Cisco Defense Orchestrator를 사용한 Meraki 관리

Cisco Defense Orchestrator를 사용한 Meraki 관리

Meraki MX는 분산형 배포을 위해 설계된 엔터프라이즈 보안 및 소프트웨어 정의 광역 네트워크(SD-WAN) 차세대 방화벽 어플라이언스입니다. 이는 Meraki 대시보드에서 원격으로 관리되며, 이제 CDO(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. Meraki 디바이스를 CDO에 온보딩하면 CDO는 Meraki 대시보드와 통신하여 해당 디바이스를 관리합니다. CDO는 MX와 직접 통신하지 않습니다. CDO는 구성 요청을 Meraki 대시보드로 안전하게 전송한 다음 새 구성을 디바이스에 적용합니다. 자세한 내용은 CDO가 Meraki와 통신하는 방법를 참조하십시오.

CDO는 개체 및 정책의 문제를 식별하고 가능한 편집 또는 대체 옵션을 생성하여 Meraki 환경을 최적화하는 데 도움이 됩니다. 이는 디바이스 및 템플릿 모두에 연결된 정책에 적용됩니다. CDO를 사용하여 다음을 수행합니다.

- 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

CDO에 디바이스를 온보딩하기 전에 Meraki 대시보드에서 계정을 생성하고 대시보드에 디바이스 또는 템플릿을 온보딩해야 합니다. 조직의 Meraki 대시보드에 계정이 없는 경우 API 토큰을 생성할 수 없으며 디바이스가 CDO와 통신하지 않습니다.

Cisco Defense Orchestrator를 사용한 Meraki 관리

Meraki MX 디바이스 또는 Meraki 템플릿을 CDO에 온보딩할 수 있습니다.

CDO 콘솔을 통해 Meraki MX 로그인 자격 증명 및 권한을 처리합니다. 올바른 자격 증명 또는 권한이 없는 경우 CDO가 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 CDO

현재 CDO는 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 생성할 수 있습니다. CDO는 디바이스를 CDO에 온보딩할 때 Meraki 대시보드에서 정의한 레이어 3 규칙을 읽습니다. 그런 다음 CDO에서 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 CDO는 다양한 개체를 사용하여 규칙을 관리합니다. CDO가 Meraki 프로토콜을 개체로 전송하는 방법에 대한 자세한 내용은 Meraki 디바이스와 연결된 개체를 참조하십시오. CDO에서 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 생성할 수 있습니다. CDO는 디바이스를 CDO에 온보딩할 때 Meraki 대시보드에서 정의한 레이어 3 규칙을 읽습니다. 그런 다음 CDO에서 FTD 또는 ASA 규칙을 관리하는 것처럼 이러한 규칙을 관리할 수 있습니다. 자세한 내용은 Meraki 액세스 제어 정책 관리를 참조하십시오.