연결 및 보안 관련 연결 이벤트

다음 주제에서는 연결 및 보안 이벤트 테이블을 사용하는 방법을 설명합니다.

연결 이벤트 정보

시스템은 자신의 매니지드 디바이스가 탐지한 연결의 로그를 생성할 수 있습니다. 이러한 로그를 연결 이벤트라고 합니다. 연결 이벤트는 *Security-Related(*보안 관련*)* 연결 이벤트(평판 기반 Security Intelligence(보안 인텔리전스) 기능이 차단한 연결)를 포함합니다.

연결 이벤트는 일반적으로 다음이 탐지한 트랜잭션을 포함합니다.

- 액세스 제어 정책
- 암호 해독 정책
- 사전 필터 정책(사전 필터나 터널 규칙이 캡처함)
- DNS 차단 목록
- URL 차단 목록
- 네트워크(IP 주소) 차단 목록

규칙 및 정책의 설정은 로깅할 연결의 종류, 로깅을 실행할 시기, 데이터를 저장할 위치를 세부적으로 제어할 수 있도록 합니다.

자세한 내용은 연결 로깅를 참조하십시오.

관련 항목

보안 인텔리전스 정보

연결과 **Security-Related Connection Events**(보안 관련 연결 이벤트) 비교

Security-Related connection events(보안 관련 연결 이벤트)는 평판 기반 Security Intelligence(보안 인텔리전스) 기능으로 세션을 차단하거나 모니터링할 때마다 생성되는 연결 이벤트입니다.

그러나 모든 Security-Related Connection Events(보안 관련 연결 이벤트)에는 동일한 연결 이벤트가 존재합니다. Security-Related Connection Events(보안 관련 연결 이벤트)는 독립적으로 보고 분석할 수 있습니다. 또한 시스템은 Security-Related Connection Events(보안 관련 연결 이벤트) 이벤트를 개별적으로 저장하고 정리합니다.

시스템은 리소스 집약적인 평가를 실행하기 전에 먼저 Security Intelligence(보안 인텔리전스)를 실행합니다. 보안 인텔리전스에 의해 연결이 차단된 경우, 그 결과로 생성된 이벤트에는 시스템이 후속 평가를 통해 수집했을 수 있는 정보(예: 사용자 ID)가 포함되지 않습니다.

참고 이 가이드에서 연결 이벤트에 대한 정보는 별도로 지정하지 않는 한 Security-Related Connection Events(보안 관련 연결 이벤트)와도 관련이 있습니다.

NetFlow 연결

매니지드 디바이스에 의해 수집된 연결 데이터를 보완하기 위해 NetFlow 엑스포터가 브로드캐스트하는 레코드를 사용하여 연결 이벤트를 생성할 수 있습니다. 이는 매니지드 디바이스에 의해 모니터링되는 것과 다른 네트워크를 NetFlow 엑스포터가가 모니터링하고 있는 경우 특히 유용합니다.

시스템은 NetFlow 레코드를 단방향 연결 종료 이벤트로 Secure Firewall Management Center 데이터베이스에 로깅합니다. 이 연결에 사용 가능한 정보는 액세스 제어 정책이 탐지하는 연결의 정보와 약간 다릅니다(NetFlow와 매니지드 디바이스 데이터의 차이점 참조).

관련 항목

NetFlow 데이터

연결 요약(그래프에 대한 집계된 데이터)

시스템에서는 5분 간격으로 수집된 연결 데이터를 연결 요약으로 취합하며, 시스템에서는 이를 사용하여 연결 그래프 및 트래픽 프로필을 생성합니다. 선택적으로, 연결 요약 데이터를 기준으로 맞춤형 워크플로를 생성할 수 있으며 이는 개별 연결 이벤트에 기반한 워크플로를 사용할 때와 같은 방식으로 사용합니다.

해당하는 연결 종료 이벤트를 연결 요약 데이터로 취합할 수는 있지만, 보안 관련 연결 이벤트에 대한 연결 요약 정보가 따로 제공되지는 않습니다.

여러 연결을 취합하려면 연결의 조건은 다음을 충족해야 합니다.

- 연결의 종료를 나타냄
- 소스 및 대상 IP 주소가 동일하며, 응답자(대상) 호스트에서 동일한 포트를 사용함
- 동일한 프로토콜을 사용함(TCP 또는 UDP)

- 동일한 애플리케이션 프로토콜을 사용함
- 동일한 매니지드 디바이스나 동일한 NetFlow 엑스포터를 사용하여 탐지함

각 연결 요약에는 총 트래픽 통계 및 요약에 나와 있는 연결 수가 포함됩니다. NetFlow 엑스포터는 단방향 연결을 생성하므로, 요약의 연결 수는 NetFlow 데이터를 기준으로 모든 연결마다 2배로 증가합니다.

연결 요약에는 요약의 취합된 연결과 관련된 모든 정보가 포함되지는 않습니다. 예를 들어, 클라이언트 정보는 연결 데이터를 연결 요약으로 취합하는 데 사용되지 않으므로 요약에는 클라이언트 정보가 포함되지 않습니다.

오래 실행되는 연결

모니터링되는 세션이 연결 데이터가 집계되는 5분 간격 2회 이상에 걸쳐 있는 경우, 해당 연결은 *long-running* 연결로 간주됩니다. 연결 요약의 연결 수를 계산할 때 long-running 연결이 시작된 5분 간격에 대해서만 수가 증가합니다.

또한 long-running 연결에서 이니시에이터 및 응답자가 전송한 패킷과 바이트 수를 계산할 때 각 5분 간격 동안 실제로 전송된 패킷과 바이트 수는 보고되지 않습니다. 그 대신, 시스템에서는 일정한 전송 속도를 추정하며 전송된 패킷과 바이트의 총 개수, 연결의 길이, 각 5분 간격 동안 발생한 연결의 부분을 기준으로 예측 수치를 계산합니다.

외부 응답자의 연결 요약 통합

연결 데이터를 저장하는 데 필요한 공간을 줄이고 연결 그래프의 렌더링 속도를 높이기 위해, 시스템에서는 다음과 같은 경우 연결 요약을 통합합니다.

- 모니터링되는 네트워크에 연결과 관련된 호스트 중 하나가 없는 경우
- 외부 호스트의 IP 주소를 제외하고 요약의 연결이 요약 어그리게이션 기준을 충족하는 경우

Analysis(분석) > Connections(연결) 하위 메뉴 페이지에서 연결 요약을 보고 연결 그래프 작업을 할 때 시스템은 모니터링되지 않는 호스트의 IP 주소 대신 외부 를 표시합니다.

이 어그리게이션으로 인해 외부 응답자와 관련된 연결 요약 또는 그래프에서 연결 데이터(즉, 개별 연결에 대한 액세스 데이터)의 테이블 보기로 드릴다운하려고 할 경우, 테이블 보기에 아무런 정보가 포함되지 않습니다.

연결 및 보안 관련 연결 이벤트 필드

참고 연결/Security-Related connection(보안 관련 연결) 이벤트 검색 페이지를 사용하여 연결과 관련된 이벤트를 검색할 수 없습니다.

액세스 제어 정책**(**시스템 로그**: ACPolicy)**

연결을 모니터링하는 액세스 제어 정책.

액세스 제어 규칙**(**시스템 로그**: AccessControlRuleName)**

연결을 처리한 액세스 제어 규칙 또는 기본 작업이자, 해당 연결과 일치한 최대 8개의 Monitor(모니터링) 규칙.

연결이 하나의 Monitor(모니터링) 규칙과 매칭될 경우, Secure Firewall Management Center에는 연결을 처리한 규칙의 이름이 표시되며 그 뒤에 Monitor(모니터링) 규칙 이름이 표시됩니다. 연결에 하나 이상의 Monitor(모니터링) 규칙과 매칭될 경우, 매칭되는 Monitor(모니터링) 규칙 수가 표시되며 `Default Action + 2 Monitor Rules(기본 작업 + 2개 모니터링 규칙)`가 그러한 예입니다.

팝업 창에 연결과 매칭되는 처음 8개 Monitor(모니터링) 규칙 목록을 표시하려면 ***N(***개수***)* Monitor Rules(**모니터링 규칙**)**를 클릭합니다.

작업**(**시스템 로그**: AccessControlRuleAction)**

연결을 로깅한 구성과 관련된 작업.

보안 인텔리전스로 모니터링된 연결의 경우, 작업은 연결에 의해 트리거되는 첫 번째 비 Monitor 액세스 제어 규칙 또는 기본 작업입니다. 이와 마찬가지로, Monitor(모니터링) 규칙과 매칭되는 트래픽은 항상 후속 규칙 또는 기본 규칙에 의해 처리되므로 Monitor(모니터링) 규칙에 의해 로깅된 연결과 관련된 작업은 Monitor(모니터링)가 될 수 없습니다. 그러나 Monitor(모니터링) 규칙과 매칭되는 연결에서 상관관계 정책 위반을 트리거할 수 있습니다.

작업	설명
허용	액세스 제어에 의해 명시적으로 허용되거나 사용자가 인터랙티브 차단을 우회했기 때문에 허용된 연결.
차단, 차단 및 재설정	차단된 연결. 예: • 사전 필터 정책에 의해 차단된 터널 및 기타 연결 • 보안 인텔리전스에 의해 차단된 연결. • SSL 정책에 의해 차단된 암호화된 연결. • 침입 정책에 따라 익스플로잇이 차단된 연결. • 파일 정책에 따라 파일(악성코드 포함)이 차단된 연결. 시스템이 침입 또는 파일을 차단하는 연결의 경우, 액세스 제어 Allow(허용) 규칙을 사용하여 심층 검사를 호출하더라도 시스템에 `Block(차단)`이 표시됩니다.
단축 경로	사전 필터 정책에 의해 경로가 단축된 비암호화 터널 및 기타 연결.
인터랙티브 차단, 인터랙티브 차단 후 재설정	시스템이 Interactive Block(인터랙티브 차단) 규칙을 사용해 사용자의 HTTP 요청을 초기에 차단하는 경우 로깅된 연결. 사용자가 시스템에 표시된 경고 페이지를 클릭할 경우, 해당 세션에 로깅된 추가 연결에는 Allow(허용) 작업이 포함됩니다.

작업	설명
신뢰	액세스 제어에서 신뢰하는 연결. 시스템은 기기 모델에 따라 신뢰하는 TCP 연결을 다르게 기록합니다.
기본 작업	액세스 제어 정책 기본 작업에서 처리한 연결
(비어 있음)	규칙과 일치하기에 충분한 패킷이 전달되기 전에 연결이 종료되었습니다. 이는 침입 방지 등의 액세스 제어 이외의 기능으로 인해 연결이 로깅되는 경우에만 발생할 수 있습니다.

애플리케이션 프로토콜**(**시스템 로그**: ApplicationProtocol)**

Secure Firewall Management Center 웹 인터페이스에서 이 값은 요약과 그래프를 제한합니다.

호스트 간 통신을 나타내며 연결에서 탐지되는 애플리케이션 프로토콜

애플리케이션 프로토콜 카테고리 및 태그

애플리케이션의 기능을 파악하는 데 도움이 될 수 있도록 애플리케이션의 특성을 분류하는 기준

애플리케이션 위험성

연결에서 탐지된 애플리케이션 트래픽과 관련된 위험성으로, 매우 높음, 높음, 중간, 낮음, 매우 낮음이 있습니다. 연결에서 탐지된 웹 애플리케이션의 각 유형에는 관련된 위험이 있습니다. 이 필드에는 그중 가장 높은 위험이 표시됩니다.

사업 타당성

연결에서 탐지된 애플리케이션 트래픽과 연계된 사업 타당성으로, 매우 높음, 높음, 중간, 낮음, 매우 낮음이 있습니다. 연결에서 탐지된 각 애플리케이션 유형에는 관련된 사업 타당성이 있습니다. 이 필드에는 그중 가장 낮은 값(가장 연관성이 적음)이 표시됩니다.

