시작하기 전에

이 장에서는 Security Cloud Control 플랫폼과 지원되는 다양한 제품에 대한 개요를 제공합니다. Cisco 방화벽 및 기타 디바이스에 대한 플랫폼의 관리 기능을 소개합니다.

Cisco Security Cloud Control 정보

Cisco Security Cloud Control은 보안 제품을 관리하고 단일 통합 인터페이스에서 보안 성과를 달성할 수 있는 보안 플랫폼입니다.

보안 제품을 통합하는 것은 간소화된 경험입니다. 시스코 보안 제품에 대한 구독을 구매하고 나면 구매한 모든 구독에 대한 단일 클레임 코드가 포함된 단일 이메일을 받게 됩니다. 새 Security Cloud Control 조직에 클레임 코드를 입력하면 모든 제품이 Security Cloud Control로 동시에 프로비저닝됩니다.

Security Cloud 제어 내에서 사용자 및 그룹 관리가 플랫폼 수준에서 이루어집니다. 이러한 사용자 및 그룹에는 역할이 할당되어 Security Cloud Control 및 통합 제품을 관리할 수 있는 권한을 정의합니다.

제품과 툴 간의 탐색은 직관적이며 모든 통합 제품에 대한 공통 플랫폼 메뉴 및 툴바 사용하여 표준화되었습니다.

Security Cloud 플랫폼의 모든 통합 제품에 다음과 같은 추가 핵심 서비스를 제공합니다.

- 플랫폼 관리: 역할 기반 액세스 제어 관리, 구독 클레임 및 제품 인스턴스의 표준화된 지역 구축과 같은 공통 서비스를 Security Cloud Control에서 제공합니다. Security Cloud Control는 이러한 기능을 중앙 집중화하여 플랫폼에서 관리되는 모든 Cisco 보안 제품에서 액세스를 프로비저닝하고 관리하는 데 있어 일관된 사용자 경험을 보장합니다. Security Cloud Control의 기본 내비게이션 바에 있는 플랫폼 관리 메뉴에서 이러한 공통 서비스에 접근할 수 있습니다.
- **AI Assistant**: Security Cloud Control의 Cisco AI Assistant AI 기반 인사이트, 자동화 및 상황별 지침을 제공하여 보안 운영을 간소화 하도록 설계되었습니다. 방화벽, Duo, 및 Secure Access를 비

롯한 Cisco 보안 제품 전반에서 보안 정책을 관리하고, 문제를 해결하고, 설정을 최적화하는 데 도움이 됩니다. 어시스턴트는 자연어 처리 및 플랫폼 간 인텔리전스를 활용하여 효율성을 높이고 사고 대응을 가속화하며 보안 워크플로우를 간소화합니다.

- **Global Search(**전역검색**)**: 플랫폼의 제품 전체에서 값을 검색할 수 있는 기능입니다.
- **Shared Objects(**공유 개체**)**: 디바이스 및 정책 전체에서 공유할 수 있는 개체를 생성하고 관리합니다.
- **Unified documentation portal(**통합문서 포털**)**: 하나의 포털 에서 모든 문서에 액세스할 수 있는 문서 "도움말" 환경입니다.

Security Cloud Control과 통합할 수 있는 제품

Security Cloud Control에서 다음 모든 보안 제품을 관리할 수 있습니다.

- AI Defense
- Security Cloud Control Firewall Management
- Multicloud Defense
- Secure Access
- Secure Workload

Security Cloud Control에서 실행할 수 있는 제품

Security Cloud Control에서 이러한 보안 제품을 실행할 수 있습니다. 이러한 제품은 출시 후에는 독립형 제품으로 작동하며 Security Cloud Control를 통해 관리할 수 없습니다. Security Cloud Control에서 그러한 제품의 라이선스를 요청하거나 비활성화만 할 수 있습니다.

Security Cloud Control 툴바 에서 9개의 점으로 이루어진 메뉴  를 클릭하여 다음 제품을 실행합니다.

- Cisco Secure Email Threat Defense
- Cisco Secure Endpoint
- Cisco Duo
- Cisco XDR

Security Cloud Control에서 지원하는 제품

Security Cloud Control와 통합 가능한 지원 제품은 다음과 같습니다.

