소개

Security Cloud Control Firewall Management (이전 Cisco Defense Orchestrator)는 시스코 방화벽 및 기타 디바이스에서 정책을 간소화하고 통합하는 클라우드 기반 보안 정책 플랫폼입니다. 정책 일관성을 간소화하고 직관적이면서도 고급 인터페이스를 제공하며, 여러 디바이스 관리자 간 구성 변경 사항을 조정합니다.

Security Cloud Control로 Meraki 관리

Meraki MX는 분산형 구축을 위해 설계된 엔터프라이즈 보안 및 소프트웨어 정의 광역 네트워크(SD-WAN) 차세대 방화벽 어플라이언스입니다. 이는 Meraki 대시보드에서 원격으로 관리되며, 이제 Security Cloud Control(이전 Cisco Defense Orchestrator)를 사용하여 Meraki MX 디바이스에서 레이어 3 네트워크 규칙을 관리할 수 있습니다. 자세한 내용은 Meraki 차세대 방화벽 기술 및 Meraki 제품 설명서를 참조하십시오. Security Cloud Control에 Meraki 디바이스를 온보딩하면 Security Cloud Control는 Meraki 대시보드와 통신하여 해당 디바이스를 관리합니다. Security Cloud Control는 MX와 직접 통신하지 않습니다. Security Cloud Control는 구성 요청을 Meraki 대시보드로 안전하게 전송한 다음, 새 구성을 디바이스에 적용합니다. 자세한 내용은 Security Cloud Control가 Meraki와 통신하는 방법, on page 2를 참조하십시오.

Security Cloud Control는 개체 및 정책의 문제를 식별하고 가능한 수정 또는 대체 옵션을 생성하여 Meraki 환경을 최적화하는 데 도움이 됩니다. 이는 디바이스 및 템플릿 모두에 연결된 정책에 적용됩니다. Security Cloud Control 사용 방법:

- 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.

Meraki MX 디바이스 온보딩

Security Cloud Control에 디바이스를 온보딩하기 전에 Meraki 대시보드에서 어카운트를 생성하고 대시보드에 디바이스 또는 템플릿을 온보딩해야 합니다. 조직의 Meraki 대시보드에 어카운트가 없는 경우 API 토큰을 생성할 수 없으며 디바이스가 Security Cloud Control와 통신하지 않습니다.

Meraki MX 디바이스 또는 Meraki 템플릿을 Security Cloud Control에 온보딩할 수 있습니다.

Security Cloud Control 콘솔을 통해 Meraki MX 로그인 자격 증명 및 권한을 처리합니다. 올바른 자격 증명 또는 권한이 없으면 Security Cloud Control가 Meraki 디바이스와 통신할 수 없습니다. 자세한 내용은 Meraki MX 자격 증명 업데이트 및 Meraki API 키 생성 및 검색을 참조하십시오.

Meraki 레이어 3 규칙 및 Security Cloud Control

현재 Security Cloud Control는 레이어 3 방화벽 규칙만 지원합니다. 레이어 3 규칙은 OSI 모델의 네트워크 레이어에서 정책을 적용합니다. 자세한 내용은 레이어 3 방화벽 규칙 사용을 참조하십시오.

Meraki 환경에서는 Meraki 대시보드에서 레이어 3 아웃바운드 규칙을 만들 수 있습니다. Security Cloud Control은 Security Cloud Control에 디바이스를 온보딩할 때 Meraki 대시보드에서 정의한 레이어 3 규칙을 읽습니다. 그런 다음 Security Cloud Control에서 FTD 또는 ASA 규칙을 관리하는 것처럼 이러한 규칙을 관리할 수 있습니다. 자세한 내용은 Meraki 액세스 제어 정책 관리를 참조하십시오.

개체

개체를 사용하여 새 액세스 제어 정책을 세부적으로 조정합니다. Meraki 대시보드는 IP 주소 또는 IP 주소 범위의 프로토콜 및 그룹을 사용합니다. 반면 Security Cloud Control은 다양한 개체를 사용하여 규칙을 관리합니다. Security Cloud Control가 Meraki 프로토콜을 개체로 전송하는 방법에 대한 자세한 내용은 Meraki 디바이스와 연결된 개체를 참조하십시오. Security Cloud Control에서 다음 개체를 생성하고 Meraki 대시보드에서 IP 그룹으로 변환할 수 있습니다.

