Cisco AnyConnect Secure Mobility Client 관리자 설명서, 릴리스 4.5

초판: 2017년 7월 5일

최종 변경: 2017년 7월 5일

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

이 설명서의 제품 관련 사양 및 정보는 예고 없이 변경될 수 있습니다. 이 설명서의 모든 설명, 정보 및 권장 사항이 정확하다고 판단되더라도 어떠한 형태의 명시적이거나 묵시적인 보증도 하지 않습니다. 모든 제품의 해당 애플리케이션에 대한 사용은 전적으로 사용자에게 책임이 있습니다.

동봉한 제품의 소프트웨어 라이센스 및 제한된 보증은 제품과 함께 제공된 정보 패킷에 설명되어 있으며 본 문서에 참조를 통해 포함됩니다. 소프트웨어 라이센스 또는 제한된 보증을 찾을 수 없는 경우 CISCO 담당자에게 문의하여 복사본을 요청하십시오.

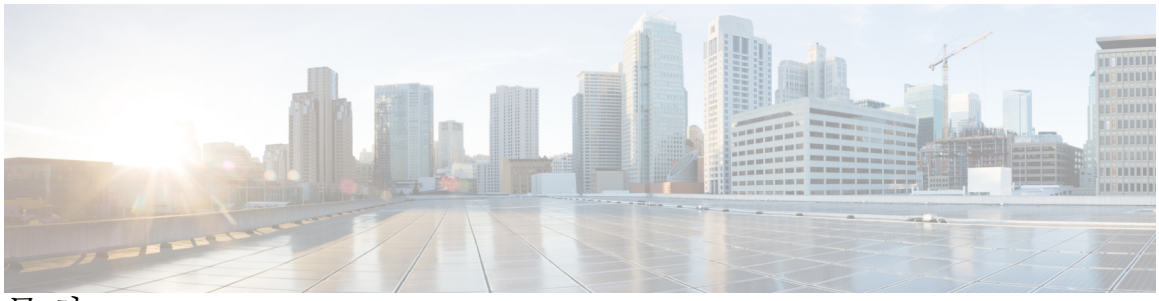
Cisco의 TCP 헤더 압축은 UNIX 운영 체제의 UCB 공개 도메인 버전의 일부로서 UCB(University of Berkeley)에서 개발된 프로그램을 적용하여 구현합니다. All rights reserved. Copyright © 1981, Regents of the University of California.

여기에 명시된 다른 모든 보증에도 불구하고 이러한 공급업체의 모든 문서 파일 및 소프트웨어는 모든 결점을 포함하여 "있는 그대로" 제공됩니다. CISCO 및 위에 언급된 모든 공급업체는 상품성, 특정 목적에의 적합성, 타인의 권리 비침해 또는 처리, 사용, 거래 행위로 발생하는 문제에 대한 묵시적 보증을 포함하여(단, 이에 한하지 않음) 묵시적이든 명시적이든 모든 종류의 보증을 부인합니다.

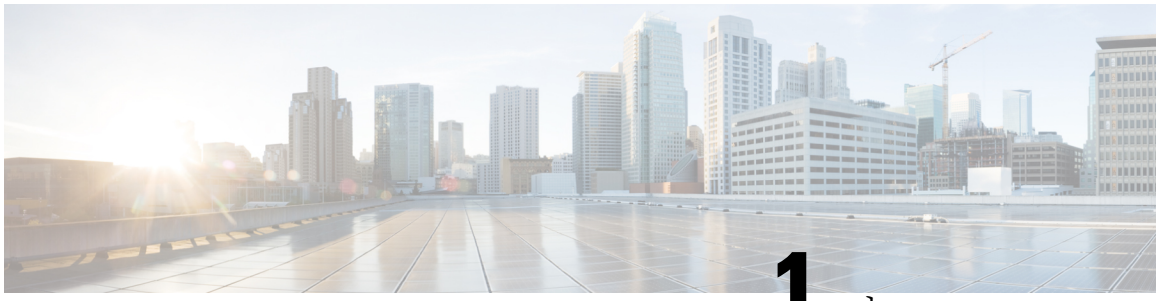
CISCO 또는 그 공급자는 이 설명서의 사용 또는 사용할 수 없음으로 인한 모든 파생적, 부수적, 직접, 간접, 특별, 징벌적 또는 기타 모든 손해(영업 이익 손실, 영업 중단, 영업 정보 손실, 또는 그 밖의 금전적 손실로 인한 손해를 포함하되 이에 제한되지 않음)에 대하여 어떠한 경우에도 책임을 지지 않으며, 이는 CISCO 또는 그 공급자가 그와 같은 손해의 가능성을 사전에 알고 있던 경우에도 마찬가지입니다.

이 문서에서 사용된 모든 IP(인터넷 프로토콜) 주소와 전화 번호는 실제 주소와 전화 번호가 아닙니다. 이 문서에 포함된 예제, 명령 표시 출력, 네트워크 토폴로지 다이어그램 및 다른 그림은 이해를 돕기 위한 자료일 뿐이며, 실제 IP 주소나 전화 번호가 사용되었다면 이는 의도하지 않은 우연의 일치입니다.

Cisco 및 Cisco 로고는 미국 및 기타 국가에서 Cisco Systems, Inc. 및/또는 계열사의 상표 또는 등록 상표입니다. Cisco 상표 목록을 보려면 다음 URL로 이동하십시오. https://www.cisco.com/go/trademarks 여기에 언급된 타사 상표는 해당 소유자의 자산입니다. "파트너"라는 용어는 사용에 있어 Cisco와 기타 회사 간의 파트너 관계를 의미하지는 않습니다. (1721R)



목 차



1 장

AnyConnect 구축

구축을 시작하기 전에

Umbrella 로밍 보안 모듈을 구축하는 경우 충돌을 방지하기 위해 기존에 설치한 Umbrella 로밍 클라이언트가 자동으로 탐지되어 제거됩니다. 기존에 설치한 Umbrella 로밍 클라이언트가 Umbrella 서비스 서브스크립션과 연결되어 있는 경우 OrgInfo.json 파일이 AnyConnect 설치 프로그램(웹 구축용으로 구성되어 있거나 Umbrella 모듈 디렉터리에 사전 구축됨)과 같은 위치에 저장되어 있는 경우가 아니면 서브스크립션은 Umbrella 로밍 보안 모듈로 자동 마이그레이션됩니다. Umbrella 로밍 보안 모듈을 구축하기 전에 Umbrella 로밍 클라이언트를 수동으로 제거할 수 있습니다.

또한 Umbrella 로밍 보안 모듈을 사용하는 경우 다음 전제조건도 완료해야 합니다.

- **Umbrella** 로밍 계정 받기**.** 로그인 페이지인 Umbrella 대시보드 http://dashboard.umbrella.com에서 AnyConnect Umbrella 로밍 보안 모듈 작동에 필요한 정보를 확인할 수 있습니다. 또한 이 사이트를 사용하여 로밍 클라이언트 활동에 대한 보고를 관리할 수 있습니다.
- 대시보드에서 **OrgInfo** 파일 다운로드**.** AnyConnect Umbrella 로밍 보안 모듈 구축을 준비하려면 Umbrella 대시보드에서 OrgInfo.json 파일을 다운로드합니다. Identities(ID) 메뉴 구조에서 **Roaming Computer(**로밍 컴퓨터**)**를 클릭한 다음 페이지 왼쪽 위 모서리에서 + 기호를 클릭합니다. 아래쪽의 AnyConnect Umbrella Roaming Security Module(AnyConnect Umbrella 로밍 보안 모듈)로 스크롤하여 **Module Profile(**모듈 프로파일**)**을 클릭합니다.

  orginfo.json 파일에는 로밍 보안 모듈이 보고를 할 위치와 시행할 정책을 파악할 수 있도록 하는 Umbrella 서비스 서브스크립션에 대한 특정 정보가 포함되어 있습니다.

AnyConnect 구축 개요

AnyConnect 구축 시에는 AnyConnect 클라이언트 및 관련 파일을 설치, 구성 및 업그레이드합니다.

Cisco AnyConnect Secure Mobility Client는 다음과 같은 방법으로 원격 사용자에게 구축될 수 있습니다.

- 사전 구축 - 엔터프라이즈 SMS(Software Management System, 소프트웨어 관리 시스템)를 사용하거나 최종 사용자가 신규 설치 및 업그레이드를 수행합니다.
- 웹 구축 - AnyConnect 패키지가 헤드엔드(ASA 또는 FTD 방화벽) 또는 ISE 서버에서 로드됩니다. 사용자가 방화벽이나 ISE에 연결할 때 AnyConnect는 클라이언트에 구축됩니다.
  - 신규 설치의 경우 사용자가 헤드엔드로 연결하여 AnyConnect 클라이언트를 다운로드합니다. 클라이언트는 수동 또는 자동(웹 실행)으로 설치됩니다.
  - AnyConnect가 이미 설치된 시스템에서 실행 중인 AnyConnect를 통해 또는 사용자를 ASA 클라이언트리스 포털로 디렉션하는 방법으로 업데이트가 수행됩니다.
- 클라우드 업데이트 - Umbrella 로밍 보안 모듈을 구축한 후에는 위의 방법 중 하나와 클라우드 업데이트를 사용하여 AnyConnect 모듈을 업데이트할 수 있습니다. 클라우드 업데이트를 사용하는 경우에는 Umbrella 클라우드 인프라에서 소프트웨어 업그레이드를 자동으로 가져오며, 관리자의 작업이 아닌 클라우드 인프라를 통해 업데이트를 추적합니다. 기본적으로 클라우드 업데이트를 통한 자동 업데이트는 비활성화되어 있습니다.

  참고 클라우드 업데이트와 관련하여 고려할 사항은 다음과 같습니다.
  - 현재 설치되어 있는 소프트웨어 모듈만 업데이트됩니다.
  - 맞춤화, 현지화 및 기타 모든 구축 유형은 지원되지 않습니다.
  - 업데이트는 데스크톱에 로그인되어 있을 때만 수행되며 VPN이 설정되어 있으면 수행되지 않습니다.
  - 업데이트가 비활성화되어 있으면 최신 소프트웨어 기능과 업데이트를 사용할 수 없습니다.
  - 클라우드 업데이트를 비활성화해도 웹 구축, 보류 업데이트 등의 다른 업데이트 메커니즘이나 설정에는 아무런 영향이 없습니다.
  - 클라우드 업데이트에서는 임시 릴리스, 패치된 버전 등 릴리스되지 않은 최신 AnyConnect 버전을 무시합니다.

AnyConnect를 구축할 때 VPN과 선택적 기능을 구성하는 클라이언트 프로파일 및 추가 기능을 활성화하는 선택적 모듈을 포함할 수 있습니다.

ASA, IOS, Microsoft Windows, Linux 및 macOS용 시스템, 관리 및 엔드포인트 요건은 AnyConnect 릴리스 노트를 참조하십시오.

AnyConnect 설치 방법 결정

AnyConnect는 ISE 2.0 이상 및 ASA 헤드엔드를 통해 웹에서 구축할 수도 있고 사전 구축할 수도 있습니다.

웹 구축

- ASA 또는 FTD 디바이스를 통한 웹 구축 - 사용자가 헤드엔드 디바이스의 AnyConnect 클라이언트리스 포털에 연결하고 AnyConnect를 다운로드하도록 선택합니다. ASA는 AnyConnect 다운로더를 다운로드합니다. AnyConnect 다운로더는 클라이언트를 다운로드 및 설치한 후 VPN 연결을 시작합니다.
- ISE를 통한 웹 구축 - 사용자가 ASA, 무선 컨트롤러, 스위치 등의 NAD(네트워크 액세스 디바이스)에 연결합니다. NAD는 사용자를 인증하고 사용자를 ISE 포털로 리디렉션합니다. AnyConnect 다운로더는 클라이언트에 설치되어 패키지 추출 및 설치를 관리하지만 VPN 연결은 시작하지 않습니다.

사전 구축

- Windows 변형과 같은 엔터프라이즈 SMS(소프트웨어 관리 시스템)을 사용합니다.
- 사용자용 설치 방법 지침과 함께 AnyConnect 파일 아카이브를 수동으로 배포합니다. 파일 아카이브 형식은 Windows의 경우 zip, Mac OS X의 경우 DMG, Linux의 경우 gzip입니다.

시스템 요건 및 라이선싱 종속성은 AnyConnect Secure Mobility Client 기능, 라이선스 및 OS 가이드를 참조하십시오.

참고 AnyConnect Posture(HostScan)를 사용하여 Mac 또는 Linux 플랫폼에서 루트 권한 활동을 수행하는 경우에는 AnyConnect Posture를 사전 구축하는 것이 좋습니다.

사용자가 **AnyConnect**를 설치하는 데 필요한 리소스 결정

다음과 같이 여러 파일 유형이 AnyConnect 구축을 구성합니다.

- AnyConnect 패키지에 포함된 AnyConnect 코어 클라이언트
- AnyConnect 패키지에 포함된 추가 기능을 지원하는 모듈
- AnyConnect 및 추가 기능을 구성하는 클라이언트 프로파일
- 구축을 사용자 정의하거나 현지화하려는 경우 언어 파일, 이미지, 스크립트 및 도움말 파일
- AnyConnect ISE Posture 및 규정 준수 모듈(OPSWAT)

AnyConnect용 엔드포인트 준비

AnyConnect에서 모바일 광대역 카드 사용

AnyConnect를 사용하기 전에 일부 3G 카드는 구성 단계를 거쳐야 합니다. 예를 들어 VZAccess Manager에는 3개의 설정이 있습니다.

- 모뎀 수동 연결
- 모뎀 자동 연결(로밍 시 제외)
- LAN 어댑터 자동 연결

LAN 어댑터 자동 연결을 선택하면 환경 설정이 NDIS 모드로 설정됩니다. VZAccess Manager가 종료된 경우에도 NDIS는 항상 사용자가 연결 상태를 유지할 수 있습니다. VZAccess Manager는 AnyConnect 설치 준비가 완료된 경우 디바이스 연결 환경 설정으로 자동 연결 LAN 어댑터를 표시합니다. AnyConnect 인터페이스가 탐지되면 3G 관리자는 인터페이스를 삭제하고 AnyConnect 연결을 허용합니다.

우선순위가 높은 연결로 이동하는 경우(유선 네트워크가 가장 우선순위가 높으며 WiFi, 모바일 광대역순), AnyConnect는 기존 연결을 끊기 전에 새 연결을 설정합니다.

Windows의 Internet Explorer 신뢰할 수 있는 사이트 목록에 ASA 추가

Active Directory 관리자는 그룹 정책을 사용하여 Internet Explorer에서 신뢰할 수 있는 사이트 목록에 ASA를 추가할 수 있습니다. 이 절차는 로컬 사용자가 Internet Explorer에서 신뢰할 수 있는 사이트를 추가하는 방법과 다릅니다.

프로시저

단계 **1** Windows 도메인 서버에서 도메인 관리자 그룹의 멤버로 로그인합니다.

단계 **2** Active Directory 사용자와 컴퓨터 MMC 스냅인을 여십시오.

단계 **3** 그룹 정책 개체를 생성할 Domain or Organizational Unit(도메인 또는 조직 단위)을 마우스 오른쪽 버튼으로 클릭하고 **Properties(**속성**)**를 클릭하십시오.

단계 **4** **Group Policy(**그룹 정책**)** 탭을 선택하고 **New(**새로 만들기**)**를 클릭하십시오.

단계 **5** 새 그룹 정책 개체의 이름을 입력하고 **Enter(**입력**)**를 누릅니다.

단계 **6** 이 새로운 정책을 일부 사용자 또는 그룹에 적용하는 것을 방지하려면 **Properties(**속성**)**를 클릭합니다. **Security** 탭을 선택합니다. 이 정책을 사용하지 못하게 하려는 사용자 또는 그룹을 추가한 다음 Allow(허용) 열에서 **Read(**읽기**)** 및 **Apply Group Policy(**그룹 정책 적용**)** 확인란의 선택을 취소합니다. **OK(**확인**)**를 클릭합니다.

단계 **7** **Edit(**수정**)**를 클릭하고 **User Configuration(**사용자 구성**)** > **Windows Settings(Windows** 설정**)** > **Internet Explorer Maintenance(Internet Explorer** 유지 관리**)** > **Security(**보안**)**를 선택합니다.

단계 **8** 오른쪽 창에서 **Security Zones and Content Ratings(**보안 영역 및 콘텐츠 등급**)**를 마우스 오른쪽 버튼으로 클릭한 다음 **Properties(**속성**)**를 클릭합니다.

단계 **9** **Import the current security zones and privacy settings(**현재 보안 영역 및 개인정보 설정 가져오기**)**를 선택합니다. 프롬프트가 표시되면 **Continue(**계속**)**를 클릭하십시오.

단계 **10** **Modify Settings(**설정 수정**)**를 클릭하고 **Trusted Sites(**신뢰할 수 있는 사이트**)**를 선택한 다음 **Sites(**사이트**)**를 클릭합니다.

단계 **11** 신뢰할 수 있는 사이트 목록에 추가할 보안 어플라이언스의 URL을 입력하고 **Add(**추가**)**를 클릭합니다. 형식에는 호스트 이름(https://vpn.mycompany.com) 또는 IP 주소(https://192.168.1.100)가 포함될 수 있습니다. 정확히 일치(https://vpn.mycompany.com)하거나 와일드카드(https://*.mycompany.com)가 사용될 수 있습니다.

단계 **12** 모든 대화 상자가 닫힐 때까지 계속해서 **Close(**닫기**)**를 클릭하고 **OK(**확인**)**를 클릭합니다.

단계 **13** 도메인 또는 포리스트 전체에 정책이 전파되도록 충분한 시간을 줍니다.

단계 **14** Internet Options(인터넷 옵션) 창에서 **OK(**확인**)**를 클릭합니다.

Internet Explorer에서 프록시 변경 차단

특정한 조건에서 AnyConnect는 Internet Explorer Tool(Internet Explorer 툴) > Internet Options(인터넷 옵션) > Connections(연결) 탭을 숨깁니다(잠금 설정). 이 탭이 표시될 경우, 탭을 사용하여 사용자가 프록시 정보를 설정할 수 있습니다. 이 탭을 숨기면 사용자가 터널을 의도적으로 또는 실수로 우회하는 것을 방지합니다. 연결을 끊으면 탭 잠금 설정이 해제됩니다. 탭 잠금은 해당 탭에 적용된 관리자 정의 정책에 따라 재정의됩니다. 잠금은 다음 경우에 적용됩니다.

- ASA 구성이 Connections(연결) 탭 잠금을 지정한 경우
- ASA 구성이 사설 측 프록시를 지정한 경우
- Windows 그룹 정책이 이전에 Connections(연결) 탭을 잠근 경우(잠금 없는 ASA 그룹 정책 설정 재정의)

프로시저

단계 **1** ASDM에서 **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 새 그룹 정책 **Edit(**편집**)** 또는 **Add(**추가**)**를 클릭합니다.

단계 **3** 탐색 창에서 **Advanced(**고급**)** > **Browser Proxy(**브라우저 프록시**)**로 이동합니다. Proxy Server Policy(프록시 서버 정책) 창이 표시됩니다.

단계 **4** **Proxy Lockdown(**프록시 잠금**)**을 클릭하여 추가 프록시 설정을 표시합니다.

단계 **5** **Inherit(**상속**)**를 선택 취소하고 다음 중에서 하나를 선택하십시오.

- **Yes(**예**)**를 선택하면 AnyConnect 세션 중에 프록시 잠금을 활성화하고 Internet Explorer Connections(연결) 탭을 숨깁니다.

- **No(**아니요**)**를 선택하면 AnyConnect 세션 중에 프록시 잠금을 비활성화하고 Internet Explorer Connections(연결) 탭을 표시합니다.

단계 **6** **OK(**확인**)**를 클릭하여 프록시 서버 정책 변경사항을 저장합니다.

단계 **7** **Apply(**적용**)**를 클릭하여 그룹 정책 변경사항을 저장합니다.

AnyConnect에서 Windows RDP 세션을 처리하는 방식 구성

AnyConnect는 Windows RDP 세션에서 VPN 연결을 허용하도록 구성할 수 있습니다. 기본적으로 RDP를 사용하여 컴퓨터에 연결된 사용자는 Cisco AnyConnect Secure Mobility Client를 통해 VPN 연결을 시작할 수 없습니다. 다음 표에서는 RDP 세션에서의 VPN 연결에 대한 로그온 및 로그아웃 옵션을 보여줍니다. 이 옵션은 VPN 클라이언트 프로파일에서 구성됩니다.

환경 설정 이름	값	SBL 모드에서 사용 가능 여부
Windows Logon Enforcement(Windows 로그온 적용**)**	• 단일 로컬 로그온(기본값) — 한 명의 로컬 사용자만 전체 VPN 연결 중에 로그온할 수 있습니다. 또한 로컬 사용자는 한 명 이상의 원격 사용자가 클라이언트 PC에 로그온되어 있는 동안 VPN 연결을 설정할 수 있습니다. 이 설정은 VPN 연결을 통해 엔터프라이즈 네트워크에서 로그온하는 원격 사용자에게 영향을 주지 않습니다. 참고 VPN 연결이 양단간 터널링에 대해 구성되어 있는 경우, VPN 연결을 위해 클라이언트 PC 라우팅 테이블이 수정된 결과가 원인이 되어 원격 로그온 연결이 끊어집니다. VPN 연결이 스플릿 터널링에 대해 구성된 경우, VPN 연결을 위한 라우팅 설정에 따라 원격 로그온의 연결이 끊어지거나 그렇지 않을 수 있습니다. • 단일 로그온 — 한 명의 사용자만 전체 VPN 연결 중에 로그온할 수 있습니다. 한 명 이상의 사용자가 로컬로 또는 원격으로 로그온하는 경우, VPN 연결을 설정할 때 연결이 허용되지 않습니다. 두 번째 사용자가 VPN 연결 중에 로컬로 또는 원격으로 로그온하는 경우, VPN 연결이 종료됩니다. 추가 로그온은 VPN 연결 중에 허용되지 않으므로 VPN 연결을 통해 원격으로 로그온할 수 없습니다. 참고 여러 동시 로그온은 지원되지 않습니다.	Yes(예)

환경 설정 이름	값	SBL 모드에서 사용 가능 여부
Windows VPN Establishment(Windows VPN 설정)	• 로컬 사용자 전용(기본값) — 원격으로 로그온한 사용자가 VPN 연결을 설정하는 것을 방지합니다. 이 기능은 AnyConnect 이전 버전의 기능과 동일합니다. • 원격 사용자 허용 — 원격 사용자가 VPN 연결을 설정하도록 허용합니다. 단, 구성된 VPN 연결 라우팅으로 인해 원격 사용자의 연결이 끊어진 경우, VPN 연결은 원격 사용자가 클라이언트 PC에 대한 액세스 권한을 다시 찾도록 종료됩니다. 원격 사용자는 VPN 연결을 종료하지 않으면서 원격 로그인 세션의 연결을 끊으려는 경우, VPN을 설정하고 90초 정도 기다려야 합니다.	No(아니요)

추가 VPN 세션 연결 옵션은 AnyConnect VPN 연결 옵션을 참조하십시오.

Windows에서의 DES 전용 SSL 암호화

기본적으로 Windows에서는 DES SSL 암호화를 지원하지 않습니다. ASA에서 DES 전용을 구성한 경우 AnyConnect 연결이 실패합니다. 이러한 운영 체제는 DES에 대해 구성하기 어려우므로 DES 전용 SSL 암호화를 위해 ASA를 구성하는 것이 좋습니다.

Linux에서 NVM 사용

Linux에서 NVM을 사용하기 전에 KDF(커널 드라이버 프레임워크)를 설정해야 합니다. AnyConnect Kernel Module을 사전 구축하거나 대상에서 드라이버를 구축하도록 선택할 수 있습니다. 대상에서 구축하도록 선택하는 경우에는 아무런 작업을 수행하지 않아도 됩니다. 구축 또는 리부팅 중에 구축 작업이 자동으로 처리됩니다.

AnyConnect 커널 모듈 구축 전제조건

대상 디바이스를 준비합니다.

- GNU Make Utility가 설치되었는지 확인합니다.
- 커널 헤더 패키지를 설치합니다.
  - RHEL의 경우 **kernel-devel-$(uname -r)** 패키지(예: kernel-devel-2.6.32-642.13.1.el6.x86_64)를 설치합니다.
  - Ubuntu의 경우 **linux-headers-$(uname -r)** 패키지(예: linux-headers-4.2.0-27-generic)를 설치합니다.

- GCC 컴파일러가 설치되었는지 확인합니다. 설치된 GCC 컴파일러의 *major.minor* 버전은 커널이 구축된 GCC 버전과 일치해야 합니다. /proc/version 파일에서 이를 확인할 수 있습니다.

사전 구축된 AnyConnect Linux 커널 모듈을 사용하여 NVM 패키징

시작하기 전에

AnyConnect 커널 모듈 구축 전제조건, 8 페이지의 전제조건을 완료합니다.

참고 보안 부팅이 활성화된 디바이스에서는 NVM이 지원되지 않습니다.

AnyConnect NVM을 사전 구축된 AnyConnect Linux 커널 모듈과 함께 패키징할 수 있습니다. 그러면 특히 여러 대상 디바이스의 OS 커널 버전이 같을 때 모든 대상 디바이스에서 해당 모듈을 구축하지 않아도 됩니다. 사전 구축 옵션을 사용하지 않으려는 경우 대상에서 구축을 사용할 수 있습니다. 해당 작업은 관리자의 입력 없이도 구축 또는 리부팅 중에 자동으로 수행됩니다.

참고 사전 구축된 AnyConnect Linux 커널 모듈의 경우에는 웹 구축이 지원되지 않습니다.

프로시저

단계 **1** AnyConnect 사전 구축 패키지(anyconnect-linux64-<*version*>-predeploy-k9.tar.gz)의 압축을 풉니다.

단계 **2** nvm 디렉터리로 이동합니다.

단계 **3** **$sudo ./build_and_package_ac_ko.sh** 스크립트를 호출합니다.

스크립트를 실행하고 나면 AnyConnect Linux 커널 모듈 빌드가 포함된 anyconnect-linux64-<*version*>-**ac_kdf_ko**-k9.tar.gz가 생성됩니다. 이 파일은 사전 구축에만 사용할 수 있습니다.

다음에 수행할 작업

대상 디바이스의 OS 커널을 업그레이드할 때는 업데이트된 Linux 커널 모듈을 포함하는 AnyConnect NVM을 재구축해야 합니다.

AnyConnect 사전 구축

AnyConnect는 최종 사용자가 설치할 파일을 배포하거나 사용자가 연결할 수 있도록 AnyConnect 파일 아카이브를 사용 가능하게 하여 수동으로 SMS를 통해 사전 구축할 수 있습니다.

AnyConnect를 설치하기 위해 파일 아카이브를 생성한 경우 아카이브의 디렉토리 구조는 클라이언트에 설치된 파일의 디렉토리 구조와 일치해야 합니다. 여기에 대한 설명은 다음 항목에 나와 있습니다. AnyConnect 프로파일 사전 구축 위치, 12 페이지

시작하기 전에

- VPN 프로파일을 수동으로 구축하는 경우 프로파일을 헤드엔드에 업로드해야 합니다. 클라이언트 시스템이 연결되면 AnyConnect는 클라이언트의 프로파일이 헤드엔드의 프로파일과 일치하는지 확인합니다. 프로파일 업데이트를 비활성화하고 헤드엔드의 프로파일이 클라이언트와 다른 경우, 수동으로 구축한 프로파일은 작동하지 않습니다.
- AnyConnect ISE Posture 프로파일을 수동으로 구축하는 경우 해당 파일 또한 ISE에 업로드해야 합니다.

프로시저

단계 **1** AnyConnect 사전 구축 패키지를 다운로드하십시오.

사전 구축용 AnyConnect 파일은 cisco.com에서 제공됩니다.

OS	**AnyConnect** 사전 구축 패키지 이름
Windows	anyconnect-win-*version*-predeploy-k9.zip
macOS	anyconnect-macos-*version*-predeploy-k9.dmg
Linux(64비트)	anyconnect-linux64-*version*-predeploy-k9.tar.gz

Linux 운영 체제에서는 Umbrella 로밍 보안 모듈을 사용할 수 없습니다.

단계 **2** 클라이언트 프로파일을 생성합니다. 일부 모듈과 기능에서는 클라이언트 프로파일이 필요합니다.

클라이언트 프로파일이 필요한 모듈은 다음과 같습니다.

- AnyConnect VPN
- AnyConnect Network Access Manager
- AnyConnect 웹 보안
- AnyConnect ISE Posture
- AnyConnect AMP Enabler
- Network Visibility Module
- Umbrella 로밍 보안 모듈

다음 모듈에서는 AnyConnect 클라이언트 프로파일이 필요하지 않습니다.

- AnyConnect VPN 로그온 전 시작

- AnyConnect 진단 및 보고 툴
- AnyConnect Posture
- AnyConnect 고객 경험 피드백

ASDM에서 클라이언트 프로파일을 생성하고 해당 파일을 PC에 복사할 수 있습니다. 또는 Windows PC에서 독립형 프로파일 편집기를 사용할 수 있습니다. Windows 독립형 편집기에 대한 자세한 내용은 프로파일 편집기 정보를 참조하십시오.

단계 **3** 필요에 따라 AnyConnect 클라이언트 및 설치 프로그램 사용자 정의 및 현지화, 47 페이지를 수행합니다.

단계 **4** 배포용 파일을 비교하십시오. 파일의 디렉토리 구조는 AnyConnect 프로파일 사전 구축 위치에 설명되어 있습니다.

단계 **5** AnyConnect 설치를 위한 모든 파일을 생성한 후 아카이브 파일에 배포하거나 파일을 클라이언트에 복사하십시오. 동일한 AnyConnect 파일을 연결할 헤드엔드, ASA 및 ISE에도 위치하도록 하십시오.

사전 구축 및 웹 구축용 **AnyConnect** 모듈 실행 파일

다음 표에는 Windows 컴퓨터에 Umbrella 로밍 보안 모듈, Network Access Manager, AMP Enabler, ISE Posture, Web Security 및 Network Visibility Module 클라이언트를 사전 구축 또는 웹 구축할 때 엔드포인트 컴퓨터에 있는 파일 이름이 나와 있습니다.

표 ***1:*** 웹 또는 사전 구축용 모듈의 파일 이름

모듈	웹 구축 설치 프로그램(다운로드됨)	사전 구축 설치 프로그램
Network Access Manager	anyconnect-win-*version*-nam-webdeploy-k9.msi	anyconnect-win-*version*-nam-predeploy-k9.msi
웹 보안	anyconnect-win-*version*-websecurity-webdeploy-k9.exe	anyconnect-win-*version*-websecurity-predeploy-k9.msi
ISE Posture	anyconnect-win-*version*-iseposture-webdeploy-k9.msi	anyconnect-win-*version*-iseposture-predeploy-k9.msi
AMP Enabler	anyconnect-win-*version*-amp-webdeploy-k9.msi	anyconnect-win-*version*-amp-predeploy-k9.exe
Network Visibility Module	anyconnect-win-*version*-nvm-webdeploy-k9.exe	anyconnect-win-*version*-nvm-predeploy-k9.msi
Umbrella 로밍 보안 모듈	anyconnect-win-*version*-umbrella-webdeploy-k9.exe	anyconnect-win-*version*-umbrella-predeploy-k9.msi

AnyConnect 4.3 이상은 Visual Studio 2015 구축 환경으로 이동되었으며, Network Access Manager 모듈 기능용으로 VS 재배포 가능 파일이 필요합니다. 이러한 파일은 설치 패키지의 일부로 설치됩니다. .msi 파일을 사용하여 Network Access Manager 모듈을 4.3 이상으로 업그레이드할 수 있지만, 먼저 AnyConnect Secure Mobility Client를 업그레이드한 다음 릴리스 4.3 이상을 실행해야 합니다.

참고 Windows 2008R2 서버를 사용하는 경우, AnyConnect Network Access Manager를 설치하려고 시도할 때 설치 오류가 발생할 수 있습니다. WLAN 서비스는 서버 운영 체제에서 기본적으로 설치되어 있지 않으므로 이 서비스를 설치하고 PC를 재부팅해야 합니다.

AnyConnect 프로파일 사전 구축 위치

클라이언트 시스템에 파일을 복사하는 경우, 다음 표에서는 파일을 배치해야 할 위치를 보여줍니다.

표 *2: AnyConnect* 코어 파일

파일	설명
anyfilename.xml	AnyConnect 프로파일 이 파일은 특정 사용자 유형에 대해 구성된 기능 및 특성 값을 지정합니다.
AnyConnectProfile.xsd	XML 스키마 형식을 정의합니다. AnyConnect는 프로파일을 확인하기 위해 이 파일을 사용합니다.

표 3: 모든 운영 체제의 프로파일 위치

운영 체제	모듈	위치
Windows	VPN을 통한 코어 클라이언트	%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile
	Network Access Manager	%ProgramData%\Cisco\ Cisco AnyConnect Secure Mobility Client\Network Access Manager\newConfigFiles
	웹 보안	%ProgramData%\Cisco\ Cisco AnyConnect Secure Mobility Client\Web Security
	고객 경험 피드백	%ProgramData%\Cisco\ Cisco AnyConnect Secure Mobility Client\CustomerExperienceFeedback
	OPSWAT	%PROGRAMFILES%\Cisco\Cisco AnyConnect Secure Mobility Client\opswat
	ISE Posture	%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\ISE Posture
	AMP Enabler	%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\AMP Enabler
	Network Visibility Module	%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\NVM
	Umbrella 로밍 보안 모듈	

운영 체제	모듈	위치
		%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Umbrella 참고 Umbrella 로밍 보안 모듈을 활성화하려면 Umbrella 대시보드에서 OrgInfo.json 파일을 다운로드하여 이름을 바꾸지 않고 이 대상 디렉터리에 저장해야 합니다. 또는 OrgInfo.json 파일을 Umbrella 로밍 보안 모듈 설치 프로그램과 함께 저장할 수도 있습니다(설치 전에 \Profiles\umbrella에 파일 저장).

운영 체제	모듈	위치
macOS	모든 다른 모듈	/opt/cisco/anyconnect/profile
	고객 경험 피드백	/opt/cisco/anyconnect/CustomerExperienceFeedback
	이진 파일	/opt/cisco/anyconnect/bin
	OPSWAT	/opt/cisco/anyconnect/lib/opswat
	라이브러리	/opt/cisco/anyconnect/lib
	UI 리소스	/Applications/Cisco/Cisco AnyConnect Secure Mobility Client.app/Contents/Resources/
	ISE Posture	/opt/cisco/anyconnect/iseposture/
	AMP Enabler	/opt/cisco/anyconnect/ampenabler/
	Network Visibility Module	/opt/cisco/anyconnect/NVM/
	Umbrella 로밍 보안 모듈	/opt/cisco/anyconnect/umbrella 참고 Umbrella 로밍 보안 모듈을 활성화하려면 Umbrella 대시보드에서 OrgInfo.json 파일을 다운로드하여 이름을 바꾸지 않고 이 대상 디렉터리에 저장해야 합니다. 또는 OrgInfo.json 파일을 Umbrella 로밍 보안 모듈 설치 프로그램과 함께 저장할 수도 있습니다(설치 전에 \Profiles\umbrella에 파일 저장).
Linux	NVM	/opt/cisco/anyconnect/NVM
	모든 다른 모듈	/opt/cisco/anyconnect/profile

독립형 애플리케이션으로 **AnyConnect** 모듈 사전 구축

Network Access Manager, Web Security 및 Umbrella 로밍 보안 모듈은 독립형 애플리케이션으로 실행할 수 있습니다. AnyConnect 코어 클라이언트가 설치되어 있지만 VPN 및 AnyConnect UI가 사용되지 않습니다.

Windows에서 SMS를 통해 독립형 모듈 구축

프로시저

단계 **1** SMS(Software Management System, 소프트웨어 관리 시스템)가 MSI 속성인 PRE_DEPLOY_DISABLE_VPN=1을 설정하도록 구성하여 VPN 기능을 비활성화합니다. 예를 들면 다음과 같습니다.

```
msiexec /package anyconnect-win-version-predeploy-k9.msi /norestart /passive
PRE_DEPLOY_DISABLE_VPN=1 /lvx* <log_file_name>
```

MSI는 MSI에 내장된 VPNDisable_ServiceProfile.xml 파일을 VPN 기능을 위해 프로파일용으로 지정된 디렉토리에 복사합니다.

단계 **2** 모듈을 설치합니다. 예를 들어 다음 CLI 명령은 웹 보안을 설치합니다.

msiexec /package anyconnect-win-*version*-websecurity-predeploy-k9.msi /norestart /passive /lvx* c:\test.log

단계 **3** DART를 설치합니다(선택 사항).

misexec /package annyconnect-win-*version*-dart-predeploy-k9.msi /norestart /passive /lvx* c:\test.log

단계 **4** 적절한 Windows 폴더에 난독화된 클라이언트 프로파일의 복사본을 저장합니다.

단계 **5** Cisco AnyConnect 서비스를 재시작합니다.

독립형 애플리케이션으로 AnyConnect 모듈 구축

사용자 컴퓨터에서 AnyConnect Network Access Manager, Web Security 및 Umbrella 로밍 보안 모듈을 독립형 애플리케이션으로 구축할 수 있습니다. DART는 이러한 애플리케이션과 함께 지원됩니다.

요구 사항

VPNDisable_ServiceProfile.xml 파일이 VPN 클라이언트 프로파일 디렉토리에서 유일한 AnyConnect 프로파일이어야 합니다.

독립형 모듈의 사용자 설치

개별 설치 프로그램을 분류하여 직접 배포할 수도 있습니다.

zip 이미지를 사용할 수 있도록 결정하고 설치 여부를 물을 경우, 사용자에게 독립형 모듈로만 설치하도록 지시합니다.

참고 Network Access Manager의 이전 설치가 컴퓨터에 존재하지 않는 경우, 사용자가 Network Access Manager 설치를 완료하려면 컴퓨터를 재부팅해야 합니다. 시스템 파일 일부를 업그레이드해야 하는 설치의 경우에도 재부팅해야 합니다.

프로시저

단계 **1** 사용자에게 AnyConnect Network Access Manager, AnyConnect Web Security 모듈 또는 Umbrella 로밍 보안 모듈을 확인하도록 지시합니다.

단계 **2** 사용자에게 **Cisco AnyConnect VPN Module(Cisco AnyConnect VPN** 모듈**)**을 선택 취소하도록 지시합니다.

이렇게 하면 코어 클라이언트의 VPN 기능이 비활성화되며 설치 유틸리티에서 VPN 기능 없이 독립형 애플리케이션으로 Network Access Manager, Web Security 또는 Umbrella 로밍 보안 모듈을 설치합니다.

단계 **3** **Lock Down Component Services(**구성 요소 서비스 잠금**)** 확인란을 선택합니다(선택 사항). 구성 요소 서비스 잠금은 사용자가 Windows 서비스를 끄거나 중지하는 것을 방지합니다.

단계 **4** 사용자에게 VPN 서비스가 없는 AnyConnect GUI를 사용할 수 있는 선택 모듈에 대해 설치 프로그램을 실행하도록 지시합니다. 사용자가 Install Selected(선택사항 설치) 버튼을 클릭한 경우, 그 결과는 다음과 같습니다.

a) 팝업 대화 상자에서 독립형 Network Access Manager, 독립형 Web Security 모듈 또는 Umbrella 로밍 보안 모듈에 대한 선택을 확인합니다.

b) 사용자가 확인을 클릭하면 설치 유틸리티가 PRE_DEPLOY_DISABLE_VPN=1 설정이 있는 AnyConnect 코어 설치 프로그램을 호출합니다.

c) 설치 유틸리티는 기존 VPN 프로파일을 모두 제거한 다음 VPNDisable_ServiceProfile.xml을 설치합니다.

d) 설치 유틸리티는 Network Access Manager, Web Security 또는 Umbrella 로밍 보안 설치 프로그램을 호출합니다.

e) Network Access Manager, Web Security 모듈 또는 Umbrella 로밍 보안 모듈이 컴퓨터에서 VPN 서비스 없이 활성화됩니다.

Windows에 사전 구축

zip 파일을 사용하여 AnyConnect 배포

zip 패키지 파일에는 개별 구성 요소 설치 프로그램과 코어 및 선택적 AnyConnect 모듈의 MSI를 실행하는 선택기 메뉴 프로그램인 설치 유틸리티가 포함되어 있습니다. 사용자에게 zip 패키지 파일을 제공하여 설치 프로그램(setup.exe)을 실행하도록 합니다. 프로그램에서 사용자가 설치할 AnyConnect 모듈을 선택하는 설치 유틸리티 메뉴가 표시됩니다. 사용자가 로드할 모듈을 선택하지 못하도록 하고자 할 수도 있습니다. 따라서 zip 파일을 사용하여 배포하려는 경우, zip을 편집하여 사용하지 않으려는 모듈을 제거하고 HTA 파일을 편집하십시오.

ISO를 배포하는 한 가지 방법은 SlySoft 또는 PowerIS 등의 가상 CS 마운트 소프트웨어를 사용하는 것입니다.

사전 구축 **zip** 수정

- 파일을 번들로 묶었을 때 생성한 프로파일을 사용하여 zip 파일을 업데이트하고 배포하지 않으려는 모듈의 설치 프로그램을 제거하십시오.
- HTA 파일을 편집하여 설치 메뉴를 개인 설정하고 배포하지 않으려는 모듈 설치 프로그램에 대한 링크를 제거하십시오.

AnyConnect zip 파일의 내용

파일	목적
GUI.ico	AnyConnect 아이콘 이미지
Setup.exe	설치 유틸리티 시작
anyconnect-win-*version*-dart-predeploy-k9.msi	DART 모듈용 MSI 설치 프로그램 파일
anyconnect-win-*version*-gina-predeploy-k9.msi	SBL 모듈용 MSI 설치 프로그램 파일
anyconnect-win-*version*-iseposture-predeploy-k9.msi	ISE Posture 모듈용 MSI 설치 프로그램
anyconnect-win-*version*-amp-predeploy-k9.exe	AMP Enabler용 MSI 설치 프로그램 파일
anyconnect-win-*version*-nvm-predeploy-k9.msi	Network Visibility Module용 MSI 설치 프로그램 파일
anyconnect-win-*version*-umbrella-predeploy-k9.msi	Umbrella 로밍 보안 모듈용 MSI 설치 프로그램 파일
anyconnect-win-*version*-nam-predeploy-k9.msi	Network Access Manager 모듈용 MSI 설치 프로그램 파일
anyconnect-win-*version*-posture-predeploy-k9.msi	포스처 모듈용 MSI 설치 프로그램 파일
anyconnect-win-*version*-websecurity-predeploy-k9.msi	Web Security 모듈용 MSI 설치 프로그램 파일
anyconnect-win-*version*-core-vpn-predeploy-k9.msi	AnyConnect 코어 클라이언트용 MSI 설치 프로그램 파일
autorun.inf	setup.exe의 정보 파일
eula.html	수락 가능한 사용 정책
setup.hta	이 사이트에 대해 사용자 정의할 수 있는 HTA(Utility HTML Application, 유틸리티 HTML 애플리케이션) 설치

SMS를 사용하여 AnyConnect 배포

zip 이미지를 통해 구축하려는 모듈에 대한 설치 프로그램(*.msi)의 압축을 푼 다음 수동으로 배포할 수 있습니다.

요구 사항

- Windows에서 AnyConnect를 설치할 때 AlwaysInstallElevated 또는 Windows UAC(User Account Control, 사용자 계정 컨트롤) 그룹 정책 설정을 비활성화해야 합니다. 그렇지 않으면 AnyConnect 설치 프로그램이 설치에 필요한 일부 디렉토리에 액세스하지 못할 수 있습니다.
- MSIE(Microsoft Internet Explorer) 사용자는 신뢰할 수 있는 사이트 목록에 헤드엔드를 추가하거나 Java를 설치해야 합니다. 신뢰할 수 있는 사이트 목록을 추가하면 ActiveX 컨트롤이 사용자의 상호 작용을 최소화하여 설치하도록 할 수 있습니다.

프로파일 구축 프로세스

- MSI 설치 프로그램을 사용하는 경우 설치 시 MSI가 Profiles 폴더에 있는 프로파일을 선택하여 적절한 폴더에 저장합니다. 적절한 폴더 경로는 CCO에서 사용 가능한 사전 구축 MSI 파일에서 제공됩니다.
- 설치 후 프로파일을 수동으로 사전 구축하는 경우, 프로파일을 수동으로 복사하거나 Altiris와 같은 SMS를 사용하여 프로파일을 적절한 폴더에 구축하십시오.
- 클라이언트에 사전 구축한 헤드엔드에서 동일한 클라이언트 프로파일을 위치시켰는지 확인하십시오. 또한 ASA에서 사용 중인 그룹 정책에 이 프로파일을 연결해야 합니다. 클라이언트 프로파일이 헤드엔드의 프로파일과 일치하지 않거나 그룹 정책에 연결되어 있지 않으면 액세스 거부를 비롯한 동작 불일치가 발생할 수 있습니다.

Windows 사전 구축 MSI 예시

설치된 모듈	명령 및 로그 파일
VPN 기능이 없는 AnyConnect 코어 클라이언트 독립형 Network Access Manager 또는 Web Security 모듈 설치 시 사용	msiexec /package anyconnect-win-*version*-core-vpn-predeploy-k9.msi /norestart /passive PRE_DEPLOY_DISABLE_VPN=1 /lvx* anyconnect-win-*version*-core-vpn-predeploy-k9-install-datetimestamp.log
VPN 기능이 있는 AnyConnect 코어 클라이언트	msiexec /package anyconnect-win-*version*-core-vpn-predeploy-k9.msi /norestart /passive /lvx* anyconnect-win-*version*-core-vpn-predeploy-k9-install-datetimestamp.log
고객 경험 피드백	msiexec /package anyconnect-win-*version*-core-vpn-predeploy-k9.msi /norestart /passive DISABLE_CUSTOMER_EXPERIENCE_FEEDBACK=1 /lvx* anyconnect-win-*version*-core-vpn-predeploy-k9-install-datetimestamp.log
DART(Diagnostic and Reporting Tool, 진단 및 보고 툴)	msiexec /package anyconnect-win-*version*-dart-predeploy-k9.msi /norestart /passive /lvx* anyconnect-win-*version*-dart-predeploy-k9-install-datetimestamp.log

설치된 모듈	명령 및 로그 파일
SBL	msiexec /package anyconnect-win-*version*-gina-predeploy-k9.msi /norestart /passive /lvx* anyconnect-win-*version*-gina-predeploy-k9-install-datetimestamp.log
Network Access Manager	msiexec /package anyconnect-win-*version*-nam-predeploy-k9.msi /norestart /passive /lvx* anyconnect-win-*version*-nam-predeploy-k9-install-datetimestamp.log
웹 보안	msiexec /package anyconnect-win-*version*-websecurity-predeploy-k9.msi /norestart/passive /lvx* anyconnect-win-*version*-websecurity-predeploy-k9-install-datetimestamp.log
VPN Posture(HostScan)	msiexec /package anyconnect-win-*version*-posture-predeploy-k9.msi /norestart/passive /lvx* anyconnect-win-*version*-posture-predeploy-k9-install-datetimestamp.log
ISE Posture	msiexec /package anyconnect-win-*version*-iseposture-predeploy-k9.msi /norestart/passive /lvx* anyconnect-win-*version*-iseposture-predeploy-k9-install-datetimestamp.log
AMP Enabler	msiexec /package anyconnect-win-*version*-amp-predeploy-k9.msi / norestart/passive /lvx* anyconnect-win-*version*-amp-predeploy-k9-install-datetimestamp.log
Network Visibility Module	msiexec /package anyconnect-win-*version*-nvm-predeploy-k9.msi / norestart/passive /lvx* anyconnect-win-*version*-nvm-predeploy-k9-install-datetimestamp.log
Umbrella 로밍 보안	msiexec /package anyconnect-win-*version*-umbrella-predeploy-k9.msi / norestart/passive /lvx* anyconnect-*version*-umbrella-predeploy-k9-install-datetimestamp.log

AnyConnect 샘플 Windows 변형

Cisco에서는 변형 사용 방식을 설명하는 문서와 함께 예시 Windows 변형을 제공합니다. 밑줄 문자(_)로 시작하는 변형은 특정 모듈 설치 프로그램에 특정 변형만 적용할 수 있는 일반 Windows 변형입니다. 알파벳 문자로 시작되는 변형은 VPN 변형입니다. 각 변형에는 변형을 사용하는 방식을 설명하는 문서가 포함되어 있습니다. 변형 다운로드는 샘플 변형-*x.x.x*.zip입니다.

Windows 사전 구축 보안 옵션

최종 사용자에게는 Cisco AnyConnect Secure Mobility Client를 호스트하는 디바이스에 대해 제한된 권한을 부여하는 것이 좋습니다. 최종 사용자가 추가 권한을 보장할 경우, 설치 프로그램은 사용자와 로컬 관리자가 엔드포인트에서 잠금으로 설정한 Windows 서비스를 끄거나 중지하지 못하도록 잠금 기능을 제공할 수 있습니다. 웹 보안 모듈에서 서비스 비밀번호를 사용하여 클라이언트를 우회 모드로 전환할 수 있습니다. 또한 사용자가 AnyConnect를 제거하지 못하도록 할 수 있습니다.

Windows 잠금 속성

각 MSI 설치 프로그램은 영(0)이 아닌 값으로 설정된 경우, 엔드포인트 디바이스에서 사용자 또는 로컬 관리자가 설치 프로그램과 연관된 Windows 서비스를 제어하지 못하도록 하는 공통 속성(LOCKDOWN)을 지원합니다. 설치 시 제공되는 샘플 변형(anyconnect-vpn-transforms-X.X.xxxxx.zip)을 사용하여 이러한 속성을 설정하고 잠금을 설정하려는 각 MSI 설치 프로그램에 그 변형을 적용할 것을 권장합니다. 잠금 옵션은 또한 ISO 설치 유틸리티 내에 있는 확인란입니다.

프로그램 추가/제거 목록에서 AnyConnect 숨기기

Windows 프로그램 추가/제거 목록을 보고 있는 사용자로부터 설치된 AnyConnect 모듈을 숨길 수 있습니다. ARPSYSTEMCOMPONENT=1을 사용하는 모든 설치 프로그램을 실행하는 경우, 해당 모듈이 Windows 프로그램 추가/제거 목록에 나타나지 않습니다.

이 속성을 설정하도록 제공한 샘플 변형(anyconnect-vpn-transforms-X.X.xxxxx.zip)을 사용하는 것이 좋습니다. 숨기려는 각 모듈에 대한 MSI 설치 프로그램 각각에 변형을 적용합니다.

Windows에서 AnyConnect 모듈 설치 및 제거 순서

모듈 설치 프로그램은 설치를 시작하기 전에 코어 클라이언트와 동일한 버전인지 확인합니다. 버전이 일치하지 않으면 모듈은 설치를 수행하지 않으며 설치 프로그램은 사용자에게 불일치 사실을 알립니다. 설치 유틸리티를 사용하는 경우 모듈이 패키지에 함께 내장 및 패키지되어 있으며 버전이 항상 일치합니다.

프로시저

단계 **1** 다음과 같은 순서로 AnyConnect 모듈을 설치합니다.

a) GUI 및 VPN 기능(SSL 및 IPsec 모두)을 설치하는 AnyConnect 코어 클라이언트 모듈을 설치합니다.
b) AnyConnect 코어 클라이언트 설치에 대해 유용한 진단 정보를 제공하는 AnyConnect DART(Diagnostics and Reporting Tool, 진단 및 보고 툴) 모듈을 설치합니다.
c) Umbrella 로밍 보안 모듈, Network Visibility Module, AMP Enabler, SBL, Network Access Manager, Web Security, Posture 모듈 또는 ISE 컴플라이언스 모듈을 원하는 순서로 설치합니다.

단계 **2** 다음과 같은 순서로 AnyConnect 모듈을 제거합니다.

a) Umbrella 로밍 보안 모듈, Network Visibility Module, AMP Enabler, Network Access Manager, Web Security, Posture, ISE 컴플라이언스 모듈 또는 SBL을 원하는 순서로 설치합니다.
b) AnyConnect 코어 클라이언트를 제거합니다.

c) DART를 마지막으로 제거합니다.

DART 정보는 제거 프로세스가 실패할 경우 유용하게 사용됩니다.

참고 설계상, AnyConnect 제거 후에도 일부 XML 파일은 남아 있습니다.

macOS에 사전 구축

macOS에서 AnyConnect 설치 및 제거

macOS용 AnyConnect는 모든 AnyConnect 모듈을 포함하는 DMG 파일에서 배포됩니다. 사용자가 DMG 파일을 연 다음 AnyConnect.pkg 파일을 실행하면 설치하는 동안 사용자를 안내하는 설치 대화 상자가 시작됩니다. 설치 유형 화면에서 사용자는 설치할 패키지(모듈) 종류를 선택할 수 있습니다.

배포에서 AnyConnect 모듈을 제거하려면 Apple pkgutil 툴을 사용하여 수정한 후 패키지에 서명하십시오. 또한 ACTransforms.xml을 사용하여 설치 프로그램을 수정할 수 있습니다. 언어 및 모양을 맞춤화할 수 있고 일부 다른 설치 작업을 변경할 수 있습니다. 이 내용은 맞춤화 장(ACTransforms.xml을 사용하여 macOS에서 설치 프로그램 동작 맞춤화, 55 페이지)에 설명되어 있습니다.

macOS에서 독립형 애플리케이션으로 AnyConnect 모듈 설치

VPN을 사용하지 않고 Web Security, Network Visibility Module 또는 Umbrella 로밍 보안 모듈만 설치할 수 있습니다. VPN 및 AnyConnect UI가 사용되지 않습니다.

다음 절차는 독립형 프로파일 편집기를 설치하고, 프로파일을 생성하고, DMG 패키지에 해당 프로파일을 추가하여 모듈을 맞춤화하는 방법에 대해 설명합니다. 또한 AnyConnect 사용자 인터페이스가 부팅 시 자동으로 시작되어 AnyConnect에서 모듈에 필요한 사용자 및 그룹 정보를 제공하도록 설정합니다.

프로시저

단계 **1** Cisco.com에서 Cisco AnyConnect Secure Mobility Client DMG 패키지를 다운로드합니다.

단계 **2** 파일을 열고 설치 프로그램에 액세스하십시오. 다운로드한 이미지는 읽기 전용 파일이라는 점에 유의하십시오.

단계 **3** 다음과 같이 디스크 유틸리티를 실행하거나 터미널 애플리케이션을 사용하여 설치 프로그램 이미지를 쓰기 가능하게 만드십시오.

```
hdiutil convert <source dmg> -format UDRW -o <output dmg>
```

단계 **4** Windows 운영 체제가 실행 중인 컴퓨터에 독립형 프로파일 편집기를 설치합니다. Custom(맞춤형) 설치나 Complete(전체) 설치의 일부분으로 설치할 AnyConnect 모듈을 선택해야 합니다. 이러한 모듈은 기본적으로 설치되지 않습니다.

단계 **5** 프로파일 편집기를 시작하고 프로파일을 생성합니다.

단계 **6** 프로파일을 `WebSecurity_ServiceProfile.xml`, `NVM_ServiceProfile.xml` 또는 대시보드에서 받은 `OrgInfo.json`으로 안전한 위치에 적절하게 저장합니다.

프로파일 편집기는 이러한 모듈용으로 프로파일의 난독화된 추가 버전(예: 웹 보안의 경우 `WebSecurity_ServiceProfile.wso`)을 생성하여 파일을 저장한 것과 같은 위치에 저장합니다(예: 웹 보안의 경우 `WebSecurity_ServiceProfile.xml`로 저장). 난독화를 완료하려면 다음 단계를 수행합니다.

a) 지정한 .wso 파일을 Windows 머신에서 macOS 설치 프로그램 패키지의 적절한 폴더 경로(예: 웹 보안의 경우 `AnyConnect x.x.x/Profiles/websecurity`)에 복사합니다. 또는 터미널 애플리케이션을 사용합니다. 웹 보안의 경우 아래 예시와 같은 명령을 사용할 수 있습니다.

```
cp <path to the wso> \Volumes\"AnyConnect <VERSION>"\Profiles\websecurity\
```

b) macOS 설치 프로그램에서 `AnyConnect x.x.x/Profiles` 디렉터리로 이동하여 편집할 `ACTransforms.xml` 파일을 TextEdit에서 엽니다. 다음과 같이 `<DisableVPN>` 요소를 **true**로 설정하여 VPN 기능이 설치되어 있지 않은지 확인합니다.

```
<ACTransforms>

<DisableVPN>true</DisableVPN>

</ACTransforms>
```

c) 이제 AnyConnect DMG 패키지를 사용자에게 배포할 준비가 되었습니다.

macOS에서 애플리케이션 제한

게이트키퍼는 시스템에서 실행할 수 있는 애플리케이션을 제한합니다. 다음 위치에서 애플리케이션 다운로드를 허용하도록 선택할 수 있습니다.

- Mac App Store
- Mac App Store 및 확인된 개발자
- 위치 무관

기본 설정은 Mac App Store 및 확인된 개발자(서명된 애플리케이션)입니다.

AnyConnect의 최신 버전은 Apple 인증서를 사용하는 서명된 애플리케이션입니다. Gatekeeper가 Mac App Store(전용)용으로 구성된 경우, Anywhere setting(AnyConnect 설정)을 선택하거나 control(컨트롤)을 클릭하여 사전 구축한 설치에서 AnyConnect 설치 및 실행을 위해 선택한 설정을 우회해야 합니다. 자세한 내용은 http://www.apple.com/macosx/mountain-lion/security.html을 참조하십시오.

Linux에 사전 구축

Linux용 모듈 설치

Linux용 개별 설치 프로그램을 분류하여 직접 배포할 수 있습니다. 사전 구축 패키지에 포함된 각 설치 프로그램은 개별적으로 실행할 수 있습니다. 압축 파일 유틸리티를 사용하여 tar.gz 파일에서 파일을 확인하고 압축을 푸십시오.

프로시저

단계 **1** GUI 및 VPN 기능(SSL 및 IPsec 모두)을 설치하는 AnyConnect 코어 클라이언트 모듈을 설치합니다.
단계 **2** AnyConnect 코어 클라이언트 설치에 관한 유용한 진단 정보를 제공하는 DART 모듈을 설치하십시오.
단계 **3** Posture 모듈 또는 ISE 컴플라이언스 모듈을 설치합니다.
단계 **4** NVM을 설치합니다.

Linux용 모듈 제거

사용자가 AnyConnect를 제거하는 순서는 중요합니다.

DART 정보는 제거 프로세스가 실패할 경우 유용하게 사용됩니다.

프로시저

단계 **1** NVM을 제거합니다.
단계 **2** Posture 모듈 또는 ISE 컴플라이언스 모듈을 제거합니다.
단계 **3** AnyConnect 코어 클라이언트를 제거합니다.
단계 **4** DART를 제거하십시오.

Linux 디바이스에서 수동으로 NVM 설치/제거

프로시저

단계 **1** AnyConnect 사전 구축 패키지의 압축을 풉니다.
단계 **2** nvm 디렉터리로 이동합니다.
단계 **3** **$sudo ./nvm_install.sh** 스크립트를 호출합니다.

/opt/cisco/anyconnect/bin/nvm_uninstall.sh를 사용하면 NVM을 제거할 수 있습니다.

Firefox를 통한 서버 인증서 확인 초기화

AnyConnect와 함께 서버 인증서를 사용하는 경우 AnyConnect가 인증서에 액세스하여 신뢰성을 확인하도록 인증서 저장소를 설정해야 합니다. 기본적으로 AnyConnect는 Firefox 인증서 저장소를 사용합니다.

Firefox 인증서 저장소 활성화

Linux 디바이스에 AnyConnect를 설치하고 AnyConnect 연결을 처음으로 시도하기 전에 Firefox 브라우저를 여십시오. Firefox를 열면 인증서 저장소를 포함하는 프로파일이 생성됩니다.

Firefox 인증서 저장소를 사용하지 않을 경우

Firefox를 사용하지 않도록 선택한 경우 Firefox 인증서 저장소를 제외하도록 로컬 정책을 구성하고 PEM 저장소를 구성해야 합니다.

다중 모듈 요건

코어 클라이언트를 하나 이상의 선택적 모듈과 함께 구축하는 경우, 각각의 설치 프로그램에 LOCKDOWN 속성을 적용해야 합니다. LOCKDOWN에 대한 설명은 Windows 사전 구축 MSI 예시, 19 페이지의 내용을 참조하십시오.

이 작업은 VPN 설치 프로그램, Network Access Manager, Web Security, Network Visibility Module 및 Umbrella 로밍 보안 모듈에서 사용할 수 있습니다.

참고 VPN 설치 프로그램에 대해 LOCKDOWN을 활성화하도록 선택하면 AMP Enabler도 잠깁니다.

Linux 디바이스에 수동으로 DART 설치

1. anyconnect-dart-linux-(ver)-k9.tar.gz를 로컬로 저장합니다.
2. 터미널에서 **tar -zxvf <***path to tar.gz file including the file name* 명령을 사용하여 tar.gz 파일의 압축을 풉니다.
3. 터미널에서 압축을 푼 폴더로 이동하고 **sudo ./dart_install.sh** 명령을 사용하여 dart_install.sh를 실행합니다.
4. 라이센스 계약서에 동의하고 설치가 완료될 때까지 기다립니다.

참고 **/opt/cisco/anyconnect/dart/dart_uninstall.sh**를 사용하여 DART를 제거만 할 수 있습니다.

AnyConnect 웹 구축

웹 구축은 헤드엔드에서 AnyConnect 소프트웨어를 가져오는 클라이언트 시스템의 AnyConnect 다운로더를 의미하거나 AnyConnect를 설치 또는 업데이트하기 위해 헤드엔드에서 포털을 사용하는 것을 의미합니다. Cisco는 브라우저 지원에 크게 의존했으며 Java 및 ActiveX를 사용해야 했던 기존 웹 실행 방식을 대체하기 위해 자동 웹 구축 플로우를 개선했습니다. 이 플로우는 초기 다운로드 시와 클라이언트리스 페이지에서의 실행 시에 제공됩니다.

ASA를 사용한 웹 구축

ASA의 클라이언트리스 포털은 AnyConnect를 웹 구축합니다. 프로세스 흐름은 다음과 같습니다.

사용자가 브라우저를 열고 ASA의 클라이언트리스 포털에 연결합니다. ASA는 클라이언트와 초기 SSL 연결을 설정하고 로그온 페이지를 엽니다. 사용자가 로그온 및 인증을 충족하면 클라이언트리스 포털 페이지에 AnyConnect 클라이언트 시작 대화 상자가 표시됩니다. AnyConnect 다운로드를 선택하면 ASA가 컴퓨터의 운영 체제에 맞는 클라이언트를 다운로드합니다. 다운로드 후 클라이언트는 스스로 설치 및 구성하며 IPsec(IKEv2) 또는 ASA에 대한 SSL 연결(웹 실행)을 설정합니다. ActiveX 또는 Java 문제로 웹 실행을 실행할 수 없는 경우, 사용자는 AnyConnect를 수동으로 다운로드할 수 있습니다.

ASA 웹 구축 제한

- 동일한 O/S용으로 여러 AnyConnect 패키지를 ASA에 로드하는 기능은 지원되지 않습니다.
- OPSWAT 정의는 웹 구축 시 VPN Posture 모듈(HostScan)에 포함되지 않습니다. 클라이언트에 OPSWAT 정의를 제공하려면 수동으로 HostScan 모듈을 구축하거나 ASA에 이 모듈을 로드해야 합니다.
- ASA에 기본적인 내부 플래시 메모리 크기만 있는 경우 ASA에서 여러 AnyConnect 클라이언트 패키지를 저장 및 로드할 경우 문제가 발생할 수 있습니다. 플래시에 패키지 파일을 보관하기 위한 충분한 공간을 갖추고 있는 경우에도, ASA에서 클라이언트 이미지의 압축을 풀고 로드할 때 캐시 메모리가 모두 소진될 수 있습니다. AnyConnect 구축 및 ASA 메모리 업그레이드 시 ASA 메모리 요구량에 대한 자세한 내용은 VPN 어플라이언스의 가장 최근 릴리스 정보를 참조하십시오.
- 사용자는 IP 주소 또는 DNS를 사용하여 ASA에 연결할 수 있지만 해당 링크 로컬 보안 게이트웨이 주소는 지원되지 않습니다.
- Internet Explorer에서 신뢰할 수 있는 사이트 목록에 웹 실행을 지원하는 보안 어플라이언스 URL을 추가해야 합니다. Windows의 Internet Explorer 신뢰할 수 있는 사이트 목록에 ASA 추가에 설명된 것과 같이 그룹 정책을 통해 이 작업을 수행할 수 있습니다.

ISE를 사용한 웹 구축

ISE 정책은 AnyConnect 클라이언트를 언제 구축할지 결정합니다. 사용자는 브라우저를 열고 ISE에서 제어하는 리소스에 연결하며, 그러면 AnyConnect 클라이언트 포털로 리디렉션됩니다. 해당 ISE 포털에서는 AnyConnect를 다운로드하고 설치할 수 있습니다. Internet Explorer에서 ActiveX 컨트롤이

설치를 안내합니다. 다른 브라우저의 경우 포털에서는 Network Setup Assistant를 다운로드하고 이 툴을 사용하여 AnyConnect를 설치할 수 있습니다.

ISE 구축 제한

- ISE와 ASA가 모두 AnyConnect를 웹 구축하는 경우, 구성 사항이 두 가지 헤드엔드에서 일치해야 합니다.
- ISE 서버는 AnyConnect ISE Posture 에이전트가 ISE 클라이언트 프로비저닝 정책에 구성된 경우 이 에이전트를 통해서만 탐지될 수 있습니다. ISE 관리자는 Agent Configuration(에이전트 구성) > Policy(정책) > Client Provisioning(클라이언트 프로비저닝) 아래에서 NAC 에이전트 또는 AnyConnect ISE Posture 모듈 중 하나를 구성합니다.

ASA에서 웹 구축 구성

WebLaunch 브라우저 제한

표 *4:* 운영 체제별 ***Weblaunch***에 대한 ***AnyConnect*** 브라우저 지원

운영 체제	브라우저
Windows 10 및 10 RS1, RS2, RS2 x86(32비트)/x64(64비트)	Internet Explorer 11 Firefox 3.51 이상
Windows 8.x x86(32비트) 및 x64(64비트)	Internet Explorer 11 Firefox 10.0.10 이상
Windows 7 SP1 x86(32비트) 및 x64(64비트)	Internet Explorer 11 Firefox 3.51 이상
macOS 10.10, 10.11 및 10.12(64비트)	Safari 9.1
Red Hat 6(64비트) Ubuntu 14.04(LTS) 및 16.04(64비트)	(RHEL 6) Firefox 3 이상 (14.04) Firefox 29.0 이상 (16.04) Firefox 29.0 이상

참고 웹 실행은 NPAPI(Netscape 플러그인 애플리케이션 프로그래밍 인터페이스) 플러그인을 지원하는 모든 브라우저에서 작동합니다.

AnyConnect 4.3 이상은 VS(Visual Studio) 2015 구축 환경으로 이동되었으며, Network Access Manager 모듈 기능용으로 VS 재배포 가능 파일이 필요합니다. 이러한 파일은 설치 패키지의 일부로 설치됩니다. .msi 파일을 사용하여 Network Access Manager 모듈을 4.3 이상으로 업그레이드할 수 있지만, 먼저 AnyConnect Secure Mobility Client를 업그레이드한 다음 릴리스 4.3 이상을 실행해야 합니다.

또한 AnyConnect Umbrella 로밍 보안 모듈을 추가하는 경우 Microsoft .NET 4.0도 필요합니다.

AnyConnect 패키지 다운로드

최신 Cisco AnyConnect Secure Mobility Client 패키지는 Cisco AnyConnect 소프트웨어 다운로드 웹 페이지에서 다운로드할 수 있습니다.

OS	AnyConnect 웹 구축 패키지 이름
Windows	anyconnect-win-*version*-webdeploy-k9.pkg
macOS	anyconnect-macos-*version*-webdeploy-k9.pkg
Linux(64비트)	anyconnect-linux64-*version*-webdeploy-k9.pkg

참고 동일 운영 체제의 서로 다른 여러 버전을 ASA에 설치해서는 안 됩니다.

ASA에서 AnyConnect 패키지 로드

프로시저

단계 1 **Configuration**(구성) > **Remote Access**(원격 액세스) > **VPN** > **Network (Client) Access**(네트워크(클라이언트) 액세스) > **AnyConnect Client Software**(**AnyConnect** 클라이언트 소프트웨어)를 탐색하십시오. AnyConnect 클라이언트 이미지 패널에 현재 ASA에 로드된 AnyConnect 이미지가 표시됩니다. 이미지가 표시되는 순서는 ASA가 원격 컴퓨터로 다운로드하는 순서입니다.

단계 2 AnyConnect 이미지를 추가하려면 **Add**(추가)를 클릭하십시오.

- ASA에 이미 업로드한 AnyConnect 이미지를 선택하려면 **Browse Flash**(플래시 찾아보기)를 클릭하십시오.
- 컴퓨터에서 로컬에 저장된 AnyConnect 이미지를 찾아보려면 **Upload**(업로드)를 클릭하십시오.

단계 3 **OK**(확인) 또는 **Upload**(업로드)를 클릭하십시오.

단계 4 **Apply**(적용)를 클릭합니다.

추가 AnyConnect 모듈 활성화

추가 기능을 활성화하려면 그룹 정책이나 로컬 사용자 구성에 새로운 모듈 이름을 지정하십시오. 추가 모듈을 활성화하면 다운로드 시간에 영향을 줄 수 있다는 점에 유의하십시오. 기능을 활성화할 경우 AnyConnect는 모듈을 VPN 엔드포인트에 다운로드해야 합니다.

참고 Start Before Logon(로그온 전 시작)을 선택하는 경우 AnyConnect 클라이언트 프로파일에서도 이 기능을 활성화해야 합니다.

프로시저

단계 **1** ASDM에서 **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 새 그룹 정책 **Edit(**편집**)** 또는 **Add(**추가**)**를 클릭합니다.

단계 **3** 탐색 창에서 **VPN Policy(VPN** 정책**)** > **AnyConnect Client(AnyConnect** 클라이언트**)**를 선택하십시오. **Client Modules to Download(**다운로드할 클라이언트 모듈**)**에서 **Add(**추가**)**를 클릭하고 해당 그룹 정책에 추가할 각 모듈을 선택하십시오. 모듈을 사용하려면 ASA에 추가하거나 업로드해야 합니다.

단계 **4** **Apply(**적용**)**를 클릭하고 그룹 정책의 변경 사항을 저장하십시오.

ASDM에서 클라이언트 프로파일 생성

ASA에서 클라이언트 프로파일을 생성하려면 먼저 ASA에 AnyConnect 웹 구축 패키지를 추가해야 합니다.

프로시저

단계 **1** **Configuration(**구성**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**)** > **AnyConnect Client Profile(AnyConnect** 클라이언트 프로파일**)**로 이동합니다.

단계 **2** 이 그룹에 연계할 클라이언트 프로파일을 선택하고 **Change Group Policy(**그룹 정책 변경**)**를 클릭합니다.

단계 **3** Change Policy for Profile policy name(프로파일 정책 이름에 대한 정책 변경) 창에서 Available Group Policies(사용 가능한 그룹 정책) 필드에서 Group Policies(그룹 정책)를 선택하고 오른쪽 화살표를 클릭하여 Policies(정책) 필드로 이동시킵니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

단계 **5** AnyConnect 클라이언트 프로파일 페이지에서 **Apply(**적용**)**를 클릭합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

단계 **7** 구성을 완료하면 **OK(**확인**)**를 클릭합니다.

ISE에서 웹 구축 구성

ISE는 AnyConnect 코어, ISE Posture 모듈 및 OPSWAT(규정 준수 모듈)를 ISE의 포스처를 지원하도록 구성하고 구축할 수 있습니다. 또한 ISE는 ASA에 연결할 때 사용될 수 있는 모든 AnyConnect 모듈 및

리소스를 구축할 수 있습니다. 사용자가 ISE에서 제어하는 리소스를 검색하는 경우는 다음과 같습니다.

- ISE가 ASA를 지원하는 경우 사용자가 ASA에 연결하고 AnyConnect를 다운로드하여 VPN에 연결합니다. ASA를 통해 AnyConnect ISE Posture가 설치되지 않은 경우 사용자가 ISE Posture를 설치할 수 있도록 AnyConnect 클라이언트 포털로 리디렉션됩니다.
- ISE가 ASA를 지원하지 않는 경우 사용자가 AnyConnect 클라이언트 포털에 연결합니다. 그러면 ISE의 AnyConnect 구성에서 정의된 AnyConnect 리소스를 설치하도록 안내됩니다. ISE Posture 상태를 알 수 없는 경우 브라우저를 AnyConnect 클라이언트 프로비저닝 포털로 리디렉션하는 것이 일반적인 구성입니다.
- 사용자가 ISE의 AnyConnect 클라이언트 프로비저닝 포털로 디렉션되는 경우 다음과 같습니다.
  - 브라우저가 Internet Explorer인 경우 ISE가 AnyConnect 다운로더를 다운로드하면 다운로더는 AnyConnect를 로드합니다.
  - 다른 브라우저의 경우 ISE가 클라이언트 프로비저닝 리디렉션 포털을 열어 NSA(Network Setup Assistant) 툴을 다운로드할 수 있는 링크를 표시합니다. 사용자가 NSA를 실행하여 ISE 서버를 검색하고 AnyConnect 다운로더를 다운로드합니다.

    Windows에서 NSA는 실행을 완료하면 스스로 삭제됩니다. macOS에서는 NSA가 실행을 완료한 경우 NSA를 수동으로 삭제해야 합니다.

ISE 문서는 다음에 대한 방법을 설명합니다.

- ISE의 AnyConnect 구성 프로파일 생성
- 로컬 머신에서 ISE로 AnyConnect 리소스 추가
- 원격 사이트에서 AnyConnect 프로비저닝 리소스 추가
- AnyConnect 클라이언트 및 리소스 구축

참고 AnyConnect ISE Posture 모듈은 검색에서 웹 프록시 기반 리디렉션을 지원하지 않으므로 리디렉션을 기반으로 하지 않는 검색을 사용하는 것이 좋습니다. Cisco Identity Services Engine 관리자 가이드의 다른 네트워크에 URL 리디렉션을 사용하지 않는 클라이언트 프로비저닝 섹션에서 추가 정보를 확인할 수 있습니다.

ISE는 다음과 같은 AnyConnect 리소스를 구성하고 구축할 수 있습니다.

- ISE Posture 모듈을 포함하는 AnyConnect 코어 및 모듈
- 프로파일: Network Visibility Module, AMP Enabler, VPN, Network Access Manager, Web Security, 고객 피드백 및 AnyConnect ISE Posture
- 사용자 정의를 위한 파일
  - UI 리소스

- 이진 파일, 연결 스크립트 및 도움말 파일

- 현지화 파일
  - 메시지 현지화를 위한 AnyConnect gettext 변환
  - Windows 설치 프로그램 변형

ISE 업로드용 AnyConnect 파일 준비

- 운영 체제용 AnyConnect 패키지 및 로컬 PC에 구축할 다른 AnyConnect 리소스를 다운로드합니다.

  참고 ASA 사용 시에는 VPN 다운로더를 통해 설치가 수행됩니다. 다운로드된 ISE Posture 프로파일은 ASA를 통해 푸시되며, 이후 프로파일 프로비저닝에 필요한 검색 호스트는 ISE Posture 모듈이 ISE에 연결하기 전에 제공됩니다. 반면 ISE 사용 시에는 ISE가 검색된 후에만 ISE Posture 모듈이 프로파일을 가져오므로 오류가 발생할 수 있습니다. 따라서 VPN에 연결할 때 ISE Posture 모듈을 푸시하려면 ASA를 사용하는 것이 좋습니다.

- 사용자가 구축할 모듈용 프로파일을 생성합니다. 최소한 AnyConnect ISE Posture 프로파일을 생성합니다.
- 사용자 정의 및 현지화 리소스를 ZIP 보관 파일(ISE에서 번들이라고 함)에 결합합니다. 번들에는 다음이 포함될 수 있습니다.
  - AnyConnect UI 리소스
  - VPN 연결 스크립트
  - 도움말 파일
  - 설치 프로그램 변형

  AnyConnect 현지화 번들에는 다음이 포함될 수 있습니다.
  - 이진 형식의 AnyConnect gettext 번역
  - 설치 프로그램 변형

ISE 번들 생성에 대한 설명은 ISE 구축용 AnyConnect 사용자 정의 및 현지화 준비를 참조하십시오.

AnyConnect를 구축하기 위한 ISE 구성

추가 AnyConnect 리소스를 업로드하고 생성하기 전에 AnyConnect 패키지를 ISE에 업로드해야 합니다.

참고 ISE에서 AnyConnect 구성 개체를 구성할 때 AnyConnect 모듈 선택에서 VPN 모듈의 선택을 취소하더라도 구축 또는 프로비저닝된 클라이언트의 VPN은 비활성화되지 않습니다. AnyConnect GUI에서 VPN 바둑판식 배열을 비활성화하려면 VPNDisable_ServiceProfile.xml을 구성해야 합니다. VPNDisable_ServiceProfile.xml은 다른 AnyConnect 파일과 함께 CCO에 있습니다.

1. ISE에서 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **results(**결과**)** > 를 선택합니다. **Client Provisioning(**클라이언트 프로비저닝**)** 을 확장하여 **Resources(**리소스**)**가 표시되면 **Resources(**리소스**)**를 선택하십시오.
2. **Add(**추가**)** > **Agent resources from local disk(**로컬 디스크의 에이전트 리소스**)**를 선택하고 AnyConnect 패키지 파일을 업로드하십시오. 구축하려는 다른 AnyConnect 리소스에 대해 로컬 디스크의 에이전트 리소스 추가를 반복하십시오.
3. **Add(**추가**)** > **AnyConnect Configuration(AnyConnect** 컨피그레이션**)** > 을 선택합니다. 이 AnyConnect 컨피그레이션에서는 다음 표에 설명된 대로 모듈, 프로파일, 맞춤화/언어 패키지 및 OPSWAT 패키지를 구성합니다.

   AnyConnect ISE Posture 프로파일은 ASA의 ISE 또는 Windows AnyConnect 프로파일 편집기에서 생성 및 편집할 수 있습니다. 다음 표에서는 각 AnyConnect 리소스의 이름과 ISE에 있는 리소스 유형의 이름에 대해 설명합니다.

   표 ***5: ISE***의 ***AnyConnect*** 리소스

프롬프트	**ISE** 리소스 유형 및 설명
AnyConnect 패키지	AnyConnectDesktopWindows AnyConnectDesktopOSX AnyConnectWebAgentWindows AnyConnectWebAgentOSX
규정 준수 모듈	AnyConnectComplianceModuleWindows AnyConnectComplianceModuleOSX
AnyConnect 프로파일	AnyConnectProfile 업로드된 AnyConnect 패키지에서 제공하는 각 프로파일에 대한 확인란이 ISE에 표시됩니다.
사용자 정의 번들	AnyConnectCustomizationBundle
현지화 번들	AnyConnectLocalizationBundle

4. 역할 또는 OS 기반 클라이언트 프로비저닝 정책을 생성하십시오. 클라이언트 프로비저닝 포스처 에이전트에 대해 AnyConnect 및 ISE 레거시 NAC/MAC 에이전트가 선택될 수 있습니다. 각 CP 정책이 AnyConnect 에이전트 또는 레거시 NAC/MAC 에이전트 중 하나의 에이전트만 프로비저닝

할 수 있습니다. AnyConnect 에이전트를 구성할 때 2단계에서 생성한 AnyConnect 구성 하나를 선택하십시오.

FTD에서 웹 구축 구성

FTD(Firepower Threat Defense) 디바이스는 ASA와 유사한 보안 게이트웨이 기능을 제공하는 NGFW(차세대 방화벽)입니다. FTD 디바이스는 AnyConnect Secure Mobility Client를 사용한 RA VPN(원격 액세스 VPN)만 지원하며 다른 클라이언트 또는 클라이언트리스 VPN 액세스는 지원되지 않습니다. IPsec IKEv2 또는 SSL을 사용하여 터널 설정 및 연결을 수행합니다. FTD 디바이스에 연결할 때 IKEv1은 지원되지 않습니다.

Windows, Mac 및 Linux AnyConnect 클라이언트는 FTD 헤드엔드에 구성되며 연결 시 구축됩니다. 그러므로 원격 사용자가 클라이언트 소프트웨어 설치와 컨피그레이션을 수행할 필요 없이 SSL 또는 IKEv2 IPsec VPN 클라이언트를 사용할 수 있는 이점이 제공됩니다. 클라이언트가 이전에 설치된 경우 사용자가 인증을 통과하면 FTD 헤드엔드에서 클라이언트의 개정 내역을 확인하고 필요에 따라 클라이언트를 업그레이드합니다.

이전에 설치된 클라이언트가 없는 경우 원격 사용자는 AnyConnect 클라이언트를 다운로드 및 설치하도록 구성된 인터페이스의 IP 주소를 입력합니다. FTD 헤드엔드는 원격 컴퓨터의 운영 체제와 일치하는 클라이언트를 다운로드 및 설치하고 보안 연결을 설정합니다.

Apple iOS 및 Android 디바이스용 AnyConnect 앱은 플랫폼 앱 스토어에서 설치됩니다. 이러한 앱에는 FTD 헤드엔드 연결을 설정하기 위한 최소 컨피그레이션이 필요합니다. 다른 헤드엔드 디바이스 및 환경과 마찬가지로 이 장에서 설명하는 대체 구축 방법을 사용하여 AnyConnect 소프트웨어를 배포할 수도 있습니다.

현재는 코어 AnyConnect VPN 모듈 및 AnyConnect VPN 프로파일만 FTD에 구성하고 엔드포인트로 배포할 수 있습니다. FMC(Firepower Management Center)의 원격 액세스 VPN 정책 마법사를 통해 이러한 기본 VPN 기능을 빠르고 쉽게 설정할 수 있습니다.

AnyConnect 및 FTD에 대한 지침 및 제한 사항

- 지원되는 VPN 클라이언트는 Cisco AnyConnect Secure Mobility Client뿐입니다. 그 외의 클라이언트 또는 네이티브 VPN은 지원되지 않습니다. 클라이언트리스 VPN은 그 자체로는 지원되지 않으며 AnyConnect Client를 구축하는 용도로만 사용됩니다.
- AnyConnect와 FTD를 사용하는 경우 AnyConnect 버전 4.0 이상과 FMC 버전 6.2.1 이상이 필요합니다.
- AnyConnect 프로파일 편집기는 FMC에서 기본적으로 지원되지 않으며 VPN 프로파일을 독립적으로 구성해야 합니다. VPN 프로파일 및 AnyConnect VPN 패키지는 FMC에 파일 개체로 추가되어 RA VPN 컨피그레이션의 일부가 됩니다.
- Secure Mobility, Network Access Manager 및 코어 VPN 기능을 제외한 기타 모든 AnyConnect 모듈과 해당 프로파일은 현재 지원되지 않습니다.
- VPN 로드 밸런싱은 지원되지 않습니다.
- 브라우저 프록시는 지원되지 않습니다.

- 클라이언트 포스처를 기반으로 하는 모든 포스처 변형(HostScan, Endpoint Posture Assessment 및 ISE) 및 동적 액세스 정책은 지원되지 않습니다.
- Firepower Threat Defense 디바이스는 AnyConnect를 맞춤화하거나 현지화하는 데 필요한 파일을 구성하거나 구축하지 않습니다.
- AnyConnect Client에서 맞춤형 속성을 사용해야 하는 기능(예: 데스크톱 클라이언트의 보류 업그레이드, 모바일 클라이언트의 앱별 VPN)은 FTD에서 지원되지 않습니다.
- FTD 헤드엔드에서 로컬로 인증을 수행할 수는 없으므로 구성된 사용자를 원격 연결에 사용할 수 없으며 FTD는 인증 증명 역할을 할 수 없습니다. 또한 다음 인증 기능은 지원되지 않습니다.
  - 2차 또는 이중 인증
  - SAML 2.0을 사용하는 SSO(Single Sign-On)
  - TACACS, Kerberos(KCD 인증) 및 RSA SDI
  - LDAP 권한 부여(LDAP 속성 맵)
  - RADIUS CoA

FTD에서 AnyConnect를 구성하고 구축하는 방법에 대한 자세한 내용은 Firepower Management Center 환경 설정 가이드, 릴리스 6.2.1 이상의 해당 릴리스에서 *Firepower Threat Defense* 원격 액세스 *VPN* 장을 참조하십시오.

AnyConnect 소프트웨어 및 프로파일 업데이트

여러 가지 방법으로 AnyConnect를 업데이트할 수 있습니다.

- AnyConnect 클라이언트 - AnyConnect에서 ASA에 연결할 때 AnyConnect 다운로더는 새 소프트웨어 또는 프로파일이 ASA에 로드되어 있는지 확인합니다. 다운로더는 클라이언트에 업데이트를 다운로드하여 VPN 터널을 설정합니다.
- 클라우드 업데이트 - Umbrella 로밍 보안 모듈이 Umbrella 클라우드 인프라에서 설치된 모든 AnyConnect 모듈에 대해 자동 업데이트를 제공할 수 있습니다. 클라우드 업데이트를 사용하는 경우에는 Umbrella 클라우드 인프라에서 소프트웨어 업그레이드를 자동으로 가져오며, 관리자의 작업이 아닌 클라우드 인프라를 통해 업데이트를 추적합니다. 기본적으로 클라우드 업데이트를 통한 자동 업데이트는 비활성화되어 있습니다.
- ASA 또는 FTD 포털 - 업데이트를 받기 위해 ASA의 클라이언트리스 포털에 연결하도록 사용자에게 지시합니다. FTD는 코어 VPN 모듈만 다운로드합니다.
- ISE - 사용자가 ISE를 연결하면 ISE는 AnyConnect 컨피그레이션을 사용하여 업데이트된 구성 요소 또는 새로운 포스처 요건이 있는지 결정합니다. 업데이트가 제공되는 경우 사용자가 ASA, 무선 컨트롤러, 스위치 등의 NAD(네트워크 액세스 디바이스)에 연결합니다. 권한이 부여되면 NAD는 사용자를 ISE 포털로 리디렉션하며, 패키지 추출 및 설치 관리를 위해 AnyConnect 다운로더가 클라이언트에 설치됩니다.

엔드 유저가 업데이트를 연기하도록 허용할 수 있으며, 헤드엔드에 업데이트를 로드하더라도 클라이언트의 업데이트는 차단할 수 있습니다.

업그레이드 예시 흐름

사전 요구 사항

다음 예에서는 다음 사항을 가정합니다.

- 클라이언트를 ISE의 AnyConnect 클라이언트 프로비저닝 포털에 리디렉션하는 시기를 결정하기 위해 클라이언트의 포스처 상태를 사용하는 ISE에서 DACL(Dynamic Authorization Control List, 동적 권한 부여 제어 목록)을 생성했으며 이 DACL이 ASA에 푸시되었습니다.
- ISE가 ASA를 지원합니다.

AnyConnect가 클라이언트에 설치됨

1. 사용자는 AnyConnect를 시작하고 자격 증명을 제공하며 Connect(연결)를 클릭합니다.
2. ASA가 SSL의 클라이언트 연결을 열고 인증 자격 증명을 ISE에 전달하면 ISE는 자격 증명을 확인합니다.
3. AnyConnect는 업그레이드를 수행하는 AnyConnect 다운로더를 실행하고 VPN 터널을 시작합니다.

ISE Posture가 ASA를 사용하여 설치되지 않은 경우 다음과 같습니다.

1. 사용자는 임의의 사이트를 찾아보며 DACL에 의해 ISE의 AnyConnect 클라이언트 프로비저닝 포털로 리디렉션됩니다.
2. 브라우저가 Internet Explorer인 경우 ActiveX 컨트롤에서 AnyConnect 다운로더를 시작합니다. 다른 브라우저에서는 AnyConnect 다운로더를 다운로드하고 시작하는 NSA(Network Setup Assistant)를 다운로드 및 실행합니다.
3. AnyConnect 다운로더는 현재 AnyConnect ISE Posture 모듈을 포함하는 ISE에 구성된 모든 AnyConnect 업그레이드를 수행합니다.
4. 클라이언트에서 ISE Posture 에이전트가 포스처를 시작합니다.

AnyConnect가 설치되지 않음

1. 사용자는 ASA 클라이언트리스 포털에 연결하는 사이트를 찾습니다.
2. 사용자는 ISE로 전달되고 확인되는 인증 자격 증명을 제공합니다.
3. AnyConnect 다운로더는 Internet Explorer에서 ActiveX 컨트롤로 시작되고 다른 브라우저에서는 Java 애플릿으로 시작됩니다.
4. AnyConnect 다운로더는 ASA에 구성된 업그레이드를 수행한 다음 VPN 터널을 시작합니다. 다운로더가 완료됩니다.

ISE Posture가 ASA를 사용하여 설치되지 않은 경우 다음과 같습니다.

1. 사용자는 사이트를 다시 찾아보며 ISE의 AnyConnect 클라이언트 프로비저닝 포털로 리디렉션됩니다.
2. Internet Explorer에서 ActiveX 컨트롤이 AnyConnect 다운로더를 시작합니다. 다른 브라우저에서는 AnyConnect 다운로더를 다운로드하고 시작하는 NSA를 다운로드 및 실행합니다.
3. AnyConnect 다운로더는 AnyConnect ISE Posture 모듈 추가를 포함하는 기존 VPN 터널을 통해 ISE에 구성된 모든 업그레이드를 수행합니다.
4. ISE Posture 에이전트가 포스처 평가를 시작합니다.

AnyConnect 자동 업데이트 비활성화

클라이언트 프로파일을 구성하고 배포하여 AnyConnect 자동 업데이트를 비활성화하거나 제한할 수 있습니다.

- VPN 클라이언트 프로파일:
  - Auto Update(자동 업데이트)가 자동 업데이트를 비활성화합니다. 이 프로파일은 AnyConnect 웹 구축 설치에 포함되거나, 기존 클라이언트 설치에 추가할 수 있습니다. 또한 사용자가 이 설정을 토글하도록 허용할 수 있습니다.
- VPN 로컬 정책 프로파일:
  - Bypass Downloader(우회 다운로더)에서 ASA의 업데이트된 콘텐츠가 클라이언트로 다운로드되는 것을 방지합니다.
  - Update Policy(업데이트 정책)를 선택하면 다른 헤드엔드에 연결할 때 소프트웨어 및 프로파일 업데이트를 세분화하여 제어할 수 있습니다.

WebLaunch 중에 AnyConnect를 다운로드하도록 사용자에게 프롬프트 표시

원격 사용자에게 웹 구축을 시작하라는 프롬프트를 표시하도록 ASA를 구성할 수 있으며 AnyConnect를 다운로드하거나 클라이언트리스 포털 페이지로 이동하는 것을 선택할 수 있는 시간을 구성할 수 있습니다.

사용자에게 AnyConnect를 다운로드하라는 프롬프트를 표시하는 것은 그룹 정책 또는 사용자 계정에서 구성됩니다. 다음 단계는 그룹 정책에서 이 기능을 설정하는 방법을 보여줍니다.

프로시저

단계 **1** ASDM에서 **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 새 그룹 정책 **Edit**(편집) 또는 **Add**(추가)를 클릭합니다.

단계 **3** 탐색 창에서 **Advanced(**고급**)** > **AnyConnect Client(AnyConnect** 클라이언트**)** > **Login Settings(**로그인 설정**)**를 선택하십시오. 필요한 경우 **Inherit(**상속**)** 확인란의 선택을 해제하고 Post Login(로그인 후) 설정을 선택하십시오.

사용자에게 프롬프트를 표시하도록 선택한 경우, Default Post Login Selection(기본 사후 로그인 선택) 영역에서 시간 제한 기간을 지정하고 해당 기간이 만료될 때 수행하는 기본 작업을 선택하십시오.

단계 **4** **OK(**확인**)** 를 클릭하고 그룹 정책에 변경 사항이 적용되었는지 확인한 다음 **Save(**저장**)**를 클릭하십시오.

사용자의 업그레이드 보류 허용

AnyConnect 자동 업데이트 비활성화에 설명된 것과 같이 AutoUpdate를 비활성화하여 사용자가 AnyConnect 업데이트를 허용하도록 할 수 있습니다. AutoUpdate는 기본적으로 활성화되어 있습니다.

또한 사용자가 보류 업데이트를 설정하여 클라이언트 업데이트를 나중으로 연기하도록 할 수 있습니다. 보류 업데이트가 구성되어 있고 클라이언트 업데이트를 사용할 수 있는 경우에는 AnyConnect에 사용자에게 업데이트할지 또는 보류할지 묻는 대화 상자가 열립니다. 보류 업데이트는 Windows, Linux 및 OS X에서 모두 지원됩니다.

ASA에서 보류 업데이트 구성

ASA에서 맞춤형 속성을 추가한 다음 그룹 정책에서 해당 속성을 참조 및 구성하여 보류 업데이트를 활성화합니다. 모든 맞춤형 속성이 보류 업그레이드를 사용하도록 생성하고 구성해야 합니다.

ASA 컨피그레이션에 맞춤형 속성을 추가하는 절차는 실행 중인 ASA/ASDM 릴리스에 따라 달라집니다. 맞춤형 속성 컨피그레이션 절차에 대해 ASA/ASDM 구축 릴리스에 해당하는 *Cisco ASA Series VPN ASDM* 환경 설정 가이드 또는 *Cisco ASA Series VPN CLI* 환경 설정 가이드를 참조하십시오.

다음 속성 및 값은 ASDM의 보류 업데이트를 구성합니다.

맞춤형 속성 *	유효한 값	기본값	참고
DeferredUpdateAllowed	true false	false	값이 true이면 보류 업데이트가 활성화됩니다. 보류 업데이트가 비활성화된 경우(false) 아래 설정이 무시됩니다.

맞춤형 속성 *	유효한 값	기본값	참고
DeferredUpdateMinimumVersion	*x.x.x*	0.0.0	업데이트를 보류하기 위해 설치해야 하는 AnyConnect의 최소 버전입니다. 최소 버전 확인은 헤드엔드에서 활성화된 모든 모듈에 적용됩니다. 모든 활성화된 모듈(VPN 포함)이 설치되지 않았거나 최소 버전과 일치하지 않는 경우, 이 연결은 보류 업데이트에 적합하지 않습니다. 이 특성이 지정되지 않은 경우, 엔드포인트에 설치된 버전에 관계없이 보류 프롬프트가 표시되거나 자동으로 해제됩니다.

맞춤형 속성 *	유효한 값	기본값	참고
DeferredUpdateDismissTimeout	0-300 (초)	150초	보류 업그레이드 프롬프트가 자동으로 해제될 때까지 표시되는 시간(초)입니다. 이 특성은 보류 업데이트 프롬프트가 표시될 예정인 경우에만 적용됩니다(최소 버전 특성이 먼저 평가됨). 이 특성을 설정하지 않은 경우, 자동 해제 기능이 비활성화되고 사용자가 응답할 때까지 대화 상자가 표시됩니다(필요시). 이 특성을 0으로 설정하면 자동 보류 또는 업그레이드가 다음에 기초하여 강제로 적용됩니다. • DeferredUpdateMinimumVersion의 설치된 버전 및 값 • DeferredUpdateDismissResponse의 값
DeferredUpdateDismissResponse	defer update	update	DeferredUpdateDismissTimeout 발생 시 적용

* 맞춤형 속성 값은 대/소문자를 구분합니다.

ISE에서 보류 업데이트 구성

프로시저

단계 **1** 다음 탐색 단계를 수행합니다.

a) **Policy(**정책**)** > **Results(**결과**)**를 선택합니다.
b) **Client Provisioning(**클라이언트 프로비저닝**)**을 확장합니다.
c) **Resources(**리소스**)**를 선택하고 **Add(**추가**)** > **Agent Resources from Local Disk(**로컬 디스크의 에이전트 리소스**)**를 클릭합니다.
d) AnyConnect pkg 파일을 업로드하고 **Submit(**제출**)**을 선택합니다.

단계 **2** 생성한 기타 모든 AnyConnect 리소스를 업로드합니다.

단계 **3** **Resources(**리소스**)**에서 업로드한 AnyConnect 패키지를 사용하여 **AnyConnect Configuration(AnyConnect** 구성**)**을 추가합니다. AnyConnect 구성에 보류 업데이트를 구성하는 필드가 있습니다.

보류 업데이트 **GUI**

다음 그림은 사용자가 업데이트를 사용할 수 있는 시점 및 보류 업데이트가 구성된 시점을 확인할 수 있는 UI를 표시합니다. 그림의 오른쪽 부분은 **DeferredUpdateDismissTimeout** 이 구성된 시점의 UI를 보여줍니다.

업데이트 정책 설정

업데이트 정책 개요

AnyConnect 소프트웨어 및 프로파일 업데이트는 사용 가능하며 헤드엔드에 연결 시 클라이언트에서 업데이트를 허용하는 경우 발생합니다. AnyConnect 업데이트용 헤드엔드를 구성하면 업데이트를 사용할 수 있습니다. VPN 로컬 정책 파일의 업데이트 정책 설정에 따라 업데이트 허용 여부가 결정됩니다.

경우에 따라 업데이트 정책을 소프트웨어 잠금이라고도 합니다. 여러 헤드엔드가 구성된 경우, 업데이트 정책을 다중 도메인 정책이라고도 합니다.

기본적으로 업데이트 정책 설정에서는 모든 헤드엔드로부터 소프트웨어 및 프로파일 업데이트를 허용합니다. 이를 제한하기 위해 다음과 같이 업데이트 정책 매개변수를 설정합니다.

- **Server Name** 목록에서 특정 헤드엔드를 지정하여 해당 헤드엔드가 모든 AnyConnect 소프트웨어 및 프로파일을 업데이트하도록 허용(권한을 부여)합니다.

  헤드엔드 서버 이름은 FQDN 또는 IP 주소일 수 있습니다. 또는 와일드카드일 수도 있습니다(예: *.example.com).

  업데이트가 발생하는 방식에 대한 전체 설명은 아래 권한 있는 서버 업데이트 정책 동작 을 참조하십시오.

- 기타 모든 지정되지 않은 헤드엔드 또는 무단 헤드엔드의 경우:
  - **Allow Software Updates From Any Server** 옵션을 사용하여 VPN 코어 모듈 및 기타 선택적 모듈의 소프트웨어 업데이트를 허용하거나 허용하지 않도록 설정합니다.
  - **Allow VPN Profile Updates From Any Server** 옵션을 사용하여 VPN 프로파일 업데이트를 허용하거나 허용하지 않도록 설정합니다.
  - **Allow Service Profile Updates From Any Server** 옵션을 사용하여 기타 서비스 모듈 프로파일 업데이트를 허용하거나 허용하지 않도록 설정합니다.
  - 모든 서버에서 **ISE Posture** 프로파일 업데이트 허용 옵션을 사용하여 ISE Posture 프로파일 업데이트를 허용하거나 허용하지 않습니다.
  - 모든 서버에서 규정준수 모듈 업데이트 허용 옵션을 사용하여 규정준수 모듈 업데이트를 허용하거나 허용하지 않습니다.

업데이트가 발생하는 방식에 대한 전체 설명은 아래 무단 서버 업데이트 정책 동작 을 참조하십시오.

