Security Cloud Control에서 이벤트 보기

이 장에서는 Security Cloud Control에서 라이브 이벤트 및 기록 이벤트를 보는 방법에 대한 정보를 제공합니다.

- 라이브 이벤트 보기, on page 1
- 과거 이벤트 보기, on page 3
- 이벤트 보기 사용자 지정, on page 3
- 이벤트 로깅 페이지의 열 표시 및 숨기기, on page 5
- 이벤트 타임스탬프의 표준 시간대 변경, 8 페이지
- 사용자 지정 가능한 이벤트 필터, on page 9
- 이벤트 로깅 페이지에서 이벤트 검색 및 필터링, 10 페이지
- Security Analytics and Logging의 이벤트 속성, on page 21

라이브 이벤트 보기

Live events(라이브 이벤트) 페이지에는 입력한 필터 및 검색 기준과 일치하는 최신 500개의 이벤트가 표시됩니다. 라이브 이벤트 페이지에 최대 500개의 이벤트가 표시되고 더 많은 이벤트가 스트리밍되는 경우, Security Cloud Control는 최신 라이브 이벤트를 표시하고 가장 오래된 라이브 이벤트를 기록 이벤트 페이지로 전송하여 총 라이브 이벤트 수를 500개로 유지합니다. 이 전송을 수행하는 데 약 1분이 걸립니다. 필터링 기준이 추가되지 않은 경우, 이벤트를 로깅하도록 구성된 규칙에 의해 생성된 모든 최신 라이브 500 이벤트가 표시됩니다.

이벤트 타임스탬프는 UTC로 표시됩니다.

라이브 이벤트가 재생 중인지 일시 중지되었는지에 상관없이 필터링 기준을 변경하면 이벤트 화면이 지워지고 수집 프로세스가 다시 시작됩니다.

Security Cloud Control 이벤트 뷰어에서 라이브 이벤트를 보려면 다음을 수행합니다.

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.

What to do next

이벤트를 재생하고 일시 중지하는 방법을 참조하십시오.

관련 정보**:**

- 라이브 이벤트 재생/일시 중지, on page 2
- 과거 이벤트 보기, on page 3
- 이벤트 보기 사용자 지정, on page 3

라이브 이벤트 재생/일시 중지

라이브 이벤트가 스트리밍될 때 라이브 이벤트를 "재생" ▶ 또는 "일시 중지" ⏸ 할 수 있습니다. 라이브 이벤트가 "재생" 중인 경우 Security Cloud Control는 이벤트 뷰어에 지정된 필터링 기준과 일치하는 이벤트를 수신된 순서대로 표시합니다. 이벤트가 일시 중지된 경우 Security Cloud Control는 라이브 이벤트 재생을 다시 시작할 때까지 라이브 이벤트 페이지를 업데이트하지 않습니다. 이벤트 재생을 다시 시작하면 Security Cloud Control는 이벤트 재생을 다시 시작한 시점부터 Live(라이브) 페이지에 이벤트를 채우기 시작합니다. 누락된 항목은 다시 채우지 않습니다.

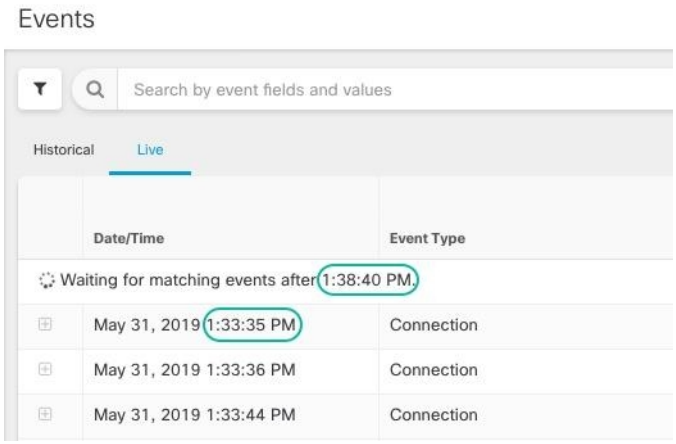
라이브 이벤트 스트리밍을 재생하거나 일시 중지했는지 여부에 관계없이 Security Cloud Control가 수신한 모든 이벤트를 보려면 **Historical(**기록**)** 탭을 클릭합니다.

라이브 이벤트 자동 일시 중지

약 5분 동안 이벤트를 표시한 후 Security Cloud Control는 라이브 이벤트의 스트림을 일시 중지한다고 경고합니다. 이때 링크를 클릭하여 다른 5분 동안 라이브 이벤트 스트리밍을 계속하거나 스트림을 중지할 수 있습니다. 준비가 되면 라이브 이벤트 스트림을 다시 시작할 수 있습니다.

이벤트 수신 및 보고

라이브 이벤트 뷰어에서 SEC(Secure Event Connector) 또는 Security Service Exchange 수신 이벤트와 Security Cloud Control 게시 이벤트 사이에 약간의 지연이 발생할 수 있습니다. Live(라이브) 페이지에서 간격을 볼 수 있습니다. 타임스탬프는 Secure Event Connector 또는 Security Service Exchange에서 이벤트가 수신된 시간입니다.



과거 이벤트 보기

Live events(라이브 이벤트) 페이지에는 입력한 필터 및 검색 기준과 일치하는 최신 500개의 이벤트가 표시됩니다. 가장 최근의 500개 이벤트보다 오래된 이벤트는 기록 이벤트 테이블로 전송됩니다. 이 전송을 수행하는 데 약 1분이 걸립니다. 그런 다음 저장한 모든 이벤트를 필터링하여 원하는 이벤트를 찾을 수 있습니다.

과거 이벤트를 보려면:

Procedure

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

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

단계 **3** 기록 탭을 클릭합니다. 기본적으로 기록 이벤트 테이블을 열면 지난 1시간 내에 수집된 이벤트가 표시되도록 필터가 설정됩니다.

이벤트 속성은 FDM(Firepower Device Manager) 또는 ASDM(Adaptive Security Device Manager)에서 보고하는 것과 거의 동일합니다.

- Firepower Threat Defense 이벤트 속성에 대한 전체 설명은 Cisco FTD 시스템 로그 메시지를 참조하십시오.
- ASA 이벤트 속성에 대한 전체 설명은 Cisco ASA Series 시스템 로그 메시지를 참조하십시오.

이벤트 보기 사용자 지정

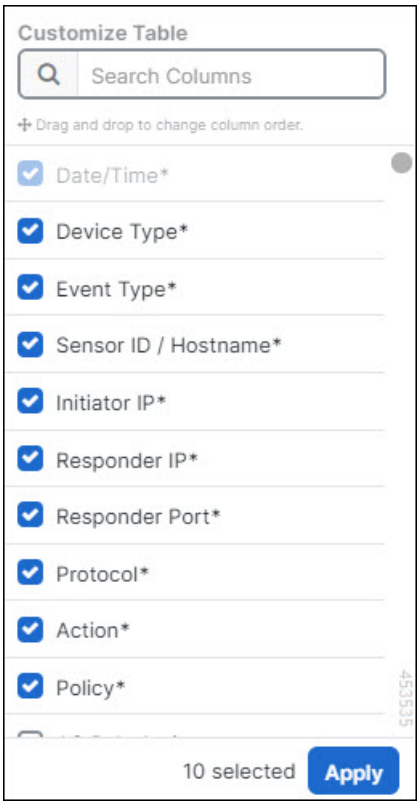
Event Logging(이벤트 로깅) 페이지에 대한 모든 변경 사항은 이 페이지에서 빠져나왔다가 나중에 다시 돌아올 때를 위해 자동으로 저장됩니다.

Note 라이브 및 기록 이벤트 보기의 구성은 동일합니다. 이벤트 보기를 사용자 정의하면 이러한 변경 사항이 Live(라이브) 및 Historical(기록) 보기에 모두 적용됩니다.

열 표시 또는 숨기기

원하는 보기에 적용되는 열 헤더만 포함하도록 라이브 및 기록 이벤트에 대한 이벤트 보기를 수정할 수 있습니다. 열 오른쪽에 있는 열 필터 아이콘 을 클릭하고 원하는 열을 선택하거나 선택 취소한 다음 **Apply(적용)**를 클릭합니다.

Figure 1: 열 표시 또는 숨기기



별표가 있는 열은 언제든지 제거할 수 있지만 기본적으로 이벤트 테이블 내에 제공됩니다.

열 검색 및 추가

기본 목록에 없는 더 많은 열을 검색하여 실시간 및 과거 이벤트 모두에 대한 이벤트 보기에 추가할 수 있습니다. 테이블을 맞춤화하기 위해 열을 많이 추가하면 성능이 저하될 수 있습니다. 데이터 검색을 빠르게 하기 위해 사용하는 열 수를 줄이는 것을 고려합니다.

또는 이벤트 옆의 + 아이콘을 클릭하여 확장하고 숨겨진 열을 볼 수 있습니다.

열 재정렬

이벤트 테이블의 열 순서를 바꿀 수 있습니다. 열 오른쪽에 있는 열 필터 아이콘 ≡ 을 클릭하면 선택한 열의 목록을 볼 수 있습니다. 그런 다음 열을 원하는 순서대로 끌어다 놓습니다. 드롭다운 메뉴의 목록 맨 위에 있는 열은 이벤트 테이블에서 가장 왼쪽 열로 나타납니다.

관련 정보:

- 이벤트 로깅 페이지에서 이벤트 필터링
- Security Analytics and Logging의 이벤트 속성

이벤트 로깅 페이지의 열 표시 및 숨기기

Event Logging(이벤트 로깅**)** 페이지에는 구성된 및 FDM 관리디바이스에서 Cisco Cloud로 전송된 이벤트가 표시됩니다.

테이블과 함께 Show/Hide(표시/숨기기) 위젯을 사용하여 **Event Logging(**이벤트 로깅**)** 페이지에서 열을 표시하거나 숨길 수 있습니다.

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** 테이블의 맨 오른쪽으로 스크롤하여 열 필터 아이콘 ≡을 클릭합니다.

단계 **4** 표시하려는 열을 선택하고, 숨기려는 열을 선택 취소합니다.

테넌트에 로그인하는 다른 사용자는 열이 다시 표시되거나 숨겨질 때까지 표시하도록 선택한 것과 동일한 열을 볼 수 있습니다.

