Cisco Secure Firewall Management Center를 사용하여 모바일 디바이스에서 애플리케이션 기반 원격 액세스 VPN(앱별 VPN) 구성

초판: 2023년 7월 31일

Cisco Secure Firewall Management Center를 사용하여 모바일 디바이스에서 애플리케이션 기반 원격 액세스 VPN(앱별 VPN) 구성

앱별 VPN 소개

원격 사용자가 Secure Client를 사용하여 모바일 디바이스에서 VPN 연결을 설정하면 개인 애플리케이션의 트래픽을 포함한 모든 트래픽이 VPN을 통해 라우팅됩니다.

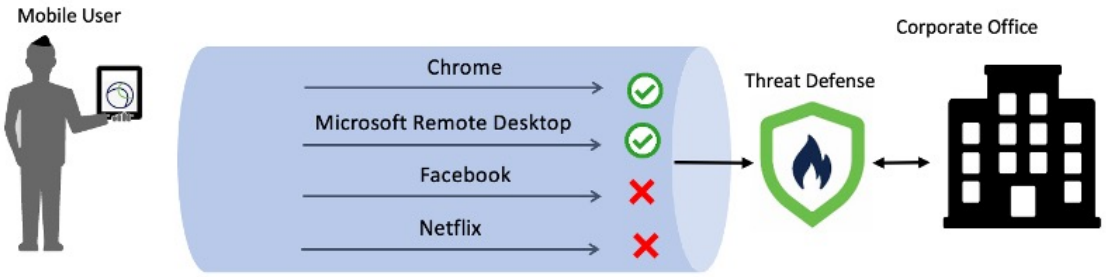
Android 또는 iOS에서 실행되는 모바일 디바이스에 대해 VPN 터널을 통과하는 애플리케이션을 제한할 수 있습니다. 이 애플리케이션 기반 원격 액세스 VPN을 앱별 VPN이라고 합니다.

앱별 VPN을 사용하려면 다음 작업을 수행해야 합니다.

1. 타사 MDM(Mobile Device Manager) 서버를 설치하고 구성합니다.
2. MDM 서버의 VPN 터널을 통과할 수 있는 승인된 애플리케이션 목록을 정의합니다.
3. MDM 서버에서 모바일 디바이스로 앱별 구성을 구축합니다.
4. 매니지드 헤드엔드 Threat Defense에서 앱별 VPN을 구성합니다.

MDM 매니지드 모바일 디바이스가 Secure Client를 사용하여 VPN에 연결되면, 클라이언트는 트래픽을 터널링하기 전에 애플리케이션을 검증합니다. Threat Defense에 구성된 앱별 정책이 이 검증을 수행합니다.

다음 그림에는 Threat Defense를 사용하는 앱별 VPN의 예가 나와 있습니다.



장점

- 기업 네트워크를 통한 VPN 트래픽을 제한하고 VPN 헤드엔드의 리소스를 확보합니다. 다음을 차단할 수 있습니다.
  - VPN을 통한 Netflix, Facebook, 유튜브 같은 애플리케이션.
  - VPN을 통한 Outlook, Webex와 같은 신뢰할 수 있는 클라우드 애플리케이션.
- 트래픽 최적화.
- 레이턴시 최소화.
- 모바일 디바이스에서 승인되지 않은 악성 애플리케이션으로부터 기업 VPN 터널을 보호합니다.

가이드의 적합성 확인

이 활용 사례는 원격 액세스 VPN을 사용하여 조직의 네트워크에 연결하는 원격 근무자를 위해 Management Center를 통해 앱별 VPN을 구성하는 네트워크 관리자를 대상으로 합니다.

버전 6.4~6.7에서는 FlexConfig를 사용하여 FTD에서 앱별 VPN을 활성화할 수 있습니다. 자세한 내용은 모바일 디바이스의 애플리케이션 기반(앱별 VPN) 원격 액세스 VPN 구성을 참조하십시오. 버전 7.0 이상에서는 Management Center UI를 사용하여 Threat Defense에서 앱별 VPN을 활성화할 수 있습니다.

시스템 요구 사항

아래 테이블에는 이 기능이 지원되는 플랫폼이 나와 있습니다.

