AWS 디바이스 구성

이 장에는 다음 섹션이 포함되어 있습니다.

AWS VPC 연결 자격 증명 업데이트

AWS VPC에 연결할 새 액세스 키 및 보안 액세스 키를 생성하는 경우 Security Cloud Control에서 연결 자격 증명을 업데이트해야 합니다. AWS 콘솔에서 자격 증명을 업데이트한 다음 아래 절차를 사용하여 Security Cloud Control 콘솔에서 자격 증명을 업데이트합니다. 자세한 내용은 *IAM* 사용자의 액세스 키 관리(https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html) 또는 *AWS* 어카운트 루트 사용자의 액세스 키 생성, 비활성화 및 삭제 (https://docs.aws.amazon.com/general/latest/gr/managing-aws-access-keys.html)을 참조하십시오.

Security Cloud Control에서 액세스 키 또는 보안 액세스 키를 변경할 수 없습니다. AWS 콘솔 또는 AWS CLI 콘솔에서 연결 자격 증명을 수동으로 관리해야 합니다.

Note 여러 AWS VPC가 Security Cloud Control 테넌트에 온보딩된 경우 한 번에 하나의 디바이스에 대한 자격 증명을 업데이트해야 합니다.

Procedure

단계 **1** 왼쪽 창에서 보안 디바이스를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭한 다음 **AWS VPC**를 클릭합니다.

단계 **3** 연결 자격 증명을 업데이트할 AWS VPC를 선택합니다.

필터 및 검색 기능을 사용하여 필요한 디바이스를 찾을 수 있습니다.

단계 4 **Device Action(**디바이스 작업**)** 창에서 **Update Credentials(**자격 증명 업데이트**)**를 클릭합니다.

단계 5 AWS VPC에 연결하는 데 사용할 새 액세스 키 및 보안 액세스 키를 입력합니다.

단계 6 **Update(**업데이트**)**를 클릭합니다.

Note
Security Cloud Control가 디바이스를 동기화하지 못하면 Security Cloud Control의 연결 상태에 "Invalid Credentials(유효하지 않은 자격 증명)"가 표시될 수 있습니다. 이 경우 유효하지 않은 사용자 이름과 비밀번호 조합을 사용하려고 시도했을 수 있습니다. 유효하지 않은 자격 증명 문제 해결의 내용을 참조하십시오.

관련 정보

- AWS VPC 온보딩

AWS Transit Gateway를 사용하여 AWS VPC 터널 모니터링

AWS(Amazon Web Service) Transit Gateway는 간소화된 피어링 관계를 허용하는 중앙 허브를 통해 엔터프라이즈 VPC(Virtual Private Cloud)를 AWS VPC에 연결하는 클라우드 라우터 역할을 합니다.

Security Cloud Control에서는 AWS Transit Gateway를 사용하여 온보딩된 AWS VPC의 연결 상태를 모니터링할 수 있습니다.

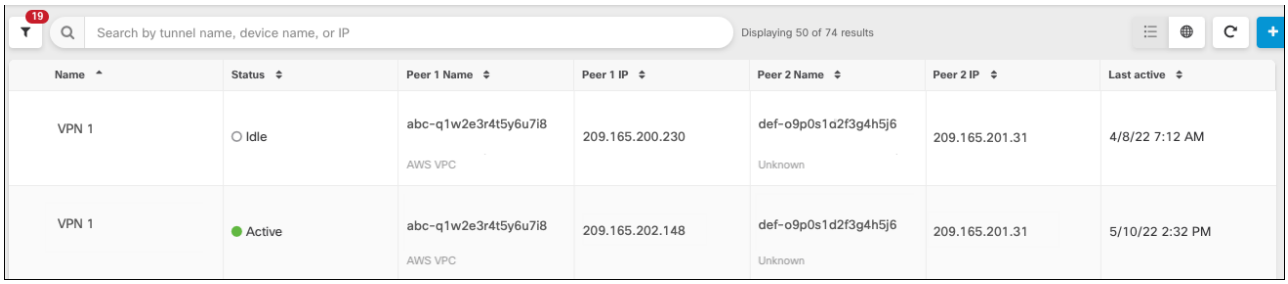
Procedure

단계 1 왼쪽 창에서 **Secure Connections(**보안 연결**)** > **Network Connections(**네트워크 연결**)** > **Site to Site VPN(**사이트 간 **VPN)**를 클릭합니다.