권한 있는 서버 업데이트 정책 동작

Server Name 목록에 나와 있는 승인된 헤드엔드에 연결하는 경우 다른 업데이트 정책 매개변수가 적용되지 않으며 다음과 같은 작업이 수행됩니다.

- 헤드엔드의 AnyConnect 패키지 버전은 소프트웨어의 업데이트 여부를 판단하기 위해 클라이언트의 버전과 비교 분석됩니다.
  - AnyConnect 패키지가 클라이언트 버전보다 이전 버전인 경우 소프트웨어 업데이트가 발생하지 않습니다.
  - AnyConnect 패키지의 버전이 클라이언트의 버전과 같은 경우 헤드엔드에서 다운로드를 위해 구성되고 클라이언트에 존재하지 않는 소프트웨어 모듈만 다운로드 및 설치됩니다.
  - AnyConnect 패키지가 클라이언트의 버전보다 신규 버전인 경우 헤드엔드에서 다운로드를 위해 구성된 소프트웨어 모듈 및 클라이언트에 이미 설치된 소프트웨어 모듈이 다운로드되고 설치됩니다.
- 헤드엔드의 VPN 프로파일, ISE Posture 프로파일 및 각 서비스 프로파일은 업데이트 여부를 판단하기 위해 클라이언트의 해당 프로파일과 비교 분석됩니다.
  - 헤드엔드의 프로파일이 클라이언트의 프로파일과 같은 경우 업데이트되지 않습니다.
  - 헤드엔드의 프로파일이 클라이언트의 프로파일과 다른 경우 다운로드됩니다.

무단 서버 업데이트 정책 동작

무단 헤드엔드에 연결할 경우, **Allow ... Updates From Any Server** 옵션을 사용하여 다음과 같이 AnyConnect 업데이트 방법을 결정합니다.

- **Allow Software Updates From Any Server:**
  - 이 옵션을 선택하면 소프트웨어 업데이트가 이러한 무단 ASA에 대해 허용됩니다. 업데이트는 위에 설명된 것과 같이 권한 있는 헤드엔드에 대한 버전 비교를 기반으로 합니다.
  - 이 옵션을 선택하지 않으면 소프트웨어 업데이트가 실행되지 않습니다. 또한 버전 비교를 기반으로 업데이트해야 하는 경우 VPN 연결 시도가 종료됩니다.
- **Allow VPN Profile Updates From Any Server:**
  - 이 옵션을 선택하면 헤드엔드의 VPN 프로파일이 클라이언트와 다른 경우 VPN 프로파일이 업데이트됩니다.
  - 이 옵션을 선택하지 않으면 VPN 프로파일은 업데이트되지 않습니다. 또한 차별화를 기반으로 VPN 프로파일을 업데이트해야 하는 경우, VPN 연결 시도가 종료됩니다.
- **Allow Service Profile Updates From Any Server:**

- 이 옵션을 선택하면 헤드엔드의 프로파일이 클라이언트와 다른 경우 각 서비스 프로파일이 업데이트됩니다.
- 이 옵션을 선택하지 않으면 서비스 프로파일은 업데이트되지 않습니다.

- **Allow ISE Posture Profile Updates From Any Server:**
  - 이 옵션을 선택하면 헤드엔드의 ISE Posture 프로파일이 클라이언트와 다른 경우 ISE Posture 프로파일이 업데이트됩니다.
  - 이 옵션을 선택하지 않으면 ISE Posture 프로파일은 업데이트되지 않습니다. ISE Posture 프로파일은 ISE Posture 에이전트가 작동하는 데 필요합니다.

- **Allow Compliance Module Updates From Any Server:**
  - 이 옵션을 선택하면 헤드엔드의 규정 준수 모듈이 클라이언트와 다른 경우 규정 준수 모듈이 업데이트됩니다.
  - 이 옵션을 선택하지 않으면 규정 준수 모듈은 업데이트되지 않습니다. 규정 준수 모듈은 ISE Posture 에이전트가 작동하는 데 필요합니다.

업데이트 정책 지침

- 권한 있는 **Server Name** 목록에서 해당 서버의 IP 주소를 나열하여 원격 사용자가 이 서버의 IP 주소를 사용하는 헤드엔드에 연결할 수 있도록 설정합니다. 사용자가 IP 주소를 사용하여 연결을 시도하지만 헤드엔드가 FQDN으로 나열된 경우, 이러한 시도는 무단 도메인에 대한 연결로 처리됩니다.
- 소프트웨어 업데이트에는 사용자 정의, 현지화, 스크립트 및 변형을 다운로드하는 기능이 포함되어 있습니다. 소프트웨어 업데이트가 허용되지 않는 경우 이러한 항목은 다운로드되지 않습니다. 일부 클라이언트에서 스크립트 업데이트를 허용하지 않는 경우 정책 시행을 위해 스크립트를 사용하지 마십시오.
- 상시 가동 을 활성화한 상태로 VPN 프로파일을 다운로드하면 클라이언트에서 기타 모든 VPN 프로파일이 삭제됩니다. 무단 또는 기업용이 아닌 헤드엔드로부터의 VPN 프로파일 업데이트를 허용 또는 허용하지 않을지 결정할 때 이 점을 고려하십시오.
- 설치 및 업데이트 정책으로 인해 VPN 프로파일이 클라이언트에 다운로드되지 않으면 다음 기능을 사용할 수 없습니다.

서비스 비활성화	신뢰할 수 없는 네트워크 정책
인증서 저장소 재정의	신뢰할 수 있는 DNS 도메인
사전 연결 메시지 표시	신뢰할 수 있는 DNS 서버
로컬 LAN 액세스	상시 가동
로그온 전 시작	종속 포털 보안정책 교정
로컬 프록시 연결	스크립팅

PPP 제외	로그오프 시 VPN 유지
자동 VPN 정책	디바이스 잠금 필요
신뢰할 수 있는 네트워크 정책	자동 서버 선택

- 다운로더는 다운로드 목록을 기록하는 별도의 텍스트 로그(UpdateHistory.log)를 생성합니다. 이 로그에는 업데이트 시간, 클라이언트를 업데이트한 ASA, 업데이트된 모듈 및 업그레이드 이전과 이후에 설치된 버전이 포함되어 있습니다. 이 로그 파일은 다음 위치에 저장됩니다.

  `%AllUsers%\Application Data\Cisco\Cisco AnyConnect Secure Mobility Client\Logs` 디렉토리

업데이트 정책 예

이 예시에서는 클라이언트의 AnyConnect 버전이 다양한 ASA 헤드엔드와 다른 경우의 클라이언트 업데이트 동작을 보여줍니다.

다음의 VPN 로컬 정책 XML 파일의 업데이트 정책을 고려하십시오.

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectLocalPolicy acversion="2.4.140"
xmlns=http://schemas.xmlsoap.org/encoding/
xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectLocalPolicy.xsd">
<FipsMode>false</FipsMode>
<BypassDownloader>false</BypassDownloader><RestrictWebLaunch>false</RestrictWebLaunch>
<StrictCertificateTrust>false</StrictCertificateTrust>
<RestrictPreferenceCaching>false</RestrictPreferenceCaching>
<RestrictTunnelProtocols>false</RestrictTunnelProtocols>
<UpdatePolicy>
<AllowSoftwareUpdatesFromAnyServer>true</AllowSoftwareUpdatesFromAnyServer>
<AllowVPNProfileUpdatesFromAnyServer>true</AllowVPNProfileUpdatesFromAnyServer>
<AllowServiceProfileUpdatesFromAnyServer>true</AllowServiceProfileUpdatesFromAnyServer>
<AllowISEProfileUpdatesFromAnyServer>false</AllowISEProfileUpdatesFromAnyServer>
<AllowComplianceModuleUpdatesFromAnyServer>true</AllowComplianceModuleUpdatesFromAnyServer>
<AuthorizedServerList>
    <ServerName>seattle.example.com</ServerName>
    <ServerName>newyork.example.com</ServerName>
     </AuthorizedServerList>
</UpdatePolicy>
</AnyConnectLocalPolicy>
```

ASA 헤드엔드 구성은 다음과 같습니다.

ASA 헤드엔드	로드된 **AnyConnect** 패키지	다운로드할 모듈
seattle.example.com	버전 3.1.05182	VPN, Network Access Manager, 웹 보안
newyork.example.com	버전 3.1.06079	VPN, Network Access Manager
raleigh.example.com	버전 3.1.07021	VPN, 포스처

클라이언트에서 AnyConnect VPN 및 Network Access Manager 모듈을 현재 실행 중인 경우, 다음 순서대로 업데이트할 수 있습니다.

- 클라이언트를 동일한 버전의 AnyConnect가 구성된 권한 있는 서버인 seattle.example.com에 연결합니다. 웹 보안 소프트웨어 모듈과 웹 보안 프로파일(사용 가능한 경우)을 다운로드 및 설치합니다. VPN 및 Network Access Manager 프로파일을 다운로드할 수 있으며 해당 프로파일이 클라이언트의 프로파일과 다른 경우, 이 프로파일도 다운로드됩니다.
- 클라이언트를 새로운 버전의 AnyConnect가 구성된 권한 있는 ASA인 newyork.example.com에 연결합니다. VPN, Network Access Manager 및 웹 보안 모듈을 다운로드하고 설치합니다. 다운로드가 가능하고 클라이언트의 프로파일과 다른 프로파일도 다운로드됩니다.
- 클라이언트를 무단 ASA인 raleigh.example.com에 연결합니다. 소프트웨어 업데이트가 허용되므로 VPN, Network Access Manager, 웹 보안 및 포스처 모듈이 모두 업그레이드됩니다. VPN 프로파일 및 서비스 프로파일 업데이트는 허용되지 않으므로 다운로드되지 않습니다. VPN 프로파일을 다른 방법으로 업데이트한 경우 연결이 종료됩니다.

AnyConnect 참조 정보

로컬 컴퓨터에 있는 사용자 환경 설정 파일의 위치

AnyConnect는 사용자 환경 설정 파일 및 전역 환경 설정 파일로 사용자 컴퓨터에 일부 프로파일 설정을 저장합니다. AnyConnect는 로컬 파일을 사용하여 클라이언트 GUI의 환경 설정 탭에 있는 사용자 제어 가능 설정을 구성하며 사용자, 그룹 및 호스트 같은 최신 연결에 대한 정보를 표시합니다.

AnyConnect는 로그온 전에 발생하는 작업에 대해 전역 파일을 사용합니다. 예를 들어 Start Before Logon(로그온 전 시작) 및 AutoConnect On Start(시작 시 AutoConnect)입니다.

다음 표에서는 클라이언트 컴퓨터에서 환경 설정 파일의 파일 이름 및 설치된 경로를 보여줍니다.

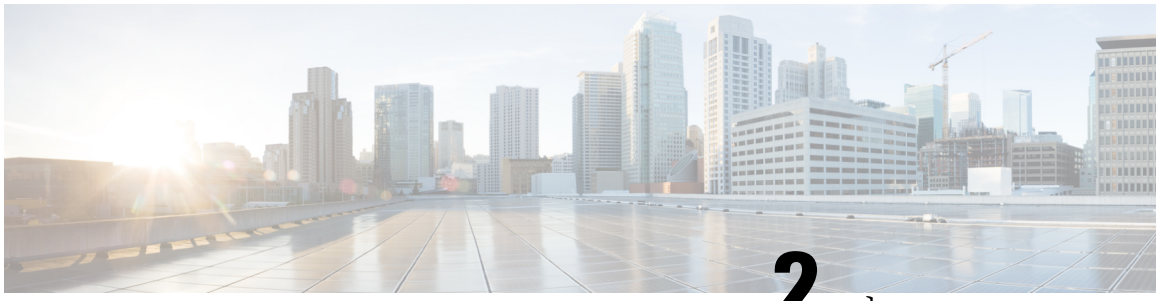
운영 체제	유형	파일 및 경로
Windows	사용자	C:\Users\username\AppData\Local\Cisco\Cisco AnyConnect VPN Client\preferences.xml
	글로벌	C:\ProgramData\Cisco\Cisco AnyConnect VPN Client\preferences_global.xml
macOS	사용자	/Users/username/.anyconnect
	글로벌	/opt/cisco/anyconnect/.anyconnect_global
Linux	사용자	/home/username/.anyconnect
	글로벌	/opt/cisco/anyconnect/.anyconnect_global

AnyConnect 및 레거시 VPN 클라이언트에서 사용되는 포트

다음 표에는 각 프로토콜에 대한 레거시 Cisco VPN 클라이언트 및 Cisco AnyConnect Secure Mobility Client 에서 사용하는 포트가 나열되어 있습니다.

프로토콜	**Cisco AnyConnect** 클라이언트 포트
TLS(SSL)	TCP 443
SSL 리디렉션	TCP 80(선택 사항)
DTLS	UDP 443(선택 사항이지만 권장됨)
IPsec/IKEv2	UDP 500, UDP 4500

프로토콜	**Cisco VPN** 클라이언트**(IPsec)** 포트
IPsec/NATT	UDP 500, UDP 4500
IPsec/NATT	UDP 500, UDP 4500
IPsec/TCP	TCP(구성 가능)
IPsec/UDP	UDP 500, UDP X(구성 가능)



2 장

AnyConnect 클라이언트 및 설치 프로그램 사용자 정의 및 현지화

AnyConnect 설치 동작 수정

지침

- 웹 구축은 클라이언트리스 SSL 포털의 일부인 AnyConnect 웹 실행을 사용합니다. 클라이언트리스 SSL 포털은 사용자 정의할 수 있지만 포털의 AnyConnect 부분은 사용자 정의할 수 없습니다. 예를 들어 Start AnyConnect(AnyConnect 시작) 버튼은 사용자 정의할 수 없습니다.

고객 경험 피드백 비활성화

고객 경험 피드백 모듈은 기본적으로 활성화되어 있습니다. 이 모듈은 사용자가 활성화하고 사용 중인 기능과 모듈에 대하여 Cisco에 익명의 정보를 제공합니다. 이 정보는 Cisco가 품질, 안정성, 성능 및 사용자 환경을 계속해서 향상할 수 있도록 사용자 경험에 대한 통찰력을 제공해 줍니다.

고객 경험 피드백 모듈을 수동으로 비활성화하려면 독립형 프로파일 편집기를 사용하여 CustomerExperience_Feedback.xml 파일을 생성합니다. AnyConnect 서비스를 중지하고 파일 이름을 CustomerExperience_Feedback.xml로 지정한 다음 C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility

Client\CustomerExperienceFeedback\ 디렉터리에 파일을 저장해야 합니다. 비활성화 플래그를 설정하여 파일을 생성하면 AnyConnect에 이 파일을 수동으로 구축할 수 있습니다. 결과를 확인하려면 AnyConnect About(정보) 메뉴를 열고 Installed Module(설치된 모듈) 섹션에 고객 경험 피드백 모듈이 나열되지 않는지 확인합니다.

다음을 사용하여 고객 경험 피드백 모듈을 비활성화할 수 있습니다.

- 고객 경험 피드백 모듈 클라이언트 프로파일 - 고객 경험 피드백 서비스 활성화를 선택 취소하고 프로파일을 배포합니다.
- MST 파일 - anyconnect-vpn-transforms-X.X.xxxxx.zip에서 anyconnect-win-disable-customer-experience-feedback.mst의 압축을 해제합니다.

설치 동작 수정(Windows)

- AnyConnect 설치 동작을 수정하려면 Windows 설치 프로그램 속성을 사용하십시오. 이 속성은 다음과 같이 사용할 수 있습니다.
  - 커맨드 라인 파라미터 — 1개 이상의 속성이 커맨드 라인 설치 프로그램 msiexec의 파라미터로 전달됩니다. 이 방법은 사전 구축용으로 웹 구축에서는 지원하지 않습니다.
  - 설치 프로그램 변형 — 변형을 통해 설치 프로그램 속성 테이블을 수정할 수 있습니다. 변형을 생성하는 데는 몇 가지 툴이 있으며 자주 사용되는 툴은 Microsoft Orca입니다. Orca 툴은 Microsoft Windows Installer SDK(Software Development Kit, 소프트웨어 개발 키트)의 일부로 Microsoft Windows SDK에 포함되어 있습니다. Windows SDK를 가져오려면 http://msdn.microsoft.com으로 이동하여 사용하는 Windows 버전에 맞는 SDK를 검색하십시오.

    변형은 사전 구축에만 사용할 수 있습니다. (다운로더가 설치 프로그램을 호출할 때는 웹 구축에 대해 Cisco에서 서명한 변형만 작동합니다.) OOB(Out of Band) 방법을 통해 고유한 변형을 적용할 수는 있지만 이 가이드에서 해당 세부사항을 설명하지는 않습니다.

- ISO 이미지에서는 설치 프로그램 `setup.hta` 가 편집할 수 있는 HTML입니다.

제한 사항

AnyConnect 제거 프롬프트를 사용자 정의할 수 없습니다.

클라이언트 설치를 사용자 정의하는 Windows Installer 속성

다음 Windows Installer 속성은 AnyConnect 설치를 사용자 정의합니다. Microsoft에서 지원하는 기타 여러 Windows Installer 속성을 활용할 수 있다는 점에 유의하십시오.

- 시스템 MTU 재설정 — VPN 설치 프로그램 속성(RESET_ADAPTER_MTU)이 1로 설정된 경우, 설치 프로그램이 모든 Windows 네트워크 어댑터 MTU 설정을 기본값으로 재설정합니다. 변경 사항을 적용하려면 시스템을 재부팅해야 합니다.
- Windows 잠금 설정 - 최종 사용자에게는 디바이스의 Cisco AnyConnect Secure Mobility Client 에 대해 제한된 권한을 부여하는 것이 좋습니다. 최종 사용자가 추가적인 권한을 보장할 경우 설치

프로그램은 사용자와 로컬 관리자가 AnyConnect 서비스를 끄거나 중지하지 못하도록 방지하는 잠금 기능을 제공할 수 있습니다. 또한 서비스 비밀번호를 사용하여 명령 프롬프트에서 서비스를 중지할 수 있습니다.

VPN, Network Access Manager, Web Security, Network Visibility Module 및 Umbrella 로밍 보안 모듈용 MSI 설치 프로그램은 공통 속성(LOCKDOWN)을 지원합니다. 이 LOCKDOWN이 영(0)이 아닌 값으로 설정된 경우, 엔드포인트 디바이스에서 사용자 또는 로컬 관리자가 설치 프로그램과 연관된 Windows 서비스를 제어하지 못합니다. 제공되는 샘플 변형을 사용하여 이 속성을 설정하고 잠금을 설정하려는 각 MSI 설치 프로그램에 변형을 적용할 것을 권장합니다. Cisco AnyConnect Secure Mobility Client 소프트웨어 다운로드 페이지에서 샘플 변형을 다운로드할 수 있습니다.

코어 클라이언트를 하나 이상의 선택적 모듈과 함께 구축하는 경우, 각각의 설치 프로그램에 LOCKDOWN 속성을 적용해야 합니다. 이 작업은 제품을 다시 설치하지 않는 한 유일한 방법이며 제거할 수 없습니다.

참고 AMP Enabler 설치 프로그램은 VPN 설치 프로그램과 통합되어 있습니다.

- ActiveX 컨트롤 켜기 — AnyConnect 사전 구축 VPN 패키지의 이전 버전에서 기본적으로 VPN WebLaunch ActiveX 컨트롤을 설치했습니다. AnyConnect 3.1에서 시작할 경우 VPN ActiveX 컨트롤 설치가 기본적으로 꺼져 있습니다. 가장 안전한 구성을 기본값으로 설정하기 위해 변경되었습니다.

  AnyConnect 클라이언트 및 선택적 모듈을 사전 구축할 때 VPN ActiveX 컨트롤을 AnyConnect와 함께 설치해야 하는 경우, msiexec 또는 변형에서 NOINSTALLACTIVEX=0 옵션을 사용해야 합니다.

- 프로그램 추가/제거 목록에서 AnyConnect 숨기기 — Windows 제어판에 있는 사용자 프로그램 추가/제거 목록에서 설치된 AnyConnect 모듈을 숨길 수 있습니다. ARPSYSTEMCOMPONENT=1을 설치 프로그램에 전달하면 해당 모듈이 설치된 프로그램 목록에 표시되는 것을 방지합니다.

  제공되는 샘플 변형을 사용하여 이 속성을 설정하고 숨기려는 각 모듈에 대한 각 MSI 설치 프로그램에 변형을 적용할 것을 권장합니다. Cisco AnyConnect Secure Mobility Client 소프트웨어 다운로드 페이지에서 샘플 변형을 다운로드할 수 있습니다.

AnyConnect 모듈에 대한 Windows Installer 속성

다음 표에서는 프로파일을 구축하기 위한 MSI 설치 커맨드 라인 호출 및 위치에 대한 예시가 제공됩니다.

설치된 모듈	명령 및 로그 파일
VPN 기능이 없는 AnyConnect 코어 클라이언트 (독립형 모듈 설치 시 사용)	msiexec /package anyconnect-win-*version*-predeploy-k9.msi /norestart /passive PRE_DEPLOY_DISABLE_VPN=1 /lvx* anyconnect-win-*version*-predeploy-k9-install-datetimestamp.log

설치된 모듈	명령 및 로그 파일
VPN 기능이 있는 AnyConnect 코어 클라이언트	msiexec /package anyconnect-win-*version*-predeploy-k9.msi /norestart /passive /lvx* anyconnect-win-*version*-predeploy-k9-install-datetimestamp.log
고객 경험 피드백	msiexec /package anyconnect-win-*version*-predeploy-k9.msi /norestart /passive DISABLE_CUSTOMER_EXPERIENCE_FEEDBACK=1 /lvx* anyconnect-win-*version*-predeploy-k9-install-datetimestamp.log
DART(Diagnostic and Reporting Tool, 진단 및 보고 툴)	msiexec /package anyconnect-win-*version*-dart-predeploy-k9.msi /norestart /passive /lvx* anyconnect-win-*version*-dart-predeploy-k9-install-datetimestamp.log
SBL	msiexec /package anyconnect-win-*version*-gina-predeploy-k9.msi /norestart /passive /lvx* anyconnect-win-*version*-gina-predeploy-k9-install-datetimestamp.log
Network Access Manager	msiexec /package anyconnect-win-*version*-nam-predeploy-k9.msi /norestart /passive /lvx* anyconnect-win-*version*-nam-predeploy-k9-install-datetimestamp.log
웹 보안	msiexec /package anyconnect-win-*version*-websecurity-predeploy-k9.msi /norestart/passive /lvx* anyconnect-win-*version*-websecurity-predeploy-k9-install-datetimestamp.log
포스처	msiexec /package anyconnect-win-*version*-posture-predeploy-k9.msi /norestart/passive /lvx* anyconnect-win-*version*-posture-predeploy-k9-install-datetimestamp.log
ISE Posture	msiexec /package anyconnect-win-*version*-iseposture-predeploy-k9.msi /norestart/passive /lvx* anyconnect-win-*version*-iseposture-predeploy-k9-install-datetimestamp.log
AMP Enabler	msiexec /package anyconnect-win-*version*-amp-predeploy-k9.msi /norestart/ passive /lvx* anyconnect-win-*version*-amp-predeploy-k9-install-datetimestamp.log

설치된 모듈	명령 및 로그 파일
Network Visibility Module	msiexec /package anyconnect-win-*version*-nvm-predeploy-k9.msi /norestart/ passive /lvx* anyconnect-win-*version*-nvm-predeploy-k9-install-datetimestamp.log
Umbrella 로밍 보안 모듈	msiexec /package anyconnect-win-*version*-umbrella-predeploy-k9.msi/norestart/ passive /lvx* anyconnect-win-*version*-predeploy-k9-install-datetimestamp.log

사용자 정의 설치 프로그램 변형을 Adaptive Security Appliance에 가져오기

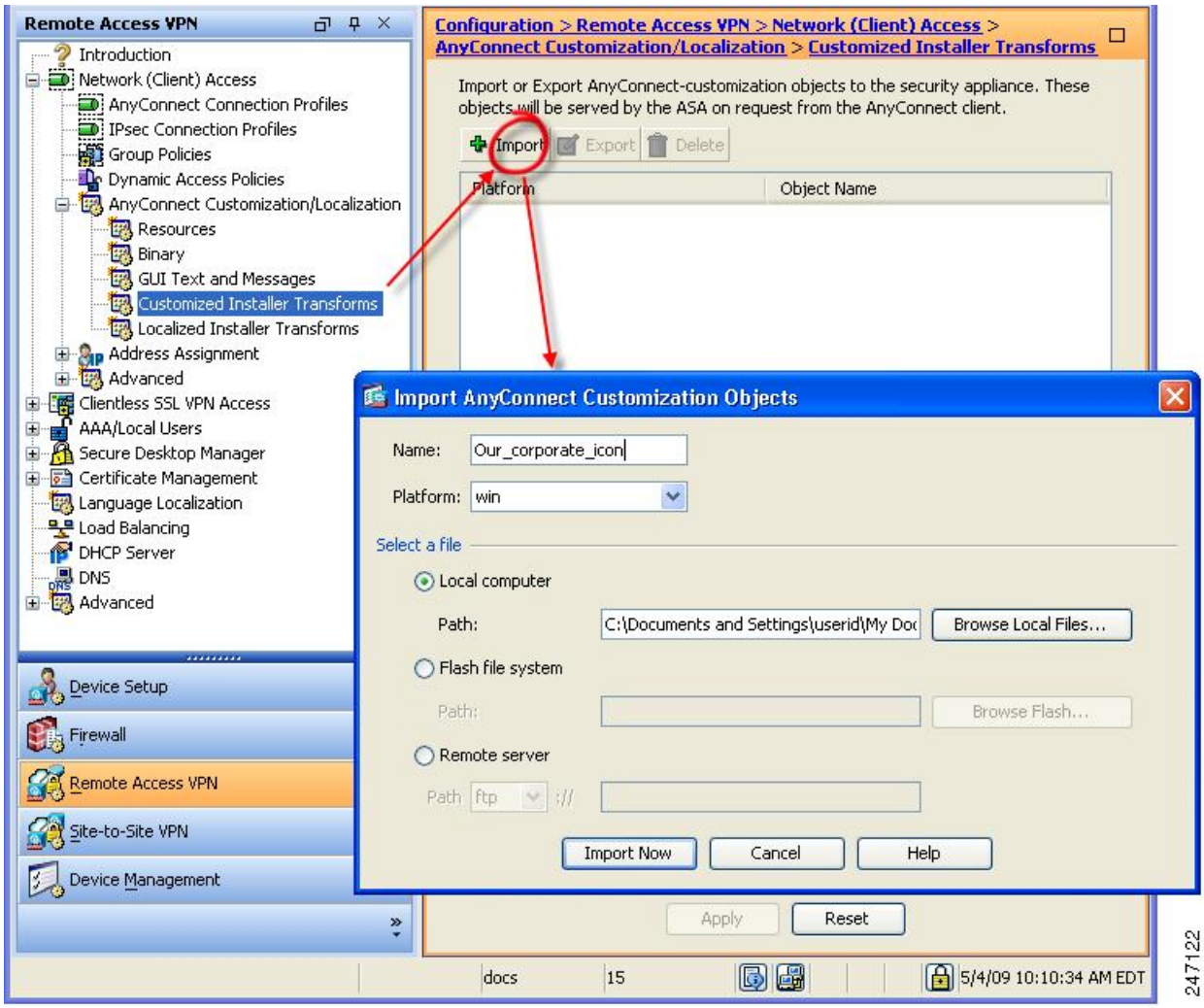
Cisco에서 제공하는 Windows 변형을 Adaptive Security Appliance에 가져오면 웹 구축 시 사용할 수 있습니다.

프로시저

단계 **1** ASDM에서 **Configuration(**구성**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**)** > **AnyConnect Customization/Localization(AnyConnect** 사용자 정의/현지화**)** > **Customized Installer Transforms(**사용자 정의 설치 프로그램 변형**)**로 이동합니다.

단계 **2** **Import(**가져오기**)**를 클릭합니다.

다음과 같이 Import AnyConnect Customization Objects(AnyConnect 사용자 정의 개체 가져오기) 창이 표시됩니다.



단계 **3** 가져올 파일의 이름을 입력하십시오. 이 이름은 다른 사용자 정의 개체의 이름과 달리 ASA에서 중요하지 않으며 편의를 위한 것입니다.

단계 **4** 플랫폼을 선택하고 가져올 파일을 지정하십시오. **Import Now(**지금 가져오기**)**를 클릭하십시오. 이제 설치 프로그램 변형 테이블에 파일이 표시됩니다.

AnyConnect 설치 프로그램 화면 현지화

AnyConnect 설치 프로그램을 통해 표시되는 메시지를 변환할 수 있습니다. ASA는 설치 프로그램을 통해 표시되는 메시지를 변환하기 위해 변형을 사용합니다. 변형은 설치를 변경하지만 원래 보안 서명된 MSI는 그대로 유지합니다. 이러한 변형은 설치 프로그램의 화면만 변환하며 클라이언트 GUI 화면은 변환하지 않습니다.

참고 AnyConnect의 모든 릴리스에는 새 소프트웨어를 사용하여 AnyConnect 패키지를 업로드할 때마다 관리자가 Adaptive Security Applicance에 업로드할 수 있는 현지화된 변형이 포함되어 있습니다. Cisco의 현지화 변형을 사용하는 경우 새 AnyConnect 패키지를 업로드할 때마다 cisco.com의 최신 릴리스를 사용하여 현지화 변형을 업데이트하십시오.

Cisco에서는 현재 30개 언어의 변형을 제공합니다. 이러한 변형은 cisco.com의 AnyConnect 소프트웨어 다운로드 페이지에서 다음 .zip 파일로 제공됩니다.

```
anyconnect-win-<VERSION>-webdeploy-k9-lang.zip
```

이 파일에서 <VERSION>은 AnyConnect 릴리스의 버전을 의미합니다(예: 4.3.xxxxx).

아카이브 파일에는 사용할 수 있는 번역에 대한 변형(.mst 파일)이 포함되어 있습니다. Cisco에서 제공하는 30개 언어에 속하지 않는 언어를 원격 사용자에게 제공해야 하는 경우 고유한 변형을 생성하여 새 언어로 ASA에 가져올 수 있습니다. Microsoft 데이터베이스 편집기인 Orca를 사용하면 기존 설치 및 새 파일을 수정할 수 있습니다. Orca는 Microsoft Windows Installer SDK(Software Development Kit, 소프트웨어 개발 키트)의 일부로 Microsoft Windows SDK에 포함되어 있습니다.

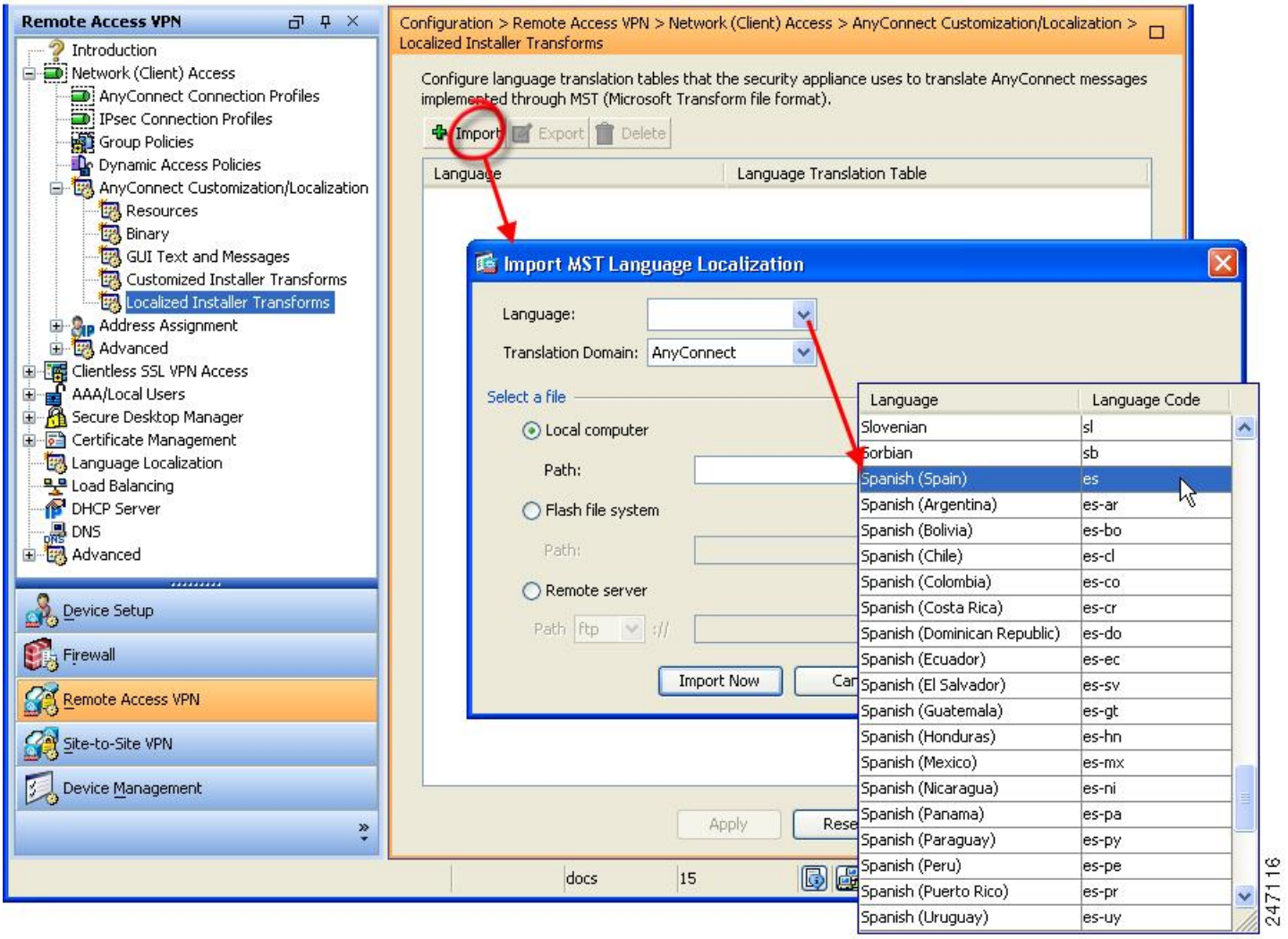
현지화된 설치 프로그램 변형을 Adaptive Security Applicance에 가져오기

다음 절차는 ASDM을 사용하여 ASA에 변형을 가져오는 방법을 보여줍니다.

프로시저

단계 **1** ASDM에서 **Configuration(**구성**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**)** > **AnyConnect Customization/Localization(AnyConnect** 사용자 정의/현지화**)** > **Localized Installer Transforms(**현지화 설치 프로그램 변형**)**로 이동합니다.

단계 **2** **Import(**가져오기**)**를 클릭합니다. 다음과 같이 Import MST Language Localization(MST 언어 현지화 가져오기) 창이 열립니다.



단계 **3** **Language**(언어) 드롭다운 목록을 클릭하여 해당 변형에 대한 언어 및 업계 승인 약어를 선택하십시오. 약어를 수동으로 입력하는 경우 브라우저 및 운영 체제에서 인식하는 약어를 사용하십시오.

단계 **4** **Import Now**(지금 가져오기)를 클릭하십시오.
테이블을 성공적으로 가져왔음을 알리는 메시지가 표시됩니다.

단계 **5** **Apply**(적용) 를 클릭하여 변경 사항을 저장합니다.

이 절차에서는 스페인어(es)로 언어를 지정했습니다. 다음 그림은 AnyConnect의 언어 목록에서 스페인어에 대한 새로운 변형을 보여줍니다.

설치 동작 수정(macOS)

제한 사항

AnyConnect 설치 프로그램을 현지화할 수 없습니다. 설치 프로그램에서 사용된 문자열의 출처는 AnyConnect 설치 프로그램이 아닌 Mac 설치 프로그램 애플리케이션입니다.

ACTransforms.xml을 사용하여 macOS에서 설치 프로그램 동작 맞춤화

.pkg 동작을 맞춤화하는 표준 방식이 macOS용으로 제공되지 않으므로 ACTransforms.xml을 생성했습니다. 이 XML 파일이 설치 프로그램과 함께 배치된 경우 설치 프로그램은 설치 실행 전에 이 파일을 읽습니다. 설치 프로그램과 관련된 특정 위치에 파일을 배치해야 합니다. 설치 프로그램은 다음과 같은 순서로 검색하여 수정 사항 여부를 확인합니다.

1. .pkg 설치 프로그램 파일과 같은 디렉토리에 있는 "프로파일" 디렉토리
2. 마운트형 디스크 이미지 볼륨의 루트에 있는 "프로파일" 디렉토리
3. 마운트형 디스크 이미지 볼륨의 루트에 있는 "프로파일" 디렉토리

XML 파일 형식은 다음과 같습니다.

```
<ACTransforms>
<PropertyName1>Value</PropertyName1>
<PropertyName2>Value</PropertyName2>
</ACTransforms>
```

예를 들어 macOS ACTransforms.xml 속성은 Web Security의 “독립형” 구축을 생성하는 DisableVPN입니다. ACTransforms.xml은 DMG 파일의 프로파일 디렉토리에 있습니다.

고객 경험 피드백 모듈 비활성화

고객 경험 피드백 모듈은 기본적으로 활성화되어 있습니다. Mac OS X에서 이 기능을 끄려면 다음을 수행하십시오.

프로시저

단계 **1** 디스크 유틸리티 또는 hdiutil을 사용하여 dmg 패키지를 읽기 전용에서 읽기/쓰기로 변환하십시오. 예를 들면 다음과 같습니다.

```
hdiutil convert anyconnect-macosx-i386-ver-k9.dmg -format UDRW -o
anyconnect-macosx-i386-ver-k9-rw.dmg
```

단계 **2** 아직 설정되지 않은 경우 ACTransforms.xml을 편집하고 다음 값을 설정하거나 추가하십시오.

```
<DisableCustomerExperienceFeedback>false</DisableCustomerExperienceFeedback>
```

설치 동작 수정(Linux)

ACTransforms.xml을 사용하여 Linux에서 설치 프로그램 동작 사용자 정의

.pkg 동작을 사용자 정의하는 표준 방식이 Linux용으로 제공되지 않으므로 ACTransforms.xml을 생성했습니다. 이 XML 파일이 설치 프로그램과 함께 배치된 경우 설치 프로그램은 설치 실행 전에 이 파일을 읽습니다. 설치 프로그램과 관련된 특정 위치에 파일을 배치해야 합니다. 설치 프로그램은 다음과 같은 순서로 검색하여 수정 사항 여부를 확인합니다.

- .pkg 설치 프로그램 파일과 같은 디렉토리에 있는 "프로파일" 디렉토리
- 마운트형 디스크 이미지 볼륨의 루트에 있는 "프로파일" 디렉토리
- .dmg 파일과 같은 디렉토리에 있는 "프로파일" 디렉토리

사전 구축 패키지의 프로파일 디렉토리에 있는 XML 파일인 ACTransforms.xml의 형식은 다음과 같습니다.

```
<ACTransforms>
<PropertyName1>Value</PropertyName1>
<PropertyName2>Value</PropertyName2>
</ACTransforms>
```

DSCP 보존 활성화

DTLS 연결 전용으로 Windows 또는 OS X 플랫폼에 DSCP(Differentiated Services Code Point) 제어를 위한 맞춤형 속성을 설정할 수 있습니다. DSCP 보존을 수행하는 경우 디바이스가 레이턴시에 민감한 트래픽의 우선순위를 지정할 수 있습니다. 라우터는 이 우선순위가 설정되어 있는지를 고려하며 우선순위가 지정된 트래픽을 표시하여 아웃바운드 연결 품질을 개선합니다.

맞춤형 속성 형식은 DSCPPreservationAllowed이고 유효한 값은 True 또는 False입니다.

참고 AnyConnect는 기본적으로 DSCP 보존을 수행합니다(True). DSCP 보존을 비활성화하려면 헤드엔드에서 맞춤형 속성 값을 false로 설정하고 연결을 다시 시작합니다.

ASDM의 **Configuration**(컨피그레이션) > **Remote Access VPN**(원격 액세스 **VPN**) > **Network (Client) Access**(네트워크(클라이언트) 액세스) > **Group Policies**(그룹 정책) > **Add/Edit**(추가/편집) > **Advanced**(고급) > **AnyConnect Client**(**AnyConnect** 클라이언트) > **Custom Attributes**(맞춤형 속성)에서 이 기능을

구성합니다. 컨피그레이션 프로세스는 Cisco ASA Series VPN 환경 설정 가이드의 해당 릴리스에서 *DSCP* 보존 활성화 섹션을 참조하십시오.

공용 DHCP 서버 경로 설정

Tunnel All Network(모든 네트워크 터널링)가 구성된 경우 로컬 DHCP 트래픽을 투명하게 전송하기 위해 AnyConnect 클라이언트 연결 시 AnyConnect는 로컬 DHCP 서버에 특정 경로를 추가합니다. 또한, 이 경로에서 데이터 유출을 방지하기 위해 AnyConnect는 호스트 머신의 LAN 어댑터에 암시적 필터를 적용하여 해당 경로에 대해 DHCP 트래픽을 제외한 모든 트래픽을 차단합니다. 외부 인터페이스에 연결하며 연결이 설정된 후 로컬 DHCP 서버를 사용하는 경우에는 가상 어댑터가 아닌 NIC를 가리키는 해당 서버로의 정적 경로가 생성됩니다. 같은 서버에서 WINS, DNS 등의 다른 서비스를 실행 중인 경우에는 VPN 세션이 설정된 후 이 경로로 인해 이러한 서비스가 중단됩니다.

Windows에서 그룹 정책 맞춤형 속성을 설정하여 DHCP 공용 서버 경로 생성을 제어할 수 있습니다. 터널 설정 시 공용 DHCP 서버 경로를 만들지 않으려면 no-dhcp-server-route 맞춤형 속성이 있어야 하며 true로 설정해야 합니다.

ASDM의 **Configuration(**컨피그레이션**) > Remote Access VPN(**원격 액세스 **VPN) > Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**) > Group Policies(**그룹 정책**) > Add/Edit(**추가/편집**) > Advanced(**고급**) > AnyConnect Client(AnyConnect** 클라이언트**) > Custom Attributes(**맞춤형 속성**)**에서 이 기능을 구성합니다. 컨피그레이션 프로세스는 Cisco ASA Series VPN 환경 설정 가이드의 해당 릴리스를 참조하십시오.

AnyConnect GUI 텍스트 및 메시지 사용자 정의

ASA(Adaptive Security Appliance)는 AnyConnect로 표시된 사용자 메시지를 번역하기 위해 변환 테이블을 사용합니다. 변환 테이블은 번역된 메시지 텍스트 문자열을 포함한 텍스트 파일입니다. ASDM 또는 변형(Windows용)을 사용하여 기존 메시지를 편집하고 추가 언어를 추가할 수 있습니다.

다음의 현지화를 위한 Windows 샘플 변형은 www.cisco.com에서 이용할 수 있습니다.

- Windows 플랫폼용 사전 구축 패키지를 위한 언어 현지화 변형 파일
- Windows 플랫폼용 웹 구축 패키지를 위한 언어 현지화 변형 파일

Windows용 AnyConnect 패키지 파일에는 AnyConnect 메시지의 기본 영어 템플릿이 포함되어 있습니다. ASA에서 AnyConnect 패키지를 로드할 때 ASA가 이 파일을 자동으로 가져옵니다. 이 템플릿은 AnyConnect 소프트웨어의 메시지 문자열에 대한 최신 변경 사항을 포함하고 있습니다. 해당 템플릿을 사용하여 다른 언어에 대한 새 변환 테이블을 생성하거나 www.cisco.com에서 제공하는 다음 변환 테이블 중 하나를 가져올 수 있습니다(Adaptive Security Appliance에 변환 테이블 가져오기, 61 페이지 참조).

- 중국어(간체)
- 중국(번체)
- 체코어

- 네덜란드어
- 프랑스어
- 프랑스어(캐나다)
- 독일어
- 헝가리어
- 이탈리아어
- 일본어
- 한국어
- 폴란드어
- 포르투갈어(브라질)
- 러시아
- 스페인어 (남미 지역)

다음 섹션에서는 원하는 언어가 제공되지 않거나 가져온 변환 테이블을 추가로 사용자 정의하려는 경우, GUI 텍스트 및 메시지를 변환하는 절차를 설명합니다.

- AnyConnect 텍스트 및 메시지 추가 또는 편집. 다음 중 한 가지 방법으로 1개 이상의 메시지 ID에 대한 메시지 텍스트를 변경할 수 있는 파일을 추가하거나 편집하여 메시지 파일을 변경할 수 있습니다.
  - 열린 대화 상자에서 텍스트에 변경사항을 입력합니다.
  - 열린 대화 상자에서 텍스트를 텍스트 편집기에 복사하고 변경을 수행한 다음 이 텍스트를 대화 상자에 다시 붙여 넣습니다.
- Adaptive Security Appliance에 변환 테이블 가져오기, 61 페이지. Save to File(파일에 저장)을 클릭하여 메시지 파일을 내보내고 파일을 편집한 후 ASDM으로 다시 가져올 수 있습니다.

ASA로 변환 테이블을 업데이트하면 클라이언트가 다시 시작되어 다른 연결에 성공할 때까지 업데이트된 메시지가 적용되지 않습니다.

참고 ASA의 클라이언트를 구축하지 않고 Altiris Agent 등의 기업 소프트웨어 구축 시스템을 사용하고 있는 경우, Gettext와 같은 카탈로그 유틸리티를 사용하여 AnyConnect 변환 테이블(anyconnect.po)을 .mo 파일로 수동 변환하고 .mo 파일을 클라이언트 컴퓨터의 적합한 폴더에 설치할 수 있습니다. 자세한 내용은 엔터프라이즈 구축용 메시지 카탈로그 생성 을 참조하십시오.

지침 및 제한 사항

AnyConnect는 모든 국가별 요건을 완전히 준수하지 못하며 다음과 같은 예외 사항이 있을 수 있습니다.

- 날짜 또는 시간 형식이 로캘 요건을 따르지 않을 수도 있습니다.
- 오른쪽에서 왼쪽 방향으로 쓰는 언어가 지원되지 않습니다.
- 일부 문자열이 하드 코드된 필드 길이로 인해 UI에서 잘립니다.
- 다음과 같이 일부 하드 코드된 영어 문자열이 유지됩니다.
  - 업데이트 시 상태 메시지
  - 신뢰할 수 없는 서버 메시지
  - 보류 업데이트 메시지

AnyConnect 텍스트 및 메시지 추가 또는 편집

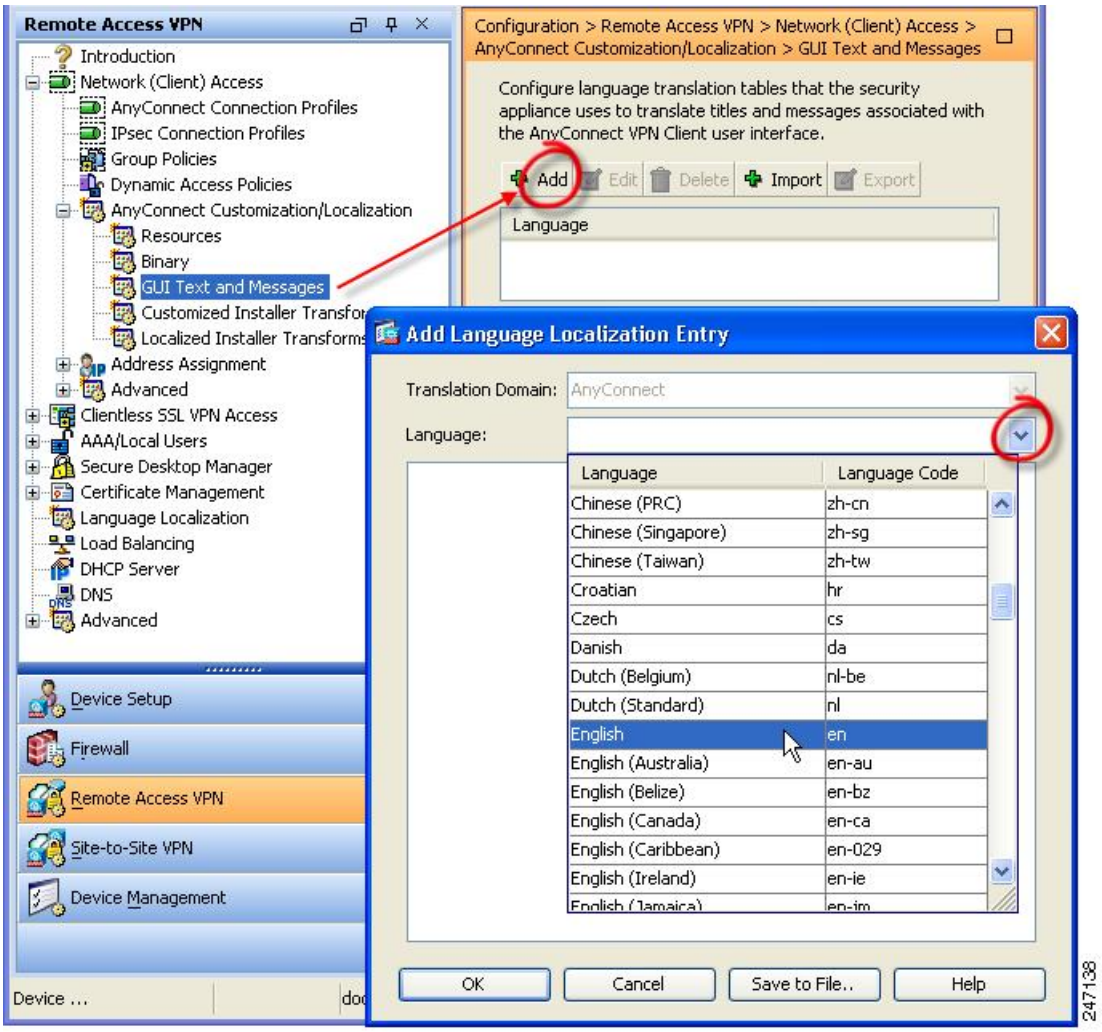
영어 변환 테이블을 추가하거나 편집하고 하나 이상의 메시지 ID에 대한 메시지 텍스트를 변경하여 AnyConnect GUI에 표시되는 영어 메시지를 변경할 수 있습니다. 메시지 파일을 열어본 이후에는 다음과 같이 파일을 편집할 수 있습니다.

- 열린 대화 상자에서 텍스트에 변경사항을 입력합니다.
- 열린 대화 상자에서 텍스트를 텍스트 편집기에 복사하고 변경을 수행한 다음 이 텍스트를 대화 상자에 다시 붙여 넣습니다.
- Save to File(파일에 저장)을 클릭하여 메시지 파일을 내보내고 파일을 편집한 후 ASDM으로 다시 가져옵니다.

프로시저

단계 **1** ASDM에서 **Configuration(**구성**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**)** > **AnyConnect Customization/Localization(AnyConnect** 사용자 정의/현지화**)** > **GUI Text and Messages(GUI** 텍스트 및 메시지**)**로 이동합니다.

단계 **2** **ADD(**추가**)**를 클릭합니다. Add Language Localization Entry(언어 현지화 항목 추가) 창이 표시됩니다.

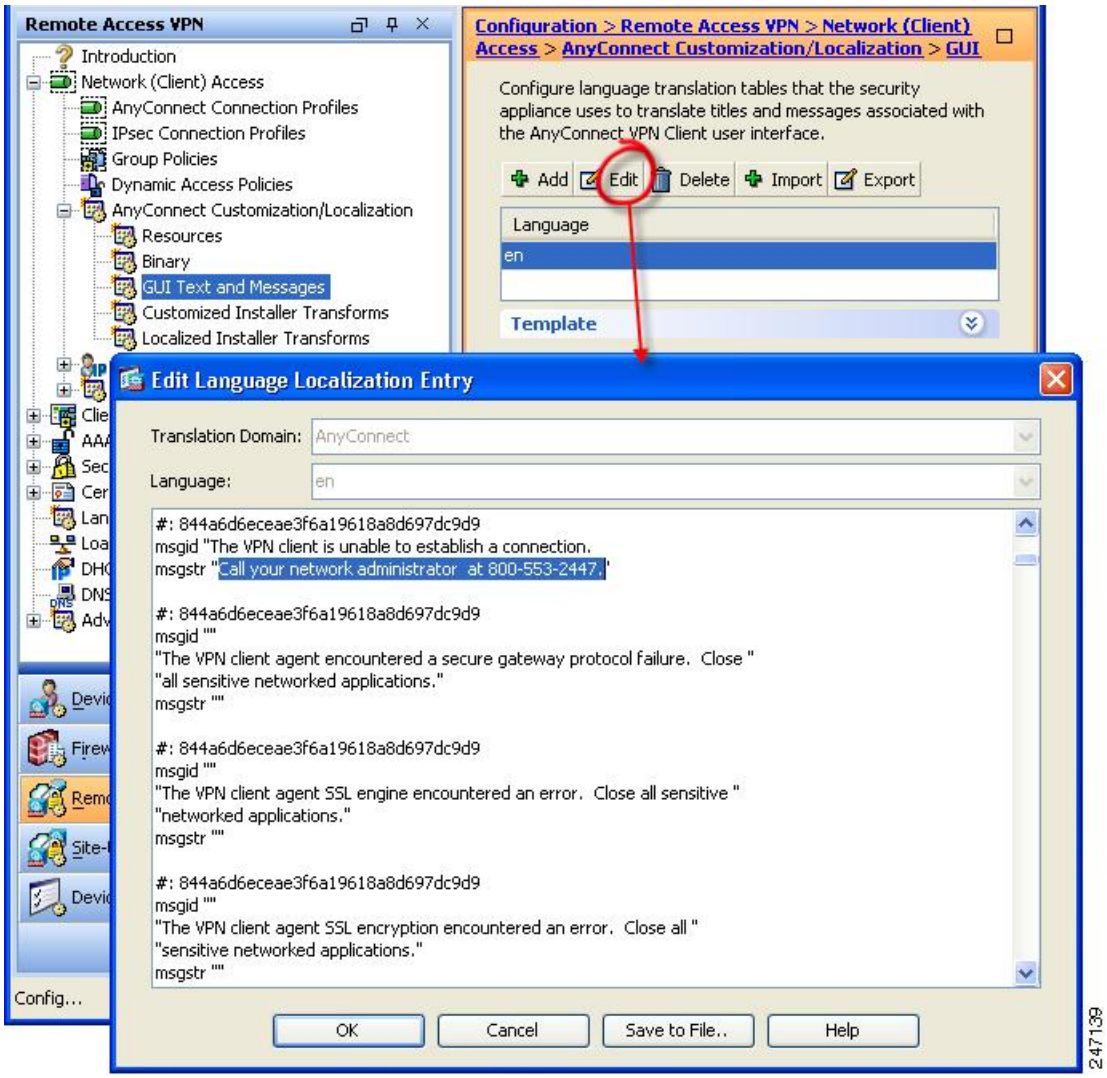


단계 **3** 언어 드롭다운 목록을 클릭하고 영어로 언어를 지정합니다. 창의 언어 목록에서 영어에 대한 변환 테이블이 표시됩니다.

단계 **4** **Edit(**편집**)**을 클릭하여 메시지 편집을 시작합니다.

Edit Language Localization Entry(언어 현지화 항목 편집) 창이 표시됩니다. msgid의 따옴표 사이에 있는 텍스트는 클라이언트에서 표시한 기본 영어 텍스트이며 변경해서는 안 됩니다. msgstr 문자열에는 msgid에 있는 기본 텍스트를 대체하기 위해 클라이언트에서 사용하는 텍스트가 포함되어 있습니다. msgstr의 따옴표 사이에 고유한 텍스트를 입력하십시오.

아래 예에서 "Call your network administrator at 800-553-2447(800-553-2447로 네트워크 관리자에게 문의하십시오)"을 입력했습니다.



단계 **5** **OK**(확인)를 클릭한 다음 **Apply**(적용)를 클릭하여 변경사항을 저장합니다.

Adaptive Security Appliance에 변환 테이블 가져오기

프로시저

단계 **1** www.cisco.com에서 원하는 변환 테이블을 다운로드하십시오.

단계 **2** ASDM에서 **Configuration**(구성) > **Remote Access VPN**(원격 액세스 VPN) > **Network (Client) Access**(네트워크(클라이언트) 액세스) > **AnyConnect Customization/Localization**(AnyConnect 사용자 정의/현지화) > **GUI Text and Messages**(GUI 텍스트 및 메시지)로 이동합니다.

단계 **3** **Import(**가져오기**)**를 클릭합니다. Import Language Localization Entry(언어 현지화 항목 가져오기) 창이 표시됩니다.

단계 **4** 드롭다운 목록에서 적절한 언어를 선택하십시오.

단계 **5** 변환 테이블을 어디에서 가져올지 지정하십시오.

단계 **6** **Import Now(**지금 가져오기**)**를 클릭하십시오. 이 변환 테이블은 해당 기본 설정 언어로 AnyConnect 클라이언트에 구축됩니다. 현지화는 AnyConnect 재시작 및 연결 후 적용됩니다.

참고 모바일 이외의 디바이스에서 실행되는 AnyConnect의 경우, Cisco Secure Desktop을 사용하지 않더라도 Cisco Secure Desktop 변환 테이블을 현지화할 Host Scan 메시지에 대한 Adaptive Security Appliance에 가져와야 합니다.

엔터프라이즈 구축용 메시지 카탈로그 생성

ASA를 사용하여 클라이언트를 구축하지 않으며 Altiris Agent와 같은 엔터프라이즈 소프트웨어 구축 시스템을 사용하는 경우, AnyConnect 변환 테이블을 Gettext와 같은 유틸리티를 사용하여 메시지 카탈로그로 수동으로 변환할 수 있습니다. .po 파일에서 .mo 파일로 테이블을 변환한 후 클라이언트 컴퓨터의 적절한 폴더에 파일을 배치합니다.

참고 GetText와 PoeEdit는 서드파티 소프트웨어 애플리케이션입니다. AnyConnect GUI 맞춤화에 권장되는 방법은 ASA에서 기본 .mo 파일을 가져온 다음 클라이언트로의 구축에 필요한 대로 편집하는 것입니다. 기본 .mo를 사용하는 경우 GetText, PoeEdit 등의 서드파티 애플리케이션에서 발생하는 변환 문제 가능성을 방지할 수 있습니다.

Gettext는 GNU 프로젝트의 유틸리티이며 명령 창에서 실행됩니다. 자세한 내용은 GNU 웹사이트(gnu.org)를 참조하십시오. 또한 Poedit와 같이 Gettext를 사용하는 GUI 기반 유틸리티를 사용할 수 있습니다. 이 소프트웨어는 poedit.net에서 제공됩니다. 다음 절차를 통해 Gettext를 사용하여 메시지 카탈로그를 생성합니다.

AnyConnect 메시지 템플릿 디렉토리

AnyConnect 메시지 템플릿은 각 운영 체제별로 아래에 나열된 폴더에 있습니다.

참고 `\l10n` 디렉토리는 아래에 나열된 각 디렉토리 경로의 일부입니다. 이 디렉토리 이름의 철자는 소문자 l("el"), 1, 0, 소문자 n입니다.

- Windows의 경우 — `<DriveLetter>:\Program Data\Cisco\Cisco AnyConnect Secure Mobility Client\l10n\<LANGUAGE-CODE>\LC_MESSAGES`
- macOS 및 Linux의 경우 - `/opt/cisco/anyconnect/l10n/<LANGUAGE-CODE>/LC_MESSAGES`

프로시저

단계 1 http://www.gnu.org/software/gettext/에서 Gettext 유틸리티를 다운로드하고 관리(원격 사용자 컴퓨터 제외)용으로 사용하는 컴퓨터에 Gettext를 설치합니다.

단계 2 AnyConnect가 설치된 컴퓨터에서 AnyConnect 메시지 템플릿인 AnyConnect.po 복사본을 검색합니다.

단계 3 원하는 대로 문자열을 변경하려면 AnyConnect.po 파일(notepad.exe 또는 일반 텍스트 편집기 사용)을 편집합니다.

단계 4 다음과 같이 .po 파일에서 .mo 파일을 생성하려면 Gettext 메시지 파일 컴파일러를 실행합니다.

msgfmt -o AnyConnect.mo AnyConnect.po

단계 5 사용자 컴퓨터에서 정확한 메시지 템플릿 디렉토리에 .mo 파일의 복사본을 위치시킵니다.

ASA에서 사용자 정의 변환 테이블에 새 메시지 병합

새 사용자 메시지는 AnyConnect의 여러 릴리스에 추가됩니다. 이 새 메시지의 변환을 활성화하기 위해 최신 클라이언트 이미지로 패키지된 변환 템플릿에 새 메시지 문자열이 추가됩니다. 이전 클라이언트에 포함된 템플릿을 기반으로 변환 테이블을 생성한 경우 새 메시지는 원격 사용자에게 자동으로 표시되지 않습니다. 변환 테이블에 새 메시지가 포함되도록 최신 템플릿과 변환 테이블을 병합해야 합니다.

병합을 수행할 수 있는 무료 서드파티 툴이 있습니다. GNU 프로젝트의 Gettext 유틸리티는 Windows에 사용할 수 있으며 명령 창에서 실행합니다. 자세한 내용은 GNU 웹사이트(gnu.org)를 참조하십시오. 또한 Poedit와 같이 Gettext를 사용하는 GUI 기반 유틸리티를 사용할 수 있습니다. 이 소프트웨어는 poedit.net에서 제공됩니다. 두 방법 모두 아래 절차에 나와 있습니다.

참고 이 절차는 이미 ASA에 최신 AnyConnect 이미지 패키지가 로드되어 있다고 가정합니다. 템플릿은 사용자가 수행해야만 내보낼 수 있습니다.

프로시저

단계 1 **Remote Access VPN(**원격 액세스 **VPN)** > **Language Localization(**언어 현지화**)** > **Templates(**템플릿**)**에서 최신 AnyConnect 변환 템플릿을 내보내시기 바랍니다. 템플릿의 파일 이름을 `AnyConnect.pot`로 내보냅니다. 이 파일 이름을 사용하면 msgmerge.exe 프로그램이 파일을 메시지 카탈로그 템플릿으로 인식할 수 있습니다.

단계 2 AnyConnect 템플릿과 변환 테이블을 병합합니다.

Windows용 Gettext 유틸리티를 사용하는 경우 명령 프롬프트 창을 열고 다음 명령을 실행합니다. 명령어는 다음과 같이 AnyConnect 변환 테이블(.po) 및 템플릿(.pot)을 병합하고 새 `AnyConnect_merged.po` 파일을 생성합니다.

```
msgmerge -o AnyConnect_merged.po AnyConnect.po AnyConnect.pot
```

다음의 예는 명령어의 결과를 보여줍니다.

```
C:\Program Files\GnuWin32\bin> msgmerge -o AnyConnect_merged.po AnyConnect.po AnyConnect.pot
..................................... done.
```

Poedit를 사용하는 경우 먼저 AnyConnect.po 파일을 열고 **File(**파일**) > Open(**열기**) > <AnyConnect.po>**로 이동합니다. 그런 다음 템플릿과 병합하고 POT 파일 <AnyConnect.pot>에서 **Catalog(**카탈로그**) > Update(**업데이트**)**로 이동합니다. Poedit에서 새 문자열 및 사용하지 않는 문자열을 모두 포함된 Update Summary(업데이트 요약) 창을 표시합니다. 다음 단계에서 가져올 파일을 저장합니다.

단계 **3** **Remote Access VPN(**원격 액세스 **VPN) > Language Localization(**언어 현지화**)**으로 병합한 변환 테이블을 가져오시기 바랍니다. **Import(**가져오기**)**를 클릭하고 언어를 지정한 후 변환 도메인으로 **AnyConnect**를 선택하시기 바랍니다. `AnyConnect_merged.po`로 가져올 수 있도록 파일을 지정하시기 바랍니다.

클라이언트에서 Windows용 기본 언어 선택

원격 사용자가 ASA에 연결하고 클라이언트를 다운로드하면 AnyConnect는 컴퓨터의 기본 설정 언어를 탐지하고 지정된 시스템 로캘을 탐지하여 적절한 변환 테이블을 적용합니다.

Windows에서 지정된 시스템 로캘을 보거나 변경하려면 다음을 수행하십시오.

프로시저

단계 **1** **Control Panel(**제어판**) > Region and Languages(**지역 및 언어**)** 대화 상자로 이동하십시오. 범주별로 제어판을 보는 경우, **Clock, Language, and Region(**시계**,** 언어 및 지역**) > Change display language(**표시 언어 변경**)**를 선택하십시오.

단계 **2** 언어/로캘 설정을 지정하고 해당 설정을 모든 사용자 계정에 대한 기본값으로 사용하도록 지정합니다.

단계 **3** 웹 보안을 사용하여 구축한 경우, 새 변환을 선택하기 위해 웹 보안 에이전트를 다시 시작하십시오.

참고 위치를 지정하지 않은 경우 AnyConnect가 언어와 같은 기본값으로 지정합니다. 예를 들어 "fr-ca" 디렉토리가 검색되지 않으면 AnyConnect는 "fr" 디렉토리를 확인합니다. 변환 사항을 보기 위해 디스플레이 언어, 위치 또는 키보드를 변경하지 않아도 됩니다.

AnyConnect GUI에 대한 사용자 정의 아이콘 및 로고 생성

본 섹션의 표에는 각 운영 체제에 대해 교체할 수 있는 AnyConnect 파일이 나열되어 있습니다. 표의 이미지는 AnyConnect VPN 클라이언트, Network Access Manager 및 웹 보안 모듈에서 사용됩니다.

제한 사항

- 맞춤형 구성 요소의 파일 이름은 AnyConnect GUI에서 사용되는 파일 이름과 일치해야 합니다. 이 파일 이름은 운영 체제마다 다르며 macOS와 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 프로그램에서 구성 요소를 변경하지 않습니다. 그러나 GUI를 사용자 정의하기 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 정의합니다. 예를 들어 company_logo.bmp를 사용자 정의 이미지로 교체하고 해당 이미지를 삭제할 경우, 클라이언트는 같은 파일 이름을 사용하여 새 이미지(또는 원래 Cisco 로고 이미지)를 가져올 때까지 계속해서 사용자 정의 이미지를 표시합니다.

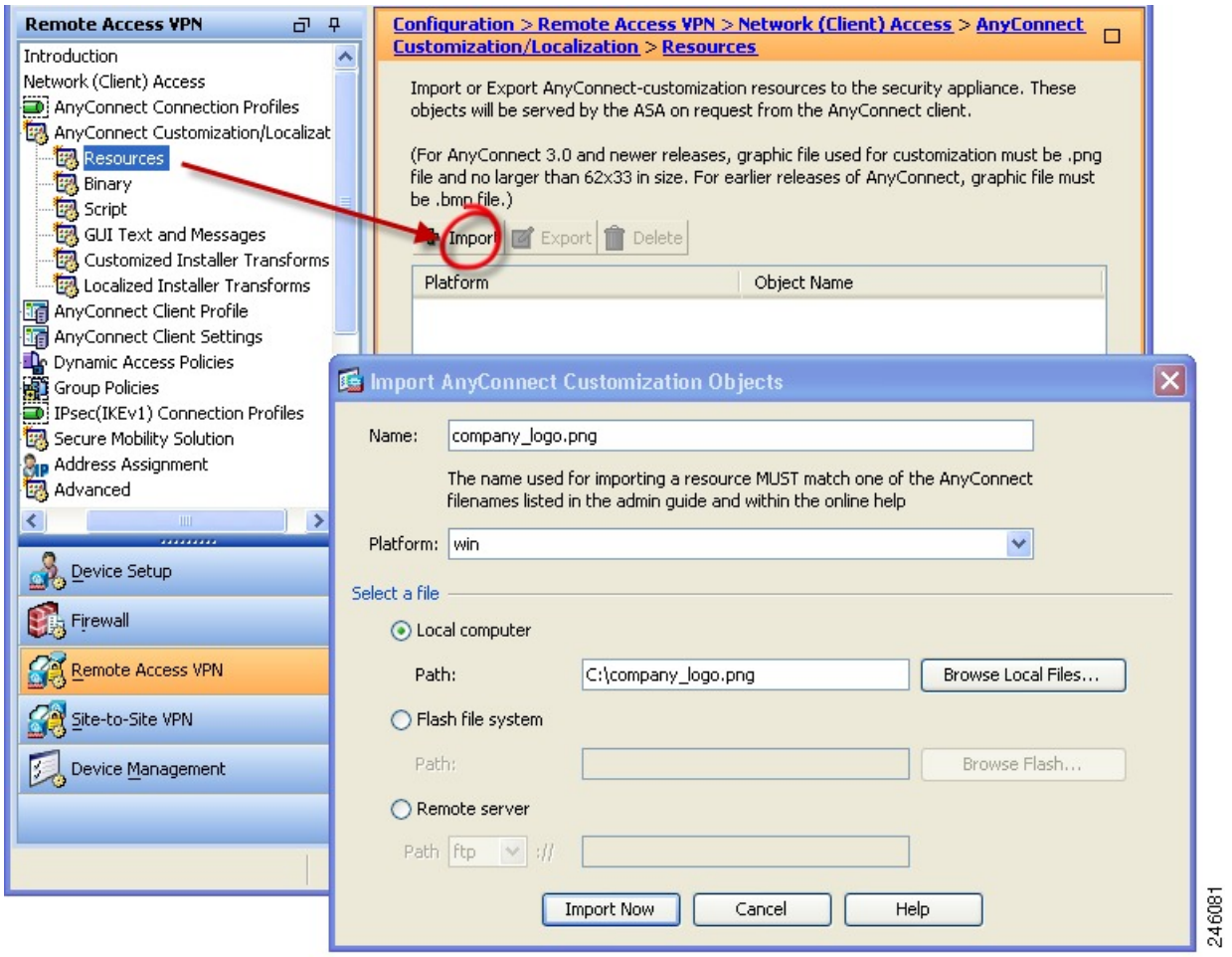
AnyConnect GUI 구성 요소 대체

클라이언트를 사용하여 새 파일을 구축하는 보안 어플라이언스로 사용자 정의 파일을 가져와 AnyConnect를 사용자 정의할 수 있습니다.

프로시저

단계 **1** ASDM에서 **Configuration(**구성**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**)** > **AnyConnect Customization/Localization(AnyConnect** 사용자 정의/현지화**)** > **Resources(**리소스**)**로 이동합니다.

단계 **2** **Import(**가져오기**)**를 클릭합니다. **Import AnyConnect Customization Objects(AnyConnect** 사용자 정의 개체 가져오기**)** 창이 표시됩니다.



단계 **3** 가져올 파일의 이름을 입력하십시오.

단계 **4** 플랫폼을 선택하고 가져올 파일을 지정하십시오. **Import Now(**지금 가져오기**)**를 클릭하십시오. 파일이 개체 목록에 표시됩니다.

Windows용 AnyConnect 아이콘 및 로고

Windows용 모든 파일은 다음 위치에 있습니다.

```
%PROGRAMFILES%\Cisco\Cisco AnyConnect Secure Mobility Client\res\
```

참고 %PROGRAMFILES%는 동일한 이름을 지닌 환경 변수를 가리킵니다. 대부분의 Windows 설치에서 환경 변수는 `C:\Program Files`입니다.

Windows 설치에 있는 파일 이름 및 설명	이미지 크기(픽셀, L x H) 및 유형
about.png Advanced(고급) 대화 상자의 오른쪽 위 모서리에 있는 About(정보) 버튼 크기는 조정할 수 없습니다. 	24 x 24 PNG
about_hover.png Advanced(고급) 대화 상자의 오른쪽 위 모서리에 있는 About(정보) 버튼 크기는 조정할 수 없습니다. 	24 x 24 PNG
app_logo.png 128 x 128이 최대 크기입니다. 사용자 정의 파일이 최대 크기가 아닌 경우, 애플리케이션에서 128 x 128 크기로 조정됩니다. 동일한 비율이 아닌 경우 확대됩니다. 	128 x 128 PNG
attention.ico 주의 또는 상호 작용이 필요한 상황임을 사용자에게 알려주는 시스템 트레이 아이콘 예를 들어 사용자 자격 증명에 대한 대화 상자입니다. 크기는 조정할 수 없습니다. 	16 x 16 ICO

Windows 설치에 있는 파일 이름 및 설명	이미지 크기(픽셀, L x H) 및 유형
company_logo.png 트레이 플라이아웃 및 Advanced(고급) 대화 상자의 왼쪽 위 모서리에 표시되는 기업 로고 97 x 58이 최대 크기입니다. 사용자 정의 파일이 최대 크기가 아닌 경우, 애플리케이션에서 97 x 58 크기로 조정됩니다. 동일한 비율이 아닌 경우 확대됩니다. 	97 x 58(최대) PNG
company_logo_alt.png About(정보) 대화 상자의 오른쪽 아래 모서리에 표시되는 기업 로고 97 x 58이 최대 크기입니다. 사용자 정의 파일이 최대 크기가 아닌 경우, 애플리케이션에서 97 x 58 크기로 조정됩니다. 동일한 비율이 아닌 경우 확대됩니다. 	97 Xx58 PNG
cues_bg.jpg 트레이 플라이아웃, Advanced(고급) 창 및 About(정보) 대화 상자의 배경 이미지 이미지가 확대되지 않으므로 너무 작은 대체 이미지를 사용하면 화면이 검은색으로 표시됩니다. 	1260 x 1024 JPEG
error.ico 하나 이상의 구성 요소로 인해 심각한 오류가 발생한 경우 이를 사용자에게 알리는 시스템 트레이 아이콘 크기는 조정할 수 없습니다. 	16 x 16 ICO

Windows 설치에 있는 파일 이름 및 설명	이미지 크기(픽셀, L x H) 및 유형
neutral.ico 클라이언트 구성 요소가 올바르게 작동 중임을 나타내는 시스템 트레이 아이콘 크기는 조정할 수 없습니다. 	16 x 16 ICO
transition_1.ico 하나 이상의 클라이언트 구성 요소가 상태(예: VPN이 연결 중이거나 Network Access Manager가 연결 중인 경우) 간에 전환 중임을 표시하는 transition_2.ico 및 transition_3.ico와 함께 표시되는 시스템 트레이 아이콘. 3개의 아이콘 파일이 연속해서 표시되며 왼쪽에서 오른쪽으로 바운드되는 하나의 아이콘으로 나타납니다. 크기는 조정할 수 없습니다. 	16 x 16 ICO
transition_2.ico 하나 이상의 클라이언트 구성 요소가 상태(예: VPN이 연결 중이거나 Network Access Manager가 연결 중인 경우) 간에 전환 중임을 표시하는 transition_1.ico 및 transition_3.ico와 함께 표시되는 시스템 트레이 아이콘. 3개의 아이콘 파일이 연속해서 표시되며 왼쪽에서 오른쪽으로 바운드되는 하나의 아이콘으로 나타납니다. 크기는 조정할 수 없습니다. 	16 x 16 ICO
transition_3.ico 하나 이상의 클라이언트 구성 요소가 상태(예: VPN이 연결 중이거나 Network Access Manager가 연결 중인 경우) 간에 전환 중임을 표시하는 transition_1.ico 및 transition_2.ico와 함께 표시되는 시스템 트레이 아이콘. 3개의 아이콘 파일이 연속해서 표시되며 왼쪽에서 오른쪽으로 바운드되는 하나의 아이콘으로 나타납니다. 크기는 조정할 수 없습니다. 	16 x 16 ICO

Windows 설치에 있는 파일 이름 및 설명	이미지 크기(픽셀, **L x H**) 및 유형
vpn_connected.ico VPN이 연결되었음을 나타내는 시스템 트레이 아이콘 크기는 조정할 수 없습니다. 	16 x 16 ICO

Linux용 AnyConnect 아이콘 및 로고

Linux용 모든 파일이 다음 위치에 있습니다.

`/opt/cisco/anyconnect/pixmaps/`

다음 표에는 교체할 수 있는 파일 및 영향을 받는 클라이언트 GUI 영역이 나열되어 있습니다.

Linux 설치에 있는 파일 이름 및 설명	이미지 크기(픽셀, **L x H**) 및 유형
company-logo.png 사용자 인터페이스의 각 탭에 나타나는 기업 로고 AnyConnect 3.0 이상에서는 62 x 33픽셀보다 큰 PNG 이미지를 사용합니다. 	142 x 92 PNG
cvc-about.png About(정보) 탭에 나타나는 아이콘 	16 x 16 PNG
cvc-connect.png Connect(연결) 버튼 옆 및 Connect(연결) 탭에 나타나는 아이콘 	16 x 16 PNG
cvc-disconnect.png Disconnect(연결 끊기) 버튼 옆에 나타나는 아이콘 	16 x 16 PNG

Linux 설치에 있는 파일 이름 및 설명	이미지 크기(픽셀, L x H) 및 유형
cvc-info.png Statistics(통계) 탭에 나타나는 아이콘 	16 x 16 PNG
systray_connected.png 클라이언트가 연결될 때 표시되는 트레이 아이콘 	16 x 16 PNG
systray_notconnected.png 클라이언트가 연결되지 않을 때 표시되는 트레이 아이콘 	16 x 16 PNG
systray_disconnecting.png 클라이언트의 연결이 끊길 때 표시되는 트레이 아이콘 	16 x 16 PNG
systray_quarantined.png 클라이언트가 격리되었을 때 표시되는 트레이 아이콘 	16 x 16 PNG
systray_reconnecting.png 클라이언트가 다시 연결될 때 표시되는 트레이 아이콘 	16 x 16 PNG
vpnui48.png 기본 프로그램 아이콘 	48 x 48 PNG

macOS용 AnyConnect 아이콘 및 로고

macOS용 모든 파일은 다음 위치에 있습니다.

/Cisco AnyConnect Secure Mobility Client/Contents/Resources

다음 표에는 교체할 수 있는 파일 및 영향을 받는 클라이언트 GUI 영역이 나열되어 있습니다.

macOS 설치에 있는 파일 이름 및 설명	이미지 크기(픽셀, **L x H**)
bubble.png 클라이언트에 연결하거나 연결을 끊을 때 나타나는 알림 풍선 	142 x 92 PNG
logo.png 오른쪽 상단 모서리의 기본 화면에 나타나는 로고 아이콘 	50 x 33 PNG
vpngui.icns 모든 아이콘 서비스(도크, 시트 및 파인더 등)에 사용되는 macOS 아이콘 파일 형식 	128 x 128 ICNS
macOS 상태 아이콘 	16 x 16 PNG

AnyConnect 클라이언트 도움말 파일 생성 및 업로드

AnyConnect 사용자에게 도움말을 제공하려면 사이트에 대한 지침이 포함된 도움말 파일을 생성하고 Adaptive Security Appliance에 로드하십시오. 사용자가 AnyConnect에 연결할 때 AnyConnect는 이 도움말 파일을 다운로드하여 AnyConnect 사용자 인터페이스에서 도움말 아이콘을 표시합니다. 사용자가 도움말 아이콘을 클릭하면 브라우저에서 도움말 파일이 열립니다. PDF와 HTML 파일이 지원됩니다.

프로시저

단계 **1** 이름이 `help_AnyConnect.html`인 HTML 파일을 생성하십시오.

단계 2 ASDM에서 **Configuration(**구성**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**)** > **AnyConnect Customization/Localization(AnyConnect** 사용자 지정/현지화**)** > **Binary(**이진 파일**)**로 이동합니다.

단계 3 **help_AnyConnect.xxx** 파일을 가져옵니다. 지원되는 형식은 PDF, HTML, HTM 및 MHT입니다.

단계 4 PC에서 AnyConnect를 불러오고 Adaptive Security Applicance에 연결합니다. 도움말 파일이 클라이언트 PC에 다운로드됩니다.
도움말 아이콘이 UI에 자동으로 추가되었는지 확인해야 합니다.

단계 5 브라우저에서 도움말 파일을 열려면 도움말 아이콘을 클릭합니다.

도움말 아이콘이 나타나지 않으면 도움말 디렉토리를 선택하여 AnyConnect 다운로더에서 이 도움말 파일을 검색할 수 있는지 확인합니다.

파일 이름의 "help_" 부분이 다운로더에서 제거되므로 운영 체제별로 다음의 디렉토리에서 AnyConnect.html을 확인해야 합니다.

- Windows —`C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Help`
- macOS - `/opt/cisco/anyconnect/help`

스크립트 작성 및 구축

AnyConnect를 통해 다음 이벤트가 발생하는 경우 스크립트를 다운로드 및 실행할 수 있습니다.

- 보안 어플라이언스를 사용하여 새 클라이언트 VPN 세션 설정 시 파일 이름 접두사가 필요하므로 *OnConnect* 스크립트로 이 이벤트에서 트리거하는 스크립트를 참조합니다.
- 보안 어플라이언스를 사용하여 클라이언트 VPN 세션 해제 시 파일 이름 접두사가 필요하므로 *OnDisconnect* 스크립트로 이 이벤트에서 트리거하는 스크립트를 참조합니다.

신뢰할 수 있는 네트워크 탐지에서 시작된 새 클라이언트 VPN 세션의 설정에서 OnConnect 스크립트(스크립트 실행을 위한 요건이 충족되었다고 가정)를 트리거하지만, 네트워크 중단 이후 지속적인 VPN 세션의 재연결 시에는 OnConnect 스크립트가 트리거되지 않습니다.

이 기능을 사용하는 방식을 보여주는 몇 가지 예는 다음과 같습니다.

- VPN 연결 시 그룹 정책 새로 고치기
- VPN 연결 시 네트워크 드라이브 매핑 및 연결을 끊은 후 매핑 취소
- VPN 연결 시 서비스에 로그온 및 연결을 끊은 후 로그오프

AnyConnect는 WebLaunch 및 독립 실행형 시작 중 시작되는 스크립트를 지원합니다.

이러한 지침에서는 스크립트를 테스트하기 위해 대상 엔드포인트의 명령행에서 스크립트를 작성 및 실행하는 방법을 사용자가 알고 있다고 가정합니다.

참고 AnyConnect 소프트웨어 다운로드 사이트에서 몇 가지의 스크립트 예제를 제공하며 이를 검토할 경우 단순한 예제라는 점을 기억하십시오. 이 예제들은 실행에 필요한 로컬 컴퓨터 요건을 충족하지 않으며 네트워크 및 사용자 요구에 대해 사용자 정의하지 않으면 사용할 가능성이 거의 없습니다. Cisco는 예제 스크립트 또는 고객 작성 스크립트를 지원하지 않습니다.

스크립팅 요건 및 한계

스크립트에 대한 다음의 요건 및 한계에 유의해야 합니다.

- 지원되는 스크립트 수 — AnyConnect는 각각 하나의 OnConnect 및 OnDisconnect 스크립트만 실행하지만 이러한 스크립트는 다른 스크립트를 시작할 수 있습니다.
- 파일 형식 — AnyConnect는 파일 이름별로 OnConnect 및 onDisconnect 스크립트를 식별합니다. 파일 확장명에 관계없이 이름이 OnConnect 또는 OnDisconnect로 시작하는 파일을 검색합니다. 접두사가 일치하는 첫 번째 스크립트가 실행됩니다. 해석된 스크립트(예: VBS, Perl 또는 Bash) 또는 실행 파일을 인식합니다.
- 스크립트 언어 — 클라이언트는 스크립트를 특정한 언어로 작성하도록 요청하지 않지만 클라이언트 컴퓨터에 설치할 스크립트를 실행할 수 있는 애플리케이션이 필요합니다. 따라서 클라이언트가 스크립트를 시작할 경우, 이 스크립트를 명령행에서 실행할 수 있어야 합니다.
- Windows 보안 환경에서 스크립트 제한 — Microsoft Windows에서 AnyConnect는 사용자가 Windows에 로그온하고 VPN 세션을 설정한 이후 스크립트를 시작만 할 수 있습니다. 따라서, 사용자 보안 환경의 제한이 이러한 스크립트에 적용되며 스크립트는 사용자에게 호출 권한이 있는 함수를 실행만 할 수 있습니다. AnyConnect는 Windows에서 스크립트 실행 중에 cmd 창을 숨깁니다. 따라서 테스트용으로 .bat 파일에서 메시지를 표시하기 위해 스크립트를 실행해도 작동하지 않습니다.
- 스크립트 활성화 — 기본적으로 클라이언트가 스크립트를 시작하지 않습니다. 스크립트를 활성화하려면 AnyConnect 프로파일인 EnableScripting 매개변수를 사용합니다. 이 경우 클라이언트는 스크립트가 필요하지 않습니다.
- 클라이언트 GUI 종료 — 클라이언트 GUI 종료 시 VPN 세션이 반드시 종료되지는 않으며 OnDisconnect 스크립트가 세션 종료 후에 실행됩니다.
- 64비트 Windows에서 스크립트 실행 — AnyConnect 클라이언트는 32비트 애플리케이션입니다. 64비트 Windows 버전에서 실행 중인 경우, cmd.exe의 32비트 버전을 사용합니다.

  32비트 cmd.exe에는 64비트 cmd.exe가 지원하는 일부 명령이 없으므로 지원되지 않는 명령을 실행하거나 부분적으로 실행 및 중지를 시도할 때 일부 스크립트에서 실행이 중지될 수 있습니다. 예를 들어 64비트 cmd.exe에서 지원되는 msg 명령은 Windows 7의 32비트 버전(%WINDIR%\SysWOW64에서 검색)에서는 파악되지 않을 수 있습니다.

  따라서 스크립트를 생성할 때 32비트 cmd.exe에서 지원하는 명령을 사용하십시오.

스크립트 작성, 테스트 및 구축

대상 운영 체제에서 스크립트를 작성하고 테스트합니다. 스크립트를 네이티브 운영 체제의 커맨드 라인에서 제대로 실행할 수 없는 경우 AnyConnect도 제대로 실행할 수 없습니다.

프로시저

단계 **1** 스크립트를 작성하고 테스트하십시오.

단계 **2** 다음에서 스크립트 구축 방법을 선택하십시오.

- 스크립트를 이진 파일로 ASA에 가져오는 ASDM을 사용합니다.

  Network (Client) Access(네트워크**(**클라이언트**)** 액세스**) > AnyConnect Customization/Localization(AnyConnect** 사용자 지정/현지화**) > Script(**스크립트**)**로 이동합니다.

  ASDM 버전 6.3 이상을 사용하는 경우, ASA는 파일 이름에 접두사 scripts_ 및 접두사 OnConnect 또는 OnDisconnect를 추가하여 파일을 스크립트로 확인합니다. 클라이언트가 연결되면 보안 어플라이언스는 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 보안 어플라이언스에 나타납니다. 원격 컴퓨터에서는 스크립트가 OnConnect_myscript.bat로 나타납니다.

  6.3 이전 버전의 ASDM을 사용하는 경우, 다음 접두사가 있는 스크립트를 가져와야 합니다.

  - scripts_OnConnect
  - scripts_OnDisconnect

    스크립트를 안정적으로 실행하려면 동일한 스크립트를 구축하도록 모든 ASA를 구성합니다. 스크립트를 수정하거나 교체할 경우 이전 버전과 동일한 이름을 사용하고 사용자가 연결할 수 있는 모든 ASA에 교체 스크립트를 할당합니다. 사용자가 연결하면 새로운 스크립트가 동일한 이름으로 스크립트를 덮어씁니다.

- 엔터프라이즈 소프트웨어 구축 시스템을 사용하여 VPN 엔드포인트에 스크립트를 수동으로 구축합니다.

  이 방법을 사용하는 경우 아래 스크립트 파일 이름 접두사를 사용합니다.

  - OnConnect
  - OnDisconnect

    다음 디렉토리에서 스크립트를 설치합니다.

    표 ***6:*** 필수 스크립트 위치

OS	Directory
Microsoft Windows	%ALLUSERSPROFILE%\Cisco\Cisco AnyConnect Secure Mobility Client\Script

OS	Directory
Linux (Linux에서 사용자, 그룹 및 기타 파일에 대한 실행 권한을 할당)	/opt/cisco/anyconnect
macOS	/opt/cisco/anyconnect/script

스크립팅을 위해 AnyConnect 프로파일 구성

프로시저

단계 1 VPN 프로파일 편집기를 열고 탐색 창에서 **Preferences(Part 2)(**환경 설정**(2**부**))** 를 선택합니다.

단계 2 **Enable Scripting(**스크립팅 활성화**)**을 선택하십시오. 클라이언트는 VPN 연결을 연결 또는 연결 끊기 할 때 스크립트를 시작합니다.

단계 3 사용자가 On Connect 및 OnDisconnect 스크립트 실행을 활성화 또는 비활성화하도록 설정하려면 **User Controllable(**사용자 제어 가능**)** 을 선택합니다.

단계 4 다른 스크립트 가능 이벤트로 전환이 발생하는 경우 실행 중인 스크립트 프로세스를 종료하도록 클라이언트를 활성화하려면 **Terminate Script On Next Event(**다음 이벤트에서 스크립트 종료**)** 를 선택합니다. 예를 들어 클라이언트는 VPN 세션이 종료된 경우 실행 중인 On Connect를 종료하며 AnyConnect가 새 VPN 세션을 시작하는 경우 실행 중인 OnDisconnect 스크립트를 종료합니다. Microsoft Windows에서 클라이언트는 On Connect 또는 OnDisconnect 스크립트가 시작한 스크립트와 해당 스크립트의 하위 스크립트도 모두 종료합니다. macOS 및 Linux에서는 클라이언트가 On Connect 또는 OnDisconnect 스크립트만 종료하며 하위 스크립트는 종료하지 않습니다.

단계 5 SBL이 VPN 세션을 설정하는 경우 클라이언트가 On Connect 스크립트를 시작하도록 하려면 **Enable Post SBL On Connect Script(**사후 **SBL On Connect** 스크립트 활성화**)** 를 선택합니다.

참고 클라이언트 프로파일을 VPN 엔드포인트로 다운로드하려면 ASA 그룹 정책에 클라이언트 프로파일을 추가해야 합니다.

스크립트 문제 해결

스크립트가 실행되지 않으면 다음과 같이 문제를 해결합니다.

프로시저

단계 1 스크립트에 `OnConnect` 또는 `OnDisconnect` 접두사 이름이 있는지 확인하십시오. 스크립트 작성, 테스트 및 구축 은 각 운영 체제에 필요한 스크립트 디렉토리를 표시합니다.

단계 2 명령행에서 스크립트를 실행해보십시오. 클라이언트가 명령행에서 실행할 수 없는 경우 해당 스크립트를 실행할 수 없습니다. 스크립트가 명령행에서 실행되지 않는 경우, 스크립트를 실행하는 애플리케이션이 설치되어 있는지 확인하고 해당 운영 체제에 스크립트를 다시 작성하도록 시도하십시오.

단계 3 VPN 엔드포인트의 스크립트 디렉토리에 OnConnect 스크립트와 OnDisconnect 스크립트가 각각 1개씩만 있는지 확인하십시오. 클라이언트가 ASA에서 OnConnect 스크립트를 다운로드한 후 다른 ASA에서 다른 파일 이름 접미사를 사용하여 두 번째 OnConnect 스크립트를 다운로드하는 경우, 클라이언트는 원하는 스크립트를 실행하지 못할 수 있습니다. 스크립트 경로가 2개 이상의 OnConnect 또는 OnDisconnect 스크립트를 포함하고 스크립트를 구축하기 위해 ASA를 사용하는 경우, 스크립트 디렉토리의 콘텐츠를 제거하고 VPN 세션을 다시 설정하십시오. 스크립트 경로가 2개 이상의 OnConnect 또는 OnDisconnect 스크립트를 포함하고 수동 구축 방법을 사용하고 있는 경우, 원치 않는 스크립트를 제거하고 VPN 세션을 다시 설정하십시오.

단계 4 운영 체제가 Linux인 경우 스크립트 파일 권한이 실행하도록 설정되어 있는지 확인하십시오.

단계 5 클라이언트 프로파일에 활성화된 스크립팅이 있는지 확인하십시오.

AnyConnect API로 사용자 정의 애플리케이션 작성 및 구축

Windows, Linux 및 macOS 컴퓨터를 사용하는 경우, AnyConnect API로 실행 가능한 고유 UI(User Interface)를 개발할 수 있습니다. AnyConnect 이진 파일을 교체하여 UI를 구축합니다.

다음 표에는 다른 운영 체제용 클라이언트 실행 파일의 파일 이름이 나열되어 있습니다.

클라이언트 **OS**	클라이언트 **GUI** 파일	클라이언트 **CLI** 파일
Windows	vpnui.exe	vpncli.exe
Linux	vpnui	vpn
macOS	ASA 구축에서 지원되지 않습니다. 그러나 Altiris 에이전트와 같은 다른 방법을 사용하여 클라이언트 GUI를 교체하는 Mac용으로 실행 파일을 구축할 수 있습니다.	vpn

실행 파일은 로고 이미지와 같이 ASA에 가져온 모든 리소스 파일을 호출할 수 있습니다. 고유한 실행 파일을 구축할 경우, 리소스 파일에 어떤 파일 이름이든 사용할 수 있습니다.

제한 사항

- Adaptive Security Appliance에서 업데이트된 AnyConnect 소프트웨어를 구축할 수 없습니다. Adaptive Security Appliance에 AnyConnect 패키지의 업데이트된 버전을 배치하면 AnyConnect 클라이언트는 사용자 정의 UI를 교체하는 업데이트를 다운로드합니다. 사용자 정의 클라이언트 및 관련 AnyConnect 소프트웨어 분배를 관리해야 합니다. ASDM을 사용하면 AnyConnect 클라이언트를 교체하기 위해 이진 파일을 업로드할 수 있지만 이 구축 기능은 사용자 정의 애플리케이션을 사용하는 경우 지원되지 않습니다.
- 웹 보안 또는 Network Access Manager를 구축하는 경우 Cisco AnyConnect Secure Mobility Client GUI를 사용하십시오.
- 로그온 전 시작이 지원되지 않습니다.

AnyConnect CLI 명령 사용

Cisco AnyConnect VPN 클라이언트는 그래픽 사용자 인터페이스(GUI)를 사용하는 대신 클라이언트 명령을 입력하려는 사용자를 위해 CLI(Command Line Interface)를 제공합니다. 다음 섹션에서는 CLI 명령 프롬프트를 실행하는 방법과 CLI를 통해 사용할 수 있는 명령에 대해 설명합니다.

- 클라이언트 CLI 프롬프트 실행, 78 페이지
- 클라이언트 CLI 명령 사용, 78 페이지
- ASA가 세션을 종료할 때 Windows 팝업 메시지 표시 차단, 80 페이지

클라이언트 CLI 프롬프트 실행

CLI 명령 프롬프트를 실행하려면 다음을 수행합니다.

- (Windows) Windows 폴더 C:/Program Files/Cisco/Cisco AnyConnect Secure Mobility Client에서 *vpncli.exe* 파일을 찾은 후에 vpncli.exe를 더블 클릭합니다.
- (Linux 및 macOS) /opt/cisco/anyconnect/bin/ 폴더에서 *vpn* 파일을 찾은 후에 *vpn* 파일을 실행합니다.

클라이언트 CLI 명령 사용

인터랙티브 모드에서 CLI를 실행하면 자체 프롬프트가 제공됩니다. 커맨드 라인을 사용할 수도 있습니다.

- connect *IP address or alias* - 클라이언트가 특정 ASA에 대한 연결을 설정합니다.
- disconnect - 클라이언트가 이전에 설정된 연결을 닫습니다.
- stats - 설정된 연결에 대한 통계를 표시합니다.
- quit - CLI 인터랙티브 모드를 종료합니다.

• exit - CLI 인터랙티브 모드를 종료합니다.

다음 예시에서는 사용자가 커맨드 라인에서 연결을 설정하고 종료하는 방법을 보여 줍니다.

Windows

```
connect 209.165.200.224
```

주소 209.165.200.224를 사용하여 보안 어플라이언스에 대한 연결을 설정합니다. 요청된 호스트에 연결한 후 AnyConnect 클라이언트는 사용자가 속한 그룹을 표시하고 사용자의 사용자 이름과 비밀번호를 입력하라는 메시지를 표시합니다. 선택적 배너가 표시되도록 지정한 경우 사용자는 해당 배너에 응답해야 합니다. 기본 응답은 n(연결 시도를 종료함)입니다. 예를 들면 다음과 같습니다.

```
VPN > connect 209.165.200.224
>>contacting host (209.165.200.224) for login information...
>>Please enter your username and password.
Group: testgroup
Username: testuser
Password: ********
>>notice: Please respond to banner.
VPN>
STOP! Please read. Scheduled system maintenance will occur tonight from 1:00-2:00 AM for
one hour.
The system will not be available during that time.

accept? [y/n] y
>> notice: Authentication succeeded. Checking for updates...
>> state: Connecting
>> notice: Establishing connection to 209.165.200.224.
>> State: Connected
>> notice: VPN session established.
VPN>
```

stats

현재 연결에 대한 통계를 표시합니다. 예를 들면 다음과 같습니다.

```
VPN > stats
[Tunnel information]

Time Connected: 01:17:33
Client Address: 192.168.23.45
Server Address: 209.165.200.224

[Tunnel Details]

Tunneling Mode: All traffic
Protocol: DTLS
Protocol Cipher: RSA_AES_256_SHA1
Protocol Compression: None

[Data Transfer]

Bytes (sent/received): 1950410/23861719
Packets (sent/received): 18346/28851
Bypassed (outbound/inbound): 0/0
Discarded (outbound/inbound): 0/0

[Secure Routes]

Network Subnet
0.0.0.0 0.0.0.0
VPN>
```

disconnect

이전에 설정한 연결을 닫습니다. 예를 들면 다음과 같습니다.

```
VPN > disconnect
>> state: Disconnecting
>> state: Disconnected
>> notice: VPN session ended.
VPN>
```

quit 또는 **exit**

두 명령 중 하나를 사용하여 CLI 인터랙티브 모드를 종료합니다. 예를 들면 다음과 같습니다.

```
quit
goodbye
>>state: Disconnected
```

Linux 또는 **Mac OS X**

```
/opt/cisco/anyconnect/bin/vpn connect 1.2.3.4
```

주소 1.2.3.4를 사용하여 ASA에 대한 연결을 설정합니다.

```
/opt/cisco/anyconnect/bin/vpn connect some_asa_alias
```

프로파일을 읽고 별칭 *some_asa_alias*를 조회하여 해당 주소를 찾는 방식으로 ASA에 대한 연결을 설정합니다.

```
/opt/cisco/anyconnect/bin/vpn stats
```

vpn 연결에 대한 통계를 표시합니다.

```
/opt/cisco/anyconnect/bin/vpn disconnect
```

vpn 세션이 있으면 연결을 끊습니다.

ASA가 세션을 종료할 때 Windows 팝업 메시지 표시 차단

ASA에서 세션 재설정을 실행하여 AnyConnect 세션을 종료하면 엔드 유저에게 다음 Windows 팝업 메시지가 표시됩니다.

```
The secure gateway has terminated the vpn connection. The following message was received
for the gateway: Administrator Reset
```

CLI 명령을 사용하여 VPN 터널을 시작하는 등의 경우에는 이 메시지를 표시하지 않을 수 있습니다. 클라이언트가 연결된 후 클라이언트 CLI를 재시작하면 이 메시지가 표시되지 않도록 할 수 있습니다. 다음 예시에는 이렇게 하는 경우의 CLI 출력이 나와 있습니다.

