Remote Access VPN Firepower Threat Defense

Firepower Threat Defense 원격 액세스 VPN 개요

Firepower Threat Defense 는 원격 액세스 SSL 및 IPsec IKEv2 VPN을 지원하는 보안 게이트웨이 기능을 제공합니다. 전체 터널 클라이언트인 AnyConnect Secure Mobility Client는 원격 사용자를 위해 보안 게이트웨이에 보안 SSL 및 IPsec-IKEv2 연결을 제공합니다. AnyConnect는 Firepower Threat Defense 디바이스에 원격 VPN 연결을 제공하는 엔드포인트 디바이스에서만 지원되는 클라이언트입니다. 이 클라이언트는 네트워크 관리자가 원격 컴퓨터에 클라이언트를 설치 및 구성하지 않아도 원격 사용자에게 SSL 또는 IPsec-IKEv2 VPN 클라이언트의 이점을 제공합니다. Windows, Mac, Linux 용 AnyConnect 모바일 클라이언트는 연결할 때 보안 게이트웨이에서 구축됩니다. Apple iOS 및 Android 디바이스용 AnyConnect 앱은 플랫폼 앱 스토어에서 설치됩니다.

Firepower Management Center의 Remote Access VPN 정책 마법사를 사용하여 기본 기능을 갖춘 SSL 및 IPsec-IKEv2 원격 액세스 VPN을 쉽고 빠르게 설정합니다. 그런 다음, 원하는 경우 정책 구성을 개선하고 Firepower Threat Defense 보안 게이트웨이 디바이스에 구축합니다.

원격 액세스 VPN 정책을 사용하여 다음 설정을 구성할 수 있습니다.

- 이중 인증, 45 페이지
- 보조 인증, 49 페이지
- 인증을 위한 LDAP 또는 Active Directory 설정, 58 페이지
- VPN 세션에 대한 암호 변경 관리, 57 페이지
- RADIUS 서버로 계정 기록 전송, 59 페이지
- 그룹 정책 또는 기타 속성 선택을 권한 부여 서버로 재정의 , 61 페이지
  - 사용자 그룹에 대한 VPN 액세스 거부, 62 페이지
  - 사용자 그룹에 대한 연결 프로파일 선택 제한, 63 페이지

다음 예시를 사용하여 제한된 대역폭을 VPN 사용자에게 할당하고, 사용자 ID 기반 액세스 제어 규칙에 VPN 식별을 사용할 수 있습니다.

- 사용자별 AnyConnect 대역폭을 제한하는 방법, 65 페이지
- 사용자 ID 기반 액세스 제어 규칙에 VPN ID를 사용하는 방법, 68 페이지

Remote Access VPN 기능

다음 섹션에서는 Firepower Threat Defense Remote Access VPN의 기능에 대해 설명합니다.

- Cisco AnyConnect Secure Mobility 클라이언트를 사용하는 SSL 및 IPsec-IKEv2 원격 액세스.
- Firepower Management Center IPv4 터널을 통한 IPv6와 같은 모든 조합을 지원합니다.
- FMC 및 FDM 모두에 대한 구성 지원. 디바이스별 재정의.
- Firepower Management Center 및 FTD HA 환경에 대한 지원.
- 여러 인터페이스 및 여러 AAA 서버에 대한 지원.
- RADIUS CoA 또는 RADIUS 동적 인증을 사용하여 Rapid Threat Containment 지원.
- Cisco AnyConnect Secure Mobility Client 버전 4.7 이상에서 DTLS v1.2 프로토콜을 지원합니다.
- AnyConnect 클라이언트 모듈은 RA VPN 연결을 위한 추가 보안 서비스를 지원합니다.

AAA

- 자체 서명 또는 CA 서명 ID 인증서를 사용하는 서버 인증.
- RADIUS 서버 또는 LDAP 또는 AD를 사용하는 AAA 사용자 이름 및 암호 기반 원격 인증.
- RADIUS 그룹 및 사용자 권한 부여 속성 및 RADIUS 계정.
- 2차 인증을 위해 추가 AAA 서버를 사용하는 이중 인증 지원.

- VPN ID를 사용하는NGFW Access Control 통합.
- Firepower Management Center 웹 인터페이스를 사용하는 LDAP 또는 AD 권한 부여 속성
- SAML 2.0을 사용하는 SSO(Single Sign-On) 지원

VPN 터널링

- 주소 할당
- 스플릿 터널링
- 스플릿 DNS
- Client Firewall ACL
- 최대 연결 및 유휴 시간에 대한 세션 시간 초과

모니터링

- 기간 및 클라이언트 애플리케이션 같은 다양한 속성으로 VPN 사용자를 표시하는 새로운 VPN 대시보드 위젯.
- 사용자 이름 및 OS 플랫폼과 같은 인증 정보를 포함하는 원격 액세스 VPN 이벤트.
- FTD Unified CLI를 통해 사용 가능한 터널 통계.

AnyConnect 구성 요소

AnyConnect Secure Mobility Client 구축

원격 액세스 VPN 정책에 AnyConnect 클라이언트 이미지 및 AnyConnect 클라이언트 프로파일을(를) 포함하여 연결 엔드포인트에 배포할 수 있습니다. 또는 다른 방법을 사용하여 클라이언트 소프트웨어를 배포할 수 있습니다. 알맞은 버전의 Cisco AnyConnect Secure Mobility Client 관리자 가이드에서 *AnyConnect* 구축 장을 참조하십시오.

이전에 설치된 클라이언트가 없는 경우 원격 사용자는 SSL 또는 IPsec-IKEv2 VPN 연결을 허용하도록 구성된 인터페이스의 브라우저에 IP 주소를 입력합니다. 보안 어플라이언스가 http:// 요청을 https://로 리디렉션하도록 구성되어 있지 않은 경우, 사용자는 URL을 https://<*address*> 형식으로 입력해야 합니다. 사용자가 URL을 입력하면 브라우저가 해당 인터페이스로 연결되고 로그인 화면이 표시됩니다.

사용자가 로그인하면, 보안 게이트웨이에서 사용자가 VPN 클라이언트를 요청하는 것으로 식별하면 원격 컴퓨터의 운영 체제에 맞는 클라이언트가 다운로드됩니다. 다운로드 후에는 클라이언트가 자동으로 설치 및 구성되어 보안 연결을 설정하며, 연결이 중지되면 보안 어플라이언스 구성에 따라 그대로 유지되거나 자동으로 제거됩니다. 이전에 설치된 클라이언트의 경우, 로그인하면 Firepower Threat Defense 보안 게이트웨이가 클라이언트 버전을 확인하고 필요에 따라 클라이언트를 업그레이드합니다.

AnyConnect Secure Mobility Client 작업

클라이언트가 보안 어플라이언스와 연결을 협상한다면, 클라이언트는 TLS(Transport Layer Security)를 사용하여 연결하고 선택에 따라 DTLS(Datagram Transport Layer Security)를 사용하여 연결합니다. DTLS는 일부 SSL 연결에서 발생하는 레이턴시 및 대역폭 문제를 방지하고 패킷 지연에 민감한 실시간 애플리케이션의 성능을 높입니다.

IPsec-IKEv2 VPN 클라이언트가 보안 게이트웨이에 연결을 시작할 경우, 협상은 IKE(Internet Key Exchange)를 통한 디바이스 인증과 그다음에 수행되는 IKE Xauth(Extended Authentication)를 사용한 사용자 인증으로 구성됩니다. 그룹 프로파일이 VPN 클라이언트에 푸시되고 IPsec SA(security association)를 생성하여 VPN을 완료합니다.

AnyConnect 클라이언트 프로파일 및 편집기

AnyConnect 클라이언트 프로파일은 XML 파일에 저장된 구성 파라미터 그룹으로, VPN 클라이언트는 이를 사용하여 운영 및 모양을 구성합니다. 이러한 매개변수(XML 태그)에는 추가적인 클라이언트 기능을 활성화할 수 있는 호스트 컴퓨터 및 설정의 이름과 주소가 포함되어 있습니다.

AnyConnect 프로파일 편집기를 사용하여 프로파일을 구성할 수 있습니다. 이 편집기는 AnyConnect 소프트웨어 패키지의 일부로 제공되는 편리한 GUI 기반 구성 툴입니다. 이 툴은 Firepower Management Center외부에서 실행되는 독립 프로그램입니다.

Remote Access VPN 인증

Remote Access VPN 서버 인증

Firepower Threat Defense 보안 게이트웨이는 항상 인증서를 사용하여 VPN 클라이언트 엔드포인트에 대한 식별 및 인증을 수행합니다.

보안 게이트웨이의 인증서를 가져오는 것은 PKI 등록이라고도 하며, Firepower Threat Defense 인증서 기반 인증에 설명되어 있습니다. 이 장에는 게이트웨이 인증서 구성, 등록 및 유지 관리에 대한 전체적인 설명이 포함되어 있습니다.

Remote Access VPN 클라이언트 AAA

SSL 및 IPsec-IKEv2 둘 다의 경우 원격 사용자 인증은 사용자 이름과 비밀번호만, 인증서만 또는 두 가지를 모두 사용하여 수행됩니다.

참고 구축에서 클라이언트 인증서를 사용하고 있는 경우, Firepower Threat Defense 또는 Firepower Management Center와 무관한 클라이언트 플랫폼에 해당 인증서를 추가해야 합니다. 클라이언트에 인증서를 입력할 수 있는 기능인 SCEP 또는 CA 서비스 등은 제공되지 않습니다.

AAA 서버는 보안 게이트웨이 역할의 매니지드 디바이스가 사용자(인증), 사용자가 수행하도록 허용된 작업(권한 부여) 및 사용자가 수행한 작업(계정)을 결정하도록 활성화합니다. AAA 서버의 몇 가지 예는 RADIUS, LDAP/AD, TACACS+ 및 Kerberos입니다. Firepower Threat Defense 디바이스에서 Remote Access VPN의 경우 인증에 대해 AD, LDAP 및 RADIUS AAA 서버가 지원됩니다.

Remote Access VPN 권한 부여에 대한 자세한 내용은 권한 및 속성 정책 시행 이해을 참조하십시오.

Remote Access VPN 정책을 추가하거나 편집하기 전에 지정하려는 영역 및 RADIUS 서버 그룹을 구성해야 합니다. 자세한 내용은 영역 생성 및 RADIUS 서버 그룹를 참조하십시오.

구성된 DNS가 없으면 디바이스는 AAA 서버 이름, 이름이 지정된 URL 및 FQDN 또는 호스트 이름이 있는 CA 서버를 확인할 수 없으며 IP 주소만 확인할 수 있습니다.

플랫폼 설정을 사용하여 DNS를 구성할 수 있습니다. 자세한 내용은 DNS 구성 및 DNS 서버 그룹 개체를 참조하십시오.

원격 사용자가 제공한 로그인 정보는 LDAP 또는 AD 영역 또는 RADIUS 서버 그룹에서 검증합니다. 이러한 엔터티는 Firepower Threat Defense 보안 게이트웨이와 통합됩니다.

참고 사용자가 Active Directory를 인증 소스로 사용하여 RA VPN으로 인증하는 경우 사용자 이름을 사용하여 로그인해야 합니다. `domain\username` 또는 `username@domain` 형식은 실패하게 됩니다. (Active Directory는 이 사용자 이름을 로그온 이름 또는 경우에 따라 `sAMAccountName`으로 참조합니다.) 자세한 내용은 MSDN의 User Naming Attributes를 참조하십시오.

RADIUS를 사용하여 인증하는 경우 사용자는 위의 형식 중 하나로 로그인할 수 있습니다.

VPN 연결을 통해 인증되면 원격 사용자는 *VPN ID*를 사용합니다. Firepower Threat Defense 보안 게이트웨이의 *ID* 정책에서 이 VPN ID를 사용하여 해당 원격 사용자에게 속하는 네트워크 트래픽을 인식하고 필터링합니다.

ID 정책은 네트워크 리소스에 대한 액세스 권한을 가진 사용자를 확인하는 액세스 제어 정책과 연결됩니다. 이러한 방식으로 원격 사용자는 네트워크 리소스에 대한 액세스가 차단되거나 허용됩니다.

자세한 내용은 영역 및 ID 정책 및 액세스 제어 정책 섹션을 참조하십시오.

관련 항목

Remote Access VPN에 대한 AAA 설정, 23 페이지

권한 및 속성 정책 시행 이해

Firepower Threat Defense 디바이스는 AAA 서버(RADIUS) 또는 Firepower Threat Defense 디바이스에 정의된 그룹 정책에서 VPN 연결에 사용자 인증 속성(사용자 자격 또는 권한이라고도 함)을 적용하도록 지원합니다. Firepower Threat Defense 디바이스에서 그룹 정책에 구성된 속성과 충돌하는 속성을 AAA 서버로부터 수신하는 경우, AAA 서버에서 오는 속성이 항상 우선 적용됩니다.

Firepower Threat Defense 디바이스에서는 다음 순서로 속성을 적용합니다.

1. **AAA** 서버의 사용자 속성 - 사용자 인증 및/또는 권한 부여가 성공적으로 수행되면 서버에서 이러한 특성을 반환합니다.
2. **Firepower Threat Defense** 디바이스에 구성된 그룹 정책 - RADIUS 서버에서 사용자에 대해 RADIUS CLASS 속성 IETF-Class-25(OU=group-policy) 값을 반환하면 Firepower Threat Defense 디바이스에서는 해당 사용자를 이름이 같은 그룹 정책에 배치하고 서버에서 반환하지 않은 그룹 정책의 모든 속성을 적용합니다.

3. 연결 프로파일에서 할당한 그룹 정책(터널 그룹으로 알려짐) - 연결 프로파일에는 연결을 위한 예비 설정이 있으며 인증 전에 사용자에게 적용되는 기본 그룹 정책을 포함합니다.

참고 Firepower Threat Defense 디바이스는 기본 그룹 정책인 *DfltGrpPolicy*에서 시스템 기본 속성 상속을 지원하지 않습니다. 연결 프로파일에 할당된 그룹 정책의 속성은 사용자 속성이나 AAA 서버의 그룹 정책에 의해 재정의되지 않는 경우 위에서 설명한 대로 사용자 세션에 사용됩니다.

관련 항목

Remote Access VPN에 대한 AAA 설정, 23 페이지

AAA 서버 연결 이해

LDAP, AD 및 RADIUS AAA 서버는 사용자 ID 처리, VPN 인증 또는 두 가지 활동 모두와 같은 용도에 따라 Firepower Threat Defense 디바이스에서 연결할 수 있어야 합니다. AAA 서버는 Remote Access VPN에서 다음 활동을 위해 사용됩니다.

- 사용자 **ID** 처리 - 관리 인터페이스를 통해 서버에 연결할 수 있어야 합니다.

  Firepower Threat Defense 디바이스에서 관리 인터페이스는 VPN에서 사용하는 일반 인터페이스와는 다른별도의 라우팅 프로세스 및 구성을 갖습니다.

- **VPN** 인증 - 서버는 , 즉 진단 인터페이스 또는 데이터 인터페이스와 같은 일반 인터페이스 중 하나를 통해 연결할 수 있어야 합니다.

  일반 인터페이스에 대해 2개의 라우팅 테이블이 사용됩니다. 진단 인터페이스 및 관리 전용으로 구성된 기타 모든 인터페이스에 대한 관리 전용 라우팅 테이블 및 데이터 인터페이스에 사용되는 데이터 라우팅 테이블입니다. 경로 조회가 완료되면 먼저 관리 전용 라우팅 테이블을 확인한 다음 데이터 라우팅 테이블을 확인합니다. 첫 번째 일치 조건은 AAA 서버에 도달하기 위해 선택됩니다.

  참고 데이터 인터페이스에 AAA 서버를 배치하는 경우 관리 전용 라우팅 정책이 데이터 인터페이스로 향하는 트래픽과 일치하지 않아야 합니다. 예를 들어 진단 인터페이스를 통한 기본 경로가 있는 경우 트래픽이 데이터 라우팅 테이블로 폴백하지 않습니다. **show route management-only** 및 **show route** 명령을 사용하여 라우팅 결정을 확인합니다.

동일한 AAA 서버에 있는 두 가지 활동의 경우 사용자 ID 처리를 위해 관리 인터페이스를 통해 서버에 연결하는 것 외에도 다음 중 하나를 수행하여 동일한 AAA 서버에 대한 VPN 인증 액세스를 제공합니다.

- 관리 인터페이스와 동일한 서브넷의 IP 주소로 진단 인터페이스를 활성화하고 구성한 다음 이 인터페이스를 통해 AAA 서버에 대한 경로를 구성합니다. 진단 인터페이스 액세스는 VPN 활동, ID 처리를 위한 관리 인터페이스 액세스에 사용됩니다.

참고 이러한 방식으로 구성하면 진단 및 관리 인터페이스와 동일한 서브넷에 데이터 인터페이스를 가질 수도 없습니다. 예를 들어 디바이스 자체를 게이트웨이로 사용할 때와 같이 관리 인터페이스와 데이터 인터페이스가 동일한 네트워크에 있으면 진단 인터페이스를 비활성화 상태로 유지해야 하기 때문에 이 솔루션을 사용할 수 없습니다.

- 데이터 인터페이스를 통해 AAA 서버에 대한 경로를 구성합니다. 데이터 인터페이스 액세스는 VPN 활동, 사용자 ID 처리를 위한 관리 인터페이스 액세스에 사용됩니다.

참고 FQDN 또는 호스트 이름을 사용하여 AAA 서버 이름, 이름이 지정된 URL 및 CA 서버를 사용하려면 각 디바이스에 DNS를 구성해야 합니다. DNS가 없으면 시스템은 IP 주소만 구성하고 사용할 수 있습니다. 플랫폼 설정을 사용하여 DNS를 구성할 수 있습니다. 자세한 내용은 DNS 구성 및 DNS 서버 그룹 개체를 참조하십시오.

여러 인터페이스에 대한 자세한 내용은 Firepower Threat Defense 일반 방화벽 인터페이스 섹션을 참조하십시오.

구축 후 다음 CLI 명령을 사용하여 Firepower Threat Defense 디바이스에서 AAA 서버 연결을 모니터링하고 문제를 해결합니다.

- **show aaa-server** - AAA 서버 통계를 표시합니다.
- **show route management-only** - 관리 전용 라우팅 테이블 항목을 봅니다.
- **show network**과 **show network-static-routes**가 관리 인터페이스 기본 경로 및 고정 경로를 확인합니다.
- **show route** - 데이터 트래픽 라우팅 테이블 항목을 봅니다.
- **ping system**과 **traceroute system**가 관리 인터페이스를 통해 AAA 서버에 대한 경로를 확인합니다.
- **ping interface** *ifname* 및 **traceroute** *destination* - 진단 및 데이터 인터페이스를 통해 AAA 서버에 대한 경로를 확인합니다.
- **test aaa-server authentication** 및 **test aaa-server authorization** - AAA 서버에서 인증 및 권한 부여를 테스트합니다.
- **clear aaa-server statistics** *groupname* 또는 **clear aaa-server statistics protocol** *protocol* - 그룹 또는 프로토콜별로 AAA 서버 통계를 지웁니다.
- **aaa-server** *groupname* **active host** *hostname* - 실패한 AAA 서버를 활성화합니다. **aaa-server** *groupname* **fail host** *hostname* - AAA 서버에 실패합니다.
- **debug ldap leveldebug aaa authentication**, **debug aaa authorization** 및 **debug aaa accounting**.

원격 액세스 VPN 라이선스 요구 사항

FTD 라이센스

FTD 원격 액세스 VPN에는 AnyConnect에 대한 강력한 암호화 및 다음 라이선스 중 하나가 필요합니다.

- AnyConnect Plus
- AnyConnect Apex
- AnyConnect VPN만

원격 액세스 VPN 요구 사항 및 사전 요건

모델 지원

FTD

지원되는 도메인

모든

사용자 역할

관리자

Remote Access VPN에 대한 지침 및 제한 사항

원격 액세스 **VPN** 정책 구성

- 신규 원격 접속 VPN 정책을 추가하려면 마법사를 사용해야만 합니다. 새 정책을 생성하려면 마법사 전체를 진행해야 합니다. 마법사를 완료하기 전에 취소할 경우 정책이 저장되지 않습니다.
- 사용자 두 명이 원격 접속 VPN 정책을 동시에 편집해서는 안 됩니다. 그러나 웹 인터페이스는 동시 편집을 차단하지 않습니다. 동시 수정이 일어날 경우, 마지막으로 저장된 컨피그레이션이 유지됩니다.
- 원격 액세스 VPN 정책이 해당 디바이스에 할당되어 있다면 한 도메인에서 다른 도메인으로 Firepower Threat Defense 디바이스를 이동할 수 없습니다.
- 클러스터 모드의 Firepower 9300 및 4100 시리즈는 원격 액세스 VPN 구성을 지원하지 않습니다.
- 잘못 구성된 FTD NAT 규칙이 있다면 원격 액세스 VPN 연결이 실패할 수 있습니다.

- 마법사를 사용하여 원격 액세스 VPN을 구성하는 동안 인라인 인증서 등록 개체를 만들 수 있지만 이를 사용하여 ID 인증서를 설치할 수는 없습니다. 인증서 등록 개체는 원격 액세스 VPN 게이트웨이로 구성되는 Firepower Threat Defense 디바이스에서 ID 인증서를 생성하는 데 사용됩니다. 디바이스에 원격 액세스 VPN 정책을 배포하기 전에 ID 인증서를 설치하십시오. 인증서 등록 개체를 기반으로 ID 인증서를 설치하는 방법에 대한 자세한 내용은 개체 관리자 섹션을 참조하십시오.
- 원격 액세스 VPN 정책 구성을 변경한 후에는 변경 내용을 Firepower Threat Defense 디바이스에 다시 구축합니다. 구성 변경을 구축하는 데 걸리는 시간은 정책 및 규칙의 복잡성, 디바이스에 전송하는 구성 유형 및 볼륨, 메모리 및 디바이스 모델과 같은 여러 요소에 따라 다릅니다. 원격 액세스 VPN 정책 변경 사항을 구축하기 전에 구성 변경 사항 구축을 위한 모범 사례 섹션을 검토하십시오.

동시 **VPN** 세션 용량 계획

최대 동시 VPN 세션은 플랫폼별 한도에 의해 관리되며 라이선스에 의존하지 않습니다. 디바이스 모델에 따라 디바이스에서 허용되는 동시 원격 액세스 VPN 세션 수에는 최대 제한이 적용됩니다. 이러한 제한은 시스템 성능이 부적절한 레벨로 저하되지 않도록 설계된 것입니다. 용량 계획 시에 이러한 제한을 사용하십시오.

디바이스 모델	최대 동시 원격 액세스 **VPN** 세션
Firepower 2110	1500
Firepower 2120	3500
Firepower 2130	7500
Firepower 2140	10000

다른 하드웨어 모델의 용량을 알고 싶다면 영업 담당자에게 문의하십시오.

참고 FTD 디바이스는 플랫폼 당 최대 세션 한도에 도달하면 VPN 연결을 거부합니다. 이 연결은 시스템 로그 메시지와 함께 거부됩니다. 시스템 로그 메시지 %ASA-4-113029 및 %ASA-4-113038는 시스템 로그 메시징 가이드를 참조하십시오. 자세한 내용은 http://www.cisco.com/c/en/us/td/docs/security/asa/syslog-guide/syslogs.html을 참조해 주십시오.

VPN에 대한 암호 사용 제어

DES 보다 큰 암호 사용을 방지하기 위해 Firepower Management Center의 다음 위치에서 사전 구축 확인을 할 수 있습니다.

Devices(디바이스**)** > **Platform Settings(**플랫폼 설정**)** > **SSL Settings(SSL** 설정**)**

Devices(디바이스**)** > **VPN** > **Remote Access(**원격 액세스**)** > **Advanced(**고급**)** > **IPsec**

SSL 설정 및 IPsec에 대한 자세한 내용은 SSL 설정 및 Remote Access VPN IPsec/IKEv2 파라미터 구성, 42 페이지을 참조하십시오.

인증, 권한 부여 및 계정 관리(AAA)

- Firepower Threat Defense 디바이스는 시스템 통합 인증 서버만 사용하는 원격 액세스 VPN 사용자의 인증을 지원하므로 로컬 사용자 데이터베이스는 지원되지 않습니다.
- 원격 액세스 VPN을 사용하려면 토폴로지의 각 디바이스에 DNS를 구성합니다. DNS가 없으면 디바이스는 AAA 서버 이름, 이름이 지정된 URL 및 FQDN 또는 호스트 이름이 있는 CA 서버를 확인할 수 없으며 IP 주소만 확인할 수 있습니다.

  플랫폼 설정을 사용하여 DNS를 구성할 수 있습니다. 자세한 내용은 DNS 구성 및 DNS 서버 그룹 개체를 참조하십시오.

클라이언트 인증서

- 구축에서 클라이언트 인증서를 사용하고 있는 경우, Firepower Threat Defense 또는 Firepower Management Center와 무관한 클라이언트 플랫폼에 해당 인증서를 추가해야 합니다. 클라이언트에 인증서를 입력할 수 있는 기능인 SCEP 또는 CA 서비스 등은 제공되지 않습니다.

AnyConnect의 지원되지 않는 기능

지원되는 VPN 클라이언트는 Cisco AnyConnect Secure Mobility Client뿐입니다. 그 외의 클라이언트 또는 네이티브 VPN은 지원되지 않습니다. 클라이언트리스 VPN은 VPN 연결에는 지원되지 않으며, 웹 브라우저를 이용해 AnyConnect 클라이언트를 구축하는 용도로만 사용됩니다.

다음 AnyConnect 기능은 FTD 보안 게이트웨이에 연결할 때는 지원되지 않습니다.

- Hostscan, Endpoint Posture Assessment 및 클라이언트 포스처 기반의 동적 액세스 정책 등의 포스처 변수.
- AnyConnect 사용자 지정 및 현지화 지원. FTD 디바이스는 이러한 기능을 위해 AnyConnect를 구성하는 데 필요한 파일을 구성하거나 구축하지 않습니다.
- FTD에서는 AnyConnect 클라이언트에 대한 맞춤 설정 속성이 지원되지 않습니다. 따라서 맞춤 설정 속성을 사용하는 모든 기능이 지원되지 않습니다. 여기에는 데스크톱 클라이언트의 Deferred Upgrade(지연된 업그레이드) 및 모바일 클라이언트의 Per-App VPN(애플리케이션별 VPN)이 포함됩니다.
- 로컬 인증입니다. VPN 사용자는 FTD 보안 게이트웨이에 구성할 수 없습니다.

