Secure Firewall ASA 이벤트 모니터링

Secure Event Connector 정보

SEC(Secure Event Connector)는 보안 분석 및 로깅 SaaS 솔루션의 구성 요소입니다. ASA 및 FDM 관리 디바이스에서 이벤트를 수신하여 Cisco Cloud에 전달합니다. Security Cloud Control는 관리자가 해당 페이지에서 또는 Cisco Secure Cloud Analytics를 사용하여 이벤트를 분석할 수 있도록 Event Logging(이벤트 로깅) 페이지에 이벤트를 표시합니다.

SEC는 네트워크 또는 AWS Virtual Private Cloud(VPC)에 구축된 Secure Device Connector 또는 네트워크에 구축된 자체 Security Cloud Control 커넥터 가상 머신에 설치됩니다.

보안 이벤트 커넥터 ID

Cisco TAC(Technical Assistance Center) 또는 기타 Security Cloud Control 지원과 협력할 때는 SEC의 ID가 필요할 수 있습니다. 이 ID는 Security Cloud Control의 Secure Connector(보안 커넥터) 페이지에 있습니다. SEC ID를 찾으려면 다음을 수행합니다.

1. 왼쪽의 Security Cloud Control 메뉴에서 **Administration(관리)** > **Secure Connectors(보안 커넥터)**를 선택합니다.
2. 식별할 SEC를 클릭합니다.
3. SEC ID는 Details(세부 정보) 창의 Tenant ID(테넌트 ID) 위에 나열되는 ID입니다.

관련 정보**:**

- ASA 디바이스에 대한 Cisco Security Analytics and Logging
- SDC 가상 머신에 SEC(Secure Event Connector) 설치, 2 페이지
- Security Cloud Control VM 이미지를 사용하여 테넌트에 대해 여러 SEC 설치
- 생성한 VM 이미지를 사용하여 테넌트에 대해 여러 SEC 설치
- Terraform 모듈을 사용하여 AWS VPC에 보안 이벤트 커넥터 설치, 20 페이지
- 보안 이벤트 커넥터 제거
- Cisco Security Analytics and Logging(SaaS) 프로비저닝 해제

보안 이벤트 커넥터 설치

SEC(보안 이벤트 커넥터)는 SDC가 있거나 없는 테넌트에 설치할 수 있습니다.

Secure Device Connector(있는 경우)와 동일한 가상 머신에 하나의 SEC를 설치할 수 있습니다. 또는 네트워크에서 유지 관리하는 자체 Security Cloud Control 커넥터 가상 머신에 SEC를 설치할 수 있습니다.

SDC 가상 머신에 SEC(Secure Event Connector) 설치

SEC(보안 이벤트 커넥터)는 ASA 및 FDM 관리 디바이스에서 이벤트를 수신하여 Cisco Cloud에 전달합니다. Security Cloud Control는 관리자가 해당 페이지에서 또는 Cisco Secure Cloud Analytics를 사용하여 이벤트를 분석할 수 있도록 Event Logging(이벤트 로깅) 페이지에 이벤트를 표시합니다.

Secure Device Connector(있는 경우)와 동일한 가상 머신에 하나의 SEC를 설치할 수 있습니다. 또는 네트워크에서 유지 관리하는 자체 Security Cloud Control 커넥터 가상 머신에 SEC를 설치할 수 있습니다.

이 문서에서는 SDC와 동일한 가상 머신에 SEC를 설치하는 방법을 설명합니다. 더 많은 SEC를 설치하려면 Security Cloud Control 이미지를 사용하여 SEC 설치, 5 페이지 또는 VM 이미지를 사용하여 SEC 설치, 12 페이지의 내용을 참조하십시오.

시작하기 전에

- Cisco Security and Analytics 로깅, 로깅 및 문제 해결 라이선스를 구매합니다. 또는 Cisco Security and Analytics 로그아웃을 먼저 시도하려면 Security Cloud Control에 로그인하고 기본 탐색 모음에서 **Events & Logs(**이벤트 및 로그**)** > **Events(**이벤트**)** > **Event Logging(**이벤트 로깅**)**를 선택하

고 **Request Trial(**평가판 요청**)**을 클릭합니다. 또한 Logging **Analytics and Detection(**로깅 분석 및 탐지 로깅**)** 및 **Total Network Analytics and Monitoring(**전체 네트워크 분석 및 모니터링**)** 라이선스를 구매하여 Secure Cloud Analytics를 이벤트에 적용할 수 있습니다.

- SDC가 설치되었는지 확인합니다. 자세한 내용은 Secure Device Connector 및 Secure Event Connector을 위한 VM 구축을 참조하십시오.
- SDC가 Security Cloud Control와 통신하는지 확인합니다.
  1. 왼쪽 창에서 **Administration(**관리**)** > **Secure Connectors(**보안 커넥터**)**를 클릭합니다.
  2. SDC의 마지막 하트비트가 SEC 설치 전 10분 미만이었으며 SDC의 상태가 활성인지 확인합니다.
- 시스템 요구 사항 - SDC를 실행하는 가상 머신에 추가 CPU 및 메모리를 할당합니다.
  - CPU: 총 6개의 CPU를 만들기 위해 SEC를 수용할 수 있도록 추가로 4개의 CPU를 할당합니다.
  - 메모리: 총 10GB의 메모리를 만들려면 SEC에 8GB의 메모리를 추가로 할당합니다.

    SEC를 수용하도록 VM의 CPU와 메모리를 업데이트한 후 VM의 전원을 켜고 Secure Connector(보안 커넥터) 페이지에 SDC가 "Active(활성)" 상태로 표시되는지 확인합니다.

프로시저

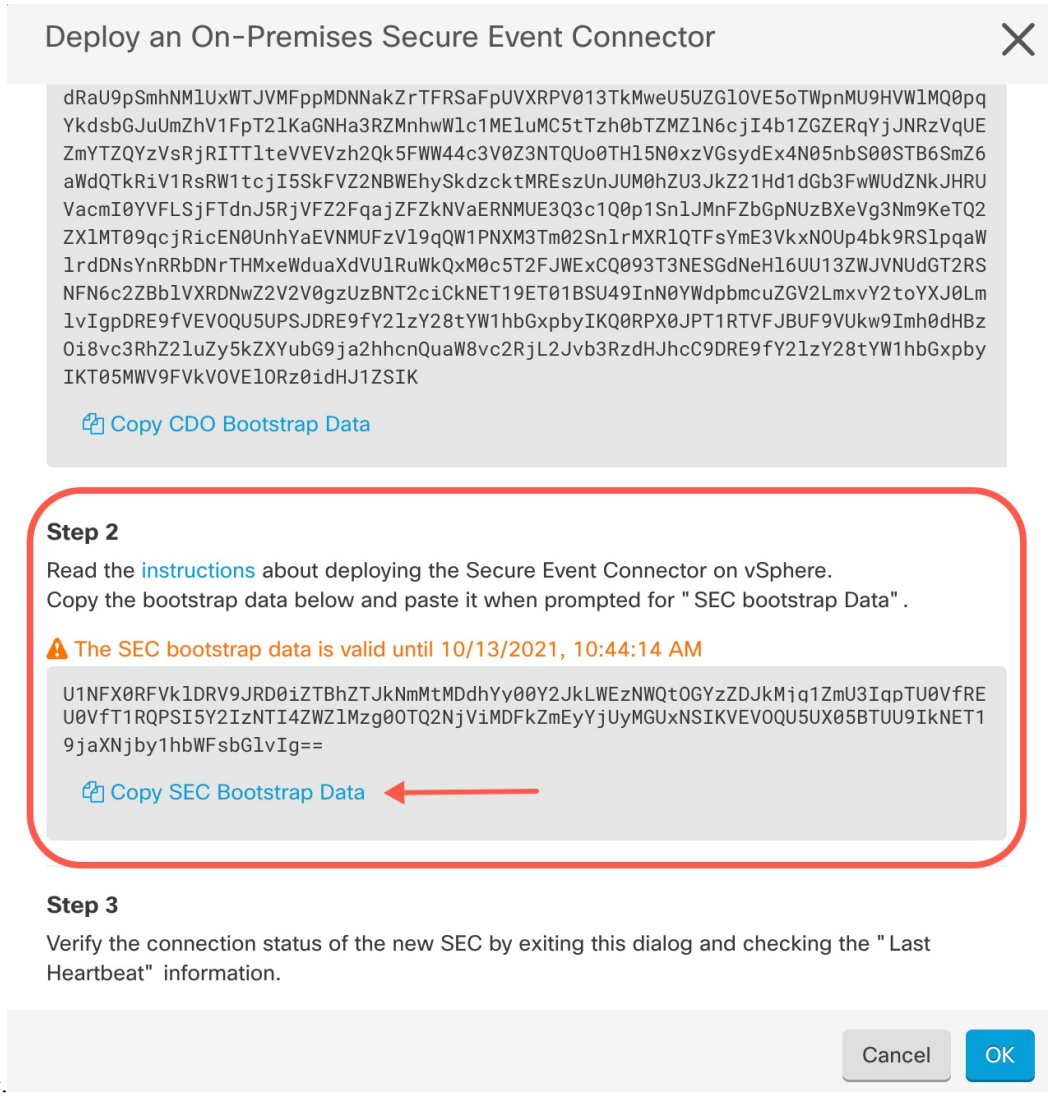
단계 **1** Security Cloud Control에 로그인합니다.

단계 **2** Security Cloud Control 플랫폼 메뉴에서, **Products(**제품**)** > **Firewall(**방화벽**)**을 클릭합니다.

단계 **3** 왼쪽 창에서 **Administration(**관리**)** > **Secure Connectors(**보안 커넥터**)**를 클릭합니다.

단계 **4**  아이콘을 클릭하고 **Secure Event Connector(**보안 이벤트 커넥터**)**를 클릭합니다.

단계 5 마법사의 1단계를 건너뛰고 2단계로 이동합니다. 마법사 2단계에서 링크를 클릭하여 **SEC** 부트스트랩 데이터를 복사합니다.



단계 6 터미널 창을 열고 SDC에 "cdo" 사용자로 로그인합니다.

단계 7 로그인한 후에는 "sdc" 사용자로 전환합니다. 암호를 묻는 메시지가 표시되면 "cdo" 사용자의 암호를 입력합니다. 다음은 이러한 명령의 예입니다.

```
[cdo@sdc-vm ~]$ sudo su sdc
[sudo] password for cdo: <type password for cdo user>
[sdc@sdc-vm ~]$
```

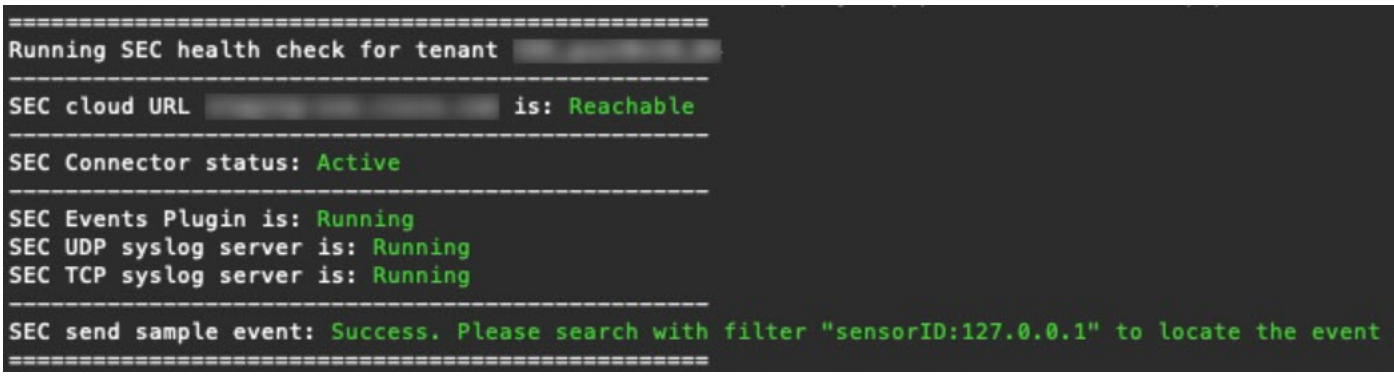
단계 8 프롬프트에서 **sec.sh** 설정 스크립트를 실행합니다.

```
[sdc@sdc-vm ~]$ /usr/local/cdo/toolkit/sec.sh setup
```

단계 9 프롬프트 끝에 4단계에서 복사한 부트스트랩 데이터를 붙여넣고 **Enter** 키를 누릅니다.

```
Please copy the bootstrap data from Setup Secure Event Connector page of Security Cloud Control:
KJHYFuYTFuIGhiJKlKnJHvHfgxTewrtwE
RtyFUiyIOHKNkJbKhvhgyRStwterTyufGUihoJpojP9UOoiUY8VHHGFXREWRtygfhVjhkOuihIuyftyXtfcghvjbkhB=
```

SEC가 온보딩되면 sec.sh는 SEC의 상태를 확인하는 스크립트를 실행합니다. 모든 상태 확인이 "녹색"인 경우 상태 확인은 이벤트 로그에 샘플 이벤트를 전송합니다. 샘플 이벤트는 이벤트 로그에 "sec-health-check"라는 정책으로 표시됩니다.



등록에 실패했거나 SEC 온 보딩에 실패했다는 메시지가 표시되면 보안 이벤트 커넥터 온보딩 장애 문제 해결로 이동하십시오.

단계 **10** SDC 및 SEC가 실행 중인 VM에 추가 구성이 필요한지 확인합니다.

- 자체 가상 머신에 SDC를 설치한 경우 생성한 VM에 설치된 SDC 및 Security Cloud Control 커넥터에 대한 추가 구성, 16 페이지을 계속 진행합니다.
- Security Cloud Control 이미지를 사용하여 SDC를 설치한 경우 "다음 작업"을 진행합니다.

다음에 수행할 작업

ASA 디바이스에 대한 SaaS(Secure Logging Analytics) 구현, 40 페이지 으로 돌아갑니다.

관련 정보:

- Secure Device Connector 문제 해결
- 보안 이벤트 커넥터 문제 해결
- SEC 온보딩 장애 문제 해결
- Secure Event Connector 등록 실패 문제 해결

Security Cloud Control 이미지를 사용하여 SEC 설치

SEC(Secure Event Connector)는 ASA 및 FTD에서 Cisco Cloud로 이벤트를 전달하므로, 라이선싱에 따라 Event Logging(이벤트 로깅) 페이지에서 해당 이벤트를 보고 Secure Cloud Analytics로 조사할 수 있습니다.

테넌트에 두 개 이상의 SEC(Secure Event Connector)를 설치하고 ASA 및 FDM 매니지드 디바이스의 이벤트를 설치한 SEC로 보낼 수 있습니다. 여러 SEC를 사용하면 서로 다른 위치에 SEC를 설치하고 Cisco Cloud에 이벤트를 전송하는 작업을 구축할 수 있습니다.

SEC 설치는 2단계로 진행됩니다.

1. Security Cloud Control VM 이미지를 사용하여 보안 이벤트 커넥터를 지원하기 위한 Security Cloud Control 커넥터 설치, 6 페이지 설치하는 모든 SEC에 대해 하나의 Security Cloud Control 커넥터가 필요합니다. Security Cloud Control 커넥터는 SDC(Secure Device Connector)와 다릅니다.
2. Security Cloud Control 커넥터 가상 머신에 보안 이벤트 커넥터 설치, 17 페이지.

참고 고유한 VM을 생성하여 Security Cloud Control 커넥터를 생성하려면 생성한 VM 이미지를 사용하여 테넌트에 대해 여러 SEC 설치를 참조하십시오.

다음 작업:

Security Cloud Control VM 이미지를 사용하여 보안 이벤트 커넥터를 지원하기 위한 Security Cloud Control 커넥터 설치, 6 페이지를 계속 진행합니다.

Security Cloud Control VM 이미지를 사용하여 보안 이벤트 커넥터를 지원하기 위한 Security Cloud Control 커넥터 설치

시작하기 전에

- Cisco Security and Analytics Logging, **Logging and Troubleshooting(**로깅 및 문제 해결**)** 라이선스를 구매하고, **Logging Analytics and Detection(**로깅 분석 및 탐지**)**, **Total Network Analytics and Monitoring(**전체 네트워크 분석 및 모니터링**)** 라이선스를 구매하여 Secure Cloud Analytics를 이벤트에 적용할 수도 있습니다.

  원하는 경우 Security Cloud Control에 로그인하여 Security Analytics and Logging(보안 분석 및 로깅) 평가판을 요청하고 기본 탐색 모음에서 **Events & Logs(**이벤트 및 로그**)** > **Events(**이벤트**)** > **Event Logging(**이벤트 로깅**)**을 선택하고 **Request Trial(**평가판 요청**)**을 클릭합니다.
- Security Cloud Control는 엄격한 인증서 확인이 필요하며 Security Cloud Control 커넥터와 인터넷 간의 웹/콘텐츠 프록시 검사를 지원하지 않습니다. 프록시 서버를 사용하는 경우 Security Cloud Control 커넥터와 Security Cloud Control간의 트래픽 검사를 비활성화합니다.
- Security Cloud Control이 프로세스에서 설치된 커넥터는 **TCP** 포트 **443**에서 인터넷에 대한 전체 아웃바운드 액세스 권한을 가져야 합니다**.**
- Secure Device Connector를 사용하여 Security Cloud Control에 연결을 검토하여 Security Cloud Control커넥터에 대한 적절한 네트워크 액세스를 확인합니다**.**
- Security Cloud Control는 vSphere 웹 클라이언트 또는 ESXi 웹 클라이언트를 사용한 Security Cloud Control 커넥터 VM OVF 이미지 설치를 지원합니다.
- Security Cloud Control는 VM vSphere 데스크톱 클라이언트를 사용한 Security Cloud Control 커넥터 VM OVF 이미지 설치를 지원하지 않습니다.
- ESXi 5.1 하이퍼바이저.
- Security Cloud Control 커넥터 및 SEC만 호스팅하는 VM의 시스템 요구 사항:

- VMware ESXi 호스트에는 vCPU 4개가 필요합니다.
- VMware ESXi 호스트에는 최소 8GB의 메모리가 필요합니다.
- VMware ESXi에는 프로비저닝 선택에 따라 가상 머신을 지원하기 위해 64GB의 디스크 공간이 필요합니다.

- 설치를 시작하기 전에 다음 정보를 수집하십시오.
  - Security Cloud Control 커넥터 VM에 사용할 고정 IP 주소.
  - 설치 프로세스 중 생성하는 **root** 및 Security Cloud Control 사용자의 비밀번호.
  - 조직에서 사용하는 DNS 서버의 IP 주소
  - SDC 주소가 있는 네트워크의 게이트웨이 IP 주소
  - 시간 서버의 FQDN 또는 IP 주소.
- Security Cloud Control 커넥터 가상 머신은 보안 패치를 정기적으로 설치하도록 구성되며, 이를 위해서는 포트 80 아웃바운드를 열어야 합니다.

프로시저

단계 **1** Security Cloud Control 커넥터를 생성할 Security Cloud Control 테넌트에 로그인합니다.

단계 **2** Security Cloud Control 플랫폼 메뉴에서, **Products(**제품**)** > **Firewall(**방화벽**)**을 클릭합니다.

단계 **3** 왼쪽 창에서 **Administration(**관리**)** > **Secure Connectors(**보안 커넥터**)**를 클릭합니다.

단계 **4** + 아이콘을 클릭하고 **Secure Event Connector(**보안 이벤트 커넥터**)**를 클릭합니다.

단계 **5** 1단계에서 **Download the Security Cloud ControlConnector VM image**(커넥터 VM 이미지 다운로드)를 클릭합니다. 이는 SEC를 설치하는 특수 이미지입니다. 최신 이미지를 사용하려면 항상 Security Cloud Control 커넥터 VM을 다운로드하십시오.

단계 **6** .zip 파일의 모든 파일을 추출합니다. 다음과 같이 표시됩니다.

- Security Cloud Control-SDC-VM-ddd50fa.ovf
- Security Cloud Control-SDC-VM-ddd50fa.mf

- Security Cloud Control-SDC-VM-ddd50fa-disk1.vmdk

단계 **7** vSphere 웹 클라이언트를 사용하여 VMware 서버에 관리자로 로그인합니다.

참고
VM vSphere 데스크톱 클라이언트를 사용하지 마십시오.

단계 **8** 지시에 따라 OVF 템플릿에서 온프레미스 Security Cloud Control 커넥터 가상 머신을 구축합니다. (템플릿을 구축하려면 .ovf, .mf 및 .vdk 파일이 필요합니다.)

단계 **9** 설정이 완료되면 VM의 전원을 켭니다.

단계 **10** 새 Security Cloud Control 커넥터 VM의 콘솔을 엽니다.

단계 **11** Security Cloud Control 사용자로 로그인합니다. 기본 암호는 `adm123`입니다.

단계 **12** 프롬프트에 `sudo sdc-onboard setup`을 입력합니다.

```
[cdo@localhost ~]$ sudo sdc-onboard setup
```

단계 **13** 프롬프트가 표시되면 Security Cloud Control 사용자의 기본 비밀번호 `adm123`을 입력합니다.

단계 **14** 지시에 따라 **root** 사용자의 새 암호를 생성합니다.

단계 **15** 지시에 따라 Security Cloud Control 사용자의 새 암호를 생성합니다.

단계 **16** 지시에 따라 Security Cloud Control 도메인 정보를 입력합니다.

단계 **17** Security Cloud Control 커넥터 VM에 사용할 고정 IP 주소를 입력합니다.

단계 **18** Security Cloud Control 커넥터 VM이 설치된 네트워크의 게이트웨이 IP 주소를 입력합니다.

단계 **19** Security Cloud Control 커넥터의 NTP 서버 주소 또는 FQDN을 입력합니다.

단계 **20** Docker 브리지 정보를 묻는 프롬프트가 표시되면 정보를 입력하거나 해당되지 않는 경우 비워두고 <Enter> 키를 누릅니다.

단계 **21** 입력을 확인합니다.

단계 **22** "지금 SDC를 설정하시겠습니까?"라는 프롬프트가 나타나면 **n**을 입력합니다.

단계 **23** Security Cloud Control 사용자로 로그인하여 Security Cloud Control 커넥터에 대한 SSH 연결을 생성합니다.

단계 **24** 프롬프트에 **`sudo sdc-onboard bootstrap`**을 입력합니다.

