원격 액세스 VPN

원격 액세스 VPN(Virtual Private Network)을 사용하면 개별 사용자가 인터넷에 연결된 컴퓨터 또는 기타 지원되는 iOS 또는 Android 디바이스를 사용하여 원격 위치에서 네트워크에 연결할 수 있습니다. 따라서 모바일 근무자가 홈 네트워크 또는 공개 Wi-Fi 네트워크 등에서 연결할 수 있습니다.

다음 주제에서는 네트워크용으로 원격 액세스 VPN을 구성하는 방법을 설명합니다.

- 원격 액세스 VPN 개요, 1 페이지
- 원격 액세스 VPN에 대한 라이선싱 요구 사항, 8 페이지
- 원격 액세스 VPN에 대한 지침 및 제한 사항, 8 페이지
- 원격 액세스 VPN 구성, 9 페이지
- 원격 액세스 VPN 컨피그레이션 관리, 15 페이지
- 원격 액세스 VPN 모니터링, 31 페이지
- 원격 액세스 VPN 트러블슈팅, 32 페이지
- 원격 액세스 VPN의 예시, 34 페이지

원격 액세스 VPN 개요

device manager를 사용하여 Secure Client 소프트웨어를 통한 원격 액세스 VPN over SSL을 구성할 수 있습니다.

Secure Client는 threat defense 디바이스와 SSL VPN 연결을 협상할 때 TLS(Transport Layer Security: 전송 계층 보안) 또는 DTLS(Datagram Transport Layer Security: 데이터그램 전송 계층 보안)를 사용하여 연결합니다. DTLS는 일부 SSL 연결에서 발생하는 레이턴시 및 대역폭 문제를 방지하고 패킷 지연에 민감한 실시간 애플리케이션의 성능을 높입니다. 클라이언트 및 threat defense 디바이스에서는 사용할 TLS/DTLS 버전을 협상합니다. 클라이언트가 지원하는 경우 DTLS가 사용됩니다.

디바이스 모델별 최대 동시 VPN 세션

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 1010	75
Firepower 1120	150
Firepower 1140	400
Firepower 2110	1500
Firepower 2120	3500
Firepower 2130	7500
Firepower 2140	10,000
Secure Firewall 3110	1500
Secure Firewall 3120	3500
Secure Firewall 3130	7500
Secure Firewall 3140	10,000
Firepower 4100 Series, 모든 모델	10,000
Firepower 9300 Appliance, 모든 모델	20,000
Threat Defense Virtual: FTDv5	50
Threat Defense Virtual: FTDv10, FTDv20, FTDv30	250
Threat Defense Virtual: FTDv50	750
Threat Defense Virtual: FTDv100	10,000
ISA 3000	25

Secure Client 소프트웨어 다운로드

원격 액세스 VPN를 구성하려면 먼저 워크스테이션에 Secure Client 소프트웨어를 다운로드해야 합니다. VPN를 정의할 때 이러한 패키지를 업로드해야 합니다.

최신 기능, 버그 수정 및 보안 패치를 적용하려면 최신 Secure Client 버전을 다운로드해야 합니다. threat defense 디바이스에서 패키지를 정기적으로 업데이트합니다.

참고 운영 체제(Windows, Mac, Linux)별로 Secure Client 패키지를 하나씩 업로드할 수 있습니다. 지정된 OS 유형의 여러 버전을 업로드할 수는 없습니다.

Secure Client 소프트웨어 패키지는 software.cisco.com에서 다운로드합니다. 클라이언트의 "전체 설치 패키지" 버전을 다운로드해야 합니다.

사용자가 Secure Client 소프트웨어를 설치할 수 있는 방법

VPN 연결을 완료하려면 사용자가 Secure Client 소프트웨어를 설치해야 합니다. 기존 소프트웨어 배포 방법을 사용하여 소프트웨어를 직접 설치할 수 있습니다. 또는 사용자가 threat defense 디바이스에서 Secure Client를 직접 설치하게 할 수도 있습니다.

소프트웨어를 설치하려면 사용자에게 워크스테이션에 대한 관리자 권한이 있어야 합니다.

Secure Client를 설치하고 나면 시스템에 새 Secure Client 버전을 업로드하는 경우 사용자가 다음 번에 VPN에 연결할 때 Secure Client가 새 버전을 탐지합니다. 그러면 시스템에서 업데이트된 클라이언트 소프트웨어를 다운로드하여 설치하라는 메시지를 사용자에게 자동으로 표시합니다. 이러한 자동화로 인해 개발자와 고객을 위한 소프트웨어 배포를 간소화할 수 있습니다.

사용자가 threat defense 디바이스에서 소프트웨어를 처음 설치하도록 하려면 사용자에게 다음 단계를 수행하도록 하십시오.

참고 안드로이드 및 iOS 사용자는 해당 앱 스토어에서 Secure Client를 다운로드해야 합니다.

프로시저

단계 **1** 웹 브라우저를 사용하여 **https://***ravpn-address*를 엽니다. 여기서 *ravpn-address*는 VPN 연결을 허용할 외부 인터페이스의 IP 주소 또는 호스트 이름입니다.

원격 액세스 VPN을 구성할 때 이 인터페이스를 식별합니다. 시스템에서 사용자에게 로그인하라는 메시지를 표시합니다.

원격 액세스 VPN 연결용 포트를 변경한 경우 URL에 맞춤형 포트를 포함해야 합니다. 예를 들어 포트를 4443으로 변경한 경우 https://ravpn.example.com:4443과 같습니다.

단계 **2** 사이트에 로그인합니다.

사용자는 원격 액세스 VPN용으로 구성된 디렉터리 서버를 사용하여 인증을 합니다. 로그인이 성공해야 설치를 계속할 수 있습니다.

로그인이 성공하면 시스템은 사용자에게 필요한 Secure Client 버전이 이미 있는지를 확인합니다. 사용자 컴퓨터에 Secure Client가 없거나 클라이언트가 하위 레벨인 경우에는 시스템에서 Secure Client 소프트웨어 설치를 자동으로 시작합니다.

설치가 완료되면, Secure Client에서 원격 액세스 VPN 연결을 완료합니다.

RADIUS 및 그룹 정책을 이용한 사용자 권한 및 속성 제어

외부 RADIUS 서버 또는 threat defense 디바이스에 정의된 그룹 정책에서 RA VPN 연결에 사용자 인증 속성(사용자 자격 또는 권한이라고도 함)을 적용할 수 있습니다. threat defense 디바이스에서 그룹 정책에 컨피그레이션된 속성과 충돌하는 속성을 AAA 서버로부터 수신하는 경우, AAA 서버에서 오는 속성이 항상 우선 적용됩니다.

threat defense 디바이스에서는 다음 순서로 속성을 적용합니다.

1. 외부 AAA 서버에 정의된 사용자 속성 - 인증 및/또는 권한 부여가 성공적으로 수행되면 서버에서 이 속성을 반환합니다.
2. threat defense 디바이스에 컨피그레이션된 그룹 정책 - RADIUS 서버에서 사용자에 대해 RADIUS CLASS 속성 IETF-Class-25(OU=group-policy) 값을 반환하면 threat defense 디바이스에서는 해당 사용자를 이름이 같은 그룹 정책에 배치하고 서버에서 반환하지 않은 그룹 정책의 모든 속성을 적용합니다.
3. 연결 프로파일에서 할당한 그룹 정책 - 연결 프로파일에는 연결을 위한 예비 설정이 있으며 인증 전에 사용자에게 적용되는 기본 그룹 정책을 포함합니다. threat defense 디바이스에 처음 접속하는 모든 사용자는 이 그룹에 속하며, 이를 통해 AAA 서버에서 반환한 사용자 속성 또는 사용자에게 할당된 그룹 정책에 없는 모든 속성을 제공합니다.

Threat Defense 디바이스에서는 벤더 ID가 3076인 RADIUS 속성을 지원합니다. 사용하는 RADIUS 서버에 이러한 속성이 정의되지 않은 경우, 수동으로 정의해야 합니다. 특성을 정의하려면 특성 이름 또는 번호, 유형, 값 및 공급업체 코드(3076)를 사용합니다.

다음 주제에서는 값이 RADIUS 서버에 정의되어 있는지 또는 값이 시스템에서 RADIUS 서버로 전송하는 값인지 여부에 따라 지원되는 속성을 설명합니다.

RADIUS 서버로 전송되는 속성

RADIUS 속성 146 및 150은 인증 및 권한 부여 요청을 위해 threat defense 디바이스에서 RADIUS 서버로 전송됩니다. 다음 속성 모두 계정 관리 시작, 중간 업데이트, 중단 요청을 위해 threat defense 디바이스에서 RADIUS 서버로 전송됩니다.

표 *1: Threat Defense*에서 *RADIUS*로 전송하는 속성

특성	속성 번호	구문, 유형	단일 또는 다중 값 지정	설명 또는 값
클라이언트 유형	150	정수	단일	VPN에 접속 중인 클라이언트의 유형: 2 = Secure Client SSL VPN
세션 유형	151	정수	단일	연결 유형: 1 = Secure Client SSL VPN
터널 그룹 이름	146	문자열	단일	threat defense 디바이스에 정의된 대로 세션을 설정하는 데 사용된 연결 프로파일의 이름입니다. 이름은 1~253자일 수 있습니다.

RADIUS 서버에서 수신한 속성

다음 사용자 권한 부여 속성은 RADIUS 서버에서 threat defense 디바이스로 전송됩니다.

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

특성	속성 번호	구문, 유형	단일 또는 다중 값 지정	설명 또는 값
Access-List-Inbound	86	문자열	단일	액세스 목록(Acess-List) 속성 둘 다 threat defense 디바이스에 컨피그레이션된 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(threat defense 디바이스로 들어가는 트래픽) 또는 아웃바운드(threat defense 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 threat defense 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.
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 threat defense 디바이스의 하위 인터페이스에 이 VLAN을 컨피그레이션해야 합니다.

이중 인증

RA VPN에 대한 이중 인증을 컨피그레이션할 수 있습니다. 이중 인증의 경우, 사용자는 사용자 이름 및 정적 암호뿐 아니라 RSA 토큰 또는 듀오 암호와 같은 추가 항목도 제공해야 합니다. 이중 인증이 두 번째 인증 소스를 사용하는 것과 다른 점은 두 가지 인증 요소가 기본 인증 소스와 연결된 RSA/듀오 서버와의 관계에 따라 단일 인증 소스에서 컨피그레이션된다는 것입니다. 보조 인증 소스로 Duo LDAP 서버를 구성하는 Duo LDAP은 예외입니다.

시스템은 이중 인증 프로세스에서 첫 번째 요소인 RADIUS 또는 AD 서버와 함께 두 번째 요소에 대해 모바일로 푸시된 RSA 토큰 및 듀오 암호에 대한 테스트를 마쳤습니다.

RSA 이중 인증

다음 접근 방식 중 하나를 사용하여 RSA를 컨피그레이션할 수 있습니다. RSA 측 컨피그레이션에 대한 내용은 RSA 문서를 참조하십시오.

- device manager에서 RADIUS 서버를 RSA 서버로 직접 정의하고 RA VPN에서 서버를 기본 인증 소스로 사용합니다.

  이 접근 방식을 사용하는 경우, 사용자는 RSA RADIUS 서버에 컨피그레이션된 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.

- 직접 통합을 지원하는 RADIUS 또는 AD 서버와 RSA 서버를 통합하고 비 RSA RADIUS 또는 AD 서버를 기본 인증 소스로 사용하도록 RA VPN을 컨피그레이션합니다. 이 경우, RADIUS/AD 서버에서는 RSA SDI를 사용하여 클라이언트와 RSA 서버 간의 이중 인증을 위임하고 오케스트레이션합니다.

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

  이 컨피그레이션에서는 비 RSA RADIUS 서버도 권한 부여 서버 및 과금 서버(선택 사항)로 사용합니다.

RADIUS를 사용하는 Duo 이중 인증

듀오 RADIUS 서버를 기본 인증 소스로 컨피그레이션할 수 있습니다. 이 접근 방식에서는 듀오 RADIUS 인증 프록시를 사용합니다.

듀오를 컨피그레이션하는 세부 절차는 https://duo.com/docs/cisco-firepower의 내용을 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 사용하는 경우, 사용자는 듀오 인증 프록시 및 연결된 RADIUS/AD 서버 둘 다에 컨피그레이션된 사용자 이름과 RADIUS/AD 서버에 컨피그레이션된 사용자 이름의 암호(다음 듀오 코드 중 하나가 바로 뒤에 나옴)를 사용해 인증해야 합니다.

- *Dou-passcode*. 예: *my-password*,**12345**.
- **push**. 예: *my-password*,**push**. **push(**푸시**)**를 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**. 전화를 사용해 듀오에게 전화 콜백 인증을 수행하도록 지시합니다.

사용자 이름 및 암호가 인증되면 듀오 인증 프록시에서는 듀오 클라우드 서비스에 접속합니다. 이를 통해 요청이 유효한 컨피그레이션 프록시 디바이스에서 발신되었는지 확인한 다음, 지시받은 대로 사용자의 모바일 디바이스에 임시 암호를 푸시합니다. 사용자가 이 암호를 수락하면 듀오에서 세션을 인증된 것으로 표시하고 RA VPN이 설정됩니다.

LDAP를 사용하는 Duo 이중 인증

기본 소스로 Microsoft AD(Microsoft Active Directory) 또는 RADIUS 서버를 함께 사용하여 Duo LDAP 서버를 보조 인증 소스로 사용할 수 있습니다. Duo LDAP를 사용하는 경우 보조 인증에서는 Duo 암호, 푸시 알림 또는 전화 통화를 사용하여 기본 인증을 검증합니다.

threat defense 디바이스에서는 TCP/636 포트를 통해 LDAPS를 사용하여 Duo LDAP과 통신합니다.

Duo LDAP 서버에서는 인증 서비스만 제공하며, ID 서비스는 제공하지 않습니다. 따라서, Duo LDAP를 기본 인증 소스로 사용하는 경우, 어떠한 대시보드에도 RA VPN 연결과 관련된 사용자 이름이 표시되지 않으며 이러한 사용자에 대한 액세스 제어 규칙을 작성할 수 없게 됩니다.

이 접근 방식을 사용하는 경우 사용자는 RADIUS/AD 서버 및 Duo LDAP 서버에 구성된 사용자 이름을 사용하여 인증해야 합니다. Secure Client에서 로그인하라는 프롬프트가 표시되면 사용자는 기본 **Password(**비밀번호**)** 필드에 RADIUS/AD 비밀번호를 입력하고 **Secondary Password(**보조 비밀번호**)**에는 Duo를 사용하여 인증하기 위해 다음 중 하나를 입력합니다. 자세한 내용은 https://guide.duo.com/anyconnect를 참조하십시오.

- *Duo passcode(Duo* 암호*)* - Duo Mobile을 통해 생성되었거나 SMS를 통해 전송되었거나 하드웨어 토큰에 의해 생성되었거나 관리자가 제공한 암호를 사용하여 인증합니다. 1234567을 예로 들 수 있습니다.
- **push(**푸시**)** - Duo Mobile 앱을 설치하고 활성화한 경우 전화기에 로그인 요청을 푸시합니다. 요청을 검토하고 **Approve(**승인**)**를 눌러 로그인합니다.
- **phone(**전화기**)** - 전화기 콜백을 사용하여 인증합니다.
- **sms** - 텍스트 메시지로 Duo 암호를 요청합니다. 로그인 시도가 실패합니다. 새 암호를 사용하여 다시 로그인합니다.

Duo LDAP 사용에 대한 자세한 설명과 예는 Duo LDAP를 사용하여 이중 인증을 구성하는 방법, 44 페이지의 내용을 참조하십시오.

원격 액세스 VPN에 대한 라이선싱 요구 사항

기본 디바이스 라이선스가 내보내기 요구 사항을 충족해야 원격 액세스 VPN을 구성할 수 있습니다. 디바이스를 등록할 때는 내보내기 제어 기능에 대해 활성화된 Smart Software Manager 어카운트를 사용하여 등록을 수행해야 합니다. 또한, 평가 라이선스로는 기능을 구성할 수 없습니다.

그뿐만 아니라 AnyConnect Plus, AnyConnect Apex 또는 AnyConnect VPN Only 원격 액세스 VPN 라이선스도 구매하고 활성화해야 합니다. 이러한 라이선스는 threat defense 디바이스에 대해 동일하게 처리되지만, ASA 소프트웨어 기반 헤드엔드와 함께 사용할 때는 각기 다른 기능 집합을 허용하도록 설계되었습니다.

라이선스를 활성화하려면 디바이스 > 스마트 라이선스 > 컨피그레이션 보기를 선택한 다음 RA VPN 라이선스 그룹에서 적절한 라이선스를 선택합니다. Smart Software Manager 어카운트에 사용 가능한 라이선스가 있어야 합니다. 라이선스를 활성화하는 방법에 대한 자세한 내용은 선택 가능한 라이선스 활성화 또는 비활성화를 참조하십시오.

자세한 내용은 *Cisco AnyConnect* 주문 가이드, http://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdf를 참조하십시오. http://www.cisco.com/c/en/us/products/security/anyconnect-secure-mobility-client/datasheet-listing.html에서는 다른 데이터 시트도 제공합니다.

원격 액세스 VPN에 대한 지침 및 제한 사항

RA VPN을 구성하는 경우 다음 지침과 제한 사항에 유의하십시오.

- 동일한 TCP 포트에 대한 동일한 인터페이스에서 device manager 액세스(관리 액세스 목록의 HTTPS 액세스)와 원격 액세스 SSL VPN을 모두 구성할 수는 없습니다. 예를 들어, 외부 인터페이스에서 원격 액세스 SSL VPN을 구성하는 경우, 포트 443에서 HTTPS 연결에 대한 외부 인터페이스도 열 수 없습니다. 동일한 인터페이스에서 두 기능을 모두 구성하는 경우 충돌을 방지하기 위해 이러한 서비스 중 하나 이상에 대해 HTTPS 포트를 변경해야 합니다.
- RA VPN 외부 인터페이스는 전역 설정입니다. 서로 다른 인터페이스에서 별도의 연결 프로파일을 구성할 수 없습니다.
- NAT 규칙의 소스 주소와 원격 액세스 VPN 주소 풀에서는 겹치는 주소를 사용할 수 없습니다.
- RADIUS 및 RSA 토큰을 사용하여 이중 인증을 구성하는 경우, 기본 인증 시간 제한 값인 12초는 너무 짧아 대부분의 경우 성공적인 인증을 허용하기 어렵습니다. 클라이언트 프로파일 구성 및 업로드, 10 페이지의 설명에 따라 맞춤형 Secure Client 프로파일을 생성한 다음 RA VPN 연결 프로파일에 적용하여 인증 시간 제한 값을 늘릴 수 있습니다. 사용자가 인증을 한 다음 RSA 토큰을 붙여넣고 토큰의 라운드트립을 확인할 수 있는 시간이 충분하도록 인증 시간 제한을 60초 이상으로 설정하는 것이 좋습니다.

원격 액세스 VPN 구성

클라이언트에 대한 원격 액세스 VPN을 활성화하려면 여러 개의 개별 항목을 구성해야 합니다. 다음 절차에서는 엔드 투 엔드 프로세스에 대해 설명합니다.

프로시저

단계 1 라이선스를 구성합니다.

두 개의 라이선스를 활성화해야 합니다.

- 디바이스를 등록할 때는 내보내기 제어 기능에 대해 활성화된 Smart Software Manager 어카운트를 사용하여 등록을 수행해야 합니다. 기본 라이선스가 내보내기 제어 요구사항을 충족해야 원격 액세스 VPN을 구성할 수 있습니다. 또한, 평가 라이선스로는 기능을 구성할 수 없습니다. 디바이스를 등록하는 절차는 디바이스 등록를 참조하십시오.
- 원격 액세스 VPN 라이선스. 자세한 내용은 원격 액세스 VPN에 대한 라이선싱 요구 사항, 8 페이지를 참조해 주십시오. 라이선스를 활성화하려면 선택 가능한 라이선스 활성화 또는 비활성화를 참조하십시오.

단계 2 인증서를 구성합니다.

클라이언트와 디바이스 간의 SSL 연결을 인증하려면 인증서가 필요합니다. VPN용으로 사전 정의된 DefaultInternalCertificate를 사용할 수도 있고 인증서를 직접 생성할 수도 있습니다.

인증에 사용되는 디렉터리 영역에 대해 암호화된 연결을 사용하는 경우에는 신뢰할 수 있는 CA 인증서를 업로드해야 합니다.

인증서 및 인증서를 업로드하는 방법에 관한 자세한 내용은 인증서 구성를 참조하십시오.

단계 3 (선택 사항). TLS/SSL 설정 지정.

기본적으로 시스템은 원격 사용자가 지원하는 모든 TLS 버전 및 암호화 암호를 사용하여 원격 액세스 VPN에 연결할 수 있도록 허용합니다. 하지만 허용된 TLS/DTLS 버전, 암호 및 Diffie-Hellman 그룹을 제한하여 더 안전한 연결을 적용할 수 있습니다. TLS / SSL 암호 설정 설정의 내용을 참조하십시오.

단계 4 (선택 사항). 클라이언트 프로파일 구성 및 업로드, 10 페이지에 전달하는 고성능 고속 어플라이언스입니다.

단계 5 원격 사용자 인증에 사용되는 ID 소스를 구성합니다.

원격 액세스 VPN 로그인이 허용되는 사용자 어카운트에 대해 다음 소스를 사용할 수 있습니다. 아니면 인증을 위해 클라이언트 인증서를 단독으로 또는 ID 소스와 함께 사용할 수 있습니다.

- AD(Active Directory) ID 영역 - 기본 인증 소스로 사용됩니다. AD(Active Directory) 서버에서 사용자 어카운트가 정의됩니다. AD ID 영역 구성를 참조하십시오.
- RADIUS 서버 그룹 - 기본 또는 보조 인증 소스로서, 권한 부여 및 계정 관리를 위한 것입니다. RADIUS 서버 그룹 구성를 참조하십시오.

- LocalIdentitySource - 기본 또는 대체 소스로 사용됩니다. 외부 서버를 사용하지 않고 디바이스에서 직접 사용자를 정의할 수 있습니다. 로컬 데이터베이스를 대체 소스로 사용하는 경우 외부 서버에 정의한 것과 같은 사용자 이름/비밀번호를 정의해야 합니다. 로컬 사용자 구성를 참조하십시오.
- Duo LDAP 서버 - 기본 또는 보조 인증 소스로 사용됩니다. Duo LDAP 서버를 기본 소스로 사용할 수는 있지만 이는 일반적인 구성이 아닙니다. 일반적으로 이를 보조 소스로 사용하여 기본 Active Directory 또는 RADIUS 서버와 함께 이중 인증을 제공합니다. 자세한 내용은 Duo LDAP를 사용하여 이중 인증을 구성하는 방법, 44 페이지를 참조해 주십시오.

단계 **6** (선택 사항). RA VPN에 대한 그룹 정책 컨피그레이션, 25 페이지

그룹 정책에서는 사용자와 관련된 속성을 정의합니다. 그룹 멤버십에 근거하여 리소스에 차등 액세스를 제공하도록 그룹 정책을 컨피그레이션할 수 있습니다. 또는 모든 연결에 기본 정책을 사용할 수 있습니다.

단계 **7** RA VPN 연결 프로파일 컨피그레이션, 16 페이지.

단계 **8** 원격 액세스 VPN을 통한 트래픽 허용, 13 페이지.

단계 **9** 원격 액세스 VPN 컨피그레이션 확인, 13 페이지.

연결을 완료할 때 문제가 발생한 경우 원격 액세스 VPN 트러블슈팅, 32 페이지의 내용을 참조하십시오.

단계 **10** (선택 사항). ID 정책을 활성화하고 패시브 인증에 사용할 규칙을 생성합니다.

패시브 사용자 인증을 활성화하는 경우 원격 액세스 VPN을 통해 로그인한 사용자는 대시보드에 표시되며 정책에서 트래픽 일치 기준으로도 사용할 수 있게 됩니다. 패시브 인증을 활성화하지 않는 경우 RA VPN 사용자는 활성 인증 정책과 일치하는 경우에만 사용 가능합니다. 대시보드에서 또는 트래픽 일치용으로 사용자 이름 정보를 가져오려면 ID 정책을 활성화해야 합니다.

클라이언트 프로파일 구성 및 업로드

Secure Client 프로파일은 Secure Client 소프트웨어와 함께 클라이언트에 다운로드됩니다. 이러한 프로파일은 시작 시의 자동 연결 및 자동 다시 연결, 그리고 엔드 유저가 Secure Client 환경 설정 및 고급 설정에서 옵션을 변경할 수 있는지 여부와 같은 여러 클라이언트 관련 옵션을 정의합니다.

원격 액세스 VPN 연결을 구성할 때 외부 인터페이스의 FQDN(모든 자격을 갖춘 호스트 이름)을 구성하는 경우 시스템에서 클라이언트 프로파일을 생성합니다. 이 프로파일은 기본 설정을 활성화합니다. 기본 동작이 아닌 동작을 수행하려는 경우에만 클라이언트 프로파일을 생성하여 업로드하면 됩니다. 클라이언트 프로파일은 선택 사항이므로 업로드하지 않으면 Secure Client는 프로파일을 통해 제어되는 모든 옵션에 대해 기본 설정을 사용합니다.

참고 첫 번째 연결에서 Secure Client가 모든 사용자 제어 가능 설정을 표시하도록 하려면 VPN 프로파일의 서버 목록에 threat defense 디바이스의 외부 인터페이스를 포함해야 합니다. 프로파일에 있는 호스트 항목으로 FQDN 또는 주소를 추가하지 않은 경우, 필터가 세션에 적용되지 않습니다. 예를 들어 인증서 일치를 생성하고 인증서가 기준과 제대로 일치하지만 해당 프로파일에 있는 호스트 항목으로 디바이스를 추가하지 않는 경우, 인증서 일치가 무시됩니다.

AMP Enabler와 같이 Secure Client에서 선택적으로 사용할 수 있는 다양한 모듈 및 Secure Client에 대한 프로파일을 생성할 수 있습니다. 이러한 모듈에 대한 프로파일을 업로드할 수 있긴 하지만 device manager에서는 Secure Client 프로파일만 생성할 수 있습니다. 그러나 device manager을 통해 모든 종류의 프로파일을 업로드한 다음 API Explorer에서 threat defense API를 사용하여 개체의 프로파일 유형을 변경할 수 있습니다. 프로파일 페이지에는 모든 유형의 모든 프로파일이 표시되지만 목록에는 프로파일 유형이 표시되지 않습니다. 절차에서는 이를 수행하는 방법을 설명합니다.

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 수정할 수 있는 방법을 설명합니다. 개체 목록에 표시되는 새 보안 클라이언트 프로파일 생성 링크를 클릭하여 프로파일 속성을 수정하면서 Secure Client 프로파일 개체를 생성할 수도 있습니다.

시작하기 전에

클라이언트 프로파일을 업로드하려면 다음을 수행해야 합니다.

- 독립형 Secure Client "프로파일 편집기 - Windows/독립형 설치 관리자(MSI)"를 다운로드하여 설치합니다. 설치 파일은 Windows 전용이며 파일 이름은 anyconnect-profileeditor-win-<version>-k9.msi입니다. 여기서 <version>은 Secure Client 버전입니다(이에 따라 파일 이름 변경). 예를 들면 anyconnect-profileeditor-win-4.3.04027-k9.msi와 같습니다. 또한 프로파일 편집기를 설치하기 전에 Java JRE 1.6 이상도 설치해야 합니다. software.cisco.com에서 Secure Client 프로파일 편집기를 다운로드합니다. 이 패키지에는 VPN 클라이언트용 프로파일 편집기뿐만 아니라 모든 프로파일 편집기가 포함되어 있습니다.
- 프로파일 편집기를 사용하여 필요한 프로파일을 생성합니다. 프로파일에서 외부 인터페이스의 호스트 이름 또는 IP 주소를 지정해야 합니다. 자세한 내용은 편집기의 온라인 도움말을 참조하십시오.

프로시저

단계 **1** 목차에서 **Objects(**개체**)**와 **Secure Client Profile(**보안 클라이언트 프로파일**)**을 차례로 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 개체를 생성하려면 + 버튼을 클릭합니다.
- 개체를 수정하려면 개체의 수정 아이콘( )을 클릭하십시오.
- 개체와 연결된 프로파일을 다운로드하려면 해당 개체의 다운로드 아이콘( )을 클릭합니다.

참조되지 않는 개체를 삭제하려면 해당 개체의 휴지통 아이콘( )을 클릭합니다.

단계 **3** 개체의 이름과 설명(선택 사항)을 입력합니다.

모듈 프로파일을 업로드하는 경우 Secure Client 프로파일과 쉽게 구분할 수 있도록 개체 이름을 사용하여 모듈 유형을 나타냅니다.

단계 **4** **Upload(**업로드**)**를 클릭하고 프로파일 편집기를 사용하여 생성한 파일을 선택합니다.

단계 **5** **Open(**열기**)**을 클릭하여 프로파일을 업로드합니다.

단계 **6** **OK(**확인**)**를 클릭하여 개체를 추가합니다.

단계 **7** 생성한 프로파일이 사실상 Secure Client 프로파일과 다른 유형인 경우 다음 단계를 완료하여 개체의 프로파일 유형을 변경하십시오.

a) More options(추가 옵션) 버튼(⋮)을 클릭하고 **API Explorer**를 선택합니다.

브라우저 설정에 따라 별도의 탭 또는 창에 API Explorer가 열립니다.

b) AnyConnectClientProfile 리소스를 엽니다.

c) GET /object /anyconnectclientprofiles 메소드를 선택하고 **Try It Out!(**시도**)** 버튼을 클릭합니다.

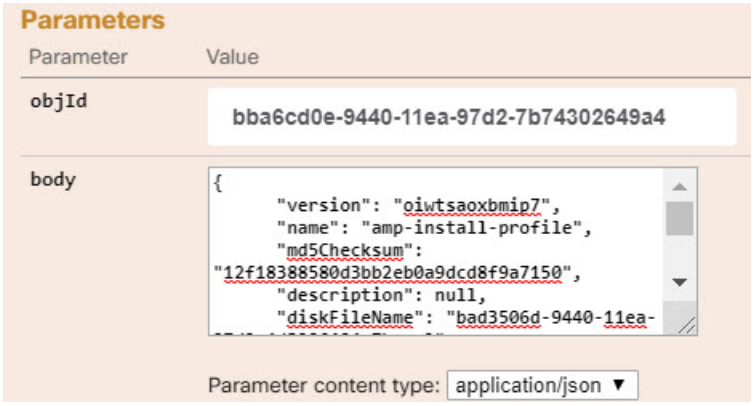
각 프로파일 개체는 다음과 같이 표시됩니다. 강조 표시된 특성이 변경해야 할 속성입니다.

```
{
      "version": "oiwtsaoxbmip7",
      "name": "amp-install-profile",
      "md5Checksum": "12f18388580d3bb2eb0a9dcd8f9a7150",
      "description": null,
      "diskFileName": "bad3506d-9440-11ea-97d2-4d3296494e7b.xml",
      "anyConnectModuleType": "ANY_CONNECT_CLIENT_PROFILE",
      "id": "bba6cd0e-9440-11ea-97d2-7b74302649a4",
      "type": "anyconnectclientprofile",
      "links": {
        "self": "https://10.89.5.38/api/fdm/v6/object/
anyconnectclientprofiles/bba6cd0e-9440-11ea-97d2-7b74302649a4"
      }
```

d) 출력에서 개체를 찾은 다음 코드를 선택하고 Ctrl + 클릭을 사용하여 이를 클립 보드에 복사합니다.

e) PUT / object/anyconnectclientprofiles/{objId} 메소드를 선택하고 **body** 필드에 내용을 붙여 넣습니다.

f) **ID** 값을 복사하여 본문 위의 **objId** 수정 상자에 붙여 넣습니다. "self" URL의 끝에서도 개체 ID를 찾을 수 있습니다.



g) 개체 본문에서 **anyConnectModuleType** 필드를 찾아 값을 프로파일 유형에 해당하는 값으로 바꿉니다. DART, FEEDBACK, WEB_SECURITY, ANY_CONNECT_CLIENT_PROFILE, AMP_ENABLER, NETWORK_ACCESS_MANAGER, NETWORK_VISIBILITY, START_BEFORE_LOGIN, ISE_POSTURE, UMBRELLA 중에서 선택합니다.

h) **body**에서 다시 **type** 값 뒤의 쉼표를 포함하여 **links** 특성을 삭제합니다.