  로컬 CA의 경우 보안 게이트웨이는 Certificate Authority의 역할을 할 수 없습니다.
- TACACS, Kerberos(KCD 인증) 및 RSA SDI
- 브라우저 프록시
- VPN 로드 밸런싱

새 Remote Access VPN 연결 구성

이 섹션에서는 Firepower Threat Defense 디바이스를 VPN 게이트웨이로 사용하고 Cisco AnyConnect를 VPN 클라이언트로 이용해 새로운 원격 액세스 VPN 정책을 구성하는 방법을 설명합니다.

	수행해야 할 작업	추가 정보
1단계	지침 및 사전 요구 사항을 검토합니다.	Remote Access VPN에 대한 지침 및 제한 사항, 8 페이지 Remote Access VPN 구성 사전 요구 사항, 11 페이지
2단계	마법사를 사용하여 원격 액세스 VPN 정책을 생성합니다.	새 Remote Access VPN 정책 생성, 12 페이지
3단계	디바이스에 구축한 액세스 제어 정책을 업데이트합니다.	Firepower Threat Defense 디바이스의 액세스 제어 정책 업데이트, 14 페이지
4단계	(선택 사항) NAT가 디바이스에 구성된 경우 NAT 면제 규칙을 구성합니다.	(선택 사항) NAT 제외 설정, 15 페이지
5단계	DNS를 구성합니다.	DNS 구성, 16 페이지
6단계	AnyConnect 클라이언트 프로파일을 추가합니다.	AnyConnect 클라이언트 프로파일 XML 파일 추가, 17 페이지
7단계	원격 액세스 VPN 정책을 구축합니다.	컨피그레이션 변경 사항 구축
8단계	(선택 사항) 원격 액세스 VPN 정책 구성을 확인합니다.	구성 확인, 18 페이지

Remote Access VPN 구성 사전 요구 사항

- Firepower Threat Defense 디바이스를 구축하고 내보내기 제어 기능이 활성화된 상태에서 필요한 라이선스로 디바이스를 관리하도록 Firepower Management Center을(를) 구성합니다. 자세한 내용은 VPN 라이선싱의 내용을 참고하십시오.
- 원격 액세스 VPN 게이트웨이 역할을 하는 각 Firepower Threat Defense 디바이스에 대한 ID 인증서를 얻는 데 사용되는 인증서 등록 개체를 구성합니다.
- Remote Access VPN 정책에서 사용 중인 RADIUS 서버 그룹 개체와 AD 또는 LDAP 영역을 구성합니다.
- Remote Access VPN 구성이 작동하려면 Firepower Threat Defense 디바이스에서 AAA 서버에 연결할 수 있는지 확인합니다. 라우팅을 구성(**Devices(**디바이스**)** > **Device Management(**디바이스

관리) > **Edit Device**(디바이스 편집) > **Routing**(라우팅))하여 AAA 서버에 대한 연결성을 보장합니다.

Remote Access VPN 이중 인증의 경우 해당 이중 인증 구성이 작동하려면 Firepower Threat Defense 디바이스에서 기본 및 보조 인증 서버에 모두 연결할 수 있는지 확인합니다.

- AnyConnect Plus, AnyConnect Apex 또는 AnyConnect VPN Only와 같은 Cisco AnyConnect 라이선스 중 하나를 구입하여 활성화하면 Firepower Threat Defense Remote Access VPN을 활성화할 수 있습니다.
- AnyConnect 이미지 파일을 Cisco 소프트웨어 다운로드 센터에서 다운로드하십시오.

  Firepower Management Center 웹 인터페이스에서 **Objects**(개체) > **Object Management**(개체 관리) > **VPN** > **AnyConnect File**(**AnyConnect** 파일)로 이동하고 새 AnyConnect 클라이언트 이미지 파일을 추가합니다.
- 사용자가 VPN 연결 시 액세스할 네트워크 인터페이스가 포함된 보안 영역 또는 인터페이스 그룹을 생성합니다. 보안 영역의 내용을 참조하십시오.
- AnyConnect 클라이언트 프로파일을 생성하려면 Cisco 소프트웨어 다운로드 센터에서 AnyConnect Profile Editor를 다운로드합니다. 독립형 프로파일 편집기를 사용하여 새로운 AnyConnect 프로파일을 만들거나 기존 프로파일을 수정할 수 있습니다.

새 Remote Access VPN 정책 생성

Remote Access VPN Policy 마법사를 통해서만 새 원격 액세스 VPN 정책을 추가할 수 있습니다. 이 마법사는 기본 기능을 사용하여 Remote Access VPN을 쉽고 빠르게 설정할 수 있도록 안내합니다. 또한 원하는 대로 추가 속성을 지정하여 정책 구성을 개선하고 Firepower Threat Defense 보안 게이트웨이 디바이스에 구축할 수 있습니다.

시작하기 전에

- Remote Access VPN 구성 사전 요구 사항, 11 페이지에 나열된 모든 전제 조건을 완료합니다.

프로시저

단계 **1** **Devices**(디바이스) > **VPN** > **Remote Access**(원격 액세스)을 선택합니다.

단계 **2** **(**추가(+)**)** 추가를 클릭하여 기본 정책 설정을 안내하는 마법사를 통해 새 Remote Access VPN 정책을 생성합니다.

마법사 전체를 진행하면서 새 정책을 생성해야 합니다. 마법사를 완료하기 전에 취소할 경우 어떤 정책도 저장되지 않습니다.

단계 **3** **Target Devices**(대상 디바이스) 및 **Protocols**(프로토콜)를 선택합니다.

여기에서 선택한 Firepower Threat Defense 디바이스는 VPN 클라이언트 사용자를 위한 Remote Access VPN 게이트웨이로 작동합니다. 목록에서 디바이스를 선택하거나 새 디바이스를 추가할 수 있습니다.

원격 액세스 VPN 정책을 생성하거나 나중에 변경할 때 Firepower Threat Defense 디바이스를 선택할 수 있습니다. 원격 액세스 VPN 정책 대상 디바이스 설정, 19 페이지의 내용을 참조하십시오.

SSL 또는 **IPSec-IKEv2** 또는 두 VPN 프로토콜을 모두 선택할 수 있습니다. Firepower Threat Defense에서는 두 프로토콜을 모두 지원하여 VPN 터널을 통해 공용 네트워크에 대한 보안 연결을 설정합니다.

참고 Firepower Threat Defense NULL 암호화를 사용하는 IPSec 터널을 지원하지 않습니다. IPSec-IKEv2를 선택한 경우 IPSec IKEv2 제안에 대해 NULL 암호화를 선택하지 않아야 합니다. IKEv2 IPsec 제안 개체 설정의 내용을 참조하십시오.

SSL 설정에 대해서는 SSL 설정의 내용을 참조하십시오.

단계 **4** **Connection Profile(**연결 프로파일**)**과 **Group Policy(**그룹 프로파일**)** 설정을 구성합니다.

연결 프로파일은 원격 사용자가 VPN 디바이스에 연결하는 방법을 정의하는 파라미터 집합을 지정합니다. 이 파라미터에는 인증을 위한 설정 및 속성, VPN 클라이언트에 대한 주소 할당 및 그룹 정책이 포함됩니다. Firepower Threat Defense 디바이스는 Remote Access VPN 정책을 구성할 때 *DefaultWEBVPNGroup*이라는 기본 연결 프로파일을 제공합니다.

자세한 내용은 연결 프로파일 설정, 19 페이지를 참고하십시오.

설정에 대한 자세한 내용은

- AAA 설정, 참조 Remote Access VPN에 대한 AAA 설정, 23 페이지
- LDAP 특성 맵, 참조 LDAP 특성 매핑 구성, 36 페이지
- SAML 2.0 SSO(Single Sign-On, 단일 인증) 인증, 참조 SAML SSO(Single Sign-On) 인증 구성, 53 페이지

그룹 정책은 VPN 사용자의 원격 액세스 VPN 경험을 정의하는 그룹 정책 개체가 저장된 속성 및 값 쌍의 집합입니다. 그룹 정책을 이용해 사용자 인증 프로파일, IP 주소, AnyConnect 설정, VLAN 매핑, 사용자 세션 설정 등의 속성을 구성합니다. RADIUS 권한 서버는 그룹 정책을 할당하거나 현재 연결 프로파일에서 그룹 정책을 가져옵니다.

자세한 내용은 그룹 정책 구성, 35 페이지를 참고하십시오.

단계 **5** VPN 사용자가 Remote Access VPN에 연결하는 데 사용할 **AnyConnect** 클라이언트 이미지를 선택합니다.

Cisco AnyConnect Secure Mobility Client는 기업 리소스에 대한 전체 VPN 프로파일링을 통해 원격 사용자에게 Firepower Threat Defense 디바이스에 대한 SSL 또는 IPSec(IKEv2) 연결을 제공합니다. Remote Access VPN 정책이 Firepower Threat Defense 디바이스에 구축된 후 VPN 사용자는 브라우저에 구성된 디바이스 인터페이스의 IP 주소를 입력하여 AnyConnect 클라이언트를 다운로드하고 설치할 수 있습니다.

AnyConnect 클라이언트 프로파일 및 클라이언트 모듈 구성에 대한 자세한 내용은 그룹 정책 AnyConnect 옵션의 내용을 참고하십시오.

단계 **6** **Network Interface and Identity Certificate(**네트워크 인터페이스 및 **ID** 인증서**)**를 선택합니다.

인터페이스 개체는 네트워크를 세그먼트로 나눠 트래픽 흐름을 관리하고 분류할 수 있도록 지원합니다. 보안 영역은 인터페이스를 그룹화합니다. 이러한 그룹의 범위는 여러 디바이스를 포괄할 수 있으며, 단일 디바이스에서 여러 영역 인터페이스 개체를 구성할 수도 있습니다. 인터페이스 개체의 유형은 두 가지입니다.

- 보안 영역 — 하나의 인터페이스가 하나의 보안 영역에만 속할 수 있습니다.
- 인터페이스 그룹 — 하나의 인터페이스가 여러 인터페이스 그룹(및 하나의 보안 영역)에 속할 수 있습니다.

단계 **7** Remote Access VPN 정책 구성의 **Summary(**요약**)**를 봅니다.

Summary(요약) 페이지에는 지금까지 구성한 모든 Remote Access VPN 설정이 표시되고 선택한 디바이스에 Remote Access VPN 정책을 구축하기 전에 수행해야 하는 추가 구성에 대한 링크가 제공됩니다.

필요한 경우 **Back(**뒤로**)**을 클릭하여 구성을 변경합니다.

단계 **8** **Finish(**마침**)**를 클릭하여 Remote Access VPN 정책의 기본 구성을 완료합니다.

마법사를 사용하여 Remote Access VPN 정책을 완료하면 정책 목록 페이지로 돌아갑니다. 기본 RA VPN 정책 구성을 완료하려면 DNS 구성을 설정하고 VPN 사용자에 대한 액세스 제어를 구성하고 NAT 제외(필요한 경우)를 활성화합니다. 그런 다음 구성을 구축하고 VPN 연결을 설정합니다.

Firepower Threat Defense 디바이스의 액세스 제어 정책 업데이트

Remote Access VPN 정책을 구축하기 전에 대상 Firepower Threat Defense 디바이스의 액세스 제어 정책을 VPN 트래픽을 허용하는 규칙으로 업데이트해야 합니다. 이 규칙은 소스를 정의된 VPN 풀 네트워크로 지정하고 대상을 회사 네트워크로 지정하여 외부 인터페이스에서 들어오는 모든 트래픽을 허용해야 합니다.

참고 Access Interface(액세스 인터페이스) 탭에서 **Bypass Access Control policy for decrypted traffic(**암호해독된 트래픽에 대해 액세스 제어 정책 우회**)(sysopt permit-vpn)**을 선택한 경우 Remote Access VPN에 대한 액세스 제어 정책을 업데이트할 필요가 없습니다.

모든 VPN 연결에 대한 옵션을 활성화하거나 비활성화합니다. 이 옵션을 비활성화하는 경우, 액세스 제어 정책 또는 사전 필터 정책에서 트래픽을 허용해야 합니다.

자세한 내용은 Remote Access VPN을 위한 액세스 인터페이스 구성, 30 페이지를 참고하십시오.

시작하기 전에

Remote Access VPN 정책 마법사를 사용하여 Remote Access VPN 정책 구성을 완료합니다.

프로시저

단계 **1** Firepower Management Center 웹 인터페이스에서 **Policies(**정책**)** > **Access Control(**액세스 제어**)**을 선택합니다.

단계 **2** Remote Access VPN 정책을 구축할 대상 디바이스에 할당된 액세스 제어 정책을 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 **3** **Add(**추가**)**를 클릭하여 새로운 규칙을 추가합니다.

단계 **4** 규칙에 대한 **Name(**이름**)**을 지정하고 **Enabled(**활성화됨**)**를 선택합니다.

단계 **5** **Action(**작업**)**, **Allow(**허용**)** 또는 **Trust(**신뢰**)**를 선택합니다.

단계 **6** **Zones(**영역**)** 탭에서 다음을 선택합니다.

a) Available Zones(사용 가능한 영역) 목록에서 외부 영역을 선택하고 **Add to Source(**소스에 추가**)**를 클릭합니다.

b) Available Zones(사용 가능한 영역) 목록에서 내부 영역을 선택하고 **Add to Destination(**대상에 추가**)**를 클릭합니다.

단계 **7** **Networks(**네트워크**)** 탭에서 다음을 선택합니다.

a) Available networks(사용 가능한 네트워크)에서 내부 네트워크(내부 인터페이스 및/또는 기업 네트워크)를 선택하고 **Add to Destination(**대상에 추가**)**을 클릭합니다.

b) **Available Networks(**사용 가능한 네트워크**)**에서 VPN address pool network(VPN 주소 풀 네트워크)를 선택하고 **Add to Source Networks(**소스 네트워크에 추가**)**를 클릭합니다.

단계 **8** 기타 필수 액세스 제어 규칙 설정을 구성하고 **Add(**추가**)**를 클릭합니다.

단계 **9** 규칙 및 액세스 제어 정책을 저장합니다.

(선택 사항) NAT 제외 설정

NAT 제외는 주소 변환을 제외하고 변환된 호스트와 원격 호스트가 모두 보호되는 호스트와의 연결을 시작할 수 있도록 허용합니다. ID NAT와 마찬가지로 특정 인터페이스의 호스트에 대한 변환은 제한하지 않습니다. 모든 인터페이스를 통한 연결에는 NAT 제외를 사용해야 합니다. 하지만 (정책 NAT처럼) NAT 제외는 변환할 실제 주소를 결정할 때 실제 주소와 대상 주소를 지정할 수 있게 활성화합니다. 고정 ID NAT를 사용하여 액세스 목록의 포트를 고려합니다.

시작하기 전에

Remote Access VPN 정책이 구축된 대상 디바이스에 NAT가 구성되어 있는지 확인합니다. NAT가 대상 디바이스에서 활성화된 경우, NAT VPN 트래픽을 제외하도록 NAT 정책을 정의해야 합니다.

프로시저

단계 **1** Firepower Management Center 웹 인터페이스에서 **Devices(**디바이스**)** > **NAT**를 클릭합니다.

단계 **2** 업데이트할 NAT 정책을 선택하거나 **New Policy(**새 정책**)** > **Threat Defense NAT**를 클릭하여 모든 인터페이스를 통한 연결을 허용하는 NAT 규칙이 있는 NAT 정책을 생성합니다.

단계 **3** **Add Rule(**규칙 추가**)**을 클릭하여 NAT 규칙을 추가합니다.

단계 **4** Add NAT Rule(NAT 규칙 추가) 창에서 다음을 선택합니다.

a) NAT Rule(NAT 규칙)을 **Manual NAT Rule(**수동 **NAT** 규칙**)**으로 선택합니다.

b) Type(유형)을 **Static(**고정**)**으로 선택합니다.

c) **Interface Objects(**인터페이스 개체**)**를 클릭하고 소스 및 대상 인터페이스 개체를 선택합니다.

참고 이 인터페이스 개체는 Remote Access VPN 정책에서 선택한 인터페이스와 동일해야 합니다.

자세한 내용은 Remote Access VPN을 위한 액세스 인터페이스 구성, 30 페이지의 내용을 참고하십시오.

a) **Translation(**변환**)**을 클릭하고 소스 및 대상 네트워크를 선택합니다.

- **Original Source(**원래 소스**)** 및 **Translated Source(**변환된 소스**)**
- **Original Destination(**원래 대상**)** 및 **Translated Destination(**변환된 대상**)**

단계 **5** Advanced(고급) 탭에서 **Do not proxy ARP on Destination Interface(**대상 인터페이스에서 **ARP** 프록시 설정 안 함**)**를 선택합니다.

Do not proxy ARP on Destination Interface(대상 인터페이스에서 **ARP** 프록시 설정 안 함**)** - 매핑된 IP 주소로 들어오는 패킷에 대해 프록시 ARP를 비활성화합니다. 매핑된 인터페이스와 동일한 네트워크의 주소를 사용하는 경우 시스템은 매핑된 주소에 대한 ARP 요청에 답하기 위해 프록시 ARP를 사용하며, 이에 따라 매핑된 주소로 가야 하는 트래픽을 가로챕니다. 디바이스가 추가 네트워크에 대한 게이트웨이가 될 필요가 없으므로 이 솔루션은 라우팅을 간소화합니다. 원하는 경우 프록시 ARP를 비활성화할 수 있습니다. 이 경우 업스트림 라우터에 적절한 경로가 있어야 합니다.

단계 **6** **OK(**확인**)**를 클릭합니다.

DNS 구성

Remote Access VPN을 사용하려면 각 Firepower Threat Defense 디바이스에 DNS를 구성합니다. DNS가 없으면 디바이스는 AAA 서버 이름, 이름이 지정된 URL 및 FQDN 또는 호스트 이름이있는 CA 서버를 확인할 수 없습니다. IP 주소만 확인할 수 있습니다.

프로시저

단계 **1** 플랫폼 설정을 사용하여 DNS 서버 상세정보 및 도메인 조회 인터페이스를 구성합니다. 자세한 내용은 DNS 구성 및 DNS 서버 그룹 개체의 내용을 참조하십시오.

단계 2 VNP 네트워크를 통해 DNS 서버에 연결할 수 있는 경우 그룹 정책에서 스플릿 터널을 구성하여 Remote Access VPN 터널을 통한 DNS 트래픽을 허용합니다. 자세한 내용은 그룹 정책 개체 설정를 참고하십시오.

AnyConnect 클라이언트 프로파일 XML 파일 추가

AnyConnect 클라이언트 프로파일은 XML 파일에 저장된 구성 파라미터 그룹으로, 클라이언트는 이를 사용하여 운영 및 모양을 구성합니다. 이러한 매개변수(XML 태그)에는 추가적인 클라이언트 기능을 활성화할 수 있는 호스트 컴퓨터 및 설정의 이름과 주소가 포함되어 있습니다.

AnyConnect 프로파일 편집기를 사용하여 AnyConnect 클라이언트 프로파일을 생성할 수 있습니다. 이 편집기는 AnyConnect 소프트웨어 패키지의 일부로 제공되는 GUI 기반 구성 툴입니다. 이 툴은 Firepower Management Center 외부에서 실행되는 독립 프로그램입니다. AnyConnect 프로파일 편집기 사용에 대한 자세한 내용은 *Cisco AnyConnect Secure Mobility Client* 관리자 설명서를 참조하십시오.

시작하기 전에

Firepower Threat Defense Remote Access VPN 정책을 사용하려면 AnyConnect 클라이언트 프로파일을 VPN 클라이언트에 할당해야 합니다. 클라이언트 프로파일이 그룹 정책에 연결됩니다.

Cisco 소프트웨어 다운로드 센터에서 AnyConnect 프로파일 편집기를 다운로드할 수 있습니다.

프로시저

단계 1 **Devices(**디바이스**)**> **VPN** > **Remote Access(**원격 액세스**)**를 선택합니다.

단계 2 원격 액세스 VPN 정책을 선택하고 **Edit(**편집**)**를 클릭합니다.
Remote Access VPN 정책에 대해 구성된 연결 프로파일이 나열됩니다.

단계 3 AnyConnect 클라이언트 프로파일을 업데이트할 연결 프로파일을 선택하고 **Edit(**편집**)**을 클릭합니다.

단계 4 **Add(**추가**)**를 클릭하여 그룹 정책을 추가하거나 **Edit Group Policy(**그룹 정책 편집**)** > **General(**일반**)** > **AnyConnect**를 클릭합니다.

단계 5 목록에서 Client Profile(클라이언트 프로파일)을 선택하거나 **Add(**추가**)** 아이콘을 클릭하여 새 프로파일을 추가합니다.

a) AnyConnect 프로파일 이름을 지정합니다.

b) **Browse(**찾아보기**)**를 클릭하고 AnyConnect 프로파일 XML 파일을 선택합니다.

참고 2단계 인증의 경우 AnyConnect 클라이언트 프로파일 XML 파일에서 시간 초과가 60 초 이상으로 업데이트되었는지 확인합니다.

c) **Save(**저장**)**를 클릭합니다.

(선택 사항) 스플릿 터널링 구성

스플릿 터널을 이용하면 보안 터널을 통한 원격 네트워크 VPN 연결이 가능하며, VPN 터널 외부의 네트워크에도 연결할 수 있습니다. VPN 사용자가 원격 액세스 VPN에 연결되어 있는 동안 외부 네트워크에 액세스하게 하려면, 분할 터널을 구성하면 됩니다. 스플릿 터널 목록을 구성하려면 표준 액세스 목록 또는 확장 액세스 목록을 생성해야 합니다.

자세한 내용은 그룹 정책 구성, 35 페이지를 참고하십시오.

프로시저

단계 **1** **Devices(**디바이스**)**> **VPN** > **Remote Access(**원격 액세스**)**를 선택합니다.

단계 **2** 원격 액세스 정책을 선택하고 **Edit(**편집**)**을 클릭합니다.

단계 **3** Connection Profile(연결 프로파일)을 선택하고 **Edit(**편집**)**을 클릭합니다.

단계 **4** **Add(**추가**)**를 클릭하여 그룹 정책을 추가하거나 **Edit Group Policy(**그룹 정책 편집**)** > **General(**일반**)** > **Split Tunneling(**스플릿 터널링**)**을 클릭합니다.

단계 **5** **IPv4 Split Tunneling(IPv4** 스플릿 터널링**)** 또는 **IPv6 Split Tunneling(IPv6** 스플릿 터널링**)** 목록에서 **Exclude networks specified below(**아래에 지정된 네트워크 제외**)**를 선택하고, VPN 트래픽에서 제외할 네트워크를 선택합니다.
스플릿 터널링 옵션이 그대로 유지되면 엔드포인트의 모든 트래픽이 VPN 연결을 통해 이동합니다.

단계 **6** **Standard Access List(**표준 액세스 목록**)** 또는 **Extended Access List(**확장 액세스 목록**)**를 클릭하고 드롭다운 목록에서 액세스 목록을 선택하거나 새 목록을 추가합니다.

단계 **7** 새 표준 액세스 목록 또는 확장 액세스 목록을 추가하기로 선택한 경우 다음을 수행합니다.

a) 새 액세스 목록에 대한 이름을 지정하고 **Add(**추가**)**를 클릭합니다.
b) Action(동작) 드롭다운에서 **Allow(**허용**)**를 선택합니다.
c) VPN 터널에서 허용할 네트워크 트래픽을 선택하고 **Add(**추가**)**를 클릭합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

관련 항목

액세스 목록

구성 확인

프로시저

단계 **1** 외부 네트워크의 시스템에서 웹 브라우저를 엽니다.

단계 **2** 원격 액세스 VPN 게이트웨이로 구성된 FTD 디바이스의 URL을 입력합니다.

단계 **3** 메시지가 표시되면 사용자 이름 및 비밀번호를 입력하고 **Logon(**로그인**)**을 클릭합니다.

참고 시스템에 AnyConnect가 설치돼 있다면 VPN에 자동으로 연결됩니다.

AnyConnect가 설치되지 않았다면 AnyConnect 클라이언트를 다운로드하라는 메시지가 표시됩니다.

단계 4 설치되지 않았다면 AnyConnect를 다운로드하고 VPN에 연결합니다.
AnyConnect 클라이언트는 자체적으로 설치됩니다. 인증에 성공하면 Firepower Threat Defense 원격 액세스 VPN 게이트웨이에 연결됩니다. 해당하는 ID 또는 QoS 정책은 원격 액세스 VPN 정책 구성에 따라 적용됩니다.

원격 액세스 VPN 정책 대상 디바이스 설정

새 Remote Access VPN 정책을 생성하는 동안 대상 디바이스를 추가하거나 나중에 변경할 수 있습니다.

프로시저

단계 1 **Devices(**디바이스**)** > **VPN** > **Remote Access(**원격 액세스**)**를 선택합니다.

단계 2 편집할 Remote Access VPN 정책 옆의 수정( )을 클릭합니다.

단계 3 **Policy Assignment(**정책 할당**)**를 클릭합니다.

단계 4 다음 중 하나를 수행합니다.

- 디바이스, 스택, 고가용성 쌍 또는 디바이스 그룹을 정책에 할당하려면 **Available Devices(**사용 가능한 디바이스**)** 목록에서 이를 선택하고 **Add(**추가**)**를 클릭합니다. 사용 가능한 디바이스를 끌어다 놓아 선택할 수도 있습니다.
- 디바이스 할당을 제거하려면 **Selected Devices(**선택한 디바이스**)** 목록의 디바이스, 스택, 고가용성 쌍 또는 디바이스 그룹 옆에 있는 삭제( )를 클릭합니다.

단계 5 **OK(**확인**)**를 클릭합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.

선택적 Remote Access VPN 구성

연결 프로파일 설정

Remote Access VPN 정책은 특정 디바이스를 대상으로 하는 연결 프로파일을 포함합니다. 이러한 정책은 터널 자체를 생성하는 방법 예를 들어 AAA를 구현하는 방법, VPN 클라이언트에 주소를 할당하는 방법(DHCP 또는 주소 풀)과 관련이 있습니다. 또한 Firepower Threat Defense 디바이스에 구성되거나 AAA 서버에서 다운로드한 그룹 정책에서 식별된 사용자 속성을 포함합니다. 디바이스는

*DefaultWEBVPNGroup*이라는 기본 연결 프로파일도 제공합니다. 마법사를 사용하여 구성된 연결 프로파일이 목록에 나타납니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **VPN** > **Remote Access(**원격 액세스**)**을 선택합니다.