클라이언트 및 클라이언트 버전**(**시스템 로그**:** 클라이언트**, ClientVersion)**

연결에서 탐지된 클라이언트 애플리케이션 및 클라이언트 버전

시스템이 연결에 사용된 특정 클라이언트를 식별하지 못할 경우, 이 필드에는 애플리케이션 프로토콜 이름에 추가된 단어 "클라이언트"가 표시되어 일반 이름을 제공합니다(예:FTP 클라이언트).

클라이언트 카테고리 및 태그

애플리케이션의 기능을 파악하는 데 도움이 될 수 있도록 애플리케이션의 특성을 분류하는 기준

Connection Counter(시스템 로그 전용**)**

다른 동시 연결에서 하나의 연결을 구분하는 카운터입니다. 이 필드 자체에는 중요한 의미가 없습니다.

다음 필드는 연결 이벤트(DeviceUUID, 첫 번째 패킷 시간, 연결 인스턴스 ID, 연결 카운터)를 전체적으로 개별 식별합니다.

Connection Instance ID(시스템 로그 전용**)**

연결 이벤트를 처리한 Snort 인스턴스입니다. 이 필드 자체에는 중요한 의미가 없습니다.

다음 필드는 연결 이벤트(DeviceUUID, 첫 번째 패킷 시간, 연결 인스턴스 ID, 연결 카운터)를 전체적으로 개별 식별합니다.

ConnectionDuration(시스템 로그만 있음**)**

이 필드는 시스템 로그 필드로만 존재합니다. Secure Firewall Management Center 웹 인터페이스에서는 존재하지 않습니다. (웹 인터페이스는 First Packet and Last PAcket(첫 번째 패킷 및 마지막 패킷) 열을 사용하여이 정보를 전달합니다.)

이 필드는 연결 종료 시 로깅이 발생하는 경우에만 값을 갖습니다. 연결 시작 시스템 로그 메시지의 경우, 이 필드는 해당 시점에 값을 알 수 없으므로 출력하지 않습니다.

연결 종료 시스템 로그 메시지의 경우, 이 필드는 첫 번째 패킷과 마지막 패킷 사이의 초 수를 나타내며 짧은 연결인 경우 0이 될 수 있습니다. 예를 들어, 시스템 로그의 타임스탬프가 12:34:56이며 ConnectionDuration이 5인 경우 첫 번째 패킷은 12:34:51입니다.

연결

연결 요약의 연결 개수. 여러 연결 요약 간격에 걸쳐 있는 long-running 연결의 경우, 첫 번째 연결 요약 간격만 증가합니다. **Connections(**연결**)** 기준을 사용하여 유의미한 검색 결과를 보려면 연결 요약 페이지가 있는 맞춤형 워크플로를 사용해야 합니다.

개수

각 행에 표시되는 정보와 매칭되는 연결의 개수. 둘 이상의 동일한 행을 생성하는 제약 조건을 적용한 경우에만 **Count(**개수**)** 필드가 나타납니다. 사용자 지정 워크플로를 생성하고 **Count(**카운트**)** 열을 드릴다운 페이지에 추가하지 않은 경우, 각 연결은 개별적으로 낭려되고 패킷과 바이트는 합산되지 않습니다.

피어 암호 해독

연결된 연결에 대한 패킷을 해독하는 VPN 피어(피어의 IKE 주소)의 IP 주소입니다.

VPN 피어 IP 주소를 보려면 액세스 제어 정책 규칙이 연결 시작 및 종료 시 로깅하도록 로깅 설정을 활성화해야 합니다. 암호 해독된 트래픽에 대해 액세스 제어 정책 우회(sysopt connection permit-vpn) 옵션을 활성화하면 암호 해독된 트래픽의 세부 정보를 볼 수 없습니다.

탐지 유형**(**시스템 로그**: DetectionType)**

이 필드에는 클라이언트 애플리케이션의 탐지 소스가 표시됩니다. **AppID** 또는 **Encrypted Visibility(**암호화된 가시성**)**일 수 있습니다.

대상 포트**/ICMP** 코드**(**시스템 로그**:** 별도 필드**- DstPort, ICMPCode)**

Secure Firewall Management Center 웹 인터페이스에서 이러한 값은 요약과 그래프를 제한합니다.

세션 responder가 사용하는 포트 또는 ICMP 코드

DestinationSecurityGroup(시스템 로그 전용**)**

이 필드는 사용 가능한 경우 **DestinationSecurityGroupTag**의 숫자 값과 연결된 텍스트 값을 보유합니다. 그룹 이름을 텍스트 값으로 사용할 수 없는 경우 이 필드에는 DestinationSecurityGroupTag 필드와 동일한 정수 값이 포함됩니다.

DestinationSecurityGroupType(시스템 로그만 해당**)**

이 필드는 보안 그룹 태그를 가져온 소스를 표시합니다.

값	설명
인라인	대상 SGT 값이 패킷에서 나옴
세션 디렉토리	대상 SGT 값이 세션 디렉토리 주제를 통해 ISE에서 제공됨
SXP	대상 SGT 값이 SXP 주제를 통해 ISE에서 제공됨

대상 **SGT(**시스템 로그**: DestinationSecurityGroupTag)**

연결에 사용되는 대상의 숫자 보안 그룹 태그(SGT) 속성입니다.

대상 SGT 값은 **DestinationSecurityGroupType** 필드에 지정된 소스에서 가져옵니다.

탐지 유형

이 필드에는 클라이언트의 탐지 소스가 표시됩니다.

디바이스

Secure Firewall Management Center 웹 인터페이스에서 이 값은 요약과 그래프를 제한합니다.

연결을 탐지한 매니지드 디바이스, 또는 NetFlow 데이터에서 생성된 연결의 경우 해당 데이터를 처리하는 매니지드 디바이스.

DeviceUUID(시스템 로그만 해당**)**

이벤트를 생성한 Firepower 디바이스의 고유 식별자입니다.

다음 필드는 연결 이벤트(DeviceUUID, 첫 번째 패킷 시간, 연결 인스턴스 ID, 연결 카운터)를 전체적으로 개별 식별합니다.

DNS 쿼리**(**시스템 로그**: DNSQuery)**

연결에서 도메인 이름을 조회하기 위해 해당 이름 서버로 제출된 DNS 쿼리.

이 필드는 DNS 필터링이 활성화된 경우 URL 필터링 일치에 대한 도메인 이름을 포함할 수도 있습니다. 이 경우 URL 필드는 비어 있으며 URL 범주 및 URL 평판 필드에는 도메인과 연결된 값이 포함됩니다.

DNS 필터링에 대한 자세한 내용은 DNS 필터링: DNS 조회 중 URL 평판 및 범주 식별의 내용을 참조하십시오.

DNS 레코드 종류**(**시스템 로그**: DNSRecordType)**

연결에서 제출된 DNS 쿼리 해결에 사용된 DNS 리소스 레코드의 유형.

DNS 응답**(**시스템 로그**: DNSResponseType)**

연결에서 쿼리를 받은 경우 이름 서버로 반환되는 DNS 응답.

DNS 싱크홀 이름**(**시스템 로그**: DNS_Sinkhole)**

시스템이 연결을 재전송한 싱크홀 서버의 이름.

DNS TTL(시스템 로그**: DNS_TTL)**

DNS 서버가 DNS 리소스 레코드를 캐시하는 초 수.

도메인

연결을 탐지한 매니지드 디바이스의 도메인, 또는 NetFlow 데이터에서 생성된 연결의 경우 해당 데이터를 처리하는 매니지드 디바이스의 도메인. 이 필드는 management center에 멀티테넌시를 구성한 경우에만 표시됩니다.

피어 암호화

연결된 연결에 대한 패킷을 암호 해독하는 VPN 피어(피어의 IKE 주소)의 IP 주소입니다.

VPN 피어 IP 주소를 보려면 액세스 제어 정책 규칙이 연결 시작 및 종료 시 로깅하도록 로깅 설정을 활성화해야 합니다.

암호화된 가시성 핑거프린트**(**시스템 로그**: EncryptedVisibilityFingerprint)**

세션에 대해 EVE(Encrypted Visibility Engine)에서 탐지한 TLS 핑거프린트입니다.

암호화된 가시성 프로세스 이름**(**시스템 로그**: EncryptedVisibilityProcessName)**

EVE(Encrypted Visibility Engine)에서 분석한 TLS 클라이언트 Hello 패킷의 프로세스 또는 클라이언트입니다.

암호화된 가시성 신뢰도 점수**(**시스템 로그**: EncryptedVisibilityConfidenceScore)**

암호화된 가시성 엔진이 올바른 프로세스를 탐지한 0~100% 범위의 신뢰도 값입니다. 예를 들어, 프로세스 이름이 Firefox이고 신뢰도 점수가 80%이면 엔진이 탐지한 프로세스가 Firefox임을 80% 신뢰하는 것입니다.

암호화된 가시성 위협 신뢰도**(**시스템 로그**: EncryptedVisibilityThreatConfidence)**

암호화된 가시성 엔진에서 탐지한 프로세스에 위협이 포함된 확률 레벨입니다. 이 필드는 위협 신뢰도 점수의 값을 기준으로 대역(Very High(매우 높음), High(높음), Medium(중간), Low(낮음) 또는 Very Low(매우 낮음))을 나타냅니다.

암호화된 가시성 위협 신뢰도 점수**(**시스템 로그**: EncryptedVisibilityThreatConfidenceScore)**

암호화된 가시성 엔진에서 탐지한 프로세스에 위협이 포함된 신뢰도 값(0~100%)입니다. 위협 신뢰도 점수가 매우 높은 경우(예: 90%) Encrypted Visibility Process Name(암호화된 가시성 프로세스 이름) 필드에 "Malware(악성코드)"가 표시됩니다.

Endpoint Location(엔드포인트 위치**)**

ISE에서 식별된 사용자를 인증하기 위해 ISE가 사용되는 네트워크 디바이스의 IP 주소.

엔드포인트 프로파일**(**시스템 로그**: Endpoint Profile)**

ISE에서 식별된 사용자의 엔드포인트 디바이스 유형.

이벤트 우선 순위**(**시스템 로그만 해당**)**

연결 이벤트가 우선 순위가 높은 이벤트인지 여부입니다. 우선 순위가 높은 이벤트는 침입, 보안 인텔리전스, 파일, 악성코드 이벤트와 관련된 연결 이벤트입니다. 이 외의 이벤트는 우선 순위가 낮은 이벤트입니다.

파일**(**시스템 로그**: FileCount)**

하나 이상의 파일 이벤트와 관련된 연결에서 탐지되거나 차단된 파일(악성코드 파일 포함)의 수.

Secure Firewall Management Center 웹 인터페이스에서 파일 보기 아이콘이 파일 목록에 링크됩니다. 아이콘의 숫자는 해당 연결에서 탐지되거나 차단된 파일(악성코드 파일 포함)의 수를 나타냅니다.

첫 번째 패킷 또는 마지막 패킷**(**시스템 로그**: ConnectionDuration** 필드를 참조하십시오**.)**

세션의 첫 번째 또는 마지막 패킷이 표시된 날짜 및 시간.

첫 번째 패킷 시간**(**시스템 로그만 해당**)**

시스템이 첫 번째 패킷을 수신한 시간입니다.

다음 필드는 연결 이벤트(DeviceUUID, 첫 번째 패킷 시간, 연결 인스턴스 ID, 연결 카운터)를 전체적으로 개별 식별합니다.

