Cisco SIG(Secure Internet Gateway)에 고객을 안전하게 연결

Cisco Defense Orchestrator를 사용한 ASA 관리

Umbrella는 인터넷 기반 위협에 대한 여러 레벨의 방어를 제공하는 Cisco의 클라우드 기반 SIG(Secure Internet Gateway) 플랫폼입니다. Umbrella는 보안 웹 게이트웨이, 방화벽, DNS 레이어 보안 및 CASB(Cloud Access Security Broker) 기능을 통합하여 위협으로부터 시스템을 보호합니다. SIG 및 DNS 보호를 활용하면 ASA 디바이스는 디바이스의 로컬 DNS 검사 정책과 Umbrella 클라우드 기반 DNS 검사 정책 모두로 보호됩니다. Umbrella는 수신 트래픽을 검사하고 탐지할 수 있는 여러 가지 방법을 제공하므로 ASA 디바이스를 FTD 차세대 방화벽(NGFW)과 비교할 수 있습니다.

현재 CDO는 Umbrella 조직과의 ASA 통합만 지원합니다.

SASE를 사용하여 브리지 구축

SASE(Secure Access Service Edge)는 네트워킹 및 보안 기능이 클라우드 에지에서 작동하여 보호 및 성능을 제공하는 단일 통합 서비스로 통합되는 미래 지향적인 프레임워크입니다. 이러한 노력을 통해 위치에 관계없이 서비스를 안전하게 통합할 수 있으며, 조직의 규모에 관계없이 네트워크를 제어하고 관리할 수 있습니다. 복잡성 감소 및 민첩한 관리는 구축이 간단하고 확장 가능하며 안전함을 의미합니다.

Umbrella 조직이란?

Umbrella 조직은 단일 라이선스 키와 연결된 다양한 사용자 역할을 가진 사용자 그룹입니다. 단일 사용자가 여러 Umbrella 조직에 액세스할 수 있습니다. 모든 Umbrella 조직은 별도의 Umbrella 인스턴스이며 자체 대시보드가 있습니다. 조직은 이름 및 조직 ID(Org ID)로 식별됩니다. 조직 ID는 가상 어플라이언스와 같은 구성 요소를 구축하기 위해 조직을 식별하는 데 사용되며, 지원 부서에서 조직 ID를 요청할 수도 있습니다.

SIG 터널이란?

SIG(Secure Internet Gateway) 터널은 ASA와 Umbrella 간에 발생하는 SIG IPSec(Internet Protocol Security) 터널의 인스턴스로, 모든 인터넷 바운드 트래픽이 검사 및 필터링을 위해 Umbrella SIG로 전달됩니다. 이 솔루션은 보안에 대한 중앙 집중식 관리를 제공하므로 네트워크 관리자가 각 브랜치에 대한 보안 설정을 별도로 관리할 필요가 없습니다.

터널이 구성된 Umbrella 조직을 온보딩하면 CDO의 사이트 간 VPN 페이지에 이러한 터널이 나열됩니다. CDO UI에서 Umbrella 조직에 대한 SASE 터널을 생성하려면 Umbrella용 SASE 터널 구성을 참조하십시오.

참고 Umbrella 조직 및 해당 피어 디바이스를 온보딩하는 경우 사이트 간 VPN 페이지는 해당 조직과 연결된 터널에 대한 모든 디바이스를 단일 항목으로 결합합니다. Tunnels(터널) 페이지를 수동으로 새로 고침하고 Umbrella 대시보드에서 변경한 내용을 읽으려면 Umbrella 터널 구성 읽기를 참조하십시오.

CDO는 Umbrella와 어떻게 통신합니까?

Umbrella 조직 및 조직과 연결된 모든 ASA 디바이스를 온보딩해야 합니다.

ASA 디바이스가 Umbrella 클라우드와 연결된 경우 디바이스와 클라우드 간에 보안 연결을 생성하려면 사이트 간 VPN SIG 터널이 필요합니다. CDO는 Umbrella 조직 및 ASA 디바이스와 통신합니다. 이 이중 통신 방법을 통해 CDO는 구성 또는 터널 변경 사항의 변경 사항을 즉시 탐지하고 Umbrella, ASA 및 터널에 대한 아웃오브바운드 변경 사항, 오류 또는 비정상 상태를 즉시 사용자에게 알릴 수 있습니다.