단계 **2** 목록에서 기존 원격 액세스 VPN 정책을 선택하고 해당 **Edit(**편집**)** 아이콘을 클릭합니다.

단계 **3** **Connection Profile(**연결 프로파일**)**을 선택하고 **Edit(**편집**)**을 클릭합니다.
연결 프로파일 편집 페이지가 표시됩니다.

단계 **4** (선택 사항) 여러 연결 프로파일을 추가합니다.
여러 연결 프로파일 설정, 20 페이지

단계 **5** VPN 클라이언트에 대한 IP 주소를 구성합니다.
VPN 클라이언트에 대한 IP 주소 설정, 21 페이지

단계 **6** (선택 사항) Remote Access VPN에 대한 AAA 설정을 업데이트합니다.
Remote Access VPN에 대한 AAA 설정, 23 페이지

단계 **7** (선택 사항) 별칭을 생성하거나 업데이트합니다.
연결 프로파일에 대한 별칭 생성 또는 업데이트, 29 페이지

단계 **8** 연결 프로파일을 저장합니다.

여러 연결 프로파일 설정

다른 VPN 사용자 그룹에 다른 권한을 부여하기로 결정한 경우 각 사용자 그룹에 대해 특정 연결 프로파일이나 그룹 정책을 구성할 수 있습니다. 예를 들어 금융 그룹에서 사설 네트워크의 특정 부분에 액세스하고 고객 지원 그룹에서 다른 부분에 액세스하며 MIS 그룹에서 기타 부분에 액세스하도록 허용할 수 있습니다. 또한, MIS 내에 있는 특정 사용자가 다른 MIS 사용자는 액세스할 수 없는 시스템에 액세스하도록 허용할 수도 있습니다. 연결 프로파일 및 그룹 정책은 이 작업을 안전하게 수행할 수 있도록 유연성을 제공합니다.

원격 액세스 정책 마법사를 사용하여 VPN 정책을 생성할 때 하나의 연결 프로파일만 구성할 수 있습니다. 나중에 더 많은 연결 프로파일을 추가할 수 있습니다. 디바이스는 *DefaultWEBVPNGroup*이라는 기본 연결 프로파일도 제공합니다.

시작하기 전에

연결 프로파일과 함께 원격 액세스 정책 마법사를 사용하여 Remote Access VPN을 구성했는지 확인합니다.

프로시저

단계 **1** Firepower Management Center 웹 인터페이스에서 **Devices(**디바이스**)**> **VPN** > **Remote Access(**원격 액세스**)**를 선택합니다.
기존 원격 액세스 정책이 나열됩니다.

단계 **2** 원격 액세스 VPN 정책을 선택하고 **Edit(**편집**)**을 클릭합니다.

단계 **3** **Add(**추가**)**를 클릭하고 Add Connection Profile(연결 프로파일 추가) 창에서 다음을 지정합니다.

a) **Connection Profile(**연결 프로파일**)**—원격 사용자가 VPN 연결에서 사용하는 이름을 제공합니다. 연결 프로파일은 원격 사용자가 VPN 디바이스에 연결하는 방법을 정의하는 파라미터 집합을 포함하고 있습니다.

b) **Client Address Assignment(**클라이언트 주소 할당**)** - 로컬 IP 주소 풀, DHCP 서버와 AAA 서버에서 원격 클라이언트에 대한 IP 주소를 할당합니다.

c) **AAA** - AAA 서버를 구성하여 보안 VPN 게이트웨이 역할의 매니지드 디바이스가 사용자(인증), 사용자가 수행하도록 허용된 작업(권한 부여) 및 사용자가 수행한 작업(계정)을 결정하도록 활성화합니다.

d) **Aliases(**별칭**)** - 연결 프로파일에 대한 대체 이름 또는 URL을 입력합니다. Remote Access VPN 관리자는 Alias name(별칭 이름) 및 Alias URL(별칭 URL)을 활성화 또는 비활성화할 수 있습니다. VPN 사용자는 AnyConnect VPN 클라이언트를 사용하여 Firepower Threat Defense 디바이스 Remote Access VPN에 연결할 때 별칭 이름을 선택할 수 있습니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

관련 항목

연결 프로파일 설정, 19 페이지

VPN 클라이언트에 대한 IP 주소 설정

클라이언트 주소 할당은 원격 액세스 VPN 사용자에게 IP 주소를 할당하는 방법을 제공합니다.

로컬 IP 주소 풀, DHCP 서버와 AAA 서버에서 원격 VPN 클라이언트에 대한 IP 주소를 지정하도록 구성할 수 있습니다. AAA 서버에 먼저 할당한 후 다른 서버에 할당합니다. **Client Address Assignment(**클라이언트 주소 할당**)** 정책을 **Advanced(**고급**)**탭에서 구성하고 할당 기준을 정의합니다. 이 연결 프로파일에 정의된 IP 풀은 연결 프로파일 관련 그룹 정책 또는 시스템 기본 그룹 정책인 **DfltGrpPolicy**에서 정의된 IP 풀이 없을 때만 사용됩니다.

IPv4 Address Pools(IPv4 주소 풀**)**—SSL VPN 라이언트가 Firepower Threat Defense 디바이스에 연결할 때 새 IP 주소가 제공됩니다. 주소 풀은 원격 클라이언트에 제공할 수 있는 주소 범위를 정의합니다. 기존 IP 주소 풀을 선택합니다. IPv4 주소 및 IPv6 주소 각각에 최대 6개의 풀을 추가할 수 있습니다.

참고 Firepower Management Center에 있는 기존 IP 풀에서 IP 주소를 사용하거나 **Add(**추가**)** 옵션을 사용하여 새 풀을 생성할 수 있습니다. Firepower Management Center에서 **Objects(**개체**) > Object Management(**개체 관리**) > Address Pools(**주소 풀**)** 경로를 사용해 IP 풀을 생성할 수 있습니다. 자세한 내용은 주소 풀를 참고하십시오.

프로시저

단계 **1** Firepower Management Center 웹 인터페이스에서 **Devices(**디바이스**)**> **VPN** > **Remote Access(**원격 액세스**)**를 선택합니다.
기존 원격 액세스 정책이 나열됩니다.

단계 **2** 원격 액세스 VPN 정책을 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 **3** 업데이트하려는 연결 프로파일을 선택하고 **Edit(**편집**)** > **Client Address Assignment(**클라이언트 주소 할당**)**를 클릭합니다.

단계 **4** **Address Pools(**주소 풀**)**에 대해 다음을 선택합니다.

a) **Add(**추가**)**를 클릭하여 IP 주소를 추가하고 **IPv4** 또는 **IPv6**를 선택하여 해당 주소 풀을 추가합니다. Available Pools(사용 가능한 풀)에서 IP 주소 풀을 선택하고 **Add(**추가**)**를 클릭합니다.

참고 여러 Firepower Threat Defense 디바이스에서 Remote Access VPN 정책을 공유하는 경우, 디바이스 레벨 개체 재정의를 사용하여 전역 정의를 각 디바이스의 고유 주소 풀로 대체하지 않으면 모든 디바이스가 동일한 주소 풀을 공유합니다. 고유 주소 풀은 디바이스가 NAT를 사용하지 않는 경우 주소 중복을 방지하기 위해 필요합니다.

b) **Add(**추가**)** 아이콘을 **Address Pools(**주소 풀**)**창에서 선택하고 새 IPv4 또는 IPv6 주소 풀을 선택합니다. IPv4 풀을 선택하는 경우 시작 및 종료 IP 주소를 제공합니다. 새 IPv6 주소 풀을 포함시키려면 **Numver of Addresses(**주소 수**)** 를 1~16384 범위에서 입력합니다. 개체가 여러 디바이스에서 공유되는 경우 IP 주소와 충돌을 방지하기 위해 **Allow Overrides(**재정의 허용**)**를 선택합니다. 자세한 내용은 주소 풀를 참고하십시오.

c) **OK(**확인**)**를 클릭합니다.

단계 **5** **DHCP Servers(DHCP** 서버**)**에 대해 다음을 선택합니다.

참고 DHCP 서버 주소는 IPv4 주소와만 구성할 수 있습니다.

a) 이름 및 DHCP(Dynamic Host Configuration Protocol) 서버 주소를 네트워크 개체로 지정합니다. **Add(**추가**)**를 클릭하여 개체 목록에서 서버를 선택합니다. DHCP 서버를 삭제하려면 **Delete(**삭제**)**를 클릭합니다.

b) 네트워크 개체를 추가하려면 **New Objects(**새 개체**)** 페이지에서 **Add(**추가**)**를 클릭합니다. 새 개체 이름, 설명, 네트워크를 입력하고 해당하는 경우 **Allow Overrides(**재정의 허용**)** 옵션을 선택합니다. 자세한 내용은 네트워크 개체 생성 및 개체 재정의 허용를 참조하십시오.

c) **OK(**확인**)**를 클릭합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

관련 항목

연결 프로파일 설정, 19 페이지

Remote Access VPN에 대한 AAA 설정

프로시저

단계 **1** **Devices(**디바이스**)** > **VPN** > **Remote Access(**원격 액세스**)**을 선택합니다.

단계 **2** 목록에서 기존 원격 액세스 VPN 정책을 선택하고 해당 **Edit(**편집**)** 아이콘을 클릭합니다.

단계 **3** 연결 프로파일을 선택하여 AAA 설정을 업데이트하고 **Edit(**편집**)** > **AAA**를 클릭합니다.

단계 **4** **Authentication(**인증**)**에 대해 다음을 선택합니다.

- **Authentication Method(**인증 방법**)** - 네트워크 및 네트워크 서비스에 대한 액세스를 허용하기 전에 사용자를 식별하는 방법을 결정합니다. 유효한 사용자 자격 증명(일반적으로 사용자 이름 및 암호)을 요구하여 액세스를 제어합니다. 클라이언트에서 인증서를 포함할 수도 있습니다. 지원되는 인증 방법은 **AAA** 전용, 클라이언트 인증서 전용 및 **AAA +** 클라이언트 인증서입니다.

  다음과 같이 **Authentication Method(**인증 방법**)**를 선택하는 경우:

  - **AAA Only(AAA** 전용**)** - **Authentication Server(**인증 서버**)**를 **RADIUS**로 선택하는 경우 Authorization Server(권한 부여 서버)는 기본적으로 동일한 값을 가집니다. 드롭다운 목록에서 **Accounting Server(**과금 서버**)**를 선택합니다. Authentication Server(인증 서버) 드롭다운 목록에서 **AD** 및 **LDAP**를 선택할 때마다 **Authorization Server(**권한 부여 서버**)** 및 **Accounting Server(**과금 서버**)**를 각각 수동으로 선택해야 합니다.

  - **Client Certificate Only(**클라이언트 인증서 전용**)** - 각 사용자가 클라이언트 인증서로 인증합니다. 클라이언트 인증서는 VPN 클라이언트 엔드포인트에서 구성해야 합니다. 기본적으로 사용자 이름은 클라이언트 인증서 필드 CN 및 OU에서 파생됩니다. 사용자 이름이 클라이언트 인증서의 다른 필드에 지정된 경우 'Primary(기본)' 및 'Secondary(보조)' 필드를 사용하여 해당 필드를 매핑합니다.

    클라이언트 인증서의 사용자 이름을 포함하는 **Map specific field(**특정 필드 매핑**)** 옵션을 선택하면 **Primary(**기본**)** 및 **Secondary(**보조**)** 필드에 **CN(Common Name)** 및 **OU(Organizational Unit)**의 기본값이 표시됩니다. **Use entire DN as username(**전체 **DN**을 사용자 이름으로 사용**)** 옵션을 선택하는 경우 시스템은 자동으로 사용자 ID를 검색합니다. 고유 이름(DN)은 사용자를 연결 프로파일과 연결할 때 식별자로 사용할 수 있는 개별 필드로 구성된 고유한 ID입니다. DN 규칙은 향상된 인증서 인증에 사용됩니다.

    Map specific field(특정 필드 매핑**)** 옵션과 관련된 기본 및 보조 필드는 다음 공통 값을 포함합니다.

    - C(국가)
    - CN(이름)
    - DNQ(DN 한정자)
    - EA(이메일 주소)
    - GENQ(세대 한정자)
    - GN(이름)

- I(이니셜)
- L(시/군/구)
- N(이름)
- O(조직)
- OU(조직 단위)
- SER(일련 번호)
- SN(성)
- SP(시/도)
- T(제목)
- UID(사용자 ID)
- UPN(사용자 계정 이름)

- **Client Certificate & AAA(**클라이언트 인증서 및 **AAA)** - 각 사용자가 클라이언트 인증서와 AAA 서버로 인증합니다. 인증에 필요한 인증서 및 AAA 설정을 선택합니다.

  어떤 인증 방법을 선택하든 **Allow connection only if user exists in authorization database(**사용자가 권한 부여 데이터베이스에 있는 경우에만 연결 허용**)**를 선택하거나 선택 취소합니다.

- **SAML** - 각 사용자가 SAML SSO(Single Sign-On) 서버를 사용하여 인증됩니다. 자세한 내용은 SAML 2.0을 사용한 SSO(Single Sign-On) 인증, 52 페이지를 참고하십시오.

- 인증 서버 - 인증은 네트워크 및 네트워크 서비스에 대한 액세스를 허용하기 전에 사용자를 식별하는 방법입니다. 인증에는 유효한 사용자 자격 증명, 인증서 또는 둘 모두가 필요합니다. 인증을 단독으로 사용하거나 권한 부여 및 어카운팅과 함께 사용할 수 있습니다.

  목록에서 영역, RADIUS 서버 그룹 또는 SSO(Single Sign-On) 서버를 선택합니다. 또는 Add(추가)를 클릭하여 인증 서버를 생성합니다.

  - **Realm(**영역**)** - LDAP 또는 AD 영역을 설정합니다. 영역 생성의 내용을 참조하십시오.
  - **RADIUS Server Group(RADIUS** 서버 그룹**)** - RADIUS 서버에 RADIUS 서버 그룹 개체를 추가합니다. RADIUS 서버 그룹의 내용을 참조하십시오.
  - **Single Sign-On Server(SSO** 서버**)** - SAML 인증을 위한 SSO(Single Sign-On) 서버 개체를 생성합니다. SSO(Single Sign-On) 서버 추가의 내용을 참조하십시오.

- **2**차 인증 사용 - VPN 세션에 대한 추가 보안을 제공하기 위해 기본 인증 외에 2차 인증이 구성됩니다. 2차 인증은 **AAA** 전용 및 클라이언트 인증서 및 **AAA** 인증 방법에만 적용됩니다.

  보조 인증은 VPN 사용자가 AnyConnect 로그인 화면에 사용자 이름 및 암호 모음 2개를 입력해야 하는 선택적 기능입니다. 인증 서버 또는 클라이언트 인증서에서 2차 사용자 이름이 미리 입

력되도록 구성할 수도 있습니다. 원격 액세스 VPN 인증은 기본 인증과 보조 인증을 모두 성공한 경우에만 부여됩니다. 인증 서버 중 하나에 연결할 수 없거나 한쪽 인증에서 장애가 발생하면 VPN 인증이 거부됩니다.

보조 인증을 구성하기 전에, 두 번째 사용자 이름과 암호에 대해 보조 인증 서버 그룹(AAA 서버)을 구성해야 합니다. 예를 들어 기본 인증 서버는 LDAP나 Active Directory 영역으로, 보조 인증은 RADIUS 서버로 설정할 수 있습니다.

참고 기본적으로 보조 인증이 필수가 아닙니다.

인증 서버 - VPN 사용자에게 보조 사용자 이름 및 암호를 제공하는 보조 인증 서버입니다.

보조 인증용 사용자 이름에서 다음을 선택하십시오.

- 프롬프트: VPN 게이트웨이에 로그인하는 동안 사용자에게 사용자 이름과 암호를 입력하라는 메시지를 표시합니다.
- 기본 인증 사용자 이름 사용: 사용자 이름은 기본 인증 서버와 2차 인증 모두에 대해 기본 인증 서버에서 가져옵니다. 두 개의 암호를 입력해야 합니다.
- 클라이언트 인증서의 사용자 이름 매핑: 클라이언트 인증서의 보조 사용자 이름을 미리 채웁니다.
  - **Map specific field(**특정 필드 매핑**)** 옵션을 선택하면 클라이언트 인증서의 사용자 이름이 포함됩니다. **Primary(**기본**)** 및 **Secondary(**보조**)** 필드에는 **CN(Common Name)** 및 **OU(Organizational Unit)** 각각의 기본값이 표시됩니다. **Use entire DN (Distinguished Name) as username(**전체 **DN**을 사용자 이름으로 사용**)** 옵션을 선택하는 경우 시스템은 자동으로 사용자 ID를 검색합니다.

    기본 및 보조 필드 매핑에 대한 자세한 내용은 인증 방법 설명을 참조하십시오.
  - 인증서의 사용자 이름을 사용자 로그인 창에 미리 채우기: AnyConnect VPN 클라이언트를 통해 사용자가 연결할 때 클라이언트 인증서에서 보조 사용자 이름을 미리 채웁니다.
    - 로그인 창에서 사용자 이름 숨기기: 보조 사용자 이름은 클라이언트 인증서에서 미리 채워지지만 미리 채워진 사용자 이름은 수정을 방지하기 위해 사용자에게 표시되지 않습니다.
- **VPN** 세션에 보조 사용자 이름 사용: 보조 사용자 이름은 VPN 세션 중에 사용자 활동을보고하는 데 사용됩니다.

단계 **5** **Authorization(**권한 부여**)**에 대해 다음을 선택합니다.

- **Authorization Server(**권한 부여 서버**)** - 인증이 완료되면 권한 부여 기능에서 인증된 각 사용자에게 사용할 수 있는 서비스 및 명령을 제어합니다. 권한 부여 기능은 사용자가 수행할 수 있도록 인가를 받은 것이 무엇인지, 즉 사용자의 실제 능력 및 제한 사항을 설명하는 일련의 속성을 결합함으로써 작동합니다. 권한 부여 기능을 사용하지 않는 경우, 인증 기능에서만 인증된 모든 사용자에게 동일한 액세스 권한을 제공합니다. 권한 부여에는 인증이 필요합니다.

원격 액세스 VPN 인증 작업 방식에 대한 자세한 내용은 권한 및 속성 정책 시행 이해, 5 페이지의 내용을 참조하십시오.

연결 프로파일에서 사용자 인증을 위해 RADIUS 서버를 구성하면 Remote Access VPN 시스템 관리자는 사용자 또는 사용자 그룹에 대해 여러 권한 부여 속성을 구성할 수 있습니다. RADIUS 서버에 구성된 권한 부여 속성은 사용자 또는 사용자 그룹에 고유할 수 있습니다. 사용자가 인증되면 이러한 특정 권한 부여 속성이 Firepower Threat Defense 디바이스에 푸시됩니다.

참고 인증 서버에서 가져온 AAA 서버 속성은 그룹 정책 또는 연결 프로파일에서 이전에 구성되었을 속성 값보다 우선합니다.

- 필요한 경우 **Allow connection only if user exists in authorization database(**사용자가 권한 부여 데이터베이스에 있는 경우에만 연결 허용**)**를 선택합니다.

  활성화된 경우 시스템은 클라이언트의 사용자 이름이 권한 부여 데이터베이스에 있어야 연결이 허용되는지 여부를 확인합니다. 사용자 이름이 권한 부여 데이터베이스에 존재하지 않으면 연결이 거부됩니다.

- 권한 부여 서버로 영역을 선택할 경우, LDAP 속성 맵을 설정해야 합니다. 인증 및 권한 부여를 위한 단일 서버 또는 다른 서버를 선택할 수 있습니다. **Configure LDAP Attribute Map(LDAP** 속성 맵 설정**)**을 클릭하여 권한 부여를 위한 LDAP 속성 맵을 추가합니다.

  참고 Firepower Threat Defense는 SAML ID 제공자를 권한 부여 서버로 지원하지 않습니다. FMC 및 FTD를 통해 SAML ID 제공자 뒤에 있는 Active Directory에 연결할 수 있는 경우, 다음 단계에 따라 권한 부여를 설정할 수 있습니다.

  - AD 서버용 영역을 추가합니다. 영역 생성의 내용을 참조하십시오.
  - 원격 액세스 VPN 연결 프로파일에서 권한 부여 서버로 영역 개체를 선택합니다.
  - 선택한 영역에 대한 LDAP 속성 맵을 설정합니다.

LDAP 속성 맵을 설정하는 방법은 LDAP 특성 매핑 구성, 36 페이지의 내용을 참조하십시오.

단계 **6** **Accounting(**계정**)**에 대해 다음을 선택합니다.

- **Accounting Server(**과금 서버**)** - 계정은 사용자가 액세스하고 있는 서비스 및 사용 중인 네트워크 리소스의 양을 추적하는 데 사용됩니다. AAA 계정이 활성화되면 네트워크 액세스 서버는 사용자 활동을 RADIUS 서버에 보고합니다. 계정 관리 정보에는 세션 시작 및 중지 시각, 사용자 이름, 각 세션의 디바이스를 통과한 바이트 수, 사용한 서비스, 각 세션의 지속 시간이 포함됩니다. 네트워크 관리, 클라이언트 요금 청구 또는 감사에 대해 이 데이터를 분석할 수 있습니다. 관리 계정 기능을 단독으로 사용하거나 인증 및 권한 부여 기능과 함께 사용할 수 있습니다.

  Remote Access VPN 세션을 설명하는 데 사용할 RADIUS 서버 그룹 개체를 지정합니다.

단계 **7** 다음 **Advanced Settings(**고급 설정**)**를 선택합니다.

- **Strip Realm from username(**사용자 이름에서 영역 제거**)** - AAA 서버로 사용자 이름을 전달하기 전에 사용자 이름에서 영역을 제거하려면 선택합니다. 예를 들어 이 옵션을 선택하고 사용자가

*domain\username*을 입력하는 경우, 도메인은 사용자 이름에서 제거되고 인증을 위해 AAA 서버로 전송됩니다. 기본적으로 이 옵션은 선택되어 있지 않습니다.

- **Strip Group from username(**사용자 이름에서 그룹 제거**)** - AAA 서버로 사용자 이름을 전달하기 전에 사용자 이름에서 그룹 이름을 제거하려면 선택합니다. 기본적으로 이 옵션은 선택되어 있지 않습니다.

  참고 영역은 관리 도메인입니다. 이러한 옵션을 활성화하면 사용자 이름에만 근거하여 인증할 수 있습니다. 이러한 옵션의 조합을 활성화할 수 있습니다. 그러나 서버에서 구분 기호를 구문 분석할 수 없는 경우, 두 확인란을 모두 선택해야 합니다.

- **Password Management(**암호 관리**)** - Remote Access VPN 사용자의 암호 관리를 활성화합니다. 암호 만료 전 또는 암호가 만료되는 날에 미리 알리려면 선택합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

관련 항목

권한 및 속성 정책 시행 이해, 5 페이지
영역 관리

RADIUS 서버 속성 Firepower Threat Defense

Firepower Threat Defense 디바이스는 Remote Access VPN 정책에서 인증 및/또는 권한 부여를 위해 구성된 외부 RADIUS 서버의 VPN 연결에 사용자 권한 속성(사용자 자격 또는 권한이라고도 함)을 적용하도록 지원합니다.

참고 Firepower Threat Defense 디바이스에서는 벤더 ID가 3076인 속성을 지원합니다.

다음 사용자 권한 부여 속성은 RADIUS 서버에서 Firepower Threat Defense 디바이스로 전송됩니다.

- RADIUS 속성 146 및 150은 인증 및 권한 부여 요청을 위해 Firepower Threat Defense 디바이스에서 RADIUS 서버로 전송됩니다.
- 세 개의 속성(146, 150, 151)은 모두 계정 관리 시작, 중간 업데이트, 중단 요청을 위해 Firepower Threat Defense 디바이스에서 RADIUS 서버로 전송됩니다.

표 ***1: Firepower Threat Defense***에서 ***RADIUS*** 서버로 전송되는 속성

특성	속성 번호	구문, 유형	단일 또는 다중 값 지정	설명 또는 값
연결 프로파일 이름 또는 터널 그룹 이름	146	문자열	단일	1자 ~ 253자
클라이언트 유형	150	정수	단일	2 = AnyConnect Client SSL VPN, 6 = AnyConnect Client IPsec VPN (IKEv2)

특성	속성 번호	구문, 유형	단일 또는 다중 값 지정	설명 또는 값
세션 유형	151	정수	단일	1 = AnyConnect Client SSL VPN, 2 = AnyConnect Client IPsec VPN (IKEv2)

표 ***2: RADIUS*** 속성이 전송되는 대상***: Firepower Threat Defense***

특성	속성 번호	구문, 유형	단일 또는 다중 값 지정	설명 또는 값
Access-List-Inbound	86	문자열	단일	두 Acess-List(액세스 목록) 속성 모두 FTD 디바이스에 구성된 ACL의 이름을 따릅니다. 스마트 CLI 확장 액세스 목록 개체 유형을 사용해 이 ACL을 생성합니다(**Device(**장치**)** > **Advanced Configuration(**고급 컨피그레이션**)** > **Smart CLI(**스마트 **CLI)** > **Objects(**개체**)** 선택). 이 ACL에서는 인바운드(FTD 디바이스로 들어가는 트래픽) 또는 아웃바운드(FTD 디바이스에서 나가는 트래픽) 방향으로 트래픽 흐름을 제어합니다.
Access-List-Outbound	87	문자열	단일	
Address-Pools	217	문자열	단일	RA VPN에 접속하는 클라이언트에 대한 주소 풀로 사용될 서브넷을 식별하는 FTD 디바이스에 정의된 네트워크 개체의 이름입니다. **Objects(**개체**)** 페이지에서 네트워크 개체를 정의합니다.
Banner1	15	문자열	단일	사용자가 로그인하면 표시할 배너입니다.
Banner2	36	문자열	단일	사용자가 로그인하면 표시할 배너의 두 번째 부분입니다. 배너2는 배너1에 추가됩니다.
다운로드 가능한 ACL	Cisco-AV-Pair	merge-dacl {before-avpair | after-avpair}		Cisco-AV-Pair 구성을 통해 지원됩니다.
필터 ACL	86, 87	문자열	단일	필터 ACL은 RADIUS 서버의 ACL 이름으로 참조됩니다. ACL 구성이 이미 Firepower Threat Defense 디바이스에 있어야 하므로 RADIUS 권한 부여 중에 ACL 구성을 사용할 수 있습니다. 86 = 액세스 목록-인바운드 87 = 액세스 목록-아웃 바운드

특성	속성 번호	구문, 유형	단일 또는 다중 값 지정	설명 또는 값
Group-Policy	25	문자열	단일	연결에 사용할 그룹 정책입니다. RA VPN **Group Policy(**그룹 정책**)** 페이지에서 그룹 정책을 생성해야 합니다. 다음 형식 중 하나를 사용할 수 있습니다. • *group policy name* • OU=*group policy name* • OU=*group policy name*;
Simultaneous-Logins	2	정수	단일	사용자가 설정하도록 허용되는 별도의 동시 연결 개수입니다(0~2147483647).
VLAN	140	정수	단일	사용자의 연결을 제한할 VLAN입니다(0~4094). 또한 FTD 디바이스의 하위 인터페이스에 이 VLAN을 컨피그레이션해야 합니다.

