Firepower eStreamer 통합 가이드

버전 6.2.3
2018년 6월 7일

Cisco Systems, Inc.
www.cisco.com
Cisco는 전 세계에 200개가 넘는 지사를 운영하고 있습니다.
주소, 전화 번호 및 팩스 번호는
다음 Cisco 웹사이트에 나와 있습니다.
www.cisco.com/go/offices에서 확인하십시오.

동봉한 제품의 소프트웨어 라이센스 및 제한된 보증은 제품과 함께 제공된 정보 패킷에 설명되어 있으며 본 문서에 참조를 통해 포함됩니다. 소프트웨어 라이센스 또는 제한 보증을 찾을 수 없는 경우 CISCO 담당자에게 사본을 요청하십시오.

Cisco의 TCP 헤더 압축은 UNIX 운영 체제의 UCB 공개 도메인 버전의 일부로서 University of California, Berkeley(UCB)에서 개발된 프로그램을 적용하여 구현합니다. All rights reserved. Copyright © 1981, Regents of the University of California.

여기에 언급된 기타 모든 보증에도 불구하고 이러한 공급자의 모든 문서 및 소프트웨어는 모든 결함이 포함된 "있는 그대로" 제공됩니다. CISCO 및 위에 언급된 모든 공급업체는 상품성, 특정 목적에의 적합성, 타인의 권리 비침해 또는 처리, 사용, 거래 행위로 발생하는 문제에 대한 묵시적 보증을 포함하여(단, 이에 한하지 않음) 묵시적이든 명시적이든 모든 종류의 보증을 부인합니다.

Cisco 또는 해당 공급업체는 피해의 가능성에 대해 언급한 경우라도 이 설계의 사용 또는 사용 불능으로 인해 발생하는 이익 손실, 데이터 손실 또는 손상을 포함하여(단, 이에 한하지 않음) 간접, 특별, 중대 또는 부수적 손해에 대해 어떠한 경우라도 책임을 지지 않습니다.

Cisco 및 Cisco 로고는 미국 및 기타 국가에서 Cisco Systems, Inc. 및/또는 계열사의 상표 또는 등록 상표입니다. Cisco 상표 목록을 보려면 다음 URL로 이동하십시오. www.cisco.com/go/trademarks 여기에 언급된 타사 상표는 해당 소유자의 자산입니다. 파트너라는 용어의 사용이 Cisco와 다른 업체 사이의 제휴 관계를 의미하는 것은 아닙니다. (1110R)

이 문서에서 사용된 모든 IP(인터넷 프로토콜) 주소와 전화 번호는 실제 주소와 전화 번호가 아닙니다. 이 문서에 포함된 예제, 명령 표시 출력, 네트워크 토폴로지 다이어그램 및 다른 그림은 이해를 돕기 위한 자료일 뿐이며, 실제 IP 주소나 전화 번호가 사용되었다면 이는 의도하지 않은 우연의 일치입니다.

목 차 2018년

소개

eStreamer라고도 하는 Cisco Event Streamer에서는 외부 클라이언트 애플리케이션으로 Firepower System 이벤트를 스트리밍할 수 있습니다. 관리 센터에서는 호스트, 검색, 상관관계, 컴플라이언스 화이트리스트, 침입, 사용자 활동, 파일, 악성코드 및 연결 데이터를, 그리고 7000/8000 Series 디바이스에서는 침입 데이터를 스트리밍할 수 있습니다.

NGIPSv, Firepower Services, Firepower Threat Defense Virtual 및 Firepower Threat Defense에서는 eStreamer가 지원되지 않습니다. 이러한 디바이스에서 이벤트를 스트리밍하려는 경우 해당 디바이스가 보고하는 관리 센터에 eStreamer를 구성할 수 있습니다.

eStreamer는 맞춤형 애플리케이션 계층 프로토콜을 사용하여 연결된 클라이언트 애플리케이션과 통신합니다. eStreamer는 단순히 클라이언트가 요청하는 데이터를 반환하는 용도로만 사용되므로, 이 가이드에서는 요청된 데이터에 대한 eStreamer 형식에 대해 중점적으로 설명합니다.

eStreamer 클라이언트를 생성하여 Firepower System과 통합할 때는 다음의 세 가지 주요 단계를 수행합니다.

1. eStreamer 애플리케이션 프로토콜을 사용하여 Management Center 또는 매니지드 디바이스와 메시지를 교환하는 클라이언트 애플리케이션을 작성합니다. 참조 클라이언트 애플리케이션은 eStreamerSDK에 포함되어 있습니다.
2. 필요한 이벤트 유형을 클라이언트 애플리케이션으로 전송하도록 관리 센터 또는 디바이스를 구성합니다.
3. 클라이언트 애플리케이션을 Management Center 또는 디바이스에 연결하고 데이터 교환을 시작합니다.

이 가이드에서는 eStreamer 버전 6.2.3 클라이언트 애플리케이션을 올바르게 생성 및 실행하는 데 필요한 정보를 제공합니다.

eStreamer 버전 6.2.3의 주요 변경 사항

예시 연결 통계 데이터 블록이 데이터 구조 예시에 추가되었습니다.

가이드 사용법

간단하게 설명하자면 eStreamer 서비스는 Firepower System에서 요청 클라이언트로 데이터를 스트리밍하기 위한 메커니즘입니다. 서비스는 다음 데이터 카테고리를 스트리밍할 수 있습니다.

- 침입 이벤트 데이터 및 이벤트 추가 데이터
- 상관관계(컴플라이언스) 이벤트 데이터

- 검색 이벤트 데이터
- 사용자 이벤트 데이터
- 이벤트의 메타데이터
- 호스트 정보
- 악성코드 이벤트 데이터

이 설명서에 포함된 대부분의 정보는 eStreamer에서 반환하는 데이터 구조에 대한 설명입니다. 이 설명서에는 다음 장이 포함되어 있습니다.

- eStreamer 애플리케이션 프로토콜 이해, 2-1페이지: eStreamer 통신의 개요를 제공하고, eStreamer 클라이언트 애플리케이션 작성을 위한 몇 가지 요구 사항을 자세히 설명하고, eStreamer 서비스로 명령을 보내고 해당 서비스에서 데이터를 받는 데 사용되는 네 가지 메시지 유형에 대해 설명합니다.
- 침입 및 상관관계 데이터 구조 이해, 3-1페이지: 침입 탐지 및 상관관계 구성 요소에서 생성된 이벤트 데이터를 반환하는 데 사용되는 데이터 형식과, 침입 및 상관관계 이벤트를 나타내는 데 사용되는 데이터 형식에 대해 설명합니다.
- 검색 및 연결 데이터 구조 이해, 4-1페이지: 검색, 사용자 및 연결 이벤트 데이터를 반환하는 데 사용되는 데이터 형식에 대해 설명합니다.
- 호스트 데이터 구조 이해, 5-1페이지: eStreamer에서 호스트 정보 요청 메시지를 수신하는 경우 전체 호스트 정보 데이터를 반환하는 데 사용하는 데이터 형식에 대해 설명합니다.
- eStreamer 구성, 6-1페이지: Management Center 또는 매니지드 디바이스에서 eStreamer를 구성하는 방법에 대해 설명합니다. 이 장에서는 eStreamer 커맨드 라인 스위치에 대해서도 설명하고, eStreamer 서비스를 수동으로 시작 및 중지하는 지침 및 eStreamer를 자동으로 시작하도록 Management Center 또는 매니지드 디바이스를 구성하는 지침도 제공합니다.
- 데이터 구조 예시, A-1페이지: 이진 형식의 eStreamer 메시지 패킷 예시를 제공합니다.
- 레거시 데이터 구조 이해, B-1페이지: 현재 제공되는 제품에서는 더 이상 사용되지 않지만 이전 클라이언트에서는 사용될 수 있는 레거시 데이터 구조에 대해 설명합니다.

전제조건

이 가이드의 정보를 이해하려면 Firepower System의 기능과 명명법 및 해당 구성 요소의 전반적인 기능(특히 이러한 구성 요소가 생성하는 이벤트 데이터의 여러 가지 유형)에 대해 잘 알고 있어야 합니다. 알 수 없는 용어나 제품과 관련된 용어의 정의는 *Firepower eStreamer 통합 가이드*에서 확인할 수 있는 경우가 많습니다.

Firepower System 릴리스의 제품 버전

이 가이드 전체에서는 버전 번호를 사용하여 Management Center 및 매니지드 디바이스에서 생성되는 이벤트의 데이터 형식에 대해 설명합니다. 각 제품의 주 릴리스별 버전은 Firepower System 제품 버전 표에 나와 있습니다.

표 1-1 Firepower System 제품 버전

릴리스	Management Center 버전	마스터 Management Center 버전	침입 센서 버전	센서 버전	매니지드 디바이스 버전
IMS 3.0	관리 콘솔 3.0	해당 없음	네트워크 센서 3.0	해당 없음	해당 없음
IMS 3.1	관리 콘솔 3.1	해당 없음	네트워크 센서 3.1	RNA 센서 1.0	해당 없음
IMS 3.2	관리 콘솔 3.2	해당 없음	네트워크 센서 3.2	RNA 센서 2.0	해당 없음
3D 시스템 4.0	Management Center 4.0	해당 없음	침입 센서 4.0	RNA 센서 3.0	해당 없음
3D 시스템 4.5	Management Center 4.5	해당 없음	침입 센서 4.5	RNA 센서 3.5	해당 없음
3D 시스템 4.6.1	Management Center 4.6.1	마스터 Management Center 4.6.1	해당 없음	해당 없음	4.6.1
3D 시스템 4.7	Management Center 4.7	마스터 Management Center 4.7	해당 없음	해당 없음	4.7
3D 시스템 4.8	Management Center 4.8	마스터 Management Center 4.8	해당 없음	해당 없음	4.8
3D 시스템 4.8.0.2	Management Center 4.8.0.2	마스터 Management Center 4.8.0.2	해당 없음	해당 없음	4.8.0.2
3D 시스템 4.9	Management Center 4.9	마스터 Management Center 4.9	해당 없음	해당 없음	4.9
3D 시스템 4.9.1	Management Center 4.9.1	마스터 Management Center 4.9.1	해당 없음	해당 없음	4.9.1
3D 시스템 4.10	Management Center 4.10	마스터 Management Center 4.10	해당 없음	해당 없음	4.10
3D 시스템 4.10.1	Management Center 4.10.1	마스터 Management Center 4.10.1	해당 없음	해당 없음	4.10.1
3D 시스템 4.10.2	Management Center 4.10.2	마스터 Management Center 4.10.2	해당 없음	해당 없음	4.10.2
3D 시스템 4.10.3	Management Center 4.10.3	마스터 Management Center 4.10.3	해당 없음	해당 없음	4.10.3
3D 시스템 5.0	Management Center 5.0	해당 없음	해당 없음	해당 없음	5.0
3D 시스템 5.1	Management Center 5.1	해당 없음	해당 없음	해당 없음	5.1

표 1-1 Firepower System 제품 버전 (계속)

릴리스	Management Center 버전	마스터 Management Center 버전	침입 센서 버전	센서 버전	매니지드 디바이스 버전
3D 시스템 5.1.1	Management Center 5.1.1	해당 없음	해당 없음	해당 없음	5.1.1
3D 시스템 5.2	Management Center 5.2	해당 없음	해당 없음	해당 없음	5.2
3D 시스템 5.3	Management Center 5.3	해당 없음	해당 없음	해당 없음	5.3
Firepower System 5.3.1	Management Center 5.3.1	해당 없음	해당 없음	해당 없음	5.3.1
Firepower System 5.4	Management Center 5.4	해당 없음	해당 없음	해당 없음	5.4
Firepower System 6.0	Management Center 6.0	해당 없음	해당 없음	해당 없음	6.0
Firepower System 6.1	Management Center 6.1	해당 없음	해당 없음	해당 없음	6.1
Firepower System 6.2	Management Center 6.2	해당 없음	해당 없음	해당 없음	6.2
Firepower System 6.2.1	Management Center 6.2.1	해당 없음	해당 없음	해당 없음	6.2.1
Firepower System 6.2.2	Management Center 6.2.2	해당 없음	해당 없음	해당 없음	6.2.2

문서 표기 규칙

eStreamer 메시지 데이터 유형 규칙 표에는 eStreamer 메시지에서 사용되는 다양한 데이터 필드 형식을 설명하기 위해 이 설명서에서 사용되는 이름이 나와 있습니다. eStreamer 서비스에서 사용되는 숫자 상수는 대개 부호 없는 정숫값입니다. 별도로 명시되지 않은 경우 비트 필드에서는 하위 비트를 사용합니다. 예를 들어 플래그 데이터 5비트가 포함된 1바이트 필드에서는 하위 5비트에 데이터가 포함됩니다.

표 1-2 eStreamer 메시지 데이터 유형 규칙

데이터 유형	설명
nn-bit field	nn비트의 비트 필드
byte	임의 형식의 데이터를 포함하는 8비트 바이트
int8	부호 있는 8비트 바이트
uint8	부호 없는 8비트 바이트
int16	부호 있는 16비트 정수
uint16	부호 없는 16비트 정수
int32	부호 있는 32비트 정수

표 1-2 eStreamer 메시지 데이터 유형 규칙 (계속)

데이터 유형	설명
uint32	부호 없는 32비트 정수
uint64	부호 없는 64비트 정수
string	문자 데이터를 포함하는 가변 길이 필드
[n]	uint8[4]과 같이 표시된 데이터 유형의 n개 인스턴스를 나타내기 위해 위의 데이터 유형 뒤에 붙는 배열 아래 첨자
variable	다양한 데이터 유형 모음
BLOB	지정되지 않은 유형의 이진 개체(대개 패킷에서 캡처된 원시 데이터)

IP 주소

Cisco 데이터베이스에서는 IPv4 주소와 IPv6 주소가 같은 필드에 BINARY 형식으로 저장됩니다. IPv6 주소를 얻으려면 주소를 `20010db80000000000000000000004321`과 같이 16진수 표기법으로 변환합니다. 데이터베이스는 80~95비트를 1로 채워 IPv4 주소 저장을 위한 RFC를 준수하므로 유효하지 않은 IPv6 주소가 생성됩니다. 예를 들어, IPv4 주소 10.5.15.1은 `00000000000000000000FFFF0A050F01`로 저장됩니다.

eStreamer 애플리케이션 프로토콜 이해

Firepower System Event Streamer(eStreamer)는 메시지 지향 프로토콜을 사용하여 클라이언트 애플리케이션으로 이벤트 및 호스트 프로파일 정보를 스트리밍합니다. 클라이언트는 Management Center에서 이벤트 및 호스트 프로파일 데이터를 요청할 수 있으며 침입 이벤트 데이터는 매니지드 디바이스에서만 요청할 수 있습니다. 클라이언트 애플리케이션은 전송할 데이터를 지정하는 요청 메시지를 제출하여 데이터 스트림을 시작합니다. 그런 다음 스트리밍이 시작된 후에 Management Center 또는 매니지드 디바이스로부터의 메시지 플로우를 제어합니다.

이 문서 전체에서는 Management Center 또는 매니지드 디바이스의 eStreamer 서비스를 eStreamer 서버 또는 eStreamer로 지칭합니다.

다음 섹션에서는 eStreamer 서비스에 연결하기 위한 요구 사항에 대해 설명하고 eStreamer 프로토콜에서 사용되는 명령 및 데이터 형식을 소개합니다.

- 연결 사양, 2-1페이지에서는 eStreamer 서비스와 클라이언트 간의 통신 플로우와, 클라이언트가 해당 플로우와 상호작용하는 방법에 대해 설명합니다.
- eStreamer 통신 단계 이해, 2-2페이지에서는 클라이언트 애플리케이션이 eStreamer 서버로 데이터 요청을 제출하고 eStreamer가 요청된 정보를 클라이언트에 제공하기 위한 통신 프로토콜에 대해 설명합니다.
- eStreamer 메시지 유형 이해, 2-6페이지에서는 eStreamer 프로토콜에서 사용되는 메시지 유형과 eStreamer에서 침입 이벤트 데이터/검색 이벤트 데이터/메타데이터/호스트 데이터를 클라이언트로 반환하는 데 사용하는 데이터 패킷의 기본 구조에 대해 설명하며 eStreamer 메시지를 해석할 수 있는 클라이언트를 작성하는 데 도움이 되는 기타 정보를 제공합니다.

연결 사양

eStreamer 서비스는 다음과 같은 작업을 수행합니다.

- SSL 연결을 통해 TCP를 사용하여 통신합니다. 클라이언트 애플리케이션은 SSL 기반 인증을 지원해야 합니다.
- 포트 8302에서 연결 요청을 수락합니다.
- 클라이언트가 모든 통신 세션을 시작하도록 기다립니다.
- 네트워크 바이트 순서(big endian)로 모든 메시지 필드를 작성합니다.
- UTF-8로 텍스트를 인코딩합니다.

eStreamer 통신 단계 이해

클라이언트와 eStreamer 서비스 간에 수행되는 통신에서는 4가지 주요 단계가 진행됩니다.

1. 클라이언트가 eStreamer 서버와의 연결을 설정하며 양 당사자가 연결을 인증합니다.

   자세한 정보는 인증된 연결 설정, 2-2페이지의 내용을 참조하십시오.

2. 클라이언트가 eStreamer 서비스에서 데이터를 요청하고 스트리밍할 데이터의 유형을 지정합니다. 단일 이벤트 요청 메시지가 이벤트 메타데이터를 포함하여 사용 가능한 이벤트 데이터의 모든 조합을 지정할 수 있습니다. 단일 호스트 프로파일 요청은 단일 호스트 또는 여러 호스트를 지정할 수 있습니다.

   다음의 두 요청 모드를 사용하여 이벤트 데이터를 요청할 수 있습니다.

   - 이벤트 스트림 요청 - 클라이언트가 요청하는 이벤트 유형 및 각 유형의 버전을 지정하는 요청 플래그가 포함된 메시지를 제출하면 eStreamer 서버가 요청된 데이터를 스트리밍하여 응답합니다.
   - 확장 요청 - 클라이언트가 확장 요청용 플래그를 설정하여 이벤트 스트림 요청과 같은 메시지 형식으로 요청을 제출합니다. 그러면 클라이언트와 eStreamer 서버 간의 메시지 상호작용이 시작됩니다. 이 상호작용을 통해 클라이언트는 이벤트 스트림 요청을 통해서는 사용할 수 없는 추가 정보 및 버전 조합을 요청합니다.

   데이터 요청에 대한 자세한 정보는 eStreamer에서 데이터 요청, 2-3페이지의 내용을 참조하십시오.

3. eStreamer가 클라이언트에 대해 요청된 데이터 스트림을 설정합니다.

   자세한 정보는 eStreamer의 데이터 수락, 2-5페이지의 내용을 참조하십시오.

4. 연결이 종료됩니다.
   자세한 정보는 연결 종료, 2-6페이지의 내용을 참조하십시오.

인증된 연결 설정

eStreamer에서 데이터를 요청하려는 클라이언트는 먼저 eStreamer 서비스와의 SSL 지원 TCP 연결을 시작해야 합니다. 클라이언트는 Management Center 또는 매니지드 디바이스에 구성된 모든 관리 인터페이스에서 요청할 수 있습니다. 클라이언트 연결에서는 관리 인터페이스에 대해 트래픽 채널 컨피그레이션이 적용되지 않으므로 연결용 인터페이스를 선택할 때 컨피그레이션을 무시해도 됩니다. 클라이언트가 연결을 시작하면 eStreamer 서버가 응답하며, 클라이언트와의 SSL 핸드셰이크가 시작됩니다. SSL 핸드셰이크의 일부분으로 eStreamer 서버는 클라이언트의 인증 인증서를 요청하고 인증서가 유효한지, 즉 eStreamer 서버의 내부 CA(내부 인증 기관)에서 서명한 것인지를 확인합니다.

참고 시스코의 권장 사항에 따라, eStreamer 서버에서 제공한 인증서가 신뢰할 수 있는 인증 기관에서 서명한 것인지도 클라이언트가 확인하도록 하는 것이 좋습니다. 이 인증서는 Management Center 또는 매니지드 디바이스에 새 eStreamer 클라이언트를 등록할 때 시스코에서 제공하는 PKCS#12 파일에 포함된 내부 CA 인증서입니다. 자세한 정보는 eStreamer 클라이언트에 대한 인증 추가, 6-3페이지의 내용을 참조하십시오.

SSL 세션이 설정되고 나면 eStreamer 서버가 연결 후 인증서 추가 확인을 수행합니다. 이 과정에서는 클라이언트 연결이 인증서에 지정된 호스트에서 시작되었는지, 그리고 인증서의 주체 이름에 적절한 값이 포함되어 있는지를 확인합니다. 연결 후 검사 중 하나에서 장애가 발생하면 eStreamer 서버는 연결을 닫습니다. 필요한 경우 클라이언트 호스트 이름 검사를 수행하지 않도록 eStreamer 서비스를 구성할 수 있습니다(자세한 정보는 eStreamer 서비스 옵션, 6-5페이지 참조).

클라이언트는 연결 후 확인을 수행하지 않아도 되지만 시스코의 권장 사항에 따라 클라이언트가 이 확인 단계를 수행하도록 하는 것이 좋습니다. 인증 인증서의 인증서 주체 이름에는 다음 필드 값이 포함되어 있습니다.

표 2-1 인증서 주체 이름 필드

필드	값
title	eStreamer
generationQualifier	server

연결 후 확인이 완료되고 나면 eStreamer 서버는 클라이언트의 데이터 요청을 기다립니다.

eStreamer에서 데이터 요청

클라이언트는 데이터 요청 관리 과정에서 다음의 하이레벨 작업을 수행합니다.

- 요청 세션 초기화(세션 설정, 2-3페이지 참조)
- eStreamer 이벤트 아카이브에서 이벤트 요청(이벤트 스트림 요청 및 확장 요청을 사용하여 이벤트 스트리밍 시작, 2-3페이지)
- 호스트 데이터 요청(호스트 데이터 요청, 2-4페이지 참조)
- 요청 변경(요청 변경, 2-5페이지 참조)

세션 설정

클라이언트는 초기 이벤트 스트림 요청을 eStreamer 서비스로 전송하여 세션을 설정합니다.

이 초기 메시지에 데이터 요청 플래그를 포함할 수도 있고, 후속 메시지에서 데이터 요청을 제출할 수도 있습니다. 이 초기 이벤트 스트림 요청 메시지 자체는 모든 eStreamer 요청(이벤트 데이터 요청 또는 호스트 데이터 요청)의 전제조건입니다. 이벤트 스트림 요청 메시지를 사용하는 방법에 대한 자세한 정보는 이벤트 스트림 요청 메시지 형식, 2-10페이지의 내용을 참조하십시오.

참고 eStreamer 클라이언트는 Management Center 또는 매니지드 디바이스에 구성된 모든 관리 인터페이스에서 요청할 수 있습니다. 클라이언트 연결에서는 관리 인터페이스에 대해 트래픽 채널 컨피그레이션이 적용되지 않으므로 연결용 인터페이스를 선택할 때 컨피그레이션을 무시해도 됩니다.

이벤트 스트림 요청 및 확장 요청을 사용하여 이벤트 스트리밍 시작

eStreamer 서비스는 이벤트 스트리밍을 위한 두 가지 요청 모드를 제공합니다. 요청에서는 이 두 모드를 결합하여 사용할 수 있습니다. 두 모드에서 모두 클라이언트는 이벤트 스트림을 요청 메시지를 사용하여 요청을 시작하되 요청 플래그 비트는 각기 다르게 설정합니다. 이벤트 스트림 메시지 형식에 대한 자세한 정보는 이벤트 스트림 요청 메시지 형식, 2-10페이지의 내용을 참조하십시오.

eStreamer는 이벤트 스트림 요청 메시지를 받으면 클라이언트 요청을 다음과 같이 처리합니다.

- 요청 메시지의 요청 플래그 필드에 비트 30이 설정되어 있지 **않은** 경우 eStreamer에서는 요청 플래그 필드에 설정된 다른 비트로 요청된 이벤트의 스트리밍을 시작합니다. 자세한 정보는 이벤트 스트림 요청 제출, 2-4페이지의 내용을 참조하십시오.

- 이벤트 스트림 요청에 비트 30일 설정되어 **있는** 경우 eStreamer에서는 확장 요청 처리 기능을 제공합니다. 이 비트를 설정하는 경우에는 확장 요청 플래그를 전송해야 합니다. 자세한 정보는 확장 요청 제출, 2-4페이지의 내용을 참조하십시오. eStreamer에서는 모든 중복 요청을 확인합니다. 플래그나 확장 요청을 여러 개 포함하여 같은 데이터의 여러 버전을 요청하는 경우에는 가장 높은 버전이 사용됩니다. 예를 들어 eStreamer는 검색 이벤트 버전 1과 6에 해당하는 플래그 요청과 버전 3에 해당하는 확장 요청을 받으면 버전 6을 전송합니다.

이벤트 스트림 요청 제출

이벤트 스트림 요청에서는 다음과 같은 단순한 프로세스를 사용합니다.

- 클라이언트가 데이터 스트림에 포함할 이벤트 및 해당 버전 레벨을 지정하는 요청 플래그 필드와 시작 날짜/시간이 포함된 요청 메시지를 eStreamer 서비스로 전송합니다.
- eStreamer가 지정된 시간부터 이벤트를 스트리밍합니다. 스트리밍 프로토콜에 대한 자세한 정보는 eStreamer의 데이터 수락, 2-5페이지의 내용을 참조하십시오.

클라이언트의 이벤트 스트림 요청 메시지 형식과 콘텐츠에 대한 자세한 정보는 이벤트 스트림 요청 메시지 형식, 2-10페이지의 내용을 참조하십시오.

클라이언트가 요청할 수 있는 이벤트 유형 및 이벤트 버전에 대한 자세한 정보는 표 2-6, 2-12페이지의 내용을 참조하십시오.

확장 요청 제출

이벤트 스트림 요청 메시지의 요청 플래그 필드에 비트 30을 설정하는 경우 확장 요청이 시작되어 서버와의 협상이 시작됩니다. 이 비트를 설정하는 경우에는 확장 요청 플래그를 전송해야 합니다. 확장 요청에서 사용할 수 있는 이벤트 유형은 표 2-22, 2-37페이지의 내용을 참조하십시오.

확장 요청의 단계는 다음과 같습니다.

- 클라이언트가 요청 플래그 비트 30이 1(확장 요청을 나타냄)로 설정된 이벤트 스트리밍 요청 메시지를 eStreamer로 전송합니다. 메시지 형식에 대한 자세한 정보는 이벤트 스트림 요청 메시지 형식, 2-10페이지의 내용을 참조하십시오.
- eStreamer가 클라이언트에서 사용 가능한 서비스 목록을 알리는 스트리밍 정보 메시지로 응답을 합니다. 스트리밍 정보 메시지에 대한 자세한 정보는 스트리밍 정보 메시지 형식, 2-31페이지의 내용을 참조하십시오.
- 클라이언트가 사용하려는 서비스를 나타내는 스트리밍 요청 메시지를 반환합니다. 이 메시지에는 해당 서비스에서 사용 가능한 이벤트 유형 및 버전의 요청 목록이 포함되어 있습니다. 요청 목록은 표준 이벤트 스트림 요청 시 요청 플래그 필드에서 설정하는 비트에 해당하는 방식으로 사용됩니다. 스트리밍 요청 메시지를 사용하여 이벤트를 요청하는 방법에 대한 자세한 정보는 "샘플 확장 요청 메시지" 섹션, 2-39페이지의 내용을 참조하십시오.
- eStreamer에서 클라이언트의 스트리밍 요청 메시지를 처리하고 메시지에 지정된 시간에 데이터 스트리밍을 시작합니다. 스트리밍 프로토콜에 대한 자세한 정보는 eStreamer의 데이터 수락, 2-5페이지의 내용을 참조하십시오.

호스트 데이터 요청

세션을 설정한 후에는 언제든지 호스트 데이터에 대한 요청을 제출할 수 있습니다. eStreamer는 Firepower System 네트워크 맵에서 요청된 호스트에 대한 정보를 생성합니다.

요청 변경

설정된 세션에 대한 요청 파라미터를 변경하려면 클라이언트가 연결을 끊고 새 세션을 요청해야 합니다.

eStreamer의 데이터 수락

참고 eStreamer 서버는 전송하는 이벤트의 기록을 보관하지 않습니다. 그러므로 클라이언트 애플리케이션이 중복 이벤트를 확인해야 합니다. 중복 이벤트는 여러 가지 이유로 인해 의도치 않게 생성될 수 있습니다. 새 스트리밍 세션을 시작할 때 새 세션의 시작점으로 클라이언트가 지정한 시간에 메시지가 여러 개 있는데 그중 일부만 이전 세션에서 전송된 경우를 예로 들 수 있습니다. eStreamer에서는 지정된 요청 기준을 충족하는 모든 메시지를 보냅니다. 애플리케이션은 그로 인해 생성되는 중복 이벤트를 탐지해야 합니다.

eStreamer에서는 작업을 수행하지 않는 동안 클라이언트로 주기적인 null 메시지를 보내 연결을 열린 상태로 유지하며, 클라이언트나 중간 호스트에서 오류 메시지를 받으면 연결을 닫습니다.

eStreamer는 요청 모드에 따라 요청된 데이터를 각기 다른 방식으로 클라이언트에 전송합니다.

이벤트 스트림 요청

클라이언트가 이벤트 스트림 요청을 제출하는 경우 eStreamer는 메시지를 기준으로 데이터 메시지를 반환합니다. 이때 클라이언트의 승인을 기다리지 않고 한 행에 여러 메시지를 포함하여 전송할 수 있습니다. 특정 시점이 되면 eStreamer는 전송을 일시 중지하고 클라이언트의 응답을 기다립니다. 클라이언트 운영 체제는 받은 데이터를 버퍼링하여 클라이언트가 적절한 속도로 처리할 수 있도록 합니다.

클라이언트 요청에 메타데이터 요청이 포함된 경우 eStreamer에서는 먼저 메타데이터를 보냅니다. 클라이언트는 이후에 수신되는 이벤트 레코드를 처리할 때 사용할 수 있도록 메타데이터를 메모리에 저장해야 합니다.

확장 요청

클라이언트가 확장 요청을 제출하는 경우 eStreamer는 메시지를 대기시켰다가 번들로 전송합니다. 이때 eStreamer는 클라이언트의 승인을 기다리지 않고 한 행에 여러 번들을 포함하여 전송할 수 있습니다. 특정 시점이 되면 eStreamer는 전송을 일시 중지하고 클라이언트의 응답을 기다립니다. 클라이언트 운영 체제는 받은 데이터를 버퍼링하여 클라이언트가 적절한 속도로 데이터를 읽을 수 있도록 합니다.

클라이언트는 메시지 단위로 각 번들의 압축을 푼 다음 레코드와 블록의 길이를 사용하여 각 메시지의 구문을 분석합니다. 각 메시지 헤더에 전체 메시지 길이를 사용하여 각 메시지 끝에 도달하는 시기를 계산할 수 있으며, 전체 번들 길이를 사용하면 번들 끝에 도달하는 시기를 파악할 수 있습니다. 번들에 콘텐츠의 색인이 없어도 번들을 올바르게 구문 분석할 수 있습니다.

메시지 번들 생성 메커니즘에 대한 자세한 정보는 메시지 번들 형식, 2-40페이지의 내용을 참조하십시오.

클라이언트가 추가 플로우 제어에 사용할 수 있는 null 메시지에 대한 자세한 정보는 null 메시지 형식, 2-8페이지의 내용을 참조하십시오.

연결 종료

eStreamer 서버는 연결을 닫기 전에 오류 메시지 전송을 시도합니다. 오류 메시지에 대한 자세한 정보는 오류 메시지 형식, 2-8페이지의 내용을 참조하십시오.

eStreamer 서버는 다음과 같은 이유로 클라이언트 연결을 닫을 수 있습니다.

- 메시지 전송 시 오류가 발생할 때마다. 이러한 메시지에는 이벤트 데이터 메시지와 eStreamer에서 활동을 수행하지 않는 기간 동안 전송하는 null Keepalive 메시지가 모두 포함됩니다.
- 클라이언트 요청을 처리하는 중에 오류가 발생하는 경우
- 클라이언트 인증에서 장애가 발생하는 경우(오류 메시지는 전송되지 않음)
- eStreamer 서비스가 종료되는 경우(오류 메시지는 전송되지 않음)

클라이언트는 언제든지 eStreamer 서버에 대한 연결을 닫을 수 있으며, 오류 메시지 형식을 사용하여 eStreamer 서버에 연결이 닫힌 이유를 알리려고 시도합니다.

eStreamer 메시지 유형 이해

eStreamer 애플리케이션 프로토콜은 표준 메시지 헤더와 여러 하위 헤더 필드 뒤에 메시지 페이로드가 포함된 레코드 데이터가 들어 있는 단순한 메시지 형식을 사용합니다. 메시지 헤더는 모든 eStreamer 메시지 유형에서 동일합니다. 자세한 정보는 eStreamer 메시지 헤더, 2-7페이지의 내용을 참조하십시오.

표 2-2 eStreamer 메시지 유형

메시지 유형	이름	설명
0	null 메시지	eStreamer 서버와 클라이언트는 모두 데이터 플로우를 제어하기 위해 null 메시지를 보냅니다. 자세한 정보는 null 메시지 형식, 2-8페이지의 내용을 참조하십시오.
1	오류 메시지	eStreamer 서버와 클라이언트는 모두 연결이 닫힌 이유를 표시하기 위해 오류 메시지를 사용합니다. 자세한 정보는 오류 메시지 형식, 2-8페이지의 내용을 참조하십시오.
2	이벤트 스트림 요청	클라이언트는 새 스트리밍 세션을 시작하고 데이터를 요청하기 위해 eStreamer 서비스에 이 메시지 유형을 전송합니다. 자세한 정보는 이벤트 스트림 요청 메시지 형식, 2-10페이지의 내용을 참조하십시오.
4	이벤트 데이터	eStreamer서비스는 이벤트 데이터와 메타데이터를 클라이언트로 보내기 위해 이 메시지 유형을 사용합니다. 자세한 정보는 이벤트 데이터 메시지 형식, 2-17페이지의 내용을 참조하십시오.
5	호스트 데이터 요청	클라이언트는 호스트 데이터를 요청하기 위해 eStreamer 서비스에 이 메시지 유형을 보냅니다. 이벤트 스트림 요청 메시지를 통해 세션을 이미 시작한 상태여야 합니다. 자세한 정보는 호스트 요청 메시지 형식, 2-26페이지의 내용을 참조하십시오.

표 2-2 eStreamer 메시지 유형 (계속)

메시지 유형	이름	설명
6	단일 호스트 데이터	eStreamer 서비스는 클라이언트가 요청한 단일 호스트 데이터를 보내기 위해 이 메시지 유형을 사용합니다. 자세한 정보는 호스트 데이터 및 여러 호스트 데이터 메시지 형식, 2-30페이지의 내용을 참조하십시오.
7	여러 호스트 데이터	eStreamer 서비스는 클라이언트가 요청한 여러 호스트 데이터를 보내기 위해 이 메시지 유형을 사용합니다. 자세한 정보는 호스트 데이터 및 여러 호스트 데이터 메시지 형식, 2-30페이지의 내용을 참조하십시오.
2049	스트리밍 요청	클라이언트는 스트림 정보 메시지에서 알림을 제공받은 이벤트 중 원하는 이벤트를 지정하기 위해 확장 요청에서 이 메시지 유형을 사용합니다. 자세한 정보는 샘플 확장 요청 메시지, 2-39페이지의 내용을 참조하십시오.
2051	스트리밍 정보	eStreamer 서비스는 클라이언트에서 사용 가능한 서비스 목록을 알리기 위해 확장 요청에서 이 메시지 유형을 사용합니다. 자세한 정보는 스트리밍 정보 메시지 형식, 2-31페이지의 내용을 참조하십시오.
4002	메시지 번들	eStreamer 서비스는 클라이언트로 스트리밍하는 메시지를 패키징하기 위해 이 메시지 유형을 사용합니다. 자세한 정보는 메시지 번들 형식, 2-40페이지의 내용을 참조하십시오.

eStreamer 메시지 헤더

모든 eStreamer 메시지는 아래 그림에 나와 있는 메시지 헤더로 시작됩니다. 다음 표에서는 헤더의 필드에 대해 설명합니다.

표 2-3 표준 eStreamer 메시지 헤더 필드

필드	데이터 유형	설명
헤더 버전	uint16	메시지에 사용되는 헤더의 버전을 나타냅니다. 현재 eStreamer 버전의 경우 이 값은 항상 1입니다.
메시지 유형	uint16	전송되는 메시지의 유형을 나타냅니다. 현재 값 목록은 표 2-2, 2-6페이지의 내용을 참조하십시오.
메시지 길이	uint32	메시지 헤더 다음에 오는 콘텐츠의 길이를 나타냅니다. 메시지 헤더 자체의 바이트는 제외됩니다. 헤더가 하나이고 데이터는 없는 메시지의 메시지 길이는 0입니다.

null 메시지 형식

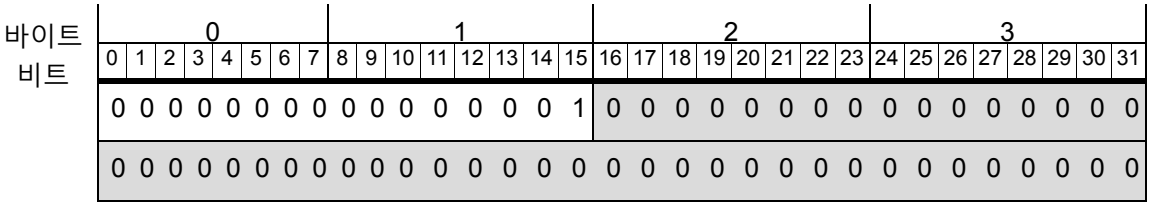
클라이언트 애플리케이션과 eStreamer 서비스는 모두 null 메시지를 전송합니다. null 메시지는 유형이 0이며 메시지 헤더 뒤에 데이터를 포함하지 않습니다.

클라이언트는 데이터를 더 수락할 준비가 되었음을 나타내기 위해 eStreamer 서버로 null 메시지를 전송합니다. eStreamer 서비스는 전송되는 데이터가 없을 때 연결을 유지하기 위해 클라이언트로 null 메시지를 전송합니다. null 메시지의 메시지 길잇값은 항상 0으로 설정됩니다.

팁 이 문서의 데이터 구조 다이어그램에서 (1) 또는 (115)와 같이 괄호 안에 들어 있는 정수는 상수 필드 값을 나타냅니다. 예를 들어 헤더 버전(1)은 설명 대상인 데이터 구조의 필드 값이 항상 1이라는 의미입니다.

아래에 null 메시지 형식이 나와 있습니다. 메시지에서 0이 아닌 값은 헤더 버전뿐입니다.

아래에는 이진 형식의 null 메시지 예시가 나와 있습니다. 이 메시지에서 0이 아닌 값은 헤더 버전 값인 1을 나타내는 두 번째 바이트뿐입니다. 메시지 유형 및 길이 필드(음영으로 표시됨)의 값은 각각 0입니다.



팁 이 가이드의 예시는 설정된 비트를 명확하게 표시하기 위해 이진 형식으로 나와 있습니다. 이벤트 요청 메시지 및 이벤트 영향 필드와 같은 일부 메시지는 이러한 형식으로 표시하는 것이 중요합니다.

오류 메시지 형식

클라이언트 애플리케이션과 eStreamer 서비스는 모두 오류 메시지를 사용합니다. 오류 메시지는 메시지 유형이 1이며 헤더, 오류 코드, 오류 텍스트 길이 및 실제 오류 텍스트를 포함합니다. 오류 텍스트는 0~65,535바이트를 포함할 수 있습니다.

클라이언트 애플리케이션용으로 맞춤형 오류 메시지를 생성할 때는 시스코의 권장 사항에 따라 오류 코드로 -1을 사용하는 것이 좋습니다.

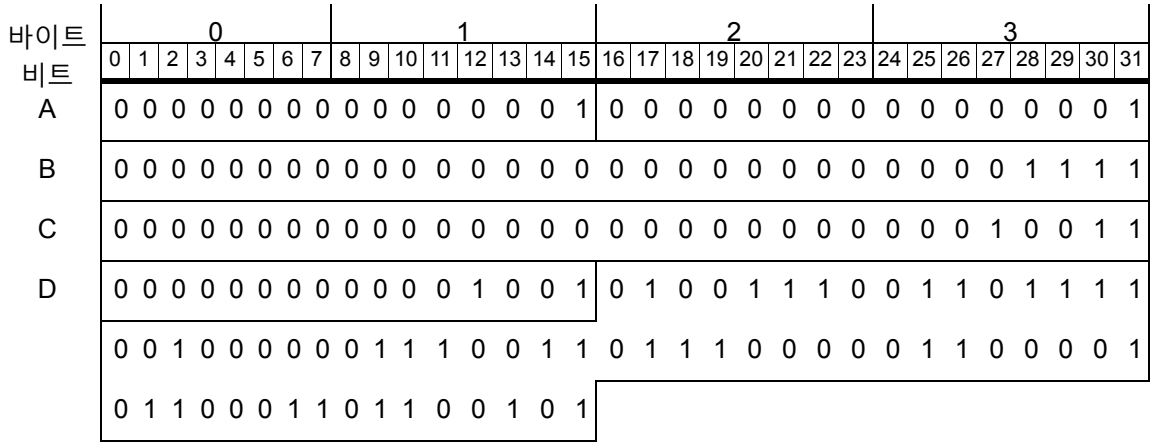
다음 그림에는 기본적인 오류 메시지 형식이 나와 있습니다. 음영으로 표시된 필드가 오류 메시지 관련 필드입니다.

다음 표에는 오류 코드 메시지의 각 필드에 대한 설명이 나와 있습니다.

표 2-4 오류 메시지 필드

필드	데이터 유형	설명
오류 코드	int32	오류를 나타내는 숫자입니다.
오류 텍스트 길이	uint16	오류 텍스트 필드에 포함된 바이트 수입니다.
오류 텍스트	variable	오류 메시지입니다. 최대 65,535바이트입니다.

다음 다이어그램에는 예시 오류 메시지가 나와 있습니다.



위의 예시에는 다음과 같은 정보가 표시되어 있습니다.

문자	설명
A	첫 2바이트는 표준 헤더 값 `1`을 나타냅니다. 두 번째 2바이트에는 전송된 내용이 오류 메시지임을 나타내는 값인 1이 표시됩니다.
B	이 줄은 뒤에 오는 메시지 데이터의 양을 나타냅니다. 이 예시에서는 헤더 뒤에 데이터 15바이트(이진 형식 `1111`)가 옵니다.

문자	설명
C	이 줄에는 오류 코드가 표시됩니다. 이 예시에서 메시지에 포함된 값은 19(10011)입니다. 그러므로 메시지에서는 오류 번호 19가 전송됩니다.
D	이 줄에는 오류 메시지의 바이트 수(1001, 9바이트)가 포함되며 그다음 9바이트에는 오류 메시지 자체가 표시됩니다. 오류 메시지 값은 ASCII 텍스트로 변환되면 "공간 없음"과 같은 의미이며 오류 코드 19와 함께 전송되는 오류 메시지임을 나타냅니다.

이벤트 스트림 요청 메시지 형식

eStreamer 클라이언트는 이벤트 스트림 요청 메시지를 사용하여 스트리밍 세션을 시작합니다. 요청 메시지에는 eStreamer 서비스가 포함해야 하는 데이터를 지정하는 비트 플래그 필드와 시작 시간이 들어 있습니다. 이 데이터는 이벤트의 모든 조합일 수도 있고 침입 이벤트 추가 데이터 및 메타데이터일 수도 있습니다. 이벤트 스트림 요청 메시지는 이벤트 스트림 요청과 확장 요청을 모두 시작할 수 있습니다. 메시지 유형은 2입니다.

호스트 프로파일 정보에 대한 단독 요청을 포함하여 모든 데이터 요청에 대해 이벤트 스트림 요청 메시지를 제출해야 합니다. 이 경우 먼저 이벤트 스트림 요청 메시지를 제출한 다음 호스트 요청 메시지(유형 5)를 제출하여 호스트 데이터를 지정합니다.

다음 그림에는 이벤트 스트림 요청 메시지 형식이 나와 있습니다. 이 메시지는 표준 헤더를 사용합니다. 음영으로 표시된 필드가 요청 메시지 관련 필드이며, 해당 설명은 다음 표에 나와 있습니다.

다음 표에는 이벤트 스트림 요청 메시지의 각 필드에 대한 설명이 나와 있습니다.

표 2-5 이벤트 스트림 요청 메시지 필드

필드	데이터 유형	설명
초기 타임스탬프	uint32	세션의 시작을 정의합니다. 시작 시간은 다음과 같이 설정합니다. • 클라이언트가 eStreamer에 연결하는 시간으로 정의하려면 모든 타임스탬프 비트를 1로 설정합니다. • 사용 가능한 가장 오래된 데이터로 정의하려면 모든 타임스탬프 비트를 0으로 설정합니다. • 지정된 날짜와 시간으로 정의하려면 UNIX 타임스탬프(1970년 1월 1일 이후의 초 단위 시간)를 지정합니다. 이와 관련한 중요 정보는 아래에서 초기 타임스탬프, 2-11페이지의 내용을 참조하십시오.
요청 플래그	bits[32]	이벤트 스트림 요청에서 반환할 메타데이터와 이벤트의 유형 및 버전을 지정합니다. 플래그 정의는 요청 플래그, 2-12페이지의 내용을 참조하십시오. 비트 30을 설정하면 확장 요청이 시작됩니다. 같은 메시지에 이벤트 스트림 요청과 함께 확장 요청을 포함할 수 있습니다.

초기 타임스탬프

참고 클라이언트 애플리케이션은 아래에서 설명하는 것처럼 이벤트 스트림 요청을 제출할 때 Initial Timestamp(초기 타임스탬프) 필드에서 아카이브 타임스탬프를 사용해야 합니다. 이렇게 하면 이벤트를 실수로 제외하는 상황을 방지할 수 있습니다. 디바이스는 "축적 전송(store and forward)" 메커니즘과 전송 지연을 사용해 Management Center로 데이터를 전송합니다. 탐지하는 디바이스가 할당한 생성 타임스탬프를 기준으로 이벤트를 요청하는 경우에는 지연된 이벤트가 누락될 수 있습니다.

세션을 시작할 때의 모범 사례는 이전 세션의 마지막 레코드 아카이브 타임스탬프("서버 타임스탬프"라고도 함)부터 전송을 시작하는 것이 좋습니다. 이것이 기술적 요구 사항은 아니지만, 해당 방식을 사용하는 것이 좋습니다. 상황에 따라서는 생성 타임스탬프를 사용하는 경우 새 스트리밍 세션에서 이벤트를 실수로 제외하게 될 수 있습니다.

스트리밍되는 이벤트에 아카이브 타임스탬프를 포함하려면 요청 플래그 필드에서 비트 23을 설정해야 합니다.

아카이브 타임스탬프는 시간 기반 이벤트에만 있습니다. 비트 23을 설정하여 확장 이벤트 헤더를 요청한 경우, 메타데이터 등 eStreamer가 생성하는 이벤트에서 이 필드의 값은 0입니다.

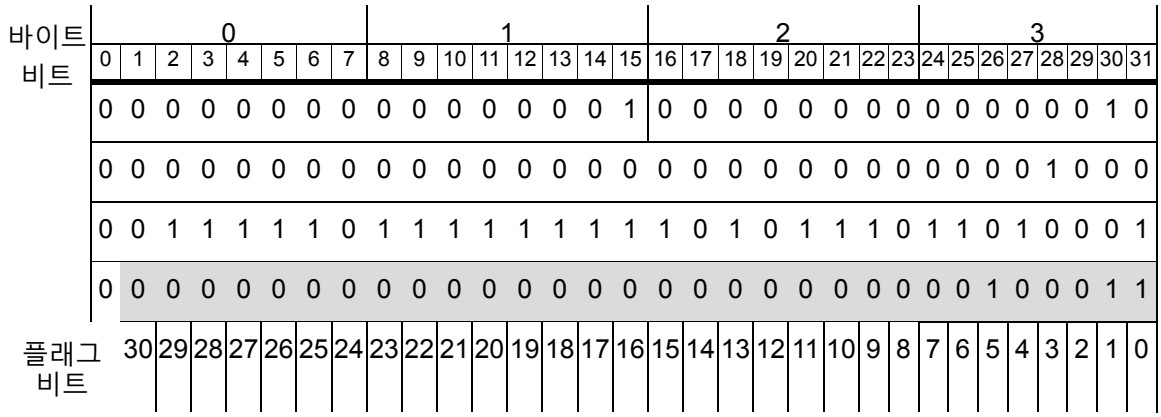
요청 플래그

eStreamer에서 전송하도록 할 이벤트의 유형을 선택하기 위해 이벤트 데이터 요청 플래그 필드에서 비트 0~29를 설정합니다. 확장 요청 모드를 활성화하려면 비트 30을 설정합니다. 비트 30을 설정하는 경우 데이터를 직접 요청하지는 않습니다. 이 비트를 설정하는 경우에는 확장 요청 플래그를 전송해야 합니다. 클라이언트는 이벤트 스트림 요청 메시지를 제출하고 나면 표시되는 서버-클라이언트 메시지 대화 상자를 통해 데이터를 요청합니다. 확장 요청에 대한 자세한 정보는 eStreamer에서 데이터 요청, 2-3페이지의 내용을 참조하십시오.

요청 플래그 필드의 비트 설정 정의는 표 2-6, 2-12페이지의 내용을 참조하십시오. 각 플래그는 이벤트 데이터의 서로 다른 버전을 요청합니다. 예를 들어 Firepower System 4.10 형식이 아닌 4.9 형식으로 데이터를 가져오려면 다른 플래그 비트를 설정합니다. 특정 제품 버전의 데이터를 요청할 때 사용하는 플래그에 대한 자세한 정보는 표 2-7, 2-16페이지의 내용을 참조하십시오.

메타데이터는 개별 메타데이터 레코드가 아닌 버전을 기준으로 요청합니다. 지원되는 각 메타데이터 버전에 대한 자세한 정보는 요청 플래그, 2-12페이지의 내용을 참조하십시오.

아래 다이어그램의 플래그 필드에서 현재 사용되는 비트는 음영으로 표시되어 있습니다.



각 요청 플래그 비트에 대한 자세한 내용은 다음 표를 참조하십시오.

표 2-6 요청 플래그

비트 필드	설명
비트 0	침입 이벤트와 관련된 패킷 데이터 전송을 요청합니다. `1`로 설정하면 침입 이벤트와 함께 패킷 데이터가 전송됩니다. `0`으로 설정하면 패킷 데이터가 전송되지 않습니다.
비트 1	침입, 검색, 상관관계 및 연결 이벤트와 관련된 버전 1 메타데이터 전송을 요청합니다. `1`로 설정하면 이벤트와 함께 버전 1 메타데이터가 전송됩니다. `0`으로 설정하면 버전 1 메타데이터가 전송되지 않습니다. 메타데이터를 사용하면 이벤트의 코딩된 필드 및 숫자 필드를 확인할 수 있습니다. eStreamer에서 클라이언트로 메타데이터를 전송하는 방식과 클라이언트가 메타데이터를 사용할 수 있는 방법에 대한 일반 정보는 메타데이터 이해, 2-41페이지의 내용을 참조하십시오.

표 2-6 요청 플래그 (계속)

비트 필드	설명
비트 2	침입 이벤트 전송을 요청합니다. 비트 2이나 비트 6 중 하나 또는 두 비트가 모두 1로 설정되어 있는데 확장 요청 플래그인 비트 30은 0으로 설정되어 있으면 시스템은 해당 요청을 버전 4.x 클라이언트의 요청으로 해석하며, 레코드 유형 104/105가 전송됩니다. 비트 2이나 비트 6 중 하나 또는 두 비트가 모두 1로 설정되어 있고 비트 30은 1로 설정되어 있는데 이벤트 유형은 지정되어 있지 않으면 시스템은 해당 요청을 버전 5.0~5.1 클라이언트의 요청으로 해석하며, 레코드 유형 207/208이 전송됩니다. 비트 30이 1로 설정된 상태에서 특정 이벤트 유형을 요청하면 비트 2 및 6과 관계없이 침입 이벤트가 전송됩니다. 레코드 유형 요청에 대한 자세한 정보는 확장 요청 제출, 2-4페이지의 내용을 참조하십시오. 비트 2, 비트 6, 비트 30이 모두 0으로 설정되어 있으면 침입 이벤트가 전송되지 않습니다. 비트 6은 비트 2와 동일한 방식으로 사용됩니다. 두 비트 중 하나를 설정하여 침입 이벤트를 요청할 수 있습니다. 이러한 두 비트 중 하나를 0으로 설정해도 다른 비트가 재정의되지는 않습니다. 비트 2를 0으로 설정하고 비트 6을 1로 설정하거나 비트 2를 1로 설정하고 비트 6을 0으로 설정하는 경우 해당 요청은 침입 이벤트 요청으로 해석됩니다.
비트 3	검색 데이터 버전 1(Management Center 3.2) 전송을 요청합니다. 0으로 설정하면 검색 데이터 버전 1이 전송되지 않습니다. 검색 이벤트에 관한 자세한 정보는 검색 및 연결 데이터 구조 이해, 4-1페이지의 내용을 참조하십시오.
비트 4	상관관계 데이터 버전 1(Management Center 3.2) 전송을 요청합니다. 0으로 설정하면 상관관계 데이터 버전 1이 전송되지 않습니다.
비트 5	영향 상관관계 이벤트(침입 영향 알림) 전송을 요청합니다. 1로 설정하면 침입 영향 알림이 전송됩니다. 0으로 설정하면 침입 영향 알림이 전송되지 않습니다. 침입 영향 알림에 대한 자세한 정보는 5.3 이상 버전용 침입 영향 알림 데이터, 3-17페이지의 내용을 참조하십시오.
비트 6	비트 6은 비트 2와 동일한 방식으로 사용됩니다. 비트 2, 2-13페이지의 내용을 참조하십시오.
비트 7	1로 설정하는 경우 검색 데이터 버전 2(Management Center 4.0~4.1) 전송을 요청합니다. 0으로 설정하면 검색 데이터 버전 2가 전송되지 않습니다.
비트 8	1로 설정하는 경우 연결 데이터 버전 1(Management Center 4.0~4.1) 전송을 요청합니다. 0으로 설정하면 연결 데이터 버전 1이 전송되지 않습니다.
비트 9	1로 설정하는 경우 상관관계 데이터 버전 2(Management Center 4.0~4.1.x) 전송을 요청합니다. 0으로 설정하면 상관관계 정책 데이터 버전 2가 전송되지 않습니다.
비트 10	1로 설정하는 경우 검색 데이터 버전 3(Management Center 4.5~4.6.1) 전송을 요청합니다. 0으로 설정하면 검색 데이터 버전 3이 전송되지 않습니다. 레거시 검색 이벤트에 관한 자세한 정보는 레거시 검색 데이터 구조, B-90페이지의 내용을 참조하십시오.
비트 11	이벤트 전송이 비활성화됩니다.
비트 12	1로 설정하는 경우 연결 데이터 버전 3(Management Center 4.5~4.6.1) 전송을 요청합니다. 0으로 설정하면 연결 데이터 버전 3이 전송되지 않습니다.
비트 13	상관관계 데이터 버전 3(Management Center 4.5~4.6.1) 전송을 요청합니다. 0으로 설정하면 상관관계 데이터 버전 3이 전송되지 않습니다.
비트 14	침입, 검색, 상관관계 및 연결 이벤트와 관련된 버전 2 메타데이터 전송을 요청합니다. 1로 설정하면 이벤트와 함께 버전 2 메타데이터가 전송됩니다. 0으로 설정하면 버전 2 메타데이터가 전송되지 않습니다. eStreamer에서 클라이언트로 메타데이터를 전송하는 방식과 클라이언트가 메타데이터를 사용할 수 있는 방법에 대한 일반 정보는 메타데이터 이해, 2-41페이지의 내용을 참조하십시오.

표 2-6 요청 플래그 (계속)

비트 필드	설명
비트 15	침입, 상관관계, 검색 및 연결 이벤트와 관련된 버전 3 메타데이터 전송을 요청합니다. 1로 설정하면 이벤트와 함께 버전 3 메타데이터가 전송됩니다. 0으로 설정하면 버전 3 메타데이터가 전송되지 않습니다. eStreamer에서 클라이언트로 메타데이터를 전송하는 방식과 클라이언트가 메타데이터를 사용할 수 있는 방법에 대한 일반 정보는 메타데이터 이해, 2-41페이지의 내용을 참조하십시오.
비트 16	사용되지 않음
비트 17	검색 데이터 버전 4(Management Center 4.7~4.8.x) 전송을 요청합니다. 0으로 설정하면 검색 데이터 버전 4가 전송되지 않습니다.
비트 18	1로 설정하는 경우 연결 데이터 버전 4(Management Center 4.7~4.9.0.x) 전송을 요청합니다. 0으로 설정하면 연결 데이터 버전 4가 전송되지 않습니다. 자세한 정보는 연결 청크 메시지, 4-55페이지의 내용을 참조하십시오.
비트 19	상관관계 데이터 버전 4(Management Center 4.7) 전송을 요청합니다. 0으로 설정하면 상관관계 데이터 버전 4가 전송되지 않습니다. Management Center 4.7 형식으로 전송되는 상관관계 이벤트에 대한 자세한 정보는 레거시 상관관계 이벤트 데이터 구조, B-258페이지의 내용을 참조하십시오.
비트 20	침입, 검색, 사용자 활동, 상관관계 및 연결 이벤트와 관련된 버전 4 메타데이터 전송을 요청합니다. 1로 설정하면 이벤트와 함께 버전 4 메타데이터가 전송됩니다. 0으로 설정하면 버전 4 메타데이터가 전송되지 않습니다. 버전 4 메타데이터에는 다음이 포함됩니다. • 상관관계(컴플라이언스) 규칙 정보 • 상관관계(컴플라이언스) 정책 정보 • 핑거프린트 레코드 • 클라이언트 애플리케이션 레코드 • 클라이언트 애플리케이션 유형 레코드 • 취약점 레코드 • 호스트 임계성 레코드 • 네트워크 프로토콜 레코드 • 호스트 속성 레코드 • 스캔 유형 레코드 • 사용자 레코드 • 서비스 탐지 디바이스(버전 2) 레코드 • 이벤트 분류(버전 2) 레코드 • 우선순위 레코드 • 규칙 정보(버전 2) • 악성코드 정보 비트 22와 함께 비트 20을 요청하면 사용자 메타데이터도 전송됩니다. eStreamer에서 클라이언트로 메타데이터를 전송하는 방식과 클라이언트가 메타데이터를 사용할 수 있는 방법에 대한 일반 정보는 메타데이터 이해, 2-41페이지의 내용을 참조하십시오.

표 2-6 요청 플래그 (계속)

비트 필드	설명
비트 21	버전 1 사용자 이벤트 전송을 요청합니다. 사용자 이벤트에 대한 자세한 정보는 사용자 레코드, 4-20페이지의 내용을 참조하십시오.
비트 22	상관관계 데이터 버전 5(Management Center 4.8.0.2~4.9.1) 전송을 요청합니다. 0으로 설정하면 상관관계 데이터 버전 5가 전송되지 않습니다. 비트 22와 함께 비트 20을 요청하면 사용자 메타데이터도 전송됩니다. 레거시 상관관계(컴플라이언스) 이벤트에 관한 자세한 정보는 레거시 상관관계 이벤트 데이터 구조, B-258페이지의 내용을 참조하십시오.
비트 23	확장 이벤트 헤더를 요청합니다. 1로 설정하면 eStreamer 서버에서 처리하도록 이벤트가 아카이브되었을 때 적용된 타임스탬프 및 나중에 사용하도록 예약된 4바이트를 포함하여 이벤트가 전송됩니다. 이 필드를 0으로 설정하면 레코드 유형과 레코드 길이만 포함된 표준 이벤트 헤더와 함께 이벤트가 전송됩니다. 이벤트 메시지 헤더에 대한 자세한 정보는 eStreamer 메시지 헤더, 2-7페이지의 내용을 참조하십시오.
비트 24	검색 데이터 버전 5(Management Center 4.9.0.x) 전송을 요청합니다. 0으로 설정하면 검색 데이터 버전 5가 전송되지 않습니다. 검색 이벤트에 관한 자세한 정보는 검색 및 연결 데이터 구조 이해, 4-1페이지의 내용을 참조하십시오.
비트 25	검색 데이터 버전 6(Management Center 4.9.1 이상) 전송을 요청합니다. 0으로 설정하면 검색 데이터 버전 6이 전송되지 않습니다. 검색 이벤트에 관한 자세한 정보는 검색 및 연결 데이터 구조 이해, 4-1페이지의 내용을 참조하십시오.
비트 26	1로 설정하는 경우 연결 데이터 버전 5(Management Center 4.9.1~4.10.x) 전송을 요청합니다. 0으로 설정하면 연결 데이터 버전 5가 전송되지 않습니다. 자세한 정보는 연결 청크 메시지, 4-55페이지의 내용을 참조하십시오.
비트 27	추가 데이터 레코드에서 침입 이벤트와 관련된 이벤트 추가 데이터를 요청합니다. 이벤트 데이터에 대한 자세한 정보는 표 3-11 침입 이벤트 추가 데이터 데이터 블록 필드, 3-28페이지의 내용을 참조하십시오.
비트 28	검색 데이터 버전 7(Management Center 4.10.0 이상) 전송을 요청합니다. 0으로 설정하면 검색 데이터 버전 7이 전송되지 않습니다. 검색 이벤트에 관한 자세한 정보는 검색 및 연결 데이터 구조 이해, 4-1페이지의 내용을 참조하십시오.
비트 29	상관관계 데이터 버전 6(Management Center 4.10~4.10.x) 전송을 요청합니다. 0으로 설정하면 상관관계 정책 데이터 버전 6이 전송되지 않습니다. 비트 29와 함께 비트 20을 요청하면 사용자 메타데이터도 전송됩니다. 상관관계 이벤트에 대한 자세한 내용은 제품의 이전 버전을 참조하십시오.
비트 30	eStreamer에 대한 확장 요청을 나타냅니다. 이 비트를 설정하는 경우에는 확장 요청 플래그를 전송해야 합니다. 확장 요청에 대한 자세한 정보는 확장 요청 제출, 2-4페이지의 내용을 참조하십시오.

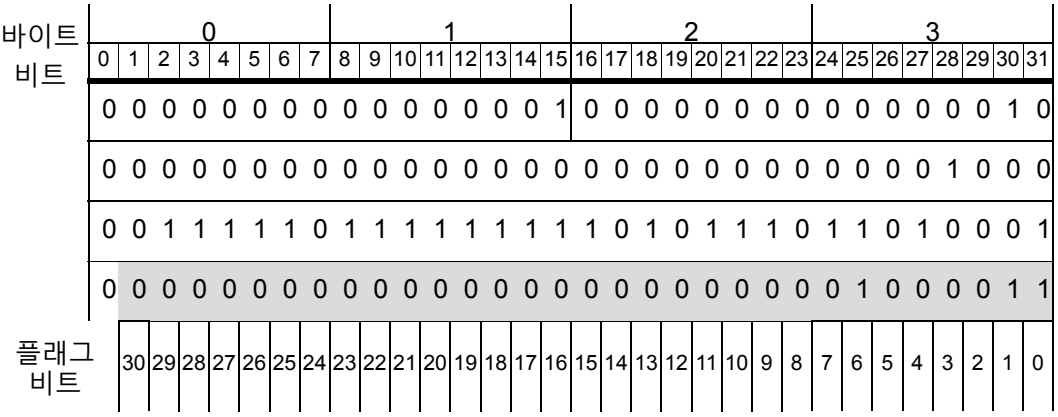
특정 버전의 데이터를 요청하는 데 사용할 플래그를 쉽게 결정하려면 아래 표를 참조하십시오. 버전 5.0 이상의 경우 확장 요청 제출, 2-4페이지에서 비트 30 사용에 대한 자세한 내용을 확인할 수 있습니다.

표 2-7 제품 버전별 이벤트 요청 플래그

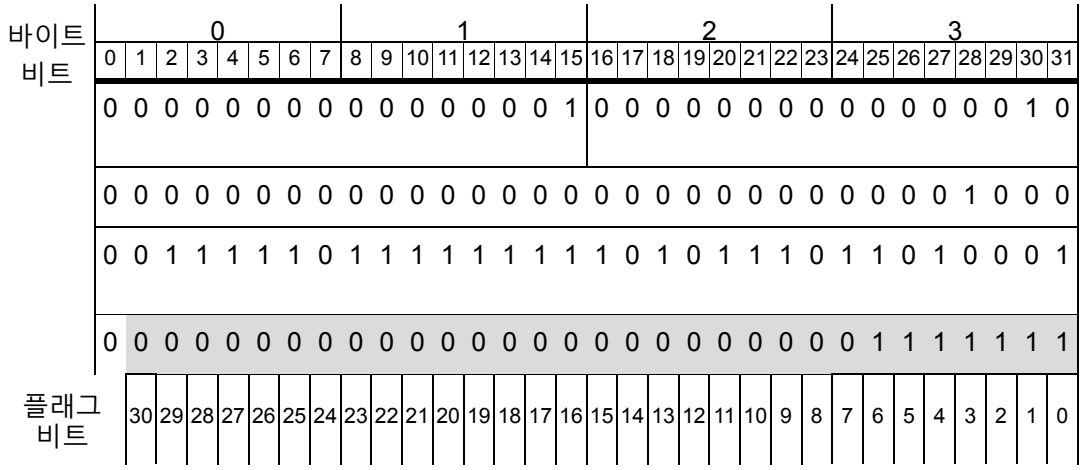
요청하는 데이터 유형	4.9.0.x	4.9.1.x	4.10.x	5.0 이상	5.1	5.1.1 이상
패킷 데이터	비트 0	비트 0	비트 0	비트 0	비트 0	비트 0
침입 이벤트	비트 2	비트 2	비트 2	비트 2	비트 2	비트 30
메타데이터	비트 20	비트 20	비트 20	비트 20	비트 20	비트 20
검색 이벤트	비트 24	비트 25	비트 28	비트 30	비트 30	비트 30
상관관계 이벤트	비트 22	비트 22	비트 29	비트 30	비트 30	비트 30
이벤트 추가 데이터	—	—	비트 27	비트 27	비트 27	비트 27
영향 이벤트 알림	비트 5	비트 5	비트 5	비트 5	비트 5	비트 5
연결 데이터	비트 18	비트 26	비트 26	비트 30	비트 30	비트 30
사용자 이벤트	비트 21	비트 21	비트 21	비트 30	비트 30	비트 30
악성코드 이벤트	—	—	—	—	—	비트 30
파일 이벤트	—	—	—	—	—	비트 30

주의 5.x 이전 버전에서는 모든 이벤트 유형에서 참조 클라이언트가 `detection engine ID`(탐지 엔진 ID) 필드의 레이블을 `sensor ID`(센서 ID)로 지정합니다.

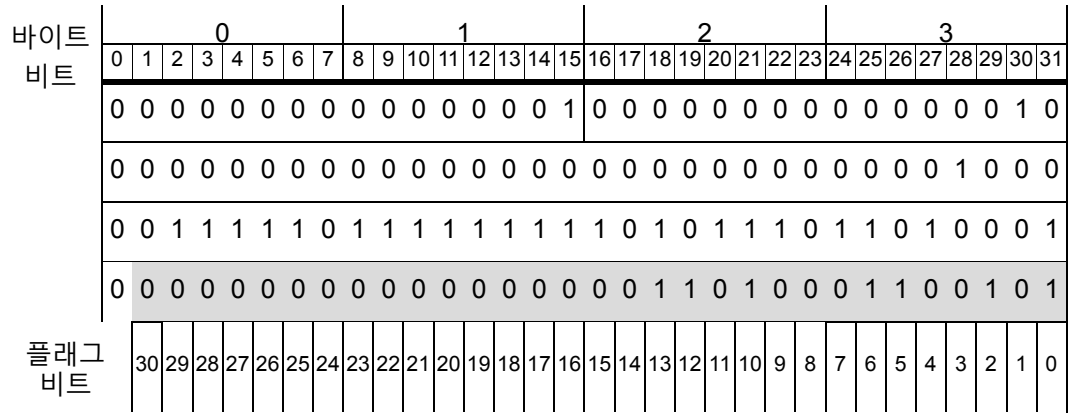
다음 예시에서는 버전 1 메타데이터 및 패킷 플래그를 모두 포함하는 유형 7 침입 이벤트(Firepower System 3.2 이상 버전과 호환됨)를 요청합니다.



침입 이벤트, 패킷, 메타데이터, 영향 알림, 정책 위반 이벤트, 버전 2.0 이벤트를 포함하여 Firepower System 3.2와 호환되는 데이터만 요청하려면 다음과 같은 메시지 형식을 사용합니다.



Management Center 4.6.1 이상 형식의 패킷 및 버전 3 메타데이터를 포함하여 유형 7 침입 영향 알림, 상관관계 이벤트, 검색 이벤트, 연결 이벤트 및 침입 이벤트를 요청하려면 다음 메시지 형식을 사용합니다.



이벤트 데이터 메시지 형식

eStreamer 서비스는 이벤트 요청을 받으면 이벤트 데이터 및 관련 메타데이터를 클라이언트로 전송합니다. 이벤트 데이터 메시지의 메시지 유형은 3입니다. 각 메시지에는 이벤트 데이터 또는 메타데이터와 함께 단일 데이터 레코드가 포함됩니다.

유형 3 메시지는 이벤트 데이터와 메타데이터만 전달합니다. eStreamer는 유형 6(단일 호스트) 및 유형 7(다중 호스트) 메시지에서 호스트 정보를 전송합니다. 호스트 메시지 형식에 대한 자세한 정보는 호스트 데이터 및 여러 호스트 데이터 메시지 형식, 2-30페이지의 내용을 참조하십시오.

이벤트 데이터 메시지 구성 이해

eStreamer에서 보내는 이벤트 데이터 및 메타데이터 메시지에는 다음 섹션이 포함됩니다.

- eStreamer 메시지 헤더 - eStreamer 메시지 헤더, 2-7페이지에 정의되어 있는 표준 메시지 헤더입니다.
- 이벤트별 하위 헤더 - 이벤트 유형별로 달라지는 필드 집합이며, 추가 이벤트 세부사항을 설명하고 뒤에 오는 페이로드 데이터 구조를 결정하는 코드를 포함합니다.
- 데이터 레코드 - 길이가 고정된 필드와 데이터 블록입니다.

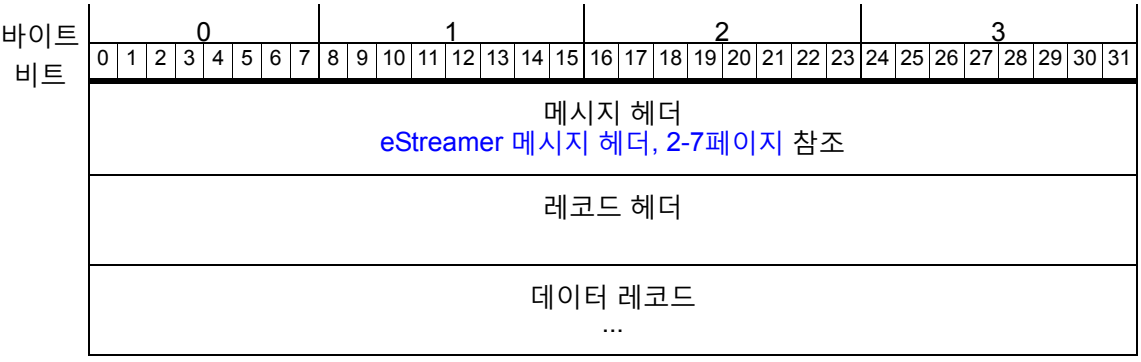
참고 클라이언트는 필드 길이를 기준으로 하여 모든 메시지의 압축을 풀어야 합니다.

이벤트 유형별 이벤트 메시지 형식은 다음 장을 참조하십시오.

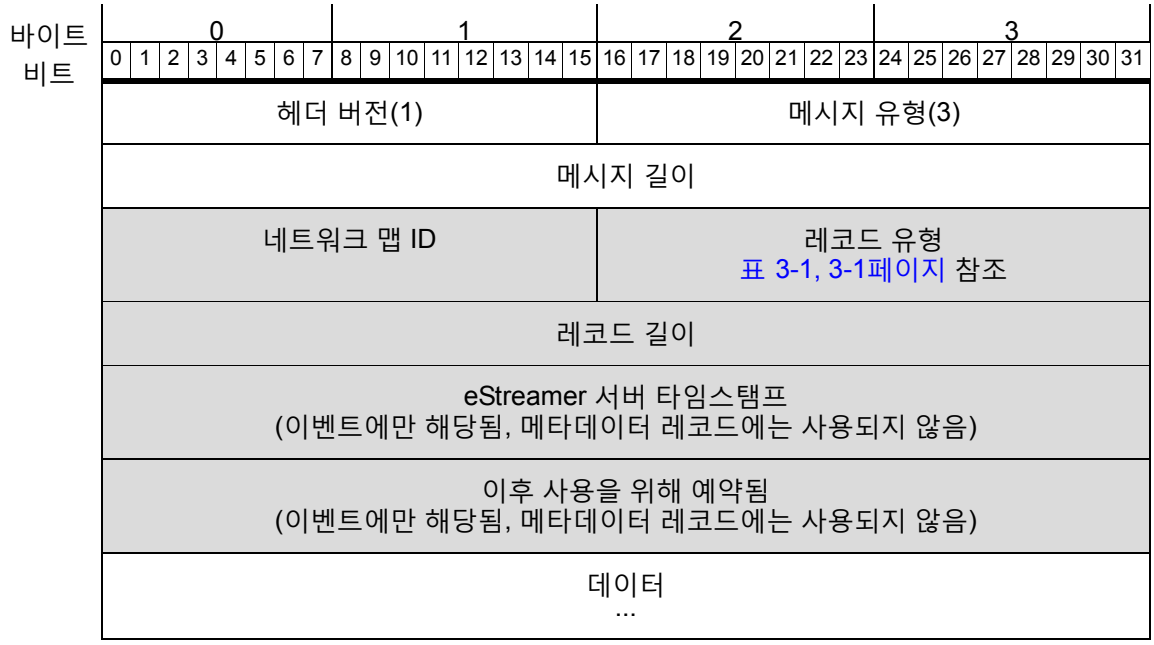
- 침입 이벤트 및 메타데이터 메시지 형식, 2-18페이지 - 침입 이벤트 데이터 레코드 및 모든 메타데이터 레코드용 형식입니다. 이러한 메시지는 고정 길이 필드를 포함합니다.
- 검색 이벤트 메시지 형식, 2-20페이지 - 검색 이벤트 또는 사용자 이벤트 데이터가 포함된 메시지용 형식입니다. 검색 메시지에는 침입 이벤트 메시지와 비슷한 표준 eStreamer 메시지 헤더 및 레코드 헤더와 함께, 이벤트 유형 및 하위 유형 필드가 포함된 고유한 검색 이벤트 헤더도 포함됩니다. 검색 이벤트 메시지의 데이터 레코드는 가변 길이 필드와 여러 캡슐화된 블록 계층을 포함할 수 있는 계열 1 블록으로 패키지됩니다.
- 연결 이벤트 메시지 형식, 2-21페이지 - 연결 통계가 포함된 메시지용 형식입니다. 이러한 메시지의 일반적인 구조는 검색 이벤트 메시지와 동일합니다. 하지만 해당 데이터 블록 유형은 연결 통계별로 다릅니다.
- 상관관계 이벤트 메시지 형식, 2-22페이지 - 상관관계(컴플라이언스) 이벤트 데이터가 포함된 메시지용 형식입니다. 이러한 메시지의 헤더는 침입 이벤트 메시지와 동일하지만 데이터 블록은 계열 1 블록입니다.
- 이벤트 추가 데이터 메시지 형식, 2-23페이지 - 침입 관련 레코드 유형을 제공하며 가변 길이 필드와 여러 중첩 데이터 블록 계층(예: 침입 이벤트 추가 데이터)을 포함하는 메시지 계열용 형식입니다. 이 메시지 계열의 구조에 대한 일반 정보는 이벤트 추가 데이터 메시지 형식, 2-23페이지의 내용을 참조하십시오. 계열 1 블록과 비슷하지만 별도로 번호가 매겨지는 이 블록 계열의 구조에 대한 자세한 정보는 데이터 블록 헤더, 2-25페이지의 내용을 참조하십시오.

침입 이벤트 및 메타데이터 메시지 형식

아래 그림에는 침입 이벤트 및 메타데이터 메시지의 일반적인 구조가 나와 있습니다.



아래 그림에는 침입 이벤트 및 메타데이터 메시지 형식의 레코드 헤더 부분에 대한 세부사항이 나와 있습니다. 레코드 헤더 필드는 음영으로 표시되어 있습니다. 그림 아래의 표에 필드의 정의가 나와 있습니다.



다음 표에는 침입 이벤트 및 메타데이터 메시지의 헤더에 있는 각 필드에 대한 설명이 나와 있습니다.

표 2-8 침입 이벤트 및 메타데이터 레코드 헤더 필드

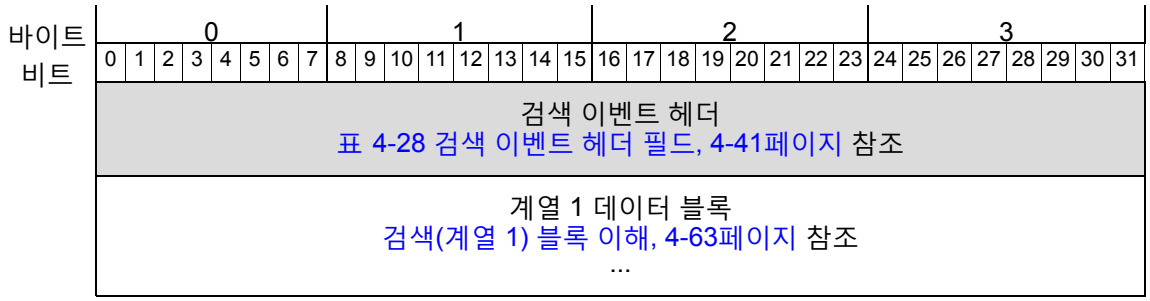
필드	데이터 유형	설명
네트워크 맵 ID	uint16	이 필드의 첫 번째 비트는 헤더가 아카이브 타임스탬프를 포함하는 확장 헤더임을 나타내는 플래그입니다. 나머지 15비트는 이벤트가 탐지된 도메인의 네트워크 맵 ID를 포함하는 선택적 필드입니다. 이 필드는 사용되지 않는 경우 비어 있습니다. 네트워크 맵 ID는 메타데이터에서 제공되는 도메인에 매핑됩니다.
레코드 유형	uint16	데이터 레코드 콘텐츠 유형을 식별합니다. 레코드 유형의 목록은 표 3-1 침입 이벤트 및 일반 메타데이터 레코드 유형, 3-1페이지의 내용을 참조하십시오.
레코드 길이	uint32	레코드 헤더 뒤의 메시지 콘텐츠 길이입니다. 레코드 헤더의 8바이트 또는 16바이트는 포함되지 않습니다. (레코드 길이 + 레코드 헤더 길이 = 메시지 길이)
eStreamer 서버 타임스탬프	uint32	eStreamer 서버에서 이벤트를 아카이브할 때 적용된 타임스탬프를 나타냅니다. 아카이브 타임스탬프라고도 합니다. 요청 메시지 플래그에 비트 23이 설정되어 있어야 이 필드가 제공됩니다.
이후 사용을 위해 예약됨	uint32	이후 사용을 위해 예약됩니다. 요청 메시지 플래그에 비트 23이 설정되어 있어야 이 필드가 제공됩니다.

검색 이벤트 메시지 형식

아래 그림에는 검색 이벤트 메시지의 구조가 나와 있습니다. 표준 eStreamer 메시지 헤더와 이벤트 레코드 헤더 뒤에는 검색 및 사용자 이벤트 메시지에서만 사용되는 검색 이벤트 헤더가 옵니다. 메시지의 검색 이벤트 헤더 섹션은 검색 이벤트 유형 및 하위 유형 필드를 포함하며, 이러한 필드가 결합되어 그 뒤에 오는 데이터 블록의 키를 생성합니다. 현재 검색 이벤트 유형 및 하위 유형은 표 4-29 유형 및 하위 유형별 검색 및 연결 이벤트, 4-42페이지의 내용을 참조하십시오.

검색 이벤트 메시지 헤더

다음 그림에서 음영으로 표시된 섹션에는 검색 이벤트 데이터 메시지 형식의 레코드 헤더 필드와 그 뒤의 이벤트 헤더 위치가 나와 있습니다. 다음 표에는 검색 이벤트 메시지 헤더의 필드 정의가 나와 있습니다.



다음 표에는 검색 이벤트 메시지의 레코드 헤더 및 이벤트 헤더 내 필드에 대한 설명이 나와 있습니다.

표 2-9 검색 이벤트 메시지 헤더 필드

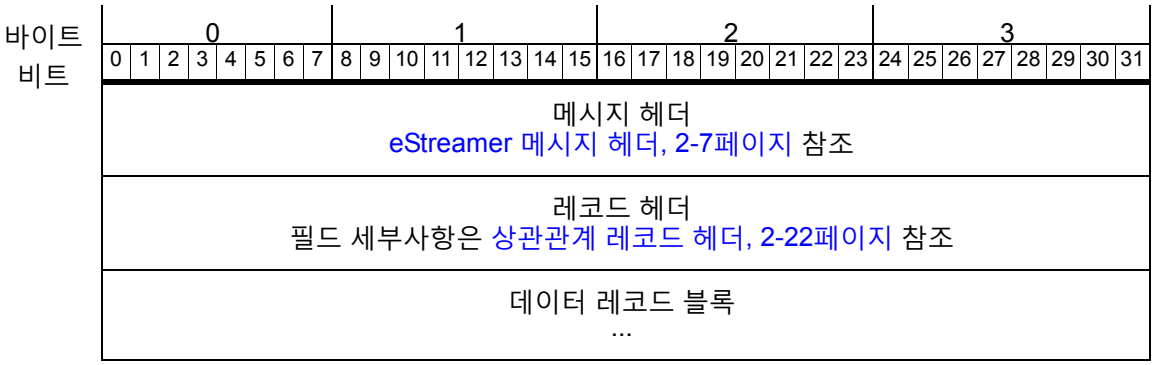
필드	데이터 유형	설명
네트워크 맵 ID	uint16	이 필드의 첫 번째 비트는 헤더가 아카이브 타임스탬프를 포함하는 확장 헤더임을 나타내는 플래그입니다. 나머지 15비트는 이벤트가 탐지된 도메인의 네트워크 맵 ID를 포함하는 선택적 필드입니다. 이 필드는 사용되지 않는 경우 비어 있습니다. 네트워크 맵 ID는 메타데이터에서 제공되는 도메인에 매핑됩니다.
레코드 유형	uint16	데이터 레코드 콘텐츠 유형을 식별합니다. 레코드 유형의 목록은 표 4-1 검색 및 연결 이벤트 레코드 유형, 4-2페이지의 내용을 참조하십시오.
레코드 길이	uint32	레코드 헤더 뒤의 메시지 콘텐츠 길이입니다. 레코드 헤더의 8바이트 또는 16바이트는 포함되지 않습니다. (레코드 길이 + 레코드 헤더 길이 = 메시지 길이)
eStreamer 서버 타임스탬프	uint32	eStreamer 서버에서 이벤트를 아카이브할 때 적용된 타임스탬프를 나타냅니다. 아카이브 타임스탬프라고도 합니다. 이벤트 스트림 요청의 요청 플래그 필드에 비트 23이 설정되어 있어야 이 필드가 제공됩니다.
이후 사용을 위해 예약됨	uint32	이후 사용을 위해 예약됩니다. 요청 메시지 플래그에 비트 23이 설정되어 있어야 이 필드가 제공됩니다.
검색 이벤트 헤더	다양하게 제공	함께 결합되어 뒤에 오는 데이터 구조에 대한 고유 키를 생성하는 여러 필드(이벤트 유형 및 하위 유형 포함)를 포함합니다. 검색 이벤트 헤더의 필드 정의는 검색 이벤트 헤더(5.2 이상), 4-40페이지의 내용을 참조하십시오.

연결 이벤트 메시지 형식

연결 통계가 포함된 메시지의 구조는 검색 이벤트 메시지와 동일합니다. 일반적인 메시지 형식 정보는 검색 이벤트 메시지 형식, 2-20페이지의 내용을 참조하십시오. 연결 이벤트 메시지는 통합하는 데이터 블록 유형 측면에서 고유합니다.

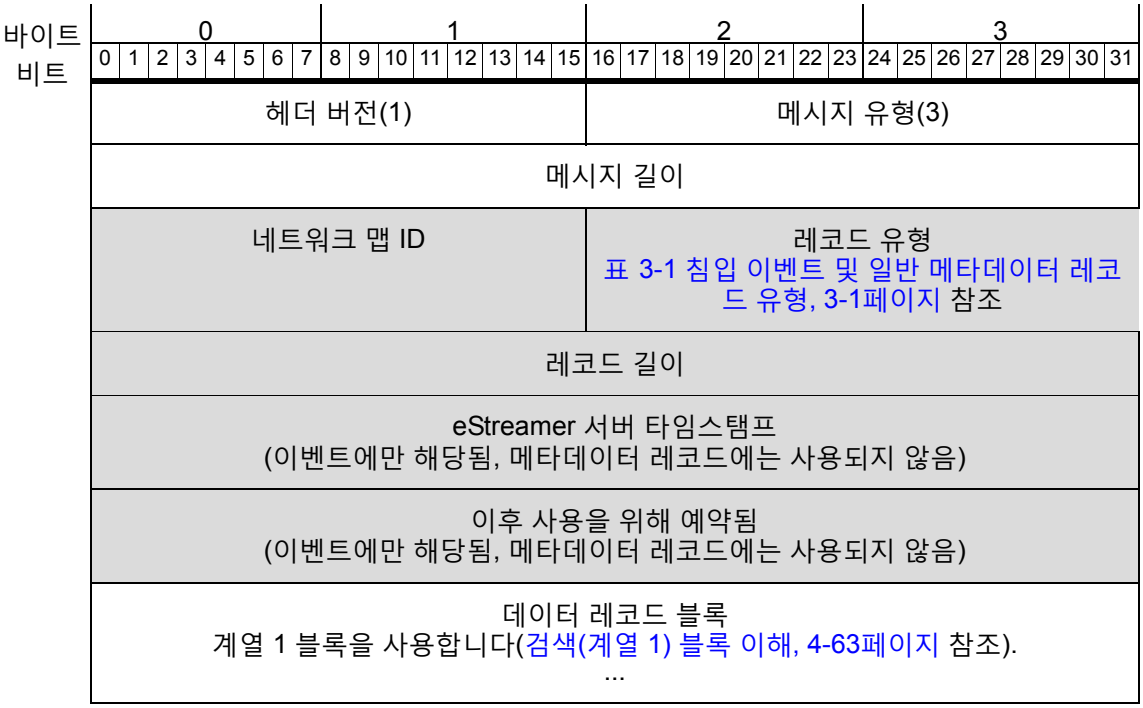
상관관계 이벤트 메시지 형식

아래 그림에는 상관관계(컴플라이언스) 이벤트 메시지의 일반적인 구조가 나와 있습니다. 표준 eStreamer 메시지 헤더와 레코드 헤더 바로 뒤에는 메시지 내 데이터 레코드 섹션의 데이터 블록이 옵니다. 상관관계 메시지는 계열 1 데이터 블록을 사용합니다.



상관관계 레코드 헤더

다음 그림에서 음영으로 표시된 섹션에는 상관관계 이벤트 메시지의 레코드 헤더 필드가 나와 있습니다. 상관관계 메시지는 계열 1 데이터 블록을 사용하지만 검색 이벤트 메시지에 표시되는 검색 헤더는 포함하지 않습니다. 이러한 메시지의 헤더 필드는 침입 이벤트 메시지와 비슷합니다. 다음 그림 아래의 표에는 상관관계 이벤트의 레코드 헤더 필드 정의가 나와 있습니다.



다음 표에는 상관관계 이벤트 메시지의 레코드 헤더에 있는 각 필드에 대한 설명이 나와 있습니다.

표 2-10 상관관계 이벤트 메시지 레코드 헤더 필드

필드	데이터 유형	설명
네트워크 맵 ID	uint16	이 필드의 첫 번째 비트는 헤더가 아카이브 타임스탬프를 포함하는 확장 헤더임을 나타내는 플래그입니다. 나머지 15비트는 이벤트가 탐지된 도메인의 네트워크 맵 ID를 포함하는 선택적 필드입니다. 이 필드는 사용되지 않는 경우 비어 있습니다. 네트워크 맵 ID는 메타데이터에서 제공되는 도메인에 매핑됩니다.
레코드 유형	uint16	데이터 레코드 콘텐츠 유형을 식별합니다. 침입, 상관관계 및 메타데이터 레코드 유형의 목록은 표 3-1, 3-1페이지의 내용을 참조하십시오.
레코드 길이	uint32	레코드 헤더 뒤의 메시지 콘텐츠 길이입니다. 레코드 헤더의 8바이트 또는 16바이트는 포함되지 않습니다. (레코드 길이 + 레코드 헤더 길이 = 메시지 길이)
eStreamer 서버 타임스탬프	uint32	eStreamer 서버에서 이벤트를 아카이브할 때 적용된 타임스탬프를 나타냅니다. 아카이브 타임스탬프라고도 합니다. 요청 메시지 플래그에 비트 23이 설정되어 있어야 이 필드가 제공됩니다. 호스트 프로파일, 메타데이터 등 Management Center에서 생성하는 데이터의 경우 필드의 값은 0입니다.
이후 사용을 위해 예약됨	uint32	이후 사용을 위해 예약됩니다. 요청 메시지 플래그에 비트 23이 설정되어 있어야 이 필드가 제공됩니다.

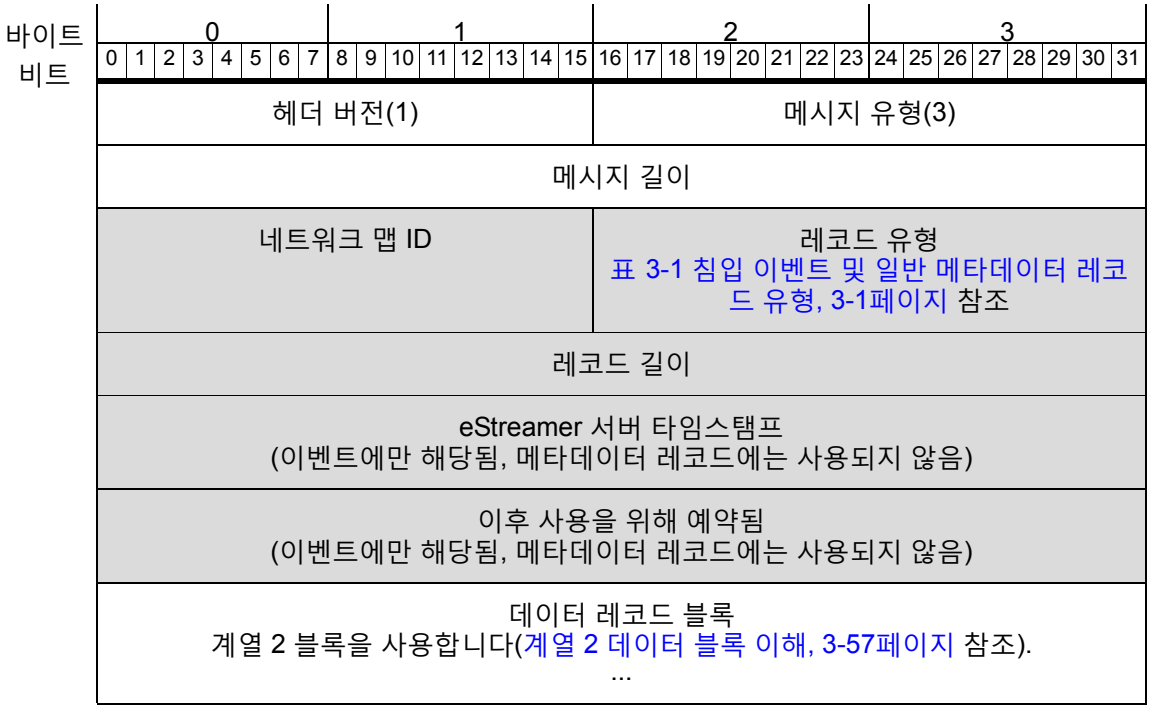
이벤트 추가 데이터 메시지 형식

아래 그림에는 이벤트 추가 데이터 메시지의 구조가 나와 있습니다. 이 메시지 그룹의 예시로는 침입 이벤트 추가 데이터 메시지가 포함됩니다.

이벤트 추가 데이터 메시지의 형식은 상관관계 이벤트 메시지와 같으며, 레코드 헤더 바로 뒤에 데이터 블록이 옵니다. 하지만 상관관계 메시지와는 달리 이벤트 추가 데이터 메시지는 계열 1 데이터 블록이 아닌 별도의 번호 매기기 순서를 사용하는 계열 2 데이터 블록을 사용합니다. 계열 2 블록 유형에 대한 자세한 정보는 계열 2 데이터 블록 이해, 3-57페이지의 내용을 참조하십시오.

이벤트 추가 데이터 메시지 레코드 헤더

다음 그림에서 음영으로 표시된 섹션에는 이벤트 추가 데이터 메시지의 레코드 헤더 필드가 나와 있습니다. 그림 아래의 표에는 이벤트 추가 데이터 메시지의 레코드 헤더 필드 정의가 나와 있습니다.



다음 표에는 이벤트 추가 데이터 메시지의 레코드 헤더에 있는 각 필드에 대한 설명이 나와 있습니다.

표 2-11 이벤트 추가 데이터 메시지 레코드 헤더 필드

필드	데이터 유형	설명
네트워크 맵 ID	uint16	이 필드의 첫 번째 비트는 헤더가 아카이브 타임스탬프를 포함하는 확장 헤더임을 나타내는 플래그입니다. 나머지 15비트는 이벤트가 탐지된 도메인의 네트워크 맵 ID를 포함하는 선택적 필드입니다. 이 필드는 사용되지 않는 경우 비어 있습니다. 네트워크 맵 ID는 메타데이터에서 제공되는 도메인에 매핑됩니다.
레코드 유형	uint16	데이터 레코드 콘텐츠 유형을 식별합니다. 이벤트 추가 데이터 레코드 유형의 목록은 표 3-1 침입 이벤트 및 일반 메타데이터 레코드 유형, 3-1페이지의 내용을 참조하십시오.
레코드 길이	uint32	레코드 헤더 뒤의 메시지 콘텐츠 길이입니다. 레코드 헤더의 8바이트 또는 16바이트는 포함되지 않습니다. (레코드 길이 + 레코드 헤더 길이 = 메시지 길이)

표 2-11 이벤트 추가 데이터 메시지 레코드 헤더 필드 (계속)

필드	데이터 유형	설명
eStreamer 서버 타임스탬프	uint32	eStreamer 서버에서 이벤트를 아카이브할 때 적용된 타임스탬프를 나타냅니다. 아카이브 타임스탬프라고도 합니다. 요청 메시지 플래그에 비트 23이 설정되어 있어야 이 필드가 제공됩니다. Management Center에서 생성되는 이벤트의 경우에는 이 필드가 없습니다.
이후 사용을 위해 예약됨	uint32	이후 사용을 위해 예약됩니다. 요청 메시지 플래그에 비트 23이 설정되어 있어야 이 필드가 제공됩니다. Management Center에서 생성되는 이벤트의 경우에는 이 필드가 없습니다.

데이터 블록 헤더

계열 1 블록과 계열 2 블록은 구조는 비슷하지만 번호 매기기 방식은 각각 고유합니다. 이러한 블록은 검색, 상관관계, 연결 또는 이벤트 추가 데이터 메시지의 데이터 부분 어디에서나 나타날 수 있습니다. 이러한 블록은 여러 중첩 레벨에서 다른 블록을 캡슐화합니다.

계열 1과 계열 2 둘 다의 데이터 블록은 아래 그림에 나와 있는 헤더 구조로 시작됩니다. 다음 표에는 헤더 필드에 대한 정보가 나와 있습니다. 헤더 바로 뒤에는 데이터 블록 유형과 관련된 데이터 구조가 옵니다.

표 2-12

필드	데이터 유형	설명
데이터 블록 유형	uint32	계열 1 블록 유형의 경우 검색(계열 1) 블록 이해, 4-63페이지의 내용을 참조하십시오. 계열 2 블록 유형의 경우 표 3-26 계열 2 블록 유형, 3-57페이지의 내용을 참조하십시오.
데이터 블록 길이	uint32	데이터 블록의 길이입니다. 데이터 바이트 수에 2개 데이터 블록 헤더 필드의 8바이트를 더한 길이입니다.

호스트 요청 메시지 형식

호스트 프로파일을 수신하려면 호스트 요청 메시지를 제출합니다. 단일 호스트 또는 IP 주소 범위로 정의된 여러 호스트에 대한 데이터를 요청할 수 있습니다.

호스트 프로파일 정보 요청을 비롯한 모든 데이터 요청의 경우 이벤트 스트림 요청 메시지를 제출하여 먼저 세션을 초기화해야 합니다. 호스트 데이터만 스트리밍하도록 설정하려는 경우 초기 이벤트 스트림 요청 메시지에서 다음의 요청 플래그 설정을 사용할 수 있습니다.

- 적절한 메타데이터 버전용으로 비트 설정(호스트 데이터 스트리밍 시 유용할 수 있음)
- 요청 플래그 설정 안 함
- 비트 11 설정(레거시 버전 eStreamer 사용 시 기본 이벤트 스트리밍을 표시하지 않으려는 경우)

초기 메시지를 제출한 후에는 호스트 요청 메시지(유형 5)를 사용하여 호스트를 지정합니다.

참고 기본 이벤트 스트리밍을 사용하는 레거시 eStreamer 버전의 경우 호스트 프로파일 데이터만 스트리밍하려면 기본 이벤트 메시지를 표시하지 않아야 합니다. 먼저 요청 플래그 필드의 비트 11이 1로 설정된 이벤트 스트림 요청 메시지를 서버에 보낸 다음 호스트 요청 메시지를 보냅니다.

아래 그림에는 호스트 요청 메시지의 형식이 나와 있습니다. 음영으로 표시된 필드가 호스트 요청 메시지 형식 관련 필드이며, 다음 표에 해당 정의가 나와 있습니다. 그 앞의 3개 필드는 표준 메시지 헤더입니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
헤더 버전(1)																	메시지 유형(5)															
메시지 길이																																
데이터 유형																																
플래그																																
시작 IP 주소																																
시작 IP 주소(계속)																																
시작 IP 주소(계속)																																
시작 IP 주소(계속)																																
종료 IP 주소																																
종료 IP 주소(계속)																																
종료 IP 주소(계속)																																
종료 IP 주소(계속)																																

다음 표에는 메시지 필드에 대한 설명이 나와 있습니다.

표 2-13 호스트 요청 메시지 필드

필드	데이터 유형	설명
데이터 유형	uint32	다음 코드를 사용하여 단일 호스트 또는 여러 호스트에 대한 데이터를 요청합니다. • 0 - 버전 3.5~4.6(단일 호스트) • 1 - 버전 3.5~4.6(여러 호스트, 블록 34 사용) • 2 - 버전 4.7~4.8(단일 호스트, 블록 47 사용) • 3 - 버전 4.7~4.8(여러 호스트, 블록 47 사용) • 4 - 버전 4.9~4.10(단일 호스트, 블록 92 사용) • 5 - 버전 4.9~4.10(여러 호스트, 블록 92 사용) • 6 - 버전 5.0.x 데이터(단일 호스트, 블록 111 사용 - 5.0~5.0.2 버전용 전체 호스트 프로파일 데이터 블록, B-274페이지 참조) • 7 - 버전 5.0.x 데이터(여러 호스트, 블록 111 사용 - 5.0~5.0.2 버전용 전체 호스트 프로파일 데이터 블록, B-274페이지 참조) • 8 - 버전 5.1.x 데이터(여러 호스트, 블록 111 사용 - 5.1.1 버전용 전체 호스트 프로파일 데이터 블록, B-283페이지 참조) • 9 - 버전 5.1.x 데이터(여러 호스트, 블록 111 사용 - 5.1.1 버전용 전체 호스트 프로파일 데이터 블록, B-283페이지 참조) • 10 - 규칙 문서 데이터(블록 27 사용 - 규칙 문서 메시지 형식, 2-29페이지 참조) • 11 - 버전 5.2.x 데이터(여러 호스트, 블록 111 사용 - 5.2.x 버전용 전체 호스트 프로파일 데이터 블록, B-292페이지 참조) • 12 - 버전 5.2.x 데이터(여러 호스트, 블록 111 사용 - 5.2.x 버전용 전체 호스트 프로파일 데이터 블록, B-292페이지 참조) • 13 - 버전 5.3 이상 데이터(여러 호스트, 블록 111 사용 - 5.3 이상 버전용 전체 호스트 프로파일 데이터 블록, 5-1페이지 참조) • 14 - 버전 5.3 이상 데이터(여러 호스트, 블록 111 사용 - 5.3 이상 버전용 전체 호스트 프로파일 데이터 블록, 5-1페이지 참조)
플래그	32비트 필드	• 0x00000001 - 호스트 프로파일의 Notes(메모) 필드에 Firepower System에 저장되어 있는 호스트에 대한 사용자 정의 정보가 입력됩니다. • 0x00000002 - 서비스 블록의 Banner(배너) 필드에 서비스에 대해 탐지된 첫 번째 패킷의 첫 256바이트가 입력됩니다. 배너는 기본적으로 비활성화되며 구성된 경우에만 사용 가능합니다.
시작 IP 주소	uint8[16]	데이터를 반환해야 하는 호스트의 IP 주소(단일 호스트에 대한 요청의 경우) 또는 IP 주소 범위의 시작 주소(여러 호스트에 대한 요청의 경우)입니다. IPv4 또는 IPv6 주소일 수 있습니다.
종료 IP 주소	uint8[16]	IP 주소 범위의 종료 주소(여러 호스트에 대한 요청의 경우) 또는 시작 IP 주소 값(단일 호스트에 대한 요청의 경우)입니다. IPv4 또는 IPv6 주소일 수 있습니다.

아래 그림에는 레거시 호스트 요청 메시지의 형식이 나와 있습니다. eStreamer는 이 요청에도 계속 응답합니다. 레거시 요청과 현재 요청의 차이점은 IPv4 주소 필드가 더 작다는 것뿐입니다. 음영으로 표시된 필드가 호스트 요청 메시지 형식 관련 필드이며, 다음 표에 해당 정의가 나와 있습니다. 그 앞의 3개 필드는 표준 메시지 헤더입니다.

다음 표에는 메시지 필드에 대한 설명이 나와 있습니다.

표 2-14 호스트 요청 메시지 필드

필드	데이터 유형	설명
데이터 유형	uint32	다음 코드를 사용하여 단일 호스트 또는 여러 호스트에 대한 데이터를 요청합니다. • 0 - 버전 3.5~4.6(단일 호스트) • 1 - 버전 3.5~4.6(여러 호스트, 블록 34 사용) • 2 - 버전 4.7~4.8(단일 호스트, 블록 47 사용) • 3 - 버전 4.7~4.8(여러 호스트, 블록 47 사용) • 4 - 버전 4.9~4.10(단일 호스트, 블록 92 사용) • 5 - 버전 4.9~4.10(여러 호스트, 블록 92 사용) • 6 - 버전 5.0 이상 데이터(단일 호스트, 블록 111 사용 - 5.3 이상 버전용 전체 호스트 프로파일 데이터 블록, 5-1페이지 참조) • 7 - 버전 5.0 이상 데이터(여러 호스트, 블록 111 사용 - 5.3 이상 버전용 전체 호스트 프로파일 데이터 블록, 5-1페이지 참조)
플래그	32비트 필드	• 0x00000001 - 호스트 프로파일의 Notes(메모) 필드에 Firepower System에 저장되어 있는 호스트에 대한 사용자 정의 정보가 입력됩니다. • 0x00000002 - 서비스 블록의 Banner(배너) 필드에 서비스에 대해 탐지된 첫 번째 패킷의 첫 256바이트가 입력됩니다. 배너는 기본적으로 비활성화되며 구성된 경우에만 사용 가능합니다.

표 2-14 호스트 요청 메시지 필드 (계속)

필드	데이터 유형	설명
시작 IP 주소	uint8[4]	데이터를 반환해야 하는 호스트의 IP 주소(단일 호스트에 대한 요청의 경우) 또는 IP 주소 범위의 시작 주소(여러 호스트에 대한 요청의 경우)입니다. 주소는 IP 주소 옥텟 형식으로 지정합니다.
종료 IP 주소	uint8[4]	IP 주소 범위의 종료 주소(여러 호스트에 대한 요청의 경우) 또는 시작 IP 주소 값(단일 호스트에 대한 요청의 경우)입니다.

규칙 문서 메시지 형식

규칙 문서 프로파일을 수신하려면 규칙 문서 메시지를 제출합니다. 생성기 ID, 서명 ID 및 수정을 기준으로 이러한 프로파일을 요청합니다.

규칙 문서 정보 요청을 비롯한 모든 데이터 요청의 경우 이벤트 스트림 요청 메시지를 제출하여 먼저 세션을 초기화해야 합니다. 호스트 데이터만 스트리밍하도록 설정하려는 경우 초기 이벤트 스트림 요청 메시지에서 다음의 요청 플래그 설정을 사용할 수 있습니다.

- 적절한 메타데이터 버전용으로 비트 설정(호스트 데이터 스트리밍 시 유용할 수 있음)
- 요청 플래그 설정 안 함
- 비트 11 설정(레거시 버전 eStreamer 사용 시 기본 이벤트 스트리밍을 표시하지 않으려는 경우)

초기 메시지를 제출한 후에는 규칙 문서 메시지(유형 10)를 사용하여 규칙을 지정합니다.

아래 그림에는 규칙 문서 메시지의 형식이 나와 있습니다. 음영으로 표시된 필드가 규칙 문서 메시지 형식 관련 필드이며, 다음 표에 해당 정의가 나와 있습니다. 그 앞의 3개 필드는 표준 메시지 헤더입니다.

예약됨(계속)
예약됨(계속)
예약됨(계속)

다음 표에는 메시지 필드에 대한 설명이 나와 있습니다.

표 2-15 규칙 문서 메시지 필드

필드	데이터 유형	설명
데이터 유형	uint32	규칙 문서 데이터 블록에 대한 데이터를 요청합니다. 이 값은 항상 10입니다. 5.2 이상 버전용 규칙 문서 데이터 블록, 3-106페이지의 내용을 참조하십시오.
플래그	32비트 필드	• 0x00000001 - 규칙 문서 데이터 블록의 Notes(메모) 필드에 Firepower System에 저장되어 있는 호스트에 대한 사용자 정의 정보가 입력됩니다. • 0x00000002 - 서비스 블록의 Banner(배너) 필드에 서비스에 대해 탐지된 첫 번째 패킷의 첫 256바이트가 입력됩니다. 배너는 기본적으로 비활성화되며 구성된 경우에만 사용 가능합니다.
서명 ID	uint32	요청한 규칙의 ID 번호입니다.
생성자 ID	uint32	요청한 규칙의 Firepower System 전처리기 ID 번호입니다.
규칙 수정	uint32	규칙 수정 번호입니다.
예약됨	uint8[20]	이 필드는 현재 사용되지 않습니다.

호스트 데이터 및 여러 호스트 데이터 메시지 형식

eStreamer는 각각 전체 호스트 프로파일 데이터 블록을 포함하는 호스트 데이터 메시지를 보내 호스트 요청에 응답합니다. eStreamer는 요청에 지정된 각 호스트에 대해 호스트 데이터 메시지 하나를 보냅니다. eStreamer는 유형 6 메시지를 사용하여 단일 호스트 프로파일에 대한 요청에 응답하고, 유형 7 메시지를 사용하여 여러 호스트에 대한 요청에 응답합니다. 유형 6 및 7 메시지의 형식은 동일하며 메시지 유형만 다릅니다.

호스트 데이터 메시지에는 레코드 유형 필드가 없습니다. 메시지 구조는 메시지에 포함된 전체 호스트 프로파일의 데이터 블록 유형과 메시지 유형을 통해 전달됩니다. 전체 호스트 프로파일 데이터 블록은 계열 내의 블록 그룹입니다.

다음 그림에는 호스트 데이터 메시지의 형식이 나와 있고, 그 아래의 표에는 음영으로 표시된 필드의 정의가 나와 있습니다.

호스트 요청 메시지 관련 필드는 다음과 같습니다.

표 2-16

필드	데이터 유형	설명
전체 호스트 프로파일 데이터 블록 유형	uint32	메시지에 포함된 전체 호스트 프로파일의 데이터의 블록 유형을 지정합니다. 표 4-30 호스트 검색 및 연결 데이터 블록 유형, 4-64페이지의 내용을 참조하십시오.
길이	uint32	메시지의 전체 호스트 프로파일의 데이터 길이입니다.
전체 호스트 프로파일 데이터 블록	variable	호스트 데이터입니다. 현재 전체 호스트 프로파일 데이터 블록 정의를 확인할 수 있는 링크는 표 4-30 호스트 검색 및 연결 데이터 블록 유형, 4-64페이지의 내용을 참조하십시오.

스트리밍 정보 메시지 형식

eStreamer 서비스는 확장 요청을 받으면 아래에서 설명하는 스트리밍 정보 메시지를 클라이언트에 보냅니다. 이 메시지는 서버의 사용 가능한 서비스 목록을 알립니다. 현재 관련 옵션은 eStreamer 서비스(6667)뿐이지만 메시지에는 다른 서비스도 나열될 수 있으며, 이러한 서비스는 무시해야 합니다. 알림이 제공되는 각 서비스는 스트리밍 서비스 요청 구조, 2-33페이지에 설명되어 있는 스트리밍 서비스 요청 구조로 표시됩니다.

아래 그림에는 스트리밍 정보 메시지의 형식이 나와 있습니다. 음영으로 표시된 필드가 이 메시지 유형 관련 필드입니다. 그 앞의 3개 필드는 표준 메시지 헤더입니다.

스트리밍 정보 메시지의 필드는 다음과 같습니다.

표 2-17 스트리밍 정보 메시지 필드

필드	데이터 유형	설명
헤더 버전	uint16	1로 설정됩니다.
메시지 유형	uint16	eStreamer 메시지 유형입니다. 스트리밍 요청 메시지의 경우 2051로 설정됩니다.
메시지 길이	uint32	메시지 헤더 뒤의 메시지 콘텐츠 길이입니다. Header Version(헤더 버전), Message Type(메시지 유형) 및 Message Length(메시지 길이) 필드의 바이트는 포함되지 않습니다.
서비스[]	array	사용 가능한 서비스의 목록입니다. 스트리밍 서비스 요청 구조, 2-33페이지의 내용을 참조하십시오.

스트리밍 요청 메시지 형식

클라이언트는 스트리밍 요청 메시지를 사용하여 eStreamer에 대해 스트리밍 정보 메시지에서 사용하려는 서비스, 그리고 스트리밍할 이벤트 유형과 버전에 대한 요청 집합을 차례로 지정합니다. 다음 그림에는 메시지 구조가 나와 있고, 그 아래의 표에는 필드의 정의가 나와 있습니다. 요청되는 서비스는 스트리밍 서비스 요청 구조, 2-33페이지에 설명되어 있는 스트리밍 서비스 요청 구조로 표시됩니다.

아래 그림에는 스트리밍 정보 메시지의 형식이 나와 있습니다. 음영으로 표시된 필드가 이 메시지 유형 관련 필드입니다. 그 앞의 3개 필드는 표준 메시지 헤더입니다.

스트리밍 요청 메시지의 필드는 다음과 같습니다.

표 2-18 스트리밍 요청 메시지 필드

필드	데이터 유형	설명
헤더 버전	uint16	1로 설정됩니다.
메시지 유형	uint16	eStreamer 메시지 유형입니다. 스트리밍 요청 메시지의 경우 2049로 설정됩니다.

표 2-18 스트리밍 요청 메시지 필드 (계속)

필드	데이터 유형	설명
메시지 길이	uint32	메시지 헤더 뒤의 메시지 콘텐츠 길이입니다. Header Version(헤더 버전), Message Type(메시지 유형) 및 Message Length(메시지 길이) 필드의 바이트는 포함되지 않습니다.
서비스[]	array	요청된 서비스 구조의 목록입니다. 스트리밍 서비스 요청 구조, 2-33페이지의 내용을 참조하십시오.