```
C:/Program Files (x86)\Cisco\Cisco AnyConnect Secure Mobility Client>vpncli
Cisco AnyConnect Secure Mobility Client (version 4.x).
Copyright (c) 2016 Cisco Systems, Inc.
All Rights Reserved.
>> state: Connected
>> state: Connected
>> notice: Connected to asa.cisco.com.
>> notice: Connected to asa.cisco.com.
>> registered with local VPN subsystem.
>> state: Connected
>> notice: Connected to asa.cisco.com.
>> state: Disconnecting
>> notice: Disconnect in progress, please wait...
>> state: Disconnected
```

```
>> notice: On a trusted network.
>> error: The secure gateway has terminated the VPN connection.
The following message was received from the secure gateway: Administrator Reset
VPN>
```

Windows 레지스트리의 다음 위치에서 엔드포인트 디바이스에 대해 이름이 SuppressModalDialogs인 32비트 double 값을 생성할 수도 있습니다. 클라이언트는 이름은 확인하지만 해당 값은 무시합니다.

- 64비트 Windows:

  HKEY_LOCAL_MACHINE/SOFTWARE\Wow6432Node\Cisco\ Cisco AnyConnect Secure Mobility Client

- 32비트 Windows:

  HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\Cisco AnyConnect Secure Mobility Client

ISE 구축용 AnyConnect 사용자 정의 및 현지화 준비

AnyConnect 현지화 번들 준비

AnyConnect 현지화 번들은 AnyConnect 현지화에 사용되는 변환 테이블 파일 및 설치 프로그램 변형 파일을 포함하는 zip 파일입니다. 이 zip 파일은 ISE의 AnyConnect를 사용자에게 구축하는 데 사용되는 ISE AnyConnect 리소스의 일부입니다. 이 zip 파일의 콘텐츠는 이 절차에 설명된 대로 AnyConnect 구축에서 지원하는 언어에 따라 정의됩니다.

시작하기 전에

ISE는 AnyConnect 현지화 번들에서 컴파일된 이진 변환 테이블이 필요합니다. gettext에는 편집에 사용되는 텍스트 .po 형식 및 실행 시간에서 사용되는 컴파일된 이진 .mo 형식으로 두 개의 파일 형식이 있습니다. 컴파일은 gettext 툴 msgfmt에서 수행됩니다. http://www.gnu.org/software/gettext/에서 Gettext 유틸리티를 다운로드하고 관리용 로컬 컴퓨터(원격 사용자 컴퓨터 제외)에 Gettext를 설치하십시오.

프로시저

단계 **1** AnyConnect 구축을 통해 사용되는 변환 테이블 파일을 가져와 준비하십시오.

a) www.cisco.com의 Cisco AnyConnect Secure Mobility Client Software Download(소프트웨어 다운로드) 페이지에서 `AnyConnect-translations-(날짜).zip` 파일을 다운로드하여 엽니다.

   zip 파일은 Cisco에서 제공하는 모든 언어 번역을 위한 *.po 파일을 포함하고 있습니다.

b) (선택 사항) 사용자 환경에 맞게 사용자 정의하거나 생성한 다른 변환 테이블 파일(*.po 파일)을 검색하십시오.

c) gettext 메시지 파일 컴파일러를 실행하여 다음과 같이 사용 중인 각 *.po 파일에서 *.mo 파일을 생성하십시오.

   msgfmt -o AnyConnect.mo AnyConnect.po

단계 **2** AnyConnect 구축을 통해 사용되는 변환 테이블 파일을 조합하십시오.

a) 로컬 컴퓨터의 작업 영역에 l10n 이라는 디렉토리를 생성하십시오.
b) l10n 아래에 포함할 각 언어의 디렉토리를 생성하고 언어 코드로 이름을 지정하십시오.

   예를 들어 프랑스어(캐나다)의 경우 fr-ch 로 지정합니다.

c) 포함할 각 컴파일된 변환 테이블을 적절하게 이름이 지정된 디렉토리에 두십시오.

   컴파일된 변환 테이블에는 *.po 파일을 추가하지 마십시오. 이 파일에는 *.mo 파일만 추가해야 합니다.

디렉토리 구조는 다음과 유사합니다. 아래 구조에서는 프랑스어(캐나다), 히브리어 및 일본어에 대한 변환 테이블을 포함하고 있습니다.

```
l10n\fr-ch\AnyConnect.mo
    \he\AnyConnect.mo
    \ja\AnyConnect.mo
```

단계 **3** (Windows 전용) AnyConnect 구축을 통해 사용되는 변환 테이블 파일을 가져와 준비하십시오.

a) www.cisco.com의 Cisco AnyConnect Secure Mobility Client 소프트웨어 다운로드 페이지에서 구축에 적용되는 언어 현지화 변형 파일을 포함하는 zip 파일을 다운로드하여 엽니다.

   zip 파일 이름은 anyconnect-win-*(버전)*-webdeploy-k9-lang.zip 또는 anyconnect-win-*(버전)*-gina-webdeploy-k9-lang.zip으로 지정됩니다.

   참고 언어 지역화 파일의 버전은 사용자의 환경에서 사용된 AnyConnect의 버전과 일치해야 합니다. AnyConnect의 최신 버전으로 업그레이드할 경우, 현지화 번들에서 사용되는 언어 현지화 파일도 같은 버전으로 업그레이드해야 합니다.

b) 사용자 환경에 맞게 사용자 정의하거나 생성한 언어 현지화 변형 파일을 검색하십시오.

단계 **4** (Windows 전용) AnyConnect 구축을 통해 사용되는 언어 현지화 파일을 조합하십시오.

a) 로컬 컴퓨터의 같은 작업 영역에 mst 라는 디렉토리를 생성하십시오.
b) mst 아래에 포함할 각 언어의 디렉토리를 생성하고 언어 코드로 이름을 지정하십시오.

   예를 들어 프랑스어(캐나다)의 경우 fr-ch 로 지정합니다.

c) 포함할 각 언어 현지화 파일을 적절하게 이름이 지정된 디렉토리에 두십시오.

디렉토리 구조는 다음과 유사합니다.

```
l10n\fr-ch\AnyConnect.mo
    \he\AnyConnect.mo
    \ja\AnyConnect.mo
mst\fr-ch\AnyConnect_fr-ca.mst
   \he\AnyConnect_he.mst
   \ja\AnyConnect_ja.mst
```

단계 **5** 표준 압축 유틸리티를 사용하여 해당 디렉토리 구조를 적절한 이름의 파일 (예:AnyConnect-Localization-Bundle-*(release)*.zip)로 압축해 AnyConnect 현지화 번들을 생성합니다.

다음에 수행할 작업

AnyConnect 현지화 번들을 사용자에게 AnyConnect를 구축하는 데 사용되는 ISE AnyConnect 리소스의 일부로서 ISE에 업로드하십시오.

AnyConnect 사용자 정의 번들 준비

AnyConnect 사용자 정의 번들은 사용자 정의 AnyConnect GUI 리소스, 사용자 정의 도움말 파일, VPN 스크립트 및 설치 프로그램 변형을 포함하는 zip 파일입니다. 이 zip 파일은 ISE의 AnyConnect를 사용자에게 구축하는 데 사용되는 ISE AnyConnect 리소스의 일부입니다. 다음과 같은 디렉토리 구조가 있습니다.

```
win\resource\
   \binary
   \transform
mac-intel\resource
         \binary
         \transform
```

맞춤화된 AnyConnect 구성 요소는 다음과 같이 Windows 및 macOS 플랫폼의 `resource`, `binary` 및 `transform` 하위 디렉터리에 포함되어 있습니다.

- 각 `resource` 하위 디렉토리에는 해당 플랫폼에 대한 모든 사용자 정의 AnyConnect GUI 구성 요소가 포함되어 있습니다.

  이 리소스를 생성하려면 AnyConnect GUI에 대한 사용자 정의 아이콘 및 로고 생성, 64 페이지의 내용을 참조하십시오.

- 각 `binary` 하위 디렉토리에는 해당 플랫폼에 대한 사용자 정의 도움말 파일 및 VPN 스크립트가 포함되어 있습니다.
  - AnyConnect 도움말 파일을 생성하려면 AnyConnect 클라이언트 도움말 파일 생성 및 업로드, 72 페이지의 내용을 참조하십시오.
  - VPN 스크립트를 생성하려면 스크립트 작성 및 구축, 73 페이지의 내용을 참조하십시오.
- 각 `transform` 하위 디렉토리에는 해당 플랫폼에 대한 설치 프로그램 변형이 포함되어 있습니다.
  - Windows 사용자 정의 설치 프로그램 변형을 생성하려면 다음 항목의 내용을 참조하십시오. 설치 동작 수정(Windows), 48 페이지
  - macOS 설치 프로그램 변형을 생성하려면 다음 항목의 내용을 참조하십시오. ACTransforms.xml을 사용하여 macOS에서 설치 프로그램 동작 맞춤화, 55 페이지

시작하기 전에

AnyConnect 사용자 정의 번들을 준비하기 전에 필요한 모든 사용자 정의 구성 요소를 생성하십시오.

프로시저

단계 1 로컬 컴퓨터의 작업 영역에 설명된 디렉토리 구조를 만드십시오.

단계 2 각 플랫폼의 사용자 정의 AnyConnect GUI 파일을 사용하여 `resources` 디렉토리를 채우십시오. 파일의 이름이 모두 적절하게 지정되어 있고 아이콘과 로고가 적절한 크기로 되어 있는지 확인하십시오.

단계 3 사용자 정의 `help_AnyConnect.html` 파일을 사용하여 `binary` 디렉토리를 채우십시오.

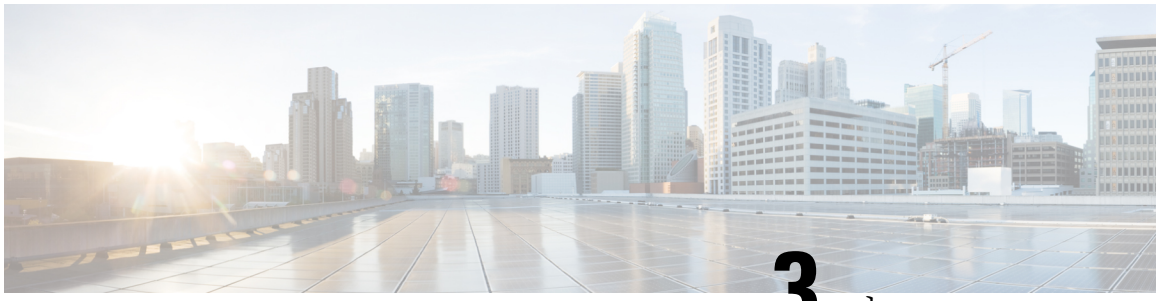
단계 4 VPN `OnConnect`와 `OnDisconnect` 스크립트 및 호출하는 추가 스크립트를 사용하여 `binary` 디렉토리를 채우십시오.

단계 5 플랫폼별 설치 프로그램 변형을 사용하여 `transform` 디렉토리를 채우십시오.

단계 6 표준 압축 유틸리티를 사용하여 해당 디렉토리 구조를 적절한 이름의 파일(예: `AnyConnect-Customization-Bundle.zip`)로 압축해 AnyConnect 사용자 정의 번들을 생성합니다.

다음에 수행할 작업

AnyConnect 사용자 정의 번들을 사용자에게 AnyConnect를 구축하는 데 사용되는 ISE AnyConnect 리소스의 일부로서 ISE에 업로드하십시오.



3 장

AnyConnect 프로파일 편집기

프로파일 편집기 정보

Cisco AnyConnect Secure Mobility Client 소프트웨어 패키지에는 모든 운영 체제용 프로파일 편집기가 포함되어 있습니다. ASA의 AnyConnect 클라이언트 이미지를 로드할 때 ASDM이 프로파일 편집기를 활성화합니다. 로컬 또는 플래시의 클라이언트 프로파일을 업로드할 수 있습니다.

여러 AnyConnect 패키지를 로드하는 경우 ASDM은 가장 최근의 AnyConnect 패키지에서 클라이언트 프로파일 편집기를 활성화합니다. 이러한 접근 방식을 통해 편집기는 로드된 최신 AnyConnect 및 이전 클라이언트에 대한 기능을 표시합니다.

Windows에서 실행되는 독립 실행형 프로파일 편집기도 있습니다.

AnyConnect 프로파일

ASDM에서 새 프로파일 추가

참고 클라이언트 프로파일을 생성하기 전에 먼저 클라이언트 이미지를 업로드해야 합니다.

프로파일은 AnyConnect의 일부로 엔드포인트에서 관리자 정의 최종 사용자 요건 및 인증 정책에 구축되어 있으며 미리 구성된 네트워크 프로파일을 최종 사용자가 사용할 수 있게 설정되어 있습니다. 프로파일 편집기를 사용하여 하나 이상의 프로파일을 생성하고 구성하십시오. AnyConnect에는 ASDM의 일부이며 독립 실행형 Windows 프로그램으로 프로파일 편집기가 포함되어 있습니다.

ASDM에서 새로운 클라이언트 프로파일을 ASA에 추가하려면 다음을 수행하십시오.

프로시저

단계 **1** ASDM을 열고 **Configuration(**구성**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**)** > **AnyConnect Client Profile(AnyConnect** 클라이언트 프로파일**)**을 선택합니다.

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** 프로파일 이름을 입력합니다.

단계 **4** 프로파일 사용 드롭다운 목록에서 프로파일을 생성 중인 대상 모듈을 선택합니다.

단계 **5** Profile Location(프로파일 위치) 필드에서 **Browse Flash(**플래시 찾아보기**)** 를 클릭하고 ASA에서 XML 파일에 대한 디바이스 파일 경로를 선택합니다(선택사항).

단계 **6** 독립 실행형 편집기를 사용하여 프로파일을 생성한 경우 해당 프로파일 정의를 사용하려면 **Upload(**업로드**)** 를 클릭합니다(선택사항).

단계 **7** 드롭다운 목록에서 AnyConnect 그룹 정책을 선택합니다(선택사항).

단계 **8** **OK(**확인**)**를 클릭합니다.

독립형 프로파일 편집기

ASDM에서 프로파일 편집기 외에 Windows용 프로파일 편집기의 독립형 버전을 사용할 수 있습니다. 클라이언트를 사전 구축할 경우, 독립형 프로파일 편집기를 사용하여 사용자가 소프트웨어 관리 시스템을 사용하는 컴퓨터에 구축하는 VPN 서비스 및 기타 모듈용으로 프로파일을 생성합니다.

프로그램 추가/제거를 사용하여 독립형 Cisco AnyConnect 프로파일 편집기 설치를 수정하거나 VPN 또는 기타 프로파일 편집기를 제거할 수 있습니다.

요구 사항

- Java — JRE 1.6.의 최소값은 프로파일 편집기에 대한 필수 구성 요소이지만 관리자가 개별적으로 구축할 수 있습니다.

참고 JRE 1.6은 독립형 프로파일 편집기 제거 시 자동으로 제거되지 않습니다. 사용자가 개별적으로 제거해야 합니다.

- 지원되는 운영 체제 — 이 애플리케이션은 Windows 7에서 테스트되었습니다. MSI만 Windows에서 실행됩니다.
- 지원되는 브라우저 — 이 애플리케이션의 도움말 파일은 Firefox와 Internet Explorer에서 지원됩니다. 다른 브라우저에서는 테스트하지 않았습니다.
- 필수 하드 드라이브 공간 — Cisco AnyConnect 프로파일 편집기 애플리케이션에는 5메가바이트 미만의 하드 드라이브 공간이 필요합니다. JRE 1.6에는 100메가바이트 미만의 하드 드라이브 공간이 필요합니다.
- 첫 번째 연결에서 클라이언트 GUI에 모든 사용자 제어 가능 설정이 표시되도록 VPN 프로파일의 서버 목록에 ASA를 포함해야 합니다. 프로파일에 있는 호스트 항목으로 FQDN 또는 ASA 주소를 추가하지 않은 경우, 필터가 이 세션에 적용되지 않습니다. 예를 들어 인증서 일치를 생성하고 인증서가 기준과 제대로 일치하지만 해당 프로파일에 있는 호스트 항목으로 ASA를 추가하지 않는 경우, 인증서 일치가 무시됩니다.

독립형 AnyConnect 프로파일 편집기 설치

독립형 AnyConnect 프로파일 편집기는 AnyConnect ISO 및 .pkg 파일과는 별도로 Windows msi 실행 파일로 배포되며 명명 규칙은 `anyconnect-profileeditor-win-<version>-k9.msi`입니다.

프로시저

단계 **1** https://software.cisco.com/download/release.html?mdfid=286281283&flowid=72322&softwareid=282364313&release=4.0.00061&relind=AVAILABLE&rellifecycle=&reltype=latest에서 `anyconnect-profileeditor-win-<version>-k9.msi`를 다운로드합니다.

단계 **2** `anyconnect-profileeditor-win-<version>-k9.msi`를 더블 클릭하여 설치 마법사를 실행합니다.

단계 **3** 시작 화면에서 **Next(**다음**)**를 클릭하십시오.

단계 **4** Choose Setup Type(설치 유형 선택) 창에서 다음 버튼 중 하나를 클릭하고 **Next(**다음**)**를 클릭하십시오.

- **Typical(**일반**)** - Network Access Manager 프로파일 편집기만 자동으로 설치합니다.
- **Custom(**맞춤형**)** - 설치할 프로파일 편집기를 선택할 수 있습니다.
- **Complete(**전체**)** - 모든 프로파일 편집기를 자동으로 설치합니다.

단계 **5** 이전 단계에서 **Typical(**일반**)** 또는 **Complete(**전체**)** 를 클릭한 경우 이 단계를 건너뛰고 다음 단계로 이동하십시오. 이전 단계에서 Custom(맞춤형)을 클릭한 경우 설치할 독립형 프로파일 편집기의 아이

콘을 클릭하고 Will be installed on local hard drive(로컬 하드 드라이브에 설치)를 선택하거나, Entire Feature will be unavailable(모든 기능을 사용할 수 없음)을 클릭하여 독립형 프로파일 편집기가 설치되지 않도록 합니다. **Next(**다음**)**를 클릭합니다.

단계 **6** Ready to Install(설치 준비 완료) 화면에서 **Install(**설치**)**을 클릭하십시오.

단계 **7** **Finish(**마침**)**를 클릭합니다.

- 독립형 AnyConnect 프로파일 편집기는 `C:\Program Files\Cisco\Cisco AnyConnect` 프로파일 편집기 디렉터리에 설치됩니다.
- **Start(**시작**)** > **All Programs(**모든 프로그램**)** > **Cisco** > **Cisco AnyConnect Profile Editor(Cisco AnyConnect** 프로파일 편집기**)**를 선택한 다음 하위 메뉴에서 사용할 독립형 프로파일 편집기를 클릭하거나, 바탕 화면에 설치된 적합한 프로파일 편집기의 바로 가기 아이콘을 클릭하여 프로파일 편집기를 실행할 수 있습니다.

독립 실행형 프로파일 편집기를 사용하여 클라이언트 프로파일 편집

보안을 위해 독립 실행형 프로파일 편집기에서만 클라이언트 프로파일 XML 파일을 편집할 수 있습니다. ASA는 독립 실행형 프로파일 편집기에서 편집된 프로파일 XML 파일만 허용합니다.

프로시저

단계 **1** 바탕 화면의 바로 가기 아이콘을 두 번 클릭하거나 **Start(**시작**)** > **All Programs(**모든 프로그램**)** > **Cisco** > **Cisco AnyConnect Profile Editor(Cisco AnyConnect** 프로파일 편집기**)**를 탐색하고 하위 메뉴에서 원하는 프로파일을 선택하여 원하는 프로파일 편집기를 실행하십시오.

단계 **2** **File(**파일**)** > **Open(**열기**)**을 선택하고 수정하려는 클라이언트 프로파일 XML 파일을 탐색하십시오.

실수로 웹 보안과 같은 기능의 클라이언트 프로파일을 VPN과 같은 다른 기능의 프로파일 편집기를 사용하여 열려고 시도한 경우, **Schema Validation failed(**스키마 검증 실패**)** 메시지가 표시되며 프로파일을 편집할 수 없게 됩니다.

실수로 종류가 같은 프로파일 편집기의 인스턴스 2개에서 같은 클라이언트 프로파일을 편집하려고 시도한 경우, 클라이언트 프로파일에 마지막으로 편집된 사항이 저장됩니다.

단계 **3** 프로파일을 변경하고 **File(**파일**)** > **Save(**저장**)**를 선택하여 변경 사항을 저장하십시오.

AnyConnect VPN 프로파일

Cisco AnyConnect Secure Mobility Client 기능은 AnyConnect 프로파일에서 활성화됩니다. 이 프로파일에는 코어 클라이언트 VPN 기능과 선택적인 클라이언트 모듈인 Network Access Manager, ISE Posture, 고객 경험 피드백 및 웹 보안에 대한 구성 설정이 포함되어 있습니다. ASA는 AnyConnect 설치 및 업데이트 시 프로파일을 구축합니다. 사용자는 프로파일을 관리하거나 수정할 수 없습니다.

모든 AnyConnect 사용자와 그룹 정책을 기반으로 하는 사용자에게 전역으로 프로파일을 구축하기 위해 ASA 또는 ISE를 구성할 수 있습니다. 일반적으로 사용자는 설치된 각 AnyConnect 모듈용의 단일 프로파일 파일을 보유하고 있습니다. 경우에 따라 두 개 이상의 VPN 프로파일을 제공할 수 있습니다. 여러 위치에서 업무를 수행하는 사용자는 두 개 이상의 VPN 프로파일이 필요할 수 있습니다.

일부 프로파일 설정은 사용자 환경 설정 파일 또는 전역 환경 설정 파일로 사용자 컴퓨터 로컬에 저장되어 있습니다. 사용자 파일에는 AnyConnect 클라이언트가 클라이언트 GUI의 환경 설정 탭에 있는 사용자 제어 가능 설정 표시 및 최종 연결에 대한 정보 표시에 필요로 하는 사용자, 그룹, 호스트 등의 정보가 포함되어 있습니다.

사용자가 없기 때문에 로그인하기 전에 해당 설정을 적용할 수 있도록 전역 파일에 사용자 제어 가능 설정에 대한 정보가 포함되어 있습니다. 예를 들어 클라이언트는 로그인하기 전에 로그온 전 시작 및/또는 시작 시 AutoConnect 설정이 활성화되어 있는지 알아야 합니다.

AnyConnect 프로파일 편집기, 환경 설정(1부)

- **Use Start Before Logon(**로그온 전 시작 사용**)**—(Windows 전용) Windows 로그인 대화 상자가 나타나기 전에 AnyConnect를 시작하여 Windows에 로그온하기 전에 VPN 연결을 통하여 사용자를 엔터프라이즈 인프라에 연결시킵니다. 인증 이후에 로그인 대화 상자가 나타나며 사용자는 평소와 같이 로그인합니다.
- **Show Pre-connect Message(**사전 연결 메시지 표시**)**—관리자는 사용자가 처음 연결을 시도하기 전에 일회성 메시지가 표시되게 설정할 수 있습니다. 예를 들어, 메시지를 통해 사용자에게 스마트카드를 판독기에 삽입해야 함을 알려줄 수 있습니다. 메시지가 AnyConnect 메시지 카탈로그에 표시되며 현지화됩니다.
- **Certificate Store(**인증서 저장소**)** - AnyConnect에서 어떤 인증서 저장소를 인증서 저장 및 읽기에 사용할지 제어합니다. 인증서 저장소에 따라 보안 게이트웨이를 구성하여 그러면 여러 인증서 인증 조합 중 특정 VPN 연결에 적합한 조합을 클라이언트에 지시해야 합니다.

  VPN 프로파일의 CertificateStore 컨피그레이션 값은 보안 게이트웨이에 적합한 인증서 유형에 따라 달라집니다(사용자 인증서 2개 또는 머신과 사용자 인증서 각각 하나).

  macOS에서 AnyConnect가 액세스할 수 있는 인증서 저장소의 추가 필터링을 허용하려는 경우 Windows 또는 macOS 드롭다운에서 인증서 저장소를 구성할 수 있습니다. macOS의 새로운 프로파일 기본 설정은 CertificateStoreMac이며 아래에 나와 있는 추가된 값을 지원합니다.

  - All(모두)(Windows용) - ASA 컨피그레이션에서 머신 하나와 사용자 인증서 하나가 허용됩니다.
  - User(사용자)(Windows용) - ASA 컨피그레이션에서 용자 인증서 2개가 허용됩니다.
  - All(모두)(macOS용) - 사용 가능한 모든 macOS 키 체인과 파일 저장소의 인증서를 사용합니다.
  - System(시스템)(macOS용) - macOS 시스템 키 체인 및 시스템 파일/PEM 저장소의 인증서만 사용합니다.
  - Login(로그인)(macOS용) - macOS 로그인 및 동적 스마트 카드 키 체인과 사용자 파일/PEM 저장소의 인증서만 사용합니다.

- **Certificate Store Override(**인증서 저장소 재정의**)**—사용자가 자신의 디바이스에 대해 관리자 권한이 없는 경우, 관리자는 AnyConnect가 Windows 머신 인증서 저장소에서 인증서를 검색하도록 지시할 수 있습니다.

  참고 머신 인증서를 사용하여 Windows에 연결하려면 이 옵션을 사용할 수 있는 사전 구축 프로파일이 있어야 합니다. 이 프로파일이 연결 전에 Windows 디바이스에 없는 경우, 인증서는 머신 저장소에서 액세스할 수 없으며 연결에 실패합니다.

  - **True** - AnyConnect가 Windows 머신 인증서 저장소에서 인증서를 검색합니다. CertificateStore가 *all*로 설정되어 있으면 CertificateStoreOverride를 *true*로 설정해야 합니다.
  - **False** - AnyConnect가 Windows 머신 인증서 저장소에서 인증서를 검색하지 않습니다.

- **AutomaticCertSelection** - 보안 게이트웨이에 여러 인증서 인증이 구성되어 있으면 이 값을 **true**로 설정해야 합니다.
- **Auto Connect on Start(**시작 시 자동 연결**)**—AnyConnect를 시작할 때 AnyConnect 프로파일에서 지정한 보안 게이트웨이 또는 클라이언트가 연결된 마지막 게이트웨이에 자동으로 VPN 연결을 설정합니다.
- **Minimize On Connect(**연결 시 최소화**)**—VPN 연결을 설정한 이후에 AnyConnect GUI가 최소화됩니다.
- **Local LAN Access(**로컬 **LAN** 액세스**)**—ASA에 대한 VPN 세션 중에 사용자가 원격 컴퓨터에 연결된 로컬 LAN에 액세스하도록 허용됩니다.

  참고 로컬 LAN 액세스를 사용하면 공용 네트워크에서 사용자 컴퓨터를 통해 기업 네트워크에 잠재적으로 보안 취약점을 유발할 수 있습니다. 또는 기본 그룹 정책에 포함된 AnyConnect 클라이언트 로컬 인쇄 방화벽 규칙을 사용하는 SSL 클라이언트 방화벽을 구축하기 위해 보안 어플라이언스(버전 8.4(1) 이상)를 구성할 수 있습니다. 이 방화벽 규칙을 활성화하려면 자동 VPN 정책, Always-On, 이 편집기에서 VPN 연결 끊기 허용, 기본 설정(2부)도 활성화해야 합니다.

- **Disable Captive Portal Detection(**종속 포털 탐지 비활성화**)** - AnyConnect 클라이언트가 수신하는 인증서의 공통 이름이 ASA 이름과 일치하지 않는 경우 종속 포털을 탐지합니다. 이 동작이 수행되면 사용자에게 인증을 하라는 프롬프트가 표시됩니다. 자체 서명 인증서를 사용하는 일부 사용자는 HTTP 종속 포털을 통해 회사 리소스에 대한 연결을 활성화하고자 할 수 있으며, 이 경우 **Disable Captive Portal Detection(**종속 포털 탐지 비활성화**)** 체크 박스를 선택해야 합니다. 관리자는 이 옵션을 사용자가 구성할 수 있도록 지정할지 여부를 결정하여 그에 따라 체크 박스를 선택할 수도 있습니다. 사용자가 옵션을 구성할 수 있도록 선택하는 경우에는 AnyConnect Secure Mobility Client UI의 Preferences(기본 설정) 탭에 체크 박스가 표시됩니다

- **Auto Reconnect(**자동 재연결**)** - 연결이 끊어진 경우 AnyConnect에서 VPN 연결을 재설정하려고 시도합니다. 자동 재연결을 사용하지 않는 경우, 연결이 끊어진 이유와 관계없이 재연결하려고 시도하지 않습니다.

  참고 사용자가 클라이언트의 동작을 제어할 수 있는 경우 Auto Reconnect(자동 재연결)를 사용합니다. AlwaysOn에서는 이 기능이 지원되지 않습니다.

  - 자동 재연결 동작
    - DisconnectOnSuspend - AnyConnect는 시스템 일시 중지 시 VPN 세션에 할당된 리소스를 해제하며 시스템 재개 이후에 재연결을 시도하지 않습니다.
    - ReconnectAfterResume(기본값) - AnyConnect는 연결이 끊어진 경우 VPN 연결을 재설정하려고 시도합니다.

- **Auto Update(**자동 업데이트**)**—이 옵션을 선택하면 클라이언트가 자동으로 업데이트됩니다. User Controllable(사용자 제어 가능)을 선택한 경우 클라이언트에서 이 설정을 재정의할 수 있습니다.
- **RSA Secure ID Integration(RSA** 보안 **ID** 통합**)** (Windows 전용) —RSA와 사용자가 상호 작용하는 방식을 제어합니다. 기본적으로 AnyConnect는 RSA 상호 작용 방식을 결정합니다(자동 설정: 허용된 소프트웨어 또는 하드웨어 토큰 모두).
- **Windows Logon Enforcement(Windows** 로그온 적용**)**—RDP(Remote Desktop Protocol, 원격 데스크톱 프로토콜) 세션에서 VPN 세션이 설정되도록 합니다. 스플릿 터널링을 그룹 정책에서 구성해야 합니다. VPN 연결을 설정한 사용자가 로그오프하는 경우, AnyConnect는 VPN 연결을 끊습니다. 원격 사용자가 연결을 설정하고 이 원격 사용자가 로그오프하는 경우 VPN 연결이 종료됩니다.
  - 단일 로컬 로그온(기본값) — 한 명의 로컬 사용자만 전체 VPN 연결 중에 로그온할 수 있습니다. 또한 로컬 사용자는 한 명 이상의 원격 사용자가 클라이언트 PC에 로그온되어 있는 동안 VPN 연결을 설정할 수 있습니다. 이 설정은 VPN 연결을 통해 엔터프라이즈 네트워크에서 로그온하는 원격 사용자에게 영향을 주지 않습니다.

    참고 VPN 연결이 양단간 터널링에 대해 구성되어 있는 경우, VPN 연결을 위해 클라이언트 PC 라우팅 테이블이 수정된 결과가 원인이 되어 원격 로그온 연결이 끊어집니다. VPN 연결이 스플릿 터널링에 대해 구성된 경우, VPN 연결을 위한 라우팅 설정에 따라 원격 로그온의 연결이 끊어지거나 그렇지 않을 수 있습니다.

  - 단일 로그온 — 한 명의 사용자만 전체 VPN 연결 중에 로그온할 수 있습니다. 한 명 이상의 사용자가 로컬로 또는 원격으로 로그온하는 경우, VPN 연결을 설정할 때 연결이 허용되지 않습니다. 두 번째 사용자가 VPN 연결 중에 로컬로 또는 원격으로 로그온하는 경우, VPN 연결이 종료됩니다. 추가 로그온은 VPN 연결 중에 허용되지 않으므로 VPN 연결을 통해 원격으로 로그온할 수 없습니다.

참고 여러 동시 로그온은 지원되지 않습니다.

- **Windows VPN Establishment(Windows VPN** 설정)—클라이언트 PC에 원격으로 로그온한 사용자가 VPN 연결을 설정할 때의 AnyConnect 동작을 결정합니다. 가능한 값은 다음과 같습니다.
  - 로컬 사용자 전용(기본값) — 원격으로 로그온한 사용자가 VPN 연결을 설정하는 것을 방지합니다. 이 기능은 AnyConnect 이전 버전의 기능과 동일합니다.
  - 원격 사용자 허용 — 원격 사용자가 VPN 연결을 설정하도록 허용합니다. 단, 구성된 VPN 연결 라우팅으로 인해 원격 사용자의 연결이 끊어진 경우, VPN 연결은 원격 사용자가 클라이언트 PC에 대한 액세스 권한을 다시 찾도록 종료됩니다. 원격 사용자는 VPN 연결을 종료하지 않으면서 원격 로그인 세션의 연결을 끊으려는 경우, VPN을 설정하고 90초 정도 기다려야 합니다.
- 스마트카드 **PIN** 지우기
- **IP Protocol Supported(IP** 프로토콜 지원됨)—AnyConnect를 사용하는 ASA에 연결하려고 시도하는 IPv4와 IPv6 주소가 모두 있는 클라이언트의 경우, AnyConnect는 연결 시작에 사용할 IP 프로토콜을 결정해야 합니다. AnyConnect는 기본적으로 IPv4를 사용하여 연결을 시도합니다. 이 시도가 실패한 경우, AnyConnect는 IPv6를 사용하여 연결을 시도합니다.

  이 필드는 최초 IP 프로토콜 및 대체 순서를 구성합니다.
  - IPv4 — ASA에 IPv4 전용 연결을 설정할 수 있습니다.
  - IPv6 — ASA에 IPv6 전용 연결을 설정할 수 있습니다.
  - IPv4, IPv6 — 먼저 ASA에 IPv4 연결을 설정하려고 시도합니다. 클라이언트가 IPv4를 사용하여 연결할 수 없는 경우, IPv6 연결을 시도합니다.
  - IPv6, IPv4 — 먼저, ASA에 IPv6 연결을 설정하려고 시도합니다. 클라이언트가 IPv6를 사용하여 연결할 수 없는 경우, IPv4 연결을 시도합니다.

참고 IPv4에서 IPv6 및 IPv6에서 IPv4 프로토콜로의 장애 조치가 VPN 세션 중에 발생할 수 있습니다. 기본 IP 프로토콜이 손실된 경우, VPN 세션은 가능한 경우 보조 IP 프로토콜을 통해 재설정됩니다.

AnyConnect 프로파일 편집기, 환경 설정(2부)

- **Disable Automatic Certificate Selection(**자동 인증서 선택 비활성화**)** (Windows 전용)-클라이언트가 인증서를 자동으로 선택하지 못하도록 설정하고 사용자에게 인증 인증서를 선택하라는 프롬프트를 표시합니다.

  관련 주제: 인증서 선택 영역 구성

- **Proxy Settings(**프록시 설정**)**-AnyConnect 프로파일의 정책이 프록시 서버에 대한 클라이언트 액세스를 제어하도록 지정합니다. 프록시 구성으로 사용자가 기업 네트워크 외부에서 터널을 설정하는 것을 방지하는 경우 이 옵션을 사용하십시오.
  - 네이티브 — 클라이언트가 AnyConnect에서 이전에 구성한 프록시 설정과 브라우저에 구성된 프록시 설정을 모두 사용할 수 있습니다. 전역 사용자 환경 설정에 구성된 프록시 설정이 브라우저 프록시 설정에 추가됩니다.
  - IgnoreProxy — 사용자의 컴퓨터에서 브라우저 프록시 설정을 무시합니다.
  - 재정의 — 공용 프록시 서버의 주소를 수동으로 구성합니다. 공용 프록시는 Linux용으로 지원되는 유일한 프록시 유형입니다. Windows도 공용 프록시를 지원합니다. 공용 프록시 주소를 사용자 제어 가능 설정으로 구성할 수 있습니다.

- **Allow Local Proxy Connections(**로컬 프록시 연결 허용**)**—기본적으로 AnyConnect에서는 Windows 사용자가 로컬 PC에서 투명 또는 비투명 프록시 서비스를 통해 VPN 세션을 설정할 수 있습니다. 로컬 프록시 연결에 대한 지원을 비활성화하려면 이 파라미터를 선택 취소합니다. 투명 프록시 서비스를 제공하는 요소의 몇 가지 예로는 일부 무선 데이터 카드에서 제공하는 가속화 소프트웨어 및 일부 안티 바이러스 소프트웨어의 네트워크 구성요소가 있습니다.

- **Enable Optimal Gateway Selection(**최적의 게이트웨이 선택사항 활성화**)** (OGS), (IPv4 클라이언트 전용) —AnyConnect는 RTT(Round Trip Time, 왕복 시간)에 기반하여 연결 또는 재연결에 가장 적합한 보안 게이트웨이를 식별하고 선택하여 사용자 개입 없이 인터넷 트래픽의 대기 시간을 최소화합니다. OGS는 보안 기능이 아니며 보안 게이트웨이 클러스터 또는 여러 클러스터 간에 로드 밸런싱을 수행하지 않습니다. OGS 활성화 및 비활성화를 제어하고 최종 사용자가 스스로 기능을 제어할지를 지정합니다. 클라이언트 GUI의 연결 탭에서 드롭다운 목록 연결에 자동 선택사항이 표시됩니다.
  - **Suspension Time Threshold(**일시 중지 시간 임계값**)** (시간) —새 게이트웨이 선택사항 계산을 호출하기 전에 VPN이 일시 중지 상태로 있어야 하는 최소 시간(시간 단위)을 입력합니다. 다음 구성 가능한 파라미터(성능 개선 임계값)와 결합하여 이 값을 최적화함으로써, 최적의 게이트웨이를 선택하고 크리덴셜을 재입력하는 횟수를 줄이는 작업 간에 적절한 균형을 찾을 수 있습니다.
  - **Performance Improvement Threshold(**성능 개선 임계값**)** (%) —시스템 재개 이후에 클라이언트를 다른 보안 게이트웨이에 재연결되게 하는 성능 개선 백분율입니다. 특정한 네트워크에 대해 이 값을 조정하여 최적의 게이트웨이를 선택하고 자격 증명 재입력을 적용하는 횟수를 줄이는 작업 간에 적절한 균형을 찾습니다. 기본값은 20%입니다.

  OGS가 활성화되어 있는 경우, 이 기능을 사용자 제어 가능으로 설정하는 것이 좋습니다.

  OGS에는 다음과 같은 제한 사항이 있습니다.
  - Always-On을 통해 작동할 수는 없습니다.
  - 자동 프록시 탐색을 통해 작동할 수는 없습니다.
  - PAC(프록시 자동 컨피그레이션) 파일을 통해 작동할 수는 없습니다.

- AAA를 사용하는 경우 다른 보안 게이트웨이로 전환 시 사용자가 자신의 자격 증명을 다시 입력해야 할 수 있습니다. 인증서를 사용하면 이 문제가 발생하지 않습니다.

- **Automatic VPN Policy(**자동 **VPN** 정책**)**(Windows 및 macOS 전용) - 신뢰할 수 있는 네트워크 탐지를 활성화하면 AnyConnect가 신뢰할 수 있는 네트워크 정책 및 신뢰할 수 없는 네트워크 정책에 따라 VPN 연결을 시작하거나 중지할 시기를 자동으로 관리할 수 있습니다. 이 설정이 비활성화된 경우 VPN 연결을 수동으로만 시작하고 중지할 수 있습니다. 자동 VPN 정책을 설정하면 사용자가 VPN 연결을 수동으로 제어하는 것을 방지할 수 없습니다.
  - **Trusted Network Policy(**신뢰할 수 있는 네트워크 정책**)**—사용자가 기업 네트워크 내부에 있는 경우(신뢰할 수 있는 네트워크) 작업 AnyConnect는 VPN 연결을 자동으로 수행합니다.
    - 연결 끊기(기본값) — 신뢰할 수 있는 네트워크가 탐지되면 VPN 연결을 끊습니다.
    - 연결 — 신뢰할 수 있는 네트워크가 탐지되면 VPN 연결을 시작합니다.
    - Do Nothing(작업 수행 안 함) - 신뢰할 수 있는 네트워크에서 아무 작업도 수행하지 않습니다. 신뢰할 수 있는 네트워크 정책 및 신뢰할 수 없는 네트워크 정책을 모두 Do Nothing(작업 수행 안 함) 으로 설정하면 신뢰할 수 있는 네트워크 탐지가 비활성화됩니다.
    - 일시 중지 — AnyConnect는 사용자가 신뢰할 수 있는 네트워크 외부에서 VPN 세션을 설정한 이후에 신뢰할 수 있는 상태로 구성된 네트워크를 시작하는 경우, 연결을 끊는 대신 VPN 세션을 일시 중지합니다. 사용자가 신뢰할 수 있는 네트워크 외부로 다시 이동하면 AnyConnect는 세션을 재개합니다. 이 기능은 신뢰할 수 있는 네트워크를 종료한 이후에 새 VPN 세션을 설정할 필요가 없으므로 사용자에게 편리한 기능입니다.
  - **Untrusted Network Policy(**신뢰할 수 없는 네트워크 정책**)**—사용자가 기업 네트워크 외부에 있는 경우(신뢰할 수 없는 네트워크) AnyConnect는 VPN 연결을 시작합니다. 이 기능은 사용자가 신뢰할 수 있는 네트워크 외부에 있는 경우 VPN 연결을 시작하여 보안 인식을 개선하는 데 도움을 줍니다.
    - 연결(기본값) — 신뢰할 수 없는 네트워크가 탐지되면 VPN 연결을 시작합니다.
    - 작업 수행 안 함 — 신뢰할 수 있는 네트워크에서 아무 작업도 수행하지 않습니다. 이 옵션은 상시 가동 VPN을 비활성화합니다. 신뢰할 수 있는 네트워크 정책 및 신뢰할 수 없는 네트워크 정책을 모두 Do Nothing(작업 수행 안 함) 으로 설정하면 신뢰할 수 있는 네트워크 탐지가 비활성화됩니다.
  - **Trusted DNS Domains(**신뢰할 수 있는 **DNS** 도메인**)**— 클라이언트가 신뢰할 수 있는 네트워크에 있는 경우, 네트워크 인터페이스에 포함될 수 있는 DNS 접미사(쉼표로 구분되는 문자열)입니다. 예를 들어 *.cisco.com입니다. 와일드카드(*)는 DNS 접미사용으로 지원됩니다.
  - **Trusted Servers(**신뢰할 수 있는 서버**) @ https://<**서버**>[:<**포트**>]** - 신뢰하는 항목으로 추가할 호스트 URL입니다. 신뢰할 수 있는 인증서를 사용하여 액세스할 수 있는 보안 웹 서버가 있어야 신뢰할 수 있는 서버로 간주됩니다. **Add(**추가**)**를 클릭하면 URL이 추가되고 인증서 해시가 미리 입력됩니다. 해시를 찾을 수 없으면 인증서 해시를 수동으로 입력하고 **Set(**설정**)**를 클릭하라는 오류 메시지 프롬프트가 표시됩니다.

참고 Trusted DNS Domains(신뢰할 수 있는 DNS 도메인) 또는 Trusted DNS Servers(신뢰할 수 있는 DNS 서버) 중 하나 이상을 정의해야 이 파라미터를 구성할 수 있습니다. Trusted DNS Domains(신뢰할 수 있는 DNS 도메인) 또는 Trusted DNS Servers(신뢰할 수 있는 DNS 서버)를 정의하지 않으면 이 필드는 비활성화됩니다.

- **Always On(Always - On 기능)** — 지원되는 Windows 또는 macOS 운영 체제 중 하나를 실행하는 컴퓨터에 사용자가 로그인하는 경우, AnyConnect에서 VPN에 자동으로 연결되는지를 결정합니다. 컴퓨터가 신뢰할 수 있는 네트워크에 있지 않은 경우, 인터넷 리소스에 액세스하는 것을 방지하여 보안 위협으로부터 컴퓨터를 보호하는 기업 정책을 적용할 수 있습니다. 정책을 할당하는 데 사용되는 일치 기준에 따라 예외를 지정하여 이 설정을 재정의하려는 경우 그룹 정책 및 동적 액세스 정책에서 상시 가동 VPN 파라미터를 설정할 수 있습니다. AnyConnect 정책에서는 상시 가동 기능을 활성화하는데 동적 액세스 정책 또는 그룹 정책은 이 기능을 비활성화하는 경우 클라이언트는 새로운 각 세션 설정에 대한 동적 액세스 정책 또는 그룹 정책과 AnyConnect 정책의 기준이 일치하면 현재 및 향후 VPN 세션에 대해 비활성화 설정을 유지합니다. 설정을 활성화한 이후에 추가 파라미터를 구성할 수 있습니다.

참고 AlwaysOn은 사용자의 개입 없이도 연결 설정 및 이중화가 실행되는 시나리오에 사용됩니다. 따라서 이 기능을 사용하는 동안에는 기본 설정(1부)에서 Auto Reconnect(자동 재연결)를 구성하거나 활성화할 필요가 없습니다.

관련 주제: 상시 가동을 사용하는 VPN 연결 필요

  - **Allow VPN Disconnect(VPN 연결 끊기 허용)**- 상시 가동 VPN 세션에 대한 Disconnect(연결 끊기) 버튼을 AnyConnect에 표시할지 여부를 결정합니다. 상시 가동 VPN 세션 사용자는 현재 VPN 세션의 성능 문제, VPN 세션 중단 이후의 재연결 문제 등이 발생하는 경우 대체 보안 게이트웨이를 선택하기 위해 Disconnect(연결 끊기)를 클릭할 수 있습니다.

    연결 끊기는 모든 인터페이스에 잠금을 설정하여 데이터 유출을 방지하고 VPN 세션 설정을 제외한 인터넷 액세스로부터 컴퓨터를 보호합니다. Disconnect(연결 끊기) 버튼을 비활성화하면 경우에 따라 앞에서 설명한 이유로 인해 VPN 액세스가 방해되거나 방지될 수 있습니다.

  - **Connect Failure Policy(연결 실패 정책)**— AnyConnect가 VPN 세션을 설정할 수 없는 경우(예: ASA에 연결할 수 없는 경우), 컴퓨터에서 인터넷에 액세스할 수 있는지 결정합니다. 이 파라미터는 상시 가동 기능 및 Allow VPN Disconnect(VPN 연결 끊기 허용)가 활성화된 경우에만 적용됩니다. 상시 가동기능을 선택한 경우, 실패 시 열림 정책은 네트워크 연결을 허용하며 실패 시 닫힘 정책은 네트워크 연결을 비활성화합니다.

- 닫힘 — VPN에 연결할 수 없는 경우 네트워크 액세스를 제한합니다. 이 설정은 엔드포인트를 보호하는 역할을 하는 사설 네트워크에서 리소스를 사용할 수 없는 경우, 네트워크 위협으로부터 기업 자산을 보호하는데 도움을 줍니다.
- 열림 — VPN에 연결할 수 없는 경우 네트워크 액세스를 허용합니다.

주의 연결 실패 시 닫힘 정책은 AnyConnect가 VPN 세션을 설정하는 데 실패하는 경우, 네트워크 액세스를 방지합니다. 이는 주로 예외적으로 보안 지속성이 항상 사용 가능한 네트워크 액세스보다 중요한 보안 조직을 위한 정책입니다. 스플릿 터널링에서 허용되고 ACL에 따라 제한되는 프린터 및 테더링 디바이스와 같은 로컬 리소스를 제외한 모든 네트워크 액세스를 방지합니다. 보안 게이트웨이를 사용할 수 없는 경우, 사용자가 VPN 외에 인터넷 액세스를 필요로 할 때 이로 인해 생산성을 저해할 수 있습니다. AnyConnect에서는 대부분의 종속 포털을 탐지합니다. 종속 포털을 탐지할 수 없는 경우, 연결 실패 시 닫힘 정책은 모든 네트워크 연결성을 방지합니다.

닫힘 연결 정책을 구축하는 경우, 단계별로 접근하는 것이 좋습니다. 예를 들어 먼저 연결 실패 시 열림 정책에 따라 상시 가동 VPN을 구축하고 사용자를 대상으로 AnyConnect가 원활하게 연결되지 않는 빈도를 조사합니다. 그런 다음 얼리 어답터 사용자에게 연결 실패 시 닫힘 정책을 소규모의 파일럿으로 구축하고 피드백을 요청합니다. 전체 구축을 고려하기 전에 피드백을 계속 요청하면서 파일럿 프로그램을 단계적으로 확장합니다. 연결 실패 시 닫힘 정책을 구축하는 동안 이 정책의 이점뿐만 아니라 네트워크 액세스 한계에 대해 VPN 사용자에게 알려주어야 합니다.

관련 주제: 종속 포털 정보

연결 실패 정책이 닫힘으로 설정된 경우, 다음 설정을 구성할 수 있습니다.

- **Allow Captive Portal Remediation(**종속 포털 보안정책 교정 허용**)**— 클라이언트가 종속 포털(핫스팟)을 탐지한 경우, AnyConnect에서 닫힘 연결 실패 정책에 따라 적용되는 네트워크 액세스 제한을 해제할 수 있습니다. 호텔 및 공항에서는 일반적으로 종속 포털을 사용하여 사용자에게 브라우저를 열고 인터넷 액세스 허용의 필수 조건을 충족시키도록 요구합니다. 기본적으로 이 파라미터는 선택이 취소된 상태에서 가장 강력한 보안을 제공하지만 클라이언트를 VPN에 연결하려고 할 때 종속 포털에서 이를 방지하는 경우, 이 파라미터를 활성화해야 합니다.
- **Remediation Timeout(**보안정책 교정 시간 제한**)**— AnyConnect에서 네트워크 액세스 제한을 해제하는데 걸리는 시간(분)입니다. 이 파라미터는 Allow Captive Portal Remediation(종속 포털 보안정책 교정 허용) 파라미터가 선택되고 클라이언트가 종속 포털을 탐지하는 경우에 적용됩니다. 일반적인 종속 포털 요건(예: 5분)을 충족하도록 충분한 시간을 지정합니다.
- **Apply Last VPN Local Resource Rules(**마지막 **VPN** 로컬 리소스 규칙 적용**)**— VPN에 연결할 수 없는 경우, 클라이언트는 로컬 LAN에 있는 리소스에 대한 액세스를

허용하는 ACL이 포함된 ASA에서 수신한 마지막 클라이언트 방화벽을 적용합니다.

관련 주제: 연결 실패 정책 구성

- **Allow Manual Host Input(**수동 호스트 입력 허용**)** - 사용자가 AnyConnect UI의 드롭다운 상자에 나열된 주소가 아닌 다른 VPN 주소를 입력할 수 있습니다. 이 체크 박스를 선택 취소하는 경우에는 드롭다운 상자의 VPN 연결만 선택할 수 있으며 사용자가 새 VPN 주소를 입력할 수 없습니다.
- **PPP Exclusion(PPP** 제외**)**— PPP 연결을 통한 VPN 터널용으로 제외 경로 결정 여부 및 방법을 지정합니다. 클라이언트는 보안 게이트웨이를 벗어난 대상용으로 터널링된 트래픽에서 보안 게이트웨이로 오는 트래픽을 제외시킬 수 있습니다. 제외 경로는 AnyConnect GUI의 경로 세부사항 표시에서 비보안 경로로 나타납니다. 이 기능을 사용자가 제어할 수 있도록 설정하면 사용자는 PPP 제외 설정을 검토하고 변경할 수 있습니다.
  - 자동 — PPP 제외를 활성화합니다. AnyConnect에서 자동으로 PPP 서버의 IP 주소를 사용합니다. 자동 탐지에서 IP 주소를 가져오지 못하는 경우에만 이 값을 변경하도록 사용자에게 지시합니다.
  - 비활성화 — PPP 제외를 적용하지 않습니다.
  - 재정의 — PPP 제외를 활성화합니다. 자동 탐지로 PPP 서버의 IP 주소를 가져오지 못하고 PPP 제외를 사용자 제어 가능 설정으로 구성한 경우에 선택합니다.

  PPP 제외가 활성화된 경우, 다음을 설정하십시오.
  - **PPP Exclusion Server IP(PPP** 제외 서버 **IP)**— PPP 제외에 사용되는 보안 게이트웨이의 IP 주소입니다.

  관련 주제: 사용자에게 PPP 제외를 재정의하도록 지시
- **Enable Scripting(**스크립팅 활성화**)**— 보안 어플라이언스 플래시 메모리에 OnConnect 및 OnDisconnect 스크립트가 있는 경우 이를 시작합니다.
  - **Terminate Script On Next Event(**다음 이벤트에서 스크립트 종료**)**— 스크립팅할 수 있는 다른 이벤트로의 전환이 발생하는 경우, 실행 중인 스크립트 프로세스를 종료합니다. 예를 들어 VPN 세션이 종료된 경우, AnyConnect에서 실행 중인 OnConnect 스크립트를 종료하며 클라이언트가 새 VPN 세션을 시작하는 경우 실행 중인 OnDisconnect 스크립트를 종료합니다. Microsoft Windows에서 클라이언트는 OnConnect 또는 OnDisconnect 스크립트가 시작한 스크립트와 해당 스크립트의 하위 스크립트도 모두 종료합니다. macOS 및 Linux에서는 클라이언트가 OnConnect 또는 OnDisconnect 스크립트만 종료하며 하위 스크립트는 종료하지 않습니다.
  - **Enable Post SBL On Connect Script(**사후 **SBL OnConnect** 스크립트 활성화**)**— OnConnect 스크립트가 있는 경우 이 스크립트를 시작하고 SBL에서 VPN 세션을 설정합니다. (VPN 엔드포인트가 Microsoft Windows를 실행 중인 경우에만 지원됨)

- **Retain VPN On Logoff(**로그오프 시 **VPN** 유지**)** — 사용자가 Windows 또는 Mac OS에서 로그오프할 경우, VPN 세션을 그대로 유지할지 결정합니다.
  - **User Enforcement(**사용자 적용**)**— 다른 사용자가 로그온하는 경우, VPN 세션을 종료할지 지정합니다. 이 파라미터는 "Retain VPN On Logoff(로그오프 시 VPN 유지)"를 선택하고 VPN 세션이 종료되었을 때 원래의 사용자가 Windows 또는 Mac OS X에서 로그오프한 경우에만 적용됩니다.
- **Authentication Timeout Values(**인증 시간 제한 값**)**—기본적으로 AnyConnect는 연결 시도를 종료하기 전에 보안 게이트웨이에서 인증을 위해 최대 12초 동안 대기합니다. 그런 다음 AnyConnect는 인증 시간 제한 초과를 나타내는 메시지를 표시합니다. 0에서 120 사이 초 단위의 수를 입력합니다.

AnyConnect 프로파일 편집기, 백업 서버

사용자가 선택한 서버에서 오류가 발생하는 경우, 클라이언트에서 사용하는 백업 서버 목록을 구성할 수 있습니다. 사용자가 선택한 서버에서 오류가 발생하는 경우, 클라이언트는 목록의 맨 위에 있는 최적의 백업 서버에 연결을 시도합니다. 연결에 실패하는 경우, 해당 클라이언트는 선택 결과에 따라 순서가 지정된 최적의 게이트웨이 선택사항 목록에서 남아 있는 각 서버에 연결을 시도합니다.

참고 AnyConnect 프로파일 편집기, 서버 목록 추가/편집, 105 페이지에 백업 서버가 정의되어 있지 않은 경우에만 여기서 구성하는 백업 서버 연결을 시도합니다. Server List(서버 목록)에 구성된 서버에 우선적으로 연결하며 여기에 나열된 백업 서버는 덮어쓰기됩니다.

Host Address(호스트 주소**)**— 백업 서버 목록에 포함되도록 IP 주소 또는 FQDN(Fully-Qualified Domain Name)을 지정합니다.

- **Add(**추가**)**— 백업 서버 목록에 호스트 주소를 추가합니다.
- **Move Up(**위로 이동**)**— 선택한 백업 서버를 목록에서 위로 이동시킵니다. 사용자가 선택한 서버에서 오류가 발생하는 경우, 클라이언트는 목록의 맨 위에 있는 백업 서버에 연결을 시도한 후 필요시 목록 아래로 이동시킵니다.
- **Move Down(**아래로 이동**)**— 선택한 백업 서버를 목록에서 아래로 이동시킵니다.
- **Delete(**삭제**)**— 서버 목록에서 백업 서버를 제거합니다.

AnyConnect 프로파일 편집기, 인증서 일치

이 창에서 자동 클라이언트 인증서 선택사항을 구체화하는 데 사용할 수 있는 다양한 특성 정의를 활성화합니다.

인증서 일치 기준을 지정하지 않은 경우, AnyConnect는 다음의 인증서 일치 규칙을 적용합니다.

- 키 사용: Digital_Signature

- 확장 키 사용: 클라이언트 인증

사양과 일치하는 기준이 프로파일에 생성되어 있는 경우, 프로파일에 분명하게 나열하지 않는 한 이 일치 규칙이 적용되지 않습니다.

- **Key Usage(**키 사용**)**— 허용 가능한 클라이언트 인증서 선택을 위해 다음의 인증서 주요 특성을 사용하십시오.
  - Decipher_Only — 데이터를 해독하며, 기타 비트(Key_Agreement 제외)는 설정되어 있지 않음
  - Encipher_Only — 데이터를 암호화하며, 모든 기타 비트(Key_Agreement 제외)는 설정되어 있지 않음
  - CRL_Sign — CRL에서 CA 서명 확인
  - Key_Cert_Sign — 인증서에서 CA 서명 확인
  - Key_Agreement — 주요 계약
  - Data_Encipherment — Key_Encipherment를 제외한 데이터 암호화
  - Key_Encipherment — 키 암호화
  - Non_Repudiation — Key_Cert_sign 또는 CRL_Sign 이외에 일부 작업에 대한 잘못된 거부로부터 보호하는 디지털 서명 확인
  - Digital_Signature — Non_Repudiation, Key_Cert_Sign 또는 CRL_Sign 이외에 디지털 서명 확인

- **Extended Key Usage(**확장 키 사용**)**— 다음의 확장 키 사용 설정을 사용하십시오. OID는 괄호 안에 포함되어 있습니다.
  - ServerAuth(1.3.6.1.5.5.7.3.1)
  - ClientAuth(1.3.6.1.5.5.7.3.2)
  - CodeSign(1.3.6.1.5.5.7.3.3)
  - EmailProtect(1.3.6.1.5.5.7.3.4)
  - IPSecEndSystem(1.3.6.1.5.5.7.3.5)
  - IPSecTunnel(1.3.6.1.5.5.7.3.6)
  - IPSecUser(1.3.6.1.5.5.7.3.7)
  - TimeStamp(1.3.6.1.5.5.7.3.8)
  - OCSPSign(1.3.6.1.5.5.7.3.9)
  - DVCS(1.3.6.1.5.5.7.3.10)
  - IKE 중개

- **Custom Extended Match Key(**사용자 정의 확장 일치 키**)** (최대 10개) — 사용자 정의 확장 일치 키를 지정합니다(최대 10개). 인증서는 사용자가 입력한 모든 지정된 키와 일치해야 합니다. OID 형식(예: 1.3.6.1.5.5.7.3.11)에 키를 입력하십시오.

  참고 OID 크기가 30자보다 긴 맞춤형 확장 일치 키를 생성하는 경우 OK(확인) 버튼을 클릭해도 해당 키는 적용되지 않습니다. OID의 최대 문자 제한은 30자입니다.

- Match only certificates with Extended key usage(확장 키 사용이 가능한 인증서만 일치) - 이전 동작은 인증서 고유 이름(DN) 일치 규칙이 설정되어 있는 경우 클라이언트가 특정 EKU OID를 포함하는 인증서 및 EKU가 없는 모든 인증서 일치를 확인하는 것이었습니다. 이제는 일관성을 유지하되 인증서를 더욱 명확하게 확인하기 위해 EKU가 없는 인증서 일치는 허용하지 않을 수 있습니다. 기본값은 고객이 알고 있는 레거시 동작을 유지하는 것입니다. 새로운 동작을 활성화하고 일치를 허용하지 않으려면 체크 박스를 클릭해야 합니다.

- 고유 이름**(DN)** (최대 10) — 허용 가능한 클라이언트 인증서 선택 관련 정확한 일치 기준에 대해 DN(Distinguished Name, 고유 이름)을 지정합니다.
  - **Name(**이름**)**— 다음은 일치에 사용할 고유 이름(DN)입니다.
    - CN — Subject Common Name(주체 공통 이름)
    - C — Subject Country(주체 국가)
    - DC—Domain Component(도메인 구성 요소)
    - DNQ—Subject Dn Qualifier(주체 Dn 한정자)
    - EA—Subject Email Address(주체 이메일 주소)
    - GENQ—Subject Gen Qualifier(주체 세대 한정자)
    - GN—Subject Given Name(주체 이름)
    - I—Subject Initials(주체 이니셜)
    - L—Subject City(주체 구/군/시)
    - N—Subject Unstruct Name(주체의 정의되지 않은 이름)
    - O—Subject Company(주체 회사)
    - OU—Subject Department(주체 부서)
    - SN—Subject Sur Name(주체 성)
    - SP—Subject State(주체 주/도)
    - ST—Subject State(주체 주/도)
    - T—Subject Title(주체 직함)

- ISSUER-CN—Issuer Common Name(발급자 공통 이름)
- ISSUER-DC—Issuer Component(발급자 구성 요소)
- ISSUER-SN—Issuer Sur Name(발급자 성)
- ISSUER-GN—Issuer Given Name(발급자 이름)
- ISSUER-N—Issuer Unstruct Name(발급자의 정의되지 않은 이름)
- ISSUER-I—Issuer Initials(발급자 이니셜)
- ISSUER-GENQ—Issuer Gen Qualifier(발급자 세대 한정자)
- ISSUER-DNQ—Issuer Dn Qualifier(발급자 Dn 한정자)
- ISSUER-C—Issuer Country(발급자 국가)
- ISSUER-L—Issuer City(발급자 구/군/시)
- ISSUER-SP—Issuer State(발급자 주/도)
- ISSUER-ST—Issuer State(발급자 주/도)
- ISSUER-O—Issuer Company(발급자 회사)
- ISSUER-OU—Issuer Department(발급자 부서)
- ISSUER-T—Issuer Title(발급자 직함)
- ISSUER-EA—Issuer Email Address(발급자 이메일 주소)

- **Pattern(**패턴**)**— 일치시킬 문자열을 지정합니다. 일치시킬 패턴에 일치시키려는 문자열의 일부만 포함해야 합니다. 패턴 일치 또는 정규식 구문은 포함시킬 필요가 없습니다. 입력된 경우, 이 구문은 검색할 문자열의 일부로 간주됩니다.

  예를 들어, 샘플 문자열이 abc.cisco.com이며 cisco.com과 일치시키려는 경우 입력한 패턴이 cisco.com이어야 합니다.

- **Operator(**연산자**)**— 이 DN에 일치 할 때 사용하는 연산자입니다.
  - Equal(같음) — ==와 동일
  - Not Equal(같지 않음) — !=와 동일

- **Wildcard(**와일드카드**)**— 와일드카드 패턴 일치를 포함할 수 있습니다. 와일드카드를 사용하면 문자열의 어느 위치에서나 패턴을 찾을 수 있습니다.

- **Match Case(**대/소문자 구분**)**— 대/소문자를 구분하는 패턴 일치를 사용할 때 선택합니다.

관련 항목

인증서 일치 구성, 165 페이지

AnyConnect 프로파일 편집기, 인증서 등록

인증서 등록을 통해 AnyConnect에서 SCEP(Simple Certificate Enrollment Protocol, 단순 인증서 등록 프로토콜)를 사용하여 클라이언트 인증에 필요한 인증서를 제공하고 갱신할 수 있습니다.

- **Certificate Expiration Threshold(**인증서 만료 임계값**)**— AnyConnect에서 사용자에게 인증서가 만료될 예정임을 경고하는 인증서 만료 전 남은 날짜 수입니다(RADIUS 비밀번호 관리에서 지원하지 않음). 기본값은 영(0)(표시된 경고 없음)입니다. 값의 범위는 영(0)부터 180일까지입니다.

- **Certificate Import Store(**인증서 가져오기 저장소**)** — 등록 인증서를 어떤 Windows 인증서 저장소에 저장할지 선택합니다.

- **Automatic SCEP Host(**자동 **SCEP** 호스트**)**— 레거시 SECP의 경우 SCEP 인증서 검색이 구성되어 있는 ASA의 호스트 이름과 연결 프로파일(터널 그룹)을 지정합니다. ASA의 FQDN(Fully Qualified Domain Name, 정규화된 도메인 이름) 또는 연결 프로파일 이름을 입력합니다. 예를 들어 호스트 이름인 asa.cisco.com과 연결 프로파일 이름인 scep_eng를 입력합니다.

- **CA URL**— 레거시 SCEP의 경우, SCEP CA 서버를 식별합니다. CA 서버의 FQDN 또는 IP 주소를 입력합니다. 예를 들어 http://ca01.cisco.com을 입력합니다.
  - **Prompt For Challenge PW(**시도용 비밀번호 프롬프트**)**— 사용자가 인증서 요청을 수동으로 생성하도록 허용할 때 사용합니다. 사용자가 **Get Certificate(**인증서 가져오기**)**를 클릭할 경우, 클라이언트에서 사용자에게 사용자 이름 및 일회용 비밀번호를 입력하도록 프롬프트를 표시합니다.
  - **Thumbprint(**지문**)**— CA의 인증서 지문입니다. SHA1 또는 MD5 해시를 사용하십시오.

  참고 CA 서버 관리자는 CA URL 및 지문을 제공할 수 있으며 발급된 서버 인증서의 “fingerprint(지문)" 또는 "thumbprint(지문)" 특성 필드가 아니라 서버에서 직접 지문을 검색해야 합니다.

- **Certificate Contents(**인증서 콘텐츠**)**— SCEP 등록 요청에 포함할 인증서 콘텐츠를 지정합니다.
  - 이름(CN) — 인증서에서의 공통 이름
  - 부서(OU) — 인증서에 지정된 부서 이름
  - 회사(O) — 인증서에 지정된 회사 이름
  - 주/도(ST) — 인증서에 이름이 지정된 주/도 식별자
  - 주/도(SP) — 다른 주/도 식별자
  - 국가(C) — 인증서에서 이름이 지정된 국가 식별자
  - 이메일(EA) — 이메일 주소. 다음 예에서 이메일(EA)은 %USER%@cisco.com입니다. %USER%는 사용자의 ASA 사용자 이름 로그인 자격 증명에 해당합니다.

- 도메인(DC) — 도메인 구성 요소. 다음 예에서 도메인(DC)은 cisco.com으로 설정됩니다.
- 성(SN) — 성
- 이름(GN) — 일반적인 의미의 이름
- UnstructName(N) — 정의되지 않은 이름
- 이니셜(I) — 사용자의 이니셜
- 한정자(GEN) — 사용자의 세대 한정자. 예를 들어 "Jr" 또는 "III."
- 한정자(DN) — 전체 DN을 위한 한정자
- 구/군/시(L) — 구/군/시 식별자
- 직함(T) — 사용자의 직함. 예를 들어 Ms., Mrs., Mr.
- CA 도메인 — SCEP 등록에 사용되며 일반적으로 CA 도메인
- 키 크기 — 등록할 인증서용으로 생성된 RSA 키의 크기

- **Display Get Certificate Button(**인증서 가져오기 표시 버튼**)**— 다음 조건에서 AnyConnect GUI에 Get Certificate(인증서 가져오기) 버튼을 표시할 때 사용합니다.
  - 인증서가 인증서 만료 임계값(RADIUS에서는 지원되지 않음)에 따라 정의한 기간 이내에 만료하도록 설정됩니다.
  - 인증서가 만료되었습니다.
  - 인증서가 없습니다.
  - 인증서 일치에 실패했습니다.

관련 항목

인증서 등록 구성, 152 페이지

AnyConnect 프로파일 편집기, 인증서 고정

사전 요구 사항

인증서 고정을 시작하기 전에 최고의 사례를 확인하려면 인증서 고정 정보, 174 페이지를 참조하십시오.

VPN 프로파일 편집기를 사용하여 기본 설정을 활성화하고 글로벌 및 호스트별 인증서 고정을 구성합니다. Global Pins(글로벌 고정) 섹션의 기본 설정이 활성화되어 있는 경우에만 Server List(서버 목록) 섹션에서 호스트별 인증서를 고정할 수 있습니다. 기본 설정을 활성화하고 나면 클라이언트가 인증서 고정 확인에 사용하는 글로벌 고정 목록을 구성할 수 있습니다. Server List(서버 목록) 섹션에 호스트별 고정을 추가하는 것은 글로벌 고정을 추가하는 것과 비슷합니다. 인증서 체인의 모든 인증서를 고정할 수 있으며, 고정하는 인증서는 고정에 필요한 정보를 계산하기 위해 프로파일 편집기로 가져오기됩니다.

Add Pin(고정 추가) - 프로파일 편집기로 인증서를 가져와서 고정하는 과정을 안내하는 인증서 고정 마법사를 시작합니다.

이 창의 Certificate Details(인증서 세부사항) 부분에서 Subject(제목) 및 Issuer(발급자) 열을 확인할 수 있습니다.

인증서 고정 마법사

서버 인증서 체인의 모든 인증서를 프로파일 편집기로 가져와 고정에 필요한 정보를 지정할 수 있습니다. 프로파일 편집기에서는 다음의 세 가지 인증서 가져오기 옵션을 지원합니다.

- 로컬 파일 찾아보기 - 컴퓨터의 로컬 위치에 있는 인증서를 선택합니다.
- URL에서 파일 다운로드 - 파일 호스팅 서버에서 인증서를 다운로드합니다.
- PEM 형식으로 정보 붙여넣기 - 인증서 시작 및 종료 헤더를 포함한 PEM 형식의 정보를 삽입합니다.

참고 DER, PEM 및 PKCS7 데이터 형식의 인증서만 가져올 수 있습니다.

AnyConnect 프로파일 편집기, 모바일 정책

AnyConnect 버전 3.0 이상에서는 Windows Mobile 디바이스를 지원하지 않습니다. Windows Mobile 디바이스 관련 정보는 *Cisco AnyConnect Secure Mobility Client* 관리자 설명서, 릴리스 *2.5*를 참조하십시오.

AnyConnect 프로파일 편집기, 서버 목록

클라이언트 GUI에 나타나는 서버 목록을 구성할 수 있습니다. 사용자는 VPN 연결을 설정하기 위해 목록에서 서버를 선택할 수 있습니다.

서버 목록 테이블의 열 항목:

- 호스트 이름 — 호스트, IP 주소 또는 FQDN(Full-Qualified Domain Name, 정규화된 도메인 이름)을 나타내기 위해 사용되는 별칭입니다.
- 호스트 주소 — 서버의 IP 주소 또는 FQDN입니다.
- 사용자 그룹 — 그룹 기반 URL을 구성하기 위해 호스트 주소와 함께 사용됩니다.
- 자동 SCEP 호스트 — 클라이언트 인증에 사용된 인증서를 프로비저닝하고 갱신하기 위해 지정된 단순 인증서 등록 프로토콜입니다.
- CA URL — 해당 서버에서 CA(Certificate Authority, 인증 기관)에 연결하는 데 사용하는 URL입니다.
- Certificate Pins(인증서 고정) - 고정 확인 중에 클라이언트에서 사용하는 호스트별 고정입니다. AnyConnect 프로파일 편집기, 인증서 고정, 103 페이지을 참조하십시오.

참고 클라이언트는 고정 확인 중에 글로벌 고정과 그에 해당하는 호스트별 고정을 사용합니다. 호스트별 고정은 인증서 고정 마법사를 사용하여 글로벌 고정을 구성하는 것과 유사한 방식으로 구성됩니다.

Add/Edit(추가/편집**)**— 상위 서버 파라미터를 지정할 수 있는 Server List Entry(서버 목록 항목) 대화상자를 실행합니다.

Delete(삭제**)**— 서버 목록에서 서버를 제거합니다.

Details(세부사항**)**— 서버에 대한 CA URL 또는 백업 서버에 대한 추가 세부사항을 표시합니다.

관련 항목

VPN 연결 서버 구성, 119 페이지

AnyConnect 프로파일 편집기, 서버 목록 추가/편집

- **Host Display Name(**호스트 표시 이름**)**— 호스트, IP 주소 또는 FQDN(Full-Qualified Domain Name, 정규화된 도메인 이름)을 나타내기 위해 사용되는 별칭을 입력합니다.
- **FQDN or IP Address(FQDN** 또는 **IP** 주소**)**— 서버의 IP 주소 또는 FQDN을 지정합니다.
  - Host Address(호스트 주소) 필드에 IP 주소 또는 FQDN을 지정한 경우, Host Name(호스트 이름) 필드의 항목은 AnyConnect 클라이언트 트레이 플라이아웃의 연결 드롭다운 목록에 있는 서버에 대한 레이블이 됩니다.
  - Hostname(호스트 이름) 필드에 FQDN만 지정하고 Host Address(호스트 주소) 필드에 IP 주소가 없는 경우, Hostname(호스트 이름) 필드에 있는 FQDN은 DNS 서버를 통해 확인됩니다.
  - IP 주소를 입력한 경우, 보안 게이트웨이의 공용 IPv4 또는 전역 IPv6 주소를 사용합니다. 링크-로컬 보안 게이트웨이 주소 사용은 지원되지 않습니다.
- **User Group(**사용자 그룹**)**— 사용자 그룹을 지정합니다.

  사용자 그룹은 호스트 주소와 함께 그룹 기반 URL을 구성하는 데 사용됩니다. 기본 프로토콜을 IPsec으로 지정한 경우, 사용자 그룹은 연결 프로파일(터널 그룹)의 정확한 이름이어야 합니다. SSL의 경우 사용자 그룹은 연결 프로파일의 그룹 URL 또는 그룹 별칭입니다.
- **Additional mobile-only settings(**추가 모바일 전용 설정**)**— Apple iOS 및 Android 모바일 디바이스를 구성하려면 선택합니다.
- **Backup Server List(**백업 서버 목록**)**

  사용자가 선택한 서버에서 장애가 발생하는 경우, 클라이언트에서 사용하는 백업 서버 목록을 구성하는 것이 좋습니다. 서버에서 오류가 발생하는 경우, 클라이언트는 목록의 맨 위에 있는 서버에 연결을 시도한 후 필요시 목록 아래로 이동시킵니다.

참고 반면 AnyConnect 프로파일 편집기, 백업 서버, 98 페이지에 구성된 백업 서버는 모든 연결 항목에 대한 글로벌 항목입니다. 백업 서버 위치에 저장한 모든 항목은 개별 서버 목록 항목으로 여기에 입력하는 항목으로 덮어쓰기 됩니다. 이 설정이 우선적으로 적용되며 권장 방식입니다.

- **Host Address(**호스트 주소**)**— 백업 서버 목록에 포함되도록 IP 주소 또는 FQDN을 지정합니다. 클라이언트에서 호스트에 연결할 수 없는 경우 백업 서버에 연결을 시도합니다.
- **Add(**추가**)**— 백업 서버 목록에 호스트 주소를 추가합니다.
- **Move Up(**위로 이동**)**— 선택한 백업 서버를 목록에서 위로 이동시킵니다. 사용자가 선택한 서버에서 오류가 발생하는 경우, 클라이언트는 목록의 맨 위에 있는 백업 서버에 연결을 시도한 후 필요시 목록 아래로 이동시킵니다.
- **Move Down(**아래로 이동**)**— 선택한 백업 서버를 목록에서 아래로 이동시킵니다.
- **Delete(**삭제**)**— 서버 목록에서 백업 서버를 제거합니다.

- **Load Balancing Server List(**로드 밸런싱 서버 목록**)**

  이 서버 목록 항목에 대한 호스트가 보안 어플라이언스의 로드 밸런싱 클러스터이며 상시 가동 기능이 활성화되어 있는 경우 이 목록에서 클러스터의 백업 디바이스를 지정하십시오. 이렇게 하지 않으면 상시 가동은 로드 밸런싱 클러스터에 있는 백업 디바이스에 대한 액세스를 차단합니다.

  - **Host Address(**호스트 주소**)**— 로드 밸런싱 클러스터에 있는 백업 디바이스의 IP 주소 또는 FQDN을 지정합니다.
  - **Add(**추가**)**— 로드 밸런싱 백업 서버 목록에 주소를 추가합니다.
  - **Delete(**삭제**)**— 목록에서 로드 밸런싱 백업 서버를 제거합니다.

- **Primary Protocol(**기본 프로토콜**)**— 이 서버에 연결하려면 SSL 또는 IKEv2를 지원하는 IPsec 중 하나를 프로토콜로 지정합니다. 기본값은 SSL입니다.
  - **Standard Authentication Only(**표준 인증 전용**)(IOS** 게이트웨이**)**— IPsec을 프로토콜로 선택한 경우, IOS 서버에 연결하기 위한 인증 방법을 제한하려면 이 옵션을 선택할 수 있습니다.

    참고 이 서버가 ASA인 경우, 인증 방법을 전용 AnyConnect EAP에서 표준 기반 방법으로 변경하면 세션 시간 제한, 유휴 시간 제한, 연결 끊김 시간 제한, 스플릿 터널링, 스플릿 DNS, MSIE 프록시 구성 및 기타 기능을 구성하기 위한 ASA 기능을 사용할 수 없습니다.

  - **Auth Method During IKE Negotiation(IKE** 협상 중 인증 방법**)** 표준 기반 인증 방법 중 하나를 선택합니다.

- **IKE Identity(IKE ID)**— 표준 기반 EAP 인증 방법을 선택하는 경우, 그룹 또는 도메인을 이 필드에 있는 클라이언트 ID로 입력할 수 있습니다. 클라이언트는 문자열을 ID_GROUP 유형 IDi 페이로드로 전송합니다. 기본적으로 문자열은 *$AnyConnectClient$* 입니다.

- **Automatic SCEP Host(**자동 **SCEP** 호스트**)** — 이 호스트는 레거시 SCEP용으로 사용됩니다.
- **CA URL**— SCEP CA 서버의 URL을 지정합니다. FQDN 또는 IP 주소를 입력합니다. 예를 들어 http://ca01.cisco.com을 입력합니다.
- **Certificate Pins(**인증서 고정**)** - 고정 확인 중에 클라이언트에서 사용하는 호스트별 고정입니다. AnyConnect 프로파일 편집기, 인증서 고정, 103 페이지을 참조하십시오.
- **Prompt For Challenge PW(**시도용 비밀번호 프롬프트**)**— 사용자가 인증서 요청을 수동으로 생성하도록 허용할 때 사용합니다. 사용자가 Get Certificate(인증서 가져오기)를 클릭할 경우, 클라이언트에서 사용자에게 사용자 이름 및 일회용 비밀번호를 입력하도록 프롬프트를 표시합니다.
- **CA Thumbprint(CA** 지문**)**— CA의 인증서 지문입니다. SHA1 또는 MD5 해시를 사용하십시오.

참고 CA 서버 관리자는 CA URL 및 지문을 제공할 수 있습니다. thumbprint(지문)는 발급한 인증서의 “fingerprint(지문)" 또는 "thumbprint(지문)" 특성 필드가 아니라 서버에서 직접 검색해야 합니다.

관련 항목

VPN 연결 서버 구성, 119 페이지

AnyConnect 프로파일 편집기, 모바일 설정

Apple iOS/Android 설정

- **Certificate Authentication(**인증서 인증**)** - 연결 항목과 연관된 인증서 인증 정책 특성에서 연결에 대해 인증서를 처리하는 방식을 지정합니다. 유효한 값은 다음과 같습니다.
  - **Automatic(**자동**)**— AnyConnect가 연결을 설정할 때 인증할 클라이언트 인증서를 자동으로 선택합니다. 이 경우 AnyConnect는 설치된 모든 인증서를 확인하고 오래된 인증서를 무시하며 VPN 클라이언트 프로파일에 정의된 인증서 일치 기준을 적용한 다음 기준과 일치하는 인증서를 사용하여 인증합니다. 디바이스 사용자가 VPN 연결을 설정하려고 시도할 때마다 이 과정이 수행됩니다.
  - **Manual(**수동**)**— AnyConnect는 프로파일이 다운로드될 때 Android 디바이스에 있는 AnyConnect 인증서 저장소에서 인증서를 검색하고 다음 작업 중 한 가지를 수행합니다.
    - AnyConnect가 VPN 클라이언트 프로파일에 정의된 인증서 일치 기준에 따라 인증서를 찾는 경우, 연결을 설정할 때 이 인증서를 연결 항목에 할당하고 해당 인증서를 사용합니다.

- 일치 인증서를 찾을 수 없는 경우, 인증서 인증 정책은 자동으로 설정됩니다.
- 할당된 인증서가 AnyConnect 인증서 저장소에서 제거된 경우, AnyConnect는 인증서 인증 정책을 Automatic(자동)으로 재설정합니다.

- **Disabled(**비활성화**)**— 클라이언트 인증서를 인증용으로 사용하지 않습니다.

- **Make this Server List Entry active when profile is imported(**프로파일을 가져올 때 이 서버 목록 항목 활성화**)**— VPN 프로파일을 이 디바이스에 다운로드한 이후에는 서버 목록 항목을 기본 연결로 정의합니다. 하나의 서버 목록 항목만 이렇게 지정할 수 있습니다. 기본값은 비활성화입니다.

Apple iOS 전용 설정

- **Reconnect when roaming between 3G/Wifi networks(3G/Wifi** 네트워크에서 로밍 시 다시 연결**)**— 이 옵션이 사용 가능한 경우(기본값), AnyConnect는 연결이 끊긴 이후, 디바이스의 절전이 해제된 이후 또는 연결 유형(예: EDGE(2G), 1xRTT(2G), 3G 또는 Wi-Fi)에서 변경사항이 발생한 이후에 다시 연결을 시도하는 데 걸리는 시간을 제한하지 않습니다. 이 기능은 네트워크를 통해 지속적인 보안 연결이 가능한 원활한 이동성을 제공합니다. 기업과 연결을 유지해야 하는 애플리케이션에 유용한 기능이지만 배터리 수명을 더 많이 소모합니다.

  네트워크 로밍을 사용할 수 없고 AnyConnect의 연결이 끊길 경우, 필요시 최대 20초 동안 연결 재설정을 시도합니다. 연결을 다시 설정할 수 없는 경우, 필요시 디바이스 사용자 또는 애플리케이션은 새로운 VPN 연결을 시작해야 합니다.

  참고 네트워크 로밍은 데이터 로밍 또는 여러 모바일 서비스 공급자 사용에 영향을 주지 않습니다.

- **Connect on Demand(**온디맨드 연결**)(**인증서 권한 부여 필요**)**— 이 필드에서 Apple iOS가 제공하는 온디맨드 연결 기능을 구성할 수 있습니다. 다른 애플리케이션에서 DNS(Domain Name System, 도메인 이름 시스템)를 사용하여 확인되는 네트워크 연결을 시작할 때마다 검사되는 규칙 목록을 생성할 수 있습니다.

  인증서 인증 필드가 Manual(수동) 또는 Automatic(자동)으로 설정된 경우에만 Connect on Demand(온디맨드 연결) 옵션이 사용됩니다. Certificate Authentication(인증서 인증) 필드가 Disabled(비활성화)로 설정되어 있는 경우에는 이 체크 박스가 흐리게 표시됩니다. 체크 박스가 흐리게 표시되는 경우에도 Match Domain or Host(도메인 또는 호스트 일치) 및 On Demand Action(온디맨드 작업) 필드에 정의되어 있는 온디맨드 연결 규칙을 구성 및 저장할 수 있습니다.

- **Match Domain or Host(**도메인 또는 호스트 일치**)**— 온디맨드 연결 규칙을 생성할 호스트 이름(host.example.com), 도메인 이름(.example.com) 또는 부분 도메인(.internal.example.com)을 입력합니다. 이 필드에 IP 주소(10.125.84.1)를 입력하지 마십시오.

- **On Demand Action(**온디맨드 작업**)**디바이스 사용자가 이전 단계에서 정의된 도메인 또는 호스트에 연결하려고 시도할 경우, 다음 작업 중 하나를 지정합니다.

- **Never connect(**연결 안 함**)** - iOS는 이 목록에 있는 규칙이 일치하는 경우, VPN 연결을 시작하지 않습니다. 이 목록에 있는 규칙은 기타 모든 목록보다 우선시됩니다.

  참고 Connect on Demand(온디맨드 연결)가 사용 가능한 경우, 애플리케이션은 서버 주소를 이 목록에 자동으로 추가합니다. 이렇게 하면 웹 브라우저를 사용하여 서버의 클라이언트리스 포털에 액세스를 시도할 경우, VPN 연결이 자동으로 설정되는 것을 방지합니다. 이 동작을 설정하지 않으려면 해당 규칙을 제거하십시오.

- **Connect if Needed(**필요시 연결**)** - iOS는 시스템이 DNS를 사용하여 주소를 확인할 수 없는 경우에만 이 목록에 있는 규칙이 일치할 때 VPN 연결을 시작합니다.
- **Always Connect(**항상 연결**)**— 항상 연결 동작은 릴리스마다 다릅니다.
  - Apple iOS 6에서 iOS는 이 목록에 있는 규칙이 일치하는 경우, 항상 VPN 연결을 시작합니다.
  - iOS 7.x에서 Always Connect가 지원되지 않는 경우, 이 목록에 있는 규칙이 일치할 때 필요시 연결 규칙으로 동작합니다.
  - 최신 릴리스에서 Always Connect가 사용되지 않는 경우, 구성된 규칙은 필요시 연결 목록으로 이동되어 그에 따라 동작합니다.

- **Add or Delete(**추가 또는 삭제**)** - Match Domain or Host(도메인 또는 호스트 일치) 및 On Demand Action(온디맨드 작업) 필드에 지정된 규칙을 규칙 테이블에 추가하거나 선택한 규칙을 규칙 테이블에서 삭제합니다.

AnyConnect 로컬 정책

AnyConnectLocalPolicy.xml은 보안 설정을 포함하는 클라이언트에 대한 XML 파일입니다. 이 파일은 ASA를 통해 구축되지 않습니다. 수동으로 설치하거나 엔터프라이즈 소프트웨어 구축 시스템을 사용하는 사용자 컴퓨터에 구축해야 합니다. 사용자 시스템에 있는 기존 로컬 정책 파일에 변경사항이 있는 경우, 시스템을 재부팅해야 합니다.

로컬 정책 파라미터 및 값

다음 파라미터는 VPN 로컬 정책 편집기 및 `AnyConnectLocalPolicy.xml` 파일에 있는 요소입니다. XML 요소는 꺾쇠괄호로 표시됩니다.

참고 수동으로 파일을 편집하고 정책 파라미터를 생략할 경우, 이 기능은 기본 동작을 활용합니다.

- <acversion>

이 파일의 모든 파라미터를 해석할 수 있는 AnyConnect 클라이언트의 최소 버전을 지정합니다. 이 버전보다 오래된 AnyConnect 버전을 실행 중인 클라이언트가 파일을 읽는 경우, 이벤트 로그 경고를 생성합니다.

형식은 acversion="<version number>"입니다.

- **FIPS Mode(FIPS** 모드**)** <FipsMode>

  클라이언트에 대해 FIPS 모드를 활성화합니다. 이 설정에 따라 클라이언트는 FIPS 표준에서 승인한 알고리즘 및 프로토콜만 사용해야 합니다.

- **Bypass Downloader(**우회 다운로더**)** <BypassDownloader>

  이 파라미터를 선택한 경우, 동적 콘텐츠의 존재 탐지 및 로컬 버전 업데이트를 수행하는 VPNDownloader.exe 모듈 시작을 비활성화합니다. 클라이언트는 변환, 사용자 정의, 선택적 모듈 및 코어 소프트웨어 업데이트를 포함하여 ASA에 존재하는 동적 콘텐츠를 확인하지 않습니다.

  Bypass Downloader(우회 다운로더)를 선택한 경우 클라이언트가 ASA에 연결되는 즉시 다음 두 가지 사항 중 한 가지가 발생합니다.

  - ASA에 있는 VPN 클라이언트 프로파일이 클라이언트에 있는 프로파일과 다른 경우, 클라이언트는 연결 시도를 중단합니다.
  - ASA에 VPN 클라이언트 프로파일이 없는 경우, 클라이언트는 VPN 연결을 수행하지만 하드 코드된 VPN 클라이언트 프로파일 설정을 사용합니다.

  참고 ASA에 VPN 클라이언트 프로파일을 구성한 경우, BypassDownloader가 참으로 설정된 상태로 클라이언트가 ASA에 연결되기 전에 클라이언트에 해당 프로파일이 설치되어야 합니다. 프로파일에 관리자 정의 정책을 포함할 수 있으므로 클라이언트 프로파일을 중앙에서 관리하기 위해 ASA를 사용하지 않는 경우, BypassDownloader의 true 설정만 권장됩니다.

- **Enable CRL Check(CRL** 확인 활성화**)**<EnableCRLCheck>

  이 기능은 *Windows* 데스크톱에 대해서만 구현됩니다. SSL 및 IPsec VPN 연결 둘 다에 대해 CRL(인증서 해지 목록) 확인을 수행할 수 있습니다. 이 설정을 활성화하면 AnyConnect는 체인의 모든 인증서에 대해 업데이트된 CRL을 검색합니다. 그런 다음 AnyConnect는 해당하는 인증서가 더 이상 신뢰해서는 안 되는 해지된 인증서 중에 포함되어 있는지 여부를 확인하고, 이 인증서가 CA(인증 기관)에서 해지한 인증서로 확인되면 연결하지 않습니다.

  CRL 확인은 기본적으로 비활성화됩니다. AnyConnect는 Enable CRL Check(CRL 확인 활성화)를 선택하거나 활성화하는 경우에만 CRL 확인을 수행하므로 최종 사용자에게 다음과 같은 결과가 발생할 수 있습니다.

  - CRL을 통해 인증서를 해지하는 경우 AnyConnect 로컬 정책 파일에서 Strict Certificate Trust(엄격한 인증서 신뢰)를 비활성화하더라도 보안 게이트웨이에 대한 연결이 무조건 실패합니다.
  - CRL 배포 포인트에 연결할 수 없는 등의 원인으로 인해 CRL을 검색할 수 없는 경우 AnyConnect 로컬 정책 파일에서 Strict Certificate Trust(엄격한 인증서 신뢰)를 활성화하면 보

안 게이트웨이에 대한 연결이 무조건 실패합니다. Strict Certificate Trust(엄격한 인증서 신뢰)를 비활성화하는 경우에는 오류를 우회하라는 메시지가 사용자에게 표시될 수 있습니다.

참고 AnyConnect는 Always-On이 활성화되어 있으면 CRL 확인을 수행할 수 없습니다. 또한 CRL 배포 포인트에 공개적으로 연결할 수 없으면 AnyConnect에서 서비스가 중단될 수 있습니다.

- **Restrict Web Launch(**웹 실행 제한**)**<RestrictWebLaunch>

  WebLaunch를 시작하기 위해 사용자가 FIPS 규정을 준수하지 않는 브라우저를 사용하는 것을 방지합니다. 이를 위해 클라이언트가 AnyConnect 터널을 시작하는 데 사용되는 보안 쿠키 획득을 방지하는 방법을 사용합니다. 클라이언트는 사용자에게 정보 메시지를 표시합니다.

- **Strict Certificate Trust(**엄격한 인증서 신뢰**)**<StrictCertificateTrust>

  이 파라미터를 선택한 경우, 원격 보안 게이트웨이를 인증할 때 AnyConnect는 확인할 수 없는 모든 인증서를 허용하지 않습니다. 이러한 인증서를 수락하도록 사용자에게 프롬프트를 표시하지 않고 대신 클라이언트는 자체 서명된 인증서를 사용하여 보안 게이트웨이 연결에 실패하고 `Local policy prohibits the acceptance of untrusted server certificates. A connection will not be established.`라고 표시합니다. 이 파라미터를 선택하지 않은 경우, 클라이언트는 사용자에게 인증서를 수락하라는 프롬프트를 표시합니다. 이는 기본 동작입니다.

  다음과 같은 이유로 인해 AnyConnect 클라이언트에 대해 엄격한 인증서 신뢰를 활성화하는 것이 좋습니다.

  - 대상이 있는 악용이 증가함에 따라 로컬 정책에서 엄격한 인증서 신뢰를 활성화하면 사용자가 공용 액세스 네트워크와 같이 신뢰할 수 없는 네트워크에서 연결 중인 경우 "중간자" 공격을 방지하는 데 도움이 됩니다.
  - 완전히 확인 가능하고 신뢰할 수 있는 인증서를 사용하는 경우에도 AnyConnect 클라이언트는 기본적으로 최종 사용자가 확인 불가능한 인증서를 수락하는 것을 허용합니다. 최종 사용자가 중간자 공격의 영향을 받는 경우, 악의적인 인증서를 수락하라는 프롬프트가 표시될 수 있습니다. 최종 사용자의 이 결정 사항을 제거하려면 엄격한 인증서 신뢰를 활성화합니다.

- **Restrict Preference Caching(**환경 설정 캐싱 제한**)** <RestrictPreferenceCaching>

  설계에 따라 AnyConnect는 디스크에 민감한 정보를 캐시하지 않습니다. 이 파라미터를 활성화하면 AnyConnect 기본 설정에 저장된 모든 유형의 사용자 정보로 이 정책을 확장합니다.

  - Credentials(자격 증명) — 해당 사용자 이름과 두 번째 사용자 이름은 캐시되지 않습니다.
  - Thumbprints(지문) — 클라이언트와 서버 인증서 지문이 캐시되지 않습니다.
  - CredentialsAndThumbprints — 인증서 지문과 사용자 이름이 캐시되지 않습니다.
  - All(모두) — 자동 환경 설정은 캐시되지 않습니다.
  - false(거짓) — 모든 환경 설정은 디스크에 기록됩니다(기본값).

- **Exclude Pem File Cert Store(PEM** 파일 인증서 저장소 제외**)** (Linux 및 macOS) <ExcludePemFileCertStore>

  클라이언트가 서버 인증서를 확인하고 클라이언트 인증서를 검색하기 위해 PEM 파일 인증서 저장소를 사용하는 것을 방지합니다.

  이 저장소는 FIPS 인증 OpenSSL을 사용하며 클라이언트 인증서 인증을 위해 인증서를 얻는 위치에 대한 정보를 지니고 있습니다. PEM 파일 인증서 저장소에서 원격 사용자가 FIPS 규정 준수 인증서 저장소를 사용하는지 확인하도록 허용합니다.

- **Exclude Mac Native Cert Store(Mac** 기본 인증서 저장소 제외**)**(macOS만 해당) <ExcludeMacNativeCertStore>

  클라이언트가 서버 인증서를 확인하고 클라이언트 인증서를 검색하기 위해 Mac 네이티브(키 집합) 인증서 저장소를 사용하는 것을 방지합니다.

- **Exclude Firefox NSS Cert Store(Firefox NSS** 인증서 저장소 제외**)**(Linux 및 macOS) <ExcludeFirefoxNSSCertStore>

  클라이언트가 서버 인증서를 확인하고 클라이언트 인증서를 검색하기 위해 Firefox NSS 인증서 저장소를 사용하는 것을 방지합니다.

  이 저장소에는 클라이언트 인증서 인증을 위해 인증서를 얻는 위치에 대한 정보가 있습니다.

- **Update Policy(**업데이트 정책**)**<UpdatePolicy>

  어떤 헤드엔드에서 클라이언트가 소프트웨어 또는 프로파일 업데이트를 얻을 수 있는지 제어합니다.

  - **Allow Software Updates From AnyServer(**모든 서버에서 소프트웨어 업데이트 허용**)** <AllowSoftwareUpdatesFromAnyServer>

    무단 서버(서버 이름 목록에 나열되지 않은 서버)에서 VPN 코어 모듈 및 기타 선택적인 모듈의 소프트웨어 업데이트를 허용 또는 허용하지 않습니다.

  - **Allow VPN Profile Updates From AnyServer(**모든 서버에서 **VPN** 프로파일 업데이트 허용**)** <AllowVPNProfileUpdatesFromAnyServer>

    무단 서버(서버 이름 목록에 나열되지 않은 서버)에서 VPN 프로파일 업데이트를 허용 또는 허용하지 않습니다.

  - **Allow Service Profile Updates From AnyServer(**모든 서버에서 서비스 프로파일 업데이트 허용**)** <AllowServiceProfileUpdatesFromAnyServer>

    무단 서버(서버 이름 목록에 나열되지 않은 서버)에서 기타 서비스 모듈 프로파일 업데이트를 허용 또는 허용하지 않습니다.

  - **Allow ISE Posture Profile Updates From Any Server(**모든 서버에서 **ISE Posture** 프로파일 업데이트 허용**)**<AllowISEProfileUpdatesFromAnyServer>

    무단 서버(서버 이름 목록에 나열되지 않은 서버)에서 ISE Posture 프로파일 업데이트를 허용 또는 허용하지 않습니다.

  - **Allow Compliance Module Updates From Any Server(**모든 서버에서 규정 준수 모듈 업데이트 허용**)**<AllowComplianceModuleUpdatesFromAnyServer>

무단 서버(서버 이름 목록에 나열되지 않은 서버)에서 규정 준수 모듈 업데이트를 허용 또는 허용하지 않습니다.

- **Server Name(**서버 이름**)** <ServerName>

  이 목록에서 권한 있는 서버를 지정합니다. 이 헤드엔드는 VPN 연결 시 모든 AnyConnect 소프트웨어 및 프로파일 전체를 업데이트할 수 있습니다. ServerName은 도메인 이름을 가진 FQDN, IP 주소, 도메인 이름 또는 와일드카드일 수 있습니다.

관련 주제: 업데이트 정책 설정

로컬 정책 파라미터 수동으로 변경

프로시저

단계 **1** 클라이언트 설치에서 AnyConnect 로컬 정책 파일(AnyConnectLocalPolicy.xml)의 복사본을 검색합니다.

표 *7:* 운영 체제 및 ***AnyConnect*** 로컬 정책 파일 설치 경로

운영 체제	설치 경로
Windows	C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client
Linux	/opt/cisco/anyconnect
macOS	/opt/cisco/anyconnect

단계 **2** 파라미터 설정을 편집합니다. AnyConnectLocalPolicy 파일을 수동으로 편집하거나 AnyConnect 프로파일 편집기 설치 프로그램을 통해 배포한 VPN 로컬 정책 편집기를 사용합니다.

단계 **3** 파일을 `AnyConnectLocalPolicy.xml` 로 저장하고 기업 소프트웨어 구축 시스템을 사용하여 원격 컴퓨터에 파일을 구축합니다.

단계 **4** 로컬 정책 파일에 변경사항을 적용하려면 원격 컴퓨터를 재부팅하십시오.

MST 파일에서 로컬 정책 파라미터 활성화

설정할 설명 및 값은 로컬 정책 파라미터 및 값 을 참조하십시오.

로컬 정책 매개변수를 변경하려면 MST 파일을 생성하십시오. MST 매개변수 이름은 AnyConnect 로컬 정책 파일(AnyConnectLocalPolicy.xml)에 있는 매개변수와 일치해야 합니다.

- LOCAL_POLICY_BYPASS_DOWNLOADER
- LOCAL_POLICY_FIPS_MODE

- LOCAL_POLICY_RESTRICT_PREFERENCE_CACHING
- LOCAL_POLICY_RESTRICT_TUNNEL_PROTOCOLS
- LOCAL_POLICY_RESTRICT_WEB_LAUNCH
- LOCAL_POLICY_STRICT_CERTIFICATE_TRUST

참고 AnyConnect 설치 시 사용자 컴퓨터의 기존 로컬 정책 파일이 자동으로 덮어쓰기되지 않습니다. 사용자 컴퓨터의 기존 정책 파일을 먼저 삭제해야 클라이언트 설치 프로그램이 새 정책 파일을 생성할 수 있습니다.

참고 로컬 정책 파일에 모든 변경 사항을 적용하려면 시스템을 재부팅해야 합니다.

FIPS 활성화 툴을 사용하여 로컬 정책 파라미터 활성화

모든 운영 체제에서 Cisco의 FIPS 활성화 툴을 사용하여 FIPS가 활성화된 AnyConnect 로컬 정책 파일을 생성할 수 있습니다. FIPS 활성화 툴은 Windows에서 관리자 권한을 사용하여 실행하거나 Linux와 macOS에서 루트 사용자로 실행하는 커맨드 라인 툴입니다.

FIPS 활성화 툴을 다운로드할 수 있는 위치에 관한 자세한 내용은 FIPS 클라이언트에 대한 라이선스 정보를 참조하십시오.

컴퓨터의 커맨드 라인에서 EnableFIPS 명령 <arguments>를 입력하여 FIPS 활성화 툴을 실행합니다. 다음과 같은 사용 노트가 FIPS 활성화 툴에 적용됩니다.

- 인수를 제공하지 않는 경우 툴이 FIPS를 활성화하고 vpnagent 서비스(Windows의 경우) 또는 vpnagent 데몬(macOS 및 Linux의 경우)을 다시 시작합니다.
- 공백을 사용하여 여러 인수를 구분하십시오.

다음 예는 Windows 컴퓨터에서 실행되는 FIPS 활성화 툴 명령을 보여줍니다.