연결 프로파일에 대한 별칭 생성 또는 업데이트

별칭에는 특정 연결 프로파일에 대한 대체 이름 또는 URL이 포함되어 있습니다. Remote Access VPN 관리자는 별칭 이름 및 별칭 URL을 활성화 또는 비활성화할 수 있습니다. VPN 사용자는 Firepower Threat Defense 디바이스에 연결하는 경우 별칭 이름을 선택할 수 있습니다. 이 디바이스에 구성된 모든 연결에서 별칭 이름 표시 기능은 켜거나 끌 수 있습니다. 또한 Remote Access VPN 연결을 시작하는 동안 엔드포인트에서 선택할 수 있는 별칭 URL 목록을 구성할 수 있습니다. 사용자가 별칭 URL을 사용하여 연결하는 경우, 시스템에서는 이 URL과 일치하는 연결 프로파일을 자동으로 로깅합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **VPN** > **Remote Access(**원격 액세스**)**을 선택합니다.

단계 **2** 사용 가능한 VPN 정책 목록에서 설정을 수정하려는 정책을 선택합니다.

단계 **3** **Connection Profile(**연결 프로파일**)**을 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 **4** **Aliases(**별칭**)**를 클릭합니다.

단계 **5** 별칭 이름을 추가하려면 다음을 수행합니다.

a) Alias Names(별칭 이름)에 **Add(**추가**)**를 클릭합니다.
b) **Alias Name(**별칭 이름**)**을 지정합니다.
c) 별칭을 활성화하려면 각 창에 있는 **Enabled(**활성화**)** 확인란을 선택합니다.
d) **OK(**확인**)**를 클릭합니다.

단계 **6** 별칭 URL을 추가하려면 다음을 수행합니다.

a) Alias URLs(별칭 URL)에 **Add(**추가**)**를 클릭합니다.

b) 목록에서 **Alias URL(**별칭 **URL)**을 선택하거나 새 URL 개체를 생성합니다. 자세한 내용은 URL 개체 생성를 참조하십시오.
c) 별칭을 활성화하려면 각 창에 있는 **Enabled(**활성화**)** 확인란을 선택합니다.
d) **OK(**확인**)**를 클릭합니다.

- **Edit(**편집**)**을 클릭하고 별칭 이름 또는 별칭 URL을 편집합니다.
- Alias name(별칭 이름) 또는 Alias URL(별칭 URL)을 삭제하려면 해당 행에 있는 **Delete(**삭제**)(**를 클릭합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

관련 항목

연결 프로파일 설정, 19 페이지

Remote Access VPN을 위한 액세스 인터페이스 구성

Access Interface(액세스 인터페이스**)** 테이블에는 디바이스 인터페이스가 포함된 인터페이스 그룹과 보안 영역이 나열됩니다. 이는 Remote Access SSL 또는 IPsec IKEv2 VPN 연결을 위해 구성됩니다. 해당 테이블에는 각 인터페이스 그룹 또는 보안 영역의 이름, 인터페이스에서 사용하는 인터페이스 신뢰 지점 및 DTLS(Datagram Transport Layer Security)의 사용 여부가 표시됩니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **VPN** > **Remote Access(**원격 액세스**)**을 선택합니다.
단계 **2** 목록에서 기존 원격 액세스 VPN 정책을 선택하고 해당 **Edit(**편집**)** 아이콘을 클릭합니다.
단계 **3** **Access Interface(**액세스 인터페이스**)**를 클릭합니다.
단계 **4** 액세스 인터페이스를 추가하려면 **Add(**추가**)**를 선택하고 **Add Access Interface(**액세스 인터페이스 추가**)** 창에서 다음에 대한 값을 지정합니다.
a) **Access Interface(**액세스 인터페이스**)** - 인터페이스가 속한 인터페이스 그룹 또는 보안 영역을 선택합니다.
인터페이스 그룹 또는 보안 영역은 라우팅 유형이어야 합니다. Remote Access VPN 연결에는 다른 인터페이스 유형이 지원되지 않습니다.
b) 다음 옵션을 선택하여 액세스 인터페이스와 프로토콜 개체를 연결합니다.

- **Enable IPSet-IKEv2(IPSet-IKEv2** 활성화**) - IKEv2** 설정을 활성화하려면 이 옵션을 선택합니다.
- **Enable SSL(SSL** 활성화**) - SSL** 설정을 활성화하려면 이 옵션을 선택합니다.
  - **Enable Datagram Transport Layer Security(Datagram Transport Layer Security** 활성화**)**를 선택합니다.

선택하면 인터페이스에서 DTLS(Datagram Transport Layer Security)를 활성화하며 SSL VPN 연결을 설정하는 AnyConnect VPN 클라이언트가 동시에 2개의 터널(SSL 터널 및 DTLS 터널)을 사용하도록 허용합니다.

DTLS를 활성화하면 특정 SSL 연결에서 발생하는 레이턴시 및 대역폭 문제를 방지하고 패킷 지연에 민감한 실시간 애플리케이션의 성능을 높입니다.

SSL 설정, TLS 및 DTLS 버전을 구성하려면 SSL 설정 정보의 내용을 참조하십시오.

AnyConnect VPN 클라이언트에 대한 SSL 설정을 구성하려면 그룹 정책 AnyConnect 옵션의 내용을 참조하십시오.

- **Configure Interface Specific Identity Certificate(**인터페이스별 **ID** 인증서 구성**)** 확인란을 선택하고 드롭다운 목록에서 **Interface Identity Certificate(**인터페이스 **ID** 인증서**)**를 선택합니다.

  인터페이스 ID 인증서를 선택하지 않는 경우 **Trustpoint(**신뢰 지점**)**가 기본적으로 사용됩니다.

  인터페이스 ID 인증서 또는 신뢰 지점을 선택하지 않는 경우 **SSL Global Identity Certificate(SSL** 전역 **ID** 인증서**)**가 기본적으로 사용됩니다.

c) **OK(**확인**)**를 클릭하여 변경 사항을 저장합니다.

단계 **5** **Access Settings(**액세스 설정**)**에서 다음을 선택합니다.

- **Allow Users to select connection profile while logging in(**사용자가 로그인 상태에서 연결 프로파일을 선택할 수 있음**)** - 여러 연결 프로파일이 있는 경우 이 옵션을 선택하면 사용자가 로그인 중에 올바른 연결 프로파일을 선택할 수 있습니다. **IPsec IKEv2** VPN에 대해 이 옵션을 선택해야 합니다.

단계 **6** **SSL Settings(SSL** 설정**)**를 구성하려면 다음 옵션을 사용합니다.

- **Web Access Port Number(**웹 액세스 포트 번호**)** - VPN 세션에 사용할 포트입니다. 기본 포트는 443입니다.
- **DTLS Port Number(DTLS** 포트 번호**)** - DTLS 연결에 대해 사용할 UDP 포트입니다. 기본 포트는 443입니다.
- **SSL Global Identity Certificate(SSL** 전역 **ID** 인증서**) - Interface Specific Identity Certificate(**인터페이스별 **ID** 인증서**)**가 제공되지 않으면 선택한 **SSL Global Identity Certificate(SSL** 전역 **ID** 인증서**)**가 모든 관련 인터페이스에 사용됩니다.

단계 **7** **IPsec-IKEv2 Settings(IPsec IKEv2** 설정**)**에서 목록의 **IKEv2 Identity Certificate(IKEv2 ID** 인증서**)**를 선택하거나 ID 인증서를 추가합니다.

단계 **8** **Save(**저장**)**를 클릭하여 액세스 인터페이스 변경 사항을 저장합니다.

관련 항목

보안 영역

Remote Access VPN 고급 옵션 설정

Cisco AnyConnect Secure Mobility Client 이미지

Cisco AnyConnect Secure Mobility Client 이미지

Cisco AnyConnect Secure Mobility Client는 기업 리소스에 대한 전체 VPN 프로파일링을 통해 원격 사용자에게 Firepower Threat Defense 디바이스에 대한 SSL 또는 IPsec(IKEv2) 연결을 제공합니다. 이전에 설치된 클라이언트가 없는 경우 원격 사용자는 브라우저에서 클라이언트리스 VPN 연결을 허용하도록 구성된 인터페이스의 브라우저에 IP 주소를 입력하여 AnyConnect 클라이언트를 다운로드하고 설치합니다. Firepower Threat Defense 디바이스는 원격 컴퓨터의 운영 체제와 일치하는 클라이언트를 다운로드합니다. 다운로드한 후 클라이언트는 보안 연결을 설치하고 설정합니다. 클라이언트를 이미 설치한 경우 사용자가 인증을 통과하면 Firepower Threat Defense 디바이스에서 클라이언트의 버전을 확인하고 필요에 따라 클라이언트를 업그레이드합니다.

Remote Access VPN 관리자는 새 AnyConnect 클라이언트 이미지 또는 추가 이미지를 VPN 정책에 연결합니다. 관리자 지원되지 않거나 단종되었으며 더 이상 필요하지 않은 클라이언트 패키지의 연결을 해제할 수 있습니다.

Firepower Management Center에서는 파일 패키지 이름을 사용하여 운영 체제의 유형을 결정합니다. 사용자가 운영 체제 정보를 나타내지 않고 파일의 이름을 바꾼 경우 유효한 운영 체제 유형을 목록 상자에서 선택해야 합니다.

AnyConnect 클라이언트 이미지 파일을 Cisco 소프트웨어 다운로드 센터에서 다운로드합니다.

관련 항목

Cisco AnyConnect Mobility Client 이미지 추가: Firepower Management Center, 32 페이지

Cisco AnyConnect Mobility Client 이미지 추가: Firepower Management Center

AnyConnect File 개체를 사용하여 Cisco AnyConnect Mobility Client 이미지를 Firepower Management Center에 업로드할 수 있습니다. 자세한 내용은 FTD 파일 개체를 참고하십시오. 클라이언트 이미지에 대한 자세한 내용은 Cisco AnyConnect Secure Mobility Client 이미지, 32 페이지 섹션을 참조하십시오.

Show re-order(순서 재구성 표시**)** 링크를 클릭하여 특정 클라이언트 이미지를 확인합니다.

참고 이미 설치된 Cisco AnyConnect 클라이언트 이미지를 삭제하려면 해당 행의 **Delete(**삭제**)**를 클릭합니다.

프로시저

단계 **1** Firepower Management Center 웹 인터페이스에서 **Devices(**디바이스**) > VPN > Remote Access(**원격 액세스**)**, 나열된 RA VPN 정책을 선택한 다음 **Advanced(**고급**)** 탭을 선택합니다.를 선택합니다.

단계 2 **AnyConnect Images(AnyConnect** 이미지**)** 대화 상자의 **Available AnyConnect Images(**사용 가능한 **AnyConnect** 이미지**)** 부분에서 **Add(**추가**)**를 클릭합니다.

단계 3 사용 가능한 AnyConnect 이미지의 이름, 파일 이름 및 설명을 입력합니다.

단계 4 **Browse(**찾아보기**)**를 클릭하여 업로드할 클라이언트 이미지를 선택할 위치로 이동합니다.

단계 5 Firepower Management Center에서 **Save(**저장**)**를 클릭하여 이미지를 업로드합니다.

Firepower Management Center에 클라이언트 이미지를 업로드하면 운영 체제는 Firepower Management Center에 업로드한 이미지에 대한 플랫폼 정보를 표시합니다.

관련 항목

Cisco AnyConnect Secure Mobility Client 이미지, 32 페이지

Remote Access VPN 클라이언트에 대한 AnyConnect 이미지 업데이트

Cisco AnyConnect 클라이언트 업데이트가 Cisco 소프트웨어 다운로드 센터에서 제공되면 패키지를 수동으로 다운로드하여 VPN 정책에 추가할 수 있으며, 이에 따라 새 AnyConnect 패키지가 운영 체제에 따라 VPN 클라이언트 시스템에서 업그레이드되도록 할 수 있습니다.

시작하기 전에

이 섹션의 지침은 새 AnyConnect 클라이언트 이미지를 Firepower Threat Defense VPN 게이트웨이에 연결하는 Remote Access VPN 클라이언트로 업데이트하는 데 도움이 됩니다. AnyConnect 이미지를 업데이트하기 전에 다음 구성이 완료되었는지 확인합니다.

- AnyConnect 이미지 파일을 Cisco 소프트웨어 다운로드 센터에서 다운로드하십시오.
- Firepower Management Center 웹 인터페이스에서 **Objects(**개체**)** > **Object Management(**개체 관리**)** > **VPN** > **AnyConnect File(AnyConnect** 파일**)**로 이동하고 새 AnyConnect 클라이언트 이미지 파일을 추가합니다.

프로시저

단계 1 Firepower Management Center 웹 인터페이스에서 **Devices(**디바이스**)**> **VPN** > **Remote Access(**원격 액세스**)**를 선택합니다.

단계 2 목록에서 기존 원격 액세스 정책을 선택하고 해당 **Edit(**편집**)**을 클릭합니다.

단계 3 **Advanced(**고급**)** > **AnyConnect Client Image(AnyConnect** 클라이언트 이미지**)** > **Add(**추가**)**를 클릭합니다.

단계 4 **Available AnyConnect Images(**사용 가능한 **AnyConnect** 이미지**)**에서 클라이언트 이미지 파일을 선택하고 **Add(**추가**)**를 클릭합니다.

필요한 AnyConnect 클라이언트 이미지가 목록에 없는 경우, **Add(**추가**)**를 클릭하여 이미지를 찾아 업로드합니다.

단계 5 Remote Access VPN 정책을 저장합니다.

Remote Access VPN 정책 변경 사항이 구축되면 Remote Access VPN 게이트웨이로 구성된 Firepower Threat Defense 디바이스에서 새 AnyConnect 클라이언트 이미지가 업데이트됩니다. 새로운 VPN 사용자가 VPN 게이트웨이에 연결하면 사용자는 클라이언트 시스템의 운영 체제에 따라 새로운 AnyConnect 클라이언트 이미지를 다운로드합니다. 기존 VPN 사용자의 경우 다음 VPN 세션에서 AnyConnect 클라이언트 이미지가 업데이트됩니다.

관련 항목

Remote Access VPN 연결 프로파일 옵션

Remote Access VPN 주소 할당 정책

Firepower Threat Defense 디바이스는 IPv4 또는 IPv6 정책을 사용하여 Remote Access VPN 클라이언트에 IP 주소를 할당할 수 있습니다. 둘 이상의 주소 할당 방법을 구성한 경우에는 Firepower Threat Defense 디바이스에서 IP 주소를 찾을 때까지 각 옵션을 검색합니다.

IPv4 또는 **IPv6** 정책

IPv4 또는 IPv6 정책을 사용하여 Remote Access VPN 클라이언트의 IP 주소를 지정할 수 있습니다. 먼저 IPv4 정책을 시도한 다음 나중에 IPv6 정책을 시도해야 합니다.

- **Use Authorization Server(**인증 서버 사용**)** - 외부 권한 부여 서버에서 사용자별로 주소를 검색합니다. IP 주소가 구성된 권한 부여 서버를 사용하는 경우 이 방법을 사용하는 것이 좋습니다. 주소 할당은 RADIUS 기반 인증 서버에서만 지원됩니다. AD/LDAP에는 지원되지 않습니다. IPv4 및 IPv6 할당 정책에 이 방법을 사용할 수 있습니다.
- **Use DHCP(DHCP** 사용**)** - 연결 프로파일에 구성된 DHCP 서버에서 IP 주소를 가져옵니다. 또한 그룹 정책에서 DHCP 네트워크 범위를 구성하여 DHCP 서버가 사용할 수 있는 IP 주소 범위를 정의할 수도 있습니다. DHCP를 사용하는 경우 **Objects(**개체**)> Object Management(**개체 관리**)> Network(**네트워크**)** 창에서 서버를 구성합니다. IPv4 할당 정책에 이 방법을 사용할 수 있습니다.

  DHCP 네트워크 범위 설정에 대한 자세한 내용은 그룹 정책 일반 옵션의 내용을 참조하십시오.
- **Use an internal address pool(**내부 주소 풀 사용**)** - 내부적으로 구성된 주소 풀은 주소 풀 할당을 구성하는 가장 간편한 방법입니다. 이 방법을 사용하는 경우 **Objects(**개체**) > Object Management(**개체 관리**) > Address Pools(**주소 풀**)** 창에서 IP 주소 풀을 만들고 연결 프로파일에서 선택합니다. IPv4 및 IPv6 할당 정책에 이 방법을 사용할 수 있습니다.
- **Reuse an IP address so many minutes after it is released(**릴리스된 후 **IP** 주소 다시 사용**)** - IP 주소가 주소 풀로 반환된 이후에 해당 IP 주소의 재사용을 지연시킵니다. 지연을 추가하면 IP 주소가 신속하게 재할당될 경우 방화벽에서 발생할 수 있는 문제를 방지하는 데 도움이 됩니다. 기본적으로 지연은 0으로 설정됩니다. 즉, Firepower Threat Defense 디바이스가 IP 주소 재사용에 지연을 적용하지 않는다는 의미입니다. 지연을 확장하려면 해당 상자를 선택하고 0분부터 480분의 범위에서 IP 주소 재할당을 지연시킬 기간(분)을 입력합니다. 이 구성 요소는 IPv4 할당 정책에 사용할 수 있습니다.

관련 항목

연결 프로파일 설정, 19 페이지
Remote Access VPN 인증, 4 페이지

인증서 맵 구성

인증서 맵을 사용하면 인증서 필드의 내용을 기반으로 사용자 인증서와 연결 프로파일을 일치시키는 규칙을 정의할 수 있습니다. 인증서 맵은 보안 게이트웨이의 인증서 인증에 사용됩니다.

규칙 또는 인증서 맵은 FTD 인증서 맵 개체에서 정의됩니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **VPN** > **Remote Access(**원격 액세스**)**을 선택합니다.

단계 **2** 목록에서 기존 원격 액세스 VPN 정책을 선택하고 해당 **Edit(**편집**)** 아이콘을 클릭합니다.

단계 **3** **Advanced(**고급**)** > **Certificate Maps(**인증서 맵**)**를 클릭합니다.

단계 **4** **General Settings for Certificate Group Matching(**인증서 그룹 일치에 대한 일반 설정**)** 창에서 다음 옵션을 선택합니다.

선택 사항은 우선 순위 기반이며 첫 번째 선택 항목과 일치하는 항목이 없는 경우 일치하는 옵션 목록이 계속됩니다. 규칙을 모두 충족할 때 매핑이 수행됩니다. 규칙이 충족되지 않으면 기본 연결 프로파일(하단에 나열됨)이 이 연결에 사용됩니다. 다음 옵션 중 일부 또는 전부를 선택하여 인증을 설정하고 클라이언트에 매핑되어야 하는 연결 프로파일(터널 그룹)을 결정합니다.

- 그룹 **URL**과 인증서 맵이 서로 다른 연결 프로파일과 일치하는 경우 그룹 **URL** 사용
- **Use the configured rules to match a certificate to a Connection Profile(**구성된 규칙을 사용하여 연결 프로파일에 인증서 일치**)** - 연결 프로파일 맵에서 여기에 정의된 규칙을 사용하도록 활성화합니다.

참고 인증서 매핑을 구성하는 작업은 인증서 기반 인증을 의미합니다. 원격 사용자에게는 구성된 인증 방법과 상관없이 클라이언트 인증서를 요구하는 메시지가 표시됩니다.

단계 **5** **Certificate to Connection Profile Mapping(**연결 프로파일에 인증서 매핑**)** 섹션에서 **Add Mapping(**매핑 추가**)**를 클릭하여 이 정책에 대한 연결 프로파일 매핑 인증서를 생성합니다.

a) **Certificate Map(**인증서 맵**)** 개체를 선택하거나 생성합니다.
b) 인증서 맵 개체의 규칙이 충족될 경우 사용해야 하는 **Connection Profile(**연결 프로파일**)**을 선택합니다.
c) 매핑을 생성하려면 **OK(**확인**)**를 클릭합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

그룹 정책 구성

그룹 정책은 원격 액세스 VPN 경험을 정의하는 그룹 정책 개체가 저장된 속성 및 값 쌍의 집합입니다. 예를 들어 그룹 정책 개체에서는 주소, 프로토콜, 연결 설정 등 일반 속성을 구성합니다.

VPN 터널이 설정된 경우 사용자에게 적용되는 그룹 정책이 결정됩니다. RADIUS 권한 서버는 그룹 정책을 할당하거나 현재 연결 프로파일에서 그룹 정책을 가져옵니다.

참고 FTD에 그룹 정책 속성 상속이 없습니다. 그룹 정책 개체 전체가 사용자에 대해 사용됩니다. 로그인 시 AAA 서버에서 식별된 그룹 정책 개체가 사용됩니다. 이를 지정하지 않은 경우, VPN 연결을 위해 구성된 기본 그룹 정책이 사용됩니다. 제공된 기본 그룹 정책은 기본값으로 설정할 수 있으나, 해당 정책이 연결 프로파일에 할당되어 있고 사용자의 다른 그룹 정책이 식별되지 않은 경우에만 사용됩니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **VPN** > **Remote Access(**원격 액세스**)**을 선택합니다.

단계 **2** 목록에서 기존 원격 액세스 VPN 정책을 선택하고 해당 **Edit(**편집**)** 아이콘을 클릭합니다.

단계 **3** **Advanced(**고급**)** > **Group Policies(**그룹 정책**)**를 클릭합니다.

단계 **4** 이 원격 액세스 VPN 정책과 연결할 하나 이상의 그룹 정책을 선택합니다. 원격 액세스 VPN 정책 생성에서 할당된 기본 그룹 정책보다 더 많습니다. **Add(**추가**)**를 클릭합니다.

Refresh(새로 고침**)** 및 **Search(**검색**)** 유틸리티를 사용하여 그룹 정책을 찾습니다. 필요하다면 새 그룹 정책 개체를 추가합니다.

단계 **5** 사용 가능한 그룹 정책에서 그룹 정책을 선택하고 **Add(**추가**)**를 클릭하여 선택합니다.

단계 **6** **OK (**확인**)**를 클릭하여 그룹 정책 선택을 완료합니다.

관련 항목

그룹 정책 개체 설정

LDAP 특성 매핑 구성

LDAP 속성 이름은 LDAP 사용자 또는 그룹 속성 이름을 Cisco에서 이해할 수 있는 이름에 매핑합니다. 속성 맵은 AD(Active Directory) 또는 LDAP 서버에 있는 속성을 Cisco 속성 이름과 동일시합니다. 모든 표준 LDAP 속성은 잘 알려진 벤더별 속성(VSA)에 매핑할 수 있습니다. 하나 이상의 LDAP 속성을 하나 이상의 Cisco LDAP 속성에 매핑할 수 있습니다. 원격 액세스 VPN 연결을 설정하는 동안 AD 또는 LDAP 서버에서 FTD 디바이스에 인증을 반환하면 FTD 디바이스에서 이 정보를 사용하여 AnyConnect 클라이언트가 연결을 완료하는 방법을 조정할 수 있습니다.

VPN 사용자에게 다른 액세스 권한 또는 VPN 콘텐츠를 제공하려는 경우 VPN 서버에서 서로 다른 VPN 정책을 설정하고 인증서를 기준으로 각 사용자에게 이러한 정책 집합을 할당할 수 있습니다. LDAP 특성 맵을 사용하여 LDAP 권한 부여를 설정하여 FTD에서 이를 수행할 수 있습니다. LDAP를 사용하여 사용자에게 그룹 정책을 할당하려면 AD(Active Directory) 특성 **memberOf**와 같은 LDAP 특성을 VPN 헤드 엔드에서 인식하는 **VPN-Group** 속성에 매핑하는 맵을 설정해야 합니다.

LDAP 특성 맵은 세 가지 구성 요소로 이루어집니다.

- **Name(**이름**)**-LDAP 속성 맵의 이름을 지정합니다. 선택한 영역을 기반으로 이름이 생성됩니다.
- **Attribute Name Mapping(**속성 이름 매핑**)** - LDAP 사용자 또는 그룹 속성 이름을 Cisco에서 이해할 수 있는 이름에 매핑합니다.

- **Attribute Value Mapping(**속성 값 매핑**)** - LDAP 사용자 또는 그룹 속성의 값을 선택한 이름 매핑에 대한 Cisco 속성의 값에 매핑합니다.

사용자가 FTD 원격 액세스 VPN에 연결할 때 **memberOf** 필드가 설정된 값과 일치하는 경우 그룹 정책 **VPN-Group**이 사용자의 VPN 세션에 적용됩니다.

LDAP 특성 맵에 사용된 그룹 정책은 원격 액세스 VPN 설정의 그룹 정책 목록에 추가됩니다. 원격 액세스 VPN 설정에서 그룹 정책이 제거되면 연결된 LDAP 특성 매핑도 제거됩니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **VPN** > **Remote Access(**원격 액세스**)**을 선택합니다.

단계 **2** 목록에서 기존 원격 액세스 VPN 정책을 선택하고 해당 **Edit(**편집**)** 아이콘을 클릭합니다.

단계 **3** **Advanced(**고급**)** > **LDAP Attribute Mapping(LDAP** 특성 매핑**)**을 클릭합니다.

단계 **4** **Add(**추가**)**를 클릭합니다.

단계 **5** Configure LDAP Attribute Map(LDAP 특성 맵 설정) 페이지에서 속성 맵을 설정할 영역을 선택합니다.

LDAP 특성 맵의 이름은 선택한 영역을 기반으로 생성됩니다. 영역을 변경하면 LDAP 특성 이름도 변경됩니다.

단계 **6** **Add(**추가**)**를 클릭합니다.