스트리밍 서비스 요청 구조

eStreamer 서비스는 알림을 제공하는 각 서비스에 대해 스트리밍 정보 메시지에서 스트리밍 서비스 요청 데이터 구조 하나를 보냅니다. eStreamer 서비스는 스트리밍 서비스 요청의 마지막 필드(포함할 이벤트 유형 목록을 제공함)는 사용하지 않습니다.

클라이언트는 eStreamer에서 스트리밍 서비스 요청 구조를 처리하며 서버로 반환하는 응답에서 동일한 구조를 사용합니다. 클라이언트가 서버로 보내는 스트리밍 서비스 요청에는 먼저 eStreamer에서 알림을 제공한 서비스에 대한 요청이 포함되고, 그다음에는 클라이언트가 수신하려는 요청된 이벤트 유형을 지정하는 스트리밍 이벤트 유형 구조의 목록이 포함됩니다.

각 스트리밍 이벤트 유형 구조에는 요청한 각 이벤트 유형에 대해 이벤트 유형과 버전을 지정하는 두 개의 필드가 포함됩니다. 스트리밍 이벤트 유형 구조에 대한 자세한 정보는스트리밍 서비스 요청 구조, 2-33페이지의 내용을 참조하십시오.

아래 그림에는 스트리밍 서비스 요청 구조의 필드가 나와 있습니다. 그림 아래의 표에 필드의 정의가 나와 있습니다.

스트리밍 서비스 요청 구조의 필드는 다음과 같습니다.

표 2-19 스트리밍 서비스 요청 필드

필드	데이터 유형	설명
유형	uint32	서비스 ID. 이 필드는 eStreamer 서버 메시지에서는 사용 가능한 서비스를 알립니다. 클라이언트 메시지에서는 요청된 서비스를 지정합니다. 현재 유효한 옵션은 다음과 같습니다. • 6667(eStreamer 서비스용)
길이	uint32	서비스 요청 길이입니다. 유형과 길이를 포함한 서비스 요청의 길이를 설명합니다. 길이에는 메시지의 모든 스트리밍 이벤트 유형 레코드와 종료 레코드가 포함되어야 합니다.
플래그	uint32	eStreamer의 스트리밍 정보 메시지에서는 항상 0입니다. 클라이언트의 스트리밍 요청 메시지에서는 원래 이벤트 스트림 요청 메시지의 플래그 설정을 복제합니다.
초기 타임스탬프	uint32	eStreamer의 스트리밍 정보 메시지에서는 항상 0입니다. 클라이언트의 스트리밍 요청 메시지에서는 원래 이벤트 스트림 요청 메시지의 타임스탬프를 복제합니다.
스트리밍 이벤트 유형	array	eStreamer의 스트리밍 정보 메시지: • 이후 사용을 위해 예약됩니다. 길이는 0입니다. 클라이언트의 스트리밍 정보 메시지: • 요청한 각 이벤트 유형당 스트리밍 이벤트 유형 엔트리가 하나씩 포함됩니다. 스트리밍 서비스 요청 구조, 2-33페이지의 내용을 참조하십시오. • 이벤트 유형 엔트리 0으로 요청 목록을 종료합니다. 이벤트 유형과 버전은 모두 0으로 설정됩니다. 스트리밍 서비스 요청 구조, 2-33페이지의 내용을 참조하십시오.

도메인 스트리밍 요청 메시지 형식

클라이언트는 도메인 스트리밍 요청 메시지를 사용하여 eStreamer에서 특정 도메인의 이벤트를 요청합니다. 다음 그림에는 메시지 구조가 나와 있고, 그 아래의 표에는 필드의 정의가 나와 있습니다. 음영으로 표시된 필드가 이 메시지 유형 관련 필드입니다. 그 앞의 3개 필드는 표준 메시지 헤더입니다.

도메인 스트리밍 요청 메시지의 필드는 다음과 같습니다.

표 2-20 도메인 스트리밍 요청 메시지 필드

필드	데이터 유형	설명
헤더 버전	uint16	1로 설정됩니다.
메시지 유형	uint16	eStreamer 메시지 유형입니다. 도메인 스트리밍 요청 메시지의 경우 2052로 설정됩니다.
메시지 길이	uint32	메시지 헤더 뒤의 메시지 콘텐츠 길이입니다. Header Version(헤더 버전), Message Type(메시지 유형) 및 Message Length(메시지 길이) 필드의 바이트는 포함되지 않습니다.
문자열 블록 유형	uint32	도메인이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	도메인 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 도메인의 바이트 수를 더한 값이 포함됩니다.
도메인	string	스트리밍 이벤트를 요청하는 도메인입니다. 비워 두는 경우 서비스는 클라이언트가 액세스할 수 있는 모든 도메인에 대해 이벤트를 스트리밍합니다.

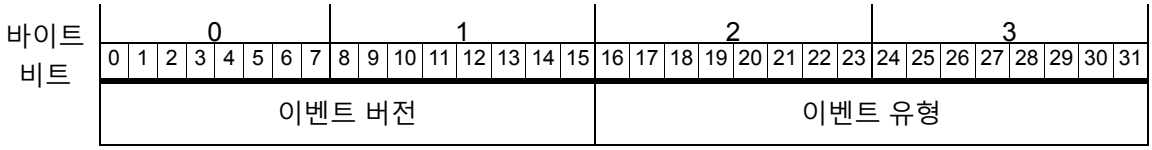
스트리밍 이벤트 유형 구조

eStreamer 클라이언트는 스트리밍 이벤트 유형 구조를 사용하여 이벤트의 버전을 지정합니다. 각 이벤트 버전/유형 조합은 이벤트 스트림에 대한 요청입니다.

스트리밍 이벤트 유형 구조 목록은 모든 필드가 0으로 설정된 구조로 끝나야 합니다. 즉, 버전과 유형을 다음과 같이 설정해야 합니다.

```
이벤트 버전 = 0
이벤트 유형 = 0
```

다음 다이어그램에는 스트리밍 이벤트 유형 구조의 형식이 나와 있습니다.



스트리밍 이벤트 유형 구조의 필드는 다음과 같습니다.

표 2-21 스트리밍 이벤트 유형 필드

필드	데이터 유형	설명
이벤트 버전	uint16	이벤트 유형의 버전 번호입니다. 각 이벤트 유형에 대해 지원되는 버전의 목록은 표 2-22 확장 요청용 이벤트 유형 및 버전, 2-37페이지의 내용을 참조하십시오.
이벤트 유형	uint16	요청된 이벤트 유형의 코드입니다. 유효한 이벤트 유형 및 버전 코드의 현재 목록은 표 2-22 확장 요청용 이벤트 유형 및 버전, 2-37페이지의 내용을 참조하십시오. 이벤트 유형의 목록은 이벤트 유형과 이벤트 버전이 모두 0으로 끝나야 합니다.

다음 표에는 클라이언트가 확장 요청에서 지정할 수 있는 이벤트 유형과 버전이 나와 있습니다. 이 표에는 각 이벤트 유형 버전에 해당하는 Management Center 소프트웨어 버전이 표시되어 있습니다. 예를 들어 Management Center 버전 4.8.0.2~4.9.1에서 지원되었던 상관관계 이벤트를 요청하려면 이벤트 유형 31, 버전 5를 요청해야 합니다. 다른 이벤트 유형으로 기록된 이벤트는 요청한 이벤트 유형의 형식과 일치하도록 업그레이드되거나 다운그레이드됩니다.

표 2-22 확장 요청용 이벤트 유형 및 버전

요청 대상...	사용할 이벤트 버전 번호...	이벤트 코드
침입 이벤트	1 - 4.8.x 이하 2 - 4.9~4.10.x 3 - 5.0~5.1 4 - 5.1.1.x 5 - 5.2.x 6 - 5.3 7 - 5.3.1 8 - 5.4.x 9 - 6.0 이상	12
메타데이터	1 - 3.2~4.5.x 2 - 4.6.0.x 3 - 4.6.1~4.6.x 4 - 4.7 이상	21
상관관계 및 컴플라이언스 화이트리스트 이벤트	1 - 3.2 이하 2 - 4.0~4.4.x 3 - 4.5~4.6.1 4 - 4.7~4.8.0.1 5 - 4.8.0.2~4.9.1.x 6 - 4.10.0~4.10.x 7 - 5.0~5.0.2 8 - 5.1~5.3.x 9 - 5.4 이상	31
검색 이벤트	1 - 3.2 이하 2 - 3.0~3.4.x 3 - 3.5~4.6.x 4 - 4.7~4.8.x 5 - 4.9.0.x 6 - 4.9.1~4.9.x.x 7 - 4.10.0~4.10.x 8 - 5.0.x 9 - 5.1.x 10 - 5.2~5.3 11 - 5.3.1 이상	61

표 2-22 확장 요청용 이벤트 유형 및 버전 (계속)

요청 대상...	사용할 이벤트 버전 번호...	이벤트 코드
연결 이벤트	1 - 4.0~4.1 3 - 4.5~4.6.1 4 - 4.7~4.9.0.x 5 - 4.9.1~4.10.x 6 - 5.0.x 7 - 5.1.0.x 8 - 5.1.1.x 9 - 5.2.x 10 - 5.3 11 - 5.3.1 12 - 5.4 13 - 5.4.0.1~5.4.0.2 14 - 6.0.x 15 - 6.1.x 16 - 6.2 이상	71
사용자 이벤트	1 - 4.7~4.10.x 2 - 5.0.x 3 - 5.1~5.1.x 4 - 5.2 5 - 6.0 6 - 6.1 7 - 6.2 이상	91
악성코드 이벤트	1 - 5.1.0.x 2 - 5.1.1.x 3 - 5.2.x 4 - 5.3 5 - 5.3.1 6 - 5.4.x 7 - 6.0 이상	101
파일 이벤트	1 - 5.1.1~5.1.x 2 - 5.2.x 3 - 5.3 4 - 5.3.1 5 - 5.4.x 6 - 6.0 이상	111
영향 상관관계 이벤트	1 - 5.2.x 이하 2 - 5.3 이상	131
목록의 종료 이벤트 유형	0	0

샘플 확장 요청 메시지

스트리밍 정보 메시지

아래 샘플에서 서버는 2개 서비스를 알립니다. 첫 번째 유형은 6667(eStreamer)이고 두 번째 유형은 5000입니다. 서버의 스트리밍 정보 메시지에서 플래그 필드와 초기 타임스탬프 필드는 0이며 메시지는 이벤트 유형을 지정하지 않습니다.

표 2-23

헤더 버전:	1	/*항상 1*/
메시지 유형:	2051	/*스트리밍 정보 메시지*/
메시지 길이	32	/*메시지 콘텐츠의 바이트 수*/
서비스[1].유형	6667	/*eStreamer 서비스 ID*/
서비스[1].길이	8	
서비스[1].플래그	0	/*서버의 플래그 없음*/
서비스[1].초기 타임스탬프	0	/*항상 0*/
서비스[2].유형	5000	/*서비스-2 ID*/
서비스[2].길이	8	
서비스[2].플래그	0	/*서버의 플래그 없음*/
서비스[2].초기 타임스탬프	0	/*항상 0*/
헤더 버전:	1	/*항상 1*/
메시지 유형:	2051	/*스트리밍 정보 메시지*/

스트리밍 요청 메시지

아래에 나와 있는 스트리밍 요청 메시지에서는 클라이언트가 서비스 유형 6667(eStreamer)을 요청하고 두 가지 이벤트 유형을 지정합니다. 그중 하나는 연결 이벤트의 버전 6(이벤트 유형 71)이고, 다른 하나는 메타데이터의 버전 4(이벤트 유형 21)입니다.

표 2-24

헤더 버전:	1	/*항상 1*/
메시지 유형:	2049	/*스트림 요청 메시지*/
메시지 길이	28	/*페이로드 바이트*/
서비스[1].유형	6667	/*eStreamer 서비스 ID*/
서비스[1].길이	20	
서비스[1].플래그	30	/*원래 플래그 값*/
서비스[1].초기 타임스탬프	0	/*원래 타임스탬프*/
서비스[1].이벤트[1].버전	6	/*버전 6*/
서비스[1].이벤트[1].유형	71	/*연결 이벤트*/

표 2-24

서비스[1].이벤트[2].버전	4	/*버전 4*/
서비스[1].이벤트[2].유형	21	/*메타데이터*/
서비스[1].이벤트[3].버전	0	/*이벤트 목록 종료*/
서비스[1].이벤트[3].유형	0	/*이벤트 목록 종료*/

메시지 번들 형식

eStreamer 서버는 클라이언트가 확장 요청을 제출하면 번들 형식으로 메시지를 보냅니다.

클라이언트는 전체 번들 수신을 승인하는 null 메시지로 응답합니다. 클라이언트는 번들의 개별 메시지 수신을 승인해서는 안 됩니다.

메시지 번들의 메시지 유형은 4002입니다.

아래 그림에는 메시지 번들의 구조가 나와 있습니다. 음영으로 표시된 필드가 번들 메시지 유형 관련 필드입니다. 그 아래의 표에는 필드 및 데이터 구조 콘텐츠에 대한 설명이 나와 있습니다.

메시지 번들 메시지의 필드는 다음과 같습니다.

표 2-25 메시지 번들 메시지 필드

필드	데이터 유형	설명
헤더 버전	uint16	항상 1입니다.
메시지 유형	uint16	항상 4002입니다.
메시지 길이	uint32	메시지 헤더 뒤의 메시지 콘텐츠 길이입니다. 번들의 Header Version(헤더 버전), Message Type(메시지 유형) 및 Message Length(메시지 길이) 필드의 바이트는 포함되지 않습니다. 클라이언트는 번들에서 메시지를 로드할 때 이 필드의 길이에서 메시지의 총 길이(헤더 포함)를 뺄 수 있습니다. 이 계산의 값이 양수이면 메시지를 더 처리할 수 있습니다.
연결 ID	uint32	서버와의 연결에 대한 고유 식별자입니다.

표 2-25 메시지 번들 메시지 필드 (계속)

필드	데이터 유형	설명
시퀀스 번호	uint32	1부터 시작하여 eStreamer 서버에서 보낸 번들마다 1씩 증가합니다.
이벤트 메시지 []	array	번들에서 서버가 스트리밍한 이벤트입니다. 각 메시지에는 메시지 버전 번호(1), 아카이브 타임스탬프(요청한 경우) 등을 비롯한 전체 헤더 집합이 포함됩니다.

메타데이터 이해

eStreamer 서버는 요청한 이벤트 레코드와 함께 메타데이터를 제공할 수 있습니다. 메타데이터를 받으려면 명시적으로 요청을 해야 합니다. 지정된 메타데이터 버전을 요청하는 방법에 대한 자세한 정보는 표 2-6 요청 플래그, 2-12페이지의 내용을 참조하십시오. 메타데이터는 이벤트 레코드의 코드 및 숫자 식별자에 대한 상황 정보를 제공합니다. 침입 이벤트에는 탐지 디바이스의 내부 식별자만 포함되어 있는데 메타데이터가 디바이스 이름을 제공하는 경우를 예로 들 수 있습니다.

메타데이터 전송

요청 메시지에서 메타데이터를 지정하는 경우 eStreamer는 관련 이벤트 레코드를 보내기 전에 관련 메타데이터 레코드를 보냅니다.

eStreamer에서는 클라이언트로 보낸 메타데이터를 추적하여 같은 메타데이터 레코드를 다시 보내지 않습니다. 클라이언트는 받은 각 메타데이터 레코드를 캐시해야 합니다. eStreamer는 세션 간의 메타데이터 전송 기록을 유지하지 않으므로 새 세션이 시작되어 요청 메시지가 메타데이터를 지정하는 경우 eStreamer는 메타데이터 스트리밍을 처음부터 재시작합니다.

침입 및 상관관계 데이터 구조 이해

eStreamer 서비스는 요청된 이벤트와 메타데이터를 클라이언트에 제공하기 위해 여러 데이터 레코드 유형을 전송합니다. 이 장에서는 다음 이벤트 데이터 유형에 대한 데이터 레코드의 구조에 대해 설명합니다.

- 매니지드 디바이스에서 생성되는 침입 이벤트 데이터 및 이벤트 추가 데이터
- Management Center에서 생성되는 상관관계(컴플라이언스) 이벤트
- 메타데이터 레코드

이 장의 다음 섹션에서는 이벤트 메시지 구조를 정의합니다.

- 침입 이벤트 및 메타 데이터 레코드 유형, 3-1페이지.

데이터 레코드 전송을 위한 eStreamer의 메시지 형식과 관련된 일반적인 개요는 이벤트 데이터 메시지 형식, 2-17페이지의 내용을 참조하십시오.

침입 이벤트 및 메타 데이터 레코드 유형

다음 표에는 침입 이벤트, 침입 이벤트 추가 데이터 및 메타데이터 메시지에 대해 현재 지원되는 모든 레코드 유형이 나와 있습니다. 이러한 레코드 유형의 데이터는 고정 길이 필드에 포함되어 있습니다. 반면 상관관계 이벤트 레코드는 가변 길이의 중첩 데이터 블록 레벨을 하나 이상 포함합니다. 아래 표에는 관련 데이터 레코드 구조 정의를 제공하는 장 하위 섹션의 링크가 나와 있습니다.

일부 레코드 유형의 경우 eStreamer에서는 둘 이상의 버전을 지원합니다. 표에는 각 버전의 상태(현재 또는 레거시)가 나와 있습니다. 현재 레코드는 최신 버전입니다. 레거시 레코드는 이후 버전으로 대체되었지만 여전히 eStreamer에서 요청될 수 있습니다.

표 3-1 침입 이벤트 및 일반 메타데이터 레코드 유형

레코드 유형	블록 유형	계열	설명	레코드 상태	데이터 형식의 설명을 확인할 수 있는 위치
2	해당 없음	해당 없음	패킷 데이터(버전 4.8.0.2 이상)	현재	4.8.0.2 이상 버전용 패킷 레코드, 3-6페이지
4	해당 없음	해당 없음	우선순위 메타데이터	현재	우선순위 레코드, 3-7페이지
9	20	1	침입 영향 알림	레거시	침입 영향 알림 데이터, B-46페이지
9	153	1	침입 영향 알림	현재	5.3 이상 버전용 침입 영향 알림 데이터, 3-17페이지

표 3-1 침입 이벤트 및 일반 메타데이터 레코드 유형 (계속)

레코드 유형	블록 유형	계열	설명	레코드 상태	데이터 형식의 설명을 확인할 수 있는 위치
62	해당 없음	2	사용자 메타데이터	현재	사용자 레코드, 3-20페이지
66	해당 없음	해당 없음	규칙 메시지 메타데이터(버전 4.6.1 이상)	현재	4.6.1 이상 버전용 규칙 메시지 레코드, 3-21페이지
67	해당 없음	해당 없음	분류 메타데이터(버전 4.6.1 이상)	현재	4.6.1 이상 버전용 분류 레코드, 3-22페이지
69	해당 없음	해당 없음	상관관계 정책 메타데이터(버전 4.6.1 이상)	현재	상관관계 정책 레코드, 3-23페이지
70	해당 없음	해당 없음	상관관계 규칙 메타데이터(버전 4.6.1 이상)	현재	상관관계 규칙 레코드, 3-25페이지
104	해당 없음	해당 없음	침입 이벤트(IPv4) 레코드(버전 4.9~4.10.x)	레거시	제품의 이전 버전
105	해당 없음	해당 없음	침입 이벤트(IPv6) 레코드(버전 4.9~4.10.x)	레거시	제품의 이전 버전
110	4	2	침입 이벤트 추가 데이터(버전 4.10.0 이상)	현재	침입 이벤트 추가 데이터 레코드, 3-27페이지
111	5	2	침입 이벤트 추가 데이터 메타데이터(버전 4.10.0 이상)	현재	침입 이벤트 추가 데이터 메타데이터, 3-28페이지
112	128	1	5.1~5.3.x 버전용 상관관계 이벤트	레거시	5.1~5.3.x 버전용 상관관계 이벤트, B-266페이지
112	156	1	5.4 이상 버전용 상관관계 이벤트	현재	5.4 이상 버전용 상관관계 이벤트, 3-44페이지
115	14	2	보안 영역 이름 메타데이터	현재	보안 영역 이름 레코드, 3-30페이지
116	14	2	인터페이스 이름 메타데이터	현재	인터페이스 이름 레코드, 3-31페이지
117	14	2	액세스 제어 정책 이름 메타데이터	현재	액세스 제어 정책 이름 레코드, 3-33페이지
118	15	2	침입 정책 이름 메타데이터	현재	침입 정책 이름 레코드, 4-22페이지
119	15	2	액세스 제어 규칙 ID 메타데이터	현재	액세스 제어 규칙 ID 레코드 메타데이터, 3-34페이지
120	해당 없음	해당 없음	액세스 제어 규칙 작업 메타데이터	현재	액세스 제어 규칙 작업 레코드 메타데이터, 4-23페이지
121	해당 없음	해당 없음	URL 카테고리 메타데이터	현재	URL 카테고리 레코드 메타데이터, 4-24페이지
122	해당 없음	해당 없음	URL 평판 메타데이터	현재	URL 평판 레코드 메타데이터, 4-25페이지
123	해당 없음	해당 없음	매니지드 디바이스 메타데이터	현재	매니지드 디바이스 레코드 메타데이터, 3-35페이지
해당 없음	64	2	액세스 제어 이름 데이터 블록	현재	액세스 제어 정책 이름 데이터 블록, 3-82페이지
124	59	2	액세스 제어 정책 규칙 이유 데이터 블록	현재	6.0 이상 버전용 액세스 제어 정책 규칙 이유 데이터 블록, 3-79페이지

표 3-1 침입 이벤트 및 일반 메타데이터 레코드 유형 (계속)

레코드 유형	블록 유형	계열	설명	레코드 상태	데이터 형식의 설명을 확인할 수 있는 위치
125	해당 없음	2	악성코드 이벤트 레코드(버전 5.1.1 이상)	현재	5.1.1 이상 버전용 악성코드 이벤트 레코드, 3-36페이지
125	24	2	악성코드 이벤트(버전 5.1.1 이상)	현재	5.1.1.x 버전용 악성코드 이벤트 데이터 블록, B-53페이지
125	33	2	악성코드 이벤트(버전 5.2.x)	레거시	5.2.x 버전용 악성코드 이벤트 데이터 블록, B-59페이지
125	35	2	악성코드 이벤트(버전 5.3)	레거시	5.3 버전용 악성코드 이벤트 데이터 블록, B-66페이지
125	44	2	악성코드 이벤트(버전 5.3.1)	레거시	5.3.1 버전용 악성코드 이벤트 데이터 블록, B-73페이지
125	47	2	악성코드 이벤트(버전 5.4.x)	현재	5.4.x 버전용 악성코드 이벤트 데이터 블록, B-80페이지
125	62	2	악성코드 이벤트(버전 6.0 이상)	현재	6.0 이상 버전용 악성코드 이벤트 데이터 블록, 3-94페이지
127	14	2	Cisco Advanced Malware Protection 클라우드 이름 메타데이터(버전 5.1 이상)	현재	Cisco Advanced Malware Protection 클라우드 이름 메타데이터, 3-37페이지
128	해당 없음	해당 없음	악성코드 이벤트 유형 메타데이터(버전 5.1 이상)	현재	악성코드 이벤트 유형 메타데이터, 3-39페이지
129	해당 없음	해당 없음	악성코드 이벤트 하위 유형 메타데이터(버전 5.1 이상)	현재	악성코드 이벤트 하위 유형 메타데이터, 3-40페이지
130	해당 없음	해당 없음	AMP for Endpoints 탐지기 유형 메타데이터(버전 5.1 이상)	현재	AMP for Endpoints 탐지기 유형 메타데이터, 3-41페이지
131	해당 없음	해당 없음	AMP for Endpoints 파일 유형 메타데이터(버전 5.1 이상)	현재	AMP for Endpoints 파일 유형 메타데이터, 3-42페이지
132	해당 없음	해당 없음	보안 상황 이름	현재	보안 상황 이름, 3-43페이지
140	27	2	5.2 이상 버전용 규칙 문서 데이터 블록	현재	5.2 이상 버전용 규칙 문서 데이터 블록, 3-106페이지
207	해당 없음	해당 없음	5.0.x~5.1 버전용 침입 이벤트(IPv4) 레코드	레거시	5.0.x~5.1 버전용 침입 이벤트(IPv4) 레코드, B-2페이지
208	해당 없음	해당 없음	5.0.x~5.1 버전용 침입 이벤트(IPv6) 레코드	레거시	5.0.x~5.1 버전용 침입 이벤트(IPv6) 레코드, B-7페이지
260	19	2	ICMP 유형 데이터 데이터 블록	현재	ICMP 유형 데이터 블록, 3-67페이지
270	20	2	ICMP 코드 데이터 블록	현재	ICMP 코드 데이터 블록, 3-69페이지
282	해당 없음	2	5.4.1 이상 버전용 보안 인텔리전스 카테고리 메타데이터	현재	5.4.1 이상 버전용 보안 인텔리전스 카테고리 메타데이터, 3-70페이지

표 3-1 침입 이벤트 및 일반 메타데이터 레코드 유형 (계속)

레코드 유형	블록 유형	계열	설명	레코드 상태	데이터 형식의 설명을 확인할 수 있는 위치
300	해당 없음	해당 없음	6.0 이상 버전용 영역 메타데이터	현재	6.0 이상 버전용 영역 메타데이터, 3-71페이지
301	58	2	6.0 이상 버전용 엔드포인트 프로파일	현재	6.0 이상 버전용 엔드포인트 프로파일 데이터 블록, 3-72페이지
302	해당 없음	해당 없음	6.0 이상 버전용 보안 그룹 메타데이터	현재	6.0 이상 버전용 보안 그룹 메타데이터, 3-73페이지
320	해당 없음	해당 없음	6.0 이상 버전용 DNS 레코드 유형 메타데이터	현재	6.0 이상 버전용 DNS 레코드 유형 메타데이터, 3-74페이지
321	해당 없음	해당 없음	6.0 이상 버전용 DNS 응답 유형 메타데이터	현재	6.0 이상 버전용 DNS 응답 유형 메타데이터, 3-76페이지
322	해당 없음	해당 없음	6.0 이상 버전용 싱크홀 메타데이터	현재	6.0 이상 버전용 싱크홀 메타데이터, 3-77페이지
350	해당 없음	해당 없음	6.0 이상 버전용 네트워크 맵 도메인 메타데이터	현재	6.0 이상 버전용 네트워크 맵 도메인 메타데이터, 3-78페이지
400	34	2	5.2.x 버전용 침입 이벤트 레코드	레거시	5.2.x 버전용 침입 이벤트 레코드, B-12페이지
400	41	2	5.3 버전용 침입 이벤트 레코드	레거시	5.3 버전용 침입 이벤트 레코드, B-19페이지
400	42	2	5.3.1 버전용 침입 이벤트 레코드	레거시	5.3.1 버전용 침입 이벤트 레코드, B-31페이지
400	45	2	5.4.x 버전용 침입 이벤트 레코드	레거시	5.4.x 버전용 침입 이벤트 레코드, B-37페이지
400	60	2	6.0 이상 버전용 침입 이벤트 레코드	현재	6.0 이상 버전용 침입 이벤트 레코드, 3-8페이지
500	32	2	파일 이벤트(버전 5.2.x)	레거시	5.2.x 버전용 파일 이벤트, B-230페이지
500	38	2	파일 이벤트(버전 5.3)	레거시	5.3 버전용 파일 이벤트, B-234페이지
500	43	2	파일 이벤트(버전 5.3.1)	레거시	5.3.1 버전용 파일 이벤트, B-240페이지
500	46	2	파일 이벤트(버전 5.4 이상)	현재	6.0 이상 버전용 파일 이벤트, 3-84페이지
502	32	2	파일 이벤트(버전 5.2.x)	레거시	5.2.x 버전용 파일 이벤트, B-230페이지
502	38	2	파일 이벤트(버전 5.3)	레거시	5.3 버전용 파일 이벤트, B-234페이지
502	43	2	파일 이벤트(버전 5.3.1)	레거시	5.3.1 버전용 파일 이벤트, B-240페이지
502	46	2	파일 이벤트(버전 5.4.x)	현재	5.4.x 버전용 파일 이벤트, B-247페이지
502	56	2	파일 이벤트(버전 6.0 이상)	현재	6.0 이상 버전용 파일 이벤트, 3-84페이지
510	해당 없음	해당 없음	5.3 이상 버전용 파일 유형 ID 메타데이터	현재	5.3 이상 버전용 파일 유형 ID 메타데이터, 3-106페이지
511	26	2	5.11~5.2.x 버전용 파일 이벤트 SHA 해시	레거시	5.1.1~5.2.x 버전용 파일 이벤트 SHA 해시, B-257페이지
511	40	2	5.3 이상 버전용 파일 이벤트 SHA 해시	현재	5.3 이상 버전용 파일 이벤트 SHA 해시, 3-104페이지

표 3-1 침입 이벤트 및 일반 메타데이터 레코드 유형 (계속)

레코드 유형	블록 유형	계열	설명	레코드 상태	데이터 형식의 설명을 확인할 수 있는 위치
515	해당 없음	해당 없음	6.0 이상 버전용 파일 로그 스토리지 메타데이터	현재	6.0 이상 버전용 파일 로그 스토리지 메타데이터, 3-111페이지
516	해당 없음	해당 없음	6.0 이상 버전용 파일 로그 샌드박스 메타데이터	현재	6.0 이상 버전용 파일 로그 샌드박스 메타데이터, 3-112페이지
517	해당 없음	해당 없음	6.0 이상 버전용 파일 로그 Spero 메타데이터	현재	6.0 이상 버전용 파일 로그 Spero 메타데이터, 3-113페이지
518	해당 없음	해당 없음	6.0 이상 버전용 파일 로그 아카이브 메타데이터	현재	6.0 이상 버전용 파일 로그 아카이브 메타데이터, 3-114페이지
519	해당 없음	해당 없음	6.0 이상 버전용 파일 로그 정적 분석 메타데이터	현재	6.0 이상 버전용 파일 로그 정적 분석 메타데이터, 3-115페이지
520	28	2	5.2 이상 버전용 지리위치 데이터 블록	현재	5.2 이상 버전용 지리위치 데이터 블록, 3-115페이지
530	해당 없음	해당 없음	6.0 이상 버전용 파일 정책 이름	현재	6.0 이상 버전용 파일 정책 이름, 3-117페이지
600	해당 없음	해당 없음	SSL 정책 이름	현재	SSL 정책 이름, 3-118페이지
601	51	2	SSL 규칙 ID	현재	SSL 규칙 ID, 3-119페이지
602	해당 없음	해당 없음	SSL 암호 그룹	현재	5.4 이상 버전용 SSL 인증서 세부사항 데이터 블록, 3-127페이지
604	해당 없음	해당 없음	SSL 버전	현재	SSL 버전, 3-122페이지
605	해당 없음	해당 없음	SSL 서버 인증서 상태	현재	SSL 서버 인증서 상태, 3-123페이지
606	해당 없음	해당 없음	SSL 실제 작업	현재	SSL 실제 작업, 3-124페이지
607	해당 없음	해당 없음	SSL 예상 작업	현재	SSL 예상 작업, 3-125페이지
608	해당 없음	해당 없음	SSL 플로우 상태	현재	SSL 플로우 상태, 3-126페이지
613	해당 없음	해당 없음	SSL URL 카테고리	현재	SSL URL 카테고리, 3-127페이지
614	50	2	5.4 이상 버전용 SSL 인증서 세부사항 데이터 블록	현재	5.4 이상 버전용 SSL 인증서 세부사항 데이터 블록, 3-127페이지
700	해당 없음	해당 없음	네트워크 분석 정책 레코드	현재	네트워크 분석 정책 이름 레코드, 3-132페이지

4.8.0.2 이상 버전용 패킷 레코드

eStreamer 서비스는 이벤트와 관련된 패킷 데이터를 패킷 레코드 내에 포함하여 전송합니다. 해당 레코드의 형식은 아래에 나와 있습니다. 패킷 플래그(요청 메시지의 Request Flags(요청 플래그) 필드에 포함된 비트 0)가 설정되어 있으면 패킷 데이터가 전송됩니다. 요청 플래그, 2-12페이지의 내용을 참조하십시오. 비트 23을 활성화하면 레코드에 확장 이벤트 헤더가 포함됩니다. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 패킷 레코드임을 나타내는 2입니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
헤더 버전(1)																	메시지 유형(4)															
메시지 길이																																
네트워크 맵 ID																	레코드 유형(2)															
레코드 길이																																
eStreamer 서버 타임스탬프(이벤트에서 비트 23이 설정된 경우에 한함)																																
이후 사용을 위해 예약됨(이벤트에서 비트 23이 설정된 경우에 한함)																																
디바이스 ID																																
이벤트 ID																																
이벤트 초																																
패킷 초																																
패킷 마이크로초																																
링크 유형																																
패킷 길이																																
패킷 데이터...																																

다음 표에는 패킷 레코드의 필드에 대한 설명이 나와 있습니다.

표 3-2 패킷 레코드 필드

필드	데이터 유형	설명
디바이스 ID	uint32	디바이스 ID 번호입니다. 버전 3 또는 4 메타데이터를 요청하면 디바이스와 상관관계가 있는 디바이스 이름을 가져올 수 있습니다. 자세한 정보는 매니지드 디바이스 레코드 메타데이터, 3-35페이지의 내용을 참조하십시오.
이벤트 ID	uint32	이벤트 ID 번호입니다.
이벤트 초	uint32	이벤트가 발생한 초 단위 시간(1970년 1월 1일 이후)입니다.
패킷 초	uint32	패킷이 캡처된 초 단위 시간(1970년 1월 1일 이후)입니다.
패킷 마이크로초	uint32	패킷이 캡처된 마이크로초(100만분의 1초) 단위의 증분 시간입니다.
링크 유형	uint32	링크 계층 유형입니다. 현재 해당 값은 항상 이더넷 계층을 나타내는 1입니다.
패킷 길이	uint32	패킷 데이터에 포함된 바이트 수입니다.
패킷 데이터	variable	실제로 캡처된 패킷 데이터(헤더 및 페이로드)입니다.

우선순위 레코드

eStreamer 서비스는 이벤트와 관련된 우선순위를 우선순위 레코드 내에 포함하여 전송합니다. 해당 레코드의 형식은 아래에 나와 있습니다. 메타데이터 플래그 중 하나(요청 메시지의 Request Flags(요청 플래그) 필드에 포함된 비트 1, 14, 15, 20)가 설정되어 있으면 우선순위 정보가 전송됩니다. 요청 플래그, 2-12페이지의 내용을 참조하십시오. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 우선순위 레코드임을 나타내는 4입니다.

다음 표에는 각 우선순위 관련 필드에 대한 설명이 나와 있습니다.

표 3-3 우선순위 레코드 필드

필드	데이터 유형	설명
우선순위 ID	uint32	우선순위 ID 번호를 나타냅니다.
이름 길이	uint16	우선순위 이름에 포함된 바이트 수입니다.
우선순위 이름	variable	우선순위 ID에 해당하는 우선순위 이름입니다(1 - 높음, 2 - 보통, 3 - 낮음).

6.0 이상 버전용 침입 이벤트 레코드

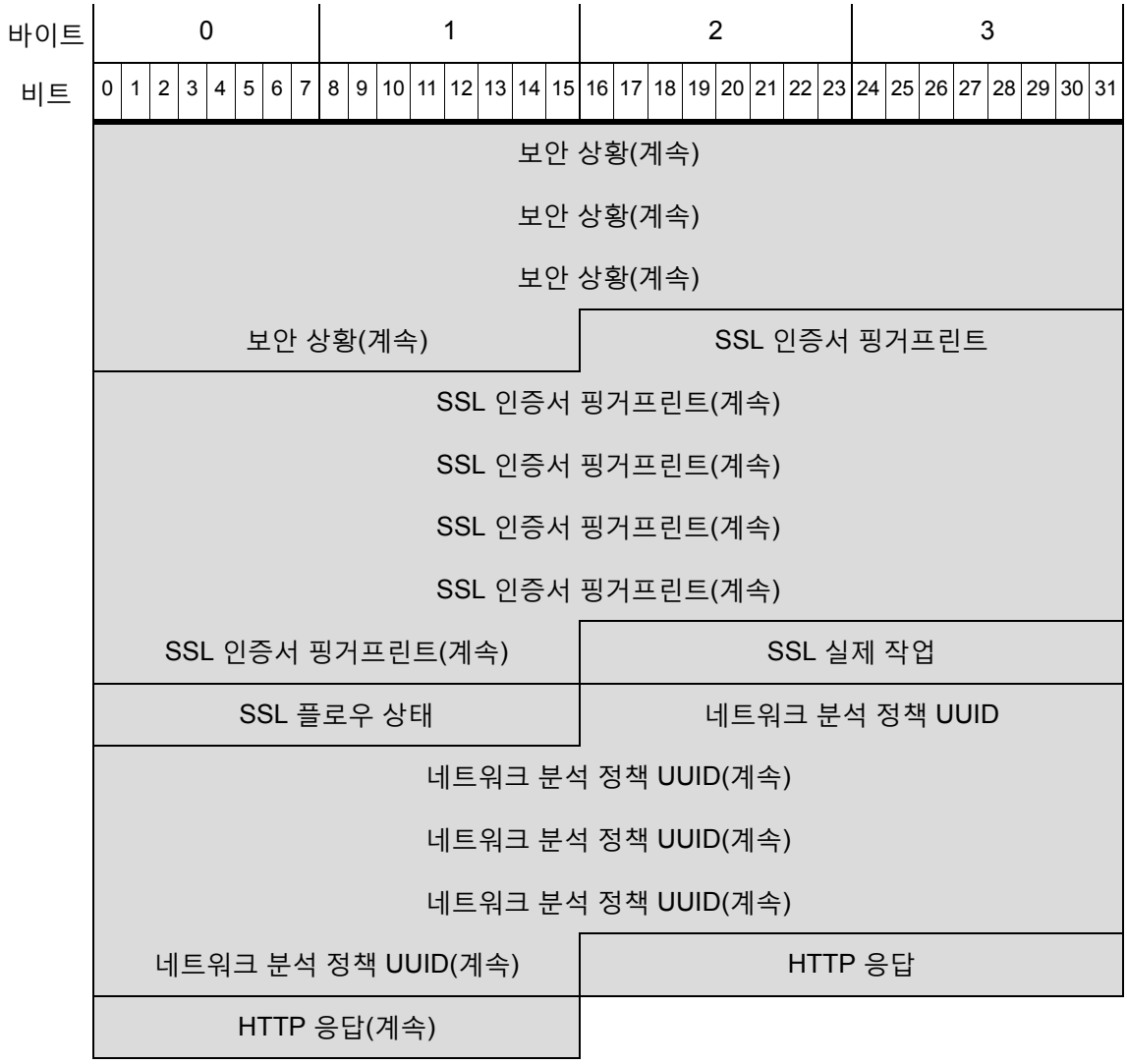
다음 그림에서 침입 이벤트 레코드의 필드는 음영으로 표시되어 있습니다. 계열 2 데이터 블록 집합에서 레코드 유형은 400이고 블록 유형은 60입니다. 이는 블록 유형 45를 대체합니다. HTTP Response(HTTP 응답) 필드가 추가되었습니다.

6.0 이상 버전의 침입 이벤트는 eStreamer에서 확장 요청을 통해서만 요청할 수 있습니다. 이렇게 하려면 스트림 요청 메시지에서 이벤트 유형 코드 12, 버전 코드 9를 요청합니다. 확장 요청 제출에 대한 자세한 정보는 확장 요청 제출, 2-4페이지의 내용을 참조하십시오.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
헤더 버전(1)																	메시지 유형(4)															
메시지 길이																																
네트워크 맵 ID																	레코드 유형(400)															
레코드 길이																																
eStreamer 서버 타임스탬프(이벤트에서 비트 23이 설정된 경우에 한함)																																
이후 사용을 위해 예약됨(이벤트에서 비트 23이 설정된 경우에 한함)																																
블록 유형(60)																																
블록 길이																																
디바이스 ID																																
이벤트 ID																																
이벤트 초																																
이벤트 마이크로초																																
규칙 ID(서명 ID)																																

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
생성자 ID																																
규칙 수정																																
분류 ID																																
우선순위 ID																																
소스 IP 주소 소스 IP 주소(계속) 소스 IP 주소(계속) 소스 IP 주소(계속)																																
대상 IP 주소 대상 IP 주소(계속) 대상 IP 주소(계속) 대상 IP 주소(계속)																																
소스 포트 또는 ICMP 유형																	대상 포트 또는 ICMP 코드														
IP 프로토콜 ID									영향 플래그								영향								차단됨							
MPLS 레이블																																
VLAN ID																	Pad															
정책 UUID 정책 UUID(계속) 정책 UUID(계속) 정책 UUID(계속)																																
사용자 ID																																
웹 애플리케이션 ID																																
클라이언트 애플리케이션 ID																																
애플리케이션 프로토콜 ID																																
액세스 제어 규칙 ID																																

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
액세스 제어 정책 UUID																																
액세스 제어 정책 UUID(계속)																																
액세스 제어 정책 UUID(계속)																																
액세스 제어 정책 UUID(계속)																																
인터페이스 인그레스 UUID																																
인터페이스 인그레스 UUID(계속)																																
인터페이스 인그레스 UUID(계속)																																
인터페이스 인그레스 UUID(계속)																																
인터페이스 이그레스(egress) UUID																																
인터페이스 이그레스(egress) UUID(계속)																																
인터페이스 이그레스(egress) UUID(계속)																																
인터페이스 이그레스(egress) UUID(계속)																																
보안 영역 인그레스 UUID																																
보안 영역 인그레스 UUID(계속)																																
보안 영역 인그레스 UUID(계속)																																
보안 영역 인그레스 UUID(계속)																																
보안 영역 이그레스(egress) UUID																																
보안 영역 이그레스(egress) UUID(계속)																																
보안 영역 이그레스(egress) UUID(계속)																																
보안 영역 이그레스(egress) UUID(계속)																																
연결 타임스탬프																																
연결 인스턴스 ID																	연결 카운터															
소스 국가																	대상 국가															
IOC 번호																	보안 상황															



다음 표에는 각 침입 이벤트 레코드 데이터 필드에 대한 설명이 나와 있습니다.

표 3-4 6.0 이상 버전용 침입 이벤트 레코드 필드

필드	데이터 유형	설명
블록 유형	unint32	침입 이벤트 데이터 블록을 시작합니다. 이 값은 항상 60입니다.
블록 길이	unint32	침입 이벤트 데이터 블록의 총 바이트 수입니다. 여기에는 침입 이벤트 블록 유형 및 길이 필드의 8바이트에 그 뒤의 데이터 바이트 수를 더한 값이 포함됩니다.
디바이스 ID	unit32	탐지 중인 매니지드 디바이스의 ID 번호를 포함합니다. 버전 3 또는 4 메타데이터를 요청하면 매니지드 디바이스 이름을 가져올 수 있습니다. 자세한 정보는 매니지드 디바이스 레코드 메타데이터, 3-35페이지의 내용을 참조하십시오.
이벤트 ID	uint32	이벤트 ID 번호입니다.

표 3-4 6.0 이상 버전용 침입 이벤트 레코드 필드 (계속)

필드	데이터 유형	설명
이벤트 초	uint32	이벤트가 탐지된 UNIX 타임스탬프(1970년 1월 1일 이후의 초 단위 시간)입니다.
이벤트 마이크로초	uint32	이벤트 탐지 타임스탬프의 마이크로초(100만분의 1초) 단위 증분 시간입니다.
규칙 ID(서명 ID)	uint32	이벤트와 일치하는 규칙 ID 번호입니다.
생성자 ID	uint32	이벤트를 생성한 Firepower System 전처리기의 ID 번호입니다.
규칙 수정	uint32	규칙 수정 번호입니다.
분류 ID	uint32	이벤트 분류 메시지의 ID 번호입니다.
우선순위 ID	uint32	이벤트와 관련된 우선순위의 ID 번호입니다.
소스 IP 주소	uint8[16]	이벤트에 사용된 소스 IPv4 또는 IPv6 주소입니다.
대상 IP 주소	uint8[16]	이벤트에 사용된 대상 IPv4 또는 IPv6 주소입니다.
소스 포트 또는 ICMP 유형	uint16	이벤트 프로토콜 유형이 TCP 또는 UDP인 경우 소스 포트 번호이거나, ICMP 트래픽에 의해 이벤트가 발생한 경우 ICMP 유형입니다.
대상 포트 또는 ICMP 코드	uint16	이벤트 프로토콜 유형이 TCP 또는 UDP인 경우 대상 포트 번호이거나, ICMP 트래픽에 의해 이벤트가 발생한 경우 ICMP 코드입니다.
IP 프로토콜 ID	uint8	IANA에서 지정한 프로토콜 번호입니다. 예를 들면 다음과 같습니다. • 0 - IP • 1 - ICMP • 6 - TCP • 17 - UDP

표 3-4 6.0 이상 버전용 침입 이벤트 레코드 필드 (계속)

필드	데이터 유형	설명
영향 플래그	bits[8]	이벤트의 영향 플래그 값입니다. 하위 8비트가 영향 레벨을 나타냅니다. 값은 다음과 같습니다. • 0x01(비트 0) - 소스 또는 대상 호스트가 시스템에서 모니터링하는 네트워크에 있습니다. • 0x02(비트 1) - 소스 또는 대상 호스트가 네트워크 맵에 있습니다. • 0x04(비트 2) - 소스 또는 대상 호스트가 이벤트의 포트에서 서버를 실행 중이거나(TCP 또는 UDP인 경우) IP 프로토콜을 사용합니다. • 0x08(비트 3) - 이벤트의 소스 또는 대상 호스트 운영 체제에 매핑된 취약점이 있습니다. • 0x10(비트 4) - 이벤트에서 탐지된 서버에 매핑된 취약점이 있습니다. • 0x20(비트 5) - 이벤트로 인해 매니지드 디바이스에서 세션이 삭제되었습니다(디바이스가 인라인, 스위치드 또는 라우티드 구축에서 실행 중인 경우에만 사용됨). Firepower System 웹 인터페이스의 차단 상태에 해당합니다. • 0x40(비트 6) - 이 이벤트를 생성한 규칙에 영향 플래그를 빨간색으로 설정하는 규칙 메타데이터가 있습니다. 소스 또는 대상 호스트가 바이러스, 트로이 목마, 기타 악성 소프트웨어에 감염되었을 가능성이 있습니다. • 0x80(비트 7) - 이벤트에서 탐지된 클라이언트에 매핑된 취약점이 있습니다. (5.0 이상 버전만 해당) 다음 영향 레벨 값은 Management Center의 특정 우선 순위에 매핑됩니다. x는 값이 0 또는 1일 수 있음을 나타냅니다. • 회색(0, 알 수 없음): 00X00000 • 빨간색(1, 취약함): XXXX1XXX, XXX1XXXX, X1XXXXXX, 1XXXXXXX (5.0 이상 버전만 해당) • 주황색(2, 잠재적으로 취약함): 00X0011X • 노란색(3, 현재 취약하지 않음): 00X0001X • 파란색(4, 알 수 없는 대상): 00X00001
영향	uint8	이벤트의 영향 플래그 값입니다. 값은 다음과 같습니다. • 1 - 빨간색(취약함) • 2 - 주황색(잠재적으로 취약함) • 3 - 노란색(현재 취약하지 않음) • 4 - 파란색(알 수 없는 대상) • 5 - 회색(알 수 없는 영향)

표 3-4 6.0 이상 버전용 침입 이벤트 레코드 필드 (계속)

필드	데이터 유형	설명
차단됨	uint8	이벤트가 차단되었는지를 나타내는 값입니다. • 0 - 차단되지 않음 • 1 - 차단 • 2 - 차단 대상이지만 컨피그레이션에서 허용하지 않음
MPLS 레이블	uint32	MPLS 레이블입니다.
VLAN ID	uint16	패킷이 생성된 VLAN의 ID를 나타냅니다.
Pad	uint16	이후 사용을 위해 예약됩니다.
정책 UUID	uint8[16]	침입 정책의 고유 식별자 역할을 하는 정책 ID 번호입니다.
사용자 ID	uint32	해당하는 경우 사용자의 내부 ID 번호입니다.
웹 애플리케이션 ID	uint32	해당하는 경우 웹 애플리케이션의 내부 ID 번호입니다.
클라이언트 애플리케이션 ID	uint32	해당하는 경우 클라이언트 애플리케이션의 내부 ID 번호입니다.
애플리케이션 프로토콜 ID	uint32	해당하는 경우 애플리케이션 프로토콜의 내부 ID 번호입니다.
액세스 제어 규칙 ID	uint32	액세스 제어 규칙의 고유 식별자 역할을 하는 규칙 ID 번호입니다.
액세스 제어 정책 UUID	uint8[16]	액세스 제어 정책의 고유 식별자 역할을 하는 정책 ID 번호입니다.
인터페이스 인그레스 UUID	uint8[16]	인그레스 인터페이스의 고유 식별자 역할을 하는 인터페이스 ID 번호입니다.
인터페이스 이그레스(egress) UUID	uint8[16]	이그레스(egress) 인터페이스의 고유 식별자 역할을 하는 인터페이스 ID 번호입니다.
보안 영역 인그레스 UUID	uint8[16]	인그레스 보안 영역의 고유 식별자 역할을 하는 영역 ID 번호입니다.
보안 영역 이그레스(egress) UUID	uint8[16]	이그레스(egress) 보안 영역의 고유 식별자 역할을 하는 영역 ID 번호입니다.
연결 타임스탬프	uint32	침입 이벤트와 관련된 연결 이벤트의 UNIX 타임스탬프(1970년 1월 1일 이후의 초 단위 시간)입니다.
연결 인스턴스 ID	uint16	연결 이벤트를 생성한 매니지드 디바이스에 있는 Snort 인스턴스의 숫자 ID입니다.
연결 카운터	uint16	1초 이내에 발생하는 연결 이벤트를 구별하는 데 사용되는 값입니다.
소스 국가	uint16	소스 호스트의 국가 코드입니다.
대상 국가	uint16	대상 호스트의 국가 코드입니다.
IOC 번호	uint16	이 이벤트와 관련된 보안 침해의 ID 번호입니다.

표 3-4 6.0 이상 버전용 침입 이벤트 레코드 필드 (계속)

필드	데이터 유형	설명
보안 상황	uint8[16]	트래픽이 통과한 보안 상황(가상 방화벽)의 ID 번호입니다. 이 필드는 다중 컨텍스트 모드의 ASA FirePOWER 디바이스에 대해서만 채워집니다.
SSL 인증서 핑거프린트	uint8[20]	SSL 서버 인증서의 SHA1 해시입니다.
SSL 실제 작업	uint16	SSL 규칙에 기반한 연결에서 수행된 작업입니다. 규칙에 명시된 작업이 가능하지 않을 수도 있으므로, 이는 예상 작업과 다를 수 있습니다. 가능한 값은 다음과 같습니다. • 0 - '알 수 없음' • 1 - '암호 해독 안 함' • 2 - '차단' • 3 - '차단 및 재설정' • 4 - '암호 해독(알려진 키)' • 5 - '암호 해독(키 교체)' • 6 - '암호 해독(재서명)'

표 3-4 6.0 이상 버전용 침입 이벤트 레코드 필드 (계속)

필드	데이터 유형	설명
SSL 플로우 상태	uint16	SSL 플로우의 상태입니다. 이 값은 작업을 수행한 이유 또는 오류 메시지가 표시된 이유를 설명합니다. 가능한 값은 다음과 같습니다. • 0 - '알 수 없음' • 1 - '일치하지 않음' • 2 - '성공' • 3 - '캐시되지 않은 세션' • 4 - '알 수 없는 암호 그룹' • 5 - '지원되지 않는 암호 그룹' • 6 - '지원되지 않는 SSL 버전' • 7 - 'SSL 압축 사용됨' • 8 - '패시브 모드에서 세션 암호 해독 불가' • 9 - '핸드셰이크 오류' • 10 - '암호 해독 오류' • 11 - '서버 이름 카테고리 조회 보류 중' • 12 - '공용 이름 카테고리 조회 보류 중' • 13 - '내부 오류' • 14 - '네트워크 파라미터 사용 불가' • 15 - '유효하지 않은 서버 인증서 핸들' • 16 - '서버 인증서 핑거프린트 사용 불가' • 17 - '주체 DN을 캐시할 수 없음' • 18 - '발급자 DN을 캐시할 수 없음' • 19 - '알 수 없는 SSL 버전' • 20 - '외부 인증서 목록 사용 불가' • 21 - '외부 인증서 핑거프린트 사용 불가' • 22 - '내부 인증서 목록이 유효하지 않음' • 23 - '내부 인증서 목록 사용 불가' • 24 - '내부 인증서 사용 불가' • 25 - '내부 인증서 핑거프린트 사용 불가' • 26 - '서버 인증서 검증 사용 불가' • 27 - '서버 인증서 검증 장애' • 28 - '유효하지 않은 작업'
네트워크 분석 정책 UUID	uint8[16]	침입 이벤트를 생성한 네트워크 분석 정책의 UUID입니다.
HTTP 응답	uint32	HTTP 요청의 응답 코드입니다.

5.3 이상 버전용 침입 영향 알림 데이터

5.3 이상 버전용 침입 영향 알림 이벤트에는 영향 이벤트에 대한 정보가 포함됩니다. 침입 이벤트를 시스템 네트워크 맵 데이터에 비교하여 영향을 확인할 때 이 이벤트가 전송됩니다. 이 이벤트는 레코드 유형이 9인 표준 레코드 헤더를 사용하며, 그 뒤에는 계열 1 블록 그룹에서 계열 1 데이터 블록 유형이 153인 침입 영향 알림 데이터 블록이 옵니다. 영향 알림 데이터 블록은 계열 1 데이터 블록 유형입니다. 계열 1 데이터 블록에 대한 자세한 정보는 검색(계열 1) 블록 이해, 4-63페이지의 내용을 참조하십시오.

요청 메시지의 Flags(플래그) 필드에서 비트 5를 설정해야 eStreamer에서 침입 영향 이벤트를 전송하도록 요청할 수 있습니다. 요청 메시지에 대한 자세한 정보는 이벤트 스트림 요청 메시지 형식, 2-10페이지의 내용을 참조하십시오. 이러한 경고의 버전 1은 IPv4만 처리합니다. 5.3에 도입된 버전 2는 IPv4와 함께 IPv6 이벤트도 처리합니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
헤더 버전(1)																	메시지 유형(4)															
메시지 길이																																
네트워크 맵 ID																	레코드 유형(9)															
eStreamer 서버 타임스탬프(이벤트에서 비트 23이 설정된 경우에 한함)																																
이후 사용을 위해 예약됨(이벤트에서 비트 23이 설정된 경우에 한함)																																
침입 영향 알림 블록 유형(153)																																
침입 영향 알림 블록 길이																																
이벤트 ID																																
디바이스 ID																																
이벤트 초																																
영향																																
소스 IP 주소 소스 IP 주소(계속) 소스 IP 주소(계속) 소스 IP 주소(계속)																																
대상 IP 주소 대상 IP 주소(계속)																																

다음 표에는 영향 이벤트의 각 데이터 필드에 대한 설명이 나와 있습니다.

표 3-5 영향 이벤트 데이터 필드

필드	데이터 유형	설명
침입 영향 알림 블록 유형	uint32	침입 영향 알림 데이터 블록이 뒤에 옴을 나타냅니다. 이 필드의 값은 항상 153입니다. 침입 이벤트 및 메타 데이터 레코드 유형, 3-1페이지의 내용을 참조하십시오.
침입 영향 알림 블록 길이	uint32	침입 영향 알림 데이터 블록의 길이를 나타냅니다. 여기에는 해당 블록 뒤에 오는 모든 데이터와 침입 영향 알림 블록 유형 및 길이의 8바이트가 포함됩니다.
이벤트 ID	uint32	이벤트 ID 번호를 나타냅니다.
디바이스 ID	uint32	매니지드 디바이스 ID 번호를 나타냅니다.
이벤트 초	uint32	이벤트가 탐지된 초 단위 시간(1970년 1월 1일 이후)을 나타냅니다.

표 3-5 영향 이벤트 데이터 필드 (계속)

필드	데이터 유형	설명
영향	bits[8]	이벤트의 영향 플래그 값입니다. 하위 8비트가 영향 레벨을 나타냅니다. 값은 다음과 같습니다. • 0x01(비트 0) - 소스 또는 대상 호스트가 시스템에서 모니터링하는 네트워크에 있습니다. • 0x02(비트 1) - 소스 또는 대상 호스트가 네트워크 맵에 있습니다. • 0x04(비트 2) - 소스 또는 대상 호스트가 이벤트의 포트에서 서버를 실행 중이거나(TCP 또는 UDP인 경우) IP 프로토콜을 사용합니다. • 0x08(비트 3) - 이벤트의 소스 또는 대상 호스트 운영 체제에 매핑된 취약점이 있습니다. • 0x10(비트 4) - 이벤트에서 탐지된 서버에 매핑된 취약점이 있습니다. • 0x20(비트 5) - 이벤트로 인해 매니지드 디바이스에서 세션이 삭제되었습니다(디바이스가 인라인, 스위치드 또는 라우티드 구축에서 실행 중인 경우에만 사용됨). Firepower System 웹 인터페이스의 차단 상태에 해당합니다. • 0x40(비트 6) - 이 이벤트를 생성한 규칙에 영향 플래그를 빨간색으로 설정하는 규칙 메타데이터가 있습니다. 소스 또는 대상 호스트가 바이러스, 트로이 목마, 기타 악성 소프트웨어에 감염되었을 가능성이 있습니다. • 0x80(비트 7) - 이벤트에서 탐지된 클라이언트에 매핑된 취약점이 있습니다. (5.0 이상 버전만 해당) 다음 영향 레벨 값은 Management Center의 특정 우선 순위에 매핑됩니다. x는 값이 0 또는 1일 수 있음을 나타냅니다. • 회색(0, 알 수 없음): 00X00000 • 빨간색(1, 취약함): xxxx1xxx, xxx1xxxx, x1xxxxxx, 1xxxxxxx (5.0 이상 버전만 해당) • 주황색(2, 잠재적으로 취약함): 00X0011X • 황색(3, 현재 취약하지 않음): 00X0001X • 파란색(4, 알 수 없는 대상): 00X00001
소스 IP 주소	uint8[16]	영향 이벤트와 관련된 호스트의 IP 주소입니다. IPv4 또는 IPv6 주소를 포함할 수 있습니다. 자세한 정보는 IP 주소, 1-5페이지의 내용을 참조하십시오.
대상 IP 주소	uint8[16]	해당하는 경우 영향 이벤트와 관련된 호스트의 대상 IP 주소입니다. IPv4 또는 IPv6 주소를 포함할 수 있습니다. 자세한 정보는 IP 주소, 1-5페이지의 내용을 참조하십시오. 대상 IP 주소가 없으면 이 값은 0입니다.
문자열 블록 유형	uint32	영향 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0으로 설정됩니다. 문자열 블록에 대한 자세한 정보는 문자열 데이터 블록, 4-72페이지의 내용을 참조하십시오.

표 3-5 영향 이벤트 데이터 필드 (계속)

필드	데이터 유형	설명
문자열 블록 길이	uint32	이벤트 설명 문자열 블록의 바이트 수입니다. 여기에는 문자열 블록 유형의 4바이트 + 문자열 블록 길이의 4바이트 + 설명의 바이트 수가 포함됩니다.
설명	string	영향 이벤트의 설명입니다.

사용자 레코드

메타데이터를 요청할 때는 Firepower System의 구성 요소가 생성하는 이벤트에서 참조되는 사용자에 대한 정보를 검색할 수 있습니다. eStreamer 서비스는 이벤트에 대한 사용자 정보가 포함된 메타데이터를 사용자 레코드 내에 포함하여 전송합니다. 해당 레코드의 형식은 아래에 나와 있습니다. 사용자 레코드는 사용자 ID와 그에 해당하는 이름을 포함합니다. 사용자 메타데이터 레코드를 사용하면 사용자 ID 값과 메타데이터 간의 상관관계를 지정하여 이벤트와 관련된 사용자 이름을 확인할 수 있습니다. 메타데이터 플래그 중 하나(요청 메시지의 Request Flags(요청 플래그) 필드에 포함된 비트 1, 14, 15, 20)가 설정되어 있으면 사용자 정보가 전송됩니다. 요청 플래그, 2-12페이지의 내용을 참조하십시오.

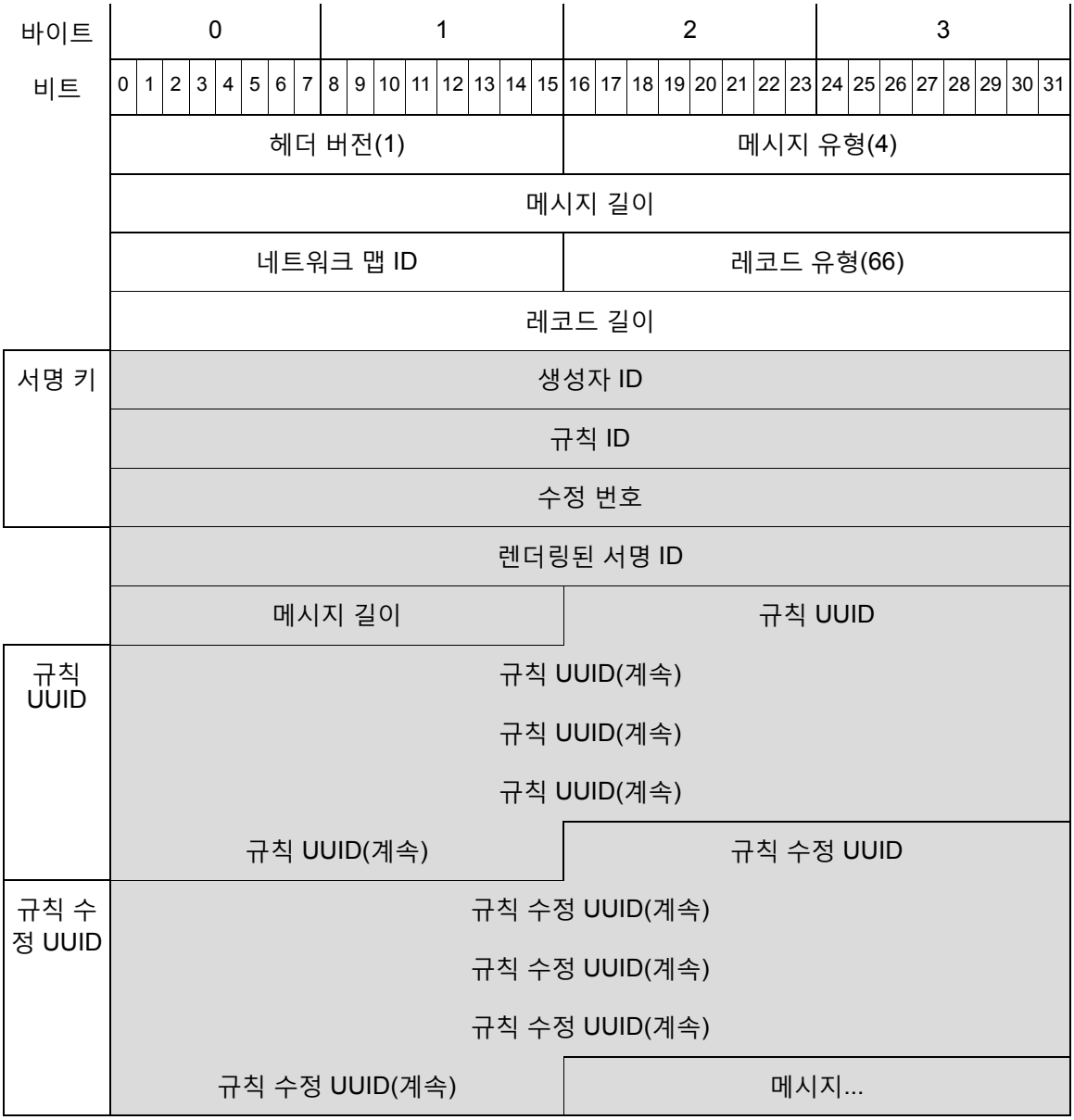
다음 표에는 사용자 레코드의 필드에 대한 설명이 나와 있습니다.

표 3-6 사용자 레코드 필드

필드	데이터 유형	설명
사용자 ID	uint32	사용자 ID 번호입니다. 이 필드는 이 레코드의 고유 키입니다.
이름 길이	uint32	사용자 이름에 포함된 바이트 수입니다.
이름	string	사용자의 이름입니다.

4.6.1 이상 버전용 규칙 메시지 레코드

이벤트에 대한 규칙 메시지 정보는 규칙 메시지 레코드 내에 포함되어 전송됩니다. 해당 레코드의 형식은 아래에 나와 있습니다. 버전 2 또는 버전 3 메타데이터를 요청하면 eStreamer 서비스가 4.6.1 이상 버전용 규칙 메시지 레코드를 전송합니다. 4.6.1 이상 버전용 규칙 메시지 레코드에는 4.6 이하 버전용 규칙 메시지 레코드와 같은 필드가 포함되어 있으며 새 UUID 및 수정 UUID 필드도 포함되어 있습니다. 해당하는 메타데이터 플래그(요청 메시지의 Request Flags(요청 플래그) 필드에 포함된 비트 14(버전 2), 비트 15(버전 3) 또는 비트 20(버전 4))가 설정되어 있으면 버전 2, 버전 3 또는 버전 4 메타데이터 정보가 전송됩니다. 요청 플래그, 2-12페이지의 내용을 참조하십시오. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 규칙 메시지 버전 2 레코드임을 나타내는 66입니다.



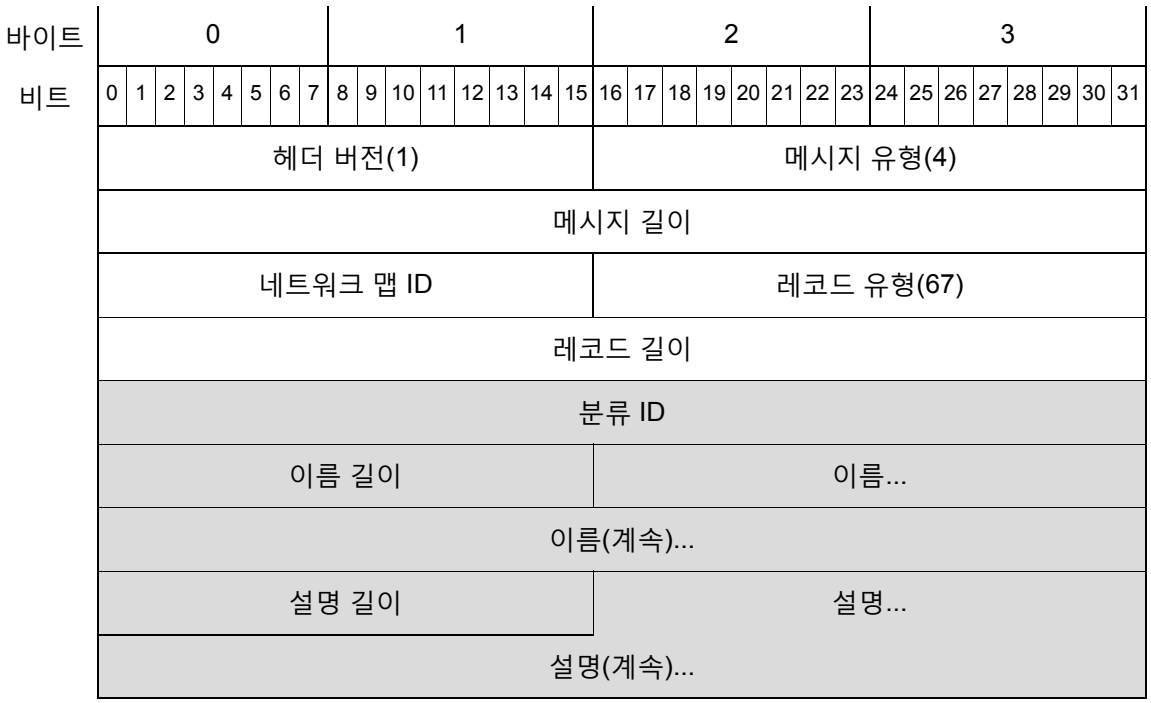
다음 표에는 각 규칙 관련 필드에 대한 설명이 나와 있습니다.

표 3-7 규칙 메시지 레코드 필드

필드	데이터 유형	설명
생성자 ID	uint32	생성기 ID 번호입니다.
규칙 ID	uint32	로컬 컴퓨터의 규칙 ID 번호입니다.
규칙 수정	uint32	규칙 수정 번호입니다. 현재 이 번호는 모든 규칙 메시지에 대해 0으로 설정됩니다.
렌더링된 서명 ID	uint32	Firepower System 인터페이스에 렌더링된 규칙 ID 번호입니다.
메시지 길이	uint16	규칙 텍스트에 포함된 바이트 수입니다.
UUID	uint8[16]	규칙의 고유 식별자 역할을 하는 규칙 ID 번호입니다.
수정 UUID	uint8[16]	수정의 고유 식별자 역할을 하는 규칙 수정 ID 번호입니다.
메시지	variable	이벤트를 트리거한 규칙 메시지입니다.

4.6.1 이상 버전용 분류 레코드

eStreamer 서비스는 이벤트에 대한 분류 정보를 4.6.1 이상 버전용 분류 레코드 내에 포함하여 전송합니다. 해당 레코드의 형식은 아래에 나와 있습니다. 4.6.1 이상 버전용 분류 레코드에는 4.6 이하 버전용 분류 레코드와 같은 필드가 포함되어 있으며 새 UUID 및 수정 UUID 필드도 포함되어 있습니다. 버전 3 또는 버전 4 메타데이터 플래그(요청 메시지의 Request Flags(요청 플래그) 필드에 포함된 비트 15 또는 20)가 설정되어 있으면 분류 정보가 전송됩니다. 요청 플래그, 2-12페이지의 내용을 참조하십시오. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 분류 버전 2 레코드임을 나타내는 67입니다.



바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
분류 UUID	분류 UUID 분류 UUID(계속) 분류 UUID(계속) 분류 UUID(계속)																															
분류 수정 UUID	분류 수정 UUID 분류 수정 UUID(계속) 분류 수정 UUID(계속) 분류 수정 UUID(계속)																															

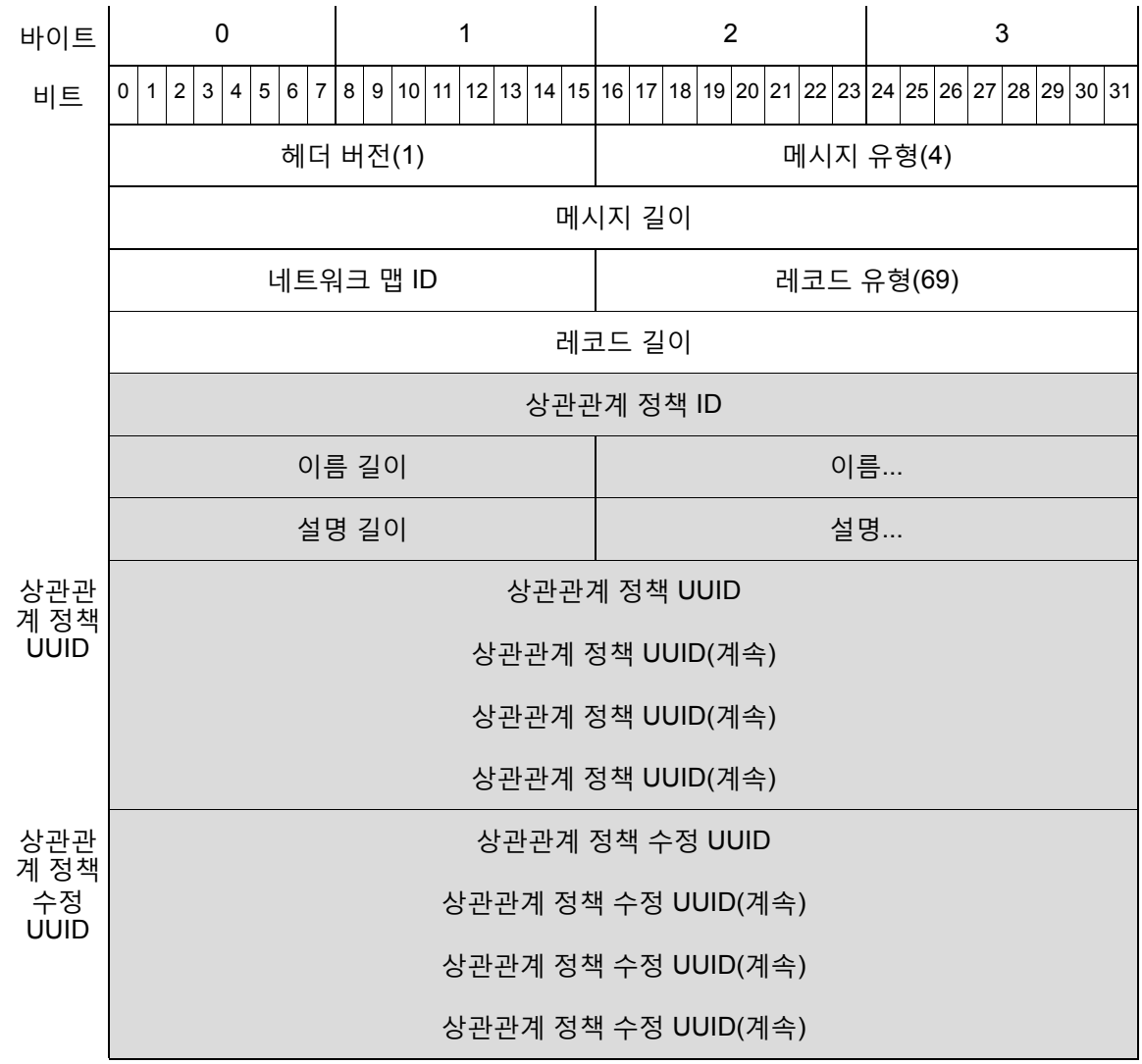
다음 표에는 분류 레코드의 필드에 대한 설명이 나와 있습니다.

표 3-8 분류 레코드 필드

필드	데이터 유형	설명
분류 ID	uint32	분류 ID 번호입니다.
이름 길이	uint16	이름에 포함된 바이트 수입니다.
이름	string	분류 이름입니다.
설명 길이	uint16	설명에 포함된 바이트 수입니다.
설명	string	분류 설명입니다.
UUID	uint8[16]	분류의 고유 식별자 역할을 하는 분류 ID 번호입니다.
수정 UUID	uint8[16]	분류 수정의 고유 식별자 역할을 하는 분류 수정 ID 번호입니다.

상관관계 정책 레코드

eStreamer 서비스는 상관관계 이벤트의 상관관계 정책이 포함된 메타데이터를 상관관계 정책 레코드 내에 포함하여 전송합니다. 해당 레코드의 형식은 아래에 나와 있습니다. 버전 3 또는 버전 4 메타데이터 플래그(요청 메시지의 Request Flags(요청 플래그) 필드에 포함된 비트 15 또는 20)가 설정되어 있으면 상관관계 정책 정보가 전송됩니다. 요청 플래그, 2-12페이지의 내용을 참조하십시오. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 상관관계 정책 레코드임을 나타내는 69입니다.



다음 표에는 상관관계 정책 레코드의 필드에 대한 설명이 나와 있습니다.

표 3-9 상관관계 정책 레코드 필드

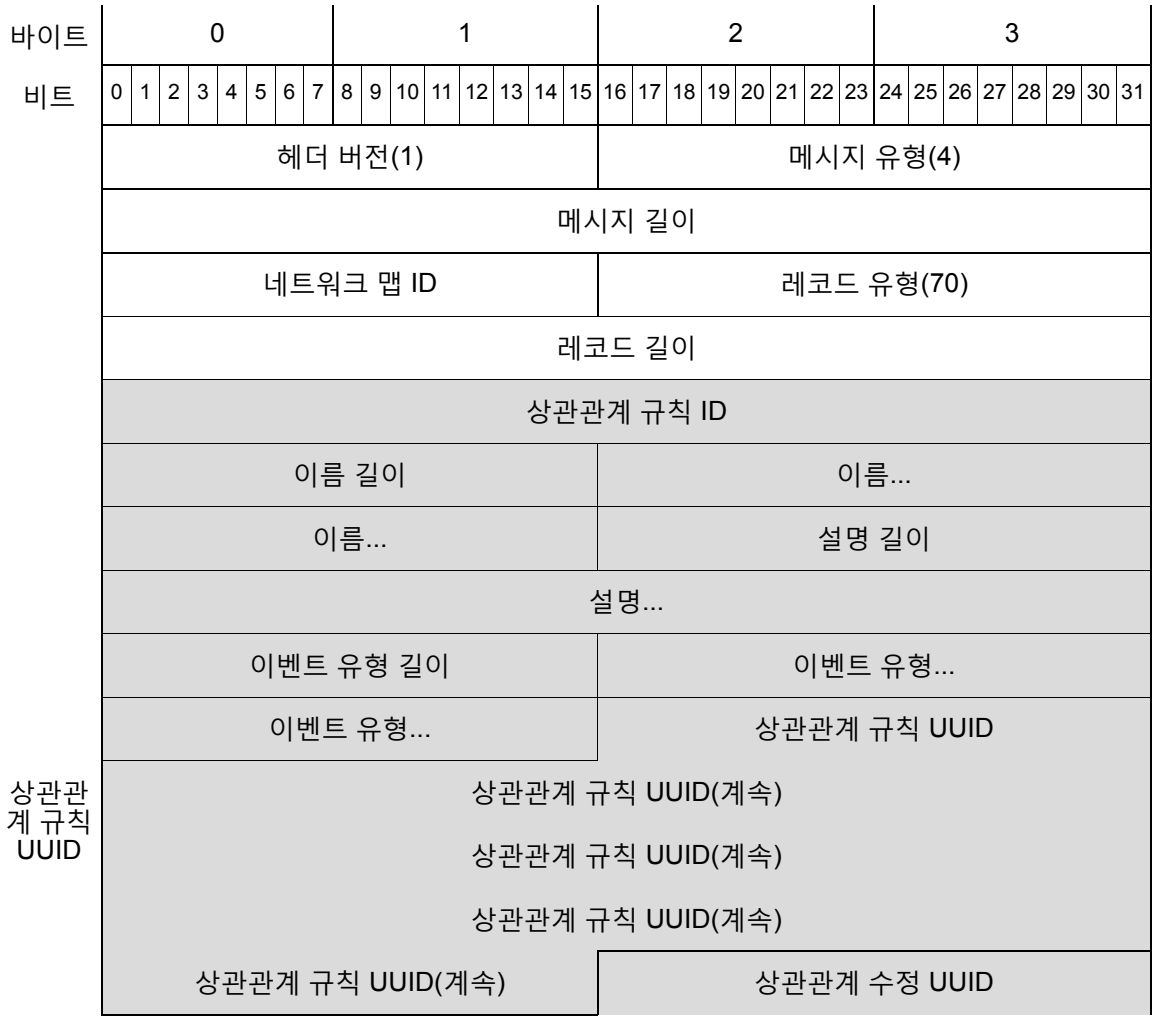
필드	데이터 유형	설명
상관관계 정책 ID	uint32	상관관계 정책 ID 번호입니다. 이 필드는 이 레코드의 고유 키입니다.
이름 길이	uint16	상관관계 정책 이름에 포함된 바이트 수입니다.
이름	string	이벤트를 트리거한 상관관계 정책의 이름입니다.
설명 길이	uint16	상관관계 정책 설명에 포함된 바이트 수입니다.
설명	string	이벤트를 트리거한 상관관계 정책의 설명입니다.

표 3-9 상관관계 정책 레코드 필드 (계속)

필드	데이터 유형	설명
UUID	uint8[16]	상관관계 정책의 고유 식별자 역할을 하는 상관관계 정책 ID 번호입니다.
수정 UUID	uint8[16]	상관관계 정책의 고유 식별자 역할을 하는 상관관계 정책 수정 ID 번호입니다.

상관관계 규칙 레코드

eStreamer 서비스는 상관관계 이벤트를 트리거한 상관관계 규칙에 대한 정보가 포함된 메타데이터를 상관관계 규칙 레코드 내에 포함하여 전송합니다. 해당 레코드의 형식은 아래에 나와 있습니다. 버전 3 또는 버전 4 메타데이터 플래그(요청 메시지의 Request Flags(요청 플래그) 필드에 포함된 비트 15 또는 20)가 설정되어 있으면 상관관계 규칙 정보가 전송됩니다. 요청 플래그, 2-12페이지의 내용을 참조하십시오. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 상관관계 규칙 레코드임을 나타내는 70입니다.



다음 표에는 상관관계 규칙 레코드의 필드에 대한 설명이 나와 있습니다.

표 3-10 상관관계 규칙 레코드 필드

필드	데이터 유형	설명
상관관계 규칙 ID	uint32	상관관계 규칙 ID 번호입니다. 이 필드는 이 레코드의 고유 키입니다.
이름 길이	uint16	상관관계 규칙 이름에 포함된 바이트 수입니다.
이름	string	이벤트를 트리거한 상관관계 규칙의 이름입니다.
설명 길이	uint16	상관관계 규칙 설명에 포함된 바이트 수입니다.
설명	string	이벤트를 트리거한 상관관계 규칙의 설명입니다.
이벤트 유형 길이	uint16	이벤트 유형 설명에 포함된 바이트 수입니다.
이벤트 유형	string	상관관계 규칙을 트리거한 이벤트의 설명입니다.
UUID	uint8[16]	상관관계 규칙의 고유 식별자 역할을 하는 상관관계 규칙 ID 번호입니다.
수정 UUID	uint8[16]	상관관계 규칙 수정의 고유 식별자 역할을 하는 상관관계 규칙 수정 ID 번호입니다.
화이트리스트 UUID	uint8[16]	화이트리스트 위반 결과로 전송된 이벤트에 대한 고유 식별자 역할을 하는 상관관계 ID 번호입니다.

침입 이벤트 추가 데이터 레코드

eStreamer 서비스는 침입 이벤트와 관련된 이벤트 추가 데이터를 침입 이벤트 추가 데이터 레코드 내에 포함하여 전송합니다. 레코드 유형은 항상 110입니다.

이벤트 추가 데이터는 캡슐화된 이벤트 추가 데이터 데이터 블록에 표시됩니다. 이 블록의 데이터 블록 유형 값은 항상 4입니다. 이벤트 추가 데이터 데이터 블록은 계열 2 데이터 블록입니다. 계열 2 데이터 블록에 대한 자세한 정보는 계열 2 데이터 블록 이해, 3-57페이지의 내용을 참조하십시오.

지원되는 추가 데이터 유형에는 IPv6 소스 및 대상 주소와 HTTP 프록시 또는 로드 밸런서를 통해 웹 서버에 연결하는 클라이언트의 원래 IP 주소(v4 또는 v6)가 포함됩니다. 아래 그림에 침입 이벤트 추가 데이터 레코드의 형식이 나와 있습니다.

요청 메시지의 Request Flags(요청 플래그) 필드에 비트 27이 설정되어 있으면 각 침입 이벤트에 대해 이벤트 추가 데이터가 수신됩니다. 비트 20을 설정하는 경우에는 침입 이벤트 추가 데이터 메타데이터, 3-28페이지에 설명되어 있는 이벤트 추가 데이터 메타데이터도 수신됩니다. 비트 23을 활성화하면 eStreamer는 확장 이벤트 헤더를 포함합니다. 요청 플래그 설정에 대한 자세한 정보는 요청 플래그, 2-12페이지의 내용을 참조하십시오.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
헤더 버전(1)																	메시지 유형(4)															
메시지 길이																																
네트워크 맵 ID																	레코드 유형(110)															
레코드 길이																																
eStreamer 서버 타임스탬프(이벤트에서 비트 23이 설정된 경우에 한함)																																
이후 사용을 위해 예약됨(이벤트에서 비트 23이 설정된 경우에 한함)																																
이벤트 추가 데이터 데이터 블록 유형(4)																																
이벤트 추가 데이터 데이터 블록 길이																																
디바이스 ID																																
이벤트 ID																																
이벤트 초																																
유형																																
BLOB 블록 유형(1)																																
BLOB 길이																																
이벤트 추가 데이터																																

이벤트 추가 데이터 블록 구조에는 Firepower System 버전 4.10에 도입된 여러 가변 길이 데이터 구조 중 하나인 BLOB 블록 유형이 포함됩니다.

다음 표에는 침입 이벤트 추가 데이터 레코드의 필드에 대한 설명이 나와 있습니다.

표 3-11 침입 이벤트 추가 데이터 데이터 블록 필드

필드	데이터 유형	설명
이벤트추가데이터 데이터 블록 유형	uint32	이벤트 추가 데이터 데이터 블록을 시작합니다. 이 값은 항상 4입니다. 블록 유형은 계열 2 블록입니다. 자세한 정보는 계열 2 데이터 블록 이해, 3-57페이지의 내용을 참조하십시오.
이벤트추가데이터 데이터 블록 길이	uint32	데이터 블록의 길이입니다. 데이터 바이트 수에 2개 데이터 블록 헤더 필드의 8바이트를 더한 길이입니다.
디바이스 ID	uint32	매니지드 디바이스 ID 번호입니다.
이벤트 ID	uint32	이벤트 ID 번호입니다.
이벤트 초	uint32	이벤트의 UNIX 타임스탬프(1970년 1월 1일 이후의 초 단위 시간)입니다.
유형	uint32	추가 데이터 유형에 대한 식별자입니다. 예를 들면 다음과 같습니다. • 2 - XFF 클라이언트(IPv6) • 9 - HTTP URI
BLOB 블록 유형	uint32	추가 데이터를 포함하는 BLOB 데이터 블록을 시작합니다. 이 값은 항상 1입니다. 블록 유형은 계열 2 블록입니다.
길이	uint32	BLOB 데이터 블록의 총 바이트 수입니다.
추가 데이터	variable	추가 데이터의 콘텐츠입니다. 데이터 유형은 Type(유형) 필드에 표시됩니다.

침입 이벤트 추가 데이터 메타데이터

eStreamer 서비스는 침입 이벤트 추가 데이터 레코드와 관련된 이벤트 추가 데이터 메타데이터를 침입 이벤트 추가 데이터 메타데이터 레코드 내에 포함하여 전송합니다. 레코드 유형은 항상 111입니다.

이벤트 추가 데이터 메타데이터는 캡슐화된 이벤트 추가 데이터 메타데이터 데이터 블록에 표시됩니다. 이 블록의 데이터 블록 유형 값은 항상 5입니다. 이벤트 추가 데이터 데이터 블록은 계열 2 데이터 블록입니다.

요청 메시지의 Request Flags(요청 플래그) 필드에 비트 20이 설정되어 있으면 이벤트 추가 데이터 메타데이터가 수신됩니다. 침입 이벤트와 이벤트 추가 데이터 메타데이터를 모두 수신하려면 비트 2도 설정해야 합니다. 요청 플래그, 2-12페이지의 내용을 참조하십시오. 비트 23을 활성화하면 레코드에 확장 이벤트 헤더가 포함됩니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
헤더 버전(1)																	메시지 유형(4)															
메시지 길이																																
네트워크 맵 ID																	레코드 유형(111)															
레코드 길이																																
eStreamer 서버 타임스탬프(이벤트에서 비트 23이 설정된 경우에 한함)																																
이후 사용을 위해 예약됨(이벤트에서 비트 23이 설정된 경우에 한함)																																
이벤트 추가 데이터 메타데이터 데이터 블록 유형(5)																																
데이터 블록 길이																																
유형																																
문자열 블록 유형(0)																																
문자열 블록 길이																																
이름...																																
문자열 블록 유형(0)																																
문자열 블록 길이																																
인코딩																																

블록 구조에는 Firepower System 버전 4.10에 도입된 여러 계열 2 가변 길이 데이터 구조 중 하나인 캡슐화된 문자열 블록 유형이 포함됩니다.

다음 표에는 이벤트 추가 데이터 메타데이터 레코드의 필드에 대한 설명이 나와 있습니다.

표 3-12 이벤트 추가 데이터 메타데이터 데이터 블록 필드

필드	데이터 유형	설명
이벤트 추가 데이터 메타데이터 데이터 블록 유형	uint32	이벤트 추가 데이터 메타데이터 데이터 블록을 시작합니다. 이 값은 항상 5입니다. 이 블록 유형은 계열 2 블록입니다.
이벤트 추가 데이터 메타데이터 데이터 블록 길이	uint32	데이터 블록의 길이입니다. 데이터 바이트 수에 2개 데이터 블록 헤더 필드의 8바이트를 더한 길이입니다.

표 3-12 이벤트 추가 데이터 메타데이터 데이터 블록 필드 (계속)

필드	데이터 유형	설명
유형	uint32	추가 데이터의 유형입니다. 관련된 이벤트 추가 데이터 레코드의 Type(유형) 필드와 일치합니다. 이 필드는 이 레코드의 고유 키입니다.
문자열 블록 유형	uint32	클라이언트 애플리케이션 버전에 대한 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다. 이 블록 유형은 계열 2 블록입니다.
문자열 블록 길이	uint32	클라이언트 애플리케이션 버전 문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이 필드의 8바이트에 버전 문자열의 바이트 수를 더한 값이 포함됩니다.
이름	string	XFF 클라이언트(IPv6) 및 HTTP URI와 같은 이벤트 추가 데이터의 유형 이름입니다.
문자열 블록 유형	uint32	클라이언트 애플리케이션 URL에 대한 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다. 이 블록 유형은 계열 2 블록입니다.
문자열 블록 길이	uint32	클라이언트 애플리케이션 URL 문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이 필드의 8바이트에 URL 문자열의 바이트 수를 더한 값이 포함됩니다.
인코딩	string	IPv4, IPv6 문자열 등 이벤트 추가 데이터에 사용되는 인코딩입니다.

보안 영역 이름 레코드

eStreamer 서비스는 침입 이벤트 또는 연결 이벤트와 관련된 보안 영역 이름에 대한 정보를 포함하는 메타데이터를 보안 영역 이름 레코드 내에 포함하여 전송합니다. 해당 레코드의 형식은 아래에 나와 있습니다. 버전 4 메타데이터 플래그(요청 메시지의 Request Flags(요청 플래그) 필드에 포함된 비트 20)가 설정되어 있으면 보안 영역 정보가 전송됩니다. 요청 플래그, 2-12페이지의 내용을 참조하십시오. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 보안 영역 이름 레코드임을 나타내는 115입니다. 이 필드에는 UUID 문자열 데이터 블록(계열 2 데이터 블록 집합 내 블록 유형 14)이 포함됩니다.

다음 표에는 보안 영역 이름 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 3-13 보안 영역 이름 데이터 블록 필드

필드	데이터 유형	설명
보안 영역 이름 데이터 블록 유형	uint32	보안 영역 이름 데이터 블록을 시작합니다. 이 값은 항상 14입니다. 블록 유형은 계열 2 블록입니다.
보안 영역 이름 데이터 블록 길이	uint32	데이터 블록의 길이입니다. 데이터 바이트 수에 2개 데이터 블록 헤더 필드의 8바이트를 더한 길이입니다.
보안 영역 UUID	uint8[16]	연결 이벤트와 관련된 보안 영역의 고유 식별자입니다. 이 필드는 이 레코드의 고유 키입니다.
문자열 블록 유형	uint32	보안 영역의 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	보안 영역 이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 이름의 바이트 수를 더한 값이 포함됩니다.
보안 영역 이름	string	보안 영역 이름입니다.

인터페이스 이름 레코드

eStreamer 서비스는 침입 이벤트 또는 연결 이벤트와 관련된 인터페이스 이름에 대한 정보를 포함하는 메타데이터를 인터페이스 이름 레코드 내에 포함하여 전송합니다. 해당 레코드의 형식은 아래에 나와 있습니다. 버전 4 메타데이터 플래그(요청 메시지의 Request Flags(요청 플래그) 필드에 포함된 비트 20)가 설정되어 있으면 인터페이스 이름 정보가 전송됩니다. 요청 플래그, 2-12페이지의 내용을 참조하십시오. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 인터페이스 이름 레코드임을 나타내는 116입니다. 이 필드에는 UUID 문자열 데이터 블록(계열 2 데이터 블록 집합 내 블록 유형 14)이 포함됩니다.

다음 표에는 인터페이스 이름 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 3-14 인터페이스 이름 데이터 블록 필드

필드	데이터 유형	설명
인터페이스 이름 데이터 블록 유형	uint32	인터페이스 이름 데이터 블록을 시작합니다. 이 값은 항상 14입니다. 블록 유형은 계열 2 블록입니다.
인터페이스 이름 데이터 블록 길이	uint32	데이터 블록의 길이입니다. 데이터 바이트 수에 2개 데이터 블록 헤더 필드의 8바이트를 더한 길이입니다.
인터페이스 UUID	uint8[16]	연결 이벤트와 관련된 인터페이스의 고유 식별자 역할을 하는 인터페이스 ID 번호입니다. 이 필드는 이 레코드의 고유 키입니다.
문자열 블록 유형	uint32	인터페이스의 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	인터페이스 이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 인터페이스 이름의 바이트 수를 더한 값이 포함됩니다.
인터페이스 이름	string	인터페이스 이름입니다.

액세스 제어 정책 이름 레코드

eStreamer 서비스는 침입 이벤트 또는 연결 이벤트를 트리거한 액세스 제어 정책의 이름에 대한 메타데이터를 액세스 제어 정책 이름 레코드 내에 포함하여 전송합니다. 해당 레코드의 형식은 아래에 나와 있습니다. 버전 4 메타데이터 플래그(요청 메시지의 Request Flags(요청 플래그) 필드에 포함된 비트 20)가 설정되어 있으면 액세스 제어 정책 이름 정보가 전송됩니다. 요청 플래그, 2-12페이지의 내용을 참조하십시오. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 액세스 제어 정책 이름 레코드임을 나타내는 117입니다. 이 필드에는 UUID 문자열 데이터 블록(계열 2 데이터 블록 집합 내 블록 유형 14)이 포함됩니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
헤더 버전(1)																	메시지 유형(4)															
메시지 길이																																
네트워크 맵 ID																	레코드 유형(117)															
레코드 길이																																
액세스 제어 정책 이름 데이터 블록(14)																																
액세스 제어 정책 이름 데이터 블록 길이																																
액세스 제어 정책 UUID																																
문자열 블록 유형(0)																																
문자열 블록 길이																																
액세스 제어 정책 이름...																																

다음 표에는 액세스 제어 정책 이름 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 3-15 액세스 제어 정책 이름 데이터 블록 필드

필드	데이터 유형	설명
액세스 제어 정책 이름 데이터 블록 유형	uint32	액세스 제어 정책 이름 데이터 블록을 시작합니다. 이 값은 항상 14입니다. 블록 유형은 계열 2 블록입니다.
액세스 제어 정책 이름 데이터 블록 길이	uint32	데이터 블록의 길이입니다. 데이터 바이트 수에 2개 데이터 블록 헤더 필드의 8바이트를 더한 길이입니다.
액세스 제어 정책 UUID	uint8[16]	침입 이벤트 또는 연결 이벤트와 관련된 액세스 제어 정책의 고유 식별자 역할을 하는 ID 번호입니다. 이 필드는 이 레코드의 고유 키입니다.
문자열 블록 유형	uint32	액세스 제어 정책의 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.

표 3-15 액세스 제어 정책 이름 데이터 블록 필드 (계속)

필드	데이터 유형	설명
문자열 블록 길이	uint32	액세스 제어 정책 이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 액세스 제어 정책 이름의 바이트 수를 더한 값이 포함됩니다.
액세스 제어 정책 이름	string	액세스 제어 정책 이름입니다.

액세스 제어 규칙 ID 레코드 메타데이터

eStreamer 서비스는 침입 이벤트 또는 연결 이벤트를 트리거한 액세스 제어 규칙에 대한 정보를 포함하는 메타데이터를 액세스 제어 규칙 ID 레코드 내에 포함하여 전송합니다. 해당 레코드의 형식은 아래에 나와 있습니다. 버전 4 메타데이터 플래그(요청 메시지의 Request Flags(요청 플래그) 필드에 포함된 비트 20)가 설정되어 있으면 액세스 제어 규칙 메타데이터가 전송됩니다. 요청 플래그, 2-12페이지의 내용을 참조하십시오. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 액세스 제어 규칙 ID 레코드임을 나타내는 119입니다. 이 필드에는 규칙 ID 데이터 블록(계열 2 데이터 블록 집합 내 블록 유형 15)이 포함됩니다.

다음 표에는 액세스 제어 규칙 ID 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 3-16 액세스 제어 규칙 ID 데이터 블록 필드

필드	데이터 유형	설명
액세스 제어 규칙 ID 데이터 블록 유형	uint32	액세스 제어 규칙 ID 데이터 블록을 시작합니다. 이 값은 항상 15입니다. 블록 유형은 계열 2 블록입니다.
액세스 제어 규칙 ID 데이터 블록 길이	uint32	데이터 블록의 길이입니다. 데이터 바이트 수에 2개 데이터 블록 헤더 필드의 8바이트를 더한 길이입니다.
액세스 제어 규칙 UUID	uint8[16]	액세스 제어 규칙의 UUID입니다. 이 필드와 Access Control Rule ID(액세스 제어 규칙 ID)는 이 레코드의 고유 키입니다.
액세스 제어 규칙 ID	uint32	연결 이벤트와 관련된 액세스 제어 정책의 규칙에 대한 내부 식별자입니다. 이 필드와 Access Control Rule UUID(액세스 제어 규칙 UUID)는 이 레코드의 고유 키입니다.
문자열 블록 유형	uint32	액세스 제어 규칙의 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 규칙 이름의 바이트 수를 더한 값이 포함됩니다.
액세스 제어 규칙 이름	string	액세스 제어 규칙 이름입니다.

매니지드 디바이스 레코드 메타데이터

eStreamer 서비스는 침입 이벤트와 연결되어 있는 매니지드 디바이스의 정보가 포함된 메타데이터를 매니지드 디바이스 레코드 내에 포함하여 전송합니다. 해당 레코드의 형식은 아래에 나와 있습니다. 버전 4 메타데이터 플래그(요청 메시지의 Request Flags(요청 플래그) 필드에 포함된 비트 20)가 설정되어 있으면 매니지드 디바이스 메타데이터가 전송됩니다. 요청 플래그, 2-12페이지의 내용을 참조하십시오. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 매니지드 디바이스 레코드임을 나타내는 123입니다.

다음 표에는 매니지드 디바이스 레코드의 필드에 대한 설명이 나와 있습니다.

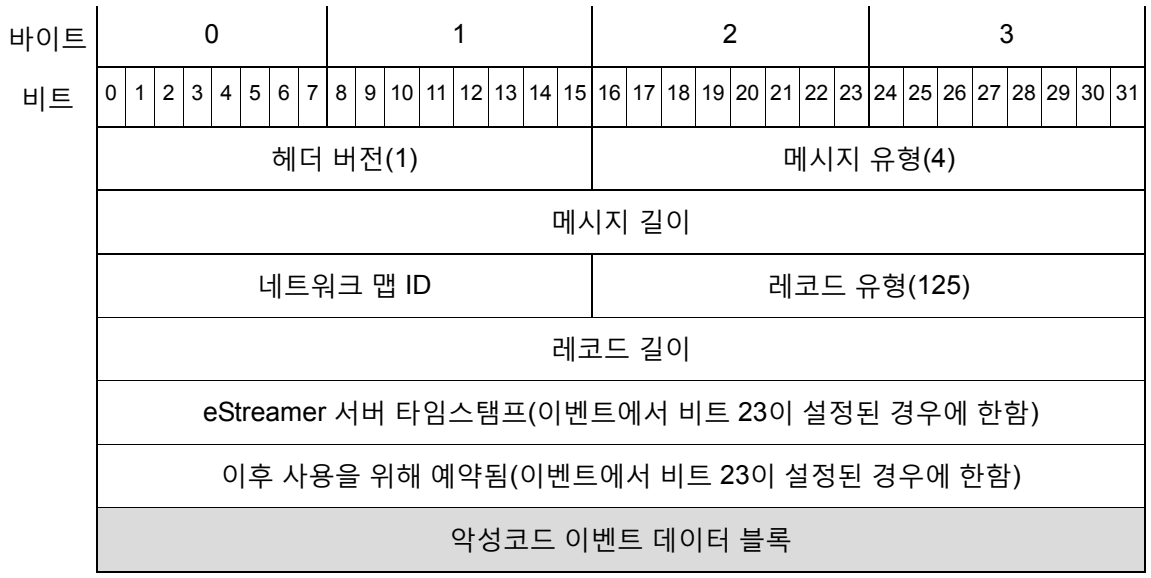
표 3-17 매니지드 디바이스 레코드 필드

필드	데이터 유형	설명
디바이스 ID	uint32	매니지드 디바이스의 ID 번호입니다. 이 필드는 이 레코드의 고유 키입니다.
이름 길이	uint32	이름에 포함된 바이트 수입니다.
이름	string	매니지드 디바이스 이름입니다.

5.1.1 이상 버전용 악성코드 이벤트 레코드

다음 그림에서 악성코드 이벤트 레코드의 필드는 음영으로 표시되어 있습니다. 레코드 유형은 125입니다.

이벤트 버전이 2이고 이벤트 코드가 101인 요청 메시지에서 악성코드 이벤트 플래그(Request Flags(요청 플래그) 필드의 비트 30)를 설정하여 악성코드 이벤트 레코드를 요청합니다. 요청 플래그, 2-12페이지의 내용을 참조하십시오. 비트 23을 활성화하면 레코드에 확장 이벤트 헤더가 포함됩니다. 이 필드에는 악성코드 이벤트 데이터 블록(계열 2 데이터 블록 집합 내 블록 유형 24, 33, 35, 44, 47 중 하나)이 포함됩니다.



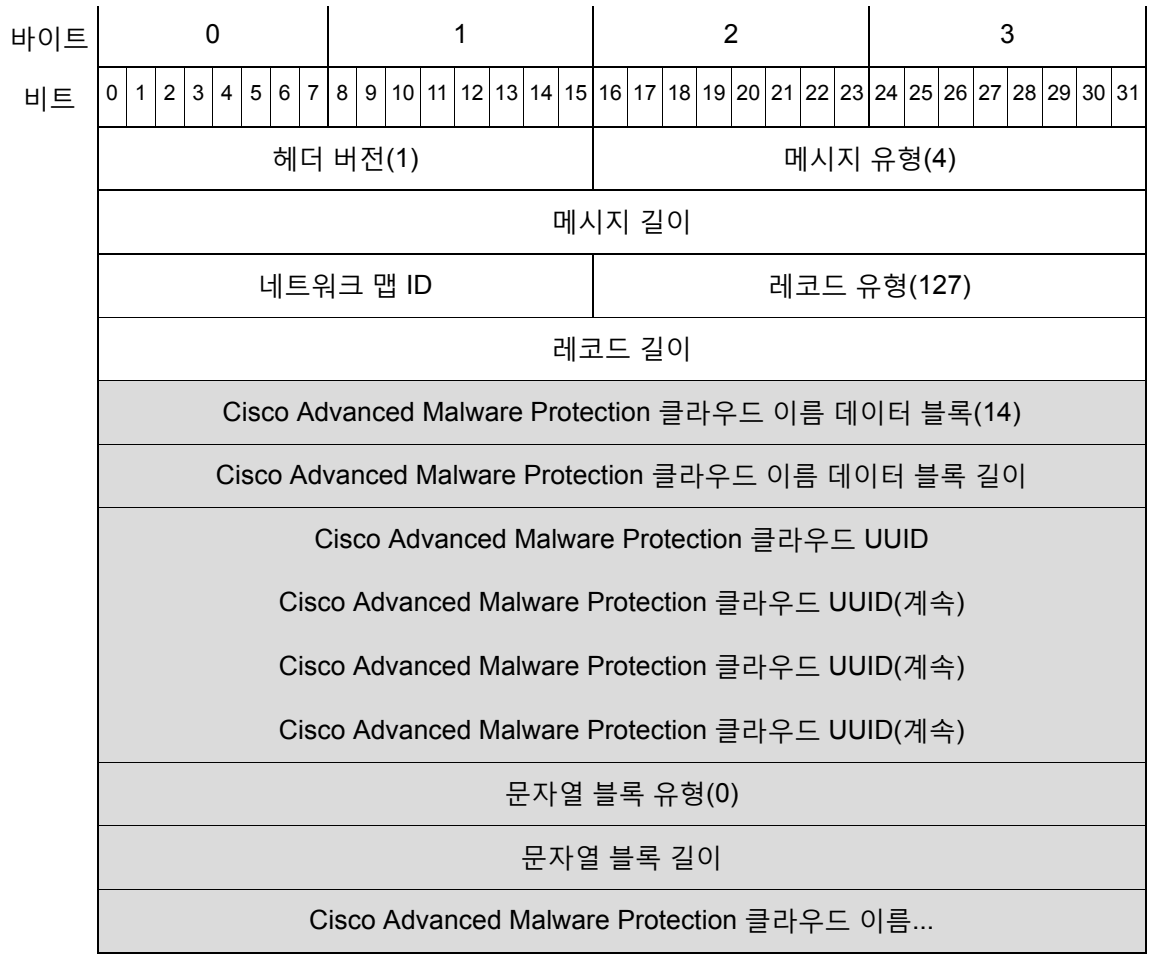
다음 표에는 각 악성코드 이벤트 레코드 데이터 필드에 대한 설명이 나와 있습니다.

표 3-18 악성코드 이벤트 레코드 필드

필드	데이터 유형	설명
악성코드 이벤트 데이터 블록	variable	악성코드 이벤트 데이터 블록을 나타냅니다. 자세한 정보는 6.0 이상 버전용 악성코드 이벤트 데이터 블록, 3-94페이지의 내용을 참조하십시오.

Cisco Advanced Malware Protection 클라우드 이름 메타데이터

eStreamer 서비스는 침입 이벤트 또는 연결 이벤트와 관련된 Cisco Advanced Malware Protection 클라우드(AMP 클라우드 또는 간단히 클라우드로 지칭됨)의 이름에 대한 정보를 포함하는 메타데이터를 Cisco Advanced Malware Protection 클라우드 이름 레코드 내에 포함하여 전송합니다. 해당 레코드의 형식은 아래에 나와 있습니다. 버전 4 메타데이터 플래그(요청 메시지의 Request Flags(요청 플래그) 필드에 포함된 비트 20)가 설정되어 있으면 AMP 클라우드 이름 정보가 전송됩니다. 요청 플래그, 2-12페이지의 내용을 참조하십시오. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 Cisco Advanced Malware Protection 클라우드 이름 레코드임을 나타내는 `127`입니다. 이 필드에는 UUID 문자열 데이터 블록(계열 2 데이터 블록 집합 내 블록 유형 14)이 포함됩니다.



다음 표에는 Cisco Advanced Malware Protection 클라우드 이름 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 3-19 Cisco Advanced Malware Protection 클라우드이름 데이터 블록 필드

필드	데이터 유형	설명
Cisco Advanced Malware Protection 클라우드 이름 데이터 블록 유형	uint32	Cisco Advanced Malware Protection 클라우드 이름 데이터 블록을 시작합니다. 이 값은 항상 14입니다. 블록 유형은 계열 2 블록입니다.
Cisco Advanced Malware Protection 클라우드 이름 데이터 블록 길이	uint32	데이터 블록의 길이입니다. 데이터 바이트 수에 2개 데이터 블록 헤더 필드의 8바이트를 더한 길이입니다.

표 3-19 Cisco Advanced Malware Protection 클라우드이름 데이터 블록 필드 (계속)

필드	데이터 유형	설명
Cisco Advanced Malware Protection 클라우드 UUID	uint8[16]	연결 이벤트와 관련된 Cisco Advanced Malware Protection 클라우드의 고유 식별자 역할을 하는 Cisco Advanced Malware Protection 클라우드 ID 번호입니다. 이 필드는 이 레코드의 고유 키입니다.
문자열 블록 유형	uint32	Cisco Advanced Malware Protection 클라우드의 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	Cisco Advanced Malware Protection 클라우드 이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Cisco Advanced Malware Protection 클라우드 이름의 바이트 수를 더한 값이 포함됩니다.
Cisco Advanced Malware Protection 클라우드 이름	string	Cisco Advanced Malware Protection 클라우드 이름입니다.

악성코드 이벤트 유형 메타데이터

eStreamer 서비스는 이벤트에 대한 악성코드 이벤트 유형 정보가 포함된 메타데이터를 악성코드 이벤트 유형 레코드 내에 포함하여 전송합니다. 해당 레코드의 형식은 아래에 나와 있습니다. 메타데이터 플래그(요청 메시지의 Request Flags(요청 플래그) 필드에 포함된 비트 20)가 설정되어 있으면 악성코드 이벤트 유형 정보가 전송됩니다. 요청 플래그, 2-12페이지의 내용을 참조하십시오. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 악성코드 이벤트 유형 레코드임을 나타내는 128입니다.

다음 표에는 악성코드 이벤트 유형 레코드의 필드에 대한 설명이 나와 있습니다.

표 3-20 악성코드 이벤트 유형 레코드 필드

필드	데이터 유형	설명
악성코드 이벤트 유형 ID	uint32	악성코드 이벤트 유형 ID 번호입니다. 이 필드는 이 레코드의 고유 키입니다.
악성코드 이벤트 유형 길이	uint32	악성코드 이벤트 유형에 포함된 바이트 수입니다.
악성코드 이벤트 유형	string	악성코드 이벤트의 유형입니다.

악성코드 이벤트 하위 유형 메타데이터

eStreamer 서비스는 이벤트에 대한 악성코드 이벤트 하위 유형 정보가 포함된 메타데이터를 악성코드 이벤트 하위 유형 레코드 내에 포함하여 전송합니다. 해당 레코드의 형식은 아래에 나와 있습니다. 메타데이터 플래그(요청 메시지의 Request Flags(요청 플래그) 필드에 포함된 비트 20)가 설정되어 있으면 악성코드 이벤트 유형 정보가 전송됩니다. 요청 플래그, 2-12페이지의 내용을 참조하십시오. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 악성코드 이벤트 하위 유형 레코드임을 나타내는 129입니다.

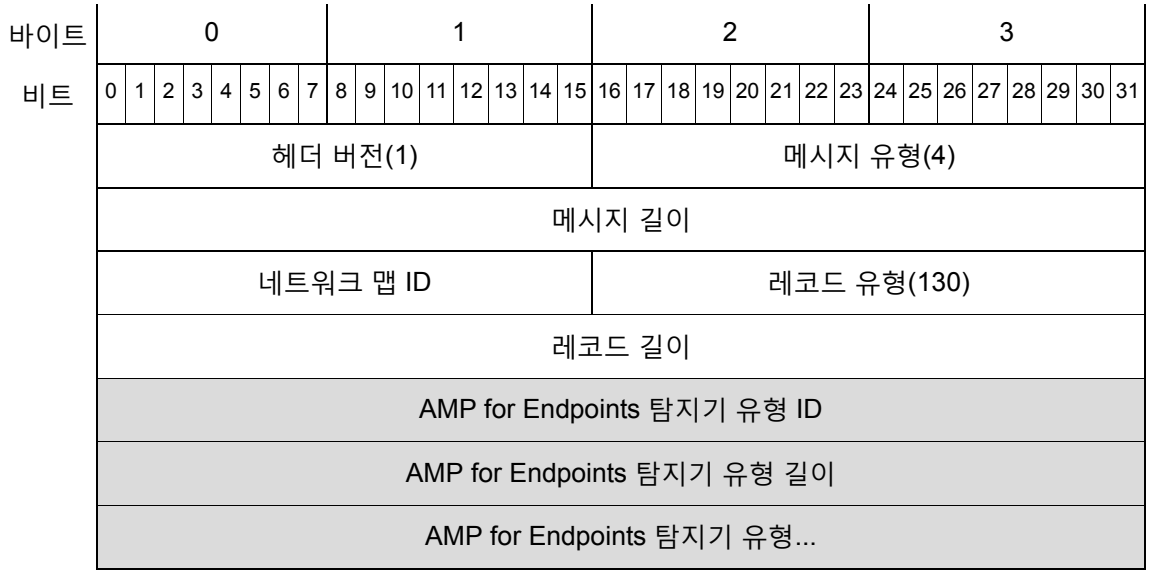
다음 표에는 악성코드 이벤트 하위 유형 레코드의 필드에 대한 설명이 나와 있습니다.

