엘리펀트 플로우 탐지 결과 구성

엘리펀트 플로우 정보

엘리펀트 플로우는 매우 크며(총 바이트), 네트워크 링크를 통해 측정되는 TCP(또는 기타 프로토콜) 플로우에 의해 설정된 네트워크 연결이 상대적으로 오래 실행됩니다. 기본적으로 엘리펀트 플로우는 10초당 1GB보다 큰 플로우 또는 연결입니다. 이로 인해 Snort 코어에서 성능 저하 또는 문제가 발생할 수 있습니다. 엘리펀트 플로우는 잠재적으로 CPU 리소스를 과도하게 사용할 수 있으며 탐지 리소스를 놓고 경쟁하는 다른 플로우에 영향을 미칠 수 있고, 레이턴시 증가나 패킷 삭제 등의 문제를 일으킬 수 있어 중요합니다.

엘리펀트 플로우 탐지 및 교정의 이점

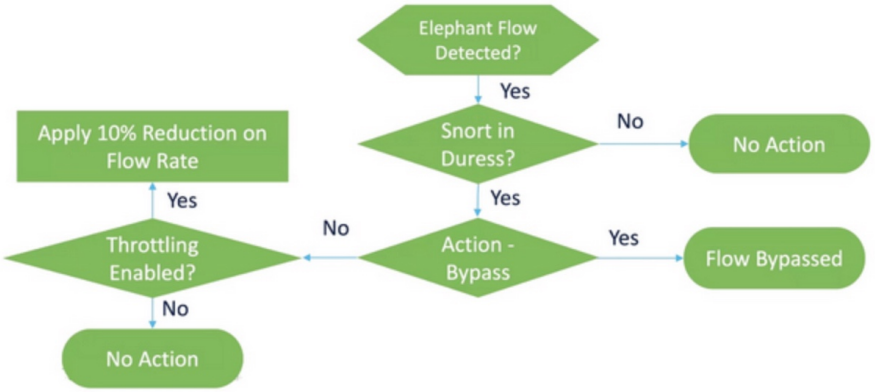
- 엘리펀트 플로우 구성을 사용하면 엘리펀트 플로우를 우회하거나 제한하는 옵션이 지원되며 사용자 지정이 가능합니다.
- 선택한 애플리케이션을 기반으로 플로우를 우회하거나 제한하도록 선택하여 의심스러운 트래픽에 대해 Snort 검사를 제공하면서 신뢰할 수 있는 트래픽을 더 많이 우회할 수 있습니다.
- 엘리펀트 플로우 교정은 특정 요건에 따라 우선순위를 지정하고 내부 애플리케이션에 더 많은 대역폭을 확보하는 데 도움이 됩니다.

엘리펀트 플로우 워크플로우

구성된 매개변수를 기준으로 엘리펀트 플로우가 탐지되면 플로우를 우회하거나 제한하도록 선택할 수 있습니다. 플로우를 우회하는 경우 해당 트래픽은 Snort 검사 없이 통과할 수 있습니다. 제한은 플로우 처리량이 감소되었음을 나타냅니다. 플로우 속도 감소는 CPU 사용률이 구성된 임계값 아래로 감소할 때까지 10% 증분으로 이루어집니다. 엘리펀트 플로우를 식별하고 추가 CPU 및 시간 창 매개변수를 충족한 후에 우회 또는 제한이 발생합니다. 엘리펀트 플로우를 식별하기 전에 침입 정책은 허용 규칙에서 구성했다고 가정하고 플로우를 처리합니다. 이는 대부분의 공격이 연결에서 매우 초기에 감지되기 때문에 엘리펀트 플로우가 완전히 검사되지 않은 상태로 시스템을 통과할 수 없다는 것을 의미합니다.

플로우가 처리되는 방식을 알아보려면 다음 다이어그램을 참조하십시오.

그림 ***1:*** 엘리펀트 플로우 워크플로우



시스템이 Snort 위협 조건(성능 문제)을 탐지하지 않는 한, 어떤 작업도 수행되지 않습니다. 플로우가 크다고 해서 플로우를 제한하거나 우회하지 않습니다. 또한 제한과 우회 작업은 함께 사용할 수 없습니다. 즉, 플로우를 우회하거나 제한할 수 있지만 둘 다 수행할 수는 없습니다.