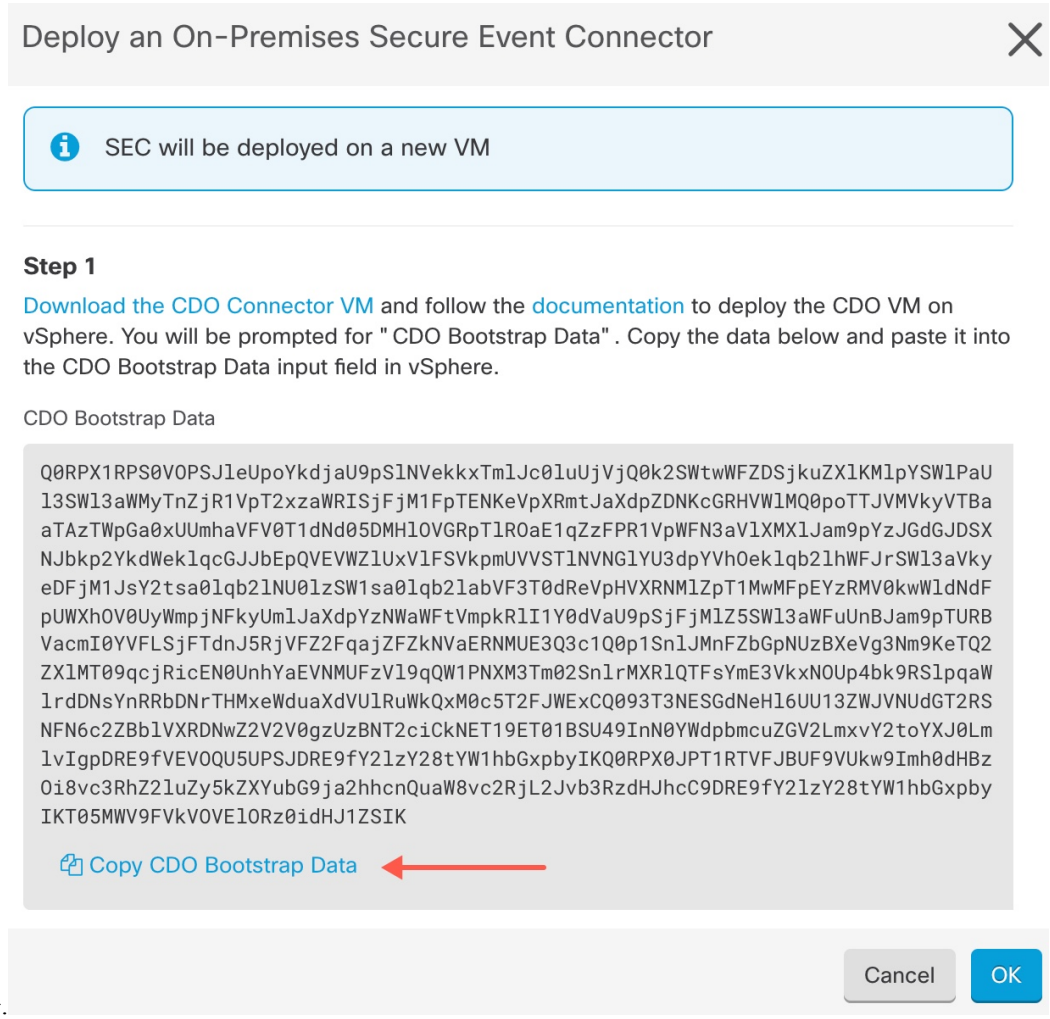
```
[cdo@localhost ~]$ sudo sdc-onboard bootstrap
```

단계 **25** 프롬프트가 표시되면 Security Cloud Control 사용자의 비밀번호를 입력합니다.

단계 **26** 프롬프트가 표시되면 Security Cloud Control로 돌아가 Security Cloud Control 부트스트랩 데이터를 복사한 다음 SSH 세션에 붙여넣습니다. Security Cloud Control 부트스트랩 데이터를 복사하려면 다음을 수행합니다.

1. Security Cloud Control에 로그인합니다.
2. 왼쪽 창에서 **Administration(**관리**)** > **Secure Connectors(**보안 커넥터**)**를 클릭합니다.
3. 온보딩을 시작한 보안 이벤트 커넥터를 선택합니다. 상태가 "Onboarding(온보딩)"으로 표시되어야 합니다.
4. **Actions(**작업**)** 창에서 **Deploy an On-Premises Secure Event Connector(**온프레미스 보안 디바이스 커넥터 구축**)**를 클릭합니다.

5. 대화 상자의 1단계에서 Security Cloud Control 부트스트랩 데이터를 복사합니



다.

단계 **27** 이 설정을 업데이트하시겠습니까?라는메시지가 표시되면 **n**을 입력합니다.

단계 **28** Security Cloud Control의 **Deploy an On-Premises Secure Event Connector(**온프레미스 보안 이벤트 커넥터 구축**)** 대화 상자로 돌아가 **OK(**확인**)**를 클릭합니다. **Secure Connector(**보안 커넥터**)** 페이지에서 Secure Event Connector(보안 이벤트 커넥터)가 노란색 Onboarding(온보딩) 상태로 표시됩니다.

다음에 수행할 작업

Security Cloud Control 커넥터 VM에 보안 이벤트 커넥터 설치, 10 페이지를 진행합니다.

Security Cloud Control 커넥터 VM에 보안 이벤트 커넥터 설치

시작하기 전에

Security Cloud Control VM 이미지를 사용하여 보안 이벤트 커넥터를 지원하기 위한 Security Cloud Control 커넥터 설치, 6 페이지에 설명된 대로 Security Cloud Control 커넥터 VM을 설치해야 합니다.

프로시저

단계 **1** Security Cloud Control에 로그인합니다.

단계 **2** Security Cloud Control 플랫폼 메뉴에서, **Products(제품)** > **Firewall(방화벽)**을 클릭합니다.

단계 **3** 왼쪽 창에서 **Administration(관리)** > **Secure Connectors(보안 커넥터)**를 선택합니다.

단계 **4** 위에서 온보딩한 Security Cloud Control 커넥터를 선택합니다. Secure Connector(보안 커넥터) 테이블에서는 이를 보안 이벤트 커넥터(보안 이벤트 커넥터)라고 하며 여전히 "Onboading(온보딩)" 상태여야 합니다.

단계 **5** 오른쪽의 작업 창에서 **Deploy an On-Premises Secure Event Connector(온프레미스 보안 디바이스 커넥터 구축)**를 클릭합니다.

단계 **6** 마법사 **2**단계에서 링크를 클릭하여 **SEC** 부트스트랩 데이터를 복사합니다.

단계 **7** Security Cloud Control 커넥터에 대한 SSH 연결을 생성하고 `cdo` 사용자로 로그인합니다.

단계 **8** 로그인한 후에는 **sdc** 사용자로 전환합니다. 암호를 묻는 메시지가 표시되면 "Security Cloud Control" 사용자의 암호를 입력합니다. 다음은 이러한 명령의 예입니다.

```
[cdo@sdc-vm ~]$ sudo su sdc
 [sudo] password for cdo: <type password for cdo user>
[sdc@sdc-vm ~]$
```

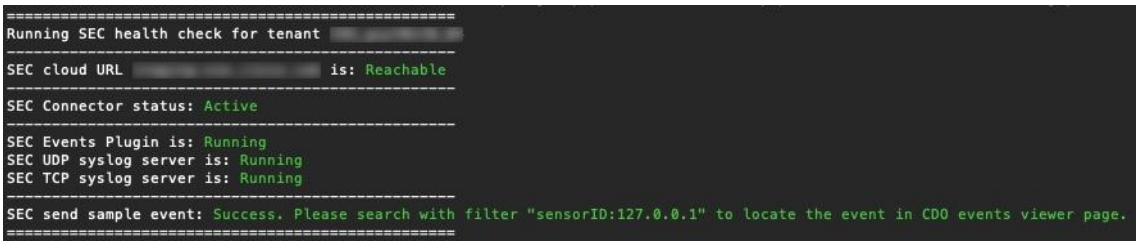
단계 **9** 프롬프트에서 sec.sh 설정 스크립트를 실행합니다.

```
[sdc@sdc-vm ~]$ /usr/local/cdo/toolkit/sec.sh setup
```

단계 **10** 프롬프트 끝에 4단계에서 복사한 부트스트랩 데이터를 붙여넣고 **Enter** 키를 누릅니다.

```
Please copy the bootstrap data from Setup Secure Event Connector page of CDO:
KJHYFuYTFuIGhiJKlKnJHvHfgxTewrtwE
 RtyFUiyIOHKNkJbKhvhgyRStwterTyufGUihoJpojP9UOoiUY8VHHGFXREWRtygfhVjhkOuihIuyftyXtfcghvjbkhB=
```

SEC가 온보딩되면 sec.sh는 SEC의 상태를 확인하는 스크립트를 실행합니다. 모든 상태 확인이 "녹색"인 경우 상태 확인은 이벤트 로그에 샘플 이벤트를 전송합니다. 샘플 이벤트는 이벤트 로그에 "sec-health-check"라는 정책으로 표시됩니다.



등록에 실패했거나 SEC 온 보딩에 실패했다는 메시지가 표시되면 SEC 온보딩 장애 문제 해결로 이동하십시오.

성공 메시지가 표시되면 Security Cloud Control로 돌아가고 온프레미스 보안 이벤트 커넥터 구축 대화 상자에서 완료를 클릭합니다.

다음에 수행할 작업

ASA 디바이스에 대한 SaaS(Secure Logging Analytics) 구현, 40 페이지 으로 돌아갑니다.

관련 정보:

- Secure Device Connector 문제 해결
- Secure Event Connector 문제 해결
- SEC 온보딩 장애 문제 해결

Ubuntu 가상 머신에 보안 이벤트 커넥터 구축

시작하기 전에

Secure Device Connector 및 Secure Event Connector을 위한 VM 구축에 설명된 대로 Ubuntu VM에 Secure Device Connector을 설치해야 합니다.

프로시저

단계 **1** Security Cloud Control에 로그인합니다.

단계 **2** Security Cloud Control 플랫폼 메뉴에서, **Products(**제품**)** > **Firewall(**방화벽**)**을 클릭합니다.

단계 **3** 왼쪽 창에서 **Administration(**관리**)** > **Secure Connectors(**보안 커넥터**)**.

단계 **4**  아이콘을 클릭하고 **Secure Event Connector(**보안 이벤트 커넥터**)**를 클릭합니다.

단계 **5** 창의 2단계에서 SEC 부트스트랩 데이터를 메모장에 복사합니다.

단계 **6** 다음 명령을 실행합니다.

```
[sdc@vm]:~$sudo su sdc
```

```
sdc@vm:/home/user$ cd /usr/local/cdo/toolkit
```

메시지가 표시되면 복사한 SEC 부트스트랩 데이터를 입력합니다.

```
sdc@vm:~/toolkit$ ./sec.sh setup
Please input the bootstrap data from Setup Secure Event Connector page of CDO:
Successfully on-boarded SEC
```

보안 이벤트 커넥터가 Security Cloud Control에서 "활성" 상태가 될 때까지 몇 분 정도 걸릴 수 있습니다.

VM 이미지를 사용하여 SEC 설치

SEC(Secure Event Connector)는 ASA 및 FTD에서 Cisco Cloud로 이벤트를 전달하므로, 라이선싱에 따라 Event Logging(이벤트 로깅) 페이지에서 해당 이벤트를 보고 Secure Cloud Analytics로 조사할 수 있습니다.

테넌트에 두 개 이상의 SEC(Secure Event Connector)를 설치하고 ASA 및 FDM 매니지드 디바이스의 이벤트를 설치한 SEC로 보낼 수 있습니다. 여러 SEC를 사용하면 서로 다른 위치에 SEC를 설치하고 Cisco Cloud에 이벤트를 전송하는 작업을 구축할 수 있습니다.

자체 VM 이미지를 사용하여 여러 SEC를 설치하는 작업은 3단계로 진행됩니다. 다음 각 단계를 수행해야 합니다.

1. VM 이미지를 사용하여 SEC를 지원하도록 Security Cloud Control 커넥터 설치, 12 페이지
2. 생성한 VM에 설치된 SDC 및 Security Cloud Control 커넥터에 대한 추가 구성, 16 페이지
3. 보안 이벤트 커넥터 설치

참고 Security Cloud Control 커넥터용 Security Cloud Control VM 이미지를 사용하는 것이 가장 쉽고 정확하며 선호되는 Security Cloud Control 커넥터 설치 방법입니다. 이 방법을 사용하려면 Security Cloud Control 이미지를 사용하여 SEC 설치, 5 페이지의 내용을 참조하십시오.

다음 작업:

VM 이미지를 사용하여 SEC를 지원하도록 Security Cloud Control 커넥터 설치, 12 페이지를 계속합니다.

VM 이미지를 사용하여 SEC를 지원하도록 Security Cloud Control 커넥터 설치

Security Cloud Control 커넥터 VM은 SEC를 설치하는 가상 머신입니다. Security Cloud Control 커넥터의 목적은 Cisco Security Analytics and Logging(SaaS) 고객을 위한 SEC를 지원하는 것입니다.

이 단계는 SEC(Secure Event Connector)를 설치하고 구성하기 위해 완료해야 하는 3단계 중 첫 번째 단계입니다. 이 절차 후에 다음 절차를 완료해야 합니다.

- 생성한 VM에 설치된 SDC 및 Security Cloud Control 커넥터에 대한 추가 구성, 16 페이지
- 보안 이벤트 커넥터 설치

시작하기 전에

- Cisco Security and Analytics Logging, **Logging and Troubleshooting(**로깅 및 문제 해결**)** 라이선스를 구매하고, **Logging Analytics and Detection(**로깅 분석 및 탐지**)**, **Total Network Analytics and Monitoring(**전체 네트워크 분석 및 모니터링**)** 라이선스를 구매하여 Secure Cloud Analytics를 이벤트에 적용할 수도 있습니다.

원하는 경우 Security Cloud Control에 로그인하여 Security Analytics and Logging(보안 분석 및 로깅) 평가판을 요청하고 기본 탐색 모음에서 **Events & Logs(**이벤트 및 로그**)** > **Events(**이벤트**)** > **Event Logging(**이벤트 로깅**)**을 선택하고 **Request Trial(**평가판 요청**)**을 클릭합니다.

- Security Cloud Control는 엄격한 인증서 확인이 필요하며 Security Cloud Control 3커넥터와 인터넷 간의 웹/콘텐츠 프록시를 지원하지 않습니다.
- **Security Cloud Control** 커넥터는 **TCP** 포트 **443**에서 인터넷에 대한 전체 아웃바운드 액세스 권한을 가져야 합니다**.**
- Secure Device Connector를 사용하여 Security Cloud Control Firewall Management에 연결을 검토하여 **Security Cloud Control**커넥터에 대한 적절한 네트워크 액세스를 확인합니다**.**
- vCenter 웹 클라이언트 또는 ESXi 웹 클라이언트와 함께 설치된 VMware ESXi 호스트

참고 vSphere 데스크톱 클라이언트를 사용한 설치는 지원되지 않습니다.

- ESXi 5.1 하이퍼바이저.
- Ubuntu 22.04 및 Ubuntu 24.04.
- Security Cloud Control 커넥터 및 SEC만 호스팅하는 VM의 시스템 요구 사항:
  - CPU: SEC를 수용할 수 있도록 4개의 CPU를 할당합니다.
  - 메모리: SEC에 대해 8GB의 메모리를 할당합니다.
  - 디스크 공간: 64GB
- 이 절차를 수행하는 사용자는 Linux 환경에서 작업하고 파일 편집을 위해 **vi** 시각적 편집기를 사용하는 데 익숙해야 합니다.
- 설치를 시작하기 전에 다음 정보를 수집하십시오.
  - Security Cloud Control 커넥터에 사용할 고정 IP 주소.
  - 설치 프로세스 중 생성하는 **root** 및 **Security Cloud Control** 사용자의 비밀번호.
  - 조직에서 사용하는 DNS 서버의 IP 주소
  - Security Cloud Control 커넥터 주소가 있는 네트워크의 게이트웨이 IP 주소
  - 시간 서버의 FQDN 또는 IP 주소.
- Security Cloud Control 커넥터 가상 머신은 보안 패치를 정기적으로 설치하도록 구성되며, 이를 위해서는 포트 80 아웃바운드를 열어야 합니다.
- 시작하기 전에: 이 절차의 명령을 복사하여 터미널 창에 붙여넣지 말고 대신 입력하십시오. 일부 명령에는 "n-대시"가 포함되며, 잘라내기 및 붙여넣기 프로세스에서 이러한 명령은 "m-대시"로 적용되어 명령이 실패할 수 있습니다.

프로시저

단계 1 Security Cloud Control에 로그인합니다.

단계 2 Security Cloud Control 플랫폼 메뉴에서, **Products(**제품**)** > **Firewall(**방화벽**)**을 클릭합니다.

단계 3 왼쪽 창에서 **Administration(**관리**)** > **Secure Connectors(**보안 커넥터**)**.

단계 4  아이콘을 클릭하고 **Secure Event Connector(**보안 이벤트 커넥터**)**를 클릭합니다.

단계 5 제공된 링크를 사용하여 "Deploy an On-Premises 보안 이벤트 커넥터(온프레미스 보안 이벤트 커넥터 구축)" 창의 2단계에서 SEC 부트스트랩 데이터를 복사합니다.

단계 6 설치가 완료되면 Security Cloud Control 커넥터의 IP 주소, 서브넷 마스크 및 게이트웨이를 지정하는 등의 기본 네트워킹을 구성합니다.

단계 7 DNS(Domain Name Server) 서버를 구성합니다.

단계 8 NTP(Network Time Protocol) 서버를 구성합니다.

단계 9 Security Cloud Control 커넥터의 CLI와의 손쉬운 상호 작용을 위해 SSH 서버를 설치합니다.

단계 10 **AWS CLI package(AWS CLI** 패키지**)** (https://docs.aws.amazon.com/cli/latest/userguide/awscli-install-linux.html)를 설치합니다.

참고
`--user` 플래그를 사용하지 마십시오.

단계 11 **Docker CE packages(Docker CE** 패키지**)** (https://docs.docker.com/install/linux/docker-ce/centos/#install-docker-ce)를 설치합니다.

참고
"저장소를 사용하여 설치" 방법을 사용합니다.

단계 12 Docker 서비스를 시작하고 부팅 시 시작되도록 활성화합니다.

```
[root@sdc-vm ~]# systemctl start docker
 [root@sdc-vm ~]# systemctl enable docker
Created symlink from /etc/systemd/system/multiuser.target.wants/docker.service to
/usr/lib/systemd/system/docker.service.
```

단계 13 두 사용자(**Security Cloud Control** 및 **sdc**)를 생성합니다. Security Cloud Control 사용자는 관리 기능을 실행하기 위해 로그인하는 사용자이며(루트 사용자를 직접 사용할 필요가 없음), SDC 사용자는 Security Cloud Control 커넥터 Docker 컨테이너를 실행하는 사용자입니다.

```
[root@sdc-vm ~]# useraddSecurity Cloud Control
 [root@sdc-vm ~]# useradd sdc –d /usr/local/Security Cloud Control
```

단계 14 crontab을 사용하도록 SDC 사용자를 구성합니다.

```
[root@sdc-vm ~]# touch /etc/cron.allow
[root@sdc-vm ~]# echo "sdc" >> /etc/cron.allow
```

단계 15 Security Cloud Control 사용자의 비밀번호를 생성합니다.

```
[root@sdc-vm ~]# passwd Security Cloud Control
Changing password for user Security Cloud Control.
```

```
New password: <type password>
Retype new password: <type password>
passwd: all authentication tokens updated successfully.
```

단계 **16** Security Cloud Control 사용자를 "wheel" 그룹에 추가하여 관리(sudo) 권한을 부여합니다.

```
[root@sdc-vm ~]# usermod -aG wheelSecurity Cloud Control
 [root@sdc-vm ~]#
```

단계 **17** Docker가 설치되면 사용자 그룹이 생성됩니다. CentOS/Docker 버전에 따라 "docker" 또는 "dockerroot"라고 부를 수 있습니다. /etc/group 파일을 확인하여 어떤 그룹이 생성되었는지 확인한 다음 sdc 사용자를 이 그룹에 추가합니다.

```
 [root@sdc-vm ~]# grep docker /etc/group
docker:x:993:
[root@sdc-vm ~]#
[root@sdc-vm ~]# usermod -aG docker sdc
[root@sdc-vm ~]#
```

단계 **18** `/etc/docker/daemon.json` 파일이 없는 경우 파일을 생성하고 아래 내용을 입력합니다. 생성되면 docker 데몬을 다시 시작합니다.

참고
"group" 키에 입력한 그룹 이름이 /etc/group 파일에서 찾은 그룹과 일치하는지 확인합니다.

```
 [root@sdc-vm ~]# cat /etc/docker/daemon.json
{
 "live-restore": true,
 "group": "docker"
}
[root@sdc-vm ~]# systemctl restart docker
[root@sdc-vm ~]#
```

단계 **19** 현재 vSphere 콘솔 세션를 사용하는 경우 SSH로 전환하고 **Security Cloud Control** 사용자로 로그인합니다. 로그인한 후에는 **sdc** 사용자로 변경합니다. 암호를 묻는 메시지가 표시되면 **Security Cloud Control** 사용자의 암호를 입력합니다.

```
[Security Cloud Control@sdc-vm ~]$ sudo su sdc
[sudo] password for Security Cloud Control: <type password for Security Cloud Control user >
[sdc@sdc-vm ~]$
```

단계 **20** 디렉터리를 **/usr/local/**Security Cloud Control로 변경합니다**.**

단계 **21** **bootstrapdata**라는 새 파일을 생성하고 구축 마법사 1단계의 부트스트랩 데이터를 이 파일에 붙여넣습니다. 파일을 **Save(**저장**)**합니다. **vi** 또는 **nano**를 사용하여 파일을 생성할 수 있습니다.