AI Defense: AI Defense는 AI 사용자 및 제공자의 위험을 해결합니다. Security Cloud Control, AI Defense에서 네트워크 가시성 및 시행 지점을 사용하여 분산형 클라우드 환경에서 승인된 AI 워크로드, 승인되지 않은 AI 워크로드, 애플리케이션, 모델, 데이터 및 사용자 액세스를 검색하기 위한 탐지 및 시행

조치를 추가합니다. AI 기반 서비스를 개발하고 제공하는 조직을 위해 AI Defense는 AI 모델이 제공되기 전에 취약점을 탐지합니다. 실행 중인 AI 애플리케이션의 경우 AI Defense 가드레일은 신속한 주입, 서비스 거부, 데이터 유출 등 빠르게 진화하는 위협을 차단합니다. 자세한 내용은 AI Defense 문서를 참조하십시오.

Security Cloud Control Firewall Management: Security Cloud Control Firewall Management (이전 Cisco Defense Orchestrator)는 Cisco 방화벽 및 기타 디바이스에서 정책을 간소화하고 통합하는 클라우드 기반 보안 정책 관리자입니다. 자세한 내용은 보안 클라우드의 방화벽 제어 설명서를 참조하십시오.

Multicloud Defense: Multicloud Defense 는 멀티 클라우드 보안에 대한 간소화된 고도로 자동화된 접근 방식을 제공합니다. 이 솔루션을 사용하면 조직은 단일 SaaS 제공 컨트롤 플레인 및 중앙 집중식 또는 분산형 PaaS 제공 데이터 플레인 아키텍처를 사용하여 멀티 클라우드 환경을 관리하고 보호할 수 있습니다. Multicloud Defense는 모든 주요 클라우드 제공자에 걸쳐 지속적인 가시성, 통합 보호 및 유동 정책 업데이트를 제공하므로 각 클라우드 제공자를 위한 솔루션에 대해 별도의 포인트 솔루션이 필요하지 않습니다. 자세한 내용은 Multicloud Defense 설명서를 참조하십시오.

Secure Access: Cisco Secure Access는 인터넷 기반 위협에 대한 여러 수준의 방어를 제공하는 클라우드 기반 플랫폼입니다. 조직의 네트워크 또는 로밍 오프네트워크 상태에서 인터넷, SaaS 애플리케이션 및 사설 디지털 리소스에 안전하게 연결합니다. 정책 규칙을 사용하여 리소스, 사용자, 디바이스 모음에 대해 보안 제어를 구성하고 시행합니다.자세한 내용은 Secure Access 설명서를 참조하십시오. Secure Access 구독에는 추가 비용 없이 Security Cloud Control를 통한 ID 인텔리전스 통합이 포함되며, 독립형 ID 인텔리전스 대시보드에 대한 액세스는 포함되지 않습니다. 자세한 내용은 Cisco Identity Intelligence와 Secure Access 통합을 참조하십시오.

Secure Workload: Cisco Secure Workload (이전 Tetration)는 단일 콘솔의 모든 워크로드, 환경 또는 위치에 걸쳐 제로 트러스트 마이크로 세그멘테이션을 원활하게 제공합니다. 모든 워크로드 상호작용에 대한 포괄적인 가시성과 강력한 AI/ML 기반 자동화 통해, Secure Workload는 측면 이동을 방지하여 공격 표면을 줄이고, 워크로드 동작 이상을 식별하고, 위협을 신속하게 치료하고, 정책 컴플라이언스를 지속적으로 모니터링합니다. 자세한 내용은 Secure Workload 설명서를 참조하십시오.

Security Cloud Control Firewall Management 정보

Security Cloud Control Firewall Management(이전 Cisco Defense Orchestrator)는 분산 환경에서 보안 정책 관리를 간소화하여 관리 대상 모든 방화벽에 걸쳐 일관된 정책을 보장합니다. 방화벽 및 디바이스는 Security Cloud Control의 제품 아래에 나열된 방화벽에서 관리됩니다.

보안 정책의 불일치를 식별하고 해결 도구를 제공함으로써 보안 정책을 최적화합니다. 이 플랫폼은 개체 및 정책 공유와 구성 템플릿 생성을 지원하여 모든 디바이스에서 정책의 일관성을 보장합니다.

Adaptive Security Device Manager(ASDM)와 같은 로컬 디바이스 관리자와 공존하며, Security Cloud Control은 자체 및 다른 관리자에 의해 수행된 구성 변경 사항을 추적하고 불일치를 조정합니다.

직관적인 사용자 인터페이스를 특징으로 하여, Security Cloud Control은 단일 플랫폼에서 다양한 기기를 관리할 수 있습니다. 고급 사용자는 보다 효율적인 관리를 위해 향상된 CLI 인터페이스를 활용할 수도 있습니다.