Umbrella 조직을 CDO에 온보딩할 때 조직의 API 키 및 암호를 사용하여 온보딩합니다. 둘 다 조직 및 해당 조직과 연결된 ASA 디바이스에 고유합니다. CDO는 조직을 온보딩하여 ASA 디바이스에 대한 정보를 요청하고 전송하는 데 사용되는 API 키 및 암호를 사용하여 Umbrella API를 통해 Umbrella 클라우드와 통신합니다. 이 수준의 통신은 ASA와 Umbrella 클라우드 간에 존재하는 SIG 터널을 손상시키지 않습니다.

Umbrella 조직이 온보딩되면 Devices & Services(디바이스 및 서비스) 페이지에 해당 조직과 연결된 모든 탐지된 ASA 디바이스가 "피어"로 표시되고 디바이스가 CDO에 온보딩되었는지 여부가 표시됩니다. 피어 디바이스가 아직 온보딩되지 않은 경우 Onboard Device(디바이스 온보드)를 클릭하여 해당 페이지에서 직접 온보딩할 수 있습니다. Umbrella 조직과 연결된 ASA 디바이스가 CDO에 온보딩된 경우 Devices & Services(디바이스 및 서비스) 페이지에 관계가 표시되고 VPN Tunnels(VPN 터널) 페이지에 디바이스와 조직 간의 터널이 표시됩니다. 조직과 연결된 ASA 디바이스가 CDO에 온보딩되지 않은 경우 디바이스와 연결된 터널이 VPN Tunnels(VPN 터널)에 표시되며 이 페이지에서 디바이스를 직접 온보딩하도록 선택할 수 있습니다.

CDO에서 Umbrella 클라우드에 액세스하려면 어떻게 해야 합니까?

Umbrella 조직이 CDO에 성공적으로 온보딩되면 조직의 대시보드 또는 CDO UI에서 Umbrella Tunnels(Umbrella 터널) 페이지로 교차 실행할 수 있습니다.

CDO UI에서 Umbrella 클라우드에 액세스하려면 Umbrella 대시보드에 대한 교차 실행, 7 페이지 및 Umbrella 터널 페이지에 대한 교차 실행, 8 페이지을 참조하십시오.

사전 요건

지원되는 하드웨어 및 소프트웨어

Umbrella 조직은 클라우드 기반이므로 버전이 없습니다. Umbrella 조직을 CDO에 온보딩하는 경우 해당 조직을 ASA 디바이스와만 연결할 수 있습니다.

Umbrella 통합의 경우 CDO는 9.1.2 이상을 실행하는 ASA 디바이스를 지원합니다. CDO가 지원하는 ASA 디바이스 모델 및 소프트웨어 목록은 클라우드 디바이스 지원 정보의 내용을 참조하십시오.

라이센싱 요건

Umbrella 조직을 CDO에 성공적으로 온보딩하려면 다음 라이선스 패키지 중 하나를 선택해야 합니다.

- Umbrella SIG Essentials
- SIG Advantage

온보딩

Umbrella 어카운트를 성공적으로 관리하려면 Umbrella 조직 온보딩 및 이와 연결된 ASA 디바이스를 모두 온보딩해야 합니다. Umbrella 조직을 온보딩하면 CDO는 해당 조직과 연결된 기존 ASA 터널을 읽고 이러한 터널의 상태 및 사용자가 생성하여 조직과 연결한 추가 터널을 모니터링합니다. Umbrella 조직을 온보딩하기 전에 일반 디바이스 요구 사항 및 온보딩 사전 요건을 검토합니다.

연결된 ASA 디바이스를 온보딩하기 전에 Umbrella 조직을 온보딩하는 경우 사이트 간 **VPN** 페이지에서 ASA 피어를 보고 VPN 페이지에서 디바이스를 온보딩할 수 있습니다.