단계 **22** 부트스트랩 데이터는 base64로 인코딩됩니다. 이를 디코딩하고 **extractedbootstrapdata**라는 파일로 내보냅니다.

```
 [sdc@sdc-vm ~]$ base64 -d /usr/local/Security Cloud Control/bootstrapdata > /usr/local/Security Cloud
 Control/extractedbootstrapdata
[sdc@sdc-vm ~]$
```

cat 명령을 실행하여 디코딩된 데이터를 확인합니다. 명령 및 디코딩된 데이터는 다음과 같이 표시됩니다.

```
[sdc@sdc-vm ~]$ cat /usr/local/Security Cloud Control/extractedbootstrapdata
Security Cloud Control_TOKEN="<token string>"
Security Cloud Control_DOMAIN="www.defenseorchestrator.com"
Security Cloud Control_TENANT="<tenant-name>"
<Security Cloud Control_URL>/sdc/bootstrap/Security Cloud
```

```
Control_acm="https://www.defenseorchestrator.com/sdc/bootstrap/tenant-name/<tenant-name-SDC>"
ONLY_EVENTING="true"
```

단계 **23** 다음 명령을 실행하여 디코딩된 부트스트랩 데이터의 섹션을 환경 변수로 내보냅니다.

```
[sdc@sdc-vm ~]$ sed -e 's/^/export /g' extractedbootstrapdata > secenv && source secenv
[sdc@sdc-vm ~]$
```

단계 **24** Security Cloud Control에서 부트스트랩 번들을 다운로드합니다.

```
 [sdc@sdc-vm ~]$ curl -H "Authorization: Bearer $Security Cloud Control_TOKEN" "$Security Cloud
Control_BOOTSTRAP_URL" -o $Security Cloud Control_TENANT.tar.gz
100 10314 100 10314 0 0 10656 0 --:--:-- --:--:-- --:--:-- 10654
[sdc@sdc-vm ~]$ ls -l /usr/local/Security Cloud Control/*SDC
-rw-rw-r--. 1 sdc sdc 10314 Jul 23 13:48 /usr/local/Security Cloud Control/Security Cloud
Control_<tenant_name>
```

단계 **25** Security Cloud Control 커넥터 tarball을 추출하고 bootstrap_sec_only.sh 파일을 실행하여 Security Cloud Control 커넥터 패키지를 설치합니다.

```
 [sdc@sdc-vm ~]$ tar xzvf /usr/local/Security Cloud Control/tenant-name-SDC
<snipped – extracted files>
[sdc@sdc-vm ~]$
[sdc@sdc-vm ~]$ /usr/local/Security Cloud Control/bootstrap/bootstrap_sec_only.sh
[2018-07-23 13:54:02] environment properly configured
download: s3://onprem-sdc/toolkit/prod/toolkit.tar to toolkit/toolkit.tar
toolkit.sh
common.sh
es_toolkit.sh
sec.sh
healthcheck.sh
troubleshoot.sh
no crontab for sdc
-bash-4.2$ crontab -l
*/5 * * * * /usr/local/Security Cloud Control/toolkit/es_toolkit.sh upgradeEventing 2>&1 >>
/usr/local/Security Cloud Control/toolkit/toolkit.log
0 2 * * * sleep 30 && /usr/local/Security Cloud Control/toolkit/es_toolkit.sh es_maintenance 2>&1 >>
/usr/local/Security Cloud Control/toolkit/toolkit.log
You have new mail in /var/spool/mail/sdc
```

다음에 수행할 작업

생성한 VM에 설치된 SDC 및 Security Cloud Control 커넥터에 대한 추가 구성, 16 페이지를 계속합니다.

생성한 VM에 설치된 SDC 및 Security Cloud Control 커넥터에 대한 추가 구성

자체 CentOS 7 가상 머신에 Security Cloud Control 커넥터를 설치한 경우, 이벤트가 SEC에 도달하도록 허용하려면 다음 추가 구성 절차 중 하나를 수행해야 합니다.

- CentOS 7 VM에서 방화벽 서비스 비활성화: 이는 Cisco에서 제공하는 SDC VM의 구성과 일치합니다.
- firewalld 서비스가 실행되도록 허용하고 방화벽 규칙을 추가하여 이벤트 트래픽이 SEC에 도달하도록 허용합니다., 17 페이지: 이는 인바운드 이벤트 트래픽을 허용하는 보다 세분화된 접근 방식입니다.

시작하기 전에

이는 SEC를 설치하고 구성하기 위해 완료해야 하는 3단계 중 두 번째 단계입니다. 아직 완료하지 않았다면 이러한 구성을 변경하기 전에 VM 이미지를 사용하여 SEC를 지원하도록 Security Cloud Control 커넥터 설치, 12 페이지를 완료합니다.

여기에 설명된 추가 구성 변경 중 하나를 완료한 후 보안 이벤트 커넥터 설치를 완료합니다.

CentOS 7 VM에서 **firewalld** 서비스를 비활성화합니다.

1. SDC VM의 CLI에 "Security Cloud Control" 사용자로 로그인합니다.
2. firewalld 서비스를 중지한 다음, 이후에 VM을 재부팅할 때 비활성화된 상태로 유지되는지 확인합니다. 메시지가 표시되면 **Security Cloud Control** 사용자의 비밀번호를 입력합니다.

```
[Security Cloud Control@SDC-VM ~]$ sudo systemctl stop firewalld
Security Cloud Control@SDC-VM ~]$ sudo systemctl disable firewalld
```

3. Docker 서비스를 다시 시작하여 Docker 관련 항목을 로컬 방화벽에 다시 삽입합니다.

```
[Security Cloud Control@SDC-VM ~]$ sudo systemctl restart docker
```

4. 보안 이벤트 커넥터 설치를 계속합니다.

firewalld 서비스가 실행되도록 허용하고 방화벽 규칙을 추가하여 이벤트 트래픽이 **SEC**에 도달하도록 허용합니다.

1. SDC VM의 CLI에 "Security Cloud Control" 사용자로 로그인합니다.
2. 구성한 TCP, UDP 또는 NSEL 포트에서 SEC로 수신되는 트래픽을 허용하도록 로컬 방화벽 규칙을 추가합니다. SEC에서 사용하는 포트에 대해서는 Cisco Security Analytics and Logging에 사용되는 디바이스의 TCP, UDP 및 NSEL 포트 찾기를 참조하십시오. 메시지가 표시되면 **Security Cloud Control** 사용자의 비밀번호를 입력합니다. 다음은 이러한 명령의 예입니다. 다른 포트 값을 지정해야 할 수 있습니다.

```
[Security Cloud Control@SDC-VM ~]$ sudo firewall-cmd --zone=public --permanent
--add-port=10125/tcp
Security Cloud Control@SDC-VM ~]$ sudo firewall-cmd --zone=public --permanent
--add-port=10025/udp
[Security Cloud Control@SDC-VM ~]$ sudo firewall-cmd --zone=public --permanent
--add-port=10425/udp
```

3. firewalld 서비스를 다시 시작하여 새 로컬 방화벽 규칙을 활성 및 영구 규칙으로 설정합니다.

```
[Security Cloud Control@SDC-VM ~]$ sudo systemctl restart firewalld
```

4. 보안 이벤트 커넥터 설치를 계속합니다.

Security Cloud Control 커넥터 가상 머신에 보안 이벤트 커넥터 설치

시작하기 전에

이 단계는 SEC(Secure Event Connector)를 설치하고 구성하기 위해 완료해야 하는 3단계 중 세 번째 단계입니다. 아직 수행하지 않은 경우 이 절차를 계속하기 전에 다음 작업을 완료합니다.

- VM 이미지를 사용하여 SEC를 지원하도록 Security Cloud Control 커넥터 설치, 12 페이지.
- 생성한 VM에 설치된 SDC 및 Security Cloud Control 커넥터에 대한 추가 구성, 16 페이지.

프로시저

단계 **1** Security Cloud Control에 로그인합니다.

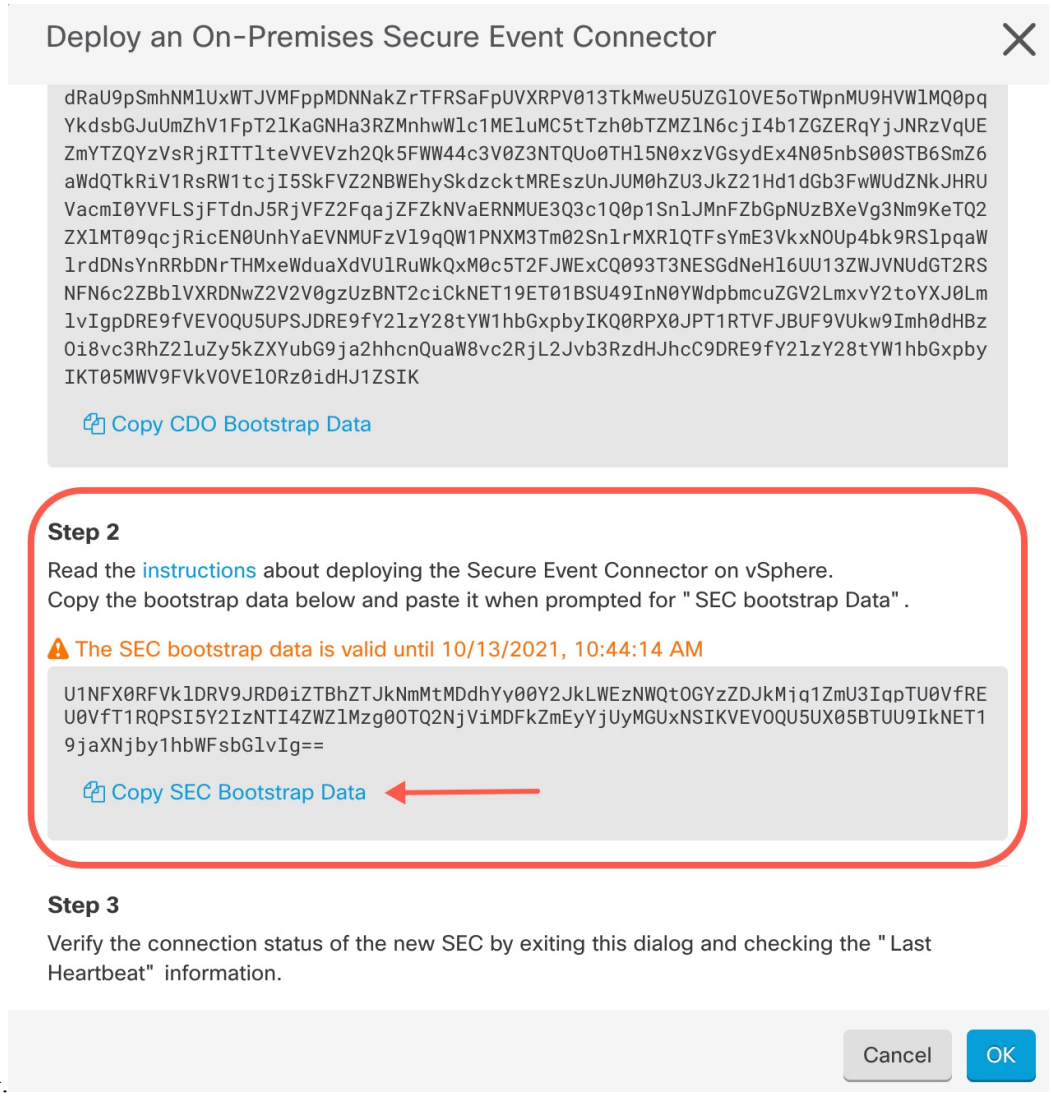
단계 **2** Security Cloud Control 플랫폼 메뉴에서, **Products(**제품**)** > **Firewall(**방화벽**)**을 클릭합니다.

단계 **3** 왼쪽 창에서 **Administration(**관리**)** > **Secure Connectors(**보안 커넥터**)**.

단계 **4** 위의 사전 요구 사항에 있는 절차를 사용하여 설치한 Security Cloud Control 커넥터를 선택합니다. Secure Connector(보안 커넥터) 테이블에서는 이를 Secure Event Connector(보안 이벤트 커넥터)로 표시됩니다.

단계 **5** 오른쪽의 작업 창에서 **Deploy an On-Premises Secure Event Connector(**온프레미스 보안 디바이스 커넥터 구축**)**를 클릭합니다.

단계 6 마법사 2단계에서 링크를 클릭하여 **SEC** 부트스트랩 데이터를 복사합니



다.

단계 7 SSH를 사용하여 Secure Connector에 연결하고 Security Cloud Control 사용자로 로그인합니다.

단계 8 로그인한 후에는 **sdc** 사용자로 전환합니다. 암호를 묻는 메시지가 표시되면 "Security Cloud Control" 사용자의 암호를 입력합니다. 다음은 이러한 명령의 예입니다.

```
[cdo@sdc-vm ~]$ sudo su sdc
[sudo] password for cdo: <type password for cdo user>
[sdc@sdc-vm ~]$
```

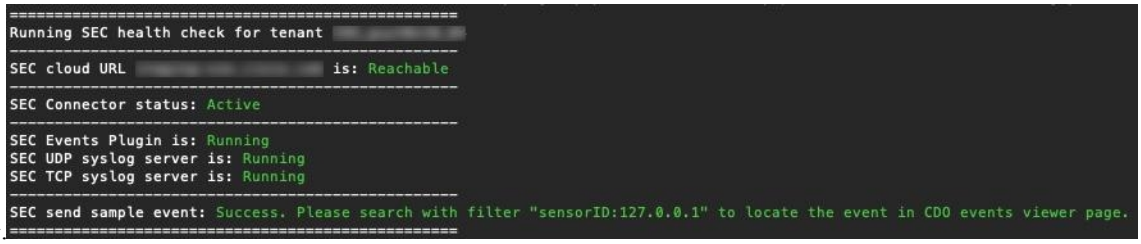
단계 9 프롬프트에서 sec.sh 설정 스크립트를 실행합니다.

```
[sdc@sdc-vm ~]$ /usr/local/cdo/toolkit/sec.sh setup
```

단계 10 프롬프트 끝에 4단계에서 복사한 부트스트랩 데이터를 붙여넣고 **Enter** 키를 누릅니다.

```
Please copy the bootstrap data from Setup Secure Event Connector page of CDO:
 KJHYFuYTFuIGhiJKlKnJHvHfgxTewrtwE
RtyFUiyIOHKNkJbKhvhgyRStwterTyufGUihoJpojP9UOoiUY8VHHGFXREWRtygfhVjhkOuihIuyftyXtfcghvjbkhB=
```

SEC가 온보딩되면 sec.sh는 SEC의 상태를 확인하는 스크립트를 실행합니다. 모든 상태 확인이 "녹색"인 경우 상태 확인은 이벤트 로그에 샘플 이벤트를 전송합니다. 샘플 이벤트는 이벤트 로그에 "sec-health-check"라는 정책으로표시됩니다.



등록에 실패했거나 SEC 온 보딩에 실패했다는 메시지가 표시되면 보안 이벤트 커넥터 온보딩 장애 문제 해결로 이동하십시오.

성공 메시지가 표시되면 **Deploy an ON-Premise Secure Event Connector(**온프레미스 보안 이벤트 커넥터 구축**)** 대화 상자에서 **Done(**완료**)**을 클릭합니다. VM 이미지에 SEC 설치를 완료했습니다.

다음에 수행할 작업

SAL SaaS의 구현을 계속하려면 이 절차로 돌아가십시오. ASA 디바이스에 대한 SaaS(Secure Logging Analytics) 구현, 40 페이지 .

관련 정보**:**

- Secure Device Connector 문제 해결
- 보안 이벤트 커넥터 문제 해결
- SEC 온보딩 장애 문제 해결
- SEC 등록 실패 문제 해결

Terraform 모듈을 사용하여 AWS VPC에 보안 이벤트 커넥터 설치

시작하기 전에

- 이 작업을 수행하려면 Security Cloud Control 테넌트에서 SAL을 활성화해야 합니다. 이 섹션에서는 SAL 라이선스가 있다고 가정합니다. 라이선스가 없는 경우 Cisco 보안 및 분석 로깅, 로깅 및 문제 해결 라이선스를 구매합니다.
- 새 SEC가 설치되어 있는지 확인합니다. 새 SEC를 생성하려면 SDC 가상 머신에 SEC(Secure Event Connector) 설치, 2 페이지의 내용을 참조하십시오.
- SEC를 설치할 때 Security Cloud Control 부트스트랩 데이터 및 SEC 부트스트랩 데이터를 적어 두십시오.

프로시저

단계 1 Terraform 레지스트리의 Secure Event Connector Terraform 모듈로 이동하고 지침에 따라 SEC Terraform 모듈을 Terraform 코드에 추가합니다.

단계 2 Terraform 코드를 적용합니다.

단계 3 `instance_id` 및 `sec_fqdn` 출력은 나중에 절차에서 필요하므로 인쇄해야 합니다.

참고
SEC 문제를 해결하려면 AWS Systems Manager Session Manager(SSM)를 사용하여 SEC 인스턴스에 연결해야 합니다. SSM을 사용하여 인스턴스에 연결하는 방법에 대한 자세한 내용은 AWS Systems Manager Session Manager 설명서를 참조하십시오.

SSH를 사용하여 SDC 인스턴스에 연결하는 포트는 보안상의 이유로 노출되지 않습니다.

단계 4 ASA에서 SEC로 로그를 전송하려면 생성한 SEC의 인증서 체인을 가져와 3단계의 출력과 함께 다음 명령을 실행하여 리프 인증서를 제거합니다.

```
rm -f /tmp/cert_chain.pem && openssl s_client -showcerts -verify 5 -connect <FQDN>:10125 < /dev/null
| awk '/BEGIN CERTIFICATE/,/END CERTIFICATE/{ if(/BEGIN CERTIFICATE/){a++}; out="/tmp/cert_chain.pem";
 if(a > 1) print >>out}'
```

단계 5 `/tmp/cert_chain.pem`의 내용을 클립보드에 복사합니다.

단계 6 다음 명령을 사용하여 SEC의 IP 주소를 기록해 둡니다.

```
nslookup <FQDN>
```

단계 7 Security Cloud Control에 로그인하고 새 트러스트 포인트 개체 추가를 시작합니다. 자세한 내용은 신뢰할 수 있는 CA 인증서 개체 추가를 참조하십시오. **Add(**추가**)**를 클릭하기 전에 **Other Options(**기타 옵션**)**에서 **Enable CA flag in basic constraints extension(**기본 제약 조건 확장에서 **CA** 플래그 활성화**)** 확인란의 선택을 취소해야 합니다.

단계 8 **Add(**추가**)**를 클릭하고 **Install Certificate(**인증서 설치**)** 페이지의 Security Cloud Control에서 생성한 CLI 명령을 복사한 다음 **Cancel(**취소**)**을 클릭합니다.

단계 9 `enrollment terminal(등록 터미널)` 아래 텍스트 클립보드에 `no ca-check`를 추가합니다.

단계 10 SSH로 ASA 디바이스에 연결하거나 Security Cloud Control에서 ASA CLI 옵션을 사용하고 다음 명령을 실행합니다.

```
DataCenterFW-1> en
Password: ****************
DataCenterFW-1# conf t
DataCenterFW-1(config)# <paste your modified ASA CLIs here and press Enter>
DataCenterFW-1(config)# wr mem
Building configuration...
Cryptochecksum: 6634f35f 4c5137f1 ab0c5cdc 9784bdb6
```

다음에 수행할 작업

SEC가 AWS SSM을 사용하여 패킷을 수신하고 있는지 확인할 수 있습니다.

다음과 유사한 로그가 표시됩니다.

```
time="2023-05-10T17:13:46.135018214Z" level=info msg="[ip-10-100-5-19.ec2.internal][util.go:67
 plugin.createTickers:func1] Events - Processed - 6/s, Dropped - 0/s, Queue size - 0"
```

보안 이벤트 커넥터 제거

경고: 이 절차는 Secure Device Connector에서 보안 이벤트 커넥터를 삭제합니다. 이렇게 하면 SaaS(Secure Logging Analytics)를 사용할 수 없습니다. 이는 되돌릴 수 없습니다. 질문이나 우려 사항이 있는 경우 이 작업을 수행하기 전에 Security Cloud Control 지원에 문의하십시오.

Secure Device Connector에서 보안 이벤트 커넥터를 제거하는 작업은 다음의 2단계 프로세스입니다.

1. Security Cloud Control에서 SEC 제거
2. SDC에서 SEC 파일을 제거합니다.

후속 작업:Security Cloud Control에서 SEC 제거 계속

Security Cloud Control에서 SEC 제거

시작하기 전에

보안 이벤트 커넥터 제거, 22 페이지을 참조하십시오.

프로시저

단계 **1** Security Cloud Control에 로그인합니다.

단계 **2** Security Cloud Control 플랫폼 메뉴에서, **Products(**제품**)** > **Firewall(**방화벽**)**을 클릭합니다.

단계 **3** 왼쪽 창에서 **Administration(**관리**)** > **Secure Connectors(**보안 커넥터**)**를 선택합니다.

단계 **4** 디바이스 유형인 보안 이벤트 커넥터가 있는 행을 선택합니다.

경고**!**
Secure Device Connector를 선택하지 않도록 주의하십시오.

단계 **5** **Actions(**작업**)** 창에서 **Remove(**제거**)**를 클릭합니다.

단계 **6** **OK(**확인**)**를 클릭하여 확인합니다.

다음에 수행할 작업

Secure Device Connector에서 Secure Event Connector를 제거하는 작업은 다음의 2단계 프로세스입니다., 23 페이지를 진행합니다.

Secure Device Connector에서 Secure Event Connector를 제거하는 작업은 다음의 2단계 프로세스입니다.

이는 SDC에서 보안 이벤트 커넥터를 제거하는 2단계 절차의 두 번째 부분입니다. 시작하기 전에 보안 이벤트 커넥터 제거, 22 페이지을 참조하십시오.

프로시저

단계 **1** 가상 머신 하이퍼바이저를 열고 SDC에 대한 콘솔 세션을 시작합니다.

단계 **2** `[cdo@sdc]$ sudo su sdc`명령을 사용하여 SDC 사용자로 전환합니다.

단계 **3** SDC 가상 머신에서 SEC를 제거하려면 다음 명령 중 하나를 사용할 수 있습니다.

- 테넌트 선택기를 사용하려는 경우(또는 VM에 테넌트가 하나뿐인 경우):

```
[sdc@tenant toolkit]$ sdc eventing delete
```

- 명령어 인수에서 테넌트를 직접 지정하는 경우:

```
[sdc@tenant toolkit]$ sdc eventing delete CDO_{tenant-name}
```

단계 **4** SEC 파일을 제거할 것인지 확인합니다.

SaaS(Secure Logging Analytics)에 사용되는 디바이스의 TCP, UDP 및 NSEL 포트 찾기

SaaS(Secure Logging Analytics)를 사용하면 ASA 또는 FDM 관리 디바이스의 이벤트를 SEC(Secure Event Connector)의 특정 UDP, TCP 또는 NSEL 포트로 전송할 수 있습니다. 그런 다음 SEC는 해당 이벤트를 Cisco 클라우드로 전달합니다.

이러한 포트가 아직 사용 중이 아닌 경우, SEC는 이벤트를 수신하는 데 포트를 제공하며, SaaS(Secure Logging Analytics) 설명서에서는 기능을 구성할 때 포트 사용을 권장합니다.

