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.

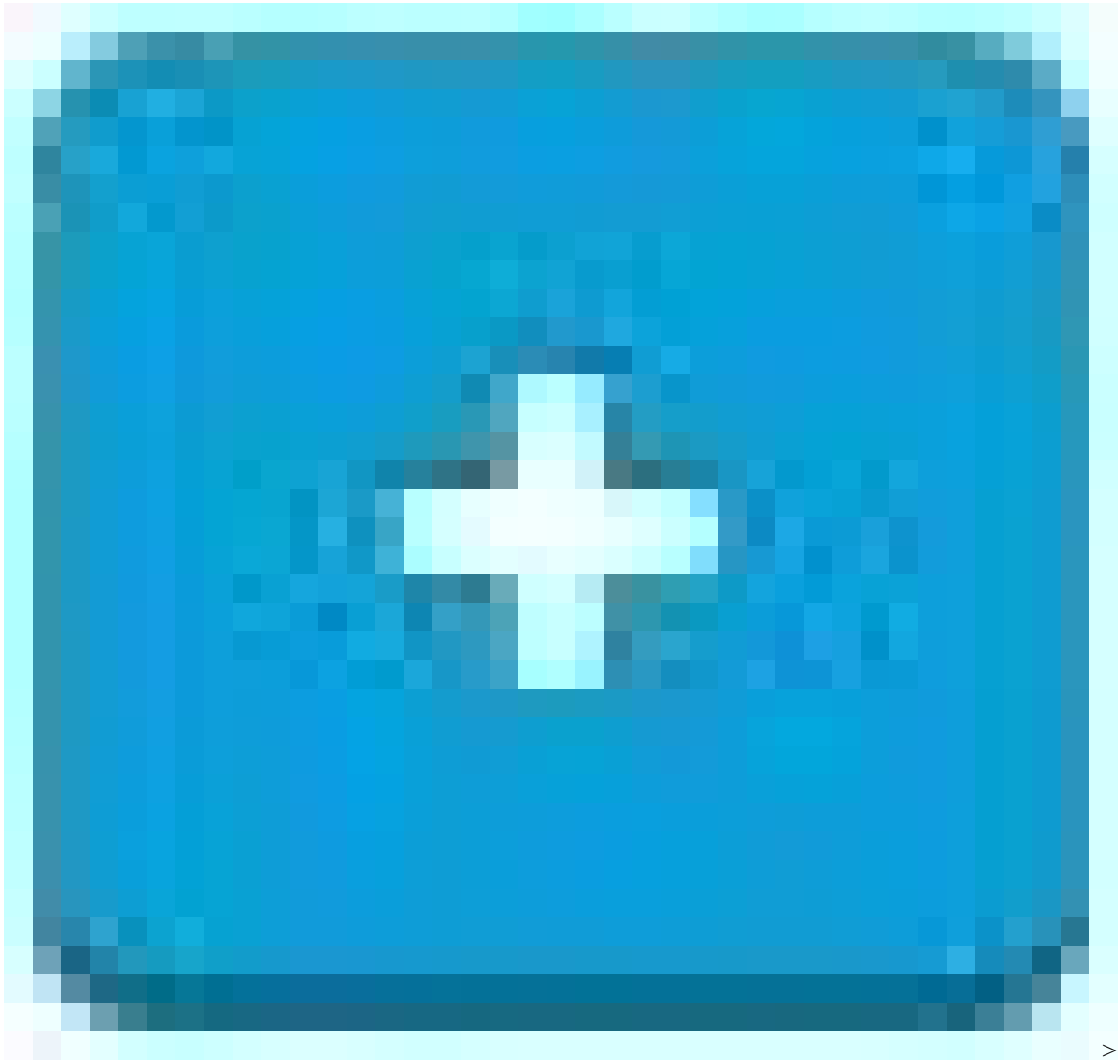
자세한 내용은 원격 디바이스 백업 예약을 참조하십시오.

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.