여러 속성 맵을 설정할 수 있습니다. 각 속성 맵에서는 이름 맵 및 값 맵을 구성해야 합니다.

참고 LDAP 특성 맵을 생성할 때 다음 지침을 따르십시오.

- LDAP 특성에 대해 하나의 매핑을 설정해야 합니다. 동일한 LDAP 특성 이름의 여러 매핑은 허용되지 않습니다.
- LDAP 특성 맵을 생성하려면 하나 이상의 이름 맵을 설정해야 합니다.
- 속성 맵이 원격 액세스 VPN 설정의 연결 프로파일과 연결되지 않은 경우 LDAP 특성 맵을 제거합니다.
- Cisco 및 LDAP 특성 이름과 값 모두에 대해 LDAP 특성 맵에서 올바른 철자와 대문자를 사용합니다.

a) **LDAP** 특성 이름을 지정한 다음 목록에서 필요한 **Cisco** 속성 이름을 선택합니다.

b) **Add Value Map(**값 맵 추가**)**을 클릭하고 **LDAP Attribute Value(LDAP** 특성 값**)** 및 **Cisco Attribute Value(Cisco** 속성 값**)**를 지정합니다.

값 맵을 더 추가하려면 이 단계를 반복합니다.

각각의 **Delete(**삭제**)** 아이콘을 클릭하여 LDAP 특성 맵, 이름 맵 또는 값 맵을 삭제할 수 있습니다.

단계 **7** **OK(**확인**)**를 클릭하여 LDAP 특성 맵 설정을 완료합니다.

단계 **8** LDAP 특성 매핑에 변경 사항을 저장하려면 **Save(**저장**)**를 클릭합니다.

관련 항목

Remote Access VPN에 대한 AAA 설정, 23 페이지
권한 및 속성 정책 시행 이해, 5 페이지

Remote Access VPN에 대한 IPsec 설정 구성

IPsec 설정은 Remote Access VPN 정책을 구성하는 동안 VPN 프로토콜로 IPsec을 선택한 경우에만 적용할 수 있습니다. 그렇지 않은 경우 Edit Access Interface(액세스 인터페이스 편집) 대화 상자를 사용하여 IKEv2를 활성화할 수 있습니다. 자세한 내용은 Remote Access VPN을 위한 액세스 인터페이스 구성, 30 페이지를 참조하십시오.

프로시저

단계 **1** **Devices(**디바이스**)** > **VPN** > **Remote Access(**원격 액세스**)**을 선택합니다.

단계 **2** 사용 가능한 VPN 정책 목록에서 설정을 수정하려는 정책을 선택합니다.

단계 **3** **Advanced(**고급**)**를 클릭합니다.

IPsec 설정 목록이 화면 왼쪽의 탐색창에 나타납니다.

단계 **4** 탐색창을 사용하여 다음 IPsec 옵션을 편집합니다.

a) **Crypto Maps(**암호화 맵**)** - Crypto Maps(암호화 맵) 페이지는 IKEv2 프로토콜이 활성화된 인터페이스 그룹을 나열합니다. 암호화 맵은 IKEv2 프로토콜이 활성화된 인터페이스에 대해 자동으로 생성됩니다. 암호화 맵을 편집하려면 Remote Access VPN 암호화 맵 설정, 38 페이지 섹션을 참조하십시오. **Access Interface(**액세스 인터페이스**)**에서 선택한 VPN 정책에 인터페이스 그룹을 추가하거나 제거할 수 있습니다. 자세한 내용은 Remote Access VPN을 위한 액세스 인터페이스 구성, 30 페이지를 참조하십시오.

b) **IKE Policy(IKE** 정책**)** - IKE Policy(IKE 정책) 페이지에는 AnyConnect 엔드포인트가 IPsec 프로토콜을 사용하여 연결할 때 선택된 VPN 정책에 적용할 수 있는 모든 IKE 정책 개체가 나열됩니다. 자세한 내용은 Remote Access VPN의 IKE 정책, 41 페이지를 참조하십시오. 새 IKE 정책을 추가하려면 IKEv2 정책 개체 구성 섹션을 참조하십시오. FTD에서는 AnyConnect IKEv2 클라이언트만 지원합니다. 타사 표준 IKEv2 클라이언트는 지원되지 않습니다.

c) **IPsec/IKEv2 Parameters(IPsec/IKEv2** 파라미터**)** - IPsec/IKEv2 Parameters(IPsec/IKEv2 파라미터) 페이지에서 IKEv2 세션 설정, IKEv2 보안 연결 설정, IPsec 설정 및 NAT Transparency 설정을 수정할 수 있습니다. 자세한 내용은 Remote Access VPN IPsec/IKEv2 파라미터 구성, 42 페이지를 참조하십시오.

단계 **5** **Save(**저장**)**를 클릭합니다.

Remote Access VPN 암호화 맵 설정

암호화 맵은 IPsec-IKEv2 프로토콜이 활성화된 인터페이스에 대해 자동으로 생성됩니다. **Access Interface(**액세스 인터페이스**)**에서 선택한 VPN 정책에 인터페이스 그룹을 추가하거나 제거할 수 있습니다. 자세한 내용은 Remote Access VPN을 위한 액세스 인터페이스 구성, 30 페이지를 참조하십시오.

프로시저

단계 **1** **Devices(**디바이스**)** > **VPN** > **Remote Access(**원격 액세스**)**을 선택합니다.

단계 **2** 사용 가능한 VPN 정책 목록에서 설정을 수정하려는 정책을 선택합니다.

단계 **3** **Advanced(**고급**)** > **Crypto Maps(**암호화 맵**)**를 클릭하고 테이블에서 행을 선택하고 **Edit(**편집**)**을 클릭하여 암호화 맵 옵션을 편집합니다.

단계 **4** **IKEv2 IPsec Proposals(IKEv2 IPsec** 제안**)**를 선택하고 터널에서 트래픽을 보호하는 데 사용할 인증 및 암호화 알고리즘을 지정하는 변환 집합을 선택합니다.

단계 **5** **Enable Reverse Route Injection(Reverse Route Injection** 활성화**)**을 선택하여 원격 터널 엔드포인트로 보호되는 네트워크 및 호스트에 대한 라우팅 프로세스에 정적 경로를 자동으로 삽입할 수 있도록 활성화합니다.

단계 **6** **Enable Client Services(**클라이언트 서비스 활성화**)**를 선택하고 포트 번호를 지정합니다.

Client Services Server는 AnyConnect Downloader가 AnyConnect 클라이언트가 요구하는 소프트웨어 업그레이드, 프로파일, 지역화 및 사용자 정의 파일, CSD, SCEP 및 기타 파일 다운로드를 수신할 수 있도록 HTTPS(SSL) 액세스를 제공합니다. 이 옵션을 선택하는 경우 클라이언트 서비스 포트 번호를 지정합니다. Client Services Server를 활성화하지 않으면 사용자가 AnyConnect 클라이언트에 필요할 수있는 파일을 다운로드할 수 없습니다.

참고 동일한 디바이스에서 실행 중인 SSL VPN에 사용하는 것과 동일한 포트를 사용할 수 있습니다. SSL VPN이 구성되어 있는 경우에도 IPsec-IKEv2 클라이언트에 대해 SSL을 통한 파일 다운로드를 활성화하려면 이 옵션을 선택해야 합니다.

단계 **7** **Enable Perfect Forward Secrecy(Perfect Forward Secrecy** 활성화**)**를 선택하고 **Modulus group(**모듈러스 그룹**)**을 선택합니다.

PFS(Perfect Forward Secrecy)를 사용하여 암호화된 각 교환에 대해 고유 세션 키를 생성하고 사용합니다. 고유 세션 키는 전체 교환이 기록되었으며 공격자가 엔드포인트 디바이스에서 사용하는 사전 공유 키 또는 개인 키를 확보했더라도 후속 암호 해독에서 교환을 보호합니다. 이 옵션을 선택하는 경우 **Modulus Group(**모듈러스 그룹**)** 목록에서 PFS 세션 키를 생성할 때 사용할 Diffie-Hellman 키 파생 알고리즘도 선택합니다.

모듈러스 그룹은 공유 암호를 각 IPsec 피어에 전송하지 않고 두 IPsec 피어 간에 파생하는 데 사용할 Diffie Hellman 그룹입니다. 대형 모듈러스는 보안성은 더 높지만, 처리 시간이 더 오래 걸립니다. 두 피어의 모듈러스 그룹이 일치해야 합니다. Remote Access VPN 구성에서 허용할 모듈러스 그룹을 선택합니다.

- 1 - Diffie-Hellman 그룹 1(768비트 모듈러스).
- 2 - Diffie-Hellman 그룹 2(1024비트 모듈러스).
- 5 - Diffie-Hellman 그룹 5(1536비트 모듈러스, 128비트 키에 적합한 보호를 제공하지만 14 그룹이 더 효과적임). AES 암호화를 사용하는 경우 이 그룹(또는 그 이상)을 사용하십시오.
- 14 - Diffie-Hellman 그룹 14(2048비트 모듈러스, 128비트 키에 적합한 보호를 제공함).
- 19 - Diffie-Hellman 그룹 19(256비트 엘립틱 커브 필드 크기).

- 20 - Diffie-Hellman 그룹 20(384비트 엘립틱 커브 필드 크기).
- 21 - Diffie-Hellman 그룹 21(521비트 엘립틱 커브 필드 크기).
- 24 - Diffie-Hellman 그룹 24(2048비트 모듈러스 및 256비트 소수 위수 하위 그룹).

단계 **8** 라이프타임 기간**(**초**)**을 지정합니다.

보안 연결(SA)의 라이프타임(초)입니다. 라이프타임이 초과되면 SA는 만료되며 두 피어 간에 SA를 재협상해야 합니다. 일반적으로 특정 지점까지는 라이프타임이 짧을수록 IKE 협상이 보다 안전합니다. 그러나 라이프타임이 길면 라이프타임이 짧은 경우에 비해 이후 IPsec 보안 연계를 더 빠르게 설정할 수 있습니다.

120~2147483647초 사이의 값을 지정할 수 있습니다. 기본값은 28800초입니다.

단계 **9** **Lifetime Size (kbytes)(**라이프타임 크기**(kbyte))**를 지정합니다.

만료되기 전에 지정된 보안 연결을 사용하여 IPsec 피어 간에 전달할 수 있는 트래픽 볼륨(KB)입니다.

10~2147483647kbyte 사이의 값을 지정할 수 있습니다. 기본값은 4,608,000킬로바이트입니다. 무제한 데이터를 허용하는 사양은 없습니다.

단계 **10** 다음 **ESPv3 Settings(ESPv3** 설정**)**를 선택합니다.

- **Validate incoming ICMP error messages(**들어오는 **ICMP** 오류 메시지 확인**)** - IPsec 터널을 통해 수신되고 비공개 네트워크의 내부 호스트로 전달되는 이러한 ICMP 오류 메시지를 검증할지 여부를 선택합니다.
- **Enable 'Do Not Fragment' Policy('**조각화 금지' 정책 활성화**)** - IPsec 하위 시스템에서 IP 헤더에 DF(Do Not Fragment) 비트가 설정된 대용량 패킷을 처리하는 방법을 정의하고 **Policy(**정책**)** 목록에서 다음 중 하나를 선택합니다.
  - Copy(복사) - DF 비트를 유지합니다.
  - Clear(지우기) - DF 비트를 무시합니다.
  - Set(설정) - DF 비트를 설정하고 사용합니다.
- Enable Traffic Flow Confidentiality (TFC) packets(TFC(Traffic Flow Confidentiality) 선택 - 패킷 활성화) - 터널을 우회하는 트래픽 프로파일을 마스킹하는 더미 TFC 패킷을 활성화합니다. **Burst(**버스트**)**, **Payload Size(**페이로드 크기**)** 및 **Timeout(**시간 초과**)** 파라미터를 사용하여 지정된 SA에서 무작위 간격으로 임의 길이의 패킷을 생성할 수 있습니다.
  - Burst(버스트) - 1~16 바이트 사이의 값을 지정합니다.
  - Payload Size(페이로드 크기) - 64~1024 바이트의 값을 지정합니다.
  - Timeout(시간 초과) - 10~ 60초 사이의 값을 지정합니다.

단계 **11** **OK(**확인**)**를 클릭합니다.

관련 항목

보안 영역

Remote Access VPN의 IKE 정책

IKE(Internet Key Exchange)는 IPsec 피어를 인증하고, IPsec 암호화 키를 협상 및 배포하고, IPsec SA(보안 연계)를 자동으로 설정하는 데 사용되는 키 관리 프로토콜입니다. IKE 협상은 2단계로 구성됩니다. 1단계에서는 두 IKE 피어 간의 보안 연계를 협상합니다. 그러면 피어가 2단계에서 안전하게 통신할 수 있습니다. 2단계 협상 중에는 IKE가 IPsec 등의 기타 애플리케이션에 대해 SA를 설정합니다. 두 단계에서는 모두 연결을 협상할 때 제안을 사용합니다. IKE 제안은 두 피어가 상호 간의 IKE 협상을 보호하는 데 사용하는 알고리즘 집합입니다. IKE 협상에서는 두 피어가 먼저 공통(공유) IKE 정책을 합의합니다. 이 정책은 후속 IKE 협상을 보호하는 데 사용되는 보안 파라미터를 제시합니다.

참고 FTD Remote Access VPN용 IKEv2만 지원합니다.

IKEv1과는 달리 IKEv2 제안의 경우, 한 그룹에서 여러 알고리즘과 모듈러스 그룹을 선택할 수 있습니다. 피어가 1단계 협상 중에 선택하기 때문에 단일 IKE 제안을 생성할 수 있도록 하지만 가장 원하는 옵션에 더 높은 우선 순위를 부여하는 여러 다른 제안을 고려하십시오. IKEv2의 경우 정책 개체가 인증을 지정하지 않으면 다른 정책이 인증 요건을 정의해야 합니다.

IKE 정책은 원격 액세스 IPsec VPN을 구성할 때 필요 합니다.

Remote Access VPN IKE 정책 구성

IKE 정책 테이블은 AnyConnect 엔드포인트가 IPsec 프로토콜을 사용하여 연결할 때 선택된 VPN 구성에 적용할 수 있는 모든 IKE 정책 개체를 지정합니다. 자세한 내용은 Remote Access VPN의 IKE 정책, 41 페이지를 참고하십시오.

참고 FTD Remote Access VPN용 IKEv2만 지원합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **VPN** > **Remote Access(**원격 액세스**)**을 선택합니다.

단계 **2** 사용 가능한 VPN 정책 목록에서 설정을 수정하려는 정책을 선택합니다.

단계 **3** **Advanced(**고급**)** > **IKE Policy(IKE** 정책**)**를 클릭합니다.

단계 **4** **Add(**추가**)**를 클릭하여 사용 가능한 IKEv2 정책 중에서 선택하거나 새 IKEv2 정책을 추가하고 다음을 지정합니다.

- **Name(**이름**)** - IKEv2 정책의 이름입니다.
- **Description(**설명**)** - IKEv2 정책에 대한 설명(선택 사항)입니다.

- **Priority(**우선 순위**)** - 우선 순위 값에 따라 일반 SA(보안 연계) 찾기를 시도할 때 두 협상 피어가 비교하는 IKE 정책의 순서가 결정됩니다.
- **Lifetime** - 보안 연결(SA)의 라이프타임(초)입니다.
- **Integrity(**무결성**)** - IKEv2 정책에 사용되는 해시 알고리즘의 무결성 알고리즘 부분입니다.
- **Encryption(**암호화**)** - 2단계 협상 보호를 위한 1단계 SA를 설정하는 데 사용되는 암호화 알고리즘입니다.
- **PRF Hash(PRF** 해시**)** - IKE 정책에 사용되는 해시 알고리즘의 의사 난수 함수(PRF) 부분입니다. IKEv2에서는 이러한 요소에 대해 서로 다른 알고리즘을 지정할 수 있습니다.
- **DH** 그룹— 암호화에 사용 되는 Diffie-hellman 그룹.

단계 **5** **Save(**저장**)**를 클릭합니다.

관련 항목

Remote Access VPN 액세스 인터페이스 옵션

Remote Access VPN IPsec/IKEv2 파라미터 구성

프로시저

단계 **1** **Devices(**디바이스**)** > **VPN** > **Remote Access(**원격 액세스**)**을 선택합니다.

단계 **2** 사용 가능한 VPN 정책 목록에서 설정을 수정하려는 정책을 선택합니다.

단계 **3** **Advanced(**고급**)** > **IPsec**> **IPsec/IKEv2 Parameters(IPsec/IKEv2** 파라미터**)**를 클릭합니다.

단계 **4** **IKEv2 Session Settings(IKEv2** 세션 설정**)**에 대해 다음을 선택합니다.

- **Identity Sent to Peer(**피어로 전송되는 **ID)** - IKE 협상 중에 피어가 자신을 식별하는 데 사용할 ID를 선택합니다.
  - **Auto(**자동**)** - 연결 유형에 따라 IKE 협상을 결정합니다. 예: 사전 공유 키의 IP 주소 또는 인증서 인증의 Cert DN(지원하지 않음)
  - **IP address(IP** 주소**)** - ISAKMP ID 정보를 교환하는 호스트의 IP 주소를 사용합니다.
  - **Hostname(**호스트 이름**)** - ISAKMP ID 정보를 교환하는 호스트의 FQDN(Fully Qualified Domain Name)을 사용합니다. 이 이름은 호스트 이름 및 도메인 이름으로 구성됩니다.
- **Enable Notification on Tunnel Disconnect(**터널 연결 해제 알림 활성화**)** - SA에서 수신한 인바운드 패킷이 해당 SA의 트래픽 선택기와 일치하지 않는 경우, 관리자가IKE 알림 피어 전송을 활성화 또는 비활성화할 수 있습니다. 이 알림의 전송은 기본적으로 비활성화되어 있습니다.
- **Do not allow device reboot until all sessions are terminated(**모든 세션이 종료될 때까지 디바이스 재부팅 허용 안 함**)** - 시스템 재부팅 전에 모든 활성 세션이 자발적으로 종료될 때까지 대기 활성화를 선택합니다. 기본적으로 비활성화되어 있습니다.

단계 **5** **IKEv2 Security Association (SA) Settings(IKEv2** 보안 연결**(SA)** 설정**)**에 대해 다음을 선택합니다.

- **Cookie Challenge(**쿠키 챌린지**)** - SA 개시 패킷에 대한 응답으로 쿠키 챌린지를 피어 디바이스로 전송할지 여부. 이는 Dos(서비스 거부) 공격 차단에 도움이 됩니다. 기본적으로 사용 가능한 SA의 50%가 협상중인 경우 쿠키 챌린지를 사용합니다. 다음 옵션 중 하나를 선택합니다.
  - **Custom(**사용자 정의**)** - 협상 중인 허용 SA 합계의 백분율인 수신 쿠키 챌린지 임계값을 지정합니다. 이렇게 하면 이후의 모든 SA 협상에 대해 쿠키 챌린지가 트리거됩니다. 범위는 0~100%이고, 기본값은 50%입니다.
  - Always(항상) - 항상 피어 디바이스에 쿠키 챌린지를 보내려면 선택합니다.
  - Never(안 함) - 피어 디바이스에 쿠키 챌린지를 보내지 않으려면 선택합니다.
-
- **Number of SAs Allowed in Negotiation(**협상에서 허용되는 **SA** 수**)** - 언제든지 협상에 참여할 수 있는 최대 SA 수를 제한합니다. Cookie Challenge(쿠키 챌린지)와 함께 사용하는 경우 효과적인 교차 확인을 위해 쿠키 챌린지 임계값을 이 한도보다 낮은 값으로 구성합니다. 기본값은 100%입니다.
- **Maximum number of SAs Allowed(**허용되는 최대 **SA** 수**)** - 허용되는 IKEv2 연결 수를 제한합니다.

단계 **6** **IPsec Settings(IPsec** 설정**)**에 대해 다음을 선택합니다.

- **Enable Fragmentation Before Encryption(**암호화 이전 단편화 활성화**)** - 이 옵션을 사용하면 트래픽이 IP 단편화를 지원하지 않는 NAT 디바이스를 통과할 수 있습니다. IP 단편화를 지원하는 NAT 디바이스의 작동을 방해하지 않습니다.
- **Path Maximum Transmission Unit Aging(**경로 최대 전송 단위 에이징**)** - SA(Security Association)의 PMTU(Path Maximum Transmission Unit) 재설정 간격인 PMTU Aging 활성화를 선택합니다.
- **Value Reset Interval(**값 재설정 간격**)** - SA(Security Association)의 PMTU 값이 원래 값으로 재설정되는 시간(분)을 입력합니다. 유효 범위는 10~30분이며, 기본값은 무제한입니다.

단계 **7** **NAT Settings(NAT** 설정**)**에 대해 다음을 선택합니다.

- **Keepalive Messages Traversal(Keepalive** 메시지 순회**)** - NAT keepalive 메시지 순회 활성화 여부를 선택합니다. NAT 순회 킵얼라이브는 VPN 연결 허브 및 스포크 사이에 위치한 디바이스(중간 디바이스)가 있는 경우 킵얼라이브 메시지 전송에 사용되며, 해당 디바이스는 IPsec flow에서 NAT를 수행합니다. 이 옵션을 선택하는 경우, 스포크와 중간 디바이스 간에 전송된 킵얼라이브 신호 간격을 초 단위로 구성하고 해당 세션이 활성임을 표시합니다. 이 값의 범위는 10~3600초입니다. 기본값은 20초입니다.
- **Interval(**간격**)** - NAT keepalive 간격을 10~3600초 범위로 설정합니다. 기본값은 20초입니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

RADIUS 동적 권한 부여

Firepower Threat Defense 에서는 동적 ACL 또는 사용자별 ACL 이름을 사용하는 VPN 원격 액세스 및 방화벽 cut-through-proxy 세션의 사용자 권한 부여에 RADIUS 서버를 이용할 수 있습니다. 동적 인증 또는 RADIUS CoA(RADIUS Change of Authorization)에 동적 ACL을 구현하려면, 이를 지원하는 RADIUS 서버를 구성해야 합니다. 사용자가 인증을 시도하면 RADIUS 서버가 다운로드 가능한 ACL 또는 ACL 이름을 Firepower Threat Defense로 전송합니다. 지정된 서비스에 대한 액세스는 ACL에 의해 허용되거나 거부됩니다. Firepower Threat Defense는 인증 세션이 만료되면 ACL을 삭제합니다.

관련 항목

RADIUS 서버 그룹
보안 영역
RADIUS 동적 권한 부여 구성, 44 페이지
RADIUS 서버 속성 Firepower Threat Defense, 27 페이지

RADIUS 동적 권한 부여 구성

시작하기 전에

- RADIUS 서버에서 참조되는 경우 보안 영역 또는 인터페이스 그룹에 하나의 인터페이스만 구성할 수 있습니다.
- 동적 권한 부여가 활성화된 RADIUS 서버는 동적 권한 부여가 작동하려면 Firepower Threat Defense 6.3 이상이 필요합니다.
- Firepower Threat Defense 6.2.3 또는 이전 버전에서는 RADIUS 서버의 인터페이스 선택이 지원되지 않습니다. 인터페이스 옵션은 구축하는 동안 재정의됩니다.

표 ***3:*** 절차

	수행해야 할 작업	추가 정보
1단계	Firepower Management Center 웹 인터페이스에 로그인합니다.	
2단계	동적 권한 부여를 위해 RADIUS 서버 개체를 구성합니다.	RADIUS 서버 그룹 옵션
3단계	CoA(Change of Authorization)가 활성화된 인터페이스를 통해 ISE 서버에 대한 경로를 구성하여 라우팅 또는 특정 인터페이스를 통한 Firepower Threat Defense에서 RADIUS 서버로의 연결을 설정합니다.	RADIUS 서버 그룹 옵션 사용자 제어를 위한 ISE/ISE-PIC 설정

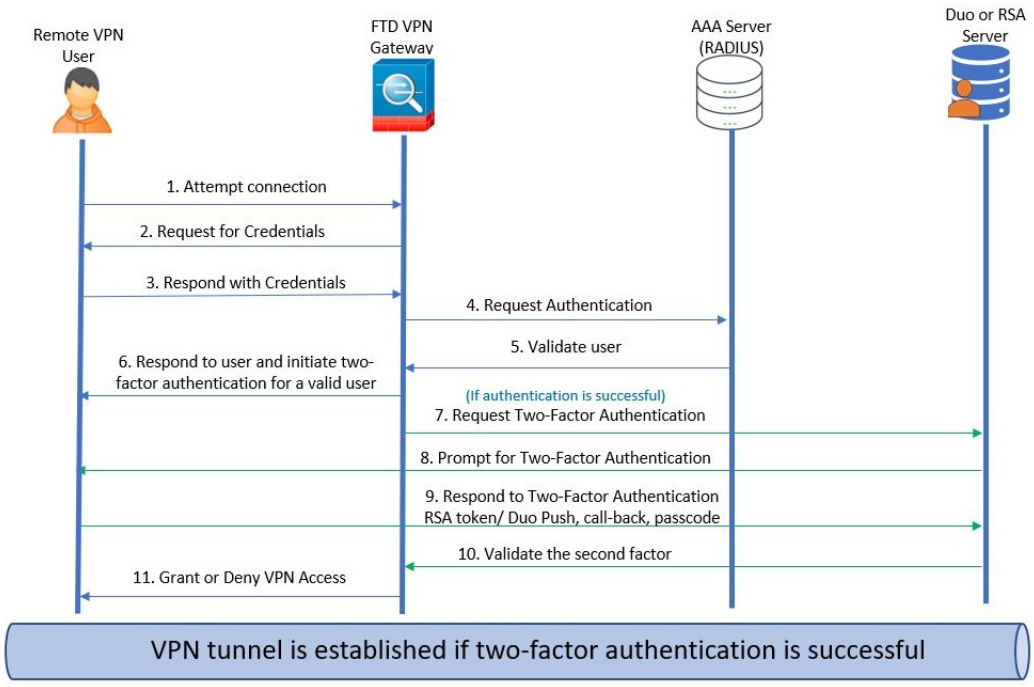
	수행해야 할 작업	추가 정보
4단계	Remote Access VPN 정책을 구성하고 동적 인증을 사용하여 만든 RADIUS 서버 그룹 개체를 선택합니다.	새 Remote Access VPN 정책 생성, 12 페이지
5단계	플랫폼 설정을 사용하여 DNS 서버 상세 정보 및 도메인 조회 인터페이스를 구성합니다.	DNS 구성, 16 페이지 DNS 서버 그룹 개체
6단계	VNP 네트워크를 통해 DNS 서버에 연결할 수 있는 경우 그룹 정책에서 스플릿 터널을 구성하여 Remote Access VPN 터널을 통한 DNS 트래픽을 허용합니다.	그룹 정책 개체 설정
7단계	구성 변경 사항을 구축합니다.	컨피그레이션 변경 사항 구축

이중 인증

Remote Access VPN에 대한 이중 인증을 구성할 수 있습니다. 이중 인증의 경우, 사용자는 사용자 이름 및 정적 암호뿐 아니라 RSA 토큰 또는 암호 같은 추가 항목도 제공해야 합니다. 이중 인증이 두 번째 인증 소스를 사용하는 것과 다른 점은 두 가지 인증 요소가 기본 인증 소스와 연결된 RSA 서버와의 관계에 따라 단일 인증 소스에서 구성된다는 것입니다.