이 표에서는 기본 열 헤더에 대해 설명합니다.

열 헤더	설명
날짜/시간	디바이스가 이벤트를 생성한 시간 기본적으로 이벤트 타임스탬프는 현지 시간대로 표시됩니다. 이벤트 타임스탬프를 UTC로 보려면 이벤트 타임스탬프의 표준 시간대 변경, on page 8을 참조하십시오.
디바이스 유형	ASA(Adaptive Security Appliance) FTD(Firepower Threat Defense)

열 헤더	설명

이벤트 유형	이 복합 열에는 다음 중 하나가 포함될 수 있습니다.
	• **FTD** 이벤트 유형
	  • Connection(연결): 액세스 제어 규칙의 연결 이벤트를 표시합니다.
	  • File(파일): 액세스 제어 규칙의 파일 정책에 의해 보고된 이벤트를 표시합니다.
	  • Intrusion(침입): 액세스 제어 규칙의 침입 정책에 의해 보고된 이벤트를 표시합니다.
	  • Malware(멀웨어): 액세스 제어 규칙의 멀웨어 정책에 의해 보고된 이벤트를 표시합니다.
	• ASA **Event Types(**이벤트 유형**)**: 이러한 이벤트 유형은 시스템 로그 또는 NetFlow 이벤트의 그룹을 나타냅니다. 어떤 Syslog ID 또는 어떤 NetFlow ID가 어떤 그룹에 포함되어 있는지에 대한 자세한 내용은 ASA 이벤트 유형을 참조하십시오.
	  • Parsed Events(구문 분석된 이벤트): 구문 분석된 시스템 로그 이벤트는 다른 시스템 로그 이벤트보다 더 많은 이벤트 속성을 포함하며, Security Cloud Control는 이러한 속성을 기반으로 더 빠르게 검색 결과를 반환할 수 있습니다. 구문 분석된 이벤트는 필터링 카테고리가 아닙니다. 그러나 구문 분석된 이벤트 ID는 Event Types(이벤트 유형) 열에 기울임꼴로 표시됩니다. 기울임꼴로 표시되지 않은 이벤트 ID는 구문 분석되지 않습니다.
	  • ASA NetFlow Event IDs(ASA NetFlow 이벤트 ID): ASA의 모든 Netflow(NSEL) 이벤트가 여기에 표시됩니다.

열 헤더	설명
센서 ID / 호스트 이름	센서 ID는 이벤트가 Security Service Exchange 또는 Secure Event Connector로 전송되는 IP 주소입니다. 이는 일반적으로 Threat Defense 또는 ASA의 관리 인터페이스입니다.
초기자 IP	이는 네트워크 트래픽 소스의 IP 주소입니다. Initiator address(이니시에이터 주소) 필드의 값은 이벤트 세부사항의 InitiatorIP(이니시에이터 IP) 필드 값에 해당합니다. 단일 주소(예: 10.10.10.100) 또는 CIDR 표기법으로 정의된 네트워크(예: 10.10.10.0/24)를 입력할 수 있습니다.
응답기 IP	이것은 패킷의 대상 IP 주소입니다. Destination address(대상 주소) 필드의 값은 이벤트 세부사항의 ResponderIP 필드에 있는 값에 해당합니다. 단일 주소(예: 10.10.10.100) 또는 CIDR 표기법으로 정의된 네트워크(예: 10.10.10.0/24)를 입력할 수 있습니다.
포트	세션 **responder**가 사용하는 포트 또는 ICMP 코드 대상 포트의 값은 이벤트 세부사항의 **ResponderPort** 값에 해당합니다.
프로토콜	이벤트의 프로토콜을 나타냅니다.

열 헤더	설명
작업	규칙에 의해 정의된 보안 작업을 지정합니다. 입력하는 값은 찾으려는 값과 정확히 일치해야 합니다. 그러나 대/소문자는 중요하지 않습니다. 연결, 파일, 침입, 멀웨어, Syslog 및 NetFlow 이벤트 유형에 대해 서로 다른 값을 입력합니다. • 연결 이벤트 유형의 경우 필터는 AC_RuleAction 특성에서 일치 항목을 검색합니다. 이러한 값은 Allow(허용), Block(차단), Trust(신뢰)일 수 있습니다. • 파일 이벤트 유형의 경우 필터는 FileAction 속성에서 일치하는 항목을 검색합니다. 이러한 값은 Allow(허용), Block(차단), Trust(신뢰)일 수 있습니다. • 침입 이벤트 유형의 경우 필터는 InLineResult 속성에서 일치하는 항목을 검색합니다. 이러한 값은 Allowed(허용됨), Blocked(차단됨), Trusted(신뢰할 수 있음)일 수 있습니다. • 멀웨어 이벤트 유형의 경우 필터는 FileAction 속성에서 일치하는 항목을 검색합니다. 이러한 값은 Cloud Lookup Timeout(클라우드 조회 시간 초과)일 수 있습니다. • Syslog 및 NetFlow 이벤트 유형의 경우 필터는 Action(작업) 속성에서 일치하는 항목을 검색합니다.
정책	이벤트를 트리거한 정책의 이름입니다. ASA 및 FDM 관리 디바이스마다 이름이 다릅니다.

관련 정보:

이벤트 로깅 페이지에서 이벤트 검색 및 필터링, on page 10

이벤트 타임스탬프의 표준 시간대 변경

Security Cloud Control 이벤트 로깅 페이지에서 이벤트 타임스탬프의 표준 시간대 표시를 변경합니다.

프로시저

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** 이벤트 로깅 페이지의 오른쪽 상단에 있는 **UTC** 시간 또는 현지 시간 버튼을 클릭하면 선택한 시간대의 이벤트 타임스탬프가 표시됩니다.

기본적으로 이벤트 타임스탬프는 현지 시간대로 표시됩니다.

사용자 지정 가능한 이벤트 필터

SaaS(Secure Logging Analytics) 고객은 자주 사용하는 맞춤형 필터를 생성하고 저장할 수 있습니다.

필터의 요소는 구성할 때 필터 탭에 저장됩니다. Event Logging(이벤트 로깅) 페이지로 돌아갈 때마다 이러한 검색을 사용할 수 있습니다. 테넌트의 다른 Security Cloud Control 사용자는 사용할 수 없습니다. 둘 이상의 테넌트를 관리하는 경우 다른 테넌트에서는 사용할 수 없습니다.

Note 필터 탭에서 작업할 때 필터 기준을 수정하면 해당 변경 사항이 사용자 지정 필터 탭에 자동으로 저장됩니다.

Procedure

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

단계 **2** 주 메뉴에서 **Events & Logs(**이벤트 및 로그**)** > **Events(**이벤트**)** > **Event Logging(**이벤트 로깅**)**을(를) 선택합니다.

단계 **3** 모든 값의 Search(검색) 필드를 지웁니다.

단계 **4** 이벤트 테이블 위에서 파란색 플러스 버튼을 클릭하여 View(보기) 탭을 추가합니다. 필터 보기에는 이름을 지정할 때까지 "View 1", "View 2", "View 3" 등의 레이블이 지정됩니다.

단계 **5** View(보기) 탭을 선택합니다.

단계 **6** 필터 표시줄을 열고 맞춤형 필터에서 원하는 필터 속성을 선택합니다. 이벤트 로깅 페이지에서 이벤트 검색 및 필터링, on page 10의 내용을 참조하십시오. 필터 특성만 맞춤형 필터에 저장됩니다.

단계 **7** 이벤트 로깅 테이블에 표시할 열을 사용자 정의합니다. 열 표시 및 숨기기에 대한 설명은 이벤트 로깅 페이지의 열 표시 및 숨기기, on page 5의 내용을 참조하십시오.

단계 **8** "View X" 레이블이 있는 필터 탭을 두 번 클릭하고 이름을 바꿉니다.

단계 **9** (선택 사항) 맞춤형 필터를 생성했으므로 이제 Search(검색) 필드에 검색 기준을 추가하여 맞춤형 필터를 변경하지 않고도 Event Logging(이벤트 로깅) 페이지에 표시되는 결과를 미세 조정할 수 있습니다. 이벤트 로깅 페이지에서 이벤트 검색 및 필터링, on page 10의 내용을 참조하십시오.

이벤트 로깅 페이지에서 이벤트 검색 및 필터링

특정 이벤트에 대한 기록 및 라이브 이벤트 테이블을 검색하고 필터링하는 것은 Security Cloud Control에서 다른 정보를 검색하고 필터링할 때와 동일한 방식으로 작동합니다. 필터 기준을 추가하면 Security Cloud Control가 **Event Logging(**이벤트 로깅**)** 페이지에 표시되는 내용을 제한하기 시작합니다. 검색 필드에 검색 기준을 입력하여 특정 값의 이벤트를 찾을 수도 있습니다. 필터링 및 검색 메커니즘을 결합하는 경우, 검색은 이벤트를 필터링한 후 표시된 결과 중에서 입력한 값을 찾으려고 시도합니다.

다음은 이벤트 로그 검색을 수행하는 옵션입니다.

- 이벤트 로깅 페이지를 사용하여 이벤트 검색, 18 페이지
- 백그라운드에서 기록 이벤트 검색, 19 페이지

필터링은 라이브 이벤트를 시간 기준으로 필터링할 수 없다는 점을 제외하고 기록 이벤트와 동일한 방식으로 라이브 이벤트에 대해 작동합니다.

이러한 필터링 방법에 대해 알아보십시오.

- 라이브 또는 과거 이벤트 필터링, 10 페이지
- NetFlow 이벤트만 필터링, 12 페이지
- ASA 또는 FDM-관리 디바이스 시스템 로그 이벤트에 대한 필터링(ASA NetFlow 이벤트 제외), 13 페이지
- 필터 요소 결합, 13 페이지

라이브 또는 과거 이벤트 필터링

이 절차에서는 이벤트 필터링을 사용하여 **Event Logging(**이벤트 로깅**)** 페이지에서 이벤트의 하위 집합을 확인하는 방법을 설명합니다. 특정 필터 기준을 반복적으로 사용하는 경우 사용자 지정 필터를 생성하여 저장할 수 있습니다. 자세한 내용은 맞춤형 이벤트 필터를 참조하십시오.

