Cisco Defense Orchestrator를 사용한 FDM-관리 디바이스 관리

Cisco Defense Orchestrator를 사용한 FDM-관리 디바이스 관리

중요 Secure Firewall device manager(FDM) 지원 및 기능은 요청 시에만 제공됩니다. 테넌트에서 Firewall Device Manager 지원을 아직 활성화하지 않은 경우 디바이스를 관리하거나 FDM 관리 디바이스에 구축할 수 없습니다. 이 플랫폼을 활성화하려면 지원 팀에 요청을 보냅니다.

Cisco Defense Orchestrator는 간소화된 관리 인터페이스와 Secure Firewall device manager 디바이스에 대한 클라우드 액세스를 제공합니다. FDM 관리 관리자는 디바이스 인터페이스와 CDO 인터페이스 간에 많은 유사성을 확인할 수 있습니다. 관리자 간에 가능한 한 일관성을 유지하기 위해 CDO를 구축했습니다.

CDO를 사용하여 물리적 또는 가상 FDM 관리 디바이스의 다음 측면을 관리합니다.

- FDM 매니지드 디바이스 온보딩
- 디바이스 관리
- 디바이스 업그레이드
- ASA-위협 방어 마이그레이션
- 인터페이스 관리
- 라우팅
- 고가용성
- 보안 정책

Cisco Defense Orchestrator를 사용한 FDM-관리 디바이스 관리

- 정책 및 구성 일관성 승격
- 사이트 간 VPN
- 원격 액세스 VPN
- 네트워크 모니터링
- Cisco Security Analytics and Logging

소프트웨어 및 하드웨어 지원

CDO는 다양한 디바이스 또는 가상 머신에 설치할 수 있는 버전 6.4 이상을 지원합니다. 자세한 내용은 FDM-관리 지원 세부 사항을 참조하십시오.

스마트 라이선스 관리

Cisco Smart License를 사용하여 FDM 관리 디바이스를 CDO에 온보딩하는 동안 또는 디바이스를 온보딩한 후에 라이선싱할 수 있습니다. 스마트 라이선싱은 워크플로우에 편리하게 내장되어 있으며 CDO 인터페이스에서 쉽게 액세스할 수 있습니다. 자세한 내용은 스마트 라이선스 적용 또는 업데이트를 참조하십시오.

참고 온보딩하려는 디바이스가 소프트웨어 버전 6.4 또는 6.5를 실행 중이고, 이미 스마트 라이선스가 있는 경우, 해당 디바이스는 Cisco Smart Software Manager에 등록되어 있을 가능성이 높습니다. 등록 키를 사용하여 **CDO**에 온보딩하기 전에 **Cisco Smart Software Manager**에서 디바이스를 등록 취소해야 합니다**.** 등록을 취소하면 디바이스에 연결된 라이선스 및 선택 가능한 모든 라이선스가 가상 어카운트에서 해제됩니다.

온보딩하려는 디바이스가 소프트웨어 버전 6.6 이상을 실행 중이고, Cisco Cloud에 이미 등록되어 있는 경우, 등록 키를 사용하여 **CDO**에 온보딩하기 전에 **Cisco Cloud Services**에서 디바이스를 등록 취소해야 합니다**.**

CDO 사용자 인터페이스

CDO GUI 및 **CLI** 인터페이스

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.

CLI 인터페이스를 사용하면 CDO에서 직접 FDM 관리 디바이스로 명령을 전송할 수 있습니다. CLI 매크로를 사용하여 일반적으로 사용되는 명령을 저장하고 실행합니다. 자세한 내용은 명령줄 인터페이스 설명서 및 CDO 명령줄 인터페이스의 내용을 참조하십시오.

API 지원

CDO는 기기의 REST API를 사용하여 FDM 관리 디바이스에서 고급 작업을 수행할 수 있는 API 도구 인터페이스를 제공합니다. 또한 이 인터페이스는 다음 기능을 제공합니다.