HTTP 참조자**(**시스템 로그**: HTTPReferer)**

연결(다른 URL에 링크를 제공하는 웹사이트 또는 다른 URL에서 링크를 가져온 웹사이트 등)에서 탐지된 HTTP 트래픽에 대해 요청된 URL의 참조 페이지를 나타내는 HTTP 참조 페이지

HTTP 응답 코드**(**시스템 로그**: HTTPResponse)**

연결을 통해 클라이언트의 HTTP 요청에 대한 응답으로 전송된 HTTP 상태 코드

인그레스/이그레스 인터페이스**(**시스템 로그**: IngressInterface, EgressInterface)**

연결과 관련된 인그레스 또는 이그레스 인터페이스. 배포에 비대칭 라우팅 구성이 포함되어 있는 경우, 인그레스 및 이그레스 인터페이스가 동일한 인라인 쌍에 속하지 않을 수 있습니다.

인그레스/이그레스 보안 영역**(**시스템 로그**: IngressZone, EgressZone)**

연결과 관련된 인그레스 또는 이그레스 보안 영역

영역이 재지정된 캡슐화된 연결의 경우, 인그레스 필드는 원래 인그레스 보안 영역 대신 할당된 터널 영역을 표시합니다. 이그레스 필드는 공란입니다.

인그레스 가상 라우터/이그레스 가상 라우터**(**시스템 로그**: IngressVRF, EgressVRF**

가상 라우팅을 사용하는 네트워크에서 트래픽이 네트워크를 진입하거나 벗어날 때 통과하는 가상 라우터의 이름입니다.

개시자/응답자 바이트**(**시스템 로그**: InitiatorBytes, ResponderBytes)**

세션 개시자가 전송했거나 세션 응답자가 수신한 총 바이트 수.

개시자/응답자 대륙

라우팅 가능한 IP가 탐지되는 경우 세션 개시자 또는 응답자의 IP 주소와 관련된 대륙.

개시자/응답자 국가

라우팅 가능한 IP가 탐지되는 경우 세션 개시자 또는 응답자의 IP 주소와 관련된 국가. 시스템에 해당 국가의 플래그 및 ISO 3166-1 alpha-3 국가 코드 아이콘이 표시됩니다. 국가의 전체 이름을 보려면 플래그 아이콘 위에 포인터를 올려놓습니다.

개시자/응답자 **IP(**시스템 로그**: SrcIP, DstIP)**

Secure Firewall Management Center 웹 인터페이스에서 이러한 값은 요약과 그래프를 제한합니다.

세션 이니시에어터 또는 응답기의 호스트 IP 주소(DNS 확인을 활성화한 경우 호스트 이름)

이니시에이터/응답자, 소스/대상, 그리고 발신자/수신자 필드 지침, 21 페이지도 참조하십시오.

Secure Firewall Management Center 웹 인터페이스에서 호스트 아이콘은 연결을 차단한 IP 주소를 식별합니다.

일반 텍스트의 경우 사전 필터 정책, 이니시에이터 및 응답자 IP 주소에 의해 차단되거나 경로가 단축된 통과 터널은 터널 엔드포인트를 나타냅니다. 이것은 터널 어느 한쪽에 있는 네트워크 디바이스의 라우팅된 인터페이스를 말합니다.

개시자/응답자 패킷**(**시스템 로그**: InitiatorPackets, ResponderPackets)**

세션 개시자가 전송했거나 세션 응답자가 수신한 총 패킷 수.

개시자 사용자**(**시스템 로그**: User)**

Secure Firewall Management Center 웹 인터페이스에서 이 값은 요약과 그래프를 제한합니다.

세션 개시자에 로그인한 사용자. 이 필드에 **No Authentication(**인증 없음**)**이 입력된 경우, 사용자 트래픽은 다음과 같습니다.

- 관련 ID 정책 없이 액세스 제어 정책과 매칭
- ID 정책에서 모든 규칙과 매칭되지 않음

해당하는 경우 사용자 이름 앞에 `<realm>\`을 입력합니다.

이니시에이터/응답자, 소스/대상, 그리고 발신자/수신자 필드 지침, 21 페이지도 참조하십시오.

침입 이벤트**(**시스템 로그**: IPSCount)**

연결과 관련된 침입 이벤트의 수(해당되는 경우).

Secure Firewall Management Center 웹 인터페이스에서 침입 이벤트 보기 아이콘이 이벤트 목록에 링크됩니다.

IOC

이벤트가 연결과 관련된 호스트에 대해 IOC(indication of compromise)를 트리거했는지 여부.

NAT 소스/대상 **IP(**시스템 로그**: NAT_InitiatorIP, NAT_ResponderIP)**

세션 개시자 또는 응답자의 NAT 변환 IP 주소입니다.

NAT 소스/대상 포트**(**시스템 로그**: NAT_InitiatorPort, NAT_ResponderPort)**

세션 개시자 또는 응답자의 NAT 변환 포트입니다.

NetBIOS 도메인**(**시스템 로그**: NetBIOSDomain)**

세션에서 사용되는 NetBIOS 도메인

NetFlow SNMP 인풋/아웃풋

NetFlow 데이터에서 생성된 연결에서 연결 트래픽이 입력되거나 NetFlow 엑스포터를 종료하는 경우 인터페이스에 대한 인터페이스 인덱스.

NetFlow 소스/대상 자동 시스템

NetFlow 데이터에서 생성된 연결에서 트래픽 소스 또는 대상에 대한 경계 게이트웨이 프로토콜 자동 시스템 번호.

NetFlow 소스/대상 접두사

NetFlow 데이터에서 생성된 연결에서 소스 또는 대상 접두사 마스크로 AND 처리된 소스 또는 대상 IP 주소.

NetFlow 소스/대상 **TOS**

NetFlow 데이터에서 생성된 연결에서 연결 트래픽이 입력되거나 NetFlow 엑스포터를 종료하는 경우 서비스 유형(TOS) 바이트에 대한 설정.

네트워크 분석 정책**(**시스템 로그**: NAPPolicy)**

이벤드 생성과 관련된 NAP(네트워크 분석 정책) (해당되는 경우).

원본 클라이언트 국가

원래 클라이언트 IP 주소가 속하는 국가. 시스템은 이 값을 얻기 위해 XFF(X-Forwarded-For), True-Client-IP 또는 맞춤 정의된 HTTP 헤더에서 원래 클라이언트 IP 주소를 추출한 다음 GeoDB(지정학적 위치 데이터베이스)를 사용하여 국가에 매핑합니다. 이 필드에 값을 입력하려면 원래 클라이언트를 기준으로 프록시 설정된 트래픽을 처리하는 액세스 제어 규칙을 활성화해야 합니다.

원래 클라이언트 **IP(**시스템 로그**: originalClientSrcIP)**

XFF(X-Forwarded-For), True-Client-IP 또는 맞춤 정의된 HTTP 헤더의 원래 클라이언트 IP 주소. 이 필드에 값을 입력하려면 원래 클라이언트를 기준으로 프록시 설정된 트래픽을 처리하는 액세스 제어 규칙을 활성화해야 합니다.

사전 필터 정책**(**시스템 로그**: Profilter Policy)**

연결을 처리하는 사전 필터 정책.

프로토콜**(**시스템 로그**: Protocol)**

Secure Firewall Management Center 웹 인터페이스:

- 이 값은 요약과 그래프를 제한합니다.
- 이 필드는 검색 필드로만 사용할 수 있습니다.

연결에 사용된 전송 프로토콜 특정 프로토콜을 검색하려면 http://www.iana.org/assignments/protocol-numbers에 열거된 이름 또는 번호 프로토콜을 사용합니다.

QoS-적용 인터페이스

속도가 제한되는 연결에서 속도 제한이 적용되는 인터페이스 이름.

QoS-손실 개시자/응답자 바이트

속도 제한으로 인해 세션 개시자 또는 세션 응답자에서 삭제된 바이트 수.

QoS-손실 개시자/응답자 패킷

속도 제한으로 인해 세션 개시자 또는 세션 응답자에서 삭제된 패킷의 수.

QoS 정책

연결 속도를 제한하는 QoS 정책.

QoS 규칙

연결 속도를 제한하는 QoS 규칙.

이유**(**시스템 로그**: AccessControlRuleReason)**

다양한 상황에서 연결이 로깅된 이유. 전체 목록은 연결 이벤트 이유, 22 페이지의 내용을 참조하십시오.

IP Block(IP 차단), DNS Block(DNS 차단), URL Block(URL 차단) 이유와의 연결은 고유 개시자-응답자 쌍당 임계값이 15초입니다. 시스템이 이러한 연결 중 하나를 차단하는 경우, 포트 또는 프로토콜에 관계없이 다음 15초 동안 이러한 두 호스트 간에 추가로 차단된 연결에 대한 연결 이벤트는 생성되지 않습니다.

참조된 호스트**(**시스템 로그**: ReferencedHost)**

연결의 프로토콜이 HTTP, 또는 HTTPS인 경우 이 필드에는 각 프로토콜이 사용했던 호스트 이름이 표시됩니다.

SecIntMatchingIP(시스템 로그만 있음**)**

매칭되는 IP 주소.

가능한 값: **`None`** (없음), **`Destination`**(대상) 또는 **`Source`**(소스).

보안 상황**(**시스템 로그**: Context)**

여러 상황 모드에서 ASA FirePOWER가 처리한 연결의 경우 트래픽이 통과한 가상 방화벽 그룹을 식별하는 메타데이터.

보안 인텔리전스 카테고리**(**시스템 로그**: URLSICategory, DNSSICategory, IPReputationSICategory)**

연결에서 차단된 URL, 도메인 또는 IP 주소를 나타내거나 포함하는 개체의 이름. 보안 인텔리전스 카테고리는 네트워크 개체 또는 그룹, 차단 목록, 맞춤형 보안 인텔리전스 목록이나 피드, 관찰 관련 TID 카테고리, 인텔리전스 피드 내 카테고리 중 하나의 이름일 수 있습니다.

Secure Firewall Management Center 웹 인터페이스에서 DNS, 네트워크(IP 주소) 및 URL 보안 인텔리전스 연결 이벤트는 단일 카테고리 필드에 통합됩니다. 시스템 로그 메시지에서 해당 이벤트는 유형별로 지정됩니다.

보안 관련 연결 이벤트에는 보안 인텔리전스 이벤트와 침입 또는 악성코드 이벤트를 트리거한 것과 같은 기타 연결 이벤트가 포함됩니다. 보안 인텔리전스 요약 워크플로우에는 모든 보안 인텔리전스 이벤트가 범주 및 개수별로 표시됩니다. 보안 인텔리전스 범주가 없는 이벤트는 그룹화되어 개수만 표시됩니다.

Intelligence Feed 카테고리에 대한 자세한 내용은 보안 인텔리전스 카테고리를 참조하십시오.

소스 디바이스

Secure Firewall Management Center 웹 인터페이스에서 이 값은 요약과 그래프를 제한합니다.

연결 생성에 사용된 데이터를 브로드캐스트하는 NetFlow 엑스포터의 IP 주소. 매니지드 디바이스에서 연결이 탐지된 경우 이 필드에 `Firepower`가 표시됩니다.

소스 포트/**ICMP** 유형**(**시스템 로그**: SrcPort, ICMPType)**

Secure Firewall Management Center 웹 인터페이스에서 이러한 값은 요약과 그래프를 제한합니다.

세션 이니시에이터가 사용하는 포트 또는 ICMP 유형

SourceSecurityGroup(시스템 로그만 해당**)**

이 필드는 사용 가능한 경우 **SourceSecurityGroupTag**의 숫자 값과 연결된 텍스트 값을 보유합니다. 그룹 이름을 텍스트 값으로 사용할 수 없는 경우이 필드에는 SourceSecurityGroupTag 필드와 동일한 정수 값이 포함됩니다. 태그는 인라인 디바이스(소스 SGT 이름이 지정되지 않음) 또는 ISE(소스를 지정 함)에서 가져올 수 있습니다.

