 전체 정보와 한계 및 제한 사항은 AnyConnect VPN 클라이언트 관리자 가이드를 참조하십시오.

Import 대화 상자의 필드:

- **Name**- 스크립트 이름을 입력합니다. 이름과 확장명을 올바르게 지정해야 합니다. 예: myscript.bat.
- **Script Type**- 스크립트 실행 시기를 선택합니다.

  AnyConnect는 ASA에서 해당 파일을 스크립트로 식별하기 위해 파일 이름에 접두사 scripts_ 및 접두사 OnConnect 또는 OnDisconnect를 추가합니다. 클라이언트가 연결되면 ASA에서는 원격

컴퓨터에 있는 적합한 대상 디렉토리에 스크립트를 다운로드하고 scripts_ 접두사를 제거하며 OnConnect 또는 OnDisconnect 접두사는 그대로 둡니다. 예를 들어 스크립트 myscript.bat를 가져오면 스크립트는 scripts_OnConnect_myscript.bat로 ASA에 나타납니다. 원격 컴퓨터에서는 스크립트가 OnConnect_myscript.bat로 나타납니다.

스크립트를 안정적으로 실행하려면 동일한 스크립트를 구축하도록 모든 ASA를 구성합니다. 스크립트를 수정하거나 교체하려는 경우, 이전 버전과 동일한 이름을 사용하고 사용자가 연결할 수 있는 모든 ASA에 교체 스크립트를 할당합니다. 사용자가 연결하면 새로운 스크립트가 동일한 이름으로 스크립트를 덮어씁니다.

- **Platform**- 파일이 실행되는 OS 플랫폼을 선택합니다.
- **Select a file**- 파일 이름이 스크립트에 입력한 이름과 같을 필요는 없습니다.

ASDM에서는 모든 소스 파일에서 파일을 가져오고, Name(이름)에 지정하는 새 이름을 만듭니다.

AnyConnect 사용자 지정 및 현지화, GUI 텍스트 및 메시지

기본 변환 테이블을 수정하거나 새로 만들어서 AnyConnect 클라이언트 GUI에 표시되는 텍스트 및 메시지를 변경할 수 있습니다. 또한 이 창은 Language Localization(언어 현지화) 창과 기능을 공유합니다. 보다 광범위한 언어 변환이 필요할 경우 **Configuration(**구성**) > Remote Access VPN(**원격 액세스 **VPN) > Language Localization(**언어 현지화**)**으로 이동합니다.

상단에 있는 툴바의 일반적인 버튼 외에도 이 창에는 **Add** 버튼 그리고 여러 추가 버튼이 제공되는 Template(템플릿) 영역이 있습니다.

Add- Add(추가) 버튼을 클릭하면 바로 수정하거나 저장할 수 있는 기본 변환 테이블 사본이 열립니다. 저장된 파일의 언어를 선택하고, 나중에 파일 내에서 텍스트 언어를 수정할 수 있습니다.

변환 테이블의 메시지를 사용자 지정할 때 msgid를 변경하지 말고 msgstr의 텍스트를 변경하십시오.

템플릿 언어를 지정합니다. 템플릿은 캐시 메모리에서 지정한 이름을 지닌 변환 테이블이 됩니다. 브라우저의 언어 옵션과 호환되는 약어를 사용합니다. 예를 들어 중국어용으로 테이블을 생성하고 IE를 사용 중인 경우, IE에서 인식할 수 있는 약어인 *zh*를 사용합니다.

템플릿 섹션

- Template(템플릿)을 클릭하여 템플릿 영역을 확장하면 기본 English(영어) 변환 테이블에 액세스할 수 있습니다.
- **View**를 클릭하여 기본 English(영어) 변환 테이블을 보고, 필요에 따라 저장할 수 있습니다.
- **Export**를 클릭하여 기본 English(영어) 변환 테이블을 보지 않고 사본을 바로 저장할 수 있습니다.

AnyConnect 사용자 지정 및 지역화, 사용자 지정된 설치 프로그램 변형

클라이언트 설치 프로그램과 함께 구축되는 고유의 변형을 만들어서 AnyConnect 클라이언트 GUI(Windows만 해당)를 보다 광범위하게 사용자 지정할 수 있습니다. ASA로 변형을 가져와서 설치 프로그램과 함께 구축합니다.

Windows에만 변형을 적용할 수 있습니다. 변형에 대한 자세한 내용은 *Cisco AnyConnect Secure Mobility Client* 관리자 가이드를 참고하십시오.

AnyConnect 사용자 지정 및 현지화, 현지화된 설치 프로그램 변형

클라이언트 설치 프로그램에서 변형과 함께 표시하는 메시지를 변환할 수 있습니다. 이 변환은 설치를 변경하지만 원래의 보안 서명된 MSI를 그대로 유지합니다. 이 변환은 설치 프로그램의 화면만 변환하며 클라이언트 GUI 화면은 변환하지 않습니다.

AnyConnect 3.1용 AnyConnect Essentials

AnyConnect Essentials는 별도로 라이선스가 제공되는 SSL VPN 클라이언트로, ASA에 완전히 구성되어 다음을 제외한 모든 AnyConnect 기능을 제공합니다.

- 클라이언트리스 SSL VPN 없음
- 선택적 Windows Mobile 지원(Windows Mobile용 AnyConnect 라이센스 필요)

AnyConnect Essentials 클라이언트는 Microsoft Windows Vista, Windows Mobile, Windows XP, Windows 2000, Linux 또는 Macintosh OS X을 실행하는 원격 엔드 유저가 Cisco SSL VPN 클라이언트의 이점을 누릴 수 있게 합니다.

AnyConnect Essentials를 활성화하려면 AnyConnect Essentials 창에서 **Enable AnyConnect Essentials(AnyConnect Essentials** 활성화**)** 확인란을 선택합니다. 이 창은 ASA에 AnyConnect Essentials 라이선스가 설치된 경우에만 나타납니다.

AnyConnect Essentials가 활성화되면 AnyConnect 클라이언트에서 Essentials 모드를 사용하고, 클라이언트리스 SSL VPN 액세스가 비활성화됩니다. AnyConnect Essentials가 비활성화되면 AnyConnect 클라이언트에서 전체 AnyConnect SSL VPN 클라이언트를 사용합니다.

참고 Configuration(구성) > Device Management(디바이스 관리) > Licensing(라이센싱) > Activation Key(액티베이션 키) 창의 AnyConnect Essentials 라이센스에 대한 상태 정보는 AnyConnect Essentials 라이센스가 설치되었는지 여부만 보여줍니다. 이 상태는 Enable AnyConnect Essentials License(AnyConnect Essentials 라이센스 활성화) 확인란 설정의 영향을 받지 않습니다.

활성 클라이언트리스 세션이 디바이스에 존재하는 경우에는 AnyConnect Essentials 모드를 활성화할 수 없습니다. SSL VPN 세션 세부사항을 보려면 SSL VPN Sessions(SSL VPN 세션) 섹션에서 **Monitoring(**모니터링**) > VPN > VPN Sessions(VPN** 세션**)** 링크를 클릭합니다. 그러면 Monitoring(모니터링) > VPN > VPN > VPN Statistics(VPN 통계) > Sessions(세션) 창이 열립니다. 세션 세부사항을 보

려면 **Filter By: Clientless SSL VPN(**필터링 기준**:** 클라이언트리스 **SSL VPN)**을 선택하고 **Filter(**필터**)**를 클릭합니다. 그러면 세션 세부사항이 표시됩니다.

세션 세부사항을 표시하지 않고 현재 활성 상태의 클라이언트리스 SSL VPN 세션 수를 보려면 **Check Number of Clientless SSL Sessions(**클라이언트리스 **SSL** 세션 수 확인**)**를 클릭합니다. SSL VPN 세션 수가 0인 경우 AnyConnect Essentials를 활성화할 수 있습니다.

참고 AnyConnect Essentials가 활성화된 경우에는 Secure Desktop이 작동하지 않습니다. 그러나 Secure Desktop을 활성화한 경우 AnyConnect Essentials를 비활성화할 수 있습니다.

AnyConnect 맞춤형 속성

맞춤형 속성은 AnyConnect 클라이언트로 전송되어 아래와 같은 기능을 구성하는 데 사용됩니다. 사용자 지정 특성에는 유형 및 명명된 값이 있습니다. 사전 정의된 사용자 지정 특성은 동적 액세스 정책과 그룹 정책 모두에서 사용됩니다. 다음과 같이 다양한 용도로 맞춤형 속성을 생성 및 설정합니다.

- **DSCP** 보존 활성화 - 이 맞춤형 속성을 설정하여 DTLS 연결을 위해 Windows 또는 Mac 운영 체제 플랫폼에서 DSCP(Differentiated Services Code Point)를 제어합니다. DSCPPreservationAllowed 맞춤형 속성 유형을 사용하면 디바이스가 레이턴시에 민감한 트래픽의 우선순위를 지정하고 우선순위가 지정된 트래픽을 표시하여 아웃바운드 연결 품질을 개선합니다. 자세한 내용은 *DSCP* 보존 활성화: http://www.cisco.com/c/en/us/td/docs/security/asa/asa98/configuration/vpn/asa-98-vpn-config/vpn-anyconnect.html 또는 http://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect44/administration/guide/b_AnyConnect_Administrator_Guide_4-4/customize-localize-anyconnect.html#reference_3B013688EC044313806A5A8557241CC5의 내용을 참고하십시오.
- 보류 업데이트를 **ASA**에서 활성화 - 이러한 맞춤형 속성이 구성되어 있고 클라이언트 업데이트를 사용할 수 있는 경우, AnyConnect가 업데이트할지 또는 보류할지를 묻는 대화 상자를 엽니다. 보류 업데이트에 대한 맞춤형 속성의 몇 가지 예로는 ASA의 버전에 따라 DeferredUpdateAllowed, DeferredUpdateMinimumVersion, DeferredUpdateDismissTimeout 및 DeferredDismissResponse가 있습니다. 자세한 내용은 *AnyConnect* 클라이언트 보류 업그레이드 활성화:http://www.cisco.com/c/en/us/td/docs/security/asa/asa98/configuration/vpn/asa-98-vpn-config/vpn-anyconnect.html 또는 http://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect44/administration/guide/b_AnyConnect_Administrator_Guide_4-4/deploy-anyconnect.html#ID-1425-0000047a의 내용을 참고하십시오.
- 동적 스플릿 터널링을 활성화 - 이 맞춤형 속성을 생성하여 호스트 DNS 도메인 이름을 기준으로 하여 터널 설정 후 스플릿 제외 터널링을 동적으로 프로비저닝할 수 있습니다. 동적 스플릿 제외 도메인을 추가하여 VPN 터널 외부에서 클라이언트에 액세스해야 하는 클라우드 또는 웹 서비스를 입력할 수 있습니다. 자세한 내용은 동적 스플릿 터널링 구성을 참고하십시오.
- 공용 **DHCP** 서버 경로를 설정 - 이 맞춤형 속성을 사용하여 Tunnel All Networks(모든 네트워크 터널링)가 구성된 경우 로컬 DHCP 트래픽을 투명하게 전송할 수 있습니다. AnyConnect는 AnyConnect 클라이언트를 연결하고 호스트 머신의 LAN 어댑터에 암시적 필터를 적용할 때 로

컬 DHCP 서버에 특정한 경로를 추가하여 해당 경로에 대해 DHCP 트래픽을 제외한 모든 트래픽을 차단합니다. 터널 설정 시 공용 DHCP 서버 경로를 만들지 않으려면 no-dhcp-server-route 맞춤형 속성이 있어야 하며 true로 설정해야 합니다. 추가 정보는 http://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect44/administration/guide/b_AnyConnect_Administrator_Guide_4-4/customize-localize-anyconnect.html#reference_1EF86D88C02C4E05AAD9DC5553A13D40 내용을 참조하십시오.

- 확장된 서브넷을 지원하도록 **Linux**를 구성 -

  circumvent-host-filtering 맞춤형 속성은 Linux가 스플릿 터널링에 대해 Tunnel Network List Below(아래 네트워크 목록 터널링)가 구성된 경우 제외된 서브넷을 지원하도록 설정합니다. 추가 정보는 확장된 서브넷을 지원하도록 Linux 구성, 81 페이지 내용을 참조하십시오.

이러한 기능을 추가로 사용하려면 정의된 맞춤형 속성 대부분을 **Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > Network (Client) Access(네트워크(클라이언트) 액세스) > Group Polices(그룹 정책)** > 메뉴에 있는 특정 그룹 정책에 연결해야 합니다.

IPsec VPN 클라이언트 소프트웨어

참고 **VPN** 클라이언트는 단종되고 지원이 중단되었습니다**.** VPN 클라이언트 구성에 대한 자세한 내용은 ASA 버전 9.2에 대한 ASDM 설명서를 참조하십시오. **Cisco AnyConnect Secure Mobility Client**로 업그레이드할 것을 권장합니다**.**

Zone Labs Integrity 서버

Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > Network (Client) Access(네트워크(클라이언트) 액세스) > Advanced(고급) > IPsec > Zone Labs Integrity Server(Zone Labs Integrity 서버) 패널에서는 ASA가 Zone Labs Integrity 서버를 지원하도록 구성할 수 있습니다. 이 서버는 비공개 네트워크에 연결하는 원격 클라이언트에 보안 정책을 적용하도록 설계된 시스템인 무결성 시스템의 일부입니다. 기본적으로 ASA는 클라이언트 PC와 방화벽 서버 간의 프록시 역할을 하며, 무결성 클라이언트와 무결성 서버 간에 필요한 모든 무결성 정보를 릴레이합니다.

참고 사용자 인터페이스에서 최대 5개의 Integrity 서버 구성을 지원하지만 보안 어플라이언스의 현재 릴리스는 한 번에 하나의 Integrity 서버를 지원합니다. 활성 서버가 실패한 경우 ASA에서 다른 Integrity 서버를 구성한 다음 클라이언트 VPN 세션을 다시 설정합니다.

- **Server IP address(서버 IP 주소)** - Integrity 서버의 IP 주소를 입력합니다. 십진수 표기법을 사용하세요.
- **Add(추가)** - Integrity 서버 목록에 새 서버 IP 주소를 추가합니다. 이 버튼은 Server IP address(서버 IP 주소) 필드에 주소를 입력하면 활성화됩니다.

- **Delete(**삭제**)** - Integrity 서버 목록에서 선택한 서버를 삭제합니다.
- **Move Up(**위로 이동**)** - Integrity 서버 목록에서 선택한 서버를 위로 이동합니다. 이 버튼은 목록에 둘 이상의 서버가 있는 경우에만 사용할 수 있습니다.
- **Move Down(**아래로 이동**)** - Integrity 서버 목록에서 선택한 서버를 아래로 이동합니다. 이 버튼은 목록에 둘 이상의 서버가 있는 경우에만 사용할 수 있습니다.
- **Server Port(**서버 포트**)** - ASA에서 활성 Integrity 서버를 수신 대기할 포트 번호를 입력합니다. 이 필드는 Integrity 서버 목록에 하나 이상의 서버가 있는 경우에만 사용할 수 있습니다. 기본 포트 번호는 5054이며, 범위는 10~10000입니다. 이 필드는 Integrity 서버 목록에 서버가 있는 경우에만 사용할 수 있습니다.
- **Interface(**인터페이스**)** - ASA에서 활성 Integrity 서버와 통신할 인터페이스를 선택합니다. 이 인터페이스 이름 메뉴는 Integrity 서버 목록에 서버가 있는 경우에만 사용할 수 있습니다.
- **Fail Timeout(**실패 시간 제한**)** - ASA에서 활성 Integrity 서버에 연결할 수 없는 것으로 선언하기 전에 대기할 시간(초)을 입력합니다. 기본값은 10이며, 범위는 5~20입니다.
- **SSL Certificate Port(SSL** 인증서 포트**)** - SSL 권한 부여에 사용할 ASA 포트를 지정합니다. 기본값은 포트 80입니다.
- **Enable SSL Authentication(SSL** 인증 활성화**)** - ASA의 원격 클라이언트 SSL 인증서 인증을 활성화하려면 선택합니다. 클라이언트 SSL 인증은 기본적으로 비활성화되어 있습니다.
- **Close connection on timeout(**시간 초과 시 연결 닫기**)** - 시간 초과 시 ASA와 Integrity 서버 간의 연결을 닫으려면 선택합니다. 기본적으로 연결은 열린 상태로 유지됩니다.
- **Apply(**적용**)** - 구성을 실행 중인 ASA에 Integrity 서버 설정을 적용하려면 클릭합니다.
- **Reset(**재설정**)** - 아직 적용되지 않은 Integrity 서버 구성 변경 사항을 제거하려면 클릭합니다.

ISE 정책 시행

Cisco ISE(Identity Services Engine)는 보안 정책 관리 및 제어 플랫폼입니다. 유선, 무선 및 VPN 연결의 액세스 제어와 보안 컴플라이언스를 자동화하고 간소화해줍니다. Cisco ISE는 주로 Cisco TrustSec과 연계하여 보안 액세스 및 게스트 액세스를 제공하고 BYOD(Bring Your Own Device) 이니셔티브를 지원하고 사용량 정책을 적용하는 데 쓰입니다.

ISE CoA(Change of Authorization: 권한 부여 변경) 기능은 설정 후 AAA(인증, 권한 부여 및 계정 관리) 세션의 특성을 변경하는 메커니즘을 제공합니다. 정책이 AAA의 사용자 또는 사용자 그룹을 변경하는 경우 CoA 패킷이 ISE에서 ASA로 직접 연결되어 인증을 다시 시작하고 새 정책을 적용할 수 있습니다. IPEP(Inline Posture Enforcement Point: 인라인 상태 시행 지점)에는 ASA로 설정된 각 VPN 세션에 대한 ACL(Access Control List: 액세스 제어 목록)이 필요하지 않습니다.

ISE 정책 시행은 다음과 같은 VPN 클라이언트에서 지원됩니다.

- IPSec
- AnyConnect

- L2TP/IPSec

시스템 흐름은 다음과 같습니다.

1. 엔드 유저가 VPN 연결을 요청합니다.
2. ASA가 ISE에 대한 사용자를 인증하고 네트워크에 제한된 액세스를 제공하는 사용자 ACL을 수신합니다.
3. 세션을 등록할 수 있도록 계정 관리 시작 메시지가 ISE로 전송됩니다.
4. NAC 에이전트 및 ISE 간에 직접 상태 평가가 이루어집니다. 이 프로세스는 ASA에 투명성을 제공합니다.
5. ISE는 CoA "정책 푸시"를 통해 ASA에 정책 업데이트를 전송합니다. 이는 강화된 네트워크 액세스 권한을 제공하는 새 사용자 ACL을 식별합니다.

참고 연결 수명 동안 후속 CoA 업데이트를 통해 ASA에 투명성을 제공하는 추가 정책 평가가 발생할 수 있습니다.

ISE COA(Change of Authorization) 구성

ISE COA(Change of Authorization) 구성에는 ISE RADIUS 서버를 포함하는 서버 그룹을 생성하고 원격 액세스 VPN 구성 프로필(터널)에서 해당 서버 그룹을 사용하는 작업이 포함됩니다.

프로시저

단계 **1** ISE 서버에 대해 RADIUS AAA 서버 그룹을 구성합니다.

다음 절차에서는 최소 구성에 대해 설명합니다. 원하는 대로 그룹에 대해 다른 설정을 조정할 수 있습니다. 대부분의 설정에는 대부분의 네트워크에 적합한 기본값이 있습니다. RADIUS AAA 서버 그룹 구성에 대한 자세한 내용은 일반 구성 가이드를 참고하십시오.

a) **Configuration(**구성**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **AAA/Local Users(AAA/**로컬 사용자**)** > **AAA Server Groups(AAA** 서버 그룹**)**를 선택합니다.
b) **AAA Server Group(AAA** 서버 그룹**)** 영역에서 **Add(**추가**)**를 클릭합니다.
c) **AAA Server Group(AAA** 서버 그룹**)** 필드에 그룹의 이름을 입력합니다.
d) **Protocol(**프로토콜**)** 드롭다운 목록에서 RADIUS 서버 유형을 선택합니다.
e) RADIUS interim-accounting-update 메시지를 정기적으로 생성하게 하려면 **Enable interim accounting update(**중간 어카운팅 업데이트 활성화**)** 및 **Update Interval(**업데이트 간격**)**을 선택합니다.

ISE는 ASA와 같은 NAS 디바이스에서 수신하는 어카운팅 레코드를 기반으로 하는 활성 세션의 디렉터리를 유지합니다. 그러나 ISE가 5일 동안 세션이 여전히 활성 상태(어카운팅 메시지 또는 포스처 트랜잭션)임을 나타내는 메시지를 수신하지 않은 경우 데이터베이스에서 세션 레코

드를 제거합니다. 장기 VPN 연결이 제거되지 않도록 하려면 모든 활성 세션에 대해 정기적으로 ISE에 interim-accounting-update 메시지를 전송하도록 그룹을 구성합니다.

이러한 업데이트를 전송할 간격을 시간 단위로 변경할 수 있습니다. 기본값은 24시간, 범위는 1~120입니다.

f) **Enable dynamic authorization(**동적 인증 활성화**)**을 선택합니다.

이 옵션은 AAA 서버 그룹에 대한 RADIUS Dynamic Authorization(ISE CoA(Change of Authorization)) 서비스를 활성화합니다. VPN 터널에서 서버 그룹을 사용하면 RADIUS 서버 그룹이 CoA 알림에 등록되고 ASA는 ISE에서 보내는 CoA 정책 업데이트를 포트에서 수신합니다. 다른 포트를 사용하도록 ISE 서버가 구성되어 있지 않은 경우, 포트(1700)를 변경하지 마십시오. 유효한 범위는 1024 ~65535입니다.

g) 인증을 위해 ISE를 사용하지 않으려는 경우 **Use authorization only mode(**권한 부여 전용 모드 사용**)**를 선택합니다.

이 옵션은 이 서버 그룹이 권한 부여에 사용될 때 RADIUS Access Request 메시지가 AAA 서버에 대해 정의된 구성된 비밀번호 방식이 아니라 "Authorize Only" 요청으로 작성됨을 의미합니다. RADIUS 서버에 대한 공통 비밀번호를 구성하지 않으면 무시됩니다.

예를 들어, 인증에 이 서버 그룹보다 인증서를 사용하려면 권한 부여 전용 모드를 사용합니다. VPN 터널에서 권한 부여 및 어카운팅에 대한 이 서버 그룹을 계속 사용합니다.

h) 서버 그룹을 저장하려면 **OK(**확인**)**를 클릭합니다.

i) 서버 그룹을 선택한 상태에서 ISE RADIUS 서버를 그룹에 추가하려면 선택한 그룹의 서버 목록에서 **Add(**추가**)**를 클릭합니다.

다음은 키 속성입니다. 필요에 따라 다른 설정에 대한 기본값을 조정할 수 있습니다.

- **Interface Name(**인터페이스 이름**)** - ISE 서버에 도달하기 위해 통과할 인터페이스입니다.
- **Server Name or IP Address(**서버 이름 또는 **IP** 주소**)** - ISE 서버의 호스트 이름 또는 IP 주소입니다.
- (선택 사항). **Server Secret Key(**서버 비밀 키**)** - 연결을 암호화하기 위한 키입니다. 키를 구성하지 않으면 연결이 암호화되지 않습니다(일반 텍스트). 이 키는 대/소문자를 구분하는 최대 127자의 영숫자 문자열로 RADIUS 서버의 키와 같은 값입니다.

j) 그룹에 서버를 추가하려면 **OK(**확인**)**를 클릭합니다.

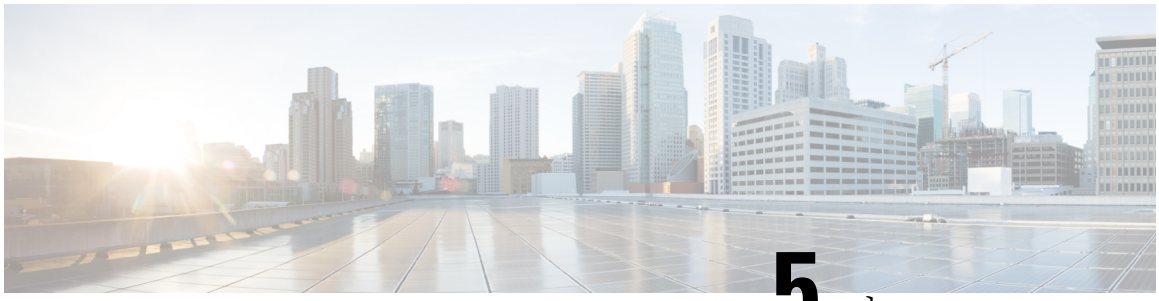
서버 그룹에 추가 ISE 서버를 추가합니다.

단계 **2** ISE 서버 그룹을 사용하도록 원격 액세스 VPN에 대한 구성 프로필을 업데이트합니다.

다음 단계에서는 ISE 관련 구성 옵션만 설명합니다. 작동하는 원격 액세스 VPN을 생성하기 위해 구성해야 하는 다른 옵션이 있습니다. 원격 액세스 VPN을 구현하기 위해 이 가이드의 다른 지침을 따르십시오.

a) **Configuration(**구성**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**)** > **AnyConnect Connection Profiles(AnyConnect** 연결 프로필**)**를 선택합니다.

b) **Connection Profiles(**연결 프로필**)** 테이블에서 프로필을 추가하거나 수정합니다.
c) **Basic(**기본**)** 페이지에서 인증 방법을 구성합니다.
   - 인증을 위해 ISE 서버를 사용하는 경우 **Authentication** > **Method(**인증 방법**)**로 **AAA**를 선택한 다음 ISE AAA 서버 그룹을 선택합니다.
   - 권한 부여에 대해서만 ISE 서버 그룹을 구성하는 경우, 다른 인증 방법(예: **Certificate(**인증서**)**)을 선택합니다.
d) **Advanced(**고급**)** > **Authorization(**권한 부여**)**페이지에서 **Authorization Server Group(**권한 부여 서버 그룹**)**에 대한 ISE 서버 그룹을 선택합니다.
e) **Advanced(**고급**)** > **Accounting(**어카운팅**)** 페이지에서 ISE 서버 그룹을 선택합니다.
f) **OK(**확인**)**를 클릭하여 변경 사항을 저장합니다.



5 장

VPN용 IP 주소

IP 주소 할당 정책 구성

ASA에서는 다음 방법 중 하나 이상을 사용하여 IP 주소를 원격 액세스 클라이언트에 할당할 수 있습니다. 둘 이상의 주소 할당 방법을 구성한 경우에는 ASA에서 IP 주소를 찾을 때까지 각 옵션을 검색합니다. 기본적으로 모든 방법이 활성화되어 있습니다.

- Use authentication server(인증 서버 사용)- 외부 인증, 권한 부여 및 어카운트 관리 서버에서 사용자 단위로 주소를 검색합니다. IP 주소가 구성된 인증 서버를 사용하는 경우 이 방법을 사용하는 것이 좋습니다. Configuration(구성) > AAA Setup(AAA 설정) 창에서 AAA 서버를 구성할 수 있습니다.IPv4 및 IPv6 할당 정책에 이 방법을 사용할 수 있습니다.

- Use DHCP(DHCP 사용)- DHCP 서버에서 IP 주소를 가져옵니다. DHCP를 사용하려면 DHCP 서버를 구성해야 합니다. DHCP 서버에서 사용할 수 있는 IP 주소 범위도 정의해야 합니다. DHCP를 사용하는 경우 Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > DHCP Server(DHCP 서버) 창에서 서버를 구성합니다. IPv4 할당 정책에 이 방법을 사용할 수 있습니다.

- **Use an internal address pool(**내부 주소 풀 사용**) -** 내부적으로 구성된 주소 풀은 주소 풀 할당을 구성하는 가장 간편한 방법입니다. 이 방법을 사용하는 경우 Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > Network (Client) Access(네트워크(클라이언트) 액세스) > Address Assignment(주소 할당) > Address Pools(주소 풀) 창에서 IP 주소 풀을 구성합니다. IPv4 및 IPv6 할당 정책에 이 방법을 사용할 수 있습니다.

  - Allow the reuse of an IP address so many minutes after it is released(해제되고 몇 분이 경과한 후 IP 주소 재사용 허용) — IP 주소가 주소 풀로 반환된 이후에 해당 IP 주소의 재사용을 지연시킵니다. 지연을 추가하면 IP 주소가 신속하게 재할당될 경우 방화벽에서 발생할 수 있는 문제를 방지하는 데 도움이 됩니다. 기본적으로 이 옵션은 선택되지 않으므로 ASA에서는 지연을 적용하지 않습니다. 이 옵션을 사용하려면 해당 상자를 선택하고 1분부터 480분의

범위에서 IP 주소 재할당을 지연시킬 기간(분)을 입력합니다.이 구성 요소는 IPv4 할당 정책에 사용할 수 있습니다.

다음 방법 중 하나를 사용하여 원격 액세스 클라이언트에 IP 주소를 할당할 방법을 지정할 수 있습니다.

IP 주소 할당 옵션 구성

프로시저

단계 **1** **Configuration(**구성**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **Network (Client) Access(**네트워크 **(**클라이언트**)** 액세스**)** > **Address Assignment(**주소 할당**)** > **Assignment Policy(**할당 정책**)**를 선택합니다.

단계 **2** IPv4 Policy(IPv4 정책) 영역에서 활성화할 주소 할당 방법을 선택하고, 비활성화할 주소 할당 방법을 선택 취소합니다. 다음 방법은 기본적으로 활성화되어 있습니다.

- Use Authentication server(인증 서버 사용): IP 주소를 제공하도록 구성한 AAA(인증, 권한 부여 및 어카운트 관리) 서버의 사용을 활성화합니다.
- Use DHCP(DHCP 사용): IP 주소를 제공하도록 구성한 DHCP(Dynamic Host Configuration Protocol) 서버의 사용을 활성화합니다.
- Use internal address pools(내부 주소 풀 사용): ASA에 구성된 로컬 주소 풀의 사용을 활성화합니다.

Use internal address pools(내부 주소 풀 사용**)**를 활성화한 경우 해제된 이후에 IPv4 주소의 재사용을 활성화할 수도 있습니다. IPv4 주소를 재사용할 수 있을 때까지의 경과 시간(분) 범위를 0분에서 480분 사이로 지정할 수 있습니다.

단계 **3** IPv6 Policy(IPv6 정책) 영역에서 활성화할 주소 할당 방법을 선택하거나 비활성화할 주소 할당 방법을 선택 취소합니다. 다음 방법은 기본적으로 활성화되어 있습니다.

- Use Authentication server(인증 서버 사용): IP 주소를 제공하도록 구성한 AAA(인증, 권한 부여 및 어카운트 관리) 서버의 사용을 활성화합니다.
- Use internal address pools(내부 주소 풀 사용): ASA에 구성된 로컬 주소 풀의 사용을 활성화합니다.

단계 **4** 적용을 클릭합니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

주소 할당 방법 보기

프로시저

Configuration(구성**) > Remote Access VPN(**원격 액세스 **VPN) > Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**) > Address Assignment(**주소 할당**) > Assignment Policy(**할당 정책**)**를 선택합니다.

로컬 **IP** 주소 풀 구성

VPN 원격 액세스 터널에 대한 IPv4 또는 IPv6 주소 풀을 구성하려면 ASDM을 열고 **Configuration(**구성**) > Remote Access VPN(**원격 액세스 **VPN) > Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**) > Address Management(**주소 관리**) > Address Pools(**주소 풀**) > Add/Edit IP Pool(IP** 풀 추가/수정**)** 을 선택합니다. 주소 풀을 삭제하려면 ASDM을 열고 **Configuration(**구성**) > Remote Access VPN(**원격 액세스 **VPN) > Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**) > Address Management(**주소 관리**) > Address Pools(**주소 풀**)**를 선택합니다. 삭제할 주소 풀을 선택하고 **Delete(**삭제**)**를 클릭합니다.

ASA에서는 연결 프로필 또는 그룹 정책을 기반으로 주소 풀을 사용하여 연결합니다. 풀을 지정하는 순서는 중요합니다. 연결 프로필 또는 그룹 정책에 대해 둘 이상의 주소 풀을 구성한 경우 ASA에서는 ASA에 추가된 순서대로 주소 풀을 사용합니다.

로컬이 아닌 서브넷에서 주소를 할당할 경우 이러한 네트워크에 대한 경로를 보다 쉽게 추가할 수 있도록 서브넷 경계에 속하는 풀을 추가하는 것이 좋습니다.

로컬 **IPv4** 주소 풀 구성

IP Pool(IP 풀) 영역에는 구성된 주소 풀이 해당 IP 주소 범위(예: 10.10.147.100~10.10.147.177)와 함께 이름별로 표시됩니다. 풀이 없는 경우 이 영역은 비어 있습니다. ASA에서는 나열된 순서대로 이러한 풀을 사용합니다. 예를 들어 첫 번째 풀의 모든 주소가 할당된 경우 다음 풀을 사용합니다.

로컬이 아닌 서브넷에서 주소를 할당할 경우 이러한 네트워크에 대한 경로를 보다 쉽게 추가할 수 있도록 서브넷 경계에 속하는 풀을 추가하는 것이 좋습니다.

프로시저

단계 **1** **Configuration(**구성**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**)** > **Address Assignment(**주소 할당**)** > **Address Pools(**주소 풀**)**를 선택합니다.

단계 **2** IPv4 주소를 추가하려면 **Add(**추가**)** > **IPv4 Address pool(IPv4** 주소 풀**)**을 클릭합니다. 기존 주소 풀을 수정하려면 주소 풀 테이블에서 주소 풀을 선택하고 **Edit(**수정**)**를 클릭합니다.

단계 **3** Add/Edit IP Pool(IP 풀 추가/수정) 대화 상자에서 다음 정보를 입력합니다.

- Pool Name(풀 이름) — 주소 풀의 이름을 입력합니다. 최대 64자까지 입력할 수 있습니다.

- Starting Address(시작 주소) — 구성된 각 풀에서 사용할 수 있는 첫 번째 IP 주소를 입력합니다. 점으로 구분된 10진수 형식(예: 10.10.147.100)을 사용합니다.
- Ending Address(끝 주소) — 구성된 각 풀에서 사용할 수 있는 마지막 IP 주소를 입력합니다. 점으로 구분된 10진수 형식(예: 10.10.147.177)을 사용합니다.
- Subnet Mask(서브넷 마스크) — 이 IP 주소 풀이 있는 서브넷을 식별합니다.

단계 **4** 적용을 클릭합니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

로컬 **IPv6** 주소 풀 구성

IP Pool(IP 풀) 영역에는 구성된 주소 풀이 시작 IP 주소 범위, 주소 접두사 및 풀에서 구성할 수 있는 주소 수와 함께 이름별로 표시됩니다. 풀이 없는 경우 이 영역은 비어 있습니다. ASA에서는 나열된 순서대로 이러한 풀을 사용합니다. 예를 들어 첫 번째 풀의 모든 주소가 할당된 경우 다음 풀을 사용합니다.

로컬이 아닌 서브넷에서 주소를 할당할 경우 이러한 네트워크에 대한 경로를 보다 쉽게 추가할 수 있도록 서브넷 경계에 속하는 풀을 추가하는 것이 좋습니다.

프로시저

단계 **1** **Configuration(**구성**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **Network (Client) Access(**네트워크 **(**클라이언트**)** 액세스**)** > **Address Assignment(**주소 할당**)** > **Address Pools(**주소 풀**)**를 선택합니다.

단계 **2** IPv6 주소를 추가하려면 **Add(**추가**)** > **IPv6 Address pool(IPv6** 주소 풀**)**을 클릭합니다. 기존 주소 풀을 수정하려면 주소 풀 테이블에서 주소 풀을 선택하고 **Edit(**수정**)**를 클릭합니다.

단계 **3** Add/Edit IP Pool(IP 풀 추가/수정) 대화 상자에서 다음 정보를 입력합니다.

- Name(이름) — 구성된 각 주소 풀의 이름을 표시합니다.

  Starting IP Address(시작 IP 주소) — 구성된 풀에서 사용할 수 있는 첫 번째 IP 주소를 입력합니다(예: 2001:DB8::1).
- Prefix Length(접두사 길이) — IP 주소 접두사 길이를 비트 단위로 입력합니다. 예를 들어 32는 CIDR 표기법에서 /32를 나타냅니다. 접두사 길이는 IP 주소 풀이 상주하는 서브넷을 정의합니다.
- Number of Addresses(주소 수) - 시작 IP 주소에서 시작하여 풀에 있는 IPv6 주소 수를 식별합니다.

단계 **4** 적용을 클릭합니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

그룹 정책에 내부 주소 풀 할당

Add or Edit Group Policy(그룹 정책 추가 또는 수정) 대화 상자에서 추가하거나 수정할 내부 네트워크(클라이언트) 액세스 그룹 정책에 대해 주소 풀, 터널링 프로토콜, 필터, 연결 설정 및 서버를 지정할 수 있습니다. 이 대화 상자의 각 필드에 대해 Inherit(상속) 확인란을 선택하면 해당 설정에 기본 그룹 정책의 값을 적용할 수 있습니다. Inherit(상속)는 이 대화 상자의 모든 특성에 대한 기본값입니다.

동일한 그룹 정책에 대해 IPv4 주소 풀과 IPv6 주소 풀을 둘 다 구성할 수 있습니다. 동일한 그룹 정책에 두 버전의 IP 주소가 모두 구성된 경우 IPv4에 대해 구성된 클라이언트는 IPv4 주소를 가져오고 IPv6에 대해 구성된 클라이언트는 IPv6 주소를 가져오며 IPv4 주소와 IPv6 주소 둘 다에 대해 구성된 클라이언트는 IPv4 주소와 IPv6 주소를 둘 다 가져옵니다.

프로시저

단계 **1** ASDM을 사용하여 ASA에 연결하고 **Configuration(**구성**) > Remote Access VPN(**원격 액세스 **VPN) > Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**) > Group Policies(**그룹 정책**)**를 선택합니다.

단계 **2** 새 그룹 정책 또는 내부 주소 풀로 구성할 그룹 정책을 생성하고 Edit(수정)를 클릭합니다.

General attributes(일반 특성) 창은 그룹 정책 대화 상자에서 기본적으로 선택되어 있습니다.

단계 **3** Address Pools(주소 풀) 필드를 사용하여 이 그룹 정책에 대한 IPv4 주소 풀을 지정할 수 있습니다. Select(선택)를 클릭하여 IPv4 주소 풀을 추가하거나 수정합니다.

단계 **4** 이 그룹 정책에 사용할 IPv6 주소 풀을 지정하려면 IPv6 Address Pools(IPv6 주소 풀) 필드를 사용합니다. Select(선택)를 클릭하여 IPv6 주소 풀을 추가하거나 수정합니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

단계 **6** **Apply(**적용**)**를 클릭합니다.

DHCP 주소 지정 구성

DHCP를 사용하여 VPN 클라이언트에 대한 주소를 할당하려면 먼저 DHCP 서버와 이 서버에서 사용할 수 있는 IP 주소 범위를 구성해야 합니다. 그런 다음 연결 프로파일을 기반으로 DHCP 서버를 정의합니다. 선택적으로 연결 프로파일 또는 사용자 이름과 연결된 그룹 정책에서 DHCP 네트워크 범위를 정의할 수도 있습니다. 이 네트워크 범위는 DHCP 서버에 사용할 IP 주소 풀을 식별하는 IP 네트워크 번호 또는 IP 주소입니다.

다음 예에서는 IP 주소 172.33.44.19에서 이름이 **firstgroup**인 연결 프로파일에 대한 DHCP 서버를 정의합니다. 또한 **remotegroup**이라는 그룹 정책에 대한 DHCP 네트워크 범위 192.86.0.0을 정의합니다. (remotegroup이라는 그룹 정책은 firstgroup이라는 연결 프로파일과 연결됩니다.) 네트워크 범위를 정의하지 않으면 DHCP 서버에서 구성된 주소 풀 순으로 IP 주소를 할당합니다. 할당되지 않은 주소를 식별할 때까지 풀을 검색합니다.

다음 구성에는 이전에 연결 프로파일 유형의 이름을 지정하고 이를 원격 액세스로 정의했으며, 그룹 정책의 이름을 지정하고 이를 내부 또는 외부로 식별한 경우에는 필요 없는 단계가 추가로 포함되어

있습니다. 이 단계는 이러한 값을 설정할 때까지 후속 tunnel-group 및 group-policy 명령에 액세스할 수 없음을 알려 주기 위해 다음 예에 나와 있습니다.

지침 및 제한 사항

클라이언트 주소를 할당할 DHCP 서버를 식별하기 위해 IPv4 주소만 사용할 수 있습니다.

DHCP를 사용하여 IP 주소 할당

DHCP 서버를 구성한 다음 이러한 서버를 사용하는 그룹 정책을 생성합니다. 사용자가 해당 그룹 정책을 선택하면 DHCP 서버에서 VPN 연결을 위한 주소를 할당합니다.

1. DHCP 서버를 구성합니다. DHCP 서버를 사용하여 AnyConnect 클라이언트에 IPv6 주소를 할당할 수 없습니다.
    1. ASDM을 사용하여 ASA에 연결합니다.
    2. Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > Network (Client) Access(네트워크(클라이언트) 액세스) > Address Assignment(주소 할당) > Assignment Policy(할당 정책)에서 DHCP가 활성화되어 있는지 확인합니다.
    3. Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > DHCP Server(DHCP 서버)를 선택하여 DHCP 서버를 구성합니다.
2. 그룹 정책에 DHCP IP 주소 지정을 할당합니다.
    1. **Configuration(**구성**) > Remote Access VPN(**원격 액세스 **VPN) > Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**) > AnyConnect Connection Profiles(AnyConnect** 연결 프로파일**)**를 선택합니다.
    2. Connection Profiles(연결 프로파일) 영역에서 **Add(**추가**)** 또는 **Edit(**수정**)**를 클릭합니다.
    3. 연결 프로파일에 대한 구성 트리에서 **Basic(**기본**)**을 클릭합니다.
    4. Client Address Assignment(클라이언트 주소 할당) 영역에서 클라이언트에 IP 주소를 할당하는 데 사용할 DHCP 서버의 IPv4 주소를 입력합니다. (예: **172.33.44.19**)
    5. 연결 프로파일과 연결된 그룹 정책을 수정하여 DHCP 범위를 정의합니다. **Configuration(**구성**) > Remote Access VPN(**원격 액세스 **VPN) > Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**) > Group Policies(**그룹 정책**)**를 선택합니다.
    6. 수정할 그룹 정책을 두 번 클릭합니다.
    7. 구성 트리에서 **Servers(**서버**)**를 클릭합니다.
    8. 아래로 화살표를 클릭하여 **More Options(**추가 옵션**)** 영역을 확장합니다.
    9. DHCP 범위 **Inherit(**상속**)**의 선택을 취소합니다.
    10. DHCP 서버에 사용할 IP 주소 풀을 식별하는 IP 네트워크 번호 또는 IP 주소를 입력합니다 (예:**192.86.0.0**)
    11. **OK(**확인**)**를 클릭합니다.

12. **Apply**(적용)를 클릭합니다.

로컬 사용자에게 IP 주소 할당

그룹 정책을 사용하도록 로컬 사용자 어카운트를 구성할 수 있으며, 일부 AnyConnect 특성도 구성할 수 있습니다. 이러한 사용자 어카운트는 IP 주소의 다른 소스가 실패한 경우 대체를 제공하므로 관리자가 계속 액세스할 수 있습니다.

시작하기 전에

사용자를 추가하거나 편집하려면 **Configuration**(구성) > **Remote Access VPN**(원격 액세스 **VPN**) > **AAA/Local Users**(**AAA**/로컬 사용자) > **Local Users**(로컬 사용자)를 선택하고 **Add**(추가) 또는 **Edit**(수정)를 클릭합니다.

기본적으로 **Inherit**(상속) 확인란은 Edit User Account(사용자 어카운트 수정) 화면의 각 설정에 대해 선택되어 있습니다. 따라서 각 사용자 어카운트에서는 기본 그룹 정책인 DfltGrpPolicy에서 해당 설정 값을 상속받습니다.

각 설정을 재정의하려면 **Inherit**(상속) 확인란의 선택을 취소하고 새 값을 입력합니다. 다음의 자세한 단계에서는 IP 주소 설정에 대해 설명합니다. 전체 구성 세부사항을 보려면 로컬 사용자에 대해 VPN 정책 특성 구성, 105 페이지 섹션을 참고하십시오.

프로시저

단계 **1** ASDM을 시작하고 **Configuration**(구성) > **Remote Access VPN**(원격 액세스 **VPN**) > **AAA/Local Users**(**AAA**/로컬 사용자) > **Local Users**(로컬 사용자)를 선택합니다.

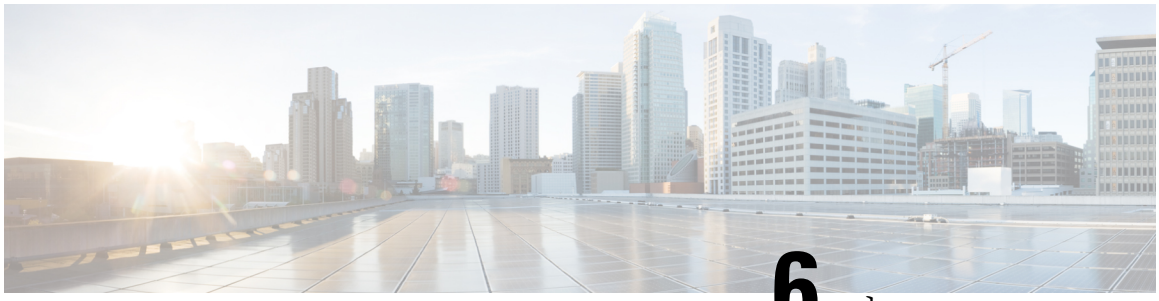
단계 **2** 구성할 사용자를 선택하고 **Edit**(수정)를 클릭합니다.

단계 **3** 왼쪽 창에서 **VPN Policy**(**VPN** 정책)를 클릭합니다.

단계 **4** 이 사용자에 대한 전용 IPv4 주소를 설정하려면 **Dedicated IPv4 Address (Optional)**(전용 **IPv4** 주소(선택 사항)) 영역에 IPv4 주소와 서브넷 마스크를 입력합니다.

단계 **5** 이 사용자에 대한 전용 IPv6 주소를 설정하려면 **Dedicated IPv6 Address (Optional)**(전용 **IPv6** 주소(선택 사항)) 영역에 IPv6 접두사와 함께 IPv6 주소를 입력합니다. IPv6 접두사는 IPv6 주소가 상주하는 서브넷을 나타냅니다.

단계 **6** **Apply**(적용)를 클릭하여 실행 중인 구성에 변경사항을 저장합니다.



6 장

동적 액세스 정책

이 장에서는 동적 액세스 정책을 구성하는 방법에 대해 설명합니다.

동적 액세스 정책 정보

VPN 게이트웨이는 동적 환경에서 작동합니다. 자주 변경되는 인트라넷 구성, 각 사용자가 조직 내에서 담당할 수 있는 여러 역할, 구성 및 보안 수준이 서로 다른 원격 액세스 사이트에서의 로그인 등 다양한 변수가 각 VPN 연결에 영향을 줄 수 있습니다. VPN 환경은 정적 구성의 네트워크보다 사용자 인증 작업이 훨씬 복잡합니다.

ASA에서는 DAP(Dynamic Access Policy)를 사용하여 이러한 많은 변수를 처리하는 권한 부여를 구성할 수 있습니다. 특정 사용자 터널 또는 세션과 연계되는 액세스 제어 특성 모음을 설정하여 동적 액세스 정책을 만들 수 있습니다. 이러한 특성은 여러 그룹 멤버십 및 엔드포인트 보안 문제를 처리합니다. 즉, ASA에서는 정의한 정책을 기반으로 특정 사용자에게 특정 세션에 대한 액세스 권한을 부여합니다. ASA에서는 하나 이상의 DAP 레코드에서 특성을 선택 및/또는 집계하여 사용자가 연결할 때 DAP를 생성합니다. 또한 원격 디바이스의 엔드포인트 보안 정보 및 인증된 사용자에 대한 AAA 권한 부여 정보를 기반으로 이러한 DAP 레코드를 선택합니다. 그런 다음 DAP 레코드를 사용자 터널 또는 세션에 적용합니다.

DAP는 다중 컨텍스트 모드에서 지원되지 않습니다.

DAP 시스템에는 주의가 필요한 다음 구성 요소가 포함되어 있습니다.

- DAP 선택 구성 파일 - ASA에서 세션을 설정하는 동안 DAP 레코드를 선택하고 적용하는 데 사용할 조건이 포함된 텍스트 파일입니다. ASA에 저장됩니다. ASDM을 사용하여 이 파일을 수정

한 후 XML 데이터 형식으로 ASA에 업로드할 수 있습니다. DAP 선택 구성 파일에는 사용자가 구성한 모든 특성이 포함됩니다. 예를 들어 AAA 특성, 엔드포인트 특성, 네트워크에서 구성된 액세스 정책과 웹 형식 ACL 필터, 포트 전달 및 URL 목록이 포함될 수 있습니다.

- DfltAccess 정책 - 항상 DAP 요약 테이블의 마지막 항목이며, 우선순위는 0입니다. 기본 액세스 정책에 대한 액세스 정책 특성을 구성할 수 있지만 AAA 또는 엔드포인트 특성은 여기에 포함되지 않으므로 구성할 수 없습니다. DfltAccess 정책은 요약 테이블의 마지막 항목이어야 하므로 삭제할 수 없습니다.

자세한 내용은 동적 액세스 배포 가이드(https://supportforums.cisco.com/docs/DOC-1369)를 참조해 주십시오.

DAP에서 지원하는 원격 액세스 프로토콜 및 상태 진단 툴

ASA에서는 사용자가 구성한 상태 평가 툴을 사용하여 엔드포인트 보안 속성을 가져옵니다. 이러한 상태 진단 툴에는 AnyConnect Posture Module, 독립적인 Host Scan 패키지, NAC가 포함됩니다.

다음 표에는 DAP에서 지원하는 각 원격 액세스 프로토콜, 해당 방법에 사용할 수 있는 상태 진단 툴 및 툴에서 제공하는 정보가 나와 있습니다.

지원되는 원격 액세스 프로토콜	**AnyConnect Posture** 모듈 **Host Scan** 패키지 **Cisco Secure Desktop** **(**활성화된 엔드포인트 진단 **Host Scan** 확장 사용 안 함**)**	**AnyConnect Posture** 모듈 **Host Scan** 패키지 **Cisco Secure Desktop** **(**활성화된 엔드포인트 진단 **Host Scan** 확장 사용**)**	**NAC**	**Cisco NAC Appliance**
	파일 정보, 레지스트리 키 값, 실행 중인 프로세스 및 운영 체제 반환	악성코드 차단 및 개인 방화벽 소프트웨어 정보 반환	NAC 상태 반환	VLAN 유형 및 VLAN ID 반환
IPsec VPN	아니요	아니요	예	예
Cisco AnyConnect VPN	예	예	예	예
클라이언트리스(브라우저 기반) SSL VPN	예	예	아니요	아니요
PIX 컷스루 프록시(상태 진단을 사용할 수 없음)	아니요	아니요	아니요	아니요

DAP를 사용한 원격 액세스 연결 순서

일반적인 원격 액세스 연결 설정 순서를 간략하게 설명하면 다음과 같습니다.

1. 원격 클라이언트에서 VPN 연결을 시도합니다.
2. ASA에서 구성된 NAC 및 Cisco Secure Desktop HostScan 값을 사용하여 상태 진단을 수행합니다.
3. ASA에서 AAA를 통해 사용자를 인증합니다. 또한 AAA 서버에서 해당 사용자에 대한 권한 부여 특성을 반환합니다.
4. ASA에서 AAA 권한 부여 속성을 세션에 적용하고 VPN 터널을 설정합니다.
5. ASA에서 사용자 AAA 권한 부여 정보 및 세션 상태 진단 정보를 기반으로 DAP 레코드를 선택합니다.
6. ASA에서 선택한 DAP 레코드로부터 DAP 속성을 집계하여 이를 DAP 정책으로 만듭니다.
7. ASA에서 DAP 정책을 세션에 적용합니다.

동적 액세스 정책에 대한 라이센싱

참고 No Payload Encryption 모델에서는 이 기능을 사용할 수 없습니다.

모델	라이센스 요건
ASAv	프리미엄 라이센스.
기타 모든 모델	AnyConnect Premium 라이센스 고급 끝점 진단 라이센스 AnyConnect Mobile 라이센스

참고 ASA 관리자는 설치한 AnyConnect 라이센스에 따라 AnyConnect Mobile 상태 DAP 특성을 다르게 사용합니다. 고급 엔드포인트 평가 라이선스는 DAP와 함께 고급 엔드포인트 평가 기능(예: 치료, Windows Mobile 디바이스 LUA 표현식 등) 기능을 지원합니다. 기본 라이선스가 포함된 DAP를 사용할 수도 있습니다. 고급 DAP는 ASA에서 라이선스 및 기능을 기반으로 하여 실행됩니다(예: AnyConnect 프리미엄 라이선스가 활성화된 상태의 안티바이러스 검사).

관련 항목

DAP에 AnyConnect 엔드포인트 특성 추가, 198 페이지

동적 액세스 정책 구성

시작하기 전에

- 특별한 설명이 없는 경우 DAP 엔드포인트 특성을 구성하려면 먼저 Host Scan을 설치해야 합니다.
- 파일, 프로세스, 레지스트리 엔드포인트 특성을 구성하기 전에 파일, 프로세스, 레지스트리 기본 Host Scan 특성을 구성하십시오. 지침을 보려면 ASDM을 시작하고 **Configuration(**구성**) > Remote Access VPN(**원격 액세스 **VPN) > Secure Desktop Manager(Secure Desktop** 관리자**) > Host Scan**을 선택한 다음 **Help(**도움말**)**를 클릭하십시오.
- DAP는 ASCII 문자만 지원합니다.

프로시저

단계 **1** ASDM을 시작하고 **Configuration(**구성**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**)** 또는 **Clientless SSL VPN Access(**클라이언트리스 **SSL VPN** 액세스**)** > **Dynamic Access Policies(**동적 액세스 정책**)**를 선택합니다.

단계 **2** 특정 악성코드 차단 또는 개인 방화벽 엔드포인트 속성을 포함하려면 창 상단에 있는 **CSD configuration(CSD** 구성**)** 링크를 클릭합니다. 그런 다음 Cisco Secure Desktop 및 HostScan 확장을 활성화합니다. 이전에 이 기능을 둘 다 활성화한 경우에는 이 링크가 표시되지 않습니다.

단계 **3** 이전에 구성한 DAP 목록을 확인합니다.

다음 필드가 테이블에 표시됩니다.

- ACL Priority(ACL 우선순위) - DAP 레코드의 우선순위를 표시합니다.

  ASA에서는 여러 DAP 레코드에서 네트워크 및 웹 형식 ACL를 집계할 때 이 값을 사용하여 ACL의 순서를 논리적으로 지정합니다. ASA에서는 우선순위 번호의 내림차순으로 레코드를 정렬하며, 우선순위가 가장 낮은 레코드가 테이블의 맨 아래에 배치됩니다. 번호가 클수록 우선순위가 높습니다. 즉, 값이 4인 DAP 레코드가 값이 2인 레코드보다 우선순위가 더 높습니다. 레코드를 수동으로 정렬할 수 없습니다.

- Name(이름) - DAP 레코드의 이름을 표시합니다.
- Network ACL List(네트워크 ACL 목록) - 세션에 적용되는 방화벽 ACL의 이름을 표시합니다.
- Web-Type ACL List(웹 형식 ACL 목록) - 세션에 적용되는 SSL VPN ACL의 이름을 표시합니다.
- Description(설명) - DAP 레코드의 용도를 설명합니다.

단계 **4** **Add(**추가**)** 또는 **Edit(**수정**)**를 클릭하여 동적 액세스 정책 추가 또는 수정, 191 페이지 작업을 수행합니다.

단계 **5** **Apply(**적용**)**를 클릭하여 DAP 구성을 저장합니다.

단계 **6** **Find(**찾기**)** 필드를 사용하여 DAP(동적 액세스 정책)를 검색합니다.

필드에 입력하기 시작하면 툴이 DAP 테이블의 모든 필드에서 시작 문자를 검색하여 일치하는 항목을 찾습니다. 와일드카드를 사용하여 검색을 확장할 수 있습니다.

예를 들어 **Find(찾기)** 필드에 **sal**을 입력하면 Sales라는 DAP는 일치하지만 Wholesalers라는 DAP는 일치하지 않습니다. **Find(찾기)** 필드에 ***sal**을 입력한 경우에는 테이블에서 **Sales** 또는 **Wholesalers**의 첫 번째 인스턴스가 검색됩니다.

단계 **7** 동적 액세스 정책 테스트, 192 페이지 를 수행하여 구성을 확인합니다.

동적 액세스 정책 추가 또는 수정

프로시저

단계 **1** ASDM을 시작하고 **Configuration(구성)** > **Remote Access VPN(원격 액세스 VPN)** > **Network (Client) Access(네트워크(클라이언트) 액세스)** 또는 **Clientless SSL VPN Access(클라이언트리스 SSL VPN 액세스)** > **Dynamic Access Policies(동적 액세스 정책)** > **Add(추가)** 또는 **Edit(수정)**를 선택합니다.

단계 **2** 이 동적 액세스 정책의 이름(필수) 및 설명(선택)을 입력합니다.

- **Policy Name(정책 이름)**은 공백 없이 4~32자로 구성된 문자열입니다.
- DAP **Description(설명)** 필드에는 최대 80자를 입력할 수 있습니다.

단계 **3** **ACL Priority(ACL 우선순위)** 필드에서 동적 액세스 정책에 대한 우선순위를 설정합니다.

보안 어플라이언스는 여기에서 설정한 순서대로 액세스 정책을 적용하며, 가장 큰 번호가 우선순위가 가장 높습니다. 유효한 값은 0~2,147,483,647이고, 기본값은 0입니다.

단계 **4** 이 DAP에 대한 선택 조건을 지정합니다.

a) Selection Criteria(선택 조건) 창에서 ANY/ALL/NONE(임의/모두/없음) 드롭다운 목록(레이블 없음)을 사용하여 모든 엔드포인트 특성을 충족하면서 이 동적 액세스 정책을 사용하려면 사용자에게 구성된 AAA 특성 값이 모두 있어야 하는지, 하나 이상 있어야 하는지 또는 없어도 되는지를 선택합니다.

중복 항목은 허용되지 않습니다. AAA 또는 엔드포인트 속성 없이 DAP 레코드를 구성한 경우에는 모든 선택 조건이 충족되므로 ASA에서 항상 해당 레코드를 선택합니다.

b) AAA Attributes(AAA 특성) 필드에서 **Add(추가)** 또는 **Edit(수정)**를 클릭하여 DAP에서 AAA 특성 선택 조건 구성, 192 페이지 작업을 수행합니다.

c) Endpoint Attributes(엔드포인트 특성) 영역에서 **Add(추가)** 또는 **Edit(수정)**를 클릭하여 DAP에서 엔드포인트 특성 선택 조건 구성, 196 페이지 작업을 수행합니다.

d) **Advanced(고급)** 필드를 클릭하여 LUA를 사용하여 DAP에서 추가 DAP 선택 조건 만들기, 208 페이지 작업을 수행합니다. 이 기능을 사용하려면 Lua 프로그래밍 언어를 알아야 합니다.

- AND/OR(그리고/또는) - 기본 선택 규칙과 여기에서 입력한 논리 식 간의 관계를 정의하려면 클릭합니다. 즉, 새 특성이 이미 설정된 AAA 및 엔드포인트 특성에 추가되는지 또는 이를 대체하는지 정의합니다. 기본값은 AND(그리고)입니다.

- Logical Expressions(논리 식) - 각 유형의 엔드포인트 특성에 대한 여러 인스턴스를 구성할 수 있습니다. 새 AAA 및/또는 엔드포인트 선택 속성을 정의하는 자유 형식의 LUA 텍스트를 입력합니다. ASDM에서는 여기에서 입력한 텍스트를 검증하지 않고 DAP XML 파일에 복사하기만 합니다. 그러면 ASA에서 구문 분석할 수 없는 식을 모두 제거하고 이를 처리합니다.

단계 **5** 이 DAP에 대한 **Access/Authorization Policy Attributes(**액세스/권한 부여 정책 특성**)**를 지정합니다.

여기에서 구성한 특성 값은 기존 사용자, 그룹, 터널 그룹 및 기본 그룹 레코드의 권한 부여 값을 포함하여 AAA 시스템의 권한 부여 값을 재정의합니다. DAP 액세스 및 권한 부여 정책 특성 구성, 215 페이지를 참고하십시오.

단계 **6** **OK(**확인**)**를 클릭합니다.

동적 액세스 정책 테스트

이 창에서는 권한 부여 특성 값 쌍을 지정하여 디바이스에 구성된 DAP 레코드 집합 검색을 테스트할 수 있습니다.

프로시저

단계 **1** AAA Attribute(AAA 특성) 및 Endpoint Attribute(엔드포인트 특성) 테이블과 연계된 Add/Edit(추가/수정) 버튼을 사용하여 특성 값 쌍을 지정합니다.

이러한 Add/Edit(추가/수정) 버튼을 클릭하면 표시되는 대화 상자는 Add/Edit AAA Attributes(AAA 특성 추가/수정) 및 Add/Edit Endpoint Attributes(엔드포인트 특성 추가/수정) 대화 상자와 유사합니다.

단계 **2** **Test(**테스트**)** 버튼을 클릭합니다.

디바이스의 DAP 하위 시스템에서는 각 레코드에 대한 AAA 및 엔드포인트 선택 특성을 평가할 때 이러한 값을 참조합니다. 결과는 **Test Results(**테스트 결과**)** 영역에 표시됩니다.

DAP에서 AAA 특성 선택 조건 구성

DAP는 AAA에서 제공하는 특성을 재정의할 수 있는 제한된 권한 부여 특성 집합을 제공하여 AAA 서비스를 보완합니다. Cisco AAA 속성 계층 또는 ASA가 RADIUS 또는 LDAP 서버에서 검색한 전체 응답 속성 집합에서 AAA 속성을 지정할 수 있습니다. ASA에서는 사용자에 대한 AAA 권한 부여 정보 및 세션에 대한 상태 진단 정보를 기반으로 DAP 레코드를 선택합니다. ASA에서는 이 정보에 따라 여러 DAP 레코드를 선택한 다음 이를 집계하여 DAP 권한 부여 속성을 만들 수 있습니다.

프로시저

AAA 특성을 DAP 레코드의 선택 조건으로 구성하려면 Add/Edit AAA Attributes(AAA 특성 추가/수정) 대화 상자에서 사용할 Cisco, LDAP 또는 RADIUS 특성을 설정합니다. 이러한 특성을 입력한 값과 같음(=) 또는 같지 않음(!=)으로 설정할 수 있습니다. 각 DAP 레코드의 AAA 특성 수에 대한 제한은 없습니다. AAA 특성에 대한 자세한 내용은 AAA 특성 정의, 195 페이지를 참조하십시오.

AAA Attributes Type(AAA 특성 유형) - 드롭다운 목록을 사용하여 Cisco, LDAP 또는 RADIUS 특성을 선택합니다.

- Cisco - AAA 계층 모델에 저장된 사용자 권한 부여 특성을 참조합니다. DAP 레코드의 AAA 선택 특성에 대해 이러한 특성의 작은 하위 집합을 지정할 수 있습니다. 예를 들면 다음과 같습니다.
  - Group Policy(그룹 정책) - VPN 사용자 세션과 연계된 그룹 정책 이름입니다. 보안 어플라이언스에 로컬로 설정되거나, RADIUS/LDAP 서버에서 IETF-Class(25) 특성으로 전송될 수 있습니다. 최대 64자입니다.
  - Assigned IP Address(할당된 IP 주소) - 정책에 대해 지정할 IPv4 주소를 입력합니다. 전체 터널 VPN 클라이언트(IPsec, L2TP/IPsec, SSL VPN AnyConnect)에 대해 할당된 IP 주소는 클라이언트리스 SSL VPN에 적용되지 않습니다. 클라이언트리스 세션에는 주소 할당이 없기 때문입니다.
  - Assigned IPv6 Address(할당된 IPv6 주소) - 정책에 대해 지정할 IPv6 주소를 입력합니다.
  - Connection Profile(연결 프로파일) - 연결 또는 터널 그룹 이름입니다. 최대 64자입니다.
  - Username(사용자 이름) - 인증된 사용자의 사용자 이름입니다. 최대 64자입니다. 로컬, RADIUS, LDAP 인증/권한 부여 또는 기타 인증 유형(예: RSA/SDI), NT 도메인 등)을 사용하는 경우에 적용됩니다.
  - =/!= - 같음/같지 않음
- LDAP - LDAP 클라이언트(보안 어플라이언스)는 모든 네이티브 LDAP 응답 특성 값 쌍을 해당 사용자의 AAA 세션과 연계된 데이터베이스에 저장합니다. LDAP 클라이언트는 검색한 순서대로 응답 특성을 데이터베이스에 기록합니다. 해당 이름을 가진 후속 특성은 모두 제거됩니다. 이 시나리오는 사용자 레코드 및 그룹 레코드를 모두 LDAP 서버에서 읽을 때 발생할 수 있습니다. 사용자 레코드 특성을 먼저 읽으며, 항상 사용자 레코드 특성이 그룹 레코드 특성에 우선합니다.

  Active Directory 그룹 멤버십을 지원하기 위해 AAA LDAP 클라이언트에서는 LDAP memberOf 응답 특성을 특수한 방식으로 처리합니다. AD memberOf 특성은 AD에서 그룹 레코드의 DN 문자열을 지정합니다. 그룹 이름은 DN 문자열의 첫 번째 CN 값입니다. LDAP 클라이언트는 DN 문자열에서 그룹 이름을 추출하여 AAA memberOf 특성으로 저장하며, 응답 특성 데이터베이스에는 LDAP memberOf 특성으로 저장합니다. LDAP 응답 메시지에 추가 memberOf 특성이 있는 경우 그룹 이름은 이러한 특성에서 추출되며, 이전의 AAA memberOf 특성과 결합되어 쉼표로 구분된 그룹 이름 문자열을 구성합니다. 이는 응답 특성 데이터베이스에서도 업데이트됩니다.

  LDAP 인증/권한 부여 서버에 대한 VPN 원격 액세스 세션에서 다음 세 가지 Active Directory 그룹(memberOf 열거형)을 반환하는 경우

  cn=Engineering,ou=People,dc=company,dc=com

cn=Employees,ou=People,dc=company,dc=com

cn=EastCoastast,ou=People,dc=company,dc=com

ASA에서는 세 가지 Active Directory 그룹(Engineering, Employees 및 EastCoast)을 처리합니다. 이 세 그룹을 조합하여 aaa.ldap 선택 조건으로 사용할 수 있습니다.

LDAP 특성은 DAP 레코드의 특성 이름 및 특성 값 쌍으로 구성됩니다. LDAP 특성 이름은 대/소문자를 구분하는 구문입니다. 예를 들어 AD 서버에서 department로 반환하는 항목 대신 LDAP 특성 Department를 지정한 경우에는 이 특성 설정을 기반으로 DAP 레코드가 일치하지 않게 됩니다.

참고 Value(값) 필드에 여러 값을 입력하려면 세미콜론(;)을 구분 기호로 사용합니다. 예를 들면 다음과 같습니다.

eng;sale; cn=Audgen VPN,ou=USERS,o=OAG

- RADIUS - RADIUS 클라이언트는 모든 네이티브 RADIUS 응답 특성 값 쌍(value pairs)을 해당 사용자의 AAA 세션과 연계된 데이터베이스에 저장합니다. RADIUS 클라이언트는 검색한 순서대로 응답 특성을 데이터베이스에 기록합니다. 해당 이름을 가진 후속 특성은 모두 제거됩니다. 이 시나리오는 사용자 레코드 및 그룹 레코드를 모두 RADIUS 서버에서 읽을 때 발생할 수 있습니다. 사용자 레코드 특성을 먼저 읽으며, 항상 사용자 레코드 특성이 그룹 레코드 특성에 우선합니다.

  RADIUS 특성은 DAP 레코드의 특성 번호 및 특성 값 쌍으로 구성됩니다.

  참고 RADIUS 특성의 경우 DAP는 특성 ID = 4096 + RADIUS ID를 정의합니다.

  예를 들면 다음과 같습니다.

  RADIUS 특성 "Access Hours"의 Radius ID = 1이므로 DAP 특성 값 = 4,096 + 1 = 4,097입니다.

  RADIUS 특성 "Member Of"의 Radius ID = 146이므로 DAP 특성 값 = 4,096 + 146 = 4,242입니다.

- LDAP 및 RADIUS 특성에는 다음이 포함됩니다.
  - Attribute ID(특성 ID) - 특성의 이름/번호를 지정합니다. 최대 64자입니다.
  - Value(값) - 특성 이름(LDAP) 또는 번호(RADIUS)입니다.

    Value(값) 필드에 여러 값을 입력하려면 세미콜론(;)을 구분 기호로 사용합니다. 예:`eng;sale; cn=Audgen VPN,ou=USERS,o=OAG`
  - =/!= - 같음/같지 않음

- LDAP에는 Get AD Groups(AD 그룹 가져오기) 버튼이 포함되어 있습니다. Active Directory 그룹 검색, 195 페이지를 참고하십시오.

Active Directory 그룹 검색

이 창에서는 Active Directory 서버에 사용 가능한 AD 그룹을 쿼리할 수 있습니다. 이 기능은 LDAP를 사용하는 Active Directory 서버에만 적용됩니다. 이 버튼을 클릭하면 Active Directory LDAP 서버에 사용자가 속한 그룹 목록(memberOf 열거형)을 쿼리합니다. 이 그룹 정보를 사용하여 동적 액세스 정책 AAA 선택 조건을 지정할 수 있습니다.

AD 그룹은 LDAP 서버에서 CLI s**how-ad-groups**명령을 사용하여 백그라운드에서 검색됩니다. ASA에서 서버의 응답을 대기하는 기본 시간은 10초입니다. aaa-server 호스트 구성 모드에서 **group-search-timeout** 명령을 사용하여 이 시간을 조정할 수 있습니다.

Edit AAA Server(AAA 서버 수정) 창에서 Group Base DN(그룹 기본 DN)을 변경하여 검색이 시작되는 Active Directory 계층 수준을 변경할 수 있습니다. 또한 ASA에서 서버의 응답을 대기하는 시간도 이 창에서 변경할 수 있습니다. 이러한 기능을 구성하려면**Configuration(**구성**) > Remote Access VPN(**원격 액세스 **VPN) > AAA/Local Users(AAA/**로컬 사용자**) > AAA Server Groups(AAA** 서버 그룹**) > Edit AAA Server(AAA** 서버 수정**)**를 선택합니다.

참고 Active Directory 서버에 많은 그룹이 있는 경우 서버에서 응답 패킷에 포함할 수 있는 데이터 양에 대한 제한에 따라 검색된 AD 그룹 목록(또는 **show ad-groups** 명령의 출력)이 잘릴 수 있습니다. 이 문제를 방지하려면 필터 기능을 사용하여 서버에서 보고되는 그룹 수를 줄이십시오.

AD Server Group(AD 서버 그룹**)** - AD 그룹을 검색할 AAA 서버 그룹의 이름입니다.

Filter By(필터 기준**)** - 표시되는 그룹을 줄이기 위해 그룹 또는 그룹의 부분 이름을 지정합니다.

Group Name(그룹 이름**)** - 서버에서 검색된 AD 그룹의 목록입니다.

AAA 특성 정의

다음 표에서는 DAP에 사용할 수 있는 AAA 선택 특성 이름을 정의합니다. Attribute Name(속성 이름) 필드는 LUA 논리 식에 각 속성 이름을 입력하는 방법을 보여 줍니다. 이 작업은 Add/Edit Dynamic Access Policy(동적 액세스 정책 추가/수정) 창의 Advanced(고급) 섹션에서 수행할 수 있습니다.

특성 유형	특성 이름	소스	값	최대 문자열 길이	설명
Cisco	aaa.cisco.grouppolicy	AAA	문자열	64	ASA에서 사용되거나 Radius/LDAP 서버에서 IETF-CLass(25) 속성으로 전송된 그룹 정책 이름
	aaa.cisco.ipaddress	AAA	입력	-	전체 터널 VPN 클라이언트(IPsec, L2TP/IPsec, SSL VPN AnyConnect)에 할당된 IP 주소
	aaa.cisco.tunnelgroup	AAA	문자열	64	연결 프로파일(터널 그룹) 이름

특성 유형	특성 이름	소스	값	최대 문자열 길이	설명
	aaa.cisco.username	AAA	문자열	64	인증된 사용자의 이름(로컬 인증/권한 부여를 사용하는 경우에 적용됨)
LDAP	aaa.ldap.<*label*>	LDAP	문자열	128	LDAP 특성 값 쌍(value pair)
RADIUS	aaa.radius.<number>	RADIUS	문자열	128	Radius 특성 값 쌍(value pair)

DAP에서 엔드포인트 특성 선택 조건 구성

엔드포인트 특성은 엔드포인트 시스템 환경, 상태 진단 결과 및 애플리케이션에 대한 정보를 포함합니다. ASA에서는 세션을 설정하는 동안 엔드포인트 속성 모음을 생성하고 이러한 속성을 해당 세션과 연결된 데이터베이스에 저장합니다. 각 DAP 레코드는 ASA에서 세션에 대해 선택하기 위해 충족해야 하는 엔드포인트 선택 속성을 지정합니다. ASA에서는 구성된 모든 조건을 충족하는 DAP 레코드만 선택합니다.

시작하기 전에

- 엔드포인트 특성을 DAP 레코드의 선택 조건으로 구성하는 작업은 동적 액세스 정책 구성, 190 페이지을 위한 더 폭넓은 프로세스에 포함됩니다. 엔드포인트 특성을 DAP의 선택 조건으로 구성하기 전에 이 절차를 검토해 주십시오.
- 엔드포인트 특성에 대한 자세한 내용은 엔드포인트 특성 정의, 205 페이지를 참조해 주십시오.
-
- Host Scan에서 메모리에 상주하는 악성코드 차단 및 개인 방화벽 프로그램을 검사하는 방법에 대한 자세한 내용은 DAP와 악성코드 차단 및 개인 방화벽 프로그램, 205 페이지 섹션을 참고하십시오.

프로시저

단계 **1** **Add**(추가) 또는 **Edit**(수정)를 클릭하고 다음 엔드포인트 특성 중 하나 이상을 선택 조건으로 추가합니다.

각 엔드포인트 특성 유형의 여러 인스턴스를 만들 수 있습니다. 각 DAP 레코드의 엔드포인트 특성 수에 대한 제한은 없습니다.

- DAP에 악성코드 차단 엔드포인트 속성 추가, 197 페이지
- DAP에 애플리케이션 특성 추가, 198 페이지
- DAP에 AnyConnect 엔드포인트 특성 추가, 198 페이지
- DAP에 파일 엔드포인트 특성 추가, 200 페이지

- DAP에 디바이스 엔드포인트 특성 추가, 200 페이지
- DAP에 NAC 엔드포인트 특성 추가, 201 페이지
- DAP에 운영 체제 엔드포인트 특성 추가, 201 페이지
- DAP에 개인 방화벽 엔드포인트 특성 추가, 202 페이지
- DAP에 정책 엔드포인트 특성 추가, 202 페이지
- DAP에 프로세스 엔드포인트 특성 추가, 203 페이지
- DAP에 레지스트리 엔드포인트 특성 추가, 203 페이지
- DAP에 여러 인증서 인증 속성 추가, 204 페이지

단계 **2** 조건과 일치하는 DAP 정책을 지정합니다.

이러한 각 엔드포인트 특성 유형에 대해 사용자에게 해당 유형의 모든 인스턴스가 있어야 하는지(Match all = AND, 기본값), 아니면 그중 하나만 있어도 되는지(Match Any = OR)를 규정하는 DAP 정책을 결정합니다.

a) **Logical Op(**논리 연산자**)**를 클릭합니다.
b) 각 엔드포인트 특성 유형에 대해 **Match Any(**일부 일치**)**(기본값) 또는 **Match All(**모두 일치**)**을 선택합니다.
c) 확인을 클릭합니다.

단계 **3** 동적 액세스 정책 추가 또는 수정, 191 페이지으로 돌아갑니다.

DAP에 악성코드 차단 엔드포인트 속성 추가

시작하기 전에

프로시저

단계 **1** **Endpoint Attribute Type(**엔드포인트 속성 유형**)** 목록 상자에서 **Anti-Malware(**악성코드 차단**)**를 선택합니다.

단계 **2** 적절한 **Installed(**설치됨**)** 또는 **Not Installed(**설치되지 않음**)** 버튼을 클릭하여 선택한 엔드포인트 속성과 해당 한정자(Name/Operation/Value(이름/작업/값) 열 아래의 필드)가 설치되어 있는지 또는 설치되어 있지 않은지 표시합니다.

단계 **3** 실시간 스캔을 활성화 또는 비활성화할지를 결정합니다.

단계 **4** **Vendor(**공급업체**)** 목록 상자에서 테스트할 악성코드 차단 공급업체의 이름을 선택합니다.

단계 **5** **Product Description(**제품 설명**)** 확인란을 선택하고 목록 상자에서 테스트할 공급업체의 제품 이름을 선택합니다.

단계 **6** **Version(**버전**)** 확인란을 선택하고 연산 필드를 **Version(**버전**)** 목록 상자에서 선택한 제품 버전 번호와 같음(=), 같지 않음(!=), 보다 작음(<), 보다 큼(>), 보다 작거나 같음(<=) 또는 보다 크거나 같음(>=)으로 설정합니다.

Version(버전) 목록 상자의 선택 항목에 x가 있는 경우(예: 3.x) x를 특정 릴리스 번호로 바꿉니다(예: 3.5).

단계 **7** **Last Update(**마지막 업데이트**)** 확인란을 선택합니다. 마지막 업데이트 이후에 경과한 일 수를 지정합니다. 여기에서 입력한 일 수 이내(<)에 업데이트가 발생해야 하는지 또는 이후(>)에 업데이트가 발생해야 하는지 지정할 수도 있습니다.

단계 **8** **OK(**확인**)**를 클릭합니다.

DAP에 애플리케이션 특성 추가

프로시저

단계 **1** **Endpoint Attribute Type(**엔드포인트 특성 유형**)** 목록 상자에서 **Application(**애플리케이션**)**을 선택합니다.

단계 **2** Client Type(클라이언트 유형) 연산 필드에서 같음(=) 또는 같지 않음(! =)을 선택합니다.

단계 **3** Client type(클라이언트 유형) 목록 상자에서 테스트할 원격 액세스 연결 유형을 지정합니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

DAP에 AnyConnect 엔드포인트 특성 추가

모바일 상태 또는 AnyConnect ID 확장(ACIDex)이라고도 하는 AnyConnect 엔드포인트 특성은 AnyConnect VPN 클라이언트에서 ASA로 상태 정보를 전달하는 데 사용됩니다. 동적 액세스 정책에서는 사용자 권한 부여에 이 엔드포인트 특성을 사용합니다.

이러한 모바일 상태 특성을 동적 액세스 정책에 포함하여 Host Scan 또는 Cisco Secure Desktop을 엔드포인트에 설치하지 않고도 적용할 수 있습니다.

일부 모바일 상태 특성은 모바일 디바이스에서만 실행되는 AnyConnect 클라이언트와 관련됩니다. 일부 모바일 상태 특성은 모바일 디바이스에서 실행되는 AnyConnect 클라이언트 및 AnyConnect 데스크톱 클라이언트 모두와 관련됩니다.

시작하기 전에

모바일 상태를 사용하려면 AnyConnect Mobile 라이센스 및 AnyConnect Premium 라이센스가 ASA에 설치되어 있어야 합니다. 이러한 라이센스를 설치한 엔터프라이즈는 DAP 특성 및 기타 기존 엔드포인트 특성을 기반으로 지원되는 모바일 디바이스에서 DAP 정책을 적용할 수 있습니다. 여기에는 모바일 디바이스에서 원격 액세스를 허용하거나 거부하는 것도 포함됩니다.

프로시저

단계 1 **Endpoint Attribute Type(**엔드포인트 특성 유형**)** 목록 상자에서 **AnyConnect**를 선택합니다.

단계 2 **Client Version(**클라이언트 버전**)** 확인란을 선택하고 연산 필드를 **Client Version(**클라이언트 버전**)** 필드에서 지정하는 AnyConnect 클라이언트 버전 번호와 같음(=), 같지 않음(!=), 보다 작음(<), 보다 큼(>), 보다 작거나 같음(<=) 또는 보다 크거나 같음(>=)으로 설정합니다.

이 필드를 사용하여 휴대폰 및 태블릿과 같은 모바일 장치 또는 데스크톱 및 노트북 컴퓨터의 클라이언트 버전을 평가할 수 있습니다.

단계 3 **Platform(**플랫폼**)** 확인란을 선택하고 연산 필드를 **Platform(**플랫폼**)** 목록 상자에서 선택하는 운영 체제와 같음(=) 또는 같지 않음(!=)으로 설정합니다.

이 필드를 사용하여 휴대폰 및 태블릿과 같은 모바일 장치의 운영 체제와 데스크톱 및 노트북 컴퓨터의 운영 체제를 평가할 수 있습니다. 플랫폼을 선택하면 Device Type(장치 유형) 및 Device Unique ID(장치 고유 ID)에 대한 추가 특성 필드가 활성화됩니다.

단계 4 **Platform Version(**플랫폼 버전**)** 확인란을 선택하고 연산 필드를 **Platform Version(**플랫폼 버전**)** 필드에서 지정하는 AnyConnect 클라이언트 버전 번호와 같음(=), 같지 않음(!=), 보다 작음(<), 보다 큼(>), 보다 작거나 같음(<=) 또는 보다 크거나 같음(>=)으로 설정합니다.

이 특성이 포함된 DAP 레코드를 만들려면 이전 단계에서 Platform(플랫폼)도 지정해야 합니다.

단계 5 Platform(플랫폼) 확인란을 선택한 경우 **Device Type(**디바이스 유형**)** 확인란을 선택할 수 있습니다. 연산 필드를 **Device Type(**디바이스 유형**)** 필드에서 선택하거나 입력하는 장치와 같음(=) 또는 같지 않음(!=)으로 설정합니다.

Device Type(디바이스 유형) 필드에 나열되지 않은 지원되는 장치가 있는 경우 Device Type(디바이스 유형) 필드에 입력할 수 있습니다. 디바이스 유형 정보를 가져오는 가장 신뢰할 수 있는 방법은 AnyConnect 클라이언트를 엔드포인트에 설치하고 ASA에 연결한 후 DAP Trace(DAP 추적)를 수행하는 것입니다. DAP 추적 결과에서 **endpoint.anyconnect.devicetype** 값을 확인합니다. 이 값을 Device Type(디바이스 유형) 필드에 입력해야 합니다.

단계 6 Platform(플랫폼) 확인란을 선택한 경우 **Device Unique ID(**디바이스 고유 **ID)** 확인란을 선택할 수 있습니다. 연산 필드를 **Device Unique ID(**디바이스 고유 **ID)** 필드에서 지정하는 디바이스의 고유 ID와 같음(=) 또는 같지 않음(!=)으로 설정합니다.

Device Unique ID(디바이스 고유 ID)는 특정 모바일 디바이스에 대한 정책을 설정할 수 있도록 개별 디바이스를 구별합니다. 디바이스의 고유 ID를 가져오려면 디바이스를 ASA에 연결하고 DAP 추적을 수행한 후 **endpoint.anyconnect.deviceuniqueid** 값을 확인해야 합니다. 이 값을 Device Unique ID(디바이스 고유 ID) 필드에 입력해야 합니다.