제품	버전	이 문서에 사용된 버전
Cisco Secure Firewall Threat Defense(구 Firepower Threat Defense/FTD)	7.0 이상	7.3

제품	버전	이 문서에 사용된 버전
Cisco Secure Firewall Management Center(구 Firepower Management Center/FMC)	7.0 이상	7.3
Cisco Secure Client(구 AnyConnect)	4.0 이상	5.0
Android 디바이스	Android 5.0 이상	-
Apple iOS 디바이스	Apple iOS 8.3 이상	-

앱별 VPN 터널 구성을 위한 사전 요건

다음을 확인하십시오.

- Management Center에서 원격 액세스 VPN 정책을 구성했는지 확인합니다.
- MDM 서버를 설정하고 각 모바일 디바이스를 MDM 서버에 등록했는지 확인합니다.

  자세한 내용은 MDM 설명서를 참조하십시오.

  MDM 서버에서 VPN 터널을 통과할 수 있는 애플리케이션을 구성하는 것이 좋습니다. 이 구성은 헤드엔드 구성을 단순화합니다.
- Cisco 소프트웨어 다운로드 센터에서 로컬 호스트에 Cisco AnyConnect 엔터프라이즈 애플리케이션 선택기를 다운로드하고 설치했는지 확인합니다.

  앱별 VPN 정책을 정의하려면 이 툴이 필요합니다.

라이선스:

- 다음 Secure Client 라이선스 중 하나가 필요합니다.

  Secure Client Premier 또는 Secure Client Advantage.
- Management Center Essentials 라이선스는 내보내기 제어 기능을 허용해야 합니다.

  System(시스템**)** > **Licenses(**라이선스**)** > **Smart Licenses(**스마트 라이선스**)**를 선택하여 Management Center에서 이 기능을 확인합니다.

Management Center를 사용하여 앱별 VPN을 구성하는 방법

단계	수행해야 할 작업	추가 정보
1	필수 구성 요소를 충족해야 합니다.	앱별 VPN 터널 구성을 위한 사전 요건, 3 페이지
2	터널에서 허용할 애플리케이션을 결정합니다.	-

단계	수행해야 할 작업	추가 정보
3	모바일 애플리케이션의 애플리케이션 ID를 확인합니다.	모바일 애플리케이션의 애플리케이션 ID 확인, 4 페이지
4	Android 및 Apple iOS 디바이스에 대한 앱별 VPN 정책을 정의합니다.	Android 및 Apple iOS 디바이스용 앱별 VPN 정책 정의, 5 페이지
5	Management Center에서 앱별 VPN 정책을 원격 액세스 VPN에 할당합니다.	Management Center에서 원격 액세스 VPN에 앱별 VPN 정책 할당, 8 페이지
6	구성을 Threat Defense에 구축합니다.	Management Center 메뉴 모음에서 **Deploy(구축)**를 클릭한 다음 **Deployment(구축)**를 선택합니다.

모바일 애플리케이션의 애플리케이션 ID 확인

헤드엔드에서 허용되는 애플리케이션 목록을 구성하려면 각 엔드포인트 유형에서 각 애플리케이션의 애플리케이션 ID를 확인해야 합니다.

참고 MDM 서버에서 앱별 정책을 구성하는 것이 좋습니다. 이 구성은 헤드엔드 구성을 단순화합니다.

애플리케이션 ID, 즉 iOS의 번들 ID는 역방향 DNS 이름입니다. 별표(*)를 와일드카드로 사용할 수 있습니다. 예를 들어 *.*는 모든 애플리케이션을 나타내고, com.cisco.*는 모든 Cisco 애플리케이션을 나타냅니다.

애플리케이션 ID를 확인하려면 다음을 수행합니다.

- **Android**
  1. 웹 브라우저에서 Google Play(https://play.google.com/store/)로 이동합니다.
  2. **Apps(앱)** 탭을 클릭합니다.
  3. VPN 터널에서 허용할 애플리케이션을 클릭합니다.

     애플리케이션 ID는 URL의 일부입니다.
  4. 'id=' 매개변수 뒤에 오는 문자열을 복사합니다.

     Microsoft 원격 데스크톱의 경우 URL은 다음과 같습니다.

     https://play.google.com/store/apps/details?id=com.microsoft.rdc.androidx. 앱 id는 com.microsoft.rdc.androidx입니다.