SourceSecurityGroupType (시스템 로그만 해당**)**

이 필드는 보안 그룹 태그를 가져온 소스를 표시합니다.

값	설명
인라인	소스 SGT 값이 패킷에서 나옴
세션 디렉토리	소스 SGT 값이 세션 디렉토리 주제를 통해 ISE에서 제공됨
SXP	소스 SGT 값은 SXP 주제를 통해 ISE에서 제공됨

소스 **SGT(**시스템 로그**: SourceSecurityGroupTag)**

연결에 사용되는 패킷의 보안 그룹 태그(SGT) 속성에 대한 숫자값 SGT는 신뢰할 수 있는 네트워크 내의 트래픽 소스 권한을 지정합니다. Cisco TrustSec 및 Cisco ISE 둘 다에서 제공되는 기능인 SGA(Security Group Access)는 패킷이 네트워크로 들어오면 속성을 적용합니다.

SSL 실제 작업**(**시스템 로그**: SSLActualAction)**

Secure Firewall Management Center 웹 인터페이스에서 이 필드는 검색 필드로만 사용됩니다.

시스템에서 검색 워크플로 페이지의 **SSL Status(SSL** 상태**)** 필드에 필드값이 표시됩니다.

시스템이 SSL 정책에서 암호화된 트래픽에 적용하는 작업.

작업	설명
차단/차단 및 재설정	차단된 암호화된 연결을 나타냅니다.
암호 해독(재서명)	다시 서명된 서버 인증서를 사용하여 암호 해독된 발신 연결을 나타냅니다.
암호 해독(대체 키)	대체된 공개 키가 있는 자체 서명된 서버 인증서를 사용하여 암호 해독된 발신 연결을 나타냅니다.
암호 해독(알려진 키)	알려진 개인 키를 사용하여 암호 해독된 수신 연결을 나타냅니다.
기본 작업	연결이 기본 작업에 의해 처리되었음을 나타냅니다.
암호해독안함	시스템이 암호 해독하지 않은 연결을 나타냅니다.

SSL 인증서 정보**(**시스템 로그**: SSLCertificate)**

Secure Firewall Management Center 웹 인터페이스에서 이 필드는 검색 필드로만 사용됩니다.

트래픽 암호화에 사용하는 공개 키 인증서에 저장된 정보로 다음을 포함합니다.

- Subject/Issuer Common Name(대상자/발급자 공용 이름)
- Subject/Issuer Organization(대상자/발급자 기관)
- Subject/Issuer Organization Unit(대상자/발급자 기관 부서)
- Not Valid Before/After(유효기간)
- Serial Number(일련 번호)
- Certificate Fingerprint(인증서 지문)
- Public Key Fingerprint(공개 키 지문)

SSL 인증서 상태**(**시스템 로그**: SSLServerCertStatus)**

이는 인증서 상태 SSL 규칙 조건을 구성한 경우에만 적용됩니다. 암호화된 트래픽이 SSL 규칙과 일치할 경우, 이 필드에는 다음 서버 인증서 상태 값 중 하나 이상이 표시됩니다.

- Self Signed(셀프 서명)
- Valid(유효)
- Invalid Signature(잘못된 서명)
- Invalid Issuer(잘못된 발급자)
- Expired(만료됨)
- Unknown(알 수 없음)

- Not Valid Yet(아직 유효하지 않음)
- Revoked(취소됨)

해독 불가능한 트래픽이 SSL 규칙과 매칭될 경우, 이 필드는 `Not Checked(확인되지 않음)`로 표시됩니다.

SSL 암호화 그룹**(**시스템 로그**: SSSLCipherSuite)**

연결을 암호화하는 데 사용되는 암호화 그룹을 나타내는 매크로 값. 암호 그룹 값 지정은 https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml의 내용을 참조하십시오.

연결에 적용된 **SSL** 암호화

이 필드는 Firepower Management Center 웹 인터페이스에서 검색 필드로만 사용할 수 있습니다.

`Yes`(예) 또는 **`no`(아니오)**를 **SSL** 검색 필드에 입력하고 TLS/SSL-암호화 또는 비암호화 연결을 확인합니다.

SSL 예상 작업**(**시스템 로그**: SSLExpectedAction)**

Secure Firewall Management Center 웹 인터페이스에서 이 필드는 검색 필드로만 사용됩니다.

유효한 SSL 규칙을 감안하여 시스템에서 트래픽 암호화에 적용할 것으로 예상되는 작업.

SSL Actual Action(SSL 실제 작업**)**에 나열된 값 중 하나를 입력합니다.

SSL 실패 이유**(**시스템 로그**: SSLFlowStatus)**

시스템이 암호화된 트래픽의 암호 해독에 실패한 이유:

- Unknown(알 수 없음)
- No Match(일치하지 않음)
- Success(TLS 필수 성공)
- Uncached Session(캐시되지 않은 세션)
- Unknown Cipher Suite(알 수 없는 암호 그룹)
- Unsupported Cipher Suite(지원되지 않는 암호 그룹)
- Unsupported SSL Version(지원되지 않는 SSL 버전)
- SSL Compression Used(SSL 압축 사용됨)
- Session Undecryptable in Passive Mode(패시브 모드에서 세션 암호 해독 불가)
- Handshake Error(핸드셰이크 오류)
- Decryption Error(암호 해독 오류)
- Pending Server Name Category Lookup(서버 이름 카테고리 조회 보류 중)
- Pending Common Name Category Lookup(공용 이름 카테고리 조회 보류 중)
- Internal Error

- Incomplete Handshake(불완전한 핸드셰이크)
- Network Parameters Unavailable(네트워크 파라미터 사용 불가)
- Invalid Server Certificate Handle(유효하지 않은 서버 인증서 처리)
- Server Certificate Fingerprint Unavailable(서버 인증서 지문 사용 불가)
- Cannot Cache Subject DN(대상자 DN 캐시 불가)
- Cannot Cache Issuer DN(발급자 DN 캐시 발가)
- Unknown SSL Version(알 수 없는 SSL 버전)
- External Certificate List Unavailable(외부 인증서 목록 사용 불가)
- External Certificate Fingerprint Unavailable(외부 인증서 지문 사용 불가)
- Internal Certificate List Invalid(내부 인증서 목록이 유효하지 않음)
- Internal Certificate List Unavailable(내부 인증서 목록 사용 불가)
- Internal Certificate Unavailable(내부 인증서 사용 불가)
- Internal Certificate Fingerprint Unavailable(내부 인증서 지문 사용 불가)
- Server Certificate Validation Unavailable(서버 인증서 검증 사용 불가)
- Server Certificate Validation Failure(서버 인증서 검증 장애)
- Invalid Action(유효하지 않은 작업)

검색 워크플로 페이지의 **SSL Status(SSL** 상태**)** 필드에 필드값이 표시됩니다.

SSL 플로우 오류

TLS/SSL 세션 도중 오류가 발생하는 경우 오류 이름 및 16진수 코드, 오류가 발생하지 않는 경우 `Success(성공)`.

SSL 플로우 플래그

암호화된 연결에 대한 처음 10개의 디버깅 수준 플래그입니다. 워크플로 페이지에서 모든 플래그를 보려면 줄임표(**...**)를 클릭합니다.).

매니지드 디바이스가 오버로드되는 경우 OVER_SUBSCRIBED라는 메시지가 표시됩니다. 자세한 내용은 TLS/SSL 초과 서브스크립션 문제 해결을 참조하십시오.

SSL 플로우 메시지

아래 키워드는 암호화된 트래픽이 TLS/SSL 핸드셰이크 중 클라이언트와 서버 간에 교환된 지정 메시지 유형과 관련되어 있음을 나타냅니다. 자세한 내용은 http://tools.ietf.org/html/rfc5246를 참조하십시오.

- HELLO_REQUEST
- CLIENT_ALERT

- SERVER_ALERT
- CLIENT_HELLO
- SERVER_HELLO
- SERVER_CERTIFICATE
- SERVER_KEY_EXCHANGE
- CERTIFICATE_REQUEST
- SERVER_HELLO_DONE
- CLIENT_CERTIFICATE
- CLIENT_KEY_EXCHANGE
- CERTIFICATE_VERIFY
- CLIENT_CHANGE_CIPHER_SPEC
- CLIENT_FINISHED
- SERVER_CHANGE_CIPHER_SPEC
- SERVER_FINISHED
- NEW_SESSION_TICKET
- HANDSHAKE_OTHER
- APP_DATA_FROM_CLIENT
- APP_DATA_FROM_SERVER
- SERVER_NAME_MISMATCH

  세션에 표시되는 서버 인증서는 대상 도메인 이름과 일치하지 않는 공통 이름 또는 SAN 값을 갖습니다.

- CERTIFICATE_CACHE_HIT

  대상 도메인 이름과 일치하는 인증서가 캐시에 있습니다.

- CERTIFICATE_CACHE_MISS

  대상 도메인 이름과 일치하는 인증서가 캐시에 없습니다.

애플리케이션이 TLS/SSL 하트비트 확장을 사용하는 경우 메시지 HEARTBEAT가 표시됩니다. 자세한 내용은 TLS 하트비트 정보를 참고하십시오.

SSL 정책**(**시스템 로그**: SSLPolicy)**

연결을 처리한 SSL 정책.

TLS 서버 ID 검색이 액세스 제어 정책 고급 설정에서 활성화되어 있고 액세스 제어 정책과 연결된 SSL 정책이 없는 경우 이 필드는 모든 SSL 이벤트에 대해 아무것도 유지하지 않습니다.

SSL 규칙**(**시스템 로그**: SSLRuleName)**

연결을 처리한 SSL 규칙 또는 기본 작업이자 해당 연결과 매칭된 첫 번째 Monitor(모니터링) 규칙입니다. 연결이 하나의 Monitor(모니터링) 규칙과 매칭된 경우, 연결을 처리한 규칙의 이름이 필드에 표시되며 그 뒤에 Monitor(모니터링) 규칙 이름이 표시됩니다.

SSLServerName(시스템 로그만 있음**)**

이 필드는 시스템 로그 필드로만 존재합니다. Secure Firewall Management Center 웹 인터페이스에서는 존재하지 않습니다.

클라이언트가 암호화된 연결을 설정한 서버의 호스트 이름.

SSL 세션 **ID(**시스템 로그**: SSLSessionID)**

TLS/SSL 핸드셰이크 도중 클라이언트와 서버 간에 협상된 16진수 Session ID.

SSL 상태

암호화된 연결을 로깅한 **SSL Actual Action(SSL** 실제 작업**)** (SSL 규칙, 기본 작업 또는 암호 해독이 불가능한 트래픽 작업)과 관련된 작업. 잠금 아이콘은 SSL 인증서 세부 정보에 링크됩니다. 인증서를 사용할 수 없는 경우(예: TLS/SSL 핸드셰이크 오류로 연결 차단), 잠금 아이콘이 흐리게 표시됩니다.

시스템이 암호화된 연결을 해독하지 못할 경우, 실행된 **SSL Actual Action(SSL** 실제 작업**)** (해독 불가능한 트래픽 작업)과 **SSL Failure Reason(SSL** 실패 이유**)**가 표시됩니다. 예를 들어, 시스템이 알 수 없는 암호 그룹으로 암호화된 트래픽을 탐지하고 추가 검사 없이 이를 허용할 경우 이 필드는 `Do Not Decrypt (Unknown Cipher Suite)`(암호 해독 하지 않음(알려지지 않은 암호화 그룹))로 표시됩니다.

암호화된 연결의 SSL 핸드셰이크가 불완전하고 시스템이 트래픽 암호 해독에 실패하면 **SSL Status(SSL** 상태**)** 필드에 `Unknown(Incomplete Handshake)`(알 수 없음(불완전한 핸드셰이크))이 표시됩니다.