단계 7 Platform(플랫폼)을 선택한 경우 **MAC Addresses Pool(MAC** 주소 풀**)** 필드에 MAC 주소를 추가할 수 있습니다. 연산 필드를 지정하는 MAC 주소와 같음(=) 또는 같지 않음(!=)으로 설정합니다. 각 MAC 주소는 xx-xx-xx-xx-xx-xx 형식(여기서 'x'는 유효한 16진수 문자(0~9, A~F 또는 a~f))이어야 합니다. 하나 이상의 공백으로 MAC 주소를 구분해야 합니다.

MAC 주소는 특정 디바이스에 대한 정책을 설정할 수 있도록 개별 시스템을 구별합니다. 시스템의 MAC 주소를 가져오려면 디바이스를 ASA에 연결하고 DAP 추적을 수행한 후

endpoint.anyconnect.macaddress 값을 확인해야 합니다. 이 값을 MAC Address Pool(MAC 주소 풀) 필드에 입력해야 합니다.

단계 **8** **OK(**확인**)**를 클릭합니다.

DAP에 파일 엔드포인트 특성 추가

시작하기 전에

파일 엔드포인트 특성을 구성하기 전에 Cisco Secure Desktop Host Scan 창에서 검사할 파일을 정의합니다. ASDM에서 **Configuration(**구성**) > Remote Access VPN(**원격 액세스 **VPN) > Secure Desktop Manager(Secure Desktop** 관리자**) > Host Scan**을 선택합니다. 자세한 내용을 보려면 해당 페이지에서 **Help(**도움말**)**를 클릭합니다.

프로시저

단계 **1** **Endpoint Attribute Type(**엔드포인트 특성 유형**)** 목록 상자에서 **File(**파일**)**을 선택합니다.

단계 **2** 적절한 **Exists(**있음**)** 또는 **Does not exist(**없음**)** 라디오 버튼을 선택하여 선택한 엔드포인트 특성 및 해당 한정자(Exists(있음)/Does not exist(없음) 버튼 아래의 필드)가 있어야 하는지 여부를 나타냅니다.

단계 **3** **Endpoint ID(**엔드포인트 **ID)** 목록 상자의 드롭다운 목록에서 검사할 파일 항목에 해당하는 엔드포인트 ID를 선택합니다.

파일 정보는 Endpoint ID(엔드포인트 ID) 목록 상자 아래에 표시됩니다.

단계 **4** **Last Update(**마지막 업데이트**)** 확인란을 선택하고 연산 필드를 특정 경과 일 수보다 적음(<) 또는 높음(>)으로 설정합니다. **days(**일**)** 필드에 경과 일 수를 입력합니다.

단계 **5** **Checksum(**체크섬**)** 확인란을 선택하고 연산 필드를 테스트할 파일의 체크섬 값과 같음(=) 또는 같지 않음(!=)으로 설정합니다.

단계 **6** **Compute CRC32 Checksum(CRC32** 체크섬 계산**)**을 클릭하여 테스트할 파일의 체크섬 값을 확인합니다.

단계 **7** **OK(**확인**)**를 클릭합니다.

DAP에 디바이스 엔드포인트 특성 추가

프로시저

단계 **1** **Endpoint Attribute Type(**엔드포인트 특성 유형**)** 목록 상자에서 **Device(**디바이스**)**를 선택합니다.

단계 2 **Host Name(**호스트 이름**)** 확인란을 선택하고 연산 필드를 테스트할 디바이스의 호스트 이름과 같음(=) 또는 같지 않음(!=)으로 설정합니다. 컴퓨터의 FQDN(정규화된 도메인 이름)이 아니라 호스트 이름만 사용합니다.

단계 3 **MAC address(MAC** 주소**)** 확인란을 선택하고 연산 필드를 테스트할 NIC(Network Interface Card)의 MAC 주소와 같음(=) 또는 같지 않음(!=)으로 설정합니다. 항목당 하나의 MAC 주소만 가능합니다. 주소는 xxxx.xxxx.xxxx 형식(여기서 x는 유효한 16진수 문자)이어야 합니다.

단계 4 **BIOS Serial Number(BIOS** 일련 번호**)** 확인란을 선택하고 연산 필드를 테스트할 디바이스의 BIOS 일련 번호와 같음(=) 또는 같지 않음(!=)으로 설정합니다. 번호 형식은 제조업체별로 다릅니다. 형식 요건은 없습니다.

단계 5 **TCP/UDP Port Number(TCP/UDP** 포트 번호**)** 확인란을 선택하고 연산 필드를 테스트할 수신 대기 상태의 TCP 또는 UDP와 같음(=) 또는 같지 않음(!=)으로 설정합니다.

TCP/UDP 콤보 상자에서 테스트할 포트 종류, 즉 TCP(IPv4), UDP(IPv4), TCP(IPv6) 또는 UDP(IPv6)를 선택합니다. 둘 이상의 포트를 테스트할 경우 DAP에서 여러 개의 개별 엔드포인트 특성 규칙을 만들고 각 규칙에서 하나의 포트를 지정합니다.

단계 6 **Version of Secure Desktop (CSD)(Secure Desktop(CSD)** 버전**)** 확인란을 선택하고 연산 필드를 엔드포인트에서 실행되는 Host Scan 이미지의 버전과 같음(=) 또는 같지 않음(!=)으로 설정합니다.

단계 7 **Version of Endpoint Assessment(**엔드포인트 진단 버전**)** 확인란을 선택하고 연산 필드를 테스트할 엔드포인트 진단(OPSWAT) 버전과 같음(=) 또는 같지 않음(!=)으로 설정합니다.

단계 8 **OK(**확인**)**를 클릭합니다.

DAP에 NAC 엔드포인트 특성 추가

프로시저

단계 1 **Endpoint Attribute Type(**엔드포인트 특성 유형**)** 목록 상자에서 **NAC**를 선택합니다.

단계 2 **Posture Status(**상태**)** 확인란을 선택하고 연산 필드를 ACS에서 받은 상태 토큰 문자열과 같음(=) 또는 같지 않음(!=)으로 설정합니다. Posture Status(상태) 텍스트 상자에 상태 토큰 문자열을 입력합니다.

단계 3 **OK(**확인**)**를 클릭합니다.

DAP에 운영 체제 엔드포인트 특성 추가

프로시저

단계 1 **Endpoint Attribute Type(**엔드포인트 특성 유형**)** 목록 상자에서 **Operating System(**운영 체제**)**을 선택합니다.

단계 2 **OS Version(OS** 버전**)** 확인란을 선택하고 연산 필드를 **OS Version(OS** 버전**)** 목록 상자에서 설정한 Windows, Mac 또는 Linux 운영 체제와 같음(=) 또는 같지 않음(!=)으로 설정합니다.

단계 3 **OS Update(OS** 업데이트**)** 확인란을 선택하고 연산 필드를 **OS Update(OS** 업데이트**)** 텍스트 상자에 입력한 Windows, Mac 또는 Linux 운영 체제용 서비스 팩과 같음(=) 또는 같지 않음(!=)으로 설정합니다.

단계 4 **OK(**확인**)**를 클릭합니다.

DAP에 개인 방화벽 엔드포인트 특성 추가

시작하기 전에

프로시저

단계 1 **Endpoint Attribute Type(**엔드포인트 특성 유형**)** 목록 상자에서 **Operating System(**운영 체제**)**을 선택합니다.

단계 2 적절한 **Installed(**설치됨**)** 또는 **Not Installed(**설치되지 않음**)** 버튼을 클릭하여 선택한 엔드포인트 속성과 해당 한정자(Name/Operation/Value(이름/작업/값) 열 아래의 필드)가 설치되어 있는지 또는 설치되어 있지 않은지 표시합니다.

단계 3 **Vendor(**공급업체**)** 목록 상자에서 테스트할 개인 방화벽 공급업체의 이름을 클릭합니다.

단계 4 **Product Description(**제품 설명**)** 확인란을 선택하고 목록 상자에서 테스트할 공급업체의 제품 이름을 선택합니다.

단계 5 **Version(**버전**)** 확인란을 선택하고 연산 필드를 **Version(**버전**)** 목록 상자에서 선택한 제품 버전 번호와 같음(=), 같지 않음(!=), 보다 작음(<), 보다 큼(>), 보다 작거나 같음(<=) 또는 보다 크거나 같음(>=)으로 설정합니다.

Version(버전**)** 목록 상자의 선택 항목에 x가 있는 경우(예: 3.x) x를 특정 릴리스 번호로 바꿉니다(예: 3.5).

단계 6 **Last Update(**마지막 업데이트**)** 확인란을 선택합니다. 마지막 업데이트 이후에 경과한 일 수를 지정합니다. 여기에서 입력한 일 수 이내(<)에 업데이트가 발생해야 하는지 또는 이후(>)에 업데이트가 발생해야 하는지 지정할 수도 있습니다.

단계 7 **OK(**확인**)**를 클릭합니다.

DAP에 정책 엔드포인트 특성 추가

프로시저

단계 1 **Endpoint Attribute Type(**엔드포인트 특성 유형**)** 목록 상자에서 **Policy(**정책**)**를 선택합니다.

단계 2 **Location(**위치**)** 확인란을 선택하고 연산 필드를 Cisco Secure Desktop Microsoft Windows 위치 프로파일과 같음(=) 또는 같지 않음(!=)으로 설정합니다. **Location(**위치**)** 텍스트 상자에 Cisco Secure Desktop Microsoft Windows 위치 프로파일 문자열을 입력합니다.

단계 3 **OK(**확인**)**를 클릭합니다.

DAP에 프로세스 엔드포인트 특성 추가

시작하기 전에

프로세스 엔드포인트 특성을 구성하기 전에 Cisco Secure Desktop Host Scan 창에서 검사할 프로세스를 정의합니다. ASDM에서 **Configuration(**구성**) > Remote Access VPN(**원격 액세스 **VPN) > Secure Desktop Manager(Secure Desktop** 관리자**) > Host Scan**을 선택합니다. 자세한 내용을 보려면 해당 페이지에서 **Help(**도움말**)**를 클릭합니다.

프로시저

단계 1 **Endpoint Attribute Type(**엔드포인트 특성 유형**)** 목록 상자에서 **Process(**프로세스**)**를 선택합니다.

단계 2 적절한 **Exists(**있음**)** 또는 **Does not exist(**없음**)** 버튼을 클릭하여 선택한 엔드포인트 특성 및 해당 한정자(Exists(있음) 및 Does not exist(없음) 버튼 아래의 필드)가 있어야 하는지 여부를 나타냅니다.

단계 3 **Endpoint ID(**엔드포인트 **ID)** 목록 상자의 드롭다운 목록에서 검사할 엔드포인트 ID를 선택합니다.

엔드포인트 ID 프로세스 정보가 목록 상자 아래에 표시됩니다.

단계 4 **OK(**확인**)**를 클릭합니다.

DAP에 레지스트리 엔드포인트 특성 추가

레지스트리 엔드포인트 특성 검사는 Windows 운영 체제에만 적용됩니다.

시작하기 전에

레지스트리 엔드포인트 특성을 구성하기 전에 Cisco Secure Desktop Host Scan 창에서 검사할 레지스트리 키를 정의합니다. ASDM에서 **Configuration(**구성**) > Remote Access VPN(**원격 액세스 **VPN) > Secure Desktop Manager(Secure Desktop** 관리자**) > Host Scan**을 선택합니다. 자세한 내용을 보려면 해당 페이지에서 **Help(**도움말**)**를 클릭합니다.

프로시저

단계 1 **Endpoint Attribute Type(**엔드포인트 특성 유형**)** 목록 상자에서 **Registry(**레지스트리**)**를 선택합니다.

단계 **2** 적절한 Exists(있음) 또는 **Does not exist(**없음**)** 버튼을 클릭하여 선택한 **Registry(**레지스트리**)** 엔드포인트 특성 및 해당 한정자(Exists(있음) 및 Does not exist(없음) 버튼 아래의 필드)가 있어야 하는지 여부를 나타냅니다.

단계 **3** **Endpoint ID(**엔드포인트 **ID)** 목록 상자의 드롭다운 목록에서 검사할 레지스트리 항목에 해당하는 엔드포인트 ID를 선택합니다.

레지스트리 정보는 Endpoint ID(엔드포인트 ID) 목록 상자 아래에 표시됩니다.

단계 **4** **Value(**값**)** 확인란을 선택하고 연산 필드를 같음(=) 또는 같지 않음(!=)으로 설정합니다.

단계 **5** 첫 번째 **Value(**값**)** 목록 상자에서 레지스트리 키를 dword 또는 문자열로 지정합니다.

단계 **6** 두 번째 Value operation(값 작업) 목록 상자에서 검사할 레지스트리 키의 값을 입력합니다.

단계 **7** 검사할 때 레지스트리 항목의 대/소문자를 무시하려면 확인란을 클릭합니다. 검색에서 대/소문자를 구분하려면 확인란을 선택하지 마십시오.

단계 **8** **OK(**확인**)**를 클릭합니다.

DAP에 여러 인증서 인증 속성 추가

수신한 인증서를 구성한 규칙에서 참조할 수 있도록 각 인증서의 인덱스를 작성할 수 있습니다. 이러한 인증서 필드를 기준으로 연결 시도를 허용하거나 거부하도록 DAP 규칙을 구성할 수 있습니다.

프로시저

단계 **1** **Configuration(**구성**) > Remote Access VPN(**원격 액세스 **VPN) > Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**) > Dynamic Access Policies(**동적 액세스 정책**) > Add Endpoint Attribute(**엔드포인트 속성 추가**)**로 이동합니다.

단계 **2** 드롭다운 메뉴에서 엔드포인트 속성 유형으로 **Multiple Certificate Authentication(**여러 인증서 인증**)**을 선택합니다.

단계 **3** 기본 설정에 따라 다음 중 하나 또는 모두를 구성합니다.

- 주체 이름
- 발급자 이름
- 주체 대체 이름
- 일련 번호

단계 **4** 저장소의 인증서를 허용하려면 인증서 저장소를 기본값인 None(없음)으로 남겨두거나 사용자 또는 머신만 허용할지 선택합니다. 사용자 또는 머신을 선택하는 경우 인증서를 가져온 저장소를 입력해야 합니다. 이 정보는 프로토콜의 클라이언트에 의해 전송됩니다.

DAP와 악성코드 차단 및 개인 방화벽 프로그램

보안 어플라이언스에서는 사용자 특성이 구성된 AAA 및 엔드포인트 특성과 일치하는 경우 DAP 정책을 사용합니다. Prelogin Assessment 및 HostScan 모듈은 구성된 엔드포인트 속성에 대한 정보를 보안 어플라이언스로 반환하며, DAP 하위 시스템에서는 이 정보를 사용하여 이러한 속성 값과 일치하는 DAP 레코드를 선택합니다.

대부분의 악성코드 차단 및 개인 방화벽 프로그램은 액티브 스캔을 지원합니다. 따라서 메모리에 상주하므로 항상 실행됩니다. HostScan에서는 다음과 같이 엔드포인트에 설치된 프로그램이 있는지, 그리고 해당 프로그램이 메모리에 상주하는지 검사합니다.

- 설치된 프로그램이 액티브 스캔을 지원하지 않는 경우 HostScan에서 해당 소프트웨어가 있는지 여부를 보고합니다. 그러면 DAP 시스템에서 해당 프로그램을 지정하는 DAP 레코드를 선택합니다.
- 설치된 프로그램이 액티브 스캔을 지원하고 해당 프로그램에 대해 액티브 스캔이 활성화된 경우 HostScan에서 해당 소프트웨어가 있는지 여부를 보고합니다. 그러면 보안 어플라이언스에서 해당 프로그램을 지정하는 DAP 레코드를 선택합니다.
- 설치된 프로그램이 액티브 스캔을 지원하고 해당 프로그램에 대해 액티브 스캔이 비활성화된 경우 HostScan에서 해당 소프트웨어가 있는지 여부를 무시합니다. 그러면 보안 어플라이언스에서 해당 프로그램을 지정하는 DAP 레코드를 선택하지 않습니다. 또한 프로그램이 설치되어 있음에도 불구하고, DAP에 대한 많은 정보가 포함된 **debug trace** 명령의 출력에 프로그램이 있는지 여부가 나타나지 않습니다.

엔드포인트 특성 정의

DAP에 사용할 수 있는 엔드포인트 선택 속성은 다음과 같습니다. Attribute Name(속성 이름) 필드에 각 속성 이름을 LUA 논리 식으로 입력하는 방법 및 Dynamic Access Policy Selection Criteria(동적 액세스 정책 선택 조건) 창의 Advanced(고급) 영역에서 사용한 작업이 표시됩니다. *label* 변수는 애플리케이션, 파일 이름, 프로세스 또는 레지스트리 항목을 식별합니다.

특성 유형	특성 이름	소스	값	최대 문자열 길이	설명
안티바이러스 (Cisco Secure Desktop 필요)	endpoint.av["*label*"].exists	HostScan	참	—	안티바이러스 프로그램이 존재함
	endpoint.av["*label*"].version		문자열	32	버전
	endpoint.av["*label*"].description		문자열	128	안티바이러스 설명
	endpoint.av["*label*"].lastupdate		integer	—	안티바이러스 정의를 업데이트한 이후에 경과한 시간(초)

특성 유형	특성 이름	소스	값	최대 문자열 길이	설명
안티스파이웨어(Cisco Secure Desktop 필요)	endpoint.as["*label*"].exists	HostScan	참	—	안티스파이웨어 프로그램이 존재함
	endpoint.as["*label*"].version		문자열	32	버전
	endpoint.as["*label*"].description		문자열	128	안티스파이웨어 설명
	endpoint.as["*label*"].lastupdate		integer	—	안티스파이웨어 정의를 업데이트한 이후에 경과한 시간(초)
개인 방화벽 (Secure Desktop 필요)	endpoint.fw["*label*"].exists	Host Scan	참	—	개인 방화벽이 존재함
	endpoint.fw["*label*"].version		문자열	32	버전
	endpoint.fw["*label*"].description		문자열	128	개인 방화벽 설명
AnyConnect (Cisco Secure Desktop 또는 Host Scan 필요 없음)	endpoint.anyconnect.clientversion	엔드포인트	버전	—	AnyConnect 클라이언트 버전
	endpoint.anyconnect.platform		문자열	—	AnyConnect 클라이언트가 설치된 운영 체제
	endpoint.anyconnect.platformversion		버전	64	AnyConnect 클라이언트가 설치된 운영 체제의 버전
	endpoint.anyconnect.devicetype		문자열	64	AnyConnect 클라이언트가 설치된 모바일 디바이스 유형
	endpoint.anyconnect.deviceuniqueid			64	AnyConnect 클라이언트가 설치된 모바일 디바이스의 고유 ID
	endpoint.anyconnect.macaddress		문자열	—	AnyConnect 클라이언트가 설치된 모바일 디바이스의 MAC 주소 xx-xx-xx-xx-xx-xx 형식(여기서 'x'는 유효한 16진수 문자)이어야 함

특성 유형	특성 이름	소스	값	최대 문자열 길이	설명
애플리케이션	endpoint.application.clienttype	애플리케이션	string	—	클라이언트 유형: CLIENTLESS ANYCONNECT IPSEC L2TP
디바이스	endpoint.device. hostname	엔드포인트	문자열	64	호스트 이름만 해당. FQDN이 아님
	endpoint.device.MAC		문자열	—	NIC(Network Interface Card)의 MAC 주소. 항목당 하나의 MAC 주소만 가능합니다. xxxx.xxxx.xxxx 형식(여기서 x는 유효한 16진수 문자)이어야 함
	endpoint.device.id		문자열	64	BIOS 일련 번호. 번호 형식은 제조업체별로 다릅니다. 형식 요건은 없습니다.
	endpoint.device.port		문자열	—	수신 대기 상태의 TCP 포트 회선당 하나의 포트를 정의할 수 있음 1~65535의 정수
	endpoint.device.protection_version		문자열	64	실행 중인 Host Scan 이미지의 버전
	endpoint.device.protection_extension		문자열	64	엔드포인트 진단(OPSWAT) 버전

특성 유형	특성 이름	소스	값	최대 문자열 길이	설명
파일	endpoint.file["*label*"].exists	Secure Desktop	참	—	파일이 존재함
	endpoint.file[“label”]. endpointid				
	endpoint.file["*label*"]. lastmodified		integer	—	파일이 마지막으로 수정된 이후에 경과한 시간(초)
	endpoint.file["*label*"]. crc.32		integer	—	파일의 CRC32 해시
NAC	endpoint.nac.status	NAC	string	—	사용자 정의 상태 문자열
Operating System(운영 체제)	endpoint.os.version	Secure Desktop	문자열	32	운영 체제
	endpoint.os.servicepack		integer	—	Windows용 서비스 팩
정책	endpoint.policy.location	Secure Desktop	문자열	64	Cisco Secure Desktop의 위치 값
프로세스	endpoint. process["*label*"].exists	Secure Desktop	참	—	프로세스가 존재함
	endpoint. process["*label*"].path		문자열	255	프로세스의 전체 경로
레지스트리	endpoint. registry["*label*"].type	Secure Desktop	*dwordstring*	—	dword
	endpoint. registry["*label*"].value		문자열	255	레지스트리 항목의 값
VLAN	endoint.vlan.type	CNA	string	—	VLAN 유형: ACCESSAUTHERRORG UESTQUARANTINEER RORSTATICTIMEOUT

LUA를 사용하여 DAP에서 추가 DAP 선택 조건 만들기

이 섹션에서는 AAA 또는 엔드포인트 속성에 대한 논리 식을 작성하는 방법에 대해 설명합니다. 이 작업을 수행하려면 LUA에 대한 수준 높은 지식이 필요합니다. LUA 프로그래밍에 대한 자세한 내용은 http://www.lua.org/manual/5.1/manual.html에서 확인할 수 있습니다.

Advanced(고급) 필드에 AAA 및/또는 엔드포인트 선택 논리 연산을 나타내는 자유 형식의 LUA 텍스트를 입력합니다. ASDM에서는 여기에서 입력한 텍스트를 검증하지 않고 DAP 정책 파일에 복사하기만 합니다. 그러면 ASA에서 구문 분석할 수 없는 식을 모두 제거하고 이를 처리합니다.

이 옵션은 위의 AAA 및 엔드포인트 특성 영역에서 지정할 수 없는 선택 조건을 추가하는 데 유용합니다. 예를 들어 지정한 조건 중 하나 이상 또는 모두를 충족하거나 지정한 조건이 없는 AAA 속성을 사용하도록 ASA를 구성할 수 있지만 엔드포인트 속성은 누적되므로 모두 충족해야 합니다. 보안 어플라이언스에서 하나의 특정 엔드포인트 속성을 사용하도록 하려면 적절한 LUA 논리 식을 만들어 여기에 입력해야 합니다.

다음 섹션에서는 LUA EVAL 식을 만드는 방법에 대한 자세한 설명과 예를 제공합니다.

- LUA EVAL 식을 만들기 위한 구문, 209 페이지
- DAP EVAL 식의 예, 213 페이지
- 추가 LUA 함수, 210 페이지

LUA EVAL 식을 만들기 위한 구문

참고 Advanced(고급) 모드를 사용해야 하는 경우 명확성을 위해 가급적 EVAL 식을 사용하는 것이 좋습니다. 그러면 프로그램을 간편하게 확인할 수 있습니다.

EVAL(<*attribute*> , <comparison>, {<*value*> | <*attribute*>}, [<type>])

<attribute>	AAA 특성 또는 Cisco Secure Desktop에서 반환되는 특성(특성 정의는 엔드포인트 특성 정의, 205 페이지 참조)	
<comparison>	다음 문자열 중 하나(따옴표 필요)	
	“EQ”	같음
	NE	같지 않음
	“LT”	보다 작음
	“GT”	보다 큼
	“LE”	보다 작거나 같음
	“GE”	보다 크거나 같음
<value>	특성을 비교할 수 있는 값이 포함된 문자열(따옴표 필요)	

<type>	다음 문자열 중 하나(따옴표 필요)	
	“string”	대/소문자를 구분하는 문자열 비교
	“”	대/소문자를 구분하지 않는 문자열 비교
	“integer”	숫자 비교, 문자열 값을 숫자로 변환
	“hex”	16진수 값을 사용하는 숫자 비교, 16진수 문자열을 16진수 숫자로 변환
	“version”	X.Y.Z. 형식의 버전 비교(X, Y, Z는 숫자)

추가 **LUA** 함수

클라이언트리스 SSL VPN에 대한 동적 액세스 정책 작업을 수행하는 경우 일치 조건을 보다 유연하게 적용해야 할 수 있습니다. 예를 들어 다음에 따라 다른 DAP를 적용할 수 있습니다.

- CheckAndMsg는 호출할 DAP를 구성할 수 있는 LUA 함수로서, 조건에 따라 사용자 메시지를 생성합니다.
- 사용자 개체에 대한 OU(Organizational Unit) 또는 다른 계층 수준
- 명명 규칙을 따르며 가능한 일치 항목이 많은 그룹 이름에는 와일드카드를 사용하는 기능이 필요할 수 있음

ASDM의 DAP 창에 있는 Advanced(고급) 섹션에서 LUA 논리 식을 만들어 이러한 유연성을 확보할 수 있습니다.

DAP CheckAndMsg 함수

ASA에서는 LUA CheckAndMsg 함수가 포함된 DAP 레코드가 선택되고 이로 인해 클라이언트리스 SSL VPN 또는 AnyConnect가 종료된 경우에만 사용자에게 메시지를 표시합니다.

CheckAndMsg 함수의 구문은 다음과 같습니다.

```
CheckAndMsg(value, “<message string if value is true>”, “<message string if value if false>”)
```

CheckAndMsg 함수를 만들 때 다음 사항에 주의해야 합니다.

- CheckAndMsg는 첫 번째 인수로 전달된 값을 반환합니다.
- 문자열 비교를 사용하지 않으려면 EVAL 함수를 첫 번째 인수로 사용해야 합니다. 예를 들면 다음과 같습니다.

```
(CheckAndMsg((EVAL(...)) , "true msg", "false msg"))
```

CheckandMsg에서 EVAL 함수 결과를 반환하면 보안 어플라이언스에서 이를 사용하여 DAP 레코드를 선택할지 여부를 결정합니다. 레코드가 선택되고 종료되면 보안 어플라이언스에서 적절한 메시지를 표시합니다.

OU 기반 일치 예

DAP의 논리 식에는 LDAP 서버에서 반환되는 많은 특성이 사용될 수 있습니다. 이러한 출력의 예를 보려면 DAP 추적 섹션을 참조하거나, debug dap trace를 실행하십시오.

LDAP 서버는 사용자 DN(Distinguished Name)을 반환합니다. 이는 디렉토리에서 사용자 개체가 있는 위치를 암시적으로 식별합니다. 예를 들어 사용자 DN이 CN=Example User, OU=Admins, dc=cisco, dc=com인 경우 이 사용자는 OU=Admins,dc=cisco,dc=com에 있습니다. 모든 관리자가 이 OU 또는 이 수준 아래의 컨테이너에 있는 경우 다음과 같이 논리 식을 사용하여 이 조건을 일치시킬 수 있습니다.

```
assert(function()
   if ( (type(aaa.ldap.distinguishedName) == "string") and
        (string.find(aaa.ldap.distinguishedName, "OU=Admins,dc=cisco,dc=com$") ~= nil) )
then
       return true
   end
   return false
end)()
```

이 예제에서 string.find 함수는 정규식을 참조합니다. 문자열 끝에 $ 기호를 사용하여 이 문자열을 distinguishedName 필드 끝에 연결합니다.

그룹 멤버십 예

AD 그룹 멤버십의 패턴 일치에 대한 기본 논리 식을 만들 수 있습니다. 사용자가 여러 그룹의 구성원일 수 있으므로 DAP에서는 LDAP 서버의 응답을 테이블의 별개 항목으로 구문 분석합니다. 다음을 수행하려면 고급 함수가 필요합니다.

- memberOf 필드를 문자열로 비교합니다(사용자가 하나의 그룹에만 속한 경우).
- 반환된 데이터의 형식이 "table"인 경우 반환된 각 memberOf 필드를 반복합니다.

이러한 목적으로 작성하고 테스트한 함수는 다음과 같습니다. 이 예에서는 사용자가 "-stu"로 끝나는 그룹의 구성원인 경우 이 DAP와 일치합니다.

```
assert(function()
   local pattern = "-stu$"
   local attribute = aaa.ldap.memberOf
   if ((type(attribute) == "string") and
       (string.find(attribute, pattern) ~= nil)) then
       return true
   elseif (type(attribute) == "table") then
       local k, v
       for k, v in pairs(attribute) do
           if (string.find(v, pattern) ~= nil) then
               return true
```

```
          end
       end
   end
   return false
end)()
```

안티바이러스 예

다음 예에서는 사용자 지정 함수를 사용하여 안티바이러스 소프트웨어가 검색되는지 확인합니다.

```
assert(function()
    for k,v in pairs(endpoint.am) do
         if (EVAL(v.exists, "EQ", "true", "string")) then
              return true
         end
    end
    return false
end)()
```

안티스파이웨어 예

다음 예에서는 사용자 지정 함수를 사용하여 안티스파이웨어가 검색되는지 확인합니다.

```
assert(function()
    for k,v in pairs(endpoint.am) do
         if (EVAL(v.exists, "EQ", "true", "string")) then
              return true
         end
    end
    return false
end)()
```

방화벽 예

다음 예에서는 사용자 지정 함수를 사용하여 방화벽이 검색되는지 확인합니다.

```
assert(function()
    for k,v in pairs(endpoint.fw) do
         if (EVAL(v.exists, "EQ", "true", "string")) then
              return true
         end
    end
    return false
end)()
```

악성코드 차단 또는 방화벽 예

다음 예에서는 맞춤형 함수를 사용하여 악성코드 차단 또는 방화벽이 검색되는지 확인합니다.

```
assert(function()
       function check(antix)
           if (type(antix) == "table") then
               for k,v in pairs(antix) do
                   if (EVAL(v.exists, "EQ", "true", "string")) then
                       return true
                   end
               end
           end
```

```
            return false
        end
        return (check(endpoint.am) or check(endpoint.fw) or check(endpoint.am))
    end)()
```

액세스 거부 예

다음 함수를 사용하여 악성코드 차단 프로그램이 없는 경우 액세스를 거부할 수 있습니다. Action(작업)이 종료로 설정된 DAP에서 사용해야 합니다.

```
assert(
    function()
for k,v in pairs(endpoint.am) do

        if (EVAL(v.exists, "EQ", "true", "string")) then

            return false

        end
    end
    return CheckAndMsg(true, "Please install antimalware software before connecting.", nil)
end)()
```

악성코드 차단 프로그램이 없는 사용자가 로그인하려고 하면 DAP에서 다음 메시지를 표시합니다.

```
Please install antimalware software before connecting.
```

DAP EVAL 식의 예

다음은 LUA 논리 식을 만드는 데 도움이 되는 예입니다.

설명	예
Windows XP에 대한 엔드포인트 테스트	`EVAL(endpoint.os.version, "EQ", "Windows XP", "string")`
CLIENTLESS 또는 CVC 클라이언트 유형에서 일치하는 항목에 대한 엔드포인트 식 테스트	`(EVAL(endpoint.application.clienttype,"EQ","CLIENTLESS") or` `EVAL(endpoint.application.clienttype, "EQ","CVC"))`

10.5.x를 제외한 Norton Antivirus 버전 10.x에 대한 엔드포인트 식 테스트	`(EVAL(endpoint.av["NortonAV"].version, "GE", "10","version")`
	`and`
	`EVAL(endpoint.av["NortonAV"].version,"LT", "10.5", "version")`
	`or`
	`EVAL(endpoint.av["NortonAV"].version, "GE", "10.6", "version")))`

설명	예
단일 안티바이러스 프로그램인 McAfee가 사용자 PC에 설치되어 있는지 검사하고, 없는 경우 메시지를 표시합니다.	(CheckAndMsg(EVAL(endpoint.av["McAfeeAV"].exists,"NE","true"), "McAfee AV was not found on your computer", nil))
지난 10일 이내(864,000초)에 McAfee 안티바이러스 정의가 업데이트되었는지 검사하고, 업데이트가 필요한 경우 메시지를 표시합니다.	((CheckAndMsg(EVAL(endpoint.av["McAfeeAV"].lastupdate,"GT","864000","integer"), "AV Update needed! Please wait for the McAfee AV till it loads the latest dat file.",nil)))
debug dap trace가 반환된 후 특정 핫픽스 검사: endpoint.os.windows.hotfix["KB923414"] = "true";	(CheckAndMsg(EVAL(endpoint.os.windows.hotfix["KB923414"],"NE","true"), "The required hotfix is not installed on your PC.",nil))

안티바이러스 프로그램 검사

엔드 유저가 악성코드 차단 소프트웨어의 문제를 알고 이를 해결할 수 있도록 메시지를 구성할 수 있습니다.

엔드 유저가 누락되거나 실행되지 않는 AV 문제를 알고 이를 해결할 수 있도록 메시지를 구성할 수 있습니다. 이렇게 하면 액세스가 거부된 경우 ASA에서 "종료" 조건을 초래하는 DAP에 대한 모든 메시지를 수집한 후 브라우저의 로그온 페이지에 표시합니다. 액세스가 허용된 경우에는 ASA에서 DAP 평가 중에 생성된 모든 메시지를 포털 페이지에 표시합니다.

다음 예에서는 이 함수를 사용하여 Norton AntiVirus 프로그램을 검사하는 방법을 보여줍니다.

1. 다음 LUA 식을 Add/Edit Dynamic Access Policy(동적 액세스 정책 추가/수정) 창의 Advanced(고급) 필드에 복사하여 붙여넣습니다(필드를 확장하려면 맨 오른쪽에 있는 이중 화살표 클릭).

```
(CheckAndMsg(EVAL(endpoint.av["NortonAV"].exists, "EQ", "false"), /
"Your Norton AV was found but the active component of it was not enabled", nil) /
or CheckAndMsg(EVAL(endpoint.av["NortonAV"].exists, "NE", "true"),/
"Norton AV was not found on your computer", nil) )
```

2. 동일한 Advanced(고급) 필드에서 **OR** 버튼을 클릭합니다.
3. 아래 Access Attributes(액세스 특성) 섹션의 맨 왼쪽에 있는 **Action(작업)** 탭에서 **Terminate(종료)**를 클릭합니다.
4. Norton Antivirus가 없거나 비활성화된 PC에서 연결합니다. 그러면 연결이 허용되지 않으며, 메시지가 깜박이는 느낌표(!)로 표시됩니다.
5. 깜박이는 느낌표(!)를 클릭하여 메시지를 확인합니다.

1.5일보다 오래된 안티바이러스 프로그램 및 정의 검사

이 예에서는 Norton 및 McAfee 안티바이러스 프로그램이 있는지와 바이러스 정의가 1.5일(10,000초)보다 오래되었는지를 검사합니다. 정의가 1.5일보다 오래된 경우에는 ASA에서 세션을 종료하고 교정 메시지 및 링크를 표시합니다. 이 작업을 완료하려면 다음 단계를 수행하십시오.

1. 모든 반환 문자가 한 줄에 있도록 반환 문자를 제거하면서 다음 LUA 식을 Add/Edit Dynamic Access Policy(동적 액세스 정책 추가/수정) 창의 Advanced(고급) 필드에 복사하여 붙여넣습니다.

```
(
 (EVAL(endpoint.av["NortonAV"].exists,"EQ","true","string")
  and CheckAndMsg(EVAL(endpoint.av["NortonAV"].lastupdate,"GT","10000",integer"),
To remediate <a href='http://www.symantec.com'>Click this link </a>",nil))
or
 (EVAL(endpoint.av["McAfeeAV"].exists,"EQ","true","string")
  and CheckAndMsg(EVAL(endpoint.av["McAfeeAV"].lastupdate,"GT","10000",integer"),
To remediate <a href='http://www.mcafee.com'>Click this link</a>",nil))
)
```

2. 동일한 Advanced(고급) 필드에서 **AND**를 클릭합니다.
3. 아래 Access Attributes(액세스 속성) 섹션의 맨 왼쪽에 있는 Action(작업) 탭에서 **Terminate(**종료**)**를 클릭합니다.
4. 1.5일보다 오래된 버전의 Norton 및 McAfee 안티바이러스 프로그램이 있는 PC에서 연결합니다. 그러면 연결이 허용되지 않으며, 메시지가 깜박이는 느낌표(!)로 표시됩니다.
5. 깜박이는 느낌표(!)를 클릭하여 교정을 위한 메시지 및 링크를 확인합니다.

DAP 액세스 및 권한 부여 정책 특성 구성

각 탭을 클릭하여 포함된 필드를 구성합니다.

프로시저

단계 **1** **Action(**작업**)** 탭을 선택하여 특정 연결 또는 세션에 적용할 특정 처리를 지정합니다.

- Continue(계속) - (기본값) 액세스 정책 특성을 세션에 적용하려면 클릭합니다.
- Quarantine(격리) - 격리를 사용하여 VPN을 통해 설정된 터널이 이미 있는 특정 클라이언트를 제한할 수 있습니다. ASA에서는 제한된 ACL을 세션에 적용하여 선택한 DAP 레코드에 따라 제한된 그룹을 구성합니다. 엔드포인트가 관리용으로 정의된 정책을 준수하지 않는 경우 사용자는 치료 서비스에 계속 액세스할 수 있지만 사용자에 대한 제한 사항이 적용됩니다. 사용자는 침해 교정을 수행한 후 다시 연결할 수 있으며, 이 경우 새 상태 진단이 호출됩니다. 이 진단에 통과하면 사용자가 연결됩니다. 이 매개변수에는 AnyConnect Secure Mobility 기능을 지원하는 AnyConnect 릴리스가 필요합니다.
- Terminate(종료) - 세션을 종료하려면 클릭합니다.

- User Message(사용자 메시지) - 이 DAP 레코드를 선택한 경우 포털 페이지에 표시할 텍스트 메시지를 입력합니다. 최대 490자입니다. 사용자 메시지가 노란색 구로 표시됩니다. 사용자가 로그인할 때 관심을 끌기 위해 이 구가 세 번 깜박인 후 정지합니다. 여러 DAP 레코드를 선택한 경우 각 레코드에 사용자 메시지가 있으면 모든 사용자 메시지가 표시됩니다.

  올바른 HTML 태그를 사용해야 하는 URL 또는 기타 내장된 텍스트를 포함할 수 있습니다. 예: 모든 계약업체는 악성코드 차단 소프트웨어 업그레이드 절차에 대한 지침을 숙지하십시오.

단계 **2** **Network ACL Filters(**네트워크 **ACL** 필터**)** 탭을 선택하여 이 DAP 레코드에 적용할 네트워크 ACL을 구성합니다.

DAP에 대한 ACL은 허용 규칙과 거부 규칙 중 하나만 포함할 수 있습니다. ACL에 허용 규칙과 거부 규칙이 둘 다 포함된 경우에는 ASA에서 ACL을 거부합니다.

- Network ACL(네트워크 ACL) 드롭다운 목록 - 이 DAP 레코드에 추가할 이미 구성된 네트워크 ACL을 선택합니다. ACL은 허용 규칙과 거부 규칙을 조합할 수 있습니다. 이 필드는 IPv4 및 IPv6 네트워크 트래픽에 대한 액세스 규칙을 정의할 수 있는 통합 ACL을 지원합니다.
- **Manage(**관리**)** - 네트워크 ACL을 추가, 수정 및 삭제하려면 클릭합니다.
- **Network ACL(**네트워크 **ACL)** 목록 - 이 DAP 레코드에 대한 네트워크 ACL을 표시합니다.
- **Add(**추가**)** - 드롭다운 목록에서 선택한 네트워크 ACL을 오른쪽에 있는 Network ACL(네트워크 ACL) 목록에 추가하려면 클릭합니다.
- **Delete(**삭제**)** - 강조 표시된 네트워크 ACL을 Network ACLs(네트워크 ACL) 목록에서 삭제하려면 클릭합니다. ASA에서 ACL을 삭제하려면 먼저 DAP 레코드에서 해당 ACL을 삭제해야 합니다.

단계 **3** **Web-Type ACL Filters (clientless)(**웹 형식 **ACL** 필터**(**클라이언트리스**))** 탭을 선택하여 이 DAP 레코드에 적용할 웹 형식 ACL을 구성합니다. DAP에 대한 ACL은 허용 규칙과 거부 규칙 중 하나만 포함할 수 있습니다. ACL에 허용 규칙과 거부 규칙이 둘 다 포함된 경우에는 ASA에서 ACL을 거부합니다.

- **Web-Type ACL(**웹 형식 **ACL)** 드롭다운 목록 - 이 DAP 레코드에 추가할 이미 구성된 웹 형식 ACL을 선택합니다. ACL은 허용 규칙과 거부 규칙의 조합이 될 수 있습니다.
- **Manage(**관리**)** - 웹 형식 ACL을 추가, 수정, 삭제하려면 클릭합니다.
- **Web-Type ACL(**웹 형식 **ACL)** 목록 - 이 DAP 레코드에 대한 웹 형식 ACL을 표시합니다.
- **Add(**추가**)** - 드롭다운 목록에서 선택한 웹 형식 ACL을 오른쪽에 있는 Web-Type ACLs(웹 형식 ACL) 목록에 추가하려면 클릭합니다.
- **Delete(**삭제**)** - 웹 형식 ACL을 Web-Type ACLs(웹 형식 ACL) 목록에서 삭제하려면 클릭합니다. ASA에서 ACL을 삭제하려면 먼저 DAP 레코드에서 해당 ACL을 삭제해야 합니다.

단계 **4** **Functions(**함수**)** 탭을 클릭하여 DAP 레코드에 대한 파일 서버 입력 및 찾아보기, HTTP 프록시, URL 입력을 구성합니다.

- **File Server Browsing(**파일 서버 찾아보기**)** - 파일 서버 또는 공유 기능에 대한 CIFS 찾아보기를 활성화하거나 비활성화합니다.

  브라우징에는 NBNS(마스터 브라우저 또는 WINS)가 필요합니다. 실패하거나 구성되지 않은 경우에는 DNS가 사용됩니다. CIFS 찾아보기 기능은 다국어를 지원하지 않습니다.

- **File Server Entry(**파일 서버 입력**)** - 사용자가 포털 페이지에서 파일 서버 경로 및 이름을 입력하는 것을 허용하거나 금지합니다. 활성화한 경우 포털 페이지에 파일 서버 입력란이 배치됩니다. 사용자는 Windows 파일의 경로 이름을 직접 입력할 수 있습니다. 파일을 다운로드, 수정 및 삭제할 수 있으며 이름을 바꿀 수도 있습니다. 또한 파일 및 폴더를 추가할 수 있습니다. 해당되는 Windows 서버에서 사용자 액세스에 대한 공유도 구성해야 합니다. 네트워크 요건에 따라 사용자는 파일에 액세스하기 전에 인증을 받아야 할 수도 있습니다.

- **HTTP Proxy(HTTP** 프록시**)** - HTTP 애플릿 프록시를 클라이언트로 전달하는 데 영향을 줍니다. 프록시는 Java, ActiveX, Flash 등 적절한 콘텐츠 변환에 방해가 되는 기술에 유용합니다. 보안 어플라이언스의 지속적인 사용을 보장하면서 변조를 우회합니다. 전달된 프록시는 브라우저의 기존 프록시 구성을 자동으로 수정하고 모든 HTTP 및 HTTPS 요청을 새 프록시 구성으로 리디렉션합니다. HTML, CSS, JavaScript, VBScript, ActiveX, Java 등 모든 클라이언트 쪽 기술을 지원합니다. 유일하게 지원하는 브라우저는 Microsoft Internet Explorer입니다.

- **URL Entry(URL** 입력**)** - 사용자가 포털 페이지에서 HTTP/HTTPS URL을 입력하는 것을 허용하거나 금지합니다. 이 기능을 활성화한 경우 사용자는 URL 입력란에 웹 주소를 입력하고 클라이언트리스 SSL VPN을 사용하여 해당 웹사이트에 액세스할 수 있습니다.

SSL VPN의 사용이 모든 사이트와의 통신 보안을 보장하는 것은 아닙니다. SSL VPN은 원격 사용자 PC 또는 워크스테이션과 기업 네트워크에 있는 ASA 간의 데이터 전송 보안을 보장합니다. 사용자가 인터넷 또는 내부 네트워크에 있는 비 HTTPS 웹 리소스에 액세스하는 경우에는 기업 ASA에서 대상 웹 서버로의 통신 보안이 유지되지 않습니다.

클라이언트리스 VPN 연결에서는 ASA가 엔드 유저 웹 브라우저와 대상 웹 서버 간의 프록시 역할을 합니다. 사용자가 SSL 지원 웹 서버에 연결하면 ASA에서 보안 연결을 설정하고 서버 SSL 인증서를 검증합니다. 엔드 유저 브라우저는 제시된 인증서를 받지 않으므로 인증서를 검사 및 검증할 수 없습니다. SSL VPN의 현재 구현에서는 만료된 인증서를 제시하는 사이트와의 통신을 허용하지 않습니다. 또한 ASA에서도 신뢰할 수 있는 CA 인증서 검증을 수행하지 않습니다. 따라서 사용자는 통신하기 전에 SSL 지원 웹 서버에서 제시하는 인증서를 분석할 수 없습니다.

사용자의 인터넷 액세스를 제한하려면 URL Entry(URL 입력) 필드에서 Disable(비활성화)을 선택합니다. 그러면 SSL VPN 사용자가 클라이언트리스 VPN 연결 시 웹을 탐색할 수 없게 됩니다.

- **Unchanged(**변경 없음**)** - (기본값) 이 세션에 적용되는 그룹 정책의 값을 사용하려면 클릭합니다.
- **Enable/Disable(**활성화/비활성화**)** - 기능을 활성화하거나 비활성화하려면 클릭합니다.
- **Auto-start(**자동 시작**)** - HTTP 프록시를 활성화하고 DAP 레코드가 이러한 기능과 연계된 애플릿을 자동으로 시작하도록 하려면 클릭합니다.

단계 **5** **Port Forwarding Lists(**포트 전달 목록**)** 탭을 선택하여 사용자 세션에 대한 포트 전달 목록을 구성합니다.

포트 전달은 그룹의 원격 사용자가 알려진 고정 TCP/IP 포트를 통해 통신하는 클라이언트/서버 애플리케이션에 액세스할 수 있도록 해줍니다. 원격 사용자는 자신의 로컬 PC에 설치된 클라이언트 애플리케이션을 사용하여 해당 애플리케이션을 지원하는 원격 서버에 안전하게 액세스할 수 있습니다. Cisco에서는 Windows 터미널 서비스, 텔넷, 보안 FTP(FTP over SSH), Perforce, Outlook Express 및 Lotus Notes 애플리케이션을 테스트했습니다. 다른 TCP 기반 애플리케이션도 작동할 수 있지만 이러한 애플리케이션은 Cisco에서 테스트하지 않았습니다.

참고 포트 전달은 일부 SSL/TLS 버전에서 작동하지 않습니다.

주의 포트 포워딩(애플리케이션 액세스) 및 디지털 인증서를 지원하려면 Sun Microsystems Java Runtime Environment(JRE)가 원격 컴퓨터에 설치되어 있어야 합니다.

- **Port Forwarding(**포트 전달**)** - 이 DAP 레코드에 적용되는 포트 전달 목록에 대한 옵션을 선택합니다. 이 필드의 다른 특성은 Port Forwarding(포트 전달)을 Enable(활성화) 또는 Auto-start(자동 시작)로 설정한 경우에만 활성화됩니다.
- **Unchanged(**변경 없음**)** - 실행 중인 구성에서 특성을 제거하려면 클릭합니다.
- **Enable/Disable(**활성화/비활성화**)** - 포트 전달을 활성화하거나 비활성화하려면 클릭합니다.
- **Auto-start(**자동 시작**)** - 포트 전달을 활성화하고 DAP 레코드가 해당 포트 전달 목록과 연계된 포트 전달 애플릿을 자동으로 시작하도록 하려면 클릭합니다.
- **Port Forwarding List(**포트 전달 목록**)** 드롭다운 목록 - DAP 레코드에 추가할 이미 구성된 포트 전달 목록을 선택합니다.
- 신규**...**- 새 포트 포워딩 목록을 구성하려면 클릭합니다.
- **Port Forwarding List(**포트 전달 목록**)(**레이블 없음) - DAP 레코드에 대한 포트 전달 목록을 표시합니다.
- **Add(**추가**)** - 드롭다운 목록에서 선택한 포트 전달 목록을 오른쪽에 있는 Port Forwarding(포트 전달) 목록에 추가하려면 클릭합니다.
- **Delete(**삭제**)** - 선택한 포트 전달 목록을 Port Forwarding(포트 전달) 목록에서 삭제하려면 클릭합니다. ASA에서 포트 포워딩 목록을 삭제하려면 먼저 DAP 레코드에서 해당 포트 포워딩 목록을 삭제해야 합니다.

단계 **6** **Bookmarks(**책갈피**)** 탭을 선택하여 특정 사용자 세션 URL에 대한 책갈피를 구성합니다.

- **Enable bookmarks(**책갈피 활성화**)** - 활성화하려면 클릭합니다. 선택을 취소하면 연결에 대한 책갈피가 포털 페이지에 표시되지 않습니다.
- **Bookmark(**책갈피**)** 드롭다운 목록 - DAP 레코드에 추가할 이미 구성된 책갈피를 선택합니다.
- 관리**...**- 책갈피를 추가, 가져오기, 내보내기 및 삭제하려면 클릭합니다.
- **Bookmarks (unlabeled)(**책갈피**(**레이블 없음**))** - DAP 레코드에 대한 URL 목록을 표시합니다.
- **Add>>(**추가**>>)** - 드롭다운 목록에서 선택한 책갈피를 오른쪽에 있는 URL 영역에 추가하려면 클릭합니다.

- **Delete(**삭제**)** - 선택한 책갈피를 URL 목록 영역에서 삭제하려면 클릭합니다. ASA에서 책갈피를 삭제하려면 먼저 DAP 레코드에서 해당 ACL을 삭제해야 합니다.

단계 **7** **Access Method(**액세스 방식**)**를 선택하여 허용된 원격 액세스 유형을 구성합니다.

- **Unchanged(**변경 없음**)** - 현재 원격 액세스 방식을 계속 사용합니다.
- **AnyConnect Client(AnyConnect** 클라이언트**)** - Cisco AnyConnect VPN 클라이언트를 사용하여 연결합니다.
- **Web-Portal(**웹 포털**)** - 클라이언트리스 VPN으로 연결합니다.
- **Both-default-Web-Portal(**기본값과 웹 포털 둘 다**)** - 클라이언트리스(기본값) 또는 AnyConnect 클라이언트를 통해 연결합니다.
- **Both-default-AnyConnect Client(**기본값과 **AnyConnect** 클라이언트 둘 다**)** - 클라이언트리스 또는 AnyConnect 클라이언트(기본값)를 통해 연결합니다.

단계 **8** **AnyConnect** 탭을 선택하여 Always-on VPN 플래그의 상태를 선택할 수 있습니다.

- Always-On VPN for AnyConnect client(AnyConnect 클라이언트용 Always-On VPN) - AnyConnect 서비스 프로파일의 Always-On VPN 플래그 설정이 변경되거나 비활성화되었는지 또는 AnyConnect 프로파일 설정을 사용해야 하는지 확인합니다.

  이 매개변수에는 Cisco AnyConnect VPN 클라이언트에 대한 Secure Mobility Solution 라이센스 지원을 제공하는 Cisco Web Security Appliance 릴리스가 필요합니다. 또한 "Secure Mobility Solution" 기능을 지원하는 AnyConnect 릴리스가 필요합니다. 자세한 내용은 *Cisco AnyConnect VPN* 클라이언트 관리자 가이드를 참조하십시오.

단계 **9** **AnyConnect Custom Attributes(AnyConnect** 사용자 지정 특성**)** 탭을 선택하여 이전에 정의된 사용자 지정 특성을 보고 이 정책에 연계합니다. 사용자 지정 특성을 정의한 다음 이를 이 정책과 연계할 수도 있습니다.

사용자 지정 특성은 AnyConnect 클라이언트로 전송되어 Deferred Upgrade(지연된 업그레이드)와 같은 기능을 구성하는 데 사용됩니다. 사용자 지정 특성에는 유형 및 명명된 값이 있습니다. 먼저 특성의 유형을 정의한 다음 이 유형의 명명된 값을 하나 이상 정의할 수 있습니다. 기능에 대해 구성할 특정 사용자 지정 특성에 대한 자세한 내용은 사용 중인 AnyConnect 릴리스에 대한 *Cisco AnyConnect Secure Mobility Client* 관리자 설명서를 참조해 주십시오.

사용자 지정 특성은 **Configuration(**구성**) > Remote Access VPN(**원격 액세스 **VPN) > Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**) > Advanced(**고급**) > AnyConnect Custom Attributes(AnyConnect** 사용자 지정 특성**)** 및 **AnyConnect Custom Attribute Names(AnyConnect** 사용자 지정 특성 이름**)**에서 사전 정의할 수 있습니다. 사전 정의된 사용자 지정 특성은 동적 액세스 정책과 그룹 정책 모두에서 사용됩니다.

DAP 추적 수행

DAP 추적에서는 연결된 모든 장치에 대한 DAP 엔드포인트 특성을 표시합니다.

프로시저

단계 **1** SSH 터미널에서 ASA에 로그온하여 특권 EXEC 모드를 시작합니다.

특권 EXEC 모드에서는 `hostname#` ASA 프롬프트가 나타납니다.

단계 **2** 터미널 창에서 세션에 대한 모든 DAP 특성을 표시하도록 DAP 디버그를 활성화합니다.

```
hostname# debug dap trace
endpoint.anyconnect.clientversion="0.16.0021";
endpoint.anyconnect.platform="apple-ios";
endpoint.anyconnect.platformversion="4.1";
endpoint.anyconnect.devicetype="iPhone1,2";
endpoint.anyconnect.deviceuniqueid="dd13ce3547f2fa1b2c3d4e5f6g7h8i9j0fa03f75";
```

단계 **3** (선택 사항) DAP 추적의 출력을 검색하려면 명령 출력을 시스템 로그로 보냅니다. ASA 로그온에 대한 자세한 내용은 *Cisco ASA Series* 일반적인 작업 *ASDM* 구성 가이드에서 로깅 구성을 참조하십시오.

DAP의 예

- DAP를 사용하여 네트워크 리소스 정의, 220 페이지
- DAP를 사용하여 WebVPN ACL 적용, 221 페이지
- CSD 검사 실행 및 DAP를 통해 정책 적용, 222 페이지

DAP를 사용하여 네트워크 리소스 정의

이 예에서는 동적 액세스 정책을 사용자 또는 그룹의 네트워크 리소스를 정의하는 한 가지 방법으로 구성하는 방법을 보여줍니다. Trusted_VPN_Access라는 DAP 정책은 클라이언트리스 VPN 액세스와 AnyConnect VPN 액세스를 허용합니다. Untrusted_VPN_Access라는 정책은 클라이언트리스 VPN 액세스만 허용합니다.

프로시저

단계 **1** ASDM에서 **Configuration**(구성) > **Remote Access VPN**(원격 액세스 **VPN**) > **Clientless SSL VPN Access**(클라이언트리스 **SSL VPN** 액세스) > **Dynamic Access Policies**(동적 액세스 정책) > **Add/Edit Dynamic Access Policy**(동적 액세스 정책 추가/수정) > **Endpoint**(엔드포인트)로 이동합니다.

단계 2 각 정책에 대해 다음 특성을 구성합니다.

특성	Trusted_VPN_Access	Untrusted_VPN_Access
Endpoint Attribute Type Policy(엔드포인트 특성 유형 정책**)**	신뢰성	신뢰 안 함
Endpoint Attribute Process(엔드포인트 특성 프로세스**)**	ieexplore.exe	—
Advanced Endpoint Assessment	AntiVirus= McAfee Attribute	
CSD Location(CSD 위치**)**	신뢰성	신뢰 안 함
LDAP memberOf(LDAP 소속 그룹**)**	Engineering, Managers	판매업체
ACL		웹 형식 ACL
액세스	**AnyConnect** 및 웹 포털	웹 포털

DAP를 사용하여 WebVPN ACL 적용

DAP는 네트워크 ACL(IPsec 및 AnyConnect용), 클라이언트리스 SSL VPN 웹 형식 ACL, URL 목록, 함수 등 액세스 정책 특성의 하위 집합을 직접 적용할 수 있습니다. 그러나 배너 또는 스플릿 터널 목록 등 그룹 정책에서 적용하는 항목은 직접 적용할 수 없습니다. DAP에서 직접 적용하는 특성에 대한 전체 메뉴는 Add/Edit Dynamic Access Policy(동적 액세스 정책 추가/수정) 창의 Access Policy Attributes(액세스 정책 특성) 탭에서 제공됩니다.

Active Directory/LDAP는 사용자 그룹 정책 멤버십을 사용자 항목에 "memberOf" 특성으로 저장합니다. AD 그룹(memberOf) = Engineering에 속한 사용자의 경우 ASA에서 구성된 웹 형식 ACL을 적용하도록 DAP를 정의합니다.

프로시저

단계 1 ASDM에서 Add AAA attributes(AAA 속성 추가) 창으로 이동합니다(**Configuration(**구성**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **Clientless SSL VPN Access(**클라이언트리스 **SSL VPN** 액세스**)** > **Dynamic Access Policies(**동적 액세스 정책**)** > **Add/Edit Dynamic Access Policy(**동적 액세스 정책 추가/수정**)** > **AAA Attributes(AAA** 속성**)** 섹션 > **Add AAA Attribute(AAA** 속성 추가**)**).

단계 2 AAA Attribute type(AAA 특성 유형)에서 드롭다운 목록을 사용하여 **LDAP**를 선택합니다.

단계 3 Attribute ID(특성 ID) 필드에서 정확히 여기에 표시된 대로 memberOf를 입력합니다. 대/소문자를 구분해야 합니다.

단계 4 Value(값) 필드에서 드롭다운 목록을 사용하여 같음(=)을 선택하고 인접 필드에 Engineering을 입력합니다.

단계 **5** 이 창의 Access Policy Attributes(액세스 정책 특성) 영역에서 Web-Type ACL Filters(웹 형식 ACL 필터) 탭을 클릭합니다.

단계 **6** Web-Type ACL(웹 형식 ACL) 드롭다운 목록을 사용하여 AD 그룹(memberOf) = Engineering의 사용자에게 적용할 ACL을 선택합니다.

CSD 검사 실행 및 DAP를 통해 정책 적용

이 예에서는 사용자가 두 개의 특정 AD/LDAP 그룹(Engineering 및 Employees)과 하나의 특정 ASA 터널 그룹에 속해 있는지 검사하는 DAP를 만듭니다. 그런 다음 해당 사용자에게 ACL을 적용합니다.

DAP에서 적용하는 ACL은 리소스에 대한 액세스를 제어합니다. 이러한 ACL은 ASA에서 모든 ACLS 정의 그룹 정책을 재정의합니다. 또한 ASA에서는 DAP에서 정의하거나 제어하지 않는 ACL(예: 스플릿 터널링 목록, 배너 및 DNS)에 대해 일반 AAA 그룹 정책 상속 규칙 및 속성을 적용합니다.

프로시저

단계 **1** ASDM에서 Add AAA attributes(AAA 속성 추가) 창으로 이동합니다(**Configuration(**구성**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **Clientless SSL VPN Access(**클라이언트리스 **SSL VPN** 액세스**)** > **Dynamic Access Policies(**동적 액세스 정책**)** > **Add/Edit Dynamic Access Policy(**동적 액세스 정책 추가/수정**)** > **AAA Attributes(AAA** 속성**)** 섹션 > **Add AAA Attribute(AAA** 속성 추가**)**).

단계 **2** AAA Attribute type(AAA 특성 유형)에서 드롭다운 목록을 사용하여 LDAP를 선택합니다.

단계 **3** Attribute ID(특성 ID) 필드에서 정확히 여기에 표시된 대로 memberOf를 입력합니다. 대/소문자를 구분해야 합니다.

단계 **4** Value(값) 필드에서 드롭다운 목록을 사용하여 같음(=)을 선택하고 인접 필드에 Engineering을 입력합니다.

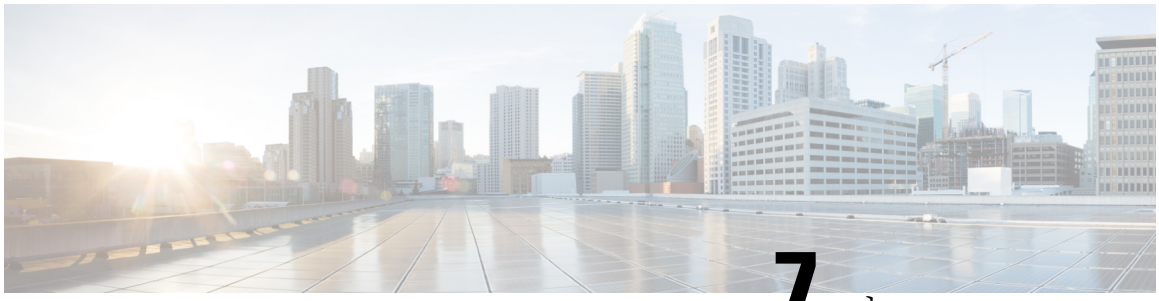
단계 **5** Attribute ID(특성 ID) 필드에서 정확히 여기에 표시된 대로 memberOf를 입력합니다. 대/소문자를 구분해야 합니다.

단계 **6** Value(값) 필드에서 드롭다운 목록을 사용하여 같음(=)을 선택하고 인접 필드에 Employees를 입력합니다.

단계 **7** AAA 특성 유형의 경우, 드롭다운 목록을 사용하여 Cisco를 선택합니다.

단계 **8** Tunnel group(터널 그룹) 상자를 선택하고 드롭다운 목록을 사용하여 같음(=)을 선택한 다음, 인접 드롭다운 목록에서 적절한 터널 그룹(연결 정책)을 선택합니다.

단계 **9** Access Policy Attributes(액세스 정책 특성) 영역의 Network ACL Filters(네트워크 ACL 필터) 탭에서 이전 단계에서 정의한 DAP 조건을 충족하는 사용자에게 적용할 ACL을 선택합니다.



7 장

이메일 프록시

이메일 프록시는 원격 이메일 기능을 클라이언트리스 SSL VPN 사용자로 확장합니다. 사용자가 이메일 프록시를 통해 이메일 세션을 시도하면 이메일 클라이언트에서 SSL 프로토콜을 사용하여 터널을 설정합니다.

이메일 프록시 프로토콜은 다음과 같습니다.

POP3S

POP3S는 클라이언트리스 SSL VPN에서 지원하는 이메일 프록시 중 하나입니다. 기본적으로 Security Appliance는 포트 995를 수신 대기하며, 포트 995 또는 구성된 포트에 대한 연결이 자동으로 허용됩니다. POP3 프록시는 이 포트의 SSL 연결만 허용합니다. SSL 터널이 설정되면 POP3 프로토콜이 시작된 다음 인증이 발생합니다. POP3S는 이메일 수신에 사용됩니다.

IMAP4S

IMAP4S는 클라이언트리스 SSL VPN에서 지원하는 이메일 프록시 중 하나입니다. 기본적으로 Security Appliance는 포트 993을 수신 대기하며, 포트 993 또는 구성된 포트에 대한 연결이 자동으로 허용됩니다. IMAP4 프록시는 이 포트의 SSL 연결만 허용합니다. SSL 터널이 설정되면 IMAP4 프로토콜이 시작된 다음 인증이 발생합니다. IMAP4S는 이메일 수신에 사용됩니다.

SMTPS

SMTPS는 클라이언트리스 SSL VPN에서 지원하는 이메일 프록시 중 하나입니다. 기본적으로 Security Appliance는 포트 988을 수신 대기하며, 포트 988 또는 구성된 포트에 대한 연결이 자동으로 허용됩니다. SMTPS 프록시는 이 포트의 SSL 연결만 허용합니다. SSL 터널이 설정되면 SMTPS 프로토콜이 시작된 다음 인증이 발생합니다. SMTPS는 이메일 전송에 사용됩니다.

이메일 프록시 구성

이메일 프록시 요건

- 로컬 위치와 원격 위치 모두에서 이메일 프록시를 통해 이메일에 액세스하려면 사용자의 이메일 프로그램에 로컬 액세스와 원격 액세스 각각에 대한 별도의 이메일 어카운트가 있어야 합니다.
- 이메일 프록시 세션에는 사용자 인증이 필요합니다.

AAA 서버 그룹 설정

프로시저

단계 **1** **Configuration(**구성**)** > **Features(**기능**)** > **VPN** > **E-mail Proxy(**이메일 프록시**)** > **AAA**로 이동합니다**.**

단계 **2** 적절한 탭(POP3S , IMAP4S 또는 SMTPS)을 선택하여 AAA 서버 그룹을 연결하고 이러한 세션에 대해 기본 그룹 정책을 구성합니다.

- AAA server groups(AAA 서버 그룹) - AAA Server Groups(AAA 서버 그룹) 패널(Configuration(구성) > Features(기능) > Properties(속성) > AAA Setup(AAA 설정) > AAA Server Groups(AAA 서버 그룹))로 이동하려면 클릭합니다. 여기에서 AAA 서버 그룹을 추가하거나 수정할 수 있습니다.
- group policies(그룹 정책) - Group Policy(그룹 정책) 패널(Configuration(구성) > Features(기능) > VPN > General(일반) > Group Policy(그룹 정책))로 이동하려면 클릭합니다. 여기에서 그룹 정책을 추가하거나 수정할 수 있습니다.
- Authentication Server Group(인증 서버 그룹) - 사용자 인증에 사용할 인증 서버 그룹을 선택합니다. 기본값은 인증 서버를 구성하지 않는 것입니다. AAA를 인증 방법으로 설정한 경우(Configuration(구성) > Features AAA(기능 AAA) > VPN > E-Mail Proxy(이메일 프록시) > Authentication(인증) 패널) AAA 서버를 구성하고 여기에서 선택해야 합니다. 그렇지 않으면 인증에 항상 실패합니다.
- Authorization Server Group(권한 부여 서버 그룹) - 사용자 인증에 사용할 권한 부여 서버 그룹을 선택합니다. 기본값은 권한 부여 서버를 구성하지 않는 것입니다.
- Accounting Server Group(어카운트 관리 서버 그룹) - 사용자 어카운트 관리에 사용할 어카운트 관리 서버 그룹을 선택합니다. 기본값은 어카운트 관리 서버를 구성하지 않는 것입니다.
- Default Group Policy(기본 그룹 정책) - AAA에서 CLASSID 특성을 반환하지 않을 때 사용자에게 적용할 그룹 정책을 선택합니다. 길이는 영숫자 4~15자여야 합니다. 기본 그룹 정책을 지정하지 않은 경우 CLASSID가 없으면 ASA에서 세션을 설정할 수 없습니다.

- Authorization Settings(권한 부여 설정) - ASA에서 권한 부여를 위해 인식하는 사용자 이름 값을 설정합니다. 이 값은 디지털 인증서로 인증하고 LDAP 또는 RADIUS 권한 부여를 필요로 하는 사용자에게 적용됩니다.
  - Use the entire DN as the username(전체 DN을 사용자 이름으로 사용) - 고유 이름을 권한 부여에 사용하려면 선택합니다.
  - Specify individual DN fields as the username(개별 DN 필드를 사용자 이름으로 지정) - 사용자 권한 부여에 사용할 특정 DN 필드를 지정하려면 선택합니다.

    두 개의 DN 필드(기본 및 보조)를 선택할 수 있습니다. 예를 들어 EA를 선택한 경우 사용자는 자신의 이메일 주소에 따라 인증합니다. 이 경우 CN(Common Name)이 John Doe이고 이메일 주소가 johndoe@cisco.com인 사용자는 John Doe 또는 johndoe로 인증할 수 없습니다. 이 사용자는 johndoe@cisco.com으로 인증해야 합니다. EA와 O를 선택한 경우 John Doe는 johndoe@cisco.com과 Cisco Systems, Inc로 인증해야 합니다.
  - Primary DN Field(기본 DN 필드) - 권한 부여를 위해 구성할 기본 DN 필드를 선택합니다. 기본값은 CN입니다. 다음과 같은 옵션이 제공됩니다.

DN 필드	정의
Country(국가) (C)	2자로 된 국가 약어입니다. 이러한 코드는 ISO 3166 국가 약어를 따릅니다.
Common Name(공통 이름) (CN)	사람, 시스템 또는 기타 실체의 이름입니다. 이는 식별 계층에서 최하위(가장 구체적) 수준에 속합니다.
DN Qualifier(DN 한정자) (DNQ)	특정 DN 특성입니다.
E-mail Address(이메일 주소) (EA)	인증서를 소유한 사람, 시스템 또는 실체의 이메일 주소입니다.
Generational Qualifier(세대 한정자) (GENQ)	Jr., Sr., III 등의 세대 한정자입니다.
Given Name(이름) (GN)	인증서 소유자의 성을 제외한 이름입니다.
Initials(이니셜) (I)	인증서 소유자의 이름 각 부분의 첫 글자입니다.
Locality(구/군/시) (L)	조직이 있는 구/군/시입니다.
Name(이름) (N)	인증서 소유자의 이름입니다.
Organization (O)(O(조직))	회사, 기관, 에이전시, 협회 또는 기타 실체의 이름입니다.
Organizational Unit (OU)(OU(조직 단위))	조직 내의 하위 그룹입니다.
Serial Number(일련 번호) (SER)	인증서의 일련 번호입니다.

DN 필드	정의
Surname(성) (SN)	인증서 소유자의 성입니다.
State/Province(주/도) (S/P)	조직이 있는 주/도입니다.
Title(직함) (T)	인증서 소유자의 직함입니다(예: Dr.)
User ID(사용자 ID) (UID)	인증서 소유자의 식별 번호입니다.

- Secondary DN Field(보조 DN 필드) - (선택 사항) 권한 부여를 위해 구성할 보조 DN 필드를 선택합니다. 기본값은 OU입니다. 위 표의 모든 옵션 외에 **None(**없음**)**이 추가로 제공됩니다. 이 옵션은 보조 필드를 포함하지 않으려는 경우에 선택합니다.

이메일 프록시의 인터페이스 식별

Email Proxy Access(이메일 프록시 액세스) 화면에서 이메일 프록시를 구성할 인터페이스를 식별할 수 있습니다. 개별 인터페이스에서 이메일 프록시를 구성 및 수정할 수 있으며, 하나의 인터페이스에 대한 이메일 프록시를 구성하고 수정한 다음 이 설정을 모든 인터페이스에 적용할 수 있습니다. 관리 전용 인터페이스 또는 하위 인터페이스에 대해서는 이메일 프록시를 구성할 수 없습니다.

프로시저

단계 **1** **Configuration(**구성**)** > **VPN** > **E-Mail Proxy(**이메일 프록시**)** > **Access(**액세스**)**로 이동하여 인터페이스에 대해 활성화된 항목을 표시합니다.

- Interface(인터페이스) - 구성된 모든 인터페이스의 이름을 표시합니다.
- POP3S Enabled(POP3S 활성화) - POP3S가 인터페이스에 대해 활성화되어 있는지 여부를 표시합니다.
- IMAP4s Enabled(IMAP4S 활성화) - IMAP4S가 인터페이스에 대해 활성화되어 있는지 여부를 표시합니다.
- SMTPS Enabled(SMTPS 활성화) - SMTPS가 인터페이스에 대해 활성화되어 있는지 여부를 표시합니다.

단계 **2** **Edit(**수정**)**를 클릭하여 강조 표시된 인터페이스에 대한 이메일 프록시 설정을 변경합니다.

이메일 프록시에 대한 인증 구성

각 이메일 프록시 유형에 대한 인증 방법을 구성합니다.

프로시저

단계 **1** **Configuration(**구성**)** > **Features(**기능**)** > **VPN** > **E-mail Proxy(**이메일 프록시**)** > **Authentication(**인증**)**으로 이동합니다**.**

단계 **2** 여러 가지 인증 방법 중에서 선택합니다.

- AAA - AAA 인증을 요구하려면 선택합니다. 이 옵션을 사용하려면 구성된 AAA 서버가 필요합니다. 사용자는 사용자 이름, 서버, 비밀번호를 제공합니다. VPN 사용자 이름과 이메일 사용자 이름이 서로 다른 경우에 한해, VPN 이름 구분 기호로 구분하여 두 사용자 이름을 모두 제공해야 합니다.
- Certificate(인증서) - 인증서 인증을 요구하려면 선택합니다.

  참고 인증서 인증은 현재 ASA 소프트웨어 릴리스의 이메일 프록시에 지원되지 않습니다.

  인증서 인증을 사용하려면 사용자에게 ASA에서 SSL 협상 중에 검증할 수 있는 인증서가 있어야 합니다. SMTPS 프록시의 경우 인증서 인증만으로 인증할 수 있지만 다른 이메일 프록시에는 두 가지 인증 방법이 필요합니다.

  인증서 인증에는 모두 동일한 CA에서 발행된 다음 세 가지 인증서가 필요합니다.

  - ASA의 CA 인증서

  - 클라이언트 PC의 CA 인증서

  - 클라이언트 PC의 웹 브라우저 인증서(경우에 따라 개인 인증서 또는 웹 브라우저 인증서라고 함)

- Piggyback HTTPS(피기백 HTTPS) - 피기백 인증을 요구하려면 선택합니다.

  이 인증 체계에서는 사용자가 클라이언트리스 SSL VPN 세션을 이미 설정해 둔 상태여야 합니다. 사용자는 이메일 사용자 이름만 제공하면 됩니다. 비밀번호는 필요하지 않습니다. VPN 사용자 이름과 이메일 사용자 이름이 서로 다른 경우에 한해, VPN 이름 구분 기호로 구분하여 두 사용자 이름을 모두 제공해야 합니다.

  IMAP는 동시 사용자 수에 제한이 없지만 하나의 사용자 이름에 허용되는 동시 로그인 수는 제한된 여러 세션을 생성합니다. IMAP 세션 수가 이 최대값을 초과한 경우 클라이언트리스 SSL VPN 연결이 만료되면 사용자는 이후에 새 연결을 설정할 수 없습니다. 이 문제에 대한 몇 가지 해결 방법이 있습니다.

  SMTPS 이메일에서 주로 피기백 인증을 사용합니다. 대부분의 SMTP 서버는 사용자의 로그인을 허용하지 않기 때문입니다.

참고 IMAP는 동시 사용자 수에 제한이 없지만 하나의 사용자 이름에 허용되는 동시 로그인 수는 제한된 여러 세션을 생성합니다. IMAP 세션 수가 이 최대값을 초과한 경우 클라이언트리스 SSL VPN 연결이 만료되면 사용자는 이후에 새 연결을 설정할 수 없습니다. 이 문제에 대한 몇 가지 해결 방법이 있습니다.

- 사용자는 IMAP 애플리케이션을 닫아 ASA와의 세션을 해제한 다음 클라이언트리스 SSL VPN 연결을 새로 설정할 수 있습니다.

- 관리자는 IMAP 사용자에 대한 동시 로그인 수를 늘릴 수 있습니다(Configuration(구성) > Features(기능) > VPN > General(일반) > Group Policy(그룹 정책) > Edit Group Policy(그룹 정책 수정) > General(일반)).

- 이메일 프록시에 대한 HTTPS/피기백 인증을 비활성화합니다.

- Mailhost(메일 호스트) - (SMTPS에만 해당) 메일 호스트 인증을 요구하려면 선택합니다. 이 옵션은 SMTPS에만 나타납니다. POP3S와 IMAP4S는 항상 메일 호스트 인증을 수행하기 때문입니다. 사용자는 이메일 사용자 이름, 서버, 비밀번호를 제공해야 합니다.

프록시 서버 식별

이 Default Server(기본 서버) 패널에서는 프록시 서버를 ASA로 식별하고 이메일 프록시의 기본 서버, 포트 및 인증되지 않은 세션 제한을 구성할 수 있습니다.

프로시저

단계 **1** **Configuration(**구성**)** > **Features(**기능**)** > **VPN** > **E-mail Proxy(**이메일 프록시**)** > **Default Servers(**기본 서버**)**로 이동합니다**.**

단계 **2** 다음 필드를 구성합니다.

- Name or IP Address(이름 또는 IP 주소) - 기본 이메일 프록시 서버의 DNS 이름 또는 IP 주소를 입력합니다.

- Port(포트) - ASA에서 이메일 프록시 트래픽을 수신 대기할 포트 번호를 입력합니다. 구성된 포트에 대한 연결이 자동으로 허용됩니다. 이메일 프록시는 이 포트의 SSL 연결만 허용합니다. SSL 터널이 설정되면 이메일 프록시가 시작된 다음 인증이 발생합니다.

  기본값은 다음과 같습니다.

  - 995(POP3S용)
  - 993(IMAP4S용)
  - 988(SMTPS용)

- Enable non-authenticated session limit(인증되지 않은 세션 제한 활성화) - 인증되지 않은 이메일 프록시 세션 수를 제한하려면 선택합니다. 인증 과정에서 세션에 대한 제한을 설정함으로써 DOS 공격을 방지할 수 있습니다. 새 세션이 설정된 제한을 초과하면 ASA에서 가장 오래된 비인증 연결을 종료합니다. 비인증 연결이 없는 경우에는 인증 중인 연결 중 가장 오래된 연결이 종료되며, 인증된 세션은 종료되지 않습니다.

이메일 프록시 연결 상태는 다음 세 가지입니다.

- Unauthenticated(인증되지 않음) - 새 이메일 연결의 상태입니다.
- Authenticating(인증 중) - 연결에서 사용자 이름이 제공된 경우의 상태입니다.
- Authenticated(인증됨) - ASA에서 연결을 인증한 경우의 상태입니다.

구분 기호 구성

이 패널에서는 이메일 프록시 인증을 위한 사용자 이름/비밀번호 구분 기호 및 서버 구분 기호를 구성합니다.

프로시저

단계 **1** **Configuration(**구성**)** > **Features(**기능**)** > **VPN** > **E-mail Proxy(**이메일 프록시**)** > **Delimiters(**구분 기호**)**로 이동합니다**.**

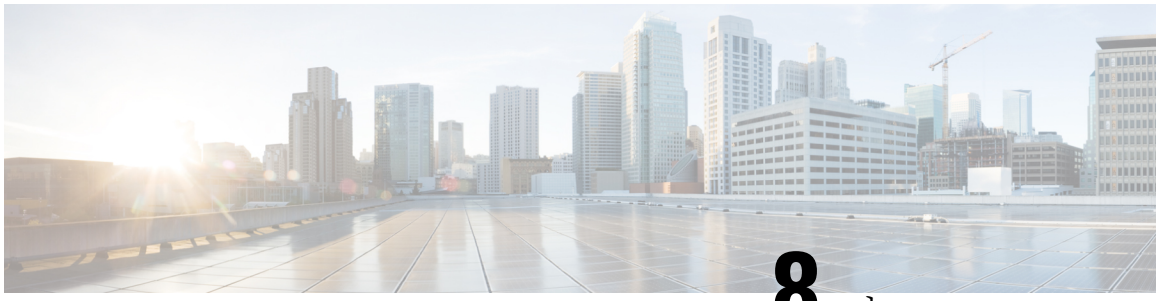
단계 **2** 다음 필드를 구성합니다.

- Username/Password Delimiter(사용자 이름/비밀번호 구분 기호) - VPN 사용자 이름을 이메일 사용자 이름과 구분하는 구분 기호를 선택합니다. 이메일 프록시에 AAA 인증을 사용할 때 VPN 사용자 이름과 이메일 사용자 이름이 다른 경우 사용자는 두 사용자 이름을 모두 제공해야 합니다. 사용자는 이메일 프록시 세션에 로그인할 때 여기에서 구성한 구분 기호로 구분된 사용자 이름을 둘 다 입력해야 하며, 이메일 서버 이름도 입력해야 합니다.

  참고 클라이언트리스 SSL VPN 이메일 프록시 사용자의 비밀번호는 구분 기호로 사용된 문자를 포함할 수 없습니다.

- Server Delimiter(서버 구분 기호) - 사용자 이름을 이메일 서버 이름과 구분하는 구분 기호를 선택합니다. 이 구분 기호는 VPN 이름 구분 기호와 달라야 합니다. 사용자는 이메일 프록시 세션에 로그인할 때 사용자 이름 필드에 자신의 사용자 이름과 서버 이름을 둘 다 입력해야 합니다.

  예를 들어 콜론(:)을 VPN 이름 구분 기호로 사용하고 @ 기호를 서버 구분 기호로 사용하는 경우, 이메일 프록시를 통해 이메일 프로그램에 로그인할 때 vpn_username:e-mail_username@server 형식으로 사용자 이름을 입력해야 합니다.



8 장

VPN 모니터링

VPN 연결 그래프 모니터링

다음 화면에서는 ASA에 대한 VPN 연결 데이터를 그래프 또는 표 형식으로 확인할 수 있습니다.

IPsec 터널 모니터링

Monitoring(모니터링) > VPN> VPN Connection Graphs(VPN 연결 그래프)> IPSec Tunnels(IPSec 터널)

보거나 내보내기 또는 인쇄 작업을 준비할 IPsec 터널 유형의 그래프 및 표를 지정할 수 있습니다.

세션 모니터링

Monitoring(모니터링) > VPN > VPN Connection Graphs(VPN 연결 그래프)> Sessions(세션)

보거나 내보내기 또는 인쇄 작업을 준비할 IPsec 세션 유형의 그래프 및 표를 지정할 수 있습니다.

VPN 통계 모니터링

다음 화면에서는 특정 원격 액세스, LAN-to-LAN, 클라이언트리스 SSL VPN 또는 이메일 프록시 세션에 대한 세부 매개변수 및 통계를 확인할 수 있습니다. 매개변수와 통계는 세션 프로토콜에 따라 다릅니다. 또한 선택한 연결 유형에 따라 통계 표의 내용이 달라집니다. 세부사항 표에는 각 세션에 대한 모든 관련 매개변수가 표시됩니다.

세션 모니터링 창

Monitoring(모니터링) > VPN > VPN Statistics(VPN 통계) > Sessions(세션)

ASA에 대한 VPN 세션 통계를 볼 수 있습니다. 이 창에 있는 두 번째 표의 내용은 Filter By(필터링 기준) 목록에서 선택한 항목에 따라 달라집니다.

참고 관리자는 비활성 상태의 사용자 수를 추적하고 통계를 확인할 수 있습니다. 최장 시간 동안 비활성 상태인 세션은 유휴로 표시되고 자동으로 로그오프되므로 라이선스 용량에 도달하지 않고 새 사용자가 로그인할 수 있습니다. **show vpn-sessiondb** CLI 명령을 사용하여 이러한 통계에 액세스할 수도 있습니다(Cisco ASA 명령 참조 가이드의 적절한 릴리스 참고).

- All Remote Access(모든 원격 액세스)

  이 표의 값이 원격 액세스(IPsec 소프트웨어 및 하드웨어 클라이언트) 트래픽과 관련이 있음을 나타냅니다.

- Username/Connection Profile(사용자 이름/연결 프로파일) - 세션의 사용자 이름 또는 로그인 이름과 연결 프로파일(터널 그룹)을 표시합니다. 클라이언트가 디지털 인증서를 사용하여 인증하는 경우에는 이 필드에 인증서의 주체 CN 또는 주체 OU가 표시됩니다.

- Group Policy Connection Profile(그룹 정책 연결 프로파일) - 세션의 터널 그룹 정책 연결 프로파일을 표시합니다.

- Assigned IP Address/Public IP Address(할당된 IP 주소/공개 IP 주소) - 이 세션의 원격 클라이언트에 할당된 비공개("할당된") IP 주소를 표시합니다. "내부" 또는 "가상" IP 주소라고도 하는 이 IP 주소를 통해 클라이언트는 비공개 네트워크에서 호스트 역할을 할 수 있습니다. 또한 이 필드에는 이 원격 액세스 세션에 대한 클라이언트의 공개 IP 주소도 표시되며, 이를 "외부" IP 주소라고도 합니다. 일반적으로 ISP에서 클라이언트에 할당하는 이 IP 주소를 통해 클라이언트는 공개 네트워크에서 호스트 역할을 할 수 있습니다.