  Google Play에서 사용할 수 없는 애플리케이션의 경우 패키지 이름 뷰어 애플리케이션을 다운로드하여 앱 ID를 추출합니다.

- **iOS**
  1. 웹 브라우저에서 Apple App Store(https://www.apple.com/in/app-store/)로 이동합니다.

2. 검색 결과에서 애플리케이션을 검색합니다.

   애플리케이션 ID는 URL의 일부입니다.

3. 'id' 문자열 뒤에 오는 숫자를 복사합니다.

   Facebook의 경우 URL은 다음과 같습니다.

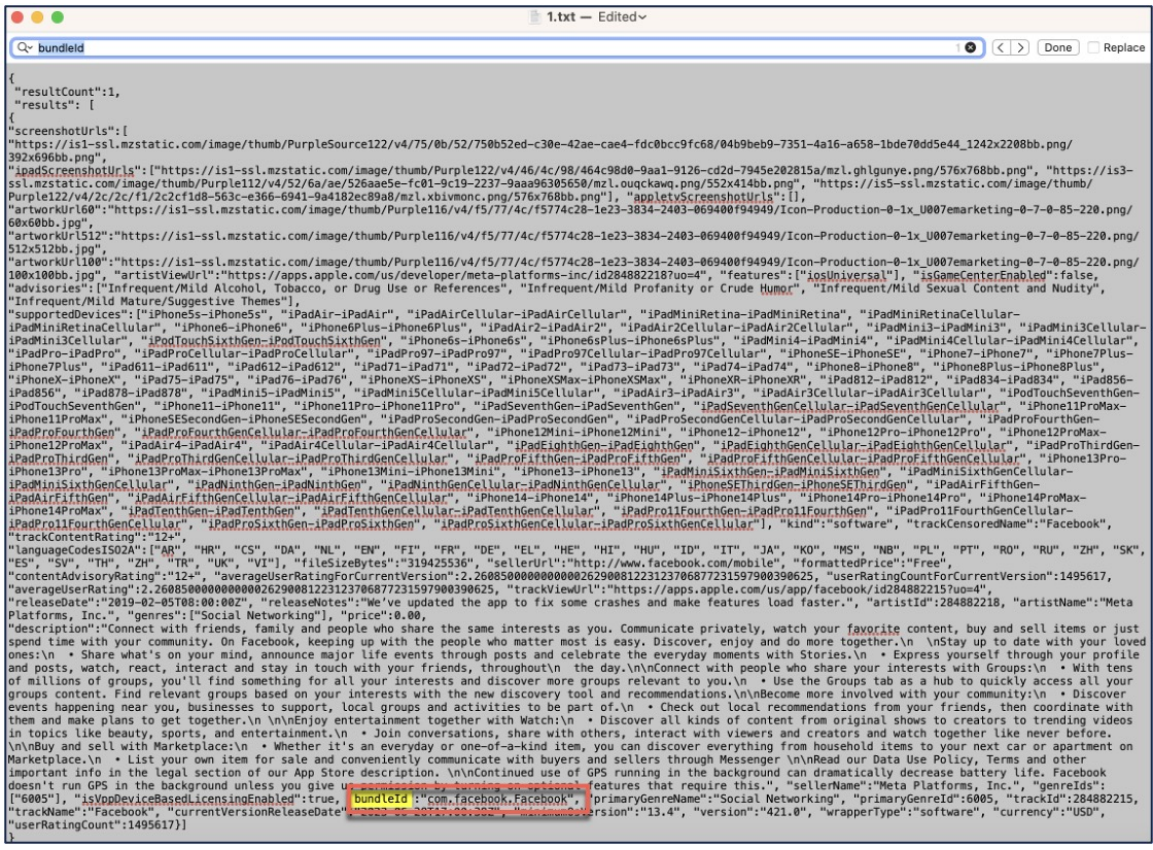
   https://apps.apple.com/in/app/facebook/id284882215. 애플리케이션 ID는 284882215입니다.

4. 새 브라우저 창을 열고 URL(https://itunes.apple.com/lookup?id=) 끝에 이 숫자를 추가합니다.

   Facebook의 경우 URL은 https://itunes.apple.com/lookup?id=284882215입니다.