이 플랫폼은 안내형 "Day 0" 경험을 제공하여 온프레미스 또는 클라우드 제공 Firewall Management Center에 위협 방어 디바이스를 신속하게 온보딩할 수 있도록 지원합니다. 주요 기능을 강조하여 잠재적 이점을 제시하고, 해당 기능의 활성화 및 설정을 지원합니다.

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 Control를 사용하여 Secure Firewall ASA 관리

Security Cloud Control(이전 Cisco Defense Orchestrator)는 모든 ASA 디바이스에서 간단하고 일관되며 안전한 보안 정책 관리 방법을 제공하는 클라우드 기반의 다중 디바이스 관리자입니다.

이 문서의 목표는 Security Cloud Control를 처음 사용하는 고객에게 개체 및 정책을 표준화하고, 매니지드 디바이스를 업그레이드하고, VPN 정책을 관리하고, 원격 작업자를 모니터링하는 데 사용할 수 있는 활동의 개요를 제공하는 것입니다. 이 문서에서는 다음 사항을 가정합니다.

- ASA가 이미 구성되어 있으며 엔터프라이즈에서 사용 중입니다.
- Security Cloud Control에서 관리하려는 ASA를 인터넷에서 직접 액세스할 수 없는 경우 네트워크에서 SDC(Secure Device Connector)를 구축해야 합니다. SDC는 Security Cloud Control와 ASA 간의 통신을 관리합니다.

  자세한 내용은 Secure Device Connector 및 Secure Event Connector을 위한 VM 구축를 참조하십시오.

Secure Device Connectors

디바이스 자격 증명을 사용하여 Security Cloud Control를 ASA에 연결하는 경우, 네트워크에서 SDC(Secure Device Connector)를 다운로드하고 구축하여 Security Cloud Control와 ASA 간의 통신을 관리하는 것이 모범 사례입니다. ASA는 모두 디바이스 자격 증명을 사용하여 Security Cloud Control에 온보딩할 수 있습니다. SDC가 ASA와 Security Cloud Control 간의 통신을 관리하는 것을 원치 않고 인터넷에서 직접 디바이스에 액세스할 수 있는 경우, 네트워크에 SDC를 설치할 필요가 없습니다. Cloud Connector를 사용하여 ASA를 Security Cloud Control에 온보딩할 수 있습니다.

테넌트에 대해 둘 이상의 SDC를 구축하면 성능 저하 없이 Security Cloud Control 테넌트를 사용하여 더 많은 디바이스를 관리할 수 있습니다. 단일 SDC에서 관리할 수 있는 디바이스의 수는 해당 디바이스에 구현된 기능 및 해당 구성 파일의 크기에 따라 달라집니다. 그러나 구축을 계획할 때는 1개의 SDC가 약 500개의 디바이스를 지원할 것으로 예상합니다.

SDC를 보려면 다음을 수행합니다.

1. Security Cloud Control에 로그인합니다.
2. Security Cloud Control 메뉴에서 **Admin(관리)** > **Secure Connector(보안 커넥터)**를 선택합니다.

디바이스 온보딩

대량으로 또는 한 번에 하나씩 ASA를 Security Cloud Control에 온보딩할 수 있습니다.

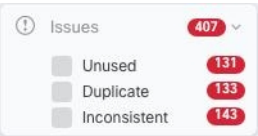
Security Cloud Control에서 지원하는 ASA 소프트웨어 및 하드웨어에 대한 자세한 내용은 지원 세부 정보의 내용을 참조하십시오.

정책 오케스트레이션

정책 오케스트레이션에는 개체 및 정책 검토가 포함됩니다. ASA 정책으로 작업할 때는 Security Cloud Control에서 "액세스 그룹"을 "액세스 정책"이라고 합니다. ASA 액세스 정책은 Security Cloud Control 메뉴 바 Policies(정책) > ASA Access Policies(ASA 액세스 정책)에서 찾을 수 있습니다.

네트워크 개체 문제 해결

시간이 지남에 따라 보안 디바이스에 더 이상 사용되지 않거나, 다른 개체와 중복되거나, 디바이스 간에 값이 일치하지 않는 개체가 있을 수 있습니다. 이러한 개체 문제를 해결 하 여 오케스트레이션 작업을 시작 합니다.