Firepower Threat Defense 이중 인증 프로세스에서 첫 번째 요소인 RADIUS 또는 AD 서버와 함께 RSA 토큰과 Duo Mobile에 대한 Duo 푸시 인증 요청이 두 번째 요소로 지원됩니다.

그림 *1:* 이중 인증



RSA 이중 인증 구성

이 작업 관련 정보:

RADIUS 또는 AD 서버를 RSA 서버의 인증 에이전트로 구성하고 Firepower Management Center의 서버를 Remote Access VPN의 기본 인증 소스로 사용할 수 있습니다.

이 접근 방식을 사용하는 경우, 사용자는 RADIUS 또는 AD 서버에 구성된 사용자 이름을 사용하여 인증하고 암호와 토큰을 쉼표로 구분하여(암호,토큰) 암호를 일회용 임시 RSA 토큰과 연결해야 합니다.

이 컨피그레이션에서는 별도의 RADIUS 서버(예: Cisco ISE에서 제공되는 것)를 사용하여 권한 부여 서비스를 제공하는 것이 일반적입니다. 두 번째 RADIUS 서버를 권한 부여 서버 및 과금 서버(선택 사항)로 컨피그레이션합니다.

시작하기 전에

Firepower Threat Defense에서 RADIUS 이중 인증을 구성하기 전에 다음 구성이 완료되었는지 확인합니다.

RSA 서버

- RADIUS 또는 Active Directory 서버를 인증 에이전트로 구성합니다.
- 구성(*sdconf.rec*) 파일을 생성하고 다운로드합니다.

- 토큰 프로파일을 생성하고 사용자에게 토큰을 할당한 후 토큰을 사용자에게 배포합니다. VPN 클라이언트 시스템에 토큰을 다운로드하고 설치합니다.

자세한 내용은 RSA SecureID Suite 설명서를 참조하십시오.

ISE 서버

- RSA 서버에서 생성된 구성(*sdconf.rec*) 파일을 가져옵니다.
- RSA 서버를 외부 ID 소스로 추가하고 공유 암호를 지정합니다.

표 *4:* 절차

	수행해야 할 작업	추가 정보
1단계	Firepower Management Center 웹 인터페이스에 로그인합니다.	
2단계	새 RADIUS 서버 그룹을 생성합니다.	RADIUS 서버 그룹 옵션
3단계	새 RADIUS 서버 그룹 내에 RADIUS 서버 또는 AD 서버를 호스트로 사용하고 시간 초과가 60초 이상인 RADIUS 서버 개체를 만듭니다.	RADIUS 서버 옵션 참고 RADIUS 또는 AD 서버는 RSA 서버에서 인증 에이전트로 구성된 서버와 동일해야 합니다. 2단계 인증의 경우 AnyConnect 클라이언트 프로파일 XML 파일에서 시간 초과가 60 초 이상으로 업데이트되었는지도 확인합니다.
4단계	마법사를 사용하여 새 Remote Access VPN 정책을 구성하거나 기존 Remote Access VPN 정책을 편집합니다.	새 Remote Access VPN 정책 생성, 12 페이지
5단계	RADIUS를 인증 서버로 선택한 다음 새로 생성된 RADIUS 서버 그룹을 인증 서버로 선택합니다.	Remote Access VPN에 대한 AAA 설정, 23 페이지
7단계	구성 변경 사항을 구축합니다.	컨피그레이션 변경 사항 구축

듀오 이중 인증 구성

이 작업 관련 정보:

듀오 RADIUS 서버를 기본 인증 소스로 컨피그레이션할 수 있습니다. 이 접근 방식에서는 듀오 RADIUS 인증 프록시를 사용합니다. (LDAPS를 통한 듀오 클라우드 서비스와의 직접 연결은 사용할 수 없습니다.)

듀오를 구성하는 자세한 단계는 https://duo.com/docs/cisco-firepower를 참조하십시오.

그런 다음, 프록시 서버로 가는 인증 요청을 전달하여 다른 RADIUS 서버 또는 AD 서버를 첫 번째 인증 요소로 사용하고 듀오 클라우드 서비스는 두 번째 요소로 사용하도록 컨피그레이션합니다.

이 접근 방식을 사용한다면, 사용자는 듀오 클라우드나 웹 서버 중 하나 및 RADIUS 서버에 구성된 사용자 이름을 사용하여 인증해야 합니다. 사용자는 RADIUS 서버에서 구성한 비밀번호를 입력하고, 다음 듀오 코드 중 하나를 입력해야 합니다.

- **Dou-passcode**. 예: *my-password*,123456.
- **push**. 예: *my-password*,**push**. 푸시를 사용하여 듀오에게 듀오 모바일 앱으로 푸시 인증을 전송하도록 지시합니다. 사용자는 이미 이 앱을 설치하여 등록했어야 합니다.
- **SMS**. 예: *my-password*,**SMS**. **SMS**를 사용하여 듀오에게 사용자의 모바일 디바이스로 새로운 암호 배치가 포함된 SMS 메시지를 전송하도록 지시합니다. **SMS**를 사용하는 경우, 사용자의 인증 시도가 실패합니다. 그러면 사용자는 다시 인증하고 두 번째 요인으로 새 암호를 입력해야 합니다.
- **phone(**전화**)**. 예: *my-password*,**phone**. 전화기 콜백으로 인증하려면 **phone(**전화기**)**를 사용합니다.

예시가 포함된 로그인 옵션 관련 정보는 https://guide.duo.com/anyconnect의 내용을 참조하십시오.

시작하기 전에

Firepower Threat Defense에서 듀오 인증 프록시를 이용한 2단계 인증을 구성하기 전에, 다음 구성을 완료했는지 확인합니다.

- 듀오 구축을 시작하기 전에 원격 액세스 VPN 사용자에 대해 작동하는 기본 인증(RADIUS 또는 AD)을 구성합니다.
- 듀오 프록시 서비스를 네트워크의 Windows 또는 Linux 장치에 설치해 듀오를 Firepower Threat Defense 원격 액세스 VPN과 통합합니다. 이 듀오 프록시 서버는 RADIUS 서버 역할도 합니다.

  다음 위치에서 최신 듀오 인증 프록시를 다운로드하여 설치합니다.

  - **Windows**: https://dl.duosecurity.com/duoauthproxy-latest.exe
  - **Linux**: https://dl.duosecurity.com/duoauthproxy-latest-src.tgz
  - https://duo.com/docs/checksums#duo-authentication-proxy에서 체크섬을 확인합니다.
- 듀오 인증 파일 `authproxy.cfg`를 구성합니다. https://duo.com/docs/cisco-firepower#configure-the-proxy 페이지의 지침에 따라 인증 구성 설정을 구성합니다.

`authproxy.cfg` 구성 파일에는 RADIUS 또는 ISE 서버, Firepower Threat Defense 디바이스, 듀오 프록시 서버 상세정보, 통합 키, 비밀 키 및 API 호스트 상세정보가 있어야 합니다.

- `authproxy.cfg` 파일에 올바른 API 호스트 정보가 있는지 확인합니다.
- **Duo Security Server(**듀오 보안 서버**)** > **Duo Admin Panel(**듀오 관리자 창**)** > **Applications(**애플리케이션**)** > **CISCO RADIUS VPN**에서 새로 설치한 듀오 프록시 서버의 기타 필수 설정(보조 인증 요소 등)을 구성합니다.

표 *5:* 절차

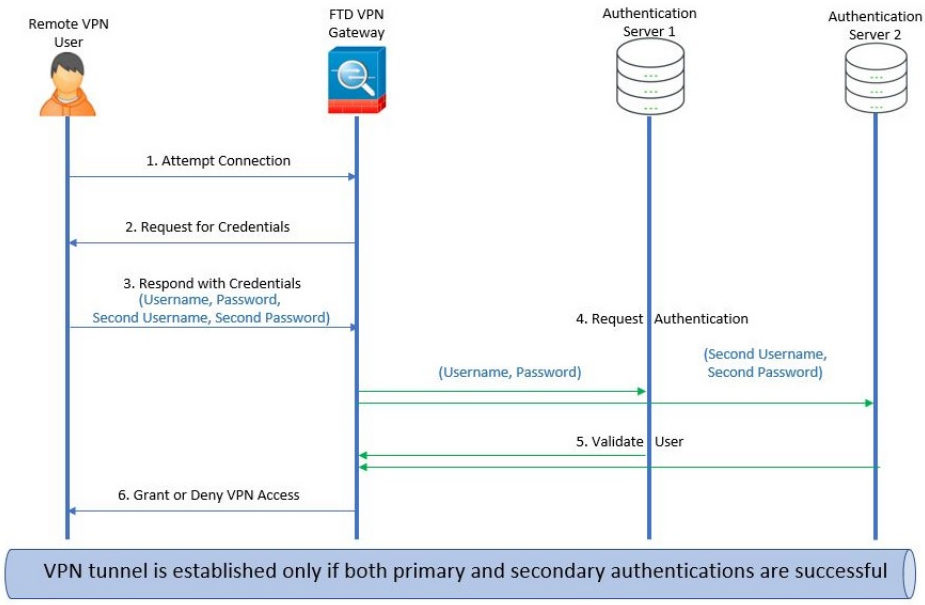
	수행해야 할 작업	추가 정보
1단계	Firepower Management Center 웹 인터페이스에 로그인합니다.	
2단계	새 RADIUS 서버 그룹을 생성합니다.	RADIUS 서버 그룹 옵션
3단계	새 RADIUS 서버 그룹 내에 듀오 프록시 서버를 호스트로 사용하고 시간 초과가 60초 이상인 RADIUS 서버 개체를 만듭니다.	RADIUS 서버 옵션 참고 2단계 인증의 경우 AnyConnect 클라이언트 프로파일 XML 파일에서 시간 초과가 60 초 이상으로 업데이트되었는지도 확인합니다.
4단계	마법사를 사용하여 새 Remote Access VPN 정책을 구성하거나 기존 Remote Access VPN 정책을 편집합니다.	새 Remote Access VPN 정책 생성, 12 페이지
5단계	RADIUS를 인증 서버로 선택한 다음, 듀오 프록시 서버로 생성한 RADIUS 서버 그룹을 인증 서버로 선택합니다.	Remote Access VPN에 대한 AAA 설정, 23 페이지
7단계	구성 변경 사항을 구축합니다.	컨피그레이션 변경 사항 구축

보조 인증

Firepower Threat Defense의 보조 인증 또는 이중 이중은 서로 다른 인증 서버 2개를 이용해 원격 액세스 VPN 연결에 레이어를 추가합니다. 보조 인증을 활성화하면, AnyConnect VPN 사용자는 자격 증명 모음 2개를 입력해야 VPN 게이트웨이에 로그인할 수 있습니다.

Firepower Threat Defense 원격 액세스 VPN은 AAA 전용과 클라이언트 인증서 및 AAA 인증 방법에서만 지원됩니다.

그림 ***2: Remote Access VPN*** 보조 또는 이중 인증



관련 항목

Remote Access VPN 보조 인증 구성, 50 페이지

Remote Access VPN 보조 인증 구성

Remote Access VPN 인증이 클라이언트 인증서와 인증 서버를 모두 사용하도록 구성되면 VPN 클라이언트 인증은 클라이언트 인증서 유효성 검사와 AAA 서버를 사용하여 수행됩니다.

시작하기 전에

- 인증 (AAA) 서버 2개, 즉 기본 및 보조 인증 서버를 구성하고, 필요한 ID 인증서를 구성합니다. 인증 서버는 RADIUS 서버나 AD 또는 LDAP 영역이 될 수 있습니다.
- 원격 액세스 VPN 구성이 작동하려면 Firepower Threat Defense 디바이스에서 AAA 서버에 연결할 수 있는지 확인합니다. 라우팅을 구성(**Devices(**디바이스**) > Device Management(**디바이스 관리**) > Edit Device(**디바이스 편집**) > Routing(**라우팅**)**)하여 AAA 서버에 대한 연결성을 보장합니다.

프로시저

단계 **1** Firepower Management Center 웹 인터페이스에서 **Devices(**디바이스**)**> **VPN** > **Remote Access(**원격 액세스**)**를 선택합니다.

단계 **2** 원격 액세스 정책을 선택하고 **Edit(**편집**)**을 클릭하거나 **Add(**추가**)**를 클릭하여 새 원격 액세스 VPN 정책을 생성합니다.

단계 **3** 새 Remote Access VPN 정책의 경우 연결 프로파일 설정을 선택하는 동안 인증을 구성합니다. 기존 구성의 경우 클라이언트 프로파일을 포함하는 연결 프로파일을 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 **4** **AAA** > **Authentication Method(**인증 방법**)**, **AAA** 또는 **Client Certificate & AAA(**클라이언트 인증서 및 **AAA)**를 클릭합니다.

- 다음과 같이 **Authentication Method(**인증 방법**)**를 선택하는 경우:

  Client Certificate & AAA(클라이언트 인증서 및 **AAA)** - 클라이언트 인증서와 AAA 서버를 모두 이용해 인증합니다.

  - **AAA - Authentication Server(**인증 서버**)**를 **RADIUS**로 선택하는 경우 Authorization Server(권한 부여 서버)는 기본적으로 동일한 값을 가집니다. 드롭다운 목록에서 **Accounting Server(**과금 서버**)**를 선택합니다. Authentication Server(인증 서버) 드롭다운 목록에서 **AD** 및 **LDAP**를 선택할 때마다 **Authorization Server(**권한 부여 서버**)** 및 **Accounting Server(**과금 서버**)**를 각각 수동으로 선택해야 합니다.
  - 어떤 인증 방법을 선택하든 **Allow connection only if user exists in authorization database(**사용자가 권한 부여 데이터베이스에 있는 경우에만 연결 허용**)**를 선택하거나 선택 취소합니다.

- **2**차 인증 사용 - VPN 세션에 대한 추가 보안을 제공하기 위해 기본 인증 외에 2차 인증이 구성됩니다. 2차 인증은 **AAA** 전용 및 클라이언트 인증서 및 **AAA** 인증 방법에만 적용됩니다.

  보조 인증은 VPN 사용자가 AnyConnect 로그인 화면에 사용자 이름 및 암호 모음 2개를 입력해야 하는 선택적 기능입니다. 인증 서버 또는 클라이언트 인증서에서 2차 사용자 이름이 미리 입력되도록 구성할 수도 있습니다. 원격 액세스 VPN 인증은 기본 인증과 보조 인증을 모두 성공한 경우에만 부여됩니다. 인증 서버 중 하나에 연결할 수 없거나 한쪽 인증에서 장애가 발생하면 VPN 인증이 거부됩니다.

  보조 인증을 구성하기 전에, 두 번째 사용자 이름과 암호에 대해 보조 인증 서버 그룹(AAA 서버)을 구성해야 합니다. 예를 들어 기본 인증 서버는 LDAP나 Active Directory 영역으로, 보조 인증은 RADIUS 서버로 설정할 수 있습니다.

  참고 기본적으로 보조 인증이 필수가 아닙니다.

  인증 서버 - VPN 사용자에게 보조 사용자 이름 및 암호를 제공하는 보조 인증 서버입니다.

  보조 인증용 사용자 이름에서 다음을 선택하십시오.

  - 프롬프트: VPN 게이트웨이에 로그인하는 동안 사용자에게 사용자 이름과 암호를 입력하라는 메시지를 표시합니다.
  - 기본 인증 사용자 이름 사용: 사용자 이름은 기본 인증 서버와 2차 인증 모두에 대해 기본 인증 서버에서 가져옵니다. 두 개의 암호를 입력해야 합니다.
  - 클라이언트 인증서의 사용자 이름 매핑: 클라이언트 인증서의 보조 사용자 이름을 미리 채웁니다.
    - **Map specific field(**특정 필드 매핑**)** 옵션을 선택하면 클라이언트 인증서의 사용자 이름이 포함됩니다. **Primary(**기본**)** 및 **Secondary(**보조**)** 필드에는 **CN(Common Name)** 및 **OU(Organizational Unit)** 각각의 기본값이 표시됩니다. **Use entire DN (Distinguished**

Name) as username(전체 **DN**을 사용자 이름으로 사용**)** 옵션을 선택하는 경우 시스템은 자동으로 사용자 ID를 검색합니다.

기본 및 보조 필드 매핑에 대한 자세한 내용은 인증 방법 설명을 참조하십시오.

- 인증서의 사용자 이름을 사용자 로그인 창에 미리 채우기: AnyConnect VPN 클라이언트를 통해 사용자가 연결할 때 클라이언트 인증서에서 보조 사용자 이름을 미리 채웁니다.
  - 로그인 창에서 사용자 이름 숨기기: 보조 사용자 이름은 클라이언트 인증서에서 미리 채워지지만 미리 채워진 사용자 이름은 수정을 방지하기 위해 사용자에게 표시되지 않습니다.

- **VPN** 세션에 보조 사용자 이름 사용: 보조 사용자 이름은 VPN 세션 중에 사용자 활동을보고하는 데 사용됩니다.

자세한 내용은 Remote Access VPN에 대한 AAA 설정, 23 페이지를 참고하십시오.

관련 항목

연결 프로파일 설정, 19 페이지

SAML 2.0을 사용한 SSO(Single Sign-On) 인증

SAML SSO(Single Sign-On) 인증 관련 정보

SAML(Security Assertion Markup Language)은 다른 상황에서 사용자의 세션을 기반으로 애플리케이션에 사용자를 로그인하기 위한 개방형 표준입니다. 조직은 사용자가 AD(Active Directory) 도메인 또는 인트라넷에 로그인할 때 사용자의 ID를 이미 알고 있습니다. 이들은 이 ID 정보를 사용하여 SAML을 사용하는 웹 기반 애플리케이션과 같은 다른 애플리케이션에 사용자를 로그인합니다. 개별 애플리케이션은 자격 증명을 저장할 필요가 없으며, 사용자는 개별 애플리케이션에 대해 서로 다른 자격 증명 집합을 기억하고 관리할 필요가 없습니다. SAML SSO(Sing Sign-On)는 한 위치(ID 제공자)에서 다른 위치(서비스 제공자)로 사용자 ID를 전송하는 방식으로 작동합니다.

SAML Single Sign-On Firepower Threat Defense

Firepower Threat Defense 디바이스는 AnyConnect Secure Mobility Client를 사용하는 원격 액세스 VPN 연결을 위한 SAML 2.0 SSO(Single Sign-On) 인증을 지원합니다. Firepower Threat Defense에서 SAML 2.0 SSO를 설정하려면 다음이 필요합니다.

- **IdP(Identity Provider)** - Duo Access Gateway는 사용자 인증을 수행하고 어설션을 발급하는 ID 제공자 역할을 합니다.
- **SP(Service Provider)** - FTD 디바이스가 서비스 제공자 역할을 하며 ID 제공자로부터 인증 어설션을 가져옵니다.

- **VPN** 클라이언트 - AnyConnect Security Mobility Client는 임베디드 브라우저를 통해 SAML 2.0 인증을 수행합니다.

SAML SSO(Single Sign-On) 인증 구성

시작하기 전에

FTD 원격 액세스 VPN으로 SAML 단일 로그인을 설정하기 전에 다음을 수행했는지 확인합니다.

- Duo로 계정 생성
- Duo Access Gateway 다운로드 및 설치
- SAML ID 제공자(Duo)에서 다음 정보를 얻습니다.
  - ID 제공자 엔티티 ID URL
  - 로그인 URL
  - 로그아웃 URL
  - ID 공급자 인증서
- **Object(**개체**)** > **Object Management(**개체 관리**)** > **AAA Server(ASA** 서버**)** > **Single Sign-on Server(SSO(Single Sign-On)** 서버**)**에서 SAML SSO(Single Sign-On) 서버 개체를 생성합니다.

참고 마법사를 사용하여 새 원격 액세스 VPN 설정을 생성할 때 연결 프로파일 설정에서 SSO(Single Sign-On) 서버 개체를 생성할 수도 있습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **VPN** > **Remote Access(**원격 액세스**)**을 선택합니다.

단계 **2** **Add(**추가**)**를 클릭하여 새 원격 액세스 VPN을 생성하거나 기존 VPN 설정을 편집합니다.

단계 **3** **Connection Profile(**연결 프로파일**)** > **AAA** 설정을 구성하고 **Authentication Method(**인증 방법**)** > **SAML**을 선택합니다.

단계 **4** 필요한 SAML SSO(Single Sign-On) 서버를 인증 서버로 선택합니다.

참고 새 원격 액세스 VPN 설정의 경우: 연결 프로파일 설정을 구성할 때 **Authentication Server(**인증 서버**)** 목록 옆의 +를 클릭하여 새 SAML SSO(Single Sign-On) 서버 개체를 생성할 수 있습니다.

SSO 서버 개체 생성에 대한 자세한 내용은 SSO(Single Sign-On) 서버 추가의 내용을 참조하십시오.

단계 **5** 원격 액세스 VPN에 대한 필요한 설정을 구성합니다.

단계 **6** 원격 액세스 VPN 설정을 저장하고 Firepower Threat Defense 디바이스에 구축합니다.

관련 항목

Remote Access VPN에 대한 AAA 설정, 23 페이지

Remote Access VPN AAA 사용자 지정

이 섹션에서는 원격 액세스 VPN에 대 한 AAA 기본 설정을 사용자 지정하는 방법을 설명합니다. 자세한 내용은 Remote Access VPN에 대한 AAA 설정, 23 페이지를 참고하십시오.

클라이언트 인증서를 통한 VPN 사용자 인증

마법사를 사용하여 새 Remote Access VPN 정책을 생성하거나 이후 정책을 편집할 때 클라이언트 인증서를 사용하여 Remote Access VPN 인증을 구성할 수 있습니다.

시작하기 전에

VPN 게이트웨이 역할을 하는 각 Firepower Threat Defense 디바이스에 대한 ID 인증서를 얻는 데 사용되는 인증서 등록 개체를 구성합니다.

프로시저

단계 **1** Firepower Management Center 웹 인터페이스에서 **Devices(**디바이스**)**> **VPN** > **Remote Access(**원격 액세스**)**를 선택합니다.

단계 **2** 원격 액세스 정책을 선택하고 **Edit(**편집**)**을 클릭하거나 **Add(**추가**)**를 클릭하여 새 원격 액세스 VPN 정책을 생성합니다.

단계 **3** 새 Remote Access VPN 정책의 경우 연결 프로파일 설정을 선택하는 동안 인증을 구성합니다. 기존 구성의 경우 클라이언트 프로파일을 포함하는 연결 프로파일을 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 **4** **AAA** > **Authentication Method(**인증 방법**)** > **Client Certificate Only(**클라이언트 인증서 전용**)**를 클릭합니다.

이 인증 방법을 통해 사용자는 클라이언트 인증서를 사용하여 인증됩니다. VPN 클라이언트 엔드포인트에서 클라이언트 인증서를 구성해야 합니다. 기본적으로 사용자 이름은 각각 클라이언트 인증서 필드 CN 및 OU에서 파생됩니다. 사용자 이름이 클라이언트 인증서의 다른 필드에 지정된 경우 'Primary(기본)' 및 'Secondary(보조)' 필드를 사용하여 해당 필드를 매핑합니다.

Map specific field(특정 필드 매핑**)** 옵션을 선택하면 클라이언트 인증서의 사용자 이름이 포함됩니다. **Primary(**기본**)** 및 **Secondary(**보조**)** 필드에는 **CN(Common Name)** 및 **OU(Organizational Unit)** 각각의 기본값이 표시됩니다. **Use entire DN as username(**전체 **DN**을 사용자 이름으로 사용**)** 옵션을 선택하는 경우 시스템은 자동으로 사용자 ID를 검색합니다. 고유 이름(DN)은 사용자를 연결 프로파일과 연결할 때 식별자로 사용할 수 있는 개별 필드로 구성된 고유한 ID입니다. DN 규칙은 향상된 인증서 인증에 사용됩니다.

- **Map specific field(**특정 필드 매핑**)** 옵션과 관련된 기본 및 보조 필드는 다음 공통 값을 포함합니다.
  - C(국가)
  - CN(이름)
  - DNQ(DN 한정자
  - EA(이메일 주소)
  - GENQ(세대 한정자)
  - GN(이름)
  - I(이니셜)
  - L(시/군/구)
  - N(이름)
  - O(조직)
  - OU(조직 단위)
  - SER(일련 번호)
  - SN(성)
  - SP(시/도)
  - T(제목)
  - UID(사용자 ID)
  - UPN(사용자 계정 이름)
- 어떤 인증 방법을 선택하든 **Allow connection only if user exists in authorization database(**사용자가 권한 부여 데이터베이스에 있는 경우에만 연결 허용**)**를 선택하거나 선택 취소합니다.

자세한 내용은 Remote Access VPN에 대한 AAA 설정, 23 페이지를 참고하십시오.

관련 항목

연결 프로파일 설정, 19 페이지
인증서 등록 개체 추가

클라이언트 인증서 및 AAA 서버를 통한 Remote Access VPN 로그인 설정

Remote Access VPN 인증이 클라이언트 인증서와 인증 서버를 모두 사용하도록 구성되면 VPN 클라이언트 인증은 클라이언트 인증서 유효성 검사와 AAA 서버를 사용하여 수행됩니다.

시작하기 전에

- VPN 게이트웨이 역할을 하는 각 Firepower Threat Defense 디바이스에 대한 ID 인증서를 얻는 데 사용되는 인증서 등록 개체를 구성합니다.
- 이 Remote Access VPN 정책에서 사용 중인 RADIUS 서버 그룹 개체와 AD 또는 LDAP 영역을 구성합니다.
- Remote Access VPN 구성이 작동하려면 Firepower Threat Defense 디바이스에서 AAA 서버에 연결할 수 있는지 확인합니다.

