연결 로깅

다음 주제에서는 모니터링하는 네트워크 상의 호스트가 실행한 연결을 기록하도록 Firepower System을 설정하는 방법을 설명합니다.

연결 로깅 정보

시스템은 자신의 매니지드 디바이스가 탐지한 연결의 로그를 생성할 수 있습니다. 이러한 로그를 연결 이벤트라고 합니다. 규칙 및 정책의 설정은 로깅할 연결의 종류, 로깅을 실행할 시기, 데이터를 저장할 위치를 세부적으로 제어할 수 있도록 합니다. *Security Intelligence(*보안 인텔리전스*)* 이벤트라는 특수한 연결 이벤트는 평판 기반 Security Intelligence(보안 인텔리전스) 기능이 차단한 연결을 나타냅니다.

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

조직의 보안 및 컴플라이언스 요구 사항에 따라 연결을 로깅해야 합니다. 연결 로깅을 설정할 때는 시스템이 여러 가지 이유로 연결을 로깅할 수 있으며, 따라서 한 곳의 로깅을 비활성화해도 일치하는 연결이 로깅되지 않는 것은 아님을 유의하십시오.

연결 이벤트에 있는 정보는 트래픽 특성, 연결을 마지막으로 처리한 설정 등의 다양한 요소에 따라 달라집니다.

참고 내보낸 NetFlow 기록에서 생성한 연결 데이터를 이용해, 매니지드 디바이스가 수집한 연결 로그를 보완할 수 있습니다. 이는 Firepower System 매니지드 디바이스가 모니터링할 수 없는 네트워크에서 NetFlow 지원 라우터 또는 기타 디바이스를 구축한 경우에 특히 유용합니다.

관련 항목

Firepower System의 Netflow 데이터

항상 로깅되는 연결

연결 이벤트 스토리지를 비활성화하지 않는 한, 시스템은 다른 로깅 설정과 관계없이 다음의 연결 종료 이벤트를 Firepower Management Center 데이터베이스에 자동으로 저장합니다.

침입과 연관된 연결

시스템은 연결이 액세스 제어 정책의 기본 작업에 의해 처리되지 않는 한, 침입 이벤트와 연관된 연결을 자동으로 로깅합니다.

액세스 제어 기본 작업과 관련된 침입 정책이 침입 이벤트를 생성할 때 시스템은 결합된 연결의 종료를 자동으로 로깅하지 않습니다. 대신, 사용자는 반드시 기본 작업 연결 로깅을 명시적으로 활성화해야 합니다. 이는 사용자가 연결 데이터를 로깅하는 것을 원하지 않을 때 침입 방지 전용 배포에 유용합니다.

그러나 기본 작업에 대한 연결 시작 로깅을 활성화하면, 시스템은 연결의 시작을 로깅하는 것 이외에도 관련 침입 정책이 작동을 이끌어낼 때 연결 종료를 분명히 로깅합니다.

파일 및 악성코드 이벤트와 연관된 연결

시스템은 파일 및 악성코드 이벤트와 연관된 연결을 자동으로 로깅합니다.

참고 클라이언트와 서버에 지속적인 연결이 설정되어 있기 때문에 NetBIOS-SSN(SMB) 트래픽 검사에 의해 생성된 파일 이벤트가 즉시 연결 이벤트를 생성하지는 않습니다. 시스템은 클라이언트 또는 서버가 세션을 종료한 후 연결 이벤트를 생성합니다.

지능형 애플리케이션 우회와 연관된 연결

시스템은 우회했거나 우회했을 가능성이 있는 IAB 관련 연결을 자동으로 로깅합니다.

모니터링되는 연결

트래픽이 다른 어느 규칙과도 일치하지 않고 기본 작업 로깅을 사용자가 활성화하지 않은 경우에도, 시스템은 모니터링되는 트래픽의 연결 종료를 로깅합니다. 자세한 내용은 모니터링된 연결에 대한 로깅, 4 페이지를 참고하십시오.

로깅할 수 있는 기타 연결

중요한 연결만 로깅하려면 규칙별로 연결 로깅을 활성화합니다. 규칙에 대한 연결 로깅을 활성화할 경우, 시스템은 해당 규칙에서 처리하는 모든 연결을 로깅합니다.

정책 기본 작업이 처리하는 연결을 로깅할 수도 있습니다. 규칙 또는 기본 작업(액세스 제어의 경우, 규칙의 검사 설정)에 따라 로깅 옵션이 달라집니다.

SSL 정책**:** 규칙 및 기본 작업

SSL 규칙 또는 SSL 정책 기본 작업과 일치하는 연결을 로깅할 수 있습니다.

차단된 연결의 경우 시스템에서 즉시 세션을 종료하고 이벤트를 생성합니다. 모니터링된 연결 및 액세스 제어 규칙으로 전달하는 연결의 경우 시스템에서 세션 종료 시 이벤트를 생성합니다.

액세스 제어 정책**:** 보안 인텔리전스 결정

평판 기능 보안 인텔리전스 기능에 의해 연결이 차단될 때마다 해당 연결을 로깅할 수 있습니다.