개체 본문은 다음과 비슷해야 합니다.

```
{
      "version": "oiwtsaoxbmip7",
      "name": "amp-install-profile",
      "md5Checksum": "12f18388580d3bb2eb0a9dcd8f9a7150",
      "description": null,
      "diskFileName": "bad3506d-9440-11ea-97d2-4d3296494e7b.xml",
      "anyConnectModuleType": "AMP_ENABLER",
      "id": "bba6cd0e-9440-11ea-97d2-7b74302649a4",
      "type": "anyconnectclientprofile"
      }
```

i) **Try It Out!(**시도**)**을 클릭합니다. 응답을 검사하여 개체가 올바르게 수정되었는지 확인합니다. 응답 코드 200 및 변경 사항을 반영하는 응답 본문을 가져와야 합니다. GET 방법을 사용하여 결과를 추가로 확인할 수 있습니다.

원격 액세스 **VPN**을 통한 트래픽 허용

다음 기법 중 하나를 사용해 원격 액세스 VPN 터널에서 트래픽 흐름을 활성화할 수 있습니다.

- **sysopt connection permit-vpn** 명령을 컨피그레이션합니다. 이 명령에서는 VPN 연결과 일치하는 트래픽을 액세스 제어 정책에서 제외합니다. 이 명령의 기본값은 **no sysopt connection permit-vpn** 입니다. 이는 액세스 제어 정책에서도 VPN 트래픽을 허용해야 한다는 의미입니다.

  이 방법은 외부 사용자가 원격 액세스 VPN 주소 풀에서 IP 주소를 스푸핑할 수 없기 때문에 VPN에서 트래픽을 더 안전하게 허용할 수 있습니다. 하지만 VPN 트래픽이 검사되지 않는다는 단점이 있습니다. 즉, 침입 및 파일 보호, URL 필터링 또는 기타 고급 기능이 트래픽에 적용되지 않습니다. 즉 트래픽에 대해 연결 이벤트가 생성되지 않고, 따라서 통계 대시보드에 VPN 연결이 반영되지 않는다는 의미이기도 합니다.

  이 명령을 컨피그레이션하려면 RA VPN 연결 프로파일에서 **Bypass Access Control policy for decrypted traffic(**암호 해독된 트래픽에 대해 액세스 제어 정책 우회**)** 옵션을 선택하십시오.

- 원격 액세스 VPN 주소 풀에서 연결을 허용하는 액세스 제어 규칙을 생성합니다. 이 방법을 사용하는 경우 VPN 트래픽이 검사되며, 연결에 고급 서비스를 적용할 수 있습니다. 하지만 외부 사용자가 IP 주소를 스푸핑하여 내부 네트워크에 액세스할 가능성이 있다는 단점이 있습니다.

원격 액세스 **VPN** 컨피그레이션 확인

원격 액세스 VPN을 구성하고 디바이스에 컨피그레이션을 구축한 후에는 원격 연결을 수행할 수 있는지 확인합니다.

문제가 발생할 경우, 트러블슈팅 항목을 충분히 읽은 후 문제를 구분하고 해결합니다. 원격 액세스 VPN 트러블슈팅, 32 페이지를 참조하십시오.

프로시저

단계 **1** 외부 네트워크에서 Secure Client를 사용하여 VPN 연결을 설정합니다.

웹 브라우저를 사용하여 **https://***ravpn-address*를 엽니다. 여기서 *ravpn-address*는 VPN 연결을 허용할 외부 인터페이스의 IP 주소 또는 호스트 이름입니다. 필요한 경우, 클라이언트 소프트웨어를 설치하여 연결을 완료합니다. 사용자가 Secure Client 소프트웨어를 설치할 수 있는 방법, 3 페이지를 참조하십시오.

원격 액세스 VPN 연결용 포트를 변경한 경우 URL에 맞춤형 포트를 포함해야 합니다. 예를 들어 포트를 4443으로 변경한 경우 https://ravpn.example.com:4443과 같습니다.

그룹 URL을 컨피그레이션한 경우, 그룹 URL도 시도해 보십시오.

단계 **2** CLI(Command Line Interface) 로그인에 설명된 대로 디바이스 CLI에 로그인합니다. 또는 CLI 콘솔을 여십시오.

단계 **3** **show vpn-sessiondb** 명령을 사용하여 현재 VPN 세션에 대한 요약 정보를 확인합니다.

통계에는 활성 Secure Client 세션, 누적 세션에 대한 정보, 최대 동시 세션 수, 비활성 세션이 표시되어야 합니다. 다음은 명령의 샘플 출력입니다.

```
> show vpn-sessiondb
--------------------------------------------------------------------------------
VPN Session Summary
--------------------------------------------------------------------------------
                            Active : Cumulative : Peak Concur : Inactive
                           ------------------------------------------------
AnyConnect Client           :      1 :         49 :           3 :        0
  SSL/TLS/DTLS              :      1 :         49 :           3 :        0
Clientless VPN              :      0 :          1 :           1
  Browser                   :      0 :          1 :           1
--------------------------------------------------------------------------------
Total Active and Inactive   :      1             Total Cumulative :     50
Device Total VPN Capacity   :  10000
Device Load                 :     0%
--------------------------------------------------------------------------------

--------------------------------------------------------------------------------
Tunnels Summary
--------------------------------------------------------------------------------
                            Active : Cumulative : Peak Concurrent
                           ------------------------------------------------
Clientless                  :      0 :          1 :               1
AnyConnect-Parent           :      1 :         49 :               3
SSL-Tunnel                  :      1 :         46 :               3
DTLS-Tunnel                 :      1 :         46 :               3
--------------------------------------------------------------------------------
Totals                      :      3 :        142
--------------------------------------------------------------------------------

--------------------------------------------------------------------------------
IPv6 Usage Summary
--------------------------------------------------------------------------------
```

```
                                Active : Cumulative : Peak Concurrent
                               ----------------------------------------
AnyConnect SSL/TLS/DTLS       :        :            :
  Tunneled IPv6               :      1 :         20 :           2
-------------------------------------------------------------------------
```

단계 **4** **show vpn-sessiondb anyconnect** 명령을 사용하여 현재 VPN 세션에 대한 세부 정보를 확인합니다.

세부 정보에는 사용된 암호화, 전송 및 수신한 바이트 수, 기타 통계 정보가 포함됩니다. VPN 연결을 사용하면 이 명령을 다시 호출할 경우 전송/수신한 바이트 수 변경 사항이 표시되어야 합니다.

```
> show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : priya                  Index        : 4820
Assigned IP  : 172.18.0.1             Public IP    : 192.168.2.20
Assigned IPv6: 2009::1
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256  DTLS-Tunnel: (1)AES256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 27731                  Bytes Rx     : 14427
Group Policy : MyRaVpn|Policy         Tunnel Group : MyRaVpn
Login Time   : 21:58:10 UTC Mon Apr 10 2017
Duration     : 0h:51m:13s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : c0a800fd012d400058ebfff2
Security Grp : none                   Tunnel Zone  : 0
```

원격 액세스 VPN 컨피그레이션 관리

원격 액세스 VPN 연결 프로파일에서는 외부 사용자가 Secure Client를 사용하여 시스템에 VPN 연결을 할 수 있게 허용하는 특성을 정의합니다. 각 프로파일에서 정의하는 것은 사용자를 인증하는 데 사용되는 AAA 서버 및 인증서, 사용자에게 IP 주소를 할당하기 위한 주소 풀, 다양한 사용자 중심 속성을 정의하는 그룹 정책입니다.

여러 사용자 그룹에 가변적인 서비스를 제공해야 하는 경우 또는 인증 소스가 여러 개인 경우, 프로파일을 여러 개 만듭니다. 예를 들어 조직이 다른 인증 서버를 사용하는 다른 조직과 병합하는 경우, 해당 인증 서버를 사용하는 새 그룹에 대해 프로파일을 만들 수 있습니다.

프로시저

단계 **1** **Device(**디바이스**)** > **Remote Access VPN(**원격 액세스 **VPN)** 그룹에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

현재 얼마나 많은 연결 프로파일 및 그룹 정책이 컨피그레이션되어 있는지 나타내는 요약 정보를 그룹에서 표시합니다.

단계 2 목차에서 **Connection Profiles(**연결 프로파일**)**을 아직 선택하지 않은 경우 클릭합니다.

단계 3 다음 중 하나를 수행합니다.

- + 버튼을 클릭하여 새 연결 프로파일을 생성합니다. 자세한 내용은 RA VPN 연결 프로파일 컨피그레이션, 16 페이지를 참고하십시오.
- 보기 버튼()을 클릭하여 연결 프로파일 및 연결 지침에 관한 요약 정보를 엽니다. 요약 정보 내에서 **Edit(**수정**)**을 클릭하여 변경할 수 있습니다.
- 삭제 버튼()을 클릭하여 더 이상 필요하지 않은 연결 프로파일을 삭제합니다.
- 목차에서 **Group Policies(**그룹 정책**)**를 선택하여 연결 프로파일에 대해 사용자 중심 속성을 정의합니다. RA VPN에 대한 그룹 정책 컨피그레이션, 25 페이지의 내용을 참조하십시오.

RA VPN 연결 프로파일 컨피그레이션

홈 네트워크 등의 외부 네트워크에 있는 사용자가 내부 네트워크에 연결할 수 있도록 원격 액세스 VPN 연결 프로파일을 생성할 수 있습니다. 다른 인증 방법을 수용하기 위해 별도 프로파일을 생성합니다.

시작하기 전에

RA(원격 액세스) VPN 연결을 구성하기 전에 다음 작업을 수행합니다.

- software.cisco.com에서 필요한 Secure Client 소프트웨어 패키지를 워크스테이션에 다운로드합니다.
- 원격 액세스 VPN 연결을 종료하는 외부 인터페이스가 동일한 포트에서 HTTPS 연결을 허용하는 관리 액세스 목록도 포함할 수는 없습니다. 관리 액세스를 위해 다른 포트를 구성하거나(데이터 인터페이스에서 관리 액세스에 대한 HTTPS 포트 구성 참조) 연결 프로파일에 대해 다른 포트를 구성합니다. 두 서비스 모두 기본적으로 포트 443을 사용하므로 하나를 변경해야 합니다.

프로시저

단계 1 **Device(**디바이스**)** > **Remote Access VPN(**원격 액세스 **VPN)** 그룹에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

현재 얼마나 많은 연결 프로파일 및 그룹 정책이 컨피그레이션되어 있는지 나타내는 요약 정보를 그룹에서 표시합니다.

단계 2 목차에서 **Connection Profiles(**연결 프로파일**)**을 아직 선택하지 않은 경우 클릭합니다.

단계 3 다음 중 하나를 수행합니다.

- + 버튼을 클릭하여 새 연결 프로파일을 생성합니다.

- 보기 버튼( )을 클릭하여 연결 프로파일 및 연결 지침에 관한 요약 정보를 엽니다. 요약 정보 내에서 **Edit(**수정**)**을 클릭하여 변경할 수 있습니다.

단계 **4** 기본 연결 속성을 컨피그레이션합니다.

- **Connection Profile Name(**연결 프로파일 이름**)** — 이 연결의 이름을 공백 없이 50자까지 입력합니다. 예를 들면 MainOffice를 입력합니다. IP 주소는 이름으로 사용할 수 없습니다.

  참고 여기서 입력하는 이름이 Secure Client 클라이언트에서 사용자에게 표시되는 연결 목록에 나타납니다. 따라서 사용자가 쉽게 이해할 수 있는 이름을 선택해야 합니다.

- **Group Alias(**그룹 별칭**)**, **Group URL(**그룹 **URL)** — 별칭에는 특정 연결 프로파일에 대한 대체 이름 또는 URL이 포함되어 있습니다. threat defense 디바이스에 연결하는 경우, VPN 사용자는 연결 목록의 Secure Client 클라이언트에서 별칭 이름을 선택할 수 있습니다. 연결 프로파일 이름이 그룹 별칭으로 자동 추가됩니다. 별칭은 최대 31자입니다.

  또한 원격 액세스 VPN 연결을 시작하는 동안 엔드포인트에서 선택할 수 있는 그룹 URL의 목록을 컨피그레이션할 수 있습니다. 사용자가 그룹 URL을 사용하여 연결하는 경우, 시스템에서는 URL과 일치하는 연결 프로파일을 자동으로 사용합니다. 이 URL은 설치된 Secure Client 클라이언트가 아직 없는 클라이언트에서 사용됩니다.

  그룹 별칭 및 URL을 필요한 만큼 추가하십시오. 이러한 별칭 및 URL은 디바이스에 정의된 모든 연결 프로파일 전반에 걸쳐 고유한 것이어야 합니다. 그룹 URL은 **https://**로 시작해야 합니다.

  예를 들어 별칭 계약자 및 그룹 URL https://ravpn.example.com/contractor가 있을 수 있습니다. Secure Client 클라이언트가 설치된 후 사용자는 연결의 Secure Client VPN 드롭다운 목록에서 그룹 별칭을 선택하기만 하면 됩니다.

단계 **5** 기본 ID 소스를 컨피그레이션하고, 선택적으로 보조 ID 소스를 컨피그레이션합니다.

이 옵션을 통해 원격 사용자가 원격 액세스 VPN 연결을 활성화하기 위해 디바이스에 인증하는 방식을 결정합니다. 가장 간단한 방식은 AAA만 사용하여 AD 영역을 선택하거나 LocalIdentitySource를 사용하는 것입니다. **Authentication Type(**인증 유형**)**에는 다음과 같은 방식을 사용할 수 있습니다.

- **AAA Only(AAA**만**)** — 사용자 이름 및 암호에 근거하여 사용자를 인증하고 사용자에게 권한을 부여합니다. 자세한 내용은 연결 프로파일에 대해 AAA 컨피그레이션, 20 페이지 섹션을 참조해 주십시오.
- **Client Certificate Only(**클라이언트 인증서만**)** — 클라이언트 디바이스 ID 인증서에 근거하여 사용자를 인증합니다. 자세한 내용은 연결 프로파일에 대한 인증서 인증 컨피그레이션, 23 페이지 섹션을 참조해 주십시오.
- **AAA and ClientCertificate(AAA** 및 **ClientCertificate)** — 사용자 이름/암호와 클라이언트 디바이스 ID 인증서를 모두 사용합니다.
- **SAML** — 기본 인증에서 SAML 서버를 사용합니다. SAML을 사용할 때는 대체 또는 보조 인증 소스를 구성할 수 없습니다. 자세한 내용은 연결 프로파일에 대해 AAA 컨피그레이션, 20 페이지를 참조해 주십시오.

단계 **6** 클라이언트에 대해 주소 풀을 컨피그레이션합니다.

주소 풀에서는 원격 클라이언트가 VPN 연결을 설정할 때 시스템에서 원격 클라이언트에 할당할 수 있는 IP 주소를 정의합니다. 자세한 내용은 RA VPN에 대한 클라이언트 주소 지정 컨피그레이션, 24 페이지를 참고하십시오.

단계 **7** **Next(**다음**)**를 클릭합니다.

단계 **8** 이 프로파일에 사용할 **Group Policy(**그룹 정책**)**를 선택합니다.

그룹 정책에서는 터널이 설정된 후에 사용자 연결에 대한 조건을 설정합니다. 시스템에는 DfltGrpPolicy라는 이름의 기본 그룹 정책이 포함되어 있습니다. 필요한 서비스를 제공하는 추가 그룹 정책을 만들 수 있습니다.

그룹 정책을 선택하는 경우, 그룹 특성에 관한 요약 정보가 표시됩니다. 변경하려면 요약 정보에서 **Edit(**수정**)**을 클릭합니다.

필요한 그룹 정책이 아직 없는 경우, 드롭다운 목록에서 **Create New Group Policy(**새 그룹 정책 생성**)**를 클릭합니다.

그룹 정책에 대한 세부 정보는 RA VPN에 대한 그룹 정책 컨피그레이션, 25 페이지의 내용을 참조하십시오.

단계 **9** **Next(**다음**)**를 클릭합니다.

단계 **10** 전역 설정을 구성합니다.

이 옵션은 모든 연결 프로파일에 적용됩니다. 첫 번째 연결 프로파일을 만들고 나면 각 후속 프로파일에 대해 이 옵션이 사전 컨피그레이션됩니다. 변경하는 경우, 컨피그레이션된 모든 연결 프로파일이 변경됩니다.

- **Certificate of Device Identity(**디바이스 **ID**의 인증서**)** — 디바이스의 ID를 설정하는 데 사용되는 내부 인증서를 선택합니다. 보안 VPN 연결을 완료하려면 클라이언트가 이 인증서를 허용해야 합니다. 인증서가 아직 없는 경우 드롭다운 목록에서 **Create New Internal Certificate(**새 내부 인증서 생성**)**를 클릭합니다. 인증서를 구성해야 합니다.
- **Outside Interface(**외부 인터페이스**)** - 사용자가 원격 액세스 VPN 연결을 설정할 때 연결하는 인터페이스입니다. 이 인터페이스는 대개 외부(인터넷 연결) 인터페이스이지만, 지원하려는 디바이스와 엔드 유저 간의 인터페이스를 선택하면 됩니다.
- 외부 인터페이스의 **FQDN(Fully-Qualified Domain Name)** - ravpn.example.com과 같은 인터페이스의 이름입니다. 이름을 지정하는 경우 시스템이 클라이언트 프로파일을 자동으로 생성할 수 있습니다.

  참고 VPN과 클라이언트에 사용되는 DNS 서버가 외부 인터페이스 IP 주소에 대해 이 이름을 확인할 수 있도록 해야 합니다. 관련 DNS 서버에 FQDN을 추가합니다.

- **Port(**포트**)** — RA VPN 연결에 사용할 TCP 포트입니다. 기본값은 443입니다. RA VPN에 사용된 것과 동일한 인터페이스에서 device manager에 연결해야 하는 경우 연결 프로파일 또는 device manager의 포트 번호를 변경해야 합니다. 두 서비스 모두 기본적으로 443을 사용합니다. 원격 액세스 VPN 연결용 포트를 변경하는 경우 사용자가 URL에 포트 번호를 포함해야 합니다.
- **Bypass Access Control policy for decrypted traffic(**암호 해독된 트래픽에 대해 액세스 제어 정책 우회**)(sysopt permit-vpn)** - VPN 트래픽을 액세스 제어 정책에 종속시킬지 여부. 암호 해독된 VPN 트래픽에는 기본적으로 액세스 제어 정책 검사가 적용됩니다. **Bypass Access Control policy for**

decrypted traffic(암호 해독된 트래픽에 대해 액세스 제어 정책 우회**)** 옵션을 활성화하면 액세스 제어 정책을 우회하지만, 원격 액세스 VPN의 경우에는 VPN 필터 ACL과 AAA 서버에서 다운로드한 인증 ACL이 VPN 트래픽에 계속 적용됩니다.

이 옵션을 선택하는 경우, 시스템에서는 전역 설정인 **sysopt connection permit-vpn** 명령을 컨피그레이션한다는 점에 유의하십시오. 이로 인해 Site-to-Site VPN 연결의 동작도 영향을 받습니다. 또한 연결 프로파일 전반에서 이 옵션에 대해 서로 다른 항목을 선택할 수 없습니다. 즉 모든 프로파일에 대해 기능을 켜거나 꺼야 합니다.

이 옵션을 선택하지 않는 경우, 외부 사용자가 원격 액세스 VPN 주소 풀의 IP 주소를 스푸핑할 수 있고, 따라서 네트워크에 액세스할 수 있습니다. 이것이 가능한 이유는 주소 풀에서 내부 리소스에 액세스할 수 있게 허용하는 액세스 제어 규칙을 생성해야 하기 때문입니다. 액세스 제어 규칙을 사용하는 경우, 소스 IP 주소만 사용하기보다 사용자 사양을 이용해 액세스를 제어하는 것이 좋습니다.

이 옵션을 선택할 경우의 단점은 VPN 트래픽이 검사되지 않는다는 것입니다. 즉 침입 및 파일 보호, URL 필터링 또는 기타 고급 기능이 트래픽에 적용되지 않습니다. 즉 트래픽에 대해 연결 이벤트가 생성되지 않고, 따라서 통계 대시보드에 VPN 연결이 반영되지 않는다는 의미이기도 합니다.

- **NAT Exempt(NAT** 제외**)** - NAT 변환에서 원격 액세스 VPN 엔드포인트와 주고받는 트래픽을 제외하려면 NAT 제외를 활성화합니다. NAT에서 VPN 트래픽을 제외하지 않는 경우 내부 인터페이스와 외부 인터페이스에 대한 기존 NAT 규칙이 주소의 RA VPN 풀에 적용되지 않는지 확인합니다. NAT 제외 규칙은 지정된 소스/대상 인터페이스 및 네트워크 조합에 대한 수동 고정 ID NAT 규칙이며 NAT 정책에서는 반영되지 않고 숨겨집니다. NAT 제외를 활성화하는 경우에는 다음 항목도 구성해야 합니다.

  이것은 전역 옵션이므로 모든 연결 프로파일에 적용된다는 점에 유의하십시오. 따라서 인터페이스와 내부 네트워크를 추가하기만 하고 교체하지 마십시오. 그러지 않으면 이미 정의한 다른 모든 연결 프로파일에 대한 NAT 제외 설정이 변경됩니다.

  - 내부 인터페이스 - 원격 사용자가 액세스할 내부 네트워크의 인터페이스를 선택합니다. NAT 규칙은 이러한 인터페이스에 대해 생성됩니다.
  - 내부 네트워크 - 원격 사용자가 액세스할 내부 네트워크를 나타내는 네트워크 개체를 선택합니다. 네트워크 목록에는 지원할 주소 풀과 동일한 IP 유형이 포함되어 있어야 합니다.

- **Secure Client Package(**보안 클라이언트 패키지**)** - RA VPN 연결에서 지원할 Secure Client 전체 설치 소프트웨어 이미지입니다. 각 패키지의 파일 이름(확장자 포함)은 60자 이하여야 합니다. Windows, Mac 및 Linux 엔드포인트에 대해 별도의 패키지를 업로드할 수 있습니다. 그러나 여러 연결 프로파일에 대해 여러 패키지를 컨피그레이션할 수는 없습니다. 다른 프로파일에 대해 패키지를 이미 컨피그레이션한 경우, 패키지가 미리 선택되어 있습니다. 패키지를 변경하면 모든 프로파일에 대해 변경이 이루어집니다.

  패키지는 software.cisco.com에서 다운로드합니다. 엔드포인트에 적합한 패키지가 아직 설치되어 있지 않으면 사용자에게 사용자 인증 후 패키지를 다운로드하여 설치하라는 메시지가 표시됩니다.

단계 **11** **Next(**다음**)**를 클릭합니다.

단계 12 요약을 검토합니다.

먼저 요약이 정확한지 확인합니다.

그런 다음 지침을 클릭하여 Secure Client 소프트웨어를 처음으로 설치하고 VPN 연결을 완료할 수 있는지를 테스트하기 위해 엔드 유저가 수행해야 하는 작업을 파악합니다. 복사를 클릭하여 이러한 지침을 클립보드에 복사한 다음 사용자에게 배포합니다.

단계 13 **Finish(**마침**)**를 클릭합니다.

다음에 수행할 작업

원격 액세스 VPN을 통한 트래픽 허용, 13 페이지의 설명대로 VPN 터널에서 트래픽이 허용되는지 확인합니다.

연결 프로파일에 대해 AAA 컨피그레이션

인증, 권한 부여, 계정 관리 (AAA) 서버에서는 사용자 이름과 암호를 사용하여 사용자에게 원격 액세스 VPN에 대한 액세스가 허용되어 있는지 확인합니다. RADIUS 서버를 사용하는 경우, 인증된 사용자들 사이에서 권한 부여 수준을 구별하여 보호받는 리소스에 대한 차등 액세스를 제공할 수 있습니다. 또한 RADIUS 계정 관리 서비스를 사용하여 사용량을 추적할 수 있습니다.

AAA를 컨피그레이션하는 경우, 기본 ID 소스를 컨피그레이션해야 합니다. 보조 및 대체 소스는 선택 사항입니다. 이중 인증을 구현하려면 RSA 토큰 또는 듀오와 같은 보조 소스를 사용하십시오.

기본 **ID** 소스 옵션

- **Primary Identity Source for User Authentication(**사용자 인증을 위한 기본 **ID** 소스**)** - 원격 사용자 인증에 사용되는 기본 ID 소스입니다. VPN 연결을 완료하려면 이 소스 또는 대체 소스(선택 사항)에서 최종 사용자를 정의해야 합니다. 다음 중 하나를 선택합니다.
  - AD(Active Directory) ID 영역. 필요한 영역이 아직 없는 경우, **Create New Identity Realm(**새 **ID** 영역 생성**)**을 클릭합니다.
  - Radius 서버 그룹.
  - LocalIdentitySource(로컬 사용자 데이터베이스) - 외부 서버를 사용하지 않고 디바이스에서 직접 사용자를 정의할 수 있습니다.
  - Duo LDAP 서버. 그러나 이 서버는 Duo LDAP를 사용하여 이중 인증을 구성하는 방법, 44 페이지에 설명된 대로 이중 인증을 제공하기 위한 보조 인증 소스로 사용되는 것이 가장 바람직합니다. 이 서버를 기본 소스로 사용하는 경우 사용자 ID 정보를 가져올 수 없고, 대시보드에 사용자 정보가 표시되지 않으며, 사용자 기반 액세스 제어 규칙을 작성할 수도 없습니다.
  - SAML 서버 SAML 서버를 사용하는 경우 대체 또는 보조 인증 소스를 구성할 수 없습니다. RADIUS를 권한 부여 서버로 사용할 수 있지만 인증이 필요하지 않도록 RADIUS 서버를 구성해야 합니다. 즉, RADIUS 서버는 SAML에서 연결을 인증한 후 권한 부여 정보를 제공합니다.

- **SAML Login Experience(SAML** 로그인 환경**)** - SAML을 기본 인증 소스로 선택한 경우 웹 인증을 완료하는 데 사용할 클라이언트 브라우저를 선택해야 합니다.
  - **VPN Client embedded browser(VPN** 클라이언트 임베디드 브라우저**)** - VPN 클라이언트는 웹 인증을 위해 임베디드 브라우저를 사용하므로 인증은 VPN 연결에만 적용됩니다. 이는 기본값이며 추가로 구성할 필요가 없습니다.
  - **Default OS Browser(**기본 **OS** 브라우저**)** - VPN 클라이언트는 웹 인증을 위해 시스템의 기본 브라우저를 사용합니다. 이 옵션은 VPN 인증과 기타 기업 로그인 간에 SSO(Single Sign-On)를 활성화합니다. 생체 인증과 같이 임베디드 브라우저에서 수행할 수 없는 웹 인증 방법을 지원하고자 하는 경우 이 옵션을 선택합니다.

    브라우저에서 웹 인증을 활성화하는 패키지를 업로드해야 합니다. 패키지는 software.cisco.com에서 다운로드합니다. 업로드하는 패키지는 SAML을 기본 OS 브라우저와 함께 사용하는 모든 연결 프로파일에서 사용됩니다. 패키지는 전역이며, 연결 프로파일에 한정되지 않습니다.

- **Fallback Local Identity Source(**대체 로컬 **ID** 소스**)** - 기본 소스가 외부 서버인데 기본 서버를 사용할 수 없는 경우, 대체 소스로 LocalIdentitySource를 선택할 수 있습니다. 로컬 데이터베이스를 대체 소스로 사용하는 경우 외부 서버에 정의한 것과 같은 로컬 사용자 이름/비밀번호를 정의해야 합니다.

Advanced options(고급 옵션**)** - **Advanced(**고급**)** 링크를 클릭하고 다음 옵션을 구성합니다.

- **Strip options(**제거 옵션**)** - 영역은 관리 도메인입니다. 다음 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.
  - **Strip Identity Source Server from Username(**사용자 이름에서 **ID** 소스 서버 제거**)** - AAA 서버로 사용자 이름을 전달하기 전에 사용자 이름에서 ID 소스 이름을 제거할지 여부. 예를 들어 이 옵션을 선택하고 사용자가 도메인\사용자 이름을 사용자 이름으로 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 제거할지 여부. 이 옵션은 username@domain 형식에서 지정된 이름에 적용되며, 도메인 및 @ 기호를 제거합니다. 기본적으로 이 옵션은 선택되어 있지 않습니다.

- **Enable Password Management(**비밀번호 관리 활성화**)** - 비밀번호가 만료될 때 사용자가 비밀번호를 변경할 수 있는지 여부를 설정합니다. 이 옵션을 선택하지 않으면 사용자의 비밀번호가 만료될 때 Secure Client는 연결을 거부하며 사용자는 AAA 서버에서 비밀번호를 변경해야 합니다. 이 옵션을 선택하면 비밀번호가 만료될 때 Secure Client에서 사용자에게 비밀번호를 변경하라는 메시지가 표시되므로 사용자에게 훨씬 더 편리합니다. 다음 옵션 중 하나를 선택합니다. 또한 AAA 서버에서 MSCHAPv2를 활성화해야 합니다.
  - **Notify user x days before password expiration(**비밀번호 만료 **x**일 전에 사용자에게 알림**)**(LDAP만 해당) - 지정한 일 수부터 시작하여 사용자에게 비밀번호 만료를 경고합니다. 1일에서 180일 사이로 설정할 수 있으며, 기본값은 14일입니다.

- **Notify user on the day of password expiration(**비밀번호 만료일에 사용자에게 알림**)** - 사용자에게 경고가 표시되지 않지만 비밀번호가 만료되면 비밀번호를 변경하라는 메시지가 계속 표시됩니다. 경고 기간을 설정하더라도 RADIUS 사용자는 항상 이 동작을 수행합니다.

보조 **ID** 소스

- **Secondary Identity Source for User Authorization(**사용자 권한 부여를 위한 보조 **ID** 소스**)** - 두 번째 ID 소스로서 선택 사항입니다. 사용자가 기본 소스로 인증에 성공하는 경우, 사용자에게 보조 소스를 사용해 인증하라는 메시지가 표시됩니다. AD 영역, RADIUS 서버 그룹, Duo LDAP 서버 또는 로컬 ID 소스를 선택할 수 있습니다.
- **Advanced options(**고급 옵션**)** - **Advanced(**고급**)** 링크를 클릭하고 다음 옵션을 컨피그레이션합니다.
  - **Fallback Local Identity Source for Secondary(**보조용 대체 시스템 로컬 **ID** 소스**)** - 보조 소스가 외부 서버인데 보조 서버를 사용할 수 없는 경우, LocalIdentitySource를 대체 소스로 선택할 수 있습니다. 로컬 데이터베이스를 대체 소스로 사용하는 경우, 보조 외부 서버에 정의한 것과 같은 로컬 사용자 이름/암호를 정의해야 합니다.
  - **Use Primary Username for Secondary Login(**보조 로그인에 기본 사용자 이름 사용**)** - 보조 ID 소스를 사용하는 경우, 시스템에서는 기본적으로 보조 소스에 대한 사용자 이름 및 암호를 모두 입력하라는 메시지를 표시합니다. 이 옵션을 선택하는 경우, 시스템에서는 보조 암호만 입력하라는 메시지를 표시하고 기본 ID 소스에 대해 인증된 보조 소스에 동일한 사용자 이름을 사용합니다. 기본 및 보조 ID 소스 모두에서 동일한 사용자 이름을 컨피그레이션하는 경우, 이 옵션을 선택합니다.
  - **Username for Session Server(**세션 서버의 사용자 이름**)** - 인증에 성공하면 사용자 이름이 이벤트 및 통계 대시보드에 표시되고, 이 이름은 사용자 또는 그룹 기반 SSL 암호 해독 및 액세스 제어 규칙에 대한 일치 여부를 확인하고 계정을 관리하는 데 사용됩니다. 두 가지 인증 소스를 사용하고 있기 때문에 기본 또는 보조 사용자 이름을 사용자 ID로 사용할지 여부를 시스템에 알려주어야 합니다. 기본적으로 기본 이름을 사용합니다.
  - **Password Type(**암호 유형**)** - 보조 서버의 암호를 가져오는 방법. 이 필드는 인증 유형으로 **AAA and Client Certificate(AAA** 및 클라이언트 인증서**)**를 선택한 경우에만 적용되며, 인증서 옵션의 경우 **Prefill username from certificate on user login window(**인증서의 사용자 이름을 사용자 로그인 창에 미리 채우기**)** 및 **Hide username in login window(**로그인 창에서 사용자 이름 숨기기**)**를 모두 선택합니다. 기본값은 **Prompt(**프롬프트**)**입니다. 이는 사용자에게 암호를 입력하라는 메시지가 표시됨을 뜻합니다.

