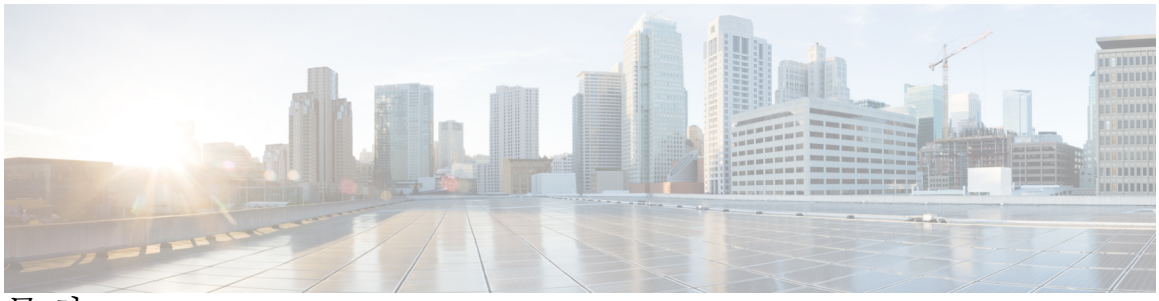
Cisco Defense Orchestrator 관련 새로운 정보

초판: 2021년 4월 16일

최종 변경: 2024년 7월 23일

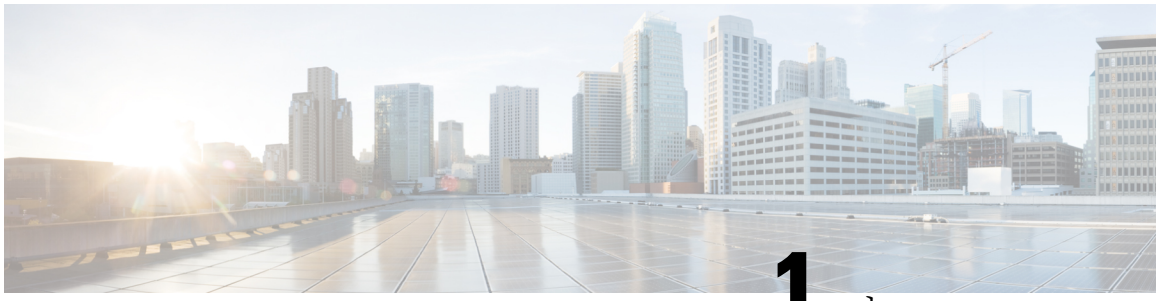
Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



목 차

부

Cisco Defense Orchestrator의 새로운 기능



1 장

2024의 새로운 기능

이 장에서는 2024년에 Cisco Defense Orchestrator에 추가된 몇 가지 기능에 대해 설명합니다.

2024년 6월

2024년 6월 6일

Cisco AI Assistant를 사용한 **Firewall** 관리

CDO 관리자는 이제 CDO(Cisco Defense Orchestrator)의 Cisco AI Assistant와 클라우드에서 제공하는 Firewall Management Center의 통합을 통해 Secure Firewall Threat Defense 정책을 더욱 효율적으로 관리할 수 있습니다. Cisco AI Assistant에는 다음과 같은 몇 가지 주요 기능이 있습니다.

- **Pre-Enabled Assistant(**사전 활성화된 어시스턴트**)**: AI Assistant는 모든 CDO 테넌트에서 기본적으로 활성화됩니다. 필요한 경우 테넌트의 General Settings(일반 설정) 페이지에서 비활성화할 수 있습니다.
- 간편한 액세스: CDO 최고 관리자 및 관리자는 로그인한 후 테넌트 대시보드의 상단 메뉴 모음에서 AI Assistant에 직접 액세스할 수 있습니다.

- **User Orientation(**사용자 방향**)**: AI Assistant 위젯을 처음 열면 사용자가 AI Assistant를 소개하고, 데이터 개인정보 보호에 대해 설명하며, 효과적인 사용을 위한 팁을 제공하는 회전식 창이 반깁니다.

- **Policy Rule Assistance(**정책 규칙 지원**)**: AI Assistant는 Secure Firewall Threat Defense 디바이스의 정책 규칙 생성 프로세스를 간소화합니다. 관리자는 간단한 프롬프트를 사용하여 액세스 제어 규칙을 신속하게 생성할 수 있습니다.
- **Product Knowledge Resource(**제품 지식 리소스**)**: AI Assistant는 CDO 및 클라우드 제공 방화벽 관리 문서를 수집했습니다. 도움이 필요한 경우 질문할 수 있습니다.
- 사용자 친화적 인터페이스:
  - **Simple Text Input Box(**단순 텍스트 입력 상자**)**: 어시스턴트를 쉽게 사용할 수 있도록 창 하단에 있습니다.
  - **Thread History(**스레드 기록**)**: AI Assistant에게 묻는 질문 또는 일련의 질문을 스레드라고 합니다. AI Assistant는 스레드 기록을 유지하므로 이미 한 질문을 참조할 수 있습니다.
  - **Feedback(**피드백**)**: 어시스턴트의 응답에 대해 좋음 또는 반대로 피드백을 제공합니다.

자세한 내용은 Cisco AI Assistant 사용 가이드를 참조하십시오.

2024년 5월

2024년 5월 30일

인도에서 **CDO!**

이제 인도의 https://in.cdo.cisco.com에서 CDO를 사용할 수 있습니다. 인도에서 https://www.getcdo.com으로 이동하여 테넌트를 직접 생성할 수 있습니다.

클라우드 제공 **Firewall Management Center**에 업데이트

Cisco Defense Orchestrator 클라우드 제공 Firewall Management Center의 플랫폼에 대한 업데이트를 릴리스했습니다. 업데이트에 포함된 여러 새로운 기능에 대해 알아보려면 클라우드 제공 Firewall Management Center에 대한 릴리스 노트를 읽어보십시오.

2024년 5월 23일

호주의 **CDO!**

이제 호주의 https://aus.cdo.cisco.com에서 CDO를 사용할 수 있습니다. 호주에서 https://www.getcdo.com으로 이동하여 직접 테넌트를 생성할 수 있습니다.

CDO API

이제 CDO는 CDO와 프로그래밍 방식으로 상호 작용할 수 있는 RESTful API를 제공합니다. API는 디바이스 관리 및 구축, 개체 관리, 검색, 변경 로그 모니터링, 사용자 관리 등 CDO의 광범위한 기능에

대한 액세스를 제공합니다. Cisco Defense Orchestrator API 설명서를 읽고 자세히 알아보십시오. CDO 테넌트의 오른쪽 상단에 있는 사용자 메뉴에서 탐색하여 CDO API 설명서로 이동할 수도 있습니다.

참고 CDO GraphQL API는 더 이상 지원되지 않거나 사용할 수 없습니다.

Firewall 마이그레이션 툴에 대한 업데이트

이제 CDO는 Firewall 마이그레이션 툴의 업데이트된 버전을 호스팅합니다. 이제 Secure Firewall ASA 디바이스에서 Threat Defense 디바이스로 마이그레이션하기 전에 네트워크와 포트 개체를 최적화할 수 있습니다. 또한 DHCP, DDNS 및 SNMPv3 구성을 FDM 관리 디바이스에서 Threat Defense 디바이스로 마이그레이션할 수 있습니다

다른 새로운 기능에 대한 자세한 내용은 Cisco Secure Firewall 마이그레이션 툴 릴리즈 노트를 참조하십시오.

CDO 테넌트 알림 및 사용자 알림 환경 설정 재배치

알림 및 사용자 환경 설정 탭이 이동되었습니다. **Settings(**설정**)** > **Notification Settings(**알림 설정**)** 왼쪽에 있는 탐색 모음에 있는 알림을 사용하여 이메일 구독 및 서드파티 서비스 통합을 관리할 수 있습니다. 사용자 환경 설정은 이제 **Username ID(**사용자 이름 **ID)** > 환경 설정 > 알림 환경 설정에 위치하며, 테넌트와 연결된 디바이스에서 특정 작업이 발생하거나 디바이스 인증서가 만료되거나 만료된 경우, 백그라운드 로그 검색이 시작, 완료 또는 실패할 때마다 트리거되도록 구성할 수 있습니다. **User Notification Preferences(**사용자 알림 환경 설정**)**는 각 개별 사용자에게 고유한 반면 **Tenant Notifications(**테넌트 알림**)**은 테넌트와 관련된 모든 사용자에게 적용됩니다. 자세한 내용은 Tenant Management(테넌트 관리)를 참조하십시오.

인증서 만료 알림

이제 CDO는 Cisco Secure Client(이전의 AnyConnect) 인증서 및 ASA, FDM-관리및 FTD 디바이스의 관리 인증서의 만료 상태를 모니터링합니다. 이러한 인증서가 만료 날짜에 가까워지거나 만료되면 사용자에게 알립니다.

디바이스 인증서 만료 알림을 참조하십시오.

2024년 5월 16일

멀티 클라우드 방어용 **Cisco Security Cloud** 제어 지원

Cisco Security Cloud Control 엔터프라이즈는 이제 기존 멀티 클라우드 방어 어카운트 추가를 지원합니다. Security Cloud 엔터프라이즈 대시보드에 멀티 클라우드 방어 타일을 추가하여 Cisco Security Cloud 포트폴리오 전체에서 다른 시스코 제품 인스턴스, 사용자 ID 및 사용자 액세스 관리의 관리를 모니터링하고 중앙 집중화할 수 있습니다. 자세한 내용은 멀티 클라우드 방어 사용자 가이드에서 Cisco Security Cloud Control에서 Multicloud Defense를 참조하십시오.

2024년 4월

2024년 4월 25일

CDO의 다크 테마

CDO에서는 이제 더욱 맞춤화 가능한 사용자 인터페이스 모양을 위해 다크 테마 옵션을 제공합니다. 오른쪽 상단 모서리에서 관리자 드롭다운을 클릭하고 **Settings(**설정**)** > **General Settings(**일반 설정**)** > **User Settings(**사용자 설정**)**로 이동한 다음 **Theme(**테마**)** 필드에서 **Dark(**다크**)**를 클릭합니다. 기본 테마는 라이트 테마입니다.

자세한 내용은 사용자 설정을 참조하십시오.

2024년 4월 18일

네트워크 개체를 온프레미스 **Secure Firewall Management Center**에 자동으로 동기화

이제 CDO의 네트워크 개체를 CDO에서 관리하는 온프레미스 FMC에 자동으로 지속적으로 동기화할 수 있습니다. 이 기능은 기본적으로 비활성화되어 있습니다. 이 기능을 활성화하려면 **Tools & Services(**툴 및 서비스**)** > **Firewall Management Center**로 이동하여, 온프레미스 FMC를 선택하고, 작업창에서 **Settings(**설정**)**를 선택하고, **Discover and Manage Network Objects(**네트워크 개체 검색 및 관리**)**를 클릭하고, **Enable automatic Sync of network objects(**네트워크 개체 자동 동기화 활성화**)**를 클릭합니다. 네트워크 개체 검색 및 관리 토글이 활성화되어 있는지 확인합니다.

자세한 내용은 온프레미스 Firewall Management Center 네트워크 개체 검색 및 관리를 참조하십시오

2024년 3월

2024년 3월 6일

개선된 **CDO** 테넌트 프로비저닝

이제 더 빠른 개선된 프로비저닝 프로세스를 사용하여 CDO 테넌트를 생성할 수 있습니다. 이미 테넌트가 있더라도 새 CDO 테넌트를 생성할 수도 있습니다. 또한 온프레미스 Firewall Management Center에서 SecureX가 활성화되지 않은 경우 이제 CDO을 통해 Cisco Secure Cloud에 등록할 수 있습니다. CDO 어카운트가 없는 경우 등록 프로세스 중에 어카운트를 생성할 수 있습니다. 자세한 내용은 CDO 테넌트 생성을 참조하십시오.

개별 **Threat Defense** 디바이스가 **Cisco Cloud**로 이벤트 로그를 전송하지 못하도록 비활성화

이제 개별 클라우드 제공 Firewall Management Center 매니지드 Threat Defense 디바이스(버전 7.4.1 이상)가 Cisco Cloud에 이벤트 로그를 전송하지 않도록 설정할 수 있습니다. 이러한 디바이스 수준 제어

를 사용하면 필요한 경우 Threat Defense 디바이스에서 클라우드로 전송된 이벤트 로그를 일시적으로 중지할 수 있습니다. Threat Defense 디바이스가 Cisco 클라우드에 이벤트 로그를 전송하지 못하도록 지정하려면 **Inventory(**인벤토리**)**를 클릭하고 해당하는 Threat Defense 디바이스를 선택한 다음 **Device Management(**디바이스 관리**)** 창에서 **Cloud Events(**클라우드 이벤트**)**를 클릭합니다.

Ubuntu에서 간소화된 보안 디바이스 커넥터 및 보안 이벤트 커넥터 설치

이제 Cisco DevNet 사이트에서 제공되는 GitHub 프로젝트 를 사용하여 Ubuntu 서버에서 보안 디바이스 커넥터 및 보안 이벤트 커넥터를 쉽게 구축할 수 있습니다. 자세한 내용은 이 문서 및 YouTube의 이 비디오를 참조하십시오.

2024년 2월

2024년 2월 13일

클라우드 제공 **Firewall Management Center**에 대한 업데이트

Cisco Defense Orchestrator 클라우드 제공 Firewall Management Center의 플랫폼에 대한 업데이트를 릴리스했습니다. 업데이트에 포함된 여러 새로운 기능에 대해 알아보려면 클라우드 제공 Firewall Management Center에 대한 릴리스 노트를 읽어보십시오.

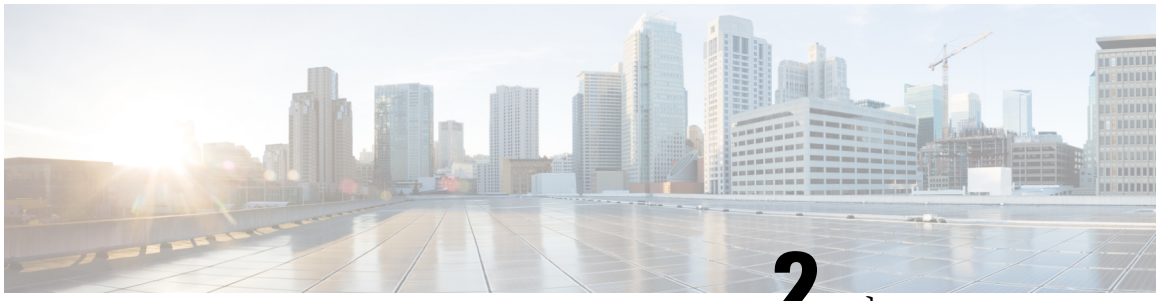
2024년 1월

2024년 1월 25일

Firewall 마이그레이션 툴에 대한 업데이트

이제 CDO는 Firewall 마이그레이션 툴의 업데이트된 버전을 호스팅합니다. 이제 Secure Firewall ASA 디바이스의 WebVPN 구성을 클라우드 제공 Firewall Management Center에서 관리하는 Threat Defense 디바이스의 Zero Trust 액세스 정책 구성으로 마이그레이션할 수 있습니다. 멀티 컨텍스트 ASA 디바이스에서 단일 인스턴스 Threat Defense 디바이스로 마이그레이션할 때, SNMP, DHCP, DVTI 구성을 ASA에서 Threat Defense 디바이스 및 ECMP 라우팅 구성으로 마이그레이션할 수도 있습니다. 릴리스에 포함된 다른 새로운 기능에 대해 알아보려면 Cisco Secure Firewall 마이그레이션 툴 릴리스 노트를 읽어보십시오.

2024년 1월 25일



2 장

2023의 주요 기능

이 장에서는 2023년에 Cisco Defense Orchestrator에 추가된 몇 가지 기능에 대해 설명합니다.

2023년 12월

2023년 12월 14일

Threat Defense 디바이스의 추가 이벤트 유형 모니터링

이제 CDO는 Threat Defense 디바이스에 대한 AAA, BotNet, Failover 및 SSL VPN과 같은 새로운 방화벽 이벤트 유형을 지원합니다.

Analytics(분석) > **Event Logging(이벤트 로깅)**으로 이동하여 **FTD Events(FTD 이벤트)** 아래에서 사용 가능한 새 이벤트 목록에서 필터링합니다. 자세한 내용은 CDO에서 이벤트 유형을 참조하십시오.

2023년 12월 7일

CDO를 사용한 온프레미스 **Firewall Management Center** 네트워크 개체 관리

이제 CDO가 관리하는 온프레미스 Firewall Management Center에서 다른 온프레미스 Firewall Management Center가 관리하는 Threat Defense 디바이스, 클라우드 제공 Firewall Management Center 및 CDO 관리 ASA와 Threat Defense 디바이스에 이르기까지 네트워크 개체를 관리하고 공유할 수 있습니다. 이는 CDO에서 관리하는 플랫폼 전반에서 네트워크 개체 정의를 일관성 있게 유지하는 데 도움이 됩니다.

온프레미스 Firewall Management Center를 온보딩한 후 **Tools & Services(**툴 및 서비스**)** > **Firewall Management Center**로 이동하여, 디바이스를 선택하고 **Settings(**설정**)**를 선택하고 **Discover and Manage Network Objects(**네트워크 개체 검색 및 관리**)** 토글 버튼을 활성화합니다.

자세한 내용은 온프레미스 Firewall Management Center 네트워크 개체 검색 및 관리를 참조하십시오

2023년 11월

2023년 11월 30일

클라우드 제공 **Firewall Management Center**에 **Secure Firewall Threat Defense** 디바이스 백업 예약

클라우드 제공 Firewall Management Center를 사용하여 관리하는 Secure Firewall Threat Defense 디바이스의 예약된 백업을 수행합니다.

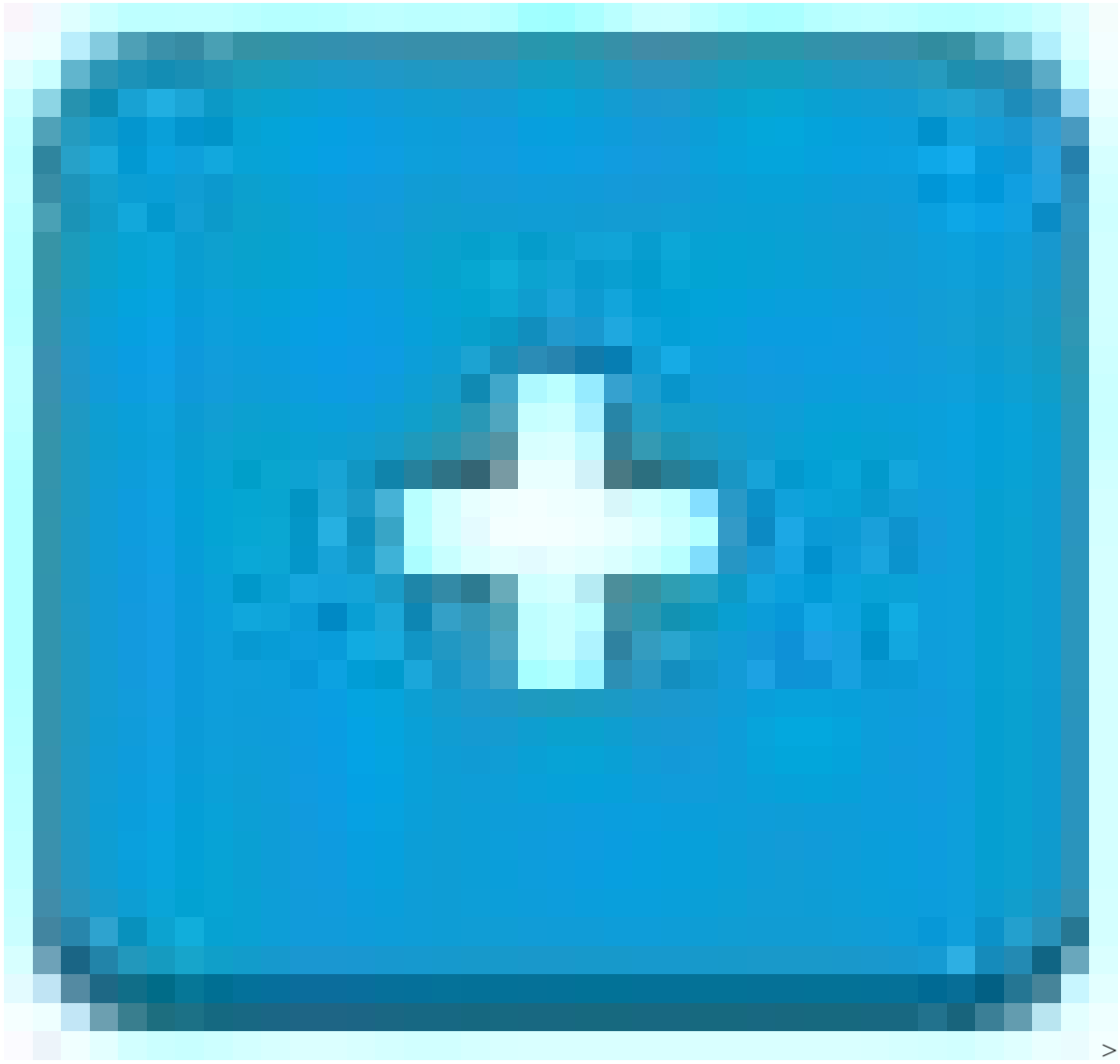
자세한 내용은 원격 디바이스 백업 예약을 참조하십시오.

2021년 11월 14일

클라우드 제공 **Firewall Management Center**에서

CDO는 이제 클라우드 제공 Firewall Management Center에 대해 개선되고 빠른 프로비저닝 프로세스를 제공합니다. 테넌트에서 클라우드 제공 Firewall Management Center를 활성화하면 CDO가 자동으로 프로비저닝되어 CDO 알림 센터와 수신 웹훅을 구성한 애플리케이션을 통해 사용자에게 알려줍

니다. 활성화하려면 **Tools & Services(**툴 및 서비스**)** > **Firewall Management Center** >



> **FMC** > **Enable Cloud-Delivered FMC(**클라우드 제공 **FMC** 활성화**)**를 클릭합니다.

자세한 내용은 CDO 테넌트에서 클라우드 제공 Firewall Management Center 활성화 및 알림 설정을 참조하십시오.

2023년 11월 2일

로우 터치 프로비저닝을 사용하여 **On-Prem Management Center**에 **Threat Defense** 디바이스 온보딩

이제 로우 터치 프로비저닝 방법으로 Threat Defense 디바이스를 온보딩할 때 온프레미스 Firewall Management Center을 관리 플랫폼으로 선택할 수 있습니다. 이는 새 디바이스 또는 이전에 구성되거나 관리되지 않은 디바이스에 대한 온프레미스 관리를 지원합니다. 자세한 내용은 로우 터치 프로비저닝을 사용하여 Secure Firewall Threat Defense 디바이스 온보딩을 참조하십시오.

2023년 10월

2023년 10월 26일

Firewall 마이그레이션 툴에 대한 업데이트

CDO는 Firewall 마이그레이션 툴의 업데이트된 버전을 호스팅합니다. 이를 사용하면 Secure Firewall ASA 디바이스에 있는 여러 투명 방화벽 모드 컨텍스트를 투명 모드 인스턴스로 병합하고 마이그레이션할 수 있습니다.

또한 사이트 간 및 원격 액세스 VPN 구성을 Fortinet 및 Palo Alto Networks 방화벽에서 시스코의 클라우드 제공 Firewall Management Center가 관리하는 Threat Defense 디바이스로 마이그레이션할 수 있습니다. 자세한 정보는 Secure Firewall 마이그레이션 툴 릴리스 노트를 참조하십시오.

2023년 10월 19일

클라우드 제공 **Firewall Management Center**에 업데이트

Cisco Defense Orchestrator 클라우드 제공 Firewall Management Center의 플랫폼에 대한 업데이트를 릴리스했습니다. 업데이트에 포함된 여러 새로운 기능에 대해 알아보려면 클라우드 제공 Firewall Management Center에 대한 릴리스 노트를 읽어보십시오. 새로운 기능의 전체 목록은 클라우드 제공 Firewall Management Center: Cisco Defense Orchestrator의 새 기능에 대한 릴리즈 노트를참조하십시오.

사이트 간 **VPN** 구성을 사용하는 **Secure Firewall Threat Defense** 디바이스를 온프레미스에서 클라우드 제공 **Firewall Management Center**로 마이그레이션

디바이스를 온프레미스 Firewall Management Center에서 클라우드 제공 Firewall Management Center로 마이그레이션할 때, 이제 Secure Firewall Threat Defense 디바이스의 사이트 간 VPN 구성은 나머지 구성과 함께 마이그레이션됩니다. 자세한 내용은 온프레미스 Management Center 매니지드 Secure Firewall Threat Defense를 클라우드 제공 Firewall Management Center로 마이그레이션을 참조하십시오.

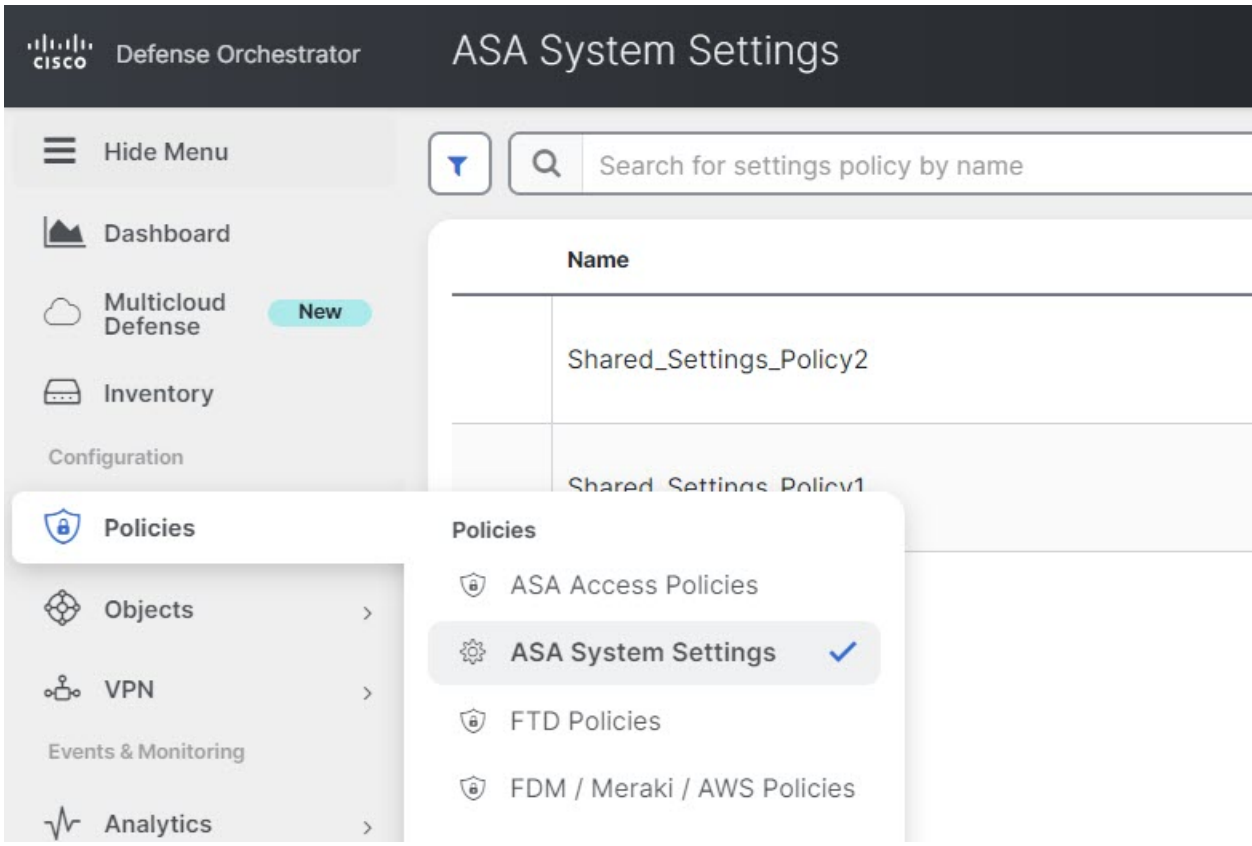
2023년 10월 12일

ASA 시스템 설정 정책

CDO는 도메인 이름 서비스, HTTP와 같은 ASA 디바이스에 대한 필수 구성을 쉽게 관리할 수 있는 시스템 설정 정책을 생성하는 기능을 제공합니다. 그러면 보안 복사 서버를 활성화하고, 메시지를 로깅하고, 액세스 제어 목록을 확인하지 않고 VPN 트래픽을 허용합니다. 이 정책은 여러 ASA 디바이스에 적용할 수 있으며, 정책에 대한 변경 사항은 이 정책을 사용하는 모든 디바이스에 적용됩니다. 또한 단일 ASA 디바이스의 디바이스별 설정을 개별적으로 수정하고 공유 시스템 설정을 디바이스별 값으로 재정의할 수 있습니다.

자세한 내용은 ASA 시스템 설정을 참조하십시오.

Policies(정책**)** -> **ASA System Settings(ASA** 시스템 설정**)**를 선택합니다.



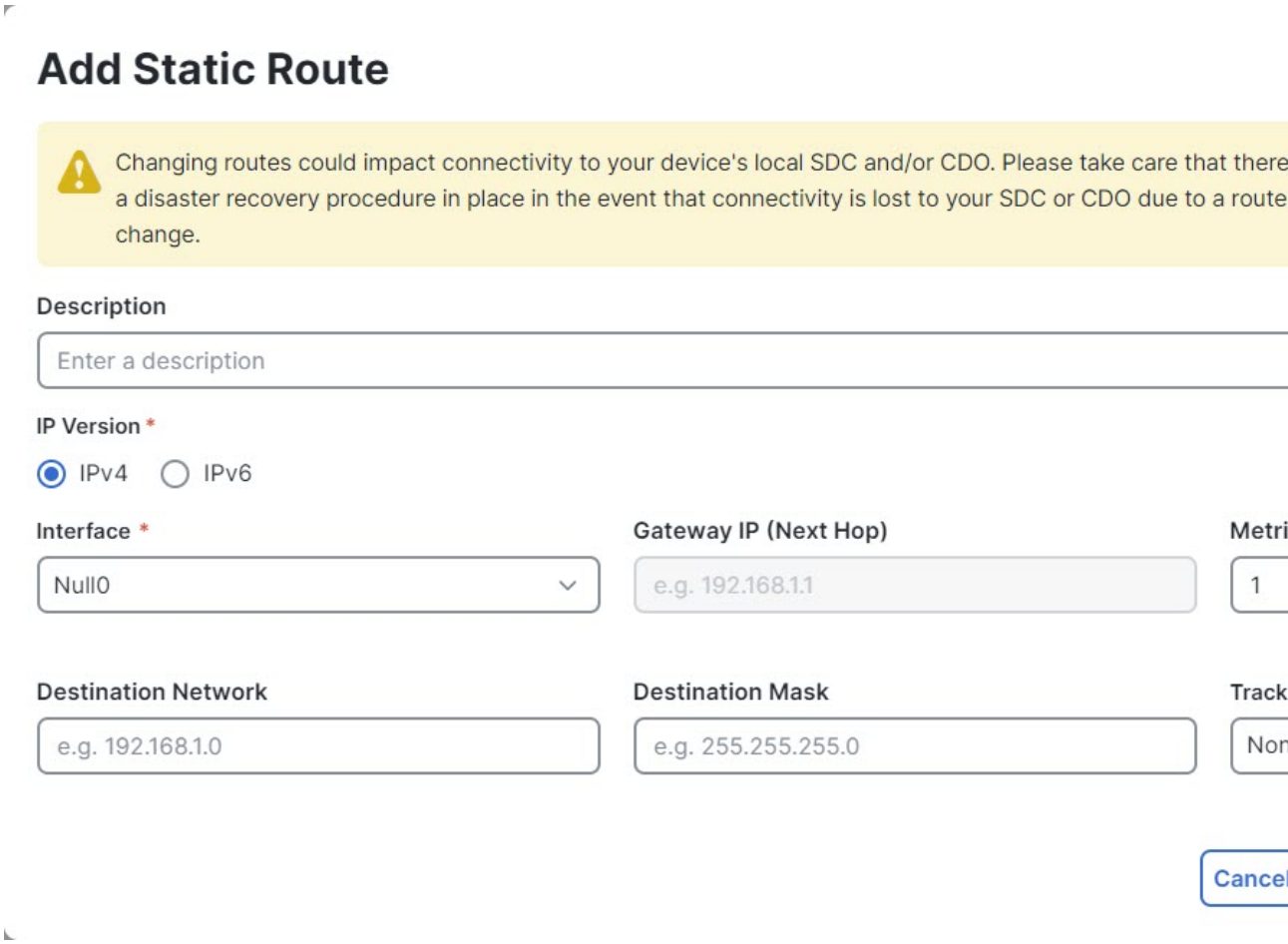
2023년 10월 5일

ASA 고정 라우팅에 대한 **CDO** 지원

이제 CDO 사용자 인터페이스를 사용하여 ASA에 대한 정적 경로를 구성할 수 있습니다. 이 기능을 사용하면 CLI를 사용할 필요 없이 특정 IPv4 또는 IPv6 대상 네트워크에 대해 트래픽을 전송할 위치를 지정할 수 있습니다.

자세한 내용은 ASA 정적 라우팅을 참조하십시오.

Inventory(인벤토리**)** > **ASA** 탭 > **Routing(**라우팅**)**을 클릭합니다.



Terraform을 사용하여 **CDO** 관리

이제 IaC(Infrastructure as Code, 코드로서의 인프라) 원칙을 사용하여 CDO 인프라의 관리를 자동화하는 데 Terraform을 사용할 수 있습니다. 이제 CDO는 보안 디바이스 커넥터 및 보안 이벤트 커넥터를 신속하게 구축할 수 있도록 Terraform 제공자 및 Terraform 모듈을 제공합니다. 자세한 내용은 Terraform을 참조하십시오.

2023년 9월

2023년 9월 14일

보안 이벤트 커넥터에 대한 탐색 변경

오른쪽 상단의 관리 메뉴를 확장하여 Secure Connector(보안 커넥터) 페이지에 더 이상 액세스할 수 없습니다. 보안 커넥터를 관리하려면 **Tools & Services(**툴 및 서비스**)** > **Secure Connectors(**보안 커넥터**)**로 이동합니다. 자세한 내용은 보안 이벤트 커넥터를 참조하십시오.

2023년 9월 7일

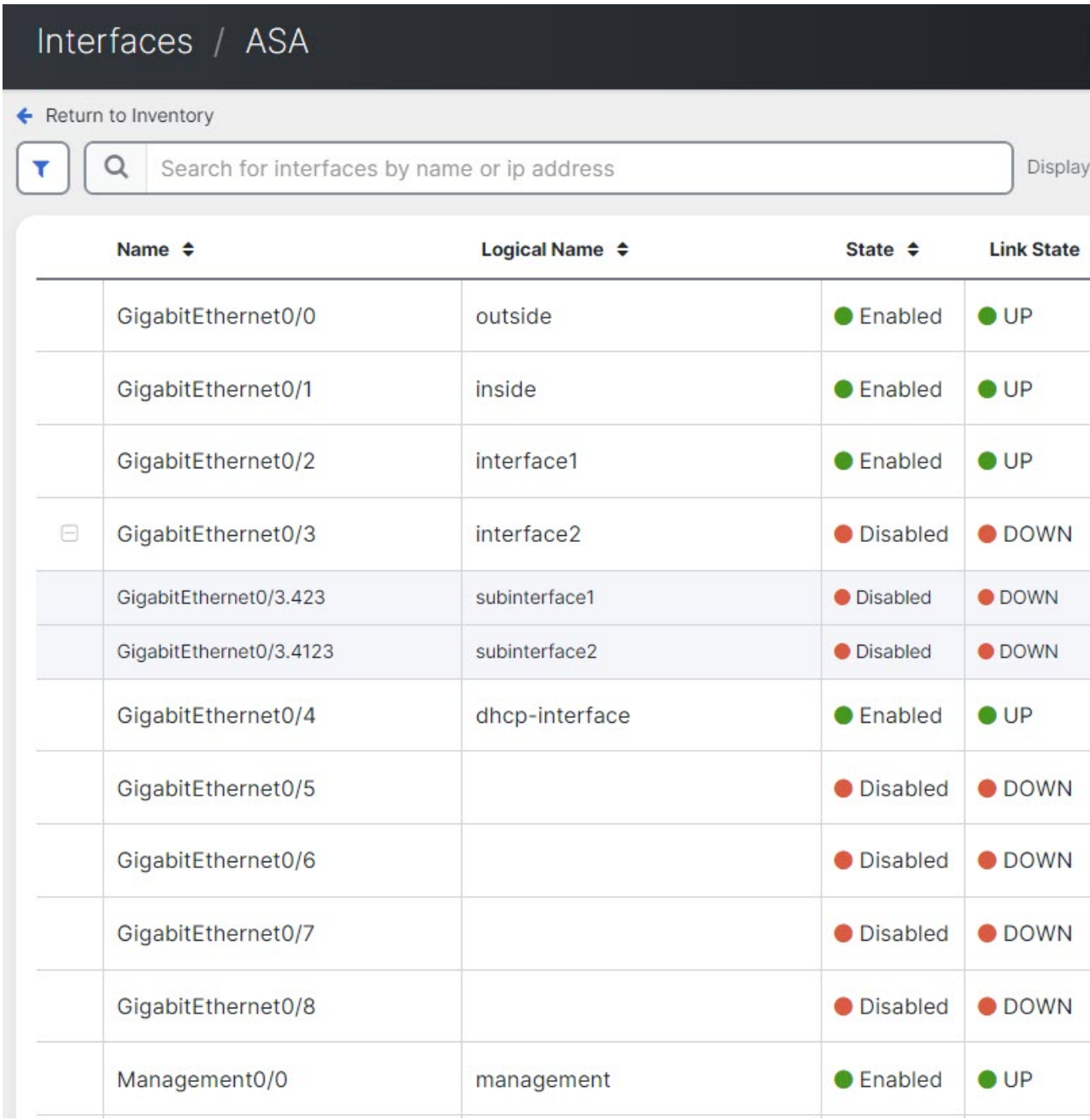
CDO 사용자 인터페이스를 사용하여 **ASA** 인터페이스 설정

이제 CDO에서 그래픽 사용자 인터페이스를 사용하여 ASA의 물리적 네트워크 인터페이스, 논리적 하위 인터페이스, VLAN, EtherChannel을 구성할 수 있습니다. 또한 경로 기반 사이트 간 VPN 중에 생성된 가상 터널 인터페이스도 볼 수 있습니다.

참고 VLAN은 디바이스 110개에 대해서만 지원됩니다.

자세한 내용은 ASA 인터페이스 구성을 참조하십시오.

Inventory(인벤토리**)**> **ASA** 설정 > **Management(**관리**)** > **Interfaces(**인터페이스**)**로 이동합니다.

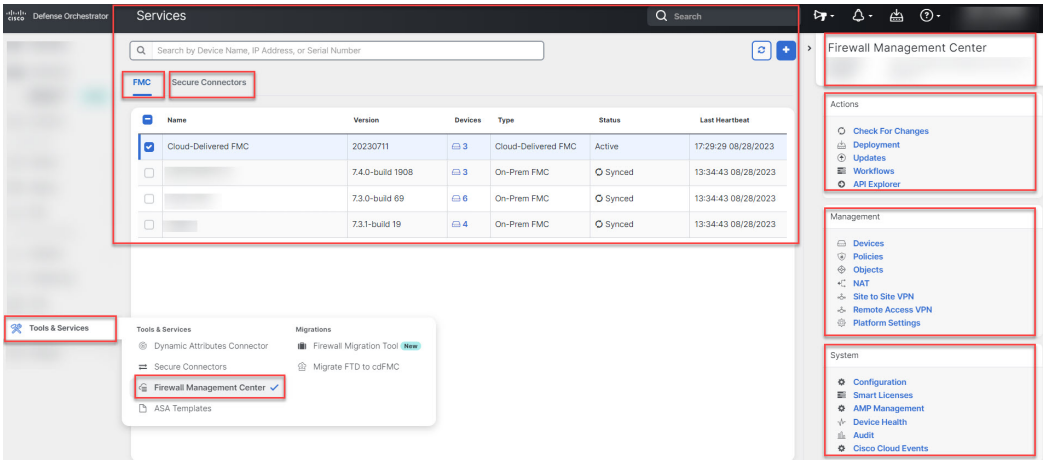

Interfaces / ASA
Return to Inventory
Search for interfaces by name or ip address
Display
Name
Logical Name
State
Link State
GigabitEthernet0/0
outside
Enabled
UP
GigabitEthernet0/1
inside
Enabled
UP
GigabitEthernet0/2
interface1
Enabled
UP
GigabitEthernet0/3
interface2
Disabled
DOWN
GigabitEthernet0/3.423
subinterface1
Disabled
DOWN
GigabitEthernet0/3.4123
subinterface2
Disabled
DOWN
GigabitEthernet0/4
dhcp-interface
Enabled
UP
GigabitEthernet0/5
Disabled
DOWN
GigabitEthernet0/6
Disabled
DOWN
GigabitEthernet0/7
Disabled
DOWN
GigabitEthernet0/8
Disabled
DOWN
Management0/0
management
Enabled
UP

2023년 8월

2023년 8월 31일

서비스 페이지에서 클라우드 제공 **FMC,** 온프레미스 **FMC** 및 보안 커넥터 관리

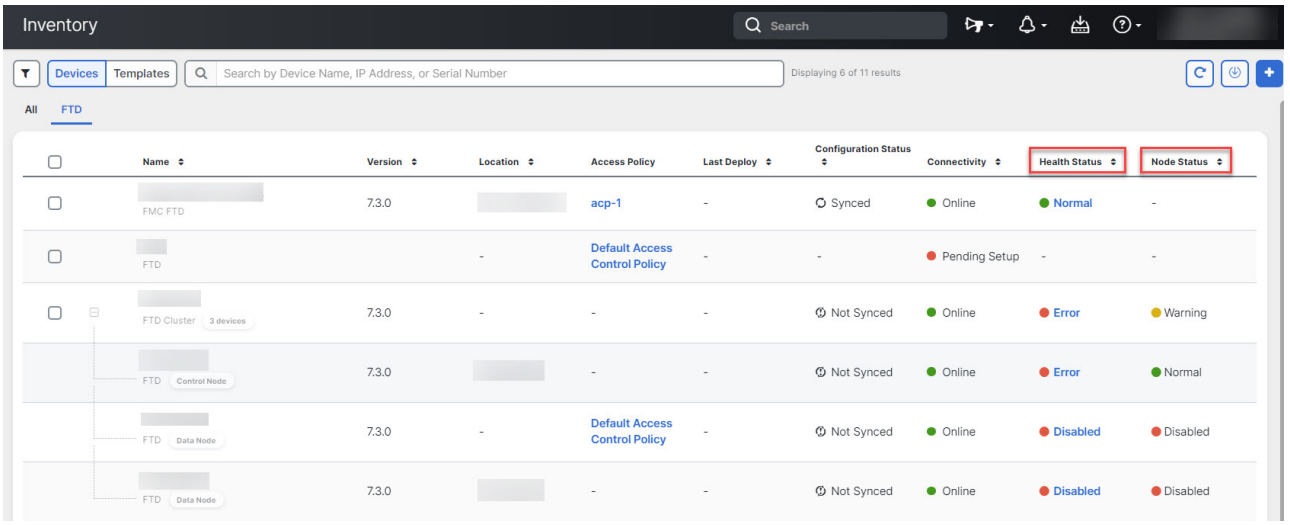
이제 클라우드 제공 Firewall Management Center, 온프레미스 Firewall Management Center 및 보안 커넥터를 새 서비스 페이지에서 관리할 수 있습니다. **Tools & Services(**툴 및 서비스**)** > **Firewall Management Center** 또는 **Secure Connectors(**보안 커넥터**)**를 선택합니다. 자세한 내용은 서비스 페이지 정보 보기를 참조하십시오.



