Cisco Defense Orchestrator를 사용한 AWS 관리

Cisco Defense Orchestrator를 사용한 AWS 관리

Cisco Defense Orchestrator를 사용하여 **AWS VPC** 관리

CDO는 AWS(Amazon Web Services) VPC(Virtual Private Cloud)를 위한 간소화된 관리 인터페이스를 제공합니다. 다른 디바이스를 관리하는 것과 동일한 인터페이스에서 AWS VPC 및 해당 구성 요소를 관리할 수 있습니다.

CDO를 사용하여 다음 작업을 수행합니다.

- AWS VPC 온보딩
- VPC 세부 정보 보기
- 보안 그룹 작업
- 다른 매니지드 디바이스와 AWS 개체 공유
- AWS 사이트 간 VPN 연결 모니터링
- AWS 디바이스에 대한 변경 사항 모니터링
- AWS 사이트 간 VPN 터널 보기

다음은 CDO가 향후 지원할 것으로 기대하는 일반적인 AWS 기능입니다.

- 보안 그룹에 대한 로드 밸런서(탄력적, 네트워크 및 애플리케이션 로드 밸런서)의 관계를 표시합니다.
- 보안 그룹에 대한 자동 확장 그룹의 관계를 표시합니다.

CDO를 사용하여 보안 그룹의 이러한 측면을 관리할 수 없습니다.

Cisco Defense Orchestrator를 사용한 AWS 관리

- 보안 그룹 생성.
- 보안 그룹을 인스턴스에 연결.
- 로드 밸런서에 보안 그룹 할당
- VPC 피어링.

온보드 AWS VPC

CDO의 온보딩 마법사를 사용하여 AWS VPC를 온보딩하는 것으로 시작합니다. 자세한 내용은 AWS VPC 온보딩을 참조하십시오.

AWS VPC에 태그가 포함된 경우 디바이스를 온보딩할 때 이러한 태그를 CDO로 가져옵니다. CDO는 태그를 레이블로 나타냅니다. 보안 클라우드 개체 또는 규칙과 달리 레이블은 AWS VPC에 자동으로 동기화되지 않습니다. 자세한 내용은 레이블 및 필터링을 참조하십시오.

CDO 콘솔을 통해 AWS VPC 로그인 자격 증명 및 권한을 처리합니다. 올바른 자격 증명 또는 권한이 없으면 CDO가 AWS VPC와 통신할 수 없습니다. 자세한 내용은 AWS VPC 연결 자격 증명 업데이트 및 IAM 사용자의 권한 변경을 참조하십시오.

AWS VPC 세부 정보 보기

AWS VPC가 온보딩되면 AWS VPC의 ID, 지역, 보안 그룹, 그리고 이러한 보안 그룹에 할당된 규칙 및 개체를 볼 수 있습니다.

보안 그룹 작업

보안 그룹은 모든 AWS 인스턴스 및 보안 그룹과 연결된 기타 엔터티에 대한 인바운드 및 아웃바운드 네트워크 트래픽을 제어하는 규칙의 모음입니다. AWS VPC를 CDO에 온보딩할 때 보안 그룹은 CDO에 보안 그룹 개체로 저장됩니다.

CDO를 사용하여 다음 작업을 수행할 수 있습니다.

- 보안 그룹에서 새 규칙을 생성합니다.
- 보안 그룹에서 변경 사항을 확인하고 규칙을 편집 및 삭제합니다.

현재는 VPC에서 새 보안 그룹을 생성할 수 없습니다.

자세한 내용은 다음 항목을 참조하십시오.

- AWS VPC 보안 그룹 및 인스턴스
- AWS VPC 보안 그룹 규칙 관리
- AWS와 기타 매니지드 디바이스 간 개체 공유

AWS와 기타 매니지드 디바이스 간 개체 공유

CDO는 규칙에서 개체를 사용하도록 지원합니다. 개체는 값의 컨테이너입니다. 예를 들어 리소스의 IP 주소를 포함하고 의미 있는 이름을 지정하는 네트워크 개체가 있을 수 있습니다. 그런 다음 리소스

Cisco Defense Orchestrator를 사용한 AWS 관리

의 리터럴 IP 주소를 사용하는 대신 액세스 규칙에서 해당 개체를 규칙 소스 또는 대상의 일부로 사용할 수 있습니다. 다른 규칙에서 해당 개체를 재사용할 수도 있습니다. 개체의 값을 한 번 변경하면 해당 개체를 사용하는 모든 규칙이 새 값을 사용하기 시작합니다.

AWS VPC를 온보딩한 후 CDO는 AWS 개념을 보안 그룹 개체 및 기존 보안 그룹 규칙에 있는 네트워크 개체 및 서비스 개체로 변환합니다.

네트워크 개체 및 서비스 개체(포트 개체라고도 함)는 CDO를 사용하여 관리하는 다른 디바이스와 AWS VPC 간에 공유할 수 있습니다. 보안 그룹 개체는 AWS에 고유합니다.

자세한 내용은 AWS와 기타 매니지드 디바이스 간 개체 공유를 참조하십시오.

AWS 사이트 간 VPN 연결 모니터링

AWS 사이트 간 VPN은 보안 터널을 통해 AWS VPC를 엔터프라이즈 네트워크에 연결합니다. 자세한 내용은 AWS 사이트 간 VPN 관리를 참조하십시오.

AWS VPC 및 AWS 보안 그룹에 대한 변경 사항 모니터링

변경 로그

변경 로그는 CDO에서 수행되는 구성 변경 사항을 지속적으로 캡처합니다. 이 단일 보기에는 지원되는 모든 디바이스 및 서비스에 대한 변경 사항이 포함됩니다. 다음은 변경 로그의 몇 가지 기능입니다.

- 디바이스 구성에 대한 변경 사항을 나란히 비교합니다.
- 모든 변경 로그 항목에 대한 일반 영어 레이블입니다.
- 디바이스의 온보딩 및 제거를 기록합니다.
- CDO 외부에서 발생하는 정책 변경 충돌 탐지.
- 인시던트 조사 또는 문제 해결 중에 누가, 무엇을, 언제 하는지에 대한 답변을 제공합니다.

변경 요청 관리

변경 요청 관리를 사용하면 서드파티 티켓팅 시스템에서 연 변경 요청 및 해당 비즈니스 근거를 변경 로그의 이벤트와 연결할 수 있습니다. CDO에서 변경 요청을 생성하고, 이를 고유한 이름으로 식별하고, 변경에 대한 설명을 입력하고, 변경 요청을 변경 로그 이벤트와 연결하려면 변경 요청 관리를 사용합니다. 나중에 변경 로그에서 변경 요청 이름을 검색할 수 있습니다.

일반 관리 작업 지원

CDO는 AWS 보안 그룹에 대해 다음과 같은 공통 관리 작업을 지원합니다.

- 디바이스 구성 대량 구축
- 모든 디바이스 구성 읽기
- 대역외 변경 탐지
- 충돌 탐지

Cisco Defense Orchestrator를 사용한 AWS 관리