    사용자가 기본 서버에 인증할 때 입력한 암호를 자동으로 사용하려면 **Primary Identity Source Password(**기본 **ID** 소스 암호**)**를 선택합니다.

    모든 사용자에 대해 동일한 암호를 사용하려면 **Common Password(**공통 암호**)**를 선택한 다음, **Common Password(**공통 암호**)** 필드에 해당 암호를 입력합니다.

추가 옵션

- **Authorization Server(**권한 부여 서버**)** - 원격 액세스 VPN 사용자를 인증하도록 컨피그레이션된 RADIUS 서버 그룹.

  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 부여를 위한 RADIUS 컨피그레이션에 대한 정보는 RADIUS 및 그룹 정책을 이용한 사용자 권한 및 속성 제어, 4 페이지의 내용을 참조하십시오.

  시스템이 그룹 정책에 정의된 것과 중복되는 권한 부여 속성을 RADIUS 서버에서 가져오는 경우, RADIUS 속성은 그룹 정책 속성을 재정의한다는 점에 유의하십시오.

- **Accounting Server(**과금 서버**)** - (선택 사항) 원격 액세스 VPN 세션에 대한 계정 관리에 사용할 RADIUS 서버 그룹입니다.

  계정 관리 기능에서는 사용자가 액세스 중인 서비스뿐 아니라 사용 중인 네트워크 리소스의 양까지도 추적합니다. threat defense 디바이스에서는 RADIUS 서버에 사용자 활동을 보고합니다. 계정 관리 정보에는 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 대한 데이터를 분석할 수 있습니다. 관리 계정 기능을 단독으로 사용하거나 인증 및 권한 부여 기능과 함께 사용할 수 있습니다.

연결 프로파일에 대한 인증서 인증 컨피그레이션

클라이언트 디바이스에 설치된 인증서를 사용해 원격 액세스 VPN 연결을 인증할 수 있습니다. 인증서 인증을 사용하는 경우 원격 액세스 사용자 연결을 검증하는 데 사용되는 신뢰할 수 있는 CA 인증서에 **Validation Usage(**검증 사용**)**에 대한 **SSL Client(SSL** 클라이언트**)** 옵션이 포함되어 있는지 확인합니다.

클라이언트 인증서를 사용하는 경우에도 보조 ID 소스, 대체 소스, 권한 부여 및 과금 서버를 컨피그레이션할 수 있습니다. 이 옵션은 AAA 옵션입니다. 자세한 내용은 연결 프로파일에 대해 AAA 컨피그레이션, 20 페이지의 내용을 참조하십시오.

다음은 인증서별 속성입니다. 기본 및 보조 ID 소스에 대해 개별적으로 이러한 속성을 컨피그레이션할 수 있습니다. 보조 소스 컨피그레이션은 선택 사항입니다.

- **Username from Certificate(**인증서의 사용자 이름**)** - 다음 중 하나를 선택하십시오.
  - **Map Specific Field(**특정 필드 매핑**)** - **Primary Field(**기본 필드**)** 및 **Secondary Field(**보조 필드**)**의 순서대로 인증서 요소를 사용합니다. 기본값은 CN(Common Name) 및 OU(Organizational Unit)입니다. 조직에 대해 작동하는 옵션을 선택합니다. 필드는 서로 결합하여 사용자 이름을 제공하고, 이 이름은 이벤트, 대시보드에서 사용되며 SSL 암호 해독 및 액세스 제어 규칙에서 일치 목적으로 사용됩니다.
  - **Use entire DN (distinguished name) as username(**전체 **DN(**고유 이름**)**을 사용자 이름으로 사용**)** - 시스템은 DN 필드에서 사용자 이름을 자동으로 파생합니다.

- **Advanced options(**고급 옵션**) - Advanced(**고급**)** 링크를 클릭하고 다음 옵션을 컨피그레이션합니다.
  - **Prefill username from certificate on user login window(**인증서의 사용자 이름을 사용자 로그인 창에 미리 채우기**)** - 사용자에게 인증하라는 메시지를 표시할 때 사용자 이름 필드에 검색된 사용자 이름을 입력할지 여부.
  - **Hide username in login window(**로그인 창에서 사용자 이름 숨기기**) - Prefill(**미리 채우기**)** 옵션을 선택하면 사용자 이름을 숨길 수 있습니다. 따라서 사용자는 암호 프롬프트에서 사용자 이름을 수정할 수 없습니다.

RA VPN에 대한 클라이언트 주소 지정 컨피그레이션

원격 액세스 VPN에 연결하는 엔드포인트에 대한 IP 주소를 시스템에서 제공할 방법이 있어야 합니다. 이 주소는 AAA 서버, DHCP 서버, 그룹 정책에 컨피그레이션된 IP 주소 풀 또는 연결 프로파일에 컨피그레이션된 IP 주소 풀에서 제공할 수 있습니다. 시스템은 순서대로 이 리소스를 시도하고 사용 가능한 주소를 가져올 때 중지했다가 이 주소를 클라이언트에 할당합니다. 따라서 동시 연결 수가 비정상적인 경우에 페일세이프를 생성할 수 있는 여러 가지 옵션을 컨피그레이션할 수 있습니다.

연결 프로파일에 대한 주소 풀을 컨피그레이션하려면 다음 방법 중 한 가지 이상을 사용하십시오.

- **AAA** 서버 - 먼저 주소 풀에 대한 서브넷을 지정하는 threat defense 디바이스에서 네트워크 개체를 컨피그레이션합니다. 그런 다음, RADIUS 서버에서 개체 이름으로 사용자에 대한 Address-Pools(217) 속성을 컨피그레이션합니다. 또한 연결 프로파일에서 인증용 RADIUS 서버를 지정합니다.
- **DHCP** - 먼저 RA VPN에 대한 IPv4 주소 범위를 하나 이상 사용하여 DHCP 서버를 컨피그레이션합니다(DHCP를 사용하여 IPv6 풀을 컨피그레이션할 수는 없음). 그런 다음, DHCP 서버의 IP 주소로 호스트 네트워크 개체를 생성합니다. 그러면 연결 프로파일의 **DHCP Servers(DHCP** 서버**)** 속성에서 이 개체를 선택할 수 있습니다. 최대 10개의 DHCP 서버를 설정할 수 있습니다.

  DHCP 서버에 주소 풀이 여러 개인 경우, 연결 프로파일에 연결하는 그룹 정책에서 **DHCP Scope(DHCP** 범위**)** 속성을 사용해 어떤 풀을 사용할지 선택할 수 있습니다. 풀의 네트워크 주소로 호스트 네트워크 개체를 생성합니다. 예를 들어 DHCP 풀에 192.168.15.0/24 및 192.168.16.0/24가 포함된 경우, DHCP 범위를 192.168.16.0으로 설정하면 192.168.16.0/24 서브넷에서 주소가 선택됩니다.
- 로컬 **IP** 주소 풀 - 먼저 서브넷을 지정하는 네트워크 개체를 최대 6개 생성합니다. IPv4 및 IPv6에 대해 별도 풀을 컨피그레이션할 수 있습니다. 그런 다음, 그룹 정책 또는 연결 프로파일의 **IPv4 Address Pool(IPv4** 주소 풀**)** 및 **IPv6 Address Pool(IPv6** 주소 풀**)** 옵션에서 이러한 개체를 선택합니다. IPv4 및 IPv6 모두 컨피그레이션할 필요는 없고 지원하려는 주소 체계만 컨피그레이션하면 됩니다.

  또한 그룹 정책 및 연결 프로파일 모두에서 풀을 컨피그레이션할 필요는 없습니다. 그룹 정책에서는 연결 프로파일 설정을 재정의하므로 그룹 정책에서 풀을 컨피그레이션하는 경우, 연결 프로파일에서 옵션을 비워두십시오.

  풀은 나열한 순서대로 사용된다는 점에 유의하십시오.

RA VPN에 대한 그룹 정책 컨피그레이션

그룹 정책은 원격 액세스 VPN 연결에 대한 일련의 사용자 중심 속성/값 쌍입니다. 연결 프로파일에서는 터널이 설정된 후 사용자 연결에 대해 조건을 설정하는 그룹 정책을 사용합니다. 그룹 정책을 사용하면 각 사용자에 대해 개별적으로 각 특성을 지정할 필요 없이 사용자 또는 사용자 그룹에 전체 특성 집합을 적용할 수 있습니다.

시스템에는 DfltGrpPolicy라는 이름의 기본 그룹 정책이 포함되어 있습니다. 필요한 서비스를 제공하는 추가 그룹 정책을 만들 수 있습니다.

프로시저

단계 **1** **Device(**디바이스**)** > **Remote Access VPN(**원격 액세스 **VPN)** 그룹에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

현재 얼마나 많은 연결 프로파일 및 그룹 정책이 컨피그레이션되어 있는지 나타내는 요약 정보를 그룹에서 표시합니다.

단계 **2** 목차에서 **Group Policies(**그룹 정책**)**를 클릭합니다.

단계 **3** 다음 중 하나를 수행합니다.

- + 버튼을 클릭하여 새 그룹을 생성합니다. 그룹 정책 페이지에서 속성에 대한 설명은 다음 주제를 참조하십시오.
  - 일반 속성, 25 페이지
  - 세션 설정 속성, 26 페이지
  - 주소 할당 속성, 27 페이지
  - 스플릿 터널링 속성, 27 페이지
  - Secure Client 속성, 28 페이지
  - 트래픽 필터 속성, 30 페이지
  - Windows 브라우저 프록시 속성, 31 페이지
- 기존 그룹 정책을 수정하려면 수정 버튼()을 클릭합니다.
- 더 이상 필요하지 않은 그룹을 삭제하려면 삭제 버튼()을 클릭합니다. 이 그룹은 현재 연결 프로파일에서 사용할 수 없습니다.

일반 속성

그룹 정책의 일반 속성에서는 그룹의 이름 및 기타 기본 설정을 정의합니다. Name(이름) 속성만 필수 속성입니다.

- **Name(**이름**)** - 그룹 정책의 이름입니다. 이름은 최대 64자까지 입력할 수 있고 공백이 허용됩니다.
- **Description(**설명**)** - 그룹 정책에 대한 설명입니다. 설명은 최대 1,024자까지 입력할 수 있습니다.
- **DNS Server(DNS** 서버**)** - VPN에 연결할 때 클라이언트가 도메인 이름 확인에 사용해야 하는 DNS 서버를 정의하는 DNS 서버 그룹을 선택합니다. 필요한 그룹이 아직 정의되지 않은 경우, **Create DNS Group(DNS** 그룹 생성**)**을 클릭하여 바로 생성합니다.
- 배너 - 로그인 시 사용자에게 표시할 배너 텍스트 또는 환영 메시지입니다. 기본값은 배너 없음입니다. 길이는 최대 496자까지 가능합니다. Secure Client 섹션 부분 HTML을 지원합니다. 원격 사용자에게 배너가 적절히 표시되게 하려면
 태그를 사용하여 줄 바꿈을 나타냅니다.
- **Default Domain(**기본 도메인**)** - RA VPN의 사용자에 대한 기본 도메인 이름입니다. example.com 등을 예로 들 수 있습니다. 이 도메인은 정규화되지 않은 호스트 이름(예: serverA.example.com이 아닌 serverA)에 추가됩니다.
- **Secure Client** 프로파일 - +를 클릭하고 이 그룹에 사용할 Secure Client 프로파일을 선택합니다. 연결 프로파일에서 외부 인터페이스에 대해 FQDN(fully-qualified domain name)을 컨피그레이션하는 경우, 기본 프로파일이 생성됩니다. 원하는 클라이언트 프로파일을 직접 업로드할 수도 있습니다. software.cisco.com에서 다운로드하여 설치할 수 있는 독립형 Secure Client 프로파일 편집기를 사용하여 이러한 프로파일을 생성합니다. 클라이언트 프로파일을 선택하지 않으면 Secure Client는 모든 옵션에 대해 기본값을 사용합니다. 이 목록의 항목은 프로파일 자체가 아니라 Secure Client 프로파일 개체입니다. 드롭다운 목록에서 **Create New Secure Client Profile(**새 보안 클라이언트 프로파일 생성**)**을 클릭하면 새 프로파일을 생성하고 업로드할 수 있습니다.

  Secure Client 프로파일 외에 AMP Enabler와 같은 Secure Client 모듈 프로파일을 선택할 수 있습니다. 모듈 유형당 하나의 프로파일을 선택할 수 있습니다.

세션 설정 속성

그룹 정책의 세션 설정에서는 사용자가 VPN을 통해 연결할 수 있는 시간과 설정할 수 있는 별도 연결의 개수를 제어합니다.

- **Maximum Connection Time(**최대 연결 시간**)** - 사용자가 로그아웃했다가 다시 연결하지 않고 VPN에 연결된 상태를 유지할 수 있는 최대 시간을 1~4473924(분)로 입력하거나 비워 둡니다. 기본값은 무제한(비워 둠)이지만 유휴 시간 제한은 계속 적용됩니다.
- **Connection Time Alert Interval(**연결 시간 알림 간격**)** - 최대 연결 시간을 지정하는 경우, 알림 간격에서는 사용자에게 앞으로 다가올 자동 연결 해제에 관해 경고를 표시하기까지 지나야 할 최대 시간을 정의합니다. 사용자는 연결 종료를 선택하고 다시 접속해 타이머를 다시 시작할 수 있습니다. 기본값은 1분입니다. 1분에서 30분까지 지정할 수 있습니다.
- **Idle Time(**유휴 시간**)** - VPN 연결이 자동으로 종료될 때까지 유휴 상태일 수 있는 시간을 1~35791394(분) 범위 내로 입력합니다. 이 연속되는 분 단위 시간 동안 연결에서 통신 활동이 없는 경우, 시스템에서는 연결을 중지합니다. 기본값은 30분입니다.
- **Idle Time Alert Interval(**유휴 시간 알림 간격**)** - 유휴 세션으로 인해 사용자에게 앞으로 다가올 자동 연결 해제에 관해 경고를 표시하기까지 지나야 할 유휴 시간입니다. 어떤 활동에서도 타이머를 재설정할 수 있습니다. 기본값은 1분입니다. 1분에서 30분까지 지정할 수 있습니다.

- **Simultaneous Login Per User(**사용자당 동시 로그인 수**)** - 한 사용자에게 허용되는 동시 연결의 최대 개수입니다. 기본값은 3입니다. 1~2147483647개의 연결을 지정할 수 있습니다. 다수의 동시 연결을 허용하면 보안이 취약해지고 성능이 저하될 수 있습니다.

주소 할당 속성

그룹 정책의 주소 할당 속성에서는 그룹에 대해 IP 주소 풀을 정의합니다. 여기에 정의된 풀은 이 그룹을 사용하는 모든 연결 프로파일에 정의된 풀을 재정의합니다. 연결 프로파일에 정의된 풀을 사용하려면 이러한 설정을 비워둡니다.

- **IPv4 Address Pool(IPv4** 주소 풀**)**, **IPv6 Address Pool(IPv6** 주소 풀**)** - 이 옵션에서는 원격 엔드포인트의 주소 풀을 정의합니다. 클라이언트가 VPN 연결을 설정하는 데 사용하는 IP 버전에 따라 이러한 풀의 주소가 클라이언트에 할당됩니다. 지원하려는 각 IP 유형에 대한 서브넷을 정의하는 네트워크 개체를 선택합니다. 해당 IP 버전을 지원하고 싶지 않은 경우, 목록을 비워두십시오. 예를 들어 IPv4 풀을 10.100.10.0/24로 정의할 수 있습니다. 주소 풀은 외부 인터페이스의 IP 주소와 동일한 서브넷에 있을 수 없습니다.

  로컬 주소 할당에 사용할 최대 6개의 주소 풀로 구성된 목록을 지정할 수 있습니다. 풀을 지정하는 순서는 중요합니다. 시스템에서는 풀이 표시되는 순서에 따라 이 풀에서 주소를 할당합니다.

- **DHCP Scope(DHCP** 범위**)** - 연결 프로파일에서 주소 풀에 대한 DHCP 서버를 컨피그레이션하는 경우, DHCP 범위에서는 이 그룹에 대한 풀에 사용할 서브넷을 식별합니다. 또한 DHCP 서버 주소에는 해당 범위에서 식별하는 동일한 서브넷에 주소가 있어야 합니다. 이 범위를 통해 사용자는 DHCP 서버에 정의된 주소 풀의 하위 집합을 선택하여 이 특정 그룹에 사용할 수 있습니다.

  네트워크 범위를 정의하지 않으면 DHCP 서버에서 구성된 주소 풀 순으로 IP 주소를 할당합니다. 할당되지 않은 주소를 식별할 때까지 풀을 검색합니다.

  범위를 지정하려면 원하는 풀과 동일한 서브넷에서 풀에 라우팅 가능한 주소를 포함하는 네트워크 개체를 선택하거나 생성합니다. DHCP 서버는 이 IP 주소가 속한 서브넷을 확인하고 해당 풀에서 IP 주소를 할당합니다.

  라우팅을 위해 가능한 경우 항상 인터페이스의 IP 주소를 사용하는 것이 좋습니다. 예를 들어 풀이 10.100.10.2-10.100.10.254이고 인터페이스 주소가 10.100.10.1/24이면 DHCP 범위로 10.100.10.1을 사용합니다. 네트워크 번호를 사용하지 마십시오. 개체가 아직 없는 경우, **Create New Network(**새 네트워크 생성**)**를 클릭합니다. IPv4 주소 지정에만 DHCP를 사용할 수 있습니다. 선택한 주소가 인터페이스 주소가 아닌 경우 범위 주소에 대한 고정 경로를 생성해야 할 수 있습니다.

스플릿 터널링 속성

그룹 정책의 스플릿 터널링 속성에서는 내부 네트워크로 가는 트래픽과 외부로 가는 트래픽을 시스템에서 각각 분별하여 처리하는 방식을 정의합니다. 스플릿 터널링은 일부 네트워크 트래픽이 VPN 터널(암호화됨)을 통과하도록 유도하고 나머지 네트워크 트래픽은 VPN 터널 외부(암호화되지 않음 또는 일반 텍스트 형식)로 보냅니다.

- **IPv4 Split Tunneling(IPv4** 스플릿 터널링**)**, **IPv6 Split Tunneling(IPv6** 스플릿 터널링**)** - 트래픽에서 IPv4와 IPv6 중 어떤 주소 지정을 사용하는지에 따라 다른 옵션을 지정할 수 있지만, 각각의

경우 옵션은 동일합니다. 스플릿 터널링을 활성화하려는 경우, 네트워크 개체를 선택해야 하는 옵션 중 하나를 지정합니다.

- **Allow all traffic over tunnel(**터널을 지나는 모든 트래픽 허용**)** - 스플릿 터널링은 실행하지 마십시오. 사용자가 RA VPN 연결을 하면 사용자의 모든 트래픽은 보호된 터널을 통과합니다. 이는 기본값입니다. 또한 이 기본값은 가장 안전한 옵션으로 간주됩니다.
- **Allow specified traffic over tunnel(**터널을 지나는 지정된 트래픽 허용**)** - 대상 네트워크 및 호스트 주소를 정의하는 네트워크 개체를 선택합니다. 이러한 대상으로 가는 모든 트래픽은 보호된 터널을 통과합니다. 기타 대상으로 가는 트래픽은 클라이언트에서 터널 외부 연결(예: 로컬 Wi-Fi 또는 네트워크 연결)로 라우팅합니다.
- **Exclude networks specified below(**아래에 지정된 네트워크 제외**)** - 대상 네트워크 또는 호스트 주소를 정의하는 네트워크 개체를 선택합니다. 이러한 대상으로 가는 모든 트래픽은 클라이언트에서 터널 외부 연결로 라우팅합니다. 기타 대상으로 가는 트래픽은 터널을 통과합니다.

- **Split DNS(**스플릿 **DNS)** - 보안 연결을 통해 일부 DNS 요청을 전송하도록 시스템을 컨피그레이션함과 동시에 클라이언트가 클라이언트에 컨피그레이션된 DNS 서버로 다른 DNS 요청을 전송하도록 허용할 수 있습니다. 다음 DNS 동작을 컨피그레이션할 수 있습니다.
  - **Send DNS Request as per split tunnel policy(**스플릿 터널 정책에 따라 **DNS** 요청 전송**)** - 이 옵션을 사용하면 스플릿 터널 옵션을 정의하는 것과 동일한 방식으로 DNS 요청이 처리됩니다. 스플릿 터널링을 활성화하는 경우, DNS 요청은 대상 주소에 근거하여 전송됩니다. 스플릿 터널링을 활성화하지 않는 경우, 모든 DNS 요청은 보호된 연결을 경유해 전송됩니다.
  - **Always send DNS requests over tunnel(**항상 터널을 통해 **DNS** 요청 전송**)** - 스플릿 터널링을 활성화하되 모든 DNS 요청을 보호된 연결을 경유해 그룹에 정의된 DNS 서버로 전송하려는 경우, 이 옵션을 선택합니다.
  - **Send only specified domains over tunnel(**지정된 도메인만 터널을 통해 전송**)** - 보호된 DNS 서버에서 특정 도메인에 대해서만 주소를 확인하게 하고 싶은 경우, 이 옵션을 선택합니다. 그런 다음, 도메인 이름을 쉼표로 구분하여 해당 도메인을 지정합니다. example.com, example1.com을 예로 들 수 있습니다. 내부 DNS 서버에서는 내부 도메인의 이름을 확인하고 외부 DNS 서버에서는 다른 모든 인터넷 트래픽을 처리하게 하려는 경우, 이 옵션을 사용합니다.

Secure Client 속성

그룹 정책의 Secure Client 속성에서는 원격 액세스 VPN 연결에 대해 Secure Client에서 사용하는 일부 SSL 및 연결 설정을 정의합니다.

SSL 설정

- **Enable Datagram Transport Layer Security (DTLS)(DTLS(Datagram Transport Layer Security)** 활성화**)** — Secure Client에서 2개의 터널(SSL 터널 및 DTLS 터널)을 동시에 사용하도록 허용할지 여부를 선택합니다. DTLS를 사용하면 일부 SSL 연결에서 발생하는 레이턴시 및 대역폭 문제를 방지하고 패킷 지연에 민감한 실시간 애플리케이션의 성능을 개선할 수 있습니다. DTLS를

활성화하지 않은 경우에는 SSL VPN 연결을 설정하는 Secure Client 사용자가 SSL 터널만 사용하여 연결합니다.

- **DTLS Compression(DTLS** 압축**)** — LZS를 사용하여 이 그룹에 대한 DTLS(Datagram Transport Layer Security) 연결을 압축할지 여부를 선택합니다. DTLS 압축은 기본적으로 비활성화되어 있습니다.
- **SSL Compression(SSL** 압축**)** — 데이터 압축을 활성화할지 여부, 활성화하는 경우 사용할 데이터 압축 방법(**Deflate(**압축 해제**)** 또는 **LZS**)을 선택합니다. SSL 압축은 기본적으로 **Disabled(**비활성화**)** 상태입니다. 데이터를 압축하면 전송 속도가 빨라지지만 각 사용자 세션에 대한 메모리 요건 및 CPU 사용량이 증가합니다. 따라서 SSL 압축으로 인해 디바이스의 전체 처리량은 줄어듭니다.
- **SSL Rekey Method(SSL** 키 재입력 방법**)**, **SSL Rekey Interval(SSL** 키 재입력 간격**)** — 클라이언트는 VPN 연결에 키를 재입력하여 암호화 키 및 초기화 벡터를 재협상할 수 있어 연결 보안이 강화됩니다. **None(**없음**)**을 선택하여 키 재입력을 비활성화합니다. 키 재입력을 활성화하려면 **New Tunnel(**새 터널**)**을 선택하여 매번 새 터널을 생성합니다. (**Existing Tunnel(**기존 터널**)** 옵션을 선택하면 **New Tunnle(**새 터널**)**과 동일한 조치가 수행됩니다.) 키 재입력을 활성화하는 경우, 키 재입력 간격도 설정하십시오. 기본값은 4분입니다. 4~10080분(일주일) 범위 내에서 간격을 설정할 수 있습니다.

연결 설정

- **Ignore the DF (Don't Fragment) bit(DF(Don't Fragment)** 비트 무시**)** — 단편화해야 하는 패킷에서 DF(Don't Fragment) 비트를 무시할지 여부를 선택합니다. 이 옵션을 선택하면 DF 비트가 설정된 패킷의 강제 단편화가 허용되므로 이 패킷이 터널을 통과할 수 있습니다.
- **Client Bypass Protocol(**클라이언트 우회 프로토콜**)** — 이 옵션을 선택하면 보안 게이트웨이에서 IPv6 트래픽만 예상할 때 IPv4 트래픽을 관리하는 방법 또는 IPv4 트래픽만 예상할 때 IPv6 트래픽을 관리하는 방법을 컨피그레이션할 수 있습니다.

  Secure Client에서 헤드엔드와의 VPN 연결을 수행할 때 헤드엔드에서는 IPv4 주소나 IPv6 주소 또는 IPv4 및 IPv6 주소 모두를 지정합니다. 헤드엔드에서 Secure Client 연결에 IPv4 주소만 또는 IPv6 주소만 지정할 경우, 헤드엔드에서 IP 주소를 지정하지 않은 네트워크 트래픽을 삭제하거나 이 트래픽이 헤드엔드를 우회하여 암호화되지 않은 또는 "일반 텍스트" 형태(활성화 및 확인된 상태)로 클라이언트에서 전송되는 것을 허용하도록 Client Bypass Protocol(클라이언트 우회 프로토콜)을 컨피그레이션할 수 있습니다.

  예를 들어 보안 게이트웨이에서 Secure Client 연결에 IPv4 주소만 지정하고 엔드포인트는 이중 스택이라고 가정합시다. 엔드포인트가 IPv6 주소에 연결하려고 시도할 때 클라이언트 우회 프로토콜이 비활성화된 경우 IPv6 트래픽이 끊기지만 클라이언트 우회 프로토콜이 활성화된 경우, IPv6 트래픽은 클라이언트에서 암호화되지 않은 상태로 전송됩니다.
- **MTU** — Secure Client에서 설정한 SSL VPN 연결의 MTU(Maximum Transmission Unit)입니다. 기본값은 1406바이트입니다. 범위는 576~1462바이트입니다.
- **Keepalive Messages Between Secure Client and VPN Gateway(**보안 클라이언트와 **VPN** 게이트웨이 간의 연결 유지 메시지**)** - 피어 간에 연결 유지 메시지를 교환하여 터널에서 데이터를 송수신

하는 데 사용할 수 있다는 것을 시연할지 여부를 선택합니다. 연결 유지 메시지는 설정된 간격에 따라 전송됩니다. 기본 간격은 20초, 유효 범위는 15~600초입니다.

- **DPD on Gateway Side Interval(**게이트웨이 측 간격의 **DPD)**, **DPD on Client Side Interval(**클라이언트 측 간격의 **DPD)** — DPD(Dead Peer Detection)를 활성화하면 피어가 더 이상 응답하지 않을 경우 VPN 게이트웨이 또는 VPN 클라이언트를 신속하게 탐지할 수 있습니다. 게이트웨이 또는 클라이언트 DPD를 별도로 활성화할 수 있습니다. DPD 메시지 전송의 기본 간격은 30초입니다. 간격은 5-3600초 사이일 수 있습니다.

트래픽 필터 속성

그룹 정책의 트래픽 필터 속성에서는 그룹에 할당된 사용자에게 부과하고 싶은 제한 사항을 정의합니다. 액세스 제어 정책 규칙을 생성하는 대신 이 속성을 사용해 RA VPN 사용자를 호스트 또는 서브넷 주소 및 프로토콜, VLAN에 따라 특정 리소스로 제한할 수 있습니다.

기본적으로 그룹 정책에 따라 RA VPN 사용자는 보호된 네트워크의 어떤 대상에 액세스하는 것도 제한되지 않습니다.

- **Access List Filter(**액세스 목록 필터**)** - 확장된 ACL(액세스 제어 목록)을 사용하여 액세스를 제한합니다. 스마트 CLI 확장 ACL 개체를 선택하거나 **Create Extended Access List(**확장 액세스 목록 생성**)**를 클릭하여 바로 생성합니다.

  확장 ACL을 통해 소스 주소, 대상 주소 및 프로토콜(예: IP 또는 TCP)을 기준으로 필터링할 수 있습니다. ACL은 하향식, 최초 일치 방식에 따라 평가되므로 특정 규칙이 다수의 일반 규칙보다 먼저 배치되도록 보장합니다. ACL의 끝에는 암묵적 "deny any(모두 거부)"가 있으므로 서브넷 몇 개에 대한 액세스만 거부하고 다른 모든 액세스는 허용하려면 ACL의 끝에 "permit any(모두 허용)" 규칙을 포함하십시오. VPN 필터는 초기 연결에만 적용됩니다. 애플리케이션 검사 작업으로 인해 열리는 SIP 미디어 연결과 같은 보조 연결에는 적용되지 않습니다.

  확장 ACL 스마트 CLI 개체를 수정하는 중에는 네트워크 개체를 생성할 수 없으므로 그룹 정책을 수정하기 전에 ACL을 생성해야 합니다. 그러지 않는 경우, 개체만 생성할 수 있습니다. 그런 다음 다시 돌아가 네트워크 개체를 생성한 후 필요한 모든 액세스 제어 항목을 생성하면 됩니다. ACL을 생성하려면 **Device(**디바이스**)** > **Advanced Configuration(**고급 구성**)** > **Smart CLI(**스마트 **CLI)** > **Objects(**개체**)**로 이동하여 개체를 생성하고 **Extended Access List(**확장 액세스 목록**)**를 개체 유형으로 선택합니다. 예시는 그룹별로 RA VPN 액세스를 제어하는 방법, 71 페이지의 내용을 참조하십시오.

- **Restrict VPN to VLAN(VPN**을 **VLAN**으로 제한**)** - “VLAN 매핑”이라고도 하는 이 속성에서는 이 그룹 정책이 적용되는 세션에 이그레스(egress) VLAN 인터페이스를 지정합니다. 시스템에서는 이 그룹에서 나오는 모든 트래픽을 선택한 VLAN으로 전달합니다.

  이 특성을 사용하여 그룹 정책에 VLAN을 할당하면 액세스 제어를 간소화할 수 있습니다. ACL을 사용하여 세션의 트래픽을 필터링하는 방법 대신 이 속성에 값을 할당하는 방법도 가능합니다. 디바이스에서 하위 인터페이스에 정의된 VLAN 번호를 반드시 지정하십시오. 값의 범위는 1에서 4094까지입니다.

Windows 브라우저 프록시 속성

그룹 정책의 Windows 브라우저 프록시 속성에서는 사용자의 브라우저에 정의된 프록시의 작동 방식과 작동 여부를 결정합니다.

Browser Proxy During VPN Session(VPN 세션 중 브라우저 프록시**)**에 대해 다음 값 중 하나를 선택할 수 있습니다.

- **No change in endpoint settings(**엔드포인트 설정에 변경 사항 없음**)** - 이 옵션을 통해 사용자는 HTTP에 대해 브라우저 프록시를 컨피그레이션하거나 컨피그레이션하지 않을 수 있으며 컨피그레이션되어 있는 경우 프록시를 사용할 수 있습니다.
- **Disable browser proxy(**브라우저 프록시 비활성화**)** - 브라우저에 대해 정의된 프록시(있는 경우)를 사용하지 않습니다. 이 경우 프록시를 통해 브라우저 연결이 설정되지 않습니다.
- **Auto detect settings(**설정 자동 탐지**)** - 클라이언트 디바이스에 대해 브라우저에서 자동 프록시 서버 감지를 사용하도록 활성화합니다.
- **Use custom settings(**사용자 정의 설정 사용**)** - HTTP 트래픽에 대해 모든 클라이언트 디바이스에서 사용해야 하는 프록시를 정의합니다. 다음 설정을 구성합니다.
  - **Proxy Server IP or Hostname(**프록시 서버 **IP** 또는 호스트네임**)**, **Port(**포트**)** - 프록시 서버의 IP 주소 또는 호스트네임, 프록시 서버에서 프록시 연결에 사용하는 포트입니다. 호스트와 포트를 합해 100자를 초과할 수 없습니다.
  - **Browser Exemption List(**브라우저 면제 목록**)** - 면제 목록의 호스트/포트에 대한 연결은 프록시를 통과하지 않습니다. 프록시를 사용해서는 안 되는 대상에 대해 모든 호스트/포트 값을 추가합니다. www.example.com port 80을 예로 들 수 있습니다. **Add(**추가**)** 링크를 클릭하여 목록에 항목을 추가합니다. 항목을 삭제하려면 휴지통 아이콘을 클릭합니다. 모든 주소와 포트를 합한 전체 프록시 예외 목록은 255자를 초과할 수 없습니다.