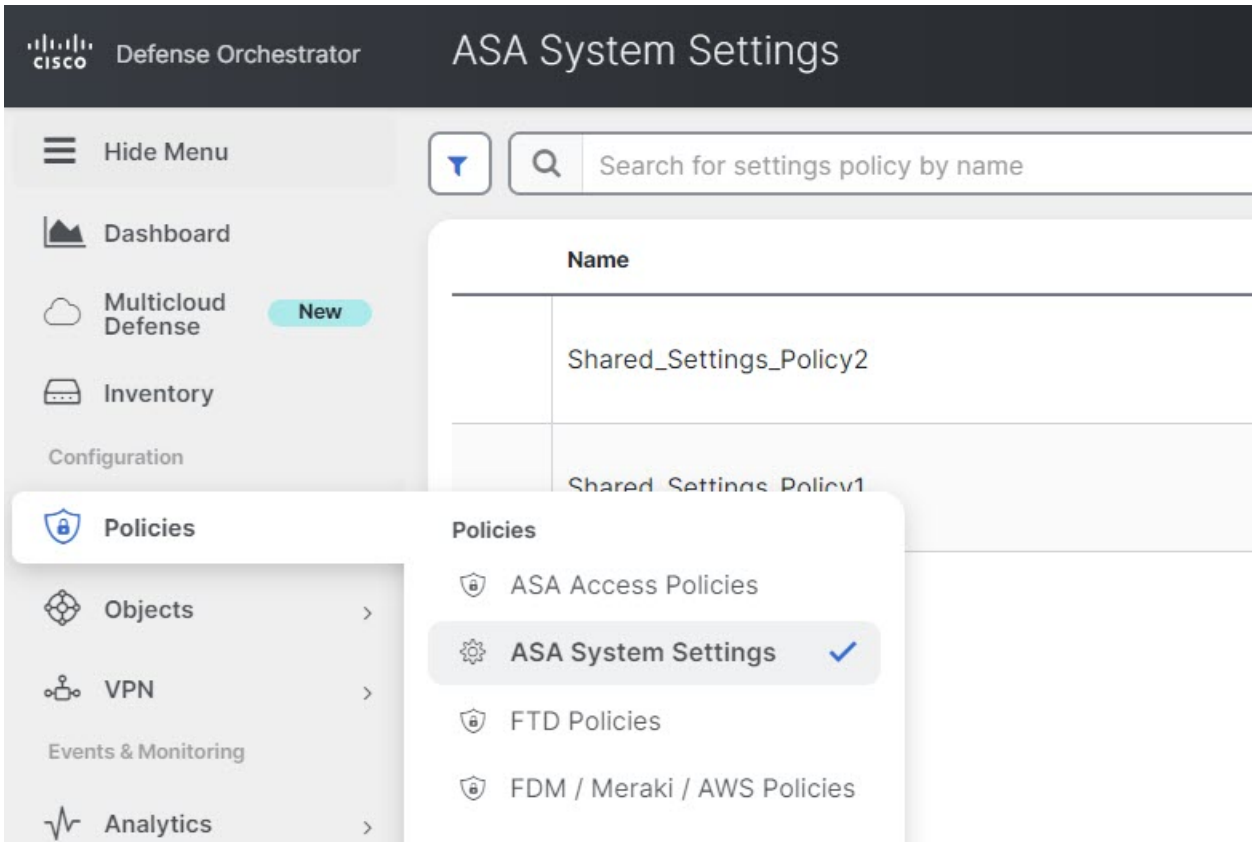
2023년 10월 12일

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.