2023년 8월 17일

Threat Defense 디바이스의 상태 파악

이제 CDO는 Inventory(인벤토리) 페이지에 Threat Defense 디바이스의 상태 및 노드 상태를 표시합니다. 디바이스 상태에 대한 자세한 내용을 확인하려면 디바이스의 상태를 클릭하여 클라우드 제공 Firewall Management Center 또는 온프레미스 Firewall Management Center 사용자 인터페이스의 디바이스 상태 모니터링 페이지로 이동합니다. 노드 상태는 클라우드에서 제공하는 Firewall Management Center에서 관리하는 Threat Defense 디바이스에 대해서만 표시됩니다.



자세한 내용은 Cisco Defense Orchestrator에서 온프레미스 FMC 관리 및 클라우드 제공 Firewall Management Center에서 Cisco Secure Firewall Threat Defense Devices 관리를 참조하십시오.

2023년 8월 3일

Firewall 마이그레이션 툴에 대한 업데이트

Cisco Defense Orchestrator는 이제 최신 버전의 Firewall 마이그레이션 툴을 호스팅합니다. 이제 Secure Firewall ASA 디바이스의 여러 컨텍스트를 라우팅 모드 인스턴스로 병합하고 클라우드 제공 Firewall Management Center에서 관리하는 Threat Defense 디바이스로 마이그레이션할 수 있습니다. 또한 마이그레이션 툴은 이제 VRF(virtual routing and forwarding, 가상 라우팅 및 포워딩) 기능을 활용하여 새로 병합된 구성의 일부가 될 멀티 컨텍스트 ASA 환경에서 관찰된 분리된 트래픽 흐름을 복제합니다.

자세한 내용은 *Cisco Defense Orchestrator* 가이드의 *Firewall* 마이그레이션 툴을 사용하여 *Firewall* 마이그레이션에서 CDO가 관리하는 Secure Firewall ASA 마이그레이션을 참조하십시오.

2023년 7월

2023년 7월 20일

GCP에서 관리하는 가상 **Threat Defense** 디바이스에 대한 **EasyDeploy**

이제 가상 Threat Defense 디바이스를 생성하는 동시에 GCP(Google Cloud Platform) 프로젝트에 구축할 수 있습니다. EasyDeploy 방법은 새 가상 디바이스를 생성한 다음 디바이스를 클라우드 환경과 연결하는 데 필요한 단계를 결합하여 절차를 간소화하고 설정에 필요한 시간을 최소화합니다.

이러한 온보딩 플로우에 대해 클라우드 제공 Firewall Management Center가 활성화되어 있어야 합니다. 자세한 내용 은 Google Cloud Platform에 Threat Defense 디바이스 구축 을 참조하십시오.

2023년 7월 13일

다른 브라우저 탭에서 **CDO** 및 클라우드 제공 **Firewall Management Center** 포털 열기

이제 다른 브라우저 탭에서 CDO 및 클라우드 제공 Firewall Management Center 포털 페이지를 열고 CDO 및 클라우드 제공 Firewall Management Center에서 동시에 작업할 수 있습니다.

자세한 내용은 서로 다른 탭에서 CDO 및 클라우드 제공 Firewall Management Center 애플리케이션을 열 수 있도록 지원을 참조하십시오.

2023년 6월

2023년 6월 29일

이벤트 뷰어에서 백그라운드 검색 예약

이제 이벤트 뷰어에서 반복적으로 검색되는 일정에 따라 백그라운드 검색을 실행할 수 있습니다. 일정은 절대 시간(예: 5월 1일~5월 5일) 또는 슬라이딩 기간(예: "마지막 날")을 지원합니다.

자세한 내용은 이벤트 뷰어에서 백그라운드 검색 예약을 참조하십시오.

새 이벤트 속성 지원

이제, 보안 그룹, 암호화된 가시성 프로세스 신뢰도 점수, 암호화된 가시성 위협 신뢰도, 암호화된 가시성 위협 신뢰도 점수, 암호화된 가시성 핑거프린트는 CDO의 이벤트 뷰어에서 지원되는 시스템 로그 이벤트 속성입니다. 이벤트 로깅 보기를 맞춤화 할 때 새로 지원되는 특성에 대한 열을 생성할 수 있습니다.

2023년 6월 15일

CDO에서 **Firewall** 마이그레이션 툴을 사용하여 **Firewall** 마이그레이션

이제 Cisco Defense Orchestrator의 Firewall 마이그레이션 툴을 사용하여 Secure Firewall ASA 디바이스, FDM 관리 Threat Defense 디바이스 및 서드파티 방화벽(예: Check Point, Palo Alto Networks, Fortinet 방화벽)에서 구성을 클라우드 제공 Firewall Management Center로 마이그레이션할 수 있습니다. 자세한 내용은 Cisco Defense Orchestrator에서 Firewall 마이그레이션 툴로 Firewall 마이그레이션 가이드를 참조하십시오.

2023년 6월 8일

AWS 및 **Azure**에서 관리하는 가상 **Threat Defense** 디바이스용 **EasyDeploy**

이제 가상 Threat Defense 디바이스를 생성하는 것과 동시에 AWS(Amazon Web Services) 또는 Azure 환경에 구축할 수 있습니다. EasyDeploy 방법은 새 가상 디바이스를 생성한 다음 디바이스를 클라우

드 환경과 연결하는 데 필요한 단계를 결합하여 절차를 간소화하고 설정에 필요한 시간을 최소화합니다.

이러한 온보딩 플로우에 대해 클라우드 제공 Firewall Management Center가 활성화되어 있어야 합니다. 자세한 내용은 AWS를 사용하여 Threat Defense 디바이스 구축 및 Azure VNet을 사용하여 Threat Defense 디바이스 구축을 각각 참조하십시오.

2023년 6월 5일

CDO에 멀티 클라우드 방어 솔루션을 도입합니다.

멀티 클라우드 방어 솔루션는 보안 정책 오케스트레이션과 클라우드 네트워크 트래픽, 클라우드 애플리케이션 및 워크로드 보호를 전문으로 합니다. 여러 클라우드 유형에 통합 보안 정책 및 웹 보호를 제공하고, 클라우드 자산에 대한 네트워크 가시성을 제공하며, 위협 인텔리전스 및 외부 로깅과 같은 서비스를 통합합니다. 이는 클라우드 어카운트로의 인그레스 트래픽 및 클라우드 어카운트에서의 이그레스 트래픽과 클라우드 어카운트 내의 "이스트-웨스트" 네트워크 트래픽을 적용합니다.

멀티 클라우드 방어 솔루션에서는 현재 AWS, Azure, Google Cloud Platform 및 Oracle OCI 클라우드 어카운트를 지원합니다.

자세한 정보는 Multicloud Defense 정보를 참조하십시오. Multicloud Defense 90일 무료 평가판으로 Multicloud Defense 솔루션을 사용해보십시오.

2023년 6월 1일

SecureX통합을 사용한 온프레미스 **Secure Firewall Management Center** 자동 검색

이제 CDO에는 CDO 어카운트에 연결된 SecureX 테넌트와 연결된 모든 온프레미스 Management Center를 온보딩할 수 있습니다. 또한 해당 온프레미스 Management Center에 연결된 Secure Firewall Threat Defense 디바이스를 온보딩합니다. 자세한 내용은 SecureX를 사용한 온프레미스 Firewall Management Center 자동 온보딩을 참조하십시오.

2023년 4월

2023년 4월 27일

이벤트 필터링 개선

이제 상대 시간 범위를 사용하여 이벤트를 추가로 필터링할 수 있습니다. 절대 시간 범위는 명시적으로 명시된 시간 프레임입니다. 상대 시간 범위의 예로는 지난 3일 또는 지난 3시간등이 있습니다. 이렇게 하면 절대 시간 범위에 반드시 포함되지 않을 수도 있는 트래픽 및 이벤트를 대상으로 지정할 수 있습니다. 자세한 내용은 이벤트 로깅 페이지에서 이벤트 검색을 참조하십시오.

2023년 3월

2023년 3월 23일

이벤트 로깅에 대한 백그라운드 검색

CDO는 검색 기준을 정의하고 정의된 검색 기준에 따라 이벤트 로그에서 이벤트를 검색하는 기능을 제공합니다. 백그라운드 검색 기능을 사용하여 백그라운드에서 이벤트 로그 검색을 수행하고 백그라운드 검색이 완료되면 검색 결과를 볼 수 있습니다.

구성한 구독 알림 및 서비스 통합을 기반으로 백그라운드 검색이 완료되면 알림을 받을 수 있습니다. 이벤트 로깅에 사용되는 백그라운드 검색에 대해 자세히 알아보십시오.

2023년 1월

2023년 1월 18일

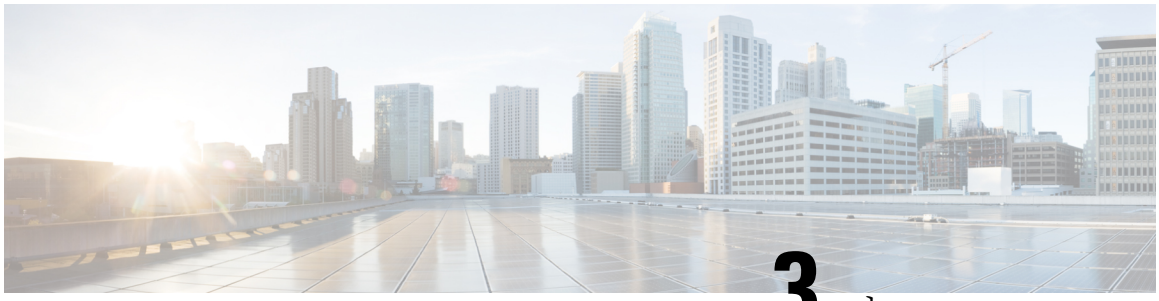
원격 액세스 **VPN** 세션 모니터링

CDO는 이제 CDO에서 클라우드 제공 Firewall Management Center를 사용하여 관리되는 FTD의 원격 액세스 VPN 세션을 모니터링할 수 있습니다.

원격 액세스 가상 프라이빗 모니터링 페이지는 다음 정보를 제공합니다.

- 활성 및 기록 세션 목록.
- 각 세션과 연결된 디바이스 및 사용자의 세부 정보.

2023년 1월 18일



3 장

2022의 주요 기능

이 장에서는 2022년에 Cisco Defense Orchestrator에 추가된 몇 가지 기능에 대해 설명합니다.

2022년 12월

2022년 12월 15일

Cisco Defense Orchestrator 클라우드 제공 Firewall Management Center의 플랫폼에 대한 업데이트를 릴리스했습니다. 업데이트에 포함된 새로운 기능에 대해 알아보려면 클라우드 제공 Firewall Management Center에 대한 릴리스 노트를 읽어보십시오.

2022년 12월 1일

ASA에 대한 경로 기반 사이트 간 **VPN** 지원

이제 Cisco Defense Orchestrator를 사용하여 가상 터널 인터페이스가 구성된 피어 사이에 사이트 간 VPN 터널을 생성할 수 있습니다. 이것은 각 터널 끝에 IPsec 프로파일이 연결된 라우팅 기반 VPN을 지원합니다. IPSec 터널로 라우팅되는 모든 트래픽은 소스/대상 서브넷에 관계없이 암호화됩니다.

VTI 기반 VPN은 다음 간에 생성할 수 있습니다.

- CDO 관리 ASA 및 모든 경로 기반 VPN 지원 디바이스.
- CDO 관리 ASA 2개.

자세한 정보는 사이트 간 가상 프라이빗 네트워크를 참조하십시오.

글로벌 검색

CDO에서 전역 검색 기능을 사용하면 CDO에서 관리하는 장치를 찾아 이동할 수 있습니다. 이제 이 기능은 CDO 사용자 인터페이스의 클라우드 제공 Firewall Management Center에서 관리되는 디바이스에 대한 검색 기능을 지원합니다. 검색 결과에서 클라우드 제공 Firewall Management Center의 해당 페이지로 이동할 수 있습니다.

자세한 내용은 전역 검색을 참조하십시오.

2022년 10월

2022년 10월 27일

Duo Admin Panel 온보딩 및 다단계 인증 로깅

이제 CDO는 Duo Admin Panel을 온보딩하고 대시보드 및 표 형식에 로그를 MFA 이벤트로 표시할 수 있습니다. 하나 이상의 디바이스의 MFA 세션을 쉼표로 구분된 값을 포함하는 파일(.csv)로 내보낼 수 있습니다.

Duo Admin Panel에서는 사용자의 이중 인증 성공 또는 실패 여부에 대한 정보가 포함된 MFA(Multi-Factor Authentication, 다단계 인증) 로그를 기록합니다.

자세한 내용은 Cisco Defense Orchestrator 가이드의 "Duo Admin Panel 온보딩" 및 "다단계 인증 이벤트 모니터링"을 참조하십시오.

2023년 10월 12일

ASA용 정책 기반 사이트 간 **VPN** 마법사

이제 CDO에서는 두 피어 사이에 정책 기반 사이트 간 VPN 터널을 구성할 수 있습니다. 즉, IPSec 터널로 라우팅되는 모든 트래픽은 소스/대상 서브넷에 관계없이 암호화됩니다.

정책 기반 사이트 간 VPN을 구성하려면 다음 조건 중 하나를 충족해야 합니다.

- 두 피어 모두 CDO 관리 ASA입니다.
- 피어 중 하나는 CDO 관리 ASA이고 다른 하나는 정책 기반 VPN 지원 디바이스입니다.

자세한 정보는 사이트 간 가상 프라이빗 네트워크를 참조하십시오.

2022년 8월

2022년 8월 4일

FDM-관리 디바이스**,** 버전 **7.2** 에 대한 **CDO** 지원

CDO는 이제 FDM 관리 디바이스용 버전 7.2를 지원합니다. CDO 지원은 다음과 같은 측면을 제공합니다.

- 버전 7.2를 실행하는 지원되는 물리적 또는 가상 FDM 관리 디바이스를 CDO에 온보딩합니다.
- 버전 6.4 이상에서 버전 7.2로 FDM 관리 디바이스를 업그레이드합니다.
- 기존 Secure Firewall Threat Defense 기능을 지원합니다.
- 버전 7.2를 실행하는 지원되는 물리적 또는 가상 디바이스를 클라우드 제공 Firewall Management Center에 온보딩합니다.

참고 CDO는 버전 7.2 릴리스에 도입된 기능을 지원하지 않습니다.

2022년 6월

2022년 6월 30일

Cisco Secure Firewall 마이그레이션 툴**, Cisco Secure Firewall Threat Defense** 마이그레이션 지원

Secure Firewall 마이그레이션 툴을 사용하면 Secure Firewall ASA 구성을 온프레미스 또는 가상 Secure Firewall Management Center 또는 Cisco Defense Orchestrator의 새로운 클라우드 제공 Firewall Management Center에서 관리하는 Cisco Secure Firewall Threat Defense로 마이그레이션할 수 있습니다. 데스크톱 툴은 서드파티 벤더인 Check Point, Palo Alto Networks 및 Fortinet의 마이그레이션도 지원합니다.

Cisco Secure Firewall 마이그레이션 툴 버전 3.0은 Threat Defense 소프트웨어 버전 7.2를 실행하는 Secure Firewall Threat Defense 디바이스로의 마이그레이션을 지원합니다. 해당 버전의 위협 방어는 CDO의 클라우드 제공 Firewall Management Center에서 관리할 수 있습니다. 마이그레이션 프로세스는 CDO의 일부이며 CDO 라이선스 이외의 특정 라이선스가 필요하지 않습니다.

Software Download(소프트웨어 다운로드) 페이지에서 Secure Firewall 마이그레이션 툴을 다운로드할 수 있습니다.

CDO는 ASA에서 실행 중인 구성의 다음 요소를 위협 방어 템플릿으로 마이그레이션하는 데 도움이 되는 마법사를 제공합니다.

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

구성을 실행하는 ASA의 이러한 요소가 마이그레이션되면 CDO의 클라우드 제공 Firewall Management Center에서 관리하는 새로운 위협 방어 디바이스에 구성을 구축할 수 있습니다.

자세한 내용은 Cisco Secure Firewall 마이그레이션 툴을 사용하여 ASA 방화벽을 Cisco Secure Firewall Threat Defense로 마이그레이션을 참고하십시오.

2022년 6월 9일

클라우드 제공 **Firewall Management Center**를 사용하여 **Cisco Secure Firewall Threat Defense** 디바이스 관리

CDO(Cisco Defense Orchestrator)는 이제 클라우드 제공 Firewall Management Center의 플랫폼입니다.

클라우드 제공 Firewall Management Center는 Secure Firewall Threat Defense 디바이스를 관리하는 SaaS(Software-as-a-Service) 제품입니다. 이는 온프레미스 Secure Firewall Management Center와 동일한 여러 기능을 제공하며, 온프레미스 Secure Firewall Management Center와 모양과 동작이 동일하며, 동일한 FMC API를 사용합니다.

이 제품은 Secure Firewall Management Center의 온프레미스 버전에서 SaaS 버전으로 이동하려는 Secure Firewall Management Center 고객을 위해 설계되었습니다.

SaaS 제품인 CDO 운영 팀은 이를 유지 관리합니다. 새로운 기능이 도입되면 CDO 운영 팀이 CDO 및 클라우드 제공 방화벽 관리자를 업데이트합니다.

마이그레이션 마법사를 사용하면 온프레미스 Secure Firewall Management Center에 등록된 Secure Firewall Threat Defense 디바이스를 클라우드 제공 Firewall Management Center로 마이그레이션할 수 있습니다.

Secure Firewall Threat Defense 디바이스 온보딩은 일련 번호를 사용하여 디바이스를 온보딩하거나 등록 키가 포함된 CLI 명령을 사용하는 등 친숙한 프로세스를 사용하여 CDO에서 수행됩니다. 디바이스가 온보딩되면 CDO와 클라우드 제공 Firewall Management Center에 모두 표시되지만 클라우드 제공 Firewall Management Center에서 디바이스를 구성합니다. 버전 7.2 이상을 실행하는 Secure Firewall Threat Defense 디바이스를 온보딩할 수 있습니다.

클라우드 제공 Firewall Management Center의 라이선스는 디바이스별 매니지드 라이선스이며 클라우드 제공 FMC 자체에는 라이선스가 필요하지 않습니다. 기존 보안 방화벽 위협 방어 디바이스는 기존 스마트 라이선스를 재사용하며, 새 보안 방화벽 위협 방어 디바이스는 FTD에서 구현된 각 기능에 대해 새 스마트 라이선스를 프로비저닝합니다.

원격 지사 구축에서 위협 방어 디바이스의 데이터 인터페이스는 디바이스의 관리 인터페이스 대신 Cisco Defense Orchestrator 관리에 사용됩니다. 대부분의 원격 지사에서는 단일 인터넷 연결만 가능하

므로 외부 CDO 액세스를 통해 중앙 집중식 관리가 가능합니다. 원격 지사 구축의 경우 CDO는 데이터 인터페이스를 통해 관리하는 위협 방어 디바이스에 대한 고가용성 지원을 제공합니다.

Security Analytics and Logging(SaaS) 또는 Security Analytics and Logging(온프레미스)을 사용하여 온보딩된 위협 방어 디바이스에서 생성된 시스템 로그 이벤트를 분석할 수 있습니다. SaaS 버전은 클라우드에 이벤트를 저장하며 CDO에서 이벤트를 볼 수 있습니다. 온프레미스 버전은 온프레미스 Secure Network Analytics 어플라이언스에 이벤트를 저장하며, 분석은 온프레미스 Secure Firewall Management Center에서 수행됩니다. 두 경우 모두 오늘날의 온프레미스 FMC와 마찬가지로 센서에서 직접 선택한 로그 컬렉터로 로그를 전송할 수 있습니다.

FTD 대시보드는 클라우드 제공 Firewall Management Center에서 관리하는 모든 위협 방어 디바이스에서 수집 및 생성된 이벤트 데이터를 포함하여 상태를 한눈에 볼 수 있도록 제공합니다. 이 대시보드를 사용하여 디바이스 상태 및 구축에 있는 디바이스의 전반적인 상태와 관련된 종합적인 정보를 볼 수 있습니다. FTD 대시보드가 제공하는 정보는 시스템에서 디바이스의 라이선스, 구성 및 구축 방법에 따라 달라집니다. FTD 대시보드에는 모든 CDO 매니지드 위협 방어 디바이스에 대한 데이터가 표시됩니다. 그러나 디바이스 기반 데이터를 필터링하도록 선택할 수 있습니다. 특정 시간 범위에 대해 표시할 시간 범위를 선택할 수도 있습니다.

Cisco Secure Dynamic Attributes Connector를 사용하면 클라우드 제공 Firewall Management Center 액세스 제어 규칙에서 다양한 클라우드 서비스 플랫폼의 서비스 태그 및 범주를 사용할 수 있습니다. IP 주소와 같은 네트워크 구성은 워크로드의 동적 특성과 IP 주소 중복의 불가피성으로 인해 가상, 클라우드 및 컨테이너 환경에서 일시적일 수 있습니다. 고객은 IP 주소 또는 VLAN이 변경되는 경우에도 방화벽 정책이 유지되도록 VM 이름 또는 보안 그룹과 같은 비 네트워크 구문을 기반으로 정책 규칙을 정의해야 합니다.

하나 이상의 매니지드 디바이스의 프록시 시퀀스를 사용하여 LDAP, Active Directory 또는 ISE/ISE-PIC 서버와 통신할 수 있습니다. 이는 Cisco Defense Orchestrator(CDO)가 Active Directory 또는 ISE/ISE-PIC 서버와 통신할 수 없는 경우에만 필요합니다. 예를 들어 CDO은(는) 퍼블릭 클라우드에 있지만 Active Directory 또는 ISE/ISE-PIC는 프라이빗 클라우드에 있을 수 있습니다.

하나의 매니지드 디바이스를 프록시 시퀀스로 사용할 수 있지만, 둘 이상의 매니지드 디바이스를 설정하는 것이 좋습니다. 그러면 하나의 매니지드 디바이스가 Active Directory 또는 ISE/ISE-PIC와 통신할 수 없는 경우 다른 매니지드 디바이스가 인계받을 수 있습니다.

모든 고객은 CDO를 사용하여 보안 방화벽 ASA, Meraki, Cisco IOS 디바이스, Secure Firewall Cloud Native, Umbrella 및 AWS 가상 프라이빗 클라우드와 같은 다른 디바이스 유형을 관리할 수 있습니다. Firepower Device Manager에서 로컬 관리용으로 구성된 Secure Firewall Threat Defense 디바이스를 CDO를 사용하여 관리하는 경우 CDO로도 계속 관리할 수 있습니다. CDO를 처음 사용하는 경우 클라우드에서 제공하는 새로운 Firewall Management Center 및 기타 모든 디바이스 유형을 사용하여 Secure Firewall Threat Defense 디바이스를 관리할 수 있습니다.

클라우드 제공 Firewall Management Center에서 지원하는 Firewall Management Center 기능에 대해 자세히 알아보십시오.

- 상태 모니터링
- Secure Firewall Threat Defense 디바이스 백업/복원
- 일정 예약
- 가져오기/내보내기

- 알림 응답을 사용한 외부 알림
- 투명 방화벽 또는 라우팅 방화벽 모드
- Secure Firewall Threat Defense 디바이스의 고가용성
- 인터페이스
- NAT(Network Access Control)
- 고정 및 기본 경로 및 기타 라우팅 구성
- 개체 관리 및 인증서
- 원격 액세스 VPN 및 사이트 간 VPN 구성
- Access Control(액세스 컨트롤) 정책
- Cisco Secure Dynamic Attributes Connector
- 침입 탐지 및 방지 정책
- 네트워크 악성코드 및 보호 및 파일 정책
- 암호화된 트래픽 처리
- 사용자 ID
- FlexConfig 정책

SecureX를 사용하여 온프레미스 **management center** 온보딩

이미 Securex 계정과 연결된 온프레미스 management center가 있는 경우 SecureX를 통해 management center를 CDO에 온보딩할 수 있습니다. SecureX를 통해 온보딩된 디바이스는 기존 방법을 통해 온보딩된 management center와 동일한 수준의 기능 지원 및 기능을 경험합니다. SecureX를 통해 management center를 CDO에 온보딩하려면 SecureX를 사용하여 온프레미스 FMC 온보딩을 참조하십시오.

참고 management center 계정이 SecureX와 연결되어 있더라도 management center 온보딩을 시도하기 전에 CDO 계정을 SecureX와 병합하는 것이 좋습니다. 자세한 내용은 CDO 및 SecureX 계정 병합을 참조하십시오.

2022년 5월

2022년 5월 12일

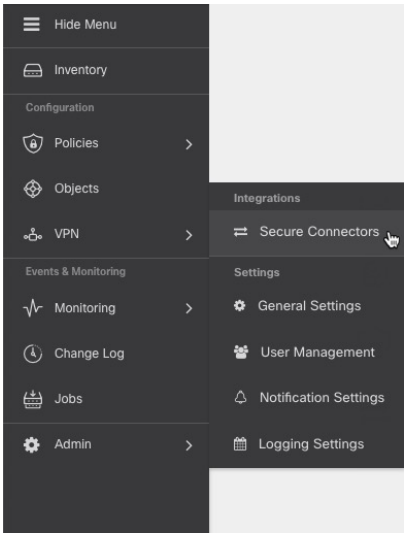
IPv6에 대한 **ASA** 정책 지원

이제 ASA 액세스 정책 및 NAT 구성에서 IPv6 주소를 포함하는 네트워크 개체 및 네트워크 그룹을 사용하는 규칙을 지원합니다. 또한 이러한 규칙은 ICMP 및 ICMPv6 프로토콜을 지정할 수 있습니다. 마지막으로, 이제 ASA는 IPv6 주소를 포함하는 AnyConnect 연결 프로파일을 지원합니다. 자세한 내용은 ASA 네트워크 정책을 참조하십시오.

보안 커넥터 페이지로 이동

CDO 메뉴 모음에서 Secure Connector(보안 커넥터) 페이지에 액세스할 수 있습니다. Secure Connector(보안 커넥터) 페이지를 보려면 **Admin(**관리자**)** > **Secure Connector(**보안 커넥터**)**를 선택합니다.

그림 *1:* 보안 커넥터 메뉴



2022년 4월

2022년 4월 14일

AWS Transit Gateway를 사용하여 **AWS VPC** 터널 모니터링

CDO는 이제 AWS Transit Gateway를 사용하여 AWS VPC 터널을 모니터링할 수 있습니다. 자세한 내용은 AWS Transit Gateway를 사용하여 AWS VPC 터널 모니터링을 참조하십시오.

2022년 4월 6일

글로벌 검색

글로벌 검색은 CDO 내에서 사용 가능한 모든 온보딩 디바이스 및 관련 개체를 검색할 수 있는 옵션을 제공합니다. 검색 결과를 통해 해당 디바이스 및 개체 페이지로 이동할 수 있습니다.

현재 CDO는 ASA, Firepower Management Center, Secure Firewall Threat Defense, Meraki 및 Secure Firewall Cloud Native 디바이스에 대한 글로벌 검색을 지원합니다.

자세한 내용은 다음 문서에서 "글로벌 검색"을 참조하십시오.

- Cisco Defense Orchestrator를 사용한 ASA 관리
- Cisco Defense Orchestrator를 사용한 FMC 관리
- Cisco Defense Orchestrator를 사용한 FTD 관리
- Cisco Defense Orchestrator를 사용한 Meraki 관리
- Cisco Defense Orchestrator를 사용하여 Cisco Secure Firewall Cloud Native 관리

Cisco Secure Firewall 3100에 대한 지원

Cisco Defense Orchestrator는 새로운 Cisco Secure Firewall 3100 Series 디바이스에서 실행되는 온보딩 ASA 및 Secure Firewall Threat Defense 디바이스를 지원합니다.

Secure Firewall Threat Defense 디바이스는 로우 터치 프로비저닝을 사용하거나 등록 키 또는 일련 번호를 사용하여 온보딩할 수 있습니다.

2022년 2월

2022년 2월 3일

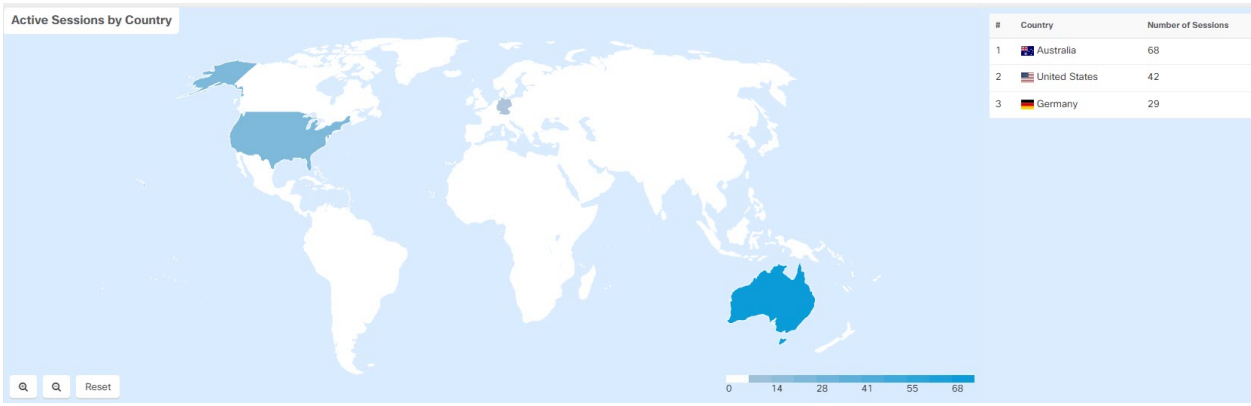
사용자 관리의 **AD(Active Directory)** 그룹

CDO에서 사용자를 더 쉽게 관리하기 위해 개별 사용자를 관리하는 대신 CDO에서 AD(Active Directory) 그룹을 매핑할 수 있습니다. 새 사용자 추가, 기존 사용자 제거 또는 역할 변경과 같은 사용자 변경 사항은 이제 CDO 내에서 아무것도 변경하지 않고 Active Directory에서 수행할 수 있습니다. 이제 CDO는 AD를 사용하는 사용자당 여러 역할도 지원합니다. 자세한 내용은 디바이스 구성 가이드의 사용자 관리 장의 "사용자 관리의 Active Directory 그룹" 섹션을 참조하십시오.

활성 원격 액세스 **VPN** 세션에 대한 향상된 차트 보기

이제 CDO는 활성 RA VPN 세션에 대한 새롭고 향상된 차트 보기를 제공합니다. 이미 익숙한 차트 외에도 CDO는 이제 RA VPN 헤드엔드에 연결된 사용자 위치의 히트맵을 표시합니다. 이 맵은 라이브 보기에서만 사용할 수 있습니다.

새 차트 보기를 보려면 RA VPN Monitoring(RA VPN 모니터링) 페이지에서 화면의 오른쪽 상단에 표시되는 **Show Charts View(**차트 보기 표시**)** 아이콘을 클릭합니다.



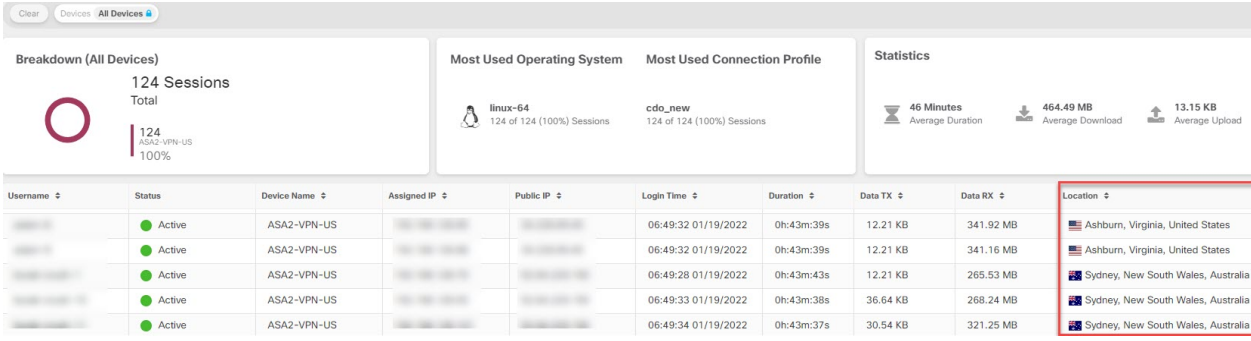
자세한 내용은 방화벽에 따라 Cisco Defense Orchestrator를 사용하여 FTD 관리, Cisco Defense Orchestrator를 사용하여 ASA 관리 또는 Cisco Defense Orchestrator를 사용하여 Cisco Secure Firewall Cloud Native 관리의 "원격 액세스 가상 사설 네트워크 세션 모니터링"을 참조하십시오.

2022년 1월

2022년 1월 20일

원격 액세스 **VPN** 사용자의 지리위치 정보

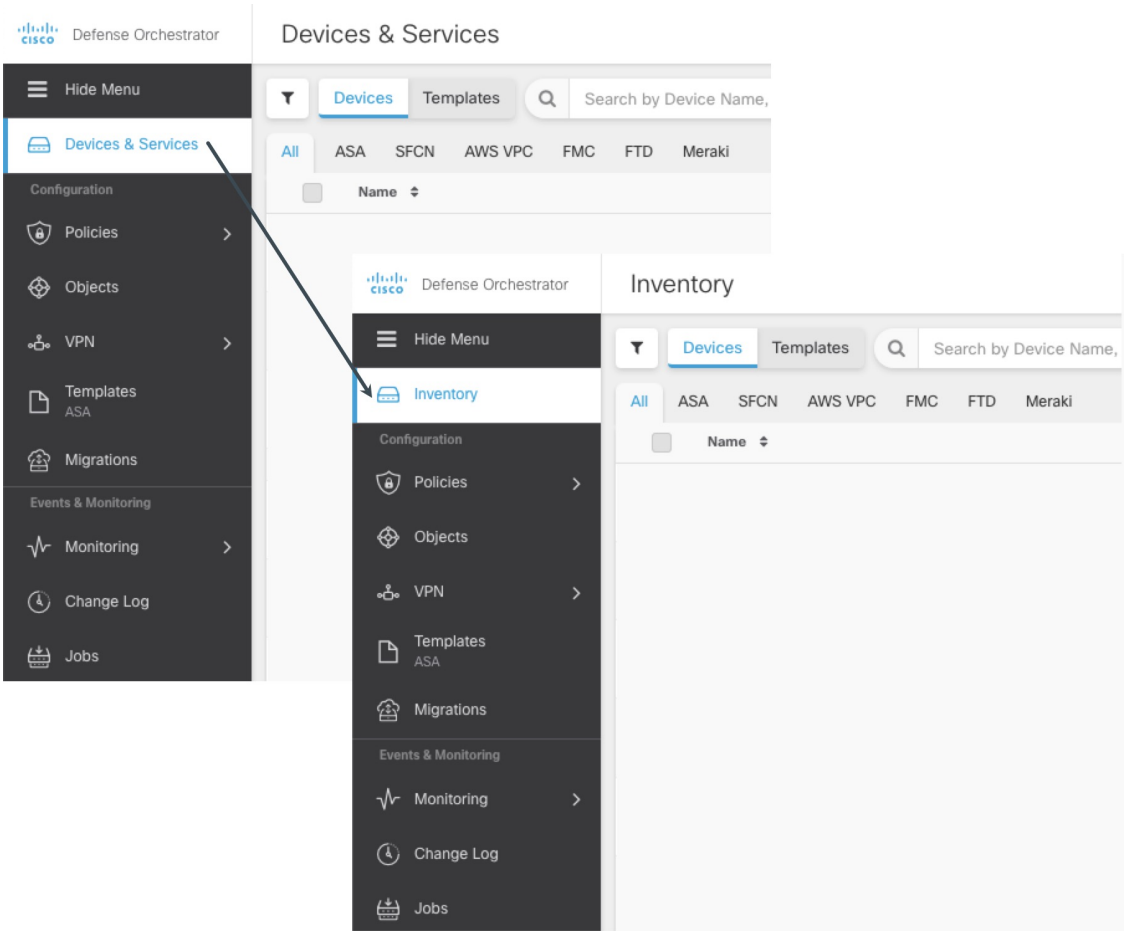
이제 원격 액세스 VPN 모니터링 페이지에 VPN 헤드엔드에 연결된 모든 사용자의 위치가 표시됩니다. CDO는 사용자의 공용 IP 주소를 지리위치로 확인하여 이 정보를 얻습니다. 이 정보는 라이브 및 기록 보기에서 사용할 수 있습니다. 왼쪽 창의 **User Details(**사용자 세부 정보**)** 영역에서 위치를 클릭하면 사용자의 정확한 위치가 맵에 표시됩니다.



참고 이 정보는 새 CDO 구축 이후에 설정된 사용자 세션에서 사용할 수 있으며 기존 사용자 세션에서는 사용할 수 없습니다.

Devices & Services(디바이스 및 서비스) 페이지 이름이 **Inventory(재고 목록)**로 변경됨

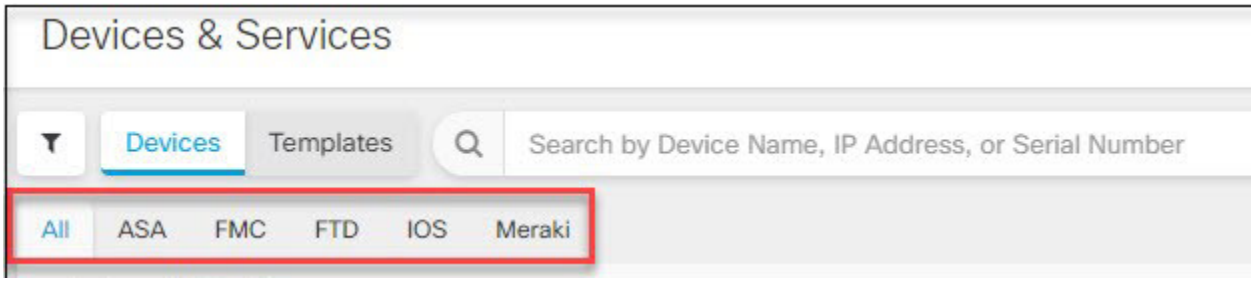
Devices & Services(디바이스 및 서비스) 페이지의 이름이 "Inventory(재고 목록)"로 변경되었습니다. Inventory(재고 목록) 테이블에는 CDO로 관리하는 모든 디바이스 및 서비스가 나열됩니다. 이름 변경으로 인해 추가되거나 제거된 기능은 없습니다.



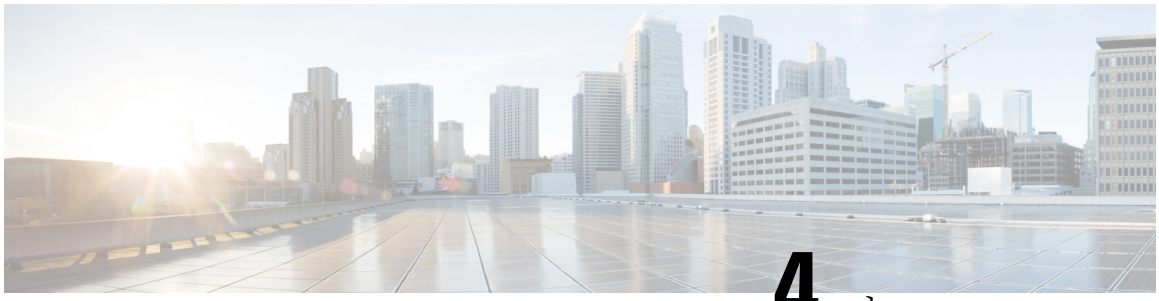
2022년 1월 13일

향상된 디바이스 및 서비스 인터페이스

이제 CDO 디바이스 및 서비스 인터페이스에서 유형에 따라 디바이스 및 템플릿을 분류하고 각 디바이스 유형 전용의 해당 탭에 표시합니다.


Devices & Services
Devices
Templates
Search by Device Name, IP Address, or Serial Number
All
ASA
FMC
FTD
IOS
Meraki

2022년 1월 13일



4 장

2021의 주요 기능

이 문서에서는 2021년에 Cisco Defense Orchestrator에 추가된 몇 가지 기능에 대해 설명합니다.

2021년 12월

2021년 12월 9일

Firepower Threat Defense, 버전 **7.1**에 대한 **CDO** 지원

CDO는 이제 FTD(Firepower Threat Defense) 버전 7.1 디바이스를 지원합니다. 다음은 CDO가 제공하는 지원 측면입니다.