Cisco Defense Orchestrator를 사용한 FDM-관리 디바이스 관리

- 이미 실행된 API 명령의 기록을 기록합니다.
- 재사용할 수 있는 시스템 정의 API 매크로를 제공합니다.
- 이미 실행한 명령 또는 다른 사용자 정의 매크로에서 표준 API 매크로를 사용하여 사용자 정의 API 매크로를 생성할 수 있습니다.

API 툴에 대한 자세한 내용은 API 툴 사용의 내용을 참조하십시오.

FDM-관리 디바이스 온보딩

FDM 매니지드 디바이스를 온보딩하기 전에 일반 디바이스 요구 사항 및 온보딩 사전 요건을 검토합니다.

등록 토큰을 사용하여 FDM 관리 디바이스를 온보딩하는 것이 가장 좋습니다. 자세한 내용은 등록 키를 사용하여 소프트웨어 버전 6.6 이상을 실행하는 FDM 관리 디바이스 온보딩을 참조하십시오.

다음과 같은 추가 방법을 사용하여 FDM 관리 디바이스를 CDO에 온보딩할 수도 있습니다.

- 사용자 이름, 비밀번호 및 IP 주소를 사용하여 FDM-관리 디바이스 온보딩
- 디바이스의 일련 번호를 사용하여 구성된 FDM 매니지드 디바이스 온보딩
- 로우터치 프로비저닝을 사용하여 FDM-관리 디바이스를 온보딩하기 위한 워크플로우 및 전제 조건

디바이스 관리

CDO를 사용하여 소프트웨어를 업그레이드하고, 고가용성을 구성하고, FDM 관리 디바이스에 대한 디바이스 설정 및 네트워크 리소스를 구성합니다.

- 시스템 설정. FDM 관리 디바이스에 라이선스를 부여하고 온보딩한 후에는 CDO에서 FDM 관리 디바이스 설정을 완전히 관리할 수 있습니다. 관리 액세스 프로토콜, 로깅 설정, DHCP 및 DNS 서버 상호 작용, 디바이스의 호스트 이름, 디바이스가 사용하는 시간 서버, URL 필터링 기본 설정을 구성할 수 있습니다.
- 보안 데이터베이스 업데이트. 필요한 경우 디바이스를 확인하고 업데이트하는 반복 작업을 통해 디바이스를 최신 상태로 유지하고 최신 보안 데이터베이스 업데이트를 준수합니다.
- 고가용성. FDM-관리 고가용성 페이지에서 HA 구성 및 작업을 관리합니다.

디바이스 업그레이드

다음 방법 중 하나를 사용하여 FDM 관리 디바이스에 대한 업그레이드를 즉시 수행하거나 예약합니다.

- 단일 FDM 관리 디바이스 업그레이드.
- 여러 FDM 관리 디바이스 업그레이드.
- FDM 관리 HA 쌍 업그레이드.

Cisco Defense Orchestrator를 사용한 FDM-관리 디바이스 관리

ASA-위협 방어 마이그레이션

CDO는 ASA(Adaptive Security Appliance)를 FDM 관리 디바이스로 마이그레이션하는 데 도움이 됩니다. CDO는 ASA에서 실행 중인 구성의 이러한 요소를 Firewall Device Manager 템플릿으로 마이그레이션하는 데 도움이 되는 마법사를 제공합니다.

이 마이그레이션은 다음 요소에 대해 지원됩니다.

- 액세스 제어 규칙(ACL)
- 인터페이스
- NAT(네트워크 주소 변환) 규칙
- 네트워크 개체 및 네트워크 그룹 개체
- 경로
- 서비스 개체 및 서비스 그룹 개체
- 사이트 간 VPN

자세한 내용은 FDM 템플릿으로 ASA 구성 마이그레이션을 참조하십시오.

인터페이스 관리

CDO를 사용하여 FDM 관리 디바이스에서 데이터 인터페이스 또는 관리/진단 인터페이스를 구성하고 편집할 수 있습니다.