원한다면 보안 인텔리전스 필터링에 모니터 한정 설정을 사용할 수 있으며, 이는 수동 구축에서 권장됩니다. 이를 통해 시스템은 차단되었을 수도 있지만 여전히 일치를 로깅하는 연결을 추가로 분석할 수 있습니다. 보안 인텔리전스 모니터링을 사용하면 또한 사용자가 보안 인텔리전스 정보를 사용하여 트래픽 프로파일을 작성할 수 있습니다.

보안 인텔리전스 필터링의 결과로 연결 이벤트를 로깅할 때 시스템은 일치하는 보안 인텔리전스 이벤트도 로깅합니다. 이 이벤트는 사용자가 별도로 보고 분석할 수 있는 특수한 연결 이벤트이며 별도로 저장되고 잘립니다. 연결에서 일치하는 IP 주소를 식별할 수 있도록 **Analysis(**분석**)** > **Connections(**연결**)** 메뉴 아래 페이지의 테이블에서 차단된 IP 주소 옆의 호스트 아이콘과 모니터링되는 IP 주소 옆의 호스트 아이콘은 약간 다르게 보입니다.

액세스 제어 정책**:** 규칙 및 기본 작업

액세스 제어 규칙 또는 액세스 제어 정책 기본 작업과 일치하는 연결을 로깅할 수 있습니다.

관련 항목

규칙 및 정책 작업이 로깅에 미치는 영향, 3 페이지

규칙 및 정책 작업이 로깅에 미치는 영향

연결 이벤트에는 어느 구성이 트래픽을 처리했는지를 포함하여 연결이 로깅된 이유에 관한 메타데이터가 포함됩니다. 연결 로깅, 규칙 작업, 정책 기본 작업을 구성할 수 있는 경우, 시스템이 일치하는 트래픽을 검사하고 처리하는 방법뿐 아니라 일치하는 트래픽에 대한 상세정보를 로깅할 수 있는 시기와 방법도 결정하십시오.

관련 항목

TLS/SSL 규칙 작업
액세스 제어 규칙 작업
연결 및 보안 인텔리전스 이벤트 필드

모니터링된 연결에 대한 로깅

트래픽이 다른 어느 규칙과도 일치하지 않고 기본 작업 로깅을 사용자가 활성화하지 않은 경우에도 시스템은 항상 다음 구성과 일치하는 트래픽의 연결 종료를 로깅합니다.

- 보안 인텔리전스 — 모니터링(또한 보안 인텔리전스도 생성)하도록 설정된 차단 목록
- SSL 규칙 — 모니터링 작업
- 액세스 제어 규칙 — 모니터링 작업

시스템은 단일 연결이 모니터 규칙과 일치할 때마다 별도의 이벤트를 생성하지 않습니다. 단일 연결이 여러 모니터 규칙과 일치할 수 있으므로 각 연결 이벤트는 일치하는 첫 번째 SSL 모니터 규칙뿐 아니라 연결과 일치하는 처음 8개의 모니터 액세스 제어 규칙에 대한 정보를 포함하고 표시합니다.

마찬가지로, 사용자가 외부 syslog 또는 SNMP 트랩 서버에 연결 이벤트를 보낼 경우, 시스템은 단일 연결이 모니터링 규칙에 일치할 때마다 별도의 경고를 보내지는 않습니다. 그보다, 연결 종료 시 시스템이 보내는 경고는 연결과 일치하는 모니터링 규칙에 관한 정보를 포함합니다.

신뢰할 수 있는 연결에 대한 로깅

다음 규칙 및 작업과 일치하는 트래픽을 포함하는 신뢰할 수 있는 연결의 시작과 종료를 로깅할 수 있습니다.

- 액세스 제어 규칙 — 신뢰 작업
- 액세스 제어 기본 작업 — 모든 트래픽 신뢰

참고 신뢰할 수 있는 연결을 로깅할 수 있더라도 로깅하지 않는 것이 좋습니다. 신뢰할 수 있는 연결은 심층 검사 또는 검색 대상이 아니므로 신뢰할 수 있는 연결 이벤트에는 제한된 정보가 포함되어 있기 때문입니다.

첫 번째 패킷의 신뢰 규칙에 의해 탐지된 TCP 연결은 연결 종료 이벤트만 생성합니다. 시스템에서는 최종 세션 패킷이 끝난 지 한 시간 후에 이벤트를 생성합니다.

시스템은 신뢰 액세스 제어 규칙이 처리하는 TCP 연결을 연결을 탐지한 디바이스에 따라 다르게 로깅합니다.

- 7000 및 8000 Series 디바이스의 경우, 첫 번째 패킷에서 신뢰 규칙에 의해 탐지된 TCP 연결은 선행 활성 모니터 규칙의 유무에 따라 다른 이벤트를 생성합니다. 모니터 규칙이 활성 상태일 경우, 시스템은 패킷을 평가하고 연결 시작 및 종료 이벤트를 모두 생성합니다. 활성 상태의 모니터 규칙이 없을 경우, 시스템은 연결 종료 이벤트만 생성합니다.
- 그 밖의 모든 모델에서는 첫 번째 패킷에서 신뢰 규칙에 의해 탐지된 TCP 연결이 연결 종료 이벤트만 생성합니다. 시스템에서는 최종 세션 패킷이 끝난 지 한 시간 후에 이벤트를 생성합니다.