- Firepower Threat Defense 버전 7.1을 실행하는 지원되는 물리적 또는 가상 디바이스를 온보딩합니다.
- Firepower Threat Defense 버전 6.4 이상에서 버전 7.1로 업그레이드합니다.
- 기존 Firepower Threat Defense 기능을 지원합니다.

다음 주의 사항은 Firepower Threat Defense, 버전 7.1 지원에 적용됩니다.

- CDO는 현재 버전 7.1을 실행하는 Firepower Threat Defense 디바이스 백업을 지원하지 않습니다. 이 기능에 대한 지원은 Firepower Threat Defense, 버전 7.1의 첫 번째 유지 보수 릴리스에서 제공될 예정입니다.
- CDO는 Firepower Threat Defense, 버전 7.1 릴리스에 도입된 기능을 지원하지 않습니다.

CDO가 현재 지원하는 FTD 기능에 대한 자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리를 참조하십시오.

새 **CDO** 문서 플랫폼

온라인 도움말

- 모든 디바이스를 설명하는 콘텐츠를 한 곳에서 확인할 수 있습니다.
- 상황별 도움말.
- 검색하는 동안 콘텐츠 일치 항목이 발견되었습니다.
- 목차에서 강조 표시된 검색 결과는 더 큰 컨텍스트로 정보를 제공합니다.

Cisco.com에서 유지 관리되는 콘텐츠

- Cisco.com의 가용성은 모든 Cisco 설명서를 하나의 사이트에 배치합니다.
- 디바이스별 구성 가이드를 사용하면 정보를 더 쉽게 찾을 수 있습니다.
- Cisco Defense Orchestrator의 새로운 기능에서는 CDO에서 사용 가능한 최신 기능에 대해 계속 설명합니다.

2021년 11월

2021년 11월 11일

새로운 **SASE** 터널 기능

이제 CDO UI에서 읽혔거나 CDO UI를 통해 생성된 SASE 터널을 편집할 수 있습니다. 이 기능은 Umbrella 조직과 이미 CDO에 온보딩된 ASA 피어 디바이스 간의 터널만 지원합니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리의 "SASE 터널 편집"을 참조하십시오.

2021년 10월

2021년 10월 21일

향상된 **SecureX** 통합

아직 CDO 테넌트와 SecureX를 연결하지 않은 사용자를 위해 CDO는 이제 SecureX와의 간소화된 통합을 제공합니다. 이 프로세스를 통해 CDO 테넌트를 SecureX 조직에 빠르고 안전하게 연결하고 클릭 한 번으로 CDO 모듈을 SecureX 대시보드에 추가할 수 있습니다. SecureX 조직이 없는 경우 이 프로세스 중에 조직을 생성할 수 있습니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "SecureX와 CDO 통합"을 참조하십시오.

CDO 저장소에서 **AnyConnect** 패키지 업로드

이제 CDO는 CDO 저장소에서 ASA 및 FTD 디바이스로의 AnyConnect 패키지 업로드를 지원합니다.

Remote Access VPN Configuration(원격 액세스 VPN 구성) 마법사는 운영 체제별로 AnyConnect 패키지를 제공하며, 이러한 패키지를 선택하여 디바이스에 업로드할 수 있습니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "CDO 저장소에서 AnyConnect 패키지 업로드" 및 *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리의 "ASA 디바이스에서 AnyConnect 소프트웨어 패키지 관리"를 참조하십시오.

2021년 9월

2021년 9월 16일

서비스 통합을 통한 **CDO** 알림

이제 CDO 알림이 Webhook과 통합됩니다. Notification Settings(알림 설정) 페이지에서 선택한 알림은 선택한 애플리케이션 또는 서비스 통합으로 전송됩니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "CDO 알림에 대한 서비스 통합 활성화"를 참조하십시오.

Cisco Security Analytics and Logging을 위한 **Cisco Secure Firewall Cloud Native** 지원

Cisco Security Analytics and Logging이 Cisco Security Analytics and Logging에서 이벤트 로깅을 지원하도록 크게 확장되었습니다.

Secure Firewall Cloud Native 로깅: Security Analytics and Logging(SAL SaaS)은 이제 모든 Secure Firewall Cloud Native 디바이스에서의 로깅을 지원합니다. 사용자는 Secure Firewall Cloud Native 이벤

트를 시스템 로그 형식, NetFlow NSEL(Security Event Logs) 형식 또는 둘 다로 Cisco Cloud에 저장하고 Cisco Secure Cloud Analytics를 사용하여 분석할 수 있습니다. 로깅 분석을 활성화하려는 고객은 상위 계층 SAL 라이선스에 필요한 텔레메트리를 제공하기 위해 NSEL 로그를 활성화해야 합니다.

- 트래픽 분석 - SAL의 트래픽 분석을 통해 Secure Firewall Cloud Native 로그를 실행할 수 있으며 CDO에서 Cisco Secure Cloud Analytics를 교차 실행하여 관찰 및 알림을 검토할 수 있습니다. 시스템 로그 이벤트를 로깅하는 Cloud Native 고객만 트래픽 분석을 활성화하려면 NSEL 로그로 전환해야 합니다.
- Logging Analytics and Detection 및 Total Network Analytics Detection - Logging Analytics and Detection 및 Total Network Analytics Detection 라이선스를 취득한 고객은 분석을 위해 Secure Cloud Analytics 포털을 프로비저닝하고 사용할 수 있습니다. Secure Cloud Analytics 탐지 항목에는 SAL 사용자가 Secure Cloud Analytics 핵심 기능의 일부로 사용할 수 있는 기타 탐지 항목 외에도 방화벽 로깅 데이터를 사용하여 특별히 활성화된 관찰 및 알림이 포함됩니다. 기존 기록 및 트러블슈팅 라이선스 보유자는 30일 동안 약정 없이 상위 라이선스의 탐지 기능을 테스트할 수 있습니다.
- 무료 평가판: 이 양식을 작성하여 모든 라이선스에 대해 약정 없는 30일 SAL 평가판을 시작할 수 있습니다. 이 평가판에는 클라우드로 데이터를 내보내는 데 필요한 최소 온프레미스 커넥터 집합만 필요합니다. 이 평가판을 사용하여 SAL 기능을 평가하고 프로덕션 환경을 지원하는 데 필요한 데이터 볼륨을 예측할 수 있습니다. 이는 SAL 라이선스에 대한 적절한 일일 볼륨을 구매하기 위한 선행 단계입니다. 이를 위해 SAL 평가판은 대부분의 사용자 볼륨에 대한 데이터를 조절하지 않습니다. 또한 예상 툴을 사용하면 SAL 일일 볼륨을 예측할 수 있습니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *Cisco Secure Firewall Cloud Native* 관리의 "Cisco Security Analytics 및 로깅"을 참조하십시오.

2021년 8월

2021년 8월 26일

CDO 및 Umbrella 통합

이제 CDO에서 Umbrella 통합을 지원합니다. Umbrella 조직을 온보딩하고 Umbrella와 ASA 디바이스 간에 존재하는 SASE 터널을 보고 관리하고 생성할 수 있습니다. ASA 디바이스는 사용하기 쉬운 보안을 위해 중앙 집중식 관리를 제공하는 Umbrella의 SIG 터널 및 검사를 활용합니다.

Umbrella 조직을 온보딩할 때는 해당 조직과 연결된 ASA 디바이스도 온보딩하는 것이 좋습니다.

Umbrella란 무엇이며 CDO와 Umbrella와 통신하는 방법에 대한 자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리를 참조하십시오.

2021년 8월 13일

FTD RA VPN에 **LDAP**를 사용하는 **Duo** 구성 지원

이제 FTD 원격 액세스 VPN 연결에 LDAP를 사용하여 Duo 2단계 인증을 구성할 수 있습니다.

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

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "LDAP를 사용한 Duo 이중 인증"을 참조하십시오.

2021년 7월

2021년 7월 8일

ASA용 디지털 인증서 관리 지원

이제 CDO가 ASA 디바이스에서 디지털 인증서를 관리합니다. ID 인증서 및 신뢰할 수 있는 CA 인증서와 같은 디지털 인증서를 신뢰 지점 개체로 추가하고 하나 이상의 매니지드 ASA 디바이스에 설치할 수 있습니다. 설치된 ID 인증서를 내보내 다른 ASA에서 신뢰 지점 구성을 수동으로 복제할 수도 있습니다.

다음 형식으로 ID 인증서를 업로드하거나 생성할 수 있습니다.

- 암호가 있는 PKCS12 파일
- 자체 서명 인증서
- 인증 기관이 서명한 CSR(Certificate Signing Request)

원격 액세스 VPN은 디지털 인증서를 사용하여 ASA 및 AnyConnect 클라이언트를 인증하여 보안 VPN 연결을 설정합니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리의 "ASA 인증서 관리"를 참조하십시오.

RA VPN ASA 및 **FTD**에 대한 **AnyConnect** 모듈 지원

이제 CDO는 ASA 및 FTD 디바이스에서 AnyConnect 모듈 관리를 지원합니다.

참고 이 기능은 소프트웨어 버전 6.7 이상을 실행하는 FTD에서 지원됩니다.

RA VPN 그룹 정책 생성의 일부로 이제 사용자가 Cisco AnyConnect VPN Client를 다운로드할 때 다운로드 및 설치할 다양한 선택적 모듈을 구성할 수 있습니다. 이러한 모듈은 웹 보안, 악성코드 방지, 네트워크 외부 로밍 방지 등의 서비스를 제공할 수 있습니다.

AnyConnect 프로파일 편집기에서 생성되고 AnyConnect 파일 개체로 CDO에 업로드된 맞춤형 구성이 포함된 프로파일과 각 모듈을 연결할 수 있습니다.

프로파일을 업로드하고 그룹 정책에 할당하는 방법에 대한 자세한 내용은 *Cisco Defense Orchestrator를 사용하여 FTD 관리*의 "RA VPN AnyConnect 클라이언트 프로파일 업로드" 및 "새 FTD RA VPN 그룹 정책 생성"을 참조하십시오.

2021년 7월 1일

Snort 3 지원

이제 CDO는 버전 6.7 이상을 실행하는 FTD 디바이스에 대해 Snort 3 처리 엔진을 지원합니다. Snort 엔진은 새 Snort 규칙을 자동으로 업데이트하여 디바이스가 최신 취약점을 준수하도록 합니다. Snort 2에서 Snort 3으로 독립형 업그레이드를 수행하거나 디바이스 시스템과 Snort 엔진을 동시에 업그레이드하여 업그레이드 경험을 간소화할 수 있습니다.

자세한 내용은 *Cisco Defense Orchestrator를 사용하여 FTD 관리*의 "Snort 3.0으로 업그레이드"를 참조하십시오.

맞춤형 침입 방지 시스템 정책

CDO는 이제 버전 6.7 이상을 실행하는 FTD 디바이스에 대해 Snort 3 및 맞춤형 IPS(Intrusion Prevention System) 정책을 지원합니다. 개선된 Snort 3 처리 엔진을 사용하면 Cisco Talos Intelligence Group(Talos)에서 제공하는 규칙을 사용하여 IPS 정책을 생성하고 사용자 지정할 수 있습니다. 모범 사례는 제공된 Talos 정책 템플릿을 기반으로 고유한 정책을 생성하고 규칙 작업을 조정해야 하는 경우 변경하는 것입니다.

참고 업그레이드에 따라 규칙이 구성되는 방식이 변경될 수 있으므로 Snort 3으로 또는 Snort 3에서 업그레이드할 때 차이점과 제한 사항에 유의해야 합니다.

자세한 내용은 *Cisco Defense Orchestrator로 FTD 관리*의 "맞춤형 Firepower 침입 방지 시스템 정책"을 참조하십시오.

2021년 6월

2021년 6월 17일

Firepower Threat Defense, 버전 **7.0**에 대한 **CDO** 지원

이제 CDO에서 FTD(Firepower Threat Defense), 7.0을 지원합니다. FTD 7.0을 실행하는 FTD 디바이스를 온보딩하거나 CDO를 사용하여 해당 버전으로 디바이스를 업그레이드할 수 있습니다. CDO는 DNS 트래픽에 대한 새로운 평판 적용 기능 외에도 기존 FTD 기능을 계속 지원합니다. 이 기능은 액세스 제어 정책 설정입니다. URL 필터링 범주 및 평판 규칙을 DNS 조회 요청에 적용하려면 이 옵션을 활성화합니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "액세스 정책 설정 구성"을 참조하십시오.

CDO는 다음 기능을 제한적으로 지원합니다.

- FTDv 계층형 라이선스 지원 - 버전 7.0은 처리량 요구 사항 및 RA VPN 세션 제한을 기반으로 FTDv 장치에 대한 성능 계층형 스마트 라이선스를 지원합니다. 현재 CDO는 계층형 스마트 라이선싱을 완전히 지원하지 않습니다. 계층형 라이선스를 사용하는 FTDv 디바이스를 온보딩할 수 있지만 CDO를 사용하여 라이선스를 업데이트할 수는 없습니다. 디바이스의 Firepower Device Manager를 사용하여 FTDv에서 라이선스를 설치하고 관리합니다.

  자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "FTD 라이선싱"을 참조하십시오.

- Scan Interface Support(스캔 인터페이스 지원) - Firepower 4100 Series 또는 9300 Series 디바이스에서 FXOS(Firepower eXtensible Operating System) Chassis Manager를 사용하여 인터페이스를 Firepower 디바이스에 추가하는 경우 FDM에서 해당 인터페이스를 구성한 다음 CDO " 변경 사항 확인"을 클릭하여 구성에서 읽을 수 있습니다.

  자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "FXOS를 사용하여 Firepower 디바이스에 추가된 인터페이스 동기화"를 참조하십시오.

- 가상 라우터 지원 - VRF 경로가 CDO에 표시되지 않습니다. 가상 경로를 지원하는 디바이스를 온보딩할 수는 있지만 CDO의 정적 라우팅 페이지에서 가상 경로를 볼 수는 없습니다.

  자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "가상 라우팅 및 포워딩 정보"를 참조하십시오.

- ECMP(Equal Cost Multi Path Routing) - CDO는 ECMP를 사용하는 디바이스를 온보딩하고 구성을 읽을 수 있지만 사용자가 이를 수정할 수는 없습니다. FDM을 통해 ECMP 구성을 생성하고 변경한 다음 CDO로 읽을 수 있습니다.

- 규칙 집합 - FTD 7.0 디바이스에는 규칙 집합을 적용할 수 없습니다.

참고 CDO가 현재 지원하는 FTD 기능에 대한 자세한 내용은 Cisco Defense Orchestrator를 사용하여 FTD 관리를 참조하십시오.

2021년 6월 10일

Cisco Secure Firewall Cloud Native 지원

CDO는 이제 Cisco Secure Firewall Cloud Native를 지원합니다. Cisco Secure Firewall Cloud Native는 확장성과 관리성을 위해 Kubernetes(K8s) 오케스트레이션을 사용하여 Cisco의 업계 최고의 보안을 CNFW(클라우드 네이티브 폼 팩터)로 원활하게 확장합니다. Amazon Elastic Kubernetes Service(Amazon EKS)는 AWS 클라우드에서 Kubernetes 애플리케이션을 시작, 실행 및 확장할 수 있는 유연성을 제공합니다. Amazon EKS는 고가용성 및 보안 클러스터를 제공하고 패치, 노드 프로비저닝, 업데이트 등의 주요 작업을 자동화합니다.

CDO는 이 방화벽의 온보딩을 허용하고 완전한 방화벽 관리를 제공합니다.

- AnyConnect RA VPN 세션에서 실시간 및 기록 데이터를 확인합니다.
- 개체를 생성 및 관리하고 네트워크에서 인그레스 및 이그레스 트래픽을 처리하는 다양한 정책에서 사용합니다.
- Kubernetes 명령줄 툴을 사용하여 CDO 외부에서 방화벽에 대한 변경 사항을 인식하고 조정합니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *Cisco Secure Firewall Cloud Native* 관리를 참조하십시오.

자세한 내용은 *Cisco Secure Firewall Cloud Native* 개요를 참조하십시오.

향상된 원격 액세스 VPN 모니터링

라이브 AnyConnect Remote Access VPN 세션을 모니터링하는 것 외에도 CDO는 이제 지난 3개월 동안 기록된 AnyConnect Remote Access VPN 세션의 기록 데이터를 모니터링할 수 있습니다.

테넌트의 모든 ASA(Adaptive Security Appliance), FTD(Firepower Threat Defense) 및 Cisco SFCN(Secure Firewall Cloud Native) VPN 헤드엔드 전반에서 VPN 세션을 모니터링할 수 있습니다.

다음은 현재 릴리스의 주요 개선 사항입니다.

- CDO에서 관리하는 모든 활성 VPN 헤드엔드의 보기를 한눈에 볼 수 있도록 직관적인 그래픽 시각적 개체를 표시합니다.
- 라이브 세션 화면에는 CDO 테넌트에서 가장 많이 사용되는 운영 체제 및 VPN 연결 프로파일이 표시됩니다. 또한 평균 세션 기간과 업로드 및 다운로드한 데이터도 표시됩니다.
- 과거 세션 화면에는 지난 24시간, 7일, 30일 동안의 모든 디바이스에 대해 기록된 데이터가 표시되는 막대 그래프가 표시됩니다.

- 디바이스 유형, 세션 길이, 업로드 및 다운로드 데이터 범위 등의 기준에 따라 검색 범위를 좁힐 수 있는 새로운 필터링 기능을 제공합니다.

VPN > **Remote Access VPN Monitoring(**원격 액세스 **VPN** 모니터링**)**을 클릭하여 탐색 모음에서 Remote Access VPN Monitoring(원격 액세스 VPN 모니터링) 화면을 엽니다.

새 사용자 역할

이제 CDO는 특정 사용자가 테넌트별로 VPN 세션을 종료할 수 있는 새로운 사용자 역할인 VPN Sessions Manager(VPN 세션 관리자) 사용자 역할을 제공합니다. 이 역할은 VPN 세션을 종료하는 작업만 허용합니다. 이 역할로 지정된 사용자는 읽기 전용 기능으로 제한됩니다.

2021년 5월

2021년 5월 27일

CDO의 향상된 디바이스 알림

이제 CDO 이메일 알림을 구독하고 CDO UI 내에서 최근 알림을 볼 수 있습니다.

테넌트와 연결된 디바이스에서 워크플로우 또는 이벤트 변경이 발생하는 경우 이메일 알림을 수신합니다. 워크플로우 변경 사항에는 구축, 업그레이드 또는 백업이 포함됩니다. 이벤트 변경에는 온라인 또는 오프라인 상태가 되는 디바이스, 충돌 탐지, HA 또는 페일오버 상태, 사이트 간 VPN 연결 상태가 포함됩니다.

참고 이러한 맞춤형 알림은 테넌트와 연결된 모든 디바이스에 적용되며 디바이스별로 적용되지 않습니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "알림 설정"을 참조하십시오.

2021년 3월

2021년 3월 25일

APJC에서 **Cisco Security Analytics and Logging** 가용성

이제 새로 가동된 도쿄 데이터 저장소를 통해 아시아(APJC) 지역에서 Cisco Security Analytics and Logging을 사용할 수 있습니다. Security Analytics가 활성화된 계정은 보안 관련 알림을 위해 호주 시드니의 Cisco Secure Cloud Analytics 서비스에 액세스할 수 있습니다. 이를 통해 아시아 지역은 미주 및 EU 지역에서 사용할 수 있는 기능과 동일하게 유지되었습니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *Cisco Secure Firewall Cloud Native* 관리의 "Cisco Security Analytics and Logging"을 참조하십시오.

2021년 3월 18일

EtherChannel 인터페이스 지원

이제 CDO는 Firepower 버전 6.5 이상을 실행하는 지원되는 모델(예: Firepower 1010, 1120, 1140, 1150, 2110, 2120, 2130, 2140)에서 EtherChannel 인터페이스 구성을 지원합니다. EtherChannel은 포트 링크 집계 기술 또는 포트 채널 아키텍처로, 여러 물리적 이더넷 링크를 그룹화하여 스위치, 라우터 및 서버 간의 링크를 제공하기 위해 하나의 논리적 이더넷 링크를 생성할 수 있습니다.

물리적 포트에 적용하는 구성은 구성을 적용하는 LAN 포트에만 영향을 미칩니다.

디바이스 지원 및 구성 제한 사항에 대한 자세한 내용은 *Cisco Defense Orchestrator*로 *FTD* 관리의 "Firepower 인터페이스 구성에 대한 지침 및 제한 사항"을 참조하십시오.

2021년 3월 15일

ASA 원격 액세스 **VPN** 지원

이제 CDO를 사용하면 ASA(Adaptive Security Appliance) 디바이스에서 RA VPN(Remote Access Virtual Private Network) 구성을 생성하여 원격 사용자가 ASA에 연결하고 원격 네트워크에 안전하게 액세스할 수 있습니다. 또한 ASDM(Adaptive Security Defense Manager) 또는 CSM(Cisco Security Manager)과 같은 다른 ASA 관리 툴을 사용하여 이미 구성된 RA VPN 설정을 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 및 IPv6 주소 지정
- 여러 ASA 디바이스에서 공유 RA VPN 구성

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리의 "ASA에 대한 원격 액세스 VPN 구성"을 참조하십시오.

ASA 파일 관리 지원

CDO는 ASA 디바이스의 플래시(disk0) 공간에 있는 파일 보기, 업로드 또는 삭제와 같은 기본 파일 관리 작업을 수행하기 위한 파일 관리 툴을 제공합니다. 이 툴을 사용하면 원격 서버에서 URL 기반 파일 업로드를 사용하여 AnyConnect 소프트웨어 이미지, DAP.xml, data.xml, 호스트 스캔 이미지 파일 등의 파일을 단일 또는 여러 ASA 디바이스에 업로드할 수 있습니다.

이 툴을 사용하면 새로 릴리스된 AnyConnect 이미지를 여러 ASA 디바이스에 동시에 업로드할 수 있습니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리의 "ASA 파일 관리"를 참조하십시오.

2021년 2월

2021년 2월 11일

다중 보안 디바이스 커넥터 지원

이제 테넌트에 대해 둘 이상의 온프레미스 SDC(Secure Device Connector)를 구축할 수 있습니다. 이를 통해 CDO를 사용하여 더 많은 디바이스를 관리하고 CDO, SDC 및 매니지드 디바이스 간의 통신 성능을 유지할 수 있습니다.

매니지드 ASA, AWS VPC 및 Meraki MX 디바이스를 SDC 간에 이동할 수 있습니다.

SDC가 여러 개 있으면 하나의 CDO 테넌트를 사용하여 격리된 네트워크 세그먼트의 디바이스를 관리할 수도 있습니다. 격리된 네트워크 세그먼트의 모든 매니지드 디바이스를 단일 SDC에 할당하여 이 작업을 수행합니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리의 "단일 CDO 테넌트에서 여러 SDC 사용"을 참조하십시오.

2021년 1월

2021년 1월 21일

FMC 개체 읽기

이제 FMC를 CDO에 온보딩하면 CDO가 FMC 매니지드 FTD 디바이스에서 개체를 가져옵니다. CDO로 가져온 개체는 읽기 전용이 됩니다. FMC 개체는 읽기 전용이지만 CDO를 사용하면 FMC에서 관리하지 않는 테넌트의 다른 디바이스에 개체의 복사본을 적용할 수 있습니다. 복사본은 원본 개체에서 연결 해제되므로 FMC에서 가져온 개체의 값을 변경하지 않고 복사본을 편집할 수 있습니다. FMC 개체는 해당 개체 유형을 지원하는 관리하는 모든 디바이스에서 사용할 수 있습니다.

자세한 내용은 Cisco Defense Orchestrator를 사용하여 FMC 관리의 "FMC 개체"를 참조하십시오.

2021년 1월 14일

CLI 명령 결과 내보내기

독립형 디바이스 또는 여러 디바이스에 실행된 CLI 명령의 결과를 쉼표로 구분된 값(.csv) 파일로 내보내 원하는 대로 정보를 필터링하고 정렬할 수 있습니다. 단일 디바이스 또는 여러 디바이스의 CLI 결과를 한 번에 내보낼 수 있습니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "CLI 명령 결과 내보내기"를 참조하십시오.

FTD 디바이스에 대한 클라우드 서비스 구성

Cisco Success Network에 연결하고 Cisco Cloud로 전송되는 이벤트를 구성하는 것은 소프트웨어 버전 6.6 이상을 실행하는 FTD 디바이스에서 구성할 수 있는 기능입니다.

Cisco Success Network

Cisco Success Network를 활성화하면 FTD를 개선하고 네트워크에서 Cisco 제품의 가치를 극대화하는 데 도움이 되는 미사용 또는 추가 기능을 알리기 위해 Cisco에 사용 정보 및 통계를 제공하게 됩니다. Cisco Success Network를 활성화하면 디바이스는 Cisco Cloud에 대한 보안 연결을 설정하고 항상 이 보안 연결을 유지합니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "Cisco Success Network에 연결"을 참조하십시오.

이벤트를 **Cisco Cloud**에 직접 전송

이제 FTD에서 Cisco Cloud로 직접 전송할 이벤트 유형을 지정할 수 있습니다. 일단 Cisco Cloud에 저장되면 클라우드 애플리케이션(예: Cisco Threat Response)을 사용하여 이벤트를 분석하고 디바이스에 발생했을 가능성이 있는 위협을 평가할 수 있습니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "Cisco Cloud에 이벤트 전송"을 참조하십시오.

웹 분석

웹 분석을 활성화하면 페이지 조회 수를 기반으로 하는 익명 제품 사용 정보가 Cisco에 제공됩니다. 이 정보에는 확인한 페이지, 특정 페이지를 사용한 시간, 브라우저 버전, 제품 버전, 디바이스 호스트 이름 등이 포함됩니다. Cisco는 이 정보를 활용해 기능 사용 패턴을 확인하고 제품을 개선할 수 있습니다. 모든 사용량 데이터는 익명으로 전송되며 민감한 데이터는 전송되지 않습니다. CDO를 사용하여 모든 버전의 FTD에서 이 기능을 구성할 수 있습니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "웹 분석 활성화 또는 비활성화"를 참조하십시오.

2021년 1월 7일

FTD HA 쌍 온보딩

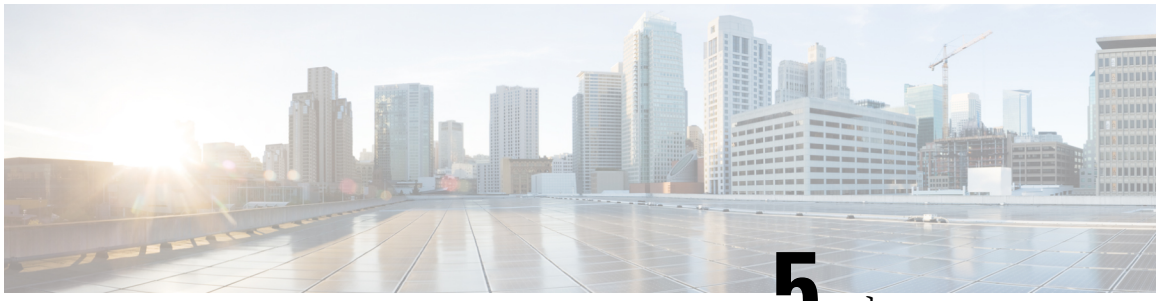
CDO는 FTD HA 쌍의 온보딩 프로세스를 개선했습니다. 등록 토큰 방법 또는 로그인 자격 증명 방법을 사용하여 HA 피어 중 하나를 온보딩하면 CDO는 해당 피어가 아직 온보딩되지 않았음을 자동으로 탐지하고 작업을 수행하라는 메시지를 표시합니다. 이 개선 사항은 두 디바이스를 온보딩하는 데 필요한 노력을 최소화하고, 피어 디바이스를 온보딩하는 데 걸리는 시간을 단축하며, 첫 번째 디바이스를 온보딩하는 데 사용한 등록 키 또는 스마트 라이선스 토큰을 재사용합니다.

액티브 또는 스탠바이 디바이스를 온보딩할 수 있으며, 일단 동기화되면 CDO는 해당 디바이스가 HA 쌍의 일부임을 항상 탐지합니다.

Note 등록 키 방법을 사용하여 FTD 디바이스를 온보딩하는 것이 좋습니다.

FTD HA 쌍 온보딩에 대한 자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "등록 키로 FTD HA 쌍 온보딩" 또는 "사용자 이름 비밀번호 및 IP 주소를 사용하여 FTD HA 쌍 온보딩"을 참조하십시오.

2021년 1월 7일



5 장

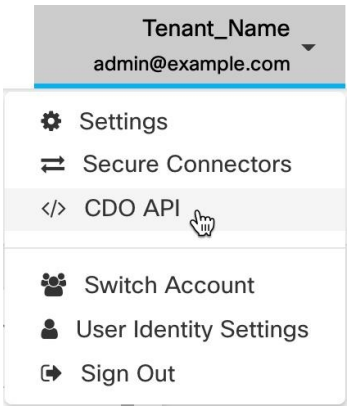
2020의 주요 기능

2020년 12월

2020년 12월 17일

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.

사용자 메뉴에서 CDO 공용 API를 선택하여 시작할 수 있습니다.

2020년 12월 10일

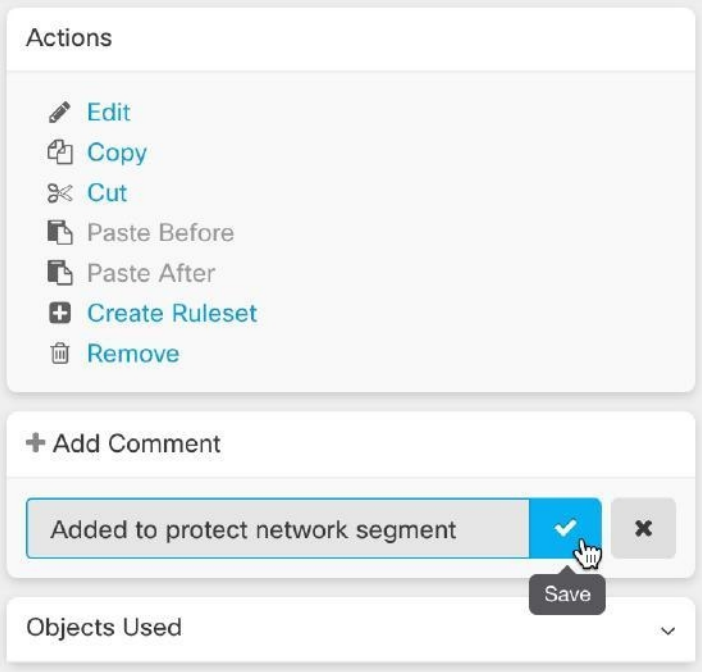
FTD 구성 내보내기

이제 FTD 디바이스의 전체 구성을 CDO가 읽을 수 있는 JSON 파일로 내보낼 수 있습니다. 관리하는 모든 CDO 테넌트에서 이 파일을 FTD 모델(FTD 템플릿)로 가져올 수 있습니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "FTD 구성 내보내기"를 참조하십시오.

FTD 규칙에 코멘트 추가

이제 FTD 정책 및 규칙 집합의 규칙에 코멘트를 추가할 수 있습니다. 규칙 코멘트는 CDO에만 표시됩니다. 이는 FTD에 기록되지 않으며 FDM에 표시되지도 않습니다.



자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "FTD 정책 및 규칙 집합의 규칙에 코멘트 추가"를 참조하십시오.

2020년 11월

2020년 11월 13일

로우 터치**(Low-Touch)** 프로비저닝 및 일련 번호 온보딩

로우 터치 프로비저닝은 FTD 소프트웨어 버전 6.7 이상을 실행하는 새로운 Firepower 1000 또는 2100 Series 디바이스를 공장에서 배송하거나 이미지 재설치한 후 네트워크에 연결하고 CDO에 자동으로 온보딩한 다음 원격으로 구성할 수 있는 기능입니다. 이렇게 하면 CDO에 디바이스를 온보딩하는 것과 관련된 많은 수동 작업이 필요하지 않습니다. 로우 터치 프로비저닝 프로세스는 물리적 디바이스에 로그인해야 하는 필요성을 최소화합니다. 직원이 네트워킹 디바이스를 사용한 경험이 적은 원격 사무실 또는 기타 위치를 위한 것입니다.

FTD 6.7 이미지가 공장에서 설치된 Firepower 1000 및 2100 Series 디바이스는 2020년 말 또는 2021년 초에 Cisco에서 주문할 수 있습니다.

디바이스의 일련 번호를 사용하여 구성된 FTD(Firepower Threat Defense) 버전 6.7 이상 디바이스를 FTD 6.7에 온보딩하고 CDO에 온보딩할 수도 있습니다.

자세한 내용은 다음 문서를 참조하십시오.

- 로우 터치 프로비저닝

- 일련 번호가 있는 FTD 6.7 디바이스 온보딩
- Cisco Firepower 1000 또는 2100 방화벽용 Firepower Easy 구축 가이드

보안 영역에 **Firepower Threat Defense** 인터페이스 할당

이제 FTD 인터페이스를 보안 영역에 할당하여 트래픽을 추가로 분류하고 관리할 수 있습니다. 자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "보안 영역에 Firepower 인터페이스 할당"을 참조하십시오.

2020년 11월 6일

Firepower Threat Defense, 버전 **6.6.1** 및 **6.7**에 대한 **CDO** 지원

CDO는 이제 FTD(Firepower Threat Defense) 버전 6.6.1 및 6.7을 지원합니다. FTD 6.6.1 또는 6.7을 실행하는 새 FTD 디바이스를 온보딩하거나 CDO를 사용하여 해당 버전으로 업그레이드할 수 있습니다. CDO는 기존 FTD 기능과 다음과 같은 새로운 FTD 6.7 기능을 계속 지원합니다.

- 보안 그룹 태그 및 SGT 그룹
- Active Directory 영역 개체

CDO가 현재 지원하는 FTD 기능에 대한 자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리를 참조하십시오.

버전 **6.7**의 **CDO TLS** 서버 **ID** 검색 및 **TLS 1.3**

이제 서버 인증서의 정보를 사용하여 TLS 1.3으로 암호화된 트래픽에서 URL 필터링 및 애플리케이션 제어를 수행할 수 있습니다. 이 기능이 작동하기 위해 트래픽 암호를 해독할 필요는 없습니다. 애플리케이션 또는 URL 필터링을 사용하는 액세스 규칙과 일치하도록 TLS 1.3으로 암호화된 트래픽의 경우 시스템은 TLS 1.3 인증서를 암호 해독해야 합니다. 암호화된 연결이 올바른 액세스 제어 규칙과 일치하는지 확인하려면 FDM(Firepower Device Manager)이든 FMC(Firepower Management Center)이든 관리 UI에서 **TLS** 서버 **ID** 검색을 활성화하는 것이 좋습니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "Firepower Threat Defense의 TLS 서버 ID 검색"을 참조하십시오.

2020년 10월

2020년 10월 15일

새 사용자 역할

이제 CDO는 정책 수정과 정책 구축의 책임을 나누는 두 가지 추가 사용자 역할을 제공합니다. 새로운 **Edit-Only(**편집 전용**)** 역할을 통해 사용자는 디바이스의 구성을 변경할 수 있지만 이러한 변경 사

항을 구축할 수는 없습니다. 새로운 **Deploy-Only(**구축 전용**)** 역할을 통해 사용자는 보류 중인 구성 변경 사항을 구축할 수 있지만 구성을 변경할 수는 없습니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FMC* 관리의 "사용자 역할"을 참조하십시오.

2020년 10월 2일

FTD API 지원

CDO는 이제 FTD 디바이스에서 고급 작업을 수행하기 위해 REST(Representational State Transfer) API(애플리케이션 프로그래밍 인터페이스) 요청을 실행할 수 있는 API 툴 인터페이스를 제공합니다. 또한 이 인터페이스는 다음 기능을 제공합니다.

- 이미 실행된 API 명령의 이력을 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.

FTD API 툴에 대한 자세한 내용은 *Cisco Defense Orchestrator*로 *FTD* 관리의 "FTD API 툴 사용"을 참조하십시오.

2020년 9월

2020년 9월 25일

멀티 테넌트 포털 지원

이제 CDO에는 다양한 지역의 테넌트에서 디바이스의 통합 보기를 제공하는 다중 테넌트 포털이 도입되었습니다. 이 보기는 단일 창에서 테넌트의 정보를 수집하는 데 도움이 됩니다. CDO 지원 팀이 요구 사항에 따라 하나 이상의 포털을 생성하도록 할 수 있습니다.

- 다음 정보를 제공하는 Device Details(디바이스 세부 정보) 보기를 제공합니다.
  - 각 디바이스에 대한 디바이스 위치, 소프트웨어 버전, 온보딩 방법 및 기타 세부 정보를 표시합니다.
  - 해당 디바이스를 소유하는 CDO 테넌트 페이지에서 디바이스를 관리할 수 있습니다.
  - 다른 지역의 CDO 테넌트에 로그인하고 해당 디바이스를 관리할 수 있는 링크를 제공합니다.
- 포털의 정보를 쉼표로 구분된 값(.csv) 파일로 내보내 분석하거나 액세스 권한이 없는 사용자에게 전송합니다.
- API 토큰을 사용하여 새 테넌트를 원활하게 추가할 수 있습니다.

- CDO에서 로그아웃하지 않고 포털 간 전환을 허용합니다.

자세한 내용은 *Cisco Defense Orchestrator를 사용하여 FTD 관리*의 "멀티 테넌트 포털 관리"를 참조하십시오.

클라우드 기반 보안 디바이스 커넥터에 대한 보안 이벤트 커넥터 지원

이제 Cisco Security Analytics and Logging(SAL SaaS) 고객은 보안 디바이스 커넥터가 Cisco Cloud에 설치된 경우 보안 이벤트 커넥터를 설치할 수 있습니다. Cisco Security Analytics and Logging을 구성하기 위해 더 이상 온프레미스 Secure Device Connector로 전환할 필요가 없습니다.

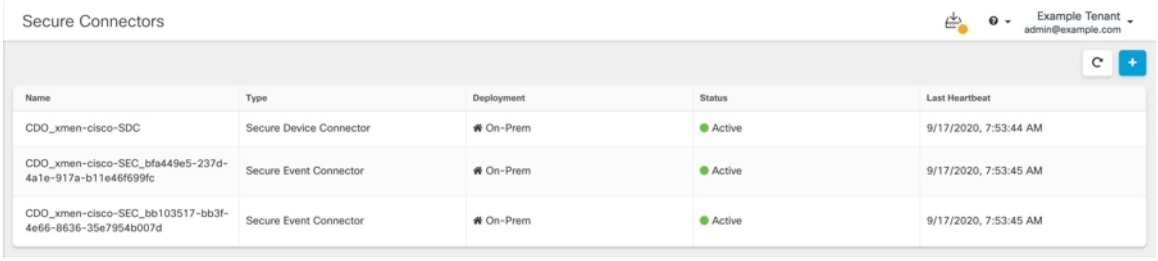
자세한 내용은 *Cisco Defense Orchestrator를 사용하여 Cisco Secure Firewall Cloud Native 관리*의 다음 항목을 참조하십시오.

- 보안 이벤트 커넥터 설치
- 클라우드 SDC가 있는 테넌트에 CDO 이미지를 사용하여 SEC 설치
- 클라우드 SDC가 있는 테넌트에 VM 이미지를 사용하여 SEC 설치

2020년 9월 17일

다중 보안 이벤트 커넥터 지원

SEC(Secure Event Connector)는 ASA 및 FTD에서 Cisco Cloud로 이벤트를 전달하므로 Cisco SAL SaaS(Security Analytics and Logging) 라이선싱에 따라 Event Logging(이벤트 로깅) 페이지에서 이벤트를 보고 Secure Cloud Analytics로 조사할 수 있습니다. 둘 이상의 SEC를 사용하면 서로 다른 위치에 설치하고 Cisco Cloud에 이벤트를 전송하는 작업을 배포할 수 있습니다.



테넌트에 추가 SEC를 설치하는 방법을 알아보려면 다음 문서를 참조하십시오.

- 온프레미스 SDC가 있는 테넌트에 CDO 이미지를 사용하여 여러 SEC 설치
- VM 이미지를 사용하여 여러 SEC 설치

자세한 내용은 *Cisco Defense Orchestrator를 사용하여 Cisco Secure Firewall Cloud Native 관리*의 "Cisco Security Analytics 및 로깅"을 참조하십시오.

2020년 8월

2020년 8월 20일

Firepower Management Center 지원

이제 CDO는 버전 6.4 이상을 실행하는 FMC(Firepower Management Center) 및 모든 매니지드 디바이스를 온보딩할 수 있습니다. FMC 지원은 FMC 온보딩, FMC에서 관리하는 디바이스 보기, FMC UI 교차 실행으로 제한됩니다.

CDO가 FMC 어플라이언스를 관리하는 방법을 검토하려면 *Cisco Defense Orchestrator*를 사용하여 *FMC* 관리를 참조하십시오.

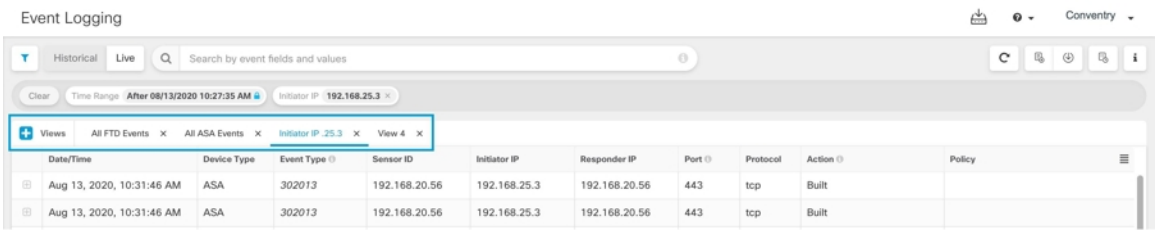
FMC 온보딩에 대한 자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FMC* 관리의 "FMC 온보딩"을 참조하십시오.

지원되는 FMC 하드웨어 및 소프트웨어 버전을 검토하려면 *Cisco Defense Orchestrator*를 사용하여 *FMC* 관리에서 "CDO의 소프트웨어 및 하드웨어 지원"을 참조하십시오.