라우팅

라우팅은 소스에서 대상까지 네트워크에 걸친 정보의 이동입니다. 라우팅에는 2가지 기본적인 작업이 포함되는데, 최적의 라우팅 경로를 결정하는 것과 네트워크를 통한 패킷 전송입니다. CDO를 사용하여 라우팅의 다음 측면을 구성합니다.

- 정적 경로 및 기본 경로 구성. CDO를 사용하여 FDM 관리 디바이스에 대한 기본 경로 및 기타 고정 경로를 정의할 수 있습니다.
- 브리지 그룹 지원. 브리지 그룹은 하나 이상의 인터페이스를 그룹화하는 가상 인터페이스입니다. 인터페이스를 그룹화하는 주요 이유는 스위치 인터페이스 그룹을 생성하기 위해서입니다. CDO를 사용하여 디바이스에서 브리지 그룹을 구성하고 편집할 수 있습니다.
- **NAT(Network Address Translation)**. NAT 규칙은 내부(프라이빗) 네트워크에서 인터넷으로 트래픽을 라우팅하는 데 도움이 됩니다. 또한 NAT 규칙은 네트워크 외부에서 내부 IP 주소를 숨겨 보안 역할을 합니다. CDO를 사용하여 디바이스에 대한 NAT 규칙을 생성하고 편집할 수 있습니다. 자세한 내용은 네트워크 주소 변환를 참조하십시오.

보안 정책

보안 정책은 네트워크 트래픽이 의도한 대상에 도달하도록 허용하거나 방지하는 최종 목표를 사용하여 네트워크 트래픽을 검사합니다. CDO를 사용하여 디바이스 보안 정책의 모든 구성 요소를 관리합니다.

Cisco Defense Orchestrator를 사용한 FDM-관리 디바이스 관리

- 규칙을 복사하여 붙여넣습니다. 정책 간에 규칙을 복사하여 붙여넣어 여러 정책에서 쉽게 공유할 수 있습니다. 자세한 내용은 FTM 액세스 제어 규칙 복사를 참조하십시오.
- **SSL** 암호 해독 정책. HTTPS와 같은 일부 프로토콜은 SSL(Secure Sockets Layer) 또는 그 후속 버전인 TLS(Transport Layer Security)를 사용하여 안전한 전송을 위해 트래픽을 암호화합니다. 시스템에서는 암호화된 연결을 검사할 수 없으므로 상위 레이어의 트래픽 특성을 고려하여 액세스 의사 결정을 내리는 액세스 규칙을 적용하려면 SSL 암호 해독 정책을 적용하여 암호를 해독해야 합니다. 자세한 내용은 FDM-관리 디바이스 SSL 암호 해독 정책을 참조하십시오.
- **ID** 정책. 연결에서 사용자 ID 정보를 수집하기 위해 ID 정책을 사용합니다. 그런 다음 대시보드에서 사용자 ID를 기준으로 사용량을 보고 사용자 또는 사용자 그룹을 기준으로 액세스 제어를 구성할 수 있습니다.
- 보안 인텔리전스 정책. 보안 인텔리전스 정책을 사용하면 소스/대상 IP 주소 또는 대상 URL을 기준으로 원치 않는 트래픽을 미리 삭제할 수 있습니다. 시스템은 액세스 제어 정책을 사용하여 차단 목록에 추가된 트래픽을 평가 전에 삭제하며, 이에 따라 사용된 시스템 리소스의 양이 줄어듭니다.
- 액세스 제어 정책. 액세스 제어 정책은 액세스 제어 규칙에 대해 네트워크 트래픽을 평가하여 네트워크 리소스에 대한 액세스를 제어합니다. Secure Firewall Device Manager는 액세스 제어 정책에 나타나는 순서대로 액세스 제어 규칙의 기준을 네트워크 트래픽과 비교합니다. 액세스 제어 규칙의 모든 트래픽 조건이 일치하면 Secure Firewall Device Manager은 규칙에 정의된 작업을 수행합니다. CDO를 사용하여 액세스 제어 정책의 모든 측면을 구성할 수 있습니다.
- TLS 1.3 서버 ID 검색. 버전 6.7에서 도입된 이 기능을 사용하면 TLS 1.3으로 암호화된 트래픽에서 URL 필터링 및 애플리케이션 제어를 수행할 수 있습니다. 자세한 내용은 Firepower Threat Defense의 TLS 서버 ID 검색을 참조하십시오.
- 침입 정책. Cisco는 Firepower System에서 여러 침입 정책을 제공합니다. 이러한 정책은 Cisco Talos Security Intelligence and Research Group에서 설계했습니다. 여기서는 고급 설정과 침입 및 전처리기 규칙 구문 상태를 설정합니다. 침입 정책은 액세스 제어 규칙의 측면입니다. 자세한 내용은 FDM 액세스 제어 규칙의 침입 정책 설정을 참조하십시오.

