Cisco Defense Orchestrator를 사용한 ASA 관리

Cisco Defense Orchestrator를 사용한 ASA 관리

CDO(Cisco Defense Orchestrator)는 모든 ASA 디바이스에서 간단하고 일관되며 안전한 보안 정책 관리 방법을 제공하는 클라우드 기반의 다중 디바이스 관리자입니다.

이 문서의 목표는 CDO(Cisco Defense Orchestrator)를 처음 사용하는 고객에게 개체 및 정책을 표준화하고, 매니지드 디바이스를 업그레이드하고, VPN 정책을 관리하고, 원격 작업자를 모니터링하는 데 사용할 수 있는 활동의 개요를 제공하는 것입니다. 이 문서에서는 다음 사항을 가정합니다.

- 30일 평가판 계정을 개설했거나 CDO를 구매했으며 Cisco에서 CDO 테넌트를 생성했습니다.
- 슈퍼 관리자 사용자에 대한 새 CDO 테넌트에 대한 초기 로그인을(를) 설정했습니다.
- ASA가 이미 구성되어 있으며 엔터프라이즈에서 사용 중입니다.
- CDO에서 관리하려는 ASA를 인터넷에서 직접 액세스할 수 없는 경우 네트워크에서 SDC(Secure Device Connector)를 구축해야 합니다. SDC는 CDO와 ASA 간의 통신을 관리합니다. 자세한 내용은 CDO의 VM 이미지를 사용하여 보안 디바이스 커넥터 구축 또는 자체 VM에 보안 디바이스 커넥터 구축를 참고하십시오.

디바이스 오케스트레이션 활동의 개요에 따라 이 문서에서는 CDO의 CLI 인터페이스, 변경 로그, 공용 REST API를 소개하고 CDO가 디바이스에서 관리할 수 있는 기타 기능에 대한 요약을 제공합니다.

시작하기

Secure Device Connectors

디바이스 자격 증명을 사용하여 CDO 를 ASA에 연결하는 경우, 네트워크에서 SDC(Secure Device Connector)를 다운로드하고 구축하여 CDO와 ASA 간의 통신을 관리하는 것이 모범 사례입니다. ASA는 모두 디바이스 자격 증명을 사용하여 CDO에 온보딩할 수 있습니다. SDC가 ASA와 CDO 간의 통신을 관리하는 것을 원치 않고 인터넷에서 직접 디바이스에 액세스할 수 있는 경우, 네트워크에 SDC를 설치할 필요가 없습니다. Cloud Connector를 사용하여 ASA를 CDO에 온보딩할 수 있습니다.

Cisco Defense Orchestrator를 사용한 ASA 관리

테넌트에 대해 둘 이상의 SDC를 구축하면 성능 저하 없이 CDO 테넌트를 사용하여 더 많은 디바이스를 관리할 수 있습니다. 단일 SDC에서 관리할 수 있는 디바이스의 수는 해당 디바이스에 구현된 기능 및 해당 구성 파일의 크기에 따라 달라집니다. 그러나 구축을 계획할 때는 1개의 SDC가 약 500개의 디바이스를 지원할 것으로 예상합니다.

SDC를 보려면 다음을 수행합니다.

1. CDO에 로그인합니다.
2. CDO 메뉴에서 **Admin(관리)** > **Secure Connector(보안 커넥터)**를 선택합니다.

디바이스 온보딩

대량으로 또는 한 번에 하나씩 ASA를 CDO에 온보딩할 수 있습니다. CDO에서 지원하는 ASA 소프트웨어 및 하드웨어에 대한 자세한 내용은 ASA 지원 세부 사항의 내용을 참조하십시오.

테넌트에서 추가 **CDO** 사용자 생성

CDO(Cisco Defense Orchestrator)에는 읽기 전용, 편집 전용, 구축 전용, 관리자, 슈퍼 관리자 등 다양한 사용자 역할이 있습니다. 사용자 역할은 각 테넌트의 각 사용자에 대해 구성됩니다. CDO 사용자가 둘 이상의 테넌트에 액세스할 수 있는 경우, 사용자 ID는 동일하지만 테넌트마다 역할이 다를 수 있습니다. 인터페이스 또는 설명서에서 읽기 전용 사용자, Admin 사용자 또는 Super Admin 사용자를 언급하는 경우 특정 테넌트에 대한 사용자의 권한 수준을 의미합니다. 다양한 유형의 사용자에게 부여되는 권한에 대한 자세한 내용은 Cisco Defense Orchestrator의 사용자 역할의 내용을 참조하십시오.