아래의 순서대로 개체 문제를 해결합니다. 초기 단계에서 수행하는 작업을 통해 이후 단계에서 해결해야 하는 문제를 해결할 수 있습니다.

1. 미사용 개체 문제 해결. Unused objects(미사용 개체) 는 디바이스에 존재하지만 다른 개체, 액세스 목록 또는 NAT 규칙에서 참조하지 않는 개체입니다.

2. 중복 개체 문제 해결. 중복 개체는 이름은 다르지만 값은 동일한 디바이스에 있는 두 개 이상의 개체입니다. 이러한 개체는 대개 실수로 생성되고 유사한 용도로 사용되며 다른 정책에서 사용됩니다. 중복 개체 문제를 해결한 후 Security Cloud Control는 유지된 개체 이름으로 영향을 받는 모든 개체 참조를 업데이트합니다.

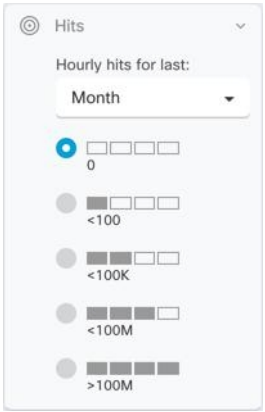
3. 불일치 개체 문제 해결. 불일치 개체는 두 개 이상의 디바이스에서 이름은 같지만 값이 다른 개체입니다. 사용자가 동일한 이름 및 콘텐츠를 사용하여 서로 다른 구성에서 개체를 생성하지만 시간이 지남에 따라 이러한 개체의 값이 달라지므로 불일치가 발생하는 경우가 있습니다. 이러한 현상은 보안 문제입니다. 오래된 리소스를 보호하는 규칙이 있을 수 있습니다.

섀도우 규칙 수정

네트워크 개체 문제를 해결했으므로 이제 섀도우 규칙에 대한 네트워크 정책을 검토하고 해결합니다. 섀도우 규칙은 ASA 액세스 정책 페이지에서 반달 모양의 배지로 표시됩니다. 액세스 정책의 규칙은 목록에서 구성되며 위에서 아래로 한 번에 하나씩 평가됩니다. 네트워크 트래픽이 정책에서 섀도우 규칙 위의 규칙과 일치하므로 정책의 섀도우 규칙은 일치하지 않습니다. 적중되지 않는 섀도우 규칙이 있는 경우 해당 규칙을 제거하거나 정책을 편집하여 규칙을 적용합니다.

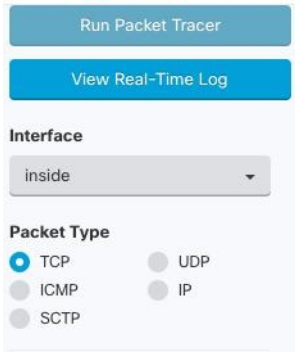
정책 적중률 평가

정책의 규칙이 실제로 네트워크 트래픽을 평가하는지 확인합니다. Security Cloud Control는 정책의 규칙에 대한 적중률 데이터를 매 시간 수집합니다. Security Cloud Control에서 디바이스를 오래 관리할수록 특정 규칙의 적중률 데이터가 더 의미가 있습니다. 관심 있는 기간의 적중 횟수를 기준으로 ASA 액세스 정책을 필터링하여 적중 여부를 확인합니다. 그렇지 않은 경우 정책을 다시 작성하거나 삭제하는 것이 좋습니다.



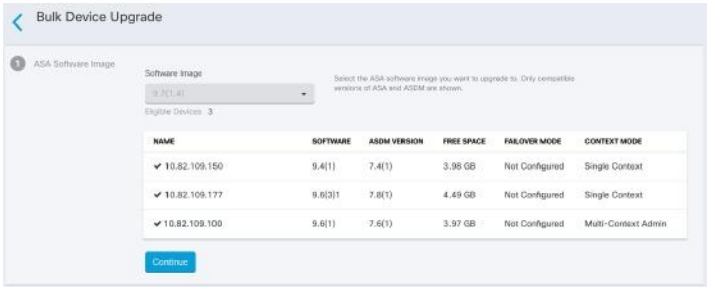
정책 문제 해결

ASA 패킷 트레이서를 사용하여 정책을 통해 가상 패킷의 경로를 테스트하고 규칙이 실수로 액세스를 차단하거나 허용하는지 확인할 수 있습니다.