원격 액세스 VPN 모니터링

원격 액세스 VPN 연결을 모니터링하고 트러블슈팅하려면 CLI 콘솔을 열거나 디바이스 CLI에 로그인하여 다음 명령을 사용합니다.

- **show vpn-sessiondb** VPN 세션에 대한 정보를 표시합니다. **clear vpn-sessiondb** 명령을 사용하여 이 통계를 재설정할 수 있습니다.
- **show webvpn** *keyword* 통계 및 설치된 AnyConnect 이미지를 비롯하여 원격 액세스 VPN 컨피그레이션에 대한 정보를 표시합니다. 사용 가능한 키워드를 보려면 **show webvpn ?**를 입력합니다.
- **show aaa-server** 원격 액세스 VPN에 사용되는 디렉터리 서버에 대한 통계를 표시합니다.

원격 액세스 VPN 트러블슈팅

원격 액세스 VPN 연결 문제는 클라이언트 또는 threat defense 디바이스 컨피그레이션에서 발생할 수 있습니다. 다음 항목에서는 발생할 수 있는 주요 트러블슈팅 문제에 관해 설명합니다.

SSL 연결 문제 트러블슈팅

사용자가 Secure Client를 다운로드하기 위해 외부 IP 주소에 대한 초기 비Secure Client SSL 연결을 설정할 수 없는 경우 다음 작업을 수행합니다.

1. 원격 액세스 VPN 연결 프로파일에 기본 포트가 아닌 포트를 구성한 경우 사용자가 URL에 포트 번호를 포함하고 있는지 확인합니다(예: https://ravpn.example.com:4443).
2. 클라이언트 워크스테이션에서 외부 인터페이스의 IP 주소에 대해 Ping을 수행할 수 있는지 확인합니다. ping을 수행할 수 없는 경우 사용자 워크스테이션에서 해당 주소로의 경로가 없는 이유를 확인합니다.
3. 클라이언트 워크스테이션에서 RA(원격 액세스) VPN 연결 프로파일에 정의되어 있는 외부 인터페이스의 FQDN(Fully Qualified Domain name)에 대해 ping을 수행할 수 있는지 확인합니다. IP 주소의 ping은 가능한데 FQDN의 ping은 불가능한 경우에는 클라이언트 및 RA VPN 연결 프로파일에서 사용하는 DNS 서버를 업데이트하여 FQDN에서 IP 주소로의 매핑을 추가해야 합니다.
4. 사용자가 외부 인터페이스에서 제공하는 인증서를 수락하는지 확인합니다. 사용자는 해당 인증서를 영구적으로 수락해야 합니다.
5. RA VPN 연결 컨피그레이션을 검사하여 올바른 외부 인터페이스를 선택했는지 확인합니다. RA VPN 사용자를 대상으로 하는 외부 인터페이스가 아닌 내부 네트워크를 대상으로 하는 내부 인터페이스를 실수로 선택하는 경우가 많습니다.
6. SSL 암호화가 정상적으로 구성되어 있으면 외부 스니퍼를 사용하여 TCP 3방향 핸드셰이크에 성공하는지 확인합니다.

Secure Client 다운로드 및 설치 문제 해결

사용자가 외부 인터페이스로의 SSL 연결을 설정할 수 있는데 Secure Client 패키지를 다운로드하여 설치할 수는 없는 경우 다음 사항을 고려하십시오.

- 클라이언트 운영 체제용 Secure Client 패키지를 업로드했는지 확인합니다. 예를 들어 사용자 워크스테이션에서 Linux를 실행하는데 Linux Secure Client 이미지를 업로드하지 않은 경우에는 설치할 수 있는 패키지가 없습니다.
- Windows 클라이언트의 경우 사용자에게는 소프트웨어를 설치할 수 있는 관리자 권한이 있어야 합니다.
- Windows 클라이언트의 경우 워크스테이션에서 ActiveX를 활성화하거나 Java JRE 1.5 이상(JRE 7 권장)을 설치해야 합니다.

- Safari 브라우저의 경우에는 Java를 활성화해야 합니다.
- 다른 브라우저를 사용해 보면 특정 브라우저에서만 다운로드와 설치에 실패할 수도 있습니다.

Secure Client 연결 문제 해결

사용자가 외부 인터페이스에 연결하여 Secure Client를 다운로드하고 설치할 수 있었는데 그 후에 Secure Client를 사용한 연결을 완료할 수는 없는 경우 다음 사항을 고려하십시오.

- 인증에 실패하는 경우, 사용자가 올바른 사용자 이름과 암호를 입력했는지, 사용자 이름이 인증 서버에 올바르게 정의되어 있는지 확인합니다. 인증 서버는 데이터 인터페이스 중 하나를 통해서도 사용할 수 있어야 합니다.

참고 인증 서버가 외부 네트워크에 있는 경우, 외부 네트워크에 대한 사이트 대 사이트 VPN 연결을 컨피그레이션하고 VPN 내에 원격 액세스 VPN 인터페이스 주소를 포함해야 합니다. 자세한 내용은 원격 액세스 VPN을 통해 외부 네트워크에서 디렉터리 서버를 사용하는 방법, 56 페이지를 참조해 주십시오.

- RA(원격 액세스) VPN 연결 프로필에서 외부 인터페이스에 대한 FQDN(Fully Qualified Domain Name)을 구성한 경우 클라이언트 디바이스에서 FQDN에 대해 ping을 수행할 수 있는지 확인합니다. IP 주소의 ping은 가능한데 FQDN의 ping은 불가능한 경우에는 클라이언트 및 RA VPN 연결 프로파일에서 사용하는 DNS 서버를 업데이트하여 FQDN에서 IP 주소로의 매핑을 추가해야 합니다. 외부 인터페이스의 FQDN을 지정할 때 생성된 기본 Secure Client 프로파일을 사용하는 경우, 사용자는 DNS가 업데이트될 때까지 IP 주소를 사용하도록 서버 주소를 수정해야 합니다.
- 사용자가 외부 인터페이스에서 제공하는 인증서를 수락하는지 확인합니다. 사용자는 해당 인증서를 영구적으로 수락해야 합니다.
- 사용자의 Secure Client에 여러 연결 프로파일이 포함되어 있으면 사용자가 올바른 프로파일을 선택하는지 확인합니다.
- 클라이언트 쪽의 모든 설정이 올바른 것으로 확인되면 threat defense 디바이스에 대한 SSH 연결을 설정하고 **debug webvpn** 명령을 입력합니다. 그런 후에 연결 시도 중에 발급된 메시지를 검사합니다.

RA VPN 트래픽 흐름 문제 트러블슈팅

사용자가 보안 RA(원격 액세스) VPN 연결을 설정할 수는 있는데 트래픽을 보내고 받을 수는 없으면 다음 작업을 수행합니다.

1. 클라이언트의 연결을 끊었다가 다시 연결합니다. 이렇게 하면 문제가 해결될 수도 있습니다.
2. Secure Client에서 트래픽 통계를 점검하여 전송 카운터와 수신 카운터의 값이 모두 증가하는지를 확인합니다. 수신된 패킷 수가 0으로 유지되는 경우, threat defense 디바이스에서 트래픽을 전혀

반환하지 않고 있는 것입니다. threat defense 컨피그레이션에 문제가 있을 가능성이 있습니다. 흔히 발생하는 문제는 다음과 같습니다.

- 액세스 규칙이 트래픽을 차단하고 있습니다. 액세스 제어 정책에서 내부 네트워크와 RA VPN 주소 풀 간의 트래픽을 차단하는 규칙을 확인하십시오. 기본 작업이 트래픽 차단인 경우에는 명시적 허용 규칙을 생성해야 할 수 있습니다.
- VPN 필터에서 트래픽을 차단하고 있습니다. 연결 프로파일에 대한 그룹 정책에 컨피그레이션된 ACL 트래픽 필터 또는 VLAN 필터를 확인합니다. 또한 파일 정책을 액세스 제어 규칙의 트래픽에 적용하는 경우, 파일 액세스나 악성코드 또는 둘 다를 제어하려면 파일 이벤트 메시지를 외부 syslog 서버로 전송하도록 시스템을 컨피그레이션할 수 있습니다.
- RA VPN 트래픽에 대해 NAT 규칙이 우회되고 있지 않습니다. 모든 내부 인터페이스의 RA VPN 연결에 대해 NAT 제외가 구성되어 있는지 확인하십시오. 또는 NAT 규칙이 내부 네트워크 및 인터페이스와 RA VPN 주소 풀 및 외부 인터페이스 간의 통신을 차단하지 않는지 확인하십시오.
- 경로가 잘못 구성되어 있습니다. 정의된 모든 경로가 유효하며 올바르게 동작하고 있는지 확인하십시오. 예를 들어, 외부 인터페이스에 고정 IP 주소가 정의되어 있는 경우 0.0.0.0/0 및 ::/0에 대한 기본 경로가 라우팅 테이블에 포함되어 있는지 확인하십시오.
- RA VPN에 구성된 DNS 서버 및 도메인 이름이 올바르며 클라이언트 시스템이 올바른 DNS 서버와 도메인 이름을 사용하고 있는지 확인하십시오. DNS 서버에 연결할 수 있는지 확인합니다.
- RA VPN의 스플릿 터널링을 활성화하는 경우, 지정된 내부 네트워크로 전송되는 트래픽은 터널을 통과하고 기타 모든 트래픽은 터널을 우회하는지(threat defense 디바이스에서 해당 트래픽을 확인할 수 없음) 확인합니다.

3. threat defense 디바이스에 SSH 연결을 설정하여 원격 액세스 VPN에 대해 트래픽이 전송 및 수신되고 있는지 확인합니다. 이렇게 하려면 다음 명령을 사용합니다.
   - **show webvpn anyconnect**
   - **show vpn-sessiondb**

원격 액세스 VPN의 예시

다음에는 원격 액세스 VPN을 구성하는 예시가 나와 있습니다.

RADIUS CoA(Change of Authorization) 구현 방법

동적 인증이라고도 하는 RADIUS CoA(Change of Authorization)에서는 threat defense 원격 액세스 VPN에 대한 엔드포인트 보안을 제공합니다. RA VPN의 주요 당면 과제는 감염된 엔드포인트로부터 내부 네트워크를 보호하는 것입니다. 또한 엔드포인트에 대한 공격을 해결하여 바이러스 또는 악성코드의 침해를 받을 때 엔드포인트 자체를 보호하는 것입니다. RA VPN 세션 전, 중, 후 모든 단계에서 엔

드포인트와 내부 네트워크를 보호해야 합니다. RADIUS CoA 기능을 통해 이 목표를 달성할 수 있습니다.

Cisco Identity Services Engine(ISE) RADIUS 서버를 사용하는 경우, CoA(Change of Authorization) 정책 시행을 컨피그레이션할 수 있습니다.

ISE CoA(Change of Authorization) 기능에서는 설정 후 AAA(인증, 권한 부여 및 계정 관리) 세션의 속성을 변경할 수 있는 메커니즘을 제공합니다. 정책에서 AAA의 사용자 또는 사용자 그룹을 변경하는 경우, ISE에서는 threat defense 디바이스로 CoA 메시지를 전송하여 인증을 다시 시작하고 새 정책을 적용합니다. IPEP(Inline Posture Enforcement Point: 인라인 보안 상태 시행 지점)에는 threat defense 디바이스로 설정된 각 VPN 세션에 대한 ACL(Access Control List: 액세스 제어 목록)이 필요하지 않습니다.

다음 주제에서는 CoA의 작동 방식 및 컨피그레이션 방법에 대해 설명합니다.

CoA(Change of Authorization)를 위한 시스템 흐름

Cisco ISE에는 프로세스, 파일, 레지스트리 항목, 안티바이러스 보호, 안티스파이웨어 보호, 호스트에 설치된 방화벽 소프트웨어 등의 기준에 대한 엔드포인트의 규정 준수를 평가하는 클라이언트 보안 상태 에이전트가 있습니다. 관리자는 엔드포인트에서 규정을 준수할 때까지 네트워크 액세스를 제한하거나 로컬 사용자 권한을 격상하여 보안정책 교정 사례를 설정할 수 있습니다. ISE Posture는 클라이언트 측 평가를 실시합니다. 클라이언트는 ISE에서 보안 상태 요건 정책을 수신하고 보안 상태 데이터 수집을 수행하며 결과를 정책과 비교하여 평가 결과를 ISE로 반송합니다.

다음은 CoA(Change of Authorization)를 위한 threat defense 디바이스, ISE, RA VPN 클라이언트 간 시스템 흐름을 설명한 것입니다.

1. 원격 사용자는 threat defense 디바이스에서 Secure Client를 사용하여 RA VPN 세션을 시작합니다.
2. threat defense 디바이스에서는 ISE 서버로 해당 사용자에 대한 RADIUS Access-Request 메시지를 전송합니다.
3. 이 시점에는 클라이언트 보안 상태를 알 수 없기 때문에 ISE에서는 알 수 없는 보안 상태에 대해 컨피그레이션된 권한 부여 정책에 사용자를 매칭합니다. 이 정책에서는 ISE가 RADIUS Access-Accept 응답에서 threat defense로 전송하는 다음 cisco-av-pair 옵션을 정의합니다.
   - **url-redirect-acl=***acl_name*, 여기서 *acl_name*은 threat defense 디바이스에 컨피그레이션된 확장 ACL의 이름입니다. 이 ACL에서는 ISE 서버로 리디렉션되어야 할 사용자 트래픽, 즉 HTTP 트래픽을 정의합니다. 예를 들면 다음과 같습니다.

     ```
     url-redirect-acl=redirect
     ```

   - **url-redirect=***url*, 여기서 URL은 트래픽이 리디렉션되어야 할 대상 URL입니다. 예를 들면 다음과 같습니다.

     ```
     url-redirect=https://ise2.example.com:8443/guestportal/gateway?sessionId=xx&action=cpp
     ```

   호스트네임을 확인할 수 있도록 데이터 인터페이스에 대해 DNS를 컨피그레이션해야 합니다. 또한 연결 프로파일에 대한 그룹 정책에서 트래픽 필터링을 컨피그레이션하는 경우, 클라이언트 풀에서 포트(예시의 TCP/8443)를 통해 ISE 서버에 연결할 수 있는지 확인합니다.

4. threat defense 디바이스에서는 RADIUS Accounting-Request 시작 패킷을 전송하고 ISE에서 오는 응답을 수신합니다. 계정 관리 요청에는 세션 ID, VPN 클라이언트의 외부 IP 주소, threat defense 디바이스의 IP 주소를 포함한 세션의 모든 상세정보가 포함되어 있습니다. ISE에서는 세션 ID를 사용해 해당 세션을 식별합니다. threat defense 디바이스에서도 주기적인 임시 계정 정보를 전송할 수 있습니다. 여기서 가장 중요한 속성은 threat defense 디바이스에서 클라이언트에 할당하는 IP 주소가 있는 Framed-IP-Address입니다.
5. 알 수 없는 보안 상태 중에 threat defense 디바이스에서는 리디렉션 ACL과 일치하는 클라이언트에서 오는 트래픽을 리디렉션 URL로 리디렉션합니다. ISE에서는 클라이언트에 필수 보안 상태 규정 준수 모듈이 있는지 확인하고, 필요한 경우 이 모듈을 설치하라는 메시지를 사용자에게 표시합니다.
6. 클라이언트 디바이스에 에이전트를 설치하고 나면 ISE 보안 상태 정책에 구성된 확인 작업이 자동으로 수행됩니다. 클라이언트는 ISE와 직접 통신합니다. 클라이언트는 ISE에 보안 상태 보고서를 전송하는데, 여기에는 SWISS 프로토콜 및 포트 TCP/UDP 8905를 사용하는 여러 교환이 포함될 수 있습니다.
7. ISE는 에이전트에서 보안 상태 보고서를 받으면 권한 부여 규칙을 다시 한번 처리합니다. 이때 보안 상태 결과를 알 수 있고 이제 다른 규칙에서는 클라이언트와 일치합니다. ISE에서는 규정 준수 또는 미준수 엔드포인트에 대한 다운로드 가능 ACL(DACL)을 포함하는 RADIUS CoA 패킷을 전송합니다. 예를 들어 준수 DACL에서는 모든 액세스를 허용할 수 있지만, 미준수 DACL에서는 모든 액세스를 거부합니다. DACL의 콘텐츠는 ISE 관리자의 책임입니다.
8. threat defense 디바이스에서는 리디렉션을 제거합니다. 이 디바이스에서 DACL을 캐싱하지 않는 경우, ISE에서 다운로드할 수 있도록 Access-Request를 전송해야 합니다. 특정 DACL은 VPN 세션에 연결되어 있으므로 디바이스 컨피그레이션의 일부가 되지 않습니다.
9. 다음번에 RA VPN 사용자가 웹 페이지에 액세스하려 할 때 사용자는 해당 세션에 대해 threat defense 디바이스에 설치된 DACL에서 허용하는 리소스에 액세스할 수 있습니다.

참고 엔드포인트에서 모든 필수 요건을 충족하지 못하고 수동 교정이 필요한 경우, Secure Client에서 교정 창이 열려 작업이 필요한 항목이 표시됩니다. 보안정책 교정 창은 네트워크 활동의 업데이트가 팝업으로 표시되어 방해하거나 중단하지 않도록 배경에서 실행됩니다. 사용자는 Secure Client의 ISE 보안 상태 바둑판식 배열 부분에 있는 **Details(**상세정보**)**를 클릭하여 탐지된 항목과 네트워크에 연결하기 위해 필요한 업데이트를 확인할 수 있습니다.

Threat Defense 디바이스에서 COA(Change of Authorization) 컨피그레이션

CoA(Change of Authorization) 정책의 대부분은 ISE 서버에서 컨피그레이션됩니다. 그러나 ISE에 올바르게 연결하려면 threat defense 디바이스를 컨피그레이션해야 합니다. 다음 절차에서는 컨피그레이션 중에서 threat defense 측을 컨피그레이션하는 방법에 대해 설명합니다.

시작하기 전에

모든 개체에서 호스트네임을 사용하는 경우, 데이터 인터페이스에 사용할 DNS 서버를 데이터 및 관리 트래픽용 DNS 설정에 설명된 대로 컨피그레이션하십시오. 일반적으로 시스템이 온전히 작동하도록 어떤 식으로든 DNS를 컨피그레이션해야 합니다.

프로시저

단계 **1** 초기 연결을 ISE로 리디렉션하기 위한 확장 ACL(Access Control List)을 컨피그레이션합니다.

리디렉션 ACL의 목적은 초기 트래픽을 ISE로 전송하여 ISE에서 클라이언트 보안 상태를 평가할 수 있게 하는 것입니다. ACL에서는 ISE에 HTTPS 트래픽을 전송해야 하지만, 이미 ISE가 대상으로 지정된 트래픽 또는 이름 확인을 위해 DNS 서버로 전송되는 트래픽은 전송해서는 안 됩니다. 샘플 리디렉션 ACL은 다음과 같이 표시될 수 있습니다.

```
access-list redirect extended deny ip any host <ISE server IP>
access-list redirect extended deny ip any host <DNS server IP>
access-list redirect extended deny icmp any any
access-list redirect extended permit tcp any any eq www
```

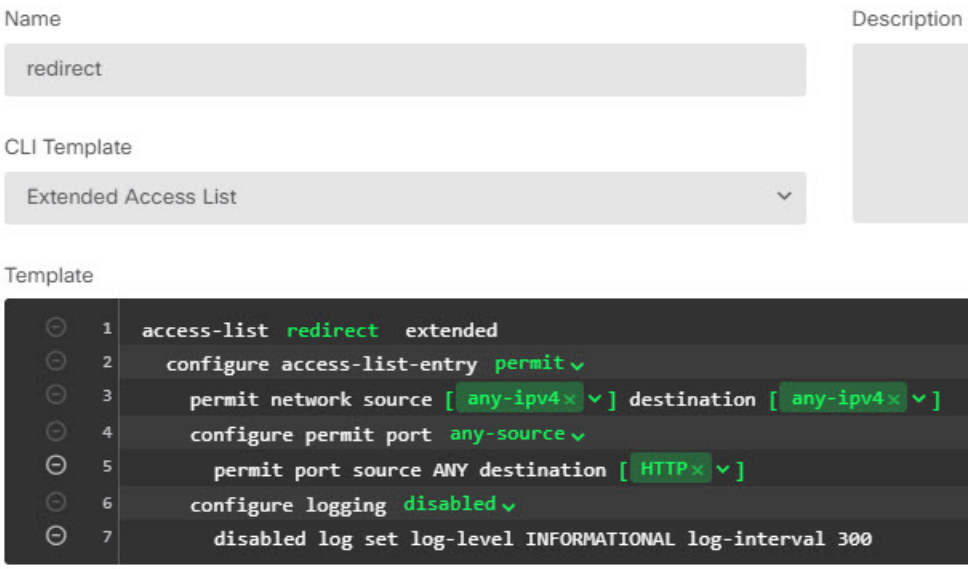
하지만 ACL에는 마지막 ACE(액세스 제어 항목)인 암시적 “deny any any”가 있다는 점에 유의하십시오. 이 예에서는 TCP 포트 www(즉 포트 80)와 일치하는 마지막 ACE가 첫 ACE 3개와 일치하는 모든 트래픽과 일치하지 않습니다. 따라서 이 ACE 3개는 이중화됩니다. 마지막 ACE로 ACL을 생성하기만 해도 동일한 결과를 얻을 수 있습니다.

리디렉션 ACL의 허용 및 거부 작업에서는 일치하는 것은 허용하고 일치하지 않는 것은 거부하여 ACL과 일치하는 트래픽을 확인할 뿐이라는 점에 유의하십시오. 트래픽이 실제로 차단되는 경우는 없으며, 거부된 트래픽은 ISE로 리디렉션되지 않을 뿐입니다.

리디렉션 ACL을 생성하려면 스마트 CLI 개체를 컨피그레이션해야 합니다.

a) **Device(**디바이스**)** > **Advanced Configuration(**고급 컨피그레이션**)** > **Smart CLI(**스마트 **CLI)** > **Objects(**개체**)**를 선택합니다.
b) +를 클릭하여 새 개체를 생성합니다.
c) ACL의 이름을 입력합니다. 예: **redirect(**리디렉션**)**.
d) **CLI Template(CLI** 템플릿**)**에서 **Extended Access List(**확장 액세스 목록**)**를 선택합니다.
e) **Template(**템플릿**)** 본문에서 다음과 같이 컨피그레이션합니다.
   - configure access-list-entry action = permit
   - source-network = any-ipv4
   - destination-network = any-ipv4
   - configure permit port = any-source
   - destination-port = HTTP
   - configure logging = disabled

ACE는 다음과 같이 표시되어야 합니다.



f) **OK(**확인**)**를 클릭합니다.

이 ACL은 다음번에 변경 사항을 구축할 때 컨피그레이션됩니다. 다른 정책에서 개체를 사용하여 구축을 강제 적용할 필요가 없습니다.

참고 이 ACL은 IPv4에만 적용됩니다. IPv6도 지원하려면 속성이 모두 동일한 두 번째 ACE를 추가하기만 하면 됩니다. 단, 소스 및 대상 네트워크용으로 선택된 any-ipv6은 제외합니다. 트래픽이 ISE 또는 DNS 서버로 리디렉션되지 않도록 다른 ACE를 추가할 수도 있습니다. 먼저 해당 서버의 IP 주소를 보류할 호스트 네트워크 개체를 생성해야 합니다.

단계 **2** 동적 권한 부여를 위해 RADIUS 서버 그룹을 컨피그레이션합니다.

동적 권한 부여라고도 하는 CoA(Change of Authorization)를 활성화하기 위해 RADIUS 서버 및 서버 그룹 개체에서 올바르게 선택해야 할 중요한 옵션이 몇 가지 있습니다. 다음 절차에서는 이러한 속성에 중점을 둡니다. 이러한 개체에 대한 자세한 내용은 RADIUS 서버 및 그룹의 내용을 참조하십시오.

a) **Objects(**개체**) > Identity Sources(ID** 소스**)**를 선택합니다.

b) **+ > RADIUS Server(RADIUS** 서버**)**를 클릭합니다.

c) 서버 이름, ISE RADIUS 서버의 호스트네임/IP 주소, 인증 포트, 서버에 컨피그레이션된 암호 키를 입력합니다. 원하는 경우, 시간 초과를 조정합니다. 이러한 옵션은 동적 권한 부여와 직접적인 관련이 없습니다.

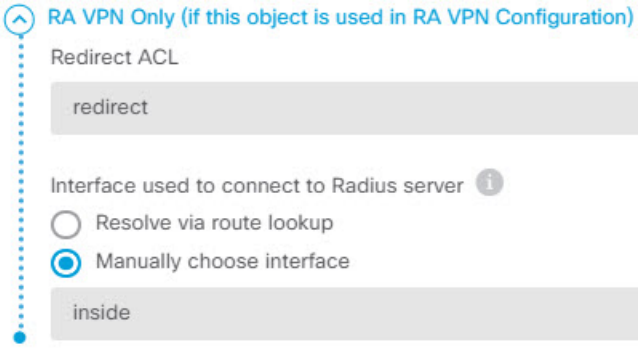
d) RA VPN Only(RA VPN 전용) 링크를 클릭하고 다음 옵션을 컨피그레이션합니다.

- **Redirect ACL(**리디렉션 **ACL)** - 리디렉션을 위해 생성한 확장 ACL을 선택합니다. 이 예에서는 ACL의 이름이 redirect입니다.
- **Interface used to connect to Radius server(RADIUS** 서버에 연결하는 데 사용할 인터페이스**) - Manually Choose Interface(**수동으로 인터페이스 선택**)**를 선택하고, 서버에 연결하기 위해 사용할 인터페이스를 선택합니다. 시스템에서 인터페이스에 CoA 리스너를 올바르게 활성화할 수 있도록 특정 인터페이스를 선택해야 합니다.

서버가 관리 주소와 동일한 네트워크에 있는 경우(진단 인터페이스 선택을 의미함), 진단 인터페이스의 IP 주소도 컨피그레이션해야 합니다. 관리 IP 주소로는 충분하지 않습니다. **Device(**디바이스**)** > **Interfaces(**인터페이스**)**로 이동하여 관리 IP 주소와 동일한 서브넷에 있는 진단 인터페이스에서 IP 주소를 설정합니다.

또한 device manager 관리 액세스를 위해 이 서버를 사용하는 경우, 이 인터페이스는 무시됩니다. 관리 액세스 시도는 항상 관리 IP 주소를 통해 인증됩니다.

다음 예는 내부 인터페이스에 대해 컨피그레이션되는 옵션을 나타낸 것입니다.



e) **OK(**확인**)**를 클릭하여 서버 개체를 저장합니다.

여러 개의 중복 ISE RADIUS 서버에 이중화 설정이 되어 있는 경우에는 이들 각 서버에 대해 서버 개체를 생성합니다.

f) **+** > **RADIUS Server Group(RADIUS** 서버 그룹**)**을 클릭합니다.

g) 서버 그룹의 이름을 입력하고, 원하는 경우 비활성 시간 및 최대 시도 횟수를 조정합니다.

h) **Dynamic Authorization(**동적 권한 부여**)** 옵션을 선택하고, ISE 서버에서 다른 포트를 사용하도록 컨피그레이션된 경우에는 포트 번호를 변경합니다. 포트 1700은 CoA 패킷에 대한 수신에 사용되는 기본 포트입니다.

i) 사용자 인증을 위해 AD 서버를 사용하도록 RADIUS 서버를 컨피그레이션하는 경우, 이 RADIUS 서버와 함께 사용되는 AD 서버를 지정하는 **Realm that Supports the RADIUS Server(RADIUS** 서버를 지원하는 영역**)**를 선택합니다. 영역이 아직 없는 경우, 목록 아래에 있는 **Create New Identity Realm(**새 **ID** 영역 생성**)**을 클릭하여 영역을 바로 컨피그레이션합니다.

j) **RADIUS Server(RADIUS** 서버**)**에서 **+** 버튼을 클릭하고 RA VPN에 대해 생성한 서버 개체를 선택합니다.

k) **OK(**확인**)**를 클릭하여 서버 그룹 개체를 저장합니다.

단계 **3** **Device(**디바이스**)** > **RA VPN** > **Connection Profiles(**연결 프로파일**)**를 선택하고, 이 RADIUS 서버 그룹을 사용하는 연결 프로파일을 생성합니다.

AAA Authentication(AAA 인증**)**을 사용하고(이것만 사용하거나 인증서와 함께 사용), **Primary Identity Source for User Authentication(**사용자 인증을 위한 기본 **ID** 소스**)**, **Authorization(**권한 부여**)** 및 **Accounting(**계정 관리**)** 옵션에서 서버 그룹을 선택합니다.

조직의 필요에 따라 다른 옵션을 모두 컨피그레이션합니다.

참고 VPN 네트워크를 통해 DNS 서버에 접속할 경우, 스플릿 터널링 속성 페이지에서 연결 프로파일에 사용되는 그룹 정책을 수정하여 **Split DNS(**스플릿 **DNS)** 옵션을 컨피그레이션합니다.

ISE에서 COA(Change of Authorization) 컨피그레이션

CoA(Change of Authorization) 컨피그레이션의 대부분은 ISE 서버에서 수행됩니다. ISE에는 엔드포인트 디바이스에서 실행되는 보안 상태 평가 에이전트가 있고, ISE에서는 디바이스와 직접 통신하여 보안 상태를 확인합니다. threat defense 디바이스에서는 기본적으로 특정 최종 사용자를 처리하는 방법에 대한 ISE의 지침을 기다립니다.

보안 상태 평가 정책 컨피그레이션에 대한 전체적인 논의는 이 문서의 범위를 벗어납니다. 그러나 다음 절차에서는 몇 가지 기본 사항에 관해 설명합니다. ISE를 컨피그레이션하기 위한 시작점으로 이것을 사용하십시오. 정확한 명령 경로, 페이지 이름 및 속성 이름은 릴리스에 따라 달라질 수 있다는 점에 유의하십시오. 사용 중인 ISE 버전에서는 다른 용어 또는 조직을 사용할 수 있습니다.

지원되는 최소 ISE 릴리스는 2.2 패치 1입니다.

시작하기 전에

이 절차에서는 ISE RADIUS 서버에서 사용자를 이미 컨피그레이션한 것으로 가정합니다.

프로시저

단계 **1** 관리 > 네트워크 리소스 > 네트워크 디바이스 > 네트워크 디바이스를 선택하고 threat defense 디바이스를 ISE 네트워크 디바이스 인벤토리에 추가한 뒤 RADIUS 설정을 구성합니다.

RADIUS 인증 설정을 선택하고 threat defense RADIUS 서버 개체에 구성된 동일한 공유 암호를 구성합니다. 원하는 경우 **CoA** 포트 번호를 변경하고 threat defense RADIUS 그룹 개체의 동일한 포트를 구성하도록 합니다.

단계 **2** **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Authorization(**권한 부여**)** > **Downloadable ACLs(**다운로드 가능한 **ACL)**를 선택합니다.

규정 준수 엔드포인트에서 사용할 것 1개와 규정 미준수 엔드포인트에서 사용할 것 1개, 즉 2개의 DACL(다운로드 가능 ACL)을 생성합니다.

예를 들어 규정 준수 엔드포인트에 대한 모든 액세스를 허용(permit ip any any)하는 반면, 규정 미준수 엔드포인트에 대한 모든 액세스를 거부(deny ip any any)할 수 있습니다. 필요에 따라 이 DACL의 복잡도를 조절하여 사용자의 규정 준수 상태에 따라 사용자가 가져야 할 정확한 액세스 권한을 제공할 수 있습니다. 권한 부여 프로파일에서 이 DACL을 사용합니다.