이 필드를 검색할 때 **SSL Actual Action(SSL** 실제 작업**)** 중 하나 이상과 **SSL Failure Reason(SSL** 실패 이유**)**를 입력하고 시스템이 처리했거나 암호 해독에 실패한 암호화된 트래픽을 확인합니다.

SSL 대상자/발급자 국가

이 필드는 Secure Firewall Management Center 웹 인터페이스에서만 검색 필드로만 사용 가능합니다.

암호화 인증서와 관련된 대상자 또는 발급자 국가의 2자 ISO 3166-1 alpha-2 국가 코드.

SSL 티켓 **ID(**시스템 로그**: SSLTicketID)**

TLS/SSL 핸드셰이크 도중 전송된 세션 티켓 정보의 16진수 해시 값

SSLURLCategory(시스템 로그만 있음**)**

암호화된 연결에서 방문한 URL의 URL 카테고리.

이 필드는 시스템 로그 필드로만 존재합니다. Secure Firewall Management Center 웹 인터페이스에서 이 필드의 값은 URL 카테고리 열에 포함됩니다.

URL도 참조하십시오.

SSL 버전**(**시스템 로그**: SSLVersion)**

연결 암호화에 사용되는 TLS/SSL 프로토콜 버전:

- 알 수 없음
- SSLv2.0
- SSLv3.0
- TLSv1.0
- TLSv1.1
- TLSV1.2
- TLSv1.3

TCP 플래그**(**시스템 로그**: TCPFlags)**

NetFlow 데이터에서 생성된 연결에서 탐지된 TCP 플래그.

이 필드를 검색할 때 쉼표로 구분된 TCP 플래그 목록을 입력하면 이러한 플래그 중 최소한 하나를 보유한 모든 연결을 볼 수 있습니다.

시간

연결 요약에서 연결을 취합하기 위해 시스템이 사용한 5분 간격의 종료 시간. 이 필드는 검색할 수 없습니다.

총 패킷

이 필드는 검색 필드로만 사용할 수 있습니다.

연결에서 전송된 패킷의 총 수.

트래픽**(KB)**

이 필드는 검색 필드로만 사용할 수 있습니다.

연결에서 전송된 데이터의 총량(단위: 킬로바이트)

터널/사전 필터 규칙**(**시스템 로그**: Tunnel** 또는 **Profiler Rule)**

연결을 처리하는 터널 규칙, 사전 필터 규칙 또는 사전 필터 정책 기본 작업.

URL, URL 카테고리 및 **URL** 평판**(**시스템 로그**: URL, URLCategory** 및 **SSLURLCategory, URLReputation)**

세션 중에 모니터링된 호스트에서 요청한 URL, 관련 카테고리 및 평판(해당되는 경우)

이벤트에서 URL 범주 및 평판을 표시하려면 액세스 제어 정책에 해당 URL 규칙을 포함하고 **URL** 탭 아래에서 URL 범주 및 URL 평판을 사용하여 규칙을 구성해야 합니다.

URL 범주 및 평판은 URL 규칙과 매칭되기 전에 연결이 처리되면 이벤트에 표시되지 않습니다.

URL 열이 비어 있고 DNS 필터링이 활성화된 경우 DNS Query(DNS 쿼리) 필드에 도메인이 표시되고 URL 범주 및 URL 평판 값이 도메인에 적용됩니다.

시스템에서 TLS/SSL 애플리케이션을 식별하거나 차단한 경우, 요청한 URL은 암호화된 트래픽에 있으므로 시스템은 SSL 인증서를 기준으로 해당 트래픽을 식별합니다. 따라서 TLS/SSL 애플리케이션의 경우, 이 필드는 인증서에 포함된 공용 이름을 나타냅니다.

위 **SSLURLCategory**도 참조하십시오.

사용자 에이전트**(**시스템 로그**: UserAgent)**

연결에서 탐지된 HTTP 트래픽에서 추출된 사용자 에이전트 문자열 애플리케이션 정보.

VLAN ID (시스템 로그**: VLAN_ID)**

연결을 트리거한 패킷에 관련된 가장 안쪽의 VLAN ID.

VPN 작업

연결과 관련된 VPN 작업입니다.

가능한 값은 다음과 같습니다.

- **Encrypt(**암호화**)**: VPN이 로깅된 연결에 대한 트래픽을 암호화합니다. 연결을 암호화하는 VPN 피어의 IP 주소를 확인하려면 **Encrypt Peer(**피어 암호화**)** 열을 참조하십시오.
- **Decrypt(**암호 해독**)**: VPN이 로깅된 연결에 대한 트래픽을 암호 해독합니다. 연결을 암호 해독하는 VPN 피어의 IP 주소를 확인하려면 **Encrypt Peer(**피어 암호화**)** 열을 참조하십시오.
- **VPN Routing(VPN** 라우팅**)**: VPN 터널을 통해 트래픽이 전환됩니다. VPN은 연결 시작 시 암호 해독을 수행하고 연결 종료 시 암호화를 수행합니다. 연결을 암호화 및 해독하는 VPN 피어의 IP 주소를 확인하려면 **Encrypt Peer(**피어 암호화**)** 및 **Decrypt Peer(**피어 암호 해독**)** 열을 참조하십시오.

웹 애플리케이션**(**시스템 로그**: WebApplication)**

연결에서 탐지된 HTTP 트래픽의 콘텐츠 또는 요청한 URL을 나타내는 웹 애플리케이션

웹 애플리케이션이 이벤트의 URL과 매칭되지 않을 경우, 해당 트래픽은 참조 트래픽(예: 광고 트래픽)일 가능성이 높습니다. 시스템이 참조 트래픽을 탐지할 경우, 시스템은 제공되는 참조 애플리케이션을 저장하고 해당 애플리케이션을 웹 애플리케이션으로 나열합니다.

시스템이 HTTP 트래픽에서 특정 웹 애플리케이션을 식별하지 못할 경우, 이 필드는 `Web Browsing(웹 브라우징)`으로 표시됩니다.

웹 애플리케이션 카테고리 및 태그

애플리케이션의 기능을 파악하는 데 도움이 될 수 있도록 애플리케이션의 특성을 분류하는 기준

연결 및 **Security-Related Connection Event(**보안 관련 연결 이벤트**)** 필드 정보

Secure Firewall Management Center 웹 인터페이스에서 **Analysis(**분석**) > Connections(**연결**)** 하위 메뉴의 테이블 형식 및 그래픽 워크플로우를 사용하여 연결 및 Security-Related connection(보안 관련 연결) 이벤트를 보고 검색할 수 있습니다.

참고 Security-Related connection event(보안 관련 연결 이벤트)마다 별도로 저장되는 동일한 연결 이벤트가 있습니다. 모든 Security-Related connection event(보안 관련 연결 이벤트)에는 내용이 채워진 **Security Intelligence Category(**보안 인텔리전스 범주**)** 필드가 있습니다.

개별 이벤트에 사용 가능한 정보는 시스템에서 연결을 로깅한 방법, 이유 및 시기에 따라 달라질 수 있습니다.

검색 제약 조건

검색 페이지에서 별표(*****)로 표시된 필드는 연결 그래프 및 연결 요약을 제한 합니다. 연결 그래프는 연결 요약에 기반하므로, 연결 요약을 제한하는 동일한 기준은 연결 그래프도 제한합니다. 잘못된 검색 제한을 사용하여 연결 요약을 검색하고 맞춤형 워크플로의 연결 요약 페이지를 사용하여 결과를 볼 경우, 잘못된 제한은 해당 사항 없음(N/A)이라는 레이블로 표시되고 취소선이 그어집니다.

Syslog 필드

대부분의 필드는 Secure Firewall Management Center 웹 인터페이스와 syslog 메시지에 모두 표시됩니다. 나열된 동등한 syslog가 없는 필드는 syslog 메시지에서 사용할 수 없습니다. 언급한 것처럼 일부 필드는 syslog 전용이며, 그 밖의 소수의 필드는 syslog 메시지에서는 별도의 필드이지만 웹 인터페이스에서는 통합된 필드이며, 그 반대의 경우도 있습니다.

이니시에이터/응답자, 소스/대상, 그리고 발신자/수신자 필드 지침

표 *1:* 용어 비교

필드	이벤트 유형	설명
이니시에이터/응답자	연결	연결의 이니시에이터/응답자. 연결의 이니시에이터가 침입 소스 또는 악성 코드 파일의 발신자와 반드시 같을 필요는 없습니다.
소스/대상	침입	공격의 소스/대상입니다. 침입 이벤트의 소스는 연결의 이니시에이터 또는 응답자일 수 있습니다.

필드	이벤트 유형	설명
발신자/수신자 (전송 중..., 수신 중...)	파일, 악성 코드	파일 또는 악성 코드의 발신자/수신자. 파일을 업로드하거나 다운로드할 수 있으므로 파일의 발신자가 반드시 연결의 이니시에이터일 필요는 없습니다.

연결 이벤트 이유

연결 이벤트의 Reason(이유) 필드는 다음과 같은 상황에서 연결이 로깅된 이유를 표시합니다.

이유	설명
콘텐츠 제한	시스템이 Safe Search 기능과 관련된 콘텐츠 제한을 적용하기 위해 패킷을 수정했습니다.
DNS 차단	시스템에서 도메인 이름 및 보안 인텔리전스 데이터를 기준으로 하여 검사 없이 연결을 거부했습니다. DNS 차단 이유는 DNS 규칙 작업에 따라 차단, 도메인을 찾을 수 없음 또는 싱크홀과 페어링됩니다.
DNS 모니터링	시스템에서 도메인 이름 및 보안 인텔리전스 데이터를 기준으로 하여 연결을 거부해야 했지만 사용자가 시스템에서 연결을 거부하는 대신 모니터링하도록 구성했습니다.
엘리펀트 플로우	연결은 전체 시스템 성능에 영향을 미칠 만큼 충분히 큰 플로우인 엘리펀트 플로우으로 간주되기에 충분합니다. 기본적으로 엘리펀트 플로우는 1GB/10초보다 큽니다. **system support elephant-flow-detection** 명령을 사용하여 threat defense CLI에서 엘리펀트 플로우 식별을 위한 바이트 및 시간 임계값을 조정할 수 있습니다. 자세한 내용은 Cisco Secure Firewall Threat Defense 명령 참조를 참고하십시오. 참고 바이트 및 시간 임계값을 모두 초과하는 경우에만 플로우가 엘리펀트 플로우로 간주됩니다. Snort, 시스템, 물리적 코어와 같은 CPU 메트릭 등의 플로우와 기타 상호 관련된 메트릭을 상호 연결하는 맞춤형 대시보드를 생성할 수 있습니다. 자세한 내용은 시스템 모니터링 및 문제 해결 장을 참조하십시오.
엘리펀트 플로우 예외	엘리펀트 플로우가 탐지되고 교정에서 제외해야 하는 플로우에 대해 정의된 L4 ACL 규칙과 일치하는 경우
파일 차단	시스템이 전송을 차단한 파일 또는 악성코드 파일이 연결에 포함되었습니다. 파일 차단 이유는 항상 차단 작업과 페어링됩니다.
파일 맞춤형 탐지	시스템이 전송을 차단한 맞춤형 탐지 목록의 파일이 연결에 포함되었습니다.
파일 모니터링	시스템이 연결에서 특정 파일 유형을 탐지했습니다.