5. 텍스트 파일을 다운로드합니다. 이름은 보통 1.txt입니다.

6. 텍스트 편집기에서 파일을 열고 'bundleId'를 검색합니다. Facebook의 경우 'bundleId'는 " com.facebook.Facebook"입니다. 이 번들 ID를 앱 ID로 사용합니다.



애플리케이션 ID 목록이 있으면 아래 절차에 설명된 대로 모바일 디바이스에 대한 정책을 정의할 수 있습니다.

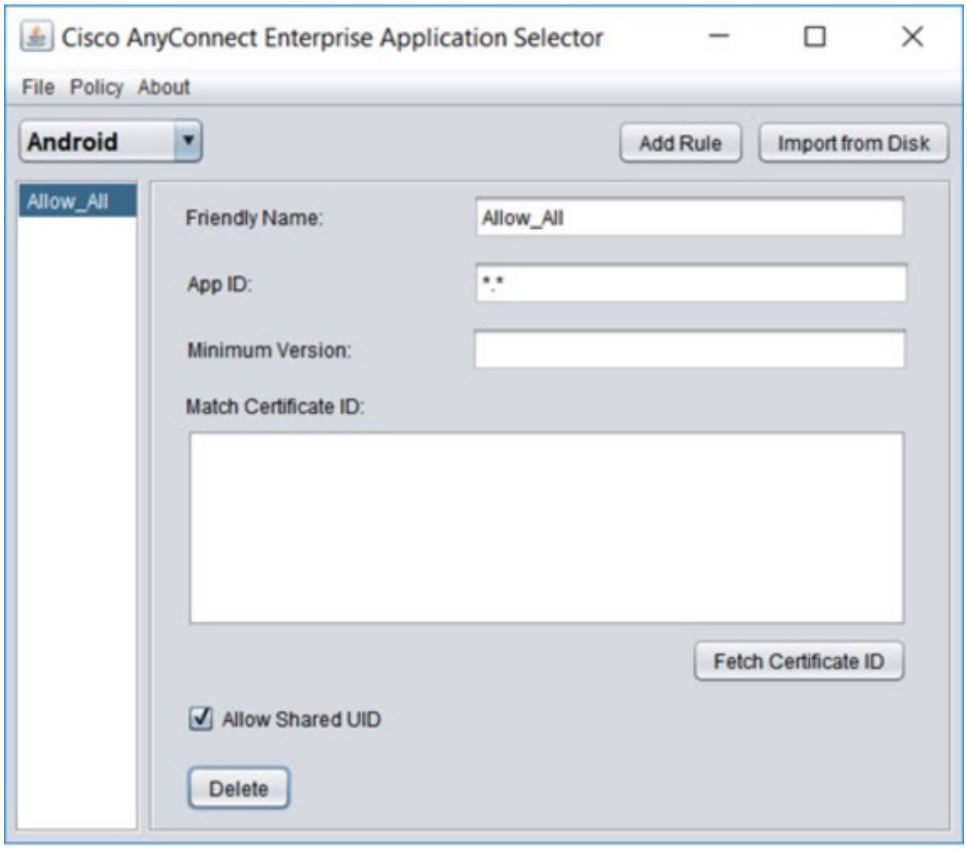
Android 및 Apple iOS 디바이스용 앱별 VPN 정책 정의

Cisco AnyConnect 엔터프라이즈 애플리케이션 선택기를 사용하여 앱별 VPN 정책을 정의합니다.