  참고 ASA(프록시)가 모든 트래픽의 소스이므로 Assigned IP Address(할당된 IP 주소) 필드는 클라이언트리스 SSL VPN 세션에 적용되지 않습니다. 하드웨어 클라이언트 세션이 네트워크 확장 모드에 있는 경우에는 해당 하드웨어 클라이언트의 비공개/내부 네트워크 인터페이스의 서브넷이 할당된 IP 주소입니다.

- Ping - 네트워크 연결을 테스트하기 위해 ICMP ping (Packet Internet Groper) 패킷을 보냅니다. 특히 ASA에서는 선택한 호스트에 ICMP 에코 요청 메시지를 보냅니다. 호스트에 연결할 수 있는 경우에는 해당 호스트에서 에코 응답 메시지를 보내며, ASA에 테스트한 호스트의 이름 및 요청을 보낸 시간과 응답을 받은 시간 사이의 경과 시간이 포함된 Success(성공) 메시지가 표시됩니다. 어떤 이유로든(예: 호스트의 작동이 중단되거나, ICMP가 호스트에서 실행되지 않거나, 경로가 구성되지 않았거나, 중간 라우터의 작동이 중단되었거나, 네트워크가 작동 중단 또는 정체된 경우 등) 시스템에 연결할 수 없는 경우에는 ASA에 테스트한 호스트의 이름이 포함된 Error(오류) 화면이 표시됩니다.

- Logout By(로그아웃 기준) - 로그아웃해야 하는 세션을 필터링하는 데 사용할 기준을 선택합니다. --All Sessions(모든 세션)-- 이외의 항목을 선택한 경우 Logout By(로그아웃 기준) 오른쪽에 있는 상자가 활성화됩니다. Logout By(로그아웃 기준)에서 Protocol(프로토콜) 값을 선택하면 상자가 목록으로 바뀌며, 이 목록에서 로그아웃 필터로 사용할 프로토콜 유형을 선택할 수 있습니다.

이 목록의 기본값은 IPsec입니다. Protocol(프로토콜) 이외의 선택 항목은 이 열에 적절한 값을 제공해야 합니다.

활성 AnyConnect 세션 모니터링

Monitoring(모니터링) > VPN > VPN Statistics(VPN 통계) > Sessions(세션)

AnyConnect 클라이언트 세션을 사용자 이름, IP 주소, 주소 유형 또는 공개 주소 순으로 정렬할 수 있습니다.

VPN 세션 세부사항 모니터링

Monitoring(모니터링) > VPN > VPN Statistics(VPN 통계) > Sessions(세션) > Details(세부사항)

선택한 세션에 대한 구성 설정, 통계, 상태 정보를 볼 수 있습니다.

- NAC Result and Posture Token(NAC 결과 및 상태 토큰)

ASA에서 NAC(Network Admission Control)를 구성한 경우에만 ASDM의 이 열에 값이 표시됩니다.

- Accepted(허용됨) - ACS에서 원격 호스트의 상태를 성공적으로 검증했습니다.
- Rejected(거부됨) - ACS에서 원격 호스트의 상태를 성공적으로 검증할 수 없습니다.
- Exempted(제외됨) - 원격 호스트가 ASA에 구성된 Posture Validation Exception(상태 검증 예외) 목록에 따라 상태 검증에서 제외되었습니다.
- Non-Responsive(응답 안 함) - 원격 호스트가 EAPoUDP Hello 메시지에 응답하지 않았습니다.
- Hold-off(보류) - 성공적인 상태 검증 후 ASA와 원격 호스트 간의 EAPoUDP 통신이 끊어졌습니다.
- N/A(해당 없음) - VPN NAC 그룹 정책에 따라 원격 호스트에 대한 NAC가 비활성화되었습니다.
- Unknown(알 수 없음) - 상태 검증이 진행 중입니다.

상태 토큰은 Access Control Server에서 구성할 수 있는 알림 텍스트 문자열입니다. ACS는 시스템 모니터링, 보고, 디버깅 및 로깅에 유용한 정보를 제공하기 위해 ASA로 상태 토큰을 다운로드합니다. NAC 결과를 따르는 일반적인 상태 토큰은 Healthy(정상), Checkup(점검), Quarantine(격리), Infected(감염됨) 또는 Unknown(알 수 없음)입니다.

Session Details(세션 세부사항) 창의 Details(세부사항) 탭에는 다음 열이 표시됩니다.

- ID - 세션에 동적으로 할당된 고유 ID입니다. 이 ID는 세션에 대한 ASA 인덱스 역할을 합니다. ASA에서는 이 인덱스를 사용하여 세션에 대한 정보를 표시하고 유지 관리합니다.
- Type(유형) - 세션의 유형입니다(IKE, IPsec 또는 NAC).
- Local Addr., Subnet Mask, Protocol, Port, Remote Addr., Subnet Mask, Protocol, and Port(로컬 주소, 서브넷 마스크, 프로토콜, 포트, 원격 주소, 서브넷 마스크, 프로토콜 및 포트) - 실제(로컬) 피어에 할당된 주소 및 포트와 외부 라우팅을 위해 이 피어에 할당된 주소 및 포트입니다.
- Encryption(암호화) - 이 세션에서 사용하는 데이터 암호화 알고리즘입니다(있는 경우).

- Assigned IP Address and Public IP Address(할당된 IP 주소 및 공개 IP 주소) - 이 세션의 원격 피어에 할당된 비공개 IP 주소를 표시합니다. '내부' 또는 '가상' IP 주소라고도 하는 할당된 IP 주소를 통해 원격 피어는 비공개 네트워크에서 호스트 역할을 할 수 있습니다. 두 번째 필드에는 이 세션의 원격 컴퓨터에 대한 공개 IP 주소가 표시됩니다. 외부 IP 주소라고도 하는 공개 IP 주소는 일반적으로 ISP에서 클라이언트에 할당합니다. 이 IP 주소를 통해 원격 컴퓨터는 공개 네트워크에서 호스트 역할을 할 수 있습니다.
- Other(기타) - 세션과 연관된 기타 특성입니다.

IKE 세션, IPsec 세션 및 NAC 세션에 적용되는 특성은 다음과 같습니다.

- Revalidation Time Interval(재검증 시간 간격) - 성공한 각 상태 검증 간에 필요한 시간 간격(초)입니다.
- Time Until Next Revalidation(다음 재검증까지의 시간) - 마지막 상태 검증 시도에 실패한 경우 0입니다. 그렇지 않으면 Revalidation Time Interval(재검증 시간 간격)과 마지막으로 상태 검증에 성공한 이후에 경과한 시간(초) 간의 차이입니다.
- Status Query Time Interval(상태 쿼리 시간 간격) - 성공한 각 상태 검증 또는 상태 쿼리 응답과 다음 상태 쿼리 응답 간에 허용되는 시간(초)입니다. 상태 쿼리는 마지막 상태 검증 후 호스트의 상태가 변경되었는지 여부를 나타내기 위해 ASA에서 원격 호스트로 보내는 요청입니다.
- EAPoUDP Session Age(EAPoUDP 세션 기간) - 마지막으로 상태 검증에 성공한 이후에 경과한 시간(초)입니다.
- Hold-Off Time Remaining(남은 보류 시간) - 마지막 상태 검증에 성공한 경우 0초입니다. 그렇지 않으면 다음 상태 검증 시도 시까지 남은 시간(초)입니다.
- Posture Token(상태 토큰) - Access Control Server에서 구성할 수 있는 알림 텍스트 문자열입니다. ACS는 시스템 모니터링, 보고, 디버깅 및 로깅에 유용한 정보를 제공하기 위해 ASA로 상태 토큰을 다운로드합니다. 일반적인 상태 토큰은 Healthy(정상), Checkup(점검), Quarantine(격리), Infected(감염됨) 또는 Unknown(알 수 없음)입니다.
- Redirect URL(리디렉션 URL) - 상태 검증 또는 클라이언트리스 인증 후 ACS는 세션에 대한 액세스 정책을 ASA로 다운로드합니다. 리디렉션 URL은 액세스 정책 페이로드의 선택적 부분입니다. ASA는 원격 호스트에 대한 모든 HTTP(포트 80) 및 HTTPS(포트 443) 요청을 리디렉션 URL(있는 경우)로 리디렉션합니다. 액세스 정책에 리디렉션 URL이 포함되지 않은 경우에는 ASA에서 원격 호스트의 HTTP 및 HTTPS 요청을 리디렉션하지 않습니다.

  리디렉션 URL은 IPsec 세션이 종료되거나 상태 재검증이 수행될 때까지 유효한 상태로 유지되며, 그 동안 ACS는 리디렉션 URL을 포함하지 않거나 다른 리디렉션 URL을 포함할 수 있는 새 액세스 정책을 다운로드합니다.

  More(추가) - 세션 또는 터널 그룹을 재검증하거나 초기화하려면 이 버튼을 누릅니다.

ACL 탭에는 세션과 일치하는 ACE가 포함된 ACL이 표시됩니다.

클러스터 로드 모니터링

Monitoring(모니터링) > VPN> VPN Statistics(VPN 통계) > Cluster Loads(클러스터 로드)

VPN 로드 밸런싱 클러스터에 있는 서버 간의 현재 트래픽 로드 분배를 확인할 수 있습니다. 서버가 클러스터에 속하지 않은 경우 해당 서버는 VPN 로드 밸런싱에 참여하지 않음을 알리는 정보 메시지가 나타납니다.

VPN 암호 모니터링

Monitoring(모니터링**) > VPN> VPN Statistics(VPN** 통계**) > Crypto Statistics(**암호 통계**)**

ASA의 현재 활성 사용자 및 관리자 세션에 대한 암호 통계를 확인할 수 있습니다. 테이블의 각 행은 하나의 암호 통계를 나타냅니다.

압축 통계 모니터링

Monitoring(모니터링**) > VPN> VPN Statistics(VPN** 통계**) > Compression Statistics(**압축 통계**)**

ASA의 현재 활성 사용자 및 관리자 세션에 대한 압축 통계를 확인할 수 있습니다. 테이블의 각 행은 하나의 압축 통계를 나타냅니다.

암호화 통계 모니터링

Monitoring(모니터링**) > VPN> VPN Statistics(VPN** 통계**) > Encryption Statistics(**암호화 통계**)**

ASA의 현재 활성 사용자 및 관리자 세션에서 사용하는 데이터 암호화 알고리즘을 확인할 수 있습니다. 테이블의 각 행은 하나의 암호화 알고리즘 유형을 나타냅니다.

글로벌 IKE/IPsec 통계 모니터링

Monitoring(모니터링**) > VPN> VPN Statistics(VPN** 통계**) > Global IKE/IPSec Statistics(**글로벌 **IKE/IPSec** 통계**)**

ASA의 현재 활성 사용자 및 관리자 세션에 대한 글로벌 IKE/IPsec 통계를 확인할 수 있습니다. 테이블의 각 행은 하나의 글로벌 통계를 나타냅니다.

NAC 세션 모니터링 요약

활성 및 누적 NAC(Network Admission Control) 세션을 확인할 수 있습니다.

- Active NAC Sessions(활성 NAC 세션) - 상태 검증을 받아야 하는 원격 피어에 대한 일반적인 통계입니다.
- Cumulative NAC Sessions(누적 NAC 세션) - 상태 검증을 받아야 하거나 이전에 받아야 했던 원격 피어에 대한 일반적인 통계입니다.
- Accepted(허용됨) - 상태 검증에 통과하여 Access Control Server로부터 액세스 정책을 부여받은 피어 수입니다.
- Rejected(거부됨) - 상태 검증에 실패하여 Access Control Server로부터 액세스 정책을 부여받지 못한 피어 수입니다.
- Exempted(제외됨) - ASA에 구성된 Posture Validation Exception(상태 검증 예외) 목록의 항목과 일치하기 때문에 상태 검증을 받을 필요가 없는 피어 수입니다.

- Non-responsive(응답 안 함) - 상태 검증을 위한 EAP(확장 가능 인증 프로토콜) over UDP 요청에 응답하지 않는 피어 수입니다. 실행 중인 CTA가 없는 피어는 이러한 요청에 응답하지 않습니다. ASA 구성에서 클라이언트리스 호스트를 지원하는 경우 Access Control Server는 클라이언트리스 호스트와 연관된 액세스 정책을 이러한 피어의 ASA로 다운로드합니다. 그렇지 않으면 ASA는 NAC 기본 정책을 할당합니다.
- Hold-off(보류) - 성공적인 상태 검증 후 ASA에서 EAPoUDP 통신이 끊어진 피어 수입니다. NAC Hold Timer(NAC 보류 타이머) 특성(Configuration(구성) > VPN > NAC)에 따라 이 유형의 이벤트와 다음 상태 검증 시도 간의 지연 시간이 결정됩니다.
- N/A(해당 없음) - VPN NAC 그룹 정책에 따라 NAC가 비활성화된 피어 수입니다.
- Revalidate All(모두 재검증) - 피어 또는 할당된 액세스 정책(즉, 다운로드한 ACL)의 상태가 변경된 경우에 클릭합니다. 이 버튼을 클릭하면 ASA에서 관리하는 모든 NAC 세션에 대한 조건 없는 상태 검증이 새로 시작됩니다. 이 버튼을 클릭하기 전에 각 세션에 적용되던 상태 검증 및 할당된 액세스 정책은 새 상태 검증에 성공하거나 실패할 때까지 유효한 상태로 유지됩니다. 이 버튼을 클릭한 경우 상태 검증에서 제외된 세션은 영향을 받지 않습니다.
- Initialize All(모두 초기화) - 피어 또는 할당된 액세스 정책(즉, 다운로드한 ACL)의 상태가 변경된 경우 세션에 할당된 리소스를 해제하려면 클릭합니다. 이 버튼을 클릭하면 ASA에서 관리하는 모든 NAC 세션의 상태 검증에 사용된 EAPoUDP 연결 및 할당된 액세스 정책이 제거되고, 조건 없는 상태 검증이 새로 시작됩니다. NAC 기본 ACL은 재검증 기간에 유효하므로 세션 초기화 때문에 사용자 트래픽이 중단될 수 있습니다. 이 버튼을 클릭한 경우 상태 검증에서 제외된 세션은 영향을 받지 않습니다.

프로토콜 통계 모니터링

Monitoring(모니터링) > VPN> VPN Statistics(VPN 통계) > Protocol Statistics(프로토콜 통계)

ASA의 현재 활성 사용자 및 관리자 세션에서 사용하는 프로토콜을 확인할 수 있습니다. 테이블의 각 행은 하나의 프로토콜 유형을 나타냅니다.

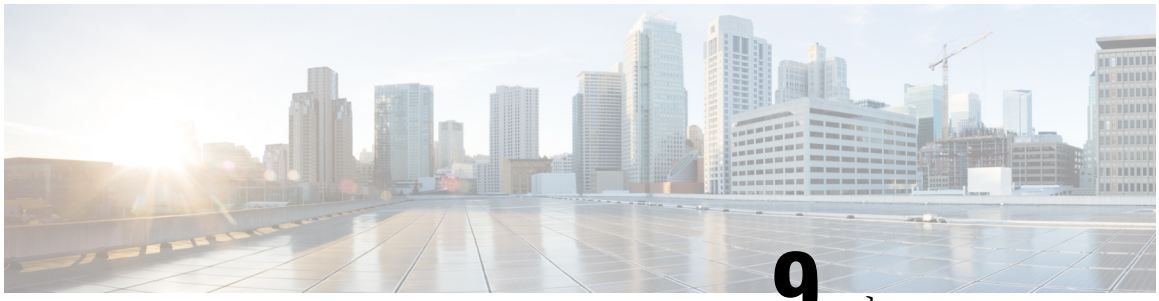
VLAN 매핑 세션 모니터링

이그레스(egress) VLAN에 할당된 세션 수를 확인할 수 있습니다. 이 세션 수는 사용 중인 각 그룹의 Restrict Access to VLAN(VLAN에 대한 액세스 제한) 매개변수 값에 의해 결정됩니다. ASA에서 모든 트래픽을 지정된 VLAN으로 전달합니다.

클라이언트리스 SSL VPN 세션에 대한 SSO 통계 모니터링

Monitoring(모니터링) > VPN > WebVPN > SSO Statistics(SSO 통계)

ASA에 대해 구성된 현재 활성 SSO 서버에 대한 단일 로그인 통계를 확인할 수 있습니다.



9 장

SSL 설정

SSL 설정

다음 위치 중 하나에 SSL 설정을 구성합니다.

- **Configuration(구성) > Device Management(디바이스 관리) > Advanced(고급) > SSL Settings(SSL 설정)**
- **Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > Advanced(고급) > SSL Settings(SSL 설정)**

ASA는 ASDM, 클라이언트리스 SSL VPN, VPN 및 브라우저 기반 세션을 위해 보안 메시지 전송을 지원하는 SSL(Secure Socket Laye) 프로토콜과 TLS(Transport Layer Security)를 사용합니다. 또한 DTLS는 AnyConnect VPN 클라이언트 연결에 사용됩니다. SSL Settings(SSL 설정) 창에서 클라이언트와 서버에 대한 SSL 버전 및 암호화 알고리즘을 구성할 수 있습니다. 또한 이전에 구성한 신뢰 지점을 특정 인터페이스에 적용하고 관련 신뢰 지점이 없는 인터페이스에 대해 대체 신뢰 지점을 구성할 수 있습니다.

참고

9.3(2) 릴리스의 경우 SSLv3 항목은 더 이상 사용되지 않습니다. 이제 기본값은 **any** 대신 **tlsv1**입니다. **any** 키워드는 더 이상 사용되지 않습니다. **any**, **sslv3** 또는 **sslv3-only**를 선택한 경우 경고와 함께 설정이 적용됩니다. 계속하려면 **OK(확인)**를 클릭하십시오. 다음 주요 ASA 릴리스에서 이 키워드는 ASA에서 제거됩니다.

9.4(1) 버전의 경우 모든 SSLv3 키워드가 ASA 구성에서 제거되고, SSLv3 지원이 ASA에서 제거되었습니다. SSLv3을 활성화한 경우 SSLv3 옵션이 포함된 명령에서 부팅 시간 오류가 표시됩니다. 그런 다음 ASA가 기본값인 TLSv1을 사용하도록 되돌아갑니다.

Citrix Mobile Receiver가 TLS 1.1/1.2 프로토콜을 지원하지 않을 수 있습니다. 호환성에 대한 자세한 내용은 https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/citrix-receiver-feature-matrix.pdf 를 참조하십시오.

필드

- **Server SSL Version(**서버 **SSL** 버전**)** - ASA가 서버로 작동할 때 사용하는 SSL/TLS 프로토콜의 최소 버전을 드롭다운 목록에서 지정합니다.

모든	SSLv2 클라이언트 Hello를 수락하고 가장 높은 일반 버전을 협상합니다.
SSL V3	SSLv2 클라이언트 Hello를 수락하고 SSLv3 이상을 협상합니다.
TLS V1	SSLv2 클라이언트 Hello를 수락하고 TLSv1 이상을 협상합니다.
TLSv1.1	SSLv2 클라이언트 Hello를 수락하고 TLSv1.1 이상을 협상합니다.
TLSV1.2	SSLv2 클라이언트 Hello를 수락하고 TLSv1.2 이상을 협상합니다.
DTLSv1	DTLSv1 클라이언트 Hello를 수락하고 DTLSv1 이상을 협상합니다.
DTLS1.2	DTLSv1.2 클라이언트 Hello를 수락하고 DTLSv1.2 이상을 협상합니다.

참고 DTLS의 구성 및 사용은 Cisco AnyConnect 원격 액세스 연결에만 적용됩니다.

TLS 세션이 안전한지 또는 DTLS 대신 동일하거나 더 높은 TLS 버전을 사용하여 DTLS 세션보다 더 안전한지 확인합니다. 이러한 점을 고려할 때 TLSV1.2는 DTLSV1.2 선택 시 허용 가능한 유일한 TLS 버전이며 모든 TLS 버전은 DTLS 1과 동일하거나 더 높은 버전이므로 DTLS1과 함께 사용될 수 있습니다.

- **Client SSL Version(**클라이언트 **SSL** 버전**)** - ASA가 클라이언트로 작동할 때 사용하는 SSL/TLS 프로토콜의 최소 버전을 드롭다운 목록에서 지정합니다. (DTLS는 SSL 클라이언트 역할에 대해 사용할 수 없음)

모든	SSLv3 클라이언트 Hello를 전송하고 SSLv3 이상을 협상합니다.
SSL V3	SSLv3 클라이언트 Hello를 전송하고 SSLv3 이상을 협상합니다.
TLS V1	TLSv1 클라이언트 Hello를 전송하고 TLSv1 이상을 협상합니다.

TLSv1.1	TLSv1.1 클라이언트 Hello를 전송하고 TLSv1.1 이상을 협상합니다.
TLSV1.2	TLSv1.2 클라이언트 Hello를 전송하고 TLSv1.2 이상을 협상합니다.

- **Diffie-Hellmann group to be used with SSL(SSL**에서 사용할 **Diffie-Hellmann** 그룹**)** - 드롭다운 목록에서 그룹을 선택합니다. 사용 가능한 옵션은 Group1 - 768-bit modulus(그룹 1 - 768비트 모듈러스), Group2 - 1024-bit modulus(그룹 2 - 1024비트 모듈러스), Group5 - 1536-bit modulus(그룹 5 - 1536비트 모듈러스), Group14 - 2048-bit modulus, 224-bit prime order(그룹 14 - 2048비트 모듈러스, 224비트 소수 위수) 및 Group24 - 2048-bit modulus, 256-bit prime order(그룹 24 - 2048비트 모듈러스, 256비트 소수 위수)입니다. 기본값은 Group2입니다.
- **ECDH group to be used with SSL(SSL**에서 사용할 **ECDH** 그룹**)** - 드롭다운 목록에서 그룹을 선택합니다. 사용 가능한 옵션은 Group19 - 256-bit EC(그룹 19 - 256비트 EC), Group20 - 384-bit EC(그룹 20 - 384비트 EC) 및 Group21 - 521-bit EC(그룹 21 - 521비트 EC)입니다. 기본값은 Group19입니다.

참고 ECDSA 및 DHE 암호가 우선 순위가 가장 높습니다.

- **Encryption(**암호화**)** - 지원할 버전, 보안 수준 및 SSL 암호화 알고리즘을 지정합니다. **Edit(**수정**)**를 클릭하여 Configure Cipher Algorithms/Custom String(암호화 알고리즘/사용자 지정 문자열 구성) 대화 상자에서 테이블 항목을 정의하거나 수정합니다. SSL 암호화 보안 수준을 선택한 다음 **OK(**확인**)**를 클릭합니다.
  - **Cipher Version(**암호화 버전**)** - ASA에서 지원하고 SSL 연결에 사용하는 암호화 버전을 나열합니다.
  - **Cipher Security Level(**암호화 보안 수준**)** - ASA에서 지원하고 SSL 연결에 사용하는 암호화 보안 수준을 나열합니다. 다음 옵션 중 하나를 선택합니다.

    All(모두**)** - NULL-SHA를 비롯한 모든 암호화를 포함합니다.

    Low(낮음**)** - NULL-SHA를 제외한 모든 암호화를 포함합니다.

    Medium(보통**)**은 NULL-SHA, DES-CBC-SHA, RC4-SHA 및 RC4-MD5를 제외한 모든 암호화를 포함합니다(기본값).

    Fips - 모든 FIPS 호환 암호화(NULL-SHA, DES-CBC-SHA, RC4-MD5, RC4-SHA 및 DES-CBC3-SHA 제외)를 포함합니다.

    High(높음**)**는 AES-256 SHA-2 암호화만 포함하며, TLS 버전 1.2에만 적용됩니다.

    Custom(사용자 지정**)**은 Cipher algorithms/custom string(암호화 알고리즘/사용자 지정 문자열) 상자에서 지정한 하나 이상의 암호화를 포함합니다. 이 옵션은 OpenSSL 암호화 정의 문자열을 사용하는 암호 그룹에 대한 모든 권한을 제공합니다.

- **Cipher Algorithms/Custom String(암호화 알고리즘/사용자 지정 문자열)** - ASA에서 지원하고 SSL 연결에 사용하는 암호화 알고리즘을 나열합니다. OpenSSL을 사용하는 암호화에 대한 자세한 내용은 https://www.openssl.org/docs/manmaster/man1/ciphers.html 섹션을 참고하십시오.

  ASA는 지원되는 암호화에 대한 우선 순위를 지정합니다. TLSv1.2에서만 지원되는 암호화는 TLSv1.1 또는 TLSv1.2에서는 지원되지 않습니다.

다음 암호화는 명시된 대로 지원됩니다.

- **Server Name Indication (SNI)(SNI(Server Name Indication))** - 도메인 이름 및 이 도메인과 연계할

암호화	TLSv1.1/DTLS V1	TLSV12
AES128-GCM-SHA256	아니요	예
AES128-SHA	예	예
AES128-SHA256	아니요	예
AES256-GCM-SHA384	아니요	예
AES256-SHA	예	예
AES256-SHA256	아니요	예
DERS-CBC-SHA	아니요	아니요
DES-CBC-SHA	예	예
DHE-RSA-AES128-GCM-SHA256	아니요	예
DHE-RSA-AES128-SHA	예	예
DHE-RSA-AES128-SHA256	아니요	예
DHE-RSA-AES256-GCM-SHA384	아니요	l
DHE-RSA-AES256-SHA	예	예
ECDHE-ECDSA-AES128-GCM-SHA256	아니요	예
ECDHE-ECDSA-AES128-SHA256	아니요	예
ECDHE-ECDSA-AES256-GCM-SHA384	아니요	예
ECDHE-ECDSA-AES256-SHA384	아니요	예
ECDHE-RSA-AES128-GCM-SHA256	예	예
ECDHE-RSA-AES128-SHA256	아니요	예
ECDHE-RSA-AES256-GCM-SHA384	아니요	예
ECDHE-RSA-AES256-SHA384	아니요	예

암호화	TLSv1.1/DTLS V1	TLSV12
NULL-SHA	아니요	아니요
RC4-MD5	아니요	아니요
RC4-SHA	아니요	아니요

을 지정합니다. **Add(**추가**)** 또는 **Edit(**수정**)**를 클릭하여 Add/Edit Server Name Indication (SNI)(SNI(Server Name Indication) 추가/수정) 대화 상자에서 각 인터페이스에 대한 도메인 및 신뢰 지점을 정의하거나 수정합니다.

- Specify domain(도메인 지정) - 도메인 이름을 입력합니다.
- Select trustpoint to associate with domain(도메인과 연계할 신뢰 지점 선택) - 드롭다운 목록에서 신뢰 지점을 선택합니다.

- **Certificates(**인증서**)** - 각 인터페이스에서 SSL 인증에 사용할 인증서를 할당합니다. **Edit(**수정**)**를 클릭하여 Select SSL Certificate(SSL 인증서 선택) 대화 상자에서 각 인터페이스에 대한 신뢰 지점을 정의하거나 수정합니다.
  - Primary Enrolled Certificate(등록된 기본 인증서) - 이 인터페이스의 인증서에 사용할 신뢰 지점을 선택합니다.
  - Load Balancing Enrolled Certificate(등록된 로드 밸런싱 인증서) - VPN 로드 밸런싱이 구성된 경우 인증서에 사용할 신뢰 지점을 선택합니다.
- **Fallback Certificate(**대체 인증서**)** - 연계된 인증서가 없는 인터페이스에 사용할 인증서를 선택하려면 클릭합니다. **None(**없음**)**을 선택하면 ASA에서 기본 RSA key-pair 및 인증서를 사용합니다.
- **Forced Certification Authentication Timeout(**강제 인증서 인증 시간 제한**)** - 인증서 인증이 시간 초과되기 전에 대기할 시간(분)을 구성합니다.
- **Apply(**적용**)** - 변경 사항을 저장하려면 클릭합니다.
- **Reset(**재설정**)** - 변경 사항을 제거하고 SSL 매개변수를 이전에 정의한 값으로 다시 설정하려면 클릭합니다.

10 장

용이한 VPN

이 장에서는 ASA를 Easy VPN 서버로 구성하는 방법 및 Cisco ASA with FirePOWER- 5506-X, 5506W-X, 5506H-X 및 5508-X 모델을 Easy VPN 원격 하드웨어 클라이언트로 구성하는 방법을 설명합니다.

Easy VPN 정보

Cisco Ezvpn은 원격 사무실 및 모바일 근무자용 VPN의 구성 및 구축을 크게 간소화합니다. Cisco Easy VPN은 사이트 대 사이트 및 원격 액세스 VPN에 유연성, 확장성 및 사용 편의성을 제공합니다. Cisco Unity 클라이언트 프로토콜을 구현하여 관리자가 Easy VPN 서버에서 대부분의 VPN 파라미터를 정의할 수 있으므로 Easy VPN Remote 구성이 간편해집니다.

FirePOWER 모델 5506-X, 5506W-X, 5506H-X, 5508-X를 사용하는 Cisco ASA는 VPN 터널을 Easy VPN 서버로 시작하는 하드웨어 클라이언트로 Easy VPN Remote를 사용하도록 지원합니다. Easy VPN 서버는 다른 ASA(모든 모델) 또는 Cisco IOS 기반 라우터가 될 수 있습니다. ASA는 Easy VPN Remote 및 Easy VPN 서버로 동시에 작동할 수 없습니다.

참고 Cisco ASA 5506-X, 5506W-X, 5506H-X, 5508-X 모델은 L2 스위칭이 아니라 L3 스위칭을 지원합니다. 내부 네트워크의 여러 호스트 또는 디바이스에서 Easy VPN Remote를 사용하는 경우 외부 스위치를 사용하십시오. ASA의 내부 네트워크에 단일 호스트가 있는 경우에는 스위치가 필요하지 않습니다.

다음 섹션에서는 Easy VPN 옵션과 설정에 대해 설명합니다. ASA를 Easy VPN Remote 하드웨어 클라이언트로 구성하려면 ASDM에서 **Configuration(구성) > VPN > Easy VPN Remote** 섹션으로 이동합니다. Easy VPN 서버에서 그룹 정책 속성을 구성하려면 **Configuration(구성) > Remote Access(원격 액세스) > Network (Client) Access(네트워크(클라이언트) 액세스) > Group Policies(그룹 정책) > Advanced(고급) > IPsec (IKEv1) Client(IPsec(IKEv1) 클라이언트) > Hardware Client(하드웨어 클라이언트)** 섹션으로 이동합니다.

Easy VPN 인터페이스

시스템 시작 시 Easy VPN 외부 및 내부 인터페이스가 보안 레벨에 따라 결정됩니다. 최저 보안 레벨의 물리적 인터페이스는 Easy VPN 서버에 대한 외부 연결에 사용됩니다. 최고 보안 레벨의 물리적 인터페이스는 보안 리소스에 대한 내부 연결에 사용됩니다. Easy VPN에서 동일한 최고 보안 레벨의 인터페이스가 둘 이상 있음을 확인하면 Easy VPN이 비활성화됩니다.

Easy VPN 연결

Easy VPN은 IPsec IKEv1 터널을 사용합니다. Easy VPN Remote 하드웨어 클라이언트의 구성은 Easy VPN 서버 헤드엔드의 VPN 구성과 호환되어야 합니다. 2차 서버를 사용하는 경우 해당 구성이 1차 서버와 동일해야 합니다.

ASA Easy VPN Remote는 1차 Easy VPN 서버의 IP 주소를 구성하며, 필요한 경우 최대 10개의 2차(백업) 서버도 구성합니다. 1차 서버에 대한 터널을 설정할 수 없는 경우, 클라이언트가 첫 번째 2차 VPN 서버에 연결하려고 시도한 다음, 8초 간격으로 VPN 서버 목록의 순서대로 시도합니다. 첫 번째 2차 서버에 대한 터널 설정에 실패하고, 이 시간 동안 1차 서버가 온라인 상태가 되는 경우, 클라이언트는 계속해서 두 번째 2차 VPN 서버에 대한 터널을 설정합니다.

1차적으로 Easy VPN 하드웨어 클라이언트 및 서버는 UDP(사용자 데이터그램 프로토콜) 패킷에서 IPsec을 캡슐화합니다. 특정 방화벽 규칙 또는 NAT 및 PAT 디바이스가 있는 일부 환경에서는 UDP를 금지합니다. 이러한 환경에서 표준 ESP(Encapsulating Security Protocol, Protocol 50) 또는 IKE(인터넷 키 교환국, UDP 500)를 사용하려면 TCP 패킷 내에서 IPsec을 캡슐화하여 보안 터널링을 활성화하도록 클라이언트 및 서버를 구성해야 합니다. 그러나 UDP를 허용하는 환경에서 IPsec over TCP를 구성하면 불필요한 오버헤드가 추가됩니다.

Easy VPN 터널 그룹

터널을 설정할 때 Easy VPN Remote에서 연결에 사용할 Easy VPN 서버에 구성된 터널 그룹을 지정합니다. Easy VPN 서버는 Easy VPN Remote 하드웨어 클라이언트로 그룹 정책 또는 사용자 속성을 푸시하여 터널 동작을 결정합니다. 특정 속성을 변경하려면 1차 또는 2차 Easy VPN 서버로 구성된 ASA에서 해당 속성을 수정해야 합니다.

작업의 Easy VPN 모드

이 모드는 엔터프라이즈 네트워크에서 터널을 통해 Easy VPN Remote 뒤에 있는 호스트에 액세스할 수 있는지 여부를 결정합니다.

- 클라이언트 모드(PAT(포트 주소 변환) 모드라고도 함)는 Easy VPN Remote 프라이빗 네트워크의 모든 디바이스를 엔터프라이즈 네트워크에 있는 디바이스와 격리합니다. Easy VPN Remote는 내부 호스트의 모든 VPN 트래픽에 대해 PAT(포트 주소 변환)를 수행합니다. Easy VPN Remote의 비공개 부분에 있는 네트워크와 주소는 숨겨져 있기 때문에 직접 액세스할 수 없습니다. Easy VPN 클라이언트 내부 인터페이스 또는 내부 호스트에 대해서는 IP 주소 관리가 필요하지 않습니다.
- 네트워크 확장 모드(NEM)는 내부 인터페이스 및 모든 내부 호스트가 터널을 통해 엔터프라이즈 네트워크 전체에서 라우팅 가능하도록 설정합니다. 내부 네트워크에 있는 호스트는 고정 IP 주소로 미리 구성되어 있는 액세스 가능한 서브넷(정적으로 또는 DHCP를 통해)에서 IP 주소를 얻습니다. PAT는 NEM에서 VPN 트래픽에 적용되지 않습니다. 이 모드에서는 내부 네트워크의 각

호스트에 대한 VPN 구성 또는 터널이 필요하지 않으며 Easy VPN Remote는 모든 호스트에 대해 터널링을 제공합니다.

Easy VPN 서버는 기본적으로 클라이언트 모드입니다. Easy VPN Remote에는 기본 모드가 없기 때문에 터널을 설정하려면 먼저 작동 모드 중 하나를 지정해야 합니다.

참고 NEM 모드에 대해 구성된 Easy VPN Remote ASA는 자동 터널 시작을 지원합니다. 자동 시작 시에는 터널을 설정하는 데 사용된 크리덴셜 구성 및 스토리지가 필요합니다. 보안 유닛 인증이 활성화된 경우, 자동 터널 시작이 비활성화됩니다.

여러 인터페이스가 구성된 네트워크 확장 모드에서 Easy VPN Remote는 가장 높은 보안 수준의 인터페이스에서 로컬로 암호화된 트래픽에 대한 터널만 구축합니다.

Easy VPN 사용자 인증

ASA Easy VPN Remote는 **vpnclient username** 명령을 사용하여 자동 로그인.

추가 보안을 위해 Easy VPN 서버에는 다음 항목이 필요할 수 있습니다.

- 보안 유닛 인증(SUA) — 사용자에게 수동으로 인증하도록 요청하면서 구성된 사용자 이름 및 비밀번호를 무시합니다. 기본적으로 SUA가 비활성화되며 Easy VPN 서버에서 SUA를 활성화합니다.
- 개별 사용자 인증(IUA) - 사용자가 Easy VPN Remote 뒤에서 엔터프라이즈 VPN 네트워크에 대한 액세스를 수신하기 전에 인증하도록 요청합니다. 기본적으로 IUA가 비활성화되며 Easy VPN 서버에서 IUA를 활성화합니다.

  IUA를 사용할 경우, Cisco IP Phone 또는 프린터와 같은 특정 디바이스는 하드웨어 클라이언트 뒤에서 개별 사용자 인증을 우회해야 합니다. 이렇게 구성하려면 **ip-phone-bypass** 명령을 사용하여를 지정하고 MAC 주소 면제 시을 사용합니다.

  또한, Easy VPN 서버는 Easy VPN 서버가 클라이언트의 액세스를 종료한 후에 유휴 시간 제한 기간을 설정하거나 제거할 수 있습니다.

Cisco Easy VPN 서버는 HTTP 트래픽을 차단하고 사용자 이름 및 비밀번호가 구성되지 않았거나 SUA가 비활성화되었거나 IUA가 활성화된 경우 사용자를 로그인 페이지로 리디렉션합니다. HTTP 리디렉션은 자동이며 Easy VPN 서버에서 구성할 필요가 없습니다.

Remote Management(원격 관리)

ASA는 Easy VPN Remote 하드웨어 클라이언트가 추가 IPsec 암호화를 사용하거나 사용하지 않고 SSH 또는 HTTPS를 사용하는 관리 액세스를 지원할 때 작동합니다.

기본적으로 관리 터널은 SSH 내부의 IPsec 암호화 또는 HTTPS 암호화를 사용합니다. 외부에서 관리 액세스를 허용하는 IPsec 암호화 레이어를 지울 수 있습니다. 터널 관리를 지우면 IPsec 암호화 레벨만 제거되며 SSH 또는 HTTPS와 같이 연결에 존재하는 다른 암호화에는 영향을 주지 않습니다.

추가 보안을 위해 Easy VPN Remote는 IPsec 암호화를 요청하고 특정 호스트 또는 회사측의 네트워크에 대한 관리 액세스를 제한할 수 있습니다.

참고 NAT 디바이스가 ASA Easy VPN Remote와 인터넷 사이에서 작동하는 경우 ASA Easy VPN Remote에서 관리 터널을 구성하지 마십시오. 해당 구성에서 원격 관리를 지웁니다.

구성에 관계없이 DHCP 요청(갱신 메시지 포함)은 IPsec 터널을 통해 흐를 수 없습니다. vpnclient 관리 터널에서도 DHCP 트래픽은 금지됩니다.

Easy VPN Remote 구성

ASA를 Easy VPN Remote 하드웨어 클라이언트로 구성합니다.

참고 FirePOWER- 5506-X, 5506W-X, 5506H-X 및 5508-X 모델을 사용하는 Cisco ASA만 Easy VPN Remote 하드웨어 클라이언트로 구성할 수 있습니다.

시작하기 전에

Easy VPN Remote를 구성하려면 다음 정보를 수집합니다.

- 1차 Easy VPN 서버 및 2차 서버(사용 가능한 경우)의 주소.
- 주소 지정 모드인 클라이언트 또는 NEM, Easy VPN Remote는 작동해야 합니다.
- Easy VPN 서버 그룹 정책 이름 및 비밀번호(사전 공유 키) 또는 원하는 그룹 정책을 선택 및 인증하는 사전 구성된 신뢰 지점.
- VPN 터널을 사용하도록 권한이 부여된 Easy VPN 서버에 구성된 사용자.

Configuration(구성) > VPN > Easy VPN Remote

Enable Easy VPN Remote(Easy VPN Remote 활성화) — Easy VPN Remote 기능을 활성화하고 구성을 위해 이 대화 상자의 나머지 필드를 사용하도록 합니다.

Mode(모드) — Client mode(클라이언트 모드) 또는 Network extension mode(네트워크 확장 모드)를 선택합니다.

- **Client mode(클라이언트 모드)** — PAT(포트 주소 변환) 모드를 사용하여 클라이언트를 기준으로 엔터프라이즈 네트워크에서 내부 호스트의 주소를 격리합니다.
- **Network extension mode(네트워크 확장 모드)** — 이러한 주소는 엔터프라이즈 네트워크에서 액세스할 수 있도록 합니다.

참고 Easy VPN Remote가 NEM을 사용 중이며 보조 서버에 연결한 경우, 각 헤드엔드에 대한 ASDM 연결을 설정하고 Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > Network (Client) Access(네트워크(클라이언트) 액세스) > Advanced(고급) > IPsec > Crypto Maps(암호화 맵)에서 생성한 암호화 맵에서 Enable Reverse Route Injection(역방향 라우팅 주입 활성화)을 확인하여 RRI를 사용하여 원격 네트워크의 동적 알림을 구성합니다.

- **Auto connect(**자동 연결**)** — Easy VPN Remote는 다음 내용 모두가 참인 경우를 제외하고, 자동 IPsec 데이터 터널을 설정합니다. 네트워크 확장 모드가 로컬에서 구성되었으며 스플릿 터널링이 Easy VPN Remote에 푸시된 그룹 정책에서 구성되었습니다. 두 가지 내용 모두 참인 경우, 이 속성을 선택하면 IPsec 데이터 터널의 설정을 자동화합니다. 기타 경우에는 이 특성은 아무런 영향을 주지 않습니다.

Group Settings(그룹 설정**)** — 사용자 인증을 위해 사전 공유 키 또는 X.509 인증서를 사용할지 여부를 지정합니다.

- **Pre-shared key(**사전 공유 키**)** — 인증을 위해 사전 공유 키 사용을 활성화하고 그룹 정책 이름 및 해당 키를 포함하는 비밀번호를 지정하기 위해 후속 Group Name(그룹 이름), Group Password(그룹 비밀번호), Confirm Password(비밀번호 확인) 필드를 사용할 수 있도록 설정합니다.
  - **Group Name(**그룹 이름**)** — 인증에 사용할 그룹 정책의 이름을 지정합니다.
  - **Group Password(**그룹 비밀번호**)** — 지정된 그룹 정책에 사용할 비밀번호를 지정합니다.
  - **Confirm Password(**비밀번호 확인**)** — 방금 입력한 그룹 비밀번호를 확인하도록 요청합니다.
- **X.509 Certificate(X.509** 인증서**)** — 인증을 위해 인증 기관에서 제공한 X.509 디지털 인증서를 사용하도록 지정합니다.
  - **Select Trustpoint(**신뢰 지점 선택**)** — IP 주소 또는 호스트 이름이 될 수 있는 신뢰 지점을 드롭다운 목록에서 선택할 수 있습니다. 신뢰 지점을 정의하려면 이 영역의 하단에 있는 신뢰 지점 구성에 대한 링크를 클릭합니다.
  - **Send certificate chain(**인증서 체인 전송**)** — 인증서 자체 뿐만 아니라 인증서 체인 전송을 활성화합니다. 이 작업은 전송 시 루트 인증서 및 하위 CA 인증서를 포함합니다.

User Settings(사용자 설정**)** — 사용자 로그인 정보를 구성합니다.

- **User Name(**사용자 이름**)** — Easy VPN Remote 연결을 위해 VPN 사용자 이름을 구성합니다. Xauth는 TACACS+ 또는 RADIUS를 사용하여 IKE 내에서 사용자를 인증할 수 있는 기능을 제공합니다. Xauth는 RADIUS 또는 다른 지원되는 사용자 인증 프로토콜을 사용하여 사용자를 인증합니다(이 경우, Easy VPN 하드웨어 클라이언트). XAUTH 사용자 이름 및 비밀번호 파라미터는 보안 장치 인증이 비활성화되고 서버에서 Xauth 크리덴셜을 요청하는 경우에 사용됩니다. 보안 장치 인증이 활성화된 경우에는 이러한 파라미터가 무시되고 ASA에서 사용자에게 사용자 이름 및 비밀번호를 묻는 프롬프트를 표시합니다.

- **User Password(**사용자 비밀번호**)** 및 **Confirm Password(**비밀번호 확인**)** —Easy VPN Remote 연결을 위해 VPN 사용자 비밀번호를 구성 및 확인합니다.

Easy VPN Server To Be Added(추가될 **Easy VPN** 서버**)** — Easy VPN 서버를 추가하거나 제거합니다. 모든 ASA는 Easy VPN 서버로 작동할 수 있습니다. 연결을 설정하려면 먼저 서버를 구성해야 합니다. ASA는 IPv4 주소, 이름 데이터베이스 또는 DNS 이름을 지원하며, 이 순서대로 주소를 확인합니다. Easy VPN 서버 목록에서 첫 번째 서버는 1차 서버입니다. 1차 서버 외에 최대 10개의 백업 서버도 지정할 수 있습니다.

- **Easy VPN Server(Easy VPN** 서버**)** — 우선 순위에 따라 구성된 Easy VPN 서버를 나열합니다.
- **Name or IP Address(**이름 또는 **IP** 주소**)** — 목록에 추가할 Easy VPN 서버의 이름 또는 IP 주소입니다.
- **Add(**추가**)** 및 **Remove(**제거**)** — Easy VPN 서버 목록에 지정된 서버를 이동 및 제거합니다.
- **Move Up(**위로 이동**)** 및 **Move Down(**아래로 이동**)** — Easy VPN 서버 목록에서 서버의 위치를 변경합니다. 이러한 버튼은 목록에 둘 이상의 서버가 있는 경우에만 사용할 수 있습니다.

Configuration(구성**) > VPN > Easy VPN Remote > Advanced(**고급**)**

MAC Exemption(MAC 면제**)** — Easy VPN Remote 연결을 위해 디바이스 패스 스루에 사용된 MAC 주소 및 마스크 집합을 구성합니다. Cisco IP Phone, 프린터 같은 특정 디바이스는 인증을 수행할 수 없으므로 개별 장치 인증에 참여할 수 없습니다. 이러한 디바이스를 수용하려면 MAC 면제 속성에서 활성화한 디바이스 패스 스루 기능은 개별 사용자 인증이 활성화된 경우 인증에서 지정된 MAC 주소를 사용하는 디바이스를 제외합니다.

- **MAC Address(MAC** 주소**)** — 인증에서 지정된 MAC 주소를 사용하는 디바이스를 제외합니다.

  MAC 주소를 지정하는 형식이며 이 필드는 마침표로 구분된 3개의 16진수 숫자(예: 45ab.ff36.9999)를 사용합니다. MAC 주소의 첫 번째 24비트는 장비 조각의 제조업체를 나타냅니다. 마지막 24비트는 16진수 형식의 장치 일련 번호입니다.

- **MAC Mask(MAC** 마스크**)** — 이 필드에서 MAC 마스크를 지정하는 형식에는 마침표로 구분된 16진수 3개가 사용됩니다. 예를 들어 MAC 마스크 ffff.ffff.ffff는 지정한 MAC 주소와 일치합니다. 모두 0인 MAC 마스크는 일치하는 MAC 주소가 없으며, MAC 마스크 ffff.ff00.0000은 같은 제조업체에서 만든 모든 장치와 일치합니다.
- **Add(**추가**)** 및 **Remove(**제거**)** — MAC 주소/마스크 목록에 지정된 MAC 주소 및 마스크 쌍을 추가하거나 제거합니다.

Tunneled Management(터널링된 관리**)** — 디바이스 관리를 위해 IPsec 암호화를 구성하고 터널을 통해 Easy VPN 하드웨어 클라이언트 연결을 관리하는 것이 허용되는 네트워크를 지정합니다.

- **Enable Tunneled Management(**터널링된 관리 활성화**)** — 관리 터널에 이미 있는 SSH 또는 HTTPS 암호화에 IPsec 암호화 레이어를 추가합니다.
- **Clear Tunneled Management(**터널링된 관리 지우기**)** — 추가 암호화 없이 관리 터널에 이미 있는 암호화를 사용합니다. Clear Tunneled Management(터널링된 관리 지우기)를 선택하면 IPsec 암호

화 레벨만 제거되며 SSH 또는 HTTPS와 같이 연결에 존재하는 다른 암호화에는 영향을 주지 않습니다.

- **IP Address/Mask(IP** 주소/마스크**)** — 이 영역에서 Enable(활성화) 또는 Clear(지우기) 기능을 사용하여 작동하도록 구성된 IP 주소 및 마스크 쌍을 나열합니다.
  - **IP Address(IP** 주소**)** — VPN 터널을 통해 Easy VPN 하드웨어 클라이언트에 대한 관리 액세스 권한을 부여할 대상 호스트 또는 네트워크의 IP 주소를 지정합니다.
  - **Mask(**마스크**)** — 해당 IP 주소에 대한 네트워크 마스크를 지정합니다.
  - **Add/Remove(**추가/제거**)** — 지정된 IP 주소 및 마스크를 IP 주소/마스크 목록으로 이동하거나 제거합니다.

IPsec Over TCP — Easy VPN Remote 연결에서 PCT 캡슐화된 IPsec을 사용하도록 구성합니다.

참고 PCT 캡슐화된 IPsec을 사용하도록 Easy VPN Remote 연결을 구성하는 경우, 큰 패킷을 전송하도록 ASA를 구성해야 합니다.

Configuration(구성**) > Remote Access VPN(**원격 액세스 **VPN) > Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**) > Advanced(**고급**) > IPsec > IPsec Fragmentation Policies(IPsec** 조각화 정책**)**으로 이동하여 외부 인터페이스를 두 번 클릭하고 DF Bit Setting Policy(DF 비트 설정 정책)를 Clear(지우기)로 설정합니다.

- **Enable(**활성화**)** — IPsec over TCP를 활성화합니다.
- **Enter Port Number(**포트 번호 입력**)** — IPsec over TCP 연결에 사용할 포트 번호를 지정합니다.

Server Certificate(서버 인증서**)** — 인증서 맵에서 지정한 특정 인증서가 있는 Easy VPN 서버에 대한 연결만 허용하도록 Easy VPN Remote 연결을 구성합니다. 이 파라미터를 사용하여 Easy VPN 서버 인증서 필터링을 활성화할 수 있습니다.

Easy VPN 서버 구성

시작하기 전에

모든 보조 Easy VPN 서버가 기본 Easy VPN 서버와 동일한 옵션 및 설정으로 구성되어 있는지 확인합니다.

프로시저

단계 **1** IPsec IKEv1을 지원하도록 Easy VPN 서버를 구성합니다. 일반 VPN 설정, 57 페이지 섹션을 참고하십시오.

단계 **2** 특정 Easy VPN 서버 속성을 설정합니다. 내부 그룹 정책, IPsec(IKEv1)에 대한 하드웨어 클라이언트 특성, 96 페이지을 참조하십시오.

Easy VPN에 대한 기능 기록

기능 이름	릴리스	기능 정보
ASA 5506-X, 5506W-X, 5506H-X 및 5508-X의 Cisco Easy VPN 클라이언트	9.5(1)	이 릴리스는 ASA 5506-X 시리즈 및 ASA 5508-X용 Cisco Easy VPN을 지원합니다. ASA는 VPN 헤드엔드에 연결할 때 VPN 하드웨어 클라이언트 역할을 합니다. ASA 뒤의 Easy VPN 포트에 있는 모든 디바이스(컴퓨터, 프린터 등)는 VPN을 통해 통신할 수 있습니다. 이러한 디바이스는 VPN 클라이언트를 개별적으로 실행할 필요가 없습니다. 참고로 하나의 ASA 인터페이스만 Easy VPN 포트 역할을 수행할 수 있습니다. 여러 디바이스를 해당 포트에 연결하려면 포트에 레이어 2 스위치를 배치한 다음 디바이스를 스위치에 연결해야 합니다. 다음 화면을 도입했습니다. **Configuration(구성) > VPN > Easy VPN Remote**

11 장

Virtual Tunnel Interface

이 장에서는 VTI 터널을 구성하는 방법에 대해 설명합니다.

Virtual Tunnel Interface 정보

ASA는 VTI(Virtual Tunnel Interface)라는 논리적 인터페이스를 지원합니다. 정책 기반 VPN 대신, Virtual Tunnel Interface가 구성된 피어 간에 VPN 터널을 생성할 수 있습니다. 이것은 각 터널 끝에 IPsec 프로필이 연결된 라우팅 기반 VPN을 지원합니다. 이를 통해 동적 또는 정적 경로를 사용할 수 있습니다. VTI에서 이그레스되는 트래픽은 암호화되어 피어로 전송되고, 연결된 SA가 VTI로 인그레스되는 트래픽의 암호를 해독합니다.

VTI를 사용하면 정적 암호화 맵 액세스 목록을 구성하고 이를 인터페이스에 매핑하기 위한 요구 사항이 없어집니다. 더 이상 모든 원격 서브넷을 추적하고 암호화 맵 액세스 목록에 포함하지 않아도 됩니다. 구축이 더 간편해지고, 동적 라우팅 프로토콜과 라우팅 기반 VPN을 지원하는 정적 VTI가 있어 가상 프라이빗 클라우드의 많은 요구 사항도 충족합니다.

Virtual Tunnel Interface에 대한 지침

IPv6

- IPv6은 지원되지 않습니다.

일반 구성 지침

- VTI는 IPsec 모드에서만 구성할 수 있습니다. ASA에서의 GRE 터널 종료는 지원되지 않습니다.
- 터널 인터페이스를 사용하여 트래픽에 대한 동적 또는 정적 경로를 사용할 수 있습니다.
- 기본 물리적 인터페이스에 따라 VTI에 대한 MTU가 자동으로 설정됩니다.

- NAT(Network Address Translation)를 적용해야 할 경우, IKE 및 ESP 패킷이 UDP 헤더에서 캡슐화됩니다.
- IKE 및 IPsec 보안 연결은 터널의 데이터 트래픽과 관계없이 지속적으로 키가 재생성됩니다. 이렇게 하면 VTI 터널이 항상 가동됩니다.
- 터널 그룹 이름은 피어가 IKEv1 id로 전송하는 항목과 일치해야 합니다.
- 터널 그룹 이름은 피어가 IKEv1 또는 IKEv2 id로 전송하는 항목과 일치해야 합니다.
- LAN-to-LAN 터널 그룹에서 IKEv1의 경우, 터널 인증 방법이 디지털 인증서이거나 적피어가 적극적인 모드를 사용하도록 구성된 경우, IP 주소가 아닌 이름을 사용할 수 있습니다.
- VTI 및 암호화 맵 구성은 동일한 물리적 인터페이스에서 공존할 수 있지만, 암호화 맵에 구성된 피어 주소와 VTI에 대한 터널 대상은 서로 다릅니다.
- 기본적으로 VTI를 통과하는 모든 트래픽이 암호화됩니다.
- VTI 인터페이스에 대한 보안 레벨 구성이 없습니다.
- 액세스 목록은 VTI를 통과하는 트래픽을 제어하기 위해 VTI 인터페이스에 적용될 수 있습니다.
- VTI에서는 BGP만 지원됩니다.

상황 모드

단일 모드에서만 지원됩니다.

방화벽 모드

라우티드 모드에서만 지원됩니다.

VTI 터널 생성

VTI 터널을 구성하려면 IPsec 제안(변형 집합)을 생성합니다. IPsec 제안을 참조하는 IPsec 프로필을 생성한 다음 IPsec 프로필을 사용하는 VTI 인터페이스를 생성해야 합니다. 동일한 IPsec 제안 및 IPsec 프로필 파라미터가 있는 원격 피어를 구성합니다. 모든 터널 파라미터가 구성된 경우 SA 협상을 시작합니다.

참고 두 VPN VTI 도메인의 일부인 ASA의 경우 물리적 인터페이스에 BGP 인접성이 있습니다.

인터페이스 상태 검사로 인해 상태 변경이 트리거되면 BGP 인접성이 새 활성 피어로 다시 설정될 때까지 물리적 인터페이스의 경로가 삭제됩니다. 이 동작은 논리적 VTI 인터페이스에는 적용되지 않습니다.

프로시저

단계 1 IPsec 제안(변형 집합)을 추가합니다.

단계 2 IPsec 프로필을 추가합니다.

단계 3 VTI 터널을 추가합니다.

IPsec 제안서(변형 집합) 추가

변형 집합은 VTI 터널에서의 보안 트래픽에 필요합니다. IPsec 프로필의 일부로 사용되었으며 VPN에서 트래픽을 보호하는 보안 프로토콜 및 알고리즘 집합입니다.

시작하기 전에

- VTI와 연결된 IKEv1 세션을 인증하기 위해 사전 공유 키 또는 인증서 중 하나를 사용할 수 있습니다. VTI에 사용되는 터널 그룹에서 사전 공유 키를 구성해야 합니다.
- IKEv1을 사용하는 인증서 기반 인증의 경우, 이니시에이터에서 사용할 트러스트 포인트를 지정해야 합니다. 응답자의 경우 터널 그룹 명령에서 트러스트 포인트를 구성해야 합니다.
- VTI와 연결된 IKE 세션을 인증하기 위해 사전 공유 키 또는 인증서 중 하나를 사용할 수 있습니다. IKEv2의 경우 비대칭 인증 방법 및 키를 사용할 수 있습니다. IKEv1 및 IKEv2의 경우, VTI에 사용되는 터널 그룹에서 사전 공유 키를 구성해야 합니다.
- IKEv1을 사용하는 인증서 기반 인증의 경우, 이니시에이터에서 사용할 신뢰 지점을 지정해야 합니다. 응답자의 경우, 터널 그룹 명령에서 트러스트 포인트를 구성해야 합니다. Ikev2의 경우 이니시에이터 및 응답자 모두에 대한 터널 그룹 명령에서 인증에 사용할 트러스트 포인트를 구성해야 합니다.

프로시저

단계 1 **Configuration**(구성) > **Site-to-Site VPN**(사이트 대 사이트 **VPN**) > **Advanced**(고급) > **IPsec Proposals(Transform Sets)(IPsec** 제안(변형 집합)**)**를 선택합니다.

단계 2 보안 연결을 설정하려면 IKEv1 또는 IKEv2를 구성합니다.

- IKEv1을 구성합니다.

a) IPsec Proposals(Transform Sets)(IPsec 제안(변형 집합)) 패널에서 **Add**(추가)를 클릭합니다.
b) **Set Name**(집합 이름)을 입력합니다.
c) **Tunnel**(터널) 확인란의 기본값을 유지합니다.
d) **ESP Encryption(ESP** 암호화) 및 **ESP Authentication(ESP** 인증)을 선택합니다.
e) **OK**(확인)를 클릭합니다.

- IKEv2를 구성합니다.

a) IKEv2 IPsec Proposals(IKEv2 IPsec 제안) 패널에서 **Add(**추가**)**를 클릭합니다.
b) **Name(**이름**)** 및 **Encryption(**암호화**)**을 입력합니다.
c) **Integrity Hash(**무결성 해시**)**를 선택합니다.
d) **OK(**확인**)**를 클릭합니다.

IPsec 프로필 추가

IPsec 프로필에는 프로필이 참조하는 IPsec 제안 또는 변형 집합에 필요한 보안 프로토콜 및 알고리즘이 포함되어 있습니다. 이를 통해 두 개의 사이트 대 사이트 VTI VPN 피어 간에 논리적 보안 통신 경로가 보장됩니다.

프로시저

단계 **1** **Configuration(**구성**)** > **Site-to-Site VPN(**사이트 대 사이트 **VPN)** > **Advanced(**고급**)** > **IPsec Proposals(Transform Sets)(IPsec** 제안**(**변형 집합**))**를 선택합니다.

단계 **2** **IPsec Profile(IPsec** 프로필**)** 패널에서 **Add(**추가**)**를 클릭합니다.

단계 **3** IPsec 프로필 **Name(**이름**)**을 입력합니다.

단계 **4** IPsec 프로필에 대해 생성한 **IKE v1 IPsec Proposal(IKE v1 IPsec** 제안**)** 또는 **IKE v2 IPsec Proposal(IKE v2 IPsec** 제안**)**을 입력합니다. IKEv1 변형 집합 또는 IKEv2 IPsec 제안서를 선택할 수 있습니다.

단계 **5** 응답자 역할만 할 VTI 터널의 끝이 필요한 경우 **Responder only(**응답자 전용**)** 체크 박스를 선택합니다.

- 응답자로만 수행하도록 VTI 터널의 한 쪽 끝을 구성할 수 있습니다. 응답자 전용 끝에서는 터널 또는 키 재생성을 시작하지 않습니다.
- IKEv2를 사용 중인 이니시에이터 끝에서 IPsec 프로필의 수명 값보다 큰 보안 연결 수명 기간을 설정합니다. 이를 통해 이니시에이터 끝을 통한 키 재생성을 성공적으로 수행하고 터널이 계속 작동하도록 보장할 수 있습니다.
- 이니시에이터 끝의 키 재생성 구성을 알 수 없는 경우, 응답자 전용 모드를 제거하여 SA를 양방향으로 설정하거나 만료를 방지하기 위해 응답자 전용 끝에서 무한 IPsec 수명 값을 구성합니다.

단계 **6** (선택 사항) **Enable security association lifetime(**보안 연결 수명 활성화**)** 체크 박스를 선택하고 보안 연결 기간 값을 킬로바이트 및 초로 입력합니다.

단계 **7** (선택 사항) PFS를 활성화하려면 **PFS Settings(PFS** 설정**)** 체크 박스를 선택하고 필수 Diffie-Hellman 그룹을 선택합니다.

PFS(Perfect Forward Secrecy)는 암호화된 각 교환에 대해 고유 세션 키를 생성합니다. 이 고유한 세션 키는 후속 암호 해독에서 교환을 보호합니다. PFS를 구성하려면 PFS 세션 키를 생성할 때 사용할 Diffie-hellman 키 파생 알고리즘을 선택해야 합니다. 키 파생 알고리즘은 IPsec 보안 연계(SA) 키를 생성합니다. 각 그룹의 크기 모듈러스는 서로 다릅니다. 대형 모듈러스는 보안성은 더 높지만, 처리 시간이 더 오래 걸립니다. 두 피어에서 일치하는 Diffie-hellman 그룹을 가져야 합니다.

이를 통해 암호 키 결정 알고리즘의 장점이 확립됩니다. ASA는 이 알고리즘을 사용하여 암호화 및 해시 키를 파생합니다.

단계 **8** (선택 사항) **Enable sending certificate(**인증서 전송 활성화**)** 체크 박스를 선택하고 VTI 터널 연결을 시작하는 동안 사용할 인증서를 정의하는 **Trustpoint(**트러스트 포인트**)**를 선택합니다. 필요한 경우 **Chain(**체인**)** 체크 박스를 선택합니다.

단계 **9** **OK(**확인**)**를 클릭합니다.

단계 **10** **IPsec Proposals(Transform Sets)(IPsec** 제안**(**변형 집합**))** 기본 패널에서 **Apply(**적용**)**를 클릭합니다.

단계 **11** **Preview CLI Commands(**미리 보기 **CLI** 명령**)** 대화 상자에서 **Send(**전송**)**를 클릭합니다.

VTI 인터페이스 추가

새 VTI 인터페이스를 생성하고 VTI 터널을 설정하려면 다음 단계를 수행합니다.

참고 활성 터널의 라우터를 사용할 수 없는 경우 터널을 가동 상태로 유지하기 위해 IP SLA를 구현합니다. http://www.cisco.com/go/asa-config의 ASA 일반 운영 구성 가이드에서 고정 경로 추적 구성을 참고하십시오.

프로시저

단계 **1** **Configuration(**구성**)** > **Device Setup(**디바이스 설정**)** > **Interface Settings(**인터페이스 설정**)** > **Interfaces(**인터페이스**)**를 선택합니다.

단계 **2** **Add(**추가**)** > **VTI Interface(VTI** 인터페이스**)**를 선택합니다. **Add VTI Interface(VTI** 인터페이스 추가**)** 창이 나타납니다.

단계 **3** **General(**일반**)** 탭에서 **VTI ID**를 입력합니다. 0~100의 값을 사용할 수 있습니다. 최대 100개의 VTI 인터페이스가 지원됩니다.

참고 수를 마이그레이션하 경우 구성 다른 장치에서 ASA 5506 디바이스에 1 ~ 100의 터널 ID 범위를 사용 합니다. 이를 통해 ASA 5506 디바이스에서 사용 가능한 1~100의 터널 범위의 호환성을 보장할 수 있습니다.

단계 **4** **Interface Name(**인터페이스 이름**)**을 입력합니다.

Enable Interface(인터페이스 활성화) 체크 박스가 선택되어 있는지 확인합니다.

단계 **5** 터널의 소스 **IP Address(IP** 주소**)**와 **Subnet Mask(**서브넷 마스크**)**를 입력합니다.

단계 **6** **Advanced(**고급**)** 탭을 클릭합니다.

모든 필드는 유효한 값을 지니거나 VPN 마법사에서 표시할 터널에 대한 선택 항목을 가져야 합니다.

단계 **7** **Destination IP(**대상 **IP)** 주소를 입력합니다.

단계 **8** **Source Interface(**소스 인터페이스**)**를 선택합니다.

단계 **9** **Tunnel Protection with IPsec Profile(IPsec** 프로필을 통한 터널 보호**)** 필드에서 IPsec 프로필을 선택합니다.

단계 **10** **Ensure the Enable Tunnel Mode IPv4 IPsec(**터널 모드 **IPv4 IPsec** 활성화 확인**)** 체크 박스를 선택합니다.

단계 **11** **OK(**확인**)**를 클릭합니다.

단계 **12** **Interfaces(**인터페이스**)** 패널에서 **Apply(**적용**)**를 클릭합니다.

단계 **13** **Preview CLI Commands(**미리 보기 **CLI** 명령**)** 대화 상자에서 **Send(**전송**)**를 클릭합니다.

업데이트된 구성을 로드한 후에 새 VTI가 인터페이스 목록에 나타납니다. 이 새 VTI는 IPsec 사이트 대 사이트 VPN을 생성할 때 사용할 수 있습니다.

12 장

VPN을 위한 외부 AAA 서버 구성

외부 AAA 서버 정보

ASA에 대해 AAA(인증, 권한 부여, 어카운트 관리)를 지원하기 위해 외부 LDAP, RADIUS 또는 TACACS+ 서버를 사용하도록 이 ASA를 구성할 수 있습니다. 외부 AAA 서버는 구성된 권한 및 특성을 적용합니다. 외부 서버를 사용하도록 ASA를 구성하려면 먼저 올바른 ASA 권한 부여 속성을 사용하여 외부 AAA 서버를 구성해야 하며 이러한 속성의 하위 집합에서 특정한 권한을 개별 사용자에게 할당해야 합니다.

권한 부여 특성의 정책 시행 이해

ASA는 VPN 연결에 사용자 권한 부여 속성(사용자 엔타이틀먼트 또는 권한이라고도 함)을 적용하는 다양한 방법을 지원합니다. 다음 조합을 통해 사용자 속성을 얻을 수 있도록 ASA를 구성할 수 있습니다.

- ASA의 DAP(Dynamic Access Policy)
- 외부 RADIUS 또는 LDAP 인증 및/또는 권한 부여 서버
- ASA의 그룹 정책

ASA에서 모든 소스의 속성을 수신하면 속성이 평가 및 병합되어 사용자 정책에 적용됩니다. 특성 간에 충돌이 있을 경우 DAP 특성이 우선적으로 적용됩니다.

ASA에서는 다음 순서로 속성을 적용합니다.

1. ASA의 DAP 속성 — 8.0(2) 버전에서 도입된 이러한 속성은 다른 모든 속성보다 우선적으로 적용됩니다. DAP에서 책갈피 또는 URL 목록을 설정하면 그룹 정책에서 설정한 책갈피 또는 URL 목록이 해당 설정으로 재정의됩니다.

2. AAA 서버의 사용자 특성 — 사용자 인증 및/또는 권한 부여가 성공적으로 수행되면 서버에서 이러한 특성을 반환합니다. ASA에서 로컬 AAA 데이터베이스의 개별 사용자에 대해 설정되는 속성과 혼동하지 마십시오(ASDM의 사용자 어카운트).
3. ASA에 구성된 그룹 정책 — RADIUS 서버에서 사용자에 대해 RADIUS CLASS 속성 IETF-Class-25(OU=*group-policy*) 값을 반환하면 ASA에서는 해당 사용자를 이름이 같은 그룹 정책에 배치하고 서버에서 반환하지 않은 그룹 정책의 모든 속성을 적용합니다.

   LDAP 서버의 경우 세션에 대한 그룹 정책을 설정하는 데 모든 특성 이름을 사용할 수 있습니다. ASA에서 구성하는 LDAP 속성 맵은 LDAP 속성을 Cisco 속성 IETF-Radius-Class에 매핑합니다.
4. 연결 프로파일을 통해 할당된 그룹 정책(CLI에서는 터널 그룹이라고 함) — 연결 프로파일에는 연결을 위한 예비 설정이 있으며 인증 전에 사용자에게 적용되는 기본 그룹 정책을 포함합니다. ASA에 연결되는 모든 사용자는 처음에 이 그룹에 소속되며, DAP, 서버에서 반환한 사용자 속성 또는 사용자에 할당된 그룹 정책에 없는 모든 속성을 제공합니다.
5. ASA에서 할당한 기본 그룹 정책(DfltGrpPolicy) — 시스템 기본 속성에서는 DAP, 사용자 속성, 그룹 정책 또는 연결 프로필에 없는 모든 값을 제공합니다.

외부 AAA 서버 사용 지침

ASA는 숫자 ID가 아니라 속성 이름을 기반으로 LDAP 속성을 적용합니다. RADIUS 특성은 이름이 아니라 숫자 ID를 통해 적용됩니다.

ASDM 7.0 버전의 경우 LDAP 특성에 cVPN3000 접두사가 포함됩니다. ASDM 7.1 이상 버전의 경우 이 접두사가 제거되었습니다.

LDAP 특성은 Radius 특성의 하위 집합으로, Radius 장에서 설명합니다.

다중 인증서 인증 구성

이제 AnyConnect SSL 및 IKEv2 클라이언트 프로토콜을 사용하여 세션당 여러 인증서를 검증할 수 있습니다. 여러 인증서 인증을 위해 프로토콜 교환을 정의하고 두 가지 세션 유형에 활용하도록 Aggregate Authentication 프로토콜이 확장되었습니다. 예를 들어 머신 인증서의 발급자 이름이 특정한 CA와 일치하는지 확인할 수 있으므로 해당 디바이스는 회사에서 발급한 디바이스인지 확인할 수 있습니다.

다중 인증서 옵션은 인증서를 통해 머신과 사용자 모두의 인증서 인증을 허용합니다. 이 옵션을 사용하지 않으면 하나 또는 다른 대상에 대한 인증서 인증만 수행할 수 있으며 두 가지 모두에 대한 인증서 인증은 수행할 수 없습니다.

사용자 이름 미리 채우기 필드로 인증서의 필드를 구문 분석하거나 AAA 및 인증서로 인증된 연결에서 후속 AAA 인증에 사용할 수 있습니다. 첫 번째 및 두 번째로 미리 채울 사용자 이름은 항상 클라이언트에서 수신한 첫 번째 인증서에서 검색됩니다.

다중 인증서 인증을 사용하면 두 개의 인증서가 인증됩니다. 클라이언트에서 수신된 첫 번째 인증서는 사전 채우기 및 username-from-certificate 기본 및 보조 사용자 이름이 구문 분석된 인증서입니다.

그런 다음 어떤 인증서를 첫 번째로 전송하고 두 번째로 전송할지 선택하기 위해 클라이언트에 대해 규칙을 구성할 수 있습니다.

다중 인증서 인증을 사용하면 연결 시도를 인증하는 데 사용된 인증서의 필드를 기반으로 정책 의사 결정을 내릴 수 있습니다. 다중 인증서 인증 중에 클라이언트에서 수신한 사용자 및 머신 인증서는 인증서 필드를 기반으로 정책을 구성할 수 있도록 DAP에 로드됩니다. DAP(Dynamic Access Policies)를 사용하여 다중 인증서 인증을 추가하여 연결 시도를 허용하거나 허용하지 않도록 규칙을 설정하려면 에서 ASA VPN ASDM 구성 가이드의 적절한 릴리스*DAP*에 여러 인증서 인증 추가를 참고하십시오.

Active Directory/LDAP VPN 원격 액세스 권한 부여의 예

이 섹션에서는 Microsoft Active Directory 서버를 사용하여 ASA에서 인증 및 권한 부여를 구성하는 절차의 예를 보여 줍니다. 여기에는 다음과 같은 항목이 포함됩니다.

- 사용자 기반 특성의 정책 시행, 259 페이지
- 특정 그룹 정책에 LDAP 사용자 배치, 261 페이지
- AnyConnect 터널에 고정 IP 주소 할당 적용, 262 페이지
- 다이얼인 액세스 허용 또는 액세스 거부 적용, 264 페이지
- 로그온 시간 및 시간 규칙 적용, 266 페이지

Cisco.com에서 제공하는 기타 구성 예에는 다음 테크노트(TechNote)가 포함되어 있습니다.

- ASA/PIX: LDAP 구성을 통해 VPN 클라이언트를 VPN 그룹 정책에 매핑하는 예
- PIX/ASA 8.0: LDAP 인증을 사용하여 로그인에서 그룹 정책을 할당하는 예

사용자 기반 특성의 정책 시행

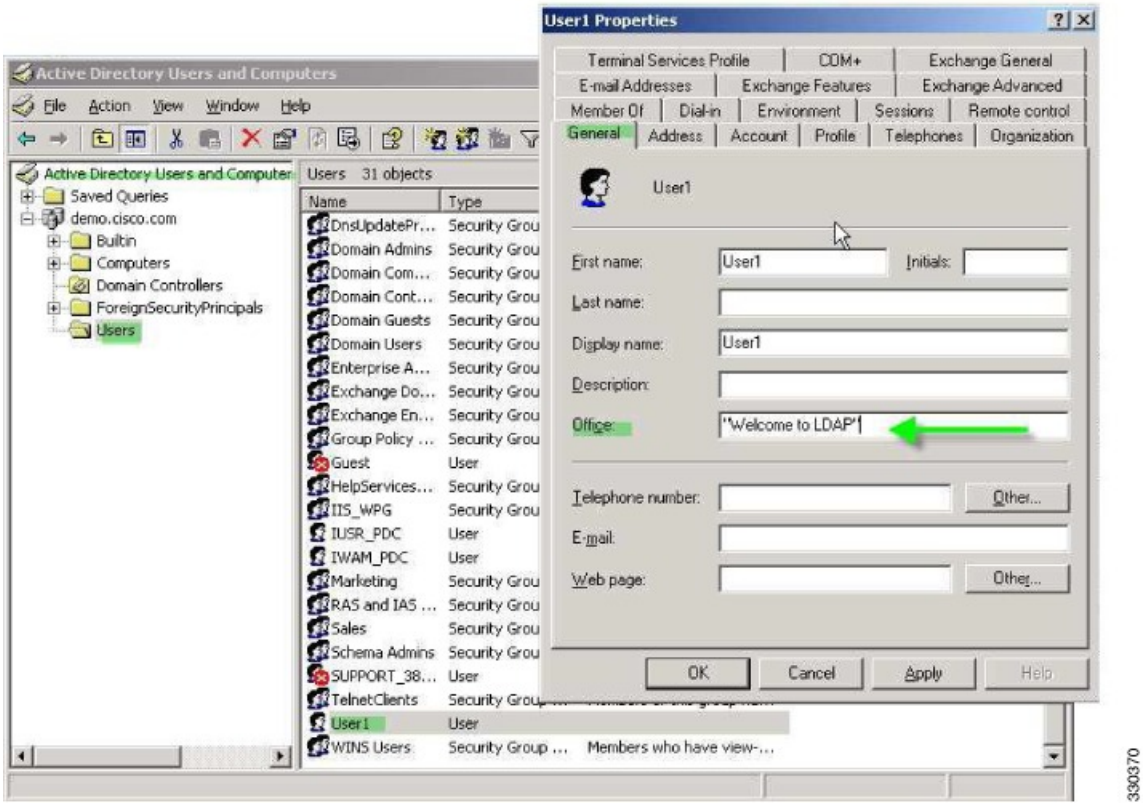
이 예에서는 모든 표준 LDAP 특성을 잘 알려진 VSA(Vendor-Specific Attribute)에 매핑할 수 있으며, 하나 또는 여러 LDAP 특성을 하나 또는 여러 Cisco LDAP 특성에 매핑할 수 있는 방법을 보여주는 간단한 배너를 사용자에게 표시합니다. 이 예는 IPsec VPN 클라이언트, AnyConnect SSL VPN 클라이언트 또는 클라이언트리스 SSL VPN을 포함한 모든 연결 유형에 적용됩니다.

AD LDAP 서버에 구성되어 있는 사용자에게 간단한 배너를 적용하려면 General(일반) 탭의 Office(사무실) 필드를 사용하여 배너 텍스트를 입력합니다. 이 필드는 physicalDeliveryOfficeName이라는 특성을 사용합니다. ASA에서 physicalDeliveryOfficeName을 Cisco 속성 Banner1에 매핑하는 속성 맵을 생성합니다.

인증되는 동안 ASA는 서버에서 physicalDeliveryOfficeName 값을 검색하여 Cisco 속성 Banner1에 매핑하고 사용자에게 배너를 표시합니다.

프로시저

단계 **1** 사용자 이름을 마우스 오른쪽 버튼으로 클릭하고 Properties(속성) 대화 상자를 연 다음 **General(**일반**)** 탭의 Office(사무실) 필드에 배너 텍스트를 입력합니다. Office(사무실) 필드에서는 AD/LDAP 특성인 physicalDeliveryOfficeName을 사용합니다.



단계 **2** ASA에서 LDAP 속성 맵을 생성합니다.

맵 배너를 생성하고 AD/LDAP 특성 physicalDeliveryOfficeName을 Cisco 특성 Banner1에 매핑합니다.

```
hostname(config)# ldap attribute-map Banner
hostname(config-ldap-attribute-map)# map-name physicalDeliveryOfficeName Banner1
```

단계 **3** LDAP 특성 맵을 AAA 서버에 연결합니다.

호스트 10.1.1.2에 대한 aaa 서버 호스트 구성 모드를 AAA 서버 그룹 MS_LDAP에 입력하고 이전에 생성한 특성 맵 배너를 연계합니다.

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map Banner
```

단계 4 배너 실행을 테스트합니다.

특정 그룹 정책에 LDAP 사용자 배치

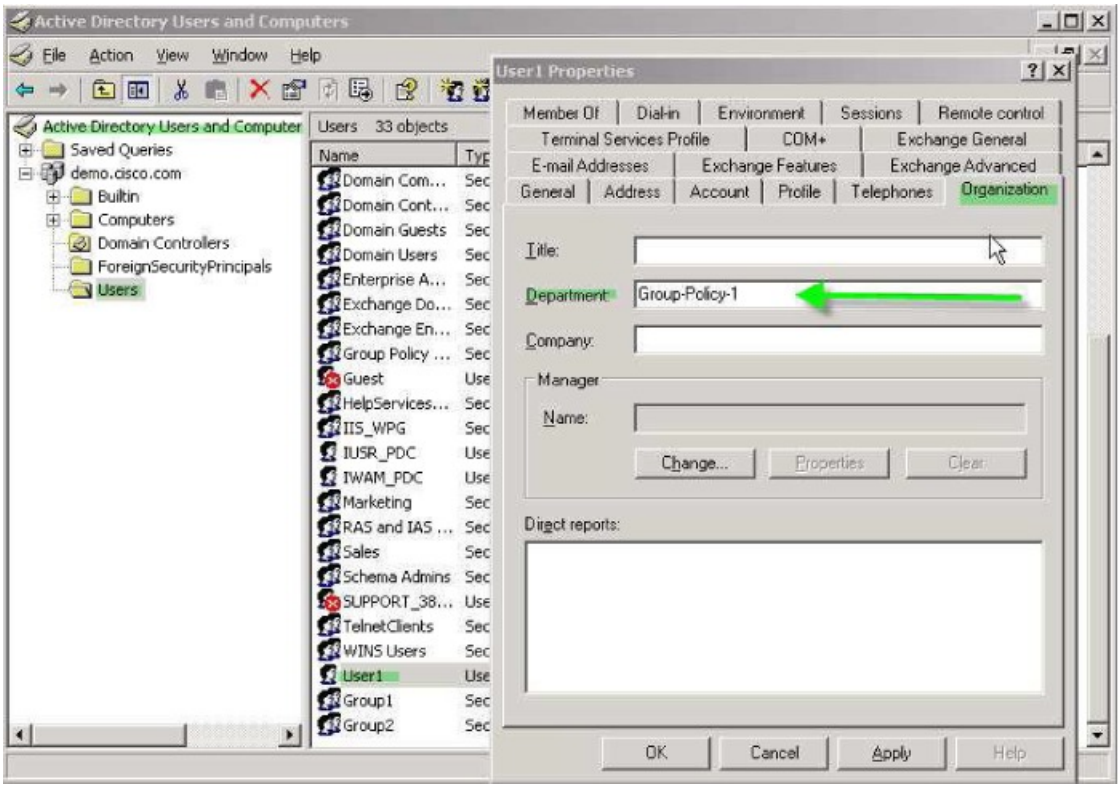
이 예는 IPsec VPN 클라이언트, AnyConnect SSL VPN 클라이언트 또는 클라이언트리스 SSL VPN을 포함한 모든 연결 유형에 적용됩니다. 이 예에서는 클라이언트리스 SSL VPN 연결을 통해 User1을 연결합니다.

특정 그룹 정책에 LDAP 사용자를 배치하려면 Organization(조직) 탭의 Department(부서) 필드를 사용하여 그룹 정책 이름을 입력합니다. 그런 다음 특성 맵을 생성하고, Department를 Cisco 특성 IETF RADIUS CLASS에 매핑합니다.

인증되는 동안 ASA는 서버에서 Department 값을 검색하여 IETF-Radius-Class에 매핑하고 User1을 그룹 정책에 배치합니다.

프로시저

단계 1 사용자 이름을 마우스 오른쪽 버튼으로 클릭하고 Properties(속성) 대화 상자를 연 다음 **Organization(**조직**)** 탭의 Department(부서) 필드에 **Group-Policy-1**을 입력합니다.



단계 2 LDAP 구성에 대한 특성 맵을 정의합니다.

AD 특성 Department를 Cisco 특성 IETF-Radius-Class에 매핑합니다.

```
hostname(config)# ldap attribute-map group_policy
hostname(config-ldap-attribute-map)# map-name Department IETF-Radius-Class
```

단계 **3** LDAP 특성 맵을 AAA 서버에 연결합니다.

호스트 10.1.1.2에 대한 aaa 서버 호스트 구성 모드를 AAA 서버 그룹 MS_LDAP에 입력하고 이전에 생성한 특성 맵 그룹 정책을 연결합니다.

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map group_policy
```

단계 **4** ASA에서 서버의 Department(부서) 필드에 입력한 대로 group-policy, *Group-policy-1*을 추가하고 사용자에게 할당할 필수 정책 특성을 구성합니다.

```
hostname(config)# group-policy Group-policy-1 external server-group LDAP_demo
hostname(config-aaa-server-group)#
```

단계 **5** 사용자가 하는 것처럼 VPN 연결을 설정하고 세션이 Group-Policy1(및 기본 그룹 정책의 적용 가능한 모든 기타 특성)에서 특성을 상속받는지 확인합니다.