차단된 연결에 대한 로깅

다음 규칙 및 작업과 일치하는 트래픽을 포함하는 차단된 연결을 로깅할 수 있습니다.

- 보안 인텔리전스 - 모니터링(보안 인텔리전스 이벤트도 생성)하도록 설정되지 않은 차단 목록
- SSL 규칙 — 차단 및 차단 후 재설정
- SSL 기본 작업 — 차단 및 차단 후 재설정
- 액세스 제어 규칙 — 차단, 차단 후 재설정, 인터랙티브 차단
- 액세스 제어 기본 작업 — 모든 트래픽 차단

인라인이 구축된(즉, 라우팅, 스위칭 또는 투명 인터페이스 혹은 인라인 인터페이스 페어링을 사용하는) 디바이스만 트래픽을 차단할 수 있습니다. 차단된 연결이 수동 배포에서 실제로 차단되는 것은 아니기 때문에, 시스템은 각 차단된 연결에 대한 여러 연결 시작 이벤트를 보고할 수 있습니다.

주의 DoS(서비스 거부) 공격 중에 차단된 TCP 연결을 로깅하는 경우 시스템 성능에 영향을 미칠 수 있으며, 데이터베이스가 유사한 다수의 이벤트로 가득 찰 수 있습니다. Block(차단) 규칙에 대한 로깅을 활성화하기 전에, 해당 규칙이 인터넷에 연결된 인터페이스 또는 DoS 공격에 취약한 다른 인터페이스의 트래픽을 모니터링하고 있는지 여부를 고려하시기 바랍니다.

차단된 연결의 연결 시작 또는 종료 로깅

차단된 연결을 로깅할 때 그 로깅 방식은 연결이 차단된 이유에 따라 달라집니다. 연결 로그를 기반으로 상관관계 규칙을 구성할 때 이 점을 기억해야 합니다.

- 암호화된 트래픽을 차단하는 SSL 규칙 및 SSL 정책 기본 작업의 경우, 연결 종료 이벤트가 로깅됩니다. 이는 세션의 첫 번째 패킷을 사용하여 연결의 암호화 여부를 확인할 수 없기 때문입니다.
- 다른 차단 작업은 연결 시작 이벤트가 로깅됩니다. 일치하는 트래픽은 추가 검사 없이 거부됩니다.

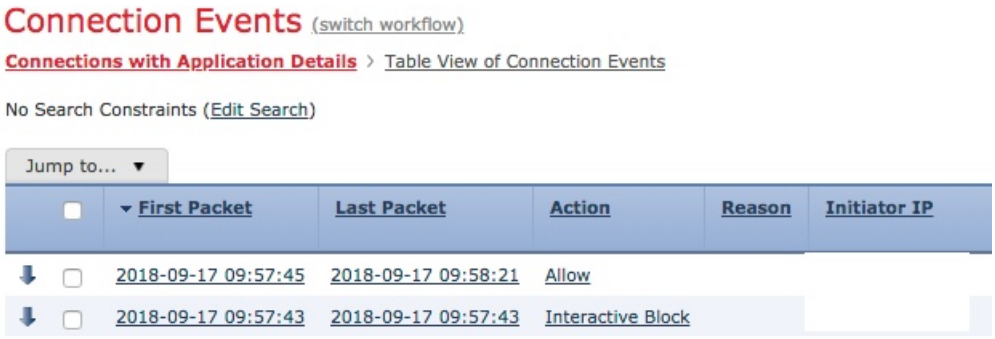
우회된 인터랙티브 차단 로깅

사용자가 금지된 웹사이트로 이동할 때 경고 페이지가 표시되도록 하는 인터랙티브 차단 액세스 제어 규칙을 사용하여 연결 종료 로깅을 구성할 수 있습니다. 이는 사용자가 경고 페이지를 클릭할 경우, 이 연결은 시스템이 모니터링 및 로깅할 수 있는 새롭게 허용된 연결로 간주되기 때문입니다.

따라서 인터랙티브 차단 또는 인터랙티브 차단 후 재설정 규칙과 일치하는 패킷의 경우, 시스템은 다음 연결 이벤트를 생성할 수 있습니다.

- 사용자 요구가 초기에 차단되고 경고 페이지가 표시되는 연결 시작 이벤트. 이 이벤트에는 `인터랙티브 차단` 또는 `인터랙티브 차단 후 재설정`이라는 연결된 작업이 있습니다.
- 사용자가 경고 페이지를 통해 클릭하고 원래 요청된 페이지를 로드하는 경우, 다중 연결 시작 또는 종료 이벤트. 이 이벤트에는 `허용` 및 `사용자 우회`의 이유라는 연결된 작업이 있습니다.

  다음 그림은 허용 다음의 인터랙티브 차단의 예를 보여줍니다.