위협을 유발하는 엘리펀트 플로우를 모두 우회하지 않으려면 특정 애플리케이션에 대해서만 우회 옵션을 제한할 수 있습니다. 성능을 제한하지 않고 신뢰하는 애플리케이션에 대한 연결의 우선순위를 정할 수 있습니다. 우회해야 하는 애플리케이션을 구성할 수 있지만, 위협을 유발하는 나머지 플로우는 제한됩니다. 이렇게 하면 대역폭은 감소하지만, 다른 신뢰할 수 없는 애플리케이션 플로우는 전체 Snort 검사를 계속 수신하게 됩니다.

샘플 비즈니스 시나리오

데이터 센터에서는 클러스터 간 데이터 복제, 가상 머신 통합, 데이터베이스 백업과 같은 여러 활동이 이루어지고 있습니다. 조직의 사용자는 OTT에서 비디오를 시청하거나 다운로드할 수 있습니다. 이러한 활동의 대역폭 사용률은 엘리펀트 플로우를 야기하고 네트워크 속도를 저하하며 중요한 작업의 성능에 영향을 줄 수 있습니다. 네트워크 관리자는 특정 요구 사항에 따라 대역폭 문제를 유발하고 해결하는 대규모 플로우에 대한 정보를 알고 싶어 합니다.

예를 들어, WebEx 트래픽(조직에서 실시간 영상 회의에 사용)에 대한 Snort 검사를 우회하도록 엘리펀트 플로우 매개변수를 구성하고 비디오, 영화 등을 포함한 나머지 애플리케이션 또는 연결을 제한하는 방법을 살펴보겠습니다.

사전 요구 사항

- Management Center 7.2.0 이상을 실행 중이며 매니지드 Threat Defense도 7.2.0 이상인지 확인합니다.
- 엘리펀트 플로우 탐지를 활성화한다고 해서 추가 연결 이벤트가 생성되지는 않습니다. 엘리펀트 플로우 탐지 기능은 이미 Management Center에 로깅되어 있는 일치하는 연결에 엘리펀트 플로우 표기법을 추가합니다. 이러한 이벤트를 로깅하려면 액세스 제어 정책에서 연결 로깅을 활성화해야 합니다**.** 특정 규칙에 대해 이 작업을 수행하거나 엘리펀트 플로우를 포함한 모든 연결을 로깅하는 Monitor(모니터) 규칙을 추가할 수 있습니다.

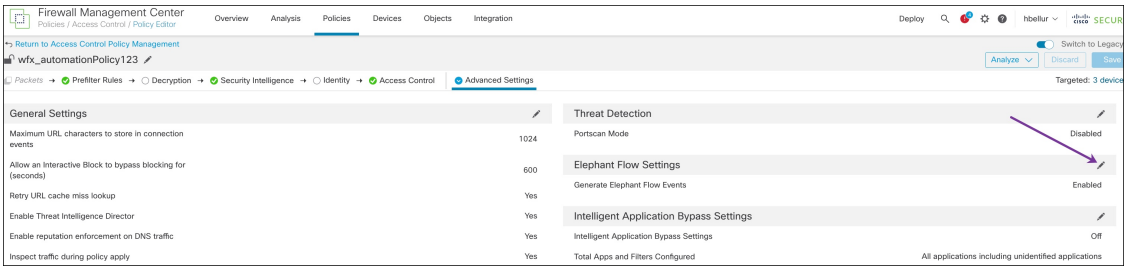
엘리펀트 플로우 매개변수 구성

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)**을 선택합니다.

단계 **2** 편집하려는 액세스 제어 정책 옆에 있는 **Edit(**편집**)**(✎)을 클릭합니다.