테넌트가 생성될 때 슈퍼 관리자 사용자가 자동으로 할당되었습니다. 슈퍼 관리자는 테넌트에서 다른 사용자를 생성할 수 있습니다. 이러한 새 사용자가 테넌트에 연결하려면 CDO의 사용자 레코드와 동일한 이메일 주소를 사용하는 Cisco Secure Sign-On 계정이 있거나 해당 계정을 생성해야 합니다. CDO에서 사용자 레코드를 생성하려면 사용자 역할에 대한 사용자 레코드 생성의 내용을 참조하십시오.

정책 오케스트레이션

정책 오케스트레이션에는 개체 및 정책 검토가 포함됩니다. ASA 정책으로 작업할 때는 CDO에서 "액세스 그룹"을 "액세스 정책"이라고 합니다. ASA 액세스 정책은 CDO 메뉴 바 Policies(정책) > ASA Access Policies(ASA 액세스 정책)에서 찾을 수 있습니다.

네트워크 개체 문제 해결

시간이 지남에 따라 보안 디바이스에 더 이상 사용되지 않거나, 다른 개체와 중복되거나, 디바이스 간에 값이 일치하지 않는 개체가 있을 수 있습니다. 이러한 개체 문제를 해결 하 여 오케스트레이션 작업을 시작 합니다.

아래의 순서대로 개체 문제를 해결합니다. 초기 단계에서 수행하는 작업을 통해 이후 단계에서 해결해야 하는 문제를 해결할 수 있습니다.

Cisco Defense Orchestrator를 사용한 ASA 관리

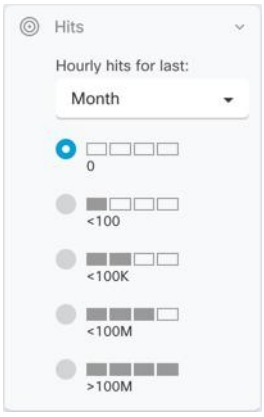
1. 미사 개체 문제 해결 Unused objects(미사용 개체) 는 디바이스에 존재하지만 다른 개체, 액세스 목록 또는 NAT 규칙에서 참조하지 않는 개체입니다.
2. 중복 개체 문제 해결 중복 개체 는 이름은 다르지만 값은 동일한 디바이스에 있는 두 개 이상의 개체입니다. 이러한 개체는 대개 실수로 생성되고 유사한 용도로 사용되며 다른 정책에서 사용됩니다. 중복 개체 문제를 해결한 후 CDO는 유지된 개체 이름으로 영향을 받는 모든 개체 참조를 업데이트합니다.
3. 불일치 개체 문제 해결. 불일치 개체 는 두 개 이상의 디바이스에서 이름은 같지만 값이 다른 개체입니다. 사용자가 동일한 이름 및 콘텐츠를 사용하여 서로 다른 구성에서 개체를 생성하지만 시간이 지남에 따라 이러한 개체의 값이 달라지므로 불일치가 발생하는 경우가 있습니다. 이러한 현상은 보안 문제입니다. 오래된 리소스를 보호하는 규칙이 있을 수 있습니다.

섀도우 규칙 수정

네트워크 개체 문제를 해결했으므로 이제 섀도우 규칙에 대한 네트워크 정책을 검토하고 해결합니다. 섀도우 규칙은 ASA 액세스 정책 페이지에서 반달 모양의 배지 로 표시됩니다. 액세스 정책의 규칙은 목록에서 구성되며 위에서 아래로 한 번에 하나씩 평가됩니다. 네트워크 트래픽이 정책에서 섀도우 규칙 위의 규칙과 일치하므로 정책의 섀도우 규칙은 일치하지 않습니다. 적중되지 않는 섀도우 규칙이 있는 경우 해당 규칙을 제거하거나 정책을 편집하여 규칙을 적용합니다.