표 3-21 악성코드 이벤트 하위 유형 레코드 필드

필드	데이터 유형	설명
악성코드 이벤트 하위 유형 ID	uint32	악성코드 이벤트 하위 유형 ID 번호입니다. 이 필드는 이 레코드의 고유 키입니다.
악성코드 이벤트 하위 유형 길이	uint32	악성코드 이벤트 하위 유형에 포함된 바이트 수입니다.
악성코드 이벤트 하위 유형	string	악성코드 이벤트 하위 유형입니다.

AMP for Endpoints 탐지기 유형 메타데이터

eStreamer 서비스는 이벤트에 대한 AMP for Endpoints 탐지기 유형 정보가 포함된 메타데이터를 AMP for Endpoints 탐지기 유형 레코드 내에 포함하여 전송합니다. 해당 레코드의 형식은 아래에 나와 있습니다. 메타데이터 플래그 중 하나(요청 메시지의 Request Flags(요청 플래그) 필드에 포함된 비트 1, 14, 15, 20)가 설정되어 있으면 AMP for Endpoints 탐지기 유형 정보가 전송됩니다. 요청 플래그, 2-12페이지의 내용을 참조하십시오. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 AMP for Endpoints 탐지기 유형 레코드임을 나타내는 130입니다.



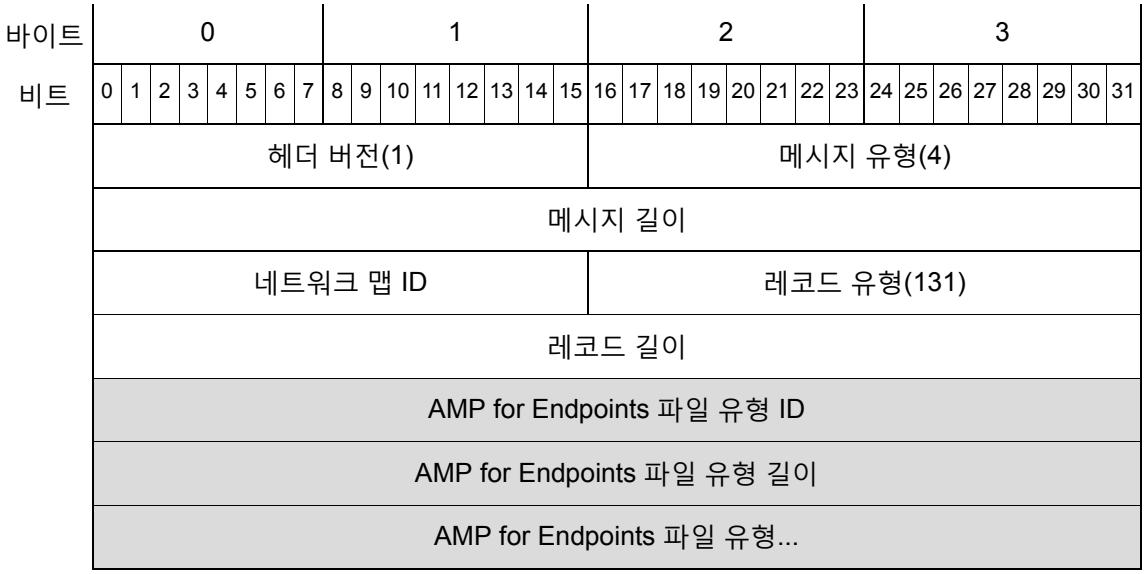
다음 표에는 AMP for Endpoints 탐지기 유형 레코드의 필드에 대한 설명이 나와 있습니다.

표 3-22 AMP for Endpoints 탐지기 유형 레코드 필드

필드	데이터 유형	설명
AMP for Endpoints 탐지기 유형 ID	uint32	AMP for Endpoints 탐지기 유형 ID 번호입니다. 이 필드는 이 레코드의 고유 키입니다.
AMP for Endpoints 탐지기 유형 길이	uint32	AMP for Endpoints 탐지기 유형에 포함된 바이트 수입니다.
AMP for Endpoints 탐지기 유형	string	AMP for Endpoints 탐지기의 유형입니다.

AMP for Endpoints 파일 유형 메타데이터

eStreamer 서비스는 이벤트에 대한 AMP for Endpoints 파일 유형 정보가 포함된 메타데이터를 AMP for Endpoints 파일 유형 레코드 내에 포함하여 전송합니다. 해당 레코드의 형식은 아래에 나와 있습니다. 메타데이터 플래그 중 하나(요청 메시지의 Request Flags(요청 플래그) 필드에 포함된 비트 1, 14, 15, 20)가 설정되어 있으면 AMP for Endpoints 파일 유형 정보가 전송됩니다. 요청 플래그, 2-12페이지의 내용을 참조하십시오. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 AMP for Endpoints 파일 유형 레코드임을 나타내는 131입니다.



다음 표에는 AMP for Endpoints 파일 유형 레코드의 필드에 대한 설명이 나와 있습니다.

표 3-23 AMP for Endpoints 파일 유형 레코드 필드

필드	데이터 유형	설명
AMP for Endpoints 파일 유형 ID	uint32	AMP for Endpoints 파일 유형 ID 번호입니다. 이 필드는 이 레코드의 고유 키입니다.
AMP for Endpoints 파일 유형 길이	uint32	AMP for Endpoints 파일 유형에 포함된 바이트 수입니다.
AMP for Endpoints 파일 유형	string	탐지된 파일의 유형입니다.

보안 상황 이름

eStreamer 서비스는 보안 상황 이름 정보가 포함된 메타데이터를 전송합니다. 해당 메타데이터의 형식은 아래에 나와 있습니다. 메타데이터 플래그 중 하나(요청 메시지의 Request Flags(요청 플래그) 필드에 포함된 비트 1, 14, 15, 20)가 설정되어 있으면 보안 상황 이름 정보가 전송됩니다. 요청 플래그, 2-12페이지의 내용을 참조하십시오. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 보안 상황 이름 레코드임을 나타내는 132입니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
헤더 버전(1)																	메시지 유형(4)															
메시지 길이																																
네트워크 맵 ID																	레코드 유형(132)															
레코드 길이																																
보안 상황 UUID 보안 상황 UUID(계속) 보안 상황 UUID(계속) 보안 상황 UUID(계속)																																
문자열 블록 유형(0)																																
문자열 블록 길이																																
보안 상황 이름...																																

다음 표에는 보안 상황 이름 레코드의 필드에 대한 설명이 나와 있습니다.

표 3-24 보안 상황 이름 레코드 필드

필드	데이터 유형	설명
보안 상황 UUID	uint8[16]	보안 상황의 UUID입니다. 이 필드는 이 레코드의 고유 키입니다.
문자열 블록 유형	uint32	보안 상황의 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	보안 상황 이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 보안 상황 이름의 바이트 수를 더한 값이 포함됩니다.
보안 상황 이름	string	보안 상황 이름입니다.

5.4 이상 버전용 상관관계 이벤트

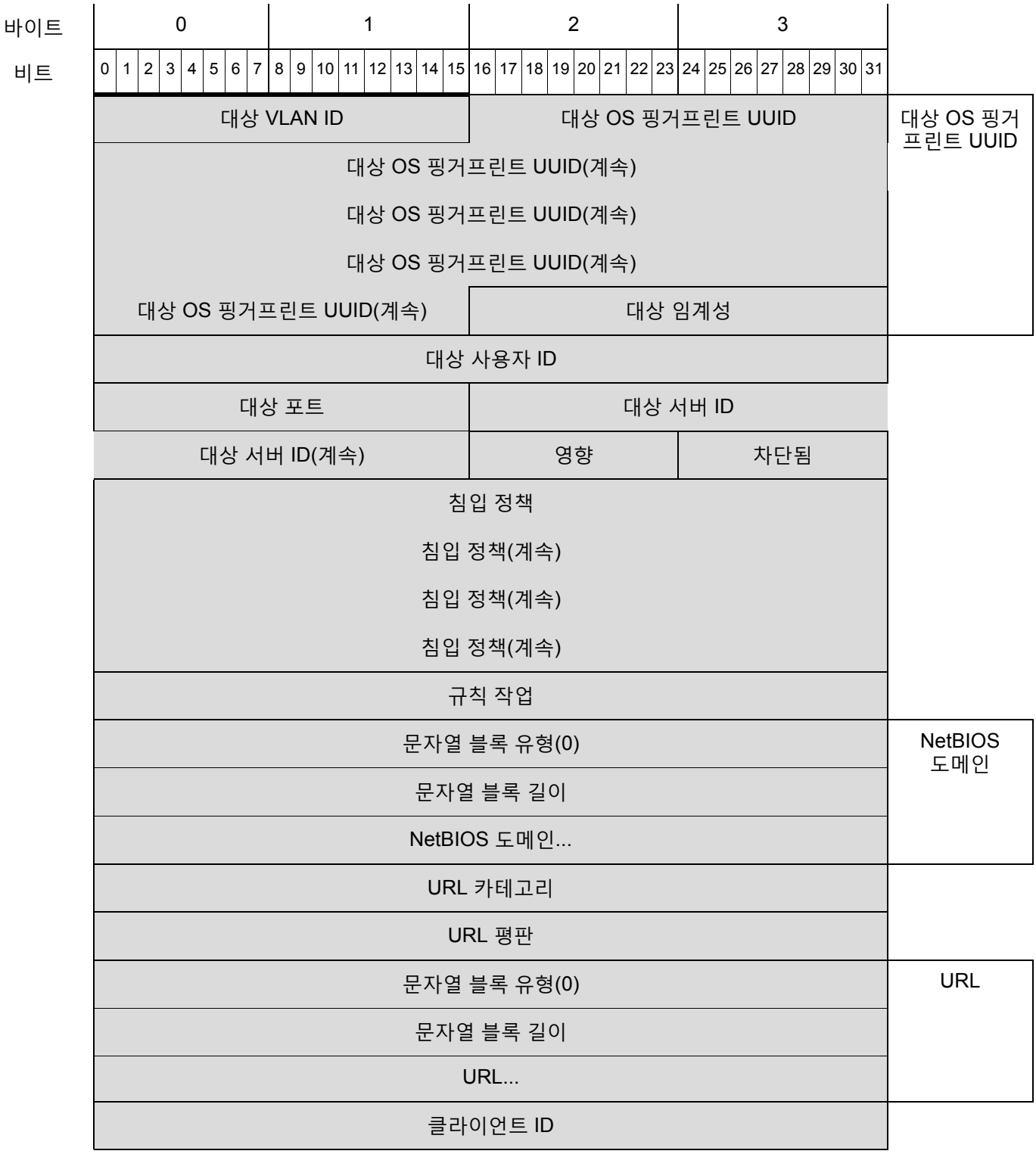
5.0 이전 버전에서는 명칭이 컴플라이언스 이벤트였던 상관관계 이벤트는 상관관계 정책 위반에 대한 정보를 포함합니다. 이 메시지는 표준 eStreamer 메시지 헤더를 사용하며 레코드 유형 112와 계열 1 데이터 블록 집합의 상관관계 데이터 블록 유형 156을 차례로 지정합니다. 데이터 블록 유형 156과 이전 버전인 블록 유형 128의 차이점은, 유형 156의 경우 IPv6 지원을 포함한다는 것입니다.

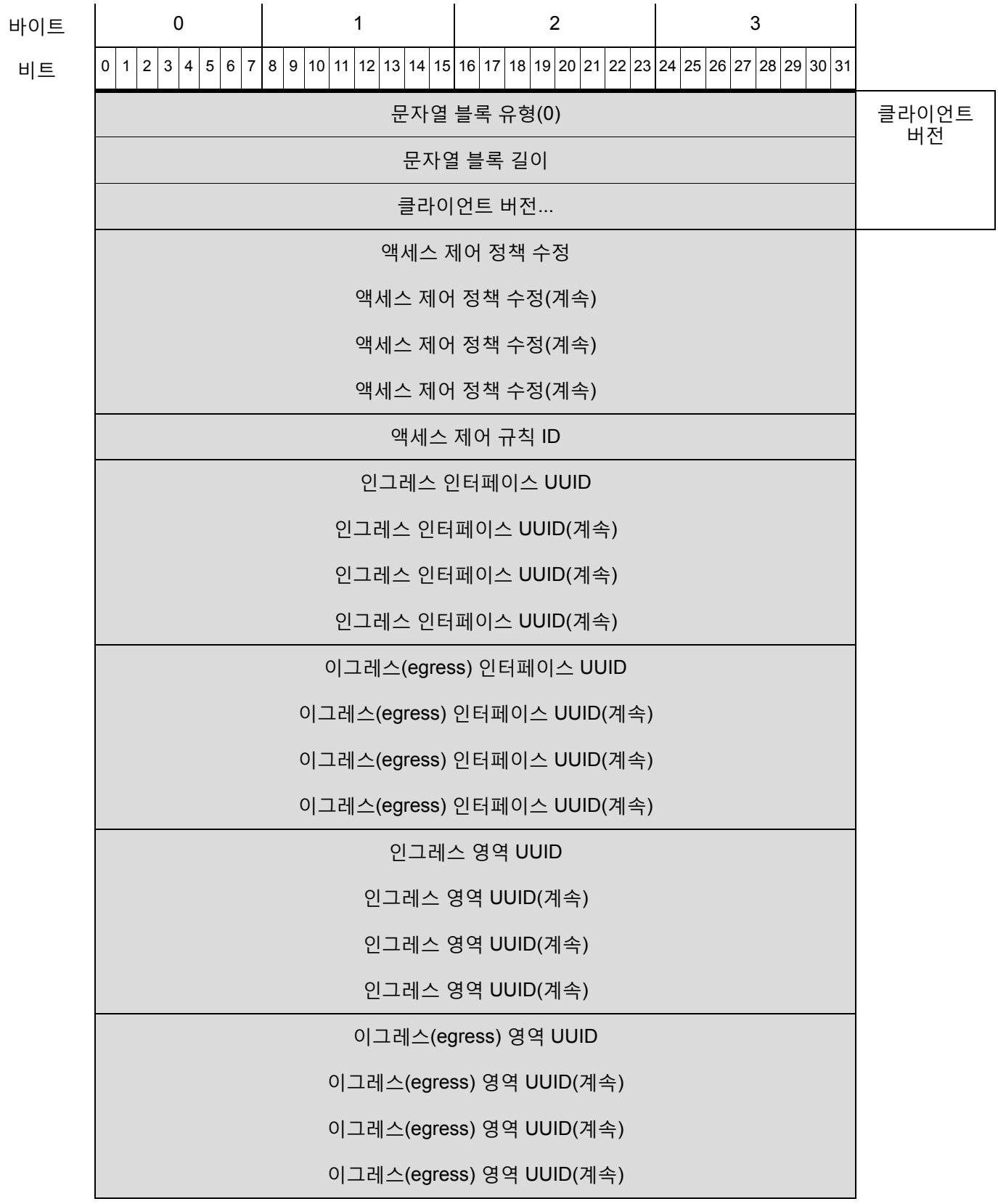
5.4 이상 버전의 상관관계 이벤트에는 지리위치, 보안 인텔리전스 및 SSL 지원을 위한 새로운 필드가 있습니다.

5.4 이상 버전의 상관관계 이벤트는 eStreamer에서 확장 요청을 통해서만 요청할 수 있습니다. 이렇게 하려면 스트림 요청 메시지에서 이벤트 유형 코드 31, 버전 코드 9를 요청합니다. 확장 요청 제출에 대한 자세한 정보는 확장 요청 제출, 2-4페이지의 내용을 참조하십시오. 필요한 경우 초기 이벤트 스트림 요청 메시지의 플래그 필드에서 비트 23을 활성화하여 확장 이벤트 헤더를 포함할 수 있습니다. 플래그 필드에서 비트 20을 활성화하여 사용자 메타데이터를 포함할 수도 있습니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
헤더 버전(1)																	메시지 유형(4)															
메시지 길이																																
네트워크 맵 ID																	레코드 유형(112)															
레코드 길이																																
eStreamer 서버 타임스탬프(이벤트에서 비트 23이 설정된 경우에 한함)																																
이후 사용을 위해 예약됨(이벤트에서 비트 23이 설정된 경우에 한함)																																
상관관계 블록 유형(156)																																
상관관계 블록 길이																																
디바이스 ID																																
(상관관계) 이벤트 초																																
이벤트 ID																																
정책 ID																																
규칙 ID																																
우선순위																																


바이트
0
1
2
3
비트
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
문자열 블록 유형(0)
문자열 블록 길이
설명...
이벤트 유형
이벤트 설명
이벤트 디바이스 ID
서명 ID
서명 생성기 ID
(트리거) 이벤트 초
(트리거) 이벤트 마이크로초
이벤트 ID
이벤트 정의 마스크
이벤트 영향 플래그
IP 프로토콜
네트워크 프로토콜
소스 IP
소스 호스트 유형
소스 VLAN ID
소스 OS 핑거프린트 UUID
소스 OS 핑거프린트 UUID
소스 OS 핑거프린트 UUID(계속)
소스 OS 핑거프린트 UUID(계속)
소스 OS 핑거프린트 UUID(계속)
소스 OS 핑거프린트 UUID(계속)
소스 임계성
소스 임계성(계속)
소스 사용자 ID
소스 사용자 ID(계속)
소스 포트
소스 서버 ID
소스 서버 ID(계속)
대상 IP
대상 IP(계속)
대상 호스트 유형


바이트
0
1
2
3
비트
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
대상 VLAN ID
대상 OS 핑거프린트 UUID
대상 OS 핑거프린트 UUID
대상 OS 핑거프린트 UUID(계속)
대상 OS 핑거프린트 UUID(계속)
대상 OS 핑거프린트 UUID(계속)
대상 OS 핑거프린트 UUID(계속)
대상 임계성
대상 사용자 ID
대상 포트
대상 서버 ID
대상 서버 ID(계속)
영향
차단됨
침입 정책
침입 정책(계속)
침입 정책(계속)
침입 정책(계속)
규칙 작업
문자열 블록 유형(0)
NetBIOS 도메인
문자열 블록 길이
NetBIOS 도메인...
URL 카테고리
URL 평판
문자열 블록 유형(0)
URL
문자열 블록 길이
URL...
클라이언트 ID


바이트
0
1
2
3
비트
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
문자열 블록 유형(0)
문자열 블록 길이
클라이언트 버전...
클라이언트 버전
액세스 제어 정책 수정
액세스 제어 정책 수정(계속)
액세스 제어 정책 수정(계속)
액세스 제어 정책 수정(계속)
액세스 제어 규칙 ID
인그레스 인터페이스 UUID
인그레스 인터페이스 UUID(계속)
인그레스 인터페이스 UUID(계속)
인그레스 인터페이스 UUID(계속)
이그레스(egress) 인터페이스 UUID
이그레스(egress) 인터페이스 UUID(계속)
이그레스(egress) 인터페이스 UUID(계속)
이그레스(egress) 인터페이스 UUID(계속)
인그레스 영역 UUID
인그레스 영역 UUID(계속)
인그레스 영역 UUID(계속)
인그레스 영역 UUID(계속)
이그레스(egress) 영역 UUID
이그레스(egress) 영역 UUID(계속)
이그레스(egress) 영역 UUID(계속)
이그레스(egress) 영역 UUID(계속)

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
소스 IPv6 주소																																
소스 IPv6 주소(계속)																																
소스 IPv6 주소(계속)																																
소스 IPv6 주소(계속)																																
대상 IPv6 주소																																
대상 IPv6 주소(계속)																																
대상 IPv6 주소(계속)																																
대상 IPv6 주소(계속)																																
소스 국가																	대상 국가															
보안 인텔리전스 UUID																																
보안 인텔리전스 UUID(계속)																																
보안 인텔리전스 UUID(계속)																																
보안 인텔리전스 UUID(계속)																																
보안 상황																																
보안 상황(계속)																																
보안 상황(계속)																																
보안 상황(계속)																																
SSL 정책 ID																																
SSL 정책 ID(계속)																																
SSL 정책 ID(계속)																																
SSL 정책 ID(계속)																																
SSL 규칙 ID(계속)																																
SSL 실제 작업																																
SSL 플로우 상태																																

레코드 구조에는 계열 1 블록인 문자열 블록 유형이 포함됩니다. 계열 1 블록에 대한 자세한 정보는 검색(계열 1) 블록 이해, 4-63페이지의 내용을 참조하십시오.

표 3-25 5.4 이상 버전용 상관관계 이벤트 데이터 필드

필드	데이터 유형	설명
상관관계 블록 유형	uint32	상관관계 이벤트 데이터 블록이 뒤에 옴을 나타냅니다. 이 필드의 값은 항상 156입니다. 검색(계열 1) 블록 이해, 4-63페이지의 내용을 참조하십시오.
상관관계 블록 길이	uint32	상관관계 데이터 블록의 길이입니다. 여기에는 상관관계 블록 유형의 8바이트에 그 뒤의 상관관계 데이터를 더한 값이 포함됩니다.
디바이스 ID	uint32	상관관계 이벤트를 생성한 매니지드 디바이스 또는 Management Center의 내부 ID 번호입니다. 값 0은 Management Center를 나타냅니다. 버전 3 메타데이터를 요청하면 매니지드 디바이스 이름을 가져올 수 있습니다. 자세한 정보는 매니지드 디바이스 레코드 메타데이터, 3-35페이지의 내용을 참조하십시오.
(상관관계) 이벤트 초	uint32	상관관계 이벤트가 생성된 시간을 나타내는 UNIX 타임스탬프입니다(1970년 1월 1일 이후의 초 단위 시간).
이벤트 ID	uint32	상관관계 이벤트 ID 번호입니다.
정책 ID	uint32	위반된 상관관계 정책의 ID 번호입니다 데이터베이스에서 정책 ID 번호를 가져오는 방법에 대한 자세한 정보는 서비스 레코드, 4-15페이지의 내용을 참조하십시오.
규칙 ID	uint32	정책을 위반하는 방식으로 트리거된 상관관계 규칙의 ID 번호입니다. 데이터베이스에서 정책 ID 번호를 가져오는 방법에 대한 자세한 정보는 서비스 레코드, 4-15페이지의 내용을 참조하십시오.
우선순위	uint32	이벤트에 할당된 우선순위입니다. 0에서 5 사이의 정숫값입니다.
문자열 블록 유형	uint32	상관관계 위반 이벤트 설명이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0으로 설정됩니다. 문자열 블록에 대한 자세한 정보는 문자열 데이터 블록, 4-72페이지의 내용을 참조하십시오.
문자열 블록 길이	uint32	이벤트 설명 문자열 블록의 바이트 수입니다. 여기에는 문자열 블록 유형의 4바이트 + 문자열 블록 길이의 4바이트 + 설명의 바이트 수가 포함됩니다.

표 3-25 5.4 이상 버전용 상관관계 이벤트 데이터 필드 (계속)

필드	데이터 유형	설명
설명	string	상관관계 이벤트의 설명입니다.
이벤트 유형	uint8	상관관계 이벤트가 트리거된 원인(침입, 호스트 검색 또는 사용자 이벤트)을 나타냅니다. • 1 - 침입 • 2 - 호스트 검색 • 3 - 사용자
이벤트 디바이스 ID	uint32	상관관계 이벤트를 트리거한 이벤트가 생성된 디바이스의 ID 번호입니다. 버전 3 메타데이터를 요청하면 디바이스 이름을 가져올 수 있습니다. 자세한 정보는 매니지드 디바이스 레코드 메타데이터, 3-35페이지의 내용을 참조하십시오.
서명 ID	uint32	이벤트가 침입 이벤트였던 경우 이벤트에 해당하는 규칙 ID 번호를 나타냅니다. 그렇지 않은 경우 값은 0입니다.
서명 생성기 ID	uint32	이벤트가 침입 이벤트였던 경우 해당 이벤트를 생성한 Firepower System 전처리기 또는 규칙 엔진의 ID 번호를 나타냅니다.
(트리거) 이벤트 초	uint32	상관관계 정책 규칙을 트리거한 이벤트의 시간을 나타내는 UNIX 타임스탬프입니다(1970년 1월 1일 이후의 초 단위 시간).
(트리거) 이벤트 마이크로초	uint32	이벤트가 탐지된 마이크로초(100만분의 1초) 단위의 증분 시간입니다.
이벤트 ID	uint32	Cisco 디바이스에서 생성된 이벤트의 ID 번호입니다.
이벤트 정의 마스크	bits[32]	이 필드에 설정된 비트는 메시지에서 해당 필드 다음에 오는 필드 중 유효한 필드를 나타냅니다. 각 비트 값의 목록은 표 3-23, 3-42페이지의 내용을 참조하십시오.

표 3-25 5.4 이상 버전용 상관관계 이벤트 데이터 필드 (계속)

필드	데이터 유형	설명
이벤트 영향 플래그	bits[8]	이벤트의 영향 플래그 값입니다. 하위 8비트가 영향 레벨을 나타냅니다. 값은 다음과 같습니다. • 0x01(비트 0) - 소스 또는 대상 호스트가 시스템에서 모니터링하는 네트워크에 있습니다. • 0x02(비트 1) - 소스 또는 대상 호스트가 네트워크 맵에 있습니다. • 0x04(비트 2) - 소스 또는 대상 호스트가 이벤트의 포트에서 서버를 실행 중이거나(TCP 또는 UDP인 경우) IP 프로토콜을 사용합니다. • 0x08(비트 3) - 이벤트의 소스 또는 대상 호스트 운영 체제에 매핑된 취약점이 있습니다. • 0x10(비트 4) - 이벤트에서 탐지된 서버에 매핑된 취약점이 있습니다. • 0x20(비트 5) - 이벤트로 인해 매니지드 디바이스에서 세션이 삭제되었습니다(디바이스가 인라인, 스위치드 또는 라우티드 구축에서 실행 중인 경우에만 사용됨). Firepower System 웹 인터페이스의 차단 상태에 해당합니다. • 0x40(비트 6) - 이 이벤트를 생성한 규칙에 영향 플래그를 빨간색으로 설정하는 규칙 메타데이터가 있습니다. 소스 또는 대상 호스트가 바이러스, 트로이 목마, 기타 악성 소프트웨어에 감염되었을 가능성이 있습니다. • 0x80(비트 7) - 이벤트에서 탐지된 클라이언트에 매핑된 취약점이 있습니다. (5.0 이상 버전만 해당) 다음 영향 레벨 값은 Management Center의 특정 우선 순위에 매핑됩니다. `x`는 값이 0 또는 1일 수 있음을 나타냅니다. • 회색(0, 알 수 없음): `00x00000` • 빨간색(1, 취약함): `xxxx1xxx`, `xxx1xxxx`, `x1xxxxxx`, `1xxxxxxx` (5.0 이상 버전만 해당) • 주황색(2, 잠재적으로 취약함): `00x0011x` • 노란색(3, 현재 취약하지 않음): `00x0001x` • 파란색(4, 알 수 없는 대상): `00x00001`
IP 프로토콜	uint8	해당하는 경우 이벤트와 관련된 IP 프로토콜의 식별자입니다.
네트워크 프로토콜	uint16	해당하는 경우 이벤트와 관련된 네트워크 프로토콜입니다.
소스 IP 주소	uint8[4]	이 필드는 예약되지만 더 이상 내용이 입력되지는 않습니다. 소스 IPv4 주소는 Source IPv6 Address(소스 IPv6 주소) 필드에 저장됩니다. 자세한 정보는 IP 주소, 1-5페이지의 내용을 참조하십시오.

표 3-25 5.4 이상 버전용 상관관계 이벤트 데이터 필드 (계속)

필드	데이터 유형	설명
소스 호스트 유형	uint8	소스 호스트의 유형입니다. • 0 - 호스트 • 1 - 라우터 • 2 - 브리지
소스 VLAN ID	uint16	해당하는 경우 소스 호스트의 VLAN ID 번호입니다.
소스 OS 핑거프린트 UUID	uint8[16]	소스 호스트 운영 체제의 고유 식별자 역할을 하는 핑거프린트 ID 번호입니다. 핑거프린트 ID에 매핑되는 값을 가져오는 방법에 대한 자세한 정보는 서비스 레코드, 4-15페이지의 내용을 참조하십시오.
소스 임계성	uint16	소스 호스트의 사용자 정의 임계성 값입니다. • 0 - 없음 • 1 - 낮음 • 2 - 보통 • 3 - 높음
소스 사용자 ID	uint32	시스템이 식별한 소스 호스트에 로그인하는 사용자의 ID 번호입니다.
소스 포트	uint16	이벤트의 소스 포트입니다.
소스 서버 ID	uint32	소스 호스트에서 실행 중인 서버의 ID 번호입니다.
대상 IP 주소	uint8[4]	이 필드는 예약되지만 더 이상 내용이 입력되지는 않습니다. 대상 IPv4 주소는 Destination IPv6 Address(대상 IPv6 주소) 필드에 저장됩니다. 자세한 정보는 IP 주소, 1-5페이지의 내용을 참조하십시오.
대상 호스트 유형	uint8	대상 호스트의 유형입니다. • 0 - 호스트 • 1 - 라우터 • 2 - 브리지
대상 VLAN ID	uint16	해당하는 경우 대상 호스트의 VLAN ID 번호입니다.
대상 OS 핑거프린트 UUID	uint8[16]	대상 호스트 운영 체제의 고유 식별자 역할을 하는 핑거프린트 ID 번호입니다. 핑거프린트 ID에 매핑되는 값을 가져오는 방법에 대한 자세한 정보는 서비스 레코드, 4-15페이지의 내용을 참조하십시오.
대상 임계성	uint16	대상 호스트의 사용자 정의 임계성 값입니다. • 0 - 없음 • 1 - 낮음 • 2 - 보통 • 3 - 높음

표 3-25 5.4 이상 버전용 상관관계 이벤트 데이터 필드 (계속)

필드	데이터 유형	설명
대상 사용자 ID	uint32	시스템이 식별한 대상 호스트에 로그인하는 사용자의 ID 번호입니다.
대상 포트	uint16	이벤트의 대상 포트입니다.
대상 서비스 ID	uint32	소스 호스트에서 실행 중인 서버의 ID 번호입니다.
영향	uint8	이벤트의 영향 플래그 값입니다. 값은 다음과 같습니다. • 1 - 빨간색(취약함) • 2 - 주황색(잠재적으로 취약함) • 3 - 노란색(현재 취약하지 않음) • 4 - 파란색(알 수 없는 대상) • 5 - 회색(알 수 없는 영향)
차단됨	uint8	침입 이벤트를 트리거한 패킷에 발생한 상황을 나타내는 값입니다. • 0 - 침입 이벤트가 삭제되지 않음 • 1 - 침입 이벤트가 삭제됨(인라인/스위치드/라우티드 구축인 경우 삭제됨) • 2 - 이벤트를 트리거한 패킷이 삭제되었을 수 있음(침입 정책이 인라인, 스위치드 또는 라우티드 구축의 디바이스에 적용된 경우)
침입 정책	uint8[16]	이벤트와 관련된 침입 정책의 UUID입니다.
규칙 작업	uint32	이벤트를 트리거한 규칙(허용, 차단 등)에 대해 사용자 인터페이스에서 선택한 작업입니다.
문자열 블록 유형	uint32	NetBIOS 도메인이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0으로 설정됩니다. 문자열 블록에 대한 자세한 정보는 문자열 데이터 블록, 4-72페이지의 내용을 참조하십시오.
문자열 블록 길이	uint32	이벤트 설명 문자열 블록의 바이트 수입니다. 여기에는 문자열 블록 유형의 4바이트 + 문자열 블록 길이의 4바이트 + NetBIOS 도메인의 바이트 수가 포함됩니다.
NetBIOS 도메인	string	NetBIOS 도메인의 이름입니다.
URL 카테고리	uint32	URL 카테고리를 지정하는 숫자입니다. 자세한 정보는 URL 카테고리 레코드 메타데이터, 4-24페이지의 내용을 참조하십시오.
URL 평판	uint32	URL 평판의 ID 번호입니다. URL 평판 레코드 메타데이터, 4-25페이지의 내용을 참조하십시오.
문자열 블록 유형	uint32	URL이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0으로 설정됩니다. 문자열 블록에 대한 자세한 정보는 문자열 데이터 블록, 4-72페이지의 내용을 참조하십시오.
문자열 블록 길이	uint32	이벤트 설명 문자열 블록의 바이트 수입니다. 여기에는 문자열 블록 유형의 4바이트 + 문자열 블록 길이의 4바이트 + URL의 바이트 수가 포함됩니다.
URL	string	상관관계 이벤트를 트리거한 URL입니다.
클라이언트 ID	uint32	이벤트를 탐지한 클라이언트의 ID 번호입니다.

표 3-25 5.4 이상 버전용 상관관계 이벤트 데이터 필드 (계속)

필드	데이터 유형	설명
문자열 블록 유형	uint32	클라이언트 버전이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0으로 설정됩니다. 문자열 블록에 대한 자세한 정보는 문자열 데이터 블록, 4-72페이지의 내용을 참조하십시오.
문자열 블록 길이	uint32	이벤트 설명 문자열 블록의 바이트 수입니다. 여기에는 문자열 블록 유형의 4바이트 + 문자열 블록 길이의 4바이트 + 클라이언트 버전의 바이트 수가 포함됩니다.
클라이언트 버전	string	이벤트를 탐지한 클라이언트의 버전입니다.
액세스 제어 정책 수정	uint8[16]	트리거된 상관관계와 관련된 규칙의 수정 번호입니다.
액세스 제어 규칙 ID	uint32	이벤트를 트리거한 규칙의 내부 식별자입니다.
인그레스 인터페이스 UUID	uint8[16]	상관관계 이벤트와 관련된 인그레스 인터페이스의 고유 식별자 역할을 하는 인터페이스 ID입니다.
이그레스(egress) 인터페이스 UUID	uint8[16]	상관관계 이벤트와 관련된 이그레스(egress) 인터페이스의 고유 식별자 역할을 하는 인터페이스 ID입니다.
인그레스 영역 UUID	uint8[16]	상관관계 이벤트와 관련된 인그레스 보안 영역의 고유 식별자 역할을 하는 영역 ID입니다.
이그레스(egress) 영역 UUID	uint8[16]	상관관계 이벤트와 관련된 이그레스(egress) 보안 영역의 고유 식별자 역할을 하는 영역 ID입니다.
소스 IPv6 주소	uint8[16]	이벤트의 소스 호스트 IP 주소(IPv6 주소 옥텟 형식)입니다.
대상 IPv6 주소	uint8[16]	이벤트의 대상 호스트 IP 주소(IPv6 주소 옥텟 형식)입니다.
소스 국가	uint16	소스 호스트의 국가 코드입니다.
대상 국가	uint16	대상 호스트의 국가 코드입니다.
보안 인텔리전스 UUID	uint8[16]	보안 인텔리전스용으로 구성된 액세스 제어 정책의 UUID입니다.
보안 상황	uint8[16]	트래픽이 통과한 보안 상황(가상 방화벽)의 ID 번호입니다. 이 필드는 다중 컨텍스트 모드의 ASA FirePOWER 디바이스에 대해서만 채워집니다.
SSL 정책 ID	uint8[16]	연결을 처리한 SSL 정책의 ID 번호입니다.
SSL 규칙 ID	uint32	연결을 처리한 SSL 규칙 또는 기본 동작의 ID 번호입니다.

표 3-25 5.4 이상 버전용 상관관계 이벤트 데이터 필드 (계속)

필드	데이터 유형	설명
SSL 실제 작업	uint32	SSL 규칙에 기반한 연결에서 수행된 작업입니다. 규칙에 명시된 작업이 가능하지 않을 수도 있으므로, 이는 예상 작업과 다를 수 있습니다. 가능한 값은 다음과 같습니다. • 0 - '알 수 없음' • 1 - '암호 해독 안 함' • 2 - '차단' • 3 - '차단 및 재설정' • 4 - '암호 해독(알려진 키)' • 5 - '암호 해독(키 교체)' • 6 - '암호 해독(재서명)'

표 3-25 5.4 이상 버전용 상관관계 이벤트 데이터 필드 (계속)

필드	데이터 유형	설명
SSL 플로우 상태	uint32	SSL 플로우의 상태입니다. 이 값은 작업을 수행한 이유 또는 오류 메시지가 표시된 이유를 설명합니다. 가능한 값은 다음과 같습니다. • 0 - '알 수 없음' • 1 - '일치하지 않음' • 2 - '성공' • 3 - '캐시되지 않은 세션' • 4 - '알 수 없는 암호 그룹' • 5 - '지원되지 않는 암호 그룹' • 6 - '지원되지 않는 SSL 버전' • 7 - 'SSL 압축 사용됨' • 8 - '패시브 모드에서 세션 암호 해독 불가' • 9 - '핸드셰이크 오류' • 10 - '암호 해독 오류' • 11 - '서버 이름 카테고리 조회 보류 중' • 12 - '공용 이름 카테고리 조회 보류 중' • 13 - '내부 오류' • 14 - '네트워크 파라미터 사용 불가' • 15 - '유효하지 않은 서버 인증서 핸들' • 16 - '서버 인증서 핑거프린트 사용 불가' • 17 - '주체 DN을 캐시할 수 없음' • 18 - '발급자 DN을 캐시할 수 없음' • 19 - '알 수 없는 SSL 버전' • 20 - '외부 인증서 목록 사용 불가' • 21 - '외부 인증서 핑거프린트 사용 불가' • 22 - '내부 인증서 목록이 유효하지 않음' • 23 - '내부 인증서 목록 사용 불가' • 24 - '내부 인증서 사용 불가' • 25 - '내부 인증서 핑거프린트 사용 불가' • 26 - '서버 인증서 검증 사용 불가' • 27 - '서버 인증서 검증 장애' • 28 - '유효하지 않은 작업'
SSL 인증서 핑거프린트	uint8[20]	SSL 서버 인증서의 SHA1 해시입니다.

계열 2 데이터 블록 이해

버전 4.10.0부터 eStreamer 서비스는 두 번째 데이터 블록 계열을 사용하여 침입 이벤트 추가 데이터 등의 특정 레코드를 패키징합니다. 해당 계열의 모든 블록 유형 목록은 표 3-26, 3-57페이지의 내용을 참조하십시오. 계열 2 블록은 계열 1 블록과 마찬가지로 가변 길이 필드 및 중첩 블록 계층 구조를 지원합니다. 계열 2 블록 유형에는 계열 1 기본 형식 블록 유형과 동일한 중첩 내부 블록 캡슐화용 메커니즘을 제공하는 기본 형식 블록이 포함되어 있습니다. 하지만 계열 2 블록과 계열 1 블록은 각각 별도의 번호 매기기 시스템을 사용합니다.

다음 예시에서는 기본 형식 블록을 사용하는 방법을 보여줍니다. 목록 데이터 블록(계열 2 블록 유형 31)은 운영 체제 핑거프린트(각각 가변 길이의 유형 87 블록 자체) 어레이를 정의합니다. 전체 유형 31 데이터 블록 길이는 Data Block Length(데이터 블록 길이) 필드에 자동으로 표시됩니다. 이 필드에는 블록 유형과 블록 길이 필드의 8바이트를 제외한 메시지의 데이터 부분 길이가 포함됩니다.

다음 표의 데이터 블록 상태 필드에는 해당 블록이 현재 블록(최신 버전)인지 아니면 레거시 블록(이전 버전에서 사용되며 eStreamer를 통해 계속 요청할 수는 있음)인지가 나와 있습니다.

표 3-26 계열 2 블록 유형

유형	콘텐츠	데이터 블록 상태	설명
0	문자열	현재	변수 문자열 데이터를 캡슐화합니다. 자세한 정보는 문자열 데이터 블록, 3-61페이지의 내용을 참조하십시오.
1	BLOB	현재	이진 데이터를 캡슐화합니다. 배너 전용으로 사용됩니다. 자세한 정보는 BLOB 데이터 블록, 3-62페이지의 내용을 참조하십시오.
2	목록	현재	다른 데이터 블록의 목록을 캡슐화합니다. 자세한 정보는 목록 데이터 블록, 3-62페이지의 내용을 참조하십시오.
3	일반 목록	현재	다른 데이터 블록의 목록을 캡슐화합니다. 역직렬화의 경우 목록 데이터 블록과 동일합니다. 자세한 정보는 일반 목록 데이터 블록, 3-63페이지의 내용을 참조하십시오.
4	이벤트 추가 데이터	현재	침입 이벤트 추가 데이터를 포함합니다. 자세한 정보는 침입 이벤트 추가 데이터 레코드, 3-27페이지의 내용을 참조하십시오.

표 3-26 계열 2 블록 유형 (계속)

유형	콘텐츠	데이터 블록 상태	설명
5	추가 데이터 유형	현재	추가 데이터 메타데이터를 포함합니다. 자세한 정보는 침입 이벤트 추가 데이터 메타데이터, 3-28페이지의 내용을 참조하십시오.
14	UUID 문자열 매핑	현재	여러 메타데이터 메시지에서 UUID 값을 설명 문자열에 매핑하는 데 사용되는 블록입니다. UUID 문자열 매핑 데이터 블록, 3-64페이지의 내용을 참조하십시오.
15	액세스 제어 정책 규칙 ID 메타데이터	현재	액세스 제어 규칙의 메타데이터를 포함합니다. 액세스 제어 정책 규칙 ID 메타데이터 블록, 3-66페이지의 내용을 참조하십시오.
16	악성코드 이벤트	레거시	Cisco Advanced Malware Protection 클라우드 내에서 탐지 또는 격리된 악성코드, 탐지 방법, 악성코드의 영향을 받은 호스트 및 사용자와 같은 악성코드 이벤트에 대한 정보가 포함됩니다. 5.1 버전용 악성코드 이벤트 데이터 블록, B-48페이지의 내용을 참조하십시오. 블록 24(5.3.1 버전용 악성코드 이벤트 데이터 블록, B-73페이지)에 의해 사용이 중단됩니다.
19	ICMP 유형 데이터 블록	현재	ICMP 유형을 설명하는 메타데이터를 포함합니다. ICMP 유형 데이터 블록, 3-67페이지의 내용을 참조하십시오.
20	ICMP 코드 데이터 블록	현재	ICMP 코드를 설명하는 메타데이터를 포함합니다. ICMP 코드 데이터 블록, 3-69페이지의 내용을 참조하십시오.
21	액세스 제어 정책 규칙 이유 데이터 블록	현재	액세스 제어 정책 규칙 이유를 설명하는 정보를 포함합니다. 6.0 이상 버전용 액세스 제어 정책 규칙 이유 데이터 블록, 3-79페이지의 내용을 참조하십시오.
22	IP 평판 카테고리 데이터 블록	현재	IP 주소가 차단된 이유를 설명하는 IP 평판 카테고리에 대한 정보를 포함합니다. 액세스 제어 정책 이름 데이터 블록, 3-82페이지의 내용을 참조하십시오.
23	파일 이벤트	레거시	소스, SHA 해시, 파일의 상태 등 파일 이벤트에 대한 정보를 포함합니다. 5.1.1.x 버전용 파일 이벤트, B-226페이지의 내용을 참조하십시오. 이는 블록 유형 32(액세스 제어 정책 규칙 ID 메타데이터 블록, 3-66페이지)로 대체됩니다.
24	악성코드 이벤트	레거시	Cisco Advanced Malware Protection 클라우드 내에서 탐지 또는 격리된 악성코드, 탐지 방법, 악성코드의 영향을 받은 호스트 및 사용자와 같은 악성코드 이벤트에 대한 정보가 포함됩니다. 5.1.1.x 버전용 악성코드 이벤트 데이터 블록, B-53페이지의 내용을 참조하십시오. 블록 16(5.1 버전용 악성코드 이벤트 데이터 블록, B-48페이지)의 사용을 중단하며 블록 33(5.3.1 버전용 악성코드 이벤트 데이터 블록, B-73페이지)에 의해 사용이 중단됩니다.

표 3-26 계열 2 블록 유형 (계속)

유형	콘텐츠	데이터 블록 상태	설명
25	침입 이벤트	레거시	침입 이벤트와 연결 및 악성코드 이벤트의 일치 여부를 확인하기 위한 정보를 비롯하여 침입 이벤트에 대한 정보를 포함합니다. 5.1.1.x 버전용 침입 이벤트 레코드, B-25페이지의 내용을 참조하십시오. 블록 34(5.2.x 버전용 침입 이벤트 레코드, B-12페이지)에 의해 사용이 중단됩니다.
26	파일 이벤트 SHA 해시	레거시	악성코드가 들어 있는 것으로 식별된 파일의 이름과 SHA 해시를 포함합니다. 5.1.1~5.2.x 버전용 파일 이벤트 SHA 해시, B-257페이지의 내용을 참조하십시오. 블록 40(5.3 이상 버전용 파일 이벤트 SHA 해시, 3-104페이지)에 의해 사용이 중단됩니다.
27	규칙 문서 데이터 블록	현재	이벤트를 생성하는 데 사용되는 규칙에 대한 정보를 포함합니다. 자세한 정보는 5.2 이상 버전용 규칙 문서 데이터 블록, 3-106페이지의 내용을 참조하십시오.
28	지리위치 데이터 블록	현재	국가 코드 및 관련 국가 이름을 포함합니다. 5.2 이상 버전용 지리위치 데이터 블록, 3-115페이지의 내용을 참조하십시오.
32	파일 이벤트	레거시	소스, SHA 해시, 파일의 상태 등 파일 이벤트에 대한 정보를 포함합니다. 5.2.x 버전용 파일 이벤트, B-230페이지의 내용을 참조하십시오. 5.1.1.x 버전용 파일 이벤트, B-226페이지의 사용을 중단하며 블록 38(5.3 버전용 파일 이벤트, B-234페이지)에 의해 사용이 중단됩니다.
33	악성코드 이벤트	현재	Cisco Advanced Malware Protection 클라우드 내에서 탐지 또는 격리된 악성코드, 탐지 방법, 악성코드의 영향을 받은 호스트 및 사용자와 같은 악성코드 이벤트에 대한 정보가 포함됩니다. 5.2.x 버전용 악성코드 이벤트 데이터 블록, B-59페이지의 내용을 참조하십시오. 블록 24(5.1.1.x 버전용 악성코드 이벤트 데이터 블록, B-53페이지)의 사용을 중단하며 블록 35(5.3 버전용 악성코드 이벤트 데이터 블록, B-66페이지)에 의해 사용이 중단됩니다.
34	침입 이벤트	레거시	침입 이벤트와 연결 및 악성코드 이벤트의 일치 여부를 확인하기 위한 정보를 비롯하여 침입 이벤트에 대한 정보를 포함합니다. 5.2.x 버전용 침입 이벤트 레코드, B-12페이지의 내용을 참조하십시오. 블록 25의 사용을 중단하며 블록 41(5.3 버전용 침입 이벤트 레코드, B-19페이지)에 의해 사용이 중단됩니다.
35	악성코드 이벤트	레거시	IOC 정보를 비롯하여 악성코드 이벤트에 대한 정보를 포함합니다. 5.3 버전용 악성코드 이벤트 데이터 블록, B-66페이지의 내용을 참조하십시오. 블록 33(5.2.x 버전용 악성코드 이벤트 데이터 블록, B-59페이지)의 사용을 중단하며 블록 44(5.3 버전용 악성코드 이벤트 데이터 블록, B-66페이지)에 의해 사용이 중단됩니다.

표 3-26 계열 2 블록 유형 (계속)

유형	콘텐츠	데이터 블록 상태	설명
38	파일 이벤트	레거시	소스, SHA 해시, 파일의 상태 등 파일 이벤트에 대한 정보를 포함합니다. 5.3 버전용 파일 이벤트, B-234페이지의 내용을 참조하십시오. 이는 블록 32의 사용을 중단하며 블록 43(6.0 이상 버전용 악성코드 이벤트 데이터 블록, 3-94페이지)에 의해 사용이 중단됩니다.
39	IOC 이름 데이터 블록	현재	IOC에 대한 정보를 포함합니다. 5.3 이상 버전용 IOC 이름 데이터 블록, 4-37페이지의 내용을 참조하십시오.
40	파일 이벤트 SHA 해시	현재	악성코드가 들어 있는 것으로 식별된 파일의 이름과 SHA 해시를 포함합니다. 5.3 이상 버전용 파일 이벤트 SHA 해시, 3-104페이지의 내용을 참조하십시오. 블록 26(5.1.1~5.2.x 버전용 파일 이벤트 SHA 해시, B-257페이지)의 사용을 중단합니다.
41	침입 이벤트	레거시	침입 이벤트와 IOC의 일치 여부를 확인하기 위한 정보를 비롯하여 침입 이벤트에 대한 정보를 포함합니다. 5.3 버전용 침입 이벤트 레코드, B-19페이지의 내용을 참조하십시오. 블록 34의 사용을 중단하며 블록 42(5.3.1 버전용 침입 이벤트 레코드, B-31페이지)에 의해 사용이 중단됩니다.
42	침입 이벤트	현재	침입 이벤트와 IOC의 일치 여부를 확인하기 위한 정보를 비롯하여 침입 이벤트에 대한 정보를 포함합니다. 5.3.1 버전용 침입 이벤트 레코드, B-31페이지의 내용을 참조하십시오. 블록 41(5.3 버전용 침입 이벤트 레코드, B-19페이지)의 사용을 중단합니다.
43	파일 이벤트	레거시	소스, SHA 해시, 파일의 상태 등 파일 이벤트에 대한 정보를 포함합니다. 5.3.1 버전용 파일 이벤트, B-240페이지의 내용을 참조하십시오. 블록 38(5.3 버전용 파일 이벤트, B-234페이지)의 사용을 중단하며 블록 46(6.0 이상 버전용 파일 이벤트, 3-84페이지)에 의해 사용이 중단됩니다.
44	악성코드 이벤트	레거시	IOC 정보를 비롯하여 악성코드 이벤트에 대한 정보를 포함합니다. 6.0 이상 버전용 악성코드 이벤트 데이터 블록, 3-94페이지의 내용을 참조하십시오. 블록 35(5.3 버전용 악성코드 이벤트 데이터 블록, B-66페이지)의 사용을 중단하며 블록 47(6.0 이상 버전용 악성코드 이벤트 데이터 블록, 3-94페이지)에 의해 사용이 중단됩니다.
46	파일 이벤트	현재	소스, SHA 해시, 파일의 상태 등 파일 이벤트에 대한 정보를 포함합니다. 6.0 이상 버전용 악성코드 이벤트 데이터 블록, 3-94페이지의 내용을 참조하십시오. 블록 43(5.3.1 버전용 파일 이벤트, B-240페이지)의 사용을 중단합니다.
47	악성코드 이벤트	현재	IOC 정보를 비롯하여 악성코드 이벤트에 대한 정보를 포함합니다. 6.0 이상 버전용 악성코드 이벤트 데이터 블록, 3-94페이지의 내용을 참조하십시오. 블록 44(5.3.1 버전용 악성코드 이벤트 데이터 블록, B-73페이지)의 사용을 중단합니다.

계열 2 기본 형식 데이터 블록

계열 2 및 계열 1 블록에는 모두 메시지 내의 가변 길이 문자열/BLOB 및 가변 길이 블록 목록을 캡슐화하는 데 사용되는 기본 형식 집합이 포함되어 있습니다. 이러한 기본 형식 블록은 위의 데이터 블록 헤더, 2-25페이지에 설명되어 있는 표준 eStreamer 블록 헤더를 포함하지만 다른 데이터 블록 내에만 표시됩니다. 지정된 블록 유형에는 어떤 숫자든 포함할 수 있습니다. 이러한 블록의 구조에 대한 자세한 내용은 다음 페이지를 참조하십시오.

- 문자열 데이터 블록, 3-61페이지
- BLOB 데이터 블록, 3-62페이지
- 목록 데이터 블록, 3-62페이지
- 일반 목록 데이터 블록, 3-63페이지
- UUID 문자열 매핑 데이터 블록, 3-64페이지
- 이름 설명 매핑 데이터 블록, 3-65페이지

문자열 데이터 블록

eStreamer 서비스는 문자열 데이터 블록을 문자열 데이터를 메시지에 포함해 전송합니다. 이 블록은 대개 운영 체제 또는 서버 이름 등을 식별하기 위한 용도로 다른 데이터 블록 내에 표시됩니다.

데이터는 포함하지 않으며 헤더 필드만 포함하는 빈 문자열 데이터 블록의 블록 길이는 8입니다. 운영 체제 벤더를 알 수 없어 운영 체제 데이터 블록의 OS Vendor(OS 벤더) 문자열 필드에 콘텐츠가 없는 경우와 같이 문자열 값의 콘텐츠가 없으면 eStreamer에서는 빈 문자열 데이터 블록을 사용합니다.

계열 2 블록 그룹에서 문자열 데이터 블록의 블록 유형은 0입니다.

참고 이 데이터 블록에서 반환되는 문자열이 항상 null로 종료되는 것은 아닙니다. 즉, 문자열 문자 뒤에 항상 0이 오는 것은 아닙니다.

다음 다이어그램에 문자열 데이터 블록의 형식이 나와 있습니다.

다음 표에는 문자열 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 3-27 문자열 블록 필드

필드	데이터 유형	설명
데이터 블록 유형	uint32	문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
데이터 블록 길이	uint32	문자열 데이터 블록 헤더와 문자열 데이터를 합한 길이(바이트 단위)입니다.
문자열 데이터	string	문자열 데이터를 포함하며, 문자열 끝에 종료 문자(null 바이트)를 포함할 수도 있습니다.

BLOB 데이터 블록

eStreamer 서비스는 BLOB 데이터 블록을 사용하여 이진 데이터를 전달합니다. 예를 들어 호스트 검색 레코드는 BLOB 블록을 사용하여 캡처한 서버 배너를 저장합니다. 계열 2 블록 그룹에서 BLOB 데이터 블록의 블록 유형은 1입니다.

다음 다이어그램에 BLOB 데이터 블록의 형식이 나와 있습니다.

다음 표에는 BLOB 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 3-28 BLOB 데이터 블록 필드

필드	데이터 유형	설명
데이터 블록 유형	uint32	BLOB 데이터 블록을 시작합니다. 이 값은 항상 1입니다.
데이터 블록 길이	uint32	BLOB 데이터 블록의 바이트 수입니다. 여기에는 BLOB 블록 유형 및 길이 필드의 8바이트에 그 뒤의 이진 데이터 길이를 더한 값이 포함됩니다.
이진 데이터	variable	서버 배너 등의 이진 데이터를 포함합니다.

목록 데이터 블록

eStreamer 서비스는 목록 데이터 블록을 사용하여 데이터 블록 목록을 캡슐화합니다. 예를 들어 eStreamer는 목록 데이터 블록을 사용하여 TCP 서버 목록(각 TCP 서버 자체가 데이터 블록임)을 전송할 수 있습니다. 계열 2 블록 그룹에서 목록 데이터 블록의 블록 유형은 2입니다.

다음 다이어그램에 목록 데이터 블록의 기본 형식이 나와 있습니다.

다음 표에는 목록 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 3-29 목록 데이터 필드

필드	데이터 유형	설명
블록 유형	uint32	목록 데이터 블록을 시작합니다. 이 값은 항상 2입니다.
블록 길이	uint32	목록 블록과 캡슐화된 데이터의 바이트 수입니다. 예를 들어 목록에 하위 서버 데이터 블록 3개가 포함되어 있으면 이 값에는 하위 서버 블록의 총 바이트 수에 목록 블록 헤더의 8바이트를 더한 값이 포함됩니다.
캡슐화된 데이터 블록	variable	캡슐화된 데이터 블록(목록 블록 길이의 최대 바이트 수까지)입니다.

일반 목록 데이터 블록

eStreamer 서비스는 일반 목록 데이터 블록을 사용하여 데이터 블록 목록을 캡슐화합니다. 예를 들어 호스트 프로파일 데이터 블록은 여러 클라이언트 애플리케이션에 대한 정보를 포함하며 일반 목록 블록을 사용하여 클라이언트 애플리케이션 데이터 블록 목록을 메시지에 포함합니다. 계열 2 블록 그룹에서 일반 목록 데이터 블록의 블록 유형은 3입니다.

다음 다이어그램에 일반 목록 데이터 블록의 기본 구조가 나와 있습니다.

다음 표에는 일반 목록 데이터 블록의 필드에 대한 설명이 나와 있습니다.

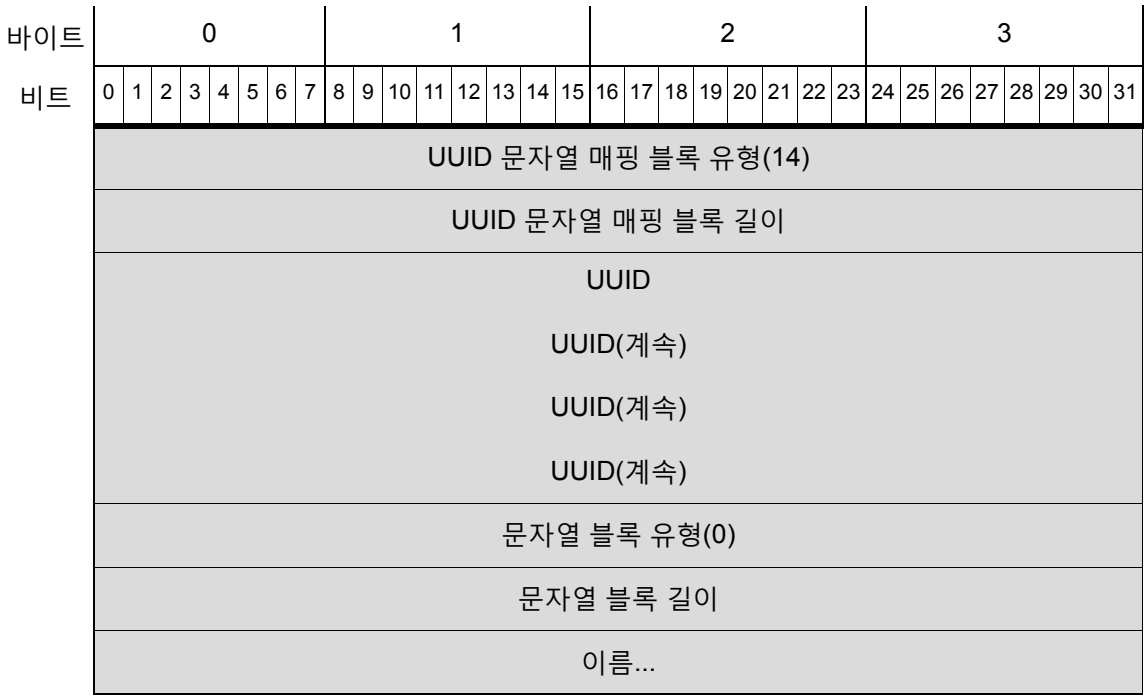
표 3-30 일반 목록 데이터 블록 필드

필드	바이트 수	설명
데이터 블록 유형	uint32	일반 목록 데이터 블록을 시작합니다. 이 값은 항상 3입니다.
데이터 블록 길이	uint32	일반 목록 블록과 캡슐화된 데이터 블록의 바이트 수입니다. 이 수에는 일반 목록 블록 헤더 필드의 8바이트에 캡슐화된 모든 데이터 블록의 총 바이트 수를 더한 값이 포함됩니다.
캡슐화된 데이터 블록	variable	캡슐화된 데이터 블록(일반 목록 블록 길이의 최대 바이트 수까지)입니다.

UUID 문자열 매핑 데이터 블록

eStreamer 서비스는 여러 메타데이터 메시지에서 UUID 문자열 매핑 데이터 블록을 사용하여 UUID 값을 설명 문자열에 매핑합니다. 계열 2에서 UUID 문자열 매핑 데이터 블록의 블록 유형은 14입니다.

다음 다이어그램에 UUID 문자열 매핑 데이터 블록의 구조가 나와 있습니다.



다음 표에는 UUID 문자열 매핑 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 3-31 UUID 문자열 매핑 데이터 블록 필드

필드	데이터 유형	설명
UUID 문자열 매핑 블록 유형	uint32	UUID 문자열 매핑 블록을 시작합니다. 이 값은 항상 14입니다.
UUID 문자열 매핑 블록 길이	uint32	UUID 문자열 매핑 블록의 총 바이트 수입니다. 여기에는 UUID 문자열 매핑 블록 유형 및 길이 필드의 8바이트에 그 뒤의 데이터 바이트 수를 더한 값이 포함됩니다.
UUID	uint8[16]	UUID가 식별하는 이벤트나 기타 개체의 고유 식별자입니다. 이 필드는 이 레코드의 고유 키입니다.
문자열 블록 유형	uint32	UUID와 관련된 설명 이름을 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Name(이름) 필드의 바이트 수를 더한 값이 포함됩니다.
이름	string	설명 이름입니다.

이름 설명 매핑 데이터 블록

eStreamer 서비스는 여러 메타데이터 메시지에서 이름 설명 매핑 데이터 블록을 사용하여 ID 값을 이름 및 설명 문자열에 매핑합니다. 계열 2에서 이름 설명 매핑 데이터 블록의 블록 유형은 61입니다.

다음 다이어그램에 이름 설명 매핑 데이터 블록의 구조가 나와 있습니다.

다음 표에는 이름 설명 매핑 데이터 블록의 필드에 대한 설명이 나와 있습니다.

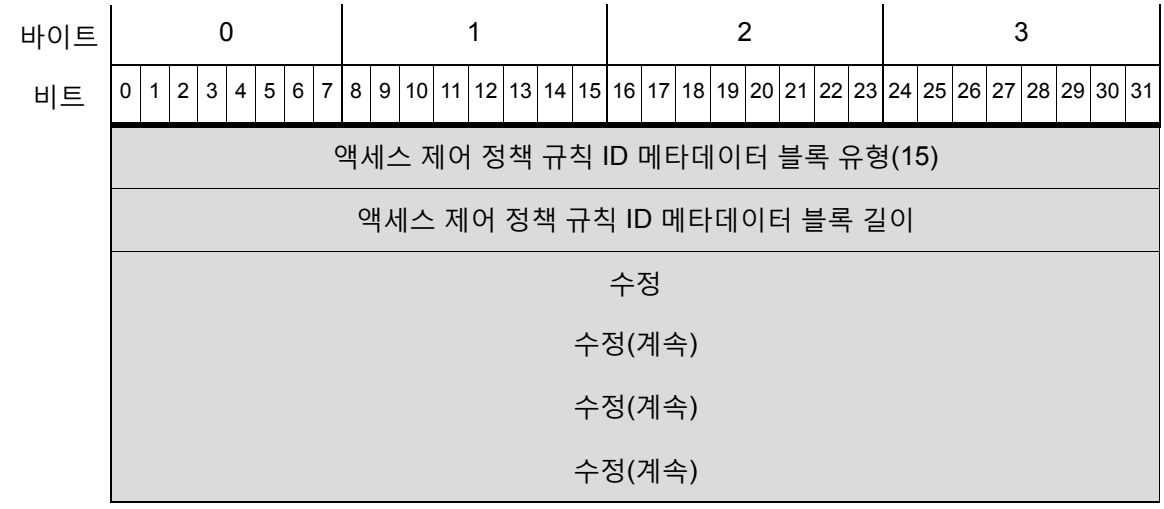
표 3-32 이름 설명 매핑 데이터 블록 필드

필드	데이터 유형	설명
이름 설명 매핑 블록 유형	uint32	이름 설명 매핑 블록을 시작합니다. 이 값은 항상 61입니다.
이름 설명 매핑 블록 길이	uint32	이름 설명 매핑 블록의 총 바이트 수입니다. 여기에는 이름 설명 매핑 블록 유형 및 길이 필드의 8바이트에 그 뒤의 데이터 바이트 수를 더한 값이 포함됩니다.
ID	unit32	ID가 식별하는 이벤트나 기타 개체의 고유 식별자입니다. 이 필드는 이 레코드의 고유 키입니다.
문자열 블록 유형	uint32	ID와 관련된 이름을 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Name(이름) 필드의 바이트 수를 더한 값이 포함됩니다.
이름	string	이벤트 또는 개체의 이름입니다.
문자열 블록 유형	uint32	ID와 관련된 설명을 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	설명 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Description(설명) 필드의 바이트 수를 더한 값이 포함됩니다.
설명	string	ID와 관련된 개체 또는 이벤트의 설명입니다.

액세스 제어 정책 규칙 ID 메타데이터 블록

eStreamer 서비스는 액세스 제어 정책 규칙 ID 메타데이터 블록을 사용하여 액세스 제어 정책 규칙 ID에 대한 정보를 포함합니다. 계열 2에서 이 데이터 블록의 블록 유형은 15입니다.

다음 다이어그램에 액세스 제어 정책 규칙 ID 메타데이터 블록의 구조가 나와 있습니다.



다음 표에는 액세스 제어 정책 규칙 ID 메타데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 3-33 액세스 제어 정책 규칙 ID 메타데이터 블록 필드

필드	데이터 유형	설명
액세스 제어 정책 규칙 ID 메타데이터 블록 유형	uint32	액세스 제어 정책 규칙 ID 메타데이터 블록을 시작합니다. 이 값은 항상 15입니다.
액세스 제어 정책 규칙 ID 메타데이터 블록 길이	uint32	액세스 제어 정책 규칙 ID 블록의 총 바이트 수입니다. 여기에는 액세스 제어 정책 규칙 ID 메타데이터 블록 유형 및 길이 필드의 8바이트에 그 뒤의 데이터 바이트 수를 더한 값이 포함됩니다.
수정	uint8[16]	트리거된 상관관계와 관련된 규칙의 수정 번호입니다.
규칙 ID	uint32	이벤트를 트리거한 규칙의 내부 식별자입니다. 이 필드는 이 레코드의 고유 키입니다.
문자열 블록 유형	uint32	액세스 제어 정책 규칙과 관련된 설명 이름을 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Name(이름) 필드의 바이트 수를 더한 값이 포함됩니다.
이름	string	액세스 제어 정책 규칙의 설명 이름입니다.

ICMP 유형 데이터 블록

eStreamer 서비스는 ICMP 유형 데이터 블록을 사용하여 ICMP 유형에 대한 정보를 포함합니다. 이 데이터 블록의 레코드 유형은 260이고 블록 유형은 계열 2의 19입니다.

다음 다이어그램에 ICMP 유형 데이터 블록의 구조가 나와 있습니다.

다음 표에는 ICMP 유형 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 3-34 ICMP 유형 데이터 블록 필드

필드	데이터 유형	설명
ICMP 유형 데이터 블록 유형	uint32	ICMP 유형 데이터 블록을 시작합니다. 이 값은 항상 19입니다.
ICMP 유형 데이터 블록 길이	uint32	ICMP 유형 데이터 블록의 총 바이트 수입니다. 여기에는 ICMP 유형 데이터 블록 유형 및 길이 필드의 8바이트에 그 뒤의 데이터 바이트 수를 더한 값이 포함됩니다.
유형	uint16	이벤트의 ICMP 유형입니다.
프로토콜	uint16	IANA에서 지정한 프로토콜 번호입니다. 예를 들면 다음과 같습니다. • 0 - IP • 1 - ICMP • 6 - TCP • 17 - UDP
문자열 블록 유형	uint32	ICMP 유형의 설명이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Description(설명) 필드의 바이트 수를 더한 값이 포함됩니다.
설명	string	이벤트에 대한 ICMP 유형 설명입니다.

ICMP 코드 데이터 블록

eStreamer 서비스는 ICMP 코드 데이터 블록을 사용하여 액세스 제어 정책 규칙 ID에 대한 정보를 포함합니다. 이 데이터 블록의 레코드 유형은 270이고 블록 유형은 계열 2의 20입니다.

다음 다이어그램에 액세스 제어 정책 규칙 ID 메타데이터 블록의 구조가 나와 있습니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	헤더 버전(1)																메시지 유형(4)															
	메시지 길이																															
	네트워크 맵 ID																레코드 유형(270)															
	ICMP 코드 데이터 블록 유형(20)																															
	ICMP 코드 데이터 블록 길이																															
	코드																유형															
설명	프로토콜																문자열 블록 유형(0)															
	문자열 블록 유형(0)(계속)																문자열 블록 길이															
	문자열 블록 길이(계속)																설명...															

다음 표에는 ICMP 코드 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 3-35 ICMP 코드 데이터 블록 필드

필드	데이터 유형	설명
ICMP 코드 데이터 블록 유형	uint32	ICMP 코드 데이터 블록을 시작합니다. 이 값은 항상 20입니다.
ICMP 코드 데이터 블록 길이	uint32	ICMP 코드 데이터 블록의 총 바이트 수입니다. 여기에는 ICMP 코드 데이터 블록 유형 및 길이 필드의 8바이트에 그 뒤의 데이터 바이트 수를 더한 값이 포함됩니다.
코드	uint16	이벤트의 ICMP 코드입니다.
유형	uint16	이벤트의 ICMP 유형입니다.
프로토콜	uint16	IANA에서 지정한 프로토콜 번호입니다. 예를 들면 다음과 같습니다. • 0 - IP • 1 - ICMP • 6 - TCP • 17 - UDP

표 3-35 ICMP 코드 데이터 블록 필드 (계속)

필드	데이터 유형	설명
문자열 블록 유형	uint32	ICMP 코드의 설명이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Description(설명) 필드의 바이트 수를 더한 값이 포함됩니다.
설명	string	이벤트에 대한 ICMP 코드 설명입니다.

5.4.1 이상 버전용 보안 인텔리전스 카테고리 메타데이터

eStreamer 서비스는 보안 인텔리전스 카테고리 정보가 포함된 메타데이터를 전송합니다. 해당 메타데이터의 형식은 아래에 나와 있습니다. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 보안 인텔리전스 카테고리 레코드임을 나타내는 282입니다.

다음 표에는 보안 상황 이름 레코드의 필드에 대한 설명이 나와 있습니다.

표 3-36 보안 상황 이름 레코드 필드

필드	데이터 유형	설명
보안 인텔리전스 UUID	uint8[16]	보안 인텔리전스의 UUID입니다. 이 필드는 이 레코드의 고유 키입니다.
문자열 블록 유형	uint32	보안 인텔리전스 카테고리가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	보안 인텔리전스 카테고리 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Profile Name(프로파일 이름) 필드의 바이트 수를 더한 값이 포함됩니다.
보안 인텔리전스 카테고리	string	보안 인텔리전스 카테고리입니다.

6.0 이상 버전용 영역 메타데이터

eStreamer 서비스는 영역 정보가 포함된 메타데이터를 전송합니다. 해당 메타데이터의 형식은 아래에 나와 있습니다. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 영역 메타데이터 레코드임을 나타내는 300입니다.

다음 표에는 영역 메타데이터 레코드의 필드에 대한 설명이 나와 있습니다.

표 3-37 영역 메타데이터 레코드 필드

필드	데이터 유형	설명
영역 ID	uint32	영역의 ID 번호입니다. 이 필드는 이 레코드의 고유 키입니다.
영역 이름 길이	uint32	영역 이름에 포함된 바이트 수입니다.
영역 이름	string	영역 이름입니다.

6.0 이상 버전용 엔드포인트 프로파일 데이터 블록

eStreamer 서비스는 엔드포인트 프로파일 데이터 블록을 사용하여 네트워크 엔드포인트에 대한 정보를 포함합니다. 이 데이터 블록의 레코드 유형은 301이고 블록 유형은 계열 2의 58입니다.

다음 다이어그램에 액세스 제어 정책 규칙 ID 메타데이터 블록의 구조가 나와 있습니다.

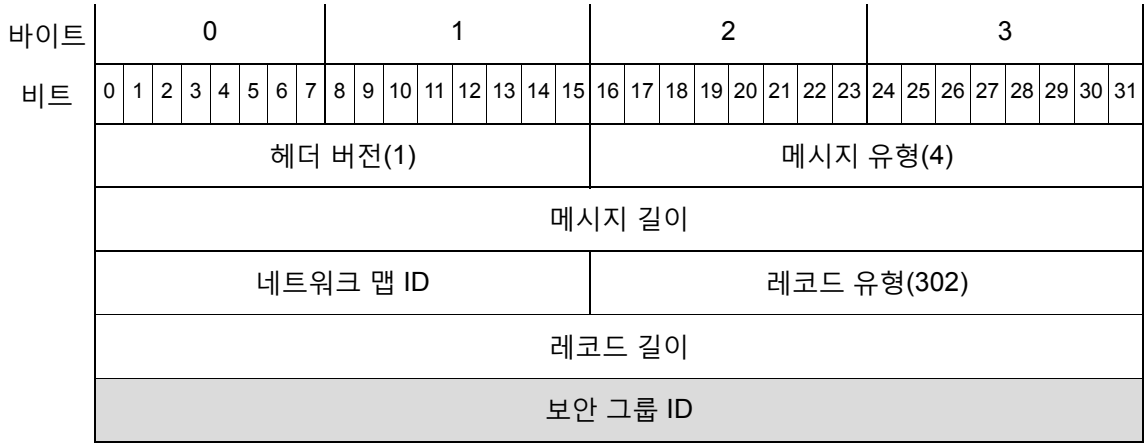
다음 표에는 엔드포인트 프로파일 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 3-38 엔드포인트 프로파일 데이터 블록 필드

필드	데이터 유형	설명
엔드포인트 프로파일 데이터 블록 유형	uint32	엔드포인트 프로파일 데이터 블록을 시작합니다. 이 값은 항상 58입니다.
엔드포인트 프로파일 데이터 블록 길이	uint32	엔드포인트 프로파일 데이터 블록의 총 바이트 수입니다. 여기에는 엔드포인트 프로파일 데이터 블록 유형 및 길이 필드의 8바이트에 그 뒤의 데이터 바이트 수를 더한 값이 포함됩니다.
ID	uint32	엔드포인트의 ID 번호입니다.
문자열 블록 유형	uint32	엔드포인트의 프로파일이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	프로파일 이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Profile Name(프로파일 이름) 필드의 바이트 수를 더한 값이 포함됩니다.
프로파일 이름	string	엔드포인트 프로파일의 이름입니다.
문자열 블록 유형	uint32	엔드포인트의 전체 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	전체 이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Full Name(전체 이름) 필드의 바이트 수를 더한 값이 포함됩니다.
전체 이름	string	엔드포인트 유형의 관계 계층 구조를 제공하는 프로파일의 FQN(Fully Qualified Name)입니다.

6.0 이상 버전용 보안 그룹 메타데이터

eStreamer 서비스는 보안 그룹 정보가 포함된 메타데이터를 전송합니다. 해당 메타데이터의 형식은 아래에 나와 있습니다. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 보안 그룹 메타데이터 레코드임을 나타내는 302입니다.



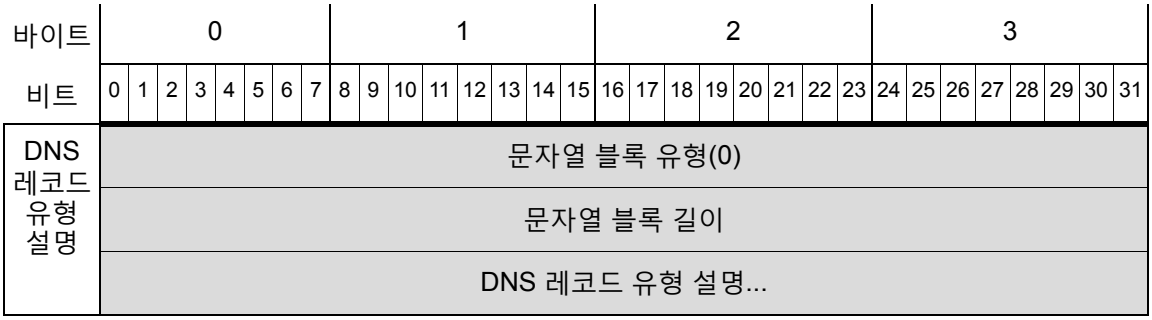
다음 표에는 보안 그룹 메타데이터 레코드의 필드에 대한 설명이 나와 있습니다.

표 3-39 보안 그룹 메타데이터 레코드 필드

필드	데이터 유형	설명
보안 그룹 ID	uint32	보안 그룹의 ID 번호입니다. 이 필드는 이 레코드의 고유 키입니다.
보안 그룹 이름 길이	uint32	보안 그룹 이름에 포함된 바이트 수입니다.
보안 그룹 이름	string	보안 그룹 이름입니다.

6.0 이상 버전용 DNS 레코드 유형 메타데이터

eStreamer 서비스는 DNS 레코드 유형 정보가 포함된 메타데이터를 전송합니다. 해당 메타데이터의 형식은 아래에 나와 있습니다. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 DNS 레코드 유형 메타데이터 레코드임을 나타내는 320입니다.



다음 표에는 DNS 레코드 유형 메타데이터 레코드의 필드에 대한 설명이 나와 있습니다.

표 3-40 DNS 레코드 유형 메타데이터 필드

필드	데이터 유형	설명
이름 설명 데이터 블록 유형	uint32	이름 설명 데이터 블록을 시작합니다. 이 값은 항상 61입니다.
이름 설명 데이터 블록 길이	uint32	이름 설명 데이터 블록의 총 바이트 수입니다. 여기에는 이름 설명 데이터 블록 유형 및 길이 필드의 8바이트에 그 뒤의 데이터 바이트 수를 더한 값이 포함됩니다.
DNS 레코드 ID	uint32	DNS 레코드의 ID 번호입니다. 이 필드는 이 레코드의 고유 키입니다.
문자열 블록 유형	uint32	DNS 레코드 유형의 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	DNS 레코드 유형 이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 DNS Record Type Name(DNS 레코드 유형 이름) 필드의 바이트 수를 더한 값이 포함됩니다.
DNS 레코드 유형 이름	string	DNS 레코드 유형의 이름입니다.
문자열 블록 유형	uint32	DNS 레코드 유형의 설명이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	DNS 레코드 유형 설명 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 DNS Record Type Description(DNS 레코드 유형 설명) 필드의 바이트 수를 더한 값이 포함됩니다.
DNS 레코드 유형 설명	string	DNS 레코드 유형의 설명입니다.

6.0 이상 버전용 DNS 응답 유형 메타데이터

eStreamer 서비스는 DNS 응답 유형 메타데이터를 전송합니다. 해당 메타데이터의 형식은 아래에 나와 있습니다. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 DNS 응답 유형 메타데이터 레코드임을 나타내는 321입니다.

다음 표에는 DNS 응답 유형 메타데이터 레코드의 필드에 대한 설명이 나와 있습니다.

표 3-41 DNS 응답 유형 메타데이터 필드

필드	데이터 유형	설명
이름 설명 데이터 블록 유형	uint32	이름 설명 데이터 블록을 시작합니다. 이 값은 항상 61입니다.
이름 설명 데이터 블록 길이	uint32	이름 설명 데이터 블록의 총 바이트 수입니다. 여기에는 이름 설명 데이터 블록 유형 및 길이 필드의 8바이트에 그 뒤의 데이터 바이트 수를 더한 값이 포함됩니다.
DNS 응답 ID	uint32	DNS 응답의 ID 번호입니다. 이 필드는 이 레코드의 고유 키입니다.

표 3-41 DNS 응답 유형 메타데이터 필드 (계속)

필드	데이터 유형	설명
문자열 블록 유형	uint32	DNS 응답 유형의 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	DNS 응답 유형 이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 DNS Response Type Name(DNS 응답 유형 이름) 필드의 바이트 수를 더한 값이 포함됩니다.
DNS 응답 유형 이름	string	DNS 응답 유형의 이름입니다.
문자열 블록 유형	uint32	DNS 응답 유형의 설명이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	DNS 응답 유형 설명 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 DNS Response Type Description(DNS 응답 유형 설명) 필드의 바이트 수를 더한 값이 포함됩니다.
DNS 응답 유형 설명	string	DNS 응답 유형의 설명입니다.

6.0 이상 버전용 싱크홀 메타데이터

eStreamer 서비스는 싱크홀 정보가 포함된 메타데이터를 전송합니다. 해당 메타데이터의 형식은 아래에 나와 있습니다. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 싱크홀 메타데이터 레코드임을 나타내는 322입니다.

다음 표에는 싱크홀 메타데이터 레코드의 필드에 대한 설명이 나와 있습니다.

표 3-42 싱크홀 메타데이터 레코드 필드

필드	데이터 유형	설명
UUID 문자열 데이터 블록 유형	uint32	UUID 문자열 데이터 블록을 시작합니다. 이 값은 항상 14입니다.
UUID 문자열 데이터 블록 길이	uint32	UUID 문자열 데이터 블록의 총 바이트 수입니다. 여기에는 UUID 문자열 데이터 블록 유형 및 길이 필드의 8바이트에 그 뒤의 데이터 바이트 수를 더한 값이 포함됩니다.
싱크홀 UUID	uint8[16]	싱크홀의 UUID 번호입니다. 이 필드는 이 레코드의 고유 키입니다.
문자열 블록 유형	uint32	싱크홀의 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	싱크홀 이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Sinkhole Name(싱크홀 이름) 필드의 바이트 수를 더한 값이 포함됩니다.
싱크홀 이름	string	싱크홀의 이름입니다.

6.0 이상 버전용 네트워크 맵 도메인 메타데이터

eStreamer 서비스는 네트워크 맵 도메인 정보가 포함된 메타데이터를 전송합니다. 해당 메타데이터의 형식은 아래에 나와 있습니다. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 네트워크 맵 도메인 메타데이터 레코드임을 나타내는 350입니다.

다음 표에는 네트워크 맵 도메인 메타데이터 레코드의 필드에 대한 설명이 나와 있습니다.

표 3-43 싱크홀 메타데이터 레코드 필드

필드	데이터 유형	설명
네트워크 맵 도메인 ID	uint32	네트워크 맵 도메인의 ID 번호입니다. 이 필드는 이 레코드의 고유 키입니다.
네트워크 맵 도메인 이름 길이	uint32	네트워크 맵 도메인 이름에 포함된 바이트 수입니다.
네트워크 맵 도메인 이름	string	네트워크 맵 도메인 이름입니다.

6.0 이상 버전용 액세스 제어 정책 규칙 이유 데이터 블록

eStreamer 서비스는 액세스 제어 규칙 정책 규칙 이유 데이터 블록을 사용하여 액세스 제어 정책 규칙 ID에 대한 정보를 포함합니다. 이 데이터 블록의 레코드 유형은 124이고 블록 유형은 계열 2의 59입니다. 이는 블록 유형 21을 대체합니다. Reason(이유) 필드의 크기는 16비트에서 32비트로 늘어났습니다.

다음 다이어그램에 액세스 제어 정책 규칙 ID 메타데이터 블록의 구조가 나와 있습니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	액세스 제어 정책 규칙 이유 데이터 블록 유형(59)																															
	액세스 제어 정책 규칙 이유 데이터 블록 길이																															
	이유																															
설명	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	설명...																															

다음 표에는 액세스 제어 정책 규칙 이유 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 3-44 액세스 제어 정책 규칙 이유 데이터 블록 필드

필드	데이터 유형	설명
액세스 제어 정책 규칙 이유 데이터 블록 유형	uint32	액세스 제어 정책 규칙 이유 데이터 블록을 시작합니다. 이 값은 항상 59입니다.
액세스 제어 정책 규칙 이유 데이터 블록 길이	uint32	액세스 제어 정책 규칙 이유 데이터 블록의 총 바이트 수입니다. 여기에는 액세스 제어 정책 규칙 이유 데이터 블록 유형 및 길이 필드의 8바이트에 그 뒤의 데이터 바이트 수를 더한 값이 포함됩니다.

표 3-44 액세스 제어 정책 규칙 이유 데이터 블록 필드 (계속)

필드	데이터 유형	설명
이유	uint32	이벤트를 트리거한 규칙에 대한 이유 번호입니다. 규칙 이유는 여러 비트가 설정되어 있을 수 있는 이진 비트맵입니다. 규칙 하나에 여러 가지 이유가 있을 수 있습니다. 비트 값은 다음과 같습니다. • **1** - IP 차단 • **2** - IP 모니터 • **4** - 사용자 우회 • **8** - 파일 모니터 • **16** - 악성코드 차단 • **32** - 침입 모니터 • **64** - 악성코드 차단 • **128** - 파일 다시 시작 차단 • **256** -파일 다시 시작 허용 • **512** - 파일 맞춤형 탐지 • **1024** - SSL 차단 • **2048** - DNS 차단 • **4096** - DNS 모니터 • **8192** - URL 차단 • **16384** - URL 모니터 • **32768** - 콘텐츠 제한 • **65536** - 지능형 앱 우회 • **131072** - WSA 위협
문자열 블록 유형	uint32	액세스 제어 정책 규칙 이유의 설명이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Description(설명) 필드의 바이트 수를 더한 값이 포함됩니다.
설명	string	규칙에 대한 이유의 설명입니다.

액세스 제어 정책 이름 데이터 블록

eStreamer 서비스는 액세스 제어 정책 이름 데이터 블록을 사용하여 액세스 제어 정책 이름에 대한 정보를 포함합니다. 계열 2에서 이 데이터 블록의 블록 유형은 64입니다.

다음 다이어그램에 액세스 제어 정책 이름 메타데이터 블록의 구조가 나와 있습니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	액세스 제어 정책 이름 데이터 블록 유형(64)																															
	액세스 제어 정책 이름 데이터 블록 길이																															
	액세스 제어 정책 UUID																															
	액세스 제어 정책 UUID(계속)																															
	액세스 제어 정책 UUID(계속)																															
	액세스 제어 정책 UUID(계속)																															
	센서 ID																															
이름	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	이름...																															

다음 표에는 액세스 제어 정책 이름 메타데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 3-45 액세스 제어 정책 정책 이름 데이터 블록 필드

필드	데이터 유형	설명
액세스 제어 정책 이름 데이터 블록 유형	uint32	액세스 제어 정책 이름 데이터 블록을 시작합니다. 이 값은 항상 64입니다.
액세스 제어 정책 이름 데이터 블록 길이	uint32	액세스 제어 정책 이름 데이터 블록의 총 바이트 수입니다. 여기에는 액세스 제어 정책 이름 데이터 블록 유형 및 길이 필드의 8바이트에 그 뒤의 데이터 바이트 수를 더한 값이 포함됩니다.
액세스 제어 정책 UUID	uint8[16]	액세스 제어 정책의 UUID입니다.
센서 ID	uint32	액세스 제어 정책과 관련된 센서의 ID 번호입니다.
문자열 블록 유형	uint32	액세스 제어 정책의 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.

표 3-45 액세스 제어 정책 정책 이름 데이터 블록 필드 (계속)

필드	데이터 유형	설명
문자열 블록 길이	uint32	이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Name(이름) 필드의 바이트 수를 더한 값이 포함됩니다.
이름	string	액세스 제어 정책의 이름입니다.

IP 평판 카테고리 데이터 블록

eStreamer 서비스는 IP 평판 카테고리 데이터 블록을 사용하여 규칙 평판 카테고리에 대한 정보를 포함합니다. 계열 2에서 이 데이터 블록의 블록 유형은 22입니다.

다음 다이어그램에 IP 평판 카테고리 데이터 블록의 구조가 나와 있습니다.

다음 표에는 IP 평판 카테고리 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 3-46 IP 평판 카테고리 데이터 블록 필드

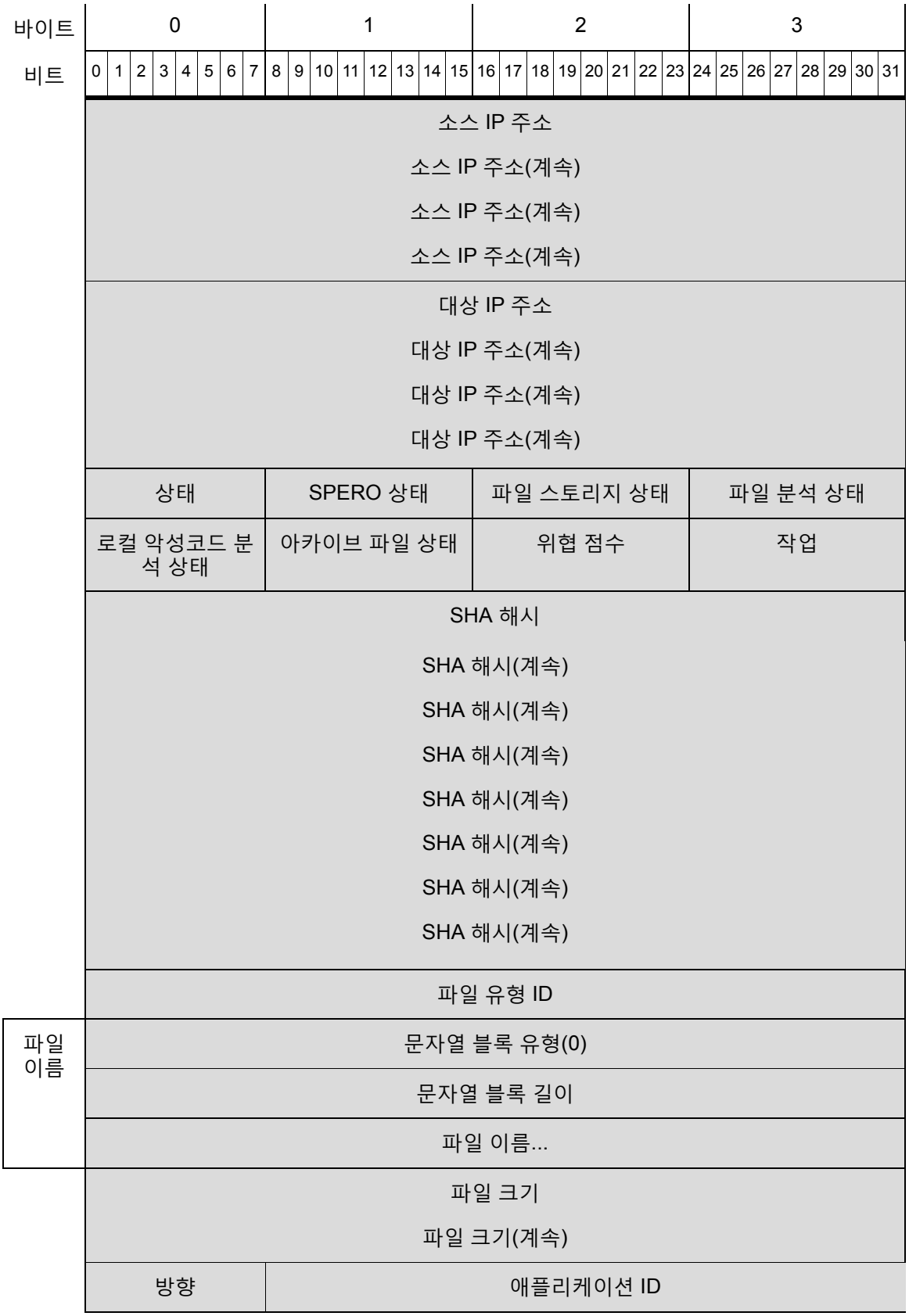
필드	데이터 유형	설명
IP 평판 카테고리 데이터 블록 유형	uint32	IP 평판 카테고리 데이터 블록을 시작합니다. 이 값은 항상 22입니다.
IP 평판 카테고리 데이터 블록 길이	uint32	IP 평판 카테고리 데이터 블록의 총 바이트 수입니다. 여기에는 IP 평판 카테고리 데이터 블록 유형 및 길이 필드의 8바이트에 그 뒤의 데이터 바이트 수를 더한 값이 포함됩니다.
규칙 ID	uint32	이벤트를 트리거한 규칙의 내부 식별자입니다.
정책 UUID	uint8[16]	이벤트를 트리거한 정책의 UUID입니다.
문자열 블록 유형	uint32	IP 평판 카테고리의 설명이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	카테고리 이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Category Name(카테고리 이름) 필드의 바이트 수를 더한 값이 포함됩니다.
카테고리 이름	string	규칙에 대한 카테고리의 이름입니다.

6.0 이상 버전용 파일 이벤트

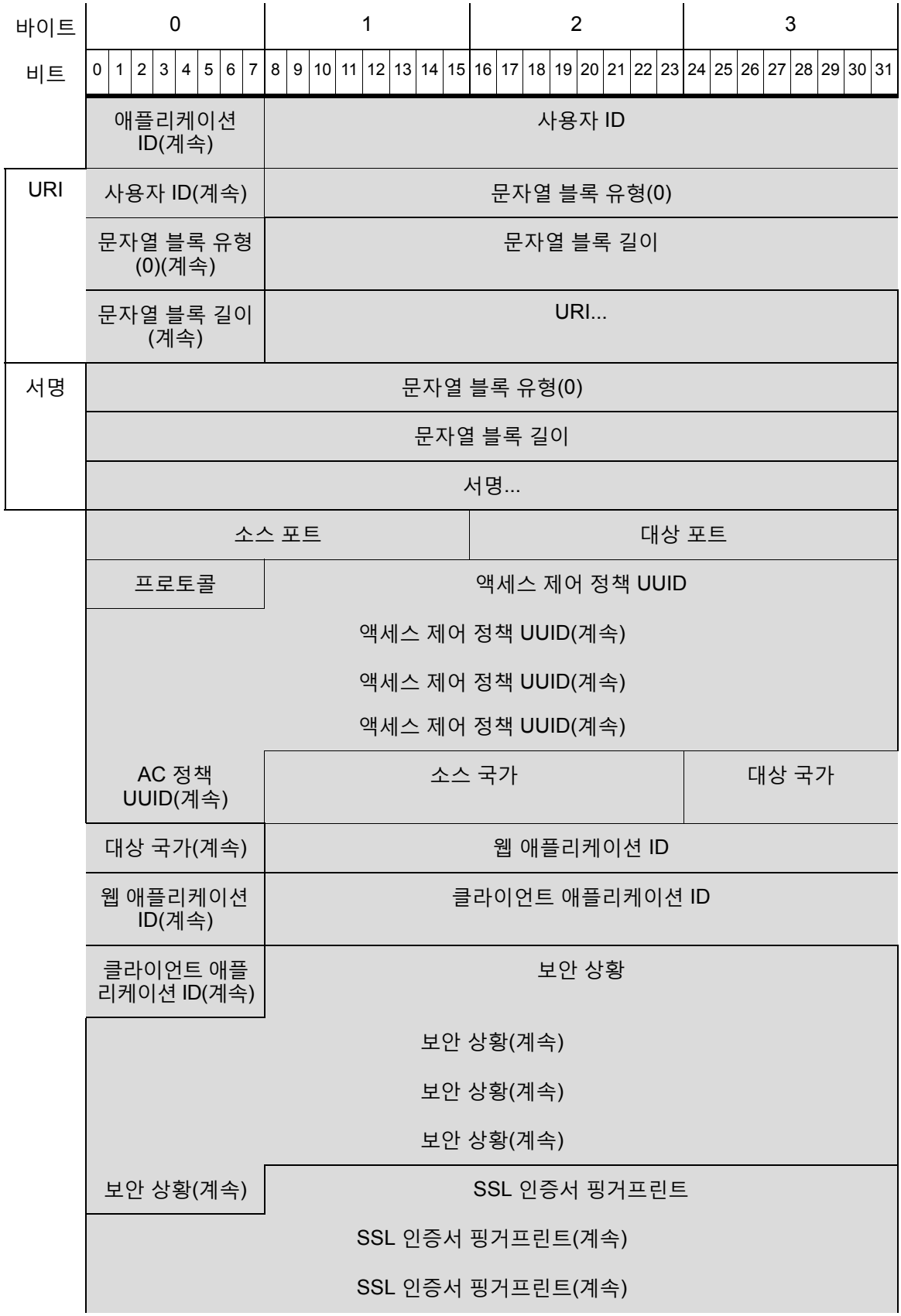
파일 이벤트 데이터 블록은 네트워크를 통해 전송되는 파일에 대한 정보를 포함합니다. 이러한 정보로는 연결 정보, 파일이 악성코드인지 여부, 그리고 파일을 식별하는 특정 정보가 포함됩니다. 계열 2 블록 그룹에서 파일 이벤트의 블록 유형은 56입니다. 이는 블록 유형 46을 대체합니다. ISE 통합, 파일 분석, 로컬 악성코드 분석 및 용량 처리 상태용 필드가 추가되었습니다.

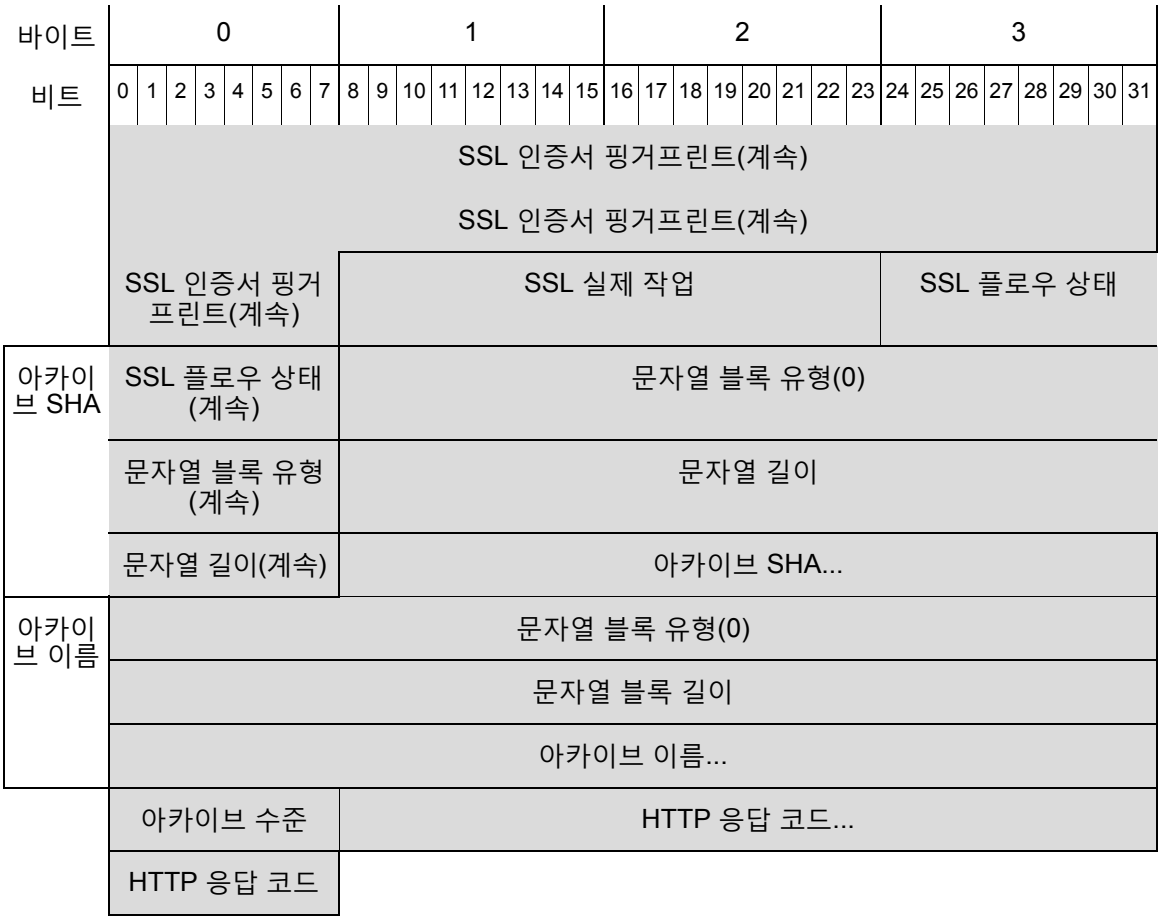
이벤트 버전이 5이고 이벤트 코드가 111인 요청 메시지에서 파일 이벤트 플래그(Request Flags(요청 플래그) 필드의 비트 30)를 설정하여 파일 이벤트 레코드를 요청합니다. 요청 플래그, 2-12페이지의 내용을 참조하십시오. 비트 23을 활성화하면 레코드에 확장 이벤트 헤더가 포함됩니다.

다음 그림에 파일 이벤트 데이터 블록의 구조가 나와 있습니다.



바이트	0	1	2	3
비트	0 1 2 3 4 5 6 7	8 9 10 11 12 13 14 15	16 17 18 19 20 21 22 23	24 25 26 27 28 29 30 31
	소스 IP 주소			
	소스 IP 주소(계속)			
	소스 IP 주소(계속)			
	소스 IP 주소(계속)			
	대상 IP 주소			
	대상 IP 주소(계속)			
	대상 IP 주소(계속)			
	대상 IP 주소(계속)			
	상태	SPERO 상태	파일 스토리지 상태	파일 분석 상태
	로컬 악성코드 분석 상태	아카이브 파일 상태	위협 점수	작업
	SHA 해시			
	SHA 해시(계속)			
	SHA 해시(계속)			
	SHA 해시(계속)			
	SHA 해시(계속)			
	SHA 해시(계속)			
	SHA 해시(계속)			
	SHA 해시(계속)			
	파일 유형 ID			
파일 이름	문자열 블록 유형(0)			
	문자열 블록 길이			
	파일 이름...			
	파일 크기			
	파일 크기(계속)			
	방향	애플리케이션 ID		


바이트
0
1
2
3
비트
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
애플리케이션 ID(계속)
사용자 ID
URI
사용자 ID(계속)
문자열 블록 유형(0)
문자열 블록 유형(0)(계속)
문자열 블록 길이
문자열 블록 길이(계속)
URI...
서명
문자열 블록 유형(0)
문자열 블록 길이
서명...
소스 포트
대상 포트
프로토콜
액세스 제어 정책 UUID
액세스 제어 정책 UUID(계속)
액세스 제어 정책 UUID(계속)
액세스 제어 정책 UUID(계속)
AC 정책 UUID(계속)
소스 국가
대상 국가
대상 국가(계속)
웹 애플리케이션 ID
웹 애플리케이션 ID(계속)
클라이언트 애플리케이션 ID
클라이언트 애플리케이션 ID(계속)
보안 상황
보안 상황(계속)
보안 상황(계속)
보안 상황(계속)
보안 상황(계속)
SSL 인증서 핑거프린트
SSL 인증서 핑거프린트(계속)
SSL 인증서 핑거프린트(계속)



다음 표에는 파일 이벤트 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 3-47 6.0 이상 버전용 파일 이벤트 데이터 블록 필드

필드	데이터 유형	설명
파일 이벤트 블록 유형	uint32	파일 이벤트 데이터 블록을 시작합니다. 이 값은 항상 56입니다.
파일 이벤트 블록 길이	uint32	파일 이벤트 블록의 총 바이트 수입니다. 여기에는 파일 이벤트 블록 유형 및 길이 필드의 8바이트에 그 뒤의 데이터 바이트 수를 더한 값이 포함됩니다.
디바이스 ID	uint32	이벤트를 생성한 디바이스의 ID입니다.
연결 인스턴스	uint16	이벤트를 생성한 디바이스의 Snort 인스턴스입니다. 이벤트를 연결 또는 침입 이벤트와 연결하는 데 사용됩니다.
연결 카운터	uint16	1초 이내에 발생하는 연결 이벤트를 구별하는 데 사용되는 값입니다.
연결 타임스탬프	uint32	관련 연결 이벤트의 UNIX 타임스탬프(1970년 1월 1일 이후의 초 단위 시간)입니다.
파일 이벤트 타임스탬프	uint32	파일 유형이 식별되고 파일 이벤트가 생성된 UNIX 타임스탬프(1970년 1월 1일 이후의 초 단위 시간)입니다.

표 3-47 6.0 이상 버전용 파일 이벤트 데이터 블록 필드 (계속)

필드	데이터 유형	설명
소스 IP 주소	uint8[16]	연결 소스의 IPv4 또는 IPv6 주소입니다.
대상 IP 주소	uint8[16]	연결 대상의 IPv4 또는 IPv6 주소입니다.
상태	uint8	파일의 악성코드 상태입니다. 가능한 값은 다음과 같습니다. • 1 - CLEAN - 파일이 정상 상태이며 악성코드가 포함되어 있지 않습니다. • 2 - UNKNOWN - 파일에 악성코드가 포함되어 있는지 알 수 없습니다. • 3 - MALWARE - 파일에 악성코드가 포함되어 있습니다. • 4 - UNAVAILABLE - 소프트웨어가 AMP 클라우드에 상태 요청을 보낼 수 없거나 AMP 클라우드 서비스가 요청에 응답하지 않았습니다. • 5 - CUSTOM SIGNATURE - 파일이 사용자가 정의한 해시와 일치하며 사용자가 지정한 방식으로 처리됩니다.
SPERO 상태	uint8	파일 분석에 SPERO 서명이 사용되었는지를 나타냅니다. 값이 1, 2 또는 3이면 SPERO 분석이 사용된 것이고 그 외의 값이면 SPERO 분석이 사용되지 않은 것입니다.
파일 스토리지 상태	uint8	파일의 저장 상태입니다. 가능한 값은 다음과 같습니다. • 1 - 파일 저장됨 • 2 - 파일 저장됨 • 3 - 파일을 저장할 수 없음 • 4 - 파일을 저장할 수 없음 • 5 - 파일을 저장할 수 없음 • 6 - 파일을 저장할 수 없음 • 7 - 파일을 저장할 수 없음 • 8 - 파일 크기가 너무 큼 • 9 - 파일 크기가 너무 작음 • 10 - 파일을 저장할 수 없음 • 11 - 파일이 저장되지 않음(상태 사용 불가)

표 3-47 6.0 이상 버전용 파일 이벤트 데이터 블록 필드 (계속)

필드	데이터 유형	설명
파일 분석 상태	uint8	동적 분석을 위해 파일이 제출되었는지 나타냅니다. 가능한 값은 다음과 같습니다. • 0 - 파일이 분석을 위해 전송되지 않음 • 1 - 분석을 위해 전송됨 • 2 - 분석을 위해 전송됨 • 4 - 분석을 위해 전송됨 • 5 - 전송하지 못함 • 6 - 전송하지 못함 • 7 - 전송하지 못함 • 8 - 전송하지 못함 • 9 - 파일 크기가 너무 작음 • 10 - 파일 크기가 너무 큼 • 11 - 분석을 위해 전송됨 • 12 - 분석 완료 • 13 - 장애(네트워크 문제) • 14 - 장애(속도 제한) • 15 - 장애(파일이 너무 큼) • 16 - 장애(파일 읽기 오류) • 17 - 장애(내부 라이브러리 오류) • 19 - 파일이 전송되지 않음(상태 사용 불가) • 20 - 장애(파일을 실행할 수 없음) • 21 - 장애(분석 시간 초과) • 22 - 분석을 위해 전송됨 • 23 - 파일 전송 파일 용량 처리됨 - 분석을 위해 샌드박스로 파일을 제출할 수 없어서 파일 용량이 처리됨(센서에 저장됨) • 25 - 파일 전송 서버 제한됨 초과 용량 처리됨 - 서버의 속도 제한으로 인해 파일 용량이 처리됨 • 26 - 통신 장애 - 클라우드 연결 장애로 인해 파일 용량이 처리됨 • 27 - 전송되지 않음 - 컨피그레이션으로 인해 파일이 전송되지 않음 • 28 - 사전 클래스 불일치 - 사전 분류에서 파일의 임베디드 개체 또는 의심스러운 개체를 찾지 못하여 동적 분석을 위해 파일이 전송되지 않음 • 29 - 전송 샌드박스 프라이빗 클라우드로 전송됨 - 파일이 동적 분석을 위해 프라이빗 클라우드로 전송됨 • 30 - 전송 샌드박스 프라이빗 클라우드로 전송되지 않음 - 파일이 분석을 위해 프라이빗 클라우드로 전송되지 않음

표 3-47 6.0 이상 버전용 파일 이벤트 데이터 블록 필드 (계속)

필드	데이터 유형	설명
로컬 악성코드 분석 상태	uint8	파일의 악성코드 분석 상태입니다. 가능한 값은 다음과 같습니다. • 0 - 파일이 분석되지 않음 • 1 - 분석 완료 • 2 - 분석 시 장애 발생 • 3 - 수동 분석 요청
아카이브 파일 상태	uint8	검사 중인 아카이브의 상태입니다. 다음과 같은 값을 사용할 수 있습니다. • 0 - N/A - 파일을 아카이브로 검사하고 있지 않음 • 1 - 보류 중 - 아카이브를 검사하는 중 • 2 - 추출됨 - 문제없이 검사함 • 3 - 장애 발생함 - 시스템 자원이 부족하여 검사하지 못함 • 4 - 수준 초과됨 - 검사는 성공했으나 아카이브에서 중첩 검사 수준이 초과됨 • 5 - 암호화됨 - 검사가 일부분 성공함(아카이브가 암호화된 아카이브이거나 암호화된 아카이브를 포함함) • 6 - 검사 불가 - 검사가 일부분 성공함(파일이 손상되었거나 형식이 잘못되었을 수 있음)
위협 점수	uint8	동적 분석 과정에서 관찰된 잠재적으로 악의적인 동작을 기준으로 한 0부터 100까지의 숫자 값입니다.
작업	uint8	파일 유형을 기반으로 파일에 조취를 취합니다. 다음과 같은 값을 사용할 수 있습니다. • 1 - 탐지 • 2 - 차단 • 3 - 악성코드 클라우드 조회 • 4 - 악성코드 차단 • 5 - 악성코드 화이트리스트 추가 • 6 - 클라우드 조회 시간 초과 • 7 - 맞춤형 탐지 • 8 - 맞춤형 탐지 차단 • 9 - 아카이브 차단(수준 초과됨) • 10 - 아카이브 차단(암호화됨) • 11 - 아카이브 차단(검사하지 못함)
SHA 해시	uint8[32]	이진 형식으로 된 파일의 SHA-256 해시입니다.

표 3-47 6.0 이상 버전용 파일 이벤트 데이터 블록 필드 (계속)

필드	데이터 유형	설명
파일 유형 ID	uint32	파일 유형에 매핑되는 ID 번호입니다. 이 필드의 의미가 이 이벤트와 함께 메타데이터에 포함되어 전송됩니다. 자세한 정보는 AMP for Endpoints 파일 유형 메타데이터, 3-42페이지의 내용을 참조하십시오.
파일 이름	string	파일의 이름입니다.
파일 크기	uint64	파일의 바이트 단위 크기입니다.
방향	uint8	파일이 업로드되었는지 아니면 다운로드되었는지를 나타내는 값입니다. 다음과 같은 값을 사용할 수 있습니다. • 1 - 다운로드 • 2 - 업로드 현재 이 값은 프로토콜에 따라 달라집니다(예: 연결이 HTTP인 경우 다운로드임).
애플리케이션 ID	uint32	파일 전송을 사용하여 애플리케이션에 매핑되는 ID 번호입니다.
사용자 ID	uint32	시스템이 식별한 대상 호스트에 로그인하는 사용자의 ID 번호입니다.
URI	string	연결의 URI(Uniform Resource Identifier)입니다.
서명	string	문자열 형식으로 된 파일의 SHA-256 해시입니다.
소스 포트	uint16	연결 소스의 포트 번호입니다.
대상 포트	uint16	연결 대상의 포트 번호입니다.
프로토콜	uint8	사용자가 지정한 IANA 프로토콜 번호입니다. 예를 들면 다음과 같습니다. • 1 - ICMP • 4 - IP • 6 - TCP • 17 - UDP 현재는 TCP만 설정 가능합니다.
액세스 제어 정책 UUID	uint8[16]	이벤트를 트리거한 액세스 제어 정책의 고유 식별자입니다.
소스 국가	uint16	소스 호스트의 국가 코드입니다.
대상 국가	uint16	대상 호스트의 국가 코드입니다.
웹 애플리케이션 ID	uint32	해당하는 경우 웹 애플리케이션의 내부 ID 번호입니다.
클라이언트 애플리케이션 ID	uint32	해당하는 경우 클라이언트 애플리케이션의 내부 ID 번호입니다.
보안 상황	uint8(16)	트래픽이 통과한 보안 상황(가상 방화벽)의 ID 번호입니다. 이 필드는 다중 컨텍스트 모드의 ASA FirePOWER 디바이스에 대해서만 채워집니다.
SSL 인증서 핑거프린트	uint8[20]	SSL 서버 인증서의 SHA1 해시입니다.