참고 Snort 3은 버전 6.7 이상을 실행하는 FDM 관리 디바이스에서 사용할 수 있습니다. Snort 2와 Snort 3 간에 전환할 수는 있지만 구성이 호환되지 않을 수 있습니다. Snort 3, 지원되는 디바이스 및 소프트웨어, 제한 사항에 대한 자세한 내용은 Snort 3.0으로 업그레이드의 내용을 참조하십시오.

- 위협 이벤트. 위협 이벤트는 Cisco Talos의 침입 정책 중 하나와 일치한 후 삭제되거나 알림이 생성된 트래픽에 대한 보고서입니다. 대부분의 경우 IPS 규칙을 조정할 필요가 없습니다. 필요한 경우 CDO에서 일치 규칙 작업을 변경하여 이벤트 처리 방식을 오버라이드할 수 있습니다. CDO는 버전 6.4 및 6.6.1의 모든 버전에서 IPS 규칙 조정을 지원합니다. CDO는 버전 6.5, 6.6.1 이외의 6.6 버전 또는 6.7 버전에서 IPS 규칙 조정을 지원하지 않습니다.
- **NAT(Network Address Translation)**. NAT 규칙은 내부(프라이빗) 네트워크에서 인터넷으로 트래픽을 라우팅하는 데 도움이 됩니다. 또한 NAT 규칙은 네트워크 외부에서 내부 IP 주소를 숨겨

Cisco Defense Orchestrator를 사용한 FDM-관리 디바이스 관리

보안 역할을 합니다. CDO를 사용하여 Firepower Threat Defense에 대한 NAT 규칙을 생성하고 편집할 수 있습니다.

정책 및 구성 일관성 승격

개체 관리

개체는 하나 이상의 보안 정책에서 사용할 수 있는 정보의 컨테이너입니다. 개체를 수정하면 해당 개체를 사용하는 다른 모든 정책에 영향을 미치므로 개체를 사용하면 정책 일관성을 쉽게 유지할 수 있습니다. 개체가 없으면 동일한 변경이 필요한 모든 정책을 개별적으로 수정해야 합니다.

CDO를 사용하여 다음 개체 유형을 생성하고 관리합니다.

- Active Directory 영역
- AnyConnect 클라이언트 프로파일
- 애플리케이션 필터
- 인증서
- DNS 그룹
- 지리위치
- Identity Source(ID 소스)
- IKEv1 정책
- IKEv1 IPsec 제안
- IKEv2 정책
- IKEv2 IPsec 제안
- 네트워크
- RA VPN 그룹 정책
- 보안 영역
- 서비스
- 보안 그룹 태그
- Syslog 서버
- URL

개체 문제 해결

CDO에서는 여러 디바이스에서 사용되는 개체를 "공유 개체"라고 부르고 Objects(개체) 페이지에서 이 배지 ⧉로 식별합니다. 때때로 공유 객체는 일부 "문제"를 발생시키고 더 이상 여러 정책 또는 디

Cisco Defense Orchestrator를 사용한 FDM-관리 디바이스 관리

바이스에서 완벽하게 공유되지 않습니다. CDO는 중복 개체 문제 해결, 미사용 개체 문제 해결 및 일관성 없는 개체 문제 해결을 쉽게 하여 디바이스와 개체 저장소를 관리할 수 있습니다.