참고 페일오버용으로 구성된 ASA 쌍이 있는 경우 두 피어의 액티브 디바이스만 온보드해야 합니다. 액티브 및 스탠바이 디바이스를 CDO에 온보딩하면 Umbrella에 이미 구성된 SASE 터널에 대한 중복 터널 정보가 생성될 수 있습니다.

네트워크 모니터링

CDO는 보안 정책의 영향을 요약한 보고서와 해당 보안 정책에 의해 트리거된 주요 이벤트를 보는 방법을 제공합니다. 또한 CDO는 디바이스에 대한 변경 사항을 기록하고 CDO에서 커밋하는 작업을 도움말 티켓 또는 기타 운영 요청과 연결할 수 있도록 이러한 변경 사항에 레이블을 지정하는 방법을 제공합니다.

변경 로그

변경 로그는 CDO에서 수행되는 구성 변경 사항을 지속적으로 캡처합니다. 이 단일 보기에는 지원되는 모든 디바이스 및 서비스에 대한 변경 사항이 포함됩니다. Umbrella는 클라우드 기반 제품이므로 변경 사항이 즉시 구축됩니다.

다음은 변경 로그의 몇 가지 기능입니다.

- 디바이스 구성에 대한 변경 사항을 나란히 비교합니다.
- 모든 변경 로그 항목에 대한 일반 영어 레이블입니다.

- 디바이스의 온보딩 및 제거를 기록합니다.
- CDO 외부에서 발생하는 정책 변경 충돌 탐지.
- 인시던트 조사 또는 문제 해결 중에 누가, 무엇을, 언제 하는지에 대한 답변을 제공합니다.
- 전체 변경 로그 또는 일부만 CSV 파일로 다운로드할 수 있습니다.

참고 Umbrella 조직과 연결된 SASE 터널을 생성, 편집 또는 삭제하면 Umbrella 조직 및 연결된 모든 ASA 디바이스에 대한 요청 및 구성 변경 사항이 나타납니다.

Umbrella 설명서

- Umbrella 도움말
- Umbrella 및 Cisco ASA 구성
- 터널을 통해 Cisco Umbrella에 연결
- Cisco Umbrella API

Umbrella 조직 온보딩

Umbrella 라이선스 요건

Umbrella 조직을 CDO에 성공적으로 온보딩하려면 Umbrella 대시보드에서 다음 라이선스 패키지 중 하나를 선택해야 합니다.

- Umbrella SIG Essentials
- SIG Advantage

현재 활성화된 라이선스를 확인하려면 Umbrella 대시보드에 로그인하여 **Admin(**관리자**)** > **Licensing(**라이선싱**)**으로 이동합니다.

API 키 및 암호 생성

Umbrella 조직을 CDO에 온보딩하기 전에 새 API 키를 생성하고 **API** 키와 해당 암호를 모두 검색합니다.

현재 API 키가 없는 경우 다음 절차를 사용하여 생성합니다.

시작하기 전에

Umbrella의 관리 API 키는 다음 Umbrella 서비스에 사용됩니다.

- 네트워크 및 도메인
- 네트워크 터널
- 사용자 및 역할
- 대상 목록
- 통신 사업자

이러한 서비스에 대한 CDO 액세스를 허용하지 않으면 Umbrella 조직을 온보딩할 수 없습니다.

단계 **1** Cisco Umbrella 대시보드에 액세스하여 조직에 로그인합니다.

단계 **2** Umbrella 대시보드의 왼쪽 탐색창에서 **Admin(**관리**)**을 클릭하고 **API Keys(API** 키**)**를 선택합니다.

단계 **3** **Create API Key(API** 키 생성**)**를 클릭합니다.

API 키가 이미 있지만 암호를 저장하지 않은 경우 **Admin(**관리자**)** > **API Keys(API** 키**)** 화면으로 이동하여 **Refresh(**새로 고침**)**를 클릭하여 키와 암호를 업데이트합니다.

단계 **4** 새 API 키와 시크릿을 생성하려면 **+** 버튼을 클릭합니다.