단계 **6** 특권 EXEC 모드에서 **debug ldap 255** 명령을 활성화하여 ASA와 서버 간 통신을 모니터링합니다. 다음은 이 명령의 샘플 출력이며, 핵심 메시지가 표시되도록 수정되었습니다.

```
[29] Authentication successful for user1 to 10.1.1.2
[29] Retrieving user attributes from server 10.1.1.2
[29] Retrieved Attributes:
[29] department: value = Group-Policy-1
[29] mapped to IETF-Radius-Class: value = Group-Policy-1
```

AnyConnect 터널에 고정 IP 주소 할당 적용

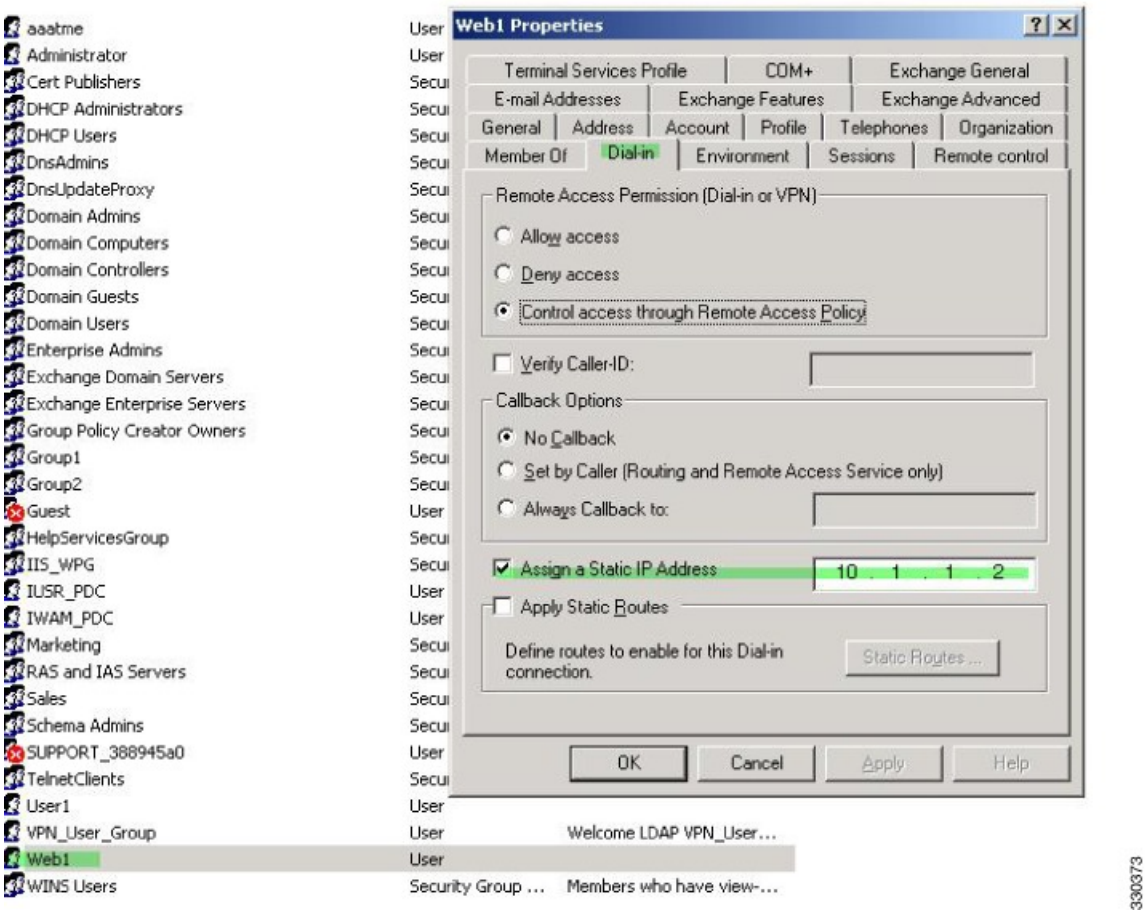
이 예는 IPsec 클라이언트 및 SSL VPN 클라이언트 등 전체 터널 클라이언트에 적용됩니다.

고정 AnyConnect의 고정 IP 할당을 적용하려면 AnyConnect 클라이언트 사용자 Web1이 고정 IP 주소를 수신하도록 구성하고 이 주소를 AD LDAP 서버에 있는 Dialin(다이얼인) 탭의 Assign Static IP Address(고정 IP 주소 할당) 필드에 입력합니다. 이 필드는 msRADIUSFramedIPAddress 특성을 사용합니다. 이 특성을 Cisco 특성인 IETF-Radius-Framed-IP-Address에 매핑하는 특성 맵을 생성합니다.

인증되는 동안 ASA는 서버에서 msRADIUSFramedIPAddress 값을 검색하여 Cisco 속성 IETF-Radius-Framed-IP-Address에 매핑하고 User1에게 고정 주소를 제공합니다.

프로시저

단계 **1** 사용자 이름을 마우스 오른쪽 버튼으로 클릭하고 Properties(속성) 대화 상자를 연 다음 **Dial-in(**다이얼인**)** 탭에서 **Assign Static IP Address(**고정 **IP** 주소 할당**)** 확인란을 선택하고 IP 주소 10.1.1.2를 입력합니다.



단계 **2** 표시된 LDAP 구성에 대한 특성 맵을 생성합니다.

다음과 같이 Static Address(고정 주소) 필드에서 사용하는 AD 특성 msRADIUSFramedIPAddress를 Cisco 특성 IETF-Radius-Framed-IP-Address에 매핑합니다.

```
hostname(config)# ldap attribute-map static_address
hostname(config-ldap-attribute-map)# map-name msRADIUSFramedIPAddress
IETF-Radius-Framed-IP-Address
```

단계 **3** LDAP 특성 맵을 AAA 서버에 연결합니다.

호스트 10.1.1.2에 대한 aaa 서버 호스트 구성 모드를 AAA 서버 그룹 MS_LDAP에 입력하고 이전에 생성한 특성 맵 static_address를 연계합니다.

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map static_address
```

단계 **4** 구성의 이 부분을 확인하여, AAA를 지정하도록 **vpn-address-assignment** 명령이 구성되었는지 확인합니다.

```
hostname(config)# show run all vpn-addr-assign
vpn-addr-assign aaa   << Make sure this is configured >>
no vpn-addr-assign dhcp
vpn-addr-assign local
hostname(config)#
```

단계 **5** AnyConnect 클라이언트를 사용하여 ASA와의 연결을 설정합니다. 사용자가 서버에 구성되어 ASA에 매핑된 IP 주소를 수신하는지 확인합니다.

단계 **6** **show vpn-sessiondb svc** 명령을 사용하여 세션 세부 사항을 보고 주소가 할당되었는지 확인합니다.

```
hostname# show vpn-sessiondb svc

Session Type: SVC
Username     : web1                   Index        : 31
Assigned IP  : 10.1.1.2              Public IP    : 10.86.181.70
Protocol     : Clientless SSL-Tunnel DTLS-Tunnel
Encryption   : RC4 AES128             Hashing      : SHA1
Bytes Tx     : 304140                 Bytes Rx     : 470506
Group Policy : VPN_User_Group         Tunnel Group : Group1_TunnelGroup
Login Time   : 11:13:05 UTC Tue Aug 28 2007
Duration     : 0h:01m:48s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none
```

다이얼인 액세스 허용 또는 액세스 거부 적용

이 예에서는 사용자가 허용한 터널링 프로토콜을 지정하는 LDAP 특성 맵을 생성합니다. Dialin(다이얼인) 탭의 Allow access(액세스 허용) 및 Deny access(액세스 거부) 설정을 Cisco 특성 Tunneling-Protocol에 매핑합니다. 이 특성은 다음 비트맵 값을 지원합니다.

값	터널링 프로토콜
1	PPTP
2	L2TP
4	IPsec(IKEv1)
8	L2TP/IPsec
16	클라이언트리스 SSL
32	SSL 클라이언트 — AnyConnect 또는 SSL VPN 클라이언트

값	터널링 프로토콜
64	IPsec(IKEv2)

[1] (1) IPsec 및 L2TP over IPsec은 동시에 지원되지 않습니다. 따라서 값 4와 8은 동시에 사용할 수 없습니다.
[2] (2) 참고 1을 참고하십시오.

이 특성을 사용하여 프로토콜에 대해 액세스 허용(TRUE) 또는 액세스 거부(FALSE) 조건을 생성하고 사용자 액세스가 허용되는 방법을 적용합니다.

다이얼인 액세스 허용 또는 액세스 거부의 또 다른 예는 테크노트 ASA/PIX: LDAP 구성을 통해 VPN 클라이언트를 VPN 그룹 정책에 매핑 예를 참조해 주십시오.

프로시저

단계 **1** 사용자 이름을 마우스 오른쪽 버튼으로 클릭하고 Properties(속성) 대화 상자를 연 다음 **Dial-in(**다이얼인**)** 탭에서 Allow Access(액세스 허용) 라디오 버튼을 클릭합니다.

참고 Control access through the Remote Access Policy(원격 액세스 정책을 통해 액세스 제어) 옵션을 선택할 경우 서버에서 값이 반환되지 않으며, 적용되는 권한은 ASA의 내부 그룹 정책 설정을 기반으로 합니다.

단계 **2** IPsec과 AnyConnect 연결을 모두 허용하는 특성 맵을 생성하십시오. 단, 클라이언트리스 SSL 연결은 거부해야 합니다.

a) 맵 tunneling_protocols를 생성합니다.

```
hostname(config)# ldap attribute-map tunneling_protocols
```

b) Allow Access(액세스 허용) 설정에서 사용하는 AD 특성 msNPAllowDialin을 Cisco 특성 Tunneling-Protocols에 매핑합니다.

```
hostname(config-ldap-attribute-map)# map-name msNPAllowDialin Tunneling-Protocols
```

c) 맵 값을 추가합니다.

```
hostname(config-ldap-attribute-map)# map-value msNPAllowDialin FALSE 48
hostname(config-ldap-attribute-map)# map-value msNPAllowDialin TRUE 4
```

단계 **3** LDAP 특성 맵을 AAA 서버에 연결합니다.

a) 호스트 10.1.1.2에 대한 aaa 서버 호스트 구성 모드를 AAA 서버 그룹 MS_LDAP에 입력합니다.

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
```

b) 사용자가 생성한 특성 맵 tunneling_protocols를 연계합니다.

```
hostname(config-aaa-server-host)# ldap-attribute-map tunneling_protocols
```

단계 **4** 특성 맵이 구성된 대로 작동하는지 확인합니다.

클라이언트리스 SSL을 사용하여 연결을 시도합니다. 사용자에게는 무단 연결 메커니즘 때문에 연결에 실패했다는 알림이 제공됩니다. IPsec은 특성 맵에 따라 허용되는 터널링 프로토콜이므로 IPsec 클라이언트가 연결됩니다.

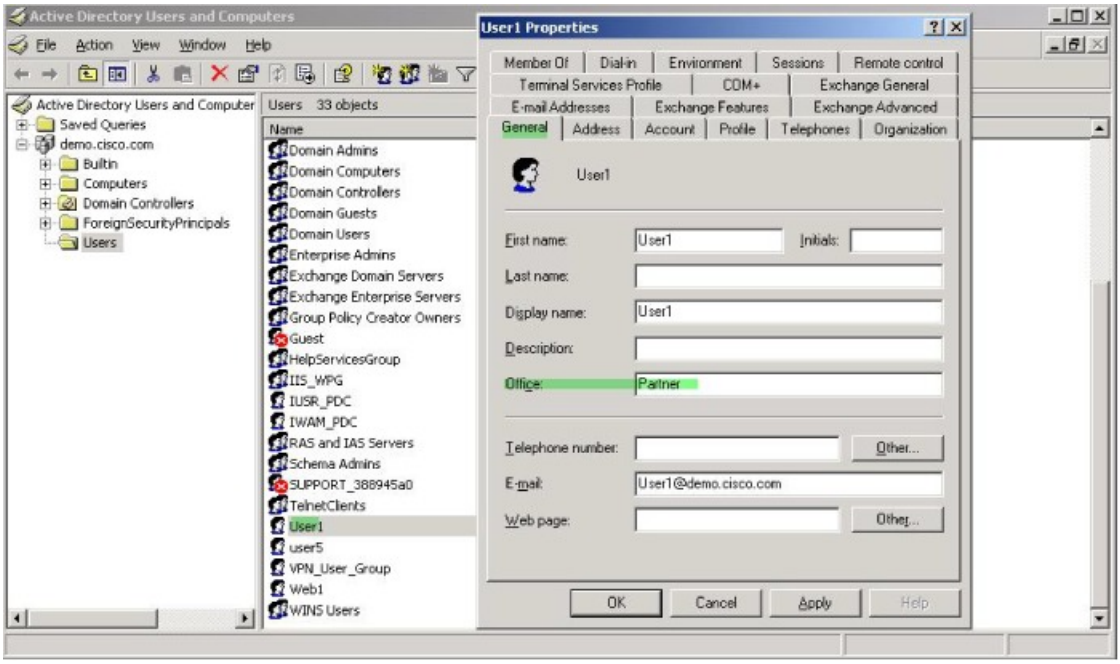
로그온 시간 및 시간 규칙 적용

다음 예에서는 비즈니스 파트너 같은 클라이언트리스 SSL 사용자가 네트워크에 액세스할 수 있도록 시간을 구성하고 적용하는 방법을 보여 줍니다.

AD 서버에서 Office(사무실) 필드를 사용하여 파트너 이름을 입력합니다. 이 필드에서는 physicalDeliveryOfficeName 특성을 사용합니다. 그런 다음 ASA에서 속성 맵을 생성하여 해당 속성을 Cisco 속성 Access-Hours에 매핑합니다. 인증되는 동안 ASA는 physicalDeliveryOfficeName 값을 검색하여 Access-Hours에 매핑합니다.

프로시저

단계 **1** 사용자를 선택하고 **Properties(**속성**)**를 마우스 오른쪽 버튼으로 클릭하고 **General(**일반**)** 탭을 엽니다.



단계 **2** 특성 맵을 생성합니다.

특성 맵 access_hours를 생성하여 Office 필드에서 사용하는 AD 특성 physicalDeliveryOfficeName을 Cisco 특성 Access-Hours에 매핑합니다.

```
hostname(config)# ldap attribute-map access_hours
hostname(config-ldap-attribute-map)# map-name physicalDeliveryOfficeName Access-Hours
```

단계 **3** LDAP 특성 맵을 AAA 서버에 연결합니다.

호스트 10.1.1.2에 대한 aaa 서버 호스트 구성 모드를 AAA 서버 그룹 MS_LDAP에 입력하고 생성한 특성 맵 access_hours를 연계합니다.

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map access_hours
```

단계 **4** 서버에서 허용되는 각 값의 시간 범위를 구성합니다.

파트너 액세스 시간을 월~금요일 오전 9시부터 오후 5시로 구성합니다.

```
hostname(config)# time-range Partner
hostname(config-time-range)# periodic weekdays 09:00 to 17:00
```

II 부

클라이언트리스 SSL VPN

13 장

클라이언트리스 SSL VPN 개요

클라이언트리스 SSL VPN 소개

클라이언트리스 SSL VPN을 통해 엔드 유저는 SSL 지원 웹 브라우저를 사용하여 어디에서나 기업 네트워크에 있는 리소스에 안전하게 액세스할 수 있습니다. 사용자는 먼저 클라이언트리스 SSL VPN 게이트웨이를 통해 인증된 다음 미리 구성된 네트워크 리소스에 액세스합니다.

참고 클라이언트리스 SSL VPN이 활성화된 경우 보안 상황(방화벽 다중 모드라고도 함) 및 활성/활성 상태 저장 장애 조치는 지원되지 않습니다.

클라이언트리스 SSL VPN은 소프트웨어 또는 하드웨어 클라이언트 없이 웹 브라우저를 사용하여 ASA에 대한 보안 원격 액세스 VPN 터널을 만듭니다. 또한 HTTP를 통해 인터넷에 연결할 수 있는 거의 모든 디바이스의 광범위한 웹 리소스, 웹 지원 애플리케이션 및 레거시 애플리케이션 모두에 안전하고 쉽게 액세스할 수 있도록 지원합니다. 그 기능은 다음과 같습니다.

- 내부 웹 사이트
- 웹 지원 애플리케이션
- NT/Active Directory 파일 공유
- Microsoft Outlook Web Access Exchange Server 2000, 2003, 2007 및 2013
- Exchange Server 2010, 8.4(2) 이상에 대한 Microsoft Web App
- Application Access(다른 TCP 기반 애플리케이션에 대한 스마트 터널 또는 포트 전달 액세스)

클라이언트리스 SSL VPN에서는 SSL/TLS1(Secure Sockets Layer 프로토콜과 그 후속 프로토콜 및 전송 계층 보안)을 사용하여 원격 사용자와 내부 서버로 구성한 지원되는 특정 내부 리소스 간의 보안

연결을 제공합니다. ASA는 프록시해야 할 연결을 인식하고 HTTP 서버는 사용자를 인증하기 위해 인증 하위 시스템과 상호 작용합니다.

네트워크 관리자는 그룹을 기준으로 하여 클라이언트리스 SSL VPN 세션 사용자별로 리소스에 대한 액세스를 제공합니다. 사용자는 내부 네트워크의 리소스에 직접 액세스할 수 없습니다.

클라이언트리스 SSL VPN에 대한 사전 요구 사항

ASA의 클라이언트리스 SSL VPN에서 지원되는 브라우저 및 플랫폼은 지원되는 VPN 플랫폼, Cisco ASA 5500 Series 섹션을 참고하십시오.

클라이언트리스 SSL VPN에 대한 지침 및 제한 사항

- ActiveX 페이지에서 ActiveX Relay를 활성화하거나 연계된 그룹 정책에 **activex-relay**를 입력해야 합니다. 이 명령을 입력하거나 스마트 터널 목록을 정책에 할당하고 엔드포인트에 있는 브라우저 프록시 예외 목록에서 프록시를 지정하는 경우, 사용자는 “shutdown.webvpn.relay.” 항목을 해당 목록에 추가해야 합니다.
- ASA는 Windows 7, Vista, Internet Explorer 8~10, Mac OS X 또는 Linux에서의 Windows 공유(CIFS) 웹 폴더에 대해 클라이언트리스 액세스를 지원하지 않습니다.
- DoD 공통 액세스 카드 및 스마트 카드를 포함하는 인증서 인증은 Safari 키체인에서만 작동합니다.
- 클라이언트리스 연결에 대해 신뢰할 수 있는 인증서를 설치한 경우에도 클라이언트는 신뢰할 수 없는 인증서 경고를 볼 수 있습니다.
- ASA는 클라이언트리스 SSL VPN 연결에 대해 DSA 또는 RSA 인증서를 지원하지 않습니다. RSA 인증서는 지원됩니다.
- 일부 도메인 기반 보안 제품에는 ASA에서 시작되는 이러한 요청 이외의 요구 사항이 있습니다.
- Modular Policy Framework의 구성 제어 검사 및 기타 검사 기능은 지원되지 않습니다.
- NAT와 PAT는 클라이언트에 적용되지 않습니다.
- 클라이언트리스 SSL VPN의 일부 구성 요소에는 JRE(Java Runtime Environment)가 필요합니다. Mac OS X v10.7 이상에서는 Java가 기본적으로 설치되지 않습니다. Mac OS X에 Java를 설치하는 방법에 대한 자세한 내용은 http://java.com/en/download/faq/java_mac.xml을 참고하십시오.
- 클라이언트리스 VPN 세션이 시작되면 RADIUS 어카운팅 시작 메시징이 생성됩니다. 주소가 클라이언트리스 VPN 세션에 할당되지 않으므로 시작 메시지에는 Framed IP 주소가 포함되지 않습니다. Layer3 VPN 연결이 이후에 클라이언트리스 포털 페이지에서 시작된 경우 주소가 할당되고 중간 업데이트 어카운팅 메시지로 RADIUS 서버에 보고됩니다. weblaunch 기능을 사용하여 Layer3 VPN 터널을 설정할 때 유사한 RADIUS 동작을 예측할 수 있습니다. 이 경우 어카운팅 시작 메시지는 사용자가 인증된 후, 그리고 Layer3 터널이 설정되기 전에 Framed IP 주소 없이 전송됩니다. 이 시작 메시지 뒤에는 Layer3 터널이 설정된 후에 중간 업데이트 메시지가 이어집니다.

클라이언트리스 포털에 대해 여러 그룹 정책을 구성한 경우 로그온 페이지의 드롭다운 목록에 표시됩니다. 목록에 있는 첫 번째 그룹 정책에 인증서가 필요한 경우 사용자에게 일치하는 인증서가 있어야 합니다. 일부 그룹 정책에서 인증서를 사용하지 않는 경우, 인증서 없는 정책을 먼저 표시하도록 목록을 구성해야 합니다. 또는 이름이 "0-Select-a-group."인 더미 그룹 정책을 생성할 수도 있습니다.

팁 알파벳순으로 또는 이름 앞에 숫자를 붙여 그룹 정책의 이름을 지정하여 먼저 표시할 정책을 제어할 수 있습니다(예: 1-AAA, 2-Certificate).

클라이언트리스 SSL VPN에 대한 라이센싱

AnyConnect Secure Mobility Client를 사용하려면 AnyConnect Plus 및 Apex 라이선스를 구매해야 합니다. 필요한 라이선스는 사용하려는 AnyConnect VPN 클라이언트와 Secure Mobility 기능 및 지원하려는 세션 수에 따라 다릅니다. 이러한 사용자 기반 라이선스에는 일반적인 BYOD 트렌드에 맞추기 위한 지원 및 소프트웨어 업데이트 액세스 권한이 포함되어 있습니다.

AnyConnect 4.4 라이선스는 ASA(또한 ISR, CSR, ASR)뿐만 아니라 ISE(Identity Services Engine), CWS(Cloud Web Security) 및 WSA(Web Security Appliance)와 같은 다른 비 VPN 헤드엔드에서 사용됩니다. 헤드엔드와 관계없이 일관된 모델이 사용되므로 헤드엔드 마이그레이션이 발생하더라도 아무런 영향을 미치지 않습니다.

AnyConnect용 라이선싱 모델에 대한 전체 설명은 http://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdf 섹션을 참고하십시오.

14 장

기본 클라이언트리스 SSL VPN 구성

각 URL 재작성

기본적으로 ASA는 모든 웹 리소스(예: HTTPS, CIFS, RDP 및 플러그인)에 대한 모든 포털 트래픽을 허용합니다. 클라이언트리스 SSL VPN은 ASA에만 유효한 리소스에 각 URL을 재작성합니다. 사용자는 이 URL을 사용하여 요청한 웹사이트에 연결되어 있는지 확인할 수 없습니다. 사용자가 피싱 웹사이트에 연결되는 위험한 상황에 처하지 않도록 클라이언트리스 액세스에 대해 구성된 정책(그룹 정책, 동적 액세스 정책 또는 두 가지 모두)에 웹 ACL을 할당하여 포털의 트래픽 흐름을 제어해야 합니다. 액세스 가능한 URL에 대한 사용자의 혼란을 방지하기 위해 이러한 정책에서 URL 입력을 해제할 것을 권장합니다.

그림 ***6:*** 사용자가 입력하는 ***URL*** 예

그림 *7:* 보안 어플라이언스가 재작성하고 브라우저 창에 표시되는 동일한 ***URL***

프로시저

단계 **1** 클라이언트리스 SSL VPN 액세스를 필요로 하는 모든 사용자에 대해 그룹 정책을 구성하고 해당 그룹 정책에 대해서만 클라이언트리스 SSL VPN을 활성화합니다.

단계 **2** 열려 있는 그룹 정책에서 **General(**일반**)** > **More Options(**추가 옵션**)** > **Web ACL(**웹 **ACL)**을 선택하고 **Manage(**관리**)**를 클릭합니다.

단계 **3** 다음 중 하나를 수행하는 웹 ACL을 생성합니다.

- 사설 네트워크에 있는 특정 대상에 대해서만 액세스를 허용합니다.
- 사설 네트워크에 대해서만 액세스를 허용하거나, 인터넷 액세스를 거부하거나, 신뢰할 수 있는 사이트에 대해서만 액세스를 허용합니다.

단계 **4** 클라이언트리스 SSL VPN 액세스를 위해 구성된 모든 정책(그룹 정책, 동적 액세스 정책 또는 두 가지 모두)에 웹 ACL을 할당합니다. DAP에 웹 ACL을 할당하려면 DAP 레코드를 수정하고 **Network ACL Filters(**네트워크 **ACL** 필터**)** 탭에서 웹 ACL을 선택합니다.

단계 **5** 브라우저 기반 연결을 설정하면 열리는 포털 페이지에서 URL 입력을 해제합니다. 그룹 정책 포털 프레임 및 DAP **Functions(**기능**)** 탭의 URL 입력 옆에 있는 **Disable(**비활성화**)**을 클릭합니다. DAP에 있는 URL 입력을 해제하려면 ASDM을 사용하여 DAP 레코드를 수정하고 **Functions(**기능**)** 탭을 클릭한 다음 URL 입력 옆에 있는 **Disable(**비활성화**)**을 선택합니다.

단계 **6** 사용자에게 포털 페이지 위에 있는 네이티브 브라우저 주소 필드에 외부 URL을 입력하거나 별도의 브라우저 창을 열어 외부 사이트를 방문하도록 안내합니다.

클라이언트리스 SSL VPN 액세스 구성

클라이언트리스 SSL VPN 액세스를 구성할 때, 다음을 수행할 수 있습니다.

- 클라이언트리스 SSL VPN 세션에 대해 ASA 인터페이스를 활성화하거나 해제합니다.
- 클라이언트리스 SSL VPN 연결에 대해 포트를 선택합니다.
- 동시 클라이언트리스 SSL VPN 세션의 최대 수를 설정합니다.

프로시저

단계 **1** 클라이언트리스 액세스에 대해 그룹 정책을 구성하거나 생성하려면 **Configuration(**구성**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **Clientless SSL VPN Access(**클라이언트리스 **SSL VPN** 액세스**)** > **Group Policies(**그룹 정책**)** 창을 선택합니다.

단계 **2** **Configuration(**구성**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **Clientless SSL VPN Access(**클라이언트리스 **SSL VPN** 액세스**)** > **Connection Profiles(**연결 프로필**)**로 이동합니다.

a) 각 ASA 인터페이스에 대해 **Allow Access(**액세스 허용**)**를 활성화하거나 해제합니다.

인터페이스 열에는 구성된 인터페이스가 나열됩니다. WebVPN 활성화 필드에는 인터페이스에 있는 클라이언트리스 SSL VPN의 상태가 표시됩니다. Yes(예) 옆에 있는 녹색 확인 표시는 클라이언트리스 SSL VPN이 활성화되었음을 나타냅니다. No(아니요) 옆에 있는 빨간색 원은 클라이언트리스 SSL VPN이 해제되어 있음을 나타냅니다.

b) **Port Setting(**포트 설정**)**을 클릭하고 클라이언트리스 SSL VPN 세션에 사용할 포트 번호(1~65,535)를 입력합니다. 기본값은 443입니다. 포트 번호를 변경하면 모든 현재 클라이언트리스 SSL VPN 연결이 종료되므로 현재 사용자가 재연결해야 합니다. 또한 ASDM 세션을 재연결하도록 확인 상자가 표시됩니다.

단계 **3** **Configuration(**구성**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **Advanced(**고급**)** > **Maximum VPN Sessions(**최대 **VPN** 세션 수**)**로 이동하고 Maximum Other VPN Sessions(최대 기타 VPN 세션 수) 필드에서 허용할 클라이언트리스 SSL VPN 세션의 최대 수를 입력합니다.

신뢰할 수 있는 인증서 풀

ASA는 신뢰할 수 있는 인증서를 트러스트 풀로 그룹화합니다. 트러스트 풀은 알려진 여러 CA 인증서를 나타내는 트러스트 포인트의 특별한 사례로 생각할 수 있습니다. ASA에는 웹 브라우저와 함께 제공되는 인증서 번들과 유사한 인증서의 기본 번들이 포함되어 있습니다. 관리자가을 실행하여 활성화할 때까지 이 기본 번들은 비활성 상태로 있습니다.

웹 브라우저에서 HTTPS 프로토콜을 사용하여 원격 서버에 연결하는 경우, 서버는 자체 식별을 위해 CA에서 서명한 디지털 인증서를 제공합니다. 웹 브라우저에는 서버 인증서의 유효성을 확인하는 데 사용되는 CA 인증서의 컬렉션이 포함되어 있습니다.

클라이언트리스 SSL VPN을 통해 원격 SSL 사용 서버에 연결할 경우, 원격 서버를 신뢰할 수 있는지, 올바른 원격 서버에 연결 중인지를 아는 것이 중요합니다. ASA 9.0은 클라이언트리스 SSL VPN에 대해 신뢰할 수 있는 CA(Certificate Authority: 인증 기관) 인증서 목록을 대상으로 SSL 서버 인증서 확인을 지원하기 시작했습니다.

Configuration(구성**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **Certificate Management(**인증서 관리**)** > **Trusted Certificate Pool(**신뢰할 수 있는 인증서 풀**)**에서 https 사이트에 대한 SSL 연결을 위해 인증서 확인을 활성화할 수 있습니다. 신뢰할 수 있는 인증서 풀의 인증서를 관리할 수도 있습니다.

참고 ASA 트러스트 풀은 Cisco IOS 트러스트 풀과 유사하지만 동일하지는 않습니다.

HTTP 서버 확인 활성화

프로시저

단계 1 ASDM에서 **Configuration(**구성**) > Remote Access VPN(**원격 액세스 **VPN) > Certificate Management(**인증서 관리**) > Trusted Certificate Pool(**신뢰할 수 있는 인증서 풀**)**을 선택합니다.

단계 2 **Enable SSL Certificate Check(SSL** 인증서 확인 활성화**)** 확인란을 선택합니다.

단계 3 서버를 확인할 수 없는 경우 연결을 끊으려면 **Disconnect User From HTTPS Site(HTTPS** 사이트에서 사용자 연결 해제**)**를 클릭합니다. 또는 확인에 실패해도 연결을 계속하도록 허용하려면 **Allow User to Proceed to HTTPS Site**를 클릭합니다.

단계 4 **Apply(**적용**)**를 클릭하여 변경 내용을 저장합니다.

인증서 번들 가져오기

여러 위치에서 다음 형식 중 하나로 된 개별 인증서 또는 인증서 번들을 가져올 수 있습니다.

- pkcs7 구조로 래핑된 DER 형식의 x509 인증서
- PEM 형식(PEM 헤더 포함)의 연결된 x509 인증서 파일

프로시저

단계 1 ASDM에서 **Configuration(**구성**) > Remote Access VPN(**원격 액세스 **VPN) > Certificate Management(**인증서 관리**) > Trusted Certificate Pool(**신뢰할 수 있는 인증서 풀**)**을 선택합니다.

단계 2 **Import Bundle(**번들 가져오기**)**을 클릭합니다.

단계 3 번들의 위치를 선택합니다.

- 번들이 컴퓨터에 저장되어 있는 경우 **Import From a File(**파일에서 가져오기**)**을 클릭한 다음 **Browse Local Files(**로컬 파일 찾아보기**)**를 클릭하고 번들을 선택합니다.
- 번들이 ASA 플래시 파일 시스템에 저장되어 있는 경우 **Import From Flash(**플래시에서 가져오기**)**를 클릭한 다음 **Browse Flash(**플래시 찾아보기**)**를 클릭하고 파일을 선택합니다.
- 번들이 서버에서 호스팅되는 경우 **Import From a URL(URL**에서 가져오기**)**을 클릭하고 목록에서 프로토콜을 선택한 다음 필드에 URL을 입력합니다.

- 서명 검증에 실패하거나 번들을 가져올 수 없는 경우, 번들 가져오기를 계속 수행하고 개별 인증서 오류를 나중에 수정합니다. 이 확인란을 선택 취소할 경우, 인증서가 하나라도 실패하면 전체 번들이 실패합니다.

단계 **4** **Import Bundle(**번들 가져오기**)**을 클릭합니다. 또는 변경을 취소하려면 Cancel(취소)을 클릭합니다.

참고 **Remove All Downloaded Trusted CA Certificates Prior to Import(**가져오기 전에 다운로드한 신뢰할 수 있는 **CA** 인증서 모두 제거**)** 확인란을 선택하여 새 번들을 가져오기 전에 신뢰 풀을 지울 수 있습니다.

신뢰 풀 내보내기

신뢰 풀을 정확하게 구성한 경우, 이 풀을 내보내야 합니다. 그러면 내보내기 후 신뢰 풀에 추가된 인증서를 제거하려는 경우 등에 신뢰 풀을 이 지점으로 복원할 수 있습니다. ASA 플래시 파일 시스템 또는 로컬 파일 시스템에 이 풀을 내보낼 수 있습니다.

ASDM에서 Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > Certificate Management(인증서 관리) > Trusted Certificate Pool(신뢰할 수 있는 인증서 풀)을 선택하고 Export Pool(풀 내보내기)을 클릭합니다.

프로시저

단계 **1** **Export to a File(**파일로 내보내기**)**을 클릭합니다.

단계 **2** **Browse Local Files(**로컬 파일 찾아보기**)**를 클릭합니다.

단계 **3** 신뢰 풀을 저장할 폴더를 선택합니다.

단계 **4** File Name(파일 이름) 상자에 신뢰 풀의 고유한 이름을 입력합니다.

단계 **5** 선택을 클릭합니다.

단계 **6** **Export Pool(**풀 내보내기**)**을 클릭하여 파일을 저장합니다. 또는 저장을 중지하려면 **Cancel(**취소**)**을 클릭합니다.

인증서 제거

모든 인증서를 제거하려면 ASDM에서 **Configuration(**구성**) > Remote Access VPN(**원격 액세스 **VPN) > Certificate Management(**인증서 관리**) > Trusted Certificate Pool(**신뢰할 수 있는 인증서 풀**)**을 선택한 다음 **Clear Pool(**풀 지우기**)**을 클릭합니다.

참고 신뢰 풀을 지우기 전에 현재 설정을 복원할 수 있도록 현재 신뢰 풀을 내보내야 합니다.

신뢰할 수 있는 기본 인증 기관 목록 복원

신뢰할 수 있는 기본 CA(Certificate Authority) 목록을 복원하려면 ASDM에서 **Configuration**(구성) > **Remote Access VPN**(원격 액세스 **VPN**) > **Certificate Management**(인증서 관리) > **Trusted Certificate Pool**(신뢰할 수 있는 인증서 풀)을 선택한 다음 **Restore Default Trusted CA List**(신뢰할 수 있는 기본 **CA** 목록 복원)를 클릭하고 **Import Bundle**(번들 가져오기)을 클릭합니다.

신뢰할 수 있는 인증서 풀의 정책 수정

프로시저

단계 **1** 해지 확인 — 풀에 있는 인증서의 해지를 확인할지 여부를 구성한 다음 CLR 또는 OCSP를 사용할지, 해지 확인에 실패할 경우 인증서를 유효하지 않다고 설정할지 여부를 구성합니다.

단계 **2** 인증서 일치 규칙 — 해지 또는 만료 확인에서 면제할 인증서 맵을 선택합니다. 인증서 맵은 인증서를 AnyConnect 또는 클라이언트리스 SSL 연결 프로필(터널 그룹이라고도 함)에 연결합니다.

인증서 맵에 대한 자세한 내용은 Certificate to Connection Profile Maps(인증서-연결 프로파일 맵), Rules(규칙), 141 페이지 섹션을 참고하십시오.

단계 **3** CRL 옵션 — 1~1440분(1140분은 24시간) 범위에서 CRL 캐시를 새로 고치는 빈도를 결정합니다.

단계 **4** 자동 가져오기 — Cisco는 신뢰할 수 있는 CA의 "기본" 목록을 정기적으로 업데이트합니다. Enable Automatic Import(자동 가져오기 활성화)를 선택하고 기본 설정을 유지하는 경우, ASA는 24시간마다 Cisco 사이트에서 신뢰할 수 있는 CA의 업데이트된 목록을 확인합니다. 목록이 변경된 경우, ASA는 새로운 신뢰할 수 있는 기본 CA 목록을 다운로드하고 가져옵니다.

신뢰 풀 업데이트

다음 조건 중 한 가지에 해당하는 경우 신뢰 풀을 업데이트해야 합니다.

- 신뢰 풀에 만료될 예정이거나 재발급된 인증서가 있는 경우
- 게시된 CA 인증서 번들에 특정 애플리케이션에서 필요로 하는 추가 인증서가 포함된 경우

전체 업데이트 시 신뢰 풀에 있는 모든 인증서가 교체됩니다.

실속 업데이트 시 새 인증서를 추가하거나 기존 인증서를 교체할 수 있습니다.

인증서 번들 제거

신뢰 풀을 지우면 기본 번들에 포함되지 않은 모든 인증서가 제거됩니다.

기본 번들은 제거할 수 없습니다. 신뢰 풀을 지우려면 ASDM에서 **Configuration**(구성) > **Remote Access VPN**(원격 액세스 **VPN**) > **Certificate Management**(인증서 관리) > **Trusted Certificate Pool**(신뢰할 수 있는 인증서 풀)을 선택한 다음 **Clear Pool**(풀 지우기)을 클릭합니다.

신뢰할 수 있는 인증서 풀의 정책 수정

프로시저

단계 **1** 해지 확인 — 풀에 있는 인증서의 해지를 확인할지 여부를 구성한 다음 CLR 또는 OCSP를 사용할지, 해지 확인에 실패할 경우 인증서를 유효하지 않다고 설정할지 여부를 구성합니다.

단계 **2** 인증서 일치 규칙 — 해지 또는 만료 확인에서 면제할 인증서 맵을 선택합니다. 인증서 맵은 인증서를 AnyConnect 또는 클라이언트리스 SSL 연결 프로필(터널 그룹이라고도 함)에 연결합니다.

인증서 맵에 대한 자세한 내용은 Certificate to Connection Profile Maps(인증서-연결 프로파일 맵), Rules(규칙), 141 페이지 섹션을 참고하십시오.

단계 **3** CRL 옵션 — 1~1440분(1140분은 24시간) 범위에서 CRL 캐시를 새로 고치는 빈도를 결정합니다.

단계 **4** 자동 가져오기 — Cisco는 신뢰할 수 있는 CA의 "기본" 목록을 정기적으로 업데이트합니다. Enable Automatic Import(자동 가져오기 활성화)를 선택하고 기본 설정을 유지하는 경우, ASA는 24시간마다 Cisco 사이트에서 신뢰할 수 있는 CA의 업데이트된 목록을 확인합니다. 목록이 변경된 경우, ASA는 새로운 신뢰할 수 있는 기본 CA 목록을 다운로드하고 가져옵니다.

Java 코드 서명자

코드 서명은 실행 가능한 코드에 디지털 서명을 추가합니다. 이 디지털 서명은 서명자를 인증하고 서명한 이후에 코드가 수정되지 않았는지 확인하는 데 필요한 정보를 제공합니다.

코드 서명 인증서는 해당 개인 키가 디지털 서명 생성에 사용되는 특수한 인증서입니다. 코드 서명에 사용되는 인증서는 CA에서 가져온 것으로, 서명된 코드 자체가 인증서 원본을 나타냅니다.

드롭다운 목록에서 Java 개체 서명에 사용하도록 구성된 인증서를 선택합니다.

Java 코드 서명자를 구성하려면 Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > Clientless SSL VPN Access(클라이언트리스 SSL VPN 액세스) > Advanced(고급) > Java Code Signer(Java 코드 서명자)를 선택합니다.

클라이언트리스 SSL VPN으로 인해 변형된 Java 개체는 나중에 신뢰 지점과 연결된 PKCS12 디지털 인증서를 사용하여 서명할 수 있습니다. Java Trustpoint(Java 신뢰 지점) 창에서 지정된 신뢰 지점 위치의 PKCS12 인증서 및 키 지정 자료를 사용하도록 클라이언트리스 SSL VPN Java 개체 서명 기능을 구성할 수 있습니다.

신뢰 지점을 가져오려면 **Configuration(구성) > Properties(속성) > Certificate(인증서) > Trustpoint(신뢰 지점) > Import(가져오기)**를 선택합니다.

플러그인에 대한 브라우저 액세스 구성

브라우저 플러그인은 웹 브라우저가 브라우저 창 내에서 클라이언트를 서버에 연결하는 등의 전용 기능을 수행하기 위해 호출하는 별도의 프로그램입니다. ASA를 사용하면 클라이언트리스 SSL VPN 세션에서 원격 브라우저로 다운로드할 플러그인을 가져올 수 있습니다. Cisco에서는 재배포하는 플러그인을 테스트하며, 경우에 따라 재배포할 수 없는 플러그인의 연결성을 테스트합니다. 그러나 현재 스트리밍 미디어를 지원하는 플러그인 가져오기는 권장하지 않습니다.

ASA는 플래시 디바이스에 플러그인을 설치할 때 다음 작업을 수행합니다.

- (Cisco 배포 플러그인만 해당) URL에 지정되어 있는 jar 파일의 압축을 풉니다.
- 파일을 ASA 파일 시스템에 작성합니다.
- ASDM에서 URL 특성 옆에 있는 드롭다운 목록을 채웁니다.
- 이후의 모든 클라이언트리스 SSL VPN 세션에 대해 플러그인을 활성화하고 포털 페이지의 Address(주소) 필드 옆에 있는 드롭다운 목록에 기본 메뉴 옵션 및 옵션을 추가합니다.

다음 페이지에는 다음 섹션에 설명된 플러그인을 추가할 경우 포털 페이지의 기본 메뉴 및 주소 필드에 대한 변경 사항이 나와 있습니다.

표 ***5:*** 클라이언트리스 ***SSL VPN*** 포털 페이지에 있는 플러그인의 효과

플러그인	포털 페이지에 추가된 기본 메뉴 옵션	포털 페이지에 추가된 주소 필드 옵션
ica	Citrix MetaFrame 서비스	ica://
rdp	Terminal Servers	rdp://
rdp2*	Terminal Servers Vista	rdp2://
ssh,telnet	SSH(Secure Shell)	ssh://
	텔넷 서비스(v1 및 v2 지원)	telnet://
vnc	가상 네트워크 컴퓨팅 서비스	vnc://

* 권장 플러그인이 아닙니다.

클라이언트리스 SSL VPN 세션에 있는 사용자가 포털 페이지에서 관련 메뉴 옵션을 클릭하면 포털 페이지에는 인터페이스에 대한 창과 도움말 창이 표시됩니다. 사용자가 드롭다운 목록에 표시된 프로토콜을 선택하고 주소 필드에서 URL을 입력하여 연결을 설정할 수 있습니다.

플러그인은 SSO(Single Sign-On: 단일 로그인)를 지원합니다.

플러그인의 사전 요구 사항

- 클라이언트리스 SSL VPN은 플러그인에 대한 원격 액세스를 제공하도록 ASA에 활성화되어 있어야 합니다.
- 플러그인에 대한 SSO 지원을 구성하려면 플러그인을 설치하고 책갈피 항목을 추가하여 서버에 대한 링크를 표시하고 책갈피를 추가할 때 SSO 지원을 지정하십시오.
- 원격 사용에 필요한 최소 액세스 권한은 게스트 권한 모드에 속합니다.
- 플러그인을 사용하려면 ActiveX 또는 Oracle JRE(Java Runtime Environment)가 필요합니다. 버전 요구 사항에 대해서는 지원되는 VPN 플랫폼, Cisco ASA 5500 Series 호환성 매트릭스를 참고하십시오.

플러그인의 제한 사항

참고 원격 데스크톱 프로토콜 플러그인은 세션 브로커를 통한 로드 밸런싱을 지원하지 않습니다. 프로토콜에서 세션 브로커의 리디렉션을 처리하는 방식으로 인해 연결이 실패합니다. 세션 브로커를 사용하지 않는 경우 플러그인이 작동합니다.

- 플러그인은 SSO(Single Sign-On: 단일 로그인)를 지원합니다. 플러그인은 입력된 동일한 자격 증명을 사용하여 클라이언트리스 SSL VPN 세션을 엽니다. 플러그인은 매크로 대체를 지원하지 않으므로 내부 도메인 비밀번호와 같은 다른 필드나 RADIUS 또는 LDAP 서버의 특성에서 SSO를 수행하는 옵션을 제공하지 않습니다.
- 상태 저장 장애 조치는 플러그인을 사용하여 설정된 세션을 그대로 유지하지 않습니다. 사용자는 장애 조치 후 다시 연결해야 합니다.
- 스테이트풀 페일오버 대신 스테이트리스 페일오버를 사용하는 경우에는 클라이언트리스 기능(예: 책갈피, 맞춤화 및 동적 액세스 정책)이 페일오버 ASA 쌍 간에 동기화되지 않습니다. 장애 조치 시 이러한 기능이 작동하지 않습니다.

플러그인 설치 전 보안 어플라이언스 준비

시작하기 전에

클라이언트리스 SSL VPN이 ASA 인터페이스에서 활성화되어 있는지 확인합니다.

IP 주소를 SSL 인증서의 CN(Common Name: 공통 이름)으로 지정하지 마십시오. 원격 사용자는 FQDN을 사용하여 ASA와의 통신을 시도합니다. 원격 PC에서 DNS 또는 System32\drivers\etc\hosts 파일의 항목을 사용하여 FQDN을 확인할 수 있어야 합니다.

프로시저

단계 **1** 클라이언트리스 SSL VPN이 ASA에서 활성화되어 있는지를 표시합니다.

show running-config

단계 **2** ASA 인터페이스에 SSL 인증서를 설치하고 원격 사용자 연결을 위해 FQDN(Fully Qualified Domain Name)을 제공합니다.

Cisco에서 재배포하는 플러그인 설치

Cisco에서는 클라이언트리스 SSL VPN 세션에서 웹 브라우저용 플러그인으로 액세스되는 다음의 오픈 소스 Java 기반 구성 요소를 재배포합니다.

시작하기 전에

클라이언트리스 SSL VPN이 ASA의 인터페이스에서 활성화되어 있는지 확인합니다. 이 작업을 수행하려면 **show running-config** 명령을 입력합니다.

표 *6: Cisco*에서 재배포하는 플러그인

프로토콜	설명	재배포되는 플러그인의 소스*
RDP	Windows Vista 및 Windows 2003 R2에서 호스팅되는 Microsoft 터미널 서비스에 액세스합니다. 원격 데스크톱 ActiveX 컨트롤을 지원합니다. RDP와 RDP2를 모두 지원하는 이 플러그인을 사용하는 것을 권장합니다. 5.1 이하 버전의 RDP 및 RDP2 프로토콜만 지원됩니다. 5.2 이상 버전은 지원되지 않습니다.	http://properjavardp.sourceforge.net/
RDP2	Windows Vista 및 Windows 2003 R2에서 호스팅되는 Microsoft 터미널 서비스에 액세스합니다. 원격 데스크톱 ActiveX 컨트롤을 지원합니다. 이 레거시 플러그인은 RDP2만 지원합니다. 이 플러그인을 사용하지 않는 것을 권장합니다. 대신 위의 RDP 플러그인을 사용하십시오.	
SSH	SSH(Secure Shell) 텔넷 플러그인을 사용하여 원격 사용자는 원격 컴퓨터에 대해 SSH(Secure Shell)(v1 또는 v2) 또는 텔넷 연결을 설정할 수 있습니다. 키보드 인터랙티브 인증은 JavaSSH에서 지원되지 않으므로 다른 인증 메커니즘 구현 시 사용되는 SSH 플러그인을 사용하여 지원할 수 없습니다.	http://javassh.org/

프로토콜	설명	재배포되는 플러그인의 소스*
VNC	가상 네트워크 컴퓨팅 플러그인을 통해 원격 사용자는 모니터, 키보드 및 마우스를 사용하여 원격 데스크톱 공유(VNC 서버 또는 서비스라고도 함)가 켜져 있는 컴퓨터를 확인하고 제어할 수 있습니다. 이 버전에서는 텍스트의 기본 색상이 변경되었으며 업데이트된 프랑스어 및 일본어 도움말 파일이 포함되어 있습니다.	http://www.tightvnc.com/

* 구축 구성 및 제한 사항에 대한 자세한 내용은 플러그인 설명서를 참조해 주십시오.

해당 플러그인은 Cisco Adaptive Security Appliance 소프트웨어 다운로드 사이트에서 다운로드할 수 있습니다.

프로시저

단계 **1** ASA를 통해 ASDM 세션을 설정하는 데 사용하는 컴퓨터에서 이름이 plugins인 임시 디렉토리를 생성하고 필요한 플러그인을 Cisco 웹사이트에서 plugins 디렉토리로 다운로드합니다.

단계 **2** **Configuration(**구성**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **Clientless SSL VPN Access(**클라이언트리스 **SSL VPN** 액세스**)** > **Portal(**포털**)** > **Client-Server Plug-ins(**클라이언트-서버 플러그인**)**를 선택합니다.

이 창에는 클라이언트리스 SSL 세션에 사용할 수 있는 현재 로드된 플러그인이 표시됩니다. 이 플러그인의 해시 및 날짜도 제공됩니다.

단계 **3** 가져오기를 클릭합니다.

단계 **4** 다음 설명에 따라 Import Client-Server Plug-in(클라이언트-서버 플러그인 가져오기) 대화 상자 필드 값을 입력합니다.

- Plug-in Name(플러그인 이름) — 다음 값 중 하나를 선택합니다.
  - **ica**는 Citrix MetaFrame 또는 웹 인터페이스 서비스에 대한 플러그인 액세스를 제공합니다.
  - **rdp**는 원격 데스크톱 프로토콜 서비스에 대한 플러그인 액세스를 제공합니다.
  - **ssh,telnet**은 SSH(Secure Shell) 및 텔넷 서비스 둘 다에 대한 플러그인 액세스를 제공합니다.
  - **vnc**는 가상 네트워크 컴퓨팅 서비스에 대한 플러그인 액세스를 제공합니다.

    참고 이 메뉴에서 문서화되지 않은 모든 옵션은 시험용이며 지원되지 않습니다.

- Select the location of the plugin file(플러그인 파일의 위치 선택) — 다음 옵션 중 하나를 선택하고 텍스트 필드에 경로를 삽입합니다.

- Local computer(로컬 컴퓨터) - 연결된 Path(경로) 필드에 플러그인의 위치 및 이름을 입력하거나 **Browse Local Files(**로컬 파일 찾아보기**)**를 클릭하고 플러그인과 로컬 파일을 선택한 다음 **Select(**선택**)**를 클릭합니다.
- Flash file system(플래시 파일 시스템) - 연결된 Path(경로) 필드에 플러그인의 위치 및 이름을 입력하거나 **Browse Flash(**플래시 찾아보기**)**를 클릭하고 플러그인과 플래시를 선택한 다음 **OK(**확인**)**를 클릭합니다.
- Remote Server(원격 서버) - 원격 서버에서 실행 중인 서비스에 따라 연결된 Path(경로) 특성 옆에 있는 드롭다운 메뉴에서 **ftp**, **tftp** 또는 **HTTP**를 선택합니다. 서버의 호스트 이름 또는 주소 및 플러그인의 경로를 옆의 텍스트 필드에 입력합니다.

단계 **5** **Import Now(**지금 가져오기**)**를 클릭합니다.

단계 **6** 적용을 클릭합니다.

이제 이후의 클라이언트리스 SSL VPN 세션에서 이 플러그인을 사용할 수 있습니다.

Citrix XenApp Server에 대한 액세스 제공

서드파티 플러그인에 대한 클라이언트리스 SSL VPN 브라우저 액세스를 제공하는 방법의 한 가지 예로, 이 섹션에서는 Citrix XenApp Server Client에 대해 클라이언트리스 SSL VPN 지원을 추가하는 방법을 설명합니다.

Citrix 플러그인이 ASA에 설치되어 있는 경우 클라이언트리스 SSL VPN 사용자는 ASA에 대한 연결을 사용하여 Citrix XenApp 서비스에 액세스할 수 있습니다.

상태 저장 장애 조치 시 Citrix 플러그인을 사용하여 설정된 세션이 그대로 유지되지 않습니다. Citrix 사용자는 장애 조치 후에 재인증해야 합니다.

Citrix 플러그인 생성 및 설치

시작하기 전에

플러그인 설치 전에 보안 애플리케이션을 준비하십시오.

Citrix "보안 게이트웨이"를 사용하지 않는 모드에서 작동하도록 Citrix Web Interface 소프트웨어를 구성해야 합니다. 그렇지 않으면 Citrix 클라이언트에서 Citrix XenApp Server에 연결할 수 없습니다.

프로시저

단계 **1** Cisco 소프트웨어 다운로드 웹사이트에서 ica-plugin.zip 파일을 다운로드합니다.

이 파일에는 Cisco에서 Citrix 플러그인에 사용하도록 사용자 지정한 파일이 포함되어 있습니다.

단계 **2** Citrix 사이트에서 Citrix Java 클라이언트를 다운로드합니다.

Citrix 웹사이트의 다운로드 영역에서 Citrix Receiver(Citrix 리시버) 및 Receiver for Other Platforms(다른 플랫폼용 리시버)를 선택하고 Find(찾기)를 클릭합니다. Receiver for Java(Java용 리시버) 하이퍼링크를 클릭하고 압축 파일을 다운로드합니다.

단계 **3** 압축 파일에서 다음 파일의 압축을 푼 다음 ica-plugin.zip 파일에 추가합니다.

- JICA-configN.jar
- JICAEngN.jar

단계 **4** Citrix Java 클라이언트에 포함된 EULA에서 웹 서버에 있는 클라이언트를 구축할 수 있는 권한을 부여하는지 확인합니다.

단계 **5** ASDM을 사용하거나 특권 EXEC 모드에서 다음 CLI 명령을 입력하여 플러그인을 설치합니다.

import webvpn plug-in protocol ica URL

URL은 ica-plugin.zip 파일의 경로 및 호스트 이름 또는 IP 주소입니다.

참고 Citrix 세션에 대한 SSO 지원을 제공하려면 책갈피를 추가해야 합니다. 간편한 보기를 위해 책갈피에서 이 URL 매개변수를 사용하는 것을 권장합니다. 예를 들어 다음과 같습니다.

ica://10.56.1.114/?DesiredColor=4&DesiredHRes=1024&DesiredVRes=768

단계 **6** SSL VPN 클라이언트리스 세션을 설정하고 책갈피를 클릭하거나 Citrix 서버에 대해 URL을 입력합니다.

필요 시 Java용 클라이언트 관리자 설명서를 사용합니다.

포트 전달 구성

포트 전달을 사용하여 사용자는 클라이언트리스 SSL VPN 연결을 통해 TCP 기반 애플리케이션에 액세스할 수 있습니다. 해당하는 애플리케이션은 다음과 같습니다.

- Lotus Notes
- Microsoft Outlook
- Microsoft Outlook Express
- Perforce
- Sametime
- 보안 FTP(FTP over SSH)
- SSH
- 텔넷
- Windows 터미널 서비스

- XDDTS

다른 TCP 기반 애플리케이션도 작동될 수 있지만 이를 대상으로 테스트를 실시하지 않았습니다. UDP를 사용하는 프로토콜은 작동하지 않습니다.

포트 전달은 클라이언트리스 SSL VPN 연결을 통해 TCP 기반 애플리케이션을 지원하는 레거시 기술입니다. 이미 이 기술을 지원하는 구성을 완료했으므로 포트 전달을 사용하도록 선택할 수 있습니다.

포트 전달에 대한 대안으로 다음 사항을 고려하십시오.

- 스마트 터널 액세스는 사용자에게 다음과 같은 이점을 제공합니다.
  - 스마트 터널은 플러그인보다 우수한 성능을 제공합니다.
  - 포트 전달과 달리 스마트 터널을 사용할 경우 로컬 애플리케이션을 로컬 포트에 연결할 필요가 없으므로 사용자 환경이 간소화됩니다.
  - 또한 포트 전달과 달리 스마트 터널은 사용자의 관리자 권한이 필요하지 않습니다.
- 포트 전달 및 스마트 터널 액세스와 달리 플러그인은 원격 컴퓨터에 클라이언트 애플리케이션을 설치할 필요가 없습니다.

ASA에서 포트 포워딩을 구성할 경우 애플리케이션에서 사용할 포트를 지정하십시오. 스마트 터널 액세스를 구성할 경우 실행 파일의 이름 또는 경로를 지정하십시오.

포트 전달을 위한 사전 요구 사항

- 포트 전달(애플리케이션 액세스) 및 디지털 인증서를 지원하려면 Oracle JRE(Java Runtime Environment) 1.5.x 이상이 원격 컴퓨터에 설치되어 있어야 합니다.
- 브라우저 기반 Mac OS X 10.5.3 Safari 사용자는 ASA의 URL에서 사용할 클라이언트 인증서를 식별해야 하며 Safari에서 URL을 해석하는 방법으로 인해 한 번은 후행 슬래시를 사용하고 한 번은 후행 슬래시를 사용하지 않습니다. 예:
  - https://example.com/
  - https://example.com

  자세한 내용은 Safari, Mac OS X 10.5.3: 클라이언트 인증서 인증의 변경사항을 참조하십시오.
- 포트 포워딩 또는 스마트 터널을 사용하는 Microsoft Windows Vista 이상 사용자는 Trusted Site(신뢰할 수 있는 사이트) 영역에 ASA의 URL을 추가해야 합니다. 신뢰할 수 있는 사이트 영역에 액세스하려면 Internet Explorer를 시작한 다음 **Tools(**도구**) > Internet Options(**인터넷 옵션**) > Security(**보안**)** 탭을 선택합니다. 또한 Vista 이상 사용자는 스마트 터널 액세스를 보다 쉽게 사용할 수 있도록 보호 모드를 해제할 수 있습니다. 단, 컴퓨터가 공격에 더욱 취약해지므로 이 방법은 권장되지 않습니다.

포트 전달의 제한 사항

- 포트 전달은 정적 TCP 포트를 사용하는 TCP 애플리케이션만 지원합니다. 동적 포트 또는 여러 TCP 포트를 사용하는 애플리케이션은 지원되지 않습니다. 예를 들어 포트 22를 사용하는 보안 FTP는 클라이언트리스 SSL VPN 포트 전달을 통해 작동하지만 포트 20 및 21을 사용하는 표준 FTP는 작동하지 않습니다.
- 포트 전달은 UDP를 사용하는 프로토콜을 지원하지 않습니다.
- 포트 전달은 MAPI(Microsoft Outlook Exchange) 프록시를 지원하지 않습니다. 그러나 Microsoft Outlook Exchange Server와 함께 Microsoft Office Outlook에 대한 스마트 터널 지원을 구성할 수 있습니다.
- 상태 저장 장애 조치에서는 애플리케이션 액세스(포트 전달 또는 스마트 터널 액세스)를 사용하여 설정된 세션을 그대로 유지하지 않습니다. 사용자는 장애 조치 후 다시 연결해야 합니다.
- 포트 전달은 개인용 정보 단말기에 대한 연결을 지원하지 않습니다.
- 포트 전달을 사용하려면 Java 애플릿을 다운로드하고 로컬 클라이언트를 구성해야 합니다. 이를 위해서는 로컬 시스템에 대한 관리자 권한이 필요하므로 사용자가 공용 원격 시스템에서 연결한 경우 애플리케이션을 사용하지 못할 수도 있습니다.

  Java 애플릿은 엔드 유저 HTML 인터페이스의 고유한 창에 표시됩니다. 여기에는 사용자가 사용할 수 있는 전달된 포트 목록의 내용뿐만 아니라 활성 상태의 포트와 전송 및 수신한 트래픽 용량(바이트)도 표시됩니다.

- 포트 포워딩 애플릿은 로컬 IP 주소 127.0.0.1을 사용하고 ASA에서 클라이언트리스 SSL VPN 연결을 통해 이를 업데이트할 수 없는 경우 로컬 포트와 원격 포트를 동일하게 표시합니다. 따라서 ASA는 로컬 프록시 ID에 대해 새 IP 주소인 127.0.0.2, 127.0.0.3 등을 생성합니다. 호스트 파일을 수정하고 다른 루프백을 사용할 수 있으므로 원격 포트는 애플릿에서 로컬 포트로 사용됩니다. 연결하려면 포트를 지정하지 않고 호스트 이름을 통해 텔넷을 사용할 수 있습니다. 정확한 로컬 IP 주소는 로컬 호스트 파일에서 사용할 수 있습니다.

포트 전달을 위한 **DNS** 구성

포트 포워딩은 확인 및 연결을 위해 원격 서버의 도메인 이름 또는 IP 주소를 ASA에 포워딩합니다. 즉 포트 포워딩 애플릿은 애플리케이션의 요청을 수락하여 ASA에 포워딩합니다. ASA에서는 포트 포워딩 애플릿을 대신해 적절한 DNS 쿼리를 생성하고 연결을 설정합니다. 포트 포워딩 애플릿은 ASA에 대한 DNS 쿼리만 생성합니다. 포트 전달 애플릿은 포트 전달 애플리케이션에서 DNS 쿼리를 시도할 때 쿼리가 루프백 주소로 리디렉션되도록 호스트 파일을 업데이트합니다.

프로시저

단계 **1** **Configuration(**구성**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **Clientless SSL VPN Access(**클라이언트리스 **SSL VPN** 액세스**)** > **Connection Profiles(**연결 프로파일**)**를 클릭합니다.

기본 클라이언트리스 SSL VPN 그룹 항목은 클라이언트리스 연결에 사용되는 기본 연결 프로파일입니다.

단계 **2** 기본 클라이언트리스 SSL VPN 그룹 항목이 클라이언트리스 연결에 사용되도록 구성된 경우 해당 항목을 강조 표시한 다음 **Edit(**수정**)**를 클릭합니다. 그렇지 않은 경우 구성에서 클라이언트리스 연결에 사용되는 연결 프로필을 강조 표시한 다음 **Edit(**수정**)**를 클릭합니다.

단계 **3** DNS 영역으로 이동하고 드롭다운 목록에서 DNS 서버를 선택합니다. ASDM에 사용할 DNS 서버가 표시되면 도메인 이름을 메모한 후 나머지 단계를 무시하고 다음 섹션으로 이동합니다. 포트 전달 목록에서 항목을 구성하는 동안 원격 서버를 지정하는 경우 동일한 도메인 이름을 입력해야 합니다. DNS 서버가 구성에 없는 경우에는 나머지 단계를 계속 진행합니다.

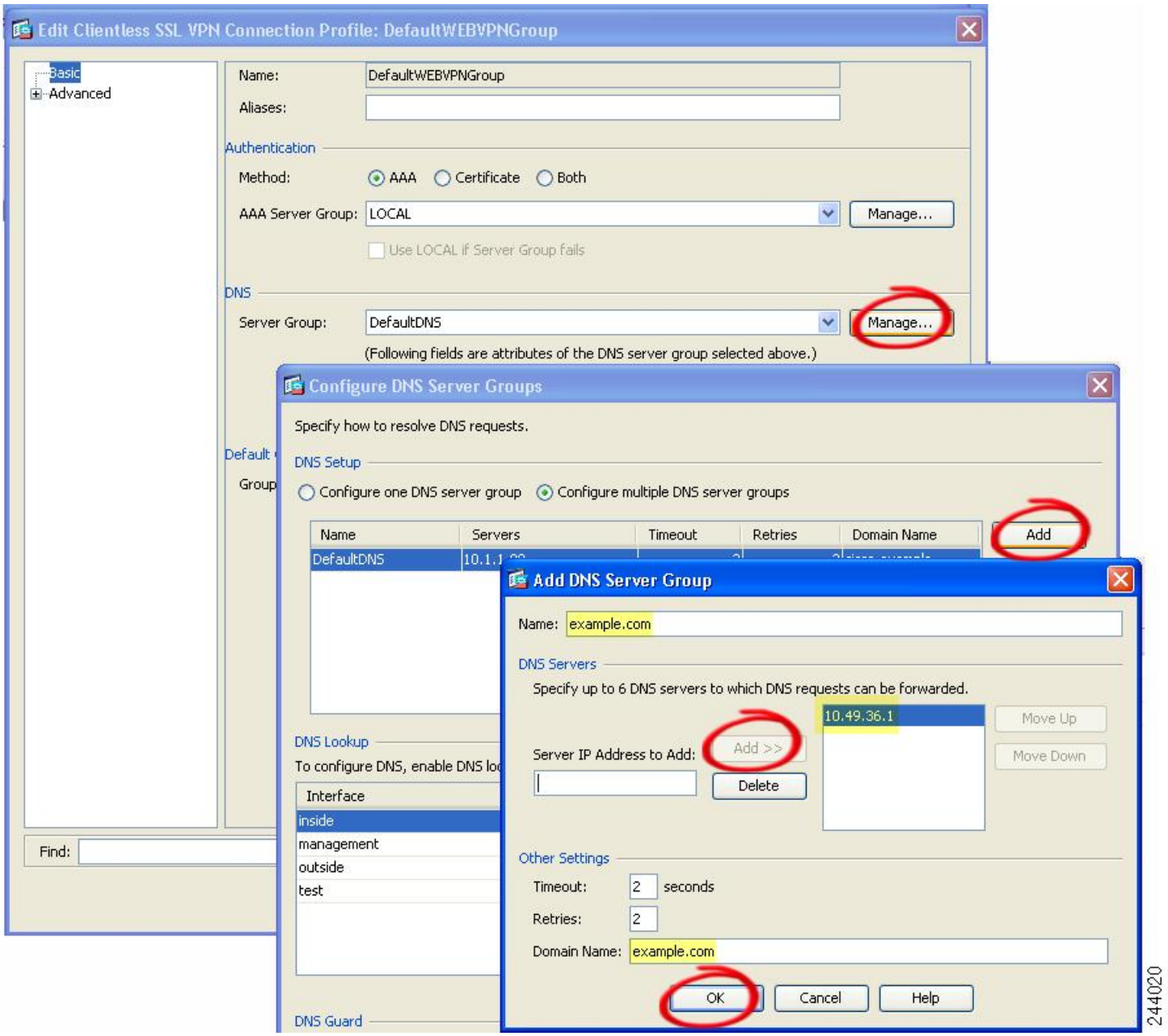
단계 **4** DNS 영역에서 **Manage(**관리**)**를 클릭합니다.

단계 **5** **Configure Multiple DNS Server Groups(**여러 **DNS** 서버 그룹 구성**)**를 클릭합니다.

단계 **6** **Add(**추가**)**를 클릭합니다.

단계 **7** Name(이름) 필드에 새 서버 그룹의 이름을 입력하고 IP 주소 및 도메인 이름을 입력합니다.

그림 *8:* 포트 전달을 위한 *DNS* 서버 값의 예



입력한 도메인 이름을 메모합니다. 이후 포트 전달 항목을 구성하는 동안 원격 서버를 지정할 때 이 메모가 필요합니다.

단계 **8** Connection Profiles(연결 프로필) 창이 다시 활성화될 때까지 **OK(**확인**)**를 클릭합니다.

단계 **9** 구성에서 클라이언트리스 연결에 사용되는 나머지 연결 프로필 각각에 대해 작업을 반복합니다.

단계 **10** **Apply(**적용**)**를 클릭합니다.

포트 전달 항목 추가/수정

Add/Edit Port Forwarding Entry(포트 전달 항목 추가/수정) 대화 상자에서는 클라이언트리스 SSL VPN 연결을 통해 액세스하기 위해 사용자 또는 그룹 정책과 연계할 TCP 애플리케이션을 지정할 수 있습니다. 다음과 같이 이 창의 특성에 값을 할당합니다.

시작하기 전에

터널을 설정하고 IP 주소로 확인하려면 Remote Server(원격 서버) 매개변수에 할당된 DNS 이름이 Domain Name(도메인 이름) 및 Server Group(서버 그룹) 매개변수와 일치해야 합니다. Domain(도메인) 및 Server Group(서버 그룹) 매개변수 두 가지에 대한 기본 설정은 DefaultDNS입니다.

프로시저

단계 **1** **ADD(**추가**)**를 클릭합니다.

단계 **2** 애플리케이션에서 사용할 TCP 포트 번호를 입력합니다. listname에 대해 로컬 포트 번호를 한 번만 사용할 수 있습니다. 로컬 TCP 서비스와의 충돌을 피하려면 1024~65535 범위의 포트 번호를 사용하십시오.

단계 **3** 원격 서버의 도메인 이름 또는 IP 주소를 입력합니다. 특정 IP 주소에 대해 클라이언트 애플리케이션을 구성할 필요가 없도록 도메인 이름을 사용하는 것을 권장합니다.

단계 **4** 애플리케이션의 잘 알려진 포트 번호를 입력합니다.

단계 **5** 애플리케이션에 대한 설명을 입력합니다. 최대 길이는 64자입니다.

단계 **6** (선택 사항) 포트 포워딩 목록을 강조 표시하고 **Assign(**할당**)**을 클릭하여 선택한 목록을 하나 이상의 그룹 정책, 동적 액세스 정책 또는 사용자 정책에 할당합니다.

포트 전달 목록 할당

클라이언트리스 SSL VPN 연결을 통해 액세스하기 위해 사용자 또는 그룹 정책과 연계할 TCP 애플리케이션의 이름이 지정된 목록을 추가하거나 수정할 수 있습니다. 각 그룹 정책 및 사용자 이름에 대해 다음 중 하나를 수행하도록 클라이언트리스 SSL VPN을 구성할 수 있습니다.

참고 이러한 옵션은 각 그룹 정책 및 사용자 이름에 대해 상호 배타적입니다. 한 가지만 사용하십시오.

- 사용자 로그인 시 포트 전달 액세스를 자동으로 시작합니다.
- 사용자 로그인 시 포트 전달 액세스를 활성화하지만 사용자가 클라이언트리스 SSL VPN 포털 페이지에서 **Application Access(**애플리케이션 액세스**) > Start Applications(**애플리케이션 시작**)**를 사용하여 수동으로 시작해야 합니다.

프로시저

단계 **1** 목록에 대한 영숫자 이름을 입력합니다. 최대 길이는 64자입니다.

단계 **2** 애플리케이션에 대한 트래픽을 수신 대기하는 로컬 포트를 입력합니다. listname에 대해 로컬 포트 번호를 한 번만 사용할 수 있습니다. 로컬 TCP 서비스와의 충돌을 피하려면 1024~65535 범위의 포트 번호를 사용하십시오.

참고 원격 서버의 IP 주소 또는 DNS 이름을 입력합니다. 특정 IP 주소에 대해 클라이언트 애플리케이션을 구성할 필요가 없도록 도메인 이름을 사용하는 것을 권장합니다.

단계 **3** 애플리케이션에 대한 트래픽을 수신 대기하는 원격 포트를 입력합니다.

단계 **4** TCP 애플리케이션을 설명합니다. 최대 길이는 64자입니다.

포트 전달 활성화 및 해제

기본적으로 포트 전달은 해제되어 있습니다.

포트 전달을 활성화한 경우 사용자는 클라이언트리스 SSL VPN 포털 페이지에서 **Application Access(**애플리케이션 액세스**) > Start Applications(**애플리케이션 시작**)**를 사용하여 수동으로 시작해야 합니다.

파일 액세스 구성

클라이언트리스 SSL VPN은 원격 사용자에게 ASA에서 실행 중인 프록시 CIFS 및/또는 FTP 클라이언트와 인터페이스로 접속할 수 있는 HTTPS 포털 페이지를 제공합니다. 클라이언트리스 SSL VPN은 사용자가 인증 요건을 충족하고 파일 속성에서 액세스를 제한하지 않는 경우에 한해, CIFS 또는 FTP를 사용하여 사용자에게 네트워크의 파일에 대한 네트워크 액세스를 제공합니다. CIFS 및 FTP 클라이언트는 파악하기 쉬우며 클라이언트리스 SSL VPN에서 제공하는 포털 페이지는 파일 시스템에 대한 직접 액세스 표시를 제공합니다.

사용자가 파일 목록을 요청하면 클라이언트리스 SSL VPN은 마스터 브라우저로 지정된 서버에 해당 목록이 포함된 서버의 IP 주소를 쿼리합니다. ASA에서 목록을 가져와 포털 페이지의 원격 사용자에게 제공합니다.

클라이언트리스 SSL VPN을 통해 사용자는 사용자 인증 요건 및 파일 속성에 따라 다음 CIFS 및 FTP 기능을 호출할 수 있습니다.

- 도메인 및 작업 그룹, 도메인 또는 작업 그룹 내의 서버, 서버 내의 공유 및 공유 또는 디렉토리 내의 파일을 탐색하고 나열합니다.
- 디렉토리를 생성합니다.
- 파일 다운로드, 업로드, 이름 바꾸기, 이동 및 삭제를 수행합니다.

ASA에서는 원격 사용자가 포털 페이지 또는 클라이언트리스 SSL VPN 세션 동안 표시되는 툴바의 메뉴에서 **Browse Networks(**네트워크 찾아보기**)**를 클릭한 경우 일반적으로 ASA와 동일한 네트워크

에 있거나 해당 네트워크에서 연결할 수 있는 마스터 브라우저, WINS 서버 또는 DNS 서버를 사용하여 네트워크에 서버 목록을 쿼리합니다.

마스터 브라우저 또는 DNS 서버는 ASA의 CIFS/FTP 클라이언트에 클라이언트리스 SSL VPN에서 원격 사용자에게 제공하는 네트워크에 있는 리소스 목록을 제공합니다.

참고 파일 액세스를 구성하기 전에 서버에 사용자가 액세스할 수 있는 공유 폴더를 구성해야 합니다.

CIFS 파일 액세스 요건 및 제한 사항

`\\Server\share\subfolder\personal` 폴더에 액세스하려면 사용자에게 공유 폴더 자체를 포함한 모든 상위 폴더에 대한 읽기 이상의 권한이 있어야 합니다.

Download(다운로드) 또는 Upload(업로드)를 사용하여 CIFS 디렉토리와 로컬 데스크톱 간에 파일을 복사하여 붙여 넣을 수 있습니다. Copy(복사) 및 Paste(붙여넣기) 버튼은 원격-원격 작업용이며 로컬-원격 또는 원격-로컬 작업에는 사용되지 않습니다.

파일을 웹 폴더에서 워크스테이션의 폴더로 드래그 앤 드롭하면 임시 파일로 표시되는 항목을 확인할 수 있습니다. 보기를 업데이트하고 전송된 파일을 표시하려면 워크스테이션의 폴더를 새로 고칩니다.

CIFS 찾아보기 서버 기능은 더블바이트 문자 공유 이름(길이가 13자를 초과하는 공유 이름)을 지원하지 않습니다. 이는 표시되는 폴더 목록에만 적용되며 폴더에 대한 사용자 액세스에는 영향을 주지 않습니다. 차선책으로 더블바이트 공유 이름을 사용하는 CIFS 폴더에 대한 책갈피를 미리 구성하거나 사용자가 cifs://server/<long-folder-name> 형식으로 폴더의 URL 또는 책갈피를 입력할 수 있습니다. 예를 들면 다음과 같습니다.