Procedure

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

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

단계 **3** **Historical(**기록**)** 또는 **Live(**라이브**)** 탭을 클릭합니다.

단계 **4** Filter(필터) 아이콘( )을 클릭합니다. 핀 아이콘( )을 클릭하고 필터 창을 열린 상태로 유지합니다.

단계 **5** 저장된 필터 요소가 없는 View(보기) 탭을 클릭합니다.

단계 **6** 필터링할 이벤트 세부 정보를 선택합니다.

- **FTD** 이벤트:
  - Connection(연결): 액세스 제어 규칙의 연결 이벤트를 표시합니다.
  - File(파일): 액세스 제어 규칙의 파일 정책에 의해 보고된 이벤트를 표시합니다.
  - Intrusion(침입): 액세스 제어 규칙의 침입 정책에 의해 보고된 이벤트를 표시합니다.
  - Malware(멀웨어): 액세스 제어 규칙의 멀웨어 정책에 의해 보고된 이벤트를 표시합니다.
- **ASA Events(ASA** 이벤트**)**: 이러한 이벤트 유형은 시스템 로그 또는 NetFlow 이벤트의 그룹을 나타냅니다.

  이벤트에 대한 자세한 내용은 Security Cloud Control이벤트 유형을 참조하십시오.
  - Parsed Events(구문 분석된 이벤트): 구문 분석된 시스템 로그 이벤트는 다른 시스템 로그 이벤트보다 더 많은 이벤트 속성을 포함하며, Security Cloud Control는 이러한 속성을 기반으로 더 빠르게 검색 결과를 반환할 수 있습니다. 구문 분석된 이벤트는 필터링 카테고리가 아닙니다. 그러나 구문 분석된 이벤트 ID는 Event Types(이벤트 유형) 열에 기울임꼴로 표시됩니다. 기울임꼴로 표시되지 않은 이벤트 ID는 구문 분석되지 않습니다.
- **Time Range(**시간 범위**)**: 표시할 기간의 시작과 끝을 선택하려면 Start(시작) 또는 End(종료) 시간 필드를 클릭합니다. 타임스탬프는 컴퓨터의 로컬 시간으로 표시됩니다.
- **Action(**작업**)**: 규칙에 의해 정의된 보안 작업을 지정합니다. 입력하는 값은 찾으려는 값과 정확히 일치해야 합니다. 그러나 대/소문자는 중요하지 않습니다. 연결, 파일, 침입, 멀웨어, Syslog 및 NetFlow 이벤트 유형에 대해 서로 다른 값을 입력합니다.
  - 연결 이벤트 유형의 경우 필터는 AC_RuleAction 특성에서 일치 항목을 검색합니다. 이러한 값은 Allow(허용), Block(차단), Trust(신뢰)일 수 있습니다.
  - 파일 이벤트 유형의 경우 필터는 FileAction 속성에서 일치하는 항목을 검색합니다. 이러한 값은 Allow(허용), Block(차단), Trust(신뢰)일 수 있습니다.
  - 침입 이벤트 유형의 경우 필터는 InLineResult 속성에서 일치하는 항목을 검색합니다. 이러한 값은 Allowed(허용됨), Blocked(차단됨), Trusted(신뢰할 수 있음)일 수 있습니다.
  - 멀웨어 이벤트 유형의 경우 필터는 FileAction 속성에서 일치하는 항목을 검색합니다. 이러한 값은 Cloud Lookup Timeout(클라우드 조회 시간 초과)일 수 있습니다.
  - Syslog 및 NetFlow 이벤트 유형의 경우 필터는 Action(작업) 속성에서 일치하는 항목을 검색합니다.
- **Sensor ID / Hostname(**센서 **ID /** 호스트 이름**)**: 센서 ID는 이벤트가 Secure Event Connector로 전송되는 관리 IP 주소입니다.

  FDM 관리 디바이스의 경우 센서 ID는 일반적으로 디바이스 관리 인터페이스의 IP 주소입니다.
- **IP** 주소

- **Initiator**이니시에이터**)**: 네트워크 트래픽 소스의 IP 주소입니다. Initiator address(이니시에이터 주소) 필드의 값은 이벤트 세부사항의 InitiatorIP(이니시에이터 IP) 필드 값에 해당합니다. 단일 주소(예: 10.10.10.100) 또는 CIDR 표기법으로 정의된 네트워크(예: 10.10.10.0/24)를 입력할 수 있습니다.
- **Responder(**응답자**)**: 패킷의 대상 IP 주소입니다. Destination address(대상 주소) 필드의 값은 이벤트 세부사항의 ResponderIP 필드에 있는 값에 해당합니다. 단일 주소(예: 10.10.10.100) 또는 CIDR 표기법으로 정의된 네트워크(예: 10.10.10.0/24)를 입력할 수 있습니다.

- 포트
  - **Initiator(**이니시에이터**)**: 세션 이니시에이터가 사용하는 포트 또는 ICMP 유형입니다. 소스 포트의 값은 이벤트 세부 정보의 InitiatorPort 값에 해당합니다. (범위 추가 - 시작 포트 종료 포트 및 이니시에이터와 응답자 사이 또는 둘 다 사이에 공백)
  - **Reponder(**응답자**)**: 세션 응답자가 사용하는 포트 또는 ICMP 코드입니다. 대상 포트의 값은 이벤트 세부사항의 ResponderPort 값에 해당합니다.

- **NetFlow**: ASA NetFlow 이벤트는 시스템 로그 이벤트와 다릅니다. NetFlow 필터는 NSEL 레코드를 생성한 모든 NetFlow 이벤트 ID를 검색합니다. 이러한 "NetFlow 이벤트 ID"는 Cisco ASA NetFlow 구현 가이드에 정의되어 있습니다.

단계 **7** (선택 사항) View(보기) 탭에서 클릭하여 필터를 사용자 지정 필터로 저장합니다.

NetFlow 이벤트만 필터링

이 절차에서는 ASA NetFlow 이벤트만 찾습니다.

Procedure

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

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

단계 **3** Filter(필터) 아이콘 ▼을 클릭하고 필터를 열린 상태로 고정합니다.

단계 **4** **NetFlow** ASA 이벤트 필터를 확인합니다.

단계 **5** 다른 모든 ASA 이벤트 필터를 지웁니다.

ASA NetFlow 이벤트만 Event Logging(이벤트 로깅) 테이블에 표시됩니다.

ASA 또는 FDM-관리 디바이스 시스템 로그 이벤트에 대한 필터링(ASA NetFlow 이벤트 제외)

이 절차에서는 Syslog 이벤트만 찾습니다.

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** Filter(필터) 아이콘 을 클릭하고 필터를 열린 상태로 고정합니다.

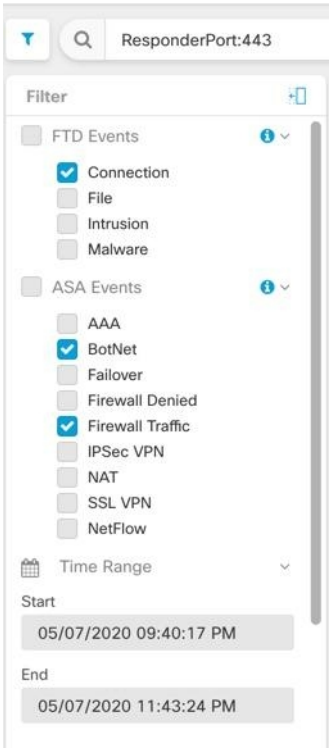
단계 **4** 필터 창 하단으로 스크롤하여 **Include NetFlow Events(NetFlow** 이벤트 포함**)**가 선택 해제되어 있는지 확인합니다.

단계 **5** ASA Events(ASA 이벤트) 필터 트리로 다시 스크롤하여 **NetFlow** 상자가 선택 취소되었는지 확인합니다.

단계 **6** ASA 또는 FTD 필터 기준의 나머지를 선택합니다.

필터 요소 결합

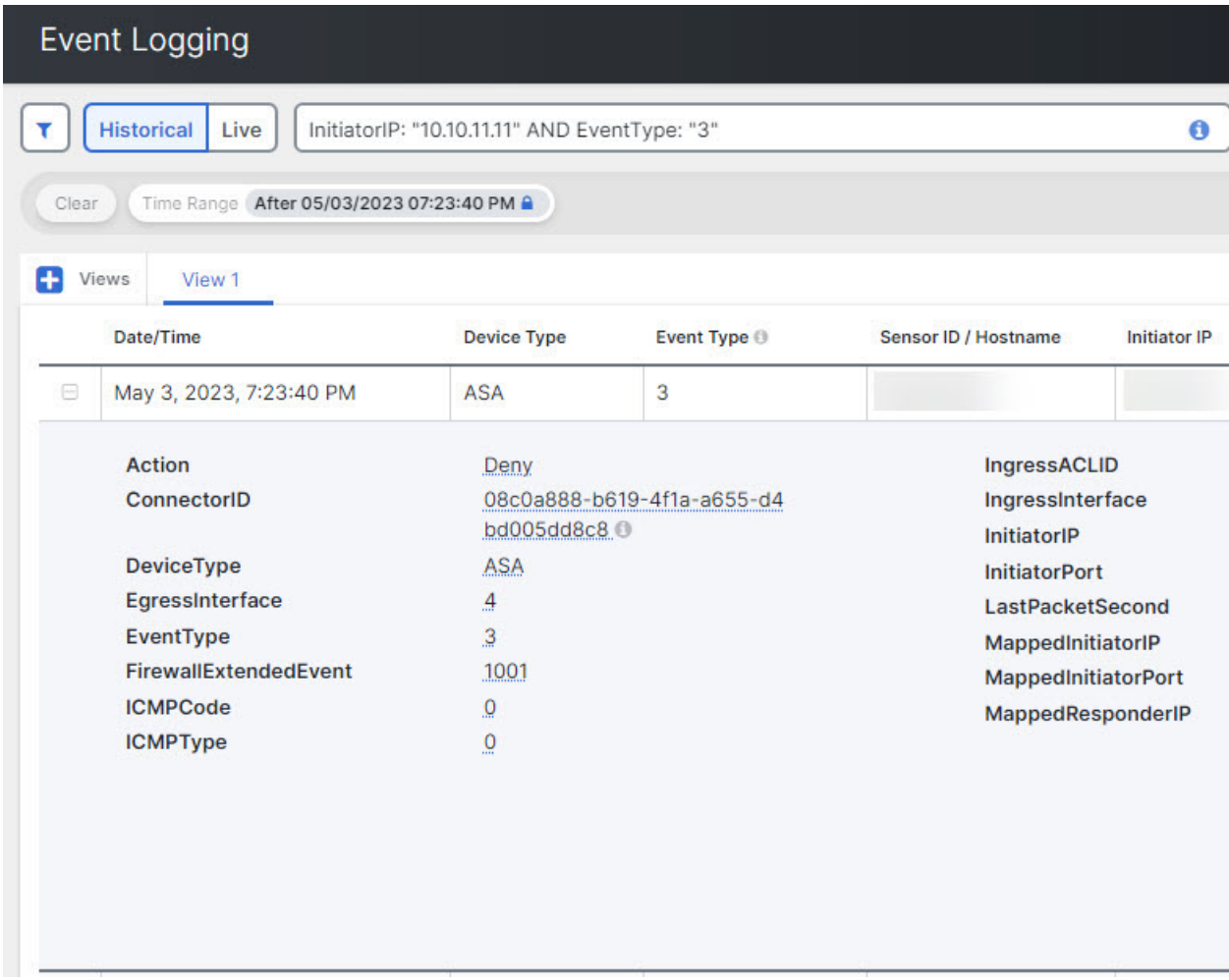
필터링 이벤트는 일반적으로 Security Cloud Control의 표준 필터링 규칙을 따릅니다. 필터링 범주는 "AND"되고 범주 내의 값은 "OR"됩니다. 필터를 사용자 고유의 검색 기준과 결합할 수도 있습니다. 이벤트 필터의 경우 그러나 디바이스 이벤트 필터도 "OR"됩니다. 예를 들어 필터에서 다음 값을 선택한 경우,