- TCP: 10125
- UDP: 10025
- NSEL: 10425

이러한 포트가 이미 사용 중인 경우 SaaS(Secure Logging Analytics)를 구성하기 전에 SEC 디바이스 세부 정보를 확인하여 실제로 이벤트를 수신하는 데 사용 중인 포트를 확인합니다.

SEC에서 사용하는 포트 번호를 찾으려면 다음을 수행합니다.

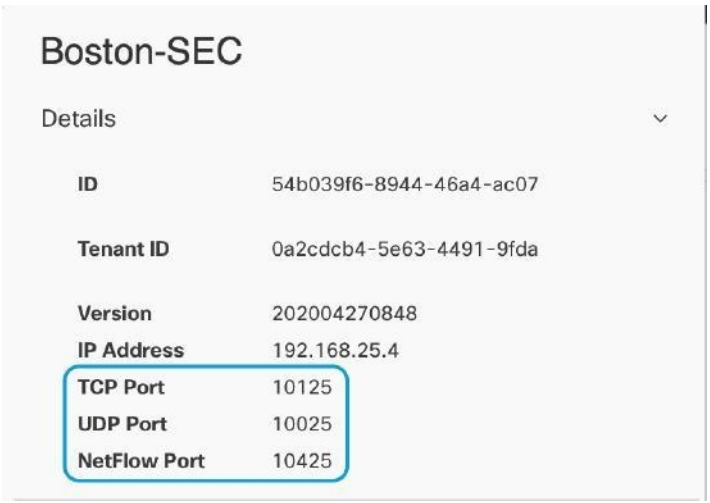
Procedure

단계 **1** Security Cloud Control 플랫폼 메뉴에서, **Products(**제품**)** > **Firewall(**방화벽**)**을 클릭합니다.

단계 **2** 왼쪽 창에서 **Administration(**관리**)** > **Integration(**통합**)** > **Firewall Management Center**를 클릭하고 **Secure Connectors(**보안 커넥터**)** 탭을 클릭합니다.

단계 **3** **Secure Connector(**보안 커넥터**)** 페이지에서 이벤트를 전송할 SEC를 선택합니다.

단계 **4** **Details(**세부 정보**)** 창에 이벤트를 전송해야 하는 TCP, UDP 및 NetFlow(NSEL) 포트가 표시됩니다.



Security Cloud Control에서 Security Analytics and Logging(SaaS) 정보

용어 참고: 이 설명서에서는 Cisco Security Analytics and Logging을 Secure Cloud Analytics 포털(Software as a Service 제품)과 함께 사용하는 경우 이러한 통합을 Cisco Security Analytics and Logging(SaaS) 또는 SAL(SaaS)이라고 합니다.

Cisco SAL(Security Analytics and Logging)을 사용하면 모든 방화벽 디바이스에서 지원되는 유형의 보안 이벤트를 캡처하고 Security Cloud Control에서 확인할 수 있습니다. 이벤트는 Cisco Cloud에 저장되며 **Event Logging(**이벤트 로깅**)** 페이지에서 볼 수 있습니다. 여기에서 이벤트를 필터링하고 검토하여 네트워크에서 어떤 보안 규칙이 트리거되고 있는지 명확하게 이해할 수 있습니다.

추가 라이선싱을 사용하면 이러한 이벤트를 캡처한 후 Security Cloud Control에서 프로비저닝된 Secure Cloud Analytics 포털로 교차 실행할 수 있습니다. Secure Cloud Analytics는 이벤트 및 네트워크 플로우 데이터에 대한 행동 분석을 수행하여 네트워크의 상태를 추적하는 SaaS(Software as a Service) 솔루션입니다. 방화벽 이벤트 및 네트워크 플로우 데이터를 비롯한 소스에서 네트워크 트래픽에 대한 정보를 수집하여 트래픽에 대한 관찰을 생성하고 트래픽 패턴을 기반으로 네트워크 엔티티의 역할을 자동으로 식별합니다. Secure Cloud Analytics는 Talos와 같은 위협 인텔리전스의 다른 소스와 결합

된 이 정보를 사용하여 본질적으로 악의적인 행동이 있음을 나타내는 경고를 생성합니다. 알림과 함께 Secure Cloud Analytics는 알림을 조사하고 악의적인 동작의 소스를 찾기 위한 더 나은 기반을 제공하기 위해 수집한 네트워크 및 호스트 가시성 및 상황 정보를 제공합니다.

Security Cloud Control에서 이벤트 유형

Secure Logging Analytics(SaaS)에 기록된 보안 이벤트를 필터링할 때, Security Cloud Control가 지원하는 ASA, FTD 및 이벤트 유형 목록에서 선택할 수 있습니다. Security Cloud Control메뉴에서 **Analytics(분석)** > **Event Logging(이벤트 로깅)**으로 이동하고 필터 아이콘을 클릭하여 이벤트를 선택합니다. 이러한 이벤트 유형은 시스템 로그 ID의 그룹을 나타냅니다. 아래 표는 어떤 시스템 로그 ID가 어떤 이벤트 유형에 포함되어 있는지 보여줍니다. 특정 시스템 로그 ID에 대한 자세한 내용은 Cisco ASA Series 시스템 로그 메시지 또는 Cisco Secure Firewall Threat Defense 시스템 로그 메시지 가이드에서 검색할 수 있습니다.

일부 시스템 로그 이벤트에는 추가 속성 "EventName"이 있습니다. attribute:value 쌍을 기준으로 필터링하여 이벤트 이름 속성을 통해 이벤트 테이블을 필터링해서 찾을 수 있습니다. 시스템 로그 이벤트에 대한 이벤트 이름 속성을 참조하십시오.

일부 시스템 로그 이벤트에는 추가 속성 "EventGroup" 및 "EventGroupDefinition"이 있습니다. attribute:value 쌍을 기준으로 필터링하여 이러한 추가 속성을 사용하여 이벤트 테이블을 필터링할 수 있습니다. 일부 시스템 로그 메시지에 대한 EventGroup 및 EventGroupDefinition 속성을 참조하십시오.

NetFlow 이벤트는 시스템 로그 이벤트와 다릅니다. **NetFlow** 필터는 NSEL 레코드를 생성한 모든 NetFlow 이벤트 ID를 검색합니다. 이러한 NetFlow 이벤트 ID는 Cisco ASA NetFlow 구현 가이드에 정의되어 있습니다.

다음 테이블에서는 Security Cloud Control가 지원하는 이벤트 유형을 설명하고 이벤트 유형에 해당하는 시스템 로그 또는 NetFlow 이벤트 번호를 나열합니다.

필터 이름	설명	해당 시스템 로그 이벤트 또는 **NetFlow** 이벤트
AAA	이는 AAA가 구성된 경우 네트워크의 리소스를 모두 사용하거나 권한을 부여하거나 인증하려는 시도가 실패 또는 잘못된 경우 시스템에서 생성하는 이벤트입니다.	109001-109035 113001-113027
봇넷	이러한 이벤트는 사용자가 멀웨어에 감염된 호스트(봇넷)를 포함할 수 있는 악의적인 네트워크에 액세스하려고 하거나 시스템이 동적 필터 차단 목록에서 도메인 또는 IP 주소와 주고받는 트래픽을 탐지하는 경우 로깅됩니다.	338001-338310

필터 이름	설명	해당 시스템 로그 이벤트 또는 **NetFlow** 이벤트
장애 조치	이러한 이벤트는 시스템이 스테이트풀 및 스테이트리스 페일오버 구성에서 오류를 탐지하거나 페일오버 발생 시 보조 방화벽 유닛에서 오류를 탐지하면 로깅됩니다.	101001-101005, 102001, 103001-103007, 104001-104004, 105001-105048 210001-210022 311001-311004 709001-709007
방화벽 거부됨	이러한 이벤트는 방화벽 시스템이 다양한 이유로 네트워크 패킷의 트래픽을 거부할 때 발생하며, 이는 잠재적으로 네트워크에 대한 공격을 의미할 수 있습니다. 보안 정책으로 인해 패킷이 삭제되거나 시스템이 동일한 소스 IP와 대상 IP를 가진 패킷을 수신하여 패킷이 삭제되는 등 다양한 패킷 삭제 이유가 있을 수 있습니다. 방화벽 거부됨 이벤트는 NetFlow에 포함될 수 있으며 NetFlow 이벤트 ID 및 시스템 로그 ID와 함께 보고될 수 있습니다.	106001, 106007, 106012, 106013, 106015, 106016, 106017, 106020, 106021, 106022, 106023, 106025, 106027
방화벽 트래픽	이는 네트워크에서의 다양한 연결 시도, 사용자 ID, 타임스탬프, 종료된 세션 등에 따라 로깅되는 이벤트입니다. 방화벽 트래픽 이벤트는 NetFlow에 포함될 수 있으며 NetFlow 이벤트 ID 및 시스템 로그 ID와 함께 보고될 수 있습니다.	106001-106100, 108001-108007, 110002-110003 201002-201013, 209003-209005, 215001 302002-302304, 302022-302027, 303002-303005, 313001-313008, 317001-317006, 324000-324301, 337001-337009 400001-400050, 401001-401005, 406001-406003, 407001-407003, 408001-408003, 415001-415020, 416001, 418001-418002, 419001-419003, 424001-424002, 431001-431002, 450001 500001-500005, 508001-508002 607001-607003, 608001-608005, 609001-609002, 616001 703001-703003, 726001

필터 이름	설명	해당 시스템 로그 이벤트 또는 **NetFlow** 이벤트
IPsec VPN	IPsec 보안 연결의 불일치가 발생하거나 시스템이 수신하는 IPsec 패킷에서 오류를 탐지하면 IPsec VPN이 구성한 방화벽에 이러한 이벤트가 로깅됩니다.	402001-402148, 602102-602305, 702304-702307
NAT	NAT 항목이 생성되거나 삭제된 경우, 그리고 NAT 풀의 모든 주소가 사용된 경우 NAT 구성 방화벽에 이러한 이벤트가 로깅됩니다.	201002-201013, 202001-202011, 305005-305012
SSL VPN	WebVPN 세션이 생성되거나 종료될 때, 사용자 액세스 오류 및 사용자 활동이 발생할 때 SSL VPN으로 구성된 방화벽에 이러한 이벤트가 로깅됩니다.	716001-716060, 722001-722053, 723001-723014, 724001-724004, 725001-725015
NetFlow	네트워크 패킷이 인터페이스를 오가는 IP 네트워크 트래픽, 타임스탬프, 사용자 ID 및 전송되는 데이터 양을 중심으로 이러한 이벤트가 로깅됩니다.	0, 1, 2, 3, 5

필터 이름	설명	해당 시스템 로그 이벤트 또는 **NetFlow** 이벤트
연결	사용자가 시스템을 통과하는 트래픽을 생성할 때 연결에 대한 이벤트를 생성할 수 있습니다. 액세스 규칙에서 연결 로깅을 활성화하여 이러한 이벤트를 생성합니다. 보안 인텔리전스 정책과 SSL 암호 해독 규칙에서 로깅을 활성화하여 연결 이벤트를 생성할 수도 있습니다. 연결 이벤트에는 탐지된 세션에 관한 데이터가 포함되어 있습니다. 모든 개별 연결 이벤트에 대한 정보는 몇 가지 요소에 따라 가용성이 결정되지만, 일반적으로는 다음과 같습니다. • 기본 연결 속성: 타임 스탬프, 소스 및 대상 IP 주소, 인그레스 및 이그레스 영역, 연결을 처리한 디바이스 등 • 시스템에서 검색하거나 유추한 추가 연결 속성: 애플리케이션, 요청된 URL 또는 연결과 관련된 사용자 등 • 연결이 로깅된 사유에 대한 메타데이터: 어떤 설정이 트래픽을 처리했는지, 연결이 허용 또는 차단되었는지, 암호화 및 해독된 연결에 대한 상세정보 등	430002, 430003

필터 이름	설명	해당 시스템 로그 이벤트 또는 **NetFlow** 이벤트
침입	시스템은 호스트 및 호스트 데이터의 가용성, 무결성 및 기밀성에 영향을 미칠 수 있는 악성 활동 탐지를 위해 네트워크를 통과하는 패킷을 검토합니다. 시스템은 침입 가능성을 식별하는 경우 익스플로잇의 날짜, 시간, 익스플로잇 유형, 그리고 공격 소스와 대상에 관한 상황 정보의 레코드인 침입 이벤트를 생성합니다. 침입 이벤트는 호출하는 액세스 제어 규칙의 로깅 구성과 관계없이 차단하거나 알리도록 설정된 모든 침입 규칙에 대해 생성됩니다.	430001
파일	파일 이벤트는 파일 정책을 기준으로 하여 시스템이 네트워크 트래픽에서 탐지하고 선택적으로 차단한 파일을 나타냅니다. 이러한 이벤트를 생성하려면 파일 정책을 적용하는 액세스 규칙에 대해 파일 로깅을 활성화해야 합니다. 시스템이 파일 이벤트를 생성하는 경우 호출하는 액세스 제어 규칙의 로깅 구성과 관계없이 시스템은 관련 연결의 종료도 로깅합니다.	430004

필터 이름	설명	해당 시스템 로그 이벤트 또는 **NetFlow** 이벤트
멀웨어	시스템은 전체적인 액세스 제어 구성의 일부로 네트워크 트래픽에서 멀웨어를 탐지할 수 있습니다. AMP for Firepower는 결과 이벤트의 상태와 멀웨어가 탐지된 방법, 위치, 시간에 대한 상황 데이터를 포함하는 멀웨어 이벤트를 생성할 수 있습니다. 이러한 이벤트를 생성하려면 파일 정책을 적용하는 액세스 규칙에 대해 파일 로깅을 활성화해야 합니다. 파일 상태는 변경될 수 있습니다(예: 정상에서 멀웨어로 또는 멀웨어에서 정상으로). AMP for Firepower가 AMP 클라우드에 파일에 대해 쿼리하고, 쿼리한지 일주일 이내에 상태가 변경되었음을 클라우드에서 확인하는 경우, 시스템에서는 회귀적 멀웨어 이벤트를 생성합니다.	430005
보안 인텔리전스	보안 인텔리전스 이벤트는 정책에 따라 차단되거나 또는 모니터링된 각 연결의 보안 인텔리전스 정책에 의해 생성된 연결 이벤트 유형입니다. 모든 보안 인텔리전스 이벤트에는 내용이 채워진 Security Intelligence Category(보안 인텔리전스 범주) 필드가 있습니다. 이러한 각 이벤트에는 해당하는 "일반" 연결 이벤트가 있습니다. 보안 인텔리전스 정책은 액세스 제어를 비롯한 다른 많은 보안 정책보다 먼저 평가되기 때문에 보안 인텔리전스에 의해 연결이 차단된 경우, 그 결과로 생성된 이벤트에는 시스템이 후속 평가를 통해 수집했을 수 있는 정보(예: 사용자 ID)가 포함되지 않습니다.	430002, 430003

Cisco Security Analytics and Logging(SaaS) 프로비저닝 해제

Cisco Security Analytics and Logging(SaaS) 유료 구독이 만료되면 새로운 이벤트 수집이 즉시 중단됩니다. 만료일로부터 90일이 지나면 기존 이벤트 데이터를 보거나 쿼리할 수 있습니다. 구독을 리뉴얼할 수 있는 유예 기간은 180일입니다.

180일의 유예 기간이 경과하도록 허용하면 시스템에서 모든 이벤트 데이터를 비웁니다. 이제 **Event Logging(**이벤트 로깅**)** 페이지에서 보안 이벤트를 확인할 수 없으며, 보안 이벤트 및 네트워크 플로우 데이터에 동적 엔터티 모델링 행동 분석이 적용되지 않습니다.

Security Analytics and Logging 라이선스

Security Analytics and Logging 구독 개요

SAL를 Security Cloud Control Firewall Management 구독에 결합할 수 있습니다. Security Cloud Control로 방화벽을 관리할 경우, 다음과 같은 방법으로 Security Analytics and Logging 엔타이틀먼트를 얻을 수 있습니다.

- 무제한 로깅 기능이 포함된 디바이스 관리: 이 옵션은 디바이스별 라이선스를 제공합니다. 방화벽 디바이스에 대한 디바이스 관리 기능과 90일간의 롤링 기간 동안 무제한 로그 저장을 포함합니다.
- 선택적 클라우드 로깅 기능이 포함된 디바이스 관리 전용: 이 옵션은 관리 기능만을 위한 디바이스별 라이선스 구매를 포함합니다. 그런 다음 Security Analytics and Logging를 별도의 클라우드 로깅 구독으로 추가할 수 있습니다. 이를 통해 특정 운영 및 규정 준수 요구 사항에 따라 로깅 데이터 저장 및 로그 보존 기간을 맞춤 설정할 수 있습니다.

90일 무료 평가판

90일 무료 체험을 신청하여 일일 데이터 입력량을 정확히 추정할 수 있습니다. Security Cloud Control에 로그인 후 **Events & Logs(**이벤트 및 로그**)** > **Events(**이벤트**)** > **Event Logging(**이벤트 로깅**)** 탭으로 이동합니다. 원하는 구독 계획을 구매하여 Security Cloud Control Firewall Management 주문 가이드의 지침에 따라 서비스를 계속할 수 있습니다.

Security Analytics and Logging 유료 구독 계층

무제한 로깅 옵션이 포함된 디바이스 관리를 사용하지 않으려면 로깅 용량을 별도로 구매할 수 있습니다. 이 독립형 Security Analytics and Logging 구독 오퍼링은 더 큰 유연성, 더 긴 기본 보존 기간 및 증가된 저장 용량 권한을 제공합니다. 이러한 구독 등급의 기본 최소 보존 기간은 1년입니다.

다음과 같은 경우 유연한 Security Analytics and Logging 구독 계층을 선택합니다.

- 방화벽 디바이스는 이미 다른 주문으로 구매했습니다.
- 특정 로깅 용량 추정치에 따라 고정된 인제스트, 저장, 로깅 보존 용량을 기준으로 계층을 구매하고자 합니다.

- 로그 보존 기간을 90일 이상으로 설정해야 합니다.

Security Analytics and Logging 구독은 Essentials, Advantage 및 Premier의 세 가지 계층으로 분류됩니다. 이 표에서는 각 계층에서 사용할 수 있는 스토리지 용량 및 로그 보존 기간에 대해 설명합니다.

설명	보존 기간	스토리지 제한	구독 기간
Cisco SAL Essentials 구독	1년, 2년 또는 3년	2TB	0~5년
Cisco SAL Advantage 구독	1년, 2년 또는 3년	4TB	0~5년
Cisco SAL Premier 구독	1년, 2년 또는 3년	10 TB	0~5년

구독 요금제에 대한 자세한 내용은 Security Cloud Control Firewall Management 주문 가이드 를참조하십시오.

Note 유료 구독의 경우, Security Analytics and Logging은 이벤트 데이터를 자동으로 관리하여 라이선스 보존 기간과 일치하도록 합니다. Security Analytics and Logging는 지정된 보존 기간보다 오래된 이벤트 데이터를 매일 삭제하며, 전체 보존 기간 내의 모든 이벤트 데이터에 대한 접근 권한을 항상 유지할 수 있도록 보장합니다.

일일 수집 속도 예측

Cisco cloud가 온보딩된 방화벽 디바이스에서 매일 수신하는 이벤트 수를 반영하는 데이터 구독 플랜을 구매해야 합니다. 이를 일일 수집 속도라고 합니다. Logging Volume Estimator 툴를 사용하여 일일 수집 속도를 예측할 수 있으며, 속도가 변경되면 데이터 요금제를 업데이트할 수 있습니다.

Security Analytics and Logging 라이선스 구독

Security Analytics and Logging 평가판 구독 시작

온보딩된 보안 디바이스가 Cisco 클라우드로 전송하는 일일 이벤트 볼륨과 일치하는 데이터 스토리지 요금제를 구매합니다. 이 양을 일일 수집 속도라고 합니다. 구매 전에 Security Analytics and Logging 무료 평가판에 참여하여 수집 속도를 정확히 추정합니다.

- 이 평가판 요금제를 사용하면 90일 동안 모든 Security Analytics and Logging 기능에 액세스할 수 있습니다.
- 90일 평가판 기간 동안 온보딩된 방화벽은 Security Analytics and Logging에 이벤트를 전송합니다. 이벤트 수집 속도를 모니터링하고, 스토리지 요구 사항을 파악하며, 성능을 평가하십시오. 이 데이터는 가장 적합한 유료 구독을 계획하고 선택하는 데 도움이 됩니다.

- 평가판이 활성화된 상태에서 유료 Security Analytics and Logging 구독을 활성화하면, Security Cloud Control는 해당 제품 인스턴스의 평가판 라이선스가 유료 라이선스로 대체되고 평가판이 종료됩니다.
- 유료 구독을 체험판에 적용하지 않기로 선택하면, 90일 후 이벤트 수집이 자동으로 중단됩니다. 이후에는 Security Analytics and Logging 기능에 액세스할 수 없습니다. 그러나 기존 로그 데이터는 체험판 만료일로부터 추가로 90일간 Security Analytics and Logging 클라우드에 보관됩니다.

참고 이 90일 유예 기간 내에 유료 Security Analytics and Logging 라이선스를 구독하지 않으면, 모든 체험판 데이터가 영구적으로 삭제됩니다.

유료 **Security Analytics and Logging** 구독 주문

Security Analytics and Logging 사용 후 계속 사용하거나 기존 로깅 기능을 업그레이드하려면 다음을 수행합니다.

1. 시험 사용 기간 동안 얻은 인사이트(일일 수집 속도, 필요한 보존 기간, 스토리지 용량)을 활용하여 가장 적합한 Security Analytics and Logging 구독 플랜을 결정합니다.
2. 적절한 Security Analytics and Logging 구독을 구매하려면 Cisco 담당자 또는 공인 파트너와 협력하십시오.

Security Analytics and Logging 구독 클레임

새로운 Security Analytics and Logging 구독을 구매한 후, Security Cloud Control내에 활성화할 수 있는 클레임 코드를 받게 됩니다. 구독 클레임 코드가 포함된 환영 이메일이 구매 과정에서 지정한 프로비저닝 담당자에게 자동으로 발송됩니다. 최종 고객 연락처를 포함시킨 경우, 해당 고객도 사본을 받게 됩니다. 구독 시작 요청일에 이 이메일을 수신하게 됩니다.

Security Cloud Control 관리자는 클레임 코드를 사용하여 조직의 구독을 활성화합니다. 구독을 신청하고 활성화하는 방법에 대한 자세한 내용은 구독 클레임을 참조하십시오.