```
cifs://server/Do you remember?
cifs://server/Do%20you%20remember%3F
```

파일 액세스 지원 추가

참고 이 절차에서는 마스터 브라우저 및 WINS 서버를 지정하는 방법에 대해 설명합니다. 한 가지 대안으로 ASDM을 사용하여 파일 공유에 대한 액세스를 제공하는 URL 목록 및 항목을 구성할 수 있습니다.

ASDM에서 공유를 추가하는 경우 마스터 브라우저나 WINS 서버가 필요하지 않습니다. 그러나 이 경우 Browse Networks(네트워크 찾아보기) 링크가 지원되지 않습니다. nbns-server 명령을 입력할 때 호스트 이름 또는 IP 주소를 사용하여 ServerA를 참조할 수 있습니다. 호스트 이름을 사용하는 경우 ASA에서는 DNS 서버가 호스트 이름을 IP 주소로 확인하도록 요구합니다.

SharePoint 액세스를 위한 클록 정확도 유지

ASA의 클라이언트리스 SSL VPN 서버는 쿠키를 사용하여 엔드포인트의 Microsoft Word와 같은 애플리케이션과 상호 작용합니다. ASA의 시간이 잘못된 경우 SharePoint 서버에 있는 문서에 액세스하면 ASA에서 설정한 쿠키 만료 시간으로 인해 Word가 제대로 작동하지 않을 수 있습니다. 오작동을 방지하려면 ASA 클록을 올바르게 설정해야 합니다. NTP 서버와 시간을 동적으로 동기화하도록 ASA를 구성하는 것이 좋습니다. 자세한 지침은 일반 운영 구성 가이드의 날짜 및 시간 설정 섹션을 참고하십시오.

VDI(Virtual Desktop Infrastructure)

ASA는 Citrix 및 VMware VDI 서버에 대한 연결을 지원합니다.

- Citrix의 경우 ASA를 사용하여 클라이언트리스 포털을 통해 사용자가 실행 중인 Citrix Receiver에 액세스할 수 있습니다.
- VMware는 (스마트 터널) 애플리케이션으로 구성됩니다.

다른 서버 애플리케이션과 마찬가지로 클라이언트리스 포털의 책갈피를 통해 VDI 서버에 액세스할 수도 있습니다.

VDI 제한 사항

- 인증서 또는 스마트 카드를 사용한 인증은 해당 형식의 인증에서 ASA를 통과하는 것을 허용하지 않기 때문에 자동 로그온이 지원되지 않습니다.
- XenApp 및 XenDesktop 서버에 XML 서비스를 설치 및 구성해야 합니다.
- 클라이언트 인증서 확인, 이중 인증, 내부 비밀번호 및 CSD(자격 증명 모음을 비롯해 모든 CSD)는 독립 실행형 모바일 클라이언트를 사용하는 경우 지원되지 않습니다.

Citrix 모바일 지원

Citrix Receiver를 실행하는 모바일 사용자는 다음 방법으로 Citrix 서버에 연결할 수 있습니다.

- AnyConnect를 통해 ASA에 연결한 다음 Citrix 서버에 연결합니다.
- AnyConnect 클라이언트를 사용하지 않고 ASA를 통해 Citrix 서버에 연결합니다. 로그온 자격 증명에는 다음이 포함될 수 있습니다.
  - Citrix 로그온 화면의 연결 프로파일 별칭(터널 그룹 별칭이라고도 함). VDI 서버에는 각각의 권한 부여 및 연결 설정이 다른 여러 그룹 정책이 있을 수 있습니다.
  - RSA 서버가 구성된 경우 RSA SecureID 토큰 값. RSA는 무효한 항목을 비롯해 초기 또는 만료된 PIN에 대한 새 PIN 입력에 대해 다음 토큰을 지원합니다.

Citrix용으로 지원되는 모바일 디바이스

- iPad — Citrix Receiver 4.x 이상 버전
- iPhone/iTouch — Citrix Receiver 4.x 이상 버전
- Android 2.x/3.x/4.0/4.1 전화기 — Citrix Receiver 2.x 이상 버전
- Android 4.0 전화기 — Citrix Receiver 2.x 이상 버전

Citrix 제한 사항

인증서 제한 사항

- 인증서/스마트카드 인증은 자동 로그온 방법으로 지원되지 않습니다.
- 클라이언트 인증서 확인 및 CSD는 지원되지 않습니다.
- 인증서의 Md5 서명은 iOS의 문제(http://support.citrix.com/article/CTX132798)에 해당하는 보안 문제로 인해 작동하지 않습니다.
- SHA2 서명은 Citrix 웹사이트(http://www.citrix.com/)에 설명된 대로 Windows 외에는 지원되지 않습니다.
- 키 크기가 1024보다 큰 경우 지원되지 않습니다.

기타 제한 사항

- HTTP 리디렉션은 지원되지 않으며 Citrix Receiver 애플리케이션은 리디렉션 시 작동하지 않습니다.
- XenApp 및 XenDesktop 서버에 XML 서비스를 설치 및 구성해야 합니다.

Citrix Mobile Receiver 사용자 로그온 정보

Citrix 서버에 연결하는 모바일 사용자의 로그온은 ASA에서 Citrix 서버를 VDI 서버 또는 VDI 프록시 서버로 구성했는지에 따라 다릅니다.

Citrix 서버가 VDI 서버로 구성된 경우 다음을 수행하십시오.

1. AnyConnect Secure Mobility Client를 사용하여 VPN 자격 증명으로 ASA에 연결합니다.
2. Citrix Mobile Receiver를 사용하여 Citrix 서버 자격 증명으로 Citrix 서버에 연결합니다(단일 로그온이 구성된 경우에는 Citrix 자격 증명이 필요하지 않음).

ASA가 VDI 프록시 서버로 구성된 경우 다음을 수행하십시오.

1. Citrix Mobile Receiver를 사용하여 VPN 및 Citrix 서버 모두에 대해 자격 증명 입력으로 ASA에 연결합니다. 첫 번째 연결이 올바르게 구성된 경우 후속 연결에서는 VPN 자격 증명만 제공하면 됩니다.

Citrix 서버의 프록시로 ASA 구성

Citrix 서버의 프록시 역할을 하도록 ASA를 구성하여 ASA 연결이 사용자에게 Citrix 서버 연결처럼 표시되도록 할 수 있습니다. ASDM에서 VDI 프록시를 활성화한 경우 AnyConnect 클라이언트가 필요하지 않습니다. 엔드 유저가 Citrix에 연결되는 방식을 보여주는 상위 수준의 단계는 다음과 같습니다.

프로시저

단계 **1** 모바일 사용자가 Citrix Receiver를 열고 ASA의 URL에 연결합니다.

단계 **2** 사용자가 Citrix 로그온 화면에서 XenApp 서버 및 VPN 자격 증명을 제공합니다.

단계 **3** 이후에는 Citrix 서버에 연결할 때마다 VPN 자격 증명만 입력하면 됩니다.

ASA를 XenApp 및 XenDesktop의 프록시로 사용하는 경우에는 Citrix 액세스 게이트웨이에 대한 요건이 필요하지 않습니다. XenApp 서버 정보가 ASA에 로깅되고 ASDM에 표시됩니다.

Citrix 서버의 주소 및 로그온 자격 증명을 구성하고 해당 VDI 서버를 그룹 정책 또는 사용자 이름에 할당합니다. 사용자 이름과 그룹 정책을 둘 다 구성한 경우에는 사용자 이름 설정이 그룹 정책 설정을 재정의합니다.

다음에 수행할 작업

http://www.youtube.com/watch?v=JMM2RzppaG8 - 이 비디오에서는 ASA를 Citrix 프록시로 사용할 경우의 이점에 대해 설명합니다.

VDI 서버 또는 VDI 프록시 서버 구성

프로시저

단계 **1** **Configuration(**구성**) > Remote Access VPN(**원격 액세스 **VPN) > Clientless SSL VPN Access(**클라이언트리스 **SSL VPN** 액세스**) > VDI Access(VDI** 액세스**)**를 선택합니다.

단계 **2** 단일 서버의 경우 **Enable VDI Server Proxy(VDI** 서버 프록시 활성화**)**를 선택하고 VDI 서버를 구성합니다.

단계 **3** VDI 서버에 여러 그룹 정책을 할당하려면 **Configure All VDI Servers(**모든 **VDI** 서버 구성**)**를 선택합니다.

단계 **4** **VDI** 서버를 추가하고 하나 이상의 그룹 정책을 할당합니다.

그룹 정책에 VDI 서버 할당

다음과 같은 방법으로 VDI 서버를 구성하고 그룹 정책에 할당합니다.

- VDI Access(VDI 액세스) 창에서 VDI 서버를 추가하고 이 서버에 그룹 정책을 할당합니다.
- 그룹 정책에 VDI 서버를 추가합니다.

프로시저

단계 **1** **Configuration(**구성**) > Remote Access VPN(**원격 액세스 **VPN) > Clientless SSL VPN Access(**클라이언트리스 **SSL VPN** 액세스**) > Group Policies(**그룹 정책**)**를 찾습니다.

단계 **2** DfltGrpPolicy를 수정하고 왼쪽 메뉴에서 More(추가) 옵션 메뉴를 확장합니다.

단계 **3** **VDI Access(VDI** 액세스**)**를 선택합니다.

단계 **4** **Add(**추가**)** 또는 **Edit(**수정**)**를 클릭하여 VDI 서버 세부 사항을 입력합니다.

- **Server(Host Name or IP Address)(**서버**(**호스트 이름 또는 **IP** 주소**))** — XenApp 또는 XenDesktop 서버의 주소입니다. 이 값은 클라이언트리스 매크로일 수 있습니다.
- **Port Number(Optional)(**포트 번호**(**선택 사항**))** — Citrix 서버에 연결하는 데 필요한 포트 번호입니다. 이 값은 클라이언트리스 매크로일 수 있습니다.
- **Active Directory Domain Name(Active Directory** 도메인 이름**)** — 가상화 인프라 서버에 로그인하는 데 필요한 도메인입니다. 이 값은 클라이언트리스 매크로일 수 있습니다.
- **Use SSL Connection(SSL** 연결 사용**)** — SSL을 사용하여 서버를 연결하려면 이 체크 박스를 선택합니다.
- **Username(**사용자 이름**)** — 가상화 인프라 서버에 로그인하는 데 필요한 사용자 이름입니다. 이 값은 클라이언트리스 매크로일 수 있습니다.
- **Password(**비밀번호**)** — 가상화 인프라 서버에 로그인하는 데 필요한 비밀번호입니다. 이 값은 클라이언트리스 매크로일 수 있습니다.

클라이언트-서버 플러그인에 대한 브라우저 액세스 구성

Client-Server Plug-in(클라이언트-서버 플러그인) 테이블에는 ASA에서 클라이언트리스 SSL VPN 세션의 브라우저가 사용할 수 있도록 설정한 플러그인이 표시됩니다.

플러그인을 추가, 변경 또는 제거하려면 다음 중 하나를 수행하십시오.

- 플러그인을 추가하려면 **Import(**가져오기**)**를 클릭합니다. Import Plug-ins(플러그인 가져오기) 대화 상자가 열립니다.
- 플러그인을 제거하려면 해당 플러그인을 선택하고 **Delete(**삭제**)**를 클릭합니다.

브라우저 플러그인 설치 정보

브라우저 플러그인은 웹 브라우저가 브라우저 창 내에서 클라이언트를 서버에 연결하는 등의 전용 기능을 수행하기 위해 호출하는 별도의 프로그램입니다. ASA를 사용하면 클라이언트리스 SSL VPN 세션에서 원격 브라우저로 다운로드할 플러그인을 가져올 수 있습니다. Cisco에서는 재배포하는 플러그인을 테스트하며, 경우에 따라 재배포할 수 없는 플러그인의 연결성을 테스트합니다. 그러나 현재 스트리밍 미디어를 지원하는 플러그인 가져오기는 권장하지 않습니다.

ASA는 플래시 디바이스에 플러그인을 설치할 때 다음 작업을 수행합니다.

- (Cisco 배포 플러그인만 해당) URL에 지정되어 있는 jar 파일의 압축을 풉니다.
- ASA 파일 시스템의 csco-config/97/plugin 디렉토리에 파일을 씁니다.
- ASDM에서 URL 특성 옆에 있는 드롭다운 목록을 채웁니다.
- 이후의 모든 클라이언트리스 SSL VPN 세션에 대해 플러그인을 활성화하고 포털 페이지의 Address(주소) 필드 옆에 있는 드롭다운 목록에 기본 메뉴 옵션 및 옵션을 추가합니다.

다음 표에는 다음 섹션에 설명된 플러그인을 추가할 경우 포털 페이지의 기본 메뉴 및 주소 필드에 대한 변경 사항이 나와 있습니다.

표 ***7:*** 클라이언트리스 ***SSL VPN*** 포털 페이지에 있는 플러그인의 효과

플러그인	포털 페이지에 추가된 기본 메뉴 옵션	포털 페이지에 추가된 주소 필드 옵션
ica	Citrix 클라이언트	citrix://
rdp	Terminal Servers	rdp://
rdp2	Terminal Servers Vista	rdp2://
ssh,telnet	SSH	ssh://
	텔넷	telnet://
vnc	VNC Client	vnc://

참고 보조 ASA는 기본 ASA에서 플러그인을 가져옵니다.

클라이언트리스 SSL VPN 세션에 있는 사용자가 포털 페이지에서 관련 메뉴 옵션을 클릭하면 포털 페이지에는 인터페이스에 대한 창과 도움말 창이 표시됩니다. 사용자가 드롭다운 목록에 표시된 프로토콜을 선택하고 주소 필드에서 URL을 입력하여 연결을 설정할 수 있습니다.

참고 일부 Java 플러그인은 대상 서비스의 세션이 설정되지 않은 경우에도 연결됨 또는 온라인 상태를 보고할 수 있습니다. 오픈 소스 플러그인은 상태를 보고하지만 ASA는 보고하지 않습니다.

브라우저 플러그인 설치 사전 요구 사항

- 보안 어플라이언스가 프록시 서버를 사용하도록 클라이언트리스 세션을 구성한 경우 플러그인이 작동하지 않습니다.

  참고 원격 데스크톱 프로토콜 플러그인은 세션 브로커를 통한 로드 밸런싱을 지원하지 않습니다. 프로토콜에서 세션 브로커의 리디렉션을 처리하는 방식으로 인해 연결이 실패합니다. 세션 브로커를 사용하지 않는 경우 플러그인이 작동합니다.

- 플러그인은 SSO(Single Sign-On: 단일 로그인)를 지원합니다. 플러그인은 입력된 동일한 자격 증명을 사용하여 클라이언트리스 SSL VPN 세션을 엽니다. 플러그인은 매크로 대체를 지원하지 않으므로 내부 도메인 비밀번호와 같은 다른 필드나 RADIUS 또는 LDAP 서버의 특성에서 SSO를 수행하는 옵션을 제공하지 않습니다.
- 플러그인에 대한 SSO 지원을 구성하려면 플러그인을 설치하고 책갈피 항목을 추가하여 서버에 대한 링크를 표시하고 책갈피를 추가할 때 SSO 지원을 지정하십시오.
- 원격 사용에 필요한 최소 액세스 권한은 게스트 권한 모드에 속합니다.

브라우저 플러그인 설치 요건

- GNU GPL(General Public License: 일반 공중 사용 허가서)에 따라 Cisco에서는 플러그인을 변경하지 않고 재배포합니다. GPL에 따라 Cisco에서는 해당 플러그인을 직접 개선할 수 없습니다.
- 클라이언트리스 SSL VPN은 플러그인에 대한 원격 액세스를 제공하도록 ASA에서 활성화되어 있어야 합니다.
- 상태 저장 장애 조치는 플러그인을 사용하여 설정된 세션을 그대로 유지하지 않습니다. 사용자는 장애 조치 후 다시 연결해야 합니다.
- 플러그인을 사용하려면 ActiveX 또는 Oracle JRE(Java Runtime Environment)가 브라우저에서 활성화되어 있어야 합니다. 64비트 브라우저용 RDP 플러그인의 ActiveX 버전은 없습니다.

RDP 플러그인 설정

RDP 플러그인을 설치하고 사용하려면 새 환경 변수를 추가해야 합니다.

프로시저

단계 **1** **My Computer(**내 컴퓨터**)**를 마우스 오른쪽 버튼으로 클릭하여 시스템 속성에 액세스한 후 **Advanced(**고급**)** 탭을 선택합니다.

단계 **2** Advanced(고급) 탭에서 환경 변수 버튼을 선택합니다.

단계 **3** 새 사용자 변수 대화 상자에서 RF_DEBUG 변수를 입력합니다.

단계 **4** 사용자 변수 섹션에서 새 환경 변수를 확인합니다.

단계 **5** 클라이언트 컴퓨터에서 8.3 이전의 버전 클라이언트리스 SSL VPN을 사용하는 경우에는 기존 Cisco Portforwarder Control을 제거해야 합니다. C:/WINDOWS/Downloaded Program Files 디렉토리로 이동하여 Portforwarder Control을 마우스 오른쪽 버튼으로 클릭하고 **Remove(**제거**)**를 선택합니다.

단계 **6** Internet Explorer 브라우저 캐시를 모두 지웁니다.

단계 **7** 클라이언트리스 SSL VPN 세션을 시작하고 RDP ActiveX 플러그인을 통해 RDP 세션을 설정합니다.

이제 Windows 애플리케이션 이벤트 뷰어에서 이벤트를 관찰할 수 있습니다.

플러그인 설치 전 보안 어플라이언스 준비

프로시저

단계 **1** 클라이언트리스 SSL VPN이 ASA 인터페이스에서 활성화되어 있는지 확인합니다.

단계 **2** 원격 사용자가 FQDN(Fully Qualified Domain Name)을 사용하여 연결하는 ASA 인터페이스에 SSL 인증서를 설치합니다.

참고 IP 주소를 SSL 인증서의 CN(Common Name: 공통 이름)으로 지정하지 마십시오. 원격 사용자는 FQDN을 사용하여 ASA와의 통신을 시도합니다. 원격 PC에서 DNS 또는 System32\drivers\etc\hosts 파일의 항목을 사용하여 FQDN을 확인할 수 있어야 합니다.

15 장

고급 클라이언트리스 SSL VPN 구성

Microsoft Kerberos 제한 위임 솔루션

많은 조직에서는 현재 ASA SSO 기능이 제공할 수 있는 것보다 더 많은 인증 방법을 사용하여 클라이언트리스 VPN 사용자를 인증하고 조직의 인증 크리덴셜을 웹 기반 리소스로 원활하게 확장하고자 합니다. 스마트 카드 및 OTP(One-time Password: 일회용 비밀번호)를 사용하여 원격 액세스 사용자를 인증하려는 수요가 증가하는 상황에서, SSO 기능은 인증이 필요할 때 정적 사용자 이름 및 비밀번호와 같이 기본적인 사용자 자격 증명만을 클라이언트리스 웹 기반 리소스에 전달하기 때문에 이러한 수요를 충족시키기에 충분하지 않습니다.

예를 들어 인증서 또는 OTP 기반 인증 방법에는 ASA가 웹 기반 리소스에 대해 SSO 액세스를 원활하게 수행하는 데 필요한 기본 사용자 이름 및 비밀번호가 포함되지 않습니다. 인증서를 사용하여 인증할 경우, 사용자 이름과 비밀번호는 ASA가 웹 기반 리소스로 확장하는 데 필요하지 않으므로 SSO에 대해 지원되지 않는 인증 방법입니다. 반면에 OTP는 정적 사용자 이름을 포함하지만 비밀번호가 동적이므로 VPN 세션 전체에서 이후에 변경됩니다. 일반적으로 웹 기반 리소스는 정적 사용자 이름 및 비밀번호를 수락하도록 구성되므로 OTP는 SSO에 대해 지원되지 않는 인증 방법이 됩니다.

Microsoft의 KCD(Kerberos Constrained Delegation)는 ASA 소프트웨어 릴리스 8.4에서 소개된 새로운 기능으로, 프라이빗 네트워크에 있는 Kerberos로 보호되는 웹 애플리케이션에 대한 액세스 권한을 제공합니다. 이러한 이점 덕분에 인증서 및 OTP 기반 인증 방법을 웹 애플리케이션으로 원활하게 확장할 수 있습니다. 따라서 SSO 및 KCD가 개별적으로 작동되더라도 이제 많은 조직에서는 ASA에서 지

원하는 모든 인증 방법을 사용하여 클라이언트리스 VPN 사용자를 인증하고 인증 크리덴셜을 웹 애플리케이션으로 원활하게 확장할 수 있습니다.

KCD 작동 방식

Kerberos는 신뢰할 수 있는 서드파티를 사용하여 네트워크에서 엔터티의 디지털 ID를 확인합니다. 이러한 엔터티(예: 호스트에서 실행 중인 사용자, 호스트 컴퓨터 및 서비스)는 보안 주체라고 하며 동일한 도메인에 있어야 합니다. 비밀 키 대신 Kerberos는 티켓을 사용하여 서버에 대해 클라이언트를 인증합니다. 티켓은 비밀 키에서 파생되며 클라이언트 ID, 암호화된 세션 키, 플래그로 구성됩니다. 각 티켓은 키 배포 센터에서 발행되며 수명이 설정되어 있습니다.

Kerberos 보안 시스템은 데이터를 암호화하여 엔터티(사용자, 컴퓨터 또는 애플리케이션)를 인증하고 네트워크 전송을 보호하기 위해 사용되는 네트워크 인증 프로토콜이므로 정보의 대상이 되는 디바이스만 암호 해독할 수 있습니다. 클라이언트리스 SSL VPN 사용자에게 Kerberos로 보호되는 모든 웹 서비스에 대한 SSO 액세스를 제공하기 위해 KCD를 구성할 수 있습니다. 이러한 웹 서비스 또는 애플리케이션의 예로는 OWA(Outlook Web Access: Outlook 웹 액세스), Sharepoint 및 IIS(Internet Information Server: 인터넷 정보 서버)가 있습니다.

Kerberos 프로토콜에 대해 프로토콜 전환 및 제한 위임이라는 두 가지 확장 기능이 구현되었습니다. 이러한 확장을 통해 클라이언트리스 SSL VPN 원격 액세스 사용자가 사설 네트워크에 있는 Kerberos 인증 애플리케이션에 액세스할 수 있습니다.

프로토콜 전환은 사용자 인증 레벨에서 다양한 인증 메커니즘을 지원하고 후속 애플리케이션 레이어에서 보안 기능(예: 상호 인증 및 제한 위임)을 위해 Kerberos 프로토콜로 전환함으로써 유연성 및 보안을 강화합니다. 제한 위임은 애플리케이션 서비스가 사용자 대신 역할을 수행할 수 있는 한계를 정하여 도메인 관리자가 애플리케이션 신뢰 경계를 지정하고 이를 적용할 수 있는 방법을 제공합니다. 이러한 유연성 덕분에 신뢰할 수 없는 서비스로 인해 손상될 가능성이 줄어들어 애플리케이션 보안 설계가 개선됩니다.

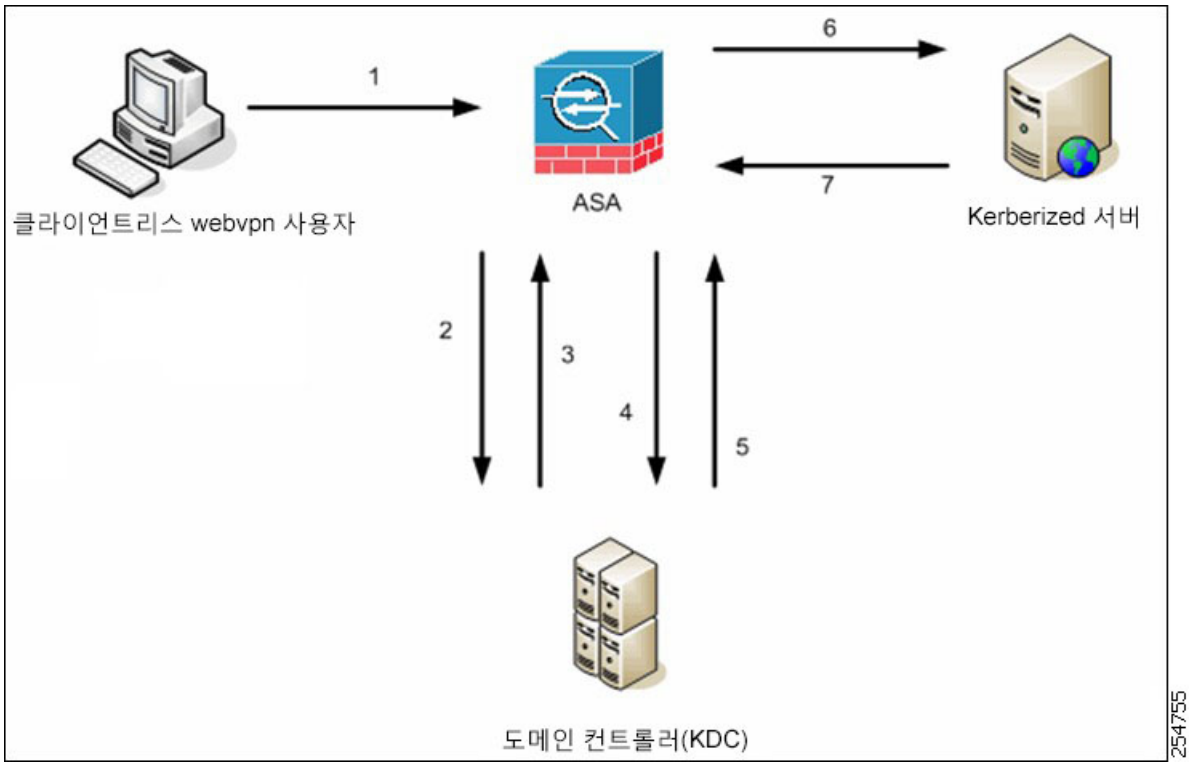
제한 위임에 대한 자세한 내용은 IETF 웹 사이트(http://www.ietf.org)에서 RFC 1510을 참조하십시오.

KCD를 통한 인증 흐름

다음 그림은 클라이언트리스 포털을 통해 위임에 대해 신뢰할 수 있는 리소스에 액세스할 때 사용자가 직간접적으로 경험하는 패킷 및 프로세스 흐름을 표시한 것입니다. 이 프로세스는 다음 작업이 완료된 상태라고 가정합니다.

- ASA에 KCD를 구성함
- Windows Active Directory에 조인하고 서비스가 위임에 대해 신뢰할 수 있는지 확인함
- Windows Active Directory 도메인의 멤버로 ASA 위임함

그림 9: KCD 프로세스



참고 클라이언트리스 사용자 세션은 사용자에 대해 구성된 인증 메커니즘을 사용하여 ASA에서 인증됩니다. (스마트 카드 크리덴셜의 경우 ASA는 디지털 인증서의 userPrincipalName을 Windows Active Directory와 비교하여 LDAP 권한을 부여합니다.)

1. 인증이 성공한 후에 사용자는 ASA 클라이언트리스 포털 페이지에 로그인합니다. 사용자는 포털 페이지에 URL을 입력하거나 책갈피를 클릭하여 웹 서비스에 액세스합니다. 웹 서비스에 인증이 필요한 경우 서버는 ASA에 크리덴셜을 요구하고 서버에서 지원하는 인증 방법 목록을 전송합니다.

참고 클라이언트리스 SSL VPN에 대한 KCD는 모든 인증 방법(RADIUS, RSA/SDI, LDAP, 디지털 인증서 등)에 지원됩니다. AAA 지원 표 (http://www.cisco.com/en/US/docs/security/asa/asa84/configuration/guide/access_aaa.html#wp1069492)를 참조하십시오.

2. 이 챌린지의 HTTP 헤더에 기반하여 ASA는 서버에 Kerberos 인증이 필요한지 판단합니다. (이는 SPNEGO 메커니즘의 일부입니다.) 백엔드 서버에 연결하는 데 Kerberos 인증이 필요한 경우, ASA는 사용자를 대신하여 자체적으로 키 배포 센터에서 서비스 티켓을 요청합니다.

3. 키 배포 센터는 요청한 티켓을 ASA에 반환합니다. 이 티켓이 ASA에 전달되는 경우에도 이 티켓에는 사용자의 권한 부여 데이터가 포함되어 있습니다. ASA는 사용자가 액세스하려는 특정 서비스에 대해 KDC에서 서비스 티켓을 요청합니다.

참고 1~3단계는 프로토콜 전환을 구성합니다. 이 단계를 수행한 후 비 Kerberos 인증 프로토콜을 사용하여 ASA에 대한 인증을 하는 모든 사용자는 Kerberos를 사용하여 키 배포 센터에 대해 자동으로 인증됩니다.

4. ASA는 사용자가 액세스하려는 특정 서비스에 대해 키 배포 센터에서 서비스 티켓을 요청합니다.
5. 키 배포 센터는 특정 서비스에 대한 서비스 티켓을 ASA에 반환합니다.
6. ASA는 서비스 티켓을 사용하여 웹 서비스에 대한 액세스 권한을 요청합니다.
7. 웹 서버는 Kerberos 서비스 티켓을 인증하고 서비스에 대한 액세스 권한을 부여합니다. 인증이 실패할 경우 적절한 오류 메시지가 표시되고 확인을 요구합니다. Kerberos 인증이 실패할 경우에 예상되는 동작은 기본 인증으로 돌아가는 것입니다.

KCD 디버그

다음 명령을 사용하여 9.5.2 버전 이전의 사례와 같이 ADI가 syslog를 내보내는 레벨을 제어하는 대신 KCD 특정 디버그 메시지에 대한 출력을 제어할 수 있습니다.

debug webvpn kcd

Active Directory에서 Windows 서비스 어카운트 추가

ASA에서의 KCD 구현에는 서비스 어카운트 즉, 컴퓨터를 추가(예: 도메인에 ASA 추가)하는 데 필요한 권한이 있는 Active Directory 사용자 어카운트가 필요합니다. 예에서 Active Directory 사용자 이름인 JohnDoe는 필수 권한이 있는 서비스 어카운트를 나타냅니다. Active Directory의 사용자 권한을 구현하는 방법에 대한 자세한 내용은 Microsoft 지원에 문의하거나 http://microsoft.com을 방문하십시오.

KCD에 대한 DNS 구성

이 섹션에서는 ASA에서 DNS를 구성하는 데 필요한 구성 절차에 대해 설명합니다. KCD를 ASA에서 인증 위임 방법으로 사용할 경우 DNS는 ASA, 도메인 컨트롤러(DC) 및 위임에 대해 신뢰할 수 있는 서비스 간에 통신 및 호스트 이름 확인을 활성화하는 데 필요합니다.

프로시저

단계 1 ASDM에서 **Configuration**(구성) > **Remote Access VPN**(원격 액세스 **VPN**) > **DNS**로 이동하여 DNS 설정을 구성합니다.

- DNS Server Group(DNS 서버 그룹) — 192.168.0.3과 같은 DNS 서버 IP 주소를 입력합니다.

• Domain Name(도메인 이름) — DC가 요소인 도메인 이름을 입력합니다.

단계 **2** 해당하는 인터페이스에서 DNS 조회를 활성화합니다. 클라이언트리스 VPN 구축에는 내부 기업 네트워크, 일반적으로 내부 인터페이스를 통한 DNS 조회가 필요합니다.

Active Directory 도메인에 가입하도록 ASA 구성

이 섹션에서는 ASA가 Active Directory 도메인의 일부로 작동하게 하는 데 필요한 구성 절차에 대해 설명합니다. KCD에서는 ASA가 Active Directory 도메인의 구성 요소가 되도록 요구합니다. 이 구성은 ASA 및 KCD 서버 간의 제한된 위임 트랜잭션에 필요한 기능을 지원합니다.

프로시저

단계 **1** ASDM에서 **Configuration(**구성**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **Clientless SSL VPN Access(**클라이언트리스 **SSL VPN)** > **Advanced(**고급**)** > **Microsoft KCD Server(Microsoft KCD** 서버**)**로 이동합니다.

단계 **2** **New(**새로 만들기**)**를 클릭하여 제한 위임을 위한 Kerberos 서버 그룹을 추가하고 다음을 구성합니다.

• 서버 그룹 구성

  • Server Group Name(서버 그룹 이름) - ASA에서 제한된 위임 구성의 이름을 정의합니다(예: 기본값인 MSKCD). 이중화를 위해 여러 서버 그룹을 구성할 수 있지만 VPN 사용자를 대신하여 서비스 티켓을 요청하는 데 사용할 KCD 서버 구성에는 하나의 서버 그룹만 할당할 수 있습니다.

  • Reactivation Mode(재활성화 모드) - 필수 모드(**Depletion(**감소형**)** 또는 **Timed(**시간 제한**)**)의 라디오 버튼을 클릭합니다. Depletion 모드에서는 그룹의 모든 서버가 비활성 상태가 되어야 실패한 서버가 재활성화됩니다. 시간 제한 모드에서 실패한 서버는 30초의 다운타임 후에 다시 활성화됩니다. 감소형이 기본 구성입니다.

  • Dead Time(데드 타임) — 감소형 재활성화 모드를 선택한 경우, 데드 타임 간격을 추가해야 합니다. 10분이 기본 구성입니다. 이 간격은 그룹에서 마지막 서버의 비활성화와 모든 서버의 후속 재활성화 간에 경과한 시간(분)을 나타냅니다.

  • Max Failed Attempts(최대 실패 횟수) — 응답하지 않는 서버를 비활성화 상태로 선언하기 전에 허용되는 실패한 연결 시도 횟수를 설정합니다. 기본값은 3회입니다.

• 서버 구성

  • Interface Name(인터페이스 이름) — 서버가 위치하는 인터페이스를 선택합니다. 일반적으로 인증 서버 구축은 내부 인터페이스를 통해 내부 기업 네트워크에 있습니다.

  • Server Name(서버 이름) — ServerHostName과 같은 도메인 컨트롤러의 호스트 이름을 정의합니다.

- Timeout(시간 제한) — 서버로부터 응답을 기다리는 최대 시간(초)을 지정합니다. 10초가 기본값입니다.

- Kerberos 매개변수
  - Server Port(서버 포트) — 88은 KCD에 사용되는 기본 및 표준 포트입니다.
  - Retry Interval(재시도 간격) — 원하는 재시도 간격을 선택합니다. 10초가 기본 구성입니다.
  - Realm(영역) — DC의 도메인 이름을 모두 대문자로 입력합니다. ASA의 KCD 구성에서는 영역 값이 대문자여야 합니다. 영역은 인증 도메인입니다. 서비스는 동일한 영역에 있는 엔터티에서만 인증 자격 증명을 수락할 수 있습니다. 영역은 ASA가 조인한 도메인 이름과 일치해야 합니다.

단계 **3** **OK(**확인**)**를 클릭하여 구성을 적용한 후 원격 액세스 사용자 대신 서비스 티켓을 요청하도록 Microsoft KCD 서버를 구성합니다.

Microsoft Kerberos 요건

kcd-server 명령이 작동하려면 ASA가 소스 도메인(ASA가 있는 도메인)과 대상 또는 리소스 도메인(웹 서비스가 있는 도메인) 간의 신뢰 관계를 설정해야 합니다. 고유 형식을 사용하는 ASA는 소스에서 대상 도메인으로 인증 경로를 교차시키고 원격 액세스 사용자를 대신하여 서비스에 액세스하는 데 필요한 티켓을 획득합니다.

이러한 인증서 경로 교차를 교차 영역 인증이라고 합니다. 교차 영역 인증의 각 단계에서 ASA는 특정 도메인에 있는 크리덴셜 및 후속 도메인과의 신뢰 관계에 의존합니다.

외부 프록시 서버 사용 구성

Proxies(프록시) 창을 사용하여 ASA가 외부 프록시 서버를 사용하여 HTTP 요청 및 HTTPS 요청을 처리하도록 구성합니다. 이 서버는 사용자와 인터넷 사이에서 중개자 역할을 합니다. 사용자가 제어하는 서버를 통해 모든 인터넷 액세스를 요청하면 보안 인터넷 액세스와 관리 제어를 보장하도록 필터링할 수 있습니다.

참고 HTTP 및 HTTPS 프록시 서비스는 개인용 정보 단말기에 연결을 지원하지 않습니다.

프로시저

단계 **1** Use an HTTP Proxy Server(HTTP 프록시 서버 사용)를 클릭합니다.

단계 **2** 해당 IP 주소 또는 호스트 이름에 따라 HTTP 프록시 서버를 식별합니다.

단계 **3** 외부 HTTP 프록시 서버의 호스트 이름 또는 IP 주소를 입력합니다.

단계 **4** HTTP 요청을 수신 대기하는 포트를 입력합니다. 기본 포트는 80입니다.

단계 **5** (선택 사항) HTTPS 프록시 서버에 전송할 수 있는 대상에서 제외할 URL 또는 쉼표로 구분된 여러 URL의 목록을 입력합니다. 이 문자열은 길이 제한이 없지만, 전체 명령이 512자를 초과해서는 안 됩니다. 리터럴 URL을 지정하거나 다음 와일드카드를 사용할 수 있습니다.

- ***** 슬래시(/) 및 마침표(.)를 포함하여 임의의 문자열과 일치시킵니다. 이 와일드카드는 영숫자 문자열과 함께 사용해야 합니다.
- **?** 슬래시 및 마침표를 포함하여 모든 단일 문자와 일치합니다.
- [x-y] x~y 범위에 속한 임의의 단일 문자와 일치시킵니다. 여기서 x, y는 ANSI 문자 세트의 한 문자와 다른 문자를 각각 나타냅니다.
- [**!**x-y] 이 범위에 속하지 않는 임의의 단일 문자와 일치시킵니다.

단계 **6** (선택 사항) 기본적인 프록시 인증을 제공하기 위해 각 HTTPS 프록시 요청에 사용자 이름을 추가하려면 이 키워드를 입력합니다.

단계 **7** 각 HTTP 요청을 통해 프록시 서버로 전송할 비밀번호를 입력합니다.

단계 **8** HTTP 프록시 서버의 IP 주소를 지정하는 대신 Specify PAC File URL(PAC 파일 URL 지정)을 선택하여 프록시 자동 구성 파일을 브라우저에 다운로드하도록 지정할 수 있습니다. 일단 다운로드된 PAC 파일은 JavaScript 기능을 사용하여 각 URL에 대한 프록시를 식별합니다. **http://**를 입력하고 프록시 자동 구성 파일의 URL을 옆 필드에 입력합니다. **http://** 부분을 생략하는 경우 ASA는 이를 무시합니다.

단계 **9** HTTPS 프록시 서버 사용 여부를 선택합니다.

단계 **10** 해당 IP 주소 또는 호스트 이름에 따라 HTTPS 프록시 서버를 식별하려면 클릭합니다.

단계 **11** 외부 HTTPS 프록시 서버의 호스트 이름 또는 IP 주소를 입력합니다.

단계 **12** HTTPS 요청을 수신 대기하는 포트를 입력합니다. 기본 포트는 443입니다.

단계 **13** (선택 사항) HTTPS 프록시 서버에 전송할 수 있는 대상에서 제외할 URL 또는 쉼표로 구분된 여러 URL의 목록을 입력합니다. 이 문자열은 길이 제한이 없지만, 전체 명령이 512자를 초과해서는 안 됩니다. 리터럴 URL을 지정하거나 다음 와일드카드를 사용할 수 있습니다.

- ***** 슬래시(/) 및 마침표(.)를 포함하여 모든 문자열과 일치합니다. 이 와일드카드는 영숫자 문자열과 함께 사용해야 합니다.
- **?** 슬래시 및 마침표를 포함하여 모든 단일 문자와 일치합니다.
- [x-y]는 x~y 범위에 속한 임의의 단일 문자와 일치합니다. 여기서 x는 ANSI 문자 세트의 한 문자, y 역시 이 세트의 또 다른 문자를 나타냅니다.
- [**!**x-y]는 이 범위에 속하지 않는 단일 문자와 일치합니다.

단계 **14** (선택 사항) 기본 프록시 인증을 제공하기 위해 각 HTTPS 프록시 요청과 사용자 이름을 함께 사용하도록 키워드를 입력합니다.

단계 **15** 각 HTTPS 요청을 통해 프록시 서버로 전송할 비밀번호를 입력합니다.

클라이언트리스 SSL VPN 세션에 HTTPS 사용

HTTPS를 구성하는 것 외에도 프로토콜 다운그레이드 공격 및 쿠키 하이재킹로부터 웹사이트를 보호해 주는 웹 보안 정책 메커니즘인 HSTS(HTTP Strict-Transport-Security)를 활성화합니다. HSTS는 다음과 같은 지시문을 전송하여 지정된 시간 제한이 만료될 때까지 UA/브라우저를 HTTPS 웹사이트로 리디렉션하여 웹 서버로 안전하게 연결할 수 있도록 합니다.

```
Strict-Transport-Security: max-age="31536000"; preload;
```

여기서 각 항목은 다음을 나타냅니다.

- max-age(최대 기간) — 구성 가능한 항목으로, 웹 서버가 HSTS 호스트로 간주되어야 하는 시간(초)과 웹 서버가 HTTPS만 사용하여 안전하게 액세스되어야 하는 시간(초 단위)을 지정합니다. 기본값은 18주(10,886,400초)입니다. 범위는 8~365일(0~31,536,000 > 초)입니다.
- preload(사전 로드) — 브라우저에 UA/브라우저에 이미 등록되어 있는 도메인 목록을 로드하도록 지시하며 이제는 HSTS 호스트로 처리되어야 합니다. 사전 로드된 목록의 구현은 UA/브라우저에 종속되며 각 UA/브라우저는 다른 지시문 실행에 대한 추가 제한 사항을 지정할 수 있습니다. 예를 들어, Chrome의 사전 로드 목록은 HSTS의 최대 기간을 최소 18주(10,886,400초)가 되도록 지정합니다.

프로시저

단계 **1** **Configuration(**구성**) > Remote Access VPN(**원격 액세스 **VPN) > Clientless SSL VPN Access(**클라이언트리스 **SSL VPN** 액세스**) > Advanced(**고급**) > Proxies(**프록시**)**를 선택합니다.

단계 **2** **Enable HSTS(HSTS** 활성화**)**를 선택합니다.

단계 **3** HSTS가 유효한 시간(초)인 **HSTS Max Age(HSTS** 최대 기간**)**를 지정합니다.

이 값의 범위는 <0-31536000>초입니다. 기본값은 10,886,400(18주)입니다. 이 제한에 도달하면 HSTS가 더 이상 적용되지 않습니다.

HSTS가 유효한 시간(초 단위)의 양입니다. 이 값의 범위는 <0-31536000>초입니다. 기본값은 10,886,400(18주)입니다. 이 제한에 도달하면 HSTS가 더 이상 적용되지 않습니다.

애플리케이션 프로파일 사용자 지정 프레임워크 구성

클라이언트리스 SSL VPN에는 APCF(Application Profile Customization Framework) 옵션이 포함되어 있어 ASA가 비표준 애플리케이션 및 웹 리소스를 처리하여 클라이언트리스 SSL VPN 연결에 대해 정확하게 표시할 수 있습니다. APCF 프로파일에는 특정 애플리케이션을 언제(이전, 이후), 어디서(헤더, 본문, 요청, 응답), 무엇(데이터)에 대해 변형할지를 지정하는 스크립트가 포함되어 있습니다. 이 스크립트는 XML로 작성되며 sed(스트림 편집기) 구문을 사용하여 문자열/텍스트를 변형합니다.

ASA에서 동시에 여러 APCF 프로필을 구성하고 실행할 수 있습니다. APCF 프로파일 스크립트 내에서 여러 APCF 규칙을 적용할 수 있습니다. ASA는 가장 오래된 규칙을 구성 기록에 따라 먼저 처리한 후 그다음으로 가장 오래된 규칙을 처리합니다.

APCF 프로필을 ASA 플래시 메모리나 HTTP, HTTPS 또는 TFTP 서버에 저장할 수 있습니다.

반드시 Cisco 직원의 도움을 받아서 APCF 프로파일을 구성할 것을 권장합니다.

APCF 프로파일 관리

APCF 프로필을 ASA 플래시 메모리나 HTTP, HTTPS, FTP 또는 TFTP 서버에 저장할 수 있습니다. 이 창을 사용하여 APCF 패키지를 추가, 수정 및 삭제하고 우선 순위대로 배열합니다.

프로시저

단계 **1** Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > Clientless SSL VPN Access(클라이언트리스 SSL VPN 액세스) > Advanced(고급) > Application Helper(애플리케이션 도우미)로 이동하여 다음 기능을 수행할 수 있습니다.

- **Add/Edit(**추가/수정**)**을 클릭하여 새 APCF 프로파일을 생성하거나 기존 프로파일을 변경합니다.
  - **Flash file(**플래시 파일**)**을 선택하여 ASA 플래시 메모리에 저장된 APCF 파일을 찾습니다.

    그런 다음 **Upload(**업로드**)**를 클릭하여 APCF 파일을 로컬 컴퓨터에서 ASA 플래시 파일 시스템으로 가져오거나, 업로드하기 위해 Browse(찾아보기)를 클릭하여 플래시 메모리에 이미 있는 APCF 파일을 선택합니다.
  - HTTP, HTTPS, FTP 또는 TFTP 서버에서 APCF 파일을 검색하려면 URL을 선택합니다.
- 기존 APCF 프로파일을 제거하려면 **Delete(**삭제**)**를 클릭합니다. 확인 또는 실행 취소가 없습니다.
- 목록에서 APCF 프로파일을 다시 정렬하려면 **Move Up(**위로 이동**)** 또는 **Move Down(**아래로 이동**)**을 클릭합니다. 이 순서에 따라 어떤 APCF 프로파일이 사용되는지 결정됩니다.

단계 **2** 목록에서 변경한 내용이 표시되지 않으면 **Refresh(**새로 고침**)**를 클릭합니다.

APCF 패키지 업로드

프로시저

단계 **1** 컴퓨터에 APCF 파일의 경로가 표시됩니다. **Browse Local(**로컬 찾아보기**)**을 클릭하여 이 필드에 경로를 자동으로 삽입하거나 경로를 입력합니다.

단계 **2** 컴퓨터에서 전송할 APCF 파일을 찾고 선택하려면 클릭합니다. Select File Path(파일 경로 선택) 대화상자에 로컬 컴퓨터에서 마지막에 액세스한 폴더의 콘텐츠가 표시됩니다. APCF 파일로 이동하여 선

택한 다음 **Open(**열기**)**을 클릭합니다. ASDM은 Local File Path(로컬 파일 경로) 필드에 파일 경로를 삽입합니다.

단계 **3** APCF 파일을 업로드할 ASA의 경로는 Flash File System Path(플래시 파일 시스템 경로)에 표시됩니다. **Browse Flash(**플래시 찾아보기**)**를 클릭하여 APCF 파일을 업로드할 ASA상의 위치를 확인할 수 있습니다. Browse Flash(플래시 찾아보기) 대화 상자가 플래시 메모리의 콘텐츠를 표시합니다.

단계 **4** 로컬 컴퓨터에서 선택한 APCF 파일의 파일 이름이 표시됩니다. 혼란을 줄이기 위해 이 이름의 사용을 권장합니다. 이 파일이 정확한 파일 이름을 표시하는지 확인하고 **OK(**확인**)**를 클릭합니다. Browse Flash(플래시 찾아보기) 대화 상자가 닫힙니다. ASDM은 Flash File System Path(플래시 파일 시스템 경로) 필드에 대상 파일 경로를 삽입합니다.

단계 **5** 컴퓨터에서 APCF 파일의 위치 및 이 파일을 다운로드할 ASA상의 위치를 확인한 경우 **Upload File(**파일 업로드**)**을 클릭합니다.

단계 **6** Status(상태) 창이 나타나고 파일 전송 기간 동안 열려 있습니다. 전송 후 Information(정보) 창에 "파일이 플래시에 성공적으로 업로드되었습니다."라는 메시지가 표시됩니다. OK(확인)를 클릭합니다. 확인을 클릭합니다. Upload Image(이미지 업로드) 대화 창은 다른 파일을 업로드할 수 있음을 나타내는 Local File Path(로컬 파일 경로) 및 Flash File System Path(플래시 파일 시스템 경로) 필드의 콘텐츠를 제거합니다. 이러한 설정을 위해 본 지침을 반복하십시오. 그렇지 않으면 **Close(**닫기**)**를 클릭합니다.

단계 **7** Upload Image(이미지 업로드) 대화 창을 닫습니다. APCF 파일을 플래시 메모리에 업로드한 이후 또는 업로드하지 않기로 결정한 경우 **Close(**닫기**)**를 클릭합니다. 파일을 업로드하는 경우, APCF 창의 APCF File Location(APCF 파일 위치) 필드에 파일 이름이 나타납니다. 업로드하지 않을 경우, Close Message(메시지 닫기) 대화 상자에 "파일을 업로드하지 않고 대화를 닫으시겠습니까?"라는 확인 상자가 표시됩니다. 파일을 업로드하지 않으려면 **OK(**확인**)**를 클릭합니다. Close Message(메시지 닫기) 및 Upload Image(이미지 업로드) 대화 상자가 닫히고 APCF Add/Edit(APCF 추가/수정) 창이 나타납니다. 그렇지 않으면 메시지 닫기 대화 상자에서 **Cancel(**취소**)**을 클릭하십시오. 대화 상자가 닫히고 필드의 값이 그대로 유지된 상태에서 Upload Image(이미지 업로드) 대화 상자가 다시 표시됩니다. **Upload File(**파일 업로드**)**을 클릭합니다.

APCF 패킷 관리

프로시저

단계 **1** 다음 명령을 사용하여 APCF 패킷을 추가, 수정, 삭제하고 우선순위대로 배열합니다.

- **APCF** 파일 위치 — APCF 패키지 위치에 대한 정보를 표시합니다. ASA 플래시 메모리나 HTTP, HTTPS, FTP 또는 TFTP 서버에 있을 수 있습니다.
- **Add/Edit(**추가/수정**)** — 신규 또는 기존 APCF 프로필을 추가하거나 수정하려면 클릭합니다.
- **Delete(**삭제**)** — 기존 APCF 프로필을 제거하려면 클릭합니다. 확인 또는 실행 취소가 없습니다.
- **Move Up(**위로 이동**)** — 목록 내에서 APCF 프로필을 다시 정렬하려면 클릭합니다. 이 목록은 ASA가 APCF 프로필을 사용하려고 시도하는 순서를 결정합니다.

단계 **2** **Flash File(**플래시 파일**)**을 클릭하여 ASA 플래시 메모리에 저장된 APCF 파일의 위치를 찾습니다.

단계 **3** 플래시 메모리에 저장된 APCF 파일의 경로를 입력합니다. 이미 경로를 추가한 경우 이 경로를 찾은 다음, 플래시 메모리에 저장된 APCF 파일에 리디렉션합니다.

단계 **4** **Browse Flash(**플래시 찾아보기**)**를 클릭하여 플래시 메모리에서 APCF 파일을 찾습니다. Browse Flash(플래시 찾아보기) 대화 창이 표시됩니다. 폴더 및 파일 열을 사용하여 APCF 파일을 찾습니다. APCF 파일을 강조표시하고 **OK(**확인**)**를 클릭합니다. Path(경로) 필드에 파일 경로가 표시됩니다.

참고 최근에 다운로드한 APCF 파일의 이름이 표시되지 않으면 **Refresh(**새로 고침**)**를 클릭합니다.

- **Upload(**업로드**)** — 로컬 컴퓨터에서 ASA 플래시 파일 시스템에 APCF 파일을 업로드하려면 클릭합니다. Upload APCF Package(APCF 패키지 업로드) 창이 표시됩니다.
- URL — HTTP, HTTPS 또는 TFTP 서버에 저장된 APCF 파일을 사용하려면 클릭합니다.
- **ftp, http, https** 및 **tftp**(레이블 없음) — 서버 유형을 식별합니다.
- **URL**(레이블 없음) — FTP, HTTP, HTTPS 또는 TFTP 서버의 경로를 입력합니다.

APCF 구문

APCF 프로파일은 다음 표에 있는 XML 태그와 함께 XML 형식 및 sed 스크립트 구문을 사용합니다.

APCF용 지침

APCF 프로파일을 잘못 사용하면 성능이 저하되고 원하지 않는 콘텐츠가 렌더링될 수 있습니다. 대부분의 경우 Cisco Engineering에서 특정한 애플리케이션 렌더링 문제를 해결하도록 APCF 프로파일을 제공합니다.

표 ***8: APCF XML*** 태그

태그	사용 환경
<APCF>...</APCF>	모든 APCF XML 파일을 여는 필수 루트 요소입니다.
<version>1.0</version>	APCF 구현 버전을 지정하는 필수 태그입니다. 현재 고유한 버전은 1.0입니다.
<application>...</application>	XML 설명의 본문을 래핑하는 필수 태그입니다.
<id> text </id>	이 특정 APCF 기능에 대해 설명하는 필수 태그입니다.
<apcf-entities>...</apcf-entities>	단일 또는 다중 APCF 엔터티를 래핑하는 필수 태그입니다.

태그	사용 환경
<js-object>…</js-object> <html-object>…</html-object> <process-request-header>...</process-request-header> <process-response-header>...</process-response-header> <preprocess-response-body>...</preprocess-response-body> <postprocess-response-body>...</postprocess-response-body>	이 태그 중 하나는 APCF 처리가 발생해야 하는 콘텐츠 또는 단계의 유형을 지정합니다.
<conditions>… </conditions>	처리를 위해 기준을 지정하는 프로세스 이전/이후 태그의 하위 요소입니다. 예: • http-버전(예: 1.1, 1.0, 0.9) • http-메서드(get, put, post, webdav) • http-스키마(“http/”, “https/” 및 기타) • server-regexp("a".."z" | "A".."Z" | "0".."9" | ".-_*[]?"를 포함하는 정규식) • server-fnmatch("a".."z" | "A".."Z" | "0".."9" | ".-_*[]?+()\{},"를 포함하는 정규식) • user-agent-regexp • user-agent-fnmatch • request-uri-regexp • request-uri-fnmatch • 두 개 이상의 조건 태그가 있는 경우 ASA는 모든 태그에 대해 논리적 AND를 수행합니다.
<action> … </action>	지정된 조건에 해당하는 콘텐츠에서 수행할 작업을 하나 이상 래핑합니다. 다음 태그를 사용하여 이러한 작업을 정의할 수 있습니다(아래에 표시). • <do> • <sed-script> • <rewrite-header> • <add-header> • <delete-header>

태그	사용 환경
<do>…</do>	다음 작업 중 하나를 정의하는 데 사용되는 작업 태그의 하위 요소: • <no-rewrite/> — 원격 서버에서 수신한 콘텐츠를 바꾸지 마십시오. • <no-toolbar/> — 툴바를 삽입하지 마십시오. • <no-gzip/> — 콘텐츠를 압축하지 마십시오. • <force-cache/> — 원래 캐싱 지침을 준수하십시오. • <force-no-cache/> — 개체를 캐시 불가능 상태로 설정하십시오. • < downgrade-http-version-on-backend> — 원격 서버에 요청을 전송할 때 HTTP/1.0을 사용합니다.
<sed-script> TEXT </sed-script>	텍스트 기반 개체의 콘텐츠를 변경하는 데 사용되는 작업 태그의 하위 요소입니다. 이 텍스트는 유효한 Sed 스크립트여야 합니다. <sed-script>는 이전에 정의한 <conditions> 태그에 적용됩니다.
<rewrite-header></rewrite-header>	작업 태그의 하위 요소입니다. 아래에 표시된 하위 요소 <header> 태그에 지정된 HTTP 헤더의 값을 변경합니다.
<add-header></add-header>	아래에 표시된 하위 요소 <header> 태그에 지정된 새 HTTP 헤더를 추가하는 데 사용되는 액션 태그의 하위 요소입니다.
<delete-header></delete-header>	아래에 표시된 하위 요소 <header> 태그에서 지정된 HTTP 헤더를 삭제하는 데 사용되는 액션 태그의 하위 요소입니다.

<header></header>	재작성, 추가 또는 삭제할 이름 HTTP 헤더를 지정합니다. 예를 들어 다음 태그는 이름이 Connection인 HTTP 헤더의 값을 변경합니다.
	
	`<rewrite-header>`
	`<header>Connection</header>`
	`<value>close</value>`
	`</rewrite-header>`

APCF 구성 예

```
<APCF>
<version>1.0</version>
<application>
  <id>Do not compress content from example.com</id>
  <apcf-entities>
      <process-request-header>
         <conditions>
           <server-fnmatch>*.example.com</server-fnmatch>
         </conditions>
           <action>
             <do><no-gzip/></do>
           </action>
      </process-request-header>
  </apcf-entities>
</application>
</APCF>

<APCF>
<version>1.0</version>
<application>
 <id>Change MIME type for all .xyz objects</id>
 <apcf-entities>
      <process-response-header>
        <conditions>
            <request-uri-fnmatch>*.xyz</request-uri-fnmatch>
        </conditions>
         <action>
           <rewrite-header>
                <header>Content-Type</header>
                <value>text/html</value>
           </rewrite-header>
         </action>
      </process-response-header>
 </apcf-entities>
</application>
</APCF>
```

세션 설정 구성

클라이언트리스 SSL VPN에서 Add/Edit Internal Group Policy(내부 그룹 정책 추가/수정) > More Options(추가 옵션) > Session Settings(세션 설정) 창에서 클라이언트리스 SSL VPN 세션 간에 개인화된 사용자 정보를 지정할 수 있습니다. 기본적으로 각 그룹 정책은 기본 그룹 정책에서 설정을 상속받습니다. 이 창을 사용하여 기본 그룹 정책 및 값을 차별화할 모든 그룹 정책에 대해 개인화된 클라이언트리스 SSL VPN 사용자 정보를 지정하십시오.

프로시저

단계 **1** **none(**없음**)**을 클릭하거나 User Storage Location(사용자 스토리지 위치) 드롭다운 메뉴에서 파일 서버 프로토콜(smb 또는 ftp)을 선택합니다. Cisco에서는 사용자 스토리지로 CIFS를 사용할 것을 권장합니다. 사용자 이름/비밀번호 또는 포트 번호를 사용하지 않고 CIFS를 설정할 수 있습니다. CIFS를 선택할 경우 다음 구문을 입력합니다.

cifs//cifs-share/user/data

smb 또는 ftp를 선택할 경우 다음 구문을 사용하여 옆에 있는 텍스트 필드에 파일 시스템 대상을 입력합니다.

username:password@host:port-number/path

예를 들면 다음과 같습니다. **mike:mysecret@ftpserver3:2323/public**

참고 구성에는 사용자 이름, 비밀번호 및 사전 공유 키가 표시되지만 ASA는 데이터를 보호하기 위해 암호화된 형태로 데이터를 저장하는 내부 알고리즘을 사용합니다.

단계 **2** 필요할 경우 보안 어플라이언스에 대한 문자열을 입력하여 스토리지 위치에 대한 사용자 액세스를 제공합니다.

단계 **3** Storage Objects(저장 개체) 드롭다운 메뉴에서 다음 옵션 중 하나를 선택하여 서버가 사용자와의 연결에서 사용하는 개체를 지정합니다. ASA는 해당 개체를 저장하여 클라이언트리스 SSL VPN 연결을 지원합니다.

- 쿠키, 자격 증명
- 쿠키
- 자격 증명

단계 **4** 세션 시간 제한을 초과하는 트랜잭션 크기 제한(KB 단위)을 입력합니다. 이 특성은 단일 트랜잭션에만 적용됩니다. 이 값보다 큰 트랜잭션만 세션 만료 시간을 재설정합니다.

인코딩

문자 인코딩은 "문자 코딩" 및 "문자 집합"이라고도 하며 데이터를 표현하기 위한 원시 데이터(예: 0 및 1)와 문자의 쌍입니다. 언어는 사용할 문자 인코딩 방법을 결정합니다. 일부 언어에서는 단일 방법을 사용하지만 나머지는 그렇지 않습니다. 일반적으로 지리적 지역에 따라 브라우저가 사용하는 기본 인코딩 방법이 결정되지만 원격 사용자가 이 방법을 변경할 수 있습니다. 브라우저는 페이지에서 지정된 인코딩을 탐지할 수 있으며 이에 따라 문서를 렌더링합니다.

인코딩 특성을 사용하여 포털 페이지에서 사용되는 문자 인코딩 방법의 값을 지정하여 사용자가 브라우저를 사용하는 지역과 브라우저에 수행한 변경사항에 관계 없이 브라우저에서 이 값을 적절하게 렌더링하도록 할 수 있습니다.

기본적으로 ASA는 공통 인터넷 파일 시스템 서버의 페이지에 "전역 인코딩 유형"을 적용합니다. "전역 인코딩 유형" 특성에 따라 전역으로 그리고, 표에 표시된 파일 인코딩 예외에 따라 개별적으로 CIFS 서버를 해당하는 문자 인코딩에 매핑하면, 파일 이름, 디렉토리 경로 및 페이지를 적절하게 렌더링하는 것이 문제인 경우 CIFS 페이지를 정확하게 처리하여 표시할 수 있습니다.

문자 인코딩 확인 또는 지정

인코딩을 통해 클라이언트리스 SSL VPN 포털 페이지에 대해 문자 인코딩을 보거나 지정할 수 있습니다.

프로시저

단계 **1** 전역 인코딩 유형은 표에 나열된 CIFS 서버의 문자열 인코딩을 제외하고 모든 클라이언트리스 SSL VPN 포털 페이지가 상속 받을 문자열 인코딩을 결정합니다. 문자열을 입력하거나 다음과 같이 가장 일반적인 값을 포함하는 드롭다운 목록에서 옵션 중 하나를 선택할 수 있습니다.

- big5
- gb2312
- ibm-850
- iso-8859-1
- shift_jis
- unicode
- windows-1252
- 없음

참고 없음을 클릭하거나 클라이언트리스 SSL VPN 세션에 있는 브라우저가 지원하지 않는 값을 지정한 경우 고유한 기본 인코딩을 사용합니다.

최대 40개의 문자로 구성된 문자열을 입력할 수 있으며 이는 http://www.iana.org/assignments/character-sets에서 확인한 유효한 문자 집합 중 하나와 동일합니다. 이 페이지에 나열된 문자 집합의 이름 또는 별칭을 사용할 수 있습니다. 이 문자열은 대/소문자를 구분하지 않습니다. 명령 인터프리터는 ASA 구성을 저장할 때 대문자를 소문자로 변환합니다.

단계 **2** 인코딩 요건이 "전역 인코딩 유형" 특성 설정과 다른 CIFS 서버의 이름 또는 IP 주소를 입력합니다. ASA는 이름을 서버와 일치시킬 때는 대/소문자를 무시하지만 직접 지정한 대/소문자는 그대로 유지합니다.

단계 **3** CIFS 서버가 클라이언트리스 SSL VPN 포털 페이지에 제공해야 하는 문자 인코딩을 선택합니다. 문자열을 입력하거나 다음과 같이 가장 일반적인 값만 포함하는 드롭다운 목록에서 다음 중 하나를 선택할 수 있습니다.

- big5
- gb2312
- ibm-850
- iso-8859-1
- shift_jis

참고 일본어 Shift_jis 문자 인코딩을 사용 중인 경우 연결된 Select Page Font(페이지 글꼴 선택) 창의 Font Family(글꼴 패밀리) 영역에서 **Do Not Specify(**지정 안 함**)**를 클릭하여 글꼴 패밀리를 제거합니다.

- unicode
- windows-1252
- 없음

없음을 클릭하거나 클라이언트리스 SSL VPN 세션에 있는 브라우저가 지원하지 않는 값을 지정한 경우 고유한 기본 인코딩을 사용합니다.

최대 40개의 문자로 구성된 문자열을 입력할 수 있으며 이는 http://www.iana.org/assignments/character-sets에서 확인한 유효한 문자 집합 중 하나와 동일합니다. 이 페이지에 나열된 문자 집합의 이름 또는 별칭을 사용할 수 있습니다. 이 문자열은 대/소문자를 구분하지 않습니다. 명령어 인터프리터는 ASA 구성을 저장할 때 대문자를 소문자로 변환합니다.

콘텐츠 캐싱 구성

캐싱은 클라이언트리스 SSL VPN의 성능을 향상시킵니다. 이는 자주 재사용되는 개체를 시스템 캐시에 저장하여 콘텐츠의 재작성 및 압축 반복 작업을 줄이도록 해줍니다. 캐시를 사용하면 많은 애플리케이션이 더 효율적으로 실행되므로 트래픽이 줄어듭니다.

참고 콘텐츠 캐시를 활성화하면 일부 시스템의 안정성이 낮아질 수 있습니다. 콘텐츠 캐시를 활성화한 후에 임의 충돌이 발생하는 경우, 콘텐츠 캐시를 비활성화하십시오.

프로시저

단계 **1** Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > Clientless SSL VPN Access(클라이언트리스 SSL VPN 액세스) > Advanced(고급) > Content Cache(콘텐츠 캐시)를 선택합니다.

단계 **2** Enable Cache(캐시 활성화)가 선택되지 않은 경우 선택하십시오.

단계 **3** 캐싱 조건을 정의합니다.

- Maximum Object Size(최대 개체 크기) — ASA가 캐시할 수 있는 문서의 최대 크기(KB)를 입력합니다. ASA는 재작성되거나 압축된 콘텐츠가 아니라 개체의 원래 콘텐츠 길이를 측정합니다. 범위는 0부터 10,000KB까지이며 기본값은 1000KB입니다.
- Minimum Object Size(최소 개체 크기) — ASA가 캐시할 수 있는 문서의 최소 크기(KB)를 입력합니다. ASA는 재작성되거나 압축된 콘텐츠가 아니라 개체의 원래 콘텐츠 길이를 측정합니다. 범위는 0부터 10,000KB까지이며 기본값은 0KB입니다.

참고 최대 개체 크기는 최소 개체 크기보다 커야 합니다.

- Expiration Time(만료 시간) — 0부터 900 사이의 정수를 입력하여 재검증 없이 개체를 캐시하는 시간(분)을 설정합니다. 기본값은 1분입니다.
- LM Factor(LM 팩터) — 1부터 100 사이의 정수를 입력하며 기본값은 20입니다.
- LM 팩터는 최종 수정 타임스탬프만 있는 개체 캐싱에 대해 정책을 설정합니다. 이렇게 하면 server-set 변경 값이 없는 개체가 재검증됩니다. ASA는 개체가 변경된 이후의 시간(만료 시간이라고도 함)을 측정합니다. 예상 만료 시간은 마지막 변경 이후 경과한 시간 곱하기 LM 팩터의 값과 동일합니다. LM 팩터를 0으로 설정하면 재인증이 즉시 적용되며 100으로 설정하면 재인증할 때까지 최장 시간이 허용됩니다.
- 만료 시간은 마지막으로 수정된 타임스탬프도 없고 명시적인 서버 설정 만료 시간도 없는 개체를 ASA가 캐시하는 총 시간을 설정합니다.
- Cache static content(정적 콘텐츠 캐시) — PDF 파일 및 이미지와 같이 재작성할 수 없는 모든 콘텐츠를 캐시하려면 선택합니다.
- Restore Cache Default(캐시 기본값 복원) — 모든 캐시 매개변수에 대해 기본값을 복원하려면 클릭합니다.

콘텐츠 재작성

Content Rewrite(콘텐츠 재작성) 창에는 콘텐츠 재작성이 활성화 또는 꺼져 있는 모든 애플리케이션이 나열됩니다.

클라이언트리스 SSL VPN에서는 JavaScript, VBScript, Java 및 멀티바이트 문자 같은 고급 요소가 포함된 콘텐츠 변형/재작성 엔진을 통해 애플리케이션 트래픽을 처리하여 HTTP 트래픽을 프록시합니다. 이러한 HTTP 트래픽에는 사용자가 SSL VPN 디바이스 내에서 애플리케이션을 사용하는지 아니면 디바이스와 관계없이 애플리케이션을 사용하는지에 따라 여러 의미 체계와 액세스 제어 규칙이 포함될 수 있습니다.

기본적으로 보안 어플라이언스는 모든 클라이언트리스 트래픽을 재작성하거나 변형합니다. 일부 애플리케이션과 웹 리소스(예: 공공 웹사이트)가 ASA를 통과하는 것을 원치 않을 수도 있습니다. 따라서 ASA에서는 사용자가 ASA를 거치지 않고 특정 사이트 및 애플리케이션을 찾아볼 수 있도록 재작성 규칙을 생성할 수 있습니다. 이는 VPN 연결의 스플릿 터널링과 유사합니다.

참고 다음은 ASA 9.0의 Content Rewriter에서 개선된 사항입니다.

- 콘텐츠 재작성 기능이 HTML5를 지원하기 위해 추가되었습니다.
- 클라이언트리스 SSL VPN 재작성 엔진은 보다 우수한 품질 및 효율성을 제공하도록 개선되었습니다. 그 결과 클라이언트리스 SSL VPN 사용자에게 더 나은 엔드 유저 경험을 제공할 수 있게 되었습니다.

재작성 규칙 생성

여러 재작성 규칙을 생성할 수 있습니다. 보안 어플라이언스는 가장 작은 수부터 지정된 순서에 따라 재작성 규칙을 검색하고 일치하는 첫 번째 규칙을 적용하므로 규칙 번호가 매우 중요합니다.

Content Rewrite(콘텐츠 재작성) 표에는 다음과 같은 열이 있습니다.

- Rule Number(규칙 번호) - 목록에서 규칙의 위치를 나타내는 정수를 표시합니다.
- Rule Name(규칙 이름) - 규칙이 적용될 애플리케이션 이름을 제공합니다.
- Rewrite Enabled(재작성 활성화) - 콘텐츠 재작성이 활성화 또는 꺼진 것으로 표시합니다.
- Resource Mask(리소스 마스크) - 리소스 마스크를 표시합니다.

프로시저

단계 **1** Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > Clientless SSL VPN Access(클라이언트리스 SSL VPN 액세스) > Advanced(고급) > Content Rewrite(콘텐츠 재작성)로 이동합니다.

단계 **2** 콘텐츠 재작성 규칙을 생성 또는 업데이트하려면 Add(추가) 또는 Edit(수정)를 클릭합니다.

단계 **3** 이 규칙을 활성화하려면 **Enable content rewrite(**콘텐츠 재작성 활성화**)**를 선택합니다.

단계 **4** 이 규칙의 번호를 입력합니다. 이 번호는 목록의 다른 규칙과 관련된 규칙의 우선 순위를 지정합니다. 번호가 없는 규칙은 목록의 끝 부분에 있습니다. 범위는 1에서 65534까지입니다.

단계 **5** (선택 사항) 규칙을 설명하는 영숫자 문자열(최대 128자)을 입력합니다.

단계 **6** 규칙을 적용할 애플리케이션 또는 리소스와 일치하도록 문자열을 입력합니다. 문자열은 최대 300자까지 가능합니다. 다음 와일드카드 중 하나를 사용할 수 있지만 최소 1개의 영숫자 문자를 지정해야 합니다.

- * — 모든 것과 일치합니다. ASDM은 * 또는 *.*로 구성된 마스크를 허용하지 않습니다.
- ? — 하나의 문자와 일치합니다.
- [!seq] — 시퀀스에 있지 않은 문자와 일치합니다.
- [seq] — 시퀀스에 있는 문자와 일치합니다.

콘텐츠 재작성 규칙의 구성 예

표 *9:* 콘텐츠 재작성 규칙

기능	콘텐츠 재작성 활성화	규칙 번호	규칙 이름	리소스 마스크
youtube.com에서 HTTP URL에 대해 재작성 기능 끄기	선택 취소됨	1	no-rewrite-youtube	*.youtube.com/*
위의 규칙과 일치하지 않는 모든 HTTP URL에 대해 재작성 기능 활성화	수표	65,535	rewrite-all	*

클라이언트리스 **SSL VPN**을 통한 이메일 사용

웹 이메일 구성: **MS Outlook Web App**

ASA는 Exchange Server 2010에 대해 Microsoft Outlook Web App을 지원하고 Exchange Server 2007, 2003 및 2000에 대해 Microsoft Outlook Web Access를 지원합니다.

프로시저

단계 **1** 이메일 서비스 URL을 주소 필드에 입력하거나 클라이언트리스 SSL VPN 세션에서 연결된 책갈피를 클릭합니다.

단계 **2** 확인 상자가 표시되면 도메인\사용자 이름 형식으로 이메일 서버 사용자 이름을 입력합니다.

단계 **3** 이메일 비밀번호를 입력합니다.

책갈피 구성

Bookmarks(책갈피) 패널에서는 책갈피 목록을 추가, 수정, 삭제, 가져오기 및 내보내기할 수 있습니다.

Bookmarks(책갈피) 패널을 사용하여 클라이언트리스 SSL VPN을 통한 액세스를 위해 서버 및 URL 목록을 구성합니다. 책갈피 목록의 구성에 따라 하나 이상의 정책(예: 그룹 정책, 동적 액세스 정책 또는 두 가지 모두)에 목록을 할당할 수 있습니다. 각 정책에는 1개의 책갈피 목록만 있을 수 있습니다. 목록 이름은 각 DAP의 URL Lists(URL 목록) 탭에 있는 드롭다운 목록에 채워집니다.

이제 일부 웹 페이지에서 자동 로그온에 대한 매크로 대체와 함께 책갈피를 사용할 수 있습니다. 이전 POST 플러그인 접근 방식은 관리자가 로그인 매크로를 사용하여 POST 책갈피를 지정하고 POST 요청을 게시하기 전에 로드하기 위해 시작 페이지를 수신하도록 생성되었습니다. 이러한 POST 플러그인 접근 방식에서는 요청 시 쿠키 또는 다른 헤더 항목이 필요하지 않습니다. 관리자는 사후 로그인 요청이 전송되는 위치를 지정하는 사전 로드 페이지 및 URL을 결정합니다. 사전 로드 페이지에서는 엔드포인트 브라우저를 자격 증명이 있는 POST 요청을 사용하는 대신 웹 서버 또는 웹 애플리케이션에 따라 전송되는 특정 정보를 가져오도록 할 수 있습니다.

기존 책갈피 목록이 표시됩니다. 책갈피 목록을 추가, 수정, 삭제, 가져오기 또는 내보내기할 수 있습니다. 액세스를 위해 서버 목록 및 URL을 구성하고 지정한 URL 목록에서 항목의 순서를 지정할 수 있습니다.

시작하기 전에

책갈피를 구성해도 사용자가 회사의 사용 정책을 위반하는 사기 사이트에 방문하는 것을 차단할 수는 없습니다. 그룹 정책, 동적 액세스 정책 또는 두 가지 모두에 책갈피 목록을 할당하는 것 외에도 트래픽 흐름에 대한 액세스 제어를 위해 이 정책에 웹 ACL을 적용하십시오. 이러한 정책에서 URL 항목을 끄면 액세스 가능한 항목에 대한 혼란을 방지할 수 있습니다.

프로시저

단계 **1** 추가할 목록의 이름을 지정하거나 수정 또는 삭제할 목록의 이름을 선택합니다.

책갈피 제목 및 실제 관련 URL이 표시됩니다.

단계 **2** (선택 사항) **Add(**추가**)**를 클릭하여 새 서버 또는 URL을 구성합니다. 다음 중 하나를 추가할 수 있습니다.

- GET 또는 Post 메서드를 사용하여 URL에 대한 책갈피 추가
- 사전 정의된 애플리케이션 템플릿에 대한 URL 추가
- 자동 로그온 애플리케이션에 대한 책갈피 추가

단계 **3** (선택 사항) **Edit(**수정**)**을 클릭하여 서버, URL 또는 표시 이름을 변경합니다.

단계 **4** (선택 사항) **Delete(**삭제**)**를 클릭하여 URL 목록에서 선택한 항목을 제거합니다. 확인 또는 실행 취소가 없습니다.

단계 **5** (선택 사항) 파일을 가져오거나 내보낼 위치를 선택합니다.

- Local computer(로컬 컴퓨터) — 로컬 PC에 있는 파일을 가져오거나 내보내려면 클릭합니다.
- Flash file system(플래시 파일 시스템) — ASA에 있는 파일을 가져오거나 내보내려면 클릭합니다.
- Remote server(원격 서버) — ASA에서 액세스할 수 있는 원격 서버에 있는 파일을 가져오려면 클릭합니다.
- Path(경로) — 파일(ftp, http 또는 https)에 액세스하는 방법을 식별하고 파일에 대한 경로를 제공합니다.

- Browse Local Files/Browse Flash...(로컬 파일 찾아보기/플래시 찾아보기) - 파일의 경로를 찾습니다.

단계 **6** (선택 사항) 책갈피를 강조 표시하고 **Assign(**할당**)**을 클릭하여 하나 이상의 그룹 정책, 동적 액세스 정책 또는 로컬 사용자에게 선택한 책갈피를 할당합니다.

단계 **7** (선택 사항) **Move Up(**위로 이동**)** 또는 **Move Down(**아래로 이동**)** 옵션을 사용하여 URL 목록에서 선택한 항목의 위치를 변경합니다.

단계 **8** OK(확인)를 클릭합니다.

다음에 수행할 작업

클라이언트리스 SSL VPN 보안 예방 조치에 대해 알아보십시오.

GET 또는 Post 메서드를 사용하여 URL에 대한 책갈피 추가

Add Bookmark Entry(책갈피 항목 추가) 대화 상자를 사용하여 URL 목록에 대한 링크 또는 책갈피를 생성할 수 있습니다.

시작하기 전에

네트워크의 공유 폴더에 액세스하려면 \\server\share\subfolder\<personal folder> 형식을 사용합니다. 사용자는 <personal folder> 위에 있는 모든 지점에 대한 권한을 나열해야 합니다.

프로시저

단계 **1** **Configuration(**구성**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **Clientless SSL VPN Access(**클라이언트리스 **SSL VPN** 액세스**)** > **Portal(**포털**)** > **Bookmarks(**책갈피**)**로 이동하고 **Add(**추가**)** 버튼을 클릭합니다.

단계 **2** 책갈피 생성에 사용할 **URL with GET or POST Method(GET** 또는 **POST** 메서드를 사용하는 **URL)**를 선택합니다.

단계 **3** 포털에 표시할 이 책갈피의 이름을 입력합니다.

단계 **4** URL 유형인 http, https, cifs 또는 ftp를 선택할 수 있는 URL 드롭다운 메뉴를 사용합니다. URL 드롭다운 목록에 설치한 모든 플러그인에 대한 유형 외에 표준 URL 유형이 표시됩니다.

단계 **5** 이 책갈피(URL)의 DNS 이름 또는 IP 주소를 입력합니다. 플러그인에 대해 서버의 이름을 입력합니다. 선택적 매개변수를 지정하려면 서버 이름 뒤에 슬래시 및 물음표 (/?)를 입력한 다음 아래 구문과 같이 매개변수 값 쌍을 구분하기 위해 앰퍼샌드를 사용합니다.

server/**?***Parameter***=***Value***&***Parameter***=***Value*

예제**:**

특정 플러그인은 입력할 수 있는 선택적 파라미터 값 쌍을 결정합니다.

host/**?DesiredColor=4&DesiredHRes=1024&DesiredVRes=768**

플러그인에 대해 SSO(Single Sign-On)을 지원하려면 파라미터 값 쌍인 **csco_sso=1**을 사용합니다.

host/**?csco_sso=1&DesiredColor=4&DesiredHRes=1024&DesiredVRes=768**

단계 **6** (선택 사항) 사전 로드 URL을 입력합니다. 사전 로드 URL을 입력할 때 실제 POST URL에 전달될 때까지 페이지 로드에 허용되는 대기 시간을 입력할 수 있습니다.

단계 **7** 부제목으로 사용자가 볼 수 있으며 책갈피 항목에 대해 설명하는 추가 텍스트를 입력합니다.

단계 **8** Thumbnail(썸네일) 드롭다운 메뉴를 사용하여 엔드 유저 포털에 있는 책갈피와 연결할 아이콘을 선택합니다.

단계 **9** 썸네일로 사용할 이미지를 가져오거나 내보내려면 **Manage(**관리**)**를 클릭합니다.

단계 **10** ASA를 통해서 대상 서버와 데이터를 주고받기 위해 스마트 터널 기능을 사용하는 책갈피를 새 창에서 열려면 클릭합니다. 모든 브라우저 트래픽을 SSL VPN 터널을 통해 안전하게 전달합니다. 이 옵션을 통해 브라우저 기반 애플리케이션에 대한 스마트 터널 지원을 제공하는 반면 Clientless SSL VPN(클라이언트리스 SSL VPN) > Portal(포털) 메뉴에서 Smart Tunnels(스마트 터널 옵션)을 사용하여 비 브라우저 기반 애플리케이션을 그룹 정책 및 사용자 이름에 할당하도록 스마트 터널 목록에 추가할 수 있습니다.

단계 **11** **Allow the Users to Bookmark the Link(**사용자에게 링크 책갈피 허용**)**를 선택하면 클라이언트리스 SSL VPN 사용자가 브라우저에서 Bookmarks(책갈피) 또는 Favorites(즐겨찾기) 옵션을 사용할 수 있습니다. 이러한 옵션에 대한 액세스를 방지하려면 선택을 취소합니다. 이 옵션을 선택하지 않은 경우 책갈피는 클라이언트리스 SSL VPN 포털의 홈 섹션에 표시되지 않습니다.

단계 **12** (선택 사항) **Advanced Options(**고급 옵션**)**를 선택하여 책갈피 특성을 추가로 구성합니다.

- URL Method(URL 메서드) - 간단한 데이터 검색을 수행하려면 **Get(**가져오기**)**을 선택합니다. 데이터 처리에 데이터 저장이나 업데이트, 제품 주문 또는 이메일 전송과 같은 변경사항이 포함되는 경우 **Post(**게시**)**를 선택합니다.
- Post Parameters(게시 매개변수) — Post URL 메서드의 세부 사항을 구성합니다.

사전 정의된 애플리케이션 템플릿에 대한 **URL** 추가

잘 정의된 특정한 애플리케이션에 대해 미리 채워진 필수 값을 포함하는 사전 정의 ASDM 템플릿을 사용자가 선택하여 이 옵션을 통해 책갈피 생성을 간단하게 수행할 수 있습니다.

시작하기 전에

사전 정의된 애플리케이션 템플릿은 현재 다음 애플리케이션에만 사용할 수 있습니다.

- Citrix XenApp
- Citrix XenDesktop
- Domino WebAccess
- Microsoft Outlook Web Access 2010
- Microsoft Sharepoint 2007

- Microsoft SharePoint 2010
- Microsoft SharePoint 2013

프로시저

단계 **1** 책갈피에서 사용자에게 표시될 이름을 입력합니다.

단계 **2** 부제목으로 사용자가 볼 수 있으며 책갈피 항목에 대해 설명하는 추가 텍스트를 입력합니다.

단계 **3** Thumbnail(썸네일) 드롭다운 메뉴를 사용하여 엔드 유저 포털에 있는 책갈피와 연결할 아이콘을 선택합니다.

단계 **4** 썸네일로 사용할 이미지를 가져오거나 내보내려면 **Manage(**관리**)**를 클릭합니다.

단계 **5** (선택 사항) Place This Bookmark on the VPN Home Page(이 북마크를 VPN 홈 페이지에 저장) 체크 박스를 선택합니다.

단계 **6** Select Auto Sign-on Application(자동 로그인 애플리케이션 선택) 목록에서 필요한 애플리케이션을 클릭합니다. 사용 가능한 애플리케이션은 다음과 같습니다.

- Citrix XenApp
- Citrix XenDesktop
- Domino WebAccess
- Microsoft Outlook Web Access 2010
- Microsoft Sharepoint 2007
- Microsoft SharePoint 2010
- Microsoft SharePoint 2013

단계 **7** 로그인 페이지로 넘어가기 전에 로드되는 페이지의 URL을 입력합니다. 이 페이지에서 로그인 화면으로 넘어가려면 사용자 상호 작용이 필요합니다. URL에 *를 사용하여 임의의 기호 수를 대체할 수 있습니다(예: http*://www.example.com/test).

단계 **8** Pre-login Page Control ID(로그인 전 페이지 제어 ID)를 입력합니다. 로그인 페이지로 이동하기 위해 로그인 전 페이지 URL의 클릭 이벤트를 가져오는 제어/태그의 ID입니다.

단계 **9** Application Parameters(애플리케이션 매개변수)를 입력합니다. 애플리케이션에 따라 다음이 포함될 수 있습니다.

- 프로토콜. HTTP 또는 HTTPS.
- 호스트 이름. 예: www.cisco.com
- Port Number(포트 번호). 애플리케이션에서 사용하는 포트입니다.
- URL Path Appendix(URL 경로 부록). 예: /Citrix/XenApp. 이 메시지는 일반적으로 자동으로 채워집니다.
- Domain(도메인). 연결할 도메인입니다.

- 사용자 이름. 사용자 이름으로 사용할 SSL VPN 변수입니다. 여러 변수를 선택하려면 Select Variable(변수 선택)을 클릭합니다.
- 비밀번호. 비밀번호로 사용할 SSL VPN 변수입니다. 여러 변수를 선택하려면 Select Variable(변수 선택)을 클릭합니다.

단계 **10** (선택 사항) 템플릿 출력을 미리 보려면 **Preview(**미리보기**)**를 클릭합니다. 템플릿을 수정하려면 Edit(수정)를 클릭할 수 있습니다.

단계 **11** 변경하려면 **OK(**확인**)**를 클릭합니다. 또는 변경을 취소하려면 Cancel(취소)을 클릭합니다.

자동 로그온 애플리케이션에 대한 책갈피 추가

이 옵션을 사용하여 복잡한 자동 로그온 애플리케이션에 대해 책갈피를 생성할 수 있습니다.

자동 로그온 애플리케이션을 구성하려면 2단계를 수행해야 합니다.

1. POST 매개변수 없이 일부 기본적인 초기 데이터를 사용하여 책갈피를 정의합니다. 사용자 또는 그룹 정책에서 사용하도록 책갈피를 저장하고 할당합니다.
2. 책갈피를 다시 수정합니다. 캡처 기능을 사용하여 SSL VPN 매개변수를 캡처하고 책갈피에서 수정합니다.

프로시저

단계 **1** 책갈피에서 사용자에게 표시될 이름을 입력합니다.

단계 **2** URL 유형인 http, https, cifs 또는 ftp를 선택할 수 있는 URL 드롭다운 메뉴를 사용합니다. 모든 가져온 플러그인의 URL 유형이 이 메뉴에 채워집니다. 포털 페이지에 있는 링크로 플러그인을 표시하려면 플러그인 URL 유형을 선택합니다.

단계 **3** 책갈피용으로 DNS 이름 또는 IP 주소를 입력합니다. 플러그인에 대해 서버의 이름을 입력합니다. 선택적 매개변수를 지정하려면 서버 이름 뒤에 슬래시 및 물음표 (/?)를 입력한 다음 아래 구문과 같이 매개변수 값 쌍을 구분하기 위해 앰퍼샌드를 사용합니다.

server/**?***Parameter*=*Value*&*Parameter*=*Value*

예제**:**

예를 들어, 특정 플러그인은 입력할 수 있는 선택적 파라미터 값 쌍을 결정합니다.

*host***/?DesiredColor=4&DesiredHRes=1024&DesiredVRes=768**

플러그인을 지원하기 위해 단일 로그인을 제공하려면 매개변수 값 쌍인 **csco_sso=1**을 사용합니다.

host**/?csco_sso=1&DesiredColor=4&DesiredHRes=1024&DesiredVRes=768**

단계 **4** 부제목으로 사용자가 볼 수 있으며 책갈피 항목에 대해 설명하는 추가 텍스트를 입력합니다.

단계 **5** Thumbnail(썸네일) 드롭다운 메뉴를 사용하여 엔드 유저 포털에 있는 책갈피와 연결할 아이콘을 선택합니다.

단계 **6** 썸네일로 사용할 이미지를 가져오거나 내보내려면 **Manage(**관리**)**를 클릭합니다.

단계 **7** (선택 사항) Place This Bookmark on the VPN Home Page(이 책갈피를 VPN 홈 페이지에 배치) 확인란을 선택합니다.

단계 **8** Login Page URL(로그인 페이지 URL)을 입력합니다. 와일드카드를 입력하는 URL에 사용할 수 있습니다. 예를 들어 http*://www.example.com/myurl*를 입력할 수 있습니다.

단계 **9** Landing Page URL(랜딩 페이지 URL)을 입력합니다. ASA에서는 애플리케이션에 대한 성공적인 로그인을 탐지하도록 랜딩 페이지를 구성해야 합니다.

단계 **10** (선택 사항) POST 스크립트를 입력합니다. 일부 웹 애플리케이션(예: Microsoft Outlook Web Access)은 로그온 양식을 제출하기 전에 요청 매개변수를 변경하기 위해 JavaScript를 실행할 수 있습니다. Post Script(사후 스크립트) 필드에서는 해당 애플리케이션에 대해 JavaScript를 입력할 수 있습니다.

단계 **11** 필요한 Form Parameters(양식 매개변수)를 추가합니다. 필요한 각 SSL VPN 변수의 경우 Add(추가)를 클릭하고 Name(이름)을 입력하며 목록에서 해당 변수를 선택합니다. 매개변수를 변경하려면 Edit(수정)를 클릭하고 제거하려면 Delete(삭제)를 클릭할 수 있습니다.

단계 **12** 로그인 페이지로 넘어가기 전에 로드되는 페이지의 URL을 입력합니다. 이 페이지에서 로그인 화면으로 넘어가려면 사용자 상호 작용이 필요합니다. URL에 *를 사용하여 임의의 기호 수를 대체할 수 있습니다(예: http*://www.example.com/test).

단계 **13** Pre-login Page Control ID(로그인 전 페이지 제어 ID)를 입력합니다. 로그인 페이지로 이동하기 위해 로그인 전 페이지 URL의 클릭 이벤트를 가져오는 제어/태그의 ID입니다.

단계 **14** 변경하려면 OK(확인)를 클릭합니다. 또는 변경을 취소하려면 Cancel(취소)을 클릭합니다.

향후 작업

다음에 수행할 작업

책갈피를 수정할 경우 HTML 매개변수 캡처 기능을 사용하여 VPN 자동 로그온 매개변수를 캡처할 수 있습니다. 그룹 정책 또는 사용자에게 먼저 책갈피를 저장하고 할당해야 합니다.

SSL VPN Username(SSL VPN 사용자 이름)을 입력한 다음 Start Capture(캡처 시작)를 클릭합니다. 그런 다음 웹 브라우저를 사용하여 VPN 세션을 시작하고 인트라넷 페이지로 이동합니다. 프로세스를 완료하려면 **Stop Capture(**캡처 중지**)**를 클릭합니다. 매개변수는 수정 시 사용할 수 있으며 책갈피에 삽입됩니다.

책갈피 목록 가져오기 및 내보내기

이미 구성된 책갈피 목록을 가져오거나 내보낼 수 있습니다. 사용할 수 있는 목록을 가져옵니다. 수정하려면 목록을 내보낸 다음 다시 가져옵니다.

프로시저

단계 **1** 이름으로 책갈피 목록을 식별합니다. 최대값은 64자이며 공백은 포함하지 않습니다.

단계 **2** 목록 파일을 가져오거나 내보낼 방법을 다음 중에서 선택합니다.

- Local computer(로컬 컴퓨터) — 로컬 PC에 있는 파일을 가져오려면 클릭합니다.
- Flash file system(플래시 파일 시스템) — ASA에 있는 파일을 내보내려면 클릭합니다.
- Remote server(원격 서버) — ASA에서 액세스할 수 있는 원격 서버에 있는 URL 목록 파일을 가져오려면 클릭합니다.
- Path(경로) — 파일(ftp, http 또는 https)에 액세스하는 방법을 식별하고 파일에 대한 경로를 제공합니다.
- Browse Local Files/Browse Flash(로컬 파일 찾아보기/플래시 찾아보기) - 파일의 경로를 찾습니다.
- Import/Export Now(지금 가져오기/내보내기) — 목록 파일을 가져오거나 내보내려면 클릭합니다.

GUI 사용자 지정 개체**(**웹 콘텐츠**)** 가져오기 및 내보내기

이 대화 상자를 사용하여 웹 콘텐츠 개체를 가져오기 및 내보내기할 수 있습니다. 웹 콘텐츠 개체의 이름과 해당 파일 유형이 표시됩니다.

웹 콘텐츠는 전체가 구성된 홈 페이지에서 엔드 유저 포털을 사용자 지정할 때 사용하는 아이콘 또는 이미지에 이르기까지 다양합니다. 이미 구성된 웹 콘텐츠를 가져오거나 내보내고 즉시 사용 가능한 웹 콘텐츠를 가져올 수 있습니다. 웹 콘텐츠를 내보내서 수정한 후 다시 가져옵니다.

프로시저

단계 **1** 파일을 가져오거나 내보낼 위치를 선택합니다.

- Local computer(로컬 컴퓨터) — 로컬 PC에 있는 파일을 가져오거나 내보내려면 클릭합니다.
- Flash file system(플래시 파일 시스템) — ASA에 있는 파일을 가져오거나 내보내려면 클릭합니다.
- Remote server(원격 서버) — ASA에서 액세스할 수 있는 원격 서버에 있는 파일을 가져오려면 클릭합니다.
- Path(경로) — 파일(ftp, http 또는 https)에 액세스하는 방법을 식별하고 파일에 대한 경로를 제공합니다.
- Browse Local Files.../Browse Flash...(로컬 파일 찾아보기.../플래시 찾아보기...) - 파일의 경로를 찾습니다.

단계 **2** 콘텐츠에 액세스하는 데 인증이 필요한지를 결정합니다.

경로의 접두사는 인증 필요 여부에 따라 달라집니다. ASA는 인증이 필요한 개체에 /+CSCOE+/를 사용하고 인증이 필요하지 않은 개체에 /+CSCOU+/를 사용합니다. ASA는 포털 페이지에서만 /+CSCOU+/

개체를 표시하는 반면, /+CSCOE+/ 개체는 로그인 시 또는 포털 페이지에서 표시되거나 사용할 수 있습니다.

단계 **3** 파일을 가져오거나 내보내려면 클릭합니다.

POST 파라미터 추가 및 수정

책갈피 항목 및 URL 목록에 대해 게시 매개변수를 구성하려면 이 창을 사용합니다.

클라이언트리스 SSL VPN 변수는 URL 및 양식 기반 HTTP 게시 작업에서 대체에 사용할 수 있습니다. 매크로라고도 알려진 변수를 통해 사용자 ID 및 비밀번호 또는 기타 입력 매개변수를 포함하는 개인화된 리소스에 액세스하도록 사용자를 구성할 수 있습니다. 이러한 리소스의 예로는 책갈피 항목, URL 목록 및 파일 공유가 있습니다.

프로시저

단계 **1** 해당 HTML 양식과 마찬가지로, 매개변수의 이름과 값을 정확하게 입력합니다. 예를 들면 다음과 같습니다.

<input name="*param_name*" value="*param_value*">

드롭다운 목록에서 제공한 변수 중 하나를 선택하거나 변수를 구성할 수 있습니다. 드롭다운 목록에서 선택할 수 있는 변수는 다음과 같습니다.

표 ***10:*** 클라이언트리스 ***SSL VPN*** 변수

번호	변수 대체	정의
1	CSCO_WEBVPN_USERNAME	SSL VPN 사용자 로그인 ID입니다.
2	CSCO_WEBVPN_PASSWORD	SSL VPN 사용자 로그인 비밀번호입니다.
3	CSCO_WEBVPN_INTERNAL_PASSWORD	SSL VPN 사용자 내부 리소스 비밀번호입니다. 캐시된 자격 증명이며 AAA 서버에서 인증되지 않습니다. 사용자가 이 값을 입력할 경우 비밀번호 값 대신 자동 로그온에 대한 비밀번호로 사용됩니다.
4	CSCO_WEBVPN_CONNECTION_PROFILE	연결 프로파일 내에 있는 SSL VPN 사용자 로그인 그룹 드롭다운, 그룹 별칭입니다.

번호	변수 대체	정의
5	CSCO_WEBVPN_MACRO1	RADIUS/LDAP 공급업체별 특성을 통해 설정합니다. ldap-attribute-map을 통해 LDAP에서 매핑한 경우 해당 변수를 사용하는 Cisco 특성은 WEBVPN-Macro-Substitution-Value1입니다. RADIUS를 통한 변수 교체는 VSA#223에서 수행됩니다.
6	CSCO_WEBVPN_MACRO2	RADIUS/LDAP 공급업체별 특성을 통해 설정합니다. ldap-attribute-map을 통해 LDAP에서 매핑한 경우 해당 변수를 사용하는 Cisco 특성은 WEBVPN-Macro-Substitution-Value2입니다. RADIUS를 통한 변수 교체는 VSA#224에서 수행됩니다.
7	CSCO_WEBVPN_PRIMARY_USERNAME	이중 인증용 기본 사용자 로그인 ID입니다.
8	CSCO_WEBVPN_PRIMARY_PASSWORD	이중 인증용 기본 사용자 로그인 비밀번호입니다.
9	CSCO_WEBVPN_SECONDARY_USERNAME	이중 인증용 보조 사용자 로그인 비밀번호입니다.
10	CSCO_WEBVPN_SECONDARY_PASSWORD	이중 인증용 보조 사용자 로그인 비밀번호입니다.
11	CSCO_WEBVPN_DYNAMIC_URL	사용자의 포털에서 다중 북마크링크를 생성할 수 있는 단일 북마크입니다.
12	CSCO_WEBVPN_MACROLIST	LDAP 속성 맵에서 제공하는 임의 크기의 목록을 사용할 수 있는 고정으로 구성된 북마크입니다.

ASA가 엔드 유저 요청(북마크 또는 POST 양식)에서 6개의 변수 문자열 중 하나를 인식하는 경우 해당 요청을 원격 서버에 전달하기 전에 이를 사용자 특정 값으로 바꿉니다.

참고 보안 어플라이언스 개입 없이 HTTP 스니퍼 추적을 수행하여 모든 애플리케이션에 대한 http-post 매개변수를 얻을 수 있습니다. http://www.ieinspector.com/httpanalyzer/downloadV2/IEHttpAnalyzerV2.exe 링크에서 HTTP 분석기라고 하는 브라우저 캡처 툴을 무료로 얻을 수 있습니다.

단계 **2** 다음 지침을 통해 해당 변수를 선택합니다.

- 변수 1~4 사용 — ASA는 사용자 이름, 비밀번호, 내부 비밀번호(선택 사항) 및 그룹에 대한 필드가 포함된 SSL VPN 로그인 페이지에서 처음 4개의 대체 값을 가져옵니다. 사용자 요청에서 이 문자열을 인식하고 원격 서버에 요청을 전달하기 전에 사용자에게 특정한 값으로 이 문자열을 대체합니다.