이 필터를 사용하면 Security Cloud Control는 Firewall Threat Defense 디바이스 연결 이벤트 또는 ASA BotNet 또는 방화벽 트래픽 이벤트 및 시간 범위의 두 번 사이에 발생한 이벤트 및 ResponderPort 443도 포함하는 이벤트를 표시합니다. 시간 범위 내의 기록 이벤트를 기준으로 필터링할 수 있습니다. 라이브 이벤트 페이지에는 항상 최신 이벤트가 표시됩니다.

특정 속성: 값 쌍 검색

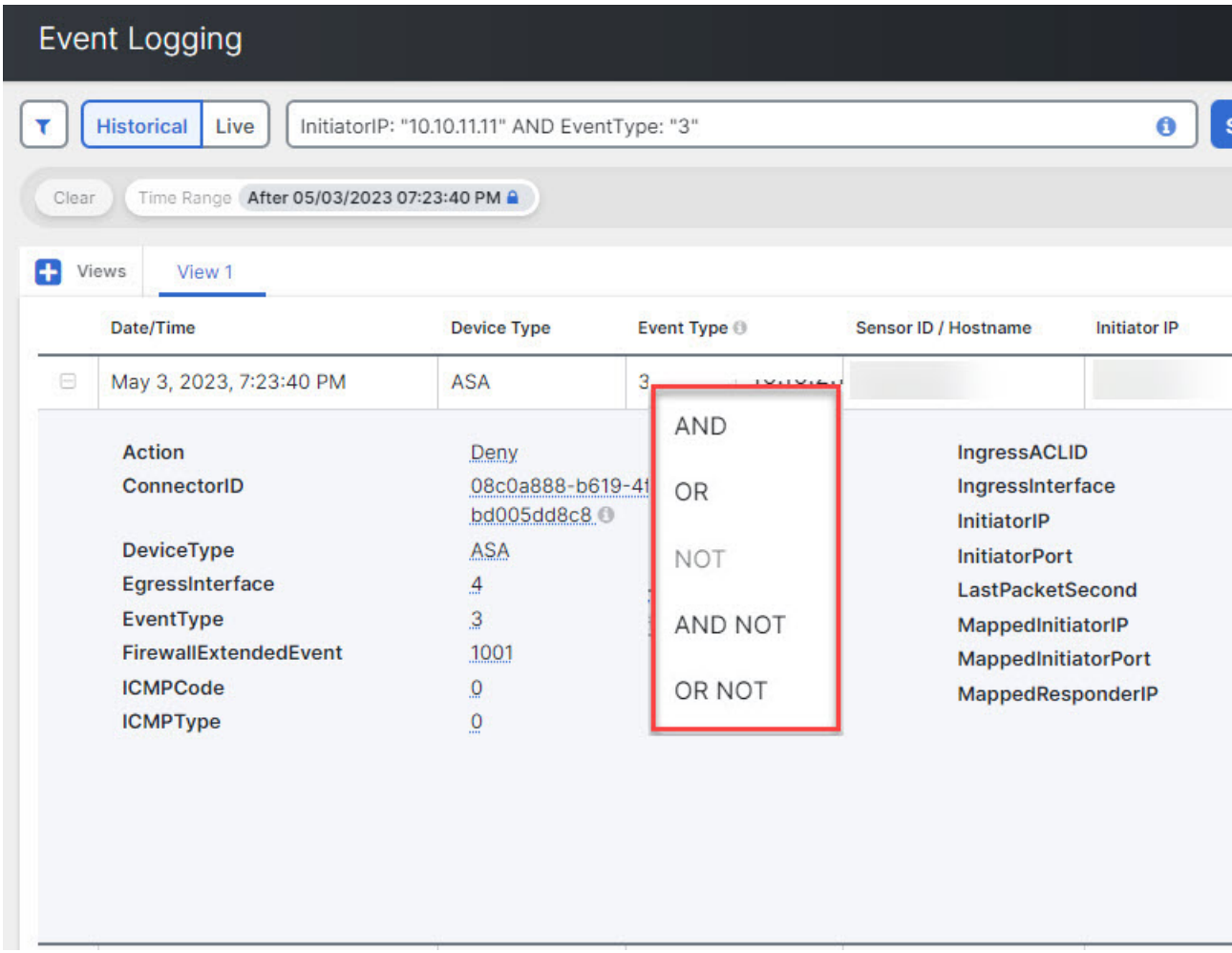
검색 필드에 이벤트 속성 및 값을 입력하여 라이브 또는 기록 이벤트를 검색할 수 있습니다. 이 작업을 수행하는 가장 쉬운 방법은 검색하려는 Event Logging(이벤트 로깅) 테이블의 속성을 클릭하는 것입니다. 그러면 Security Cloud Control가 Search(검색) 필드에 해당 속성을 입력합니다. 롤오버하면 클릭할 수 있는 이벤트가 파란색으로 표시됩니다. 예를 들면 다음과 같습니다.



이 예에서는 InitiatorIP 값 10.10.11.11을 롤오버하고 이를 클릭하여 검색을 시작했습니다. 이니시에이터 IP 및 해당 값이 검색 문자열에 추가되었습니다. 다음으로, Event Type(이벤트 유형) 3를 클릭하여 검색 문자열에 추가하고 Security Cloud Control에서 AND를 추가했습니다. 따라서 이 검색의 결과는 10.10.11.11에서 시작된 이벤트 및 3 이벤트 유형의 목록이 됩니다.

위의 예에서 값 3 옆에 돋보기가 있습니다. 돋보기를 롤오버하는 경우 AND, OR, AND NOT, OR NOT 연산자를 선택하여 검색에 추가할 값을 입력할 수도 있습니다.

아래 예에서는 "OR"가 선택되었습니다. 이 검색의 결과는 10.10.11.11에서 시작된 이벤트 또는 106023 이벤트 유형의 목록이 됩니다. 검색 필드가 비어 있고 테이블에서 값을 마우스 오른쪽 버튼으로 클릭하면 다른 값이 없으므로 NOT만 사용할 수 있습니다.



값을 롤오버하고 파란색으로 강조 표시되면 해당 값을 검색 문자열에 추가할 수 있습니다.

AND, OR, NOT, AND NOT, OR NOT 필터 연산자

검색 문자열에서 사용되는 "AND", "OR", "NOT", "AND NOT" 및 "OR NOT"의 동작은 다음과 같습니다.

AND

필터 문자열에서 AND 연산자를 사용하여 모든 특성을 포함하는 이벤트를 찾습니다. AND 연산자는 검색 문자열을 시작할 수 없습니다.

예를 들어 아래의 검색 문자열은 이니시에이터IP 주소 10.10.10.43에서 시작되고 이니시에이터 포트 59614에서 전송된 TCP 프로토콜 AND를 포함하는 이벤트를 검색합니다. 각 추가 AND 문을 사용하여 기준을 충족하는 이벤트의 수가 점점 더 적을 것으로 예상됩니다.

```
Protocol: "tcp" AND InitiatorIP: "10.10.10.43" AND InitiatorPort: "59614"
```

또는

필터 문자열에서 OR 연산자를 사용하여 특성을 포함하는 이벤트를 찾습니다. OR 연산자는 검색 문자열을 시작할 수 없습니다.

예를 들어 아래의 검색 문자열은 TCP 프로토콜을 포함하는 이벤트를 포함하는 이벤트, 또는 이니시에이터 IP 주소 10.10.10.43에서 시작된 또는 이니시에이터 포트 59614에서 전송된 이벤트를 표시합니다. 각 추가 OR 문에서 기준을 충족하는 이벤트의 수가 점점 더 커질 것으로 예상됩니다.

```
Protocol: "tcp" OR InitiatorIP: "10.10.10.43" OR InitiatorPort: "59614"
```

NOT

특정 속성이 있는 이벤트를 제외하려면 검색 문자열의 시작 부분에만 이를 사용하십시오. 예를 들어 이 검색 문자열은 InitiatorIP 192.168.25.3인 이벤트를 결과에서 제외합니다.

```
NOT InitiatorIP: "192.168.25.3"
```

AND NOT

특정 특성을 포함하는 이벤트를 제외하려면 필터 문자열에서 AND NOT 연산자를 사용합니다. AND NOT은 검색 문자열의 시작 부분에 사용할 수 없습니다.