단계 **3** **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Authorization(**권한 부여**)** > **Authorization Profile(**권한 부여 프로파일**)**을 선택하고 필요한 프로파일을 컨피그레이션합니다.

다음 상태에 대한 프로파일이 필요합니다. 각각에 대한 최소 속성이 나열됩니다.

- **Unknown(**알 수 없음**)** - 알 수 없는 보안 상태 프로파일이 기본 보안 상태 프로파일입니다. 모든 엔드포인트는 RA VPN 연결을 처음 설정하는 경우 이 정책에 매칭됩니다. 이 규칙의 요점은 리디렉션 ACL 및 URL을 적용하고, 엔드포인트에 보안 상태 에이전트가 아직 없는 경우 다운로드하는 것입니다. 에이전트가 설치되어 있지 않은 경우 또는 설치에 실패한 경우, 엔드포인트는 이 프로파일에 연결된 상태를 유지할 수 있습니다. 그러지 않으면 엔드포인트는 보안 상태를 평가한 후 규정 준수 또는 미준수 프로파일로 이동합니다.

  최소 속성은 다음과 같습니다.

  - **Name(**이름**)** - 예: PRE_POSTURE
  - **Access Type(**액세스 유형**)** - **ACCESS_ACCEPT**를 선택합니다.
  - 일반 작업 - 웹 리디렉션**(CWA, MDM, NSP, CPP)**을 선택하고 클라이언트 프로비저닝**(**상태**)**를 선택한 후 threat defense 디바이스에 구성한 리디렉션 ACL의 이름을 입력합니다. 아직 선택하지 않은 경우 **Value(**값**)**에서 **Client Provisioning Portal(**클라이언트 프로비저닝 포털**)**을 선택합니다.
  - **Attribute Details(**속성 상세정보**)**에서는 url-redirect-acl 및 url-redirect에 대한 2개의 cisco-av-pair 값을 표시해야 합니다. ISE에서 이 데이터를 threat defense 디바이스로 전송하고, 이 디바이스에서는 기준을 RA VPN 사용자 세션에 적용합니다.

- **Compliant(**규정 준수**)** - 보안 상태 평가 완료 후 엔드포인트에 대해 컨피그레이션된 모든 요구사항을 엔드포인트가 충족하는 경우, 클라이언트는 규정을 준수하는 것으로 간주되며 이 프로파일을 가져옵니다. 일반적으로 이 클라이언트에 전체 액세스 권한을 부여합니다.

  최소 속성은 다음과 같습니다.

  - **Name(**이름**)** - 예: FULL_ACCESS
  - **Access Type(**액세스 유형**)** - **ACCESS_ACCEPT**를 선택합니다.
  - **Common Tasks(**일반 작업**)** - **DACL Name(DACL** 이름**)**을 선택하고, 규정 준수 사용자에 대해 다운로드 가능 ACL을 선택합니다(예: PERMIT_ALL_TRAFFIC). ISE에서 ACL을 threat defense 디바이스로 전송하고, 이 디바이스에서는 이 ACL을 사용자 세션에 적용합니다. 이 DACL은 사용자 세션에 대한 초기 리디렉션 ACL을 대체합니다.

- **Non-compliant(**규정 미준수**)** - 보안 상태 평가를 통해 엔드포인트가 모든 요건을 충족하지 못한다는 것이 확인되는 경우, 카운트다운이 실행되는데 이 시간 동안 클라이언트에서는 필요한 업데이트를 설치하는 것과 같은 방법으로 엔드포인트를 규정 준수 상태로 가져올 수 있습니다. Secure Client이 컴플라이언스 문제가 있는 사용자를 안내합니다. 카운트다운을 하는 동안 엔드포인트는 알 수 없는 규정 준수 상태를 유지합니다. 카운트다운이 만료된 후에도 엔드포인트가 여전히 규정 미준수 상태를 유지하는 경우, 세션은 규정 미준수로 표시되며 규정 미준수 프로파일을 가져옵니다. 일반적으로 이 엔드포인트에 대한 모든 액세스를 금지하거나 최소한 몇 가지 방법으로 액세스를 제한합니다.

  최소 속성은 다음과 같습니다.

  - **Name(**이름**)** - 예: Non_Compliant
  - **Access Type(**액세스 유형**)** - **ACCESS_ACCEPT**를 선택합니다.

- **Common Tasks(**일반 작업**) - DACL Name(DACL** 이름**)**을 선택하고, 규정 미준수 사용자에 대해 다운로드 가능 ACL을 선택합니다(예: DENY_ALL_TRAFFIC). ISE에서 ACL을 threat defense 디바이스로 전송하고, 이 디바이스에서는 이 ACL을 사용자 세션에 적용합니다. 이 DACL은 사용자 세션에 대한 초기 리디렉션 ACL을 대체합니다.

단계 **4** **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Client Provisioning(**클라이언트 프로비저닝**)** > **Resources(**리소스**)**를 선택하고 다음 리소스를 컨피그레이션합니다.

- **AnyConnect package(AnyConnect** 패키지**)** - 헤드 엔드 패키지 파일로서, software.cisco.com에서 다운로드합니다. 지원하는 클라이언트 플랫폼에 대한 별도 패키지가 필요하므로 AnyConnectDesktopWindows와 같은 여러 가지 유형을 구성해야 할 수도 있습니다.
- **ISE Posture Configuration File(Type: AnyConnectProfile)(ISE** 보안 상태 구성 파일**(**유형**: AnyConnectProfile))** - 이 구성 파일에서는 규정 준수 모듈에서 엔드 유저의 디바이스를 평가하는 데 사용하는 설정을 정의합니다. 이 파일에서는 사용자가 규정 미준수 디바이스를 규정 준수 상태로 가져올 수 있는 시간의 길이도 정의합니다.
- 컴플라이언스 모듈 패키지**(**유형**: ComplianceModule)** - Secure Client 컴플라이언스 모듈 파일은 설치된 AnyConnect 패키지에 공급되어 엔드포인트 컴플라이언스를 확인하는 파일입니다. **Add Resource from Cisco Site(Cisco** 사이트에서 리소스 추가**)** 명령을 사용하여 이 파일을 다운로드합니다. 구성한 Secure Client 패키지에 따라 올바른 모듈을 다운로드했는지 확인합니다. 그렇지 않은 경우 사용자는 다운로드를 실패합니다. ISEComplianceModule 폴더의 Secure Client 목록에 있는 software.cisco.com에서도 파일을 확인할 수 있습니다.
- **Anyconnect** 구성 파일**(**유형**: AnyConnectConfig)** - 이 Secure Client 릴리스별 설정은 적용할 **AnyConnect** 패키지, 컴플라이언스 모듈, **ISE** 상태를 정의합니다. 패키지는 OS별로 되어 있기 때문에 지원할 각 클라이언트 OS(예: Windows, MAC, Linux)에 대해 별도 컨피그레이션 파일을 생성합니다.

단계 **5** **Policy(**정책**)** > **Client Provisioning(**클라이언트 프로비저닝**)**을 선택하고 클라이언트 프로비저닝 정책을 컨피그레이션합니다.

예를 들어 CoA를 구현해야 하는 각 운영 체제에 대해 CoA_ClientProvisionWin과 같은 이름의 새 규칙을 생성합니다. 규칙에 대해 적절한 운영 체제를 선택하고 결과에서 해당 OS에 대해 생성한 Secure Client 구성 파일을 에이전트로 선택합니다.

교체하려는 기본 OS별 규칙을 비활성화합니다.

단계 **6** 보안 상태 정책을 컨피그레이션합니다.

이 단계에서는 조직에 의미가 있는 보안 상태 요건을 개발합니다.

- **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Conditions(**조건**)** > **Posture(**보안 상태**)**를 선택하고 충족해야 하는 단순 보안 상태 조건을 정의합니다. 예를 들어 사용자에게 특정 애플리케이션을 설치하도록 요구할 수 있습니다.
- **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Posture(**보안 상태**)** > **Requirements(**요건**)**를 선택하고, 엔드포인트에 대해 규정 준수 모듈 요건을 정의합니다.

- **Policy(**정책**)** > **Posture(**보안 상태**)** > **Posture Policy(**보안 상태 정책**)**를 선택하고 지원되는 운영 체제에 대한 정책을 컨피그레이션합니다.

단계 **7** **Policy(**정책**)** > **Policy Sets(**정책 집합**)** > **Default(**기본값**)** > **Authorization Policy(**권한 부여 정책**)**를 선택하고 정책을 생성합니다.

각 규정 준수 조건에 대해 규칙을 추가합니다. 이 샘플 값은 이전 단계의 예시에 따른 것입니다.

- 알 수 없음: 사전 보안 상태 및 보안 상태 다운로드의 경우
  - Name(이름) - 예: PRE_POSTURE
  - Condition(조건) - ”Session-PostureStatus EQUALS Unknown” 및 “Radius-NAS-Port-Type EQUALS Virtual”
  - Profiles(프로파일) - 예: PRE_POSTURE
- 규정 준수: 보안 상태 요건을 충족하는 클라이언트의 경우
  - Name(이름) - 예: FULL_ACCESS
  - Condition(조건) - ”Session-PostureStatus EQUALS Compliant” 및 “Radius-NAS-Port-Type EQUALS Virtual”
  - Profiles(프로파일) - 예: FULL_ACCESS
- 규정 미준수: 보안 상태 요건 충족에 실패하는 클라이언트의 경우
  - Name(이름) - 예: NON-COMPLIANT
  - Condition(조건) - ”Session-PostureStatus EQUALS NonCompliant” 및 “Radius-NAS-Port-Type EQUALS Virtual”
  - Profiles(프로파일) - 예: Non_Compliant

단계 **8** (선택 사항). **Administration(**관리**)** > **Settings(**설정**)** > **Posture(**보안 상태**)** > **Reassessments(**재평가**)**를 선택하고 보안 상태 재평가를 활성화합니다.

기본적으로 보안 상태는 연결 시에만 평가됩니다. 보안 상태 재평가를 활성화하여 연결된 엔드포인트의 보안 상태를 주기적으로 확인할 수 있습니다. 재평가 간격을 설정하여 재평가가 실행되는 빈도를 결정할 수 있습니다.

시스템에서 재평가에 실패하는 경우, 시스템에서 어떻게 응답해야 하는지 정의할 수 있습니다. 사용자가 계속 진행하도록 허용하거나(연결 유지) 사용자를 로그오프하거나 시스템을 교정하도록 사용자에게 요청할 수 있습니다.

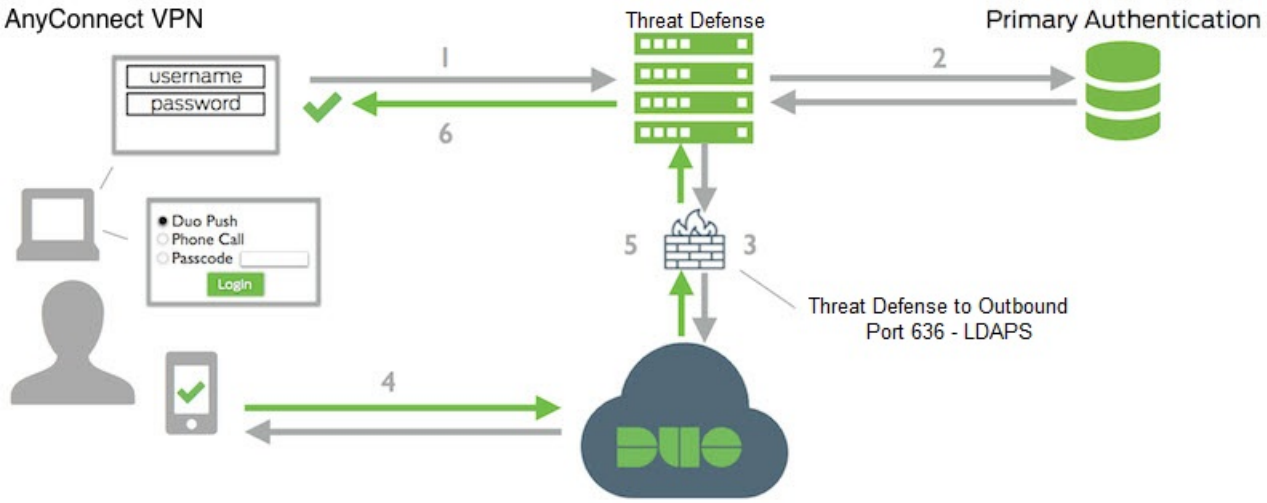
Duo LDAP를 사용하여 이중 인증을 구성하는 방법

기본 소스로 Microsoft AD(Microsoft Active Directory) 또는 RADIUS 서버를 함께 사용하여 Duo LDAP 서버를 보조 인증 소스로 사용할 수 있습니다. Duo LDAP를 사용하는 경우 보조 인증에서는 Duo 암호, 푸시 알림 또는 전화 통화를 사용하여 기본 인증을 검증합니다.

다음 주제에서는 구성에 대해 자세히 설명합니다.

Duo LDAP 보조 인증을 위한 시스템 플로우

다음 그래픽에는 LDAP를 사용하여 이중 인증을 제공하기 위해 threat defense 및 Duo가 함께 작동하는 방법이 나와 있습니다.



다음은 시스템 플로우에 대한 설명입니다.

1. 사용자는 threat defense 디바이스에 대한 원격 액세스 VPN 연결을 설정하고 사용자 이름과 비밀번호를 입력합니다.
2. Threat Defense에서는 기본 인증 서버(Active Directory 또는 RADIUS일 수 있음)를 사용하여 이 기본 인증 시도를 인증합니다.
3. 기본 인증이 작동하는 경우 threat defense에서는 보조 인증에 대한 요청을 Duo LDAP 서버로 전송합니다.
4. 그런 다음, Duo에서 푸시 알림, 암호를 사용한 문자 메시지 또는 전화 통화를 통해 사용자를 개별적으로 인증합니다. 사용자는 이 인증을 성공적으로 완료해야 합니다.
5. Duo에서는 사용자가 성공적으로 인증되었는지 여부를 나타내기 위해 threat defense 디바이스에 응답합니다.
6. 보조 인증에 성공하면 threat defense 디바이스에서 사용자의Secure Client와 원격 액세스 VPN 연결을 설정합니다.

Duo LDAP 보조 인증 구성

다음 절차에서는 Duo LDAP를 보조 인증 소스로 사용하여 원격 액세스 VPN에 이중 인증을 구성하는 엔드 투 엔드 프로세스에 대해 설명합니다. 이 구성을 완료하려면 Duo를 사용하는 어카운트가 있어야 하며 Duo에서 일부 정보를 얻어야 합니다.

프로시저

단계 **1** Duo 어카운트를 생성하고 통합 키, 비밀 키 및 API 호스트 이름을 가져옵니다.

프로세스는 간단히 다음과 같습니다. 자세한 내용은 Duo 웹 사이트인 https://duo.com을 참조하십시오.

a) Duo 어카운트에 등록합니다.
b) Duo 관리 패널에 로그인하여 **Applications(**애플리케이션**)**로 이동합니다.
c) 애플리케이션 목록에서 **Protect an Application(**애플리케이션 보호**)**을 클릭하고 Cisco SSL VPN을 찾습니다. **Protect this Application(**이 애플리케이션 보호**)**을 클릭하여 통합 키, 비밀 키 및 API 호스트 이름을 가져옵니다. 도움이 필요한 경우 Duo *Getting Started* 가이드(https://duo.com/docs/getting-started)를 참조하십시오.

단계 **2** Duo LDAP 서버의 Duo LDAP ID 소스를 생성합니다.

threat defense API를 사용하여 Duo LDAP 개체를 생성해야 합니다. device manager을 사용하여 생성할 수는 없습니다. API Explorer를 사용하거나 고유한 클라이언트 애플리케이션을 작성하여 개체를 생성할 수 있습니다. 다음 절차에서는 API Explorer를 사용하여 개체를 생성하는 방법을 설명합니다.

a) device manager에 로그인하고 추가 옵션 버튼(⋮)을 클릭한 후 **API Explorer**를 선택합니다.

브라우저 설정에 따라 별도의 탭 또는 창에 API Explorer가 열립니다.

b) (선택 사항). 시스템에서 Duo LDAP 서버에 연결할 때 사용해야 하는 인터페이스를 식별하는 데 필요한 값을 가져옵니다.

인터페이스를 지정하지 않으면 시스템에서 라우팅 테이블을 사용합니다. 필요한 경우 Duo LDAP 서버에 대한 정적 경로를 생성할 수 있습니다. 또는 Duo LDAP 개체에서 사용할 인터페이스를 지정할 수 있습니다. 인터페이스를 지정하려는 경우 인터페이스 그룹의 다양한 GET 메서드를 사용하여 필요한 값을 가져옵니다. 물리적 인터페이스, 하위 인터페이스, EtherChannel 또는 VLAN 인터페이스를 사용할 수 있습니다. 예를 들어, 물리적 인터페이스의 값을 가져오려면 GET /devices/default/interfaces 메서드를 사용하여 사용해야 하는 인터페이스의 개체를 찾습니다. 인터페이스 개체에서는 다음과 같은 값이 필요합니다.

- id
- type
- version
- name

c) **DuoLDAPIdentitySource** 머리글을 클릭하여 그룹을 엽니다.

d) **POST /object/duoldapidentitysources** 메서드를 클릭합니다.

e) **Parameters(**파라미터**)** 머리글 아래의 **body(**본문**)** 요소에서 오른쪽의 **Data Type(**데이터 유형**)** 열에 있는 **Example Value(**예시 값**)** 표시 상자를 클릭합니다. 이 작업을 수행하면 본문 값 수정 상자에 예시가 로드됩니다.

f) **body value(**본문 값**)** 수정 상자에서 다음 작업을 수행합니다.

- 특성 줄인 **version**, **id**를 삭제합니다. 이러한 특성은 PUT 호출에 필요하지만 POST에는 필요하지 않습니다.
- **name**에는 개체의 이름(예: Duo-LDAP-server)을 입력합니다.
- **description**에는 참조 목적으로 개체에 대한 의미 있는 설명을 입력하거나 특성 줄을 삭제합니다.
- **apiHostname**에는 Duo 어카운트에서 가져온 API 호스트 이름을 입력합니다. 호스트 이름은 X가 고유한 값으로 교체되면 API-XXXXXXXX.DUOSECURITY.COM과 유사하게 표시되어야 합니다. 대문자는 필요하지 않습니다.
- **port**에는 LDAPS에 사용할 TCP 포트를 입력합니다. 포트는 다른 포트를 사용하도록 Duo에서 지시한 경우를 제외하고는 636이어야 합니다. 액세스 제어 목록에서 이 포트를 통해 Duo LDAP 서버에 대한 트래픽을 허용하는지 확인해야 합니다.
- **timeout**에는 Duo 서버에 연결할 시간 제한(초)을 입력합니다. 이 값은 1~300초일 수 있습니다. 기본값은 120입니다. 기본값을 사용하려면 120을 입력하거나 특성 줄을 삭제합니다.
- **integrationKey**에는 Duo 어카운트에서 가져온 통합 키를 입력합니다.
- **secretKey**에는 Duo 어카운트에서 가져온 비밀 키를 입력합니다. 이 키는 이후에 마스킹됩니다.
- **interface**에는 Duo LDAP 서버에 연결하는 데 사용할 인터페이스의 ID, 유형, 버전 및 이름 값을 입력하거나 후행 닫는 중괄호를 포함하여 인터페이스 특성을 정의하는 데 사용되는 6개의 줄을 삭제합니다.
- **type**의 값은 duoldapidentitysource로 남겨 둡니다.

예를 들어, 개체 본문은 다음과 유사하게 표시될 수 있습니다. 여기에서 apiHostname 및 integrationKey는 난독 처리되지만, 의도적으로 위조한 비밀 키가 표시됩니다.

```
{
  "name": "Duo-LDAP-server",
  "description": "Duo LDAP server for RA VPN",
  "apiHostname": "API-XXXXXXXX.DUOSECURITY.COM",
  "port": 636,
  "timeout": 120,
  "integrationKey": "XXXXXXXXXXXXXXXXXXXX",
  "secretKey": "123456789",
  "type": "duoldapidentitysource"
}
```

g) **Try It Out!(**시도**)** 버튼을 클릭합니다.

시스템에서 디바이스 구성에 개체를 게시하기 위해 **curl** 명령을 실행합니다. 여기에는 curl 명령, 응답 본문 및 응답 코드가 표시됩니다. 유효한 본문을 생성한 경우 **Response Code(**응답 코드**)** 필드에 **200**이 표시되어야 합니다.

오류가 발생한 경우 응답 본문에서 오류 메시지를 확인합니다. 본문 값을 수정하고 다시 시도할 수 있습니다.

h) 상단 메뉴에서 **Device(**디바이스**)**를 클릭하여 device manager으로 돌아갑니다.

i) 목차에서 **Objects(**개체**)**와 **Identity Sources(ID** 소스**)**를 차례로 클릭합니다.

Duo LDAP 개체가 목록에 표시되어야 합니다. 표시되지 않는 경우, API Explorer로 돌아가 개체를 다시 생성해 보십시오. GET 메서드를 사용하여 실제로 생성되었는지 여부를 확인할 수 있습니다.

device manager을 사용하여 개체를 삭제할 수는 있지만 개체를 수정하거나 내용을 볼 수는 없습니다. 이러한 작업을 수행할 때는 API를 사용해야 합니다. 관련된 메서드가 **DuoLDAPIdentitySource** 그룹에 표시됩니다.

단계 **3** Duo 웹 사이트의 신뢰할 수 있는 CA 인증서를 device manager에 업로드합니다.

threat defense 시스템에는 Duo LDAP 서버에 대한 연결을 검증하는 데 필요한 인증서가 있어야 합니다. 이 절차를 사용하여 인증서를 가져오고 업로드할 수 있으며 이 절차는 Google Chrome 브라우저를 통해 수행되었습니다. 브라우저마다 정확한 단계는 다를 수 있습니다. 또는 https://www.digicert.com/digicert-root-certificates.htm으로 직접 이동하여 인증서를 다운로드할 수 있지만, 다음과 같은 절차가 일반적이며 이를 사용하여 모든 사이트에 대해 신뢰할 수 있는 루트 CA 인증서를 가져올 수 있습니다.

a) 브라우저에서 https://duo.com을 엽니다.

b) 브라우저의 URL 필드에서 사이트 정보 링크를 클릭한 다음, **Certificate(**인증서**)** 링크를 클릭합니다. 이 작업을 수행하면 인증서 정보 대화 상자가 열립니다.

c) **Certificate Path(**인증서 경로**)** 탭을 클릭하고 경로의 루트(상위) 레벨을 선택합니다. 이 경우에는 DigiCert입니다.

d) DigiCert를 선택하고 **View Certificate(**인증서 보기**)**를 클릭합니다. 이 작업을 수행하면 새 Certificate(인증서) 대화 상자가 열리고 General(일반) 탭에 인증서가 DigiCert High Assurance EV Root CA로 발급되었음이 표시되어야 합니다. 이 인증서는 device manager에 업로드해야 하는 루트 CA 인증서입니다.

e) **Details(**세부 사항**)** 탭을 클릭한 다음, **Copy To File(**파일에 복사**)** 버튼을 클릭하여 인증서 다운로드 마법사를 시작합니다.

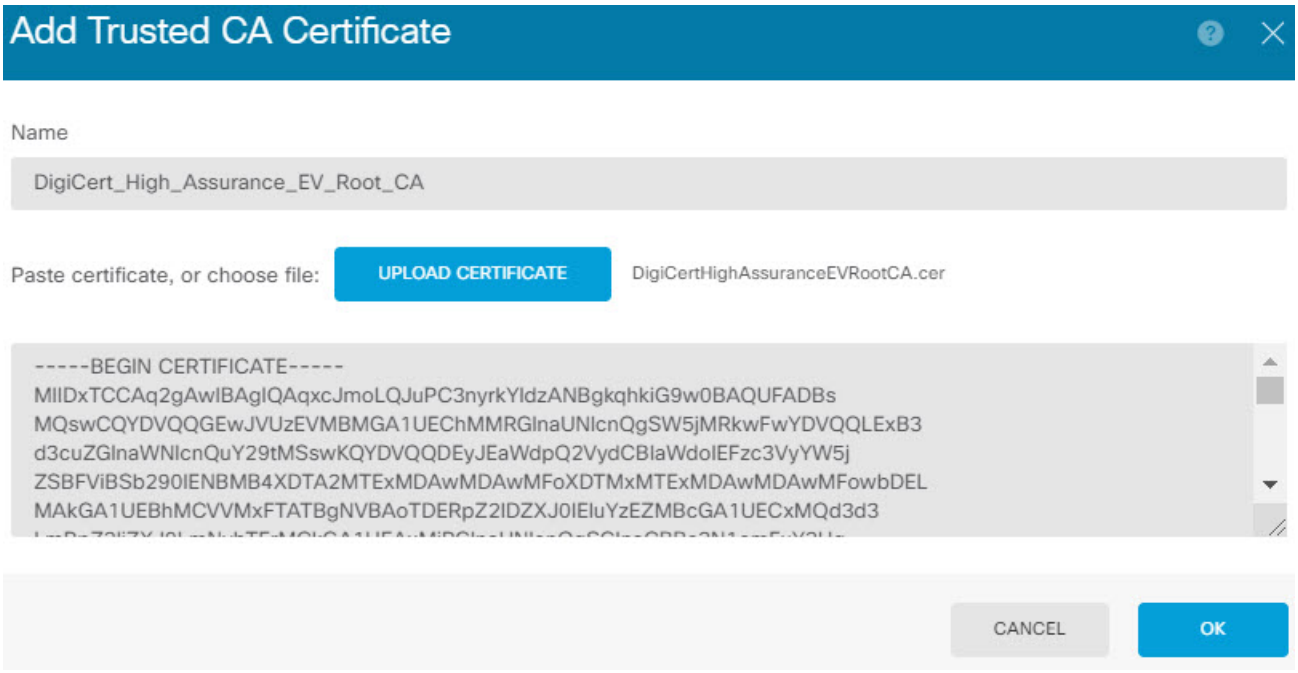
f) 이 마법사를 사용하여 워크스테이션에 인증서를 다운로드합니다. 기본 DER 형식을 사용하여 다운로드합니다.

g) device manager에서 **Objects(**개체**)** > **Certificates(**인증서**)**를 선택합니다.

h) **+** > **Add Trusted CA Certificate(**신뢰받는 **CA** 인증서 추가**)**를 클릭합니다.

i) 인증서의 이름(예: DigiCert_High_Assurance_EV_Root_CA)을 입력합니다. 공백은 허용되지 않습니다.

j) **Upload Certificate(**인증서 업로드**)**를 클릭하고 다운로드한 파일을 선택합니다.



k) **OK(**확인**)**를 클릭합니다.

단계 **4** 인증 시간 제한에 60초 이상을 지정하는 프로필을 생성하려면 Secure Client 프로필 편집기를 사용합니다.

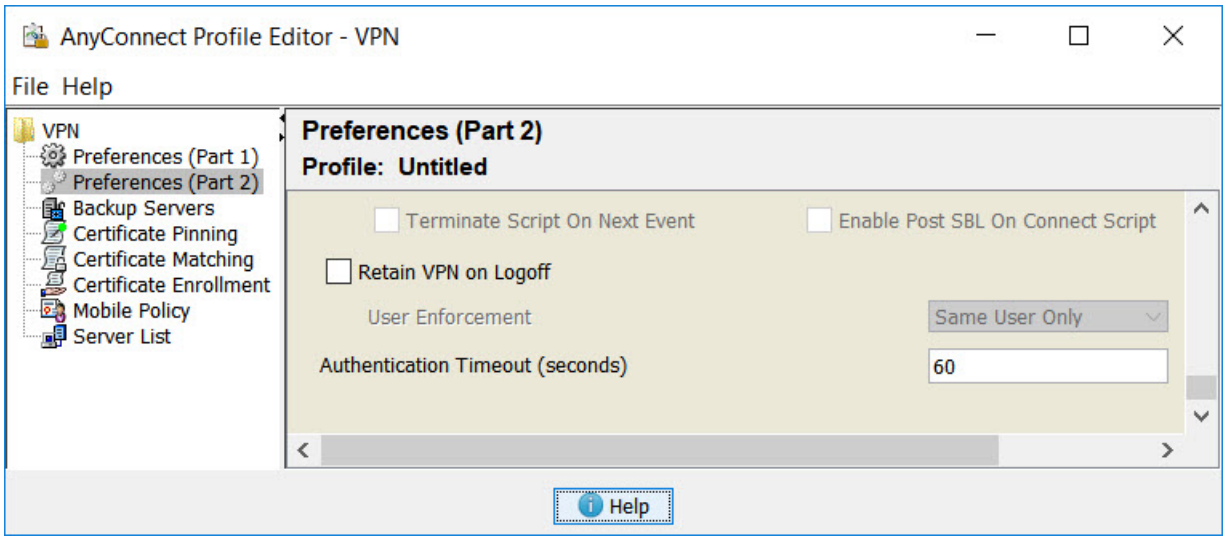
사용자에게 Duo 암호를 얻고 보조 인증을 완료할 추가 시간을 제공해야 합니다. 60초 이상 제공하는 것이 좋습니다.

Secure Client 프로필을 생성하고 업로드하는 방법에 대한 자세한 내용은 클라이언트 프로파일 구성 및 업로드, 10 페이지를 참조하십시오. 다음 절차에서는 인증 시간 제한만 구성한 후 프로필을 threat defense에 업로드하는 방법에 대해 설명합니다. 다른 설정을 변경하려는 경우 지금 하면 됩니다.

a) 아직 작업을 수행하지 않은 경우, Secure Client 프로필 편집기 패키지를 다운로드하여 설치합니다. 이는 Cisco Software Center(software.cisco.com)(Secure Client 버전용 폴더)에서 찾을 수 있습니다.

b) Secure Client **VPN Profile Editor(VPN** 프로필 편집기**)**를 엽니다.

c) 목차에서 **Preferences(Part 2)(**기본 설정**(**파트 **2))**를 선택하고 페이지 끝으로 스크롤한 다음, **Authentication Timeout(**인증 시간 제한**)**을 60 이상으로 변경합니다. 다음 이미지는 AnyConnect 4.7 VPN 프로필 편집기의 이미지입니다(이전 버전 또는 후속 버전의 경우 다를 수 있음).



d) **File(**파일**)** > **Save(**저장**)**를 선택하고 프로필 XML 파일을 적절한 이름(예: duo-ldap-profile.xml)의 워크스테이션에 저장합니다.

이제 VPN 프로필 편집기 애플리케이션을 닫으면 됩니다.

e) device manager에서 **Objects(**개체**)** > **Secure Client Profiles(**보안 클라이언트 프로파일**)**를 선택합니다.

f) +를 클릭하여 새 프로필 개체를 생성합니다.

g) 개체의 **Name(**이름**)**을 입력합니다. 예를 들어, Duo-LDAP-profile입니다.

h) **Upload(**업로드**)**를 클릭하고 생성한 XML 파일을 선택합니다.

i) **OK(**확인**)**를 클릭합니다.

단계 **5** 그룹 정책을 생성하고 정책에서 Secure Client 프로필을 선택합니다.

사용자에게 할당하는 그룹 정책으로 인해 연결의 여러 측면이 제어됩니다. 다음 절차에서는 프로필 XML 파일을 그룹에 할당하는 방법에 대해 설명합니다. 그룹 정책으로 수행할 수 있는 작업에 대한 자세한 내용은 RA VPN에 대한 그룹 정책 컨피그레이션, 25 페이지를 참조하십시오.

a) **Device(**디바이스**)** > **Remote Access VPN(**원격 액세스 **VPN)**에서 **View Configuration(**구성 보기**)**을 클릭합니다.

b) 목차에서 **Group Policies(**그룹 정책**)**를 선택합니다.

c) DfltGrpPolicy를 수정하거나 +를 클릭하고 새 그룹 정책을 생성합니다. 예를 들어 모든 사용자를 대상으로 단일 원격 액세스 VPN 연결 프로필이 필요한 경우, 기본 그룹 정책을 수정하는 것이 바람직합니다.

d) General(일반) 페이지에서 다음 속성을 구성합니다.