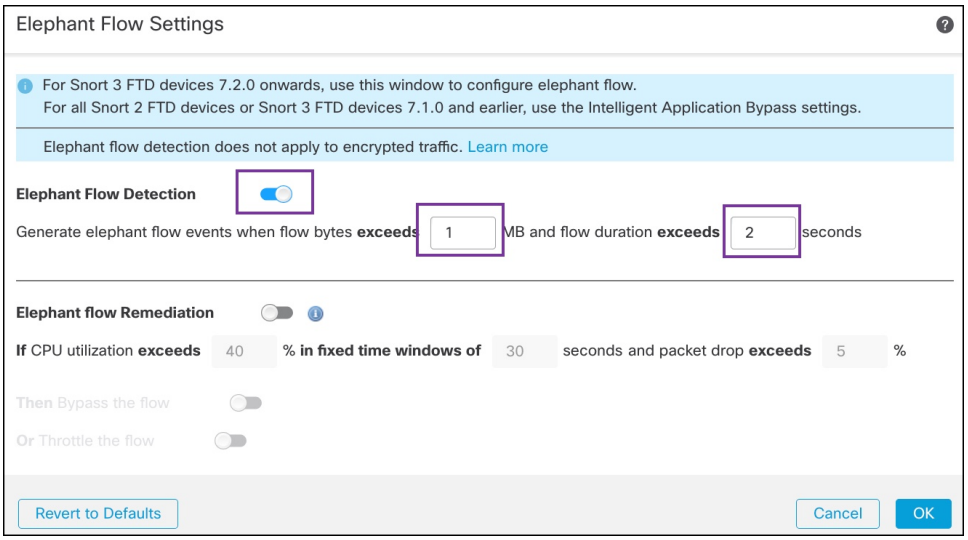
단계 **3** 패킷 플로우 라인 끝에 있는 **More(**더 보기**)** 드롭다운에서 **Advanced Settings(**고급 설정**)**를 선택합니다.

단계 **4** **Elephant Flow Settings(**엘리펀트 플로우 설정**)** 옆에 있는 **Edit(**편집**)**(✎)을 클릭합니다.



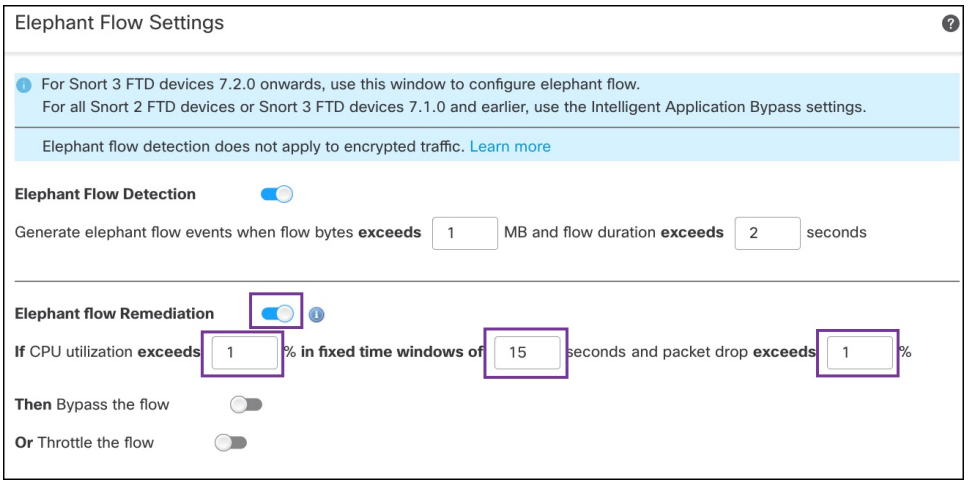
단계 **5** **Elephant Flow Detection(**엘리펀트 플로우 탐지**)** 토글 버튼은 기본적으로 활성화되어 있습니다. 기본 설정은 탐지만 활성화하며, 기본 작업은 구성되지 않습니다. 탐지 설정을 사용하면 플로우 바이트 및 기간을 조정하여 시스템에서 엘리펀트 플로우를 식별할 수 있습니다.

다음 그림에 나와 있는 것처럼 테스트 설정으로 플로우 바이트 및 기간 매개변수를 구성합니다.