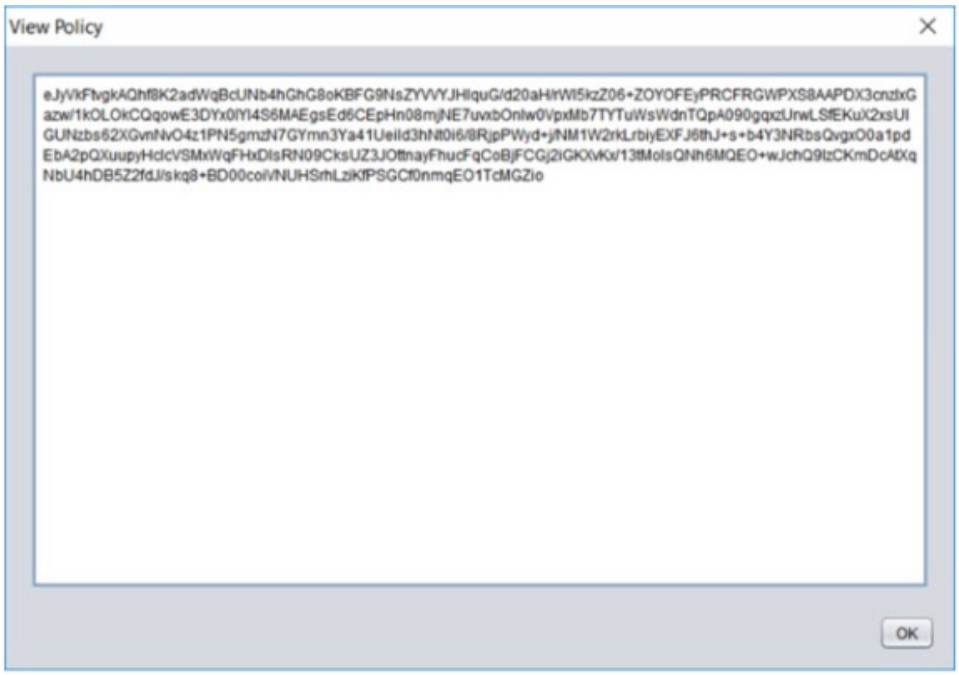
간단한 'Allow All(모두 허용)' 정책을 생성한 후 MDM에 허용되는 애플리케이션을 정의하는 것이 좋습니다. 그러나 헤드엔드에서 목록을 허용하고 제어할 애플리케이션 목록을 지정할 수 있습니다. 특정 애플리케이션을 포함하려면 고유한 이름과 애플리케이션의 앱 ID를 사용하여 각 애플리케이션에 별도의 규칙을 생성합니다.

AnyConnect 엔터프라이즈 애플리케이션 선택기를 사용하여 Android 및 iOS 플랫폼을 모두 지원하는 **Allow All(**모두 허용**)** 정책(와일드카드 정책)을 생성하려면 다음을 수행합니다.

1. 플랫폼 유형으로 드롭다운 목록에서 **Android** 또는 **iOS**를 선택합니다.
2. 다음 옵션을 구성합니다.
   - **Friendly Name(**식별 이름**)** - 정책의 이름을 입력합니다. 예를 들어 Allow_All로 지정할 수 있습니다.
   - **App ID(**앱 **ID)** - 가능한 모든 애플리케이션과 일치하도록 *.*를 입력합니다.
   - 다른 옵션은 그대로 둡니다.