- **Name(**이름**)** - 새 프로필의 경우 이름을 입력합니다. 예를 들어, Duo-LDAP-group과 같이 입력합니다.
- **Secure Client Profile(**보안 클라이언트 프로파일**)** - +를 클릭하고 생성한 Secure Client 클라이언트 프로필 개체를 선택합니다.

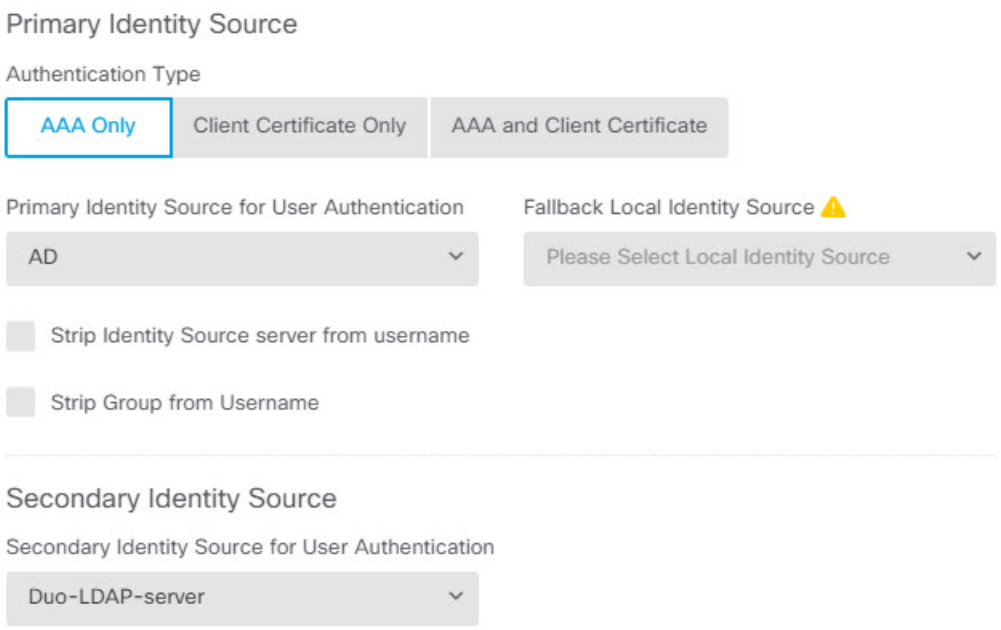
e) 그룹 프로필을 저장하려면 **OK(**확인**)**를 클릭합니다.

단계 **6** Duo-LDAP 보조 인증에 사용할 원격 액세스 VPN 연결 프로필을 생성하거나 수정합니다.

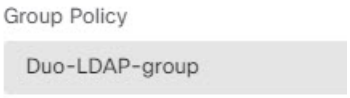
연결 프로필을 구성하는 단계는 여러 가지가 있으며 RA VPN 연결 프로파일 컨피그레이션, 16 페이지에 설명되어 있습니다. 다음 절차에서는 Duo-LDAP를 보조 인증 소스로 활성화하고 Secure Client 프로파일을 적용하기 위한 주요 변경 사항에 대해서만 설명합니다. 새 연결 프로필의 경우 나머지 필수 필드를 구성해야 합니다. 이 절차에서는 기존 연결 프로필을 수정하는 중이며 이러한 두 가지 설정만 변경하면 된다고 가정합니다.

a) RA VPN 페이지의 목차에서 **Connection Profiles(**연결 프로필**)**를 선택합니다.
b) 기존 연결 프로필을 수정하거나 새 프로필을 생성합니다.
c) Primary Identity Source(기본 ID 소스) 아래에서 다음을 구성합니다.

- **Authentication Type(**인증 유형**) - AAA Only(AAA** 전용**)** 또는 **AAA and Client Certificate(AAA** 및 클라이언트 인증서**)** 중 하나를 선택합니다. AAA를 사용하지 않는 한, 이중 인증을 구성할 수 없습니다.
- **Primary Identity Source for User Authentication(**사용자 인증을 위한 기본 **ID** 소스**)** - 기본 Active Directory 또는 RADIUS 서버를 선택합니다. Duo-LDAP ID 소스를 기본 소스로 선택할 수 있습니다. 그러나 Duo-LDAP에서는 인증 서비스만 제공하며 ID 서비스는 제공하지 않습니다. 따라서 이를 기본 인증 소스로 사용하는 경우, 어떠한 대시보드에도 RA VPN 연결과 관련된 사용자 이름이 표시되지 않으며, 이러한 사용자에 대한 액세스 제어 규칙을 작성할 수 없게 됩니다. 원하는 경우 로컬 ID 소스로의 대체 기능을 구성할 수 있습니다.
- **Secondary Identity Source(**보조 **ID** 소스**)** - Duo-LDAP ID 소스를 선택합니다.



d) **Next(**다음**)**를 클릭합니다.
e) Remote User Experience (원격 사용자 환경) 페이지에서 생성했거나 수정한 **Group Policy(**그룹 정책**)**를 선택합니다.



f) 이 페이지 및 다음 페이지인 Global Settings(글로벌 설정)에서 **Next(**다음**)**를 클릭합니다.

g) **Finish(**마침**)**를 클릭하여 연결 프로필에 변경 사항을 저장합니다.

단계 **7** 변경 사항을 커밋합니다.

a) 웹 페이지의 오른쪽 상단에 있는 **Deploy Changes(**변경 사항 구축**)** 아이콘을 클릭합니다.

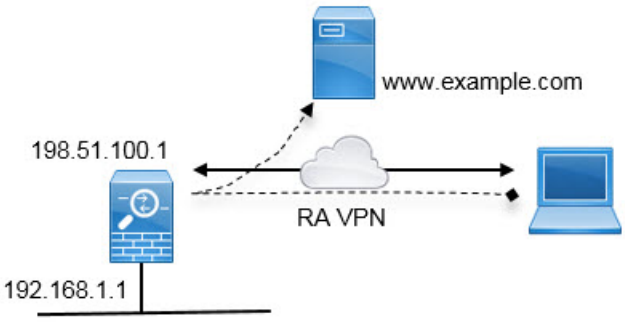
b) **Deploy Now(**지금 구축**)** 버튼을 클릭합니다.

구축이 완료될 때까지 기다리거나 **OK(**확인**)**를 클릭하고 나중에 작업 목록 또는 구축 기록을 확인할 수 있습니다.

원격 액세스 VPN 사용자에게 외부 인터페이스를 통해 인터넷 액세스를 제공하는 방법(헤어피닝)

원격 액세스 VPN에서는 원격 네트워크의 사용자가 디바이스를 통해 인터넷에 액세스하도록 할 수 있습니다. 그러나 원격 사용자는 인터넷에 연결되는 것과 동일한 인터페이스(외부 인터페이스)를 통해 디바이스에 진입하므로 인터넷 트래픽이 외부 인터페이스로 다시 나가도록 바운스해야 합니다. 이 기술을 헤어피닝이라고도 합니다.

다음 그림에 예시가 나와 있습니다. 외부 인터페이스 198.51.100.1에 원격 액세스 VPN이 구성되어 있습니다. 여기서 내부 네트워크로의 트래픽은 디바이스를 계속 통과하게 하면서 인터넷 바인딩 트래픽은 외부 인터페이스로 다시 나가도록 원격 사용자의 VPN 터널을 분할할 수 있습니다. 따라서 원격 사용자가 www.example.com 등의 인터넷 서버로 이동하려는 경우 해당 연결은 먼저 VPN을 통과한 다음 198.51.100.1 인터페이스에서 인터넷으로 다시 라우팅됩니다.



다음 절차에서는 이 서비스를 구성하는 방법을 설명합니다.

시작하기 전에

이 예시에서는 이미 디바이스를 등록했고 원격 액세스 VPN 라이선스를 적용했으며 Secure Client 이미지를 업로드했다고 가정합니다. 또한 ID 정책에서도 사용되는 ID 영역을 구성했다고 가정합니다.

프로시저

단계 **1** 원격 액세스 VPN 연결을 컨피그레이션합니다.

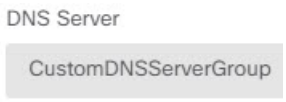
컨피그레이션하려면 연결 프로파일 외에도 맞춤형 그룹 정책이 필요합니다. 헤어피닝은 일반적인 컨피그레이션이며, 그룹 정책의 필수 설정이 일반적으로 적용됩니다. 이 예시에서는 새 그룹 정책을 생성하는 대신 기본 그룹 정책을 수정할 것입니다. 둘 중 한 가지 접근 방식을 선택할 수 있습니다.

a) **Device(**디바이스**)** > **Remote Access VPN(**원격 액세스 **VPN)** 그룹에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

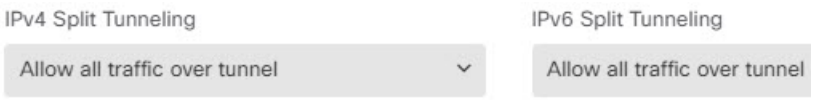
b) 목차에서 **Group Policies(**그룹 정책**)**을 클릭한 후 DfltGrpPolicy 개체에 대해 수정 아이콘()을 클릭합니다.

c) 기본 그룹 정책을 다음과 같이 변경합니다.

- **General(**일반**)** 페이지의 **DNS Server(DNS** 서버**)**에서 도메인 이름을 확인하기 위해 VPN 엔드포인트에서 사용해야 하는 서버를 정의하는 DNS 서버 그룹을 선택합니다.



- **Split Tunneling(**스플릿 터널링**)** 페이지에서 **IPv4** 및 **IPv6 Split Tunneling(IPv6** 스플릿 터널링**)**에 대해 **Allow all traffic over tunnel option(**터널 옵션을 통해 모든 트래픽 허용**)**을 선택합니다. 이것이 기본 설정이므로 이미 올바르게 컨피그레이션되어 있을 수 있습니다.



참고 이것은 헤어피닝 활성화에 중요한 설정입니다**.** 여기서 모든 트래픽을 VPN 게이트웨이로 이동하게 할 수 있습니다. 스플릿 터널링은 원격 클라이언트가 VPN 외부의 로컬 또는 인터넷 사이트에 직접 액세스하도록 허용하는 방식입니다.

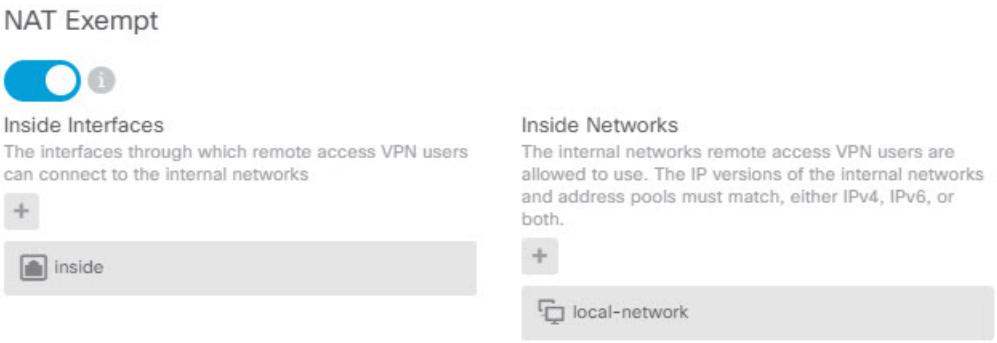
d) 기본 그룹 정책에 대한 변경 사항을 저장하려면 **OK(**확인**)**를 클릭합니다.

e) **Connection Profiles(**연결 프로파일**)**를 클릭하고 기존 프로파일을 수정하거나 새 프로파일을 생성합니다.

f) 연결 프로파일에서 마법사를 두루 탐색하여 기타 RA VPN 컨피그레이션에 대해 원하는 모든 옵션을 컨피그레이션합니다. 그러나 헤어피닝을 활성화하려면 다음 옵션을 올바르게 컨피그레이션해야 합니다.

- 2단계의 **Group Policy(**그룹 정책**)**입니다. 헤어피닝에 대해 맞춤형 그룹 정책을 선택합니다.

- 3단계의 **NAT Exempt(NAT 제외)**. 이 기능을 활성화합니다. 내부 인터페이스를 선택한 다음, 내부 네트워크를 정의하는 네트워크 개체를 선택합니다. 이 예시에서는 개체에 192.168.1.0/24를 지정해야 합니다. 내부 네트워크로 이동하는 RA VPN 트래픽의 경우 주소 변환이 수행되지 않습니다. 하지만 헤어피닝된 트래픽은 외부 인터페이스에서 나가므로 NAT가 수행됩니다. NAT 면제는 내부 인터페이스에만 적용되기 때문입니다. 다른 연결 프로파일을 정의한 경우, 컨피그레이션이 모든 연결 프로파일에 적용되므로 기존 설정에 추가해야 한다는 점에 유의하십시오.



참고 **NAT Exempt(NAT 제외)** 옵션은 헤어핀 컨피그레이션에 대한 기타 중요 설정입니다.

g) (선택 사항). **Global Settings(**전역 설정**)** 단계에서 **Bypass Access Control policy for decrypted traffic(**암호 해독된 트래픽에 대해 액세스 제어 정책 우회**) (sysopt permit-vpn)** 옵션을 선택합니다.

이 옵션을 선택하면 RA VPN 풀 주소에서 발신되는 트래픽을 허용하도록 액세스 제어 규칙을 컨피그레이션할 필요가 없어집니다. 이 옵션에서는 향상된 보안을 제공합니다(외부 사용자가 풀에서 주소를 스푸핑할 수 없음). 그러나 이것은 RA VPN 트래픽에 대해서는 URL 필터링 및 침입 방지를 포함한 검사가 면제됨을 뜻합니다. 장점과 단점을 고려한 후 이 옵션을 선택할지 결정하십시오.

h) RA VPN 컨피그레이션을 검토한 다음, **Finish(**마침**)**를 클릭합니다.

단계 **2** 외부 인터페이스에서 외부 IP 주소의 포트로 나가는 모든 연결을 변환하는 NAT 규칙(인터페이스 PAT)을 구성합니다.

초기 디바이스 컨피그레이션을 완료하면 InsideOutsideNatRule이라는 NAT 규칙이 생성됩니다. 이 규칙은 외부 인터페이스를 통해 디바이스에서 나가는 모든 인터페이스의 IPv4 트래픽에 인터페이스 PAT를 적용합니다. 외부 인터페이스는 "Any" 소스 인터페이스에 포함되므로 필요한 규칙을 수정하거나 삭제한 경우가 아니면 규칙이 이미 존재합니다.

다음 절차에서는 필요한 규칙을 생성하는 방법을 설명합니다.

a) **Policies(**정책**)** > **NAT**를 클릭합니다.

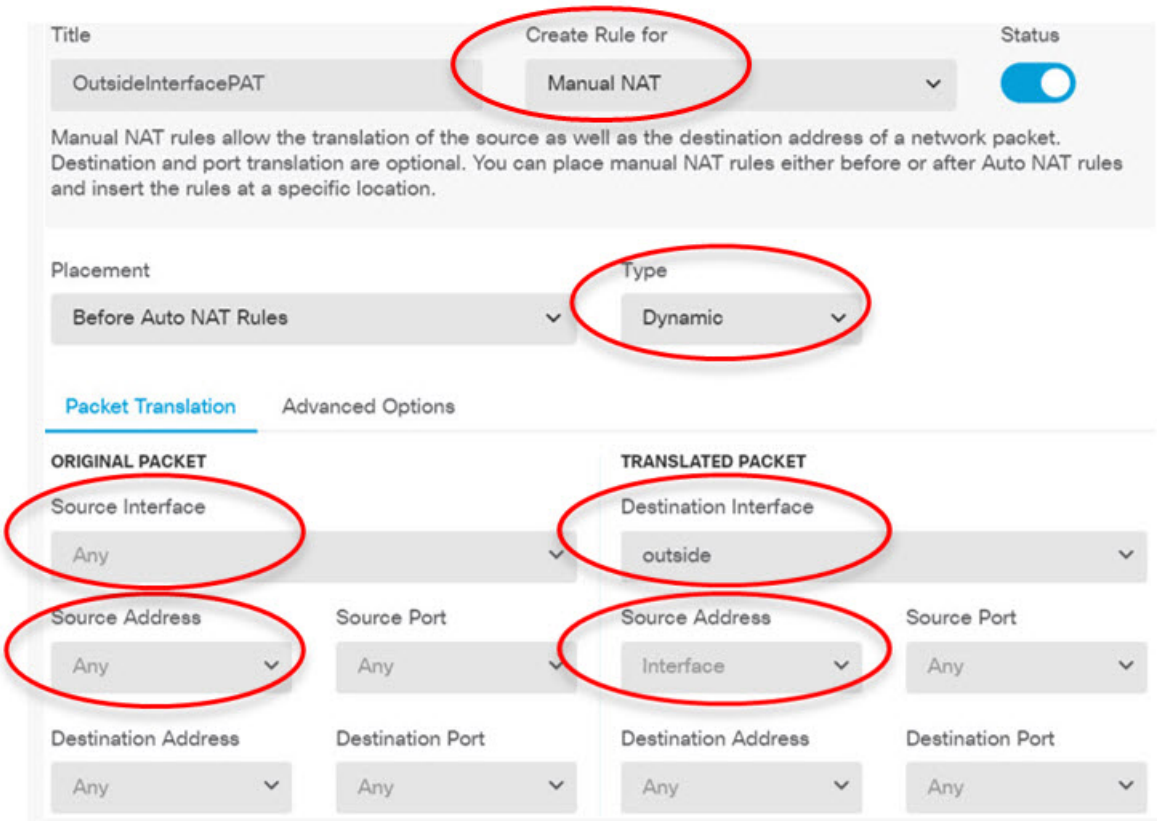
b) 다음 중 하나를 수행합니다.

- InsideOutsideNatRule을 수정하려면 **Action(**작업**)** 열 위에 마우스를 놓고 수정 아이콘( )을 클릭합니다.
- 새 규칙을 생성하려면 **+**를 클릭합니다.

c) 다음 속성을 사용하여 규칙을 구성합니다.

- **Title(**제목**)** - 새 규칙의 경우 의미 있는 이름을 공백 없이 입력합니다. 예를 들어 OutsideInterfacePAT를 입력합니다.
- **Create Rule For(**규칙 생성 대상**)** - **Manual NAT(**수동 **NAT)**.
- **Placement(**배치**)** - **Before Auto NAT Rules(**자동 **NAT** 규칙 앞**)**(기본값).
- **Type(**유형**)** - **Dynamic(**동적**)**.
- **Original Packet(**원본 패킷**)** - **Source Address(**소스 주소**)**의 경우 Any(모두) 또는 any-ipv4를 선택합니다. **Source Interface(**소스 인터페이스**)**의 경우 기본값인 Any(모두)를 선택해야 합니다. 기타 모든 Original Packet(원본 패킷) 옵션의 경우 기본값인 Any(모두)를 유지합니다.
- **Translated Packet(**변환된 패킷**)** - **Destination Interface(**대상 인터페이스**)**의 경우 outside(외부)를 선택합니다. **Translated Address(**변환된 주소**)**의 경우 **Interface(**인터페이스**)**를 선택합니다. 기타 모든 Translated Packet(변환된 패킷) 옵션의 경우 기본값인 Any(모두)를 유지합니다.

다음 그림에는 소스 주소로 Any(모두)를 선택하는 간단한 사례가 나와 있습니다.



d) **OK(**확인**)**를 클릭합니다.

단계 **3** (연결 프로파일에서 **Bypass Access Control policy for decrypted traffic(**암호 해독된 트래픽에 대해 액세스 제어 정책 우회**) (sysopt permit-vpn)**을 컨피그레이션하지 않는 경우.) 원격 액세스 VPN 주소 풀에서 액세스를 허용하는 액세스 제어 규칙을 구성합니다.

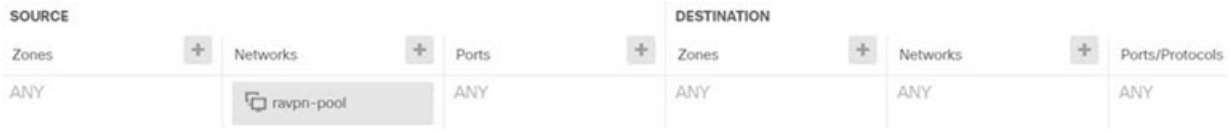
연결 프로파일에서 **Bypass Access Control policy for decrypted traffic(**암호 해독된 트래픽에 대해 액세스 제어 정책 우회**) (sysopt permit-vpn)**을 선택하는 경우, RA VPN 풀 주소에서 발신되는 트래픽은 액세스 제어 정책을 우회합니다. 트래픽에 적용할 액세스 제어 규칙을 작성할 수 없습니다. 옵션을 비활성화하는 경우에만 규칙을 작성해야 합니다.

다음 예시에서는 주소 풀에서 특정 대상으로의 트래픽을 허용합니다. 구체적인 요구 사항에 맞게 이 예시를 조정할 수 있습니다. 또한 이 규칙 앞에 원치 않는 트래픽을 필터링하여 제거하는 차단 규칙을 배치할 수도 있습니다.

a) **Policies(**정책**)** > **Access Control(**액세스 제어**)**을 클릭합니다.
b) +를 클릭하여 새 규칙을 생성합니다.
c) 다음 속성을 사용하여 규칙을 구성합니다.

- **Order(**순서**)** - 연결을 찾아 차단하는 다른 규칙 앞에 해당 규칙을 넣도록 정책 내의 위치를 선택합니다. 기본적으로는 규칙이 정책의 끝에 추가됩니다. 나중에 규칙을 재배치해야 하는 경우 이 옵션을 수정하거나, 규칙을 끌어서 표의 원하는 슬롯에 놓을 수 있습니다.
- **Title(**제목**)** - 의미 있는 이름을 공백 없이 입력합니다. 예를 들어 RAVPN-address-pool을 입력합니다.

- **Action(**작업**) - Allow(**허용**)**. 이 트래픽의 프로토콜 위반 또는 침입을 검사하지 않으려는 경우 Trust(신뢰)를 선택할 수 있습니다.
- **Source/Destination(**소스/대상**)** 탭 - **Source(**소스**)** > **Network(**네트워크**)**의 경우 주소 풀의 RA VPN 연결 프로파일에서 사용한 것과 같은 개체를 선택합니다. 기타 모든 Source(소스) 및 Destination(대상) 옵션의 경우 기본값인 Any(모두)를 유지합니다.



- **Application(**애플리케이션**)**, **URL** 및 **Users(**사용자**)** 탭 - 이러한 탭에서는 기본 설정, 즉 아무 설정도 선택하지 않은 상태를 유지합니다.
- **Intrusion(**침입**)**, **File(**파일**)** 탭 - 선택적으로 위협이나 악성코드를 검사하기 위한 침입 또는 파일 정책을 선택할 수 있습니다.
- **Logging(**로깅**)** 탭 - 선택적으로 연결 로깅을 활성화할 수 있습니다.

d) **OK(**확인**)**를 클릭합니다.

단계 **4** 변경 사항을 커밋합니다.

a) 웹 페이지의 오른쪽 상단에 있는 **Deploy Changes(**변경 사항 구축**)** 아이콘을 클릭합니다.

b) **Deploy Now(**지금 구축**)** 버튼을 클릭합니다.

구축이 완료될 때까지 기다리거나 **OK(**확인**)**를 클릭하고 나중에 작업 목록 또는 구축 기록을 확인할 수 있습니다.

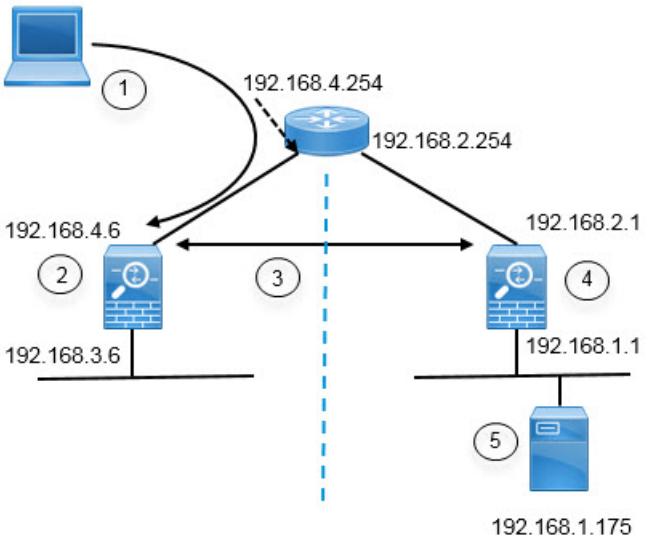
원격 액세스 VPN을 통해 외부 네트워크에서 디렉터리 서버를 사용하는 방법

모바일 작업자와 재택 근무자가 내부 네트워크에 안전하게 연결할 수 있도록 원격 액세스 VPN을 구성할 수 있습니다. 연결의 보안은 권한이 있는 사용자만 진입할 수 있도록 사용자 연결을 인증하는 디렉터리 서버에 따라 달라집니다.

디렉터리 서버가 내부 네트워크가 아닌 외부 네트워크에 있는 경우에는 외부 인터페이스에서 디렉터리 서버를 포함하는 네트워크로의 사이트 대 사이트 VPN 연결을 구성해야 합니다. 사이트 대 사이트 **VPN** 컨피그레이션을 수행할 때 기억해야 할 한 가지 사항은, 디렉터리 서버가 있는 디바이스의 원격 네트워크와 사이트 대 사이트 VPN 연결의 "내부" 네트워크 내에 원격 액세스 VPN 디바이스의 외부 인터페이스 주소를 포함해야 한다는 것입니다. 다음 절차에서 이에 대해 자세히 설명하겠습니다.

참고 가상 관리 인터페이스의 게이트웨이로 데이터 인터페이스를 사용하는 경우 이 컨피그레이션은 ID 정책용 디렉터리 사용도 활성화합니다. 데이터 인터페이스를 관리 게이트웨이로 사용하지 않는 경우에는 관리 네트워크에서 사이트 대 사이트 VPN 연결에 참여하는 내부 네트워크로의 경로가 있는지 확인하십시오.

이 활용 사례에서는 다음 네트워크 시나리오를 구현합니다.



그림의 설명선	**Description**
1	192.168.4.6에 대한 VPN 연결을 설정하는 원격 액세스 호스트. 클라이언트는 172.18.1.0/24 주소 풀의 주소를 가져옵니다.
2	원격 액세스 VPN을 호스팅하는 사이트 A
3	사이트 A 및 사이트 B threat defense 디바이스의 외부 인터페이스 간 사이트 대 사이트 VPN 터널.
4	디렉터리 서버를 호스팅하는 사이트 B
5	사이트 B의 내부 네트워크에 있는 디렉터리 서버

시작하기 전에

이 활용 사례에서는 디바이스 설정 마법사의 단계에 따라 일반 베이스라인 컨피그레이션을 설정했다고 가정합니다. 구체적으로 다음과 같습니다.

- inside_zone에서 outside_zone으로 이동하는 트래픽을 허용(신뢰)하는 Inside_Outside_Rule 액세스 제어 규칙이 있습니다.
- inside_zone 및 outside_zone 보안 영역은 각각 내부 및 외부 인터페이스를 포함합니다.

- 내부 인터페이스에서 외부 인터페이스로 이동하는 모든 트래픽에 대해 인터페이스 PAT를 수행하는 InsideOutsideNATRule이 있습니다. 기본적으로 내부 브리지 그룹을 사용하는 디바이스에는 인터페이스 PAT에 대한 여러 규칙이 있을 수 있습니다.
- 외부 인터페이스를 가리키는 0.0.0.0/0에 대한 고정 IPv4 경로가 있습니다. 이 예시에서는 외부 인터페이스에 대해 고정 IP 주소를 사용한다고 가정하지만, DHCP를 사용하여 정적 경로를 동적으로 가져올 수도 있습니다. 이 예시에서는 다음 정적 경로를 사용한다고 가정합니다.
  - 사이트 A: 외부 인터페이스, 게이트웨이: 192.168.4.254
  - 사이트 B: 외부 인터페이스, 게이트웨이: 192.168.2.254

프로시저

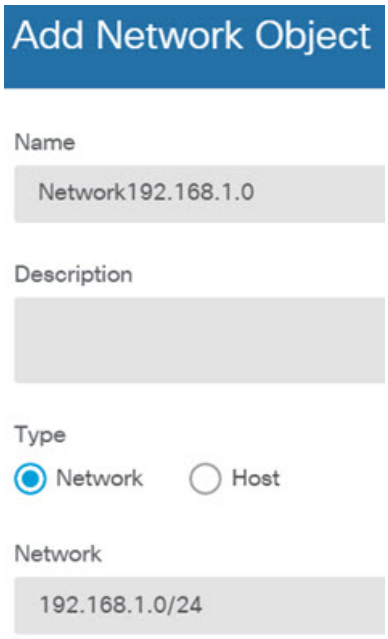
단계 **1** 디렉터리 서버를 호스팅하는 사이트 **B**에서 사이트 대 사이트 VPN 연결을 구성합니다.

a) **Device(**디바이스**)**를 클릭한 다음 사이트 대 사이트 VPN 그룹에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

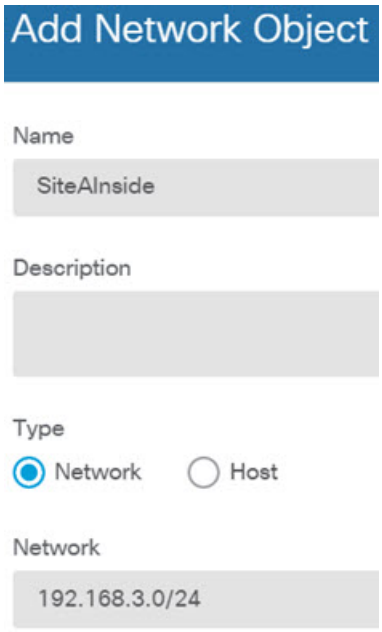
b) **+** 버튼을 클릭합니다.

c) 엔드포인트 설정에 대해 다음 옵션을 구성합니다.

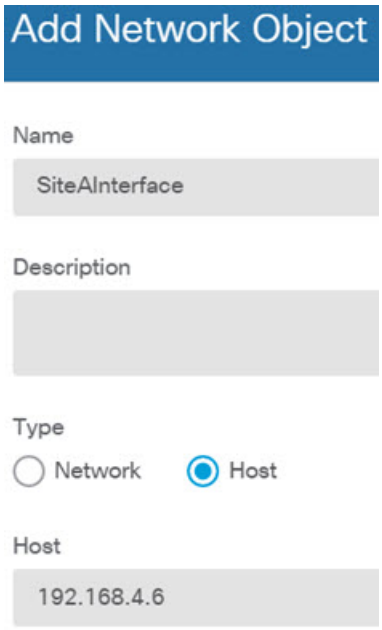
- **Connection Profile Name(**연결 프로파일 이름**)** — 사이트 A에 대한 연결임을 나타내는 SiteA와 같은 이름을 입력합니다.
- 로컬 사이트 - 이러한 옵션은 로컬 엔드포인트를 정의합니다.
  - **Local VPN Access Interface(**로컬 **VPN** 액세스 인터페이스**)** — 외부 인터페이스(다이어그램에서 주소가 192.168.2.1인 인터페이스)를 선택합니다.
  - **Local Network(**로컬 네트워크**) - +**를 클릭하고 VPN 연결에 참여해야 하는 로컬 네트워크를 식별하는 네트워크 개체를 선택합니다. 디렉터리 서버는 이 네트워크에 있으므로 사이트 대 사이트 VPN에 참여할 수 있습니다. 개체가 아직 없다고 가정하고, **Create New Network(**새 네트워크 생성**)**를 클릭하여 192.168.1.0/24 네트워크에 대한 개체를 구성합니다. 개체를 저장한 후 드롭다운 목록에서 해당 개체를 선택하고 **OK(**확인**)**를 클릭합니다.