템플릿

Secure Firewall Device Manager 템플릿은 온보딩된 FDM 관리 디바이스 구성의 전체 복사본입니다. 그런 다음 해당 템플릿을 수정하고 관리하는 다른 FDM 관리 디바이스를 구성하는 데 사용할 수 있습니다. Secure Firewall Device Manager 템플릿은 디바이스 간의 정책 일관성을 촉진합니다. 자세한 내용은 FDM 템플릿을 참조하십시오.

고가용성

CDO를 사용하면 FDM 매니지드 디바이스의 고가용성 쌍을 쉽게 구성하고 관리할 수 있습니다. 기존 HA 쌍을 온보딩하거나 CDO에서 HA 쌍을 생성할 수 있습니다. HA 구성을 사용하면 업그레이드 기간 또는 예기치 않은 디바이스 장애와 같이 디바이스를 사용할 수 없는 시나리오에서 보안 네트워크를 유지할 수 있습니다. 장애 조치 모드에서 스탠바이 디바이스는 이미 액티브 상태가 되도록 구성되어 있습니다. 즉, HA 디바이스 중 하나를 사용할 수 없는 경우에도 다른 디바이스가 트래픽을 계속 처리합니다.

CDO에서 FDM 관리 HA 쌍을 업그레이드할 수 있습니다. 자세한 내용은 FDM-관리 고가용성 쌍 업그레이드를 참조하십시오.

가상 프라이빗 네트워크 구성

사이트 간 **VPN**

VPN(가상 사설망)은 보안되지 않은 네트워크를 통해 개인 데이터를 서로 안전하게 전송하여 네트워크를 네트워크에 연결하는 여러 원격 피어로 구성됩니다. CDO는 터널을 사용하여 IP 기반 네트워크를 통한 전달을 위해 일반 IP 패킷 내에서 데이터 패킷을 캡슐화하고, 암호화를 사용하여 개인 정보를 보호하고 인증을 통해 데이터 무결성을 보장합니다. 자세한 내용은 사이트 간 VPN을 참조하십시오.

가상 사설 네트워크에 대한 자세한 내용은 Firepower Device Manager용 Cisco Firepower Threat Defense 구성 가이드를 참조하십시오.

원격 액세스 **VPN**

RA(Remote Access) VPN을 통해 개인은 지원되는 노트북, 데스크톱 및 모바일 디바이스를 사용하여 네트워크에 대한 보안 연결을 설정할 수 있습니다. CDO는 FDM 관리 디바이스에서 RA VPN을 설정할 수 있는 직관적인 사용자 인터페이스를 제공합니다. AnyConnect는 FDM 관리 디바이스에 대한 RA VPN 연결을 위해 엔드포인트 디바이스에서 지원되는 유일한 클라이언트입니다.

CDO는 FDM 관리 디바이스에서 RA VPN 기능의 다음 측면을 지원합니다.

- 프라이버시, 인증 및 데이터 무결성을 위한 TLS(Transport Layer Security) 또는 DTLS(Datagram Transport Layer Security)
- SSL 클라이언트 기반 원격 액세스
- IPv4 and IPv6 addressing
- 여러 FDM 관리 디바이스에서 공유 RA VPN 구성

Cisco Defense Orchestrator를 사용한 FDM-관리 디바이스 관리

자세한 내용은 RA VPN을 참조하십시오. 가상 사설 네트워크에 대한 자세한 내용은 Firepower Device Manager용 Cisco Firepower Threat Defense 구성 가이드를 참조하십시오.

네트워크 모니터링

CDO는 보안 정책의 영향과 해당 보안 정책에 의해 트리거된 주요 이벤트를 보는 방법을 요약한 보고서를 제공합니다. CDO는 또한 디바이스에 대한 변경 사항을 기록하고 이러한 변경 사항에 레이블을 지정하는 방법을 제공하므로 CDO에서 수행하는 작업을 지원 티켓 또는 기타 운영 요청과 연결할 수 있습니다.