```
EnableFIPS rwl=false sct=true bd=true fm=false
```

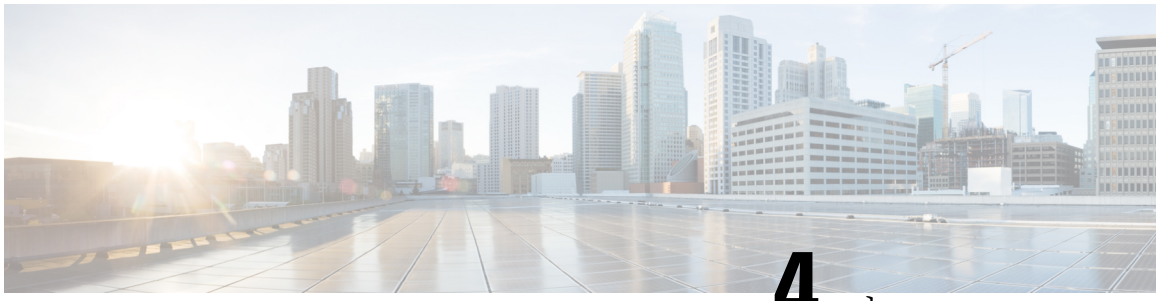
다음 예는 Linux 또는 macOS 컴퓨터에서 실행되는 명령을 보여줍니다.

```
./EnableFIPS rwl=false sct=true bd=true fm=false
```

다음 표에서는 FIPS 활성화 툴을 통해 구성할 수 있는 정책 설정을 보여줍니다. 인수는 AnyConnect 로컬 정책 파일의 파라미터와 일치합니다.

정책 설정	인수 및 구문
FIPS mode(FIPS 모드)	fm=[true | false]

정책 설정	인수 및 구문
Bypass downloader(우회 다운로더)	bd=[true | false]
Restrict weblaunch(WebLaunch 제한)	rwl=[true | false]
Strict certificate trust(엄격한 인증서 신뢰)	sct=[true | false]
Restrict preferences caching(환경 설정 캐시 제한)	rpc=[Credentials | Thumbprints | CredentialsAndThumbprints | All | false]
Exclude FireFox NSS certificate store(FireFox NSS 인증서 저장소 제외) (Linux 및 macOS)	efn=[true | false]
Exclude PEM file certificate store(PEM 파일 인증서 저장소 제외)(Linux 및 macOS)	epf=[true | false]
Exclude Mac native certificate store(Mac 기본 인증서 저장소 제외)(macOS만 해당)	emn=[true | false]



4 장

VPN 액세스 구성

VPN을 통한 연결 및 연결 끊기

AnyConnect VPN 연결 옵션

AnyConnect 클라이언트는 VPN 세션을 자동으로 연결, 다시 연결 또는 연결 해제할 수 있는 여러 옵션을 제공합니다. 이러한 옵션은 사용자에게 VPN에 연결할 수 있는 편리한 방법을 제공하고 네트워크 보안 요건을 지원합니다.

AnyConnect 연결 시작 및 재시작

사용자가 수동으로 연결할 보안 게이트웨이의 이름과 주소를 제공하도록 VPN 연결 서버 구성 하십시오.

편리한 자동 VPN 연결을 제공하려면 다음 AnyConnect 기능을 선택하십시오.

- 로그온 전 Windows VPN 연결 자동 시작
- AnyConnect 시작 시 자동으로 VPN 연결 시작
- 자동으로 VPN 연결 재시작

또한 더 높은 수준의 네트워크 보안을 실행하거나 VPN에 대한 네트워크 액세스만 제한하려면 다음 자동 VPN 정책을 사용하십시오.

- 신뢰할 수 있는 네트워크 탐지 정보
- 상시 가동을 사용하는 VPN 연결 필요
- 종속 포털 핫스팟 탐지 및 보안정책 교정 사용

AnyConnect 연결 재협상 및 유지 관리

작업이 없는 경우에도 ASA에서 사용자가 이용할 수 있는 AnyConnect VPN 연결을 유지하는 시간을 정할 수 있습니다. VPN 세션이 유휴 상태인 경우, 연결을 종료하거나 재협상할 수 있습니다.

- Keepalive(킵얼라이브) - ASA가 킵얼라이브 메시지를 정기적으로 전송합니다. 이 메시지는 ASA에 의해 무시되지만 클라이언트와 ASA 간의 디바이스를 사용하여 연결을 유지 관리하는 데 유용합니다.

  ASDM 또는 CLI를 사용하여 Keepalive를 구성하는 지침은 Cisco ASA Series VPN 환경 설정 가이드의 *Keepalive* 활성화 섹션을 참조하십시오.

- Dead Peer Detection(데드 피어 탐지) - ASA 및 AnyConnect 클라이언트가 "R-U-There" 메시지를 전송합니다. 이 메시지는 IPsec의 킵얼라이브 메시지보다 전송 빈도가 낮습니다. ASA(게이트웨이) 및 AnyConnect 클라이언트가 모두 DPD 메시지를 전송할 수 있도록 설정하고 시간 제한 간격을 구성할 수 있습니다.

  - 클라이언트가 ASA의 DPD 메시지에 응답하지 않는 경우, ASA는 세션을 "Waiting to Resume(재개 대기 중)" 모드로 전환하기 전에 한 번 더 시도합니다. 이 모드를 통해 사용자는 네트워크를 로밍하거나 절전 모드로 전환하여 나중에 연결을 복구할 수 있습니다. 유휴 시간 제한이 발생하기 전에 사용자가 다시 연결하지 않으면 ASA가 터널을 종료합니다. 권장되는 게이트웨이 DPD 간격은 300초입니다.

  - ASA가 클라이언트의 DPD 메시지에 응답하지 않는 경우, 클라이언트는 터널을 종료하기 전에 다시 시도합니다. 권장되는 게이트웨이 DPD 간격은 30초입니다.

    ASDM 내에서 DPD를 구성하는 지침은 Cisco ASA Series VPN 환경 설정 가이드의 해당 릴리스에서 데드 피어 탐지 구성을 참조하십시오.

- 권장 방법:

  - Group Policy(그룹 정책) > Advanced(고급) > AnyConnect Client(AnyConnect 클라이언트) > Dead Peer Detection(데드 피어 탐지)에서 클라이언트 DPD를 30초로 설정하십시오.

  - Group Policy(그룹 정책) > Advanced(고급) > AnyConnect Client(AnyConnect 클라이언트) > Dead Peer Detection(데드 피어 탐지)에서 서버 DPD를 300초로 설정하십시오.

  - Group Policy(그룹 정책) > Advanced(고급) > AnyConnect Client(AnyConnect 클라이언트) > Key Regeneration(키 다시 생성)에서 SSL과 IPsec의 Rekey(키 교체)를 1시간으로 설정하십시오.

AnyConnect 연결 종료

AnyConnect 연결을 종료하려면 사용자가 보안 게이트웨이에 대한 엔드포인트를 다시 인증하고 새 VPN 연결을 생성해야 합니다.

다음 연결 파라미터는 시간 제한을 기준으로 하여 VPN 세션을 종료합니다.

- Maximum Connect Time(최대 연결 시간) - 최대 사용자 연결 시간을 분 단위로 설정합니다. 이 시간이 경과하면 연결이 자동으로 종료됩니다. 무제한 연결 시간(기본값)을 허용할 수도 있습니다.

- VPN 유휴 시간 제한 - 지정된 시간 동안 세션이 비활성화될 때 사용자의 세션을 종료합니다. VPN 유휴 시간 제한을 구성하지 않으면 기본 유휴 시간 제한이 사용됩니다.
- Default 유휴 시간 제한 - 지정된 시간 동안 세션이 비활성화될 때 사용자의 세션을 종료합니다. 기본값은 30분입니다. 기본값은 1800초입니다.

이러한 파라미터를 설정하려면 Cisco ASA Series VPN 환경 설정 가이드의 해당 릴리스에서 그룹 정책에 대해 *VPN* 세션 유휴 시간 제한 지정 섹션을 참조하십시오.

VPN 연결 서버 구성

AnyConnect VPN 서버 목록은 VPN 사용자가 연결할 보안 게이트웨이를 식별하는 호스트 이름과 호스트 주소 쌍으로 구성됩니다. 호스트 이름은 별칭, FQDN 또는 IP 주소일 수 있습니다.

서버 목록에 추가된 호스트는 AnyConnect GUI의 연결 드롭다운 목록에 표시됩니다. 그런 다음 사용자는 VPN 연결을 시작하도록 드롭다운 목록에서 선택할 수 있습니다. 목록의 맨 위에 있는 호스트는 기본 서버로, GUI 드롭다운 목록에서 맨 먼저 표시됩니다. 이 목록에서 대체 서버를 선택하면 선택한 서버는 새 기본 서버가 됩니다.

일단 서버 목록에 서버를 추가한 후에는 세부사항을 보고 서버 항목을 편집하거나 삭제할 수 있습니다. 서버 목록에 서버를 추가하려면 다음 절차를 따르십시오.

프로시저

단계 **1** VPN 프로파일 편집기를 열고 탐색 창에서 **Server List(**서버 목록**)** 를 선택합니다.

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** 서버의 호스트 이름 및 주소를 다음과 같이 구성합니다.

a) 호스트, FQDN 또는 IP 주소를 나타내기 위해 사용되는 별칭인 **Host Display Name(**호스트 표시 이름**)**을 입력합니다. 이름에 "&" 또는 "<" 문자를 사용하지 마십시오. FQDN 또는 IP 주소를 입력한 경우, 다음 단계에서 **FQDN** 또는 **IP Address(IP** 주소**)** 를 입력할 필요가 없습니다.

IP 주소를 입력한 경우, 보안 게이트웨이의 공용 IPv4 또는 전역 IPv6 주소를 사용합니다. 링크-로컬 보안 게이트웨이 주소 사용은 지원되지 않습니다.

b) 호스트 표시 이름에 입력하지 않은 경우 호스트의 **FQDN** 또는 **IP Address(IP** 주소**)** 를 입력합니다(선택 사항).

c) **User Group(**사용자 그룹**)**을 지정합니다(선택 사항).

AnyConnect는 사용자 그룹과 함께 FQDN 또는 IP 주소를 사용하여 그룹 URL을 구성합니다.

단계 **4** **Backup Server List(**백업 서버 목록**)**에 백업 서버로 대체할 서버를 입력합니다. 이름에 "&" 또는 "<" 문자를 사용하지 마십시오.

참고 반면 Server(서버) 메뉴의 Backup Server(백업 서버) 탭에 입력하는 내용은 모든 연결 항목에 대한 글로벌 항목입니다. Backup Server(백업 서버) 위치에 저장한 모든 항목은 개별 서버 목록 항목으로 여기에 입력하는 항목으로 덮어쓰기됩니다. 이 설정이 우선적으로 적용되며 권장 방식입니다.

단계 **5** (선택 사항) **Load Balancing Server List(**로드 밸런싱 서버 목록**).**에 로드 밸런싱 서버를 추가합니다. 이름에 "&" 또는 "<" 문자는 사용하지 마십시오.

이 서버 목록 항목에 대한 호스트가 보안 어플라이언스의 로드 밸런싱 클러스터를 지정하는 경우 상시 가동 기능이 활성화되어 있으면 클러스터의 로드 밸런싱 디바이스를 이 목록에 추가합니다. 이렇게 하지 않으면 상시 가동 은 로드 밸런싱 클러스터에 있는 디바이스에 대한 액세스를 차단합니다.

단계 **6** 클라이언트가 이 ASA에 사용할 수 있도록 **Primary Protocol(**기본 프로토콜**)** 을 지정하십시오.

a) SSL(기본값) 또는 IPsec을 선택합니다.

IPsec을 지정한 경우 사용자 그룹은 연결 프로파일(터널 그룹)의 정확한 이름이어야 합니다. SSL의 경우 사용자 그룹은 연결 프로파일의 그룹 URL 또는 그룹 별칭입니다.

b) IPsec을 지정한 경우 **Standard Authentication Only(**표준 인증 전용**)** 를 선택하여 기본 인증 방법(전용 AnyConnect EAP)을 비활성화하고 드롭다운 목록에서 방법을 선택합니다.

참고 전용 AnyConnect EAP에서 표준 기반 방법으로 인증 방법을 변경하면 세션 시간 제한, 유휴 시간 제한, 연결 끊김 시간 제한, 스플릿 터널링, 스플릿 DNS, MSIE 프록시 구성 및 기타 기능을 구성하기 위한 ASA 기능이 비활성화됩니다.

단계 **7** 다음과 같이 이 서버에 대해 SCEP를 구성하십시오(선택 사항).

a) SCEP CA 서버의 URL을 지정합니다. FQDN 또는 IP 주소를 입력합니다. 예를 들어 http://ca01.cisco.com을 입력합니다.

b) 사용자가 인증서 요청을 수동으로 생성하도록 활성화하려면 **Prompt For Challenge PW(**시도용 비밀번호 프롬프트**)** 를 선택합니다. 사용자가 **Get Certificate(**인증서 가져오기**)**를 클릭할 경우, 클라이언트에서 사용자에게 사용자 이름 및 일회용 비밀번호를 입력하도록 프롬프트를 표시합니다.

c) CA의 인증서 지문을 입력합니다. SHA1 또는 MD5 해시를 사용하십시오. CA 서버 관리자는 CA URL 및 지문을 제공할 수 있으며 발급한 인증서의 “fingerprint(지문)" 또는 "thumbprint(지문)" 특성 필드가 아니라 서버에서 직접 지문을 검색해야 합니다.

단계 **8** **OK(**확인**)**를 클릭합니다.

관련 항목

AnyConnect 프로파일 편집기, 서버 목록, 104 페이지
AnyConnect 프로파일 편집기, 서버 목록 추가/편집, 105 페이지

로그온 전 Windows VPN 연결 자동 시작

로그온 전 시작 정보

SBL(Start Before Logon, 로그온 전 시작)이라는 기능을 사용하면 Windows로 로그온하기 전에 엔터프라이즈 인프라에 대한 VPN 연결을 설정할 수 있습니다.

SBL을 설치하고 활성화한 후 Network Connection(네트워크 연결) 버튼을 누르면 AnyConnect VPN 및 Network Access Manager UI가 실행됩니다.

또한 SBL은 Network Access Manager 바둑판식 배열을 포함하며 사용자가 구성한 홈 네트워크 프로파일을 사용하여 연결을 허용합니다. SBL 모드에서 허용되는 네트워크 프로파일에는 비802-1X 인증 모드를 사용하는 모든 미디어 유형이 포함됩니다.

SBL은 Windows 시스템에서만 사용할 수 있으며 Windows 버전에 따라 다른 메커니즘을 사용하여 구현됩니다.

- Windows에서는 AnyConnect SBL을 구현하는 데 PLAP(Pre-Login Access Provider, 사전 로그인 액세스 공급자)가 사용됩니다.

  PLAP에서 Ctrl+Alt+Del 키 조합을 사용하면 창이 열립니다. 이 창에서는 시스템에 로그인하거나 창의 오른쪽 하단에 있는 Network Connect(네트워크 연결) 버튼을 사용하여 네트워크 연결(PLAP 구성 요소)을 활성화할 수 있습니다.

  PLAP는 Windows 32비트 및 64비트 버전을 지원합니다.

사용자를 위해 SBL 활성화를 고려해 볼 수 있는 경우는 다음과 같습니다.

- 사용자의 컴퓨터가 Active Directory 인프라에 통합된 경우입니다.
- 사용자에게 Microsoft Active Directory 인프라를 통한 인증이 필요한 네트워크 연결 드라이브가 있는 경우입니다.
- 사용자의 컴퓨터에 캐시된 자격 증명이 없는 경우(그룹 정책이 캐시된 자격 증명을 허용 안 함)입니다. 이 경우 사용자는 컴퓨터에 액세스하기 전에 확인되어야 하는 자격 증명을 위해 기업 네트워크의 도메인 컨트롤러와 통신할 수 있어야 합니다.
- 사용자가 네트워크 리소스에서 실행하거나 네트워크 리소스에 액세스해야 하는 로그온 스크립트를 실행해야 하는 경우입니다. SBL이 활성화되면 사용자는 사무실에 있을 때 일반적으로 실행되는 로컬 인프라 및 로그온 스크립트에 액세스할 수 있는 권한을 가집니다. 여기에는 도메인 로그온 스크립트, 그룹 정책 개체 및 사용자가 시스템에 로그인할 때 일반적으로 발생하는 기타 Active Directory 기능이 포함되어 있습니다.
- 인프라에 대한 연결이 필요할 수 있는 MS NAP/CS NAC와 같은 네트워킹 구성 요소가 존재하는 경우입니다.

로그온 전 시작 제한 사항

- AnyConnect는 빠른 사용자 전환과 호환되지 않습니다.
- AnyConnect는 서드파티의 로그온 전 시작 애플리케이션에서 시작할 수 없습니다.

로그온 전 시작 구성

프로시저

단계 **1** AnyConnect 로그온 전 시작 모듈 설치

단계 2 AnyConnect 프로파일에서 SBL 활성화

AnyConnect 로그온 전 시작 모듈 설치

AnyConnect 설치 프로그램은 기반 운영 체제를 탐지하고 AnyConnect SBL 모듈의 적절한 AnyConnect DLL을 시스템 디렉토리에 위치시킵니다. Windows 7 또는 Windows 2008 서버에서 설치 프로그램은 사용 중인 운영 체제가 32비트 또는 64비트 버전인지 판단하고 적절한 PLAP 구성 요소 즉, vpnplap.dll 또는 vpnplap64.dll을 설치합니다.

참고 VPNGINA 또는 PLAP 구성 요소는 설치한 상태로 두고 AnyConnect를 제거한 경우, VPNGINA 또는 PLAP 구성 요소가 비활성화되고 원격 사용자에게 표시되지 않습니다.

SBL 모듈을 사전 구축하거나, 다운로드하도록 ASA를 구성할 수 있습니다. AnyConnect를 사전 구축하는 경우, 로그온 전 시작 모듈은 코어 클라이언트 소프트웨어를 먼저 설치해야 합니다. MSI 파일을 사용하여 AnyConnect 코어 및 로그온 전 시작 구성 요소를 사전 구축할 경우, 주문 권한이 있어야 합니다.

프로시저

단계 1 ASDM에서 **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 새 그룹 정책 **Edit**(편집) 또는 **Add**(추가)를 클릭합니다.

단계 3 왼쪽 탐색 창에서 **Advanced**(고급) > **AnyConnect Client**(**AnyConnect** 클라이언트)를 선택하십시오.

단계 4 다운로드할 선택적 클라이언트 모듈 설정에서 **Inherit**(상속) 를 선택 해제하십시오.

단계 5 드롭다운 목록에서 **AnyConnect SBL** 모듈을 선택하십시오.

AnyConnect 프로파일에서 SBL 활성화

시작하기 전에

- SBL은 호출될 때 네트워크 연결이 있어야 합니다. 경우에 따라 이는 불가능할 수 있습니다. 무선 연결이 무선 인프라에 연결할 사용자의 자격 증명에 따라 달라질 수 있기 때문입니다. SBL 모드가 로그온의 자격 증명 단계 앞에 사용되므로 이 시나리오에서는 연결을 사용할 수 없습니다. 이러한 경우 SBL이 작동하도록 로그온에서 자격 증명을 캐시하도록 무선 연결을 구성하거나 다른 무선 인증을 구성해야 합니다.
- Network Access Manager가 설치된 경우 적절한 연결이 가능하도록 머신 연결을 구축해야 합니다.

프로시저

단계 **1** VPN 프로파일 편집기를 열고 탐색 창에서 **Preferences(Part 1)(**환경 설정**(1**부**))** 를 선택합니다.

단계 **2** **Use Start Before Logon(**로그온 전 시작 사용**)**을 선택하십시오.

단계 **3** 원격 사용자에게 SBL 제어 권한을 주려면 **User Controllable(**사용자 제어 가능**)**을 선택하십시오(선택 사항).

참고 SBL이 적용되려면 사용자가 원격 컴퓨터를 재부팅해야 합니다.

로그온 전 시작 문제 해결

프로시저

단계 **1** AnyConnect 프로파일이 ASA에 로드되고 구축될 준비가 되었는지 확인하십시오.

단계 **2** 이전 프로파일을 삭제하십시오(*.xml로 하드 드라이브에서 위치 검색).

단계 **3** Windows 프로그램 추가/제거 기능을 사용하여 SBL 구성 요소를 제거하십시오. 컴퓨터를 재부팅하고 다시 테스트하십시오.

단계 **4** 이벤트 뷰어에서 사용자의 AnyConnect 로그인을 지우고 다시 테스트하십시오.

단계 **5** 보안 어플라이언스로 되돌아가서 AnyConnect를 다시 설치하십시오.

단계 **6** 다시 재부팅하십시오. 두 번째 재부팅에서 Start Before Logon(로그온 전 시작) 프롬프트가 표시되어야 합니다.

단계 **7** DART 번들을 수집하여 AnyConnect 관리자에게 보내십시오.

단계 **8** 다음과 같은 오류가 나타날 경우 사용자의 AnyConnect 프로파일을 삭제하십시오.

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

단계 **9** .tmpl 파일에 돌아가서 xml 파일로 복사본을 저장하고 해당 xml 파일을 기본 프로파일로 사용하십시오.

AnyConnect 시작 시 자동으로 VPN 연결 시작

이 기능은 Auto Connect on Start(시작 시 자동 연결)라고 하며 AnyConnect가 시작되면 VPN 클라이언트 프로파일에서 지정한 보안 게이트웨이와의 VPN 연결을 자동으로 설정하는 기능입니다.

Auto Connect on Start(시작 시 자동 연결)는 기본적으로 비활성화되어 있으며 사용자에게 보안 게이트웨이를 지정하거나 선택하도록 요청합니다.

프로시저

단계 1 VPN 프로파일 편집기를 열고 탐색 창에서 **Preferences(Part 1)**(환경 설정(1부)) 를 선택합니다.

단계 2 **Auto Connect on Start**(시작 시 자동 연결)를 선택합니다.

단계 3 사용자에게 Auto Connect on Start(시작 시 자동 연결)에 대한 제어 권한을 부여하려면 **User Controllable**(사용자 제어 가능)을 선택하십시오(선택 사항).

Windows 시스템에서 로그온 전 시작(PLAP) 구성

SBL(Start Before Logon, 로그온 전 시작) 기능은 사용자가 Windows에 로그인하기 전에 VPN 연결을 시작합니다. 그러면 사용자가 컴퓨터에 로그온하기 전에 회사 인프라에 연결할 수 있습니다.

SBL AnyConnect 기능은 연결 가능한 자격 증명 제공자인 PLAP(Pre-Login Access Provider, 사전 로그인 액세스 공급자)로 알려져 있습니다. 프로그래밍 방식 네트워크 관리자는 이 기능을 통해 자격 증명을 수집하거나 로그온 전에 네트워크 리소스에 연결하는 등의 특정 작업을 수행할 수 있습니다. PLAP는 지원되는 모든 Windows 운영 체제에서 SBL 기능을 제공합니다. PLAP는 vpnplap.dll 및 vpnplap64.dll을 각각 사용하여 32비트 및 64비트 버전 운영 체제를 지원합니다. PLAP 기능은 x86 및 x64를 지원합니다.

PLAP 설치

vpnplap.dll 및 vpnplap64.dll 구성 요소는 기존 설치에 포함되어 있으므로 보안 어플라이언스에서 단일 애드온 SBL 패키지를 로드할 수 있습니다. 그러면 대상 플랫폼에 적합한 구성 요소가 설치됩니다. PLAP는 선택적인 기능입니다. 설치 프로그램은 기본 운영 체제를 탐지하여 적절한 DLL을 시스템 디렉토리에 배치합니다. Windows 7 이상 버전 또는 Windows 2008 서버에서 설치 프로그램은 사용 중인 운영 체제가 32비트 버전인지 아니면 64비트 버전인지 확인한 다음 적절한 PLAP 구성 요소를 설치합니다.

참고 PLAP 구성 요소는 설치한 상태로 두고 AnyConnect를 제거하는 경우 PLAP 구성 요소가 비활성화되며 원격 사용자에게 표시되지 않습니다.

PLAP는 설치 후 사용자 프로파일 <profile.xml> 파일을 수정하여 SBL을 활성화할 때까지 활성화되지 않습니다. AnyConnect 프로파일에서 SBL 활성화, 122 페이지을 참조하십시오. PLAP를 활성화한 후에 사용자는 Switch User(사용자 전환)를 클릭한 다음 화면 오른쪽 아래에서 Network Connect(네트워크 연결) 아이콘을 클릭하여 Network Connect(네트워크 연결) 구성 요소를 호출합니다.

참고 사용자는 사용자 인터페이스를 실수로 최소화한 경우 **Alt+Tab** 키 조합을 눌러 사용자 인터페이스를 복구할 수 있습니다.

PLAP를 사용하여 Windows PC에 로그온

프로시저

단계 1 사용자가 Windows 시작 창에서 **Ctrl+Alt+Del** 키 조합을 누릅니다.

Switch User(사용자 전환) 버튼이 포함된 로그온 창이 나타납니다.

단계 2 사용자가 **Switch User(**사용자 전환**)**를 클릭합니다. Network Connect(네트워크 연결) 창이 표시됩니다. 사용자가 AnyConnect 연결을 통해 이미 연결된 상태에서 **Switch User(**사용자 전환**)**를 클릭하면 해당 VPN 연결이 유지됩니다. 사용자가 **Network Connect(**네트워크 연결**)**를 클릭하면 원래 VPN 연결이 종료됩니다. 사용자가 **Cancel(**취소**)**을 클릭하면 VPN 연결이 종료됩니다.

단계 3 사용자가 창 오른쪽 하단에 있는 **Network Connect(**네트워크 연결**)** 버튼을 클릭하여 AnyConnect를 시작합니다. AnyConnect 로그온 창이 열립니다.

단계 4 사용자가 이 GUI를 사용하여 일반적인 방법으로 로그인합니다.
이 예에서는 설치되어 있는 연결 제공자가 AnyConnect뿐이라고 가정합니다. 여러 제공자가 설치되어 있으면 사용자는 이 창에 표시되는 항목 중에서 사용할 제공자를 선택해야 합니다.

단계 5 사용자가 연결되면 Network Connect(네트워크 연결) 창과 비슷한 화면이 표시됩니다. Network Connect(네트워크 연결) 창과 달리 이 화면의 오른쪽 하단에는 Microsoft Disconnect(Microsoft 연결 끊기) 버튼이 있습니다. 이 버튼은 정상적으로 연결되었다는 것만을 나타냅니다.

단계 6 사용자가 로그온과 연결된 아이콘을 클릭합니다.
연결이 설정되면 로그온 상태가 몇 분 동안 유지됩니다. 사용자 로그온 세션은 유휴 시간 제한인 약 2분 후에 시간이 초과되며, 이 시간이 지나면 AnyConnect PLAP 구성 요소에 대해 연결 끊기가 실행되어 VPN 터널의 연결이 끊깁니다.

PLAP를 사용하여 AnyConnect에서 연결 끊기

VPN 세션이 정상적으로 설정되고 나면 PLAP 구성 요소의 원래 창이 다시 표시되며 윈도우 오른쪽 아래에는 Disconnect(연결 끊기) 버튼이 표시됩니다.

사용자가 **Disconnect(**연결 끊기**)**를 클릭하면 VPN 터널의 연결이 끊깁니다.

터널 연결은 **Disconnect(**연결 끊기**)** 버튼 클릭에 대한 응답으로 명시적으로 끊길 뿐 아니라 다음과 같은 상황에서도 끊깁니다.

- 사용자가 PLAP를 사용하여 PC에 로그온한 다음 **Cancel(**취소**)**을 누르는 경우
- 사용자가 시스템에 로그온하기 전에 PC가 종료되는 경우
- Windows에서 사용자 로그온 세션의 시간이 초과되어 "로그온하려면 Ctrl+Alt+Del을 누르십시오."라는 화면이 다시 표시되는 경우

이 동작은 AnyConnect가 아닌 Windows PLAP 아키텍처의 기능입니다.

자동으로 VPN 연결 재시작

Auto Reconnect(자동 재연결)가 활성화된 경우(기본값) AnyConnect는 초기 연결에 사용된 미디어에 관계 없이 VPN 세션 중단 상태에서 복구하고 세션을 재설정합니다. 예를 들어 유선, 무선 또는 3G에서 세션을 재설정할 수 있습니다. Auto Reconnect(자동 재연결)이 활성화된 경우, 시스템 일시 중지 또는 시스템 재개 시 재연결 동작을 지정하십시오. 시스템 일시 중지는 Windows의 "최대 절전 모드" 또는 macOS/Linux의 "절전 모드"와 같은 저전력 대기 모드입니다. 시스템 재개는 시스템 일시 중지 이후의 복구 모드입니다.

Auto Reconnect(자동 재연결)를 비활성화한 경우, 클라이언트는 연결이 끊어진 원인과 관계 없이 재연결하려고 시도하지 않습니다. Cisco에서는 이 기능을 위해 기본 설정(활성화)을 사용할 것을 적극 권장합니다. 이 설정을 비활성화하면 불안정한 연결을 통한 VPN 연결을 중단시킬 수 있습니다.

프로시저

단계 **1** VPN 프로파일 편집기를 열고 탐색 창에서 **Preferences(Part 1)(**환경 설정**(1**부**))** 를 선택합니다.

단계 **2** **Auto Reconnect(**자동 재연결**)**를 선택합니다.

단계 **3** 다음 자동 재연결 동작을 선택하십시오.

- Disconnect On Suspend(일시 중지 시 연결 끊기) — (기본값) AnyConnect는 시스템 일시 중지 시 VPN 세션에 할당된 리소스를 해제하며 시스템 재개 이후에 재연결을 시도하지 않습니다.
- Reconnect After Resume(재개 후 재연결) — 클라이언트는 시스템 일시 중지 시 VPN 세션에 할당된 리소스를 유지하며 시스템 재개 이후에 재연결을 시도합니다.

신뢰할 수 있는 네트워크 탐지를 사용하여 연결 및 연결 끊기

신뢰할 수 있는 네트워크 탐지 정보

TND(Trusted Network Detection, 신뢰할 수 있는 네트워크 탐지)는 사용자가 기업 네트워크 내부(신뢰할 수 있는 네트워크)에 있을 때 AnyConnect가 자동으로 VPN 연결을 해제하고 사용자가 기업 네트워크 외부(신뢰할 수 없는 네트워크)에 있을 때 VPN 연결을 시작할 수 있는 기능을 제공합니다.

TND는 사용자의 VPN 연결 수동 설정 권한을 방해하지 않으며 사용자가 신뢰할 수 있는 네트워크에서 수동으로 시작한 VPN 연결을 끊지 않습니다. 사용자가 신뢰할 수 없는 네트워크에 먼저 연결하고 신뢰할 수 있는 네트워크로 이동하는 경우 TND는 VPN 세션의 연결만 끊습니다. 예를 들어 사용자가 집에서 VPN을 연결한 후 기업 사무실로 이동하는 경우 TND는 VPN 세션의 연결을 끊습니다.

참고 웹 보안 모듈에 해당하는 기능은 웹 보안 구성 장에서 신뢰할 수 있는 보안 네트워크 탐지 사용을 참조하십시오.

TND는 AnyConnect VPN 클라이언트 프로파일에서 구성하며, ASA 구성은 변경할 필요가 없습니다. 신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 전환을 인식한 경우 AnyConnect가 수행하는 작업 또는 정책을 지정하고 신뢰할 수 있는 네트워크와 서버를 식별해야 합니다.

신뢰할 수 있는 네트워크 탐지에 대한 지침

- TND 기능은 AnyConnect GUI를 제어하며 자동으로 연결을 시작하므로 항상 GUI를 실행해야 합니다. 사용자가 GUI를 종료하는 경우, TND는 VPN 연결을 자동으로 시작하지 않습니다.
- 또한 AnyConnect가 SBL(Start-Before-Logon, 로그온 전 시작)을 실행 중인 경우, 사용자는 신뢰할 수 있는 네트워크로 이동하며 컴퓨터에 표시된 SBL 창이 자동으로 닫힙니다.
- 상시 가동 이 구성 또는 구성되지 않은 신뢰할 수 있는 네트워크 탐지는 IPv4 및 IPv6 네트워크를 통해 ASA에 대한 IPv6 및 IPv4 VPN 연결에서 지원됩니다.
- 사용자 컴퓨터에 있는 여러 개의 프로파일은 TND 구성이 다른 경우, 문제를 일으킬 수 있습니다.

  사용자가 이전에 TND 활성화 프로파일을 수신한 경우, 시스템이 다시 시작되는 즉시 AnyConnect가 마지막에 연결했던 보안 어플라이언스에 연결을 시도하며 이는 사용자가 원하지 않는 동작일 수 있습니다. 다른 보안 어플라이언스에 연결하려면 수동으로 연결을 끊고 해당 헤드엔드에 재연결해야 합니다. 다음 해결책을 통해 이러한 문제를 방지할 수 있습니다.

  - 기업 네트워크에서 모든 ASA에 로드된 클라이언트 프로파일에서 TND를 활성화합니다.
  - 모든 ASA를 나열하는 한 개의 프로파일을 호스트 항목 섹션에서 생성하고 이 프로파일을 모든 ASA에 로드합니다.
  - 사용자가 여러 개의 다른 프로파일을 가질 필요가 없는 경우, 모든 ASA에 있는 프로파일에 동일한 프로파일 이름을 사용합니다. 각 ASA는 기존 프로파일을 재정의합니다.

- Linux에서 TND를 사용하려면 대상(RHEL/Ubuntu) 디바이스에서 네트워크 관리자를 적절하게 설치하고 실행해야 하며 네트워크 관리자가 네트워크 인터페이스를 유지 보수하고 있어야 합니다.

신뢰할 수 있는 네트워크 탐지 구성

프로시저

단계 **1** VPN 프로파일 편집기를 열고 탐색 창에서 **Preferences(Part 1)(**환경 설정**(1**부**))** 를 선택합니다.

단계 **2** **Automatic VPN Policy(**자동 **VPN** 정책**)**를 선택하십시오.

단계 **3** **Trusted Network Policy(**신뢰할 수 있는 네트워크 정책**)**를 선택합니다.

이 단계는 사용자가 기업 네트워크(신뢰할 수 있는 네트워크) 내부에 있는 경우 클라이언트가 수행하는 작업입니다. 옵션은 다음과 같습니다.

- 연결 끊기 — (기본값) 클라이언트가 신뢰할 수 있는 네트워크에서 VPN 연결을 종료합니다.
- 연결 — 클라이언트가 신뢰할 수 있는 네트워크에서 VPN 연결을 시작합니다.

- 작업 수행 안 함 — 클라이언트가 신뢰할 수 있는 네트워크에서 아무 작업도 수행하지 않습니다. 신뢰할 수 있는 네트워크 정책 및 신뢰할 수 없는 네트워크 정책을 모두 작업 수행 안 함으로 설정하면 TND(Trusted Network Detection, 신뢰할 수 있는 네트워크 탐지)가 비활성화됩니다.
- 일시 중지 — AnyConnect는 사용자가 신뢰할 수 있는 네트워크 외부에서 VPN 세션을 설정한 이후에 신뢰할 수 있는 상태로 구성된 네트워크를 시작하는 경우, 연결을 끊는 대신 VPN 세션을 일시 중지합니다. 사용자가 신뢰할 수 있는 네트워크 외부로 다시 이동하면 AnyConnect는 세션을 재개합니다. 이 기능은 신뢰할 수 있는 네트워크를 종료한 이후에 새 VPN 세션을 설정할 필요가 없으므로 사용자에게 편리한 기능입니다.

단계 **4** **Untrusted Network Policy(**신뢰할 수 없는 네트워크 정책**)**를 선택합니다.

이 단계는 사용자가 기업 네트워크 외부에 있는 경우 클라이언트가 수행하는 작업입니다. 옵션은 다음과 같습니다.

- 연결 — 신뢰할 수 없는 네트워크가 탐지되면 클라이언트가 VPN 연결을 시작합니다.
- 작업 수행 안 함 — 신뢰할 수 없는 네트워크가 탐지되면 클라이언트가 아무 작업도 수행하지 않습니다. 이 옵션은 상시 가동 VPN을 비활성화합니다. 신뢰할 수 있는 네트워크 정책 및 신뢰할 수 없는 네트워크 정책을 모두 **Do Nothing(**작업 수행 안 함**)** 으로 설정하면 신뢰할 수 있는 네트워크 탐지가 비활성화됩니다.

단계 **5** **Trusted DNS Domains(**신뢰할 수 있는 **DNS** 도메인**)**를 지정합니다.

클라이언트가 신뢰할 수 있는 네트워크에 있는 경우 네트워크 인터페이스에 포함될 수 있는 DNS 접미사(쉼표로 구분되는 문자열)를 지정합니다. DNS 접미사를 스플릿 DNS 목록에 추가하고 ASA에서 기본 도메인을 지정한 경우 여러 DNS 접미사를 할당할 수 있습니다.

AnyConnect 클라이언트는 다음 순서로 DNS 접미사 목록을 구축합니다.

- 헤드엔드에서 전달한 도메인
- 헤드엔드에서 전달한 스플릿 DNS 접미사 목록
- 공용 인터페이스의 DNS 접미사(구성된 경우). 그렇지 않은 경우, 기본 DNS 접미사의 상위 접미사와 함께 기본 및 연결 특정 접미사(고급 TCP/IP 설정에서 해당 상자가 선택된 경우)

일치시킬 **DNS** 접미사**:**	**TrustedDNSDomains**에 사용할 값**:**
example.com(전용)	*example.com
example.com AND anyconnect.example.com	*.example.com OR example.com, anyconnect.example.com
asa.example.com AND anyconnect.example.com	*.example.com OR asa.example.com, anyconnect.example.com

단계 **6** **Trusted DNS Servers(**신뢰할 수 있는 **DNS** 서버**)**를 지정합니다.

클라이언트가 신뢰할 수 있는 네트워크에 있는 경우 네트워크 인터페이스에 포함될 수 있는 모든 DNS 서버 주소(쉼표로 구분되는 문자열)입니다. 예를 들어 203.0.113.1,2001:DB8::1입니다. 와일드카드(*)는 IPv4 및 IPv6 DNS 서버 주소용으로 지원됩니다.

DNS를 통해 확인 가능한 헤드엔드 서버용 DNS 항목이 있어야 합니다. IP 주소를 사용하여 연결하는 경우에는 mus.cisco.com을 확인할 수 있는 DNS 서버가 필요합니다. DNS를 통해 mus.cisco.com을 확인할 수 없는 경우에는 종속 포털 탐지가 정상적으로 작동하지 않습니다.

참고 TrustedDNSDomains, TrustedDNSServers 중 하나 또는 두 가지 모두를 구성할 수 있습니다. TrustedDNSServers를 구성한 경우 모든 DNS 서버를 입력하여 사이트가 모두 신뢰할 수 있는 네트워크에 포함되도록 하십시오.

활성 인터페이스는 VPN 프로파일에 있는 모든 규칙과 일치하는 경우 신뢰할 수 있는 네트워크에 포함된 것으로 간주됩니다.

단계 **7** 신뢰하는 항목으로 추가할 호스트 URL을 지정합니다. 신뢰할 수 있는 인증서를 사용하여 액세스할 수 있는 보안 웹 서버가 있어야 신뢰할 수 있는 서버로 간주됩니다. **Add(**추가**)**를 클릭하면 URL이 추가되고 인증서 해시가 미리 입력됩니다. 해시를 찾을 수 없으면 인증서 해시를 수동으로 입력하고 **Set(**설정**)**를 클릭하라는 오류 메시지 프롬프트가 표시됩니다.

참고 Trusted DNS Domains(신뢰할 수 있는 DNS 도메인) 또는 Trusted DNS Servers(신뢰할 수 있는 DNS 서버) 중 하나 이상을 정의해야 이 파라미터를 구성할 수 있습니다. Trusted DNS Domains(신뢰할 수 있는 DNS 도메인) 또는 Trusted DNS Servers(신뢰할 수 있는 DNS 서버)를 정의하지 않으면 이 필드는 비활성화됩니다.

상시 가동을 사용하는 VPN 연결 필요

상시 가동 VPN 정보

상시 가동 작업은 VPN 세션이 활성 상태가 아닌 경우 컴퓨터가 신뢰할 수 있는 네트워크에 연결되어 있지 않으면 인터넷 리소스에 액세스하지 못하도록 합니다. 이러한 상황에서 VPN을 항상 켜진 상태로 적용하면 보안 위협으로부터 컴퓨터가 보호됩니다.

상시 가동 을 활성화하면 사용자가 로그인한 이후 또는 신뢰할 수 없는 네트워크가 탐지되는 즉시 VPN 세션이 자동으로 설정됩니다. VPN 세션은 사용자가 컴퓨터에서 로그아웃하거나 세션 타이머 또는 유휴 세션 타이머(ASA 그룹 정책에 지정됨)가 만료될 때까지 열린 상태로 유지됩니다. 세션이 여전히 열려 있는 경우 AnyConnect는 세션을 다시 활성화하기 위해 연결 재설정을 계속해서 시도하며, 그렇지 않은 경우 새 VPN 세션 설정을 계속해서 시도합니다.

VPN 프로파일에서 상시 가동 을 활성화하면 AnyConnect는 다운로드한 다른 모든 AnyConnect 프로파일을 삭제하여 엔드포인트를 보호하고 ASA에 연결하도록 구성된 공용 프록시를 무시합니다.

상시 가동을 활성화할 때는 다음 AnyConnect 옵션도 고려해야 합니다.

- 사용자의 상시 가동 VPN 세션 연결 끊기 허용: AnyConnect는 사용자에게 상시 가동 VPN 세션 연결 끊기 기능을 제공합니다. **Allow VPN Disconnect**를 활성화하면 VPN 세션을 설정하는 즉시

AnyConnect에 Disconnect(연결 끊기) 버튼이 표시됩니다. 기본적으로상시 가동 VPN을 활성화하면 프로파일 편집기에서 Disconnect(연결 끊기) 버튼을 활성화할 수 있습니다.

Disconnect(연결 끊기) 버튼을 누르면 모든 인터페이스가 잠기므로 데이터 유출이 방지되고 VPN 세션 설정을 제외한 인터넷 액세스로부터 컴퓨터가 보호됩니다. 상시 가동 VPN 세션 사용자는 Disconnect(연결 끊기)를 클릭하여 현재 VPN 세션의 성능 문제 또는 VPN 세션 중단 이후의 재연결 문제 발생 시 사용할 대체 보안 게이트웨이를 선택할 수 있습니다.

- 연결 실패 정책 설정: 연결 실패 정책은 상시 가동 VPN이 활성화되어 있는데 AnyConnect에서 VPN 세션을 설정할 수 없는 경우 컴퓨터가 인터넷에 액세스 가능한지를 결정합니다. Always-On에 대한 연결 실패 정책 설정을 참조하십시오.
- 종속 포털 핫스팟 처리: 종속 포털 핫스팟 탐지 및 보안정책 교정 사용을 참조하십시오.

상시 가동 VPN 제한 사항

- 상시 가동이 활성화되어 있지만 사용자가 로그온하지 않은 경우, AnyConnect에서 VPN 연결을 설정하지 않습니다. AnyConnect는 로그인 후에 VPN 연결을 시작합니다.
- 상시 가동 VPN은 프록시를 통한 연결을 지원하지 않습니다.

상시 가동 VPN 지침

위협에 대한 보호를 강화하기 위해 상시 가동 VPN을 구성하는 경우에는 다음과 같이 추가적인 보호 수단을 사용하는 것이 좋습니다.

- CA(Certificate Authority, 인증 기관)로부터 디지털 인증서를 구매하고 보안 게이트웨이에 등록할 것을 적극 권장합니다. ASDM은 **Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > Certificate Management(인증서 관리) > Identity Certificates(ID 인증서)** 패널에서 **Enroll ASA SSL VPN with Entrust(Entrust를 통해 ASA SSL VPN 등록)** 버튼을 제공하여 공용 인증서를 편리하게 등록하도록 해줍니다.
- 미리 정의된 ASA에만 연결하도록 상시 가동 이 구성되어 있는 프로파일을 엔드포인트에 대해 사전 구축합니다. 사전 구축은 Rogue 서버와의 접속을 방지합니다.
- 사용자가 프로세스를 종료할 수 없도록 관리자 권한을 제한합니다. 관리자 권한이 있는 PC 사용자는 에이전트를 중지하여 상시 가동 정책을 우회할 수 있습니다. 상시 가동의 보안을 완전히 유지하려는 경우, 사용자에 대한 로컬 관리자 권한을 거부해야 합니다.
- Windows 컴퓨터의 Cisco 하위 폴더, 일반적으로 `C:\ProgramData`로 액세스를 제한합니다.
- 제한된 권한 또는 표준 권한이 있는 사용자는 종종 프로그램 데이터 폴더에 대한 쓰기 액세스 권한을 가질 수 있습니다. 사용자는 이 액세스 권한을 사용하여 AnyConnect 프로파일 파일을 삭제하는 방법으로 상시 가동 기능을 우회할 수 있습니다.
- Windows 사용자를 위한 GPO(Group Policy Object, 그룹 정책 개체)를 사전에 구축하여 제한된 권한을 가진 사용자가 GUI를 종료하는 것을 방지하십시오. macOS 사용자를 위해 이에 상응하는 수단을 사전 구축하십시오.

상시 가동 VPN 구성

프로시저

단계 1 AnyConnect VPN 클라이언트 프로파일에서 상시 가동 구성
단계 2 서버 목록에 로드 밸런싱 백업 클러스터 요소 추가(선택사항)
단계 3 Always-On VPN에서 사용자 면제(선택사항)

AnyConnect VPN 클라이언트 프로파일에서 상시 가동 구성

시작하기 전에

상시 가동 VPN을 사용하려면 ASA에 유효하고 신뢰할 수 있는 서버 인증서를 구성해야 합니다. 이렇게 하지 않으면 VPN에 오류가 발생하며 인증서가 유효하지 않음을 나타내는 이벤트가 기록됩니다. 또한 서버 인증서가 엄격한 인증서 신뢰 모드를 통과하는지를 확인하면 Rogue 서버에 대한 VPN 연결을 잠그는 상시 가동 VPN 프로파일의 다운로드를 방지할 수 있습니다.

프로시저

단계 1 VPN 프로파일 편집기를 열고 탐색 창에서 **Preferences(Part 2)**(환경 설정(2부)) 를 선택합니다.
단계 2 **Automatic VPN Policy**(자동 VPN 정책)를 선택하십시오.
단계 3 신뢰할 수 있는 네트워크 탐지 구성
단계 4 **Always On**을 선택하십시오.
단계 5 **Allow VPN Disconnect**(VPN 연결 끊기 허용)를 선택하거나 선택하지 않습니다(선택 사항).
단계 6 연결 실패 정책 구성(선택 사항)
단계 7 종속 포털 보안정책 교정 구성(선택 사항)

서버 목록에 로드 밸런싱 백업 클러스터 요소 추가

상시 가동 VPN은 AnyConnect VPN 세션의 로드 밸런싱에 영향을 줍니다. 상시 가동 VPN이 비활성화되어 있는 경우 클라이언트는 로드 밸런싱 클러스터 내의 마스터 디바이스에 연결할 때 마스터 디바이스로부터 모든 백업 클러스터 요소로의 리디렉션을 준수합니다. 상시 가동 이 활성화되어 있는 경우 클라이언트는 백업 클러스터 요소의 주소가 클라이언트 프로파일의 서버 목록에 지정되어 있지 않으면 마스터 디바이스로부터의 리디렉션을 준수하지 않습니다. 따라서 서버 목록에 모든 백업 클러스터 요소를 추가해야 합니다.

클라이언트 프로파일에서 백업 클러스터 요소의 주소를 지정하려면 ASDM을 사용하여 다음 절차에 따라 로드 밸런싱 백업 서버 목록을 추가하십시오.

프로시저

단계 **1** VPN 프로파일 편집기를 열고 탐색 창에서 **Server List(**서버 목록**)** 를 선택합니다.

단계 **2** 로드 밸런싱 클러스터의 마스터 디바이스인 서버를 선택하고 **Edit(**편집**)**을 클릭합니다.

단계 **3** 모든 로드 밸런싱 클러스터 요소의 FQDN 또는 IP 주소를 입력합니다.

Always-On VPN에서 사용자 면제

상시 가동 정책을 재정의하도록 면제를 구성할 수 있습니다. 특정 개인이 다른 회사를 통해 VPN 세션을 설정하도록 허용하거나, 비법인 자산에 대한 상시 가동 정책을 면제하려는 경우를 예로 들 수 있습니다.

ASA에서 그룹 정책 및 동적 액세스 정책에 설정된 면제는 상시 가동 정책을 재정의합니다. 정책을 지정하기 위해 사용된 일치 기준에 따라 면제를 지정합니다. AnyConnect 정책에서는 상시 가동 기능을 활성화하는데 동적 액세스 정책 또는 그룹 정책은 이 기능을 비활성화하는 경우 클라이언트는 새로운 각 세션 설정에 대한 동적 액세스 정책 또는 그룹 정책과 AnyConnect 정책의 기준이 일치하면 현재 및 향후 VPN 세션에 대해 비활성화 설정을 유지합니다.

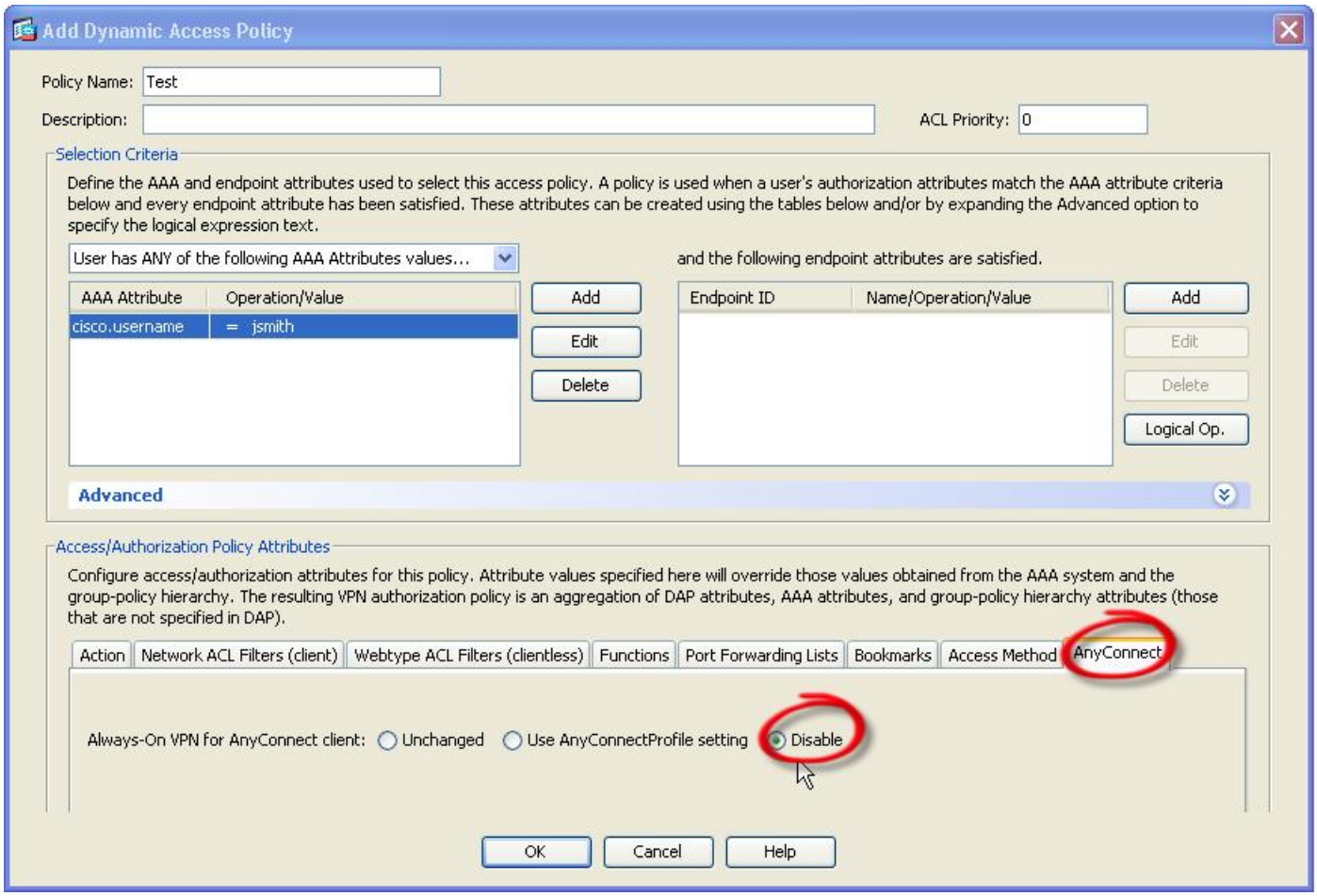
이 절차는 세션을 비법인 자산에 일치시키는 AAA 엔드포인트 기준을 사용하는 동적 액세스 정책을 구성합니다.

프로시저

단계 **1** **Configuration(**구성**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**)** > **Dynamic Access Policies(**동적 액세스 정책**)** > **Add(**추가**)** 또는 **Edit(**편집**)**을 선택하십시오.

단계 **2** 상시 가동 VPN에서 사용자를 면제할 기준을 구성합니다. 예를 들어 AAA 특성을 사용자의 로그온 ID와 일치하도록 지정하려면 선택 기준 영역을 사용하십시오.

단계 **3** Dynamic Access Policy(동적 액세스 정책) Add(추가) 또는 Edit(편집) 창의 아래쪽 가운데에 있는 **AnyConnect** 탭을 클릭하십시오.



단계 **4** "AnyConnect 클라이언트에 대한상시 가동 VPN" 옆에 있는 **Disable(**비활성화**)**을 클릭하십시오.

Always-On에 대한 연결 실패 정책 설정

연결 실패 정책 정보

연결 실패 정책은 상시 가동 VPN이 활성화되어 있고 AnyConnect에서 VPN 세션을 설정할 수 없는 경우 컴퓨터가 인터넷에 액세스 가능한지를 결정합니다. 이는 보안 게이트웨이에 도달할 수 없거나 AnyConnect가 종속 포털 핫스팟의 존재를 탐지하지 못한 경우에 발생할 수 있습니다.

열림 정책은 전체 네트워크 액세스를 허용하고 이를 통해 사용자는 인터넷 또는 기타 로컬 네트워크 리소스에 대한 액세스가 필요한 작업을 계속 수행할 수 있습니다.

닫힘 정책은 VPN 세션이 설정될 때까지 모든 네트워크 연결을 비활성화합니다. AnyConnect는 컴퓨터를 연결할 수 있는 보안 게이트웨이에 대해 제한되지 않은 엔드포인트로부터 모든 트래픽을 차단하는 패킷 필터를 활성화하여 이를 수행합니다.

연결 실패 정책에 관계없이 AnyConnect는 계속해서 VPN 연결 설정을 시도합니다.

연결 실패 정책 설정 지침

전체 네트워크 액세스를 허용하는 열림 정책을 사용할 경우 다음 사항을 고려하십시오.

- VPN 세션이 설정될 때까지 보안 및 보호 기능을 사용할 수 없으므로 엔드포인트 디바이스는 웹 기반 악성코드에 감염되거나 민감한 데이터가 유출될 수 있습니다.
- Disconnect(연결 끊기) 버튼을 활성화하고 사용자가 **Disconnect(**연결 끊기**)**를 클릭하는 경우 열림 연결 실패 정책이 적용되지 않습니다.

VPN 세션이 설정될 때까지 모든 네트워크 연결을 비활성화하는 닫힘 정책을 사용할 경우, 다음 사항을 고려하십시오.

- 닫힘 정책은 사용자가 VPN 외부에서 인터넷에 액세스해야 하는 경우, 생산성을 저해할 수 있습니다.
- 닫힘 정책은 엔드포인트를 보호하는 사설 네트워크에 있는 리소스를 사용할 수 없는 경우, 네트워크 위협으로부터 기업 자산을 보호하는 데 목적이 있습니다. 스플릿 터널링에서 허용하는 프린터 및 테더링 디바이스와 같은 로컬 리소스를 제외하고 모든 네트워크 액세스를 방지하기 때문에 엔드포인트는 항상 웹 기반 악성코드 및 민감한 데이터 유출로부터 보호를 받습니다.
- 이는 보안 지속성이 항상 사용 가능한 네트워크 액세스보다 중요한 보안 조직에 유용한 옵션입니다.
- 닫힘 정책은 특히 종속 포털 보안정책 교정 기능을 활성화하지 않는 한 이를 방지합니다.
- **Apply Last VPN Local Resources(**마지막 **VPN** 로컬 리소스 적용**)**를 클라이언트 프로파일에서 활성화한 경우, 가장 최근의 VPN 세션에서 적용한 로컬 리소스 규칙을 적용하도록 허용할 수 있습니다. 예를 들어 이 규칙은 활성 동기화 및 로컬 인쇄에 대한 액세스를 결정할 수 있습니다.
- 닫힘 정책에 관계없이 상시 가동 기능이 활성화된 경우 AnyConnect 소프트웨어를 업그레이드하는 동안 네트워크가 차단 해제되며 열립니다.
- 닫힘 연결 정책을 구축하는 경우, 단계별로 접근하는 것이 좋습니다. 예를 들어 먼저 연결 실패 시 열림 정책에 따라 상시 가동을 구축하고 사용자를 대상으로 AnyConnect가 원활하게 연결되지 않는 빈도를 조사합니다. 그런 다음 얼리 어답터 사용자에게 연결 실패 시 닫힘 정책을 소규모의 파일럿으로 구축하고 피드백을 요청합니다. 전체 구축을 고려하기 전에 피드백을 계속 요청하면서 파일럿 프로그램을 단계적으로 확장합니다. 연결 실패 시 닫힘 정책을 구축하는 동안 이 정책의 이점뿐만 아니라 네트워크 액세스 한계에 대해 VPN 사용자에게 알려주어야 합니다.

주의 연결 실패 시 닫힘 정책은 AnyConnect가 VPN 세션을 설정하는 데 실패하는 경우, 네트워크 액세스를 방지합니다. 연결 실패 시 닫힘 정책을 구현하는 경우 매우 주의해야 합니다.

연결 실패 정책 구성

상시 가동 기능이 활성화된 경우에만 연결 실패 정책을 구성하십시오. 기본적으로 연결 실패 정책은 VPN에 연결할 수 없는 경우 인터넷 액세스가 차단되므로 닫힙니다. 이러한 상황에서 인터넷 액세스를 허용하려면 연결 실패 정책을 열린 상태로 설정해야 합니다.

프로시저

단계 1 VPN 프로파일 편집기를 열고 탐색 창에서 **Preferences(Part 2)(환경 설정(2부))** 를 선택합니다.

단계 2 다음 설정 중 하나에 **Connect Failure Policy(연결 실패 정책)** 매개변수를 설정합니다.

- Closed — (기본값) 보안 게이트웨이에 연결할 수 없는 경우 네트워크 액세스를 제한합니다.
- Open — 클라이언트가 보안 게이트웨이에 연결할 수 없는 경우 브라우저 및 다른 애플리케이션을 통한 네트워크 액세스를 허용합니다.

단계 3 닫힘 정책을 지정한 경우 다음을 수행하십시오.

a) 종속 포털 보안정책 교정 구성을 수행합니다.

b) 네트워크 액세스가 비활성화되어 있는 동안 마지막 VPN 세션의 로컬 디바이스 규칙을 유지하려면 **Apply Last VPN Local Resources(마지막 VPN 로컬 리소스 적용)** 를 선택합니다.

종속 포털 핫스팟 탐지 및 보안정책 교정 사용

종속 포털 정보

공항, 커피숍, 호텔 등 Wi-Fi 및 유선 액세스를 제공하는 여러 시설에서 사용자는 액세스 권한을 얻기 전에 비용을 지불하거나 사용 제한 정책을 준수하거나 두 가지를 모두 해야 합니다. 이러한 시설에서는 종속 포털이라는 기술을 사용하여 사용자가 브라우저를 열고 액세스를 위한 조건을 수락할 때까지 애플리케이션에 연결하지 못하도록 합니다. 종속 포털 탐지란 이 제한 사항을 인식하는 기능이며 종속 포털 보안정책 교정이란 네트워크 액세스 권한을 얻기 위해 종속 포털 핫스팟의 요건을 충족시키는 프로세스입니다.

종속 포털은 추가 구성이 필요하지 않은 VPN 연결을 시작할 때 AnyConnect에서 자동으로 탐지됩니다. 또한 AnyConnect는 종속 포털이 탐지되는 동안 브라우저 구성 설정을 수정하지 않으며 종속 포털을 자동으로 교정하지 않습니다. 종속 포털 보안정책 교정은 최종 사용자가 수행합니다. AnyConnect는 현재 구성에 따라 종속 포털이 탐지되면 반응합니다.

- 상시 가동이 비활성화되어 있거나, 상시 가동이 활성화되어 있고 연결 실패 정책이 열려 있는 경우 다음 메시지가 각 연결 시도마다 표시됩니다.

  ```
  The service provider in your current location is restricting access to the Internet.
  You need to log on with the service provider before you can establish a VPN session.
  You can try this by visiting any website with your browser.
  ```

  최종 사용자는 핫스팟 공급자의 요건을 충족시켜 종속 포털 보안정책 교정을 수행해야 합니다. 이러한 요건은 네트워크 액세스 비용 지불, 사용 제한 정책 서명 또는 두 가지 모두이거나 공급자가 정의한 일부 다른 요건일 수 있습니다.

- 상시 가동이 활성화되어 있고 연결 실패 정책이 닫혀 있는 경우에는 종속 포털 보안정책 교정을 명시적으로 활성화해야 합니다. 종속 포털 보안정책 교정을 활성화하는 경우 최종 사용자는 위

에 설명된 대로 종속 포털 보안정책 교정을 수행할 수 있습니다. 종속 포털 보안정책 교정을 비활성화하는 경우에는 각 연결 시도마다 다음 메시지가 표시되며 VPN을 연결할 수 없습니다.

```
The service provider in your current location is restricting access to the Internet.
The AnyConnect protection settings must be lowered for you to log on with the service
provider. Your current enterprise security policy does not allow this.
```

종속 포털 보안정책 교정 구성

상시 가동 기능이 활성화되어 있고 Connect Failure Policy(연결 실패 정책)가 닫힘으로 설정된 경우에만 종속 포털 보안정책 교정을 구성하십시오. 이 경우 종속 포털 보안정책 교정을 구성하면 종속 포털에서 연결을 방지하는 경우 AnyConnect의 VPN에 대한 연결이 허용됩니다.

참고 NVM Linux에서는 종속 포털 치료가 지원되지 않습니다. 해당 OS에서는 종속 포털 탐지만 지원됩니다.

Connect Failure Policy(연결 실패 정책)가 열림으로 설정되어 있거나 상시 가동 이 활성화되지 않은 경우, 사용자의 네트워크 액세스가 제한되지 않으며 AnyConnect VPN 클라이언트 프로파일에서 특정 구성을 수행하지 않고도 종속 포털의 보안정책을 교정할 수 있습니다.

기본적으로 종속 포털 보안정책 교정은 최상의 보안을 제공하도록 비활성화되어 있습니다.

프로시저

단계 **1** VPN 프로파일 편집기를 열고 탐색 창에서 **Preferences(Part 1)(**환경 설정**(1**부**))** 를 선택합니다.

단계 **2** **Allow Captive Portal Remediation(**종속 포털 치료 허용**)**을 선택합니다.

이 설정은 닫힘 연결 실패 정책에 따른 네트워크 액세스 제한을 해제합니다.

단계 **3** Remediation Timeout(보안정책 교정 시간 제한)을 지정합니다.

AnyConnect에서 네트워크 액세스 제한을 해제하는 시간(분)을 입력합니다. 종속 포털 요건을 충족하려면 사용자에게 충분한 시간이 필요합니다.

종속 포털 탐지 및 보안정책 교정 문제 해결

AnyConnect는 다음 상황에서 종속 포털에 위치한다고 잘못 가정할 수 있습니다.

- AnyConnect가 잘못된 서버 이름(CN)이 포함된 인증서가 있는 ASA에 접속을 시도하는 경우, AnyConnect 클라이언트는 "종속 포털" 환경에 있다고 판단합니다.

  이를 방지하려면 ASA 인증서가 올바르게 구성되어 있는지 확인하십시오. 인증서의 CN 값은 VPN 클라이언트 프로파일의 ASA 서버 이름과 일치해야 합니다.

- ASA 전에 네트워크에 다른 디바이스가 있는 경우, 이 디바이스는 ASA에 대한 HTTPS 액세스를 차단함으로써 ASA에 접속하려는 클라이언트의 시도에 응답하고 AnyConnect 클라이언트는 "종속 포털" 환경에 있다고 판단합니다. 이 상황은 사용자가 내부 네트워크에 있으며 방화벽을 통해 ASA에 연결하는 경우, 발생할 수 있습니다.

  기업 내부에서 ASA에 대한 액세스를 제한해야 하는 경우 ASA의 주소에 대한 HTTP 및 HTTPS 트래픽이 HTTP 상태를 반환하지 않도록 방화벽을 구성하십시오. ASA로 전송된 HTTP/HTTPS 요청에서 예기치 않은 응답을 반환하지 않도록 하려면 ASA에 대한 HTTP/HTTPS 액세스를 허용하거나 완전히 차단(블랙홀이라고도 함)해야 합니다.

사용자가 종속 포털 보안정책 교정 페이지에 액세스할 수 없는 경우 다음을 수행하도록 요청하십시오.

- 보안정책 교정 작업을 수행하는 한 개의 브라우저를 제외하고 인스턴트 메시징 프로그램, 이메일 클라이언트, IP 전화기 클라이언트 등 HTTP를 사용하는 모든 애플리케이션을 종료합니다.

  종속 포털은 반복적인 연결 시도를 무시함으로써 적극적으로 DoS 공격을 억제하여 클라이언트 말단에서 공격 시간이 초과되도록 합니다. HTTP 연결을 수행하는 많은 애플리케이션의 시도로 인해 이 문제가 악화됩니다.

- 네트워크 인터페이스를 비활성화한 다음 다시 활성화합니다. 이 작업은 종속 포털 탐지 재시도를 작동시킵니다.

- 컴퓨터를 다시 시작합니다.

L2TP 또는 PPTP를 통한 AnyConnect 구성

일부 국가에서 ISP는 L2TP(Layer 2 Tunneling Protocol, 계층 2 터널링 프로토콜) 및 PPTP(Point-to-Point Tunneling Protocol, Point-to-Point 터널링 프로토콜) 지원이 필요합니다.

PPP(Point-to-Point Protocol, Point-to-Point 프로토콜) 연결을 통해 보안 게이트웨이로 향하는 트래픽을 전송하기 위해 AnyConnect는 외부 터널에서 생성되는 Point-to-Point 어댑터를 사용합니다. PPP 연결을 통해 VPN 터널을 설정할 경우, 클라이언트는 ASA를 벗어난 대상으로 향하는 터널링된 트래픽에서 ASA로 향하는 트래픽을 제외시켜야 합니다. 제외 경로 결정 여부 및 결정 방법을 지정하려면 AnyConnect 프로파일에서 PPP 제외 설정을 사용하십시오. 제외 경로는 AnyConnect GUI의 경로 세부사항 표시에서 비보안 경로로 나타납니다.

프로시저

단계 **1** VPN 프로파일 편집기를 열고 탐색 창에서 **Preferences(Part 2)(**환경 설정**(2**부**))** 를 선택합니다.

단계 **2** **PPP Exclusion(PPP** 제외**)** 방법을 선택하십시오. 또한 이 필드에 대해 **User Controllable(**사용자 제어 가능**)**을 선택하여 사용자가 다음 설정을 확인하고 변경할 수 있게 합니다.

- 자동 — PPP 제외를 활성화합니다. AnyConnect에서 자동으로 PPP 서버의 IP 주소를 사용합니다. 자동 탐지에서 IP 주소를 가져오지 못하는 경우에만 이 값을 변경하도록 사용자에게 지시합니다.

- 재정의 — PPP 제외를 활성화합니다. 자동 탐지에서 PPP 서버의 IP 주소를 가져오지 못하고 PPP 제외 UserControllable 값이 true인 경우, 사용자에게 다음 섹션의 지침에 따라 이 설정을 사용하도록 지시하십시오.
- 비활성화 — PPP 제외를 적용하지 않습니다.

단계 **3** **PPP Exclusion Server IP(PPP** 제외 서버 **IP)** 필드에서 연결에 사용되는 PPP 서버의 IP 주소를 입력합니다. 이 필드에 대해 **User Controllable(**사용자 제어 가능**)**을 선택하여 사용자가 preferences.xml 파일을 통해 PPP 서버의 이 IP 주소를 변경할 수 있게 합니다.

다음에 수행할 작업

preferences.xml 파일 변경에 대한 자세한 내용은 "사용자에게 *PPP* 제외를 재정의하도록 지시" 섹션을 참조하십시오.

사용자에게 **PPP** 제외를 재정의하도록 지시

자동 탐지가 작동하지 않고 PPP Exclusion(PPP 제외) 필드를 사용자가 제어할 수 있도록 구성한 경우, 사용자는 로컬 컴퓨터에서 AnyConnect 환경 설정 파일을 편집하여 설정을 재정의할 수 있습니다.

프로시저

단계 **1** Notepad(메모장) 같은 편집기를 사용하여 환경 설정 XML 파일을 여십시오.

이 파일은 사용자의 컴퓨터에서 다음 경로 중에 있습니다.

- Windows: %LOCAL_APPDATA%\Cisco\Cisco AnyConnect Secure Mobility Client\preferences.xml 예를 들면 다음과 같습니다.
- macOS: /Users/username/.anyconnect
- Linux: /home/username/.anyconnect

단계 **2** 재정의 값 및 PPP 서버의 IP 주소를 지정하는 동안 `<ControllablePreferences>`아래에 PPPExclusion 세부사항을 삽입하십시오. 주소는 올바른 형식의 IPv4 주소여야 합니다. 예를 들면 다음과 같습니다.

```
<AnyConnectPreferences>
<ControllablePreferences>
<PPPExclusion>Override
<PPPExclusionServerIP>192.168.22.44</PPPExclusionServerIP></PPPExclusion>
</ControllablePreferences>
</AnyConnectPreferences>
```

단계 **3** 파일을 저장하십시오.

단계 **4** 종료하고 AnyConnect를 다시 시작하십시오.

AnyConnect 프록시 연결 구성

AnyConnect 프록시 연결 정보

AnyConnect는 로컬, 공용 및 전용 프록시를 통해 VPN 세션을 지원합니다.

- 로컬 프록시 연결:

  로컬 프록시는 AnyConnect와 동일한 PC에서 실행되고 경우에 따라 투명 프록시로 사용되기도 합니다. 투명 프록시 서비스의 몇 가지 예로는 일부 무선 데이터 카드에서 제공하는 가속화 소프트웨어 또는 Kaspersky와 같은 일부 안티 바이러스 소프트웨어의 네트워크 구성 요소가 있습니다.

  로컬 프록시 사용은 AnyConnect VPN 클라이언트 프로파일에서 활성화 또는 비활성화되어 있습니다. 로컬 프록시 연결 허용을 참조하십시오.

- 공용 프록시 연결:

  공용 프록시는 일반적으로 웹 트래픽을 익명화하는 데 사용됩니다. Windows가 공용 프록시를 사용하도록 구성된 경우 AnyConnect에서 이 연결을 사용합니다. 공용 프록시는 macOS와 Linux에서 기본 연결 및 재정의 연결을 모두 지원합니다.

  공용 프록시 구성에 대해서는 공용 프록시 연결 구성(Windows)에 설명되어 있습니다.

- 전용 프록시 연결:

  전용 프록시 서버는 기업의 사용 정책에 기반하여 기업 사용자가 특정 웹 사이트(예: 포르노, 도박 또는 게임 사이트)에 액세스하지 못하도록 하기 위해 기업 네트워크에서 사용됩니다.

  터널이 설정된 후 브라우저에 전용 프록시 설정을 다운로드하도록 그룹 정책을 구성합니다. 이 설정은 VPN 세션 종료 후에 원래 상태로 돌아갑니다. 사설 프록시 연결 구성을 참조하십시오.

참고 프록시 서버를 통한 AnyConnect SBL 연결은 Windows 운영 체제 버전과 시스템(머신) 구성 또는 기타 서드파티 프록시 소프트웨어 기능에 따라 달라집니다. 따라서 Microsoft 또는 사용 중인 서드파티 프록시 애플리케이션에서 제공하는 시스템 전체의 프록시 설정을 참조하십시오.

VPN 클라이언트 프로파일을 통한 클라이언트 프록시 제어

VPN 클라이언트 프로파일은 클라이언트 시스템의 프록시 연결을 차단하거나 리디렉션할 수 있습니다. Windows 또는 Linux의 경우 공용 프록시 서버의 주소를 직접 구성하거나 사용자가 구성하도록 허용할 수 있습니다.

VPN 클라이언트 프로파일의 프록시 설정 구성에 대한 자세한 내용은 AnyConnect 프로파일 편집기, 환경 설정(2부)을 참조하십시오.

클라이언트리스 지원을 위한 프록시 자동 구성 파일 생성

ASA 버전 중 일부는 AnyConnect 구성에서 AnyConnect 세션을 설정한 후에 프록시 서버를 통해 클라이언트리스 포털 액세스를 지원해야 합니다. AnyConnect는 이러한 지원이 가능하도록 PAC(Proxy Auto-Configuration) 파일을 사용하여 클라이언트의 프록시 설정을 수정합니다. AnyConnect는 ASA가 전용 프록시 설정을 지정하지 않는 경우에만 이 파일을 생성합니다.

AnyConnect 프록시 연결 요건

프록시 연결 유형에 대한 OS 지원은 다음과 같습니다.

프록시 연결 유형	Windows	macOS	Linux
로컬 프록시	예	아니요	아니요
사설 프록시	지원(Internet Explorer의 경우)	지원(Safari의 경우)	아니요
공용 프록시	지원(IE 및 재정의)	지원(재정의 및 기본)	지원(재정의및 기본)

프록시 연결 제한 사항

- IPv6 프록시가 모든 유형의 프록시 연결에 지원되지는 않습니다.
- 프록시를 통한 연결은 상시 가동 기능이 활성화된 경우 지원되지 않습니다.
- VPN 클라이언트 프로파일이 로컬 프록시에 대한 액세스를 허용해야 합니다.

로컬 프록시 연결 허용

프로시저

단계 **1** VPN 프로파일 편집기를 열고 탐색 창에서 **Preferences(Part 2)(**환경 설정**(2**부**))** 를 선택합니다.

단계 **2** **Allow Local Proxy Connections(**로컬 프록시 연결 허용**)**를 선택(기본값)하거나 선택하지 않습니다. 로컬 프록시는 기본적으로 비활성화되어 있습니다.

공용 프록시

공용 프록시는 Windows 및 Linux 플랫폼에서 지원됩니다. 프록시 서버는 클라이언트 프로파일에 설정되어 있는 환경 설정에 따라 선택됩니다. 프록시 재정의의 경우 AnyConnect는 프로파일에서 프록시 서버를 추출합니다. 릴리스 4.1에서는 Linux 및 macOS의 기본 프록시 컨피그레이션과 함께 Mac에서 프록시가 추가로 지원됩니다.

Linux에서는 AnyConnect가 실행되기 전에 기본 프록시 설정이 엑스포트됩니다. 설정을 변경하는 경우에는 컴퓨터를 다시 시작해야 합니다.

프록시 서버를 인증하려면 사용자 이름 및 비밀번호가 필요합니다. AnyConnect는 프록시 서버가 인증이 필요한 상태로 구성된 경우 기본 및 NTLM 인증을 지원합니다. AnyConnect 대화 상자에서 인증 프로세스를 관리합니다. 프록시 서버를 성공적으로 인증한 후 AnyConnect는 ASA 사용자 이름과 비밀번호를 묻는 프롬프트를 표시합니다.

공용 프록시 연결 구성(Windows)

Windows에서 공용 프록시 연결을 구성하려면 다음 단계를 따르십시오.

프로시저

단계 1 Internet Explorer 또는 제어판에서 **Internet Options**(인터넷 옵션)를 엽니다.
단계 2 **Connections**(연결) 탭을 선택하고 **LAN Settings**(LAN 설정) 버튼을 클릭합니다.
단계 3 프록시 서버를 사용하도록 LAN을 구성하고 프록시 서버의 IP 주소를 입력합니다.

공용 프록시 연결 구성(macOS)

프로시저

단계 1 시스템 환경 설정으로 이동한 다음 연결되어 있는 해당 인터페이스를 선택합니다.
단계 2 **Advanced**(고급)를 클릭합니다.
단계 3 새 창에서 **Proxies**(프록시) 탭을 선택합니다.
단계 4 HTTPS 프록시를 활성화합니다.
단계 5 오른쪽 패널의 Secure Proxy Server(보안 프록시 서버) 필드에 프록시 서버 주소를 입력합니다.

공용 프록시 연결 구성(Linux)

Linux에서 공용 프록시 연결을 설정하려면 환경 변수를 설정해야 합니다.

사설 프록시 연결 구성

프로시저

단계 1 ASA 그룹 정책의 사설 프록시 정보를 구성합니다. *Cisco ASA Series VPN* 환경 설정 가이드의 내부 그룹 정책용 브라우저 프록시 구성 섹션을 참조하십시오.

참고 macOS 환경에서는 ASA에서 VPN 연결을 통해 푸시다운한 프록시 정보를 터미널을 열어 **`scutil --proxy`**를 실행할 때까지 브라우저에서 확인할 수 없습니다.

단계 2 브라우저 프록시 설정을 무시하도록 클라이언트 구성(선택 사항)

단계 **3** Internet Explorer 연결 탭 잠금(선택 사항)

브라우저 프록시 설정을 무시하도록 클라이언트 구성

사용자 PC의 Microsoft Internet Explorer 또는 Safari 프록시 구성 설정을 무시하도록 AnyConnect 프로파일에서 정책을 지정할 수 있습니다. 이렇게 하면 사용자가 기업 네트워크 외부에서 터널을 설정하지 못하도록 하며 AnyConnect가 바람직하지 않거나 불법적인 프록시 서버를 통해 연결되지 못하도록 할 수 있습니다.

프로시저

단계 **1** VPN 프로파일 편집기를 열고 탐색 창에서 **Preferences(Part 2)**(환경 설정(**2**부)) 를 선택합니다.

단계 **2** 프록시 설정 드롭다운 목록에서 **IgnoreProxy**를 선택합니다. 프록시를 무시하면 클라이언트에서 모든 프록시 설정을 무시하게 됩니다. ASA에서 다운로드한 프록시에 대해서 아무 작업도 수행되지 않습니다.

Internet Explorer 연결 탭 잠금

특정한 조건에서 AnyConnect는 Internet Explorer Tool(Internet Explorer 툴) > Internet Options(인터넷 옵션) > Connections(연결) 탭을 숨깁니다. 이 탭이 표시될 경우, 탭을 사용하여 사용자가 프록시 정보를 설정할 수 있습니다. 이 탭을 숨기면 사용자가 터널을 의도적으로 또는 실수로 우회하는 것을 방지합니다. 탭 잠금은 연결 해제 시 취소되고 해당 탭에 적용된 관리자 정의 정책에 따라 교체됩니다. 잠금 기능이 발생하는 조건은 다음과 같습니다.

- ASA 구성이 Connections(연결) 탭 잠금을 지정한 경우
- ASA 구성이 사설 측 프록시를 지정한 경우
- Windows 그룹 정책이 이전에 Connections(연결) 탭을 잠근 경우(잠금 없는 ASA 그룹 정책 설정 재정의)

그룹 정책에서 프록시 잠금을 허용 또는 허용하지 않도록 ASA를 구성할 수 있습니다. ASDM를 사용하여 이 작업을 수행하려면 다음 절차를 따르십시오.

프로시저

단계 **1** ASDM에서 **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 새 그룹 정책 **Edit**(편집) 또는 **Add**(추가)를 클릭합니다.

단계 **3** 탐색 창에서 **Advanced**(고급) > **Browser Proxy**(브라우저 프록시)로 이동하십시오. Proxy Server Policy(프록시 서버 정책) 창이 표시됩니다.

단계 **4** **Proxy Lockdown**(프록시 잠금)을 클릭하여 추가 프록시 설정을 표시합니다.

단계 **5** **Inherit(**상속**)** 의 선택을 해제하고 **Yes(**예**)** 를 선택하여 프록시 잠금을 활성화하고 AnyConnect 세션 중에 Internet Explorer 연결 탭을 숨기거나 **No(**아니요**)** 를 선택하여 프록시 잠금을 비활성화하고 AnyConnect 세션 중에 Internet Explorer 연결 탭을 표시하십시오.

단계 **6** **OK(**확인**)**를 클릭하여 프록시 서버 정책 변경사항을 저장합니다.

단계 **7** **Apply(**적용**)**를 클릭하여 그룹 정책 변경사항을 저장합니다.

프록시 설정 확인

- Windows의 경우: 아래 레지스트리에서 프록시 설정을 찾습니다.

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
```

- macOS의 경우: 터미널 창을 열고 다음을 입력합니다.

```
scutil --proxy
```

VPN 트래픽 선택 및 제외

VPN을 우회하도록 IPv4 또는 IPv6 트래픽 구성

ASA가 IPv6 트래픽만 예상할 때 AnyConnect 클라이언트에서 IPv4 트래픽을 관리하는 방법 또는 ASA가 IPv4 트래픽만 예상할 때 AnyConnect에서 IPv6 트래픽을 관리하는 방법을 클라이언트 우회 프로토콜 설정을 사용하여 구성할 수 있습니다.

AnyConnect 클라이언트에서 ASA에 VPN 연결을 설정하는 경우 ASA는 클라이언트에 IPv4, IPv6 또는 두 주소 모두를 할당할 수 있습니다.

클라이언트 우회 프로토콜이 IP 프로토콜용으로 활성화되어 있고 주소 풀이 해당 프로토콜에 대해 구성되지 않은 경우(즉, 해당 프로토콜의 IP 주소가 ASA를 통해 클라이언트에 할당되지 않음), 해당 프로토콜을 사용하는 모든 IP 트래픽이 VPN 터널을 통해 전송되지 않습니다. IP 트래픽은 터널 외부로 전송됩니다.

클라이언트 우회 프로토콜이 비활성화되어 있고 주소 풀이 해당 프로토콜에 대해 구성되지 않은 경우, 클라이언트는 VPN 터널이 설정되면 해당 IP 프로토콜에 대한 모든 트래픽을 삭제합니다.

예를 들어 ASA에서 AnyConnect 연결에 IPv4 주소만 할당하고 엔드포인트가 이중 스택이라고 가정합니다. 엔드포인트가 IPv6 주소에 연결하려고 시도할 때 클라이언트 우회 프로토콜이 비활성화되어 있는 경우 IPv6 트래픽이 삭제됩니다. 클라이언트 우회 프로토콜이 활성화되어 있는 경우 IPv6 트래픽은 클라이언트에서 암호화되지 않은 상태로 전송됩니다.

그룹 정책의 ASA에 클라이언트 우회 프로토콜을 구성합니다.

프로시저

단계 **1** ASDM에서 **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 새 그룹 정책 **Edit**(편집) 또는 **Add**(추가)를 클릭합니다.

단계 **3** **Advanced**(고급) > **AnyConnect**를 선택하십시오.

단계 **4** 기본 그룹 정책이 아닌 그룹 정책인 경우 **Client Bypass Protocol**(클라이언트 우회 프로토콜)옆에서 **Inherit**(상속) 를 선택 취소합니다.

단계 **5** 다음 옵션 중 하나를 선택합니다.

- ASA가 주소를 할당하지 않은 IP 트래픽을 삭제하려면 **Disable**(비활성화) 을 클릭합니다.
- 암호화되지 않은 상태로 IP 트래픽을 전송하려면 **Enable**(활성화) 을 클릭합니다.

단계 **6** **OK**(확인)를 클릭합니다.

단계 **7** **Apply**(적용)를 클릭합니다.

로컬 프린터 및 테더링 디바이스가 지원되는 클라이언트 방화벽 구성

Cisco ASA Series 환경 설정 가이드의 로컬 프린터 및 테더링 디바이스가 지원되는 클라이언트 방화벽 섹션을 참조하십시오.

스플릿 터널링 구성

스플릿 터널링이 네트워크(클라이언트) 액세스 그룹 정책에 구성되어 있습니다. Cisco ASA Series VPN 환경 설정 가이드의 *AnyConnect* 트래픽용 스플릿 터널링 구성 섹션을 참조하십시오.

ASDM에서 그룹 정책을 변경한 후 **Configuration**(구성) > **Remote Access VPN**(원격 액세스 **VPN**) > **Network (Client) Access**(네트워크(클라이언트) 액세스) > **AnyConnect Connection Profiles**(**AnyConnect** 연결 프로파일) > **Add/Edit**(추가/편집) > **Group Policy**(그룹 정책)에서 그룹 정책이 연결 프로파일과 연결되어 있는지 확인하십시오.

동적 스플릿 터널링 정보

동적 스플릿 터널링은 ASDM 그룹 정책 컨피그레이션의 Exclude Network List Below(아래 네트워크 목록 제외) 옵션을 사용하여 구성된 현재 스플릿 터널링 옵션을 개선하기 위해 설계된 것입니다. 동적 스플릿 터널링 제외는 일반적으로 스플릿 터널링을 정의하는 데 사용되는 정적 제외뿐 아니라, 특정 서비스와 관련된 트래픽을 런타임에 VPN 터널에서 동적으로 제외해야 하는 시나리오도 처리합니다. 여러 클라우드 기반 서비스가 같은 IP 풀에서 호스트되는데 사용자의 위치 또는 클라우드에서 호스트되는 컴퓨팅 리소스의 부하에 따라 서로 다른 IP 주소로 확인되는 경우를 예로 들 수 있습니다. 관리자가 이와 같은 서비스 중 하나만 VPN 터널에서 제외하려는 경우 정적 제외를 사용하여 해당 정

책을 정의하기는 어렵습니다. 특히 ISP NAT, 6to4, 4to6 및 기타 네트워크 변환 기법도 고려하는 경우에는 정책 정의가 더욱 까다롭습니다.

정적 스플릿 터널링과 동적 스플릿 터널링 간의 상호운용성

정적 터널 및 동적 터널 제외 또는 포함이 함께 사용될 수 있습니다. 터널 설정 시에는 정적 스플릿 터널링이 적용되는 반면, 터널이 이미 연결되어 있는 상태에서 제외하거나 포함할 도메인에 대한 트래픽이 생성되면 동적 스플릿 터널링이 적용됩니다. 동적 스플릿 터널링은 "모두 터널링", "스플릿 포함" 및 "스플릿 제외" 터널링에 적용됩니다.

- Tunnel All Networks(모든 네트워크 터널링) - VPN 터널의 모든 제외가 동적으로 수행됩니다.
- Exclude Specific Networks(특정 네트워크 제외) - 사전 구성된 정적 제외에 동적 제외가 추가됩니다.
- Include Specific Networks(특정 네트워크 포함) - 제외된 호스트 이름의 IP 주소 하나 이상이 스플릿 포함 네트워크와 중복되는 경우에만 동적 제외가 수행됩니다. 그렇지 않은 경우에는 트래픽이 VPN 터널에서 이미 제외된 상태이므로 동적 제외가 수행되지 않습니다.

향상된 동적 스플릿 제외 터널링은 "모두 터널링" 및 "스플릿 제외" 터널링에 적용됩니다. 동적 스플릿 제외 도메인과 동적 스플릿 포함 도메인 및 스플릿 포함 터널링이 모두 구성되어 있는 경우에 생성되는 컨피그레이션은 향상된 동적 스플릿 포함 터널링입니다.

동적 제외는 아직 제외되지 않은 IP 주소에만 적용됩니다. 정적 및 동적 제외가 모두 적용되어 있는 상태에서 새 동적 제외를 시행해야 하는 경우에는 이미 적용된 제외와의 충돌이 발생할 수 있습니다. 제외된 도메인 이름과 일치하는 DNS 응답의 일부분인 모든 IP 주소를 포함하는 동적 제외를 시행하면 아직 제외되지 않은 주소만 제외 대상으로 고려됩니다.

정적 또는 동적 스플릿 터널링을 활성화하면 Umbrella 로밍 보안 보호가 활성화됩니다. Umbrella 클라우드 확인자가 연결 가능하며 VPN 터널을 통해 프로브할 수 있는 경우가 아니면 해당 확인자를 정적으로 VPN 터널에서 제외해야 할 수 있습니다.

동적 스플릿 터널링 사용 알림

VPN 터널이 연결되어 있는 동안에는 여러 가지 방식으로 동적 스플릿 터널링에 대해 설정된 옵션을 확인할 수 있습니다.

- Statistics(통계) 탭 - ASA 그룹 정책에 구성된 VPN 터널에서 제외되는 도메인 이름을 포함하는 Dynamic Tunnel Exclusions(동적 터널 제외)가 표시됩니다.
- Export Stats(내보내기 통계) - VPN 터널링에서 제외되는 도메인 이름과 IPv4 및 IPv6용 터널 모드가 포함된 파일이 생성됩니다.
- Route Details(경로 세부사항) 탭 - IPv4 및 IPv6 동적 스플릿 제외 경로와, 제외된 각 IP 주소에 해당하는 호스트 이름이 표시됩니다.
- VPN 컨피그레이션 로그 메시지 - VPN 터널에서 제외되는 도메인 수가 표시됩니다.

동적 스플릿 터널링 구성

시작하기 전에

동적 스플릿 터널링 정보, 144 페이지을 참조하십시오.

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 ASA에서 그룹 정책에 추가하는 방식으로 동적 스플릿 터널링을 구성합니다. GUI 단계는 *Cisco ASA Series VPN ASDM* 환경 설정 가이드에서 동적 스플릿 터널링 구성을 참조하십시오.

프로시저

단계 **1** 다음 명령을 사용하여 WebVPN 컨텍스트에서 맞춤형 속성 유형을 정의합니다. `anyconnect-custom-attr dynamic-split-exclude-domains description dynamic split exclude domains`

단계 **2** VPN 터널 외부의 클라이언트가 액세스해야 하는 각 클라우드/웹 서비스에 대해 맞춤형 속성 이름을 정의합니다. 예를 들어 Google 웹 서비스와 관련된 DNS 도메인 이름 목록을 표시하려면 Google_domains를 추가합니다. 속성 값에는 VPN 터널에서 제외할 도메인 이름 목록이 포함됩니다. 이 목록은 다음 목록을 예시로 사용하여 각 이름을 CSV(쉼표로 구분된 값) 형식으로 생성해야 합니다.
`anyconnect-custom-data dynamic-split-exclude-domains webex_service_domains webex.com, webexconnect.com, tags.tiqcdn.com`

단계 **3** 그룹 정책 속성 컨텍스트에서 실행되는 다음 명령을 사용하여 앞에서 정의한 맞춤형 속성을 특정 정책 그룹에 연결합니다. `anyconnect-custom dynamic-split-exclude-domains value webex_service_domains`

스플릿 DNS

스플릿 DNS가 네트워크(클라이언트) 액세스 그룹 정책에 구성되어 있는 경우, AnyConnect는 특정 DNS 쿼리를 개인 DNS 서버(그룹 정책에도 구성되어 있음)에 터널링합니다. 기타 모든 DNS 쿼리는 DNS 확인용으로 암호화되지 않은 상태에서 클라이언트 운영 체제의 DNS 확인자로 이동합니다. 스플릿 DNS가 구성되지 않은 경우, AnyConnect는 모든 DNS 쿼리를 터널링합니다.

스플릿 DNS 요건

스플릿 DNS는 표준 및 업데이트 쿼리(A, AAAA, NS, TXT, MX SOA, ANY, SRV, PTR 및 CNAME)를 지원합니다. 터널링된 네트워크의 쿼리와 일치하는 PTR 쿼리는 터널을 통해 사용할 수 있습니다.

AnyConnect 스플릿 DNS는 Windows와 macOS 플랫폼에서 지원됩니다.

macOS에서 AnyConnect는 다음 조건 중 하나를 충족하는 경우에만 특정 IP 프로토콜에 정확한 스플릿 DNS를 사용할 수 있습니다.

- 스플릿 DNS는 하나의 IP 프로토콜(IPv4 등)용으로 구성되었으며 클라이언트 우회 프로토콜은 그룹 정책에서 기타 IP 프로토콜(IPv6 등)용으로 구성되었습니다(기타 IP 프로토콜용으로 구성된 주소 풀 없음).

• 스플릿 DNS는 이 두 가지 IP 프로토콜용으로 구성됩니다.

스플릿 DNS 구성

그룹 정책에서 스플릿 DNS를 구성하려면 다음을 수행하십시오.

프로시저

단계 1 최소 1개 이상의 DNS 서버를 구성합니다.

Cisco ASA Series VPN 환경 설정 가이드의 내부 그룹 정책용 서버 속성 구성 섹션을 참조하십시오.

지정된 개인 DNS 서버가 클라이언트 플랫폼에 대해 구성된 DNS 서버와 중복되지 않는지 확인합니다. 서버가 중복되는 경우 이름 확인 기능이 제대로 작동하지 않으며 쿼리가 삭제될 수 있습니다.

단계 2 스플릿 포함 터널링 구성:

Configuration(구성) > **Remote Access VPN**(원격 액세스 **VPN**) > **Network (Client) Access**(네트워크(클라이언트) 액세스) > **Group Policies**(그룹 정책) > **Advanced**(고급) > **Split Tunneling**(스플릿 터널링) 창에서 **Tunnel Network List Below**(아래 네트워크 목록 터널링) 정책을 선택하고 터널링할 주소의 **Network List**(네트워크 목록)를 지정합니다.

스플릿 DNS는 Exclude Network List Below(아래 네트워크 목록 제외) 스플릿 터널링 정책을 지원하지 않습니다. 스플릿 DNS를 구성하려면 Tunnel Network List Below(아래 네트워크 목록 터널링) 스플릿 터널링 정책을 사용해야 합니다.

단계 3 스플릿 DNS 구성:

Configuration(구성) > **Remote Access VPN**(원격 액세스 **VPN**) > **Network (Client) Access**(네트워크(클라이언트) 액세스) > **Group Policies**(그룹 정책) > **Advanced**(고급) > **Split Tunneling**(스플릿 터널링) 창에서 **Send All DNS lookups through tunnel**(터널을 통해 모든 **DNS** 조회 전송)을 선택 취소하고 **DNS Names**(**DNS** 이름)에서 쿼리를 터널링할 도메인 이름을 지정합니다.

다음에 수행할 작업

ASDM에서 그룹 정책을 변경한 후 **Configuration**(구성) > **Remote Access VPN**(원격 액세스 **VPN**) > **Network (Client) Access**(네트워크(클라이언트) 액세스) > **AnyConnect Connection Profiles**(**AnyConnect** 연결 프로파일) > **Add/Edit**(추가/편집) > **Group Policy**(그룹 정책)에서 그룹 정책이 연결 프로파일과 연결되어 있는지 확인하십시오.

AnyConnect 로그를 사용하여 스플릿 DNS 확인

스플릿 DNS가 활성화되어 있는지 확인하려면 AnyConnect 로그에서 "수신한 VPN 세션 구성 설정" 이 포함된 항목을 검색합니다. 해당 항목은 스플릿 DNS가 활성화되어 있는지를 나타냅니다. IPv4 및 IPv6 스플릿 DNS에 대한 개별 로그 항목이 있습니다.

스플릿 DNS를 사용하는 도메인 확인

도메인 이름 확인을 위해 운영 체제의 DNS 확인자를 사용하는 모든 툴 또는 애플리케이션을 사용할 수 있습니다. 예를 들어 ping이나 웹 브라우저를 사용하여 스플릿 DNS 솔루션을 테스트할 수 있습니다. nslookup 또는 dig과 같은 다른 툴은 OS DNS 확인자를 우회합니다.

클라이언트를 사용하여 스플릿 DNS에 사용되는 도메인을 확인하려면 다음 단계를 수행하십시오.

프로시저

단계 **1** **ipconfig/all** 을 실행하고 DNS 접미사 검색 목록 옆에 나열된 도메인을 기록합니다.

단계 **2** VPN 연결을 설정하고 다시 DNS 접미사 검색 목록 옆에 나열된 도메인을 확인합니다.

터널을 설정한 후에 추가되는 도메인은 스플릿 DNS에 사용되는 도메인입니다.

참고 이 프로세스에서는 ASA에서 푸시된 도메인이 클라이언트 호스트에 이미 구성되어 있는 도메인과 중복되지 않는다고 가정합니다.

VPN 인증 관리

중요한 보안 고려 사항

- 사용자가 실수로 Rogue 서버의 인증서를 신뢰하도록 브라우저를 구성할 가능성이 있고 보안 게이트웨이에 연결할 때 사용자가 보안 경고에 응답해야 하는 불편함이 발생할 수 있으므로 보안 게이트웨이에서 자체 서명된 인증서를 사용하지 않는 것이 좋습니다.
- 다음과 같은 이유로 인해 AnyConnect 클라이언트에 대해 엄격한 인증서 신뢰를 활성화하는 것이 좋습니다.

  Strict Certificate Trust(엄격한 인증서 신뢰)를 구성하려면 로컬 정책 파라미터 및 값 섹션(로컬 정책 파라미터 및 값, 109 페이지)을 참조하십시오.

서버 인증서 처리 구성

서버 인증서 확인

- (Windows에만 해당됨) SSL 및 IPsec VPN 연결 둘 다에 대해 CRL(인증서 해지 목록) 확인을 수행할 수 있습니다. 프로파일 편집기에서 활성화되어 있는 경우 AnyConnect는 체인의 모든 인증서에 대해 업데이트된 CRL을 검색합니다. 그런 다음 해당하는 인증서가 더 이상 신뢰해서는 안 되는 해지된 인증서 중에 포함되어 있는지 여부를 확인하고, 이 인증서가 인증 증명에 의해 해지된 인증서로 확인되면 연결하지 않습니다. 자세한 내용은 로컬 정책 파라미터 및 값, 109 페이지을 참조하십시오.