사용자 지정 가능한 이벤트 필터

Cisco SAL SaaS(Security Analytics and Logging) 고객은 반복 사용을 위해 Event Logging(이벤트 로깅) 페이지에서 맞춤형 이벤트 필터를 생성하고 저장할 수 있습니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *Cisco Secure Firewall Cloud Native* 관리의 "맞춤형 이벤트 필터"를 참조하십시오.



이벤트 로깅 페이지의 향상된 검색 기능

Cisco Security Analytics and Logging(SAL SaaS) 고객은 이제 Event Logging(이벤트 로깅) 페이지의 검색 기능에 대한 다음과 같은 개선 사항을 활용할 수 있습니다.

- 요소 속성을 클릭하여 검색 필드에 추가합니다.

- Event Logging(이벤트 로깅) 페이지의 열을 끌어 놓아 원하는 방식으로 이벤트 정보를 확인합니다.
- Event Logging(이벤트 로깅) 페이지의 새로운 AND NOT 및 OR NOT 검색 연산자는 더욱 세분화된 이벤트 검색 기능을 제공합니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *Cisco Secure Firewall Cloud Native* 관리의 "이벤트 로깅에서 이벤트 검색 및 필터링"을 참조하십시오.

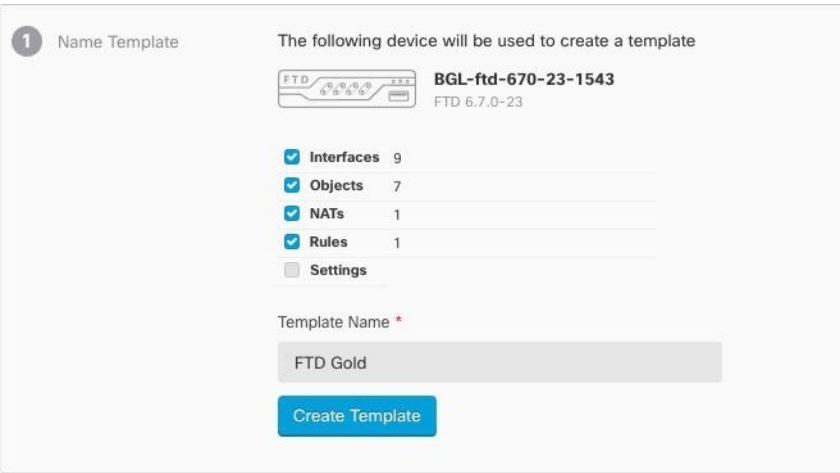
2020년 8월 13일

사용자 지정 충돌 탐지 폴링 간격

이제 디바이스 유형 또는 이전에 구성한 폴링 간격과 상관없이 디바이스별로 맞춤형 폴링 간격을 구성할 수 있습니다. 여기에는 디바이스 상태 또는 탐지된 대역 외 변경 사항에 대한 탐지가 포함됩니다. 자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "디바이스 변경에 대한 폴링 예약"을 참조하십시오.

맞춤형 **FTD** 템플릿

이제 온보딩된 FTD 디바이스 구성에서 하나 이상의 부분(액세스 규칙, NAT 규칙, 설정, 인터페이스 및 개체)을 선택하여 맞춤형 FTD 템플릿을 생성할 수 있습니다. 다른 FTD에 맞춤형 템플릿을 적용하면 포함된 부분을 기반으로 기존 구성이 유지, 업데이트 또는 제거됩니다. 그러나 CDO에서는 모든 부분을 선택하여 완전한 템플릿을 생성하고 다른 FTD에 적용할 수 있습니다. 자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "FTD 템플릿"을 참조하십시오.



2020년 7월

2020년 7월 30일

개체 재정의

CDO는 사용자가 지정한 장치에 사용하는 공유 네트워크 개체에 대한 대체 값을 제공할 수 있는 "개체 재정의"를 도입합니다. 필요한 경우 개별 디바이스의 정책을 바꾸지 않고도 디바이스 전반에 걸쳐 사용이 가능한 작은 공유 정책 집합을 생성할 수 있습니다. 개체 재정의를 사용하면 공유 정책 또는 규칙 집합에서 사용하는 일부 또는 모든 디바이스에서 재정의할 수 있는 개체를 생성할 수 있습니다.

개체를 재정의하려면 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "개체 재정의"를 참조하십시오.

향상된 네트워크 그룹 마법사

새 네트워크 개체를 즉시 생성하고 기존 개체를 수정할 수 있도록 네트워크 그룹 편집 마법사가 개선되었습니다. 또한 공유 네트워크 그룹이 정의된 디바이스에 디바이스별 추가 값을 추가할 수 있습니다.

네트워크 그룹 마법사의 개선 사항에 대한 자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "Firepower 네트워크 개체 또는 네트워크 그룹 생성 또는 수정" 및 ASA 네트워크 개체 및 네트워크 그룹 생성 또는 수정"을 참조하십시오.

2020년 7월 9일

RA VPN 및 이벤트 보기 사용자 지정

이제 RA VPN(Remote Access Virtual Private Network)에 대해 생성된 테이블과 라이브 및 기록 이벤트 보기를 모두 사용자 지정할 수 있습니다. 요구 사항에 가장 적합하고 포트폴리오에 중요한 방식으로 테이블을 구성하고 저장합니다.

사용자 지정과 관련된 자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 다음 섹션을 참조하십시오.

- 원격 액세스 VPN 모니터링 보기 사용자 지정
- CDO의 기록 이벤트 보기

2020년 7월 2일

SecureX

이제 CDO를 SecureX에 통합하여 디바이스, 정책 및 테넌트당 적용된 개체의 요약을 제공하여 보안 포트폴리오 전반에서 가시성 및 자동화를 강화할 수 있습니다. CDO 및 SecureX를 통합하는 방법에 대한 자세한 내용은 SecureX를 참조하십시오.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *Cisco Secure Firewall Cloud Native* 관리의 다음 항목을 참조하십시오.

- SecureX 및 CDO
- CDO에서 SecureX 연결

Cisco Security Analytics and Logging(SAL SaaS) 이벤트 다운로드

Event Logging(이벤트 로깅) 페이지에서 ASA 및 FTD 이벤트를 필터링한 후 이제 압축된 .CSV 파일로 결과를 다운로드할 수 있습니다.

- downloadable.CSV 파일에 추가하는 이벤트는 시간 범위로 정의됩니다.
- 단일 .CSV 파일은 최대 약 50GB의 압축 정보를 수용할 수 있습니다.
- 다운로드 가능한 파일의 생성은 병렬로 수행할 수 있습니다.
- 생성된 .CSV 파일은 Cisco Cloud에 저장되며 여기에서 직접 다운로드됩니다. 이러한 파일은 CDO/Secure Cloud Analytics 서버 리소스를 사용하지 않습니다.
- 완료된 downloadable.CSV 파일은 7일 동안 저장된 후 삭제됩니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *Cisco Secure Firewall Cloud Native* 관리의 "이벤트 다운로드"를 참조하십시오.

2020년 6월

2020년 6월 18일

Firepower Threat Defense 개요 보고서

이제 온보딩된 일부 또는 모든 Firepower Threat Defense(FTD) 디바이스에서 맞춤형 개요 보고서를 생성할 수 있습니다. 이 보고서는 암호화된 트래픽, 인터셉트된 위협, 탐지된 웹 범주 등의 운영 통계 모음을 표시합니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 다음 항목을참조하십시오.

- FTD 개요 보고서
- 보고서 관리

Cisco Security Analytics and Logging 개선 사항

ASA 시스템 로그 및 **NSEL** 이벤트 지원

ASA의 이벤트 로깅을 지원하도록 Cisco Security Analytics and Logging(Cisco Security Analytics 및 로깅)이 크게 확장되었습니다.

- **ASA** 로깅: SAL SaaS(Security Analytics and Logging)는 이제 관리 방법에 관계없이 모든 Cisco ASA 방화벽에서의 로깅을 지원합니다. 사용자는 ASA 로그를 시스템 로그 형식, NSEL(NetFlow Security Event Logs) 형식 또는 둘 다로 전송할 수 있습니다. 로깅 분석을 활성화하려는 고객은 상위 계층 SAL 라이선스에 필요한 텔레메트리를 제공하기 위해 NSEL 로그를 활성화해야 합니다.

  기존 FTD 로깅 외에도 CDO는 Cisco 보안 포트폴리오의 첫 번째 제품으로 Cisco의 전체 방화벽 플릿에 대한 로깅을 집계하고 통합합니다.

  자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리에서 다음 항목을 참조하십시오.

  - ASA 디바이스에 대한 Cisco Security Analytics and Logging
  - ASA 디바이스에 대한 Cisco Security Analytics and Logging 구현

- 장기 저장 및 다운로드: 사용자는 이제 SAL을 처음 주문할 때 또는 나중에 애드온으로 1년, 2년 또는 3년 동안 로그를 저장하도록 선택할 수 있습니다. 방화벽 로깅의 기본 보존 기간은 90일로 유지됩니다. 자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리의 "보안 애널리틱스 및 로깅 이벤트 스토리지"를 참조하십시오.
- 트래픽 분석: FTD 연결 레벨 로그 및 ASA(NSEL) 로그는 모두 SAL의 트래픽 분석을 통해 실행할 수 있으며, 관찰 및 알림은 SecureX 로그인을 사용하여 Secure Cloud Analytics에 교차 실행하여 검토할 수 있습니다. 시스템 로그를 기록하는 ASA 고객만 트래픽 분석을 활성화하기 위해 NSEL 로그로 전환해야 합니다. Logging Analytics and Detection 및 Total Network Analytics and Detection 라이선스를 취득한 고객은 추가 비용 없이 분석을 위해 Secure Cloud Analytics 포털을

프로비저닝하고 사용할 수 있습니다. Secure Cloud Analytics 탐지 항목에는 SAL 사용자가 Secure Cloud Analytics 핵심 기능의 일부로 사용할 수 있는 기타 탐지 항목 외에도 방화벽 로깅 데이터를 사용하여 특별히 활성화된 관찰 및 알림이 포함됩니다. 기존 기록 및 트러블슈팅 라이선스 보유자는 30일 동안 약정 없이 상위 라이선스의 탐지 기능을 테스트할 수 있습니다.

- 무료 평가판: 이 양식을 작성하여 모든 라이선스에 대해 약정 없는 30일 SAL 평가판을 시작할 수 있습니다. 이 로우 터치 평가판에는 클라우드로 데이터를 내보내는 데 필요한 최소 온프레미스 커넥터 집합만 필요합니다. 이 평가판을 사용하여 SAL 기능을 평가하고 프로덕션 환경을 지원하는 데 필요한 데이터 볼륨을 예측할 수 있습니다. 이는 SAL 라이선스에 대한 적절한 일일 볼륨을 구매하기 위한 선행 단계입니다. 이를 위해 SAL 평가판은 대부분의 사용자 볼륨에 대한 데이터를 조절하지 않습니다. 또한 예상 툴을 사용하면 SAL 일일 볼륨을 예측할 수 있습니다.

보안 분석 및 로깅을 위한 향상된 이벤트 모니터링

- 이제 CDO의 Event Logging(이벤트 로깅) 페이지에서 ASA 이벤트를 유형별로 필터링할 수 있습니다. 모든 시스템 로그 이벤트 또는 NSEL 이벤트를 개별적으로 또는 함께 볼 수 있습니다.
- 대부분의 ASA 시스템 로그 이벤트는 구문 분석되어 이벤트에 대한 자세한 정보를 제공합니다. 이 세부 정보는 Secure Cloud Analytics에서 이벤트를 분석하는 데 사용할 수 있습니다.
- 보려는 정보 열만 표시하고 나머지는 숨김으로써 Event Logging(이벤트 로깅) 페이지의 보기를 맞춤화할 수 있습니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리의 "이벤트 로깅에서 이벤트 필터링"을 참조하십시오.

2020년 6월 4일

원격 액세스 **VPN** 세션 모니터링 및 종료

이제 CDO를 사용하여 테넌트의 모든 ASA(Adaptive Security Appliance) 및 FTD(Firepower Threat Defense) VPN 헤드엔드 전반에서 라이브 AnyConnect Remote Access VPN 세션을 모니터링할 수 있습니다. 총 활성 VPN 세션 수, 현재 연결된 사용자 및 세션 수, 수신 및 전송된 데이터의 양에 대한 정보를 수집합니다.

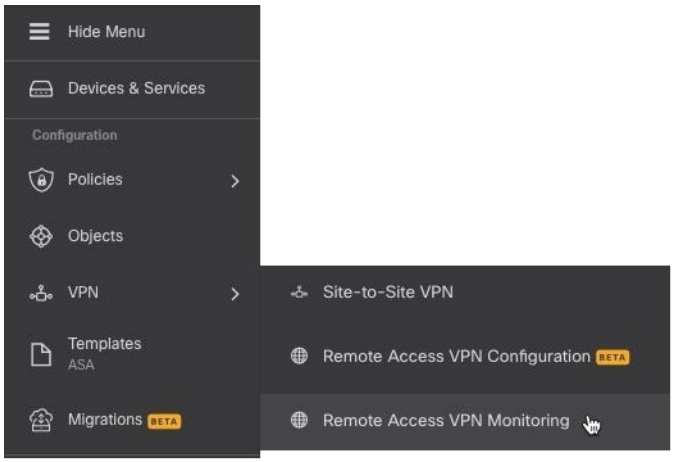
테넌트에서 각 RA VPN 헤드엔드의 성능을 보고, 헤드엔드별로 세션을 필터링하고, VPN 모니터링 테이블에서 보려는 세션 속성을 선택할 수 있습니다. 또한 하나 이상의 디바이스의 RA VPN 세션을 쉼표로 구분된 값(.csv) 파일로 내보낼 수 있습니다. 자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *Cisco Secure Firewall Cloud Native* 관리의 "CSV 파일로 RA VPN 세션 내보내기"를 참고하십시오.

ASA에서 단일 사용자의 모든 활성 RA VPN 세션을 종료하고 ASA에서 모든 사용자의 모든 활성 RA VPN 세션을 종료할 수 있습니다.

자세한 내용은 다음 주제를 참고하십시오.

- *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리의 ASA에서 활성 RA VPN 세션 연결 끊기
- *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 FTD에서 활성 RA VPN 세션 연결 끊기

VPN > Remote Access VPN Monitoring(원격 액세스 **VPN** 모니터링**)**을 클릭하여 탐색 모음에서 Remote Access VPN Monitoring(원격 액세스 VPN 모니터링) 화면을 엽니다.



AWS Virtual Private Cloud Management - 무료 평가판

CDO에서 90일 동안 무료로 AWS VPC를 관리해 보십시오. CDO에서 Devices & Services(디바이스 및 서비스) 페이지를 열고 AWS VPC를 온보딩하여 시작합니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *AWS* 관리의 "AWS VPC 온보딩"을 참조하십시오.

새로운 기능 타일

이제 CDO 랜딩 페이지에 최신 기능과 CDO가 해당 기능을 구현한 시기를 보여주는 새로운 기능 타일이 있습니다. 관심 있는 기능이 있는 경우 기능의 제목을 클릭하여 해당 기능에 대한 설명서를 읽어보십시오.

2020년 5월

2020년 5월 20일

새 **API** 전용 사용자

이제 CDO를 통해 슈퍼 관리자는 CDO REST API 호출 시 CDO에 인증하기 위한 API 토큰을 생성하는 데 사용할 수 있는 "API 전용 사용자"를 생성할 수 있습니다. 이 사용자 어카운트 및 해당 API 토큰은 원래 슈퍼 관리자가 조직을 떠난 후에도 계속 작동합니다.

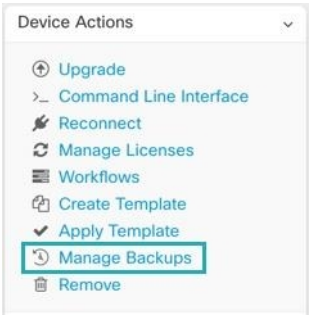
자세한 내용은 Cisco Defense Orchestrator를 사용하여 FTD 관리의 "API 전용 사용자 생성"을 참조하십시오.

2020년 5월 7일

Firepower Threat Defense 디바이스 백업

이제 CDO를 사용하여 FTD(Firepower Threat Defense)의 시스템 구성을 백업할 수 있습니다. CDO를 사용하여 다음을 수행할 수 있습니다.

- 온디맨드 방식으로 디바이스를 백업합니다.
- 매일부터 매달 선택한 시간에 주기로 반복 백업을 예약합니다.
- 백업을 다운로드하고 FDM(Firepower Device Manager)을 사용하여 복원합니다.



자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "FTD 백업"을 참조하십시오.

2020년 4월

2020년 4월 16일

Firepower Threat Defense 6.6.0을 실행하는 디바이스에 대한 **CDO** 지원

이제 CDO에서 FTD 6.6.0 디바이스를 관리합니다. 다음은 CDO가 제공하는 새로운 지원 측면입니다.

- Firepower Threat Defense(FTD) 6.6.0을 실행하는 디바이스 온보딩
- FTD 6.4.x 이상 디바이스를 FTD 6.6.0 디바이스로 업그레이드 디바이스는 개별 FTD 또는 고가용성 쌍으로 구성된 FTD일 수 있습니다. 다음 주의 사항은 업그레이드 지원에 적용됩니다.
  - Firepower 4100 및 Firepower 9300 디바이스에 대한 업그레이드는 현재 지원되지 않습니다.
  - 고객은 CDO의 업그레이드 페이지에 있는 드롭다운을 사용하여 FTD 6.6.0으로 업그레이드할 수 있습니다.
- CDO는 FTD 기능에 대한 지원을 지속적으로 개발하고 새로운 기능 지원이 준비되는 대로 릴리스합니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "Firepower Threat Defense 지원 세부 사항"을 참조하십시오.

2020년 4월 9일

Firepower Threat Defense 명령줄 인터페이스

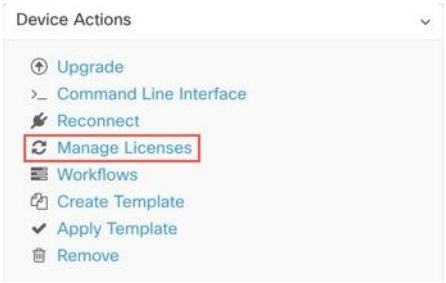
이제 CDO에서 직접 FTD 디바이스에 CLI 요청을 실행할 수 있습니다.

자세한 내용은 *Cisco Defense Orchestrator*로 *FTD* 관리의 "CDO 명령줄 인터페이스 사용"을 참조하십시오.

2020년 4월 2일

Firepower Threat Defense 디바이스용 라이선스 관리 개선

이제 FTD 디바이스 라이선스 정보 보기, 라이선스 활성화 및 비활성화, 라이선스 새로 고침을 모두 Devices & Services(디바이스 및 서비스) 페이지의 Device Actions(디바이스 작업) 창에서 단일 버튼으로 관리할 수 있습니다.



2020년 3월

2020년 3월 26일

FTD 보안 데이터베이스 업데이트

CDO를 사용하면 FTD 디바이스를 온보딩할 때 보안 데이터베이스를 즉시 업데이트하는 동시에 향후 업데이트를 예약할 수 있습니다. 이 기능은 SRU, SI(보안 인텔리전스), VDB(취약성) 및 지리위치 데이터베이스를 업데이트합니다. 향후 업데이트는 온보딩 프로세스의 일부로만 예약할 수 있습니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "FTD 보안 데이터베이스 업데이트"를 참조하십시오.

FTD 서비스 개체의 포트 범위 지원

이제 CDO는 다양한 포트 번호를 포함하는 서비스 개체(FTD에서는 포트 개체라고도 함) 생성을 지원합니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "Firepower 서비스 개체 생성 및 편집"을 참조하십시오.

2020년 3월 24일

Cisco Secure 로그인 도메인 마이그레이션

2020년 3월 24일 화요일 오후 5시(태평양 일광 절약 시간)에 Cisco Security Single Sign-on 솔루션의 공식 도메인이 https://security.cisco.com에서 https://sign-on.security.cisco.com(으)로 이동되었습니다.

저장된 링크를 업데이트하고 비밀번호 관리자가 새 URL을 참조하도록 업데이트하는 것이 좋습니다.

이렇게 하면 짧은 기간 동안 CDO에 대한 액세스가 제한되지만, 로컬 디바이스 관리자 또는 SSH 연결을 사용하여 업데이트를 수행하는 기능은 제한되지 않습니다.

문제가 발생하는 경우 기술 지원을 제공할 수 있는 Cisco TAC에 문의하십시오.

2020년 3월 12일

FTD 규칙 집합

CDO에 Firepower Threat Defense 디바이스용 규칙 집합이 도입되었습니다. 규칙 집합은 여러 FTD 디바이스에서 공유할 수 있는 액세스 제어 규칙의 모음입니다. 규칙 집합의 규칙에 대한 모든 변경 사항은 해당 규칙 집합을 사용하는 다른 FTD 디바이스에 영향을 미칩니다. FTD 정책은 디바이스별(로컬) 규칙과 공유(규칙 집합) 규칙을 모두 포함할 수 있습니다. FTD 디바이스의 기존 규칙에서 규칙 집합을 생성할 수도 있습니다.

이 기능은 현재 Firepower Threat Defense 6.5 이상 릴리스를 실행하는 디바이스에서 사용할 수 있습니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "FTD 규칙 집합"을 참조하십시오.

2020년 3월 5일

FTD 정책 내에서 또는 다른 **FTD** 정책으로 규칙 복사 또는 이동

이제 한 FTD의 정책에서 다른 FTD의 정책으로 규칙을 복사하거나 이동할 수 있습니다. 또한 규칙이 네트워크 트래픽을 평가하는 순서를 세부적으로 조정할 수 있도록 FTD 정책 내에서 규칙을 더 쉽게 이동할 수 있습니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "FTD 액세스 제어 규칙 복사" 및 "FTD 액세스 제어 규칙 이동"을 참조하십시오.

FTD 버전 **6.5** 이상으로의 **AnyConnect** 소프트웨어 패키지 업로드

이제 CDO의 원격 액세스 VPN 마법사를 사용하여 원격 서버에서 FTD 6.5 이상을 실행하는 FTD(Firepower Threat Defense) 디바이스로 AnyConnect 패키지를 업로드할 수 있습니다. 원격 서버가 HTTP 또는 HTTPS 프로토콜을 지원하는지 확인합니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "FTD 버전 6.5 이상을 실행하는 FTD 디바이스에 AnyConnect 소프트웨어 패키지 업로드"를 참조하십시오.

2020년 3월 3일

CDO 인터페이스의 용어 업데이트

디바이스를 관리하려면 CDO(Cisco Defense Orchestrator)의 자체 데이터베이스에 디바이스 구성 복사본이 저장되어 있어야 합니다. CDO는 구성을 "읽을 때" 디바이스에 저장된 구성의 복사본을 만들어 CDO의 데이터베이스에 저장합니다. 읽기 작업을 수행할 때 수행 중인 작업을 더 잘 설명하기 위해 일부 인터페이스 옵션의 이름을 변경했습니다.

새로운 용어는 다음과 같습니다.

- 변경 사항 확인. 디바이스의 구성 상태가 Synced(동기화됨)인 경우 Check for Changes(변경 사항 확인) 링크를 사용할 수 있습니다. Check for Changes(변경 사항 확인)를 클릭하면 CDO가 디바이스 구성의 복사본을 디바이스 구성의 복사본과 비교하도록 지시합니다. 차이가 있는 경우 CDO는 디바이스에 저장된 복사본으로 디바이스 구성의 복사본을 즉시 덮어씁니다.
- 변경 사항 취소. 디바이스의 구성이 Not Synced(동기화되지 않음)인 경우 Discard Changes(변경 사항 취소)를 클릭하면 CDO가 디바이스 구성 복사본에 적용한 모든 변경 사항이 삭제되고 디바이스에 있는 구성의 복사본으로 덮어씁니다.
- 검토 없이 수락.이 작업은 CDO의 디바이스 구성 복사본을 디바이스에 저장된 구성의 복사본으로 덮어씁니다. CDO는 작업을 확인하라는 메시지를 표시하지 않습니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "구성 변경 사항 읽기, 삭제, 확인 및 구축"을 참조하십시오.

2020년 2월

2020년 2월 6일

Firepower 1010에 대한 스위치 포트 모드 지원

이제 CDO는 Firepower 1010 디바이스에 대한 스위치 포트 모드 기능을 완벽하게 지원합니다.

구성 지침 및 제한 사항에 대한 자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "FTD에 대한 스위치 포트 모드 인터페이스" 및 "스위치 포트 모드에 대한 FTD VLAN 구성"을 참조하십시오.

2020년 1월

2020년 1월 22일

사이트 대 사이트 연결을 위한 동적 피어 지원

이제 피어의 VPN 인터페이스 중 하나에 동적 IP 주소가 있는 경우 두 피어 간에 사이트 간 VPN 터널을 구성할 수 있습니다. 이 동적 피어는 매니지드 FTD 디바이스 또는 엑스트라넷 디바이스일 수 있습니다.

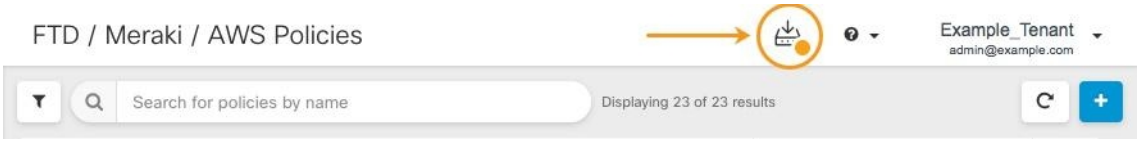
자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "동적으로 주소가 지정된 피어를 사용하여 사이트 간 VPN 연결 구성"을 참조하십시오.

2020년 1월 16일

향상된 구축 경험

CDO는 구축 워크플로를 개선했습니다. 이제 추가 구축 아이콘이 CDO 전체에서 표시됩니다. 더 이상 구성 변경 사항을 구축하기 위해 Devices & Services(디바이스 및 서비스) 페이지로 돌아갈 필요가 없습니다.

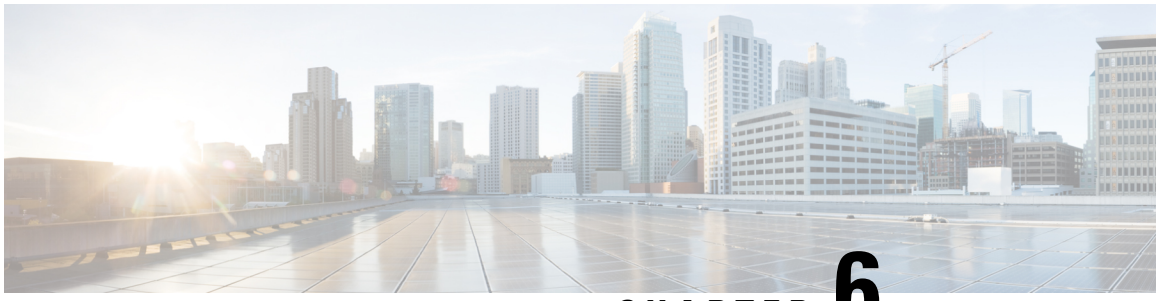
구축 아이콘에 주황색 점이 포함되어 있으면 CDO로 관리하는 디바이스 중 하나 이상(구축 준비가 된 디바이스)이 하나 이상 변경되었음을 나타냅니다.



자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축"을 참조하십시오.

대량 작업 취소

이제 여러 디바이스에서 수행한 활성 대량 작업을 취소할 수 있습니다. 예를 들어 4개의 매니지드 디바이스를 다시 연결하려고 시도했는데 그 중 3개의 디바이스가 성공적으로 다시 연결되었지만 네 번째 디바이스는 다시 연결에 성공하거나 실패하지 않았습니다. 이제 **Jobs(**작업**)** 페이지로 이동하여 진행 중인 대량 작업을 찾은 다음 Cancel(취소)을 클릭하여 작업을 중지할 수 있습니다.



CHAPTER 6

2019의 주요 기능

2019년 11월

2019년 11월

Firepower Threat Defense 6.5.0을 실행하는 디바이스에 대한 **CDO** 지원

이제 CDO에서 FTD 6.5.0 디바이스를 관리합니다. 다음은 CDO가 제공하는 지원 측면입니다.

- Firepower Threat Defense(FTD) 6.5.0을 실행하는 디바이스 온보딩
- Firepower 4100 및 Firepower 9300과 같은 추가 Firepower 시리즈 디바이스를 지원합니다.
- Microsoft Azure에서 가상 FTD 인스턴스를 지원합니다. 지원되는 디바이스의 전체 목록은 Cisco Defense Orchestrator를 사용하여 FTD 관리의 "Firepower Threat Defense 지원 세부 사항"을 참조하십시오.
- 디바이스는 개별 FTD 또는 고가용성 쌍으로 구성된 FTD일 수 있습니다. 자세한 내용은 Cisco Defense Orchestrator를 사용하여 FTD 관리의 "Firepower 소프트웨어 업그레이드 경로"를 참조하십시오. 다음 주의 사항은 업그레이드 지원에 적용됩니다.
  - 디바이스가 관리용 데이터 인터페이스를 사용하는 경우 6.5.0을 실행하는 FTD에 대해서는 HA 쌍 업그레이드가 지원되지 않습니다.
  - Firepower 4100 및 Firepower 9300 디바이스의 업그레이드는 현재 지원되지 않습니다.

- 고객은 CDO의 업그레이드 페이지에 있는 드롭다운을 사용하여 FTD 6.5.0으로 업그레이드할 수 있습니다. 6.5 이미지 다운로드를 위해 디바이스에 제공되는 링크는 HTTP입니다. 이는 다운로드가 HTTPS를 통해 수행된 경우보다 이미지 다운로드 시간이 약간 더 길어질 수 있음을 의미합니다. 또한 FTD의 아웃바운드 HTTP 트래픽이 차단되면 이미지 다운로드가 실패합니다.

- Firepower 1010에 FTD 6.5.0이 설치되면 일반 방화벽 인터페이스 또는 레이어 2 하드웨어 스위치 포트로 실행되도록 인터페이스를 구성할 수 있습니다. 현재 CDO의 스위치 모드 지원은 읽기 전용입니다. 스위치 포트 모드에 대한 인터페이스를 생성하거나 수정하려면 FDM 콘솔을 사용합니다. CDO는 Firepower 1010s에서 스위치 포트 모드에 대한 지원을 계속 개발하고 있으며, 완전한 지원이 제공되는 경우 새로운 기능에서 발표할 예정입니다.
- 등록 토큰을 사용하여 FTD 6.5.0 디바이스를 온보딩하는 경우, 보안 이벤트 커넥터를 사용하지 않고 연결 이벤트, 파일 및 악성코드 이벤트, 침입 이벤트를 Cisco Cloud에 직접 전송할 수 있습니다. Cisco Defense Orchestrator를 사용하여 FTD 관리의 "Cisco Security Analytics 및 로깅 구현"을 참조하십시오.
- FTD 6.4.x 기능에 대한 지속적인 지원. CDO는 FTD 6.5 기능에 대한 지원을 지속적으로 개발하고 있으며 준비가 완료되는 대로 지원을 릴리스할 예정입니다.

CDO에서 지원하는 FTD 기능에 대한 자세한 내용은 Cisco Defense Orchestrator를 사용하여 FTD 관리를 참조하십시오.

사이트 간 **VPN** 연결에 대한 **IKEv1** 지원

이제 CDO에서 IKEv1(Internet Key Exchange 버전 1)을 사용하여 사이트 간 VPN 터널을 생성할 수 있습니다. 이는 IKEv2(Internet Key Exchange 버전 2)를 지원하지 않는 레거시 방화벽에서 사이트 간 VPN을 구성하는 데 도움이 됩니다. IKE(Internet Key Exchange)는 IPsec 피어를 인증하고, IPsec 암호화 키를 협상 및 배포하고, IPsec SA(보안 연계)를 자동으로 설정하는 데 사용되는 키 관리 프로토콜입니다.

자세한 내용은 Cisco Defense Orchestrator를 사용하여 FTD 관리의 "사이트 간 가상 프라이빗 네트워크"를 참조하십시오.

Firepower Threat Defense 템플릿 개선

이제 CDO에서 FTD 템플릿의 일부 측면을 매개변수화하여 템플릿을 추가로 사용자 지정할 수 있습니다. 자세한 내용은 Cisco Defense Orchestrator를 사용하여 FTD 관리의 "FTD 템플릿 구성"을 참조하십시오.

스마트 라이선스 관리

이제 CDO 내에서 Firepower Threat Defense 디바이스용 Cisco 스마트 라이선스를 관리할 수 있습니다. 스마트 라이선싱은 워크플로우에 편리하게 내장되어 있으며 CDO 인터페이스에서 쉽게 액세스할 수 있습니다. 이제 CDO 내에서 다음 Cisco 스마트 라이선싱 작업을 수행할 수 있습니다.

- 등록 토큰을 사용하여 FTD 디바이스를 온보딩하는 동안 스마트 라이선스 적용
- 디바이스에 적용된 라이선스 보기

- Cisco Smart Software Manager로 라이선스 등록
- 디바이스에 대해 서로 다른 라이선스 유형 활성화 및 비활성화

자세한 내용은 Cisco Defense Orchestrator를 사용하여 FTD 관리의 "등록 토큰을 사용하여 Firepower Threat Defense 디바이스 온보딩" 및 "온보딩된 FTD 스마트 라이선싱"을 참조하십시오.

2019년 10월

2019년 10월

Amazon Web Services 지원

이제 CDO가 AWS VPC를 관리합니다!

AWS(Amazon Web Services) VPC(Virtual Private Cloud)는 AWS 어카운트와 연결된 가상 프라이빗 클라우드를 사용자에게 제공하는 상업용 클라우드 컴퓨팅 서비스입니다. 이 네트워크는 자체 데이터 센터에서 운영하는 기존 네트워크와 매우 유사하며 AWS의 확장 가능한 인프라를 사용한다는 이점이 있습니다.

CDO는 개체 및 규칙의 문제를 식별하고 해결 방법을 제공하여 AWS VPC를 최적화하도록 도와줍니다. CDO 사용:

- FTD 또는 ASA 디바이스와 함께 AWS VPC 환경을 관리합니다.
- AWS VPC와 연결된 모든 보안 그룹 규칙을 동시에 관리합니다.
- FTD 및 ASA 디바이스와 같이 지원되는 다른 플랫폼에서 호환되는 개체로 보안 그룹 규칙을 생성하고 맞춤화합니다.
- AWS VPC 사이트 간 VPN 연결을 봅니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *AWS* 관리를 참조하십시오.

CDO를 사용하여 **ASA**를 **FTD** 디바이스로 마이그레이션

CDO는 ASA(Adaptive Security Appliance)를 FTD(Firepower Threat Defense) 디바이스로 마이그레이션하는 데 도움이 됩니다. CDO는 ASA에서 실행 중인 구성의 다음 요소를 FTD 템플릿으로 마이그레이션하는 데 도움이 되는 마법사를 제공합니다.

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

- 서비스 개체 및 서비스 그룹 개체

구성을 실행하는 ASA의 이러한 요소가 FTD 템플릿으로 마이그레이션되면 CDO에서 관리하는 새 FTD 디바이스에 FTD 템플릿을 적용할 수 있습니다. FTD 디바이스는 템플릿에 정의된 구성을 채택하므로 이제 FTD가 ASA에서 실행 중인 구성의 일부 측면으로 구성됩니다.

CDO를 사용하여 ASA를 FTD로 마이그레이션하는 프로세스에 대한 자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리의 "ASA를 FTD로 마이그레이션 워크플로우"를 참조하십시오.

Cisco, Cisco Secure Sign-on 및 **Duo Multi-Factor Authentication**을 사용하는 새로운 **SSO(Single Sign-On)** 솔루션 소개

CDO는 이 새로운 솔루션을 채택하고 고객 테넌트를 Cisco Secure Sign-on IdP(Identity Provider) 및 Duo Security 다단계 인증자로 변환합니다.

Cisco Secure Sign-On을 사용하면 다음과 같은 이점을 얻을 수 있습니다.

- 강력하고 탄력적인 **ID**: AICPA SOC 2, CSA-Star 및 ISO 27001을 포함하여 가장 높은 업계 표준을 충족하는 보안입니다. 또한 고객을 위해 분리된 FedRAMP 및 HIPAA 환경을 지원합니다.
- **Duo MFA(Multi-Factor Authentication)**: Cisco Secure Sign-On과 통합된 Duo MFA는 적응형, 계층화된, 간소화된 인증을 의미합니다. 푸시 알림 한 번, 탭 한 번으로 즉시 액세스
- 원활한 워크플로우를 위한 **SSO(Single Sign-In)**: 단일 사용자 이름과 비밀번호를 입력하면 모든 디바이스에서 모든 애플리케이션에 액세스하는 동시에 워크플로우 전체에서 상황을 유지할 수 있습니다.
- 맞춤형 환경: Cisco Secure Sign-On 대시보드에서 업무용 앱을 원하는 방식으로 정렬할 수 있습니다. 탭과 검색 창을 사용하면 정리할 수 있습니다.

Note

- 자체 SSO(Single Sign-On) ID 제공자를 사용하여 CDO에 로그인하는 경우 Cisco Secure Sign-On 및 Duo로의 전환이 영향을 미치지 않습니다. 고유한 로그인 솔루션을 계속 사용합니다.
- CDO 무료 평가판을 사용 중인 경우 이 전환이 영향을 미칩니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *AWS* 관리의 "Cisco Secure Sign-On ID 제공자로 마이그레이션"을 참조하십시오.

Cisco Security Analytics and Logging(Secure Cloud Analytics와의 통합 포함**)**

Cisco Security Analytics and Logging은 네트워크 가시성을 개선하여 실시간으로 위협을 신속하게 탐지하고 대규모로 자신 있게 인시던트를 치료할 수 있습니다.

Cisco Security Analytics and Logging을 사용하면 모든 FTD(Firepower Threat Defense) 디바이스에서 연결, 침입, 파일, 악성코드 및 보안 인텔리전스 이벤트를 캡처하여 CDO의 한 곳에서 볼 수 있습니다.

이벤트는 Cisco Cloud에 저장되며 CDO의 Event Logging(이벤트 로깅) 페이지에서 볼 수 있습니다. 이 페이지에서 이벤트를 필터링하고 검토하여 네트워크에서 트리거되는 보안 규칙을 명확하게 파악할 수 있습니다. Logging and Troubleshooting(기록 및 문제 해결) 패키지는 이러한 기능을 제공합니다.

방화벽 분석 및 모니터링 패키지를 통해 시스템은 FTD 이벤트에 Secure Cloud Analytics 동적 엔티티 모델링을 적용하고 행동 모델링 분석을 사용하여 Secure Cloud Analytics 관찰 및 알림을 생성할 수 있습니다. 전체 네트워크 분석 및 모니터링 패키지를 구입하는 경우 시스템은 FTD 이벤트와 네트워크 트래픽 모두에 동적 엔터티 모델링을 적용하고 관찰 및 알림을 생성합니다. Cisco SSO(Single Sign-On, 단일 인증)를 사용하여 CDO에서 사용자에게 프로비저닝된 Secure Cloud Analytics 포털로 교차 실행할 수 있습니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "Cisco Security Analytics and Logging"을 참조하십시오.

2019년 9월

2019년 9월

등록 토큰을 사용하여 **Firepower Threat Defense** 디바이스 온보딩

이제 IP 주소, 사용자 이름 및 비밀번호를 사용하는 대신 등록 토큰을 사용하여 FTD 디바이스를 온보딩할 수 있습니다. 이는 DHCP를 사용하여 FTD에 IP 주소가 할당된 경우 특히 유용합니다. 어떤 이유로 해당 IP 주소가 변경되어도 FTD는 CDO에 연결된 상태로 유지됩니다. 또한 FTD는 로컬 영역 네트워크에 주소를 가질 수 있으며, 외부 네트워크에 액세스할 수 있는 한 이 방법을 사용하여 CDO에 온보딩할 수 있습니다.

이 온보딩 방법은 현재 FTD 6.4 릴리스 및 defenseorchestrator.cisco.com에 연결하는 고객에게 제공됩니다. defenseorchestrator.cisco.eu에 연결하는 고객은 아직 사용할 수 없습니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "등록 키로 FTD 온보딩"을 참조하십시오.

2019년 8월

2019년 8월

Cisco Security Analytics and Logging

Cisco Security Analytics and Logging은 네트워크 가시성을 개선하여 실시간으로 위협을 신속하게 탐지하고 대규모로 자신 있게 인시던트를 치료할 수 있습니다.

Firepower Threat Defense를 위한 원격 액세스 VPN 지원

RA(Remote Access) VPN을 통해 개인은 지원되는 노트북 컴퓨터, 데스크톱 및 모바일 디바이스를 사용하여 네트워크에 대한 보안 연결을 설정할 수 있습니다. CDO는 온보딩한 FTD(Firepower Threat Defense) 디바이스에서 RA VPN을 설정할 수 있는 직관적인 사용자 인터페이스를 제공합니다.

AnyConnect는 RA VPN 연결을 제공하는 엔드포인트 디바이스에서만 지원되는 클라이언트입니다.

CDO는 FTD 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 및 IPv6 주소 지정
- 여러 FTD 디바이스에서 공유 RA VPN 구성

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "원격 액세스 가상 사설 네트워크"를 참조하십시오.

Firepower Threat Defense 고가용성 이미지 업그레이드 지원

이제 CDO에서 FTD HA 쌍을 업그레이드할 수 있습니다. 장애 조치 쌍을 업그레이드할 때 CDO는 원하는 업그레이드 이미지를 두 디바이스에 모두 복사합니다. CDO는 기본 디바이스가 활성 모드가 아닌 경우 임시로 해당 모드를 이동한 다음 보조 디바이스를 업그레이드합니다. 보조 디바이스가 성공적으로 업그레이드되면 기본 디바이스가 업그레이드됩니다. 장애 조치 쌍은 네트워크 중단을 최소화하기 위해 디바이스를 한 번에 하나씩 업그레이드합니다.

장애 조치 쌍을 업그레이드하려면 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "FTD 고가용성 쌍 업그레이드"를 참조하십시오.

Firepower Threat Defense 디바이스를 위한 사이트 간 VPN

이제 Firepower Threat Defense 디바이스를 위한 사이트 간 VPN이 정식 출시되었습니다!