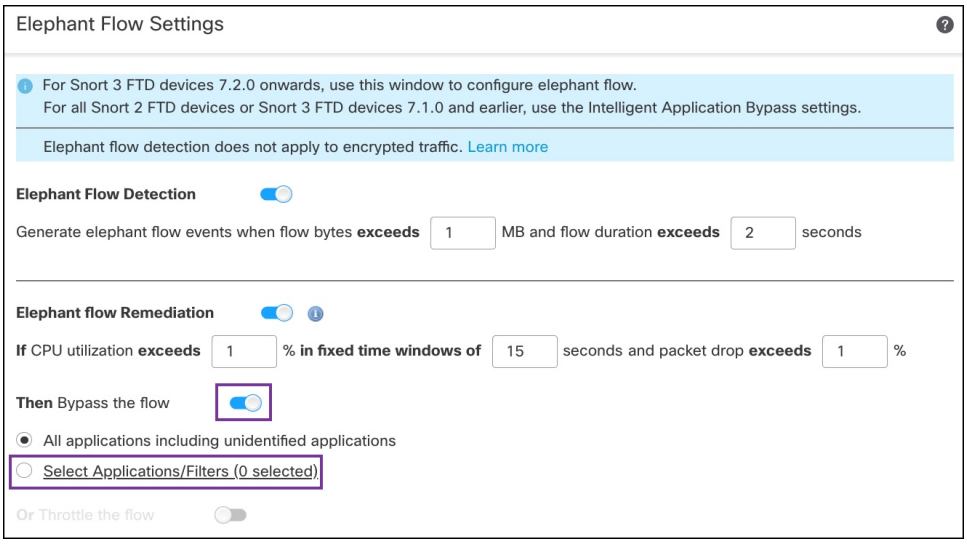


단계 **6** **Elephant Flow Remediation(**엘리펀트 플로우 교정**)** 토글 버튼을 활성화합니다. 엘리펀트 플로우가 탐지되면 플로우를 우회하거나 제한하도록 선택할 수 있습니다. 플로우를 우회하면 트래픽이 Snort 검사 없이 통과할 수 있습니다. 제한은 플로우 처리량이 감소되었음을 나타냅니다. CPU 사용률이 구성된 임계값 미만으로 감소할 때까지 10% 단위로 속도 감소가 이루어집니다.

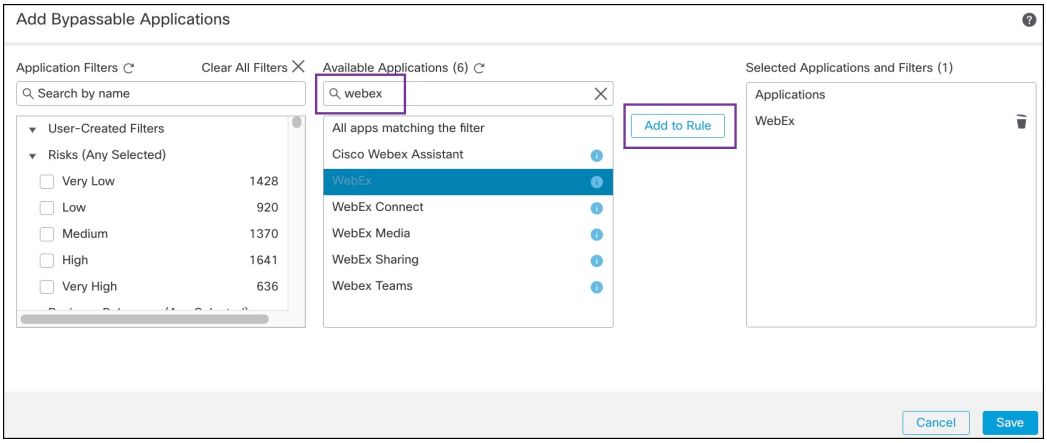
다음 그림에 표시된 것과 같이 엘리펀트 플로우 교정 매개변수를 테스트 설정으로 구성합니다.



단계 **7** **Bypass the flow(**플로우 우회**)** 토글 버튼을 활성화하고 **Select Applications/Filters(**애플리케이션/필터 선택**)** 라디오 버튼을 클릭합니다.



단계 **8** **Application Filters(**애플리케이션 필터**)**에서 **WebEx** 애플리케이션을 검색하여 선택하고, 규칙에 추가한 다음 **Save(**저장**)**를 클릭합니다. 즉, 구성된 매개변수에 따라 이러한 WebEx 연결이 엘리펀트 플로우로 탐지되면 WebEx 연결이 신뢰되고 우선순위가 지정되며 Snort 검사를 건너뜁니다.



단계 **9** 위협을 유발하는 나머지 플로우를 제한하려면 **Throttle(**제한**)** 토글 버튼을 활성화합니다. 이렇게 하면 Snort 위협 조건이 충족될 때까지 다른 모든 플로우의 속도가 10%씩 느려집니다.

단계 **10** **OK(**확인**)**를 클릭합니다.

단계 **11** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참조하십시오.