Security Analytics and Logging 구독 리뉴얼

활성 Security Analytics and Logging 구독을 유지하면 지속적인 기록과 과거 데이터 접근이 보장됩니다.

- Security Analytics and Logging 구독이 리뉴얼되지 않고 만료되면 방화벽에서 이벤트 수집이 즉시 중단됩니다.
- 구독이 만료된 후에도 기존 이벤트 데이터를 90일 동안 계속해서 조회하고 검색할 수 있습니다. 90일이 지나면 이벤트 데이터에 더 이상 액세스할 수 없습니다.
- 기존 데이터는 구독 만료일로부터 180일간의 유예 기간 동안 Security Analytics and Logging 클라우드에 보관됩니다.
- 이 180일 유예 기간 내에 Security Analytics and Logging 구독을 리뉴얼하지 않으면, 모든 이벤트 데이터가 Security Analytics and Logging 클라우드에서 영구적으로 삭제됩니다.

Security Analytics and Logging 라이선스 정보 보기

부여받은 월간 스토리지 한도 및 이벤트 스토리지 보존 기간과 같은 Security Analytics and Logging 라이선스 정보를 확인합니다. 별도의 Security Analytics and Logging 라이선스 및 데이터 플랜이 없는 경우, 90일 롤링 데이터 스토리지 세부 정보가 라이선스 정보에 표시됩니다.

프로시저

단계 **1** Security Cloud Control 플랫폼 메뉴에서, **Products(**제품**)** > **Firewall(**방화벽**)**을 클릭합니다.

단계 **2** 왼쪽 탐색 모음에서 **Administration(**관리**)** > **Logging Settings(**로깅 설정**)**.

단계 **3** **View Logging Storage Usage(**로깅 스토리지 사용량 보기**)** 버튼을 클릭합니다.

팁
또는 왼쪽 내비게이션 바 에서 **Events & Logs(**이벤트 및 로그**)** > **Events(**이벤트**)** > **Event Logging(**이벤트 로깅**)** 로 이동한 다음 **Storage Utilization(**스토리지 사용**)** 버튼을 클릭하여 보안 애널리틱스 및 로깅 라이선스 정보를 확인합니다.

Event Logging Insights and Storage Usage(이벤트 로깅 인사이트 및 스토리지 사용량) 대시보드는 Security Analytics and Logging 라이선스 구독에 대한 포괄적인 개요를 제공합니다:

- **Retention policy(**보존 정책**)**: 구독에 따른 이벤트 로그 보존 기간을 표시합니다. Security Analytics and Logging는 보존 기간보다 오래된 이벤트 데이터를 매일 제거하며, 전체 보존 기간 내 모든 이벤트 데이터에 대한 액세스 권한을 항상 유지하도록 보장합니다.
- **Storage capacity(**스토리지 용량**)**: Security Analytics and Logging 라이선스에 따라 부여된 총 데이터, 현재 사용된 스토리지의 양 및 남은 사용 가능한 스토리지를 표시합니다.

보안 애널리틱스 및 로깅 데이터 계획 사용량 보기 및 이벤트 수집 속도

현재 보안 애널리틱스 및 로깅 스토리지 사용량을 확인하고 이벤트 로깅 추세를 분석합니다. 이벤트 유형, 디바이스 유형 및 개별 디바이스별로 스토리지 사용량 추세를 분석하여 스토리지 사용 패턴에 대한 심층적인 인사이트를 얻을 수 있습니다. 데이터 시각화를 활용하여 신속하고 간편한 분석을 수행함으로써, 현재 스토리지 용량을 평가하고 스토리지 사용량이 보안 분석 및 로깅 라이선스에 지정된 한도에 근접할 경우 로깅 속도를 줄이기 위한 조치를 취할 수 있습니다.

Procedure

단계 **1** Security Cloud Control 플랫폼 메뉴에서, **Products(**제품**)** > **Firewall(**방화벽**)**을 클릭합니다.

단계 **2** 왼쪽 탐색 모음에서 **Administration(**관리**)** > **Logging Settings(**로깅 설정**)**를 클릭합니다.

단계 **3** 로깅 스토리지 사용량 보기를 클릭합니다.

Tip
또는 왼쪽 탐색 모음에서 **Events & Logs(**이벤트 및 로그**)** > **Events(**이벤트**)** > **Event Logging(**이벤트 로깅**)**로 이동한 다음 이벤트 로깅 인사이트 및 스토리지 사용량 버튼을 클릭하여 보안 애널리틱스 및 로깅 스토리지 사용량 및 이벤트 수집 추세를 확인합니다.

단계 **4** 다음 대시보드를 사용하여 스토리지 사용량을 맞춤 설정하고 분석하며, 방화벽 구축 환경의 이벤트 로깅 동향에 대한 더 많은 인사이트를 얻습니다.

- **Usage Trends(**사용 추세**)** 대시보드에는 지난 12개월 동안의 스토리지 사용량이 표시됩니다. 막대 위에 마우스를 올려 놓으면 해당 월의 데이터 사용량을 확인할 수 있습니다.
- **EPS(**초당 이벤트 수**)** 추세 대시보드에는 온보딩된 디바이스의 이벤트 수집 속도가 표시됩니다. 특정 시간대 또는 특정 디바이스에 대해 초당 이벤트 추세 보기를 맞춤 설정하여 더 세분화된 데이터를 확인합니다. 지난 1주, 2주, 3주 또는 1개월 동안의 데이터를 필터링할 수 있습니다.

  Note
  디바이스 드롭다운 목록에는 이벤트를 Cisco Security Cloud 에 전송하는 매니지드 방화벽 디바이스가 표시됩니다.

- **Utilization by event type(**이벤트 유형별 사용량**)** 추세: 다양한 이벤트 유형별로 사용된 이벤트 데이터 저장 용량을 일일 바이트 단위로 표시합니다. 이 위젯을 사용하여 이벤트 유형별 스토리지 사용량을 모니터링하고, 특정 이벤트 유형에 대한 스토리지 사용량의 급증 또는 비정상적인 변화를 식별합니다. 이 인사이트를 통해 특정 이벤트 유형에 대한 로깅 설정을 조정하고 스토리지 사용량을 관리할 수 있습니다.
- **Utilization by Device type Trends(**디바이스 유형별 사용량 추세**)**: 매니지드 디바이스 유형별로 일일 사용 이벤트 데이터 저장 용량을 바이트 단위로 표시합니다. 이 위젯을 사용하여 디바이스 유형별 저장소 사용량을 모니터링하고, 특정 디바이스 유형의 저장소 사용량에서 급증 현상이나 비정상적인 변화를 식별합니다.
- **Utilization by device Trend(**디바이스별 사용량**)**: Security Cloud 제어에 이벤트를 전송하는 각 보안 디바이스에서 사용된 이벤트 데이터 스토리지를 일일 바이트 단위로 표시합니다. 이 위젯은 저장소 사용량이 초당 평균 바이트 수를 초과하는 디바이스에 집중하여 사용성 향상을 위해 상위 5개 디바이스만 표시합니다. 이 위젯을 사용하여 각 디바이스의 저장소 사용량을 모니터링하고 급증 또는 비정상적인 변화를 식별합니다. 이 인사이트를 통해 특정 디바이스에 대한 로깅 설정을 조정하고 저장소 사용을 효과적으로 관리할 수 있습니다.

이벤트 스토리지 기간 연장 및 이벤트 스토리지 용량 늘리기

롤링 이벤트 스토리지를 확장하거나 이벤트 클라우드 스토리지의 용량을 늘리려면 다음 단계를 수행하십시오.

프로시저

단계 **1** Cisco Commerce에 사용자 계정으로 로그인합니다.
단계 **2** Security Cloud Control PID를 선택합니다.

단계 3 프롬프트에 따라 스토리지 용량의 길이 또는 용량을 업그레이드합니다.

증가된 비용은 기존 라이선스의 남은 기간에 따라 비례 배분됩니다. 자세한 지침은 Cisco Defense Orchestrator 제품 견적에 대한 지침을 참조하십시오.

보안 애널리틱스 및 로깅 알림 보기

매니지드 방화벽 디바이스에 대해 보안 애널리틱스 및 로깅 및 구성과 FTD 이벤트 설정에 대한 경고를 확인합니다.

프로시저

단계 1 Security Cloud Control 플랫폼 메뉴에서, **Products(**제품**)** > **Firewall(**방화벽**)**을 클릭합니다.

단계 2 왼쪽 탐색 모음에서 **Administration(**관리**)** > **Logging Settings(**로깅 설정**)**.

단계 3 **View Logging Storage Usage(**로깅 스토리지 사용량 보기**)** 버튼을 클릭합니다.

팁
또는 왼쪽 내비게이션 바 에서 **Events & Logs(**이벤트 및 로그**)** > **Events(**이벤트**)** > **Event Logging(**이벤트 로깅**)** 로 이동한 다음 **Storage Utilization(**스토리지 사용**)** 버튼을 클릭하여 보안 애널리틱스 및 로깅 라이선스 정보를 확인합니다.

Alerts and Notifications(알림 및 알림**)**섹션에는 이벤트 기록에 영향을 미치는 설정에 대한 알림이 표시됩니다. 문제 해결을 위한 작업을 수행할 수 있습니다. 이러한 설정 중 일부는 다음과 같습니다.

- 클라우드 설정으로 이벤트 전송이 비활성화됩니다.
- 클라우드 설정으로 이벤트 전송이 디바이스 레벨에서 비활성화됩니다.
- 보안 이벤트 커넥터를 사용할 수 없게 됩니다.
- 이벤트 수집 속도가 증가합니다.

Security Analytics and Logging 라이선스에 대한 FAQ

내 **Security Analytics and Logging** 할당량에 대해 어떤 데이터가 계산됩니까**?**

Cisco 클라우드 또는 Secure Event Connector로 직접 전송된 모든 이벤트는 Security Analytics and Logging에 누적되며 데이터 할당량에 포함됩니다.

이벤트 뷰어를 필터링해도 Security Analytics and Logging에 저장된 이벤트 수는 줄어들지 않습니다. 이렇게 하면 이벤트 뷰어에 표시되는 이벤트 수만 줄어듭니다.

스토리지 할당량을 빠르게 사용하고 있습니다. 어떻게 해야 합니까?

이 문제를 해결하는 두 가지 방법은 다음과 같습니다.

- 추가 스토리지를 요청합니다.
- 이벤트를 로깅하는 규칙의 수를 줄이는 것을 고려합니다. SSL 정책 규칙, 보안 인텔리전스 규칙, 액세스 제어 규칙, 침입 정책, 파일 및 멀웨어 정책에서도 이벤트를 로깅할 수 있습니다. 현재 기록 중인 내용을 검토하여 구성한 모든 규칙 및 정책의 이벤트를 기록해야 하는지 여부를 검토합니다.

Security Analytics and Logging 라이선스가 만료되면 데이터는 어떻게 됩니까?

유료 Security Analytics and Logging 라이선스가 만료되면 방화벽에서 이벤트 수집이 즉시 중지됩니다. 그러나 기존 데이터는 180일간의 유예 기간 동안 Security Analytics and Logging 클라우드에서 계속 액세스 가능하며, 이 유예 기간 동안 유료 라이선스를 리뉴얼하면 서비스 중단 없이 계속 이용할 수 있습니다. 180일 이내에 라이선스를 리뉴얼하지 않으면 모든 데이터가 영구적으로 삭제됩니다.

보존 기간이 **1**년이고 기간이 **5**년인 **Security Analytics and Logging** 구독 구매한 경우, 내 데이터가 **5**년 동안 모두 저장됩니까?

보존 기간은 각 로그가 저장되는 기간을 정의합니다. 1년의 보존 기간으로 인해, 특정 시점에서는 가장 최근 1년간의 로그 데이터만 이용 가능합니다. 1년 이상 된 로그 데이터는 새로운 데이터가 수집됨에 따라 덮어쓰기되거나 삭제됩니다. 5년 기간이란 해당 기간 동안 데이터가 계속 수집되지만, 보존 기간 제한은 로그 데이터 자체에 적용됨을 의미합니다.

ASA에 대한 SAL SaaS(Security Analytics and Logging) 정보

Security Analytics and Logging(SaaS)를 사용하면 ASA에서 모든 시스템 로그 이벤트 및 NSEL(Netflow Secure Event Logging)을 캡처하여 Security Cloud Control에서 한 곳에서 볼 수 있습니다.

이벤트는 Cisco Cloud에 저장되며 Security Cloud Control의 Event Logging(이벤트 로깅) 페이지에서 볼 수 있습니다. 여기에서 이벤트를 필터링하고 검토하여 네트워크에서 어떤 보안 규칙이 트리거되고 있는지 명확하게 이해할 수 있습니다. **Logging and Troubleshooting(**기록 및 문제 해결**)** 패키지는 이러한 기능을 제공합니다.

시스템은 로깅 분석 및 탐지 패키지(이전 방화벽 분석 및 로깅 패키지)를 사용하여 FTD 이벤트에 Secure Cloud Analytics 동적 엔티티 모델링을 적용하고 행동 모델링 분석을 사용하여 Secure Cloud Analytics 관찰 및 알림을 생성할 수 있습니다. 전체 네트워크 분석 및 모니터링 패키지를 구입하는 경우 시스템은 FTD 이벤트와 네트워크 트래픽 모두에 동적 엔터티 모델링을 적용하고 관찰 및 알림을 생성합니다. Cisco SSO(Single Sign-On, 단일 인증)를 사용하여 Security Cloud Control에서 사용자에게 프로비저닝된 Secure Cloud Analytics 포털로 교차 실행할 수 있습니다.

라이선싱

이 솔루션을 구성하려면 다음 계정 및 라이선스가 필요합니다.

- **Security Cloud Control**: Security Cloud Control 테넌트가 있어야 합니다.

- **Secure Device Connector**: Secure Device Connector에 대한 별도의 라이선스는 없습니다.
- **Secure Event Connector**: Secure Event Connector에 대한 별도의 라이선스는 없습니다.
- **Secure Logging Analytics(SaaS)**: Security Analytics and Logging 라이선스, on page 31를 참조하십시오.
- **ASA(Adaptive Security Appliance)**: 기본 라이선스 이상입니다.

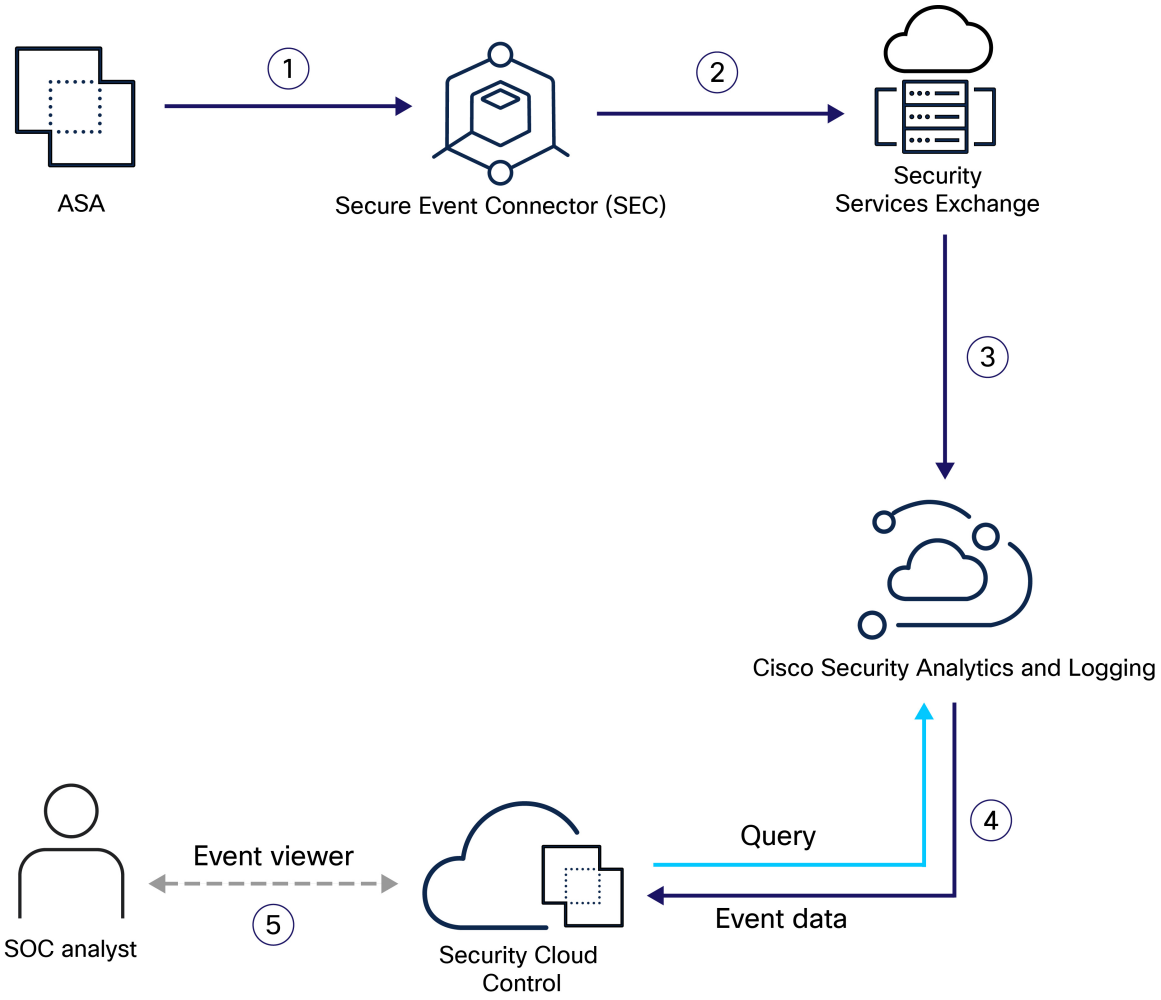
다음 단계

ASA 디바이스에 대한 SaaS(Secure Logging Analytics) 구현으로 이동

Security Cloud Control에서 ASA 이벤트 표시 방법

이 다이어그램은 ASA 디바이스가 Security Cloud Control와 시스템 시스템 로그 및 NSEL 이벤트를 공유하는 방법에 대해 설명합니다.

그림 *1: ASA* 이벤트가 *Security Cloud Control*에 표시되는 방법



단계	설명
1	시스템 로그 및 NSEL 이벤트를 Syslog 서버인 것처럼 Secure Event Connector 중 하나에 전달하고 디바이스에서 로깅을 활성화하도록 ASA를 구성합니다. ASA에서 로깅이 활성화되고 네트워크 트래픽이 액세스 제어 규칙 기준과 일치하면 syslog 이벤트 및 NSEL 이벤트가 생성됩니다. ASA 디바이스는 시스템 로그 및 NSEL 이벤트를 구성된 Secure Event Connector로 전달합니다.
2	Secure Event Connector는 이벤트를 보안 서비스 익스체인지로 전달합니다.
3	보안 서비스 익스체인지는 모든 ASA 디바이스의 이벤트 데이터를 집계하여 JSON 형식으로 변환한 다음 저장을 위해 Security Analytics and Logging으로 전송합니다.
4	Security Analytics and Logging는 다양한 서비스를 사용하여 이벤트 데이터를 처리하여 Security Cloud Control에서 사용할 수 있도록 분류 및 보강합니다.

단계	설명
5	Security Cloud Control는 이벤트 데이터를 클라우드 데이터 저장소에 저장합니다. Security Cloud Control는 저장된 데이터를 쿼리하여 SOC Analyst에게 관련 정보를 제공합니다.

ASA 디바이스에 대한 SaaS(Secure Logging Analytics) 구현

시작하기 전에

- ASA 디바이스용 SaaS(Secure Logging Analytics)를 검토하여 다음에 대해 알아보십시오.
  - Cisco Cloud로 이벤트를 전송하는 방법
  - 솔루션의 애플리케이션
  - 필요한 라이선스
  - 필요한 데이터 요금제
- Security Cloud Control 테넌트를 생성하기 위해 매니지드 서비스 제공자 또는 Security Cloud Control 영업 담당자에게 문의했습니다.
- Secure Device Connector를 검토합니다. SDC를 사용하여 Security Cloud Control를 ASA에 연결하는 것은 "모범 사례"로 간주되지만 필수 사항은 아닙니다.
- 네트워크에서 SDC를 구축하려는 경우 이 방법을 사용하여 설치할 수 있습니다.
  - Secure Device Connector 및 Secure Event Connector을 위한 VM 구축를 사용합니다.
- 테넌트에 대해 하나 이상의 SEC를 설치했으며 모든 ASA에서 테넌트에 온보딩된 SEC로 이벤트를 전송할 수 있습니다.

Cisco SaaS(Security Analytics and Logging)를 구현하고 보안 이벤트 커넥터를 통해 **Cisco Cloud**로 이벤트를 전송하는 워크플로우

1. 위의 "시작하기 전에"를 검토하여 환경이 올바르게 구성되었는지 확인하십시오.
2. 사용자 이름 및 비밀번호를 사용하는 Security Cloud Control에 ASA 디바이스 온보딩
3. ASA 시스템 로그 이벤트를 Cisco Cloud로 전송합니다.
4. Security Cloud Control 매크로를 사용하여 ASA 디바이스용 NSEL 구성
5. 이벤트가 Security Cloud Control에 표시되는지 확인합니다. 내비게이션 바에서 **Events & Logs(**이벤트 및 로그**)** > **Events(**이벤트**)** > **Event Logging(**이벤트 로깅**)**을 선택합니다. 라이브 이벤트를 보려면 **Live(**라이브**)** 탭을 클릭합니다.

6. **Firewall Analytics and Monitoring**(방화벽 분석 및 모니터링) 또는 **Total Network Analytics and Monitoring**(총 네트워크 분석 및 모니터링) 라이선스가 있는 경우 다음 섹션인 **Cisco Secure Cloud Analytics**를 사용하여 이벤트 분석을 계속 진행합니다.

Cisco Secure Cloud Analytics를 사용하여 이벤트 분석

Firewall Analytics and Monitoring(방화벽 분석 및 모니터링) 또는 **Total Network Analytics and Monitoring**(전체 네트워크 분석 및 모니터링) 라이선스가 있는 경우 이전 단계와 함께 다음을 수행합니다.