CDO를 사용하면 서로 다른 지리적 위치에 있는 두 사이트 간에 보안 연결을 설정할 수 있습니다. 이러한 피어는 IPv4와 IPv6 주소를 사용하여 내부 주소와 외부 주소를 함께 포함할 수 있습니다. Site-to-Site 터널은 IPsec(Internet Protocol Security) 프로토콜 제품군 및 인터넷 키 교환 버전 2(IKEv2)를 사용하여 구축됩니다. VPN 연결이 설정되면 로컬 게이트웨이의 뒤에 있는 호스트는 보안 VPN 터널을 통해 원격 게이트의 뒤에 있는 호스트와 연결할 수 있습니다. CDO에 온보딩된 디바이스에 대해 다음 시나리오에서 사이트 간 IPsec 연결을 생성할 수 있습니다.

- 두 매니지드 디바이스 간
- 매니지드 디바이스와 다른 Cisco 피어 간
- 매니지드 디바이스와 서드파티 피어 간

Firepower Threat Defense 고가용성 지원

CDO는 Firepower Threat Defense 방화벽에 대한 고가용성(HA) 지원을 일반 공급합니다! 이제 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.

독립형 FTD 디바이스에 지원되는 대부분의 기능은 HA에 대해 구성된 디바이스도 지원합니다. 자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "FTD 고가용성"을 참조하십시오.

제공 예정... FTD HA 업그레이드 지원 현재 HA 쌍을 업그레이드해야 하는 경우에는 액티브 디바이스의 FDM 콘솔을 통해 업그레이드를 실행해야 합니다.

2019년 7월

2019년 7월

ASA 디바이스에 대한 시간 범위 개체

이제 시간 범위 개체를 사용하여 네트워크 정책의 규칙을 맞춤화할 수 있습니다. 이러한 개체를 사용하면 일회성 또는 반복 규칙을 실행하고 네트워크에서 트래픽을 처리하는 방법을 맞춤화할 수 있습니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리의 "ASA 시간 범위 개체"를 참조하십시오.

Firepower Threat Defense 지원

CDO는 일반적으로 사용 가능한 Firepower Threat Defense 방화벽에 대한 지원을 제공합니다!

CDO는 Firepower Threat Defense 디바이스에 대한 간소화된 관리 인터페이스 및 클라우드 액세스를 원하는 방화벽 관리자를 위해 설계되었습니다. FDM(Firepower Device Manager) 관리자는 FDM 인터페이스와 CDO 인터페이스 간에 많은 유사성을 확인할 수 있습니다. 관리자 간에 가능한 한 일관성을 유지하기 위해 CDO를 구축했습니다.

이제 CDO는 ASA 5508-x, ASA 5515-x, ASA 5525-x, ASA 5545-x, ASA 5555-x, FTD 2100 시리즈 디바이스, FTD 1000 시리즈 디바이스 또는 가상 FTD 디바이스에 설치되었을 때 FTD 버전 6.4.0 이상을 실행하는 Firepower Threat Defense(FTD) 디바이스를 관리할 수 있습니다.

CDO를 사용하여 물리적 또는 가상 FTD(Firepower Threat Defense) 디바이스의 다음 측면을 관리합니다.

- 디바이스 관리
- 디바이스 업그레이드
- 인터페이스 관리

- 라우팅
- 보안 정책
- 정책 및 구성 일관성 승격
- 변경 추적
- 네트워크 모니터링

Firepower 1000 Series 및 Virtual FTD를 포함하여 모든 CDO FTD PID는 CCW에서 주문할 수 있습니다. PID는 플랫폼에 따라 다르지만 ASA 및 FTD에 공통적으로 적용됩니다. 자세한 내용은 Salesconnect의 주문 가이드를 참조하십시오.

지원되는 기능에 대한 자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리를 참조하십시오.

Meraki MX 지원

이제 CDO에서 Meraki MX 방화벽 정책을 관리합니다!

Meraki MX는 분산형 구축을 위해 설계된 엔터프라이즈 보안 및 소프트웨어 정의 광역 네트워크(SD-WAN) 차세대 방화벽 어플라이언스입니다. 이제 Cisco Defense Orchestrator를 사용하여 Meraki MX 디바이스에서 레이어 3 네트워크 규칙을 관리할 수 있습니다.

CDO는 개체 및 정책의 문제를 식별하고 해결 방법을 제공하여 Meraki 환경을 최적화하도록 도와줍니다. 이는 디바이스 및 템플릿 모두에 연결된 정책에 적용됩니다.

CDO를 사용하여 다음을 수행합니다.

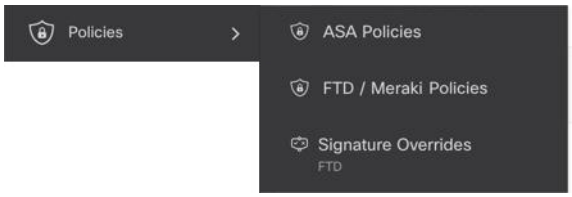
- 하나 이상의 Meraki 디바이스에서 정책을 동시에 관리합니다.
- 모든 환경에서 FTD 및 ASA 디바이스와 함께 Meraki 정책 또는 템플릿을 모니터링하고 관리합니다.
- Meraki 템플릿을 사용하여 여러 네트워크를 관리합니다.
- FTD 및 ASA 디바이스와 같이 지원되는 다른 플랫폼에서 호환되는 개체로 액세스 규칙을 맞춤화합니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *Meraki* 관리를 참조하십시오.

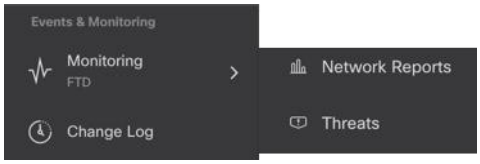
업데이트된 **GUI** 탐색

CDO의 UI 탐색이 더 쉬워졌습니다.

이제 내비게이션 바의 정책 메뉴에서 디바이스 또는 기능별로 그룹화된 정책을 안내합니다. Cisco에서는 현재 테넌트에 있는 정책에 연결하는 데 필요한 메뉴 경로만 노출합니다.



FTD의 모든 모니터링 기능은 내비게이션 바의 **Events & Monitoring(**이벤트 및 모니터링**)** 영역에서 그룹화됩니다. Monitoring(모니터링) 메뉴에는 **Network Reports(**네트워크 보고서**)** 및 **Threats(**위협**)**가 표시됩니다.



2019년 5월

2019년 5월

디바이스 연결 문제 해결

이 툴을 사용하면 SDC(Secure Device Connector)와 디바이스 간의 연결 문제를 테스트하거나 트러블슈팅할 수 있습니다. 디바이스가 온보딩에 실패하거나 온보딩 전에 CDO가 디바이스에 연결할 수 있는지 확인하려는 경우 이 연결을 테스트할 수 있습니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "SDC를 사용하여 보안 디바이스 커넥터 문제 해결"을 참조하십시오.

2019년 4월

2019년 4월

CDO 사용자 환경을 개선하는 데 도움이 될 수 있습니다.

저희는 귀하의 CDO 사용자 경험에 대해 알고자 하며, 이제 저희에게 쉽게 알려줄 수 있습니다. CDO 포털에서 나가지 않고도 피드백을 제공할 수 있도록 Help(도움말) 메뉴에 **Provide Feedback(**피드백 제공**)** 버튼을 추가했습니다. 마음에 드는 점과 개선할 점을 알려주십시오.

피드백을 남길 때 귀사에서 귀하의 역할을 알려주십시오. 네트워크 운영 센터, 보안 운영 센터에 있습니까? 아니면 모든 IT 센터에 있습니까? 완료하려는 작업을 알려주십시오. 보안 정책을 수정하거나 변경 로그에서 항목을 찾으십니까?

피드백을 남기는 방법은 다음과 같습니다.

단계 **1** CDO에 로그인합니다.

단계 **2** 테넌트 및 계정 이름 옆에 있는 help(도움말) 버튼을 클릭하고 **Provide Feedback(**피드백 제공**)**을 선택합니다.

단계 **3** 피드백을 입력하고 **Send Email(**이메일 전송**)**을 클릭합니다. 이렇게 하면 로컬 메일 서버에 수동으로 전송해야 하는 이메일이 생성됩니다.

Cisco 지원 담당자가 최대한 빨리 응답해 드리겠습니다.

2019년 2월

2019년 2월

보안 디바이스 커넥터에 영향을 주는 컨테이너 권한 에스컬레이션 취약점**: cisco-sa-20190215-runc**

Cisco PSIRT(제품 보안 사고 대응 팀)는 Docker의 심각도가 높은 취약성에 대해 설명하는 보안 자문 **cisco-sa-20190215-runc**를 게시했습니다. 취약성에 대한 전체 설명은 전체 PSIRT 팀 자문을 참조하십시오.

이 취약성은 모든 CDO 고객에게 영향을 미칩니다.

- CDO의 클라우드 구축 SDC(Secure Device Connector)를 사용하는 고객은 CDO 운영 팀에서 교정 단계를 이미 수행했으므로 아무 작업도 수행할 필요가 없습니다.
- 온프레미스에 구축된 SDC를 사용하는 고객은 최신 Docker 버전을 사용하도록 SDC 호스트를 업그레이드해야 합니다.

CDO 표준 SDC 호스트 및 맞춤형 SDC 호스트를 업데이트하는 방법에 대한 지침은 보안 디바이스 커넥터에 영향을 미치는 컨테이너 권한 에스컬레이션 취약성: cisco-sa-20190215-runc를 참조하십시오.

ASA 디바이스 대량 온보딩 시 레이블 추가

이제 ASA 디바이스를 대량 온보딩할 때 맞춤형 디바이스 레이블을 지정할 수 있습니다. 자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리의 "ASA 대량 온보딩"을 참조하십시오.

Cisco IOS 디바이스 지원

CDO(Cisco Defense Orchestrator)를 사용하면 Cisco IOS 디바이스를 관리할 수 있습니다. 이러한 디바이스에 대해 지원되는 기능은 다음과 같습니다.

- Cisco IOS 디바이스 온보딩
- 디바이스 구성 보기
- 디바이스에서 정책 및 구성 변경 종료

- 대역 외 변경 사항 탐지
- 명령줄 인터페이스 지원
- 개별 CLI 명령 및 명령 그룹을 편집 및 재사용 가능한 매크로로 전환할 수 있습니다.
- SSH 핑거프린트 변경 사항 탐지 및 관리
- 변경 로그에서 IOS 디바이스에 대한 변경 사항 보기

자동 구축 예약

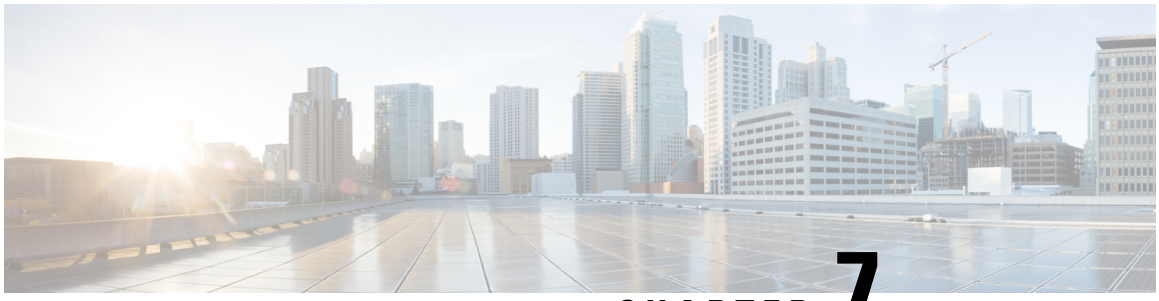
CDO를 사용하여 하나 이상의 디바이스에 대한 구성을 변경한 후에는 편리한 날짜와 시간에 해당 디바이스에 대한 구축을 예약할 수 있습니다. 예를 들어 유지 보수 기간 동안 또는 네트워크 트래픽이 적은 시간에 구축이 이루어지도록 예약할 수 있습니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리의 "자동 구축 예약 옵션 활성화" 및 "자동 구축 예약"을 참조하십시오.

용어 변경: **CDO**가 관리하는 디바이스에 변경 사항 **"구축"**

디바이스 구성의 CDO 로컬 복사본에 대한 변경 사항을 디바이스 자체로 전송하는 것을 설명하는 용어를 업데이트했습니다. 이전에는 "쓰기"라는 단어를 사용하여 해당 전송을 설명했지만 이제는 "구축"이라는 단어를 사용하여 해당 전송을 설명합니다.

CDO를 사용하여 디바이스의 구성을 관리하고 변경하면 CDO는 변경 사항을 구성 파일의 자체 복사본에 저장합니다. 이러한 변경 사항은 디바이스에 "구축"될 때까지 CDO에서 "준비된" 것으로 간주됩니다. 준비된 구성 변경은 디바이스를 통해 실행되는 네트워크 트래픽에 영향을 주지 않습니다. CDO가 디바이스에 변경 사항을 "구축"한 후에야 디바이스를 통해 실행되는 트래픽에 영향을 미칩니다. CDO는 디바이스의 구성에 변경 사항을 구축할 때 변경된 구성의 요소만 덮어씁니다. 디바이스에 저장된 전체 구성 파일을 덮어쓰지 않습니다.



CHAPTER 7

2018의 주요 기능

2018년 11월

2018년 11월 22일

대역외 변경 사항 자동 수락

이제 매니지드 디바이스에서 직접 구성을 변경하고 Defense Orchestrator에서 이를 탐지하면 자동으로 수락하도록 설정할 수 있습니다. Defense Orchestrator를 모니터링하고 대역 외 변경 사항을 수동으로 수락할 필요가 없습니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리의 "디바이스에서 대역외 변경 사항을 자동으로 수락"을 참조하십시오.

2018년 11월 8일

시스템 개체 필터

시스템 개체 필터를 사용하면 개체 테이블에서 가장 중요한 개체를 볼 수 있습니다.

일부 디바이스는 공통 서비스에 대해 사전 정의된 개체와 함께 제공됩니다. 이러한 시스템 개체는 이미 생성되어 규칙 및 정책에서 사용할 수 있으므로 편리합니다. 개체 테이블에는 여러 시스템 개체가 있을 수 있습니다. 시스템 개체는 편집하거나 삭제할 수 없습니다.

Show System Objects(시스템 개체 표시)는 기본적으로 "꺼짐"입니다. 개체 테이블에 시스템 개체를 표시하려면 필터 표시줄에서 Show System Objects(시스템 개체 표시)를 선택합니다. 개체 테이블에서 시스템 개체를 숨기려면 필터 표시줄에서 Show System Objects(시스템 개체 표시)를 선택하지 않은 상태로 둡니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리의 "개체 필터"를 참조하십시오.

2018년 9월

2018년 9월 20일

정책 내보내기 개선 사항

지정된 시간 범위로 ASA 정책을 내보내면 이제 시간 범위 개체 이름이 .CSV 파일에 포함됩니다. 이렇게 하면 정책의 규칙이 활성화되는 시점을 더 잘 파악할 수 있습니다.

CLI 처리 개선 사항

Defense Orchestrator는 실행하는 ASA CLI 명령에서 더 이상 후행 공백을 잘라내지 않습니다.

문서 업데이트

변경 로그 항목 및 "Diff(차이)" 페이지의 내용을 명확하게 이해할 수 있도록 ASA 변경 로그 및 "Diff(차이)" 설명서가 추가되었습니다. 구성 변경의 전후 비교를 참조하십시오. 자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리의 "변경 로그"를 참조하십시오.

2018년 9월 13일

관심 있는 변경 로그 항목만 내보내기

이전에는 전체 Defense Orchestrator의 변경 로그만 내보낼 수 있었습니다. 이제 변경 로그에 필터 및 검색 기준을 적용하고 원하는 항목만 내보낼 수 있습니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "CSV 파일로 변경 로그 내보내기"를 참조하십시오.

2018년 9월 6일

새 슈퍼 관리자 역할이 새 사용자 레코드를 생성하고 사용자 역할을 변경할 수 있음

Defense Orchestrator에서 슈퍼 관리자 역할에 대한 지원을 추가했습니다. 이 새 역할에는 관리자 역할의 모든 권한이 있으며 사용자 레코드를 관리할 수 있는 추가 권한이 있습니다. Defense Orchestrator 지원 팀은 기존 관리자 계정을 슈퍼 관리자로 업그레이드할 수 있습니다. 사용자에게 슈퍼 관리자 역할이 있으면 지원 티켓을 열지 않고도 추가 사용자 레코드를 생성하고 관리할 수 있습니다.

회사에서 SAML IdP(Identity Provider)를 Defense Orchestrator와 통합한 경우 이제 Defense Orchestrator 계정에 대한 사용자 액세스를 완전히 관리할 수 있습니다.

여러 Defense Orchestrator 계정을 보유한 매니지드 서비스 제공자는 이제 Defense Orchestrator를 사용하여 지원 티켓을 열지 않고도 기존 사용자에 대한 계정 액세스 권한을 부여하고 취소할 수 있습니다.

회사에서 Defense Orchestrator의 기본 ID 제공자(OneLogin)를 사용하는 경우 계속해서 지원 티켓을 열어 새 사용자 어카운트를 생성해야 하지만 지원 티켓을 열지 않고도 Defense Orchestrator 어카운트에 대한 액세스를 취소할 수 있습니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "사용자 관리"를 참조하십시오.

2018년 8월 16일

변경 로그 개선 사항

CDO를 통해 ASA를 변경하고 구성 변경에 성공하면 변경 로그에 변경에 사용된 CLI 명령이 표시됩니다.

CDO를 통해 ASA를 변경한 경우 구성 변경이 실패하면 Change Log(변경 로그)는 실패한 CLI 명령을 표시하고 해당 명령을 쉽게 찾을 수 있도록 별표로 묶어 표시합니다.

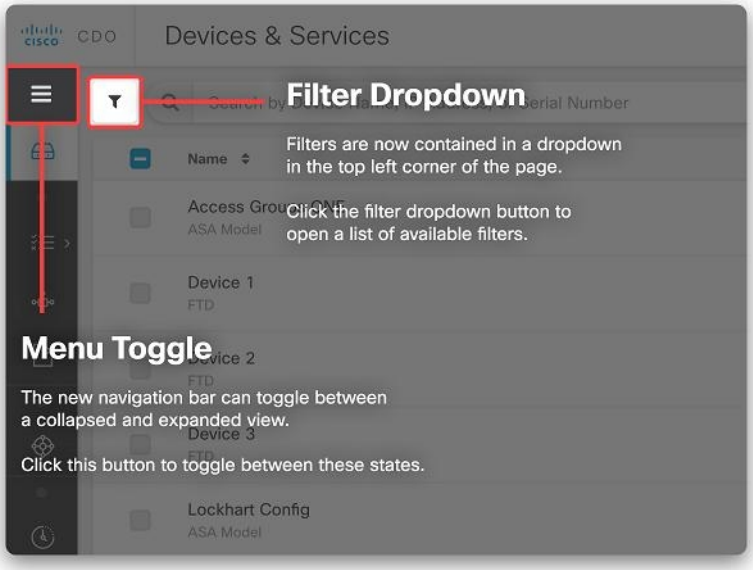
성공하거나 실패한 명령을 보려면 변경이 수행된 디바이스의 변경 로그를 열고 작업에 대한 항목을 찾은 다음 로그 항목의 끝에 있는 + 버튼을 클릭하여 확장합니다.

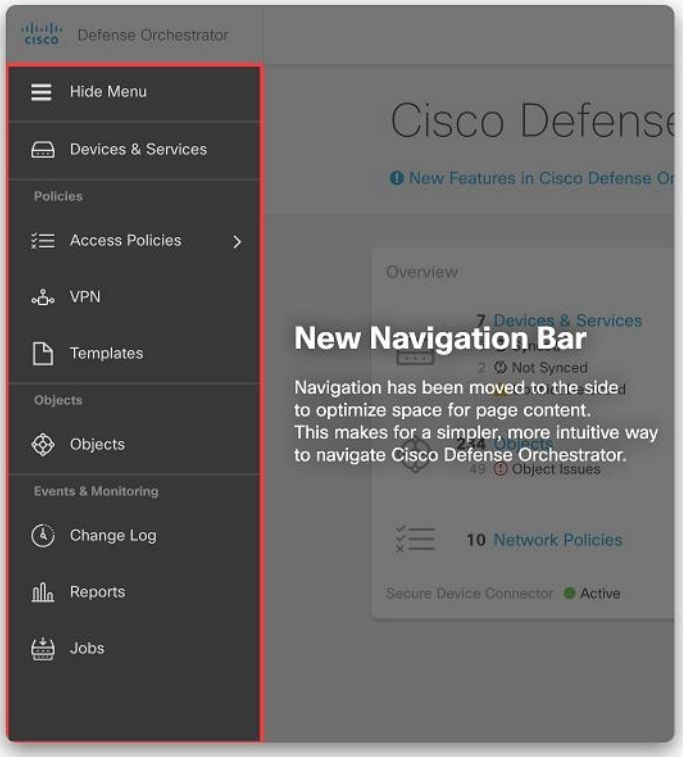
2018년 7월

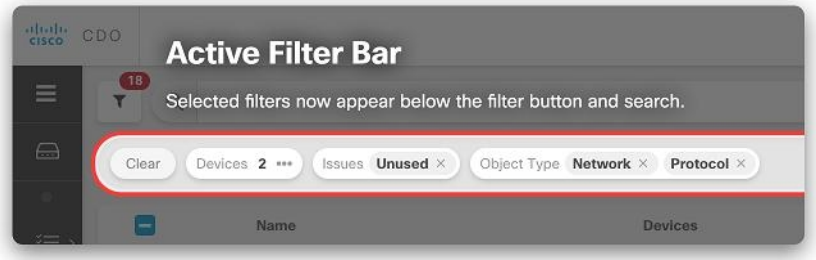
2018년 7월 26일

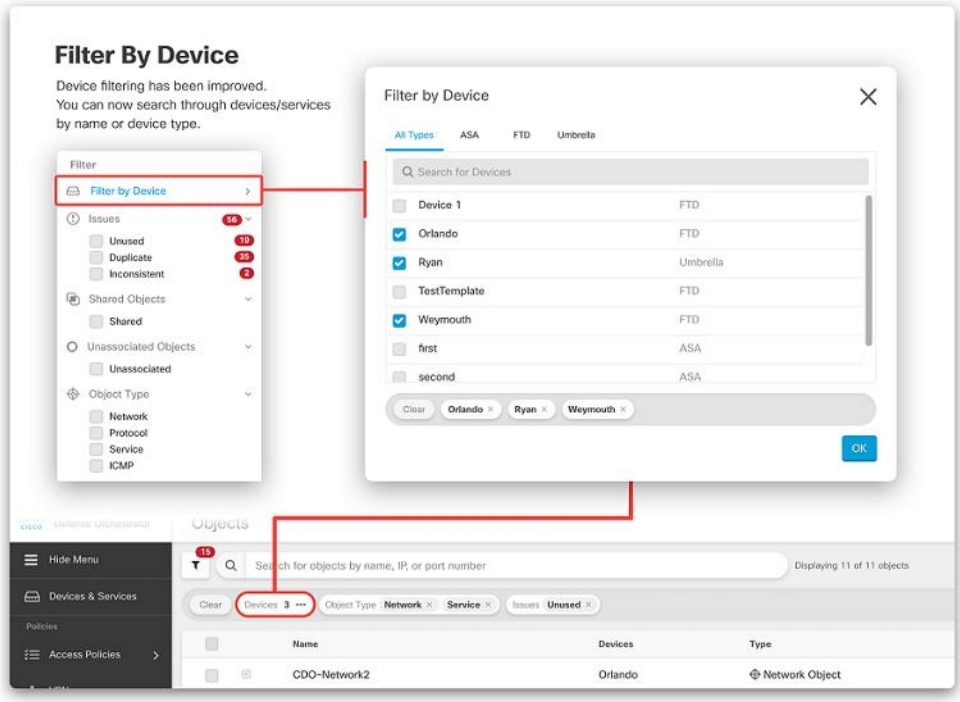
새 **CDO UI**

탐색 및 필터링을 재설계하여 환경을 보다 직관적으로 관리할 수 있도록 지원합니다.


CDO
Devices & Services
Filter Dropdown
Filters are now contained in a dropdown in the top left corner of the page.
Click the filter dropdown button to open a list of available filters.
Name
Device 1
FTD
Menu Toggle
The new navigation bar can toggle between a collapsed and expanded view.
Click this button to toggle between these states.
Lockhart Config
ASA Model

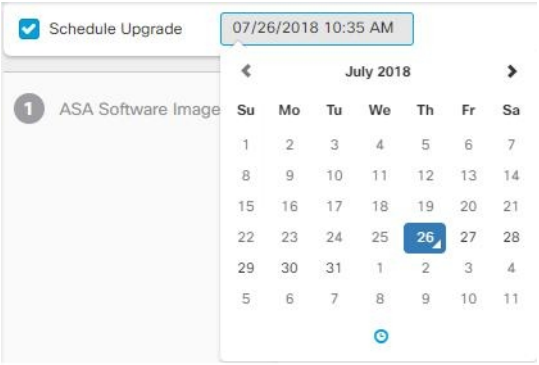

Defense Orchestrator
Hide Menu
Devices & Services
Policies
Access Policies
VPN
Templates
Objects
Objects
Events & Monitoring
Change Log
Reports
Jobs
Cisco Defens
New Features in Cisco Defense Or
Overview
7 Devices & Services
2 Not Synced
49 Object Issues
10 Network Policies
Secure Device Connector Active
New Navigation Bar
Navigation has been moved to the side to optimize space for page content.
This makes for a simpler, more intuitive way to navigate Cisco Defense Orchestrator.





디바이스 업그레이드 예약

이제 디바이스에 대한 소프트웨어 업그레이드를 예약할 수 있습니다. Device Upgrade(디바이스 업그레이드) 페이지에서 Schedule Upgrade(업그레이드 예약) 확인란을 선택하고 이후 날짜 및 시간을 구성합니다. 자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리의 "디바이스 및 서비스 업그레이드"를 참조하십시오.



대량 자격 증명 업데이트

이제 CDO가 여러 ASA 디바이스의 ASA에 한 번에 연결하는 데 사용하는 자격 증명을 업데이트할 수 있습니다. Devices & Services(디바이스 및 서비스) 페이지에서 여러 ASA 디바이스를 선택하고 Update Credentials(자격 증명 업데이트)를 클릭합니다. 자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리의 "ASA 연결 자격 증명 업데이트"를 참조하십시오.

디바이스 위치 업데이트

이제 IP 주소 옆에 있는 edit(편집) 버튼을 클릭하여 온보딩된 ASA의 디바이스 위치를 업데이트할 수 있습니다.

2018년 7월 20일

자격 증명 업데이트

이제 CDO가 ASA에 연결하는 데 사용하는 자격 증명을 업데이트할 수 있습니다. ASA를 온보딩하는 과정에서 CDO가 ASA에 연결하는 데 사용해야 하는 사용자 이름 및 비밀번호를 입력했습니다. 이전에는 이러한 자격 증명을 변경하거나 비밀번호를 변경하려면 CDO에서 ASA를 제거하고 새 자격 증명을 사용하여 다시 온보딩해야 했습니다. 이제 ASA를 다시 온보딩하지 않고도 자격 증명을 변경할 수 있습니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리의 "ASA 연결 자격 증명 업데이트"를 참조하십시오.

2018년 7월 12일

새 **ASA** 기본 규칙 동작

새 규칙이 ASA 네트워크 정책에 추가되면 기본적으로 "Permit(허용)" 작업이 할당됩니다.

내보낸 디바이스 목록에 테넌트 이름이 포함됨

특정 테넌트의 디바이스 목록을 내보내면 이제 테넌트의 이름이 내보낸 파일 이름에 통합됩니다.

자세한 내용은 Cisco Defense Orchestrator를 사용하여 ASA 관리의 "디바이스 및 서비스 목록 내보내기"를 참조하십시오.

네트워크 그룹 대량 입력

이제 ASA 네트워크 개체 그룹을 생성하거나 수정할 때 IP 주소를 한 번에 하나씩 추가하는 대신 대량으로 추가할 수 있습니다.

자세한 내용은 Cisco Defense Orchestrator를 사용하여 ASA 관리의 "ASA 네트워크 개체 및 네트워크 그룹 생성 또는 수정"을 참조하십시오.

2018년 5월

2018년 5월 24일

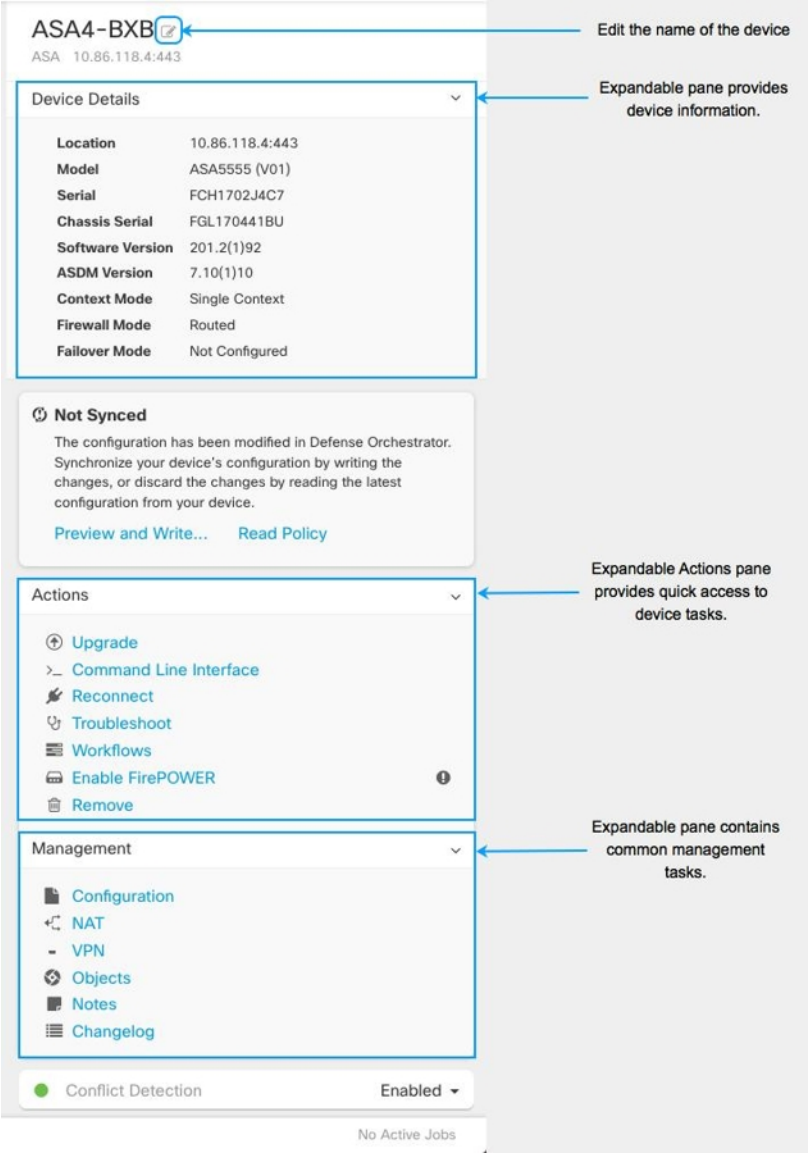
시간 기반 **ASA** 네트워크 정책 지원

시간 기반 ASA 네트워크 정책은 시간을 기준으로 네트워크 및 리소스에 대한 액세스를 허용합니다. 시간은 시간 범위 개체로 정의됩니다. 시간 범위 개체에는 시작 시간과 종료 시간이 있으며 반복 이벤트로 정의할 수도 있습니다. 자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리의 "정책에 대한 시간 범위 정의"를 참조하십시오.

2018년 5월 17일

새 디바이스 세부사항 패널 레이아웃

디바이스 정보 및 일반적으로 사용되는 명령 버튼을 더 쉽게 찾을 수 있도록 디바이스 세부 정보 패널을 재구성했습니다.



ASA 전역 액세스 정책 지원

이제 CDO를 사용하여 ASA에 대한 전역 액세스 정책을 생성할 수 있습니다. 전역 액세스 정책은 ASA의 모든 인터페이스에 적용되는 네트워크 정책입니다. 이는 인바운드 네트워크 트래픽에 적용됩니다. CDO를 사용하면 전역 액세스 정책을 한 ASA에서 다른 ASA로 복사하여 디바이스 간에 일관성을 유지할 수 있습니다. 자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리의 "ASA 전역 액세스 정책 구성"을 참조하십시오.

ASA 디바이스를 위한 **NAT(Network Address Translation)** 규칙 마법사

다음과 같은 활용 사례를 위해 ASA 디바이스에서 NAT 규칙을 생성하는 데 도움이 되는 새로운 NAT(Network Address Translation) 규칙 마법사가 있습니다.

- 내부 사용자에 대한 인터넷 액세스 활성화

- 인터넷에 내부 서버 노출

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리의 "네트워크 주소 변환 규칙 마법사"를 참조하십시오.

2018년 4월

2018년 4월 26일

새 트러블슈팅 설명서

ASA를 재부팅한 후 CDO(Cisco Defense Orchestrator)와 ASA가 연결되지 않으면 ASA가 CDO의 Secure Device Connector에서 지원하지 않는 OpenSSL 암호 그룹을 사용하도록 대체되었기 때문일 수 있습니다. "ASA Fails to Reconnect to CDO After Reboot(재부팅 후 ASA가 CDO에 다시 연결하지 못함)" 트러블슈팅 항목 테스트에서는 지원되는 암호 그룹 목록 및 치료 단계를 제공합니다.

2018년 4월 5일

ACE(Access Control Entry) 제한 계산

CDO는 개별 규칙의 ACE(Access Control Entry) 수, 네트워크 정책 및 ASA에서 실행 중인 총 수를 표시합니다. ASA가 처리할 수 있는 ACE의 수에는 하드 코딩된 제한이 없지만, 액세스 제어 항목의 수가 너무 많아지면 ASA의 성능이 저하됩니다. 자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리의 "액세스 제어 항목(ACE)"을 참조하십시오.

2018년 3월

2018년 3월 22일

지원되지 않는 디바이스

CDO는 현재 **ASASM(ASA Service Module)**을 지원합니다.

2018년 3월 15일

읽기 전용 사용자

읽기 전용 사용자 역할을 생성했습니다. 읽기 전용 사용자는 CDO의 모든 항목을 볼 수 있지만 어떤 페이지에서도 생성, 업데이트, 구성 또는 삭제할 수는 없습니다. 디바이스를 온보딩할 수도 없습니다.

읽기 전용 사용자에게는 모든 페이지에서 "Read Only User(읽기 전용 사용자). You cannot make configuration pages(구성 페이지를 만들 수 없습니다)."라는 파란색 배너가 표시되며

사용자 관리 테이블에서 역할에 따라 식별됩니다. 자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리의 "사용자 역할"을 참조하십시오.

연결 자격 증명 업데이트

디바이스를 온보딩할 때 해당 디바이스의 사용자 이름과 비밀번호를 지정합니다. Cisco Defense Orchestrator는 이러한 자격 증명을 사용하여 디바이스에 연결하고 디바이스에 명령을 전송할 때 해당 사용자 역할을 합니다. 디바이스에서 사용자 또는 비밀번호가 변경되면 해당 변경 사항을 반영하도록 디바이스 자격 증명을 업데이트할 수 있습니다.

자세한 내용은 다음 주제를 참고하십시오.

- ASA 연결 자격 증명 업데이트 - *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리
- AWS 연결 자격 증명 업데이트 - *Cisco Defense Orchestrator*를 사용하여 *AWS* 관리
- Meraki MX 연결 자격 증명 업데이트 - *Cisco Defense Orchestrator*를 사용하여 *Meraki* 관리

향상된 네트워크 정책 필터링

이제 정책이 실행되는 ASA를 먼저 파악하지 않고도 적중 횟수를 기준으로 네트워크 정책을 필터링할 수 있습니다. 이를 통해 구축의 어디에서나 적중 횟수가 0인 네트워크 정책을 찾을 수 있습니다. 자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리의 "사용 사례 필터링"을 참조하십시오.

네트워크 정책 규칙 내보내기

각 Access-Group 또는 Crypto-Map의 콘텐츠를 .csv 파일로 내보낼 수 있습니다. 이 .csv는 각 ACL(Access Control List) 및 CDO가 각 ACL에 대해 보유한 데이터를 표시합니다. 자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리의 "네트워크 정책 규칙 내보내기"를 참조하십시오.

2018년 3월 7일

새로운 **CDO** 포털

사용자가 알아야 할 사항, 수행해야 하는 작업 및 수행해야 하는 위치를 신속하게 전달할 수 있도록 포털을 재설계했습니다.

맞춤형 **URL** 업그레이드

이제 자체 이미지 저장소에서 유지 관리하는 ASA 소프트웨어 및 ASDM 이미지를 사용하여 ASA 디바이스를 업그레이드할 수 있습니다. ASA에 인터넷에 대한 아웃바운드 액세스 권한이 없거나 CDO의 이미지 저장소에 없는 이미지를 원하는 경우 ASA를 업그레이드하는 가장 좋은 방법입니다. FTP,

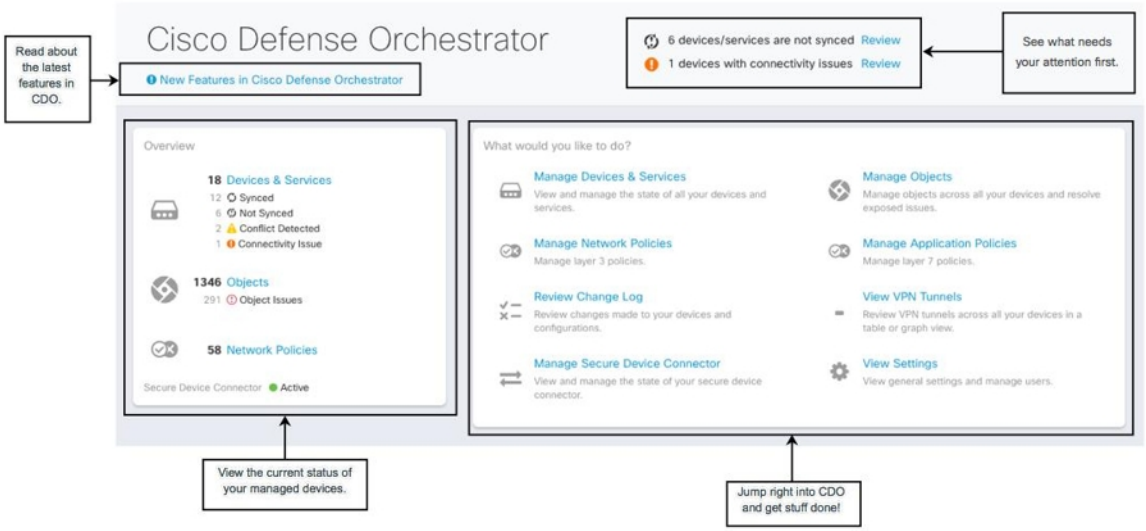
TFTP, HTTP, HTTPS, SCP 및 SMB 프로토콜 중 하나를 사용하여 저장소에서 이미지를 검색할 수 있습니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리의 "맞춤형 URL 업그레이드"를 참조하십시오.

디바이스 참고 사항

이제 CDO에서 나가지 않고도 특정 ASA에 대한 메모를 단일 일반 텍스트 파일에 저장할 수 있습니다. 자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리의 "디바이스 참고 사항"을 참조하십시오.

2018년 2월



2018년 2월 29일

테넌트와 연결된 모든 계정 보기

이제 **User Management(**사용자 관리**)** 화면에서 테넌트와 연결된 모든 사용자를 볼 수 있습니다. 여기에는 지원 티켓을 해결하기 위해 사용자 어카운트와 일시적으로 연결된 모든 Cisco 지원 엔지니어가 포함됩니다.

테넌트와 연결된 사용자를 보려면 다음을 수행합니다.

1. 사용자 메뉴에서 **Settings(**설정**)**를 선택합니다.
2. **User Management(**사용자 관리**)**를 클릭합니다.

테넌트에 대한 **Cisco** 액세스 관리

Cisco 지원에서는 지원 티켓을 해결하거나 둘 이상의 고객에게 영향을 미치는 문제를 사전에 해결하기 위해 사용자를 테넌트와 연결합니다. 그러나 원하는 경우 어카운트 설정을 변경하여 Cisco 지원에서 어카운트에 액세스하는 것을 방지할 수 있습니다. 자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "일반 설정"을 참조하십시오.

테넌트와 연결된 모든 계정 보기

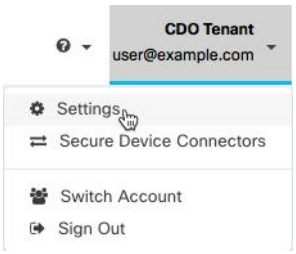
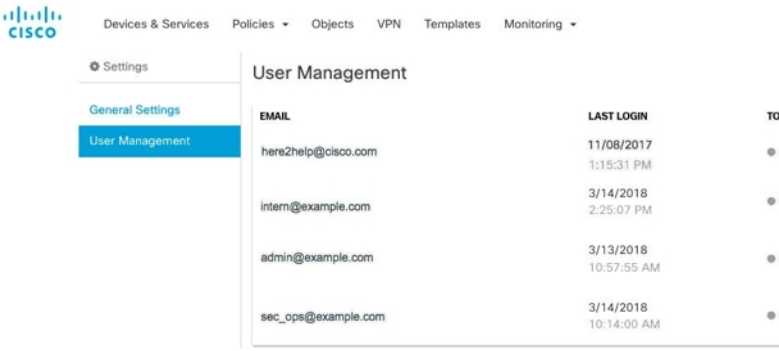
이제 **User Management(**사용자 관리**)** 화면에서 테넌트와 연결된 모든 사용자를 볼 수 있습니다. 여기에는 지원 티켓을 해결하기 위해 사용자 어카운트와 일시적으로 연결된 모든 Cisco 지원 엔지니어가 포함됩니다.

테넌트와 연결된 사용자를 보려면 다음을 수행합니다.

SUMMARY STEPS

1. 사용자 메뉴에서 **Settings(**설정**)**를 선택합니다.
2. **User Management(**사용자 관리**)**를 클릭합니다.

DETAILED STEPS

	명령 또는 동작	목적
단계 **1**	사용자 메뉴에서 **Settings(**설정**)**를 선택합니다.	
단계 **2**	**User Management(**사용자 관리**)**를 클릭합니다.	