- 사용자가 서버 인증서를 사용하여 구성된 ASA에 연결한 경우, 신뢰 체인(루트, 중개 디바이스 등)에 문제가 있는 경우에도 해당 인증서를 신뢰하고 가져오기 위한 확인란이 계속 표시됩니다. 다른 인증서 문제가 있는 경우 확인란이 표시되지 않습니다.
- FQDN을 통해 수행 중인 SSL 연결은 FQDN을 사용하는 초기 확인이 실패할 경우, 이름 확인을 위해 FQDN에서 확인한 IP 주소로 2차 서버 인증서 확인을 수행하지 않습니다.
- IPsec 및 SSL 연결은 서버 인증서에 키 사용이 포함된 경우, 특성에 DigitalSignature 및 KeyAgreement 또는 KeyEncipherment를 포함해야 합니다. 서버 인증서에 EKU가 포함된 경우, 특성에 serverAuth(SSL 및 IPsec용) 또는 ikeIntermediate(IPsec 전용)를 포함해야 합니다. 참고로 KU 또는 EKU를 수락하기 위해 서버 인증서에 이를 포함할 필요는 없습니다.
- IPsec 연결은 서버 인증서에서 이름 확인을 수행합니다. 다음 규칙은 IPsec 이름 확인에 적용됩니다.
  - 주제 대체 이름 확장에 관련 특성이 함께 제공되는 경우, 이름 확인은 주제 대체 이름에 대해서만 수행됩니다. 관련 특성에는 모든 인증서의 DNS 이름 특성이 포함되며 IP 주소에 연결이 진행 중인 경우에는 IP 주소 특성도 포함됩니다.
  - 주제 대체 이름 확장이 제공되지 않거나 제공되지만 관련된 특성을 포함하지 않는 경우, 이름 확인은 인증서의 제목에서 발견된 공통 이름 특성에 대해 수행됩니다.
  - 인증서에서 이름 확인을 위해 와일드카드를 사용하는 경우, 와일드카드는 첫 번째(맨 왼쪽) 하위 도메인에만 있어야 하며 또한 이 하위 도메인에 있는 마지막(맨 오른쪽) 문자여야 합니다. 규정을 준수하지 않는 와일드카드 항목은 이름 확인을 위해 무시됩니다.
- OSX의 경우 만료된 인증서는 키 체인 액세스가 "Show Expired Certificates(만료된 인증서 표시)"로 구성된 경우에만 표시됩니다. 만료된 인증서는 기본적으로 숨겨져 있어서 사용자에게 혼란을 줄 수 있습니다.

유효하지 않은 서버 인증서 처리

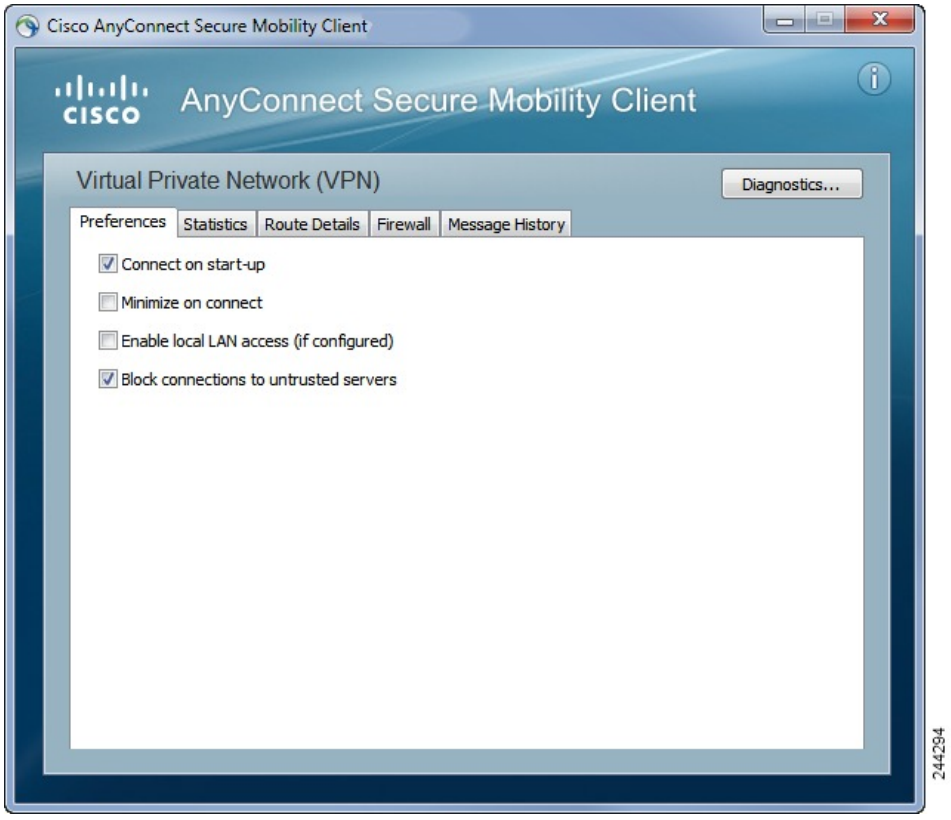
신뢰할 수 없는 네트워크의 모바일 사용자에 대한 대상 공격이 증가함에 따라 심각한 보안 침입을 차단할 수 있도록 클라이언트의 보안 보호 기능을 개선했습니다. 기본 클라이언트 동작이 중간자 공격(Man-in-the-Middle Attack)에 대응하여 추가 방어 계층을 제공하도록 변경되었습니다.

사용자 상호 작용

사용자가 보안 게이트웨이에 연결을 시도할 때 인증서 오류(예: 만료됨, 유효하지 않은 날짜, 잘못된 키 사용 또는 CN 불일치)가 발생하는 경우, Change Settings(설정 변경) 및 Keep Me Safe(사용자 보안 유지) 버튼이 있는 빨간색 대화 상자가 사용자에게 표시됩니다.

참고 Linux의 경우 대화 상자가 본 문서에 표시된 대화 상자와 다를 수 있습니다.

- **Keep Me Safe(**사용자 보안 유지)를 클릭하면 연결이 취소됩니다.
- **Change Settings(**설정 변경**)**를 클릭하여 AnyConnect의 Advanced(고급) > VPN > Preferences(환경 설정)를 열면 신뢰할 수 없는 서버에 대한 연결을 활성화할 수 있습니다. 현재 연결 시도는 취소됩니다.



사용자가 **Block connections to untrusted servers(**신뢰할 수 없는 서버에 대한 연결 차단**)**확인란의 선택을 취소하고 신뢰할 수 없는 CA가 인증서에 관련된 유일한 문제인 경우, 사용자가 다음에 해당 보안 게이트웨이에 대한 연결을 시도할 때 사용자에게 Certificate Blocked Error(차단된 인증서 오류) 대화 상자가 표시되지 않고 다음 대화 상자만 표시됩니다.

사용자가 **Always trust this VPN server and import the certificate(**이 **VPN** 서버를 항상 신뢰하고 인증서 가져오기**)** 확인란을 선택하면 이후 해당 보안 게이트웨이에 연결할 때 사용자에게 프롬프트가 더 이상 표시되지 않습니다.

참고 사용자가 **AnyConnect Advanced(**고급**) > VPN > Preferences(**기본 설정**)**에서 **Block connections to untrusted servers(**신뢰할 수 없는 연결 차단**)**의 확인란을 선택하거나 사용자의 컨피그레이션이 지침 및 제한 사항 항목 섹션 아래에 설명된 모드 목록 중 한 가지 조건을 충족하는 경우, AnyConnect가 유효하지 않은 서버 인증서를 거부합니다.

향상된 보안 동작

클라이언트가 올바르지 않은 서버 인증서를 허용하면 해당 인증서가 클라이언트의 인증서 저장소에 저장됩니다. 이전에는 인증서의 지문만 저장되었습니다. 사용자가 유효하지 않은 서버 인증서를 항상 신뢰하고 가져오도록 선택한 경우에만 유효하지 않은 인증서가 저장됩니다.

최종 사용자의 보안 수준을 자동으로 낮추는 관리 재정의 기능은 없습니다. 엔드 유저의 이전 보안 결정 사항을 완전히 제거하려면 사용자의 로컬 정책 파일에서 **Strict Certificate Trust(**엄격한 인증서 신뢰**)**를 활성화하십시오. Strict Certificate Trust(엄격한 인증서 신뢰)를 활성화하면 사용자에게 오류 메시지가 표시되고 연결이 실패하지만 사용자 프롬프트는 표시되지 않습니다.

로컬 정책 파일에서 Strict Certificate Trust(엄격한 인증서 신뢰)를 활성화하는 방법에 대한 자세한 내용은 *AnyConnect* 로컬 정책 파라미터 및 값 섹션(로컬 정책 파라미터 및 값, 109 페이지)을 참조하십시오.

지침 및 제한 사항

다음과 같은 경우 유효하지 않은 서버 인증서가 거부됩니다.

- AnyConnect VPN 클라이언트 프로파일에서 Always-On 기능이 활성화되어 있고 적용된 그룹 정책 또는 DAP로 인해 꺼지지 않습니다.
- 클라이언트에서 로컬 정책의 Strict Certificate Trust(엄격한 인증서 신뢰)가 활성화되어 있습니다.
- AnyConnect는 로그온 전에 시작되도록 구성되어 있습니다.
- 머신 인증서 저장소의 클라이언트 인증서가 인증에 사용됩니다.

인증서 전용 인증 구성

사용자 이름 및 비밀번호가 있는 AAA 또는 디지털 인증서(또는 두 가지 모두)를 사용하여 사용자를 인증할지 여부를 지정할 수 있습니다. 인증서 전용 인증을 구성한 경우 사용자는 디지털 인증서에 연결할 수 있고 사용자 ID와 비밀번호를 제공할 필요가 없습니다.

여러 그룹을 사용하는 환경에서 인증서 전용 인증을 지원하기 위해 두 개 이상의 그룹 URL을 프로비저닝할 수 있습니다. 각 그룹 URL에는 그룹별 인증서 맵을 생성할 수 있도록 사용자 정의된 데이터의 일부 조각이 있는 다양한 클라이언트 프로파일이 포함되어 있습니다. 예를 들어 이 프로세스에서 인증서가 ASA에 제공될 경우 이 그룹에서 사용자를 배치하도록 엔지니어링의 Department_OU 값이 ASA에서 프로비저닝될 수 있습니다.

참고 보안 게이트웨이에 클라이언트를 인증하는 데 사용되는 인증서는 유효하고 신뢰할 수 있어야(CA에서 서명함) 합니다. 자체 서명된 클라이언트 인증서는 사용할 수 없습니다.

프로시저

단계 **1** **Configuration(**구성**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**)** > **AnyConnect Connection Profiles(AnyConnect** 연결 프로파일**)**로 이동합니다. 연결 프로파일을 선택하고 Edit(편집)를 클릭합니다. Edit AnyConnect Connection Profile(AnyConnect 연결 프로파일 편집) 창이 열립니다.

단계 **2** 창이 표시되지 않으면 창의 왼쪽 창에서 탐색 트리의 **Basic(**기본**)** 노드를 클릭합니다. 창의 오른쪽 창에 있는 **Authentication(**인증**)** 영역에서 **Certificate(**인증서**)**방법을 활성화합니다.

단계 **3** **OK(**확인**)** 를 클릭하여 변경사항을 적용합니다.

인증서 등록 구성

Cisco AnyConnect Secure Mobility Client 는 SCEP(Simple Certificate Enrollment Protocol, 단순 인증서 등록 프로토콜)를 사용하여 클라이언트 인증의 일부로 인증서를 프로비저닝하고 갱신합니다. SCEP를 사용하는 인증서 등록은 AnyConnect IPsec 및 ASA에 대한 SSL VPN 연결에서 다음 방법으로 지원됩니다.

- SCEP 프록시: ASA는 클라이언트와 CA(Certificate Authority, 인증 기관) 간에 SCEP 요청과 응답을 위한 프록시로 작동합니다.
  - 클라이언트가 CA에 직접 액세스하지 않으므로 CA는 AnyConnect 클라이언트가 아니라 ASA에 액세스할 수 있어야 합니다.
  - 등록은 클라이언트에서 항상 자동으로 시작됩니다. 사용자가 관여할 필요가 없습니다.
- 레거시 SCEP: AnyConnect 클라이언트는 인증서를 등록 및 구입하기 위해 CA와 직접 통신합니다.
  - CA는 설정된 VPN 터널을 통해 또는 클라이언트가 있는 동일한 네트워크에서 직접, ASA가 아닌 AnyConnect 클라이언트에 액세스할 수 있어야 합니다.
  - 등록은 클라이언트에서 자동으로 시작되며 구성된 경우 사용자가 수동으로 시작할 수도 있습니다.

관련 항목

AnyConnect 프로파일 편집기, 인증서 등록, 102 페이지

SCEP 프록시 등록 및 운영

다음 단계에서는 AnyConnect 및 ASA가 SCEP 프록시에 대해 구성된 경우 인증서를 얻고 인증서 기반 연결을 수행하는 방법에 대해 설명합니다.

1. 사용자는 인증서 및 AAA 인증 모두에 대해 구성된 연결 프로파일을 사용하여 ASA 헤드엔드에 연결합니다. ASA는 클라이언트에서 인증을 위해 인증서 및 AAA 자격 증명을 요청합니다.
2. 사용자는 자신의 AAA 자격 증명을 입력하지만 유효한 인증서를 사용할 수 없습니다. 이러한 상황으로 인해 입력한 AAA 자격 증명을 사용하여 터널을 설정한 이후에 클라이언트에서 자동 SCEP 등록 요청을 전송합니다.
3. ASA는 CA에 등록 요청을 전달하며 CA 응답을 클라이언트에 반환합니다.
4. SCEP 등록에 성공하면 클라이언트는 구성 메시지를 사용자에게 제공하고 현재 세션과의 연결을 끊습니다. 사용자는 이제 인증서 인증을 사용하여 ASA 터널 그룹에 연결할 수 있습니다.

   SCEP 등록에 실패하면 클라이언트는 구성 메시지를 사용자에게 제공하고 현재 세션과의 연결을 끊습니다. 사용자는 관리자에게 문의해야 합니다.

기타 SCEP 프록시 운영 고려 사항:

- 구성이 완료된 경우, 클라이언트는 사용자 개입 없이 만료 전 자동으로 인증서를 갱신합니다.
- SCEP 프록시 등록 시 SSL 및 IPsec 터널 인증서 인증을 위해 SSL을 사용합니다.

레거시 SCEP 등록 및 운영

다음 단계에서는 AnyConnect가 레거시 SCEP에 대해 구성되어 있을 때의 인증서 획득 방법 및 인증서 기반 연결 방법에 관해 설명합니다.

1. 사용자가 인증서 인증을 위해 구성된 터널 그룹을 사용하여 ASA 헤드엔드에 대한 연결을 시작할 때 ASA는 클라이언트에서 인증에 필요한 인증서를 요청합니다.
2. 유효한 인증서는 클라이언트에서 사용할 수 없습니다. 연결을 설정할 수 없습니다. 이 인증서 실패는 SCEP를 등록해야 함을 나타냅니다.
3. 사용자는 클라이언트 프로파일에서 구성된 자동 SCEP 호스트와 주소가 일치하는 AAA 인증에 대해서만 구성된 터널 그룹을 사용하여 ASA 헤드엔드에 대한 연결을 시작해야 합니다. ASA는 클라이언트에서 AAA 자격 증명을 요청합니다.
4. 클라이언트가 사용자에게 AAA 자격 증명을 입력하라는 대화 상자를 표시합니다.

   클라이언트가 수동 등록을 위해 구성되고 클라이언트가 SCEP 등록을 시작해야 한다는 것을 알고 있는 경우(2단계 참조) 자격 증명 대화 상자에 **Get Certificate(**인증서 가져오기**)** 버튼이 표시됩니다. 클라이언트에 네트워크의 CA에 대한 직접 액세스 권한이 있는 경우, 사용자가 이 버튼을 클릭하여 인증서를 수동으로 가져올 수 있습니다.

참고 CA에 대한 액세스가 설정된 VPN 터널에 의존하는 경우 현재 설정된 VPN 터널이 없으므로 이 시점에서는 수동으로 등록할 수 없습니다(AAA 자격 증명을 입력하지 않은 경우).

5. 사용자가 AAA 자격 증명을 입력하고 VPN 연결을 설정합니다.
6. 클라이언트가 SCEP 등록을 시작해야 한다는 것을 알고 있습니다(2단계 참조). 설정된 VPN 터널을 통해 CA에 등록 요청을 시작하고 CA로부터 응답을 수신합니다.
7. SCEP 등록에 성공하면 클라이언트는 구성 메시지를 사용자에게 제공하고 현재 세션과의 연결을 끊습니다. 사용자는 이제 인증서 인증을 사용하여 ASA 터널 그룹에 연결할 수 있습니다.

   SCEP 등록에 실패하면 클라이언트는 구성 메시지를 사용자에게 제공하고 현재 세션과의 연결을 끊습니다. 사용자는 관리자에게 문의해야 합니다.

기타 레거시 SCEP 운영 고려 사항:

- 클라이언트가 수동 등록을 위해 구성되어 있고 **Certificate Expiration Threshold(**인증서 만료 임계값**)** 가 충족되면 표시된 터널 그룹 선택 대화 상자에 **Get Certificate(**인증서 가져오기**)** 버튼이 표시됩니다. 사용자는 이 버튼을 클릭하여 인증서를 수동으로 갱신할 수 있습니다.
- 인증서가 만료되고 클라이언트에 더 이상 유효한 인증서가 없는 경우 클라이언트가 레거시 SCEP 등록 프로세스를 반복합니다.

인증 기관 요건

- IOS CS를 포함하여 모든 SCEP 호환 CA, Windows Server 2003 CA 및 Windows Server 2008 CA가 지원됩니다.
- CA는 자동 허용 모드여야 하며 인증서에 대한 폴링은 지원되지 않습니다.
- 일부 CA에서 추가 보안 계층을 위해 사용자에게 등록 비밀번호를 이메일로 보내도록 구성할 수 있습니다. CA 비밀번호는 사용자를 식별하기 위해 인증 기관에 전송되는 시도용 비밀번호 또는

토큰입니다. 그런 다음 AnyConnect 클라이언트 프로파일에서 비밀번호를 구성할 수 있으며 이 프로파일은 CA가 인증서를 허용하기 전에 확인하는 SCEP 요청의 일부가 됩니다. 수동 레거시 SCEP 등록을 사용하는 경우, 클라이언트 프로파일에서 CA 비밀번호를 활성화하는 것이 좋습니다.

인증서 등록에 대한 지침

- ASA에 대한 클라이언트리스 브라우저 기반의 VPN 액세스에서는 SCEP 프록시를 지원하지 않습니다. 단 WebLaunch(클라이언트 없이 시작한 AnyConnect)는 지원합니다.
- ASA 로드 밸런싱 기능은 SCEP 등록을 통해 지원됩니다.
- ASA는 클라이언트에서 수신한 요청을 로그하지만 등록이 실패한 원인은 표시하지 않습니다. 연결 문제를 CA 또는 클라이언트에서 디버깅해야 합니다.
- ASA에서 인증서 전용 인증 및 인증서 매핑:

  여러 그룹을 사용하는 환경에서 인증서 전용 인증을 지원하기 위해 두 개 이상의 그룹 URL을 프로비저닝할 수 있습니다. 각 그룹 URL에는 그룹별 인증서 맵을 생성할 수 있도록 사용자 정의된 데이터의 일부 조각이 있는 다양한 클라이언트 프로파일이 포함되어 있습니다. 예를 들어 이 프로세스에서 인증서가 ASA에 제공될 경우 이 터널 그룹에서 사용자를 배치하도록 엔지니어링의 Department_OU 값이 ASA에서 프로비저닝될 수 있습니다.
- 정책 적용을 위한 등록 연결 식별:

  ASA에서 aaa.cisco.sceprequired 특성을 사용하여 등록 연결을 확인하고 선택한 DAP 레코드에서 적절한 정책을 적용할 수 있습니다.
- Windows 인증서 경고:

  Windows 클라이언트가 처음으로 인증 기관의 인증서를 검색하려고 시도할 경우, 경고가 나타날 수 있습니다. 사용자는 프롬프트가 표시되면 Yes(예)를 클릭해야 합니다. 이렇게 해야 루트 인증서를 가져올 수 있습니다. 클라이언트 인증서와의 연결 기능에는 영향을 주지 않습니다.

SCEP 프록시 인증서 등록 구성

SCEP 프록시 등록을 위한 VPN 클라이언트 프로파일 구성

프로시저

단계 1 VPN 프로파일 편집기를 열고 탐색 창에서 **Certificate Enrollment(**인증서 등록**)** 를 선택합니다.

단계 2 **Certificate Enrollment(**인증서 등록**)**를 선택합니다.

단계 3 등록 인증서에서 어떤 **Certificate Contents(**인증서 콘텐츠**)** 를 요청할지 구성합니다. 인증서 필드의 정의에 대해서는 AnyConnect 프로파일 편집기, 인증서 등록을 참조하십시오.

참고
- %machineid%를 사용하는 경우, 데스크톱 클라이언트에 HostScan/Posture를 로드해야 합니다.
- 모바일 클라이언트의 경우, 적어도 1개의 인증서 필드를 지정해야 합니다.

SCEP 프록시 등록을 지원하기 위한 ASA 구성

SCEP 프록시의 경우 단일 ASA 연결 프로파일이 인증서 등록 및 인증서로 인증된 VPN 연결을 지원합니다.

프로시저

단계 1 그룹 정책을 생성합니다(예: cert_group). 다음 필드를 설정하십시오.
- General(일반) 설정의 **SCEP Forwarding URL(SCEP** 전달 **URL)**에서CA에 URL을 입력합니다.
- Advanced(고급) > AnyConnect Client(AnyConnect 클라이언트) 창에서 다운로드할 클라이언트 프로파일에 대해 **Inherit(**상속**)**를 선택 취소하고 SCEP 프록시에 대해 구성된 클라이언트 프로파일을 지정합니다. 예를 들어, ac_vpn_scep_proxy 클라이언트 프로파일을 지정합니다.

단계 2 인증서 등록 및 인증서로 인증된 연결을 위해 연결 프로파일을 생성합니다(예: cert_tunnel).
- 인증: 모두(AAA 및 인증서)
- 기본 그룹 정책: cert_group
- Advanced(고급) > General(일반)에서 **Enable SCEP Enrollment for this Connction Profile(**이 연결 프로파일에 대해 **SCEP** 등록 활성화**)**을 선택합니다.
- Advanced(고급) > GroupAlias/Group URL(그룹 별칭/그룹 URL)에서 이 연결 프로파일에 대한 그룹(cert_group)을 포함하는 그룹 URL을 생성합니다.

레거시 SCEP 인증서 등록 구성

레거시 SCEP 등록을 위한 VPN 클라이언트 프로파일 구성

프로시저

단계 1 VPN 프로파일 편집기를 열고 탐색 창에서 **Certificate Enrollment(**인증서 등록**)** 를 선택합니다.

단계 2 **Certificate Enrollment(**인증서 등록**)**를 선택합니다.

단계 3 클라이언트가 인증서를 검색하도록 지시하려면 **Automatic SCEP Host(**자동 **SCEP** 호스트**)** 를 지정하십시오.

SCEP 인증서 검색을 위해 구성된 연결 프로파일(터널 그룹)의 FQDN 또는 IP 주소 및 별칭을 입력합니다. 예를 들어 **asa.cisco.com**이 ASA의 호스트 이름이며 **scep_eng**가 연결 프로파일의 별칭인 경우, **asa.cisco.com/scep-eng**를 입력합니다.

사용자가 연결을 시작할 경우 선택하거나 지정한 주소는 레거시 SCEP 등록이 성공하도록 정확하게 이 값과 일치해야 합니다. 예를 들어 이 필드가 FQDN으로 설정되어 있지만 사용자가 IP 주소를 지정한 경우 SCEP 등록에 실패합니다.

단계 **4** 인증 기관 특성을 구성하십시오.

참고 CA 서버 관리자는 CA URL 및 지문을 제공할 수 있습니다. 발급한 인증서의 "fingerprint(지문)" 또는 "thumbprint(지문)" 특성 필드가 아니라 서버에서 직접 thumbprint(지문)를 검색합니다.

a) SCEP CA 서버를 식별하려면 CA URL을 지정하십시오. FQDN 또는 IP 주소를 입력합니다. 예: **http://ca01.cisco.com/certsrv/mscep/mscep.dll**.
b) 사용자 이름과 일회용 비밀번호를 묻는 프롬프트를 사용자에게 표시하려면 **Prompt For Challenge PW(**시도용 비밀번호 프롬프트**)** 를 선택합니다(선택 사항).
c) CA 인증서용 thumbprint(지문)를 입력합니다(선택 사항). SHA1 또는 MD5 해시를 사용하십시오. 예: `8475B661202E3414D4BB223A464E6AAB8CA123AB`.

단계 **5** 등록 인증서에서 어떤 **Certificate Contents(**인증서 콘텐츠**)** 를 요청할지 구성하십시오. 인증서 필드의 정의에 대해서는 AnyConnect 프로파일 편집기, 인증서 등록을 참조하십시오.

참고 %machineid%를 사용하는 경우, 클라이언트에 HostScan/Posture를 로드합니다.

단계 **6** 사용자가 수동으로 인증 인증서 프로비저닝 또는 갱신을 요청하도록 허용하려면 **Display Get Certificate Button(**인증서 가져오기 표시 버튼**)**을 선택합니다(선택 사항). 이 버튼은 인증서 인증이 실패할 경우 사용자에게 표시됩니다.

단계 **7** 서버 목록에서 특정 호스트에 대해 SCEP를 활성화합니다(선택 사항). 이렇게 하면 위에서 설명한 Certificate Enrollment(인증서 등록) 창에서 SCEP 설정을 재정의합니다.

a) 탐색 창에서 **Server List(**서버 목록**)** 를 선택합니다.
b) 서버 목록 항목을**Add(**추가**)** 하거나 **Edit(**편집**)** 합니다.
c) 5단계와 6단계에 설명된 대로 자동 SCEP 호스트 및 인증 기관 특성을 지정합니다.

레거시 SCEP 등록을 지원하기 위한 ASA 구성

ASA의 레거시 SCEP의 경우 인증서 등록을 위해 연결 프로파일 및 그룹 정책을 생성하고 인증서 권한 부여 VPN 연결을 위해 두 번째 연결 프로파일 및 그룹 정책을 생성해야 합니다.

프로시저

단계 **1** 등록을 위해 그룹 정책을 생성합니다(예: cert_enroll_group). 다음 필드를 설정하십시오.

Advanced(고급) > AnyConnect Client(AnyConnect 클라이언트) 창에서 다운로드할 클라이언트 프로파일에 대해 **Inherit(**상속**)**를 선택 취소하고 레거시 SCEP에 대해 구성된 클라이언트 프로파일을 지정합니다. 예를 들어, ac_vpn_legacy_scep 클라이언트 프로파일을 지정합니다.

단계 **2** 권한 부여를 위해 두 번째 그룹 정책을 생성합니다(예: cert_auth_group).

단계 **3** 등록을 위해 연결 프로파일을 생성합니다(예: cert_enroll_tunnel). 다음 필드를 설정하십시오.

- Basic(기본) 창에서 인증 방법을 AAA로 설정합니다.
- Basic(기본) 창에서 기본 그룹 정책을 cert_enroll_group으로 설정합니다.
- Advanced(고급) > GroupAlias/Group URL(그룹 별칭/그룹 URL)에서 이 연결 프로파일에 대한 등록 그룹(cert_enroll_group)을 포함하는 그룹 URL을 생성합니다.
- ASA에서 연결 프로파일을 활성화하지 마십시오. 사용자가 그룹에 액세스할 수 있도록 그룹을 사용자에게 노출시킬 필요는 없습니다.

단계 **4** 권한 부여를 위해 연결 프로파일을 생성합니다(예: cert_auth_tunnel). 다음 필드를 설정하십시오.

- Basic(기본) 창에서 인증 방법을 인증서로 설정합니다.
- Basic(기본) 창에서 기본 그룹 정책을 cert_auth_group으로 설정합니다.
- ASA에서 이 연결 프로파일을 활성화하지 마십시오. 사용자가 그룹에 액세스할 수 있도록 그룹을 사용자에게 노출시킬 필요는 없습니다.

단계 **5** 각 그룹 정책의 General(일반) 창에서 **Connection Profile (Tunnel Group) Lock(**연결 프로파일**(**터널 그룹**)** 잠금**)** 을 해당하는 SCEP 연결 프로파일에 설정하여 트래픽을 SCEP 구성 연결 프로파일로 제한합니다(선택 사항).

SCEP에 대한 Windows 2008 서버 인증 기관 설정

인증 기관 소프트웨어가 Windows 2008 서버에서 실행 중인 경우, AnyConnect를 통해 SCEP를 지원하는 서버에 대한 다음 구성 중 하나를 변경해야 할 수 있습니다.

인증 기관에서 SCEP 비밀번호 비활성화

다음 단계에서는 SCEP 시도용 비밀번호를 비활성화하는 방법에 대해 설명하며 비활성화되면 클라이언트는 SCEP 등록 전에 OOB(Out of Band) 비밀번호를 제공할 필요가 없습니다.

프로시저

단계 **1** 인증 기관 서버에서 레지스트리 편집기를 시작합니다. 레지스트리 편집기는 **Start(**시작**)** > **Run(**실행**)**을 선택하고 **regedit**를 입력한 다음 **OK(**확인**)**를 클릭하여 시작할 수 있습니다.

단계 **2** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP\EnforcePassword로 이동합니다.

EnforcePassword 키가 존재하지 않으면 새로운 키로 생성합니다.

단계 3 EnforcePassword를 편집하여 '0'으로 설정합니다. 이 키가 존재하지 않으면 REG-DWORD로 생성합니다.

단계 4 regedit를 종료하고 인증 기관 서버를 재부팅합니다.

인증 기관에서 SCEP 템플릿 설정

다음 단계에서는 인증서 템플릿을 생성하고 기본 SCEP 템플릿으로 지정하는 방법을 설명합니다.

프로시저

단계 1 서버 관리자를 실행하십시오. Start(시작) > Admin Tools(관리 툴) > Server Manager(서버 관리자)를 선택하면 이 작업을 수행할 수 있습니다.

단계 2 Roles(역할) > Certificate Services(인증서 서비스) 또는 AD Certificate Services(AD 인증서 서비스)를 확장하십시오.

단계 3 CA Name(CA 이름) > Certificate Templates(인증서 템플릿)로 이동하십시오.

단계 4 **Certificate Templates(**인증서 템플릿**) > Manage(**관리**)**를 마우스 오른쪽 버튼으로 클릭하십시오.

단계 5 Cert Templates Console(인증서 템플릿 콘솔)에서 User template(사용자 템플릿)을 마우스 오른쪽 버튼으로 클릭하고 **Duplicate(**복제**)**를 선택하십시오.

단계 6 새 템플릿을 위한 **Windows Server 2008** 버전 을 선택하고 **OK(**확인**)**를 클릭하십시오.

단계 7 템플릿 디스플레이 이름을 NDES-IPSec-SSL과 같이 설명이 포함된 이름으로 변경하십시오.

단계 8 사이트의 유효성 기간을 조정하십시오. 대부분 사이트에서는 인증서 만료를 방지하기 위해 3년 이상을 선택합니다.

단계 9 Cryptography(암호화) 탭에서 구축를 위한 키의 최소 크기를 설정하십시오.

단계 10 Subject Name(제목 이름) 탭에서 **Supply in Request(**요청 시 공급**)**를 선택하십시오.

단계 11 Extensions(확장) 탭에서 애플리케이션 정책에 최소한 다음이 포함되도록 설정하십시오.

- 클라이언트 인증
- IP 보안 엔드 시스템
- IP 보안 IKE 중개
- IP 보안 터널 종료
- IP 보안 사용자

이 값은 SSL 또는 IPsec에 유효합니다.

단계 12 새 템플릿을 저장하려면 **Apply(**적용**)**를 클릭한 다음 **OK(**확인**)** 를 클릭하십시오.

단계 13 Server manager(서버 관리자) > Certificate Services(인증서 서비스) - CA Name(CA 이름)에서 Certificate Templates(인증서 템플릿)를 마우스 오른쪽 버튼으로 클릭하십시오. New(새로 만들기) > Certificate Template to Issue(발급할 인증서 템플릿)를 선택하고 생성한 새 템플릿(이 예에서는 NDES-IPSec-SSL)을 선택한 다음 **OK(**확인**)**를 클릭하십시오.

단계 **14** 레지스트리를 편집하십시오. Start(시작) > Run(실행), regedit를 선택하고 **OK(**확인**)**를 클릭하여 이 작업을 수행합니다.

단계 **15** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP로 이동하십시오.

단계 **16** 다음 3가지 키의 값을 **NDES-IPSec-SSL**로 설정하십시오.

- EncryptionTemplate
- GeneralPurposeTemplate
- SignatureTemplate

단계 **17** **Save(**저장**)**를 클릭하고 인증 기관 서버를 재부팅하십시오.

인증서 만료 알림 구성

AnyConnect에서 인증 인증서가 만료될 예정임을 사용자에게 경고하도록 구성합니다. **Certificate Expiration Threshold(**인증서 만료 임계값**)** 설정은 AnyConnect에서 인증서가 만료될 예정임을 사용자에게 경고하는 인증서 만료 날짜 이전 일수를 지정합니다. AnyConnect는 인증서가 실제로 만료되거나 새 인증서를 획득할 때까지 연결할 때마다 사용자에게 경고합니다.

참고 인증서 만료 임계값 기능은 RADIUS에서는 사용할 수 없습니다.

프로시저

단계 **1** VPN 프로파일 편집기를 열고 탐색 창에서 **Certificate Enrollment(**인증서 등록**)** 를 선택합니다.

단계 **2** **Certificate Enrollment(**인증서 등록**)**를 선택합니다.

단계 **3** **Certificate Expiration Threshold(**인증서 만료 임계값**)**를 지정합니다.

이 값은 인증서 만료 날짜 이전 일수이며 AnyConnect는 인증서가 만료될 예정임을 사용자에게 경고합니다.

기본값은 0(표시된 경고 없음)입니다. 범위는 0일에서 180일까지입니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

인증서 선택 영역 구성

다음 단계는 클라이언트 시스템에서 인증서를 검색 및 선택하는 방법을 구성하는 AnyConnect 프로파일에서의 모든 위치에 대한 설명입니다. 모든 단계가 필수사항은 아니며 사용자가 기준을 지정하지 않은 경우, AnyConnect는 기본 키 일치를 사용합니다.

AnyConnect는 Windows에 있는 브라우저 인증서 저장소를 읽습니다. Linux의 경우 PEM(프라이버시 향상 메일) 형식의 파일 저장소를 생성해야 합니다. macOS의 경우 PEM(프라이버시 향상 메일) 형식 파일 저장소나 키 체인을 사용할 수 있습니다.

프로시저

단계 **1** Windows 및 macOS:사용할 인증서 저장소 구성, 161 페이지

VPN 클라이언트 프로파일의 AnyConnect에서 어떤 인증서 저장소가 사용되는지 지정합니다.

단계 **2** Windows만 해당: 인증 인증서를 선택하도록 Windows 사용자에게 프롬프트 표시, 164 페이지

유효한 인증서 목록을 사용자에게 제공하여 사용자가 세션을 인증하기 위해 인증서를 선택할 수 있도록 AnyConnect를 구성합니다.

단계 **3** macOS 및 Linux 환경: macOS 및 Linux용 PEM 인증서 저장소 생성, 164 페이지

단계 **4** macOS 및 Linux 환경: VPN 로컬 정책 프로파일에서 제외할 인증서 저장소를 선택합니다.

단계 **5** 인증서 일치 구성, 165 페이지

저장소에서 인증서를 검색할 경우 AnyConnect에서 일치를 시도할 키를 구성합니다. 키 및 확장 키를 지정하고 사용자 정의 확장 키를 추가할 수 있습니다. 또한 일치하도록 AnyConnect에 대한 고유 이름에 있는 연산자 값에 패턴을 지정할 수 있습니다.

사용할 인증서 저장소 구성

Windows 및 macOS의 경우에는 VPN 클라이언트 프로파일에서 사용할 수 있도록 AnyConnect용으로 별도의 인증서 저장소가 제공됩니다. 인증서 인증 조합을 하나 또는 여러 개 추가할 수 있으며, 여러 인증서 인증 선택 항목 중 특정 VPN 연결에 적합한 선택 항목을 클라이언트에 지시하도록 보안 게이트웨이를 구성할 수 있습니다. 예를 들어 로컬 정책 파일에서 ExcludeMacNativeCertStore를 *true*로 설정하여 AnyConnect가 사용자 및 시스템 파일 인증서 저장소와 같은 파일 인증서 저장소만 사용하도록 강제 지정하는 동시에 프로파일 기반 인증서 저장소를 Login(로그인)으로 설정하여 AnyConnect가 사용자 파일 저장소 외에 로그인 및 동적 스마트 카드 키 체인과 같은 인증서 저장소만 사용하도록 강제 지정하는 경우, 이 두 가지 필터링이 결합되어 AnyConnect가 사용자 파일 인증서 저장소만 사용하도록 하는 엄격한 정책이 적용됩니다.

컴퓨터에서 관리자 권한이 있는 사용자는 두 가지 인증서 저장소 모두에 액세스할 수 있습니다. 관리자 권한이 없는 사용자는 사용자 인증서 저장소에만 액세스할 수 있습니다. 일반적으로 Windows 사용자는 관리자 권한이 없습니다. 사용자에게 관리자 권한이 없는 경우에도 **Certificate Store Override(**인증서 저장소 재정의**)** 를 선택하면 AnyConnect에서 머신 저장소에 액세스할 수 있습니다.

참고 머신 저장소에 대한 액세스 제어는 Windows 버전 및 보안 설정에 따라 다를 수 있습니다. 이러한 이유로 인해 사용자에게 관리자 권한이 있지만 머신 저장소에서 인증서를 사용하지 못할 수 있습니다. 이 경우 **Certificate Store Override(**인증서 저장소 재정의**)** 를 선택하면 머신 저장소에 액세스할 수 있습니다.

다음 표에서는 AnyConnect가 **Certificate Store(**인증서 저장소**)**에서 검색되는 내용에 기반하여 클라이언트에서 인증서를 검색하는 방법 및 **Certificate Store Override(**인증서 저장소 재정의**)**가 선택되는지 여부에 대해 설명합니다.

인증서 저장소 설정	인증서 저장소 재정의 설정	**AnyConnect** 검색 전략
모두(Windows의 경우)	삭제됨	AnyConnect는 모든 인증서 저장소를 검색합니다. 사용자에게 관리자 권한이 없는 경우 AnyConnect에서 머신 저장소에 액세스할 수 없습니다. 이 설정이 기본값입니다. 이 설정은 대부분의 경우 적합합니다. 특정한 이유 또는 시나리오 요건에 변경 요청이 없는 한 이 설정을 변경하지 마십시오.
모두(Windows의 경우)	선택됨	AnyConnect는 모든 인증서 저장소를 검색합니다. 사용자에게 관리자 권한이 없는 경우 AnyConnect에서 머신 저장소에 액세스할 수 있습니다.
모두(macOS의 경우)	선택됨	AnyConnect가 사용 가능한 모든 macOS 키 체인과 파일 저장소의 인증서를 사용합니다.
사용자(Windows의 경우)	해당 사항 없음	AnyConnect는 사용자 인증서 저장소에서만 검색합니다. 관리자 권한이 없는 사용자가 이 인증서 저장소에 액세스할 수 있기 때문에 인증서 저장소 재정의가 적용되지 않습니다.
시스템(macOS의 경우)	선택됨	AnyConnect가 macOS 시스템 키 체인 및 시스템 파일/PEM 저장소의 인증서만 사용합니다.
로그인(macOS의 경우)	선택됨	AnyConnect가 macOS 로그인 및 동적 스마트 카드 키 체인과 사용자 파일/PEM 저장소의 인증서만 사용합니다.

다중 인증서 인증 사용

시작하기 전에

- 데스크톱 플랫폼(Windows, OS X, Linux)에서만 지원됩니다.
- VPN 프로파일에 *AutomaticCertSelection*이 활성화되어 있어야 합니다.
- VPN 프로파일에서 설정하는 인증서 일치 컨피그레이션에 따라 다중 인증서 인증에 사용 가능한 인증서 수가 제한됩니다.

참고 SCEP는 지원되지 않습니다.

프로시저

단계 **1** **Certificate Store(**인증서 저장소**)**를 설정합니다.

- 머신과 사용자 인증서가 하나씩인 경우 VPN 프로파일에서 CertificateStore를 **All(**모두**)**로 설정하고 2단계에 설명된 대로 *CertficateStoreOverride*를 활성화합니다.
- 사용자 인증서가 두 개인 경우 VPN 프로파일에서 CertificateStore를 **All(**모두**)** 또는 **User(**사용자**)**로 설정하되 2단계에 설명된 대로 *CertificateStoreOverride*는 그대로 유지합니다.

단계 **2** 사용자에게 관리자 권한이 없는 경우 AnyConnect가 머신 인증서 저장소를 검색하도록 허용하려면 **Certificate Store Override(**인증서 저장소 재정의**)**를 선택합니다.

기본 인증서 인증 사용

프로시저

단계 **1** **Certificate Store(**인증서 저장소**)**를 설정합니다.

- 모두 — (기본값) AnyConnect 클라이언트에서 인증서 위치를 찾기 위해 모든 인증서 저장소를 사용하도록 지시합니다.
- 머신 — AnyConnect 클라이언트가 인증서 조회를 Windows 로컬 머신 인증서 저장소로 제한하도록 지시합니다.
- 사용자 — AnyConnect 클라이언트가 인증서 조회를 로컬 사용자 인증서 저장소로 제한하도록 지시합니다.

단계 **2** 사용자에게 관리자 권한이 없는 경우 AnyConnect가 머신 인증서 저장소를 검색하도록 허용하려면 **Certificate Store Override(**인증서 저장소 재정의**)**를 선택합니다.

인증 인증서를 선택하도록 Windows 사용자에게 프롬프트 표시

사용자에게 유효한 인증서 목록을 표시하고 사용자가 세션을 인증할 인증서를 선택하도록 AnyConnect를 구성할 수 있습니다. 만료된 인증서가 유효하지 않은 것으로 간주되는 것은 아닙니다. 예를 들어 SCEP를 사용하는 경우 서버가 클라이언트에 새 인증서를 발급할 수 있습니다. 이 경우 만료된 인증서를 지우면 클라이언트가 서버에 전혀 연결하지 못하게 될 수 있으므로 수동 개입 및 OOB(Out of Band) 배포가 필요합니다. AnyConnect는 구성된 인증서 일치 규칙을 기준으로 하여 키 사용, 키 유형/길이 등의 보안 관련 속성에 따라서만 클라이언트 인증서를 제한합니다. 이 구성은 Windows에서만 사용할 수 있습니다. 기본적으로 사용자 인증서 선택은 비활성화되어 있습니다.

프로시저

단계 **1** VPN 프로파일 편집기를 열고 탐색 창에서 **Preferences(Part 2)(**환경 설정**(2**부**))** 를 선택합니다.

단계 **2** 인증서 선택을 활성화하려면 **Disable Certificate Selection(**인증서 선택 비활성화**)**선택을 해제하십시오.

단계 **3** **User Controllable(**사용자 제어 가능**)**은 **Advanced(**고급**)** > **VPN** > **Preferences(**환경 설정**)** 창에서 사용자가 자동 인증서 선택을 켜고 끄는 것을 원하지 않는 경우에 선택을 해제하십시오.

macOS 및 Linux용 PEM 인증서 저장소 생성

AnyConnect는 PEM(Privacy Enhanced Mail, 개인정보 향상 메일) 형식의 파일 저장소에서 인증서 검색을 지원합니다. AnyConnect는 원격 컴퓨터에 있는 파일 시스템에서 PEM 형식의 인증서 파일을 읽고 확인하며 서명합니다.

시작하기 전에

모든 상황에서 클라이언트가 적절한 인증서를 획득할 수 있으려면 파일이 다음 요건을 충족해야 합니다.

- 모든 인증서 파일이 확장명 .pem으로 끝나야 합니다.
- 모든 개인 키 파일이 확장명 .key로 끝나야 합니다.
- 클라이언트 인증서 및 해당 개인 키는 파일 이름이 동일해야 합니다. 예를 들어 client.pem 및 client.key입니다.

팁 PEM 파일의 복사본을 보관하는 대신 PEM 파일에 대한 소프트 링크를 사용할 수 있습니다.

PEM 파일 인증서 저장소를 생성하려면 아래에 나열된 경로 및 폴더를 생성하십시오. 이 폴더에서 적절한 인증서를 배치하십시오.

PEM 파일 인증서 저장소 폴더	저장된 인증서 유형
~/.cisco/certificates/ca(1) ~ 참고 홈 디렉토리입니다.	신뢰할 수 있는 CA 및 루트 인증서
~/.cisco/certificates/client	클라이언트 인증서
~/.cisco/certificates/client/private	개인 키

머신 인증서는 루트 디렉토리를 제외하고 PEM 파일 인증서와 동일합니다. 머신 인증서의 경우 /opt/.cisco가 ~/.cisco를 대체합니다. 기타 경우 나열된 인증서의 경로, 폴더 및 유형이 적용됩니다.

인증서 일치 구성

AnyConnect는 특정 키 집합과 일치하는 인증서로 인증서 검색을 제한할 수 있습니다. 인증서 일치는 **Certificate Matching(**인증서 일치**)** 창에서 AnyConnect VPN 클라이언트 프로파일에 설정된 전역 기준입니다. 기준은 다음과 같습니다.

- 키 사용
- 확장 키 사용
- 고유 이름

관련 항목

AnyConnect 프로파일 편집기, 인증서 일치, 98 페이지

키 사용 구성

Key Usage(키 사용**)** 를 선택하면 키는 AnyConnect가 사용할 수 있는 인증서를 선택된 키 중 최소한 하나를 보유한 인증서로 제한합니다. 지원되는 집합이 VPN 클라이언트 프로파일의 **Key Usage(**키 사용**)** 목록에 나열되어 있으며 다음을 포함합니다.

- DECIPHER_ONLY
- ENCIPHER_ONLY
- CRL_SIGN
- KEY_CERT_SIGN
- KEY_AGREEMENT
- DATA_ENCIPHERMENT
- KEY_ENCIPHERMENT
- NON_REPUDIATION
- DIGITAL_SIGNATURE

하나 이상의 기준을 지정한 경우 인증서가 일치 인증서로 간주되려면 최소한 하나 이상의 기준과 일치해야 합니다.

확장 키 사용 구성

Extended Key Usage(확장 키 사용**)** 를 선택하면 키는 AnyConnect가 사용할 수 있는 인증서를 해당 키가 있는 인증서로 제한합니다. 다음 표에는 해당 OID(object identifiers, 개체 식별자)와 함께 잘 알려진 제한이 나열되어 있습니다.

제한	**OID**
ServerAuth	1.3.6.1.5.5.7.3.1
ClientAuth	1.3.6.1.5.5.7.3.2
CodeSign	1.3.6.1.5.5.7.3.3
EmailProtect	1.3.6.1.5.5.7.3.4
IPSecEndSystem	1.3.6.1.5.5.7.3.5
IPSecTunnel	1.3.6.1.5.5.7.3.6
IPSecUser	1.3.6.1.5.5.7.3.7
TimeStamp	1.3.6.1.5.5.7.3.8
OCSPSign	1.3.6.1.5.5.7.3.9
DVCS	1.3.6.1.5.5.7.3.10
IKE 중개	1.3.6.1.5.5.8.2.2

사용자 정의 확장 일치 키 구성

이 문서의 일부 예제에서 사용되는 1.3.6.1.5.5.7.3.11 등의 기타 모든 OID는 "사용자 정의" OID로 간주됩니다. 관리자는 알려진 집합에 원하는 OID가 없으면 고유한 OID를 추가할 수 있습니다.

인증서 고유 이름 구성

Distinguished Name(고유 이름**)** 표에는 클라이언트가 사용할 수 있는 인증서를 특정한 기준 및 기준 일치 조건과 일치하는 인증서로 제한하는 인증서 식별자가 포함되어 있습니다. **Add(**추가**)** 버튼을 클릭하여 기준을 목록에 추가하고 추가된 기준의 내용과 일치하도록 값 또는 와일드카드를 설정합니다.

식별자	설명
CN	SubjectCommonName
SN	SubjectSurName
GN	SubjectGivenName
N	SubjectUnstructName

식별자	설명
I	SubjectInitials
GENQ	SubjectGenQualifier
DNQ	SubjectDnQualifier
C	SubjectCountry
L	SubjectCity
SP	SubjectState
ST	SubjectState
O	SubjectCompany
OU	SubjectDept
T	SubjectTitle
EA	SubjectEmailAddr
DC	DomainComponent
ISSUER-CN	IssuerCommonName
ISSUER-SN	IssuerSurName
ISSUER-GN	IssuerGivenName
ISSUER-N	IssuerUnstructName
ISSUER-I	IssuerInitials
ISSUER-GENQ	IssuerGenQualifier
ISSUER-DNQ	IssuerDnQualifier
ISSUER-C	IssuerCountry
ISSUER-L	IssuerCity
ISSUER-SP	IssuerState
ISSUER-ST	IssuerState
ISSUER-O	IssuerCompany
ISSUER-OU	IssuerDept
ISSUER-T	IssuerTitle
ISSUER-EA	IssuerEmailAddr
ISSUER-DC	IssuerDomainComponent

Distinguished Name(고유 이름**)** 에는 0개 또는 한 개 이상의 일치 기준이 포함됩니다. 인증서가 일치 인증서로 간주되려면 지정된 모든 기준과 일치해야 합니다. **Distinguished Name(**고유 이름**)** 일치는 인증서가 지정된 문자열을 포함해야 하는지 지정하며 이 문자열의 와일드카드 사용 여부도 지정합니다.

SAML을 사용하는 VPN 인증

ASA 릴리스 9.7.1과 통합된 SAML 2.0을 사용하여 초기 세션 인증을 수행할 수 있습니다. AnyConnect 4.6에는 이전 릴리스에 통합되어 있던 기본(외부) 브라우저 대신 제공되는 임베디드 브라우저를 포함하는 개선된 버전의 SAML 통합이 도입되었습니다. SAML 인증용으로 구성된 터널 그룹에 연결할 때 AnyConnect는 임베디드 브라우저 창을 열어 인증 프로세스를 완료합니다. 모든 SAML 시도에서는 새 브라우저 세션을 사용하며, 브라우저 세션은 AnyConnect에만 사용됩니다(다른 브라우저와는 세션 상태가 공유되지 않음). 각 SAML 인증 시도가 시작될 때는 세션 상태가 없지만 각 인증 시도 간에는 영구 쿠키가 보존됩니다.

SAML을 사용할 때는 다음 지침을 따르십시오.

- SAML 기능을 사용하려면 ASA의 NTP(Network Time Protocol) 서버와 IdP NTP 서버를 동기화해야 합니다.
- ASDM의 VPN 마법사는 현재 SAML 컨피그레이션을 지원하지 않습니다.
- SAML IdP *NameID* 속성은 사용자의 사용자 이름을 확인하며 권한 부여, 계정 관리 및 VPN 세션 데이터베이스에 사용됩니다.
- 사용자가 SAML을 통해 VPN 세션을 설정할 때마다 IdP(Identity Provider)에 재인증하도록 하려는 경우에는 AnyConnect 프로파일 편집기, 환경 설정(1부), 89 페이지에서 Auto Reconnect(자동 재연결)를 *ReconnectAfterResume*으로 설정해야 합니다.

SAML이 정상적으로 작동하도록 하려면 최신 WebDeploy 버전 이상으로 업그레이드해야 합니다.

- anyconnect-macos-4.4.01054-webdeploy-k9.pkg
- anyconnect-win-4.4.01054-webdeploy-k9.pkg
- anyconnect-linux64-4.4.01054-webdeploy-k9.pkg

추가 컨피그레이션 세부사항은 Cisco ASA Series VPN 환경 설정 가이드의 해당 릴리스(9.7 이상)에서 *SAML 2.0*을 사용하는 *SSO* 섹션을 참조하십시오.

SDI 토큰(SoftID) 통합을 사용하는 VPN 인증

Windows 7 x86(32비트) 및 x64(64비트)에서 실행 중인 RSA SecurID 클라이언트 소프트웨어 버전 1.1과 이후 버전에 대한 지원을 AnyConnect에 통합합니다.

RSA SecurID 소프트웨어 인증자는 사용자가 회사 자산에 대한 안전한 보안 액세스를 위해 관리해야 할 항목 수를 줄여줍니다. 원격 디바이스에 있는 RSA SecurID 소프트웨어 토큰은 60초마다 변경되는 임의의 일회용 암호를 생성합니다. SDI는 하드웨어 및 소프트웨어 토큰을 사용하는 일회용 비밀번호 생성 기술을 나타내는 Security Dynamics, Inc. 기술을 의미합니다.

일반적으로 사용자는 툴 트레이에서 AnyConnect 아이콘을 클릭하고 연결 프로파일을 선택한 다음 인증 대화 상자에서 적절한 자격 증명을 입력하여 AnyConnect에 연결합니다. 로그인(시도) 대화 상자는 사용자가 속해 있는 터널 그룹에 대해 구성된 인증 유형과 일치합니다. 로그인 대화 상자의 입력 필드는 어떠한 입력이 인증에 필요한지 명확하게 표시합니다.

SDI 인증을 위해 원격 사용자는 AnyConnect 소프트웨어 인터페이스에 PIN(Personal Identification Number, 개인 식별 번호)을 입력하고 RSA SecurID 암호를 받습니다. 사용자가 보안 애플리케이션에 암호를 입력한 후 RSA 인증 관리자는 이 암호를 확인하고 사용자에게 액세스 권한을 허용합니다.

RSA SecurID 하드웨어나 소프트웨어 토큰을 사용하는 사용자는 암호 또는 PIN 입력 여부를 나타내는 입력 필드뿐만 아니라 요건에 대한 추가 정보를 제공하는 대화 상자 하단의 상태 표시줄을 확인합니다. 사용자는 AnyConnect 사용자 인터페이스에 소프트웨어 토큰 PIN 또는 암호를 직접 입력합니다.

초기 로그인 대화 상자는 설정에 따라 다릅니다. 사용자는 기본 로그인 페이지, 주요 인덱스 URL, 터널 그룹 로그인 페이지 또는 터널 그룹 URL(URL 또는 터널 그룹)을 통해 보안 게이트웨이에 액세스할 수 있습니다. 기본 로그인 페이지를 통해 보안 게이트웨이에 액세스하려면 네트워크(클라이언트) 액세스 AnyConnect 연결 프로파일 페이지에서 "Allow user to select connection(사용자가 연결을 선택하도록 허용)" 확인란을 설정해야 합니다. 두 경우 모두 보안 게이트웨이에서 클라이언트 로그인 페이지를 전송합니다. 기본 로그인 페이지는 사용자가 선택한 터널 그룹 드롭다운 목록을 포함하지만 터널 그룹 로그인 페이지는 터널 그룹이 URL에 지정되어 있기 때문에 이 목록을 포함하지 않습니다.

기본 로그인 페이지의 경우(연결 프로파일 또는 터널 그룹의 드롭다운 목록 포함) 기본 터널 그룹의 인증 유형이 비밀번호 입력 필드 레이블에 대한 초기 설정을 결정합니다. 예를 들어 기본 터널 그룹이 SDI 인증을 사용하는 경우 필드 레이블은 “Passcode(암호)”이지만 기본 터널 그룹이 NTLM 인증을 사용하는 경우 필드 레이블은 "Password(비밀번호)"입니다. 릴리스 2.1 이상 버전에서 필드 레이블은 다른 터널 그룹의 사용자 선택에 따라 동적으로 업데이트되지 않습니다. 터널 그룹 로그인 페이지의 경우 필드 레이블이 터널 그룹 요건과 일치해야 합니다.

클라이언트는 비밀번호 입력 필드에 RSA SecurID 소프트웨어 토큰 PIN 입력을 지원합니다. RSA SecurID 토큰 소프트웨어가 설치되어 있으며 터널 그룹 인증 유형이 SDI인 경우 필드 레이블은 "Passcode(암호)"이며 상태 표시줄에는 "사용자 이름 및 암호 또는 소프트웨어 토큰 PIN을 입력하십시오."라고 표시됩니다. PIN을 사용하는 경우 동일한 터널 그룹 및 사용자 이름에 대한 다음 연속 로그인의 필드 레이블은 "PIN"입니다. 클라이언트는 입력된 PIN을 사용하여 RSA SecurID 소프트웨어 토큰 DLL에서 암호를 검색합니다. 성공적인 인증을 통해 클라이언트는 터널 그룹, 사용자 이름 및 인증 유형을 저장하고 저장된 터널 그룹은 새 기본 터널 그룹이 됩니다.

AnyConnect는 모든 SDI 인증에 대한 암호를 채택합니다. 비밀번호 입력 레이블이 "PIN"인 경우에도 사용자는 상태 표시줄의 지시에 따라 암호를 계속 입력할 수 있습니다. 클라이언트는 암호를 그대로 보안 게이트웨이에 전송합니다. 암호가 사용되는 경우, 동일한 터널 그룹 및 사용자 이름에 대한 다음 연속 로그인에 필드 레이블 "Passcode(암호)"가 있습니다.

RSASecureIDIntegration 프로파일 설정에는 다음과 같이 3개의 가능한 값이 있습니다.

- 자동 — 클라이언트는 먼저 한 가지 방법을 시도하고 이 방법이 실패할 경우 다른 방법을 시도합니다. 기본값은 사용자 입력을 토큰 암호(HardwareToken)로 처리하는 것이며 이 방법이 실패하면 사용자 입력을 소프트웨어 토큰 PIN(SoftwareToken)으로 처리합니다. 인증이 성공하면 성공한 방법이 새로운 SDI 토큰 유형으로 설정되며 사용자 환경 설정 파일에서 캐시됩니다. 다음 인증 시도 시 SDI 토큰 유형은 어떤 방법을 먼저 시도할지를 정의합니다. 일반적으로 현재 인증 시도에 사용되는 토큰은 마지막으로 성공한 인증 시도에서 사용된 토큰과 같습니다. 단 사용자 이

름 또는 그룹 선택사항을 변경하는 경우, 입력 필드 레이블에 표시된 것과 같이 기본 방법을 먼저 시도하기 위해 되돌아갑니다.

참고 SDI 토큰 유형에는 자동 설정을 위한 의미만 포함되어 있습니다. 인증 모드가 자동이 아닌 경우, SKI 토큰 유형의 로그를 무시할 수 있습니다. HardwareToken은 기본값으로, 다음 번 토큰 모드 시작을 방지합니다.

- SoftwareToken — 클라이언트가 사용자 입력을 항상 소프트웨어 토큰 PIN으로 해석하며 입력 필드 레이블이 "PIN:"입니다.
- HardwareToken — 클라이언트가 사용자 입력을 항상 소프트웨어 토큰 암호로 해석하며 입력 필드 레이블이 "Passcode:(암호:)"입니다.

참고 AnyConnect는 여러 토큰에서 RSA 소프트웨어 토큰 클라이언트 소프트웨어로 가져온 토큰 선택사항을 지원하지 않습니다. 대신 클라이언트는 RSA SecurID 소프트웨어 토큰 GUI를 통해 선택한 기본값을 사용합니다.

SDI 인증 교환 범주

모든 SDI 인증 교환은 다음 범주 중 하나에 속합니다.

- 일반적인 SDI 인증 로그인
- 새 사용자 모드
- 새 PIN 모드
- PIN 지우기 모드
- 다음 토큰 코드 모드

일반적인 SDI 인증 로그인

일반적인 로그인 시도는 항상 첫 번째 시도입니다. SDI 인증 사용자는 사용자 이름 및 암호 또는 PIN 필드에 각각 사용자 이름 및 토큰 암호 또는 소프트웨어 토큰의 경우 PIN을 제공해야 합니다. 클라이언트는 보안 게이트웨이(중앙 사이트 디바이스)에 정보를 반환하고 보안 게이트웨이는 인증 서버(SDI 또는 RADIUS 프록시를 통한 SDI)를 통해 인증을 확인합니다.

인증 서버에서 인증 요청을 허용하는 경우, 보안 게이트웨이는 클라이언트에 성공 페이지를 다시 전송하며 인증 교환이 완료됩니다.

암호가 허용되지 않는 경우, 인증에 실패하며 보안 게이트웨이가 오류 메시지와 함께 새 로그인 시도 페이지를 전송합니다. SDI 서버에서 암호 실패 임계값에 도달한 경우, SDI 서버는 다음 토큰 코드 모드로 토큰을 전환합니다.

새 사용자 모드, **PIN** 지우기 모드 및 새 **PIN** 모드

PIN은 SDI 서버에서만 지울 수 있으며 네트워크 관리자만 이 작업을 수행할 수 있습니다.

새 사용자 모드, PIN 지우기 모드 및 새 PIN 모드에서 AnyConnect는 "다음 암호" 로그인 시도 시 사용하기 위해 사용자가 생성한 PIN 또는 시스템 할당 PIN을 캐시합니다.

PIN 지우기 모드 및 새 사용자 모드는 원격 사용자의 관점에서 볼 때 동일하며 보안 게이트웨이에서 둘 다 동일하게 처리됩니다. 두 경우 모두 원격 사용자는 새 PIN을 입력하거나 SDI 서버에서 새 PIN을 할당받아야 합니다. 유일한 차이점은 초기 시도에 대한 사용자 응답입니다.

새 PIN 모드의 경우 일반 시도에서와 같이 기존 PIN을 사용하여 암호를 생성합니다. PIN 지우기 모드의 경우, 하드웨어 토큰용으로 PIN을 사용하지 않으며 사용자는 토큰 코드만 입력합니다. 8개의 연속적인 0(00000000)으로 구성된 PIN을 사용하여 RSA 소프트웨어 토큰용 암호가 생성됩니다. 두 경우 모두 PIN 값이 있으면 SDI 서버 관리자는 사용자에게 사용할 PIN 값을 알려줘야 합니다.

SDI 서버에 새 사용자를 추가하면 기존 사용자의 PIN을 삭제하는 것과 동일한 결과가 발생합니다. 두 경우 모두 사용자는 새 PIN을 제공하거나 SDI 서버에서 새 PIN을 할당받아야 합니다. 이 모드에서, 하드웨어 토큰용으로 사용자는 RSA 디바이스의 토큰 코드만 입력합니다. 두 경우 모두 PIN 값이 있으면 SDI 서버 관리자는 사용자에게 사용할 PIN 값을 알려줘야 합니다.

새 **PIN** 생성

현재 PIN이 없는 경우, 시스템이 구성된 방식에 따라 SDI 서버는 다음 조건 중 하나를 충족해야 합니다.

- 시스템에서 사용자에게 새 PIN을 할당해야 합니다(기본값).
- 사용자가 새 PIN을 생성해야 합니다.
- 사용자가 PIN을 생성할지 또는 시스템에서 PIN을 할당할지 선택할 수 있습니다.

원격 사용자가 PIN을 생성할지 또는 시스템에서 PIN을 할당할지 선택하도록 SDI 서버가 구성된 경우, 로그인 화면에 이 옵션을 보여주는 드롭다운 목록이 표시됩니다. 상태 표시줄은 프롬프트 메시지를 제공합니다.

시스템 할당 PIN의 경우, SDI 서버에서 사용자가 로그인 페이지에 입력하는 암호를 허용하면 보안 게이트웨이는 클라이언트에 시스템 할당 PIN을 전송합니다. 클라이언트는 사용자가 새 PIN을 확인했으며 시스템이 "다음 암호" 시도를 계속 수행함을 나타내는 응답을 보안 게이트웨이에 다시 전송합니다.

사용자가 새 PIN을 생성하도록 선택하는 경우, AnyConnect에서는 이 PIN을 입력할 대화 상자가 표시됩니다. PIN은 4자리에서 8자리의 숫자여야 합니다. PIN은 일종의 비밀번호이므로 사용자가 이 입력 필드에 입력하는 내용은 모두 별표로 표시됩니다.

RADIUS 프록시를 통한 PIN 확인은 별도의 시도로 처음 대화 상자 다음에 발생합니다. 클라이언트는 새 PIN을 보안 게이트웨이에 전송하고 보안 게이트웨이는 "다음 암호" 시도를 계속합니다.

"다음 암호**"** 및 **"**다음 토큰 코드**"** 시도

"다음 암호" 시도의 경우, 클라이언트는 새 PIN 생성 또는 할당 작업 중에 캐시된 PIN 값을 사용하여 RSA SecurID 소프트웨어 토큰 DLL에서 다음 암호를 검색하고 사용자에게 프롬프트를 표시하지 않

고 이 암호를 보안 게이트웨이에 반환합니다. 마찬가지로 소프트웨어 토큰을 위한 "다음 토큰 코드" 시도의 경우, 클라이언트는 RSA SecurID 소프트웨어 토큰 DLL에서 다음 토큰 코드를 검색합니다.

네이티브 SDI와 RADIUS SDI 비교

네트워크 관리자는 다음 모드 중 하나에서 SDI 인증을 허용하도록 보안 게이트웨이를 구성할 수 있습니다.

- 네이티브 SDI는 SDI 인증을 처리하기 위해 SDI 서버와 직접 통신할 수 있는 보안 게이트웨이의 네이티브 기능을 의미합니다.
- RADIUS SDI는 SDI 서버와 통신하는 RADIUS SDI 프록시를 사용하여 SDI 인증을 수행하는 보안 게이트웨이의 프로세스를 의미합니다.

네이티브 SDI 및 RADIUS SDI는 원격 사용자에게 동일하게 나타납니다. SDI 메시지는 SDI 서버에서 구성할 수 있으므로 ASA의 메시지 텍스트는 SDI 서버의 메시지 텍스트와 일치해야 합니다. 그렇지 않으면 원격 클라이언트 사용자에게 표시된 프롬프트가 인증 시 필요한 작업에 적합하지 않을 수 있습니다. AnyConnect가 응답하지 않고 인증이 실패할 수 있습니다.

일부 예외를 포함하여 RADIUS SDI 요청은 기본적으로 네이티브 SDI 교환을 미러링합니다. 궁극적으로 네이티브 SDI와 RADIUS SDI 모두 SDI 서버와 통신하므로 클라이언트에서 필요한 정보 및 정보가 요청되는 순서는 같습니다.

인증 시 RADIUS 서버는 ASA에 대한 액세스 요청 메시지를 제공합니다. 이러한 챌린지 메시지 안에는 SDI 서버의 텍스트를 포함하는 응답 메시지가 있습니다. 메시지 텍스트는 ASA가 SDI 서버와 직접 통신하는 경우와 RADIUS 프록시를 통해 통신하는 경우에 서로 다릅니다. 따라서 AnyConnect에 대한 네이티브 SDI 서버로 표시되도록 ASA는 RADIUS 서버의 메시지를 해석해야 합니다.

또한 SDI 메시지는 SDI 서버에 구성할 수 있으므로 ASA의 메시지 텍스트는 SDI 서버의 메시지 텍스트와 전체 또는 부분적으로 일치해야 합니다. 그렇지 않으면 인증 시 필요한 작업에 적합하지 않은 프롬프트가 원격 클라이언트 사용자에게 표시될 수 있습니다. AnyConnect가 응답하지 않고 인증이 실패할 수 있습니다.

RADIUS/SDI 메시지를 지원하기 위한 ASA 구성

SDI별 RADIUS 응답 메시지를 해석하고 AnyConnect 사용자에게 적절한 조치에 대해 프롬프트를 표시하도록 ASA를 구성하려면 SDI 서버와의 직접적인 통신을 시뮬레이션하는 방식으로 RADIUS 응답 메시지를 전달하도록 연결 프로파일(터널 그룹)을 구성해야 합니다. SDI 서버에 대해 인증 중인 사용자는 이 연결 프로파일을 통해 연결해야 합니다.

프로시저

단계 1 **Configuration**(구성) > **Remote Access VPN**(원격 액세스 **VPN**) > **Network (Client) Access**(네트워크(클라이언트) 액세스) > **AnyConnect Connection Profiles**(**AnyConnect** 연결 프로파일)로 이동합니다.

단계 2 SDI별 RADIUS 응답 메시지를 해석하기 위해 구성하려는 연결 프로파일을 선택하고 **Edit**(편집)를 클릭합니다.

단계 3 **Edit AnyConnect Connection Profile(AnyConnect** 연결 프로파일 편집**)** 창에서 왼쪽 탐색 창의 Advanced(고급) 노드를 확장하고 **Group Alias/Group URL(**그룹 별칭/그룹 **URL)**을 선택합니다.

단계 4 **Enable the display of SecurID messages on the login screen(**로그인 화면에서 **SecurID** 메시지 표시 활성화**)**을 선택합니다.

단계 5 **OK(**확인**)**를 클릭합니다.

단계 6 **Configuration(**컨피그레이션**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **AAA/Local Users(AAA/** 로컬 사용자**)** > **AAA Server Groups(AAA** 서버 그룹**)**를 선택합니다.

단계 7 AAA 서버 그룹을 추가하려면 **Add(**추가**)** 를 클릭하십시오.

단계 8 Edit AAA Server Group(AAA 서버 그룹 편집) 대화 상자에서 AAA 서버 그룹을 구성하고 **OK(**확인**)**를 클릭합니다.

단계 9 **AAA Server Groups(AAA** 서버 그룹**)** 영역에서 방금 생성한 AAA 서버 그룹을 선택한 다음 **Servers in the Selected Group(**선택한 그룹에 있는 서버**)** 영역에서 **Add(**추가**)** 를 클릭합니다.

단계 10 SDI 메시지 영역에서 **Message Table(**메시지 테이블**)** 영역을 확장합니다. 메시지를 편집하려면 메시지 텍스트 필드를 더블 클릭합니다. ASA에 있는 RADIUS 응답 메시지 텍스트를 RADIUS 서버에서 전송된 메시지 텍스트와 전체 또는 부분에서 일치하도록 구성합니다.

다음 표는 각 메시지의 메시지 코드, 기본 RADIUS 응답 메시지 텍스트 및 기능을 보여줍니다.

참고 ASA에서 사용하는 기본 메시지 텍스트는 Cisco Secure Access Control Server(ACS)에서 사용하는 기본 메시지 텍스트입니다. Cisco Secure ACS를 사용 중이며 Cisco Secure ACS에서 기본 메시지 텍스트를 사용 중인 경우, ASA에서 메시지 텍스트를 구성할 필요가 없습니다.

보안 어플라이언스는 이 표에 나타나는 순서대로 문자열을 검색하므로 메시지 텍스트에 사용하는 문자열이 다른 문자열의 하위 집합이 아닌지 확인해야 합니다. 예를 들어 "new PIN"은 new-pin-sup 및 next-ccode-and-reauth 모두에 대한 기본 메시지 텍스트의 하위 집합입니다. new-pin-sup를 "새 PIN"으로 구성한 경우, 보안 어플라이언스가 RADIUS 서버에서 "다음 카드 코드가 있는 새 PIN"을 수신할 때 텍스트를 next-ccode-and-reauth 코드 대신 new-pin-sup 코드에 일치시킵니다.

메시지 코드	기본 **RADIUS** 응답 메시지 텍스트	기능
next-code	다음 암호를 입력하십시오.	사용자가 PIN 없이 다음 토큰 코드를 입력해야 함을 나타냅니다.
new-pin-sup	새 PIN을 기억하십시오.	새 시스템 PIN이 제공되었음을 나타내며 해당 사용자용 PIN을 표시합니다.
new-pin-meth	사용자 고유의 PIN을 입력하시겠습니까?	새 PIN을 생성하기 위해 새 PIN 방법을 사용하는 사용자로부터의 요청입니다.
new-pin-req	새 영숫자 PIN을 입력하십시오.	사용자가 생성한 PIN을 나타내며 사용자에게 PIN을 입력하도록 요청합니다.

메시지 코드	기본 **RADIUS** 응답 메시지 텍스트	기능
new-pin-reenter	PIN 다시 입력:	사용자 제공 PIN 확인을 위해 ASA에서 내부적으로 사용됩니다. 클라이언트는 사용자에게 프롬프트를 표시하지 않고 PIN을 확인합니다.
new-pin-sys-ok	새 PIN이 승인되었습니다.	사용자 제공 PIN이 승인되었음을 나타냅니다.
next-ccode-and-reauth	다음 카드 코드가 있는 새 PIN입니다.	PIN 작업에 따라 사용자가 다음 토큰 코드를 기다려야 하며 인증을 위해 새 PIN과 다음 토큰 코드를 모두 입력해야 함을 나타냅니다.
ready-for-sys- pin	시스템에서 생성한 PIN을 승인합니다.	사용자가 시스템에서 생성한 PIN을 사용할 준비가 되었음을 나타내기 위해 ASA에서 내부적으로 사용됩니다.

단계 **11** **OK(**확인**)**를 클릭한 다음 **Apply(**적용**)**, **Save(**저장**)**를 순서대로 클릭합니다.

인증서 고정 정보

AnyConnect 인증서를 고정하면 서버 인증서 체인이 실제로 연결 중인 서버에서 제공된 것인지를 탐지할 수 있습니다. VPN 프로파일 설정을 통해 사용법을 파악할 수 있는 이 기능은 AnyConnect 서버 인증서 확인 정책에 추가된 기능입니다. AnyConnect 로컬 정책 파일의 엄격한 인증서 신뢰 설정은 인증서 고정 검사에 영향을 주지 않습니다. VPN 프로파일에서 글로벌로 또는 호스트별로 고정을 구성할 수 있습니다. 기본 호스트용으로 구성된 고정은 서버 목록의 백업 호스트에도 유효합니다. 사용자는 인증서 고정 검사를 수행하는 기본 설정을 제어할 수 없습니다. 고정 확인이 실패하면 VPN 연결이 종료됩니다.

참고 AnyConnect는 기본 설정이 활성화되어 있으며 연결 중인 서버의 VPN 프로파일에 고정이 있을 때만 고정 확인을 수행합니다.

VPN 프로파일 편집기 AnyConnect 프로파일 편집기, 인증서 고정, 103 페이지에서 기본 설정을 활성화하고 글로벌 및 호스트별 인증서 고정을 구성할 수 있습니다.

인증서 고정을 구성하고 유지 보수할 때는 주의해야 합니다. 기본 설정을 지정할 때는 다음 권장 사항을 고려하십시오.

- 루트 및/또는 중간 인증서는 CA 생산업체가 운영 체제에서 적절하게 유지 보수하므로 고정합니다.
- CA 손상 시 백업으로 사용할 수 있도록 서로 다른 CA의 여러 루트 및/또는 중간 인증서를 고정합니다.
- CA를 쉽게 전환할 수 있도록 여러 루트 및/또는 중간 인증서를 고정합니다.
- 리프 인증서를 고정하는 경우에는 인증서 갱신 시 공개 키가 유지되도록 같은 인증서 서명 요청을 사용합니다.
- 서버 목록의 모든 연결 호스트를 고정합니다.

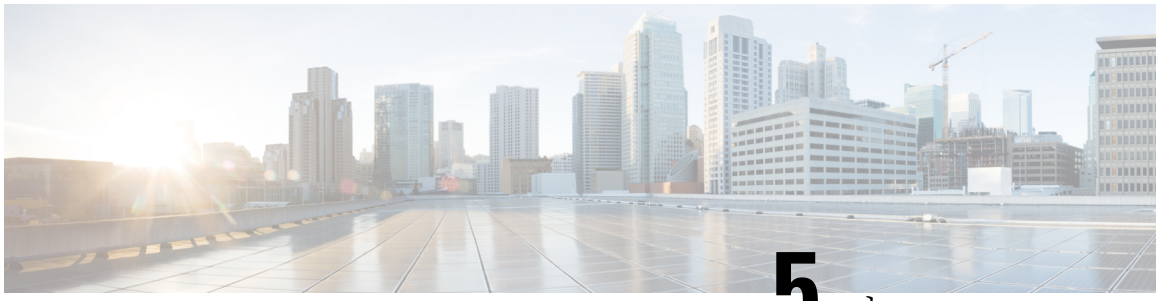
글로벌 및 호스트별 고정

인증서 고정은 글로벌로 또는 호스트별로 구성할 수 있습니다. 대다수 연결 호스트에 유효한 고정은 글로벌 고정으로 구성됩니다. 루트 중간 인증 증명을 구성하고 VPN 프로파일의 글로벌 고정 아래에서 와일드카드 리프 인증서를 구성하는 것이 좋습니다. 연결 호스트에만 유효한 고정은 호스트별 고정으로 간주됩니다. VPN 프로파일의 호스트별 고정 아래에서 리프 자체 서명 인증서를 구성하는 것이 좋습니다.

참고 AnyConnect는 고정 확인 중에 해당하는 연결 서버용 글로벌 고정 및 호스트별 고정을 확인합니다.

참고 여러 VPN 프로파일에 적용되는 글로벌 고정은 병합되지 않습니다. VPN 연결용 파일 연결 서버에서 고정을 엄격하게 고려합니다.

참고 Global Pins(글로벌 고정) 섹션에서 인증서 고정 기본 설정이 활성화되어 있어야 호스트별 인증서를 고정할 수 있습니다.



5 장

Network Access Manager 구성

이 장에서는 Network Access Manager 구성에 대한 개요뿐만 아니라 사용자 정책과 네트워크 프로파일의 추가 및 구성 지침을 제공합니다.

Network Access Manager 정보

Network Access Manager는 정책에 따라 보안 계층 2 네트워크를 제공하는 클라이언트 소프트웨어입니다. 이 소프트웨어는 최적의 계층 2 액세스 네트워크를 탐지 및 선택하고 유선 및 무선 네트워크 액세스를 위한 디바이스 인증을 수행합니다. Network Access Manager는 사용자와 디바이스 ID 및 보안 액세스에 필요한 네트워크 액세스 프로토콜을 관리합니다. 또한 최종 사용자가 관리자가 정의한 정책을 위반하는 연결을 하지 않도록 지능적으로 작동합니다.

Network Access Manager는 단일 홈 방식으로 사용하도록 설계되었으므로 네트워크 연결을 한 번에 하나만 허용합니다. 또한 유선 연결의 우선순위가 무선 연결보다 높으므로 유선 연결로 네트워크에 연결하면 무선 어댑터가 비활성화되며 IP 주소가 지정되지 않습니다.

참고 Network Access Manager는 Mac OS X이나 Linux에서는 지원되지 않습니다.

참고 Windows OS에서 ISE Posture를 사용 중인 경우에는 AnyConnect ISE Posture를 시작하기 전에 Network Access Manager를 설치해야 합니다.

Cisco AnyConnect Secure Mobility Client 의 Network Access Manager 구성 요소는 다음과 같은 주요 기능을 지원합니다.

- 유선(IEEE 802.3) 및 무선(IEEE 802.11) 네트워크 어댑터

- Windows 7을 사용하는 일부 모바일 광대역(3G) 네트워크 어댑터 (Microsoft 모바일 광대역 API를 지원하는 WAN 어댑터 필요)
- Windows 머신 자격 증명을 사용한 사전 로그인 인증
- Windows 로그온 자격 증명을 사용한 단일 로그온 사용자 인증
- 간소화된 IEEE 802.1X 구성
- IEEE MACsec 유선 암호화 및 엔터프라이즈 정책 제어
- EAP 방법:
  - EAP-FAST, PEAP, EAP-TTLS, EAP-TLS 및 LEAP(EAP-MD5, EAP-GTC 및 IEEE 802.3 유선 전용 EAP-MSCHAPv2)
- 내부 EAP 방법:
  - PEAP - EAP-GTC, EAP-MSCHAPv2 및 EAP TLS
  - EAP-TTLS - EAP-MD5, EAP-MSCHAPv2 및 레거시 방법 (PAP, CHAP, MSCHAP 및 MSCHAPv2)
  - EAP-FAST - GTC, EAP-MSCHAPv2 및 EAP-TLS
- 암호화 모드 - 정적 WEP(개방 또는 공유), 동적 WEP, TKIP 및 AES
- 키 설정 프로토콜 - WPA, WPA2/802.11i
- AnyConnect는 다음 환경에서 스마트 카드가 제공된 자격 증명을 지원합니다.
  - Windows의 경우 Microsoft CAPI 및 CAPI 1.0 및 2.0(CNG)
  - Windows의 로그온은 ECDSA 인증서를 지원하지 않습니다. 따라서 Network Access Manager SSO(Single Sign-On)는 ECDSA 클라이언트 인증서를 지원하지 않습니다.

Suite B와 FIPS

다음 기능은 FIPS에서 인증되며 예외사항은 다음에 나열되어 있습니다.

- ACS 및 ISE는 Suite B를 지원하지 않지만 OpenSSL 1.x가 있는 FreeRADIUS 2.x는 지원합니다. Microsoft NPS 2008은 부분적으로 Suite B를 지원합니다(NPS 인증서가 계속 RSA로 암호화되어야 함).
- 802.1X/EAP는 전환용 Suite B 프로파일만 지원합니다(RFC 5430에 정의된 대로). TLS 1.2는 지원되지 않습니다.
- MACsec은 Windows 7에서 FIPS 규정을 준수합니다.
- ECDH(Elliptic Curve Diffie-Hellman) 키 교환은 Windows 7에서 지원됩니다.
- ECDSA 클라이언트 인증서는 Windows 7에서 지원됩니다.

- OS 저장소에 있는 ECDSA CA 인증서는 Windows 7에서 지원됩니다.
- 네트워크 프로파일(PEM으로 인코딩됨)에 있는 ECDSA CA 인증서는 Windows 7에서 지원됩니다.
- 서버의 ECDSA 인증서 체인 확인은 Windows 7에서 지원됩니다.

단일 로그인 "단일 사용자" 적용

Microsoft Windows에서는 여러 사용자가 동시에 로그온할 수 있지만 Cisco AnyConnect Network Access Manager는 네트워크 인증을 단일 사용자로 제한합니다. AnyConnect Network Access Manager는 로그온한 사용자 수와 관계없이 데스크톱 또는 서버 당 한 명의 사용자에 대해 활성화될 수 있습니다. 단일 사용자 로그인 적용은 한 명의 사용자만 시스템에 언제든 한 번 로그인할 수 있으며 관리자는 현재 로그인한 사용자를 강제로 로그오프할 수 없음을 의미합니다.

Network Access Manager 클라이언트 모듈이 Windows 데스크톱에 설치된 경우, 기본 동작은 단일 사용자 로그온을 적용하는 것입니다. 서버에 설치된 경우, 기본 동작은 단일 사용자 로그인 적용을 완화하는 것입니다. 어느 경우에나 기본 동작을 변경하기 위해 레지스트리를 수정하거나 추가할 수 있습니다.

제한 사항

- Windows 관리자는 현재 로그온한 사용자를 강제로 로그오프시킬 수 없습니다.
- 연결된 워크스테이션에 대한 RDP는 동일한 사용자에 대해 지원됩니다.
- 동일한 사용자로 간주되려면 동일한 자격 증명 형식이어야 합니다. 예를 들어 user/example은 user@example.com과 동일하지 않습니다.
- 또한 스마트 카드 사용자는 동일한 PIN을 지녀야 동일한 사용자로 간주됩니다.

단일 로그인 단일 사용자 적용 구성

Windows 워크스테이션 또는 서버에서 여러 명의 사용자를 처리하는 방식을 변경하려면 레지스트리에서 EnforceSingleLogon의 값을 변경하십시오.