예를 들어 이 필터 문자열은 InitiatorIP 192.168.25.3인 이벤트를 표시하지만 ResponderIP 주소가 10.10.10.1인 이벤트는 표시하지 않습니다.

```
InitiatorIP: "192.168.25.3" AND NOT ResponderIP: "10.10.10.1"
```

NOT과 AND NOT을 조합하여 여러 속성을 제외할 수도 있습니다. 예를 들어 이 필터 문자열은 InitiatorIP 192.168.25.3의 이벤트 및 ResponderIP 10.10.10.1의 이벤트를 제외합니다.

```
NOT InitiatorIP: "192.168.25.3" AND NOT ResponderIP: "10.10.10.1"
```

OR NOT

특정 요소를 제외하는 검색 결과를 포함하려면 OR NOT 연산자를 사용합니다. OR NOT 연산자는 검색 문자열의 시작 부분에 사용할 수 없습니다.

예를 들어 이 검색 문자열은 프로토콜이 TCP인 이벤트 또는 InitiatorIP가 10.10.10.43인 이벤트 또는 InitiatorPort 59614가 아닌 이벤트를 찾습니다.

```
Protocol: "tcp" OR InitiatorIP: "10.10.10.43" OR NOT InitiatorPort: "59614"
```

(프로토콜: "tcp") OR (InitiatorIP: "10.10.10.43") OR (NOT InitiatorPort: "59614")를 검색할 수도 있습니다.

와일드카드 검색

이벤트 내에서 결과를 찾으려면 **attribute:value** 검색의 value 필드에서 와일드카드를 나타내려면 별표(*)를 사용합니다. 예를 들어, 이 필터 문자열

```
URL:*feedback*
```

은 문자열 **feedback**을 포함하는 이벤트의 URL 특성 필드에서 문자열을 찾습니다.

관련 정보**:**

- 이벤트 로깅 페이지의 열 표시 및 숨기기
- Security Analytics and Logging의 이벤트 속성

이벤트 로깅 페이지를 사용하여 이벤트 검색

Event Logging(이벤트 로깅**)** 페이지에서 검색 및 백그라운드 검색 기능을 사용하여 로깅된 모든 이벤트 및 필요한 정보를 검색할 수 있습니다. 기록 이벤트에 대한 보고서만 생성할 수 있습니다.

프로시저

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

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

단계 **3** **Historical(**기록**)** 또는 **Live(**라이브**)** 탭을 클릭합니다.

단계 **4** 검색 창에 검색 쿼리를 입력하고 **Search(**검색**)**를 클릭하여 검색을 실행합니다.

또는, 빠르게 이벤트를 검색하려면 검색 상자를 클릭하여 **Sample Filters(**샘플 필터**)** 목록에서 선택할 수도 있습니다. 샘플 필터를 사용하여 검색창에 검색어를 빠르게 입력한 후, 특정 요구 사항에 맞게 수정합니다. 샘플 필터를 사용하는 방법에 대한 자세한 내용은 샘플 필터를 사용하여 이벤트 검색, 18 페이지을 참조하십시오.

단계 **5** (선택 사항) 검색 페이지에서 벗어나 있는 동안 백그라운드에서 검색을 실행하고 보고서를 생성하려면 다음을 수행합니다.

a) 검색 쿼리를 입력하고 **Search(**검색**)** 드롭다운 목록에서 **Schedule Report(**보고서 예약**)**를 선택합니다.

b) **Generate Report(**보고서 생성**)**를 클릭합니다.

검색 작업이 대기열에 추가되며, 완료 시 알림이 표시됩니다. 백그라운드에서 여러 검색을 실행할 수 있습니다.

보고서 예약에 대한 자세한 내용은 백그라운드에서 검색 보고서를 생성하도록 예약, 19 페이지을 참조하십시오.

단계 **6** (선택 사항) 검색 보고서를 보고 관리하려면 **Reports(**보고서**)**를 클릭합니다. 이 보기에서는 다음 작업을 수행할 수 있습니다.

- **Reports(**보고서**)** 페이지에서 검색 보고서를 보거나 다운로드하거나 삭제할 수 있습니다.
- **Schedule(**보고서**)**를 클릭하여 일회성 보고서를 생성하거나 반복 보고서를 예약합니다.
- **View Notification Settings(**알림 설정 보기**)**를 클릭하여 **Notification Preferences(**알림 환경설정**)** 페이지로 이동하여 알림 설정을 확인하거나 수정합니다.

다음에 수행할 작업

반복 검색이 필요한 경우 일회성 보고서를 반복 보고서 일정으로 변환할 수 있습니다. 자세한 내용은 백그라운드에서 검색 보고서를 생성하도록 예약, 19 페이지를 참조하십시오.

샘플 필터를 사용하여 이벤트 검색

샘플 필터를 사용하면 전체 검색어를 입력하지 않고도 일반적인 검색 쿼리를 빠르게 구성할 수 있습니다. 필터를 선택하고 특정 요구 사항에 맞게 쿼리 매개변수를 수정합니다.

프로시저

단계 **1** **Event Logging(**이벤트 로깅**)** 페이지에서 검색 창을 클릭합니다. 검색 창 아래에 **Sample Filters(**샘플 필터**)** 목록이 나타납니다.

단계 **2** 드롭다운 목록에서 필터를 선택합니다. 검색창에는 해당 검색어가 자동으로 입력됩니다.

단계 **3** 사전 정의된 쿼리의 값을 수정하여 검색을 구체화하십시오.

예

- 특정 웹사이트와 관련된 이벤트를 검색하려면 **Wildcard URL(**와일드카드 **URL)**을 선택합니다. 검색 창에 **URL: "*.sharepoint.com"**이 표시됩니다. 그런 다음 sharepoint.com을 조사하고자 하는 다른 도메인으로 변경할 수 있습니다.
- 특정 디바이스와 관련된 이벤트를 검색하려면 **Specific Host(**특정 호스트**)**를 선택합니다. 검색 창에 **InitiatorIP: "192.168.55.55" OR ResponderIP: "192.168.55.55"**가 표시됩니다. 192.168.55.55를 모니터링하려는 디바이스의 IP 주소로 변경하십시오.

단계 **4** **Search(**검색**)**를 클릭합니다.

백그라운드에서 기록 이벤트 검색

Security Cloud Control은 검색 기준을 정의하고 해당 기준에 따라 이벤트 로그를 검색할 수 있도록 합니다. 보고서 기능을 사용하면 백그라운드에서 이벤트 로그 검색을 수행하고 보고서를 생성할 수 있습니다.

알림 환경설정에 따라 보고서 생성이 완료되면 알림을 받게 됩니다.

Reports(보고서**)** 페이지에서 보고서를 보거나 다운로드하거나 삭제할 수 있습니다. 또한, 일회성 보고서 또는 반복 보고서를 생성하도록 예약할 수 있습니다. 알림 설정 페이지로 이동하여 구독 옵션을 보거나 수정합니다.

백그라운드에서 검색 보고서를 생성하도록 예약

Event Logging(이벤트 로깅**)** 페이지의 **Report(**보고서**)** 기능을 사용하여 백그라운드에서 일회성 또는 예약된 이벤트 로그 검색을 실행하고 보고서를 생성합니다. 예약된 검색은 언제든지 수정하거나 취소할 수 있습니다. 일회성 검색 쿼리를 반복 검색으로 수정할 수도 있습니다.

참고
- 기록 이벤트에 대해서만 보고서를 생성하도록 예약할 수 있습니다.
- 시작, 완료 또는 실패한 보고서에 대한 알림을 수신하도록 선택할 수 있습니다.

예약하고 보고서를 생성하려면 다음 단계를 수행합니다.

프로시저

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

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

단계 **3** **Historical(**기록**)** 탭을 클릭하여 기록 이벤트 데이터를 볼 수 있습니다.

단계 **4** 검색 창에 검색 쿼리를 입력합니다.

단계 **5** **Search(**검색**)** 드롭다운을 클릭하고 **Schedule Report(**보고서 예약**)**를 선택합니다.

단계 **6** (선택 사항) 식별을 위한 보고서의 이름을 입력합니다.

단계 **7** 기본적으로 **Generate report now(**지금 보고서 생성**)** 확인란이 선택되어 있습니다. 선택하면 저장 시 보고서 생성이 시작됩니다.

단계 **8** **Setup recurring schedule(**반복 예약 설정 **)**을 확인하고 다음 설정을 구성합니다.

- **Search(**검색**) Logs for the Last(**최근 검색 로그**)**: 로그를 얼마나 이전까지 검색할지 지정합니다.
- **Frequency(**빈도**)**: 예약 검색을 수행할 빈도와 검색을 실행할 시간을 지정합니다.

단계 **9** 창 하단에서 예약된 검색 기준을 확인합니다. **Schedule and Generate Now(**지금 예약 및 생성**)**를클릭합니다. 즉시 검색을 시작하도록 선택하지 않은 경우 **Schedule Report(**보고서 예약**)**를 클릭합니다.

다음에 수행할 작업

예역된 검색 보고서는 Security Cloud Control에서 자동으로 삭제하기 전 최대 7일 동안 확인할 수 있습니다.

검색 보고서 다운로드

검색 결과 및 일정 쿼리는 Security Cloud Control가 자동으로 제거하기 전까지 7일 동안 저장됩니다. 보고서 사본을 CSV 형식으로 다운로드할 수 있습니다.

프로시저

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

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

단계 **3** **Reports(**보고서**)**를 클릭합니다.

단계 **4** **Actions(**작업**)** 열에서 보고서 옆에 있는 **Download(**다운로드**)**를 클릭하여 보고서를 다운로드합니다. .CSV 형식의 보고서 파일은 로컬 드라이브의 기본 저장 위치에 자동으로 다운로드됩니다.

단계 **5** (선택 사항) 검색 쿼리를 보고 보고서를 다운로드하려면 다음 단계를 수행합니다.

a) **Queries(**쿼리**)** 탭을 클릭합니다.
b) 검색 쿼리 세부 정보를 보려면 보고서를 확장합니다.
c) 확인하고 다운로드할 보고서 옆에 있는 **View Reports(**보고서 보기**)**를 클릭합니다.

d) **Download(**다운로드**)**를 클릭합니다.

