클라우드 제공 Firewall Management Center 2022의 새로운 기능

2022년 12월 13일

표 *1:* 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 ***2:*** 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