  ```
  For example, if a URL list contains the link,
  http://someserver/homepage/CSCO_WEBVPN_USERNAME.html, the ASA translates it to the
  following unique links:

  For USER1, the link becomes http://someserver/homepage/USER1.html

  For USER2, the link is http://someserver/homepage/USER2.html

  In the following case, cifs://server/users/CSCO_WEBVPN_USERNAME lets the ASA map a file
   drive to specific users:
  For USER1, the link becomes cifs://server/users/USER1
  For USER 2, the link is cifs://server/users/USER2
  ```

- 변수 5~6 사용 - 매크로 5 및 6의 값은 RADIUS 또는 LDAP VSA(Vendor-Specific Attributes)입니다. 이 값을 사용하여 RADIUS 또는 LDAP 서버에 구성된 대체를 설정할 수 있습니다.

- 변수 7~10 사용 — ASA가 엔드 유저 요청(북마크 또는 POST 양식)에서 4개의 변수 문자열 중 하나를 인식하는 경우 요청을 원격 서버에 전달하기 전에 사용자 특정 값으로 바꿉니다.

  ```
  The following example sets a URL for the homepage:
  WebVPN-Macro-Value1 (ID=223), type string, is returned as wwwin-portal.example.com
  WebVPN-Macro-Value2 (ID=224), type string, is returned as 401k.com

  To set a home page value, you would configure the variable substitution as
  https://CSCO_WEBVPN_MACRO1, which would translate to https://wwwin-portal.example.com.
  ```

- 변수 11 사용 — 이러한 북마크는 CSCO_WEBVPN_DYNAMIC_URL이 매핑되어 있는 LDAP 속성 맵을 기반으로 생성됩니다. 구분 기호 파라미터를 사용하여, LDAP에서 수신한 문자열이 값 목록으로 구문 분석됩니다. URL 필드에서 사용되거나 책갈피에서 POST 파라미터로 사용될 경우, 구문 분석된 LDAP 문자열의 각 값에 대한 북마크가 생성됩니다.
  CSCO_WEBVPN_DYNAMIC_URL을 사용하는 북마크 구성의 예는 다음과 같습니다.

  ```
  <bookmark>
      <title>Test Bookmark</title>
      <method>post</method>
      <favorite>yes</favorite>
      <url>http://CSCO_WEBVPN_DYNAMIC_URL1(".")</url>
      <subtitle></subtitle>
      <thumbnail></thumbnail>
      <smart-tunnel>no</smart-tunnel>
      <login-page-url></login-page-url>
      <landing-page-url></landing-page-url>
      <pre-login-page-url></pre-login-page-url>
  ```

```
    <control-id></control-id>
    <<post-param>
        <value>value1</value>
        <name>parameter1</name>
    </post-param>
</bookmark>
```

CSCO_WEBVPN_DYNAMIC_URL은 LDAP 속성 맵에서 구성되며 host1.cisco.com, host2.cisco.com 및 host3.cisco.com에 매핑됩니다. 구분 기호에 따라 http://host1.cisco.com, http://host2.cisco.com 및 http://host3.cisco.com을 통해 이 단일 구성으로 생성된 3개의 북마크와 3개의 URL을 얻을 수 있습니다.

또한 이 매크로를 POST 파라미터의 일부로 사용할 수 있습니다.

```
<bookmark>
    <title>Test Bookmark</title>
    <method>post</method>
    <favorite>yes</favorite>
    <url>http://www.myhost.cisco.com</url>
    <subtitle></subtitle>
    <thumbnail></thumbnail>
    <smart-tunnel>no</smart-tunnel>
    <login-page-url></login-page-url>
    <landing-page-url></landing-page-url>
    <pre-login-page-url></pre-login-page-url>
    <control-id></control-id>
    <post-param>
        <value>CSCO_WEBVPN_DYNAMIC_URL(";")</value>
        <name>host</name>
    </bookmark>
```

매핑된 동일한 LDAP 속성을 사용할 경우 대상 URL http://www.myhost.cisco.com을 통해 3개의 북마크가 생성되며, 각 북마크는 각기 다른 POST 파라미터, 이름 호스트및 값(host1.cisco.com, host2.cisco.com, host3.cisco.com)을 가집니다.

참고 북마크에서는 CSCO_WEBVPN_DYNAMIC_URL만 사용할 수 있습니다. Citrix Mobile Receiver에 대한 vdi CLI 구성과 같은 매크로를 지원하는 다른 위치에서는 이를 사용할 수 없습니다. 외부 포털 페이지를 정의하는 데에도 사용할 수 없습니다.

- 변수 12 사용 — 이 매크로에서는 인덱스, 구분 기호 및 이스케이프 등의 세 가지 파라미터를 입력으로 사용합니다. 인덱스는 목록에서 선택할 요소의 수를 지정하는 정수이며 이는 관리자가 제공합니다. 구분 기호는 LDAP 매핑 문자열을 값 목록으로 구분하는 데 사용되는 문자이며 매크로를 사용할 때마다 한 개의 구분 기호를 사용합니다. 이 문자열은 관리자가 제공합니다. *Escape*는 ASA의 요청으로 대체되기 전에 LDAP 문자열을 적용하기 위해 선택합니다.

  예를 들어, CSCO_WEBVPN_MACROLIST(2, ",", url-encode)는 목록에서 두 번째 값을 사용하고 단일 쉼표를 구분 기호로 사용하여 문자열을 목록으로 구분하도록 지정합니다. 이 값은 백엔드에 대한 ASA의 요청으로 대체될 때 URL로 인코딩됩니다. 이스케이프 루틴의 경우, 다음 값이 사용됩니다.

  - *None* — 백엔드 서버에 전송하기 전에 문자열 값에서 변환이 발생하지 않습니다.
  - *url-code* — 구문 분석된 각 값은 URL로 인코딩되며 URL에서 특수 문자를 구성하는 예약된 문자 목록은 제외됩니다.
  - *url-encode-data* — 구문 분석된 각 값은 URL 인코딩을 사용하여 완벽하게 변환됩니다.

- *base64* — 구문 분석된 각 값은 base 64로 인코딩됩니다.

CSCO_WEBVPN_MACROLIST1을 사용하는 북마크 구성의 예는 다음과 같습니다.

```
<bookmark>
    <title>MyHost</title>
    <method>post</method>
    <favorite>yes</favorite>
    <url>http://www.myhost.cisco.com</url>
    <subtitle></subtitle>
    <thumbnail></thumbnail>
    <smart-tunnel>no</smart-tunnel>
    <login-page-url><login-page-url>
    <landing-page-url></landing-page-url>
    <pre-login-page-url></pre-login-page-url>
    <control-id></control-id>
    <post-param>
        <value>CSCO_WEBVPN_MACROLIST1(1, ";", url-encode-data)>/value>
        <name>param1</name>
        <value>CSCO_WEBVON_MACROLIST1(2, ";", url-encode-data)</value>
        <name>param2</name>
        <value>CSCO_WEBVPN_MACROLIST1(3, ";", url-encode-data)</value>
        <name>param3</name>
    </post-param>
</bookmark>
```

이 북마크를 사용하여 www.myhost.cisco.com으로 이동하고 3개의 POST 파라미터인 param1, param2, param3을 자동으로 서버에 전송할 수 있습니다. ASA는 백엔드로 전송하기 전에 CSCO_WEBVPN_MACROLIST1에 대한 값을 파라미터로 대체합니다.

참고 다른 매크로가 사용되는 경우 언제든지 CSCO_WEBVPN_MACROLIST를 사용할 수 있습니다.

- 이를 수행하기 위해 가장 좋은 방법은 ASDM에서 홈 페이지 URL 매개변수를 구성하는 것입니다. 스크립트 쓰기 또는 업로드를 수행하지 않고 관리자는 스마트 터널을 통해 연결할 그룹 정책의 홈페이지를 지정할 수 있습니다. ASDM의 Network Client SSL VPN(네트워크 클라이언트 SSL VPN) 또는 Clientless SSL VPN Access(클라이언트리스 SSL VPN 액세스) 섹션에서 Add/Edit Group Policy(그룹 정책 추가/수정) 창으로 이동합니다. 경로는 다음과 같습니다.
  - Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > Network(Client) Access(네트워크(클라이언트) 액세스) > Group Policies(그룹 정책) > Add/Edit Group Policy(그룹 정책 추가/수정) > Advanced(고급) > SSL VPN Client(SSL VPN 클라이언트) > Customization(사용자 지정) > Homepage URL attribute(홈페이지 URL 특성)
  - Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > Clientless SSL VPN Access(클라이언트리스 SSL VPN 액세스) > Group Policies(그룹 정책) > Add/Edit Group Policy(그룹 정책 추가/수정) > More Options(추가 옵션) > Customization(사용자 지정) > Homepage URL attribute(홈페이지 URL 특성)

단계 **3** 북마크 또는 URL 항목을 설정합니다. HTTP Post를 통해 OTP(One-time Password: 일회용 비밀번호)로 SSL VPN을 인증한 후 정적 내부 비밀번호로 OWA 이메일에 액세스하여 OWA 리소스에 로그온할 수 있습니다. 이를 수행하기 위해 가장 좋은 방법은 다음 경로 중 하나를 사용하여 ASDM에서 책갈피 항목을 추가 또는 수정하는 것입니다.

- Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > Clientless SSL VPN Access(클라이언트리스 SSL VPN 액세스) > Portal(포털) > Bookmarks(책갈피) > Add/Edit Bookmark Lists(책갈피 목록 추가/수정) > Add/Edit Bookmark Entry(책갈피 항목 추가/수정) > Advanced Options(고급 옵션) 영역 > Add/Edit Post Parameters(게시 매개변수 추가/수정)(URL Method attribute(URL 메서드 특성)에서 **Post(**게시**)**를 클릭해야 사용 가능)
- Network(Client) Access(네트워크(클라이언트) 액세스) > Dynamic Access Policies(동적 액세스 정책) > Add/Edit Dynamic Access Policy(동적 액세스 정책 추가/수정) > URL Lists(URL 목록) 탭 > Manage(관리) 버튼 > Configured GUI Customization Objects(구성된 GUI 사용자 지정 개체) > Add/Edit(추가/수정) 버튼 > Add/Edit Bookmark List(책갈피 목록 추가/수정) > Add/Edit Bookmark Entry(책갈피 항목 추가/수정) > Advanced Options(고급 옵션) 영역 > Add/Edit Post Parameters(게시 매개변수 추가/수정)

단계 **4** 파일 공유(CIFS) URL 대체를 구성하여 유연한 북마크 구성을 설정합니다. URL cifs://server/CSCO_WEBVPN_USERNAME을 구성한 경우 ASA는 이를 자동으로 사용자의 파일 공유 홈 디렉토리에 매핑합니다. 이 방법은 또한 비밀번호와 내부 비밀번호 대체에 사용할 수 있습니다. 다음은 URL 대체의 예입니다.

```
cifs://CSCO_WEBVPN_USERNAME:CSCO_WEBVPN_PASSWORD@server
cifs://CSCO_WEBVPN_USERNAME:CSCO_WEBVPN_INTERNAL_PASSWORD@server
cifs://domain;CSCO_WEBVPN_USERNAME:CSCO_WEBVPN_PASSWORD@server
cifs://domain;CSCO_WEBVPN_USERNAME:CSCO_WEBVPN_INTERNAL_PASSWORD@server
cifs://domain;CSCO_WEBVPN_USERNAME:CSCO_WEBVPN_PASSWORD@server/CSCO_WEBVPN_USERNAME
cifs://domain;CSCO_WEBVPN_USERNAME:CSCO_WEBVPN_INTERNAL_PASSWORD@server/CSCO_WEBVPN_USERNAME
```

외부 포털 사용자 지정

외부 포털 기능을 사용하여 미리 구성된 포털을 사용하는 대신 고유한 포털을 생성할 수 있습니다. 고유한 포털을 구성하는 경우, 클라이언트리스 포털을 무시하고 POST 요청을 전송하여 해당 포털을 검색할 수 있습니다.

프로시저

단계 **1** **Configuration(**구성**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **Clientless SSL VPN Access(**클라이언트리스 **SSL VPN** 액세스**)** > **Portal(**포털**)** > **Customization(**맞춤화**)**을 선택합니다. 필요한 사용자 지정을 강조표시하고 **Edit(**수정**)**를 선택합니다.

단계 **2** Enable External Portal(외부 포털 활성화) 확인란을 선택합니다.

단계 **3** URL 필드에서 POST 요청이 허용되도록 필요한 외부 포털을 입력합니다.

16 장

정책 그룹

스마트 터널 액세스

다음 섹션에서는 클라이언트리스 SSL VPN 세션에서 스마트 터널 액세스를 활성화하는 방법에 대해 설명하며 해당 액세스를 통해 제공되는 애플리케이션을 지정하고 애플리케이션 사용에 대한 참고사항을 제공합니다.

스마트 터널 액세스를 구성하려면 스마트 터널 액세스에 사용할 수 있는 하나 이상의 애플리케이션을 포함하는 스마트 터널 목록과 이 목록에 연계된 엔드포인트 운영 체제를 생성합니다. 각 그룹 정책 또는 로컬 사용자 정책은 하나의 스마트 터널 목록을 지원하므로 지원할 비 브라우저 기반 애플리케이션을 스마트 터널 목록으로 그룹화해야 합니다. 목록을 생성한 후 하나 이상의 그룹 정책 또는 로컬 사용자 정책에 목록을 할당합니다.

다음 섹션에서는 스마트 터널 및 이를 구성하는 방법에 대해 설명합니다.

- 스마트 터널 로그오프 구성, 349 페이지

스마트 터널 정보

스마트 터널은 보안 어플라이언스를 경로로, ASA를 프록시로 사용하는 클라이언트리스(브라우저 기반) SSL VPN 세션을 사용하여 TCP 기반 애플리케이션과 개인 사이트를 연결합니다. 스마트 터널 액세스 권한을 부여할 애플리케이션을 식별하고 각 애플리케이션에 대한 로컬 경로를 지정할 수 있습니다. Microsoft Windows에서 실행 중인 애플리케이션의 경우 스마트 터널 액세스 부여를 위한 조건으로 체크섬의 SHA-1 해시 일치를 요청할 수 있습니다.

Lotus SameTime 및 Microsoft Outlook은 스마트 터널 액세스 권한을 부여할 애플리케이션의 예입니다.

애플리케이션이 클라이언트 또는 웹 지원 애플리케이션인지에 따라 스마트 터널에서 다음 절차 중 하나를 수행하도록 구성합니다.

- 클라이언트 애플리케이션의 스마트 터널 목록을 하나 이상 생성한 다음 이 목록을 스마트 터널 액세스가 필요한 그룹 정책 또는 로컬 사용자 정책에 할당합니다.
- 스마트 터널 액세스에 사용할 수 있는 웹 지원 애플리케이션의 URL을 지정하는 책갈피 목록 항목을 하나 이상 생성한 다음 이 목록을 스마트 터널 액세스가 필요한 그룹 정책 또는 로컬 사용자 정책에 할당합니다.

또한 클라이언트리스 SSL VPN 세션을 통한 스마트 터널 연결에서 로그인 자격 증명 제출을 자동화하도록 웹 지원 애플리케이션을 나열할 수 있습니다.

스마트 터널의 혜택

스마트 터널 액세스를 통해 클라이언트 TCP 기반 애플리케이션에서 브라우저 기반 VPN 연결을 사용하여 서비스에 액세스할 수 있습니다. 이는 플러그인 및 레거시 기술인 포트 전달과 비교하여 사용자에게 다음과 같은 이점을 제공합니다.

- 스마트 터널은 플러그인보다 우수한 성능을 제공합니다.
- 포트 전달과 달리 스마트 터널을 사용할 경우 로컬 애플리케이션을 로컬 포트에 연결할 필요가 없으므로 사용자 환경이 간소화됩니다.
- 또한 포트 전달과 달리 스마트 터널은 사용자의 관리자 권한이 필요하지 않습니다.

플러그인의 장점은 클라이언트 애플리케이션을 원격 컴퓨터에 설치할 필요가 없다는 점입니다.

스마트 터널에 대한 사전 요구 사항

스마트 터널에서 지원되는 브라우저 및 플랫폼은 지원되는 VPN 플랫폼, Cisco ASA 5500 Series 섹션을 참고하십시오.

다음 요건 및 제한 사항은 Windows에서의 스마트 터널 액세스에 적용됩니다.

- Windows의 ActiveX 또는 Oracle JRE(Java Runtime Environment)(JRE 6 이상 권장)를 브라우저에서 활성화해야 합니다.

- Winsock 2에서만 TCP 기반 애플리케이션을 스마트 터널 액세스에 사용할 수 있습니다.
- Mac OS X의 경우에만 Java Web Start를 브라우저에서 활성화해야 합니다.

스마트 터널에 대한 지침

- 스마트 터널은 Microsoft Windows 및 보안 어플라이언스를 실행하는 컴퓨터 사이에 위치한 프록시만 지원합니다. 스마트 터널은 Windows에서 전체 시스템에 적용되는 매개변수를 설정하는 Internet Explorer 구성을 사용합니다. 이 구성에는 프록시 정보가 포함될 수 있습니다.
  - Windows 컴퓨터에서 ASA에 액세스하는 데 프록시가 필요한 경우 클라이언트의 브라우저에 정적 프록시 항목이 있어야 하며 연결할 호스트가 클라이언트의 프록시 예외 목록에 있어야 합니다.
  - Windows 컴퓨터에서 ASA에 액세스하는 데 프록시가 필요하지 않지만 호스트 애플리케이션에 액세스하는 데 프록시가 필요한 경우, ASA가 클라이언트의 프록시 예외 목록에 있어야 합니다.

  프록시 시스템은 정적 프록시 항목의 클라이언트 구성 또는 자동 구성으로 정의되거나 PAC 파일별로 정의될 수 있습니다. 정적 프록시 구성만 스마트 터널에서 현재 지원됩니다.
- KCD(Kerberos Constrained Delegation: Kerberos 제한 위임)는 스마트 터널에 대해 지원되지 않습니다.
- Windows의 경우 명령 확인 상자에서 시작한 애플리케이션에 스마트 터널 액세스를 추가하려면 “cmd.exe”가 애플리케이션의 상위이므로 스마트 터널 목록의 단일 항목인 프로세스 이름에서 “cmd.exe”를 지정하고 다른 항목에서 애플리케이션 자체에 대한 경로를 지정해야 합니다.
- HTTP 기반 원격 액세스를 통해 일부 서브넷은 VPN 게이트웨이에 대한 사용자 액세스를 차단할 수 있습니다. 이 문제를 해결하려면 웹 및 엔드 유저 간에 트래픽을 라우팅하도록 ASA 앞에 프록시를 배치합니다. 이 프록시는 연결 방법을 지원해야 합니다. 인증이 필요한 프록시의 경우 스마트 터널은 기본 다이제스트 인증 유형만 지원합니다.
- 스마트 터널을 시작할 때 ASA는 브라우저 프로세스가 동일한 경우 기본적으로 VPN 세션을 통해 모든 브라우저 트래픽을 전달합니다. 또한 ASA는 tunnel-all 정책(기본값)이 적용되는 경우에만 이 작업을 수행합니다. 사용자가 브라우저 프로세스의 또 다른 인스턴스를 시작하는 경우 VPN 세션을 통해 모든 트래픽을 전달합니다. 브라우저 프로세스가 동일하며 보안 어플라이언스가 URL에 대한 액세스를 제공하지 않는 경우, 사용자는 브라우저를 열 수 없습니다. 해결책으로 tunnel-all이 아닌 터널 정책을 할당합니다.
- 상태 저장 대체작동은 스마트 터널 연결을 유지하지 않습니다. 사용자는 장애 조치 후 다시 연결해야 합니다.
- 스마트 터널의 Mac 버전은 POST 책갈피, 양식 기반 자동 로그온 또는 POST 매크로 대체를 지원하지 않습니다.
- Mac OS X 사용자의 경우 포털 페이지에서 시작된 애플리케이션만 스마트 터널 연결을 설정할 수 있습니다. 이 필요 조건은 Firefox에 대한 스마트 터널 지원에도 적용됩니다. 스마트 터널을 처음 사용하는 동안 Firefox를 사용하여 Firefox의 또 다른 인스턴스를 시작하려면 csco_st라는 사용

자 프로파일이 필요합니다. 이 사용자 프로파일이 없는 경우 새로 만들라는 메시지가 표시됩니다.

- Mac OS X에서 SSL 라이브러리에 동적으로 연결된 TCP를 사용하는 애플리케이션은 스마트 터널에서 작업을 수행할 수 있습니다.
- 스마트 터널은 Mac OS X에서 다음을 지원하지 않습니다.
  - 프록시 서비스
  - 자동 로그온
  - 2단계 네임 스페이스를 사용하는 애플리케이션
  - 텔넷, SSH 및 cURL 같은 콘솔 기반 애플리케이션
  - dlopen 또는 dlsym을 사용하여 libsocket 호출을 찾는 애플리케이션
  - libsocket 호출을 찾기 위해 정적으로 연결된 애플리케이션
- Mac OS X는 프로세스에 대한 전체 경로를 필요로 하며 대/소문자를 구분합니다. 각 사용자 이름에 대해 경로를 지정하는 것을 방지하려면 물결표(~)를 부분 경로 앞에 삽입합니다(예: ~/bin/vnc).
- Mac 및 Windows 디바이스의 Chrome 브라우저에서 스마트 터널을 지원하기 위한 새로운 방법이 마련되었습니다. Chrome Smart Tunnel Extension은 Chrome에서 더 이상 지원하지 않는 NPAPI(Netscape PluginApplication Program Interface)를 바꿨습니다.

  이미 설치되어 있는 확장 프로그램 없이 Chrome에서 스마트 터널 사용 북마크를 클릭한 경우, 확장 프로그램을 받을 수 있는 Chrome 웹 스토어로 리디렉션됩니다. 새 Chrome 설치 시 사용자는 확장자를 다운로드하도록 Chrome 웹 스토어로 이동하게 됩니다. 확장 프로그램은 스마트 터널을 실행하는 데 필요한 이진 파일을 ASA에서 다운로드합니다.

  Chrome의 기본 다운로드 위치는 현재 사용자의 다운로드 폴더여야 합니다. 또는 Chrome의 다운로드 설정이 'Ask every time(매번 묻기)'인 경우, 사용자는 다운로드 받을 때 다운로드 폴더를 선택해야 합니다.

  스마트 터널을 사용하는 동안 일반적인 북마크 및 애플리케이션 구성은 새 확장 프로그램을 설치하고 다운로드 위치를 지정하는 프로세스 이외에는 변경되지 않습니다.

스마트 터널 구성(예: **Lotus**)

참고 이 예에서 지침은 애플리케이션용으로 스마트 터널 지원을 추가하는 데 필요한 최소한의 지침을 제공합니다. 자세한 내용은 아래 섹션의 필드 설명을 참조하십시오.

프로시저

단계 **1** **Configuration**(구성) **> Remote Access VPN > Clientless SSL VPN Access** > **Portal**(포털) > **Smart Tunnels**(스마트 터널)을 선택합니다.

단계 **2** 애플리케이션을 추가할 스마트 터널 목록을 더블 클릭하거나 **Add**(추가)를 클릭하여 애플리케이션 목록을 생성하고 List Name(목록 이름) 필드에서 이 목록의 이름을 입력하고 **Add**(추가)를 클릭합니다.

예를 들어 Smart Tunnels(스마트 터널) 창에서 **Add**(추가)를 클릭한 후 List Name(목록 이름) 필드에서 Lotus를 입력하고 **Add**(추가)를 클릭합니다.

단계 **3** Add or Edit Smart Tunnel List(스마트 터널 목록 추가 또는 수정) 대화 상자에서 **Add**(추가)를 클릭합니다.

단계 **4** 스마트 터널 목록에 있는 항목에 대한 고유한 인덱스 역할을 하도록 Application ID(애플리케이션 ID) 필드에서 문자열을 입력합니다.

단계 **5** Process Name(프로세스 이름) 대화 상자에 애플리케이션의 파일 이름 및 확장명을 입력합니다.

다음 표는 Lotus를 지원하는 데 필요한 애플리케이션 ID 문자열 예 및 연계된 경로를 보여줍니다.

표 ***11:*** 스마트 터널 예***: Domino Server 6.5.5***를 통한 ***Lotus 6.0 Thick Client***

애플리케이션 **ID** 예	필요한 최소 프로세스 이름
lotusnotes	notes.exe
lotusnlnotes	nlnotes.exe
lotusntaskldr	ntaskldr.exe
lotusnfileret	nfileret.exe

단계 **6** OS 옆에 **Windows**를 선택합니다.

단계 **7** **OK**(확인)를 클릭합니다.

단계 **8** 목록에 추가할 각 애플리케이션에 대해 단계를 반복합니다.

단계 **9** Add or Edit Smart Tunnel List(스마트 터널 목록 추가 또는 수정) 대화 상자에서 **OK**(확인)를 클릭합니다.

단계 **10** 다음과 같이 연계된 애플리케이션에 스마트 터널 액세스를 제공하려면 그룹 정책 및 로컬 사용자 정책에 목록을 할당합니다.

- 그룹 정책에 목록을 할당하려면 **Configuration**(구성) **> Remote Access VPN> Clientless SSL VPN Access > Group Policies > Add** 또는 **Edit > Portal**을 선택하고 Smart Tunnel List(스마트 터널 목록) 드롭다운에서 스마트 터널 이름을 선택합니다.

- 로컬 사용자 정책에 목록을 할당하려면 **Configuration(**구성**) > Remote Access VPN> AAA Setup > Local Users > Add** 또는 **Edit > VPN Policy > Clientless SSL VPN**을 선택하고 Smart Tunnel List(스마트 터널 목록) 드롭다운에서 스마트 터널 이름을 선택합니다.

터널링할 애플리케이션 구성 간소화

스마트 터널 애플리케이션 목록은 터널에 대한 액세스 권한이 부여된 애플리케이션을 기본적으로 필터링한 것입니다. 기본값은 브라우저에서 시작된 모든 프로세스에 대한 액세스를 허용하는 것입니다. 스마트 터널이 활성화된 책갈피에서 클라이언트리스 세션은 웹 브라우저에서 시작한 프로세스에만 액세스 권한을 부여합니다. 비 브라우저 애플리케이션의 경우 관리자는 모든 애플리케이션을 터널링하도록 선택할 수 있으므로 엔드 유저가 호출하는 애플리케이션에 대해 알아야 할 필요가 없습니다.

참고 이 구성은 Windows 플랫폼에만 해당됩니다.

다음 표는 액세스 권한이 부여된 프로세스의 상태를 보여줍니다.

상태	스마트 터널이 활성화된 책갈피	스마트 터널 애플리케이션 액세스
지정된 애플리케이션 목록	애플리케이션 목록에 있는 프로세스 이름과 일치하는 모든 프로세스에 액세스 권한이 부여됩니다.	애플리케이션 목록의 프로세스 이름과 일치하는 프로세스에만 액세스 권한이 부여됩니다.
스마트 터널이 해제됨	모든 프로세스(및 하위 프로세스)에 액세스 권한이 부여됩니다.	프로세스에 액세스 권한이 부여되지 않습니다.
스마트 터널 모든 애플리케이션 확인란을 선택합니다.	모든 프로세스(및 하위 프로세스)에 액세스 권한이 부여됩니다. 참고 이 프로세스에는 동일한 브라우저 프로세스에서 웹 페이지에 서비스를 제공하는 경우 비 스마트 터널 웹 페이지에서 시작한 프로세스가 포함됩니다.	브라우저를 시작한 사용자가 소유한 모든 프로세스에 액세스 권한이 부여되지만 해당하는 원래 프로세스의 하위 프로세스에는 액세스 권한이 부여되지 않습니다.

프로시저

단계 **1** **Configuration(**구성**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **AAA/Local Users(AAA/**로컬 사용자**)** > **Local Users(**로컬 사용자**)**를 선택합니다.

단계 **2** User Account(사용자 어카운트) 창에서 수정하려는 사용자 이름을 강조 표시합니다.

단계 **3** **Edit(**편집**)**을 클릭합니다. Edit User Account(사용자 어카운트 수정) 창이 나타납니다.

단계 **4** Edit User Account(사용자 어카운트 수정) 창의 왼쪽 사이드바에서 **VPN Policy(VPN** 정책**)** > **Clientless SSL VPN(**클라이언트리스 **SSL VPN)**을 클릭합니다.

단계 **5** 다음 중 하나를 수행하십시오.

- **smart tunnel_all_applications** 확인란을 선택합니다. 모든 애플리케이션은 목록을 생성하지 않거나 엔드 유저가 외부 애플리케이션에 대해 호출할 실행 파일을 알지 못한 상태에서 터널링됩니다.
- 또는 다음 터널 정책 옵션 중에서 선택합니다.
  - 스마트 터널 정책 매개변수에서 **Inherit(**상속**)** 확인란을 선택 취소합니다.
  - 네트워크 목록에서 선택하고 지정된 네트워크에 대해 스마트 터널 사용, 지정된 네트워크에 대해 스마트 터널 사용 안 함 또는 모든 네트워크 트래픽에 대해 터널 사용 터널 옵션 중 하나를 지정합니다.

스마트 터널 액세스에 사용할 수 있도록 애플리케이션 추가

각 ASA의 클라이언트리스 SSL VPN을 구성할 때 스마트 터널 목록을 지원하며, 각 목록은 스마트 터널 액세스에 사용할 수 있는 하나 이상의 애플리케이션을 식별합니다. 각 그룹 정책 또는 사용자 이름은 하나의 스마트 터널 목록만 지원하므로 지원할 애플리케이션의 각 집합을 스마트 터널 목록으로 그룹화해야 합니다.

Add or Edit Smart Tunnel Entry(스마트 터널 항목 추가 또는 수정) 대화 상자에서 스마트 터널 목록의 애플리케이션 특성을 지정할 수 있습니다.

프로시저

단계 **1** **Configuration(**구성**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **Clientless SSL VPN Access(**클라이언트리스 **SSL VPN** 액세스**)** > **Portal(**포털**)** > **Smart Tunnels(**스마트 터널**)**로 이동하여 수정할 스마트 터널 애플리케이션 목록을 선택하거나 새 목록을 추가합니다.

단계 **2** 새 목록의 경우 애플리케이션 또는 프로그램 목록에 고유한 이름을 입력합니다. 공백은 사용하지 마십시오.

스마트 터널 목록의 구성 이후에는 목록 이름이 클라이언트리스 SSL VPN 그룹 정책 및 로컬 사용자 정책의 스마트 터널 목록 특성 옆에 나타납니다. 구성할 다른 목록과 콘텐츠 또는 목적을 쉽게 구별하도록 이름을 할당합니다.

단계 **3** Add(추가)를 클릭하고 이 스마트 터널 목록에 필요한 만큼 애플리케이션을 추가합니다. 다음은 매개변수에 대한 설명입니다.

- Application ID(애플리케이션 ID) - 스마트 터널 목록의 항목 이름을 지정하려면 문자열을 입력합니다. 이 사용자 지정 이름은 저장된 다음 GUI로 반환됩니다. 문자열은 운영 체제에 고유합니다. 일반적으로 스마트 터널 액세스 권한이 부여되는 애플리케이션의 이름을 지정합니다. 다른 경

로 또는 해시 값을 지정하도록 선택하는 애플리케이션의 여러 버전을 지원하려면 이 특성을 사용하여 각 목록 항목에서 지원하는 애플리케이션의 운영 체제, 이름 및 버전을 지정하도록 항목을 구분할 수 있습니다. 문자열은 최대 64자까지 허용됩니다.

- Process Name(프로세스 이름) - 애플리케이션에 대한 파일 이름 또는 경로를 입력합니다. 문자열은 최대 128자까지 허용됩니다.

  Windows에서는 이 값이 원격 호스트에 있는 애플리케이션 경로의 오른쪽과 정확하게 일치해야 애플리케이션에 스마트 터널 액세스 자격을 부여합니다. Windows용 파일 이름만 지정하는 경우 SSL VPN은 애플리케이션에 스마트 터널 액세스에 대한 자격을 부여하기 위해 원격 호스트에서의 위치 제한을 적용하지 않습니다.

  경로를 지정하고 사용자가 다른 위치에서 애플리케이션을 설치한 경우 이 애플리케이션에는 자격이 부여되지 않습니다. 이 애플리케이션은 입력한 값과 문자열의 오른쪽이 일치하는 경우에 한하여 어떤 경로에든 위치할 수 있습니다.

  원격 호스트에 있는 여러 경로 중 하나에 있는 경우, 애플리케이션에 스마트 터널 액세스 권한을 부여하려면 이 필드에서 애플리케이션의 이름 및 확장명을 지정하거나 각 경로에 대해 고유한 스마트 터널 항목을 생성합니다.

  참고 스마트 터널 액세스에 갑자기 문제가 발생하는 경우 Process Name(프로세스 이름) 값이 애플리케이션 업그레이드의 최신 상태가 아니라는 의미일 수 있습니다. 예를 들어, 애플리케이션에 대한 기본 경로가 애플리케이션을 제작하는 회사를 인수한 이후 및 다음 애플리케이션 업그레이드 이후에 변경될 때가 있습니다.

  Windows의 경우 명령 확인 상자에서 시작한 애플리케이션에 스마트 터널 액세스를 추가하려면 “cmd.exe”가 애플리케이션의 상위이므로 스마트 터널 목록의 단일 항목인 프로세스 이름에서 “cmd.exe”를 지정하고 다른 항목에서 애플리케이션 자체에 대한 경로를 지정해야 합니다.

- OS — 애플리케이션의 호스트 운영 체제를 지정하려면 **Windows** 또는 **Mac**을 클릭합니다.

- 해시(선택 사항이며 Windows에만 적용 가능) - 이 값을 얻으려면 애플리케이션의 체크섬(실행 파일의 체크섬)을 SHA-1 알고리즘을 사용하여 해시를 계산하는 유틸리티에 입력합니다. 이러한 유틸리티의 예로 Microsoft FCIV(File Checksum Integrity Verifier)가 있으며 http://support.microsoft.com/kb/841290/에서 얻을 수 있습니다. FCIV를 설치한 후에는 해시할 애플리케이션의 임시 사본을 공백 없는 경로(예: c:/fciv.exe)에 둔 후 커맨드 라인에 **fciv.exe -sha1** application을 입력하여(예: **fciv.exe -sha1 c:\msimn.exe**) SHA-1 해시를 표시합니다.

  SHA-1 해시는 항상 16진수 40자입니다.

  스마트 터널 액세스를 위해 애플리케이션에 권한을 부여하기 전에 먼저 클라이언트리스 SSL VPN이 애플리케이션 ID와 일치하는 애플리케이션의 해시를 계산합니다. 결과가 해시 값과 일치하는 경우 스마트 터널 액세스를 위해 애플리케이션에 자격을 부여합니다.

  해시를 입력하면 SSL VPN이 애플리케이션 ID에 지정한 문자열과 일치하는 불법적인 파일에 자격을 부여하지 않도록 합리적으로 보장할 수 있습니다. 애플리케이션의 각 버전 또는 패치마다 체크섬이 다르기 때문에 입력하는 hash가 원격 호스트의 특정 버전 또는 특정 패치하고만 일치할 수도 있습니다. 애플리케이션의 두 가지 이상의 버전에 대해 해시를 지정하려면 각 해시 값에 대해 고유한 스마트 터널 항목을 생성하십시오.

참고 해시 값을 입력하고 애플리케이션의 이후 버전 또는 패치에서 스마트 터널 액세스를 지원해야 하는 경우, 스마트 터널 목록을 업데이트된 상태로 유지해야 합니다. 스마트 터널 액세스에 갑자기 문제가 발생할 경우는 애플리케이션 업그레이드로 인해 hash 값이 더이상 유효하지 않다는 의미일 수도 있습니다. 해시를 입력하지 않는 방법으로 이 문제를 방지할 수 있습니다.

단계 **4** 애플리케이션을 저장하려면 **OK(**확인**)**를 클릭하고 이 스마트 터널 목록에 필요한 만큼의 애플리케이션을 생성합니다.

단계 **5** 스마트 터널 목록 생성을 완료한 경우, 이 목록을 활성화하려면 다음과 같이 그룹 정책 또는 로컬 사용자 정책에 할당해야 합니다.

- 그룹 정책에 목록을 할당하려면 **Config > Remote Access VPN> Clientless SSL VPN Access > Group Policies > Add** 또는 **Edit > Portal**을 선택하고 Smart Tunnel List(스마트 터널 목록) 속성 옆에 있는 드롭다운 목록에서 스마트 터널 이름을 선택합니다.
- 로컬 사용자 정책에 목록을 할당하려면 **Config > Remote Access VPN> AAA Setup > Local Users > Add** 또는 **Edit > VPN Policy > Clientless SSL VPN**을 선택하고 Smart Tunnel List(스마트 터널 목록) 속성 옆에 있는 드롭다운 목록에서 스마트 터널 이름을 선택합니다.

표 ***12:*** 스마트 터널 항목 예

스마트 터널 지원	애플리케이션 **ID(**고유한 문자열이면 사용 가능**)**	프로세스 이름	**OS**
Mozilla Firefox.	firefox	firefox.exe	Windows
Microsoft Outlook Express	outlook-express	msimn.exe	Windows
보다 제한적인 대체 — 실행 파일이 미리 정의된 경로에 있는 경우에만 Microsoft Outlook Express.	outlook-express	\Program Files\Outlook Express\msimn.exe	Windows
Mac에서 새 터미널 창을 엽니다. 동일한 터미널 창에서 실행된 모든 후속 애플리케이션은 일회용 비밀번호 구현으로 인해 실패합니다.	terminal	터미널	Mac
새 창에 대해 스마트 터널을 시작합니다.	new-terminal	Terminal open -a MacTelnet	Mac

스마트 터널 지원	애플리케이션 ID(고유한 문자열이면 사용 가능)	프로세스 이름	OS
Mac 터미널 창에서 애플리케이션을 시작합니다.	curl	Terminal curl www.example.com	Mac

스마트 터널 목록 정보

각 그룹 정책 및 사용자 이름에 대해 다음 중 하나를 수행하도록 클라이언트리스 SSL VPN을 구성할 수 있습니다.

- 사용자 로그인 시 자동으로 스마트 터널 액세스를 시작합니다.
- 사용자 로그인 시 스마트 터널 액세스를 활성화하지만, 사용자가 클라이언트리스 SSL VPN 포털 페이지에서 **Application Access** > **Start Smart Tunnels** 버튼을 사용하여 이 기능을 수동으로 시작하도록 요청해야 합니다.

참고 스마트 터널 로그온 옵션은 각 그룹 정책 및 사용자 이름에 대해 상호 배타적입니다. 한 가지만 사용하십시오.

스마트 터널 자동 로그온 서버 목록 생성

Smart Tunnel Auto Sign-on Server List(스마트 터널 자동 로그온 서버 목록) 대화 상자에서 스마트 터널 설정 동안 로그인 자격 증명 제출을 자동화하는 서버 목록을 추가하거나 수정할 수 있습니다. 스마트 터널을 통한 자동 로그온은 Internet Explorer 및 Firefox용으로 사용할 수 있습니다.

프로시저

단계 **1** Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > Clientless SSL VPN Access(클라이언트리스 SSL VPN 액세스) > Portal(포털) > Smart Tunnels(스마트 터널)로 이동하고 스마트 터널 자동 로그인 서버 목록을 확장합니다.

단계 **2** Add(추가)를 클릭하고 구성할 다른 목록과 콘텐츠 또는 목적을 쉽게 구별할 수 있도록 원격 서버 목록에 고유한 이름을 입력합니다. 문자열은 최대 64자까지 허용됩니다. 공백은 사용하지 마십시오.

다음에 수행할 작업

참고 스마트 터널 자동 로그인 목록을 생성하면 해당 목록 이름이 클라이언트리스 SSL VPN 그룹 정책 및 로컬 사용자 정책 구성의 스마트 터널 아래에 있는 자동 로그인 서버 목록 특성 옆에 나타납니다.

스마트 터널 자동 로그온 서버 목록에 서버 추가

다음 단계는 스마트 터널 연결에서 자동 로그온을 제공하고 해당 목록을 그룹 정책 또는 로컬 사용자에게 할당할 서버 목록에 서버를 추가하는 방법에 대해 설명합니다.

프로시저

단계 **1** **Configuration(**구성**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **Clientless SSL VPN Access(**클라이언트리스 **SSL VPN** 액세스**)** > **Portal(**포털**)** > **Smart Tunnels(**스마트 터널**)**로 이동하여 목록 중 하나를 선택하고 **Edit(**수정**)**을 클릭합니다.

단계 **2** Add Smart Tunnel Auto Sign-On Server List(스마트 터널 자동 로그인 서버 목록 추가) 대화 상자에서 Add(추가) 버튼을 클릭하고 하나 이상의 스마트 터널 서버를 추가합니다.

단계 **3** 자동 인증할 서버의 호스트 이름 또는 IP 주소를 입력합니다.

- 호스트 이름을 선택한 경우 자동으로 인증할 호스트 이름 또는 와일드카드 마스크를 입력합니다. 다음 와일드카드 문자를 사용할 수 있습니다.
  - *는 문자 수에 관계 없이 일치하거나 문자가 없는 경우 일치합니다.
  - ?는 모든 단일 문자와 일치합니다.
  - []는 대괄호 안에 명시된 범위에 있는 모든 단일 문자와 일치합니다.
  - 예를 들어, *.example.com을 입력합니다. 이 옵션을 사용하면 IP 주소의 동적 변경으로부터 구성을 보호합니다.
- IP 주소를 선택한 경우 IP 주소를 입력합니다.

  참고 Firefox는 와일드카드, IP 주소를 사용하는 서브넷 또는 넷마스크가 있는 호스트 마스크를 지원하지 않으므로 정확한 호스트 이름 또는 IP 주소를 사용해야 합니다. 예를 들어, Firefox에서 *.cisco.com을 입력할 경우 email.cisco.com을 호스팅하기 위한 자동 로그온이 실패합니다.

단계 **4** Windows 도메인(선택 사항) — 인증에 필요한 경우, Windows 도메인을 사용자 이름에 추가하려면 클릭합니다. 이렇게 하면 스마트 터널 목록을 하나 이상의 그룹 정책 또는 로컬 사용자 정책에 할당할 때 도메인 이름이 지정됩니다.

단계 **5** HTTP 기반 자동 로그온(선택 사항)

- 인증 영역 — 영역은 웹사이트의 보호 영역과 연계되며 인증 도중에 인증 확인 상자 또는 HTTP 헤더 중 하나에서 브라우저에 다시 전달됩니다. 자동 로그온이 구성되고 영역 문자열이 지정되면 사용자는 웹 애플리케이션(Outlook Web Access 등)에 영역 문자열을 구성하고 로그온하지 않고 웹 애플리케이션에 액세스할 수 있습니다.

  인트라넷에서 웹 페이지의 소스 코드에 사용되는 주소 형식을 사용합니다. 브라우저 액세스를 위한 스마트 터널 자동 로그온을 구성 중이며 일부 웹 페이지에서 호스트 이름을 사용하고 다른 웹 페이지에서 IP 주소를 사용하거나 알 수 없는 경우, 다른 스마트 터널 자동 로그온 항목에서 두 가지 모두를 지정합니다. 그렇지 않은 경우 웹 페이지의 링크가 지정한 형식과 다른 형식을 사용하는 경우, 사용자가 이 형식을 클릭하면 실패합니다.

  참고 관리자가 해당하는 영역을 모르는 경우 로그온을 한 번 수행하고 확인 상자 대화에서 문자열을 가져와야 합니다.

- 포트 번호 — 해당하는 호스트에 대해 포트 번호를 지정합니다. Firefox의 경우 포트 번호를 지정하지 않으면 자동 로그온이 HTTP 및 HTTPS에서 수행되며 기본 포트 번호 80 및 443에서 각각 액세스됩니다.

단계 **6** 확인을 클릭합니다.

단계 **7** 스마트 터널 자동 로그인 서버 목록의 구성에 따라 이 목록을 활성화하려면 다음과 같이 그룹 정책 또는 로컬 사용자 정책에 할당해야 합니다.

- 그룹 정책에 목록을 할당하려면 다음을 수행하십시오.

  1. **Configuration(**구성**) > Remote Access VPN(**원격 액세스 **VPN) > Clientless SSL VPN Access(**클라이언트리스 **SSL VPN** 액세스**) > Group Policies(**그룹 정책**)**로 이동하여 그룹 정책을 엽니다.
  2. Portal(포털) 탭을 선택하고 스마트 터널 영역을 찾은 다음 자동 로그온 서버 목록 특성 옆에 있는 드롭다운 목록에서 자동 로그온 서버 목록을 선택합니다.

- 로컬 사용자 정책에 목록을 할당하려면 다음을 수행하십시오.

  1. **Configuration > Remote Access VPN > AAA/Local Users > Local Users**를 선택하고 자동 로그인 서버 목록을 할당할 대상 로컬 사용자를 수정합니다.
  2. VPN Policy(VPN 정책) > Clientless SSL VPN(클라이언트리스 SSL VPN)으로 이동하고 스마트 터널 영역 아래에서 자동 로그인 서버 설정을 찾습니다.
  3. Inherit(상속)의 선택을 취소하고 자동 로그인 서버 목록 특성 옆에 있는 드롭다운 목록에서 서버 목록을 선택합니다.

스마트 터널 액세스 활성화 및 해제

기본적으로 스마트 터널은 해제되어 있습니다.

스마트 터널 액세스를 활성화한 경우 사용자는 클라이언트리스 SSL VPN 포털 페이지에서 **Application Access** > **Start Smart Tunnels** 버튼을 사용하여 수동으로 이 기능을 시작해야 합니다.

스마트 터널 로그오프 구성

이 섹션에서는 스마트 터널이 제대로 로그오프되었는지 확인하는 방법에 대해 설명합니다. 스마트 터널은 모든 브라우저 창이 닫힌 경우 로그오프될 수 있습니다. 또는 알림 아이콘을 마우스 오른쪽 버튼으로 클릭하고 로그아웃을 확인할 수 있습니다.

참고 포털에서 로그아웃 버튼을 사용할 것을 적극 권장합니다. 이 방법은 클라이언트리스 SSL VPN과 관련이 있고 스마트 터널의 사용 여부에 관계없이 로그오프됩니다. 알림 아이콘은 독립 실행형 애플리케이션을 브라우저 없이 사용하는 경우에만 사용해야 합니다.

상위 프로세스 종료 시 스마트 터널 로그오프 구성

이 사례에서는 로그오프하려면 모든 브라우저를 닫아야 합니다. 이제 스마트 터널 수명은 프로세스 수명의 시작과 연관이 있습니다. 예를 들어 Internet Explorer에서 스마트 터널을 시작한 경우 iexplore.exe가 실행 중이 아니면 스마트 터널이 꺼집니다. 스마트 터널은 사용자가 로그아웃하지 않고 모든 브라우저를 닫는 경우에도 VPN 세션이 종료되었는지 판단할 수 있습니다.

참고 브라우저 프로세스가 느려지는 경우 의도하지 않은 결과이며 엄격히 말해 오류의 결과입니다. Secure Desktop을 사용 중인 경우 사용자가 Secure Desktop에서 모든 브라우저를 닫은 경우에도 브라우저 프로세스가 다른 데스크톱에서 실행될 수 있습니다. 따라서 스마트 터널은 현재 데스크톱에 더 이상 창이 보이지 않는 경우 모든 브라우저 인스턴스를 gone(없음)으로 선언합니다.

알림 아이콘을 통한 스마트 터널 로그오프 구성

브라우저를 닫는 경우 세션이 그대로 유지되도록 상위 프로세스를 종료할 때 로그오프를 해제하도록 선택할 수 있습니다. 이 사례에서 시스템 트레이의 알림 아이콘을 사용하여 로그아웃합니다. 이 아이콘은 사용자가 로그아웃하기 위해 아이콘을 클릭할 때까지 그대로 유지됩니다. 사용자가 로그아웃하기 전에 세션이 만료된 경우 이 아이콘은 다음 연결이 시도될 때까지 그대로 유지됩니다. 시스템 트레이에서 업데이트하려면 세션 상태를 기다려야 할 수 있습니다.

참고 이 아이콘은 SSL VPN에서 로그아웃하기 위한 대체 방법입니다. VPN 세션 상태에 대한 표시기가 아닙니다.

프로시저

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

단계 **2** 시스템 트레이 라디오 버튼에서 > **Click on smart-tunnel logoff(**스마트 터널 로그오프 클릭**)** 아이콘을 활성화합니다.

단계 **3** 창의 Smart Tunnel Networks(스마트 터널 네트워크) 부분에서 **Add(**추가**)**를 선택하고 아이콘을 포함해야 하는 네트워크의 IP 주소 및 호스트 이름을 모두 입력합니다.

참고 아이콘을 마우스 오른쪽 버튼으로 클릭하는 경우 SSL VPN에서 로그아웃하도록 사용자에게 확인 상자를 표시하는 단일 메뉴 항목이 나타납니다.

클라이언트리스 **SSL VPN** 캡처 툴

클라이언트리스 SSL VPN CLI에는 WebVPN 연결을 통해 제대로 표시되지 않은 웹사이트에 대한 정보를 기록할 수 있는 캡처 툴이 포함되어 있습니다. 이 툴에서 기록하는 데이터는 Cisco 고객 지원 담당자가 문제를 해결하는 데 도움이 됩니다.

클라이언트리스 SSL VPN 캡처 툴의 출력은 다음과 같이 두 개의 파일로 구성됩니다.

- mangled.1, 2,3, 4... 등(웹 페이지 작업에 따라) 변조 파일은 클라이언트리스 SSL VPN 연결에서 이 페이지를 전송하는 VPN Concentrator의 html 작업을 기록합니다.
- original.1,2,3,4... 등(웹 페이지 작업에 따라) 원본 파일은 VPN Concentrator로 전송된 URL 파일입니다.

캡처 툴을 사용하여 파일 출력을 열고 보려면 Administration(관리) | File Management(파일 관리)로 이동합니다. 출력 파일을 압축하고 Cisco 지원 담당자에게 전송합니다.

참고 클라이언트리스 SSL VPN 캡처 툴을 사용하면 VPN Concentrator 성능에 영향을 줍니다. 출력 파일을 생성한 후에 캡처 툴을 해제해야 합니다.

포털 액세스 규칙 구성

이러한 개선 사항을 통해 고객은 HTTP 헤더에 있는 데이터에 기반하여 클라이언트리스 SSL VPN 세션을 허용하거나 거부하도록 전역 클라이언트리스 SSL VPN 액세스 정책을 구성할 수 있습니다. ASA가 클라이언트리스 SSL VPN 세션을 거부하는 경우 엔드포인트에 오류 코드를 즉시 반환합니다.

ASA가 이 액세스 정책을 평가한 후에 엔드포인트는 ASA에 대해 인증을 실시합니다. 따라서 이러한 세션이 거부되는 경우 엔드포인트에 추가 연결을 시도하더라도 ASA 처리 리소스가 더 적게 소모됩니다.

프로시저

단계 **1** ASDM을 시작하고 **Configuration(**구성**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **Clientless SSL VPN Access(**클라이언트리스 **SSL VPN** 액세스**)** > **Portal(**포털**)** > **Portal Access Rule(**포털 액세스 규칙**)**을 선택합니다.

Portal Access Rule(포털 액세스 규칙) 창이 열립니다.

단계 **2** 포털 액세스 규칙을 생성하려면 **Add(**추가**)**를 클릭하거나 기존 규칙을 선택하고 **Edit(**수정**)** > 을 클릭합니다**.**

포털 액세스 규칙 추가(또는 수정) 대화 상자가 열립니다.

단계 **3** Rule Priority(규칙 우선순위) 필드에 규칙 번호를 1부터 65535까지 입력합니다.

1부터 65535의 우선순위 순서에 따라 규칙이 처리됩니다.

단계 **4** User Agent(사용자 에이전트) 필드에서 HTTP 헤더에서 찾을 사용자 에이전트의 이름을 입력합니다.

- 문자열 주위에 와일드카드(*)를 사용하여 문자열을 일반화합니다(예: *Thunderbird*). 검색 문자열에서 와일드카드를 사용할 것을 권장합니다. 와일드카드가 없는 경우, 규칙은 어떤 문자열과도 일치하지 않거나 예상보다 훨씬 적은 문자열과 일치할 수 있습니다.
- 문자열에 공백이 포함된 경우 ASDM은 규칙을 저장할 때 문자열의 시작과 끝에 따옴표를 자동으로 추가합니다. 예를 들어 `my agent`를 입력하면 ASDM은 문자열을 "`my agent`"로 저장합니다. 그런 다음 ASA는 `my agent`와 일치하는 내용을 검색합니다.

  ASA에서 문자열에 추가한 따옴표와 일치해야 하는 경우가 아니면 공백이 있는 문자열에 따옴표를 추가하지 마십시오. 예를 들어 "`my agent`"를 입력한 경우 ASDM은 문자열을 "`\"my agent\"`"로 저장하고 "`my agent`"와 일치하는 내용을 찾으려고 시도하지만 `my agent`는 찾지 않습니다.
- 공백을 포함하는 문자열에 와일드카드를 사용하기 위해 전체 문자열을 와일드카드로 시작하고 끝나게 하면(예: `*my agent*`) ASDM이 규칙을 저장할 때 문자열 주위에 따옴표를 자동으로 사용합니다.

단계 **5** Action(작업) 필드에서 **Deny(**거부**)** 또는 **Permit(**허용**)**을 선택합니다.

ASA가 이 설정에 따라 클라이언트리스 SSL VPN 연결을 거부하거나 허용합니다.

단계 **6** Returned HTTP Code(반환된 HTTP 코드) 필드에 HTTP 메시지 코드를 입력합니다.

HTTP 메시지 번호 403은 이 필드에서 사전에 채워지며 포털 액세스 규칙에 대한 기본값입니다. 메시지 코드의 허용되는 범위는 200에서 599까지입니다.

단계 **7** **OK(**확인**)**를 클릭합니다.

단계 **8** **Apply(**적용**)**를 클릭합니다.

클라이언트리스 SSL VPN 성능 최적화

ASA는 클라이언트리스 SSL VPN 성능 및 기능을 최적화하는 다양한 방법을 제공합니다. 성능 개선에는 웹 개체 캐싱 및 압축이 포함됩니다. 기능 조정에는 콘텐츠 변형 및 proxy-bypass에 대한 제한 설정이 포함됩니다. APCF는 콘텐츠 변형을 조정하는 추가적인 방법을 제공합니다.

콘텐츠 변형 구성

기본적으로 ASA는 사용자가 SSL VPN 디바이스 내부에서 또는 이와 개별적으로 애플리케이션에 액세스 중인지에 따라 다른 의미 체계 및 액세스 제어 규칙을 포함할 수 있는 HTTP 트래픽을 프록시하기 위해 JavaScript 및 Java 같은 최신 요소를 포함하는 콘텐츠 변환/재작성 엔진을 통해 모든 클라이언트리스 SSL VPN 트래픽을 처리합니다.

일부 웹 리소스는 매우 개별적으로 처리해야 합니다. 다음 섹션에서는 이러한 처리 방법을 제공하는 기능에 대해 설명합니다. 관련된 조직 및 웹 콘텐츠의 요건에 따라 이 기능 중 하나를 사용할 수 있습니다.

프록시 우회 사용

애플리케이션 및 웹 리소스가 프록시 우회가 제공하는 특수한 콘텐츠 재작성 기능을 이용하여 더욱 효율적으로 활용되는 경우 프록시 우회를 사용하도록 ASA를 구성할 수 있습니다. 프록시 우회는 원래 콘텐츠를 최소한으로 변경하는 콘텐츠 재작성의 대체 방법입니다. 사용자 지정 웹 애플리케이션에 주로 유용합니다.

여러 개의 프록시 우회 항목을 구성할 수 있습니다. 항목을 구성한 순서는 중요하지 않습니다. 인터페이스 및 경로 마스크 또는 인터페이스 및 포트는 프록시 우회 규칙을 고유하게 식별합니다.

네트워크 구성에 따라 경로 마스크 대신 포트를 사용하여 프록시 우회를 구성한 경우, 해당 포트가 ASA에 액세스할 수 있도록 방화벽 구성을 변경해야 할 수도 있습니다. 경로 마스크를 사용하여 이러한 제한사항을 방지하십시오. 단, 경로 마스크는 변경될 수 있으므로 이러한 가능성을 없애려면 여러 경로 마스크 명령문을 사용해야 할 수도 있습니다.

경로란 URL에서 .com, .org 또는 기타 도메인 이름 유형 뒤에 나오는 모든 것입니다. 예를 들어 URL www.example.com/hrbenefits에서는 *hrbenefits*가 경로입니다. 마찬가지로 URL www.example.com/hrinsurance에서는 *hrinsurance*가 경로입니다. 모든 hr 사이트에 대한 프록시 우회를 사용하려면 /hr*와 같이 * 와일드카드를 사용하여 명령이 여러 번 사용되는 것을 방지할 수 있습니다.

ASA가 콘텐츠 재작성을 거의 또는 전혀 수행하지 않는 경우에 대해 규칙을 설정할 수 있습니다.

프로시저

단계 **1** **Configuration(**구성**) > Remote Access VPN(**원격 액세스 **VPN) > Clientless SSL VPN Access(**클라이언트리스 **SSL VPN** 액세스**) > Advanced(**고급**) > Proxy Bypass(**프록시 우회**)**로 이동합니다.

단계 **2** 프록시 우회에 대한 인터페이스 이름을 선택합니다.

단계 **3** 프록시 우회에 대해 다음과 같이 포트 또는 URI를 지정합니다.

- Port(포트) - (라디오 버튼) 프록시 우회에 포트를 사용하려면 클릭합니다. 유효한 포트 번호는 20000에서 21000까지입니다.
- Port(포트)(필드) - ASA가 프록시 우회를 위한 부분을 남겨 둘 수 있도록 높은 숫자의 포트를 입력합니다.
- Path Mask(경로 마스크) - (라디오 버튼) 프록시 우회에 URL을 사용하려면 클릭합니다.
- Path Mask(경로 마스크) - (필드) 프록시 우회에 대해 URL을 입력합니다. 정규 표현식을 포함할 수 있습니다.

단계 **4** 프록시 우회에 대해 다음과 같이 대상 URL을 정의합니다.

- URL — (드롭다운 목록) 프로토콜로 http 또는 https를 클릭합니다.
- URL(텍스트 필드) — 프록시 우회를 적용할 URL을 입력합니다.

단계 **5** 콘텐츠를 재작성하도록 지정합니다. 선택 사항은 없음 또는 XML, 링크 및 쿠키의 조합입니다.

- XML — XML 콘텐츠를 재작성하려면 선택합니다.
- Hostname(호스트 이름) - 링크를 재작성하려면 선택합니다.

17 장

클라이언트리스 SSL VPN 원격 사용자

이 장에서는 사용자 원격 시스템에 대한 구성 요건 및 작업을 간략하게 설명합니다. 또한 사용자가 클라이언트리스 SSL VPN을 시작하는 데 도움이 되는 정보를 제공합니다. 다음의 섹션이 포함됩니다.

참고 ASA가 클라이언트리스 SSL VPN에 대해 구성되어 있는지 확인하십시오.

클라이언트리스 SSL VPN 원격 사용자

이 장에서는 사용자 원격 시스템에 대한 구성 요건 및 작업을 간략하게 설명합니다. 또한 사용자가 클라이언트리스 SSL VPN을 시작하는 데 도움이 되는 정보를 제공합니다. 다음의 섹션이 포함됩니다.

참고 ASA가 클라이언트리스 SSL VPN에 대해 구성되어 있는지 확인하십시오.

사용자 이름 및 비밀번호

네트워크에 따라 원격 세션 동안 사용자는 컴퓨터, 인터넷 서비스 공급자, 클라이언트리스 SSL VPN, 메일 또는 파일 서버 또는 기업 애플리케이션 중 하나 또는 모두에 로그온해야 할 수 있습니다. 사용자는 고유한 사용자 이름 및 비밀번호 또는 PIN 같은 다양한 정보가 필요한 여러 가지 다른 상황에서 인증해야 할 수 있습니다. 사용자에게 필수 액세스 권한이 있는지 확인합니다.

다음 표에서는 클라이언트리스 SSL VPN 사용자가 알아야 할 사용자 이름 및 비밀번호 유형을 보여줍니다.

표 ***13:*** 클라이언트리스 ***SSL VPN*** 사용자에게 제공할 사용자 이름 및 비밀번호

로그인 사용자 이름/비밀 번호 유형		입력 시기
컴퓨터	컴퓨터 액세스	컴퓨터 시작 시
인터넷 서비스 공급자	인터넷 액세스	인터넷 서비스 공급자에 연결 시
클라이언트리스 SSL VPN	원격 네트워크 액세스	클라이언트리스 SSL VPN 세션 시작 시
파일 서버	원격 파일 서버 액세스	원격 파일 서버에 액세스하기 위해 클라이언트리스 SSL VPN 파일 브라우징 기능 사용 시
기업 애플리케이션 로그인	방화벽 보호 내부 서버 액세스	내부의 보호되는 웹 사이트에 액세스하기 위해 클라이언트리스 SSL VPN 웹 브라우징 기능 사용 시
메일 서버	클라이언트리스 SSL VPN을 통한 원격 메일 서버 액세스	이메일 메시지 전송 또는 수신 시

보안 팁 전달

다음과 같은 보안 팁을 전달합니다.

- 항상 클라이언트리스 SSL VPN 세션에서 로그아웃하거나, 클라이언트리스 SSL VPN 툴바에서 로그아웃 아이콘을 클릭하거나, 브라우저를 닫습니다.
- 클라이언트리스 SSL VPN의 사용이 모든 사이트와의 통신 보안을 보장하는 것은 아닙니다. 클라이언트리스 SSL VPN은 원격 컴퓨터 또는 워크스테이션과 기업 네트워크에 있는 ASA 간의 데이터 전송 보안을 보장합니다. 사용자가 인터넷 또는 내부 네트워크에 있는 비 HTTPS 웹 리소스에 액세스하는 경우에는 기업 ASA에서 대상 웹 서버로의 통신 보안이 유지되지 않습니다.

클라이언트리스 **SSL VPN** 기능을 사용하도록 원격 시스템 구성

다음 표에는 클라이언트리스 SSL VPN을 사용하도록 원격 시스템 설정하는 작업, 이 작업에 대한 요구 사항/사전 요구 사항 및 권장 사용 방법이 포함되어 있습니다.

사용자 어카운트를 구성한 방식에 따라 각 클라이언트리스 SSL VPN 사용자가 사용할 수 있는 기능이 다를 수 있습니다. 또한 다음 표에는 사용자 작업별로 정보가 구성되어 있습니다.

표 ***14:*** 클라이언트리스 ***SSL VPN*** 원격 시스템 구성 및 엔드 유저 요구 사항

작업	원격 시스템 또는 엔드 유저 요건	사양 또는 사용 제안
클라이언트리스 **SSL VPN** 시작	인터넷에 연결	다음을 비롯한 모든 인터넷 연결이 지원됩니다. • 홈 DSL, 케이블 또는 다이얼업 • 공용 키오스크 • 호텔 연결 • 공항 무선 노드 • 인터넷 카페
	클라이언트리스 SSL VPN 지원 브라우저	클라이언트리스 SSL VPN에 대해 다음 브라우저를 권장합니다. 다른 브라우저는 클라이언트리스 SSL VPN 기능을 완벽하게 지원하지 않을 수 있습니다. Microsoft Windows의 경우: • Internet Explorer 8 • Firefox 8 Linux의 경우: • Firefox 8 Mac OS X의 경우: • Safari 5 • Firefox 8
	브라우저에서 사용 가능한 쿠키	쿠키는 포트 전달을 통한 애플리케이션 액세스를 위해 브라우저에서 활성화되어야 합니다.
	클라이언트리스 SSL VPN의 URL	다음 형식의 HTTPS 주소: https://address 여기서 address는 클라이언트리스 SSL VPN이 활성화된 ASA(또는 로드 밸런싱 클러스터)의 인터페이스 IP 주소 또는 DNS 호스트 이름입니다. 예를 들어 https://10.89.192.163 또는 https://cisco.example.com입니다.

작업	원격 시스템 또는 엔드 유저 요건	사양 또는 사용 제안
	클라이언트리스 SSL VPN 사용자 이름 및 비밀번호	
	[선택 사항] 로컬 프린터	클라이언트리스 SSL VPN은 웹 브라우저에서 네트워크 프린터로의 인쇄를 지원하지 않습니다. 로컬 프린터로의 인쇄는 지원됩니다.
클라이언트리스 **SSL VPN** 연결에서 부동 툴바 사용		부동 툴바를 사용하면 클라이언트리스 SSL VPN 사용을 간소화할 수 있습니다. 툴바를 사용하여 URL을 입력하고 파일 위치를 찾아보며 기본 브라우저 창에 방해되지 않게 사전 구성된 웹 연결을 선택할 수 있습니다. 팝업을 차단하도록 브라우저를 구성한 경우 부동 툴바를 표시할 수 없습니다. 부동 툴바는 현재의 클라이언트리스 SSL VPN 세션을 나타냅니다. **Close** 버튼을 클릭하면 ASA는 클라이언트리스 SSL VPN 세션을 닫도록 확인 상자를 표시합니다. 팁 텍스트를 텍스트 필드에 붙여넣으려면 Ctrl-V를 사용합니다. (마우스 오른쪽 버튼 클릭은 클라이언트리스 SSL VPN 툴바에서 활성화되지 않습니다.)

작업	원격 시스템 또는 엔드 유저 요건	사양 또는 사용 제안
웹 브라우징	보호된 웹 사이트에 대한 사용자 이름 및 비밀번호	클라이언트리스 SSL VPN의 사용이 모든 사이트와의 통신 보안을 보장하는 것은 아닙니다. "보안 팁 전달, 356 페이지"을 참조하십시오.

		클라이언트리스 SSL VPN을 통한 웹 브라우징의 모양과 느낌은 사용자에게 익숙하지 않을 수 있습니다. 예를 들면 다음과 같습니다.
		• 클라이언트리스 SSL VPN의 제목 표시줄은 각각의 웹 페이지 위에 표시됩니다.
		• 다음 방법으로 웹 사이트에 액세스합니다.
		  • 클라이언트리스 SSL VPN 홈 페이지의 Enter Web Address(웹 주소 입력) 필드에서 URL 입력
		  • 클라이언트리스 SSL VPN 홈 페이지의 사전 구성 웹사이트 링크 클릭
		  • 앞의 두 가지 방법 중 하나를 통해 액세스되는 웹 페이지에서 링크 클릭
		  또한 특정한 어카운트를 구성한 방법에 따라 다음과 같을 수도 있습니다.
		• 일부 웹사이트가 차단됨
		• 클라이언트리스 SSL VPN 홈 페이지에서 링크로 나타나는 웹사이트만 사용 가능

작업	원격 시스템 또는 엔드 유저 요건	사양 또는 사용 제안
네트워크 브라우징 및 파일 관리	공유 원격 액세스에 대해 구성된 파일 권한	클라이언트리스 SSL VPN을 통해 공유 폴더 및 파일에만 액세스할 수 있습니다.
	보호되는 파일 서버에 대한 서버 이름 및 비밀번호	—
	폴더 및 파일이 위치한 도메인, 작업 그룹, 서버 이름	사용자는 조직 네트워크를 통해 자신의 파일을 찾는 방법에 익숙하지 않을 수 있습니다.
	—	복사가 진행 중인 동안 **Copy File to Server** 명령을 중단하거나 다른 화면으로 이동하지 마십시오. 작업을 중단하면 불완전한 파일이 서버에 저장될 수 있습니다.

<table>
<tr><th>작업</th><th>원격 시스템 또는 엔드 유저 요건</th><th>사양 또는 사용 제안</th></tr>
<tr><td rowspan="7">애플리케이션 사용

(포트 전달 또는 애플리케이션 액세스라고도 함)</td><td colspan="2">참고 Mac OS X에서 Safari 브라우저만 이 기능을 지원합니다.</td></tr>
<tr><td colspan="2">참고 이 기능을 사용하려면 Oracle JRE(Java Runtime Environment)를 설치하고 로컬 클라이언트를 구성해야 하며 이를 위해서는 로컬 시스템에 대한 관리자 권한이 필요하므로 사용자가 공용 원격 시스템에서 연결한 경우 애플리케이션을 사용하지 못할 수도 있습니다.</td></tr>
<tr><td colspan="2">사용자는 항상 애플리케이션 사용을 마칠 때 Close 아이콘을 클릭하여 Application Access(애플리케이션 액세스) 창을 닫아야 합니다. 창을 제대로 닫지 못하면 애플리케이션 액세스 또는 애플리케이션 자체에 액세스할 수 없습니다.</td></tr>
<tr><td>클라이언트 애플리케이션이 설치됨</td><td>—</td></tr>
<tr><td>브라우저에서 사용 가능한 쿠키</td><td>—</td></tr>
<tr><td>관리자 권한</td><td>호스트 파일 수정 시 필요하므로 DNS 이름을 사용하여 서버를 지정하는 경우 사용자는 컴퓨터에 대한 관리자 액세스 권한을 지녀야 합니다.</td></tr>
<tr><td>Oracle JRE(Java Runtime Environment)가 설치되어 있습니다.

브라우저에서 JavaScript를 활성화해야 합니다. 기본적으로 활성화되어 있습니다.</td><td>JRE가 설치되지 않은 경우 사용할 수 있는 사이트로 사용자를 안내하는 팝업 창이 표시됩니다.

드문 경우지만 포트 전달 애플릿이 Java 예외 오류로 인해 실패합니다. 이 경우 다음을 수행하십시오.

1. 브라우저 캐시를 지우고 브라우저를 닫습니다.

2. Java 아이콘이 컴퓨터 작업 표시줄에 없는지 확인합니다. Java의 모든 인스턴스를 닫습니다.

3. 클라이언트리스 SSL VPN 세션을 설정하고 포트 전달 Java 애플릿을 실행합니다.</td></tr>
</table>

작업	원격 시스템 또는 엔드 유저 요건	사양 또는 사용 제안
	필요 시 클라이언트 애플리케이션이 구성됨 참고 Microsoft Outlook 클라이언트에는 이 구성 단계가 필요하지 않습니다. 비 Windows 클라이언트 애플리케이션은 모두 구성해야 합니다. Windows 애플리케이션에 구성이 필요한지 판단하려면 Remote Server(원격 서버)의 값을 확인하십시오. • 원격 서버에 서버 호스트 이름이 포함된 경우, 클라이언트 애플리케이션을 구성할 필요가 없습니다. • 원격 서버 필드에 IP 주소가 포함된 경우, 클라이언트 애플리케이션을 구성해야 합니다.	클라이언트 애플리케이션을 구성하려면 서버의 로컬로 매핑된 IP 주소 및 포트 번호를 사용합니다. 이 정보를 찾으려면 다음을 수행하십시오. 1. 원격 시스템에서 클라이언트리스 SSL VPN을 시작하고 클라이언트리스 SSL VPN 홈 페이지에서 Application Access(애플리케이션 액세스) 링크를 클릭합니다. 애플리케이션 액세스 창이 나타납니다. 2. 이름 열에서 사용할 서버의 이름을 찾은 다음 로컬 열에서 해당 클라이언트 IP 주소 및 포트 번호를 식별합니다. 3. 이 IP 주소 및 포트 번호를 사용하여 클라이언트 애플리케이션을 구성합니다. 구성 단계는 클라이언트 애플리케이션마다 다릅니다.
	참고 클라이언트리스 SSL VPN에서 실행 중인 애플리케이션에서 URL(예: 이메일 메시지의 URL)을 클릭해도 클라이언트리스 SSL VPN을 통해 사이트가 열리지 않습니다. 클라이언트리스 SSL VPN에서 사이트를 열려면 URL을 Enter (URL) Address((URL) 주소 입력) 필드에 붙여넣습니다.	
애플리케이션 액세스를 통한 이메일 사용	애플리케이션 액세스에 대한 요건 충족(애플리케이션 사용 참조)	메일을 사용하려면 클라이언트리스 SSL VPN 홈 페이지에서 애플리케이션을 액세스를 시작합니다. 이제 메일 클라이언트를 사용할 수 있습니다.
	참고 IMAP 클라이언트를 사용 중이며 메일 서버 연결이 손실되거나 새 연결을 설정할 수 없는 경우, IMAP 애플리케이션을 닫고 클라이언트리스 SSL VPN을 재시작합니다.	
	기타 이메일 클라이언트	Microsoft Outlook Express 5.5 및 6.0 버전의 테스트는 완료되었습니다.

작업	원격 시스템 또는 엔드 유저 요건	사양 또는 사용 제안
웹 액세스를 통한 이메일 사용	웹 기반 이메일 제품이 설치됨	지원되는 제품은 다음과 같습니다. • Outlook Web Access 최적의 결과를 위해서는 Internet Explorer 8.x 이상 또는 Firefox 8.x 이상에서 OWA를 사용하십시오. • Lotus Notes 다른 웹 기반 이메일 제품도 작동해야 하지만 이는 검증되지 않았습니다.
이메일 프록시를 통한 이메일 사용	SSL 활성화 메일 애플리케이션이 설치됨 ASA SSL 버전을 TLSv1 전용으로 설정하지 마십시오. Outlook 및 Outlook Express는 TLS를 지원하지 않습니다.	지원되는 메일 애플리케이션: • Microsoft Outlook • Microsoft Outlook Express 버전 5.5 및 6.0 다른 SSL 활성화 메일 클라이언트도 작동해야 하지만 이는 검증되지 않았습니다.
	메일 애플리케이션이 구성됨	

클라이언트리스 SSL VPN 데이터 캡처

CLI capture 명령을 사용하여 클라이언트리스 SSL VPN 연결에서 올바르게 표시되지 않는 웹사이트에 대한 정보를 기록할 수 있습니다. 이 데이터는 Cisco 고객 지원 엔지니어가 문제를 해결하는 데 도움이 됩니다. 다음 섹션에서는 캡처 명령을 사용하는 방법에 대해 설명합니다.

• 캡처 파일 만들기, 364 페이지
• 브라우저를 사용하여 캡처 데이터 표시, 364 페이지

참고 클라이언트리스 SSL VPN 캡처를 활성화하면 ASA 성능에 영향을 줍니다. 따라서 문제 해결에 필요한 캡처 파일을 생성한 후에는 캡처를 꺼야 합니다.

캡처 파일 만들기

프로시저

단계 **1** 클라이언트리스 SSL VPN 캡처 유틸리티를 시작하여 패킷을 캡처합니다.

capture *capture-name* **type webvpn user** *csslvpn-username*

- *capture-name*은 캡처에 할당한 이름으로, 캡처 파일의 이름 앞에도 추가됩니다.
- *csslvpn-username*은 캡처하기 위해 일치시킬 사용자 이름입니다.

예제:

```
hostname# capture hr type webvpn user user2
```

단계 **2** **no** 버전의 명령을 사용하여 캡처를 중지합니다.

no capture *capture-name*

예제:

```
hostname# no capture hr
```

캡처 유틸리티는 *capture_name*.zip 파일을 생성하며 이 파일은 비밀번호 **koleso**를 사용하여 암호화됩니다.

단계 **3** 이 .zip 파일을 Cisco로 전송하거나 Cisco TAC 서비스 요청에 첨부합니다.

단계 **4** .zip 파일 내용을 보려면 비밀번호 **koleso**를 사용하여 파일의 압축을 풉니다.

브라우저를 사용하여 캡처 데이터 표시

프로시저

단계 **1** 클라이언트리스 SSL VPN 캡처 유틸리티를 시작합니다.

capture *capture-name* **type webvpn user** *csslvpn-username*

- *capture-name*은 캡처에 할당한 이름으로, 캡처 파일의 이름 앞에도 추가됩니다.
- *csslvpn-username*은 캡처하기 위해 일치시킬 사용자 이름입니다.

예제:

```
hostname# capture hr type webvpn user user2
```

단계 **2** 브라우저를 열고 주소 상자에 다음을 입력합니다.

https://*ASA*의 *IP* 주소 또는 호스트이름**/webvpn_capture.html**

캡처된 내용이 스니퍼 형식으로 표시됩니다.

단계 **3** **no** 버전의 명령을 사용하여 캡처를 중지합니다.

no capture *capture-name*

예제**:**