표 3-47 6.0 이상 버전용 파일 이벤트 데이터 블록 필드 (계속)

필드	데이터 유형	설명
SSL 실제 작업	uint16	SSL 규칙에 기반한 연결에서 수행된 작업입니다. 규칙에 명시된 작업이 가능하지 않을 수도 있으므로, 이는 예상 작업과 다를 수 있습니다. 가능한 값은 다음과 같습니다. • 0 - '알 수 없음' • 1 - '암호 해독 안 함' • 2 - '차단' • 3 - '차단 및 재설정' • 4 - '암호 해독(알려진 키)' • 5 - '암호 해독(키 교체)' • 6 - '암호 해독(재서명)'

표 3-47 6.0 이상 버전용 파일 이벤트 데이터 블록 필드 (계속)

필드	데이터 유형	설명
SSL 플로우 상태	uint16	SSL 플로우의 상태입니다. 이 값은 작업을 수행한 이유 또는 오류 메시지가 표시된 이유를 설명합니다. 가능한 값은 다음과 같습니다. • 0 - '알 수 없음' • 1 - '일치하지 않음' • 2 - '성공' • 3 - '캐시되지 않은 세션' • 4 - '알 수 없는 암호 그룹' • 5 - '지원되지 않는 암호 그룹' • 6 - '지원되지 않는 SSL 버전' • 7 - 'SSL 압축 사용됨' • 8 - '패시브 모드에서 세션 암호 해독 불가' • 9 - '핸드셰이크 오류' • 10 - '암호 해독 오류' • 11 - '서버 이름 카테고리 조회 보류 중' • 12 - '공용 이름 카테고리 조회 보류 중' • 13 - '내부 오류' • 14 - '네트워크 파라미터 사용 불가' • 15 - '유효하지 않은 서버 인증서 핸들' • 16 - '서버 인증서 핑거프린트 사용 불가' • 17 - '주체 DN을 캐시할 수 없음' • 18 - '발급자 DN을 캐시할 수 없음' • 19 - '알 수 없는 SSL 버전' • 20 - '외부 인증서 목록 사용 불가' • 21 - '외부 인증서 핑거프린트 사용 불가' • 22 - '내부 인증서 목록이 유효하지 않음' • 23 - '내부 인증서 목록 사용 불가' • 24 - '내부 인증서 사용 불가' • 25 - '내부 인증서 핑거프린트 사용 불가' • 26 - '서버 인증서 검증 사용 불가' • 27 - '서버 인증서 검증 장애' • 28 - '유효하지 않은 작업'
문자열 블록 유형	uint32	아카이브 SHA가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.

표 3-47 6.0 이상 버전용 파일 이벤트 데이터 블록 필드 (계속)

필드	데이터 유형	설명
문자열 블록 길이	uint32	아카이브 SHA 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 침입 정책 이름의 바이트 수를 더한 값이 포함됩니다.
아카이브 SHA	string	파일이 포함된 상위 아카이브의 SHA1 해시입니다.
문자열 블록 유형	uint32	아카이브 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	아카이브 이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 침입 정책 이름의 바이트 수를 더한 값이 포함됩니다.
아카이브 이름	string	상위 아카이브의 이름입니다.
아카이브 수준	uint8	파일이 중첩된 계층의 수입니다. 예를 들어 텍스트 파일이 zip 아카이브에 들어 있는 경우 이 항목의 값은 1입니다.
HTTP 응답 코드	uint32	HTTP 응답 코드

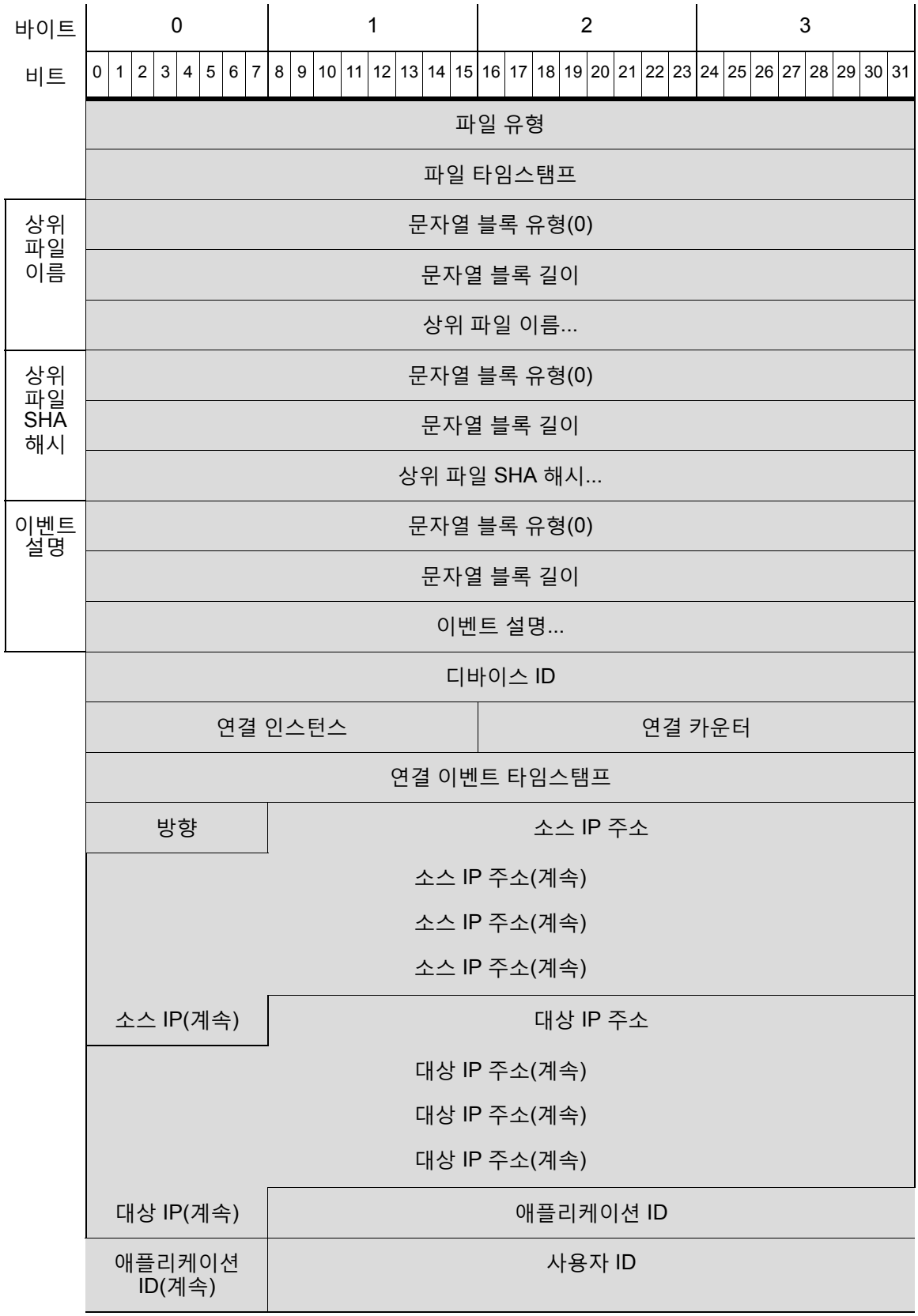
6.0 이상 버전용 악성코드 이벤트 데이터 블록

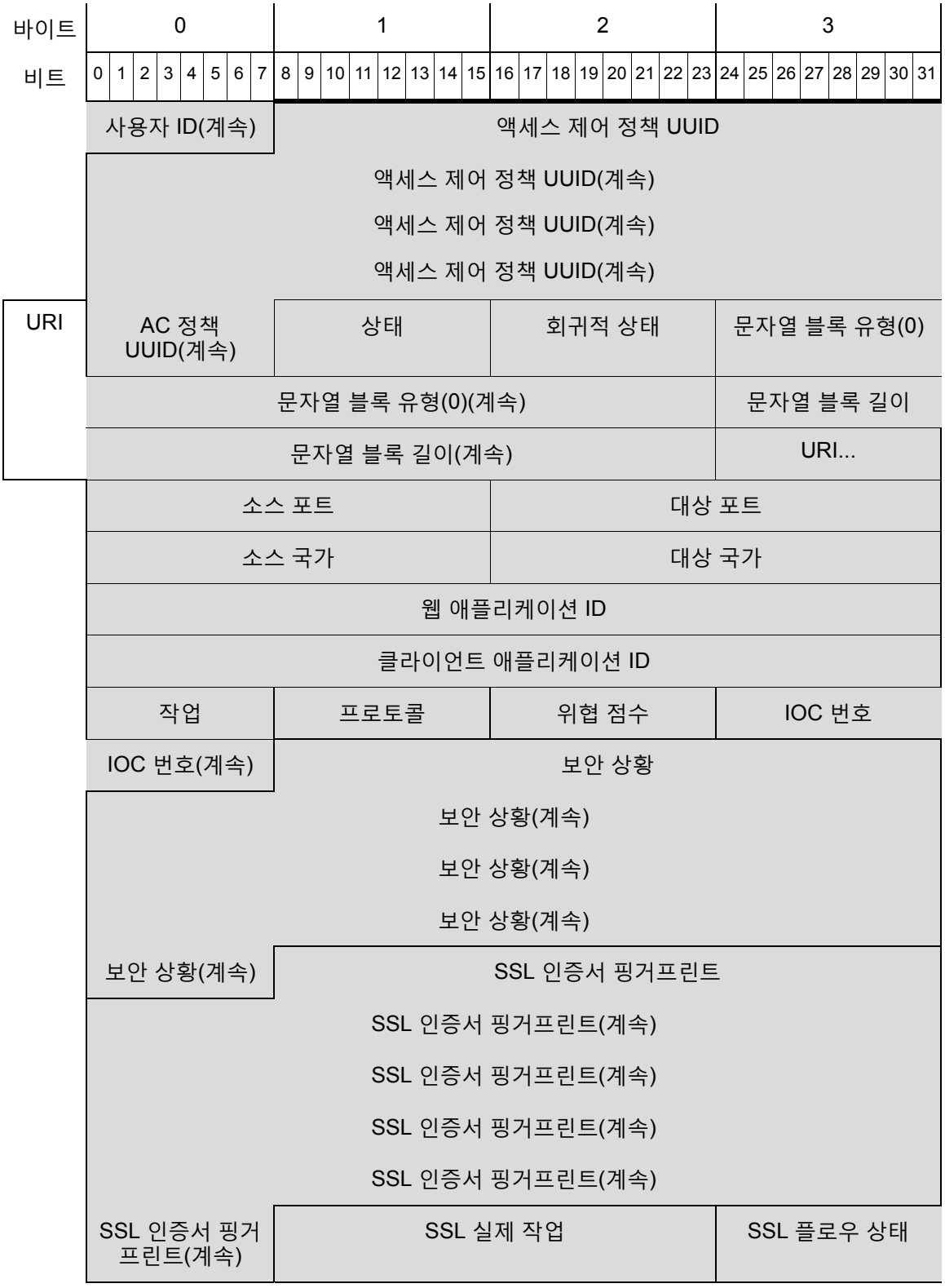
eStreamer 서비스는 악성코드 이벤트 데이터 블록을 사용하여 악성코드 이벤트에 대한 정보를 저장합니다. 이러한 이벤트에는 클라우드 내에서 탐지 또는 격리된 악성코드, 탐지 방법, 악성코드의 영향을 받은 호스트 및 사용자에 대한 정보가 포함됩니다. 계열 2 블록 그룹에서 악성코드 이벤트 데이터 블록의 블록 유형은 62입니다. 이는 블록 47을 대체합니다. HTTP 응답용 필드가 추가되었습니다.

이벤트 버전이 7이고 이벤트 코드가 101인 요청 메시지에서 악성코드 이벤트 플래그(Request Flags(요청 플래그) 필드의 비트 30)를 설정하여 악성코드 이벤트 레코드의 일부분으로 이벤트를 요청합니다.

다음 그림에 악성코드 이벤트 데이터 블록의 구조가 나와 있습니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	클라우드 UUID																															
	클라우드 UUID(계속)																															
	클라우드 UUID(계속)																															
	클라우드 UUID(계속)																															
	악성코드 이벤트 타임스탬프																															
	이벤트 유형 ID																															
	이벤트 하위 유형 ID																															
탐지 이름	탐지기 ID								문자열 블록 유형(0)																							
	문자열 블록 유형(0)(계속)								문자열 블록 길이																							
	문자열 블록 길이(계속)								탐지 이름...																							
사용자	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	사용자...																															
파일 이름	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	파일 이름...																															
파일 경로	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	파일 경로...																															
파일 SHA 해시	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	파일 SHA 해시...																															
	파일 크기																															


바이트
0
1
2
3
비트
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
파일 유형
파일 타임스탬프
상위 파일 이름
문자열 블록 유형(0)
문자열 블록 길이
상위 파일 이름...
상위 파일 SHA 해시
문자열 블록 유형(0)
문자열 블록 길이
상위 파일 SHA 해시...
이벤트 설명
문자열 블록 유형(0)
문자열 블록 길이
이벤트 설명...
디바이스 ID
연결 인스턴스
연결 카운터
연결 이벤트 타임스탬프
방향
소스 IP 주소
소스 IP 주소(계속)
소스 IP 주소(계속)
소스 IP 주소(계속)
소스 IP(계속)
대상 IP 주소
대상 IP 주소(계속)
대상 IP 주소(계속)
대상 IP 주소(계속)
대상 IP(계속)
애플리케이션 ID
애플리케이션 ID(계속)
사용자 ID


바이트
0
1
2
3
비트
0 1 2 3 4 5 6 7
8 9 10 11 12 13 14 15
16 17 18 19 20 21 22 23
24 25 26 27 28 29 30 31
사용자 ID(계속)
액세스 제어 정책 UUID
액세스 제어 정책 UUID(계속)
액세스 제어 정책 UUID(계속)
액세스 제어 정책 UUID(계속)
URI
AC 정책 UUID(계속)
상태
회귀적 상태
문자열 블록 유형(0)
문자열 블록 유형(0)(계속)
문자열 블록 길이
문자열 블록 길이(계속)
URI...
소스 포트
대상 포트
소스 국가
대상 국가
웹 애플리케이션 ID
클라이언트 애플리케이션 ID
작업
프로토콜
위협 점수
IOC 번호
IOC 번호(계속)
보안 상황
보안 상황(계속)
보안 상황(계속)
보안 상황(계속)
보안 상황(계속)
SSL 인증서 핑거프린트
SSL 인증서 핑거프린트(계속)
SSL 인증서 핑거프린트(계속)
SSL 인증서 핑거프린트(계속)
SSL 인증서 핑거프린트(계속)
SSL 인증서 핑거프린트(계속)
SSL 실제 작업
SSL 플로우 상태

다음 표에는 악성코드 이벤트 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 3-48 6.0 이상 버전용 악성코드 이벤트 데이터 블록 필드

필드	데이터 유형	설명
악성코드 이벤트 블록 유형	uint32	악성코드 이벤트 데이터 블록을 시작합니다. 이 값은 항상 62입니다.
악성코드 이벤트 블록 길이	uint32	악성코드 이벤트 데이터 블록의 총 바이트 수입니다. 여기에는 악성코드 이벤트 블록 유형 및 길이 필드의 8바이트에 그 뒤의 데이터 바이트 수를 더한 값이 포함됩니다.
에이전트 UUID	uint8[16]	악성코드를 보고하는 AMP for Endpoints 에이전트의 내부 고유 ID입니다.
클라우드 UUID	uint8[16]	악성코드 이벤트가 시작된 AMP 클라우드의 내부 고유 ID입니다.
악성코드 이벤트 타임스탬프	uint32	악성코드 이벤트 생성 타임스탬프입니다.
이벤트 유형 ID	uint32	악성코드 이벤트 유형의 내부 ID입니다.
이벤트 하위 유형 ID	uint32	악성코드를 탐지하도록 유도한 작업의 내부 ID입니다.
탐지기 ID	uint8	악성코드를 탐지한 탐지 기술의 내부 ID입니다.
문자열 블록 유형	uint32	탐지 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	탐지 이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Detection Name(탐지 이름) 필드의 바이트 수를 더한 값이 포함됩니다.
탐지 이름	string	탐지 또는 격리된 악성코드의 이름입니다.

표 3-48 6.0 이상 버전용 악성코드 이벤트 데이터 블록 필드 (계속)

필드	데이터 유형	설명
문자열 블록 유형	uint32	사용자 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	사용자 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 User(사용자) 필드의 바이트 수를 더한 값이 포함됩니다.
사용자	string	Cisco 에이전트가 설치되어 있으며 악성코드 이벤트가 발생한 컴퓨터의 사용자입니다. 이러한 사용자는 사용자 검색에 연결되지 않습니다.
문자열 블록 유형	uint32	파일 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	파일 이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 File Name(파일 이름) 필드의 바이트 수를 더한 값이 포함됩니다.
파일 이름	string	탐지 또는 격리된 파일의 이름입니다.
문자열 블록 유형	uint32	파일 경로가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	파일 경로 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 File Path(파일 경로) 필드의 바이트 수를 더한 값이 포함됩니다.
파일 경로	string	탐지 또는 격리된 파일의 파일 경로이며, 파일 이름은 포함되지 않습니다.
문자열 블록 유형	uint32	파일 SHA 해시가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	파일 SHA 해시 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 File SHA Hash(파일 SHA 해시) 필드의 바이트 수를 더한 값이 포함됩니다.
파일 SHA 해시	string	탐지 또는 격리된 파일의 SHA-256 해시 값이 렌더링된 문자열입니다.
파일 크기	uint32	탐지 또는 격리된 파일의 바이트 크기입니다.
파일 유형	uint32	탐지 또는 격리된 파일의 파일 유형입니다. 이 필드의 의미가 이 이벤트와 함께 메타데이터에 포함되어 전송됩니다. 자세한 정보는 AMP for Endpoints 파일 유형 메타데이터, 3-42페이지의 내용을 참조하십시오.
파일 타임스탬프	uint32	탐지 또는 격리된 파일이 생성된 UNIX 타임스탬프(1970년 1월 1일 이후의 초 단위 시간)입니다.
문자열 블록 유형	uint32	상위 파일 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.

표 3-48 6.0 이상 버전용 악성코드 이벤트 데이터 블록 필드 (계속)

필드	데이터 유형	설명
문자열 블록 길이	uint32	상위 파일 이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Parent File Name(상위 파일 이름) 필드의 바이트 수를 더한 값이 포함됩니다.
상위 파일 이름	string	탐지가 발생했을 때 탐지 또는 격리된 파일에 액세스한 파일의 이름입니다.
문자열 블록 유형	uint32	상위 파일 SHA 해시가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	상위 파일 SHA 해시 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Parent File SHA Hash(상위 파일 SHA 해시) 필드의 바이트 수를 더한 값이 포함됩니다.
상위 파일 SHA 해시	string	탐지가 발생했을 때 탐지 또는 격리된 파일에 액세스한 상위 파일의 SHA-256 해시 값입니다.
문자열 블록 유형	uint32	이벤트 설명이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	이벤트 설명 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Event Description(이벤트 설명) 필드의 바이트 수를 더한 값이 포함됩니다.
이벤트 설명	string	이벤트 유형과 관련된 추가 이벤트 정보입니다.
디바이스 ID	uint32	이벤트를 생성한 디바이스의 ID입니다.
연결 인스턴스	uint16	이벤트를 생성한 디바이스의 Snort 인스턴스입니다. 이벤트를 연결 또는 IDS 이벤트와 연결하는 데 사용됩니다.
연결 카운터	uint16	1초 이내에 발생하는 연결 이벤트를 구별하는 데 사용되는 값입니다.
연결 이벤트 타임스탬프	uint32	연결 이벤트의 타임스탬프입니다.
방향	uint8	파일이 업로드되었는지 아니면 다운로드되었는지를 나타냅니다. 다음과 같은 값을 사용할 수 있습니다. • 1 - 다운로드 • 2 - 업로드 현재 이 값은 프로토콜에 따라 달라집니다(예: 연결이 HTTP인 경우 다운로드임).
소스 IP 주소	uint8[16]	연결 소스의 IPv4 또는 IPv6 주소입니다.
대상 IP 주소	uint8[16]	연결 대상의 IPv4 또는 IPv6 주소입니다.
애플리케이션 ID	uint32	파일 전송을 사용하여 애플리케이션에 매핑되는 ID 번호입니다.
사용자 ID	uint32	시스템이 식별한 대상 호스트에 로그인하는 사용자의 ID 번호입니다.
액세스 제어 정책 UUID	uint8[16]	이벤트를 트리거한 액세스 제어 정책의 고유 식별자 역할을 하는 ID 번호입니다.

표 3-48 6.0 이상 버전용 악성코드 이벤트 데이터 블록 필드 (계속)

필드	데이터 유형	설명
상태	uint8	파일의 악성코드 상태입니다. 가능한 값은 다음과 같습니다. • 1 - CLEAN - 파일이 정상 상태이며 악성코드가 포함되어 있지 않습니다. • 2 - UNKNOWN - 파일에 악성코드가 포함되어 있는지 알 수 없습니다. • 3 - MALWARE - 파일에 악성코드가 포함되어 있습니다. • 4 - UNAVAILABLE - 소프트웨어가 AMP 클라우드에 상태 요청을 보낼 수 없거나 AMP 클라우드 서비스가 요청에 응답하지 않았습니다. • 5 - CUSTOM SIGNATURE - 파일이 사용자가 정의한 해시와 일치하며 사용자가 지정한 방식으로 처리됩니다.
회귀적 상태	uint8	상태가 업데이트된 경우 파일의 상태입니다. 상태가 업데이트되지 않은 경우 이 필드에는 Disposition(상태) 필드와 동일한 값이 포함됩니다. 가능한 값은 Disposition(상태) 필드와 동일합니다.
문자열 블록 유형	uint32	URI가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	URI 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 URI 필드의 바이트 수를 더한 값이 포함됩니다.
URI	string	연결의 URI입니다.
소스 포트	uint16	연결 소스의 포트 번호입니다.
대상 포트	uint16	연결 대상의 포트 번호입니다.
소스 국가	uint16	소스 호스트의 국가 코드입니다.
대상 국가	uint16	대상 호스트의 국가 코드입니다.
웹 애플리케이션 ID	uint32	해당하는 경우 탐지된 웹 애플리케이션의 내부 ID 번호입니다.
클라이언트 애플리케이션 ID	uint32	해당하는 경우 탐지된 클라이언트 애플리케이션의 내부 ID 번호입니다.

표 3-48 6.0 이상 버전용 악성코드 이벤트 데이터 블록 필드 (계속)

필드	데이터 유형	설명
작업	uint8	파일 유형을 기반으로 파일에 조취를 취합니다. 다음과 같은 값을 사용할 수 있습니다. • 1 - 탐지 • 2 - 차단 • 3 - 악성코드 클라우드 조회 • 4 - 악성코드 차단 • 5 - 악성코드 화이트리스트 추가 • 6 - 클라우드 조회 시간 초과 • 7 - 맞춤형 탐지 • 8 - 맞춤형 탐지 차단 • 9 - 아카이브 차단(수준 초과됨) • 10 - 아카이브 차단(암호화됨) • 11 - 아카이브 차단(검사하지 못함)
프로토콜	uint8	사용자가 지정한 IANA 프로토콜 번호입니다. 예를 들면 다음과 같습니다. • 1 - ICMP • 4 - IP • 6 - TCP • 17 - UDP 현재는 TCP만 설정 가능합니다.
위협 점수	uint8	동적 분석 과정에서 관찰된 잠재적으로 악의적인 동작을 기준으로 한 0부터 100까지의 숫자 값입니다.
IOC 번호	uint16	이 이벤트와 관련된 보안 침해의 ID 번호입니다.
보안 상황	uint8(16)	트래픽이 통과한 보안 상황(가상 방화벽)의 ID 번호입니다. 이 필드는 다중 컨텍스트 모드의 ASA FirePOWER 디바이스에 대해서만 채워집니다.
SSL 인증서 핑거프린트	uint8[20]	SSL 서버 인증서의 SHA1 해시입니다.
SSL 실제 작업	uint16	SSL 규칙에 기반한 연결에서 수행된 작업입니다. 규칙에 명시된 작업이 가능하지 않을 수도 있으므로, 이는 예상 작업과 다를 수 있습니다. 가능한 값은 다음과 같습니다. • 0 - '알 수 없음' • 1 - '암호 해독 안 함' • 2 - '차단' • 3 - '차단 및 재설정' • 4 - '암호 해독(알려진 키)' • 5 - '암호 해독(키 교체)' • 6 - '암호 해독(재서명)'

표 3-48 6.0 이상 버전용 악성코드 이벤트 데이터 블록 필드 (계속)

필드	데이터 유형	설명
SSL 플로우 상태	uint16	SSL 플로우의 상태입니다. 이 값은 작업을 수행한 이유 또는 오류 메시지가 표시된 이유를 설명합니다. 가능한 값은 다음과 같습니다. • 0 - '알 수 없음' • 1 - '일치하지 않음' • 2 - '성공' • 3 - '캐시되지 않은 세션' • 4 - '알 수 없는 암호 그룹' • 5 - '지원되지 않는 암호 그룹' • 6 - '지원되지 않는 SSL 버전' • 7 - 'SSL 압축 사용됨' • 8 - '패시브 모드에서 세션 암호 해독 불가' • 9 - '핸드셰이크 오류' • 10 - '암호 해독 오류' • 11 - '서버 이름 카테고리 조회 보류 중' • 12 - '공용 이름 카테고리 조회 보류 중' • 13 - '내부 오류' • 14 - '네트워크 파라미터 사용 불가' • 15 - '유효하지 않은 서버 인증서 핸들' • 16 - '서버 인증서 핑거프린트 사용 불가' • 17 - '주체 DN을 캐시할 수 없음' • 18 - '발급자 DN을 캐시할 수 없음' • 19 - '알 수 없는 SSL 버전' • 20 - '외부 인증서 목록 사용 불가' • 21 - '외부 인증서 핑거프린트 사용 불가' • 22 - '내부 인증서 목록이 유효하지 않음' • 23 - '내부 인증서 목록 사용 불가' • 24 - '내부 인증서 사용 불가' • 25 - '내부 인증서 핑거프린트 사용 불가' • 26 - '서버 인증서 검증 사용 불가' • 27 - '서버 인증서 검증 장애' • 28 - '유효하지 않은 작업'
문자열 블록 유형	uint32	아카이브 SHA가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	아카이브 SHA 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 침입 정책 이름의 바이트 수를 더한 값이 포함됩니다.

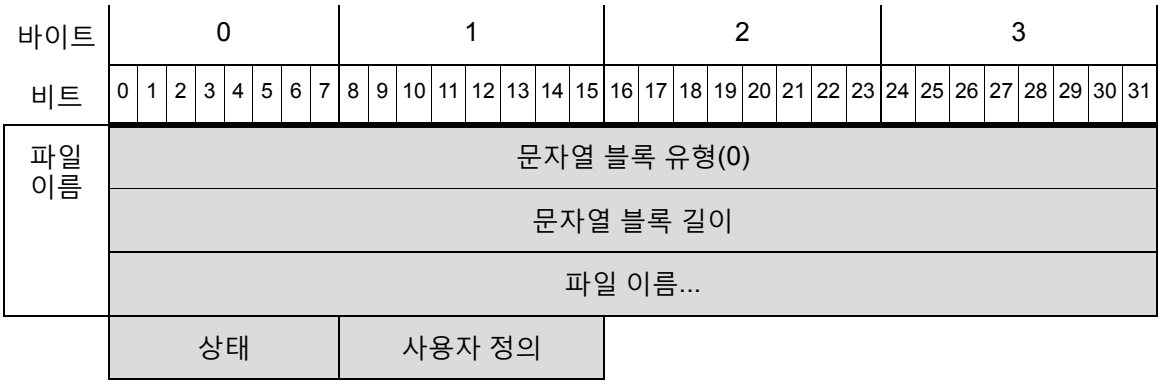
표 3-48 6.0 이상 버전용 악성코드 이벤트 데이터 블록 필드 (계속)

필드	데이터 유형	설명
아카이브 SHA	string	파일이 포함된 상위 아카이브의 SHA1 해시입니다.
문자열 블록 유형	uint32	아카이브 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	아카이브 이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 침입 정책 이름의 바이트 수를 더한 값이 포함됩니다.
아카이브 이름	string	상위 아카이브의 이름입니다.
아카이브 수준	uint8	파일이 중첩된 계층의 수입니다. 예를 들어 텍스트 파일이 zip 아카이브에 들어 있는 경우 이 항목의 값은 1입니다.
HTTP 응답	uint32	HTTP 요청의 응답 코드입니다.

5.3 이상 버전용 파일 이벤트 SHA 해시

eStreamer 서비스는 파일 이벤트 SHA 해시 데이터 블록을 사용하여 파일 SHA 해시의 매핑 메타데이터를 파일 이름에 포함합니다. 계열 2 데이터 블록 목록에서 이 블록의 블록 유형은 40입니다. 확장 요청(이벤트 코드 111)에서 파일 로그 이벤트를 요청했으며 비트 20을 설정하거나 이벤트 버전이 5이고 이벤트 코드가 21인 메타데이터를 요청하는 경우 이 블록 유형을 요청할 수 있습니다.

다음 다이어그램에 파일 이벤트 해시 데이터 블록의 구조가 나와 있습니다.



다음 표에는 파일 이벤트 SHA 해시 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 3-49 파일 이벤트 SHA 해시 데이터 블록 필드

필드	데이터 유형	설명
파일 이벤트 SHA 해시 블록 유형	uint32	파일 이벤트 SHA 해시 블록을 시작합니다. 이 값은 항상 `40`입니다.
파일 이벤트 SHA 해시 블록 길이	uint32	파일 이벤트 SHA 해시 블록의 총 바이트 수입니다. 여기에는 파일 이벤트 SHA 해시 블록 유형 및 길이 필드의 8바이트에 그 뒤의 데이터 바이트 수를 더한 값이 포함됩니다.
SHA 해시	uint8[32]	이진 형식으로 된 파일의 SHA-256 해시입니다.
문자열 블록 유형	uint32	파일과 관련된 설명 이름을 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 `0`입니다.
문자열 블록 길이	uint32	이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Name(이름) 필드의 바이트 수를 더한 값이 포함됩니다.
파일 이름 또는 상태	string	파일을 설명하는 이름 또는 상태입니다. 파일이 정상 상태이면 이 값은 `Clean`입니다. 파일 상태를 알 수 없는 경우 이 값은 `Neutral`입니다. 파일에 악성코드가 포함되어 있으면 파일 이름이 지정됩니다.
상태	uint8	파일의 악성코드 상태입니다. 가능한 값은 다음과 같습니다. • `1` - CLEAN - 파일이 정상 상태이며 악성코드가 포함되어 있지 않습니다. • `2` - UNKNOWN - 파일에 악성코드가 포함되어 있는지 알 수 없습니다. • `3` - MALWARE - 파일에 악성코드가 포함되어 있습니다. • `4` - UNAVAILABLE - 소프트웨어가 AMP 클라우드에 상태 요청을 보낼 수 없거나 AMP 클라우드 서비스가 요청에 응답하지 않았습니다. • `5` - CUSTOM SIGNATURE - 파일이 사용자가 정의한 해시와 일치하며 사용자가 지정한 방식으로 처리됩니다.
사용자 정의	uint8	파일 이름이 제공된 방식을 나타냅니다. • `0` - AMP에서 정의함 • `1` - 사용자 정의

5.3 이상 버전용 파일 유형 ID 메타데이터

eStreamer 서비스는 이벤트에 대한 파일 유형 정보가 포함된 메타데이터를 파일 유형 ID와 함께 전송합니다. 해당 메타데이터의 형식은 아래에 나와 있습니다. 이 레코드는 파일 유형 ID를 파일 유형 이름에 매핑합니다. 메타데이터 플래그 중 하나(요청 메시지의 Request Flags(요청 플래그) 필드에 포함된 비트 1, 14, 15, 20)가 설정되어 있으면 파일 유형 ID 정보가 전송됩니다. 요청 플래그, 2-12페이지의 내용을 참조하십시오. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 파일 유형 ID 레코드임을 나타내는 510입니다.

다음 표에는 파일 유형 ID 레코드의 필드에 대한 설명이 나와 있습니다.

표 3-50 파일 유형 ID 레코드 필드

필드	데이터 유형	설명
파일 유형 ID	uint32	파일 유형 ID 번호입니다. 이 필드는 이 레코드의 고유 키입니다.
파일 유형 길이	uint32	파일 유형 이름에 포함된 바이트 수입니다.
파일 유형 이름	string	데이터 유형을 설명하는 이름입니다.

5.2 이상 버전용 규칙 문서 데이터 블록

eStreamer 서비스는 규칙 문서 데이터 블록을 사용하여 알림을 생성하는 데 사용된 규칙에 대한 정보를 포함합니다. 계열 2 데이터 블록 집합에서 이 블록의 블록 유형은 27입니다. 유형이 10인 호스트 요청 메시지를 사용하여 이 블록을 요청할 수 있습니다. 자세한 정보는 호스트 요청 메시지 형식, 2-26페이지의 내용을 참조하십시오.

다음 다이어그램에 규칙 문서 데이터 블록의 구조가 나와 있습니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	규칙 문서 블록 유형(27)																															
	규칙 문서 블록 길이																															
	서명 ID																															
	생성자 ID																															
	수정																															
요약	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	요약...																															
영향	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	영향...																															
세부 정보	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	세부 정보																															
영향을 받는 시스템	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	영향을 받는 시스템...																															
공격 시나리오	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	공격 시나리오...																															
공격 용이성	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	공격 용이성...																															

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
오탐	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	오탐...																															
미탐	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	미탐...																															
정정 작업	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	정정 작업...																															
도움을 주신 분들	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	도움을 주신 분들...																															
추가 참조 자료	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	추가 참조 자료...																															

다음 표에는 규칙 문서 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 3-51 규칙 문서 데이터 블록 필드

필드	데이터 유형	설명
규칙 문서 데이터 블록 유형	uint32	규칙 문서 데이터 블록을 시작합니다. 이 값은 항상 27입니다.
규칙 문서 데이터 블록 길이	uint32	규칙 문서 데이터 블록의 총 바이트 수입니다. 여기에는 규칙 문서 데이터 블록 유형 및 길이 필드의 8바이트에 그 뒤의 데이터 바이트 수를 더한 값이 포함됩니다.
규칙 ID(서명 ID)	uint32	이벤트와 일치하는 규칙 ID 번호입니다.
생성자 ID	uint32	이벤트를 생성한 Firepower System 전처리기의 ID 번호입니다.
규칙 수정	uint32	규칙 수정 번호입니다.

표 3-51 규칙 문서 데이터 블록 필드 (계속)

필드	데이터 유형	설명
문자열 블록 유형	uint32	규칙과 관련된 요약을 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Summary(요약) 필드의 바이트 수를 더한 값이 포함됩니다.
요약	string	위협 또는 취약점에 대한 설명입니다.
문자열 블록 유형	uint32	규칙과 관련된 영향을 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Impact(영향) 필드의 바이트 수를 더한 값이 포함됩니다.
영향	string	보안 침해가 이러한 취약점을 이용하여 여러 시스템에 어떤 영향을 미칠 수 있는지 나타냅니다.
문자열 블록 유형	uint32	규칙과 관련된 세부 정보를 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Detailed Information(세부 정보) 필드의 바이트 수를 더한 값이 포함됩니다.
세부 정보	string	근본적인 취약점, 규칙에서 실제로 찾는 항목, 영향을 받는 시스템에 관한 정보입니다.
문자열 블록 유형	uint32	규칙과 관련된 영향을 받는 시스템 목록을 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Affected Systems(영향을 받는 시스템) 필드의 바이트 수를 더한 값이 포함됩니다.
영향을 받는 시스템	string	취약점에 의해 영향을 받은 시스템입니다.
문자열 블록 유형	uint32	규칙과 관련된 가능한 공격 시나리오를 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Attack Scenarios(공격 시나리오) 필드의 바이트 수를 더한 값이 포함됩니다.
공격 시나리오	string	가능한 공격의 예시입니다.
문자열 블록 유형	uint32	규칙과 관련된 공격 용이성을 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Ease of Attack(공격 용이성) 필드의 바이트 수를 더한 값이 포함됩니다.
공격 용이성	string	공격의 난이도(간단, 중간, 강력함, 어려움) 및 스크립트를 사용하여 공격을 수행할 수 있는지를 나타냅니다.

표 3-51 규칙 문서 데이터 블록 필드 (계속)

필드	데이터 유형	설명
문자열 블록 유형	uint32	규칙과 관련된 가능한 오탐을 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 False Positives(오탐) 필드의 바이트 수를 더한 값이 포함됩니다.
오탐	string	오탐이 발생할 수 있는 예시입니다. 기본값은 None Known(확인된 예시 없음)입니다.
문자열 블록 유형	uint32	규칙과 관련된 가능한 미탐을 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 False Negatives(미탐) 필드의 바이트 수를 더한 값이 포함됩니다.
미탐	string	미탐이 발생할 수 있는 예시입니다. 기본값은 None Known(확인된 예시 없음)입니다.
문자열 블록 유형	uint32	규칙과 관련된 정정 작업을 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Corrective Action(정정 작업) 필드의 바이트 수를 더한 값이 포함됩니다.
정정 작업	string	패치, 업그레이드 또는 취약점을 제거하거나 완화하기 위한 기타 수단에 관한 정보입니다.
문자열 블록 유형	uint32	규칙에 도움을 주신 분들이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Contributors(도움을 주신 분들) 필드의 바이트 수를 더한 값이 포함됩니다.
도움을 주신 분들	string	규칙 및 기타 관련 문서 작성자의 연락처 정보입니다.
문자열 블록 유형	uint32	규칙과 관련된 추가 참조 자료를 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Additional References(추가 참조 자료) 필드의 바이트 수를 더한 값이 포함됩니다.
추가 참조 자료	string	추가 정보 및 참조입니다.

6.0 이상 버전용 파일 로그 스토리지 메타데이터

eStreamer 서비스는 파일 로그 스토리지 정보가 포함된 메타데이터를 전송합니다. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 파일 로그 스토리지 메타데이터 레코드임을 나타내는 515입니다.

다음 표에는 파일 로그 스토리지 메타데이터 레코드의 필드에 대한 설명이 나와 있습니다.

표 3-52 파일 로그 스토리지 메타데이터 레코드 필드

필드	데이터 유형	설명
파일 로그 스토리지 상태	uint32	파일 로그 스토리지 상태를 나타내는 번호입니다. 이 필드는 이 레코드의 고유 키입니다.
파일 로그 스토리지 상태 설명 길이	uint32	파일 로그 스토리지 상태 설명에 포함된 바이트 수입니다.
파일 로그 스토리지 상태 설명	string	파일 로그 스토리지 상태를 설명하는 이름입니다.

6.0 이상 버전용 파일 로그 샌드박스 메타데이터

eStreamer 서비스는 파일 로그 샌드박스 정보가 포함된 메타데이터를 전송합니다. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 파일 로그 샌드박스 메타데이터 레코드임을 나타내는 516입니다.

다음 표에는 파일 로그 샌드박스 메타데이터 레코드의 필드에 대한 설명이 나와 있습니다.

표 3-53 파일 로그 샌드박스 메타데이터 레코드 필드

필드	데이터 유형	설명
파일 로그 샌드박스 상태	uint32	파일 로그 샌드박스 상태를 나타내는 번호입니다. 이 필드는 이 레코드의 고유 키입니다.
파일 로그 샌드박스 상태 설명 길이	uint32	파일 로그 샌드박스 상태 설명에 포함된 바이트 수입니다.
파일 로그 샌드박스 상태 설명	string	파일 로그 샌드박스 상태를 설명하는 이름입니다.

6.0 이상 버전용 파일 로그 Spero 메타데이터

eStreamer 서비스는 파일 로그 Spero 정보가 포함된 메타데이터를 전송합니다. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 파일 로그 Spero 메타데이터 레코드임을 나타내는 517입니다.

다음 표에는 파일 로그 Spero 메타데이터 레코드의 필드에 대한 설명이 나와 있습니다.

표 3-54 파일 로그 Spero 메타데이터 레코드 필드

필드	데이터 유형	설명
파일 로그 Spero 상태	uint32	파일 로그 Spero 상태를 나타내는 번호입니다. 이 필드는 이 레코드의 고유 키입니다.
파일 로그 Spero 상태 설명 길이	uint32	파일 로그 Spero 상태 설명에 포함된 바이트 수입니다.
파일 로그 Spero 상태 설명	string	파일 로그 Spero 상태를 설명하는 이름입니다.

6.0 이상 버전용 파일 로그 아카이브 메타데이터

eStreamer 서비스는 파일 로그 아카이브 정보가 포함된 메타데이터를 전송합니다. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 파일 로그 아카이브 메타데이터 레코드임을 나타내는 518입니다.

다음 표에는 파일 로그 아카이브 메타데이터 레코드의 필드에 대한 설명이 나와 있습니다.

표 3-55 파일 로그 아카이브 메타데이터 레코드 필드

필드	데이터 유형	설명
파일 로그 아카이브 상태	uint32	파일 로그 아카이브 상태를 나타내는 번호입니다. 이 필드는 이 레코드의 고유 키입니다.
파일 로그 아카이브 상태 설명 길이	uint32	파일 로그 아카이브 상태 설명에 포함된 바이트 수입니다.
파일 로그 아카이브 상태 설명	string	파일 로그 아카이브 상태를 설명하는 이름입니다.

6.0 이상 버전용 파일 로그 정적 분석 메타데이터

eStreamer 서비스는 파일 로그 정적 분석 정보가 포함된 메타데이터를 전송합니다. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 파일 로그 정적 분석 메타데이터 레코드임을 나타내는 519입니다.

다음 표에는 파일 로그 정적 분석 메타데이터 레코드의 필드에 대한 설명이 나와 있습니다.

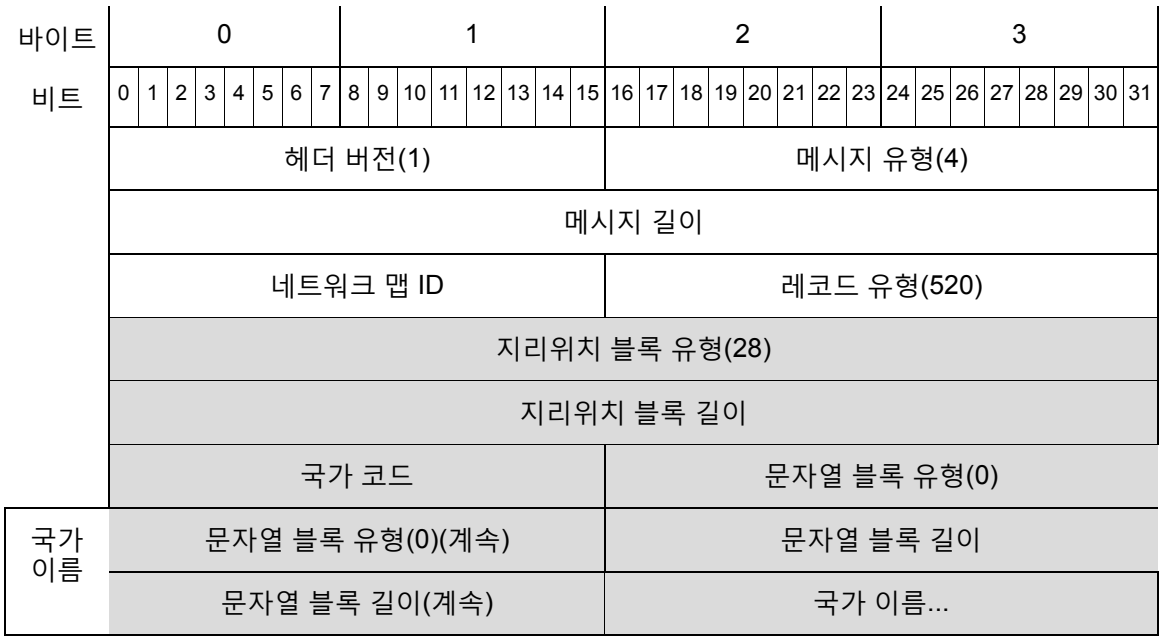
표 3-56 파일 로그 정적 분석 메타데이터 레코드 필드

필드	데이터 유형	설명
파일 로그 정적 분석 상태	uint32	파일 로그 정적 분석 상태를 나타내는 번호입니다. 이 필드는 이 레코드의 고유 키입니다.
파일 로그 정적 분석 상태 설명 길이	uint32	파일 로그 정적 분석 상태 설명에 포함된 바이트 수입니다.
파일 로그 정적 분석 상태 설명	string	파일 로그 정적 분석 상태를 설명하는 이름입니다.

5.2 이상 버전용 지리위치 데이터 블록

국가 이름에 대한 국가 코드 매핑을 포함하는 데이터 블록입니다. 레코드 유형은 520이고 블록 유형은 계열 2의 28입니다. 이 블록은 지리위치 정보가 포함된 모든 이벤트의 메타데이터로 표시됩니다. 메타데이터 요청 시 이벤트에 국가 코드의 값이 있으면 다른 메타데이터와 함께 이 블록이 반환됩니다.

다음 다이어그램에 지리위치 데이터 블록의 구조가 나와 있습니다.



다음 표에는 지리위치 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 3-57 지리위치 데이터 블록 필드

필드	데이터 유형	설명
지리위치 데이터 블록 유형	uint32	지리위치 데이터 블록을 시작합니다. 이 값은 항상 28입니다.
지리위치 데이터 블록 길이	uint32	지리위치 데이터 블록의 총 바이트 수입니다. 여기에는 지리위치 데이터 블록 유형 및 길이 필드의 8바이트에 그 뒤의 데이터 바이트 수를 더한 값이 포함됩니다.
국가 코드	uint16	국가 코드입니다.
문자열 블록 유형	uint32	국가 코드와 관련된 국가 이름을 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Country Name(국가 이름) 필드의 바이트 수를 더한 값이 포함됩니다.
국가 이름	string	국가 코드와 관련된 국가의 이름입니다.

6.0 이상 버전용 파일 정책 이름

eStreamer 서비스는 파일 정책 이름 정보가 포함된 메타데이터를 전송합니다. 해당 메타데이터의 형식은 아래에 나와 있습니다. 메타데이터 플래그 중 하나(요청 메시지의 Request Flags(요청 플래그) 필드에 포함된 비트 1, 14, 15, 20)가 설정되어 있으면 파일 정책 이름 정보가 전송됩니다. 요청 플래그, 2-12페이지의 내용을 참조하십시오. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 파일 정책 이름 레코드임을 나타내는 530입니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	헤더 버전(1)																메시지 유형(4)															
	메시지 길이																															
	네트워크 맵 ID																레코드 유형(530)															
	레코드 길이																															
	UUID 문자열 블록 유형(14)																															
	UUID 문자열 블록 길이																															
	파일 정책 UUID 파일 UUID(계속) 파일 UUID(계속) 파일 UUID(계속)																															
파일 정책 이름	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	파일 정책 이름...																															

다음 표에는 파일 정책 이름 레코드의 필드에 대한 설명이 나와 있습니다.

표 3-58 파일 정책 이름 필드

필드	데이터 유형	설명
UUID 문자열 데이터 블록 유형	uint32	UUID 문자열 데이터 블록을 시작합니다. 이 값은 항상 14입니다.
UUID 문자열 데이터 블록 길이	uint32	UUID 문자열 데이터 블록의 총 바이트 수입니다. 여기에는 UUID 문자열 데이터 블록 유형 및 길이 필드의 8바이트에 그 뒤의 데이터 바이트 수를 더한 값이 포함됩니다.

표 3-58 파일 정책 이름 필드 (계속)

필드	데이터 유형	설명
파일 정책 UUID	uint8[16]	파일 정책의 UUID입니다. 이 필드는 이 레코드의 고유 키입니다.
문자열 블록 유형	uint32	파일 정책의 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	SSL 정책 이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 파일 정책 이름의 바이트 수를 더한 값이 포함됩니다.
파일 정책 이름	string	파일 정책의 이름입니다.

SSL 정책 이름

eStreamer 서비스는 SSL 정책 이름 정보가 포함된 메타데이터를 전송합니다. 해당 메타데이터의 형식은 아래에 나와 있습니다. 메타데이터 플래그 중 하나(요청 메시지의 Request Flags(요청 플래그) 필드에 포함된 비트 1, 14, 15, 20)가 설정되어 있으면 SSL 정책 이름 정보가 전송됩니다. 요청 플래그, 2-12페이지의 내용을 참조하십시오. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 SSL 정책 이름 레코드임을 나타내는 600입니다.

다음 표에는 SSL 정책 이름 레코드의 필드에 대한 설명이 나와 있습니다.

표 3-59 SSL 정책 이름 레코드 필드

필드	데이터 유형	설명
UUID 문자열 데이터 블록 유형	uint32	UUID 문자열 데이터 블록을 시작합니다. 이 값은 항상 14입니다.
UUID 문자열 데이터 블록 길이	uint32	UUID 문자열 데이터 블록의 총 바이트 수입니다. 여기에는 UUID 문자열 데이터 블록 유형 및 길이 필드의 8바이트에 그 뒤의 데이터 바이트 수를 더한 값이 포함됩니다.
SSL 정책 UUID	uint8[16]	SSL 정책의 UUID입니다. 이 필드는 이 레코드의 고유 키입니다.
문자열 블록 유형	uint32	SSL 정책의 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	SSL 정책 이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 SSL 정책 이름의 바이트 수를 더한 값이 포함됩니다.
SSL 정책 이름	string	SSL 정책의 이름입니다.

SSL 규칙 ID

eStreamer 서비스는 SSL 규칙 ID 정보가 포함된 메타데이터를 전송합니다. 해당 메타데이터의 형식은 아래에 나와 있습니다. 메타데이터 플래그 중 하나(요청 메시지의 Request Flags(요청 플래그) 필드에 포함된 비트 1, 14, 15, 20)가 설정되어 있으면 SSL 규칙 ID 정보가 전송됩니다. 요청 플래그, 2-12페이지의 내용을 참조하십시오. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 SSL 규칙 ID 레코드임을 나타내는 601입니다.

다음 표에는 SSL 규칙 ID 레코드의 필드에 대한 설명이 나와 있습니다.

표 3-60 SSL 정책 이름 레코드 필드

필드	데이터 유형	설명
수정	uint8[16]	SSL 규칙 수정의 UUID입니다. 이 필드는 Rule ID(규칙 ID)와 함께 이 레코드의 고유 키를 구성합니다.
규칙 ID	uint32	SSL 규칙의 ID 번호입니다. 이 필드는 Revision(수정)과 함께 이 레코드의 고유 키를 구성합니다.
문자열 블록 유형	uint32	SSL 규칙의 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	SSL 규칙 이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 SSL 규칙 이름의 바이트 수를 더한 값이 포함됩니다.
SSL 규칙 이름	string	SSL 규칙의 이름입니다.

SSL 암호 그룹

eStreamer 서비스는 이벤트에 대한 SSL 암호 그룹 정보가 포함된 메타데이터를 SSL 암호 ID와 함께 전송합니다. 해당 메타데이터의 형식은 아래에 나와 있습니다. 이 레코드는 SSL 암호 ID를 SSL 암호 그룹 이름에 매핑합니다. 메타데이터 플래그 중 하나(요청 메시지의 Request Flags(요청 플래그) 필드에 포함된 비트 1, 14, 15, 20)가 설정되어 있으면 SSL 암호 그룹 정보가 전송됩니다. 요청 플래그, 2-12페이지의 내용을 참조하십시오. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 SSL 암호 그룹 레코드임을 나타내는 602입니다.

다음 표에는 SSL 암호 그룹 레코드의 필드에 대한 설명이 나와 있습니다.

표 3-61 SSL 암호 그룹 필드

필드	데이터 유형	설명
SSL 암호 ID	uint32	SSL 암호 ID 번호입니다. 이 필드는 이 레코드의 고유 키입니다.
SSL 암호 그룹 이름 길이	uint32	SSL 암호 그룹 이름에 포함된 바이트 수입니다.
SSL 암호 그룹 이름	string	SSL 암호 그룹을 설명하는 이름입니다.

SSL 버전

eStreamer 서비스는 이벤트에 대한 SSL 버전 정보가 포함된 메타데이터를 SSL 버전과 함께 전송합니다. 해당 메타데이터의 형식은 아래에 나와 있습니다. 이 레코드는 SSL 버전 ID를 SSL 버전 이름에 매핑합니다. 메타데이터 플래그 중 하나(요청 메시지의 Request Flags(요청 플래그) 필드에 포함된 비트 1, 14, 15, 20)가 설정되어 있으면 SSL 암호 그룹 정보가 전송됩니다. 요청 플래그, 2-12페이지의 내용을 참조하십시오. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 SSL 버전 레코드임을 나타내는 604입니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
헤더 버전(1)																	메시지 유형(4)															
메시지 길이																																
네트워크 맵 ID																	레코드 유형(604)															
레코드 길이																																
SSL 버전 ID																																
SSL 버전 이름 길이																																
SSL 버전 이름...																																

다음 표에는 SSL 버전 레코드의 필드에 대한 설명이 나와 있습니다.

표 3-62 SSL 버전 필드

필드	데이터 유형	설명
SSL 버전 ID	uint32	SSL 버전 ID 번호입니다. 이 필드는 이 레코드의 고유 키입니다.
SSL 버전 이름	uint32	SSL 버전 이름에 포함된 바이트 수입니다.
SSL 암호 그룹 이름	string	SSL 버전을 설명하는 이름입니다.

SSL 서버 인증서 상태

eStreamer 서비스는 SSL 서버 인증서 상태 정보가 포함된 메타데이터를 전송합니다. 해당 메타데이터의 형식은 아래에 나와 있습니다. 메타데이터 플래그 중 하나(요청 메시지의 Request Flags(요청 플래그) 필드에 포함된 비트 1, 14, 15, 20)가 설정되어 있으면 SSL 서버 인증서 상태 정보가 전송됩니다. 요청 플래그, 2-12페이지의 내용을 참조하십시오. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 SSL 서버 인증서 상태 레코드임을 나타내는 605입니다.

다음 표에는 SSL 서버 인증서 상태 레코드의 필드에 대한 설명이 나와 있습니다.

표 3-63 SSL 서버 인증서 상태 레코드 필드

필드	데이터 유형	설명
SSL 서버 인증서 상태	uint32	SSL 서버 인증서 상태 번호입니다. 이 필드는 이 레코드의 고유 키입니다.
SSL 서버 인증서 상태 설명 길이	uint32	SSL 서버 인증서 상태 설명에 포함된 바이트 수입니다.
SSL 서버 인증서 상태 설명	string	SSL 서버 인증서 상태의 설명입니다.

SSL 실제 작업

eStreamer 서비스는 SSL 실제 작업 정보가 포함된 메타데이터를 전송합니다. 해당 메타데이터의 형식은 아래에 나와 있습니다. 메타데이터 플래그 중 하나(요청 메시지의 Request Flags(요청 플래그) 필드에 포함된 비트 1, 14, 15, 20)가 설정되어 있으면 SSL 실제 작업 정보가 전송됩니다. 요청 플래그, 2-12페이지의 내용을 참조하십시오. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 SSL 실제 작업 레코드임을 나타내는 606입니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
헤더 버전(1)																	메시지 유형(4)															
메시지 길이																																
네트워크 맵 ID																	레코드 유형(606)															
레코드 길이																																
SSL 실제 작업 번호																																
SSL 실제 작업 설명 길이																																
SSL 실제 작업 설명...																																

다음 표에는 SSL 실제 작업 레코드의 필드에 대한 설명이 나와 있습니다.

표 3-64 SSL 실제 작업 필드

필드	데이터 유형	설명
SSL 실제 작업 번호	uint32	SSL 실제 작업을 지정하는 숫자입니다. 이 필드는 이 레코드의 고유 키입니다.
SSL 실제 작업 설명 길이	uint32	SSL 실제 작업 설명에 포함된 바이트 수입니다.
SSL 실제 작업 설명	string	SSL 실제 작업의 설명입니다.

SSL 예상 작업

eStreamer 서비스는 SSL 예상 작업 정보가 포함된 메타데이터를 전송합니다. 해당 메타데이터의 형식은 아래에 나와 있습니다. 메타데이터 플래그 중 하나(요청 메시지의 Request Flags(요청 플래그) 필드에 포함된 비트 1, 14, 15, 20)가 설정되어 있으면 SSL 예상 작업 정보가 전송됩니다. 요청 플래그, 2-12페이지의 내용을 참조하십시오. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 SSL 예상 작업 레코드임을 나타내는 607입니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
헤더 버전(1)																	메시지 유형(4)															
메시지 길이																																
네트워크 맵 ID																	레코드 유형(607)															
레코드 길이																																
SSL 예상 작업 번호																																
SSL 예상 작업 설명 길이																																
SSL 예상 작업 설명...																																

다음 표에는 SSL 예상 작업 레코드의 필드에 대한 설명이 나와 있습니다.

표 3-65 SSL 실제 작업 필드

필드	데이터 유형	설명
SSL 예상 작업 번호	uint32	SSL 예상 작업을 지정하는 숫자입니다. 이 필드는 이 레코드의 고유 키입니다.
SSL 예상 작업 설명 길이	uint32	SSL 예상 작업 설명에 포함된 바이트 수입니다.
SSL 예상 작업 설명	string	SSL 예상 작업의 설명입니다.

SSL 플로우 상태

eStreamer 서비스는 SSL 플로우 상태 정보가 포함된 메타데이터를 전송합니다. 해당 메타데이터의 형식은 아래에 나와 있습니다. 메타데이터 플래그 중 하나(요청 메시지의 Request Flags(요청 플래그) 필드에 포함된 비트 1, 14, 15, 20)가 설정되어 있으면 SSL 플로우 상태 정보가 전송됩니다. 요청 플래그, 2-12페이지의 내용을 참조하십시오. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 SSL 플로우 상태 레코드임을 나타내는 608입니다.

다음 표에는 SSL 플로우 상태 레코드의 필드에 대한 설명이 나와 있습니다.

표 3-66 SSL 플로우 상태 필드

필드	데이터 유형	설명
SSL 플로우 상태 번호	uint32	SSL 플로우 상태를 지정하는 숫자입니다. 이 필드는 이 레코드의 고유 키입니다.
SSL 플로우 상태 설명 길이	uint32	SSL 플로우 상태 설명에 포함된 바이트 수입니다.
SSL 플로우 상태 설명	string	SSL 플로우 상태의 설명입니다.

SSL URL 카테고리

eStreamer 서비스는 SSL URL 카테고리 정보가 포함된 메타데이터를 전송합니다. 해당 메타데이터의 형식은 아래에 나와 있습니다. 메타데이터 플래그 중 하나(요청 메시지의 Request Flags(요청 플래그) 필드에 포함된 비트 1, 14, 15, 20)가 설정되어 있으면 SSL URL 카테고리 정보가 전송됩니다. 요청 플래그, 2-12페이지의 내용을 참조하십시오. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 SSL URL 카테고리 레코드임을 나타내는 613입니다.

다음 표에는 SSL URL 카테고리 레코드의 필드에 대한 설명이 나와 있습니다.

표 3-67 SSL URL 카테고리 필드

필드	데이터 유형	설명
SSL URL 카테고리 번호	uint32	SSL URL 카테고리를 지정하는 숫자입니다. 이 필드는 이 레코드의 고유 키입니다.
SSL URL 카테고리 설명 길이	uint32	SSL 서버 URL 카테고리 설명에 포함된 바이트 수입니다.
SSL URL 카테고리 설명	string	SSL URL 카테고리의 설명입니다.

5.4 이상 버전용 SSL 인증서 세부사항 데이터 블록

SSL 인증서와 관련한 세부 정보를 제공하는 데이터 블록입니다. 레코드 유형은 614이고 블록 유형은 계열 2의 50입니다. 이 블록은 SSL 정보가 포함된 모든 이벤트의 메타데이터로 표시됩니다. 여기에는 악성코드 이벤트, 파일 이벤트, 침입 이벤트, 연결 이벤트 및 상관관계 이벤트가 포함됩니다.

다음 다이어그램에 SSL 인증서 세부사항 데이터 블록의 구조가 나와 있습니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
헤더 버전(1)																	메시지 유형(4)															
메시지 길이																																
네트워크 맵 ID																	레코드 유형(614)															
레코드 길이																																
SSL 인증서 세부사항 블록 유형(50)																																
SSL 인증서 세부사항 블록 길이																																
핑거프린트 SHA 해시																																
핑거프린트 SHA 해시(계속)																																
핑거프린트 SHA 해시(계속)																																
핑거프린트 SHA 해시(계속)																																
핑거프린트 SHA 해시(계속)																																
공개 키 SHA 해시																																
공개 키 SHA 해시(계속)																																
공개 키 SHA 해시(계속)																																
공개 키 SHA 해시(계속)																																
공개 키 SHA 해시(계속)																																
일련번호																																
일련번호(계속)																																
일련번호(계속)																																
일련번호(계속)																																
일련번호 길이																																

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
주체 공통 이름	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	주체 공통 이름...																															
주체 조직	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	주체 조직...																															
주체 조직 단위	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	주체 조직 단위...																															
주체 국가	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	주체 국가...																															
발급자 공통 이름	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	발급자 공통 이름...																															
발급자 조직	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	발급자 조직...																															
발급자 조직 단위	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	발급자 조직 단위...																															
발급자 국가	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	발급자 국가...																															

다음 표에는 SSL 인증서 세부사항 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 3-68 SSL 인증서 세부사항 데이터 블록 필드

필드	데이터 유형	설명
SSL 인증서 세부사항 데이터 블록 유형	uint32	SSL 인증서 세부사항 데이터 블록을 시작합니다. 이 값은 항상 50입니다.
SSL 인증서 세부사항 데이터 블록 길이	uint32	SSL 인증서 세부사항 데이터 블록의 총 바이트 수입니다. 여기에는 SSL 인증서 세부사항 데이터 블록 유형 및 길이 필드의 8바이트에 그 뒤의 데이터 바이트 수를 더한 값이 포함됩니다.
핑거프린트 SHA 해시	uint8[20]	SSL 서버 인증서의 SHA1 해시입니다.
공개 키 SHA 해시	uint8[20]	인증서 내에 있는 공개 키를 인증하는 데 사용되는 SHA 해시 값입니다.
일련번호	uint8[20]	발급 CA가 할당한 일련번호입니다. 이 번호는 길이가 20바이트를 초과할 수는 없으며 Serial Number Length(일련번호 길이) 필드에 지정된 대로 20바이트보다 작을 수는 있습니다.
일련번호 길이	uint32	바이트 단위의 일련번호 길이입니다.
문자열 블록 유형	uint32	보안 침해와 관련된 카테고리를 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Category(카테고리) 필드의 바이트 수를 더한 값이 포함됩니다.
주체 공통 이름	string	SSL 인증서의 주체 공통 이름입니다. 이는 일반적으로 인증서 주체의 호스트 및 도메인 이름이지만, 다른 정보가 포함될 수도 있습니다.
문자열 블록 유형	uint32	보안 침해와 관련된 이벤트 유형을 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Event Type(이벤트 유형) 필드의 바이트 수를 더한 값이 포함됩니다.
주체 조직	string	인증서 주체의 조직입니다.
문자열 블록 유형	uint32	보안 침해와 관련된 이벤트 유형을 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.

표 3-68 SSL 인증서 세부사항 데이터 블록 필드 (계속)

필드	데이터 유형	설명
문자열 블록 길이	uint32	이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Event Type(이벤트 유형) 필드의 바이트 수를 더한 값이 포함됩니다.
주체 조직 단위	string	인증서 주체의 조직 단위입니다.
문자열 블록 유형	uint32	보안 침해와 관련된 이벤트 유형을 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Event Type(이벤트 유형) 필드의 바이트 수를 더한 값이 포함됩니다.
주체 국가	string	인증서 주체의 국가입니다.
문자열 블록 유형	uint32	보안 침해와 관련된 카테고리를 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Category(카테고리) 필드의 바이트 수를 더한 값이 포함됩니다.
발급자 공통 이름	string	SSL 인증서의 발급자 공통 이름입니다. 이는 일반적으로 인증서 발급자의 호스트 및 도메인 이름이지만, 다른 정보가 포함될 수도 있습니다.
문자열 블록 유형	uint32	보안 침해와 관련된 이벤트 유형을 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Event Type(이벤트 유형) 필드의 바이트 수를 더한 값이 포함됩니다.
발급자 조직	string	인증서 발급자의 조직입니다.
문자열 블록 유형	uint32	보안 침해와 관련된 이벤트 유형을 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Event Type(이벤트 유형) 필드의 바이트 수를 더한 값이 포함됩니다.
발급자 조직 단위	string	인증서 발급자의 조직 단위입니다.
문자열 블록 유형	uint32	보안 침해와 관련된 이벤트 유형을 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Event Type(이벤트 유형) 필드의 바이트 수를 더한 값이 포함됩니다.
발급자 국가	string	인증서 발급자의 국가입니다.
유효 시작 날짜	uint32	인증서가 발급된 시간의 Unix 타임스탬프입니다.
유효 종료 날짜	uint32	인증서 유효 기간이 종료되는 시간의 Unix 타임스탬프입니다.

네트워크 분석 정책 이름 레코드

eStreamer 서비스는 네트워크 분석 정책 이름 정보가 포함된 메타데이터를 전송합니다. 해당 메타데이터의 형식은 아래에 나와 있습니다. 메타데이터 플래그 중 하나(요청 메시지의 Request Flags(요청 플래그) 필드에 포함된 비트 1, 14, 15, 20)가 설정되어 있으면 네트워크 분석 정책 이름 정보가 전송됩니다. 요청 플래그, 2-12페이지의 내용을 참조하십시오. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 네트워크 분석 정책 이름 레코드임을 나타내는 700입니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	헤더 버전(1)																메시지 유형(4)															
	메시지 길이																															
	네트워크 맵 ID																레코드 유형(700)															
	레코드 길이																															
	UUID 문자열 블록 유형(14)																															
	UUID 문자열 블록 길이																															
	네트워크 분석 정책 UUID 네트워크 분석 UUID(계속) 네트워크 분석 UUID(계속) 네트워크 분석 UUID(계속)																															
문자열 블록	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	네트워크 분석 정책 이름...																															

다음 표에는 네트워크 분석 정책 이름 레코드의 필드에 대한 설명이 나와 있습니다.

표 3-69 네트워크 분석 정책 이름 레코드 필드

필드	데이터 유형	설명
UUID 문자열 데이터 블록 유형	uint32	UUID 문자열 데이터 블록을 시작합니다. 이 값은 항상 14입니다.
UUID 문자열 데이터 블록 길이	uint32	UUID 문자열 데이터 블록의 총 바이트 수입니다. 여기에는 UUID 문자열 데이터 블록 유형 및 길이 필드의 8바이트에 그 뒤의 데이터 바이트 수를 더한 값이 포함됩니다.
네트워크 분석 정책 UUID	uint8[16]	네트워크 분석 정책의 UUID입니다. 이 필드는 이 레코드의 고유 키입니다.
문자열 블록 유형	uint32	네트워크 분석 정책의 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	네트워크 분석 정책 이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 네트워크 분석 정책 이름의 바이트 수를 더한 값이 포함됩니다.
네트워크 분석 정책 이름	string	네트워크 분석 정책의 이름입니다.

검색 및 연결 데이터 구조 이해

이 장에서는 eStreamer 검색 및 연결 이벤트의 메시지에 사용되는 데이터 구조 및 해당 이벤트의 메타데이터에 대해 자세히 설명합니다. 검색 및 연결 이벤트 메시지는 같은 일반 메시지 형식 및 데이터 블록 계열을 사용합니다. 각 메시지의 차이점은 데이터 블록 자체의 콘텐츠입니다.

검색 이벤트에는 다음과 같은 두 가지 이벤트 하위 카테고리가 포함됩니다.

- 호스트 검색 이벤트: 패킷 콘텐츠에서 탐지된 호스트에서 실행 중인 애플리케이션과 호스트 취약점을 비롯하여 매니지드 네트워크의 새 호스트와 변경된 호스트를 식별합니다.
- 사용자 이벤트: 새 사용자 및 로그인 등의 사용자 활동 탐지를 보고합니다.

연결 이벤트는 모니터링되는 호스트와 기타 모든 호스트 간의 세션 트래픽에 대한 정보를 보고합니다. 연결 정보에는 트랜잭션의 첫 번째/마지막 패킷, 소스 및 대상 IP 주소, 소스 및 대상 포트, 송신/수신된 패킷과 바이트의 수가 포함됩니다. 해당하는 경우 연결 이벤트는 세션에 사용되는 클라이언트 애플리케이션 및 URL도 보고합니다.

eStreamer 서버에서 검색 또는 연결 이벤트를 요청하는 방법에 대한 자세한 정보는 요청 플래그, 2-12페이지의 내용을 참조하십시오.

eStreamer 이벤트 데이터 메시지의 일반적인 구조와 콘텐츠에 대한 정보는 이벤트 데이터 메시지 구성 이해, 2-18페이지의 내용을 참조하십시오.

검색 및 연결 이벤트 데이터 구조에 대한 자세한 내용은 이 장의 다음 섹션을 참조하십시오.

- 검색 및 연결 이벤트 데이터 메시지, 4-2페이지에서는 호스트 검색, 사용자 및 연결 메시지에 eStreamer가 사용하는 구조에 대해 대략적으로 설명합니다.
- 검색 및 연결 이벤트 레코드 유형, 4-2페이지에서는 검색 및 연결 이벤트의 레코드 유형에 대해 설명합니다.
- 검색 이벤트의 메타데이터, 4-6페이지에서는 이벤트의 사용자 ID를 사용자 이름으로 변환하는 등 숫자 및 코딩된 데이터를 텍스트로 변환하기 위한 상황 정보 확인용으로 요청할 수 있는 메타데이터 레코드에 대해 설명합니다.
- 검색 이벤트 헤더(5.2 이상), 4-40페이지에서는 모든 검색 및 연결 메시지에 사용되는 표준 이벤트 헤더의 구조와 이벤트 유형 및 이벤트 하위 유형 필드에 표시될 수 있는 값에 대해 설명합니다. 이벤트 유형 및 하위 유형 필드에서는 메시지에서 전달되는 데이터 레코드의 구조를 추가로 정의합니다.
- 이벤트 유형별 호스트 검색 구조, 4-44페이지에서는 다양한 호스트 검색 이벤트 유형에 대해 eStreamer가 사용하는 데이터 레코드의 구조에 대해 설명합니다.
- 이벤트 유형별 사용자 데이터 구조, 4-62페이지에서는 다양한 사용자 이벤트 유형에 대해 eStreamer가 사용하는 데이터 레코드의 구조에 대해 설명합니다.

- 검색(계열 1) 블록 이해, 4-63페이지에서는 검색 및 연결 이벤트 메시지에 복합 레코드를 전달하는 데 사용되는 데이터 블록 구조 계열에 대해 설명합니다. 계열 1 데이터 블록은 상관관계 이벤트에도 표시됩니다.
- 5.0 이상 버전용 사용자 취약점 데이터 블록, 4-158페이지에서는 복합 사용자 이벤트 레코드를 전달하는 데 사용되는 기타 계열 1 블록 구조에 대해 설명합니다.

팁 샘플 검색 이벤트를 보여 주는 예시는 "데이터 구조 예시" 섹션, A-1페이지의 내용을 참조하십시오.

검색 및 연결 이벤트 데이터 메시지

eStreamer는 다음 항목을 포함하는 동일한 메시지 구조로 검색 및 연결 이벤트의 데이터를 패키징합니다.

- 네트워크 맵 ID(옵션)
- 레코드 유형을 정의하는 레코드 헤더
- 이벤트를 식별하고 특성을 지정하며 이벤트 유형 및 하위 유형을 구체적으로 식별하는 검색 이벤트 헤더. 자세한 정보는 검색 이벤트 헤더(5.2 이상), 4-40페이지의 내용을 참조하십시오.
- 블록 헤더와 데이터 블록으로 구성된 데이터 레코드. 검색 및 연결 이벤트 데이터 메시지는 계열 1 데이터 블록을 사용합니다. 자세한 정보는 호스트 검색 및 연결 데이터 블록, 4-64페이지 또는 5.0 이상 버전용 사용자 취약점 데이터 블록, 4-158페이지의 내용을 참조하십시오.

검색 및 연결 이벤트 레코드 유형

다음 표에는 호스트 검색 및 연결 이벤트의 이벤트 레코드 유형과 각 레코드 유형의 이벤트 메시지 구조를 확인할 수 있는 링크가 나와 있습니다. 목록에는 메타데이터 레코드 유형도 포함되어 있습니다. 일부 레코드는 특정 데이터 부분을 저장하는 단일 데이터 블록을 포함합니다. 이러한 데이터 블록은 대다수 데이터 유형을 포함하는 계열 1 블록과 검색 데이터를 구체적으로 포함하는 계열 2 블록으로 구분됩니다. 또한 표에는 각 버전의 상태(현재 또는 레거시)도 나와 있습니다. 현재 레코드는 최신 버전입니다. 레거시 레코드는 이후 버전으로 대체되었지만 여전히 eStreamer에서 요청될 수 있습니다.

표 4-1 검색 및 연결 이벤트 레코드 유형

레코드 유형	포함하는 블록 유형	계열	설명	레코드 상태	데이터 형식의 설명을 확인할 수 있는 위치
10	139	1	새 호스트 탐지됨	현재	새 호스트 및 호스트 마지막 확인 메시지, 4-45페이지
11	103	1	새 TCP 서버	현재	서버 메시지, 4-46페이지
12	103	1	새 UDP 서버	현재	서버 메시지, 4-46페이지
13	4	1	새 네트워크 프로토콜	현재	새 네트워크 프로토콜 메시지, 4-47페이지
14	4	1	새 전송 프로토콜	현재	새 전송 프로토콜 메시지, 4-47페이지
15	122	1	새 클라이언트 애플리케이션	현재	클라이언트 애플리케이션 메시지, 4-47페이지
16	103	1	TCP 서버 정보 업데이트	현재	서버 메시지, 4-46페이지
17	103	1	UDP 서버 정보 업데이트	현재	서버 메시지, 4-46페이지

표 4-1 검색 및 연결 이벤트 레코드 유형 (계속)

레코드 유형	포함하는 블록 유형	계열	설명	레코드 상태	데이터 형식의 설명을 확인할 수 있는 위치
18	53	1	OS 정보 업데이트	현재	운영 체제 업데이트 메시지, 4-49페이지
19	해당 없음	해당 없음	호스트 시간 초과	현재	IP 주소 재사용됨 및 호스트 시간 초과/삭제됨 메시지, 4-50페이지
20	해당 없음	해당 없음	호스트 IP 주소 재사용됨	현재	IP 주소 재사용됨 및 호스트 시간 초과/삭제됨 메시지, 4-50페이지
21	해당 없음	해당 없음	호스트 삭제됨: 호스트 한도 도달함	현재	IP 주소 재사용됨 및 호스트 시간 초과/삭제됨 메시지, 4-50페이지
22	해당 없음	해당 없음	홉 변경	현재	홉 변경 메시지, 4-50페이지
23	해당 없음	해당 없음	TCP 포트 닫힘	현재	TCP 및 UDP 포트 닫힘/시간 초과 메시지, 4-51페이지
24	해당 없음	해당 없음	UDP 포트 닫힘	현재	TCP 및 UDP 포트 닫힘/시간 초과 메시지, 4-51페이지
25	해당 없음	해당 없음	TCP 포트 시간 초과	현재	TCP 및 UDP 포트 닫힘/시간 초과 메시지, 4-51페이지
26	해당 없음	해당 없음	UDP 포트 시간 초과	현재	TCP 및 UDP 포트 닫힘/시간 초과 메시지, 4-51페이지
27	해당 없음	해당 없음	MAC 정보 변경	현재	MAC 주소 메시지, 4-51페이지
28	해당 없음	해당 없음	호스트에 대해 추가 MAC 탐지됨	현재	MAC 주소 메시지, 4-51페이지
29	해당 없음	해당 없음	호스트 IP 주소 변경됨	현재	IP 주소 변경 메시지, 4-48페이지
31	해당 없음	해당 없음	호스트가 라우터/브리지로 식별됨	현재	호스트가 브리지/라우터로 식별됨 메시지, 4-52페이지
34	14	1	VLAN 태그 정보 업데이트	현재	VLAN 태그 정보 업데이트 메시지, 4-52페이지
35	122	1	클라이언트 애플리케이션 시간 초과	현재	클라이언트 애플리케이션 메시지, 4-47페이지
42	35	1	NetBIOS 이름 변경	현재	NetBIOS 이름 변경 메시지, 4-53페이지
44	해당 없음	해당 없음	호스트 삭제됨: 호스트 한도 도달함	현재	IP 주소 재사용됨 및 호스트 시간 초과/삭제됨 메시지, 4-50페이지
45	37	1	배너 업데이트	현재	배너 업데이트 메시지, 4-53페이지
46	55	1	호스트 속성 추가	현재	속성 메시지, 4-57페이지
47	55	1	호스트 속성 업데이트	현재	속성 메시지, 4-57페이지
48	55	1	호스트 속성 삭제	현재	속성 메시지, 4-57페이지
51	103	1	TCP 서버 신뢰도 업데이트	레거시	서버 메시지, 4-46페이지
52	103	1	UDP 서버 신뢰도 업데이트	레거시	서버 메시지, 4-46페이지

표 4-1 검색 및 연결 이벤트 레코드 유형 (계속)

레코드 유형	포함하는 블록 유형	계열	설명	레코드 상태	데이터 형식의 설명을 확인할 수 있는 위치
53	53	1	OS 신뢰도 업데이트	레거시	운영 체제 업데이트 메시지, 4-49페이지
54	해당 없음	해당 없음	핑거프린트 메타데이터	현재	핑거프린트 레코드, 4-7페이지
55	해당 없음	해당 없음	클라이언트 애플리케이션 메타데이터	현재	클라이언트 애플리케이션 레코드, 4-9페이지
57	해당 없음	해당 없음	취약점 메타데이터	현재	취약점 레코드, 4-9페이지
58	해당 없음	해당 없음	임계성 메타데이터	현재	임계성 레코드, 4-12페이지
59	해당 없음	해당 없음	네트워크 프로토콜 메타데이터	현재	네트워크 프로토콜 레코드, 4-12페이지
60	해당 없음	해당 없음	속성 메타데이터	현재	속성 레코드, 4-13페이지
61	해당 없음	해당 없음	스캔 유형 메타데이터	현재	스캔 유형 레코드, 4-14페이지
63	해당 없음	해당 없음	서버 메타데이터	현재	서비스 레코드, 4-15페이지
71	144	1	연결 통계	레거시	5.2.x 버전용 연결 통계 데이터 블록, B-139페이지
71	152	1	연결 통계	레거시	5.3 버전용 연결 통계 데이터 블록, B-154페이지
71	154	1	연결 통계	레거시	5.3.1 버전용 연결 통계 데이터 블록, B-161페이지
71	155	1	연결 통계	레거시	5.4 버전용 연결 통계 데이터 블록, B-168페이지
71	157	1	연결 통계	레거시	5.4.1 버전용 연결 통계 데이터 블록, B-181페이지
71	160	1	연결 통계	레거시	6.0.x 버전용 연결 통계 데이터 블록, B-194페이지
71	163	1	연결 통계	현재	6.2 이상 버전용 연결 통계 데이터 블록, 4-120페이지
73	136	1	연결 청크	현재	연결 청크 메시지, 4-55페이지
74	해당 없음	해당 없음	OS 사용자 설정	현재	사용자 서버 및 운영 체제 메시지, 4-58페이지
75	해당 없음	해당 없음	서버 사용자 설정	현재	사용자 서버 및 운영 체제 메시지, 4-58페이지
76	83	1	프로토콜 사용자 삭제	현재	사용자 프로토콜 메시지, 4-59페이지
77	60	1	클라이언트 애플리케이션 사용자 삭제	현재	사용자 클라이언트 애플리케이션 메시지, 4-59페이지
78	78	1	주소 사용자 삭제	현재	사용자가 호스트 추가 및 삭제 메시지, 4-56페이지
79	77	1	서버 사용자 삭제	현재	서버 사용자 삭제 메시지, 4-56페이지
80	80	1	유효한 취약점 사용자 설정	현재	4.6.1 이상 버전용 취약점 사용자 설정 메시지, 4-55페이지
81	80	1	유효하지 않은 취약점 사용자 설정	현재	4.6.1 이상 버전용 취약점 사용자 설정 메시지, 4-55페이지

표 4-1 검색 및 연결 이벤트 레코드 유형 (계속)

레코드 유형	포함하는 블록 유형	계열	설명	레코드 상태	데이터 형식의 설명을 확인할 수 있는 위치
82	81	1	호스트 임계성 사용자 설정	현재	호스트 임계성 사용자 설정 메시지, 4-57페이지
83	55	1	속성값 사용자 설정	현재	속성값 메시지, 4-58페이지
84	82	1	속성값 사용자 삭제	현재	속성값 메시지, 4-58페이지
85	78	1	사용자가 호스트 추가	현재	사용자가 호스트 추가 및 삭제 메시지, 4-56페이지
86	해당 없음	해당 없음	사용자가 서버 추가	현재	사용자 서버 및 운영 체제 메시지, 4-58페이지
87	60	1	사용자가 클라이언트 애플리케이션 추가	현재	사용자 클라이언트 애플리케이션 메시지, 4-59페이지
88	83	1	사용자가 프로토콜 추가	현재	사용자 프로토콜 메시지, 4-59페이지
89	142	1	사용자가 스캔 결과 추가	현재	스캔 결과 추가 메시지, 4-60페이지
90	해당 없음	해당 없음	소스 유형 레코드	현재	소스 유형 레코드, 4-16페이지
91	해당 없음	해당 없음	소스 애플리케이션 레코드	현재	소스 애플리케이션 레코드, 4-16페이지
92	120	1	사용자 삭제됨 변경 이벤트	현재	사용자 수정 메시지, 4-62페이지
93	120	1	사용자 제거됨 변경 이벤트	현재	사용자 수정 메시지, 4-62페이지
94	120	1	새 사용자 식별 이벤트	현재	사용자 수정 메시지, 4-62페이지
95	121	1	사용자 로그인 변경 이벤트	현재	사용자 정보 업데이트 메시지 블록, 4-62페이지
96	해당 없음	해당 없음	소스 탐지기 레코드	현재	소스 탐지기 레코드, 4-17페이지
98	57	2	사용자 레코드	현재	사용자 레코드, 4-20페이지
101	해당 없음	해당 없음	새 OS 이벤트	현재	새 운영 체제 메시지, 4-60페이지
102	94	1	ID 충돌 이벤트	현재	ID 충돌 및 ID 시간 초과 시스템 메시지, 4-61페이지
103	94	1	ID 시간 초과 이벤트	현재	ID 충돌 및 ID 시간 초과 시스템 메시지, 4-61페이지
106	해당 없음	해당 없음	서드파티 스캐너 취약점 레코드	현재	서드파티 스캐너 취약점 레코드, 4-18페이지
107	122	1	클라이언트 애플리케이션 업데이트	현재	클라이언트 애플리케이션 메시지, 4-47페이지
109	해당 없음	해당 없음	웹 애플리케이션 레코드	현재	웹 애플리케이션 레코드, 4-21페이지
115	해당 없음	해당 없음	보안 영역 이름 레코드	현재	보안 영역 이름 레코드, 3-30페이지
116	14	2	인터페이스 이름 레코드	현재	인터페이스 이름 레코드, 3-31페이지

표 4-1 검색 및 연결 이벤트 레코드 유형 (계속)

레코드 유형	포함하는 블록 유형	계열	설명	레코드 상태	데이터 형식의 설명을 확인할 수 있는 위치
117	14	2	액세스 제어 정책 이름 메타데이터	현재	액세스 제어 정책 이름 레코드, 3-33페이지
118	14	2	침입 정책 이름 레코드	현재	침입 정책 이름 레코드, 4-22페이지
119	14	2	액세스 제어 규칙 ID 레코드	현재	액세스 제어 규칙 ID 레코드 메타데이터, 3-34페이지
120	해당 없음	해당 없음	액세스 제어 규칙 작업 레코드	현재	액세스 제어 규칙 작업 레코드 메타데이터, 4-23페이지
121	해당 없음	해당 없음	URL 카테고리 레코드	현재	URL 카테고리 레코드 메타데이터, 4-24페이지
122	해당 없음	해당 없음	URL 평판 메타데이터	현재	URL 평판 레코드 메타데이터, 4-25페이지
124	21	2	액세스 제어 규칙 이유 메타데이터	현재	액세스 제어 규칙 이유 메타데이터, 4-26페이지
145	64	2	액세스 제어 정책 메타데이터	현재	액세스 제어 정책 메타데이터, 4-28페이지
146	64	2	사전 필터 정책 메타데이터	현재	사전 필터 정책 메타데이터, 4-29페이지
147	21	2	터널 또는 사전 필터 규칙 메타데이터	현재	터널 또는 사전 필터 규칙 메타데이터, 4-31페이지
160	7	1	호스트 IOC 설정 메시지	현재	호스트 IOC 설정 메시지, 4-61페이지
161	39	2	5.3 이상 버전용 IOC 이름 데이터 블록	현재	5.3 이상 버전용 IOC 이름 데이터 블록, 4-37페이지
280	22	2	보안 인텔리전스 카테고리 메타데이터	현재	보안 인텔리전스 카테고리 메타데이터, 4-32페이지
281	해당 없음	해당 없음	보안 인텔리전스 소스/대상 레코드	현재	보안 인텔리전스 소스/대상 레코드, 4-34페이지

검색 이벤트의 메타데이터

메타데이터 버전 번호로 메타데이터를 요청할 수 있습니다. 사용 중인 Firepower System 버전에 해당하는 메타데이터 버전은 메타데이터 이해, 2-41페이지의 내용을 참조하십시오. eStreamer에서 메타데이터 레코드를 스트리밍하는 방법에 대한 중요 정보는 메타데이터 전송, 2-41페이지의 내용을 참조하십시오.

호스트 검색 및 사용자 이벤트 레코드에 대한 다양한 메타데이터 레코드 유형의 구조에 대한 자세한 내용은 다음 항목을 참조하십시오.

- 핑거프린트 레코드, 4-7페이지
- 클라이언트 애플리케이션 레코드, 4-9페이지
- 취약점 레코드, 4-9페이지
- 임계성 레코드, 4-12페이지
- 네트워크 프로토콜 레코드, 4-12페이지

- 속성 레코드, 4-13페이지
- 스캔 유형 레코드, 4-14페이지
- 서비스 레코드, 4-15페이지
- 소스 유형 레코드, 4-16페이지
- 소스 애플리케이션 레코드, 4-16페이지
- 소스 탐지기 레코드, 4-17페이지
- 서드파티 스캐너 취약점 레코드, 4-18페이지
- 사용자 레코드, 4-20페이지
- 웹 애플리케이션 레코드, 4-21페이지
- 침입 정책 이름 레코드, 4-22페이지
- 액세스 제어 규칙 작업 레코드 메타데이터, 4-23페이지
- URL 카테고리 레코드 메타데이터, 4-24페이지
- URL 평판 레코드 메타데이터, 4-25페이지
- 액세스 제어 규칙 이유 메타데이터, 4-26페이지
- 보안 인텔리전스 카테고리 메타데이터, 4-32페이지
- 보안 인텔리전스 소스/대상 레코드, 4-34페이지

침입 및 상관관계 이벤트에 대한 메타데이터 레코드는 침입 이벤트 및 메타 데이터 레코드 유형, 3-1페이지의 내용을 참조하십시오.

핑거프린트 레코드

eStreamer 서비스는 이벤트의 핑거프린트 메타데이터를 핑거프린트 레코드 내에 포함하여 전송합니다. 해당 레코드의 형식은 아래에 나와 있습니다. 메타데이터 플래그 중 하나(요청 메시지의 Request Flags(요청 플래그) 필드에 포함된 비트 1, 14, 15, 20)가 설정되어 있으면 핑거프린트 메타데이터가 전송됩니다. 요청 플래그, 2-12페이지의 내용을 참조하십시오. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 핑거프린트 레코드임을 나타내는 54입니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
헤더 버전(1)																	메시지 유형(4)															
메시지 길이																																
네트워크 맵 ID																	레코드 유형(54)															
레코드 길이																																

다음 표에는 핑거프린트 레코드의 필드에 대한 설명이 나와 있습니다.

표 4-2 핑거프린트 레코드 필드

필드	데이터 유형	설명
핑거프린트 UUID	uint8[16]	운영 체제의 고유 식별자 역할을 하는 핑거프린트 ID 번호입니다. 이 필드는 이 레코드의 고유 키입니다.
OS 이름 길이	uint32	운영 체제 이름에 포함된 바이트 수입니다.
OS 이름	string	핑거프린트에 해당하는 운영 체제 이름입니다.
OS 벤더 길이	uint32	운영 체제 벤더 이름에 포함된 바이트 수입니다.
OS 벤더	string	핑거프린트에 해당하는 운영 체제 벤더의 이름입니다.
OS 버전 길이	uint32	운영 체제 버전에 포함된 바이트 수입니다.
OS 버전	string	핑거프린트에 해당하는 운영 체제 버전입니다.

클라이언트 애플리케이션 레코드

eStreamer 서비스는 이벤트의 클라이언트 애플리케이션 메타데이터를 클라이언트 애플리케이션 레코드 내에 포함하여 전송합니다. 해당 레코드의 형식은 아래에 나와 있습니다. 메타데이터 플래그 중 하나(요청 메시지의 Request Flags(요청 플래그) 필드에 포함된 비트 1, 14, 15, 20)가 설정되어 있으면 클라이언트 애플리케이션 메타데이터가 전송됩니다. 요청 플래그, 2-12페이지의 내용을 참조하십시오. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 클라이언트 애플리케이션 레코드임을 나타내는 55입니다.

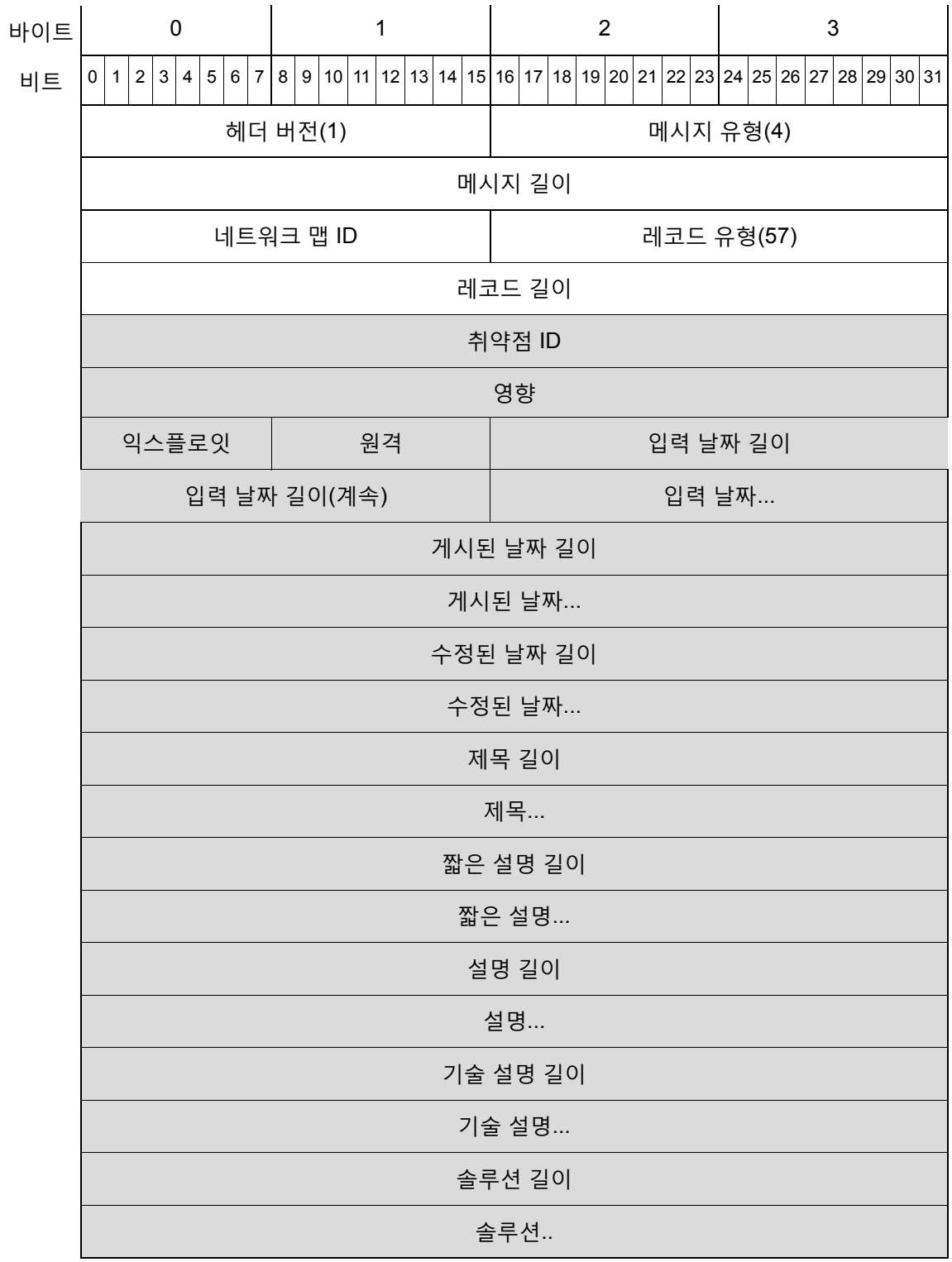
다음 표에는 클라이언트 애플리케이션 레코드의 필드에 대한 설명이 나와 있습니다.

표 4-3 클라이언트 애플리케이션 레코드 필드

필드	데이터 유형	설명
애플리케이션 ID	uint32	클라이언트 애플리케이션의 애플리케이션 ID 번호입니다. 이 필드는 이 레코드의 고유 키입니다.
이름 길이	uint32	이름에 포함된 바이트 수입니다.
이름	string	클라이언트 애플리케이션 이름입니다.

취약점 레코드

eStreamer 서비스는 이벤트에 대한 취약점 정보가 포함된 메타데이터를 취약점 레코드 내에 포함하여 전송합니다. 해당 레코드의 형식은 아래에 나와 있습니다. 메타데이터 플래그 중 하나(요청 메시지의 Request Flags(요청 플래그) 필드에 포함된 비트 1, 14, 15, 20)가 설정되어 있으면 취약점 정보가 전송됩니다. 요청 플래그, 2-12페이지의 내용을 참조하십시오. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 취약점 레코드임을 나타내는 57입니다.


바이트
0
1
2
3
비트
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
헤더 버전(1)
메시지 유형(4)
메시지 길이
네트워크 맵 ID
레코드 유형(57)
레코드 길이
취약점 ID
영향
익스플로잇
원격
입력 날짜 길이
입력 날짜 길이(계속)
입력 날짜...
게시된 날짜 길이
게시된 날짜...
수정된 날짜 길이
수정된 날짜...
제목 길이
제목...
짧은 설명 길이
짧은 설명...
설명 길이
설명...
기술 설명 길이
기술 설명...
솔루션 길이
솔루션..

다음 표에는 취약점 레코드의 필드에 대한 설명이 나와 있습니다.

표 4-4 취약점 레코드 필드

필드	데이터 유형	설명
취약점 ID	uint32	취약점 ID 번호입니다. 이 필드는 이 레코드의 고유 키입니다.
영향	uint32	침입 데이터, 호스트 검색 이벤트, 취약점 평가의 상관관계를 통해 결정되는 영향 레벨에 따라 나타낸 취약점이 미치는 영향입니다. 이 값은 1에서 10까지이며 10은 가장 심각한 경우를 의미합니다. 취약성의 영향력 값은 Bugtraq 항목의 작성자에 의해 결정됩니다.
익스플로잇	uint8	취약점에 대해 알려진 익스플로잇이 있는지를 나타냅니다. 가능한 값은 다음과 같습니다. • 0 - 예 • 1 - 아니요
원격	uint8	네트워크에서 취약점을 익스플로잇할 수 있는지를 나타냅니다. 가능한 값은 다음과 같습니다. • 0 - 예 • 1 - 아니요 • 비어 있음 - 원격 익스플로잇에 대한 취약점을 알 수 없음
입력 날짜 길이	uint32	입력 날짜 필드의 길이입니다.
입력 날짜	string	데이타베이스에 취약점이 입력된 날짜입니다.
게시된 날짜 길이	uint32	게시된 날짜 필드의 길이입니다.
게시된 날짜	string	취약점이 게시된 날짜입니다.
수정된 날짜 길이	uint32	수정된 날짜 필드의 길이입니다.
수정된 날짜	string	해당하는 경우 취약점을 가장 최근에 수정한 날짜입니다.
제목 길이	uint32	제목 필드의 길이입니다.
제목	string	취약점의 제목입니다.
짧은 설명 길이	uint32	짧은 설명 필드의 길이입니다.
짧은 설명	string	취약점에 대한 요약 설명입니다.
설명 길이	uint32	설명 필드의 길이입니다.
설명	string	취약점에 대한 일반적인 설명입니다.
기술 설명 길이	uint32	기술 설명 필드의 길이입니다.
기술 설명	string	취약점에 대한 기술적 설명입니다.
솔루션 길이	uint32	솔루션 필드의 길이입니다.
솔루션	string	취약점에 대한 솔루션입니다.

임계성 레코드

eStreamer 서비스는 이벤트에 대한 호스트 임계성 정보가 포함된 메타데이터를 임계성 레코드 내에 포함하여 전송합니다. 해당 레코드의 형식은 아래에 나와 있습니다. 메타데이터 플래그 중 하나(요청 메시지의 Request Flags(요청 플래그) 필드에 포함된 비트 1, 14, 15, 20)가 설정되어 있으면 임계성 정보가 전송됩니다. 요청 플래그, 2-12페이지의 내용을 참조하십시오. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 임계성 레코드임을 나타내는 58입니다.

다음 표에는 임계성 레코드의 필드에 대한 설명이 나와 있습니다.

표 4-5 임계성 레코드 필드

필드	데이터 유형	설명
임계성 ID	uint32	임계성 ID 번호입니다. 이 필드는 이 레코드의 고유 키입니다.
이름 길이	uint32	임계성 레벨에 포함된 바이트 수입니다.
이름	string	임계성 레벨입니다.

네트워크 프로토콜 레코드

eStreamer 서비스는 이벤트에 대한 네트워크 프로토콜 정보가 포함된 메타데이터를 네트워크 프로토콜 레코드 내에 포함하여 전송합니다. 해당 레코드의 형식은 아래에 나와 있습니다. 메타데이터 플래그 중 하나(요청 메시지의 Request Flags(요청 플래그) 필드에 포함된 비트 1, 14, 15, 20)가 설정되어 있으면 네트워크 프로토콜 정보가 전송됩니다. 요청 플래그, 2-12페이지의 내용을 참조하십시오. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 네트워크 프로토콜 레코드임을 나타내는 59입니다.

다음 표에는 네트워크 프로토콜 레코드의 필드에 대한 설명이 나와 있습니다.

표 4-6 네트워크 프로토콜 레코드 필드

필드	데이터 유형	설명
네트워크 프로토콜 ID	uint32	네트워크 프로토콜 ID 번호입니다. 이 필드는 이 레코드의 고유 키입니다.
이름 길이	uint32	네트워크 프로토콜 이름에 포함된 바이트 수입니다.
이름	string	네트워크 프로토콜의 이름입니다.

속성 레코드

eStreamer 서비스는 이벤트에 대한 속성 정보가 포함된 메타데이터를 속성 레코드 내에 포함하여 전송합니다. 해당 레코드의 형식은 아래에 나와 있습니다. 메타데이터 플래그 중 하나(요청 메시지의 Request Flags(요청 플래그) 필드에 포함된 비트 1, 14, 15, 20)가 설정되어 있으면 속성 정보가 전송됩니다. 요청 플래그, 2-12페이지의 내용을 참조하십시오. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 속성 레코드임을 나타내는 60입니다.

다음 표에는 속성 레코드의 필드에 대한 설명이 나와 있습니다.

표 4-7 속성 레코드 필드

필드	데이터 유형	설명
속성 ID	uint32	속성 ID 번호입니다. 이 필드는 이 레코드의 고유 키입니다.
이름 길이	uint32	속성 이름에 포함된 바이트 수입니다.
이름	string	속성의 이름입니다.

스캔 유형 레코드

eStreamer 서비스는 이벤트에 대한 스캔 유형 정보가 포함된 메타데이터를 스캔 유형 레코드 내에 포함하여 전송합니다. 해당 레코드의 형식은 아래에 나와 있습니다. 메타데이터 플래그 중 하나(요청 메시지의 Request Flags(요청 플래그) 필드에 포함된 비트 1, 14, 15, 20)가 설정되어 있으면 스캔 유형 정보가 전송됩니다. 요청 플래그, 2-12페이지의 내용을 참조하십시오. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 스캔 유형 레코드임을 나타내는 61입니다.

다음 표에는 스캔 유형 레코드의 필드에 대한 설명이 나와 있습니다.

표 4-8 스캔 유형 레코드 필드

필드	데이터 유형	설명
스캔 유형 ID	uint32	스캔 유형 ID 번호입니다. 이 필드는 이 레코드의 고유 키입니다.
이름 길이	uint32	스캔 유형 이름에 포함된 바이트 수입니다.
이름	string	스캔 유형의 이름입니다.

서비스 레코드

eStreamer 서비스는 이벤트에 대한 서비스 정보가 포함된 메타데이터를 서비스 레코드 내에 포함하여 전송합니다. 해당 레코드의 형식은 아래에 나와 있습니다. 서비스 애플리케이션 프로토콜의 애플리케이션 ID에서는 메타데이터에 대한 상호 참조를 제공합니다. 메타데이터 플래그 중 하나(요청 메시지의 Request Flags(요청 플래그) 필드에 포함된 비트 1, 14, 15, 20)가 설정되어 있으면 서비스 정보가 전송됩니다. 요청 플래그, 2-12페이지의 내용을 참조하십시오. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 서비스 레코드임을 나타내는 63입니다.

다음 표에는 서비스 레코드의 필드에 대한 설명이 나와 있습니다.

표 4-9 서비스 레코드 필드

필드	데이터 유형	설명
애플리케이션 ID	uint32	애플리케이션 프로토콜의 애플리케이션 ID 번호입니다. 이 필드는 이 레코드의 고유 키입니다.
이름 길이	uint32	서비스 이름에 포함된 바이트 수입니다.
이름	string	애플리케이션 프로토콜의 이름입니다. 애플리케이션 ID가 65535인 경우 이름은 unknown입니다.

소스 유형 레코드

eStreamer 서비스는 이벤트에 해당하는 소스 애플리케이션에 대한 정보가 포함된 메타데이터를 소스 유형 레코드 내에 포함하여 전송합니다. 해당 레코드의 형식은 아래에 나와 있습니다. 메타데이터 플래그 중 하나(요청 메시지의 Request Flags(요청 플래그) 필드에 포함된 비트 1, 14, 15, 20)가 설정되어 있으면 소스 유형 정보가 전송됩니다. 요청 플래그, 2-12페이지의 내용을 참조하십시오. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 소스 유형 레코드임을 나타내는 90입니다.

다음 표에는 소스 유형 레코드의 필드에 대한 설명이 나와 있습니다.

표 4-10 소스 유형 레코드 필드

필드	데이터 유형	설명
소스 유형 ID	uint32	소스 유형의 ID 번호입니다. 이 필드는 이 레코드의 고유 키입니다.
이름 길이	uint32	소스 유형 이름에 포함된 바이트 수입니다.
이름	string	소스 유형의 이름입니다.

소스 애플리케이션 레코드

eStreamer 서비스는 호스트 검색에 이벤트에 해당하는 소스 애플리케이션에 대한 정보가 포함된 메타데이터를 소스 애플리케이션 레코드 내에 포함하여 전송합니다. 해당 레코드의 형식은 아래에 나와 있습니다. 메타데이터 플래그 중 하나(요청 메시지의 Request Flags(요청 플래그) 필드에 포함된 비트 1, 14, 15, 20)가 설정되어 있으면 소스 애플리케이션 정보가 전송됩니다. 요청 플래그, 2-12페이지의 내용을 참조하십시오. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 소스 애플리케이션 레코드임을 나타내는 91입니다.

다음 표에는 소스 애플리케이션 레코드의 필드에 대한 설명이 나와 있습니다.

표 4-11 소스 애플리케이션 레코드 필드

필드	데이터 유형	설명
소스 애플리케이션 ID	uint32	소스 애플리케이션의 ID 번호입니다. 이 필드는 이 레코드의 고유 키입니다.
이름 길이	uint32	소스 애플리케이션 이름에 포함된 바이트 수입니다.
이름	string	소스 애플리케이션의 이름입니다.

소스 탐지기 레코드

eStreamer 서비스는 호스트 검색에 이벤트에 해당하는 소스 애플리케이션에 대한 정보가 포함된 메타데이터를 소스 유형 레코드 내에 포함하여 전송합니다. 해당 레코드의 형식은 아래에 나와 있습니다. 메타데이터 플래그 중 하나(요청 메시지의 Request Flags(요청 플래그) 필드에 포함된 비트 1, 14, 15, 20)가 설정되어 있으면 소스 유형 정보가 전송됩니다. 요청 플래그, 2-12페이지의 내용을 참조하십시오. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 소스 탐지기 레코드임을 나타내는 96입니다.

다음 표에는 소스 탐지기 레코드의 필드에 대한 설명이 나와 있습니다.

표 4-12 소스 탐지기 레코드 필드

필드	데이터 유형	설명
소스 탐지기 ID	uint32	소스 탐지기의 ID 문자열입니다. 이 필드는 이 레코드의 고유 키입니다.
이름 길이	uint32	소스 유형 이름에 포함된 바이트 수입니다.
이름	string	소스 탐지기의 이름입니다.

서드파티 스캐너 취약점 레코드

eStreamer 서비스는 이벤트에 대한 서드파티 취약점 정보가 포함된 메타데이터를 서드파티 스캐너 취약점 레코드 내에 포함하여 전송합니다. 해당 레코드의 형식은 아래에 나와 있습니다. 메타데이터 플래그 중 하나(요청 메시지의 Request Flags(요청 플래그) 필드에 포함된 비트 1, 14, 15, 20)가 설정되어 있으면 취약점 정보가 전송됩니다. 요청 플래그, 2-12페이지의 내용을 참조하십시오. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 서드파티 스캐너 취약점 레코드임을 나타내는 106입니다.

다음 표에는 취약점 레코드의 필드에 대한 설명이 나와 있습니다.

표 4-13 서드파티 스캐너 취약점 레코드 필드

필드	데이터 유형	설명
취약점 ID	uint32	서드파티 취약점 ID 번호입니다. 이 필드는 Scanner Type(스캐너 유형)과 함께 이 레코드의 고유 키를 구성합니다.
스캐너 유형	uint32	서드파티 스캐너 유형입니다. 이 필드는 Vulnerability ID(취약점 ID)와 함께 이 레코드의 고유 키를 구성합니다.
제목 길이	uint32	제목 필드의 길이입니다.
제목	string	취약점의 제목입니다.
설명 길이	uint32	설명 필드의 길이입니다.
설명	string	취약점에 대한 일반적인 설명입니다.
CVE ID 길이	uint32	CVE ID 필드의 길이입니다.
CVE ID	string	취약점의 CVE(일반 취약점 및 노출) ID 번호입니다.
BugTraq ID 길이	uint32	BugTraq ID 필드의 길이입니다.
BugTraq ID	string	취약점의 BugTraq ID 번호입니다.

사용자 레코드

eStreamer 서비스는 시스템에서 탐지된 사용자에 대한 정보가 포함된 메타데이터를 사용자 유형 레코드 내에 포함하여 전송합니다. 해당 레코드의 형식은 아래에 나와 있습니다. 버전 4 메타데이터 및 정책 이벤트 요청 플래그(각각 요청 메시지의 Request Flags(요청 플래그) 필드에 포함된 비트 20, 22)가 설정되어 있으면 사용자 정보가 전송됩니다. 요청 플래그, 2-12페이지의 내용을 참조하십시오. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 사용자 레코드임을 나타내는 98입니다.

다음 표에는 사용자 레코드의 필드에 대한 설명이 나와 있습니다.

표 4-14 사용자 레코드 필드

필드	데이터 유형	설명
사용자 데이터 블록 유형	uint32	사용자 데이터 블록을 시작합니다. 이 값은 항상 57입니다. 블록 유형은 계열 2 블록입니다.
사용자 데이터 블록 길이	uint32	데이터 블록의 길이입니다. 데이터 바이트 수에 2개 데이터 블록 헤더 필드의 8바이트를 더한 길이입니다.
사용자 ID	uint32	사용자의 고유 식별자입니다. 이 필드는 이 레코드의 고유 키입니다.

표 4-14 사용자 레코드 필드 (계속)

필드	데이터 유형	설명
프로토콜	uint32	사용자를 탐지하거나 보고하는 데 사용되는 프로토콜입니다. 가능한 값은 다음과 같습니다. • 165 - FTP • 426 - SIP • 547 - AOL Instant Messenger • 683 - IMAP • 710 - LDAP • 767 - NTP • 773 - Oracle Database • 788 - POP3 • 1755 - MDNS
문자열 블록 유형	uint32	사용자 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	사용자 이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Username(사용자 이름) 필드의 바이트 수를 더한 값이 포함됩니다.
사용자 이름	string	사용자의 이름입니다.

웹 애플리케이션 레코드

시스템은 사용 가능한 경우 웹사이트에서 HTTP 트래픽의 콘텐츠를 탐지합니다. 호스트 검색 이벤트의 웹 애플리케이션 메타데이터에는 WMV, QuickTime 등 특정 유형의 콘텐츠가 포함될 수 있습니다.

eStreamer 서비스는 이벤트의 웹 애플리케이션 메타데이터를 웹 애플리케이션 레코드 내에 포함하여 전송합니다. 해당 레코드의 형식은 아래에 나와 있습니다. 메타데이터 플래그 중 하나(요청 메시지의 Request Flags(요청 플래그) 필드에 포함된 비트 1, 14, 15, 20)가 설정되어 있으면 웹 애플리케이션 메타데이터가 전송됩니다. 요청 플래그, 2-12페이지의 내용을 참조하십시오. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 웹 애플리케이션 레코드임을 나타내는 109입니다.

다음 표에는 웹 애플리케이션 레코드의 필드에 대한 설명이 나와 있습니다.

표 4-15 웹 애플리케이션 레코드 필드

필드	데이터 유형	설명
애플리케이션 ID	uint32	웹 애플리케이션의 애플리케이션 ID 번호입니다. 이 필드는 이 레코드의 고유 키입니다.
이름 길이	uint32	이름에 포함된 바이트 수입니다.
이름	string	웹 애플리케이션 콘텐츠 이름입니다.

침입 정책 이름 레코드

eStreamer 서비스는 연결 이벤트의 침입 정책 이름 정보가 포함된 메타데이터를 침입 정책 이름 레코드 내에 포함하여 전송합니다. 해당 레코드의 형식은 아래에 나와 있습니다. 메타데이터 플래그 중 하나(요청 메시지의 Request Flags(요청 플래그) 필드에 포함된 버전 4 메타데이터 비트 20)가 설정되어 있으면 침입 정책 이름 정보가 전송됩니다. 요청 플래그, 2-12페이지의 내용을 참조하십시오. Message Length(메시지 길이) 필드 뒤에 표시되는 침입 정책 이름 레코드 필드의 값은 해당 레코드가 침입 정책 이름 레코드임을 나타내는 118입니다. 이 필드에는 UUID 문자열 데이터 블록(계열 2 데이터 블록 집합 내 블록 유형 14)이 포함됩니다.

다음 표에서는 침입 정책 이름 데이터 블록의 필드에 대해 설명합니다.

표 4-16 침입 정책 이름 데이터 블록 필드

필드	데이터 유형	설명
침입 정책 이름 데이터 블록 유형	uint32	침입 정책 이름 데이터 블록을 시작합니다. 이 값은 항상 14입니다. 블록 유형은 계열 2 블록입니다.
침입 정책 이름 데이터 블록 길이	uint32	데이터 블록의 길이입니다. 데이터 바이트 수에 2개 데이터 블록 헤더 필드의 8바이트를 더한 길이입니다.
침입 정책 UUID	uint8[16]	연결 이벤트와 관련된 침입 정책의 고유 식별자입니다. 이 필드는 이 레코드의 고유 키입니다.
문자열 블록 유형	uint32	침입 정책의 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	침입 정책 이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 침입 정책 이름의 바이트 수를 더한 값이 포함됩니다.
침입 정책 이름	string	침입 정책 이름입니다.

액세스 제어 규칙 작업 레코드 메타데이터

eStreamer 서비스는 트리거된 액세스 제어 규칙과 관련된 작업을 포함하는 메타데이터를 액세스 제어 규칙 작업 레코드 내에 포함하여 전송합니다. 해당 레코드의 형식은 아래에 나와 있습니다. 버전 4 메타데이터 플래그(요청 메시지의 Request Flags(요청 플래그) 필드에 포함된 비트 20)가 설정되어 있으면 액세스 제어 규칙 작업 정보가 전송됩니다. 요청 플래그, 2-12페이지의 내용을 참조하십시오. Message Length(메시지 길이) 필드 뒤에 표시되는 액세스 제어 규칙 작업 레코드 필드의 값은 해당 레코드가 액세스 제어 규칙 작업 레코드임을 나타내는 120입니다.

다음 표에는 액세스 제어 규칙 작업 레코드의 필드에 대한 설명이 나와 있습니다.