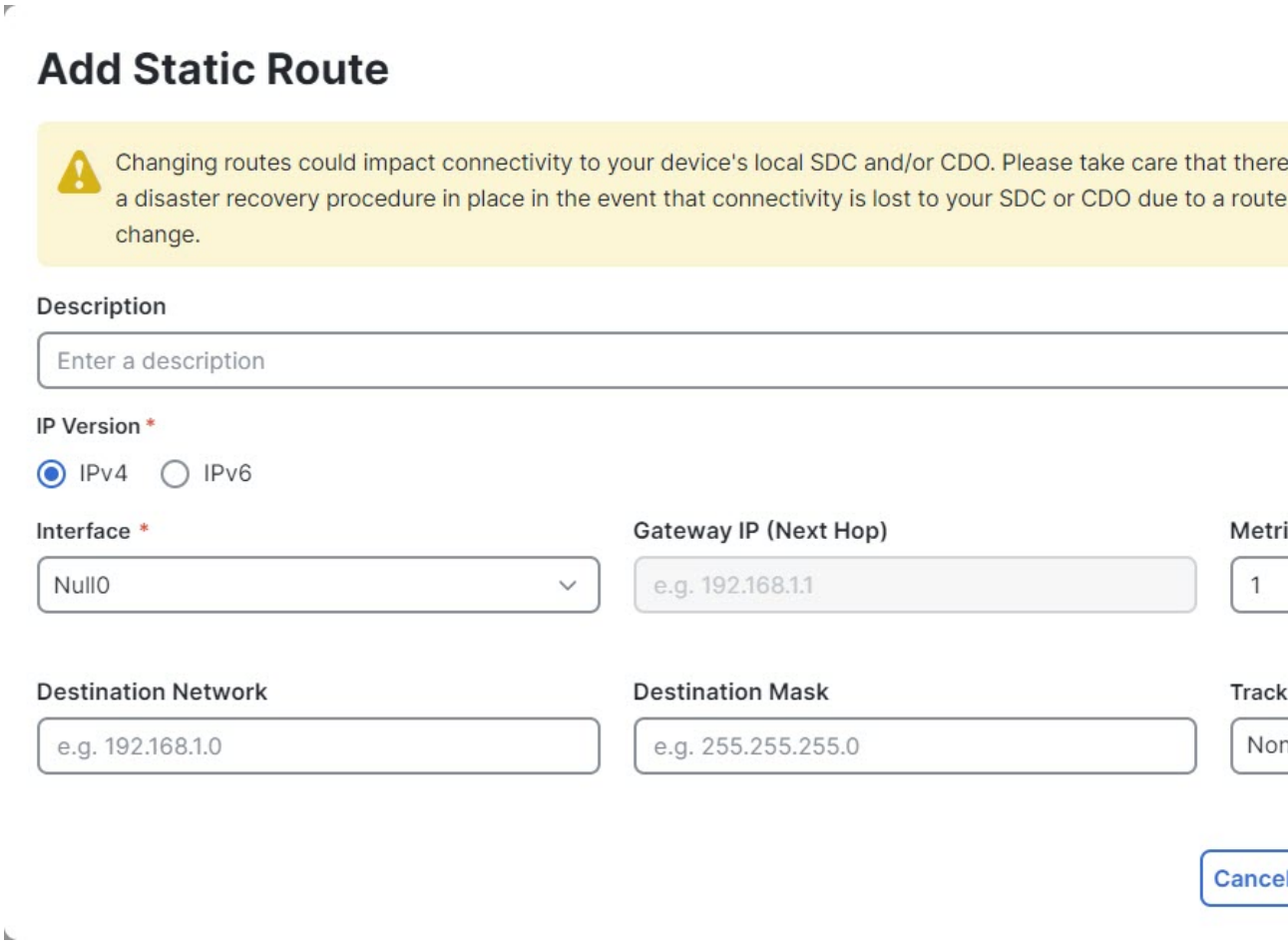
2023년 10월 5일

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