```
hostname# no capture hr
```

18 장

클라이언트리스 SSL VPN 사용자

비밀번호 관리

비밀번호가 만료될 예정인 경우 선택적으로 엔드 유저에게 경고하도록 ASA를 구성할 수 있습니다.

ASA는 RADIUS 및 LDAP 프로토콜에 대한 비밀번호 관리를 지원합니다. “password-expire-in-days" 옵션은 LDAP에 대해서만 지원됩니다.

IPsec 원격 액세스 및 SSL VPN 터널 그룹에 대해 비밀번호 관리를 구성할 수 있습니다.

비밀번호 관리를 구성하는 경우, ASA는 로그인 시 원격 사용자에게 사용자의 현재 비밀번호가 만료 예정이거나 이미 만료되었음을 알립니다. 그런 다음 ASA에서는 사용자에게 비밀번호를 변경할 기회를 제공합니다. 현재 비밀번호가 아직 만료되지 않은 경우, 사용자는 이 비밀번호를 사용하여 계속 로그인할 수 있습니다.

이 명령은 이러한 알림을 지원하는 AAA 서버에 유효합니다.

ASA 릴리스 7.1 이상에서는 MS-CHAPv2를 지원하는 RADIUS 구성 또는 LDAP로 인증할 때 일반적으로 다음 연결 유형에 대한 비밀번호 관리를 지원합니다.

- AnyConnect VPN 클라이언트
- IPsec VPN Client
- 클라이언트리스 SSL VPN

RADIUS 서버(예: Cisco ACS)는 인증 요청을 다른 인증 서버로 프록시할 수 있습니다. 그러나 ASA 관점에서 보면 RADIUS 서버와만 통신하는 것입니다.

시작하기 전에

- 기본 LDAP에는 SSL 연결이 필요합니다. LDAP에 대한 비밀번호 관리를 시도하기 전에 LDAP over SSL을 활성화해야 합니다. 기본적으로 LDAP는 포트 636을 사용합니다.
- 인증을 위해 LDAP 디렉토리 서버를 사용 중인 경우, 비밀번호 관리가 Sun Java System Directory Server(이전 이름은 Sun ONE Directory Server) 및 Microsoft Active Directory에서 지원됩니다.
  - Sun - Sun 디렉토리 서버에 액세스하려면 ASA에 구성된 DN이 이 서버의 기본 비밀번호 정책에 액세스할 수 있어야 합니다. 디렉토리 관리자 또는 디렉토리 관리자 권한이 있는 사용자를 DN으로 사용할 것을 권장합니다. 또는 기본 비밀번호 정책에 ACI를 배치할 수 있습니다.
  - Microsoft - Microsoft Active Directory에서 비밀번호 관리를 활성화하려면 LDAP over SSL을 구성해야 합니다.
- MSCHAP를 지원하는 일부 RADIUS 서버는 현재 MSCHAPv2를 지원하지 않습니다. 이 명령에는 MSCHAPv2가 필요하므로 공급업체에 확인하십시오.
- Kerberos/Active Directory(Windows 비밀번호) 또는 NT 4.0 도메인의 이러한 연결 유형에 대해서는 비밀번호 관리가 지원되지 않습니다.
- LDAP의 경우 시중에 출시된 여러 LDAP 서버 전용의 비밀번호 변경 방법이 있습니다. 현재 ASA에서는 Microsoft Active Directory 및 Sun LDAP 서버에만 사용할 수 있는 독점적 비밀번호 관리 로직을 구축하고 있습니다.
- RADIUS 또는 LDAP 인증이 구성되어 있지 않으면 ASA는 이 명령을 무시합니다.

프로시저

단계 **1** **Configuration(**구성**) > Remote Access VPN(**원격 액세스 **VPN) > Clientless SSL VPN Access(**클라이언트리스 **SSL VPN** 액세스**) > Connection Profiles(**연결 프로파일**) > Add or Edit(**추가 또는 수정**) > Advanced(**고급**) > General(**일반**) > Password Management(**비밀번호 관리**)**로 이동합니다.

단계 **2** Enable password management(비밀번호 관리 활성화) 옵션을 클릭합니다.

클라이언트리스 **SSL VPN**에서 단일 로그인 사용

SAML 2.0을 사용하는 **SSO**

SSO 및 **SAML 2.0** 정보

ASA는 클라이언트리스 VPN 엔드 유저가 클라이언트리스 VPN과 프라이빗 네트워크 외부의 다른 SAAS 애플리케이션 사이를 전환할 때 자신의 크리덴셜을 한 번만 입력할 수 있도록 SAML 2.0을 지원합니다.

예를 들어, 엔터프라이즈 고객이 PingIdentity를 SAML IdP(Identity Provider)로 활성화하고 SAML 2.0 SSO가 활성화된 Rally, Salesforce, Oracle OEM, Microsoft ADFS, Onelogin 또는 Dropbox에 어카운트가 있는 경우입니다. SAML 2.0 SSO가 SP(서비스 제공자)로 지원되도록 ASA를 구성하면 엔드 유저가 한 번만 로그인하여 클라이언트리스 VPN을 포함한 이 모든 서비스에 액세스할 수 있습니다.

또한 AnyConnect 4.4 클라이언트가 SAML 2.0을 사용하여 SAAS 기반 애플리케이션에 액세스할 수 있도록 AnyConnect SAML 지원이 추가되었습니다. AnyConnect 4.6에는 이전 릴리스에 통합되어 있던 기본(외부) 브라우저 대신 제공되는 임베디드 브라우저를 포함하는 개선된 버전의 SAML 통합이 도입되었습니다. 내장 브라우저를 포함하여 새롭게 개선된 버전을 사용하려면 AnyConnect 4.6(또는 이상), ASA 9.7.1.24(또는 이상), 9.8.2.28(또는 이상) 또는 9.9.2.1(또는 이상)로 업그레이드해야 합니다.

ASA는 SAML이 터널 그룹, 기본 터널 그룹 또는 기타 그룹에 대한 인증 방법으로 구성되었을 때 SP가 활성화됩니다. 클라이언트리스 VPN 엔드 유저는 활성화된 ASA 또는 SAML IdP에 액세스하여 SSO(Single Sign On)를 시작합니다. 이러한 각 시나리오의 내용은 다음과 같습니다.

SAML SP 시작 **SSO**

엔드 유저가 클라이언트리스 VPN을 사용하여 ASA에 액세스하여 로그인을 시작하는 경우 다음과 같이 로그인 동작이 진행됩니다.

1. 클라이언트리스 VPN 엔드 유저가 SAML 사용 터널 그룹을 액세스하거나 선택하는 경우, 엔드 유저는 인증을 위해 SAML idP로 리디렉션됩니다. 사용자가 그룹 URL에 직접 액세스하는 경우(이 경우 리디렉션이 자동)를 제외하고 사용자에게 메시지가 표시됩니다.

   ASA는 브라우저에서 SAML IdP로 리디렉션하는 SAML 인증 요청을 생성합니다.

2. IdP에서 엔드 유저에게 크리덴셜을 요구하고 엔드 유저는 로그인합니다. 입력한 크리덴셜은 IdP 인증 구성을 충족해야 합니다.

3. IdP 응답이 브라우저에 다시 전송되고 ASA의 로그인 URL에 게시됩니다. ASA는 로그인을 완료하는 응답을 확인합니다.

SAML IdP 시작 **SSL**

사용자가 IdP에 액세스하여 로그인을 시작하는 경우 다음과 같이 로그인 동작이 진행됩니다.

1. 엔드 유저는 IdP에 액세스합니다. IdP는 IdP의 인증 구성에 따라 엔드 유저에게 크리덴셜을 요구합니다. 엔드 유저는 크리덴셜을 제출하고 IdP에 로그인합니다.
2. 일반적으로, 엔드 유저는 IdP로 구성된 SAML 사용 서비스 목록을 가져옵니다. 엔드 유저는 ASA를 선택합니다.
3. SAML 응답이 브라우저에 다시 전송되고 ASA의 로그인 URL에 게시됩니다. ASA는 로그인을 완료하는 응답을 확인합니다.

CoT(Circle of Trust)

ASA와 SAML IdP(Identity Provider) 간의 신뢰 관계는 구성된 인증서(ASA 트러스트 포인트)를 통해 설정되어야 합니다.

엔드 유저와 SAML IdP(Identity Provider) 간의 신뢰 관계는 IdP에 구성된 인증을 통해 설정됩니다.

SAML 시간 제한

SAML 어설션에는 다음과 같은 NotBefore 및 NotOnOrAfter가 있습니다. <saml:Conditions NotBefore="2015-03-10T19:47:41Z" NotOnOrAfter="2015-03-10T20:47:41Z">

ASA에 구성된 SAML 시간 제한은 NotBefore 및 시간 제한의 합계가 NotOnOrAfter보다 빠르면 NotOnOrAfter를 재정의합니다. NotBefore + 시간 제한이 NotOnOrAfter보다 느리면 NotOnOrAfter가 적용됩니다.

시간 제한은 시간 제한 이후에 어설션이 다시 사용되지 못하도록 매우 짧아야 합니다. SAML 기능을 사용하려면 ASA의 NTP(Network Time Protocol) 서버와 IdP NTP 서버를 동기화해야 합니다.

프라이빗 네트워크에서의 지원

SAML 2.0 기반 서비스 공급자 IdP는 프라이빗 네트워크에서 지원됩니다. SAML IdP를 프라이빗 클라우드에 구축할 경우, ASA 및 기타 SAML 사용 서비스는 피어 위치에 있거나 모두 프라이빗 네트워크에 있게 됩니다. 사용자와 서비스 간의 게이트웨이로 ASA를 사용할 경우, IdP에서의 인증이 제한된 익명 webvpn 세션과 함께 처리되며 IdP와 사용자 간의 모든 트래픽이 변환됩니다. 사용자가 로그인할 때 ASA는 해당하는 속성이 있는 세션을 수정하고 IdP 세션을 저장합니다. 이 경우, 크리덴셜을 다시 입력하지 않고 프라이빗 네트워크에서 서비스 제공자를 사용할 수 있습니다.

SAML IdP *NameID* 속성은 사용자의 사용자 이름을 확인하며 권한 부여, 계정 관리 및 VPN 세션 데이터베이스에 사용됩니다.

참고 프라이빗 및 퍼블릭 네트워크 간에 인증 정보를 교환할 수 없습니다. 모두 내부 및 외부 서비스 제공자에 대해 모두 동일한 IdP를 사용하는 경우 개별적으로 인증해야 합니다. 외부 서비스와 내부 전용 IdP를 함께 사용할 수 없습니다. 외부 전용 IdP는 프라이빗 네트워크의 서비스 제공자와 함께 사용할 수 없습니다.

SAML 2.0에 대한 지침 및 제한 사항

- SAML 2.0 SSO는 클라이언트리스 VPN 기능을 지원하므로 다음과 같이 클라이언트리스 VPN와 동일한 제한 및 허용 사항이 있습니다.
  - 다중 컨텍스트 모드 및 로드 밸런싱은 지원되지 않습니다.
  - 액티브/스탠바이 페일오버는 지원되지만 액티브/액티브 페일오버는 지원되지 않습니다.
  - IPv4 및 IPv6 세션은 지원됩니다.
- ASA는 모든 SAML Idp에서 지원되는 SAML 2.0 Redirect-POST 바인딩을 지원합니다.
- ASA는 SAML SP로만 작동합니다. ASA는 게이트웨이 모드 또는 피어 모드의 IdP로 작동할 수 없습니다.
- 이 SAML SSO SP 기능은 함께 사용할 수 없는 인증 방법입니다. AAA 및 인증서와 함께 사용할 수 없습니다.
- 사용자 이름/비밀번호 인증, 인증서 인증 및 KCD를 기반으로 하는 기능은 지원되지 않습니다. 예를 들어, 인스턴스, 사용자 이름/비밀번호 사전 채우기 기능, 양식 기반 자동 로그인, 매크로 대체 기반 자동 로그인, KCD SSO 등이 있습니다.
- DAP는 SAML 지원 터널 그룹에 대해 지원되지 않습니다.
- 기존 클라이언트리스 VPN 시간 제한 설정은 SAML 세션에 여전히 적용됩니다.
- ASA 관리자는 인증 어설션 및 적절한 시간 제한 동작을 올바르게 처리하기 위해 ASA와 SAML IdP 간의 클럭 동기화를 확인해야 합니다.
- ASA 관리자는 다음 사항을 고려하면서 ASA와 IdP에 모두 유효한 서명 인증서를 유지해야 합니다.
  - IdP 서명 인증서는 ASA에서 IdP를 구성하는 경우 필수입니다.
  - ASA는 IdP에서 수신된 서명 인증서에 대해서는 해지 확인을 하지 않습니다.
- SAML 어설션에는 NotBefore 및 NotOnOrAfter 조건이 있습니다. ASA SAML에서 구성된 시간 제한은 이러한 조건과 다음과 같이 상호 작용합니다.
  - 시간 제한은 NotBefore 및 시간 제한의 합계가 NotOnOrAfter보다 빠르면 NotOnOrAfter를 재정의합니다.
  - NotBefore + 시간 제한이 NotOnOrAfter보다 느리면 NotOnOrAfter가 적용됩니다.
  - NotBefore 속성이 없는 경우 ASA는 로그인 요청을 거부합니다. NotOnOrAfter 속성이 없으며 SAML 시간 제한이 설정되지 않은 경우 ASA는 로그인 요청을 거부합니다.
- AnyConnect를 통해 SAML을 사용할 경우, 다음과 같은 추가 지침을 따릅니다.
  - 신뢰할 수 없는 서버 인증서는 내장 브라우저에서 허용되지 않습니다.
  - CLI 또는 SBL 모드에서는 임베디드 브라우저 SAML 통합이 지원되지 않습니다.

- 웹 브라우저에서 설정된 SAML 인증은 AnyConnect와 공유되지 않으며 반대의 경우도 마찬가지입니다.
- 구성에 따라 임베디드 브라우저가 포함된 헤드엔드에 연결할 때는 다양한 방법이 사용됩니다. 예를 들어 AnyConnect의 경우 IPv6 연결보다 IPv4 연결이 기본적으로 사용될 수 있는 반면 임베디드 브라우저의 경우 IPv6이 기본적으로 사용될 수도 있고 그 반대의 방식이 적용될 수도 있습니다. 마찬가지로 AnyConnect는 프록시 사용을 시도한 후 장애가 발생하면 프록시 없음으로 대체할 수 있는 반면 임베디드 브라우저의 경우에는 프록시 사용을 시도한 후 장애가 발생하면 탐색을 중지할 수 있습니다.
- SAML 기능을 사용하려면 ASA의 NTP(Network Time Protocol) 서버와 IdP NTP 서버를 동기화해야 합니다.
- ASDM의 VPN 마법사는 현재 SAML 구성을 지원하지 않습니다.
- 내부 IdP를 사용하여 로그인한 후에는 SSO를 사용하여 내부 서버에 액세스할 수 없습니다.
- SAML IdP NameID 속성은 사용자의 사용자 이름을 확인하며 권한 부여, 계정 관리 및 VPN 세션 데이터베이스에 사용됩니다.

SAML 2.0 IdP(Identity Provider) 구성

시작하기 전에

SAML IdP(Identity Provider)용 로그인 및 로그아웃 URL을 가져옵니다. IdP의 웹사이트에서 URL을 가져오거나 이러한 URL의 메타데이터 파일에서 해당 정보를 얻을 수 있습니다.

프로시저

단계 **1** (선택 사항) IdP가 내부 네트워크인지를 결정하는 플래그를 설정하려면 **internal** 명령을 사용합니다. 그런 다음 ASA는 게이트웨이 모드로 작동합니다.

단계 **2** **forceauthn**을 사용하는 경우 SAML 인증 요청이 발생하면 IdP(Identity Provider)가 이전의 보안 컨텍스트에 의존하는 대신 직접 인증하게 됩니다. 이 설정은 기본값입니다. 따라서 비활성화하려면 **no forceauthn**을 사용합니다.

단계 **3** ASDM에서 **Configuration(**구성**) > Remote Access VPN(**원격 액세스 **VPN) > Clientless SSL VPN Access(**클라이언트리스 **SSL VPN) > Advanced(**고급**) > Single Sign On Servers(SSO(Single Sign On)** 서버**)**로 이동합니다.

이전에 구성한 모든 SAML 2.0 IdP가 여기에 나열되며 **Add(**추가**)** 또는 **Delete(**삭제**)**를 위해 다음에 설명된 것과 같이 **Edit(**수정**)**할 수 있습니다.

단계 **4** 새 IdP 엔터티를 추가하려면 **Add(**추가**)**를 클릭합니다.

단계 **5** 아래 설명에 따라 다음 필드에 내용을 입력합니다.

- **Sign In URL(**로그인 **URL)** — IdP에 서명할 때 사용할 URL입니다. URL 값은 4~500자를 포함해야 합니다.

- **Sign Out URL(**로그아웃 **URL)** — (선택 사항) IdP에서 로그아웃할 때 리디렉션하기 위한 URL입니다. Url 값은 4~500자를 포함해야 합니다.
- **Base URL(**기본 **URL)** — (선택 사항) 이 URL은 엔드 유저가 ASA로 다시 리디렉션하도록 서드 파티 IdP에 제공됩니다.

  기본 URL이 구성되어 있는 경우, **show saml metadata**에서 AssertionConsumerService 및 SingleLogoutService 속성의 기본 URL로 사용합니다.

  기본 URL이 구성되어 있지 않은 경우, URL은 ASA의 호스트 이름 및 도메인 이름에 따라 결정됩니다. 예를 들어, 호스트 이름이 `ssl-vpn`이며 도메인 이름이 `cisco.com`인 경우 `https://ssl-vpn.cisco.com`을 사용합니다.

  show saml metadata를 입력할 때 기본 URL이나 호스트 이름/도메인 이름이 구성되어 있지 않은 경우, 오류가 발생합니다.
- **Identity Provider Certificate(IdP(Identity Provider)** 인증서**)** — SAML 어설션을 확인하려면 ASA의 IdP 인증서를 포함하는 트러스트 포인트를 지정합니다. 이전에 구성한 트러스트 포인트를 선택합니다.
- **Service Provider Certificate(**서비스 제공자 인증서**)** — (선택 사항) ASA의 서명 또는 암호화된 SAML 어설션을 확인하려면 ASA(SP)의 IdP용 인증서를 포함하는 신뢰 지점을 지정합니다. 이전에 구성한 트러스트 포인트를 선택합니다.
- **Request Signature(**서명 요청**)** — 드롭다운을 사용하여 SAML IdP 서버에 대해 선호하는 서명 방법을 선택합니다. rsa-sha1, rsa-sha256, rsa-sha384 또는 rsa-sha512를 선택할 수 있습니다.
- **Request Timeout(**요청 시간 제한**)** — (선택 사항) SAML 요청의 시간 제한입니다.

  이 옵션이 지정된 경우, NotBefore 및 timeout-in-seconds의 합계가 NotOnOrAfter보다 빠르다면 NotOnOrAfter를 재정의합니다.

  이 구성이 지정되지 않은 경우, 어설션에서 NotBefore 및 NotOnOrAfter가 유효성을 확인하는 데 사용됩니다.
- **Enable the Signature(**서명 활성화**)** — SAML 요청에서 서명을 활성화 또는 비활성화(기본 설정)합니다.
- **Enable the Internal(**내부 활성화**)** — IdP가 내부 네트워크에 있는지 여부를 확인하려면 활성화 또는 비활성화(기본 설정)합니다.

  참고 내부 IdP를 사용하여 로그인한 후에는 SSO를 사용하여 내부 서버에 액세스할 수 없습니다.
- Enable the Force Re-authentication(강제 재인증 활성화) — SAML 인증 요청이 발생하는 경우, 이 설정이 활성화되어 있으면 IdP(Identity Provider)가 이전의 보안 컨텍스트에 의존하는 대신 직접 인증하게 됩니다. 강제 재인증 활성화가 기본값입니다.

단계 **6** **OK(**확인**)**를 클릭합니다.
새 IdP 엔터티가 이 페이지에 나열됩니다.

예

다음 웹 페이지는 Onelogin을 위한 URL을 얻는 방법의 예를 보여 줍니다.

https://onelogin.zendesk.com/hc/en-us/articles/202767260-Configuring-SAML-for-Clarizen

다음 웹 페이지는 메타데이터를 사용하여 OneLogin에서 URL을 찾을 수 있는 방법의 예입니다.

http://onlinehelp.tableau.com/current/online/en-us/saml_config_onelogin.htm

다음에 수행할 작업

ASA를 SAML 2.0 서비스 제공자(SP)로 구성, 374 페이지에 설명된 대로 연결 프로필에 SAML 인증을 적용합니다.

ASA를 SAML 2.0 서비스 제공자(SP)로 구성

특정 터널 그룹을 SAML SP로 구성하려면 이 절차를 수행합니다.

참고 AnyConnect 4.4 또는 4.5를 통한 SAML 인증을 사용하면서 ASA 버전 9.7.1.24(또는 이상), 9.8.2.28(또는 이상) 또는 9.9.2.1(또는 이상)(릴리스 날짜: 2018년 4월 18일)을 구축하는 경우, 기본 SAML 동작은 내장된 브라우저이며 이는 AnyConnect 4.4 및 4.5에서 지원되지 않습니다. 따라서 AnyConnect 4.4 및 4.5 클라이언트가 외부(기본) 브라우저를 사용하는 SAML로 인증할 수 있으려면 Connection Profiles(연결 프로필) 영역에서 **SAML External Browser(SAML** 외부 브라우저**)** 체크 박스를 활성화해야 합니다.

SAML External Browser(SAML 외부 브라우저**)** 체크 박스는 AnyConnect 4.6 이상으로 업그레이드하는 사용자가 마이그레이션을 하려고 할 때 사용합니다. 보안 제한이 있으므로, 이 솔루션을 AnyConnect 소프트웨어를 업그레이드하는 동안의 임시 마이그레이션 방편으로만 사용하십시오. 이 체크 박스는 나중에는 사용되지 않습니다.

프로시저

단계 **1** ASDM에서 **Configuration(**구성**) > Remote Access VPN(**원격 액세스 **VPN) > Clientless SSL VPN Access(**클라이언트리스 **SSL VPN** 액세스**) > Connection Profiles(**연결 프로필**) > Add/Edit(**추가/수정**)**으로 이동합니다.

단계 **2** 이 터널 그룹에 대해 **Saml**을 인증 방법으로 선택합니다.

단계 **3** **SAML Identity Provider(SAML IdP(Identity Provider))** 섹션에서 이전에 구성한 **SAML Server(SAML** 서버**)**를 선택하거나 새 서버를 추가하려면 **Manage(**관리**)**를 클릭합니다.
기존 SAML 구성을 수정한 경우 이 작업으로 인해 터널 그룹에 대해 IdP가 다시 활성화됩니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

수락한 변경 사항을 기반으로 어떤 CLI 명령이 생성되었는지 알려 주는 Preview CLI Commands(CLI 명령 미리보기) 창이 나타납니다. 그런 다음 **Send(**전송**)**를 클릭하여 ASA에 명령을 전송할 수 있습니다.

자동 로그인 사용

Auto Sign-on(자동 로그온) 창 또는 탭에서 클라이언트리스 SSL VPN 사용자를 위한 자동 로그온을 구성하거나 수정할 수 있습니다. 자동 로그온은 내부 네트워크에 이미 배치된 SSO 방법이 없는 경우, 사용할 수 있는 간소화된 단일 로그인 방법입니다. 특정 내부 서버에 대해 자동 로그인이 구성된 경우 ASA는 ASA에 로그온하기 위해 클라이언트리스 SSL VPN 사용자가 입력한 로그인 크리덴셜(사용자 이름 및 비밀번호)을 이 특정 내부 서버에 전달합니다. ASA가 특정 범위의 서버에 대해 지정된 인증 방법에 응답하도록 구성합니다. ASA가 응답하도록 구성할 수 있는 인증 방법에는 기본(HTTP), NTLM, FTP 및 CIFS가 있으며, 모든 방법을 사용하도록 할 수도 있습니다.

사용자 이름 및 비밀번호의 조회가 ASA에서 실패하는 경우, 빈 문자열이 대체되며 자동 로그온을 사용할 수 없는 경우와 마찬가지로 동작이 다시 변환됩니다.

자동 로그온은 특정한 내부 서버에 대해 SSO를 구성하기 위한 간단한 방법입니다. 이 섹션에서는 자동 로그온을 통해 SSO를 설정하는 절차에 대해 설명합니다.

다음 필드가 표시됩니다.

- IP Address(IP 주소) — 뒤에 오는 마스크와 함께, 인증할 서버의 IP 주소 범위를 Add/Edit Auto Sign-on(자동 로그온 추가/수정) 대화 상자를 사용하여 구성된 대로 표시합니다. 서버 URI 또는 서버 IP 주소 및 마스크 중 하나를 사용하여 서버를 지정할 수 있습니다.
- Mask(마스크) — 앞의 IP 주소와 함께, 자동 로그온 추가/수정 대화 상자를 사용하여 자동 로그온을 지원하도록 구성된 서버의 IP 주소 범위를 표시합니다.
- URI — 자동 로그온 추가/수정 대화 상자를 사용하여 구성된 서버를 식별하는 URI 마스크를 표시합니다.
- Authentication Type(인증 유형) — 자동 로그온 추가/수정 대화 상자를 사용하여 구성된 대로 기본(HTTP), NTLM, FTP 및 CIFS 또는 이 모든 방법의 인증 유형을 표시합니다.

시작하기 전에

- 인증이 필요하지 않거나 ASA와 다른 크리덴셜을 사용하는 서버에 대해 자동 로그인을 활성화하지 마십시오. 자동 로그인이 활성화된 경우 ASA는 사용자 스토리지에 어떤 크리덴셜이 있는지 관계없이 ASA에 로그인하기 위해 사용자가 입력한 로그인 크리덴셜을 전달합니다.
- 특정 범위의 서버 대해 한 가지 방법(예: HTTP 기본)을 구성한 후 해당 서버 중 하나에서 다른 방법(예: NTLM)을 사용하여 인증을 시도하는 경우, ASA는 사용자 로그인 크리덴셜을 해당 서버에 전달하지 않습니다.

프로시저

단계 **1** 자동 로그온 명령 추가 또는 수정을 클릭합니다. 자동 로그온 명령은 자동 로그온 기능 및 특정 인증 방법을 사용하여 다양한 내부 서버를 정의합니다.

단계 **2** 자동 로그온 테이블에서 선택한 자동 로그온 명령 삭제를 클릭합니다.

단계 **3** IP 주소 및 마스크를 사용하여 다양한 내부 서버를 지정하려면 **IP Block(IP** 차단**)**을 클릭합니다.

- IP Address(IP 주소) — 자동 로그온을 구성 중인 범위에 있는 첫 번째 서버의 IP 주소를 입력합니다.
- Mask(마스크) — 서브넷 마스크 메뉴에서 자동 로그온을 지원하는 서버의 서버 주소 범위를 정의하는 서브넷 마스크를 선택합니다.

단계 **4** URI를 클릭하여 URI를 통해 자동 로그온을 지원하는 서버를 지정한 다음 이 URI를 이 버튼 옆에 있는 필드에 입력합니다.

단계 **5** 서버에 할당된 인증 방법을 결정합니다. 지정된 범위의 서버에 대해 기본 HTTP 인증 요청, NTLM 인증 요청, FTP 및 CIFS 인증 요청에 응답하도록 ASA를 구성할 수 있으며, 이 모든 방법을 사용하는 요청에 응답하도록 구성할 수도 있습니다.

- Basic(기본) — 서버가 기본(HTTP) 인증을 지원하는 경우 이 버튼을 클릭합니다.
- NTLM — 서버가 NTLMv1 인증을 지원하는 경우 이 버튼을 클릭합니다.
- FTP/CIFS — 서버가 FTP 및 CIFS 인증을 지원하는 경우 이 버튼을 클릭합니다.
- Basic, NTLM and FTP/CIFS — 서버가 위의 모든 인증을 지원하는 경우 이 버튼을 클릭합니다.

사용자 이름 및 비밀번호 요건

네트워크에 따라 원격 세션 동안 사용자는 컴퓨터, 인터넷 서비스 공급자, 클라이언트리스 SSL VPN, 메일 또는 파일 서버 또는 기업 애플리케이션 중 하나 또는 모두에 로그온해야 할 수 있습니다. 사용자는 고유한 사용자 이름 및 비밀번호 또는 PIN 같은 다양한 정보가 필요한 여러 가지 다른 상황에서 인증해야 할 수 있습니다. 다음 표에서는 클라이언트리스 SSL VPN 사용자가 알아야 할 사용자 이름 및 비밀번호 유형을 보여줍니다.

로그인 사용자 이름**/**비밀 번호 유형		입력 시기
컴퓨터	컴퓨터 액세스	컴퓨터 시작 시
인터넷 서비스 공급자	인터넷 액세스	인터넷 서비스 공급자에 연결 시
클라이언트리스 SSL VPN	원격 네트워크 액세스	클라이언트리스 SSL VPN 시작

로그인 사용자 이름/비밀 번호 유형		입력 시기
파일 서버	원격 파일 서버 액세스	원격 파일 서버에 액세스하기 위해 클라이언트리스 SSL VPN 파일 브라우징 기능 사용 시
기업 애플리케이션 로그인	방화벽 보호 내부 서버 액세스	내부의 보호되는 웹 사이트에 액세스하기 위해 클라이언트리스 SSL VPN 웹 브라우징 기능 사용 시
메일 서버	클라이언트리스 SSL VPN을 통한 원격 메일 서버 액세스	이메일 메시지 전송 또는 수신 시

보안 팁 전달

사용자에게 항상 툴바에서 로그아웃 아이콘을 클릭하여 클라이언트리스 SSL VPN 세션을 닫도록 알려주십시오. (브라우저 창을 닫아도 세션은 닫히지 않습니다.)

클라이언트리스 SSL VPN은 원격 PC 또는 워크스테이션과 기업 네트워크에 있는 ASA 간의 데이터 전송 보안을 보장합니다. 클라이언트리스 SSL VPN을 사용하는 사용자에게 모든 사이트와의 통신 보안이 보장되지는 않음을 알려주십시오. 사용자가 인터넷 또는 내부 네트워크에 있는 비 HTTPS 웹 리소스에 액세스하는 경우에는 기업 ASA에서 대상 웹 서버로의 통신은 암호화되지 않으므로 개별적인 통신이 아닙니다.

클라이언트리스 SSL VPN 기능을 사용하도록 원격 시스템 구성

이 섹션에서는 클라이언트리스 SSL VPN을 사용하도록 원격 시스템을 설정하는 방법에 대해 설명합니다.

- 이메일 프록시를 통한 이메일 사용, 383 페이지
- 스마트 터널 사용, 383 페이지

사용자 어카운트를 다르게 구성할 수 있으며 다른 클라이언트리스 SSL VPN 기능을 개별 사용자가 사용할 수 있습니다.

클라이언트리스 SSL VPN 정보

다음을 비롯한 지원되는 모든 연결을 사용하여 인터넷에 연결할 수 있습니다.

- 홈 DSL, 케이블 또는 다이얼업
- 공용 키오스크
- 호텔 핫스팟
- 공항 무선 노드
- 인터넷 카페

참고 클라이언트리스 SSL VPN에서 지원되는 웹 브라우저 목록에 대해서는 지원되는 VPN 플랫폼, Cisco ASA 5500 Series의 내용을 참고하십시오.

클라이언트리스 SSL VPN에 대한 사전 요구 사항

- 쿠키는 포트 전달을 통한 애플리케이션 액세스를 위해 브라우저에서 활성화되어야 합니다.
- 클라이언트리스 SSL VPN의 URL이 있어야 합니다. URL은 https://*address* 형식의 https 주소여야 하며, 여기서 *address*는 SSL VPN이 활성화된 ASA(또는 로드 밸런싱 클러스터) 인터페이스의 IP 주소 또는 DNS 호스트 이름입니다. 예를 들어, https://cisco.example.com입니다.
- 클라이언트리스 SSL VPN 사용자 이름과 비밀번호가 있어야 합니다.

참고 클라이언트리스 SSL VPN은 로컬 인쇄를 지원하지만 기업 네트워크에 있는 프린터에 대해 VPN을 통한 인쇄는 지원하지 않습니다.

클라이언트리스 SSL VPN 부동 툴바 사용

부동 툴바를 사용하면 클라이언트리스 SSL VPN 사용을 간소화할 수 있습니다. 툴바를 사용하여 URL을 입력하고 파일 위치를 찾아보며 기본 브라우저 창에 방해되지 않게 사전 구성된 웹 연결을 선택할 수 있습니다.

부동 툴바는 현재의 클라이언트리스 SSL VPN 세션을 나타냅니다. **Close** 버튼을 클릭하면 ASA에서 클라이언트리스 SSL VPN 세션을 종료하라는 메시지를 표시합니다.

팁 텍스트를 텍스트 필드에 붙여넣으려면 Ctrl-V를 사용합니다. (마우스 오른쪽 버튼 클릭 기능은 클라이언트리스 SSL VPN 세션 중에 표시되는 툴바에서 꺼집니다.)

참고 팝업을 차단하도록 브라우저를 구성한 경우 부동 툴바를 표시할 수 없습니다.

웹 브라우징

클라이언트리스 SSL VPN의 사용이 모든 사이트와의 통신 보안을 보장하는 것은 아닙니다. 보안 팁 전달, 377 페이지를 참고하십시오.

클라이언트리스 SSL VPN을 통한 웹 브라우징의 모양과 느낌은 사용자에게 익숙하지 않을 수 있습니다. 예를 들면 다음과 같습니다.

- 클라이언트리스 SSL VPN의 제목 표시줄은 각각의 웹 페이지 위에 나타납니다.
- 다음 방법으로 웹사이트에 액세스합니다.
  - 클라이언트리스 SSL VPN 홈 페이지의 **Enter Web Address(**웹 주소 입력**)** 필드에서 URL 입력
  - 클라이언트리스 SSL VPN 홈 페이지의 사전 구성 웹사이트 링크 클릭
  - 앞의 두 가지 방법 중 하나를 통해 액세스되는 웹 페이지에서 링크 클릭
  - 보호 웹사이트에 대한 사용자 이름 및 비밀번호가 필요합니다.

특정 어카운트를 구성하는 방법에 따라 다음과 같은 결과가 발생할 수 있습니다.

- 일부 웹사이트가 차단됨
- 클라이언트리스 SSL VPN 홈 페이지에서 링크로 나타나는 웹사이트만 사용 가능

또한 특정한 어카운트를 구성한 방법에 따라 다음과 같을 수도 있습니다.

- 일부 웹사이트가 차단됨
- 클라이언트리스 SSL VPN 홈 페이지에서 링크로 나타나는 웹사이트만 사용 가능

네트워크 브라우징(파일 관리)

사용자는 조직 네트워크를 통해 자신의 파일을 찾는 방법에 익숙하지 않을 수 있습니다.

참고 복사가 진행 중인 동안 **Copy File to Server** 명령을 중단하거나 다른 화면으로 이동하지 마십시오. 작업을 중단하면 불완전한 파일이 서버에 저장될 수 있습니다.

다음 사항을 기억하는 것이 중요합니다.

- 공유 원격 액세스를 위한 파일 권한을 구성해야 합니다.
- 보호 파일 서버에 대해 서버 이름 및 비밀번호가 있어야 합니다.
- 폴더 및 파일이 위치한 도메인, 작업 그룹 및 서버 이름이 있어야 합니다.

참고 클라이언트리스 SSL VPN을 통해 공유 폴더 및 파일에만 액세스할 수 있습니다.

원격 파일 탐색기 사용

원격 파일 탐색기는 웹 브라우저에서 기업 네트워크를 찾아보는 방법을 사용자에게 제공합니다. 사용자가 Cisco SSL VPN 포털 페이지에서 원격 파일 시스템 아이콘을 클릭하면 트리 및 폴더 보기로 원격 파일 시스템을 표시하는 사용자 시스템에서 애플릿이 실행됩니다.

참고 이 기능을 사용하려면 Oracle JRE(Java Runtime Environment)가 사용자 컴퓨터에 설치되어 있어야 하며 Java가 웹 브라우저에 활성화되어 있어야 합니다. 원격 파일을 실행하려면 JRE 1.6 이상이 필요합니다.

브라우저에서 사용자는 다음을 수행할 수 있습니다.

- 원격 파일 시스템 찾아보기
- 파일 이름 바꾸기
- 원격 파일 시스템 내에서 원격 및 로컬 파일 시스템 간에 파일 이동 또는 복사
- 파일의 대용량 업로드 및 다운로드

  브라우저에서 파일을 클릭한 후 Operations(작업) > Download(다운로드)를 선택하고 Save(저장) 대화 상자에서 파일을 저장할 위치 및 이름을 제공하여 파일을 다운로드할 수 있습니다.

  대상 폴더를 클릭한 후 Operations(작업) > Upload(업로드)를 선택하고 Open(열기) 대화 상자에서 파일의 위치 및 이름을 제공하여 파일을 업로드할 수 있습니다.

  이 기능에는 다음과 같은 제한 사항이 있습니다.

  - 사용자는 액세스가 허용되지 않는 하위 폴더를 볼 수 없습니다.
  - 사용자 액세스가 허용되지 않는 파일은 브라우저에 표시되는 경우에도 이동하거나 복사할 수 없습니다.

- 중첩된 폴더의 최대 깊이는 32입니다.
- 트리 보기는 끌어 놓기 복사 방법을 지원하지 않습니다.
- 파일을 원격 파일 탐색기의 여러 인스턴스 간에 이동하는 경우 모든 인스턴스는 동일한 서버(root 공유)를 탐색 중이어야 합니다.
- 원격 파일 탐색기는 최대 1500개의 파일 및 폴더를 단일 폴더에서 표시할 수 있습니다. 폴더가 이 한계를 초과하는 경우 표시할 수 없습니다.

포트 전달 사용

포트 포워딩을 사용하려면 서버의 로컬로 매핑된 IP 주소 및 포트 번호를 사용하여 클라이언트 애플리케이션을 구성해야 합니다.

- 사용자는 항상 애플리케이션 사용을 마칠 때 **Close** 아이콘을 클릭하여 애플리케이션 액세스 창을 닫아야 합니다. 창을 제대로 종료하지 못하면 애플리케이션 액세스 또는 애플리케이션 자체가 해제될 수 있습니다.

시작하기 전에

- Mac OS X에서 Safari 브라우저만 이 기능을 지원합니다.
- 클라이언트 애플리케이션이 설치되어 있어야 합니다.
- 브라우저에서 쿠키를 활성화해야 합니다.
- 호스트 파일 수정 시 필요하므로 DNS 이름을 사용하여 서버를 지정하는 경우 PC에서 관리자 액세스 권한이 있어야 합니다.
- Oracle JRE(Java Runtime Environment)가 설치되어 있어야 합니다.

  JRE가 설치되지 않은 경우 사용할 수 있는 사이트로 사용자를 안내하는 팝업 창이 표시됩니다. 드문 경우지만 포트 전달 애플릿이 Java 예외 오류로 인해 실패합니다. 이 경우 다음을 수행하십시오.

  1. 브라우저 캐시를 지우고 브라우저를 닫습니다.
  2. Java 아이콘이 컴퓨터 작업 표시줄에 없는지 확인합니다.
  3. Java의 모든 인스턴스를 닫습니다.
  4. 클라이언트리스 SSL VPN 세션을 설정하고 포트 전달 Java 애플릿을 실행합니다.
- 브라우저에서 JavaScript를 활성화해야 합니다. 기본적으로 활성화되어 있습니다.
- 필요 시 클라이언트 애플리케이션을 구성해야 합니다.

참고 Microsoft Outlook 클라이언트에는 이 구성 단계가 필요하지 않습니다. 비 Windows 클라이언트 애플리케이션은 모두 구성해야 합니다. Windows 애플리케이션에 구성이 필요한지를 판단하려면 Remote Server(원격 서버) 필드의 값을 확인하십시오. 원격 서버 필드에 서버 호스트 이름이 포함된 경우, 클라이언트 애플리케이션을 구성할 필요가 없습니다. 원격 서버 필드에 IP 주소가 포함된 경우, 클라이언트 애플리케이션을 구성해야 합니다.

프로시저

단계 **1** 클라이언트리스 SSL VPN 세션을 시작하고 홈 페이지에서 **Application Access(**애플리케이션 액세스**)** 링크를 클릭합니다. 애플리케이션 액세스 창이 나타납니다.

단계 **2** 이름 열에서 사용할 서버의 이름을 찾은 다음 로컬 열에서 해당 클라이언트 IP 주소 및 포트 번호를 식별합니다.

단계 **3** 이 IP 주소 및 포트 번호를 사용하여 클라이언트 애플리케이션을 구성합니다. 구성 단계는 클라이언트 애플리케이션마다 다릅니다.

참고 클라이언트리스 SSL VPN 세션에서 실행 중인 애플리케이션에서 URL(예: 이메일 메시지의 URL)을 클릭해도 해당 세션에 사이트가 열리지 않습니다. 세션에서 사이트를 열려면 URL을 Enter Clientless SSL VPN(URL) Address(클라이언트리스 SSL VPN(URL) 주소 입력) 필드에 붙여 넣습니다.

포트 전달을 통한 이메일 사용

메일을 사용하려면 클라이언트리스 SSL VPN 홈 페이지에서 애플리케이션을 액세스를 시작합니다. 이제 메일 클라이언트를 사용할 수 있습니다.

참고 IMAP 클라이언트를 사용 중이며 메일 서버 연결이 손실되거나 새 연결을 설정할 수 없는 경우, IMAP 애플리케이션을 닫고 클라이언트리스 SSL VPN을 재시작합니다.

애플리케이션 액세스 및 기타 메일 클라이언트의 요건을 모두 충족해야 합니다.

Microsoft Outlook Express 5.5 및 6.0 버전의 테스트는 완료되었습니다.

웹 액세스를 통한 이메일 사용

다음 이메일 애플리케이션이 지원됩니다.

- Exchange Server 2010에 대한 Microsoft Outlook Web App

OWA에는 Internet Explorer 7 이상 또는 Firefox 3.01 이상이 필요합니다.

- Exchange Server 2007, 2003 및 2000에 대한 Microsoft Outlook Web Access

  최적의 결과를 위해 Internet Explorer 8.x 이상 또는 Firefox 8.x 이상에서 OWA를 사용하십시오.

- Lotus iNotes

참고 웹 기반 이메일 제품이 설치되어 있어야 하고 다른 웹 기반 이메일 애플리케이션도 작동해야 하지만 아직 검증되지 않았습니다.

이메일 프록시를 통한 이메일 사용

다음 레거시 이메일 애플리케이션이 지원됩니다.

- Microsoft Outlook 2000 및 2002
- Microsoft Outlook Express 5.5 및 6.0

클라이언트리스 SSL VPN을 통한 이메일 사용, 322 페이지에서 메일 애플리케이션에 대한 지침과 예를 참조하십시오.

시작하기 전에

SSL 활성화 메일 애플리케이션이 설치되어 있어야 합니다.

ASA SSL 버전을 TLSv1 Only(TLSv1 전용)로 설정하지 마십시오. Outlook 및 Outlook Express는 TLS를 지원하지 않습니다.

보유한 메일 애플리케이션이 제대로 구성되어 있어야 합니다.

다른 SSL 활성화 클라이언트도 작동해야 하지만 이는 검증되지 않았습니다.

스마트 터널 사용

스마트 터널을 사용하는 데 관리자 권한은 필요하지 않습니다.

참고 Java는 포트 전달자로 자동으로 다운로드되지 않습니다.

- 스마트 터널에는 Windows의 ActiveX 또는 JRE와 Mac OS X의 Java Web Start 중 하나가 필요합니다.
- 브라우저에서 쿠키를 활성화해야 합니다.
- 브라우저에서 JavaScript를 활성화해야 합니다.
- Mac OS X는 전면 프록시를 지원하지 않습니다.

- 지원되는 운영 체제 및 브라우저만 사용하십시오.
- TCP 소켓 기반 애플리케이션만 지원됩니다.

19 장

모바일 디바이스를 통한 클라이언트리스 SSL VPN

모바일 디바이스에서 클라이언트리스 SSL VPN 사용

Pocket PC 또는 기타 인증 모바일 디바이스에서 클라이언트리스 SSL VPN에 액세스할 수 있습니다. ASA 관리자 또는 클라이언트리스 SSL VPN 사용자는 인증된 모바일 디바이스에서 클라이언트리스 SSL VPN을 사용하기 위해 특별한 작업을 수행할 필요가 없습니다.

Cisco에서는 다음의 모바일 디바이스 플랫폼을 인증했습니다.

- HP iPaq H4150
- Pocket PC 2003
- Windows CE 4.20.0, 빌드 14053
- PIE(Pocket Internet Explorer)
- ROM 버전 1.10.03ENG
- ROM 날짜: 2004년 7월 16일

클라이언트리스 SSL VPN의 모바일 디바이스 버전에는 몇 가지 차이점이 있습니다.

- 배너 웹 페이지는 클라이언트리스 SSL VPN 팝업 창을 대체합니다.
- 아이콘 막대는 표준 클라이언트리스 SSL VPN 부동 툴바를 대체합니다. 이 막대는 Go(이동), Home(홈) 및 Logout(로그아웃) 버튼을 표시합니다.
- Show Toolbar(툴바 표시) 아이콘은 기본 클라이언트리스 SSL VPN 포털 페이지에 포함되지 않습니다.
- 클라이언트리스 SSL VPN에서 로그아웃하는 즉시 경고 메시지에서 PIE 브라우저를 제대로 닫기 위한 지침을 제공합니다. 이 지침을 준수하지 않고 일반적인 방법으로 브라우저 창을 닫은 경

우, PIE는 클라이언트리스 SSL VPN 또는 HTTPS를 사용하는 보안 웹사이트로부터 연결을 끊지 않습니다.

모바일을 통한 클라이언트리스 **SSL VPN**의 제한 사항

- 클라이언트리스 SSL VPN은 OWA 2000 및 OWA 2003 기본 인증을 지원합니다. 기본 인증이 OWA 서버에 구성되어 있지 않고 클라이언트리스 SSL VPN 사용자가 해당 서버에 액세스하려고 시도하는 경우 액세스가 거부됩니다.
- 지원되지 않는 클라이언트리스 SSL VPN 기능:
  - 애플리케이션 액세스 및 기타 Java 종속 기능
  - HTTP 프록시
  - Citrix Metaframe 기능(PDA에 해당하는 Citrix ICA 클라이언트 소프트웨어가 없는 경우)

20 장

클라이언트리스 SSL VPN 사용자 지정

클라이언트리스 SSL VPN 사용자 환경 사용자 지정

로그온, 포털 및 로그아웃 페이지를 포함하여 클라이언트리스 SSL VPN 사용자 환경을 사용자 지정할 수 있습니다. 여기에는 두 가지 방법이 있습니다. Add/Edit Customization Object(사용자 지정 개체 추가/수정) 창에서 사전 정의된 페이지 구성 요소를 사용자 지정할 수 있습니다. 이 창에서 페이지를 맞춤화하는 데 사용되는 ASA에 저장된 XML 파일(맞춤형 개체)을 추가하거나 변경할 수 있습니다. 또는 XML 파일을 로컬 컴퓨터나 서버로 내보내고 XML 태그를 변경한 다음 이 파일을 ASA로 다시 가져올 수 있습니다. 두 가지 방법 중 하나로 연결 프로파일 또는 그룹 정책에 적용할 사용자 지정 개체를 생성합니다.

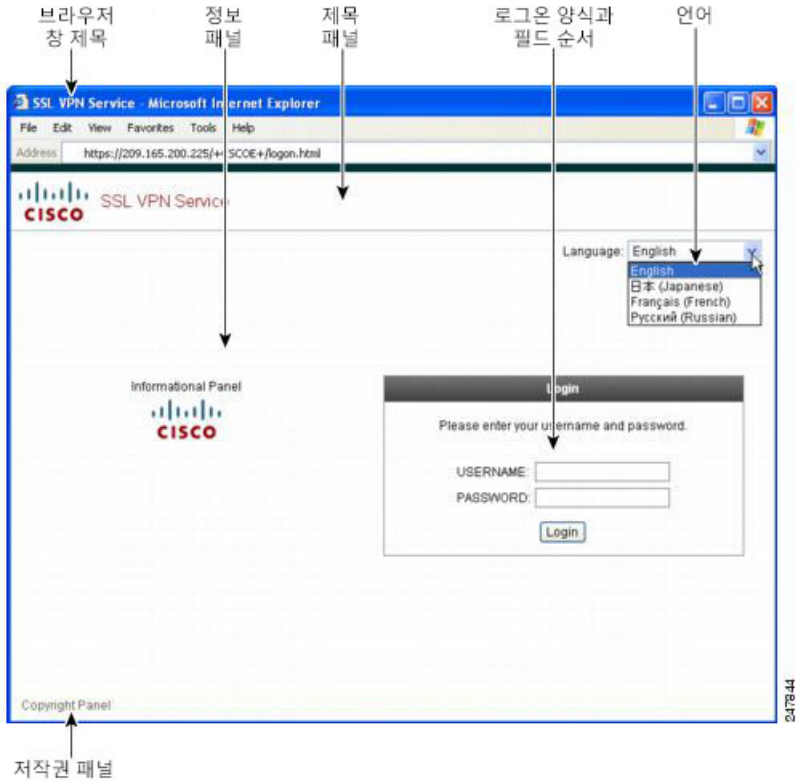
로그온 페이지에서 사전 정의된 구성 요소를 맞춤화하는 대신 고유한 페이지를 생성한 후 이 페이지를 ASA로 가져와 전체 맞춤화할 수 있습니다.

제목, 언어 옵션 및 사용자 메시지 등을 포함하여 로그온 페이지의 사전 정의된 구성 요소를 사용자 지정할 수 있습니다. 또는 이 페이지를 고유한 사용자 지정 페이지(전체 사용자 지정)로 완전히 교체할 수 있습니다.

사용자 지정 편집기를 사용하여 로그온 페이지 사용자 지정

다음 그림에서는 다음과 같이 사용자 지정할 수 있는 로그온 페이지 및 사전 정의된 구성 요소를 보여줍니다.

그림 *10:* 클라이언트리스 로그온 페이지의 구성 요소



로그온 페이지의 모든 구성 요소를 사용자 지정하려면 다음 절차를 따르십시오. **Preview(**미리보기**)** 버튼을 클릭하여 각 구성 요소에 대한 변경 사항을 미리 볼 수 있습니다.

프로시저

단계 **1** 사전 정의된 사용자 지정을 지정합니다. **Logon Page(**로그온 페이지**)**로 이동하여 **Customize pre-defined logon page components(**사전 정의된 로그온 페이지 구성 요소 맞춤화**)**를 선택합니다. 브라우저 창의 제목을 지정합니다.

단계 **2** 제목 패널을 표시하고 사용자 지정합니다. **Logon Page(**로그온 페이지**) > Title Panel(**제목 패널**)**로 이동하여 **Display title panel(**제목 패널 표시**)**을 선택합니다. 제목으로 표시할 텍스트를 입력하고 로고를 지정합니다. 글꼴 스타일을 지정합니다.

단계 **3** 표시할 언어 옵션을 지정합니다. **Logon Page(**로그온 페이지**) > Language(**언어**)**로 이동하여 **Enable Language Selector(**언어 선택기 활성화**)**를 선택합니다. 원격 사용자에게 표시할 언어를 추가하거나 삭제합니다. 목록에 포함된 언어에는 Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > Language Localization(언어 현지화)에서 구성한 변환 테이블이 필요합니다.

사용자 이름 및 비밀번호 필드의 라벨이 사용자가 선택한 언어에 따라 변경됩니다.

단계 **4** 로그온 양식을 사용자 지정합니다. **Logon Page(**로그온 페이지**) > Logon Form(**로그온 양식**)**으로 이동합니다. 패널에서 양식의 텍스트 및 글꼴 스타일을 사용자 지정합니다. 보조 인증 서버가 연결 프로파일에 구성되어 있는 경우에만 보조 비밀번호 필드가 사용자에게 나타납니다.

단계 **5** 로그온 양식 필드의 위치를 정렬합니다. **Logon Page(**로그온 페이지**) > Form Fields Order(**양식 필드 순서**)**로 이동합니다. 필드가 표시되는 순서를 변경하려면 위로 화살표 및 아래로 화살표 버튼을 사용합니다.

단계 **6** 사용자에게 메시지를 추가합니다. **Logon Page(**로그온 페이지**) > Informational Panel(**정보 패널**)**로 이동하여 **Display informational panel(**정보 패널 표시**)**을 선택합니다. 패널에 표시할 텍스트를 추가하고 로그온 양식과 관련 있는 패널의 위치를 변경하며 이 패널에서 표시할 로고를 지정합니다.

단계 **7** 저작권 정보를 표시합니다. **Logon Page(**로그온 페이지**) > Copyright Panel(**저작권 패널**)**로 이동하여 Display copyright panel(저작권 패널 표시)을 선택합니다. 저작권 용도로 표시할 텍스트를 추가합니다.

단계 **8** **OK(**확인**)**를 클릭한 다음 수정한 맞춤형 개체에 변경 사항을 적용합니다.

다음에 수행할 작업

전체 사용자 지정된 페이지로 로그온 페이지 대체를 읽어 봅니다.

전체 사용자 지정된 페이지로 로그온 페이지 대체

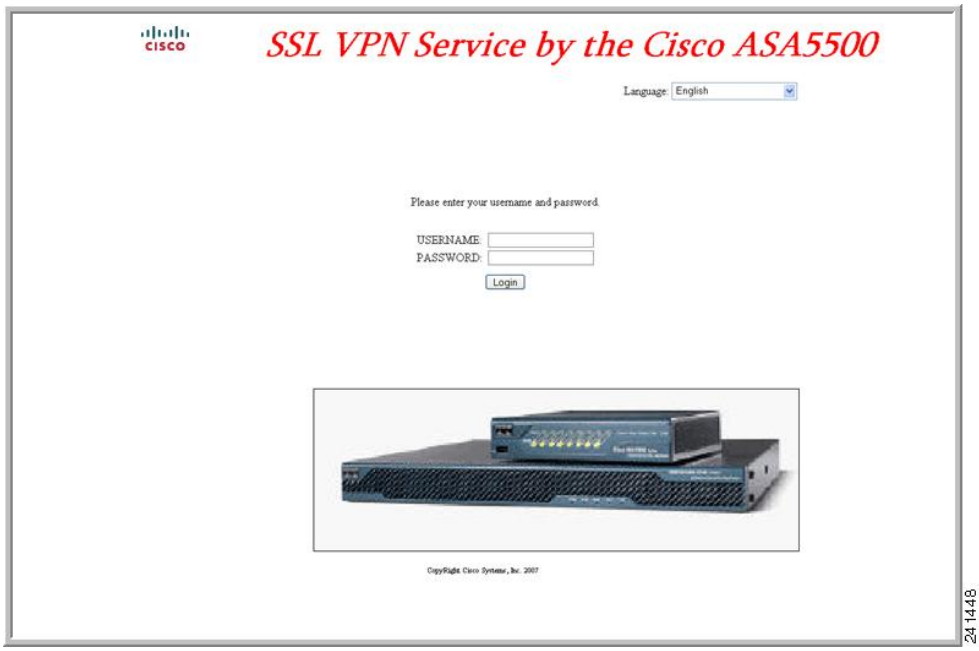
제공되는 로그온 페이지의 특정한 구성 요소를 변경하는 대신 고유한 사용자 지정 로그인 화면을 사용하려는 경우, Full Customization(전체 사용자 지정) 기능을 사용하여 이러한 고급 사용자 지정을 수행할 수 있습니다.

Full Customization(전체 맞춤화)을 사용하여 고유한 로그인 화면을 위한 HTML을 입력하고 ASA에서 로그인 양식 및 언어 선택기 드롭다운 목록을 생성하는 함수를 호출하는 Cisco HTML 코드를 삽입합니다.

이 문서에서는 HTML 코드에 필요한 수정 사항과 코드를 사용하도록 ASA를 구성하는 데 필요한 작업에 대해 설명합니다.

다음 그림은 전체 사용자 지정 기능을 통해 활성화된 사용자 지정 로그인 화면의 간단한 예를 보여줍니다.

그림 *11:* 로그온 페이지의 전체 사용자 지정 예



사용자 지정 로그인 화면 파일 생성

다음은 HTML 코드의 예이며 다음과 같은 형식으로 표시됩니다.

```
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
<title>New Page 3</title>
<base target="_self">
</head>

<p align="center">
<img border="0" src="/+CSCOU+/cisco_logo.jpg" width="188" height="48"><font face="Snap ITC"
 size="6" color="#FF00FF">
</font><font face="Snap ITC" color="#FF00FF" size="7"> </font><i><b><font color="#FF0000"
size="7" face="Sylfaen"> SSL VPN Service by the Cisco ASA5500</font></b></i></p>

<body onload="csco_ShowLoginForm('lform');csco_ShowLanguageSelector('selector')">

<table>

<tr><td colspan=3 height=20 align=right><div id="selector" style="width:
300px"></div></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr>
<td height="379"></td>
<td height="379"></td>
<td align=middle valign=middle>
<div id=lform >
<p> </p>
<p> </p>
<p> </p>
<p>Loading...</p>
</div>
</td>
```

```
</tr>
<tr>
<td width="251"></td>
<td width="1"></td>
<td align=right valign=right width="800">
<img border="1" src="/+CSCOU+/asa5500.jpg" width="660" height="220" align="middle">
</td></tr>
</table>
```

들여쓰기한 코드는 화면에서 로그인 양식 및 언어 선택기를 삽입합니다. 기능 **csco_ShowLoginForm('lform')** 은 로그온 양식을 삽입합니다. **csco_ShowLanguageSelector('selector')** 는 언어 선택기를 삽입합니다.

프로시저

단계 **1** 파일 이름을 logon.inc로 지정합니다. 파일을 가져올 때 ASA는 이 파일 이름을 로그온 화면으로 인식합니다.

단계 **2** /+CSCOU+/를 포함하도록 파일에서 사용되는 이미지의 경로를 수정합니다.

인증 전에 원격 사용자에게 표시되는 파일은 경로 /+CSCOU+/로 표시되는 ASA 캐시 메모리의 특정 영역에 있어야 합니다. 따라서 파일에 있는 각 이미지의 소스에 이 경로가 포함되어야 합니다. 예를 들면 다음과 같습니다.

src=”/+CSCOU+/asa5520.gif”

단계 **3** 아래의 특수한 HTML 코드를 삽입합니다. 이 코드에는 화면에 로그인 양식과 언어 선택기를 삽입하는 앞서 설명한 Cisco 함수가 포함되어 있습니다.

```
<body onload="csco_ShowLoginForm('lform');csco_ShowLanguageSelector('selector')">

<table>

<tr><td colspan=3 height=20 align=right><div id="selector" style="width:
300px"></div></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr>
<td height="379"></td>
<td height="379"></td>
<td align=middle valign=middle>
<div id=lform >
<p> </p>
<p> </p>
<p> </p>
<p>Loading...</p>
</div>
</td>
</tr>
<tr>
<td width="251"></td>
<td width="1"></td>
<td align=right valign=right width="800">
<img border="1" src="/+CSCOU+/asa5500.jpg" width="660" height="220" align="middle">
</td></tr>
```

```
</table>
```

파일 및 이미지 가져오기

프로시저

단계 **1** Clientless SSL VPN Access(클라이언트리스 SSL VPN 액세스) > Portal(포털) > Web Contents(웹 콘텐츠)로 이동합니다.

단계 **2** 가져오기를 클릭합니다.

a) **Source(**소스**)** 옵션을 선택하고 웹 콘텐츠 파일 경로를 입력합니다.

b) **Destination(**대상**)** 영역에서 Require Authentication to access its content(콘텐츠에 액세스하려면 인증 필요)에 대해 No(아니요)를 선택합니다. 이렇게 하면 사용자가 인증 전에도 액세스 가능한 플래시 메모리 영역에 파일이 저장됩니다.

단계 **3** **Import Now(**지금 가져오기**)**를 클릭합니다.

사용자 지정 로그인 화면을 사용하도록 보안 어플라이언스 구성

프로시저

단계 **1** Clientless SSL VPN Access(클라이언트리스 SSL VPN 액세스) > Portal(포털) > Customization(사용자 지정)의 테이블에서 사용자 지정 개체를 선택하고 Edit(수정)를 클릭합니다.

단계 **2** 탐색 창에서 **Logon Page(**로그온 페이지**)**를 선택합니다.

단계 **3** **Replace pre-defined logon page with a custom page(**사전 정의된 로그온 페이지를 사용자 지정 페이지로 대체**)**를 선택합니다.

단계 **4** **Manage(**관리**)**를 클릭하여 로그온 페이지 파일을 가져옵니다.

단계 **5** 사용자가 인증 전에도 로그온 페이지를 볼 수 있도록 Destination(대상) 영역에서 No(아니요)를 선택합니다.

단계 **6** Edit Customization Object(맞춤형 개체 수정) 창으로 돌아가서 **General(**일반**)**을 클릭하고 원하는 연결 프로필 및/또는 그룹 정책에 대한 맞춤형 개체를 활성화합니다.

클라이언트리스 **SSL VPN** 엔드 유저 설정

이 섹션은 엔드 유저에 대해 클라이언트리스 SSL VPN을 설정하는 시스템 관리자를 위한 내용입니다. 이 섹션에서는 엔드 유저 인터페이스를 사용자 지정하는 방법에 대해 설명하고 원격 시스템을 위

한 구성 요구 사항 및 작업을 요약합니다. 이 요약에는 클라이언트리스 SSL VPN을 사용하여 원격 시스템을 시작하기 위해 사용자와 통신하는 정보가 지정되어 있습니다.

엔드 유저 인터페이스 정의

클라이언트리스 SSL VPN 엔드 유저 인터페이스는 일련의 HTML 패널로 구성됩니다. 사용자는 ASA 인터페이스 IP 주소를 https://*address* 형식으로 입력하여 클라이언트리스 SSL VPN에 로그온합니다. 가장 먼저 표시되는 패널은 로그인 화면입니다.

클라이언트리스 **SSL VPN** 홈 페이지 보기

사용자가 로그인하면 포털 페이지가 열립니다.

홈 페이지에 구성한 클라이언트리스 SSL VPN 기능이 모두 표시되며 이 모양에는 선택한 로고, 텍스트 및 색상이 반영되어 있습니다. 이 샘플 홈 페이지에는 특정 파일 공유 식별을 제외한 모든 사용 가능한 클라이언트리스 SSL VPN 기능이 포함되어 있습니다. 이 페이지를 통해 사용자는 네트워크를 찾아보고 URL을 입력하며 특정 웹 사이트에 액세스하고 애플리케이션 액세스(포트 전달 및 스마트 터널)를 사용하여 TCP 애플리케이션에 액세스할 수 있습니다.

클라이언트리스 **SSL VPN Application Access** 패널 보기

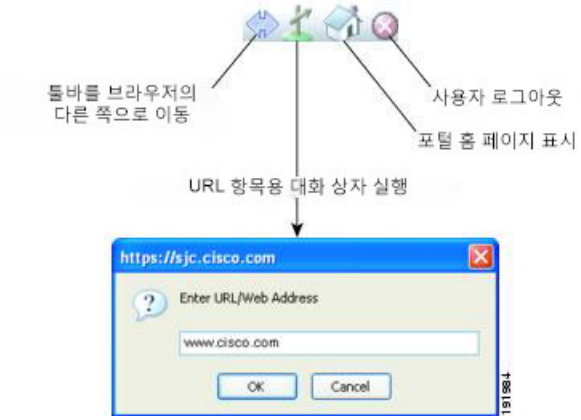
포트 전달 또는 스마트 터널을 시작하기 위해 사용자는 Application Access(애플리케이션 액세스) 상자에서 **Go(**이동**)** 버튼을 클릭합니다. Application Access 창이 열리고 이 클라이언트리스 SSL VPN 연결에 대해 구성된 TCP 애플리케이션이 표시됩니다. 이 패널이 열린 상태에서 애플리케이션을 사용하기 위해 사용자는 일반적인 방식으로 애플리케이션을 시작합니다.

참고 상태 저장 장애 조치는 애플리케이션 액세스를 사용하여 설정된 세션을 그대로 유지하지 않습니다. 사용자는 장애 조치 후 다시 연결해야 합니다.

부동 툴바 보기

다음 그림에 표시된 부동 툴바는 현재의 클라이언트리스 SSL VPN 세션을 나타냅니다.

그림 *12:* 클라이언트리스 *SSL VPN*의 부동 툴바



부동 툴바의 다음 특성에 유의하십시오.

- 툴바를 사용하여 URL을 입력하고 파일 위치를 찾아보며 기본 브라우저 창에 방해되지 않게 사전 구성된 웹 연결을 선택할 수 있습니다.
- 팝업을 차단하도록 브라우저를 구성한 경우 부동 툴바를 표시할 수 없습니다.
- 툴바를 닫으면 ASA에서 클라이언트리스 SSL VPN 세션을 종료하라는 메시지를 표시합니다.

클라이언트리스 SSL VPN 페이지 사용자 지정

클라이언트리스 SSL VPN 사용자에게 표시되는 포털 페이지의 모양을 변경할 수 있습니다. 예를 들어 사용자가 보안 어플라이언스에 연결할 때 표시되는 로그인 페이지, 보안 어플라이언스가 사용자를 인증한 이후에 사용자에게 표시되는 홈 페이지, 사용자가 애플리케이션을 시작할 때 표시되는 애플리케이션 액세스 창 및 사용자가 클라이언트리스 SSL VPN 세션을 로그아웃할 때 표시되는 로그아웃 페이지가 포함됩니다.

포털 페이지를 사용자 지정한 후에 사용자 지정을 저장하고 특정 연결 프로파일, 그룹 정책 또는 사용자에게 이를 적용할 수 있습니다. ASA를 다시 로드하거나 클라이언트리스 SSL을 끈 다음 활성화할 때까지 변경 사항은 적용되지 않습니다.

개별 사용자 또는 사용자 그룹에 대한 포털 페이지 모양을 변경하도록 보안 어플라이언스가 활성화하여 많은 사용자 지정 개체를 생성하고 저장할 수 있습니다.

사용자 지정 정보

ASA는 맞춤형 개체를 사용하여 사용자 화면의 모양을 정의합니다. 사용자 지정 개체는 원격 사용자에게 표시되는 사용자 지정 가능한 화면의 모든 항목에 대한 XML 태그를 포함하는 XML 파일에서 컴파일됩니다. ASA 소프트웨어에는 원격 PC로 내보낼 수 있는 맞춤형 템플릿이 포함되어 있습니다. 이 템플릿을 수정하고 새 맞춤형 개체로 ASA에 다시 가져올 수 있습니다.

사용자 지정 개체를 내보내면 XML 태그를 포함한 XML 파일이 지정된 URL에 생성됩니다. 사용자 지정 개체 *Template*을 통해 생성된 XML 파일은 빈 XML 태그를 포함하고 있으며 새로운 사용자 지정

개체를 만들기 위한 기본 사항을 제공합니다. 이 개체는 변경하거나 캐시 메모리에서 삭제할 수 없으나 내보내거나 수정하거나 새 맞춤형 개체로 다시 ASA에 가져올 수는 있습니다.

사용자 지정 개체, 연결 프로파일 및 그룹 정책

사용자가 처음 연결할 때 연결 프로파일(터널 그룹)에서 식별한 이름이 *DfltCustomization*인 기본 사용자 지정 개체에서 로그온 화면이 어떻게 표시될지 결정됩니다. 연결 프로파일 목록이 활성화되어 있고 사용자가 고유한 사용자 지정이 있는 다른 그룹을 선택하면 화면이 새로운 그룹에 대해 사용자 지정 개체를 반영하도록 변경됩니다.

원격 사용자가 인증되면 그룹 정책에 사용자 지정 개체가 할당되었는지 여부에 따라 화면 모양이 결정됩니다.

사용자 지정 템플릿 수정

이 섹션에는 사용자 지정 템플릿의 콘텐츠를 보여주며 정확한 XML 태그를 신속하게 선택하고 화면에 적용되는 변경을 수행하는 데 도움이 되는 편리한 그림이 수록되어 있습니다.

텍스트 편집기 또는 XML 파일을 수정하는 XML 편집기를 사용할 수 있습니다. 다음 예는 사용자 지정 템플릿의 XML 태그를 보여줍니다. 일부 중복 태그는 더 쉽게 볼 수 있도록 제거되었습니다.

```
<custom>
   <localization>
      <languages>en,ja,zh,ru,ua</languages>
      <default-language>en</default-language>
   </localization>
    <auth-page>
      <window>
          <title-text l10n="yes"><![CDATA[SSL VPN Service</title-text>
      </window>
      <full-customization>
          <mode>disable</mode>
          <url></url>
      </full-customization>
      <language-selector>
        <mode>disable</mode>
        <title l10n="yes">Language:</title>
        <language>
          <code>en</code>
          <text>English</text>
        </language>
        <language>
          <code>zh</code>
          <text>(Chinese)</text>
        </language>
        <language>
          <code>ja</code>
          <text>(Japanese)</text>
        </language>
        <language>
          <code>ru</code>
          <text>(Russian)</text>
        </language>
        <language>
          <code>ua</code>
          <text>(Ukrainian)</text>
        </language>
```

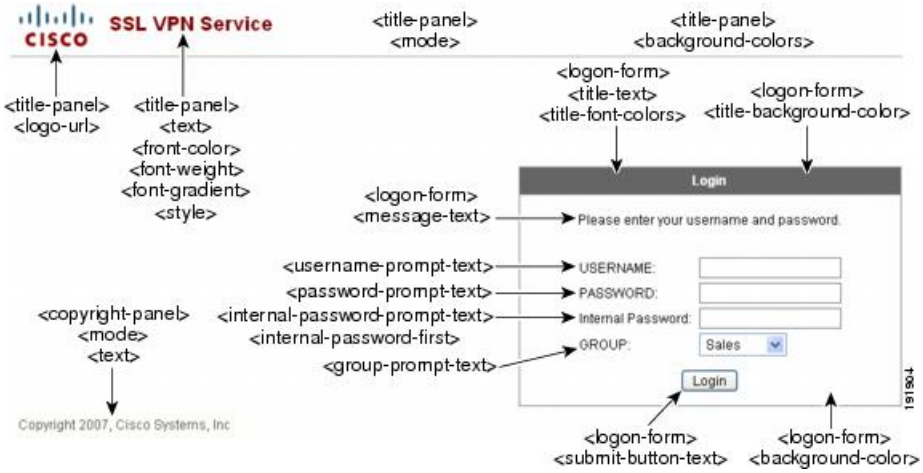
```
      </language-selector>
      <logon-form>
          <title-text l10n="yes"><![CDATA[Login</title-text>
          <title-background-color><![CDATA[#666666</title-background-color>
          <title-font-color><![CDATA[#ffffff</title-font-color>
          <message-text l10n="yes"><![CDATA[Please enter your username and
password.</message-text>
          <username-prompt-text l10n="yes"><![CDATA[USERNAME:</username-prompt-text>
          <password-prompt-text l10n="yes"><![CDATA[PASSWORD:</password-prompt-text>
          <internal-password-prompt-text l10n="yes">Internal
Password:</internal-password-prompt-text>
          <internal-password-first>no</internal-password-first>
          <group-prompt-text l10n="yes"><![CDATA[GROUP:</group-prompt-text>
          <submit-button-text l10n="yes"><![CDATA[Login</submit-button-text>
          <title-font-color><![CDATA[#ffffff</title-font-color>
          <title-background-color><![CDATA[#666666</title-background-color>
          <font-color>#000000</font-color>
          <background-color>#ffffff</background-color>
          <border-color>#858A91</border-color>
      </logon-form>
      <logout-form>
          <title-text l10n="yes"><![CDATA[Logout</title-text>
          <message-text l10n="yes"><![CDATA[Goodbye.<br>

For your own security, please:<br>

<li>Clear the browser's cache

<li>Delete any downloaded files

<li>Close the browser's window</message-text>
          <login-button-text l10n="yes">Logon</login-button-text>
          <hide-login-button>no</hide-login-button>
          <title-background-color><![CDATA[#666666</title-background-color>
          <title-font-color><![CDATA[#ffffff</title-font-color>
          <title-font-color><![CDATA[#ffffff</title-font-color>
          <title-background-color><![CDATA[#666666</title-background-color>
          <font-color>#000000</font-color>
          <background-color>#ffffff</background-color>
          <border-color>#858A91</border-color>
      </logout-form>
      <title-panel>
         <mode>enable</mode>
         <text l10n="yes"><![CDATA[SSL VPN Service</text>
         <logo-url l10n="yes">/+CSCOU+/csco_logo.gif</logo-url>
         <gradient>yes</gradient>
         <style></style>
         <background-color><![CDATA[#ffffff</background-color>
         <font-size><![CDATA[larger</font-size>
         <font-color><![CDATA[#800000</font-color>
         <font-weight><![CDATA[bold</font-weight>
      </title-panel>
      <info-panel>
        <mode>disable</mode>
        <image-url l10n="yes">/+CSCOU+/clear.gif</image-url>
        <image-position>above</image-position>
        <text l10n="yes"></text>
      </info-panel>
      <copyright-panel>
         <mode>disable</mode>
         <text l10n="yes"></text>
      </copyright-panel>
    </auth-page>
    <portal>
```

```
<title-panel>
   <mode>enable</mode>
   <text l10n="yes"><![CDATA[SSL VPN Service</text>
   <logo-url l10n="yes">/+CSCOU+/csco_logo.gif</logo-url>
   <gradient>yes</gradient>
   <style></style>
   <background-color><![CDATA[#ffffff</background-color>
   <font-size><![CDATA[larger</font-size>
   <font-color><![CDATA[#800000</font-color>
   <font-weight><![CDATA[bold</font-weight>
</title-panel>
<browse-network-title l10n="yes">Browse Entire Network</browse-network-title>
<access-network-title l10n="yes">Start AnyConnect</access-network-title>
<application>
   <mode>enable</mode>
   <id>home</id>
   <tab-title l10n="yes">Home</tab-title>
   <order>1</order>
</application>
<application>
   <mode>enable</mode>
   <id>web-access</id>
   <tab-title l10n="yes"><![CDATA[Web Applications</tab-title>
   <url-list-title l10n="yes"><![CDATA[Web Bookmarks</url-list-title>
   <order>2</order>
</application>
<application>
   <mode>enable</mode>
   <id>file-access</id>
   <tab-title l10n="yes"><![CDATA[Browse Networks</tab-title>
   <url-list-title l10n="yes"><![CDATA[File Folder Bookmarks</url-list-title>
   <order>3</order>
</application>
<application>
   <mode>enable</mode>
   <id>app-access</id>
   <tab-title l10n="yes"><![CDATA[Application Access</tab-title>
   <order>4</order>
</application>
<application>
   <mode>enable</mode>
   <id>net-access</id>
   <tab-title l10n="yes">AnyConnect</tab-title>
   <order>4</order>
</application>
<application>
   <mode>enable</mode>
   <id>help</id>
   <tab-title l10n="yes">Help</tab-title>
   <order>1000000</order>
</application>
<toolbar>
   <mode>enable</mode>
   <logout-prompt-text l10n="yes">Logout</logout-prompt-text>
   <prompt-box-title l10n="yes">Address</prompt-box-title>
   <browse-button-text l10n="yes">Browse</browse-button-text>
   <username-prompt-text l10n="yes"></username-prompt-text>
</toolbar>
<column>
   <width>100%</width>
   <order>1</order>
</column>
<pane>
   <type>TEXT</type>
```

```
            <mode>disable</mode>
            <title></title>
            <text></text>
            <notitle></notitle>
            <column></column>
            <row></row>
            <height></height>
         </pane>
         <pane>
            <type>IMAGE</type>
            <mode>disable</mode>
            <title></title>
            <url l10n="yes"></url>
            <notitle></notitle>
            <column></column>
            <row></row>
            <height></height>
         </pane>
         <pane>
            <type>HTML</type>
            <mode>disable</mode>
            <title></title>
            <url l10n="yes"></url>
            <notitle></notitle>
            <column></column>
            <row></row>
            <height></height>
         </pane>
         <pane>
            <type>RSS</type>
            <mode>disable</mode>
            <title></title>
            <url l10n="yes"></url>
            <notitle></notitle>
            <column></column>
            <row></row>
            <height></height>
         </pane>
         <url-lists>
            <mode>group</mode>
         </url-lists>
         <home-page>
            <mode>standard</mode>
            <url></url>
         </home-page>
      </portal>
</custom>
```

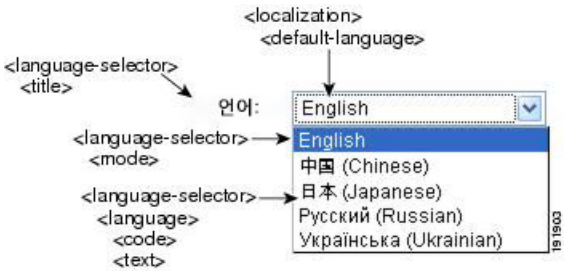
다음 그림에서는 로그온 페이지 및 사용자 지정 XML 태그를 보여줍니다. 이러한 모든 태그는 더 높은 수준의 태그인 <auth-page> 안에 중첩됩니다.

그림 ***13:*** 로그온 페이지 및 연계된 ***XML*** 태그



다음 그림은 로그온 페이지에서 사용 가능한 언어 선택기 드롭다운 목록 및 이 기능을 사용자 지정하는 XML 태그를 보여줍니다. 모든 해당 태그는 더 높은 수준의 <auth-page> 태그 안에 중첩됩니다.

그림 ***14:*** 로그온 화면의 언어 선택기 및 연계된 ***XML*** 태그

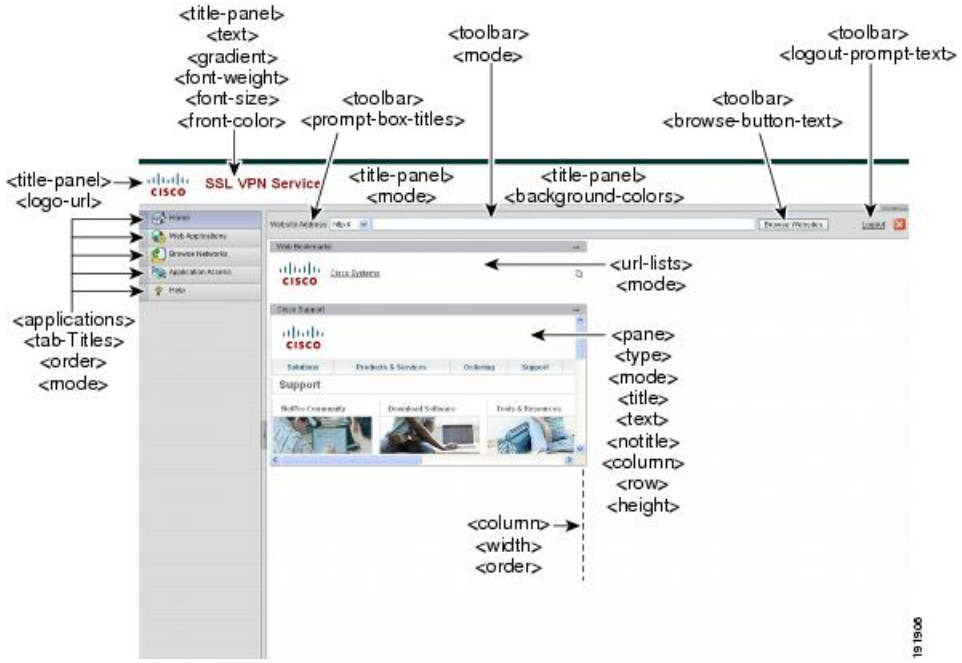


다음 그림은 로그온 페이지에서 사용 가능한 정보 패널 및 이 기능을 사용자 지정하는 XML 태그를 보여줍니다. 이 정보는 로그인 상자의 왼쪽 또는 오른쪽에 나타날 수 있습니다. 해당 태그는 더 높은 수준의 <auth-page> 태그 안에 중첩됩니다.

그림 ***15:*** 로그온 화면의 정보 패널 및 연계된 ***XML*** 태그

다음 그림에서는 포털 페이지 및 이 기능을 사용자 지정하는 XML 태그를 보여줍니다. 해당 태그는 더 높은 수준의 <auth-page> 태그 안에 중첩됩니다.

그림 ***16:*** 포털 페이지 및 연계된 ***XML*** 태그



로그인 화면 고급 사용자 지정

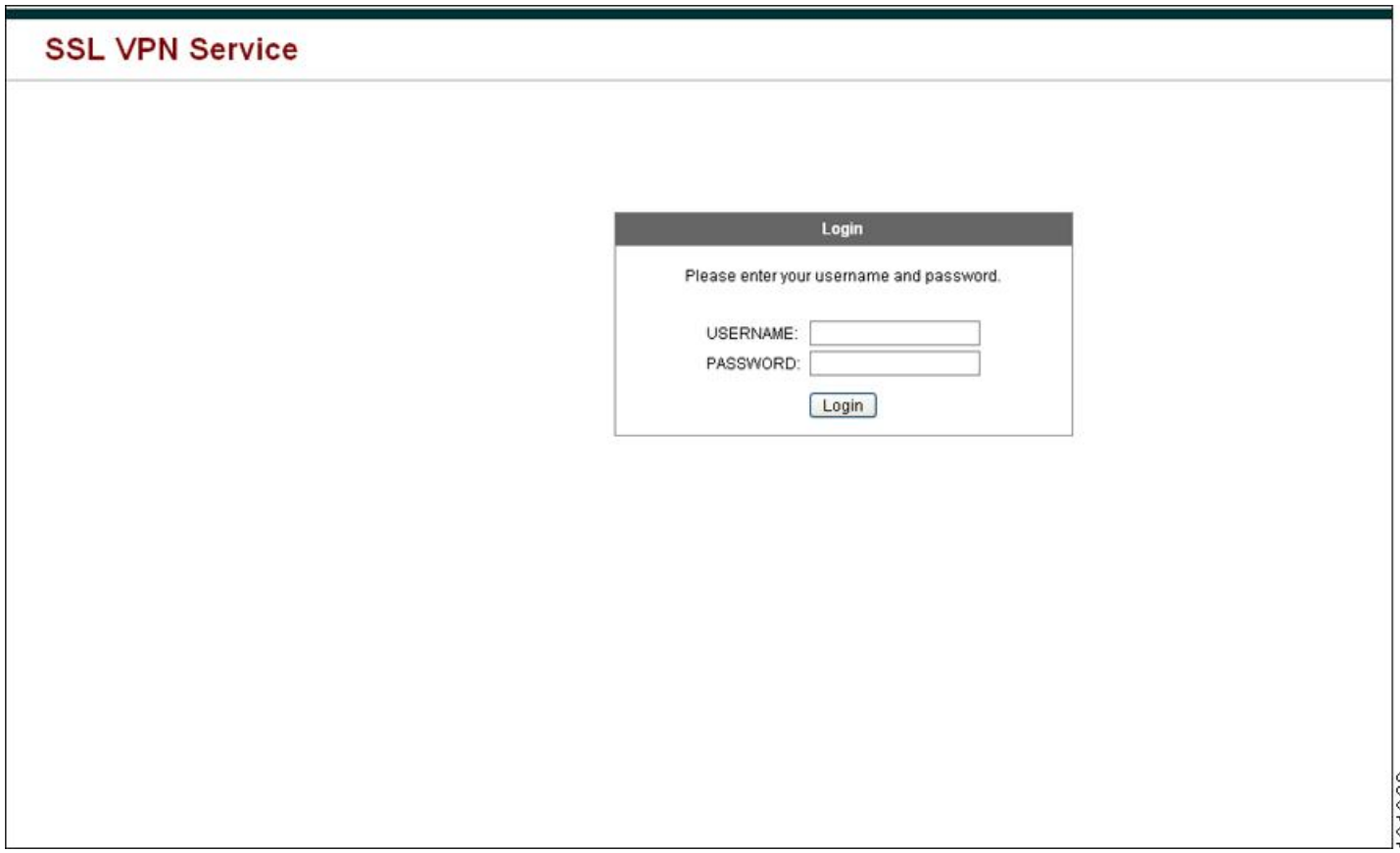
제공되는 로그인 페이지의 특정한 화면 요소를 변경하는 대신 고유한 사용자 지정 로그인 화면을 사용하려는 경우, Full Customization(전체 사용자 지정) 기능을 사용하여 이러한 고급 사용자 지정을 수행할 수 있습니다.

전체 맞춤화를 사용하여 고유한 로그인 화면에 HTML을 제공하고 ASA에서 로그인 양식 및 언어 선택기 드롭다운 목록을 생성하는 함수를 호출하는 Cisco HTML 코드를 삽입합니다.

이 섹션에서는 HTML 코드에 필요한 수정 사항과 코드를 사용하도록 ASA를 구성하는 데 필요한 작업에 대해 설명합니다.

다음 그림은 클라이언트리스 SSL VPN 사용자에게 표시되는 표준 Cisco 로그인 화면을 보여줍니다. 로그인 양식은 HTML 코드로 호출되는 함수를 사용하여 표시됩니다.

그림 ***17:*** 표준 ***Cisco*** 로그인 페이지

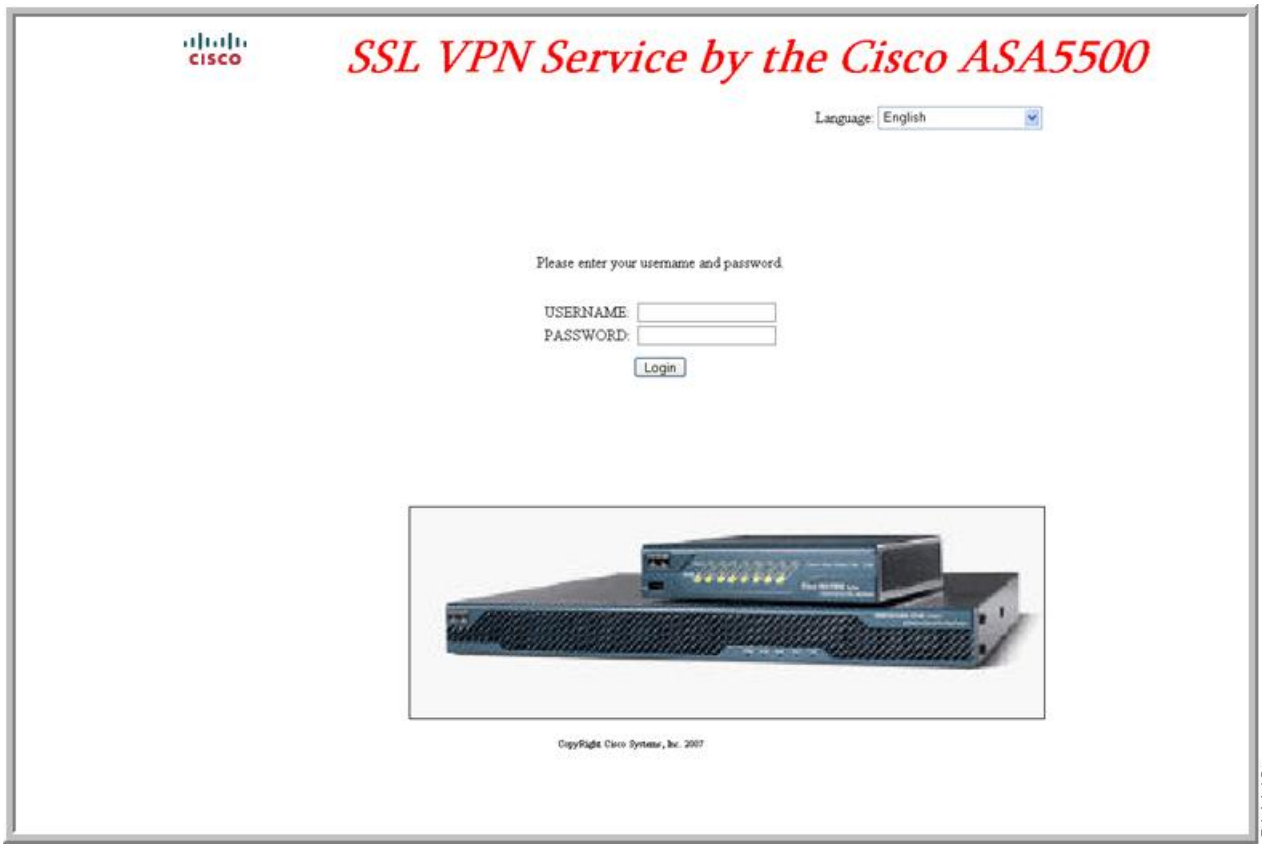


다음 그림에서는 언어 선택기 드롭다운 목록을 보여줍니다. 이 기능은 클라이언트리스 SSL VPN 사용자에 대한 옵션이며 로그인 화면의 HTML 코드에 있는 함수를 사용하여 호출됩니다.

그림 ***18:*** 언어 선택기 드롭다운 목록

다음 그림은 전체 사용자 지정 기능을 통해 활성화된 사용자 지정 로그인 화면의 간단한 예를 보여줍니다.

그림 ***19:*** 로그인 화면의 전체 사용자 지정 예



다음은 HTML 코드의 예이며 다음과 같은 형식으로 표시됩니다.