표 4-17 액세스 제어 규칙 작업 레코드 필드

필드	데이터 유형	설명
액세스 제어 규칙 작업 ID	uint32	액세스 제어 규칙 작업의 ID 번호입니다. 이 필드는 이 레코드의 고유 키입니다.
이름 길이	uint32	이름에 포함된 바이트 수입니다.
이름	string	방화벽 규칙 작업 이름입니다.

URL 카테고리 레코드 메타데이터

eStreamer 서비스는 연결 로그의 URL과 관련된 카테고리 이름을 포함하는 메타데이터를 URL 카테고리 레코드 내에 포함하여 전송합니다. 해당 레코드의 형식은 아래에 나와 있습니다. 버전 4 메타데이터 플래그(요청 메시지의 Request Flags(요청 플래그) 필드에 포함된 비트 20)가 설정되어 있으면 URL 카테고리 정보가 전송됩니다. 요청 플래그, 2-12페이지의 내용을 참조하십시오. Message Length(메시지 길이) 필드 뒤에 표시되는 레코드 필드의 값은 해당 레코드가 URL 카테고리 레코드임을 나타내는 `121`입니다.

다음 표에는 URL 카테고리 레코드의 필드에 대한 설명이 나와 있습니다.

표 4-18 URL 카테고리 레코드 필드

필드	데이터 유형	설명
URL 카테고리 ID	uint32	URL 카테고리의 ID 번호입니다. 이 필드는 이 레코드의 고유 키입니다.
이름 길이	uint32	이름에 포함된 바이트 수입니다.
이름	string	URL 카테고리 이름입니다.

URL 평판 레코드 메타데이터

eStreamer 서비스는 연결 로그의 URL과 관련된 평판(위험 레벨)을 포함하는 메타데이터를 URL 평판 레코드 내에 포함하여 전송합니다. 해당 레코드의 형식은 아래에 나와 있습니다. 버전 4 메타데이터 플래그(요청 메시지의 Request Flags(요청 플래그) 필드에 포함된 비트 20)가 설정되어 있으면 URL 평판 정보가 전송됩니다. 요청 플래그, 2-12페이지의 내용을 참조하십시오. Message Length(메시지 길이) 필드 뒤에 표시되는 URL 평판 메타데이터 레코드 필드의 값은 해당 레코드가 URL 평판 메타데이터 레코드임을 나타내는 `122`입니다.

다음 표에는 URL 평판 레코드의 필드에 대한 설명이 나와 있습니다.

표 4-19 URL 평판 레코드 필드

필드	데이터 유형	설명
URL 평판 ID	uint32	URL 평판의 ID 번호입니다. 이 필드는 이 레코드의 고유 키입니다.
이름 길이	uint32	이름에 포함된 바이트 수입니다.
이름	string	URL 평판 이름입니다.

액세스 제어 규칙 이유 메타데이터

eStreamer 서비스는 액세스 제어 규칙이 침입 이벤트 또는 연결 이벤트를 트리거한 이유에 대한 정보를 포함하는 메타데이터를 액세스 제어 규칙 이유 레코드 내에 포함하여 전송합니다. 해당 레코드의 형식은 아래에 나와 있습니다. 버전 4 메타데이터 플래그(요청 메시지의 Request Flags(요청 플래그) 필드에 포함된 비트 20)가 설정되어 있으면 액세스 제어 규칙 이유 메타데이터가 전송됩니다. 요청 플래그, 2-12페이지의 내용을 참조하십시오. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 액세스 제어 규칙 이유 레코드임을 나타내는 124입니다. 이 레코드는 5.1 이상 버전용 액세스 제어 규칙 이유 데이터 블록, 4-201페이지에 설명되어 있는 액세스 제어 규칙 이유 블록을 포함합니다. 액세스 제어 규칙 이유 데이터 블록은 계열 2의 블록 유형 21입니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
헤더 버전(1)																	메시지 유형(4)															
메시지 길이																																
네트워크 맵 ID																	레코드 유형(124)															
레코드 길이																																
액세스 제어 규칙 이유 블록 유형(21)																																
액세스 제어 규칙 블록 길이																																
액세스 제어 규칙 이유																	문자열 블록 유형(0)															
문자열 블록 유형(0)(계속)																	문자열 블록 길이															
문자열 블록 길이(계속)																	설명...															

다음 표에는 액세스 제어 규칙 ID 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 4-20 액세스 제어 규칙 이유 메타데이터 필드

필드	데이터 유형	설명
액세스 제어 규칙 이유 블록 유형	uint32	액세스 제어 규칙 이유 블록을 시작합니다. 이 값은 항상 21입니다. 이 블록은 계열 2 데이터 블록입니다.
액세스 제어 규칙 이유 블록 길이	uint32	액세스 제어 규칙 이유 블록의 총 바이트 수입니다. 여기에는 액세스 제어 규칙 이유 블록 유형 및 길이 필드의 8바이트에 그 뒤의 데이터 바이트 수를 더한 값이 포함됩니다.
액세스 제어 규칙 이유	uint16	액세스 제어 규칙이 연결을 로깅한 이유입니다. 이 필드는 이 레코드의 고유 키입니다. 이벤트를 트리거한 규칙에 대한 이유 번호입니다. 규칙 이유는 여러 비트가 설정되어 있을 수 있는 이진 비트맵입니다. 규칙 하나에 여러 가지 이유가 있을 수 있습니다. 비트 값은 다음과 같습니다. • **1** - IP 차단 • **2** - IP 모니터 • **4** - 사용자 우회 • **8** - 파일 모니터 • **16** - 악성코드 차단 • **32** - 침입 모니터 • **64** - 악성코드 차단 • **128** - 파일 다시 시작 차단 • **256** -파일 다시 시작 허용 • **512** - 파일 맞춤형 탐지 • **1024** - SSL 차단 • **2048** - DNS 차단 • **4096** - DNS 모니터 • **8192** - URL 차단 • **16384** - URL 모니터 • **32768** - 콘텐츠 제한 • **65536** - 지능형 앱 우회 • **131072** - WSA 위협
문자열 블록 유형	uint32	액세스 제어 규칙 이유와 관련된 설명 이름을 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Description(설명) 필드의 바이트 수를 더한 값이 포함됩니다.
설명	string	액세스 제어 규칙 이유의 설명입니다.

액세스 제어 정책 메타데이터

eStreamer 서비스는 침입 이벤트 또는 연결 이벤트를 트리거한 액세스 제어 정책에 대한 정보를 포함하는 메타데이터를 액세스 제어 정책 메타데이터 레코드 내에 포함하여 전송합니다. 해당 레코드의 형식은 아래에 나와 있습니다. 버전 4 메타데이터 플래그(요청 메시지의 Request Flags(요청 플래그) 필드에 포함된 비트 20)가 설정되어 있으면 액세스 제어 규칙 정책 메타데이터가 전송됩니다. 요청 플래그, 2-12페이지의 내용을 참조하십시오. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 액세스 제어 정책 메타데이터 레코드임을 나타내는 145입니다. 이 레코드는 6.0 이상 버전용 액세스 제어 정책 메타데이터 블록, 4-205페이지에 설명되어 있는 액세스 제어 정책 메타데이터 블록을 포함합니다. 액세스 제어 정책 메타데이터 블록은 계열 2의 블록 유형 64입니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	헤더 버전(1)																메시지 유형(4)															
	메시지 길이																															
	네트워크 맵 ID																레코드 유형(145)															
	레코드 길이																															
	액세스 제어 정책 메타데이터 블록 유형(64)																															
	액세스 제어 정책 메타데이터 블록 길이																															
AC 정책 UUID	액세스 제어 정책 UUID																															
	액세스 제어 정책 UUID(계속)																															
	액세스 제어 정책 UUID(계속)																															
	액세스 제어 정책 UUID(계속)																															
	센서 ID																															
정책 이름	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	정책 이름...																															

다음 표에는 액세스 제어 정책 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 4-21 액세스 제어 정책 메타데이터 필드

필드	데이터 유형	설명
액세스 제어 정책 메타데이터 블록 유형	uint32	액세스 제어 정책 메타데이터 블록을 시작합니다. 이 값은 항상 64입니다. 이 블록은 계열 2 데이터 블록입니다.
액세스 제어 정책 메타데이터 블록 길이	uint32	액세스 제어 정책 메타데이터 블록의 총 바이트 수입니다. 여기에는 액세스 제어 정책 메타데이터 블록 유형 및 길이 필드의 8바이트에 그 뒤의 데이터 바이트 수를 더한 값이 포함됩니다.
액세스 제어 정책 UUID	uint8[16]	액세스 제어 정책의 UUID입니다. 이 필드는 이 레코드의 고유 키입니다.
센서 ID	uint32	액세스 제어 정책과 관련된 센서의 ID 번호입니다. 이 필드는 이 레코드의 고유 키입니다.
문자열 블록 유형	uint32	액세스 제어 정책과 관련된 설명 이름을 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Name(이름) 필드의 바이트 수를 더한 값이 포함됩니다.
이름	string	액세스 제어 정책의 이름입니다.

사전 필터 정책 메타데이터

eStreamer 서비스는 침입 이벤트 또는 연결 이벤트를 트리거한 사전 필터 정책에 대한 정보를 포함하는 메타데이터를 사전 필터 정책 레코드 내에 포함하여 전송합니다. 해당 레코드의 형식은 아래에 나와 있습니다. 버전 4 메타데이터 플래그(요청 메시지의 Request Flags(요청 플래그) 필드에 포함된 비트 20)가 설정되어 있으면 사전 필터 정책 메타데이터가 전송됩니다. 요청 플래그, 2-12페이지의 내용을 참조하십시오. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 사전 필터 정책 메타데이터 레코드임을 나타내는 146입니다. 이 레코드는 6.0 이상 버전용 액세스 제어 정책 메타데이터 블록, 4-205페이지에 설명되어 있는 액세스 제어 정책 메타데이터 블록을 포함합니다. 액세스 제어 정책 메타데이터 블록은 계열 2의 블록 유형 64입니다.

다음 표에는 사전 필터 정책 메타데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 4-22 사전 필터 정책 메타데이터

필드	데이터 유형	설명
사전 필터 블록 유형	uint32	사전 필터 정책 블록을 시작합니다. 이 값은 항상 64입니다. 이 블록은 계열 2 데이터 블록입니다.
사전 필터 정책 블록 길이	uint32	사전 필터 정책 블록의 총 바이트 수입니다. 여기에는 사전 필터 정책 블록 유형 및 길이 필드의 8바이트에 그 뒤의 데이터 바이트 수를 더한 값이 포함됩니다.
액세스 제어 정책 UUID	uint8[16]	액세스 제어 정책의 UUID입니다. 이 필드는 Sensor ID(취약점 ID)와 함께 이 레코드의 고유 키를 구성합니다.
센서 ID	uint32	액세스 제어 정책과 관련된 센서의 ID 번호입니다. 이 필드는 Access Control Policy UUID(액세스 제어 정책 UUID)와 함께 이 레코드의 고유 키를 구성합니다.
문자열 블록 유형	uint32	사전 필터 정책과 관련된 설명 이름을 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Name(이름) 필드의 바이트 수를 더한 값이 포함됩니다.
이름	string	사전 필터 정책의 이름입니다.

터널 또는 사전 필터 규칙 메타데이터

eStreamer 서비스는 터널 또는 사전 필터 규칙이 침입 이벤트 또는 연결 이벤트를 트리거한 이유에 대한 정보를 포함하는 메타데이터를 터널 또는 사전 필터 규칙 이유 레코드 내에 포함하여 전송합니다. 해당 레코드의 형식은 아래에 나와 있습니다. 버전 4 메타데이터 플래그(요청 메시지의 Request Flags(요청 플래그) 필드에 포함된 비트 20)가 설정되어 있으면 터널 또는 사전 필터 규칙 이유 메타데이터가 전송됩니다. 요청 플래그, 2-12페이지의 내용을 참조하십시오. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 터널 또는 사전 필터 규칙 이유 레코드임을 나타내는 147입니다.

이러한 레코드는 콘텐츠가 동일하므로 액세스 제어 규칙 데이터 블록, 4-200페이지에 설명되어 있는 액세스 제어 규칙 이유 블록을 포함합니다. 액세스 제어 규칙 이유 데이터 블록은 계열 2의 블록 유형 15입니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	헤더 버전(1)																메시지 유형(4)															
	메시지 길이																															
	네트워크 맵 ID																레코드 유형(147)															
	레코드 길이																															
	액세스 제어 규칙 블록 유형(15)																															
	액세스 제어 규칙 블록 길이																															
AC 정책 UUID	액세스 제어 정책 UUID																															
	액세스 제어 정책 UUID(계속)																															
	액세스 제어 정책 UUID(계속)																															
	액세스 제어 정책 UUID(계속)																															
	액세스 제어 규칙 ID																															
	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	이름...																															

다음 표에는 터널 또는 사전 필터 규칙 이유 메타데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 4-23 터널 또는 사전 필터 규칙 이유 메타데이터 필드

필드	데이터 유형	설명
액세스 제어 규칙 블록 유형	uint32	액세스 제어 규칙 블록을 시작합니다. 이 값은 항상 15입니다. 이 블록은 액세스 제어 규칙뿐 아니라 터널 및 사전 필터 규칙에도 사용됩니다.
액세스 제어 규칙 블록 길이	uint32	액세스 제어 규칙 블록의 총 바이트 수입니다. 여기에는 액세스 제어 규칙 블록 유형 및 길이 필드의 8바이트에 그 뒤의 데이터 바이트 수를 더한 값이 포함됩니다.
액세스 제어 규칙 UUID	uint8[16]	액세스 제어 규칙의 UUID입니다. 이 필드는 이 레코드의 고유 키입니다. 이 필드는 Access Control Rule ID(액세스 제어 규칙 ID)와 함께 이 레코드의 고유 키를 구성합니다.
액세스 제어 규칙 ID	uint32	액세스 제어 규칙의 ID 번호입니다. 이 필드는 Access Control Rule UUID(액세스 제어 규칙 UUID)와 함께 이 레코드의 고유 키를 구성합니다.
문자열 블록 유형	uint32	액세스 제어 규칙 UUID 및 액세스 제어 규칙 ID와 관련된 설명 이름을 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Name(이름) 필드의 바이트 수를 더한 값이 포함됩니다.
이름	string	설명 이름입니다.

보안 인텔리전스 카테고리 메타데이터

eStreamer 서비스는 보안 인텔리전스 카테고리에 대한 정보가 포함된 메타데이터를 보안 인텔리전스 카테고리 레코드 내에 포함하여 전송합니다. 해당 레코드의 형식은 아래에 나와 있습니다. 버전 4 메타데이터 플래그(요청 메시지의 Request Flags(요청 플래그) 필드에 포함된 비트 20)가 설정되어 있으면 보안 인텔리전스 카테고리 메타데이터가 전송됩니다. 요청 플래그, 2-12페이지의 내용을 참조하십시오. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 보안 인텔리전스 카테고리 레코드임을 나타내는 280입니다. 이 레코드는 5.1 이상 버전용 보안 인텔리전스 카테고리 데이터 블록, 4-203페이지에 설명되어 있는 보안 인텔리전스 카테고리 데이터 블록을 포함합니다. 보안 인텔리전스 카테고리 데이터 블록은 계열 2의 블록 유형 22입니다.

다음 표에는 보안 인텔리전스 카테고리 레코드의 필드에 대한 설명이 나와 있습니다.

표 4-24 보안 인텔리전스 카테고리 메타데이터 필드

필드	데이터 유형	설명
보안 인텔리전스 카테고리 블록 유형	uint32	보안 인텔리전스 카테고리 데이터 블록을 시작합니다. 이 값은 항상 22입니다. 이 블록은 계열 2 데이터 블록입니다.
보안 인텔리전스 카테고리 블록 길이	uint32	보안 인텔리전스 카테고리 블록의 총 바이트 수입니다. 여기에는 보안 인텔리전스 카테고리 블록 유형 및 길이 필드의 8바이트에 그 뒤의 데이터 바이트 수를 더한 값이 포함됩니다.
보안 인텔리전스 목록 ID	uint32	연결에 의해 트리거된 IP 블랙리스트 또는 화이트리스트의 ID입니다. 이 필드는 Access Control Policy UUID(액세스 제어 정책 UUID)와 함께 이 레코드의 고유 키를 구성합니다.
액세스 제어 정책 UUID	uint8[16]	보안 인텔리전스용으로 구성된 액세스 제어 정책의 UUID입니다. 이 필드는 Security Intelligence List ID(보안 인텔리전스 목록 ID)와 함께 이 레코드의 고유 키를 구성합니다.
문자열 블록 유형	uint32	보안 인텔리전스 목록과 관련된 설명 이름을 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.

표 4-24 보안 인텔리전스 카테고리 메타데이터 필드 (계속)

필드	데이터 유형	설명
문자열 블록 길이	uint32	이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Security Intelligence List Name(보안 인텔리전스 목록 이름) 필드의 바이트 수를 더한 값이 포함됩니다.
보안 인텔리전스 목록 이름	string	연결에 의해 트리거된 IP 카테고리 블랙리스트 또는 화이트리스트의 이름입니다.

보안 인텔리전스 소스/대상 레코드

eStreamer 서비스는 보안 인텔리전스가 탐지한 IP 주소가 소스 IP 주소인지 아니면 대상 IP 주소인지에 대한 정보가 포함된 메타데이터를 보안 인텔리전스 소스/대상 레코드 내에 포함하여 전송합니다. 해당 레코드의 형식은 아래에 나와 있습니다. 메타데이터 플래그 중 하나(요청 메시지의 Request Flags(요청 플래그) 필드에 포함된 비트 1, 14, 15, 20)가 설정되어 있으면 소스/대상 IP 정보가 전송됩니다. 요청 플래그, 2-12페이지의 내용을 참조하십시오. Message Length(메시지 길이) 필드 뒤에 표시되는 Record Type(레코드 유형) 필드의 값은 해당 레코드가 보안 인텔리전스 소스/대상 레코드임을 나타내는 `281`입니다.

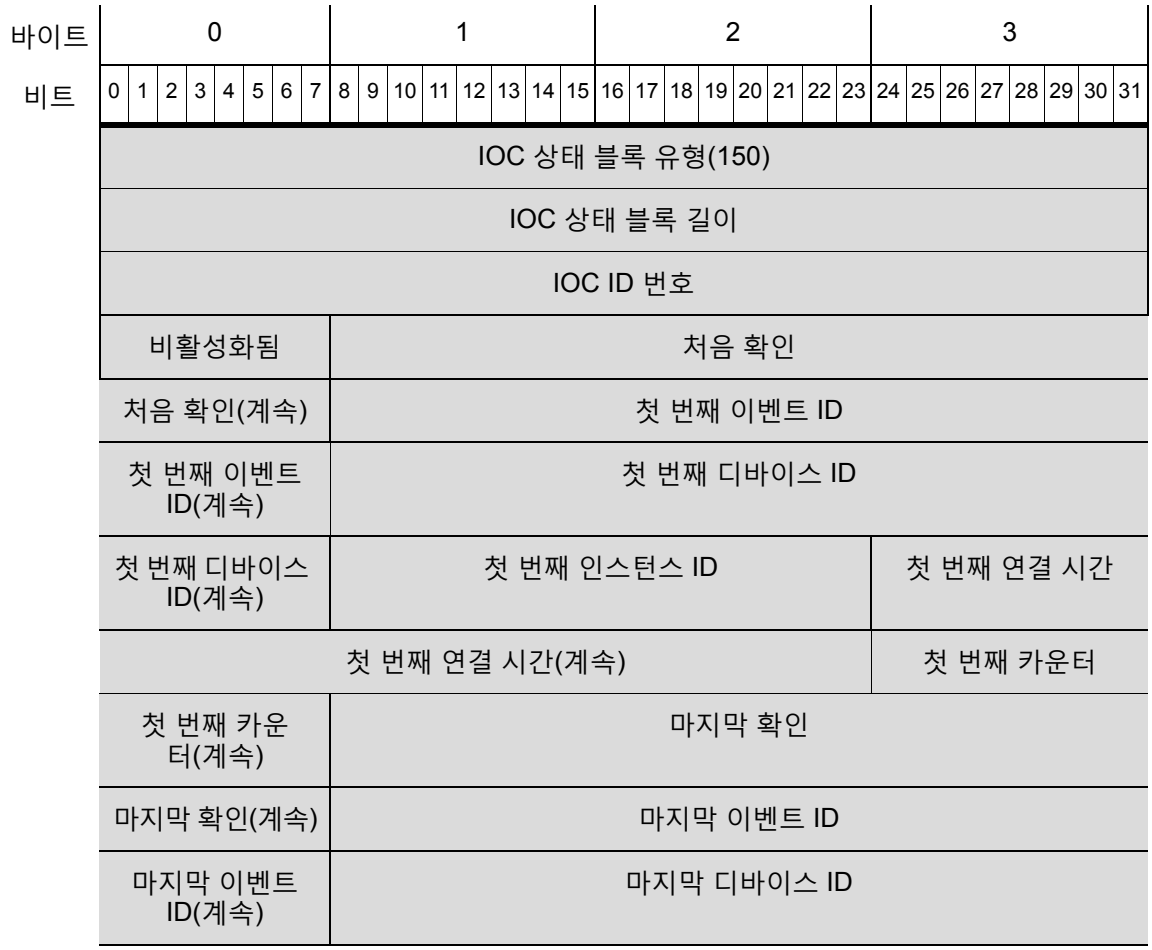
다음 표에는 보안 인텔리전스 소스/대상 레코드의 필드에 대한 설명이 나와 있습니다.

표 4-25 보안 인텔리전스 소스/대상 레코드 필드

필드	데이터 유형	설명
보안 인텔리전스 소스/대상 ID	uint32	보안 인텔리전스 소스/대상 ID 번호입니다. 이 필드는 이 레코드의 고유 키입니다.
보안 인텔리전스 소스/대상 길이	uint32	보안 인텔리전스 소스/대상에 포함된 바이트 수입니다.
보안 인텔리전스 소스/대상	string	탐지된 IP 주소가 소스 IP 주소인지 아니면 대상 IP 주소인지를 나타냅니다.

5.3 이상 버전용 IOC 상태 데이터 블록

IOC(보안 침해 지표) 상태 데이터 블록은 IOC에 대한 정보를 제공합니다. 이 블록은 계열 1의 블록 유형 150이며, 호스트 추적기가 호스트의 보안 침해에 대한 정보를 저장하는 데 사용됩니다. 다음 다이어그램에 IOC 상태 데이터 블록의 구조가 나와 있습니다.



다음 표에서는 IOC 상태 데이터 블록의 구성 요소에 대해 설명합니다.

표 4-26 IOC 상태 데이터 블록 필드

필드	데이터 유형	설명
IOC 상태 데이터 블록 유형	uint32	IOC 상태 데이터 블록을 시작합니다. 이 값은 항상 150입니다.
IOC 상태 데이터 블록 길이	uint32	IOC 상태 데이터 블록의 총 바이트 수입니다. 여기에는 IOC 상태 데이터 블록 유형 및 길이 필드의 8바이트에 그 뒤의 데이터 바이트 수를 더한 값이 포함됩니다.
IOC ID 번호	uint32	보안 침해의 고유한 ID 번호입니다.
비활성화됨	uint8	호스트에서 보안 침해가 비활성화되었는지를 나타냅니다. • 0 - 보안 침해가 비활성화되지 않았습니다. • 1 - 보안 침해가 비활성화되었습니다.
처음 확인	uint32	이 보안 침해가 처음 확인되었을 때의 Unix 타임스탬프입니다.
첫 번째 이벤트 ID	uint32	이 보안 침해가 처음 확인된 이벤트의 ID 번호입니다.
첫 번째 디바이스 ID	uint32	IOC를 처음 탐지한 센서의 ID입니다.
첫 번째 인스턴스 ID	uint16	보안 침해를 처음 탐지한 매니지드 디바이스에 있는 Snort 인스턴스의 숫자 ID입니다.
첫 번째 연결 시간	uint32	이 보안 침해가 처음 확인된 연결의 Unix 타임스탬프입니다.
첫 번째 카운터	uint16	이 보안 침해가 마지막으로 확인된 연결의 카운터입니다. 동시에 진행되는 여러 연결을 구분하는 데 사용됩니다.
마지막 확인	uint32	이 보안 침해가 마지막으로 확인되었을 때의 Unix 타임스탬프입니다.
마지막 이벤트 ID	uint32	이 보안 침해가 마지막으로 확인된 이벤트의 ID 번호입니다.
마지막 디바이스 ID	uint32	IOC를 가장 최근에 탐지한 센서의 ID입니다.
마지막 인스턴스 ID	uint16	보안 침해를 마지막으로 탐지한 매니지드 디바이스에 있는 Snort 인스턴스의 숫자 ID입니다.

표 4-26 IOC 상태 데이터 블록 필드 (계속)

필드	데이터 유형	설명
마지막 연결 시간	uint32	이 보안 침해가 마지막으로 확인된 연결의 Unix 타임스탬프입니다.
마지막 카운터	uint16	이 보안 침해가 마지막으로 확인된 연결의 카운터입니다. 동시에 진행되는 여러 연결을 구분하는 데 사용됩니다.

5.3 이상 버전용 IOC 이름 데이터 블록

이 데이터 블록은 IOC(보안 침해 지표)의 카테고리와 이벤트 유형을 제공합니다. 레코드 유형은 161이고 블록 유형은 계열 2의 39입니다. 이 블록은 IOC 정보가 포함된 모든 이벤트의 메타데이터로 표시됩니다. 여기에는 악성코드 이벤트, 파일 이벤트, 침입 이벤트가 포함됩니다.

다음 다이어그램에 IOC 이름 데이터 블록의 구조가 나와 있습니다.

다음 표에서는 IOC 이름 데이터 블록의 필드에 대해 설명합니다.

표 4-27 IOC 이름 데이터 블록 필드

필드	데이터 유형	설명
IOC 이름 데이터 블록 유형	uint32	IOC 이름 데이터 블록을 시작합니다. 이 값은 항상 39입니다.
IOC 이름 데이터 블록 길이	uint32	IOC 이름 데이터 블록의 총 바이트 수입니다. 여기에는 IOC 이름 데이터 블록 유형 및 길이 필드의 8바이트에 그 뒤의 데이터 바이트 수를 더한 값이 포함됩니다.
IOC ID 번호	uint32	보안 침해의 고유한 ID 번호입니다.
문자열 블록 유형	uint32	보안 침해와 관련된 카테고리를 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Category(카테고리) 필드의 바이트 수를 더한 값이 포함됩니다.
카테고리	string	보안 침해의 카테고리입니다. 가능한 값은 다음과 같습니다. • CnC Connected • Exploit Kit • High Impact Attack • Low Impact Attack • Malware Detected • Malware Executed • Dropper Infection • Java Compromise • Word Compromise • Adobe Reader Compromise • Excel Compromise • PowerPoint Compromise • QuickTime Compromise
문자열 블록 유형	uint32	보안 침해와 관련된 이벤트 유형을 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Event Type(이벤트 유형) 필드의 바이트 수를 더한 값이 포함됩니다.

표 4-27 IOC 이름 데이터 블록 필드 (계속)

필드	데이터 유형	설명
이벤트 유형	string	보안 침해의 이벤트 유형입니다. 가능한 값은 다음과 같습니다. • Adobe Reader launched shell • Dropper Infection Detected by AMP for Endpoints • Excel Compromise Detected by AMP for Endpoints • Excel launched shell • Impact 1 Intrusion Event - attempted-admin • Impact 1 Intrusion Event - attempted-user • Impact 1 Intrusion Event - successful-admin • Impact 1 Intrusion Event - successful-user • Impact 1 Intrusion Event - web-application-attack • Impact 2 Intrusion Event - attempted-admin • Impact 2 Intrusion Event - attempted-user • Impact 2 Intrusion Event - successful-admin • Impact 2 Intrusion Event - successful-user • Impact 2 Intrusion Event - web-application-attack • Intrusion Event - exploit-kit • Intrusion Event - malware-backdoor • Intrusion Event - malware-cnc • Java Compromise Detected by AMP for Endpoints • Java launched shell • PDF Compromise Detected by AMP for Endpoints • PowerPoint Compromise Detected by AMP for Endpoints • PowerPoint launched shell • QuickTime Compromise Detected by AMP for Endpoints • QuickTime launched shell • Security Intelligence Event - CnC • Security Intelligence Event - DNS CnC • Security Intelligence Event - DNS Malware • Security Intelligence Event - DNS Phishing • Security Intelligence Event - Sinkhole CnC • Security Intelligence Event - Sinkhole Malware • Security Intelligence Event - Sinkhole Phishing • Security Intelligence Event - URL CnC • Security Intelligence Event - URL Malware • Security Intelligence Event - URL Phishing • Suspected Botnet Detected by AMP for Endpoints • Threat Detected by AMP for Endpoints - Executed • Threat Detected by AMP for Endpoints - Not Executed • Threat Detected in File Transfer • Word Compromise Detected by AMP for Endpoints • Word launched shell

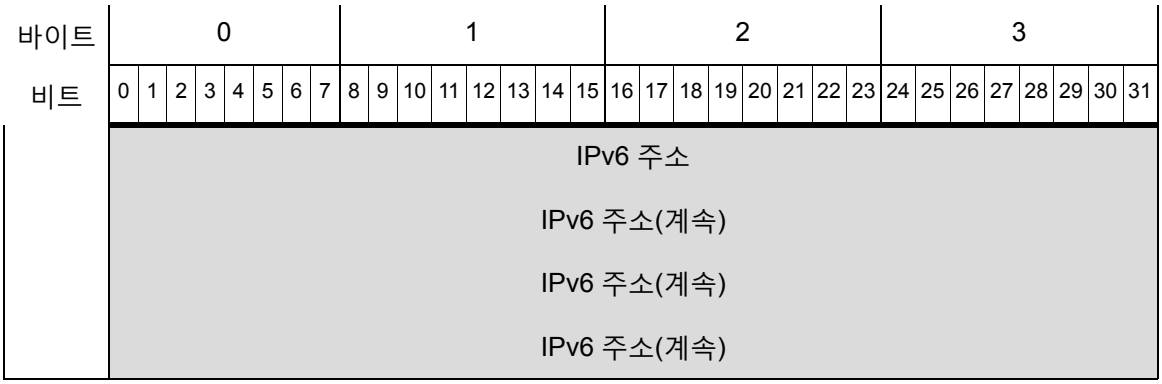
검색 이벤트 헤더(5.2 이상)

검색 및 연결 이벤트 메시지에는 검색 이벤트 헤더가 포함됩니다. 이 헤더는 이벤트의 유형과 하위 유형, 이벤트가 발생한 시간과 디바이스, 그리고 메시지의 이벤트 데이터 구조에 대한 정보를 전달합니다. 이 헤더 뒤에는 실제 호스트 검색, 사용자 또는 연결 이벤트 데이터가 옵니다. 구조는 이벤트 유형별 호스트 검색 구조, 4-44페이지에 설명되어 있는 각 이벤트 유형/하위 유형 값과 연결됩니다. 이 헤더는 IPv6을 지원하며 5.0~5.1.1.x 버전용 검색 이벤트 헤더, B-90페이지의 사용을 중단합니다.

검색 이벤트 헤더의 이벤트 유형 및 이벤트 하위 유형 필드는 전송된 이벤트 메시지의 구조를 식별합니다. 이벤트 데이터 블록의 구조가 확인되면 프로그램이 메시지를 적절하게 구문 분석할 수 있습니다.

다음 다이어그램에서 음영으로 표시된 행은 검색 이벤트 헤더의 형식을 나타냅니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	헤더 버전(1)																메시지 유형(4)															
	메시지 길이																															
	네트워크 맵 ID																레코드 유형															
	레코드 길이																															
	eStreamer 서버 타임스탬프(이벤트에서 비트 23이 설정된 경우에 한함)																															
	이후 사용을 위해 예약됨(이벤트에서 비트 23이 설정된 경우에 한함)																															
검색 이벤트 헤더	디바이스 ID																															
	레거시 IP 주소																															
	MAC 주소																															
	MAC 주소(계속)																IPv6 있음								이후 사용을 위해 예약됨							
	이벤트 초																															
	이벤트 마이크로초																															
	이벤트 유형																															
	이벤트 하위 유형																															
	파일 번호(내부 전용)																															
	파일 위치(내부 전용)																															



다음 표에는 검색 이벤트 헤더에 대한 설명이 나와 있습니다.

표 4-28 검색 이벤트 헤더 필드

필드	데이터 유형	설명
디바이스 ID	uint32	검색 이벤트를 생성한 디바이스의 ID 번호입니다. 버전 3 및 4 메타데이터를 요청하면 디바이스의 메타데이터를 가져올 수 있습니다. 자세한 정보는 매니지드 디바이스 레코드 메타데이터, 3-35페이지의 내용을 참조하십시오.
레거시 IP 주소	uint32	이 필드는 예약되지만 더 이상 내용이 입력되지는 않습니다. IPv4 주소는 IPv6 Address(IPv6 주소) 필드에 저장됩니다. 자세한 정보는 IP 주소, 1-5페이지의 내용을 참조하십시오.
MAC 주소	uint8[6]	이벤트와 관련된 호스트의 MAC 주소입니다.
IPv6 있음	uint8	호스트에 IPv6 주소가 있음을 나타내는 플래그입니다.
이후 사용을 위해 예약됨	uint8	이후 사용을 위해 예약됨
이벤트 초	uint32	시스템에서 이벤트를 생성한 UNIX 타임스탬프(1970년 1월 1일 이후의 초 단위 시간)입니다.
이벤트 마이크로초	uint32	시스템이 이벤트를 생성한 마이크로초(100만분의 1초) 단위의 증분 시간입니다.
이벤트 유형	uint32	이벤트 유형(새 이벤트의 경우 `1000`, 변경 이벤트의 경우 `1001`, 사용자 입력 이벤트의 경우 `1002`, 전체 호스트 프로파일의 경우 `1050`)입니다. 사용 가능한 이벤트 유형의 목록은 이벤트 유형별 호스트 검색 구조, 4-44페이지의 내용을 참조하십시오.
이벤트 하위 유형	uint32	이벤트 하위 유형입니다. 사용 가능한 이벤트 하위 유형의 목록은 이벤트 유형별 호스트 검색 구조, 4-44페이지의 내용을 참조하십시오.
파일 번호	byte[4]	직렬 파일 번호입니다. 이 필드는 Cisco 내부용이므로 무시해도 됩니다.
파일 위치	byte[4]	직렬 파일에서 이벤트의 위치입니다. 이 필드는 Cisco 내부용이므로 무시해도 됩니다.
IPv6 주소	uin8[16]	IPv6 주소입니다. Has IPv6(IPv6 있음) 플래그가 설정되어 있으면 이 필드가 있으며 사용됩니다.

검색 및 연결 이벤트 유형 및 하위 유형

Event Type(이벤트 유형) 및 Event Subtype(이벤트 하위 유형) 필드의 값은 호스트 검색 또는 사용자 데이터 메시지에 포함된 이벤트를 식별하고 분류합니다. 또한 메시지의 데이터 구조도 식별합니다.

다음 표에는 검색 및 연결 이벤트의 이벤트 유형 및 하위 유형이 나와 있습니다.

표 4-29 유형 및 하위 유형별 검색 및 연결 이벤트

이벤트명	이벤트 유형	이벤트 하위 유형
새 호스트	1000	1
새 TCP 서버	1000	2
새 네트워크 프로토콜	1000	3
새 전송 프로토콜	1000	4
새 IP - IP 트래픽	1000	5
새 UDP 서버	1000	6
새 클라이언트 애플리케이션	1000	7
새 OS	1000	8
새 IPv6 - IPv6 트래픽	1000	9
호스트 IP 주소 변경됨	1001	1
OS 정보 업데이트	1001	2
호스트 IP 주소 재사용됨	1001	3
취약점 변경	1001	4
홉 변경	1001	5
TCP 서버 정보 업데이트	1001	6
호스트 시간 초과	1001	7
TCP 포트 닫힘	1001	8
UDP 포트 닫힘	1001	9
UDP 서버 정보 업데이트	1001	10
TCP 포트 시간 초과	1001	11
UDP 포트 시간 초과	1001	12
MAC 정보 변경	1001	13
호스트에 대해 추가 MAC 탐지됨	1001	14
호스트 마지막 확인	1001	15
호스트가 라우터/브리지로 식별됨	1001	16
연결 통계	1001	17
VLAN 태그 정보 업데이트	1001	18
호스트 삭제됨: 호스트 한도 도달함	1001	19
클라이언트 애플리케이션 시간 초과	1001	20
NetBIOS 이름 변경	1001	21

표 4-29 유형 및 하위 유형별 검색 및 연결 이벤트 (계속)

이벤트명	이벤트 유형	이벤트 하위 유형
NetBIOS 도메인 변경	1001	22
호스트 삭제됨: 호스트 한도 도달함	1001	23
배너 업데이트	1001	24
TCP 서버 신뢰도 업데이트	1001	25
UDP 서버 신뢰도 업데이트	1001	26
ID 충돌	1001	29
ID 시간 초과	1001	30
보조 호스트 업데이트	1001	31
클라이언트 애플리케이션 업데이트	1001	32
유효한 취약점 사용자 설정(레거시)	1002	1
유효하지 않은 취약점 사용자 설정(레거시)	1002	2
주소 사용자 삭제(레거시)	1002	3
서버 사용자 삭제(레거시)	1002	4
호스트 임계성 사용자 설정	1002	5
호스트 속성 추가	1002	6
호스트 속성 업데이트	1002	7
호스트 속성 삭제	1002	8
호스트 속성 설정 값(레거시)	1002	9
호스트 속성 삭제 값(레거시)	1002	10
스캔 결과 추가	1002	11
취약점 자격 사용자 설정	1002	12
사용자 정책 제어	1002	13
프로토콜 삭제	1002	14
클라이언트 애플리케이션 삭제	1002	15
운영 체제 사용자 설정	1002	16
사용자 계정 확인됨	1002	17
사용자 계정 업데이트	1002	18
서버 사용자 설정	1002	19
주소 사용자 삭제(현재)	1002	20
서버 사용자 삭제(현재)	1002	21
유효한 취약점 사용자 설정(현재)	1002	22
유효하지 않은 취약점 사용자 설정(현재)	1002	23
사용자 호스트 임계성	1002	24
호스트 속성 설정 값(현재)	1002	25
호스트 속성 삭제 값(현재)	1002	26
사용자가 호스트 추가	1002	27

표 4-29 유형 및 하위 유형별 검색 및 연결 이벤트 (계속)

이벤트명	이벤트 유형	이벤트 하위 유형
사용자가 서버 추가	1002	28
사용자가 클라이언트 애플리케이션 추가	1002	29
사용자가 프로토콜 추가	1002	30
앱 다시 로드	1002	31
계정 삭제	1002	32
연결 통계	1003	1
연결 청크	1003	2
새 사용자 ID	1004	1
사용자 로그인	1004	2
사용자 ID 삭제	1004	3
사용자 ID 삭제됨: 사용자 한도 도달	1004	4
호스트 IOC 설정 유형	1008	1
전체 호스트 프로파일	1050	해당 없음

팁 각 이벤트 유형/하위 유형에 사용되는 데이터 구조에 대한 자세한 정보는 이벤트 유형별 호스트 검색 구조, 4-44페이지의 내용을 참조하십시오.

이벤트 유형별 호스트 검색 구조

eStreamer에서는 검색 이벤트 헤더에 나와 있는 이벤트 유형에 따라 호스트 검색 이벤트 메시지를 작성합니다. 다음 하위 섹션에서는 각 이벤트 형식에 대해 대략적으로 설명합니다.

- NetBIOS 이름 변경 메시지, 4-53페이지
- 배너 업데이트 메시지, 4-53페이지
- 정책 제어 메시지, 4-54페이지
- 연결 통계 데이터 메시지, 4-54페이지
- 연결 청크 메시지, 4-55페이지
- 4.6.1 이상 버전용 취약점 사용자 설정 메시지, 4-55페이지
- 사용자가 호스트 추가 및 삭제 메시지, 4-56페이지
- 서버 사용자 삭제 메시지, 4-56페이지
- 호스트 임계성 사용자 설정 메시지, 4-57페이지
- 속성 메시지, 4-57페이지
- 속성값 메시지, 4-58페이지
- 사용자 서버 및 운영 체제 메시지, 4-58페이지
- 사용자 프로토콜 메시지, 4-59페이지
- 사용자 클라이언트 애플리케이션 메시지, 4-59페이지
- 스캔 결과 추가 메시지, 4-60페이지
- 새 운영 체제 메시지, 4-60페이지
- ID 충돌 및 ID 시간 초과 시스템 메시지, 4-61페이지
- 호스트 IOC 설정 메시지, 4-61페이지

다음 섹션의 데이터 블록 다이어그램에는 호스트 검색 이벤트 메시지에서 반환되는 각 레코드 데이터 블록이 나와 있습니다.

새 호스트 및 호스트 마지막 확인 메시지

새 호스트 및 호스트 마지막 확인 이벤트 메시지에는 5.2 이상 버전용 호스트 프로파일 데이터 블록, 4-164페이지에 설명되어 있는 것처럼 표준 검색 이벤트 헤더 및 호스트 프로파일 데이터 블록이 포함되어 있습니다. 호스트 프로파일 데이터 블록은 계열 1의 블록 유형 139입니다.

호스트 마지막 확인 메시지에는 검색 탐지 정책에 설정된 업데이트 간격 이내에 변경된 호스트의 서버에 대한 서버 정보만 포함됩니다. 즉, 시스템에서 마지막으로 정보를 보고한 이후에 변경된 서버만 호스트 마지막 확인 메시지에 포함됩니다.

참고 호스트 프로파일 데이터 블록은 메시지를 생성한 시스템 버전에 따라 달라집니다. 호스트 프로파일 데이터 블록의 레거시 버전에 대한 자세한 정보는 레거시 호스트 데이터 구조, B-274페이지의 내용을 참조하십시오.

서버 메시지

다음 TCP 및 UDP 서버 이벤트 메시지에는 검색 이벤트 헤더(5.2 이상), 4-40페이지에 설명되어 있는 표준 검색 이벤트 헤더와 4.10.0 이상 버전용 호스트 서버 데이터 블록, 4-138페이지에 설명되어 있는 서버 데이터 블록(계열 1의 블록 유형 103)이 차례로 포함되어 있습니다.

- 새 TCP 서버
- 새 UDP 서버
- TCP 서버 정보 업데이트
- UDP 서버 정보 업데이트
- TCP 서버 신뢰도 업데이트
- UDP 서버 신뢰도 업데이트

참고 서버 데이터 블록은 메시지를 생성한 시스템 버전에 따라 달라집니다. 서버 데이터 블록의 레거시 버전에 대한 자세한 정보는 레거시 데이터 구조 이해, B-1페이지의 내용을 참조하십시오.

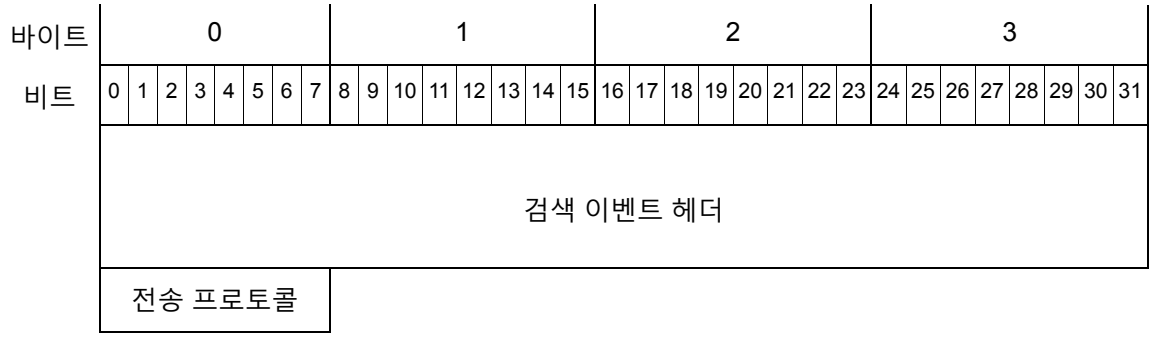
이러한 각 이벤트는 다음 형식을 사용합니다.

새 네트워크 프로토콜 메시지

새 네트워크 프로토콜 이벤트 메시지에는 검색 이벤트 헤더(5.2 이상), 4-40페이지에 설명되어 있는 표준 검색 이벤트 헤더와 네트워크 프로토콜의 2바이트 필드(아래 표에 설명되어 있는 프로토콜 값을 사용함)가 차례로 포함되어 있습니다.

새 전송 프로토콜 메시지

새 전송 프로토콜 이벤트 메시지에는 검색 이벤트 헤더(5.2 이상), 4-40페이지에 설명되어 있는 표준 검색 이벤트 헤더(계열 1의 블록 유형 4)와 전송 프로토콜 번호의 1바이트 필드(아래 표에 설명되어 있는 값을 사용함)가 차례로 포함되어 있습니다.



클라이언트 애플리케이션 메시지

새 클라이언트 애플리케이션, 클라이언트 애플리케이션 업데이트 및 클라이언트 애플리케이션 시간 초과 이벤트는 형식이 동일하며 검색 이벤트 헤더(5.2 이상), 4-40페이지에 설명되어 있는 표준 검색 이벤트 헤더와 클라이언트 애플리케이션 데이터 블록(5.0 이상 버전용 호스트 클라이언트 애플리케이션 데이터 블록, 4-156페이지 참조, 계열 1의 블록 유형 122)을 차례로 포함합니다. 전송되는 이벤트에 따라 검색 이벤트 헤더의 레코드 유형, 이벤트 유형 및 이벤트 하위 유형이 달라집니다.

참고 클라이언트 애플리케이션 데이터 블록은 메시지를 생성한 시스템 버전에 따라 달라집니다. 클라이언트 애플리케이션 데이터 블록의 레거시 버전에 대한 자세한 정보는 레거시 데이터 구조 이해, B-1페이지의 내용을 참조하십시오.

IP 주소 변경 메시지

다음 호스트 검색 메시지는 검색 이벤트 헤더(5.2 이상), 4-40페이지에 설명되어 있는 표준 검색 이벤트 헤더를 포함하며 서로 다른 두 가지 형식(구조)으로 되어 있습니다. 그중 하나는 IP 주소 4바이트를 포함하는 형식이고 다른 하나는 IP 주소 16바이트를 포함하는 형식입니다.

다음과 같은 경우에는 IP 주소 옥텟에서 IP 주소에 4바이트가 사용됩니다.

- 새 IPv4 - IPv4 트래픽
- 호스트 IP 주소 변경됨(RNA 이벤트 버전이 10 미만인 경우)

다음과 같은 경우에는 IP 주소에 16바이트가 사용됩니다.

- 새 IPv6 - IPv6 트래픽
- 호스트 IP 주소 변경됨(RNA 이벤트 버전이 10인 경우)

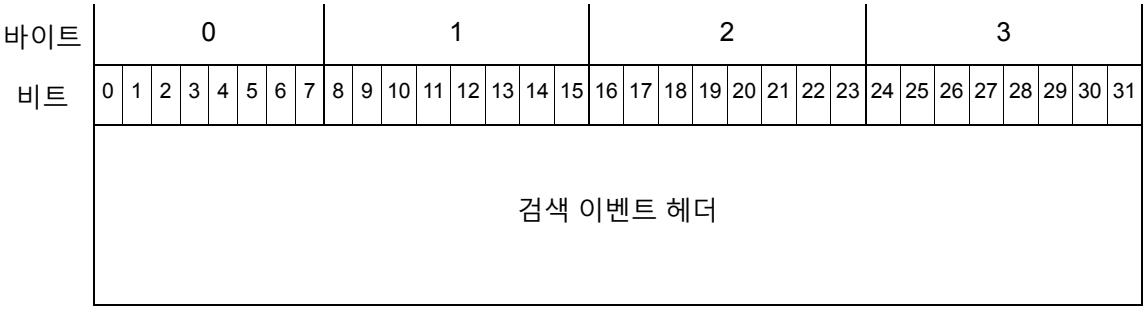
운영 체제 업데이트 메시지

OS 정보 업데이트 이벤트 메시지에는 검색 이벤트 헤더(5.2 이상), 4-40페이지에 설명되어 있는 표준 검색 이벤트 헤더와 3.5 이상 버전용 운영 체제 데이터 블록, 4-87페이지에 설명되어 있는 운영 체제 데이터 블록(계열 1의 블록 유형 53)이 차례로 포함되어 있습니다.

IP 주소 재사용됨 및 호스트 시간 초과/삭제됨 메시지

다음 호스트 이벤트 메시지에는 검색 이벤트 헤더(5.2 이상), 4-40페이지에 설명되어 있는 표준 검색 이벤트 헤더만 포함되며 다른 데이터는 포함되지 않습니다.

- 호스트 IP 주소 재사용됨
- 호스트 시간 초과
- 호스트 삭제됨: 호스트 한도 도달함
- 호스트 삭제됨: 호스트 한도 도달함



홉 변경 메시지

홉 변경 이벤트 메시지에는 검색 이벤트 헤더(5.2 이상), 4-40페이지에 설명되어 있는 표준 검색 이벤트 헤더와 홉 수의 1바이트 필드가 차례로 포함되어 있습니다.

TCP 및 UDP 포트 닫힘/시간 초과 메시지

TCP 및 UDP 포트 닫힘 및 포트 시간 초과 이벤트 메시지에는 검색 이벤트 헤더(5.2 이상), 4-40페이지에 설명되어 있는 표준 검색 이벤트 헤더와 포트 번호의 2바이트 필드가 차례로 포함되어 있습니다.

MAC 주소 메시지

MAC 정보 변경 및 호스트에 대해 추가 MAC 탐지됨 메시지에는 검색 이벤트 헤더(5.2 이상), 4-40페이지에 설명되어 있는 표준 검색 이벤트 헤더, TTL 값 1바이트, MAC 주소 6바이트, 그리고 MAC 주소가 실제 ARP/DHCP 트래픽을 통해 MAC 주소로 탐지되었는지를 나타내는 1바이트가 포함되어 있습니다.

참고 4.9.x 버전을 실행 중인 시스템에서 MAC 주소 메시지가 수신되는 경우에는 메시지 내용에 따라 MAC 주소 데이터 블록의 길이를 확인하고 디코딩해야 합니다. 데이터 블록 길이가 8바이트(헤더 포함 시 16바이트)인 경우 MAC 주소 메시지, 4-51페이지의 내용을 참조하십시오. 데이터 블록 길이가 12바이트(헤더 포함 시 20바이트)인 경우 4.9 이상 버전용 호스트 MAC 주소, 4-117페이지의 내용을 참조하십시오.

MAC 정보 변경 및 호스트에 대해 추가 MAC 탐지됨 메시지 내에서는 MAC 주소 데이터 블록 헤더가 사용되지 **않습니다**.

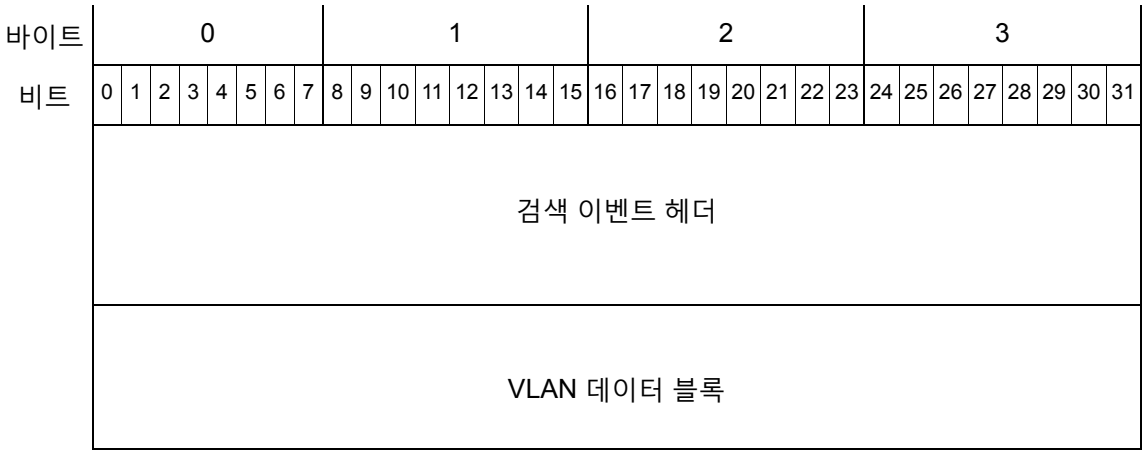
호스트가 브리지/라우터로 식별됨 메시지

호스트가 브리지/라우터로 식별됨 이벤트 메시지에는 검색 이벤트 헤더(5.2 이상), 4-40페이지에 설명되어 있는 표준 검색 이벤트 헤더와 호스트 유형과 일치하는 값의 4바이트 필드가 차례로 포함되어 있습니다.

- 0 - 호스트
- 1 - 라우터
- 2 - 브리지

VLAN 태그 정보 업데이트 메시지

VLAN 태그 정보 업데이트 이벤트에는 검색 이벤트 헤더(5.2 이상), 4-40페이지에 설명되어 있는 표준 검색 이벤트 헤더와 VLAN 데이터 블록, 4-78페이지에 설명되어 있는 VLAN 데이터 블록이 차례로 포함되어 있습니다. 계열 1 블록 그룹에서 VLAN 데이터 블록의 블록 유형은 14입니다.



NetBIOS 이름 변경 메시지

NetBIOS 이름 변경 이벤트 메시지는 검색 이벤트 헤더(5.2 이상), 4-40페이지에 설명되어 있는 표준 검색 이벤트 헤더와 문자열 정보 데이터 블록, 4-80페이지에 설명되어 있는 문자열 정보 데이터 블록이 차례로 포함되어 있습니다. 문자열 정보 데이터 블록은 계열 1의 블록 유형 35입니다.

참고 Firepower System에서는 현재 NetBIOS 도메인 변경 이벤트가 생성되지 않습니다.

배너 업데이트 메시지

배너 업데이트 이벤트 메시지에는 검색 이벤트 헤더(5.2 이상), 4-40페이지에 설명되어 있는 표준 검색 이벤트 헤더와 서버 배너 데이터 블록, 4-79페이지에 설명되어 있는 서버 배너 데이터 블록이 차례로 포함되어 있습니다. 서버 배너 데이터 블록은 계열 1의 블록 유형 37입니다.

정책 제어 메시지

정책 제어 메시지 이벤트에는 검색 이벤트 헤더(5.2 이상), 4-40페이지에 설명되어 있는 표준 검색 이벤트 헤더와 정책 제어 메시지 데이터 블록이 차례로 포함되어 있습니다. 정책 제어 메시지 데이터 블록의 형식은 시스템 버전에 따라 달라집니다. 현재 버전용 정책 제어 메시지 데이터 블록 형식에 대한 자세한 정보는 정책 엔진 제어 메시지 데이터 블록, 4-88페이지의 내용을 참조하십시오.

연결 통계 데이터 메시지

연결 통계 이벤트에는 검색 이벤트 헤더(5.2 이상), 4-40페이지에 설명되어 있는 표준 검색 이벤트 헤더와 연결 통계 데이터 블록이 차례로 포함되어 있습니다. 각 연결 통계 데이터 블록 버전의 문서에 해당 블록을 사용하는 시스템 버전이 포함되어 있습니다. 6.1 이상 버전용 연결 통계 데이터 블록 형식에 대한 자세한 정보는 6.2 이상 버전용 연결 통계 데이터 블록, 4-120페이지의 내용을 참조하십시오.

참고 연결 통계 데이터 블록은 메시지를 생성한 시스템 버전에 따라 달라집니다. 레거시 버전에 대한 자세한 내용은 레거시 데이터 구조 이해, B-1페이지에서 연결 통계 데이터 블록을 참조하십시오.

연결 청크 메시지

연결 청크 이벤트에는 검색 이벤트 헤더(5.2 이상), 4-40페이지에 설명되어 있는 표준 검색 이벤트 헤더와 연결 청크 데이터 블록이 차례로 포함됩니다. 형식은 시스템 버전에 따라 다릅니다. 현재 버전용 연결 청크 데이터 블록 형식에 대한 자세한 정보는 6.1 이상 버전용 연결 청크 데이터 블록, 4-102페이지의 내용을 참조하십시오. 연결 청크 데이터 블록은 계열 1의 블록 유형 136입니다.

4.6.1 이상 버전용 취약점 사용자 설정 메시지

유효한 취약점 사용자 설정, 유효하지 않은 취약점 사용자 설정 및 취약점 자격 사용자 설정 메시지는 표준 검색 이벤트 헤더(검색 이벤트 헤더(5.2 이상), 4-40페이지 참조)와 사용자 취약점 변경 데이터 블록(4.7 이상 버전용 사용자 취약점 변경 데이터 블록, 4-108페이지 참조, 계열 1의 블록 유형 80)을 차례로 포함하는 동일한 데이터 형식을 사용합니다. 레코드 유형, 이벤트 유형 및 이벤트 하위 유형으로 각 메시지를 구별할 수 있습니다.

사용자가 호스트 추가 및 삭제 메시지

다음 호스트 입력 이벤트 메시지에는 표준 검색 이벤트 헤더(검색 이벤트 헤더(5.2 이상), 4-40페이지 참조)와 사용자 호스트 데이터 블록(4.7 이상 버전용 사용자 호스트 데이터 블록, 4-107페이지 참조, 계열 1의 블록 유형 78)이 차례로 포함되어 있습니다.

- 주소 사용자 삭제
- 사용자가 호스트 추가

서버 사용자 삭제 메시지

서버 사용자 삭제 메시지에는 표준 검색 이벤트 헤더(검색 이벤트 헤더(5.2 이상), 4-40페이지 참조)와 사용자 서버 목록 데이터 블록(사용자 서버 목록 데이터 블록, 4-105페이지 참조)이 차례로 포함되어 있습니다. 사용자 서버 목록 데이터 블록은 계열 1의 블록 유형 77입니다.

호스트 임계성 사용자 설정 메시지

호스트 임계성 사용자 설정 메시지에는 표준 검색 이벤트 헤더(검색 이벤트 헤더(5.2 이상), 4-40페이지 참조)와 사용자 임계성 변경 데이터 블록(4.7 이상 버전용 사용자 임계성 변경 데이터 블록, 4-110페이지 참조)이 차례로 포함되어 있습니다. 사용자 임계성 변경 데이터 블록은 계열 1의 블록 유형 81입니다.

속성 메시지

다음 이벤트 메시지에는 검색 이벤트 헤더(5.2 이상), 4-40페이지에 설명되어 있는 표준 검색 이벤트 헤더와 4.7 이상 버전용 속성 정의 데이터 블록, 4-89페이지에 설명되어 있는 속성 정의 데이터 블록(계열 1의 블록 유형 55)이 차례로 포함되어 있습니다.

- 호스트 속성 추가
- 호스트 속성 업데이트
- 호스트 속성 삭제

이러한 각 이벤트는 다음 형식을 사용합니다.

속성값 메시지

다음 이벤트 메시지에는 검색 이벤트 헤더(5.2 이상), 4-40페이지에 설명되어 있는 표준 검색 이벤트 헤더와 4.7 이상 버전용 사용자 속성값 데이터 블록, 4-111페이지에 설명되어 있는 사용자 속성값 데이터 블록(계열 1의 블록 유형 82)이 차례로 포함되어 있습니다.

- 호스트 속성값 설정
- 호스트 속성값 삭제

이러한 각 이벤트는 다음 형식을 사용합니다.

사용자 서버 및 운영 체제 메시지

다음 이벤트 메시지에는 검색 이벤트 헤더(5.2 이상), 4-40페이지에 설명되어 있는 표준 검색 이벤트 헤더와 5.1 이상 버전용 사용자 제품 데이터 블록, 4-171페이지에 설명되어 있는 사용자 제품 데이터 블록(계열 1의 블록 유형 60)이 차례로 포함되어 있습니다.

- 운영 체제 정의 설정
- 서버 정의 설정
- 서버 추가

이러한 각 이벤트는 다음 형식을 사용합니다.

사용자 프로토콜 메시지

다음 이벤트 메시지에는 검색 이벤트 헤더(5.2 이상), 4-40페이지에 설명되어 있는 표준 검색 이벤트 헤더와 4.7 이상 버전용 사용자 프로토콜 목록 데이터 블록, 4-113페이지에 설명되어 있는 사용자 프로토콜 목록 데이터 블록(계열 1의 블록 유형 83)이 차례로 포함되어 있습니다.

- 프로토콜 삭제
- 프로토콜 추가

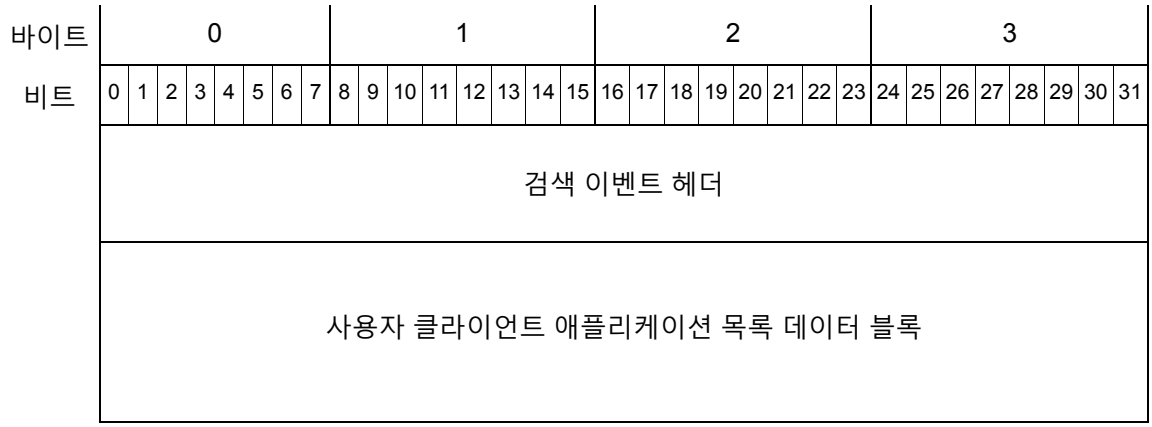
이러한 각 이벤트는 다음 형식을 사용합니다.

사용자 클라이언트 애플리케이션 메시지

다음 이벤트 메시지에는 검색 이벤트 헤더(5.2 이상), 4-40페이지에 설명되어 있는 표준 검색 이벤트 헤더와 사용자 클라이언트 애플리케이션 목록 데이터 블록, 4-95페이지에 설명되어 있는 사용자 클라이언트 애플리케이션 목록 데이터 블록(계열 1의 블록 유형 60)이 차례로 포함되어 있습니다.

- 클라이언트 애플리케이션 삭제
- 클라이언트 애플리케이션 추가

이러한 각 이벤트는 다음 형식을 사용합니다.



스캔 결과 추가 메시지

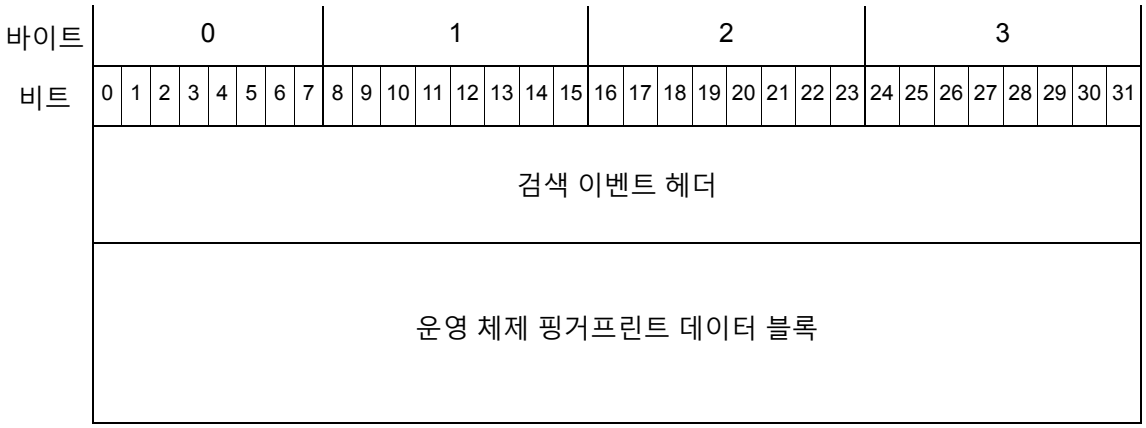
스캔 결과 추가 이벤트 메시지에는 검색 이벤트 헤더(5.2 이상), 4-40페이지에 설명되어 있는 표준 검색 이벤트 헤더와 5.2 이상 버전용 스캔 결과 데이터 블록, 4-136페이지에 설명되어 있는 스캔 결과 데이터 블록이 차례로 포함되어 있습니다. 검색 결과 데이터 블록은 계열 1의 블록 유형 142입니다.

이 이벤트는 다음과 같은 형식을 사용합니다.

새 운영 체제 메시지

새 OS 이벤트 메시지에는 검색 이벤트 헤더(5.2 이상), 4-40페이지에 설명되어 있는 표준 검색 이벤트 헤더와 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 4-161페이지에 설명되어 있는 운영 체제 핑거프린트 데이터 블록이 차례로 포함되어 있습니다.

이 이벤트는 다음과 같은 형식을 사용합니다.



ID 충돌 및 ID 시간 초과 시스템 메시지

ID 충돌 및 ID 시간 초과 이벤트 메시지에는 각각 검색 이벤트 헤더(5.2 이상), 4-40페이지에 설명되어 있는 표준 검색 이벤트 헤더와 ID 데이터 블록, 4-115페이지에 설명되어 있는 ID 데이터 블록이 차례로 포함되어 있습니다. ID 데이터 블록은 계열 1의 블록 유형 94입니다. 핑거프린트 소스 ID에서 충돌이나 시간 초과가 발생하면 이러한 메시지가 생성됩니다.

이 이벤트는 다음과 같은 형식을 사용합니다.

호스트 IOC 설정 메시지

호스트 IOC 설정 이벤트 메시지에는 검색 이벤트 헤더(5.2 이상), 4-40페이지에 설명되어 있는 표준 검색 이벤트 헤더와 정수(INT32) 데이터 블록, 4-78페이지에 설명되어 있는 정수 데이터 블록이 차례로 포함되어 있습니다. 이 정수 데이터 블록에는 호스트에 대한 IOC 설정의 ID 번호가 포함됩니다.

이 이벤트는 다음과 같은 형식을 사용합니다.

이벤트 유형별 사용자 데이터 구조

eStreamer에서는 검색 이벤트 헤더에 나와 있는 이벤트 유형에 따라 사용자 이벤트 메시지를 작성합니다. 다음 하위 섹션에서는 각 이벤트 형식에 대해 대략적으로 설명합니다.

- 사용자 수정 메시지, 4-62페이지
- 사용자 정보 업데이트 메시지 블록, 4-62페이지

사용자 수정 메시지

시스템 탐색을 통해 다음 이벤트가 발생하면 사용자 수정 메시지가 전송됩니다.

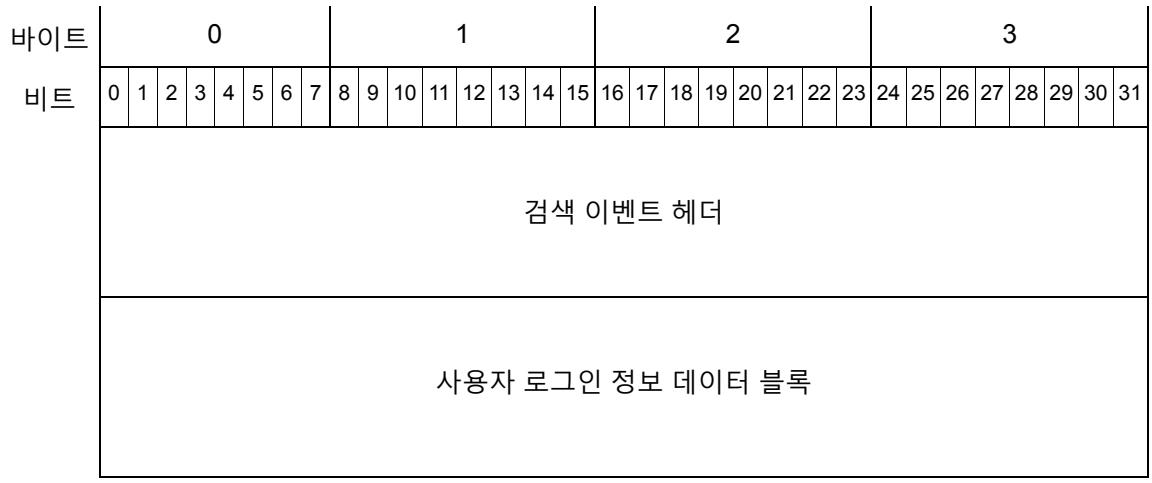
- 새 사용자가 탐지되는 경우(새 사용자 ID 이벤트 - 이벤트 유형 1004, 하위 유형 1)
- 사용자가 제거되는 경우(사용자 ID 삭제 이벤트 - 이벤트 유형 1004, 하위 유형 3)
- 사용자가 삭제되는 경우(사용자 ID 삭제됨: 사용자 한도 도달 이벤트 - 이벤트 유형 1004, 하위 유형 4)

사용자 수정 이벤트에는 검색 이벤트 헤더(5.2 이상), 4-40페이지에 설명되어 있는 표준 검색 이벤트 헤더와 6.0 이상 버전용 사용자 정보 데이터 블록, 4-189페이지에 설명되어 있는 사용자 정보 데이터 블록이 포함됩니다. 사용자 정보 데이터 블록은 계열 1의 블록 유형 120입니다.

사용자 정보 업데이트 메시지 블록

시스템에서 사용자의 로그인 변경(사용자 로그인 이벤트 - 이벤트 유형 1004, 하위 유형 2)을 탐지하면 사용자 정보 업데이트 메시지가 전송됩니다.

사용자 정보 업데이트 이벤트에는 검색 이벤트 헤더(5.2 이상), 4-40페이지에 설명되어 있는 표준 검색 이벤트 헤더와 6.2 이상 버전용 사용자 로그인 정보 데이터 블록, 4-195페이지에 설명되어 있는 사용자 로그인 정보 데이터 블록이 포함됩니다. 사용자 로그인 정보 데이터 블록은 계열 1의 블록 유형 121입니다.



검색(계열 1) 블록 이해

대다수 검색 및 연결 이벤트에는 계열 1 데이터 구조 그룹의 데이터 블록이 하나 이상 통합되어 있습니다. 각 계열 1 데이터 블록 유형은 특정 유형의 정보를 전달합니다. 블록 유형 번호는 블록의 데이터 앞에 있는 데이터 블록 헤더에 표시됩니다. 블록 헤더 형식에 대한 자세한 정보는 데이터 블록 헤더, 2-25페이지의 내용을 참조하십시오.

계열 1 데이터 블록 헤더

계열 1 데이터 블록 헤더에는 계열 2 블록 헤더와 마찬가지로 블록 유형 번호 및 블록 길이를 포함하는 32비트 정수 필드 2개가 있습니다.

참고 데이터 블록 길이 필드에는 전체 데이터 블록의 바이트 수가 포함됩니다. 여기에는 2개 데이터 블록 헤더 필드의 8바이트가 포함됩니다.

일부 블록 계열 1 유형의 경우에는 블록 헤더 바로 뒤에 원시 데이터가 옵니다. 더 복잡한 블록 유형에서는 헤더 뒤에 표준 고정 길이 필드가 올 수도 있고, 다른 계열 1 데이터 블록 또는 블록 목록을 캡슐화하는 계열 1 기본 형식 블록의 헤더가 올 수도 있습니다.

계열 1 기본 형식 데이터 블록

계열 1 및 계열 2 블록에는 모두 메시지 내의 가변 길이 문자열/BLOB 및 가변 길이 블록 목록을 캡슐화하는 기본 형식 집합이 포함되어 있습니다. 이러한 기본 형식 블록에는 위에서 설명한 표준 계열 1 블록 헤더가 있습니다. 이러한 기본 형식은 다른 계열 1 데이터 블록에만 표시됩니다. 지정된 블록 유형에는 어떤 숫자든 포함할 수 있습니다. 기본 형식 블록의 구조에 대한 자세한 내용은 다음 항목을 참조하십시오.

- 문자열 데이터 블록, 4-72페이지
- BLOB 데이터 블록, 4-73페이지
- 목록 데이터 블록, 4-74페이지
- 일반 블록 목록, 4-75페이지

호스트 검색 및 연결 데이터 블록

호스트 검색 및 연결 이벤트의 블록 유형 목록은 표 4-30, 4-64페이지의 내용을 참조하십시오. 사용자 이벤트의 블록 유형에 대한 설명은 표 4-85, 4-179페이지에 나와 있습니다. 이러한 블록은 모두 계열 1 데이터 블록입니다.

아래 표의 각 항목에는 데이터 블록이 정의되어 있는 하위 섹션의 링크가 포함되어 있습니다. 각 블록 유형에는 상태(현재 또는 레거시)가 표시되어 있습니다. 현재 데이터 블록은 최신 버전입니다. 레거시 데이터 블록은 이전 버전 제품에서 사용되며, eStreamer에서 해당 메시지 유형을 계속 요청할 수 있습니다.

표 4-30 호스트 검색 및 연결 데이터 블록 유형

유형	콘텐츠	데이터 블록 상태	설명
0	문자열	현재	문자열 데이터를 포함합니다. 자세한 정보는 문자열 데이터 블록, 4-72페이지의 내용을 참조하십시오.
1	하위 서버	현재	서버에서 탐지된 하위 서버에 대한 정보를 포함합니다. 자세한 정보는 하위 서버 데이터 블록, 4-75페이지의 내용을 참조하십시오.
4	프로토콜	현재	프로토콜 데이터를 포함합니다. 자세한 정보는 프로토콜 데이터 블록, 4-77페이지의 내용을 참조하십시오.
7	정수 데이터	현재	정수(숫자) 데이터를 포함합니다. 자세한 정보는 정수(INT32) 데이터 블록, 4-78페이지의 내용을 참조하십시오.
10	BLOB	현재	이진 데이터의 원시 블록을 포함하며 배너 전용으로 사용됩니다. 자세한 정보는 BLOB 데이터 블록, 4-73페이지의 내용을 참조하십시오.
11	목록	현재	다른 데이터 블록의 목록을 포함합니다. 자세한 정보는 목록 데이터 블록, 4-74페이지의 내용을 참조하십시오.
14	VLAN	현재	VLAN 정보를 포함합니다. 자세한 정보는 VLAN 데이터 블록, 4-78페이지의 내용을 참조하십시오.

표 4-30 호스트 검색 및 연결 데이터 블록 유형 (계속)

유형	콘텐츠	데이터 블록 상태	설명
20	침입 영향 알림	현재	침입 영향 알림 정보를 포함합니다. 침입 영향 알림 이벤트의 헤더는 다른 데이터 블록과 약간 다릅니다. 자세한 정보는 5.3 이상 버전용 침입 영향 알림 데이터, 3-17페이지의 내용을 참조하십시오.
31	일반 목록	현재	호스트 프로파일 블록에서 클라이언트 애플리케이션 블록 등의 블록 목록을 캡슐화하기 위한 일반 목록 정보를 포함합니다. 자세한 정보는 일반 블록 목록, 4-75페이지의 내용을 참조하십시오.
35	문자열 정보	현재	문자열 정보를 포함합니다. 예를 들어 취약점 스캔 데이터 블록에서 사용되는 경우 문자열 정보 데이터 블록은 CVE ID 번호 데이터를 포함합니다. 문자열 정보 데이터 블록, 4-80페이지의 내용을 참조하십시오.
37	서버 배너	현재	서버 배너 데이터를 포함합니다. 자세한 정보는 서버 배너 데이터 블록, 4-79페이지의 내용을 참조하십시오.
38	속성 주소	레거시	이전 버전 제품에 설명되어 있는 호스트 속성 주소를 포함합니다. 후속 버전 블록은 146입니다.
39	속성 목록 항목	현재	호스트 속성 목록 항목 값을 포함합니다. 자세한 정보는 속성 목록 항목 데이터 블록, 4-82페이지의 내용을 참조하십시오.
42	호스트 클라이언트 애플리케이션	레거시	이전 버전 제품에 설명되어 있는 새 클라이언트 애플리케이션 이벤트에 대한 클라이언트 애플리케이션 정보를 포함합니다.
47	전체 호스트 프로파일	레거시	이전 버전 제품에 설명되어 있는 전체 호스트 프로파일 정보를 포함합니다.
48	속성값	현재	호스트 속성의 속성 ID 번호와 값을 포함합니다. 자세한 정보는 속성값 데이터 블록, 4-83페이지의 내용을 참조하십시오.
51	전체 하위 서버	현재	서버에서 탐지된 하위 서버에 대한 정보를 포함합니다. 전체 서버 정보 블록 및 전체 호스트 프로파일에서 참조됩니다. 각 하위 서버의 취약점 정보를 포함합니다. 자세한 정보는 전체 하위 서버 데이터 블록, 4-84페이지의 내용을 참조하십시오.
53	운영 체제	현재	버전 3.5 이상의 운영 체제 정보를 포함합니다. 자세한 정보는 3.5 이상 버전용 운영 체제 데이터 블록, 4-87페이지의 내용을 참조하십시오.
54	정책 엔진 제어 메시지	현재	사용자 정책 제어 변경 사항에 대한 정보를 포함합니다. 자세한 정보는 정책 엔진 제어 메시지 데이터 블록, 4-88페이지의 내용을 참조하십시오.
55	속성 정의	현재	속성 정의에 대한 정보를 포함합니다. 자세한 정보는 4.7 이상 버전용 속성 정의 데이터 블록, 4-89페이지의 내용을 참조하십시오.
56	연결 통계	레거시	이전 버전 제품에 설명되어 있는 4.7~4.9.0 버전의 연결 통계 이벤트에 대한 정보를 포함합니다.

표 4-30 호스트 검색 및 연결 데이터 블록 유형 (계속)

유형	콘텐츠	데이터 블록 상태	설명
57	사용자 프로토콜	현재	사용자 입력의 프로토콜 정보를 포함합니다. 자세한 정보는 사용자 프로토콜 데이터 블록, 4-92페이지의 내용을 참조하십시오.
59	사용자 클라이언트 애플리케이션	레거시	사용자 입력의 클라이언트 애플리케이션 데이터를 포함합니다. 자세한 정보는 5.0~5.1 버전용 사용자 클라이언트 애플리케이션 데이터 블록, B-93페이지의 내용을 참조하십시오. 블록 138로 대체됩니다.
60	사용자 클라이언트 애플리케이션 목록	현재	사용자 클라이언트 애플리케이션 데이터 블록 목록을 포함합니다. 자세한 정보는 사용자 클라이언트 애플리케이션 목록 데이터 블록, 4-95페이지의 내용을 참조하십시오.
61	IP 범위 사양	레거시	IP 주소 범위 사양을 포함합니다. 자세한 정보는 5.0~5.1.1.x 버전용 IP 범위 사양 데이터 블록, B-310페이지의 내용을 참조하십시오. 블록 141로 대체됩니다.
62	속성 사양	현재	속성 이름 및 값을 포함합니다. 자세한 정보는 속성 사양 데이터 블록, 4-98페이지의 내용을 참조하십시오.
63	MAC 주소 사양	현재	MAC 주소 범위 사양을 포함합니다. 자세한 정보는 MAC 주소 사양 데이터 블록, 4-99페이지의 내용을 참조하십시오.
64	IP 주소 사양	현재	IP 및 MAC 주소 사양 블록의 목록이 포함되어 있습니다. 자세한 정보는 주소 사양 데이터 블록, 4-100페이지의 내용을 참조하십시오.
65	사용자 제품	레거시	서드파티 애플리케이션에서 가져온 호스트 입력 데이터(서드파티 애플리케이션 문자열 매핑 포함)를 포함합니다. 자세한 정보는 5.0.x 버전용 사용자 제품 데이터 블록, B-97페이지의 내용을 참조하십시오. 5.0용으로 도입된 후속 버전 블록 유형 118의 구조는 블록 유형 65와 동일합니다.
66	연결 청크	레거시	연결 청크 정보를 포함합니다. 자세한 정보는 5.0~5.1 버전용 연결 청크 데이터 블록, B-145페이지의 내용을 참조하십시오. 5.0용으로 도입된 후속 버전 블록 유형 119의 구조는 블록 유형 66과 동일합니다.
67	수정 사항 목록	현재	호스트에 적용된 수정 사항을 포함합니다. 자세한 정보는 수정 목록 데이터 블록, 4-103페이지의 내용을 참조하십시오.
71	일반 스캔 결과	레거시	이전 버전 제품에 설명되어 있는 네트워크 맵 스캔의 결과를 포함합니다.
72	스캔 결과	레거시	이전 버전 제품에 설명되어 있는 서드파티 스캔의 결과를 포함합니다.

표 4-30 호스트 검색 및 연결 데이터 블록 유형 (계속)

유형	콘텐츠	데이터 블록 상태	설명
76	사용자 서버	현재	사용자 입력 이벤트의 서버 정보를 포함합니다. 자세한 정보는 사용자 서버 데이터 블록, 4-104페이지의 내용을 참조하십시오.
77	사용자 서버 목록	현재	사용자 서버 블록의 목록을 포함합니다. 자세한 정보는 사용자 서버 목록 데이터 블록, 4-105페이지의 내용을 참조하십시오.
78	사용자 호스트	현재	사용자 호스트 입력 이벤트의 호스트 범위에 대한 정보를 포함합니다. 자세한 정보는 4.7 이상 버전용 사용자 호스트 데이터 블록, 4-107페이지의 내용을 참조하십시오.
79	사용자 취약점	레거시	이전 버전 제품에 설명되어 있는 호스트 하나 이상의 취약점에 대한 정보를 포함합니다. 버전 5.0용으로 도입된 후속 버전 블록의 블록 유형은 124입니다.
80	사용자 호스트 취약점 변경	현재	비활성화 또는 활성화된 취약점 목록을 포함합니다. 자세한 정보는 4.7 이상 버전용 사용자 취약점 변경 데이터 블록, 4-108페이지의 내용을 참조하십시오.
81	사용자 임계성	현재	호스트 하나 이상의 임계성 변경 사항에 대한 정보를 포함합니다. 자세한 정보는 4.7 이상 버전용 사용자 임계성 변경 데이터 블록, 4-110페이지의 내용을 참조하십시오.
82	사용자 속성값	현재	호스트 하나 이상의 속성값 변경 사항을 포함합니다. 자세한 정보는 4.7 이상 버전용 사용자 속성값 데이터 블록, 4-111페이지의 내용을 참조하십시오.
83	사용자 프로토콜 목록	현재	호스트 하나 이상의 프로토콜 목록을 포함합니다. 자세한 정보는 4.7 이상 버전용 사용자 프로토콜 목록 데이터 블록, 4-113페이지의 내용을 참조하십시오.
85	취약점 목록	현재	호스트에 적용되는 취약점을 포함합니다. 자세한 정보는 4.9.0 이상 버전용 호스트 취약점 데이터 블록, 4-114페이지의 내용을 참조하십시오.
86	취약점 스캔	레거시	이전 버전 제품에 설명되어 있는 스캔을 통해 탐지된 취약점에 대한 정보를 포함합니다.
87	운영 체제 핑거프린트	레거시	운영 체제 핑거프린트 목록을 포함합니다. 자세한 정보는 5.0~5.0.2 버전용 운영 체제 핑거프린트 데이터 블록, B-127페이지의 내용을 참조하십시오. 버전 5.1용으로 도입된 후속 버전 블록의 블록 유형은 130입니다.
88	서버 정보	레거시	이전 버전 제품에 설명되어 있는 서버 핑거프린트에 사용되는 서버 정보를 포함합니다.
89	호스트 서버	레거시	이전 버전 제품에 설명되어 있는 호스트에 대한 서버 정보를 포함합니다.

표 4-30 호스트 검색 및 연결 데이터 블록 유형 (계속)

유형	콘텐츠	데이터 블록 상태	설명
90	전체 호스트 서버	레거시	이전 버전 제품에 설명되어 있는 호스트에 대한 서버 정보를 포함합니다.
91	호스트 프로파일	레거시	호스트에 대한 프로파일 정보를 포함합니다. 자세한 정보는 5.2 이상 버전용 호스트 프로파일 데이터 블록, 4-164페이지의 내용을 참조하십시오. 버전 5.1용으로 도입된 후속 버전 블록의 블록 유형은 132입니다.
92	전체 호스트 프로파일	레거시	이전 버전 제품에 설명되어 있는 전체 호스트 프로파일 정보를 포함합니다. 데이터 블록 47을 대체합니다.
94	ID 데이터	현재	호스트의 ID 데이터를 포함합니다. 자세한 정보는 ID 데이터 블록, 4-115페이지의 내용을 참조하십시오.
95	호스트 MAC 주소	현재	호스트의 MAC 주소 정보를 포함합니다. 자세한 정보는 4.9 이상 버전용 호스트 MAC 주소, 4-117페이지의 내용을 참조하십시오.
96	보조 호스트 업데이트	현재	보조 보조 호스트 업데이트, 4-118페이지에서 보고하는 MAC 주소 정보의 목록을 포함합니다.
97	웹 애플리케이션	레거시	이전 버전 제품에 설명되어 있는 웹 애플리케이션 데이터 목록을 포함합니다. 버전 5.0용으로 도입된 후속 버전 블록의 블록 유형은 123입니다.
98	호스트 서버	레거시	이전 버전 제품에 설명되어 있는 호스트에 대한 서버 정보를 포함합니다.
99	전체 호스트 서버	레거시	이전 버전 제품에 설명되어 있는 호스트에 대한 서버 정보를 포함합니다.
100	호스트 클라이언트 애플리케이션	레거시	이전 버전 제품에 설명되어 있는 새 클라이언트 애플리케이션 이벤트에 대한 클라이언트 애플리케이션 정보를 포함합니다. 버전 5.0용으로 도입된 후속 버전 블록 유형 122의 구조는 블록 유형 100과 동일합니다.
101	연결 통계	레거시	이전 버전 제품에 설명되어 있는 4.9.1 이상 버전의 연결 통계 이벤트에 대한 정보를 포함합니다.
102	스캔 결과	레거시	취약점에 대한 정보를 포함하며 스캔 결과 추가 이벤트 내에서 사용됩니다. 5.0~5.1.1.x 버전용 스캔 결과 데이터 블록, B-95페이지의 내용을 참조하십시오.
103	호스트 서버	현재	호스트에 대한 서버 정보를 포함합니다. 자세한 정보는 4.10.0 이상 버전용 호스트 서버 데이터 블록, 4-138페이지의 내용을 참조하십시오.
104	전체 호스트 서버	현재	호스트에 대한 서버 정보를 포함합니다. 자세한 정보는 4.10.0 이상 버전용 전체 호스트 서버 데이터 블록, 4-140페이지의 내용을 참조하십시오.

표 4-30 호스트 검색 및 연결 데이터 블록 유형 (계속)

유형	콘텐츠	데이터 블록 상태	설명
105	서버 정보	레거시	서버 핑거프린트에 사용되는 서버 정보를 포함합니다. 자세한 정보는 4.10.x, 5.0~5.0.2 버전용 서버 정보 데이터 블록, 4-144페이지의 내용을 참조하십시오. 5.0용으로 도입된 후속 버전 블록 유형 117의 구조는 블록 유형 105와 동일합니다.
106	전체 서버 정보	현재	호스트에서 탐지된 서버에 대한 정보를 포함합니다. 자세한 정보는 전체 서버 정보 데이터 블록, 4-147페이지의 내용을 참조하십시오.
108	일반 스캔 결과	현재	네트워크 맵 스캔의 결과를 포함합니다. 자세한 정보는 4.10.0 이상 버전용 일반 스캔 결과 데이터 블록, 4-149페이지의 내용을 참조하십시오.
109	취약점 스캔	현재	서드파티 스캔에서 탐지된 취약점에 대한 정보를 포함합니다. 4.10.0 이상 버전용 취약점 스캔 데이터 블록, 4-151페이지의 내용을 참조하십시오.
111	전체 호스트 프로파일	레거시	전체 호스트 프로파일 정보를 포함합니다. 자세한 정보는 5.0~5.0.2 버전용 전체 호스트 프로파일 데이터 블록, B-274페이지의 내용을 참조하십시오. 데이터 블록 92를 대체합니다.
112	전체 호스트 클라이언트 애플리케이션	현재	새 클라이언트 애플리케이션 이벤트에 대한 클라이언트 애플리케이션 정보를 포함하며, 취약점 목록이 들어 있습니다. 자세한 정보는 5.0 이상 버전용 전체 호스트 클라이언트 애플리케이션 데이터 블록, 4-154페이지의 내용을 참조하십시오.
115	연결 통계	레거시	5.0~5.0.2 버전의 연결 통계 이벤트에 대한 정보를 포함합니다. 자세한 정보는 5.0~5.0.2 버전용 연결 통계 데이터 블록, B-128페이지의 내용을 참조하십시오. 버전 5.1용으로 도입된 후속 버전 블록의 블록 유형은 126입니다.
117	서버 정보	현재	서버 핑거프린트에 사용되는 서버 정보를 포함합니다. 자세한 정보는 4.10.x, 5.0~5.0.2 버전용 서버 정보 데이터 블록, 4-144페이지의 내용을 참조하십시오.
118	사용자 제품	레거시	서드파티 애플리케이션에서 가져온 호스트 입력 데이터(서드파티 애플리케이션 문자열 매핑 포함)를 포함합니다. 자세한 정보는 5.0.x 버전용 사용자 제품 데이터 블록, B-97페이지의 내용을 참조하십시오. 5.0에서 대체된 이전 버전 블록 유형 65의 구조는 이 블록 유형과 같습니다. 버전 5.1용으로 도입된 후속 버전 블록의 블록 유형은 132입니다.
119	연결 청크	레거시	버전 4.10.1~5.1의 연결 청크 정보를 포함합니다. 자세한 정보는 5.0~5.1 버전용 연결 청크 데이터 블록, B-145페이지의 내용을 참조하십시오. 후속 버전 블록은 136입니다.

표 4-30 호스트 검색 및 연결 데이터 블록 유형 (계속)

유형	콘텐츠	데이터 블록 상태	설명
122	호스트 클라이언트 애플리케이션	현재	5.0 이상 버전의 새 클라이언트 애플리케이션 이벤트에 대한 클라이언트 애플리케이션 정보를 포함합니다. 자세한 정보는 5.0 이상 버전용 호스트 클라이언트 애플리케이션 데이터 블록, 4-156페이지의 내용을 참조하십시오. 이는 블록 유형 100을 대체합니다.
123	웹 애플리케이션	현재	5.0 이상 버전의 웹 애플리케이션 데이터를 포함합니다. 자세한 정보는 5.0 이상 버전용 웹 애플리케이션 데이터 블록, 4-119페이지의 내용을 참조하십시오. 이는 블록 유형 97을 대체합니다.
124	사용자 취약점	현재	호스트 하나 이상의 취약점에 대한 정보를 포함합니다. 5.0 이상 버전용 사용자 취약점 데이터 블록, 4-158페이지의 내용을 참조하십시오. 이는 블록 유형 79를 대체합니다.
125	연결 통계	레거시	이전 버전 제품에 설명되어 있는 4.10.2 이상 버전의 연결 통계 이벤트에 대한 정보를 포함합니다. 버전 5.1용으로 도입된 후속 버전 블록의 블록 유형은 115입니다.
126	연결 통계	레거시	5.1 버전의 연결 통계 이벤트에 대한 정보를 포함합니다. 자세한 정보는 5.1 버전용 연결 통계 데이터 블록, B-133페이지의 내용을 참조하십시오. 이는 블록 유형 115를 대체합니다. 이 블록 유형은 블록 유형 137로 대체됩니다.
130	운영 체제 핑거프린트	현재	운영 체제 핑거프린트 목록을 포함합니다. 자세한 정보는 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 4-161페이지의 내용을 참조하십시오. 이는 블록 유형 87을 대체합니다.
131	모바일 디바이스 정보	현재	탐지된 모바일 디바이스 하드웨어에 대한 정보를 포함합니다. 자세한 정보는 5.1 이상 버전용 모바일 디바이스 정보 데이터 블록, 4-163페이지의 내용을 참조하십시오.
132	호스트 프로파일	레거시	호스트에 대한 프로파일 정보를 포함합니다. 자세한 정보는 5.2.x 버전용 전체 호스트 프로파일 데이터 블록, B-292페이지의 내용을 참조하십시오. 이는 블록 유형 91을 대체합니다. 블록 139로 대체됩니다.
134	사용자 제품	현재	서드파티 애플리케이션에서 가져온 호스트 입력 데이터(서드파티 애플리케이션 문자열 매핑 포함)를 포함합니다. 자세한 정보는 5.1 이상 버전용 사용자 제품 데이터 블록, 4-171페이지의 내용을 참조하십시오. 이전 버전 블록 유형 118을 대체합니다.
135	전체 호스트 프로파일	레거시	전체 호스트 프로파일 정보를 포함합니다. 자세한 정보는 5.1.1 버전용 전체 호스트 프로파일 데이터 블록, B-283페이지의 내용을 참조하십시오. 데이터 블록 111을 대체합니다.

표 4-30 호스트 검색 및 연결 데이터 블록 유형 (계속)

유형	콘텐츠	데이터 블록 상태	설명
136	연결 청크	현재	연결 청크 정보를 포함합니다. 자세한 정보는 6.1 이상 버전용 연결 청크 데이터 블록, 4-102페이지의 내용을 참조하십시오. 블록 119를 대체합니다.
137	연결 통계	레거시	5.1.1 버전의 연결 이벤트에 대한 정보를 포함합니다. 자세한 정보는 5.0~5.1 버전용 연결 청크 데이터 블록, B-145페이지의 내용을 참조하십시오. 이는 블록 유형 126을 대체합니다. 이는 블록 유형 144로 대체됩니다.
138	사용자 클라이언트 애플리케이션	현재	사용자 입력의 클라이언트 애플리케이션 데이터를 포함합니다. 자세한 정보는 5.1.1 이상 버전용 사용자 클라이언트 애플리케이션 데이터 블록, 4-93페이지의 내용을 참조하십시오. 이는 블록 유형 59를 대체합니다.
139	호스트 프로파일	현재	호스트에 대한 프로파일 정보를 포함합니다. 자세한 정보는 5.2 이상 버전용 호스트 프로파일 데이터 블록, 4-164페이지의 내용을 참조하십시오. 이는 블록 유형 132를 대체합니다.
140	전체 호스트 프로파일	레거시	전체 호스트 프로파일 정보를 포함합니다. 자세한 정보는 5.3 이상 버전용 전체 호스트 프로파일 데이터 블록, 5-1페이지의 내용을 참조하십시오. 데이터 블록 135를 대체합니다.
141	IP 범위 사양	현재	IP 주소 범위 사양을 포함합니다. 자세한 정보는 5.2 이상 버전용 IP 주소 범위 데이터 블록, 4-96페이지의 내용을 참조하십시오. 이는 블록 61을 대체합니다.
142	스캔 결과	현재	취약점에 대한 정보를 포함하며 스캔 결과 추가 이벤트 내에서 사용됩니다. 5.2 이상 버전용 스캔 결과 데이터 블록, 4-136페이지의 내용을 참조하십시오. 이는 블록 102를 대체합니다.
143	호스트 IP	현재	호스트 IP 주소 및 마지막 확인 정보를 포함합니다. 자세한 정보는 호스트 IP 주소 데이터 블록, 4-99페이지의 내용을 참조하십시오.
144	연결 통계	레거시	5.2.x 버전의 연결 이벤트에 대한 정보를 포함합니다. 자세한 정보는 5.2.x 버전용 연결 통계 데이터 블록, B-139페이지의 내용을 참조하십시오. 이는 블록 유형 137을 대체합니다.
146	속성 주소	현재	5.2 이상 버전의 호스트 속성 주소를 포함합니다. 자세한 정보는 5.2 이상 버전용 속성 주소 데이터 블록, 4-81페이지의 내용을 참조하십시오. 이는 블록 유형 38을 대체합니다.
140	전체 호스트 프로파일	현재	전체 호스트 프로파일 정보를 포함합니다. 자세한 정보는 5.3 이상 버전용 전체 호스트 프로파일 데이터 블록, 5-1페이지의 내용을 참조하십시오. 데이터 블록 135를 대체합니다.

표 4-30 호스트 검색 및 연결 데이터 블록 유형 (계속)

유형	콘텐츠	데이터 블록 상태	설명
152	연결 통계	레거시	5.3 이상 버전의 연결 이벤트에 대한 정보를 포함합니다. 자세한 정보는 5.3 버전용 연결 통계 데이터 블록, B-154페이지의 내용을 참조하십시오. 이는 블록 유형 144를 대체합니다.
154	연결 통계	레거시	5.3 버전의 연결 이벤트에 대한 정보를 포함합니다. 자세한 정보는 5.3.1 버전용 연결 통계 데이터 블록, B-161페이지의 내용을 참조하십시오. 이는 블록 유형 152를 대체합니다.
155	연결 통계	레거시	5.4 버전의 연결 이벤트에 대한 정보를 포함합니다. 자세한 정보는 5.4 버전용 연결 통계 데이터 블록, B-168페이지의 내용을 참조하십시오. 이는 블록 유형 154를 대체합니다.
157	연결 통계	레거시	5.4.1 버전의 연결 이벤트에 대한 정보를 포함합니다. 자세한 정보는 5.4.1 버전용 연결 통계 데이터 블록, B-181페이지의 내용을 참조하십시오. 이는 블록 유형 155를 대체합니다.
160	연결 통계	레거시	5.4.1 버전의 연결 이벤트에 대한 정보를 포함합니다. 자세한 정보는 6.0.x 버전용 연결 통계 데이터 블록, B-194페이지의 내용을 참조하십시오. 이는 블록 유형 157을 대체합니다.
163	연결 통계	현재	6.0 이상 버전의 연결 이벤트에 대한 정보를 포함합니다. 자세한 정보는 6.2 이상 버전용 연결 통계 데이터 블록, 4-120페이지의 내용을 참조하십시오. 이는 블록 유형 160을 대체합니다.

문자열 데이터 블록

문자열 데이터 블록은 계열 1 블록의 문자열 데이터를 전송하는 데 사용됩니다. 이 블록은 대개 운영 체제 또는 서버 이름 등을 설명하기 위한 용도로 다른 계열 1 데이터 블록 내에 표시됩니다.

빈 문자열 데이터 블록(문자열 데이터가 없는 문자열 데이터 블록)은 블록 길잇값이 8이며, 뒤따라 0바이트의 문자열 데이터가 옵니다. 운영 체제 벤더를 알 수 없어 운영 체제 데이터 블록의 OS Vendor(OS 벤더) 문자열 필드에 콘텐츠가 없는 경우와 같이 문자열 값의 콘텐츠가 없으면 빈 문자열 데이터 블록이 반환됩니다.

계열 1 블록 그룹에서 문자열 데이터 블록의 블록 유형은 0입니다.

참고 이 데이터 블록에서 반환되는 문자열이 항상 null로 종료되는 것은 아닙니다. 즉, 문자열이 0으로 끝나지 않을 수도 있습니다.

다음 다이어그램에 문자열 데이터 블록의 형식이 나와 있습니다.

다음 표에는 문자열 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 4-31 문자열 데이터 블록 필드

필드	데이터 유형	설명
문자열 블록 유형	uint32	문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	문자열 데이터 블록 헤더와 문자열 데이터를 합한 길이입니다.
문자열 데이터	string	문자열 데이터를 포함하며, 문자열 끝에 종료 문자(null 바이트)를 포함할 수도 있습니다.

BLOB 데이터 블록

BLOB 데이터를 사용하여 이진 데이터를 전달할 수 있습니다. 예를 들어 이진 데이터는 시스템이 캡처한 서버 배너를 저장하는 데 사용됩니다. 계열 1 블록 그룹에서 BLOB 데이터 블록의 블록 유형은 10입니다.

다음 다이어그램에 BLOB 데이터 블록의 형식이 나와 있습니다.

다음 표에는 BLOB 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 4-32 BLOB 데이터 블록 필드

필드	데이터 유형	설명
BLOB 블록 유형	uint32	BLOB 데이터 블록을 시작합니다. 이 값은 항상 10입니다.
BLOB 블록 길이	uint32	BLOB 데이터 블록의 바이트 수입니다. 여기에는 BLOB 블록 유형 및 길이 필드의 8바이트에 그 뒤의 이진 데이터 길이를 더한 값이 포함됩니다.
이진 데이터	variable	이진 데이터(대개 서버 배너)를 포함합니다.

목록 데이터 블록

목록 데이터 블록은 계열 1 데이터 블록 목록을 캡슐화하는 데 사용됩니다. 예를 들어 TCP 서버 목록을 전송하는 경우에는 데이터가 포함된 서버 데이터 블록이 목록 데이터 블록에 캡슐화됩니다. 계열 1 블록 그룹에서 목록 데이터 블록의 블록 유형은 11입니다.

다음 다이어그램에 목록 데이터 블록의 기본 형식이 나와 있습니다.

다음 표에는 목록 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 4-33 목록 데이터 블록 필드

필드	데이터 유형	설명
목록 블록 유형	uint32	목록 데이터 블록을 시작합니다. 이 값은 항상 11입니다.
목록 블록 길이	uint32	목록 블록과 캡슐화된 데이터의 바이트 수입니다. 예를 들어 목록에 하위 서버 데이터 블록 3개가 포함되어 있으면 이 값에는 하위 서버 블록의 바이트 수에 목록 블록 헤더의 8바이트를 더한 값이 포함됩니다.
캡슐화된 데이터 블록	variable	캡슐화된 데이터 블록(목록 블록 길이의 최대 바이트 수까지)입니다.

일반 블록 목록

일반 목록 데이터 블록은 계열 1 데이터 블록 목록을 캡슐화하는 데 사용됩니다. 예를 들어 호스트 프로파일 데이터 블록 내에서 클라이언트 애플리케이션 정보를 전송하는 경우 일반 목록 데이터 블록을 통해 클라이언트 애플리케이션 데이터 블록 목록이 캡슐화됩니다. 계열 1 블록 그룹에서 일반 목록 데이터 블록의 블록 유형은 31입니다.

다음 다이어그램에 일반 목록 데이터 블록의 기본 구조가 나와 있습니다.

다음 표에는 일반 목록 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 4-34 일반 목록 데이터 블록 필드

필드	바이트 수	설명
일반 목록 블록 유형	uint32	일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	일반 목록 블록과 캡슐화된 데이터 블록의 바이트 수입니다. 이 수에는 일반 목록 블록 헤더 필드의 8바이트에 캡슐화된 모든 데이터 블록의 바이트 수를 더한 값이 포함됩니다.
캡슐화된 데이터 블록	variable	캡슐화된 데이터 블록(목록 블록 길이의 최대 바이트 수까지)입니다.

하위 서버 데이터 블록

하위 서버 데이터 블록은 개별 하위 서버(같은 호스트의 다른 서버가 호출하며 관련 취약점을 포함하는 서버)에 대한 정보를 전달합니다. 계열 1 블록 그룹에서 하위 서버 데이터 블록의 블록 유형은 1입니다.

다음 다이어그램에 하위 서버 데이터 블록의 형식이 나와 있습니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
하위 서버 이름	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	하위 서버 이름...																															
벤더 이름	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	벤더 이름...																															
버전 버전	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	버전...																															

다음 표에는 하위 서버 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 4-35 하위 서버 데이터 블록 필드

필드	데이터 유형	설명
하위 서버 블록 유형	uint32	하위 서버 데이터 블록을 시작합니다. 이 값은 항상 1입니다.
하위 서버 블록 길이	uint32	하위 서버 데이터 블록의 총 바이트 수입니다. 여기에는 하위 서버 블록 유형 및 길이 필드의 8바이트에 그 뒤의 데이터 바이트 수를 더한 값이 포함됩니다.
문자열 블록 유형	uint32	하위 서버 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	하위 서버 이름 문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이 필드의 값에 하위 서버 이름의 바이트 수를 더한 값이 포함됩니다.
하위 서버 이름	string	하위 서버의 이름입니다.
문자열 블록 유형	uint32	하위 서버 벤더가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	벤더 이름 문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이 필드의 값에 벤더 이름의 바이트 수를 더한 값이 포함됩니다.
벤더 이름	string	하위 서버 벤더 이름입니다.
문자열 블록 유형	uint32	하위 서버 버전이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.

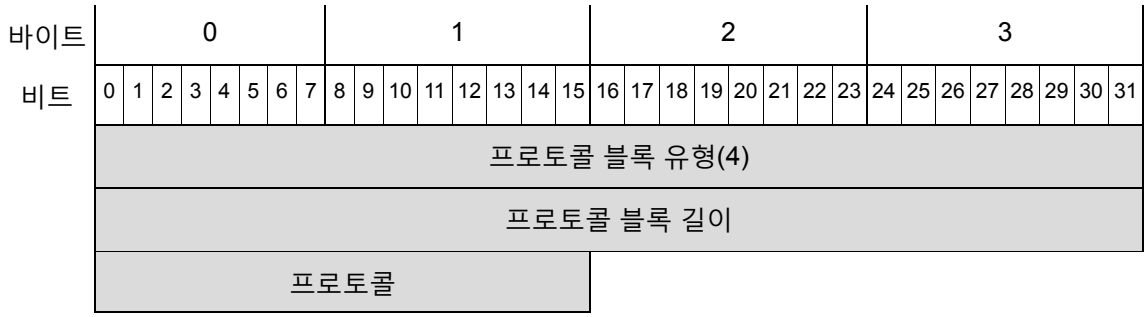
표 4-35 하위 서버 데이터 블록 필드 (계속)

필드	데이터 유형	설명
문자열 블록 길이	uint32	하위 서버 버전 문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이 필드의 값에 버전의 바이트 수를 더한 값이 포함됩니다.
버전	string	하위 서버 버전입니다.

프로토콜 데이터 블록

프로토콜 데이터 블록에서는 프로토콜이 정의됩니다. 이 데이터 블록은 블록 유형, 블록 길이 및 프로토콜을 식별하는 IANA 프로토콜 번호만 포함하는 매우 단순한 데이터 블록입니다. 계열 1 블록 그룹에서 프로토콜 데이터 블록의 블록 유형은 4입니다.

다음 그림에 프로토콜 데이터 블록의 형식이 나와 있습니다.



다음 표에는 프로토콜 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 4-36 프로토콜 데이터 블록 필드

필드	데이터 유형	설명
프로토콜 블록 유형	uint32	프로토콜 데이터 블록을 시작합니다. 이 값은 항상 4입니다.
프로토콜 블록 길이	uint32	프로토콜 데이터 블록의 바이트 수입니다. 이 값은 항상 10입니다.
프로토콜	uint16	IANA 프로토콜 번호 또는 이더 타입입니다. 이는 전송 계층 프로토콜과 네트워크 계층 프로토콜에서 서로 다르게 처리됩니다. 전송 계층 프로토콜은 IANA 프로토콜 번호로 식별됩니다. 예를 들면 다음과 같습니다. • 6 - TCP • 17 - UDP 네트워크 계층 프로토콜은 IEEE 등록 기관 이더 타입의 10진수 형식으로 식별됩니다. 예를 들면 다음과 같습니다. • 2048 - IP

정수(INT32) 데이터 블록

정수(INT32) 데이터 블록은 목록 데이터 블록에서 32비트 정수 데이터를 전달하는 데 사용됩니다.
계열 1 블록 그룹에서 정수 데이터 블록의 블록 유형은 7입니다.
다음 다이어그램에 정수 데이터 블록의 형식이 나와 있습니다.

다음 표에는 정수 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 4-37 정수 데이터 블록 필드

필드	데이터 유형	설명
정수 블록 유형	uint32	정수 데이터 블록을 시작합니다. 값은 항상 7입니다.
정수 블록 길이	uint32	정수 데이터 블록의 바이트 수입니다. 이 값은 항상 12입니다.
정수	uint32	정숫값을 포함합니다.

VLAN 데이터 블록

VLAN 데이터 블록에는 호스트에 대한 VLAN 태그 정보가 포함됩니다. 계열 1 블록 그룹에서 VLAN 데이터 블록의 블록 유형은 14입니다. 다음 다이어그램에 VLAN 데이터 블록의 형식이 나와 있습니다.

다음 표에는 VLAN 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 4-38 VLAN 데이터 블록 필드

필드	데이터 유형	설명
VLAN 블록 유형	uint32	VLAN 데이터 블록을 시작합니다. 이 값은 항상 14입니다.
VLAN 블록 길이	uint32	VLAN 데이터 블록의 바이트 수입니다. 이 값은 항상 12입니다.
VLAN ID	uint16	호스트가 구성원으로 포함된 VLAN을 나타내는 VLAN ID 번호를 포함합니다.
VLAN 유형	uint8	VLAN 태그에 캡슐화된 패킷 유형입니다. • 0 — 이더넷 • 1 — 토큰 링
VLAN 우선순위	uint8	VLAN 태그에 포함된 우선순위 값입니다.

서버 배너 데이터 블록

서버 배너 데이터 블록은 호스트에서 실행 중인 서버의 배너에 대한 정보를 제공합니다. 이 블록에는 서버 포트, 프로토콜 및 배너 데이터가 포함됩니다. 계열 1 블록 그룹에서 서버 배너 데이터 블록의 블록 유형은 37입니다.

다음 다이어그램에 서버 배너 데이터 블록의 형식이 나와 있습니다.

참고 이 다이어그램에서 블록 유형 필드 옆에 있는 별표(*)는 메시지가 계열 1 데이터 블록 인스턴스를 포함하지 않을 수도 있고 하나 이상 포함할 수도 있음을 나타냅니다.

다음 표에는 서버 배너 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 4-39 서버 배너 데이터 블록 필드

필드	데이터 유형	설명
서버 배너 블록 유형	uint32	서버 배너 데이터 블록을 시작합니다. 이 값은 항상 37입니다.
서버 배너 블록 길이	uint32	서버 배너 데이터 블록의 총 바이트 수입니다. 여기에는 서버 배너 블록 유형 및 길이 필드의 8바이트에 그 뒤의 데이터 바이트 수를 더한 값이 포함됩니다.
포트	uint16	서버가 실행되는 포트 번호입니다.
프로토콜	uint8	서버의 프로토콜 번호입니다.
BLOB 블록 유형	uint32	서버 배너 데이터를 포함하는 BLOB 데이터 블록을 시작합니다. 이 값은 항상 10입니다.
길이	uint32	BLOB 데이터 블록의 총 바이트 수(보통 264바이트)입니다.
배너	byte[*n*]	서버 이벤트에 포함되는 패킷의 첫 *n*개 바이트입니다. 여기서 *n*은 256 이하의 숫자입니다.

문자열 정보 데이터 블록

문자열 정보 데이터 블록은 문자열 데이터를 포함합니다. 예를 들어 문자열 정보 데이터 블록은 취약점 스캔 데이터 블록 내에서 CVE(일반 취약점 및 노출) ID 문자열을 전달하는 데 사용됩니다. 계열 1 블록 그룹에서 문자열 정보 데이터 블록의 블록 유형은 35입니다.

다음 다이어그램에 문자열 정보 데이터 블록의 형식이 나와 있습니다.

다음 표에는 문자열 정보 데이터 블록의 필드에 대한 설명이 나와 있습니다.