이유	설명
파일 재시작 허용	파일 전송이 파일 차단 또는 악성코드 차단 파일 규칙에 의해 원래 차단되었다가, 해당 파일을 허용하는 새 액세스 제어 정책이 구축된 후 HTTP 세션이 자동으로 재시작되었습니다. 이 이유는 인라인 구축에서만 표시됩니다.
파일 재시작 차단	파일 전송이 파일 탐지 또는 악성코드 클라우드 조회 파일 규칙에 의해 원래 허용되었다가, 해당 파일을 차단하는 새 액세스 제어 정책이 구축된 후 HTTP 세션이 자동으로 중지되었습니다. 이 이유는 인라인 구축에서만 표시됩니다.
인텔리전트 애플리케이션 바이패스	인텔리전트 애플리케이션 우회(IAB) 모드: • 작업이 Trust(신뢰)인 경우, IAB는 우회 모드였습니다. 일치하는 트래픽은 추가 검사 없이 통과합니다. • 작업이 Allow(허용)인 경우, IAB는 테스트 모드였습니다. 일치하는 트래픽은 추가 검사가 가능했습니다.
침입 차단	Snort2 엔진 - 시스템이 연결에서 탐지된 익스플로잇(침입 정책 위반)을 차단했거나 차단할 수도 있었음을 나타냅니다. 침입 차단 이유는 차단된 익스플로잇의 경우 차단 작업과, 차단될 수도 있었던 익스플로잇의 경우 허용과 페어링됩니다. Snort3 엔진 - "would have dropped(삭제되었을 수 있음)" 결과가 있는 경우 "Intrusion block(침입 차단)" 대신 연결 이벤트 이유가 비어 있습니다. "would have dropped(삭제되었을 수 있음)" 이벤트는 채워지는 연결 이벤트 사유와 관련하여 "Allow(허용)"과 동일하게 처리됩니다.
침입 모니터링	시스템이 연결에서 탐지된 익스플로잇을 탐지했지만 차단하지는 않았습니다. 트리거된 침입 규칙의 상태가 이벤트 생성으로 설정되어 있으면 이러한 현상이 나타납니다.
IP 차단	시스템에서 IP 주소 및 보안 인텔리전스 데이터를 기준으로 하여 검사 없이 연결을 거부했습니다. IP 차단 이유는 항상 차단 작업과 페어링됩니다.
IP Monitor	시스템에서 IP 주소 및 보안 인텔리전스 데이터를 기준으로 하여 연결을 거부해야 했지만 사용자가 시스템에서 연결을 거부하는 대신 모니터링하도록 구성했습니다.
SSL 차단	시스템에서 TLS/SSL 검사 구성에 기반하여 암호화된 연결을 차단했습니다. SSL 차단 이유는 항상 차단 작업과 페어링됩니다.
URL 차단	시스템에서 URL 및 보안 인텔리전스 데이터를 기준으로 하여 검사 없이 연결을 거부했습니다. URL 차단 이유는 항상 차단 작업과 페어링됩니다.
URL 모니터링	시스템에서 URL 및 보안 인텔리전스 데이터를 기준으로 하여 연결을 거부해야 했지만 사용자가 시스템에서 연결을 거부하는 대신 모니터링하도록 구성했습니다.

이유	설명
사용자 바이패스	시스템에서 사용자의 HTTP 요청을 처음에 차단했지만 사용자가 경고 페이지를 클릭하여 사이트를 봤습니다. 사용자 바이패스 이유는 항상 허용 작업과 페어링됩니다.

연결 이벤트 필드 채우기 요구 사항

연결 이벤트, , 보안 관련 연결 이벤트 또는 연결 요약에 사용할 수 있는 정보는 여러 요인에 따라 달라집니다.

어플라이언스 모델 및 라이선스

대다수의 기능은 대상 디바이스에서 특정 라이선스 기능을 활성화해야 하며, 특정 모델에서만 사용 가능한 기능도 많습니다.

트래픽 특성

시스템은 네트워크 트래픽에 존재하고 탐지 가능한 정보만 보고합니다. 예를 들어 이니시에이터 호스트와 연결된 사용자가 없거나, 프로토콜이 DNS, HTTP 또는 HTTPS가 아닌 연결에서 참조 호스트가 탐지되지 않을 수 있습니다.

기원/탐지 방법: 트래픽 기반 탐지 대 **NetFlow**

NetFlow 전용 필드를 제외하고, NetFlow 기록에서 사용 가능한 정보는 트래픽 기반 탐지가 생성한 정보에 비해 더욱 제한됩니다(NetFlow와 매니지드 디바이스 데이터의 차이점 참조).

평가 단계

각 유형의 트래픽 검사와 제어는 유연성과 성능을 최대화할 수 있는 방식으로 발생합니다.

예를 들어 시스템은 리소스 집약적인 평가를 실행하기 전에 먼저 보안 인텔리전스를 실행합니다. 보안 인텔리전스에 의해 연결이 차단된 경우, 그 결과로 생성된 이벤트에는 시스템이 후속 평가를 통해 수집했을 수 있는 정보(예: 사용자 ID)가 포함되지 않습니다.

로깅 방법: 연결의 시작 또는 종료

시스템이 연결을 탐지한 경우, 연결의 시작/종료(또는 두 시점 모두) 시점 중 연결을 언제 로깅할 수 있는지는 사용자가 시스템의 연결 탐지 및 처리 방식을 어떻게 구성하느냐에 따라 달라집니다.

Beginning-of-connection 이벤트에는 세션 기간 중에 트래픽을 검사하여 확인해야 하는 정보(예: 전송된 총 데이터의 양, 연결의 마지막 패킷의 타임스탬프)가 포함되지 않습니다. Beginning-of-connection 이벤트에는 세션의 애플리케이션 또는 URL 트래픽에 대한 정보가 없을 수 있으며, 세션의 암호화에 대한 세부 정보도 포함되지 않습니다. 일반적으로 Beginning-of-connection 로깅은 차단된 연결에 대한 유일한 옵션입니다.

연결 이벤트 유형**:** 개별 대 요약

연결 요약에는 취합된 연결과 관련된 모든 정보가 포함되지 않습니다. 예를 들어, 클라이언트 정보는 연결 데이터를 연결 요약으로 취합하는 데 사용되지 않으므로 요약에는 클라이언트 정보가 포함되지 않습니다.

연결 그래프는 연결 종료 로그만 사용하는 연결 요약 데이터를 기준으로 합니다. 연결 시작 데이터만 기록하도록 시스템을 설정하는 경우, 연결 그래프 및 연결 요약 이벤트 보기에 데이터가 포함되지 않습니다.

참고 보안 관련 연결 이벤트에는 보안 인텔리전스 이벤트와 침입 또는 악성코드 이벤트를 트리거한 것과 같은 기타 연결 이벤트가 포함됩니다. **Security Intelligence Summary(**보안 인텔리전스 요약**)** 워크플로우는 보안 인텔리전스 범주가 없는 보안 관련 연결 이벤트를 그룹화하고 **Security Intelligence Category(**보안 인텔리전스 범주**)** 값 없이 개수를 표시합니다.

기타 설정

연결에 영향을 주는 기타 설정으로는 다음과 같은 항목이 있습니다.

- ISE 관련 필드는 Active Directory 도메인 컨트롤러를 통해 인증한 사용자와 관련된 연결에서 ISE를 설정하는 경우에만 채워집니다. 연결 이벤트는 LDAP, RADIUS, 또는 RSA 도메인 컨트롤러를 통해 인증한 사용자의 ISE 데이터는 포함하지 않습니다.
- 보안 그룹 태그 (SGT) 필드는 ISE를 ID 소스로 설정하거나 맞춤형 SGT 규칙 조건을 추가하는 경우에만 채워집니다.
- 사전 필터 관련 필드(보안 영역 필드의 터널 영역 정보 포함)는 사전 필터 정책이 처리한 연결에서만 채워집니다.
- TLS/SSL 관련 필드는 암호 해독 정책을 통해 처리되는 암호화된 연결에서만 채워집니다. 트래픽을 암호화하지 않아도 된다면 Do Not Decrypt 규칙 작업을 사용하여 필드의 값을 확인할 수 있습니다.
- 파일 정보 필드는 파일 정책과 관련된 액세스 컨트롤 규칙이 기록한 연결에서만 채워집니다.
- 침입 정보 필드는 침입 정책과 관련되거나 기본 작업을 사용하는 액세스 컨트롤 규칙이 기록한 연결에서만 채워집니다.
- QoS 관련 필드는 속도 제한의 영향을 받는 연결에서만 채워집니다.
- Reason(원인) 필드는 사용자가 Interactive Block(인터랙티브 차단) 설정을 우회하는 경우 같은 특정 상황에서만 채워집니다.
- Domain(도메인) 필드는 Secure Firewall Management Center에 멀티테넌시를 구성한 경우에만 표시됩니다.
- 액세스 컨트롤 정책의 고급 설정에서는 HTTP 세션에서 모니터링된 호스트에서 요청한 각 URL의 연결 로그에 저장되는 특성의 수를 제어합니다. 이 설정을 사용하여 URL 로깅을 비활성화할

경우, 카테고리 및 평판 데이터가 존재하고 이를 계속 볼 수 있는 경우에도 시스템에서는 연결 로그에 개별 URL을 표시하지 않습니다.

- 연결 이벤트에서 URL 범주 및 평판을 표시하려면 액세스 제어 정책에 해당 URL 규칙을 포함하고 **URL** 탭 아래에서 URL 범주 및 URL 평판을 사용하여 규칙을 구성해야 합니다. URL 범주 및 평판은 URL 규칙과 매칭되기 전에 연결이 처리되면 이벤트에 표시되지 않습니다.

관련 항목

NetFlow와 매니지드 디바이스 데이터의 차이점

연결 이벤트 필드에서 제공되는 정보

이 항목의 표에는 시스템이 연결 및 보안 인텔리전스 필드를 채울 수 있는 경우가 나와 있습니다. 표의 열은 다음 이벤트 유형을 나타냅니다.

- 출처: 직접 - System 매니지드 디바이스에서 탐지 및 처리된 연결을 나타내는 이벤트.
- 출처: NetFlow - NetFlow 엑스포터에서 내보낸 연결을 나타내는 이벤트
- 로깅: 시작 - 시작 시에 로깅되는 연결을 나타내는 이벤트
- 로깅: 종료 - 종료 시에 로깅되는 연결을 나타내는 이벤트

표에서 "예"는 시스템이 연결 이벤트 필드를 채워야 한다는 의미가 아니라 채울 수 있다는 의미입니다. 시스템은 네트워크 트래픽에 존재하고 탐지 가능한 정보만 보고합니다. 예를 들어 TLS/SSL 관련 필드는 암호화 정책을 통해 처리되는 암호화된 연결의 기록에 대해서만 채워집니다.