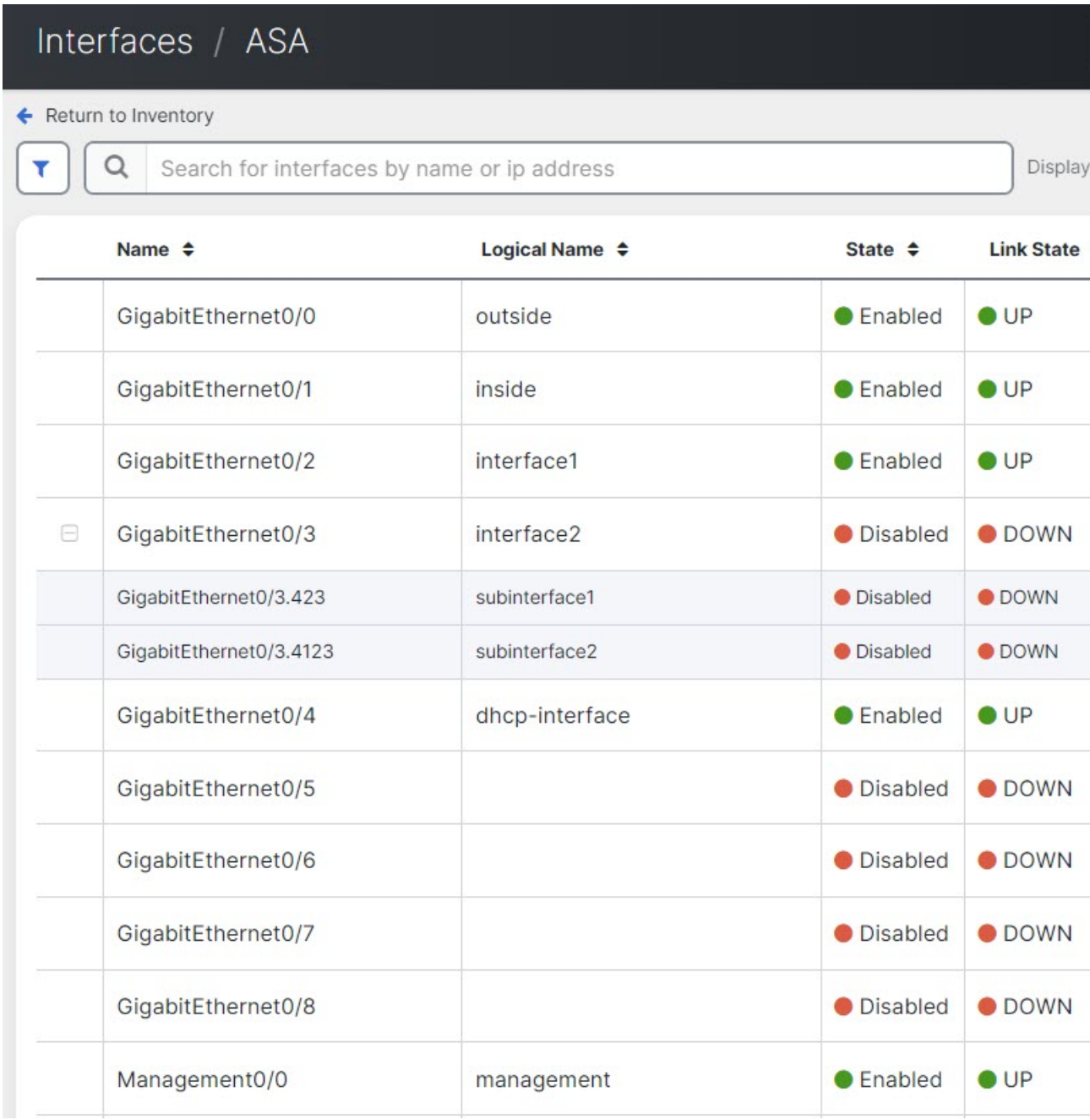
CDO 사용자 인터페이스를 사용하여 **ASA** 인터페이스 설정

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.