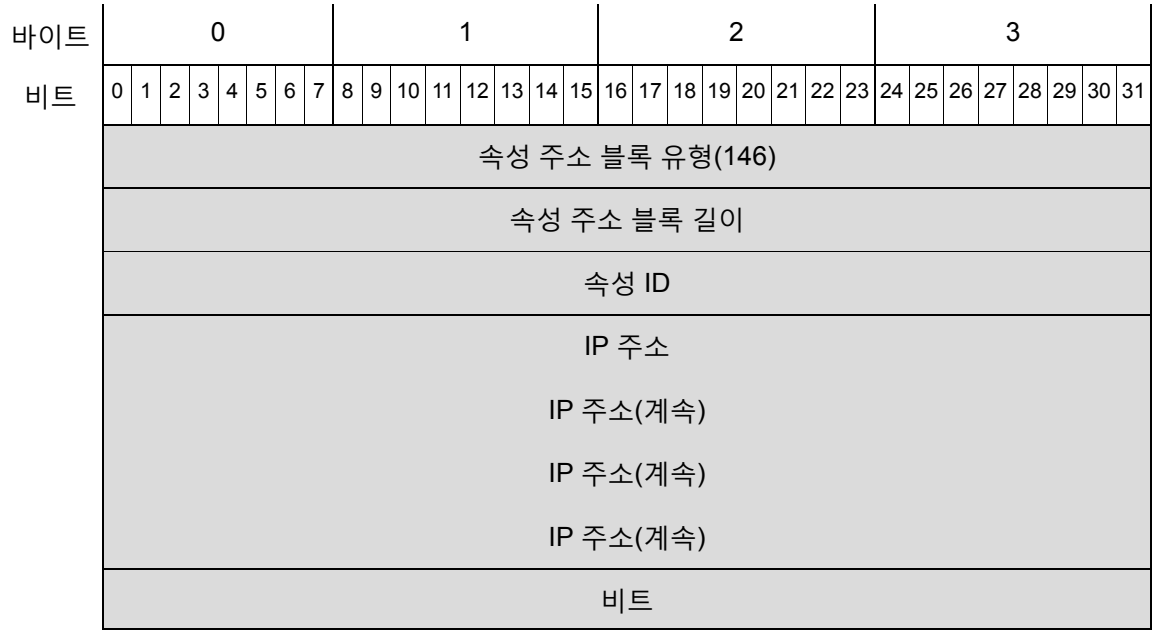
표 4-40 문자열 정보 데이터 블록 필드

필드	데이터 유형	설명
문자열 정보 블록 유형	uint32	문자열 정보 데이터 블록을 시작합니다. 이 값은 항상 35입니다.
문자열 정보 블록 길이	uint32	문자열 정보 데이터 블록 헤더 및 문자열 정보 데이터를 합한 길이입니다.
문자열 블록 유형	uint32	값에 대한 문자열 데이터 블록을 시작합니다.
문자열 블록 길이	uint32	값에 대한 문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이의 8바이트에 값의 바이트 수를 더한 값이 포함됩니다.
값	string	문자열 정보 데이터 블록을 사용하는 취약점 데이터 블록에 대한 CVE(일반 취약점 및 노출) ID 번호의 값입니다.

5.2 이상 버전용 속성 주소 데이터 블록

속성 주소 데이터 블록은 속성 목록 항목을 포함하며 속성 정의 데이터 블록 내에서 사용됩니다. 계열 1 블록 그룹에서 속성 주소 데이터 블록의 블록 유형은 146입니다.

다음 다이어그램에 속성 주소 데이터 블록의 기본 구조가 나와 있습니다.



다음 표에는 속성 주소 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 4-41 5.2 이상 버전용 속성 주소 데이터 블록

필드	데이터 유형	설명
속성 주소 블록 유형	uint32	속성 주소 데이터 블록을 시작합니다. 이 값은 항상 146입니다.
속성 주소 블록 길이	uint32	속성 주소 데이터 블록의 바이트 수입니다. 여기에는 속성 주소 블록 유형 및 길이의 8바이트에 그 뒤의 속성 주소 데이터 바이트 수를 더한 값이 포함됩니다.
속성 ID	uint32	해당하는 경우 영향을 받는 속성의 ID 번호입니다.
IP 주소	uint8[16]	주소가 자동으로 할당된 경우 호스트의 IP 주소입니다. 이 주소는 IPv4 또는 IPv6일 수 있습니다.
비트	uint32	IP 주소가 자동으로 할당된 경우 넷마스크를 계산하는 데 사용되는 주요 비트를 포함합니다.

속성 목록 항목 데이터 블록

속성 목록 항목 데이터 블록은 속성 목록 항목을 포함하며 속성 정의 데이터 블록 내에서 사용됩니다. 계열 1 블록 그룹에서 속성 목록 항목 데이터 블록의 블록 유형은 39입니다.

다음 다이어그램에 속성 목록 항목 데이터 블록의 기본 구조가 나와 있습니다.

다음 표에는 속성 목록 항목 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 4-42 속성 목록 항목 데이터 블록 필드

필드	데이터 유형	설명
속성 목록 항목 블록 유형	uint32	속성 목록 항목 데이터 블록을 시작합니다. 이 값은 항상 39입니다.
속성 목록 항목 블록 길이	uint32	속성 목록 항목 데이터 블록의 바이트 수입니다. 여기에는 속성 목록 항목 블록 유형 및 길이의 8바이트에 그 뒤의 속성 목록 항목 데이터 바이트 수를 더한 값이 포함됩니다.
속성 ID	uint32	해당하는 경우 영향을 받는 속성의 ID 번호입니다.
문자열 블록 유형	uint32	속성 목록 항목 이름에 대해 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	속성 목록 항목 이름에 대한 문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이의 8바이트에 값의 속성 목록 항목 이름의 바이트 수를 더한 값이 포함됩니다.
이름	string	속성 목록 항목 이름입니다.

속성값 데이터 블록

속성값 데이터 블록은 호스트 속성의 속성 ID 번호와 값을 전달합니다. 이벤트에 나와 있는 호스트에 적용된 각 속성의 속성값 데이터 블록은 전체 호스트 프로파일 데이터 블록 목록에 포함되어 있습니다. 계열 1 블록 그룹에서 속성값 데이터 블록의 블록 유형은 48입니다.

다음 다이어그램에 속성값 데이터 블록의 형식이 나와 있습니다.

다음 표에는 속성값 데이터 블록의 구성 요소에 대한 설명이 나와 있습니다.

표 4-43 속성값 데이터 블록 필드

필드	데이터 유형	설명
속성값 블록 유형	uint32	속성값 데이터 블록을 시작합니다. 이 값은 항상 48입니다.
속성값 블록 길이	uint32	속성값 데이터 블록의 총 바이트 수입니다. 여기에는 속성값 블록 유형 및 길이 필드의 8바이트에 그 뒤의 속성 블록 데이터 바이트 수를 더한 값이 포함됩니다.
속성 ID	uint32	속성의 ID 번호입니다.
속성 유형	uint32	영향을 받는 속성의 유형입니다. 가능한 값은 다음과 같습니다. • 0 - 값으로 텍스트가 포함된 속성입니다. 문자열 데이터를 사용합니다. • 1 - 범위 내의 값이 포함된 속성입니다. 정수 데이터를 사용합니다. • 2 - 가능한 값 목록이 포함된 속성입니다. 정수 데이터를 사용합니다. • 3 - 값으로 URL이 포함된 속성입니다. 문자열 데이터를 사용합니다. • 4 - 값으로 이진 BLOB가 포함된 속성입니다. 문자열 데이터를 사용합니다.
속성 정숫값	uint32	해당하는 경우 속성의 정숫값입니다.
문자열 블록 유형	uint32	속성 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이 필드의 값에 속성 이름의 바이트 수를 더한 값이 포함됩니다.
속성값	string	속성의 값입니다.

전체 하위 서버 데이터 블록

전체 하위 서버 데이터 블록은 호스트에서 탐지된 서버와 연결되어 있는 하위 서버에 대한 정보를 전달하며, 호스트의 하위 서버에 대한 벤더/버전 및 관련 VDB 및 서드파티 취약점과 같은 하위 서버 관련 정보를 포함합니다. 하위 서버는 고유한 관련 취약점이 있는 서버의 로드 가능 모듈입니다. 전체 호스트 서버 데이터 블록은 호스트에서 탐지되는 각 하위 서버의 전체 하위 서버 데이터 블록을 포함합니다. 계열 1 블록 그룹에서 전체 하위 서버 데이터 블록의 블록 유형은 51입니다.

참고 다음 다이어그램에서 계열 1 데이터 블록 이름 옆에 있는 별표(*)는 데이터 블록 인스턴스가 여러 개 나올 수 있음을 나타냅니다.

다음 다이어그램에 전체 하위 서버 데이터 블록의 형식이 나와 있습니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
전체 하위 서버 블록 유형(51)																																
전체 하위 서버 블록 길이																																
문자열 블록 유형(0)																																
문자열 블록 길이																																
하위 서버 이름 문자열...																																
문자열 블록 유형(0)																																
문자열 블록 길이																																
하위 서버 벤더 이름 문자열...																																
문자열 블록 유형(0)																																
문자열 블록 길이																																
하위 서버 버전 문자열...																																
일반 목록 블록 유형(31)																																
일반 목록 블록 길이																																
(VDB) 호스트 취약점 데이터 블록*																																
일반 목록 블록 유형(31)																																
일반 목록 블록 길이																																
(서드파티 스캔) 호스트 취약점 데이터 블록*																																

다음 표에는 전체 하위 서버 데이터 블록의 구성 요소에 대한 설명이 나와 있습니다.

표 4-44 전체 하위 서버 데이터 블록 필드

필드	데이터 유형	설명
전체 하위 서버 블록 유형	uint32	전체 하위 서버 데이터 블록을 시작합니다. 이 값은 항상 51입니다.
전체 하위 서버 블록 길이	uint32	전체 하위 서버 데이터 블록의 총 바이트 수입니다. 여기에는 전체 하위 서버 블록 유형 및 길이 필드의 8바이트에 그 뒤의 전체 하위 서버 데이터 바이트 수를 더한 값이 포함됩니다.

표 4-44 전체 하위 서버 데이터 블록 필드 (계속)

필드	데이터 유형	설명
문자열 블록 유형	uint32	하위 서버 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	하위 서버 이름 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 하위 서버 이름의 바이트 수를 더한 값이 포함됩니다.
하위 서버 이름	string	하위 서버 이름입니다.
문자열 블록 유형	uint32	하위 서버 벤더 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	벤더 이름 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 하위 서버 벤더 이름의 바이트 수를 더한 값이 포함됩니다.
하위 서버 벤더 이름	string	하위 서버 벤더의 이름입니다.
문자열 블록 유형	uint32	하위 서버 버전이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	하위 서버 버전 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 하위 서버 버전의 바이트 수를 더한 값이 포함됩니다.
하위 서버 버전	string	하위 서버 버전입니다.
일반 목록 블록 유형	uint32	VDB 취약점 데이터를 전달하는 호스트 취약점 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 호스트 취약점 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
VDB 호스트 취약점 데이터 블록*	variable	Cisco에서 식별한 호스트 취약점에 대한 정보를 포함하는 호스트 취약점 데이터 블록입니다. 이 데이터 블록에 대한 설명은 4.9.0 이상 버전용 호스트 취약점 데이터 블록, 4-114페이지의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	서드파티 취약점 스캔 데이터를 전달하는 호스트 취약점 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 호스트 취약점 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
서드파티 스캔 호스트 취약점 데이터 블록*	variable	서드파티 취약점 스캐너에서 식별한 호스트 취약점에 대한 정보를 포함하는 호스트 취약점 데이터 블록입니다. 이 데이터 블록에 대한 설명은 4.9.0 이상 버전용 호스트 취약점 데이터 블록, 4-114페이지의 내용을 참조하십시오.

3.5 이상 버전용 운영 체제 데이터 블록

계열 1 블록 그룹에서 3.5 이상 버전용 운영 체제 데이터 블록의 블록 유형은 53입니다. 이 블록에는 핑거프린트 UUID(범용 고유 식별자)가 포함됩니다. 다음 다이어그램에 3.5 이상 버전의 운영 체제 데이터 블록 형식이 나와 있습니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	운영 체제 블록 유형(53)																															
	운영 체제 블록 길이																															
	신뢰도																															
OS 핑거프린트 UUID	핑거프린트 UUID 핑거프린트 UUID(계속) 핑거프린트 UUID(계속) 핑거프린트 UUID(계속)																															

다음 표에는 v3.5 운영 체제 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 4-45 3.5 이상 버전 운영 체제 데이터 블록 필드

필드	데이터 유형	설명
운영 체제 데이터 블록 유형	uint32	운영 체제 데이터 블록을 시작합니다. 이 값은 항상 53입니다.
운영 체제 데이터 블록 길이	uint32	운영 체제 데이터 블록의 바이트 수입니다. 이 값은 항상 28(데이터 블록 유형 및 길이 필드의 8바이트 + 신뢰도 값의 4바이트 + 핑거프린트 UUID 값의 16바이트)이어야 합니다.
신뢰도	uint32	신뢰도 백분율 값입니다.
핑거프린트 UUID	uint8[16]	운영 체제의 고유 식별자 역할을 하는 옥텟 형식의 핑거프린트 ID 번호입니다. 핑거프린트 UUID는 Cisco 데이터베이스의 운영 체제 이름, 벤더 및 버전에 매핑됩니다.

정책 엔진 제어 메시지 데이터 블록

정책 엔진 제어 메시지 데이터 블록은 정책 유형의 제어 메시지 콘텐츠를 전달합니다. 계열 1 블록 그룹에서 정책 엔진 제어 메시지 데이터 블록의 블록 유형은 54입니다.

다음 다이어그램에 정책 엔진 제어 메시지 데이터 블록의 형식이 나와 있습니다.

다음 표에는 정책 엔진 제어 메시지 데이터 블록의 구성 요소에 대한 설명이 나와 있습니다.

표 4-46 정책 엔진 제어 메시지 데이터 블록 필드

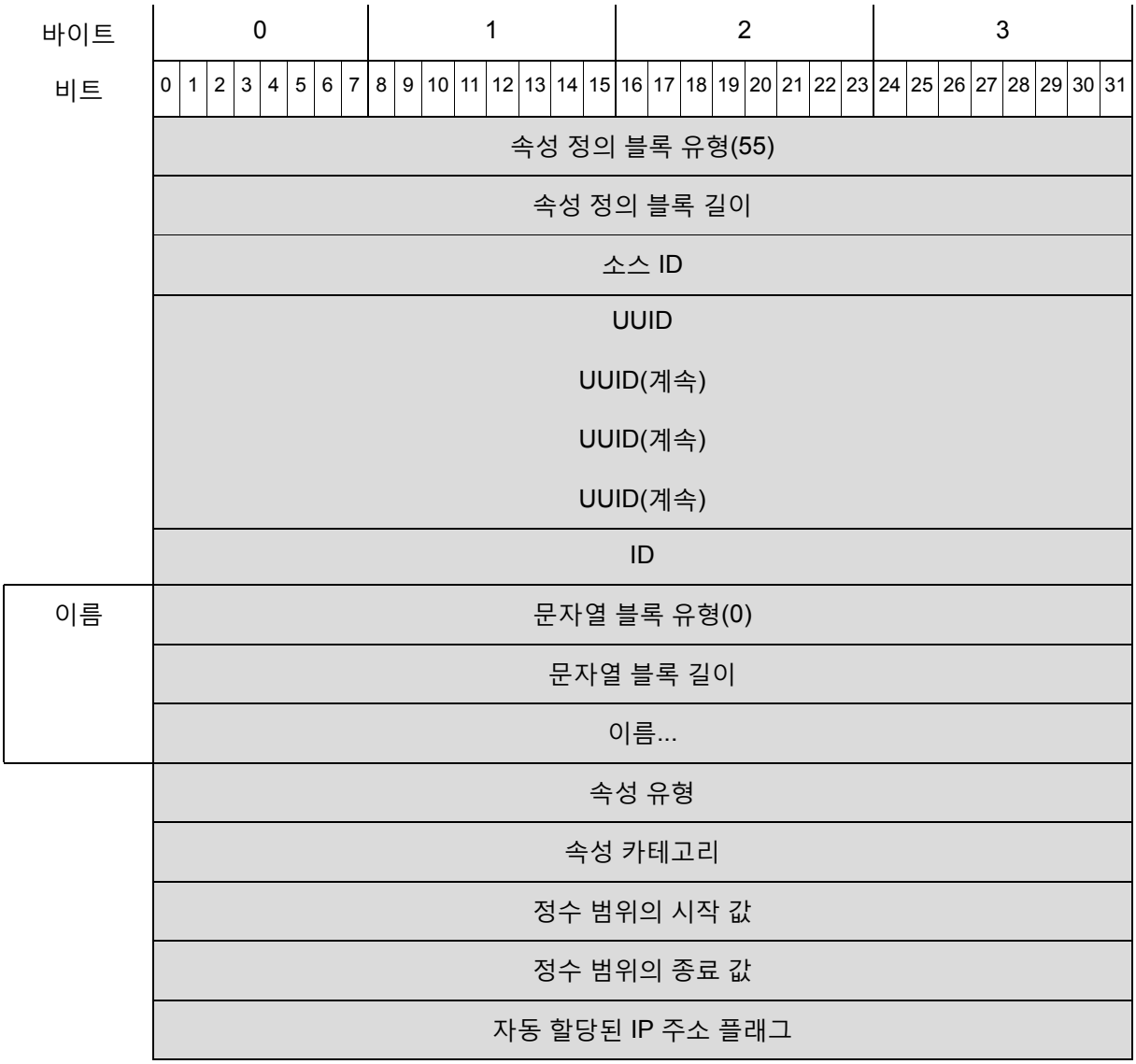
필드	데이터 유형	설명
정책 엔진 제어 메시지 블록 유형	uint32	정책 엔진 제어 메시지 데이터 블록을 시작합니다. 이 값은 항상 54입니다.
정책 엔진 제어 메시지 길이	uint32	정책 엔진 제어 메시지 데이터 블록의 총 바이트 수입니다. 여기에는 정책 엔진 제어 블록 유형 및 길이 필드의 8바이트에 그 뒤의 정책 엔진 제어 데이터 바이트 수를 더한 값이 포함됩니다.
유형	uint32	이벤트에 대한 정책의 유형을 나타냅니다.
문자열 블록 유형	uint32	제어 메시지를 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	제어 메시지 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 제어 메시지의 바이트 수를 더한 값이 포함됩니다.
제어 메시지	uint32	정책 엔진의 제어 메시지입니다.

4.7 이상 버전용 속성 정의 데이터 블록

속성 정의 데이터 블록은 속성 생성, 변경 또는 삭제 이벤트의 속성 정의를 포함하며 호스트 속성 추가 이벤트(이벤트 유형 1002, 하위 유형 6), 호스트 속성 업데이트 이벤트(이벤트 유형 1002, 하위 유형 7) 및 호스트 속성 삭제 이벤트(이벤트 유형 1002, 하위 유형 8) 내에서 사용됩니다. 계열 1 블록 그룹에서 속성 정의 데이터 블록의 블록 유형은 55입니다.

이러한 이벤트에 대한 자세한 정보는 속성 메시지, 4-57페이지의 내용을 참조하십시오.

다음 다이어그램에 속성 정의 데이터 블록의 기본 구조가 나와 있습니다.



다음 표에는 속성 정의 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 4-47 속성 정의 데이터 블록 필드

필드	데이터 유형	설명
속성 정의 블록 유형	uint32	속성 정의 데이터 블록을 시작합니다. 이 값은 항상 55입니다.
속성 정의 블록 길이	uint32	속성 정의 데이터 블록의 바이트 수입니다. 여기에는 속성 정의 블록 유형 및 길이의 8바이트에 그 뒤의 속성 정의 데이터 바이트 수를 더한 값이 포함됩니다.
소스 ID	uint32	속성 데이터 소스에 매핑되는 ID 번호입니다. 소스 유형에 따라 RNA, 사용자, 스캐너 또는 서드파티 애플리케이션에 매핑될 수 있습니다.
UUID	uint8[16]	영향을 받는 속성의 고유 식별자 역할을 하는 ID 번호입니다.
속성 ID	uint32	해당하는 경우 영향을 받는 속성의 ID 번호입니다.
문자열 블록 유형	uint32	속성 정의 이름에 대한 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	속성 정의 이름에 대한 문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이의 8바이트에 값의 속성 정의 이름의 바이트 수를 더한 값이 포함됩니다.
이름	string	속성 정의 이름입니다.

표 4-47 속성 정의 데이터 블록 필드 (계속)

필드	데이터 유형	설명
속성 유형	uint32	속성의 유형입니다. 가능한 값은 다음과 같습니다. • 0 - 값으로 텍스트가 포함된 속성입니다. 문자열 데이터를 사용합니다. • 1 - 범위 내의 값이 포함된 속성입니다. 정수 데이터를 사용합니다. • 2 - 가능한 값 목록이 포함된 속성입니다. 정수 데이터를 사용합니다. • 3 - 값으로 URL이 포함된 속성입니다. 문자열 데이터를 사용합니다. • 4 - 값으로 이진 BLOB가 포함된 속성입니다. 문자열 데이터를 사용합니다.
속성 카테고리	uint32	속성 카테고리입니다.
범위의 시작 값	uint32	정의된 속성의 정수 범위에서 첫 번째 값입니다.
범위의 종료 값	uint32	정의된 속성의 정수 범위에서 마지막 값입니다.
자동 할당된 IP 주소 플래그	uint32	IP 주소가 속성을 기반으로 자동 할당되는지를 나타내는 플래그입니다.
목록 블록 유형	uint32	속성 목록 항목을 전달하는 속성 목록 항목 데이터 블록으로 구성된 목록 데이터 블록을 시작합니다. 이 값은 항상 11입니다.
목록 블록 길이	uint32	목록의 바이트 수입니다. 이 수에는 목록 블록 유형 및 길이 필드의 8바이트에 캡슐화된 모든 속성 목록 항목 데이터 블록을 더한 값이 포함됩니다. 이 필드 뒤에는 속성 목록 항목 데이터 블록이 없을 수도 있고 하나 이상 올 수도 있습니다.
속성 목록 항목 블록 유형	uint32	첫 번째 속성 목록 항목 데이터 블록을 시작합니다. 이 데이터 블록 뒤에는 목록 블록 길이 필드에 정의된 제한까지 다른 속성 목록 항목 데이터 블록이 올 수 있습니다.
속성 목록 항목 블록 길이	uint32	속성 목록 항목 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 헤더 필드의 8바이트에 속성 목록 항목의 바이트 수를 더한 값이 포함됩니다.
속성 목록 항목	variable	속성 목록 항목 데이터 블록, 4-82페이지에 설명되어 있는 속성 목록 항목 데이터입니다.
목록 블록 유형	uint32	속성이 포함된 호스트의 IP 주소를 전달하는 속성 주소 데이터 블록으로 구성된 목록 데이터 블록을 시작합니다. 이 값은 항상 11입니다.
목록 블록 길이	uint32	목록의 바이트 수입니다. 이 수에는 목록 블록 유형 및 길이 필드의 8바이트에 캡슐화된 모든 속성 주소 데이터 블록을 더한 값이 포함됩니다. 이 필드 뒤에는 속성 주소 데이터 블록이 없을 수도 있고 하나 이상 올 수도 있습니다.

표 4-47 속성 정의 데이터 블록 필드 (계속)

필드	데이터 유형	설명
속성 주소 블록 유형	uint32	첫 번째 속성 주소 데이터 블록을 시작합니다. 이 데이터 블록 뒤에는 목록 블록 길이 필드에 정의된 제한까지 다른 속성 주소 데이터 블록이 올 수 있습니다.
속성 주소 블록 길이	uint32	속성 주소 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 헤더 필드의 8바이트에 속성 주소의 바이트 수를 더한 값이 포함됩니다.
속성 주소	variable	5.2 이상 버전용 속성 주소 데이터 블록, 4-81페이지에 설명되어 있는 속성 주소 데이터입니다.

사용자 프로토콜 데이터 블록

사용자 프로토콜 데이터 블록은 추가된 프로토콜, 프로토콜의 유형, 그리고 프로토콜 내 호스트의 IP 주소 및 MAC 주소 범위 목록에 대한 정보를 포함하는 데 사용됩니다. 계열 1 블록 그룹에서 사용자 프로토콜 데이터 블록의 블록 유형은 57입니다.

다음 다이어그램에 사용자 프로토콜 데이터 블록의 기본 구조가 나와 있습니다.

다음 표에는 사용자 프로토콜 데이터 블록의 필드에 대한 설명이 나와 있습니다.

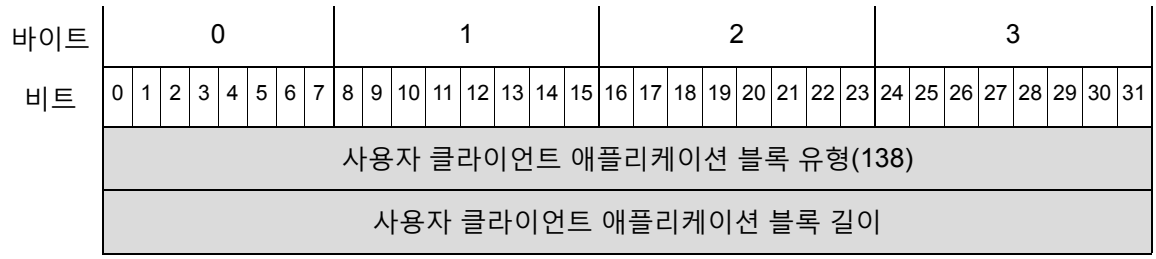
표 4-48 사용자 프로토콜 데이터 블록 필드

필드	바이트 수	설명
사용자 프로토콜 블록 유형	uint32	사용자 프로토콜 데이터 블록을 시작합니다. 이 값은 항상 57입니다.
사용자 프로토콜 블록 길이	uint32	사용자 프로토콜 데이터 블록의 총 바이트 수입니다. 여기에는 사용자 프로토콜 블록 유형 및 길이 필드의 8바이트에 그 뒤의 사용자 프로토콜 데이터 바이트 수를 더한 값이 포함됩니다.
일반 목록 블록 유형	uint32	IP 주소 범위 데이터를 전달하는 IP 범위 사양 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 IP 범위 사양 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
IP 범위 사양 데이터 블록*	variable	사용자 입력의 IP 주소 범위에 대한 정보가 포함된 IP 범위 사양 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.2 이상 버전용 IP 주소 범위 데이터 블록, 4-96페이지의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	MAC 주소 범위 데이터를 전달하는 MAC 범위 사양 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 MAC 범위 사양 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
MAC 범위 사양 데이터 블록*	variable	사용자 입력의 MAC 주소 범위에 대한 정보가 포함된 MAC 범위 사양 데이터 블록입니다. 이 데이터 블록에 대한 설명은 MAC 주소 사양 데이터 블록, 4-99페이지의 내용을 참조하십시오.
프로토콜 유형	uint8	프로토콜의 유형을 나타냅니다. 프로토콜은 IP와 같은 네트워크 계층 프로토콜의 경우 0이거나, TCP/UDP와 같은 전송 계층 프로토콜의 경우 1일 수 있습니다.
프로토콜	uint16	데이터 블록에 포함된 데이터의 프로토콜을 나타냅니다.

5.1.1 이상 버전용 사용자 클라이언트 애플리케이션 데이터 블록

사용자 클라이언트 애플리케이션 데이터 블록에는 클라이언트 애플리케이션 데이터의 소스에 대한 정보, 데이터를 추가한 사용자의 ID 번호 및 IP 주소 범위 데이터 블록 목록이 포함됩니다. 버전 6.2.3에 추가된 페이로드 ID는 레코드와 관련된 애플리케이션 인스턴스를 지정합니다. 계열 1 블록 그룹에서 사용자 클라이언트 애플리케이션 데이터 블록의 블록 유형은 138입니다. 이 데이터 블록은 블록 유형 59를 대체합니다.

다음 다이어그램에 사용자 클라이언트 애플리케이션 데이터 블록의 기본 구조가 나와 있습니다.



다음 표에는 사용자 클라이언트 애플리케이션 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 4-49 사용자 클라이언트 애플리케이션 데이터 블록 필드

필드	바이트 수	설명
사용자 클라이언트 애플리케이션 블록 유형	uint32	사용자 클라이언트 애플리케이션 데이터 블록을 시작합니다. 이 값은 항상 138입니다.
사용자 클라이언트 애플리케이션 블록 길이	uint32	사용자 클라이언트 애플리케이션 데이터 블록의 총 바이트 수입니다. 여기에는 사용자 클라이언트 애플리케이션 블록 유형 및 길이 필드의 8바이트에 그 뒤의 사용자 클라이언트 애플리케이션 데이터 바이트 수를 더한 값이 포함됩니다.
일반 목록 블록 유형	uint32	IP 주소 범위 데이터를 전달하는 IP 범위 사양 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 IP 범위 사양 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
IP 범위 사양 데이터 블록*	variable	사용자 입력의 IP 주소 범위에 대한 정보가 포함된 IP 범위 사양 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.2 이상 버전용 IP 주소 범위 데이터 블록, 4-96페이지의 내용을 참조하십시오.
애플리케이션 프로토콜 ID	uint32	해당하는 경우 애플리케이션 프로토콜의 내부 ID 번호입니다.
클라이언트 애플리케이션 ID	uint32	해당하는 경우 탐지된 클라이언트 애플리케이션의 내부 ID 번호입니다.

표 4-49 사용자 클라이언트 애플리케이션 데이터 블록 필드 (계속)

필드	바이트 수	설명
문자열 블록 유형	uint32	클라이언트 애플리케이션 버전이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	클라이언트 애플리케이션 버전 문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이 필드의 값에 버전의 바이트 수를 더한 값이 포함됩니다.
버전	string	클라이언트 애플리케이션 버전입니다.
페이로드 유형	uint32	이 필드는 이전 버전과의 호환성을 위해 포함되며 값은 항상 0입니다.
웹 애플리케이션 ID	uint32	해당하는 경우 웹 애플리케이션의 내부 ID 번호입니다.

사용자 클라이언트 애플리케이션 목록 데이터 블록

사용자 클라이언트 애플리케이션 목록 데이터 블록에는 클라이언트 애플리케이션 데이터의 소스에 대한 정보, 데이터를 추가한 사용자의 ID 번호 및 클라이언트 애플리케이션 블록 목록이 포함됩니다. 계열 1 블록 그룹에서 사용자 클라이언트 애플리케이션 목록 데이터 블록의 블록 유형은 60입니다.

다음 다이어그램에 사용자 클라이언트 애플리케이션 목록 데이터 블록의 기본 구조가 나와 있습니다.

다음 표에는 사용자 클라이언트 애플리케이션 목록 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 4-50 사용자 클라이언트 애플리케이션 목록 데이터 블록 필드

필드	바이트 수	설명
사용자 클라이언트 애플리케이션 목록 블록 유형	uint32	사용자 클라이언트 애플리케이션 목록 데이터 블록을 시작합니다. 이 값은 항상 60입니다.
사용자 클라이언트 애플리케이션 목록 블록 길이	uint32	사용자 클라이언트 애플리케이션 목록 데이터 블록의 총 바이트 수입니다. 여기에는 사용자 클라이언트 애플리케이션 목록 블록 유형 및 길이 필드의 8바이트에 그 뒤의 사용자 클라이언트 애플리케이션 목록 데이터 바이트 수를 더한 값이 포함됩니다.
소스 유형	uint32	데이터 소스의 유형에 매핑되는 번호입니다. • 0 - RNA에서 클라이언트 데이터를 탐지한 경우 • 1 - 사용자가 클라이언트 데이터를 제공한 경우 • 2 - 서드파티 스캐너에서 클라이언트 데이터를 탐지한 경우 • 3 - nmimport.pl 등의 커맨드 라인 툴이나 호스트 입력 API 클라이언트에서 클라이언트 데이터를 제공한 경우
소스 ID	uint32	영향을 받는 클라이언트 애플리케이션을 추가한 소스에 매핑되는 ID 번호입니다. 소스 유형에 따라 RNA, 사용자, 스캐너 또는 서드파티 애플리케이션에 매핑될 수 있습니다.
일반 목록 블록 유형	uint32	일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	일반 목록 블록과 캡슐화된 데이터 블록의 바이트 수입니다. 이 수에는 일반 목록 블록 헤더 필드의 8바이트에 캡슐화된 모든 데이터 블록의 바이트 수를 더한 값이 포함됩니다.
사용자 클라이언트 애플리케이션 블록	variable	캡슐화된 사용자 클라이언트 애플리케이션 데이터 블록(목록 블록 길이의 최대 바이트 수까지)입니다. 사용자 클라이언트 애플리케이션 데이터 블록에 대한 자세한 정보는 5.1.1 이상 버전용 사용자 클라이언트 애플리케이션 데이터 블록, 4-93페이지의 내용을 참조하십시오.

5.2 이상 버전용 IP 주소 범위 데이터 블록

5.2 이상 버전용 IP 주소 범위 데이터 블록은 IP 주소 범위를 전달합니다. IP 주소 범위 데이터 블록은 사용자 프로토콜, 사용자 클라이언트 애플리케이션, 주소 사양, 사용자 제품, 사용자 서버, 사용자 호스트, 사용자 취약점, 사용자 임계성 및 사용자 속성값 데이터 블록에 사용됩니다. 계열 1 블록 그룹에서 IP 주소 범위 데이터 블록의 블록 유형은 141입니다.

다음 다이어그램에 IP 주소 범위 데이터 블록의 형식이 나와 있습니다.

다음 표에는 IP 주소 범위 사양 데이터 블록의 구성 요소에 대한 설명이 나와 있습니다.

표 4-51 IP 주소 범위 데이터 블록 필드

필드	데이터 유형	설명
IP 주소 범위 블록 유형	uint32	IP 주소 범위 데이터 블록을 시작합니다. 이 값은 항상 61입니다.
IP 주소 범위 블록 길이	uint32	IP 주소 범위 데이터 블록의 총 바이트 수입니다. 여기에는 IP 주소 범위 블록 유형 및 길이 필드의 8바이트에 그 뒤의 IP 주소 범위 데이터 바이트 수를 더한 값이 포함됩니다.
IP 주소 범위 시작	uint8[16]	IP 주소 범위의 시작 IP 주소입니다.
IP 주소 범위 끝	uint8[16]	IP 주소 범위의 끝 IP 주소입니다.

속성 사양 데이터 블록

속성 사양 데이터 블록은 속성 이름 및 값을 전달합니다. 계열 1 블록 그룹에서 속성 사양 데이터 블록의 블록 유형은 62입니다.

다음 다이어그램에 속성 사양 데이터 블록의 형식이 나와 있습니다.

다음 표에는 속성 사양 데이터 블록의 구성 요소에 대한 설명이 나와 있습니다.

표 4-52 속성 사양 데이터 블록 필드

필드	데이터 유형	설명
속성 사양 블록 유형	uint32	속성 사양 데이터 블록을 시작합니다. 이 값은 항상 62입니다.
문자열 블록 유형	uint32	속성 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	속성 이름 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 속성 이름의 바이트 수를 더한 값이 포함됩니다.
속성값	uint32	속성의 값입니다.
문자열 블록 유형	uint32	속성 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	속성 이름 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 속성 이름의 바이트 수를 더한 값이 포함됩니다.
속성 이름	uint32	속성의 이름입니다.

호스트 IP 주소 데이터 블록

호스트 IP 주소 데이터 블록은 개별 IP 주소를 전달합니다. IP 주소는 IPv4 또는 IPv6 주소일 수 있습니다. 호스트 IP 주소 데이터 블록은 사용자 프로토콜, 주소 사양 및 사용자 호스트 데이터 블록에 사용됩니다. 계열 1 블록 그룹에서 호스트 IP 데이터 블록의 블록 유형은 143입니다.

다음 다이어그램에 호스트 IP 주소 데이터 블록의 형식이 나와 있습니다.

다음 표에는 호스트 IP 주소 데이터 블록의 구성 요소에 대한 설명이 나와 있습니다.

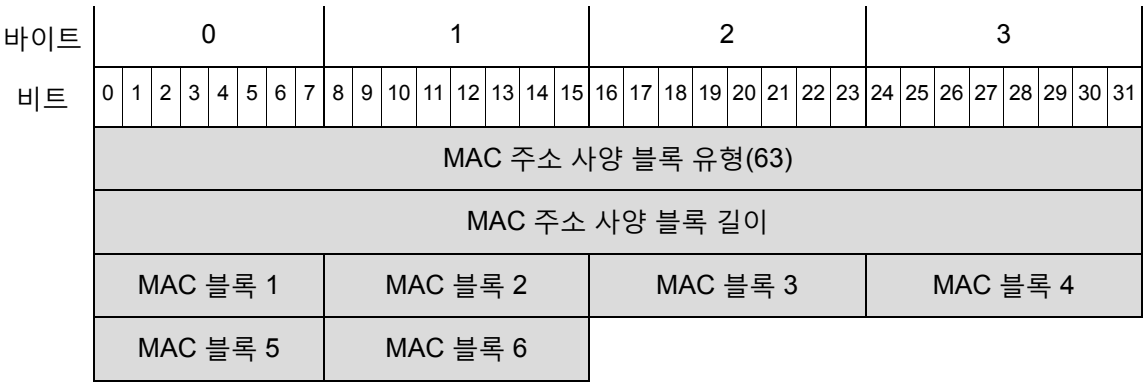
표 4-53 호스트 IP 주소 데이터 블록 필드

필드	데이터 유형	설명
호스트 IP 주소 블록 유형	uint32	호스트 IP 주소 데이터 블록을 시작합니다. 이 값은 항상 143입니다.
호스트 IP 블록 길이	uint32	호스트 IP 주소 데이터 블록의 총 바이트 수입니다. 여기에는 호스트 IP 블록 유형 및 길이 필드의 8바이트에 그 뒤의 호스트 IP 주소 데이터 바이트 수를 더한 값이 포함됩니다.
IP 주소	uint8[16]	IP 주소입니다. IPv4 또는 IPv6일 수 있습니다.
마지막 확인	uint32	IP 주소가 마지막으로 탐지된 시간을 나타내는 UNIX 타임스탬프입니다.

MAC 주소 사양 데이터 블록

MAC 주소 사양 데이터 블록은 개별 MAC 주소를 전달합니다. MAC 주소 사양 데이터 블록은 사용자 프로토콜, 주소 사양 및 사용자 호스트 데이터 블록에 사용됩니다. 계열 1 블록 그룹에서 MAC 주소 사양 데이터 블록의 블록 유형은 63입니다.

다음 다이어그램에 MAC 주소 사양 데이터 블록의 형식이 나와 있습니다.



다음 표에는 MAC 주소 사양 데이터 블록의 구성 요소에 대한 설명이 나와 있습니다.

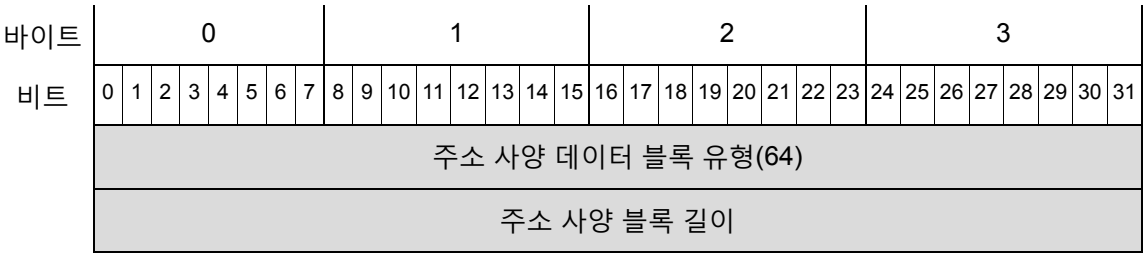
표 4-54 MAC 주소 사양 데이터 블록 필드

필드	데이터 유형	설명
MAC 주소 사양 블록 유형	uint32	MAC 주소 사양 데이터 블록을 시작합니다. 이 값은 항상 63입니다.
MAC 주소 사양 블록 길이	uint32	MAC 주소 사양 데이터 블록의 총 바이트 수입니다. 여기에는 MAC 주소 사양 블록 유형 및 길이 필드의 8바이트에 그 뒤의 MAC 주소 사양 데이터 바이트 수를 더한 값이 포함됩니다.
MAC 주소 블록 1~6	uint8	순차적 MAC 주소 블록입니다.

주소 사양 데이터 블록

주소 사양 데이터 블록은 IP 주소 범위 사양 및 MAC 주소 사양 목록을 포함하는 데 사용됩니다. 계열 1 블록 그룹에서 주소 사양 데이터 블록의 블록 유형은 64입니다.

다음 다이어그램에 주소 사양 데이터 블록의 기본 구조가 나와 있습니다.



다음 표에는 주소 사양 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 4-55 주소 사양 데이터 블록 필드

필드	바이트 수	설명
주소 사양 데이터 블록 유형	uint32	주소 사양 데이터 블록을 시작합니다. 이 값은 항상 64입니다.
주소 사양 블록 길이	uint32	주소 사양 데이터 블록의 총 바이트 수입니다. 여기에는 주소 사양 블록 유형 및 길이 필드의 8바이트에 그 뒤의 주소 사양 데이터 바이트 수를 더한 값이 포함됩니다.
일반 목록 블록 유형	uint32	일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	일반 목록 블록과 캡슐화된 데이터 블록의 바이트 수입니다. 이 수에는 일반 목록 블록 헤더 필드의 8바이트에 캡슐화된 모든 데이터 블록의 바이트 수를 더한 값이 포함됩니다.
IP 주소 범위 사양 데이터 블록	variable	캡슐화된 IP 주소 범위 사양 데이터 블록(목록 블록 길이의 최대 바이트 수까지)입니다. 자세한 정보는 5.2 이상 버전용 IP 주소 범위 데이터 블록, 4-96페이지의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	일반 목록 블록과 캡슐화된 데이터 블록의 바이트 수입니다. 이 수에는 일반 목록 블록 헤더 필드의 8바이트에 캡슐화된 모든 데이터 블록의 바이트 수를 더한 값이 포함됩니다.
MAC 주소 사양 데이터 블록	variable	캡슐화된 MAC 주소 사양 데이터 블록(목록 블록 길이의 최대 바이트 수까지)입니다. 자세한 정보는 MAC 주소 사양 데이터 블록, 4-99페이지의 내용을 참조하십시오.

6.1 이상 버전용 연결 청크 데이터 블록

연결 청크 데이터 블록은 연결 데이터를 전달하며 5분 동안 누적된 연결 로그 데이터를 저장합니다. 6.1 이상 버전에는 Original Client IP Address(원래 클라이언트 IP 주소)라는 새 필드가 도입되었습니다. 계열 1 블록 그룹에서 연결 청크 데이터 블록의 블록 유형은 164입니다. 이는 블록 유형 136을 대체합니다.

다음 다이어그램에 연결 청크 데이터 블록의 형식이 나와 있습니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
연결 청크 블록 유형(136)																																
연결 청크 블록 길이																																
이니시에이터 IP 주소																																
응답자 IP 주소																																
원래 클라이언트 IP 주소																																
시작 시간																																
애플리케이션 프로토콜																																
응답자 포트																	프로토콜								연결 유형							
NetFlow 탐지기 IP 주소																																
전송한 패킷 전송한 패킷(계속)																																
수신된 패킷 수신된 패킷(계속)																																
전송된 바이트 전송된 바이트(계속)																																
수신된 바이트 수신된 바이트(계속)																																
연결																																

다음 표에는 연결 청크 데이터 블록의 구성 요소에 대한 설명이 나와 있습니다.

표 4-56 연결 청크 데이터 블록 필드

필드	데이터 유형	설명
연결 청크 블록 유형	uint32	연결 청크 데이터 블록을 시작합니다. 이 값은 항상 164입니다.
연결 청크 블록 길이	uint32	연결 청크 데이터 블록의 총 바이트 수입니다. 여기에는 연결 청크 블록 유형 및 길이 필드의 8바이트에 그 뒤의 연결 청크 데이터 바이트 수를 더한 값이 포함됩니다.
이니시에이터 IP 주소	uint8(4)	이 연결 유형의 이니시에이터 IP 주소입니다. 이 주소를 원래 클라이언트 및 응답자 IP 주소와 함께 사용하여 동일한 연결을 식별합니다.
응답자 IP 주소	uint8(4)	이 연결 유형의 응답자 IP 주소입니다. 이 주소를 이니시에이터 및 원래 클라이언트 IP 주소와 함께 사용하여 동일한 연결을 식별합니다.
원래클라이언트 IP 주소	uint8(4)	요청이 생성된 프록시를 사용하는 호스트의 IP 주소입니다. 이 주소를 이니시에이터 및 응답자 IP 주소와 함께 사용하여 동일한 연결을 식별합니다.
시작 시간	uint32	연결 청크의 시작 시간입니다.
애플리케이션 프로토콜	uint32	연결에 사용된 프로토콜의 ID 번호입니다.
응답자 포트	uint16	연결 청크의 응답자가 사용하는 포트입니다.
프로토콜	uint8	사용자 정보를 포함하는 패킷의 프로토콜입니다.
연결 유형	uint8	연결의 유형입니다.
NetFlow 탐지기 IP 주소	uint8[4]	연결을 탐지한 NetFlow 디바이스의 IP 주소(IP 주소 옥텟 형식)입니다.
전송한 패킷	uint64	연결 청크에서 보낸 패킷의 수입니다.
수신된 패킷	uint64	연결 청크에서 받은 패킷의 수입니다.
전송된 바이트	uint64	연결 청크에서 보낸 바이트 수입니다.
수신된 바이트	uint64	연결 청크에서 받은 바이트 수입니다.
연결	uint32	5분 동안의 연결 수입니다.

수정 목록 데이터 블록

수정 목록 데이터 블록은 호스트에 적용되는 수정 사항을 전달합니다. 영향을 받는 호스트에 적용된 각 수정 사항에 대한 수정 목록 데이터 블록은 사용자 제품 데이터 블록에 포함됩니다. 계열 1 블록 그룹에서 수정 목록 데이터 블록의 블록 유형은 67입니다.

다음 다이어그램에 수정 목록 데이터 블록의 형식이 나와 있습니다.

다음 표에는 수정 목록 데이터 블록의 구성 요소에 대한 설명이 나와 있습니다.

표 4-57 수정 목록 데이터 블록 필드

필드	데이터 유형	설명
수정 목록 블록 유형	uint32	수정 목록 데이터 블록을 시작합니다. 이 값은 항상 67입니다.
수정 목록 블록 길이	uint32	수정 목록 데이터 블록의 총 바이트 수입니다. 여기에는 수정 목록 블록 유형 및 길이 필드의 8바이트에 그 뒤의 수정 ID 데이터 바이트 수를 더한 값이 포함됩니다.
수정 ID	uint32	수정 사항의 ID 번호입니다.

사용자 서버 데이터 블록

사용자 서버 데이터 블록은 사용자 입력 이벤트의 서버 세부사항을 포함합니다. 계열 1 블록 그룹에서 사용자 서버 데이터 블록의 블록 유형은 76입니다.

다음 다이어그램에 사용자 서버 데이터 블록의 기본 구조가 나와 있습니다.

다음 표에는 사용자 서버 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 4-58 사용자 서버 데이터 블록 필드

필드	바이트 수	설명
사용자 서버 데이터 블록 유형	uint32	사용자 서버 데이터 블록을 시작합니다. 이 값은 항상 76입니다.
사용자 서버 블록 길이	uint32	사용자 서버 데이터 블록의 총 바이트 수입니다. 여기에는 사용자 서버 블록 유형 및 길이 필드의 8바이트에 그 뒤의 사용자 서버 데이터 바이트 수를 더한 값이 포함됩니다.
일반 목록 블록 유형	uint32	일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	일반 목록 블록과 캡슐화된 데이터 블록의 바이트 수입니다. 이 수에는 일반 목록 블록 헤더 필드의 8바이트에 캡슐화된 모든 데이터 블록의 바이트 수를 더한 값이 포함됩니다.
IP 주소 범위 사양 데이터 블록	variable	캡슐화된 IP 주소 범위 사양 데이터 블록(목록 블록 길이의 최대 바이트 수까지)입니다.
포트	uint16	서버에서 사용하는 포트입니다.
프로토콜	uint16	IANA 프로토콜 번호 또는 이더 타입입니다. 이는 전송 계층 프로토콜과 네트워크 계층 프로토콜에서 서로 다르게 처리됩니다. 전송 계층 프로토콜은 IANA 프로토콜 번호로 식별됩니다. 예를 들면 다음과 같습니다. • 6 - TCP • 17 - UDP 네트워크 계층 프로토콜은 IEEE 등록 기관 이더 타입의 10진수 형식으로 식별됩니다. 예를 들면 다음과 같습니다. • 2048 - IP

사용자 서버 목록 데이터 블록

사용자 서버 목록 데이터 블록은 사용자 입력 이벤트의 서버 데이터 블록 목록을 포함합니다. 계열 1 블록 그룹에서 사용자 서버 목록 데이터 블록의 블록 유형은 77입니다. 다음 다이어그램에 사용자 서버 목록 데이터 블록의 기본 구조가 나와 있습니다.

다음 표에는 사용자 서버 목록 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 4-59 사용자 서버 목록 데이터 블록 필드

필드	바이트 수	설명
사용자 서버 목록 데이터 블록 유형	uint32	사용자 서버 목록 데이터 블록을 시작합니다. 이 값은 항상 77입니다.
사용자 서버 목록 블록 길이	uint32	사용자 서버 목록 데이터 블록의 총 바이트 수입니다. 여기에는 사용자 서버 목록 블록 유형 및 길이 필드의 8바이트에 그 뒤의 사용자 서버 목록 데이터 바이트 수를 더한 값이 포함됩니다.
소스 유형	uint32	데이터 소스의 유형에 매핑되는 번호입니다. • 0 - RNA에서 서버 데이터를 탐지한 경우 • 1 - 사용자가 서버 데이터를 제공한 경우 • 2 - 서드파티 스캐너에서 서버 데이터를 탐지한 경우 • 3 - nmimport.pl 등의 커맨드 라인 툴이나 호스트 입력 API 클라이언트에서 서버 데이터를 제공한 경우
소스 ID	uint32	서버 데이터 소스에 매핑되는 ID 번호입니다. 소스 유형에 따라 RNA, 사용자, 스캐너 또는 서드파티 애플리케이션에 매핑될 수 있습니다.
일반 목록 블록 유형	uint32	일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	일반 목록 블록과 캡슐화된 데이터 블록의 바이트 수입니다. 이 수에는 일반 목록 블록 헤더 필드의 8바이트에 캡슐화된 모든 데이터 블록의 바이트 수를 더한 값이 포함됩니다.
사용자 서버 데이터 블록	variable	캡슐화된 사용자 서버 데이터 블록(목록 블록 길이의 최대 바이트 수까지)입니다.

4.7 이상 버전용 사용자 호스트 데이터 블록

사용자 호스트 데이터 블록은 사용자가 호스트 추가 및 삭제 메시지, 4-56페이지에서 사용자 호스트 입력 이벤트의 호스트 범위 및 사용자/소스 ID 관련 정보를 포함하는 데 사용됩니다. 계열 1 블록 그룹에서 사용자 호스트 데이터 블록의 블록 유형은 78입니다.

다음 다이어그램에 사용자 호스트 데이터 블록의 기본 구조가 나와 있습니다.

다음 표에는 사용자 호스트 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 4-60 사용자 호스트 데이터 블록 필드

필드	바이트 수	설명
사용자 호스트 블록 유형	uint32	사용자 호스트 데이터 블록을 시작합니다. 이 값은 항상 78입니다.
사용자 호스트 블록 길이	uint32	사용자 호스트 데이터 블록의 총 바이트 수입니다. 여기에는 사용자 호스트 블록 유형 및 길이 필드의 8바이트에 그 뒤의 사용자 호스트 데이터 바이트 수를 더한 값이 포함됩니다.
일반 목록 블록 유형	uint32	IP 주소 범위 데이터를 전달하는 IP 범위 사양 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 IP 범위 사양 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
IP 범위 사양 데이터 블록*	variable	사용자 입력의 IP 주소 범위에 대한 정보가 포함된 IP 범위 사양 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.2 이상 버전용 IP 주소 범위 데이터 블록, 4-96페이지의 내용을 참조하십시오.

표 4-60 사용자 호스트 데이터 블록 필드 (계속)

필드	바이트 수	설명
일반 목록 블록 유형	uint32	MAC 주소 범위 데이터를 전달하는 MAC 범위 사양 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 MAC 범위 사양 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
MAC 범위 사양 데이터 블록*	variable	사용자 입력의 MAC 주소 범위에 대한 정보가 포함된 MAC 범위 사양 데이터 블록입니다. 이 데이터 블록에 대한 설명은 MAC 주소 사양 데이터 블록, 4-99페이지의 내용을 참조하십시오.
소스 ID	uint32	호스트 데이터를 추가했거나 업데이트한 소스에 매핑되는 ID 번호입니다. 소스 유형에 따라 RNA, 사용자, 스캐너 또는 서드파티 애플리케이션에 매핑될 수 있습니다.
소스 유형	uint32	데이터 소스의 유형에 매핑되는 번호입니다. • 0 - RNA에서 호스트 데이터를 탐지한 경우 • 1 - 사용자가 호스트 데이터를 제공한 경우 • 2 - 서드파티 스캐너에서 호스트 데이터를 탐지한 경우 • 3 - nmimport.pl 등의 커맨드 라인 툴이나 호스트 입력 API 클라이언트에서 호스트 데이터를 제공한 경우

4.7 이상 버전용 사용자 취약점 변경 데이터 블록

사용자 취약점 변경 데이터 블록에는 호스트에 대해 비활성화된 취약점 목록, 취약점을 비활성화한 사용자의 ID 번호, 취약점 변경 사항을 제공한 소스 관련 정보 및 임계성 값이 포함됩니다. 계열 1 블록 그룹에서 사용자 취약점 변경 데이터 블록의 블록 유형은 80입니다. 이전 사용자 취약점 변경 데이터 블록의 변경 사항에는 취약점 비활성화를 저장하기 위해 목록 데이터 블록 대신 일반 목록 데이터 블록을 사용했다는 정보와 새 소스 유형 필드가 포함됩니다. 이 데이터 블록은 4.6.1 이상 버전용 취약점 사용자 설정 메시지, 4-55페이지에 설명되어 있는 사용자 취약점 변경 메시지에 사용됩니다.

다음 다이어그램에 사용자 취약점 변경 데이터 블록의 기본 구조가 나와 있습니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
취약점 확인 응답 블록	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
	사용자 취약점 데이터 블록...*																															

다음 표에는 일반 목록 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 4-61 사용자 취약점 변경 데이터 블록 필드

필드	바이트 수	설명
사용자 취약점 변경 데이터 블록 유형	uint32	사용자 취약점 변경 데이터 블록을 시작합니다. 이 값은 항상 80입니다.
사용자 취약점 변경 블록 길이	uint32	사용자 취약점 변경 데이터 블록의 총 바이트 수입니다. 여기에는 호스트 취약점 블록 유형 및 길이 필드의 8바이트에 그 뒤의 호스트 취약점 데이터 바이트 수를 더한 값이 포함됩니다.
소스 ID	uint32	호스트 취약점 변경 값을 업데이트했거나 추가한 소스에 매핑되는 ID 번호입니다. 소스 유형에 따라 RNA, 사용자, 스캐너 또는 서드파티 애플리케이션에 매핑될 수 있습니다.
소스 유형	uint32	데이터 소스의 유형에 매핑되는 번호입니다. • 0 - RNA에서 호스트 취약점 데이터를 탐지한 경우 • 1 - 사용자가 호스트 취약점 데이터를 제공한 경우 • 2 - 서드파티 스캐너에서 호스트 취약점 데이터를 탐지한 경우 • 3 - nmimport.pl 등의 커맨드 라인 툴이나 호스트 입력 API 클라이언트에서 호스트 취약점 데이터를 제공한 경우
유형	uint32	취약점의 유형입니다.
일반 목록 블록 유형	uint32	일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	일반 목록 블록과 캡슐화된 데이터 블록의 바이트 수입니다. 이 수에는 일반 목록 블록 헤더 필드의 8바이트에 캡슐화된 모든 데이터 블록의 바이트 수를 더한 값이 포함됩니다.
사용자 취약점 데이터 블록	variable	캡슐화된 사용자 취약점 데이터 블록(목록 블록 길이의 최대 바이트 수까지)입니다. 자세한 정보는 5.0 이상 버전용 사용자 취약점 데이터 블록, 4-158페이지의 내용을 참조하십시오.

4.7 이상 버전용 사용자 임계성 변경 데이터 블록

사용자 임계성 데이터 블록은 호스트 임계성이 변경된 호스트의 IP 주소 범위 사양 목록, 임계성 값을 업데이트한 사용자의 ID 번호, 임계성 값을 제공한 소스에 대한 정보 및 임계성 값을 포함하는 데 사용됩니다. 계열 1 블록 그룹에서 사용자 임계성 데이터 블록의 블록 유형은 81입니다. 이전 사용자 임계성 데이터 블록의 변경 사항에는 IP 주소를 저장하기 위해 목록 데이터 블록 대신 일반 목록 데이터 블록을 사용했다는 정보와 새 소스 유형 필드가 포함됩니다.

사용자 임계성 데이터 블록은 호스트 임계성 사용자 설정 메시지, 4-57페이지에 설명되어 있는 호스트 임계성 사용자 설정 메시지에 사용됩니다.

다음 다이어그램에 사용자 임계성 데이터 블록의 기본 구조가 나와 있습니다.

다음 표에는 사용자 임계성 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 4-62 사용자 임계성 데이터 블록 필드

필드	바이트 수	설명
사용자 임계성 데이터 블록 유형	uint32	사용자 임계성 데이터 블록을 시작합니다. 이 값은 항상 81입니다.
사용자 임계성 블록 길이	uint32	사용자 임계성 데이터 블록의 총 바이트 수입니다. 여기에는 사용자 임계성 블록 유형 및 길이 필드의 8바이트에 그 뒤의 사용자 임계성 데이터 바이트 수를 더한 값이 포함됩니다.
일반 목록 블록 유형	uint32	일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	일반 목록 블록과 캡슐화된 데이터 블록의 바이트 수입니다. 이 수에는 일반 목록 블록 헤더 필드의 8바이트에 캡슐화된 모든 데이터 블록의 바이트 수를 더한 값이 포함됩니다.
IP 주소 범위 사양 데이터 블록	variable	캡슐화된 IP 주소 범위 사양 데이터 블록(목록 블록 길이의 최대 바이트 수까지)입니다.

표 4-62 사용자 임계성 데이터 블록 필드 (계속)

필드	바이트 수	설명
소스 ID	uint32	사용자 임계성 값을 업데이트했거나 추가한 소스에 매핑되는 ID 번호입니다. 소스 유형에 따라 RNA, 사용자, 스캐너 또는 서드파티 애플리케이션에 매핑될 수 있습니다.
소스 유형	uint32	데이터 소스의 유형에 매핑되는 번호입니다. • 0 - RNA에서 사용자 임계성 값을 제공한 경우 • 1 - 사용자가 사용자 임계성 값을 제공한 경우 • 2 - 서드파티 스캐너가 사용자 임계성 값을 제공한 경우 • 3 - nmimport.pl 등의 커맨드 라인 툴이나 호스트 입력 API 클라이언트에서 사용자 임계성 값을 제공한 경우
임계성 값	uint32	사용자 임계성 값입니다.

4.7 이상 버전용 사용자 속성값 데이터 블록

사용자 속성값 데이터 블록에는 속성값이 변경된 호스트를 나타내는 IP 주소 범위 목록이 포함되며 속성값을 추가한 사용자의 ID 번호, 속성값을 제공한 소스 관련 정보, 속성값이 포함된 BLOB 데이터 블록도 함께 포함됩니다. 계열 1 블록 그룹에서 사용자 속성값 데이터 블록의 블록 유형은 82입니다. 이전 사용자 속성값 데이터 블록의 변경 사항에는 IP 주소를 저장하기 위해 목록 데이터 블록 대신 일반 목록 데이터 블록을 사용했다는 정보와 새 소스 유형 필드가 포함됩니다.

다음 다이어그램에 사용자 속성값 데이터 블록의 구조가 나와 있습니다.

다음 표에는 사용자 속성값 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 4-63 사용자 속성값 데이터 블록 필드

필드	바이트 수	설명
사용자 속성값 데이터 블록 유형	uint32	사용자 속성값 데이터 블록을 시작합니다. 이 값은 항상 82입니다.
사용자 속성값 블록 길이	uint32	속성값 데이터 블록의 총 바이트 수입니다. 여기에는 사용자 속성값 블록 유형 및 길이 필드의 8바이트에 그 뒤의 사용자 속성값 데이터 바이트 수를 더한 값이 포함됩니다.
일반 목록 블록 유형	uint32	일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	일반 목록 블록과 캡슐화된 데이터 블록의 바이트 수입니다. 이 수에는 일반 목록 블록 헤더 필드의 8바이트에 캡슐화된 모든 데이터 블록의 바이트 수를 더한 값이 포함됩니다.
IP 주소 범위 사양 데이터 블록	variable	각각 시작 IP 주소와 끝 IP 주소가 있는 IP 주소 범위 사양 데이터 블록(목록 블록 길이의 최대 바이트 수까지)입니다.
소스 ID	uint32	속성 데이터를 추가했거나 업데이트한 소스에 매핑되는 ID 번호입니다. 소스 유형에 따라 RNA, 사용자, 스캐너 또는 서드파티 애플리케이션에 매핑될 수 있습니다.
소스 유형	uint32	데이터 소스의 유형에 매핑되는 번호입니다. • 0 - RNA에서 사용자 속성값을 제공한 경우 • 1 - 사용자가 사용자 속성값을 제공한 경우 • 2 - 서드파티 스캐너가 사용자 속성값을 제공한 경우 • 3 - nmimport.pl 등의 커맨드 라인 툴이나 호스트 입력 API 클라이언트에서 사용자 속성값을 제공한 경우
속성 ID	uint32	업데이트된 속성의 ID 번호입니다.
BLOB 블록 유형	uint32	BLOB 데이터 블록을 시작합니다. 이 값은 항상 10입니다.
BLOB 블록 길이	uint32	BLOB 데이터 블록의 바이트 수입니다. 여기에는 BLOB 블록 유형 및 길이 필드의 8바이트에 그 뒤의 이진 데이터 길이를 더한 값이 포함됩니다.
값	variable	이진 형식의 사용자 속성값을 포함합니다.

4.7 이상 버전용 사용자 프로토콜 목록 데이터 블록

사용자 프로토콜 목록 데이터 블록은 프로토콜 데이터의 소스 관련 정보, 데이터를 추가한 사용자의 ID 번호 및 사용자 프로토콜 데이터 블록 목록을 포함하는 데 사용됩니다. 계열 1 블록 그룹에서 사용자 프로토콜 목록 데이터 블록의 블록 유형은 83입니다. 사용자 프로토콜 데이터 블록에 대한 자세한 정보는 사용자 프로토콜 데이터 블록, 4-92페이지의 내용을 참조하십시오.

사용자 프로토콜 목록 데이터 블록은 사용자 프로토콜 메시지, 4-59페이지에 설명되어 있는 사용자 프로토콜 메시지에 사용됩니다.

다음 다이어그램에 사용자 프로토콜 목록 데이터 블록의 기본 구조가 나와 있습니다.

다음 표에는 일반 목록 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 4-64 사용자 프로토콜 목록 데이터 블록 필드

필드	바이트 수	설명
사용자 프로토콜 목록 블록 유형	uint32	사용자 프로토콜 목록 데이터 블록을 시작합니다. 이 값은 항상 `83`입니다.
사용자 프로토콜 목록 블록 길이	uint32	사용자 프로토콜 목록 데이터 블록의 총 바이트 수입니다. 여기에는 사용자 프로토콜 목록 블록 유형 및 길이 필드의 8바이트에 그 뒤의 사용자 프로토콜 목록 데이터 바이트 수를 더한 값이 포함됩니다.
소스 유형	uint32	데이터 소스의 유형에 매핑되는 번호입니다. • `0` - RNA에서 프로토콜 데이터를 제공한 경우 • `1` - 사용자가 프로토콜 데이터를 제공한 경우 • `2` - 서드파티 스캐너에서 프로토콜 데이터를 제공한 경우 • `3` - `nmimport.pl` 등의 커맨드 라인 툴이나 호스트 입력 API 클라이언트에서 프로토콜 데이터를 제공한 경우

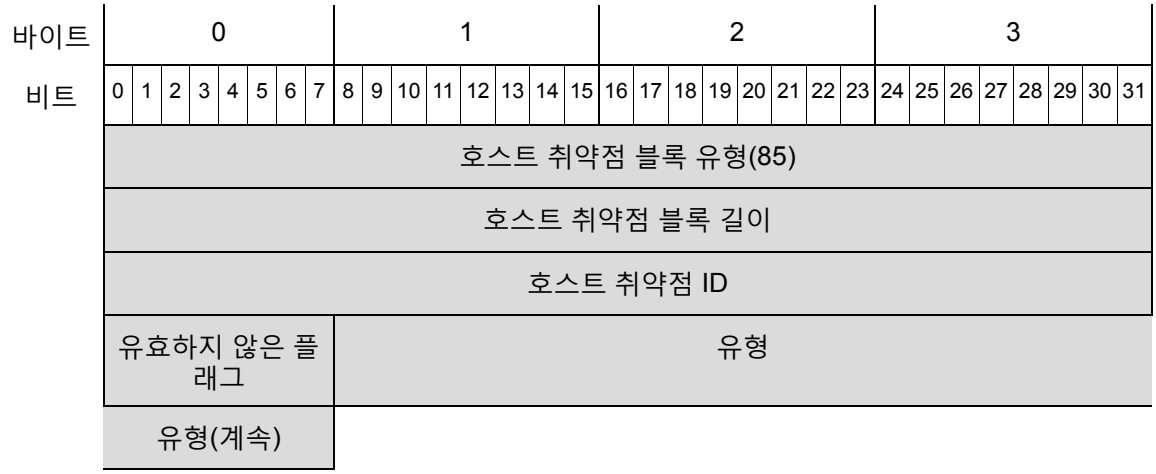
표 4-64 사용자 프로토콜 목록 데이터 블록 필드 (계속)

필드	바이트 수	설명
소스 ID	uint32	영향을 받는 프로토콜의 소스에 매핑되는 ID 번호입니다. 소스 유형에 따라 RNA, 사용자, 스캐너 또는 서드파티 애플리케이션에 매핑될 수 있습니다.
일반 목록 블록 유형	uint32	일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	일반 목록 블록과 캡슐화된 데이터 블록의 바이트 수입니다. 이 수에는 일반 목록 블록 헤더 필드의 8바이트에 캡슐화된 모든 데이터 블록의 바이트 수를 더한 값이 포함됩니다.
사용자 프로토콜 데이터 블록	variable	캡슐화된 사용자 프로토콜 데이터 블록(목록 블록 길이의 최대 바이트 수까지)입니다.

4.9.0 이상 버전용 호스트 취약점 데이터 블록

호스트 취약점 데이터 블록은 호스트에 적용되는 취약점을 전달합니다. 각 호스트 취약점 데이터 블록은 이벤트에 포함된 호스트에 대한 취약점 하나를 설명합니다. 호스트 취약점 데이터 블록은 전체 호스트 프로파일, 전체 호스트 서버 및 전체 하위 서버 데이터 블록에 표시됩니다. 계열 1 블록 그룹에서 호스트 취약점 데이터 블록의 블록 유형은 85입니다.

다음 다이어그램에 호스트 취약점 데이터 블록의 형식이 나와 있습니다.



다음 표에는 호스트 취약점 데이터 블록의 구성 요소에 대한 설명이 나와 있습니다.

표 4-65 호스트 취약점 데이터 블록 필드

필드	데이터 유형	설명
호스트 취약점 블록 유형	uint32	호스트 취약점 데이터 블록을 시작합니다. 이 값은 항상 85입니다.
호스트 취약점 블록 길이	uint32	호스트 취약점 데이터 블록의 총 바이트 수입니다. 여기에는 호스트 취약점 블록 유형 및 길이 필드의 8바이트에 그 뒤의 호스트 취약점 데이터 바이트 수를 더한 값이 포함됩니다.

표 4-65 호스트 취약점 데이터 블록 필드 (계속)

필드	데이터 유형	설명
호스트 취약점 ID	uint32	취약점의 ID 번호입니다.
유효하지 않은 플래그	uint8	취약점이 호스트에 유효한지를 나타내는 값입니다.
유형	uint32	취약점의 유형입니다.

ID 데이터 블록

계열 1 블록 그룹에서 ID 데이터 블록의 블록 유형은 94입니다. ID 데이터 블록은 운영 체제 또는 서버 핑거프린트 소스의 ID가 충돌하거나 시간이 초과되었음을 나타내는 ID 충돌 및 ID 시간 초과 메시지에서 사용됩니다. 해당 데이터 블록은 보고된 ID, 즉 활성 소스 ID(사용자, 스캐너 또는 애플리케이션)와 충돌하는 것으로 식별된 ID를 설명합니다. 자세한 정보는 ID 충돌 및 ID 시간 초과 시스템 메시지, 4-61페이지의 내용을 참조하십시오.

다음 다이어그램에 4.9 이상 버전의 ID 데이터 블록 형식이 나와 있습니다.

다음 표에는 Cisco ID 데이터 블록의 필드에 대한 설명이 나와 있습니다.

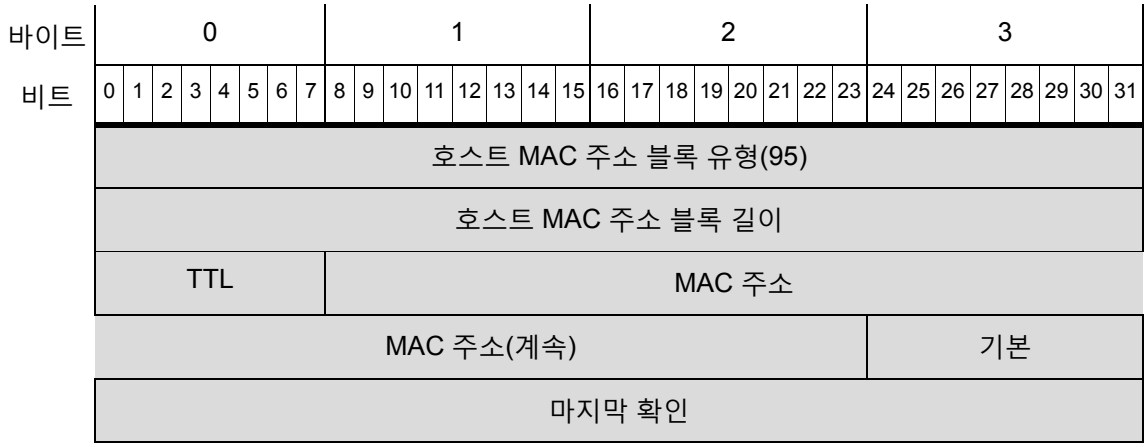
표 4-66 ID 데이터 블록 필드

필드	데이터 유형	설명
ID 데이터 블록 유형	uint32	ID 데이터 블록을 시작합니다. 이 값은 항상 94입니다.
ID 데이터 블록 길이	uint32	ID 데이터 블록의 바이트 수입니다. 이 값은 항상 40(데이터 블록 유형 및 길이 필드와 소스 유형 및 ID 필드의 16바이트 + 핑거프린트 UUID 값의 16바이트 + 포트의 2바이트 + 프로토콜의 2바이트 + SM ID의 4바이트)이어야 합니다.
ID 데이터 소스 유형	uint32	데이터 소스의 유형에 매핑되는 번호입니다. • 0 - RNA에서 핑거프린트 데이터를 제공한 경우 • 1 - 사용자가 핑거프린트 데이터를 제공한 경우 • 2 - 서드파티 스캐너에서 핑거프린트 데이터를 제공한 경우 • 3 - nmimport.pl 등의 커맨드 라인 툴이나 호스트 입력 API 클라이언트에서 핑거프린트 데이터를 제공한 경우
ID 데이터 소스 ID	uint32	핑거프린트 데이터 소스에 매핑되는 ID 번호입니다. 소스 유형에 따라 RNA, 사용자, 스캐너 또는 서드파티 애플리케이션에 매핑될 수 있습니다.
UUID	uint8[16]	ID가 운영 체제 ID인 경우 핑거프린트의 고유 식별자로 사용되는 옥텟 형식의 ID 번호입니다.
포트	uint16	ID가 서버 ID인 경우 서버 데이터가 포함된 패킷에 사용되는 포트를 나타냅니다.
프로토콜	uint16	ID가 서버 ID인 경우 서버 데이터가 포함된 패킷에 사용되는 이더 타입이나 네트워크 프로토콜의 IANA 번호를 나타냅니다. 이는 전송 계층 프로토콜과 네트워크 계층 프로토콜에서 서로 다르게 처리됩니다. 전송 계층 프로토콜은 IANA 프로토콜 번호로 식별됩니다. 예를 들면 다음과 같습니다. • 6 - TCP • 7 - UDP 네트워크 계층 프로토콜은 IEEE 등록 기관 이더 타입의 10진수 형식으로 식별됩니다. 예를 들면 다음과 같습니다. • 2048 - IP
서버 맵 ID	uint32	ID가 서버 ID인 경우 서버의 ID, 벤더, 버전 조합을 표시하는 서버 맵 ID를 나타냅니다.

4.9 이상 버전용 호스트 MAC 주소

계열 1 블록 그룹에서 호스트 MAC 주소 데이터 블록의 블록 유형은 95입니다. 이 블록에는 호스트 데이터의 TTL(Time to Live) 값과 MAC 주소, 호스트의 기본 서브넷 및 호스트의 마지막 확인 값이 포함됩니다.

다음 다이어그램에 4.9 이상 버전의 호스트 MAC 주소 데이터 블록 형식이 나와 있습니다.



다음 표에는 호스트 MAC 주소 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 4-67 호스트 MAC 주소 데이터 블록 필드

필드	데이터 유형	설명
호스트 MAC 주소 데이터 블록 유형	uint32	호스트 MAC 주소 데이터 블록을 시작합니다. 이 값은 항상 95입니다.
호스트 MAC 주소 데이터 블록 길이	uint32	호스트 MAC 주소 데이터 블록의 바이트 수입니다. 이 값은 항상 20(데이터 블록 유형 및 길이 필드의 8바이트 + TTL 값의 1바이트 + MAC 주소의 6바이트 + 기본 서브넷의 1바이트 + 마지막 확인 값의 4바이트)이어야 합니다.
TTL	uint8	호스트 핑거프린트를 생성하는 데 사용되는 패킷의 TTL 값 간 차이를 나타냅니다.
MAC 주소	uint8 [6]	호스트의 MAC 주소를 나타냅니다.
기본	uint8	호스트의 기본 서브넷을 나타냅니다.
마지막 확인	uint32	트래픽에서 호스트가 마지막으로 확인된 시간을 나타냅니다.

보조 호스트 업데이트

보조 호스트 업데이트 데이터 블록은 호스트가 있는 서브넷이 아닌 다른 서브넷을 모니터링하는 디바이스에서 보조 호스트 업데이트로 전송된 호스트에 대한 정보를 포함합니다. 이 블록은 보조 업데이트 변경 이벤트(이벤트 유형 1001, 하위 유형 31) 내에서 사용됩니다. 계열 1 블록 그룹에서 보조 호스트 업데이트 데이터 블록의 블록 유형은 96입니다.

다음 다이어그램에 보조 호스트 업데이트 데이터 블록의 형식이 나와 있습니다.

다음 표에는 보조 호스트 업데이트 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 4-68 보조 호스트 업데이트 데이터 블록 필드

필드	데이터 유형	설명
보조 호스트 업데이트 블록 유형	uint32	보조 호스트 업데이트 데이터 블록을 시작합니다. 이 값은 항상 96입니다.
보조 호스트 업데이트 블록 길이	uint32	보조 호스트 업데이트 데이터 블록의 바이트 수입니다. 여기에는 보조 호스트 업데이트 블록 유형 및 길이 필드의 8바이트에 그 뒤의 보조 호스트 업데이트 데이터 바이트 수를 더한 값이 포함됩니다.
IP 주소	uint8[4]	업데이트에서 설명하는 호스트의 IP 주소(IP 주소 옥텟 형식)입니다.
목록 블록 유형	uint32	호스트 MAC 주소 데이터를 전달하는 호스트 MAC 주소 데이터 블록으로 구성된 목록 데이터 블록을 시작합니다. 이 값은 항상 11입니다.

표 4-68 보조 호스트 업데이트 데이터 블록 필드 (계속)

필드	데이터 유형	설명
목록 블록 길이	uint32	목록의 바이트 수입니다. 이 수에는 목록 블록 유형 및 길이 필드의 8바이트에 캡슐화된 모든 호스트 MAC 주소 데이터 블록을 더한 값이 포함됩니다. 이 필드 뒤에는 호스트 MAC 주소 데이터 블록이 없을 수도 있고 하나 이상 올 수도 있습니다.
호스트 MAC 주소 블록 유형	uint32	보조 호스트를 설명하는 호스트 MAC 주소 데이터 블록을 시작합니다. 이 값은 항상 95입니다.
호스트 MAC 주소 데이터 블록 길이	uint32	호스트 MAC 주소 데이터 블록의 바이트 수입니다. 이 값은 항상 20(데이터 블록 유형 및 길이 필드의 8바이트 + TTL 값의 1바이트 + MAC 주소의 6바이트 + 기본 서브넷의 1바이트 + 마지막 확인 값의 4바이트)이어야 합니다.
호스트 MAC 주소 데이터 블록	string	업데이트의 호스트 MAC 주소 관련 정보입니다.

5.0 이상 버전용 웹 애플리케이션 데이터 블록

계열 1 블록 그룹에서 5.0 이상 버전용 웹 애플리케이션 데이터 블록의 블록 유형은 123입니다. 이 데이터 블록은 탐지된 HTTP 클라이언트 요청의 웹 애플리케이션을 설명합니다.

다음 다이어그램에 5.0 이상 버전의 웹 애플리케이션 데이터 블록 형식이 나와 있습니다.

다음 표에는 웹 애플리케이션 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 4-69 웹 애플리케이션 데이터 블록 필드

필드	데이터 유형	설명
웹 애플리케이션 데이터 블록 유형	uint32	웹 애플리케이션 데이터 블록을 시작합니다. 이 값은 항상 123입니다.
웹 애플리케이션 데이터 블록 길이	uint32	웹 애플리케이션 데이터 블록의 바이트 수입니다. 여기에는 웹 애플리케이션 데이터 블록 유형 및 길이의 8바이트에 그 뒤의 애플리케이션 ID 필드 바이트 수를 더한 값이 포함됩니다.
애플리케이션 ID	uint32	웹 애플리케이션의 애플리케이션 ID입니다.

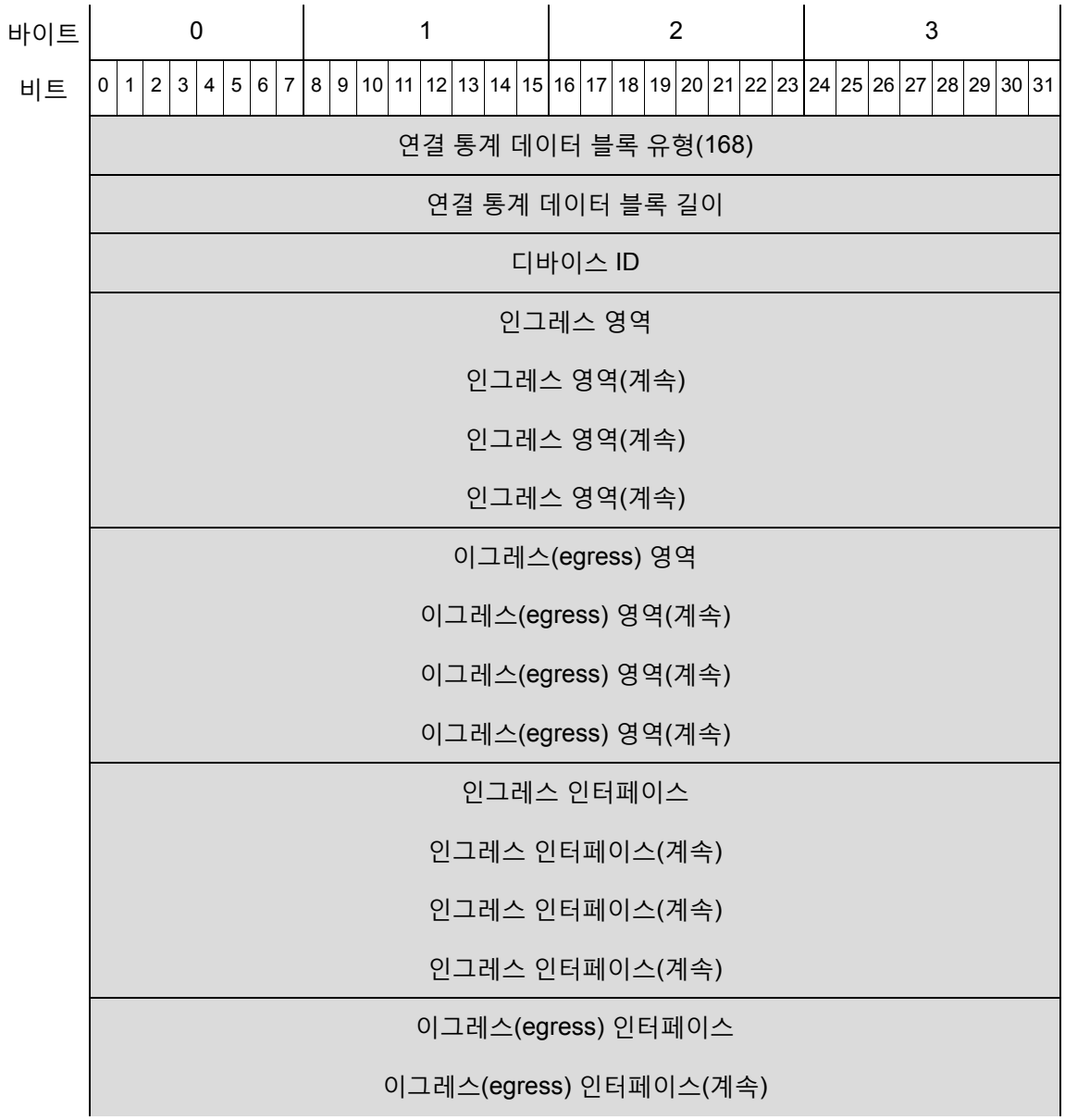
6.2 이상 버전용 연결 통계 데이터 블록

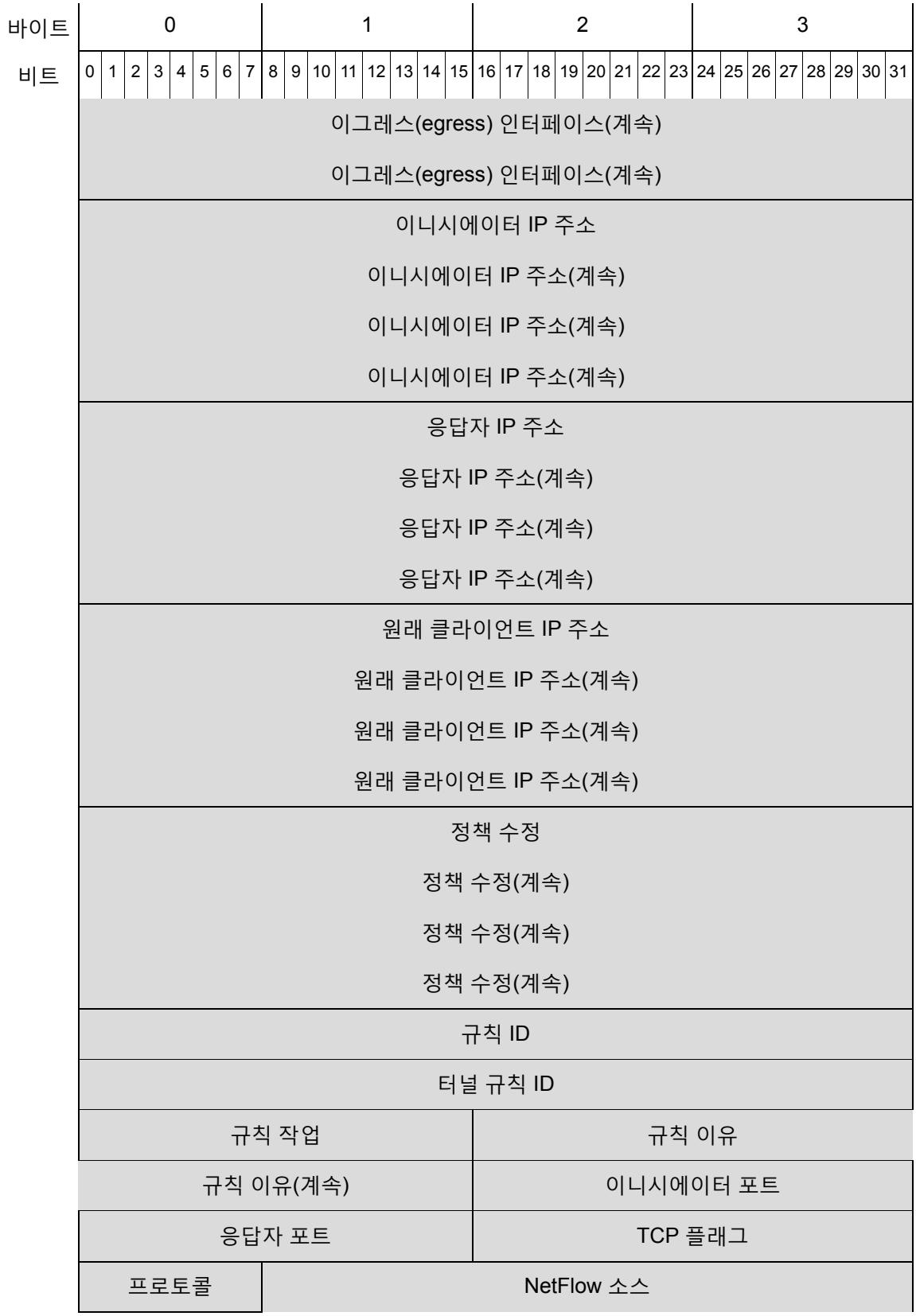
연결 통계 데이터 블록은 연결 데이터 메시지에 사용됩니다. 6.2 이상 버전용 연결 통계 데이터 블록에는 세 번째 Security Intelligence(보안 인텔리전스) 필드가 추가되었습니다. 계열 1 블록 그룹에서 6.2 이상 버전용 연결 통계 데이터 블록의 블록 유형은 168입니다. 이는 블록 유형 163(6.1.x 버전용 연결 통계 데이터 블록, B-209페이지)을 대체합니다.

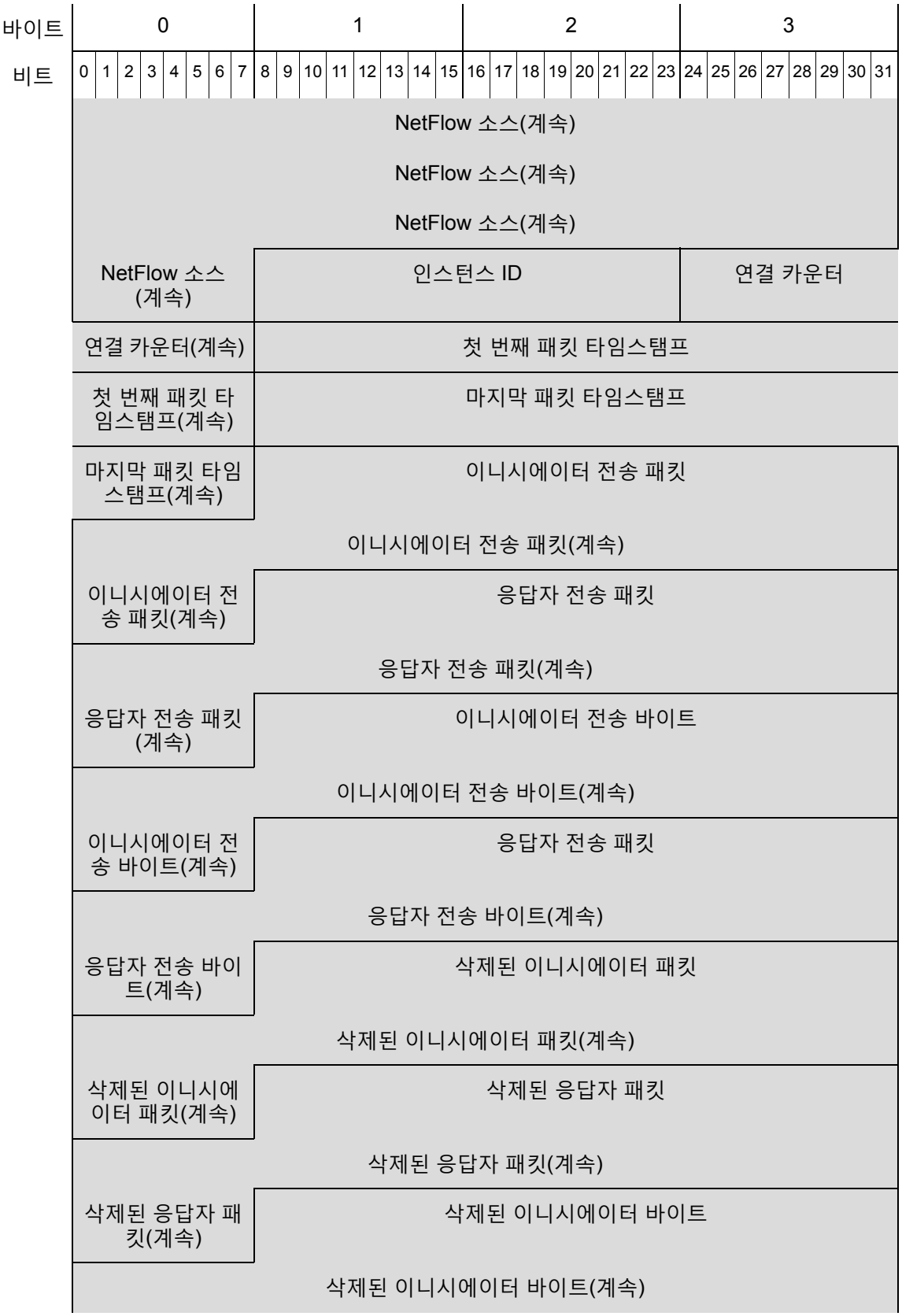
이벤트 버전이 13이고 이벤트 코드가 71인 요청 메시지에서 확장 이벤트 플래그(Request Flags(요청 플래그) 필드의 비트 30)를 설정하여 연결 이벤트 레코드를 요청합니다. 요청 플래그, 2-12페이지의 내용을 참조하십시오. 비트 23을 활성화하면 레코드에 확장 이벤트 헤더가 포함됩니다.

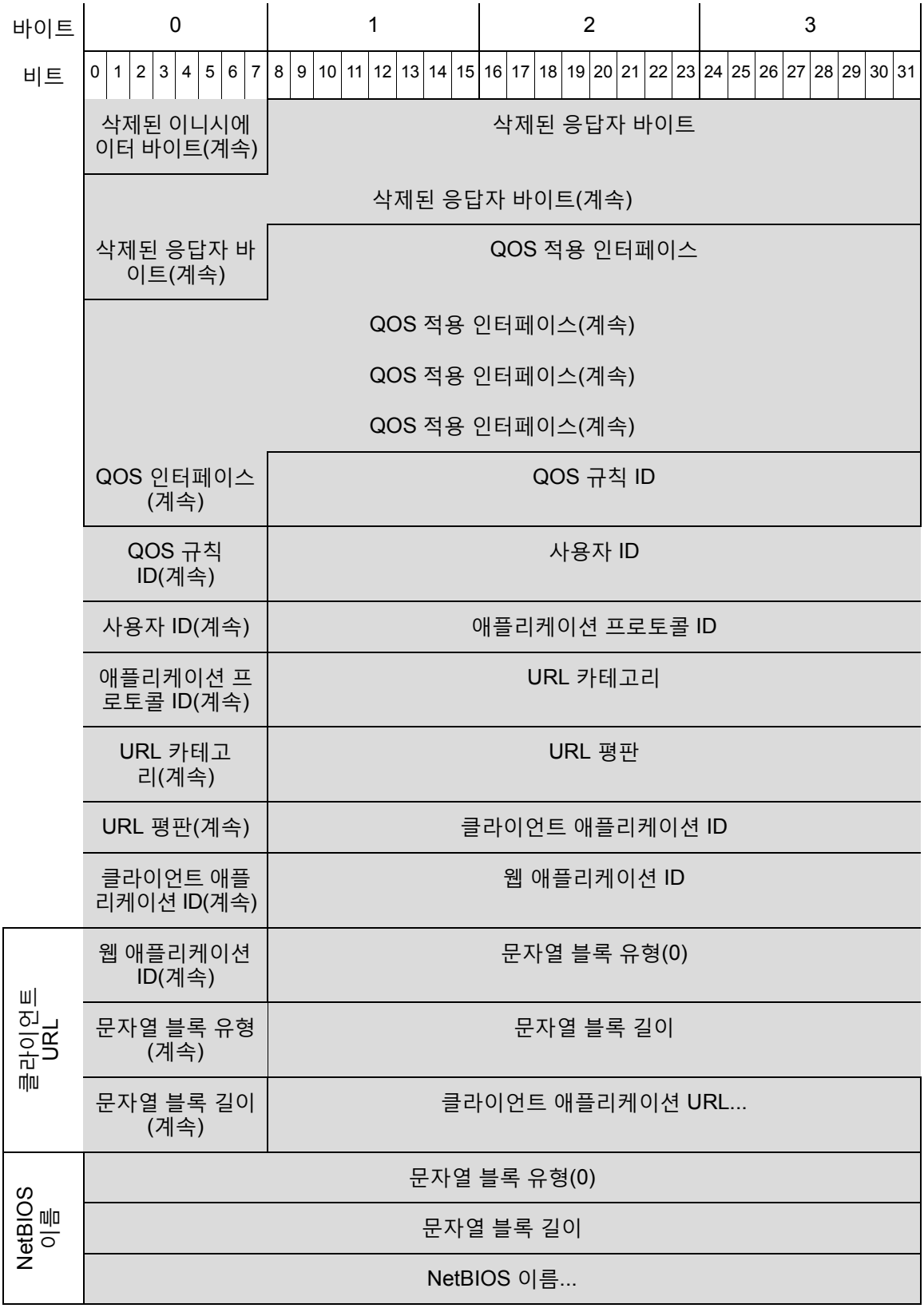
연결 통계 데이터 메시지에 대한 자세한 정보는 연결 통계 데이터 메시지, 4-54페이지의 내용을 참조하십시오.

다음 다이어그램에 6.2 이상 버전의 연결 통계 데이터 블록 형식이 나와 있습니다.

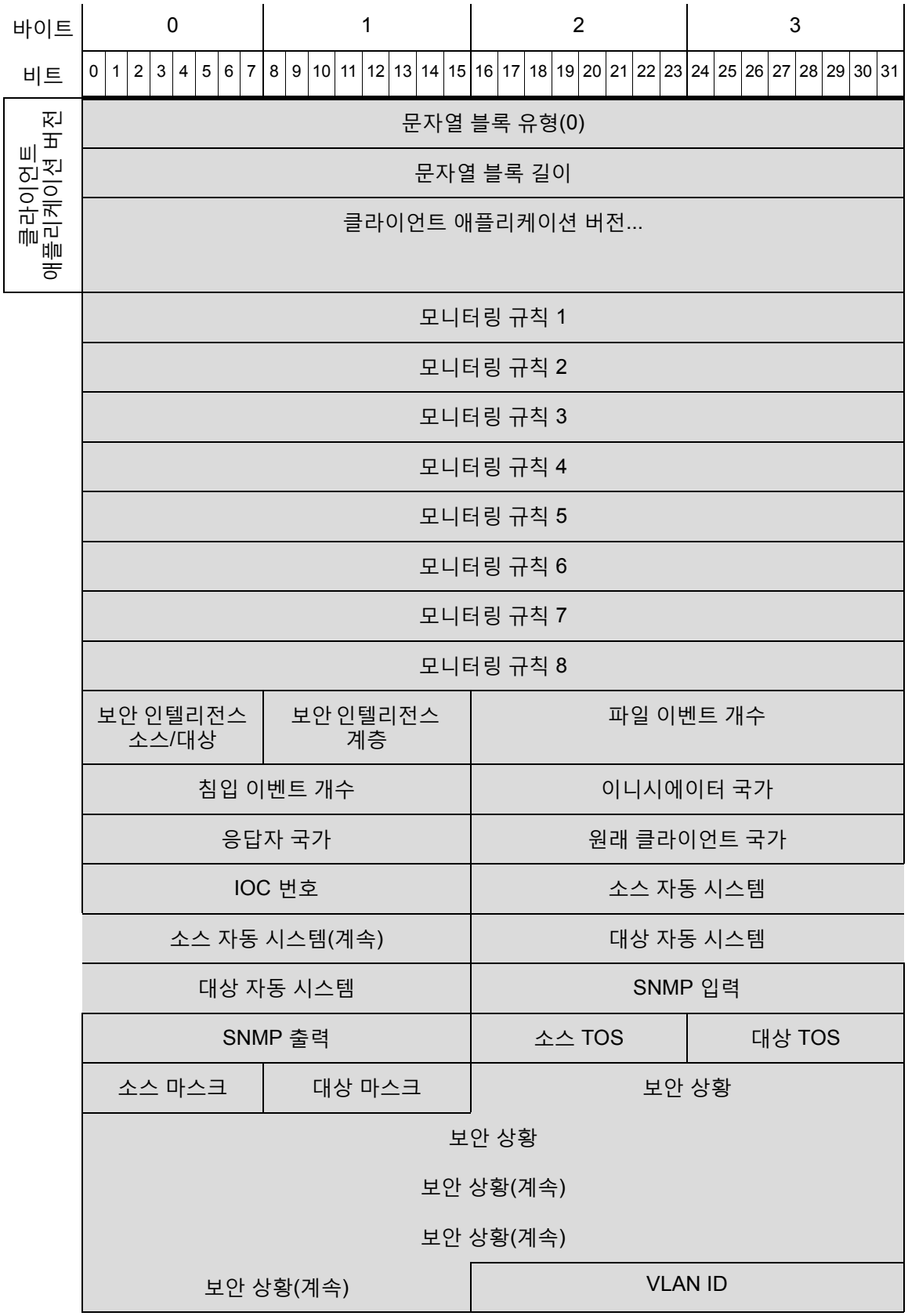


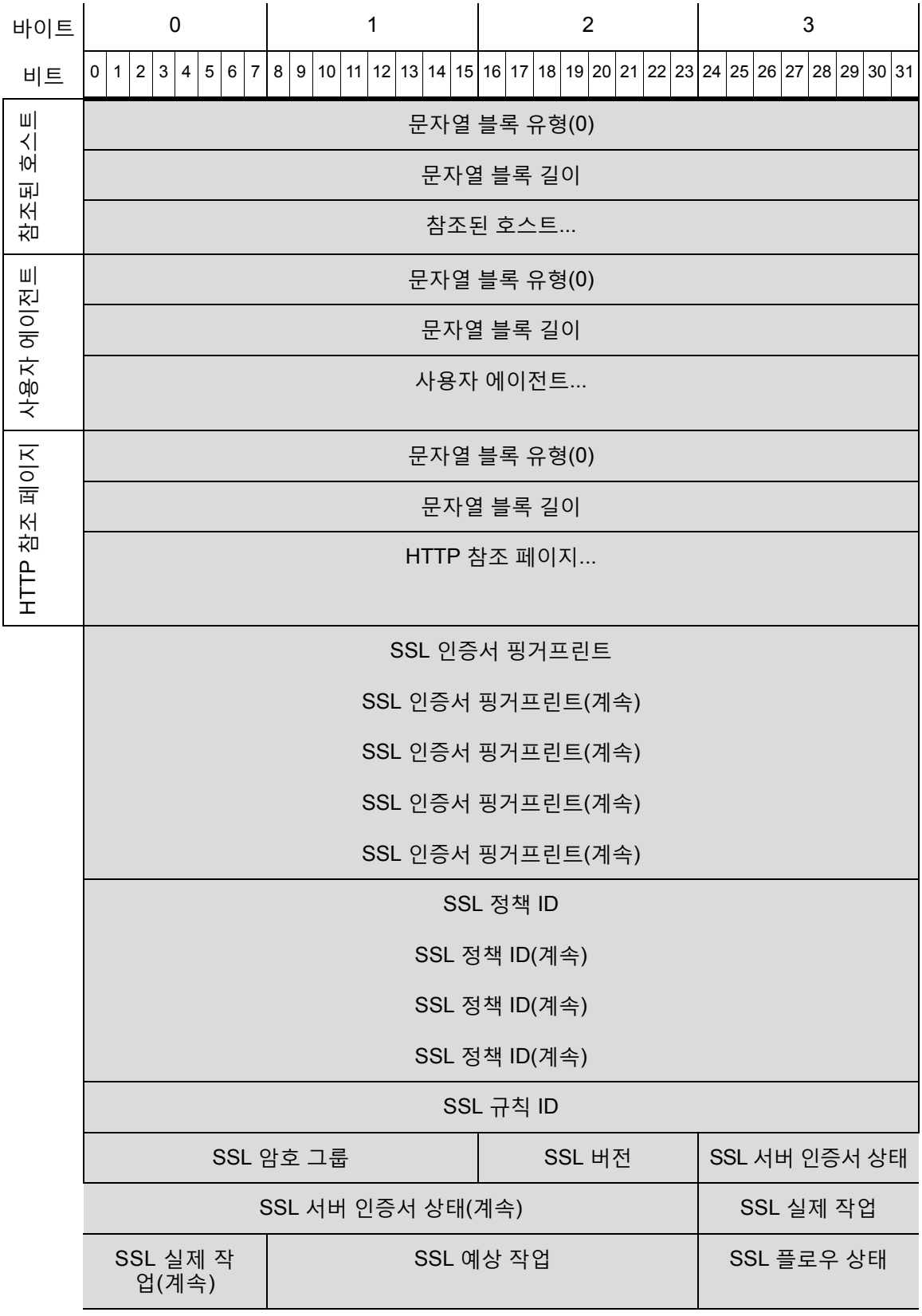

바이트
0
1
2
3
비트
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
이그레스(egress) 인터페이스(계속)
이그레스(egress) 인터페이스(계속)
이니시에이터 IP 주소
이니시에이터 IP 주소(계속)
이니시에이터 IP 주소(계속)
이니시에이터 IP 주소(계속)
응답자 IP 주소
응답자 IP 주소(계속)
응답자 IP 주소(계속)
응답자 IP 주소(계속)
원래 클라이언트 IP 주소
원래 클라이언트 IP 주소(계속)
원래 클라이언트 IP 주소(계속)
원래 클라이언트 IP 주소(계속)
정책 수정
정책 수정(계속)
정책 수정(계속)
정책 수정(계속)
규칙 ID
터널 규칙 ID
규칙 작업
규칙 이유
규칙 이유(계속)
이니시에이터 포트
응답자 포트
TCP 플래그
프로토콜
NetFlow 소스


바이트
0
1
2
3
비트
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
NetFlow 소스(계속)
NetFlow 소스(계속)
NetFlow 소스(계속)
NetFlow 소스 (계속)
인스턴스 ID
연결 카운터
연결 카운터(계속)
첫 번째 패킷 타임스탬프
첫 번째 패킷 타임스탬프(계속)
마지막 패킷 타임스탬프
마지막 패킷 타임스탬프(계속)
이니시에이터 전송 패킷
이니시에이터 전송 패킷(계속)
이니시에이터 전송 패킷(계속)
응답자 전송 패킷
응답자 전송 패킷(계속)
응답자 전송 패킷 (계속)
이니시에이터 전송 바이트
이니시에이터 전송 바이트(계속)
이니시에이터 전송 바이트(계속)
응답자 전송 패킷
응답자 전송 바이트(계속)
응답자 전송 바이트(계속)
삭제된 이니시에이터 패킷
삭제된 이니시에이터 패킷(계속)
삭제된 이니시에이터 패킷(계속)
삭제된 응답자 패킷
삭제된 응답자 패킷(계속)
삭제된 응답자 패킷(계속)
삭제된 이니시에이터 바이트
삭제된 이니시에이터 바이트(계속)

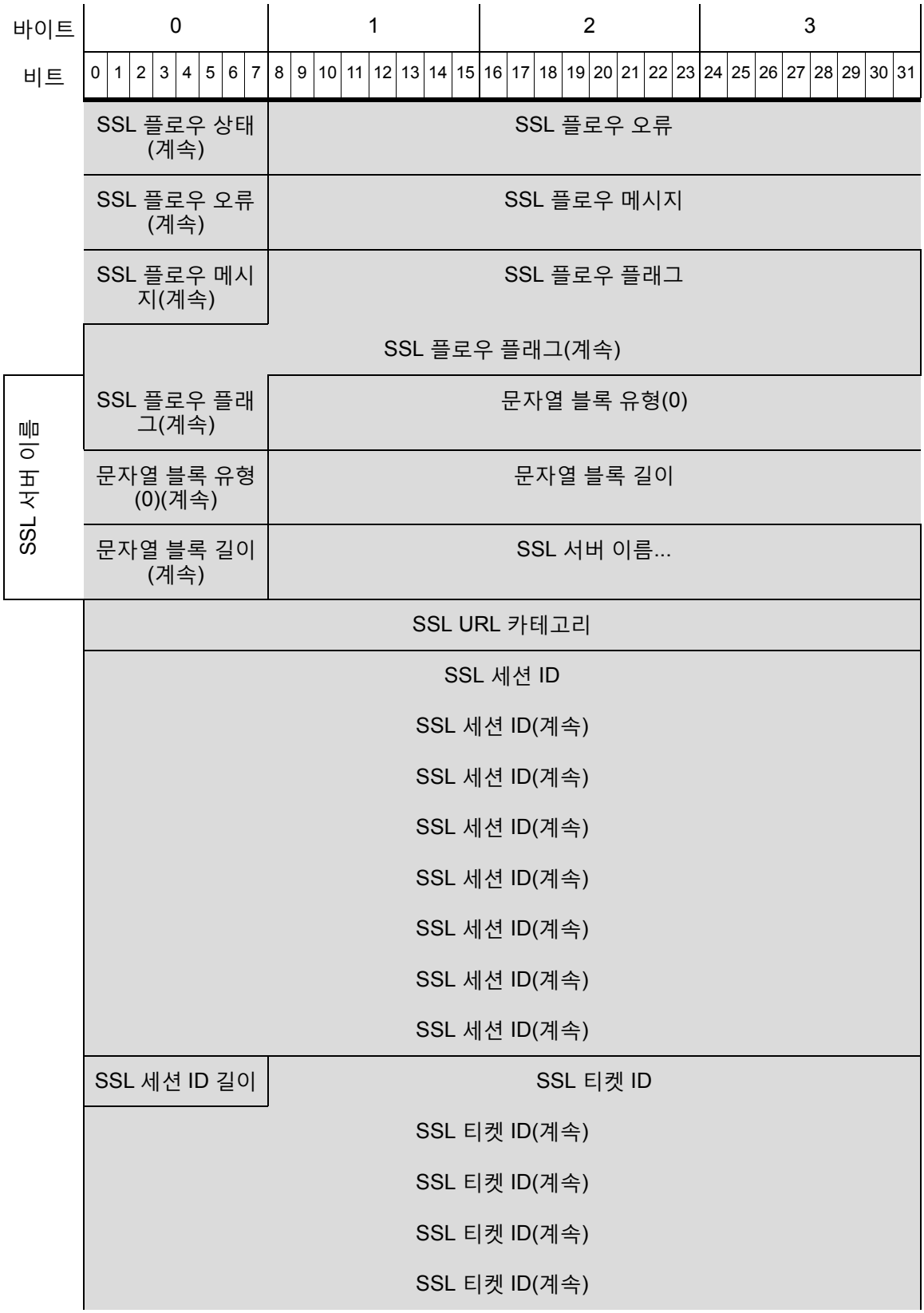


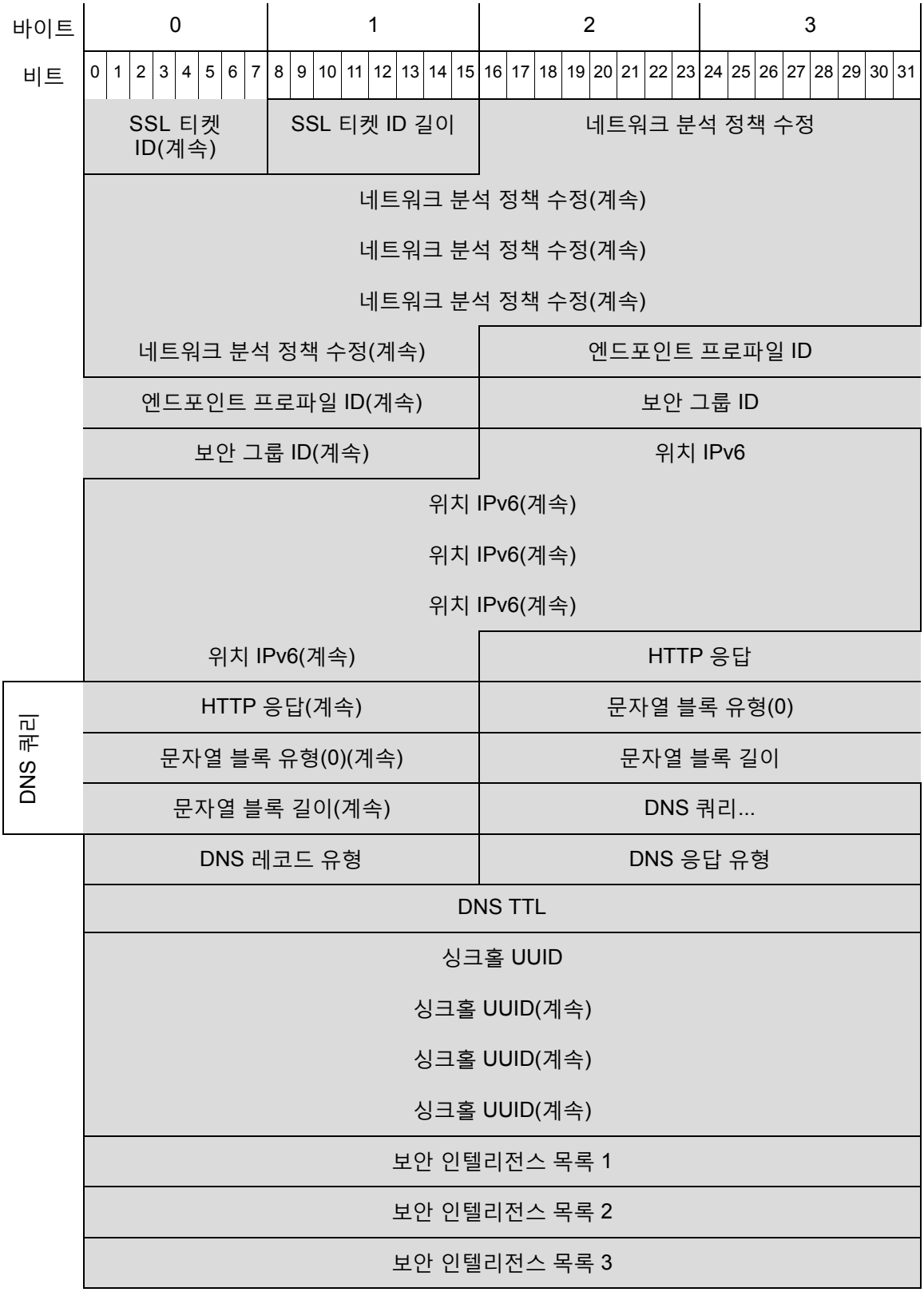
바이트	0				1				2				3			
비트	0 1 2 3 4 5 6 7				8 9 10 11 12 13 14 15				16 17 18 19 20 21 22 23				24 25 26 27 28 29 30 31			
	삭제된 이니시에이터 바이트(계속)				삭제된 응답자 바이트											
	삭제된 응답자 바이트(계속)															
					QOS 적용 인터페이스											
					QOS 적용 인터페이스(계속)											
					QOS 적용 인터페이스(계속)											
					QOS 적용 인터페이스(계속)											
	QOS 인터페이스(계속)				QOS 규칙 ID											
	QOS 규칙 ID(계속)				사용자 ID											
	사용자 ID(계속)				애플리케이션 프로토콜 ID											
	애플리케이션 프로토콜 ID(계속)				URL 카테고리											
	URL 카테고리(계속)				URL 평판											
	URL 평판(계속)				클라이언트 애플리케이션 ID											
	클라이언트 애플리케이션 ID(계속)				웹 애플리케이션 ID											
클라이언트 URL	웹 애플리케이션 ID(계속)				문자열 블록 유형(0)											
	문자열 블록 유형(계속)				문자열 블록 길이											
	문자열 블록 길이(계속)				클라이언트 애플리케이션 URL...											
NetBIOS 이름	문자열 블록 유형(0)															
	문자열 블록 길이															
	NetBIOS 이름...															