엘리펀트 플로우에 대한 이벤트 보기

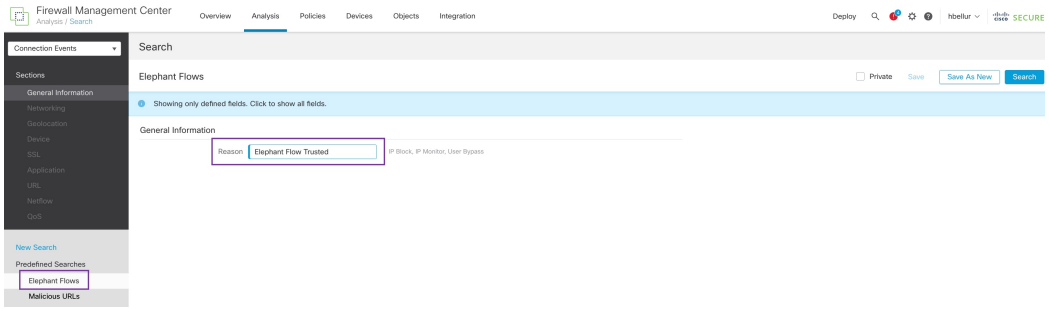
엘리펀트 플로우 설정을 구성한 후 연결 이벤트를 모니터링하여 플로우가 탐지, 우회 또는 제한되었는지 확인합니다. 연결 이벤트의 **Reason(**사유**)** 필드에서 이 정보를 확인할 수 있습니다. 엘리펀트 플로우 연결의 세 가지 유형은 다음과 같습니다.

- 엘리펀트 플로우
- 엘리펀트 플로우 제한
- 엘리펀트 플로우 신뢰

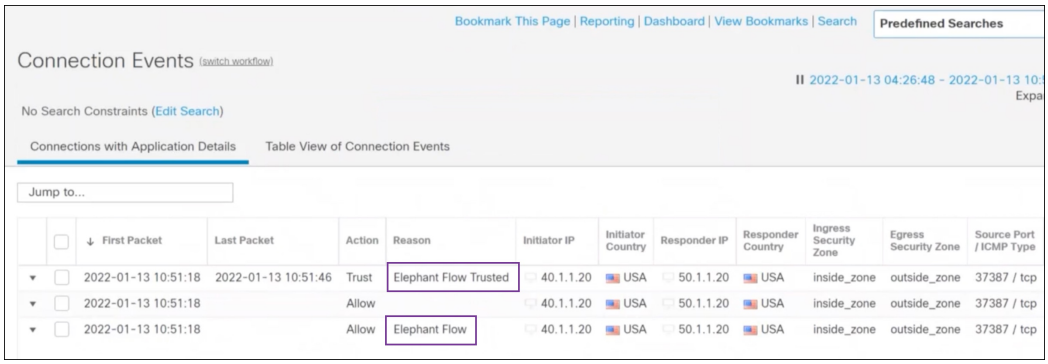
단계 **1** **Analysis(**분석**)** > **Connections(**연결**)** > **Events(**이벤트**)**를 선택합니다. **Unified Events(**통합 이벤트**)** 뷰어에서 이벤트를 볼 수도 있습니다.

단계 **2** **Connection Events(**연결 이벤트**)** 페이지의 **Predefined Search(**사전 정의된 검색**)** 드롭다운 목록에서 **Elephant Flows(**엘리펀트 플로우**)**를 선택하여 엘리펀트 플로우 이벤트를 표시합니다.

팁 **Elephant Flow Trusted(**엘리펀트 플로우 신뢰**)** 또는 **Elephant Flow Throttled(**엘리펀트 플로우 제한**)** 이벤트 유형을 보려면 페이지 왼쪽 상단 모서리에 있는 **Edit Search(**검색 편집**)** 링크를 클릭하고 **Reason(**사유**)** 필드에서 왼쪽 패널의 **Elephant Flow(**엘리펀트 플로우**)**를 선택합니다. 검색하려는 대상에 따라 **Elephant Flow Trusted(**엘리펀트 플로우 신뢰**)** 또는 **Elephant Flow Throttled(**엘리펀트 플로우 제한**)**를 입력합니다.



단계 **3** 플로우 중에 탐지되어 **Reason(**사유**)** 필드에 **Elephant Flow(**엘리펀트 플로우**)**로 표시된 엘리펀트 플로우를 확인합니다. 플로우 종료 시에는 우회되고 **Reason(**사유**)** 필드에 **Elephant Flow Trusted(**엘리펀트 플로우 신뢰**)**가 표시됩니다.



