Security Cloud Control에 디바이스 온보딩

라이브 디바이스와 모델 디바이스를 모두 Security Cloud Control에 온보딩할 수 있습니다. 모델 디바이스는 Security Cloud Control를 사용하여 보고 편집할 수 있는 업로드된 구성 파일입니다.

대부분의 라이브 디바이스 및 서비스는 Secure Device Connector가 Security Cloud Control를 디바이스 또는 서비스에 연결할 수 있도록 개방형 HTTPS 연결을 필요로 합니다.

이 장에는 다음 섹션이 포함되어 있습니다.

AWS VPC 온보딩

AWS VPC를 Security Cloud Control에 온보딩하려면 다음 절차를 수행합니다.

Before you begin

Note Security Cloud Control는 피어링된 AWS VPC를 지원하지 않습니다. 피어 VPC에 정의된 보안 그룹을 참조하는 피어링된 VPC를 온보딩하려고 하면 온보딩 프로세스가 실패합니다.

AWS(Amazon Web Services) VPC(Virtual Private Cloud)를 Security Cloud Control에 온보딩하기 전에 다음 사전 요건을 검토합니다.

- AWS VPC를 온보딩하려면 IAM(Identity and Access Management) 콘솔을 사용하여 생성한 AWS VPC의 액세스 키 및 보안 액세스 키가 필요합니다. 자세한 내용은 보안 자격 증명 이해 및 가져오기를 참조하십시오.
- Security Cloud Control가 AWS VPC와 통신할 수 있도록 권한을 구성합니다. 자세한 내용은 IAM 사용자의 권한 변경을 참조하십시오. 필수 권한은 다음 예를 참조하십시오.

```
"cloudformation:CreateStack",
"cloudformation:CreateStackInstances",
"cloudformation:DescribeStackInstance",
"cloudformation:DescribeStackResource",
"cloudformation:DescribeStackResources",
```

```
"cloudformation:DescribeStacks",
"ec2:AllocateAddress",
"ec2:AllocateHosts",
"ec2:AssignPrivateIpAddresses",
"ec2:AssociateAddress",
"ec2:AssociateDhcpOptions",
"ec2:AssociateRouteTable",
"ec2:AssociateSubnetCidrBlock",
"ec2:AttachInternetGateway",
"ec2:AttachNetworkInterface",
"ec2:AuthorizeSecurityGroupEgress",
"ec2:AuthorizeSecurityGroupIngress",
"ec2:CreateDhcpOptions",
"ec2:CreateEgressOnlyInternetGateway",
"ec2:CreateInternetGateway",
"ec2:CreateNetworkAcl",
"ec2:CreateNetworkInterface",
"ec2:CreateNetworkInterfacePermission",
"ec2:CreateRoute",
"ec2:CreateRouteTable",
"ec2:CreateSecurityGroup",
"ec2:CreateSubnet",
"ec2:CreateTags",
"ec2:DescribeAddresses",
"ec2:DescribeAddressesAttribute",
"ec2:DescribeAvailabilityZones",
"ec2:DescribeDhcpOptions",
"ec2:DescribeEgressOnlyInternetGateways",
"ec2:DescribeInstanceStatus",
"ec2:DescribeInstances",
"ec2:DescribeInternetGateways",
"ec2:DescribeNetworkAcls",
"ec2:DescribeNetworkInterfaceAttribute",
"ec2:DescribeNetworkInterfacePermissions",
"ec2:DescribeNetworkInterfaces",
"ec2:DescribeRegions",
"ec2:DescribeRouteTables",
"ec2:DescribeSecurityGroupReferences",
"ec2:DescribeSecurityGroupRules",
"ec2:DescribeSecurityGroups",
"ec2:DescribeSubnets",
"ec2:DescribeTags",
"ec2:DescribeTransitGatewayVpcAttachments",
"ec2:DescribeTransitGateways",
"ec2:DescribeVpcs",
"ec2:DescribeVpnGateways",
"ec2:ModifyNetworkInterfaceAttribute",
"ec2:ModifySecurityGroupRules",
"ec2:ModifySubnetAttribute",
"ec2:RunInstances",
"sts:GetCallerIdentity"
```

Procedure

단계 **1** 왼쪽 창에서 보안 디바이스를 클릭합니다.

단계 **2** 디바이스 온보딩을 시작하려면  를 클릭합니다.

단계 **3** **AWS VPC**를 클릭합니다.