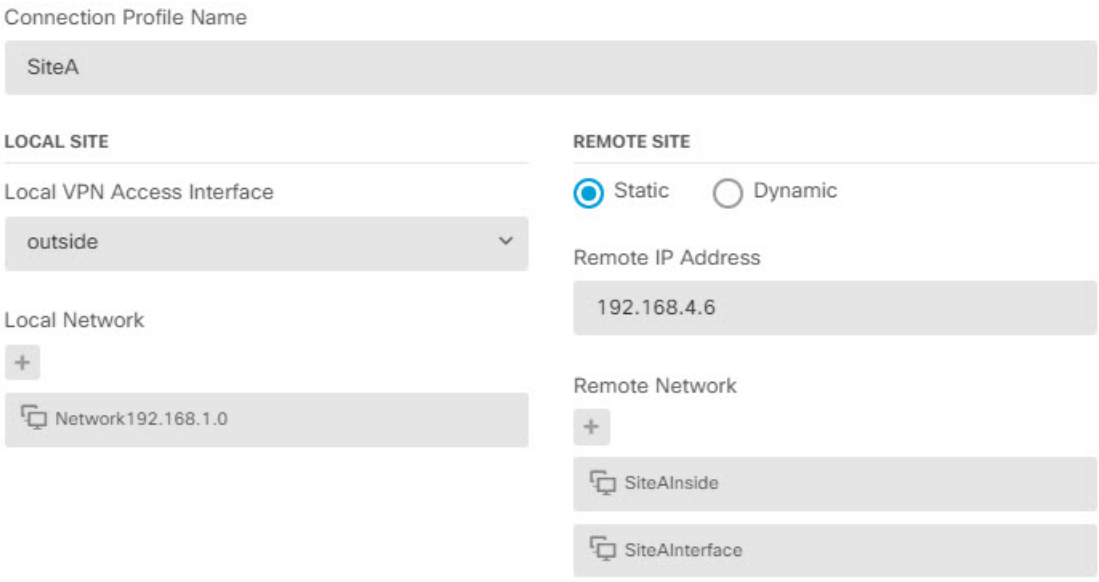
- 원격 사이트 - 이러한 옵션은 원격 엔드포인트를 정의합니다.
  - **Remote IP Address(**원격 **IP** 주소**)** — VPN 연결을 호스팅할 원격 VPN 피어 인터페이스의 IP 주소인 192.168.4.6을 입력합니다.
  - **Remote Network(**원격 네트워크**)** — **+**를 클릭하고 VPN 연결에 참여해야 하는 원격 네트워크를 식별하는 네트워크 개체를 선택합니다. **Create New Network(**새 네트워크 생성**)**를 클릭하고 다음 개체를 구성한 후에 목록에서 해당 개체를 선택합니다.
    1. SiteAInside, 네트워크, 192.168.3.0/24



2. SiteAInterface, 호스트, 192.168.4.6. 이 개체를 구성할 때 주의해야 할 점은, 해당 인터페이스에서 호스팅되는 **RA VPN**이 디렉터리 서버를 사용할 수 있도록 사이트 대 사이트 **VPN** 연결용 원격 네트워크의 일부분으로 원격 액세스 **VPN** 연결 지점 주소를 포함해야 한다는 것입니다.



개체 구성을 완료하고 나면 엔드포인트 설정이 다음과 같이 표시됩니다.



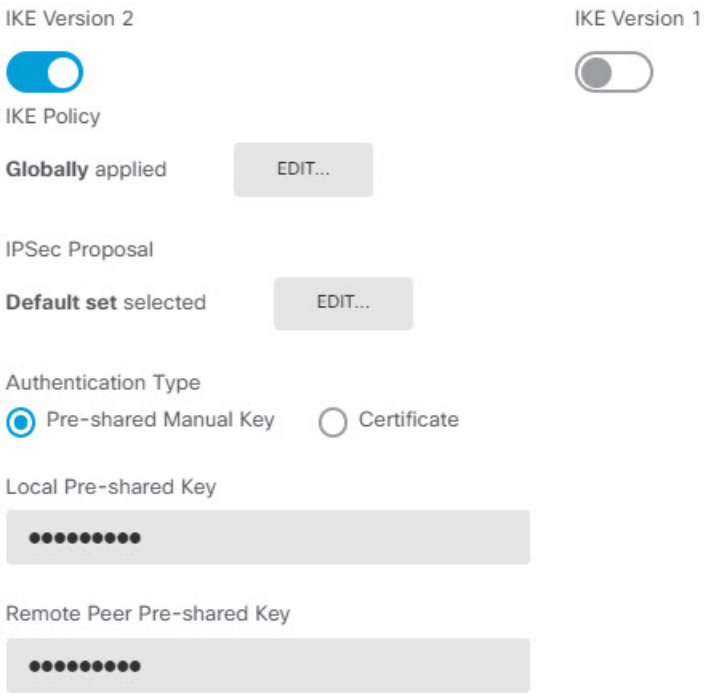
d) **Next(**다음**)**를 클릭합니다.

e) VPN에 대한 프라이버시 컨피그레이션을 정의합니다.

이 활용 사례에서는 강력한 암호화 사용을 허용하는 내보내기 제어 기능을 사용할 수 있다고 가정합니다. 라이선스 컴플라이언스와 요구사항을 충족하도록 이러한 예시 설정을 조정하십시오.

- **IKE** 버전 **2**, **IKE** 버전 **1** - **IKE** 버전 **2**는 활성화되고 **IKE** 버전 **1**은 비활성화된 기본값을 유지합니다.
- **IKE** 정책 - 수정을 클릭하여 **AES-GCM-NULL-SHA** 및 **AES-SHA-SHA**를 활성화하고 **DES-SHA-SHA**를 비활성화합니다.
- **IPsec** 제안 - 수정을 클릭하고 IPSec 제안 선택 대화 상자에서 +를 클릭한 다음 기본값 설정을 클릭하여 기본 AES-GCM 제안을 선택합니다.
- 로컬 사전 공유 키, 원격 피어 사전 공유 키 - VPN 연결을 위한 원격 디바이스와 이 디바이스에 정의된 키를 입력합니다. IKEv2에서는 이러한 키가 다를 수 있습니다. 키는 영숫자 1~127자가 될 수 있습니다. 사이트 **A** 디바이스에서 사이트 대 사이트 **VPN** 연결을 생성할 때 동일한 문자열을 구성해야 하므로 이러한 키를 기억해 두어야 합니다**.**

IKE 정책은 다음과 같이 표시됩니다.



f) 추가 옵션을 구성합니다.

- **NAT Exempt(NAT** 제외**)** — 내부 네트워크를 호스팅하는 인터페이스(이 예시에서는 내부 인터페이스)를 선택합니다. 일반적으로는 사이트 대 사이트 VPN 터널 내 트래픽의 IP 주소를 변환하지 않습니다. 이 옵션은 로컬 네트워크가 단일 라우팅 인터페이스(브리지 그룹 멤버 아님) 뒤에 있는 경우에만 작동합니다. 로컬 네트워크가 둘 이상의 라우팅 인터페이스 또는 하나 이상의 브리지 그룹 멤버 뒤에 있는 경우에는 NAT 제외 규칙을 수동으로 생

성해야 합니다. 필요한 규칙을 수동으로 생성하는 방법에 대한 자세한 내용은 NAT에서 사이트 대 사이트 VPN 트래픽 제외를 참조하십시오.

- **Diffie-Helman Group for Perfect Forward Secrecy(PFS(Perfect Forward Secrecy)를 위한 Diffie-Hellman)** 그룹 — 그룹 **19**를 선택합니다. 이 옵션은 PFS(Perfect Forward Secrecy)를 사용하여 암호화된 각 교환에 대해 고유 세션 키를 생성하고 사용할지를 결정합니다. 고유 세션 키는 전체 교환이 기록되었으며 공격자가 엔드포인트 디바이스에서 사용하는 사전 공유 키 또는 개인 키를 확보했더라도 후속 암호 해독에서 교환을 보호합니다. 옵션에 대한 설명은 사용할 Diffie-Hellman 모듈러스 그룹 결정를 참조하십시오.

옵션은 다음과 같이 표시됩니다.

g) **Next(**다음**)**를 클릭합니다.

h) 요약을 검토하고 **Finish(**종료**)**를 클릭합니다.

요약 정보가 클립보드에 복사됩니다. 해당 정보를 문서에 붙여넣은 다음 원격 피어를 구성하는 데 사용하거나 피어 구성 담당자에게 보낼 수 있습니다.

i) 웹 페이지의 오른쪽 상단에 있는 **Deploy Changes(**변경 사항 구축**)** 아이콘을 클릭합니다.

j) **Deploy Now(**지금 구축**)** 버튼을 클릭하고 구축이 정상적으로 완료될 때까지 기다립니다.

이제 사이트 B 디바이스는 사이트 대 사이트 VPN 연결의 한쪽을 호스팅할 준비가 되었습니다.

단계 **2** 사이트 **B** 디바이스에서 로그아웃하고 사이트 **A** 디바이스에 로그인합니다.

단계 **3** 원격 액세스 VPN을 호스팅할 사이트 **A**에서 사이트 대 사이트 VPN 연결을 구성합니다.

a) **Device(**디바이스**)**를 클릭한 다음 사이트 대 사이트 VPN 그룹에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

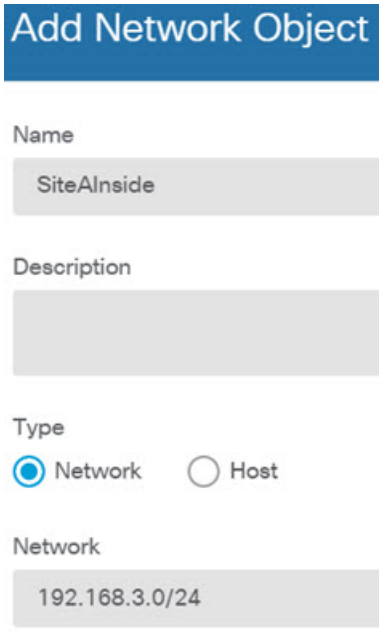
b) **+** 버튼을 클릭합니다.

c) 엔드포인트 설정에 대해 다음 옵션을 구성합니다.

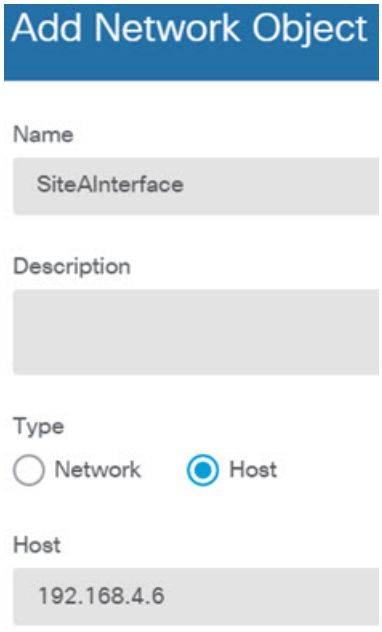
- **Connection Profile Name(**연결 프로파일 이름**)** — 사이트 B에 대한 연결임을 나타내는 SiteB와 같은 이름을 입력합니다.
- 로컬 사이트 - 이러한 옵션은 로컬 엔드포인트를 정의합니다.
  - **Local VPN Access Interface(**로컬 **VPN** 액세스 인터페이스**)** — 외부 인터페이스(다이어그램에서 주소가 192.168.4.6인 인터페이스)를 선택합니다.
  - **Local Network(**로컬 네트워크**)** — **+**를 클릭하고 VPN 연결에 참여해야 하는 로컬 네트워크를 식별하는 네트워크 개체를 선택합니다. **Create New Network(**새 네트워크 생

성)를 클릭하고 다음 개체를 구성한 후에 목록에서 해당 개체를 선택합니다. 사이트 B 디바이스에서 같은 개체를 생성했어도 사이트 A 디바이스에서 해당 개체를 다시 생성해야 합니다.

1. SiteAInside, 네트워크, 192.168.3.0/24

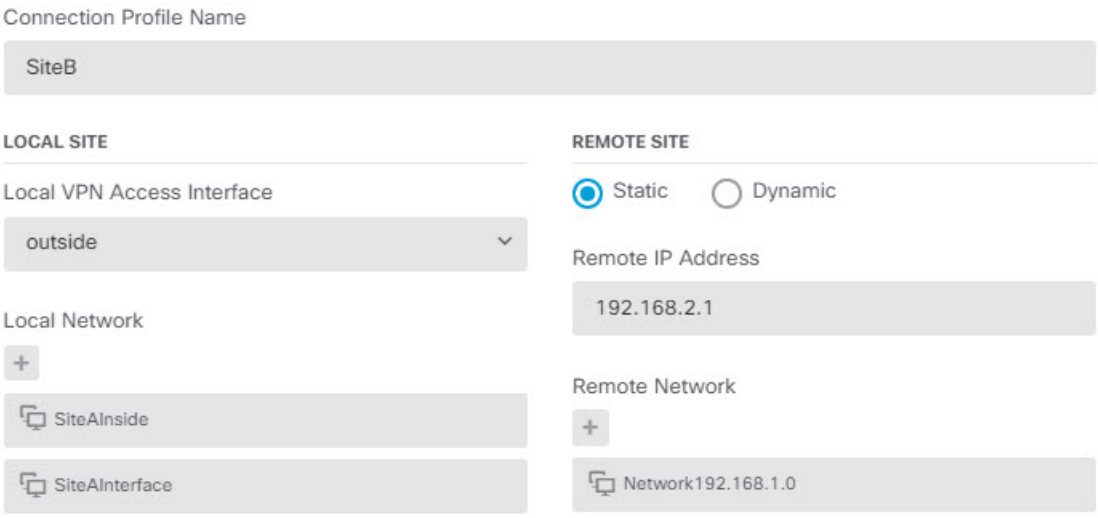


2. SiteAInterface, 호스트, 192.168.4.6. 이 개체를 구성할 때 주의해야 할 점은, 해당 인터페이스에서 호스팅되는 RA VPN이 원격 네트워크의 디렉터리 서버를 사용할 수 있도록 사이트 대 사이트 VPN 연결용 내부 네트워크의 일부분으로 원격 액세스 VPN 연결 지점 주소를 포함해야 한다는 것입니다.



- 원격 사이트 - 이러한 옵션은 원격 엔드포인트를 정의합니다.
  - **Remote IP Address(**원격 **IP** 주소**)** — VPN 연결을 호스팅할 원격 VPN 피어 인터페이스의 IP 주소인 192.168.2.1을 입력합니다.
  - **Remote Network(**원격 네트워크**)** — **+**를 클릭하고 VPN 연결에 참여해야 하는 원격 네트워크를 식별하는 네트워크 개체(디렉터리 서버를 포함하는 개체)를 선택합니다. 새 네트워크 생성을 클릭하여 192.168.1.0/24 네트워크에 대한 개체를 구성합니다. 개체를 저장한 후 드롭다운 목록에서 해당 개체를 선택하고 **OK(**확인**)**를 클릭합니다. 사이트 **B** 디바이스에서 같은 개체를 생성했어도 사이트 **A** 디바이스에서 해당 개체를 다시 생성해야 합니다**.**

개체 구성을 마치면 엔드포인트 설정이 다음과 같이 표시됩니다. 로컬/원격 네트워크는 사이트 B 설정과 반대입니다. 포인트 투 포인트 연결의 양쪽은 항상 이렇게 표시되어야 합니다.

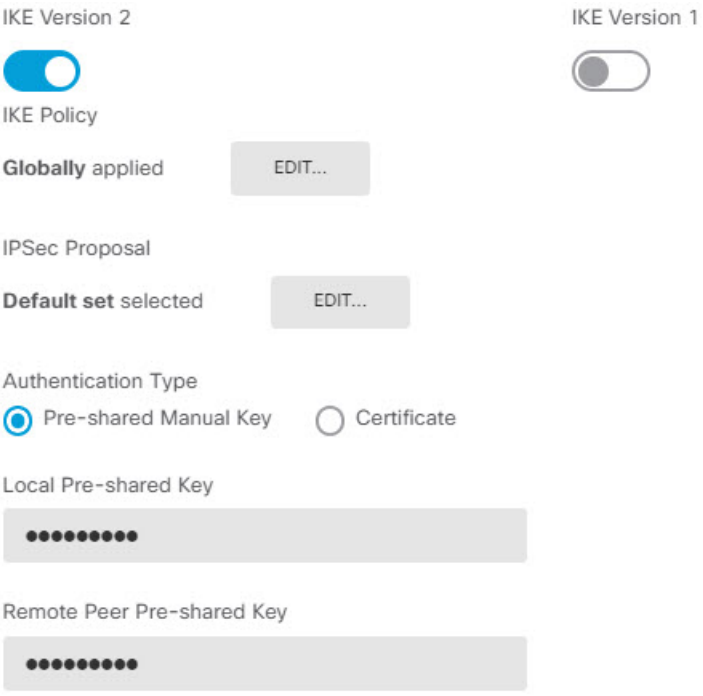


d) **Next(**다음**)**를 클릭합니다.

e) VPN에 대한 프라이버시 컨피그레이션을 정의합니다.

사이트 B에서와 동일한 IKE 버전, 정책, IPsec 제안 및 사전 공유 키를 구성하되 로컬 사전 공유 키와 원격 사전 공유 키를 반대로 구성해야 합니다.

IKE 정책은 다음과 같이 표시됩니다.



f) 추가 옵션을 구성합니다.

- **NAT Exempt(NAT** 제외**)** — 내부 네트워크를 호스팅하는 인터페이스(이 예시에서는 내부 인터페이스)를 선택합니다. 일반적으로는 사이트 대 사이트 VPN 터널 내 트래픽의 IP 주소

를 변환하지 않습니다. 이 옵션은 로컬 네트워크가 단일 라우팅 인터페이스(브리지 그룹 멤버 아님) 뒤에 있는 경우에만 작동합니다. 로컬 네트워크가 둘 이상의 라우팅 인터페이스 또는 하나 이상의 브리지 그룹 멤버 뒤에 있는 경우에는 NAT 제외 규칙을 수동으로 생성해야 합니다. 필요한 규칙을 수동으로 생성하는 방법에 대한 자세한 내용은 NAT에서 사이트 대 사이트 VPN 트래픽 제외를 참조하십시오.

- **Diffie-Helman Group for Perfect Forward Secrecy(PFS(Perfect Forward Secrecy)**를 위한 **Diffie-Hellman)** 그룹 — 그룹 **19**를 선택합니다.

옵션은 다음과 같이 표시됩니다.

g) **Next(**다음**)**를 클릭합니다.
h) 요약을 검토하고 **Finish(**종료**)**를 클릭합니다.
i) 웹 페이지의 오른쪽 상단에 있는 **Deploy Changes(**변경 사항 구축**)** 아이콘을 클릭합니다.

j) **Deploy Now(**지금 구축**)** 버튼을 클릭하고 구축이 정상적으로 완료될 때까지 기다립니다.

이제 사이트 A 디바이스는 사이트 대 사이트 VPN 연결의 반대쪽을 호스팅할 준비가 되었습니다. 사이트 B가 호환 설정으로 이미 구성되어 있으므로 두 디바이스는 VPN 연결을 협상합니다.

디바이스 CLI에 로그인한 다음 디렉터리 서버 ping을 수행하여 연결을 확인할 수 있습니다. **show ipsec sa** 명령을 사용하여 세션 정보를 확인할 수도 있습니다.

단계 **4** 사이트 **A**에서 디렉터리 서버를 구성합니다. 테스트를 클릭하여 연결이 있는지 확인합니다.

a) 목차에서 **Objects(**개체**)**와 **Identity Sources(ID** 소스**)**를 차례로 선택합니다.
b) **+** > **AD**를 클릭합니다.
c) 기본 영역 속성을 구성합니다.

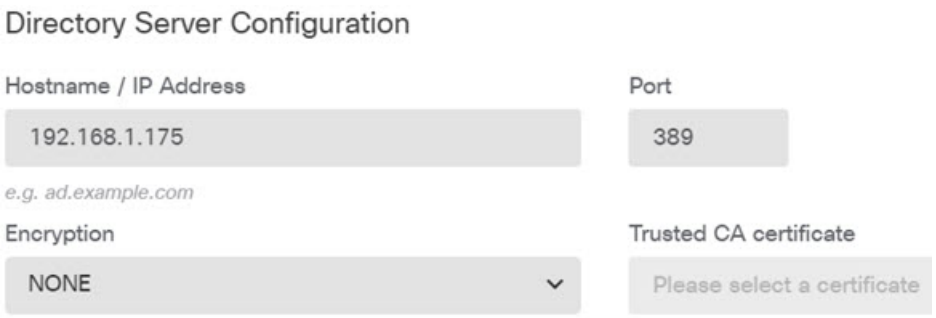
- **Name(**이름**)** — 디렉토리 영역의 이름입니다. AD와 같은 이름이 지정되어 있을 수 있습니다.
- **Type(**유형**)** - 디렉터리 서버의 유형입니다. 지원되는 유형은 Active Directory뿐이며 이 필드의 내용은 변경할 수 없습니다.
- **Directory Username(**디렉터리 사용자 이름**)**, **Directory Password(**디렉터리 비밀번호**)** - 검색하려는 사용자 정보에 대한 적절한 권한이 있는 사용자의 고유 사용자 이름 및 비밀번호입니다. Active Directory의 경우에는 사용자에게 상승된 권한이 필요하지 않습니다. 도메인에 어떤 사용자라도 지정할 수 있습니다. 사용자 이름은 모든 자격 요건에 부합해야 합니다(예: 단지 Administrator가 아닌 Administrator@example.com).

참고 시스템은 이 정보에서 ldap-login-dn 및 ldap-login-password를 생성합니다. 예를 들어 Administrator@example.com은 cn=administrator,cn=users,dc=example,dc=com으로 변환됩니다. cn=users는 항상 이 변환에 포함되므로 일반 이름 "users" 폴더 아래에 여기서 지정하는 사용자를 구성해야 합니다.

- **Base DN(기본 DN)** - 사용자 및 그룹 정보를 검색하거나 쿼리하기 위한 디렉터리 트리, 즉 사용자와 그룹의 공통 상위 항목입니다. cn=users,dc=example,dc=com을 예로 들 수 있습니다. 기본 DN을 찾는 방법에 대한 자세한 내용은 디렉터리 기본 DN 결정를 참조하십시오.
- **AD Primary Domain(AD 기본 도메인)** - 디바이스가 조인해야 하는 정규화된 Active Directory 도메인 이름입니다. example.com 등을 예로 들 수 있습니다.

d) 디렉터리 서버 속성을 구성합니다.

- **Hostname/IP Address(호스트 이름/IP 주소)** - 디렉터리 서버의 호스트 이름 또는 IP 주소입니다. 서버에 대한 암호화된 연결을 사용하는 경우에는 IP 주소가 아닌 FQDN(Fully-Qualified Domain Name)을 입력해야 합니다. 이 예시에서는 192.168.1.175를 입력합니다.
- **Port(포트)** - 서버와의 통신에 사용되는 포트 번호입니다. 기본값은 389입니다. 암호화 방법으로 LDAPS를 선택하는 경우에는 포트 636을 사용합니다. 이 예시에서는 389를 유지합니다.
- **Encryption(암호화)** - 사용자 및 그룹 정보를 다운로드하기 위해 암호화된 연결을 사용할지를 선택합니다. 기본값은 **None(없음)**입니다. 이 옵션은 사용자 및 그룹 정보를 일반 텍스트로 다운로드함을 의미합니다. RA VPN의 경우 **LDAPS**(LDAP over SSL)를 사용할 수 있습니다. 이 옵션을 선택하는 경우 포트 636을 사용합니다. RA VPN은 STARTTLS를 지원하지 않습니다. 이 예시에서는 없음을 선택합니다.
- **Trusted CA Certificate(신뢰할 수 있는 CA 인증서)** - 암호화 방법을 선택하는 경우 CA(인증 증명) 인증서를 업로드하여 시스템과 디렉터리 서버 간에 신뢰할 수 있는 연결을 설정합니다. 인증서를 사용하여 인증하는 경우에는 인증서의 서버 이름이 서버 호스트 이름/IP 주소와 일치해야 합니다. 예를 들어 IP 주소로 192.168.1.175를 사용하는데 인증서의 주소는 ad.example.com이면 연결은 실패합니다.



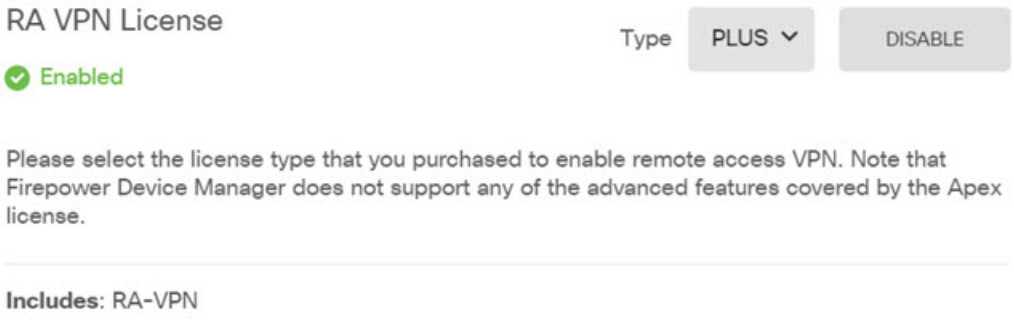
e) **Test(**테스트**)** 버튼을 클릭하여 시스템이 서버에 연결할 수 있는지 확인합니다.

시스템은 별도의 프로세스를 사용하여 서버에 액세스하므로, 연결이 특정 사용 유형에는 작동하지만 다른 유형에는 작동하지 않음을 나타내는 오류가 발생합니다. 연결을 ID 정책에는 사용할 수 있지만, 원격 액세스 VPN에는 사용할 수 없는 경우를 예로 들 수 있습니다. 서버에 연결할 수 없는 경우에는 IP 주소와 호스트 이름이 올바른지와 DNS 서버에 호스트 이름의 항목이 있는지 등을 확인합니다. 또한, 사이트 대 사이트 VPN 연결이 작동하고, 사이트 A의 외부 인터페이스 주소를 VPN에 포함했으며, NAT가 디렉터리 서버에 대한 트래픽을 변환하지 않는지 확인합니다. 서버에 대한 정적 경로도 구성해야 할 수 있습니다.

f) **OK(**확인**)**를 클릭합니다.

단계 **5** **Device(**디바이스**)** > **Smart License(**스마트 라이선스**)** > **View Configuration(**컨피그레이션 보기**)**을 클릭하고 RA VPN 라이선스를 활성화합니다.

RA VPN 라이선스를 활성화하는 경우 구매한 라이선스의 유형을 선택합니다. Plus나 Apex 중 하나 또는 둘 다를 선택하거나 VPN Only를 선택할 수 있습니다. 자세한 내용은 원격 액세스 VPN에 대한 라이선싱 요구 사항, 8 페이지를 참고하십시오.

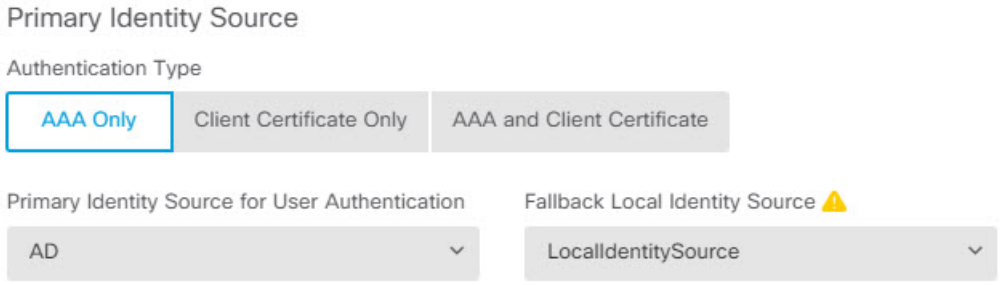


단계 **6** 사이트 A에서 원격 액세스 VPN을 구성합니다.

a) **Device(**디바이스**)** > **Remote Access VPN(**원격 액세스 **VPN)** 그룹에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다. **Connection Profiles(**연결 프로파일**)** 페이지 있어야 합니다.

b) 연결 프로파일을 생성하거나 수정합니다.

c) 마법사의 첫 번째 단계에서는 프로파일 이름을 컨피그레이션하고 AD 영역을 기본 인증 소스로 선택합니다. 선택적으로 로컬 데이터베이스를 대체 ID 소스로 선택할 수 있습니다.



d) 주소 풀을 컨피그레이션합니다.

이 예시에서는 +를 클릭한 후 IPv4 주소 풀에서 **Create New Network(**새 네트워크 생성**)**를 선택하고 172.18.1.0/24 네트워크용 개체를 생성한 후 이 개체를 선택합니다. 그러면 클라이언트에 이 풀의 주소가 할당됩니다. IPv6 풀은 비워 둡니다. 주소 풀은 외부 인터페이스의 IP 주소와 동일한 서브넷에 있을 수 없습니다.

개체는 다음과 같이 표시됩니다.

풀 사양은 다음과 같이 표시됩니다.

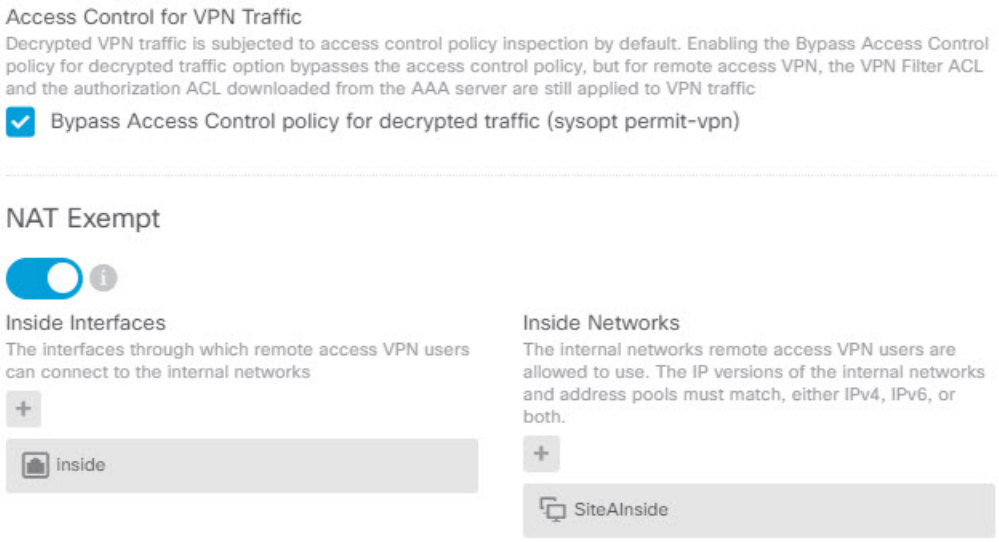
e) **Next(**다음**)**를 클릭한 다음, 적절한 그룹 정책을 선택합니다.

선택한 정책에 대한 요약 정보를 확인합니다. DNS 서버가 컨피그레이션되어 있는지 확인합니다. 그렇지 않은 경우, 지금 바로 정책을 수정하고 DNS를 컨피그레이션합니다.

f) **Next(**다음**)**를 클릭하고, 전역 설정에서 **Bypass Access Control policy for decrypted traffic(**암호 해독된 트래픽에 대해 액세스 제어 정책 우회**) (sysopt permit-vpn)** 옵션을 선택하고 **NAT Exempt(NAT** 제외**)** 옵션을 컨피그레이션합니다.

NAT Exempt(NAT 제외**)**에 대해서는 다음 옵션을 컨피그레이션해야 합니다. 다른 연결 프로파일을 정의한 경우, 컨피그레이션이 모든 연결 프로파일에 적용되므로 기존 설정에 추가해야 한다는 점에 유의하십시오.

- **Inside Interfaces(**내부 인터페이스**)** — 내부 인터페이스를 선택합니다. 이러한 인터페이스는 원격 사용자가 액세스할 내부 네트워크용 인터페이스입니다. NAT 규칙은 이러한 인터페이스에 대해 생성됩니다.
- **Inside Networks(**내부 네트워크**)** — SiteAInside 네트워크 개체를 선택합니다. 이러한 개체는 원격 사용자가 액세스할 내부 네트워크를 나타내는 네트워크 개체입니다.



g) 지원하는 플랫폼에 대한 Secure Client 패키지를 업로드합니다.

h) **Next(**다음**)**를 클릭하고 설정을 확인합니다.

먼저 요약이 정확한지 확인합니다.

그런 다음 지침을 클릭하여 Secure Client 소프트웨어를 처음으로 설치하고 VPN 연결을 완료할 수 있는지를 테스트하기 위해 엔드 유저가 수행해야 하는 작업을 파악합니다. 복사를 클릭하여 이러한 지침을 클립보드에 복사한 다음 텍스트 파일이나 이메일에 붙여넣습니다.

i) **Finish(**종료**)**를 클릭합니다.