허용된 연결에 대한 로깅

다음 규칙 및 작업과 일치하는 트래픽을 포함하 허용된 연결을 로깅할 수 있습니다.

- SSL 규칙 —**Decrypt(**암호 해독**)** 작업
- SSL 규칙 —**Do not decrypt(**암호 해독 안 함**)** 작업
- SSL 기본 작업—**Do not decrypt(**암호 해독 안 함**)**
- 액세스 제어 규칙—**Allow(**허용**)** 작업
- 액세스 제어 기본 작업 —**Network Discovery Only(**네트워크 검색 전용**)** 및 침입 방지 옵션

이러한 구성에 대한 로깅을 활성화하면 연결이 기록되며 다음 단계인 검사 및 트래픽 처리를 허가(또는 지정)합니다. SSL 로깅 시 항상 연결이 종료되며, 액세스 제어 구성에서 연결 시작 로깅을 다시 할 수 있습니다.

액세스 제어 규칙 또는 기본 작업을 사용하여 트래픽을 허용하는 경우, 연결된 침입 정책을 사용하여 트래픽을 추가 검사하고 침입을 차단할 수 있습니다. 액세스 제어 규칙의 경우, 파일 정책을 사용하여 악성코드를 비롯한 금지된 파일을 탐지하고 차단할 수도 있습니다. 연결 이벤트 스토리지를 비활성화하지 않으면 시스템은 침입, 파일, 악성코드 이벤트에 연결된 허용되는 연결 대부분을 자동으로 로깅합니다. 자세한 내용은 항상 로깅되는 연결, 2 페이지를 참조하십시오.

암호화된 페이로드와의 연결은 심층 검사 대상이 아니므로 암호화된 연결의 연결 이벤트에는 제한된 정보가 포함되어 있습니다.

허용된 연결에 대한 파일 및 악성코드 이벤트 로깅

파일 정책이 파일을 탐지하거나 차단하면 다음 이벤트 중 하나를 Firepower Management Center 데이터베이스에 로깅합니다.

- 파일 이벤트 - 악성코드 파일을 포함하여 탐지되거나 차단된 파일을 나타냅니다.
- 악성코드 이벤트 - 탐지되거나 차단된 악성코드 파일만 나타냅니다.
- 회귀적 악성코드 이벤트 - 이전에 탐지된 파일에 대한 악성코드 속성이 변경되는 경우 생성됩니다.

액세스 제어 규칙마다 이 로깅을 비활성화할 수 있습니다. 파일 및 악성코드 이벤트 스토리지를 완전히 비활성화할 수도 있습니다.

참고 파일 및 악성코드 이벤트 로깅 활성화를 유지하는 것이 좋습니다.

연결 시작 또는 종료 로깅

연결은 시작 또는 종료 시에 로깅할 수 있으며, 차단된 트래픽의 경우에는 다음 예외가 적용됩니다.

- 차단된 트래픽 - 차단된 트래픽은 추가 검사 없이 즉시 거부되기 때문에, 일반적으로는 차단된 트래픽의 연결 시작 이벤트만 로깅할 수 있습니다. 로깅할 고유 연결 종료는 존재하지 않습니다.
- 블랙리스트에 포함된 암호화된 트래픽-SSL 정책에서 연결 로깅을 활성화하면 연결 시작이 아닌 연결 종료가 로깅됩니다. 이는 시스템에서 세션의 첫 번째 패킷을 사용하여 연결의 암호화 여부를 확인할 수 없고 따라서 즉시 암호화 세션을 차단할 수 없기 때문입니다.

성능을 최적화하려면, 연결의 시작 또는 종료를 로깅하시기 바랍니다. 동시에 하는 것은 안됩니다. 어떤 이유로든 연결을 모니터링하면 반드시 연결 종료가 로깅됩니다. 차단되지 않은 단일 연결의 경우 연결 종료 이벤트는 연결 시작 이벤트의 모든 정보 및 세션 과정에서 수집된 정보를 포함합니다.

다음 표에서는 연결 시작 및 연결 종료 이벤트의 차이점과 각 로깅의 장점을 설명합니다.

표 *1:* 연결 시작 이벤트와 연결 종료 이벤트 비교

	연결 시작 이벤트	연결 종료 이벤트
생성 가능 대상	연결 시작이 탐지될 때(또는 애플리케이션이나 URL 식별에 따라 이벤트가 생성되는 경우 처음 몇 개의 패킷 이후에)	시스템이 다음을 수행하는 경우 • 연결 차단을 탐지하는 경우 • 일정 시간이 지난 후 연결 종료를 탐지하지 않는 경우 • 메모리 제약 조건 때문에 더 이상 세션을 추적할 수 없는 경우
로깅 가능 대상	SSL 정책에 의해 차단된 연결을 제외한 모든 연결	대부분의 연결
포함 대상	첫 번째 패킷(또는 이벤트 생성이 애플리케이션 또는 URL ID에 의존하는 경우 처음 몇 패킷)에서 확인될 수 있는 정보만	연결 시작 이벤트의 모든 정보와 세션 기간에 트래픽을 검사하여 확인한 정보(예: 총 데이터 전송량, 연결의 마지막 패킷의 타임스탬프)