단계 **5** 이름을 입력하고 API 키에 다음 범위를 추가합니다.

- 배포.
- 정책.

단계 **6** 키 생성를 클릭합니다.

단계 **7** API 키 및 해당 암호를 복사합니다. 사용할 준비가 될 때까지 참고 또는 .txt 파일에 임시로 붙여넣는 것이 좋습니다.

Umbrella 조직 ID

조직을 CDO에 성공적으로 온보딩하려면 Umrbrella 조직의 조직 ID를 사용하여 조직 ID를 찾은 다음 로그인 자격 증명과 함께 사용해야 합니다.

단계 **1** Cisco Umbrella 대시보드에 액세스하여 조직에 로그인합니다.

단계 **2** 페이지 URL에는 숫자 식별자가 포함됩니다. 예를 들어 https://dashboard.umbrella.com/o/**123456**/#/overview의 조직 ID는 **123456**입니다.

단계 **3** URL에서 조직 ID를 복사합니다. 사용할 준비가 될 때까지 메모에 임시로 붙여넣는 것이 좋습니다.

Umbrella 조직 온보딩

Umbrella 조직을 CDO에 온보딩하려면 다음 절차를 따릅니다.

시작하기 전에

이 환경을 온보딩하기 전에 Umbrella 라이선스 요건, 4 페이지을 읽어보십시오.

단계 1 Umbrella 대시보드에서 Umbrella 조직 ID, 5 페이지 및 API 키 및 암호 생성, 4 페이지을 찾습니다. 이 절차 중에 이러한 항목을 사용할 수 있도록 준비합니다.

단계 2 CDO에 로그인합니다.

단계 3 내비게이션 바에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 4 파란색 더하기 버튼을 클릭하여 디바이스 온보딩을 시작합니다.

단계 5 **Umbrella Organization(Umbrella** 조직**)**을 클릭합니다.

단계 6 Umbrella 대시보드에서 생성한 Umbrella 네트워크 디바이스의 **API** 키와 해당 암호, Umbrella 대시보드 URL의 조직 **ID**를 입력합니다.

단계 7 **Next(**다음**)**를 클릭합니다.

단계 8 (선택 사항) 디바이스의 고유한 레이블을 추가합니다. 나중에 이 레이블을 기준으로 디바이스 목록을 필터링할 수 있습니다.

단계 9 **Go to Inventory(**재고 목록으로 이동**)**를 클릭합니다.

Umbrella 조직을 CDO에 다시 연결

경고! CDO는 저장된 자격 증명이 유효하지 않은 경우 Umbrella 조직에서 구성 변경 사항을 성공적으로 구축하거나 읽을 수 없지만, CDO는 조직과 연결된 ASA 디바이스에서 변경 사항을 성공적으로 구축하거나 읽을 수는 있습니다. 자격 증명이 업데이트되고 검증되면 이로 인해 문제가 발생할 수 있습니다. 구성 변경 사항을 구축하기 전에 조직 자격 증명을 업데이트하는 것이 좋습니다.

Umbrella 조직에 대한 API 키 및 암호가 새로 고쳐졌거나 시간이 초과된 경우 또는 Environment를 온보딩한 후 Cisco+ Secure Connect 선택를 활성화했는데 자격 증명이 더 이상 유효하지 않은 경우, 디바이스를 CDO에 수동으로 다시 연결해야 합니다. 다음 절차를 사용하여 다시 연결합니다.

단계 1 Umbrella 대시보드로 이동합니다. Umbrella 대시보드의 왼쪽 탐색창에서 **Admin(**관리**)**을 클릭하고 Umbrella 관리 **API** 키를 선택합니다.

단계 2 **Refresh(**새로 고침**)**를 클릭합니다. API 키 및 암호 새로 고침을 확인합니다.

단계 3 API 키 및 해당 암호를 복사합니다.

단계 4 CDO에 로그인합니다.

단계 5 **Inventory(**인벤토리**)** 페이지로 이동합니다.

단계 6 필터 또는 검색 창을 사용하여 Umbrella 조직을 찾습니다.