```
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
<title>New Page 3</title>
<base target="_self">
</head>

<p align="center">
<img border="0" src="/+CSCOU+/cisco_logo.jpg" width="188" height="48"><font face="Snap ITC"
 size="6" color="#FF00FF">
</font><font face="Snap ITC" color="#FF00FF" size="7"> </font><i><b><font color="#FF0000"
size="7" face="Sylfaen"> SSL VPN Service by the Cisco ASA5500</font></b></i></p>

<body onload="csco_ShowLoginForm('lform');csco_ShowLanguageSelector('selector')">

<table>

<tr><td colspan=3 height=20 align=right><div id="selector" style="width:
300px"></div></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr>
<td height="379"></td>
<td height="379"></td>
<td align=middle valign=middle>
<div id=lform >
<p> </p>
```

```
<p> </p>
<p> </p>
<p>Loading...</p>
</div>
</td>
</tr>
<tr>
<td width="251"></td>
<td width="1"></td>
<td align=right valign=right width="800">
<img border="1" src="/+CSCOU+/asa5500.jpg" width="660" height="220" align="middle">
</td></tr>

</table>
```

들여쓰기한 코드는 화면에서 로그인 양식 및 언어 선택기를 삽입합니다. 이 기능은 **csco_ShowLoginForm('lform')** 로그온 양식을 삽입합니다. **csco_ShowLanguageSelector('selector')** 는 언어 선택기를 삽입합니다.

HTML 파일 수정

프로시저

단계 **1** 파일 이름을 logon.inc로 지정합니다. 파일을 가져올 때 ASA는 로그온 화면에서 이 파일 이름을 인식합니다.

단계 **2** /+CSCOU+/를 포함하도록 파일에서 사용되는 이미지의 경로를 수정합니다.

경로 /+CSCOU+/로 표시된 ASA 캐시 메모리의 특정 영역에서 인증을 수행하기 전에 원격 사용자에게 표시되는 파일입니다. 따라서 파일에 있는 각 이미지의 소스에 이 경로가 포함되어야 합니다.

예를 들면 다음과 같습니다.

src="/+CSCOU+/asa5520.gif"

단계 **3** 아래의 특수한 HTML 코드를 삽입합니다. 이 코드에는 화면에 로그인 양식과 언어 선택기를 삽입하는 앞서 설명한 Cisco 함수가 포함되어 있습니다.

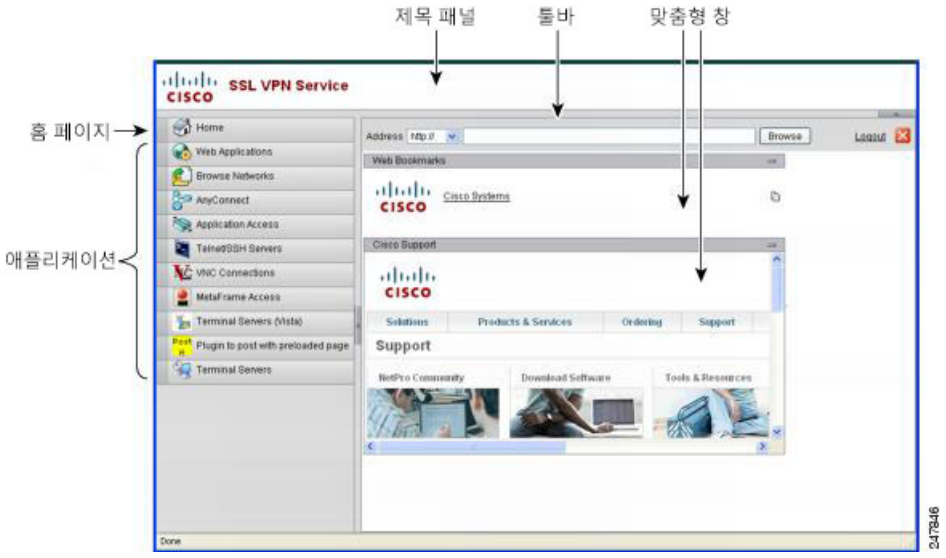
```
<body onload="csco_ShowLoginForm('lform');csco_ShowLanguageSelector('selector')">

<table>

<tr><td colspan=3 height=20 align=right><div id="selector" style="width:
300px"></div></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr>
<td height="379"></td>
<td height="379"></td>
<td align=middle valign=middle>
<div id=lform >
<p> </p>
<p> </p>
<p> </p>
<p>Loading...</p>
</div>
```

```
</td>
</tr>
<tr>
<td width="251"></td>
<td width="1"></td>
<td align=right valign=right width="800">
<img border="1" src="/+CSCOU+/asa5500.jpg" width="660" height="220" align="middle">
</td></tr>

</table>
```

포털 페이지 사용자 지정

다음 그림에서는 다음과 같이 사용자 지정할 수 있는 포털 페이지 및 사전 정의된 구성 요소를 보여 줍니다.

그림 ***20:*** 포털 페이지의 사용자 지정 가능한 구성 요소



페이지의 구성 요소 사용자 지정뿐만 아니라 텍스트, 이미지, RSS 피드 또는 HTML을 표시하는 사용자 지정 창으로 포털 페이지를 나눌 수 있습니다.

포털 페이지를 사용자 지정하려면 다음 절차를 따르십시오. Preview(미리보기) 버튼을 클릭하여 각 구성 요소의 변경 사항을 미리 볼 수 있습니다.

프로시저

단계 **1** **Configuration**(구성) > **Remote Access VPN**(원격 액세스 **VPN**) > **Clientless SSL VPN Access**(클라이언트리스 **SSL VPN** 액세스) > **Portal**(포털) > **Customization**(맞춤화)을 선택합니다.

단계 **2** **Add**(추가)를 클릭합니다.

단계 **3** **Customization Object Name**(맞춤형 개체 이름) 필드에서 맞춤화에 사용할 이름을 입력합니다.

단계 **4** 왼쪽 창에서 **Portal Page(**포털 페이지**)**를 클릭합니다.

단계 **5** **Browser Window Title(**브라우저 창 제목**)** 필드에 제목을 입력합니다.

단계 **6** 제목 패널을 표시 및 맞춤화하려면 **Title Panel(**제목 패널**)**을 클릭하고 **Display title panel(**제목 패널 표시**)** 체크 박스를 선택합니다. 제목으로 표시할 텍스트를 입력하고 로고를 지정합니다. 글꼴 스타일을 지정할 수도 있습니다.

단계 **7** 툴바를 활성화 및 맞춤화하려면 **Toolbar(**툴바**)**를 클릭하고 **Display toolbar(**툴바 표시**)** 체크 박스를 선택합니다. 필요에 따라 **Prompt Box Title(**프롬프트 상자 제목**)**, **Browse Button Text(**찾아보기 버튼 텍스트**)** 및 **Logout Prompt(**로그아웃 프롬프트**)**를 맞춤화합니다.

툴바를 활성화하면 로그인할 때 사용한 사용자 이름도 표시됩니다. **Username(**사용자 이름**)** 필드는 유효한 키워드로 **Username**을 포함해야 합니다.

단계 **8** 애플리케이션 목록을 맞춤화하려면 **Applications(**애플리케이션**)**를 클릭하고 **Show navigation panel(**탐색 패널 표시**)** 체크 박스를 선택합니다. 클라이언트-서버 플러그인과 포트 포워딩 애플리케이션을 포함하여 ASA 구성에서 활성화한 애플리케이션은 테이블에 표시됩니다. 필요에 따라 이 테이블에서 해당 애플리케이션을 활성화하거나 비활성화하십시오.

단계 **9** 포털 페이지 공간에서 맞춤형 창을 생성하려면 **Custom Panes(**맞춤형 창**)**를 클릭합니다. 열의 수와 열의 너비를 구성합니다. 필요한 경우 맞춤형 창을 생성하고 창을 텍스트, 이미지, RSS 피드 또는 HTML 페이지에 사용할 행 및 열로 나눕니다.

단계 **10** 홈 페이지 URL을 지정하려면 **Home Page(**홈 페이지**)**를 클릭하고 **Enable custom intranet web page(**맞춤형 인트라넷 웹 페이지 활성화**)** 체크 박스를 선택합니다. 책갈피 정리 방식을 정의하는 책갈피 모드를 선택합니다.

단계 **11** **Timeout Alerts(**시간 제한 알림**)**를 클릭하여 시간 초과 알림 메시지 및 툴팁을 구성합니다.

단계 **12** **OK(**확인**)**를 클릭합니다.

다음에 수행할 작업

사용자 지정 포털 시간 제한 알림 구성을 읽어 봅니다.

사용자 지정 포털 시간 제한 알림 구성

클라이언트리스 SSL VPN 기능의 사용자가 VPN 세션에서 시간을 관리할 수 있도록 클라이언트리스 SSL VPN 포털 페이지에 클라이언트리스 VPN 세션이 만료할 때까지 남은 총 시간을 보여주는 카운트다운 타이머가 표시됩니다. 세션은 구성한 최대 허용 연결 시간의 마지막에 도달했거나 비활성화로 인해 시간 제한을 초과할 수 있습니다.

사용자 지정 메시지를 생성하여 사용자 세션이 유휴 시간 제한 또는 세션 시간 제한으로 인해 종료될 예정임을 사용자에게 알릴 수 있습니다. 사용자 지정 메시지는 기본 유휴 시간 제한 메시지를 교체합니다. 기본 메시지는 "`Your session will expire in` **%s**`(세션이 %s 후에 만료됩니다).`"입니다.메시지에 있는 `%s` 자리 표시자는 카운트다운 타이머가 작동되면 바뀝니다.

프로시저

단계 **1** ASDM을 시작하고 **Configuration(**구성**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **Clientless SSL VPN Access(**클라이언트리스 **SSL VPN** 액세스**)** > **Portal(**포털**)** > **Customization(**맞춤화**)**을 선택합니다.

단계 **2** **Add(**추가**)**를 클릭하여 새 사용자 지정 개체를 추가하거나 기존 사용자 지정 개체를 선택하고 **Edit(**수정**)**를 클릭하여 사용자 지정 유휴 시간 제한 메시지를 기존 사용자 지정 개체에 추가합니다.

단계 **3** Add/Edit Customization Object(사용자 지정 개체 추가/수정) 창에서 탐색 트리에 있는 포털 페이지 노드를 확장하고 **Timeout Alerts(**시간 제한 알림**)**를 클릭합니다.

단계 **4** **Enable alert visual tooltip(**시각적 툴팁 알림 활성화**)(**타이머 카운트다운의 빨간색 배경**)**을 선택합니다. 이렇게 하면 빨간색 배경에서 툴팁으로 카운트다운 타이머가 표시됩니다. 사용자가 남은 시간 영역을 클릭하면 이 시간 영역이 사용자 지정 시간 제한 알림 메시지를 표시하도록 확장됩니다. 이 상자를 선택하지 않으면 사용자에게 팝업 창으로 사용자 지정 시간 제한 알림이 표시됩니다.

단계 **5** 유휴 시간 제한 메시지 상자 및 세션 시간 제한 메시지 상자에 메시지를 입력합니다. 메시지의 예는 다음과 같습니다. `Warning: Your session will end in %s(경고: 세션이 %s 후에 종료됩니다). 작업을 마치고 애플리케이션을 종료할 준비를 하십시오.`

단계 **6** **OK(**확인**)**를 클릭합니다.

단계 **7** **Apply(**적용**)**를 클릭합니다.

사용자 지정 개체 파일에서 사용자 지정 시간 제한 알림 지정

필요한 경우 ASA 외부의 기존 사용자 지정 개체 파일을 수정하여 ASA에 가져올 수 있습니다.

시간 제한 메시지는 XML 사용자 지정 개체 파일의 <timeout-alerts> XML 요소에서 구성됩니다. <timeout-alerts> 요소는 <portal> 요소의 하위입니다. <portal> 요소는 <custom> 요소의 하위입니다.

<timeout-alerts> 요소는 <portal> 하위 요소의 순서에서 <home-page> 요소 다음, <application> 요소 이전에 위치합니다.

<timeout-alerts>의 다음 하위 요소를 지정해야 합니다.

- <alert-tooltip> – "예"로 설정하면 사용자에게 툴팁으로 빨간색 배경에 카운트다운 타이머가 표시됩니다. 카운트다운 타이머를 클릭하면 사용자 지정 메시지를 표시하도록 툴팁이 확장됩니다. "아니요"로 설정하거나 정의하지 않은 경우 사용자는 팝업 창으로 사용자 지정 메시지를 수신합니다.
- <session-timeout-message> – 이 요소에서 사용자 지정 세션 시간 제한 메시지를 입력합니다. 이 요소를 설정하고 비워 두지 않는 경우 사용자는 기본 메시지 대신 사용자 지정 메시지를 수신합니다. 메시지에 있는 %s 자리 표시자는 카운트다운 타이머를 작동시키면 교체됩니다.
- <idle-timeout-message> – 이 요소에서 사용자 지정 유휴 시간 제한 메시지를 입력합니다. 이 요소를 설정하고 비워 두지 않는 경우 사용자는 기본 메시지 대신 사용자 지정 메시지를 수신합니다. %s 자리 표시자는 카운트다운 타이머를 작동시키면 교체됩니다.

향후 작업

사용자 지정 개체 가져오기 및 내보내기 그리고 XML 기반 포털 사용자 지정 개체 및 URL 목록 생성을 읽어 보십시오.

시간 제한 알림 요소 및 하위 요소 구성 예

이 예에서는 <portal> 요소의 <timeout-alerts> 요소만 보여줍니다.

이 예를 기존 사용자 지정 개체에 잘라 붙여 넣지 마십시오.

```
  <portal>
      <window></window>
      <title-panel></title-panel>
      <toolbar></toolbar>
      <url-lists></url-lists>
      <navigation-panel></navigation-panel>
      <home-page>
      <timeout-alerts>
          <alert-tooltip>yes</alert-tooltip>
          <idle-timeout-message>You session expires in %s due to
idleness.</idle-timeout-message>
          <session-timeout-message>Your session expires in %s.</session-timeout-message>
      </timeout-alerts>
      <application></application>
      <column></column>
      <pane></pane>
      <external-portal></external-portal>
  </portal>
```

로그아웃 페이지 사용자 지정

다음 그림에서는 사용자 지정할 수 있는 로그아웃 페이지를 보여줍니다.

그림 ***21:*** 로그아웃 페이지의 구성 요소

로그아웃 페이지를 사용자 지정하려면 다음 절차를 따르십시오. Preview(미리보기) 버튼을 클릭하여 각 구성 요소에 대한 변경사항을 미리 볼 수 있습니다.

프로시저

단계 **1** 로그아웃 페이지로 이동합니다. 필요에 따라 제목 또는 텍스트를 사용자 지정합니다.

단계 **2** 사용자의 편의를 위해 로그아웃 페이지에 로그인 버튼을 표시할 수 있습니다. 이렇게 하려면 Show logon button(로그온 버튼 표시)을 선택합니다. 필요한 경우 버튼 텍스트를 사용자 지정합니다.

단계 **3** 제목 글꼴 또는 배경을 원하는 대로 사용자 지정합니다.

단계 **4** **OK(**확인**)**를 클릭한 다음 수정한 사용자 지정 개체에 변경 사항을 적용합니다.

사용자 지정 개체 추가

프로시저

단계 **1** **Add(**추가**)**를 클릭하고 새 사용자 지정 개체에 이름을 입력합니다. 최대값은 64자이며 공백은 포함하지 않습니다.

단계 **2** (선택 사항) **Find(**찾기**)**를 클릭하여 맞춤형 개체를 검색합니다. 필드에 입력하기 시작하면 툴이 모든 필드에서 시작 문자를 검색하여 일치하는 항목을 찾습니다. 와일드카드를 사용하여 검색을 확장할 수 있습니다. 예를 들어 Find(찾기) 필드에 *sal*을 입력하면 sales라는 사용자 지정 개체는 일치하지만 wholesalers라는 사용자 지정 개체는 일치하지 않습니다. Find(찾기) 필드에 **sal*을 입력한 경우에는 테이블에서 sales 또는 wholesalers의 첫 번째 인스턴스가 검색됩니다.

위로 화살표 및 아래로 화살표를 사용하여 일치하는 다음 문자열 위 또는 아래로 건너뜁니다. 검색에서 대/소문자를 구분하려면 **Match Case(**대/소문자 구분**)** 확인란을 선택합니다.

단계 **3** 로그인하는 동안 포털 페이지의 Password(비밀번호) 필드를 클릭하면 화면 키보드가 키보드를 활성화합니다. Username(사용자 이름) 상자에 대해서는 활성화되지 않습니다. 화면 키보드를 포털 페이지에 언제 표시할지 지정할 수 있습니다. 선택 항목은 다음과 같습니다.

- 화면 키보드를 표시하지 않음
- 로그인 페이지에만 표시
- 인증이 필요한 모든 포털 페이지에 표시

단계 **4** (선택 사항) 맞춤형 개체를 강조 표시하고 **Assign(**할당**)**을 클릭하여 선택한 개체를 하나 이상의 그룹 정책, 연결 프로필 또는 로컬 사용자에게 할당합니다.

사용자 지정 개체 가져오기/내보내기

기존 사용자 지정 개체를 가져오거나 내보낼 수 있습니다. 엔드 유저에게 적용할 개체를 가져옵니다. 수정하기 위해 ASA에 이미 있는 맞춤형 개체를 내보낸 다음 다시 가져올 수 있습니다.

프로시저

단계 **1** 이름으로 사용자 지정 개체를 식별합니다. 최대값은 64자이며 공백은 포함하지 않습니다.

단계 **2** 사용자 지정 파일을 가져오거나 내보내려면 다음 방법 중에서 선택합니다.

- Local computer(로컬 컴퓨터) — 로컬 PC에 있는 파일을 가져오려면 이 방법을 선택합니다.
- Path(경로) — 파일에 대한 경로를 제공합니다.
- Browse Local Files(로컬 파일 찾아보기) - 파일의 경로를 찾습니다.
- Flash file system(플래시 파일 시스템) — ASA에 있는 파일을 내보내려면 이 방법을 선택합니다.
- Path(경로) — 파일에 대한 경로를 제공합니다.
- Browse Flash(플래시 찾아보기) - 파일의 경로를 찾습니다.
- Remote server(원격 서버) — ASA에서 액세스할 수 있는 원격 서버에 있는 맞춤형 파일을 가져오려면 이 옵션을 선택합니다.
- Path(경로) — 파일(ftp, http 또는 https)에 액세스하는 방법을 식별하고 파일에 대한 경로를 제공합니다.

단계 **3** 파일을 가져오거나 내보내려면 클릭합니다.

XML 사용자 지정 파일 구조의 이해

다음 그림은 XML 사용자 지정 개체의 파일 구조를 나타냅니다.

참고 매개변수/태그가 없으면 기본/상속 값이 생성되며 있는 경우 빈 문자열이라도 매개변수/태그가 설정됩니다.

표 ***15: XML*** 기반 사용자 지정 파일 구조

태그	유형	값	사전 설정 값	설명
custom	노드	—	—	루트 태그
auth-page	노드	—	—	인증 페이지 구성의 태그 컨테이너

window	노드	—	—	브라우저 창
title-text	문자열	임의의 문자열	빈 문자열	—
title-panel	노드	—	—	로고 및 텍스트가 있는 페이지 맨 위 창
mode	text	enable|disable	disable	—
text	text	임의의 문자열	빈 문자열	—
logo-url	text	임의의 URL	빈 이미지 URL	—
copyright-panel	노드	—	—	저작권 정보가 있는 페이지 맨 아래 창
mode	text	enable|disable	disable	—
text	text	임의의 URL	빈 문자열	—
info-panel	노드	—	—	사용자 지정 텍스트 및 이미지가 있는 창
mode	문자열	enable|disable	disable	—
image-position	문자열	above|below	above	텍스트와 관련된 이미지 위치
image-url	문자열	임의의 URL	빈 이미지	—
text	문자열	임의의 문자열	빈 문자열	—
logon-form	노드	—	—	사용자 이름, 비밀번호, 그룹 확인 상자가 있는 양식
title-text	문자열	임의의 문자열	Logon	—
message-text	문자열	임의의 문자열	빈 문자열	—
username-prompt-text	문자열	임의의 문자열	Username	—
password-prompt-text	문자열	임의의 문자열	비밀번호	—
internal-password-prompt-text	문자열	임의의 문자열	Internal Password	—

group-prompt-text	문자열	임의의 문자열	그룹	—
submit-button-text	문자열	임의의 문자열	Logon	
logout-form	노드	—	—	로그아웃 메시지 및 로그인하거나 창을 닫는 버튼이 있는 양식
title-text	문자열	임의의 문자열	Logout	—
message-text	문자열	임의의 문자열	빈 문자열	—
login-button-text	문자열	임의의 문자열	로그인	
close-button-text	문자열	임의의 문자열	Close window	—
language-selector	노드	—	—	언어를 선택하는 드롭다운 목록
mode	문자열	enable|disable	disable	—
title	text	—	언어	언어를 선택하기 위한 확인 상자 텍스트
language	노드(다중)	—	—	—
code	string	—	—	—
text	string	—	—	—
portal	노드	—	—	포털 페이지 구성의 태그 컨테이너
window	노드	—	—	인증 페이지 설명 참조
title-text	문자열	임의의 문자열	빈 문자열	—
title-panel	노드	—	—	인증 페이지 설명 참조
mode	문자열	enable|disable	Disable	—
text	문자열	임의의 문자열	빈 문자열	—
logo-url	문자열	임의의 URL	빈 이미지 URL	—

navigation-panel	노드	—	—	애플리케이션 탭이 포함된 왼쪽에 있는 창
mode	문자열	enable|disable	enable	—
application	노드(다중)	—	해당 없음	노드는 ID별로 구성된 애플리케이션에 대한 기본값을 변경합니다.
id	문자열	재고 애플리케이션의 경우 web-access file-access app-access net-access help ins의 경우: 고유한 플러그인	해당 없음	—
tab-title	string	—	해당 없음	—
order	숫자	—	해당 없음	요소를 정렬하는 데 사용되는 값. 기본 요소 순서 값은 단계 1000, 2000, 3000 등이 있습니다. 예를 들어, 첫 번째와 두 번째 요소 간에 요소를 삽입하려면 1001부터 1999 사이의 값을 사용합니다.
url-list-title	string	—	해당 없음	애플리케이션에 책갈피가 있는 경우 그룹화된 책갈피에 대한 패널의 제목입니다.
mode	문자열	enable|disable	해당 없음	v
toolbar	노드	—	—	—

mode	문자열	enable|disable	Enable	—
prompt-box-title	문자열	임의의 문자열	주소:	URL 확인 상자 목록의 제목
browse-button-text	문자열	임의의 문자열	둘러보기	찾아보기 버튼 텍스트
logout-prompt-text	문자열	임의의 문자열	Logout	—
column	노드(다중)	—	—	기본적으로 한 개의 열이 표시됩니다.
width	string	—	해당 없음	—
order	숫자	—	해당 없음	요소를 정렬하는 데 사용되는 값.
url-lists	노드	—	—	명시적으로 해제되지 않은 경우 포털 홈 페이지의 기본 요소로 간주되는 URL 목록
mode	문자열	group | nogroup	group	모드: group - 애플리케이션 유형별(예: 웹 책갈피, 파일 책갈피)로 그룹화한 요소 no-group - 개별 창에 표시된 URL 목록 disable - 기본적으로 URL 목록을 표시 안 함
panel	노드 (다중)	—	—	추가 창을 구성할 수 있음
mode	문자열	enable|disable	—	구성을 제거하지 않고 패널을 일시적으로 해제하는 데 사용됨
title	string	—	—	—

type	string	—	—	Supported types: RSS 이미지 텍스트 HTML
url	string	—	—	RSS, 이미지 또는 HTML 유형 창의 URL
url-mode	string	—	—	모드: 변조, 변조 안 함
text	string	—	—	텍스트 유형 창에 대한 텍스트
column	숫자	—	—	—

사용자 지정 구성 예

다음 예에서는 다음의 사용자 지정 옵션을 보여줍니다.

- 파일 액세스 애플리케이션의 탭 숨기기
- 웹 액세스 애플리케이션의 제목 및 순서 변경
- 홈 페이지에서 2개의 열 정의
- RSS 창 추가
- 두 번째 창의 맨 위에 3개의 창(텍스트, 이미지 및 html) 추가

```
<custom name="Default">
  <auth-page>

    <window>
          <title-text l10n="yes">title WebVPN Logon</title>
    </window>

    <title-panel>
         <mode>enable</mode>
         <text l10n="yes">EXAMPLE WebVPN</text>
         <logo-url>http://www.example.com/images/EXAMPLE.gif</logo-url>
    </title-panel>

    <copyright>
         <mode>enable</mode>
         <text l10n="yes">(c)Copyright, EXAMPLE Inc., 2006</text>
    </copyright>

    <info-panel>
        <mode>enable</mode>
```

```
        <image-url>/+CSCOE+/custom/EXAMPLE.jpg</image-url>
      <text l10n="yes">
            <![CDATA[
            <div>
            <b>Welcome to WebVPN !.</b>
            </div>

      </text>
    </info-panel>
    <logon-form>
      <form>
          <title-text l10n="yes">title WebVPN Logon</title>
          <message-text l10n="yes">message WebVPN Logon</title>
          <username-prompt-text l10n="yes">Username</username-prompt-text>
          <password-prompt-text l10n="yes">Password</password-prompt-text>
          <internal-password-prompt-text l10n="yes">Domain
password</internal-password-prompt-text>
          <group-prompt-text l10n="yes">Group</group-prompt-text>
          <submit-button-text l10n="yes">Logon</submit-button-text>
      </form>
    </logon-form>
    <logout-form>
      <form>
          <title-text l10n="yes">title WebVPN Logon</title>
          <message-text l10n="yes">message WebVPN Logon</title>
          <login-button-text l10n="yes">Login</login-button-text>
          <close-button-text l10n="yes">Logon</close-button-text>
      </form>
    </logout-form>

    <language-slector>
      <language>
          <code l10n="yes">code1</code>
          <text l10n="yes">text1</text>
      </language>
      <language>
          <code l10n="yes">code2</code>
          <text l10n="yes">text2</text>
      </language>
    </language-slector>

  </auth-page>
  <portal>

    <window>
          <title-text l10n="yes">title WebVPN Logon</title>
    </window>

    <title-panel>
         <mode>enable</mode>
         <text l10n="yes">EXAMPLE WebVPN</text>
         <logo-url>http://www.example.com/logo.gif</logo-url>
    </title-panel>

    <navigation-panel>
         <mode>enable</mode>
    </navigation-panel>

    <application>
            <id>file-access</id>
            <mode>disable</mode>
    </application>
    <application>
            <id>web-access</id>
```

```
            <tab-title>EXAMPLE Intranet</tab-title>
            <order>3001</order>
      </application>

     <column>
            <order>2</order>
            <width>40%</width>
    <column>
     <column>
            <order>1</order>
            <width>60%</width>
    <column>

    <url-lists>
      <mode>no-group</mode>
    </url-lists>

    <pane>
     <id>rss_pane</id>
      <type>RSS</type>
     <url>rss.example.com?id=78</url>
    </pane>
    <pane>
      <type>IMAGE</type>
     <url>http://www.example.com/logo.gif</url>
      <column>1</column>
      <row>2</row>
     </pane>

    <pane>
      <type>HTML</type>
     <title>EXAMPLE news</title>
     <url>http://www.example.com/news.html</url>
      <column>1</column>
      <row>3</row>
     </pane>

    </portal>

  </custom>
```

사용자 지정 템플릿 사용

이름이 Template(템플릿)인 사용자 지정 템플릿에는 태그를 사용하는 방법을 설명하는 해당하는 주석과 함께 현재 적용된 모든 태그가 포함되어 있습니다. **export** 명령을 사용하여 다음과 같이 ASA에서 맞춤형 템플릿을 다운로드할 수 있습니다.

```
hostname# export webvpn customization Template tftp://webserver/default.xml
hostname#
```

Template 파일을 변경하거나 삭제할 수 없습니다. 파일을 내보낼 때 이 예에서와 같이 파일을 새 이름인 default.xml로 저장합니다. 조직의 요건을 충족하는 맞춤형 개체를 생성하도록 이 파일을 변경한 다음, 파일을 ASA에 default.xml 또는 다른 원하는 이름으로 가져옵니다. 예를 들면 다음과 같습니다.

```
hostname# import webvpn customization General tftp://webserver/custom.xml
hostname#
```

custom.xml이라는 XML 개체를 가져오고 ASA에서 이름을 General로 지정합니다.

사용자 지정 템플릿

이름이 Template인 사용자 지정 템플릿은 다음과 같습니다.

```
<?xml version="1.0" encoding="UTF-8" ?>
- <!--  Copyright (c) 2008,2009 by Cisco Systems, Inc. All rights reserved.  Note: all white
 spaces in tag values are significant and preserved.   Tag: custom Description: Root
customization tag  Tag: custom/languages Description: Contains list of languages, recognized
 by ASA Value: string containing comma-separated language codes. Each language code is
    a set dash-separated alphanumeric characters, started with        alpha-character (for
 example: en, en-us, irokese8-language-us) Default value: en-us Tag: custom/default-language
 Description: Language code that is selected when the client and the server
were not able to negotiate the language automatically.              For example the set of
 languages configured in the browser              is "en,ja", and the list of languages,
specified by              'custom/languages' tag is "cn,fr", the default-language will be
            used. Value: string, containing one of the language coded, specified in
'custom/languages' tag above. Default value: en-us
********************************************************** Tag: custom/auth-page Description:
 Contains authentication page settings
********************************************************** Tag: custom/auth-page/window
Description: Contains settings of the authentication page browser window  Tag:
custom/auth-page/window/title-text Description: The title of the browser window of the
authentication page Value: arbitrary string Default value: Browser's default value
********************************************************** Tag: custom/auth-page/title-panel
 Description: Contains settings for the title panel  Tag: custom/auth-page/title-panel/mode
 Description: The title panel mode Value: enable|disable Default value: disable Tag:
custom/auth-page/title-panel/text Description: The title panel text. Value: arbitrary string
 Default value: empty string  Tag: custom/auth-page/title-panel/logo-url Description: The
URL of the logo image (imported via "import webvpn webcontent") Value: URL string Default
value: empty image URL  Tag: custom/auth-page/title-panel/background-color Description: The
 background color of the title panel Value: HTML color format, for example #FFFFFF Default
 value: #FFFFFF  Tag: custom/auth-page/title-panel/font-color Description: The background
color of the title panel Value: HTML color format, for example #FFFFFF Default value: #000000
  Tag: custom/auth-page/title-panel/font-weight Description: The font weight Value: CSS
font size value, for example bold, bolder,lighter etc. Default value: empty string  Tag:
custom/auth-page/title-panel/font-size Description: The font size Value: CSS font size
value, for example 10pt, 8px, x-large, smaller etc. Default value: empty string     Tag:
custom/auth-page/title-panel/gradient Description: Specifies using the background color
gradient Value: yes|no Default value:no  Tag: custom/auth-page/title-panel/style Description:
 CSS style of the title panel Value: CSS style string Default value: empty string
**********************************************************  Tag:
custom/auth-page/copyright-panel Description: Contains the copyright panel settings  Tag:
custom/auth-page/copyright-panel/mode Description: The copyright panel mode Value:
enable|disable Default value: disable  Tag: custom/auth-page/copyright-panel/text Description:
 The copyright panel text Value: arbitrary string Default value: empty string
********************************************************** Tag: custom/auth-page/info-panel
 Description: Contains information panel settings  Tag: custom/auth-page/info-panel/mode
Description: The information panel mode Value: enable|disable Default value: disable  Tag:
 custom/auth-page/info-panel/image-position Description: Position of the image, above or
below the informational panel text Values: above|below Default value: above  Tag:
custom/auth-page/info-panel/image-url Description: URL of the information panel image
(imported via "import webvpn webcontent") Value: URL string Default value: empty image URL
  Tag: custom/auth-page/info-panel/text Description: Text of the information panel Text:
arbitrary string Default value: empty string
**********************************************************  Tag: custom/auth-page/logon-form
 Description: Contains logon form settings  Tag: custom/auth-page/logon-form/title-text
Description: The logon form title text Value: arbitrary string Default value: "Logon"  Tag:
 custom/auth-page/logon-form/message-text Description: The message inside of the logon form
 Value: arbitrary string Default value: empty string  Tag:
custom/auth-page/logon-form/username-prompt-text Description: The username prompt text
```

```
Value: arbitrary string Default value: "Username"  Tag:
custom/auth-page/logon-form/password-prompt-text Description: The password prompt text
Value: arbitrary string Default value: "Password"  Tag:
custom/auth-page/logon-form/internal-password-prompt-text Description: The internal password
 prompt text Value: arbitrary string Default value: "Internal Password"  Tag:
custom/auth-page/logon-form/group-prompt-text Description: The group selector prompt text
Value: arbitrary string Default value: "Group"   Tag:
custom/auth-page/logon-form/submit-button-text Description: The submit button text Value:
arbitrary string Default value: "Logon"  Tag:
custom/auth-page/logon-form/internal-password-first Description: Sets internal password
first in the order Value: yes|no Default value: no   Tag:
custom/auth-page/logon-form/title-font-color Description: The font color of the logon form
 title Value: HTML color format, for example #FFFFFF Default value: #000000  Tag:
custom/auth-page/logon-form/title-background-color Description: The background color of the
 logon form title Value: HTML color format, for example #FFFFFF Default value: #000000
Tag: custom/auth-page/logon-form/font-color Description: The font color of the logon form
Value: HTML color format, for example #FFFFFF Default value: #000000  Tag:
custom/auth-page/logon-form/background-color Description: The background color of the logon
 form Value: HTML color format, for example #FFFFFF Default value: #000000
********************************************************** Tag: custom/auth-page/logout-form
 Description: Contains the logout form settings  Tag: custom/auth-page/logout-form/title-text
 Description: The logout form title text Value: arbitrary string Default value: "Logout"
Tag: custom/auth-page/logout-form/message-text Description: The logout form message text
Value: arbitrary string Default value: Goodbye.              For your own security, please:
               Clear the browser's cache               Delete any downloaded files
          Close the browser's window  Tag: custom/auth-page/logout-form/login-button-text
Description: The text of the button sending the user to the logon page Value: arbitrary
string Default value: "Logon"  **********************************************************
Tag: custom/auth-page/language-selector Description: Contains the language selector settings
  Tag: custom/auth-page/language-selector/mode Description: The language selector mode
Value: enable|disable Default value: disable  Tag: custom/auth-page/language-selector/title
 Description: The language selector title Value: arbitrary string Default value: empty
string  Tag: custom/auth-page/language-selector/language (multiple) Description: Contains
the language settings  Tag: custom/auth-page/language-selector/language/code Description:
The code of the language Value (required): The language code string  Tag:
custom/auth-page/language-selector/language/text Description: The text of the language in
the language selector drop-down box Value (required): arbitrary string
********************************************************** Tag: custom/portal Description:
 Contains portal page settings  **********************************************************
 Tag: custom/portal/window Description: Contains the portal page browser window settings
Tag: custom/portal/window/title-text Description: The title of the browser window of the
portal page Value: arbitrary string Default value: Browser's default value
********************************************************** Tag: custom/portal/title-panel
Description: Contains settings for the title panel  Tag: custom/portal/title-panel/mode
Description: The title panel mode Value: enable|disable Default value: disable  Tag:
custom/portal/title-panel/text Description: The title panel text. Value: arbitrary string
Default value: empty string  Tag: custom/portal/title-panel/logo-url Description: The URL
of the logo image (imported via "import webvpn webcontent") Value: URL string Default value:
 empty image URL  Tag: custom/portal/title-panel/background-color Description: The background
 color of the title panel Value: HTML color format, for example #FFFFFF Default value:
#FFFFFF  Tag: custom/auth-pa/title-panel/font-color Description: The background color of
the title panel Value: HTML color format, for example #FFFFFF Default value: #000000  Tag:
 custom/portal/title-panel/font-weight Description: The font weight Value: CSS font size
value, for example bold, bolder,lighter etc. Default value: empty string  Tag:
custom/portal/title-panel/font-size Description: The font size Value: CSS font size value,
 for example 10pt, 8px, x-large, smaller etc. Default value: empty string Tag:
custom/portal/title-panel/gradient Description: Specifies using the background color gradient
 Value: yes|no Default value:no  Tag: custom/portal/title-panel/style Description: CSS style
 for title text Value: CSS style string Default value: empty string
********************************************************** Tag: custom/portal/application
(multiple) Description: Contains the application setting  Tag: custom/portal/application/mode
 Description: The application mode Value: enable|disable Default value: enable  Tag:
custom/portal/application/id Description: The application ID. Standard application ID's
are: home, web-access, file-access, app-access, network-access, help Value: The application
```

```
 ID string Default value: empty string  Tag: custom/portal/application/tab-title Description:
 The application tab text in the navigation panel Value: arbitrary string Default value:
empty string  Tag: custom/portal/application/order Description: The order of the application's
 tab in the navigation panel. Applications with lesser order go first. Value: arbitrary
number Default value: 1000  Tag: custom/portal/application/url-list-title Description: The
 title of the application's URL list pane (in group mode) Value: arbitrary string Default
value: Tab tite value concatenated with "Bookmarks"
********************************************************** Tag: custom/portal/navigation-panel
 Description: Contains the navigation panel settings  Tag: custom/portal/navigation-panel/mode
 Description: The navigation panel mode Value: enable|disable Default value: enable
********************************************************** Tag: custom/portal/toolbar
Description: Contains the toolbar settings  Tag: custom/portal/toolbar/mode Description:
The toolbar mode Value: enable|disable Default value: enable  Tag:
custom/portal/toolbar/prompt-box-title Description: The universal prompt box title Value:
arbitrary string Default value: "Address" Tag: custom/portal/toolbar/browse-button-text
Description: The browse button text Value: arbitrary string Default value: "Browse"  Tag:
custom/portal/toolbar/logout-prompt-text Description: The logout prompt text Value: arbitrary
 string Default value: "Logout"  **********************************************************
  Tag: custom/portal/column (multiple) Description: Contains settings of the home page
column(s)  Tag: custom/portal/column/order Description: The order the column from left to
right. Columns with lesser order values go
first Value: arbitrary number Default value: 0  Tag: custom/portal/column/width Description:
 The home page column width Value: percent Default value: default value set by browser Note:
 The actual width may be increased by browser to accommodate content
**********************************************************  Tag: custom/portal/url-lists
Description: Contains settings for URL lists on the home page  Tag:
custom/portal/url-lists/mode Description: Specifies how to display URL lists on the home
page:              group URL lists by application (group) or              show individual
URL lists (nogroup).              URL lists fill out cells of the configured columns, which
 are not taken             by custom panes.             Use the attribute value "nodisplay"
 to not show URL lists on the home page.  Value: group|nogroup|nodisplay Default value:
group ********************************************************** Tag: custom/portal/pane
(multiple) Description: Contains settings of the custom pane on the home page  Tag:
custom/portal/pane/mode Description: The mode of the pane Value: enable|disable Default
value: disable  Tag: custom/portal/pane/title Description: The title of the pane Value:
arbitrary string Default value: empty string  Tag: custom/portal/pane/notitle Description:
 Hides pane's title bar Value: yes|no Default value: no  Tag: custom/portal/pane/type
Description: The type of the pane. Supported types:              TEXT - inline arbitrary
text, may contain HTML tags;              HTML - HTML content specified by URL shown in the
 individual iframe;              IMAGE - image specified by URL              RSS - RSS feed
 specified by URL Value: TEXT|HTML|IMAGE|RSS Default value: TEXT  Tag: custom/portal/pane/url
 Description: The URL for panes with type  HTML,IMAGE or RSS Value: URL string Default
value: empty string  Tag: custom/portal/pane/text Description: The text value for panes
with type TEXT Value: arbitrary string Default value:empty string  Tag:
custom/portal/pane/column Description: The column where the pane located. Value: arbitrary
 number Default value: 1  Tag: custom/portal/pane/row Description: The row where the pane
is located Value: arbitrary number Default value: 1  Tag: custom/portal/pane/height
Description: The height of the pane Value: number of pixels Default value: default value
set by browser   ********************************************************** Tag:
custom/portal/browse-network-title Description: The title of the browse network link Value:
 arbitrary string Default value: Browse Entire Network   Tag:
custom/portal/access-network-title Description: The title of the link to start a network
access session Value: arbitrary string Default value: Start AnyConnect  -->
- <custom>
- <localization>
<languages>en,ja,zh,ru,ua</languages>
<default-language>en</default-language>
</localization>
- <auth-page>
- <window>
- <title-text l10n="yes">
- <![CDATA[
WebVPN Service
```

```
</title-text>
</window>
- <language-selector>
<mode>disable</mode>
<title l10n="yes">Language:</title>
- <language>
<code>en</code>
<text>English</text>
</language>
- <language>
<code>zh</code>
<text>?? (Chinese)</text>
</language>
- <language>
<code>ja</code>
<text>?? (Japanese)</text>
</language>
- <language>
<code>ru</code>
<text>??????? (Russian)</text>
</language>
- <language>
<code>ua</code>
<text>?????????? (Ukrainian)</text>
</language>
</language-selector>
- <logon-form>
- <title-text l10n="yes">
- <![CDATA[
Login

</title-text>
- <title-background-color>
- <![CDATA[
#666666

</title-background-color>
- <title-font-color>
- <![CDATA[
#ffffff

</title-font-color>
- <message-text l10n="yes">
- <![CDATA[
Please enter your username and password.

</message-text>
- <username-prompt-text l10n="yes">
- <![CDATA[
USERNAME:

</username-prompt-text>
- <password-prompt-text l10n="yes">
- <![CDATA[
PASSWORD:

</password-prompt-text>
<internal-password-prompt-text l10n="yes" />
<internal-password-first>no</internal-password-first>
- <group-prompt-text l10n="yes">
- <![CDATA[
GROUP:

</group-prompt-text>
```

```
- <submit-button-text l10n="yes">
- <![CDATA[
Login

</submit-button-text>
- <title-font-color>
- <![CDATA[
#ffffff

</title-font-color>
- <title-background-color>
- <![CDATA[
#666666

</title-background-color>
<font-color>#000000</font-color>
<background-color>#ffffff</background-color>
</logon-form>
- <logout-form>
- <title-text l10n="yes">
- <![CDATA[
Logout

</title-text>
- <message-text l10n="yes">
- <![CDATA[
Goodbye.

</message-text>
</logout-form>
- <title-panel>
<mode>enable</mode>
- <text l10n="yes">
- <![CDATA[
WebVPN Service

</text>
<logo-url l10n="yes">/+CSCOU+/csco_logo.gif</logo-url>
<gradient>yes</gradient>
<style />
- <background-color>
- <![CDATA[
#ffffff

</background-color>
- <font-size>
- <![CDATA[
larger

</font-size>
- <font-color>
- <![CDATA[
#800000

</font-color>
- <font-weight>
- <![CDATA[
bold

</font-weight>
</title-panel>
- <info-panel>
<mode>disable</mode>
<image-url l10n="yes">/+CSCOU+/clear.gif</image-url>
```

```
<image-position>above</image-position>
<text l10n="yes" />
</info-panel>
- <copyright-panel>
<mode>disable</mode>
<text l10n="yes" />
</copyright-panel>
</auth-page>
- <portal>
- <title-panel>
<mode>enable</mode>
- <text l10n="yes">
- <![CDATA[
WebVPN Service

</text>
<logo-url l10n="yes">/+CSCOU+/csco_logo.gif</logo-url>
<gradient>yes</gradient>
<style />
- <background-color>
- <![CDATA[
#ffffff

</background-color>
- <font-size>
- <![CDATA[
larger

</font-size>
- <font-color>
- <![CDATA[
#800000

</font-color>
- <font-weight>
- <![CDATA[
bold

</font-weight>
</title-panel>
<browse-network-title l10n="yes">Browse Entire Network</browse-network-title>
<access-network-title l10n="yes">Start AnyConnect</access-network-title>
- <application>
<mode>enable</mode>
<id>home</id>
<tab-title l10n="yes">Home</tab-title>
<order>1</order>
</application>
- <application>
<mode>enable</mode>
<id>web-access</id>
- <tab-title l10n="yes">
- <![CDATA[
Web Applications

</tab-title>
- <url-list-title l10n="yes">
- <![CDATA[
Web Bookmarks

</url-list-title>
<order>2</order>
</application>
- <application>
```

```
<mode>enable</mode>
<id>file-access</id>
- <tab-title l10n="yes">
- <![CDATA[
Browse Networks

</tab-title>
- <url-list-title l10n="yes">
- <![CDATA[
File Folder Bookmarks

</url-list-title>
<order>3</order>
</application>
- <application>
<mode>enable</mode>
<id>app-access</id>
- <tab-title l10n="yes">
- <![CDATA[
Application Access

</tab-title>
<order>4</order>
</application>
- <application>
<mode>enable</mode>
<id>net-access</id>
<tab-title l10n="yes">AnyConnect</tab-title>
<order>4</order>
</application>
- <application>
<mode>enable</mode>
<id>help</id>
<tab-title l10n="yes">Help</tab-title>
<order>1000000</order>
</application>
- <toolbar>
<mode>enable</mode>
<logout-prompt-text l10n="yes">Logout</logout-prompt-text>
<prompt-box-title l10n="yes">Address</prompt-box-title>
<browse-button-text l10n="yes">Browse</browse-button-text>
</toolbar>
- <column>
<width>100%</width>
<order>1</order>
</column>
- <pane>
<type>TEXT</type>
<mode>disable</mode>
<title />
<text />
<notitle />
<column />
<row />
<height />
</pane>
- <pane>
<type>IMAGE</type>
<mode>disable</mode>
<title />
<url l10n="yes" />
<notitle />
<column />
<row />
```

```
<height />
</pane>
- <pane>
<type>HTML</type>
<mode>disable</mode>
<title />
<url l10n="yes" />
<notitle />
<column />
<row />
<height />
</pane>
- <pane>
<type>RSS</type>
<mode>disable</mode>
<title />
<url l10n="yes" />
<notitle />
<column />
<row />
<height />
</pane>
- <url-lists>
<mode>group</mode>
</url-lists>
</portal>
</custom>
```

도움말 사용자 지정

ASA는 클라이언트리스 세션 중에 애플리케이션 창에 도움말 콘텐츠를 표시합니다. 각 클라이언트리스 애플리케이션 창은 사전 결정된 파일 이름을 사용하여 자체 도움말 파일 콘텐츠를 표시합니다. 예를 들어, 애플리케이션 액세스 패널에 표시되는 도움말 콘텐츠는 이름이 app-access-hlp.inc인 파일에서 가져옵니다. 다음 표는 도움말 콘텐츠에 대한 클라이언트리스 애플리케이션 패널 및 사전 결정된 파일 이름을 보여줍니다.

표 ***16:*** 클라이언트리스 애플리케이션

애플리케이션 유형	패널	파일 이름
표준	Application Access	app-access-hlp.inc
표준	Browse Networks	file-access-hlp.inc
표준	AnyConnect Client	net-access-hlp.inc
표준	Web Access	web-access-hlp.inc
플러그인	MetaFrame Access	ica-hlp.inc
플러그인	Terminal Servers	rdp-hlp.inc
플러그인	Telnet/SSH 서버	ssh,telnet-hlp.inc
플러그인	VNC Connections	vnc-hlp.inc

[3] 이 플러그인은 sshv1 및 sshv2를 모두 수행할 수 있습니다.

Cisco에서 제공하는 도움말 파일을 사용자 지정하거나 다른 언어로 도움말 파일을 생성할 수 있습니다. 그런 다음 Import(가져오기) 버튼을 사용하여 해당 파일을 ASA 플래시 메모리에 복사하면 후속 클라이언트리스 세션 중에 이를 표시할 수 있습니다. 이전에 가져온 도움말 콘텐츠 파일을 내보내고 사용자 지정하며 플래시 메모리에 다시 가져올 수 있습니다.

프로시저

단계 **1** **Import(**가져오기**)**를 클릭하여 Import Application Help Content(애플리케이션 도움말 콘텐츠 가져오기) 대화 상자를 실행합니다. 이 대화 상자에서 클라이언트리스 세션 동안 표시할 새로운 도움말 콘텐츠를 플래시 메모리로 가져올 수 있습니다.

단계 **2** (선택 사항) **Export(**내보내기**)**를 클릭하여 테이블에서 선택해 이전에 가져온 도움말 콘텐츠를 검색합니다.

단계 **3** (선택 사항) **Delete(**삭제**)**를 클릭하여 테이블에서 선택해 이전에 가져온 도움말 콘텐츠를 삭제합니다.

단계 **4** 브라우저에서 렌더링한 언어의 약어가 표시됩니다. 이 필드는 파일 변환에 사용되지 않으며 파일에서 사용된 언어를 표시합니다. 테이블에 있는 약어와 연계된 언어 이름을 식별하기 위해 브라우저에서 렌더링한 언어 목록이 표시됩니다. 예를 들어 대화 창은 다음 절차 중 하나를 사용하는 경우 언어 및 연계된 언어 코드를 표시합니다.

- Internet Explorer를 열고 **Tools(**도구**) > Internet Options(**인터넷 옵션**) > Languages(**언어**) > Add(**추가**)**를 선택합니다.
- Mozilla Firefox를 열어 **Tools(**도구**) > Options(**옵션**) > Advanced(**고급**) > General(**일반**)**을 선택하고 Language(언어) 옆에 있는 **Choose(**선택**)**를 클릭한 다음 **Select a language to add(**추가할 언어 선택**)**를 클릭합니다.

도움말 콘텐츠 파일을 가져올 때와 같은 파일 이름이 제공됩니다.

Cisco에서 제공한 도움말 파일 사용자 지정

Cisco에서 제공하는 도움말 파일을 사용자 지정하려면 먼저 플래시 메모리 카드에서 가져온 파일의 복사본이 필요합니다.

프로시저

단계 **1** 브라우저를 사용하여 ASA에 클라이언트리스 세션을 설정합니다.

단계 **2** 다음 표에서 "보안 어플라이언스의 플래시 메모리에 있는 도움말 파일의 URL"에 있는 문자열을 ASA의 주소에 추가하고 아래 설명된 대로 언어를 대체하여 도움말 파일을 표시한 다음 **Enter(**확인**)** 키를 누릅니다.

표 ***17:*** 클라이언트리스 애플리케이션에 대해 ***Cisco***에서 제공하는 도움말 파일

애플리케이션 유형	패널	보안 어플라이언스의 플래시 메모리에 있는 도움말 파일의 **URL**
표준	Application Access	/+CSCOE+/help/*language*/app-access-hlp.inc
표준	Browse Networks	/+CSCOE+/help/*language*/file-access-hlp.inc
표준	AnyConnect Client	/+CSCOE+/help/*language*/net-access-hlp.inc
표준	Web Access	/+CSCOE+/help/*language*/web-access-hlp.inc
플러그인	Terminal Servers	/+CSCOE+/help/*language*/rdp-hlp.inc
플러그인	Telnet/SSH Servers	/+CSCOE+/help/*language*/ssh,telnet-hlp.inc
플러그인	VNC Connections	/+CSCOE+/help/*language*/vnc-hlp.inc

*language(*언어*)*는 브라우저에서 렌더링한 언어의 약어입니다. 이 약어는 파일 변환에 사용되지 않으며 파일에서 사용된 언어를 표시합니다. 영어로 Cisco에서 제공하는 도움말 파일의 경우 약어 **en**을 입력합니다.

다음 예의 주소는 터미널 서버 도움말의 영어 버전을 표시합니다.

https://address_of_security_appliance**/+CSCOE+/help/en/rdp-hlp.inc**

단계 **3** **File(**파일**)** > **Save (Page) As(**다른 이름으로**(**페이지**)** 저장**)**를 선택합니다.

참고 File Name(파일 이름) 상자의 콘텐츠를 변경하지 마십시오.

단계 **4** 다른 이름으로 저장 유형 옵션을 **Web Page, HTML only(**웹 페이지**, HTML** 전용**)**로 변경하고 **Save(**저장**)**를 클릭합니다.

단계 **5** 기본 설정 HTML 편집기를 사용하여 파일을 사용자 지정합니다.

참고 대부분의 HTML 태그를 사용할 수는 있지만 문서 및 그 구조를 정의하는 태그는 사용하지 마십시오. 예를 들어, <html>, <title>, <body>, <head><h1>, <h2> 등은 사용하지 마십시오. <b> 태그와 같은 문자 태그와 <p>, <ol>, 및 <li> 태그를 구조 콘텐츠에 사용할 수 있습니다.

단계 **6** 원본 파일 이름 및 내선 번호를 사용하여 파일을 HTML 전용으로 저장합니다. 파일 이름에 추가 파일 이름 확장자가 없는지 확인합니다.

다음에 수행할 작업

ASDM으로 돌아가 **Configuration(**구성**) > Remote Access VPN > Clientless SSL VPN Access** > **Portal(**포털**)** > **Help Customization(**도움말 맞춤화**)** > **Import(**가져오기**)**를 선택하여 수정된 도움말 파일을 플래시 메모리에 가져옵니다.

Cisco에서 제공하지 않는 언어로 도움말 파일 작성

표준 HTML을 사용하여 다른 언어로 도움말 파일을 생성합니다. 지원할 각 언어에 대해 개별 폴더를 생성하는 것을 권장합니다.

참고 대부분의 HTML 태그를 사용할 수는 있지만 문서 및 구조를 정의하는 태그는 사용하지 마십시오. (예: 다음 태그는 사용하지 마십시오. <html>, <title>, <body>, <head><h1>, <h2> 등. <b> 태그와 같은 문자 태그는 사용할 수 있습니다. <p>, <ol>, 및 <li> 구조 콘텐츠에 대한 태그도 사용할 수 있습니다.

파일을 HTML 전용으로 저장합니다. 파일 이름 열에 있는 파일 이름을 사용합니다.

ASDM으로 돌아가 **Configuration(**구성**) > Remote Access VPN > Clientless SSL VPN Access** > **Portal(**포털**) > Help Customization(**도움말 맞춤화**) > Import(**가져오기**)**를 선택하여 새 도움말 파일을 플래시 메모리에 가져옵니다.

애플리케이션 도움말 콘텐츠 가져오기/내보내기

Import Application Help Content(애플리케이션 도움말 콘텐츠 가져오기) 대화 상자를 사용하여 클라이언트리스 세션 동안 포털 페이지에 표시하기 위해 플래시 메모리에 도움말 파일을 가져옵니다. Export Application Help Content(애플리케이션 도움말 콘텐츠 내보내기) 대화 상자를 사용하여 후속 수정을 위해 이전에 가져온 도움말 파일을 검색합니다.

프로시저

단계 **1** Language(언어) 필드는 브라우저에서 렌더링하는 언어를 지정하지만 파일 변환에 사용되지는 않습니다. (이 필드는 Export Application Help Content(애플리케이션 도움말 콘텐츠 내보내기) 대화 상자에서 비활성 상태입니다.) Language(언어) 필드 옆에 있는 점을 클릭하고 Browse Language Code(언어 코드 찾아보기) 대화 상자에 표시되는 언어를 포함하는 행을 두 번 클릭합니다. Language Code(언어 코드) 필드의 약어가 행에 있는 약어와 일치하는지 확인하고 **OK(**확인**)**를 클릭합니다.

단계 **2** 도움말 콘텐츠를 제공하는 데 필요한 언어가 Browse Language Code(언어 코드 찾아보기) 대화 상자에 표시되지 않는 경우, 다음을 수행합니다.

a) 브라우저에서 렌더링한 약어 및 언어 목록을 표시합니다.

b) 언어에 대한 약어를 Language Code(언어 코드) 필드에 입력하고 **OK(**확인**)**를 클릭합니다.

또는

점 왼쪽에 있는 Language(언어) 텍스트 상자에 약어를 입력할 수도 있습니다.

대화 상자는 다음 절차 중 하나를 사용하는 경우 언어 및 연계된 언어 코드를 표시합니다.

- Internet Explorer를 열고 **Tools(**도구**) > Internet Options(**인터넷 옵션**) > Languages(**언어**) > Add(**추가**)**를 선택합니다.

- Mozilla Firefox를 열어 **Tools(**도구**) > Options(**옵션**) > Advanced(**고급**) > General(**일반**)**을 선택하고 Language(언어) 옆에 있는 **Choose(**선택**)**를 클릭한 다음 **Select a language to add(**추가할 언어 선택**)**를 클릭합니다.

단계 **3** 가져오는 경우 File Name(파일 이름) 드롭다운 목록에서 새 도움말 콘텐츠 파일을 선택합니다. 내보내는 경우 이 필드를 사용할 수 없습니다.

단계 **4** 소스 파일(가져오는 경우) 또는 대상 파일(내보내는 경우)에 대해 다음의 매개변수를 구성합니다.

- Local computer(로컬 컴퓨터) — 소스 또는 대상 파일이 로컬 컴퓨터에 있는지 표시합니다.
  - Path(경로) — 소스 또는 대상 파일의 경로를 식별합니다.
  - Browse Local Files(로컬 파일 찾아보기) - 소스 또는 대상 파일의 로컬 컴퓨터를 찾으려면 클릭합니다.
- Flash file system(플래시 파일 시스템) — 소스 또는 대상 파일이 ASA의 플래시 메모리에 있는지 표시합니다.
  - Path(경로) — 플래시 메모리에서 소스 또는 대상 파일의 경로를 식별합니다.
  - Browse Flash(플래시 찾아보기) - 소스 또는 대상 파일의 플래시 메모리를 찾으려면 클릭합니다.
- Remote server(원격 서버) — 소스 또는 대상 파일이 원격 서버에 있는지 표시합니다.
  - Path(경로) — 파일 전송(복사) 방법을 ftp, tftp 또는 http(가져오기만 해당) 중에서 선택하고 경로를 지정합니다.

책갈피 도움말 사용자 지정

ASA는 선택한 각 책갈피에 대해 애플리케이션 패널에 도움말 콘텐츠를 표시합니다. 이 도움말 파일을 사용자 지정하거나 다른 언어로 도움말 파일을 생성할 수 있습니다. 그런 다음 도움말 파일을 플래시 메모리로 가져와서 후속 세션 동안 표시할 수 있습니다. 또한 이전에 가져온 도움말 콘텐츠 파일을 검색하고, 수정하고, 플래시 메모리로 다시 가져올 수 있습니다.

각 애플리케이션 패널에서는 미리 정해진 파일 이름을 사용하여 고유의 도움말 파일 콘텐츠를 표시합니다. 각 항목의 예상 위치는 ASA의 플래시 메모리 내의 /+CSCOE+/help/*language*/ URL입니다. 다음 표에서는 사용자가 VPN 세션을 위해 유지 관리할 수 있는 도움말 파일 각각에 대한 세부사항을 보여줍니다.

표 ***18: VPN*** 애플리케이션 도움말 파일

애플리케이션 유형	패널	보안어플라이언스의플래시 메모리에 있는도움말 파일의 **URL**	**Cisco**에서 영어로 된 도움말 파일을 제공했습니까**?**
표준	Application Access	/+CSCOE+/help/*language*/app-access-hlp.inc	예
표준	Browse Networks	/+CSCOE+/help/*language*/file-access-hlp.inc	예
표준	AnyConnect Client	/+CSCOE+/help/*language*/net-access-hlp.inc	예
표준	Web Access	/+CSCOE+/help/*language*/web-access-hlp.inc	예
플러그인	MetaFrame Access	/+CSCOE+/help/*language*/ica-hlp.inc	아니요
플러그인	Terminal Servers	/+CSCOE+/help/*language*/rdp-hlp.inc	예
플러그인	Telnet/SSH Servers	/+CSCOE+/help/*language*/ssh,telnet-hlp.inc	예
플러그인	VNC Connections	/+CSCOE+/help/*language*/vnc-hlp.inc	예

*language*는 브라우저에서 렌더링한 언어의 약어입니다. 이 필드는 파일 변환에 사용되지 않으며 파일에서 사용된 언어를 표시합니다. 특정 언어 코드를 지정하려면 브라우저에서 렌더링한 언어 목록에서 언어 약어를 복사합니다. 예를 들어 대화 창은 다음 절차 중 하나를 사용하는 경우 언어 및 연계된 언어 코드를 표시합니다.

- Internet Explorer를 열고 **Tools(**도구**) > Internet Options(**인터넷 옵션**) > Languages(**언어**) > Add(**추가**)**를 선택합니다.
- Mozilla Firefox를 열어 **Tools(**도구**) > Options(**옵션**) > Advanced(**고급**) > General(**일반**)**을 선택하고 Language(언어) 옆에 있는 **Choose(**선택**)**를 클릭한 다음 **Select a language to add(**추가할 언어 선택**)**를 클릭합니다.

언어 변환 이해

ASA는 전체 클라이언트리스 SSL VPN 세션에 대한 언어 변환 기능을 제공합니다. 언어 변환에는 로그인, 로그아웃 배너와 플러그인 및 AnyConnect와 같은 인증 후에 표시되는 포털 페이지가 포함됩니다. 원격 사용자에게 표시되는 기능 영역 및 메시지는 변환 도메인으로 구성됩니다. 다음 표는 변환 도메인 및 변환되는 기능 영역을 보여줍니다.

언어 변환 도메인 옵션

변환 도메인	변환되는 기능 영역
AnyConnect	Cisco AnyConnect VPN Client의 사용자 인터페이스에 표시되는 메시지입니다.
banners	VPN 액세스가 클라이언트리스 연결에 대해 거부되는 경우 표시되는 메시지

변환 도메인	변환되는 기능 영역
CSD	CSD(Cisco Secure Desktop)의 메시지입니다.
customization	로그인 및 로그아웃 페이지, 포털 페이지 및 사용자가 사용자 지정할 수 있는 모든 메시지
plugin-ica	Citrix 플러그인의 메시지입니다.
plugin-rdp	Remote Desktop Protocol 플러그인의 메시지입니다.
plugin-rdp2	Java 원격 데스크톱 프로토콜 플러그인에 대한 메시지입니다.
plugin-telnet,ssh	Telnet 및 SSH 플러그인의 메시지입니다.
plugin-vnc	VNC 플러그인의 메시지입니다.
PortForwarder	포트 전달 사용자에게 표시되는 메시지
url-list	사용자가 포털 페이지에서 URL 북마크에 대해 지정하는 텍스트입니다.
webvpn	모든 Layer 7, AAA 및 사용자 지정 불가능한 포털 메시지입니다.

ASA에는 표준 기능의 일부인 각 도메인에 대한 변환 테이블 템플릿이 포함되어 있습니다. 플러그인용 템플릿은 플러그인에 포함되어 있으며 고유한 변환 도메인을 정의합니다.

제공하는 URL에서 템플릿의 XML 파일을 생성하는 변환 도메인에 대해 템플릿을 내보낼 수 있습니다. 이 파일의 메시지 필드는 비어 있습니다. 플래시 메모리에 있는 새로운 변환 테이블 개체를 생성하기 위해 이 메시지를 수정하고 템플릿을 가져올 수 있습니다.

또한 기존의 변환 테이블을 내보낼 수 있습니다. 생성한 XML 파일에 이전에 수정한 메시지가 표시됩니다. 동일한 언어 이름의 이 XML 파일을 다시 가져오면 새 버전의 변환 테이블 개체가 생성되고 이전 메시지를 덮어씁니다.

일부 템플릿은 정적이지만 일부는 ASA의 구성에 기초하여 변경됩니다. 클라이언트리스 사용자에 대해 로그온 및 로그아웃 페이지, 포털 페이지 및 URL 북마크를 사용자 지정할 수 있으므로 **ASA generates the customization** 및 **url-list**는 변환 도메인 템플릿을 동적으로 생성하고 템플릿은 자동으로 이 기능 영역의 변경 사항을 반영합니다.

변환 테이블을 생성한 후, 그룹 정책 또는 사용자 특성을 생성하고 적용하는 사용자 지정 개체에 사용할 수 있습니다. AnyConnect 변환 도메인을 예외로 하면 변환 테이블에 아무런 영향을 주지 않으며, 사용자 지정 개체를 생성하고 해당 개체에 사용할 변환 테이블을 식별하며 그룹 정책 또는 사용자에 대한 사용자 지정을 지정할 때까지 메시지가 사용자 화면에서 변환되지 않습니다. AnyConnect 도메인에 대한 변환 테이블 변경 사항은 AnyConnect 클라이언트 사용자에게 바로 표시됩니다.

변환 테이블 수정

프로시저

단계 **1** Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > Language Localization(언어 현지화)으로 이동합니다. Language Localization(언어 현지화) 창이 표시되면 **Add(**추가**)**를 클릭합니다.

단계 **2** 드롭다운 상자에서 언어 현지화 템플릿을 선택합니다. 상자에 있는 항목은 변환된 기능 영역에 해당됩니다.

단계 **3** 템플릿 언어를 지정합니다. 템플릿은 캐시 메모리에서 지정한 이름을 지닌 변환 테이블이 됩니다. 브라우저의 언어 옵션과 호환되는 약어를 사용합니다. 예를 들어 중국어용으로 테이블을 생성하고 IE를 사용 중인 경우, IE에서 인식할 수 있는 약어인 *zh*를 사용합니다.

단계 **4** 변환 테이블을 수정합니다. 변환할 msgid 필드별로 표시한 각 메시지에 대해 연계된 msgstr 필드의 따옴표 사이에 변환한 텍스트를 입력합니다. 아래는 Connected(연결됨) 메시지를 msgstr 필드에서 스페인어 텍스트로 입력한 예를 보여줍니다.

```
msgid "Connected"
msgstr "Conectado"
```

단계 **5** **OK(**확인**)**를 클릭합니다.

변환 테이블 추가

템플릿에 기반하여 새 변환 테이블을 추가하거나 이 창에서 이미 가져온 변환 테이블을 수정할 수 있습니다.

프로시저

단계 **1** 새 변환 테이블의 기초로 사용하고 수정할 템플릿을 선택합니다. 이 템플릿은 변환 도메인으로 구성되며 기능의 특정한 영역에 영향을 줍니다.

단계 **2** 드롭다운에서 변환 도메인을 선택합니다.

단계 **3** 언어를 지정합니다. 브라우저의 언어 옵션과 호환되는 약어를 사용합니다. ASA는 이 이름을 지닌 새 변환 테이블을 생성합니다.

단계 **4** 편집기를 사용하여 메시지 변환을 변경합니다. 메시지 ID 필드(msgid)에는 기본 변환이 포함됩니다. 메시지 문자열 필드(msgstr)는 변환을 제공하는 msgid 뒤에 옵니다. 변환을 생성하려면 msgstr 문자열의 따옴표 사이에 변환된 텍스트를 입력하십시오. 예를 들어, 메시지 “Connected”를 스페인어 변환을 통해 변환하려면 다음과 같이 msgstr 따옴표 사이에 스페인어 텍스트를 입력합니다.

```
msgid "Connected"
msgstr "Conectado"
```

변경한 후에 **Apply(**적용**)**를 클릭하여 변환 테이블을 가져옵니다.

21 장

클라이언트리스 SSL VPN 문제 해결

애플리케이션 액세스 사용 시 호스트 파일 오류 복구

애플리케이션 액세스를 방해할 수 있는 호스트 파일 오류를 방지하기 위해 애플리케이션 액세스 사용을 마치면 Application Access(애플리케이션 액세스) 창을 올바르게 닫습니다. 이렇게 하려면 닫기 아이콘을 클릭합니다.

애플리케이션 액세스가 비정상적으로 종료되는 경우 `hosts` 파일은 클라이언트리스 SSL VPN 사용자 지정 상태로 유지됩니다. 클라이언트리스 SSL VPN은 hosts.webvpn 파일을 검색하여 다음에 애플리케이션 액세스를 시작하는 상태를 확인합니다. 파일을 발견한 경우, `Backup HOSTS File Found` 오류 메시지가 나타나고 애플리케이션 액세스가 일시적으로 해제됩니다.

애플리케이션 액세스를 잘못 종료하면 원격 액세스 클라이언트/서버 애플리케이션이 불안정한 상태로 남습니다. 클라이언트리스 SSL VPN을 사용하지 않고 이 애플리케이션을 시작하려고 하는 경우, 제대로 작동하지 않을 수 있습니다. 이 경우 정상적으로 연결된 호스트를 사용하지 못할 수 있습니다. 이러한 상황은 일반적으로 집에서 원격으로 애플리케이션을 실행하는 경우, 컴퓨터를 종료하기 전에 애플리케이션 액세스 창을 종료하지 못하고 나중에 사무실에서 애플리케이션을 실행하려고 시도하는 경우 발생할 수 있습니다.

Application Access(애플리케이션 액세스) 창을 제대로 닫지 않은 경우 다음 오류가 발생할 수 있습니다.

- 다음에 애플리케이션 액세스를 시작하려고 시도하는 경우, 애플리케이션 액세스가 해제되고 `Backup HOSTS File Found` 오류 메시지가 표시될 수 있습니다.
- 애플리케이션을 로컬로 실행 중인 경우에도 애플리케이션이 해제되거나 제대로 작동하지 않을 수 있습니다

이러한 오류는 부적절한 방법으로 애플리케이션 액세스 창을 종료하는 경우 발생할 수 있습니다. 예를 들면 다음과 같습니다.

- 애플리케이션 액세스 사용 중에 브라우저 충돌
- 애플리케이션 액세스 사용 중에 정전 또는 시스템 종료 발생
- 작업 중에 애플리케이션 액세스 창을 최소화한 다음, 창이 활성화되어 있는 상태(단, 최소화된 상태)에서 컴퓨터 종료

호스트 파일 이해

로컬 시스템의 호스트 파일은 IP 주소를 호스트 이름에 매핑합니다. 애플리케이션 액세스를 시작하는 경우, 클라이언트리스 SSL VPN은 클라이언트리스 SSL VPN 특정 항목을 추가하여 이 호스트 파일을 수정합니다. Application Access(애플리케이션 액세스) 창을 올바르게 닫아 애플리케이션 액세스를 중지하면 이 파일이 원래 상태로 되돌아갑니다.

애플리케이션 액세스 호출 전...	호스트 파일은 원래 상태입니다.
애플리케이션 액세스 시작 시....	• 클라이언트리스 SSL VPN은 호스트 파일을 hosts.webvpn에 복사한 다음 백업을 생성합니다. • 클라이언트리스 SSL VPN은 클라이언트리스 SSL VPN 특정 정보를 삽입하여 호스트 파일을 수정합니다.
애플리케이션 액세스 중지 시...	• 클라이언트리스 SSL VPN은 백업 파일을 `hosts` 파일에 복사한 다음 호스트 파일을 원래 상태로 복원합니다. • 클라이언트리스 SSL VPN은 hosts.webvpn을 삭제합니다.
애플리케이션 액세스 완료 후...	호스트 파일은 원래 상태입니다.

참고 Microsoft 안티스파이웨어 소프트웨어는 포트 전달 Java 애플릿이 호스트 파일을 변경하는 것을 차단합니다. 안티스파이웨어 소프트웨어를 사용 중인 경우 호스트 파일 변경사항을 허용하는 방법에 대해서는 www.microsoft.com을 참조하십시오.

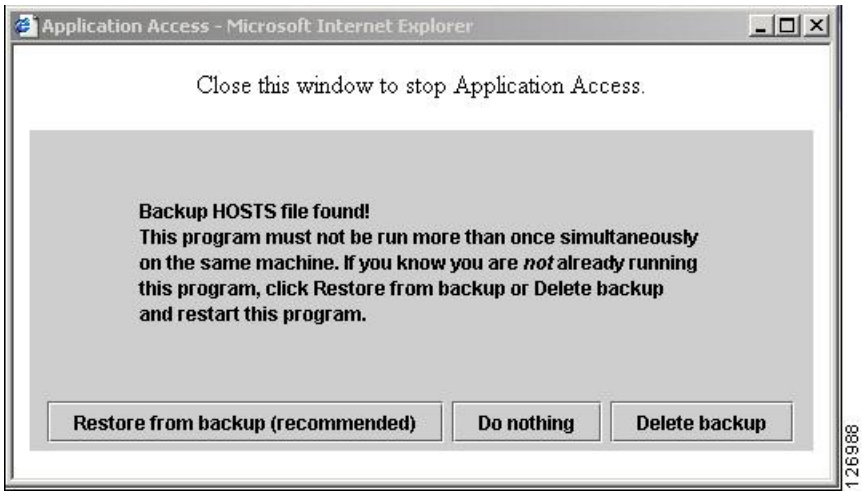
클라이언트리스 SSL VPN을 사용하여 호스트 파일 자동으로 재구성

원격 액세스 서버에 연결할 수 있는 경우, 다음 단계에 따라 호스트 파일을 다시 구성하고 애플리케이션에 액세스와 애플리케이션을 모두 다시 활성화합니다.

프로시저

단계 **1** 클라이언트리스 SSL VPN을 시작하고 로그인합니다.

Applications Access(애플리케이션 액세스**)** 링크를 클릭합니다.



단계 **2** 다음 옵션 중 하나를 선택합니다.

- **Restore from backup(**백업에서 복원**)** — 클라이언트리스 SSL VPN이 정상 종료를 강제로 실행합니다. hosts.webvpn 백업 파일을 `hosts` 파일에 복사하여 이 파일을 원래 상태로 복원한 다음 hosts.webvpn을 삭제합니다. 그런 다음 애플리케이션 액세스를 다시 시작해야 합니다.
- **Do Nothing(**작업 수행 안 함**)** — 애플리케이션 액세스를 시작하지 않습니다. 원격 액세스 홈 페이지가 다시 표시됩니다.
- **Delete backup(**백업 삭제**)** — 클라이언트리스 SSL VPN이 hosts.webvpn 파일을 삭제하여 호스트 파일이 해당 클라이언트리스 SSL VPN 사용자 지정 상태가 됩니다. 원래 `hosts` 파일 설정이 손실됩니다. 그런 다음 클라이언트리스 SSL VPN 사용자 지정 호스트 파일을 새 원본으로 사용하여 애플리케이션 액세스가 시작됩니다. 호스트 파일 설정이 손실되어도 문제가 없는 경우에만 이 옵션을 선택합니다. 애플리케이션 액세스가 잘못 종료된 이후에 직접 또는 사용하는 프로그램에서 호스트 파일을 수정한 경우, 다른 옵션 중 하나를 선택하거나 호스트 파일을 수동으로

호스트 파일 수동 재구성

현재 위치에서 원격 액세스 서버에 연결할 수 없거나 호스트 파일을 사용자 지정했으며 수정사항이 손실되는 것을 원치 않는 경우, 다음 단계에 따라 호스트 파일을 다시 구성하고 애플리케이션에 액세스와 애플리케이션을 모두 다시 활성화합니다.

프로시저

단계 **1** 호스트 파일을 찾아 수정합니다. 가장 일반적인 위치는 c:\windows\sysem32\drivers\etc\hosts입니다.

단계 **2** `# added by WebVpnPortForward` 문자열을 포함하는 행이 있는지 확인합니다. 이 문자열을 포함하는 행이 있는 경우 호스트 파일이 클라이언트리스 SSL VPN에 맞춤화되어 있는 것입니다. 호스트 파일이 클라이언트리스 SSL VPN 사용자 지정 파일인 경우, 다음 예와 유사합니다.

```
server1 # added by WebVpnPortForward
server1.example.com invalid.cisco.com # added by WebVpnPortForward
server2 # added by WebVpnPortForward
server2.example.com invalid.cisco.com # added by WebVpnPortForward
server3 # added by WebVpnPortForward
server3.example.com invalid.cisco.com # added by WebVpnPortForward

# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to hostnames. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding hostname.
# The IP address and the hostname should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     cisco.example.com          # source server
#       38.25.63.10     x.example.com              # x client host

123.0.0.1       localhost
```

단계 **3** `# added by WebVpnPortForward` 문자열을 포함하는 행을 삭제합니다.

단계 **4** 파일을 저장하고 닫습니다.

단계 **5** 클라이언트리스 SSL VPN을 시작하고 로그인합니다.

단계 **6** **Application Access(**애플리케이션 액세스**)** 링크를 클릭합니다.

WebVPN 조건부 디버깅

원격 액세스 VPN에서 다중 세션이 실행 중인 경우 로그의 크기 때문에 트러블슈팅이 어려울 수 있습니다. **debug webvpn condition** 명령을 사용하여 더 정확하게 디버그 프로세스 대상을 지정할 수 있도록 필터를 설정할 수 있습니다.

debug webvpn condition { **group** *name* | **p-ipaddress** *ip_address* [{ **subnet** *subnet_mask* | **prefix** *length*}] | **reset** | **user** *name*}

여기서 각 항목은 다음을 나타냅니다.

- 그룹 정책(터널 그룹 또는 연결 프로필 이외)의 **group** *name* 필터.

- 클라이언트의 공용 IP 주소에 대한 **p-ipaddress** *ip_address* [{ **subnet** *subnet_mask* | **prefix** *length*}] 필터. 서브넷 마스크(IPv4용) 또는 접두사(IPv6용)는 선택 사항입니다.
- **reset** 모든 필터 재설정. **no debug webvpn condition** 명령을 사용하여 특정 필터를 끌 수 있습니다.
- 사용자 이름을 기준으로 하는 **user** *name* 필터.

조건을 여러 개 구성하는 경우 조건들이 결합되어(AND로 처리) 모든 조건이 충족될 경우에만 디버그가 표시됩니다.

조건 필터를 설정한 후 기본 **debug webvpn** 명령을 사용하여 디버그를 켭니다. 조건을 설정하는 것만으로 디버그가 활성화되지는 않습니다. 현재 디버깅 상태를 보려면 **show debug** 및 **show webvpn debug-condition** 명령을 사용합니다.

다음은 사용자 jdoe에 대해 조건부 디버그를 활성화하는 예를 보여 줍니다.

```
asa3(config)# debug webvpn condition user jdoe

asa3(config)# show webvpn debug-condition
INFO: Webvpn conditional debug is turned ON
INFO: User name filters:
INFO: jdoe

asa3(config)# debug webvpn
INFO: debug webvpn  enabled at level 1.

asa3(config)# show debug
debug webvpn  enabled at level 1
INFO: Webvpn conditional debug is turned ON
INFO: User name filters:
INFO: jdoe
```

클라이언트리스 **SSL VPN** 사용자에게 관리자 알림 보내기

프로시저

단계 **1** 기본 ASDM 애플리케이션 창에서 **Tools(**툴**)** > **Administrator's Alert Message to Clientless SSL VPN Users(**클라이언트리스 **SSL VPN** 사용자에 대한 관리자 알림 메시지**)**를 선택합니다.

단계 **2** 전송하려는 새 알림 내용 또는 수정한 알림 내용을 입력한 다음 **Post Alert(**알림 게시**)**를 클릭합니다.

단계 **3** 현재 알림 내용을 제거하고 새 알림 내용을 입력하려면 **Cancel Alert(**알림 취소**)**를 클릭합니다.

클라이언트리스 SSL VPN 세션 쿠키 보호

외부 애플리케이션뿐만 아니라 Flash 애플리케이션 및 Java 애플릿과 같은 내장된 개체는 일반적으로 기존 세션 쿠키를 기반으로 서버와 함께 작동합니다. 이러한 애플리케이션은 초기화될 때 일부 JavaScript를 사용하여 브라우저에서 쿠키를 가져옵니다. 클라이언트리스 SSL VPN 세션 쿠키에 httponly 플래그를 추가하면 클라이언트 쪽 스크립트가 아닌 브라우저에만 세션 쿠키가 표시되므로, 세션 공유가 불가능해집니다.

시작하기 전에

- 활성 클라이언트리스 SSL VPN 세션이 없는 경우에만 VPN 세션 쿠키 설정을 변경합니다.
- **show vpn-sessiondb webvpn** 명령을 사용하여 클라이언트리스 SSL VPN 세션의 상태를 확인합니다.
- 모든 클라이언트리스 SSL VPN 세션에서 로그아웃하려면 **vpn-sessiondb logoff webvpn** 명령을 사용합니다.
- 다음 클라이언트리스 SSL VPN 기능은 **http-only-cookie** 명령이 활성 상태일 때 작동하지 않습니다.
  - Java 플러그인
  - Java 재작성기
  - 포트 전달
  - 파일 브라우저
  - 데스크톱 애플리케이션(예: MS Office 애플리케이션)을 필요로 하는 Sharepoint 기능
  - AnyConnect 웹 실행
  - Citrix Receiver, XenDesktop 및 Xenon
  - 기타 비 브라우저 기반 애플리케이션 및 브라우저 플러그인 기반 애플리케이션

서드파티에서 Javascript와 같은 클라이언트 측 스크립트를 통해 클라이언트리스 SSL VPN 세션 쿠키에 액세스하는 것을 방지하려면 다음 단계를 수행합니다.

프로시저

단계 **1** **Configuration**(구성) > **Remote Access VPN**(원격 액세스 **VPN**) > **Clientless SSL VPN Access**(클라이언트리스 **SSL VPN** 액세스) > **Advanced**(고급) > **HTTP Cookie**(**HTTP** 쿠키)를 선택합니다.

단계 **2** **Enable HTTP-only VPN cookies**(**HTTP** 전용 **VPN** 쿠키 사용) 확인란을 선택합니다.

참고 Cisco TAC에서 권장하는 경우에만 이 설정을 사용하십시오. 지침 섹션에 나와 있는 클라이언트리스 SSL VPN 기능은 경고 없이 작동하지 않으므로 이 명령을 사용하면 보안 위험에 노출됩니다.

단계 **3** 변경 사항을 저장하려면 **Apply(**적용**)**를 클릭합니다.