ASA 및 ASDM 업그레이드

그런 다음 최신 버전의 ASA 및 ASDM으로 업그레이드합니다. 고객은 Security Cloud Control를 사용하여 ASA를 업그레이드할 때 75%~90%의 시간 절약을 보고했습니다.



Security Cloud Control는 단일 상황 또는 다중 상황 모드에서 개별 ASA 또는 여러 ASA에 설치된 ASA 및 ASDM 이미지를 업그레이드할 수 있는 마법사를 제공합니다. Security Cloud Control는 ASA 및 ASDM 이미지 데이터베이스를 유지 관리합니다.

Security Cloud Control는 백그라운드에서 필요한 업그레이드 호환성 검사를 수행합니다. 마법사는 호환되는 ASA 및 ASDM 이미지를 선택하고 설치하고 디바이스를 재부팅하여 업그레이드를 완료하는 프로세스를 안내합니다. Security Cloud Control는 사용자가 Security Cloud Control에서 선택한 이미지가 ASA에 복사되어 설치된 이미지인지 확인하여 업그레이드 프로세스를 보호합니다.

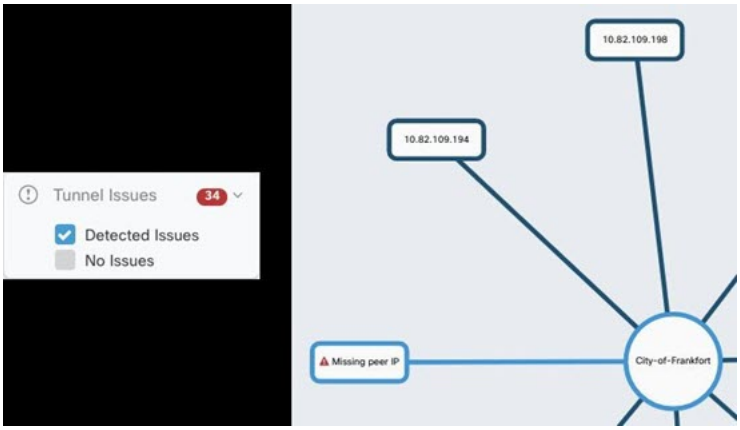
Security Cloud Control는 주기적으로 데이터베이스를 검토하고 최신 ASA 및 ASDM 이미지를 데이터베이스에 추가합니다. Security Cloud Control는 일반적으로 사용 가능한(GA) 이미지만 지원하며 데이터베이스에 맞춤형 이미지를 추가하지 않습니다. 목록에 특정 GA 이미지가 표시되지 않으면 지원 문의 페이지에서 Cisco TAC에 문의하십시오. 설정된 지원 티켓 SLA를 사용하여 요청을 처리하고 누락된 GA 이미지를 업로드합니다.

단일 ASA에서 ASA 및 ASDM 이미지 업그레이드를 검토한 다음 자체 저장소의 이미지를 사용하여 여러 ASA 업그레이드에서 ASA 업그레이드에 대해 자세히 알아보십시오.

VPN 연결 모니터링 및 관리

사이트 간 VPN 문제 검토

Security Cloud Control는 네트워크의 ASA 디바이스에 존재하는 VPN 문제를 보고합니다. VPN 피어 목록을 표시 하는 테이블 또는 허브 및 스포크 토폴로지의 VPN 연결을 표시 하는 맵 등 두 가지 방법으로 환경을 볼 수 있습니다. 필터 사이드바를 사용하여 주의가 필요한 VPN 터널을 검색합니다.



Security Cloud Control를 사용하여 VPN 터널 평가:

- 사이트 간 VPN 터널 연결 확인
- 누락된 피어가 있는 VPN 터널 찾기
- 암호화 키 문제가 있는 VPN 피어 찾기
- 터널에 대해 정의된 불완전하거나 잘못 구성된 액세스 목록 찾기
- 터널 구성에서 문제 찾기

관리되지 않는 사이트 간 VPN 피어 온보딩

Security Cloud Control는 관리되지 않는 VPN 피어도 식별합니다. 이러한 디바이스를 식별하면 관리되지 않는 사이트 간 VPN 피어 온보딩에서 디바이스를 온보딩하고 Security Cloud Control를 통해 관리합니다.

ASA 원격 액세스 VPN 지원

Security Cloud Control를 사용하면 ASA를 통해 연결할 때 사용자가 엔터프라이즈 리소스에 안전하게 액세스할 수 있도록 원격 액세스 VPN(Remote Access Virtual Private Network) 구성을 생성할 수 있습니다. ASA가 Security Cloud Control에 온보딩된 경우 Security Cloud Control는 ASDM 또는 CSM(Cisco Security Manager)을 사용하여 이미 구성된 원격 액세스 VPN 설정을 인식하므로 Security Cloud Control로 관리할 수 있습니다.