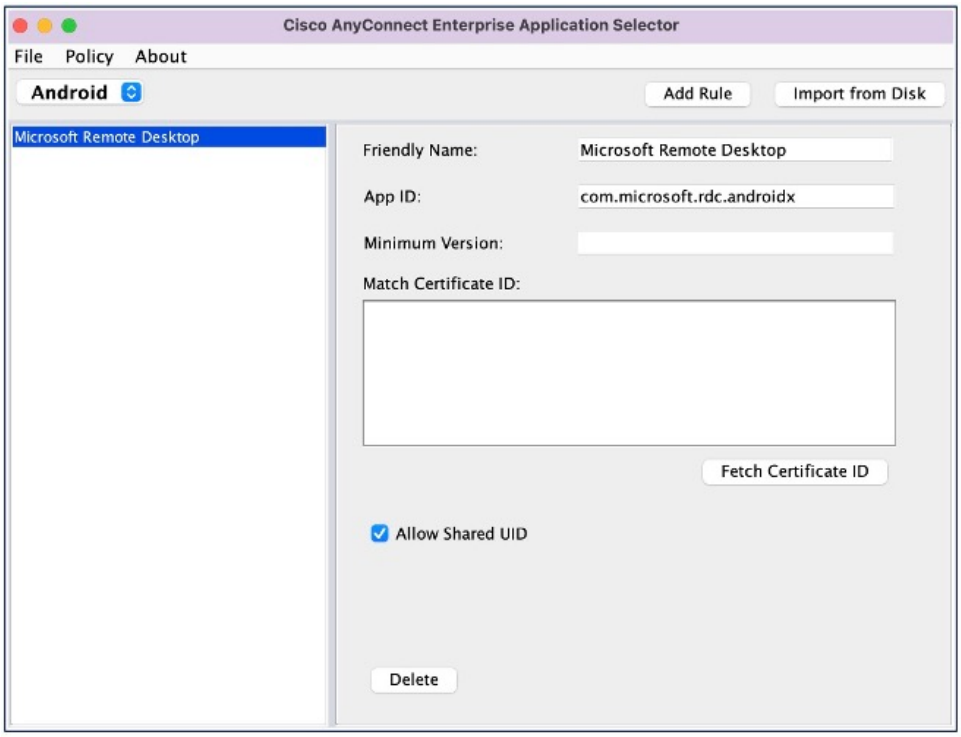


3. **Policy(**정책**)** > **View Policy(**정책 보기**)**를 선택하여 정책에 대한 base64 인코딩 문자열을 가져옵니다. 이 문자열에는 Threat Defense가 정책을 확인하도록 허용하는 암호화된 XML 파일이 포함되어 있습니다. 이 값을 복사합니다. 다음 단계에서 Threat Defense에 앱별 VPN을 구성할 때 이 문자열이 필요합니다.



AnyConnect 엔터프라이즈 애플리케이션 선택기를 사용하여 Microsoft 원격 데스크톱 애플리케이션에 대한 정책을 생성하려면 다음을 수행합니다.

1. 플랫폼 유형으로 드롭다운 목록에서 **Android**를 선택합니다.
2. 다음 옵션을 구성합니다.
   - **Friendly Name(**식별 이름**)** - 정책 이름을 입력합니다.
   - **App ID(**앱 **ID)** - Android의 경우 com.microsoft.rdc.androidx를 입력합니다.
   - 다른 옵션은 그대로 둡니다.



3. **Policy(**정책**)** > **View Policy(**정책 보기**)**를 선택하여 정책에 대한 base64 인코딩 문자열을 가져옵니다.

Management Center에서 원격 액세스 VPN에 앱별 VPN 정책 할당

프로시저

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

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

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

단계 **4** **Edit Group Policy(**그룹 정책 편집**)**를 클릭합니다.

단계 **5** **Secure Client** 탭을 클릭합니다.

단계 **6** **Custom Attributes(**사용자 지정 속성**)**를 클릭하고 +를 클릭합니다.

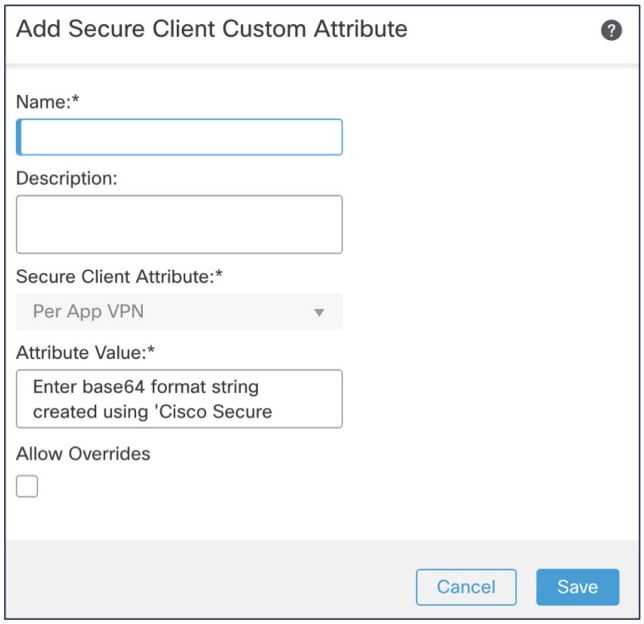
단계 **7** **Secure Client Attribute(Secure Client** 속성**)** 드롭다운 목록에서 Per App VPN(앱별 VPN)을 선택합니다.

단계 **8** **Custom Attribute Object(**사용자 지정 속성 개체**)** 드롭다운 목록에서 개체를 선택하거나 +를 클릭하여 개체를 추가합니다.