총괄 요약 보고서

개요 보고서는 암호화된 트래픽, 차단된 위협, 탐지된 웹 카테고리 등의 운영 통계 모음을 표시합니다. 네트워크 트래픽이 FDM 관리 디바이스에서 액세스 규칙 또는 정책을 트리거할 때 보고서의 데이터가 생성됩니다. 디바이스가 보고서에 반영되는 이벤트를 생성할 수 있도록 악성코드 및 라이선스를 활성화하고 액세스 규칙에 대한 파일 로깅을 활성화하는 것이 좋습니다.

보고서에서 제공하는 내용과 이를 사용하여 네트워크 인프라를 개선하는 방법에 대한 자세한 내용은 FDM-관리 디바이스 개요 보고서를 참조하십시오. 보고서를 생성하고 관리하려면 보고서 관리를 참조하십시오.

Cisco Security Analytics and Logging

Cisco SaaS(Security Analytics and Logging)를 사용하면 모든 FDM 관리 디바이스에서 연결, 침입, 파일, 맬웨어 및 보안 인텔리전스 이벤트를 캡처하고, CDO의 한 곳에서 볼 수 있습니다.

이벤트는 Cisco Cloud에 저장되며 CDO의 Event Logging(이벤트 로깅) 페이지에서 볼 수 있습니다. 여기에서 이벤트를 필터링하고 검토하여 네트워크에서 어떤 보안 규칙이 트리거되고 있는지 명확하게 이해할 수 있습니다. **Logging and Troubleshooting(**기록 및 문제 해결**)** 패키지는 이러한 기능을 제공합니다.

방화벽 분석 및 모니터링 패키지를 통해 시스템은 FDM 관리 디바이스 이벤트에 Secure Cloud Analytics 동적 엔터티 모델링을 적용하고, 행동 모델링 분석을 사용하여 Secure Cloud Analytics 관찰 및 알림을 생성할 수 있습니다. **Total Network Analytics and Monitoring(**전체 네트워크 분석 및 모니터링**)** 패키지를 보유한 경우, 시스템은 FDM 관리 디바이스 이벤트와 네트워크 트래픽 모두에 동적 엔터티 모델링을 적용하고, 관찰 및 경고를 생성합니다. Cisco SSO(Single Sign-On, 단일 인증)를 사용하여 CDO에서 사용자에게 프로비저닝된 Secure Cloud Analytics 포털로 교차 실행할 수 있습니다. 자세한 내용은 Cisco Security Analytics and Logging(Cisco 보안 분석 및 기록)을 참조하십시오.

변경 로그

변경 로그는 CDO에서 수행되는 구성 변경 사항을 지속적으로 캡처합니다. 이 단일 보기에는 지원되는 모든 디바이스 및 서비스에 대한 변경 사항이 포함됩니다. 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.

Cisco Defense Orchestrator를 사용한 FDM-관리 디바이스 관리

- CDO 외부에서 발생하는 정책 변경 충돌을 탐지합니다.
- 인시던트 조사 또는 문제 해결 중에 누가, 무엇을, 언제 하는지에 대한 답변을 제공합니다.
- 전체 변경 로그 또는 일부만 CSV 파일로 다운로드할 수 있습니다.

변경 요청 관리

변경 요청 관리를 사용하면 서드파티 티켓팅 시스템에서 연 변경 요청 및 해당 비즈니스 근거를 변경 로그의 이벤트와 연결할 수 있습니다. CDO에서 변경 요청을 생성하고, 이를 고유한 이름으로 식별하고, 변경에 대한 설명을 입력하고, 변경 요청을 변경 로그 이벤트와 연결하려면 변경 요청 관리를 사용합니다. 나중에 변경 로그에서 변경 요청 이름을 검색할 수 있습니다.

Cisco Defense Orchestrator를 사용한 FDM-관리 디바이스 관리