테넌트에 대한 **Cisco** 액세스 관리

Cisco 지원에서는 지원 티켓을 해결하거나 둘 이상의 고객에게 영향을 미치는 문제를 사전에 해결하기 위해 사용자를 테넌트와 연결합니다. 그러나 원하는 경우 어카운트 설정을 변경하여 Cisco 지원에서 어카운트에 액세스하는 것을 방지할 수 있습니다. 확인 Hyperconverged PSS에게 문의하십시오.

2018년 2월 15일

CLI 매크로를 사용하여 **ASA** 관리

CDO는 ASA에서 맞춤 설정하고 실행할 수 있는 완전한 CLI 기반 명령 및 명령 템플릿 목록을 제공합니다. 이러한 CLI 매크로는 단일 ASA 또는 ASA에서 대량으로 실행할 수 있습니다. 정기적으로 수행하는 모니터링 또는 유지 보수 작업이 있습니까? 고유한 CLI 기반 명령을 생성하여 CDO에 저장하고 필요할 때 재사용할 수 있습니다.

CLI 매크로를 사용하여 ASA 관리

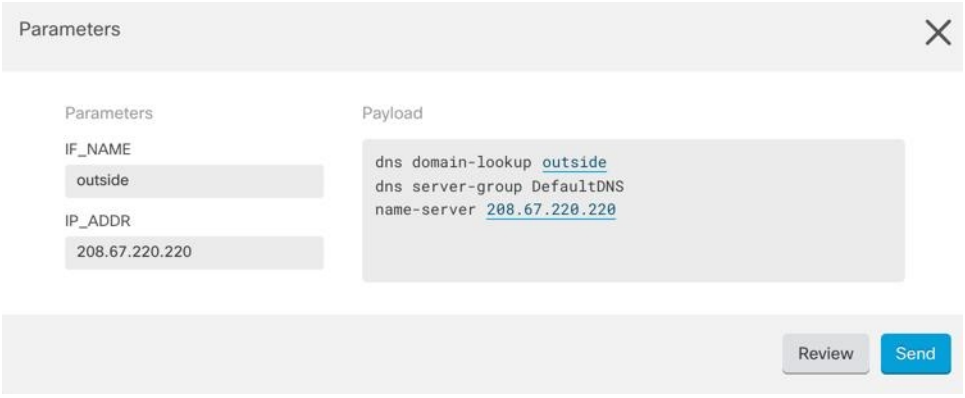
CDO는 ASA에서 맞춤 설정하고 실행할 수 있는 완전한 CLI 기반 명령 및 명령 템플릿 목록을 제공합니다. 이러한 CLI 매크로는 단일 ASA 또는 ASA에서 대량으로 실행할 수 있습니다. 정기적으로 수행하는 모니터링 또는 유지 보수 작업이 있습니까? 고유한 CLI 기반 명령을 생성하여 CDO에 저장하고 필요할 때 재사용할 수 있습니다.

다음은 CLI 매크로를 사용하여 ASA에서 DNS 서버를 구성하는 예입니다.

단계 **1** 구성해야 하는 디바이스를 선택합니다.

단계 **2** Configure DNS Macro(DNS 매크로 구성)를 선택합니다.

단계 **3** 매개변수 필드에 사용자 정보를 입력합니다.

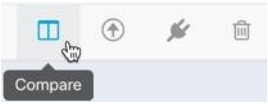


단계 **4** 모든 ASA로 전송합니다.

2018년 2월 11일

ASA 구성 비교

이제 두 개의 ASA 구성을 쉽게 비교할 수 있습니다. Devices & Services(디바이스 및 서비스) 페이지에서 두 개의 ASA를 선택하고 Compare(비교) 버튼을 클릭합니다. CDO는 디바이스의 구성을 나란히 비교합니다. 자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리의 "ASA 구성 비교"를 참조하십시오.



2018년 1월

2018년 1월 31일

CDO를 사용하여 최근 **Cisco ASA** 보안 권고의 위험 완화

2018년 1월 29일, Cisco 제품 보안 사고 대응 팀(PSIRT)은 ASA 및 Firepower 보안 취약성에 대해 설명하는 보안 권고 cisco-sa-20180129-asa1을 게시했습니다. *Cisco ASA* 자문 *cisco-sa-20180129-asa1*에서 *CDO*를 사용하여 자문의 영향을 받는 ASA를 찾고 패치가 적용된 ASA 버전으로 업그레이드하는 방법을 알아보려면 문서 cisco-sa-20180129-asa1을 참조하십시오.

긴 **CLI** 시퀀스를 허용하는 **CDO**

CLI의 명령 상자에 긴 명령 목록을 입력하면 CDO는 ASA API에 대해 한 번에 실행할 수 있도록 명령을 여러 명령으로 분할하려고 시도합니다. CDO가 명령에서 적절한 분리를 결정할 수 없는 경우 힌트를 입력하라는 프롬프트가 표시됩니다. 예를 들면 다음과 같습니다.

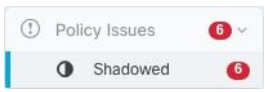
오류: CDO가 600자를 초과하는 이 명령의 일부를 실행하려고 시도했습니다. 적절한 명령 구분 지점이 어디인지에 대한 힌트를 CDO에 제공할 수 있습니다. 명령 목록 사이에 빈 행을 추가하면 됩니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리의 "ASA 명령줄 인터페이스"를 참조하십시오.

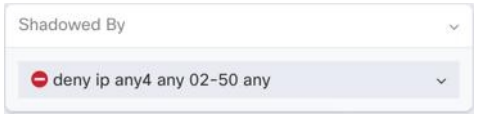
2018년 1월 18일

새도우 규칙 문제 관리를 위한 개선 사항

- ASA 네트워크 정책 문제 필터는 정책에 새도잉 규칙이 있는지 여부를 나타냅니다.



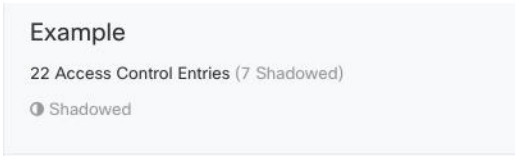
- ASA 네트워크 정책의 규칙 옆에 새 배지 ⚠가 있으면 해당 규칙이 정책의 다른 규칙을 섀도잉하고 있음을 나타냅니다.
- 섀도우 규칙의 경우, 네트워크 정책 세부 정보 창은 정책에서 규칙을 섀도잉하는 규칙을 식별합니다.



- 섀도우 규칙 문제 해결에 대한 새 설명서입니다.

CDO에서 **ASA** 네트워크 정책의 액세스 제어 항목 계산

CDO(Cisco Defense Orchestrator)는 ASA 네트워크 정책의 모든 규칙에서 파생된 ACE(Access Control Entry) 수를 계산하여 네트워크 정책 세부사항 창의 상단에 해당 합계를 표시합니다. 네트워크 정책의 규칙 중 하나라도 섀도 처리된 경우 해당 번호도 나열됩니다.

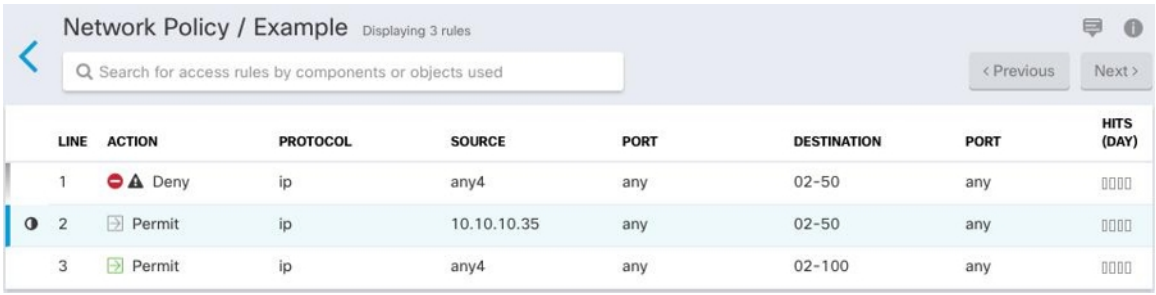


또한 CDO는 네트워크 정책의 단일 규칙에서 파생된 ACE의 수를 표시하고 네트워크 정책 세부 정보 창에 해당 정보를 표시합니다. 다음은 해당 목록의 예입니다.

ASA에는 디바이스에서 생성되는 ACE 수에 대한 권장 제한이 있습니다. 이러한 권장 사항을 따르면 ASA에서 최적의 속도로 네트워크 트래픽을 처리할 수 있습니다. 사용되지 않는 규칙 또는 숨겨진 규칙을 삭제하면 ACE 카운트를 줄이는 데 도움이 됩니다.

네트워크 정책의 번호가 매겨진 라인

CDO는 네트워크 정책에서 규칙을 쉽게 읽을 수 있도록 번호를 매깁니다. 정책에서 규칙을 추가 및 삭제하거나 순서를 변경하면 라인 번호가 다시 매겨집니다.



2018년 1월 4일

향상된 **ASA** 네트워크 정책 관리

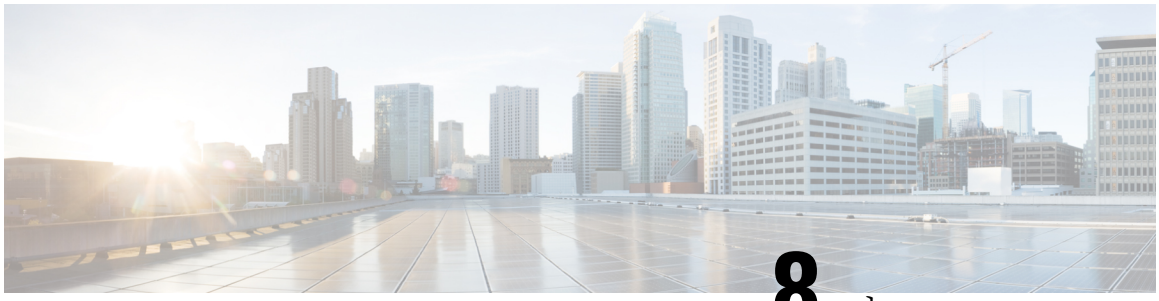
이제 ASA 네트워크 정책을 사용하여 이러한 작업을 수행할 수 있습니다!

- **ASA** 디바이스 간에 정책을 복사하여 붙여넣습니다. 한 ASA에서 다른 ASA로 정책을 복사하여 특정 인터페이스에 할당합니다.
- 정책 내에서 규칙을 잘라내고 붙여넣습니다. 규칙 테이블에서 규칙을 잘라내고 붙여넣어 정책 내에서 규칙의 우선순위를 변경합니다.
- 정책 간에 규칙을 복사하여 붙여넣습니다. 한 정책에서 다른 정책으로 규칙을 복사하여 정책 일관성을 높입니다. 이러한 정책은 동일한 디바이스에 있을 수도 있고 다른 디바이스에 있을 수도 있습니다.

이러한 개선 사항은 ASA 네트워크 정책 생성, 정책의 규칙 활성화 또는 비활성화, 정책의 규칙에 의해 생성된 활동 로깅 등의 기존 기능을 보완합니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리의 "ASA 네트워크 개체 및 네트워크 그룹 생성 또는 수정" 및 "ASA 네트워크 정책"을 참조하고 페이지 하단의 항목 화살표를 사용하여 ASA 네트워크 정책 설명서를 탐색하십시오.

◀ ASA Network Policies | Edit an ASA Network Policy ▶



8 장

2017의 주요 기능

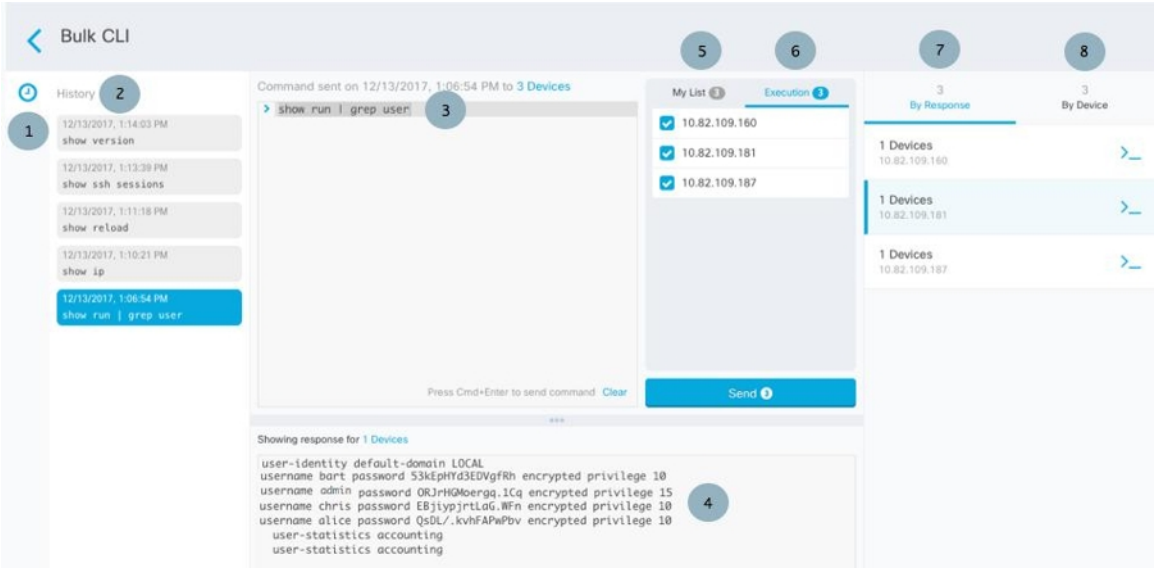
이 문서에서는 2017년에 Cisco Defense Orchestrator에 추가된 몇 가지 기능을 중점적으로 설명합니다.

2017년 12월

2017년 12월 14일

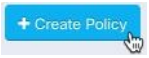
대량 명령줄 인터페이스

CDO(Cisco Defense Orchestrator)는 관리자가 하나의 명령을 여러 디바이스에 동시에 전송할 수 있는 기능을 제공하여 디바이스 전체에서 일관된 구성을 촉진합니다. CDO는 대량 CLI 명령에 대한 응답을 응답 유형 및 디바이스 유형별로 그룹화하므로 어떤 ASA가 특정 응답을 반환했으며 어떤 디바이스에 특정 명령이 전송되었는지를 확인할 수 있습니다. CDO는 명령을 다시 실행하거나 수정할 수 있도록 명령의 기록 목록을 유지 관리합니다. 자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리의 "대량 명령줄 인터페이스"를 참조하십시오.



ASA 네트워크 정책 생성

이제 ASA에 대한 네트워크 정책을 생성할 수 있습니다. 정책에 규칙을 추가하고, 정책 내에서 규칙의 순서를 변경하고, 정책 내에서 규칙을 활성화 또는 비활성화할 수 있으며, 한 ASA에서 다른 ASA로 해당 정책을 복사할 수 있습니다. 시작하려면 *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리의 "ASA 네트워크 정책 생성"을 참조하십시오.



2017년 11월

2017년 11월 9일

대량 운영

특정 CDO 구성 작업은 여러 디바이스에서 동시에 수행할 수 있습니다. 이 작업은 "대량으로" 수행할 수 있습니다. 이 기능을 사용하면 시간이 절약되고 디바이스 간의 일관성이 향상됩니다. 이는 대량으로 수행할 수 있는 작업 및 이를 보완하기 위해 추가된 몇 가지 추가 기능입니다.

대량 **ASA** 및 **ASDM** 업그레이드

이제 CDO의 업그레이드 마법사를 사용하여 여러 ASA에서 ASA 및 ASDM 이미지를 동시에 업그레이드할 수 있습니다. 백그라운드에서 필요한 모든 업그레이드 단계를 수행하여 프로세스를 쉽게 수행합니다. 마법사는 호환되는 ASA 및 ASDM 소프트웨어 이미지를 선택하고 설치하고 디바이스를 재부팅하여 업그레이드를 완료하는 프로세스를 안내합니다. Cisco에서는 CDO에서 선택한 이미지가 ASA에 복사되고 설치된 이미지인지 확인하여 업그레이드 프로세스를 보호합니다. 자세한 내용은

*Cisco Defense Orchestrator*를 사용하여 *ASA* 관리의 "대량 ASA 및 ASDM 업그레이드"를 참조하십시오.

대량 읽기 구성

CDO 외부의 디바이스에 대한 구성이 변경되면 CDO에 저장된 디바이스의 구성과 디바이스의 로컬 구성은 더 이상 동일하지 않습니다. 이 경우 CDO는 관리자에게 경고하기 위해 "충돌 탐지됨" 메시지를 표시합니다. 관리자는 CDO의 구성을 디바이스에 저장된 구성으로 덮어쓰는 "정책 읽기" 작업을 수행합니다. 이제 두 구성이 동일하며 "동기화"됩니다. 대량 읽기 구성 기능을 사용하면 관리자가 동시에 여러 디바이스에서 이 작업을 수행할 수 있습니다.

대량 읽기 구성의 또 다른 용도는 CDO에 준비된 변경 사항이 디바이스에 기록되는 것을 방지하는 것입니다. 디바이스에서 CDO로 구성을 읽어 CDO의 모든 준비된 변경 사항을 덮어씁니다. 이는 필요한 경우 CDO에서 디바이스 구성에 대한 변경 사항을 되돌리는 좋은 방법일 수도 있습니다. 자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리의 "대량 읽기 구성"을 참조하십시오.

디바이스 대량 다시 연결

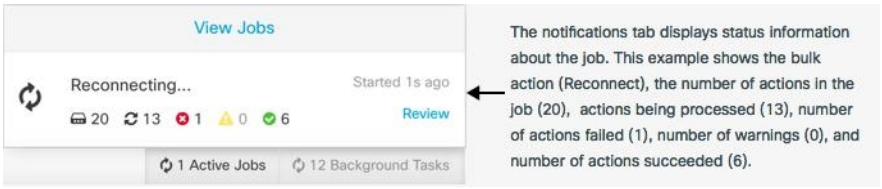
관리자는 CDO를 통해 둘 이상의 매니지드 디바이스를 CDO에 동시에 다시 연결할 수 있습니다. CDO가 관리하는 디바이스가 "unreachable(연결할 수 없음)"로 표시되면 CDO는 더 이상 대역 외 구성 변경 사항을 탐지하거나 디바이스를 관리할 수 없습니다. 디바이스에 대한 CDO 관리를 복원하는 첫 번째 단계는 디바이스를 다시 연결하는 것입니다. 자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리의 "디바이스 대량 다시 연결"을 참조하십시오.

충돌 탐지 대량 활성화 및 비활성화

여러 디바이스에 대한 충돌 탐지를 동시에 활성화하거나 비활성화할 수 있습니다. 충돌 탐지를 활성화하면 CDO 외부에서 디바이스가 변경된 경우 인스턴스에 알림이 표시됩니다. 자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리의 "충돌 탐지 활성화"를 참조하십시오.

작업 알림

알림 탭은 CDO의 오른쪽 하단에 있습니다. 작업에서 진행 중인 작업의 활성 개수를 표시합니다.



작업 페이지

Jobs(작업) 페이지에는 대량 작업의 상태, 성공 및 실패에 대한 정보가 표시됩니다. 작업 테이블에서 색상으로 구분된 행은 성공하거나 실패한 개별 작업을 나타냅니다. 자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리의 "작업 페이지"를 참조하십시오.

실패한 작업에 대한 작업 다시 시작

CDO는 대량 작업을 기억하고 실패한 개별 작업을 식별하며 실패한 작업에 대해서만 작업을 다시 실행하여 시간을 절약합니다. 작업 페이지를 검토할 때 대량 작업에서 하나 이상의 작업이 실패한 경우 필요한 수정을 수행한 후 대량 작업을 다시 실행할 수 있습니다. CDO는 실패한 작업에 대해서만 작

업을 다시 실행합니다. 자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리의 "작업이 실패한 대량 작업 다시 시작"을 참조하십시오.

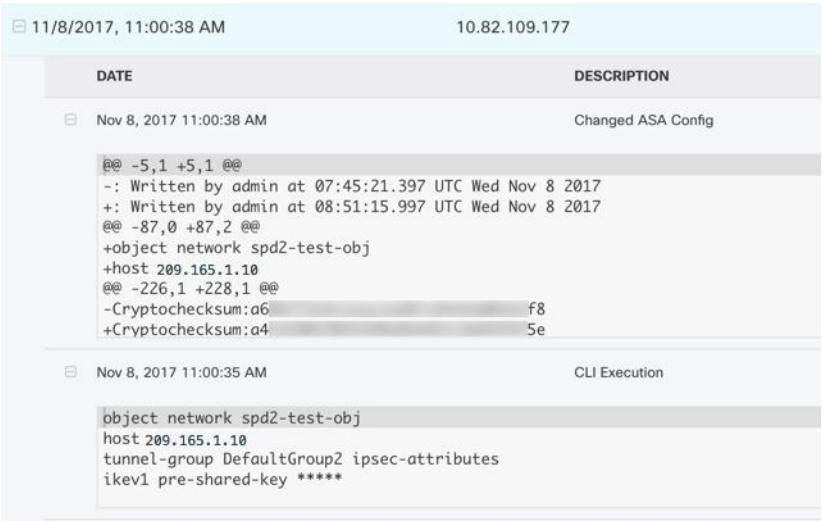
NAT 설명서

다음과 같은 활용 사례에 대한 문서화된 절차가 있습니다.

- 공용 IP 주소를 사용하여 인터넷에 연결하도록 내부 네트워크의 서버 활성화
- 공용 IP 주소의 특정 포트에서 사용자가 내부 네트워크의 서버를 사용할 수 있도록 설정
- 사설 IP 주소 범위를 공용 IP 주소 범위로 변환

CLI 로깅

CDO를 사용하여 ASA에서 CLI 명령을 실행할 때마다 이제 명령 및 명령의 결과가 디바이스의 변경 로그에 기록됩니다. 아래 예에서 CLI Execution(CLI 실행) 행의 항목에는 전송된 명령이 표시되고 Changed ASA Config(변경된 ASA 구성) 행에는 명령의 결과로 구성 파일에서 변경된 내용이 표시됩니다.



2017년 10월

2017년 10월 19일

ASA의 대량 온보딩

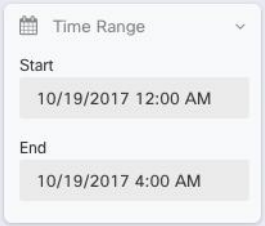
이제 단일 배치에서 여러 ASA를 CDO에 온보딩할 수 있습니다. 자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리의 "ASA 대량 온보딩"을 참조하십시오.

공유 네트워크 정책

CDO(Cisco Defense Orchestrator)는 여러 ASA에서 사용하는 동일한 네트워크 정책을 찾아 네트워크 정책 페이지에서 식별합니다. 공유 네트워크 정책이 있는 경우 정책을 한 번 변경하고 정책을 공유하는 다른 디바이스에 변경 사항을 배포할 수 있습니다. 이렇게 하면 디바이스 간에 네트워크 정책이 일관되게 유지됩니다. 자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리의 "공유 네트워크 정책"을 참조하십시오.

시간 및 날짜 기준으로 변경 로그 필터링

이제 변경 로그에서 시간 및 날짜별로 이벤트를 필터링할 수 있습니다. Monitoring(모니터링) > Change Log(로그 변경)로 이동하여 필터 표시줄에서 이 시간 및 날짜 달력을 찾습니다.



2017년 10월 12일

Packet Tracer

패킷 트레이서는 액세스 및 정책 문제를 해결하는 데 도움이 됩니다. 패킷 트레이서는 가상 패킷을 네트워크로 전송하고 저장된 라우팅 구성, NAT 규칙 및 정책 구성이 해당 패킷과 상호 작용하는 방식을 평가합니다. 예를 들어, 규칙이 패킷을 삭제하는 경우 패킷 트레이서는 해당 규칙을 식별하고 사용자가 규칙을 평가하고 수정할 수 있도록 해당 규칙에 대한 링크를 제공합니다. 패킷 트레이서는 라이브, 온라인, 물리적 또는 가상 ASA(Adaptive Security Appliance)에서 사용할 수 있습니다. 자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리의 "ASA 패킷 트레이서"를 참조하십시오.

2017년 10월 5일

새로운 **Screencast**

CDO를 사용하여 액티브/스탠바이 장애 조치 쌍으로 구성된 단일 ASA 또는 2개의 ASA를 업그레이드하는 방법을 보여주는 새로운 screencast.

2017년 9월

2017년 9월 28일

업데이트된 문서

- Resolve configuration Conflicts(구성 충돌 해결) - 디바이스가 "동기화되지 않음"이거나 "충돌 탐지됨"을 보고할 때 수행할 작업을 설명하는 트러블슈팅 항목입니다.
- 구성 변경 사항이 액티브-액티브 페일오버 모드에서 ASA에 적용됨 - 페일오버 모드에서 액티브-액티브 쌍으로 구성된 ASA의 구성 변경에 대한 중요한 정보를 제공합니다.
- 인증서 문제 해결 - CDO가 인증서를 거부할 수 있는 이유와 인증서에 대해 수행할 작업을 설명하는 트러블슈팅 항목입니다.
- FAQ(자주 묻는 질문) 페이지가 업데이트되었습니다.

2017년 9월 14일

CDO 서비스 상태 페이지

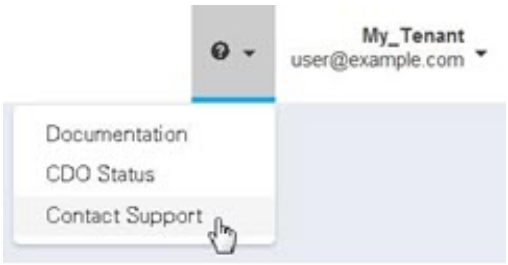
CDO는 https://status.defenseorchestrator.com/에서 고객 대면 서비스 상태 페이지를 유지 관리합니다. 이 페이지에는 CDO 서비스가 작동 중인지 여부와 서비스 중단 여부가 표시됩니다. 일별, 주별 또는 월별 그래프로 가동 시간 정보를 볼 수 있습니다.

CDO 서비스가 다운될 경우 상태 페이지에서 **Subscribe to Updates(**업데이트 구독**)**를 클릭하여 알림을 받을 수 있습니다.

CDO 지원 페이지

고객은 이제 CDO 인터페이스를 통해 지원을 받을 수 있습니다.

- 유료 고객은 새로운 Contact Support(지원 문의) 페이지에서 **Support Case Manager(**지원 케이스 관리자**)**를 클릭하여 Cisco의 TAC(Technical Assistance Center)에서 직접 지원 케이스를 열어야 합니다.
- 모든 데모, 내부 및 평가판 고객은 Contact Support(지원 문의) 페이지의 세부 정보 요청 양식에 질문을 입력하여 cdo.support@cisco.com으로 이메일을 보낼 수 있습니다. Cisco 지원 담당자가 최대한 빨리 응답해 드리겠습니다.



2017년 9월 7일

디바이스의 외부 링크

이제 외부 리소스에 대한 하이퍼링크를 생성하여 CDO로 관리하는 디바이스와 연결할 수 있습니다. 이 기능을 사용하여 검색 엔진, 설명서 리소스, 회사 Wiki 또는 선택한 다른 URL에 대한 편리한 링크를 만들 수 있습니다. 외부 링크를 원하는 만큼 디바이스에 연결할 수 있습니다. 동일한 링크를 여러 디바이스와 동시에 연결할 수도 있습니다.

2017년 8월

2017년 8월 17일

새 개체 함수

- 중복, 불일치 및 사용되지 않는 개체 해결: 개체 문제를 해결할 때 네트워크 및 서비스 개체에 대한 가시성이 향상됩니다. 그룹에 있는 모든 개체의 통합 보기가 표시되므로 개체를 더 쉽게 비교할 수 있습니다. 개체 문제를 병합, 이름 바꾸기 또는 무시하여 해결할 수 있는 명령 버튼도 있습니다.
- 새로운 개체 필터링: 찾고 있는 개체를 찾기 위한 더 정확한 검색 기능.

2017년 8월 10일

액티브/스탠바이 페일오버 쌍으로 구성된 **ASA**로 업그레이드

CDO는 액티브/스탠바이 페일오버 쌍으로 구성된 ASA 업그레이드를 포함하도록 업그레이드 마법사의 기능을 확장했습니다. 개별 ASA를 업그레이드할 때와 동일한 마법사 기능을 사용하지만 이제 액티브/스탠바이 페일오버 쌍을 업그레이드할 수 있습니다. 이 기능에 대한 자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리의 "액티브-스탠바이 쌍에서 ASA 및 ASDM 이미지 업그레이드"를 참조하십시오.

2017년 8월 3일

단일 상황 또는 다중 상황 모드에서 개별 **ASA**로 업그레이드

이제 CDO에서는 단일 또는 상황 또는 다중 상황 모드에서 개별 ASA에 설치된 ASA 및 ASDM 이미지를 업그레이드할 수 있는 마법사를 제공합니다. 백그라운드에서 필요한 모든 업그레이드 단계를 수행하여 프로세스를 쉽게 수행합니다. 마법사는 호환되는 ASA 소프트웨어 및 ASDM 이미지를 선택하고 설치하고 디바이스를 재부팅하여 업그레이드를 완료하는 프로세스를 안내합니다. Cisco에서는 CDO에서 선택한 이미지가 ASA에 복사되고 설치된 이미지인지 확인하여 업그레이드 프로세스를 보호합니다.

Devices & Services(디바이스 및 서비스) 페이지의 Details(세부 정보) 창에서 클릭하여 업그레이드를 시작합니다. 자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리의 "ASA 및 ASDM 이미지 업그레이드"를 참조하십시오.

2017년 6월

2017년 6월 20일

디바이스 및 서비스 목록 내보내기

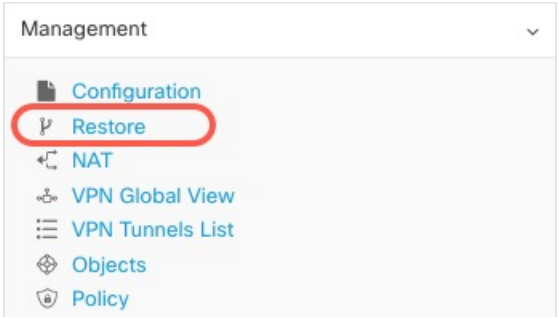
이제 **Inventory(**인벤토리**)** 페이지의 디바이스 및 서비스 목록을 쉼표로 구분된 값(.csv) 파일로 내보낼 수 있습니다. 여기에서 Microsoft Excel과 같은 스프레드시트 애플리케이션에서 파일을 열어 목록의 항목을 정렬하고 필터링할 수 있습니다.

자세한 내용은 Cisco Defense Orchestrator를 사용하여 FTD 관리의 "CSV 파일로 변경 로그 내보내기"를 참고하십시오.

2017년 6월 13일

ASA 구성 복원

이제 ASA를 이전에 저장한 구성 중 하나로 되돌릴 수 있습니다. 이는 예기치 않거나 원치 않는 결과를 초래한 구성 변경 사항을 편리하게 제거할 수 있는 방법입니다. 복원할 ASA 구성을 선택합니다. CDO는 해당 구성과 메모리에 저장된 마지막 구성을 비교하여 보여줍니다. 원하는 구성을 복원하는 것이 마음에 들면 복원할 수 있습니다.



자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리의 "ASA 구성 복원"을 참조하십시오.

2017년 5월

2017년 5월 3일

변경 요청 관리.

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

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "변경 요청 관리"를 참조하십시오.

2017년 4월

향상된 검색: 이제 Inventory(재고 목록) 페이지 검색 창에서 부분 일치를 지원하므로 원하는 디바이스 또는 서비스를 더 쉽게 찾을 수 있습니다.

VPN: 다양한 사용 편의성 개선.

2017년 2월

Cisco Defense Orchestrator 새 **EMEA** 사이트

AVC(Application Visibility Control) ID 프로파일 지원

2017년 1월

읽기 전용 **IPSec VPN** 터널 관리

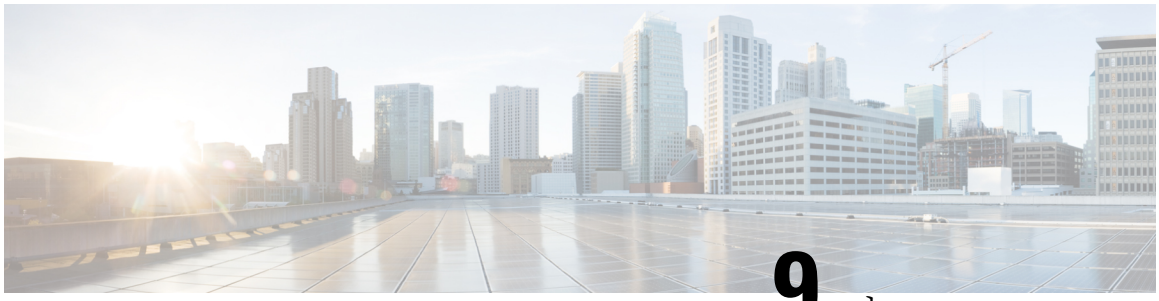
이제 Cisco Defense Orchestrator에서 IPsec Site-to-Site VPN ASA 디바이스 구성의 구문 분석 및 처리를 지원합니다. 네트워크 기반 VPN 터널 다이어그램을 사용할 수 있으며 단일 피어에 연결된 모든 터널의 전체 보기, 액세스 정책, 키 교환 암호화 및 연결 상태를 포함한 터널 세부 정보를 제공합니다. 또한 CDO는 조직의 온보딩된 ASA 디바이스의 구성에서 사용 가능한 모든 터널의 전체 보기를 제공합니다. CDO의 새로운 VPN 관리 기능은 조직 및 네트워크 운영 엔지니어에게 다음을 제공합니다.

- 디바이스 단위 및 모든 디바이스에 걸쳐 전체 VPN 터널 시각화
- 터널 연결 상태를 사용하여 터널 구성을 쉽게 식별하고 액세스 정책 및 cryptomap 암호화를 한눈에 볼 수 있습니다.

*VPN*은 안전하지만 안정적이고 안전한 통신을 보장하려면 올바르게 구성해야 합니다. *CDO*는 사용자가 *VPN* 구성의 조직 보기를 활성화하여 부풀려지고 오래된 정책을 줄이는 데 도움이 될 수 있습니다.

네트워크 및 서비스 단일 개체 지원

현재 사용 가능한 개체 그룹 지원 외에도 Cisco Defense Orchestrator에서는 액세스 규칙을 수정하는 동안 네트워크 및 서비스 유형의 단일 개체를 생성하거나 개체 페이지에서 직접 생성할 수 있습니다.



9 장

2016의 주요 기능

이 문서에서는 2016년에 Cisco Defense Orchestrator에 추가된 몇 가지 기능에 대해 설명합니다.

2016년 12월

2016년 12월 22일

NAT 정책 관리

이제 Cisco Defense Orchestrator에서는 사용하기 쉬운 탐색 마법사 및 고급 인터페이스 기반 다이어그램을 통해 NAT 정책 읽기, 수정, 검색 및 생성을 지원하여 ASA 디바이스에 정의된 NAT 정책(및 해당 순서)의 전체 목록을 표시합니다.

2016년 12월 15일

사용되지 않는 이름(개체) 변환

디바이스의 구성에 레거시(사용되지 않는) 이름이 포함되어 있습니까? 이제 Cisco Defense Orchestrator에서는 개체 문제를 해결하는 동안 개체, 개체 그룹 및 이름 전체를 조사하여 정책에 사용되는 모든 개체의 일관성을 제공하고 이름을 개체로 변환하는 작업을 지원합니다.

2016년 11월

2016년 11월 18일

완전하게 섀도잉된 규칙 지원

모든 트래픽은 규칙 집합 순서대로 규칙에 의해 처리되므로, 이제 의도된 트래픽을 처리하지 않는 불필요한 네트워크 정책을 필터링하고 식별할 수 있습니다. 네트워크 정책을 변경하면 CDO는 편집되거나 추가된 규칙이 다른 규칙에 의해 섀도잉되는 경우 경고를 보냅니다.

2016년 11월 8일

온프레미스 보안 디바이스 커넥터

Cisco Defense Orchestrator는 CDO와 지원되는 디바이스 및 서비스 간의 직접 통신을 활성화합니다. 이 통신은 원격 위치와 CDO 클라우드 서비스 간의 프록시 역할을 하는 CDO SDC(Secure Device Connector)에 의해 활성화됩니다. 이 서비스는 이제 다음과 같은 두 가지 구축 모델에서 사용할 수 있습니다.

On-Prem Secure Device Connector - On-Prem Secure Device Connector는 요청된 계정 전용으로 사전 구성된 가상 어플라이언스입니다.

클라우드 보안 디바이스 커넥터 – 모든 클라우드 보안 디바이스 커넥터는 Cisco Defense Orchestrator 팀에서 자동으로 프로비저닝되고 관리됩니다.

2016년 9월

2016년 9월 29일

변경 로그

온보딩된 디바이스 및 서비스 전체에서 단일 보기 내에서 Cisco Defense Orchestrator를 통해 수행되는 애플리케이션(layer7) 및 네트워크(layer3) 정책 변경 사항을 지속적으로 캡처합니다. 새로운 변경 로그는 최신 변경 사항을 한눈에 볼 수 있도록 나열하며, 디바이스, 변경 상태, 사용자 등을 기준으로 추가 수정을 정렬하고 필터링할 수 있습니다. 새로운 변경 로그 기능을 통해 조직은 다음을 수행할 수 있습니다.

- 네트워크 및 애플리케이션 정책 변경(신규, 수정 및 삭제된 규칙, 온보딩 또는 삭제된 디바이스 및 서비스 등)의 인라인 증분 보기(diff) 전과 후
- 정책 변경 충돌(Cisco Defense Orchestrator 외부에서 발생) 및 디바이스 또는 서비스에 대한 덮어쓰기 탐지

- 사고 조사 또는 트러블슈팅 중에 사용자, 대상 및 시기에 대한 답변 가능
- 공통 형식 또는 서드파티 모니터링 시스템으로 내보내기

Note 현재 Cisco Defense Orchestrator에서 관리하는 디바이스 및 서비스는 처음 구축하거나 읽은 후에만 변경 로그 이벤트 수집을 시작합니다. 자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "FTD 디바이스에 대한 보안 로깅 분석"을 참조하십시오.

적중률**.** 이제 Cisco Defense Orchestrator를 사용하면 네트워크 운영 사용자가 안전하고 확장 가능한 정책 오케스트레이션 외에 정책 규칙 결과를 평가할 수 있으므로, 클라우드의 단일 창에서 보다 정확한 정책 분석 및 근본 원인에 대한 즉각적인 조치 가능한 피벗을 위한 간단한 시각화를 제공할 수 있습니다. 새로운 적중률 기능을 통해 조직은 다음을 수행할 수 있습니다.

- 보안 상태를 증가하는 사용되지 않는 정책 규칙을 제거합니다.
- 병목 현상을 즉시 식별하여 방화벽 성능을 최적화하고 정확하고 효율적인 우선순위를 적용합니다(가장 많이 트리거되는 정책 규칙이 우선순위가 높음).
- 구성된 데이터 보존(1년)에 대한 디바이스 또는 정책 규칙 재설정 시에도 적중률 기록 정보 유지
- 실행 가능한 정보를 기반으로 의심스러운 섀도우 및 사용되지 않는 규칙에 대한 검증을 강화합니다. 업데이트 또는 삭제에 대한 의심 제거
- 사전 정의된 시간 간격(일, 주, 월, 연도) 및 실제 적중 횟수(0, >100, >100k 등)를 활용하여 전체 정책에 대한 컨텍스트에서 정책 규칙 사용을 시각화하여 네트워크를 통과하는 패킷에 대한 영향을 평가

2016년 9월 23일

사용자 인터페이스 재설계**:** 밝은 테마로 변경

Cisco Defense Orchestrator 사용자 경험을 보다 직관적이고 쉽게 설명할 수 있는 Cisco 스타일로 조정된 새로운 사용자 경험 테마로 재설계합니다. 사용해 보십시오!

다중 개체 지원

이제 Cisco Defense Orchestrator 개체 관리를 사용하면 개체 및 개체 그룹 값을 인라인으로 편집할 수 있을 뿐만 아니라 단일 액세스 목록 매개변수에서 여러 개체를 참조할 수 있습니다. 사용자 정의 개체 그룹에 자동으로 할당합니다(dm_inline_* 개체 생성 필요 없음).

대역외 정책 수정 승인 또는 거부

수행된 원격 변경 사항 또는 변경 사항(디바이스 또는 서비스에서)을 식별할 뿐만 아니라 식별된 대역 외 변경 사항을 실시간으로 승인하거나 거부하는 기능을 통해 정책 오케스트레이션 적용을 개선합니다.

2016년 8월

2016년 8월 18일

위임 관리자 지원

위임 관리자 지원. Cisco Defense Orchestrator를 사용하면 할당된 계정 간에 더 쉽고 빠르게 피벗할 수 있도록 사용자당 둘 이상의 단일 계정(테넌트)을 관리할 수 있으며, 계정 보안을 유지하고 계정(테넌트) 간에 완전한 데이터를 분리할 수 있습니다.

사전 정의 템플릿 가져오기 및 내보내기

사전 정의된 템플릿 가져오기를 활성화합니다. 조직에서 사용하거나 서드파티에서 제공하는 사전 정의된 디바이스 구성 템플릿을 활용하여 조직의 모든 디바이스 및 서비스를 온보딩하는 확장 가능한 오케스트레이션을 활성화합니다.

디바이스 및 서비스 연결 상태 관리

디바이스 연결 상태 평가. 디바이스 및 서비스 가용성 상태를 지속적으로 모니터링할 수 있도록 새로운 " *Reconnect(*다시 연결*)*" 버튼이 추가되었으며, 모든 변경 또는 작업에 대한 알림은 자동으로 또는 온디맨드 방식으로 수행되어야 합니다(예: 디바이스 자격 증명 업데이트, 디바이스 인증서 갱신).

2016년 8월 11일

향상된 템플릿 관리

템플릿 개선 사항을 관리합니다. 새 디바이스 템플릿 구성 파일을 생성하거나 기존 디바이스 템플릿 구성 파일을 업데이트할 때, Cisco Defense Orchestrator 사용자는 이제 디바이스 구성 파일 전체에서 쉽게 검색할 수 있으며, 어카운트의 디바이스 전체에서 사용할 수 있도록 새 매개변수 또는 기존 매개변수에 여러 값을 할당할 수 있습니다.