연결 이벤트 필드	출처: 직접	출처: **NetFlow**	로깅: 시작	로깅: 종료
액세스 제어 정책	예	아니요	예	예
Access Control Rule	예	아니요	예	예
작업	예	아니요	예	예
Application Protocol(애플리케이션 프로토콜)	예	예	사용 가능한 경우	예
애플리케이션 프로토콜 카테고리 및 태그	예	아니요	사용 가능한 경우	예
애플리케이션 위험성	예	아니요	사용 가능한 경우	예
Business Relevance	예	아니요	사용 가능한 경우	예
클라이언트	예	아니요	사용 가능한 경우	예

연결 이벤트 필드	출처: 직접	출처: **NetFlow**	로깅: 시작	로깅: 종료
클라이언트 카테고리 및 태그	예	아니요	사용 가능한 경우	예
클라이언트 버전	예	아니요	사용 가능한 경우	예
연결	예	예	아니요	예
개수	예	예	예	예
대상 포트/ICMP 유형	예	예	예	예
Destination SGT(대상 SGT)	예	아니요	예	예
디바이스	예	예	예	예
도메인	예	예	예	예
DNS Query(DNS 쿼리)	예	아니요	예	예
DNS 레코드 유형	예	아니요	예	예
DNS 응답	예	아니요	예	예
DNS 싱크홀 이름	예	아니요	예	예
DNS TTL	예	아니요	예	예
이그레스 인터페이스	예	아니요	예	예
이그레스 보안 영역	예	아니요	예	예
엔드포인트 위치	예	아니요	예	예
Endpoint Profile(엔드포인트 프로파일)	예	아니요	예	예
파일	예	아니요	아니요	예
첫 번째 패킷	예	예	예	예
HTTP 참조 페이지	예	아니요	아니요	예
HTTP 응답 코드	예	아니요	예	예
인그레스 인터페이스	예	아니요	예	예
인그레스 보안 영역	예	아니요	예	예
초기자 바이트	예	예	유용하지 않음	예

연결 이벤트 필드	출처: 직접	출처: **NetFlow**	로깅: 시작	로깅: 종료
Initiator Country	예	아니요	예	예
초기자 IP	예	예	예	예
초기자 패킷	예	예	유용하지 않음	예
Initiator User	예	예	예	예
침입 이벤트	예	아니요	아니요	예
침입 정책	예	아니요	예	예
IOC(보안 침해 지표)	예	아니요	예	예
마지막 패킷	예	예	아니요	예
NetBIOS 도메인	예	아니요	예	예
NetFlow 소스/대상 자동 시스템	아니요	예	아니요	예
NetFlow 소스/대상 접두사	아니요	예	아니요	예
NetFlow 소스/대상 TOS	아니요	예	아니요	예
NetFlow SNMP 인풋/아웃풋	아니요	예	아니요	예
Network Analysis Policy	예	아니요	예	예
원본 클라이언트 국가	예	아니요	예	예
원본 클라이언트 IP	예	아니요	예	예
사전 필터 정책	예	아니요	예	예
QoS-적용 인터페이스	예	아니요	아니요	예
QoS-손실 이니시에이터 바이트	예	아니요	아니요	예
QoS-손실 이니시에이터 패킷	예	아니요	아니요	예
QoS-손실 Responder 바이트	예	아니요	아니요	예
QoS-손실 Responder 패킷	예	아니요	아니요	예
QoS 정책	예	아니요	아니요	예
QoS 규칙	예	아니요	아니요	예
이유	예	아니요	예	예
참조된 호스트	예	아니요	아니요	예

연결 이벤트 필드	출처: 직접	출처: **NetFlow**	로깅: 시작	로깅: 종료
응답기 바이트	예	예	유용하지 않음	예
Responder Country	예	아니요	예	예
응답기 IP	예	예	예	예
응답기 패킷	예	예	유용하지 않음	예
보안 상황 (ASA 전용)	예	아니요	예	예
Security Intelligence Category	예	아니요	예	예
Source Device	예	예	예	예
Source Port/ICMP Type	예	예	예	예
Source SGT(소스 SGT)	예	아니요	예	예
SSL Certificate Status	예	아니요	아니요	예
SSL Cipher Suite	예	아니요	아니요	예
SSL Flow Error	예	아니요	아니요	예
SSL Flow Flags	예	아니요	아니요	예
SSL Flow Messages	예	아니요	아니요	예
해독 정책	예	아니요	아니요	예
해독 규칙	예	아니요	아니요	예
SSL Session ID	예	아니요	아니요	예
SSL Status	예	아니요	아니요	예
SSL Version	예	아니요	아니요	예
TCP 플래그	아니요	예	아니요	예
시간	예	예	아니요	예
터널/사전 필터 규칙	예	아니요	예	예
URL	예	아니요	사용 가능한 경우	예
URL Category(URL 범주)	예	아니요	사용 가능한 경우	예

연결 이벤트 필드	출처: 직접	출처: **NetFlow**	로깅: 시작	로깅: 종료
URL Reputation(URL 평판)	예	아니요	사용 가능한 경우	예
사용자 에이전트	예	아니요	아니요	예
VLAN ID	예	아니요	예	예
웹 애플리케이션	예	아니요	사용 가능한 경우	예
웹 애플리케이션 카테고리 및 태그	예	아니요	사용 가능한 경우	예

연결 및 보안 관련 연결 이벤트 테이블 사용

Secure Firewall Management Center을(를) 사용하여 연결 또는 보안 관련 연결의 테이블을 볼 수 있습니다. 그런 다음 찾고 있는 정보에 따라 이벤트 보기를 조작할 수 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

연결 그래프에 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 이벤트의 테이블 보기에서 종료되는 미리 정의된 워크플로를 사용할 수 있습니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다.

연결 또는 보안 인텔리전스 워크플로 테이블을 사용하는 경우, 여러 일반적인 작업을 수행할 수 있습니다.

드릴다운 페이지에서 연결 이벤트를 제한할 경우, 동일한 이벤트의 패킷 및 바이트가 합산됩니다. 하지만 맞춤형 워크플로를 사용 중이고 드릴다운 페이지에 **Count(**카운트**)** 열을 추가하지 않은 경우, 이벤트가 개별적으로 나열되고 패킷과 바이트는 합산되지 않습니다.

시스템에서 생성되는 연결 이벤트가 25개를 넘는 경우, **Connection Events(**연결 이벤트**)** 테이블 보기는 얼마나 많은 이벤트 페이지를 사용할 수 있는지 표시하는 대신 여러 개 중 하나를 표시합니다.

시작하기 전에

이 작업을 수행하려면 관리자 또는 보안 분석가 사용자여야 합니다.

프로시저

단계 **1** 다음 중 하나를 선택합니다.

- **Analysis(**분석**)** > **Connections(**연결**)** > **Events(**이벤트**)** (연결 이벤트의 경우)
- **Analysis(**분석**)** > **Connections(**연결**)** > **Security-Related Events(**보안 관련 이벤트**)**

참고 테이블 대신 연결 그래프가 표시되는 경우, 워크플로 제목별로 **(**워크플로 전환**)**을 클릭하고 미리 정의된 **Connection Events(**연결 이벤트**)** 워크플로 또는 맞춤형 워크플로를 선택합니다. 미리 정의된 연결 이벤트 워크플로(연결 그래프 포함)는 연결의 테이블 보기에서 종료됩니다.

단계 **2** 다음 옵션을 이용할 수 있습니다.

- Time Range(시간 범위) - 시간 범위를 조정합니다. 이벤트가 표시되지 않는 경우에 유용합니다. 타임 윈도우 변경 참조.
- Data Source(데이터 소스)-Security Analytics and Logging(보안 애널리틱스)를 사용하여 데이터가 원격으로 저장되어 있고 데이터 소스를 변경해야 하는 충분한 이유가 있는 경우 데이터 소스를 선택합니다. 이 옵션에 대한 중요한 정보는 Secure Network Analytics 어플라이언스에 저장된 연결 이벤트로 Secure Firewall Management Center에서 작업의 내용을 참조하십시오.
- Field Names(필드 이름) - 테이블 열의 콘텐츠에 대해 자세히 알아봅니다. 연결 및 보안 관련 연결 이벤트 필드, 3 페이지 참조.

  팁 이벤트의 테이블 보기에는 여러 필드가 기본적으로 숨겨져 있습니다. 표시되는 필드를 변경하려면 임의의 열 이름에서 **x**를 클릭하여 필드 선택기를 표시합니다.

- 추가 정보 - 시스템 외부의 사용 가능한 소스에 있는 데이터를 보려면 이벤트 값을 마우스 오른쪽 버튼으로 클릭합니다. 표시되는 옵션은 데이터 유형에 따라 다르며 공개 소스를 포함합니다. 다른 소스는 구성한 리소스에 따라 달라집니다. 자세한 내용은 웹 기반 리소스를 사용한 이벤트 조사 섹션을 참조해 주십시오.
- 외부 인텔리전스 - 이벤트에 대한 정보를 수집하려면 테이블에서 이벤트 값을 마우스 오른쪽 버튼으로 클릭하고 Cisco 또는 서드파티 인텔리전스 소스에서 선택합니다. 예를 들어 Cisco Talos에서 의심스러운 IP 주소에 대한 상세정보를 얻을 수 있습니다. 표시되는 옵션은 데이터 유형 및 시스템에서 구성된 통합에 따라 달라집니다. 자세한 내용은 웹 기반 리소스를 사용한 이벤트 조사를 참고하십시오.
- 호스트 프로필 - IP 주소의 호스트 프로필을 보려면 **Host Profile(**호스트 프로필**)**을 클릭하거나 활성 IOC(Indication of Compromise) 태그가 있는 호스트의 경우에는 IP 주소 옆에 표시되는 **Compromised Host(**보안 침해된 호스트**)**를 클릭합니다.
- 사용자 프로파일 - 사용자 ID 정보를 보려면 **User Identity(**사용자 **ID)** 옆에 표시되는 사용자 아이콘 또는 IOC와 연결된 사용자라면 **Red User(**빨간색 사용자**)**를 클릭합니다.
- 파일 및 악성코드 - 연결에서 탐지되거나 차단된 악성코드를 포함한 파일을 보려면 **View Files(**파일 보기**)**을 클릭하고 연결 내에서 탐지된 파일 및 악성코드 보기, 32 페이지에 설명된 대로 계속합니다.
- 침입 이벤트 - 연결에 연결된 침입과 우선 순위 및 영향을 보려면 **Intrusion Events(**침입 이벤트**)** 열에서 **Intrusion Events(**침입 이벤트**)**을 클릭하고 연결과 관련된 침입 이벤트 보기, 34 페이지에 설명된 대로 계속합니다.

팁 하나 이상의 연결에 연결된 침입, 파일 또는 악성코드 이벤트를 빠르게 보려면 테이블의 확인란을 사용하여 연결을 선택한 다음 **Jump to(**이동**)** 드롭다운 목록에서 적절한 옵션을 선택합니다. 액세스 제어 규칙 평가 전에 차단되기 때문에 보안 인텔리전스에 의해 차단된 연결에 연결된 파일 또는 침입이 없을 수도 있습니다. 연결을 차단하기보다는 모니터링하도록 보안 인텔리전스를 구성했다면 보안 인텔리전스 이벤트의 경우에만 이 정보를 볼 수 있습니다.

- 인증서 - 연결을 암호화하는 데 사용할 수 있는 인증서에 대한 상세정보를 보려면 **SSL Status(SSL** 상태**)** 열에서 **Enabled Lock(**활성화된 잠금**)**을 클릭합니다.
- 제한 - 표시되는 열을 제한하려면 숨기려는 열 머리글의 **Close(**닫기**)** (✕)을 클릭합니다. 표시되는 팝업 창에서 **Apply(**적용**)**를 클릭합니다.

  팁 다른 열을 숨기거나 표시하려면 **Apply(**적용**)**를 클릭하기 전에 해당 확인란을 선택하거나 확인 취소합니다. 비활성화된 열을 보기에 다시 추가하려면 검색 제약 조건을 확장한 다음 Disabled Columns(비활성화된 열) 아래에서 열 이름을 클릭합니다.

- 이벤트 삭제 - (보안 관련 연결 이벤트 테이블만 해당) 현재 제한된 보기에서 일부 또는 모든 항목을 삭제하려면 삭제할 항목 옆의 확인란을 선택한 다음 **Delete(**삭제**)**를 클릭하거나 **Delete All(**모두 삭제**)**을 클릭합니다.
- 드릴다운 - 드릴다운 페이지 사용 참조.

  팁 로깅된 연결과 일치한 여러 모니터 규칙 중 하나를 사용하여 드릴다운하려면 *N* **Monitor Rules** 값을 클릭합니다. 표시되는 팝업 창에서 연결 이벤트를 제한하는 데 사용할 모니터 규칙을 클릭합니다.