Security Analytics and Logging의 이벤트 속성

이벤트 속성 설명

Security Cloud Control에서 사용하는 이벤트 속성은 FDM(Firepower Device Manager) 또는 ASDM(Adaptive Security Device Manager)에서 보고하는 것과 거의 동일합니다.

- ASA(Adaptive Security Appliance) 이벤트 속성에 대한 전체 설명은 Cisco ASA Series 시스템 로그 메시지를 참조하십시오.

일부 ASA 시스템 로그 이벤트는 "구문 분석"되며, 다른 이벤트에는 attribute:value 쌍을 사용하여 이벤트 로깅 테이블의 내용을 필터링할 때 사용할 수 있는 추가 속성이 있습니다. 시스템 로그 이벤트의 다른 중요한 속성은 다음 추가 항목을 참조하십시오.

- 구문 분석된 ASA 시스템 로그 이벤트
- 일부 시스템 로그 메시지에 대한 EventGroup 및 EventGroupDefinition 속성
- 시스템 로그 이벤트에 대한 이벤트 이름 속성
- 시간 속성

일부 시스템 로그 메시지에 대한 EventGroup 및 EventGroupDefinition 속성

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. 예를 들어 Event Logging(이벤트 로깅) 테이블의 검색 필드에 `apfw:415*`를 입력하여 애플리케이션 방화벽 이벤트를 필터링할 수 있습니다.

Syslog 메시지 클래스와 연결된 메시지 **ID** 번호

EventGroup	**EventGroupDefinition**	시스템 로그 메시지 **ID** 번호**(**처음 **3**자리**)**
aaa/auth	사용자 인증	109, 113
acl/session	액세스 목록/사용자 세션	106
apfw	애플리케이션 방화벽	415
bridge	투명 방화벽	110, 220
ca	PKI 인증 기관	717
citrix	Citrix 클라이언트	723

EventGroup	EventGroupDefinition	시스템 로그 메시지 ID 번호(처음 3자리)
clst	클러스터링	747
cmgr	카드 관리	323
config	CLI(Command Line Interface)	111, 112, 208, 308
csd	Secure Desktop	724
cts	Cisco TrustSec	776
dap	Dynamic Access Policy	734
eap, eapoudp	Network Admission Control용 EAPoUDP 또는 EAP	333, 334
eigrp	EIGRP 라우팅	336
email	이메일 프록시	719
ipaa/envmon	환경 모니터링	735
HA	페일오버	101, 102, 103, 104, 105, 210, 311, 709
idfw	ID 기반 방화벽	746
ids	Intrusion Detection System(침입 탐지 시스템)	733
ids/ips	침입 탐지 시스템/침입 방지 시스템	400
ikev2	IKEv2 툴킷	750, 751, 752
ip	IP 스택	209, 215, 313, 317, 408
ipaa	IP 주소 할당	735
ips	Intrusion Protection System(침입 방지 시스템)	401, 420
ipv6	IPv6	325
l4tm	차단 목록, 허용 목록, 그레이리스트	338
lic	라이선싱	444
mdm-proxy	MDM 프록시	802
nac	NAC(Network Admission Control)	731, 732
vpn/nap	IKE 및 IPsec/네트워크 액세스 포인트	713
np	네트워크 프로세서	319

EventGroup	EventGroupDefinition	시스템 로그 메시지 ID 번호(처음 3자리)
ospf	OSPF 라우팅	318, 409, 503, 613
passwd	비밀번호 암호화	742
PP	전화 프록시	337
rip	RIP 라우팅	107, 312
rm	리소스 관리자	321
sch	Smart Call Home	120
session	사용자 세션	108, 201, 202, 204, 302, 303, 304, 314, 405, 406, 407, 500, 502, 607, 608, 609, 616, 620, 703, 710
session/natpat	사용자 세션/NAT 및 PAT	305
snmp	SNMP	212
ssafe	ScanSafe	775
ssl/np ssl	SSL 스택/NP SSL	725
svc	SSL VPN 클라이언트	722
sys	시스템	199, 211, 214, 216, 306, 307, 315, 414, 604, 605, 606, 610, 612, 614, 615, 701, 711, 741
tre	트랜잭션 규칙 엔진	780
ucime	UC-IME	339
tag-switching	서비스 태그 스위칭	779
td	위협 탐지	733
VM	VLAN 매핑	730
vpdn	PPTP 및 L2TP 세션	213, 403, 603
vpn	IKE 및 IPSEC	316, 320, 402, 404, 501, 602, 702, 713, 714, 715
vpnc	VPN 클라이언트	611
vpnfo	VPN 페일오버	720
vpnlb	VPN 로드 밸런싱	718
vxlan	VXLAN	778
webfo	WebVPN 페일오버	721
webvpn	WebVPN 및 AnyConnect Client	716

EventGroup	EventGroupDefinition	시스템 로그 메시지 ID 번호(처음 3자리)
session/natpat	사용자 세션/NAT 및 PAT	305

Syslog 이벤트에 대한 이벤트 이름 속성

일부 시스템 로그 이벤트에는 추가 속성 "EventName"이 있습니다. attribute:value 쌍을 기준으로 필터링하여 EventName 특성을 사용하여 이벤트 테이블을 필터링하여 찾을 수 있습니다. 예를 들어 Event Logging(이벤트 로깅) 테이블의 검색 필드에 **EventName:"Denied IP Packet"**을 입력하여 "Denied IP packet(거부된 IP 패킷)"에 대한 이벤트를 필터링할 수 있습니다.

시스템 로그 이벤트 **ID** 및 이벤트 이름 테이블

- AAA 시스템 로그 이벤트 ID 및 이벤트 이름
- 봇넷 시스템 로그 이벤트 ID 및 이벤트 이름
- 페일오버 시스템 로그 이벤트 ID 및 이벤트 이름
- 방화벽 거부 시스템 로그 이벤트 ID 및 이벤트 이름
- 방화벽 트래픽 시스템 로그 이벤트 ID 및 이벤트 이름
- ID 기반 방화벽 시스템 로그 이벤트 ID 및 이벤트 이름
- IPSec 시스템 로그 이벤트 ID 및 이벤트 이름
- NAT 시스템 로그 이벤트 ID 및 이벤트 이름
- SSL VPN 시스템 로그 이벤트 ID 및 이벤트 이름

AAA 시스템 로그 이벤트 **ID** 및 이벤트 이름

이벤트 ID	이벤트 이름
109001	AAA Begin
109002	AAA Failed
109003	AAA Server Failed
109005	Authentication Success
109006	Authentication Failed
109007	Authorization Success
109008	Authorization Failed
109010	AAA Pending
109011	AAA Session Started

이벤트 ID	이벤트 이름
109012	AAA Session Ended
109013	AAA
109014	AAA Failed
109016	AAA ACL not found
109017	AAA Limit Reach
109018	AAA ACL Empty
109019	AAA ACL error
109020	AAA ACL error
109021	AAA error
109022	AAA HTTP limit reached
109023	AAA auth required
109024	Authorization Failed
109025	Authorization Failed
109026	AAA error
109027	AAA Server error
109028	AAA Bypassed
109029	AAA ACL error
109030	AAA ACL error
109031	Authentication Failed
109032	AAA ACL error
109033	Authentication Failed
109034	Authentication Failed
109035	AAA Limit Reach
113001	AAA Session limit reach
113003	AAA overridden
113004	AAA Successful
113005	Authorization Rejected
113006	AAA user locked

이벤트 ID	이벤트 이름
113007	AAA User unlocked
113008	AAA successful
113009	AAA retrieved
113010	AAA Challenge received
113011	AAA retrieved
113012	Authentication Successful
113013	AAA error
113014	AAA error
113015	Authentication Rejected
113016	AAA Rejected
113017	AAA Rejected
113018	AAA ACL error
113019	AAA Disconnected
113020	AAA error
113021	AAA Logging Fail
113022	AAA Failed
113023	AAA reactivated
113024	AAA Client certification
113025	AAA Authentication fail
113026	AAA error
113027	AAA error

봇넷 시스템 로그 이벤트 **ID** 및 이벤트 이름

이벤트 ID	이벤트 이름
338001	Botnet Source Block List
338002	Botnet Destination Block List
338003	Botnet Source Block List
338004	Botnet Destination Block List

이벤트 ID	이벤트 이름
338101	Botnet Source Allow List
338102	Botnet destination Allow List
338202	Botnet destination Grey
338203	Botnet Source Grey
338204	Botnet Destination Grey
338301	Botnet DNS Intercepted
338302	Botnet DNS
338303	Botnet DNS
338304	Botnet Download successful
338305	Botnet Download failed
338306	Botnet Authentication failed
338307	Botnet Decrypt failed
338308	Botnet Client
338309	Botnet Client
338310	Botnet dyn filter failed

페일오버 시스템 로그 이벤트 **ID** 및 이벤트 이름

이벤트 ID	이벤트 이름
101001	Failover Cable OK
101002	Failover Cable BAD
101003	Failover Cable not connected
101004	Failover Cable not connected
101005	Failover Cable reading error
102001	Failover Power failure
103001	No response from failover mate
103002	Failover mate interface OK
103003	Failover mate interface BAD
103004	Failover mate reports failure

이벤트 ID	이벤트 이름
103005	Failover mate reports self failure
103006	Failover version incompatible
103007	Failover version difference
104001	Failover role switch
104002	Failover role switch
104003	Failover unit failed
104004	Failover unit OK
106100	Permit/Denied by ACL
210001	Stateful Failover error
210002	Stateful Failover error
210003	Stateful Failover error
210005	Stateful Failover error
210006	Stateful Failover error
210007	Stateful Failover error
210008	Stateful Failover error
210010	Stateful Failover error
210020	Stateful Failover error
210021	Stateful Failover error
210022	Stateful Failover error
311001	Stateful Failover update
311002	Stateful Failover update
311003	Stateful Failover update
311004	Stateful Failover update
418001	Denied Packet to Management
709001	Failover replication error
709002	Failover replication error
709003	Failover replication start
709004	Failover replication complete

이벤트 ID	이벤트 이름
709005	Failover receive replication start
709006	Failover receive replication complete
709007	Failover replication failure
710003	Denied access to Device

