엘리펀트 플로우 탐지

엘리펀트 플로우는 네트워크 링크를 통해 측정된 TCP(또는 기타 프로토콜) 플로우에 의해 설정된 매우 큰(총 바이트) 연속 플로우입니다. 기본적으로 엘리펀트 플로우는 1GB/10초보다 큰 상태입니다. 이로 인해 Snort 코어에서 성능 저하가 발생할 수 있습니다. 엘리펀트 플로우는 많지 않지만 일정 기간 동안 총 대역폭의 과도한 공유를 차지할 수 있습니다. 이로 인해 높은 CPU 사용률, 패킷 삭제 등의 문제가 발생할 수 있습니다.

management center 7.2.0부터(Snort 3 디바이스만 해당) 엘리펀트 플로우 기능을 사용하여 엘리펀트 플로우를 탐지하고 교정할 수 있습니다. 이는 시스템 스트레스를 줄이고 언급된 문제를 해결하는 데 도움이 됩니다.

- 엘리펀트 플로우 탐지 및 교정 정보, 1 페이지
- Intelligent Application Bypass에서 엘리펀트 플로우 업그레이드, 2 페이지
- 엘리펀트 플로우 구성, 2 페이지

엘리펀트 플로우 탐지 및 교정 정보

엘리펀트 플로우 탐지 기능을 사용하여 엘리펀트 플로우를 탐지하고 교정할 수 있습니다. 적용할 수 있는 교정 작업은 다음과 같습니다.

- **Bypass elephant flow(**엘리펀트 플로우 우회**)** - Snort 검사를 우회하도록 엘리펀트 플로우를 구성할 수 있습니다. 구성된 경우 Snort는 해당 플로우에서 패킷을 수신하지 않습니다.
- **Throttle elephant flow(**엘리펀트 플로우 제한**)** - 플로우에 속도 제한을 적용하고 플로우를 계속 검사합니다. 플로우 속도는 동적으로 계산되며, 플로우 속도의 10%가 감소합니다. Snort는 판정(플로우 속도가 10% 감소한 QoS 플로우)을 방화벽 엔진으로 전송합니다. 식별되지 않은 애플리케이션을 포함하여 모든 애플리케이션을 우회하도록 선택하는 경우, 어떤 플로우에 대해서도 스로틀 작업(속도 제한)을 구성할 수 없습니다.

참고 엘리펀트 플로우 탐지가 작동하려면 Snort 3가 탐지 엔진이어야 합니다.

Intelligent Application Bypass에서 엘리펀트 플로우 업그레이드

IAB(Intelligent Application Bypass)는 7.2.0 이상 버전의 Snort 3 디바이스에 더 이상 사용되지 않습니다.

7.2.0 이상을 실행하는 디바이스의 경우, AC 정책의 **Elephant Flow Settings(**엘리펀트 플로우 설정**)**(Advanced settings(고급 설정) 탭)에서 엘리펀트 플로우 설정을 구성해야 합니다.

7.2.0 이상으로 업그레이드한 후 Snort 3 디바이스를 사용하는 경우 엘리펀트 플로우 설정은 **Intelligent Application Bypass Settings(IAB(Intelligent Application Bypass)** 설정**)** 섹션이 아닌 **Elephant Flow Settings(**엘리펀트 플로우 설정**)** 섹션에서 선택 및 구축됩니다. 따라서 엘리펀트 플로우 구성 설정으로 마이그레이션되지 않은 디바이스는 다음 구축 시 엘리펀트 플로우 구성을 잃게 됩니다.

다음 표에는 Snort 3 또는 Snort 2 엔진을 실행하는 7.2.0 이상 버전 및 7.1.0 이하 버전에 적용할 수 있는 IAB 또는 엘리펀트 플로우 구성이 나와 있습니다.

Management Center	**Threat Defense**	엘리펀트 플로우 또는 **IAB** 구성
Management Center 7.0 또는 7.1	Snort 2 디바이스	IAB의 구성을 적용할 수 있습니다.
	Snort 3 디바이스	IAB의 구성을 적용할 수 있습니다.
Management Center 7.2.0	Snort 2 디바이스	IAB의 구성을 적용할 수 있습니다.
	Snort 3 디바이스(7.1.0 이하)	IAB의 구성을 적용할 수 있습니다.
	Snort 3 디바이스(7.2.0 이상)	엘리펀트 플로우의 구성을 적용할 수 있습니다.