. 템플릿 생성 및 관리에 대한 자세한 내용은 Cisco Defense Orchestrator를 사용하여 FTD 관리의 "템플릿"을 참조하십시오.

II 부

클라우드 제공 Firewall Management Center의 새로운 기능

10 장

클라우드 제공 Firewall Management Center 2024의 새로운 기능

2024년 6월 6일

Cisco AI Assistant를 사용한 **Firewall** 관리

CDO 관리자는 이제 CDO(Cisco Defense Orchestrator)의 Cisco AI Assistant와 클라우드에서 제공하는 Firewall Management Center의 통합을 통해 Secure Firewall Threat Defense 정책을 더욱 효율적으로 관리할 수 있습니다. Cisco AI Assistant에는 다음과 같은 몇 가지 주요 기능이 있습니다.

- **Pre-Enabled Assistant(**사전 활성화된 어시스턴트**)**: AI Assistant는 모든 CDO 테넌트에서 기본적으로 활성화됩니다. 필요한 경우 테넌트의 General Settings(일반 설정) 페이지에서 비활성화할 수 있습니다.
- 간편한 액세스: CDO 최고 관리자 및 관리자는 로그인한 후 테넌트 대시보드의 상단 메뉴 모음에서 AI Assistant에 직접 액세스할 수 있습니다.

- **User Orientation(**사용자 방향**)**: AI Assistant 위젯을 처음 열면 사용자가 AI Assistant를 소개하고, 데이터 개인정보 보호에 대해 설명하며, 효과적인 사용을 위한 팁을 제공하는 회전식 창이 반깁니다.
- **Policy Rule Assistance(**정책 규칙 지원**)**: AI Assistant는 Secure Firewall Threat Defense 디바이스의 정책 규칙 생성 프로세스를 간소화합니다. 관리자는 간단한 프롬프트를 사용하여 액세스 제어 규칙을 신속하게 생성할 수 있습니다.

- **Product Knowledge Resource(**제품 지식 리소스**)**: AI Assistant는 CDO 및 클라우드 제공 방화벽 관리 문서를 수집했습니다. 도움이 필요한 경우 질문할 수 있습니다.
- 사용자 친화적 인터페이스:
  - **Simple Text Input Box(**단순 텍스트 입력 상자**)**: 어시스턴트를 쉽게 사용할 수 있도록 창 하단에 있습니다.
  - **Thread History(**스레드 기록**)**: AI Assistant에게 묻는 질문 또는 일련의 질문을 스레드라고 합니다. AI Assistant는 스레드 기록을 유지하므로 이미 한 질문을 참조할 수 있습니다.
  - **Feedback(**피드백**)**: 어시스턴트의 응답에 대해 좋음 또는 반대로 피드백을 제공합니다.

자세한 내용은 Cisco AI Assistant 사용 가이드를 참조하십시오.

2024년 5월 30일

표 *1:* 버전 ***20240514*** 기능

기능	최소 **Threat Defense**	세부 정보
플랫폼 마이그레이션		
클러스터된 Threat Defense 디바이스를 온프레미스 Management Center에서 클라우드 제공 Firewall Management Center로 마이그레이션합니다.	7.0.6 7.2.1	클러스터된 Secure Firewall Threat Defense 디바이스는 이제 온프레미스 Management Center에서 클라우드 제공 Firewall Management Center로 마이그레이션할 때 나머지 구성과 함께 마이그레이션됩니다. 참조: 온프레미스 Management Center 관리 Secure Firewall Threat Defense를 클라우드 제공 Firewall Management Center로 마이그레이션
구축 및 정책 관리		
변화 관리.	Any(모든)	조직에서 변경 사항을 구축하기 전에 감사 추적 및 공식 승인을 포함하여 구성 변경에 대한 보다 공식적인 프로세스를 구현해야 하는 경우 변화 관리를 활성화할 수 있습니다. 이 기능을 활성화하기 위해 시스템 (⚙) > **Configuration(**구성**)** > **Change Management(**변경 관리**)** 페이지가 추가되었습니다. 활성화하면 시스템 (⚙) > **Change Management Workflow(**변경 관리 워크플로우**)** 페이지와 메뉴에 새로운 **Ticket(**티켓**)** ( ) 빠른 액세스 아이콘이 나타납니다. 참조: 변화 관리

2024년 4월 2일

이 릴리스에서는 안정성, 강화 및 성능 향상을 소개합니다.

2024년 2월 13일

표 *2:* 버전 *20240203* 기능

기능	최소 **Threat Defense**	세부정보
플랫폼		
Threat Defense 버전 7.4.1 지원.	7.4.1	이제 버전 7.4.1을 실행하는 Threat Defense 디바이스를 관리할 수 있습니다.
Secure Firewall 3130 및 3140용 네트워크 모듈	7.4.1	Secure Firewall 3130 및 3140은 이제 다음 네트워크 모듈을 지원합니다. • 2포트 100G QSFP+ 네트워크 모듈(FPR3K-XNM-2X100G) 참조: Cisco Secure Firewall 3110, 3120, 3130 및 3140 하드웨어 설치 설명서
Firepower 9300 네트워크 모듈용 광학 트렌시버입니다.	7.4.1	Firepower 9300은 이제 다음 광학 트렌시버를 지원합니다. • QSFP-40/100-SRBD • QSFP-100G-SR1.2 • QSFP-100G-SM-SR 다음 네트워크 모듈에서는 아래와 같습니다. • FPR9K-NM-4X100G • FPR9K-NM-2X100G • FPR9K-DNM-2X100G 참조: Cisco Firepower 9300 하드웨어 설치 가이드
Secure Firewall 3100에 대한 성능 프로파일 지원.	7.4.1	이제 플랫폼 설정 정책에서 사용 가능한 성능 프로파일 설정이 Secure Firewall 3100에 적용됩니다. 이전에는 이 기능이 Firepower 4100/9300, Secure Firewall 4200 및 Threat Defense Virtual에서 지원되었습니다. 참조: 성능 프로파일 구성
NAT		

기능	최소 **Threat Defense**	세부정보
NAT 규칙을 편집하는 동안 네트워크 그룹을 생성합니다.	Any(모든)	이제 NAT 규칙을 편집하면서 네트워크 개체 외에 네트워크 그룹을 생성할 수 있습니다. 참조: 여러 디바이스에 대한 NAT 규칙 사용자 지정
디바이스 관리		
사용자 정의 VRF 인터페이스에서 지원되는 디바이스 관리 서비스.	Any(모든)	Threat Defense 플랫폼 설정(NetFlow, SSH 액세스, SNMP 호스트, 시스템 로그 서버)에서 구성된 디바이스 관리 서비스는 이제 사용자 정의 VRF(가상 라우팅 및 포워딩) 인터페이스에서 지원됩니다. 플랫폼 제한: 컨테이너 인스턴스 또는 클러스터된 디바이스에서는 지원되지 않습니다. 참조: 플랫폼 설정
SD-WAN		
SD-WAN 요약 대시보드	7.4.1	WAN Summary(WAN 요약) 대시보드는 WAN 디바이스 및 해당 인터페이스의 스냅샷을 제공합니다. WAN 네트워크에 대한 인사이트와 디바이스 상태, 인터페이스 연결, 애플리케이션 처리량 및 VPN 연결에 대한 정보를 제공합니다. WAN 링크를 모니터링하고 사전 및 신속한 복구 조치를 수행할 수 있습니다. 또한 **Application Monitoring(**애플리케이션 모니터링**)** 탭을 사용하여 WAN 인터페이스 애플리케이션 성능을 모니터링할 수도 있습니다. 신규/수정된 화면: **Analysis(**분석**)** > **SD-WAN Summary(SD-WAN** 요약**)** 참조: SD-WAN 요약 대시보드
액세스 제어**: ID**		

기능	최소 **Threat Defense**	세부정보
여러 Active Directory 영역(영역 시퀀스)에 대한 캡티브 포털 지원.	7.4.1	업그레이드 영향**.** 사용자 지정 인증 양식을 업데이트합니다**.** LDAP 영역이나 Microsoft Active Directory 영역 또는 영역 시퀀스에 대해 활성 인증을 구성할 수 있습니다. 또한 영역 또는 영역 시퀀스를 사용하여 활성 인증으로 폴백되는 패시브 인증 규칙을 구성할 수 있습니다. 필요에 따라 액세스 제어 규칙에서 동일한 ID 정책을 공유하는 매니지드 디바이스 간에 세션을 공유할 수 있습니다. 또한 사용자가 이전에 액세스한 것과 다른 매니지드 디바이스를 사용하여 시스템에 액세스할 때 다시 인증을 요구할 수도 있습니다. HTTP Response(HTTP 응답) 페이지 인증 유형을 사용하는 경우 Threat Defense를 업그레이드한 뒤 사용자 지정 인증 양식에 **`<select name="realm" id="realm"></select>`**를 추가해야 합니다. 이를 통해 사용자는 영역을 선택할 수 있습니다. 제한 사항: Microsoft Azure Active Directory에서 지원되지 않습니다. 신규/수정된 화면: • **Policies(**정책**)** > **Identity(ID)** > **(**정책 편집**)** > **Active Authentication(**활성 인증**)** > **Share active authentication sessions across firewalls(**방화벽을 통해 활성 인증 세션 공유**)** • **Identity policy(ID** 정책**)** > **(**편집**)** > **Add Rule(**규칙 추가**)** > **Passive Authentication(**패시브 인증**)** > **Realms & Settings(**영역 및 설정**)** > **Use active authentication if passive or VPN identity cannot be established(**패시브 또는 **VPN ID**를 설정할 수 없는 경우 활성 인증 사용**)** • **Identity policy(ID** 정책**)** > **(**편집**)** > **Add Rule(**규칙 추가**)** > **Active Authentication(**활성 인증**)** > **Realms & Settings(**영역 및 설정**)** > **Use active authentication if passive or VPN identity cannot be established(**패시브 또는 **VPN ID**를 설정할 수 없는 경우 활성 인증 사용**)** 참조: 사용자 제어에 대한 캡티브 포털 구성 방법

기능	최소 **Threat Defense**	세부정보
방화벽 전체에서 캡티브 포털 활성 인증 세션 공유.	7.4.1	인증 세션이 이전에 연결했던 디바이스가 아닌 다른 매니지드 디바이스로 전송될 때 사용자에게 인증을 하도록 해야 하는지 여부를 결정합니다. 조직에서 사용자가 위치 또는 사이트를 변경할 때마다 인증을 요구하는 경우 이 옵션을 비활성화해야 합니다. • (기본값) 사용자가 활성 인증 ID 규칙과 연결된 매니지드 디바이스에 인증하도록 허용하려면 활성화합니다. • 활성 인증 규칙이 구축된 다른 매니지드 디바이스에서 이미 인증을 한 경우에도, 사용자가 다른 매니지드 디바이스를 통해 인증해야 하는 경우에는 비활성화합니다. 신규/수정된 화면: **Policies(**정책**)** > **Identity(ID)** > **(**정책 편집**)** > **Active Authentication(**활성 인증**)** > **Share active authentication sessions across firewalls(**방화벽을 통해 활성 인증 세션 공유**)** 참조: 사용자 제어에 대한 캡티브 포털 구성 방법
구축 및 정책 관리		
마지막 구축 이후의 구성 변경에 대한 보고서 조회 및 생성.	모두	마지막 구축 이후 구성 변경에 대한 다음 보고서를 생성, 확인 및 다운로드(zip 파일)할 수 있습니다. • 각 디바이스에 대한 정책 변경 보고서에서 정책의 추가, 변경, 삭제 또는 디바이스에 구축할 개체를 미리 봅니다. • 통합 보고서는 정책 변경 보고서 생성 상태에 따라 각 디바이스를 분류합니다. 이는 Threat Defense 디바이스를 업그레이드한 후에 구축하기 전 업그레이드에서 변경된 사항을 확인할 수 있도록 하는 데 특히 유용합니다. 신규/수정된 화면: **Deploy(**구축**)** > **Advanced Deploy(**고급 구축**)**. 참조: 여러 디바이스에 대한 다운로드 정책 변경 보고서
제안된 릴리스 알림.	모두	새로운 제안 릴리스가 제공되면 Management Center에서 알림을 보냅니다. 지금 업그레이드하지 않으려면 시스템에서 나중에 알림을 보내도록 하거나 다음 제안 릴리스까지 알림을 연기할 수 있습니다. 새 업그레이드 페이지에는 제안된 릴리스도 표시됩니다. 참조: Cisco Secure Firewall Management Center의 릴리스별 새로운 기능
Threat Defense 업그레이드 마법사에서 되돌리기 활성화.	모두	이제 Threat Defense 업그레이드 마법사에서 되돌리기를 활성화할 수 있습니다. 기타 버전 제한: Threat Defense를 버전7.2이상으로 업그레이드해야 합니다. 참조: 클라우드 제공 Firewall Management Center용 Cisco Secure Firewall Threat Defense 업그레이드 가이드

기능	최소 **Threat Defense**	세부정보
Threat Defense 업그레이드 마법사에서 자세한 업그레이드 상태 보기.	모두	이제 Threat Defense 업그레이드 마법사의 마지막 페이지에서 업그레이드 진행 상황을 모니터링할 수 있습니다. 이 기능은 Device Management(디바이스 관리) 페이지의 Upgrade(업그레이드) 탭 및 Message Center에서 기존 모니터링 기능으로 추가됩니다. 새 업그레이드 플로우를 시작하지 않은 경우 **Devices(**디바이스**)** > **Threat Defense Upgrade(Threat Defense** 업그레이드**)**를 사용하면 현재(또는 가장 최근에 완료된) 디바이스 업그레이드의 세부 상태를 확인할 수 있는 마지막 마법사 페이지로 돌아갑니다. 참조: 클라우드 제공 Firewall Management Center용 Cisco Secure Firewall Threat Defense 업그레이드 가이드
FXOS 업그레이드에 포함되는 펌웨어 업그레이드.	모두	새시**/FXOS** 업그레이드 영향**.** 펌웨어 업그레이드로 인해 추가 재부팅이 발생합니다**.** Firepower 4100/9300의 경우, 이제 버전 2.14.1로의 FXOS 업그레이드에는 펌웨어 업그레이드가 포함됩니다. 디바이스의 펌웨어 구성 요소가 FXOS 번들에 포함된 것보다 오래된 경우, FXOS 업그레이드 시 펌웨어도 업데이트됩니다. 펌웨어가 업그레이드되면 디바이스가 두 번(FXOS용으로 한 번, 펌웨어용으로 한 번) 재부팅됩니다. 소프트웨어 및 운영 체제를 업그레이드할 때와 마찬가지로 펌웨어 업그레이드 중에는 구성을 변경하거나 구축하지 마십시오. 시스템이 비활성 상태로 나타나더라도 펌웨어 업그레이드 중에 수동으로 재부팅하거나 종료하지 마십시오. 참조: Cisco Firepower 4100/9300 업그레이드 가이드
업그레이드		

기능	최소 **Threat Defense**	세부정보
업그레이드 시작 페이지 및 패키지 관리 개선.	Any(모든)	새로운 업그레이드 페이지를 사용하면 업그레이드를 더 쉽게 선택하고, 다운로드하고, 관리하고, 전체 구축에 적용할 수 있습니다. 이 페이지에는 현재 구축에 적용되는 모든 업그레이드 패키지가 나열되며, 제안된 릴리스는 특별히 표시됩니다. Cisco에서 패키지를 쉽게 선택하고 직접 다운로드할 수 있으며 수동으로 패키지를 업로드하고 삭제할 수 있습니다. 해당 유지 보수 릴리스에 적어도 하나의 어플라이언스가 있는 경우(또는 패치를 수동으로 업로드한 경우) 패치는 나열되지 않습니다. 핫픽스를 수동으로 업로드해야 합니다. 신규/수정된 화면: • 시스템 (⚙) > 제품 업그레이드를 통해 이제 디바이스를 업그레이드하고 업그레이드 패키지를 관리할 수 있습니다. • 시스템 (⚙) > **Content Updates(**콘텐츠 업데이트**)**에서는 이제 침입 규칙, VDB, GeoDB를 업데이트할 수 있습니다. • **Devices(**디바이스**) > Threat Defense Upgrade(Threat Defense** 업그레이드**)**를 사용하면 Threat Defense 업그레이드 마법사로 바로 이동합니다. 지원이 중단된 화면/옵션: • 시스템 (⚙) > **Updates(**업데이트**)**는 더 이상 사용되지 않습니다. 이제 모든 Threat Defense 업그레이드가 마법사를 사용합니다. • Threat Defense 업그레이드 마법사의 **Add Upgrade Package(**업그레이드 패키지 추가**)** 버튼이 새 업그레이드 페이지로 연결되는 **Manage Upgrade Packages(**업그레이드 패키지 관리**)** 링크로 교체되었습니다. 참조: 클라우드 제공 Firewall Management Center용 Cisco Secure Firewall Threat Defense 업그레이드 가이드
관리		
소프트웨어 업그레이드 직접 다운로드에 대한 인터넷 액세스 요구 사항을 업데이트했습니다.	모두	Management Center 소프트웨어 업그레이드 패키지의 직접 다운로드 위치를 sourcefire.com에서 amazonaws.com으로 변경했습니다. 참조: 인터넷 액세스 요구 사항
예약된 작업은 패치와 VDB 업데이트만 다운로드합니다.	모두	**Download Latest Update(**최신 업데이트 다운로드**)** 예약 작업은 유지 보수 릴리스를 더 이상 다운로드하지 않습니다. 이제 적용 가능한 최신 패치와 VDB 업데이트만 다운로드합니다. 유지 보수(및 주요) 릴리스를 Management Center에 직접 다운로드하려면 시스템 (⚙) > **Product Upgrades(**제품 업그레이드**)**를 사용하십시오. 참조: 소프트웨어 업데이트 자동화

기능	최소 **Threat Defense**	세부정보
Snort 2	Snort 2를 포함하는 모두	VDB 363 이상의 경우 시스템은 이제 Snort 2를 실행하는 메모리가 적은 디바이스에 더 작은 VDB(*VDB lite*라고도 함)를 설치합니다. 더 작은 VDB에는 동일한 애플리케이션이 포함되어 있지만, 탐지 패턴이 더 적습니다. 더 작은 VDB를 사용하는 디바이스는 전체 VDB를 사용하는 디바이스에 비해 일부 애플리케이션 식별을 누락할 수 있습니다. 더 낮은 메모리 디바이스: ASA-5508-X, ASA 5516-X 참조: 취약성 데이터베이스 업데이트
지원 중단된 기능		
사용 중단됨: FlexConfig와 함께 DHCP 릴레이 신뢰할 수 있는 인터페이스.	모두	이제 Management Center 웹 인터페이스를 통해 인터페이스를 신뢰할 수 있는 인터페이스로 구성하여 DHCP 옵션 82를 유지할 수 있습니다. 이렇게 하면 기존 FlexConfig를 제거해야 하지만, 이러한 설정은 모든 FlexConfig를 재정의합니다. 참조: DHCP 릴레이 에이전트 구성
사용되지 않음: 다운로드 가능한 액세스 제어 목록을 FlexConfig를 사용하는 RADIUS ID 소스에 대한 Cisco 속성-값 쌍 ACL과 병합.	모두	이 기능은 이제 Management Center 웹 인터페이스에서 지원됩니다.
사용 중단됨: 이벤트 상태 알림의 빈번한 소모.	7.4.1	Disk Usage(디스크 사용량) 상태 모듈에서 더 이상 빈번한 이벤트 소모로 알림을 보내지 않습니다. 매니지드 디바이스에 상태 정책을 구축하거나(알림 표시 중지), 디바이스를 버전 7.4.1 이상으로 업그레이드(알림 전송 중지)할 때까지 이러한 알림이 계속 표시될 수 있습니다. 참조: 이벤트 상태 모니터 알림의 디스크 사용량 및 소모

11 장

클라우드 제공 Firewall Management Center 2023의 새로운 기능

2023년 11월 30일

표 *3:* 새로운 기능*:* 버전 ***20231117***

기능	최소 **Threat Defense**	세부정보
관리		
클라우드 제공 Firewall Management Center에 Secure Firewall Threat Defense 디바이스 백업 예약	모두	클라우드 제공 Firewall Management Center를 사용하여 관리하는 Secure Firewall Threat Defense 디바이스의 예약된 백업을 수행합니다. 자세한 내용은 원격 디바이스 백업 예약을 참조하십시오.

2023년 10월 19일

표 ***4:*** 새로운 기능***:*** 버전 ***20230929***

기능	최소 **Threat Defense**	세부정보
플랫폼		
Threat Defense 버전 7.4.0 지원.	7.4.0	이제 버전 7.4.0을 실행하는 Threat Defense 디바이스를 관리할 수 있습니다. 7.4.0 버전은 Secure Firewall 4200에서만 사용 가능합니다. 버전 7.4.0이 필요한 기능의 경우 Secure Firewall 4200을 사용해야 합니다. 기타 모든 플랫폼에 대한 지원은 7.4.1 버전에서 다시 시작됩니다.
Secure Firewall 4200.	7.4.0	이제 클라우드 제공 Firewall Management Center를 사용하여 Secure Firewall 4215, 4225 및 4245를 관리할 수 있습니다. 이러한 디바이스는 다음의 새로운 네트워크 모듈을 지원합니다. • 2포트 100G QSFP+ 네트워크 모듈(FPR4K-XNM-2X100G) • 4포트 200G QSFP+ 네트워크 모듈(FPR4K-XNM-4X200G) 참조: Cisco Secure Firewall 4215, 4225 및 4245 하드웨어 설치 가이드
Secure Firewall 4200에 대한 성능 프로파일 지원.	7.4.0	이제 플랫폼 설정 정책에서 사용 가능한 성능 프로파일 설정이 Secure Firewall 4200에 적용됩니다. 이전에는 이 기능이 Firepower 4100/9300 및 Threat Defense Virtual에서만 지원되었습니다. 참조: 성능 프로파일 구성
클라우드에서 제공 Firewall Management 시스템의 번호지정 규칙입니다.	모두	클라우드 제공 Firewall Management 시스템은 CDO의 기능입니다. 문제 해결을 위해 FMC 서비스 페이지에서 클라우드 제공 Firewall Management Center의 버전 번호를 식별합니다. 참조: 서비스 페이지 정보 보기
플랫폼 마이그레이션		
Firepower 1000/2100에서 Secure Firewall 3100으로 마이그레이션.	모두	이제 Firepower 1000/2100에서 Secure Firewall 3100으로 구성을 쉽게 마이그레이션할 수 있습니다. 신규/수정된 화면: **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Migrate(**마이그레이션**)** 플랫폼 제한: Firepower 1010 또는 1010E에서 마이그레이션이 지원되지 않습니다. 참조: 새 모델로 구성 마이그레이션.

기능	최소 **Threat Defense**	세부정보
Firepower Management Center 1000/2500/4500에서 클라우드 제공 Firewall Management Center로 디바이스를 마이그레이션합니다.	모두	

기능	최소 **Threat Defense**	세부정보
		Firepower Management Center 1000/2500/4500에서 클라우드 제공 Firewall Management Center. 디바이스를 마이그레이션하려면 온프레미스 Management Center를 버전 7.0.3(7.0.5 권장)에서 버전 7.4.0으로 일시적으로 업그레이드해야 합니다. 버전 7.0 Management Center에서는 클라우드로의 디바이스 마이그레이션을 지원하지 않으므로, 이 임시 업그레이드가 필요합니다. 또한 버전 7.0.3 이상(7.0.5 권장)을 실행하는 독립형 및 고가용성 Threat Defense 디바이스만 마이그레이션에 적합합니다. 클러스터 마이그레이션은 현재 지원되지 않습니다. 중요 버전 7.4.0은 마이그레이션 프로세스가 진행되는 동안 1000/2500/4500에서만 지원됩니다. Management Center 업그레이드와 디바이스 마이그레이션 간의 시간을 최소화해야 합니다. 마이그레이션 프로세스를 요약하면 다음과 같습니다. **1.** 업그레이드 및 마이그레이션을 준비합니다. 릴리스 노트, 업그레이드 설명서, 마이그레이션 가이드에 요약된 모든 사전 요건을 읽고, 이해하고, 충족합니다. 업그레이드하기 전에 온프레미스 Management Center가 "준비된 상태"여야 합니다. 즉 마이그레이션할 디바이스만 관리하고, VPN 영향 등 구성 영향을 평가하고, 새로 구축되었고, 완전히 백업되었고, 모든 어플라이언스가 정상적으로 작동하는지 여부 등을 확인하는 것이 중요합니다. 또한 클라우드 테넌트를 프로비저닝하고, 라이선스를 부여하고, 준비해야 합니다. 여기에는 보안 이벤트 로깅에 대한 전략을 포함해야 합니다. 지원되지 않는 버전을 실행하므로, 애널리틱스를 위해 온프레미스 Management Center를 유지할 수 없습니다. **2.** 온프레미스 Management Center 및 모든 매니지드 디바이스를 버전 7.0.3 이상(버전 7.0.5 권장)으로 업그레이드합니다. 최소 버전을 이미 실행하고 있는 경우 이 단계를 건너뛸 수 있습니다. **3.** 온프레미스 Management Center를 버전 7.4.0으로 업그레이드합니다. 업그레이드 패키지를 Management Center에 업로드하기 전에 압축을 풉니다(untar 제외). 다운로드 위치: 특별 릴리스. **4.** 온프레미스 Management Center를 CDO에 온보딩합니다. **5.** 마이그레이션 가이드에 설명된 대로, 모든 디바이스를 온프레미스 Management Center에서 클라우드 제공 Firewall Management Center로 마이그레이션합니다. 마이그레이션할 디바이스를 선택할 때는 **Delete FTD from On-Prem FMC(**온프레미스 **FMC**에서 **FTD** 삭제**)**를 선택해야 합니다. 변경 사항을 커밋하거나 14일이 경과하지 않는 한 디바이스는 완전히 삭제되지 않습니다.

기능	최소 **Threat Defense**	세부정보
		6. 마이그레이션 성공을 확인합니다. 마이그레이션이 예상대로 작동하지 않는 경우, 14일 이내에 원래대로 되돌리지 않으면 자동으로 커밋됩니다. 그러나 버전 7.4.0은 일반적인 작업에 지원되지 않습니다. 온프레미스 Management Center를 지원되는 버전으로 되돌리려면 마이그레이션된 디바이스를 제거하고, 버전 7.0.x로 이미지를 다시 설치하고, 백업에서 복원한 다음 디바이스를 재등록해야 합니다. 참조: • Cisco Secure Firewall Threat Defense 릴리스 노트 • Cisco Firepower Management Center 업그레이드 설명서, 버전 6.0–7.0 • 온프레미스 Management Center 매니지드 Secure Firewall Threat Defense를 클라우드 제공 Firewall Management Center로 마이그레이션 마이그레이션 프로세스의 어느 시점에서든 질문이 있거나 지원이 필요할 경우 Cisco TAC에 문의해 주십시오.
FTD에서 클라우드로의 마이그레이션에서 S2S VPN 지원. VPN 정책이 포함된 Threat Defense 디바이스를 온프레미스에서 클라우드 제공 Firewall Management Center로 마이그레이션합니다.	7.0.3-7.0.x 7.2 이상	디바이스를 온프레미스 Firewall Management Center에서 클라우드 제공 Firewall Management Center로 마이그레이션할 때, 이제 Secure Firewall Threat Defense 디바이스의 사이트 간 VPN 구성은 나머지 구성과 함께 마이그레이션됩니다. 참조 : 온프레미스 Management Center 매니지드 Secure Firewall Threat Defense를 클라우드 제공 Firewall Management Center로 마이그레이션
인터페이스		

기능	최소 **Threat Defense**	세부정보
관리 및 진단 인터페이스 병합.	7.4.0	업그레이드 영향**.** 업그레이드 후 인터페이스를 병합합니다**.** 7.4 이상 버전을 사용하는 새 디바이스의 경우 레거시 진단 인터페이스를 사용할 수 없습니다. 병합된 관리 인터페이스만 사용할 수 있습니다. 7.4 이상으로 업그레이드하고 다음의 경우: • 진단 인터페이스에 대한 구성이 없는 경우 인터페이스가 자동으로 병합됩니다. • 진단 인터페이스에 대한 구성이 있는 경우 인터페이스를 수동으로 병합하거나 별도의 진단 인터페이스를 계속 사용할 수 있습니다. 진단 인터페이스에 대한 지원은 이후 릴리스에서 제거되므로 가능한 빨리 인터페이스를 병합해야 합니다. 병합 모드는 기본적으로 데이터 라우팅 테이블을 사용하도록 AAA 트래픽의 동작을 변경합니다. 관리 전용 라우팅 테이블은 설정에서 관리 전용 인터페이스(관리 포함)를 지정한 경우에만 사용할 수 있습니다. 플랫폼 설정의 경우, 다음을 의미합니다. • 더 이상 진단을 위해 HTTP, ICMP 또는 SMTP를 활성화할 수 없습니다. • SNMP의 경우, 진단 대신 관리에서 호스트를 허용할 수 있습니다. • 시스템 로그 서버의 경우, 진단 대신 관리에서 연결할 수 있습니다. • 시스템 로그 서버 또는 SNMP 호스트에 대한 플랫폼 설정에서 이름으로 진단 인터페이스를 지정하는 경우, 병합된 디바이스와 병합되지 않은 디바이스에 대해 별도의 플랫폼 설정 정책을 사용해야 합니다. • 인터페이스를 지정하지 않으면 DNS 조회가 더 이상 관리 전용 라우팅 테이블로 대체되지 않습니다. 신규/수정된 화면: **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interfaces(**인터페이스**)** 신규/수정된 명령: **show management-interface convergence** 참조: 관리 및 진단 인터페이스 병합

기능	최소 **Threat Defense**	세부정보
VXLAN VTEP IPv6 지원.	7.4.0	이제 VXLAN VTEP 인터페이스에 대한 IPv6 주소를 지정할 수 있습니다. IPv6는 Threat Defense Virtual 클러스터 제어 링크 또는 Geneve 캡슐화에 대해 지원되지 않습니다. 신규/수정된 화면: • **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Edit Device(**디바이스 편집**)** > **VTEP** > **Add VTEP(VTEP** 추가**)** • **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Edit Devices(**디바이스 편집**)** > **Interfaces(**인터페이스**)** > **Add Interfaces(**인터페이스 추가**)** > **VNI Interface(VNI** 인터페이스**)** 참조: Geneve 인터페이스 구성
BGP 및 관리 트래픽에 대한 루프백 인터페이스 지원.	7.4.0	이제 AAA, BGP, DNS, HTTP, ICMP, IPsec 플로우 오프로드, NetFlow, SNMP, SSH 및 시스템 로그에 루프백 인터페이스를 사용할 수 있습니다. 신규/수정된 화면: **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > Edit device(디바이스 편집) > **Interfaces(**인터페이스**)** > **Add Interfaces(**인터페이스 추가**)** > **Loopback Interface(**루프백 인터페이스**)** 참조: 루프백 인터페이스 구성
루프백 및 관리 유형 인터페이스 그룹 개체.	7.4.0	관리 전용 또는 루프백 인터페이스로만 인터페이스 그룹 개체를 만들 수 있습니다. DNS 서버, HTTP 액세스 또는 SSH와 같은 관리 기능에 이러한 그룹을 사용할 수 있습니다. 루프백 인터페이스를 활용할 수 있는 모든 기능에 루프백 그룹을 사용할 수 있습니다. 그러나 DNS는 관리 인터페이스를 지원하지 않습니다. 신규/수정된 화면: **Objects(**개체**)** > **Object Management(**개체 관리**)** > **Interface(**인터페이스**)** > **Add(**추가**)** > **Interface Group(**인터페이스 그룹**)** 참조: 인터페이스
고가용성/확장성		
Threat Defense 고가용성을 위한 "잘못된 페일오버" 감소	7.4.0	기타 버전 제한: Threat Defense 버전 7.3.x에서는 지원되지 않습니다. 참조: 하트비트 모듈 리던던시(redundancy)
SD-WAN		

기능	최소 **Threat Defense**	세부정보
HTTP 경로 모니터링을 사용 하는 정책 기반 라우팅.	7.2.0	PBR(정책 기반 라우팅)은 이제 특정 대상 IP의 메트릭 대신 애플리케이션 도메인의 HTTP 클라이언트를 통해 경로 모니터링으로 수집된 성능 메트릭(RTT, 지터(Jitter), 패킷 손실 및 MOS)을 사용할 수 있습니다. HTTP 기반 애플리케이션 모니터링 옵션은 인터페이스에 대해 기본적으로 활성화되어 있습니다. 모니터링되는 애플리케이션과 경로 결정에 인터페이스 순서가 있는 일치 ACL을 사용하여 PBR 정책을 구성할 수 있습니다. 신규/수정된 화면: **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > Edit device(디바이스 편집) > Edit interface(인터페이스 편집) > **Path Monitoring(**경로 모니터링**)** > **Enable HTTP based Application Monitoring(HTTP** 기반 애플리케이션 모니터링 활성화**)** 체크 박스. 플랫폼 제한: 클러스터된 디바이스에서는 지원되지 않습니다. 참조: 경로 모니터링 설정 구성
사용자 ID 및 SGT를 사용하는 정책 기반 라우팅.	7.4.0	이제 사용자 및 사용자 그룹과 PBR 정책의 SGT를 기준으로 네트워크 트래픽을 분류할 수 있습니다. PBR 정책에 대한 확장 ACL을 정의하는 동안 ID 및 SGT 개체를 선택할 수 있습니다. 신규/수정된 화면: **Objects(**개체**)** > **Object Management(**개체 관리**)** > **Access List(**액세스 목록**)** > **Extended(**확장**)** > Add/Edit Extended Access List(확장 액세스 목록 추가/편집) > Add/Edit Extended Access List Entry(확장 액세스 목록 항목 추가/편집) > **Users(**사용자**)** 및 **Security Group Tag(**보안 그룹 태그**)** 참조: 확장 ACL 개체 구성
VPN		
Secure Firewall 4200에 대한 VTI 루프백 인터페이스의 IPsec 플로우 오프로드	7.4.0	Secure Firewall 4200에서는 VTI 루프백 인터페이스를 통한 적격 IPsec 연결이 기본적으로 오프로드됩니다. 이전에는 이 기능이 Secure Firewall 3100의 물리적 인터페이스에 지원되었습니다. FlexConfig 및 **flow-offload-ipsec** 명령을 사용하여 구성을 변경할 수 있습니다. 기타 요구 사항: FPGA 펌웨어 6.2 이상 참조: IPSec 플로우 오프로드

기능	최소 **Threat Defense**	세부정보
Secure Firewall 4200에 대한 암호화 디버깅 개선 사항.	7.4.0	암호화 디버깅이 다음과 같이 개선되었습니다. • 암호화 아카이브는 이제 텍스트 및 바이너리 형식으로 제공됩니다. • 추가 SSL 카운터를 디버깅에 사용할 수 있습니다. • 디바이스를 재부팅하지 않고 ASP 테이블에서 중단된 암호화 규칙을 제거합니다. 신규/수정된 CLI 명령: **show counters** 참조: 암호화 아카이브 사용 문제 해결
VPN: 원격 액세스		
보안 클라이언트 메시지, 아이콘, 이미지 및 연결/연결 해제 스크립트를 사용자 지정합니다.	7.2.0	이제 Secure Client를 사용자 지정하고 이러한 사용자 지정 값을 VPN 헤드엔드에 구축할 수 있습니다. 지원되는 Secure Client 사용자 지정은 다음과 같습니다. • GUI 텍스트 및 메시지 • 아이콘 및 이미지 • 스크립트 • 이진 • 맞춤형 설치 프로그램 변환 • 현지화된 설치 프로그램 변환 Threat Defense는 최종 사용자가 Secure Client에서 연결할 때 이러한 사용자 지정을 엔드포인트에 배포합니다. 신규/수정된 화면: • **Objects(**개체**)** > **Object Management(**개체 관리**)** > **VPN** > **Secure Client Customization(Secure Client** 사용자 지정**)** • **Devices(**디바이스**)** > **Remote Access(**원격 액세스**)** > Edit VPN policy(VPN 정책 편집) > **Advanced(**고급**)** > **Secure Client Customization(Secure Client** 사용자 지정**)** 참조: Secure Client 사용자 지정
VPN: 사이트 간		

기능	최소 **Threat Defense**	세부정보
손쉽게 NAT 변환에서 사이트 간 VPN 트래픽 제외.	모두	이제 NAT 변환에서 사이트 간 VPN 트래픽을 보다 쉽게 제외할 수 있게 되었습니다. 신규/수정된 화면: • 엔드포인트에 대한 NAT 제외 활성화: **Devices(**디바이스**)** > **VPN** > **Site To Site(**사이트 간**)** > **Add/Edit Site to Site VPN(**사이트 간 **VPN** 추가/편집**)** > **Add/Edit Endpoint(**엔드포인트 추가/편집**)** > **Exempt VPN traffic from network address translation(**네트워크 주소 변환에서 **VPN** 트래픽 제외**)** • NAT 정책이 없는 디바이스에 대한 NAT 제외 규칙 보기: **Devices(**디바이스**)** > **NAT** > **NAT Exemptions(NAT** 제외**)** • 단일 디바이스에 대한 NAT 제외 규칙 보기: **Devices(**디바이스**)** > **NAT** > **Threat Defense NAT Policy(Threat Defense NAT** 정책**)** > **NAT Exemptions(NAT** 제외**)** 참조: NAT 제외
손쉽게 VPN 노드에 대한 IKE 및 IPsec 세션 세부 정보 조회.	모두	사이트 간 VPN 대시보드에서 VPN 노드의 IKE 및 IPsec 세션 세부 정보를 사용자 친화적인 형식으로 볼 수 있습니다. 신규/수정된 화면: **Overview(**개요**)** > **Site to Site VPN(**사이트 간 **VPN)** > Tunnel Status(터널 상태) 위젯 아래에서 토폴로지에 마우스 포인터를 올려 **View(**보기**)**를 클릭한 다음 **CLI Details(CLI** 세부 정보**)** 탭 클릭. 참조: 사이트 간 VPN 모니터링
액세스 제어**:** 위협 탐지 및 애플리케이션 식별		
민감한 데이터 검색 및 마스킹.	Snort 3를 포함하는 7.4.0	업그레이드 영향**.** 기본 정책의 새 규칙이 적용됩니다**.** 사회 보장 번호, 신용카드 번호, 이메일 같은 민감한 데이터가 인터넷에 고의적으로 또는 실수로 유출될 수 있습니다. 민감한 데이터 탐지는 발생할 수 있는 민감한 데이터 유출에 대한 이벤트를 탐지하고 생성하는 데 사용되며, 상당한 양의 PII(개인 식별 정보) 데이터가 전송되는 경우에만 이벤트를 생성합니다. 민감한 데이터 탐지 기능은 기본 제공 패턴을 사용하여 이벤트 출력에서 PII를 마스킹할 수 있습니다. 데이터 마스킹 비활성화는 지원되지 않습니다. 참조: Snort 3의 사용자 지정 규칙

기능	최소 **Threat Defense**	세부정보
클라이언트리스 Zero Trust 액세스.	Snort 3를 포함하는 7.4.0	외부의 SAML IdP(Identity Provider) 정책을 사용하여 네트워크 내부(온프레미스) 또는 외부(원격)에서 보호된 웹 기반 리소스, 애플리케이션, 데이터에 대한 액세스를 인증하고 권한을 부여할 수 있는 Zero Trust Access를 도입했습니다. 구성은 ZTAP(Zero Trust 애플리케이션 정책), 애플리케이션 그룹 및 애플리케이션으로 이루어집니다. 신규/수정된 화면: • **Policies(**정책**)** > **Zero Trust Application(Zero Trust** 애플리케이션**)** • **Analysis(**분석**)** > **Connections(**연결**)** > **Events(**이벤트**)** • **Overview(**개요**)** > **Dashboard(**대시보드**)** > **Zero Trust** 신규/수정된 CLI 명령: • **show running-config zero-trust application** • **show running-config zero-trust application-group** • **show zero-trust sessions** • **show zero-trust statistics** • **show cluster zero-trust statistics** • **clear zero-trust sessions application** • **clear zero-trust sessions user** • **clear zero-trust statistics** 참조: Zero Trust Access.
라우팅		
IPv6 네트워크에서 BGP에 대한 정상 재시작을 구성합니다.	7.3.0	이제 매니지드 디바이스 버전 7.3 이상에서 IPv6 네트워크에 대한 BGP 정상 재시작을 구성할 수 있습니다. 신규/수정된 화면: **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > Edit device(디바이스 편집) > **Routing(**라우팅**)** > **BGP** > **IPv6** > **Neighbor(**인접 항목**)** > Add/Edit Neighbor(인접 항목 추가/편집). 참조: BGP 인접 항목 설정 구성

기능	최소 **Threat Defense**	세부정보
가상 라우팅 및 동적 VTI.	7.4.0	이제 경로 기반 사이트 간 VPN에 대해 동적 VTI를 사용하여 가상 라우터를 구성할 수 있습니다. 신규/수정된 화면: **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > Edit Device(디바이스 편집) > **Routing(**라우팅**)** > **Virtual Router Properties(**가상 라우터 특성**)** > **Available Interfaces(**사용 가능한 인터페이스**)** 아래의 Dynamic VTI interfaces(동적 VTI 인터페이스) 플랫폼 제한: 네이티브 모드 독립형 또는 고가용성 디바이스에서만 지원됩니다. 컨테이너 인스턴스 또는 클러스터된 디바이스에서는 지원되지 않습니다. 참조: 가상 라우터 및 동적 VTI 정보
액세스 제어**:** 위협 탐지 및 애플리케이션 식별		
암호화된 가시성 엔진 개선 사항.	Snort 3를 포함하는 7.4.0	EVE(암호화된 가시성 엔진)에서 이제 다음을 수행할 수 있습니다. • 위협 점수를 기반으로 암호화된 트래픽의 악의적인 통신을 차단합니다. • EVE에서 탐지된 프로세스를 기반으로 클라이언트 애플리케이션을 결정합니다. • 탐지를 위해 조각화된 Client Hello 패킷을 리어셈블합니다. 신규/수정된 화면: 액세스 제어 정책의 고급 설정을 사용하여 EVE를 활성화하고 이러한 설정을 구성합니다. 참조: 암호화된 가시성 엔진
특정 네트워크와 포트가 엘리펀트플로우를 우회하거나 제한하지 않도록 제외.	Snort 3를 포함하는 7.4.0	이제 특정 네트워크 및 포트가 엘리펀트 플로우를 우회하거나 제한하지 않도록 제외할 수 있습니다. 신규/수정된 화면: • 액세스 제어 정책의 고급 설정에서 엘리펀트 플로우 탐지를 구성할 때 **Elephant Flow Remediation(**엘리펀트 플로우 교정**)** 옵션을 활성화하는 경우, 이제 **Add Rule(**규칙 추가**)**을 클릭하여 우회하거나 제한하지 않도록 제외할 트래픽을 지정할 수 있습니다. • 시스템에서 우회하거나 제한하지 않도록 제외되는 엘리펀트 플로우를 탐지하면 **Elephant Flow Exempted(**엘리펀트 플로우 제외**)**라는 이유와 함께 중간 플로우 연결 이벤트를 생성합니다. 플랫폼 제한: Firepower 2100 Series에서는 지원되지 않습니다. 참조: 엘리펀트 플로우 탐지

기능	최소 **Threat Defense**	세부정보
개선된 JavaScript 검사.	Snort 3를 포함하는 7.4.0	JavaScript를 표준화하고 표준화된 콘텐츠에 대해 규칙을 매칭하여 JavaScript 검사를 개선했습니다. 참조: HTTP 검사기 및 Cisco Secure Firewall Management Center Snort 3 구성 가이드
액세스 제어**: ID**		
Management Center의 Cisco Secure Dynamic Attributes Connector.	Any(모든)	이제 Management Center에서 Cisco Secure Dynamic Attributes Connector를 구성할 수 있습니다. 이전에는 독립형 애플리케이션으로만 사용할 수 있었습니다. 참조: Cisco Secure Dynamic Attributes Connector
이벤트 로깅 및 분석		
Management Center 웹 인터페이스에서 Threat Defense 디바이스를 NetFlow 엑스포터로 구성.	Any(모든)	NetFlow는 패킷 플로우에 대한 통계를 제공하는 Cisco IOS 애플리케이션입니다. 이제 Management Center 웹 인터페이스를 사용하여 Threat Defense 디바이스를 NetFlow 엑스포터로 구성할 수 있습니다. 기존 NetFlow FlexConfig가 있고 웹 인터페이스에서 구성을 다시 실행하는 경우, 더 이상 사용되지 않는 FlexConfig를 제거할 때까지 구축할 수 없습니다. 신규/수정된 화면: **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)** > **Threat Defense Settings Policy(Threat Defense** 설정 정책**)** > **NetFlow** 참조: NetFlow 구성
상태 모니터링		
새로운 asp 삭제 메트릭.	7.4.0	600개가 넘는 새로운 asp(가속화된 보안 경로) 삭제 메트릭을 새 디바이스 상태 대시보드 또는 기존 디바이스 상태 대시보드에 추가할 수 있습니다. **ASP Drops(ASP** 삭제**)** 메트릭 그룹을 선택해야 합니다. 신규/수정된 화면: 시스템 (⚙) > **Health(**상태**)** > **Monitor(**모니터**)** > **Device(**디바이스**)** 참조: show asp drop 명령 사용법
관리		
인증서 해지 확인 시 IPv6 URL 지원	7.4.0	이전에는 Threat Defense가 IPv4 OCSP URL만 지원했습니다. 이제 Threat Defense는 IPv4 및 IPv6 OCSP URL을 모두 지원합니다. 참조: 인증서 등록 개체 해지 옵션
Threat Defense 백업 파일을 안전한 원격 위치에 저장합니다.	모두	디바이스를 백업하면 클라우드 제공 Firewall Management Center는 백업 파일을 안전한 클라우드 스토리지에 저장합니다. 참조 : 백업/복구
유용성, 성능 및 문제 해결		

기능	최소 **Threat Defense**	세부정보
사용 편의성 개선 사항.	모두	이제 다음을 수행할 수 있습니다. • 시스템 (⚙) > 스마트 라이선스에서 Threat Defense 클러스터용 스마트 라이선싱을 관리합니다. 이전에는 Device Management(디바이스 관리) 페이지를 사용해야 했습니다. 참조: 클러스터링용 라이선스 • Message Center 알림에 대한 보고서를 다운로드합니다. 메시지 센터에서 **Show Notifications(**알림 표시**)** 슬라이더 옆에 있는 새로운 **Download Report(**보고서 다운로드**)** 아이콘을 클릭합니다. 참조: 시스템 메시지 관리. • 등록된 모든 디바이스에 대한 보고서를 다운로드합니다. **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**에서 페이지 오른쪽 상단에 있는 새로운 **Download Device List Report(**디바이스 목록 보고서 다운로드**)** 링크를 클릭합니다. 참조: 매니지드 디바이스 목록 다운로드. • 사용자 지정 상태 모니터링 대시보드를 쉽게 생성하고 기존 대시보드를 편리하게 편집합니다. 참조: 디바이스 메트릭 연계
Secure Firewall 4200에 대해 패킷 캡처로 캡처할 트래픽 방향 지정.	7.4.0	Secure Firewall 4200에서는 **capture** 명령과 함께 새로운 **direction** 키워드를 사용할 수 있습니다. 신규/수정된 CLI 명령: **capture***capture_name***switchinterface***interface_name* [**direction** { **both** | **egress** | **ingress** }] 참조: Cisco Secure Firewall Threat Defense 명령 참조
Management Center REST API		
클라우드 제공 Firewall Management Center REST API.	기능에 따라 다름	Management center REST API의 변경 사항에 대한 자세한 내용은 API 빠른 시작 가이드에서 새로운 기능을 참조하십시오.