프로시저

단계 **1** Firepower Management Center 웹 인터페이스에서 **Devices(**디바이스**)**> **VPN** > **Remote Access(**원격 액세스**)**를 선택합니다.

단계 **2** 기존 원격 액세스 정책을 선택하고 **Edit(**편집**)**을 클릭하거나 **Add(**추가**)**를 클릭하여 새 원격 액세스 VPN 정책을 생성합니다.

단계 **3** 새 Remote Access VPN 정책의 경우 연결 프로파일 설정을 선택하는 동안 인증을 구성합니다. 기존 구성의 경우 클라이언트 프로파일을 포함하는 연결 프로파일을 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 **4** **AAA** > **Authentication Method(**인증 방법**)**, **Client Certificate & AAA(**클라이언트 인증서 및 **AAA)**를 클릭합니다.

- 다음과 같이 **Authentication Method(**인증 방법**)**를 선택하는 경우:

  Client Certificate & AAA(클라이언트 인증서 및 **AAA)** - 두 가지 인증 유형이 모두 수행됩니다.

  - **AAA - Authentication Server(**인증 서버**)**를 **RADIUS**로 선택하는 경우 Authorization Server(권한 부여 서버)는 기본적으로 동일한 값을 가집니다. 드롭다운 목록에서 **Accounting Server(**과금 서버**)**를 선택합니다. Authentication Server(인증 서버) 드롭다운 목록에서 **AD** 및 **LDAP**를 선택할 때마다 **Authorization Server(**권한 부여 서버**)** 및 **Accounting Server(**과금 서버**)**를 각각 수동으로 선택해야 합니다.
  - **Client Certificate(**클라이언트 인증서**)** - 사용자가 클라이언트 인증서로 인증합니다. 클라이언트 인증서는 VPN 클라이언트 엔드포인트에서 구성해야 합니다. 기본적으로 사용자 이름은 각각 클라이언트 인증서 필드 CN & OU에서 파생됩니다. 사용자 이름이 클라이언트 인증서의 다른 필드에 지정된 경우 'Primary(기본)' 및 'Secondary(보조)' 필드를 사용하여 해당 필드를 매핑합니다.

    Map specific field(특정 필드 매핑**)** 옵션을 선택하면 클라이언트 인증서의 사용자 이름이 포함됩니다. **Primary(**기본**)** 및 **Secondary(**보조**)** 필드에는 **CN(Common Name)** 및 **OU(Organizational Unit)** 각각의 기본값이 표시됩니다. **Use entire DN as username(**전체 **DN**을 사용자 이름으로 사용**)** 옵션을 선택하는 경우 시스템은 자동으로 사용자 ID를 검색합니다. 고유 이름(DN)은 사용자를 연결 프로파일과 연결할 때 식별자로 사용할 수 있는 개별 필드로 구성된 고유한 ID입니다. DN 규칙은 향상된 인증서 인증에 사용됩니다.

    Map specific field(특정 필드 매핑**)** 옵션과 관련된 기본 및 보조 필드는 다음 공통 값을 포함합니다.

- C(국가)
- CN(이름)
- DNQ(DN 한정자
- EA(이메일 주소)
- GENQ(세대 한정자)
- GN(이름)
- I(이니셜)
- L(시/군/구)
- N(이름)
- O(조직)
- OU(조직 단위)
- SER(일련 번호)
- SN(성)
- SP(시/도)
- T(제목)
- UID(사용자 ID)
- UPN(사용자 계정 이름)

- 어떤 인증 방법을 선택하든 **Allow connection only if user exists in authorization database(**사용자가 권한 부여 데이터베이스에 있는 경우에만 연결 허용**)**를 선택하거나 선택 취소합니다.

자세한 내용은 Remote Access VPN에 대한 AAA 설정, 23 페이지를 참고하십시오.

관련 항목

연결 프로파일 설정, 19 페이지
인증서 등록 개체 추가

VPN 세션에 대한 암호 변경 관리

암호 관리를 사용하면 Remote Access VPN 관리자는 암호 만료 시 Remote Access VPN 사용자에 대한 알림 설정을 구성할 수 있습니다. 암호 관리는 인증 방법 AAA Only(AAA 전용) 및 Client Certificate & AAA(클라이언트 인증서 및 AAA)를 통해 AAA 설정에서 사용할 수 있습니다. 자세한 내용은 Remote Access VPN에 대한 AAA 설정, 23 페이지를 참고하십시오.

프로시저

단계 1 Firepower Management Center 웹 인터페이스에서 **Devices(**디바이스**)**> **VPN** > **Remote Access(**원격 액세스**)**를 선택합니다.

단계 2 원격 액세스 정책을 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 3 AAA 설정이 포함된 연결 프로파일을 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 4 **AAA** > **Advanced Settings(**고급 설정**)** > **Password Management(**비밀번호 관리**)**를 선택합니다.

단계 5 **Enable Password Management(**비밀번호 관리 활성화**)**를 선택하고 다음 중 하나를 선택합니다.

- Notify User(사용자에게 알림) - 비밀번호가 만료되기 전에 사용자에게 알립니다. 입력란에 일 수를 지정합니다.
- Notify user on the day password expiration(비밀번호 만료 당일에 사용자에게 알림) - 비밀번호가 만료되는 당일에만 사용자에게 알립니다.

단계 6 **Save(**저장**)**를 클릭합니다.

관련 항목

연결 프로파일 설정, 19 페이지

인증을 위한 LDAP 또는 Active Directory 설정

인증을 위해 LDAP 또는 Active Directory(AD) 서버에서 VPN을 구성하려는 경우 Firepower Management Center 웹 인터페이스에서 속성 맵이 직접 지원되지 않으므로 FlexConfig 개체를 사용하여 속성 맵을 구성해야 합니다.

시작하기 전에

LDAP 또는 AD에 대한 영역 개체를 생성했는지 확인합니다.

프로시저

단계 1 Firepower Management Center 웹 인터페이스에서 **Devices(**디바이스**)**> **VPN** > **Remote Access(**원격 액세스**)**를 선택합니다.

단계 2 LDAP 또는 AD 영역 개체를 인증 서버로 사용하여 Remote Access VPN 정책을 생성합니다. 또는 기존 Remote Access VPN 구성을 편집하고 LDAP 또는 AD 영역을 인증 서버로 선택합니다.

단계 3 **Objects(**개체**)** > **Object Management(**개체 관리**)** > **FlexConfig** > **FlexConfig Object(FlexConfig** 개체**)**를 선택합니다.

단계 4 FlexConfig 정책을 생성하고 append 섹션에 다음 두 FlexConfig 개체를 생성 및 할당합니다.

FlexConfig 정책 설정의 내용을 참조하십시오.

a) **Deployment type**: Once 및 **Type**: Append를 사용하여 LDAP 특성 맵용 FlexConfig 개체를 생성합니다.

개체 본문에 다음을 입력합니다.

```
lda attribute-map <LDAP_Map_for_VPN_Access>
          map-name  memberOf Group-Policy
          map-value memberOf CN=APP-SSL-VPN Managers,CN=Users,OU=stbu,DC=cisco,DC=com
LabAdminAccessGroupPolicy
          map-value memberOf CN=cisco-Eng,CN=Users,OU=stbu,DC=cisco,DC=com
VPNAccessGroupPolicy
```

b) **Deployment type**: Everytime 및 **Type**: Append를 사용하여 LDAP 특성 맵에 연결되는 FlexConfig 개체를 생성합니다.

참고 Firepower Management Center에 의해 무효화되므로 LDAP-attribute-map 연결을 복원하기 위해 이 매핑이 필요합니다.

개체 본문에 다음을 입력합니다.

```
aaa-server <LDAP/AD_Realm_name> host <AD Server IP>
          ldap-attribute-map <LDAP_Map_for_VPN_Access>
          exit
```

Remote Access VPN 정책 구성에 추가한 연결 프로파일의 AAA 서버 설정에 사용된 LDAP 영역 이름과 동일한 *aaa-server*를 사용합니다.

자세한 내용은 FlexConfig 텍스트 개체 설정를 참고하십시오.

a) **Save(**저장**)**를 클릭합니다.

FlexConfig 정책에서 FlexConfig 개체의 순서가 LDAP 특성 맵 FlexConfig 개체이고 그 뒤에 AAA 서버 개체가 오는지 확인합니다.

이렇게 하면 LDAP 특성 맵이 구성되어 Firepower Threat Defense 디바이스의 LDAP 서버 구성과 연결됩니다.

관련 항목

FlexConfig 개체 구성

RADIUS 서버로 계정 기록 전송

Remote Access VPN의 계정 기록은 VPN 관리자가 사용자가 액세스하는 서비스 및 사용자가 사용하는 네트워크 리소스의 양을 추적할 수 있도록 도와줍니다. 계정 관리 정보에는 사용자 세션 시작 및 중지 시각, 사용자 이름, 각 세션의 디바이스를 통과한 바이트 수, 사용한 서비스, 각 세션의 지속시간이 포함됩니다. 네트워크 관리, 클라이언트 요금 청구 또는 감사에 대해 이 데이터를 분석할 수 있습니다.

관리 계정 기능을 단독으로 사용하거나 인증 및 권한 부여 기능과 함께 사용할 수 있습니다. AAA 계정을 활성화하면 네트워크 액세스 서버가 구성된 계정 서버에 사용자 작업을 보고합니다. 모든 사용자 활동 정보가 Firepower Management Center에서 RADIUS 서버로 전송되도록 RADIUS 서버를 과금 서버로 구성할 수 있습니다.

참고 Remote Access VPN AAA 설정에서 인증, 권한 부여 및 계정을 위해 동일한 RADIUS 서버 또는 별도의 RADIUS 서버를 사용할 수 있습니다.

시작하기 전에

인증 요청이나 계정 기록을 전송할 RADIUS 서버로 RADIUS 그룹 개체를 구성합니다. RADIUS 서버 그룹 옵션의 내용을 참조하십시오.

Firepower Threat Defense 디바이스에서 RADIUS 서버에 연결할 수 있는지 확인합니다. **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Edit Device(**디바이스 편집**)** > **Routing(**라우팅**)**에서 Firepower Management Center에 대한 라우팅을 구성하여 RADIUS 서버에 대한 연결성을 보장합니다.

프로시저

단계 **1** Firepower Management Center 웹 인터페이스에서 **Devices(**디바이스**)**> **VPN** > **Remote Access(**원격 액세스**)**를 선택합니다.

단계 **2** 원격 액세스 정책을 선택하고 **Edit(**편집**)**을 클릭하거나 새 원격 액세스 VPN 정책을 생성합니다.

단계 **3** AAA 설정이 포함된 연결 프로파일을 선택하고 **Edit(**편집**)** > **AAA**를 클릭합니다.

단계 **4** RADIUS 서버를 **Accounting Server(**과금 서버**)**로 선택합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

관련 항목

연결 프로파일 설정, 19 페이지
Remote Access VPN에 대한 AAA 설정, 23 페이지

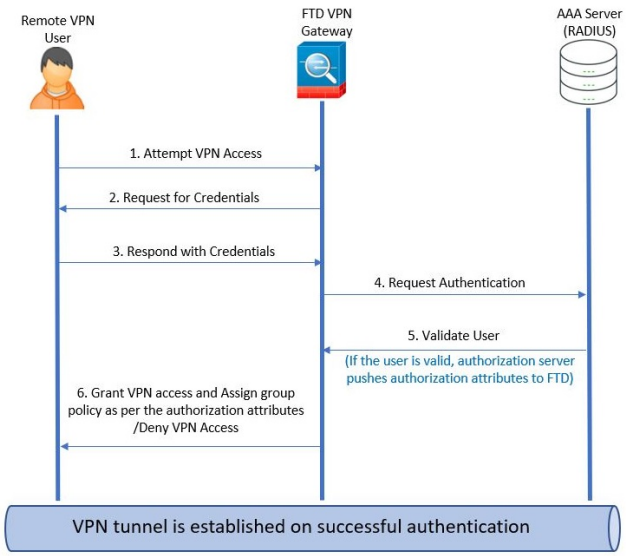
권한 부여 서버에 그룹 정책 선택 위임

VPN 터널이 설정된 경우 사용자에게 적용되는 그룹 정책이 결정됩니다. 마법사를 사용하여 원격 액세스 VPN을 생성하는 동안 연결 프로파일 그룹 정책을 선택하거나, 나중에 연결 프로파일의 연결 정책을 업데이트하면 됩니다. 하지만 AAA(RADIUS) 서버를 그룹 정책을 할당하도록 구성하거나, 현재 연결 프로파일에서 가져올 수도 있습니다. Firepower Threat Defense 디바이스에서 연결 프로파일에 구성된 속성과 충돌하는 속성을 AAA 서버로부터 수신하는 경우, AAA 서버에서 오는 속성이 항상 우선 적용됩니다.

IETF RADIUS 속성 25를 전송하고 해당 그룹 정책 이름에 매핑하여, 사용자 또는 사용자 그룹에 대한 인증 프로파일을 설정하도록 ISE 또는 RADIUS 서버를 구성할 수 있습니다. 특정 그룹 정책을 사용자 또는 사용자 그룹에 지정하여 다운로드 가능한 ACL을 푸시하고, 배너를 설정하고, VLAN을 제한하고, 세션에 SGT을 적용하는 고급 옵션을 구성할 수 있습니다. 이러한 속성은 VPN 연결이 설정될 때 해당 그룹에 속한 모든 사용자에게 적용됩니다.

자세한 내용은 Cisco Identity Services Engine 관리자 가이드의 Configure Standard Authorization Policies(표준 인증 정책 구성) 섹션과 RADIUS 서버 속성 Firepower Threat Defense, 27 페이지의 내용을 참조하십시오.

그림 ***3: AAA*** 서버의 ***Remote Access VPN*** 그룹 정책 선택



관련 항목

그룹 정책 개체 설정
연결 프로파일 설정, 19 페이지

그룹 정책 또는 기타 속성 선택을 권한 부여 서버로 재정의

Remote Access VPN 사용자가 VPN에 연결할 때 연결 프로파일에 구성된 그룹 정책 및 기타 속성이 사용자에게 할당됩니다. 하지만 원격 액세스 VPN 시스템 관리자는 사용자 또는 사용자 그룹에 대한 권한 부여 프로파일을 설정하기 위해 ISE 또는 RADIUS 서버를 구성하여 그룹 정책 및 기타 속성의 선택 사항을 권한 부여 서버에 위임할 수 있습니다. 사용자가 인증되면 이러한 특정 권한 부여 속성이 Firepower Threat Defense 디바이스에 푸시됩니다.

시작하기 전에

RADIUS를 인증 서버로 사용하여 Remote Access VPN 정책을 구성해야 합니다.

프로시저

단계 **1** Firepower Management Center 웹 인터페이스에서 **Devices(**디바이스**)**> **VPN** > **Remote Access(**원격 액세스**)**를 선택합니다.

단계 **2** 원격 액세스 정책을 선택하고 **Edit(**편집**)**을 클릭합니다.

단계 **3** 아직 구성되지 않은 경우 권한 부여 서버로 RADIUS 또는 ISE를 선택합니다.

단계 4 **Advanced(**고급**)** > **Group Policies(**그룹 정책**)**를 선택하고 필요한 그룹 정책을 추가합니다. 그룹 정책 개체에 대한 세부 정보는 그룹 정책 개체 설정의 내용을 참조하십시오.

하나의 그룹 정책 연결 프로 파일, 매핑할 수 있습니다. 그러나 Remote Access VPN 정책에서 여러 그룹 정책을 만들 수 있습니다. 이러한 그룹 정책은 ISE 또는 RADIUS 서버에서 참조될 수 있으며 권한 부여 서버에 권한 부여 속성을 지정하여 연결 프로파일에 구성된 그룹 정책을 대체하도록 구성할 수 있습니다.

단계 5 대상 Firepower Threat Defense 디바이스에서 구성을 구축합니다.

단계 6 권한 서버에서 IP 주소 및 다운로드할 수 있는 ACL에 대한 RADIUS 속성을 사용하여 권한 부여 프로파일을 생성합니다.

그룹 정책이 Remote Access VPN에 대해 선택된 권한 부여 서버에서 구성되면 그룹 정책은 사용자가 인증된 후 Remote Access VPN 사용자에 대한 연결 프로파일에 구성된 그룹 정책보다 우선합니다.

관련 항목

그룹 정책 개체 설정

사용자 그룹에 대한 VPN 액세스 거부

인증된 사용자 또는 사용자 그룹이 VPN을 사용할 수 없도록 하려는 경우 그룹 정책을 구성하여 VPN 액세스를 거부할 수 있습니다. Remote Access VPN 정책에서 그룹 정책을 구성하고 권한 부여를 위해 ISE 또는 RADIUS 서버 구성에서 이 정책을 참조할 수 있습니다.

시작하기 전에

원격 액세스 정책 마법사를 사용하여 Remote Access VPN을 구성하고 Remote Access VPN 정책에 대한 인증 설정을 구성했는지 확인합니다.

프로시저

단계 1 Firepower Management Center 웹 인터페이스에서 **Devices(**디바이스**)**> **VPN** > **Remote Access(**원격 액세스**)**를 선택합니다.

단계 2 원격 액세스 정책을 선택하고 **Edit(**편집**)**을 클릭합니다.

단계 3 **Advanced(**고급**)** > **Group Policies(**그룹 정책**)**를 클릭합니다.

단계 4 그룹 정책을 선택하고 새 그룹 정책 **Edit(**편집**)**를 클릭하거나 새 그룹 정책을 추가합니다.

단계 5 **Advanced(**고급**)** > **Session Settings(**세션 설정**)**를 선택하고 **Simultaneous Login Per User(**사용자별 동시 로그인**)**를 0으로 설정합니다.
이렇게 하면 사용자 또는 사용자 그룹이 VPN에 한 번도 연결되지 않습니다.

단계 6 **Save(**저장**)**를 클릭하여 그룹 정책을 저장한 다음 Remote Access VPN 구성을 저장합니다.

단계 7 해당 사용자/사용자 그룹에 대한 권한 부여 프로파일을 설정하여 IETF RADIUS 속성 25를 전송하고 해당 그룹 정책 이름에 매핑하도록 ISE 또는 RADIUS 서버를 구성합니다.

단계 8 ISE 또는 RADIUS 서버를 원격 액세스 VPN 정책의 인증 서버로 구성합니다.

단계 **9** 원격 액세스 VPN 정책을 저장하고 구축합니다.

관련 항목

연결 프로파일 설정, 19 페이지

사용자 그룹에 대한 연결 프로파일 선택 제한

사용자 또는 사용자 그룹에 단일 연결 프로파일을 적용하려는 경우 연결 프로파일을 비활성화할 수 있으며, 이에 따라 사용자가 AnyConnect VPN 클라이언트를 사용하여 연결할 때 그룹 별칭 또는 URL을 선택할 수 없습니다.

예를 들어 조직에서 휴대폰 사용자, 회사에서 발급한 노트북 사용자 또는 개인 노트북 사용자와 같은 다른 VPN 사용자 그룹에 특정 구성을 사용하려는 경우 이러한 각 사용자 그룹에 특정한 프로파일 연결을 구성하고 사용자가 VPN에 연결할 때 적절한 연결 프로파일을 적용할 수 있습니다.

AnyConnect 클라이언트는 기본적으로 Firepower Management Center에서 구성되고 Firepower Threat Defense에 구축된 연결 프로파일 목록(연결 프로파일 이름, 별칭 또는 별칭 URL 기준)을 표시합니다. 사용자 정의 연결 프로파일이 구성되지 않은 경우 AnyConnect는 *DefaultWEBVPNGroup* 연결 프로파일을 표시합니다. 다음 절차를 사용하여 사용자 그룹에 단일 연결 프로파일을 적용합니다.

시작하기 전에

- Firepower Management Center 웹 인터페이스에서 인증 방법과 함께 Remote Access VPN 정책 마법사를 사용하여 'Client Certificate Only(클라이언트 인증서 전용)' 또는 'Client Certificate + AAA(클라이언트 인증서 + AAA)'로 Remote Access VPN을 구성합니다. 인증서에서 사용자 이름 필드를 선택합니다.
- 권한 부여를 위해 ISE 또는 RADIUS 서버를 구성하고 그룹 정책을 권한 부여 서버와 연결합니다.

프로시저

단계 **1** Firepower Management Center 웹 인터페이스에서 **Devices(**디바이스**)**> **VPN** > **Remote Access(**원격 액세스**)**를 선택합니다.

단계 **2** 원격 액세스 정책을 선택하고 **Edit(**편집**)**을 클릭합니다.

단계 **3** **Access Interfaces(**액세스 인터페이스**)**를 선택하고 **Allow Users to select connection profile while logging in(**사용자가 로그인 상태에서 연결 프로파일을 선택할 수 있음**)**을 비활성화합니다.

단계 **4** **Advanced(**고급**)** > **Certificate Maps(**인증서 맵**)**를 클릭합니다.

단계 **5** **Use the configured rules to match a certificate to a Connection Profile(**구성된 규칙을 사용하여 연결 프로파일에 인증서 일치**)**을 선택합니다.

단계 **6** **Certificate Map Name(**인증서 맵 이름**)**을 선택하거나 **Add(**추가**)** 아이콘을 클릭하여 인증서 규칙을 추가합니다.

단계 **7** **Connection Profile(**연결 프로파일**)**을 선택하고 **Ok(**확인**)**를 클릭합니다.

이 구성을 사용하면 사용자가 AnyConnect 클라이언트에서 연결할 때 사용자가 매핑된 연결 프로파일을 갖게 되며 VPN을 사용하도록 인증됩니다.

관련 항목

그룹 정책 개체 설정

연결 프로파일 설정, 19 페이지

Remote Access VPN 클라이언트에 대한 AnyConnect 클라이언트 프로파일 업데이트

AnyConnect 클라이언트 프로파일은 AnyConnect의 일부로 VPN 클라이언트 시스템에 구축할 관리자 정의 최종 사용자 요구 사항 및 인증 정책이 포함된 XML 파일입니다. 사전 구성된 네트워크 프로파일을 최종 사용자가 사용할 수 있게 지원합니다.

독립적인 구성 도구인 GUI 기반 AnyConnect 프로파일 편집기를 사용하여 AnyConnect 클라이언트 프로파일을 생성할 수 있습니다. 독립형 프로파일 편집기를 사용하여 새로운 AnyConnect 프로파일을 만들거나 기존 프로파일을 수정할 수 있습니다. Cisco 소프트웨어 다운로드 센터에서 프로파일 편집기를 다운로드할 수 있습니다.

자세한 내용은 Cisco AnyConnect Secure Mobility Client 관리자 가이드에서 해당 릴리스의 AnyConnect 프로파일 편집기 장을 참조하십시오.

시작하기 전에

- 원격 액세스 정책 마법사를 사용하여 Remote Access VPN을 구성하고 Firepower Threat Defense 디바이스에 구성을 구축했는지 확인합니다. 새 Remote Access VPN 정책 생성, 12 페이지의 내용을 참조하십시오.
- Firepower Management Center 웹 인터페이스에서 **Objects(**개체**)** > **Object Management(**개체 관리**)** > **VPN** > **AnyConnect File(AnyConnect** 파일**)**로 이동하고 새 AnyConnect 클라이언트 이미지를 추가합니다.

프로시저

단계 **1** Firepower Management Center 웹 인터페이스에서 **Devices(**디바이스**)**> **VPN** > **Remote Access(**원격 액세스**)**를 선택합니다.

단계 **2** 원격 액세스 VPN 정책을 선택하고 **Edit(**편집**)**을 클릭합니다.

단계 **3** 편집할 클라이언트 프로파일을 포함하는 연결 프로파일을 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 **4** **Edit Group Policy(**그룹 정책 편집**)** > **AnyConnect** > **Profiles(**프로파일**)**를 클릭합니다.

단계 **5** 목록에서 클라이언트 프로파일 XML 파일을 선택하거나 **Add(**추가**)**를 클릭하여 새 클라이언트 프로파일을 추가합니다.

단계 **6** 그룹 정책, 연결 프로파일 및 Remote Access VPN 정책을 저장합니다.

단계 **7** 변경 사항을 구축하고

클라이언트 프로파일에 대한 변경 사항은 VPN 클라이언트가 Remote Access VPN 게이트웨이에 연결할 때 업데이트됩니다.

관련 항목

그룹 정책 개체 설정

Remote Access VPN 예시

사용자별 AnyConnect 대역폭을 제한하는 방법

이 섹션에서는 사용자가 Cisco AnyConnect VPN 클라이언트를 이용해 Firepower Threat Defense 원격 액세스 VPN 게이트웨이에 연결할 때, VPN 사용자가 사용하는 최대 대역폭을 제한하는 방법을 설명합니다. 단일 사용자 또는 사용자 그룹이 전체 리소스를 차지하지 않도록, Firepower Threat Defense에서 QoS(Quality of service)를 이용해 최대 대역폭을 제한할 수 있습니다. 이 구성을 이용하면 중요한 트래픽에 우선순위를 부여하고, 대역폭 독점을 방지하고, 네트워크를 관리할 수 있습니다. 트래픽이 최대 속도를 초과하면 Firepower Threat Defense에서 초과 트래픽을 취소합니다.

	수행해야 할 작업	추가 정보
1단계	영역을 만들고 설정합니다.	Active Directory 영역 생성 및 설정, 65 페이지.
2단계	새로 생성한 영역에서 사용 가능한 사용자 또는 그룹에 대한 QoS 정책 및 QoS 규칙을 생성합니다.	QoS 정책 및 규칙 생성, 66 페이지
3단계	원격 액세스 VPN 정책을 구성하고 사용자 인증을 위해 새로 생성한 영역을 선택합니다.	Remote Access VPN 정책 생성 또는 업데이트, 67 페이지
4단계	원격 액세스 VPN 정책을 구축합니다.	컨피그레이션 변경 사항 구축

Active Directory 영역 생성 및 설정

이 섹션에서는 영역을 생성하고, 활동을 모니터링할 VPN 사용자 및 사용자 그룹을 지정하는 방법을 설명합니다.

프로시저

단계 **1** Firepower Management Center 웹 인터페이스에서 **System(**시스템**)** > **Integration(**통합**)** > **Realms(**영역**)**를 선택합니다.

단계 **2** **New realm(**새 영역**)**을 클릭하고, 영역 상세정보를 지정한 다음 **OK(**확인**)**를 클릭합니다.