1. Cisco Secure Cloud Analytics 포털 프로비저닝.
2. **Total Network Analytics and Monitoring** 라이선스를 구매한 경우 하나 이상의 Secure Cloud Analytics 센서를 내부 네트워크에 구축합니다. 전체 네트워크 분석 및 보고를 위한 Cisco Secure Cloud Analytics 센서 구축의 내용을 참조하십시오.
3. Cisco SSO(Single Sign-On) 자격 증명에 연결된 Secure Cloud Analytics 사용자 어카운트를 생성하도록 사용자를 초대합니다. Security Cloud Control에서 Cisco Secure Cloud Analytics 알림 보기의 내용을 참조하십시오.
4. FTD 이벤트에서 생성된 Secure Cloud Analytics 알림을 모니터링하려면 Security Cloud Control에서 Secure Cloud Analytics로 교차 실행합니다. Security Cloud Control에서 Cisco Secure Cloud Analytics 알림 보기을 참조하십시오.

Security Cloud Control에서 교차 실행하여 **Cisco Secure Cloud Analytics** 알림 검토

Firewall Analytics and Monitoring(방화벽 분석 및 모니터링) 또는 **Total Network Analytics and Monitoring**(총 네트워크 분석 및 모니터링) 라이선스를 사용하면 Security Cloud Control에서 Secure Cloud Analytics로 교차 실행하여 FTD 이벤트에 의해 생성된 알림을 검토할 수 있습니다.

자세한 내용은 다음 문서를 참조하십시오.

-
- Security Cloud Control에서 Cisco Secure Cloud Analytics 알림 보기
- Secure Cloud Analytics 및 동적 엔티티 모델링
- Firepower Threat Defense 이벤트 기반 알림 작업

보안 이벤트 커넥터 문제 해결

다음 문제 해결 항목을 사용하여 다음에 대한 상태 및 로깅 정보를 수집합니다.

- 보안 이벤트 커넥터 온보딩 실패 문제 해결
- 문제 해결 로그 파일 이벤트 로깅
- 상태 확인을 사용하여 보안 이벤트 커넥터의 상태 학습

워크플로우

보안 및 분석 로깅 이벤트를 사용한 문제 해결에서는 Cisco Security Analytics 및 로깅에서 생성된 이벤트를 사용하여 사용자가 네트워크 리소스에 액세스할 수 없는 이유를 확인하는 방법을 설명합니다.

Firepower Threat Defense 이벤트 기반 알림 작업도 참조하십시오.

Security Cloud Control 매크로를 사용하여 Cisco Cloud로 ASA 시스템 로그 이벤트 전송

명령줄 인터페이스를 사용하여 ASA 시스템 로그 이벤트를 Cisco Cloud에 전송에 설명된 모든 명령을 사용하는 Security Cloud Control 매크로를 생성하고 동일한 배치의 모든 ASA에서 해당 매크로를 실행하여 Cisco Cloud에 이벤트를 전송하도록 모든 ASA를 구성할 수 있습니다.

Security Cloud Control의 매크로 툴을 사용하면 CLI 명령 목록을 어셈블하고, 명령 syntax(명령문)의 요소를 매개변수로 변환한 다음, 두 번 이상 사용 가능하게끔 명령 목록을 저장할 수 있습니다. 매크로는 한 번에 둘 이상의 디바이스에서 실행할 수도 있습니다.

검증된 매크로를 사용하면 디바이스 간의 구성 일관성이 향상되고, 명령줄 인터페이스를 사용할 때 발생할 수 있는 syntax(명령문) 오류가 방지됩니다.

자세한 내용을 읽기 전에, 매크로 사용 방법을 이해하기 위해 Security Cloud Control Firewall Management 구성 가이드에서 매크로 사용 메커니즘을 이해하시기 바랍니다. 이 문서에서는 최종 매크로 어셈블에 대해서만 설명합니다.

ASA SaaS(Security Analytics and Logging) 매크로 생성

다음 절차에서 볼 수 있는 서식에는 ASA CLI 명령과 매크로 형식의 두 가지 유형이 있습니다. ASA CLI 명령은 ASA 구문 규칙을 따르도록 작성되었습니다. Security Cloud Control에서 CLI 사용에 대한 자세한 내용은 명령줄 인터페이스 사용을 참조하십시오.

시작하기 전에 별도의 창에서 Send ASA Syslog Events to the Cisco Cloud(ASA Syslog 이벤트를 Cisco Cloud에 전송)를 열고 이 절차와 동시에 읽어보십시오. 그러면 매크로를 생성할 때 명령 설명을 읽을 수 있습니다.

Note 로깅 구성이 이미 ASA에 있는 경우 Security Cloud Control에서 매크로를 실행해도 기존 로깅 구성이 모두 지워지지는 않습니다. 대신, Security Cloud Control 매크로에 정의된 설정이 이미 있는 것과 병합됩니다.

Procedure

단계 **1** 일반 텍스트 편집기를 열고 아래의 지침 및 옵션에 따라 매크로로 변환할 명령 목록을 생성합니다. Security Cloud Control는 매크로에 작성된 순서대로 명령을 실행합니다. 일부 명령에는 매크로를 실행할 때 입력하는 {{parameters}} 값이 있습니다.

단계 **2** ASA가 Syslog 서버인 것처럼 **SEC**에 메시지를 보내도록 구성합니다**.**

메시지를 전송할 syslog 서버로 SEC를 지정하려면 **logging host** 명령을 사용합니다. 테넌트에 온보딩한 SEC 중 하나에 이벤트를 보낼 수 있습니다.

logging host 명령은 이벤트를 보낼 TCP 또는 UDP 포트를 지정합니다. 어떤 포트를 사용해야 하는지 확인하려면 Cisco Security Analytics 및 Logging에 사용되는 디바이스의 TCP, UDP 및 NSEL 포트 찾기를 참조하십시오.

logging host*interface_nameSEC_IP_address* { **tcp/port** | **udp/port** }

시스템 로그 이벤트를 SEC로 전송하는 데 사용하는 프로토콜에 따라 이 명령을 두 개의 서로 다른 매크로 중 하나로 설정합니다.

logging host {{interface_name}} {{SEC_ip_address}} tcp/{{port_number}}

logging host {{interface_name}} {{SEC_ip_address}} udp/{{port)_number}}

(선택 사항) TCP를 사용하는 경우 매크로의 명령 목록에 이 명령을 추가할 수 있습니다. 매개변수가 필요하지 않습니다.

logging permit-hostdown

단계 **3** 어떤 **syslog** 메시지를 **syslog** 서버에 전송할지 지정합니다**.**

logging trap 명령을 사용하여 syslog 서버로 보내야 하는 syslog 메시지를 지정합니다.

logging trap { *severity_level* | *message_list* }

심각도 수준별로 SEC로 전송되는 이벤트를 정의하려면 명령을 다음 매크로로 전환합니다.

logging trap {{severity_level}}

메시지 목록의 일부인 SEC에 이벤트만 보내려면 명령을 다음 매크로로 변환합니다.

logging trap {{message_list_name}}

이전 단계에서 **logging trap message_list** 명령을 선택한 경우 메시지 목록에서 syslog를 정의해야 합니다. 매크로를 생성할 때 명령 설명을 읽을 수 있도록 Create a Custom Event List(맞춤형 이벤트 목록 생성)를 엽니다. 다음 명령으로 시작합니다.

logging list*name* { **level***level* [**class***message_class*] | **message***start_id* [*-end_id*] }

이를 다음과 같이 분류합니다.

logging list {{message_list_name}} level {{security_level}}

logging list {{message_list_name}} level {{security_level}} class {{message_class}}

logging list {{message_list_name}} message {{syslog_range_or_number}}

마지막 변형에서는 메시지 파라미터 {{syslog_range_or_number}}를 단일 syslog ID(106023) 또는 범위(302013-302018)로 입력할 수 있습니다. 메시지 목록을 만들려면 원하는 만큼의 줄에서 하나 이상의 명령 변형을 사용합니다. 단일 매크로에서 동일한 이름의 모든 매개변수는 사용자가 입력한 것과 동일한 값을 사용한다는 점에 유의하십시오. Security Cloud Control는 빈 매개변수가 있는 매크로를 실행하지 않습니다.

Important
logging list 명령은 매크로에서 **logging trap** 명령 앞에 와야 합니다. 먼저 목록을 정의하면 **logging trap** 명령에서 사용할 수 있습니다. 아래의 샘플 매크로를 참조하십시오.

단계 **4** (선택 사항) syslog 타임스탬프를 추가합니다**.** ASA에서 발생한 시스템 로그 메시지에 날짜와 시간을 추가하려면 이 명령을 추가합니다. 타임스탬프 값은 **SyslogTimestamp** 필드에 표시됩니다. 이 명령을 명령 목록에 추가합니다. 매개변수는 필요하지 않습니다.

logging timestamp

Note
버전 9.10(1)부터 ASA는 이벤트 시스템 로그에서 RFC 5424에 따라 타임스탬프를 활성화하는 옵션을 제공합니다. 이 옵션을 활성화하면 syslog 메시지의 모든 타임스탬프가 RFC 5424 형식에 따라 시간을 표시합니다. 다음은 RFC 5424 형식의 샘플 출력입니다.

```
 <166>2018-06-27T12:17:46Z asa : %ASA-6-110002: Failed to locate egress interface for protocol from
src interface :src IP/src port to dest IP/dest port
```

.

단계 **5** (선택 사항) EMBLEM 형식이 아닌 syslog 메시지에 디바이스 **ID**를 포함합니다**.** 매크로를 생성할 때 명령 설명을 읽을 수 있도록 Include the Device ID in Non-EMBLEM Format Syslog Messages(EMBLEM 형식이 아닌 Syslog 메시지에 디바이스 ID 포함)를 엽니다. 이는 매크로의 기반이 되는 CLI 명령입니다.

logging device-id {**cluster-id** | **context-name** | **hostname** | **ipaddress** *interface_name* [**system**] | **string***text*}

이를 다음과 같이 분류합니다.

logging device-id cluster-id

logging device-id context-name

logging device-id hostname

logging device-id ipaddress {{interface_name}} **system**

logging device-id string {{text_16_char_or_less}}

단계 **6** 로깅을 활성화합니다**.** 이 명령을 그대로 매크로에 추가합니다. 매개변수가 없습니다.

logging enable

단계 **7** 매크로의 마지막 줄에 쓰기 **write memory**를 추가하지 마십시오**.** 대신 **show running-config logging** 명령을 추가하여 ASA의 시작 구성에 커밋하기 전에 입력한 로깅 명령의 결과를 검토합니다.

show running-config logging

단계 **8** 구성이 변경되었다고 확신하는 경우 **write memory** 명령에 대한 별도의 매크로를 생성하거나 Security Cloud Control의 대량 명령줄 인터페이스 툴을 사용하여 매크로를 사용하여 구성한 모든 디바이스에 명령을 실행할 수 있습니다.

write memory

단계 **9** (선택 사항) 액세스 제어 규칙 "permit" 이벤트에 대한 로깅을 활성화합니다. 이 단계는 ASA Syslog 이벤트를 Cisco Cloud로 전송 절차에 설명되어 있지만 이 매크로에는 포함되어 있지 않습니다. 대신 Security Cloud Control GUI에서 수행됩니다.

단계 **10** 매크로를 저장합니다.

Example

다음은 단일 매크로로 결합된 명령 목록의 샘플입니다.

```
logging host {{interface_name}} {{SEC_ip_address}} {{tcp_or_udp}}/{{port_number}}
logging permit-hostdown
logging list {{message_list_name}} level {{security_level}}
logging list {{message_list_name}} message {{syslog_range_or_number_1}}
logging list {{message_list_name}} message {{syslog_range_or_number_2}}
logging trap {{message_list_name}}
logging device-id cluster-id
logging enable
show running-config logging
```

Note 서로 다른 특정 syslog ID 또는 범위를 추가하는 몇 가지 logging list 명령이 있습니다. {{syslog_range_or_number_X}} 매개변수에는 숫자 또는 기타 구분자가 필요합니다. 그렇지 않으면 매크로가 채워질 때 값이 모두 동일하게 됩니다. 또한 모든 매개변수에 값이 지정되지 않은 경우 Security Cloud Control는 매크로를 실행하지 않으므로 실행하려는 명령만 매크로에 포함해야 한다는 점에 유의하십시오. 모든 syslog ID가 동일한 목록에 포함되므로 event_list_name이 각 줄에서 동일하게 유지됩니다.

What to do next

매크로 실행

ASA Security Analytics and Logging Macro(보안 분석 및 로깅 매크로)를 생성하고 저장한 후 매크로를 실행하여 ASA 시스템 로그 이벤트를 Cisco Cloud로 전송합니다.

명령줄 인터페이스를 사용하여 Cisco Cloud에 ASA 시스템 로그 이벤트 전송

이 절차에서는 ASA 시스템 로그 이벤트를 SEC(Secure Event Connector)에 전달한 다음 로깅을 활성화하는 방법을 설명합니다. 이러한 절차에서는 해당 워크플로우를 완료하는 데 필요한 사항만 설명합니다. ASA에서 로깅을 구성할 수 있는 모든 방법에 대한 자세한 내용은 ASDM1: Cisco ASA 시리즈 일반 운영 ASDM 구성 가이드 또는 CLI 1권: Cisco ASA 시리즈 일반 운영 CLI 구성 가이드의 모니터링 장을 참조하십시오.

지원되는 **ASA** 명령에 대한 제한 사항

Security Cloud Control는 아직 다음 Syslog 명령 또는 메시지 형식을 지원하지 않습니다.

- Syslog의 EMBLEM 형식
- 보안 Syslog

ASA용 Security Cloud Control 명령줄 인터페이스

이 절차의 모든 작업은 ASA용 Security Cloud Control의 명령줄 인터페이스에서 진행하게 됩니다. 명령줄 인터페이스 페이지를 열려면 다음을 수행합니다.

Procedure

단계 **1** 왼쪽 탐색 모음에서 **Security Devices(**보안 디바이스**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **3** 적절한 디바이스 유형 탭을 클릭하고 로깅을 활성화할 ASA를 선택합니다.

단계 **4** 오른쪽의 Device Actions(디바이스 작업) 창에서 **>_Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다.

단계 **5** **Command Line Interface(**명령줄 인터페이스**)** 탭을 클릭합니다. 이제 프롬프트에서 아래에 설명된 명령을 입력할 준비가 되었습니다.

모든 명령을 입력한 후 **Send(**전송**)**를 클릭합니다. Security Cloud Control의 CLI 인터페이스는 ASA에 직접 연결되므로 명령은 디바이스의 실행 중인 구성에 즉시 기록됩니다. ASA의 시작 구성에 변경 사항을 기록하려면 `write memory` 명령을 추가로 실행해야 합니다.

보안 이벤트 커넥터에 ASA Syslog 이벤트 전달

ASA 시스템 로그 이벤트를 온보딩한 SEC(Secure Event Connector) 중 하나로 전달한 다음 로깅을 활성화하려면 다음 절차에서 작업을 완료해야 합니다.

Procedure

단계 **1** ASA가 Syslog 서버인 것처럼 SEC에 메시지를 보내도록 구성합니다.

단계 **2** SEC에 전송할 모든 로그의 심각도 레벨 또는 시스템 로그 이벤트 목록을 결정합니다.

단계 **3** 로깅을 활성화합니다.

단계 **4** 변경 사항을 ASA의 시작 구성에 저장합니다.

CLI를 사용하여 ASA 시스템 로그 이벤트를 Cisco 클라우드로 전송

Procedure

단계 **1** ASA가 **Syslog** 서버인 것처럼 **SEC**에 메시지를 보내도록 구성합니다**.**

ASA에서 Cisco Cloud로 시스템 로그 이벤트를 전송할 때 외부 Syslog 서버인 것처럼 SEC로 전달하면 SEC에서 Cisco Cloud로 메시지를 전달합니다.

syslog 메시지를 SEC에 보내려면 다음 단계를 수행합니다.

a. TCP 또는 UDP를 사용하여 ASA가 Syslog 서버인 것처럼 SEC에 메시지를 전송하도록 ASA를 구성합니다. SEC는 IPv4 또는 IPv6 주소를 사용할 수 있습니다. TCP 또는 UDP 포트로 이벤트를 전송합니다. 어떤 포트를 사용해야 하는지 확인하려면 Cisco Security Analytics 및 Logging에 사용되는 디바이스의 TCP, UDP 및 NSEL 포트 찾기를 참조하십시오.

다음은 **logging host** 명령 구문의 예입니다.

logging host *interface_name SEC_IP_address* [[**tcp/port**] | [**udp/port**]]

예:

```
 > logging host mgmt 192.168.1.5 tcp/10125
> logging host mgmt 192.168.1.5 udp/10025
> logging host mgmt 2002::1:1 tcp/10125
> logging host mgmt 2002::1:1 udp/10025
```

- **interface_name** 인수는 메시지가 Syslog 서버로 전송되는 ASA 인터페이스를 지정합니다. SDC와의 통신에 이미 사용 중인 동일한 ASA 인터페이스를 통해 SDC에 시스템 로그 메시지를 보내는 것이 "모범 사례"입니다.
- **SEC_IP_address** 인수는 SEC가 설치된 VM의 IP 주소를 포함해야 합니다.
- **tcp/port** 또는 **udp/port** 키워드-인수 쌍은 시스템 로그 메시지가 TCP 프로토콜 및 관련 포트 또는 UDP 프로토콜 및 관련 포트를 사용하여 전송되도록 지정합니다. UDP 또는 TCP를 사용하여 syslog 서버에 데이터를 전송하도록 ASA를 구성할 수 있지만 둘 다 사용할 수는 없습니다. 프로토콜을 지정하지 않으면 기본 프로토콜은 UDP입니다.

  TCP를 지정한 경우 ASA는 Syslog 서버의 장애를 감지하고 보호 조치로서 ASA를 통한 새로운 연결을 차단합니다. TCP syslog 서버에 대한 연결에 관계없이 새 연결을 허용하려면 b 단계를 참조하십시오. UDP를 지정한 경우 ASA는 Syslog 서버의 작동 여부에 관계없이 새 연결을 계속 허용합니다. 유효한 값

  Note
  두 개의 개별 syslog 서버로 ASA 메시지를 전송하려는 경우, 다른 syslog 서버의 적절한 인터페이스, IP 주소, 프로토콜 및 포트를 사용하여 두 번째 logging host 명령을 실행할 수 있습니다.

b. (선택 사항) TCP를 통해 이벤트를 SEC로 전송하는 경우 SEC가 중단되었거나 ASA의 로그 대기열이 꽉 차면 새 연결이 차단됩니다. syslog 서버가 백업되고 로그 대기열이 비워지면 새로운 연결이 다시 허용됩니다. TCP Syslog 서버에 대한 연결에 관계없이 새 연결을 허용하려면 이 명령을 사용하여 TCP 연결 Syslog 서버가 다운될 때 새 연결을 차단하는 기능을 비활성화합니다.

logging permit-hostdown

예:

```
> logging permit-hostdown
```

단계 **2** 다음 명령으로 어떤 시스템 로그 메시지를 **Syslog** 서버에 전송할지 지정합니다**.**

logging trap { severity_level | message_list }

예:

```
> logging trap 3
> logging trap asa_syslogs_to_cloud
```

심각도 레벨 숫자(1~7) 또는 이름을 지정할 수 있습니다. 예를 들어 심각도를 3으로 설정한 경우 ASA는 심각도 레벨 3, 2, 1에 대해 syslog 메시지를 보냅니다.

message_list 인수는 사용자 지정 이벤트 목록을 생성한 경우 해당 목록의 이름으로 교체됩니다. 사용자 지정 이벤트 목록을 지정할 때는 해당 목록에 있는 시스템 로그 메시지만 보안 이벤트 커넥터로 전송합니다. 위의 예에서 asa_syslogs_to_cloud는 이벤트 목록의 이름입니다.

message_list를 사용하면 Cisco Cloud로 전송되는 syslog 메시지를 엄격하게 정의하여 비용을 절약할 수 있습니다.

message_list를 생성하려면 Create a Custom Event List(맞춤형 이벤트 목록 생성)를 참조하십시오. 데이터 수집 및 스토리지 비용에 대한 자세한 내용은 Security Analytics and Logging 라이선스, on page 31를 참조하십시오.

단계 **3** **(**선택 사항**) syslog** 타임스탬프 추가

logging timestamp 명령을 사용하여 syslog 메시지가 ASA에서 생성된 날짜 및 시간을 메시지에 추가합니다. 타임스탬프 값은 **SyslogTimestamp** 필드에 표시됩니다.

예:

```
> logging timestamp
```

Note
버전 9.10(1)부터 ASA는 이벤트 시스템 로그에서 RFC 5424에 따라 타임스탬프를 활성화하는 옵션을 제공합니다. 이 옵션을 활성화하면 syslog 메시지의 모든 타임스탬프가 RFC 5424 형식에 따라 시간을 표시합니다. 다음은 RFC 5424 형식의 샘플 출력입니다.

```
<166>2018-06-27T12:17:46Z asa : %ASA-6-110002: Failed to locate egress interface for protocol from src
interface :src IP/src port to dest IP/dest port.
```

단계 **4** **(**선택 사항**) EMBLEM** 형식이 아닌 **syslog** 메시지에 디바이스 **ID** 포함

디바이스 ID는 특정 ASA에서 전송된 모든 syslog 메시지를 쉽게 구분하는 데 도움이 되는 syslog 메시지에 삽입할 수 있는 ID입니다. 지침은 Non-EMBLEM 형식 Syslog 메시지에 디바이스 ID 포함을 참조하십시오.

단계 **5** **(**선택 사항**)** 액세스 제어 규칙 **"permit"** 이벤트에 대한 로깅 활성화

액세스 제어 규칙이 리소스에 대한 액세스를 거부하면 이벤트가 자동으로 로깅됩니다. 액세스 제어 규칙이 리소스에 대한 액세스를 허용할 때 생성되는 이벤트도 로깅하려면, 액세스 제어 규칙에 대한 로깅을 켜고 심각도 유형을 구성해야 합니다. 개별 네트워크 액세스 제어 규칙에 대한 로깅을 설정하는 방법에 대한 지침은 Log Rule Activity(규칙 활동 로깅)를 참조하십시오.

Note

액세스 제어 규칙 "permit" 이벤트에 대한 로깅을 활성화하면 일일 이벤트 수집 속도를 기반으로 하므로 구매한 데이터 플랜을 더 많이 사용하게 됩니다.

단계 **6** 로깅 활성화

명령 프롬프트에서 logging enable을 입력합니다. ASA에서 로깅은 개별 규칙이 아니라 전체 디바이스에 대해 활성화됩니다.

예:

```
> logging enable
```

Note
현재 Security Cloud Control는 보안 로깅 활성화를 지원하지 않습니다.

단계 **7** 시작 구성에 변경 사항 저장

명령 프롬프트에서 write memory를 입력합니다. ASA에서 로깅은 개별 규칙이 아니라 전체 디바이스에 대해 활성화됩니다.