AnyConnect는 RA VPN 연결을 제공하는 엔드포인트 디바이스에서만 지원되는 클라이언트입니다.

Security Cloud Control는 ASA 디바이스에서 원격 액세스 VPN 기능의 다음 측면을 지원합니다.

- SSL 클라이언트 기반 원격 액세스
- IPv4 및 IPv6 주소 지정
- 여러 ASA 디바이스에서 공유 RA VPN 구성

자세한 내용은 ASA에 대한 원격 액세스 가상 프라이빗 네트워크 구성를 참조하십시오.

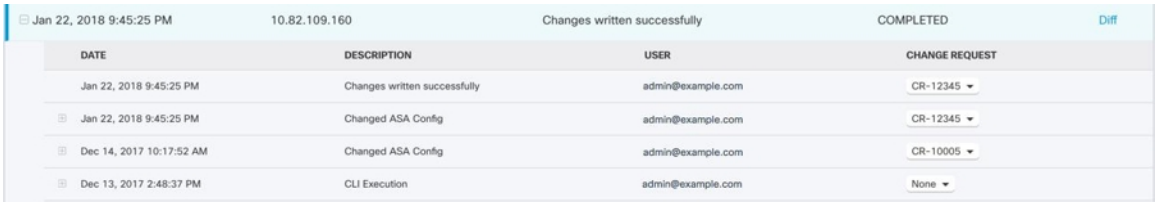
디바이스 구성 동기화 모니터링

Security Cloud Control는 데이터베이스에 저장한 디바이스 구성을 ASA에 설치된 디바이스 구성과 주기적으로 비교합니다. Security Cloud Control에 온보딩한 ASA는 여전히 디바이스의 ASDM(Adaptive Security Device Manager)에서 관리할 수 있으므로 Security Cloud Control는 구성이 디바이스의 구성과 동일한지 확인하고 차이점을 알려줍니다. Synced(동기화됨), Not Synced(동기화되지 않음) 또는 Conflict Detected(충돌 탐지됨) 디바이스 상태에 대한 자세한 내용은 충돌 탐지의 내용을 참조하십시오.

변경 로그에서 변경 사항 추적

디바이스의 구성에 대한 변경 사항은 Security Cloud Control에서 변경 로그 관리에 기록됩니다. 변경 로그에는 Security Cloud Control에서 디바이스로 구축된 변경 사항, 디바이스에서 Security Cloud Control로 가져온 변경 사항, 해당 변경 사항의 "차이"를 볼 수 있는 기능, 변경된 내용, 발생한 시간, 수행한 사람 등의 정보가 표시됩니다.

회사의 추적 번호를 사용하는 맞춤형 라벨을 생성하여 변경 사항에 적용할 수도 있습니다. 변경 로그에서 해당 맞춤형 라벨, 날짜 범위, 특정 사용자 또는 변경 유형별로 변경 목록을 필터링하여 원하는 항목을 찾을 수 있습니다.



이전 구성 복원

"실행 취소"하려는 ASA를 변경하는 경우 Security Cloud Control를 사용하여 디바이스를 이전 구성으로 복원할 수 있습니다. 자세한 내용은 ASA 구성 복원를 참조하십시오.

명령줄 인터페이스 및 명령 매크로를 사용하여 디바이스 관리

Security Cloud Control는 그래픽 사용자 인터페이스(GUI)와 명령줄 인터페이스(CLI)를 모두 제공하는 웹 기반 관리 제품으로, 디바이스를 한 번에 하나씩 관리하거나 여러 디바이스를 동시에 관리할 수 있습니다.

ASA CLI 사용자는 CLI 툴의 추가 기능을 높이 평가할 것입니다. 다음은 SSH 세션으로 디바이스에 연결하는 대신 Security Cloud Control의 CLI 툴을 사용하는 몇 가지 이유입니다.