단계 2 **VPN Tunnels(VPN** 터널**)**페이지에는 Security Cloud Control 테넌트에서 관리하는 모든 네트워크 터널의 연결 상태가 표시됩니다. VPN 터널의 연결 상태는 활성 또는 유휴 상태일 수 있습니다.

단계 3 VPC를 선택하고 **Actions(**작업**)** 아래에서 **Check Connectivity(**연결 확인**)**를 클릭하여 터널에 대한 실시간 연결 확인을 트리거하고 터널이 현재 활성 또는 유휴 상태인지를 식별합니다. 온디맨드 연결 확인 링크를 클릭하지 않으면 온보딩된 모든 디바이스에서 사용 가능한 모든 터널의 확인이 10분마다 수행됩니다.

Note
VPN 터널의 연결이 다운되면 Security Cloud Control에서 알림을 표시합니다. 그러나 링크가 백업된 경우 알림 프롬프트가 표시되지 않습니다.



사이트 간 VPN 터널 검색 및 필터링

필터 사이드바 를 검색 필드와 함께 사용하여 VPN 터널 다이어그램에 표시된 VPN 터널 검색에 집중할 수 있습니다.

Procedure

단계 **1** 왼쪽 창에서 **Secure Connections(**보안 연결**)** > **Network Connections(**네트워크 연결**)** > **Site to Site VPN(**사이트 간 **VPN)**를 클릭하여 VPN 페이지를 엽니다.

단계 **2** 필터 아이콘 을 클릭하여 필터 창을 엽니다.

단계 **3** 다음 필터를 사용하여 검색을 구체화합니다.

- **Filter by Device(**디바이스별 필터링**)** - **Filter by Device(**디바이스별 필터링**)**를 클릭하고 디바이스 유형 탭을 선택한 후 필터링을 통해 찾으려는 디바이스를 선택합니다.
- **Tunnel Issues(**터널 문제**)** - 터널의 양쪽에 문제가 있음을 탐지했는지 여부입니다. 디바이스에 문제가 있는 몇 가지 예로는 연결된 인터페이스 또는 피어 IP 주소 또는 액세스 목록 누락, IKEv1 제안 불일치 등이 있습니다(AWS VPC VPN 터널에서는 터널 문제 탐지를 아직 사용할 수 없음).
- **Devices/Services(**디바이스/서비스**)** -디바이스 유형을 기준으로 필터링합니다.
- **Status(**상태**)** – 터널 상태는 활성 또는 유휴 상태일 수 있습니다.
  - **Active(**활성**)** - 네트워크 패킷이 VPN 터널을 통과하는 열린 세션이 있거나 성공적인 세션이 설정되었고 아직 시간 초과되지 않았습니다. Active(활성)는 터널이 활성 상태이고 관련성이 있음을 나타내는 데 도움이 될 수 있습니다.
  - 유휴 - Security Cloud Control는 이 터널에 대해 열려 있는 세션을 검색할 수 없습니다. 터널이 사용 중이 아니거나 이 터널에 문제가 있을 수 있습니다.
- **Onboarded(**온보딩됨**)** - Security Cloud Control에서 디바이스를 관리하거나 Security Cloud Control에서 관리하지 않을 수 있습니다(관리되지 않음).

- **Managed(관리됨)** - Security Cloud Control가 관리하는 디바이스별로 필터링합니다.
- **Unmanaged(관리되지 않음)** - Security Cloud Control가 관리하지 않는 디바이스로 필터링합니다.

- **Device Types(디바이스 유형)** - 터널의 한쪽이 라이브(연결된 디바이스) 디바이스인지 아니면 모델 디바이스인지 여부입니다.

단계 **4** 검색 창에 디바이스 이름 또는 IP 주소를 입력하여 필터링된 결과를 검색할 수도 있습니다. 검색은 대/소문자를 구분하지 않습니다.