엘리펀트 플로우 교정 제외 구성

교정에서 제외할 플로우에 대한 L4 ACL(액세스 제어 목록) 규칙을 구성할 수 있습니다. 플로우가 엘리펀트 플로우로 탐지되고 해당 플로우가 정의된 규칙과 일치하는 경우 해당 플로우는 교정 작업에서 제외됩니다.

시작하기 전에

Management Center 7.4.0 이상을 실행해야 하며, 매니지드 Threat Defense도 7.4.0 이상이어야 합니다.

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)**을 선택합니다.

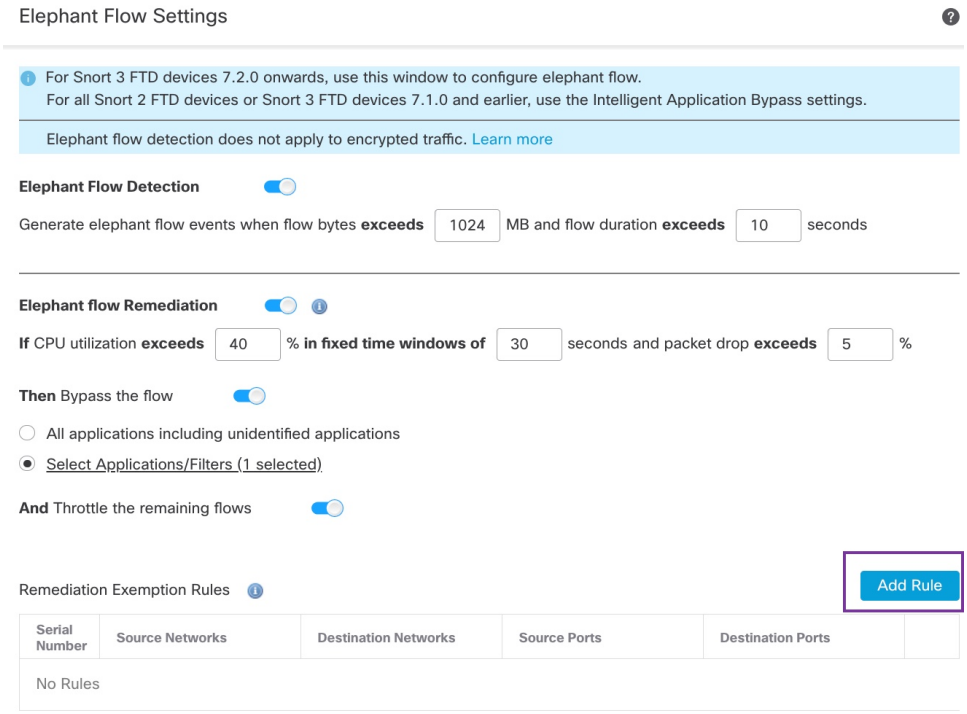
단계 **2** 편집하려는 액세스 제어 정책 옆에 있는 **Edit(**편집**)**( )을 클릭합니다.

단계 **3** 패킷 플로우 라인 끝에 있는 **More(**더 보기**)** 드롭다운에서 **Advanced Settings(**고급 설정**)**를 선택합니다.

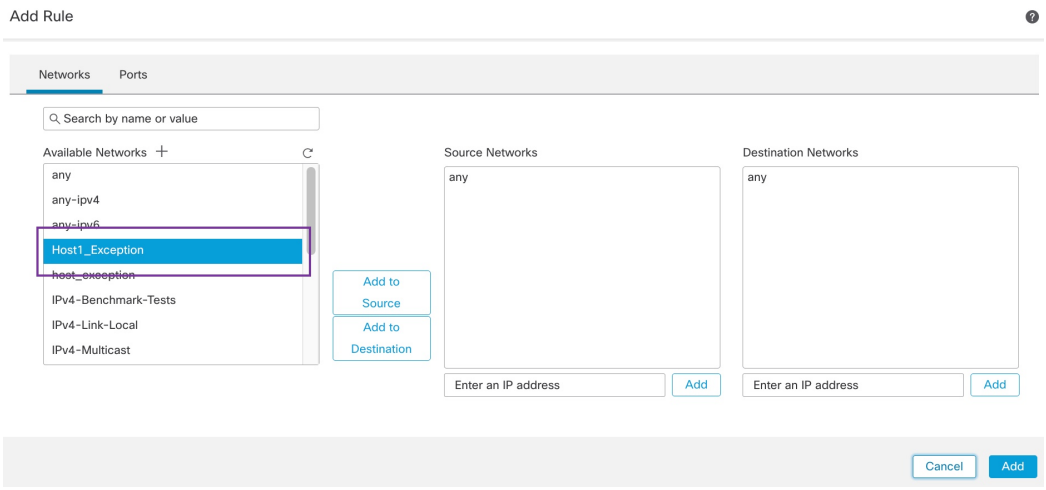
단계 **4** **Elephant Flow Settings(**엘리펀트 플로우 설정**)** 옆에 있는 **Edit(**편집**)**( )을 클릭합니다.