Windows에서 레지스트리 키는 **EnforceSingleLogon**이며 OverlayIcon 키와 동일한 레지스트리 위치에 있습니다.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential
Providers\{B12744B8-5BB7-463a-B85E-BB7627E73002}
```

단일 또는 여러 사용자 로그온을 구성하려면 이름이 EnforceSingleLogon인 DWORD를 추가하고 값으로 1 또는 0을 지정합니다.

Windows의 경우:

- 1은 한 명의 사용자로 로그온을 제한합니다.
- 0은 여러 사용자의 로그온을 허용합니다.

Network Access Manager 구축

Network Access Manager는 AnyConnect의 일부로 구축됩니다. Network Access Manager 및 다른 모듈과 함께 AnyConnect를 설치하는 방법에 대한 자세한 내용은 AnyConnect 구축 개요를 참조하십시오.

지침

- Windows 네트워크 상태 작업 트레이 아이콘 문제 — Network Access Manager가 Windows 네트워크 관리를 재정의합니다. 따라서 Network Access Manager를 설치한 후에는 네트워크 상태 아이콘을 사용하여 네트워크에 연결할 수 없습니다.

  권장 조치 Windows 그룹 정책에서 **Remove the networking icon(**네트워킹 아이콘 제거**)**을 설정하여 작업 트레이에서 Windows 네트워크 아이콘을 제거하십시오. 이 설정은 트레이 아이콘에만 영향을 미칩니다. 사용자는 제어판을 사용하여 계속 네이티브 무선 네트워크를 생성할 수 있습니다.

- Windows 7의 숨겨진 네트워크 및 네트워크 선택 — Network Access Manager가 Network Access Manager 네트워크 스캔 목록에서 구성된 네트워크에만 연결을 시도합니다.

  Windows 7에서는 Network Access Manager가 숨겨진 SSID를 검색합니다. 첫 번째 숨겨진 SSID가 발견되면 검색을 중단합니다. 숨겨진 네트워크가 여러 개 구성된 경우 Network Access Manager가 다음과 같이 SSID를 선택합니다.

  - 관리자가 정의한 숨겨진 첫 번째 기업 네트워크. 워크스테이션의 기본 구성은 1이고 서버에 대한 기본값은 0입니다.
  - 관리자가 정의한 숨겨진 네트워크
  - 관리자가 정의한 숨겨진 첫 번째 네트워크. Network Access Manager가 한 번에 1개의 비브로드캐스트 SSID만 검색할 수 있으므로 Cisco에서는 사이트에 하나의 숨겨진 기업 네트워크만 사용할 것을 권장합니다.

- 네트워크 연결의 일시적 손실 또는 더 긴 연결 시간 — Network Access Manager를 설치하기 전에 Windows에서 네트워크를 정의한 경우, Windows 연결 관리자가 종종 해당 네트워크로 연결을 시도합니다.

  권장 조치 네트워크가 범위 내에 있는 경우 모든 Windows 정의 네트워크에 대한 **Connect Automatically(**자동 연결**)**를 해제하거나 Windows 정의 네트워크를 모두 삭제하십시오.

- Network Access Manager 모듈이 클라이언트 시스템에 처음 설치된 경우, 일부 기존 Windows 7 또는 이후 무선 프로파일을 Network Access Manager 프로파일로 변환하도록 이 모듈을 구성할 수 있습니다. 다음의 기준에 일치하는 인프라 네트워크를 변환할 수 있습니다.

  - 개방성
  - 정적 WEP
  - WPA/WPA2 Personal
  - 비GPO 네이티브 Wi-Fi 사용자 네트워크 프로파일만 변환됩니다.

- 프로파일을 변환하는 동안 WLAN 서비스가 시스템에서 실행되고 있어야 합니다.
- Network Access Manager XML 구성 파일(userConfiguration.xml)이 이미 존재하는 경우 변환이 수행되지 않습니다.

네트워크 프로파일 변환을 활성화하려면 PROFILE_CONVERSION 속성값을 1로 설정하는 MSI 변형을 생성하여 MSI 패키지에 적용하십시오. 또는 커맨드 라인에서 PROFILE_CONVERSION 속성을 1로 바꾸고 MSI 패키지를 설치하십시오. (예: **msiexec /i AnyConnect nam Win the 3.1.xxxxx k9.msi PROFILE_CONVERSION=1**)

- ISE Posture 시작 전에 Network Access Manager를 설치해야 합니다. ISE Posture는 네트워크 변경 이벤트 및 802.1x WiFi를 탐지하기 위해 Network Access Manager 플러그인을 사용합니다.

DHCP 연결 비활성화 테스트

네트워크가 동적 IP 주소를 사용하도록 구성되어 있으면 Windows OS 서비스는 DHCP를 사용하여 연결을 설명하려고 시도합니다. 그러나 운영 체제 프로세스가 DHCP 트랜잭션을 완료했음을 Network Access Manager에 알리기 전까지 최대 2분이 걸릴 수 있습니다. Network Access Manager는 OS를 통한 연결 설정 시 긴 지연을 방지하고 네트워크 연결을 확인하기 위해 OS DHCP 트랜잭션과 함께 DHCP 트랜잭션을 트리거합니다.

연결 테스트를 위해 NAM을 통한 DHCP 트랜잭션 사용을 비활성화하려는 경우 다음 레지스트리 키를 DWORD로 추가하고 값을 아래에 나와 있는 대로 설정합니다.

- 64비트 Windows - HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Cisco\Cisco AnyConnect Network Access Manager\DisableDHCP를 1로 설정합니다.
- 32비트 Windows - HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\Cisco AnyConnect Network Access Manager\DisableDHCP를 1로 설정합니다.

참고 Network Access Manager DHCP 연결 테스트는 비활성화하지 않는 것이 좋습니다. 이 테스트를 비활성화하면 연결 시간이 더 오래 걸리는 경우가 많기 때문입니다.

Network Access Manager 프로파일

Network Access Manager 프로파일은 ASDM에서 독립 실행형 Windows 애플리케이션으로 사용 가능한 Network Access Manager 프로파일 편집기에 구성됩니다.

클라이언트 정책 창

Client Policy(클라이언트 정책**)** 창을 사용하여 클라이언트 정책 옵션을 구성할 수 있습니다. 다음 섹션이 포함됩니다.

연결 설정:

사용자의 로그온 전 또는 로그온 이후에 네트워크 연결 시도 여부를 정의할 수 있습니다.

- **Default Connection Timeout(**기본 연결 시간 제한**)**— 사용자가 생성한 네트워크에 대한 연결 시간 제한으로 사용할 시간(초)입니다. 기본값은 40초입니다.
- **Before User Logon(**사용자 로그온 전**)**— 사용자가 로그온하기 전에 네트워크에 연결합니다. 지원되는 사용자 로그온 유형에는 사용자 계정(Kerberos) 인증, 사용자 GPO 로드 및 GPO 기반 로그온 스크립트 실행이 포함됩니다. 사용자 로그온 전을 선택한 경우 사용자 로그온 허용 전 대기 시간도 설정할 수 있습니다.
- **Time to wait before allowing user to Logon(**사용자 로그온 허용 전 대기 시간**)**— Network Access Manager가 완벽한 네트워크 연결을 설정하기 위해 대기하는 최대(최악) 시간(초)을 지정합니다. 네트워크 연결을 이 시간 이내에 설정할 수 없는 경우, Windows 로그온 프로세스에서 사용자 로그온을 계속됩니다. 기본값은 5초입니다.

  참고 Network Access Manager가 무선 연결을 관리하도록 구성된 경우 무선 연결을 설정하는 데 걸릴 수 있는 추가 시간으로 인해 **Time to wait before allowing user to Logon(**사용자 로그온 허용 전 대기 시간**)** 을 30초 이상으로 설정해야 합니다. DHCP를 통해 IP 주소를 얻는 데 필요한 시간도 고려해야 합니다. 2개 이상의 네트워크 프로파일이 구성된 경우, 2개 이상의 연결 시도를 포함하도록 값을 늘려야 합니다.

- **After User Logon(**사용자 로그온 후**)**— 사용자가 Windows에 로그온한 이후에 네트워크에 연결합니다.

미디어

어떤 미디어 유형을 Network Access Manager 클라이언트에서 제어할지 지정합니다.

- **Manage Wi-Fi(wireless) Media(Wi-Fi (**무선**)** 미디어 관리**)**— Wi-Fi 미디어 관리 및 선택적으로 WPA/WPA2 핸드셰이크 검증을 활성화합니다.

  IEEE 802.11i 무선 네트워킹 표준에서는 신청자(이 경우 Network Access Manager)가 액세스 포인트 RSN IE(Robust Secure Network Information Exchange, 강력한 보안 네트워크 정보 교환)를 검증해야 한다고 지정합니다. IE는 키 유도 중에 IEEE 801.X 프로토콜 패킷의 EAPOL 키 데이터로 전송되고, 비콘/프로브 응답 프레임 내에서 발견된 액세스 포인트 RSN IE와 일치해야 합니다.

- **Enable validation of WPA/WPA2 handshake(WPA/WPA2** 핸드셰이크 검증 활성화**)**— WPA/WPA2 핸드셰이크를 검증합니다. 이 옵션을 선택하지 않으면 이 선택적인 검증 단계를 건너뜁니다.

  참고 일부 어댑터는 액세스 포인트 RSN IE를 지속적으로 제공하지 않으므로 인증 시도가 실패하고 클라이언트에 연결되지 않습니다.

- **Default Association Timeout(**기본 연계 시간 제한**)(**초**)** — WPA/WPA2 핸드셰이크를 활성화한 경우, 기본 연계 시간 제한을 지정해야 합니다.
- **Manage Wired (IEEE 802.3) Media(**유선**(IEEE 802.3)** 미디어 관리**)**— 유선 연결 관리를 활성화합니다.
- **Manage Mobile Broadband(3G) Media(**모바일 광대역**(3G)** 미디어 관리**)**— Windows 7 모바일 광대역 어댑터 관리를 활성화합니다. 이 기능은 기본적으로 비활성화되어 있습니다.

참고 이 기능은 베타 릴리스 상태입니다. Cisco TAC는 베타 릴리스에 대한 지원을 제공하지 않습니다.

- **Enable Data Roaming(**데이터 로밍 활성화**)**— 데이터 로밍 허용 여부를 결정합니다.

최종 사용자 제어

사용자에 대해 다음 제어 권한을 구성할 수 있습니다.

- **Disable Client(**클라이언트 비활성화**)**— AnyConnect UI를 사용하는 유선 및 무선 미디어에 대한 Network Access Manager의 관리를 사용자가 비활성화 및 활성화하도록 허용합니다.
- **Display user groups(**사용자 그룹 표시**)**— 사용자가 생성한 그룹(CSSC 5.x에서 생성됨)이 관리자 정의 그룹과 일치하지 않는 경우에도 이 그룹을 표시하고 연결 가능하도록 설정합니다.
- **Specify a script or application to run when connected(**연결 시 스크립트 또는 애플리케이션을 실행하도록 지정**)**— 네트워크 연결 시 사용자가 스크립트 또는 애플리케이션을 실행하도록 허용합니다.

참고 스크립팅 설정은 사용자가 구성한 단일한 네트워크에 특정하며 해당 네트워크가 연결된 상태로 전환될 때 사용자가 로컬 파일(.exe, .bat 또는 .cmd)을 실행하도록 허용합니다. 충돌을 방지하기 위해 스크립팅 기능은 사용자가 관리자 정의 네트워크가 아니라 사용자 정의 네트워크용으로만 스크립트 또는 애플리케이션을 구성하도록 허용합니다. 이 기능에서는 사용자가 스크립트 실행에 대한 관리자 네트워크를 변경하는 것을 허용하지 않습니다. 따라서 관리자 네트워크용 인터페이스를 사용할 수 없습니다. 또한 실행 중인 스크립트를 사용자가 구성하도록 허용하지 않은 경우, 이 기능은 Network Access Manager GUI에 표시되지 않습니다.

- **Auto-connect(**자동 연결**)**— 사용자가 연결을 선택하지 않아도 네트워크에 자동으로 연결됩니다. 기본값은 자동 연결입니다.

관리 상태

- **Service Operation(**서비스 작업**)**— 해당 서비스를 꺼 놓은 경우, 이 프로파일을 사용하는 클라이언트는 계층 2 연결을 설정하기 위해 연결할 수 없습니다.
- **FIPS Mode(FIPS** 모드**)**— FIPS 모드를 활성화한 경우, Network Access Manager가 정부 요건을 충족시키는 방법으로 암호화 작업을 수행합니다.

  FIPS(Federal Information Processing Standard 140-2 레벨 1)는 암호화 모듈에 대한 보안 요건을 지정하는 미국 정부 표준입니다. FIPS는 소프트웨어와 하드웨어의 종류에 따라 MACsec 또는 Wi-Fi용 Network Access Manager에서 지원됩니다.

  표 ***8: Network Access Manager***의 ***FIPS*** 지원

미디어**/**운영 체제	**Windows 7**
MACsec과 연결됨	Intel HW MACsec 가능 NIC 또는 하드웨어가 아닌 MACsec을 사용하는 경우 FIPS 규정 준수
Wi-Fi	FIPS 규정을 준수하지 않음

인증 정책 창

인증 정책 창에서 모든 네트워크 연결에 적용되는 연계 및 인증 네트워크 필터를 생성할 수 있습니다. 연계 또는 인증 모드 중 하나를 선택하지 않은 경우, 사용자는 Wi-Fi 네트워크 인증에 연결할 수 없습니다. 모드의 하위 집합을 선택한 경우, 사용자는 해당 유형에 대해서만 네트워크에 연결할 수 있습니다. 각 필수 연계 또는 인증 모드를 선택하거나 **Select All(**모두 선택**)**을 선택합니다.

내부 방식은 특정한 인증 프로토콜로만 제한될 수 있습니다. 내부 방식은 Allowed Authentication Mode(허용된 인증 모드) 창에서 외부 방식(터널링) 아래에 들여쓰기 되었습니다.

인증 프로토콜을 선택하기 위한 메커니즘은 현재 클라이언트 인증 데이터베이스와 통합됩니다. 보안 무선 LAN 구축 시에는 사용자용으로 새로운 인증 시스템을 생성할 필요가 없습니다.

내부 터널링에 사용 가능한 EAP 방식은 내부 방식 자격 증명 유형 및 외부 터널링 방식을 기반으로 합니다. 다음 목록에서 각각의 외부 터널 방식은 각 자격 증명 유형에 대해 지원되는 내부 방식 유형입니다.

- PEAP
  - 비밀번호 자격 증명: EAP-MSCHAPv2 또는 EAP-GTC
  - 토큰 자격 증명: EAP-GTC
  - 인증서 자격 증명: EAP-TLS
- EAP-FAST
  - 비밀번호 자격 증명: EAP-MSCHAPv2 또는 EAP-GTC
  - 토큰 자격 증명: EAP-GTC

- 인증서 자격 증명: EAP-TLS

- EAP-TTLS
  - 비밀번호 자격 증명: EAP-MSCHAPv2, EAP-MD5, PAP(L), CHAP(L), MSCHAP(L), MSCHAP-v2(레거시)
  - 토큰 자격 증명: PAP(레거시). 시도/응답 방법이 토큰 기반 인증에 적합하지 않으므로 Network Access Manager에서 지원하는 기본 토큰 옵션은 PAP입니다.
  - 인증서 자격 증명: 해당 없음

네트워크 창

네트워크 창에서 엔터프라이즈 사용자를 위해 미리 정의된 네트워크를 구성할 수 있습니다. 모든 그룹이 사용할 수 있는 네트워크를 구성하거나 특정 네트워크에서 그룹을 생성할 수 있습니다. 네트워크 창은 기존 창에 창을 추가할 수 있는 마법사를 표시하고 **Next(**다음**)**를 클릭하여 추가 구성 옵션으로 진행하게 해줍니다.

그룹은 기본적으로 구성된 연결(네트워크)의 컬렉션입니다. 모든 구성된 연결은 그룹에 속하거나 모든 그룹의 요소여야 합니다.

참고 이전 버전과의 호환성을 위해 Cisco Secure Services Client로 구축된 관리자가 생성한 네트워크는 SSID를 브로드캐스트하지 않는 hidden network로 처리됩니다. 단 사용자 네트워크는 SSID를 브로드캐스트하는 네트워크로 처리됩니다.

관리자만 새 그룹을 생성할 수 있습니다. 그룹이 구성에 정의되어 있지 않은 경우, 프로파일 편집기가 자동 생성 그룹을 생성합니다. 자동 생성 그룹에는 관리자 정의 그룹에 할당되지 않은 네트워크가 포함되어 있습니다. 클라이언트는 활성 그룹에 정의된 연결을 사용하여 네트워크 연결을 생성하려고 시도합니다. 네트워크 그룹 창에서 **Create Networks(**네트워크 생성**)** 옵션의 설정에 따라 최종 사용자는 활성 그룹에 사용자 네트워크를 추가하거나 사용자 네트워크를 삭제할 수 있습니다.

정의된 네트워크는 목록의 맨 위에 있는 모든 그룹에서 사용할 수 있습니다. 전역 네트워크에 있는 네트워크를 제어하므로 최종 사용자가 연결할 수 있고 사용자 정의 네트워크에 있는 경우에도 엔터프라이즈 네트워크를 지정할 수 있습니다. 최종 사용자는 관리자 구성 네트워크를 수정하거나 제거할 수 없습니다.

참고 최종 사용자는 globalNetworks 섹션에 있는 네트워크를 제외하고 네트워크를 그룹에 추가할 수 있습니다. 이러한 네트워크는 모든 그룹에 존재하므로 프로파일 편집기를 사용하여 생성만 가능합니다.

엔터프라이즈 네트워크의 일반적인 최종 사용자는 이 클라이언트를 사용할 그룹에 대한 지식을 필요로 하지 않습니다. 활성 그룹은 구성의 첫 번째 그룹이지만 한 그룹만 사용할 수 있는 경우, 클라이언트는 활성 그룹을 알 수 없으며 표시하지 않습니다. 그러나 두 개 이상의 그룹이 존재할 경우, UI에는 활성 그룹이 선택되었는지를 나타내는 그룹 목록이 표시됩니다. 그러면 사용자는 활성 그룹에서

선택할 수 있으며 이 설정은 재부팅 시에도 지속됩니다. 네트워크 그룹 창에서 **Create Networks(**네트워크 생성**)** 옵션의 설정에 따라 최종 사용자는 그룹을 사용하지 않고 고유한 네트워크를 추가하거나 삭제할 수 있습니다.

참고 그룹 선택사항은 재부팅 및 네트워크 복구(트레이 아이콘을 마우스 오른쪽 버튼으로 클릭하고 **Network Repair(**네트워크 복구**)**를 선택 시 작동) 시에도 유지됩니다. Network Access Manager가 복구되거나 다시 시작된 경우, 이전 활성 그룹이 사용됩니다.

네트워크, 미디어 유형 페이지

네트워크 창 미디어 유형 페이지에서 유선 또는 무선 네트워크를 생성하거나 편집할 수 있습니다. 이 설정은 선택에 따라 달라집니다.

다음 섹션은 첫 번째 대화 상자에 포함되어 있습니다.

- 이름 — 이 네트워크에 대해 표시된 이름을 입력합니다.
- 그룹 멤버십 — 이 프로파일을 사용해야 하는 네트워크 그룹을 선택합니다.
- 네트워크 미디어 — 유선 또는 Wi-Fi(무선)를 선택합니다. Wi-Fi를 선택한 경우 다음 파라미터를 구성할 수 있습니다.
  - SSID — 무선 네트워크의 SSID(Service Set Identifier, 서비스 집합 ID)를 입력합니다.
  - Hidden Network — SSID를 브로드캐스트하지 않는 경우에도 네트워크에 대한 연결을 허용합니다.
  - Corporate Network — 네트워크가 근접한 위치에 있는 경우 기업용으로 구성된 네트워크에 대한 연결을 먼저 적용합니다. corporate network가 브로드캐스트하지 않는(hidden) SSID를 사용하며 hidden network로 구성된 경우, Network Access Manager는 hidden SSID를 적극적으로 탐색하고 corporate SSID가 범위 내에 있으면 연결을 설정합니다.
  - Association Timeout — Network Access Manager가 사용 가능한 네트워크를 재평가하기 전에 특정한 무선 네트워크와의 연계를 대기하는 시간을 입력합니다. 기본 association timeout은 5초입니다.
- 일반 설정
  - 스크립트 또는 애플리케이션 — 로컬 시스템에서 실행할 파일 경로 및 파일 이름을 입력하거나 폴더를 검색하고 하나를 선택합니다. 다음 규칙은 스크립트 및 애플리케이션에 적용됩니다.

    .exe, .bat 또는 .cmd 확장명이 있는 파일이 허용됩니다.

    사용자가 관리자가 생성한 네트워크에 정의된 스크립트 또는 애플리케이션을 변경하지 못할 수도 있습니다.

    프로파일 편집기를 사용하여 경로 및 스크립트 또는 애플리케이션 파일 이름만 지정할 수 있습니다. 스크립트 또는 애플리케이션이 사용자 머신에 존재하지 않는 경우에는 오류 메

시지가 나타납니다. 사용자는 스크립트 또는 애플리케이션이 머신에 없다는 사실을 통보받으며 시스템 관리자에게 문의해야 합니다.

애플리케이션이 사용자의 경로에 존재하지 않는 경우, 실행할 애플리케이션의 전체 경로를 지정해야 합니다. 애플리케이션이 사용자의 경로에 존재하는 경우, 애플리케이션 또는 스크립트 이름만 지정할 수 있습니다.

- 연결 시간 제한 — Network Access Manager가 다른 네트워크에 연결하려고 시도하거나(연결 모드가 자동인 경우) 다른 어댑터를 사용하기 전에 네트워크 연결을 설정하기 위해 대기하는 시간(초)을 입력합니다.

참고 일부 스마트카드 인증 시스템에서 인증을 완료하는 데 약 60초가 필요합니다. 스마트카드 사용 시 특히 연결에 성공하기 전에 여러 네트워크에서 시도해야 할 경우, 연결 시간 제한 값을 늘려야 합니다.

네트워크, 보안 수준 페이지

네트워크 마법사의 보안 수준 페이지에서 개방형 네트워크, 인증 네트워크 또는 공유 키 네트워크(무선 네트워크 미디어의 경우에만 표시됨)를 선택하십시오. 해당 네트워크 유형별로 구성 흐름이 서로 다르며 다음 섹션에 설명되어 있습니다.

- 인증 네트워크 구성— 보안 엔터프라이즈에 권장합니다.
- 개방형 네트워크 구성— 권장하지 않지만 종속 포털 환경을 통한 게스트 액세스를 제공하는 데 사용할 수 있습니다.
- 공유 키 네트워크 구성— 작은 사무실이나 가정과 같은 무선 네트워크에 권장합니다.

인증 네트워크 구성

보안 수준 섹션에서 인증 네트워크를 선택한 경우, 아래 설명된 바와 같이 추가 창이 나타납니다. 이 창에서 설정 구성을 완료한 경우, **Next(**다음**)** 버튼을 클릭하거나 **Connection Type(**연결 유형**)** 탭을 선택하여 네트워크 연결 유형 대화 상자를 엽니다.

802.1X 설정 창

네트워크 구성에 따라 IEEE 802.1X 설정을 조정하십시오.

참고 AnyConnect ISE Posture가 Network Access Manager를 사용하여 설치된 경우, ISE Posture는 Network Access Manager 플러그인을 사용하여 네트워크 변경 이벤트 및 802.1X WiFi를 탐지합니다.

- authPeriod(초) — 인증이 시작될 경우, 이 설정은 시간이 초과하여 인증자에게 인증을 다시 시작하도록 요청하기 전에 인증 메시지 신청자가 인증 메시지가 나타나는 동안 대기하는 시간을 결정합니다.

- heldPeriod(초) — 인증이 실패할 경우, 이 설정은 다른 인증 시도를 수행하기 전에 신청자가 대기하는 시간을 정의합니다.
- startPeriod(초) — EAPOL 시작 메시지에 대한 응답을 인증자로부터 수신하지 못한 경우, EAPOL 시작 메시지의 재전송 간 시간 간격(초)입니다.
- maxStart — 신청자가 인증자가 없다고 추측하기 전에 IEEE 801.X 프로토콜 패킷, EAPOL 키 데이터 또는 EAPoL 시작을 전송하여 신청자가 인증자를 통해 인증을 시작하는 횟수입니다. 이 경우 신청자는 데이터 트래픽을 허용합니다.

팁 인증을 시작하려고 시도하는 데 걸린 총 시간이 네트워크 연결 타이머보다 적은 경우(startPeriod x maxStart < 네트워크 연결 타이머)와 같이 startPeriod 및 maxStart를 주의깊게 설정하여 열려 있는 네트워크와 인증 네트워크 모두에서 작업을 수행할 수 있도록 단일 인증 유선 연결을 구성할 수 있습니다.

이 시나리오에서 클라이언트에 DHCP 주소를 확보하고 네트워크 연결을 완료할 수 있는 충분한 시간을 제공하려면 네트워크 연결 타이머를 startPeriod x maxStart초만큼 늘려야 합니다.

이와 반대로 인증이 성공한 이후에만 데이터 트래픽을 허용하려면 startPeriod 및 maxStart가 인증을 시작하려고 시도하는 데 걸린 총 시간이 네트워크 연결 타이머보다 큰 경우(startPeriod x maxStart > 네트워크 연결 타이머)에 해당하는지 확인하십시오.

보안 창

유선 네트워크에서만 표시됩니다.

Security(보안) 창에서 다음 매개변수에 대한 값을 선택하십시오.

- Key Management — MACsec 지원 유선 네트워크를 통해 사용할 키 관리 프로토콜을 결정합니다.
  - None — 키 관리 프로토콜이 사용되지 않고 유선 암호화가 수행되지 않습니다.
  - MKA — 신청자가 MACsec 키 계약 프로토콜 정책 및 암호화 키 협상을 시도합니다. MACsec은 유선 네트워크에 MAC 계층 암호화를 제공하는 MAC 계층 보안입니다. MACsec 프로토콜은 암호화로 MAC 수준의 프레임을 보장하는 수단을 나타내며 MKA(MACsec Key Agreement, MACsec 키 계약) 엔터티를 사용하여 암호화 키를 협상하고 배포합니다.
- Encryption
  - None — 데이터 트래픽이 무결성 검사를 완료했으나 암호화되지 않았습니다.
  - MACsec: AES-GCM-128 — 이 옵션은 키 관리를 위해 MKA를 선택한 경우에만 사용할 수 있습니다. 이 값을 통해 데이터 트래픽이 AES-GCM-128을 사용하여 암호화됩니다.

자세한 내용은 ID 기반 네트워킹 서비스: Mac 보안 을 참조하십시오.

포트 인증 예외 정책 창

이 창은 유선 네트워크에서만 표시됩니다.

포트 인증 예외 정책 창을 통해 인증 과정 중에 IEEE 802.1X 신청자의 동작을 조정할 수 있습니다. 포트 예외가 활성화되지 않은 경우, 신청자는 기존 동작을 계속하고 전체 구성이 성공적으로 완료되는 경우에만(또는 본 섹션의 앞부분에서 설명한 것과 같이 인증의 maxStarts 번호가 인증자의 응답 없이 시작된 후) 포트를 엽니다. 다음 옵션 중 하나를 선택하십시오.

- 인증 전 데이터 트래픽 허용 — 인증 시도 전 데이터 트래픽을 허용합니다.
- 다음과 같은 경우에도 인증 후 데이터 트래픽을 허용합니다.
  - EAP 실패 — 선택 시 신청자가 인증을 시도합니다. 인증이 실패할 경우 신청자가 인증 실패에도 불구하고 데이터 트래픽을 허용합니다.
  - EAP는 성공했지만 키 관리 실패 — 선택 시 신청자가 키 서버와 키를 협상하려고 했으나 어떤 이유로든 키 협상에 실패한 경우 데이터 트래픽을 허용합니다. 이 설정은 키 관리가 구성된 경우에만 사용할 수 있습니다. 키 관리가 None(없음)으로 설정된 경우 확인란이 흐리게 표시됩니다.

제한 MACsec은 ACS 버전 5.1 이상 및 MACsec 가능 스위치가 필요합니다. ACS 또는 스위치 구성은 *Catalyst 3750-X* 및 *3560-X* 스위치 소프트웨어 구성 가이드 를 참조하십시오.

연계 모드

이 창은 무선 네트워크에서만 나타납니다.

다음 중에서 연계 모드를 선택하십시오.

- WEP
- WAP 엔터프라이즈(TKIP)
- WPA 엔터프라이즈(AES)
- WPA 2 엔터프라이즈(TKIP)
- WPA 2 엔터프라이즈(AES)
- CCKM(TKIP) — (Cisco CB21AG 무선 NIC 필요)
- CCKM(AES) — (Cisco CB21AG 무선 NIC 필요)

개방형 네트워크 구성

개방형 네트워크는 인증 또는 암호화를 사용하지 않습니다. 개방형(비보안) 네트워크를 생성하려면 다음 단계를 따르십시오.

프로시저

단계 **1** 보안 수준 페이지에서 **Open Network(**개방형 네트워크**)** 를 선택합니다. 이 선택사항은 최소 보안 네트워크를 제공하고 게스트 액세스 무선 네트워크용으로 권장됩니다.

단계 **2** **Next(**다음**)**를 클릭합니다.

단계 **3** 연결 유형을 결정합니다.

공유 키 네트워크 구성

Wi-Fi 네트워크에서는 엔드포인트 및 네트워크 액세스 포인트 간에 데이터를 암호화할 때 사용하도록 공유 키를 사용하여 암호 키를 파생시킬 수 있습니다. WPA 또는 WPA2 Personal로 설정된 공유 키를 사용하면 소규모 사무실 또는 재택 사무실에 적합한 중간 수준의 보안 등급이 제공됩니다.

참고 공유 키 보안은 엔터프라이즈 무선 네트워크에는 권장되지 않습니다.

공유 키 네트워크를 보안 수준으로 설정하려는 경우 다음 단계를 따르십시오.

프로시저

단계 **1** **Shared Key Network(**공유 키 네트워크**)**를 선택합니다.

단계 **2** 보안 수준 창에서 **Next(**다음**)**를 클릭합니다.

단계 **3** **User Connection(**사용자 연결**)** 또는 **Machine Connection(**머신 연결**)**을 지정합니다.

단계 **4** **Next(**다음**)**를 클릭합니다.

단계 **5** 공유 키 유형 — 공유 키 유형을 결정하는 공유 키 연결 모드를 지정합니다. 선택 항목은 다음과 같습니다.

- WEP — 정적 WEP 암호화와 레거시 IEEE 802.11 개방형 시스템의 연결
- 공유 — 정적 WEP 암호화와 레거시 IEEE 802.11 공유 키의 연결
- WPA/WPA2-Personal — 암호 PSK(pre-shared key, 사전 공유 키)에서 암호화 키를 파생시키는 Wi-Fi 보안 프로토콜입니다.

단계 **6** 레거시 IEEE 802.11 WEP 또는 공유 키를 선택하는 경우 40비트, 64비트, 104비트 또는 128비트를 선택하십시오. 40비트 또는 64비트 WEP 키는 5자의 ASCII 문자 또는 10개의 16진수여야 합니다. 104비트 또는 128비트 WEP 키는 13자의 ASCII 문자 또는 26개의 16진수여야 합니다.

단계 **7** WPA 또는 WPA2 Personal을 선택한 경우 사용할 암호화 유형(TKIP/AES)을 선택한 다음 공유 키를 입력합니다. 키는 8자에서 63자의 ASCII 문자 또는 정확하게 64개의 16진수로 입력해야 합니다. 공유 키가 ASCII 문자로 구성된 경우 **ASCII** 를 선택합니다. 공유 키에 64개의 16진수가 포함된 경우 **Hexadecimal(16**진수**)**을 선택합니다.

단계 **8** **Done(**완료**)**을 클릭합니다. 그런 다음 **OK(**확인**)**를 클릭하십시오.

네트워크, 네트워크 연결 유형 창

이 섹션에서는 Network Access Manager 프로파일 편집기의 보안 수준을 따르는 네트워크 창의 네트워크 연결 유형 창에 관해 설명합니다. 다음 연결 유형 중 하나를 선택하십시오.

- 머신 연결 — Windows Active Directory에 저장된 디바이스의 이름이 권한 부여를 위해 사용됩니다. 머신 연결은 일반적으로 사용자 자격 증명이 연결에 필요하지 않을 때 사용합니다. 사용자가 로그오프되고 사용자 자격 증명을 이용할 수 없더라도 종단국이 네트워크에 로그온해야 하는 경우, 이 옵션을 선택하십시오. 이 옵션은 일반적으로 사용자가 액세스하기 전에 도메인에 연결하고 네트워크에서 GPO 및 기타 업데이트를 얻기 위해 사용합니다.

  참고 알려진 네트워크가 없는 경우, VPN은 SBL(start before login, 로그인 전 시작)에 실패합니다. Before User Logon(사용자 로그온 전) 및 머신 연결 권한 부여를 위해 Network Access Manager를 구성하는 경우 Network Access Manager가 사용자에게 네트워크 정보를 요청하고 VPN SBL이 성공합니다.

- 사용자 연결 — 사용자 자격 증명이 권한 부여를 위해 사용됩니다.

  클라이언트 정책 창에서 Before User Logon(사용자 로그온 전)이 선택된 경우 사용자가 Windows 시작 화면에 로그온 자격 증명을 입력한 후 Network Access Manager가 사용자의 자격 증명을 수집합니다. Network Access Manager는 Windows가 사용자의 창 세션을 시작하는 동안 네트워크 연결을 설정합니다.

  클라이언트 정책 창에서 After User Logon(사용자 로그온 후)이 선택된 경우 사용자가 Windows에 로그온한 후 Network Access Manager가 연결을 시작합니다.

  사용자가 로그오프하면 현재 사용자 네트워크 연결이 종료됩니다. 머신 네트워크 프로파일을 사용할 수 있는 경우 NAM이 머신 네트워크에 다시 연결합니다.

- 머신 및 사용자 연결 — 보안 수준 창에서 선택한 것과 같이 인증 중인 네트워크를 구성하는 경우에만 사용할 수 있습니다. 머신 ID 및 사용자 자격 증명이 모두 사용되지만 머신 파트는 사용자가 디바이스에 로그온하지 않는 경우에만 유효합니다. 두 파트의 설정은 같지만 머신 연결을 위한 인증 유형 및 자격 증명은 사용자 연결의 인증 유형 및 자격 증명과 다를 수 있습니다.

  사용자가 로그인하지 않은 경우 머신 연결을 사용하고, 사용자가 로그인한 경우 사용자 연결을 사용하여 PC가 항상 네트워크에 연결되게 하려면 이 옵션을 선택하십시오.

  EAP—FAST는 EAP 방법으로 구성될 때(다음 창에서) EAP 연결이 지원됩니다. 이는 Network Access Manager에서 머신 및 사용자가 알려진 엔터티인지, 기업에서 관리하는지 확인한다는 것을 의미합니다.

  네트워크 연결 유형을 선택하면 선택한 네트워크 연결 유형을 위한 EAP 방법 및 자격 증명을 선택할 수 있는 추가 탭이 네트워크 대화 상자에 표시됩니다.

네트워크, 사용자 또는 머신 인증 페이지

네트워크 연결 유형을 선택한 후 해당 연결 유형에 대한 인증 방법을 선택하십시오. 인증 방법을 선택하면 선택한 방법에 표시가 업데이트되며 사용자는 추가 정보를 제공해야 합니다.

참고 MACsec을 활성화한 경우 PEAP, EAP-TLS 또는 EAP-FAST와 같은 키 유도를 지원하는 EAP 방법을 선택했는지 확인하십시오. 또한 MACsec이 활성화되지 않은 경우에도 Network Access Manager를 사용하면 MACsec을 계산하는 MTU가 1,500개에서 1,468개로 줄어듭니다.

EAP 개요

EAP는 처리 중인 전송 프로토콜에서 분리되는 인증 프로토콜의 요건을 지정하는 IETF RFC입니다. 이 분리를 통해 전송 프로토콜(예: IEEE 802.1X, UDP 또는 RADIUS)이 인증 프로토콜에 대한 변경 없이 EAP 프로토콜을 처리할 수 있습니다.

기본적인 EAP 프로토콜은 다음과 같이 네 가지 패킷 유형으로 이루어져 있습니다.

- EAP 요청 - 인증자가 요청 패킷을 신청자에게 전송합니다. 각 EAP 요청에는 사용할 신청자 ID 및 EAP 유형과 같은 요청 항목을 나타내는 유형 필드가 있습니다. 시퀀스 번호를 통해 인증자 및 피어가 EAP 응답을 각 EAP 요청에 일치시킬 수 있습니다.
- EAP 응답 - 신청자가 인증자에게 응답 패킷을 전송하고 시퀀스 번호를 사용하여 시작 EAP 요청을 일치시킵니다. 응답이 부정(NAK)이 아닌 경우 일반적으로 EAP 응답의 유형은 EAP 요청과 일치합니다.
- EAP 성공 - 인증이 성공하면 인증자가 신청자에게 성공 패킷을 전송합니다.
- EAP 실패 - 인증이 실패하면 인증자가 신청자에게 실패 패킷을 전송합니다.

EAP를 IEEE 802.11X 시스템에서 사용할 경우 액세스 포인트가 EAP 통과 모드에서 작동합니다. 이 모드에서는 액세스 포인트가 코드, ID 및 길이 필드를 확인한 후 신청자로부터 수신한 EAP 패킷을 AAA 서버에 전달합니다. AAA 서버 인증자로부터 수신한 패킷은 신청자에게 전달됩니다.

EAP-GTC

EAP-GTC는 간단한 사용자 이름과 비밀번호 인증을 기반으로 하는 EAP 인증 방법입니다. 시도 응답 방법을 사용하지 않고 사용자 이름과 비밀번호가 암호화되지 않은 텍스트로 전달됩니다. 이 방법은 터널링 EAP 메서드(아래의 터널링 EAP 메서드 참조) 내에서 또는 OTP(One Time Password, 일회용 비밀번호)를 사용하는 경우 권장됩니다.

EAP-GTC는 상호 인증을 제공하지 않습니다. 클라이언트만 인증하므로 Rogue 서버가 사용자의 자격 증명을 가져올 수도 있습니다. 상호 인증이 필요한 경우 EAP-GTC가 터널링 EAP 메서드 내부에서 사용되어 서버 인증을 제공합니다.

EAP-GTC를 통해 키 요소가 제공되지 않으므로 MACsec의 경우 이 방법을 사용할 수 없습니다. 추가 트래픽 암호화에 대한 키 요소가 필요한 경우, EAP-GTC가 터널링 EAP 메서드 내부에서 사용되어 키 요소 및 필요에 따라 내부 및 외부 EAP 메서드 암호화 바인딩을 제공합니다.

다음과 같이 2가지 비밀번호 소스 옵션이 있습니다.

- 비밀번호를 사용하여 인증 - 보호 수준이 양호한 유선 환경에만 적합합니다.
- 토큰을 사용하여 인증 - 토큰 코드 또는 OTP의 수명이 짧기 때문에(일반적으로 약 10초) 보안 수준이 더 강력합니다.

참고 Network Access Manager, 인증자 또는 EAP-GTC 프로토콜은 비밀번호와 토큰 코드를 구별할 수 없습니다. 이러한 옵션은 Network Access Manager 내의 자격 증명 수명에만 영향을 줍니다. 비밀번호는 로그아웃한 후에도 기억될 수 있으나 토큰 코드는 인증할 때마다 토큰 코드를 묻는 프롬프트가 사용자에게 표시되므로 기억될 수 없습니다.

비밀번호를 인증에 사용하는 경우 인증자에게 암호화되지 않은 텍스트로 전달되므로 해시된 비밀번호를 사용하는 데이터베이스에 대한 인증을 위해 이 프로토콜을 사용할 수 있습니다. 데이터베이스 누출의 가능성이 있는 경우 이 방법을 사용하는 것이 좋습니다.

EAP-TLS

EAP-TLS(EAP-Transport Layer Security, EAP 전송 계층 보안)는 TLS 프로토콜(RFC 2246)을 기반으로 하는 IEEE 802.1X EAP 인증 알고리즘입니다. TLS는 X.509 디지털 인증서를 기반으로 상호 인증 방법을 사용합니다. EAP-TLS 메시지 교환은 상호 인증, 암호 세트 협상, 키 교환, 클라이언트 및 인증 서버 간 확인 및 트래픽 암호화에 사용할 수 있는 키 요소를 제공합니다.

아래 목록에서는 EAP-TLS 클라이언트 인증서가 유선 및 무선 연결에 대한 강력한 인증을 제공할 수 있는 주된 원인을 보여줍니다.

- 인증은 주로 사용자에 의한 간섭 없이 자동으로 발생합니다.
- 사용자 비밀번호에 대한 종속성이 없습니다.
- 디지털 인증서가 강력한 인증 보호 기능을 제공합니다.
- 메시지 교환이 공개 키 암호화로 보호됩니다.
- 인증서가 사전 공격(Dictionary Attack)에 취약하지 않습니다.
- 인증 과정을 통해 데이터 암호화 및 서명의 키가 상호 결정됩니다.

EAP-TLS에는 2가지 옵션이 포함되어 있습니다.

- 서버 인증서 확인 - 서버 인증서 검증을 활성화합니다.
- 빠른 재연결 활성화 - TLS 세션 재개를 활성화하여 클라이언트 및 서버에 TLS 세션 데이터가 보존되어 있는 한 축약된 TSL 핸드셰이크를 사용하여 훨씬 더 빠르게 재인증할 수 있습니다.

참고 Disable When Using a Smart Card(스마트카드 사용 시 비활성화) 옵션은 머신 연결 인증에 사용할 수 없습니다.

EAP-TTLS

EAP-TTLS(EAP-Tunneled Transport Layer Security, EAP 터널링 전송 계층 보안)는 EAP-TLS 기능을 확장하는 2단계 프로토콜입니다. 1단계에서는 완전한 TLS 세션을 시행하고 2단계에서 사용되는 세션 키를 유도하여 서버와 클라이언트 간에 특성을 안전하게 터널링합니다. 2단계 도중 터널링된 특성을 사용하면 다양한 메커니즘을 사용하여 추가로 인증할 수 있습니다.

Network Access Manager는 EAP-TTLS 인증 시 사용된 내부 및 외부 방법의 암호화 바인딩을 지원하지 않습니다. 암호화 바인딩이 필요한 경우 EAP-FAST를 사용해야 합니다. 암호화 바인딩은 공격자가 자격 증명 정보를 모르는 상태에서 사용자의 연결을 가로채는 중간자 공격(Man-in-the-Middle Attack)의 특수 클래스로부터 보호합니다.

2단계에서 사용할 수 있는 인증 메커니즘에는 다음과 같은 프로토콜이 포함되어 있습니다.

- PAP(Password Authentication Protocol, 비밀번호 인증 프로토콜) - ID를 증명하기 위해 피어에 간단한 방법을 제공하는 양방향 핸드셰이크를 사용합니다. 인증이 승인되거나 실패할 때까지 ID/비밀번호 쌍은 피어에 의해 인증자에게 반복적으로 전달됩니다. 상호 인증이 필요한 경우에는 1단계에서 서버 인증서를 확인하도록 EAP-TTLS를 구성해야 합니다.

  비밀번호가 인증자에게 전달되었으므로 해시된 비밀번호를 사용하여 데이터베이스에 대한 인증 시 해당 프로토콜을 사용할 수 있습니다. 데이터베이스 누출의 가능성이 있는 경우 이 방법을 사용하는 것이 좋습니다.

  참고 토큰 및 OTP 기반 인증을 위해 EAP-TTLS PAP를 사용할 수 있습니다.

- CHAP(Challenge Handshake Authentication Protocol, 챌린지 핸드셰이크 인증 프로토콜) - 해당 피어의 ID를 검증하기 위해 3방향 핸드셰이크를 사용합니다. 상호 인증이 필요한 경우 1단계에서 서버 인증서를 확인하도록 EAP-TTLS를 구성해야 합니다. 이 시도 응답 방법을 사용하여 인증자의 데이터베이스에 암호화되지 않은 텍스트 비밀번호를 저장해야 합니다.
- MS-CHAP(Microsoft CHAP) - 해당 피어의 ID를 검증하기 위해 3방향 핸드셰이크를 사용합니다. 상호 인증이 필요한 경우 1단계에서 서버 인증서를 확인하도록 EAP-TTLS를 구성해야 합니다. 비밀번호의 NT 해시를 기반으로 이러한 시도 응답 방법을 사용하려면 인증자 데이터베이스에 암호화되지 않은 텍스트 비밀번호 또는 최소한 비밀번호의 NT 해시를 저장해야 합니다.
- MS-CHAPv2 - 응답 패킷의 피어 시도와 성공 패킷의 인증자 응답을 포함하여 피어 간의 상호 인증을 제공합니다. 클라이언트는 서버보다 먼저 인증됩니다. 사전 공격(Dictionary Attack)을 막기 위해 클라이언트보다 먼저 서버를 인증해야 하는 경우 1단계에서 서버의 인증서를 확인하도록 EAP-TTLS를 구성해야 합니다. 비밀번호의 NT 해시를 기반으로 이러한 시도 응답 방법을 사용하려면 인증자 데이터베이스에 암호화되지 않은 텍스트 비밀번호 또는 최소한 비밀번호의 NT 해시를 저장해야 합니다.

EAP-TTLS 구성

- EAP — 다음 EAP 방법 중 하나를 사용할 수 있습니다.
  - EAP-MD5(EAP Message Digest 5) — 피어의 ID를 확인하기 위해 3방향 핸드셰이크를 사용합니다(CHAP와 유사). 이 시도 응답 방법을 사용하는 경우 인증자의 데이터베이스에서 암호화되지 않은 텍스트 비밀번호를 저장해야 합니다.
  - EAP-MSCHAPv2 — 피어의 ID를 확인하기 위해 3방향 핸드셰이크를 사용합니다. 클라이언트는 서버보다 먼저 인증됩니다. 사전 공격(Dictionary Attack) 방지 등을 위해 서버를 클라이언트보다 먼저 인증해야 하는 경우, 1단계에서 서버 인증서를 확인하도록 EAP-TTLS를 구성해야 합니다. 비밀번호의 NT 해시에서 이 시도 응답 방법을 사용하는 경우 사용자는 암호화되지 않은 텍스트 비밀번호 또는 최소한 비밀번호의 NT 해시 중 하나를 인증자의 데이터베이스에 저장해야 합니다.
- EAP-TTLS 설정
  - 서버 ID 확인 — 서버 인증서 검증을 활성화합니다.

    참고 이 옵션을 활성화한 경우 RADIUS 서버에 설치된 서버 인증서에 서버 인증의 EKU(Extended Key Usage, 확장 키 사용)가 포함되었는지 확인하십시오. RADIUS 서버가 인증 중에 구성한 인증서를 클라이언트에 전송하는 경우, 인증서에는 네트워크 액세스 및 인증을 위한 이 서버 인증 설정이 포함되어야 합니다.
  - 빠른 재연결 활성화 — 내부 인증을 건너뛸지 또는 인증자가 제어하는지 관계 없이 외부 TLS 세션 재개만 활성화합니다.

    참고 Disable When Using a Smart Card(스마트카드 사용 시 비활성화)는 머신 연결 인증에서 사용할 수 없습니다.
- 내부 방법 — TLS 터널이 생성된 후에 사용되는 내부 방법을 지정합니다. Wi-Fi 미디어 유형에만 사용할 수 있습니다.

PEAP 옵션

PEAP(Protected EAP, 보호된 EAP)는 터널링 TLS 기반의 EAP 방법입니다. 내부 인증 방법의 암호화를 위해 클라이언트 인증 전 서버 인증에 TLS를 사용합니다. 내부 인증은 신뢰할 수 있는 암호로 보호된 터널 내부에서 발생하고 인증서, 토큰 및 비밀번호를 포함하여 여러 다른 내부 인증 방법을 지원합니다. Network Access Manager는 PEAP 인증 도중 사용된 내부 및 외부 방법의 암호화 바인딩을 지원하지 않습니다. 암호화 바인딩이 필요한 경우 EAP-FAST를 사용해야 합니다. 암호화 바인딩은 공격자가 자격 증명 정보를 모르는 상태에서 사용자의 연결을 가로채는 중간자 공격(Man-in-the-Middle Attack)의 특수 클래스로부터 보호합니다.

PEAP는 다음과 같은 서비스를 제공하여 EAP 방법을 보호합니다.

- EAP 패킷에 대한 TLS 터널 생성
- 메시지 인증
- 메시지 암호화
- 클라이언트에 대한 서버 인증

다음과 같은 인증 방법을 사용할 수 있습니다.

- 비밀번호를 사용하여 인증
  - EAP-MSCHAPv2 — 피어의 ID를 확인하기 위해 3방향 핸드셰이크를 사용합니다. 클라이언트는 서버보다 먼저 인증됩니다. 사전 공격(Dictionary Attack) 방지 등을 위해 클라이언트보다 먼저 서버를 인증해야 하는 경우, 서버의 인증서를 확인하도록 PEAP를 구성해야 합니다. 비밀번호의 NT 해시를 기반으로 시도 응답 방법을 사용하려면 인증자 데이터베이스에 암호화되지 않은 텍스트 비밀번호 또는 최소한 비밀번호의 NT 해시를 저장해야 합니다.
  - EAP-GTC(EAP Generic Token Card, 일반 토큰 카드) — 사용자 이름 및 비밀번호를 전달하는 EAP 봉투를 정의합니다. 상호 인증이 필요한 경우 서버의 인증서를 확인하도록 PEAP를 구성해야 합니다. 비밀번호가 인증자에게 암호화되지 않은 텍스트로 전달되므로 해시된 비밀번호가 있는 데이터베이스에 대한 인증을 위해 이 프로토콜을 사용할 수 있습니다. 데이터베이스 누출의 가능성이 있는 경우 이 방법을 사용하는 것이 좋습니다.
- 인증서를 사용하는 EAP-TLS
  - EAP-TLS — 사용자 인증서를 전달하는 EAP 봉투를 정의합니다. 중간자 공격(유효한 사용자의 연결 가로채기)을 방지하려면 같은 인증자에 대한 인증을 위해 PEAP(EAP-TLS)와 EAP-TLS 프로파일을 혼용하지 않는 것이 좋습니다. 이에 따라 적절하게 인증자를 구성해야 합니다(일반 및 터널링된 EAP-TLS를 모두 활성화 안 함).

PEAP 구성

- PEAP-EAP 설정
  - 서버 ID 확인 — 서버 인증서 검증을 활성화합니다.

참고 이 옵션을 활성화한 경우 RADIUS 서버에 설치된 서버 인증서에 서버 인증의 EKU(Extended Key Usage, 확장 키 사용)가 포함되었는지 확인하십시오. RADIUS 서버가 인증 중에 구성한 인증서를 클라이언트에 전송하는 경우, 인증서에는 네트워크 액세스 및 인증을 위한 이 서버 인증 설정이 포함되어야 합니다.

  - 빠른 재연결 활성화 — 외부 TLS 세션 재개만 활성화합니다. 인증자는 내부 인증을 건너뛸지 여부를 제어합니다.

- 스마트카드 사용 시 비활성화 — 인증을 위해 스마트카드를 사용할 경우 빠른 재연결을 사용하지 않습니다. 스마트카드는 사용자 연결에만 적용됩니다.
- 토큰 및 EAP GTC를 사용하여 인증 — 머신 인증에 사용할 수 없습니다.

- 자격 증명 소스를 기반으로 하는 내부 방법
  - EAP-MSCHAPv2 및/또는 EAP-GTC용 비밀번호를 사용하여 인증합니다.
  - EAP-TLS의 경우 인증서를 사용하여 인증합니다.
  - 토큰 및 EAP-GTC를 사용하여 인증 — 머신 인증에 사용할 수 없습니다.

참고 사용자가 로그온하기 전에 Windows에서 스마트카드 지원을 사용할 수 없습니다.

EAP-FAST 설정

EAP-FAST는 유연하고 간편한 구축과 관리를 제공하는 IEEE 802.1X 인증 유형으로 다양한 사용자 및 비밀번호 데이터베이스 유형, 서버에서 시작하는 비밀번호 만료와 변경 및 디지털 인증서(선택 사항)를 지원합니다.

EAP-FAST는 인증서를 사용하지 않고 사전 공격(Dictionary Attack)으로부터 보호를 제공하는 IEEE 802.1X EAP 유형을 구축하려는 고객을 위해 개발되었습니다.

AnyConnect 3.1부터는 머신 및 사용자 연결을 구성할 때 EAP 체이닝이 지원됩니다. 즉 Network Access Manager에서 머신과 사용자가 알려진 엔터티이며 기업에서 관리하고 있는지 확인함을 의미하므로 기업 네트워크에 연결된 사용자 소유의 자산을 관리하는 데 유용합니다. EAP 체이닝에 대한 자세한 내용은 RFC 3748을 참조하십시오.

EAP-FAST는 TLS 메시지를 EAP 내에서 캡슐화하며 다음과 같이 3가지 프로토콜 단계로 구성되어 있습니다.

1. 프로비저닝 단계에서는 ADHP(Authenticated Diffie-Hellman Protocol)를 사용하여 PAC(Protected Access Credential)라는 공유 보안 자격 증명을 통해 클라이언트를 프로비저닝합니다.
2. 터널 설정 단계에서는 터널을 설정하기 위해 PAC를 사용합니다.
3. 인증 단계에서는 인증 서버가 사용자의 자격 증명(토큰, 사용자 이름/비밀번호 또는 디지털 인증서)을 인증합니다.

다른 터널링 EAP 방법과 달리 EAP-FAST는 내부 및 외부 방법 간에 암호화 바인딩을 제공하여 공격자가 유효한 사용자 연결을 가로채는 중간자 공격(Man-in-the-Middle Attack)의 특수 클래스를 방지합니다.

EAP-FAST 구성

- EAP-FAST 설정

- 서버 ID 확인 — 서버 인증서 검증을 활성화합니다. 이 옵션을 활성화하면 관리 유틸리티에 2개의 추가 대화 상자가 생성되고 Network Access Manager 프로파일 편집기 작업 목록에 추가 인증서 창이 추가됩니다.

  참고 이 옵션을 활성화한 경우 RADIUS 서버에 설치된 서버 인증서에 서버 인증의 EKU(Extended Key Usage, 확장 키 사용)가 포함되었는지 확인하십시오. RADIUS 서버가 인증 중에 구성한 인증서를 클라이언트에 전송하는 경우, 인증서에는 네트워크 액세스 및 인증을 위한 이 서버 인증 설정이 포함되어야 합니다.

- 빠른 재연결 활성화 — 세션 재개를 활성화합니다. EAP-FAST에서 인증 세션을 재개하는 2가지의 메커니즘은 내부 인증 및 TLS 세션 재개를 대체하는 사용자 권한 부여 PAC와 단축된 외부 TLS 핸드셰이크에 허용되는 TLS 세션 재개입니다. 빠른 재연결 활성화 매개변수는 두 가지 메커니즘을 모두 활성화 또는 비활성화합니다. 인증자가 사용할 메커니즘을 선택합니다.

  참고 머신 PAC는 단축된 TLS 핸드셰이크를 제공하고 내부 인증을 삭제합니다. 이 제어 기능은 PAC 매개변수 활성화/비활성화를 수행하여 처리됩니다.

  참고 Disable When Using a Smart Card(스마트카드 사용 시 비활성화) 옵션은 사용자 연결 권한 부여에만 사용할 수 있습니다.

- 자격 증명 소스 기반 내부 방법 — 비밀번호 또는 인증서를 사용하여 인증할 수 있습니다.
  - EAP-MSCHAPv2 또는 EAP-GTC용 비밀번호를 사용하여 인증합니다. EAP-MSCHAPv2는 상호 인증을 제공하지만 서버를 인증하기 전에 클라이언트를 인증합니다. 먼저 인증된 서버와 상호 인증을 수행하려면 인증된 프로비저닝 전용으로 EAP-FAST를 구성하고 서버 인증서를 확인합니다. 비밀번호의 NT 해시에 기반하여 시도 응답 방법을 사용하는 경우 EAP-MSCHAPv2는 사용자에게 암호화되지 않은 텍스트 비밀번호 또는 최소한 비밀번호의 NT 해시 중 하나를 인증자의 데이터베이스에 저장하도록 요청합니다. 비밀번호가 EAP-GTC 내에서 암호화되지 않은 텍스트로 인증자에게 전달되므로 데이터베이스에 대한 인증을 위해 이 프로토콜을 사용할 수 있습니다.
  - 비밀번호 기반 내부 방법을 사용하는 경우, 인증되지 않은 PAC 프로비저닝을 허용하기 위해 추가 옵션을 사용할 수 있습니다.
  - 인증서를 사용하여 인증 — 인증서를 사용하여 인증하기 위해 다음 기준을 결정합니다. 요청 시 클라이언트 인증서를 암호화되지 않은 텍스트로 전송하고 터널 내부에 있는 클라이언트 인증서만 전송하거나 터널에서 EAP TLS를 사용하여 클라이언트 인증서를 전송합니다.
  - 토큰 및 EAP-GTC를 사용하여 인증합니다.

- PAC 사용 — EAP-FAST 인증에 PAC를 사용하도록 지정할 수 있습니다. PAC는 최적화된 네트워크 인증을 위해 클라이언트에 배포된 자격 증명입니다.

참고 일반적으로 대부분의 인증 서버에서 EAP-FAST에 대해 PAC를 사용하기 때문에 PAC 옵션을 사용합니다. 이 옵션을 제거하기 전에 인증 서버가 EAP-FAST에 대해 PAC를 사용하지 않는지 확인하고 그렇지 않은 경우 클라이언트의 인증 시도가 실패합니다. 인증 서버가 인증된 PAC 프로비저닝을 지원하는 경우 Cisco에서는 인증되지 않은 프로비저닝을 비활성화할 것을 권장합니다. 인증되지 않은 프로비저닝은 서버 인증서를 확인하지 않으며 침입자가 사전 기반 공격을 마운트하도록 활성화할 수 있습니다.

LEAP 설정

LEAP(Lightweight EAP)는 무선 네트워크를 지원합니다. EAC(Extensible Authentication Protocol, 확장 가능 인증 프로토콜) 프레임워크를 기반으로 하며 Cisco에서 WEP보다 보안이 강력한 프로토콜을 만들기 위해 개발되었습니다.

참고 강력한 비밀번호를 적용하고 정기적으로 비밀번호를 만료하지 않으면 LEAP가 사전 공격(Dictionary Attack)의 대상이 됩니다. Cisco에서는 인증 방법이 사전 공격에 취약하지 않은 EAP-FAST, PEAP 또는 EAP-TLS의 사용을 권장합니다.

LEAP 설정은 사용자 인증에 대해서만 사용할 수 있습니다.

- 로그 오프 후 사용자 연결 확장 - 사용자가 로그 오프해도 연결된 상태를 유지합니다. 같은 사용자가 다시 로그온하는 경우 네트워크 연결이 계속 활성화됩니다.

자세한 내용은 Cisco LEAP 사전 공격 취약점 을 참조하십시오.

네트워크 자격 증명 정의

Networks(네트워크) > Credentials(자격 증명) 창에서 사용자 및/또는 머신 자격 증명을 사용할지 지정하고 신뢰할 수 있는 서버 검증 규칙을 구성하십시오.

사용자 자격 증명 구성

EAP 대화에 두 개 이상의 EAP 인증 방법이 포함될 수 있으며 해당 인증 각각에 대해 요청되는 ID는 다를 수 있습니다(예: 머신 인증 후 사용자 인증). 예를 들어 피어는 nouser@cisco.com의 ID가 인증 요청을 cisco.com EAP 서버로 라우팅하도록 처음에 요청할 수 있습니다. 하지만 TLS 세션이 협상되면 피어가 johndoe@cisco.com의 ID를 요청할 수 있습니다. 따라서 사용자의 ID를 통해 보호 기능이 제공되는 경우에도 로컬 인증 서버에서 대화가 종료되지 않는 한 대상 영역이 반드시 일치할 필요는 없습니다.

사용자 연결의 경우 [username] 및 [domain] 자리 표시자 패턴을 사용하면 다음 조건이 적용됩니다.

- 클라이언트 인증서가 인증에 사용되는 경우 — 다양한 X509 인증서 속성에서 [username] 및 [password]에 대한 자리 표시자 값을 가져옵니다. 속성은 첫 번째 일치 항목에 따라 아래 설명된 순서대로 분석됩니다. 예를 들어, ID가 사용자 인증용으로 userA@example.com(username=userA 및 domain=example.com)이며 머신 인증용으로 hostA.example.com(username=hostA 및 domain=example.com)인 경우, 다음 속성이 분석됩니다.
- 사용자 인증서 기반 인증의 경우:
  - SubjectAlternativeName: UPN = userA@example.com
  - Subject = .../CN=userA@example.com/...
  - Subject = userA@eample.com
  - Subject = .../CN=userA/DC=example/DC=com/...
  - Subject = userA(도메인 없음)
- 머신 인증서 기반 인증의 경우:
  - SubjectAlternativeName: DNS = hostA.example.com
  - Subject = .../DC=hostA.example.com/...
  - Subject = .../CN=hostA.example.com/...
  - Subject = hostA.example.com
- 자격 증명 소스가 최종 사용자인 경우 — 사용자가 입력하는 정보에서 자리 표시자 값을 가져옵니다.
- 자격 증명을 운영 체제에서 가져온 경우 — 로그온 정보에서 자리 표시자 값을 가져옵니다.
- 정적 자격 증명인 경우 — 자리 표시자를 사용하지 않습니다.

자격 증명 창에서 연계된 네트워크 인증에 필요한 자격 증명을 지정할 수 있습니다.

프로시저

단계 **1** 보호된 ID 패턴에 대해 사용자 ID를 정의합니다. Network Access Manager가 다음의 ID 자리 표시자 패턴을 지원합니다.

- [username] — 사용자 이름을 지정합니다. 사용자가 username@domain 또는 domain\username을 입력할 경우 이 도메인 부분이 제거됩니다.
- [raw] — 사용자가 입력한 대로 정확하게 사용자 이름을 지정합니다.
- [domain] — 사용자 디바이스의 도메인을 지정합니다.

단계 **2** 보호되지 않는 일반적인 ID 패턴을 지정합니다.

협상해야 할 세션은 ID 요청을 받고 무결성 보호 또는 인증 없이 암호화되지 않은 상태에서 응답합니다. 이 세션은 스누핑 및 패킷 수정의 영향을 받습니다.

- anonymous@[domain] — 값이 암호화되지 않은 텍스트로 전송될 경우 사용자 ID를 숨기기 위해 터널링된 방법에서 자주 사용됩니다. 실제 사용자 ID는 보호되는 ID로 내부 방법에서 제공됩니다.
- [username]@[domain] — 터널링되지 않은 방법에서 사용됩니다.

  참고 보호되지 않는 ID 정보가 암호화되지 않은 텍스트로 전송됩니다. 초기의 암호화되지 않은 텍스트 ID 요청 또는 응답이 손상된 경우 서버는 TLS 세션이 한 번 설정되면 ID를 확인할 수 없다는 사실을 발견합니다. 예를 들어 사용자 ID는 유효하지 않거나 EAP 서버에서 처리하는 영역 내에 있지 않을 수 있습니다.

단계 **3** 보호 ID 패턴을 지정합니다.

스누핑으로부터 사용자 ID를 보호하기 위해 암호화되지 않은 텍스트 ID가 올바른 영역에 대한 인증 요청 라우팅을 사용하는 데 필요한 정보만 제공할 수 있습니다.

- [username]@[domain]
- 사용자 ID(자리 표시자 없음)로 사용할 실제 문자열

단계 **4** 다음과 같이 추가 사용자 자격 증명 정보를 제공합니다.

- 단일 로그인 자격 증명 사용 — 운영 체제의 로그온 정보에서 자격 증명을 가져옵니다. 로그온 자격 증명이 실패할 경우 Network Access Manager가 일시적으로(다음 로그온 시까지) 사용자를 전환하고 GUI를 사용하여 사용자에게 자격 증명을 입력하라는 프롬프트를 표시합니다.

  참고 Network Access Manager 및 SSO와 함께 Windows 로그인 크리덴셜을 자동으로 사용할 수는 없습니다. Network Access Manager와 함께 SSO를 사용하려면 로그온 크리덴셜을 가로채야 합니다. 따라서 설치 또는 로그오프 후에 리부팅해야 한다는 프롬프트가 표시됩니다.

- 정적 자격 증명 사용 - 이 프로파일 편집기가 제공하는 네트워크 프로파일에서 사용자 자격 증명을 가져옵니다. 정적 자격 증명이 실패할 경우 Network Access Manager는 새 구성이 로드될 때까지 이 자격 증명을 다시 사용하지 않습니다.

  참고 이 필드에는 앰퍼샌드 문자를 사용할 수 없습니다.

- 자격 증명용 프롬프트 - 다음에 지정된 대로 AnyConnect GUI를 사용하여 최종 사용자로부터 자격 증명을 가져옵니다.
  - 영구 기억 - 이 자격 증명이 영구 기억됩니다. 기억된 자격 증명이 실패할 경우, 자격 증명을 다시 입력하라는 프롬프트가 표시됩니다. 자격 증명은 파일로 보관되고 로컬 머신 비밀번호를 사용하여 암호화됩니다.
  - 사용자 로그온 동안 기억 — 사용자가 로그오프할 때까지 자격 증명을 기억합니다. 기억된 자격 증명이 실패할 경우, 사용자에게 자격 증명을 다시 입력하라는 프롬프트가 표시됩니다.

- 기억 안 함 — 자격 증명을 기억하지 않습니다. Network Access Manager는 인증을 위해 자격 증명 정보가 필요할 때마다 사용자에게 프롬프트를 표시합니다.

단계 **5** 인증서가 필요할 경우 인증에 사용할 인증서 소스를 결정합니다.

- 스마트카드 또는 OS 인증서 — Network Access Manager는 OS 인증서 저장소 또는 스마트카드에 있는 인증서를 사용합니다.
- 스마트카드 인증서 전용 — Network Access Manager는 스마트카드에 있는 인증서만 사용합니다.

단계 **6** 스마트카드 PIN 기억 파라미터에서 Network Access Manager가 스마트카드에서 인증서를 검색하는 데 사용한 PIN을 얼마나 오래 기억할지 결정합니다. 사용 가능한 옵션에 대해서는 2단계를 참조하십시오.

참고 PIN은 인증서보다 오래 보관되지 않습니다.

일부 스마트카드는 스마트카드 칩과 드라이버에 따라 다른 방법에 비해 연결하는 데 시간이 오래 걸릴 수 있으며 CSP(Cryptographic Service Provider, 암호화 서비스 공급자) 및 KSP(Key Storage Provider, 주요 스토리지 공급자)라고도 합니다. 연결 시간 제한을 늘리면 네트워크에서 스마트카드 기반 인증을 수행하는 데 충분한 시간을 제공할 수 있습니다.

머신 자격 증명 구성

EAP 대화에 두 개 이상의 EAP 인증 방법이 포함될 수 있으며 해당 인증 각각에 대해 요청되는 ID는 다를 수 있습니다(예: 머신 인증 후 사용자 인증). 예를 들어 피어는 nouser@example.com의 ID가 인증 요청을 cisco.com EAP 서버로 라우팅하도록 처음에 요청할 수 있습니다. 하지만 TLS 세션이 협상되면 피어가 johndoe@example.com의 ID를 요청할 수 있습니다. 따라서 사용자의 ID를 통해 보호 기능이 제공되는 경우에도 로컬 인증 서버에서 대화가 종료되지 않는 한 대상 영역이 반드시 일치할 필요는 없습니다.

머신 연결의 경우 [username] 및 [domain] 자리 표시자를 사용하면 다음 조건이 적용됩니다.

- 클라이언트 인증서가 인증에 사용되는 경우 — 다양한 X509 인증서 속성에서 [username] 및 [password]에 대한 자리 표시자 값을 가져옵니다. 속성은 첫 번째 일치 항목에 따라 아래 설명된 순서대로 분석됩니다. 예를 들어, ID가 사용자 인증용으로 userA@cisco.com(username=userA 및 domain=cisco.com)이며 머신 인증용으로 hostA.cisco.com(username=hostA 및 domain=cisco.com)인 경우, 다음 속성이 분석됩니다.
- 사용자 인증서 기반 인증의 경우:
  - SubjectAlternativeName: UPN = userA@example.com
  - Subject = .../CN=userA@example.com/...
  - Subject = userA@example.com
  - Subject = .../CN=userA/DC=example.com/...
  - Subject = userA(도메인 없음)

- 머신 인증서 기반 인증의 경우:
  - SubjectAlternativeName: DNS = hostA.example.com
  - Subject = .../DC=hostA.example.com/...
  - Subject = .../CN=hostA.example.com/...
  - Subject = hostA.example.com
- 클라이언트 인증서가 인증에 사용되지 않는 경우 — 운영 체제에서 자격 증명을 가져옵니다. 이때 [username] 자리 표시자는 할당된 머신 이름을 나타냅니다.

자격 증명 패널에서 원하는 머신 자격 증명을 지정할 수 있습니다.

프로시저

단계 **1** 보호된 ID 패턴에 대해 머신 ID를 정의합니다. Network Access Manager가 다음의 ID 자리 표시자 패턴을 지원합니다.

- [username] — 사용자 이름을 지정합니다. 사용자가 username@domain 또는 domain\username을 입력할 경우, 이 도메인 부분이 제거됩니다.
- [raw] — 사용자가 입력한 대로 정확하게 사용자 이름을 지정합니다.
- [domain] — 사용자 PC의 도메인을 지정합니다.

단계 **2** 일반적인 보호되지 않는 머신 ID 패턴을 정의합니다.

협상해야 할 세션은 ID 요청을 받고 무결성 보호 또는 인증 없이 암호화되지 않은 상태에서 응답합니다. 이 세션은 스누핑 및 패킷 수정의 영향을 받습니다.

- host/anonymous@[domain]
- 머신 ID(자리 표시자 없음)로 전송할 실제 문자열

단계 **3** 보호되는 머신 ID 패턴을 정의합니다.

스누핑으로부터 사용자 ID를 보호하기 위해 암호화되지 않은 텍스트 ID가 올바른 영역에 대한 인증 요청 라우팅을 사용하는 데 필요한 정보만 제공할 수 있습니다. 일반적으로 보호되는 머신 ID 패턴은 다음과 같습니다.

- host/[username]@[domain]
- 머신 ID(자리 표시자 없음)로 사용할 실제 문자열

단계 **4** 다음과 같이 추가 머신 자격 증명 정보를 제공합니다.

- 머신 자격 증명 사용 — 운영 체제에서 자격 증명을 가져옵니다.

- 정적 자격 증명 사용 — 구축 파일로 전송할 실제 정적 비밀번호를 지정합니다. 정적 자격 증명은 인증서 기반 인증에 적용되지 않습니다.

올바른 인증서를 선택하도록 *Network Access Manager* 설정

클라이언트 인증 중에 인증서가 두 개 있으면 Network Access Manager는 인증서 속성을 기준으로 하여 최적의 인증서를 자동으로 선택합니다. 기본 설정 인증서의 기준은 고객별로 다르므로 다음 필드를 구성하여 인증서 선택을 확인하고 인증서 선택을 재정의하는 데 사용하려는 규칙을 제공해야 합니다.

여러 인증서가 같은 규칙과 일치하거나 규칙과 일치하는 인증서가 없는 경우 ACE 엔진은 인증서 우선순위를 지정하는 알고리즘을 통해 실행되어 특정 기준에 따라 인증서 하나를 선택합니다. 이러한 기준으로는 인증서에 개인 키가 있는지 여부, 인증서가 머신 저장소의 인증서인지 여부 등이 있습니다. 여러 인증서의 우선순위가 같은 경우 ACE 엔진은 해당 우선순위 내에서 처음으로 발견하는 인증서를 선택합니다.

프로시저

단계 **1** AnyConnect 프로파일 편집기에서 **Networks(**네트워크**)** 탭을 선택합니다.

단계 **2** 편집할 네트워크를 선택합니다.

단계 **3** **Machine Credentials(**머신 크리덴셜**)** 탭을 선택합니다.

단계 **4** 페이지 하단에서 **Use Certificate Matching Rule(**인증서 일치 규칙 사용**)**을 선택합니다.

단계 **5** Certificate Field(인증서 필드) 드롭다운 메뉴에서 검색 기준에 사용할 필드를 선택합니다.

단계 **6** Match(일치) 드롭다운 메뉴에서 검색에 해당 필드와 정확히 일치하는 항목을 포함할지(Equals(같음) 선택) 아니면 필드의 일부분이 일치하는 항목을 포함할지(Includes(포함) 선택)를 결정합니다.

단계 **7** Value(값) 필드에 인증서 검색 기준을 입력합니다.

신뢰할 수 있는 서버 검증 규칙 구성

Validate Server Identity(서버 ID 확인) 옵션이 EAP 방법용으로 구성된 경우, 인증서 패널은 인증서 서버 또는 기관에 대한 검증 규칙을 구성할 수 있도록 활성화됩니다. 검증 규칙 결과에 따라 인증서 서버 또는 기관을 신뢰할 수 있는지 결정됩니다.

인증서 서버 검증 규칙을 정의하려면 다음 단계를 따르십시오.

프로시저

단계 **1** **Certificate Field(**인증서 필드**)** 및 **Match(**일치**)** 열에 대해 선택 가능한 설정이 나타나는 경우, 드롭다운 화살표를 클릭하고 원하는 설정을 선택합니다.

단계 **2** Value(값) 필드에 값을 입력합니다.

단계 **3** 규칙 아래에서 **Add(**추가**)**를 클릭합니다.

단계 **4** Certificate Trusted Authority(인증서 신뢰 기관) 창에서 다음 옵션 중 하나를 선택하십시오.

- OS에 설치된 모든 루트 CA(Certificate Authority, 인증 기관) 신뢰 — 이 옵션을 선택한 경우, 로컬 머신 또는 인증서 저장소만 서버 인증서 체인 검증에 고려됩니다.
- 루트 CA(Certificate Authority, 인증 기관) 인증서 포함

  참고 루트 CA(Certificate Authority, 인증 기관) 인증서 포함 옵션을 선택한 경우, **Add(**추가**)**를 클릭하여 CA 인증서를 구성에 가져오십시오. Windows 인증서 저장소에서 내보낸 인증서를 사용 중인 경우에는 "Base 64 encoded X.509 (.cer)(Base 64로 인코딩된 X.509(.cer))" 옵션을 사용합니다.

네트워크 그룹 창

Network Groups(네트워크 그룹) 창에서는 특정 그룹에 네트워크 연결을 할당합니다. 연결을 그룹으로 분류하면 다음과 같은 여러 장점이 있습니다.

- 연결을 시도할 때 사용자 환경이 향상됩니다. 여러 개의 숨겨진 네트워크가 구성되면 클라이언트는 성공적으로 연결할 때까지 정의된 순서대로 숨겨진 네트워크의 목록을 확인합니다. 이 같은 경우 그룹은 연결에 필요한 시간을 크게 줄이는 데 사용됩니다.
- 구성된 연결을 더욱 쉽게 관리할 수 있습니다. 한 회사에서 여러 역할을 하거나 같은 영역을 자주 방문하는 사용자가 선택 가능한 네트워크의 목록을 더욱 쉽게 관리할 수 있도록 네트워크를 그룹으로 조정하려는 경우 사용자의 네트워크에서 관리자 네트워크를 분리할 수 있습니다.

배포 패키지의 일부로 정의된 네트워크는 잠겨 있어 사용자가 구성 설정을 편집하거나 네트워크 프로파일을 제거하는 것을 방지합니다.

네트워크를 전체적으로 정의할 수 있습니다. 이렇게 할 경우 네트워크는 전역 네트워크 섹션에 표시됩니다. 이 섹션은 유선 및 무선 네트워크 유형으로 나누어집니다. 이러한 유형의 네트워크에서는 정렬 순서 편집만 수행할 수 있습니다.

모든 비전역 네트워크는 그룹으로 존재해야 합니다. 기본적으로 한 개의 그룹이 생성되며 모든 네트워크가 전역 상태인 경우 사용자는 해당 그룹을 삭제할 수 있습니다.

프로시저

단계 **1** 드롭다운 목록에서 그룹을 선택하십시오.

단계 **2** 최종 사용자가 해당 그룹에서 네트워크를 생성할 수 있도록 허용하려면 **Create networks(**네트워크 생성**)** 를 선택하십시오. 구축된 경우 이를 선택하지 않으면 Network Access Manager가 해당 그룹에서 사용자가 생성한 네트워크를 삭제합니다. 이로 인해 사용자는 다른 그룹에서 네트워크 구성을 다시 입력해야 할 수 있습니다.

단계 **3** 그룹이 AnyConnect GUI를 사용하여 활성 그룹으로 선택된 경우, 최종 사용자가 스캔 목록을 볼 수 있도록 허용하려면 **See scan list(**스캔 목록 보기**)** 를 선택하십시오. 또는 사용자가 스캔 목록을 보지 못

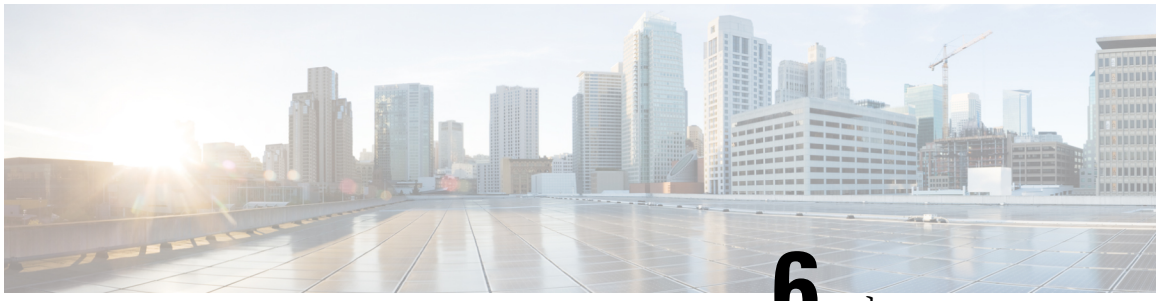
하게 제한하려면 확인란의 선택을 해제하십시오. 예를 들어 사용자가 주변 디바이스에 실수로 연결하는 것을 방지하려면 스캔 목록 액세스를 제한해야 합니다.

참고 해당 설정은 그룹별로 적용됩니다.

단계 **4** 그룹 드롭다운 목록에서 선택한 그룹의 네트워크를 삽입하고 제거하려면 오른쪽 화살표 및 왼쪽 화살표를 사용하십시오. 네트워크가 현재 그룹에서 이동할 경우, 기본 그룹에 위치하게 됩니다. 기본 그룹이 편집될 경우 기본 그룹에서 네트워크를 이동시킬 수 없습니다(> 버튼 사용).

참고 주어진 네트워크 내에서 각 네트워크의 표시 이름은 고유해야 합니다. 따라서 1개의 그룹에는 같은 표시 이름을 사용하는 2개 이상의 네트워크가 포함될 수 없습니다.

단계 **5** 그룹 내 네트워크의 우선순위를 변경하려면 위로 화살표 및 아래로 화살표를 사용하십시오.



6 장

포스처 구성

AnyConnect Secure Mobility Client는 VPN Posture(HostScan) 모듈 및 ISE Posture 모듈을 제공합니다. 이 두 모듈은 안티 바이러스, 안티스파이웨어, 호스트에 설치된 방화벽 소프트웨어 등에 대한 엔드포인트 규정 준수를 평가하는 기능을 Cisco AnyConnect Secure Mobility Client 에 제공합니다. 그런 다음 엔드포인트가 규정을 준수할 때까지 네트워크 액세스를 제한하거나 로컬 사용자 권한을 상승시켜 보안정책 교정 사례를 설정할 수 있습니다.

VPN Posture는 운영 체제, 안티 바이러스, 안티스파이웨어 및 호스트에 설치된 소프트웨어를 수집하는 애플리케이션인 hostscan_version.pkg와 함께 제공됩니다. ISE Posture는 AnyConnect 및 NAC 에이전트를 둘 다 구축하지 않고 ISE 통제 네트워크에 액세스할 때 클라이언트를 하나 구축합니다. ISE Posture는 AnyConnect 제품(웹 보안, network access manager 등과 유사)에 추가 보안 구성 요소로 설치하도록 선택할 수 있는 모듈입니다. 릴리스 3.x에서 AnyConnect 번들의 일부였던 HostScan은 현재 개별적으로 설치합니다.

ISE Posture는 클라이언트 측 평가를 실시합니다. 클라이언트는 헤드엔드에서 포스처 요건 정책을 수신하고 포스처 데이터 수집을 수행하며 결과를 정책과 비교하여 평가 결과를 헤드엔드에 전송합니다. ISE에서 엔드포인트의 규정 준수 여부를 실제로 결정하는 경우에도 정책에 대한 엔드포인트의 고유한 평가를 사용합니다.

반면 HostScan은 ASA가 엔드포인트 특성(운영 체제, IP 주소, 레지스트리 항목, 로컬 인증서, 파일 이름 등) 목록만 요청하는 경우 서버 측 평가를 실시하고 이 특성들은 HostScan에서 반환됩니다. 정책 평가에 대한 결과를 바탕으로 어떤 호스트가 보안 어플라이언스에 대해 원격 액세스 연결을 생성하도록 허용되는지 제어할 수 있습니다.

참고 HostScan 및 ISE Posture 에이전트는 함께 사용하지 않는 것이 좋습니다. 서로 다른 두 포스처 에이전트를 실행하면 예기치 않은 결과가 발생하기 때문입니다.

다음 포스처 확인은 HostScan에서 지원되지만 ISE Posture에서는 지원되지 않습니다.

- 호스트 이름
- IP 주소
- MAC 주소
- 포트 번호

- OPSWAT 버전
- BIOS 일련 번호
- 개인 방화벽
- 체크섬 유효성 검증을 통한 파일 검사
- 인증서 필드 특성

ISE Posture 모듈이 제공하는 기능

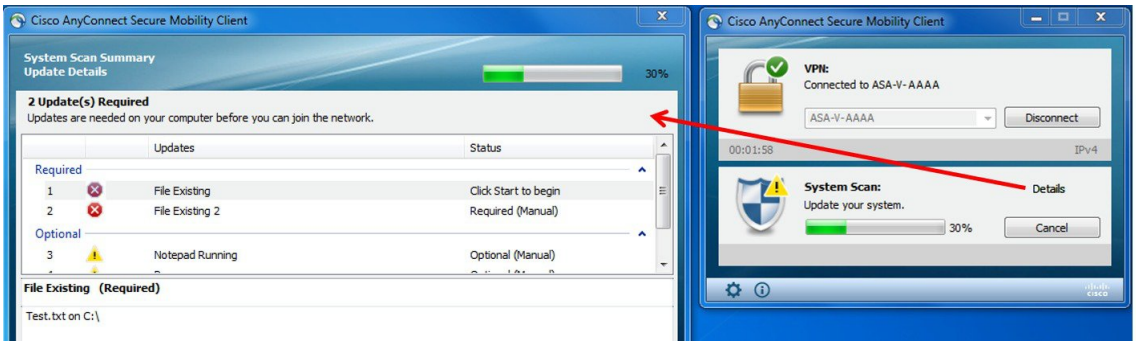
포스처 확인

ISE Posture 모듈은 포스처 확인을 수행하기 위해 OPSWAT v3 또는 v4 라이브러리를 사용합니다. 초기 포스처 확인에서는 모든 필수 요건을 충족하지 못한 엔드포인트를 비준수로 간주합니다. 다른 엔드포인트 승인 상태는 알 수 없는 포스처 또는 규정 준수(필수 요건 충족) 상태입니다.

포스처 확인 단계 도중 오류가 발생했으나 AnyConnect를 계속 실행할 수 있는 경우 사용자에게 통지되지만 가능하면 포스처 확인이 계속됩니다. 필수 포스처 확인 도중 오류가 발생하는 경우 확인이 실패로 표시됩니다. 모든 필수 요건이 충족하는 경우 네트워크 액세스 권한이 부여됩니다. 그렇지 않으면 사용자가 포스처 프로세스를 다시 시작할 수 있습니다.

필요한 보안정책 교정

보안정책 교정 창은 네트워크 활동의 업데이트가 팝업으로 표시되어 방해하거나 중단하지 않도록 배경에서 실행됩니다. AnyConnect UI의 ISE Posture 바둑판식 배열 부분에 있는 **Details(**세부사항**)**를 클릭하여 네트워크에 연결하기 전에 탐지된 항목과 필요한 업데이트를 확인할 수 있습니다. 수동 보안정책 교정이 필요한 경우 보안정책 교정 창이 열리고 작업이 필요한 항목이 표시됩니다. System Scan Summary: Update Details(시스템 스캔 요약: 업데이트 세부사항) 창은 업데이트 진행 상황, 할당된 업데이트 시간 중 남은 시간, 기타 요건의 상태 및 시스템 규정 준수 상태를 보여줍니다.



관리자는 ISE Posture 프로세스의 끝부분에서 네트워크 사용 정책을 구성할 수 있습니다. 정책에 액세스할 때 액세스 VLAN에 액세스 권한이 부여되기 전에 사용자가 동의해야 하는 필수 사용 약관을 볼 수 있습니다.

선택적 업데이트만 남은 경우 **Skip(**건너뛰기**)**을 선택하여 다음 질문으로 건너뛰거나 **Skip All(**모두 건너뛰기**)**을 선택하여 남아있는 모든 보안정책 교정을 무시할 수 있습니다. 시간상 선택적 보안정책 교정을 건너뛰더라도 네트워크 액세스를 계속 유지 관리할 수 있습니다.

보안정책 교정 이후(또는 요건에서 보안정책 교정이 필요하지 않은 시기를 확인한 이후) 사용 제한 정책 알림을 받을 수 있습니다. 또한 네트워크 액세스를 위한 정책에 동의해야 하며, 동의하지 않는 경우 액세스가 제한됩니다. 보안정책 교정의 이 부분에서 AnyConnect UI의 포스처 바둑판식 배열 부분에 "시스템 스캔: 네트워크 사용 제한 정책"이 표시됩니다.

보안정책 교정이 완료되면 업데이트가 필요한 목록에 있는 모든 확인란이 초록색 확인란에 완료 상태로 표시됩니다. 보안정책 교정 이후 에이전트가 ISE에 포스처 결과를 전송합니다.

참고 Symantec 제품의 아키텍처가 변경되어 ISE Posture는 Symantec AV 12.1.x 이상 버전의 치료를 지원할 수 없습니다.

패치 관리 검사 및 치료

AnyConnect 4.x와 Microsoft SCCM(System Center Configuration Manager)을 통합하면 패치 관리 검사 및 패치 관리 치료 기능이 제공됩니다. 이 기능은 엔드포인트에서 누락된 중요 패치 상태를 검사하여 소프트웨어 패치를 트리거해야 하는지를 확인합니다. Windows 엔드포인트에서 누락된 중요 패치가 없으면 패치 관리 검사에 통과하게 됩니다. 패치 관리 치료는 하나 이상의 중요 패치가 Windows 엔드포인트에서 누락된 경우에 한해 관리자 레벨 사용자에 대해서만 트리거됩니다.

SCCM 클라이언트가 패치를 설치할 때 해당 설치가 리부팅 전에 수행되면 SCCM 클라이언트는 머신이 리부팅되는 즉시 패치의 설치 상태(설치됨 또는 설치되지 않음)를 보고합니다. 그러나 SCCM 클라이언트가 패치를 설치할 때 해당 설치가 리부팅 후에 시작되는 경우 SCCM 클라이언트는 패치 상태를 즉시 보고하지 않습니다.

AnyConnect 컴플라이언스 모듈은 이 시점에서 SCCM 클라이언트에 대해 강제로 상태 제공을 요청할 수 없습니다. 패치에 따라 SCCM 클라이언트가 응답할 때까지 기다려야 할 수도 있지만 알려진 패치에 대한 대부분의 랩 결과에서는 약 10분 이내에 클라이언트가 응답하는 것으로 확인되었습니다.

WSUS(Windows Server Update Services) 검색 API의 경우에도 유사한 행동이 관찰되지만 응답 시간은 더 오래 걸립니다(경우에 따라 20~30분). Windows 업데이트에서는 Windows OS뿐만 아니라 Microsoft Office와 같은 모든 Microsoft 제품의 누락된 패치를 확인합니다.

ISE에 대해 정책 조건을 설정하는 방법을 알아보려면 정책 조건을 참조하십시오. 패치 관리 치료에 대한 추가 정보를 확인하려면 패치 관리 치료를 참조하십시오.

엔드포인트 규정 준수 재평가

엔드포인트가 규정을 준수하는 것으로 간주되고 네트워크 액세스 권한이 부여된 이후에는 관리자가 구성한 제어에 기반하여 엔드포인트를 선택에 따라 주기적으로 재평가할 수 있습니다. 수동 재평가 포스처 확인은 초기 포스처 확인과 다릅니다. 확인에 실패하면 관리자가 설정에 구성해둔 경우 사용자에게 수정 옵션이 제공됩니다. 구성 설정은 하나 이상의 필수 요건을 충족하지 않는 경우에도 사용자가 신뢰할 수 있는 네트워크 액세스를 유지하는지를 제어합니다. 초기 포스처 평가에서는 모든 필수 요건을 충족하지 못하면 엔드포인트를 비준수로 간주합니다. 이 기능은 기본적으로 비활성화로 설정되어 있으며 사용자 역할용으로 활성화되어 있는 경우 포스처를 1시간에서 24시간 간격으로 재평가합니다.

관리자는 결과를 계속, 로그 오프 또는 수정으로 설정할 수 있으며 실행 및 유예 시간 등의 다른 옵션을 구성할 수 있습니다.

Cisco Temporal Agent

Cisco Temporal Agent는 사용자가 신뢰할 수 있는 네트워크에 액세스할 때 컴플라이언스 상태를 공유하기 위해 Windows 또는 macOS 환경에서 사용됩니다. ISE UI에서 Cisco Temporal Agent의 컨피그레이션을 수행합니다. 엔드포인트가 인터넷 액세스를 시도할 때마다 Cisco Temporal Agent 압축 해제 파일 .exe(Windows용) 또는 dmg(macOS용)가 엔드포인트에 다운로드됩니다. 사용자는 컴플라이언스 검사를 위해 다운로드된 실행 파일이나 dmg를 실행해야 합니다. 관리자 권한은 필요하지 않습니다.

그러면 UI가 자동으로 실행되어 검사를 시작해 엔드포인트의 규정 준수 여부를 확인합니다. 컴플라이언스 검사가 완료되고 나면 ISE UI에 정책이 구성되어 있는 방식에 따라 ISE가 필요한 작업을 수행할 수 있습니다.

Windows에서는 실행 파일의 압축이 자동으로 풀리며, 이 파일의 압축이 풀리면 컴플라이언스 검사에 필요한 모든 dll 및 기타 파일이 임시 폴더에 저장됩니다. 압축이 풀린 모든 파일과 실행 파일은 컴플라이언스 검사가 완료되고 나면 삭제됩니다. 파일과 실행 파일을 완전히 제거하려면 사용자가 UI를 종료해야 합니다.

ISE UI의 자세한 컨피그레이션 단계는 *Cisco Identity Services Engine* 관리자 가이드, 릴리스 *2.3*의 Cisco Temporal Agent 워크플로를 참조하십시오.

Cisco Temporal Agent의 제한 사항

- macOS에서는 VLAN으로 제어되는 Temporal Agent용 포스처 환경이 지원되지 않습니다. 루트 권한이 없으면 어댑터 새로고침(DHCP 새로고침) 프로세스가 수행될 수 없기 때문입니다. Temporal Agent는 사용자 프로세스로만 실행할 수 있습니다. ACL로 제어되는 포스처 환경의 경우 엔드포인트의 IP 새로고침이 필요하지 않으므로 지원됩니다.

- 치료 중에 네트워크 인터페이스가 수행되는 경우에는 사용자가 현재 UI를 종료하고 전체 절차를 다시 수행해야 합니다.
- macOS에서는 dmg 파일을 삭제할 수 없습니다.
- Temporal Agent 설치 프로그램은 실행한 후 엔드포인트에서 실행 중일 때 브라우저 뒤에 숨겨질 수 있습니다. Temporal Agent 애플리케이션 상태 수집을 진행하려면 엔드 유저가 브라우저를 최소화해야 합니다. 대부분의 Windows 10 사용자에게는 이 문제가 발생합니다. 이러한 클라이언트에서는 높은 보안 상태로 실행되는 서드파티 애플리케이션을 허용하기 위해 UAC 모드가 높음으로 설정되기 때문입니다.
- Cisco Temporal Agent에서 지원하지 않는 상태는 다음과 같습니다.
  - 서비스 상태-macOS - 시스템 데몬 검사
  - 서비스 상태-macOS - 데몬 또는 사용자 에이전트 검사
  - PM - 최신 상태 검사
  - PM - 활성화 검사
  - DE -암호화 위치 기반 검사

선택 모드를 위한 포스처 정책 개선 사항

필수 검사 통과 여부에 관계없이 선택 모드에서 장애가 발생한 요건 검사에 대한 치료를 수행할 수 있습니다. 치료에 대한 메시지는 AnyConnect ISE Posture UI에 표시되며, 장애가 발생한 항목과 치료 작업이 필요한 항목을 확인할 수 있습니다.

- 선택 모드의 수동 치료 - System Scan Summary(시스템 스캔 요약) 화면에는 특정 상황에서 장애가 발생한 경우 치료가 필요할 수 있는 선택 모드 상태가 표시됩니다. Start(시작)를 수동으로 클릭하여 치료를 하거나 Skip(건너뛰기)을 클릭할 수 있습니다. 치료 시에 장애가 발생하더라도 해당 요건은 선택 사항이므로 엔드포인트의 규정 준수 상태는 유지됩니다. System Summary(시스템 요약)에는 치료를 건너뛰었는지, 치료 시에 장애가 발생했는지, 아니면 치료가 성공했는지가 표시됩니다.
- 선택 모드의 자동 치료 - 선택적 업데이트를 적용할 때 참고 정보가 표시되는 System Scan(시스템 스캔) 타일을 모니터링할 수 있습니다. 치료는 자동으로 수행되므로 치료를 시작하라는 메시지는 표시되지 않습니다. 자동 치료 시에 장애가 발생하면 치료를 시도할 수 없다는 메시지가 표시됩니다. 그리고 원하는 경우 치료 작업을 건너뛰도록 선택할 수도 있습니다.

하드웨어 인벤토리 파악

ISE UI의 Context Visibility(상황 가시성) 아래에 Endpoints(엔드포인트) > Hardware(하드웨어) 탭이 추가되었습니다. 이 탭에서 엔드포인트 하드웨어 정보를 단시간 내에 수집, 분석 및 보고할 수 있습니다. 메모리 용량이 낮은 엔드포인트, 엔드포인트의 BIOS 모델/버전 등을 찾는 등 원하는 정보를 수집할 수 있습니다. 그리고 확인된 정보에 따라 자산 구매를 계획하기 전에 메모리 용량을 늘리거나, BIOS 버전을 업그레이드하거나, 요건을 평가할 수 있습니다. Manufacturers Utilization(제조업체 사용률) 데

슬렛에는 Windows 또는 macOS가 설치된 엔드포인트에 대한 하드웨어 인벤토리 세부사항이 표시되며, Endpoint Utilizations(엔드포인트 사용률) 데슬렛에는 엔드포인트의 CPU, 메모리 및 디스크 사용률이 표시됩니다. 자세한 내용은 *Cisco Identity Services Engine* 관리자 가이드, 릴리스 *2.3*의 Hardware(하드웨어) 탭을 참조하십시오.

스텔스 모드

관리자는 AnyConnect UI 타일이 엔드 유저 클라이언트에서 숨겨져 있는 동안 ISE Posture를 구성할 수 있습니다. 이 경우 팝업은 표시되지 않으며 사용자의 개입이 필요한 모든 시나리오에서는 기본 작업이 수행됩니다. 이 기능은 Windows 및 Mac 운영 체제에서 사용 가능합니다.

Cisco Identity Services Engine 관리자 가이드의 포스처 정책 구성 섹션을 참조하십시오. 이 섹션의 정보를 참조하여 클라이언트리스 상태에서 스텔스 모드를 비활성화 또는 활성화로 지정할 수 있습니다.

ISE Posture 프로파일 편집기, 218 페이지에서 프로파일을 매핑한 다음 AnyConnect 컨피그레이션을 ISE의 Client Provisioning(클라이언트 프로비저닝) 페이지에 매핑하면 AnyConnect가 초기 포스처 요청 중에 포스처 프로파일을 읽고 원하는 모드로 설정한 다음 선택한 모드와 관련된 정보를 ISE에 전송할 수 있습니다. 모드 및 기타 요인(예: ID 그룹, OS, 컴플라이언스 모듈)에 따라 Cisco ISE는 적절한 정책과의 일치 여부를 확인합니다.

Cisco Identity Services Engine 관리자 가이드에서 스텔스 모드 구축 및 해당 영향을 참조하십시오.

ISE Posture 사용 시에는 스텔스 모드에서 다음 기능을 설정할 수 없습니다.

- 모든 수동 치료
- 링크 치료
- 파일 치료
- WSUS에 UI 치료 표시
- GUI 치료 활성화
- AUP 정책

포스처 정책 시행

엔드포인트에 설치된 소프트웨어의 전반적인 가시성을 개선할 수 있도록 다음과 같은 포스처 개선 사항이 제공됩니다.

- 엔드포인트 방화벽 제품의 상태를 점검하여 해당 제품이 실행 중인지를 확인할 수 있습니다. 원하는 경우 초기 포스처 및 PRA(주기적 재평가) 중에 방화벽을 활성화하고 정책을 시행할 수 있습니다. 관련 설정을 지정하려면 Cisco Identity Services Engine 환경 설정 가이드의 방화벽 조건 설정 섹션을 참조하십시오.
- 마찬가지로 엔드포인트에 설치된 애플리케이션의 쿼리를 실행할 수 있습니다. 원치 않는 애플리케이션이 실행 중이거나 설치되어 있으면 해당 애플리케이션을 중지하거나 원치 않는 애플리

케이션을 제거할 수 있습니다. 관련 설정을 지정하려면 ISE UI에서 Cisco Identity Services Engine 환경 설정 가이드 섹션의 애플리케이션 치료 섹션을 참조하십시오.

UDID 통합

디바이스에 설치되어 있는 AnyConnect는 자체 UDID(고유 식별자)를 AnyConnect의 모든 모듈과 공유합니다. 엔드포인트의 식별자인 이 UDID는 끝점 속성으로 저장되므로 MAC 주소가 아닌 특정 끝점에서 포스처를 제어할 수 있습니다. 그런 다음 UDID를 기준으로 끝점을 쿼리할 수 있습니다. UDID는 엔드포인트가 연결하는 방법과 관계없이, 그리고 업그레이드 또는 제거 시에도 변경되지 않는 상수입니다. 그러면 ISE UI의 Context Visibility(상황 가시성) 페이지(**Context Visibility(**상황 가시성**) > Endpoints(**엔드포인트**) > Compliance(**컴플라이언스**)**에서 NIC가 여러 개인 엔드포인트에 대해 여러 항목이 아닌 하나의 항목을 표시할 수 있습니다.

애플리케이션 모니터링

포스처 클라이언트는 동적 변경 사항을 관찰하여 정책 서버에 다시 보고할 수 있도록 여러 엔드포인트 속성을 지속적으로 모니터링할 수 있습니다. 포스처 정책이 구성된 방식에 따라 안티스파이웨어, 안티 바이러스, 악성코드 차단, 방화벽 등에 대해 설치되어 실행 중인 애플리케이션과 같은 여러 속성을 모니터링할 수 있습니다. 애플리케이션 조건 설정에 대한 자세한 내용은 Cisco Identity Services Engine 관리자 가이드의 연속 엔드포인트 속성 모니터링 섹션을 참조하십시오.

USB 스토리지 디바이스 탐지

USB 대용량 스토리지 디바이스를 Windows 엔드포인트에 연결하면 포스처 클라이언트가 해당 디바이스를 탐지하여 포스처 정책 차단에 따라 디바이스를 차단하거나 허용할 수 있습니다. 엔드포인트의 위치가 ISE로 제어되는 동일 네트워크로 유지된다면 에이전트는 USB 탐지를 사용하여 해당 엔드포인트를 계속 모니터링합니다. 이 기간 동안 기준과 일치하는 USB 디바이스가 연결되면 지정한 치료 작업이 수행됩니다. 또한 정책 서버로 사고가 보고됩니다.

USB 스토리지 탐지에서는 OPSWAT v4 컴플라이언스 모듈을 사용합니다. ISE UI의 **Work Centers(**작업 센터**) > Posture(**포스처**) > Policy Elements(**정책 요소**) > USB**에 있는 PRA(주기적 재평가 정책)에서 USB 검사를 구성해야 합니다.

참고 검사와 치료는 순차적으로 수행되므로 다른 검사에 대해 PRA 유예 시간을 최솟값으로 설정하면 USB 검사 처리 시의 지연을 방지할 수 있습니다. 유예 시간은 ISE UI의 **Work Centers(**작업 센터**) > Posture(**포스처**) > Settings(**설정**) > Reassessment Config(**재평가 컨피그레이션**)**에서 설정합니다.

ISE UI에서 USB 스토리지 탐지를 구성하는 단계는 USB 대용량 스토리지 검사 워크플로를 참조하십시오.

자동 규정 준수

포스처 리스를 통해 ISE 서버는 포스처를 완전히 건너뛰고 간단하게 시스템을 규정 준수 상태로 둘 수 있습니다. 이 기능을 사용하면 시스템이 최근 배치될 때 네트워크 간의 전환이 지연되지 않습니다. ISE Posture 에이전트는 ISE 서버가 발견된 직후에 상태 메시지를 UI로 전송하고 시스템의 규정 준수 여부를 표시합니다. Settings(설정) > Posture(포스처) > General Settings(일반 설정)의 ISE UI에서 최초 규정 준수 검사 이후 엔드포인트가 다음 포스처 규정 준수를 검사할 때까지의 기간을 지정할 수 있습니다. 규정 준수 상태는 사용자가 하나의 통신 인터페이스에서 다른 통신 인터페이스로 전환하는 경우에도 유지되어야 합니다.

참고 포스처 리스를 사용하면 세션이 ISE에서 유효한 경우 엔드포인트는 포스처를 알 수 없는 상태에서 규정 준수 상태로 전환해야 합니다.

VLAN 모니터링 및 전환

일부 사이트에서는 다른 VLAN 또는 서브넷을 사용하여 기업 그룹 및 액세스 수준에 대해 네트워크를 파티션합니다. ISE에서의 CoA(Change of Authorization, 권한 부여 변경)는 VLAN 변경사항을 지정합니다. 또한 세션 종료와 같은 관리자 작업으로 인해 변경이 발생합니다. VPN 연결 중에 VLAN 변경사항을 지원하려면 ISE Posture 프로파일에서 다음 설정을 구성하십시오.

- VLAN Detection Interval(VLAN 탐지 간격) — 에이전트가 VLAN 전환을 탐지하는 빈도 및 모니터링 비활성화 여부를 결정합니다. 이 간격이 0을 제외한 값으로 설정된 경우 VLAN 모니터링이 활성화됩니다. 이 값을 Mac OS X용으로 최소한 5로 설정하십시오.

  VLAN 모니터링은 예상치 않은 VLAN 변경사항을 탐지하기 위해 Mac에서만 필요하지만 Windows와 Mac OS X 모두에서 구현됩니다. VPN이 연결되었거나 acise(기본 AnyConnect ISE 프로세스)가 실행 중이지 않은 경우 자동으로 비활성화됩니다. 유효한 범위는 0초에서 900초입니다.

- Enable Agent IP Refresh(에이전트 IP 새로 고침 활성화) — 선택하지 않은 경우 ISE는 네트워크 전환 지연 값을 에이전트에 전송합니다. 이 설정을 선택한 경우 ISE는 에이전트에 DHCP 릴리스를 전송하고 값을 갱신하며 에이전트는 최신 IP 주소를 검색하기 위해 IP 새로 고침을 수행합니다.

- DHCP Release Delay(DHCP 릴리스 지연) 및 DHCP Renew Delay(DHCP 갱신 지연) — IP 새로 고침 및 Enable Agent IP Refresh(에이전트 IP 새로 고침 활성화) 설정과 함께 사용됩니다. Enable Agent IP Refresh(에이전트 IP 새로 고침 활성화) 확인란을 선택하고 이 값이 0이 아닌 경우, 에이전트는 릴리스 지연 시간(초) 동안 대기하고 IP 주소를 새로 고치며 갱신 지연 시간(초) 동안 대기합니다. VPN이 연결되어 있는 경우 IP 새로 고침은 자동으로 비활성화됩니다.
- Network Transition Delay(네트워크 전환 지연) — VLAN 모니터링이 Enable Agent IP Refresh(에이전트 IP 새로 고침 활성화) 확인란에서 에이전트에 의해 비활성화 또는 활성화된 경우 사용됩니다. 이러한 지연은 VLAN이 사용되지 않는 경우 버퍼를 추가하며 에이전트가 서버로부터의 정확한 상태를 대기하도록 적절한 시간을 제공합니다. ISE는 에이전트에 이 값을 전송합니다. ISE UI의 전역 설정에서 네트워크 전환 지연 값을 설정한 경우, ISE Posture 프로파일 편집기의 값은 이 값을 덮어씁니다.

참고 ASA는 VLAN 변경사항을 지원하지 않기 때문에 클라이언트가 ASA를 통해 ISE에 연결된 경우 이러한 설정이 적용되지 않습니다.

문제 해결

상태가 완료된 후에도 엔드포인트 디바이스가 네트워크에 액세스할 수 없는 경우 다음 사항을 확인하십시오.

- VLAN 변경사항은 ISE UI에 구성되어 있습니까?
  - 대답이 "예"인 경우, DHCP 릴리스 지연 및 갱신 지연이 프로파일에 설정됩니까?
  - 두 가지 설정 모두 0인 경우, 네트워크 전환 지연이 프로파일에 설정됩니까?

AnyConnect ISE 플로우를 방해하는 작업

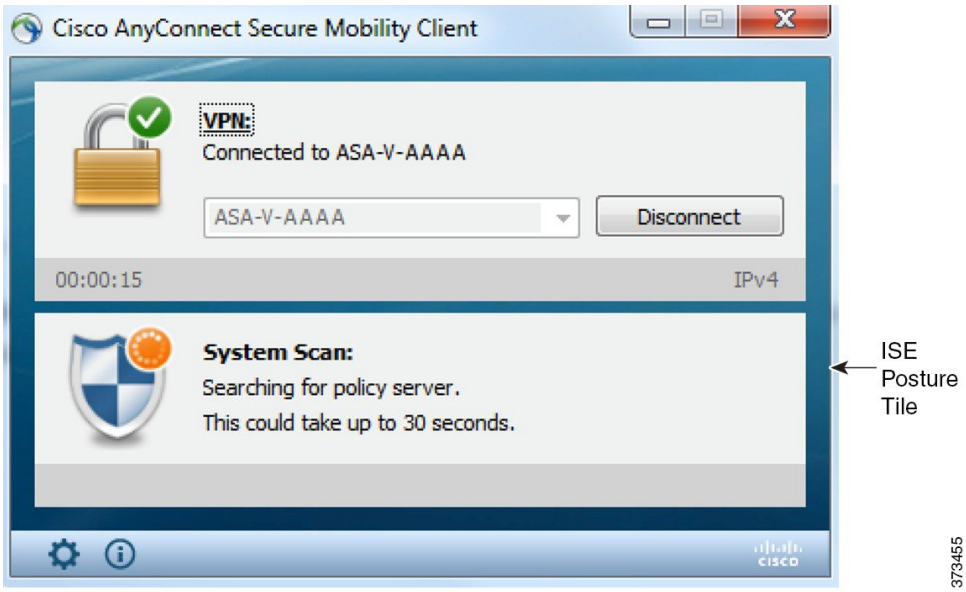
여러 가지 이유로 AnyConnect ISE Posture 플로우가 초기 포스처 재평가 또는 수동 재평가 중에 중단될 수 있습니다.

- 사용자의 AnyConnect ISE 취소 — 포스처 확인 및 보안정책 교정 도중 사용자가 AnyConnect ISE를 취소할 수 있습니다. UI에서 사용자에게 취소가 진행 중이라고 즉시 알리지만 이는 엔드포인트를 의심스러운 상태로 두는 것을 피하려고 할 때만 발생해야 합니다. 서드파티 소프트웨어가 사용된 경우 일부 취소에 재부팅이 필요할 수도 있습니다. AnyConnect UI의 포스처 바둑판식 배열 부분에 취소 이후 규정 준수 상태가 표시됩니다.
- 보안정책 교정 타이머 만료 — 포스처 요건을 충족하기 위한 관리자 제어 시간이 만료되었습니다. 평가 보고서가 헤드엔드로 전달됩니다. 수동 재평가 중에 사용자는 네트워크 액세스를 유지하고 포스처 평가를 통해 모든 필수 요건이 충족될 때 네트워크 액세스 권한이 부여됩니다.
- 포스처 확인 도중 오류 발생 — 포스처 확인 단계 도중 오류가 발생했으나 AnyConnect를 계속 실행할 수 있는 경우, 사용자에게 통지되지만 가능한 경우 포스처 확인이 계속 수행됩니다. 필수 포스처 확인 도중 오류가 발생하는 경우 확인이 실패로 표시됩니다. 모든 필수 요건이 충족하는 경우 네트워크 액세스 권한이 부여됩니다. 그렇지 않으면 사용자가 포스처 프로세스를 다시 시작할 수 있습니다.
- 보안정책 교정 도중 오류 발생 — 보안정책 교정 단계 도중 오류가 발생했으나 AnyConnect ISE Posture를 계속 실행할 수 있는 경우 사용자에게 통지됩니다. 실패한 보안정책 교정 단계가 필수 포스처 요건과 관련된 경우, AnyConnect ISE Posture가 보안정책 교정 프로세스를 중단합니다. 실패한 보안정책 교정 단계가 선택 사항인 상태 요건과 관련된 경우, 다음 단계로 진행하여 ISE Posture 작업을 완료하려고 시도합니다. 모든 필수 요건이 충족하는 경우 네트워크 액세스 권한이 부여됩니다. 그렇지 않으면 사용자가 포스처 프로세스를 다시 시작할 수 있습니다.
- 기본 게이트웨이 변경 — 기본 게이트웨이에 대한 변경 사항으로 인해 사용자가 신뢰할 수 있는 네트워크에 액세스하지 못하게 되면 ISE Posture가 ISE 재검색을 시도합니다. AnyConnect UI의 ISE Posture 바둑판식 배열 부분에 ISE Posture가 재검색 모드로 전환될 때 ISE Posture의 상태가 표시됩니다.

- AnyConnect와 ISE 간의 연결 해제 — 엔드포인트가 규정을 준수하는 것으로 간주되고 네트워크 액세스 권한이 부여되면 다양한 네트워크 시나리오가 발생할 수 있습니다. 엔드포인트에서 네트워크의 연결이 완전히 끊길 수 있으며 ISE가 다운되고 세션 시간 초과 또는 수동 재시작 등으로 인해 ISE Posture가 실패하거나 ASA를 지원하는 ISE에서 VPN 터널 연결이 끊길 수 있습니다.

ISE Posture 상태

AnyConnect ISE Posture가 예상대로 작동하고 네트워크 액세스를 차단하는 경우, AnyConnect UI의 ISE Posture 바둑판식 배열에서 "시스템 스캔: 정책 서버 검색"이 표시됩니다. Windows 작업 관리자 또는 Mac OS X 시스템 로그에서 이 프로세스가 실행 중인지 확인할 수 있습니다. 서비스가 실행 중이 아닌 경우 AnyConnect UI의 ISE Posture 바둑판식 배열에서 "시스템 스캔: 서비스를 사용할 수 없습니다."라고 표시됩니다.



네트워크 변경사항에서 검색 단계를 시작합니다. AnyConnect ISE Posture를 사용하여 기본 인터페이스의 기본 경로가 변경되면 에이전트가 다시 검색 프로세스로 돌아갑니다. 예를 들어 WiFi 및 기본 LAN이 연결되어 있는 경우, 에이전트는 검색을 다시 시작합니다. 마찬가지로 WiFi 및 기본 LAN이 연결되어 있지만 WiFi가 연결이 끊어진 경우 에이전트는 검색을 다시 시작하지 않습니다.

AnyConnect UI의 ISE Posture 바둑판식 배열에서 "시스템 스캔" 이후에 다음 상태 메시지를 확인할 수 있습니다.

- 제한됨 또는 연결 안 됨 — 연결이 없기 때문에 검색이 발생하지 않습니다. AnyConnect ISE Posture 에이전트가 네트워크의 잘못된 엔드포인트에서 검색을 수행 중일 수 있습니다.
- 현재 WiFi에서 시스템 스캔이 필요하지 않음 — 보안되지 않은 WiFi가 탐지되어 검색이 발생하지 않습니다. AnyConnect ISE Posture 에이전트는 LAN에서만 검색을 시작하며 802.1X 인증을 사용하는 경우, VPN에서 무선으로 검색을 시작합니다. WiFi가 보안되지 않았거나 에이전트 프로파일에서 OperateOnNonDot1XWireless를 1로 설정하여 이 기능을 비활성화했습니다.

- 권한이 없는 정책 서버 — 호스트가 ISE 네트워크의 서버 이름 규칙과 일치하지 않으며 이로 인해 네트워크 액세스가 제한되거나 불가능합니다.
- AnyConnect 다운로더가 업데이트 중... — 다운로더가 호출되고 패키지 버전과 비교하여 AnyConnect 구성을 다운로드하고 필요한 업그레이드를 수행합니다.
- 시스템 스캐닝 중... — 안티 바이러스 및 안티스파이웨어 보안 제품에 대한 스캐닝이 시작되었습니다. 이 프로세스 중에 네트워크가 변경된 경우, 에이전트는 로그 파일 생성 프로세스를 재사용하고 상태가 "정책 서버 탐지 안 됨"으로 돌아갑니다.
- AnyConnect 스캔 우회 — 네트워크가 Cisco NAC Agent를 사용하도록 구성됩니다.
- 사용자가 취소한 신뢰할 수 없는 정책 서버 — 시스템 스캔 환경 설정 탭을 사용하여 AnyConnect UI에서 신뢰할 수 없는 서버에 대한 연결을 차단 해제하는 경우, 팝업 창에서 AnyConnect 다운로더의 보안 경고를 수신합니다. 이 경고 페이지에서 **Cancel Connection(**연결 취소**)**을 클릭하면 ISE Posture 바둑판식 배열이 이 상태로 변경됩니다.
- 네트워크의 수락 가능한 사용 정책 — 네트워크에 대한 액세스를 위해서는 사용자가 수락 가능한 사용 정책을 확인하고 수락해야 합니다. 정책을 거부하면 네트워크 액세스가 제한됩니다.
- 네트워크 설정 업데이트 — Settings(설정) > Posture(포스처) > General Settings(일반 설정)의 ISE UI에서 네트워크 전환 간에 발생해야 하는 지연 시간(초)을 지정할 수 있습니다.
- 규정이 준수되지 않음. 업데이트 시간이 만료됨 — 보안정책 교정을 위해 설정된 시간이 만료되었습니다.
- 규정 준수. 네트워크 액세스 허용됨 — 보안정책 교정이 완료됩니다. System Scan(시스템 스캔) > Scan Summary(스캔 요약)는 상태를 완료로 표시합니다.
- 정책 서버 탐지 안 됨 — ISE 네트워크를 찾을 수 없습니다. 30초 후에 에이전트가 프로브 속도를 늦춥니다. 기본 네트워크 액세스가 적용됩니다.

엔드포인트에서의 동시 사용자

여러 명의 사용자가 네트워크 연결을 동시에 공유하는 엔드포인트에 로그인하면 AnyConnect ISE는 별도의 포스처 평가를 지원하지 않습니다. AnyConnect ISE를 실행할 첫 번째 사용자가 성공적으로 포스처를 설정했으며 엔드포인트에 신뢰할 수 있는 네트워크 액세스 권한이 부여된 경우 엔드포인트의 다른 모든 사용자가 네트워크 액세스를 상속합니다. 이를 방지하기 위해 관리자가 엔드포인트에서 동시 사용자를 허용하는 기능을 비활성화할 수 있습니다.

포스처 모듈 로깅

ISE Posture의 경우 이벤트는 네이티브 운영 체제 이벤트 로그에 기록됩니다(Windows 이벤트 로그 뷰어 또는 Mac OS X 시스템 로그).

VPN Posture(HostScan)의 경우 오류 및 경고를 syslogs(Windows 이외 용) 및 이벤트 뷰어(Windows용)로 이동시킵니다. 사용 가능한 모든 메시지가 로그 파일로 이동합니다.

VPN Posture(HostScan) 모듈 구성 요소는 운영 체제, 권한 수준 및 시작 메커니즘(웹 실행 또는 AnyConnect)을 기준으로 최대 3개의 로그에 출력됩니다.

- cstub.log - AnyConnect 웹 실행이 사용될 경우 로깅을 캡처합니다.
- libcsd.log - VPN Posture API를 사용하는 AnyConnect 스레드에서 생성됩니다. 디버깅 항목은 로깅 수준 구성에 따라 이 로그에서 생성됩니다.
- cscan.log - 스캐닝 실행 파일(cscan.exe)에서 생성되며 VPN Posture를 위한 기본 로그입니다. 디버깅 항목은 로깅 수준 구성에 따라 이 로그에서 생성됩니다.

포스처 모듈의 로그 파일 및 위치

ISE Posture의 경우, 설치된 AnyConnect 버전의 고유한 하위 폴더에 이벤트가 포함되어 있어 나머지 AnyConnect 이벤트에서 쉽게 분리됩니다. 각 뷰어에서는 키워드 검색 및 필터링을 할 수 있습니다. 웹 에이전트 이벤트는 표준 애플리케이션 로그에 기록합니다.

문제 해결을 위해 ISE Posture 요건 정책 및 평가 보고서는 이벤트 로그가 아니라 엔드포인트에 있는 별도의 난독 처리된 파일에 로그됩니다. aciseposture와 같이 일부 로그 파일 크기는 프로파일에서 관리자가 구성할 수 있지만 UI 로그 크기는 미리 정의되어 있습니다.

프로세스가 비정상적으로 종료될 때마다 다른 AnyConnect 모듈에서 제공하는 것과 동일하게 미니 덤프 파일이 생성됩니다.

VPN Posture(HostScan)의 경우 파일이 사용자 홈 폴더의 다음 디렉터리에 있습니다.

- (Windows 외) - .cisco/hostscan/log
- (Windows) - C:\Users\<user_name>\AppData\Local\Cisco HostScan\log\cscan.log

ISE Posture 프로파일 편집기

관리자는 독립형 편집기를 사용하도록 선택하여 포스처 프로파일을 생성한 다음 ISE에 업로드할 수 있습니다. 그렇지 않은 경우 내장된 포스처 프로파일 편집기가 정책 요소 아래의 ISE UI에서 구성됩니다. AnyConnect 구성 편집기가 ISE에서 시작되면 AnyConnect 소프트웨어 및 연결된 모듈, 프로파일, OPSWAT 및 모든 사용자 정의를 통해 완료되는 AnyConnect 구성을 생성합니다. ASA에서 ISE Posture용 독립형 프로파일 편집기에는 다음 파라미터가 포함되어 있습니다.

- 에이전트 동작
- **IP** 주소 변경

  최적의 사용자 경험을 위해 권장 사항에 따라 아래 값을 설정하십시오.

  - **VLAN detection interval(VLAN** 탐지 간격**)**— 에이전트가 클라이언트 IP 주소를 새로 고치기 전에 VLAN 변경사항을 탐지하려고 시도하는 간격입니다. 유효한 범위는 0초에서 900초이며 권장 값은 5초입니다.

- **Ping or ARP(ping** 또는 **ARP)**— IP 주소 변경사항 탐지를 위한 방법입니다. 권장 설정은 ARP입니다.
- **Maximum timeout for ping(ping** 최대 시간 제한**)**— ping 시간 제한은 1초에서 10초입니다.
- **Enable agent IP refresh(**에이전트 **IP** 새로 고침 활성화**)**— VLAN 변경사항 탐지를 활성화하려면 선택합니다.
- **DHCP renew delay(DHCP** 갱신 지연**)**— IP를 새로 고친 후 에이전트가 대기하는 시간(초)입니다. Enable Agent IP Refresh(에이전트 IP 새로 고침 활성화)를 사용하는 경우, 이 값을 구성하십시오. 이 값이 0이 아닌 경우, 에이전트는 이 전환 시간에 IP 새로 고침을 수행합니다. VPN이 새로 고침 중에 탐지되면 새로 고침이 비활성화됩니다. 유효한 값은 0초에서 60초이며 권장 값은 5초입니다.
- **DHCP release delay(DHCP** 릴리스 지연**)**— 에이전트가 IP 새로 고침을 지연하는 시간(초)입니다. Enable Agent IP Refresh(에이전트 IP 새로 고침 활성화)를 사용하는 경우, 이 값을 구성하십시오. 이 값이 0이 아닌 경우, 에이전트는 이 전환 시간에 IP 새로 고침을 수행합니다. VPN이 새로 고침 중에 탐지되면 새로 고침이 비활성화됩니다. 유효한 값은 0초에서 60초이며 권장 값은 5초입니다.
- **Network transition delay(**네트워크 전환 지연**)**— 에이전트가 계획된 IP 변경사항을 대기할 수 있도록 네트워크 모니터링을 일시 중지한 시간 범위(초 단위)입니다. 권장 값은 5초입니다.

• 포스처 프로토콜

- **Discovery host(**검색 호스트**)**— 에이전트가 연결할 수 있는 서버입니다. 독립형 프로파일 편집기의 경우 단일 호스트만 입력하십시오.
- **Server name rules(**서버 이름 규칙**)**— 에이전트가 연결될 수 있는 서버를 정의한 와일드카드의 쉼표로 구분된 이름(예: .cisco.com) 목록입니다.
- **Call Home List(Call Home** 목록**)** - 로드 밸런싱, 조회 모니터링/트러블슈팅 또는 해당 노드에서 기본 PSN(정책 서비스 노드)에 매핑된 DNS(다중 시나리오의 경우)에 사용하려는 FQDN을 입력합니다. 이 목록을 구성하면 조회 모니터링 및 트러블슈팅용 첫 번째 프로브가 Call Home으로 전송됩니다. 리디렉션 네트워크에서 비리디렉션 네트워크로 마이그레이션하는 동안 이 목록을 구성해야 합니다.
- **PRA retransmission time(PRA** 재전송 시간**)**— 수동 재평가 통신 실패가 발생한 경우 이 에이전트 재시도 기간이 지정됩니다. 유효한 범위는 60초에서 3600초입니다.

고급 패널

AnyConnect Secure Mobility Client UI의 Advanced(고급) 패널은 각 구성 요소에 대한 영역으로 통계, 사용자 환경 설정 및 구성 요소 관련 추가 정보를 표시합니다. AnyConnect 시스템 트레이의 **Advanced Window for all components(**모든 구성 요소를 위한 고급 창**)** 아이콘을 클릭하면 새 시스템 스캔 섹션에 다음 탭이 포함됩니다.

참고 이러한 통계, 사용자 환경 설정, 메시지 기록 등은 Mac OS X의 Statistics(통계) 창에 표시됩니다. Preferences(환경 설정)는 Windows에서와 같은 탭 방향이 아닌 Preferences(환경 설정) 창에 있습니다.

- Preferences(환경 설정) — 신뢰할 수 없는 서버에 대한 연결을 차단하면 다운로더 프로세스 도중, 인증서를 신뢰할 수 없고 확인되지 않은 ISE 서버에 대해 "신뢰할 수 없는 서버가 차단됨"이라는 메시지가 표시됩니다. 차단을 비활성화한 경우 AnyConnect는 잠재적으로 악의적인 네트워크 디바이스에 대한 연결을 차단하지 않습니다.
- Statistics(통계) - 현재의 ISE Posture 상태(규정 준수 또는 비준수), OPSWAT 버전 정보, 사용 제한 정책의 상태, 포스처의 최종 실행 타임스탬프, 누락된 요건뿐만 아니라 문제 해결을 위해 표시해야 한다고 간주되는 기타 통계를 제공합니다.
- Security Products(보안 제품) - 시스템에 설치된 악성코드 차단 제품의 목록에 액세스합니다.
- Scan Summary(스캔 요약) - 사용자는 사용자가 볼 수 있도록 관리자가 구성한 모든 포스처 항목을 볼 수 있습니다. 예를 들어, 포스처 항목 구성을 통해 시스템에 배치된 모든 항목을 볼 수도 있고 포스처 확인에 실패하여 보안정책 교정이 필요한 항목만 볼 수도 있습니다.
- Message History(메시지 기록) - 구성 요소에 관해 시스템 트레이로 전송된 모든 상태 메시지의 기록을 제공합니다. 이 기록은 문제 해결에 도움이 됩니다.

VPN Posture(HostScan) 모듈이 제공하는 기능

HostScan

HostScan은 사용자가 SAS에 연결한 후 로그인하기 전에 원격 디바이스에 설치되는 패키지이며 기본 모듈, 엔드포인트 평가 모듈 및 고급 엔드포인트 평가 모듈의 임의 조합으로 구성됩니다.

참고 AnyConnect 릴리스 3.x에서는 이 패키지가 hostscan_version.pkg 파일에 번들로 제공되어 HostScan 이미지 아래 ASA에서 업데이트하고 HostScan이 작동하도록 활성화해야 했습니다. 이제는 별도로 설치됩니다.

기본 기능

HostScan은 Cisco 클라이언트리스 SSL VPN 또는 AnyConnect VPN 클라이언트 세션을 설정하는 원격 디바이스의 운영 체제 및 서비스 팩을 자동으로 식별합니다.

HostScan이 엔드포인트에서 특정 프로세스, 파일 및 레지스트리 키를 검사하도록 구성할 수도 있습니다. HostScan은 전체 터널 설정 이전에 이러한 검사를 수행하고 기업 소유, 개인 및 공용 컴퓨터 간에 구분할 수 있도록 이 정보를 ASA에 전송합니다. 해당 정보를 평가에서도 사용할 수 있습니다.

참고 사전 로그인 평가 및 반환 인증서 정보는 제공되지 않습니다. HostScan은 인증 방법이 아니며 연결을 시도하는 디바이스에 있는 정보만 확인할 뿐입니다.

또한 HostScan은 구성된 DAP 엔드포인트 기준에 대한 평가를 위해 다음과 같은 추가 값을 자동으로 반환합니다.

- Microsoft Windows, Mac OS 및 Linux 운영 체제
- Microsoft 기술 자료 번호(KB)
- 호스트 이름, MAC 주소, BIOS 시리얼 번호, 포트 번호(레거시 속성), TCP/UDP 포트 번호, 개인 정보 보호, 엔드포인트 평가의 버전(OPSWAT)과 같은 디바이스 엔드포인트 속성 유형

참고 HostScan은 Windows 클라이언트 시스템의 Microsoft 소프트웨어 업데이트에 관한 서비스 릴리스(GDR) 정보를 수집합니다. 서비스 릴리스는 여러 핫픽스를 포함합니다. 서비스 릴리스의 엔드포인트 특성은 핫픽스가 아닌 DAP 규칙에서 사용됩니다.

엔드포인트 평가

엔드포인트 평가는 안티 바이러스 및 안티스파이웨어 애플리케이션의 대규모 수집, 관련 정의 업데이트 및 방화벽에 대해 원격 컴퓨터를 검사하는 HostScan 확장 기능입니다. 이 기능을 사용하면 ASA가 특정 DAP(Dynamic Access Policy, 동적 액세스 정책)를 세션에 할당하기 전 요건을 충족하기 위해 엔드포인트 기준을 결합할 수 있습니다.

자세한 내용은 Cisco ASA Series VPN 환경 설정 가이드의 해당하는 버전에서 동적 액세스 정책 섹션을 참조하십시오.

고급 엔드포인트 평가: 안티 바이러스, 안티스파이웨어 및 방화벽 치료

Windows, Mac OS X 및 Linux 데스크톱에서 고급 엔드포인트 평가는 해당 소프트웨어가 별도의 애플리케이션이 치료를 시작하도록 허용하는 경우 안티 바이러스, 안티스파이웨어 및 개인 방화벽 보호의 여러 측면에 대한 치료 시작을 시도할 수 있습니다.

참고 AnyConnect 4.4.x는 HostScan 4.3.05050 이전의 HostScan 릴리스와 호환되지 않습니다. 그러나 AnyConnect 4.4.x는 HostScan 4.3.05050 이하 버전과 호환되며, 4.3.05050(또는 HostScan 4.3.x 릴리스 이후)을 ASDM에서 HostScan 이미지로 사용해야 합니다. 이렇게 하려면 Configuration(컨피그레이션) > Remote Access VPN(원격 액세스 VPN) > Secure Desktop Manager > Host Scan image(Host Scan 이미지)에서 해당 버전을 선택합니다.

안티 바이러스 - 다음과 같은 안티 바이러스 소프트웨어의 구성 요소 보안정책을 교정합니다.

- 강제 파일 시스템 보호 - 비활성화된 안티 바이러스 소프트웨어를 활성화합니다.

- 강제 바이러스 정의 업데이트 - 안티 바이러스 정의가 고급 엔드포인트 평가 컨피그레이션을 통해 정의된 기간(일) 동안 업데이트되지 않은 경우 바이러스 정의 업데이트를 시작합니다.

안티스파이웨어 - 안티스파이웨어 정의가 고급 엔드포인트 평가 컨피그레이션을 통해 정의된 기간(일) 동안 업데이트되지 않은 경우 안티스파이웨어 정의 업데이트를 시작합니다.

개인 방화벽 - 고급 엔드포인트 평가 구성에 정의된 요구 사항을 충족하지 않는 방화벽 설정 및 규칙을 재구성합니다. 예를 들면 다음과 같습니다.

- 방화벽 활성화 또는 비활성화
- 애플리케이션 실행 방지 또는 허용
- 포트를 차단 또는 열기

참고 이 기능은 일부 개인 방화벽에서만 지원됩니다.

최종 사용자가 성공적으로 VPN에 연결한 후 안티 바이러스 또는 개인 방화벽을 비활성화하는 경우, 고급 엔드포인트 평가 기능은 약 60초 이내에 해당 애플리케이션을 다시 활성화하려고 시도합니다.

HostScan용 안티 바이러스 애플리케이션 구성

VPN Posture(HostScan) 모듈을 설치하기 전에 안티 바이러스 소프트웨어를 "화이트리스트"에 구성하거나 다음과 같이 이 애플리케이션에 대한 보안 예외를 설정합니다. 안티 바이러스 애플리케이션은 다음 애플리케이션의 동작을 악의적으로 잘못 해석할 수 있습니다.

- cscan.exe
- ciscod.exe
- cstub.exe

동적 액세스 정책과의 통합

ASA는 HostScan 기능을 DAP(Dynamic Access Policies, 동적 액세스 정책)에 통합합니다. 구성에 따라 DAP를 할당하기 위한 조건으로 ASA는 선택적 AAA 특성 값과 함께 하나 이상의 엔드포인트 특성 값을 사용합니다. DAP의 엔드포인트의 특성에서 지원하는 HostScan 기능에는 OS 탐지, 정책, 기본 결과 및 엔드포인트 평가가 포함됩니다.

단일 특성을 지정하거나 DAP를 세션에 할당하기 위해 필요한 조건을 구성하는 특성들을 결합할 수 있습니다. DAP는 엔드포인트 AAA 특성 값에 적합한 수준의 네트워크 액세스를 제공합니다. ASA는 구성한 엔드포인트 기준이 모두 충족될 때 DAP를 적용합니다.

Cisco ASA Series VPN 환경 설정 가이드에서 동적 액세스 정책 구성 섹션을 참조하십시오.

DAP의 BIOS 일련 번호

VPN Posture(HostScan)는 호스트의 BIOS 시리얼 번호를 검색할 수 있습니다. DAP(Dynamic Access Policy, 동적 액세스 정책)를 사용하여 해당 BIOS 일련 번호를 기반으로 ASA에 대한 VPN 연결을 허용 또는 방지할 수 있습니다.

BIOS를 DAP 엔드포인트 특성으로 지정

프로시저

단계 **1** ASDM에 로그인합니다.

단계 **2** **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 선택하십시오.

단계 **3** Configure Dynamic Access Policies(동적 액세스 정책 구성) 패널에서 BIOS를 DAP 엔드포인트 특성으로 지정하려면 **Add(**추가**)** 또는 **Edit(**편집**)** 를 클릭합니다.

단계 **4** 엔드포인트 ID 테이블 오른쪽에서 **Add(**추가**)**를 클릭합니다.

단계 **5** Endpoint Attribute Type(엔드포인트 특성 유형) 필드에서 **Device(**디바이스**)**를 선택합니다.

단계 **6** **BIOS Serial Number(BIOS** 일련 번호**)** 확인란을 선택하고 **=** (같음) 또는 **!=** (같지 않음)을 선택한 후 BIOS Serial Number(BIOS 일련 번호) 필드에 BIOS 번호를 입력합니다. Endpoint Attribute(엔드포인트 특성) 대화 상자에서 변경 사항을 저장하려면 **OK(**확인**)** 를 클릭합니다.

단계 **7** Edit Dynamic Access Policy(동적 액세스 정책 편집)에 대한 변경 사항을 저장하려면 **OK(**확인**)** 를 클릭합니다.

단계 **8** Dynamic Access Policy(동적 액세스 정책)에 대한 변경 사항을 저장하려면 **Apply(**적용**)** 를 클릭합니다.

단계 **9** **Save(**저장**)**를 클릭합니다.

BIOS 일련 번호를 얻는 방법

- Windows —http://support.microsoft.com/kb/558124
- Mac OS X —http://support.apple.com/kb/ht1529
- Linux — 다음 명령을 사용합니다.