단계 **7** Device Actions(디바이스 작업) 창에서 **Reconnect(**다시 연결**)**를 클릭합니다. CDO는 저장된 API 키 및 암호가 더 이상 유효하지 않음을 확인합니다.

단계 **8** 적절한 팝업 창에 API 키와 암호를 붙여넣습니다.

단계 **9** **Continue(**계속**)**를 클릭합니다.

단계 **10** CDO가 새 키와 암호가 유효함을 확인하면 **Close(**닫기**)**를 클릭합니다.

Umbrella 대시보드에 대한 교차 실행

ASA 디바이스 및 Umbrella 조직이 CDO에 성공적으로 온보딩되면 CDO UI에서 조직의 대시보드로 교차 실행할 수 있습니다.

디바이스의 Umbrella 대시보드를 교차 실행하려면 다음 절차를 수행합니다.

단계 **1** CDO에 로그인합니다.

단계 **2** **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 **3** Umbrella 조직을 찾거나 필터링합니다.

단계 **4** Management(관리) 창에서 **Manage Umbrella Organization(Umbrella** 조직 관리**)**을 클릭합니다. CDO가 브라우저에서 선택한 조직과 연결된 Umbrella 대시보드를 여는 새 탭을 실행했습니다.

CDO에서 디바이스 삭제

CDO에서 디바이스를 삭제하려면 다음 절차를 따르십시오.

단계 **1** CDO에 로그인합니다.

단계 **2** **Inventory(**인벤토리**)** 페이지로 이동합니다.

단계 **3** 삭제할 디바이스를 찾아 디바이스 행에서 디바이스를 확인하고 선택합니다.

단계 **4** 오른쪽에 있는 디바이스 작업 패널에서 **Remove(**제거**)**를 선택합니다.

단계 **5** 메시지가 표시되면 **OK(**확인**)**를 선택하여 선택한 디바이스 제거를 확인합니다. 디바이스를 온보딩 상태로 유지하려면 **Cancel(**취소**)**을 선택합니다.

Umbrella 조직 구성

Umbrella 터널 구성 읽기

Umbrella 조직이 CDO에 온보딩되면 수동으로 CDO가 Umbrella에서 터널 구성을 요청하고 업데이트하도록 강제할 수 있습니다. 여기에는 추가, 삭제 또는 편집된 터널이 포함됩니다.

경고! Umbrella 조직 자격 증명이 유효하지 않은 것으로 간주되거나 조직을 온보딩한 이후에 변경된 터널이 CDO에서 삭제된 경우 CDO는 해당 조직과 연결된 ASA 디바이스에만 터널 구성을 배포할 수 있습니다. 자격 증명을 업데이트하면 CDO가 Umbrella 구성을 읽고 삭제된 터널을 다시 채웁니다. Umbrella 조직에는 터널이 있지만 ASA 디바이스에는 없는 터널로 인해 동기화 문제가 발생하며 ASA 디바이스가 조직에 피어로 표시되지 않을 수 있습니다.

단계 **1** CDO에 로그인합니다.

단계 **2** **Devices & Services(**디바이스 및 서비스**)** 페이지에서 **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **3** **SFCN** 탭을 클릭합니다.

단계 **4** Umbrella 조직을 선택하여 강조 표시합니다.

단계 **5** 작업 창에서 **Read Tunnels(**터널 읽기**)**를 선택합니다.

Umbrella 터널 페이지에 대한 교차 실행

ASA 디바이스 및 Umbrella 조직이 CDO에 성공적으로 온보딩되면 CDO UI에서 터널용 Umbrellas 대시보드로 교차 실행할 수 있습니다.

디바이스의 Umbrella 터널 페이지를 교차 실행하려면 다음 절차를 수행합니다.

단계 **1** CDO에 로그인합니다.

단계 **2** VPN 창으로 이동합니다. **Site-to-Site VPN(**사이트 간 **VPN)**을 선택합니다.

단계 **3** 강조 표시되도록 원하는 터널을 선택합니다.