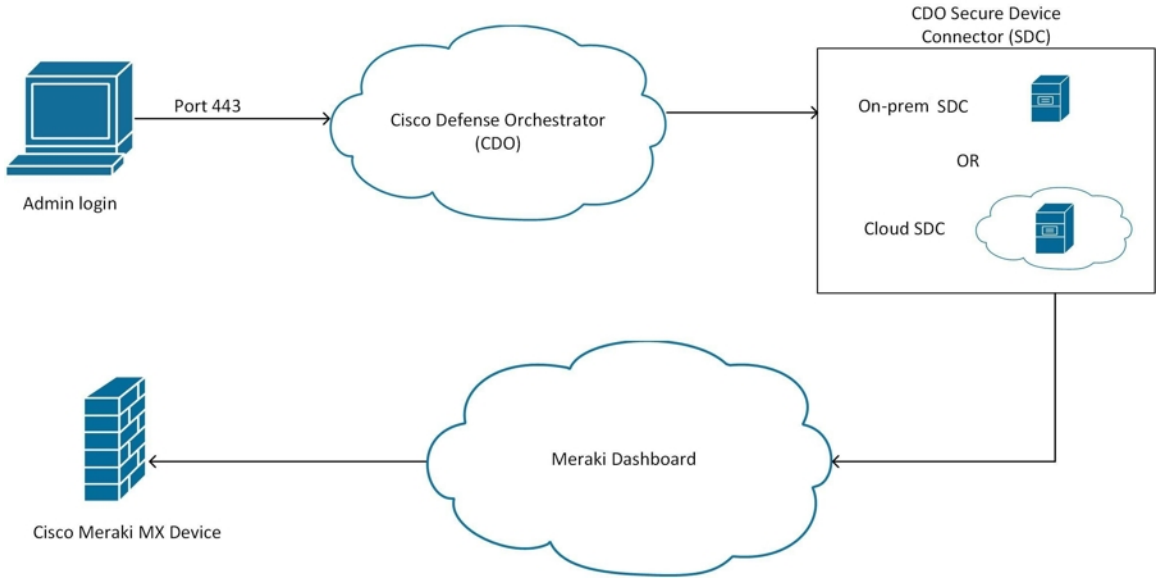
- 네트워크 개체 또는 개체 그룹
- 네트워크 서비스(포트) 개체

Meraki 환경에서는 Meraki 대시보드에서 레이어 3 아웃바운드 규칙을 만들 수 있습니다. Security Cloud Control은 Security Cloud Control에 디바이스를 온보딩할 때 Meraki 대시보드에서 정의한 레이어 3 규칙을 읽습니다. 그런 다음 Security Cloud Control에서 FTD 또는 ASA 규칙을 관리하는 것처럼 이러한 규칙을 관리할 수 있습니다. 자세한 내용은 Meraki 액세스 제어 정책 관리를 참조하십시오.

Security Cloud Control가 Meraki와 통신하는 방법

Security Cloud Control에서 Meraki 디바이스에 구축

Security Cloud Control는 구성 변경 사항을 Meraki MX 디바이스에 직접 구축하지 않습니다. 구축은 여러 단계 프로세스입니다. 아래 다이어그램을 참조하십시오.



Meraki MX 디바이스에 대해 Security Cloud Control에서 변경하는 구성은 구축을 결정할 때까지 Security Cloud Control에서 스테이징됩니다. 설정 변경 사항을 구축 때, Security Cloud Control 는 해당 변경 사항을 Meraki 대시보드로 전달하고, 여기서 Meraki MX 디바이스에 변경 사항이 구현됩니다. Security Cloud Control 는 방화벽 정책을 관리하는 반면 Meraki 대시보드 는 정책이 적용되는 네트워크 를 관리합니다. 두 작업 모두 Meraki MX 디바이스를 통과하는 트래픽 플로우 및 처리 방식에 영향을 미칩니다.

이전 테넌트가 있는 일부 고객은 SDC를 통해 Meraki MX 디바이스를 Security Cloud Control에 연결할 수 있습니다. 이러한 고객인 경우 이 방법을 계속 사용하거나 Meraki MX를 다시 온보딩하거나 연결 자격 증명을 업데이트하여 SDC를 제거할 수 있습니다. Security Cloud Control를 Meraki MX에 연결하는 데 SDC가 필요하지 않습니다.