단계 **7** 웹 페이지의 오른쪽 상단에 있는 **Deploy Changes(**변경 사항 구축**)** 아이콘을 클릭합니다.

단계 **8** **Deploy Now(**지금 구축**)** 버튼을 클릭하고 구축이 정상적으로 완료될 때까지 기다립니다.

이제 사이트 A 디바이스는 RA VPN 연결을 수락할 준비가 되었습니다. 외부 사용자에게 Secure Client 클라이언트를 설치하고 VPN 연결을 완료하도록 합니다.

디바이스 CLI에 로그인한 다음 **show vpn-sessiondb anyconnect** 명령을 사용해 세션 정보를 확인하면 연결을 확인할 수 있습니다.

그룹별로 RA VPN 액세스를 제어하는 방법

그룹 정책에 따라 내부 리소스에 대한 차등 액세스를 제공하도록 원격 액세스 VPN 연결 프로파일을 컨피그레이션할 수 있습니다. 예를 들어 직원에게는 무제한 액세스를 제공하되 계약업체에는 단일 내부 네트워크 외에는 액세스를 제공하지 않는 경우, 그룹 정책을 사용해 서로 다른 ACL을 정의하여 액세스를 적절히 제한할 수 있습니다.

다음 예에서는 192.168.2.0/24 내부 서브넷에만 액세스해야 하는 계약업체에 대해 RA VPN 연결을 설정하는 방법을 보여줍니다. 정규 직원의 경우, VPN에 대해 정의된 트래픽 필터가 없는 기본 그룹 정책을 사용할 수 있습니다. 이러한 사용자에게 제한을 적용하려면 기본 그룹 정책을 수정하고, 아래에 설명된 대로 구성된 ACL을 적용할 수 있습니다.

시작하기 전에

이 절차에서는 계약업체에 사용할 ID 소스를 이미 생성했다고 가정합니다. 이 소스는 정규 직원에게 사용하는 것과 다를 수 있습니다. 이 ID 소스는 액세스 제한과 딱히 관련이 없으므로 이 예시에서는 생략했습니다.

또한 이 예시에서는 "inside2" 인터페이스가 192.168.2.0/24 서브넷을 호스팅하도록 컨피그레이션되어 있고 IP 주소는 192.168.2.1(서브넷에 있는 다른 주소도 허용됨)이라고 가정합니다.

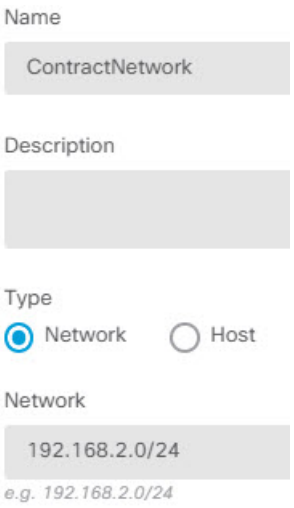
프로시저

단계 **1** RA VPN 트래픽을 제한하기 위한 확장 ACL(액세스 제어 목록)을 컨피그레이션합니다.

타겟인 192.168.2.0/24를 정의하는 네트워크 개체를 먼저 컨피그레이션한 다음, 액세스 목록을 정의하는 스마트 CLI 개체를 생성해야 합니다. ACL은 종단에 암시적 거부가 있기 때문에 서브넷에 대한 액세스만 허용해야 하고, 서브넷 외부의 모든 IP 주소로 전송되는 트래픽은 거부됩니다. 이 예시는 IPv4에만 적용되므로 특정 서브넷에 대한 IPv6 액세스를 제한하기 위해 개체를 구성할 수도 있습니다. 네트워크 개체를 생성하고 동일한 ACL에 IPv6 기반 ACE를 추가하기만 하면 됩니다.

a) **Objects(**개체**)** > **Networks(**네트워크**)**를 선택하고 필요한 개체를 생성합니다.

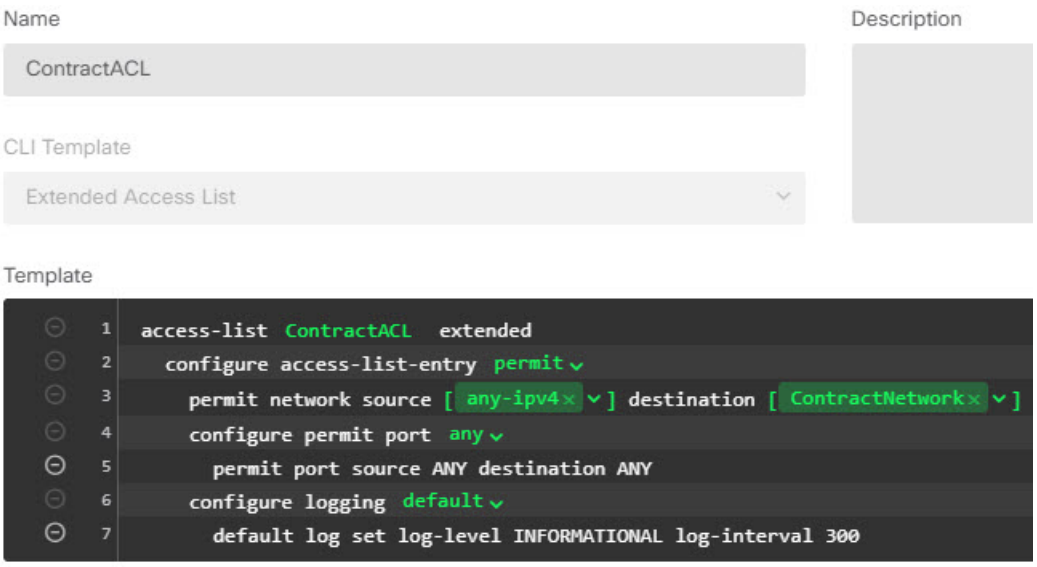
예를 들어 개체에 ContractNetwork라는 이름을 지정합니다. 개체는 다음과 비슷해야 합니다.



b) **Device(**디바이스**)** > **Advanced Configuration(**고급 컨피그레이션**)** > **Smart CLI(**스마트 **CLI)** > **Objects(**개체**)**를 선택합니다.
c) **+**를 클릭하여 새 개체를 생성합니다.
d) ACL의 이름을 입력합니다. 예: **ContractACL**.
e) **CLI Template(CLI** 템플릿**)**에서 **Extended Access List(**확장 액세스 목록**)**를 선택합니다.
f) **Template(**템플릿**)** 본문에서 다음과 같이 컨피그레이션합니다.

- configure access-list-entry action = permit
- source-network = any-ipv4
- destination-network = ContractNetwork object
- configure permit port = any
- configure logging = default

ACE는 다음과 같이 표시되어야 합니다.



g) **OK(**확인**)**를 클릭합니다.

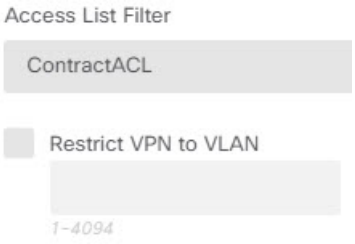
이 ACL은 다음번에 변경 사항을 구축할 때 컨피그레이션됩니다. 다른 정책에서 개체를 사용하여 구축을 강제 적용할 필요가 없습니다.

단계 **2** ACL을 사용하는 그룹 정책을 생성합니다.

최소한 그룹 정책에 대한 DNS 서버도 컨피그레이션해야 합니다. 필요에 따라 다른 옵션을 컨피그레이션할 수 있습니다. 다음 절차에서는 이 활용 사례와 관련이 있는 한 가지 설정에 중점을 둡니다.

a) **Device(**장치**)** > **RA VPN** > **Group Policies(**그룹 정책**)**를 선택합니다.
b) 새 그룹 정책을 생성하려면 **+**를 클릭합니다.
c) **General(**일반**)** 페이지에서 **ContractGroup**과 같이 정책의 이름을 입력합니다.
d) 목차에서 **Traffic Filters(**트래픽 필터**)**를 클릭합니다.
e) **Access List Filter(**액세스 목록 필터**)**에서 ContractACL 개체를 선택합니다.

이 예에서는 VLAN 옵션을 비워 둡니다. 필터링 목적으로 VLAN을 설정하고 VLAN에 대해 하위 인터페이스를 컨피그레이션하는 방법도 있습니다.



f) 그룹 정책을 저장하려면 **OK(**확인**)**를 클릭합니다.

단계 **3** 계약업체를 위한 연결 프로파일을 컨피그레이션합니다.

a) RA VPN 페이지의 목차에서 **Connection Profiles(**연결 프로파일**)**를 클릭합니다.
b) **+** 버튼을 클릭하여 새 연결 프로파일을 생성합니다.

c) 마법사의 1단계를 완료하고 **Next(**다음**)**를 클릭합니다.

예를 들어 Contractors와 같이 프로파일에 대한 이름을 입력합니다.

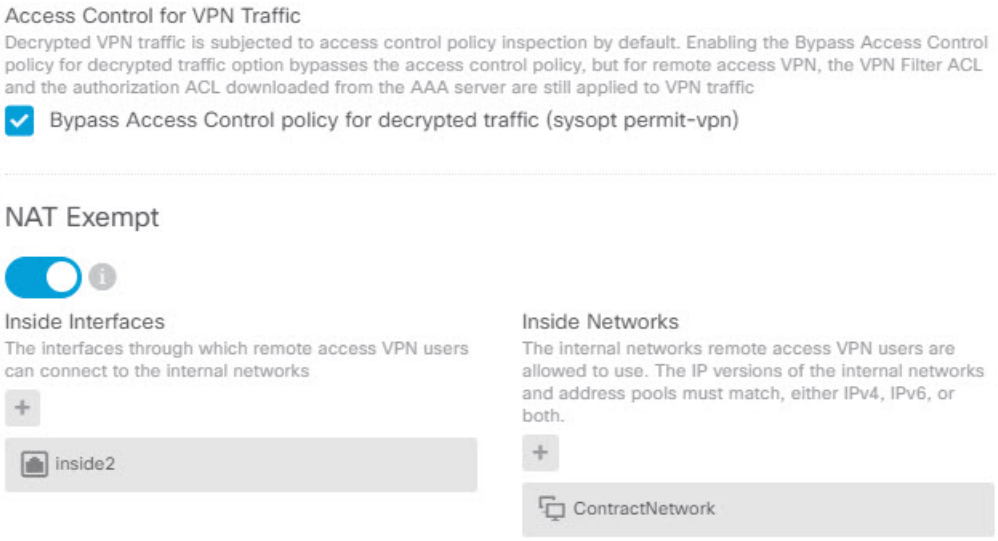
평상시와 같이 나머지 옵션을 컨피그레이션합니다. 여기에는 계약업체를 위한 적절한 인증 소스를 선택하고 주소 풀을 정의하는 작업이 포함됩니다.

d) 계약업체에 대해 컨피그레이션한 그룹 정책을 선택하고 **Next(**다음**)**를 클릭합니다.

e) 전역 설정에서 **Bypass Access Control policy for decrypted traffic(**암호 해독된 트래픽에 대해 액세스 제어 정책 우회**) (sysopt permit-vpn)** 옵션을 선택하고 **NAT Exempt(NAT** 제외**)** 옵션을 컨피그레이션합니다.

NAT Exempt(NAT 제외**)**에 대해서는 다음 옵션을 컨피그레이션해야 합니다. 다른 연결 프로파일을 정의한 경우, 컨피그레이션이 모든 연결 프로파일에 적용되므로 기존 설정에 추가해야 한다는 점에 유의하십시오.

- **Inside Interfaces(**내부 인터페이스**) - inside2** 인터페이스를 선택합니다. 이러한 인터페이스는 원격 사용자가 액세스할 내부 네트워크용 인터페이스입니다. NAT 규칙은 이러한 인터페이스에 대해 생성됩니다.
- **Inside Networks(**내부 네트워크**)** - ContractNetwork 네트워크 개체를 선택합니다. 이러한 개체는 원격 사용자가 액세스할 내부 네트워크를 나타내는 네트워크 개체입니다.



f) 지원하는 플랫폼에 대한 Secure Client 패키지를 업로드합니다.

g) **Next(**다음**)**를 클릭하고 설정을 확인합니다.

먼저 요약이 정확한지 확인합니다.

그런 다음 지침을 클릭하여 Secure Client 소프트웨어를 처음으로 설치하고 VPN 연결을 완료할 수 있는지를 테스트하기 위해 엔드 유저가 수행해야 하는 작업을 파악합니다. 복사를 클릭하여 이러한 지침을 클립보드에 복사한 다음 텍스트 파일이나 이메일에 붙여넣습니다.

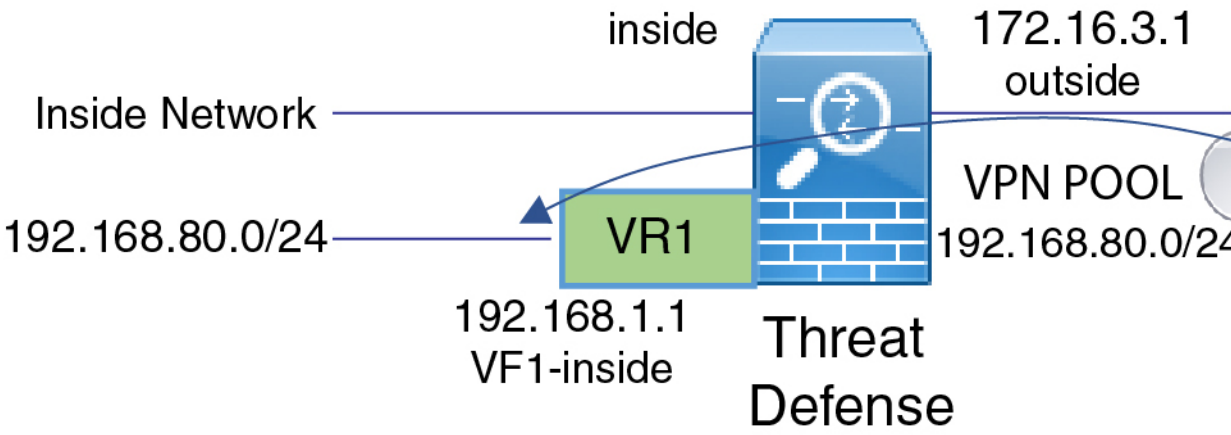
h) **Finish(**종료**)**를 클릭합니다.

RA VPN 액세스를 다른 가상 라우터의 내부 네트워크에 허용하는 방법

디바이스에서 여러 가상 라우터를 구성하는 경우에는 전역 가상 라우터에서 RA VPN을 구성해야 합니다. 사용자 지정 가상 라우터에 할당된 인터페이스에는 RA VPN을 구성할 수 없습니다.

가상 라우터의 라우팅 테이블은 별도이므로 RA VPN 사용자가 다른 가상 라우터에 속한 네트워크에 액세스해야 하는 경우 정적 경로를 생성해야 합니다.

다음과 같은 사례를 가정해보십시오. 이 경우 RA VPN 사용자는 172.16.3.1의 외부 인터페이스에 연결되며 192.168.80.0/24 풀 내에 IP 주소가 지정됩니다. 이 사용자는 이제 전역 가상 라우터에 연결된 내부 네트워크에 액세스할 수 있습니다. 그러나 사용자는 가상 라우터 VR1의 일부인 192.168.1.0/24 네트워크에 연결할 수 없습니다. VR1 네트워크와 RA VPN 사용자 간의 트래픽 흐름을 허용하려면 정적 경로를 두 가지 방식으로 모두 구성해야 합니다.



시작하기 전에

이 예에서는 RA VPN을 이미 구성하고 가상 라우터를 정의했으며 적절한 가상 라우터에 인터페이스를 구성 및 할당한 것으로 가정합니다.

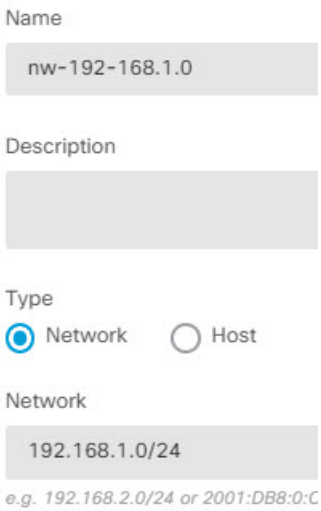
프로시저

단계 **1** 전역 가상 라우터에서 VR1으로의 경로 유출을 구성합니다.

이 경로를 사용하면 VPN 풀에서 Secure Client 할당 IP 주소로 VR1 가상 라우터에서 192.168.1.0/24 네트워크에 액세스할 수 있습니다.

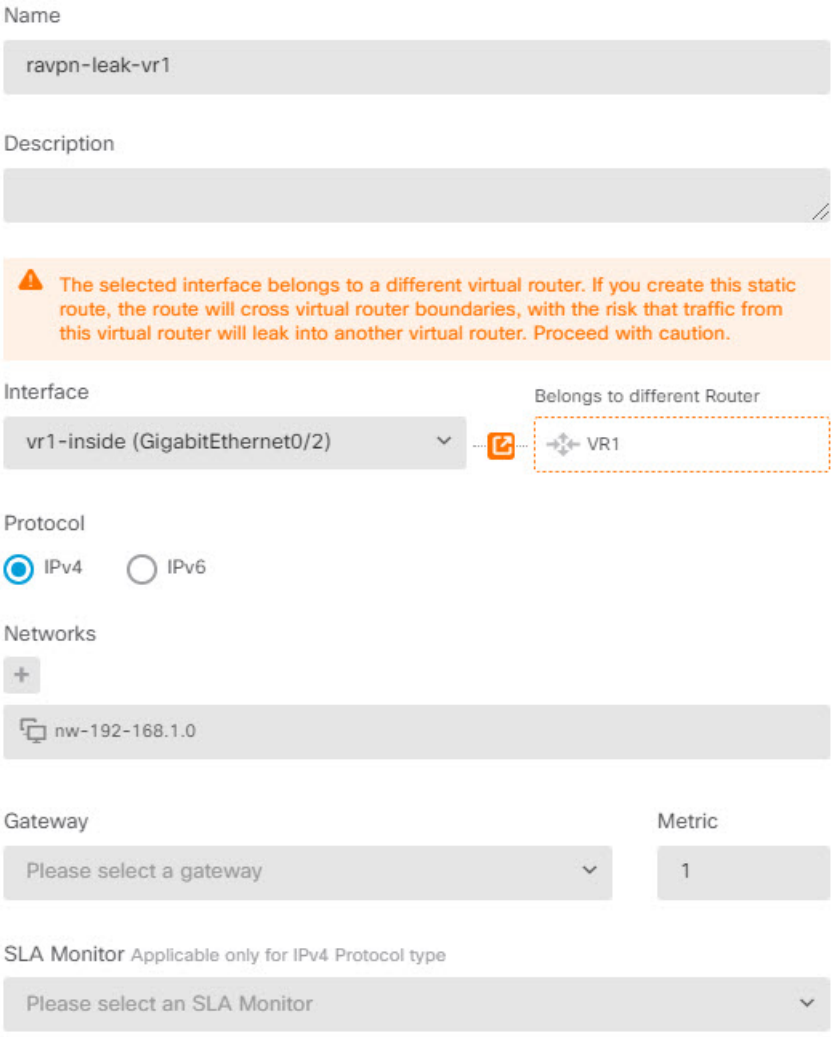
a) **Device(**디바이스**)** > **Routing(**라우팅**)** > **View Configuration(**구성 보기**)**을 선택합니다.
b) 전역 가상 라우터의 View Icon(아이콘 보기)을 클릭합니다.
c) 전역 라우터에 대한 **Static Routing(**정적 라우팅**)** 탭에서 **+**를 클릭하고 다음과 같이 경로를 구성합니다.

- **Name(**이름**)**-모든 이름(예: **ravpn-leak-vr1**)이 수행됩니다.
- **Interface(**인터페이스**)** — **vr1-inside**를 선택합니다.
- **Protocol(**프로토콜**)** — **IPv4**를 선택합니다.
- **Network(**네트워크**)**—192.168.1.0/24 네트워크를 정의하는 개체를 선택합니다. 필요한 경우 **Create New Network(**새 네트워크 생성**)**를 클릭하면 바로 개체를 생성할 수 있습니다.



- **Gateway(**게이트웨이**)** — 이 항목은 비워둡니다. 다른 가상 라우터로 경로를 유출할 경우에는 게이트웨이 주소를 선택하지 않습니다.

대화 상자가 다음과 비슷하게 표시됩니다.



d) **OK(**확인**)**를 클릭합니다.

단계 **2** VR1에서 전역 가상 라우터로의 경로 유출을 구성합니다.

이 경로를 사용하면 192.168.1.0/24 네트워크의 엔드포인트가 VPN 풀에서 Secure Client 할당 IP 주소에 대한 연결을 시작할 수 있습니다.

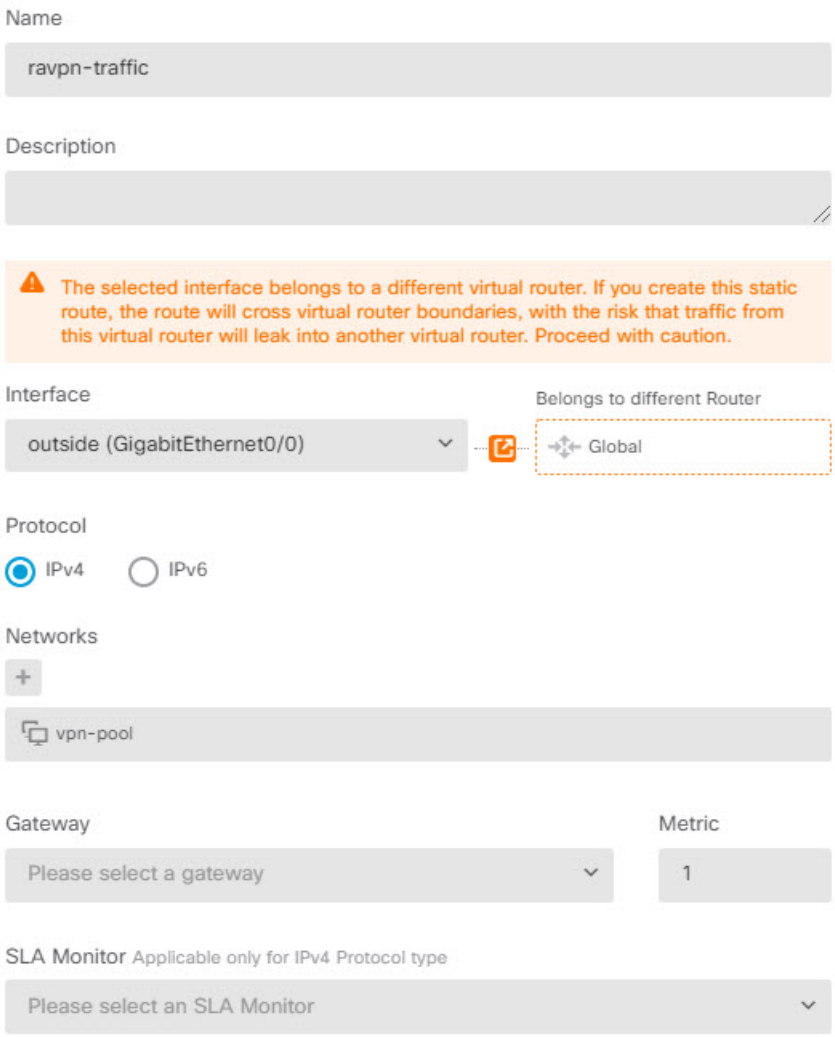
a) 가상 라우터 드롭다운 목록에서 **VR1**을 선택하여 VR1 구성으로 전환합니다.

b) VR1 가상 라우터에 대한 **Static Routing(**정적 라우팅**)** 탭에서 +를 클릭하고 다음과 같이 경로를 구성합니다.

- **Name(**이름**)** - 모든 이름(예: **ravpn-traffic**)이 수행됩니다.
- **Interface(**인터페이스**)** — **outside**를 선택합니다.
- **Protocol(**프로토콜**)** — **IPv4**를 선택합니다.
- **Natwork(**네트워크**)** - VPN 풀에 대해 생성한 개체(예: **vpn-pool**)를 선택합니다.

- **Gateway(**게이트웨이**)** — 이 항목은 비워둡니다. 다른 가상 라우터로 경로를 유출할 경우에는 게이트웨이 주소를 선택하지 않습니다.

대화 상자가 다음과 비슷하게 표시됩니다.



c) **OK(**확인**)**를 클릭합니다.

다음에 수행할 작업

RA VPN 주소 풀과 사용자 지정 가상 라우터의 IP 주소 간에 중복 항목이 있는 경우 IP 주소에서 고정 NAT 규칙을 또한 사용하여 적절한 라우팅을 활성화해야 합니다. 그러나 중복되지 않도록 간단히 RA VPN 주소 풀을 변경하는 것이 훨씬 쉽습니다.

Secure Client 아이콘 및 로고를 맞춤화하는 방법

Windows 및 Linux 클라이언트 시스템에서 Secure Client 앱의 아이콘과 로고를 맞춤화할 수 있습니다. 아이콘의 이름은 미리 정의되어 있으며 업로드하는 이미지의 파일 유형 및 크기에 대한 특정 제한이 있습니다.

GUI를 맞춤화하기 위해 고유한 실행 파일을 구축할 경우 어떠한 파일명도 사용할 수 있지만, 이 예에서는 맞춤화된 프레임워크를 구축하지 않고 단순히 아이콘과 로고를 교체한다고 가정합니다.

대체할 수 있는 여러 이미지가 있으며 파일 이름은 플랫폼에 따라 다릅니다. 맞춤화 옵션, 파일 이름, 유형 및 크기에 대한 자세한 내용은 *Cisco Secure Client* 관리자 가이드에서 Secure Client 및 설치 프로그램의 맞춤화 및 현지화에 대한 챕터를 참조하십시오. 예를 들어 4.8 클라이언트 챕터는 다음에서 사용할 수 있습니다.

https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect48/administration/guide/b_AnyConnect_Administrator_Guide_4-8/customize-localize-anyconnect.html

시작하기 전에

이 예의 목적을 위해 Windows 클라이언트의 다음 이미지를 교체합니다. 이미지가 최대 크기와 다른 경우 시스템에서는 자동으로 이를 최대 크기로 조정하고 필요한 경우 이미지를 늘립니다.

- app_logo.png

  이 애플리케이션 로고 이미지는 애플리케이션 아이콘이며 최대 크기는 128 x 128 픽셀입니다.

- company_logo.png

  이 기업 로고 이미지는 트레이 플라이아웃 및 Advanced(고급) 대화 상자의 왼쪽 위 모서리에 표시됩니다. 최대 크기는 97 x 58 픽셀입니다.

- company_logo_alt.png

  다른 기업 로고 이미지는 About(정보) 대화 상자의 오른쪽 아래 모서리에 표시됩니다. 최대 크기는 97 x 58 픽셀입니다.

이러한 파일을 업로드하려면 threat defense 디바이스가 액세스할 수있는 서버에 파일을 배치해야 합니다. TFTP, FTP, HTTP, HTTPS 또는 SCP 서버를 사용할 수 있습니다. 이러한 파일에서 이미지를 가져오는 URL에는 서버 설정에 필요한대로 경로 및 사용자 이름/비밀번호가 포함될 수 있습니다. 이 예에서는 TFTP를 사용합니다.

프로시저

단계 **1** 맞춤화된 아이콘 및 로고를 사용해야 하는 RA VPN 헤드엔드 역할을 하는 각 threat defense 디바이스에 이미지 파일을 업로드합니다.

a) SSH 클라이언트를 사용하여 디바이스 CLI에 로그인합니다.

b) CLI에서 **system support diagnostic-cli** 명령을 입력하여 진단 CLI 모드를 시작합니다.

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
```

```
Type help or '?' for a list of available commands.

ftdv1>
```

참고 메시지를 읽어보십시오! **Ctrl+a**를 누른 다음 **d**를 눌러 진단 CLI에서 나와 일반 threat defense CLI 모드로 돌아와야 합니다.

c) 명령 프롬프트를 참고합니다. 일반 CLI에서는 > 만 사용하는 반면, 진단 CLI의 사용자 EXEC 모드에서는 호스트 이름 + >를 사용합니다. 이 예에서는 ftdv1>입니다. #를 종료 문자로 사용하는 특별 권한 EXEC 모드를 시작해야 합니다(예 : ftdv1 #). 프롬프트에 이미 #이 있는 경우 이 단계를 건너 뜁니다. 그렇지 않으면 enable 명령을 입력하고 비밀번호를 입력하지 않고 비밀번호 프롬프트에서 Enter를 누릅니다.

```
ftdv1> enable
Password:
ftdv1#
```

d) **copy** 명령을 사용하여 각 파일을 호스팅 서버에서 threat defense 디바이스의 disk0으로 복사합니다. disk0:/anyconnect-images/와 같은 하위 디렉토리에 이들을 배치할 수 있습니다. **mkdir** 명령을 사용하여 새 폴더를 생성할 수 있습니다.

예를 들어 TFTP 서버의 IP 주소가 10.7.0.80이고 새 디렉토리를 생성하려는 경우 명령은 다음과 유사합니다. 첫 번째 예 이후에는 **copy** 명령에 대한 응답이 생략됩니다.

```
ftdv1# mkdir disk0:anyconnect-images

Create directory filename [anyconnect-images]? yes

Created dir disk0:/anyconnect-images

ftdv1# copy /noconfirm tftp://10.7.0.80/app_logo.png
disk0:/anyconnect-images/app_logo.png

Accessing tftp://10.7.0.80/app_logo.png...!!!!!!
Writing file disk0:/anyconnect-images/app_logo.png...
!!!!!!
12288 bytes copied in 1.000 secs (12288 bytes/sec)

ftdv1# copy /noconfirm tftp://10.7.0.80/company_logo.png
disk0:/anyconnect-images/company_logo.png
ftdv1# copy /noconfirm tftp://10.7.0.80/company_logo_alt.png
disk0:/anyconnect-images/company_logo_alt.png
```

단계 **2** 클라이언트 시스템에 설치할 때 진단 CLI의 **import webvpn** 명령을 사용하여 Secure Client에 이러한 이미지를 다운로드하도록 지시합니다.

import webvpn AnyConnect-customization type resource platform win name *filename* **disk0:**/*directoryname/filename*

이 명령은 Windows용입니다. Linux의 경우 **win** 키워드를 클라이언트에 따라 **linux** 또는 **linux-64**으로 대체합니다.

예를 들어 이전 단계에서 업로드한 파일을 가져오고 진단 CLI에 아직 있다고 가정합니다.

```
ftdv1# import webvpn AnyConnect-customization type resource platform win
name app_logo.png disk0:/anyconnect-images/app_logo.png
```

```
ftdv1# import webvpn AnyConnect-customization type resource platform win
name company_logo.png disk0:/anyconnect-images/company_logo.png

ftdv1# import webvpn AnyConnect-customization type resource platform win
name company_logo_alt.png disk0:/anyconnect-images/company_logo_alt.png
```

단계 **3** 컨피그레이션을 확인합니다.

- 가져온 파일을 확인하려면 진단 CLI의 특별 권한 EXEC 모드에서 **show import webvpn AnyConnect-customization** 명령을 사용하십시오.
- 이미지가 클라이언트에 다운로드되었는지 확인하려면 사용자가 클라이언트를 실행할 때 이미지가 표시되어야 합니다. Windows 클라이언트에서 다음 폴더를 확인할 수도 있습니다. 여기서 %PROGRAMFILES%는 일반적으로 c:\Program Files로 확인됩니다.

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

다음에 수행할 작업

기본 이미지로 돌아가려면 맞춤화한 각 이미지에 대해(진단 CLI 특별 권한 EXEC 모드에서) **revert webvpn** 명령을 사용합니다. 명령은 다음과 같습니다.

revert webvpn AnyConnect-customization type resource platform win name *filename*

import webvpn에서와 마찬가지로 해당 클라이언트 플랫폼을 맞춤화한 경우, **win**을 **linux** 또는 **linux-64**로 대체하고 가져온 각 이미지 파일 이름에 대해 명령을 개별적으로 실행합니다. 예를 들면 다음과 같습니다.

```
ftdv1# revert webvpn AnyConnect-customization type resource platform win
name app_logo.png

ftdv1# revert webvpn AnyConnect-customization type resource platform win
name company_logo.png

ftdv1# revert webvpn AnyConnect-customization type resource platform win
name company_logo_alt.png
```