예:

```
> write memory
```

관련 정보**:**

- SDC 가상 머신에 SEC(Secure Event Connector) 설치, on page 2
- 테넌트에 대한 두 번째 또는 후속 SEC 설치

사용자 지정 이벤트 목록 생성

다음 방법 중 하나를 사용하여 Cisco Cloud에 ASA 시스템 로그 이벤트를 전송할 때 맞춤형 이벤트 목록을 생성합니다.

- 명령줄 인터페이스를 사용하여 Cisco Cloud에 ASA 시스템 로그 이벤트 전송
- Security Cloud Control 매크로를 사용하여 Cisco Cloud로 ASA 시스템 로그 이벤트 전송

다음 세 가지 기준에 따라 message_list라고도 하는 이벤트 목록을 생성할 수 있습니다.

- 이벤트 클래스
- 심각도
- 메시지 ID

특정 로깅 대상(예: syslog 서버 또는 Secure Event Connector)으로 보낼 사용자 지정 이벤트 목록을 생성하려면 다음 단계를 수행하십시오.

Procedure

단계 **1** 왼쪽 탐색 모음에서 **Security Devices(**보안 디바이스**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **3** 해당 탭을 클릭하고 맞춤형 이벤트 목록에 포함할 시스템 로그 메시지가 있는 ASA를 선택합니다.

단계 **4** **Device Actions(**디바이스 작업**)** 창에서 **>_Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다.

단계 **5** ASA에 **logging list** 명령을 실행하려면 이 명령 구문을 사용합니다.

logging list *name* { **level** *level* [**class** *message_class*] | **message** *start_id* [*-end_id*] }

name 인수는 목록의 이름을 지정합니다. **level** *level* 키워드 및 인수 쌍은 심각도 레벨을 지정합니다. **class** *message_class* 키워드-인수 쌍은 특정 메시지 클래스를 지정합니다. **message** *start_id* [*-end_id*] 키워드-인수 쌍은 개별 시스템 로그 메시지 숫자 또는 숫자 범위를 지정합니다.

Note
심각도 레벨 이름을 syslog 메시지 목록의 이름으로 사용하지 마십시오. 금지된 이름에는 긴급, 경고, 중요 , 오류, 알림, 정보 및 디버깅이 포함됩니다. 마찬가지로 이벤트 목록 이름의 맨 앞에 이러한 단어의 처음 3개 글자를 사용하지 마십시오. 예를 들어 "err"로 시작하는 이벤트 목록 이름을 사용하지 마십시오.

- 심각도에 따라 이벤트 목록에 **syslog** 메시지를 추가합니다**.** 예를 들어 심각도를 3으로 설정한 경우 ASA는 심각도 레벨 3, 2, 1에 대해 syslog 메시지를 보냅니다.

  예:

  ```
  > logging list asa_syslogs_to_cloud level 3
  ```

- 다른 기준에 따라 시스템 로그 메시지를 이벤트 목록에 추가합니다**.**

  이전 단계와 동일한 명령을 입력하여 기존 메시지 목록의 이름과 추가 기준을 지정합니다. 목록에 추가할 각 기준에 대한 새로운 명령을 입력합니다. 예를 들어 다음과 같이 목록에 포함할 syslog 메시지에 대한 기준을 지정할 수 있습니다.

  - 302013~302018 범위에 해당하는 시스템 로그 메시지 ID.
  - 심각도 레벨이 중요 이상인 모든 syslog 메시지(긴급, 경고 또는 중요).
  - 심각도 레벨이 경고 이상인 모든 HA 클래스 시스템 로그 메시지(긴급, 알림, 심각, 오류 또는 경고).

    예:

    ```
    > logging list asa_syslogs_to_cloud message 302013-302018
    > logging list asa_syslogs_to_cloud level critical
    > logging list asa_syslogs_to_cloud level warning class ha
    ```

    Note
    다음 조건을 하나라도 충족하면 syslog 메시지가 로깅됩니다. syslog 메시지가 조건을 둘 이상 충족하는 경우 메시지는 한 번만 로깅됩니다.

단계 **6** 시작 구성에 변경 사항 저장

명령 프롬프트에서 **write memory**를 입력합니다.

예:

```
> write memory
```

디바이스 ID를 EMBLEM 이외 형식 Syslog 메시지에 포함

EMBLEM 형식이 아닌 시스템 로그 메시지에 디바이스 ID를 포함하도록 ASA를 구성할 수 있습니다. syslog 메시지에 대해 1가지 디바이스 ID 유형만 지정할 수 있습니다. 다음 절차에서 이 절차를 참조하십시오.

- 명령줄 인터페이스를 사용하여 Cisco Cloud에 ASA 시스템 로그 이벤트 전송
- Security Cloud Control 매크로를 사용하여 Cisco Cloud로 ASA 시스템 로그 이벤트 전송

이 디바이스 식별자는 Event Logging(이벤트 로깅) 페이지에 표시되는 시스템 로그 이벤트의 SensorID 필드에 반영됩니다.

Procedure

단계 **1** 디바이스 ID를 할당하려는 시스템 로그 메시지가 있는 ASA를 선택합니다.

단계 **2** Device Actions(디바이스 작업) 창에서 **>_Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다.

단계 **3** 디바이스에 **logging device-id** 명령을 실행하려면 이 명령 syntax(명령문)를 사용합니다.

logging device-id { **cluster-id** | **context-name** | **hostname** | **ipaddress***interface_name* [**system**] | **string***text* }

예:

```
> logging device-id hostname
> logging device-id context-name
> logging device-id string Cambridge
```

context-name 키워드는 현재 컨텍스트의 이름을 디바이스 ID로 사용하도록 지정합니다(다중 컨텍스트 모드에만 적용). 다중 컨텍스트 모드에서 관리자 컨텍스트 모드를 위해 디바이스 ID 로깅을 활성화하는 경우 시스템 실행 공간에서 발생하는 메시지는 시스템의 디바이스 ID를 사용하고 관리자 컨텍스트에서 발생하는 메시지는 관리자 컨텍스트의 이름을 디바이스 ID로 사용합니다.

Note
ASA 클러스터에서는 항상 선택된 인터페이스에 대해 기본 유닛 IP 주소를 사용합니다.

cluster-id 키워드는 클러스터에서 개별 ASA 유닛의 부트 구성 고유 이름을 디바이스 ID로 지정합니다.

hostname 키워드는 ASA의 호스트 이름을 디바이스 ID로 사용하도록 지정합니다.

ipaddress *interface_name* 키워드-인수 쌍은 *interface_name*으로 지정된 인터페이스 IP 주소를 디바이스 ID로 사용하도록 지정합니다. **ipaddress** 키워드를 사용하는 경우 시스템 로그 메시지가 전송되는 인터페이스에 관계없이 디바이스 ID가 지정된 ASA 인터페이스 IP 주소가 됩니다. 클러스터 환경에서 **system** 키워드는 디바이스 ID가 인터페이스의 시스템 IP 주소가 되도록 만듭니다. 이 키워드는 디바이스에서 전송되는 모든 syslog 메시지에 대해 하나의 일관된 디바이스 ID를 제공합니다.

string *text* 키워드-인수 쌍은 문자열이 디바이스 ID로 사용되도록 지정합니다. 문자열은 최대 16자를 포함할 수 있습니다.

공백 또는 다음 문자를 사용할 수 없습니다.

- &(앰퍼샌드)
- `(작은따옴표)
- "(큰따옴표)
- <(보다 작음)
- >(보다 큼)
- ? (물음표)

단계 **4** 시작 구성에 변경 사항 저장

명령 프롬프트에서 **write memory**를 입력합니다.

예:

```
> write memory
```

ASA 디바이스용 NSEL(Network Security Event Logging)

ASA의 기본 시스템 로그 메시지에는 ASA에서 보고한 이벤트가 위협을 나타내는지 여부를 Secure Cloud Analytics에서 판단하는 데 필요한 데이터가 많이 부족합니다. NSEL(Netflow Secure Event Logging)은 해당 데이터와 함께 Secure Cloud Analytics를 제공합니다.

"플로우는 네트워크 디바이스를 통과하는 몇 가지 공통 속성이 있는 패킷의 단방향 시퀀스로 정의됩니다. 이렇게 수집된 플로우는 외부 디바이스인 NetFlow 컬렉터로 내보내집니다. 네트워크 플로우는 매우 세분화됩니다. 예를 들어 플로우 레코드에는 IP 주소, 패킷 및 바이트 수, 타임스탬프, ToS(서비스 유형), 애플리케이션 포트, 입력 및 출력 인터페이스 등의 세부 정보가 포함됩니다."[1]

Cisco ASA는 NetFlow 버전 9 서비스를 지원합니다. NSEL의 ASA 구현은 플로우에서 중요한 이벤트를 나타내는 레코드만 내보내는 스테이트풀 IP 플로우 추적 방법을 제공합니다. 스테이트풀 플로우 추적에서 추적된 플로우는 일련의 상태 변경을 거칩니다.

이 문서에서는 Security Cloud Control 매크로를 사용하여 ASA에 대해 NetFlow를 구성하는 간단한 방법을 설명합니다. Cisco ASA NetFlow 구현 가이드는 ASA에서 NetFlow를 구성하는 방법에 대한 매우 자세한 설명을 제공하며, 이 콘텐츠와 함께 유용한 리소스를 찾을 수 있습니다.

다음 작업

Security Cloud Control 매크로를 사용하여 ASA 디바이스용 NSEL 구성으로 이동합니다.

관련 문서

- Security Cloud Control 매크로를 사용하여 ASA 디바이스용 NSEL 구성

- ASA에서 NSEL(NetFlow Secure Event Logging) 구성 삭제
- ASA 전역 정책의 이름 확인

1. ("Cisco Systems NetFlow 서비스 내보내기 버전 9." 인터넷 엔지니어링 태스크 포스, 네트워크 워킹 그룹, 코멘트 요청: 3954, 2004년 10월, B. Claise, Ed. https://www.ietf.org/rfc/rfc3954.txt)

Security Cloud Control 매크로를 사용하여 ASA 디바이스용 NSEL 구성

ASA는 NSEL(NetFlow Secure Event Logging)을 사용하여 세부 연결 이벤트 데이터를 보고합니다. 양방향 플로우 통계를 포함하는 Secure Cloud Analytics를 이 연결 이벤트 데이터에 적용할 수 있습니다. 이 절차에서는 ASA 디바이스에서 NSEL을 구성하고 이러한 NSEL 이벤트를 플로우 컬렉터로 전송하는 방법을 설명합니다. 이 경우 플로우 컬렉터는 SEC(Secure Event Connector)입니다.

이 절차는 **NSEL** 구성 매크로를 참조하십시오.

```
 flow-export destination {{interface}} {{SEC_IPv4_address}} {{SEC_NetFlow_port}}
flow-export template timeout-rate {{timeout_rate_in_mins}}
flow-export delay flow-create {{delay_flow_create_rate_in_secs}}
flow-export active refresh-interval {{refresh_interval_in_mins}}
class-map {{flow_export_class_name}}
     match {{add_this_traffic_to_class_map}}
policy-map {{global_policy_map_name}}
     class {{flow_export_class_name}}
          flow-export event-type {{event_type}} destination {{SEC_IPv4_address}}
service-policy {{global_policy_map_name}} global
logging flow-export-syslogs disable
show run flow-export
show run policy-map {{global_policy_map_name}}
show run class-map {{flow_export_class_name}}
```

다음은 모든 기본값, 클래스 맵의 일반 이름 및 global_policy에 추가된 클래스 맵이 포함된 Configure NSEL 매크로의 예입니다. 이러한 절차를 완료하면 매크로는 다음과 유사합니다.

```
 flow-export destination {{interface}} {{SEC_IPv4_address}} {{SEC_NetFlow_port}}
flow-export template timeout-rate 60
flow-export delay flow-create 55
flow-export active refresh-interval 1
class-map flow_export_class_map
     match any
policy-map global_policy
     class flow_export_class_map
          flow-export event-type all destination {{SEC_IPv4_address}}
logging flow-export-syslogs disable
show run flow-export
show run policy-map global_policy
show run class-map flow_export_class_map
```

시작하기 전에

다음 정보를 수집합니다.

- 이전에 Security Cloud Control 매크로로 작업한 적이 없는 경우 Security Cloud Control Firewall Management 구성 가이드에서 매크로에 대해 읽어보십시오.
- ASA에서 데이터를 수신할 SEC의 IPv4 주소

- SEC에 데이터를 보낼 asa의 인터페이스
- NetFlow 이벤트 전송에 사용되는 UDP 포트 번호 SaaS(Secure Logging Analytics)에 사용되는 디바이스의 TCP, UDP 및 NSEL 포트 찾기, on page 23의 내용을 참조하십시오.
- ASA 전역 정책의 이름 확인, on page 61

워크플로우

이 워크플로우에 따라 Security Cloud Control 매크로를 사용하여 ASA 디바이스에 대한 NSEL을 구성합니다. 각 단계를 수행해야 합니다.

1. NSEL 매크로 구성 열기 , on page 54.
2. NSEL 메시지의 대상 및 SEC로 전송되는 간격 정의, on page 55.
3. SEC로 전송될 NSEL 이벤트를 정의하는 클래스 맵 생성, on page 56.
4. NSEL 이벤트에 대한 정책 맵 정의, on page 57.
5. 중복된 시스템 로그 메시지 비활성화, on page 57.
6. 매크로 검토 및 전송, on page 59.

다음 작업

NSEL 매크로 구성 열기 , on page 54로 이동하여 위의 워크플로를 시작합니다.

NSEL 매크로 구성 열기

Before you begin

이는 더 긴 워크플로의 첫 번째 부분입니다. 시작하기 전에 Security Cloud Control 매크로를 사용하여 ASA 디바이스용 NSEL 구성, on page 53의 내용을 참조하십시오.

Procedure

단계 **1** **Security Devices(**보안 디바이스 **)** 페이지에서 **Devices(**디바이스**)** 탭을 클릭합니다.
단계 **2** 적절한 디바이스 유형 탭을 클릭하고 NSEL(NetFlow Secure Event Logging)을 구성할 ASA를 선택합니다.
단계 **3** **Device Actions(**디바이스 작업**)** 창에서 **Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다.
단계 **4** Macro(매크로) 별   을 클릭하여 사용 가능한 매크로 목록을 표시합니다.
단계 **5** 매크로 목록에서 **Configuring NSEL(NSEL** 구성**)**을 선택합니다.
단계 **6** Macro(매크로) 상자에서 **View Parameters(**매개변수 보기**)**를 클릭합니다.

What to do next

NSEL 메시지의 대상 및 SEC로 전송되는 간격 정의, on page 55를 진행합니다.

NSEL 메시지의 대상 및 SEC로 전송되는 간격 정의

NSEL 메시지는 테넌트에 온보딩한 SEC 중 하나로 전송할 수 있습니다. 이 지침은 매크로의 이 섹션을 참조하십시오.

flow-export destination {{interface}} {{SEC_IPv4_address}} {{SEC_NetFlow_port}}

flow-export template timeout-rate {{timeout_rate_in_mins}}

flow-export delay flow-create {{delay_flow_create_rate_in_secs}}

flow-export active refresh-interval {{refresh_interval_in_mins}}

Before you begin

이는 더 큰 워크플로우의 일부입니다. 시작하기 전에 Security Cloud Control 매크로를 사용하여 ASA 디바이스용 NSEL 구성, on page 53의 내용을 참조하십시오.

Procedure

단계 **1** **flow-export destination** 명령은 NetFlow 패킷이 전송되는 컬렉터를 정의합니다. 이 경우 SEC로 전송됩니다. 다음 매개변수에 대한 필드를 입력합니다.

- **{{interface}}** - NetFlow 이벤트가 전송되는 ASA의 인터페이스 이름을 입력합니다.
- **{{SEC_IPv4_address}}** - SEC의 IPv4 주소를 입력합니다. SEC는 플로우 컬렉터 역할을 합니다.
- **{{SEC_NetFlow_port}}** - NetFlow 패킷이 전송되는 SEC의 UDP 포트 번호를 입력합니다.

단계 **2** **flow-export template timeout-rate** 명령은 템플릿 레코드가 구성된 모든 출력 대상으로 전송되는 간격을 지정합니다.

- **{{timeout_rate_in_mins}}** - 템플릿을 재전송할 때까지의 시간(분)을 입력합니다. **60**분 값을 사용하는 것이 좋습니다. SEC는 템플릿을 처리하지 않습니다. 숫자가 크면 SEC에 대한 트래픽이 줄어듭니다.

단계 **3** **flow-export delay flow-create** 명령은 flow-create 이벤트의 전송을 지정된 시간(초)만큼 지연시킵니다. 이 값은 권장 Active Timeout(활성 시간 초과) 값과 일치하며 ASA에서 내보낸 플로우 이벤트 수를 줄입니다. 이 속도에서 NSEL 이벤트는 연결 종료 시 또는 연결 생성 후 55초 중 더 빠른 시점에 Security Cloud Control에 처음 표시됩니다. 이 명령이 구성되지 않은 경우 지연이 없으며 플로우가 생성되는 즉시 flow-create 이벤트가 내보내집니다.

- **{{delay_flow_create_rate_in_secs}}** - 플로우 생성 이벤트 전송 간의 지연 시간(초)을 입력합니다. **55**초 값을 사용하는 것이 좋습니다.

단계 **4** **flow-export active refresh-interval** 명령은 수명이 긴 플로우에 대한 상태 업데이트가 ASA에서 전송되는 빈도를 정의합니다. 유효한 값은 1분~60분입니다. Flow Update Interval(플로우 업데이트 간격) 필드에서 **flow-export active refresh-interval**을 **flow-export delay flow-create** 간격보다 5초 이상 크게 구성하면 flow-update 이벤트가 flow-creation 이벤트보다 먼저 표시되지 않습니다.

- **{{refresh_interval_in_mins}}-1**분 값을 사용하는 것이 좋습니다. 유효한 값은 1분~60분입니다.

What to do next

SEC로 전송될 NSEL 이벤트를 정의하는 클래스 맵 생성, on page 56를 진행합니다.

SEC로 전송될 NSEL 이벤트를 정의하는 클래스 맵 생성

매크로의 다음 명령은 클래스의 모든 NSEL 이벤트를 그룹화한 다음 해당 클래스를 SEC(Secure Event Connector)로 내보냅니다. 이 지침은 매크로의 이 섹션을 참조하십시오.

class-map {{flow_export_class_name}}

match {{add_this_traffic_to_class_map}}

Before you begin

이는 더 큰 워크플로우의 일부입니다. 시작하기 전에 Security Cloud Control 매크로를 사용하여 ASA 디바이스용 NSEL 구성, on page 53의 내용을 참조하십시오.

Procedure

단계 **1** **class-map** 명령은 SEC로 내보낼 NSEL 트래픽을 식별하는 클래스 맵의 이름을 지정합니다.

- **{{flow-export-class-name}}**- 클래스 맵의 이름을 입력합니다. 이름의 길이는 최대 40자입니다. "class-default"라는 이름 그리고 "_internal" 또는 "_default"로 시작하는 모든 이름은 예약되어 있습니다. 모든 유형의 클래스 맵은 동일한 네임스페이스를 사용하므로, 다른 클래스 맵 유형에서 사용된 이름을 재사용할 수 없습니다.

단계 **2** 클래스 맵과 연결될(일치하는) 트래픽을 식별합니다. **{{add_this_traffic_to_class_map}}**의 값에 대해 다음 옵션 중 하나를 선택합니다.

- **{{add_this_traffic_to_class_map}}** 필드에 **any**를 입력합니다. NSEL 트래픽에 대한 모든 트래픽 유형을 모니터링합니다. **"any"** 값을 사용하는 것이 좋습니다**.**
- **{{add_this_traffic_to_class_map}}** 필드에 **access-list *name-of-access-list***를 입력합니다. 이렇게 하면 생성한 액세스 목록과 연결된 모든 트래픽이 연결됩니다. 자세한 내용은 Cisco ASA NetFlow 구현 가이드에서 모듈러 정책 프레임워크를 통한 플로우 내보내기 구성을 참조하십시오.

What to do next

NSEL 이벤트에 대한 정책 맵 정의, on page 57를 계속합니다.

NSEL 이벤트에 대한 정책 맵 정의

이 작업은 이전 작업에서 생성한 클래스에 NetFlow 내보내기 작업을 할당하고 새 정책 맵에 클래스를 할당합니다. 이 지침은 매크로의 이 섹션을 참조하십시오.

policy-map {{global_policy_map_name}}

class {{flow_export_class_name}}

flow-export event-type {{event_type}} destination {{SEC_IPv4_address}}

Before you begin

이는 더 큰 워크플로우의 일부입니다. 시작하기 전에 Security Cloud Control 매크로를 사용하여 ASA 디바이스용 NSEL 구성, on page 53의 내용을 참조하십시오.

Procedure

단계 **1** **policy-map** 명령은 policy-map을 생성합니다. 다음 작업에서는 이 정책 맵을 전역 정책과 연결합니다.

- **{{global_policy_map_name}}** - 정책 맵의 이름을 입력합니다. 방화벽의 기존 전역 정책 이름(있는 경우)을 사용하는 것이 좋습니다. 전역 정책의 기본 이름은 **global_policy**입니다. ASA 글로벌 정책의 이름 결정을 참조하십시오. Cisco ASA NetFlow 구현 가이드의 Configure Flow-Export Actions Through Modular Policy Framework(모듈형 정책 프레임워크를 통한 플로우 내보내기 작업 구성)에 따라 새 정책 맵을 생성하고 전역적으로 적용하는 경우 나머지 검사 정책은 비활성화됩니다.

단계 **2** **class** 명령은 SEC로 전송될 NSEL 이벤트를 정의하는 클래스 맵 생성, on page 56에서 생성한 클래스 맵의 이름을 상속합니다.

단계 **3** **flow-export event-type** {{event-type}} **destination** {{IPv4_address}} 명령은 플로우 컬렉터(이 경우 SEC)로 전송해야 하는 이벤트 유형을 정의합니다.

- **{{event-type}}** - event_type 키워드는 필터링되는 지원 이벤트의 이름입니다. **"all"** 값을 사용하는 것이 좋습니다.
- **{{SEC_IPv4_address}}** -SEC의 IPv4 주소입니다. 해당 값은 NSEL 메시지의 대상 및 SEC로 전송되는 간격 정의, on page 55에 입력한 값에서 상속됩니다.

What to do next

중복된 시스템 로그 메시지 비활성화, on page 57를 계속합니다.