- Security Cloud Control는 명령에 필요한 사용자 모드를 알고 있습니다. 명령을 실행하기 위해 권한 수준을 높이거나 낮출 필요가 없으며, 명령을 실행하기 위해 특정 명령 컨텍스트를 입력할 필요도 없습니다.
- Security Cloud Control는 하므로 목록에서 명령을 선택하여 쉽게 다시 실행할 수 있습니다.
- CLI 작업은 변경 로그에 기록되므로 전송된 명령과 수행한 작업을 읽을 수 있습니다.
- 명령을 대량 모드에서 실행할 수 있으며, 이를 통해 여러 디바이스에 개체 또는 정책을 동시에 구축할 수 있습니다.
- Security Cloud Control는 한 CLI 매크로를 제공합니다.. CLI 매크로는 있는 그대로 실행할 수 있는 즉시 사용 가능한 명령 또는 완료하고 실행할 수 있는 "공란 채우기" CLI 명령입니다. 하나의 디바이스에서 이러한 명령을 실행하거나 동시에 여러 ASA에 명령을 전송할 수 있습니다.
- CLI는 전체 ASA 구성 파일을 제공합니다. 이를 보거나 고급 사용자인 경우 CLI 명령을 실행하여 변경하지 않고 직접 편집하고 변경 사항을 저장할 수 있습니다.

Cisco Security Analytics and Logging

추가 라이선스를 통해 Cisco Security Analytics and Logging은 ASA에서 발생하는 syslog 이벤트 및 NSEL(Netflow Secure Event Logging) 이벤트를 SEC(Secure Event Connector)로 전송할 수 있게 하며, SEC는 이를 Cisco 클라우드로 전달합니다. 클라우드에 있으면 Security Cloud Control의 이벤트 로깅 페이지에서 해당 이벤트를 볼 수 있습니다. 여기서 이벤트를 필터링하고 검토하여 네트워크에서 트리거하는 보안 규칙을 명확하게 이해할 수 있습니다. 자세한 내용은 보안 클라우드의 이벤트를 참조하십시오.

이벤트 모니터링 외에도 Security Cloud Control에서 Secure Cloud Analytics 포털을 실행하여 로깅된 이벤트에 대한 행동 분석을 수행할 수 있습니다.

Cisco Security Analytics and Logging을 구현하는 방법에 대한 자세한 설명은 ASA 디바이스에 대한 SaaS(Secure Logging Analytics) 구현의 내용을 참조하십시오.

다음 작업

이제 ASA의 온보딩 및 정책 조정을 시작할 수 있습니다.

Firewall 대시보드

Firewall 대시보드는 다양한 범주에서 테넌트 레벨 세부 정보를 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.

대시보드는 **Top Insights & Alerts(**주요 인사이트 및 알림**)**, **Top Actions(**주요 조치**)** 및 **Top Information(**주요 정보**)**의 세 가지 주요 섹션으로 나뉩니다. 각 섹션은 최적의 보안 및 운영 통제를 유지하는 데 도움이 되는 다양한 범주의 통찰력을 제공합니다.

인사이트 및 알림

이 섹션은 **AIOps** 인사이트가 테넌트에 대해 활성화된 경우에만 표시됩니다. Elephant 플로우로 인한 높은 트래픽, RA VPN 예측, 액세스 제어 정책 이상, 높은 CPU 및 메모리 사용량, 스노트 CPU 및 메모리 사용량과 관련된 인사이트를 확인할 수 있습니다.

상위 작업

이 섹션은 **AIOps** 인사이트가 테넌트에 대해 활성화된 경우에만 표시됩니다. 활성화된 경우 다음 위젯을 볼 수 있습니다.

- **Policy Analyzer and Optimizer(**정책 분석기 및 옵티마이저**)**: 방화벽 성능을 개선하기 위한 보안 정책을 분석하고 이상 징후를 탐지하며 최적화 권장 사항을 제공합니다.

  자세한 내용은 Policy Analyzer and Optimizer(정책 분석기 및 옵티마이저)를 참조하십시오.

- **AIOps Insights(AIOps** 인사이트**)**: 모든 활성 인사이트와 추세에 대한 자세한 정보를 제공하여 구성, 상태 및 운영 또는 트래픽 및 용량별로 이상 항목을 분류합니다.

  자세한 내용은 AIOps 인사이트를 참조하십시오.

- **Feature Adoption(**기능 채택**)**: 사용 패턴을 최적화하고 보안 조치를 개선하기 위해 기능 채택률에 대한 인사이트를 제공합니다.

  내용은 기능 채택 평가 및 개선을 참조하십시오.

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. 위젯은 **Issues(**문제**)**, **Pending Actions(**보류 중인 작업**)**, **Other(**기타**)** 및 **Online(**온라인**)**으로 분류된 총 디바이스 수를 표시합니다.