단계 **5** 엘리펀트 플로우 탐지 및 교정 매개변수를 구성했는지 확인합니다. 엘리펀트 플로우 매개변수 구성, 3 페이지의 내용을 참조하십시오.

단계 **6** **Remediation Exemption Rules(**교정 제외 규칙**)** 옆에 있는 **Add Rule(**규칙 추가**)** 버튼을 클릭합니다.



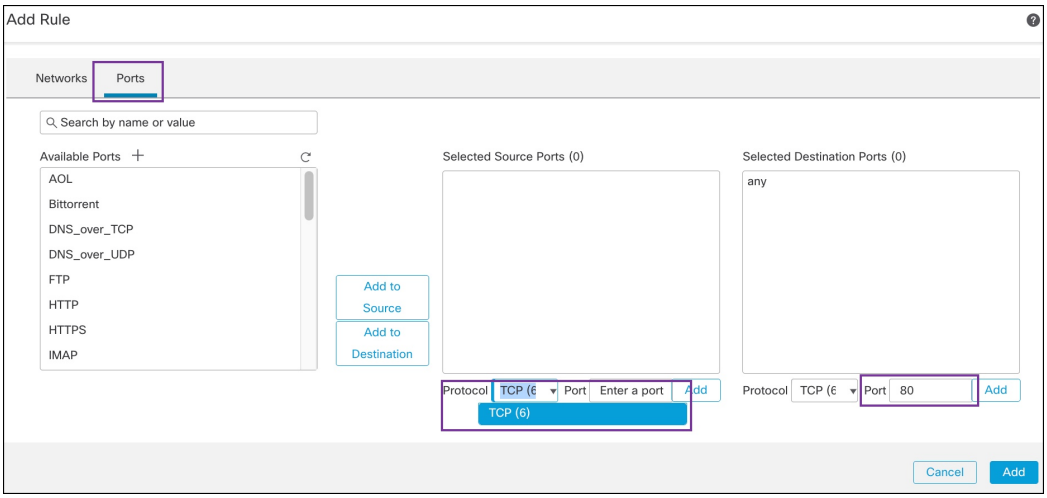
단계 **7** **Available Networks(**사용 가능한 네트워크**)** 목록에서 엘리펀트 플로우 교정에서 제외하도록 구성된 호스트를 선택합니다. 이 예에서는 "Host1_Exception"이라는 호스트를 생성했습니다.