중복된 시스템 로그 메시지 비활성화

이 지침은 매크로의 이 섹션을 참조하십시오. 명령을 수정할 필요가 없습니다.

logging flow-export-syslogs disable

NetFlow를 활성화하여 플로우 정보를 내보내면 다음 표의 시스템 로그 메시지가 중복됩니다. 동일한 정보를 NetFlow를 통해 내보내므로 성능을 위해 중복 시스템 로그 메시지를 비활성화하는 것이 좋습니다.

Note NSEL 및 시스템 로그 메시지가 모두 활성화된 경우 두 로깅 유형 간에 시간순으로 정렬되지 않습니다.

Syslog 메시지	설명	**NSEL** 이벤트 **ID**	**NSEL** 확장 이벤트 **ID**
106100	액세스 제어 규칙(ACL)이 발생할 때마다 생성됨	1 — 플로우가 생성됨(ACL에서 플로우를 허용한 경우) 3 — 플로우가 거부됨(ACL에서 플로우를 거부한 경우)	0 — ACL이 플로우를 허용한 경우 1001 — 인그레스 ACL에서 플로우를 거부함 1002 — 이그레스 ACL에서 플로우를 거부함
106015	첫 번째 패킷이 SYN 패킷이 아니므로 TCP 플로우가 거부됨	3 — 플로우가 거부됨	1004 — 첫 번째 패킷이 TCP SYN 패킷이 아니므로 플로우가 거부됨
106023	**access-group** 명령을 통해 인터페이스에 연결된 ACL에서 플로우를 거부한 경우	3 — 플로우가 거부됨	1001 — 인그레스 ACL에서 플로우를 거부함 1002 — 이그레스 ACL에서 플로우를 거부함
302013, 302015, 302017, 302020	TCP, UDP, GRE, ICMP 연결 생성	1 — 플로우가 생성됨	0 — 무시함
302014, 302016, 302018, 302021	TCP, UDP, GRE, ICMP 연결 해체	2 — 플로우가 삭제됨	0 — 무시함 >2000 — 플로우가 해체됨
313001	디바이스에 대한 ICMP 패킷이 거부됨	3 — 플로우가 거부됨	1003 — 구성으로 인해 To-the-box 플로우가 거부됨
313008	디바이스에 대한 ICMP v6 패킷이 거부됨	3 — 플로우가 거부됨	1003 — 구성으로 인해 To-the-box 플로우가 거부됨
710003	디바이스 인터페이스에 대한 연결 시도가 거부됨	3 — 플로우가 거부됨	1003 — 구성으로 인해 To-the-box 플로우가 거부됨

중복 시스템 로그 메시지를 비활성화하지 않으려면 이 매크로를 편집하고 이 줄만 삭제할 수 있습니다.

logging flow-export-syslogs disable

NetFlow 관련 시스템 로그 메시지 비활성화 및 다시 활성화의 절차에 따라 나중에 개별 시스템 로그 메시지를 활성화하거나 비활성화할 수 있습니다.

매크로 검토 및 전송

Before you begin

이는 더 큰 워크플로우의 일부입니다. 시작하기 전에 Security Cloud Control 매크로를 사용하여 ASA 디바이스용 NSEL 구성, on page 53의 내용을 참조하십시오.

Procedure

단계 **1** 매크로의 필드를 입력한 후 **Review(**검토**)**를 클릭하여 ASA로 전송되기 전에 명령을 검토합니다.

단계 **2** 명령에 대한 응답이 만족스러우면 **Send(**전송**)**를 클릭합니다.

단계 **3** 명령을 전송한 후 "일부 명령이 실행 중인 구성을 변경했을 수 있습니다."라는 메시지와 함께 두 개의 링크가 표시될 수 있습니다.

- **Write to Disk(**디스크에 쓰기**)**를 클릭하면 이 명령으로 수행한 변경 사항과 실행 중인 구성의 다른 모든 변경 사항이 디바이스의 시작 구성에 저장됩니다.
- **Dismiss(**해제**)**를 클릭하면 메시지가 사라집니다.

Security Cloud Control 매크로를 사용하여 ASA 디바이스용 NSEL 구성, on page 53에 설명된 워크플로우를 완료했습니다.

ASA에서 NSEL(NetFlow Secure Event Logging) 구성 삭제

이 절차에서는 SEC(Secure Event Connector)를 NSEL 플로우 컬렉터로 지정하는 ASA에서 NSEL(NetFlow Secure Event Logging) 구성을 삭제하는 방법을 설명합니다. 이 절차에서는 Security Cloud Control 매크로를 사용하여 ASA 디바이스용 NSEL 구성에 설명된 매크로를 반대로 수행합니다.

이 절차는 **DELETE NSEL** 매크로를 참조하십시오.

```
policy-map {{flow_export_policy_name}}
no class {{flow_export_class_name}}
no class-map {{flow_export_class_name}}
no flow-export destination {{interface}} {{IPv4_address}} {{NetFlow_port}}
no flow-export template timeout-rate {{timeout_rate_in_mins}}
no flow-export delay flow-create {{delay_flow_create_rate_in_secs}}
no flow-export active refresh-interval {{refresh_interval_in_mins}}
logging flow-export-syslogs enable
show run flow-export
```

```
show run policy-map {{flow_export_policy_name}}
show run class-map {{flow_export_class_name}}
```

DELETE-NSEL 매크로 열기

Procedure

단계 **1** **Security Devices(**보안 디바이스 **)** 페이지에서 **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **2** 적절한 디바이스 유형 탭을 클릭하고 NSEL(NetFlow Secure Event Logging) 구성을 삭제할 ASA를 선택합니다.

단계 **3** **Device Actions(**디바이스 작업**)** 창에서 **Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다.

단계 **4** 매크로 별표(Macros)를 클릭하여 사용 가능한 매크로 목록을 표시합니다.

단계 **5** 매크로 목록에서 **DELETE-NSEL**을 선택합니다.

단계 **6** Macro(매크로) 상자에서 **View Parameters(**매개변수 보기**)**를 클릭합니다.

매크로에 값을 입력하여 **No** 명령 완료

ASA CLI는 명령의 "no" 형식을 사용하여 삭제합니다. 매크로의 필드를 입력하여 명령의 "no" 형식을 완성합니다.

Procedure

단계 **1** policy-map {{flow_export_policy_name}}

- **{{flow_export_policy_name}}** - 정책 맵 이름의 값을 입력합니다.

단계 **2** no class {{flow_export_class_name}}

- **{{flow_export_class_name}}** - 클래스 맵 이름의 값을 입력합니다.

단계 **3** no class-map {{flow_export_class_name}}

- **{{flow_export_class_name}}** - 클래스 맵 이름의 값이 위의 단계에서 상속됩니다.

단계 **4** no flow-export destination {{interface}} {{IPv4_address}} {{NetFlow_port}}

- **{{interface}}** - NetFlow 이벤트가 전송된 ASA의 인터페이스 이름을 입력합니다.
- **{{IPv4_address}}** - SEC의 IPv4 주소를 입력합니다. SEC는 플로우 컬렉터 역할을 합니다.
- **{{NetFlow_port}}** - NetFlow 패킷이 전송되는 SEC의 UDP 포트 번호를 입력합니다.

단계 **5** no flow-export template timeout-rate {{timeout_rate_in_mins}}

- **{{timeout_rate_in_mins}}** - flow-export 템플릿 제한 시간을 입력합니다.

단계 **6** no flow-export delay flow-create {{delay_flow_create_rate_in_secs}}

- **{{delay_flow_create_rate_in_secs}}** - flow-export 지연 플로우 생성 속도를 입력합니다.

단계 **7** no flow-export active refresh-interval {{refresh_interval_in_mins}}

- **{{refresh_interval_in_mins}}** - flow-export 활성 새로 고침 간격을 입력합니다.

ASA 전역 정책의 이름 확인

ASA의 전역 정책 이름을 확인하려면 다음 절차를 수행합니다.

Procedure

단계 **1** **Security Devices(**보안 디바이스**)** 페이지에서 전역 정책의 이름을 찾을 디바이스를 선택합니다.

단계 **2** Device Actions(디바이스 작업) 창에서 **>_Command Reference(**명령 참조**)**를 선택합니다.

단계 **3** Command Line Interface(명령줄 인터페이스) 창의 프롬프트에 다음을 입력합니다.

show running-config service-policy

아래 예의 출력에서 global_policy는 전역 정책의 이름입니다.

예:

> **show running-config service-policy**

service-policy global_policy global

NSEL 데이터 플로우 문제 해결

NSEL(Netflow Secure Event Logging) 구성을 했으면 다음 절차를 사용하여 NSEL 이벤트가 사용자 ASA에서 Cisco Cloud로 전송되고 Cisco Cloud가 이를 수신하는지 확인합니다.

ASA가 NSEL 이벤트를 SEC(보안 이벤트 커넥터)로 보낸 다음 Cisco Cloud로 보내도록 구성된 후에는 데이터가 즉시 흐르지 않습니다. NET에서 생성되는 NSEL 관련 트래픽이 있다고 가정하면 첫 번째 NSEL 패킷이 ASA에 도착하는 데 몇 분 정도 걸릴 수 있습니다.

Note 이 워크플로우는 "flow-export counters" 명령 및 "capture" 명령을 사용하여 NSEL 데이터 플로우 문제를 해결하는 방법을 보여줍니다. 이러한 명령 사용에 대한 자세한 내용은CLI Book 1: Cisco ASA 시리즈 일반 운영 CLI 구성 가이드의 "패킷 캡처" 및 Cisco ASA NetFlow 구현 가이드의 "NSEL 모니터링"을 참조하십시오.

다음 세 가지 작업을 수행합니다.

- NetFlow 패킷이 SEC로 전송되고 있는지 확인
- Cisco Cloud에서 NetFlow 패킷을 수신하고 있는지 확인

NSEL 이벤트가 SEC로 전송되고 있는지 확인

두 명령 중 하나를 사용하여 NSEL 패킷이 SEC로 전송되고 있는지 확인합니다.

- flow-export counters
- capture

"flow-export counters" 명령을 사용하여 전송되는 **flow-export** 패킷 및 **NSEL** 오류 확인

- NSEL 이벤트를 SEC로 전송하도록 ASA를 구성했는지 확인합니다 Security Cloud Control 매크로를 사용하여 ASA 디바이스용 NSEL 구성을 참조하십시오.
- SEC IP 주소는 NSEL 이벤트의 플로우 컬렉터 주소입니다. 테넌트에 둘 이상의 SEC를 온보딩한 경우 올바른 IP 주소를 사용하고 있는지 확인합니다.
- NetFlow 이벤트를 전달하는 데 사용되는 UDP 포트 번호를 찾습니다. Cisco Security Analytics and Logging에 사용되는 디바이스의 TCP, UDP 및 NSEL 포트 찾기를 참조하십시오.
- NSEL 이벤트를 전송하는 ASA에서 권장되는 인터페이스는 관리 인터페이스입니다. 인터페이스가 다를 수 있습니다.

Security Cloud Control의 명령줄 인터페이스를 사용하여 NSEL에 대해 구성한 ASA에 이러한 명령을 전송합니다.

Procedure

단계 **1** 탐색창에서 **Security Devices(**보안 디바이스**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **3** 적절한 디바이스 탭을 클릭하고 NSEL 이벤트를 SEC로 전송하도록 구성한 ASA를 선택합니다.

단계 **4** 오른쪽의 **Device Actions(**디바이스 작업**)** 창에서 **Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다.

단계 **5** `clear flow-export counters` 명령을 실행하여 플로우 내보내기 카운터를 재설정합니다. 이렇게 하면 새 이벤트가 수신되는지 쉽게 확인할 수 있도록 clear export flow 카운터가 0으로 재설정됩니다.

예시:

```
> clear flow-export counters

Done!
```

단계 **6** NSEL 패킷의 대상, 전송된 패킷 수 및 오류를 확인하려면 show flow-export counters 명령을 실행합니다.

예시:

```
>show flow-export counters
```

```
대상: management 209.165.200.225 10425

Statistics:

packets sent 25000

오류:

block allocation errors 0

invalid interface 0

template send failure 0

no route to collector 0

source port allocation 0
```

위의 출력에서 목적지 줄은 NSEL 이벤트가 전송된 ASA의 인터페이스, SEC의 IP 주소, SEC의 포트 10425를 보여줍니다. 또한 25000의 전송된 패킷도 표시 됩니다.

오류가 없고 패킷이 전송되는 경우 아래의 Cisco Cloud에서 NetFlow 패킷이 수신되고 있는지 확인으로 건너뛰십시오.

오류 설명:

- **block allocation errors(**블록 할당 오류**)** -블록 할당 오류가 수신되면 ASA가 플로우 엑스포터에 메모리를 할당하지 않은 것입니다.
  - 복구 작업: Cisco TAC(Technical Assistance Center)에 문의합니다.
- **invalid interface(**잘못된 인터페이스**)** - NSEL 이벤트를 SEC로 전송하려고 하지만 플로우 내보내기에 대해 정의한 인터페이스가 전송하도록 구성되지 않았음을 나타냅니다.
  - 복구 작업: NSEL을 구성할 때 선택한 인터페이스를 검토합니다. 관리 인터페이스를 사용하는 것이 좋습니다. 사용자의 인터페이스는 다를 수 있습니다.
- **template send failure(**템플릿 전송 실패**)** - NSEL을 정의해야 하는 템플릿이 올바르게 구문 분석되지 않았습니다.
  - 복구 작업: Security Cloud Control 지원에 문의하십시오.
- **no route to collector(**컬렉터에 대한 경로 없음**)**-ASA에서 SEC로의 네트워크 경로가 없음을 나타냅니다
  - 복구 작업:
    - NSEL을 구성할 때 SEC에 사용한 IP 주소가 올바른지 확인합니다.
    - SEC의 상태가 Active(활성)이고 최근 하트비트를 전송했는지 확인합니다. SDC에 연결할 수 없음을 참조하십시오.
    - Secure Device Connector의 상태가 Active(활성)이고 최근 하트비트를 전송했는지 확인합니다.

- **source port allocation(**소스 포트 할당**)** - ASA에 잘못된 포트가 있음을 나타낼 수 있습니다.

"capture" 명령을 사용하여 ASA에서 SEC로 전송된 NSEL 패킷 캡처

- NSEL 이벤트를 SEC로 전송하도록 ASA를 구성했는지 확인합니다 Security Cloud Control 매크로를 사용하여 ASA 디바이스용 NSEL 구성을 참조하십시오.
- SEC IP 주소는 NSEL 이벤트의 플로우 컬렉터 주소입니다. 테넌트에 둘 이상의 SEC를 온보딩한 경우 올바른 IP 주소를 사용하고 있는지 확인합니다.
- NetFlow 이벤트를 전달하는 데 사용되는 UDP 포트 번호를 찾습니다. Cisco Security Analytics and Logging에 사용되는 디바이스의 TCP, UDP 및 NSEL 포트 찾기를 참조하십시오.
- NSEL 이벤트를 전송하는 ASA에서 권장되는 인터페이스는 관리 인터페이스입니다. 인터페이스가 다를 수 있습니다.

Security Cloud Control의 명령줄 인터페이스를 사용하여 NSEL에 대해 구성한 ASA에 이러한 명령을 전송합니다.

프로시저

단계 **1** 탐색창에서 **Security Devices(**보안 디바이스**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **3** 적절한 디바이스 유형 탭을 클릭하고 NSEL 이벤트를 SEC로 전송하도록 구성한 ASA를 선택합니다.

단계 **4** 오른쪽의 **Device Actions(**디바이스 작업**)** 창에서 **Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다.

단계 **5** 명령 창에서 이 **capture** 명령을 실행합니다.

>**capture***capture_name***interface***interface_name* **match udp any host** *IP_of_SEC***eq***NetFlow_port*

어디에서

- *capture_name*은 패킷 캡처의 이름입니다.
- *interface_name*은 NSEL 패킷이 ASA를 나가는 인터페이스의 이름입니다.
- *IP_of_SEC*는 SEC VM의 IP 주소입니다.
- *NetFlow_port*는 NSEL 이벤트가 전송되는 포트입니다.

이렇게 하면 패킷 캡처가 시작됩니다.

단계 **6** 캡처된 패킷을 보려면 **show capture** 명령을 실행합니다.

> show capture*capture_name*

여기서 *capture_name*은 이전 단계에서 정의한 패킷 캡처의 이름입니다.

다음은 캡처 시간, 패킷이 전송된 IP 주소, IP 주소 및 패킷이 전송된 포트를 표시하는 출력의 예입니다. 이 예에서 192.168.25.4는 SEC의 IP 주소이고 포트 10425는 NSEL 이벤트를 수신하는 SEC의 포트입니다.

캡처된 6개의 패킷

```
1: 14:23:51.706308 192.168.0.169.16431 > 192.168.25.4.10425: udp 476
2: 14:23:53.923017 192.168.0.169.16431 > 192.168.25.4.10425: udp 248
3: 14:24:07.411904 192.168.0.169.16431 > 192.168.25.4.10425: udp 1436
4: 14:24:07.411920 192.168.0.169.16431 > 192.168.25.4.10425: udp 1276
5: 14:24:21.021208 192.168.0.169.16431 > 192.168.25.4.10425: udp 112
6: 14:24:27.444755 192.168.0.169.16431 > 192.168.25.4.10425: udp 196
```

단계 **7** 패킷 캡처를 수동으로 중지하려면 **capture stop** 명령을 실행합니다.

> capture *capture_name***stop**

여기서 *capture_name*은 이전 단계에서 정의한 패킷 캡처의 이름입니다.

Cisco Cloud에서 NetFlow 패킷을 수신하고 있는지 확인

시작하기 전에

NSEL 이벤트가 ASA에서 전송되고 있는지 확인합니다.

라이브 NSEL 이벤트 확인

라이브 이벤트와 기록 이벤트를 모두 확인합니다.

이 절차에서는 Cisco Cloud가 지난 1시간 내에 수신한 NSEL 이벤트를 필터링합니다.

Procedure

단계 **1** Security Cloud Control 플랫폼 메뉴에서, **Products(**제품**)** > **Firewall(**방화벽**)**을 클릭합니다.

단계 **2** 왼쪽 창에서 **Events & Logs(**이벤트 및 로그**)** > **Events(**이벤트**)** > **Event Logging(**이벤트 로깅**)**를 선택합니다.

단계 **3** **Live(**라이브**)** 탭을 클릭합니다.

단계 **4** 이벤트 필터를 고정으로 엽니다.

단계 **5** ASA 이벤트 섹션에서 **NetFlow**가 선택되어 있는지 확인합니다.

단계 **6** NSEL 이벤트를 전송하도록 구성한 ASA의 IP 주소를 Sensor ID(센서 ID) 필드에 입력합니다.

단계 **7** 필터의 맨 아래에서 **Include NetFlow Events(NetFlow** 이벤트 포함**)**가 선택되어 있는지 확인합니다.

이전 NSEL 이벤트 확인

이 절차는 Cisco 클라우드가 지정한 기간 내에 수신한 NSEL 이벤트를 필터링합니다.

Procedure

단계 **1** Security Cloud Control 플랫폼 메뉴에서, **Products(**제품**)** > **Firewall(**방화벽**)**을 클릭합니다.

단계 **2** 왼쪽 창에서 **Events & Logs(**이벤트 및 로그**)** > **Events(**이벤트**)** > **Event Logging(**이벤트 로깅**)**를 선택합니다.

단계 **3** 기록 탭을 클릭합니다.

단계 **4** 이벤트 필터를 고정으로 엽니다.

단계 **5** ASA 이벤트 섹션에서 **NetFlow**가 선택되어 있는지 확인합니다.

단계 **6** Security Cloud Control가 NSEL 이벤트를 수신한 적이 있는지 확인할 수 있도록 시작 시간을 충분히 이전으로 설정합니다.

단계 **7** NSEL 이벤트를 전송하도록 구성한 ASA의 IP 주소를 Sensor ID(센서 ID) 필드에 입력합니다.

단계 **8** 필터의 맨 아래에서 **Include NetFlow Events(NetFlow** 이벤트 포함**)**가 선택되어 있는지 확인합니다.

구문 분석된 **ASA** 시스템 로그 이벤트

구문 분석된 시스템 로그 이벤트는 다른 시스템 로그 이벤트보다 더 많은 이벤트 속성을 포함하며, 구문 분석된 특정 필드에서 검색할 수 있습니다. SEC는 지정한 모든 ASA 이벤트를 Cisco Cloud로 전달하지만, 아래 테이블의 시스템 로그 메시지만 구문 애널리틱스됩니다. 구문 분석된 모든 시스템 로그 이벤트는 식별을 돕기 위해 이탤릭체로 표시됩니다.

시스템 로그에 대한 자세한 설명은 Cisco ASA Series 시스템 로그 메시지를 참조하십시오.

시스템 로그 **ID**	시스템 로그 범주	시스템 로그 메시지의 목적
106015	Firewall	상태가 잘못된 TCP 거부를 나타냅니다.
106023	Firewall	실제 IP 패킷이 ACL에 의해 거부되었습니다. 이 메시지는 ACL에 대해 로그 옵션을 활성화하지 않은 경우에도 나타납니다.
106100	액세스 목록/사용자 세션	패킷이 ACL에 의해 허용되거나 거부되었습니다.
113019	사용자 인증	중요 AnyConnect
302013, 302015, 302017, 302020	사용자 세션	TCP, UDP, GRE 및 ICMP 연결 생성을 위한 연결 시작 및 종료 Syslog.

시스템 로그 ID	시스템 로그 범주	시스템 로그 메시지의 목적
302014, 302016, 302018, 302021	사용자 세션	TCP, UDP, GRE 및 ICMP 연결 생성을 위한 연결 시작 및 종료 Syslog.
302020 - 302021	사용자 세션	ICMP 세션 설정 및 해제.
305006	사용자 세션/NAT 및 PAT	NAT 연결 실패
305011-305014	사용자 세션/NAT 및 PAT	NAT 빌드/해체 관련
313001, 313008	IP 스택	상자에 거부된 연결을 나타냅니다.
414004	시스템	중요 AnyConnect
609001 - 609002	Firewall	영역에 연결된 호스트 **ip-address**에 대해 네트워크 상태 컨테이너가 예약/제거되었습니다.
710002,710004 710005	사용자 세션	상자 연결 실패
710003	사용자 세션	상자에 거부된 연결을 나타냅니다.
746012, 746013	사용자 세션	중요 AnyConnect

관련 정보:

- 명령줄 인터페이스를 사용하여 Cisco Cloud에 ASA 시스템 로그 이벤트 전송
- 이벤트 로깅 페이지에서 이벤트 필터링