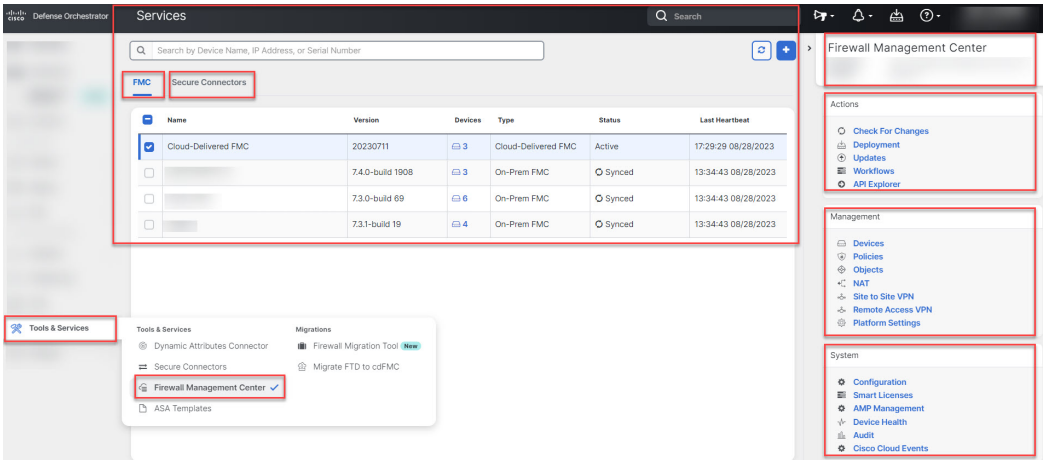

Interfaces / ASA
Return to Inventory
Search for interfaces by name or ip address
Display
Name
Logical Name
State
Link State
GigabitEthernet0/0
outside
Enabled
UP
GigabitEthernet0/1
inside
Enabled
UP
GigabitEthernet0/2
interface1
Enabled
UP
GigabitEthernet0/3
interface2
Disabled
DOWN
GigabitEthernet0/3.423
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

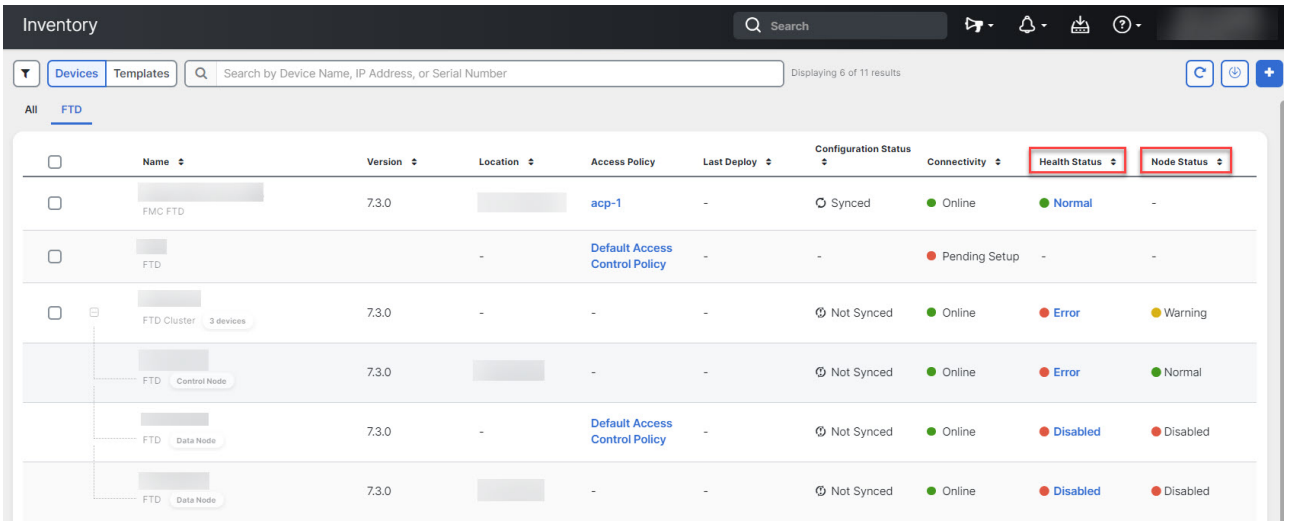
이제 클라우드 제공 Firewall Management Center, 온프레미스 Firewall Management Center 및 보안 커넥터를 새 서비스 페이지에서 관리할 수 있습니다. **Tools & Services(**툴 및 서비스**)** > **Firewall Management Center** 또는 **Secure Connectors(**보안 커넥터**)**를 선택합니다. 자세한 내용은 서비스 페이지 정보 보기를 참조하십시오.



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