클라우드 제공 Firewall Management Center 2023의 새로운 기능

2023년 11월 30일

표 *1:* 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 *2:* 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 ***3:*** 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 ***4:*** 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 ***5:*** 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 ***6:*** 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 *7:* 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 *8:* 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.