	연결 시작 이벤트	연결 종료 이벤트
유용한 경우	다음을 로깅하려는 경우 • 차단된 연결 • 연결 종료 정보가 사용자에게 상관 없기 때문에 연결의 시작 한정	다음을 원하는 경우 • SSL 정책이 처리한 암호화된 연결을 로깅하려는 경우 • 세션 기간 동안 수집된 정보에 관한 모든 종류의 상세 분석 작업을 수행하거나, 해당 정보를 사용하여 상호 규칙을 이끌어내려는 경우 • 연결 개요(집계된 연결 데이터)를 살펴보고, 그래픽 형식으로 연결 데이터를 살펴보기 트래픽 프로파일을 만들고 사용하려는 경우

Firepower Management Center 대 외부 로깅

연결 및 Security Intelligence(보안 인텔리전스) 이벤트 로그를 Firepower Management Center에 저장하는 경우, Firepower System의 보고, 분석, 데이터 상관광계 기능을 사용할 수 있습니다. 예를 들면 다음과 같습니다.

- 대시보드 및 컨텍스트 탐색기에서는 시스템에서 로깅한 연결을 그래픽 화면에서 한눈에 볼 수 있습니다.
- 이벤트 보기(Analysis(분석) 메뉴에서 사용할 수 있는 대부분의 옵션)는 시스템이 로깅한 연결에 대한 상세정보를 제공하며, 이러한 정보는 그래프 또는 표 형식 포맷으로 표시하거나 보고서로 요약할 수 있습니다.
- 트래픽 프로파일에서는 정상적인 네트워크 트래픽에 대한 프로파일을 생성하는 데 연결 데이터를 사용합니다. 그런 다음 이 프로파일을 비정상적인 동작을 탐지하고 추적하는 데 기준으로 사용할 수 있습니다.
- 상관관계 정책에서는 특정 유형의 연결 또는 트래픽 프로파일 변경에 대한 이벤트를 생성하고 응답(예: 알림, 외부 교정)을 트리거할 수 있습니다.

Firepower Management Center에서 저장할 수 있는 이벤트 숫자는 모델에 따라 달라집니다.

참고 이 기능을 사용하려면 반드시 연결을 (대부분의 경우에는 연결 시작이 아닌 연결 종료를) 로깅해야 합니다. 따라서 중요한 연결, 즉 로깅된 침입, 금지된 파일, 악성코드와 관련된 연결은 자동으로 로깅됩니다.

다음을 사용하여 외부 시스템 로그나 SNMP 트랩 서버 또는 다른 외부 툴에 이벤트를 로깅할 수도 있습니다.

- 모든 디바이스에서 외부 로깅:

  설정한 연결은 경고 응답이라고 합니다.

- FTD 디바이스에서 외부 로깅:

  시스템 로그 구성 관련 정보 및 SNMP 트랩 구성를 참조하십시오.

- 외부 로깅과 관련된 추가 옵션:

  외부 툴을 사용하여 이벤트 분석의 내용을 참조하십시오.

관련 항목

Firepower Management Center 알림 응답

연결 로깅 제한사항

다음 항목은 로깅할 수 없음:

- 8000 Series 단축 경로 규칙으로 단축 경로가 지정된 연결
- 일반 텍스트의 외부 세션, 캡슐화된 연결이 액세스 제어로 검사되는 통과 터널
- 3방향 핸드셰이크가 완료되지 않은 경우의 TCP 연결입니다.

  이러한 연결은 실행 시 Firepower 구축에 대한 서비스 거부 공격의 기회를 제공할 것으로 로깅되지는 않습니다.

  그러나 다음 해결 방법을 사용하여 실패한 연결을 모니터링하거나 디버깅할 수는 있습니다.

  - 명령줄 인터페이스에서 **show asp drops** 사용 명령을 사용합니다.

연결 이벤트에 있어야 할 정보가 존재하지 않는다면, 연결 이벤트 필드 채우기 요구 사항 및 연결 이벤트 필드에서 제공되는 정보 섹션을 참조하십시오.

이벤트가 이벤트 뷰어에 표시되는 경우

다음 내용은 모든 유형의 이벤트에 적용됩니다.

- Analysis(분석) 메뉴의 페이지를 찾는 경우에는 페이지를 새로고침해야 새 이벤트가 표시됩니다.
- 일반적으로 이벤트는 트래픽이 탐지된 시점에서 몇 초 이내에 확인할 수 있습니다. 그러나 외부의 과도한 트래픽 조건, 낮은 대역폭 네트워크에서 많은 디바이스를 관리하는 FMC, 이벤트 백업 등의 작업 중에 이벤트 처리가 일시 중지되는 등의 상황에서는 임의 지연이 발생할 수 있습니다.

연결 로깅 모범 사례

로깅하려는 연결만 로깅하려면 다음 모범 사례를 사용하십시오.