정책 적중률 평가

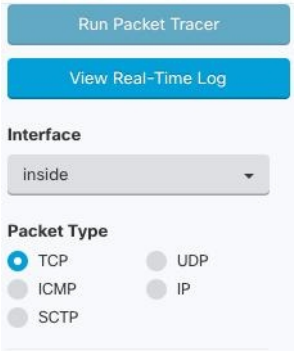
정책의 규칙이 실제로 네트워크 트래픽을 평가하는지 확인합니다. CDO는 1시간마다 정책의 규칙에 대한 적중률 데이터를 수집합니다. CDO에서 디바이스를 오래 관리할수록 특정 규칙의 적중률 데이터가 더 의미가 있습니다. 관심 있는 기간의 적중 횟수를 기준으로 ASA 액세스 정책을 필터링하여 적중 여부를 확인합니다. 그렇지 않은 경우 정책을 다시 작성하거나 삭제하는 것이 좋습니다.



정책 문제 해결

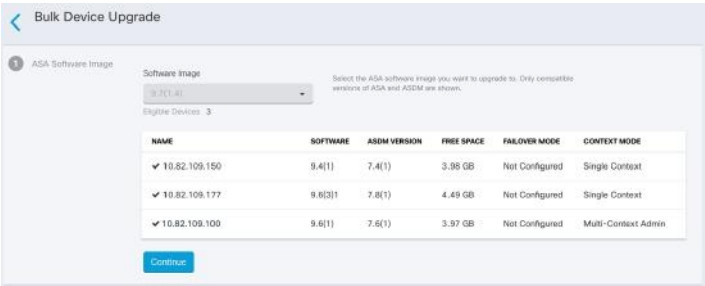
ASA 패킷 트레이서를 사용하여 정책을 통해 가상 패킷의 경로를 테스트하고 규칙이 실수로 액세스를 차단하거나 허용하는지 확인할 수 있습니다.

Cisco Defense Orchestrator를 사용한 ASA 관리



ASA 및 ASDM 업그레이드

그런 다음 최신 버전의 ASA 및 ASDM으로 업그레이드합니다. 고객은 CDO를 사용하여 ASA를 업그레이드할 때 75%~90%의 시간 절약을 보고했습니다.



CDO는 단일 상황 또는 다중 상황 모드에서 개별 ASA 또는 여러 ASA에 설치된 ASA 및 ASDM 이미지를 업그레이드할 수 있는 마법사를 제공합니다. CDO는 ASA 및 ASDM 이미지의 데이터베이스를 유지 관리합니다.

CDO는 백그라운드에서 필요한 업그레이드 호환성 검사를 수행합니다. 마법사는 호환되는 ASA 및 ASDM 이미지를 선택하고 설치하고 디바이스를 재부팅하여 업그레이드를 완료하는 프로세스를 안내합니다. CDO는 CDO에서 선택한 이미지가 ASA에 복사되고 설치된 이미지인지 확인하여 업그레이드 프로세스를 보호합니다.

CDO는 주기적으로 데이터베이스를 검토하고 최신 ASA 및 ASDM 이미지를 추가합니다. CDO는 일반적으로 사용 가능한(GA) 이미지만 지원하며 데이터베이스에 맞춤형 이미지를 추가하지 않습니다. 목록에 특정 GA 이미지가 표시되지 않으면 지원 문의 페이지에서 Cisco TAC에 문의하십시오. 설정된 지원 티켓 SLA를 사용하여 요청을 처리하고 누락된 GA 이미지를 업로드합니다.