단계 **4** Access Key ID(액세스 키 ID) 및 Secret Access Key(암호 액세스 키) 자격 증명을 입력하여 AWS 어카운트에 연결합니다. 생성된 이름 목록은 로그인 자격 증명을 제공한 AWS VPC에서 검색됩니다.

단계 **5** **Connect(**연결**)**를 클릭합니다.

단계 **6** 드롭다운 메뉴에서 영역을 선택합니다. 선택한 지역은 VPC가 로컬이어야 합니다.

단계 **7** **Select(**선택**)**를 클릭합니다.

단계 **8** 드롭다운 메뉴를 사용하여 올바른 AWS 이름을 선택합니다. 생성된 이름 목록은 로그인 자격 증명을 제공한 AWS VPC에서 검색됩니다. 드롭다운 메뉴에서 원하는 AWS VPC를 선택합니다. AWS VPC ID 이름은 고유하며 ID가 동일한 인스턴스가 두 개 이상 있을 수 없습니다.

단계 **9** **Select(**선택**)**를 클릭합니다.

단계 **10** Security Cloud Control UI에 표시할 이름을 입력합니다.

단계 **11** **Continue(**계속**)**를 클릭합니다.

단계 **12** (선택 사항) 디바이스의 레이블을 입력합니다. AWS VPC에 대한 레이블을 생성하는 경우 테이블이 디바이스에 자동으로 동기화되지 않습니다. AWS 콘솔에서 수동으로 레이블을 태그로 다시 생성해야 합니다. 자세한 내용은 AWS VPC의 레이블 및 태그를 참조하십시오.

단계 **13** **Continue(**계속**)**를 클릭합니다.

단계 **14** **Security Devices(**보안 디바이스**)** 페이지로 돌아갑니다. 디바이스가 성공적으로 온보딩되면 Configuration Status(구성 상태)가 "Synced(동기화됨)"이고 Connectivity(연결성) 상태가 "Online(온라인)"으로 표시됩니다.

관련 정보**:**

- AWS VPC 연결 자격 증명 업데이트
- AWS VPC 정책
- Security Cloud Control의 AWS VPC 및 보안 그룹
- AWS와 기타 매니지드 디바이스 간 개체 공유

지원되는 디바이스, 소프트웨어 및 하드웨어

Security Cloud Control는 여러 보안 플랫폼에서 보안 정책과 디바이스 구성을 관리할 수 있는 클라우드 기반 관리 솔루션입니다. Security Cloud Control는 전체 정책 및 구성을 중앙에서 관리합니다.

- Cisco Secure Firewall ASA, 온프레미스 및 가상 모두
- Cisco Secure FTD(Firewall Threat Defense), 온프레미스 및 가상 모두
- Cisco Catalyst SD-WAN Manager
- Cisco Secure Firewall Management Center, 온프레미스
- Cisco Meraki MX
- Cisco IOS 디바이스
- Cisco Umbrella

- AWS 보안 그룹

이 문서에서는 Security Cloud Control가 지원하는 디바이스, 소프트웨어 및 하드웨어에 대해 설명합니다. Security Cloud Control가 지원하지 않는 소프트웨어 및 디바이스는 지적하지 않습니다. 소프트웨어 버전 또는 디바이스 유형에 대한 지원을 명시적으로 요청하지 않는 경우 지원되지 않습니다.

Cisco Secure Firewall ASA

Cisco ASA(Adaptive Security Appliance)는 방화벽, VPN, 침입 방지 기능이 통합된 보안 디바이스입니다. 무단 액세스, 사이버 위협 및 데이터 유출로부터 네트워크를 보호하고, 단일 플랫폼에서 강력한 보안 서비스를 제공합니다. Security Cloud Control 는 ASA 디바이스 관리를 지원하며, 구성 관리를 간소화 하고 네트워크 인프라 전반에서 규정 준수 를 보장하는 기능을 제공합니다.

Cisco Secure Firewall Threat Defense

Firewall Threat Defense는 기존 방화벽 기능과 고급 위협 보호 기능을 통합합니다. 침입 방지, 애플리케이션 제어, URL 필터링, 고급 멀웨어 보호 등 포괄적인 보안 기능을 제공합니다. FTD는 ASA 하드웨어 어플라이언스, Cisco 방화벽 하드웨어 어플라이언스 및 가상 환경에 구축할 수 있습니다. Cisco Firewall Management Center, Security Cloud Control, Firewall Device Manager 등 다양한 관리 인터페이스를 통해 Threat Defense 디바이스를 관리할 수 있습니다.