- 이 페이지 탐색 - 워크플로 페이지 이동 툴 참조.
- 페이지 간 이동 - 현재 제약 조건을 유지한 상태로 현재 워크플로의 페이지 간에 이동하려면, 워크플로 페이지의 왼쪽 상단에서 해당하는 페이지 링크를 클릭합니다.
- 이벤트 보기 간 이동 - 다른 이벤트 보기로 이동하여 연결된 이벤트를 보려면 **Jump to(**이동**)**를 클릭하고 드롭다운 목록에서 이벤트 보기를 선택합니다.
- 정렬 - 워크플로의 데이터를 정렬하려면 열 제목을 클릭합니다. 정렬 순서를 반대로 하려면 열 제목을 다시 클릭합니다.

관련 항목

개요: 워크플로
이벤트 보기 구성

연결 내에서 탐지된 파일 및 악성코드 보기

파일 정책과 하나 이상의 액세스 제어 규칙을 연결할 경우, 시스템은 일치하는 트래픽에서 파일(악성코드 포함)을 탐지할 수 있습니다. 이러한 규칙에 의해 로깅된 연결과 연결된 파일 이벤트(있는 경우)

를 보려면 Analysis(분석) > Connections(연결) 메뉴 옵션을 사용하십시오. Secure Firewall Management Center에서는 파일 목록 대신 **Files(**파일**)** 열에 파일 보기()를 표시합니다. 파일 보기의 숫자는 해당 연결에서 탐지되거나 차단된 파일(악성코드 파일 포함)의 수를 나타냅니다.

모든 파일 및 악성코드 이벤트가 연결에 연결되는 것은 아닙니다. 구체적으로 말씀드리면,

- AMP for Endpoints가 탐지하는 악성코드 이벤트("엔드포인트 기반 악성코드 이벤트")는 연결에 연결되지 않습니다. 이러한 이벤트는 AMP for Endpoints 구축에서 가져옵니다.
- 많은 IMAP 지원 이메일 클라이언트는 사용자가 애플리케이션을 종료해야 종료되는 단일 IMAP 세션을 사용합니다. long-running 연결은 시스템에 의해 로깅되지만 세션에서 다운로드된 파일은 세션이 종료될 때까지 연결에 연결되지 않습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

시작하기 전에

이 작업을 수행하려면 관리자 또는 보안 분석가 사용자여야 합니다.

프로시저

단계 **1** **Analysis(**분석**) > Connections(**연결**)**로 이동하여 관련 옵션을 선택합니다.

단계 **2** 연결 이벤트 테이블을 사용할 때 **View Files(**파일 보기**)**를 클릭합니다.
연결에서 탐지된 파일 목록과 그 유형 및 (해당되는 경우) 악성코드 속성이 포함된 팝업 창이 표시됩니다.

단계 **3** 다음 옵션을 이용할 수 있습니다.

- 보기 - 파일 이벤트의 테이블 보기를 보려면 파일의 **View(**보기**)**를 클릭합니다.
- 보기 - 악성코드 이벤트의 테이블 보기에서 세부 사항을 보려면 악성코드 악성코드 파일의 **View(**보기**)**를 클릭합니다.
- 추적 - 네트워크를 통한 파일의 전송을 추적하려면 파일의 **Trajectory(**경로 전송**)**를 클릭합니다.
- 보기 - AMP for Networks에 의해 탐지된 모든 연결의 탐지된 파일 또는 악성코드 이벤트("네트워크 기반 악성코드 이벤트")의 세부 정보를 보려면 **View File Events(**파일 이벤트 보기**)** 또는 **View Malware Events(**악성코드 이벤트 보기**)**를 클릭합니다.

관련 항목

개요: 워크플로
이벤트 보기 구성

연결과 관련된 침입 이벤트 보기

침입 정책을 액세스 제어 규칙 또는 기본 작업과 연결할 경우, 시스템은 일치하는 트래픽에서 익스플로잇을 탐지할 수 있습니다. 로깅된 연결에 연결된 침입 이벤트(있는 경우)와 우선 순위 및 영향을 보려면 Analysis(분석) > Connections(연결) 메뉴 옵션을 사용하십시오.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

시작하기 전에

이 작업을 수행하려면 관리자 또는 보안 분석가 사용자여야 합니다.

프로시저

단계 **1** **Analysis(분석) > Connections(연결)**로 이동하여 관련 옵션을 선택합니다.

단계 **2** 연결 이벤트 테이블을 사용할 때 **Intrusion Events(침입 이벤트)** 열에서 **Intrusion Events(침입 이벤트)**를 클릭합니다.

단계 **3** 나타나는 팝업 창에서 다음 옵션을 이용할 수 있습니다.

- **Listed Event's View(나열된 이벤트의 보기)**를 클릭하여 패킷 보기에서 세부 정보를 확인합니다.
- **View Intrusion Events(침입 이벤트 보기)**를 클릭하여 연결에 연결된 모든 침입 이벤트에 대한 세부 정보를 봅니다.

관련 항목

개요: 워크플로

이벤트 보기 구성

암호화된 연결 인증서 상세정보

Analysis(분석) > Connections(연결) 메뉴 아래의 옵션을 사용하여 시스템이 처리하는 연결을 암호화하는 데 사용되는 공개 키 인증서(사용할 수 있는 경우)를 표시할 수 있습니다. 인증서에는 다음 정보가 포함됩니다.

표 *2:* 암호화된 연결 인증서 상세정보

속성	설명
Subject/Issuer Common Name(주체/발급자 공용 이름)	인증서 주체 또는 인증서 발급자의 호스트 및 도메인 이름입니다.
Subject/Issuer Organization(주체/발급자 조직)	인증서 주체 또는 인증서 발급자가 속한 조직입니다.

속성	설명
Subject/Issuer Organization Unit(주체/발급자 조직 단위)	인증서 주체 또는 인증서 발급자가 속한 조직 단위입니다.
Not Valid Before/After(유효기간)	인증서가 유효한 날짜입니다.
일련 번호	발급 CA가 할당한 일련번호입니다.
Certificate Fingerprint(인증서 지문)	인증서를 인증하는 데 사용되는 SHA 해시 값입니다.
Public Key Fingerprint(공개 키 지문)	인증서 내에 있는 공개 키를 인증하는 데 사용되는 SHA 해시 값입니다.

관련 항목

개요: 워크플로

이벤트 보기 구성

연결 요약 페이지 보기

Connection Summary(연결 요약) 페이지는 연결 이벤트에 대한 검색에 의해 제한되는 맞춤형 역할이 있고 Connection Summary(연결 요약) 페이지에 대한 명시적인 메뉴 기반 액세스 권한이 부여된 사용자에게만 표시됩니다. 이 페이지는 다양한 기준으로 구성된 모니터링되는 네트워크에서의 활동 그래프를 제공합니다. 예를 들어 Connections over Time 그래프에는 사용자가 선택한 간격 동안 모니터링되는 네트워크에서의 총 연결 수가 표시됩니다.

연결 요약 그래프에서는 연결 그래프에서 수행할 수 있는 작업을 거의 모두 동일하게 수행할 수 있습니다. 하지만 Connection Summary(연결 요약) 페이지의 그래프는 집계된 데이터를 기반으로 하기 때문에 그래프가 기반하는 개별 연결 이벤트를 검사할 수는 없습니다. 즉, 연결 요약 그래프에서는 연결 데이터 테이블 보기로 드릴다운할 수 없습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** **Overview(**개요**)** > **Summary(**요약**)** > **Connection Summary(**연결 요약**)**을(를) 선택합니다.

단계 **2** **Select Device(**디바이스 선택**)** 목록에서 요약을 보려는 디바이스를 선택하거나 **All(**모두**)**을 선택하여 모든 디바이스의 요약을 봅니다.

단계 **3** 연결 그래프를 조작하고 분석하려면 연결 이벤트 그래프 사용에 설명된 대로 진행합니다.

팁 기본 시간 범위에 영향을 주지 않고 추가 분석을 수행할 수 있도록 연결 그래프를 분리하려면 **View(**보기**)**를 클릭합니다.

관련 항목

사용자 역할 에스컬레이션 활성화

연결 및 보안 인텔리전스 이벤트 기록

기능	버전	세부 사항	최소 Threat Defense
새 연결 이벤트 이유 - 엘리펀트 플로우.	7.1	연결 이벤트 이유, 22 페이지의 내용을 참조하십시오.	모든
NAT 변환 IP 주소 및 포트	7.1	연결 및 보안 인텔리전스 이벤트 테이블에 4개의 새로운 필드가 추가되었습니다. • NAT 소스 IP • NAT 대상 IP • NAT 소스 포트 • NAT 대상 포트	모든
원격으로 저장된 특정 이벤트로 작업할 때 데이터 소스를 선택하는 기능	7.0	보고 플로우 히스토리의 내용을 참조하십시오.	모든
DNS 필터링	7.0 6.7(베타 기능)	DNS 필터링이 활성화된 경우: • DNS Query(DNS 쿼리) 필드에는 DNS 필터링 일치와 관련된 도메인이 포함될 수 있습니다. • URL 필드가 비어 있더라도 DNS 쿼리, URL 범주 및 URL 평판에 값이 있는 경우, DNS 필터링 기능으로 인해 이벤트가 생성되고 범주 및 평판이 DNS 쿼리에 지정된 도메인에 적용됩니다. • Cisco Secure Firewall Management Center 디바이스 구성 가이드의 *DNS* 필터링 및 이벤트도 참고하십시오.	모든

기능	배포	최소 Threat Defense	세부 사항
사용자 지정 테이블의 연결 이벤트 지원 제거	6.6.0	Any	6.6.0에서 연결 이벤트에 대한 사용자 지정 테이블을 생성할 수 없습니다. 업그레이드하는 경우, 연결 이벤트에 대한 기존 사용자 지정 테이블을 계속 사용할 수 있으나 결과가 항상 반환되지 않습니다. 다른 유형의 사용자 지정 테이블에는 변화가 없습니다. 신규/수정된 화면: **Analysis(분석) > Advanced(고급) > Custom Tables(사용자 지정 테이블)**의 Tables(테이블) 옵션 플랫폼: management center
삭제 및 모든 연결 이벤트 삭제 기능 제거	6.6.0	Any	6.6.0에서 삭제 및 모두 삭제 버튼이 연결 이벤트 테이블 페이지에서 제거되었습니다. 모든 연결 이벤트를 제거하려면 데이터 비우기 및 저장의 내용을 참조하십시오. 신규/수정된 화면: **Analysis(분석) > Connections(연결) > Events(이벤트)** 플랫폼: management center
VRF 및 SGT의 새 필드	6.6.0	Any	모든 연결 이벤트에 다음 필드가 추가되었습니다. • 이그레스 가상 라우터(시스템 로그: IngressVRF) • 이그레스 가상 라우터(시스템 로그: EgressVRF) • DestinationSecurityGroupType(시스템 로그만 해당) • SourceSecurityGroupType(시스템 로그만 해당)
신규 및 변경된 보안 그룹 태그 필드	6.5.0	Any	management center 웹 인터페이스의 필드 변경 사항: • 변경된 필드: 보안 그룹 태그가 소스 SGT로 변경 • 새 필드: 대상 SGT 시스템 로그 필드 변경 사항: • 변경된 필드: SecurityGroup이 SourceSecurityGroupTag로 변경 • 새 필드: • SourceSecurityGroup • DestinationSecurityGroup • DestinationSecurityGroupTag 지원되는 플랫폼: management center 및 매니지드 디바이스

기능	버전	세부 사항	최소 Threat Defense
새 시스템 로그 필드: 이벤트 우선순위	6.5	새 필드는 IPS 이벤트 선순위로 식별합니다.	침입, 파일, 악성코드 또는 보안 인텔리전스 이벤트와 연관된 연결 이벤트를 높은 우
시스템 로그의 연결 이벤트 통합 식별자	6.4.0.4	새 시스템 로그 필드는 연결 이벤트(DeviceUUID, 첫 번째 패킷 시간, 연결 인스턴스 ID, 연결 카운터)를 전체적으로 개별 식별합니다.	