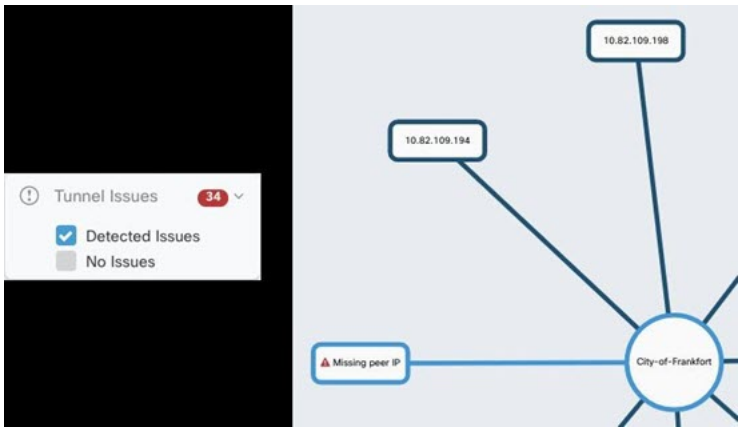
단일 ASA에서 ASA 및 ASDM 이미지 업그레이드을 검토한 다음 자체 저장소의 이미지를 사용하여 여러 ASA 업그레이드에서 ASA 업그레이드에 대해 자세히 알아보십시오.

VPN 연결 모니터링 및 관리

사이트 간 VPN 문제 검토

CDO는 네트워크의 ASA 디바이스에 존재하는 VPN 문제를 보고합니다. VPN 피어 목록을 표시 하는 테이블 또는 허브 및 스포크 토폴로지의 VPN 연결을 표시 하는 맵 등 두 가지 방법으로 환경을 볼 수 있습니다. 필터 사이드바를 사용하여 주의가 필요한 VPN 터널을 검색합니다.

Cisco Defense Orchestrator를 사용한 ASA 관리



CDO를 사용하여 VPN 터널 평가:

- 사이트 투 사이트 VPN 터널 연결 확인
- 누락된 피어가 있는 VPN 터널 찾기
- 암호화 키 문제가 있는 VPN 피어 찾기
- 터널에 대해 정의된 불완전하거나 잘못 구성된 액세스 목록 찾기
- 터널 구성에서 문제 찾기

관리되지 않는 사이트 간 **VPN** 피어 온보딩

CDO는 관리되지 않는 VPN 피어도 식별합니다. 이러한 디바이스를 식별하면 관리되지 않는 디바이스 온보딩에서 디바이스를 온보딩하고 CDO를 통해 관리합니다.

ASA 원격 액세스 **VPN** 지원

CDO를 사용하면 ASA를 통해 연결할 때 사용자가 엔터프라이즈 리소스에 안전하게 액세스할 수 있도록 RA VPN(Remote Access Virtual Private Network) 구성을 생성할 수 있습니다. ASA가 CDO에 온보딩된 경우 CDO는 ASDM 또는 CSM(Cisco Security Manager)을 사용하여 이미 구성된 RA VPN 설정을 인식하므로 CDO로 관리할 수 있습니다.

AnyConnect는 RA VPN 연결을 제공하는 엔드포인트 디바이스에서만 지원되는 클라이언트입니다.

CDO는 ASA 디바이스에서 RA VPN 기능의 다음 측면을 지원합니다.

- SSL 클라이언트 기반 원격 액세스
- IPv4 and IPv6 addressing
- 여러 ASA 디바이스에서 공유 RA VPN 구성

자세한 내용은 ASA에 대한 원격 액세스 VPN 구성을 참조하십시오.