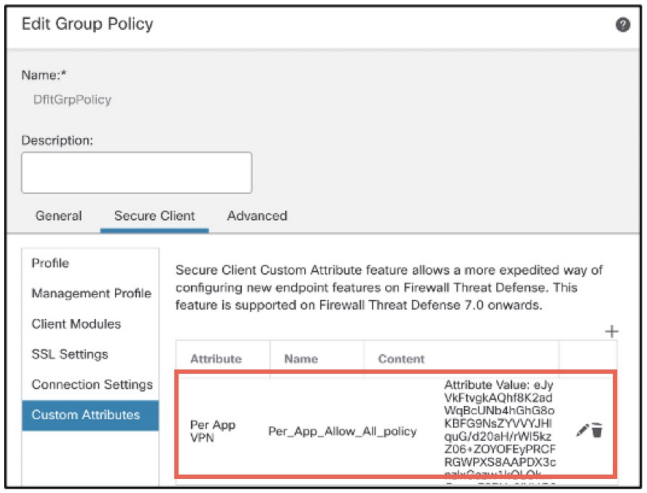
앱별 VPN에 대한 새 사용자 지정 속성 개체를 추가하는 경우:

1. 이름과 설명을 입력합니다.

2. **Attribute Value(**속성 값**)** 필드에 Cisco AnyConnect 엔터프라이즈 애플리케이션 선택기의 base64 인코딩 정책 문자열을 지정합니다.



단계 **9** **Save(**저장**)** 및 **Add(**추가**)**를 차례로 클릭합니다.



단계 **10** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

1. 구성을 Threat Defense에 구축합니다.
2. Secure Client를 사용하여 Threat Defense에 대한 VPN 연결을 설정합니다.

3. 앱별 VPN 구성 확인.

앱별 VPN 구성 확인

Threat Defense에서

Threat Defense에서 다음 명령을 사용하여 앱별 구성을 확인합니다.

명령	설명
show run webvpn	Secure Client 구성의 세부 정보를 확인합니다.
show run group-policy <group_policy_name>	Secure Client에 대한 원격 액세스 VPN 그룹 정책의 세부 정보를 확인합니다.
show vpn-sessiondb anyconnect	활성 Secure Client VPN 세션의 세부 정보를 확인합니다.
show run anyconnect-custom-data	앱별 구성의 세부 정보를 확인합니다.

sh run webvpn의 출력 샘플은 다음과 같습니다.

```
firepower# sh run webvpn
 webvpn
 enable inside
 anyconnect-custom-attr perapp description Per-App Allow
 http-headers
 hsts-server
 enable
 max-age 31536000
 include-sub-domains
 no preload
 hsts-client
 enable
 x-content-type-options
 x-xss-protection
 content-security-policy
 anyconnect image disk0:/csm/cisco-secure-client-win-5.0.03076-webdeploy-k9 1 regex "Windows"

 anyconnect enable
 tunnel-group-list enable
 cache
 no disable
 error-recovery disable
```

sh run anyconnect-custom-data의 출력 샘플은 다음과 같습니다.

```
firepower# sh run anyconnect-custom-data
anyconnect-custom-data perapp PerAppPolicy
eJw9kFtvgkAQhf8K2ae2GC+rqPFNgYjgBcUL2PRhCyuuZVlkuRv/
```

sh running-config group-policy의 출력 샘플은 다음과 같습니다.

```
firepower# sh running-config group-policy
 group-policy DfltGrpPolicy attributes
 vpn-tunnel-protocol ikev2 ssl-client
```

```
user-authentication-idle-timeout none
anyconnect-custom perapp value PerAppPolicy
webvpn
anyconnect keep-installer none
anyconnect modules value none
anyconnect ask none default anyconnect
http-comp none
activex-relay disable
file-entry disable
file-browsing disable
url-entry disable
deny-message none
```

엔드포인트

엔드포인트가 Threat Defense와 VPN 연결을 설정한 후 Secure Client의 통계 아이콘을 클릭합니다.

- **Tunnel Mode(**터널 모드**)**는 "Tunnel All Traffic(모든 트래픽 터널링)"이 아닌 "Application Tunnel(애플리케이션 터널)"이 됩니다.
- **Tunneled Apps(**터널링된 앱**)**에는 MDM에서 터널링을 위해 활성화한 애플리케이션이 나열됩니다.