단계 **4** Actions(작업) 창에서 **Manage Tunnel in Umbrella(Umbrella**에서 터널 관리**)**를 클릭합니다. CDO가 브라우저에서 Tunnels Overview(터널 개요) 페이지를 여는 새 탭을 실행합니다.

Umbrella용 SASE 터널 구성

다음 절차를 사용하여 Umbrella 조직에 대한 SASE 터널을 생성합니다.

시작하기 전에

터널을 생성할 Umbrella 조직 및 ASA 디바이스가 이미 CDO에 온보딩되어 있어야 합니다.

방금 구축한 터널과 연결된 ASA 또는 Umbrella 조직이 비정상 상태인 경우 CDO가 터널을 성공적으로 구축하지 못할 수 있습니다. 문제가 발생하는 경우 Cisco TAC에 문의하십시오.

단계 **1** CDO에 로그인합니다.

단계 **2** **VPN** 창으로 이동합니다. **Site-to-Site VPN(**사이트 간 **VPN)**을 선택합니다.

단계 **3** 파란색 더하기 버튼을 클릭하고 **Create SASE Tunnel(SASE** 터널 생성**)**을 선택합니다.

단계 **4** Umbrella 피어 정보를 입력합니다.

- **Umbrella** 선택 - 원하는 **Umbrella** 조직을 선택합니다.
- **Datacenter(**데이터 센터**)** - 헤드엔드 데이터 센터를 선택합니다. Umbrella 조직과 연결된 ASA와 지리적으로 가까운 데이터 센터를 선택하는 것이 좋습니다.

단계 **5** ASA 피어 정보를 입력합니다.

- **Select ASA Device(ASA** 디바이스 선택**)** - 드롭다운 목록에서 Umbrella 조직과 연결된 ASA 디바이스를 선택한 다음 **Select(**선택**)**를 클릭합니다.
- **Public Facing Interface(**공용 인터페이스**)** - 공개적으로 라우팅할 수 있는 고정 IPv4 주소를 선택합니다. 사용된 주소는 NAT에 사용할 수 없습니다.
- **LAN Address(LAN** 주소**)** - LAN 서브넷을 제어하는 LAN 인터페이스를 선택합니다. LAN에 대해 하나 이상의 인터페이스를 선택해야 합니다.
- **Virtual Tunnel Interface** - Umbrella 조직 및 ASA 피어 디바이스를 선택하면 이 필드가 자동으로 채워집니다. 필요한 경우 새 VTI로 사용할 IP 주소를 수동으로 입력할 수 있습니다.

단계 **6** Umbrella 조직 및 ASA 피어 디바이스를 선택하면 암호가 자동으로 채워집니다. **Confirm Passphrase(**암호 확인**)**도 자동으로 채워집니다. 필요한 경우 이러한 필드를 수동으로 입력할 수 있습니다.

단계 **7** (선택 사항) 팝업 창 하단에 있는 **Deploy changes to ASA(ASA**에 변경 사항 즉시 구축**)** 토글은 기본적으로 활성화되어 있습니다. 활성화하면 SASE 터널 구성이 터널 구성에서 선택한 ASA 피어에 즉시 구축됩니다. 변경 사항을 스테이징하고 나중에 구축하려면 옵션을 수동으로 전환하여 비활성화합니다.

단계 **8** **Deploy(**구축**)**를 클릭합니다. 선택적으로, 이 SASE 터널을 구축하는 동시에 다른 터널을 생성하려면 **Deploy and Create Another(**구축 및 다른 생성**)**를 클릭합니다. 구축이 완료되면 터널이 VPN Tunnels(VPN 터널) 페이지에 표시됩니다. **Deploy and Create Another SASE tunnel(**다른 **SASE** 터널 구축 및 생성**)**을 선택하는 경우 CDO는 Umbrella 조직 선택 사항과 **Deploy changes to ASA immediately(**즉시 **ASA**에 변경 사항 구축**)** 토글 설정을 모두 저장하고 이러한 선택 사항을 다음 터널 구성에 자동으로 적용합니다. 구축하기 전에 이러한 선택 사항을 수동으로 변경할 수 있습니다.