바이트
0
1
2
3
비트
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
클라이언트 애플리케이션 버전
문자열 블록 유형(0)
문자열 블록 길이
클라이언트 애플리케이션 버전...
모니터링 규칙 1
모니터링 규칙 2
모니터링 규칙 3
모니터링 규칙 4
모니터링 규칙 5
모니터링 규칙 6
모니터링 규칙 7
모니터링 규칙 8
보안 인텔리전스 소스/대상
보안 인텔리전스 계층
파일 이벤트 개수
침입 이벤트 개수
이니시에이터 국가
응답자 국가
원래 클라이언트 국가
IOC 번호
소스 자동 시스템
소스 자동 시스템(계속)
대상 자동 시스템
대상 자동 시스템
SNMP 입력
SNMP 출력
소스 TOS
대상 TOS
소스 마스크
대상 마스크
보안 상황
보안 상황
보안 상황(계속)
보안 상황(계속)
보안 상황(계속)
VLAN ID



바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
참조된 호스트	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	참조된 호스트...																															
사용자 에이전트	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	사용자 에이전트...																															
HTTP 참조 페이지	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	HTTP 참조 페이지...																															
	SSL 인증서 핑거프린트																															
	SSL 인증서 핑거프린트(계속)																															
	SSL 인증서 핑거프린트(계속)																															
	SSL 인증서 핑거프린트(계속)																															
	SSL 인증서 핑거프린트(계속)																															
	SSL 정책 ID																															
	SSL 정책 ID(계속)																															
	SSL 정책 ID(계속)																															
	SSL 정책 ID(계속)																															
	SSL 규칙 ID																															
	SSL 암호 그룹																SSL 버전								SSL 서버 인증서 상태							
	SSL 서버 인증서 상태(계속)																								SSL 실제 작업							
	SSL 실제 작업(계속)								SSL 예상 작업																SSL 플로우 상태							


바이트
0
1
2
3
비트
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
SSL 플로우 상태 (계속)
SSL 플로우 오류
SSL 플로우 오류 (계속)
SSL 플로우 메시지
SSL 플로우 메시지(계속)
SSL 플로우 플래그
SSL 플로우 플래그(계속)
SSL 서버 이름
SSL 플로우 플래그(계속)
문자열 블록 유형(0)
문자열 블록 유형(0)(계속)
문자열 블록 길이
문자열 블록 길이 (계속)
SSL 서버 이름...
SSL URL 카테고리
SSL 세션 ID
SSL 세션 ID(계속)
SSL 세션 ID(계속)
SSL 세션 ID(계속)
SSL 세션 ID(계속)
SSL 세션 ID(계속)
SSL 세션 ID(계속)
SSL 세션 ID(계속)
SSL 세션 ID 길이
SSL 티켓 ID
SSL 티켓 ID(계속)
SSL 티켓 ID(계속)
SSL 티켓 ID(계속)
SSL 티켓 ID(계속)


바이트
0
1
2
3
비트
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
SSL 티켓 ID(계속)
SSL 티켓 ID 길이
네트워크 분석 정책 수정
네트워크 분석 정책 수정(계속)
네트워크 분석 정책 수정(계속)
네트워크 분석 정책 수정(계속)
네트워크 분석 정책 수정(계속)
엔드포인트 프로파일 ID
엔드포인트 프로파일 ID(계속)
보안 그룹 ID
보안 그룹 ID(계속)
위치 IPv6
위치 IPv6(계속)
위치 IPv6(계속)
위치 IPv6(계속)
위치 IPv6(계속)
HTTP 응답
HTTP 응답(계속)
문자열 블록 유형(0)
문자열 블록 유형(0)(계속)
문자열 블록 길이
문자열 블록 길이(계속)
DNS 쿼리...
DNS 쿼리
DNS 레코드 유형
DNS 응답 유형
DNS TTL
싱크홀 UUID
싱크홀 UUID(계속)
싱크홀 UUID(계속)
싱크홀 UUID(계속)
보안 인텔리전스 목록 1
보안 인텔리전스 목록 2
보안 인텔리전스 목록 3

다음 표에는 6.2 이상 버전용 연결 통계 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 4-70 6.2 이상 버전용 연결 통계 데이터 블록 필드

필드	데이터 유형	설명
연결 통계 데이터 블록 유형	uint32	6.2 이상 버전용 연결 통계 데이터 블록을 시작합니다. 값은 항상 168입니다.
연결 통계 데이터 블록 길이	uint32	연결 통계 데이터 블록의 바이트 수입니다. 여기에는 연결 통계 블록 유형 및 길이 필드의 8바이트에 그 뒤의 연결 데이터 바이트 수를 더한 값이 포함됩니다.
디바이스 ID	uint32	연결 이벤트를 탐지한 디바이스입니다.
인그레스 영역	uint8[16]	정책 위반을 트리거한 이벤트의 인그레스 보안 영역입니다.
이그레스 (egress) 영역	uint8[16]	정책 위반을 트리거한 이벤트의 이그레스(egress) 보안 영역입니다.
인그레스 인터페이스	uint8[16]	인바운드 트래픽용 인터페이스입니다.
이그레스 (egress) 인터페이스	uint8[16]	아웃바운드 트래픽용 인터페이스입니다.
이니시에이터 IP 주소	uint8[16]	연결 이벤트에서 설명하는 세션을 시작한 호스트의 IP 주소(IP 주소 옥텟 형식)입니다.
응답자 IP 주소	uint8[16]	시작 호스트에 응답한 호스트의 IP 주소(IP 주소 옥텟 형식)입니다.
원래 클라이언트 IP 주소	uint8[16]	요청이 생성된 프록시를 사용하는 호스트의 IP 주소(IP 주소 옥텟 형식)입니다.
정책 수정	uint8[16]	해당하는 경우 트리거된 상관관계와 관련된 규칙의 수정 번호입니다.
규칙 ID	uint32	해당하는 경우 이벤트를 트리거한 규칙의 내부 식별자입니다.
터널 규칙 ID	uint32	해당하는 경우 이벤트를 트리거한 터널 규칙의 내부 식별자입니다.
규칙 작업	uint16	해당 규칙(허용, 차단 등)에 대해 사용자 인터페이스에서 선택한 작업입니다.
규칙 이유	uint32	규칙이 이벤트를 트리거한 이유입니다.
이니시에이터 포트	uint16	시작 호스트에 사용되는 포트입니다.
응답자 포트	uint16	응답 호스트에 사용되는 포트입니다.
TCP 플래그	uint16	연결 이벤트에 대한 모든 TCP 플래그를 나타냅니다.
프로토콜	uint8	IANA에서 지정한 프로토콜 번호입니다.
NetFlow 소스	uint8[16]	연결에 대한 데이터를 내보낸 NetFlow 지원 디바이스의 IP 주소입니다.
인스턴스 ID	uint16	이벤트를 생성한 매니지드 디바이스의 Snort 인스턴스의 숫자 ID입니다.
연결 카운터	uint16	1초 이내에 발생하는 연결 이벤트를 구별하는 데 사용되는 값입니다.

표 4-70 6.2 이상 버전용 연결 통계 데이터 블록 필드 (계속)

필드	데이터 유형	설명
첫 번째 패킷 타임스탬프	uint32	세션에서 첫 번째 패킷이 교환된 날짜의 시간의 UNIX 타임스탬프입니다.
마지막 패킷 타임스탬프	uint32	세션에서 마지막 패킷이 교환된 날짜의 시간의 UNIX 타임스탬프입니다.
이니시에이터 전송 패킷	uint64	시작 호스트에서 전송한 패킷 수입니다.
응답자 전송 패킷	uint64	응답 호스트에서 전송한 패킷 수입니다.
이니시에이터 전송 바이트	uint64	시작 호스트에서 전송한 바이트 수입니다.
응답자 전송 바이트	uint64	응답 호스트에서 전송한 바이트 수입니다.
삭제된 이니시에이터 패킷	uint64	속도 제한으로 인해 세션 이니시에이터에서 삭제된 패킷 수입니다.
삭제된 응답자 패킷	uint64	속도 제한으로 인해 세션 응답자에서 삭제된 패킷 수입니다.
삭제된 이니시에이터 바이트	uint64	속도 제한으로 인해 세션 이니시에이터에서 삭제된 바이트 수입니다.
삭제된 응답자 바이트	uint64	속도 제한으로 인해 세션 응답자에서 삭제된 바이트 수입니다.
QOS 적용 인터페이스	uint8[16]	속도가 제한되는 연결에서 속도 제한이 적용되는 인터페이스 이름입니다.
QOS 규칙 ID	uint32	해당하는 경우 연결에 적용된 QoS(Quality of Service) 규칙의 내부 ID 번호입니다.
사용자 ID	uint32	트래픽을 생성한 호스트에 마지막으로 로그인한 사용자의 내부 ID 번호입니다.
애플리케이션 프로토콜 ID	uint32	애플리케이션 프로토콜의 애플리케이션 ID입니다.
URL 카테고리	uint32	URL 카테고리의 내부 ID 번호입니다.
URL 평판	uint32	URL 평판의 내부 ID 번호입니다.
클라이언트 애플리케이션 ID	uint32	해당하는 경우 탐지된 클라이언트 애플리케이션의 내부 ID 번호입니다.
웹 애플리케이션 ID	uint32	해당하는 경우 탐지된 웹 애플리케이션의 내부 ID 번호입니다.
문자열 블록 유형	uint32	클라이언트 애플리케이션 URL에 대한 문자열 데이터 블록을 시작합니다. 이 값은 항상 `0`입니다.
문자열 블록 길이	uint32	클라이언트 애플리케이션 URL 문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이 필드의 8바이트에 클라이언트 애플리케이션 URL 문자열의 바이트 수를 더한 값이 포함됩니다.
클라이언트 애플리케이션 URL	string	해당하는 경우 클라이언트 애플리케이션이 액세스한 URL입니다. 예를 들면 `/files/index.html`과 같습니다.

표 4-70 6.2 이상 버전용 연결 통계 데이터 블록 필드 (계속)

필드	데이터 유형	설명
문자열 블록 유형	uint32	호스트 NetBIOS 이름에 대한 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이 필드의 8바이트에 NetBIOS 이름 문자열의 바이트 수를 더한 값이 포함됩니다.
NetBIOS 이름	string	호스트 NetBIOS 이름 문자열입니다.
문자열 블록 유형	uint32	클라이언트 애플리케이션 버전에 대한 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	클라이언트 애플리케이션 버전에 대한 문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이의 8바이트에 버전의 바이트 수를 더한 값이 포함됩니다.
클라이언트 애플리케이션 버전	string	클라이언트 애플리케이션 버전입니다.
모니터링 규칙 1	uint32	연결 이벤트와 관련된 첫 번째 모니터 규칙의 ID입니다.
모니터링 규칙 2	uint32	연결 이벤트와 관련된 두 번째 모니터 규칙의 ID입니다.
모니터링 규칙 3	uint32	연결 이벤트와 관련된 세 번째 모니터 규칙의 ID입니다.
모니터링 규칙 4	uint32	연결 이벤트와 관련된 네 번째 모니터 규칙의 ID입니다.
모니터링 규칙 5	uint32	연결 이벤트와 관련된 다섯 번째 모니터 규칙의 ID입니다.
모니터링 규칙 6	uint32	연결 이벤트와 관련된 여섯 번째 모니터 규칙의 ID입니다.
모니터링 규칙 7	uint32	연결 이벤트와 관련된 일곱 번째 모니터 규칙의 ID입니다.
모니터링 규칙 8	uint32	연결 이벤트와 관련된 여덟 번째 모니터 규칙의 ID입니다.
보안 인텔리전스 소스/대상	uint8	소스 또는 대상 IP 주소가 IP 블랙리스트와 일치했는지를 나타냅니다.
보안 인텔리전스 계층	uint8	IP 블랙리스트와 일치한 IP 계층입니다.
파일 이벤트 개수	uint16	1초 이내에 발생하는 파일 이벤트를 구별하는 데 사용되는 값입니다.
침입 이벤트 개수	uint16	1초 이내에 발생하는 침입 이벤트를 구별하는 데 사용되는 값입니다.
이니시에이터 국가	uint16	시작 호스트의 국가 코드입니다.
응답자 국가	uint16	응답 호스트의 국가 코드입니다.
원래 클라이언트 국가	uint16	요청이 생성된 프록시를 사용하는 호스트의 국가 코드입니다.
IOC 번호	uint16	이 이벤트와 관련된 보안 침해의 ID 번호입니다.
소스 자동 시스템	uint32	소스의 AS 번호(원본 또는 피어)입니다.
대상 자동 시스템	uint32	대상의 AS 번호(원본 또는 피어)입니다.
SNMP 입력	uint16	입력 인터페이스의 SNMP 인덱스입니다.
SNMP 출력	uint16	출력 인터페이스의 SNMP 인덱스입니다.
소스 TOS	uint8	들어오는 인터페이스에 대한 서비스 유형 바이트 설정입니다.

표 4-70 6.2 이상 버전용 연결 통계 데이터 블록 필드 (계속)

필드	데이터 유형	설명
대상 TOS	uint8	나가는 인터페이스에 대한 서비스 유형 바이트 설정입니다.
소스 마스크	uint8	소스 주소 접두사 마스크입니다.
대상 마스크	uint8	대상 주소 접두사 마스크입니다.
보안 상황	uint8(16)	트래픽이 통과한 보안 상황(가상 방화벽)의 ID 번호입니다. 이 필드는 다중 컨텍스트 모드의 ASA FirePOWER 디바이스에 대해서만 채워집니다.
VLAN ID	uint16	호스트가 구성원으로 포함된 VLAN을 나타내는 VLAN ID 번호입니다.
문자열 블록 유형	uint32	참조된 호스트 이름을 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	참조된 호스트 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Referenced Host(참조된 호스트) 필드의 바이트 수를 더한 값이 포함됩니다.
참조된 호스트	string	HTTP 또는 DNS로 제공되는 호스트 이름 정보입니다.
문자열 블록 유형	uint32	사용자 에이전트를 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	사용자 에이전트 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 User Agent(사용자 에이전트) 필드의 바이트 수를 더한 값이 포함됩니다.
사용자 에이전트	string	세션에서 UserAgent 헤더 필드의 정보입니다.
문자열 블록 유형	uint32	HTTP 참조 페이지를 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	HTTP 참조 페이지 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 HTTP Referer(HTTP 참조 페이지) 필드의 바이트 수를 더한 값이 포함됩니다.
HTTP 참조 페이지	string	페이지가 생성된 사이트입니다. HTTP 트래픽의 참조 페이지 헤더 정보에서 찾을 수 있습니다.
SSL 인증서 핑거프린트	uint8[20]	SSL 서버 인증서의 SHA1 해시입니다.
SSL 정책 ID	uint8[16]	연결을 처리한 SSL 정책의 ID 번호입니다.
SSL 규칙 ID	uint32	연결을 처리한 SSL 규칙 또는 기본 동작의 ID 번호입니다.
SSL 암호 그룹	uint16	SSL 연결에서 사용되는 암호화 그룹입니다. 값은 10진수 형식으로 저장됩니다. 값으로 지정되는 암호 그룹은 `www.iana.org/assignments/tls-parameters/tls-parameters.xhtml`을 참조하십시오.
SSL 버전	uint8	연결을 암호화하는 데 사용된 SSL 또는 TLS 프로토콜 버전입니다.

표 4-70 6.2 이상 버전용 연결 통계 데이터 블록 필드 (계속)

필드	데이터 유형	설명
SSL 서버 인증서 상태	uint32	SSL 인증서의 상태입니다. 가능한 값은 다음과 같습니다. • 0 - 확인되지 않음 - 서버 인증서 상태를 평가하지 않았습니다. • 1 - 알 수 없음 - 서버 인증서 상태를 확인할 수 없습니다. • 2 - 유효 - 서버 인증서가 유효합니다. • 4 - 자체 서명 - 서버 인증서가 자체 서명되었습니다. • 16 - 유효하지 않은 발급자 - 서버 인증서의 발급자가 유효하지 않습니다. • 32 - 유효하지 않은 서명 - 서버 인증서의 서명이 유효하지 않습니다. • 64 - 만료됨 - 서버 인증서가 만료되었습니다. • 128 - 아직 유효하지 않음 - 서버 인증서가 아직 유효하지 않습니다. • 256 - 해지됨 - 서버 인증서가 해지되었습니다.
SSL 실제 작업	uint16	SSL 규칙에 기반한 연결에서 수행된 작업입니다. 규칙에 명시된 작업이 가능하지 않을 수도 있으므로, 이는 예상 작업과 다를 수 있습니다. 가능한 값은 다음과 같습니다. • 0 - '알 수 없음' • 1 - '암호 해독 안 함' • 2 - '차단' • 3 - '차단 및 재설정' • 4 - '암호 해독(알려진 키)' • 5 - '암호 해독(키 교체)' • 6 - '암호 해독(재서명)'
SSL 예상 작업	uint16	SSL 규칙에 기반한 연결에서 수행해야 하는 작업입니다. 가능한 값은 다음과 같습니다. • 0 - '알 수 없음' • 1 - '암호 해독 안 함' • 2 - '차단' • 3 - '차단 및 재설정' • 4 - '암호 해독(알려진 키)' • 5 - '암호 해독(키 교체)' • 6 - '암호 해독(재서명)'

표 4-70 6.2 이상 버전용 연결 통계 데이터 블록 필드 (계속)

필드	데이터 유형	설명
SSL 플로우 상태	uint16	SSL 플로우의 상태입니다. 이 값은 작업을 수행한 이유 또는 오류 메시지가 표시된 이유를 설명합니다. 가능한 값은 다음과 같습니다. • 0 - '알 수 없음' • 1 - '일치하지 않음' • 2 - '성공' • 3 - '캐시되지 않은 세션' • 4 - '알 수 없는 암호 그룹' • 5 - '지원되지 않는 암호 그룹' • 6 - '지원되지 않는 SSL 버전' • 7 - 'SSL 압축 사용됨' • 8 - '패시브 모드에서 세션 암호 해독 불가' • 9 - '핸드셰이크 오류' • 10 - '암호 해독 오류' • 11 - '서버 이름 카테고리 조회 보류 중' • 12 - '공용 이름 카테고리 조회 보류 중' • 13 - '내부 오류' • 14 - '네트워크 파라미터 사용 불가' • 15 - '유효하지 않은 서버 인증서 핸들' • 16 - '서버 인증서 핑거프린트 사용 불가' • 17 - '주체 DN을 캐시할 수 없음' • 18 - '발급자 DN을 캐시할 수 없음' • 19 - '알 수 없는 SSL 버전' • 20 - '외부 인증서 목록 사용 불가' • 21 - '외부 인증서 핑거프린트 사용 불가' • 22 - '내부 인증서 목록이 유효하지 않음' • 23 - '내부 인증서 목록 사용 불가' • 24 - '내부 인증서 사용 불가' • 25 - '내부 인증서 핑거프린트 사용 불가' • 26 - '서버 인증서 검증 사용 불가' • 27 - '서버 인증서 검증 장애' • 28 - '유효하지 않은 작업'
SSL 플로우 오류	uint32	자세한 SSL 오류 코드입니다. 이러한 값은 지원용으로 필요할 수 있습니다.

표 4-70 6.2 이상 버전용 연결 통계 데이터 블록 필드 (계속)

필드	데이터 유형	설명
SSL 플로우 메시지	uint32	SSL 핸드셰이크 도중 클라이언트와 서버 간에 교환된 메시지입니다. 자세한 내용은 http://tools.ietf.org/html/rfc5246을 참조하십시오. • 0x00000001 — NSE_MT__HELLO_REQUEST • 0x00000002 — NSE_MT__CLIENT_ALERT • 0x00000004 — NSE_MT__SERVER_ALERT • 0x00000008 — NSE_MT__CLIENT_HELLO • 0x00000010 — NSE_MT__SERVER_HELLO • 0x00000020 — NSE_MT__SERVER_CERTIFICATE • 0x00000040 — NSE_MT__SERVER_KEY_EXCHANGE • 0x00000080 — NSE_MT__CERTIFICATE_REQUEST • 0x00000100 — NSE_MT__SERVER_HELLO_DONE • 0x00000200 — NSE_MT__CLIENT_CERTIFICATE • 0x00000400 — NSE_MT__CLIENT_KEY_EXCHANGE • 0x00000800 — NSE_MT__CERTIFICATE_VERIFY • 0x00001000 — NSE_MT__CLIENT_CHANGE_CIPHER_SPEC • 0x00002000 — NSE_MT__CLIENT_FINISHED • 0x00004000 — NSE_MT__SERVER_CHANGE_CIPHER_SPEC • 0x00008000 — NSE_MT__SERVER_FINISHED • 0x00010000 — NSE_MT__NEW_SESSION_TICKET • 0x00020000 — NSE_MT__HANDSHAKE_OTHER • 0x00040000 — NSE_MT__APP_DATA_FROM_CLIENT • 0x00080000 — NSE_MT__APP_DATA_FROM_SERVER
SSL 플로우 플래그	uint64	암호화된 연결에 대한 디버깅 레벨 플래그입니다. 가능한 값은 다음과 같습니다. • 0x00000001 - NSE_FLOW__VALID - 다른 필드를 유효하게 만들려면 설정해야 함 • 0x00000002 - NSE_FLOW__INITIALIZED - 처리 준비가 완료된 내부 구조 • 0x00000004 - NSE_FLOW__INTERCEPT - SSL 세션이 중단됨
문자열 블록 유형	uint32	SSL 서버 이름을 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	SSL 서버 이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 SSL Server Name(SSL 서버 이름) 필드의 바이트 수를 더한 값이 포함됩니다.

표 4-70 6.2 이상 버전용 연결 통계 데이터 블록 필드 (계속)

필드	데이터 유형	설명
SSL 서버 이름	string	SSL Client Hello의 서버 이름 표시에서 제공된 이름입니다.
SSL URL 카테고리	uint32	서버 이름 및 인증서 일반 이름에서 확인된 플로우의 카테고리입니다.
SSL 세션 ID	uint8[32]	클라이언트와 서버가 세션 재사용에 동의하는 경우 SSL 핸드셰이크 중에 사용되는 세션 ID의 값입니다.
SSL 세션 ID 길이	uint8	SSL 세션 ID의 길이입니다. 세션 ID는 32바이트를 초과할 수는 없으며 32바이트보다 작을 수는 있습니다.
SSL 티켓 ID	uint8[20]	클라이언트와 서버가 세션 티켓 사용에 동의하는 경우 사용되는 세션 티켓의 해시입니다.
SSL 티켓 ID 길이	uint8	SSL 티켓 ID의 길이입니다. 티켓 ID는 20바이트를 초과할 수는 없으며 20바이트보다 작을 수는 있습니다.
네트워크 분석 정책 수정	uint8[16]	연결 이벤트와 관련된 네트워크 분석 정책의 수정 버전입니다.
엔드포인트 프로파일 ID	uint32	ISE가 식별한 연결 엔드포인트에서 사용하는 디바이스 유형의 ID 번호입니다. 각 DC에 대해 고유하며 메타데이터에서 확인 가능합니다.
보안 그룹 ID	uint32	정책을 기준으로 ISE가 사용자에게 할당하는 ID 번호입니다.
위치 IPv6	uint8[16]	ISE와 통신하는 인터페이스의 IP 주소입니다. IPv4 또는 IPv6일 수 있습니다.
HTTP 응답	uint32	HTTP 요청의 응답 코드입니다.
문자열 블록 유형	uint32	DNS 쿼리에 대한 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이 필드의 8바이트에 DNS 쿼리 문자열의 바이트 수를 더한 값이 포함됩니다.
DNS 쿼리	string	DNS 서버에 전송되는 쿼리의 콘텐츠입니다.
DNS 레코드 유형	uint16	DNS 레코드 유형에 해당하는 숫자 값입니다.
DNS 응답 유형	uint16	DNS 응답 유형에 해당하는 숫자 값입니다.
DNS TTL	uint32	DNS 응답의 초 단위 TTL(Time to Live)입니다.
싱크홀 UUID	uin8[16]	싱크홀 개체와 관련된 수정 UUID입니다.
보안 인텔리전스 목록 1	uint32	이벤트와 관련된 보안 인텔리전스 목록으로, 관련된 메타데이터의 보안 인텔리전스 목록에 매핑됩니다. 3개의 보안 인텔리전스 목록이 연결과 관련되어 있을 수 있습니다.
보안 인텔리전스 목록 2	uint32	이벤트와 관련된 보안 인텔리전스 목록으로, 관련된 메타데이터의 보안 인텔리전스 목록에 매핑됩니다. 3개의 보안 인텔리전스 목록이 연결과 관련되어 있을 수 있습니다.
보안 인텔리전스 목록 3	uint32	이벤트와 관련된 보안 인텔리전스 목록으로, 관련된 메타데이터의 보안 인텔리전스 목록에 매핑됩니다. 3개의 보안 인텔리전스 목록이 연결과 관련되어 있을 수 있습니다.

5.2 이상 버전용 스캔 결과 데이터 블록

스캔 결과 데이터 블록은 취약점을 설명하며 스캔 결과 추가 이벤트(이벤트 유형 1002, 하위 유형 11) 내에서 사용됩니다. 계열 1 블록 그룹에서 스캔 결과 데이터 블록의 블록 유형은 142입니다. 이는 블록 유형 102를 대체합니다. 버전 5.2에서는 IP 주소 필드의 크기가 16바이트로 늘어났습니다.

다음 다이어그램에 스캔 결과 데이터 블록의 형식이 나와 있습니다.

바이트	0								1								2								3								
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
	스캔 결과 블록 유형(142)																																
	스캔 결과 블록 길이																																
	사용자 ID																																
	스캔 유형																																
	IP 주소 IP 주소(계속) IP 주소(계속) IP 주소(계속)																																
	포트																프로토콜																
	플래그																목록 블록 유형(11)																취약점 스캔 목록
	목록 블록 유형(11)																목록 블록 길이																
취약점 목록	목록 블록 길이																취약점 스캔 블록 유형(109)																
	취약점 스캔 블록 유형(109)																취약점 스캔 블록 길이																
	취약점 스캔 블록 길이																취약점 데이터...																
	목록 블록 유형(11)																																일반 스캔 결과 목록
	목록 블록 길이																																
스캔 결과 목록	일반 스캔 결과 블록 유형(108)																																
	일반 스캔 결과 블록 길이																																
	일반 스캔 결과...																																

다음 표에는 스캔 결과 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 4-71 스캔 결과 데이터 블록 필드

필드	데이터 유형	설명
스캔 결과 블록 유형	uint32	스캔 결과 데이터 블록을 시작합니다. 이 값은 항상 142입니다.
스캔 결과 블록 길이	uint32	취약점 스캔 데이터 블록의 바이트 수입니다. 여기에는 취약점 스캔 블록 유형 및 길이 필드의 8바이트에 그 뒤의 취약점 스캔 데이터 바이트 수를 더한 값이 포함됩니다.
사용자 ID	uint32	스캔 결과를 가져왔거나 스캔 결과가 생성된 스캔을 실행한 사용자의 사용자 ID 번호를 포함합니다.
스캔 유형	uint32	결과가 시스템에 추가된 방법을 나타냅니다.
IP 주소	uint8[16]	결과에서 취약점의 영향을 받는 호스트의 IP 주소(IP 주소 옥텟 형식)입니다.
포트	uint16	결과에서 취약점의 영향을 받는 하위 서버가 사용하는 포트입니다.
프로토콜	uint16	IANA 프로토콜 번호 또는 이더 타입입니다. 이는 전송 계층 프로토콜과 네트워크 계층 프로토콜에서 서로 다르게 처리됩니다. 전송 계층 프로토콜은 IANA 프로토콜 번호로 식별됩니다. 예를 들면 다음과 같습니다. • 6 - TCP • 17 - UDP 네트워크 계층 프로토콜은 IEEE 등록 기관 이더 타입의 10진수 형식으로 식별됩니다. 예를 들면 다음과 같습니다. • 2048 - IP
플래그	uint16	예약됨
목록 블록 유형	uint32	전송 취약점 스캔 데이터를 전달하는 취약점 스캔 데이터 블록으로 구성된 목록 데이터 블록을 시작합니다. 이 값은 항상 11입니다.
목록 블록 길이	uint32	목록의 바이트 수입니다. 이 수에는 목록 블록 유형 및 길이 필드의 8바이트에 캡슐화된 모든 취약점 스캔 데이터 블록을 더한 값이 포함됩니다. 이 필드 뒤에는 취약점 스캔 데이터 블록이 없을 수도 있고 하나 이상 올 수도 있습니다.

표 4-71 스캔 결과 데이터 블록 필드 (계속)

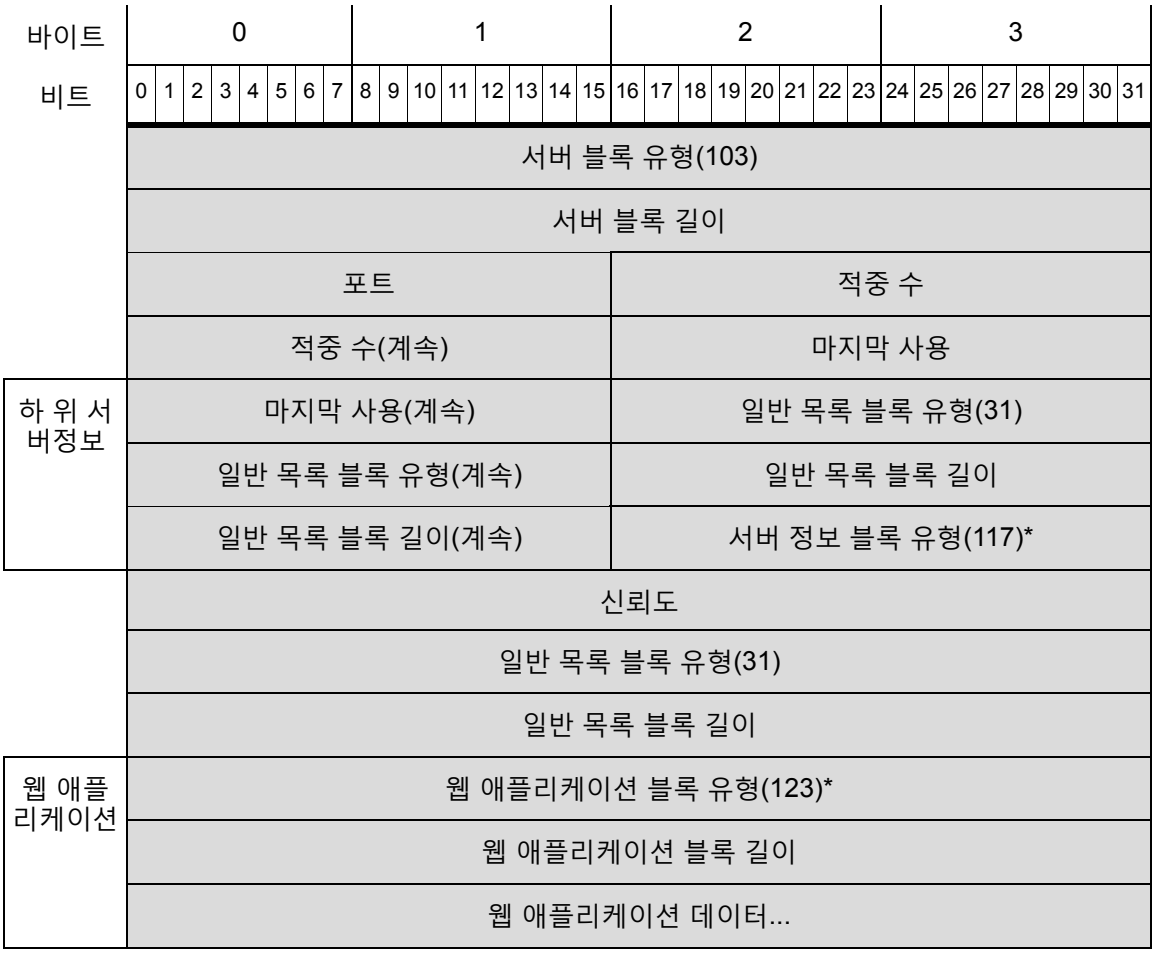
필드	데이터 유형	설명
취약점 스캔 블록 유형	uint32	스캔 중에 탐지된 취약점을 설명하는 취약점 스캔 데이터 블록을 시작합니다. 이 값은 항상 109입니다.
취약점 스캔 블록 길이	uint32	취약점 스캔 데이터 블록의 바이트 수입니다. 여기에는 취약점 스캔 블록 유형 및 길이 필드의 8바이트에 그 뒤의 취약점 스캔 데이터 바이트 수를 더한 값이 포함됩니다.
취약점 데이터	string	각 취약점과 관련된 정보입니다.
목록 블록 유형	uint32	전송 취약점 스캔 데이터를 전달하는 취약점 스캔 데이터 블록으로 구성된 목록 데이터 블록을 시작합니다. 이 값은 항상 11입니다.
목록 블록 길이	uint32	목록의 바이트 수입니다. 이 수에는 목록 블록 유형 및 길이 필드의 8바이트에 캡슐화된 모든 취약점 스캔 데이터 블록을 더한 값이 포함됩니다. 이 필드 뒤에는 취약점 스캔 데이터 블록이 없을 수도 있고 하나 이상 올 수도 있습니다.
일반 스캔 결과 블록 유형	uint32	스캔 중에 탐지된 서버 및 운영 체제 데이터를 설명하는 일반 스캔 결과 데이터 블록을 시작합니다. 이 값은 항상 108입니다.
일반 스캔 결과 블록 길이	uint32	일반 스캔 결과 데이터 블록의 바이트 수입니다. 여기에는 일반 스캔 결과 블록 유형 및 길이 필드의 8바이트에 그 뒤의 스캔 결과 데이터 바이트 수를 더한 값이 포함됩니다.
일반 스캔 결과 데이터	string	각 스캔 결과와 관련된 정보입니다.
일반 목록 블록 유형	uint32	서드파티 애플리케이션의 호스트 입력 데이터를 전달하는 사용자 제품 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 사용자 제품 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
사용자 제품 데이터 블록*	variable	호스트 입력 데이터를 포함하는 사용자 제품 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 사용자 제품 데이터 블록, 4-171페이지의 내용을 참조하십시오.

4.10.0 이상 버전용 호스트 서버 데이터 블록

호스트 서버 데이터 블록은 호스트에서 탐지된 서버에 대한 정보를 전달합니다. 이 블록에는 탐지된 각 서버에 해당하는 블록이 포함되며, 서버가 실행 중인 웹 애플리케이션에 해당하는 웹 애플리케이션 데이터 블록의 목록도 포함됩니다. 호스트 서버 데이터 블록은 신규 및 변경된 TCP/UDP 서버에 대한 메시지에 포함됩니다. 자세한 정보는 서버 메시지, 4-46페이지의 내용을 참조하십시오. 계열 1 블록 그룹에서 호스트 서버 데이터 블록의 블록 유형은 103입니다.

참고 다음 다이어그램에서 데이터 블록 이름 옆에 있는 별표(*)는 데이터 블록 인스턴스가 여러 개 나올 수 있음을 나타냅니다.

다음 다이어그램에 호스트 서버 데이터 블록의 형식이 나와 있습니다.



다음 표에는 호스트 서버 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 4-72 호스트 서버 데이터 블록 필드

필드	데이터 유형	설명
호스트 서버 블록 유형	uint32	호스트 서버 데이터 블록을 시작합니다. 이 값은 항상 103입니다.
호스트 서버 블록 길이	uint32	호스트 서버 데이터 블록의 총 바이트 수입니다. 여기에는 호스트 서버 블록 유형 및 길이 필드의 8바이트에 그 뒤의 데이터 바이트 수를 더한 값이 포함됩니다.
포트	uint16	서버가 실행되는 포트 번호입니다.
적중 수	uint32	서버에서 수신한 적중 수입니다.
마지막 사용	uint32	시스템이 사용 중인 서버를 마지막으로 탐지한 시간을 나타내는 UNIX 타임스탬프입니다.
일반 목록 블록 유형	uint32	일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.

표 4-72 호스트 서버 데이터 블록 필드 (계속)

필드	데이터 유형	설명
일반 목록 블록 길이	uint32	일반 목록 블록과 캡슐화된 하위 서버 정보 데이터 블록의 바이트 수입니다. 이 수에는 일반 목록 블록 헤더 필드의 8바이트에 캡슐화된 모든 데이터 블록의 바이트 수를 더한 값이 포함됩니다.
서버 정보 데이터 블록*	variable	서버 정보 데이터 블록(목록 블록 길이의 최대 바이트 수까지)입니다. 자세한 정보는 4.10.x, 5.0~5.0.2 버전용 서버 정보 데이터 블록, 4-144페이지의 내용을 참조하십시오.
신뢰도	uint32	신뢰도 퍼센트입니다.
일반 목록 블록 유형	uint32	일반 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	일반 블록과 캡슐화된 웹 애플리케이션 데이터 블록의 바이트 수입니다. 이 수에는 일반 목록 블록 헤더 필드의 8바이트에 캡슐화된 모든 웹 애플리케이션 데이터 블록의 바이트 수를 더한 값이 포함됩니다.
웹애플리케이션 데이터 블록*	variable	캡슐화된 웹 애플리케이션 데이터 블록(목록 블록 길이의 최대 바이트 수까지)입니다. 자세한 정보는 5.0 이상 버전용 웹 애플리케이션 데이터 블록, 4-119페이지의 내용을 참조하십시오.

4.10.0 이상 버전용 전체 호스트 서버 데이터 블록

전체 호스트 서버 데이터 블록은 서버 포트, 사용 빈도, 가장 최근 업데이트, 데이터 정확도의 신뢰도, 호스트에 대한 해당 서버 관련 Cisco 및 서드파티 취약점 등 서버에 대한 정보를 전달합니다. 전체 호스트 서버 데이터 블록은 서버에 있는 각 하위 서버의 전체 하위 서버 정보 데이터 블록을 포함합니다. 각 전체 호스트 프로파일 데이터 블록은 호스트에 있는 각 TCP 및 UDP 서버의 전체 호스트 서버 데이터 블록을 포함합니다. 계열 1 블록 그룹에서 전체 호스트 서버 데이터 블록의 블록 유형은 104입니다.

참고 다음 다이어그램에서 계열 1 데이터 블록 이름 옆에 있는 별표(*)는 데이터 블록 인스턴스가 여러 개 나올 수 있음을 나타냅니다.

다음 다이어그램에 전체 서버 데이터 블록의 형식이 나와 있습니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
하위 서버 - Cisco	적중 수(계속)																일반 목록 블록 유형(31)															
	일반 목록 블록 유형(계속)																일반 목록 블록 길이															
	일반 목록 블록 길이(계속)																전체 서버 정보 데이터 블록(106)*															
하위 서버 - 사용자	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
	전체 서버 정보 데이터 블록 유형(106)*																															
하위 서버 - 스캐너	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
	전체 서버 정보 데이터 블록(106)*																															
하위 서버 - 애플리케이션	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
	전체 서버 정보 데이터 블록(106)*																															
	신뢰도																															
서버 배너	BLOB 블록 유형(10)																															
	BLOB 블록 길이																															
	서버 배너 데이터...																															
VDB 취약점	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
	(VDB) 호스트 취약점 데이터 블록(85)*																															
서드파티/ VDB 취약점	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
	(서드파티/VDB) 호스트 취약점 데이터 블록(85)*																															

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
서드파티 호스트 취약점	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
	(서드파티) 호스트 취약점 데이터 블록(85)*																															
웹 애플리케이션	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
	웹 애플리케이션 데이터(123)*																															

다음 표에는 전체 서버 데이터 블록의 구성 요소에 대한 설명이 나와 있습니다.

표 4-73 4.10.0 이상 버전용 전체 서버 데이터 블록 필드

필드	데이터 유형	설명
전체 서버 블록 유형	uint32	전체 서버 데이터 블록을 시작합니다. 이 값은 항상 104입니다.
전체 서버 블록 길이	uint32	전체 서버 데이터 블록의 총 바이트 수입니다. 여기에는 전체 서버 블록 유형 및 길이 필드의 8바이트에 그 뒤의 전체 서버 데이터 바이트 수를 더한 값이 포함됩니다.
포트	uint16	서버 포트 번호입니다.
적중 수	uint32	서버에서 수신한 적중 수입니다.
일반 목록 블록 유형	uint32	탐지된 하위 서버 데이터의 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 하위 서버 정보 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
하위 서버 정보 - Cisco 데이터 블록*	variable	Cisco에서 탐지한 호스트 서버의 하위 서버에 대한 정보를 포함하는 전체 서버 정보 데이터 블록입니다. 이 데이터 블록에 대한 설명은 전체 서버 정보 데이터 블록, 4-147페이지의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	사용자가 추가한 하위 서버 데이터를 전달하는 하위 서버 정보 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 서버 정보 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
하위 서버 정보 - 사용자가 추가한 데이터 블록*	variable	사용자가 추가한 호스트의 하위 서버에 대한 정보를 포함하는 전체 서버 정보 데이터 블록입니다. 이 데이터 블록에 대한 설명은 전체 서버 정보 데이터 블록, 4-147페이지의 내용을 참조하십시오.

표 4-73 4.10.0 이상 버전용 전체 서버 데이터 블록 필드 (계속)

필드	데이터 유형	설명
일반 목록 블록 유형	uint32	스캐너가 추가한 하위 서버 데이터를 전달하는 하위 서버 정보 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 하위 서버 정보 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
하위 서버 정보 - 스캔에서 추가된 데이터 블록*	variable	스캐너가 추가한 호스트의 하위 서버에 대한 정보를 포함하는 전체 서버 정보 데이터 블록입니다. 이 데이터 블록에 대한 설명은 전체 서버 정보 데이터 블록, 4-147페이지의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	애플리케이션이 추가한 하위 서버 데이터를 전달하는 하위 서버 정보 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 하위 서버 정보 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
하위 서버 정보 - 애플리케이션에서 추가된 데이터 블록*	variable	애플리케이션 추가한 호스트의 하위 서버에 대한 정보를 포함하는 전체 서버 정보 데이터 블록입니다. 이 데이터 블록에 대한 설명은 전체 서버 정보 데이터 블록, 4-147페이지의 내용을 참조하십시오.
신뢰도	uint32	전체 서버 데이터의 ID 정확성에 대한 Cisco의 신뢰도 퍼센트입니다.
BLOB 블록 유형	uint32	배너 데이터를 포함하는 BLOB 데이터 블록을 시작합니다. 이 값은 항상 10입니다.
BLOB 블록 길이	uint32	BLOB 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 배너의 바이트 수를 더한 값이 포함됩니다.
서버 배너 데이터	byte[*n*]	서버 이벤트에 포함되는 패킷의 첫 *n*개 바이트입니다. 여기서 *n*은 256 이하의 숫자입니다.
일반 목록 블록 유형	uint32	Cisco 취약점 데이터를 전달하는 호스트 취약점 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 호스트 취약점 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
(VDB) 호스트 취약점 데이터 블록*	variable	VDB(취약점 데이터베이스)의 호스트 취약점에 대한 정보를 포함하는 호스트 취약점 데이터 블록입니다. 이 데이터 블록에 대한 설명은 4.9.0 이상 버전용 호스트 취약점 데이터 블록, 4-114페이지의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	서드파티 스캐너에서 제공한 서드파티 호스트 취약점 데이터를 전달하며 VDB에 이미 카탈로그화된 취약점 정보를 포함하는 호스트 취약점 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 호스트 취약점 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.

표 4-73 4.10.0 이상 버전용 전체 서버 데이터 블록 필드 (계속)

필드	데이터 유형	설명
(서드파티/VDB) 호스트 취약점 데이터 블록*	variable	VDB(취약점 데이터베이스)에 카탈로그화된 호스트 취약점에 대한 정보를 포함하며 서드파티 스캐너에서 제공한 호스트 취약점 데이터 블록입니다. 이 데이터 블록에 대한 설명은 4.9.0 이상 버전용 호스트 취약점 데이터 블록, 4-114페이지의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	서드파티 스캐너에서 생성된 서드파티 호스트 취약점 데이터를 전달하는 호스트 취약점 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 호스트 취약점 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
서드파티 스캔 호스트 취약점 데이터 블록*	variable	서드파티 스캐너에서 식별되었지만 VDB에는 카탈로그화되어 있지 않은 취약점에 대한 서드파티 취약점 데이터를 포함하는 호스트 취약점 데이터 블록입니다. 이 데이터 블록에 대한 설명은 4.9.0 이상 버전용 호스트 취약점 데이터 블록, 4-114페이지의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	일반 목록 블록과 캡슐화된 웹 애플리케이션 데이터 블록의 바이트 수입니다. 이 수에는 일반 목록 블록 헤더 필드의 8바이트에 캡슐화된 모든 데이터 블록의 바이트 수를 더한 값이 포함됩니다.
웹 애플리케이션 데이터 블록*	variable	캡슐화된 웹 애플리케이션 데이터 블록(목록 블록 길이의 최대 바이트 수까지)입니다.

4.10.x, 5.0~5.0.2 버전용 서버 정보 데이터 블록

서버 정보 데이터 블록은 서버 ID, 서버 벤더/버전, 소스 정보 등 서버에 대한 정보를 전달합니다. 계열 1 블록 그룹에서 서버 정보 데이터 블록의 블록 유형은 4.10.x 버전의 경우 105, 5.0~5.0.2 버전의 경우 117입니다. 서버 정보 데이터 블록은 호스트 서버 블록 및 전체 호스트 서버 데이터 블록 내의 목록에서 전달됩니다. 자세한 정보는 4.10.0 이상 버전용 호스트 서버 데이터 블록, 4-138페이지 및 4.10.0 이상 버전용 전체 호스트 서버 데이터 블록, 4-140페이지의 내용을 참조하십시오.

다음 다이어그램에 서버 정보 데이터 블록의 형식이 나와 있습니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	서버 벤더 이름 문자열...																															
	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	서버 버전 문자열...																															
	마지막 사용																															
	소스 유형																															
	소스 ID																															
	목록 블록 유형(11)																															
	목록 블록 길이																															
하위 서버	하위 서버 블록 형식(1)*																															
	하위 서버 블록 길이																															
	하위 서버 데이터...																															

다음 표에는 서버 정보 데이터 블록의 구성 요소에 대한 설명이 나와 있습니다.

표 4-74 서버 정보 데이터 블록 필드

필드	데이터 유형	설명
서버 정보 블록 유형	uint32	서버 정보 데이터 블록을 시작합니다. 블록 유형은 4.10.x 버전의 경우 105, 5.0 이상 버전의 경우 117입니다.
서버 정보 블록 길이	uint32	서버 정보 데이터 블록의 총 바이트 수입니다. 여기에는 서버 정보 블록 유형 및 길이 필드의 8바이트 + 서버 ID의 4바이트 + 벤더 이름 블록 유형 및 길이의 8바이트 + 벤더 이름의 추가 4바이트 + 버전 문자열 블록 유형 및 길이의 8바이트 + 버전 문자열의 추가 4바이트 + 마지막 사용/소스 유형/소스 ID 필드의 각 4바이트가 포함됩니다.
애플리케이션 ID	uint32	탐지된 서버에서 실행되는 애플리케이션 프로토콜의 애플리케이션 ID입니다.
문자열 블록 유형	uint32	서버 벤더 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.

표 4-74 서버 정보 데이터 블록 필드 (계속)

필드	데이터 유형	설명
문자열 블록 길이	uint32	벤더 이름 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 서버 벤더 이름의 바이트 수를 더한 값이 포함됩니다.
서버 벤더 이름	string	서버 벤더의 이름입니다.
문자열 블록 유형	uint32	서버 버전이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	서버 버전 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 서버 버전의 바이트 수를 더한 값이 포함됩니다.
서버 버전	string	서버 버전입니다.
마지막 사용 시간	uint32	트래픽에서 서버 정보가 마지막으로 사용된 시간을 나타냅니다.
소스 유형	uint32	데이터 소스의 유형에 매핑되는 번호입니다. • 0 - RNA에서 서버 데이터를 제공한 경우 • 1 - 사용자가 서버 데이터를 제공한 경우 • 2 - 서드파티 스캐너에서 서버 데이터를 제공한 경우 • 3 - nmimport.pl 등의 커맨드 라인 툴이나 호스트 입력 API 클라이언트에서 서버 데이터를 제공한 경우
소스 ID	uint32	서버 데이터 소스에 매핑되는 ID 번호입니다. 소스 유형에 따라 RNA, 사용자, 스캐너 또는 서드파티 애플리케이션에 매핑될 수 있습니다.
목록 블록 유형	uint32	하위 서버 데이터 블록의 목록을 시작합니다. 이 값은 항상 11입니다.
목록 블록 길이	uint32	목록 데이터 블록의 바이트 수입니다. 여기에는 목록 블록 유형 및 길이 필드의 8바이트에 그 뒤의 캡슐화된 하위 서버 데이터 블록 바이트 수를 더한 값이 포함됩니다.
하위 서버 블록 유형	uint32	첫 번째 하위 서버 데이터 블록을 시작합니다. 이 데이터 블록 뒤에는 목록 블록 길이 필드에 정의된 제한까지 다른 하위 서버 데이터 블록이 올 수 있습니다.
하위 서버 블록 길이	uint32	각 하위 서버 데이터 블록의 총 바이트 수입니다. 여기에는 하위 서버 블록 유형 및 길이 필드의 8바이트에 그 뒤의 데이터 바이트 수를 더한 값이 포함됩니다.
하위 서버 데이터	variable	하위 서버 데이터 블록, 4-75페이지에 설명되어 있는 하위 서버 데이터입니다.

전체 서버 정보 데이터 블록

전체 서버 정보 데이터 블록은 서버의 애플리케이션 프로토콜, 벤더/버전, 관련된 하위 서버의 목록 등 호스트에서 탐지된 서버에 대한 정보를 전달합니다. 각 하위 서버에 대한 정보는 전체 하위 서버 데이터 블록에 의해 포함됩니다(전체 하위 서버 데이터 블록, 4-84페이지 참조). 계열 1 블록 그룹에서 전체 서버 정보 데이터 블록의 블록 유형은 106입니다.

참고 다음 다이어그램에서 계열 1 데이터 블록 이름 옆에 있는 별표(*)는 데이터 블록 인스턴스가 여러 개 나올 수 있음을 나타냅니다.

다음 다이어그램에 전체 서버 정보 데이터 블록의 형식이 나와 있습니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	전체 서버 블록 유형(106)																															
	전체 서버 블록 길이																															
	애플리케이션 프로토콜 ID																															
벤더	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	벤더 이름 문자열...																															
버전	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	버전 문자열...																															
	마지막 사용																															
	소스 유형																															
	소스 ID																															
	목록 블록 유형(11)																															
	목록 블록 길이																															
하위 서버	전체 하위 서버 블록 유형(51)*																															
	전체 하위 서버 블록 길이																															
	전체 하위 서버 데이터...																															

다음 표에는 전체 서버 정보 데이터 블록의 구성 요소에 대한 설명이 나와 있습니다.

표 4-75 전체 서버 정보 데이터 블록 필드

필드	데이터 유형	설명
전체 서버 정보 블록 유형	uint32	전체 서버 정보 데이터 블록을 시작합니다. 이 값은 항상 106입니다.
전체 서버 정보 블록 길이	uint32	전체 서버 정보 데이터 블록의 총 바이트 수입니다. 여기에는 전체 서버 블록 유형 및 길이 필드의 8바이트에 그 뒤의 전체 서버 데이터 바이트 수를 더한 값이 포함됩니다.
애플리케이션 프로토콜 ID	uint32	서버에서 실행되는 애플리케이션 프로토콜의 애플리케이션 ID입니다.
문자열 블록 유형	uint32	애플리케이션 프로토콜 벤더 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	벤더 이름 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 벤더 이름의 바이트 수를 더한 값이 포함됩니다.
벤더 이름	string	서버 벤더의 이름입니다.
문자열 블록 유형	uint32	애플리케이션 프로토콜 버전이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 버전의 바이트 수를 더한 값이 포함됩니다.
버전	string	서버의 버전입니다.
마지막 사용	uint32	시스템이 사용 중인 서버를 마지막으로 탐지한 시간을 나타내는 UNIX 타임스탬프입니다.
소스 유형	uint32	데이터 소스의 유형에 매핑되는 번호입니다. • 0 - RNA에서 서버 데이터를 제공한 경우 • 1 - 사용자가 서버 데이터를 제공한 경우 • 2 - 서드파티 스캐너에서 클라이언트 데이터를 제공한 경우 • 3 - nmimport.pl 등의 커맨드 라인 툴이나 호스트 입력 API 클라이언트에서 서버 데이터를 제공한 경우
소스 ID	uint32	서버 데이터 소스에 매핑되는 ID 번호입니다. 소스 유형에 따라 RNA, 사용자, 스캐너 또는 서드파티 애플리케이션에 매핑될 수 있습니다.
목록 블록 유형	uint32	하위 서버 데이터를 전달하는 전체 서버 정보 데이터 블록으로 구성된 목록 데이터 블록을 시작합니다. 이 값은 항상 11입니다.
목록 블록 길이	uint32	목록의 바이트 수입니다. 이 수에는 목록 블록 유형 및 길이 필드의 8바이트에 캡슐화된 모든 전체 하위 서버 데이터 블록을 더한 값이 포함됩니다. 이 필드 뒤에는 전체 하위 서버 데이터 블록이 없을 수도 있고 하나 이상 올 수도 있습니다.

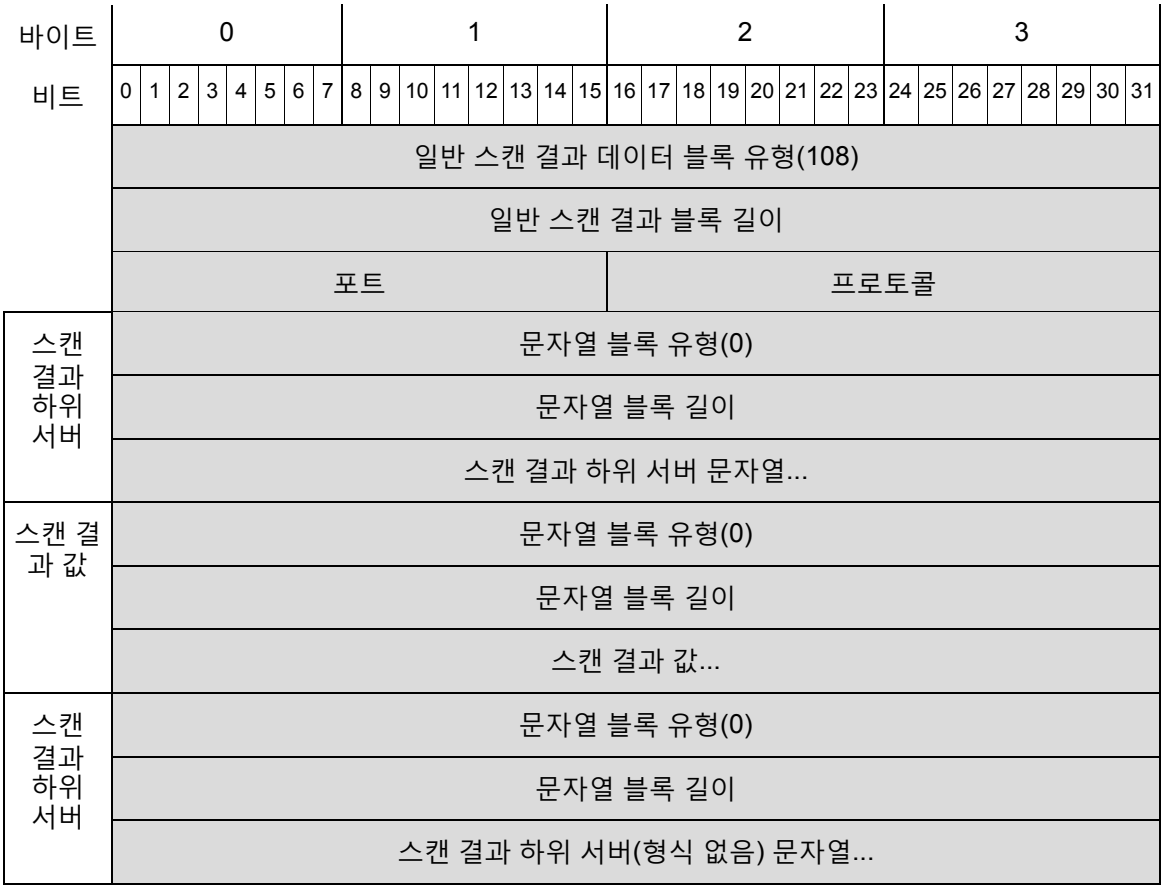
표 4-75 전체 서버 정보 데이터 블록 필드 (계속)

필드	데이터 유형	설명
전체 하위 서버 블록 유형	uint32	첫 번째 전체 하위 서버 데이터 블록을 시작합니다. 이 데이터 블록 뒤에는 목록 블록 길이 필드에 정의된 제한까지 다른 전체 하위 서버 데이터 블록이 올 수 있습니다.
전체 하위 서버 블록 길이	uint32	각 전체 하위 서버 데이터 블록의 총 바이트 수입니다. 여기에는 전체 하위 서버 블록 유형 및 길이 필드의 8바이트에 그 뒤의 데이터 바이트 수를 더한 값이 포함됩니다.
전체 하위 서버 데이터 블록*	uint32	서버의 하위 서버를 포함하는 전체 하위 서버 데이터 블록입니다. 이 데이터 블록에 대한 설명은 전체 하위 서버 데이터 블록, 4-84페이지의 내용을 참조하십시오.

4.10.0 이상 버전용 일반 스캔 결과 데이터 블록

일반 스캔 결과 데이터 블록은 스캔 결과를 포함하며 5.2 이상 버전용 스캔 결과 데이터 블록, 4-136페이지에서 사용됩니다. 계열 1 블록 그룹에서 일반 스캔 결과 데이터 블록의 블록 유형은 108입니다.

다음 다이어그램에 일반 스캔 결과 데이터 블록의 기본 구조가 나와 있습니다.



다음 표에는 일반 스캔 결과 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 4-76 일반 스캔 결과 데이터 블록 필드

필드	바이트 수	설명
일반 스캔 결과 데이터 블록 유형	uint32	일반 스캔 결과 데이터 블록을 시작합니다. 이 값은 항상 108입니다.
일반 스캔 결과 블록 길이	uint32	일반 스캔 결과 데이터 블록의 총 바이트 수입니다. 여기에는 일반 스캔 결과 블록 유형 및 길이 필드의 8바이트에 그 뒤의 스캔 결과 데이터 바이트 수를 더한 값이 포함됩니다.
포트	uint16	결과에서 취약점의 영향을 받는 서버가 사용하는 포트입니다.
프로토콜	uint16	IANA 프로토콜 번호 또는 이더 타입입니다. 이는 전송 계층 프로토콜과 네트워크 계층 프로토콜에서 서로 다르게 처리됩니다. 전송 계층 프로토콜은 IANA 프로토콜 번호로 식별됩니다. 예를 들면 다음과 같습니다. • 6 - TCP • 17 - UDP 네트워크 계층 프로토콜은 IEEE 등록 기관 이더 타입의 10진수 형식으로 식별됩니다. 예를 들면 다음과 같습니다. • 2048 - IP
문자열 블록 유형	uint32	하위 서버가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	하위 서버 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 하위 서버의 바이트 수를 더한 값이 포함됩니다.
스캔 결과 하위 서버	string	하위 서버입니다.
문자열 블록 유형	uint32	값이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	값 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 값의 바이트 수를 더한 값이 포함됩니다.
스캔 결과 값	string	스캔 결과 값입니다.
문자열 블록 유형	uint32	하위 서버가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.

표 4-76 일반 스캔 결과 데이터 블록 필드 (계속)

필드	바이트 수	설명
문자열 블록 길이	uint32	하위 서버 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 하위 서버의 바이트 수를 더한 값이 포함됩니다.
스캔 결과 하위 서버	string	하위 서버(형식 없음)입니다.
문자열 블록 유형	uint32	값이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	값 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 값의 바이트 수를 더한 값이 포함됩니다.
스캔 결과 값	string	스캔 결과 값(형식 없음)입니다.

4.10.0 이상 버전용 취약점 스캔 데이터 블록

취약점 스캔 데이터 블록은 취약점을 설명하며 스캔 결과 데이터 블록 내에서 사용됩니다. 스캔 결과 데이터 블록은 스캔 결과 추가 이벤트(이벤트 유형 1002, 하위 유형 11)에서 사용됩니다. 자세한 정보는 5.2 이상 버전용 스캔 결과 데이터 블록, 4-136페이지 및 스캔 결과 추가 메시지, 4-60페이지의 내용을 참조하십시오. 계열 1 블록 그룹에서 취약점 스캔 데이터 블록의 블록 유형은 109입니다.

다음 다이어그램에 취약점 스캔 데이터 블록의 형식이 나와 있습니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
설명	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	설명...																															
정상 이름	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	정상 취약점 이름...																															
설명 정상	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	정상 설명...																															
Bugtraq ID	목록 블록 유형(11)																															
	목록 블록 길이																															
	정수 데이터 블록(Bugtraq ID)...																															
CVE ID	목록 블록 유형(11)																															
	목록 블록 길이																															
	CVE ID...																															

다음 표에는 취약점 스캔 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 4-77 취약점 스캔 데이터 블록 필드

필드	데이터 유형	설명
취약점 스캔 블록 유형	uint32	취약점 스캔 데이터 블록을 시작합니다. 이 값은 항상 109입니다.
취약점 스캔 블록 길이	uint32	취약점 스캔 데이터 블록의 바이트 수입니다. 여기에는 취약점 스캔 블록 유형 및 길이 필드의 8바이트에 그 뒤의 취약점 스캔 데이터 바이트 수를 더한 값이 포함됩니다.
포트	uint16	취약점의 영향을 받는 하위 서버가 사용하는 포트입니다.

표 4-77 취약점 스캔 데이터 블록 필드 (계속)

필드	데이터 유형	설명
프로토콜	uint16	IANA 프로토콜 번호 또는 이더 타입입니다. 이는 전송 계층 프로토콜과 네트워크 계층 프로토콜에서 서로 다르게 처리됩니다. 전송 계층 프로토콜은 IANA 프로토콜 번호로 식별됩니다. 예를 들면 다음과 같습니다. • 6 - TCP • 17 - UDP 네트워크 계층 프로토콜은 IEEE 등록 기관 이더 타입의 10진수 형식으로 식별됩니다. 예를 들면 다음과 같습니다. • 2048 - IP
문자열 블록 유형	uint32	ID에 대한 문자열 데이터 블록을 시작합니다.
문자열 블록 길이	uint32	ID에 대한 문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이의 8바이트에 ID의 바이트 수를 더한 값이 포함됩니다.
ID	string	보고된 취약점을 탐지한 스캔 유틸리티에서 지정한 해당 취약점의 ID입니다. 예를 들어 Qualys 스캔에서 탐지된 취약점의 경우 이 필드에는 Qualys ID가 표시됩니다.
문자열 블록 유형	uint32	취약점 이름에 대한 문자열 데이터 블록을 시작합니다.
문자열 블록 길이	uint32	취약점 이름에 대한 문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이의 8바이트에 값의 취약점 이름의 바이트 수를 더한 값이 포함됩니다.
이름	string	취약점의 이름입니다.
문자열 블록 유형	uint32	취약점 설명에 대한 문자열 데이터 블록을 시작합니다.
문자열 블록 길이	uint32	취약점 설명에 대한 문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이의 8바이트에 값의 취약점 설명의 바이트 수를 더한 값이 포함됩니다.
설명	string	취약점의 설명입니다.
문자열 블록 유형	uint32	취약점 이름에 대한 문자열 데이터 블록을 시작합니다.
문자열 블록 길이	uint32	취약점 이름에 대한 문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이의 8바이트에 값의 취약점 이름의 바이트 수를 더한 값이 포함됩니다.
정상 이름	string	취약점의 이름(형식 없음)입니다.
문자열 블록 유형	uint32	취약점 설명에 대한 문자열 데이터 블록을 시작합니다.
문자열 블록 길이	uint32	취약점 설명에 대한 문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이의 8바이트에 값의 취약점 설명의 바이트 수를 더한 값이 포함됩니다.
정상 설명	string	취약점의 설명(형식 없음)입니다.
목록 블록 유형	uint32	Bugtraq ID 번호 목록에 대한 목록 데이터 블록을 시작합니다.

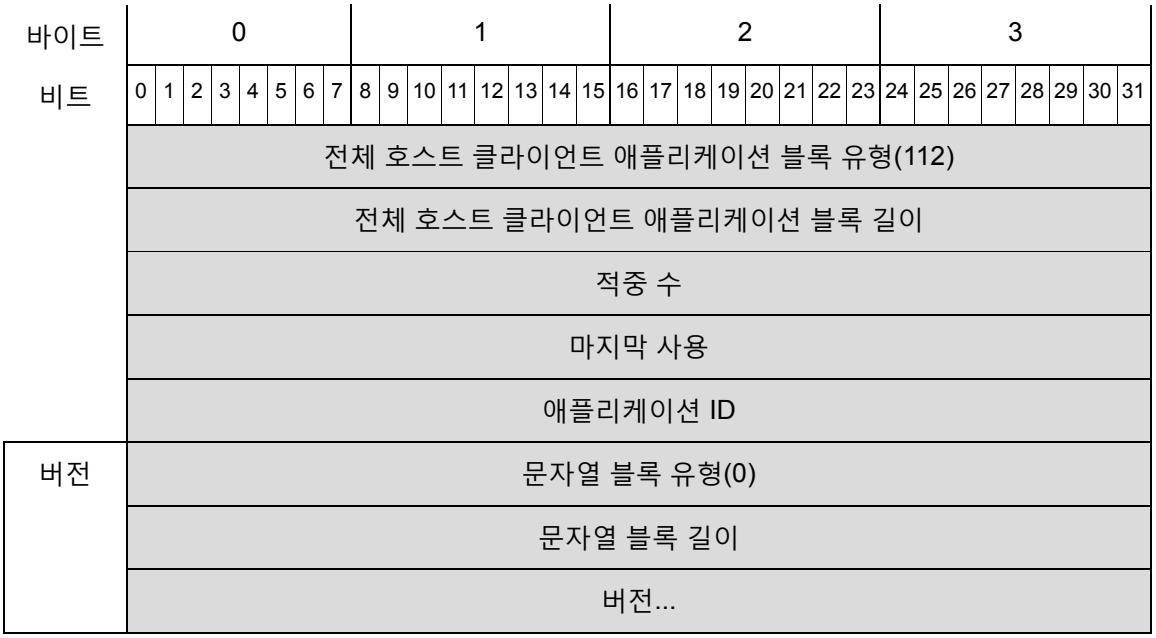
표 4-77 취약점 스캔 데이터 블록 필드 (계속)

필드	데이터 유형	설명
목록 블록 길이	uint32	Bugtraq ID 번호 목록에 대한 목록 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이의 8바이트에 Bugtraq ID가 포함된 정수 데이터 블록의 바이트 수를 더한 값이 포함됩니다.
Bugtraq ID	string	Bugtraq ID 번호 목록을 구성하는 0개 이상의 정수(INT32) 데이터 블록을 포함합니다. 이러한 데이터 블록에 대한 자세한 정보는 정수(INT32) 데이터 블록, 4-78페이지의 내용을 참조하십시오.
목록 블록 유형	uint32	CVE(일반 취약점 및 노출) ID 번호 목록에 대한 목록 데이터 블록을 시작합니다.
목록 블록 길이	uint32	CVE ID 번호에 대한 목록 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이의 8바이트에 CVE ID 번호의 바이트 수를 더한 값이 포함됩니다.
CVE ID	string	CVE ID 번호 목록을 구성하는 0개 이상의 문자열 정보 데이터 블록을 포함합니다. 이러한 데이터 블록에 대한 자세한 정보는 문자열 정보 데이터 블록, 4-80페이지의 내용을 참조하십시오.

5.0 이상 버전용 전체 호스트 클라이언트 애플리케이션 데이터 블록

5.0 이상 버전용 전체 호스트 클라이언트 애플리케이션 데이터 블록은 클라이언트 애플리케이션을 설명하며 관련된 웹 애플리케이션 및 취약점의 추가 목록을 제공합니다. 전체 호스트 클라이언트 애플리케이션 데이터 블록은 전체 호스트 프로파일 데이터 블록(유형 111) 내에서 사용됩니다. 계열 1 블록 그룹에서 이 데이터 블록의 블록 유형은 112입니다.

다음 다이어그램에 5.0 이상 버전용 전체 호스트 클라이언트 애플리케이션 데이터 블록의 기본 구조가 나와 있습니다.



바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
웹 애플리케이션	웹 애플리케이션 블록 유형(123)*																															
	웹 애플리케이션 블록 길이																															
	웹 애플리케이션 데이터...																															
	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
취약점	취약점 블록 유형(85)*																															
	취약점 블록 길이																															
	취약점 데이터...																															

다음 표에는 전체 호스트 클라이언트 애플리케이션 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 4-78 5.0 이상 버전용 전체 호스트 클라이언트 애플리케이션 데이터 블록 필드

필드	데이터 유형	설명
전체 호스트 클라이언트 애플리케이션 블록 유형	uint32	전체 호스트 클라이언트 애플리케이션 데이터 블록을 시작합니다. 이 값은 항상 112입니다.
전체 호스트 클라이언트 애플리케이션 블록 길이	uint32	전체 호스트 클라이언트 애플리케이션 데이터 블록의 바이트 수입니다. 여기에는 클라이언트 애플리케이션 블록 유형 및 길이의 8바이트에 그 뒤의 클라이언트 애플리케이션 데이터 바이트 수를 더한 값이 포함됩니다.
적중 수	uint32	시스템이 사용 중인 클라이언트 애플리케이션을 탐지한 횟수입니다.
마지막 사용	uint32	시스템이 사용 중인 클라이언트를 마지막으로 탐지한 시간을 나타내는 UNIX 타임스탬프입니다.
애플리케이션 ID	uint32	해당하는 경우 탐지된 클라이언트 애플리케이션의 애플리케이션 ID입니다.
문자열 블록 유형	uint32	클라이언트 애플리케이션 버전에 대한 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.

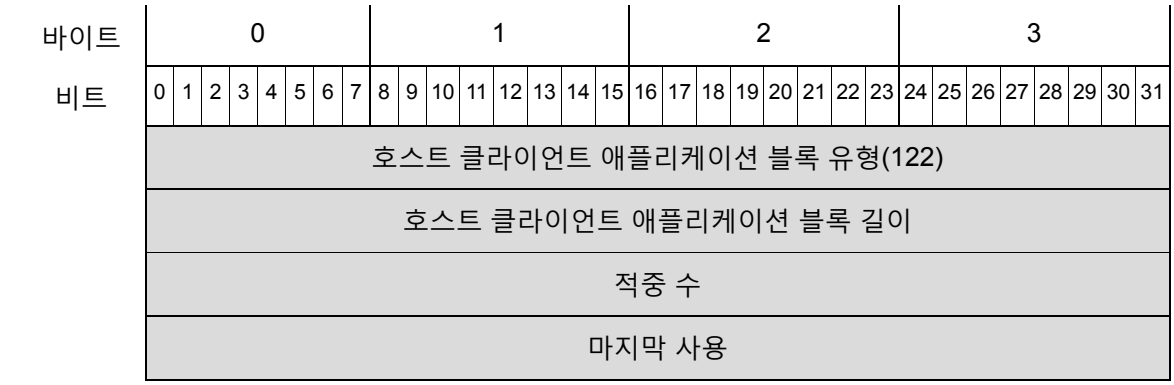
표 4-78 5.0 이상 버전용 전체 호스트 클라이언트 애플리케이션 데이터 블록 필드 (계속)

필드	데이터 유형	설명
문자열 블록 길이	uint32	클라이언트 애플리케이션 이름에 대한 문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이의 8바이트에 클라이언트 애플리케이션 버전의 바이트 수를 더한 값이 포함됩니다.
버전	string	클라이언트 애플리케이션 버전입니다.
일반 목록 블록 유형	uint32	일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	일반 목록 블록과 캡슐화된 웹 애플리케이션 데이터 블록의 바이트 수입니다. 이 수에는 일반 목록 블록 헤더 필드의 8바이트에 캡슐화된 모든 데이터 블록의 바이트 수를 더한 값이 포함됩니다.
웹 애플리케이션 데이터 블록	variable	캡슐화된 웹 애플리케이션 데이터 블록(일반 목록 블록 길이의 최대 바이트 수까지)입니다.
일반 목록 블록 유형	uint32	일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	일반 목록 블록과 캡슐화된 취약점 데이터 블록의 바이트 수입니다. 이 수에는 일반 목록 블록 헤더 필드의 8바이트에 캡슐화된 모든 취약점 데이터 블록의 바이트 수를 더한 값이 포함됩니다.
취약점 데이터 블록	variable	캡슐화된 취약점 데이터 블록(일반 목록 블록 길이의 최대 바이트 수까지)입니다.

5.0 이상 버전용 호스트 클라이언트 애플리케이션 데이터 블록

5.0 이상 버전용 호스트 클라이언트 애플리케이션 데이터 블록은 클라이언트 애플리케이션을 설명하며 새 클라이언트 애플리케이션 이벤트(이벤트 유형 1000, 하위 유형 7), 클라이언트 애플리케이션 시간 초과 이벤트(이벤트 유형 1001, 하위 유형 20) 및 클라이언트 애플리케이션 업데이트 이벤트(이벤트 유형 1001, 하위 유형 32) 내에서 사용됩니다. 계열 1 블록 그룹에서 4.10.2 이상 버전용 호스트 클라이언트 애플리케이션 데이터 블록의 블록 유형은 122입니다.

다음 다이어그램에 5.0 이상 버전용 호스트 클라이언트 애플리케이션 데이터 블록의 기본 구조가 나와 있습니다.



다음 표에는 호스트 클라이언트 애플리케이션 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 4-79 호스트 클라이언트 애플리케이션 데이터 블록 필드

필드	데이터 유형	설명
클라이언트 애플리케이션 블록 유형	uint32	호스트 클라이언트 애플리케이션 데이터 블록을 시작합니다. 이 값은 항상 122입니다.
클라이언트 애플리케이션 블록 길이	uint32	클라이언트 애플리케이션 데이터 블록의 바이트 수입니다. 여기에는 클라이언트 애플리케이션 블록 유형 및 길이의 8바이트에 그 뒤의 클라이언트 애플리케이션 데이터 바이트 수를 더한 값이 포함됩니다.
적중 수	uint32	시스템이 사용 중인 클라이언트 애플리케이션을 탐지한 횟수입니다.
마지막 사용	uint32	시스템이 사용 중인 클라이언트를 마지막으로 탐지한 시간을 나타내는 UNIX 타임스탬프입니다.
ID	uint32	해당하는 경우 탐지된 클라이언트 애플리케이션의 ID 번호입니다.
애플리케이션 프로토콜 ID	uint32	해당하는 경우 애플리케이션 프로토콜의 내부 ID 번호입니다.
문자열 블록 유형	uint32	클라이언트 애플리케이션 버전에 대한 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.

표 4-79 호스트 클라이언트 애플리케이션 데이터 블록 필드 (계속)

필드	데이터 유형	설명
문자열 블록 길이	uint32	클라이언트 애플리케이션 버전에 대한 문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이의 8바이트에 클라이언트 애플리케이션 버전의 바이트 수를 더한 값이 포함됩니다.
버전	string	클라이언트 애플리케이션 버전입니다.
일반 목록 블록 유형	uint32	일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	일반 목록 블록과 캡슐화된 웹 애플리케이션 데이터 블록의 바이트 수입니다. 이 수에는 일반 목록 블록 헤더 필드의 8바이트에 캡슐화된 모든 데이터 블록의 바이트 수를 더한 값이 포함됩니다.
웹 애플리케이션 데이터 블록	variable	캡슐화된 웹 애플리케이션 데이터 블록(목록 블록 길이의 최대 바이트 수까지)입니다. 캡슐화된 데이터 블록(블록 유형 123)에 대한 자세한 정보는 5.0 이상 버전용 웹 애플리케이션 데이터 블록, 4-119페이지의 내용을 참조하십시오.

5.0 이상 버전용 사용자 취약점 데이터 블록

사용자 취약점 데이터 블록은 취약점을 설명하며 사용자 취약점 변경 데이터 블록 내에서 사용됩니다. 사용자 취약점 변경 데이터 블록은 유효한 취약점 사용자 설정 이벤트와 유효하지 않은 취약점 사용자 설정 이벤트에서 사용됩니다. 계열 1 블록 그룹에서 5.0 이상 버전용 사용자 취약점 데이터 블록의 블록 유형은 124입니다. 이는 블록 유형 79를 대체합니다. 사용자 취약점 변경 데이터 블록에 대한 자세한 정보는 4.7 이상 버전용 사용자 취약점 변경 데이터 블록, 4-108페이지의 내용을 참조하십시오.

다음 다이어그램에 사용자 취약점 데이터 블록의 형식이 나와 있습니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
서드파티 취약점 UUID	서드파티 취약점 UUID																															
	UUID(계속)																															
	UUID(계속)																															
	UUID(계속)																															
	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	취약점 문자열...																															
	클라이언트 애플리케이션 ID																															
	애플리케이션 프로토콜 ID																															
	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	버전 문자열...																															

다음 표에는 사용자 취약점 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 4-80 사용자 취약점 데이터 블록 필드

필드	데이터 유형	설명
사용자 취약점 블록 유형	uint32	사용자 취약점 데이터 블록을 시작합니다. 이 값은 항상 124입니다.
사용자 취약점 블록 길이	uint32	사용자 취약점 데이터 블록의 바이트 수입니다. 여기에는 사용자 취약점 블록 유형 및 길이 필드의 8바이트에 그 뒤의 사용자 취약점 데이터 바이트 수를 더한 값이 포함됩니다.
일반 목록 블록 유형	uint32	IP 주소 범위 데이터를 전달하는 IP 범위 사양 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 IP 범위 사양 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
IP 범위 사양 데이터 블록*	variable	사용자 입력의 IP 주소 범위입니다. 이 데이터 블록에 대한 설명은 5.2 이상 버전용 IP 주소 범위 데이터 블록, 4-96페이지의 내용을 참조하십시오.
포트	uint16	취약점의 영향을 받는 서버가 사용하는 포트입니다. 클라이언트 애플리케이션 취약점의 경우 값은 0입니다.

표 4-80 사용자 취약점 데이터 블록 필드 (계속)

필드	데이터 유형	설명
프로토콜	uint16	취약점의 영향을 받는 서버가 사용하는 프로토콜의 이더 타입 또는 IANA 프로토콜 번호입니다. 이는 전송 계층 프로토콜과 네트워크 계층 프로토콜에서 서로 다르게 처리됩니다. 전송 계층 프로토콜은 IANA 프로토콜 번호로 식별됩니다. 예를 들면 다음과 같습니다. • 6 - TCP • 17 - UDP 네트워크 계층 프로토콜은 IEEE 등록 기관 이더 타입의 10진수 형식으로 식별됩니다. 예를 들면 다음과 같습니다. • 2048 - IP 클라이언트 애플리케이션 취약점의 경우 값은 0입니다.
취약점 ID	uint32	Cisco 취약점 ID입니다.
서드파티 취약점 UUID	uint8 [16]	서드파티 취약점의 고유 ID 번호(있는 경우)입니다. 그렇지 않은 경우 값은 0입니다.
문자열 블록 유형	uint32	취약점 이름에 대한 문자열 데이터 블록을 시작합니다. 값은 항상 0입니다.
문자열 블록 길이	uint32	취약점 이름에 대한 문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이의 8바이트에 값의 취약점 이름의 바이트 수를 더한 값이 포함됩니다.
취약점 이름	string	취약점 이름입니다.
클라이언트 애플리케이션 ID	uint32	클라이언트 애플리케이션의 애플리케이션 ID입니다. 서버 취약점의 경우 값은 0입니다.
애플리케이션 프로토콜 ID	uint32	클라이언트 애플리케이션이 사용하는 애플리케이션 프로토콜의 애플리케이션 ID입니다. 서버 취약점의 경우 값은 0입니다.
문자열 블록 유형	uint32	버전 문자열에 대한 문자열 데이터 블록을 시작합니다. 값은 항상 0입니다.
문자열 블록 길이	uint32	버전에 대한 문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이의 8바이트에 클라이언트 애플리케이션 버전 문자열의 바이트 수를 더한 값이 포함됩니다.
버전	string	클라이언트 애플리케이션 버전입니다. 서버 취약점의 경우 값은 0입니다.

5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록

계열 1 블록 그룹에서 운영 체제 핑거프린트 데이터 블록의 블록 유형은 130입니다. 이 블록은 핑거프린트 UUID(범용 고유 식별자)와 핑거프린트 유형, 핑거프린트 소스 유형 및 핑거프린트 소스 ID를 포함합니다.

다음 다이어그램에 5.1 이상 버전의 운영 체제 핑거프린트 데이터 블록 형식이 나와 있습니다.

<table>
<tr><td>바이트</td><td colspan="8">0</td><td colspan="8">1</td><td colspan="8">2</td><td colspan="8">3</td></tr>
<tr><td>비트</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td></tr>
<tr><td></td><td colspan="32">운영 체제 핑거프린트 블록 유형(130)</td></tr>
<tr><td></td><td colspan="32">운영 체제 핑거프린트 블록 길이</td></tr>
<tr><td rowspan="4">OS 핑거프린트 UUID</td><td colspan="32">핑거프린트 UUID</td></tr>
<tr><td colspan="32">핑거프린트 UUID(계속)</td></tr>
<tr><td colspan="32">핑거프린트 UUID(계속)</td></tr>
<tr><td colspan="32">핑거프린트 UUID(계속)</td></tr>
<tr><td rowspan="4"></td><td colspan="32">핑거프린트 유형</td></tr>
<tr><td colspan="32">핑거프린트 소스 유형</td></tr>
<tr><td colspan="32">핑거프린트 소스 ID</td></tr>
<tr><td colspan="32">마지막 확인</td></tr>
<tr><td rowspan="3">모바일 디바이스 정보</td><td colspan="8">TTL 차이</td><td colspan="24">일반 목록 블록 유형(31)</td></tr>
<tr><td colspan="8">일반 목록 블록 유형(계속)</td><td colspan="24">일반 목록 블록 길이</td></tr>
<tr><td colspan="8">일반 목록 블록 길이(계속)</td><td colspan="24">모바일 디바이스 정보 데이터 블록*</td></tr>
</table>

다음 표에는 운영 체제 핑거프린트 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 4-81 운영 체제 핑거프린트 데이터 블록 필드

필드	데이터 유형	설명
운영 체제 핑거프린트 데이터 블록 유형	uint32	운영 체제 데이터 블록을 시작합니다. 이 값은 항상 130입니다.
운영 체제 데이터 블록 길이	uint32	운영 체제 핑거프린트 데이터 블록의 바이트 수입니다. 여기에는 운영 체제 핑거프린트 데이터 블록의 블록 유형 및 길이 8바이트에 그 뒤의 운영 체제 핑거프린트 데이터 바이트 수를 더한 값이 포함됩니다.
핑거프린트 UUID	uint8[16]	운영 체제의 고유 식별자 역할을 하는 옥텟 형식의 핑거프린트 ID 번호입니다. 핑거프린트 UUID는 VDB(취약점 데이터베이스)의 운영 체제 이름, 벤더 및 버전에 매핑됩니다.
핑거프린트 유형	uint32	핑거프린트의 유형을 나타냅니다.
핑거프린트 소스 유형	uint32	운영 체제 핑거프린트를 제공한 소스의 유형(예: 사용자 또는 스캐너)을 나타냅니다.
핑거프린트 소스 ID	uint32	운영 체제 핑거프린트를 제공한 사용자의 로그인 이름에 매핑되는 ID 번호입니다.
마지막 확인	uint32	트래픽에서 핑거프린트가 마지막으로 확인된 시간을 나타냅니다.
TTL 차이	uint8	핑거프린트의 TTL 값과 호스트 핑거프린트를 생성하는 데 사용되는 패킷에서 확인된 TTL 값 간 차이를 나타냅니다.
일반 목록 블록 유형	uint32	일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	일반 목록 블록과 캡슐화된 데이터 블록의 바이트 수입니다. 이 수에는 일반 목록 블록 헤더 필드의 8바이트에 캡슐화된 모든 데이터 블록의 바이트 수를 더한 값이 포함됩니다.
모바일 디바이스 정보 데이터 블록	variable	캡슐화된 모바일 디바이스 정보 데이터 블록(목록 블록 길이의 최대 바이트 수까지)입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 모바일 디바이스 정보 데이터 블록, 4-163페이지의 내용을 참조하십시오.

5.1 이상 버전용 모바일 디바이스 정보 데이터 블록

다음 다이어그램에 모바일 디바이스 정보 데이터 블록의 형식이 나와 있습니다. 이 데이터 블록에는 호스트가 마지막으로 탐지된 시간, 모바일 디바이스 정보 및 모바일 디바이스의 탈옥 여부가 포함됩니다. 계열 1 블록 그룹에서 모바일 디바이스 정보 데이터 블록의 블록 유형은 131입니다.

다음 표에는 5.1 이상 버전에서 반환되는 모바일 디바이스 정보 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 4-82 5.1 이상 버전용 모바일 디바이스 정보 데이터 블록 필드

필드	데이터 유형	설명
모바일 디바이스 정보 블록 유형(131)	uint32	운영 체제 데이터 블록을 시작합니다. 이 값은 항상 131입니다.
모바일 디바이스 정보 블록 길이	uint32	모바일 디바이스 정보 데이터 블록의 바이트 수입니다. 여기에는 모바일 디바이스 정보 데이터 블록 유형 및 길이의 8바이트에 그 뒤의 모바일 디바이스 정보 바이트 수를 더한 값이 포함됩니다.
문자열 블록 유형	uint32	모바일 디바이스 문자열에 대한 문자열 데이터 블록을 시작합니다. 이 값은 문자열 데이터를 나타내는 0으로 설정됩니다.
문자열 블록 길이	uint32	모바일 디바이스 문자열 데이터 블록의 바이트 수를 나타냅니다. 여기에는 문자열 블록 유형 및 길이 필드의 8바이트에 그 뒤의 모바일 디바이스 문자열 데이터 바이트 수를 더한 값이 포함됩니다.
모바일 디바이스 문자열 데이터	variable	탐지된 호스트의 모바일 디바이스 하드웨어 정보를 포함합니다.
모바일 디바이스 마지막 확인	uint32	모바일 디바이스가 마지막으로 확인된 타임스탬프를 포함합니다.

표 4-82 5.1 이상 버전용 모바일 디바이스 정보 데이터 블록 필드 (계속)

필드	데이터 유형	설명
모바일	uint32	호스트가 모바일 디바이스인지를 나타내는 true-false 플래그입니다.
탈옥됨	uint32	호스트가 탈옥된 모바일 디바이스인지를 나타내는 true-false 플래그입니다.

5.2 이상 버전용 호스트 프로파일 데이터 블록

다음 다이어그램에 호스트 프로파일 데이터 블록의 형식이 나와 있습니다. 또한 이 데이터 블록은 호스트 임계성 값은 포함하지 않지만 VLAN 유무 표시기는 포함합니다. 그리고 이 데이터 블록은 호스트의 NetBIOS 이름을 전달할 수 있습니다. 계열 1 블록 그룹에서 호스트 프로파일 데이터 블록의 블록 유형은 139입니다. 이 데이터 블록은 이제 IPv6 주소를 지원하며 클라이언트 애플리케이션 데이터 블록이 추가되었습니다.

참고 이 다이어그램에서 블록 유형 필드 옆에 있는 별표(*)는 메시지가 계열 1 데이터 블록 인스턴스를 포함하지 않을 수도 있고 하나 이상 포함할 수도 있음을 나타냅니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	호스트 프로파일 블록 유형(139)																															
	호스트 프로파일 블록 길이																															
	IP 주소 IP 주소(계속) IP 주소(계속) IP 주소(계속)																															
서버 핑거프린트	홉								기본/보조								일반 목록 블록 유형(31)															
	일반 목록 블록 유형(계속)																일반 목록 블록 길이															
	일반 목록 블록 길이(계속)																서버 핑거프린트 데이터 블록*															
클라이언트 핑거프린트	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
	클라이언트 핑거프린트 데이터 블록*																															

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
SMB 핑거프린트	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
	SMB 핑거프린트 데이터 블록*																															
DHCP 핑거프린트	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
	DHCP 핑거프린트 데이터 블록*																															
모바일 디바이스 핑거프린트	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
	모바일 디바이스 핑거프린트 데이터 블록*																															
IPv6 서버 핑거프린트	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
	IPv6 서버 핑거프린트 데이터 블록*																															
IPv6 클라이언트 핑거프린트	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
	IPv6 클라이언트 핑거프린트 데이터 블록*																															
IPv6 DHCP 핑거프린트	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
	IPv6 DHCP 핑거프린트 데이터 블록*																															
사용자 에이전트 핑거프린트	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
	사용자 에이전트 핑거프린트 데이터 블록*																															
TCP 서버 블록*	목록 블록 유형(11)																															TCP 목록 서버
	목록 블록 길이																															
	TCP 서버 데이터 블록																															

바이트	0								1								2								3								
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
UDP 서버 블록*	목록 블록 유형(11)																																UDP 목록 서버
	목록 블록 길이																																
	UDP 서버 데이터 블록																																
네트워크 프로토콜 블록*	목록 블록 유형(11)																																네트워크 목록 프로토콜
	목록 블록 길이																																
	네트워크 프로토콜 데이터 블록																																
전송 프로토콜 블록*	목록 블록 유형(11)																																전송 목록 프로토콜
	목록 블록 길이																																
	전송 프로토콜 데이터 블록																																
MAC 주소 블록*	목록 블록 유형(11)																																MAC 목록 주소
	목록 블록 길이																																
	호스트 MAC 주소 데이터 블록																																
	호스트 마지막 확인																																
	호스트 유형																																
	모바일								탈옥됨								VLAN 유무								VLAN ID								
클라이언트 앱 데이터	VLAN ID(계속)								VLAN 유형								VLAN 우선순위								일반 목록 블록 유형(31)								클라이언트 목록 애플리케이션
	일반 목록 블록 유형(31)(계속)																								일반 목록 블록 길이								
	일반 목록 블록 길이(계속)																								클라이언트 애플리케이션 데이터 블록								
NetBIOS 이름	문자열 블록 유형(0)																																
	문자열 블록 길이																																
	NetBIOS 문자열 데이터...																																

다음 표에는 5.2 이상 버전에서 반환되는 호스트 프로파일 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 4-83 5.2 이상 버전용 호스트 프로파일 데이터 블록 필드

필드	데이터 유형	설명
호스트프로파일 블록 유형	uint32	5.2 이상 버전용 호스트 프로파일 데이터 블록을 시작합니다. 이 값은 항상 139입니다.
호스트프로파일 블록 길이	uint32	호스트 프로파일 데이터 블록의 바이트 수입니다. 여기에는 호스트 프로파일 블록 유형 및 길이 필드의 8바이트에 그 뒤의 호스트 프로파일 데이터에 포함된 바이트 수를 더한 값이 포함됩니다.
IP 주소	uint8(16)	호스트의 IP 주소입니다. IPv4 또는 IPv6일 수 있습니다.
홉	uint8	호스트에서 디바이스로의 홉 수입니다.
기본/보조	uint8	호스트가 호스트를 탐지한 디바이스의 기본 네트워크에 있는지 아니면 보조 네트워크에 있는지를 나타냅니다. • 0 - 호스트가 기본 네트워크에 있습니다. • 1 - 호스트가 보조 네트워크에 있습니다.
일반 목록 블록 유형	uint32	서버 핑거프린트를 사용하여 식별된 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
운영 체제 핑거프린트(서버 핑거프린트) 데이터 블록*	variable	서버 핑거프린트를 사용하여 식별된 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 4-161페이지의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	클라이언트 핑거프린트를 사용하여 식별된 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
운영 체제 핑거프린트(클라이언트 핑거프린트) 데이터 블록*	variable	클라이언트 핑거프린트를 사용하여 식별된 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 4-161페이지의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	SMB 핑거프린트를 사용하여 식별된 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
운영 체제 핑거프린트(SMB 핑거프린트) 데이터 블록*	variable	SMB 핑거프린트를 사용하여 식별된 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 4-161페이지의 내용을 참조하십시오.

표 4-83 5.2 이상 버전용 호스트 프로파일 데이터 블록 필드 (계속)

필드	데이터 유형	설명
일반 목록 블록 유형	uint32	DHCP 핑거프린트를 사용하여 식별된 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
운영 체제 핑거프린트(DHCP 핑거프린트) 데이터 블록*	variable	DHCP 핑거프린트를 사용하여 식별된 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 4-161페이지의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	모바일 디바이스 핑거프린트를 사용하여 식별된 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
운영 체제 핑거프린트(모바일) 데이터 블록*	variable	모바일 디바이스 핑거프린트를 사용하여 식별된 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 4-161페이지의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	IPv6 서버 핑거프린트를 사용하여 식별된 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
운영 체제 핑거프린트(IPv6 서버) 데이터 블록*	variable	IPv6 서버 핑거프린트를 사용하여 식별된 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 4-161페이지의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	IPv6 클라이언트 핑거프린트를 사용하여 식별된 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
운영 체제 핑거프린트(IPv6 클라이언트) 데이터 블록*	variable	IPv6 클라이언트 핑거프린트를 사용하여 식별된 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 4-161페이지의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	IPv6 DHCP 핑거프린트를 사용하여 식별된 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.

표 4-83 5.2 이상 버전용 호스트 프로파일 데이터 블록 필드 (계속)

필드	데이터 유형	설명
운영 체제 핑거프린트(IPv6 DHCP 핑거프린트) 데이터 블록*	variable	IPv6 DHCP 핑거프린트를 사용하여 식별된 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 4-161페이지의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	사용자 에이전트 핑거프린트를 사용하여 식별된 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
운영 체제 핑거프린트(사용자 에이전트 핑거프린트) 데이터 블록*	variable	사용자 에이전트 핑거프린트를 사용하여 식별된 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 4-161페이지의 내용을 참조하십시오.
목록 블록 유형	uint32	TCP 서버 데이터를 전달하는 서버 데이터 블록으로 구성된 목록 데이터 블록을 시작합니다. 이 값은 항상 11입니다.
목록 블록 길이	uint32	목록의 바이트 수입니다. 이 수에는 목록 블록 유형 및 길이 필드의 8바이트에 캡슐화된 모든 서버 데이터 블록을 더한 값이 포함됩니다. 이 필드 뒤에는 서버 데이터 블록이 없을 수도 있고 하나 이상 올 수도 있습니다.
TCP 서버 데이터 블록	variable	TCP 서버를 설명하는 호스트 서버 데이터 블록입니다. 이 데이터 블록에 대한 설명은 4.10.0 이상 버전용 호스트 서버 데이터 블록, 4-138페이지의 내용을 참조하십시오.
목록 블록 유형	uint32	UDP 서버 데이터를 전달하는 서버 데이터 블록으로 구성된 목록 데이터 블록을 시작합니다. 이 값은 항상 11입니다.
목록 블록 길이	uint32	목록의 바이트 수입니다. 이 수에는 목록 블록 유형 및 길이 필드의 8바이트에 캡슐화된 모든 서버 데이터 블록을 더한 값이 포함됩니다. 이 필드 뒤에는 서버 데이터 블록이 없을 수도 있고 하나 이상 올 수도 있습니다.
UDP 서버 데이터 블록	uint32	UDP 서버를 설명하는 호스트 서버 데이터 블록입니다. 이 데이터 블록에 대한 설명은 4.10.0 이상 버전용 호스트 서버 데이터 블록, 4-138페이지의 내용을 참조하십시오.
목록 블록 유형	uint32	네트워크 프로토콜 데이터를 전달하는 프로토콜 데이터 블록으로 구성된 목록 데이터 블록을 시작합니다. 이 값은 항상 11입니다.
목록 블록 길이	uint32	목록의 바이트 수입니다. 이 수에는 목록 블록 유형 및 길이 필드의 8바이트에 캡슐화된 모든 프로토콜 데이터 블록을 더한 값이 포함됩니다. 이 필드 뒤에는 프로토콜 데이터 블록이 없을 수도 있고 하나 이상 올 수도 있습니다.

표 4-83 5.2 이상 버전용 호스트 프로파일 데이터 블록 필드 (계속)

필드	데이터 유형	설명
네트워크 프로토콜 데이터 블록	uint32	네트워크 프로토콜을 설명하는 프로토콜 데이터 블록입니다. 이 데이터 블록에 대한 설명은 프로토콜 데이터 블록, 4-77페이지의 내용을 참조하십시오.
목록 블록 유형	uint32	전송 프로토콜 데이터를 전달하는 프로토콜 데이터 블록으로 구성된 목록 데이터 블록을 시작합니다. 이 값은 항상 11입니다.
목록 블록 길이	uint32	목록의 바이트 수입니다. 이 수에는 목록 블록 유형 및 길이 필드의 8바이트에 캡슐화된 모든 프로토콜 데이터 블록을 더한 값이 포함됩니다. 이 필드 뒤에는 전송 프로토콜 데이터 블록이 없을 수도 있고 하나 이상 올 수도 있습니다.
전송 프로토콜 데이터 블록	uint32	전송 프로토콜을 설명하는 프로토콜 데이터 블록입니다. 이 데이터 블록에 대한 설명은 프로토콜 데이터 블록, 4-77페이지의 내용을 참조하십시오.
목록 블록 유형	uint32	MAC 주소 데이터 블록으로 구성된 목록 데이터 블록을 시작합니다. 이 값은 항상 11입니다.
목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 MAC 주소 데이터 블록을 포함한 목록의 바이트 수입니다.
호스트 MAC 주소 데이터 블록	uint32	호스트 MAC 주소를 설명하는 호스트 MAC 주소 데이터 블록입니다. 이 데이터 블록에 대한 설명은 4.9 이상 버전용 호스트 MAC 주소, 4-117페이지의 내용을 참조하십시오.
호스트 마지막 확인	uint32	시스템이 호스트 활동을 마지막으로 탐지한 시간을 나타내는 UNIX 타임스탬프입니다.
호스트 유형	uint32	호스트 유형을 나타냅니다. 다음 값이 표시될 수 있습니다. • 0 - 호스트 • 1 - 라우터 • 2 - 브리지 • 3 - NAT 디바이스 • 4 - LB(로드 밸런서)
모바일	uint8	호스트가 모바일 디바이스인지를 나타내는 true-false 플래그입니다.
탈옥됨	uint8	호스트가 탈옥도 된 모바일 디바이스인지를 나타내는 true-false 플래그입니다.
VLAN 유무	uint8	VLAN의 유무를 나타냅니다. • 0 - 예 • 1 - 아니요
VLAN ID	uint16	호스트가 구성원으로 포함된 VLAN을 나타내는 VLAN ID 번호입니다.
VLAN 유형	uint8	VLAN 태그에 캡슐화된 패킷 유형입니다.
VLAN 우선순위	uint8	VLAN 태그에 포함된 우선순위 값입니다.

표 4-83 5.2 이상 버전용 호스트 프로파일 데이터 블록 필드 (계속)

필드	데이터 유형	설명
문자열 블록 유형	uint32	호스트 클라이언트 애플리케이션 데이터에 대한 문자열 데이터 블록을 시작합니다. 이 값은 항상 112입니다.
문자열 블록 길이	uint32	문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이 필드의 8바이트에 호스트 클라이언트 애플리케이션 데이터의 바이트 수를 더한 값이 포함됩니다.
호스트 클라이언트애플리케이션 데이터 블록	variable	클라이언트 애플리케이션 데이터 블록의 목록입니다. 이 데이터 블록에 대한 설명은 5.0 이상 버전용 전체 호스트 클라이언트 애플리케이션 데이터 블록, 4-154페이지의 내용을 참조하십시오.
문자열 블록 유형	uint32	호스트 NetBIOS 이름에 대한 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이 필드의 8바이트에 NetBIOS 이름 문자열의 바이트 수를 더한 값이 포함됩니다.
NetBIOS 이름	string	호스트 NetBIOS 이름 문자열입니다.

5.1 이상 버전용 사용자 제품 데이터 블록

사용자 제품 데이터 블록은 서드파티 애플리케이션에서 가져온 호스트 입력 데이터(서드파티 애플리케이션 문자열 매핑 포함)를 전달합니다. 이 데이터 블록은 5.2 이상 버전용 스캔 결과 데이터 블록, 4-136페이지 및 사용자 서버 및 운영 체제 메시지, 4-58페이지에서 사용됩니다. 계열 1 블록 그룹에서 사용자 제품 데이터 블록의 블록 유형은 4.7~4.10.1 이전 버전의 경우 65, 4.10.2~5.0.x 버전의 경우 118, 5.1 이상 버전의 경우 134입니다. 블록 유형 65와 118의 구조는 동일합니다.

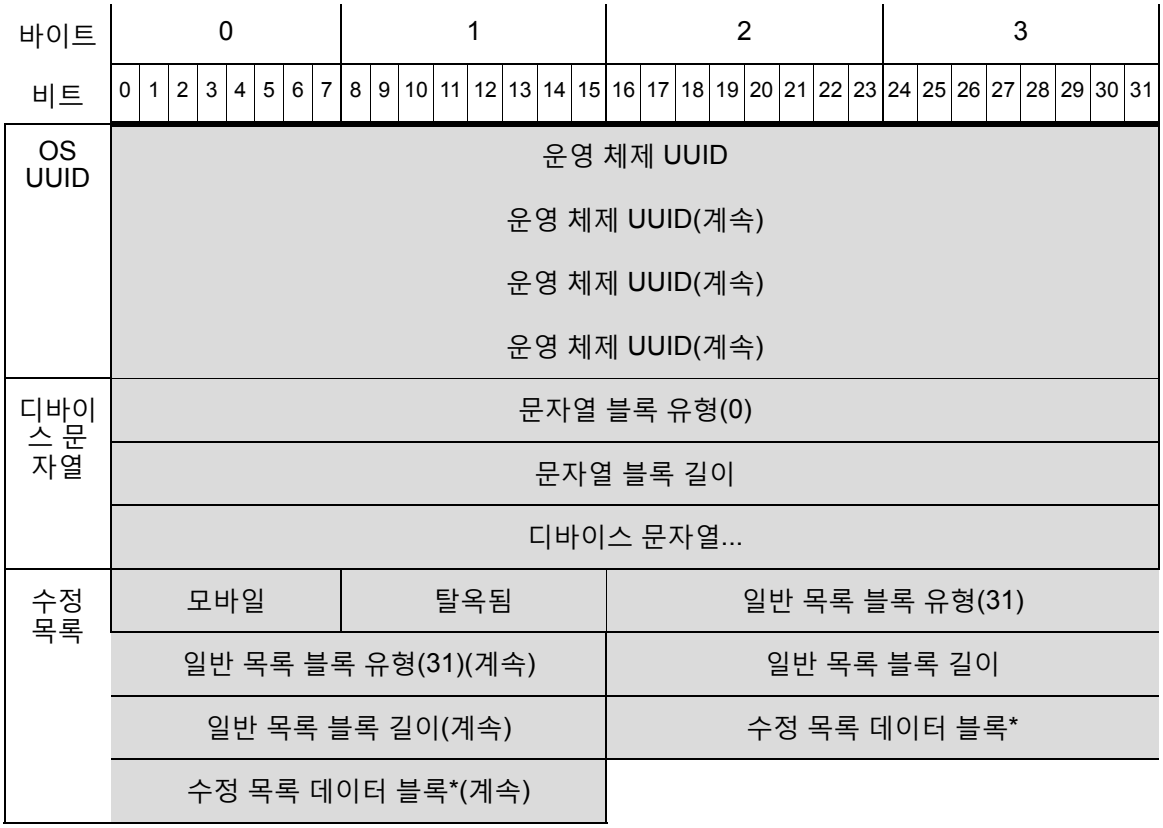
참고 다음 다이어그램에서 데이터 블록 이름 옆에 있는 별표(*)는 데이터 블록 인스턴스가 여러 개 나올 수 있음을 나타냅니다.

다음 다이어그램에 사용자 제품 데이터 블록의 형식이 나와 있습니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
사용자 제품 데이터 블록 유형(134)																																
사용자 제품 블록 길이																																
소스 ID																																
소스 유형																																


바이트
0
1
2
3
비트
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
IP 주소 범위
일반 목록 블록 유형(31)
일반 목록 블록 길이
IP 범위 사양 데이터 블록*
포트
프로토콜
사용자 제품 삭제
맞춤형 벤더 문자열
문자열 블록 유형(0)
문자열 블록 길이
맞춤형 벤더 문자열...
맞춤형 제품 문자열
문자열 블록 유형(0)
문자열 블록 길이
맞춤형 제품 문자열...
맞춤형 버전 문자열
문자열 블록 유형(0)
문자열 블록 길이
맞춤형 버전 문자열...
소프트웨어 ID
서버 ID
벤더 ID
제품 ID
주버전 문자열
문자열 블록 유형(0)
문자열 블록 길이
주 버전 문자열...
부버전 문자열
문자열 블록 유형(0)
문자열 블록 길이
부 버전 문자열...

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
수정 문자열	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	수정 문자열...																															
끝 주 버전 문자열	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	끝 주 버전 문자열...																															
끝 부 버전 문자열	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	끝 부 버전 문자열...																															
끝수정 문자열	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	끝 수정 문자열...																															
빌드 문자열	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	빌드 문자열...																															
패치 문자열	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	패치 문자열...																															
확장 문자열	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	확장 문자열...																															



다음 표에는 사용자 제품 데이터 블록의 구성 요소에 대한 설명이 나와 있습니다.

표 4-84 사용자 제품 데이터 블록 필드

필드	데이터 유형	설명
사용자 제품 데이터 블록 유형	uint32	사용자 제품 데이터 블록을 시작합니다. 5.1 이상 버전의 경우 이 값은 `134`입니다.
사용자 제품 블록 길이	uint32	사용자 제품 데이터 블록의 총 바이트 수입니다. 여기에는 사용자 제품 블록 유형 및 길이 필드의 8바이트에 그 뒤의 사용자 제품 데이터 바이트 수를 더한 값이 포함됩니다.
소스 ID	uint32	데이터를 가져온 소스에 매핑되는 ID 번호입니다. 소스 유형에 따라 RNA, 사용자, 스캐너 또는 서드파티 애플리케이션에 매핑될 수 있습니다.
소스 유형	uint32	데이터 소스의 유형에 매핑되는 번호입니다. • `0` - RNA에서 데이터를 제공한 경우 • `1` - 사용자가 데이터를 제공한 경우 • `2` - 서드파티 스캐너에서 데이터를 제공한 경우 • `3` - `nmimport.pl` 등의 커맨드 라인 툴이나 호스트 입력 API 클라이언트에서 데이터를 제공한 경우

표 4-84 사용자 제품 데이터 블록 필드 (계속)

필드	데이터 유형	설명
일반 목록 블록 유형	uint32	IP 주소 범위 데이터를 전달하는 IP 범위 사양 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 IP 범위 사양 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
IP 범위 사양 데이터 블록*	variable	사용자 입력의 IP 주소 범위에 대한 정보가 포함된 IP 범위 사양 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.2 이상 버전용 IP 주소 범위 데이터 블록, 4-96페이지의 내용을 참조하십시오.
포트	uint16	사용자가 지정한 포트입니다.
프로토콜	uint16	IANA 프로토콜 번호 또는 이더 타입입니다. 이는 전송 계층 프로토콜과 네트워크 계층 프로토콜에서 서로 다르게 처리됩니다. 전송 계층 프로토콜은 IANA 프로토콜 번호로 식별됩니다. 예를 들면 다음과 같습니다. • 6 - TCP • 17 - UDP 네트워크 계층 프로토콜은 IEEE 등록 기관 이더 타입의 10진수 형식으로 식별됩니다. 예를 들면 다음과 같습니다. • 2048 - IP
사용자 제품 삭제	uint32	사용자 OS 정의가 호스트에서 삭제되었는지를 나타냅니다. • 0 - 아니요 • 1 - 예
문자열 블록 유형	uint32	사용자 입력에 지정된 맞춤형 벤더 이름을 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	맞춤형 벤더 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 벤더 이름의 바이트 수를 더한 값이 포함됩니다.
맞춤형 벤더 이름	string	사용자 입력에 지정된 맞춤형 벤더 이름입니다.
문자열 블록 유형	uint32	사용자 입력에 지정된 맞춤형 제품 이름을 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	맞춤형 제품 이름 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 제품 이름의 바이트 수를 더한 값이 포함됩니다.
맞춤형 제품 이름	string	사용자 입력에 지정된 맞춤형 제품 이름입니다.
문자열 블록 유형	uint32	사용자 입력에 지정된 맞춤형 버전을 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	맞춤형 버전 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 버전의 바이트 수를 더한 값이 포함됩니다.
맞춤형 버전	string	사용자 입력에 지정된 맞춤형 버전입니다.

표 4-84 사용자 제품 데이터 블록 필드 (계속)

필드	데이터 유형	설명
소프트웨어 ID	uint32	데이터베이스 내 서버 또는 운영 체제의 특정 수정에 대한 식별자입니다.
서버 ID	uint32	사용자 입력에 지정된 호스트 서버의 애플리케이션 프로토콜에 대한 Firepower System 애플리케이션 식별자입니다.
벤더 ID	uint32	지정한 서드파티 운영 체제가 Firepower System OS 정의에 매핑될 때 해당 서드파티 운영 체제의 벤더 식별자입니다.
제품 ID	uint32	지정한 서드파티 운영 체제 문자열이 Firepower System OS 정의에 매핑될 때 해당 서드파티 운영 체제 문자열의 제품 ID 문자열입니다.
문자열 블록 유형	uint32	사용자 입력의 서드파티 운영 체제 문자열이 매핑되는 Firepower System 운영 체제 정의의 주 버전 번호가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	주 버전 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 버전의 바이트 수를 더한 값이 포함됩니다.
주 버전	string	서드파티 OS 문자열이 매핑되는 Firepower System 운영 체제 정의의 주 버전입니다.
문자열 블록 유형	uint32	서드파티 OS 문자열이 매핑되는 Firepower System 운영 체제 정의의 부 버전 번호가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	부 버전 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 버전의 바이트 수를 더한 값이 포함됩니다.
부 버전	string	사용자 입력의 서드파티 OS 문자열이 매핑되는 Firepower System 운영 체제 정의의 부 버전 번호입니다.
문자열 블록 유형	uint32	사용자 입력의 서드파티 운영 체제 문자열이 매핑되는 Firepower System 운영 체제 정의의 수정 번호가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	수정 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 수정 번호의 바이트 수를 더한 값이 포함됩니다.
수정	string	사용자 입력의 서드파티 OS 문자열이 매핑되는 Firepower System 운영 체제 정의의 수정 번호입니다.
문자열 블록 유형	uint32	서드파티 운영 체제 문자열이 매핑되는 Firepower System 운영 체제 정의의 마지막 주 버전이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	끝 주 버전 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 버전의 바이트 수를 더한 값이 포함됩니다.
끝 주 버전	string	사용자 입력의 서드파티 OS 문자열이 매핑되는 Firepower System 운영 체제 정의의 주 버전 번호 범위에서 마지막 버전 번호입니다.

표 4-84 사용자 제품 데이터 블록 필드 (계속)

필드	데이터 유형	설명
문자열 블록 유형	uint32	서드파티 운영 체제 문자열이 매핑되는 Firepower System 운영 체제 정의의 마지막 부 버전이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	끝 부 버전 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 버전의 바이트 수를 더한 값이 포함됩니다.
끝 부 버전	string	사용자 입력의 서드파티 OS 문자열이 매핑되는 Firepower System 운영 체제 정의의 부 버전 번호 범위에서 마지막 버전 번호입니다.
문자열 블록 유형	uint32	서드파티 OS 문자열이 매핑되는 Firepower System 운영 체제 정의의 마지막 수정 번호가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	끝 수정 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 수정 번호의 바이트 수를 더한 값이 포함됩니다.
끝 수정	string	사용자 입력의 서드파티 OS 문자열이 매핑되는 Firepower System 운영 체제 정의의 수정 번호 범위에서 마지막 수정 번호입니다.
문자열 블록 유형	uint32	서드파티 OS 문자열이 매핑되는 Firepower System 운영 체제의 빌드 번호가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	빌드 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 빌드 번호의 바이트 수를 더한 값이 포함됩니다.
빌드	string	사용자 입력의 서드파티 OS 문자열이 매핑되는 Firepower System 운영 체제의 빌드 번호입니다.
문자열 블록 유형	uint32	서드파티 OS 문자열이 매핑되는 Firepower System 운영 체제의 패치 번호가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	패치 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 패치 번호의 바이트 수를 더한 값이 포함됩니다.
패치	string	사용자 입력의 서드파티 OS 문자열이 매핑되는 Firepower System 운영 체제의 패치 번호입니다.
문자열 블록 유형	uint32	서드파티 운영 체제 문자열이 매핑되는 Firepower System OS의 확장 번호가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	확장 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 확장 번호의 바이트 수를 더한 값이 포함됩니다.
확장	string	사용자 입력의 서드파티 OS 문자열이 매핑되는 Firepower System 운영 체제의 확장 번호입니다.
UUID	uint8 [x16]	운영 체제의 고유 ID 번호를 포함합니다.