표 ***5:*** 사용 중단된 기능***:*** 버전 ***20230929***

기능	**Threat Defense**에서 사용되지 않음	세부정보
사용되지 않음: FlexConfig를 사용하는 NetFlow	모두	이제 Management Center 웹 인터페이스에서 Threat Defense 디바이스를 NetFlow 엑스포터로 구성할 수 있습니다. 이렇게 하면 더 이상 사용되지 않는 FlexConfig를 제거할 때까지 구축할 수 없습니다. 참조: NetFlow 구성
사용되지 않음: 높은 비관리 디스크 사용량 알림.	7.0.6 7.2.4 7.4.0	디스크 사용량 상태 모듈은 더 이상 높은 비관리 디스크 사용량에 대해 알림을 전송하지 않습니다. 매니지드 디바이스에 상태 정책을 구축하거나(알림 표시 중지), 디바이스를 버전 7.0.6, 7.2.4 또는 7.4로 업그레이드(알림 전송 중지)할 때까지 이러한 알림은 계속 표시될 수 있습니다. 나머지 디스크 사용량 알림에 대한 자세한 내용은 디스크 사용량 및 이벤트 드레인 상태 모니터 알림을 참고하십시오.

2023년 8월 3일

표 ***6:*** 새로운 기능***:*** ***2023***년 ***8***월 ***3***일

기능	설명
Firewall 마이그레이션 툴에 대한 업데이트	Cisco Defense Orchestrator는 이제 최신 버전의 Firewall 마이그레이션 툴을 호스팅합니다. 이제 Secure Firewall ASA 디바이스의 여러 컨텍스트를 라우팅 모드 인스턴스로 병합하고 클라우드 제공 Firewall Management Center에서 관리하는 Threat Defense 디바이스로 마이그레이션할 수 있습니다. 또한 마이그레이션 툴은 이제 VRF(virtual routing and forwarding, 가상 라우팅 및 포워딩) 기능을 활용하여 새로 병합된 구성의 일부가 될 멀티 컨텍스트 ASA 환경에서 관찰된 분리된 트래픽 흐름을 복제합니다. 자세한 내용은 *Cisco Defense Orchestrator* 가이드의 *Firewall* 마이그레이션 툴을 사용하여 *Firewall* 마이그레이션에서 CDO가 관리하는 Secure Firewall ASA 마이그레이션을 참조하십시오.

2023년 7월 20일

표 ***7:*** 새로운 기능***: 2023***년 ***7***월 ***20***일

기능	설명
GCP에서 관리하는 가상 Threat Defense 디바이스에 대한 EasyDeploy	이제 가상 Threat Defense 디바이스를 생성하는 동시에 GCP(Google Cloud Platform) 프로젝트에 구축할 수 있습니다. EasyDeploy 방법은 새 가상 디바이스를 생성한 다음 디바이스를 클라우드 환경과 연결하는 데 필요한 단계를 결합하여 절차를 간소화하고 설정에 필요한 시간을 최소화합니다. 이러한 온보딩 플로우에 대해 클라우드 제공 Firewall Management Center가 활성화되어 있어야 합니다. 자세한 내용 은 Google Cloud Platform에 Threat Defense 디바이스 구축 을 참조하십시오. 최소 Threat Defense: • 7.0.3 이상 7.0.x 버전 • 7.2 이상 버전

2023년 6월 8일

표 ***8:*** 새로운 기능***: 2023***년 ***6***월 ***8***일

기능	설명
AWS 또는 Azure를 사용하는 Secure Firewall Threat Defense를 위한 EasyDeploy	이제 AWS 또는 Azure 환경에서 동시에 Secure Firewall Threat Defense 디바이스를 생성하고 구축할 수 있습니다. CDO로 디바이스를 온보딩하고 클라우드 제공 Firewall Management Center에서 환경을 관리합니다. 자세한 내용은 AWS를 사용하여 Threat Defense 디바이스 구축 및 Azure VNet을 사용하여 Threat Defense 디바이스 구축을 각각 참조하십시오. 최소 Threat Defense: • 7.0.3 이상 7.0.x 버전 • 7.2 이상 버전

2023년 5월 25일

표 ***9:*** 새로운 기능***: 2023***년 ***5***월 ***25***일

기능	설명
위협 Threat Defense 7.3.1 지원.	이제 버전 7.3.1을 실행하는 Threat Defense 디바이스를 관리할 수 있습니다.
Firepower 1010E.	이제 클라우드 제공 Firewall Management Center을 사용하는 PoE(power over Ethernet)를 지원하지 않는 Firepower 1010E를 를 사용하여 관리할 수 있습니다. 최소 Threat Defense: 7.2.3

2023년 3월 9일

이 릴리스에서는 안정성, 강화 및 성능 향상을 소개합니다.

2023년 2월 16일

이 릴리스에서는 안정성, 강화 및 성능 향상을 소개합니다.

2023년 1월 18일

표 ***10:*** 새로운 기능***: 2023***년 ***1***월 ***18***일

기능	설명
원격 액세스 **VPN**	

기능	설명
CDO에서 원격 액세스 VPN 세션을 모니터링합니다.	이제 CDO를 사용하여 클라우드 제공 Firewall Management Center에서 관리하는 Threat Defense 디바이스에서 RA VPN 세션을 모니터링할 수 있습니다. 활성 세션 및 기록 세션의 목록은 물론 각 세션과 연결된 디바이스 및 사용자의 세부 정보도 볼 수 있습니다. 지원되는 Threat Defense 버전: • 7.0.3 이상 7.0.x 버전 • 7.2 이상 버전 자세한 내용은 구성 가이드에서 원격 액세스 VPN 세션 모니터링을 참조하십시오.

12 장

클라우드 제공 Firewall Management Center 2022의 새로운 기능

2022년 12월 13일

표 *11:* 새로운 기능*: 2022*년 *12*월 *13*일

기능	설명
CDO 및 **Threat Defense** 업그레이드에 대한 온보딩	
추가 디바이스 지원 및 온보딩	이제 클러스터링된 디바이스, AWS VPC 환경 및 Azure VNET 환경을 클라우드 제공 Firewall Management Center에 온보딩할 수 있습니다. 현재 이러한 디바이스를 온보딩하려면 로그인 자격 증명이 필요합니다. 클러스터링된 디바이스는 지정된 관리 플랫폼에서 이미 구성되어 있어야 합니다. 자세한 내용은 https://docs.defenseorchestrator.com의 다음 항목을 참조하십시오. • 클러스터 온보딩 • AWS VPC와 연결된 디바이스 온보딩 • Azure VNet 환경 온보딩

기능	설명
무인 Threat Defense 업그레이드	Threat Defense 업그레이드 마법사는 이제 새로운 무인 모드 메뉴를 사용하여 무인 업그레이드를 지원합니다. 업그레이드할 대상 버전 및 디바이스를 선택하고 몇 가지 업그레이드 옵션을 지정한 다음 단계를 수행하면 됩니다. 로그아웃하거나 브라우저를 닫을 수도 있습니다. 무인 업그레이드에서는 시스템에서 자동으로 필요한 업그레이드 패키지를 디바이스에 복사하고 호환성 및 준비도 확인을 수행한 다음 업그레이드를 시작합니다. 마법사를 수동으로 진행할 때와 마찬가지로 업그레이드 단계를 "통과"하지 않는 디바이스(예: 검사 실패)는 다음 단계에 포함되지 않습니다. 업그레이드가 완료되면 확인 및 업그레이드 후 작업을 시작합니다. 복사 및 확인 단계 중에 무인 모드를 일시 중지하고 다시 시작할 수 있습니다. 그러나 무인 모드를 일시 중지해도 진행 중인 작업은 중지되지 않습니다. 시작된 복사 및 확인은 완료될 때까지 실행됩니다. 마찬가지로, 무인 모드를 중지하여 진행 중인 업그레이드를 취소할 수 없습니다. 업그레이드를 취소하려면 Device Management(디바이스 관리) 페이지의 Upgrade(업그레이드) 탭 및 메시지 센터에서 액세스할 수 있는 Upgrade Status(업그레이드 상태) 팝업을 사용합니다. Management Center용 Cisco Secure Firewall Threat Defense 업그레이드 설명서의 *Threat Defense* 업그레이드를 참조하십시오.
Snort 3으로 자동 업그레이드	Threat Defense에서 버전 7.3 이상으로 업그레이드하는 경우 더 이상 Snort 2를 Snort 3으로 업그레이드 옵션을 비활성화할 수 없습니다. 소프트웨어 업그레이드 후에는 설정을 구축할 때 모든 적격 디바이스가 Snort 2에서 Snort 3으로 업그레이드됩니다. 개별 디바이스를 다시 전환할 수는 있지만 Snort 2는 향후 릴리스에서 더 이상 사용되지 않으므로 지금 사용을 중지하는 것이 좋습니다. 맞춤형 침입 또는 네트워크 분석 정책 사용으로 인한 자동 업그레이드 부적격 디바이스의 경우, 향상된 탐지 및 성능을 위해 Snort 3으로 수동 업그레이드하는 것이 좋습니다. 마이그레이션 지원은 Cisco Secure Firewall Management Center Snort 3 구성 가이드를 참조하십시오.

기능	설명
Firepower 4100/9300의 CDO 매니지드 Secure Firewall Threat Defense 디바이스	Firepower 4100/9300은 하나 이상의 논리적 디바이스를 설치할 수 있는 유연한 보안 플랫폼입니다. Management Center에 Threat Defense기능을 추가하기 전에 Secure Firewall 섀시 관리자 또는 FXOS CLI를 사용하여 섀시 인터페이스를 구성하고 논리적 디바이스를 추가하고 인터페이스를 Firewall 4100/9300 섀시의 디바이스에 할당해야 합니다. 이제 디바이스를 생성할 때 CDO를 관리자로 구성하여 Firepower 4100/9300에서 CDO 매니지드 독립형 논리적 Threat Defense 디바이스를 생성할 수 있습니다. Cisco Defense Orchestrator에서 클라우드 제공 Firewll Management Center를 사용하여 Firewall Threat Defense 관리
인터페이스	
IPv6 DHCP 개선 사항	DHCP(Dynamic Host Configuration Protocol)는 IP 주소와 같은 네트워크 구성 매개 변수를 DHCP 클라이언트에 제공합니다. Threat Defense 디바이스에서는 위협 방어 디바이스 인터페이스에 연결된 DHCP 클라이언트에 DHCP 서버를 제공할 수 있습니다. DHCP 서버는 DHCP 클라이언트에 직접 네트워크 컨피그레이션 매개변수를 제공합니다. 이제 클라우드 제공 Firewall Management Center은 Secure Firewall Threat Defense 디바이스에 대해 다음과 같은 IPv6 주소 지정 기능을 지원합니다: • DHCPv6 주소 클라이언트: Threat Defense는 DHCPv6 서버에서 IPv6 전역 주소 및 선택 사항인 기본 경로를 가져옵니다. • DHCPv6 접두사 위임 클라이언트: Threat Defense는 DHCPv6 서버에서 위임된 접두사를 가져옵니다. 그런 다음 이러한 접두사를 사용하여 SLAAC(Stateless Address Auto Configuration) 클라이언트가 동일한 네트워크에서 IPv6 주소를 자동으로 구성할 수 있도록 다른 Threat Defense 인터페이스 주소를 구성할 수 있습니다. • 위임된 접두사에 대한 BGP 라우터 알림. • DHCPv6 스테이트리스 서버: Threat Defense는 SLAAC 클라이언트가 위협 방어에 IR(정보 요청) 패킷을 보낼 때 SLAAC 클라이언트에 도메인 이름 등의 기타 정보를 제공합니다. Threat Defense는 IR 패킷만 수락하고 클라이언트에 주소를 할당하지는 않습니다. 자세한 내용은 Cisco Defense Orchestrator에서 클라우드 제공 Firewall Management Center로 Firewall Threat Defense 관리에서 *IPv6* 주소 지정 구성을 참조하십시오.

기능	설명
루프백 인터페이스 지원	루프백 인터페이스는 물리적 인터페이스를 에뮬레이트하는 소프트웨어 인터페이스입니다. IPv4 및 IPv6 주소를 사용하는 여러 물리적 인터페이스를 통해 연결할 수 있습니다. 고정 및 동적 VTI VPN 터널의 이중화를 위해 루프백 인터페이스를 구성할 수 있습니다. Cisco Defense Orchestrator에서 클라우드 제공 Firewall Management Center를 사용하여 Firewall Threat Defense 관리에서 일반 방화벽 인터페이스를 참조하십시오.
Azure 게이트웨이 로드 밸런서의 Threat Defense Virtual에 대해 페어링된 프록시 VXLAN	Azure 게이트웨이 로드 밸런서(GWLB)와 함께 사용하기 위해 Azure에서 가상 Threat Defense에 대해 페어링된 프록시 모드 VXLAN 인터페이스를 구성할 수 있습니다. 가상 Threat Defense는 페어링된 프록시에서 VXLAN 세그먼트를 활용하여 단일 NIC에서 외부 인터페이스 및 내부 인터페이스를 정의합니다. Cisco Defense Orchestrator에서 클라우드 제공 Firewall Management Center를 사용하여 Firewall Threat Defense 관리에서 퍼블릭 클라우드의 *Threat Defense Virtual* 클러스터링을 참조하십시오.
이중화 관리자 액세스 데이터 인터페이스	이제 관리자 액세스를 위해 데이터 인터페이스를 사용할 때 기본 인터페이스가 다운되는 경우 관리 기능을 대신하도록 보조 데이터 인터페이스를 구성할 수 있습니다. 디바이스는 SLA 모니터링을 사용하여 고정 경로 및 두 인터페이스를 모두 포함하는 ECMP(Equal-Cost Multi-Path) 영역의 실행 가능성을 추적하므로 관리 트래픽이 두 인터페이스를 모두 사용할 수 있습니다. 자세한 내용은 Cisco Defense Orchestrator에서 클라우드 제공 Firewall Management Center로 Firewall Threat Defense 관리에서 이중화 관리자 액세스 데이터 인터페이스 구성을 참조하십시오.
원격 액세스 **VPN**	
원격 액세스 VPN의 TLS 1.3	이제 TLS 1.3을 사용하여 원격 액세스 VPN 연결을 암호화할 수 있습니다. Threat Defense Platform(위협 방어 플랫폼) 설정을 사용하여 디바이스가 원격 액세스 VPN 서버 역할을 할 때 TLS 1.3 프로토콜을 사용해야 하도록 지정합니다. Cisco Defense Orchestrator에서 클라우드 제공 Firewall Management Center를 사용하여 Firewall Threat Defense의 플랫폼 설정을 참조하십시오.
사이트 대 사이트 **VPN**	

기능	설명
동적 Virtual Tunnel Interface 지원	동적 VTI를 생성하고 이를 사용하여 허브 및 스포크 토폴로지에서 경로 기반 사이트 간 VPN을 구성할 수 있습니다. 이전에는 고정 VTI만 사용하여 허브 및 스포크 토폴로지에서 경로 기반 사이트 간 VPN을 구성할 수 있었습니다. 동적 VTI를 사용 하면 대규모 엔터프라이즈 허브 및 스포크 구축을 위한 피어를 쉽게 구성할 수 있습니다. 단일 동적 VTI는 허브의 여러 고정 VTI 구성을 대체할 수 있습니다. 허브 구성을 변경하지 않고 허브에 새 스포크를 추가할 수 있습니다. Cisco Defense Orchestrator에서 클라우드 제공 Firewall Management Center를 사용하여 Firewall Threat Defense의 *Secure Firewall Threat Defense*용 사이트 간 *VPN*을 참조하십시오.
라우팅	
양방향 포워딩 탐지 지원	클라우드 제공 Firewall Management Center는 이제 Secure Firewall Threat Defense 디바이스에서 BFD(Bidirectional Forwarding Detection) 구성을 지원합니다. BFD는 두 시스템 간에 전달되는 모든 데이터 프로토콜 상의 유니캐스트, 포인트 투 포인트 모드에서 작동합니다. 그러나 Threat Defense에서 BFD는 BGP 프로토콜에서만 지원됩니다. 디바이스의 BFD 구성에는 템플릿 및 정책을 생성하고 BGP 네이버 설정에서 BFD 지원을 활성화하는 작업이 포함됩니다. 자세한 내용은 Cisco Defense Orchestrator에서 클라우드 제공 Firewall Management Center로 Firewall Threat Defense 관리에서 *Bidirectional Forwarding Detection* 라우팅을 참조하십시오.
Virtual Tunnel Interface에서 EIGRP (IPv4) 라우팅 지원	이제 EIGRP(IPv4) 라우팅이 Virtual Tunnel Interface에서 지원됩니다. 이제 EIGRP(IPv4) 프로토콜을 사용하여 라우팅 정보를 공유하고 피어 간에 VTI 기반 VPN 터널을 통해 트래픽 흐름을 라우팅할 수 있습니다. Cisco Defense Orchestrator에서 클라우드 제공 Firewall Management Center를 사용하여 Firewall Threat Defense의 *VTI*용 추가 구성을 참조하십시오.
OSPF를 위한 Virtual Tunnel Interface(VTI) 지원	IPv4 또는 IPv6 OSPF는 Threat Defense 디바이스의 VTI 인터페이스에서 구성할 수 있습니다. OSPF를 사용하여 라우팅 정보를 공유하고 디바이스 간에 VTI 기반 VPN 터널을 통해 트래픽을 라우팅할 수 있습니다. Cisco Defense Orchestrator에서 클라우드 제공 Firewall Management Center를 사용하여 Firewall Threat Defense 관리의 *Secure Firewall Threat Defense*용 사이트 간 *VPN*을 참조하십시오.
액세스 제어 및 위협 탐지	

기능	설명
암호 해독 정책	기능을 더 잘 반영하기 위해 *SSL* 정책에서 암호 해독 정책으로 이름이 변경되었습니다. 이제 하나 이상의 **Decrypt - Resign(**암호 해독 - 다시 서명**)** 또는 **Decrypt - Known Key(**암호 해독 - 알려진 키**)** 규칙을 동시에 사용하여 암호 해독 정책을 구성할 수 있습니다. **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Decryption(**해독**)**로 이동하여 시작하십시오. 이제 Create Decryption Policy(암호 해독 정책 생성) 대화 상자에 **Outbound Connections(**아웃바운드 연결**)** 및 **Inbound Connections(**인바운드 연결**)**라는 두 개의 탭 페이지가 있습니다. **Outbound Connections(**아웃바운드 연결**)** 탭 페이지를 사용하여 **Decrypt - Resign(**암호 해독 - 다시 서명**)** 규칙 작업으로 하나 이상의 암호 해독 규칙을 구성합니다. (동시에 인증 기관을 업로드하거나 생성할 수 있습니다.) CA와 네트워크 및 포트의 각 조합은 하나의 암호 해독 규칙을 생성합니다. Inbound Connections(인바운드 연결) 탭 페이지를 사용하여 Decrypt - Known Key(암호 해독 - 알려진 키) 규칙 작업으로 하나 이상의 암호 해독 규칙을 구성합니다. (서버의 인증서를 동시에 업로드할 수 있습니다.) 서버 인증서와 네트워크 및 포트의 각 조합은 하나의 암호 해독 규칙을 생성합니다.
상태 모니터링	
클라우드 제공 Firewall Management Center 구축 알림 CDO	CDO은 이제 클라우드 제공 Firewall Management Center에서 수행되는 구축의 상태를 알려줍니다. 알림 메시지에는 구축의 성공, 실패 또는 진행 중 여부에 대한 정보, 구축 시간 및 날짜, 클라우드 제공 Firewall Management Center의 구축 기록 페이지에 대한 링크가 포함됩니다. 자세한 내용은 Cisco Defense Orchestrator를 사용한 FDM 디바이스 관리의 알림을 참조하십시오.
클러스터 상태 모니터링 설정	이제 클라우드 제공 Firewall Management Center 웹 인터페이스에서 클러스터 상태 모니터 설정을 수정할 수 있습니다. 이전 버전에서 FlexConfig를 사용하여 이러한 설정을 구성하는 경우, 시스템은 구축을 허용하지만 FlexConfig 설정이 우선적으로 적용되므로 구성을 다시 실행하라는 경고를 표시합니다. Cisco Defense Orchestrator에서 클라우드 제공 Firewall Management Center를 사용하여 Firewall Threat Defense 관리의 클러스터 상태 모니터링 설정 편집을 참조하십시오.

기능	설명
디바이스 클러스터에 대한 향상된 상태 모니터링	이제 각 클러스터의 상태 모니터를 사용하여 전체 클러스터 상태, 로드 분포 메트릭, 성능 메트릭, CCL(클러스터 제어 링크) 및 데이터 처리량 등을 볼 수 있습니다. Cisco Defense Orchestrator에서 클라우드 제공 Firewall Management Center를 사용하여 Firewall Threat Defense 관리의 클러스터 상태 모니터를 참조하십시오.
새 상태 모니터링 알림	클라우드 제공 Firewall Management Center에서는 이제 Firepower 4100/9300 섀시의 온도 및 전원 공급 장치를 모니터링할 수 있는 새로운 상태 모듈을 제공합니다. 새로운 Environment Status(환경 상태) 및 Power Supply(전력 공급 장치) 상태 모듈을 사용하여 맞춤형 상태 대시보드를 생성하고 물리적 어플라이언스의 온도 및 전원 공급 장치에 대한 임계값을 설정할 수 있습니다. Cisco Defense Orchestrator에서 클라우드 제공 Firewall Management Center를 사용하여 Firewall Threat Defense 관리의 상태 모니터 알림을 참조하십시오.
라이선싱	
통신 사업자 라이선스	Cisco Smart Licensing은 시스코 포트폴리오 및 조직 전체에서 소프트웨어를 보다 쉽고 빠르고 일관적인 방식으로 구매하고 관리할 수 있는 유연한 라이선싱 모델입니다. 클라우드 제공 Firewall Management Center는 이제 기존 스마트 라이선스 외에 통신 사업자 라이선스를 지원합니다. 통신 사업자 라이선스는 GTP/GPRS, Diameter, SCTP 및 M3UA 검사 구성을 허용합니다. Cisco Defense Orchestrator에서 클라우드 제공 Firewall Management Center를 사용하여 Firewall Threat Defense 관리의 라이선스를 참조하십시오.
유용성, 성능 및 문제 해결	
코어 할당 성능 프로파일	Secure Firewall Threat Defense 디바이스의 CPU 코어는 Lina 및 Snort의 두 가지 기본 시스템 프로세스에 할당됩니다. Lina는 VPN 연결, 라우팅 및 기타 기본 레이어 3/4 처리를 처리합니다. Snort는 침입 및 악성코드 방지, URL 필터링, 애플리케이션 필터링 및 심층 패킷 검사가 필요한 기타 기능을 포함한 고급 검사를 제공합니다. 이제 성능 프로파일을 사용하여 데이터 플레인 및 Snort에 할당된 시스템 코어의 백분율을 조정하여 시스템 성능을 조정할 수 있습니다. VPN 및 침입 정책의 상대적 사용에 따라 원하는 성능 프로파일을 선택할 수 있습니다. 자세한 내용은 Cisco Defense Orchestrator에서 클라우드 제공 Firewall Management Center로 Firewall Threat Defense 관리에서 성능 프로파일 구성을 참조하십시오.
ID	

기능	설명
프록시 시퀀스	프록시 시퀀스는 LDAP, Active Directory 또는 ISE/ISE-PIC 서버와 통신하는 데 사용할 수 있는 하나 이상의 매니지드 디바이스입니다. 이는 Cisco Defense Orchestrator(CDO)가 Active Directory 또는 ISE/ISE-PIC 서버와 통신할 수 없는 경우에만 필요합니다. (예를 들어 CDO는 퍼블릭 클라우드에 있지만 Active Directory 또는 ISE/ISE-PIC는 프라이빗 클라우드에 있을 수 있습니다.) 하나의 매니지드 디바이스를 프록시 시퀀스로 사용할 수 있지만, 둘 이상의 매니지드 디바이스를 설정하는 것이 좋습니다. 그러면 하나의 매니지드 디바이스가 Active Directory 또는 ISE/ISE-PIC와 통신할 수 없는 경우 다른 매니지드 디바이스가 인계받을 수 있습니다. **Integration(**통합**)** > **Other Integrations(**기타 통합**)** > **Realms(**영역**)** > **Proxy Sequence(**프록시 시퀀스**)**으로 이동하여 프록시 시퀀스를 생성합니다.

2022년 10월 20일

정책 기반 경로 맵에서 다음 홉 **IP** 주소 구성 지원

PBR(Policy-Based Routing)은 대상 네트워크 기준이 아니라 소스 포트, 대상 주소, 대상 포트, 프로토콜, 애플리케이션 또는 이러한 개체의 조합과 같은 우선순위를 기반으로 지정된 애플리케이션에 대한 네트워크 트래픽을 라우팅하는 데 도움이 됩니다. 예를 들어, PBR을 사용하여 높은 대역폭, 비용이 많이 드는 링크를 통해 높은 우선순위 네트워크 트래픽을 라우팅하고 낮은 대역폭, 낮은 비용 링크를 통해 낮은 우선순위 네트워크 트래픽을 라우팅할 수 있습니다.

이제 클라우드 제공 Firewall Management Center는 정책 기반 경로 맵을 생성할 때 다음 홉 IP 주소 정의를 지원합니다. 자세한 내용은 Cisco Defense Orchestrator에서 클라우드 제공 Firewall Management Center로 Firewall Threat Defense 관리에서 정책 기반 라우팅 정보 및 정책 기반 라우팅 정책 구성을 참조하십시오.

URL 필터링 개선 사항

URL 필터링을 사용하면 네트워크의 사용자가 사용할 수 있는 웹 사이트에 대한 액세스를 제어할 수 있습니다. 디바이스에 URL 필터링 라이선스가 필요한 범주 및 평판을 기준으로 웹사이트를 필터링하거나 URL을 지정하여 수동으로 필터링할 수 있습니다. 더 빠르고 스마트한 URL 필터링 방법인 범주 및 평판 기반 필터링은 Cisco의 최신 위협 인텔리전스 정보를 사용하므로 사용하는 것이 좋습니다.

클라우드 제공 Firewall Management Center는 이제 로컬 데이터베이스 정보를 사용하는 대신 Cisco Talos 클라우드에서 직접 최신 URL 범주 및 평판 정보를 쿼리할 수 있습니다. 로컬 데이터베이스는 24~48시간마다 업데이트됩니다. 자세한 내용은 Cisco Defense Orchestrator에서 클라우드 제공 Firewall Management Center로 Firewall Threat Defense 관리에서 *URL* 필터링 옵션을 참조하십시오.

클라우드 제공 **Firewall Management Center**을 사용하여 **Secure Firewall Threat Defense**와 **Umbrella** 터널 통합

이제 클라우드 제공 Firewall Management Center을 사용하는 Threat Defense 디바이스에서 Umbrella로 IPsec IKEv2 터널을 자동으로 구축할 수 있습니다. 이 터널은 검사 및 필터링을 위해 모든 인터넷 바운드 트래픽을 Umbrella SIG(Secure Internet Gateway)로 전달합니다. 간단한 마법사를 사용하여 새로운 유형의 정적 VTI 기반 사이트 간 VPN 토폴로지인 SASE 토폴로지를 생성하여 Umbrella 터널을 구성하고 구축합니다.

자세한 내용은 Cisco Defense Orchestrator에서 클라우드 제공 Firewall Management Center로 Firewall Threat Defense 관리에서 *Umbrella SASE* 토폴로지 정보를 참조하십시오.

FTD에서 클라우드로의 마이그레이션에서 원격 액세스 **VPN** 정책 지원

이제 CDO는 FTD를 클라우드로 마이그레이션하는 동안 원격 액세스 VPN 정책을 가져옵니다.

자세한 내용은 Cisco Defense Orchestrator에서 클라우드 제공 Firewall Management Center로 Firewall Threat Defense 관리에서 *FTD*를 클라우드로 마이그레이션을 참조하십시오.

Flex 구성 라우팅 정책 마이그레이션

클라우드 제공 Firewall Management Center는 이제 사용자 인터페이스에서 Migration Config(마이그레이션 구성) 옵션을 사용하여 Flex 구성 ECMP, VxLAN 및 EIGRP 정책의 마이그레이션을 지원합니다.

자세한 내용은 Cisco Defense Orchestrator에서 클라우드 제공 Firewall Management Center로 Firewall Threat Defense 관리에서 *FlexConfig* 정책 마이그레이션을 참조하십시오.

Smart Licensing 표준화

클라우드 제공 Firewall Management Center에서 사용하는 라이선스 이름이 변경되었습니다.

표 ***12:*** 스마트 라이선스 이름 변경

이전 이름	이제	새 이름
Base	이제	Essentials
위협	이제	IPS
Malware	이제	악성코드 방어
RA VPN/AnyConnect 라이선스	이제	Cisco Secure Client
AnyConnect Plus	이제	Secure Client Advantage
AnyConnect Apex	이제	Secure Client Premier
AnyConnect Apex 및 Plus	이제	Secure Client Premier 및 Advantage
AnyConnect VPN만	이제	Secure Client VPN 전용

자세한 내용은 Cisco Defense Orchestrator에서 클라우드 제공 Firewall Management Center로 Firewall Threat Defense 관리에서 라이선스 유형 및 제한 사항을 참조하십시오.

2022년 6월 9일

CDO(Cisco Defense Orchestrator)는 이제 클라우드 제공 Firewall Management Center의 플랫폼입니다.

클라우드 제공 Firewall Management Center는 Secure Firewall Threat Defense 디바이스를 관리하는 SaaS(Software-as-a-Service) 제품입니다. 이는 온프레미스 Secure Firewall Management Center와 동일한 여러 기능을 제공하며, 온프레미스 Secure Firewall Management Center와 모양과 동작이 동일하며, 동일한 FMC API를 사용합니다.

이 제품은 Secure Firewall Management Center의 온프레미스 버전에서 SaaS 버전으로 이동하려는 Secure Firewall Management Center 고객을 위해 설계되었습니다.

SaaS 제품인 CDO 운영 팀은 이를 유지 관리합니다. 새로운 기능이 도입되면 CDO 운영 팀이 CDO 및 클라우드 제공 방화벽 관리자를 업데이트합니다.

마이그레이션 마법사를 사용하면 온프레미스 Secure Firewall Management Center에 등록된 Secure Firewall Threat Defense 디바이스를 클라우드 제공 Firewall Management Center로 마이그레이션할 수 있습니다.

Secure Firewall Threat Defense 디바이스 온보딩은 일련 번호를 사용하여 디바이스를 온보딩하거나 등록 키가 포함된 CLI 명령을 사용하는 등 친숙한 프로세스를 사용하여 CDO에서 수행됩니다. 디바이스가 온보딩되면 CDO와 클라우드 제공 Firewall Management Center에 모두 표시되지만 클라우드 제공 Firewall Management Center에서 디바이스를 구성합니다. 버전 7.2 이상을 실행하는 Secure Firewall Threat Defense 디바이스를 온보딩할 수 있습니다.

클라우드 제공 Firewall Management Center의 라이선스는 디바이스별 매니지드 라이선스이며 클라우드 제공 FMC 자체에는 라이선스가 필요하지 않습니다. 기존 Secure Firewall Threat Defense 디바이스는 기존 스마트 라이선스를 재사용하며, 새 Secure Firewall Threat Defense 디바이스는 FTD에서 구현된 각 기능에 대해 새 스마트 라이선스를 프로비저닝합니다.

원격 지사 구축에서 Threat Defense 디바이스의 데이터 인터페이스는 디바이스의 관리 인터페이스 대신 Cisco Defense Orchestrator 관리에 사용됩니다. 대부분의 원격 지사에서는 단일 인터넷 연결만 가능하므로 외부 CDO 액세스를 통해 중앙 집중식 관리가 가능합니다. 원격 지사 구축의 경우 CDO는 데이터 인터페이스를 통해 관리하는 Threat Defense 디바이스에 대한 고가용성 지원을 제공합니다.

Security Analytics and Logging(SaaS) 또는 Security Analytics and Logging(온프레미스)을 사용하여 온보딩된 Threat Defense 디바이스에서 생성된 시스템 로그 이벤트를 분석할 수 있습니다. SaaS 버전은 클라우드에 이벤트를 저장하며 CDO에서 이벤트를 볼 수 있습니다. 온프레미스 버전은 온프레미스 Secure Network Analytics 어플라이언스에 이벤트를 저장하며, 분석은 온프레미스 Secure Firewall Management Center에서 수행됩니다. 두 경우 모두 오늘날의 온프레미스 FMC와 마찬가지로 센서에서 직접 선택한 로그 컬렉터로 로그를 전송할 수 있습니다.

FTD 대시보드는 클라우드 제공 Firewall Management Center에서 관리하는 모든 Threat Defense 디바이스에서 수집 및 생성된 이벤트 데이터를 포함하여 상태를 한눈에 볼 수 있도록 제공합니다. 이 대시보드를 사용하여 디바이스 상태 및 구축에 있는 디바이스의 전반적인 상태와 관련된 종합적인 정보를 볼 수 있습니다. FTD 대시보드가 제공하는 정보는 시스템에서 디바이스의 라이선스, 구성 및 구

축 방법에 따라 달라집니다. FTD 대시보드에는 모든 CDO 매니지드 Threat Defense 디바이스에 대한 데이터가 표시됩니다. 그러나 디바이스 기반 데이터를 필터링하도록 선택할 수 있습니다. 특정 시간 범위에 대해 표시할 시간 범위를 선택할 수도 있습니다.

Cisco Secure Dynamic Attributes Connector를 사용하면 클라우드 제공 Firewall Management Center 액세스 제어 규칙에서 다양한 클라우드 서비스 플랫폼의 서비스 태그 및 범주를 사용할 수 있습니다. IP 주소와 같은 네트워크 구성은 워크로드의 동적 특성과 IP 주소 중복의 불가피성으로 인해 가상, 클라우드 및 컨테이너 환경에서 일시적일 수 있습니다. 고객은 IP 주소 또는 VLAN이 변경되는 경우에도 방화벽 정책이 유지되도록 VM 이름 또는 보안 그룹과 같은 비 네트워크 구문을 기반으로 정책 규칙을 정의해야 합니다.

하나 이상의 매니지드 디바이스의 프록시 시퀀스를 사용하여 LDAP, Active Directory 또는 ISE/ISE-PIC 서버와 통신할 수 있습니다. 이는 Cisco Defense Orchestrator(CDO)가 Active Directory 또는 ISE/ISE-PIC 서버와 통신할 수 없는 경우에만 필요합니다. 예를 들어 CDO은(는) 퍼블릭 클라우드에 있지만 Active Directory 또는 ISE/ISE-PIC는 프라이빗 클라우드에 있을 수 있습니다.

하나의 매니지드 디바이스를 프록시 시퀀스로 사용할 수 있지만, 둘 이상의 매니지드 디바이스를 설정하는 것이 좋습니다. 그러면 하나의 매니지드 디바이스가 Active Directory 또는 ISE/ISE-PIC와 통신할 수 없는 경우 다른 매니지드 디바이스가 인계받을 수 있습니다.

모든 고객은 CDO를 사용하여 Secure Firewall ASA, Meraki, Cisco IOS 디바이스, Umbrella 및 AWS 가상 프라이빗 클라우드와 같은 다른 디바이스 유형을 관리할 수 있습니다. Firepower Device Manager에서 로컬 관리용으로 구성된 Secure Firewall Threat Defense 디바이스를 CDO를 사용하여 관리하는 경우 CDO로도 계속 관리할 수 있습니다. CDO를 처음 사용하는 경우 클라우드에서 제공하는 새로운 Firewall Management Center 및 기타 모든 디바이스 유형을 사용하여 Secure Firewall Threat Defense 디바이스를 관리할 수 있습니다.

클라우드 제공 Firewall Management Center에서 지원하는 Firewall Management Center 기능에 대해 자세히 알아보십시오.

- 상태 모니터링
- Secure Firewall Threat Defense 디바이스 백업/복원
- 일정 예약
- 가져오기/내보내기
- 알림 응답을 사용한 외부 알림
- 투명 방화벽 또는 라우팅 방화벽 모드
- Secure Firewall Threat Defense 디바이스의 고가용성
- 인터페이스
- NAT(Network Access Control)
- 고정 및 기본 경로 및 기타 라우팅 구성
- 개체 관리 및 인증서
- 원격 액세스 VPN 및 사이트 간 VPN 구성

- Access Control(액세스 컨트롤) 정책
- Cisco Secure Dynamic Attributes Connector
- 침입 탐지 및 방지 정책
- 네트워크 악성코드 및 보호 및 파일 정책
- 암호화된 트래픽 처리
- 사용자 ID
- FlexConfig 정책