SASE 터널 수정

기존 SASE 터널을 수정하려면 다음 절차를 수행합니다.

단계 **1** CDO에 로그인합니다.

단계 **2** **VPN** 창으로 이동합니다. **Site-to-Site VPN(**사이트 간 **VPN)**을 선택합니다.

단계 **3** 수정할 터널을 선택합니다.

단계 **4** 작업 창에서 **Edit(**편집**)**를 클릭합니다.

단계 **5** SASE 터널의 다음 필드를 편집합니다.

- **Name(**이름**)** - CDO 및 Umbrella 대시보드에 표시되는 SASE 터널의 이름을 변경합니다.
- **Umbrella** 피어의 데이터 센터 - 드롭다운 메뉴에서 새 헤드엔드 데이터 센터를 선택합니다.
- **ASA Peer's Public Facing Interface(ASA** 피어의 공용 인터페이스**)** - 드롭다운 메뉴에서 새 IPv4 주소를 선택합니다.
- **ASA Peer's LAN Interfaces(ASA** 피어의 **LAN** 인터페이스**)** - 드롭다운 메뉴에서 하나 이상의 새 LAN 인터페이스를 선택합니다.
- **ASA VTI(Virtual Tunnel Interface)** 주소 - VTI를 수동으로 편집합니다.
- **Passphrase(**암호**)** - 터널의 암호를 수동으로 수정합니다.
- **Confirm Passphrase(**암호 확인**)** - 암호와 일치하도록 이 항목을 수동으로 수정하고 새 값을 확인합니다.

단계 **6** (선택 사항) 팝업 창 하단에 있는 **Deploy changes to ASA(ASA**에 변경 사항 즉시 구축**)** 토글은 기본적으로 활성화되어 있습니다. 활성화하면 SASE 터널 구성이 터널 구성에서 선택한 ASA 피어에 즉시 구축됩니다. 변경 사항을 스테이징하고 나중에 구축하려면 옵션을 수동으로 전환하여 비활성화합니다. 변경 사항을 스테이징하고 나중에 구축하도록 선택하는 경우 **Inventory(**인벤토리**)** 페이지에서 ASA 피어 상태가 `Deploy Pending(구축 보류 중)`으로 표시됩니다.

단계 **7** **Save Updates(**업데이트 저장**)**를 선택합니다.

Umbrella에서 SASE 터널 삭제

CDO UI를 통해 SASE 터널을 삭제하려면 다음 절차를 수행합니다.

시작하기 전에

SASE 터널을 삭제하려면 연결된 ASA가 CDO에서 동기화된 상태여야 합니다. 디바이스가 비정상인 경우 터널을 삭제할 수 없습니다.

CDO에서 SASE 터널을 삭제하면 ASA 디바이스 및 연결된 Umbrella 조직에서 터널이 제거됩니다.

경고**!** Umbrella 조직 자격 증명이 유효하지 않은 것으로 간주되거나 조직을 온보딩한 이후 변경된 경우 CDO에서 터널을 삭제하면, CDO는 조직과 연결된 ASA 디바이스에만 터널 구성을 배포할 수 있습니다. 자격 증명을 업데이트하면 CDO가 Umbrella 구성을 읽고 삭제된 터널을 다시 채웁니다. Umbrella 조직에는 터널이 있지만 ASA 디바이스에는 없는 터널로 인해 동기화 문제가 발생하며 ASA 디바이스가 조직에 피어로 표시되지 않을 수 있습니다. 조직과 연결된 터널을 삭제하기 전에 Umbrella 자격 증명을 확인하는 것이 좋습니다.

단계 **1** CDO에 로그인합니다.

단계 **2** **VPN** 창으로 이동합니다. **Site-to-Site VPN(**사이트 간 **VPN)**을 선택합니다.

단계 **3** CDO에서 삭제할 터널을 선택합니다.

단계 **4** Actions(작업) 창에서 **Delete(**삭제**)**를 클릭합니다.

단계 **5** 터널 삭제를 확인하고 **OK(**확인**)**를 클릭합니다.