```
/usr/bin/hal-get-property --udi /org/freedesktop/Hal/devices/computer --key
system.hardware.serial
```

ASA에서 활성화된 HostScan 이미지 결정

ASDM을 열고 **Configuration(**구성**) > Remote Access VPN(**원격 액세스 **VPN) > HostScan Image(HostScan** 이미지**)**를 선택하십시오.

HostScan 업그레이드

msiexec를 사용하여 AnyConnect 및 HostScan를 수동으로 업그레이드하는 경우 먼저 AnyConnect를 업그레이드한 후에 HostScan을 업그레이드해야 합니다.

OPSWAT 지원 차트

OPSWAT 지원 차트에는 사용 중인 안티 바이러스, 안티스파이웨어 및 방화벽 애플리케이션을 위한 제품 이름 및 버전 정보가 포함되어 있습니다. HostScan은 v2 OPSWAT API를 지원하며 ISE Posture 규정 준수 모듈은 v3 및 v4 OPSWAT API를 지원합니다. 이 두 버전의 구성에서 가장 큰 차이점은 v2는 라이브러리 파일을 업체별로 구성하는 반면 v3는 제품 유형별로 구성한다는 점입니다.

AnyConnect 릴리스 4.3 이상 버전이나 ISE 2.1 이상 버전을 사용하는 경우 ISE 컴플라이언스 모듈용으로 OPSWAT v3 또는 v4를 사용하도록 선택할 수 있습니다. 악성코드 차단용 컨피그레이션은 ISE UI의 **Work Centers**(작업 센터) **> Posture**(포스처) **> Posture Elements**(포스처 요소) **> Conditions**(조건) **> Antimalware**(악성코드 차단)에 있습니다.

AnyConnect 4.4.x는 HostScan 4.3.05017 이전의 HostScan 릴리스와 호환되지 않습니다. 그러나 AnyConnect 4.4.x는 HostScan 4.3.05017 이하 버전과 호환되며, HostScan 4.3.05017(또는 HostScan 4.3.x 릴리스 이후)을 ASDM에서 HostScan 이미지로 사용해야 합니다(Configuration(컨피그레이션) > Remote Access VPN(원격 액세스 VPN) > Secure Desktop Manager > Host Scan image(Host Scan 이미지)).

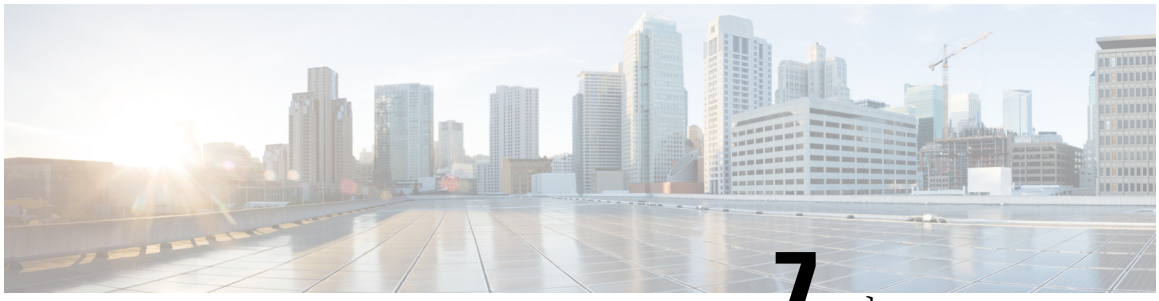
라이브러리(zip 파일) 내에 있는 이러한 개별 XML 파일은 OPSWAT, Inc.에서 디지털 서명하며 라이브러리 자체는 Cisco 인증서로 코드 서명한 단일한 자동 압축 풀기 실행 파일로 패키지됩니다.

헤드엔드(ISE 또는 ASA) 및 엔드포인트 간에 버전 번호가 불일치할 경우, OPSWAT 컴플라이언스 모듈이 업데이트 또는 다운그레이드됩니다. 이러한 업그레이드 또는 다운그레이드는 의무사항이며 헤드엔드에 대한 연결이 설정되는 즉시 최종 사용자의 개입 없이 자동으로 발생합니다.

HostScan에서 OPSWAT 바이너리는 패키지의 일부분이며 HostScan 지원 차트를 다운로드할 수 있습니다.

AnyConnect ISE Posture의 경우에는 OPSWAT 바이너리가 별도의 설치 프로그램으로 패키지되어 있습니다.

OPSWAT v3 및 v4 라이브러리를 ISE에 업로드할 수 있으며 로컬 파일 시스템에서 또는 ISE 업데이트 피드 URL을 통해 직접 ISE에 수동으로 로드할 수 있습니다.



7 장

웹 보안 구성

웹 보안 모듈 정보

AnyConnect 웹 보안 모듈은 HTTP 트래픽 경로를 Cisco Cloud Web Security 스캐닝 프록시로 지정하는 엔드포인트 구성 요소입니다.

Cisco Cloud Web Security는 각 요소를 동시에 분석하기 위해 웹 페이지의 요소를 해체합니다. 예를 들어 특정 웹 페이지에 HTTP, 플래시 및 Java 요소가 결합된 경우 별도의 "scanlets"가 이러한 각 요소를 병렬로 분석합니다. 그런 다음 Cisco Cloud Web Security는 Cisco ScanCenter 관리 포털에 정의된 보안 정책에 따라 안전하거나 적합한 내용은 허용하고 악의적이거나 적합하지 않은 내용은 차단합니다. 이는 소수의 내용이 적합하지 않아 전체 웹 페이지가 제한되는 경우 "과도한 차단"을 방지하고, 일부 적합하지 않거나 유해한 내용이 페이지에서 전달되고 있지만 전체 페이지가 허용된 경우 "부족한 차단"을 방지합니다. Cisco Cloud Web Security는 기업 네트워크를 활성화 또는 비활성화할 때 사용자를 보호합니다.

전 세계의 많은 Cisco Cloud Web Security 스캐닝 프록시를 통해 AnyConnect 웹 보안의 이점을 누리고 있는 사용자는 대기 시간을 최소화하는 가장 빠른 응답 시간 으로 트래픽을 Cisco Cloud Web Security 스캐닝 프록시로 라우트할 수 있습니다.

또한 기업 LAN에 있는 엔드포인트를 식별할 수 있도록 신뢰할 수 있는 보안 네트워크 탐지 기능을 구성할 수 있습니다. 이 기능이 활성화된 경우 기업 LAN에서 발생한 네트워크 트래픽은 Cisco Cloud Web Security 스캐닝 프록시를 우회합니다. 해당 트래픽의 보안은 Cisco Cloud Web Security가 아닌 기업 LAN의 다른 방법 및 디바이스를 통해 관리됩니다.

AnyConnect 웹 보안의 특성 및 기능은 AnyConnect 프로파일 편집기를 사용하여 편집하는 AnyConnect 웹 보안 클라이언트 프로파일을 통해 구성됩니다.

Cisco ScanCenter는 Cisco Cloud Web Security용 관리 포털입니다. Cisco ScanCenter를 사용하여 생성되거나 구성된 일부 구성 요소 또한 AnyConnect 웹 보안 클라이언트 프로파일에서 통합됩니다.

참고 ISE 서버는 웹 보안 클라이언트 프로파일의 Exceptions(예외) 창에서 구성된 정적 예외 목록에 항상 나열되어야 합니다.

일반적인 웹 보안 구성

프로시저

단계 **1** 클라이언트 프로파일의 Cisco Cloud Web Security 스캐닝 프록시를 구성하십시오.

단계 **2** 프로파일 편집기의 Cisco Cloud Web Security 스캐닝 프록시 기존 목록과 http://www.scansafe.cisco.com/ 웹사이트에서 다운로드한 스캐닝 프록시 목록을 비교했을 때 일치하지 않는 경우, 스캐닝 프록시 목록 업데이트 (선택 사항)

단계 **3** 사용자에게 스캐닝 프록시 표시 또는 숨기기(선택 사항)

단계 **4** 기본 스캐닝 프록시 선택

단계 **5** HTTPS 웹 트래픽을 필터링하도록 HTTP(S) 트래픽 수신 대기 포트 지정 (선택 사항)

단계 **6** 웹 스캐닝 서비스에서 엔드포인트 트래픽 제외 또는 포함에 대한 호스트, 프록시 또는 정적 예외 사항을 구성하십시오. 이 구성을 통해 지정된 IP 주소로부터 네트워크 트래픽에 대한 평가를 제한합니다.

단계 **7** 사용자 제어 구성 및 가장 빠른 스캐닝 프록시 응답 시간 계산. 이 구성을 통해 사용자가 연결할 Cisco Cloud Web Security 스캐닝 프록시를 선택합니다.

단계 **8** 기업 LAN에서 시작되는 네트워크 트래픽이 Cisco Cloud Web Security를 우회하게 하려면 신뢰할 수 있는 보안 네트워크 탐지 사용

단계 **9** Cisco Cloud Web Security 프록시에 대한 인증 및 그룹 멤버십 전송 구성. 이 구성을 통해 기업 도메인 또는 Active Directory 그룹의 Cisco ScanCenter를 기반으로 사용자를 인증합니다.

클라이언트 프로파일의 **Cisco Cloud Web Security** 스캐닝 프록시

Cisco Cloud Web Security는 웹 콘텐츠를 분석하여 안전한 콘텐츠를 브라우저에 전달하고 보안 정책을 기반으로 악의적인 콘텐츠를 차단합니다. 스캐닝 프록시는 Cisco Cloud Web Security가 웹 콘텐츠를 분석하는 Cisco Cloud Web Security 프록시 서버입니다. AnyConnect 웹 보안 프로파일 편집기의 스캐닝 프록시 패널은 AnyConnect 웹 보안 모듈이 웹 네트워크 트래픽을 전송하는 Cisco Cloud Web Security 스캐닝 프록시를 정의합니다.

IPv6 웹 트래픽에 대한 지침

IPv6 주소, 도메인 이름, 주소 범위 또는 와일드카드의 예외가 지정되어 있지 않으면 IPv6 웹 트래픽이 스캐닝 프록시로 전송됩니다. 사용자가 연결하려는 URL의 IPv4 주소가 있는 경우 스캐닝 프록시

가 DNS를 조회합니다. 스캐닝 프록시가 IPv4 주소를 찾으면 연결을 위해 사용합니다. IPv4 주소를 찾을 수 없는 경우 연결이 끊깁니다.

모든 IPv6 트래픽이 검사 프록시를 우회하게 하려면 모든 IPv6 트래픽에 대해 ::/0 정적 예외를 추가하십시오. 이 예외를 통해 모든 IPv6 트래픽이 모든 스캐닝 프록시를 우회하므로 IPv6 트래픽이 웹 보안 모듈을 통해 보호되지 않습니다.

참고 Windows를 실행하는 컴퓨터에서 AnyConnect가 사용자 ID를 지정하지 않는 경우 내부 IP 주소가 사용자 ID처럼 사용됩니다. 예를 들어 enterprise_domains 프로파일 항목을 지정하지 않은 경우 내부 IP 주소를 사용하여 Cisco ScanCenter에서 리포트를 생성합니다.

Mac OS X을 실행하는 컴퓨터에서 Mac이 도메인으로 바인딩되는 경우 웹 보안 모듈이 로그인된 컴퓨터의 도메인을 보고할 수 있습니다. 도메인으로 바인딩되지 않는 경우에는 웹 보안 모듈이 Mac의 IP 주소 또는 현재 로그인된 사용자 이름을 보고할 수 있습니다.

사용자가 스캐닝 프록시를 선택하는 방법

프로파일이 구성된 방식에 따라 사용자가 스캐닝 프록시를 선택하거나 AnyConnect 웹 보안 모듈이 사용자를 응답 시간이 가장 빠른 스캐닝 프록시에 연결합니다.

- 클라이언트 프로파일이 사용자 제어를 허용하는 경우 사용자가 Cisco AnyConnect Secure Mobility Client 웹 보안 트레이의 Settings(설정) 탭에서 스캐닝 프록시를 선택할 수 있습니다.
- 클라이언트 프로파일이 자동 스캐닝 프록시 선택 환경 설정을 활성화한 경우 AnyConnect 웹 보안 모듈에서 스캐닝 프록시를 가장 빠른 것부터 가장 느린 것까지 순서대로 나열하고 사용자를 응답 시간이 가장 빠른 스캐닝 프록시에 연결합니다.
- 클라이언트 프로파일이 사용자 제어를 허용하지 않지만 **Automatic Scanning Proxy Selection(**자동 스캐닝 프록시 선택**)** 이 활성화되어 있는 경우, 응답 시간이 원래 연결된 기본 스캐닝 프록시보다 훨씬 더 빠르면 AnyConnect 웹 보안이 사용자를 기본 스캐닝 프록시에서 응답 시간이 가장 빠른 스캐닝 프록시로 전환합니다.
- 사용자가 현재 스캐닝 프록시로부터 로밍하기 시작하고 클라이언트 프로파일에 **Automatic Scanning Proxy Selection(**자동 스캐닝 프록시 선택**)** 이 구성되어 있는 경우, 응답 시간이 현재 스캐닝 프록시보다 훨씬 더 빠르면 AnyConnect 웹 보안이 사용자를 새 스캐닝 프록시로 전환합니다.

AnyConnect 웹 보안이 Windows의 확장된 AnyConnect 트레이 아이콘, Advanced Settings(고급 설정) 탭 및 AnyConnect GUI의 Advanced Statistics(고급 통계)에서 활성화된 스캐닝 프록시 이름을 표시하므로 사용자는 연결된 스캐닝 프록시를 알 수 있습니다.

스캐닝 프록시 목록 업데이트

웹 보안 프로파일 편집기의 스캐닝 프록시 목록은 편집할 수 없습니다. 웹 보안 프로파일 편집기의 테이블에서 Cisco Cloud Web Security 스캐닝 프록시를 추가하거나 제거할 수 없습니다.

웹 보안 프로파일 편집기를 시작하면 Cisco Cloud Web Security 웹사이트를 통해 스캐닝 프록시 목록을 자동으로 업데이트하여 스캐닝 프록시의 현재 목록을 유지합니다.

AnyConnect 웹 보안 클라이언트 프로파일을 추가 또는 편집할 때 프로파일 편집기는 Cisco Cloud Web Security 스캐닝 프록시의 기존 목록과 http://www.scansafe.cisco.com 에서 다운로드한 스캐닝 프록시 목록을 비교합니다. 목록이 오래된 경우, "스캐닝 프록시 목록이 최신이 아닙니다."라는 메시지와 Update List(목록 업데이트)라는 레이블의 명령 버튼이 표시됩니다. 스캐닝 프록시 목록을 가장 최신의 Cisco Cloud Web Security 스캐닝 프록시 목록으로 업데이트하려면 **Update List(**목록 업데이트**)** 를 클릭하십시오.

Update List(목록 업데이트)를 클릭하면 프로파일 편집기가 기존 구성을 최대한 많이 유지합니다. 프로파일 편집기가 기본 스캐닝 프록시 설정 및 기존 Cisco Cloud Web Security 스캐닝 프록시의 표시/숨기기 설정을 유지합니다.

사용자에게 스캐닝 프록시 표시 또는 숨기기

사용자가 ASA에 대한 VPN 연결을 설정하면 ASA가 클라이언트 프로파일을 엔드포인트에 다운로드합니다. AnyConnect 웹 보안 클라이언트 프로파일은 어떤 Cisco Cloud Web Security 스캐닝 프록시가 사용자에게 표시되는지 판단합니다.

로밍 사용자에 대한 이점을 최대화하려면 모든 사용자에게 Cisco Cloud Web Security 스캐닝 프록시를 모두 표시하는 것이 좋습니다.

사용자는 다음과 같은 방법으로 AnyConnect 웹 보안 클라이언트 프로파일의 스캐닝 프록시 목록에서 "Display(표시)"가 표시된 스캐닝 프록시와 상호 작용합니다.

- Cisco Cloud Web Security 스캐닝 프록시는 Cisco AnyConnect Secure Mobility Client 인터페이스의 웹 보안 패널 Advanced(고급) 설정에서 사용자에게 표시됩니다.
- AnyConnect 웹 보안 모듈은 스캐닝 프록시를 응답 시간 순으로 정렬할 때 "Display(표시)"가 표시된 Cisco Cloud Web Security 스캐닝 프록시를 테스트합니다.
- 사용자는 프로파일이 사용자 제어를 허용하는 경우, 연결하는 Cisco Cloud Web Security 스캐닝 프록시 종류를 선택할 수 있습니다.
- AnyConnect 웹 보안 클라이언트 프로파일의 스캐닝 프록시 테이블에 “Hide(숨기기)”가 표시된 Cisco Cloud Web Security 스캐닝 프록시는 스캐닝 프록시를 응답 시간 순으로 정렬할 때 사용자에게 표시되거나 평가되지 않습니다. 사용자는 “Hide(숨기기)”가 표시된 스캐닝 프록시에 연결할 수 없습니다.

시작하기 전에

AnyConnect 웹 보안 클라이언트 프로파일을 생성하십시오.

프로시저

단계 **1** 다음 방법 중 하나를 사용하여 웹 보안 로파일 편집기를 시작합니다.

- ASDM을 열고 **Configuration(**구성**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**)** > **AnyConnect Client Profile(AnyConnect** 클라이언트 프로파일**)**을 선택합니다.

- Windows의 독립 실행형 모드에서 **Start(**시작**)** > **All Programs(**모든 프로그램**)** > **Cisco** > **Cisco AnyConnect Profile Editor(Cisco AnyConnect** 프로파일 편집기**)** > **Web Security Profile Editor(**웹 보안 프로파일 편집기**)**를 선택합니다.

단계 **2** 편집할 웹 보안 클라이언트 프로파일을 여십시오.

단계 **3** Cisco Cloud Web Security 스캐닝 프록시를 숨기거나 표시하려면 다음을 수행하십시오.

- 숨기려는 스캐닝 프록시를 선택하고 Hide(숨기기)를 클릭하십시오.
- 표시할 스캐닝 프록시의 이름을 선택하고 Display(표시)를 클릭하십시오. 모든 Cisco Cloud Web Security 스캐닝 프록시를 표시하는 것이 권장되는 구성입니다.

단계 **4** AnyConnect 웹 보안 클라이언트 프로파일을 저장하십시오.

기본 스캐닝 프록시 선택

사용자는 네트워크에 처음 연결할 때 기본 스캐닝 프록시로 라우트됩니다. 기본적으로 생성 프로파일은 다음과 같은 Cisco Cloud Web Security 스캐닝 프록시 특성을 가지고 있습니다.

- 스캐닝 프록시 목록은 사용자가 액세스할 수 있고 모두 "Display(표시)"라고 표시된 모든 Cisco Cloud Web Security 스캐닝 프록시로 채워집니다.
- 기본 Cisco Cloud Web Security 스캐닝 프록시는 미리 선택되어 있습니다.
- AnyConnect 웹 보안 모듈이 HTTP 트래픽을 수신 대기하고 있는 포트 목록은 일부 포트에서 프로비저닝됩니다.

프로시저

단계 **1** 다음 방법 중 하나를 사용하여 웹 보안 로파일 편집기를 시작합니다.

- ASDM을 열고 **Configuration(**구성**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**)** > **AnyConnect Client Profile(AnyConnect** 클라이언트 프로파일**)**을 선택합니다.
- Windows의 독립 실행형 모드에서 **Start(**시작**)** > **All Programs(**모든 프로그램**)** > **Cisco** > **Cisco AnyConnect Profile Editor(Cisco AnyConnect** 프로파일 편집기**)** > **Web Security Profile Editor(**웹 보안 프로파일 편집기**)**를 선택합니다.

단계 **2** 편집할 웹 보안 클라이언트 프로파일을 여십시오.

단계 **3** **Default Scanning Proxy(**기본 스캐닝 프록시**)** 필드에서 기본 스캐닝 프록시를 선택하십시오.

단계 **4** AnyConnect 웹 보안 클라이언트 프로파일을 저장하십시오.

HTTP(S) 트래픽 수신 대기 포트 지정

Scan Safe 웹 스캐닝 서비스는 기본적으로 HTTP 웹 트래픽을 분석하므로 이를 구성하면 HTTPS 웹 트래픽을 필터링할 수 있습니다. 웹 보안 클라이언트 프로파일에서, 이러한 유형의 네트워크 트래픽을 "수신 대기"하려는 웹 보안 포트를 지정하십시오.

프로시저

단계 **1** 다음 방법 중 하나를 사용하여 웹 보안 로파일 편집기를 시작합니다.

- ASDM을 열고 **Configuration(**구성**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**)** > **AnyConnect Client Profile(AnyConnect** 클라이언트 프로파일**)**을 선택합니다.
- Windows의 독립 실행형 모드에서 **Start(**시작**)** > **All Programs(**모든 프로그램**)** > **Cisco** > **Cisco AnyConnect Profile Editor(Cisco AnyConnect** 프로파일 편집기**)** > **Web Security Profile Editor(**웹 보안 프로파일 편집기**)**를 선택합니다.

단계 **2** 편집할 웹 보안 클라이언트 프로파일을 여십시오.

단계 **3** **Traffic Listen Port(**트래픽 수신 대기 포트**)** 필드에 HTTP 트래픽, HTTPS 트래픽 또는 두 가지를 모두 "수신 대기"하기를 원하는 웹 보안 모듈의 논리적인 포트 번호를 입력하십시오.

단계 **4** 웹 보안 클라이언트 프로파일을 저장합니다.

공용 프록시를 구성하도록 **Windows** 인터넷 옵션 구성

공용 프록시는 일반적으로 웹 트래픽을 익명화하는 데 사용됩니다. 인증 프록시 서버라고도 하는 공용 프록시 서버에는 사용자 이름과 비밀번호가 필요할 수도 있습니다. AnyConnect 웹 보안은 두 가지 인증 유형(기본 및 NTLM)을 지원합니다. 프록시 서버가 인증이 필요하도록 구성되어 있으면 AnyConnect 웹 보안은 런타임에 프록시를 탐지하고 인증 프로세스를 관리합니다. 프록시 서버에 정상적으로 인증되면 AnyConnect 웹 보안은 공용 프록시를 통해 웹 트래픽을 Cisco Cloud Web Security 스캐닝 프록시로 라우팅합니다. AnyConnect 웹 보안은 프록시 자격 증명을 암호화하여 메모리에 안전하게 캐시하므로 사용자가 프록시 네트워크에서 비프록시 네트워크로 이동했다가 같은 네트워크로 돌아오더라도 자격 증명을 다시 요구하지 않습니다. 공용 프록시 사용 시에는 서비스를 다시 시작할 필요가 없습니다. 사용자가 비프록시 네트워크로 이동하면 AnyConnect 웹 보안은 런타임에 해당 이동을 자동으로 탐지하여 Cisco Cloud Web Security 스캐닝 프록시로 웹 트래픽을 직접 보내기 시작합니다.

Windows 인터넷 옵션이 클라이언트에서 공용 프록시를 사용하도록 구성되어 있으면 AnyConnect는 해당 연결을 사용합니다.

참고 Windows에서는 기본 및 NTLM 공용 프록시가 지원됩니다. Mac에서는 기본 공용 프록시만 지원됩니다.

1. Internet Explorer 또는 제어판에서 Internet Options(인터넷 옵션)를 엽니다.
2. Connections(연결) 탭을 선택하고 **LAN settings(LAN** 설정**)**를 클릭합니다.
3. 프록시 서버를 사용하도록 LAN을 구성합니다.
4. 프록시 서버의 IP 주소 또는 호스트 이름을 입력합니다. FTP/HTTP/HTTPS용으로 별도의 프록시가 구성되어 있는 경우에는 HTTPS 프록시만 고려합니다.

제한 사항

- 공용 프록시를 통한 IPv6 및 TND는 지원되지 않습니다.
- AnyConnect 웹 보안 예외 목록에 프록시 IP를 포함해서는 안 됩니다. 프록시 IP를 포함하는 경우 트래픽이 AnyConnect 웹 보안으로 전송되지 않습니다.
- 프록시 포트가 기본 웹 포트와 다른 경우에는 AnyConnect 웹 보안 프로파일의 kdf 수신 대기 포트 목록에 프록시 포트를 추가해야 합니다.

웹 스캐닝 서비스에서 엔드포인트 트래픽 제외 또는 포함

특정 네트워크 트래픽을 Cisco Cloud Web Security 스캐닝에 포함하거나 스캐닝에서 제외하려면 웹 보안 프로파일 편집기를 사용하여 해당 트래픽에 대한 예외를 구성하십시오. 다음과 같이 예외의 여러 범주를 구성할 수 있습니다.

- Host Exceptions(호스트 예외) 또는 Host Inclusions(호스트 포함) - Host Exceptions(호스트 예외)를 구성하면 입력하는 IP 주소(공용/사설, 호스트 이름 또는 서브넷)를 우회합니다. Host Inclusions(호스트 포함)를 구성하면 입력하는 IP 주소(공용/사설, 호스트 이름 또는 서브넷)를 웹 보안 프록시로 전달하며 나머지 트래픽은 모두 우회합니다.

  참고 AnyConnect는 Host Exceptions(호스트 예외)에 나와 있는 트래픽을 계속 가로챌 수 있습니다.

- Proxy Exceptions(프록시 예외) - 여기에 나열된 내부 프록시 서버는 스캐닝에서 제외됩니다.
- Static Exceptions(정적 예외) - 여기에 나열된 IP 주소 또는 호스트 이름은 스캐닝 및 AnyConnect에서 제외됩니다.

ISE 서버 요건

ISE 서버는 웹 보안 클라이언트 프로파일의 Exceptions(예외) 창에서 구성된 정적 예외 목록에 항상 나열되어야 합니다. 또한 웹 보안 모듈이 ISE Posture 프로브를 우회하여 ISE Posture 클라이언트가 ISE 서버에 연결되어야 합니다. ISE Posture 프로파일은 다음의 순서에 따라 네트워크 프로브를 전송하여 ISE 서버를 검색합니다.

1. 기본 게이트웨이

2. 검색 호스트
3. enroll.cisco.com
4. 이전에 연결한 ISE 서버

호스트 예외 제외 또는 포함

시작하기 전에

- 피싱 사이트를 포함할 수 있으므로 *.cisco.*와 같이 최상위 도메인의 양쪽에 와일드카드를 사용하지 마십시오.
- 기본 호스트 예외 항목을 삭제하거나 변경하지 마십시오.

Host Exceptions(호스트 제외) 또는 Host Inclusions(호스트 포함)를 구성할 수 있습니다. Host Exceptions(호스트 제외)를 선택하면 Cisco Cloud Web Security 프록시가 지정된 IP 주소를 우회합니다. Host Inclusions(호스트 포함)를 선택하면 지정된 IP 주소가 Cisco Cloud Web Security 프록시로 전달되고 나머지 모든 트래픽은 우회됩니다. 참고로 AnyConnect는 제외된 호스트 예외에서 인터넷 트래픽을 계속 가로챌 수 있습니다. 웹 보안 및 AnyConnect에서 모두 트래픽을 제외하려면 정적 예외를 구성하십시오.

프로시저

단계 **1** Host Exceptions(호스트 제외) 또는 Host Inclusions(호스트 포함)를 선택합니다.

단계 **2** 1단계에서 선택한 항목에 따라 우회 또는 전달할 IP 주소(공용/사설, 호스트 이름 또는 서브넷)를 추가합니다.

단계 **3** 다음 구문을 사용하여 서브넷과 IP 주소를 입력하십시오.

구문	예
개별 IPv4 및 IPv6 주소	10.255.255.255 2001:0000:0234:C1AB:0000:00A0:AABC:003F
CIDR(Classless Inter-Domain Routing, 클래스리스 도메인 간 라우팅) 표시법	10.0.0.0/8 2001:DB8::/48
정규화된 도메인 이름	windowsupdate.microsoft.com ipv6.google.com 참고 example.com과 같은 부분 도메인은 지원되지 않습니다.
정규화된 도메인 이름 또는 IP 주소의 와일드카드	127.0.0.* *.cisco.com

참고 Web Security가 호스트 예외 목록의 도메인 이름을 사용하도록 구성되어 있으면 사용자가 Web Security 프록시를 우회하기 위해 호스트 HTTP 헤더 항목을 스푸핑할 수 있습니다. 예외 목록에서 호스트 이름 대신 IP 주소를 사용하면 이러한 위험을 완화할 수 있습니다.

Web Security 및 로밍 보안 호환성에 필요한 호스트 예외

Umbrella 로밍 보안 모듈을 Web Security 모듈과 함께 구축하는 경우에는 *.opendns.com을 호스트 예외로 구성해야 합니다. 이렇게 하지 않으면 Umbrella 로밍 보안 DNS 보호를 완전히 우회하게 됩니다.

또한 Web Security 및 Umbrella 로밍 보안 모듈 호환성에 필요한 정적 예외, 234 페이지에서 설명하는 정적 예외 제외도 구성해야 합니다.

프록시 예외 제외

프록시 예외 영역에서 권한 있는 내부 프록시의 IP 주소를 입력합니다(예: `172.31.255.255`).

필드에 IPv4 및 IPv6 주소를 지정할 수 있지만, 주소와 함께 포트 번호를 지정할 수 없습니다. CIDR 주석을 사용하여 IP 주소를 지정할 수 없습니다.

IP 주소를 지정하여 Cisco Cloud Web Security가 이 서버에 대한 웹 데이터를 가로채고 SSL을 사용하여 주소를 통해 데이터를 터널링하는 것을 방지합니다. 이를 통해 프록시 서버를 중단 없이 작동할 수 있습니다. 프록시 서버를 여기에서 추가하지 않는 경우, SSL 터널로 Cisco Cloud Web Security 트래픽을 확인합니다.

프록시 서버를 통과하는 브라우저 트래픽을 제외하려는 경우에는 해당 트래픽이 전달되지 않도록 Host Exceptions(호스트 예외)에 해당 호스트 이름을 나열해야 합니다. Proxy Exception(프록시 예외) 목록에 나열되어 있지 않은 프록시를 통과하는 트래픽에 대해서만 정적 예외를 구성할 수는 없습니다.

이 목록에 없는 프록시의 경우 웹 보안에서 SSL을 사용하여 프록시를 통해 터널링을 시도합니다. 따라서 사용자가 인터넷 액세스를 위해 프록시를 네트워크 외부로 이동시켜야 하는 다른 회사 사이트에 있는 경우, Cisco Cloud Web Security는 개방형 인터넷 연결에서 작업하는 것과 마찬가지로 동일한 수준의 지원을 제공합니다.

정적 예외 제외

Cisco Cloud Web Security를 우회해야 하는 트래픽을 판단하고 CIDR(Classless Inter-Domain Routing, 클래스리스 도메인 간 라우팅) 표시법에 개별 IP 주소의 목록 또는 IP 주소 범위를 추가합니다. 목록에 VPN 게이트웨이의 진입 IP 주소를 포함하십시오. AnyConnect 릴리스 4.3.02039 이상 버전에서는 이제 스캐닝에서 제외할 호스트 이름을 추가할 수 있습니다. Web Security은 검사를 위해 Cloud Web Security 프록시로 해당 HTTP/HTTPS 트래픽을 전달하지 않습니다.

IP 주소가 같은 호스트 이름이 여러 개인데 그중 하나만 Static Exceptions(정적 예외) 목록에 구성되어 있으면 Web Security에서 해당 트래픽을 제외합니다.

http://www.ietf.org/rfc/rfc1918.txt 에서 설명한 사설 IP 주소는 기본적으로 정적 예외 목록에 포함되어 있습니다.

참고 정적 예외 목록 범위에 포함되는 IP 주소를 사용하는 프록시 서버가 있는 경우, 해당 예외를 호스트 예외 목록으로 이동하십시오. 예를 들어 10.0.0.0/8은 정적 예외 목록에 표시됩니다. 10.1.2.3에 프록시가 있으면 10.0.0.0/8을 호스트 예외 목록으로 이동하십시오. 그렇지 않으면 이 프록시로 전송되는 트래픽이 Cloud Web Security를 우회합니다.

CIDR 표시법을 사용하여 IPv4 및 IPv6 주소와 주소의 범위를 지정할 수 있습니다. 정규화된 도메인 이름을 지정할 수 없으며 IP 주소에서 와일드카드를 사용할 수 없습니다. 올바른 구문 예는 다음과 같습니다.

```
10.10.10.5
192.0.2.0/24
```

참고 SSL VPN 집중디바이스의 IP 주소를 정적 제외 목록에 추가하십시오.

Web Security 및 Umbrella 로밍 보안 모듈 호환성에 필요한 정적 예외

Umbrella 로밍 보안 모듈과 Web Security 모듈 간의 상호운용성을 보장하려면 AnyConnect로 프로비저닝되는 Web Security 프로파일에서 다음 예외를 구성해야 합니다.

- 77.67.54.0/27
- 77.67.54.32/27
- 77.67.54.64/27
- 77.67.54.96/27
- 77.67.54.128/27
- 77.67.54.160/27
- 67.215.64.0/19
- 204.194.232.0/21
- 208.67.216.0/21
- 208.69.32.0/21
- 185.60.84.0/22
- 146.112.61.0/22
- 146.112.128.0/18

또한 Web Security 및 로밍 보안 호환성에 필요한 호스트 예외, 233 페이지에서 설명하는 호스트 예외 제외도 구성해야 합니다.

사용자 제어 구성 및 가장 빠른 스캐닝 프록시 응답 시간 계산

사용자가 연결할 Cisco Cloud Web Security 스캐닝 프록시를 선택하도록 하려면 다음을 수행하십시오.

프로시저

단계 **1** 다음 방법 중 하나를 사용하여 웹 보안 로파일 편집기를 시작합니다.

- ASDM을 열고 **Configuration(**구성**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**)** > **AnyConnect Client Profile(AnyConnect** 클라이언트 프로파일**)**을 선택합니다.
- Windows의 독립 실행형 모드에서 **Start(**시작**)** > **All Programs(**모든 프로그램**)** > **Cisco** > **Cisco AnyConnect Profile Editor(Cisco AnyConnect** 프로파일 편집기**)** > **Web Security Profile Editor(**웹 보안 프로파일 편집기**)**를 선택합니다.

단계 **2** 편집할 웹 보안 클라이언트 프로파일을 여십시오.

단계 **3** **Preferences(**환경 설정**)**를 클릭합니다.

단계 **4** **User Controllable(**사용자 제어 가능**)**을 선택합니다. 이 옵션이 기본 설정입니다. 사용자 제어 가능 옵션은 사용자가 AnyConnect 인터페이스에서 자동 타워 선택 및 응답 시간 기준으로 스캐닝 프록시 정렬 설정을 변경할 수 있는지 여부를 결정합니다.

단계 **5** 웹 보안의 경우 스캐닝 프록시를 자동으로 선택하려면 **Automatic Scanning Proxy Selection(**자동 스캐닝 프록시 선택**)**을 선택합니다. 이 경우 **Order Scanning Proxies by Response Time(**응답 시간 기준으로 스캐닝 프록시 정렬**)**이 자동으로 선택됩니다.

- **Automatic Scanning Proxy Selection(**자동 스캐닝 프록시 선택**)**을 선택한 경우, 웹 보안은 가장 빠르게 응답하는 스캐닝 프록시를 판단하고 사용자를 해당 스캐닝 프록시에 자동으로 연결합니다.
- **Automatic Scanning Proxy Selection(**자동 스캐닝 프록시 선택**)**을 선택하지 않은 상태에서 **Order Scanning Proxies by Response Time(**응답 시간 기준으로 스캐닝 프록시 정렬**)**이 계속 선택된 상태이면, 사용자에게 연결할 수 있는 스캐닝 프록시 목록이 가장 빠른 응답 시간부터 가장 느린 응답 시간 순서로 표시됩니다.
- **Automatic Scanning Proxy Selection(**자동 스캐닝 프록시 선택**)**을 선택하지 않은 경우, 사용자는 AnyConnect 사용자 인터페이스에서 이 기능을 활성화할 수 있지만 한 번 활성화하면 다시 끌 수 없습니다.

  참고 Automatic Scanning Proxy Selection(자동 스캐닝 프록시 선택)을 활성화한 경우, 일시적인 통신 중단 및 장애가 발생하여 활성 스캐닝 프록시 선택이 자동으로 변경될 수 있습니다. 스캐닝 프록시를 변경하면 경우에 따라 다른 언어를 사용하는 다른 국가에 있는 스캐닝 프록시에서 검색 결과가 반환되는 것과 같은 예기치 않은 동작이 발생시켜 바람직하지 않을 수 있습니다.

단계 **6** **Order Scanning Proxies by Response Time(**응답 시간 기준으로 스캐닝 프록시 정렬**)**을 선택한 경우, 가장 빠르게 응답하는 스캐닝 프록시를 계산하기 위해 다음 설정을 구성하십시오.

- **Enable Test Interval(**테스트 간격 활성화**)**: 각 성능 테스트 실행 사이의 시간(시간/분 단위)이며 기본적으로 2분입니다. 테스트가 실행되지 않게 하려면 Enable Test Interval(테스트 간격 활성화) 확인란을 선택 취소하여 테스트 간격을 해제합니다.
- **Test Inactivity Timeout(**테스트 비활성화 시간 제한**)**: 사용자 비활성화로 인해 웹 보안이 응답 시간 테스트를 일시 중지한 이후의 시간(분)입니다. 웹 보안은 스캐닝 프록시에서 연결 시도가 있는 경우 바로 테스트를 재개합니다. 고객 지원 부서에서 지시하지 않는 한 이 설정을 변경하지 마십시오.

참고 **Ordering Scanning Proxies by Response Time(**응답 시간 기준으로 스캐닝 프록시 정렬**)** 테스트는 테스트 간격 시간 기준으로 계속 실행되며 예외사항은 다음과 같습니다.

- 신뢰할 수 있는 보안 네트워크 탐지가 활성화되어 있고 머신이 기업 LAN에 있음을 탐지했습니다.
- 웹 보안 라이센스 키가 분실되었거나 유효하지 않습니다.
- 사용자가 구성된 시간 동안 비활성화 상태로 테스트 비활성화 시간 제한 임계값에 도달했습니다.

단계 **7** Secure Trusted Network Detection(신뢰할 수 있는 보안 네트워크 탐지)을 클릭하여 활성화합니다. 이 기능은 엔드포인트가 회사 LAN에 존재하는 경우 물리적으로 또는 VPN 연결을 통해 탐지합니다. 이 기능이 활성화된 경우 기업 LAN에서 발생한 네트워크 트래픽은 Cisco Cloud Web Security 스캐닝 프록시를 우회합니다.

단계 **8** https 필드에서 신뢰할 수 있는 서버 각각의 URL을 입력한 다음 **Add(**추가**)**를 클릭합니다. URL에는 포트 주소가 포함될 수 있습니다. 프로파일 편집기에서 신뢰할 수 있는 서버에 연결을 시도합니다. 연결이 불가능하지만 서버 인증서의 SHA-256 해시를 알고 있는 경우 **Certificate hash(**인증서 해시**)** 상자에 이를 입력하고 **Set(**설정**)**를 클릭합니다.

단계 **9** 웹 보안 클라이언트 프로파일을 저장합니다.

다음에 수행할 작업

자세한 내용은 *ScanCenter* 관리자 설명서, 릴리스 *5.2*를 참조하십시오.

신뢰할 수 있는 보안 네트워크 탐지 사용

신뢰할 수 있는 보안 네트워크 탐지 기능은 엔드포인트가 회사 LAN에 존재하는 경우 물리적으로 또는 VPN 연결을 통해 탐지합니다. 신뢰할 수 있는 보안 네트워크 탐지 기능이 활성화되어 있는 경우, 회사 LAN에서 시작되는 모든 네트워크 트래픽이 Cisco Cloud Web Security 스캐닝 프록시를 우회합니다. 이 트래픽의 보안은 Cisco Cloud Web Security가 아닌 다른 방법 및 회사 LAN의 디바이스 설정에 따라 관리됩니다.

신뢰할 수 있는 보안 네트워크 탐지 기능은 클라이언트가 알려진 URL(주소, IP 또는 FQDN)에서 서버에 있는 SSL 인증서의 SHA-256 해시(지문)를 사용하는 기업 네트워크에 연결되어 있는지 확인합니다. 인증서에서 사용하는 암호화 알고리즘은 SHA-256 해시를 사용할 수 있는 경우 외에는 문제가 되지 않습니다.

신뢰할 수 있는 보안 네트워크 탐지 기능을 사용하지 않도록 선택하고 네트워크에 프록시가 있는 경우(예를 들어 Cisco Cloud Web Security Connector), 프로파일 편집기의 Exceptions(예외) 패널에 있는 프록시 예외 목록에 각 프록시를 추가해야 합니다.

다중 서버: 2개 이상의 서버를 정의하는 경우, 클라이언트가 두 번 연속으로 연결을 시도해도 첫 번째 서버에 연결하지 못하면 두 번째 서버에 연결을 시도합니다. 목록에 있는 모든 서버에 연결을 시도한 후, 클라이언트가 5분 동안 기다린 다음 첫 번째 서버에 다시 연결을 시도합니다.

참고 내부 네트워크 외부에서 작동할 때 신뢰할 수 있는 보안 네트워크 탐지 기능은 DNS 요청을 작성하고 제공된 HTTPS 서버에 연결을 시도합니다. Cisco에서는 내부 네트워크 외부에서 사용 중인 머신에서 이러한 요청을 통해 사용자 조직의 명칭 및 내부 구조가 노출되지 않도록 앨리어싱을 사용할 것을 적극 권장합니다.

시작하기 전에

- 프록시 예외 제외
- 웹 보안의 영향을 받지 않는 트래픽을 필요로 하는 DLP(Data Loss Prevention, 데이터 유출 방지) 어플라이언스와 같은 일부 서드파티 솔루션에 대해 신뢰할 수 있는 보안 네트워크 탐지 기능을 구성해야 합니다.
- 프로파일 편집 시 SSL 인증서가 호스팅된 서버에 직접 연결되어 있는지 확인하십시오.

프로시저

단계 **1** 다음 방법 중 하나를 사용하여 웹 보안 로파일 편집기를 시작합니다.

- ASDM을 열고 **Configuration**(구성) > **Remote Access VPN**(원격 액세스 **VPN**) > **Network (Client) Access**(네트워크(클라이언트) 액세스) > **AnyConnect Client Profile**(**AnyConnect** 클라이언트 프로파일)을 선택합니다.
- Windows의 독립 실행형 모드에서 **Start**(시작) > **All Programs**(모든 프로그램) > **Cisco** > **Cisco AnyConnect Profile Editor**(**Cisco AnyConnect** 프로파일 편집기) > **Web Security Profile Editor**(웹 보안 프로파일 편집기)를 선택합니다.

단계 **2** 편집하려는 웹 보안 클라이언트 프로파일을 엽니다.

단계 **3** Web Security(웹 보안) 트리 창에서 **Preferences**(환경 설정) 를 클릭합니다.

단계 **4** **Enable Trusted Network Detection**(신뢰할 수 있는 네트워크 탐지 활성화)을 선택합니다.

단계 **5** **https** 필드에서 신뢰할 수 있는 서버 각각의 URL을 입력한 다음 **Add**(추가)를 클릭합니다. URL에는 포트 주소가 포함될 수 있습니다. 프로파일 편집기에서 신뢰할 수 있는 서버에 연결을 시도합니다.

연결이 불가능하지만 서버 인증서의 SHA-256 해시를 알고 있는 경우 **Certificate hash(**인증서 해시**)** 상자에 이를 입력하고 **Set(**설정**)**를 클릭합니다.

참고 프록시 뒤에 있는 신뢰할 수 있는 서버는 지원되지 않습니다.

단계 **6** 웹 보안 클라이언트 프로파일을 저장합니다.

신뢰할 수 있는 보안 네트워크 탐지 사용 안 함

신뢰할 수 있는 보안 네트워크 탐지를 사용하지 않도록 선택하고 네트워크에 프록시가 있는 경우(예를 들어 Cisco Cloud Web Security Connector), 프로파일 편집기에서 예외 패널에 있는 프록시 예외 목록에 각 프록시를 추가해야 합니다.

Cisco Cloud Web Security 프록시에 대한 인증 및 그룹 멤버십 전송 구성

시작하기 전에

Windows를 사용하여 필터 끄기 및 활성화, 247 페이지

프로시저

단계 **1** 다음 방법 중 하나를 사용하여 웹 보안 로파일 편집기를 시작합니다.

- ASDM을 열고 **Configuration(**구성**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**)** > **AnyConnect Client Profile(AnyConnect** 클라이언트 프로파일**)**을 선택합니다.
- Windows의 독립 실행형 모드에서 **Start(**시작**)** > **All Programs(**모든 프로그램**)** > **Cisco** > **Cisco AnyConnect Profile Editor(Cisco AnyConnect** 프로파일 편집기**)** > **Web Security Profile Editor(**웹 보안 프로파일 편집기**)**를 선택합니다.

단계 **2** 편집하려는 웹 보안 클라이언트 프로파일을 엽니다.

단계 **3** **Authentication(**인증**)**을 클릭하십시오.

단계 **4** **Proxy Authentication License Key(**프록시 인증 라이센스 키**)** 필드에서 회사 키, 그룹 키 또는 Cisco ScanCenter에서 작성한 사용자 키와 일치하는 라이센스 키를 입력합니다. 엔터프라이즈 도메인을 기반으로 사용자를 인증하려면 생성한 회사 키를 입력하십시오. Cisco ScanCenter 또는 Active Directory 그룹을 기준으로 사용자를 인증하려면 생성한 그룹 키를 입력하십시오. 기본적으로 태그는 비어 있습니다. 태그가 비워져 있으면 웹 보안 모듈이 pass-through(통과) 모드에서 작동합니다.

단계 **5** **Service Password(**서비스 비밀번호**)**를 입력합니다. 웹 보안 모듈의 기본 비밀번호는 websecurity입니다. 프로파일을 사용자 정의하는 경우 이 비밀번호를 변경하십시오. 다른 문자를 사용하면 Windows 명령 셸이 제어 문자로 잘못 파악하거나 XML에서 특수한 의미를 지닐 수 있으므로 비밀번호는 영숫자 문자(a-z, A-Z, 0-9) 및 다음과 같은 특수 문자만 포함해야 합니다.

```
~ @ # $ % * - _ + = { } [ ] : , . ? /
```

관리자 권한이 있는 사용자는 이 비밀번호를 통해 웹 보안 서비스를 중지할 수 있습니다. 관리자 권한이 있는 사용자 또는 관리자 권한이 없는 사용자 모두 이 비밀번호 없이 웹 보안 서비스를 시작할 수 있습니다.

단계 **6** 각 HTTP 요청을 통해 스캐닝 프록시 서버 엔터프라이즈 도메인 정보 및 Cisco Cloud Web Security 또는 Active Directory 그룹 정보를 전송합니다. 스캐닝 프록시는 사용자의 도메인 및 그룹 멤버십에 대해 파악한 정보를 기반으로 트래픽 필터링 규칙을 적용합니다.

참고 스캐닝 서버 프록시에 사용자 정의 사용자 이름 및 그룹 정보를 전송하려면 이 단계를 건너뛰고 7단계로 이동하십시오. 엔터프라이즈에서 Active Directory를 사용하지 않는 경우에도 7단계로 건너뛰십시오.

a) **Enable Enterprise Domains(**엔터프라이즈 도메인 활성화**)**를 클릭합니다. 목록에서 **All Domains(**모든 도메인**)**를 클릭합니다. All Domains(모든 도메인) 옵션을 선택한 경우, 해당 머신이 도메인에 있으면 사용자가 속한 도메인과 일치하며 사용자 이름 및 그룹 멤버십 정보가 Cisco Cloud Web Security 스캐닝 프록시에 전송됩니다. 이 옵션은 두 개 이상의 도메인이 존재하는 회사에 유용합니다.

b) 또는 **Specify Individual Domains(**개별 도메인 지정**)**를 클릭합니다.

NetBIOS 형식으로 각 도메인 이름을 입력하고 Add(추가)를 클릭합니다. 예를 들어 `example.cisco.com` 의 NetBIOS 형식은 cisco입니다. DNS 형식(abc.def.com)을 사용하여 도메인 이름을 입력하지 마십시오.

엔터프라이즈 도메인 이름 필드에 도메인 이름을 지정하는 경우, Cisco Cloud Web Security는 현재 로그인한 Active Directory 사용자를 식별하고 사용자의 Active Directory 그룹을 열거하며 해당 정보를 매번 요청을 통해 스캐닝 프록시에 전송합니다.

c) Cisco Cloud Web Security 스캐닝 프록시에 대한 HTTP 요청에서 그룹 정보를 포함 또는 제외하려면 사용 목록에서 **Group Include List(**그룹 포함 목록**)** 또는 **Group Exclude List(**그룹 제외 목록**)**를 클릭합니다. 값은 일치하는 문자열의 하위 문자열이 될 수 있습니다.

Group Include List(그룹 포함 목록**)**. **Group Include List(**그룹 포함 목록**)**를 선택한 후에 Cisco Cloud Web Security 또는 Active Directory 그룹 이름을 그룹 포함 목록에 추가합니다. 이러한 그룹 이름은 HTTP 요청을 통해 Cisco Cloud Web Security 스캐닝 프록시 서버로 전송됩니다. 지정한 엔터프라이즈 도메인의 사용자가 요청하는 경우, HTTP 요청은 사용자의 그룹 멤버십에 따라 필터링됩니다. 사용자가 그룹 구성원이 아닌 경우 HTTP 요청은 필터링 규칙의 기본 집합을 사용하여 필터링됩니다.

Group Exclude List(그룹 제외 목록**)**. **Group Exclude List(**그룹 제외 목록**)**에 Cisco Cloud Web Security 또는 Active Directory 그룹 이름을 추가합니다. 이러한 그룹 이름은 HTTP 요청을 통해 Cisco Cloud Web Security 스캐닝 프록시 서버로 전송되지 않습니다. 사용자가 Group Exclude List(그룹 제외 목록)에 있는 그룹 중 하나에 속하는 경우, 해당 그룹 이름은 스캐닝 프록시 서버에 전송되지 않으며, 사용자의 HTTP 요청은 다른 그룹 멤버십으로 필터링되거나 최소한 Active Directory 또는 Cisco Cloud Web Security 그룹 제휴가 없는 사용자에 대해 정의된 필터링 규칙의 기본 집합으로 필터링됩니다.

단계 **7** 스캐닝 프록시 서버의 사용자 지정 이름을 전송하려면 **Custom matching and reporting for machines not joined to domains(**도메인에 속하지 않은 컴퓨터에 대한 사용자 지정 일치 및 보고**)**를 클릭합니다.

a) 목록에서 컴퓨터의 이름을 사용하려면 **Computer Name(**컴퓨터 이름**)** 을 클릭합니다. 또는 로컬 사용자 이름을 사용하려면 **Local User(**로컬 사용자**)** 를 클릭합니다. 또는 **Custom Name(**사용자 정의 이름**)** 을 클릭하고 사용자 정의 이름을 입력합니다. 이는 문자열로 정의될 수 있습니다. 문자열을 입력하지 않은 경우 컴퓨터의 IP 주소가 스캐닝 프록시 서버에 대신 전송됩니다. 이 사용자 이름 또는 IP 주소는 사용자 정의 사용자의 HTTP 트래픽을 식별하는 Cisco ScanCenter 보고서에서 사용됩니다.

b) **Authentication Group(**인증 그룹**)** 필드에서 최대 256자의 영숫자 문자로 이루어진 사용자 정의 그룹 이름을 입력하고 **Add(**추가**)**를 클릭합니다.

HTTP 요청이 스캐닝 프록시 서버로 전송될 때 사용자 정의 그룹 이름이 전송되고 이 이름과 일치하는 그룹 이름이 스캐닝 프록시 서버에 있는 경우, 해당 HTTP 트래픽은 사용자 정의 그룹 이름과 관련된 규칙에 따라 필터링됩니다. 일치하는 사용자 정의 그룹이 스캐닝 프록시 서버에 정의되지 않은 경우, HTTP 요청은 기본 규칙에 따라 필터링됩니다.

사용자 정의 사용자 이름만 구성하고 사용자 정의 그룹은 구성하지 않은 경우, HTTP 요청은 스캐닝 프록시 서버의 기본 규칙으로만 필터링됩니다.

단계 **8** 웹 보안 클라이언트 프로파일을 저장합니다.

고급 웹 보안 설정

웹 보안 클라이언트 프로파일의 Advanced(고급) 패널은 Cisco 고객 지원 엔지니어가 문제를 해결하는 데 도움을 줄 수 있는 몇 가지 설정을 보여줍니다. 고객 지원을 통해 지시가 있는 경우에만 해당 패널의 설정을 변경하십시오.

프로파일 편집기의 Advanced(고급) 패널에서 다음 작업을 수행하십시오.

- KDF 수신 대기 포트 구성, 240 페이지
- 포트가 수신 연결을 대기하는 방법 구성, 241 페이지
- 시간 제한/재시도가 발생하는 시기 구성, 242 페이지
- DNS 조회, 242 페이지
- 디버그 설정, 242 페이지
- 트래픽 차단 및 허용, 243 페이지

KDF 수신 대기 포트 구성

KDF(Kernel Driver Framework, 커널 드라이버 프레임워크)는 목적지 포트로 트래픽 수신 대기 포트 중 하나를 사용하는 모든 연결을 가로채고 트래픽을 KDF 수신 대기 포트에 전달합니다. 웹 스캐닝 서비스는 KDF 수신 대기 포트로 전달된 모든 트래픽을 분석합니다.

시작하기 전에

고객 지원 부서에서 지시하지 않는 한 이 설정을 변경하지 마십시오.

프로시저

단계 **1** 다음 방법 중 하나를 사용하여 웹 보안 로파일 편집기를 시작합니다.

- ASDM을 열고 **Configuration(**구성**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**)** > **AnyConnect Client Profile(AnyConnect** 클라이언트 프로파일**)**을 선택합니다.
- Windows의 독립 실행형 모드에서 **Start(**시작**)** > **All Programs(**모든 프로그램**)** > **Cisco** > **Cisco AnyConnect Profile Editor(Cisco AnyConnect** 프로파일 편집기**)** > **Web Security Profile Editor(**웹 보안 프로파일 편집기**)**를 선택합니다.

단계 **2** 편집하려는 웹 보안 클라이언트 프로파일을 엽니다.

단계 **3** Web Security(웹 보안) 트리 창에서 **Advanced(**고급**)** 를 클릭합니다.

단계 **4** **KDF Listen Port(KDF** 수신 대기 포트**)** 필드에 KDF 수신 대기 포트를 지정합니다.

단계 **5** 웹 보안 클라이언트 프로파일을 저장합니다.

포트가 수신 연결을 대기하는 방법 구성

서비스 통신 포트는 AnyConnect GUI 구성 요소 및 일부 다른 유틸리티 구성 요소에서 수신되는 연결을 웹 스캐닝 서비스가 수신 대기하는 포트입니다.

시작하기 전에

고객 지원 부서에서 지시하지 않는 한 이 설정을 변경하지 마십시오.

프로시저

단계 **1** 다음 방법 중 하나를 사용하여 웹 보안 로파일 편집기를 시작합니다.

- ASDM을 열고 **Configuration(**구성**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**)** > **AnyConnect Client Profile(AnyConnect** 클라이언트 프로파일**)**을 선택합니다.
- Windows의 독립 실행형 모드에서 **Start(**시작**)** > **All Programs(**모든 프로그램**)** > **Cisco** > **Cisco AnyConnect Profile Editor(Cisco AnyConnect** 프로파일 편집기**)** > **Web Security Profile Editor(**웹 보안 프로파일 편집기**)**를 선택합니다.

단계 **2** 편집할 웹 보안 클라이언트 프로파일을 선택하고 **Edit(**편집**)**를 클릭합니다. **Web Security(**웹 보안**)** 트리 창에서 **Advanced(**고급**)** 를 클릭합니다.

단계 **3** **Service Communication Port(**서비스 통신 포트**)**를 수정합니다.

단계 **4** 웹 보안 클라이언트 프로파일을 저장합니다.

참고 기본값인 5300에서 포트를 변경하는 경우, 웹 보안 서비스 및 AnyConnect GUI 구성 요소를 다시 시작하십시오.

시간 제한/재시도가 발생하는 시기 구성

연결 시간 제한 설정을 사용하여 웹 보안이 스캐닝 프록시를 사용하지 않고 인터넷에 액세스를 시도하기 전에 시간 제한을 설정할 수 있습니다. 설정을 비워둘 경우 기본값인 4초가 사용됩니다. 이 설정을 통해 사용자는 재시도하기 전에 시간이 제한될 때까지 기다리지 않고 유료 네트워크 서비스에 더욱 신속하게 액세스할 수 있습니다.

프로시저

단계 **1** 다음 방법 중 하나를 사용하여 웹 보안 로파일 편집기를 시작합니다.

- ASDM을 열고 **Configuration(**구성**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**)** > **AnyConnect Client Profile(AnyConnect** 클라이언트 프로파일**)**을 선택합니다.
- Windows의 독립 실행형 모드에서 **Start(**시작**)** > **All Programs(**모든 프로그램**)** > **Cisco** > **Cisco AnyConnect Profile Editor(Cisco AnyConnect** 프로파일 편집기**)** > **Web Security Profile Editor(**웹 보안 프로파일 편집기**)**를 선택합니다.

단계 **2** 편집하려는 웹 보안 클라이언트 프로파일을 엽니다.

단계 **3** Web Security(웹 보안) 트리 창에서 **Advanced(**고급**)** 를 클릭합니다.

단계 **4** **Connection Timeout(**연결 시간 제한**)** 필드를 변경합니다.

단계 **5** 웹 보안 클라이언트 프로파일을 저장합니다.

DNS 조회

프로파일 편집기의 Advanced(고급) 패널에는 도메인 이름 서버 조회를 관리하기 위해 여러 개의 필드가 있습니다. 이 설정은 DNS 조회를 위한 최적의 값으로 구성되었습니다.

지침

고객 지원 부서에서 지시하지 않는 한 이 설정을 변경하지 마십시오.

디버그 설정

디버그 수준은 구성 가능한 필드입니다.

지침

고객 지원 부서에서 지시하지 않는 한 이 설정을 변경하지 마십시오.

트래픽 차단 및 허용

Cisco Cloud Web Security 프록시 서버에 대한 연결을 설정할 수 없는 경우, 트래픽을 차단하려면 연결 실패 정책 목록에서 **Fail Close(**실패 닫기**)** 를 선택합니다. 또는 **Fail Open(**실패 열기**)** 을 선택하여 트래픽을 허용합니다.

Cisco Cloud Web Security 프록시 서버에 대한 연결을 설정할 수 없지만, 종속 포털(예: Wi-Fi 핫스팟)이 탐지되는 경우, 트래픽을 허용하려면 **When a captive portal is detected(**종속 포털이 탐지되는 시기**)** 목록에서 **Fail Open(**실패 열기**)** 을 선택합니다. 또는 **Fail Close(**실패 닫기**)** 를 선택하여 트래픽을 차단합니다.

참고 호스트, 프록시 또는 정적 예외가 종속 포털 주소를 포함하도록 구성된 경우, **Fail Close(**실패 닫기**)** 를 선택해도 트래픽이 차단되지 않습니다.

기타 사용자 정의 가능한 웹 보안 옵션

내보내기 옵션

일반 텍스트 웹 보안 클라이언트 프로파일 파일 내보내기

난독 처리된 웹 보안 클라이언트 프로파일을 ASA에서 내보내고 엔드포인트 디바이스에 배포합니다.

프로시저

단계 **1** ASDM을 열고 **Configuration(**구성**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**)** > **AnyConnect Client Profile(AnyConnect** 클라이언트 프로파일**)**을 선택합니다.

단계 **2** 편집하려는 웹 보안 클라이언트 프로파일을 선택한 후 **Export(**내보내기**)**를 클릭하십시오.

단계 **3** 파일을 저장할 로컬 폴더를 찾으십시오. Local Path(로컬 경로) 필드의 파일 이름을 편집하면 웹 보안 클라이언트 프로파일이 새 파일 이름으로 저장됩니다.

단계 **4** **Export(**내보내기**)**를 클릭합니다.

ASDM에서 웹 보안 클라이언트 프로파일의 일반 텍스트 `filename.wsp` 버전을 내보냅니다.

DART 번들에 대한 일반 텍스트 웹 보안 클라이언트 프로파일 파일 내보내기

Cisco 고객 서비스에 DART(Diagnostic AnyConnect Reporting Tool, 진단 AnyConnect 보고 툴) 번들을 보내야 하는 경우, DART 번들과 함께 웹 보안 클라이언트 프로파일 파일(`filename.wsp` 또는 `filename.xml`)의 일반 텍스트 버전을 보내십시오. Cisco 고객 서비스에서는 난독 처리된 버전을 읽을 수 없습니다.

프로파일 편집기의 독립 실행형 버전은 웹 보안 프로파일 파일을 2가지 버전으로 생성합니다. 한 파일은 파일 이름이 `filename.wso`로 난독 처리되고 다른 한 파일은 파일 이름 `filename.xml`을 사용하며 일반 텍스트로 생성됩니다.

Cisco 고객 서비스에 DART 번들을 보내기 전에 DART 번들에 웹 보안 클라이언트 프로파일에 대한 일반 텍스트 버전을 추가하십시오.

ASDM의 일반 텍스트 웹 보안 클라이언트 프로파일 파일 편집 및 가져오기

일반 텍스트 웹 보안 클라이언트 프로파일 파일을 내보낸 경우, AnyConnect 웹 보안 프로파일 편집기에서 지원되지 않는 편집을 허용하는 XML 편집기 또는 일반 텍스트를 사용하여 로컬 컴퓨터에서 편집할 수 있습니다. 고객 지원팀에서 지시한 경우에만 웹 보안 클라이언트 프로파일의 일반 텍스트 버전을 변경하십시오. 편집기를 가져오려면 다음 절차를 사용하십시오.

시작하기 전에

파일을 가져와 선택한 웹 보안 클라이언트 프로파일의 콘텐츠를 덮어씁니다.

프로시저

단계 **1** ASDM을 열고 **Configuration(**구성**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**)** > **AnyConnect Client Profile(AnyConnect** 클라이언트 프로파일**)**을 선택합니다.

단계 **2** 편집하려는 웹 보안 클라이언트 프로파일을 선택한 후 **Export(**내보내기**)**를 클릭하십시오.

단계 **3** `filename.wsp`를 변경한 다음 AnyConnect 클라이언트 프로파일 페이지로 돌아가서 편집한 파일의 프로파일 이름을 선택하십시오.

단계 **4** **Import(**가져오기**)**를 클릭합니다.

단계 **5** 웹 보안 클라이언트 프로파일의 편집된 버전을 검색하여 **Import(**가져오기**)**를 클릭하십시오.

난독 처리된 웹 보안 클라이언트 프로파일 파일 내보내기

프로시저

단계 **1** ASDM을 열고 **Tools(**툴**)** > **File Management(**파일 관리**)**를 선택하십시오.

단계 **2** File Management(파일 관리) 화면에서 **File Transfer(**파일 전송**)** > **Between Local PC and Flash(**로컬 **PC** 및 플래시 사이**)**를 선택하고 파일 전송 대화 상자를 사용하여 난독 처리된 `filename.wso` 클라이언트 프로파일 파일을 로컬 컴퓨터로 전송하십시오.

웹 보안에 대한 스플릿 터널 제외 구성

사용자가 VPN 세션을 설정한 경우, 모든 네트워크 트래픽이 VPN 터널을 통해 전송됩니다. 하지만 AnyConnect 사용자가 웹 보안을 사용 중이라면 엔드포인트에서 시작되는 HTTP 트래픽은 터널에서 제외되고 Cloud Web Security 스캐닝 프록시에 직접 전송되어야 합니다.

Cloud Web Security 스캐닝 프록시용 트래픽에 대해 스플릿 터널 제외를 설정하려면 그룹 정책에서 **Set up split exclusion for Web Security(**웹 보안에 대한 스플릿 제외 설정**)** 버튼을 사용합니다.

시작하기 전에

- AnyConnect 클라이언트에서 사용할 웹 보안 구성
- 그룹 정책을 생성하고 웹 보안을 사용하여 구성된 AnyConnect 클라이언트용으로 연결 프로파일을 할당

신뢰할 수 있는 보안 네트워크 탐지 기능을 사용하며 웹 보안 및 VPN이 동시에 활성 상태가 되게 하려면 HTTPS 서버가 VPN 터널을 통해 연결되지 않도록 네트워크를 구성하십시오. 이 방법으로 사용자가 기업 LAN에 있는 경우에만 웹 보안 기능이 우회 모드로 전환됩니다.

프로시저

단계 **1** ASDM에서 **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 새 그룹 정책 **Edit(**편집**)** 또는 **Add(**추가**)**를 클릭합니다.

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

단계 **4** **Set up split exclusion for Web Security(**웹 보안에 대한 스플릿 제외 설정**)**를 클릭합니다.

단계 **5** 웹 보안 스플릿 제외에 사용된 새 액세스 목록을 입력하거나 기존 액세스 목록을 선택합니다. ASDM은 네트워크 목록에서 사용할 액세스 목록을 설정합니다.

단계 **6** 새 목록의 경우 **Create Access List(**액세스 목록 생성**)**를 클릭하거나 기존 목록의 경우 **Update Access List(**액세스 목록 업데이트**)**를 클릭합니다.

단계 **7** **OK(**확인**)**를 클릭합니다.

다음에 수행할 작업

스캐닝 프록시가 추가된 경우 이 절차에서 생성한 통합 액세스 목록을 새 정보로 업데이트합니다.

Cisco Cloud Web Security의 호스팅된 프로파일 사용

AnyConnect 릴리스 3.0.4부터 웹 보안 호스팅 클라이언트 프로파일용 Cisco ScanCenter 호스팅 구성이 웹 보안 클라이언트에 대해 새로운 구성을 제공하는 기능을 제공합니다. 웹 보안을 사용하는 디바이스는 클라우드를 통해 새로운 웹 보안 호스팅 클라이언트 프로파일을 다운로드할 수 있습니다. 호스트 구성 파일은 Cisco ScanCenter 서버에 있습니다.

또한 AnyConnect 클라이언트는 AnyConnect 바이너리의 하드 코딩된 호스트 이름을 통해 리소스 서비스에서 컨피그레이션 파일을 다운로드해야 합니다. **hostedconfig.scansafe.net/**(IP: 46.155.41.2)에 대해 요청을 실행하며 교환은 TCP 포트 443을 통해 암호화됩니다.

호스팅 컨피그레이션을 사용하는 경우 TCP 포트 443을 통해 AnyConnect Web Security용 CWS 타워/프록시의 인그레스 IP에 액세스할 수 있습니다(일반 모드에서 구축하는 경우에는 포트 8080도 사용 가능함). AnyConnect Web Security용 타워/프록시의 전체 목록은 Cisco ScanCenter 관리 가이드의 **Prepare(준비)** 섹션에서 제공됩니다. 클라이언트는 TCP 포트 80에서 80.254.145.118에 액세스할 수 있어야 합니다. 이 포트에서 프록시 타워 목록을 가져오며 자체적으로 최신 상태를 유지하기 때문입니다. Web Security 모듈은 TCP 포트 80을 통해 Verisign에 연결하도록 설정해야 합니다. 이 범위에서 클라이언트는 Tj.symbcb.com, T1.symcb.com 및 T2.symcb.com의 해지 인증서를 확인합니다.

웹 보안 프로파일 편집기를 사용하여 클라이언트 프로파일 파일을 생성한 다음 암호화되지 않은 텍스트 XML 파일을 Cisco ScanCenter 서버에 업로드하십시오. 이 XML 파일은 유효한 라이선스 키(Cisco Cloud Web Security에서 정의되어 호스트되는 호스팅 컨피그레이션에 연결된 것과 같은 회사, 그룹 또는 사용자 라이선스 키가 포함됨)를 포함해야 합니다. 새 컨피그레이션 파일이 호스팅 컨피그레이션 서버에 적용되고 최대 8시간이 지난 후 클라이언트는 해당 파일을 검색합니다.

호스팅 컨피그레이션 기능은 호스팅 컨피그레이션(Cisco ScanCenter) 서버에서 새 클라이언트 프로파일 파일을 검색할 때 라이선스 키를 사용합니다. 새 클라이언트 프로파일 파일이 서버에 있으면 기존 Web Security 클라이언트 프로파일의 라이선스가 호스팅 서버의 클라이언트 프로파일과 연계된 라이선스와 같은 경우, Web Security를 사용하는 디바이스가 자동으로 서버를 폴링하고 새 클라이언트 프로파일 파일을 다운로드합니다. 새 클라이언트 프로파일이 다운로드된 경우, 사용자가 새 클라이언트 프로파일 파일을 사용할 수 있도록 하기 전까지 웹 보안에서는 같은 파일을 다시 다운로드하지 않습니다.

라이선스 키에 관한 자세한 내용은 *Cisco ScanCenter* 관리자 가이드, 릴리스 *5.2*를 참조하십시오.

시작하기 전에

- Cisco Cloud Web Security 라이선스 키를 포함하는 유효한 클라이언트 프로파일을 사용하여 Web Security 클라이언트 디바이스를 설치하십시오.
- 웹 보안 에이전트 서비스 재시작 옵션은 서비스를 다시 시작하는 필수 권한이 있는 사용자만 이용할 수 있습니다.
- ACWS 에이전트를 실행하는 클라이언트 머신의 신뢰할 수 있는 루트 인증 증명 저장소에는 Thawte 기본 루트 CA 및 Thawte SSL CA - G2가 있어야 합니다.

프로시저

단계 **1** 웹 보안 프로파일 편집기를 사용하여 웹 보안 디바이스에 대한 새 클라이언트 프로파일을 생성하십시오. 이 클라이언트 프로파일은 Cisco Cloud Web Security 라이선스 키를 포함해야 합니다.

단계 **2** 클라이언트 프로파일 파일을 암호화되지 않은 텍스트 XML 파일로 저장하십시오. 이 파일을 Cisco ScanCenter 서버에 업로드하십시오. 파일이 업로드되면 웹 보안 클라이언트에서 새 클라이언트 프로파일을 사용할 수 있도록 하십시오.

단계 **3** 기업에 호스팅 컨피그레이션 기능이 활성화된 경우 새 클라이언트 프로파일을 업로드하고 기업의 Cisco ScanCenter를 통해 적용합니다. 호스팅 클라이언트 프로파일은 라이선스와 연계됩니다. 다른 라이선스(예: 다른 그룹 라이선스 키)를 사용 중인 경우 각 라이선스에는 자체 클라이언트 프로파일이 연결되어 있을 수 있습니다. 그런 다음 사용자가 사용하도록 구성된 라이선스에 따라 다른 클라이언트 프로파일을 서로 다른 사용자에게 푸시할 수 있습니다. 라이선스마다 다양한 컨피그레이션을 저장하고 클라이언트가 다운로드할 기본 클라이언트 프로파일을 설정합니다. 기본적으로 해당 클라이언트 프로파일을 선택하여 Cisco ScanCenter의 호스팅 컨피그레이션 영역에 저장된 컨피그레이션의 다른 수정 버전 중 하나로 전환할 수 있습니다. 라이선스는 하나의 클라이언트 프로파일에만 연계됩니다. 따라서 하나 이상의 수정 버전이 라이선스에 연계되면 하나의 기본값만 사용할 수 있습니다.

Cisco AnyConnect 웹 보안 에이전트 끄기 및 활성화

다음 단계를 수행하여 웹 트래픽을 차단하는 Cisco AnyConnect 웹 보안 에이전트의 기능을 끄고 활성화할 수 있습니다.

Windows를 사용하여 필터 끄기 및 활성화

프로시저

단계 **1** 명령 프롬프트 창을 엽니다.

단계 **2** **%PROGRAMFILES%\Cisco\Cisco AnyConnect Secure Mobility Client** 폴더로 이동하십시오.

단계 **3** 다음과 같이 필터링을 활성화 또는 비활성화하십시오.

- 필터링을 활성화하려면 **acwebsecagent.exe -enablesvc**를 입력하십시오.
- 필터링을 비활성화하려면 **acwebsecagent.exe -disablesvc -servicepassword**를 입력하십시오.

Mac OS X을 사용하여 필터 끄기 및 활성화

서비스 비밀번호는 웹 보안 프로파일 편집기의 인증 패널에서 구성됩니다.

프로시저

단계 **1** 터미널 애플리케이션을 실행하십시오.

단계 **2** `/opt/cisco/anyconnect/bin` 폴더로 이동하십시오.

단계 **3** 다음과 같이 필터링을 활성화 또는 비활성화하십시오.

- 필터링을 활성화하려면 **./acwebsecagent -enablesvc**를 입력하십시오.

- 필터링을 비활성화하려면 **./acwebsecagent -disablesvc -servicepassword**를 입력하십시오.

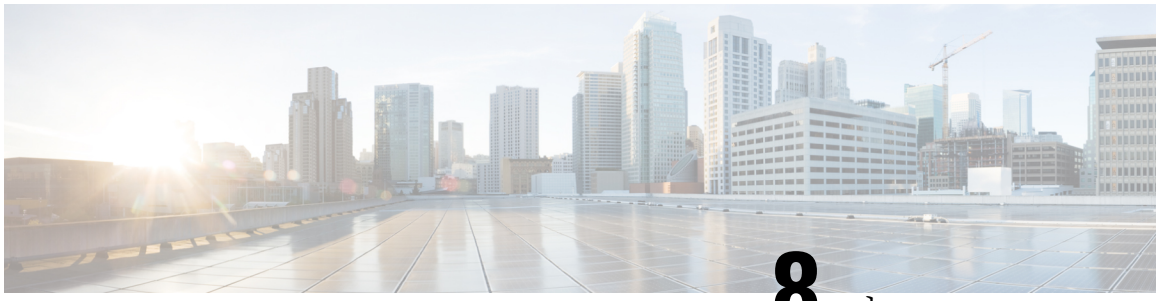
웹 보안 로깅

Windows

모든 웹 보안 메시지는 Windows 이벤트 뷰어에서 `Event Viewer (Local)\Cisco AnyConect Web Security Module` 폴더에 기록됩니다. 이벤트 뷰어에서 웹 보안이 기록하는 이벤트는 Cisco Technical Assistance Center 엔지니어가 분석합니다.

Mac OS X

시스템 로그 또는 콘솔에서 웹 보안 메시지를 볼 수 있습니다.



8 장

AMP Enabler 구성

AMP Enabler 정보

AnyConnect AMP Enabler는 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. 이러한 접근 방식을 통해 AnyConnect 사용자 기반 관리자에게는 네트워크에서 발생할 수 있는 악성코드 위협을 탐지하고 제거하며 엔터프라이즈의 데이터 손상을 보호하는 추가 보안 에이전트가 제공됩니다. AMP Enabler가 있으면 대역폭과 다운로드에 소요되는 시간이 줄어들고, 포털 측 변경도 하지 않아도 되며, 엔드포인트로 인증 자격 증명을 보내지 않고도 필요한 작업을 수행할 수 있습니다.

AMP Enabler 구축

AMP for Endpoints 소프트웨어를 적절하게 배포하려면 다음 워크플로를 진행해야 합니다.

1. AMP for Endpoints 포털에 로그인합니다.
2. AMP for Endpoints 포털에서 적절한 정책을 구성합니다. 설정한 정책에 따라 적절한 AMP for Endpoints 소프트웨어 패키지가 구축됩니다. 소프트웨어 패키지는 Windows의 경우 .exe 파일이고 Mac의 경우 .pkg 파일입니다. Windows의 경우 재배포 가능 .exe를 선택할 수 있습니다.
3. 생성된 키트(Windows 또는 Mac)를 로컬 서버에 다운로드합니다.
4. ASA 또는 ISE 헤드엔드에 로그인하여 AMP Enabler를 생성한 다음 저장합니다.

참고 특히 ISE Posture를 사용할 때는 하나의 헤드엔드(ASA 또는 ISE)용으로만 프로파일을 구성하는 것이 좋습니다.

5. ASA 또는 ISE 헤드엔드의 선택적 모듈 목록에서 AMP Enabler 모듈을 선택하고 AMP Enabler 프로파일도 지정합니다.

   생성된 프로파일은 AnyConnect AMP Enabler에 사용됩니다. AMP Enabler는 이 프로파일과 함께 ASA 또는 ISE 헤드엔드에서 엔드포인트로 푸시됩니다.

AMP Enabler 프로파일 편집기

관리자는 독립 실행형 편집기를 사용하도록 선택하여 AMP Enabler 프로파일을 생성한 다음 ASA에 업로드할 수 있습니다. 이렇게 하지 않으면 내장된 AMP Enabler 프로파일 편집기가 ISE UI의 Policy Elements(정책 요소) 아래 위치 또는 ASDM에서 구성됩니다. 신뢰할 수 있는 로컬 웹 서버가 AMP 프로파일 편집기에서 작동하도록 하려면 keytool 명령을 사용하여 루트 CA 인증서를 JAVA 인증서 저장소로 가져와야 합니다.

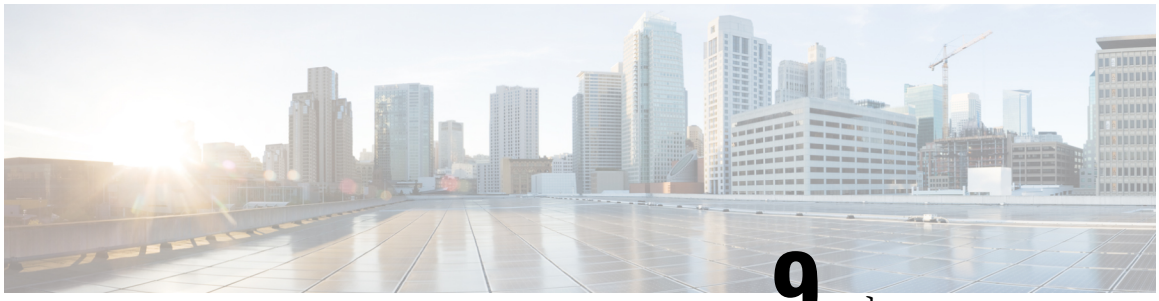
Windows: keytool -import -keystore [JAVA-HOME]/lib/security/cacerts -storepass changeit -trustcacerts -alias root -file [PATH_TO_THE_CERTIFICATE]/certnew.cer

Mac: sudo keytool-import-keystore [JAVA-HOME]/lib/security/cacerts -storepass changeit -trustcacerts -alias root -file [PATH_TO_THE_CERTIFICATE]/certnew.cer

- 이름
- 설명
- Install AMP for Endpoints(AMP for Endpoints 설치) - AMP for Endpoints를 설치하도록 이 프로파일을 구성하려면 선택합니다.
- Uninstall AMP for Endpoints(AMP for Endpoints 제거) - AMP for Endpoints를 제거하도록 이 프로파일을 구성하려면 선택합니다. 제거를 선택하는 경우 다른 필드에는 내용을 입력하지 않아도 됩니다.
- Windows Installer - .exe 파일이 있는 URL 또는 로컬 호스팅 서버 주소를 입력합니다.
- Mac Installer - .pkg 파일이 있는 URL 또는 로컬 호스팅 서버 주소를 입력합니다.
- Check(확인) - URL에 대해 확인을 실행하여 유효한지 여부를 파악하려면 클릭합니다. 유효한 URL은 연결이 가능하며 신뢰할 수 있는 인증서를 포함하는 URL입니다. 이 URL에서 서버에 연결할 수 있으며 연결이 설정되는 경우 프로파일을 저장하면 됩니다.
- Add to Start Menu(시작 메뉴에 추가) - 시작 메뉴 바로 가기를 생성합니다.
- Add to Desktop(바탕 화면에 추가) - 바탕 화면 아이콘을 생성합니다.
- Add to Context Menu(상황에 맞는 메뉴에 추가) - 이 옵션을 선택하는 경우 원하는 파일이나 폴더를 마우스 오른쪽 버튼으로 클릭하고 Scan Now(지금 스캔)를 선택하여 스캔을 활성화할 수 있습니다.

AMP Enabler의 상태

AMP의 실제 다운로드 및 설치와 관련된 메시지는 AnyConnect UI의 AMP Enabler 타일에 부분 타일로 나타납니다. 설치 후에는 모든 AMP 관련 메시지가 엔드포인트용 AMP UI에 표시됩니다. 예를 들어 사용자는 악성코드 방지용 보호 기능을 설치하거나 제거할 때 메시지를 확인하여 작업 실패 또는 재부팅 필요 여부를 파악할 수 있습니다.



9 장

Network Visibility Module

Network Visibility Module 정보

관리되지 않는 디바이스에서 작업을 하는 사용자가 갈수록 늘어나고 있으므로 엔터프라이즈 관리자가 네트워크 내부와 외부에서 수행되는 작업을 파악하기가 어려워졌습니다. NVM(Network Visibility Module)은 온프레미스 또는 오프프레미스의 엔드포인트에서 다양한 플로우 상황 정보를 수집하며, Stealthwatch와 같은 Cisco 솔루션 또는 Splunk와 같은 서드파티 솔루션과 함께 사용하는 경우 네트워크에 연결된 디바이스 및 사용자 행동을 파악하는 기능을 제공합니다. 엔터프라이즈 관리자는 이러한 정보와 행동을 파악한 후에 용량 및 서비스 계획, 감사, 컴플라이언스 및 보안 분석을 수행할 수 있습니다. NVM은 다음과 같은 서비스를 제공합니다.

- 네트워크 설계에서 정보를 토대로 하여 애플리케이션을 더 효율적으로 개선할 수 있도록 애플리케이션 사용을 모니터링하는 서비스(VzFlow 프로토콜 사양의 확장 IPFIX 컬렉터 요소)
- 애플리케이션, 사용자 또는 엔드포인트의 논리 그룹을 분류하는 서비스
- 기업 자산을 추적하고 마이그레이션 활동을 계획하는 데 도움이 되는 이상 징후 가능성을 찾는 서비스

이 기능을 사용하면 전체 인프라 구축이 아닌 텔레메트리를 대상으로 지정할지 여부를 선택할 수 있습니다. NVM은 다음 정보를 더욱 효율적으로 파악하기 위해 엔드포인트 텔레메트리를 수집합니다.

- 디바이스 - 엔드포인트(위치는 관계없음)
- 사용자 - 엔드포인트에 로그인한 사용자
- 애플리케이션 - 트래픽을 생성하는 항목
- 위치 - 트래픽이 생성된 네트워크 위치

- 대상 - 해당 트래픽을 전송하려 했던 실제 FQDN

신뢰할 수 있는 네트워크에서 AnyConnect NVM은 Cisco의 컬렉터(예: Stealthwatch)나 서드파티 생산업체의 컬렉터(예: LiveAction)로 플로우 기록을 내보냅니다. 이 컬렉터는 파일 분석을 수행하고 UI 인터페이스를 제공합니다. 플로우 레코드는 사용자의 기능에 대한 정보를 제공하며 값은 ID와 함께 내보내집니다. 예를 들어 LoggedInUserAccountType은 12361로, ProcessUserAccountType은 12362로, ParentProcessUserAccountType은 12363으로 내보냅니다. Splunk와 같은 타 서드파티 생산업체의 컬렉터도 보고서 확인을 위한 UI 인터페이스를 제공할 수 있습니다. 대다수 엔터프라이즈 IT 관리자는 이러한 데이터로 자체 시각화 템플릿을 작성하고자 하므로, Splunk 앱 플러그인을 통해 몇 가지 샘플 기본 템플릿이 제공됩니다.

데스크톱 AnyConnect의 NVM

기존에는 플로우 컬렉터에서 스위치나 라우터의 인터페이스를 시작하거나 종료할 때 IP 네트워크 트래픽을 수집하는 기능을 제공했습니다. 플로우 컬렉터는 네트워크에서 혼잡이 발생하는 소스, 플로우의 경로 등만 확인할 수 있었으며 그 외의 정보는 거의 확인할 수 없었습니다. 엔드포인트에 NVM이 있으면 디바이스 유형, 사용자, 애플리케이션 등의 다양한 엔드포인트 상황 정보로 플로우가 보완됩니다. 따라서 수집 플랫폼의 기능에 따라 플로우 기록에 대해 더욱 적절한 작업을 수행할 수 있습니다. NVM에서 제공한 내보낸 데이터(IPFIX를 통해 전송됨)는 Cisco NetFlow 컬렉터는 물론 Splunk, IBM Qradar, LiveAction 등의 기타 서드파티 플로우 수집 플랫폼과도 호환됩니다. 자세한 내용은 플랫폼별 통합 설명서를 참조하십시오. 예를 들어 Splunk 통합 관련 정보는 https://www.cisco.com/c/en/us/support/docs/security/anyconnect-secure-mobility-client/200600-Install-and-Configure-Cisco-Network-Visi.html 을 통해 제공됩니다.

Network Visibility Module을 설치하도록 선택하는 경우 AnyConnect Secure Mobility Client UI의 About(정보) 화면에는 이 모듈이 설치된 항목으로 나열됩니다. NVM이 실행 중일 때는 AnyConnect UI에 다른 항목이 표시되지 않습니다.

이 기능이 활성화되어 있으면 NVM용 AnyConnect 프로파일은 ISE 또는 ASA 헤드엔드에서 푸시됩니다. ISE 헤드엔드에서는 Web Security, Network Access Manager 등에서와 마찬가지로 독립형 프로파일 편집기를 사용하여 NVM 서비스 프로파일 XML을 생성한 다음 ISE에 업로드하고 새 NVM 모듈에 매핑할 수 있습니다. ASA 헤드엔드에서는 독립형 또는 ASDM 프로파일 편집기를 사용할 수 있습니다.

VPN 상태가 연결됨으로 변경될 때와 엔드포인트가 신뢰할 수 있는 네트워크에 있을 때 NVM은 알림을 받습니다.

참고 Linux에서 NVM을 사용 중인 경우에는 Linux에서 NVM 사용, 8 페이지의 예비 단계를 완료했는지 확인하십시오.

모바일 AnyConnect의 NVM

NVM(Network Visibility Module)은 Google Play 스토어에서 제공되는 Cisco AnyConnect Secure Mobility Client for Android의 최신 버전(릴리스 4.0.09xxx)에 포함되어 있습니다. NVM은 Samsung Knox 버전

2.8 이상을 실행 중인 Samsung 디바이스에서 지원됩니다. 다른 모바일 디바이스는 현재 지원되지 않습니다. 모바일 NVM 관련 정보는 *Cisco AnyConnect Secure Mobility Client* 관리자 가이드 릴리스 *4.0* 의 모바일 디바이스의 *AnyConnect* 장에서 모바일용 *NVM* 구성 절차를 참조하십시오.

Android의 Network Visibility는 서비스 프로파일 컨피그레이션의 일부분입니다. Android에서 NVM을 구성하려는 경우 AnyConnect NVM 프로파일 편집기에서 AnyConnect NVM 프로파일이 생성된 다음 MDM(Mobile Device Management)을 통해 Samsung 모바일 디바이스로 푸시됩니다. 모바일 디바이스용으로 NVM을 구성하려면 AnyConnect 릴리스 4.4.3 이상의 AnyConnect NVM 프로파일 편집기가 필요합니다.

지침

- NVM은 Samsung Knox 버전 2.8 이상을 실행 중인 Samsung 디바이스에서 지원됩니다. 다른 모바일 디바이스는 현재 지원되지 않습니다.
- 모바일 디바이스에서는 IPv4를 통한 컬렉터 연결만 지원됩니다. IPv6은 지원되지 않습니다.
- Java 기반 앱의 데이터 수집은 지원되지 않습니다.

NVM 사용 방법

다음과 같은 상황에서 NVM을 사용할 수 있습니다.

- 보안 사고가 발생한 후 사용자의 네트워크 기록에서 유출 가능성을 감사하려는 경우
- 시스템 또는 관리 권한이 사용자 머신에서 실행되고 있는 네트워크 연결 프로세스에 영향을 주는 방식을 확인하려는 경우
- 레거시 OS를 실행 중인 모든 디바이스의 목록을 가져오려는 경우
- 네트워크에서 가장 많은 네트워크 대역폭을 사용하여 실행 중인 애플리케이션을 확인하려는 경우
- 네트워크에서 사용 중인 Firefox의 버전 수를 확인하려는 경우
- 네트워크에서 IPv6을 사용하는 Chrome.exe 연결의 퍼센트를 확인하려는 경우

NVM 프로파일 편집기

프로파일 편집기에서는 수집 서버의 IP 주소 또는 FQDN을 구성합니다. 또한 데이터 수집 정책을 맞춤화하여 전송할 데이터 유형 및 데이터 익명화 여부를 선택할 수도 있습니다.

Network Visibility Module은 IPv4 주소를 사용하여 단일 스택 IPv4와의 연결을 설정하거나, IPv6 주소를 사용하여 단일 스택 IPv6과의 연결을 설정하거나, OS의 기본 설정에 따라 IP 주소에 대한 이중 스택 IPv4/IPv6과의 연결을 설정할 수 있습니다.

참고 Network Visibility Module은 신뢰할 수 있는 네트워크에 있을 때만 플로우 정보를 전송합니다. 기본적으로는 데이터가 수집되지 않습니다. 데이터는 프로파일에 수집하도록 구성되어 있을 때만 수집되며 엔드포인트가 연결되어 있으면 계속 수집됩니다. 신뢰할 수 없는 네트워크에서 수집이 수행되는 경우에는 엔드포인트가 신뢰할 수 있는 네트워크에 있을 때 데이터가 캐시되어 전송됩니다. NVM은 VPN의 TND 기능을 사용하여 엔드포인트가 신뢰할 수 있는 네트워크에 있는지를 파악합니다. 또한 VPN이 연결된 상태이면 엔드포인트가 신뢰할 수 있는 네트워크에 있는 것으로 간주되어 플로우 정보가 전송됩니다. NVM별 시스템 로그에 TND 사용이 표시됩니다. TND 파라미터 설정에 대한 자세한 내용은 AnyConnect 프로파일 편집기, 환경 설정(2부), 92 페이지을 참조하십시오.

- **Desktop(**데스크톱**)** 또는 **Mobile(**모바일**)** - NVM을 설정할 디바이스(데스크톱 또는 모바일 디바이스)를 결정합니다. **Desktop(**데스크톱**)**이 기본값입니다. Mobile(모바일)은 향후 지원될 예정입니다.
- 컬렉터 컨피그레이션
  - **IP Address/FQDN(IP** 주소**/FQDN)** - 컬렉터의 IPv4 또는 IPv6 IP 주소/FQDN을 지정합니다.
  - **Port(**포트**)** - 컬렉터가 수신 대기하는 포트 번호를 지정합니다.
- 캐시 컨피그레이션
  - **Max Size(**최대 크기**)** - 데이터베이스가 도달할 수 있는 최대 크기를 지정합니다. 이전에는 캐시 크기에 사전 설정된 제한이 적용되었지만 이제는 프로파일 내에서 해당 제한을 구성할 수 있습니다. 캐시의 데이터는 암호화된 형식으로 저장되며 루트 권한을 사용하는 프로세스에서만 데이터를 암호 해독할 수 있습니다.

    크기 제한에 도달하면 최신 데이터를 저장할 수 있도록 가장 오래된 데이터가 공간에서 삭제됩니다.
  - **Max Duration(**최대 기간**)** - 저장할 데이터에 해당하는 기간(일)을 지정합니다. Max Size(최대 크기)도 설정하는 경우 먼저 도달하는 제한이 우선적으로 적용됩니다.

    기간 제한에 도달하면 가장 최근의 데이터를 저장할 수 있도록 가장 오래된 데이터가 공간에서 삭제됩니다. Max Duration(최대 기간)만 구성하면 크기 제한은 사용되지 않으며 두 옵션을 모두 비활성화하면 크기는 50MB로 제한됩니다.
- **Periodic Flow Reporting(**정기적인 플로우 보고**)(**선택 사항, 데스크톱에만 적용됨**)** - 정기적인 플로우 보고를 활성화하려면 선택합니다. 서버 연결이나 다운로드 등의 플로우 보고는 신뢰할 수 있는 네트워크에 있는 동안이나 VPN을 사용하는 동안 구성한 간격으로 수행됩니다. 정기적인 플로우 보고는 기본적으로 비활성화됩니다.
- **Aggregation Interval(**집계 간격**)** - NVM 타이머를 맞춤화하여 Cisco nvzFlow가 데이터를 내보내는 시기를 정의할 수 있습니다. 컬렉터 환경이 오버런되지 않도록 간격을 지정하십시오. 기본값은 5초입니다.
- **Throttle Rate(**스로틀 속도**)** - 스로틀은 엔드 유저에 대한 영향을 최소화할 수 있도록 캐시에서 컬렉터로 데이터를 전송하는 속도를 제어합니다. 실시간 데이터와 캐시된 데이터 둘 다에 스로

틀을 적용할 수 있습니다(캐시된 데이터가 있는 경우). 스로틀 속도는 Kbps 단위로 입력합니다. 기본값은 500Kbps입니다.

이 고정된 기간이 지난 후에 캐시된 데이터를 내보냅니다. 이 기능을 비활성화하려면 0을 입력합니다.

- **Collection Mode(**수집 모드**)** - collection mode is off(수집 모드가 해제됨), trusted network only(신뢰할 수 있는 네트워크에서만), untrusted network only(신뢰할 수 없는 네트워크에서만) 또는 all networks(모든 네트워크) 중 하나를 선택하여 엔드포인트에서 데이터를 수집해야 하는 시기를 지정합니다.

- **Collection Criteria(**수집 기준**)** - 관련 데이터만 분석하면 되도록 데이터 수집 중에 불필요한 브로드캐스트를 줄일 수 있습니다. 다음 옵션을 사용하여 데이터 수집을 제어합니다.

  - **Broadcast packets(**브로드캐스트 패킷**)** 및 **Multicast packets(**멀티캐스트 패킷**)(**데스크톱에만 적용됨**)** - 효율성을 높이기 위해 기본적으로 브로드캐스트 및 멀티캐스트 패킷 수집은 해제됩니다. 그러면 백엔드 리소스에 대해 소요되는 시간이 감소합니다. 브로드캐스트 및 멀티캐스트 패킷에 대해 수집을 활성화하고 데이터를 필터링하려면 체크 박스를 클릭합니다.

  - **KNOX only(KNOX**만**)**(선택 사항, 모바일 관련) - 선택하는 경우 KNOX 워크스페이스에서만 데이터를 수집합니다. 기본적으로 이 필드는 선택되지 않으며 워크스페이스 내부와 외부의 데이터가 수집됩니다.

- **Data Collection Policy(**데이터 수집 정책**)** - 데이터 수집 정책을 추가하고 네트워크 유형 또는 연결 시나리오와 연결할 수 있습니다. 여러 인터페이스를 동시에 활성화할 수 있으므로 VPN 트래픽과 그 외의 트래픽에 각기 다른 정책을 적용할 수 있습니다.

  Add(추가)를 클릭하면 Data Collection Policy(데이터 수집 정책) 창이 나타납니다. 정책을 생성할 때는 다음 지침에 유의하십시오.

  - 정책을 생성하지 않거나 네트워크 유형과 연결하지 않으면 기본적으로 모든 필드가 보고 및 수집됩니다.

  - 각 데이터 수집 정책은 하나 이상의 네트워크 유형과 연결해야 하지만 같은 네트워크 유형에 두 가지 정책을 연결할 수는 없습니다.

  - 네트워크 유형이 더 구체적인 정책이 우선적으로 적용됩니다. 예를 들어 VPN은 신뢰할 수 있는 네트워크의 일부분이므로 네트워크 유형으로 VPN이 포함된 정책이 네트워크로 신뢰함을 지정한 정책보다 우선적으로 적용됩니다.

  - 선택한 수집 모드에 따라 적용되는 네트워크용으로만 데이터 수집 정책을 생성할 수 있습니다. 예를 들어 **Collection Mode(**수집 모드**)**를 **Trusted Network Only(**신뢰할 수 있는 네트워크에서만**)**로 설정하는 경우에는 **Untrusted Network Type(**신뢰할 수 없는 네트워크 유형**)**용으로 **Data Collection Policy(**데이터 수집 정책**)**을 생성할 수 없습니다.

  - 이전 AnyConnect 릴리스의 프로파일을 최신 AnyConnect 릴리스 프로파일 편집기에서 열면 프로파일이 최신 릴리스로 자동 변환됩니다. 변환 시에는 이전에 익명화되었던 것과 같은 필드를 제외하는 데이터 수집 정책이 모든 네트워크에 대해 추가됩니다.

  - **Name(**이름**)** - 생성하는 정책의 이름을 지정합니다.

- **Network Type(**네트워크 유형**)** - VPN, trusted(신뢰함) 또는 untrusted(신뢰하지 않음) 중 하나를 선택하여 수집 모드나 데이터 수집 정책이 적용되는 네트워크를 결정합니다. trusted(신뢰함)를 선택하는 경우 정책이 VPN 사례에도 적용됩니다.
- 포함/제외
  - **Type(**유형**)** - 데이터 수집 정책에 **Include(**포함**)** 또는 **Exclude(**제외**)**할 필드를 결정합니다. 기본값은 **Exclude(**제외**)**입니다. 선택하지 않는 모든 필드는 수집되며, 선택되는 필드는 없습니다.
  - **Fields(**필드**)** - 데이터 수집 정책에 포함할 필드를 결정합니다. 네트워크 유형 및 포함하거나 제외하는 필드에 따라 NVM은 엔드포인트에서 적절한 데이터를 수집합니다.

    자세한 내용은 NVM의 수집 파라미터, 256 페이지를 참조하십시오.

    AnyConnect 릴리스 4.4 이상 버전의 경우 이제 인터페이스의 네트워크 상태를 신뢰할 수 있는지 여부를 지정하는 인터페이스 상태와 SSID를 선택할 수 있습니다.
  - **Optional Anonymization Fields(**선택적 익명화 필드**)** - 같은 엔드포인트의 레코드 간에 상관관계를 설정하는 동시에 프라이버시는 유지하려는 경우 원하는 필드를 익명화하도록 선택합니다. 그러면 해당 필드가 실제 값이 아닌 값의 해시로 전송됩니다. 필드의 하위 집합을 익명화에 사용할 수 있습니다.

    포함하거나 제외하도록 표시한 필드는 익명화에 사용할 수 없습니다. 마찬가지로 익명화하도록 선택한 필드는 포함하거나 제외할 수 없습니다.

- **Acceptable Use Policy(**사용 제한 정책**)**(선택 사항, 모바일 관련) - **Edit(**편집**)**를 클릭하여 대화 상자에서 모바일 디바이스용 사용 제한 정책을 정의합니다. 정의를 완료한 후 **OK(**확인**)**를 클릭합니다. 최대 4000자를 입력할 수 있습니다.

  NVM을 구성하고 나면 사용자에게 이 메시지가 표시됩니다. 원격 사용자는 NVM 활동 거부를 선택할 수 없습니다. 네트워크 관리자는 MDM 기능을 사용하여 NVM을 제어합니다.

프로파일은 `NVM_ServiceProfile.xml`로 저장합니다. 이 이름을 정확하게 지정하여 프로파일을 저장해야 합니다. 그렇지 않으면 NVM이 데이터를 수집 및 전송하지 못합니다.

NVM의 수집 파라미터

다음 파라미터는 엔드포인트에서 수집되어 컬렉터로 내보내기됩니다.

표 ***9:*** 엔드포인트 ***ID***

파라미터	설명/참고
Virtual Station Name	
UDID	Universally Unique Identifier(범용 고유 식별자)입니다. 각 플로우에 해당하는 엔드포인트를 고유하게 식별합니다. 데스크톱의 HostScan과도 이 UDID 값을 보고합니다.

파라미터	설명/참고
OS Name	
OS Version	
SystemManufacturer	
System Type	기타 플랫폼의 경우에는 `x86` 또는 `x64`로 설정됩니다.
OS Edition	

표 ***10:*** 인터페이스 정보

파라미터	설명/참고
Endpoint UDID	UDID와 동일합니다.
Interface UID	
Interface Index	
Interface Type	
Interface Name	
Interface Details List	상태 및 SSID(InterfaceDetailsList의 속성)입니다. 인터페이스의 네트워크 상태(신뢰할 수 있음/신뢰할 수 없음)와 연결의 SSID를 나타냅니다.
Interface MAC address	Windows 및 Mac OS에만 해당됩니다.

표 ***11:*** 플로우 정보

프로토콜 식별자	설명/참고
Source IPv4 Add	
Destination IPv4 Addr	
Source Transport Port	
Destination Transport Port	
Source IPv6 Addr	
Destination IPv6 Addr	
Start Sec End Sec	플로우 시작 또는 종료의 절대 타임스탬프입니다.
Flow UDID	UDID와 동일합니다.

프로토콜 식별자	설명/참고
Logged In User	
Logged In User Account Type	Windows 및 Mac OS에만 해당됩니다.
Process Account	
Process Account type	Windows 및 Mac OS에만 해당됩니다.
Process Name	
Process Hash	
Parent Process Account	
Parent Process Account Type	Windows 및 Mac OS에만 해당됩니다.
Parent Process Name	
Parent Process Hash	
DNS Suffix	엔드포인트의 플로우와 연결된 인터페이스에서 구성됩니다.
L4ByteCountIn	
L4ByteCountOut	
Destination Hostname	엔드포인트의 대상 IP로 확인되는 실제 FQDN입니다.
Interface UID	
Module Name List	
Module Hash List	

참고 NVM은 주기적으로 엔드포인트 ID에 대한 정보도 전송합니다.

NVM 상태를 제공하는 고객 피드백 모듈

고객 피드백 모듈 모음 부분에서는 NVM이 설치되어 있는지 여부, 일일 플로우 수 및 DB 크기에 대한 데이터를 제공합니다.

10 장

Umbrella 로밍 보안

Umbrella 로밍 보안 모듈을 사용하려면 Professional, Insights, Platform 또는 MSP 패키지가 포함된 Cisco Umbrella 로밍 서비스 서브스크립션이 필요합니다. Cisco Umbrella 로밍은 활성 VPN이 없을 때 DNS 레이어 보안을 제공하며, Cisco Umbrella 서브스크립션은 네트워크 내부와 외부에서 모두 지능형 프록시 및 IP 레이어 시행 기능을 추가로 제공합니다. 또한 Cisco Umbrella 서브스크립션에서는 콘텐츠 필터링, 다양한 정책, 강력한 보고 기능, Active Directory 통합 기능 등도 제공합니다. 서브스크립션에 관계없이 동일한 Umbrella 로밍 보안 모듈이 사용됩니다.

Umbrella 로밍 모듈 프로파일(OrgInfo.json)은 각 구축을 해당하는 서비스와 연결하며 해당 보호 기능은 자동으로 활성화됩니다.

Umbrella 대시보드에서는 로밍 보안 모듈에서 시작되는 모든 인터넷 활동을 실시간으로 파악할 수 있습니다. 정책과 보고서의 세분화 레벨은 Umbrella 서브스크립션에 따라 다릅니다.

각 서비스 레벨 서브스크립션에 포함된 기능을 자세히 비교한 내용은 https://umbrella.cisco.com/products/packages를 참조하십시오.

Umbrella 로밍 클라이언트 및 Umbrella 로밍 보안 모듈 비호환성

Umbrella 로밍 보안 모듈과 Umbrella 로밍 클라이언트는 호환되지 않습니다. Umbrella 로밍 보안 모듈을 구축하는 경우 충돌을 방지하기 위해 로밍 보안 모듈 설치 중에 기존에 설치한 Umbrella 로밍 클라

이언트가 자동으로 탐지되어 제거됩니다. 기존에 설치한 Umbrella 로밍 클라이언트가 Umbrella 서비스 서브스크립션과 연결되어 있는 경우 OrgInfo.json 파일이 AnyConnect 설치 프로그램(웹 구축용으로 구성되어 있거나 Umbrella 모듈 디렉터리에 사전 구축됨)과 같은 위치에 저장되어 있는 경우가 아니면 서브스크립션은 Umbrella 로밍 보안 모듈로 자동 마이그레이션됩니다. Umbrella 로밍 보안 모듈을 구축하기 전에 Umbrella 로밍 클라이언트를 수동으로 제거할 수도 있습니다.

Cisco Umbrella 계정 받기

로그인 페이지인 Umbrella 대시보드(http://dashboard.umbrella.com/)에서 구축에 포함할 AnyConnect Umbrella 로밍 보안 모듈용 프로파일(OrgInfo.json)을 받을 수 있습니다. 또한 이 페이지에서 로밍 클라이언트 활동에 대한 보고와 정책도 관리할 수 있습니다.

대시보드에서 OrgInfo 파일 다운로드

OrgInfo.json 파일은 로밍 보안 모듈이 보고를 할 위치와 시행할 정책을 파악할 수 있도록 하는 Umbrella 대시보드 인스턴스에 대한 특정 정보입니다.

Umbrella 로밍 보안 모듈 구축을 준비하려면 Umbrella 대시보드(https://dashboard.umbrella.com)에서 OrgInfo.json 파일을 다운로드해야 합니다.

Identities(ID) 메뉴 구조에서 **Roaming Computers(**로밍 컴퓨터**)**를 클릭한 다음 페이지 왼쪽 위 모서리에서 + 기호를 클릭합니다. 아래쪽의 AnyConnect Umbrella Roaming Security Module(AnyConnect Umbrella 로밍 보안 모듈)로 스크롤하여 **Module Profile(**모듈 프로파일**)**을 클릭합니다. 특정 설치/구축 단계와 구체적인 패키지 및 파일 정보는 AnyConnect 구축 개요, 2 페이지를 참조하십시오.

참고 처음으로 구축하는 OrgInfo.json 파일은 데이터 하위 디렉터리(/umbrella/data)에 복사되는데, 이 디렉터리에는 다른 등록 파일도 여러 개 생성됩니다. 그러므로 대체 OrgInfo.json 파일을 구축해야 하는 경우에는 데이터 하위 디렉터리를 삭제해야 합니다. Umbrella 로밍 보안 모듈을 제거하고(그러면 데이터 하위 디렉터리가 삭제됨) 새 OrgInfo.json 파일을 사용하여 모듈을 다시 설치할 수도 있습니다.

Umbrella 로밍 보안 작동 및 실행

AnyConnect를 배포할 때 추가 기능을 활성화하기 위해 포함할 수 있는 선택적 모듈 중 하나가 Umbrella 로밍 보안 모듈입니다.

참고 Web Security 모듈과 함께 Umbrella 로밍 보안 모듈을 구축하는 경우에는 Web Security 및 로밍 보안 호환성에 필요한 호스트 예외, 233 페이지 및 Web Security 및 Umbrella 로밍 보안 모듈 호환성에 필요한 정적 예외, 234 페이지에 나와 있는 정적 예외 제외 및 호스트 예외를 구성해야 합니다.

Windows 7 SP1 사용자의 경우 설치 또는 최초 사용 전에 Microsoft .NET Framework 4.0을 설치하는 것이 좋습니다. Umbrella 서비스는 시작 시 .NET Framework 4.0 이상 버전이 설치되어 있는지를 확인합니다. 해당 버전이 탐지되지 않으면 Umbrella 로밍 보안 모듈이 활성화되지 않으며 메시지가 표시됩니다. 계속 진행하여 .NET Framework를 설치하려면 컴퓨터를 리부팅하여 Umbrella 로밍 보안 모듈을 활성화해야 합니다.

OrgInfo.json 파일 구성

orginfo.json 파일에는 보안 로밍 모듈이 보고를 할 위치와 시행할 정책을 파악할 수 있도록 하는 Umbrella 서비스 서브스크립션에 대한 특정 정보가 포함되어 있습니다. ASA 또는 ISE에서 CLI나 GUI를 사용하여 OrgInfo.json 파일을 구축하고 Umbrella 로밍 보안 모듈을 활성화할 수 있습니다. 아래 단계에서는 모듈을 ASA에서 활성화하는 방법과 ISE에서 활성화하는 방법을 차례로 설명합니다.

ASA CLI

1. Umbrella 대시보드(https://dashboard.umbrella.com)에서 받은 OrgInfo.json 파일을 ASA 파일 시스템에 업로드합니다.
2. 컨피그레이션에 적합하게 그룹 정책 이름을 조정하여 다음 명령을 실행합니다.