AWS VPC 터널에 대한 변경 기록 보기

AWS VPC 터널에 대한 변경 기록을 보려면 다음을 수행합니다.

프로시저

단계 **1** 왼쪽 창에서 **Monitor(모니터링)** > **Events & Logs(이벤트 및 로그)** > **Log(로그)** > **Change Log(변경 로그)**를 클릭합니다.

단계 **2** **Change Log(로그 변경)** 페이지에서 필터 아이콘을 클릭하고 **Filter by device(디바이스 별 필터)** 탭을 선택한 후 **AWS VPC**를 클릭합니다.

단계 **3** 기록을 검토할 AWS VPC를 선택하고 **OK(확인)** 를 클릭합니다.

관련 정보

- Security Cloud Control에서 변경 로그 관리

AWS VPC 정책

Security Cloud Control는 사용자에게 AWS 어카운트과 연결된 AWS(Amazon Web Services) VPC(Virtual Private Cloud) 전체에서 보안 정책을 일관되게 유지할 수 있는 기능을 제공합니다. 또한 Security Cloud Control을 사용하여 여러 디바이스 유형에서 개체를 공유할 수 있습니다. 자세한 내용은 다음 항목을 참조하십시오.

Security Cloud Control의 AWS VPC 및 보안 그룹

AWS VPC 보안 그룹 규칙

AWS 보안 그룹은 모든 AWS EC2 인스턴스 및 보안 그룹과 연결된 기타 엔터티에 대한 인바운드 및 아웃바운드 네트워크 트래픽을 제어하는 규칙의 모음입니다.

AWS(Amazon Web Services) 콘솔과 마찬가지로 Security Cloud Control는 각 규칙을 개별적으로 표시합니다. SDC가 인터넷에 액세스할 수 있으면 다음 환경에 대한 AWS VPC(Virtual Private Cloud) 규칙을 생성하고 관리할 수 있습니다.

- 동일한 AWS VPC 내의 다른 보안 그룹과 주고받는 정보를 허용하는 보안 그룹입니다.
- IPv4 또는 IPv6 주소와 주고받는 것을 허용하는 보안 그룹입니다.

AWS 보안 그룹을 포함하는 Security Cloud Control에서 규칙을 생성할 때는 다음 제한 사항에 유의하십시오.

- 인바운드 트래픽을 허용하는 규칙의 경우, 소스는 동일한 AWS VPC, IPv4 또는 IPv6 CIDR 블록 또는 단일 IPv4 또는 IPv6 주소에 있는 하나 이상의 보안 그룹 개체일 수 있습니다. 인바운드 규칙은 하나의 보안 그룹 개체만 대상으로 포함할 수 있습니다.
- 아웃바운드 트래픽을 허용하는 규칙의 경우 대상은 동일한 AWS VPC에 있는 하나 이상의 보안 그룹 개체, 접두사 목록 ID, IPv4 또는 IPv6 CIDR 블록, 단일 IPv4 또는 IPv6 주소일 수 있습니다. 아웃바운드 규칙은 하나의 보안 그룹 개체만 소스로 포함할 수 있습니다.
- Security Cloud Control는 여러 엔터티(예: 둘 이상의 포트 또는 서브넷)를 포함하는 규칙을 AWS VPC에 구축하기 전에 별도의 규칙으로 변환합니다.
- 규칙을 추가하거나 제거하면 보안 그룹과 연결된 모든 AWS 엔터티에 변경 사항이 자동으로 적용됩니다.
- AWS 보안 그룹은 최대 60개의 인바운드 규칙과 60개의 아웃바운드 규칙을 호스팅하도록 제한됩니다. 이 제한은 IPv4 규칙 및 IPv6 규칙에 대해 별도로 적용됩니다. Security Cloud Control에서 생성된 추가 규칙은 총 규칙 수에 포함됩니다. 즉, Security Cloud Control에 온보딩하여 60 규칙 제한을 초과할 수 없습니다.