방화벽 거부 시스템 로그 이벤트 **ID** 및 이벤트 이름

이벤트 ID	이벤트 이름
106001	Denied by Security Policy
106002	Outbound Deny
106006	Denied by Security Policy
106007	Denied Inbound UDP
106008	Denied by Security Policy
106010	Denied by Security Policy
106011	Denied Inbound
106012	Denied due to Bad IP option
106013	Dropped Ping to PAT IP
106014	Denied Inbound ICMP
106015	Denied by Security Policy
106016	Denied IP Spoof
106017	Denied due to Land Attack
106018	Denied outbound ICMP
106020	Denied IP Packet
106021	Denied TCP
106022	Denied Spoof packet
106023	Denied IP Packet
106025	Dropped Packet failed to Detect context
106026	Dropped Packet failed to Detect context
106027	Dropped Packet failed to Detect context

이벤트 **ID**	이벤트 이름
106100	Permit/Denied by ACL
418001	Denied Packet to Management
710003	Denied access to Device

방화벽 트래픽 시스템 로그 이벤트 **ID** 및 이벤트 이름

이벤트 **ID**	이벤트 이름
108001	Inspect SMTP
108002	Inspect SMTP
108003	Inspect ESMTP Dropped
108004	Inspect ESMTP
108005	Inspect ESMTP
108006	Inspect ESMTP Violation
108007	Inspect ESMTP
110002	No Router found
110003	Failed to Find Next hop
209003	Fragment Limit Reach
209004	Fragment invalid Length
209005	Fragment IP discard
302003	H245 Connection Start
302004	H323 Connection start
302009	Restart TCP
302010	Connection USAGE
302012	H225 CALL SIGNAL CONN
302013	Built TCP
302014	Teardown TCP
302015	Built UDP
302016	Teardown UDP
302017	Built GRE

이벤트 ID	이벤트 이름
302018	Teardown GRE
302019	H323 Failed
302020	Built ICMP
302021	Teardown ICMP
302022	Built TCP Stub
302023	Teardown TCP Stub
302024	Built UDP Stub
302025	Teardown UDP Stub
302026	Built ICMP Stub
302027	Teardown ICMP Stub
302033	Connection H323
302034	H323 Connection Failed
302035	Built SCTP
302036	Teardown SCTP
303002	FTP file download/upload
303003	Inspect FTP Dropped
303004	Inspect FTP Dropped
303005	Inspect FTP reset
313001	ICMP Denied
313004	ICMP Drop
313005	ICMP Error Msg Drop
313008	ICMP ipv6 Denied
324000	GTP Pkt Drop
324001	GTP Pkt Error
324002	Memory Error
324003	GTP Pkt Drop
324004	GTP Version 지원하지 않음
324005	GTP Tunnel Failed

이벤트 ID	이벤트 이름
324006	GTP Tunnel Failed
324007	GTP Tunnel Failed
337001	Phone Proxy SRTP Failed
337002	Phone Proxy SRTP Failed
337003	Phone Proxy SRTP Auth Fail
337004	Phone Proxy SRTP Auth Fail
337005	Phone Proxy SRTP no Media Session
337006	Phone Proxy TFTP Unable to Create File
337007	Phone Proxy TFTP Unable to Find File
337008	Phone Proxy Call Failed
337009	Phone Proxy Unable to Create Phone Entry
400000	IPS IP options-Bad Option List
400001	IPS IP options-Record Packet Route
400002	IPS IP options-Timestamp
400003	IPS IP options-Security
400004	IPS IP options-Loose Source Route
400005	IPS IP options-SATNET ID
400006	IPS IP options-Strict Source Route
400007	IPS IP Fragment Attack
400008	IPS IP Impossible Packet
400009	IPS IP Fragments Overlap
400010	IPS ICMP Echo Reply
400011	IPS ICMP Host Unreachable
400012	IPS ICMP Source Quench
400013	IPS ICMP Redirect
400014	IPS ICMP Echo Request
400015	IPS ICMP Time Exceeded for a Datagram
400017	IPS ICMP Timestamp Request

이벤트 ID	이벤트 이름
400018	IPS ICMP Timestamp Reply
400019	ICMP Information Request
400020	IPS ICMP Information Reply
400021	ICMP Address Mask Request
400022	ICMP Address Mask Request
400023	IPS Fragmented ICMP Traffic
400024	IPS Large ICMP Traffic
400025	IPS Ping of Death Attack
400026	IPS TCP NULL flags
400027	IPS TCP SYN+FIN flags
400028	IPS TCP FIN only flags
400029	IPS FTP Improper Address Specified
400030	IPS FTP Improper Port Specified
400031	IPS UDP Bomb attack
400032	IPS UDP Snork attack
400033	IPS UDP Chargen DoS attack
400034	IPS DNS HINFO Request
400035	IPS DNS Zone Transfer
400036	IPS DNS Zone Transfer from High Port
400037	IPS DNS Request for All Records
400038	IPS RPC Port Registration
400039	IPS RPC Port Unregistration
400040	IPS RPC Dump
400041	IPS Proxied RPC Request
400042	IPS YP server Portmap Request
400043	IPS YP bind Portmap Request
400044	IPS YP password Portmap Request
400045	IPS YP update Portmap Request

이벤트 ID	이벤트 이름
400046	IPS YP transfer Portmap Request
400047	IPS Mount Portmap Request
400048	IPS Remote execution Portmap Request
400049	IPS Remote execution Attempt
400050	IPS Statd Buffer Overflow
406001	Inspect FTP Dropped
406002	Inspect FTP Dropped
407001	Host Limit Reach
407002	Embryonic limit Reached
407003	Established limit Reached
415001	Inspect Http Header Field Count
415002	Inspect Http Header Field Length
415003	Inspect Http body Length
415004	Inspect Http content-type
415005	Inspect Http URL length
415006	Inspect Http URL Match
415007	Inspect Http Body Match
415008	Inspect Http Header match
415009	Inspect Http Method match
415010	Inspect transfer encode match
415011	Inspect Http Protocol Violation
415012	Inspect Http Content-type
415013	Inspect Http Malformed
415014	Inspect Http Mime-Type
415015	Inspect Http Transfer-encoding
415016	Inspect Http Unanswered
415017	Inspect Http Argument match
415018	Inspect Http Header length

이벤트 ID	이벤트 이름
415019	Inspect Http status Matched
415020	Inspect Http non-ASCII
416001	Inspect SNMP dropped
419001	Dropped packet
419002	Duplicate TCP SYN
419003	Packet modified
424001	Denied IP Packet
424002	Dropped Packet
431001	Dropped RTP
431002.	Dropped RTCP
500001	Inspect ActiveX
500002	Inspect Java
500003	Inspect TCP Header
500004	Inspect TCP Header
500005	Inspect Connection Terminated
508001	Inspect DCERPC Dropped
508002	Inspect DCERPC Dropped
509001	Prevented No Forward Cmd
607001	Inspect SIP
607002	Inspect SIP
607003	Inspect SIP
608001	Inspect Skinny
608002	Inspect Skinny dropped
608003	Inspect Skinny dropped
608004	Inspect Skinny dropped
608005	Inspect Skinny dropped
609001	Built Local-Host
609002	Teardown Local Host

이벤트 ID	이벤트 이름
703001	H225 Unsupported Version
703002	H225 Connection
726001	Inspect Instant Message

ID 기반 방화벽 시스템 로그 이벤트 **ID** 및 이벤트 이름

이벤트 ID	이벤트 이름
746001	Import started
746002	Import complete
746003	Import failed
746004	Exceed user group limit
746005	AD Agent down
746006	AD Agent out of sync
746007	Netbios response failed
746008	Netbios started
746009	Netbios stopped
746010	Import user failed
746011	Exceed user limit
746012	User IP add
746013	User IP delete
746014	FQDN Obsolete
746015	FQDN resolved
746016	DNS lookup failed
746017	Import user issued
746018	Import user done
746019	Update AD Agent failed

IPSec 시스템 로그 이벤트 **ID** 및 이벤트 이름

이벤트 ID	이벤트 이름
402114	Invalid SPI received

이벤트 ID	이벤트 이름
402115	Unexpected protocol received
402116	Packet doesn't match identity
402117	Non-IPSEC packet received
402118	Invalid fragment offset
402119	Anti-Replay check failure
402120	Authentication failure
402121	Packet dropped
426101	cLACP Port Bundle
426102	cLACP Port Standby
426103	cLACP Port Moved To Bundle From Standby
426104	cLACP Port Unbundled
602103	Path MTU updated
602104	Path MTU exceeded
602303	New SA created
602304	SA deleted
702305	SA expiration - Sequence rollover
702307	SA expiration - Data rollover

NAT 시스템 로그 이벤트 **ID** 및 이벤트 이름

이벤트 ID	이벤트 이름
201002	Max connection Exceeded for host
201003	Embryonic limit exceed
201004	UDP connection limit exceed
201005	FTP connection failed
201006	RCMD connection failed
201008	New connection Disallowed
201009	Connection Limit exceed
201010	Embryonic Connection limit exceeded
201011	Connection Limit exceeded
201012	Per-client embryonic connection limit exceeded
201013	Per-client connection limit exceeded
202001	Global NAT exhausted

이벤트 ID	이벤트 이름
202005	Embryonic connection error
202011	Connection Limit exceeded
305005	No NAT group found
305006	Translation failed
305007	Connection dropped
305008	NAT allocation issue
305009	NAT Created
305010	NAT teardown
305011	PAT created
305012	PAT teardown
305013	Connection denied

SSL VPN 시스템 로그 이벤트 **ID** 및 이벤트 이름

이벤트 ID	이벤트 이름
716001	WebVPN Session Started
716002	WebVPN Session Terminated
716003	WebVPN User URL access
716004	WebVPN User URL access denied
716005	WebVPN ACL error
716006	WebVPN User Disabled
716007	WebVPN Unable to Create
716008	WebVPN Debug
716009	WebVPN ACL error
716010	WebVPN User access network
716011	WebVPN User access
716012	WebVPN User Directory access
716013	WebVPN User file access
716014	WebVPN User file access
716015	WebVPN User file access
716016	WebVPN User file access
716017	WebVPN User file access
716018	WebVPN User file access