중요한 연결만 로깅하려면 액세스 제어 규칙별로 연결 로깅을 활성화합니다.

항상 로깅되는 연결

시스템이 자동으로 다음을 로깅합니다.

- 탐지된 파일, 악성코드, 침입, Intelligent Application Bypass(IAB)와 관련된 일부 연결.

  자세한 내용은 항상 로깅되는 연결, 2 페이지를 참고하십시오.

- 모니터링되는 연결.

  자세한 내용은 모니터링된 연결에 대한 로깅, 4 페이지를 참고하십시오.

로깅하지 않을 연결

다음에 대한 로깅을 활성화하지 마십시오.

- 신뢰 작업이 포함된 액세스 제어 규칙.

  신뢰할 수 있는 연결은 심층 검사 또는 검색 대상이 아니므로 신뢰할 수 있는 연결 이벤트에는 제한된 정보가 포함되어 있습니다.

- 수동 구축에서 차단 규칙에 대한 로깅을 활성화하지 마십시오. 디바이스가 인라인으로 구축되었다면 시스템이 차단했을 연결을 로깅하려면 차단 규칙 대신 모니터링 규칙을 사용합니다.

  인라인이 구축된(즉, 라우팅, 스위칭 또는 투명 인터페이스 혹은 인라인 인터페이스 페어링을 사용하는) 디바이스만 트래픽을 차단할 수 있습니다. 차단된 연결이 수동 배포에서 실제로 차단되는 것은 아니기 때문에, 시스템은 각 차단된 연결에 대한 여러 연결 시작 이벤트를 보고할 수 있습니다.

- 관심이 없는 트래픽. 예는 다음과 같습니다.
  - 신뢰할 수 있는 DNS 호스트에 대한 DNS 요청과 같은 허용되는 특정 트래픽.
  - 서비스 솔루션과 관련이 없는 인프라 트래픽.

  (앞서 언급했듯이 이 트래픽에서 위협을 계속 모니터링할 수 있습니다.)

항상 로깅되는 연결, 2 페이지에서 설명한 것처럼 위 항목에 대한 로깅을 비활성화하더라도 침입 이벤트, 악성코드, IAB는 여전히 로깅됩니다.

다른 곳에서 로깅되는 것은 로깅하지 마십시오.

다른 디바이스 또는 서비스가 네트워크 세그먼트의 연결 데이터를 로깅하고 있는 경우, Firepower Management Center에서 해당 세그먼트의 데이터에 대한 로깅을 비활성화합니다. 예는 다음과 같습니다.

- 라우터가 Firepower Management Center와 동일한 네트워크 세그먼트에서 연결 이벤트를 로깅하는 경우, 상관관계 정책 또는 트래픽 프로파일 같은 다른 목적으로 이러한 연결 이벤트를 로깅해야 하는 경우가 아니라면 Firepower Management Center에서 동일한 연결을 로깅하지 마십시오.

  상관관계 정책에 대한 자세한 내용은 상관관계 정책 및 규칙 소개를 참조하십시오. 트래픽 프로파일에 대한 자세한 내용은 트래픽 프로파일 소개의 내용을 참조하십시오.

- Stealthwatch를 사용하여 스위치와 라우터에서 보고되는 NetFlow 레코드를 활용해 잠재적인 동작 이상 징후와 의심스러운 트래픽 패턴을 식별하는 경우, 이러한 세그먼트를 모니터링하는 규칙에 대한 연결 로깅을 비활성화하고 대신 네트워크의 해당 부분에 대한 동작 분석을 Stealthwatch에 의존할 수 있습니다.

  자세한 내용은 Stealthwatch 설명서를 참조하십시오.

연결의 시작 또는 종료를 로깅합니다**(**둘 다가 아니라**).**

연결 시작 또는 종료 로깅 중에서 선택할 수 있는 경우, 연결 종료 로깅을 활성화합니다. 이것은 연결 종료가 세션 기간 동안 수집된 정보뿐 아니라 연결 시작 이벤트의 정보도 로깅하기 때문입니다.

차단된 연결을 로깅하려고 하거나 연결 종료 정보가 중요하지 않은 경우에만 연결 시작을 로깅하십시오.

자세한 내용은 연결 시작 또는 종료 로깅, 7 페이지를 참고하십시오.

차단된 트래픽에 대한 로깅

차단된 트래픽은 추가 검사 없이 즉시 거부되기 때문에 일반적으로는 연결 시작 이벤트만 로깅할 수 있습니다.

자세한 내용은 차단된 연결에 대한 로깅, 5 페이지를 참고하십시오.

외부 위치에 이벤트 로깅

회사 보안 정책에서 허용하는 경우, 다음 중 하나를 사용하여 로그를 외부 소스에 스트리밍하면 Firepower Management Center에서 디스크 공간을 절약할 수 있습니다.

- Firepower Management Center 또는 7000 또는 8000 시리즈 디바이스에서 맞춤 개발된 클라이언트 애플리케이션으로 로그를 스트리밍할 수 있는 eStreamer입니다. 자세한 내용은 *Firepower eStreamer* 통합 가이드를 참조하십시오.
- 알림 응답이라고 하는 Syslog 또는 SNMP 트랩. 자세한 내용은 Firepower Management Center 알림 응답를 참고하십시오.

