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