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.

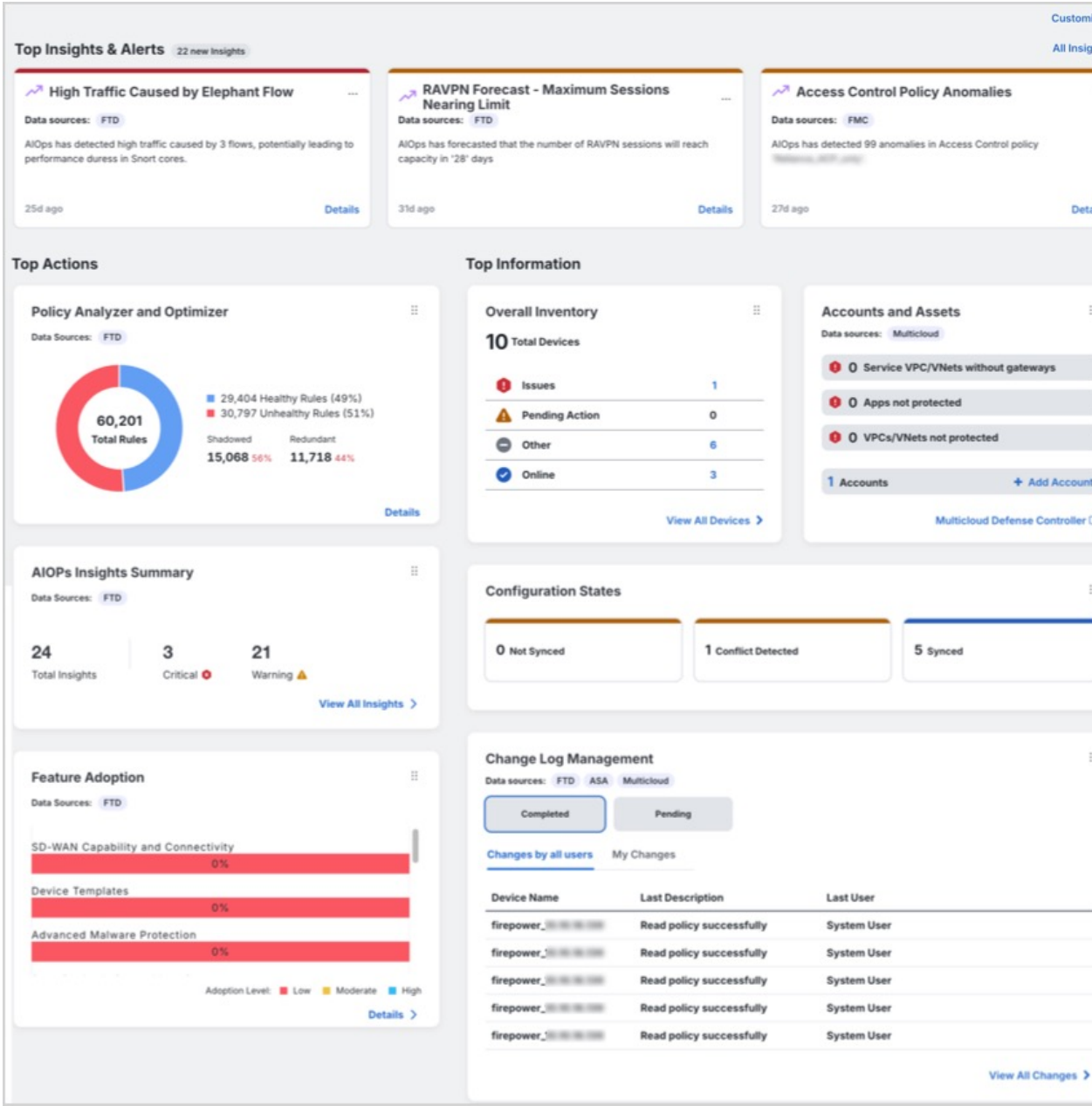
- 어카운트 및 자산:
  - 멀티 클라우드 어카운트 및 리소스를 효과적으로 추적하고 관리할 수 있습니다. 여기에서 Multicloud Defense 컨트롤러를 실행할 수 있습니다.
  - **+Add Account(+**어카운트 추가**)**를 클릭하여 새 어카운트을 추가합니다.

  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.

그림 ***1: AIOps*** 인사이트가 활성화된 대시보드



발표

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