```
webvpn
 anyconnect profiles orginfo disk0:/orginfo.json

group-policy DfltGrpPolicy attribute
 webvpn
  anyconnect profiles value orginfo type umbrella
```

ASDM GUI

1. **Configuration(**컨피그레이션**) > Remote Access VPN(**원격 액세스 **VPN) > Network (Client) Access(**네트워크(클라이언트) 액세스**) > AnyConnect Client Profiles(AnyConnect** 클라이언트 프로파일**)**로 이동합니다.
2. **Add(**추가**)**를 선택합니다.
3. 프로파일 이름을 제공합니다.
4. Profile Usage(프로파일 사용) 드롭다운 메뉴에서 Umbrella 보안 로밍 클라이언트 유형을 선택합니다. Profile Location(프로파일 위치) 필드에 OrgInfo.json 파일이 입력됩니다.
5. **Upload(**업로드**)**를 클릭하고 대시보드에서 다운로드한 OrgInfo.json 파일의 위치로 이동합니다.
6. Group Policy(그룹 정책) 드롭다운 메뉴에서 정책을 DfltGrpPolicy에 연결합니다. 그룹 정책에서 새 모듈 이름을 지정하려면 추가 AnyConnect 모듈 활성화, 28 페이지의 내용을 참조하십시오.

ISE

ISE에서 모듈을 활성화하려면 다음 단계를 수행합니다.

1. Umbrella 대시보드 https://dashboard.umbrella.com에서 OrgInfo.json을 업로드합니다.
2. 파일 이름을 OrgInfo.xml로 바꿉니다.

3. AnyConnect를 구축하기 위한 ISE 구성, 31 페이지의 단계를 수행합니다.

Umbrella 로밍 보안 모듈의 일부분으로 IP 레이어 시행

IP 레이어 시행은 구매한 Umbrella 패키지에 따라 일부 고객에게 제공되는 선택적 기능입니다. 이 AnyConnect 관리자 가이드에서는 이 기능을 사용하기 위한 요건을 설명하지 않습니다. IP 레이어 시행에 대한 정보를 확인하려면 https://docs.umbrella.com/product/umbrella/6-adding-ip-layer-enforcement/를 참조하십시오.

클라우드 업데이트

Umbrella 로밍 보안 모듈이 Umbrella 클라우드 인프라에서 설치된 모든 AnyConnect 모듈에 대해 자동 업데이트를 제공할 수 있습니다. 클라우드 업데이트를 사용하는 경우에는 Umbrella 클라우드 인프라에서 소프트웨어 업그레이드를 자동으로 가져오며, 관리자의 작업이 아닌 클라우드 인프라를 통해 업데이트를 추적합니다.

기본적으로 클라우드 업데이트를 통한 자동 업데이트는 비활성화되어 있습니다. Umbrella 로밍 보안과 AnyConnect의 나머지 요소에 대해 클라우드 업데이트를 활성화하려면 Umbrella 대시보드에 로그인합니다. **Identities(ID) > Roaming Computers(**로밍 컴퓨터**)** > Settings(설정) 아이콘(기어 아이콘) 아래에서 **Automatically update AnyConnect, including VPN module, whenever new versions are released(**새 버전이 릴리스될 때마다 **VPN** 모듈을 비롯한 **AnyConnect** 자동 업데이트**)**를 선택합니다. VPN이 활성화되어 있는 동안에는 업데이트가 수행되지 않습니다. 기본적으로 이 옵션은 선택되어 있지 않습니다.

클라우드 업데이트와 관련하여 고려할 사항은 다음과 같습니다.

- 현재 설치되어 있는 소프트웨어 모듈만 업데이트됩니다.
- 맞춤화, 현지화 및 기타 모든 구축 유형은 지원되지 않습니다.
- 업데이트는 데스크톱에 로그인되어 있을 때만 수행되며 VPN이 설정되어 있으면 수행되지 않습니다.
- 업데이트가 비활성화되어 있으면 최신 소프트웨어 기능과 업데이트를 사용할 수 없습니다.
- 클라우드 업데이트를 비활성화해도 웹 구축, 보류 업데이트 등의 다른 업데이트 메커니즘이나 설정에는 아무런 영향이 없습니다.
- 클라우드 업데이트에서는 임시 릴리스, 패치된 버전 등 릴리스되지 않은 최신 AnyConnect 버전이 설치된 디바이스를 무시합니다.

보안 정책 구성 및 보고서 검토

보호 기능을 활용하고, 보고 정보를 확인하고, 정책을 구성하려면 Cisco Umbrella 로밍 계정이 있어야 합니다. 자세한 설명을 확인하려면 https://docs.umbrella.com/product/umbrella/ 또는 https://support.umbrella.com을 방문하여 추가 정보를 확인하십시오.

로밍 컴퓨터는 설치 후 90분~2시간 내에 Umbrella 대시보드에 표시됩니다. https://dashboard.umbrella.com으로 이동하여 인증을 한 다음 **Identities(ID) > Roaming Computers(**로밍 컴퓨터**)**로 이동하면 로밍 클라이언트(활성/비활성 클라이언트)의 목록과 설치된 각 클라이언트에 대한 세부사항이 표시됩니다.

처음에는 기본 보안 필터링 레벨의 기본 정책이 로밍 컴퓨터에 적용됩니다. 이 기본 정책은 대시보드의 Policies(정책) 섹션이나 Cisco Umbrella 계정의 Configuration(컨피그레이션) > Policy(정책)에서 확인할 수 있습니다.

로밍 클라이언트의 보고 기능은 Reports(보고서) 섹션 아래에 있습니다. Activity Search(활동 검색) 보고서를 선택하면 Umbrella 로밍 보안 모듈이 설치되어 있으며 VPN이 꺼져 있는 컴퓨터의 DNS 트래픽을 확인할 수 있습니다.

엔드포인트에 표시할 UI 변경 사항 암호 해독

AnyConnect UI 내에서 Umbrella 로밍 보안 모듈 타일에서는 현재 상태가 제공됩니다.

상태	아이콘 색	설명	상태
예약	주황색	연결 상태를 확인하는 중입니다. Umbrella 모듈이 보호 상태를 아직 확인하지 못했습니다.	이 작동 상태는 다음과 같은 상황에서 나타납니다. • 모듈을 처음 활성화하는 경우 • 네트워크 인터페이스가 변경되는 경우(예: 새 네트워크 어댑터 탐지, 기존 어댑터의 IP 변경, 새 VPN 터널이 설정되거나 해제됨)
열림	노란색	현재 *Umbrella*로 보호되지 않습니다. Umbrella 확인자의 연결 문제로 인해 로컬 Umbrella 모듈 DNS 보호가 활성화되어 있지 않습니다. 하나 이상의 활성 네트워크 연결이 있지만 로밍 클라이언트가 활성 연결을 통해 Umbrella 서비스에 연결할 수 없습니다. 시스템의 DNS 설정이 원래 설정(DHCP 또는 정적)으로 되돌아갑니다.	이 작동 상태는 다음과 같은 상황에서 나타납니다. • Umbrella 확인자(208.67.222.222)에 대한 UDP 포트 443 또는 UDP 포트 53 연결이 없는 경우 • 로컬 네트워크에 Umbrella DNS VA가 구성되어 있지 않은 경우 • VPN 터널이 일시적으로 해제 또는 설정 상태인 경우

상태	아이콘 색	설명	상태
방어	녹색	*Umbrella*로 보호됩니다. DNS 쿼리가 암호화되지 않았습니다. 로컬 Umbrella 모듈 DNS 보호가 활성화되어 있으며 암호화되지 않은 DNS 요청이 Umbrella 확인자로 전송됩니다.	모듈을 처음 활성화하거나 네트워크 인터페이스가 변경되는 경우 이 상태가 발생할 수 있습니다.
암호화	녹색	*Umbrella*로 보호됩니다. DNS 쿼리가 암호화되었습니다. 로컬 Umbrella 모듈 DNS 보호가 활성화되어 있으며 암호화된 DNS 요청이 Umbrella 확인자로 전송됩니다.	이 작동 상태는 다음과 같은 상황에서 나타납니다. • Umbrella 확인자(209.67.222.222)에 대한 UDP 포트 443 연결이 설정된 경우 • Umbrella 확인자(208.67.222.222)에 대한 TCP 포트 443 및 TCP 포트 53 연결이 설정된 경우
보호된 네트워크	녹색	*Umbrella*로 보호되는 네트워크에 있습니다. 현재 엔드포인트 네트워크가 Umbrella 확인자를 사용하여 보호되므로 로컬 Umbrella 모듈 DNS 보호가 활성화되어 있지 않습니다. 로밍 클라이언트가 DNS 설정을 DHCP를 통해 또는 정적으로 설정되었던 항목으로 되돌렸습니다. 연결은 암호화되지 않습니다.	이 작동 상태는 다음과 같은 상황에서 나타납니다. • 현재 엔드포인트 네트워크 이그레스(egress) IP 주소가 엔드포인트와 같은 Umbrella 계정에 등록되어 있는 경우 • 사용되는 확인자가 Umbrella 클라우드 확인자(208.67.222.222, 208.67.220.220)인 경우 • Umbrella 대시보드를 통해 구성된 정책인 "Disable Behind Protected Networks(보호된 네트워크에서는 비활성화)"에 따라 보호된 네트워크에서는 Umbrella 모듈을 비활성화해야 하는 경우 참고 모든 Cisco Umbrella 로밍 패키지 고객의 경우 네트워크 레벨 보호 기능이 제공되지 않기 때문에 이 상태가 나타날 수 없습니다.

상태	아이콘 색	설명	상태
가상 어플라이언스로 보호됨	녹색	*Umbrella* 가상 어플라이언스로 보호됩니다. Umbrella 가상 어플라이언스가 온프레미스 DNS 확인자로 구성되어 있으므로 로컬 Umbrella 모듈 DNS 보호가 활성화되어 있지 않습니다. 로밍 클라이언트가 자체적으로 비활성화되며 DNS 설정을 DHCP를 통해 또는 정적으로 설정되었던 항목으로 되돌립니다. 연결은 암호화되지 않습니다.	DHCP를 통해 또는 정적으로 엔드포인트에 구성된 DNS 주소가 Umbrella VA 주소이면 이 작동 상태가 나타납니다.
Umbrella 신뢰할 수 있는 네트워크 상태	회색	신뢰된 네트워크에 있는 동안에는 비활성화됩니다. 현재 엔드포인트 네트워크가 Umbrella 신뢰할 수 있는 네트워크로 구성되어 있으므로 로컬 Umbrella 모듈 DNS 보호가 활성화되어 있지 않습니다.	이 작동 상태는 다음과 같은 상황에서 나타납니다. • Umbrella 대시보드가 매직 도메인 이름으로 구성된 경우 • 로컬 DNS 확인자에 해당 매직 도메인 이름이나 레코드가 구성된 경우
VPN 신뢰할 수 있는 네트워크 상태	회색	신뢰된 네트워크에 있는 동안에는 비활성화됩니다. 현재 엔드포인트 네트워크가 AnyConnect VPN 신뢰할 수 있는 네트워크로 구성되어 있으므로 로컬 Umbrella 모듈 DNS 보호가 활성화되어 있지 않습니다.	이 작동 상태는 다음과 같은 상황에서 나타납니다. • AnyConnect VPN 모듈이 신뢰할 수 있는 네트워크 탐지 상태를 신뢰함으로 보고하는 경우 • AnyConnect VPN 터널이 연결되어 있지 않거나 전체 터널 모드로 설정되어 있는 경우 • Umbrella 대시보드를 통해 구성된 정책에 따라 AnyConnect VPN 신뢰할 수 있는 네트워크에서는 Umbrella 모듈을 비활성화해야 하는 경우 참고 이 설정은 모든 로밍 패키지 고객에게 적용되며 관리자가 변경할 수 없습니다.

상태	아이콘 색	설명	상태
VPN 상태로 인해 비활성화됨	회색	*VPN*이 활성화되어 있는 동안에는 비활성화됩니다. 현재 엔드포인트에 활성 AnyConnect VPN 터널이 설정되어 있으므로 로컬 Umbrella 모듈 DNS 보호가 활성화되어 있지 않습니다.	이 작동 상태는 다음과 같은 상황에서 나타납니다. • AnyConnect VPN 모듈이 신뢰할 수 있는 네트워크 탐지 상태를 신뢰하지 않음으로 보고하는 경우 • AnyConnect VPN 터널이 전체 터널 모드로 설정되어 있는 경우 • Umbrella 대시보드를 통해 구성된 정책에 따라 AnyConnect VPN 터널이 설정되어 있을 때는 Umbrella 모듈을 비활성화해야 하는 경우 참고 이 설정은 모든 로밍 패키지 고객에게 적용되며 관리자가 변경할 수 없습니다.
OrgInfo.json 상태 없음	빨간색	현재 *Umbrella*로 보호되지 않습니다. 프로파일을 찾을 수 없음. 현재 엔드포인트에 활성 AnyConnect VPN 터널이 설정되어 있으므로 로컬 Umbrella 모듈 DNS 보호가 활성화되어 있지 않습니다.	OrgInfo.json 파일이 적절한 디렉터리에 구축되지 않은 경우 이 작동 상태가 나타납니다. Windows: %ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Umbrella macOS: opt/cisco/anyconnect/umbrella
에이전트 사용 불가 상태	빨간색	현재 *Umbrella*로 보호되지 않습니다. 서비스를 사용할 수 없습니다. Umbrella 에이전트가 실행되고 있지 않으므로 로컬 Umbrella 모듈 DNS 보호가 활성화되어 있지 않습니다.	충돌이나 수동 서비스 중지로 인해 Umbrella 에이전트 서비스가 현재 실행되고 있지 않으면 이 작동 상태가 나타납니다.
.NET 종속성 상태 누락 (Windows에만 해당됨)	빨간색	현재 *Umbrella*로 보호되지 않습니다. Microsoft 4.0 NET Framework가 설치되어 있지 않습니다. Umbrella 에이전트가 실행되고 있지 않으므로 로컬 Umbrella 모듈 DNS 보호가 활성화되어 있지 않습니다. .NET 런타임 프레임워크가 없습니다.	.NET 4.0 런타임이 없어서 Umbrella 에이전트 서비스가 실행되고 있지 않으면 이 작동 상태가 나타납니다.

AnyConnect UI에도 Umbrella 로밍 보안 모듈의 통계 및 메시지 기록이 표시됩니다.

진단 정보 해석

모든 Cisco Umbrella 로밍 보안 모듈 문제를 진단하려면 DART 보고서를 실행해야 합니다. Umbrella 관련 문제 및 트러블슈팅 세부사항은 docs.umbrella.com을 참조하십시오.

11 장

로컬 정책에서 FIPS 활성화

FIPS, NGE 및 AnyConnect 정보

AnyConnect는 C3M(Cisco Common Cryptographic Module)을 통합합니다. 이 Cisco SSL 구현에는 NGE(Next Generation Encryption, 차세대 암호화) 알고리즘의 일부로 FIPS(Federal Information Processing Standard, 연방 정부 정보 처리 표준) 140-2 정책 준수 암호화 모듈 및 NSA(National Security Agency, 미국 국가 안전 보장국) Suite B 암호화가 포함됩니다.

NGE는 보안 및 성능 요건의 확대를 위해 새로운 암호화, 인증, 디지털 서명 및 키 교환 알고리즘을 도입합니다. RFC 6279는 디바이스가 미국 FIPS 140-2 표준을 충족하기 위해 지원해야 하는 Suite B 암호화 알고리즘을 정의합니다.

AnyConnect 구성 요소는 헤드엔드, ASA 또는 IOS 라우터의 구성을 기반으로 FIPS 표준 암호화를 협상하고 사용합니다. 다음 AnyConnect 클라이언트 모듈은 FIPS를 지원합니다.

- AnyConnect 코어 VPN — VPN 클라이언트용 FIPS 규정 준수는 사용자 컴퓨터 로컬 정책 파일의 FIPS 모드 매개변수를 사용하여 활성화됩니다. Suite B 암호화는 IKEv2/IPsec VPN 연결에서만 사용할 수 있습니다. 자세한 내용과 절차는 AnyConnect 코어 VPN 클라이언트에 대한 FIPS 구성을 참조하십시오.

  AnyConnect 로컬 정책 파일인 AnyConnectLocalPolicy.xml은 로컬 클라이언트에 적용되는 FIPS 모드 이외에 추가 보안 설정도 포함합니다. 이는 ASA를 통해 구축되지 않으므로 수동으로 설치하거나 엔터프라이즈 소프트웨어 구축 시스템을 사용하여 구축해야 합니다. 이 프로파일 사용에 대한 자세한 내용은 AnyConnect 로컬 정책을 참조하십시오.

- AnyConnect Network Access Manager — Network Access Manager용 FIPS 규정 준수는 AnyConnectLocalPolicy.xml 파일의 FIPS 모드 매개변수 및 Network Access Manager 프로파일의 FIPS 모드 매개변수를 사용하여 활성화됩니다. Network Access Manager용 FIPS는 Windows에서 지원됩니다. 자세한 내용과 절차는 Network Access Manager용 FIPS 구성을 참조하십시오.

AnyConnect의 FIPS 기능

기능	코어 VPN 모듈	Network Access Manager 모듈
대칭 암호화 및 무결성을 위한 AES-GCM 지원	IKEv2 페이로드 암호화 및 인증을 위한 128, 192 및 256비트 키 ESP 패킷 암호화 및 인증	소프트웨어(Windows)에서 유선 트래픽을 암호화하는 802.1AE(MACsec)용 128비트 키
해시용 SHA-2 지원, 256/384/512 비트의 SHA	IKEv2 페이로드 인증 및 ESP 패킷 인증 (Windows 7 이상 및 macOS 10.7 이상)	TLS 기반 EAP 방법으로 SHA-2 인증서 사용 가능
키 교환용 ECDH 지원	그룹 19, 20 및 21의 IKEv2 키 교환 및 IKEv2 PFS	TLS 기반 EAP 방법(Windows)에서 ECDH 사용 가능
디지털 서명, 비대칭 암호화 및 인증, 256, 384 및 521비트 Elliptic Curve에 대한 ECDSA 지원	IKEv2 사용자 인증 및 서버 인증서 확인	TLS 기반 EAP 방법으로 ECDSA 인증서 사용 가능
추가 지원:	NULL 암호화를 제외한 IPsecV3용의 모든 필수 암호화 알고리즘 IKEv2용 Diffie-Hellman 그룹 14 및 24 DTLS 및 IKEv2용 4096비트 키를 사용하는 RSA 인증서	해당 없음

[1] Linux에서는AnyConnect 파일 저장소만 ECDSA용으로 지원됩니다. 파일 저장소에 인증서를 추가하려면 Mac 및 Linux용 PEM 인증서 저장소 생성을 참조하십시오.

[2] IPsecV3에는 ESN(Extended Sequence Number, 확장된 시퀀스 번호)을 지원해야 한다고 지정되어 있지만 AnyConnect는 ESN을 지원하지 않습니다.

AnyConnect FIPS 요건

- Suite B 암호화는 IKEv2/IPsec VPN 연결에서만 사용할 수 있습니다.
- FIPS 및/또는 Suite B 지원은 보안 게이트웨이에 필요합니다. Cisco에서는 ASA 버전 9.0 이상에서 Suite B 기능과 ASA 버전 8.4.1 이상에서 FIPS 기능을 제공합니다.
- ECDSA 인증서 요건:
  - 곡선 수준과 같거나 이보다 큰 다이제스트 수준이어야 합니다. 예를 들어 EC-384 키는 SHA2-384 이상을 사용해야 합니다.
  - Windows 7 이상, macOS 10.7 이상, Red Hat Enterprise Linux 6.x 또는 6.4(64비트) 및 Ubuntu 12.4 및 12.10(64비트)에서 지원됩니다. ECDSA 스마트 카드는 Windows 7에서만 지원됩니다.

AnyConnect FIPS의 한계

- AnyConnect는 TLS/DTLS, SRTP 및 SSH Suite B를 지원하지 않습니다.
- EAP 방법은 SHA-2를 사용하여 서명된 인증서를 검증할 때 TLS 기반 EAP를 제외하고 SHA-2를 지원하지 않습니다.
- TLS v1.2 핸드셰이킹이 지원되지 않습니다.
- TLS v1.2 인증서 인증이 지원되지 않습니다.

AnyConnect FIPS에 대한 지침

- AnyConnect 클라이언트의 통계 패널(전송 정보 제목 아래)에 사용 중인 암호의 이름이 표시됩니다.
- AES-GCM이 계산 집약적인 알고리즘이므로 이 알고리즘을 사용하는 경우, 전체 데이터 속도가 느려질 수 있습니다. 일부 새로운 Intel 프로세서에는 AES-GCM의 성능을 개선하도록 특별히 도입된 특수 지침이 포함되어 있습니다. AnyConnect는 이 프로세서가 새로운 지침 지원을 실행 중인지 자동으로 탐지합니다. 새로운 지침 지원을 실행 중인 경우, AnyConnect는 새로운 지침을 사용하여 특수 지침이 없는 프로세서에 비해 VPN 데이터 속도를 상당히 개선합니다. 새로운 지침을 지원하는 프로세서 목록은 http://ark.intel.com/Search/FeatureFilter?productType=processors&AESTech=true를 참조하십시오. 자세한 내용은 http://software.intel.com/en-us/articles/intel-carry-less-multiplication-instruction-and-its-usage-for-computing-the-gcm-mode/를 참조하십시오.
- 암호화 및 무결성 확인 모두 하나의 작업으로 수행 중인 결합 모드 암호화 알고리즘은 하드웨어 암호화 가속 기능을 갖춘 SMP ASA 게이트웨이(5585, 5515-X 등)에서만 지원됩니다. AES-GCM은 Cisco에서 지원하는 결합 모드 암호화 알고리즘입니다.

  참고 IKEv2 정책에는 일반 또는 결합 모드 암호화 알고리즘 중 하나가 포함될 수 있지만 두 가지 유형 모두는 포함될 수 없습니다. 결합 모드 알고리즘이 IKEv2 정책에서 구성된 경우, 모든 일반 모드 알고리즘이 비활성화되므로 유효한 통합 알고리즘만 NULL입니다.

  IKEv2 IPsec 제안서는 각각 다른 모델을 사용하며 동일한 제안서에서는 일반 모드 및 결합 모드 암호화 알고리즘을 모두 지정할 수 있습니다. 이러한 용도로 사용자는 두 가지 모두에 대해 무결성 알고리즘을 구성해야 하며 NULL이 아닌 무결성 알고리즘을 AES-GCM 암호화를 통해 구성되도록 합니다.
- ASA가 SSL 및 IPsec용으로 다른 서버 인증서를 사용하여 구성된 경우, 신뢰할 수 있는 인증서를 사용하십시오. IPsec 및 SSL 인증서가 서로 다른 Suite B(ECDSA) 신뢰할 수 없는 인증서를 사용하는 경우 포스처 평가, WebLaunch 또는 다운로더 오류가 발생할 수 있습니다.

AnyConnect FIPS 레지스트리 변경으로 인한 엔드포인트 문제 방지

코어 AnyConnect 클라이언트에 대한 FIPS를 활성화하면 엔드포인트에서 Windows 레지스트리 설정이 변경됩니다. 엔드포인트의 다른 구성 요소는 AnyConnect가 FIPS를 활성화하고 암호화 사용을 시작한 것을 탐지할 수 있습니다. 예를 들어 RDP에서는 서버가 FIPS 규정 준수 암호화를 사용해야 하므로 Microsoft 터미널 서비스 클라이언트의 RDP(Remote Desktop Protocol, 원격 데스크톱 프로토콜)가 작동하지 않습니다.

이러한 문제를 방지하기 위해 암호화, 해싱 및 서명에 대해 FIPS 규정 준수 알고리즘 사용 파라미터를 비활성화로 변경하여 Windows Local System Cryptography(Windows 로컬 시스템 암호화) 설정에서 FIPS 암호화를 일시적으로 비활성화할 수 있습니다. 엔드포인트 디바이스를 재부팅하여 이 설정을 다시 활성화 상태로 변경할 수 있다는 점에 유의하십시오.

다음 표에서는 사용자가 알아야 할 AnyConnect의 Windows 레지스트리 변경사항을 보여줍니다.

레지스트리 키	변경
HKLM\System\CurrentControlSet\ Control\Lsa	FIPSAlgorithmPolicy는 0에서 1로 변경되었습니다.
HKCU\Software\Microsoft\Windows\ CurrentVersion\Internet Settings	SecureProtocols 설정이 원래 설정대로 0x080의 비트 “or”을 수행하여 TLSV1으로 변경되었습니다.
HKLM\Software\Policies\Microsoft\ Windows\CurrentVersion\Internet	SecureProtocols 설정이 원래 설정대로 0x080의 비트 “or”을 수행하여 TLSV1으로 변경되었습니다. 이렇게 하면 그룹 정책에 대해 TLSv1이 설정됩니다.

AnyConnect 코어 VPN 클라이언트에 대한 FIPS 구성

AnyConnect 코어 VPN에 대한 FIPS 활성화

프로시저

단계 1 AnyConnect 프로파일 편집기에서 VPN 로컬 정책 프로파일을 열거나 생성하십시오.

단계 2 **FIPS Mode(FIPS 모드)**를 선택하십시오.

단계 3 VPN 로컬 정책 프로파일을 저장하십시오.

FIPS가 활성화되었음이 나타나도록 프로파일의 이름을 지정하는 것이 좋습니다.

Windows 설치 시 FIPS 활성화

Windows 설치 시 Cisco MST 파일을 표준 MSI 설치 파일에 적용하여 AnyConnect 로컬 정책에서 FIPS를 활성화할 수 있습니다. 이 MST 파일을 다운로드할 수 있는 위치 정보는 FIPS에 대해 받은 라이센스 정보를 참조하십시오. 설치하면 활성화된 FIPS로 AnyConnect 로컬 정책 파일이 생성됩니다. 이 유틸리티를 실행한 후 사용자의 시스템을 업데이트하십시오.

참고 이 MST는 FIPS만 활성화합니다. 다른 매개변수를 변경하지 않습니다. Windows 설치 도중 다른 로컬 정책 설정을 변경하려면 MST 파일에서 로컬 정책 파라미터 활성화를 참조하십시오.

Network Access Manager용 FIPS 구성

FIPS 및 비FIPS 네트워크 모두에 동시에 연결되거나 FIPS 네트워크에만 연결되도록 Network Access Manager를 구성할 수 있습니다.

프로시저

단계 **1** Network Access Manager용 FIPS 활성화

FIPS를 활성화하면 Network Access Manager를 FIPS 및 비FIPS 네트워크 모두에 연결할 수 있습니다.

단계 **2** 필요시 Network Access Manager용 FIPS 모드 적용 참조

FIPS 모드를 적용하면 FIPS 네트워크로 Network Access Manager 연결을 제한합니다.

Network Access Manager용 FIPS 활성화

프로시저

단계 **1** 다음을 수행하여 AnyConnect 로컬 정책에서 FIPS 모드를 활성화하십시오.

a) AnyConnect 프로파일 편집기에서 VPN 로컬 정책 프로파일을 열거나 생성하십시오.
b) **FIPS Mode(FIPS 모드)**를 선택하십시오.
c) VPN 로컬 정책 프로파일을 저장하십시오.

프로파일은 FIPS가 활성화되었음이 나타나도록 이름을 지정하는 것이 좋습니다.

단계 **2** 다음을 수행하여 AnyConnect Network Access Manager 클라이언트 프로파일에서 FIPS 모드를 활성화하십시오.

a) AnyConnect 프로파일 편집기에서 Network Access Manager 프로파일을 열거나 생성하십시오.

b) **Client Policy(**클라이언트 정책**)** 구성 창을 선택하십시오.
c) **Administrative Status(**관리 상태**)** 섹션에서 Enable for **FIPS Mode**(FIPS 모드 활성화)를 선택하십시오.
d) Network Access Manager 프로파일을 저장하십시오.

FIPS가 활성화되었음이 나타나도록 프로파일의 이름을 지정하는 것이 좋습니다.

Network Access Manager용 FIPS 모드 적용

Network Access Manager 프로파일에서 허용된 연계와 암호화 모드 및 인증 방법을 제한하여 엔터프라이즈 직원들이 FIPS 규정을 준수하는 네트워크에만 연결할 수 있도록 합니다.

먼저 Network Access Manager용 FIPS 활성화하여 FIPS 모드를 적용할 수 있도록 해야 합니다.

프로시저

단계 **1** AnyConnect 프로파일 편집기에서 Network Access Manager 프로파일을 여십시오.
단계 **2** Network Access Manager FIPS 규정 준수에는 개인 WPA2 Personal(WPA2-PSK)과 WPA2 Enterprise(802.1X)를 포함하여 FIPS 승인된 AES 암호화 모드가 필요합니다.
단계 **3** Network Access Manager FIPS 지원은 EAP 방식 EAP-TLS, EAP-TTLS, PEAP, EAP-FAST 및 LEAP를 포함합니다.
단계 **4** Network Access Manager 프로파일을 저장하십시오.

FIPS만 연결되었음이 나타나도록 프로파일의 이름을 지정하는 것이 좋습니다.

12 장

Cisco AnyConnect 고객 경험 피드백 모듈

참고 기본적으로 개인 및 기업 데이터가 수집됩니다.

CEF(Customer Experience Feedback, 고객 경험 피드백) 모듈은 고객이 사용하고 활성화한 기능 및 모듈에 대한 정보를 제공합니다. 이 정보를 바탕으로 사용자 경험에 대한 통찰력을 얻을 수 있으므로 Cisco는 AnyConnect의 품질, 안정성, 성능 및 사용자 경험을 지속적으로 개선할 수 있습니다.

정보 수집 및 사용에 대한 자세한 내용은 AnyConnect Secure Mobility Client 보충 자료에 액세스할 수 있는 Cisco 온라인 개인정보 보호정책 중요 사항 페이지를 참조하십시오. 모든 데이터는 익명으로 수집되며 개인 식별 데이터를 포함하지 않습니다. 또한 이 데이터는 안전하게 전송됩니다.

Cisco는 다음 유형의 데이터를 수집합니다.

- 사용성 데이터 — 자세한 내용은 개인정보 보호정책을 참조하십시오. 이 데이터는 한 달에 한 번 수집 및 전송됩니다.
- 웹 위협 데이터 — 위협이 보고될 때마다 전송됩니다.
- 충돌 보고서 — AnyConnect에서 생성된 충돌 덤프 파일을 24시간마다 확인 및 수집한 다음 고객 경험 피드백 서버에 전송합니다.

고객 경험 피드백 모듈의 주요 구성 요소는 다음과 같습니다.

- 피드백 모듈 — 정보를 수집하고 서버에 이 정보를 주기적으로 전송하는 AnyConnect 소프트웨어 구성 요소입니다.
- Cisco 피드백 서버 — 고객 경험 피드백 데이터를 수집하고 이 데이터를 Raw 포맷으로 임시 저장소에 저장하는 Cisco 소유의 클라우드 인프라입니다.

• 고객 경험 피드백 구성, 275 페이지

고객 경험 피드백 구성

AnyConnect 고객 경험 피드백 모듈은 AnyConnect를 통해 구축되며 기본적으로 활성화되어 있습니다. 고객 경험 피드백 프로파일을 생성하여 전송되는 피드백을 수정할 수 있습니다(경험 피드백 전체

제외 포함). 이 방법은 피드백 모듈을 비활성화하기 위해 권장되는 방법이지만 AnyConnect 구축 시 피드백 모듈을 모두 제거할 수 있습니다.

시작하기 전에

고객 경험 피드백 모듈은 자동으로 활성화됩니다.

프로시저

단계 **1** 독립 실행형 고객 경험 피드백 프로파일 편집기를 열거나 ASDM에서 다음을 수행하십시오. **Configuration(**구성**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **Network (Client) Access(**네트워크**(**클라이언트**)** 액세스**)** > **AnyConnect Client Profiles(AnyConnect** 클라이언트 프로파일**)**로 이동합니다.

단계 **2** **Feedback Service Profile(**피드백 서비스 프로파일**)**의 프로파일 사용을 통해 AnyConnect 클라이언트 프로파일을 생성합니다.

단계 **3** 피드백을 제공하지 않으려는 경우 **Enable customer Experience Feedback Service(**고객 경험 피드백 서비스 활성화**)**를 선택 취소합니다.

설치 후 언제든지 피드백을 비활성화할 수 있습니다.

단계 **4** AnyConnect에서 생성된 충돌 보고서를 전송하지 않으려면 **Include Crash Report(**충돌 보고서 포함**)**를 선택 취소합니다.

기본값은 충돌 보고서를 포함합니다.

단계 **5** 선택한 고객 키 또는 ID를 입력하십시오.

이 ID를 사용하여 Cisco는 조직의 정보를 식별할 수 있습니다.

13 장

AnyConnect 문제 해결

문제 해결을 위한 정보 수집

통계 세부사항 보기

관리자 또는 최종 사용자가 현재 AnyConnect 세션에 대한 통계 정보를 볼 수 있습니다.

프로시저

단계 **1** Windows에서 **Advanced Window(고급 창)** > **Statistics(통계)** > **VPN drawer(VPN 드로어)**로 이동합니다. Linux에서 사용자 GUI에 있는 **Details(세부사항)** 버튼을 클릭합니다.

단계 **2** 클라이언트 컴퓨터에 로드된 패키지에 따라 다음 옵션 중에서 선택합니다.

- **Export Stats(통계 내보내기)**— 최신 분석 및 디버깅을 위해 연결 통계를 텍스트 파일로 저장합니다.
- **Reset(재설정)**— 연결 정보를 영(0)으로 재설정합니다. AnyConnect는 즉시 새 데이터 수집을 시작합니다.

- **Diagnostics(**진단**)**— 클라이언트 연결 분석 및 디버깅을 위해 특정 로그 파일 및 진단 정보가 함께 포함된 AnyConnect DART(Diagnostics and Reporting Tool, 진단 및 보고 툴) 마법사를 시작합니다.

DART를 실행하여 문제 해결을 위한 데이터 수집

DART는 AnyConnect 설치 및 연결 문제 해결을 위해 데이터를 수집하는 데 사용할 수 있는 AnyConnect 진단 및 보고 툴입니다. DART에서 Cisco Technical Assistance Center(TAC) 분석을 위한 로그, 상태 및 진단 정보를 조합합니다.

DART 마법사는 AnyConnect가 실행되는 디바이스에서 실행됩니다. DART에는 관리자 권한이 필요하지 않습니다. AnyConnect에서 DART를 실행하거나 AnyConnect 없이 자체적으로 DART를 실행할 수 있습니다.

지원되는 운영 체제는 다음과 같습니다.

- Windows
- macOS
- Linux

프로시저

단계 **1** 다음과 같이 DART를 실행하십시오.

- Windows 디바이스의 경우 Cisco AnyConnect Secure Mobility Client를 시작합니다.
- Linux 디바이스의 경우 **Applications(**애플리케이션**)** > **Internet(**인터넷**)** > **Cisco DART**

  또는 /opt/cisco/anyconnect/dart/dartui를 선택하십시오.
- Mac 디바이스의 경우 **Applications(**애플리케이션**)** > **Cisco** > **Cisco DART** 를 선택하십시오.

단계 **2** **Statistics(**통계**)** 탭을 클릭한 다음 **Diagnostics(**진단**)**를 클릭합니다.

단계 **3** **Default(**기본값**)** 또는 **Custom(**사용자 정의**)** 번들 생성을 선택하십시오.

- Default(기본값) - AnyConnect 로그 파일, 컴퓨터에 관한 일반적인 정보 및 DART가 수행한 작업과 수행하지 않은 작업의 요약 등 일반적인 로그 파일과 진단 정보가 포함됩니다. 번들은 기본 이름이 `DARTBundle.zip`이며 로컬 데스크톱에 저장됩니다.
- Custom(사용자 정의) — 번들에 포함할 파일(또는 기본 파일) 및 번들을 저장할 위치를 지정할 수 있습니다.

  Linux 및 macOS에 올바르게 적용된 경로 및 필터링 변경 사항은 로그에 포함되지 않으므로 중요한 이벤트를 더 효율적으로 확인할 수 있습니다. 이 옵션을 사용하지 않는 경우에는 syslog 이벤트 속도 제한에 도달하면 중요한 이벤트가 삭제되어 필요한 이벤트를 놓칠 수 있습니다. 또한 캡처 필터링 설정을 사용하면 Mac용 시스템 pf 컨피그레이션 파일과 AnyConnect 필터링 컨피그레

이션 파일을 모두 확인할 수 있습니다. Linux의 경우에는 DART에 iptables 및 ip6tables 출력이 표시됩니다. 단, sudo를 통해 DART 툴을 실행하는 경우가 아니면 이러한 컨피그레이션 중 대부분에 대한 액세스는 제한됩니다.

참고 macOS의 경우 사용 가능한 옵션은 **Default(**기본값**)**뿐입니다. 번들에 포함할 파일을 사용자 지정할 수 없습니다.

참고 **Custom(**사용자 정의**)**을 선택하는 경우 번들에 포함할 파일을 구성할 수 있으며 파일의 다른 저장 위치를 지정할 수 있습니다.

단계 **4** DART가 파일의 기본 목록을 수집하는 시간이 오래 걸리는 것으로 보이는 경우 **Cancel(**취소**)**을 클릭하고 DART를 다시 실행하여 일부 파일만 선택하는 **Custom(**사용자 정의**)** 을 선택하십시오.

단계 **5** **Default(**기본값**)**를 선택한 경우 DART가 번들을 생성하기 시작합니다. **Custom(**사용자 정의**)**을 선택한 경우 계속해서 마법사 프롬프트를 따라 로그, 환경 설정 파일, 진단 정보 및 기타 사용자 정의를 선택하십시오.

로그를 수집하여 설치 또는 제거 문제에 대한 데이터 수집(Windows용)

AnyConnect 설치 또는 제거 시에 장애가 발생하는 경우 로그를 수집해야 합니다. DART 모음에는 이 장애를 진단하는 기능이 없기 때문입니다.

AnyConnect 파일의 압축을 푼 것과 같은 디렉터리에서 msiexec 명령을 실행합니다.

- 설치 장애의 경우 다음 명령을 입력합니다.

  ```
  C:/temp>msiexec /i anyconnect-win-version-pre-deploy-k9.msi /lvx c:/Temp/ac-install.log?
  ```

  여기서 *c:/temp/ac-install.log?* 에는 선택한 파일 이름을 입력할 수 있습니다.

- 제거 장애의 경우 다음 명령을 입력합니다.

  ```
  c:/temp/msiexec /x anyconnect-win-version-pre-deploy-k9.msi /lvx c:/Temp/ac-install.log?
  ```

  여기서 *c:/temp/ac-uninstall.log?*에는 선택한 파일 이름을 입력할 수 있습니다.

참고 제거 장애의 경우 현재 설치되어 있는 버전과 관련된 MSI를 사용해야 합니다.

위의 명령을 변경하여 올바르게 설치 또는 제거되지 않은 Windows의 모듈에 대한 정보를 캡처할 수 있습니다.

컴퓨터 시스템 정보 가져오기

Windows의 경우 **msinfo32 /nfo c:\msinfo.nfo**를 입력하십시오.

Systeminfo 파일 덤프 가져오기

Windows의 경우 sysinfo 명령 프롬프트에서 **c:\sysinfo.txt** 를 입력하십시오.

레지스트리 파일 확인

SetupAPI 로그 파일에 있는 항목은 아래와 같이 찾을 수 없는 파일을 나타냅니다.

```
E122 Device install failed. Error 2: The system cannot find the file specified.
E154 Class installer failed. Error 2: The system cannot fine the file specified.
```

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce 레지스트리 키가 존재하는지 확인하십시오. 이 레지스트리 키가 없는 경우 모든 inf 설치 패키지의 사용은 금지됩니다.

AnyConnect 로그 파일 위치

로그는 다음 파일에 보존됩니다.

Windows —\Windows\Inf\setupapi.app.log or \Windows\Inf\setupapi.dev.log

- Windows—\Windows\Inf\setupapi.app.log or \Windows\Inf\setupapi.dev.log

참고 Windows에서 숨겨진 파일을 표시해야 합니다.

초기 웹 구축 설치인 경우, 로그 파일은 사용자별 임시 디렉토리에 있습니다.

%TEMP%\anyconnect-win-4.X.xxxxx-k9-install-yyyyyyyyyyyyyy.log.

업그레이드가 최적의 게이트웨이에서 시작된 경우, 로그 파일은 다음 위치에 있습니다.

%WINDIR%\TEMP\anyconnect-win-3.X.xxxxx-k9-install-yyyyyyyyyyyyyy.log.

설치할 클라이언트의 버전에 대한 최근 파일을 확보하십시오. *xxx*는 버전에 따라 다르며 *yyyyyyyyyyyyy*는 설치 날짜 및 시간을 나타냅니다.

AnyConnect 연결 또는 연결 끊기 문제

AnyConnect 초기 연결 설정 안 함 또는 연결 끊기 안 함

문제점 AnyConnect가 초기 연결을 설정하지 않거나 Cisco AnyConnect Secure Mobility Client 창에서 Disconnect(연결 끊기)를 클릭하면 예상치 않은 결과가 발생할 수 있습니다.

해결 방법 다음을 확인합니다.

- Citrix Advanced Gateway Client 버전 2.2.1을 사용 중인 경우, Citrix에서 CtxLsp.dll 문제를 해결할 때까지 Citrix Advanced Gateway Client를 제거합니다.
- AT&T Sierra 무선 875 카드가 포함된 AT&T Communication Manager 버전 6.2 또는 6.7을 사용 중인 경우, 다음 단계에 따라 문제를 해결하십시오.
  1. Aircard에서 가속화를 비활성화합니다.
  2. **AT&T Communication Manager > Tools(**툴**) > Settings(**설정**) > Acceleration(**가속화**) > Startup(**시작**)**을 시작합니다.
  3. **manual**을 입력합니다.
  4. **Stop(**중지**)**을 클릭합니다.
- 연결 실패 표시를 검색하려면 다음과 같이 ASA에서 구성 파일을 가져오십시오.
  - ASA 콘솔에서 **write net x.x.x.x:ASA-Config.txt**를 입력합니다. 여기서 *x.x.x.x*는 네트워크에 있는 TFTP 서버의 IP 주소입니다.
  - ASA 콘솔에서 **show running-config**를 입력합니다. 구성 파일을 잘라 텍스트 편집기에 붙여 넣고 저장합니다.
- 다음과 같이 ASA 이벤트 로그 보기:
  1. ASA 콘솔에서 ssl, webvpn, anyconnect 및 인증 이벤트를 보려면 다음 행을 추가합니다.

     ```
     config terminal
     logging enable
     logging timestamp
     logging class auth console debugging
     logging class webvpn console debugging
     logging class ssl console debugging
     logging class anyconnect console debugging
     ```

  2. AnyConnect 클라이언트 연결을 시도하고 연결 오류가 발생하면 콘솔에서 로그 정보를 잘라 텍스트 편집기에 붙여 넣고 저장합니다.
  3. **`no logging enable`**을 입력하여 로깅을 비활성화합니다.
- Windows 이벤트 뷰어를 사용하여 클라이언트 컴퓨터에서 Cisco AnyConnect VPN 클라이언트 로그를 가져오십시오.
  1. **Start(**시작**) > Run(**실행**)**을 선택하고 **`eventvwr.msc /s`**를 입력합니다.
  2. Windows 7의 애플리케이션 및 서비스 로그에서 `Cisco AnyConnect VPN Client(Cisco AnyConnect VPN 클라이언트)`를 찾고 **Save Log File As..(**다른 이름으로 로그 파일 저장**)**를 선택합니다.
  3. `AnyConnectClientLog.evt`와 같은 파일 이름을 할당합니다. `.evt` 파일 형식을 사용해야 합니다.
- Windows 진단 디버그 유틸리티를 수정합니다.
  1. WinDbg 문서에서와 같이 vpnagent.exe 프로세스를 첨부합니다.
  2. IPv6/IPv4 IP 주소 할당과 상충하는 부분이 있는지 판단합니다. 확인된 모든 충돌에 대한 이벤트 로그를 참조하십시오.

3. 충돌이 확인된 경우, 사용 중인 클라이언트 컴퓨터 레지스트리에 추가 라우팅 디버그를 추가합니다. 이러한 충돌은 AnyConnect 이벤트 로그에 다음과 같이 표시될 수 있습니다.

```
Function: CRouteMgr:modifyRoutingTable Return code: 0xFE06000E File: .\VpnMgr.cpp
Line:1122
Description: ROUTEMGR_ERROR_ROUTE_TABLE_VERIFICATION_FAILED.
Termination reason code 27: Unable to successfully verify all routing table
modifications are correct.

Function: CChangeRouteTable::VerifyRouteTable Return code: 0xFE070007
File: .\RouteMgr.cpp Line: 615 Description: ROUTETABLE_ERROR_NOT_INITIALIZED
gr.cpp Line: 615 Description: ROUTETABLE_ERROR_NOT_INITIALIZED
```

4. 특정 레지스트리 항목(Windows) 또는 파일(Linux 및 macOS)을 추가하여 연결의 일회성 라우트 디버깅을 활성화합니다.
   - 32비트 Windows에서 DWORD 레지스트리 값은 다음과 같습니다.
     `HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\Cisco AnyConnect Secure Mobility Client\DebugRoutesEnabled`
   - 64비트 Windows에서 DWORD 레지스트리 값은 다음과 같습니다.
     `HKEY_LOCAL_MACHINE\Software\WOW6432node\Cisco\Cisco AnyConnect Secure Mobility Client\DebugRoutesEnabled`
   - Linux 또는 macOS에서 sudo 터치 명령을 사용하여 다음 경로에서 파일을 생성합니다.
     `/opt/cisco/anyconnect/debugroutes`

참고 터널 연결이 시작되면 키 또는 파일이 삭제됩니다. 이 파일의 키 또는 콘텐츠 값은 키 또는 파일의 기존 값이 디버깅 활성화에 충분하므로 중요하지 않습니다.

VPN 연결을 시작합니다. 이 키 또는 파일이 검색되었을 때 두 개의 라우트 디버그 텍스트 파일이 시스템의 임시 디렉토리(일반적으로 Windows의 경우 C:\Windows\Temp이고 Mac 또는 Linux의 경우 /tmp)에 생성됩니다. 두 개의 파일(debug_routechangesv4.txt4 및 debug_routechangesv6.txt)은 이미 존재하는 경우 덮어쓰기됩니다.

트래픽을 전달하지 않는 AnyConnect

문제점 AnyConnect 클라이언트가 연결된 사설 네트워크에 데이터를 전송할 수 없습니다.

해결 방법 다음을 확인합니다.

- AT&T Sierra 무선 875 카드가 포함된 AT&T Communication Manager 버전 6.2 또는 6.7을 사용 중인 경우, 다음 단계에 따라 문제를 해결하십시오.
  1. Aircard에서 가속화를 비활성화합니다.
  2. AT&T Communication Manager > Tools(툴) > Settings(설정) > Acceleration(가속화) > Startup(시작)을 시작합니다.

3. **manual**을 입력합니다.
4. **Stop(**중지**)**을 클릭합니다.

- vpn-sessiondb 세부사항 anyconnect 필터 이름 <username> 명령 표시의 출력을 가져옵니다. 출력에서 필터 이름을 XXXXX로 지정하고 access-list XXXXX 명령 표시를 위해 아래와 같은 출력을 가져옵니다. ACL에서 의도한 트래픽 흐름을 차단하고 있지 않은지 확인합니다.
- AnyConnect VPN Client(AnyConnect VPN 클라이언트) > Statistics(통계) > Details(세부사항) > Export(내보내기)(AnyConnect ExportedStats.txt DART)에서 DART 파일 또는 출력을 가져옵니다. 통계, 인터페이스 및 라우팅 테이블을 확인합니다.
- NAT 명령문용 ASA 구성 파일을 확인합니다. NAT를 활성화한 경우, 네트워크 주소 변환에서 클라이언트로의 데이터 반환을 면제해야 합니다. 예를 들어 AnyConnect 풀의 IP 주소를 NAT 면제시키려면 다음 코드를 사용하십시오.

```
access-list in_nat0_out extended permit ip any 10.136.246.0 255.255.255.0
ip local pool IPPool1 10.136.246.1-10.136.246.254 mask 255.252.0.0
nat (inside) 0 access-list in_nat0_out
```

- 터널링 기본 게이트웨이에서 설정이 활성화되어 있는지 확인합니다. 기존의 기본 게이트웨이는 암호 해독되지 않은 트래픽을 위한 최종 경로입니다.

```
route outside 0.0.209.165.200.225
route inside 0 0 10.0.4.2 tunneled
```

  VPN 클라이언트가 VPN Gateway의 라우팅 테이블에 없는 리소스에 액세스해야 하는 경우, 패킷이 표준 기본 게이트웨이를 통해 라우팅됩니다. VPN Gateway는 내부 라우팅 테이블 전체를 포함할 필요가 없습니다. 터널링 키워드를 사용하는 경우 IPsec/SSL VPN 연결에서 전송되는 암호 해독된 트래픽을 라우트에서 처리합니다. 표준 트래픽은 최후의 방법으로 209.165.200.225에 라우팅되며, VPN에서 전송되는 트래픽은 10.0.4.2에 라우팅되고 암호 해독됩니다.

- AnyConnect를 사용하여 터널을 설정하기 전후에 ipconfig /all의 텍스트 덤프 및 라우트 프린트 출력을 수집합니다.
- 클라이언트의 네트워크 패킷 캡처를 수행하거나 ASA에서 캡처를 사용할 수 있습니다.

참고 일부 애플리케이션(Microsoft Outlook 등)이 터널을 통해 작동하지 않을 경우, 허용된 크기를 확인하려면 ping의 확장 집합이 있는 네트워크에서 알려진 디바이스를 ping합니다(예: ping -| 500, ping -| 1000, ping -| 1500 및 ping -| 2000). Ping 결과는 네트워크의 단편화 문제에 대한 단서를 제공합니다. 사용자의 단편화 경험에 대비하여 특별한 그룹을 구성하고 이 그룹의 anyconnect mtu를 1200으로 설정할 수 있습니다. 또한 기존 IPsec 클라이언트에서 MTU.exe 설정 유틸리티를 복사하여 물리적 어댑터 MTU를 1300에 적용할 수 있습니다. 재부팅 시 차이점을 인지하고 있는지 확인하십시오.

VPN 서비스 실패

VPN 서비스 연결 실패

문제점 "계속 진행할 수 없습니다. VPN 서비스에 접속할 수 없습니다."라는 메시지가 나타납니다. AnyConnect용 VPN 서비스가 실행되고 있지 않습니다.

해결 방법 다른 애플리케이션이 서비스와 충돌하는지를 확인합니다. 서비스와 충돌하는 대상 판단을 참조하십시오.

서비스와 충돌하는 대상 판단

다음 절차는 부팅 시 서버의 초기화 또는 다른 실행 서비스(예를 들어 서비스 시작 실패와 같은 이유)와 충돌하는지 판단합니다.

프로시저

단계 **1** Windows 관리 툴에서 서비스를 확인하여 Cisco AnyConnect VPN 에이전트가 실행되고 있지 않은지 확인하십시오. 실행하고 있으나 오류 메시지가 계속 표시되는 경우, 워크스테이션의 다른 VPN 애플리케이션을 비활성화하거나 제거해야 할 수도 있습니다. 해당 조치를 취한 후 재부팅하여 이 단계를 반복하십시오.

단계 **2** Cisco AnyConnect VPN 에이전트를 시작해 보십시오.

단계 **3** 서비스를 시작할 수 없었다고 알리는 메시지가 있는지 이벤트 뷰어에서 AnyConnect 로그를 확인하십시오. 2단계의 수동 재시작에 대한 타임스탬프 및 워크스테이션이 부팅된 시기를 확인하십시오.

단계 **4** 충돌 메시지의 동일한 일반 타임스탬프가 있는지 이벤트 뷰어에서 시스템 및 애플리케이션 로그를 확인하십시오.

단계 **5** 로그가 서비스 시작 실패를 나타내는 경우, 다음 중 하나를 표시하는 동일한 타임스탬프에 대한 기타 정보 메시지가 있는지 찾아보십시오.

- 없는 파일 — 독립 실행형 MSI 설치에서 AnyConnect 클라이언트를 다시 설치하여 없는 파일을 배제하십시오.
- 다른 종속 서비스의 지연 — 시동 작업을 비활성화하여 워크스테이션의 부팅시간 속도를 높이십시오.
- 다른 애플리케이션 또는 서비스와 충돌 — 다른 서비스에서 vpnagent가 사용 중인 포트와 동일한 포트에서 수신 대기하고 있는지 또는 일부 HIDS 소프트웨어에서 본 소프트웨어가 포트에서 수신 대기하는 것을 차단하고 있는지 확인하십시오.

단계 **6** 로그가 원인을 직접 표시하지 않는 경우 직접 실행해 보면서 충돌을 확인하십시오. 가능성이 가장 높은 원인이 확인되면 서비스 패널에서 해당 서비스(VPN 제품, HIDS 소프트웨어, spybot 클리너, 스니퍼, 안티바이러스 소프트웨어 등)를 비활성화하십시오.

단계 **7** 재부팅합니다. VPN 에이전트 서비스가 여전히 시작되지 않는 경우 운영 체제의 기본 설치를 통해 설치하지 않은 서비스 사용을 해제하십시오.

VPN 클라이언트 드라이버에서 오류 발생(Microsoft Windows 업데이트 이후)

문제점 최근에 Microsoft certclass.inf 파일을 업데이트한 경우, VPN 연결을 설정하려고 시도할 때 다음 메시지가 표시됩니다.

```
The VPN client driver has encountered an error.
```

C:\WINDOWS\setupapi.log에서 다음 오류를 확인할 수 있습니다.

```
#W239 The driver signing class list "C:\WINDOWS\INF\certclass.inf" was missing or invalid.
 Error 0xfffffbf8: Unknown Error. Assuming all device classes are subject to driver signing
 policy.
```

해결 방법 명령 프롬프트에서 **C:\>systeminfo**를 입력하거나 C:\WINDOWS\WindowsUpdate.log를 확인하여 최근에 설치된 업데이트를 확인합니다. VPN 드라이버를 복구하려면 지침을 따르십시오.

VPN 클라이언트 드라이버 오류 복구

앞에서 수행된 단계에서 카탈로그가 손상되지 않았음을 나타내더라도 중요한 파일이 서명되지 않은 파일로 덮어쓰여졌을 수 있습니다. 오류가 계속 발생하는 경우 Microsoft에서 사례를 열고 드라이버 서명 데이터베이스가 손상된 원인을 확인하십시오.

프로시저

단계 **1** 관리자로 명령 프롬프트를 여십시오.

단계 **2** **net stop CryptSvc**를 입력하십시오.

단계 **3** **esentutl /g %systemroot% \ System32 \ catroot2 \ {F750E6C3-38EE-11D1-85E5-00C04FC295EE} \ catdb** 를 입력하여 유효성을 확인하도록 데이터베이스를 분석하고 %/WINDIR% \ system32 \ catroot2에 catroot2_old 디렉토리의 이름을 변경하십시오.

단계 **4** 프롬프트가 표시되면 **OK(확인)** 를 선택하여 복구를 시도하십시오. 명령 프롬프트를 종료하고 재부팅하십시오.

드라이버 충돌

VPNVA.sys 드라이버 충돌 해결

문제점 VPNVA.sys 드라이버가 충돌합니다.

해결 방법 Cisco AnyConnect 가상 어댑터에 바인딩된 중간 드라이버를 찾아서 선택 취소합니다.

vpnagent.exe 드라이버 충돌 해결

프로시저

단계 **1** c:\vpnagent라는 디렉토리를 생성하십시오.

단계 **2** 작업 관리자에서 Process(프로세스) 탭을 살펴보고 vpnagent.exe의 프로세스 PID를 판단하십시오.

단계 **3** 명령 프롬프트를 열고 디버깅 툴을 설치한 디렉토리를 변경하십시오. 기본적으로 Windows용 디버깅 툴은 `C:\Program Files\Debugging Tools`에 있습니다.

단계 **4** **cscript vpnagent4.vbs -crash -p PID -o c:\vpnagent -nodumponfirst**를 입력하십시오. 여기서 *PID*는 **vpnagent.exe**의 PID입니다.

단계 **5** 창을 최소화된 상태로 여십시오. 모니터링하는 동안 시스템을 로그오프할 수 없습니다.

단계 **6** 충돌이 발생하면 c:\vpnagent의 콘텐츠를 zip 파일로 수집하십시오.

단계 **7** crashdmp 파일을 세밀하게 진단하려면 **!analyze -v** 를 사용하십시오.

Network Access Manager의 링크/드라이버 문제

Network Access Manager에서 유선 어댑터를 인식하지 못할 경우, 네트워크 케이블의 플러그를 뽑았다가 다시 삽입을 시도하십시오. 작동하지 않으면 링크 문제가 있을 수 있습니다. Network Access Manager가 어댑터의 올바른 링크 상태를 판단할 수 없는 경우도 있습니다. NIC 드라이버의 연결 속성을 확인합니다. 고급 패널에서 "Wait for Link(링크 대기)" 옵션이 있을 수 있습니다. 이 설정이 켜져 있는 경우, 유선 NIC 드라이버 초기화 코드에서 자동 협상을 완료하기 위해 대기하며 링크가 있는지 판단합니다.

기타 충돌

AnyConnect 충돌

문제점 리부팅한 후 “시스템이 오류에서 복구되었습니다.”라는 메시지를 수신했습니다.

해결 방법 C:\DOCUME~1\jsmith\LOCALS~1\Temp와 같은 %temp% 디렉터리에서 .log 및 .dmp 생성 파일을 수집합니다. 파일을 복사하거나 백업합니다. .log 또는 .dmp 파일 백업 방법을 참조하십시오.

.log 또는 .dmp 파일 백업 방법

프로시저

단계 **1** Start(시작) > Run(실행) 메뉴에서 Microsoft 유틸리티 Dr. Watson(Drwtsn32.exe)을 실행합니다.

단계 **2** 다음을 구성하고 **OK(**확인**)**를 클릭하십시오.

```
Number of Instructions     : 25
Number of Errors to Save : 25
Crash Dump Type    : Mini
Dump Symbol Table : Checked
Dump All Thread Contexts : Checked
Append to Existing Log File : Checked
Visual Notification : Checked
Create Crash Dump File : Checked
```

단계 **3** 클라이언트 컴퓨터에서 Start(시작) > Run(실행) 메뉴에 **eventvwr.msc /s** 를 입력하여 Windows 이벤트 뷰어로부터 Cisco AnyConnect VPN 클라이언트 로그를 가져오십시오.

단계 **4** Windows 7의 애플리케이션 및 서비스 로그에서 **Cisco AnyConnect VPN Client(Cisco AnyConnect VPN** 클라이언트**)**를 찾고 **Save Log File As..(**다른 이름으로 로그 파일 저장**)**를 선택합니다. .evt 파일 형식으로 AnyConnectClientLog.evt와 같은 파일 이름을 할당합니다.

vpndownloader에서의 AnyConnect 충돌(LSP(Layered Service Provider, 계층화된 서비스 공급자) 모듈 및 NOD32 AV)

문제점 AnyConnect에서 연결을 설정하려고 시도할 때 ssl 세션을 성공적으로 인증하고 구축하지만 LSP 또는 NOD32 AV를 사용할 경우 AnyConnect 클라이언트가 vpndownloader에서 충돌합니다.

해결 방법 버전 2.7에서 인터넷 모니터링 구성 요소를 제거하고 ESET NOD32 AV 버전 3.0으로 업그레이드합니다.

블루 스크린(AT & T 다이얼러)

문제점 AT & T 다이얼러를 사용 중인 경우, 클라이언트 운영 체제에서 경우에 따라 블루 스크린이 나타나 미니 덤프 파일을 생성할 수 있습니다.

해결 방법 최신 7.6.2 AT&T Global Network Client로 업그레이드하십시오.

보안 경고

Microsoft Internet Explorer 보안 경고

문제점 다음 텍스트가 포함된 보안 경고 창이 Microsoft Internet Explorer에 나타납니다.

```
Information you exchange with this site cannot be viewed or changed by others. However,
there is a problem with the site's security certificate. The security certificate was issued
 by a company you have not chosen to trust. View the certificate to determine whether you
want to trust the certifying authority.
```

해결 방법 신뢰할 수 있는 사이트로 인식되지 않는 ASA에 연결할 때 이 경고가 나타날 수 있습니다. 이 경고를 방지하려면 클라이언트에 신뢰할 수 있는 루트 인증서를 설치합니다. 클라이언트에 신뢰할 수 있는 루트 인증서 설치를 참조하십시오.

"알 수 없는 기관에서 인증" 경고

문제점 "알 수 없는 기관에서 웹 사이트 인증" 경고 창이 브라우저에 나타날 수 있습니다. 보안 경고 창의 상단 절반 부분에는 다음 텍스트가 표시됩니다.

```
Unable to verify the identity of <Hostname_or_IP_address> as a trusted site.
```

해결 방법 신뢰할 수 있는 사이트로 인식되지 않는 ASA에 연결할 때 이 보안 경고가 나타날 수 있습니다. 이 경고를 방지하려면 클라이언트에 신뢰할 수 있는 루트 인증서를 설치합니다. 클라이언트에 신뢰할 수 있는 루트 인증서 설치를 참조하십시오.

클라이언트에 신뢰할 수 있는 루트 인증서 설치

시작하기 전에

신뢰할 수 있는 루트 인증서로 사용되는 인증서를 생성하거나 얻으십시오.

참고 클라이언트에 신뢰할 수 있는 루트 인증서로 자체 서명된 인증서를 설치하면 짧은 기간에 보안 인증서 경고를 피할 수 있습니다. 그러나 사용자가 실수로 Rogue 서버의 인증서를 신뢰하도록 브라우저를 구성하거나 보안 게이트웨이 연결 시 보안 경고에 대해 응답해야 하는 불편함이 있으므로 권장하지 않습니다.

프로시저

단계 **1** Security Alert(보안 경고) 창에서 **View Certificate(**인증서 보기**)** 를 클릭하십시오.

단계 **2** **Install Certificate(**인증서 설치**)**를 클릭합니다.

단계 **3** **Next(**다음**)**를 클릭합니다.

단계 4 **Place all certificates in the following store(**다음 저장소에 모든 인증서 보관**)**를 선택하십시오.

단계 5 **Browse(**찾아보기**)**를 클릭합니다.

단계 6 드롭다운 목록에서 **Trusted Root Certification Authorities(**신뢰할 수 있는 루트 인증 기관**)**를 선택하십시오.

단계 7 계속해서 Certificate Import(인증서 가져오기) 마법사 프롬프트를 따르십시오.

연결 중단

유선 연결 도입 시 무선 연결 중단(Juniper Odyssey Client)

문제점 Odyssey 클라이언트에서 무선 억제를 활성화하는 경우 유선 연결을 설정하면 무선 연결이 중단됩니다. 무선 억제를 비활성화하면 무선 연결이 예상대로 작동합니다.

해결 방법 Odyssey 클라이언트 구성

Odyssey 클라이언트 구성

프로시저

단계 1 네트워크 연결에서 연결 속성에 표시되는 어댑터의 이름을 복사합니다. 레지스트리를 편집하는 경우, 변경하기 전에 백업을 수행하고 잘못 수정할 경우 심각한 문제가 발생할 수 있으므로 주의하십시오.

단계 2 레지스트리를 열고 HKEY_LOCAL_MACHINE\SOFTWARE\Funk Software, Inc.\odyssey\client\configuration\options\adapterType\virtual로 이동합니다.

단계 3 virtual 아래에서 새 문자열 값을 생성합니다. 네트워크 속성의 어댑터 이름을 레지스트리 부분에 복사합니다. 추가 레지스트리 설정은 한 번 저장된 후에 고객 MSI가 생성되어 다른 클라이언트로 푸시 다운될 때 복사됩니다.

ASA에 대한 연결 실패(Kaspersky AV Workstation 6.x)

문제점 Kaspersky 6.0.3이 설치된 경우(비활성화된 경우도 해당), ASA에 대한 AnyConnect 연결이 CSTP 상태 = CONNECTED(연결됨) 이후에 바로 실패합니다. 다음 메시지가 나타납니다.

```
SVC message: t/s=3/16: Failed to fully establish a connection to the secure gateway (proxy
 authentication, handshake, bad cert, etc.).
```

해결 방법 Kaspersky를 제거하고 Kaspersky 포럼에서 추가 업데이트를 확인하십시오.

UDP DTLS 연결 안 됨(McAfee Firewall 5)

문제점 McAfee Firewall 5를 사용 중인 경우, UDP DTLS 연결을 설정할 수 없습니다.

해결 방법 McAfee Firewall 중앙 콘솔에서 **Advanced Tasks(**고급 작업**) > Advanced options and Logging(**고급 옵션 및 로깅**)**을 선택하고 McAfee Firewall에서 **Block incoming fragments automatically(**수신 프래그먼트 자동으로 차단**)** 확인란을 선택 취소합니다.

호스트 디바이스에 대한 연결 실패(Microsoft 라우팅 및 원격 액세스 서버)

문제점 RRAS를 사용 중인 경우, AnyConnect에서 호스트 디바이스에 대한 연결을 설정하려고 시도할 때 다음의 종료 오류가 이벤트 로그에 반환됩니다.

```
Termination reason code 29 [Routing and Remote Access service is running]
The Windows service “Routing and Remote Access” is incompatible with the Cisco AnyConnect
VPN Client.
```

해결 방법 RRAS 서비스를 비활성화합니다.

실패한 연결/자격 증명(로드 밸런서) 없음

문제점 크리덴셜이 없어 연결에 실패합니다.

해결 방법 서드파티 로드 밸런서는 ASA 디바이스의 로드에 대해 파악하지 못합니다. ASA의 로드 밸런서 기능이 디바이스에서 VPN 부하를 균일하게 배포할 수 있으므로 내부 ASA 로드 밸런싱 기능을 사용하는 것이 좋습니다.

설치 실패

AnyConnect가 다운로드에 실패(Wave EMBASSY 신뢰 제품군)

문제점 AnyConnect 클라이언트가 다운로드되지 않고 다음 오류 메시지가 표시됩니다.

“Cisco AnyConnect VPN Client Downloader has encountered a problem and needs to close.”

해결 방법 1.2.1.38 버전에 대한 패치 업데이트를 업로드하여 모든 dll 문제를 해결합니다.

비호환성 문제

라우팅 테이블(Bonjour Printing Service) 업데이트 실패

문제점 Bonjour Printing Service를 사용 중인 경우, AnyConnect 이벤트 로그는 IP 전달 테이블을 식별하지 못했음을 나타냅니다.

해결 방법 명령 프롬프트에서 **net stop** "**bonjour service**"를 입력하여 BonJour Printing Service를 비활성화합니다. mDNSResponder(1.0.5.11)의 최신 버전은 Apple에서 제작했습니다. 이 문제를 해결하기 위해 Bonjour의 새 버전을 iTunes와 함께 제공하고 Apple 웹 사이트에서 별도로 다운로드할 수 있습니다.

TUN 버전 비호환(OpenVPN 클라이언트)

문제점 TUN 버전이 이 시스템에 이미 설치되어 있으며 AnyConnect 클라이언트와 호환되지 않음을 나타내는 오류가 발생합니다.

해결 방법 Viscosity OpenVPN 클라이언트를 제거합니다.

Winsock 카탈로그 충돌(LSP 증상 2 충돌)

문제점 클라이언트에 LSP 모듈이 있으면 Winsock 카탈로그가 충돌할 수 있습니다.

해결 방법 LSP 모듈을 제거합니다.

느린 데이터 처리량(LSP 증상 3 충돌)

문제점 Windows 7 사용 시 NOD32 Antivirus V4.0.468 x64를 사용하는 경우 느린 데이터 처리량 문제가 발생할 수 있습니다.

해결 방법 SSL 프로토콜 스캐닝을 비활성화합니다. SSL 프로토콜 스캐닝 비활성화를 참조하십시오.

SSL 프로토콜 스캐닝 비활성화

프로시저

단계 **1** 고급 설정에서 **Protocol Filtering(**프로토콜 필터링**)** > **SSL** 로 이동하여 SSL 프로토콜 스캐닝을 활성화하십시오.

단계 **2** **Web access protection(**웹 액세스 보호**)** > **HTTP, HTTPS** 로 이동한 다음 **Do not use HTTPS protocol checking(HTTPS** 프로토콜 검사 사용 안 함**)**을 선택하십시오.

단계 **3** **Protocol filtering(**프로토콜 필터링**)** > **SSL** 로 돌아가 **SSL protocol scanning(SSL** 프로토콜 스캐닝**)**을 비활성화하십시오.

DPD 실패(EVDO 무선 카드 및 Venturi 드라이버)

문제점 클라이언트 연결 끊김이 발생한 동안 EVDO 무선 카드 및 Venturi 드라이버를 사용하면 이벤트 로그에서 다음을 보고합니다.

```
%ASA-5-722037: Group <Group-Name> User <User-Name> IP <IP-Address> SVC closing connection:
 DPD failure.
```

해결 방법

- 애플리케이션, 시스템 및 AnyConnect 이벤트 로그에서 관련 연결 끊기 이벤트가 있는지 확인하고 동시에 NIC 카드 재설정이 적용되었는지 확인합니다.
- Venturi 드라이버가 최신 버전인지 확인합니다. AT&T Communications Manager 6.7 버전에서 **Use Rules Engine(**규칙 엔진 사용**)**을 비활성화합니다.

DTLS 트래픽 실패(DSL 라우터)

문제점 DSL 라우터와 연결하는 경우 협상이 정상적으로 진행되어도 DTLS 트래픽에 장애가 발생할 수 있습니다.

해결 방법 초기 설정으로 Linksys 라우터에 연결합니다. 이 설정을 통해 안정적인 DTLS 세션과 중단 없는 ping을 사용할 수 있습니다. DTLS 반환 트래픽을 허용하는 규칙을 추가합니다.

NETINTERFACE_ERROR(CheckPoint 및 Kaspersky와 같은 기타 서드파티 소프트웨어)

문제점 SSL 연결을 수행하기 위해 사용되는 컴퓨터 네트워크에서 운영 체제 정보를 검색하려 할 때 보안 게이트웨이에 대한 연결을 완전하게 설정하는 데 실패했다는 메시지가 AnyConnect 로그에 표시할 수 있습니다.

해결 방법

- 무결성 에이전트를 제거한 다음 AnyConnect를 설치 중인 경우 TCP/IP를 활성화합니다.
- 무결성 에이전트 설치에서 SmartDefense를 비활성화했는지, TCP/IP를 선택했는지 확인합니다.
- 서드파티 소프트웨어가 네트워크 인터페이스 정보를 검색하는 동안 운영 체제 API 호출을 가로채거나 차단하는 경우 의심되는 AV, FW, AS 등이 있는지 확인합니다.
- AnyConnect 어댑터의 인스턴스가 하나만 디바이스 관리자에 나타나는지 확인합니다. 하나의 인스턴스만 있는 경우, AnyConnect를 통해 인증하고 5초 후에 디바이스 관리자의 어댑터를 수동으로 활성화합니다.
- 모든 의심되는 드라이버가 AnyConnect 어댑터 내에 활성화되어 있는 경우, Cisco AnyConnect VPN 클라이언트 연결 창에서 선택을 모두 취소하여 해당 드라이버를 비활성화합니다.

성능 문제(가상 머신 네트워크 서비스 드라이버)

문제점 일부 가상 머신 네트워크 서비스 디바이스에서 AnyConnect를 사용할 때 성능 문제가 발생했습니다.

해결 방법 AnyConnect 가상 어댑터 내의 모든 인스턴스 메시징 디바이스에 대한 바인딩을 선택 취소합니다. 애플리케이션 dsagent.exe는 C:\Windows\System\dgagent 내에 위치합니다. 이 프로세스 목록에는 나타나지 않더라도 TCPview(sysinternals)를 통해 소켓을 열어 이 애플리케이션을 볼 수 있습니다. 이 프로세스를 종료할 경우, AnyConnect의 정상적인 작동으로 돌아갑니다.

알려진 서드파티 애플리케이션 충돌

다음의 서드파티 애플리케이션에는 Cisco AnyConnect Secure Mobility Client와의 알려진 문제가 있습니다.

- Adobe 및 Apple — Bonjour Printing Service
  - Adobe Creative Suite 3
  - Bonjour Printing Service
  - iTunes
- AT&T Communications Manager 6.2 및 6.7 버전
  - AT&T Sierra 무선 875 카드
- AT&T Global Dialer
- Citrix Advanced Gateway Client 2.2.1 버전
- 방화벽 충돌
  - 서드파티 방화벽은 ASA 그룹 정책에 구성된 방화벽 기능을 방해할 수 있습니다.
- Juniper Odyssey Client
- Kaspersky AV Workstation 6.x
- McAfee Firewall 5
- Microsoft Internet Explorer 8
- Microsoft 라우팅 및 원격 액세스 서버
- Microsoft Windows 업데이트
- OpenVPN 클라이언트
- 로드 밸런서
- Wave EMBASSY 신뢰 제품군
- LSP(Layered Service Provider, 계층화된 서비스 공급자) 모듈 및 NOD32 AV
- EVDO 무선 카드 및 Venturi 드라이버
- DSL 라우터
- CheckPoint 및 Kaspersky와 같은 기타 서드파티 소프트웨어
- 가상 머신 네트워크 서비스 드라이버