Cisco Defense Orchestrator를 사용한 ASA 관리

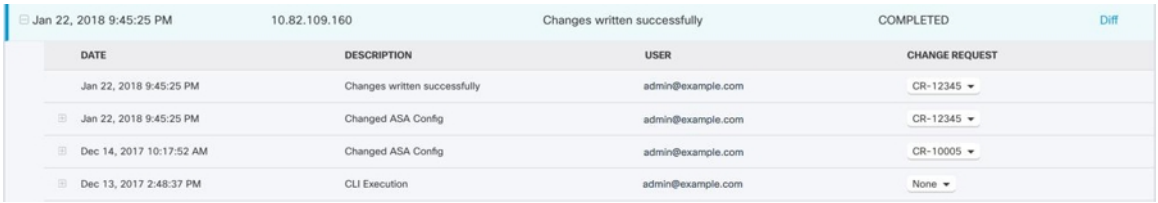
디바이스 구성 동기화 모니터링

CDO는 데이터베이스에 저장한 디바이스 구성을 ASA에 설치된 디바이스 구성과 주기적으로 비교합니다. CDO에 등록한 ASA는 여전히 디바이스의 ASDM(Adaptive Security Device Manager)에서 관리할 수 있으므로 CDO의 구성이 디바이스의 구성과 동일한지 확인하고 차이점을 알려줍니다. Synced(동기화됨), Not Synced(동기화되지 않음) 또는 Conflict Detected(충돌 탐지됨) 디바이스 상태에 대한 자세한 내용은 충돌 탐지의 내용을 참조하십시오.

변경 로그에서 변경 사항 추적

디바이스의 구성에 대한 변경 사항은 변경 로그에 기록됩니다. 변경 로그에는 CDO에서 디바이스로 구축된 변경 사항, 디바이스에서 CDO로 가져온 변경 사항, 해당 변경 사항의 "차이"를 볼 수 있는 기능, 변경된 내용, 발생한 시간, 수행한 사람 등의 정보가 표시됩니다.

회사의 추적 번호를 사용하는 맞춤형 라벨을 생성하여 변경 사항에 적용할 수도 있습니다. 변경 로그에서 해당 맞춤형 라벨, 날짜 범위, 특정 사용자 또는 변경 유형별로 변경 목록을 필터링하여 원하는 항목을 찾을 수 있습니다.



이전 구성 복원

"실행 취소"하려는 ASA를 변경하는 경우 CDO를 사용하여 디바이스를 이전 구성으로 복원할 수 있습니다. 자세한 내용은 Secure Firewall ASA 구성 복원 정보을 참조하십시오.

명령줄 인터페이스 및 명령 매크로를 사용하여 디바이스 관리

CDO는 그래픽 사용자 인터페이스(GUI)와 명령줄 인터페이스(CLI)를 모두 제공하는 웹 기반 관리 제품으로, 디바이스를 한 번에 하나씩 관리하거나 여러 디바이스를 동시에 관리할 수 있습니다.

ASA CLI 사용자는 CLI 툴의 추가 기능을 높이 평가할 것입니다. 다음은 SSH 세션으로 디바이스에 연결하는 대신 CDO의 CLI 툴을 사용하는 몇 가지 이유입니다.

- CDO는 명령에 필요한 사용자 모드를 알고 있습니다. 명령을 실행하기 위해 권한 수준을 높이거나 낮출 필요가 없으며, 명령을 실행하기 위해 특정 명령 컨텍스트를 입력할 필요도 없습니다.
- CDO는 하므로 목록에서 명령을 선택하여 쉽게 다시 실행할 수 있습니다.
- CLI 작업은 변경 로그에 기록되므로 전송된 명령과 수행한 작업을 읽을 수 있습니다.
- 명령을 대량 모드에서 실행할 수 있으며, 이를 통해 여러 디바이스에 개체 또는 정책을 동시에 구축할 수 있습니다.
- CDO는 한 CLI 매크로를 제공합니다.. CLI 매크로는 있는 그대로 실행할 수 있는 즉시 사용 가능한 명령 또는 완료하고 실행할 수 있는 "공란 채우기" CLI 명령입니다. 하나의 디바이스에서 이러한 명령을 실행하거나 동시에 여러 ASA에 명령을 전송할 수 있습니다.

- CLI는 전체 ASA 구성 파일을 제공합니다. 이를 보거나 고급 사용자인 경우 CLI 명령을 실행하여 변경하지 않고 직접 편집하고 변경 사항을 저장할 수 있습니다.

CDO 공용 API

CDO는 공용 API를 게시하고 문서, 예시 및 테스트를 위한 플레이그라운드를 제공했습니다. 공용 API의 목표는 CDO UI에서 일반적으로 수행할 수 있는 많은 작업을 코드에서 간단하고 효과적으로 수행할 수 있는 방법을 제공하는 것입니다.