Warning 기존 규칙을 편집하면 편집된 규칙이 삭제되고 새 세부 정보로 새 규칙이 생성됩니다. 이로 인해 새 규칙을 생성할 수 있을 때까지 해당 규칙에 의존하는 트래픽이 매우 짧은 기간 동안 삭제됩니다. 새 규칙을 생성하는 경우에는 이러한 현상이 발생하지 않습니다.

AWS 콘솔에서 생성할 수 있는 규칙 유형에 대한 자세한 내용은 AWS 보안 그룹 개체를 참조하십시오. AWS VPC와 연결할 수 있는 개체에 대한 자세한 내용은 AWS 보안 그룹 및 클라우드 보안 그룹 개체의 내용을 참조하십시오.

관련 정보

- 보안 그룹 규칙 생성, on page 6
- 보안 그룹 규칙 편집, on page 7
- 보안 그룹 규칙 삭제, on page 8

보안 그룹 규칙 생성

기본적으로 AWS(Amazon Web Services) VPC(Virtual Private Cloud)는 모든 네트워크 트래픽을 차단합니다. 즉, 모든 규칙이 트래픽 **Allow(**허용**)**로 자동 구성됩니다. 이 작업은 편집할 수 없습니다.

Note 새 보안 그룹 규칙을 생성할 때는 이를 보안 그룹과 연결해야 합니다.

AWS 콘솔은 둘 이상의 소스 또는 대상을 포함하는 규칙을 지원하지 않습니다. 즉, 둘 이상의 엔터티를 포함하는 단일 보안 그룹 규칙을 구축하는 경우 Security Cloud Control는 AWS VPC에 구축하기 전에 규칙을 별도의 규칙으로 변환합니다. 예를 들어, 2개의 포트 범위에서 하나의 클라우드 보안 그룹 개체로 트래픽을 허용하는 인바운드 규칙을 생성하는 경우, Security Cloud Control는 이를 2개의 개별 규칙으로 변환합니다. (1) 첫 번째 포트 범위에서 보안 그룹으로의 트래픽을 허용하고 (2) 두 번째 포트 범위에서 보안 그룹으로의 트래픽을 허용합니다.

다음 절차를 사용하여 보안 그룹 규칙을 생성합니다.

Procedure

단계 **1** 왼쪽 창에서 보안 디바이스를 클릭합니다.

단계 **2** **Test Templates(**테스트 템플릿**)** 탭을 클릭합니다.

단계 **3** **AWS** 탭을 클릭하고 액세스 제어 정책을 수정할 AWS VPC 디바이스 템플릿을 선택합니다.

단계 **4** 오른쪽의 Management(관리) 창에서 **Policy(**정책**)**를 선택합니다.

단계 **5** 규칙을 추가할 보안 그룹 옆에 있는 파란색 플러스 버튼을 클릭합니다.

단계 **6** **Inbound(**인바운드**)** 또는 **Outbound(**아웃바운드**)**를 클릭합니다.

- **Inbound(**인바운드**)** 규칙 - 소스 네트워크는 하나 이상의 IPv4 주소, IPv6 주소 또는 클라우드 보안 그룹 개체를 포함할 수 있습니다. 대상 네트워크는 단일 클라우드 보안 그룹 개체로 정의되어야 합니다.
- **Outbound(**아웃바운드**)** 규칙 - 소스 네트워크는 단일 클라우드 보안 그룹 개체로 정의되어야 합니다. 대상 네트워크는 하나 이상의 IPv4 주소, IPv6 주소 또는 보안 그룹 개체를 포함할 수 있습니다.

단계 **7** 규칙 이름을 입력합니다. 영숫자, 공백 및 특수 문자(+, ., _, -)는 사용할 수 있습니다.

단계 **8** 다음 탭의 속성을 적절하게 조합하여 트래픽 일치 기준을 정의합니다.

- **Source(**소스**) - Source(**소스**)** 탭을 클릭하고 네트워크(네트워크 및 대륙 포함)를 추가하거나 제거합니다. 포트 또는 포트 범위를 소스로 정의할 수 없습니다.