이벤트 레코드의 최대 수를 지정합니다.

데이터베이스에 저장될 수 있는 레코드의 최소 및 최대 수를 고려하십시오. 예를 들어 가상 Firepower Management Center는 기본적으로 천만 개의 이벤트를 저장하지만 이벤트 최대 수는 5천만 개입니다. **System(**시스템**)** > **Configuration(**구성**)** > **Database(**데이터베이스**)**로 이동하여 필요에 맞게 크기를 조정하십시오.

모든 Firepower Management Center 모델 목록과 이벤트 데이터베이스 크기는 데이터베이스 이벤트 제한 수의 내용을 참조하십시오.

연결 이벤트에 표시되는 항목 제어

연결 이벤트에 표시되는 행 수를 지정하려면 Firepower Management Center 오른쪽 상단에서 사용자 이름을 클릭하고 **User Preferences(**사용자 환경 설정**)** > **Event View Settings(**이벤트 보기 설정**)**를 클릭합니다. 페이지당 최대 1,000개의 이벤트를 설정할 수 있습니다.

연결 이벤트 보고서 설정

연결 이벤트가 누락되지 않도록 .csv 형식의 자동화된 보고서를 설정하여 필요에 따라 일정한 간격으로 생성되도록 예약할 수 있습니다. 자세한 내용은 다음을 참고하십시오.

- 리포트 디자이너(**Analysis(**분석**)** > **Connection(**연결**)** > **Events(**이벤트**)** > **Report Designer(**리포트 디자이너**)**): 보고서 템플릿 생성 사용.
- 작업 예약(**System(**시스템**)** > **Tools(**도구**)** > **Scheduling(**예약**)**): 작업 예약 관련 정보.

연결 로깅 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자
- 액세스 관리자
- Network Admin(네트워크 관리자)

연결 로깅 설정

다음 섹션에서는 다양한 규칙 및 조건에 맞게 연결 로깅을 설정하는 방법을 설명합니다.

SSL 규칙으로 암호 해독 가능 연결 로깅

SSL 규칙은 NGIPSv 디바이스에 적용되지 않습니다.

프로시저

단계 **1** SSL 정책 편집기에서 로깅을 설정하려는 규칙 옆에 있는 수정( )을 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **2** **Logging(**로깅**)**을 클릭합니다.

단계 **3** **Log at End of Connection(**연결 종료 시 로깅**)** 확인란을 선택합니다.

모니터링되는 트래픽의 경우, 연결 종료 로깅이 필요합니다.

단계 **4** 연결 이벤트를 전송할 위치를 지정합니다.

이러한 연결 이벤트에서 Firepower Management Center 기반의 분석을 수행하려는 경우 이벤트 뷰어로 이벤트를 전송합니다. 이것은 모니터링되는 트래픽의 경우에 필요합니다.

단계 **5** **Save(**저장**)**를 클릭하여 규칙을 저장하십시오.

단계 **6** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.

보안 인텔리전스로 연결 로깅

보안 인텔리전스 정책에는 Threat Smart 라이선스 또는 Protection Classic 라이센스가 필요합니다.

프로시저

단계 **1** 액세스 제어 정책 편집기에서 **Security Intelligence(**보안 인텔리전스**)**를 클릭합니다.

단계 **2** 로깅( )을 클릭하여 다음 기준을 바탕으로 Security Intelligenge(보안 인텔리전스) 로깅을 활성화합니다.

- IP 주소 기준 - **Networks(**네트워크**)** 옆에 있는 로깅을 클릭합니다.
- URL 기준 - **URLs** 옆에 있는 로깅을 클릭합니다.
- 도메인 이름 기준 - **DNS Policy(DNS** 정책**)** 드롭다운 목록 옆에 있는 로깅을 클릭합니다.

컨트롤이 흐리게 표시되는 경우에는 상위 정책에서 설정이 상속되거나 컨피그레이션을 수정할 권한이 없는 것입니다. 구성이 잠금 해제되어 있으면 **Inherit from base policy(**기본 정책에서 상속**)**의 선택을 취소하여 수정을 활성화합니다.

단계 **3** **Log Connections(**로그 연결**)** 확인란을 선택합니다.

단계 **4** 연결 및 보안 인텔리전스 이벤트를 전송할 위치를 지정합니다.

Firepower Management Center 기반 분석을 수행하거나 차단 목록에 있는 개체를 모니터링 전용으로 설정하려면, 이벤트를 이벤트 뷰어로 전송합니다.

단계 **5** **OK(**확인**)**를 클릭하여 로깅 옵션을 설정합니다.

단계 **6** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.

액세스 제어 규칙으로 연결 로깅

어떤 규칙 작업 및 심층 검사 옵션을 선택했는가에 따라 로깅 옵션이 달라집니다(규칙 및 정책 작업이 로깅에 미치는 영향, 3 페이지 참조).