소프트웨어 및 하드웨어 호환성에 대한 자세한 내용은 Cisco Secure Firewall Threat Defense 호환성 가이드를 참조하십시오.

Firewall Device Manager는 Threat Defense 디바이스 관리를 위해 명시적으로 설계된 웹 기반 관리 인터페이스입니다. Threat Defense 디바이스를 구성하고 모니터링하는 간소화된 접근 방식을 제공하므로 소규모 구축 또는 직관적인 인터페이스를 선호하는 조직에 이상적입니다.

FDM은 네트워크 설정, 액세스 제어 정책, NAT 규칙, VPN 구성, 모니터링 및 기본 문제 해결을 위한 기본 구성 기능을 제공합니다. 일반적으로 웹 브라우저를 통해 액세스하는 FDM은 FTD 디바이스에서 직접 사용할 수 있으므로 추가 관리 서버나 어플라이언스가 필요하지 않습니다.

Cisco Catalyst SD-WAN Manager

Security Cloud Control는 Catalyst SD-WAN에 대한 중앙 집중식 관리를 제공하여 조직이 네트워크 전반에 걸쳐 보안 정책을 효율적으로 구성, 모니터링 및 시행할 수 있도록 합니다. 이 통합은 또한 Catalyst SD-WAN Manager에서의 고급 문제 해결, 규칙 최적화 및 변경 관리를 용이하게 합니다.

소프트웨어 및 하드웨어 호환성에 대한 자세한 내용은 Cisco Catalyst SD-WAN 디바이스 호환성 가이드를 참조하십시오.

Cisco Secure Firewall Management Center

Security Cloud Control는 안전한 통합을 구축하고, 보안 디바이스를 검색하고, 중앙 집중식 정책 관리를 가능하게 하여 온프레미스 Firewall Management Center의 관리를 간소화합니다. 방화벽 규칙, VPN 설정, 침입 방지 정책과 같은 보안 정책을 FMC의 모든 디바이스에서 효율적으로 관리하고 구축할 수 있습니다.

Cisco Meraki MX

Meraki MX 어플라이언스는 분산 구축을 위해 설계된 엔터프라이즈급 보안 및 SD-WAN 차세대 방화벽 어플라이언스입니다. Security Cloud Control는 Meraki MX 디바이스에서 레이어 3 네트워크 규칙 관리를 지원합니다. Meraki 디바이스를 Security Cloud Control에 온보딩할 경우, 이는 Meraki 대시보드 와 통신하여 디바이스를 관리합니다. Security Cloud Control 는 설정 요청을 Meraki 대시보드 로 안전하게 전송하며, Meraki 대시보드에서 새 설정을 디바이스에 적용합니다. 중앙 집중식 정책 관리, 백업 및 복원, 모니터링 및 보고, 규정 준수 확인, 자동화 기능 등이 Security Cloud Control의 Cisco Meraki MX 지원의 주요 기능입니다.

Cisco IOS 디바이스

Cisco IOS는 라우팅, 스위칭 및 기타 네트워킹 프로토콜을 포함한 네트워크 기능을 관리하고 제어할 수 있습니다. Cisco 네트워크 디바이스를 구성하고 유지 관리하기 위한 일련의 기능과 명령을 제공하여 다양한 규모와 복잡한 네트워크 내에서 효율적인 커뮤니케이션과 관리를 가능하게 합니다.

Cisco Umbrella

Security Cloud Control는 Umbrella ASA 통합과 같은 통합을 통해 Cisco Umbrella를 관리합니다. 이를 통해 관리자는 인터페이스별 정책을 사용하여 Umbrella 구성에 Cisco ASA(Adaptive Security Appliance)를 포함할 수 있습니다. 이러한 통합을 통해 ASA에서는 DNS 쿼리를 Umbrella로 리디렉션할 수 있으며 Umbrella의 DNS 보안, 웹 필터링 및 위협 인텔리전스 기능을 활용하여 네트워크 보안을 강화할 수 있습니다.

AWS 보안 그룹

Security Cloud Control는 AWS(Amazon Web Services) VPC(Virtual Private Clouds, 가상 프라이빗 클라우드를 위한 간소화된 관리 인터페이스를 제공합니다. 주요 기능으로는 AWS 사이트 간 VPN 연결 모니터링, AWS 디바이스 변경 사항 추적, AWS 사이트 간 VPN 터널 보기 등이 있습니다.

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.