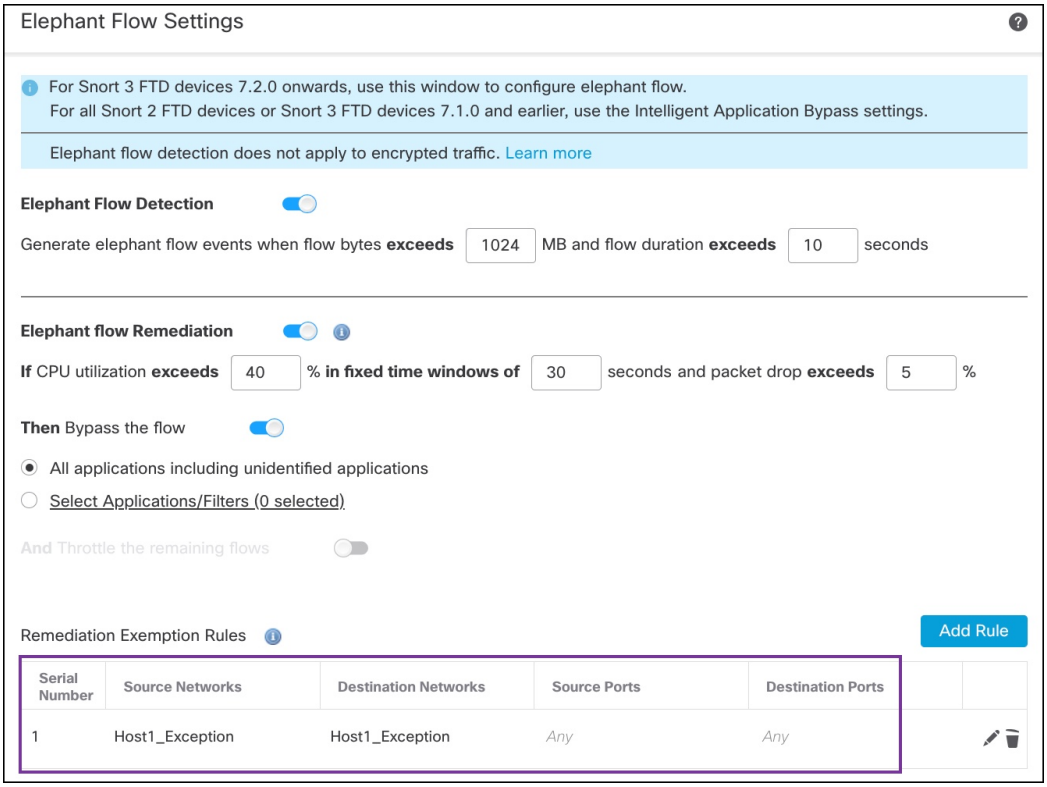
단계 **8** 필요에 따라 **Add to Source(**소스에 추가**)** 또는 **Add to Destination(**대상에 추가**)**을 클릭하여 이 호스트를 소스 또는 대상에 추가합니다.

단계 **9** **Ports(**포트**)** 탭을 클릭합니다.

단계 **10** 소스 포트에 대해 **Protocol as TCP(TCP**형 프로토콜**)**를 선택하고 목적지 포트로 **80**을 입력한 다음 **Add(**추가**)**를 클릭합니다.



단계 **11** **OK(**확인**)**를 클릭합니다.



단계 **12** **Save(**저장**)**를 클릭합니다.

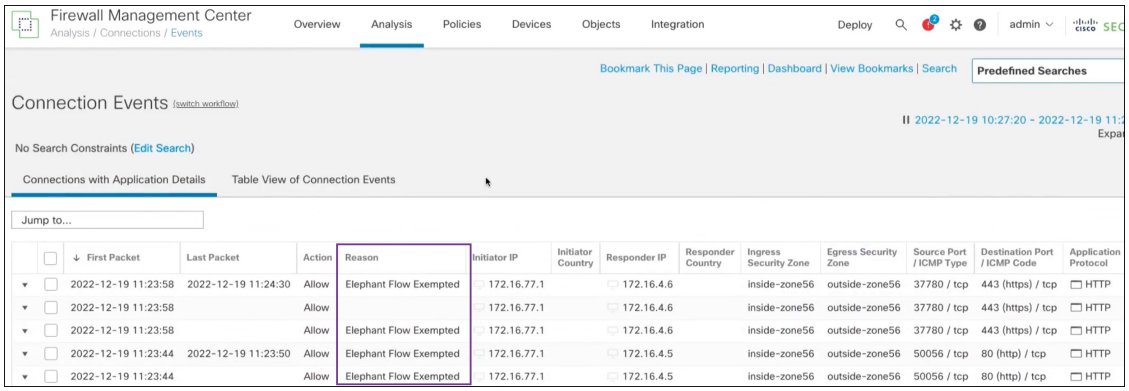
다음에 수행할 작업

구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참조하십시오.

엘리펀트 플로우 교정 제외에 대한 이벤트 보기

단계 **1** **Analysis(**분석**)** > **Connections(**연결**)** > **Events(**이벤트**)**를 선택합니다. **Unified Events(**통합 이벤트**)** 뷰어에서 이벤트를 볼 수도 있습니다.

단계 **2** 교정에서 제외된 엘리펀트 플로우를 확인합니다. **Reason(**사유**)** 필드에 **Elephant Flow Exempted(**엘리펀트 플로우 제외됨**)**가 표시됩니다.



추가 참조 자료

자세한 개념 정보는 이 가이드에 나와 있는 Snort 3의 엘리펀트 플로우 탐지 장이나 다음 링크의 콘텐츠를 참조하십시오.

- 엘리펀트 플로우 탐지