엘리펀트 플로우 구성

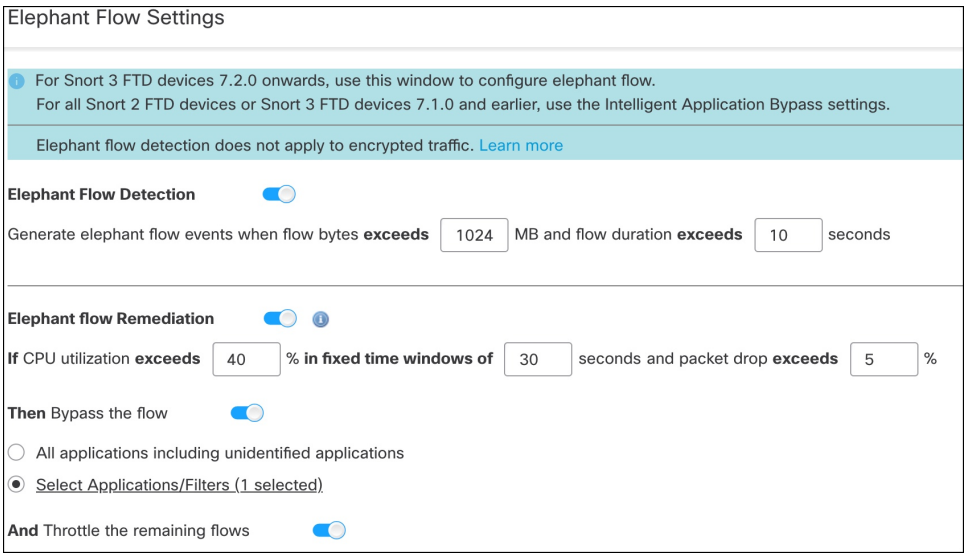
엘리펀트 플로우에서 작업을 수행하도록 엘리펀트 플로우를 구성할 수 있습니다. 이는 시스템 위협, 높은 CPU 사용률, 패킷 삭제 등의 문제를 해결하는 데 도움이 됩니다.

주의 Snort를 통해 처리하지 않는 사전 필터링되거나, 신뢰할 수 있거나, 빠르게 전달된 플로우에는 엘리펀트 플로우 탐지를 적용할 수 없습니다. Snort에서 엘리펀트 플로우를 탐지하므로 암호화된 트래픽에는 엘리펀트 플로우 탐지를 적용할 수 없습니다.

단계 **1** 액세스 제어 정책 편집기에서 패킷 플로우 라인 끝에 있는 **More(**더 보기**)** 드롭다운 화살표에서 **Advanced Settings(**고급 설정**)**를 클릭합니다. 그런 다음 **Elephant Flow Settings(**엘리펀트 플로우 설정**)** 옆에 있는 **Edit(**편집**)**( )을 클릭합니다.

보기 아이콘**(View(**보기**)** ( ))이 대신 표시되는 경우에는 설정이 상위 정책에서 상속되거나 설정을 수정할 권한이 없는 것입니다. 구성이 잠금 해제되어 있으면 **Inherit from base policy(**기본 정책에서 상속**)**의 선택을 취소하여 수정을 활성화합니다.

그림 ***1:*** 엘리펀트 플로우 탐지 구성



단계 **2** **Elephant Flow Detection(**엘리펀트 플로우 탐지**)** 토글 버튼은 기본적으로 활성화되어 있습니다. 플로우 바이트 및 플로우 지속 시간의 값을 구성할 수 있습니다. 설정된 값을 초과하면 엘리펀트 플로우 이벤트가 생성됩니다.

단계 **3** 엘리펀트 플로우를 교정하려면 **Elephant Flow Remediation(**엘리펀트 플로우 교정**)** 토글 버튼을 활성화합니다.

단계 **4** 엘리펀트 플로우의 교정 기준을 설정하려면 CPU 사용률(%), 고정 기간의 지속 시간 및 패킷 삭제율(%) 값을 구성합니다.

단계 **5** 엘리펀트 플로우 교정이 구성된 기준을 충족하는 경우 다음 작업을 수행할 수 있습니다.