이 API를 사용하려면 GraphQL을 알아야 합니다. 이는 매우 배우기 쉬우며, 공식 가이드 (https://graphql.org/learn/)를 통해 쉽고 간단하게 읽을 수 있습니다. GraphQL은 유연하고 강력한 유형이며 자동 문서화되기 때문에 선택했습니다.

전체 스키마 설명서를 찾으려면 GraphQL 플레이그라운드로 이동하여 페이지 오른쪽에 있는 docs(문서) 탭을 클릭합니다.

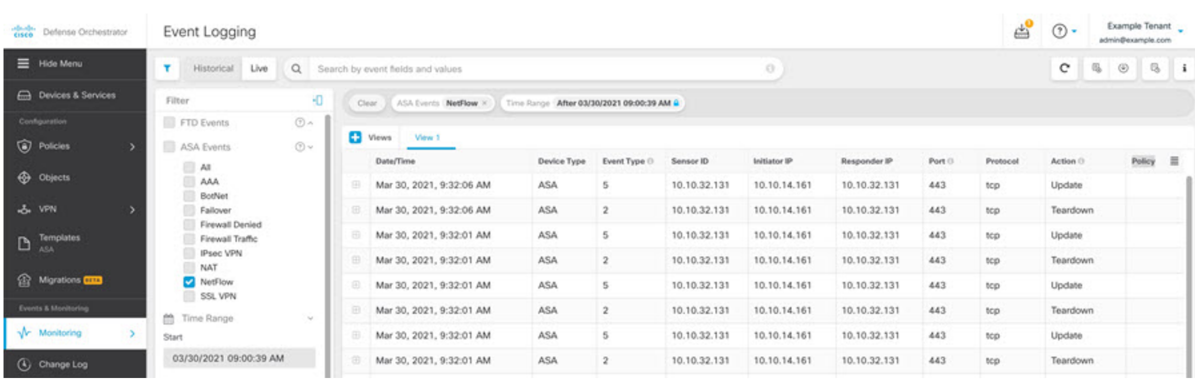
CDO Public API는 이 링크에서 실행하거나 사용자 메뉴에서 **</>CDO API**를 선택하여 실행할 수 있습니다.

CDO와 SecureX 통합

Cisco SecureX 플랫폼은 가시성을 통합하고 자동화를 가능하게 하며 네트워크, 엔드포인트, 클라우드 및 애플리케이션 전반에서 보안을 강화하는 일관된 경험을 위해 Cisco의 광범위한 통합 보안 포트폴리오와 고객의 인프라를 연결합니다. 통합 플랫폼에서 기술을 연결함으로써 SecureX는 측정 가능한 통찰력, 바람직한 결과 및 더할 나위 없는 팀 간 협업을 제공합니다. SecureX 및 CDO 및 CDO을 SecureX에 추가 방법에 대해 자세히 알아볼 수 있습니다.

Cisco Security Analytics and Logging

Cisco Security Analytics and Logging은 추가 라이센싱을 통해 시스템 로그 이벤트 및 Netflow Secure Event Logging(NSEL) 이벤트를 ASA에서 보안 이벤트 커넥터(SEC)로 전송한 다음 Cisco Cloud로 전달할 수 있습니다. 클라우드에 있으면 CDO의 Event Logging(이벤트 로깅) 페이지에서 해당 이벤트를 볼 수 있습니다. 여기서 이벤트를 필터링하고 검토하여 네트워크에서 트리거하는 보안 규칙을 명확하게 이해할 수 있습니다.



이벤트 모니터링 외에도 CDO에서 Secure Cloud Analytics 포털을 실행하여 로깅된 이벤트에 대한 행동 분석을 수행할 수 있습니다.

Cisco Defense Orchestrator를 사용한 ASA 관리

Cisco Security Analytics and Logging을 구현하는 방법에 대한 자세한 설명은 ASA 디바이스에 대한 SaaS(Secure Logging Analytics) 구현의 내용을 참조하십시오.

향후 작업

이제 ASA의 온보딩 및 정책 조정을 시작할 수 있습니다.

도움이 필요한 경우

CDO GUI에서 지원 메뉴를 클릭하여 지원 팀에 문의하거나, 질문하거나, 제품 설명서를 읽을 수 있습니다.