Security Cloud Control와 Meraki 대시보드의 한 가지 차이점은 개체를 사용한다는 것입니다. Meraki 대시보드에서 생성된 규칙의 경우 Security Cloud Control는 Meraki IP 주소 그룹 또는 IP 주소 범위를 규칙 및 디바이스 정책에 연결하거나 연결할 수 있는 개체로 변환합니다. Security Cloud Control에서 생성된 개체를 Meraki 어플라이언스에 구축할 때 Meraki 대시보드는 해당 개체를 다시 IP 주소 그룹 또는 범위로 변환합니다. Security Cloud Control의 개체는 다른 디바이스 플랫폼과 호환되므로 고유하고 다양합니다. Security Cloud Control에 온보딩된 다른 디바이스가 있는 경우 모든 디바이스에 대해 단일 개체를 생성할 수 있습니다. 자세한 내용은 Meraki 디바이스와 연결된 개체를 참조하십시오.

관련 정보:

- Meraki MX를 Security Cloud Control에 온보딩
- Meraki 액세스 제어 정책

Security Cloud Control Firewall Management 정보

Security Cloud Control Firewall Management (이전 Cisco Defense Orchestrator)는 Cisco 방화벽 및 기타 디바이스에서 정책을 간소화하고 통합하는 클라우드 기반 보안 정책 관리자입니다. 방화벽 및 디바이스는 Security Cloud Control의 제품 아래에 나열된 방화벽에서 관리됩니다.

불일치 사항을 식별하고 이를 수정할 수 있는 툴을 제공하여 보안 정책을 최적화할 수 있도록 지원합니다. 개체 및 정책을 공유하고 설정 템플릿을 만드는 방법을 제공하여 디바이스 전반에 걸쳐 정책 일관성을 유지합니다.

Security Cloud Control이 ASDM(Adaptive Security Device Manager)와 같은 로컬 디바이스 관리자와 공존하기 때문에, Security Cloud Control 및 다른 관리자에 의해 수행된 구성 변경 사항을 추적한 후 관리자 간 차이를 조정합니다.

Security Cloud Control은 다양한 디바이스를 한 곳에서 관리할 수 있는 직관적인 사용자 인터페이스를 제공합니다. 기존 CLI 인터페이스에 몇 가지 개선 사항이 추가되어 고급 사용자가 관리 효율성을 더욱 높일 수도 있습니다.

또한 온프레미스 또는 클라우드 제공 Firewall Management Center에 위협 방어 디바이스를 신속하게 온보딩할 수 있도록 안내하는 "Day 0" 경험을 제공합니다. 또한 여러분이 활용할 수 있는 다른 주요 기능들을 제시하고, 이를 활성화하고 구성하는 데 도움을 줍니다.

디바이스 온보딩

디바이스를 온보딩하기 전에 설치 마법사를 성공적으로 완료하고 디바이스에 라이선스를 부여했는지 확인합니다. 그런 다음 Security Cloud Control의 온보딩 마법사를 사용하여 디바이스를 온보딩합니다. Security Cloud Control는 대규모 구축을 손쉽게 관리할 수 있습니다.

디바이스 및 서비스 온보딩을 참조하십시오.

참고 디바이스를 Security Cloud Control 테넌트에 온보딩하면 한 Security Cloud Control 테넌트 간에 디바이스를 마이그레이션할 수 없습니다. 디바이스를 새 테넌트로 이동하려면 해당 디바이스를 새 테넌트에 다시 등록해야 합니다.

Security Cloud Control이 지원하는 디바이스의 전체 목록은 지원되는 디바이스, 소프트웨어 및 하드웨어를 참조하십시오.

Cisco 온라인 개인정보 보호정책

Cisco Systems, Inc. 및 자회사("Cisco"로 통칭)에서는 개인 정보를 보호하고 사용자가 Cisco 웹사이트에서 그리고 시스코 제품 및 서비스("솔루션")의 사용에서 유익한 경험을 할 수 있도록 최선을 다하고 있습니다. Cisco 온라인 개인정보 보호정책을 주의 깊게 읽고 Cisco에서 개인 정보를 수집, 사용, 공유 및 보호하는 방법을 명확하게 이해하십시오.