- **Destination(대상) - Destination(대상)** 탭을 클릭하고 트래픽이 도착하는 네트워크(네트워크 및 대륙 포함) 또는 포트를 추가하거나 제거합니다. 기본값은 "Any(모두)"입니다.
  - 참고**:**

    정의된 네트워크 개체가 없으면 AWS 콘솔에서 IPv4(0.0.0.0/0)에 대한 규칙과 IPv6(::0/0)에 대한 규칙의 두 가지 규칙으로 변환됩니다.

단계 **9** **Save(저장)**를 클릭합니다.

단계 **10** 지금 변경 사항을 검토하고 구축하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

Caution
구축에 실패하면 Security Cloud Control는 AWS VPC의 상태를 구축을 시도하기 전의 상태로 되돌립니다. 이는 "최선의 노력"을 기반으로 수행됩니다. AWS는 상태를 유지하지 않으므로 이 롤백 시도는 실패할 수 있습니다. 이 경우 AWS 관리 콘솔에 로그인하고 AWS VPC를 이전 구성으로 수동으로 되돌린 다음 Security Cloud Control에서 변경 사항을 읽어야 합니다.

보안 그룹 규칙 편집

Security Cloud Control를 사용하여 AWS VPC에 대한 액세스 제어 규칙을 편집하려면 다음 절차를 수행합니다.

Procedure

단계 **1** 왼쪽 창에서 보안 디바이스를 클릭합니다.

단계 **2** **Devices(디바이스)** 탭을 클릭하여 디바이스를 찾거나 **Templates(템플릿)** 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 **3** **AWS** 탭을 클릭하고 액세스 제어 정책을 수정할 AWS VPC를 선택합니다.

단계 **4** 오른쪽의 **Management(관리)** 창에서 **Policy(정책)**를 선택합니다.

단계 **5** 기존 보안 그룹 규칙을 편집하려면 규칙을 선택하고 Actions(작업) 창에서 편집 아이콘을 클릭합니다. (간단한 편집은 편집 모드를 시작하지 않고 인라인으로 수행할 수도 있습니다.) 규칙 제한 및 예외는 AWS VPC 보안 그룹 규칙을 참조하십시오.

단계 **6** **Save(저장)**를 클릭합니다.

단계 **7** 지금 변경 사항을 검토하고 구축하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

Caution
구축에 실패하면 Security Cloud Control는 AWS VPC의 상태를 구축을 시도하기 전의 상태로 되돌립니다. 이는 "최선의 노력"을 기반으로 수행됩니다. AWS는 상태를 유지하지 않으므로 이 롤백 시도는 실패할 수 있습니다. 이 경우 AWS 관리 콘솔에 로그인하고 AWS VPC를 이전 구성으로 수동으로 되돌린 다음 AWS VPC 디바이스 구성과 Security Cloud Control의 구성 간의 변경 사항을 폴링해야 합니다.

보안 그룹 규칙 삭제

Procedure

단계 **1** 왼쪽 창에서 보안 디바이스를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾거나 **Templates(**템플릿**)** 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 **3** **AWS** 탭을 클릭하고 액세스 제어 정책을 수정할 AWS VPC를 선택합니다.

단계 **4** 오른쪽의 **Management(**관리**)** 창에서 **Policy(**정책**)**를 선택합니다.

단계 **5** 더 이상 필요하지 않은 보안 그룹 규칙을 삭제하려면 규칙을 선택하고 **Actions(**작업**)** 창에서 제거 아이콘을 클릭합니다.

단계 **6** 지금 변경 사항을 검토하고 구축하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

Caution
구축에 실패하면 Security Cloud Control는 AWS VPC의 상태를 구축을 시도하기 전의 상태로 되돌립니다. 이는 "최선의 노력"을 기반으로 수행됩니다. AWS는 상태를 유지하지 않으므로 이 롤백 시도는 실패할 수 있습니다. 이 경우 AWS 관리 콘솔에 로그인하고 AWS VPC를 이전 구성으로 수동으로 되돌린 다음 AWS VPC 디바이스 구성과 Security Cloud Control의 구성 간의 변경 사항을 폴링해야 합니다.

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.