이벤트 ID	이벤트 이름
716019	WebVPN User file access
716020	WebVPN User file access
716021	WebVPN user access file denied
716022	WebVPN Unable to connect proxy
716023	WebVPN session limit reached
716024	WebVPN User access error
716025	WebVPN User access error
716026	WebVPN User access error
716027	WebVPN User access error
716028	WebVPN User access error
716029	WebVPN User access error
716030	WebVPN User access error
716031	WebVPN User access error
716032	WebVPN User access error
716033	WebVPN User access error
716034	WebVPN User access error
716035	WebVPN User access error
716036	WebVPN User login successful
716037	WebVPN User login failed
716038	WebVPN User Authentication Successful
716039	WebVPN User Authentication Rejected
716040	WebVPN User logging denied
716041	WebVPN ACL hit count
716042	WebVPN ACL hit
716043	WebVPN Port forwarding
716044	WebVPN Bad Parameter
716045	WebVPN Invalid Parameter
716046	WebVPN connection terminated
716047	WebVPN ACL usage
716048	WebVPN memory issue
716049	WebVPN Empty SVC ACL
716050	WebVPN ACL error

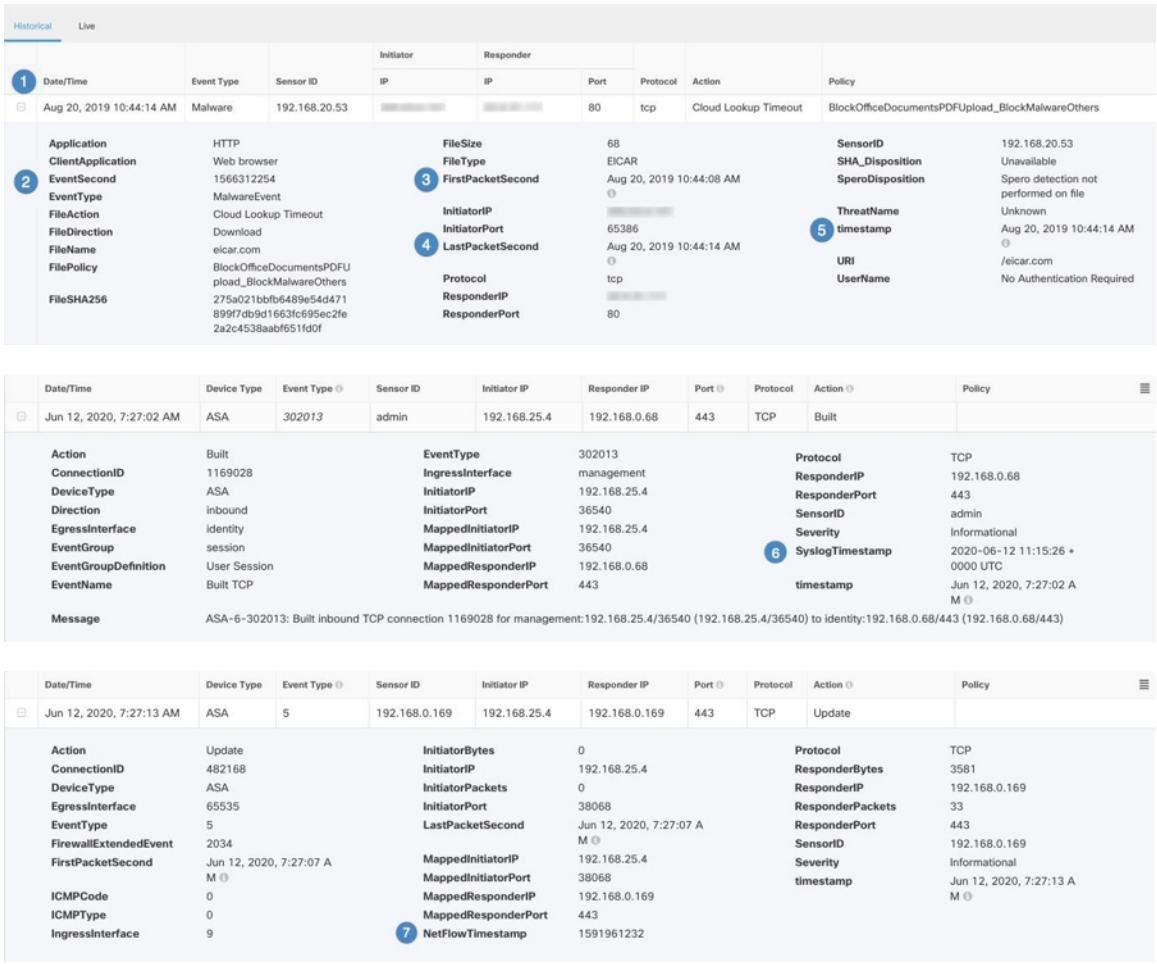
이벤트 ID	이벤트 이름
716051	WebVPN ACL error
716052	WebVPN Session Terminated
716053	WebVPN SSO Server added
716054	WebVPN SSO Server deleted
716055	WebVPN Authentication Successful
716056	WebVPN Authentication Failed
716057	WebVPN Session terminated
716058	WebVPN Session lost
716059	WebVPN Session resumed
716060	WebVPN Session Terminated
722001	WebVPN SVC Connect request error
722002	WebVPN SVC Connect request error
722003	WebVPN SVC Connect request error
722004	WebVPN SVC Connect request error
722005	WebVPN SVC Connect update issue
722006	WebVPN SVC Invalid address
722007	WebVPN SVC Message
722008	WebVPN SVC Message
722009	WebVPN SVC Message
722010	WebVPN SVC Message
722011	WebVPN SVC Message
722012	WebVPN SVC Message
722013	WebVPN SVC Message
722014	WebVPN SVC Message
722015	WebVPN SVC invalid frame
722016	WebVPN SVC invalid frame
722017	WebVPN SVC invalid frame
722018	WebVPN SVC invalid frame
722019	WebVPN SVC Not Enough Data
722020	WebVPN SVC no address
722021	WebVPN Memory issue
722022	WebVPN SVC connection established

이벤트 ID	이벤트 이름
722023	WebVPN SVC connection terminated
722024	WebVPN Compression Enabled
722025	WebVPN Compression Disabled
722026	WebVPN Compression reset
722027	WebVPN Decompression reset
722028	WebVPN Connection Closed
722029	WebVPN SVC Session terminated
722030	WebVPN SVC Session terminated
722031	WebVPN SVC Session terminated
722032	WebVPN SVC connection Replacement
722033	WebVPN SVC Connection established
722034	WebVPN SVC New connection
722035	WebVPN Received Large packet
722036	WebVPN transmitting Large packet
722037.	WebVPN SVC connection closed
722038	WebVPN SVC session terminated
722039	WebVPN SVC invalid ACL
722040	WebVPN SVC invalid ACL
722041	WebVPN SVC IPv6 not available
722042	WebVPN invalid protocol
722043	WebVPN DTLS disabled
722044	WebVPN unable to request address
722045	WebVPN Connection terminated
722046	WebVPN Session terminated
722047	WebVPN Tunnel terminated
722048	WebVPN Tunnel terminated
722049	WebVPN Session terminated
722050	WebVPN Session terminated
722051	WebVPN address assigned
722053	WebVPN Unknown client
723001	WebVPN Citrix connection Up
723002	WebVPN Citrix connection Down

이벤트 ID	이벤트 이름
723003	WebVPN Citrix no memory issue
723004	WebVPN Citrix bad flow control
723005	WebVPN Citrix no channel
723006	WebVPN Citrix SOCKS error
723007	WebVPN Citrix connection list broken
723008	WebVPN Citrix invalid SOCKS
723009	WebVPN Citrix invalid connection
723010	WebVPN Citrix invalid connection
723011	WebVPN citrix Bad SOCKS
723012	WebVPN Citrix Bad SOCKS
723013	WebVPN Citrix invalid connection
723014	WebVPN Citrix connected to Server
724001	WebVPN Session not allowed
724002	WebVPN Session terminated
724003	WebVPN CSD
724004	WebVPN CSD
725001	SSL handshake Started
725002	SSL Handshake completed
725003	SSL Client session resume
725004	SSL Client request Authentication
725005	SSL Server request authentication
725006	SSL Handshake failed
725007	SSL Session terminated
725008	SSL Client Cipher
725009	SSL Server Cipher
725010	SSL Cipher
725011	SSL Device choose Cipher
725012	SSL Device choose Cipher
725013	SSL Server choose cipher
725014.	SSL LIB error
725015	SSL client certificate failed

시스템 로그 이벤트의 시간 속성

Event Logging(이벤트 로깅) 페이지에서 다양한 타임스탬프의 목적을 이해하면 원하는 이벤트를 필터링하고 찾을 수 있습니다.



번호	라벨	설명
1	날짜/시간	SEC(Secure Event Connector)가 이벤트를 처리한 시간. 방화벽이 해당 트래픽을 검사한 시간과 다를 수 있습니다. 타임스탬프와 동일한 값입니다.
2	EventSecond	LastPacketSecond와 같음.

번호	라벨	설명
3	FirstPacketSecond	연결이 열린 시간입니다. 이때 방화벽은 패킷을 검사합니다. FirstPacketSecond의 값은 LastPacketSecond에서 ConnectionDuration을 빼서 계산됩니다. 연결 시작 시 로깅된 연결 이벤트의 경우 FirstPacketSecond, LastPacketSecond 및 EventSecond 값은 모두 동일합니다.
4	LastPacketSecond	연결이 닫힌 시간입니다. 연결 종료 시 로깅된 연결 이벤트의 경우, LastPacketSecond 및 EventSecond는 동일합니다.
5	timestamp	SEC(Secure Event Connector)가 이벤트를 처리한 시간. 방화벽이 해당 트래픽을 검사한 시간과 다를 수 있습니다. 날짜/시간과 동일한 값입니다.
6	시스템 로그 타임스탬프	'logging timestamp'가 사용되는 경우 시스템 로그가 시작된 시간을 나타냅니다. 시스템 로그에 이 정보가 없으면 SEC가 이벤트를 수신한 시간이 반영됩니다.
7	NetflowTimeStamp	ASA에서 NetFlow 패킷을 채운 다음 플로우 컬렉터로 전송할 충분한 플로우 레코드/이벤트 수집을 완료한 시간입니다.