단계 **3** 표시되는 탭에 필요한 상세정보를 입력하고 **Save(**저장**)**를 클릭합니다.

- **Directory(**디렉터리**)** - 한 영역에 하나 이상의 디렉터리를 지정할 수 있으며, 이 경우 사용자 제어를 위해 각 도메인 컨트롤러는 영역의 **Directory(**디렉터리**)** 페이지에 나열된 순서에 따라 사용자 및 그룹 인증서에 맞게 쿼리됩니다.

  영역 디렉터리 설정의 내용을 참조하십시오.

- **Realm Configuration(**영역 구성**)** - 영역을 생성하는 동안 입력한 영역 설정을 업데이트할 수 있습니다.

- **User Download(**사용자 다운로드**)** - 사용자와 그룹을 Firepower Management Center에 대한 다운로드 대상에 추가하거나 대상에서 제외할 수 있습니다.

단계 **4** **State(**상태**)**를 오른쪽으로 밀어 사용자 제어용으로 영역을 사용할 수 있게 합니다. 영역 관리의 내용을 참조하십시오.

단계 **5** 다운로드를 클릭해 사용자와 사용자 그룹을 Firepower Management Center에 다운로드합니다. 의 내용을 참조하십시오.사용자 및 그룹 다운로드의 내용을 참조하십시오.

단계 **6** **Save(**저장**)**를 클릭합니다.

관련 항목

영역 생성

QoS 정책 및 규칙 생성

매니지드 디바이스의 속도 제한을 제어하기 위해 구축된 QoS 정책 영역을 선택해 QoS 정책을 생성하여 사용자나 사용자 그룹이 사용할 수 있는 VPN 대역폭을 제한할 수 있습니다. 각 QoS 정책은 여러 장치를 대상으로 할 수 있습니다. 각 디바이스에는 한 번에 하나의 QoS 정책을 구축할 수 있습니다.

프로시저

단계 **1** Firepower Management Center 웹 인터페이스에서 **Devices(**디바이스**)** > **QoS** > **New Policy(**새 정책**)**를 선택합니다.

단계 **2** **Name(**이름**)**을 입력하고 필요한 경우, **Description(**설명**)**을 입력합니다.

단계 **3** QoS 정책을 구축할 **Available Devices(**사용 가능한 디바이스**)**를 선택하고 **Add to Policy(**정책에 추가**)**를 클릭하거나, **Selected Devices(**선택한 디바이스**)**로 끌어다 놓습니다.

참고 원격 액세스 VPN 정책을 구축하려는 디바이스와 동일한 디바이스를 선택합니다. 정책을 구축하기 전에 디바이스를 할당해야 합니다.

단계 **4** QoS 정책 **Rules(**규칙**)**에서 **Add Rule(**규칙 추가**)**을 클릭합니다.

단계 **5** **Name(**이름**)**을 입력합니다.

단계 **6** 규칙 구성 요소를 구성합니다.

- **Enabled(**활성화**)** - 규칙이 Enabled(활성화) 상태인지 여부를 지정합니다.

- **Apply QoS On(QoS** 적용 켜기**)** - 대상 인터페이스 개체의 인터페이스 또는 소스 인터페이스 개체의 인터페이스 중 속도를 제한하려는 인터페이스를 선택합니다. 이때 선택은 생성된 인터페이스 제약(Any(모든)이 아닌)에 일치해야 합니다.
- **Traffic Limit Per Interface(**인터페이스별 트래픽 제한**)** - Mbit/초 단위로 다운로드 제한 용량 및 업로드 제한 용량을 입력합니다. Unlimited(무제한) 기본값은 해당 방향의 일치하는 트래픽의 속도 제한을 방지합니다.
- **Users(**사용자**)** - **Users(**사용자**)** 탭을 클릭하고 VPN 트래픽을 제한할 새로 생성한 영역 및 사용자를 선택합니다. 추가할 조건에 해당하는 다른 탭을 클릭합니다. Apply QoS On(QoS 적용)에 대한 선택에 해당하는 소스 또는 대상 인터페이스 조건을 구성해야 합니다.
- **Comments(**코멘트**)** - Comments(코멘트) 탭을 클릭하고, 코멘트를 추가하고, **OK(**확인**)**를 클릭합니다.

단계 **7** 규칙을 저장합니다.

정책 편집기에서 규칙 위치를 설정합니다. 이렇게 하려면 규칙을 클릭하여 끌거나 오른쪽 클릭 메뉴를 사용하여 잘라내고 붙여넣습니다. 규칙은 번호가 지정되며 1부터 시작합니다. 시스템은 오름차순 규칙 번호에 따라 하향식 순서로 트래픽이 규칙과 일치하는지를 확인합니다. 트래픽에 일치하는 첫 번째 규칙이 트래픽을 처리하는 규칙입니다. 규칙 순서가 올바르면 네트워크 트래픽 처리에 필요한 리소스가 줄어들면서 규칙 선점이 방지됩니다.

단계 **8** **Save**를 클릭하여 정책을 저장합니다.

관련 항목

QoS 정책 생성

QoS 정책을 사용한 속도 제한

Remote Access VPN 정책 생성 또는 업데이트

프로시저

단계 **1** Firepower Management Center 웹 인터페이스에서 **Devices(**디바이스**)**> **VPN** > **Remote Access(**원격 액세스**)**를 선택합니다.

단계 **2** 마법사를 사용하여 원격 액세스 VPN 정책을 생성합니다. 새로 생성한 영역을 인증 서버로 선택하거나 기존 원격 액세스 VPN 정책을 편집하고 다음을 수행합니다.

a) VPN 사용자에게 할당할 연결 프로파일을 선택하고 **Edit(**편집**)**을 클릭합니다.

b) **AAA** > **Authentication Method(**인증 방법**)** > **AAA or Certificate & AAA(AAA** 또는 인증서 및 **AAA)**를 선택합니다.

c) 필요한 영역을 인증 서버로 선택합니다.

d) 필요하다면 다른 연결 프로파일 옵션을 업데이트하고 연결 프로파일을 저장합니다.

단계 **3** 원격 액세스 VPN 정책에 필요한 구성을 완료하고 **Save(**저장**)**를 클릭합니다.

관련 항목

새 Remote Access VPN 연결 구성, 11 페이지
연결 프로파일 설정, 19 페이지

사용자 ID 기반 액세스 제어 규칙에 VPN ID를 사용하는 방법

	수행해야 할 작업	추가 정보
1단계	영역을 만들고 설정합니다.	Active Directory 영역 생성 및 설정, 65 페이지.
2단계	ID 정책을 생성하고 ID 규칙을 추가합니다.	ID 정책 및 ID 규칙 생성, 69 페이지.
3단계	ID 정책을 액세스 제어 정책과 연결합니다.	ID 정책을 액세스 제어 정책과 연결, 69 페이지
4단계	원격 액세스 VPN 정책을 구성하고 사용자 인증을 위해 새로 생성한 영역을 선택합니다.	Remote Access VPN 정책 생성 또는 업데이트, 67 페이지
5단계	원격 액세스 VPN 정책을 구축합니다.	컨피그레이션 변경 사항 구축

Active Directory 영역 생성 및 설정

이 섹션에서는 영역을 생성하고, 활동을 모니터링할 VPN 사용자 및 사용자 그룹을 지정하는 방법을 설명합니다.

프로시저

단계 **1** Firepower Management Center 웹 인터페이스에서 **System(**시스템**)** > **Integration(**통합**)** > **Realms(**영역**)**를 선택합니다.

단계 **2** **New realm(**새 영역**)**을 클릭하고, 영역 상세정보를 지정한 다음 **OK(**확인**)**를 클릭합니다.

단계 **3** 표시되는 탭에 필요한 상세정보를 입력하고 **Save(**저장**)**를 클릭합니다.

- **Directory(**디렉터리**)** - 한 영역에 하나 이상의 디렉터리를 지정할 수 있으며, 이 경우 사용자 제어를 위해 각 도메인 컨트롤러는 영역의 **Directory(**디렉터리**)** 페이지에 나열된 순서에 따라 사용자 및 그룹 인증서에 맞게 쿼리됩니다.

  영역 디렉터리 설정의 내용을 참조하십시오.

- **Realm Configuration(**영역 구성**)** - 영역을 생성하는 동안 입력한 영역 설정을 업데이트할 수 있습니다.

- **User Download(**사용자 다운로드**)** - 사용자와 그룹을 Firepower Management Center에 대한 다운로드 대상에 추가하거나 대상에서 제외할 수 있습니다.

단계 **4** **State(**상태**)**를 오른쪽으로 밀어 사용자 제어용으로 영역을 사용할 수 있게 합니다. 영역 관리의 내용을 참조하십시오.

단계 **5** 다운로드를 클릭해 사용자와 사용자 그룹을 Firepower Management Center에 다운로드합니다. 의 내용을 참조하십시오.사용자 및 그룹 다운로드의 내용을 참조하십시오.

단계 **6** **Save(**저장**)**를 클릭합니다.

관련 항목

영역 생성

ID 정책 및 ID 규칙 생성

ID 정책에는 트래픽과 관련된 영역 및 인증 방법에 따라 사용자 인증을 수행하는 ID 규칙이 포함됩니다. ID 규칙은 트래픽 집합을 영역 및 인증 방법(패시브 인증, 활성 인증, 인증 없음)과 연결합니다. 사용하려는 영역 및 인증 방법을 완전히 구성해야 ID 규칙에서 해당 영역과 방법을 호출할 수 있습니다.

프로시저

단계 **1** Firepower Management Center 웹 인터페이스에서 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Identity(ID)**를 선택하고 **New Policy(**새 정책**)**를 클릭합니다.

단계 **2** **Name(**이름**)**과 **Description(**설명**)**을 입력하고 **Save(**저장**)**를 클릭합니다.

단계 **3** 정책에 규칙을 추가하려면 **Add Rule(**규칙 추가**)**를 클릭하고 **Name(**이름**)**을 입력합니다.

단계 **4** 규칙이 **Enabled(**활성화**)** 상태인지 여부를 지정합니다.

단계 **5** 기존 카테고리에 규칙을 추가하려면 규칙을 **Insert(**삽입**)**할 위치를 나타냅니다. 새 카테고리를 추가하려면 **Add Category(**카테고리 추가**)**를 클릭합니다.

단계 **6** 목록에서 규칙 **Action(**작업**)**을 선택하고 원격 액세스 VPN에서 소스 인터페이스로 구성한 인터페이스를 선택합니다.

단계 **7** **Realms & Settings(**영역 및 설정**)**를 클릭하고, **Realms(**영역**)** 목록에서 ID 규칙에 대해 생성한 새 영역을 선택합니다. 원격 액세스 VPN 정책에서 사용자 인증을 위해 선택한 것과 같은 영역을 선택했는지 확인합니다.

단계 **8** 선택한 영역에서 있는 사용자의 기본 설정을 구성하고 기타 필요한 규칙 옵션을 선택합니다.

단계 **9** **Add(**추가**)**를 클릭하여 규칙을 저장한 다음 ID 정책을 저장합니다.

관련 항목

ID 정책 생성 및 관리

ID 정책을 액세스 제어 정책과 연결

원격 액세스 VPN 정책을 구축할 Firepower Threat Defense 디바이스에 구축한 액세스 제어 정책을 ID 정책과 연결해야 합니다.

프로시저

단계 **1** Firepower Management Center 웹 인터페이스에서 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Access Control(**액세스 제어**)**을 선택합니다.

단계 **2** 필요한 액세스 제어 정책을 선택하고 **Edit(**편집**)**을 클릭합니다.

단계 **3** 액세스 제어 정책 편집기에서 **Advanced(**고급**)**를 클릭합니다.

단계 **4** **Identity Policy Settings(ID** 정책 설정**)** 영역에서 수정( )을 클릭합니다.

보기 아이콘(보기 ( ))이 대신 표시되는 경우에는 설정이 상위 정책에서 상속되거나 설정을 수정할 권한이 없는 것입니다. 구성이 잠금 해제되어 있으면 **Inherit from base policy(**기본 정책에서 상속**)**의 선택을 취소하여 수정을 활성화합니다.

단계 **5** 드롭다운 목록에서 ID 정책을 선택합니다.

편집을 클릭하여 ID 정책을 수정할 수 있습니다.

단계 **6** **OK(**확인**)**를 클릭합니다.

단계 **7** **Save(**저장**)**를 클릭하여 액세스 제어 정책을 저장합니다.

관련 항목

ID 정책 생성 및 관리

Remote Access VPN 정책 생성 또는 업데이트

프로시저

단계 **1** Firepower Management Center 웹 인터페이스에서 **Devices(**디바이스**)**> **VPN** > **Remote Access(**원격 액세스**)**를 선택합니다.

단계 **2** 마법사를 사용하여 원격 액세스 VPN 정책을 생성합니다. 새로 생성한 영역을 인증 서버로 선택하거나 기존 원격 액세스 VPN 정책을 편집하고 다음을 수행합니다.

a) VPN 사용자에게 할당할 연결 프로파일을 선택하고 **Edit(**편집**)**을 클릭합니다.

b) **AAA** > **Authentication Method(**인증 방법**)** > **AAA or Certificate & AAA(AAA** 또는 인증서 및 **AAA)**를 선택합니다.

c) 필요한 영역을 인증 서버로 선택합니다.

d) 필요하다면 다른 연결 프로파일 옵션을 업데이트하고 연결 프로파일을 저장합니다.

단계 **3** 원격 액세스 VPN 정책에 필요한 구성을 완료하고 **Save(**저장**)**를 클릭합니다.

관련 항목

새 Remote Access VPN 연결 구성, 11 페이지
연결 프로파일 설정, 19 페이지

AnyConnect 관리 VPN 터널 구성

관리 VPN 터널은 VPN 사용자가 VPN에 연결하지 않고도 클라이언트 시스템의 전원을 켤 때마다 회사 네트워크에 대한 연결을 제공합니다. 이를 통해 조직은 소프트웨어 패치 및 업데이트를 통해 엔드포인트를 최신 상태로 유지할 수 있습니다. 사용자 시작 VPN 터널이 설정되면 관리 터널의 연결이 끊어집니다.

이 섹션에서는 FTD에서 AnyConnect 관리 VPN 터널을 구성하는 방법에 대해 설명합니다. FMC 웹 인터페이스를 사용하여 FTD에서 AnyConnect 관리 터널을 구성하려면 다음 설정이 필요합니다.

- 인증서 기반 인증 및 그룹 URL이 있는 연결 프로파일
- **AnyConnect** 관리 **VPN** 프로파일 파일, 필요한 경우 그룹 URL 및 백업 서버로 서버를 구성했습니다.
- 관리 VPN 프로파일이 포함된 그룹 정책, 명시적으로 포함된 네트워크가 포함된 스플릿 터널링, 클라이언트 바이 패스 프로토콜, 배너 없음

AnyConnect 관리 VPN 터널을 구성하는 자세한 지침은 FTD에서 AnyConnect 관리 VPN 터널 구성, 72 페이지의 내용을 참조하십시오.

AnyConnect 관리 VPN 터널 요구 사항 및 사전 요건

소프트웨어 및 설정 요구 사항

FMC 웹 인터페이스를 통해 FTD를 사용하여 AnyConnect 관리 터널을 설정하기 전에 다음 사항을 확인하십시오.

- FTD 및 FMC 버전 6.7.0 이상을 사용하고 있는지 확인합니다.
- AnyConnect VPN Webdeploy 패키지 4.7 이상을 다운로드하여 FTD 원격 액세스 VPN에 업로드합니다.
- 인증서 인증이 연결 프로파일에 설정되어 있는지 확인합니다.
- 그룹 정책에 배너가 설정되어 있지 않은지 확인합니다.
- 관리 터널 그룹 정책에서 스플릿 터널링 설정을 확인합니다.

인증서 요구 사항

- FTD에는 원격 액세스 VPN에 대한 유효한 ID 인증서가 있어야 하며, 로컬 인증 기관(CA)의 루트 인증서가 FTD에 있어야 합니다.
- 관리 VPN 터널에 연결하는 엔드포인트에는 유효한 ID 인증서가 있어야 합니다.
- FTD의 ID 인증서에 대한 CA 인증서는 엔드포인트에 설치해야 하며, 엔드포인트에 대한 CA 인증서는 FTD에 설치해야 합니다.

- 동일한 로컬 CA에서 발급한 ID 인증서가 머신 저장소에 있어야 합니다.

  Windows의 경우에는 인증서 저장소고, macOS의 경우에는 시스템 키체인입니다.

AnyConnect 관리 VPN 터널의 제한 사항

- AnyConnect 관리 VPN 터널은 인증서 인증만 지원하며 AAA 기반 인증은 지원하지 않습니다.
- 공용 또는 프라이빗 프록시 설정은 지원되지 않습니다.
- 관리 VPN 터널이 연결되어 있으면 AnyConnect 클라이언트 업그레이드 및 AnyConnect 모듈 다운로드가 지원되지 않습니다.

FTD에서 AnyConnect 관리 VPN 터널 구성

프로시저

단계 **1** 마법사를 사용하여 원격 액세스 **VPN** 정책을 생성:

원격 액세스 VPN 구성에 대한 자세한 내용은 새 Remote Access VPN 연결 구성, 11 페이지을 참조하십시오.

단계 **2** 관리 **VPN** 터널에 대한 연결 프로파일 설정을 구성:

참고 AnyConnect 관리 VPN 터널에만 사용할 새 연결 프로파일을 생성하는 것이 좋습니다.

a) 생성한 원격 액세스 VPN 정책을 수정합니다.
b) 관리 VPN 터널에 사용할 연결 프로파일을 선택하고 수정합니다.
c) **AAA** > **Authentication Method(**인증 방법**)**을 클릭하고 **Client Certificate Only(**클라이언트 인증서만**)**를 선택합니다. 필요에 따라 인증 및 계정 설정을 구성합니다.
d) 연결 프로파일의 **Aliases(**별칭**)** 탭을 클릭합니다.
e) 연결 프로파일에 대해 URL 별칭 아래에서 **Add(+)(**추가**(+))** 그리고 **URL Alias(URL** 별칭**)**를 클릭합니다.
f) **Enabled(**활성화됨**)**를 클릭하여 URL을 활성화합니다.
g) **OK(**확인**)**를 클릭한 다음 **Save(**저장**)**를 클릭하여 연결 프로파일 설정을 저장합니다.

연결 프로파일 설정에 대한 자세한 내용은 연결 프로파일 설정, 19 페이지의 내용을 참조하십시오.

단계 **3** **AnyConnect** 프로파일 편집기를 사용하여 관리 터널 프로파일을 생성:

a) **Cisco** 소프트웨어 다운로드 센터에서 AnyConnect VPN 관리 터널 독립형 프로파일 편집기를 아직 다운로드하지 않은 경우 다운로드합니다.
b) VPN 사용자에 대한 필수 설정으로 관리 터널 프로파일을 생성하고 파일을 저장합니다.
c) 연결 프로파일에서 구성한 그룹 URL을 사용하여 서버 목록의 서버를 구성합니다.

프로파일 편집기를 사용한 관리 프로파일 생성에 대한 자세한 내용은 *Cisco AnyConnect Secure Mobility Client Administrator Guide*를 참조하십시오.

단계 **4** 관리 터널 개체 생성:

a) Firepower Management Center 웹 인터페이스에서 **Object(**개체**)** > **Object Management(**개체 관리**)** > **VPN** > **AnyConnect File(AnyConnect** 파일**)**로 이동합니다
b) **Add AnyConnect File(AnyConnect** 파일 추가**)**을 클릭합니다.
c) AnyConnect 파일의 이름을 지정합니다.
d) **Browse(**찾아보기**)**를 클릭하고 저장한 관리 터널 프로파일 파일을 선택합니다.
e) **File Type(**파일 유형**)** 드롭 다운을 클릭하고 **AnyConnect Management VPN Profile (AnyConnect** 관리 **VPN** 프로필**)**을 선택합니다.
f) **Save(**저장**)**를 클릭합니다.

참고 또한 그룹 정책에 대한 AnyConnect 설정을 생성하거나 업데이트할 때 관리 터널 개체를 생성합니다. 그룹 정책 AnyConnect 옵션의 내용을 참조하십시오.

단계 **5** 관리 프로파일을 그룹 정책과 연결하고 그룹 정책 설정을 구성:

관리 터널 VPN 연결에 사용되는 연결 프로파일과 연결된 그룹 정책에 관리 VPN 프로파일을 추가해야 합니다. 사용자가 연결하면 그룹 정책에 이미 매핑된 사용자 VPN 프로파일과 함께 관리 VPN 프로파일이 다운로드되어 관리 VPN 터널 기능을 활성화합니다.

주의 **No Banner(**배너 없음**)**: 그룹 정책 설정에 배너가 구성되어 있지 않은지 확인합니다. **Group Policy(**그룹 정책**)** > **General Settings(**일반 설정**)** > **Banner(**배너**)**에서 배너 설정을 확인할 수 있습니다.

a) 관리 VPN 터널 용으로 생성한 연결 프로파일을 수정합니다.
b) **Edit Group Policy(**그룹 정책 편집**)** > **AnyConnect** > **Management Profiles(**관리 프로파일**)**를 클릭합니다.
c) **Management VPN Profile(**관리 **VPN** 프로파일**)** 드롭 다운을 클릭하고 생성한 관리 프로파일 파일 개체를 선택합니다.

참고 +를 클릭하고 새 AnyConnect 관리 VPN 프로파일 개체를 추가할 수도 있습니다.

d) **Save(**저장**)**를 클릭합니다.

단계 **6** 그룹 정책에서 스플릿 터널링 구성:

a) **Edit Group Policy(**그룹 정책 편집**)** > **General(**일반**)** > **Split Tunneling(**스플릿 터널링**)**을 클릭합니.
b) IPv4 또는 IPv6 스플릿 터널링 드롭 다운에서 **Tunnel networks specified below(**아래 지정된 터널 네트워크**)**를 선택합니다.
c) 스플릿 터널 네트워크 목록 유형, 즉 **Standard Access List(**표준 액세스 목록**)** 또는 **Extended Access List(**확장 액세스 목록**)**를 선택한 다음 관리 VPN 터널을 통한 트래픽을 허용하는 데 필요한 액세스 목록을 선택합니다.
d) 스플릿 터널 설정을 저장하려면 **Save(**저장**)**를 클릭합니다.

AnyConnect 맞춤형 속성

AnyConnect 관리 VPN 터널에는 기본적으로 스플릿에 터널링 구성이 포함되어야 합니다. 모든 터널링을 위해 스플릿 터널링이 포함된 관리 VPN 터널을 구축하도록 그룹 정책에서 AnyConnect 맞춤 속성을 구성하는 경우 FMC 6.7 웹 인터페이스가 AnyConnect 맞춤 속성을 지원하지 않으므로 FlexConfig를 사용하여 해당 구성을 수행할 수 있습니다.

다음은 AnyConnect 맞춤 속성에 대한 명령 예입니다.

```
webvpn
 anyconnect-custom-attr ManagementTunnelAllAllowed description ManagementTunnelAllAllowed
anyconnect-custom-data ManagementTunnelAllAllowed true true
group-policy MGMT_Tunnel attributes
 anyconnect-custom ManagementTunnelAllAllowed value true
```

단계 **7** 원격 액세스 **VPN** 정책 구축**,** 확인 및 모니터링:

a) 관리 VPN 터널 구성을 FTD에 구축합니다.

참고 클라이언트 시스템은 관리 터널 VPN 프로파일을 클라이언트 머신에 다운로드하려면 FTD 원격 액세스 VPN에 한 번 연결해야 합니다.

b) **AnyConnect Secure Mobility Client** > **VPN** > **Statistics(**통계**)**에서 AnyConnect 관리 VPN 터널을 확인할 수 있습니다.

show vpn-sessiondb anyconnect 명령을 사용하여 FTD 명령 프롬프트에서 관리 VPN 세션 세부 정보를 확인할 수도 있습니다.

c) FMC 웹 인터페이스에서 **Analysis(**분석**)**를 클릭하여 관리 터널 세션 정보를 확인합니다.

관련 항목

연결 프로파일 설정, 19 페이지
FTD 그룹 정책 개체

원격 액세스 VPN 히스토리

기능	버전	세부 사항
다중 인증서 인증	7.0	Firepower Management Center 다중 인증서 기반 인증을 통해 FTD는 사용자의 ID 인증서를 인증하는 것 외에도 머신 또는 디바이스 인증서를 검증, 즉 디바이스가 기업 발행 디바이스라는 점을 보장하고 AnyConnect 클라이언트를 사용하여 RAVPN 액세스를 허용합니다.

기능	버전	세부 사항
VPN 로드 밸런싱	7.0	VPN로드 밸런싱은 둘 이상의 디바이스를 논리적으로 그룹화하고 처리량 및 기타 트래픽 매개변수를 고려하지 않고 그룹화된 디바이스간에 원격 액세스 VPN 세션을 동일하게 분산합니다.
AnyConnect 맞춤형 속성	7.0	Firepower Management Center AnyConnect 맞춤형 속성을 지원하며, FTD에서 이러한 기능에 대한 하드 코딩된 지원을 추가하지 않고도 AnyConnect 클라이언트 기능을 구성할 수 있는 인프라를 제공합니다.
선택적 정책 구축	7.0	이제 구축 중에 원격 액세스 VPN 및 사이트 대 사이트 VPN 구성에 대한 변경 사항을 포함하거나 제외하도록 선택할 수 있습니다.
AnyConnect 모듈 구성 지원	6.7	Firepower Management Center 이제 추가 보안을 위해 AnyConnect 모듈 및 프로파일을 구성할 수 있습니다.
LDAP 권한 부여 지원	6.7	Firepower Management Center를 사용하여 원격 액세스 VPN에 대한 LDAP 권한 부여를 구성할 수 있습니다.
원격 액세스 VPN에 대한 SAML SSO(Single Sign-On) 지원	6.7	원격 액세스 VPN에 대한 인증서버로 SAML 2.0 서버를 구성할 수 있습니다.
AnyConnect 관리 VPN 터널 지원	6.7	FTD 원격 액세스 VPN은 VPN 사용자가 VPN에 연결하지 않고도 회사 엔드포인트의 전원을 켤 때 엔드포인트에 대한 VPN 연결을 허용하는 AnyConnect 관리 VPN 터널 구성을 지원합니다.
DTLS(Datagram Transport Layer Security) 1.2 지원	6.6	DTLS 1.2는 이제 기본 SSL 암호 그룹의 일부이며 TLS 1.2와 함께 구성할 수 있습니다.