Security Cloud Control 대시보드

Security Cloud Control 대시보드는 다양한 범주에 걸쳐 조직 수준의 세부 정보을 모니터링하고 관리하기 위한 중앙 허브입니다. 로그인하면 중요한 인사이트와 보안 및 운영 효율성 최적화하기 위한 작업을 제공하는 맞춤형 대시보드에 액세스할 수 있습니다.

대시보드 사용자 맞춤화

표시되는 위젯을 맞춤 설정하여 대시보드를 특정 요구 사항에 맞게 조정합니다.

1. **Home** 페이지에서 **Customize(**맞춤화**)**를 클릭합니다.
2. 대시보드에 표시할 위젯을 선택하거나 선택을 해제합니다.
3. 위젯을 끌어다 놓아 원하는 대로 정렬할 수 있습니다.

상위 정보

이 섹션에서는 다양한 테넌트 수준 메트릭에 대한 상세한 인사이트를 제공합니다. 활성화된 경우 다음 위젯을 볼 수 있습니다.

- **Configuration States(**구성 상태**)**: 사용자의 디바이스에 설정된 구성과 Security Cloud Control에서 유지 관리하는 구성 간의 불일치를 나타냅니다. 이 비교를 통해 존재할 수 있는 불일치나 충돌을 식별하는 데 도움이 됩니다.

  자세한 내용은 디바이스 관리를 참조하십시오.

- **Change Log Management(**변경 로그 관리**)**: 정확한 운영 제어를 위해 변경 로그를 관리하는 데 도움이 됩니다. 위젯에 **Completed(**완료됨**)** 및 **Pending(**보류 중**)** 변경 로그가 표시됩니다.

  자세한 내용은 Change Logs(변경 로그)를 참조하십시오.

- **RA VPN Sessions(RA VPN** 세션**)**: 원격 액세스 VPN 세션을 모니터링할 수 있습니다.

  자세한 내용은 RA VPN 세션을 참조하십시오.

- **Overall Inventory(**전체 재고 목록**)**: 모든 디바이스의 상태를 모니터링할 수 있습니다. **Issues(**문제**)**, **Pending Actions(**보류 중인 작업**)**, **Other(**기타**)**, **Online(**온라인**)**으로 분류된 총 디바이스 수와 하드웨어 지원 기간이 가까워지거나 만료된 위젯의 총 수가 표시됩니다.

  자세한 내용은 모든 디바이스를 참조하십시오.

- **Site-to-Site VPN(**사이트 간 **VPN)**: 사이트 간 VPN 연결을 관리하고 평가하는 데 도움이 됩니다. 위젯에 총 VPN 터널 수와 **Active(**활성**)** 및 **Idle(**유휴**)**의 비율이 표시됩니다.

  자세한 내용은 사이트 간 VPN을 참조하십시오.

- 어카운트 및 자산:
  - 멀티 클라우드 어카운트 및 리소스를 효과적으로 추적하고 관리할 수 있습니다. 여기에서 Multicloud Defense 컨트롤러를 실행할 수 있습니다.
  - **+Add Account(+**어카운트 추가**)**를 클릭하여 새 어카운트을 추가합니다.

자세한 내용은 Multicloud Defense Controller를 참조하십시오.

- **Top Risky Destinations(**상위 위험한 대상**)**: 액세스 권한이 부여된 상위 위험한 대상을 식별하고 모니터링하는 데 도움이 됩니다. 위젯은 애플리케이션 및 URL 범주를 나열하며, 지난 90일, 60일 또는 30일 동안의 데이터를 필터링할 수 있습니다. 허용된 트래픽(기본값)과 차단된 트래픽 사이에서 필터링할 수 있습니다.
- **Top Intrusion and Malware Events(**상위 침입 및 멀웨어 이벤트**)**: 상위 침입 및 멀웨어 이벤트를 모니터링하고 대응할 수 있습니다. 위젯은 침입 이벤트와 멀웨어이벤트를 표시하며, 지난 90일, 60일, 30일 동안의 데이터를 필터링할 수 있습니다. 허용된 이벤트(기본값)와 차단된 이벤트 사이에서 필터링할 수 있습니다.

발표

최신 Security Cloud Control 기능 및 업데이트를 보려면 알림 아이콘 클릭합니다. 목록에 있는 항목에 대한 추가 정보가 필요할 경우 관련 문서 링크가 제공됩니다.

번역에 관하여
Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.

번역에 관하여
Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.