1. **Bypass the flow(**플로우 우회**)** - 선택한 애플리케이션 또는 필터에 대해 Snort 검사를 우회하려면 이 버튼을 활성화합니다. 다음 중에서 선택합니다.

   - **All applications including unidentified applications(**알 수 없는 애플리케이션을 포함한 모든 애플리케이션**)** - 모든 애플리케이션 트래픽을 우회하려면 이 옵션을 선택합니다. 이 옵션을 구성하는 경우 어떤 플로우의 스로틀 작업(속도 제한)도 구성할 수 없습니다.

   - **Select Applications/Filters(**애플리케이션/필터 선택**)** - 트래픽을 우회할 애플리케이션 또는 필터를 선택하려면 이 옵션을 선택합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드의 액세스 제어 규칙 장에 있는 애플리케이션 조건 및 필터 구성 주제를 참조하십시오.

2. **Throttle flow(**플로우 제한**)** – 플로우에 속도 제한을 적용하고 플로우를 계속 검사하려면 이 버튼을 활성화합니다. 애플리케이션 또는 필터를 선택하여 Snort 검사를 우회하고 나머지 플로우를 제한할 수 있습니다.

참고 제한된 엘리펀트 플로우에서 시스템이 위협을 받지 않는 경우(즉, Snort 패킷 삭제율이 구성된 임계값보다 작은 경우) 스로틀이 자동으로 제거됩니다. 따라서 속도 제한도 제거됩니다.

다음과 같은 Threat Defense 명령을 사용하여 제한된 엘리펀트 플로우에서 스로틀을 수동으로 제거할 수도 있습니다.

- **clear efd-throttle <5-tuple/all> bypass** — 이 명령은 제한된 엘리펀트 플로우에서 스로틀을 제거하고 Snort 검사를 우회합니다.
- **clear efd-throttle <5-tuple/all>** — 이 명령은 제한된 엘리펀트 플로우에서 스로틀을 제거하고 Snort 검사를 계속합니다. 이 명령을 사용하면 엘리펀트 플로우 교정을 건너뛰게 됩니다.

  이러한 명령에 대한 자세한 내용은 Cisco Secure Firepower Threat Defense 명령 참조에 나와 있습니다.

주의 Cisco Firepower 2100 Series 디바이스에서는 엘리펀트 플로우에 대한 작업 수행(플로우 우회 및 제한)이 지원되지 않습니다.

단계 **6** **Remediation Exemption Rule(**교정 제외 규칙**)** 섹션에서 **Add Rule(**규칙 추가**)**을 클릭하여 교정에서 제외할 플로우에 대한 L4 ACL(액세스 제어 목록) 규칙을 설정합니다.

단계 **7** **Add Rule(**규칙 추가**)** 창에서 **Networks(**네트워크**)** 탭을 사용하여 네트워크 세부 정보(소스 네트워크와 대상 네트워크)를 추가합니다. **Ports(**포트**)** 탭에서 소스 포트와 목적지 포트를 추가합니다.

엘리펀트 플로우가 탐지되고 정의된 규칙과 일치하는 경우, **Connection Events(**연결 이벤트**)**의 **Reason(**이유**)** 열 헤더에서 **Elephant Flow Exempted(**엘리펀트 플로우 제외**)**라는 이유가 있는 이벤트가 생성됩니다.

단계 **8** **Remediation Exemption Rule(**교정 제외 규칙**)** 섹션에서 교정 작업에서 제외되는 플로우를 볼 수 있습니다.

단계 **9** **OK(**확인**)**를 클릭하여 엘리펀트 플로우 설정을 저장합니다.

단계 **10** **Save(**저장**)**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

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

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

- 엘리펀트 플로우
- 엘리펀트 플로우 제한
- 엘리펀트 플로우 신뢰

주의 엘리펀트 플로우 탐지를 단독으로 활성화하면 엘리펀트 플로우에 대한 연결 이벤트가 생성되지 않습니다. 연결 이벤트가 이미 다른 이유로 로깅되어 있고 플로우가 엘리펀트 플로우인 경우 **Reason(**사유**)** 필드에 이 정보가 포함됩니다. 그러나 모든 엘리펀트 플로우를 로깅하려면 해당 액세스 제어 규칙에서 연결 로깅을 활성화해야 합니다.

자세한 내용은 Cisco Secure Firewall 엘리펀트 플로우 탐지를 참조하십시오.