프로시저

단계 **1** 액세스 컨트롤 정책 편집기에서 로깅을 구성하려는 규칙 옆에 있는 수정( )을 클릭합니다.

보기 ( )가 대신 표시되는 경우에는 설정이 상위 정책에서 상속되거나 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **2** **Logging(**로깅**)** 탭을 클릭합니다.

단계 **3** **Log at Beginning of Connection(**연결 시작 시 로그**)** 또는 **Log at End of Connection(**연결 종료 시 로그**)** 중 원하는 로그 방식을 선택합니다.

성능을 최적화하려면, 연결의 시작 또는 종료를 로깅하시기 바랍니다. 동시에 하는 것은 안됩니다.

단계 **4** (선택 사항) **Log Files(**로그 파일**)** 확인란을 선택하여 연결과 결합된 파일 및 악성코드 이벤트를 로깅합니다.

이 옵션은 활성화된 상태로 유지하는 것이 좋습니다.

단계 **5** 연결 이벤트를 전송할 위치를 지정합니다.

- **Event Viewer(**이벤트 뷰어**)**: 이러한 연결 이벤트를 대상으로 Firepower Management Center 기반 분석을 수행하고 싶거나 규칙 작업이 **Monitor(**모니터링**)**일 경우, 연결 이벤트를 Firepower Management Center 웹 인터페이스로 전송합니다.
- **Syslog Server(**시스템 로그 서버**)**: 연결 이벤트를 Access Control Policy(액세스 컨트롤 정책)의 Logging(로깅) 탭에 설정된 시스템 로그 서버로 전송합니다(재정의한 경우는 예외).

  Show Overrides(재정의 표시**)**: 액세스 컨트롤 정책에 구성한 설정을 오버라이드하는 옵션을 표시합니다.

- **Override Severity(**심각도 재정의**)**: 이 옵션을 선택하고 규칙의 심각도를 선택하면, 해당 규칙에 대한 연결 이벤트는 Access Control Policy(액세스 컨트롤 정책)의 Logging(로깅) 탭에 설정된 심각도와는 상관없이 선택된 심각도를 갖게 됩니다.
- **Override Default Syslog Destination(**기본 시스템 로그 대상 재정의**)**: 이 규칙의 연결 이벤트에 대해 생성된 시스템 로그를 이 알림에서 지정하는 대상으로 전송합니다.

- **SNMP Trap(SNMP** 트랩**)**: 연결 이벤트는 선택된 SNMP 트랩으로 전송됩니다.

단계 **6** **Save(**저장**)**를 클릭하여 규칙을 저장하십시오.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.

정책 기본 작업으로 연결 로깅

정책의 기본 작업은 시스템이 정책 내 규칙 중 어느 것과도 일치하지 않는 트래픽을 어떻게 처리할 것인지 결정합니다(일치 및 로깅되지만 트래픽을 검사하거나 처리하지 않는의 모니터링 규칙은 예외).

SSL 정책 기본 작업의 로깅 설정은 해독 불가능한 세션을 로깅하는 방법도 제어합니다.

프로시저

단계 **1** 정책 편집기에서 **Default Action(**기본 작업**)** 드롭다운 목록 옆에 있는 로깅( )을 클릭합니다.

단계 **2** 일치하는 연결을 언제 로깅할지 지정합니다.

- Log at Beginning of Connection(연결 시작 시 로깅) — SSL 기본 작업에는 지원되지 않습니다.
- Log at End of Connection(연결 종료 시 로깅) — 액세스 제어 **Block All Traffic(**모든 트래픽 차단**)** 기본 작업을 선택한 경우 지원되지 않습니다.

성능을 최적화하려면, 연결의 시작 또는 종료를 로깅하시기 바랍니다. 동시에 하는 것은 안됩니다.

컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다. 액세스 제어 정책의 경우, 상위 정책에서 컨피그레이션을 상속할 수도 있습니다.

단계 **3** 연결 이벤트를 전송할 위치를 지정합니다.

이러한 연결 이벤트에서 Firepower Management Center 기반의 분석을 수행하려는 경우 이벤트 뷰어로 이벤트를 전송합니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

단계 **5** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.

긴 URL의 로깅 제한

HTTP 트래픽에 대한 연결 종료 이벤트는 모니터링되는 호스트가 요청한 URL을 기록합니다. 저장된 URL 문자 수를 비활성화하거나 제한하면 시스템 성능을 높일 수 있습니다. URL 로깅을 비활성화해도(어떤 문자도 보관하지 않아도) URL 필터링은 영향받지 않습니다. 시스템은 요청된 URL을 기반으로 트래픽을 필터링하며, 시스템이 해당 URL을 기록하지 않는 경우도 마찬가지입니다.

프로시저

단계 **1** 액세스 제어 정책 편집기에서 **Advanced(**고급**)**를 클릭한 다음 **General Settings(**일반 설정**)** 옆에 있는 수정( )을 클릭합니다.

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

단계 **2** 연결 이벤트에 저장하고자 하는 최대 **URL** 문자를 입력합니다.

단계 **3** **OK(**확인**)**를 클릭합니다.

단계 **4** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.