표 4-84 사용자 제품 데이터 블록 필드 (계속)

필드	데이터 유형	설명
문자열 블록 유형	uint32	사용자 입력의 디바이스 하드웨어 정보를 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	빌드 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 빌드 번호의 바이트 수를 더한 값이 포함됩니다.
디바이스 문자열	string	모바일 디바이스 하드웨어 정보입니다.
모바일	uint8	운영 체제가 모바일 디바이스에서 실행되고 있는지를 나타내는 true-false 플래그입니다.
탈옥됨	uint8	모바일 디바이스의 운영 체제가 탈옥되었는지 나타내는 true-false 플래그입니다.
일반 목록 블록 유형	uint32	지정한 IP 주소 범위의 호스트에 적용된 수정과 관련한 사용자 입력 데이터를 전달하는 수정 목록 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 수정 목록 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
수정 목록 데이터 블록*	variable	호스트에 적용된 수정에 대한 정보를 포함하는 수정 목록 데이터 블록입니다. 이 데이터 블록에 대한 설명은 수정 목록 데이터 블록, 4-103페이지의 내용을 참조하십시오.

사용자 데이터 블록

사용자 데이터 블록은 사용자 이벤트 메시지에 표시되며 계열 1 데이터 블록의 하위 집합입니다. 계열 1 데이터 블록의 일반 형식에 대한 자세한 정보는 검색(계열 1) 블록 이해, 4-63페이지의 내용을 참조하십시오.

참고 사용자 데이터 블록 헤더의 데이터 블록 길이 필드에는 데이터 블록의 바이트 수가 포함됩니다. 여기에는 2개 데이터 블록 헤더 필드의 8바이트가 포함됩니다.

다음 표에는 사용자 이벤트 메시지에 표시될 수 있는 사용자 데이터 블록이 나와 있습니다. 데이터 블록은 데이터 블록 유형을 기준으로 나열됩니다. 현재 데이터 블록은 최신 버전입니다. 레거시 블록은 지원되기는 하지만 현재 Firepower System 버전에서 생성되지는 않는 블록입니다.

표 4-85 사용자 데이터 블록 유형

유형	콘텐츠	데이터 블록 카테고리	설명
73	사용자 로그인 정보	레거시	시스템에서 탐지한 사용자의 로그인 정보 변경 사항이 포함됩니다. 자세한 정보는 5.0~5.0.2 버전용 사용자 로그인 정보 데이터 블록, B-104페이지의 내용을 참조하십시오. 버전 5.0용으로 도입된 후속 버전 블록 유형의 구조는 블록 유형 73과 동일하지만 필드의 데이터는 다릅니다.
74	사용자 계정 업데이트 메시지	현재	사용자 계정 정보의 변경 사항이 포함됩니다. 자세한 정보는 사용자 계정 업데이트 메시지 데이터 블록, 4-180페이지의 내용을 참조하십시오.
75	4.7~4.10.x 버전의 사용자 정보	레거시	시스템에서 탐지한 사용자의 정보 변경 사항이 포함됩니다. 자세한 정보는 5.x 버전용 사용자 정보 데이터 블록, B-117페이지의 내용을 참조하십시오. 버전 6.0용으로 도입된 후속 버전 블록의 블록 유형은 158입니다.
120	5.x 버전의 사용자 정보	현재	시스템에서 탐지한 사용자의 정보 변경 사항이 포함됩니다. 자세한 정보는 5.x 버전용 사용자 정보 데이터 블록, B-117페이지의 내용을 참조하십시오. 블록 유형 75를 대체하며 이는 블록 유형 158로 대체됩니다.
121	사용자 로그인 정보	레거시	시스템에서 탐지한 사용자의 로그인 정보 변경 사항이 포함됩니다. 자세한 정보는 5.0~5.0.2 버전용 사용자 로그인 정보 데이터 블록, B-104페이지의 내용을 참조하십시오. 이벤트에서 탐지된 애플리케이션 프로토콜 ID에 해당하는 5.0 이상 버전의 애플리케이션 ID를 저장하는 Protocol(프로토콜) 필드의 콘텐츠에 포함된 블록 73과는 다릅니다. 버전 5.1용으로 도입된 후속 버전 블록의 블록 유형은 127입니다.
127	사용자 로그인 정보	레거시	시스템에서 탐지한 사용자의 로그인 정보 변경 사항이 포함됩니다. 자세한 정보는 5.1~5.4.x 버전용 사용자 로그인 정보 데이터 블록, B-105페이지의 내용을 참조하십시오. 이는 블록 유형 121을 대체합니다. 6.0용으로 도입된 후속 버전 블록의 블록 유형은 159입니다.
150	IOC 상태	현재	보안 침해에 대한 정보를 포함합니다. 자세한 정보는 5.3 이상 버전용 IOC 상태 데이터 블록, 4-35페이지의 내용을 참조하십시오.
158	6.0 이상 버전의 사용자 정보	현재	시스템에서 탐지한 사용자의 정보 변경 사항이 포함됩니다. 자세한 정보는 6.0 이상 버전용 사용자 정보 데이터 블록, 4-189페이지의 내용을 참조하십시오. 블록 유형 120을 대체합니다.
159	사용자 로그인 정보	레거시	시스템에서 탐지한 사용자의 로그인 정보 변경 사항이 포함됩니다. 자세한 정보는 6.0.x 버전용 사용자 로그인 정보 데이터 블록, B-107페이지의 내용을 참조하십시오. 이는 블록 유형 127을 대체합니다.

표 4-85 사용자 데이터 블록 유형(계속)

유형	콘텐츠	데이터 블록 카테고리	설명
165	사용자 로그인 정보	레거시	시스템에서 탐지한 사용자의 로그인 정보 변경 사항이 포함됩니다. 자세한 정보는 6.1.x 버전용 사용자 로그인 정보 데이터 블록, B-114페이지의 내용을 참조하십시오. 이는 블록 유형 159를 대체합니다. 이는 블록 유형 167로 대체됩니다.
166	VPN 세션 정보	현재	시스템에서 탐지한 VPN 세션의 정보가 포함됩니다. 자세한 정보는 6.2 이상 버전용 VPN 세션 데이터 블록, 4-192페이지의 내용을 참조하십시오.
167	사용자 로그인 정보	현재	시스템에서 탐지한 사용자의 로그인 정보 변경 사항이 포함됩니다. 자세한 정보는 6.2 이상 버전용 사용자 로그인 정보 데이터 블록, 4-195페이지의 내용을 참조하십시오. 이는 블록 유형 165를 대체합니다.

사용자 계정 업데이트 메시지 데이터 블록

사용자 계정 업데이트 메시지 데이터 블록은 사용자 계정 정보 업데이트에 대한 정보를 전달합니다.

계열 1 블록 그룹에서 사용자 계정 업데이트 메시지 데이터 블록의 블록 유형은 74입니다.

다음 다이어그램에 사용자 계정 업데이트 메시지 데이터 블록의 형식이 나와 있습니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	사용자 계정 업데이트 메시지 블록 유형(74)																															
	사용자 계정 업데이트 메시지 블록 길이																															
사용자 이름	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	사용자 이름...																															
이름	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	이름...																															
중간 이니셜	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	중간 이니셜...																															

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
성	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	성...																															
전체 이름	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	전체 이름...																															
호칭	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	호칭...																															
직원 ID	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	직원 ID...																															
주소	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	주소...																															
시/군/구	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	시/군/구...																															
주/도	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	주/도...																															
국가/ 지역	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	국가/지역...																															

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
우편 번호	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	우편번호...																															
건물	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	건물...																															
위치	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	위치...																															
호	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	호...																															
회사	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	회사...																															
사업부	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	사업부...																															
부서	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	부서...																															
사무실	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	사무실...																															

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
메일 보관함	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	메일 보관함...																															
이메일	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	이메일...																															
전화	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	전화...																															
IP 폰	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	IP 폰...																															
사용자 1	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	사용자 1...																															
사용자 2	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	사용자 2...																															
사용자 3	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	사용자 3...																															
사용자 4	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	사용자 4...																															

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
이메일 별칭 1	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	이메일 별칭 1...																															
이메일 별칭 2	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	이메일 별칭 2...																															
이메일 별칭 3	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	이메일 별칭 3...																															

다음 표에는 사용자 계정 업데이트 메시지 데이터 블록의 구성 요소에 대한 설명이 나와 있습니다.

표 4-86 사용자 계정 업데이트 메시지 데이터 블록 필드

필드	데이터 유형	설명
사용자 계정 업데이트 메시지 블록 유형	uint32	사용자 계정 업데이트 메시지 데이터 블록을 시작합니다. 이 값은 항상 74입니다.
사용자 계정 업데이트 메시지 블록 길이	uint32	사용자 계정 업데이트 메시지 데이터 블록의 총 바이트 수입니다. 여기에는 사용자 계정 업데이트 메시지 블록 유형 및 길이 필드의 8바이트에 그 뒤의 사용자 계정 업데이트 메시지 데이터 바이트 수를 더한 값이 포함됩니다.
문자열 블록 유형	uint32	사용자의 사용자 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	사용자 이름 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 사용자 이름의 바이트 수를 더한 값이 포함됩니다.
사용자 이름	string	사용자의 사용자 이름입니다.
문자열 블록 유형	uint32	사용자의 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	이름 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 이름의 바이트 수를 더한 값이 포함됩니다.
이름	string	사용자의 이름입니다.

표 4-86 사용자 계정 업데이트 메시지 데이터 블록 필드 (계속)

필드	데이터 유형	설명
문자열 블록 유형	uint32	사용자의 중간 이니셜이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	중간 이니셜 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 중간 이니셜의 바이트 수를 더한 값이 포함됩니다.
중간 이니셜	string	사용자의 중간 이니셜입니다.
문자열 블록 유형	uint32	사용자의 성이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	성 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 성의 바이트 수를 더한 값이 포함됩니다.
성	string	사용자의 성입니다.
문자열 블록 유형	uint32	사용자의 전체 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	전체 이름 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 전체 이름의 바이트 수를 더한 값이 포함됩니다.
전체 이름	string	사용자의 전체 이름입니다.
문자열 블록 유형	uint32	사용자의 호칭이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	호칭 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 호칭의 바이트 수를 더한 값이 포함됩니다.
호칭	string	사용자의 호칭입니다.
문자열 블록 유형	uint32	사용자의 직원 ID가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	직원 ID 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 직원 ID의 바이트 수를 더한 값이 포함됩니다.
직원 ID	string	사용자의 직원 ID입니다.
문자열 블록 유형	uint32	사용자의 주소가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	주소 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 주소의 바이트 수를 더한 값이 포함됩니다.
주소	string	사용자의 주소입니다.
문자열 블록 유형	uint32	사용자 주소의 시/군/구가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	시/군/구 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 시/군/구의 바이트 수를 더한 값이 포함됩니다.

표 4-86 사용자 계정 업데이트 메시지 데이터 블록 필드 (계속)

필드	데이터 유형	설명
시/군/구	string	사용자 주소의 시/군/구입니다.
문자열 블록 유형	uint32	사용자 주소의 주/도가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	주/도 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 주/도의 바이트 수를 더한 값이 포함됩니다.
주/도	string	사용자의 주/도입니다.
문자열 블록 유형	uint32	사용자 주소의 국가 또는 지역이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	국가 또는 지역 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 국가 또는 지역의 바이트 수를 더한 값이 포함됩니다.
국가 또는 지역	string	사용자 주소의 국가 또는 지역입니다.
문자열 블록 유형	uint32	사용자 주소의 우편번호가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	우편번호 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 우편번호의 바이트 수를 더한 값이 포함됩니다.
우편번호	string	사용자 주소의 우편번호입니다.
문자열 블록 유형	uint32	사용자 주소의 건물이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	건물 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 건물 이름의 바이트 수를 더한 값이 포함됩니다.
건물	string	사용자 주소의 건물입니다.
문자열 블록 유형	uint32	사용자 주소의 위치가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	위치 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 위치 이름의 바이트 수를 더한 값이 포함됩니다.
위치	string	사용자 주소의 위치입니다.
문자열 블록 유형	uint32	사용자 주소의 호가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	호 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 호의 바이트 수를 더한 값이 포함됩니다.
호	string	사용자 주소의 호입니다.
문자열 블록 유형	uint32	사용자 주소의 회사가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.

표 4-86 사용자 계정 업데이트 메시지 데이터 블록 필드 (계속)

필드	데이터 유형	설명
문자열 블록 길이	uint32	회사 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 회사 이름의 바이트 수를 더한 값이 포함됩니다.
회사	string	사용자 주소의 회사입니다.
문자열 블록 유형	uint32	사용자 주소의 사업부가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	사업부 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 사업부 이름의 바이트 수를 더한 값이 포함됩니다.
사업부	string	사용자 주소의 사업부입니다.
문자열 블록 유형	uint32	사용자 주소의 부서가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	부서 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 부서의 바이트 수를 더한 값이 포함됩니다.
부서	string	사용자 주소의 부서입니다.
문자열 블록 유형	uint32	사용자 주소의 사무실이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	사무실 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 사무실의 바이트 수를 더한 값이 포함됩니다.
사무실	string	사용자 주소의 사무실입니다.
문자열 블록 유형	uint32	사용자 주소의 메일 보관함이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	메일 보관함 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 메일 보관함의 바이트 수를 더한 값이 포함됩니다.
메일 보관함	string	사용자 주소의 메일 보관함입니다.
문자열 블록 유형	uint32	사용자의 이메일 주소가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	이메일 주소 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 이메일 주소의 바이트 수를 더한 값이 포함됩니다.
이메일	string	사용자의 이메일 주소입니다.
문자열 블록 유형	uint32	사용자의 전화번호가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	전화번호 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 전화번호의 바이트 수를 더한 값이 포함됩니다.
전화	string	사용자의 전화번호입니다.

표 4-86 사용자 계정 업데이트 메시지 데이터 블록 필드 (계속)

필드	데이터 유형	설명
문자열 블록 유형	uint32	사용자의 인터넷 전화번호가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	인터넷 전화번호 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 인터넷 전화번호의 바이트 수를 더한 값이 포함됩니다.
인터넷 전화	string	사용자의 인터넷 전화번호입니다.
문자열 블록 유형	uint32	사용자의 대체 사용자 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	사용자 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 사용자 이름의 바이트 수를 더한 값이 포함됩니다.
사용자 1	string	사용자의 대체 사용자 이름입니다.
문자열 블록 유형	uint32	사용자의 대체 사용자 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	사용자 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 사용자 이름의 바이트 수를 더한 값이 포함됩니다.
사용자 2	string	사용자의 대체 사용자 이름입니다.
문자열 블록 유형	uint32	사용자의 대체 사용자 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	사용자 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 사용자 이름의 바이트 수를 더한 값이 포함됩니다.
사용자 3	string	사용자의 대체 사용자 이름입니다.
문자열 블록 유형	uint32	사용자의 대체 사용자 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	사용자 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 사용자 이름의 바이트 수를 더한 값이 포함됩니다.
사용자 4	string	사용자의 대체 사용자 이름입니다.
문자열 블록 유형	uint32	사용자의 이메일 별칭이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	이메일 별칭 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 이메일 별칭의 바이트 수를 더한 값이 포함됩니다.
이메일 별칭 1	string	사용자의 이메일 별칭입니다.
문자열 블록 유형	uint32	사용자의 이메일 별칭이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	이메일 별칭 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 이메일 별칭의 바이트 수를 더한 값이 포함됩니다.

표 4-86 사용자 계정 업데이트 메시지 데이터 블록 필드 (계속)

필드	데이터 유형	설명
이메일 별칭 2	string	사용자의 이메일 별칭입니다.
문자열 블록 유형	uint32	사용자의 이메일 별칭이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	이메일 별칭 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 이메일 별칭의 바이트 수를 더한 값이 포함됩니다.
이메일 별칭 3	string	사용자의 이메일 별칭입니다.

6.0 이상 버전용 사용자 정보 데이터 블록

사용자 정보 데이터 블록은 사용자 수정 메시지에서 사용되며 탐지, 제거 또는 삭제된 사용자에 대한 정보를 전달합니다. 자세한 정보는 사용자 수정 메시지, 4-62페이지의 내용을 참조하십시오.

계열 1 블록 그룹에서 사용자 정보 데이터 블록의 블록 유형은 6.0 이상 버전의 경우 158입니다. 이 데이터 블록에는 새 엔드포인트 프로파일, 보안 인텔리전스 및 IPv6 필드가 포함되어 있습니다.

계열 1 블록 그룹에서 사용자 정보 데이터 블록의 블록 유형은 4.7~4.10.x 버전의 경우 75, 5.x 버전의 경우 120입니다. 자세한 정보는 5.x 버전용 사용자 정보 데이터 블록, B-117페이지의 내용을 참조하십시오.

다음 다이어그램에 사용자 정보 데이터 블록의 형식이 나와 있습니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
성	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	성...																															
이메일	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	이메일...																															
부서	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	부서...																															
전화	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	전화...																															
	엔드포인트 프로파일 ID																															
	보안 그룹 ID																															
	위치 IPv6 주소																															
	위치 IPv6 주소(계속)																															
	위치 IPv6 주소(계속)																															
	위치 IPv6 주소(계속)																															

다음 표에는 사용자 정보 데이터 블록의 구성 요소에 대한 설명이 나와 있습니다.

표 4-87 사용자 정보 데이터 블록 필드

필드	데이터 유형	설명
사용자 정보 블록 유형	uint32	사용자 정보 데이터 블록을 시작합니다. 값은 158입니다.
사용자 정보 블록 길이	uint32	사용자 정보 데이터 블록의 총 바이트 수입니다. 여기에는 사용자 정보 블록 유형 및 길이 필드의 8바이트에 그 뒤의 사용자 정보 데이터 바이트 수를 더한 값이 포함됩니다.
사용자 ID	uint32	사용자의 ID 번호입니다.
문자열 블록 유형	uint32	사용자의 사용자 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	사용자 이름 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 사용자 이름의 바이트 수를 더한 값이 포함됩니다.
사용자 이름	string	사용자의 사용자 이름입니다.
영역 ID	uint32	ID 영역에 해당하는 정수 ID입니다.
프로토콜	uint32	사용자 정보를 포함하는 패킷의 프로토콜입니다.
문자열 블록 유형	uint32	사용자의 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	이름 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 이름의 바이트 수를 더한 값이 포함됩니다.
이름	string	사용자의 이름입니다.
문자열 블록 유형	uint32	사용자의 성이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	사용자 성 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 성의 바이트 수를 더한 값이 포함됩니다.
성	string	사용자의 성입니다.
문자열 블록 유형	uint32	사용자의 이메일 주소가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	이메일 주소 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 이메일 주소의 바이트 수를 더한 값이 포함됩니다.
이메일	string	사용자의 이메일 주소입니다.
문자열 블록 유형	uint32	사용자의 부서가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	부서 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 부서의 바이트 수를 더한 값이 포함됩니다.
부서	string	사용자의 부서입니다.

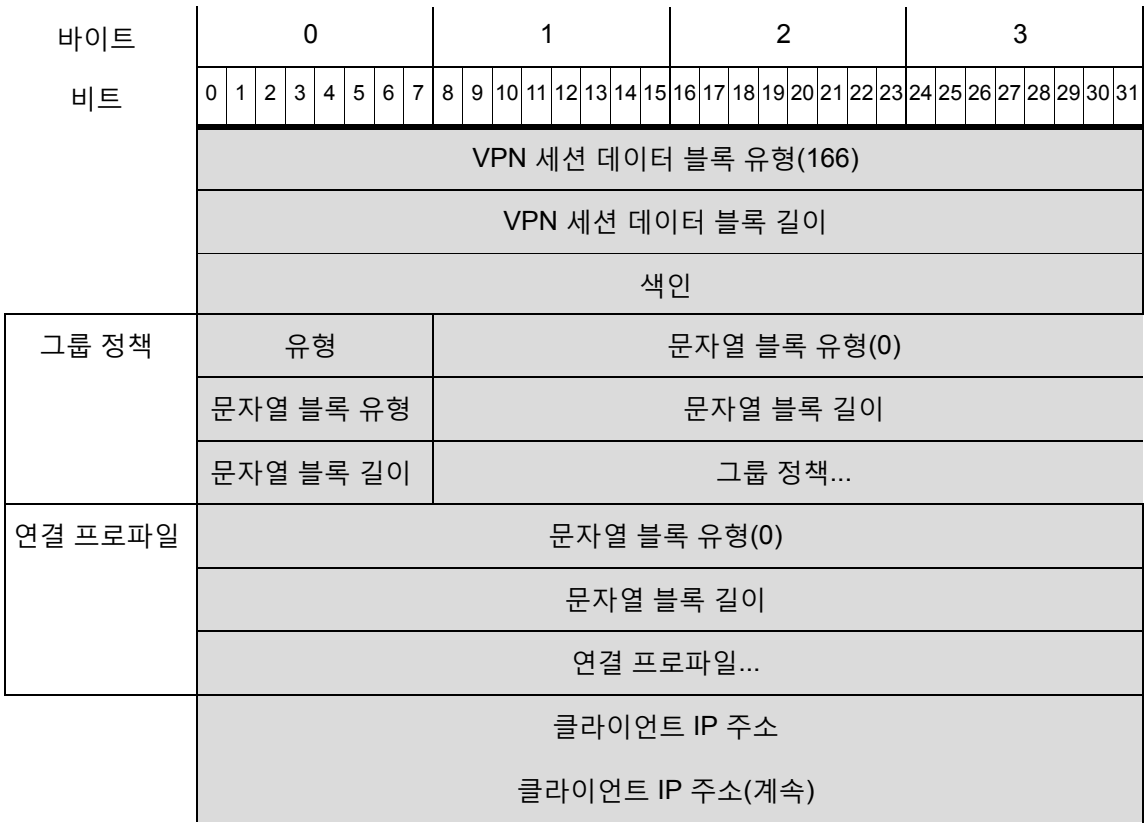
표 4-87 사용자 정보 데이터 블록 필드 (계속)

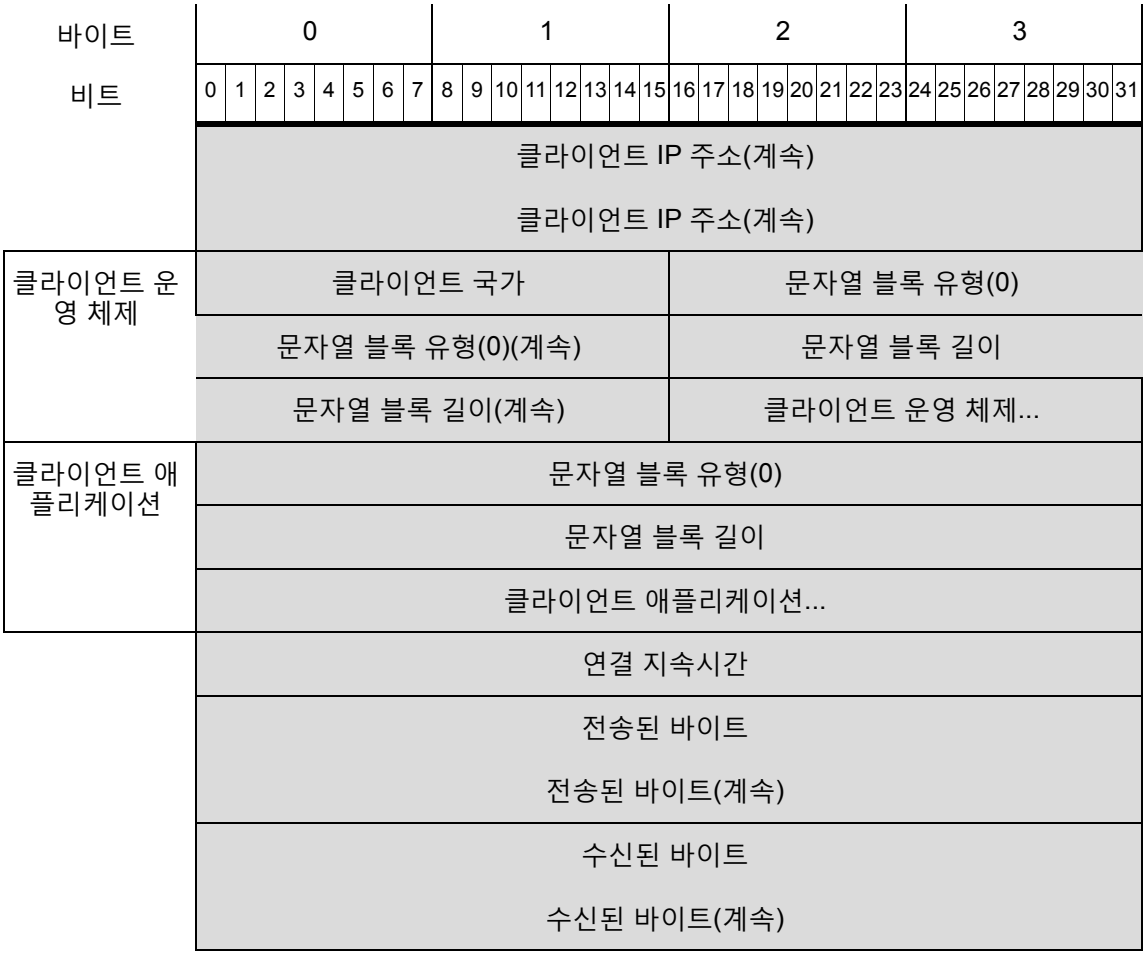
필드	데이터 유형	설명
문자열 블록 유형	uint32	사용자의 전화번호가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	전화번호 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 전화번호의 바이트 수를 더한 값이 포함됩니다.
전화	string	사용자의 전화번호입니다.
엔드포인트 프로파일 ID	uint32	연결 엔드포인트에서 사용하는 디바이스 유형의 ID 번호입니다. 각 방어 센터에 대해 고유하며 메타데이터에서 확인 가능합니다.
보안 그룹 ID	uint32	네트워크 트래픽 그룹의 ID 번호입니다.
위치 IPv6 주소	uint16[8]	ISE와 통신하는 인터페이스의 IP 주소입니다. IPv4 또는 IPv6일 수 있습니다.

6.2 이상 버전용 VPN 세션 데이터 블록

계열 1 블록 그룹에서 6.2 이상 버전용 VPN 세션 데이터 블록의 블록 유형은 166입니다. 이 데이터 블록은 VPN 세션 정보를 설명합니다.

다음 다이어그램에 6.2 이상 버전의 VPN 세션 데이터 블록 형식이 나와 있습니다.





다음 표에는 VPN 세션 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 4-88 VPN 세션 데이터 블록 필드

필드	데이터 유형	설명
VPN 세션 데이터 블록 유형	uint32	VPN 세션 데이터 블록을 시작합니다. 이 값은 항상 166입니다.
VPN 세션 블록 길이	uint32	VPN 세션 데이터 블록의 바이트 수입니다. 여기에는 VPN 세션 데이터 블록 유형 및 길이의 8바이트에 그 뒤의 VPN 세션 데이터 필드 바이트 수를 더한 값이 포함됩니다.
색인	uint32	세션을 식별하기 위해 VPN 디바이스에서 생성한 번호입니다.

표 4-88 VPN 세션 데이터 블록 필드 (계속)

필드	데이터 유형	설명
유형	uint8	VPN 세션의 유형입니다. 사용 가능한 값은 다음과 같습니다. • 0 - 알 수 없음 • 1 - Cisco IKEv1 클라이언트 • 2 - AnyConnect IKEv1 클라이언트 • 3 - AnyConnect SSL • 4 - WebVPN 클라이언트리스 • 5 - 사이트 대 사이트 IKEv2 • 6 - 사이트 대 사이트 IKEv2 • 7 - 일반 IKEv2 RA 클라이언트
문자열 블록 유형	uint32	VPN 세션에 대한 그룹 정책이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	사용자 이름 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 그룹 정책의 바이트 수를 더한 값이 포함됩니다.
그룹 정책	string	VPN 세션 설정 시 클라이언트에 할당된 그룹 정책의 이름입니다.
문자열 블록 유형	uint32	VPN 세션의 연결 프로파일이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	사용자 이름 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 연결 프로파일의 바이트 수를 더한 값이 포함됩니다.
연결 프로파일	string	VPN 세션에서 사용되는 연결 프로파일(터널 그룹)의 이름입니다.
클라이언트 IP 주소	uint8[16]	VPN 클라이언트 디바이스의 IP 주소입니다.
클라이언트 국가	uint16	VPN 클라이언트의 국가 코드입니다.
문자열 블록 유형	uint32	클라이언트 디바이스에서 사용하는 운영 체제가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	사용자 이름 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 운영 체제 이름의 바이트 수를 더한 값이 포함됩니다.
클라이언트운영 체제	string	클라이언트 디바이스의 운영 체제입니다.
문자열 블록 유형	uint32	클라이언트 디바이스에서 사용하는 VPN 애플리케이션이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	사용자 이름 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 VPN 애플리케이션의 바이트 수를 더한 값이 포함됩니다.
클라이언트 애플리케이션	string	클라이언트 디바이스용 VPN 애플리케이션입니다.
연결 지속시간	uint32	VPN 세션의 지속시간(초)입니다. VPN 로그아웃 작업의 경우에만 지정되며 그 외의 경우에는 값이 0입니다.

표 4-88 VPN 세션 데이터 블록 필드 (계속)

필드	데이터 유형	설명
전송된 바이트	uint64	VPN 세션 중에 VPN 클라이언트에 전송된 바이트 수입니다. VPN 로그아웃 작업의 경우에만 지정되며 그 외의 경우에는 값이 0입니다.
수신된 바이트	uint64	VPN 세션 중에 VPN 클라이언트에서 수신된 바이트 수입니다. VPN 로그아웃 작업의 경우에만 지정되며 그 외의 경우에는 값이 0입니다.

6.2 이상 버전용 사용자 로그인 정보 데이터 블록

사용자 로그인 정보 데이터 블록은 사용자 정보 업데이트 메시지에 사용되며 탐지된 사용자의 로그인 정보 변경 사항을 전달합니다. 자세한 정보는 사용자 정보 업데이트 메시지 블록, 4-62페이지의 내용을 참조하십시오.

계열 1 블록 그룹에서 사용자 로그인 정보 데이터 블록의 블록 유형은 6.2 이상 버전의 경우 167입니다. 이 데이터 블록은 VPN 지원을 위한 새 필드를 포함하며, 이는 블록 유형 165를 대체합니다. 자세한 정보는 6.1.x 버전용 사용자 로그인 정보 데이터 블록, B-110페이지의 내용을 참조하십시오.

아래 그림에 사용자 로그인 정보 데이터 블록의 형식이 나와 있습니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	엔드포인트 프로파일 ID																															
	보안 그룹 ID																															
	프로토콜																															
	포트																범위 시작															
	시작 포트																종료 포트															
이메일	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	이메일...																															
	IPv6 주소 IPv6 주소(계속) IPv6 주소(계속) IPv6 주소(계속)																															
	위치 IPv6 주소 위치 IPv6 주소(계속) 위치 IPv6 주소(계속) 위치 IPv6 주소(계속)																															
보고자	로그인 유형								인증 유형								문자열 블록 유형(0)															
	문자열 블록 유형(0)(계속)																문자열 블록 길이															
	문자열 블록 길이(계속)																보고자...															
설명	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	설명...																															

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
VPN 세션	VPN 세션 데이터 블록 유형(166)																															
	VPN 세션 데이터 블록 길이																															
	VPN 세션...																															

다음 표에는 사용자 로그인 정보 데이터 블록의 구성 요소에 대한 설명이 나와 있습니다.

표 4-89 사용자 로그인 정보 데이터 블록 필드

필드	데이터 유형	설명
사용자 로그인 정보 블록 유형	uint32	사용자 로그인 정보 데이터 블록을 시작합니다. 6.2 이상 버전의 경우 이 값은 167입니다.
사용자 로그인 정보 블록 길이	uint32	사용자 로그인 정보 데이터 블록의 총 바이트 수입니다. 여기에는 사용자 로그인 정보 블록 유형 및 길이 필드의 8바이트에 그 뒤의 사용자 로그인 정보 데이터 바이트 수를 더한 값이 포함됩니다.
타임스탬프	uint32	이벤트의 타임스탬프입니다.
IPv4 주소	uint32	이 필드는 예약되지만 더 이상 내용이 입력되지는 않습니다. IPv4 주소는 IPv6 Address(IPv6 주소) 필드에 저장됩니다. 자세한 정보는 IP 주소, 1-5페이지의 내용을 참조하십시오.
문자열 블록 유형	uint32	사용자의 사용자 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	사용자 이름 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 사용자 이름의 바이트 수를 더한 값이 포함됩니다.
사용자 이름	string	사용자의 사용자 이름입니다.
문자열 블록 유형	uint32	도메인이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	사용자 이름 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 도메인의 바이트 수를 더한 값이 포함됩니다.
도메인	string	사용자가 로그인한 도메인입니다.
사용자 ID	uint32	사용자의 ID 번호입니다.
영역 ID	uint32	ID 영역에 해당하는 정수 ID입니다.
엔드포인트 프로파일 ID	uint32	연결 엔드포인트에서 사용하는 디바이스 유형의 ID 번호입니다. 각 DC에 대해 고유하며 메타데이터에서 확인 가능합니다.
보안 그룹 ID	uint32	네트워크 트래픽 그룹의 ID 번호입니다.

표 4-89 사용자 로그인 정보 데이터 블록 필드 (계속)

필드	데이터 유형	설명
프로토콜	uint32	사용자를 탐지하거나 보고하는 데 사용되는 프로토콜입니다. 가능한 값은 다음과 같습니다. • 165 - FTP • 426 - SIP • 547 - AOL Instant Messenger • 683 - IMAP • 710 - LDAP • 767 - NTP • 773 - Oracle Database • 788 - POP3 • 1755 - MDNS
포트	uint16	사용자가 탐지된 포트 번호입니다.
범위 시작	uint16	TS 에이전트에서 사용하는 포트 범위의 시작 포트입니다.
시작 포트	uint16	개별 사용자에게 할당된 TS 에이전트 범위의 시작 포트입니다.
종료 포트	uint16	개별 사용자에게 할당된 TS 에이전트 범위의 종료 포트입니다.
문자열 블록 유형	uint32	사용자의 이메일 주소가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	이메일 주소 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 이메일 주소의 바이트 수를 더한 값이 포함됩니다.
이메일	string	사용자의 이메일 주소입니다.
IPv6 주소	uint8[16]	로그인 중인 사용자가 탐지된 호스트의 IPv6 주소(IP 주소 옥텟 형식)입니다.
위치 IPv6 주소	uint8[16]	사용자가 가장 최근에 로그인한 IP 주소입니다. IPv4 또는 IPv6 주소일 수 있습니다.
로그인 유형	uint8	탐지된 사용자 로그인의 유형입니다.
인증 유형	uint8	사용자가 사용한 인증의 유형입니다. 값은 다음 중 하나일 수 있습니다. • 0 - 인증 필요 없음 • 1 - 패시브 인증, AD 에이전트 또는 ISE 세션 • 2 - 종속 포털 정상 인증 • 3 - 종속 포털 게스트 인증 • 4 - 종속 포털 인증 장애
문자열 블록 유형	uint32	보고자 값이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	보고자 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 Reported By(보고자) 필드의 바이트 수를 더한 값이 포함됩니다.

표 4-89 사용자 로그인 정보 데이터 블록 필드 (계속)

필드	데이터 유형	설명
보고자	string	이 활동의 보고자(예: Active Directory 서버의 이름)입니다.
문자열 블록 유형	uint32	설명 값이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	설명 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 Description(설명) 필드의 바이트 수를 더한 값이 포함됩니다.
설명	string	로그인 또는 로그오프 활동의 설명입니다.
VPN 세션 블록 유형	uint32	VPN 세션 데이터가 포함된 VPN 세션 데이터 블록을 시작합니다. 이 값은 항상 166입니다.
VPN 세션 데이터 블록 길이	uint32	VPN 세션 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 VPN 세션 데이터 블록의 바이트 수를 더한 값이 포함됩니다.
VPN 세션 데이터	VPN 세션 데이터	로그인이 탐지된 VPN 세션과 관련된 경우 해당 VPN 세션과 관련된 정보입니다. VPN 세션이 있을 때만 사용됩니다.

검색 및 연결 이벤트 계열 2 데이터 블록

다음 표의 데이터 블록 상태 필드에는 해당 블록이 현재 블록(최신 버전)인지 아니면 레거시 블록(이전 버전에서 사용되며 eStreamer를 통해 계속 요청할 수는 있음)인지가 나와 있습니다.

표 4-90 검색 및 연결 이벤트 계열 2 블록 유형

유형	콘텐츠	데이터 블록 상태	설명
15	액세스 제어 규칙	현재	액세스 제어 규칙 메타데이터 메시지에서 정책 UUID 및 규칙 ID 값을 설명 문자열에 매핑하는 데 사용됩니다. 액세스 제어 규칙 데이터 블록, 4-200페이지의 내용을 참조하십시오.
21	액세스 제어 규칙 이유	현재	액세스 제어 규칙 메타데이터 메시지에서 액세스 제어 규칙 이유를 설명 문자열에 매핑하는 데 사용됩니다. 5.1 이상 버전용 액세스 제어 규칙 이유 데이터 블록, 4-201페이지의 내용을 참조하십시오.
22	보안 인텔리전스 카테고리	현재	보안 인텔리전스 정보를 저장하는 데 사용됩니다. 5.1 이상 버전용 보안 인텔리전스 카테고리 데이터 블록, 4-203페이지의 내용을 참조하십시오.
57	사용자 데이터	현재	사용자 레코드 메타데이터 메시지에서 사용자 ID 번호, 사용자가 탐지된 프로토콜 및 사용자 이름을 제공하는 데 사용됩니다. 사용자 데이터 블록, 4-204페이지의 내용을 참조하십시오.

액세스 제어 규칙 데이터 블록

eStreamer서비스는 액세스 제어 규칙 메타데이터 메시지의 액세스 제어 규칙 데이터 블록을 사용하여 정책 UUID 및 규칙 ID 조합을 설명 문자열에 매핑합니다. 계열 2 블록 그룹에서 액세스 제어 규칙 데이터 블록의 블록 유형은 15입니다.

다음 그림에 액세스 제어 규칙 데이터 블록의 구조가 나와 있습니다.

다음 표에는 액세스 제어 규칙 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 4-91 액세스 제어 규칙 데이터 블록 필드

필드	데이터 유형	설명
액세스 제어 규칙 블록 유형	uint32	액세스 제어 규칙 블록을 시작합니다. 이 값은 항상 15입니다.
액세스 제어 규칙 블록 길이	uint32	액세스 제어 규칙 블록의 총 바이트 수입니다. 여기에는 액세스 제어 규칙 블록 유형 및 길이 필드의 8바이트에 그 뒤의 데이터 바이트 수를 더한 값이 포함됩니다.
액세스 제어 규칙 UUID	uint8[16]	액세스 제어 규칙의 고유 식별자입니다. 이 필드는 Access Control Rule ID(액세스 제어 규칙 ID)와 함께 이 레코드의 고유 키를 구성합니다.
액세스 제어 규칙 ID	uint32	액세스 제어 규칙의 내부 Cisco 식별자입니다. 이 필드는 Access Control Rule UUID(액세스 제어 규칙 UUID)와 함께 이 레코드의 고유 키를 구성합니다.

표 4-91 액세스 제어 규칙 데이터 블록 필드 (계속)

필드	데이터 유형	설명
문자열 블록 유형	uint32	액세스 제어 규칙 UUID 및 액세스 제어 규칙 ID와 관련된 설명 이름을 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Name(이름) 필드의 바이트 수를 더한 값이 포함됩니다.
이름	string	설명 이름입니다.

5.1 이상 버전용 액세스 제어 규칙 이유 데이터 블록

eStreamer 서비스는 액세스 제어 규칙 이유 메타데이터 메시지의 액세스 제어 규칙 이유 데이터 블록을 사용하여 액세스 제어 이유를 설명 문자열에 매핑합니다. 계열 2 블록 그룹에서 액세스 제어 규칙 이유 데이터 블록의 블록 유형은 21입니다.

다음 그림에 액세스 제어 규칙 이유 데이터 블록의 구조가 나와 있습니다.

다음 표에는 액세스 제어 규칙 이유 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 4-92 액세스 제어 규칙 이유 데이터 블록 필드

필드	데이터 유형	설명
액세스 제어 규칙 이유 블록 유형	uint32	액세스 제어 규칙 이유 블록을 시작합니다. 이 값은 항상 21입니다.
액세스 제어 규칙 이유 블록 길이	uint32	액세스 제어 규칙 이유 블록의 총 바이트 수입니다. 여기에는 액세스 제어 규칙 이유 블록 유형 및 길이 필드의 8바이트에 그 뒤의 데이터 바이트 수를 더한 값이 포함됩니다.

표 4-92 액세스 제어 규칙 이유 데이터 블록 필드 (계속)

필드	데이터 유형	설명
액세스 제어 규칙 이유	uint16	액세스 제어 규칙이 연결을 로깅한 이유입니다. 이 필드는 이 레코드의 고유 키입니다. 이벤트를 트리거한 규칙에 대한 이유 번호입니다. 규칙 이유는 여러 비트가 설정되어 있을 수 있는 이진 비트맵입니다. 규칙 하나에 여러 가지 이유가 있을 수 있습니다. 비트 값은 다음과 같습니다. • **1** - IP 차단 • **2** - IP 모니터 • **4** - 사용자 우회 • **8** - 파일 모니터 • **16** - 악성코드 차단 • **32** - 침입 모니터 • **64** - 악성코드 차단 • **128** - 파일 다시 시작 차단 • **256** -파일 다시 시작 허용"] • **512** - 파일 맞춤형 탐지 • **1024** - SSL 차단 • **2048** - DNS 차단 • **4096** - DNS 모니터 • **8192** - URL 차단 • **16384** - URL 모니터 • **32768** - 콘텐츠 제한 • **65536** - 지능형 앱 우회 • **131072** - WSA 위협
문자열 블록 유형	uint32	액세스 제어 규칙 이유와 관련된 설명 이름을 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Description(설명) 필드의 바이트 수를 더한 값이 포함됩니다.
설명	string	액세스 제어 규칙 이유의 설명입니다.

5.1 이상 버전용 보안 인텔리전스 카테고리 데이터 블록

eStreamer 서비스는 액세스 제어 규칙 메타데이터 메시지의 보안 인텔리전스 카테고리 데이터 블록을 사용하여 보안 인텔리전스 정보를 스트리밍합니다. 계열 2 블록 그룹에서 보안 인텔리전스 카테고리 데이터 블록의 블록 유형은 22입니다.

다음 그림에 보안 인텔리전스 카테고리 데이터 블록의 구조가 나와 있습니다.

다음 표에는 보안 인텔리전스 카테고리 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 4-93 보안 인텔리전스 카테고리 데이터 블록 필드

필드	데이터 유형	설명
보안 인텔리전스 카테고리 블록 유형	uint32	보안 인텔리전스 카테고리 데이터 블록을 시작합니다. 이 값은 항상 22입니다.
보안 인텔리전스 카테고리 블록 길이	uint32	보안 인텔리전스 카테고리 블록의 총 바이트 수입니다. 여기에는 보안 인텔리전스 카테고리 블록 유형 및 길이 필드의 8바이트에 그 뒤의 데이터 바이트 수를 더한 값이 포함됩니다.
보안 인텔리전스 목록 ID	uint32	연결에 의해 트리거된 IP 블랙리스트 또는 화이트리스트의 ID입니다. 이 필드는 Access Control Policy UUID(액세스 제어 정책 UUID)와 함께 이 레코드의 고유 키를 구성합니다.

표 4-93 보안 인텔리전스 카테고리 데이터 블록 필드 (계속)

필드	데이터 유형	설명
액세스 제어 정책 UUID	uint8[16]	보안 인텔리전스용으로 구성된 액세스 제어 정책의 UUID입니다. 이 필드는 Security Intelligence List ID(보안 인텔리전스 목록 ID)와 함께 이 레코드의 고유 키를 구성합니다.
문자열 블록 유형	uint32	보안 인텔리전스 목록과 관련된 설명 이름을 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Security Intelligence List Name(보안 인텔리전스 목록 이름) 필드의 바이트 수를 더한 값이 포함됩니다.
보안 인텔리전스 목록 이름	string	연결에 의해 트리거된 보안 인텔리전스 카테고리 IP 블랙리스트 또는 화이트리스트의 이름입니다.

사용자 데이터 블록

eStreamer서비스는 사용자 레코드 메타데이터 메시지의 사용자 데이터 블록을 사용하여 사용자 ID 번호, 사용자가 탐지된 프로토콜 및 사용자 이름을 제공합니다. 계열 2 블록 그룹에서 사용자 데이터 블록의 블록 유형은 57입니다.

다음 그림에 사용자 데이터 블록의 구조가 나와 있습니다.

다음 표에는 사용자 데이터 블록의 필드에 대한 설명이 나와 있습니다.

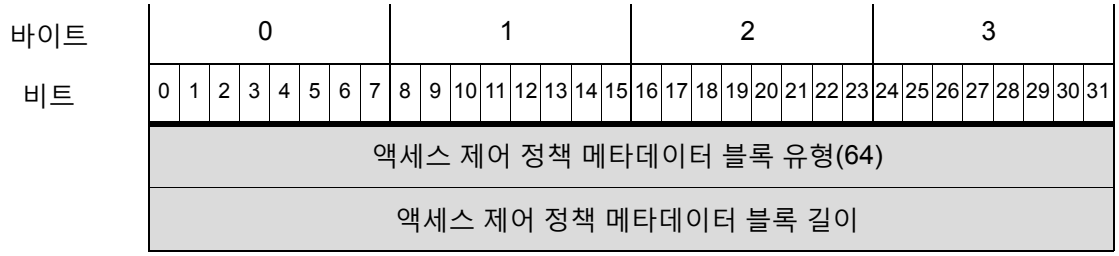
표 4-94 사용자 데이터 블록 필드

필드	데이터 유형	설명
사용자 블록 유형	uint32	사용자 블록을 시작합니다. 이 값은 항상 57입니다.
사용자 블록 길이	uint32	사용자 데이터 블록의 총 바이트 수입니다. 여기에는 사용자 블록 유형 및 길이 필드의 8바이트에 그 뒤의 데이터 바이트 수를 더한 값이 포함됩니다.
사용자 ID	uint32	사용자의 고유 식별자입니다. 이 필드는 이 레코드의 고유 키입니다.
프로토콜	uint32	사용자를 탐지하거나 보고하는 데 사용되는 프로토콜입니다. 가능한 값은 다음과 같습니다. • 165 - FTP • 426 - SIP • 547 - AOL Instant Messenger • 683 - IMAP • 710 - LDAP • 767 - NTP • 773 - Oracle Database • 788 - POP3 • 1755 - MDNS
문자열 블록 유형	uint32	사용자 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	사용자 이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Username(사용자 이름) 필드의 바이트 수를 더한 값이 포함됩니다.
사용자 이름	string	사용자의 이름입니다.

6.0 이상 버전용 액세스 제어 정책 메타데이터 블록

eStreamer 서비스는 액세스 제어 정책 메타데이터 메시지의 액세스 제어 정책 메타데이터 데이터 블록을 사용하여 액세스 제어 정책 정보를 제공합니다. 계열 2 블록 그룹에서 액세스 제어 규칙 정책 메타데이터 블록의 블록 유형은 64입니다.

다음 그림에 액세스 제어 정책 메타데이터 블록의 구조가 나와 있습니다.



바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
AC 정책 UUID	액세스 제어 정책 UUID																															
	액세스 제어 정책 UUID(계속)																															
	액세스 제어 정책 UUID(계속)																															
	액세스 제어 정책 UUID(계속)																															
	센서 ID																															
정책 이름	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	정책 이름...																															

다음 표에는 액세스 제어 정책 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 4-95 액세스 제어 정책 데이터 블록 필드

필드	데이터 유형	설명
액세스 제어 정책 메타데이터 블록 유형	uint32	액세스 제어 정책 메타데이터 블록을 시작합니다. 이 값은 항상 64입니다.
액세스 제어 정책 메타데이터 블록 길이	uint32	액세스 제어 정책 메타데이터 블록의 총 바이트 수입니다. 여기에는 액세스 제어 정책 메타데이터 블록 유형 및 길이 필드의 8바이트에 그 뒤의 데이터 바이트 수를 더한 값이 포함됩니다.
액세스 제어 정책 UUID	uint8[16]	액세스 제어 정책의 UUID입니다. 이 필드는 이 레코드의 고유 키입니다.
센서 ID	uint32	액세스 제어 정책과 관련된 센서의 ID 번호입니다.
문자열 블록 유형	uint32	액세스 제어 정책과 관련된 설명 이름을 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Name(이름) 필드의 바이트 수를 더한 값이 포함됩니다.
이름	string	액세스 제어 정책의 이름입니다.

호스트 데이터 구조 이해

이 장에서는 단일 호스트를 설명하는 데이터 집합을 전달하는 전체 호스트 프로파일 데이터 블록의 형식에 대해 설명합니다. eStreamer 서버는 호스트 데이터 요청 시 이러한 블록을 생성하여 전송합니다. 클라이언트 요청 절차, 메시지 구조 및 전달 방법에 대한 자세한 정보는 호스트 데이터 및 여러 호스트 데이터 메시지 형식, 2-30페이지의 내용을 참조하십시오.

eStreamer는 계열 1 데이터 블록 구조를 사용하여 이러한 전체 호스트 프로파일 블록을 패키징합니다. 계열 1 블록의 일반적인 구조는 계열 1 데이터 블록 헤더, 4-63페이지의 내용을 참조하십시오. 전체 호스트 프로파일 데이터 블록은 캡슐화된 블록을 여러 개 포함합니다. 이러한 개별 블록에 대한 설명은 검색 및 연결 데이터 구조 이해, 4-1페이지에서 각 블록이 정의되어 있는 하위 섹션에 나와 있습니다.

현재 및 레거시 전체 호스트 프로파일 데이터 블록에 대한 자세한 내용은 다음 섹션을 참조하십시오.

- 5.3 이상 버전용 전체 호스트 프로파일 데이터 블록, 5-1페이지에서는 현재 전체 호스트 프로파일 데이터 블록 구조에 대해 설명합니다.
- 5.0~5.0.2 버전용 전체 호스트 프로파일 데이터 블록, B-274페이지에서는 버전 5.0~5.0.2용 레거시 전체 호스트 프로파일 데이터 블록 구조에 대해 설명합니다.

5.3 이상 버전용 전체 호스트 프로파일 데이터 블록

5.3 이상 버전용 전체 호스트 프로파일 데이터 블록에는 호스트 하나를 설명하는 전체 데이터 집합이 포함됩니다. 이 블록은 아래 그림에 나와 있는 형식으로 되어 있습니다. 해당 형식에 대한 설명은 다음 표에 나와 있습니다. 목록 데이터 블록을 제외하고는 캡슐화된 데이터 블록의 필드는 그림에 나와 있지 않습니다. 이러한 캡슐화된 데이터 블록에 대해서는 검색 및 연결 데이터 구조 이해, 4-1페이지에서 별도로 설명합니다. 전체 호스트 프로파일 데이터 블록의 블록 유형 값은 149입니다. 이는 이전 버전(블록 유형 140)을 대체합니다.

참고 다음 다이어그램에서 블록 이름 옆에 있는 별표(*)는 데이터 블록 인스턴스가 여러 개 나올 수 있음을 나타냅니다.

다음 다이어그램에 5.3 이상 버전의 전체 호스트 프로파일 데이터 블록 형식이 나와 있습니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	전체 호스트 프로파일 데이터 블록(149)																															
	데이터 블록 길이																															
	호스트 ID 호스트 ID(계속) 호스트 ID(계속) 호스트 ID(계속)																															
IP 주소	목록 블록 유형(11)																															
	목록 블록 길이																															
	IP 주소 데이터 블록(143)*																															
	홉								일반 목록 블록 유형(31)																							
	일반 목록 블록 유형(계속)								일반 목록 블록 길이																							
파생된 OS 핑거프린트	일반 목록 블록 길이(계속)								운영 체제 핑거프린트 블록 유형(130)*																							
	OS 핑거프린트 블록 유형(130)*(계속)								운영 체제 핑거프린트 블록 길이																							
	OS 핑거프린트 블록 길이(계속)								운영 체제 파생 핑거프린트 데이터...																							
	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
서버 핑거프린트	운영 체제 핑거프린트 블록 유형(130)*																															
	운영 체제 핑거프린트 블록 길이																															
	운영 체제 서버 핑거프린트 데이터...																															
	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
클라이언트 핑거프린트	운영 체제 핑거프린트 블록 유형(130)*																															
	운영 체제 핑거프린트 블록 길이																															
	운영 체제 클라이언트 핑거프린트 데이터...																															
	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
VDB 네이티브 핑거프린트 1	운영 체제 핑거프린트 블록 유형(130)*																															
	운영 체제 핑거프린트 블록 길이																															
	운영 체제 VDB 핑거프린트 데이터...																															
	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
VDB 네이티브 핑거프린트 2	운영 체제 핑거프린트 블록 유형(130)*																															
	운영 체제 핑거프린트 블록 길이																															
	운영 체제 VDB 핑거프린트 데이터...																															
	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
사용자 핑거프린트	운영 체제 핑거프린트 블록 유형(130)*																															
	운영 체제 핑거프린트 블록 길이																															
	운영 체제 사용자 핑거프린트 데이터...																															
	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
스캔 핑거프린트	운영 체제 핑거프린트 블록 유형(130)*																															
	운영 체제 핑거프린트 블록 길이																															
	운영 체제 스캔 핑거프린트 데이터...																															
	일반 목록 블록 유형(31)																															

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	일반 목록 블록 길이																															
애플리케이션 핑거프린트	운영 체제 핑거프린트 블록 유형(130)*																															
	운영 체제 핑거프린트 블록 길이																															
	운영 체제 애플리케이션 핑거프린트 데이터...																															
충돌 핑거프린트	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
	운영 체제 핑거프린트 블록 유형(130)*																															
	운영 체제 핑거프린트 블록 길이																															
	운영 체제 충돌 핑거프린트 데이터...																															
모바일 핑거프린트	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
	운영 체제 핑거프린트 블록 유형(130)*																															
	운영 체제 핑거프린트 블록 길이																															
	운영 체제 모바일 핑거프린트 데이터...																															
IPv6 서버 핑거프린트	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
	운영 체제 핑거프린트 블록 유형(130)*																															
	운영 체제 핑거프린트 블록 길이																															
	운영 체제 IPv6 서버 핑거프린트 데이터...																															
IPv6 클라이언트 핑거프린트	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
	운영 체제 핑거프린트 블록 유형(130)*																															
	운영 체제 핑거프린트 블록 길이																															
	운영 체제 IPv6 클라이언트 핑거프린트 데이터...																															

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
IPv6 DHCP 핑거프린트	운영 체제 핑거프린트 블록 유형(130)*																															
	운영 체제 핑거프린트 블록 길이																															
	운영 체제 IPv6 DHCP 핑거프린트 데이터...																															
	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
사용자 에이전트 핑거프린트	운영 체제 핑거프린트 블록 유형(130)*																															
	운영 체제 핑거프린트 블록 길이																															
	운영 체제 사용자 에이전트 핑거프린트 데이터...																															
(TCP) 전체 서버 데이터	목록 블록 유형(11)...																															
	목록 블록 길이...																															
	(TCP) 전체 서버 데이터 블록(104)*																															
(UDP) 전체 서버 데이터	목록 블록 유형(11)																															
	목록 블록 길이																															
	(UDP) 전체 서버 데이터 블록(104)*																															
네트워크 프로토콜 데이터	목록 블록 유형(11)																															
	목록 블록 길이																															
	(네트워크) 프로토콜 데이터 블록(4)*																															
전송 프로토콜 데이터	목록 블록 유형(11)																															
	목록 블록 길이																															
	(전송) 프로토콜 데이터 블록(4)*																															

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
MAC 주소 데이터	목록 블록 유형(11)																															
	목록 블록 길이																															
	호스트 MAC 주소 데이터 블록(95)*																															
	마지막 확인																															
	호스트 유형																															
	비즈니스 임계성																VLAN ID															
	VLAN 유형								VLAN 우선순위								일반 목록 블록 유형(31)															
호스트 클라이언트 데이터	일반 목록 블록 유형(계속)																일반 목록 블록 길이															
	일반 목록 블록 길이(계속)																전체 호스트 클라이언트 애플리케이션 데이터 블록(112)*															
NetBios 이름	문자열 블록 유형(0)																															
이름	문자열 블록 길이																															
	NetBIOS 이름 문자열...																															
메모 데이터	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	메모 문자열...																															
(VDB) 호스트 취약점	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
	(VDB) 호스트 취약점 데이터 블록(85)*																															
서드파티/VDB 호스트 취약점	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
	(서드파티/VDB) 호스트 취약점 데이터 블록(85)*																															
서드파티 스캔 호스트 취약점	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
	(서드파티 스캔) 원래 취약점 ID가 포함된 호스트 취약점 데이터 블록(85)*																															

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
속성 값 데이터	목록 블록 유형(11)																															
	목록 블록 길이																															
	속성값 데이터 블록*																															
	모바일								탈옥됨								일반 목록 블록 유형(31)															
IOC 상태	일반 목록 블록 유형(계속)																일반 목록 블록 길이															
	일반 목록 블록 길이(계속)																IOC 상태 데이터 블록(150)*															

다음 표에는 5.3 이상 버전용 전체 호스트 프로파일 레코드의 구성 요소에 대한 설명이 나와 있습니다.

표 5-1 5.3 이상 버전용 전체 호스트 프로파일 레코드 필드

필드	데이터 유형	설명
호스트 ID	uint8[16]	호스트의 고유 ID 번호로, UUID입니다.
목록 블록 유형	uint32	TCP 서비스 데이터를 전달하는 IP 주소 데이터 블록으로 구성된 목록 데이터 블록을 시작합니다. 이 값은 항상 11입니다.
목록 블록 길이	uint32	목록의 바이트 수입니다. 이 수에는 목록 블록 유형 및 길이 필드의 8바이트에 캡슐화된 모든 IP 주소 데이터 블록의 길이를 더한 값이 포함됩니다.
IP 주소	variable	호스트의 IP 주소와 각 IP 주소가 마지막으로 확인된 시간입니다. 이 데이터 블록에 대한 설명은 호스트 IP 주소 데이터 블록, 4-99페이지의 내용을 참조하십시오.
홉	uint8	호스트에서 디바이스로의 네트워크 홉 수입니다.
일반 목록 블록 유형	uint32	기존 핑거프린트에서 호스트에 대해 파생된 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
운영 체제 파생 핑거프린트 데이터 블록*	variable	기존 핑거프린트에서 호스트에 대해 파생된 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 4-161페이지의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	서버 핑거프린트를 사용하여 식별된 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.

표 5-1 5.3 이상 버전용 전체 호스트 프로파일 레코드 필드 (계속)

필드	데이터 유형	설명
운영 체제 핑거프린트(서버 핑거프린트) 데이터 블록*	variable	서버 핑거프린트를 사용하여 식별된 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 4-161페이지의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	클라이언트 핑거프린트를 사용하여 식별된 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
운영 체제 핑거프린트(클라이언트 핑거프린트) 데이터 블록*	variable	클라이언트 핑거프린트를 사용하여 식별된 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 4-161페이지의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	Cisco VDB 핑거프린트를 사용하여 식별된 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
운영 체제 핑거프린트(VDB 네이티브 핑거프린트 1) 데이터 블록*	variable	Cisco VDB(취약점 데이터베이스)의 핑거프린트를 사용하여 식별된 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 4-161페이지의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	Cisco VDB 핑거프린트를 사용하여 식별된 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
운영 체제 핑거프린트(VDB 네이티브 핑거프린트 2) 데이터 블록*	variable	Cisco VDB(취약점 데이터베이스)의 핑거프린트를 사용하여 식별된 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 4-161페이지의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	사용자가 추가한 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
운영 체제 핑거프린트(사용자 핑거프린트) 데이터 블록*	variable	사용자가 추가한 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 4-161페이지의 내용을 참조하십시오.

표 5-1 5.3 이상 버전용 전체 호스트 프로파일 레코드 필드 (계속)

필드	데이터 유형	설명
일반 목록 블록 유형	uint32	취약점 스캐너가 추가한 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
운영 체제 핑거프린트(스캔 핑거프린트) 데이터 블록*	variable	취약점 스캐너가 추가한 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 4-161페이지의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	애플리케이션이 추가한 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
운영 체제 핑거프린트(애플리케이션 핑거프린트) 데이터 블록*	variable	애플리케이션이 추가한 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 4-161페이지의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	핑거프린트 충돌 해결을 통해 선택된 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
운영 체제 핑거프린트(충돌 핑거프린트) 데이터 블록*	variable	핑거프린트 충돌 해결을 통해 선택된 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 4-161페이지의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	모바일 디바이스 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
운영 체제 핑거프린트(모바일) 데이터 블록*	variable	모바일 디바이스 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 4-161페이지의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	IPv6 서버 핑거프린트를 사용하여 식별된 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.

표 5-1 5.3 이상 버전용 전체 호스트 프로파일 레코드 필드 (계속)

필드	데이터 유형	설명
운영 체제 핑거프린트(IPv6 서버 핑거프린트) 데이터 블록*	variable	IPv6 서버 핑거프린트를 사용하여 식별된 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 4-161페이지의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	IPv6 클라이언트 핑거프린트를 사용하여 식별된 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
운영 체제 핑거프린트(IPv6 클라이언트 핑거프린트) 데이터 블록*	variable	IPv6 클라이언트 핑거프린트를 사용하여 식별된 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 4-161페이지의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	IPv6 DHCP 핑거프린트를 사용하여 식별된 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
운영 체제 핑거프린트(IPv6 DHCP) 데이터 블록*	variable	IPv6 DHCP 핑거프린트를 사용하여 식별된 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 4-161페이지의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	사용자 에이전트 핑거프린트를 사용하여 식별된 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
운영 체제 핑거프린트(사용자 에이전트) 데이터 블록*	variable	사용자 에이전트 핑거프린트를 사용하여 식별된 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 4-161페이지의 내용을 참조하십시오.
목록 블록 유형	uint32	TCP 서비스 데이터를 전달하는 전체 서버 데이터 블록으로 구성된 목록 데이터 블록을 시작합니다. 이 값은 항상 11입니다.
목록 블록 길이	uint32	목록의 바이트 수입니다. 이 수에는 목록 블록 유형 및 길이 필드의 8바이트에 캡슐화된 모든 전체 서버 데이터 블록의 길이를 더한 값이 포함됩니다.
(TCP) 전체 서버 데이터 블록*	variable	호스트의 TCP 서비스에 대한 데이터를 전달하는 전체 서버 데이터 블록의 목록입니다. 이 데이터 블록에 대한 설명은 4.10.0 이상 버전용 전체 호스트 서버 데이터 블록, 4-140페이지의 내용을 참조하십시오.
목록 블록 유형	uint32	UDP 서비스 데이터를 전달하는 전체 서버 데이터 블록으로 구성된 목록 데이터 블록을 시작합니다. 이 값은 항상 11입니다.

표 5-1 5.3 이상 버전용 전체 호스트 프로파일 레코드 필드 (계속)

필드	데이터 유형	설명
목록 블록 길이	uint32	목록의 바이트 수입니다. 이 수에는 목록 블록 유형 및 길이 필드의 8바이트에 캡슐화된 모든 전체 서버 데이터 블록의 길이를 더한 값이 포함됩니다.
(UDP) 전체 서버 데이터 블록*	variable	호스트의 UDP 하위 서버에 대한 데이터를 전달하는 전체 서버 데이터 블록의 목록입니다. 이 데이터 블록에 대한 설명은 4.10.0 이상 버전용 전체 호스트 서버 데이터 블록, 4-140페이지의 내용을 참조하십시오.
목록 블록 유형	uint32	네트워크 프로토콜 데이터를 전달하는 프로토콜 데이터 블록으로 구성된 목록 데이터 블록을 시작합니다. 이 값은 항상 11입니다.
목록 블록 길이	uint32	목록의 바이트 수입니다. 이 수에는 목록 블록 유형 및 길이 필드의 8바이트에 캡슐화된 모든 프로토콜 데이터 블록의 길이를 더한 값이 포함됩니다.
(네트워크) 프로토콜 데이터 블록*	variable	호스트의 네트워크 프로토콜에 대한 데이터를 전달하는 프로토콜 데이터 블록의 목록입니다. 이 데이터 블록에 대한 설명은 프로토콜 데이터 블록, 4-77페이지의 내용을 참조하십시오.
목록 블록 유형	uint32	전송 프로토콜 데이터를 전달하는 프로토콜 데이터 블록으로 구성된 목록 데이터 블록을 시작합니다. 이 값은 항상 11입니다.
목록 블록 길이	uint32	목록의 바이트 수입니다. 이 수에는 목록 블록 유형 및 길이 필드의 8바이트에 캡슐화된 모든 프로토콜 데이터 블록의 길이를 더한 값이 포함됩니다.
(전송) 프로토콜 데이터 블록*	variable	호스트의 전송 프로토콜에 대한 데이터를 전달하는 프로토콜 데이터 블록의 목록입니다. 이 데이터 블록에 대한 설명은 프로토콜 데이터 블록, 4-77페이지의 내용을 참조하십시오.
목록 블록 유형	uint32	MAC 주소 데이터 블록이 포함된 목록 데이터 블록을 시작합니다. 이 값은 항상 11입니다.
목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 호스트 MAC 주소 데이터 블록을 포함한 목록의 바이트 수입니다.
호스트 MAC 주소 데이터 블록*	variable	호스트 MAC 주소 데이터 블록의 목록입니다. 이 데이터 블록에 대한 설명은 4.9 이상 버전용 호스트 MAC 주소, 4-117페이지의 내용을 참조하십시오.
마지막 확인	uint32	시스템이 호스트 활동을 마지막으로 탐지한 시간을 나타내는 UNIX 타임스탬프입니다.
호스트 유형	uint32	호스트 유형을 나타냅니다. 값은 다음과 같습니다. • 0 - 호스트 • 1 - 라우터 • 2 - 브리지 • 3 -NAT(Network Address Translation) 디바이스 • 4 - LB(로드 밸런서)
비즈니스 임계성	uint16	비즈니스에 대한 호스트의 임계성을 나타냅니다.
VLAN ID	uint16	호스트가 구성원으로 포함된 VLAN을 나타내는 VLAN ID 번호입니다.

표 5-1 5.3 이상 버전용 전체 호스트 프로파일 레코드 필드 (계속)

필드	데이터 유형	설명
VLAN 유형	uint8	VLAN 태그에 캡슐화된 패킷 유형입니다.
VLAN 우선순위	uint8	VLAN 태그에 포함된 우선순위 값입니다.
일반 목록 블록 유형	uint32	클라이언트 애플리케이션 데이터를 전달하는 호스트 취약점 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 클라이언트 애플리케이션 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
전체 호스트 클라이언트 애플리케이션 데이터 블록*	variable	클라이언트 애플리케이션 데이터 블록의 목록입니다. 이 데이터 블록에 대한 설명은 5.0 이상 버전용 전체 호스트 클라이언트 애플리케이션 데이터 블록, 4-154페이지의 내용을 참조하십시오.
문자열 블록 유형	uint32	호스트 NetBIOS 이름에 대한 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이 필드의 8바이트에 NetBIOS 이름 문자열의 바이트 수를 더한 값이 포함됩니다.
NetBIOS 이름	string	호스트 NetBIOS 이름 문자열입니다.
문자열 블록 유형	uint32	호스트 메모에 대한 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	메모 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 메모의 바이트 수를 더한 값이 포함됩니다.
메모	string	호스트에 대한 메모 호스트 속성의 콘텐츠를 포함합니다.
일반 목록 블록 유형	uint32	VDB 취약점 데이터를 전달하는 호스트 취약점 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
(VDB) 호스트 취약점 데이터 블록*	variable	Cisco VDB(취약점 데이터베이스)에서 식별된 취약점에 대한 호스트 취약점 데이터 블록의 목록입니다. 이 데이터 블록에 대한 설명은 4.9.0 이상 버전용 호스트 취약점 데이터 블록, 4-114페이지의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	서드파티 취약점 스캔 데이터를 전달하는 호스트 취약점 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
(서드파티/VDB) 호스트 취약점 데이터 블록*	variable	Cisco VDB(취약점 데이터베이스)에 카탈로그화된 호스트 취약점에 대한 정보를 포함하며 서드파티 스캐너에서 제공한 호스트 취약점 데이터 블록입니다. 이 데이터 블록에 대한 설명은 4.9.0 이상 버전용 호스트 취약점 데이터 블록, 4-114페이지의 내용을 참조하십시오.

표 5-1 5.3 이상 버전용 전체 호스트 프로파일 레코드 필드 (계속)

필드	데이터 유형	설명
일반 목록 블록 유형	uint32	서드파티 취약점 스캔 데이터를 전달하는 호스트 취약점 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
(서드파티 스캔) 호스트 취약점 데이터 블록*	variable	서드파티 스캐너에서 제공한 호스트 취약점 데이터 블록입니다. 이러한 데이터 블록의 호스트 취약점 ID는 Cisco에서 탐지한 ID가 아니라 서드파티 스캐너 ID입니다. 이 데이터 블록에 대한 설명은 4.9.0 이상 버전용 호스트 취약점 데이터 블록, 4-114페이지의 내용을 참조하십시오.
목록 블록 유형	uint32	속성 데이터를 전달하는 속성값 데이터 블록으로 구성된 목록 데이터 블록을 시작합니다. 이 값은 항상 11입니다.
목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 데이터 블록을 포함한 목록 데이터 블록의 바이트 수입니다.
속성값 데이터 블록*	variable	속성값 데이터 블록의 목록입니다. 이 목록의 데이터 블록에 대한 설명은 속성값 데이터 블록, 4-83페이지의 내용을 참조하십시오.
모바일	uint8	운영 체제가 모바일 디바이스에서 실행되고 있는지를 나타내는 true-false 플래그입니다.
탈옥됨	uint8	모바일 디바이스의 운영 체제가 탈옥되었는지 나타내는 true-false 플래그입니다.
일반 목록 블록 유형	uint32	IOC 상태 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 IOC 상태 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
IOC 상태 데이터 블록*	variable	호스트의 보안 침해에 대한 정보가 포함된 IOC 상태 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.3 이상 버전용 IOC 상태 데이터 블록, 4-35페이지의 내용을 참조하십시오.

eStreamer 구성

클라이언트 애플리케이션을 생성한 후에는 eStreamer 서버에 애플리케이션을 연결하고 eStreamer 서비스를 시작하여 데이터 교환을 시작할 수 있습니다.

참고 *eStreamer 서버*는 eStreamer 서비스를 실행 중인 Management Center 또는 매니지드 디바이스(버전 4.9 이상)입니다.

eStreamer 및 클라이언트 상호 작용을 관리하려면 다음 작업을 수행합니다.

1. eStreamer 서버에서 eStreamer를 활성화합니다.

   eStreamer 서버에 대한 액세스를 허용하고, 클라이언트를 추가하고, 인증된 연결을 설정하기 위한 인증 크리덴셜을 생성하는 방법에 대한 자세한 정보는 eStreamer 서버에서 eStreamer 구성, 6-1페이지의 내용을 참조하십시오.

2. 필요한 경우 수동으로 eStreamer 서비스(eStreamer)를 실행합니다. 서비스를 중지/시작하고, 서비스 상태를 확인하고, 커맨드 라인 옵션을 사용하여 클라이언트-서버 통신을 디버그할 수 있습니다.

   자세한 정보는 eStreamer 서비스 관리, 6-4페이지의 내용을 참조하십시오.

3. 필요에 따라 eStreamer 참조 클라이언트를 사용하여 연결 또는 데이터 스트림을 트러블슈팅하려면 클라이언트를 실행할 컴퓨터에 참조 클라이언트를 설치합니다.

   eStreamer 참조 클라이언트 구성, 6-6페이지의 내용을 참조하십시오.

eStreamer 서버에서 eStreamer 구성

라이센스: 모두

eStreamer 서버로 사용할 Management Center 또는 매니지드 디바이스가 클라이언트 애플리케이션으로 이벤트 스트리밍을 시작할 수 있도록 하려면 클라이언트로 이벤트를 전송하고, 클라이언트에 대한 정보를 제공하고, 통신 설정 시 사용할 인증 크리덴셜 집합을 생성하도록 eStreamer 서버를 구성해야 합니다. Management Center 또는 매니지드 디바이스 사용자 인터페이스에서 이 모든 작업을 수행할 수 있습니다.

자세한 내용은 다음 섹션을 참조하십시오.

- eStreamer 이벤트 유형 구성, 6-2페이지
- eStreamer 클라이언트에 대한 인증 추가, 6-3페이지

eStreamer 이벤트 유형 구성

라이센스: 모두

eStreamer 서버가 이벤트를 요청하는 클라이언트 애플리케이션에 전송할 수 있는 이벤트 유형을 제어할 수 있습니다.

매니지드 디바이스 또는 Management Center에서 사용 가능한 이벤트 유형은 다음과 같습니다.

- 침입 이벤트
- 침입 이벤트 패킷 데이터
- 침입 이벤트 추가 데이터

Management Center에서 사용할 수 있는 이벤트 유형은 다음과 같습니다.

- 검색 이벤트(연결 이벤트도 활성화할 수 있음)
- 상관관계 및 화이트리스트 이벤트
- 영향 플래그 알림
- 사용자 활동 이벤트
- 악성코드 이벤트
- 파일 이벤트

스택형 3D9900 쌍의 기본 디바이스와 보조 디바이스는 개별 매니지드 디바이스인 것처럼 Management Center에 침입 이벤트를 보고합니다. 3D9900 스택의 기본 디바이스에서 eStreamer 클라이언트와의 통신을 구성하는 경우에는 보조 디바이스에서도 클라이언트를 구성해야 합니다. 클라이언트 컨피그레이션은 복제되지 않습니다. 마찬가지로 클라이언트를 삭제할 때는 두 디바이스에서 모두 삭제합니다. 스택 컨피그레이션에서 3D9900을 관리하는 Management Center용으로 eStreamer 클라이언트를 구성하는 경우 Management Center는 두 매니지드 디바이스에서 같은 이벤트를 보고하더라도 두 디바이스에서 수신하는 모든 이벤트를 보고합니다.

고가용성 컨피그레이션에서 Management Center에 eStreamer 클라이언트를 구성하는 경우에는 기본 Management Center에서 보조 Management Center로 클라이언트 컨피그레이션이 복제되지 않습니다.

eStreamer에서 캡처되는 이벤트 유형을 구성하려면 다음을 수행합니다.

액세스: 관리자

1단계 **System(시스템) > Integration(통합) > eStreamer**를 선택합니다.

2단계 **eStreamer**를 클릭합니다.

eStreamer Event Configuration(이벤트 컨피그레이션) 메뉴가 포함된 eStreamer 페이지가 나타납니다.

3단계 eStreamer에서 캡처하여 요청 클라이언트로 전달하도록 할 이벤트 유형 옆에 있는 체크 박스를 선택합니다. 체크 박스가 현재 선택되어 있지 않으면 해당 데이터가 캡처되고 있지 않은 것입니다. 체크 박스 선택을 취소해도 이미 캡처된 데이터는 삭제되지 않습니다.

Management Center 또는 매니지드 디바이스에서 다음 중 하나 또는 전체를 선택할 수 있습니다.

- 매니지드 디바이스에서 생성된 침입 이벤트를 전송하는 **Intrusion Events(침입 이벤트)**
- 침입 이벤트와 관련된 패킷을 전송하는 **Intrusion Event Packet Data(침입 이벤트 패킷 데이터)**
- 침입 이벤트와 관련된 추가 데이터(HTTP 프록시 또는 로드 밸런서를 통해 웹 서버에 연결하는 클라이언트의 원래 IP 주소와 관련된 URI 등)를 전송하는 **Intrusion Event Extra Data(침입 이벤트 추가 데이터)**

또한 Management Center에서 다음 중 하나 또는 전체를 선택할 수 있습니다.

- 호스트 검색 이벤트를 전송하는 **Discovery Events(검색 이벤트)**
- 상관관계 및 화이트리스트 이벤트를 전송하는 **Correlation Events(상관관계 이벤트)**
- Management Center에 의해 생성된 영향 알림을 전송하는 **Impact Flag Alerts(영향 플래그 알림)**
- 사용자 이벤트를 전송하는 **User Activity Events(사용자 활동 이벤트)**
- 침입 이벤트에 대한 추가 데이터(HTTP 프록시 또는 로드 밸런서를 통해 웹 서버에 연결하는 클라이언트의 원래 IP 주소와 관련된 URI 등)를 전송하는 **Intrusion Event Extra Data(침입 이벤트 추가 데이터)**

참고 이렇게 하면 eStreamer 서버에서 전송할 수 있는 이벤트를 제어할 수 있습니다. 클라이언트 애플리케이션은 해당 애플리케이션이 수신하도록 할 이벤트 유형을 계속 구체적으로 요청해야 합니다. 자세한 정보는 요청 플래그, 2-12페이지의 내용을 참조하십시오.

4단계 **Save(저장)**를 클릭합니다.

설정이 저장되고 선택한 이벤트는 요청 시 eStreamer클라이언트에 전달됩니다.

eStreamer 클라이언트에 대한 인증 추가

라이센스: 모두

eStreamer가 클라이언트로 이벤트를 전송하려면 eStreamer 서버의 피어 데이터베이스에 클라이언트를 추가해야 합니다. 또한 eStreamer 서버에서 생성된 인증 인증서를 클라이언트에 복사해야 합니다.

eStreamer 클라이언트를 추가하려면 다음을 수행합니다.

액세스: 관리자

1단계 **System(시스템) > Integration(통합) > eStreamer**를 선택합니다.

eStreamer 페이지가 나타납니다.

2단계 **Create Client(클라이언트 생성)**를 클릭합니다.

Create Client(클라이언트 생성) 페이지가 나타납니다.

3단계 **Hostname(호스트 이름)** 필드에 eStreamer 클라이언트를 실행하는 호스트의 IP 주소 또는 호스트 이름을 입력합니다.

참고 호스트 이름을 사용하는 경우 호스트 입력 서버는 호스트를 IP 주소로 확인할 수 **있어야 합니다**. DNS 확인을 설정하지 않은 경우, 이를 먼저 구성하거나 IP 주소를 사용해야 합니다.

4단계 인증서 파일을 암호화하려면, **Password(비밀번호)** 필드에 비밀번호를 입력합니다.

5단계 **Save(저장)**를 클릭합니다.

eStreamer 서버는 클라이언트 컴퓨터가 Management Center의 포트 8302에 액세스하도록 허용하며 클라이언트-서버 인증 중에 사용할 인증 인증서를 생성합니다. eStreamer Client(eStreamer 클라이언트) 페이지가 다시 나타나며 **eStreamer Clients(eStreamer 클라이언트)** 아래에 새 클라이언트가 나열됩니다.

6단계 인증서 파일 옆에 있는 다운로드 아이콘( )을 클릭합니다.

7단계 SSL 인증을 위해 클라이언트 컴퓨터에서 사용하는 디렉터리에 인증서 파일을 저장합니다.

이제 클라이언트가 Management Center에 연결할 수 있습니다.

팁 클라이언트에 대한 액세스를 취소하려면, 제거할 호스트 옆에 있는 삭제 아이콘( )을 클릭합니다. Management Center에서 호스트 입력 서비스를 재시작할 필요는 없으며, 액세스는 즉시 취소됩니다.

eStreamer 서비스 관리

라이센스: 모두

사용자 인터페이스에서 eStreamer 서비스를 관리할 수 있습니다. 그러나 커맨드 라인을 사용하여 서비스를 시작하고 중지할 수도 있습니다. 다음 섹션에서는 eStreamer 커맨드 라인 옵션에 대해 설명합니다.

- eStreamer 서비스 시작 및 중지, 6-4페이지에서는 eStreamer 서비스를 시작하고 중지하는 방법을 설명합니다.
- eStreamer 서비스 옵션, 6-5페이지에서는 eStreamer 서비스에 사용할 수 있는 커맨드 라인 옵션 및 해당 옵션을 사용하는 방법을 설명합니다.

eStreamer 서비스 시작 및 중지

라이센스: 모두

`manage_estreamer.pl` 스크립트를 사용하여 eStreamer 서비스를 관리할 수 있습니다. 이 경우 서비스를 시작, 중지, 다시 로드 및 재시작할 수 있습니다.

팁 eStreamer 초기화 스크립트에 커맨드 라인 옵션을 추가할 수도 있습니다. 자세한 정보는 eStreamer 서비스 옵션, 6-5페이지의 내용을 참조하십시오.

다음 표에는 Management Center 또는 매니지드 디바이스에서 사용할 수 있는 `manage_estreamer.pl` 스크립트의 옵션에 대한 설명이 나와 있습니다.

표 6-1 eStreamer 관리 옵션

옵션	설명	선택해야 하는 옵션 번호...
enable	서비스를 시작합니다.	3
disable	서비스를 중지합니다.	2
restart	서비스를 재시작합니다.	4
status	서비스가 실행 중인지를 나타냅니다.	1

eStreamer 서비스 옵션

라이센스: 모두

eStreamer에서는 서비스를 트러블슈팅할 수 있는 여러 가지 서비스 옵션을 제공합니다. 다음 표에 설명되어 있는 옵션을 eStreamer 서비스에 사용할 수 있습니다.

표 6-2 eStreamer 서비스 옵션

옵션	설명
`--debug`	디버그 레벨 로깅을 사용하여 eStreamer를 실행합니다. 오류는 syslog에 저장되며 `--nodaemon`과 함께 사용하는 경우 화면에 나타납니다.
`--nodaemon`	포그라운드 프로세스로 eStreamer를 실행합니다. 오류는 화면에 나타납니다.
`--nohostcheck`	호스트 이름 확인을 비활성화하여 eStreamer를 실행합니다. 즉, 클라이언트 호스트 이름이 클라이언트 인증서의 subjectAltName:dNSName 엔트리에 포함된 호스트 이름과 일치하지 않아도 액세스는 계속 허용됩니다. `nohostcheck` 옵션은 네트워크 DNS 및/또는 NAT 컨피그레이션으로 인해 호스트 이름 확인이 실패하는 경우에 유용합니다. 기타 모든 보안 검사는 수행됩니다. ⚠ **주의** 이 옵션을 활성화하면 시스템의 보안 레벨이 낮아질 수 있습니다.

먼저 eStreamer 서비스를 중지한 다음 원하는 옵션을 사용하여 서비스를 실행하고, 마지막으로 서비스를 재시작하는 방식으로 위의 옵션을 사용하십시오. 예를 들어 디버그 모드에서 eStreamer 서비스 실행, 6-5페이지에 제공된 지침에 따라 eStreamer 기능을 디버그할 수 있습니다.

디버그 모드에서 eStreamer 서비스 실행

라이센스: 모두

디버그 모드에서 eStreamer 서비스를 실행하여 터미널 화면에서 서비스가 생성하는 각 상태 메시지를 확인할 수 있습니다. 다음 절차에 따라 디버깅을 수행합니다.

디버그 모드에서 eStreamer 서비스를 실행하려면 다음을 수행합니다.

액세스: 관리자

1단계 SSH를 사용하여 Management Center 또는 매니지드 디바이스에 로그인합니다.

2단계 `manage_estreamer.pl`을 사용하고 옵션 `2`를 선택하여 eStreamer 서비스를 중지합니다.

3단계 `./usr/local/sf/bin/sfestreamer --nodaemon --debug`를 사용하여 디버그 모드에서 eStreamer 서비스를 재시작합니다.

서비스의 상태 메시지가 터미널 화면에 나타납니다.

4단계 디버깅이 완료되면 `manage_estreamer.pl`을 사용하고 옵션 `4`를 선택하여 일반 모드에서 서비스를 재시작합니다.

eStreamer 참조 클라이언트 구성

eStreamer SDK와 함께 제공되는 *참조 클라이언트*는 eStreamer API를 사용할 수 있는 방법을 보여 주기 위해 포함된 샘플 클라이언트 스크립트 및 Perl 모듈 집합입니다. 이러한 스크립트와 모듈을 실행하여 eStreamer 출력의 내용을 파악할 수도 있고, 맞춤형으로 빌드한 클라이언트 설치 시의 문제를 디버그하기 위해 해당 스크립트와 모듈을 사용할 수도 있습니다.

참조 클라이언트를 설정하는 방법에 대한 자세한 내용은 다음 섹션을 참조하십시오.

- eStreamer Perl 참조 클라이언트 설정, 6-6페이지
- eStreamer Perl 참조 클라이언트 실행, 6-12페이지

eStreamer Perl 참조 클라이언트 설정

eStreamer Perl 참조 클라이언트를 사용하려면 먼저 환경 및 요구 사항에 맞게 샘플 스크립트를 구성해야 합니다.

자세한 내용은 다음 섹션을 참조하십시오.

- eStreamer Perl 참조 클라이언트 이해, 6-6페이지
- eStreamer 참조 클라이언트에 대한 통신 구성, 6-7페이지
- Perl 참조 클라이언트의 일반 전제조건 로드, 6-8페이지
- Perl SNMP 참조 클라이언트의 전제조건 로드, 6-8페이지
- 테스트 스크립트를 통해 요청하는 데이터 이해, 6-8페이지
- 테스트 스크립트를 통해 요청하는 데이터 유형 수정, 6-9페이지
- Perl 참조 클라이언트용 인증서 생성, 6-11페이지

eStreamer Perl 참조 클라이언트 이해

eStreamer Perl 참조 클라이언트가 포함된 `eStreamerSDK.zip` 패키지는 Cisco 지원 사이트에서 다운로드할 수 있습니다. `eStreamerSDK.zip` 패키지에는 다음 파일이 포함되어 있습니다.

- `SF_CUSTOM_ALERT.MIB`

  이 MIB 파일은 `snmp.pm` 파일에서 SNMP용 트랩을 설정하는 데 사용됩니다.

- `SFRecords.pm`

  이 Perl 모듈은 검색 메시지 레코드 블록의 정의를 포함합니다.

- `SFStreamer.pm`

  이 Perl 모듈은 Perl 클라이언트가 호출하는 함수를 포함합니다.

- `SFPkcs12.pm`

  이 Perl 모듈은 클라이언트 인증서를 구문 분석하며 클라이언트가 eStreamer 서버에 연결하도록 허용합니다.

- `SFRNABlocks.pm`

  이 Perl 모듈은 검색 데이터 블록의 정의를 포함합니다.

- `ssl_test.pl`

  이 Perl 스크립트를 사용하면 SSL 연결을 통해 침입 이벤트 요청을 테스트할 수 있습니다.

- `OutputPlugins/csv.pm`

  이 Perl 모듈은 CSV(쉼표로 구분된 값) 형식으로 침입 이벤트를 인쇄합니다.

- `OutputPlugins/print.pm`

  이 Perl 모듈은 사용자가 읽을 수 있는 형식으로 이벤트를 인쇄합니다.

- `OutputPlugins/snmp.pm`

  이 Perl 모듈은 지정된 SNMP 서버로 이벤트를 보냅니다.

- `OutputPlugins/pcap.pm`

  이 Perl 모듈은 패킷 캡처를 pcap 파일로 저장합니다.

- `OutputPlugins/syslog.pm`

  이 Perl 모듈은 로컬 syslog 서버로 이벤트를 보냅니다.

eStreamer 참조 클라이언트에 대한 통신 구성

참조 클라이언트는 데이터 통신에 SSL(Secure Sockets Layer)을 사용합니다. 클라이언트로 사용할 컴퓨터에 OpenSSL을 설치하고 환경에 적합하게 해당 컴퓨터를 구성해야 합니다.

참고 Linux 운영 체제에 처음 설치할 때는 이 다운로드의 일부분으로 `libssl-dev` 구성 요소를 설치해야 합니다.

클라이언트에서 SSL을 설정하려면 다음을 수행합니다.

1단계 http://openssl.org/source/에서 OpenSSL을 다운로드합니다.

2단계 `/usr/local/src`에 소스의 압축을 풉니다.

3단계 구성 스크립트를 실행하여 소스를 구성합니다.

4단계 컴파일된 소스를 만들고 설치합니다.

Perl 참조 클라이언트의 일반 전제조건 로드

eStreamer Perl 참조 클라이언트를 실행하려면 클라이언트 컴퓨터에 `IO::Socket::SSL` Perl 모듈을 설치해야 합니다. 이 모듈은 수동으로 설치할 수도 있고 `cpan`을 사용하여 설치할 수도 있습니다.

참고 `Net::SSLeay` 모듈이 클라이언트 컴퓨터에 설치되어 있지 않은 경우에는 해당 모듈도 설치합니다. `Net::SSLeay`는 OpenSSL을 사용한 통신에 필요합니다.

또한 OpenSSL도 설치하고 eStreamer 서버에 대한 SSL 연결을 지원하도록 구성해야 합니다. 자세한 정보는 eStreamer 참조 클라이언트에 대한 통신 구성, 6-7페이지의 내용을 참조하십시오.

Perl SNMP 참조 클라이언트의 전제조건 로드

Perl 참조 클라이언트의 eStreamer SNMP 모듈을 실행하려면 클라이언트 운영 체제용으로 제공되는 최신 `net-snmp` Perl 모듈을 클라이언트 컴퓨터에 설치해야 합니다.

Perl 참조 클라이언트 다운로드 및 압축 풀기

eStreamer Perl 참조 클라이언트가 포함된 `EventStreamerSDK.zip` 파일은 Cisco 지원 사이트에서 다운로드할 수 있습니다.

클라이언트를 실행하려는 Linux 운영 체제를 실행 중인 컴퓨터에 zip 파일의 압축을 풉니다.

테스트 스크립트를 통해 요청하는 데이터 이해

기본적으로 참조 클라이언트에서 `ssl_test -o` 설정을 사용할 때는 다음 표에 나와 있는 데이터를 요청합니다.

표 6-3 출력 플러그인으로 수행하는 기본 요청

구문...	호출하는 플러그인...	전송하는 요청...	요청하려는 데이터...
`./ssl_test.pl` *`eStreamerServerName`* `-h HostIPAddresses`	해당 없음	비트 11이 `1`로 설정된 호스트 요청(메시지 유형 5)	호스트 데이터(호스트 데이터 및 여러 호스트 데이터 메시지 형식, 2-30페이지 참조)
`./ssl_test.pl` *`eStreamerServerName`* `-d "Global \ domain \ subdomain"`	해당 없음	지정된 도메인이나 하위 도메인에 대한 이벤트 스트림 요청	지정된 도메인에 대한 스트리밍 이벤트 정보(도메인 스트리밍 요청 메시지 형식, 2-35페이지 참조)
`./ssl_test.pl` *`eStreamerServerName`* `-o print -f` *`TextFile`*	OutputPlugins/print.pm	비트 2 및 20~24가 `1`로 설정된 이벤트 스트림 요청(메시지 유형 2)	이벤트 데이터(이벤트 스트림 요청 메시지 형식, 2-10페이지, 상관관계 정책 레코드, 3-23페이지, 상관관계 규칙 레코드, 3-25페이지, 검색 이벤트의 메타데이터, 4-6페이지, 이벤트 유형별 호스트 검색 구조, 4-44페이지 및 이벤트 유형별 사용자 데이터 구조, 4-62페이지 참조) 이벤트 스트림 요청에서 비트 2가 설정되어 있으므로 eStreamer는 유형 1 침입 이벤트를 전송합니다.

표 6-3 출력 플러그인으로 수행하는 기본 요청 (계속)

구문...	호출하는 플러그인...	전송하는 요청...	요청하려는 데이터...
`./ssl_test.pl eStreamerServerName -o pcap -f TargetPCAPFile`	OutputPlugins/pcap.pm	비트 0 및 23이 1로 설정된 이벤트 스트림 요청(메시지 유형 2)	패킷 데이터(이벤트 데이터 메시지 형식, 2-17페이지 및 4.8.0.2 이상 버전용 패킷 레코드, 3-6페이지 참조) 이벤트 스트림 요청에서 비트 0이 설정되어 있으므로 eStreamer는 패킷 데이터만 전송합니다.
`./ssl_test.pl eStreamerServerName -o csv -f CSVFile`	OutputPlugins/csv.pm	비트 2 및 23이 1로 설정된 이벤트 스트림 요청(메시지 유형 2)	침입 이벤트 데이터(이벤트 데이터 메시지 형식, 2-17페이지 및 6.0 이상 버전용 침입 이벤트 레코드, 3-8페이지 참조) 이벤트 스트림 요청에서 비트 2가 설정되어 있으므로 eStreamer는 유형 1 침입 이벤트를 전송합니다.
`./ssl_test.pl eStreamerServerName -o snmp -f SNMPServer`	OutputPlugins/snmp.pm	비트 2, 20 및 23이 1로 설정된 이벤트 스트림 요청(메시지 유형 2)	침입 이벤트 데이터(이벤트 데이터 메시지 형식, 2-17페이지 및 6.0 이상 버전용 침입 이벤트 레코드, 3-8페이지 참조) 이벤트 스트림 요청에서 비트 2가 설정되어 있으므로 eStreamer는 유형 1 침입 이벤트를 전송합니다.
`./ssl_test.pl eStreamerServerName -o syslog`	OutputPlugins/syslog.pm	비트 2, 20 및 23이 1로 설정된 이벤트 스트림 요청(메시지 유형 2)	침입 이벤트 데이터(이벤트 데이터 메시지 형식, 2-17페이지 및 6.0 이상 버전용 침입 이벤트 레코드, 3-8페이지 참조) 이벤트 스트림 요청에서 비트 2가 설정되어 있으므로 eStreamer는 유형 1 침입 이벤트를 전송합니다.

테스트 스크립트를 통해 요청하는 데이터 유형 수정

`SFStreamer.pm` Perl 모듈은 샘플 스크립트에서 데이터를 요청하는 데 사용할 수 있는 여러 요청 플래그 변수를 정의합니다. 다음 표에는 이벤트 스트림 요청 메시지에서 각 요청 플래그를 설정하기 위해 호출해야 하는 요청 플래그 변수가 나와 있습니다. 출력 모듈 중 하나를 사용하여 다른 데이터를 요청하려는 경우 모듈의 `$FLAG` 설정을 편집하면 됩니다.

요청 플래그에 대한 자세한 내용과 각 플래그에 해당하는 제품 버전은 요청 플래그, 2-12페이지의 내용을 참조하십시오.

표 6-4 샘플 스크립트에서 사용되는 요청 플래그 변수

변수	설정되는 요청 플래그...	요청하려는 데이터...
`$FLAG_PKTS`	0	패킷 데이터
`$FLAG_METADATA`	1	버전 1 메타데이터
`$FLAG_IDS`	2	유형 1 침입 이벤트
`$FLAG_RNA`	3	버전 1 검색 이벤트
`$FLAG_POLICY_EVENTS`	4	버전 1 상관관계 이벤트
`$FLAG_IMPACT_ALERTS`	5	침입 영향 알림
`$FLAG_IDS_IMPACT_FLAG`	6	유형 7 침입 이벤트
`$FLAG_RNA_EVENTS_2`	7	버전 2 검색 이벤트

표 6-4 샘플 스크립트에서 사용되는 요청 플래그 변수 (계속)

변수	설정되는 요청 플래그...	요청하려는 데이터...
$FLAG_RNA_FLOW	8	버전 1 연결 데이터
$FLAG_POLICY_EVENTS_2	9	버전 2 상관관계 이벤트
$FLAG_RNA_EVENTS_3	10	버전 3 검색 이벤트
$FLAG_HOST_ONLY	11	$FLAG_HOST_SINGLE(호스트 하나) 또는 $FLAG_HOST_MULTI(여러 호스트)와 함께 전송하는 경우 이벤트 데이터가 없는 호스트 데이터만 요청
$FLAG_RNA_FLOW_3	12	버전 3 연결 데이터
$FLAG_POLICY_EVENTS_3	13	버전 3 상관관계 이벤트
$FLAG_METADATA_2	14	버전 2 메타데이터
$FLAG_METADATA_3	15	버전 3 메타데이터
$FLAG_RNA_EVENTS_4	17	버전 4 검색 이벤트
$FLAG_RNA_FLOW_4	18	버전 4 연결 데이터
$FLAG_POLICY_EVENTS_4	19	버전 4 상관관계 이벤트
$FLAG_METADATA_4	20	버전 4 메타데이터
$FLAG_RUA	21	사용자 활동 이벤트
$FLAG_POLICY_EVENTS_5	22	버전 5 상관관계 이벤트
$FLAGS_SEND_ARCHIVE_TIMESTAMP	23	eStreamer 서버에서 처리하도록 이벤트가 아카이브되었을 때 적용된 타임스탬프를 포함하는 확장 이벤트 헤더
$FLAG_RNA_EVENTS_5	24	버전 5 검색 이벤트
$FLAG_RNA_EVENTS_6	25	버전 6 검색 이벤트
$FLAG_RNA_FLOW_5	26	버전 5 연결 데이터
$FLAG_EXTRA_DATA	27	침입 이벤트 추가 데이터 레코드
$FLAG_RNA_EVENTS_7	28	버전 7 검색 이벤트
$FLAG_POLICY_EVENTS_6	29	버전 6 상관관계 이벤트
$FLAG_DETAIL_REQUEST	30	eStreamer에 대한 확장 요청

주의 5.x 이전 버전에서는 모든 이벤트 유형에서 참조 클라이언트가 detection engine ID(탐지 엔진 ID) 필드의 레이블을 sensor ID(센서 ID)로 지정합니다.

Perl 참조 클라이언트용 인증서 생성

라이센스: 모두

Perl 참조 클라이언트를 사용하려면 클라이언트를 실행하려는 컴퓨터용으로 Management Center 또는 매니지드 디바이스에서 인증서를 생성해야 합니다. 그런 다음 인증서 파일을 클라이언트 컴퓨터에 다운로드하여 인증서(`server.crt`) 및 RSA 키 파일(`server.key`)을 생성하는 데 사용합니다.

Perl 참조 클라이언트용 인증서를 생성하려면 다음을 수행합니다.

액세스: 관리자

1단계 **System(시스템) > Integration(통합) > eStreamer**를 선택합니다.

eStreamer 페이지가 나타납니다.

2단계 **Create Client(클라이언트 생성)**를 클릭합니다.

Create Client(클라이언트 생성) 페이지가 나타납니다.

3단계 **Hostname(호스트 이름)** 필드에 eStreamer 클라이언트를 실행하는 호스트의 IP 주소 또는 호스트 이름을 입력합니다.

참고 호스트 이름을 사용하는 경우 호스트 입력 서버는 호스트를 IP 주소로 확인할 수 **있어야 합니다**. DNS 확인을 설정하지 않은 경우, 이를 먼저 구성하거나 IP 주소를 사용해야 합니다.

4단계 인증서 파일을 암호화하려면, **Password(비밀번호)** 필드에 비밀번호를 입력합니다.

5단계 **Save(저장)**를 클릭합니다.

eStreamer 서버는 클라이언트 컴퓨터가 Management Center의 포트 8302에 액세스하도록 허용하며 클라이언트-서버 인증 중에 사용할 인증 인증서를 생성합니다. eStreamer Client(eStreamer 클라이언트) 페이지가 다시 나타나며 **eStreamer Clients(eStreamer 클라이언트)** 아래에 새 클라이언트가 나열됩니다.

6단계 인증서 파일 옆에 있는 다운로드 아이콘( )을 클릭합니다.

7단계 SSL 인증을 위해 클라이언트 컴퓨터에서 사용하는 디렉터리에 인증서 파일을 저장합니다.

이제 클라이언트가 Management Center에 연결할 수 있습니다.

팁 클라이언트에 대한 액세스를 취소하려면, 제거할 호스트 옆에 있는 삭제 아이콘( )을 클릭합니다. Management Center에서 호스트 입력 서비스를 재시작할 필요는 없으며, 액세스는 즉시 취소됩니다.

eStreamer Perl 참조 클라이언트 실행

eStreamer Perl 참조 클라이언트 스크립트는 Linux 커널이 설치된 64비트 운영 체제에서 사용하도록 설계된 것이지만 클라이언트 머신이 eStreamer Perl 참조 클라이언트 설정, 6-6페이지에 정의된 전제조건을 충족한다면 모든 POSIX 기반 64비트 운영 체제에서 작동합니다.

자세한 내용은 다음 섹션을 참조하십시오.

호스트 요청을 사용하여 SSL을 통한 클라이언트 연결 테스트

`ssl_test.pl` 스크립트를 사용하여 eStreamer 서버와 eStreamer 클라이언트 간의 연결을 테스트할 수 있습니다. `ssl_test.pl` 스크립트는 모든 레코드 유형을 처리하여 STDOUT 또는 사용자가 지정한 출력 플러그인에 인쇄합니다. 출력 옵션 없이 `-h` 옵션을 사용하는 경우 지정한 호스트에 대한 호스트 데이터가 터미널로 스트리밍됩니다.

참고 이 스크립트를 사용하여 패킷 데이터를 출력 플러그인으로 보내지 않고 스트리밍할 수는 없습니다. STDOUT에 원시 패킷 데이터를 인쇄하는 작업이 터미널의 작동을 방해하기 때문입니다.

`ssl_test.pl` 스크립트를 사용하여 표준 출력으로 호스트 데이터를 전송하려면 다음 구문을 사용합니다.

```
./ssl_test.pl eStreamerServerIPAddress -h HostIPAddresses
```

예를 들어 IP 주소 10.10.0.4를 사용한 eStreamer 서버로의 연결을 통해 10.0.0.0/8 서브넷의 호스트에 대한 호스트 데이터 수신을 테스트하려면 다음 구문을 사용합니다.

```
./ssl_test.pl 10.10.0.4 -h 10.0.0.0/8
```

참조 클라이언트를 사용하여 PCAP 캡처

참조 클라이언트를 사용하여 PCAP 파일의 스트리밍된 패킷 데이터를 캡처하면 클라이언트가 수신하는 데이터의 구조를 확인할 수 있습니다. `-o pcap` 출력 옵션을 사용할 때 대상 파일을 지정하려면 `-f`를 사용해야 합니다.

`ssl_test.pl` 스크립트를 사용하여 PCAP 파일의 스트리밍된 패킷 데이터를 캡처하려면 다음 구문을 사용합니다.

```
./ssl_test.pl eStreamerServerIPAddress -o pcap -f ResultingPCAPFile
```

예를 들어 IP 주소 10.10.0.4를 통해 eStreamer 서버에서 스트리밍된 이벤트를 사용하여 이름이 `test.pcap`인 PCAP 파일을 만들려면 다음 구문을 사용합니다.

```
./ssl_test.pl 10.10.0.4 -o pcap -f test.pcap
```

참조 클라이언트를 사용하여 CSV 레코드 캡처

참조 클라이언트를 사용하여 CSV 파일의 스트리밍된 침입 이벤트 데이터를 캡처하면 클라이언트가 수신하는 데이터의 구조를 확인할 수도 있습니다.

`streamer_csv.pl` 스크립트를 실행하려면 다음 구문을 사용합니다.

`./ssl_test.pl` *`eStreamerServerIPAddress`* `-o csv -f` *`ResultingCSVFile`*

예를 들어 IP 주소 10.10.0.4를 통해 eStreamer 서버에서 스트리밍된 이벤트를 사용하여 이름이 `test.csv`인 CSV 파일을 만들려면 다음 구문을 사용합니다.

```
./ssl_test.pl 10.10.0.4 -o csv -f test.csv
```

참조 클라이언트를 사용하여 SNMP 서버로 레코드 보내기

참조 클라이언트를 사용하여 SNMP 서버로 침입 이벤트 데이터를 스트리밍할 수도 있습니다. 이벤트를 수신해야 하는 SNMP 트랩 서버의 이름을 지정하려면 `-f` 옵션을 사용합니다. 이 출력 방법을 사용하려면 경로에 `snmptrapd`라는 이진 파일이 필요하므로, 해당 방법은 UNIX 유형 시스템에서만 작동합니다.

SNMP 서버로 침입 이벤트를 보내려면 다음 구문을 사용합니다.

```
./ssl_test.pl eStreamerServerIPAddress -o snmp
   -f SNMPServerName
```

예를 들어 IP 주소 10.10.0.4를 통해 eStreamer 서버에서 스트리밍되는 이벤트를 사용하여 10.10.0.3에서 SNMP 서버로 이벤트를 보내려면 다음 구문을 사용합니다.

```
./ssl_test.pl 10.10.0.4 -o snmp -f 10.10.0.3
```

참조 클라이언트를 사용하여 Syslog에 이벤트 로깅

참조 클라이언트를 사용하여 클라이언트의 로컬 syslog 서버로 침입 이벤트를 스트리밍할 수도 있습니다.

syslog로 이벤트를 보내려면 다음 구문을 사용합니다.

```
./ssl_test.pl eStreamerServerIPAddress -o syslog
```

예를 들어 IP 주소 10.10.0.4를 통해 eStreamer 서버에서 스트리밍된 이벤트를 로깅하려면 다음 구문을 사용합니다.

```
./ssl_test.pl 10.10.0.4 -o syslog
```

IPv6 주소에 연결

참조 클라이언트를 사용하여 기본 관리 인터페이스를 통해 IPv6 주소로 Management Center에 연결할 수 있습니다. 이렇게 하려면 Socket6 및 IO::Socket::INET6 Perl 모듈이 클라이언트 머신에 설치되어 있어야 하며, `-ipv6` 옵션이나 단축된 형식인 `-i`를 사용해야 합니다.

ssl_test.pl 스크립트를 사용하여 IPv6 주소를 지정하려면 다음 구문을 사용합니다.

```
./ssl_test.pl -ipv6 eStreamerServerIPAddress
```

또는

```
./ssl_test.pl -i eStreamerServerIPAddress
```

예를 들어 IPv6 주소 `2001:470:e09c:20:7c1e:5248:1bf7:2ea0`을 사용하여 Management Center에 연결하려면 다음 구문을 사용합니다.

```
./ssl_test.pl -ipv6 2001:470:e09c:20:7c1e:5248:1bf7:2ea0
```

데이터 구조 예시

이 부록에는 선택한 침입, 상관관계 및 검색 이벤트의 데이터 구조 예시가 포함되어 있습니다. 각 비트가 설정되는 방식을 명확하게 보여 주기 위해 각 예시는 이진 형식으로 표시되어 있습니다.

자세한 내용은 다음 섹션을 참조하십시오.

- 침입 이벤트 데이터 구조 예시
- 검색 데이터 구조 예시, 페이지 A-31

침입 이벤트 데이터 구조 예시

이 섹션에는 eStreamer에서 침입 이벤트에 대해 전송할 수 있는 데이터 구조의 예시가 포함되어 있습니다. 제공되는 예시는 다음과 같습니다.

- Management Center 5.4 이상 버전용 침입 이벤트 예시, 페이지 A-2
- 침입 영향 알림 예시, 페이지 A-7
- 패킷 레코드 예시, 페이지 A-8
- 분류 레코드 예시, 페이지 A-10
- 우선순위 레코드 예시, 페이지 A-11
- 규칙 메시지 레코드 예시, 페이지 A-12
- 6.1.x 버전용 연결 통계 데이터 블록 예시, 페이지 A-14
- 5.1 이상 버전 사용자 이벤트 예시, 페이지 A-28

Management Center 5.4 이상 버전용 침입 이벤트 예시

다음 다이어그램에 예시 이벤트 레코드가 나와 있습니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	1	1	0
3	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	1	1	0
5	0	1	0	1	0	0	1	1	1	0	1	1	0	1	0	0	0	0	1	0	1	1	1	1	0	0	1	0	1	1	1	1
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	0	1
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	1	1	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	1	1	0	0
11	0	1	0	1	0	0	1	1	1	0	1	1	0	1	0	0	0	0	1	0	1	1	1	1	0	0	1	0	1	1	1	1
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	0	1	0	1	1	1	0	0	1	1	1	0
13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	1	1	1
15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1
18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	0	0	0	0	1	0	1	0	0	0	0	0	0	1	0	1	0	0	1	1	1	1	0	1	1	1	0	1	1	1	0	0
19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	0	0	0	0	1	0	1	0	0	0	0	0	0	1	0	1	0	0	1	1	1	0	0	0	1	0	0	0	0	1	0	1
20	1	0	0	0	0	0	0	0	1	1	1	1	1	0	1	0	0	0	0	1	1	1	1	1	1	0	0	1	0	0	0	0
21	0	0	0	0	0	1	1	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
24	1	0	1	0	1	0	0	0	0	0	0	1	1	0	0	1	1	1	0	1	0	0	1	1	0	1	1	1	1	1	1	0
	0	0	0	0	0	0	0	1	1	1	1	1	0	1	0	1	0	0	0	1	0	0	0	1	1	1	1	0	0	1	0	0
	1	0	1	0	0	1	0	0	1	0	0	0	0	1	0	1	1	1	0	1	0	0	0	0	0	1	1	1	0	0	0	1
	1	0	0	0	1	1	1	1	0	0	0	0	1	1	1	0	1	0	0	0	1	0	0	1	1	0	1	0	0	0	1	0
25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
26	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	0	0	1	1	1
27	0	1	1	1	0	1	1	1	0	0	1	1	0	1	0	1	1	0	0	1	0	1	1	0	1	0	1	0	0	1	0	0
28	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	1	0	0	1	0	0
29	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
30	1	1	0	0	0	0	0	1	0	1	0	0	0	1	0	0	0	0	1	0	1	1	1	0	0	1	0	0	1	1	1	0
	0	0	0	0	0	0	0	1	1	1	1	1	0	1	0	1	0	0	0	1	0	0	0	1	1	1	1	0	0	1	0	0
	1	0	1	0	0	1	0	1	1	1	1	1	0	1	1	0	1	0	1	1	0	0	1	1	0	0	0	0	1	0	0	1
	0	1	0	0	0	0	0	1	1	0	0	1	0	1	1	1	1	0	0	1	1	1	1	1	0	0	0	1	0	1	0	0
31	0	1	1	0	1	0	0	1	0	0	0	1	0	1	0	1	1	0	1	0	1	0	0	1	0	0	0	1	1	0	1	0
	1	1	1	1	1	1	1	0	0	0	1	1	1	0	0	1	0	0	0	1	0	0	0	1	1	1	1	0	0	0	1	1
	1	0	1	1	0	1	0	0	0	1	0	1	0	0	1	0	0	0	0	1	0	1	0	0	1	1	0	0	1	1	0	1
	1	0	1	0	1	0	1	1	0	0	0	1	0	1	0	0	1	1	0	0	1	1	1	1	1	0	0	1	1	1	0	0
32	0	1	1	0	1	0	0	1	0	0	0	1	0	1	0	1	1	0	1	0	1	0	0	1	0	0	0	1	1	0	1	0
	1	1	1	1	1	1	1	0	0	0	1	1	1	0	0	1	0	0	0	1	0	0	0	1	1	1	1	0	0	0	1	1
	1	0	1	1	0	1	0	0	0	1	0	1	0	0	1	0	0	0	0	1	0	1	0	0	1	1	0	0	1	1	0	1

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	1	0	1	0	1	0	1	1	0	0	0	1	0	1	0	0	1	1	0	0	1	1	1	1	1	0	0	1	1	1	0	0
33	0	0	1	0	1	1	0	1	1	1	1	0	0	1	1	0	1	1	1	1	0	0	1	1	0	0	1	1	0	0	0	0
	1	1	1	1	1	1	1	0	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	1	1	1	0	0	0	1	1
	1	0	1	0	0	0	1	0	1	1	1	0	0	1	0	0	1	1	0	0	1	0	1	0	0	1	0	0	0	0	0	1
	1	0	0	1	1	1	1	1	0	1	1	1	1	1	1	0	0	1	0	0	0	1	1	0	1	0	0	1	0	0	1	1
34	0	0	1	0	1	1	0	1	1	1	1	0	0	1	1	0	1	1	1	1	0	0	1	1	0	0	1	1	0	0	0	0
	1	1	1	1	1	1	1	0	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	1	1	1	0	0	0	1	1
	1	0	1	0	0	0	1	0	1	1	1	0	0	1	0	0	1	1	0	0	1	0	1	0	0	1	0	0	0	0	0	1
	1	0	0	1	1	1	1	1	0	1	1	1	1	1	1	0	0	1	0	0	0	1	1	0	1	0	0	1	0	0	1	1
35	0	1	0	1	0	0	1	1	1	0	1	1	0	1	0	0	0	0	1	0	1	1	1	1	0	0	1	0	1	1	1	1
36	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	1	1	0	0	0	0	1	1	0
37	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
38	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
39	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
40	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
41	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
42	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
43	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
44	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0																

위의 예시에는 다음과 같은 이벤트 정보가 표시되어 있습니다.

숫자	설명
1	이 줄의 첫 2바이트는 표준 헤더 값 1을 나타냅니다. 두 번째 2바이트는 메시지가 데이터 메시지(메시지 유형 4)임을 나타냅니다.
2	이 줄은 다음에 오는 메시지의 길이가 294바이트임을 나타냅니다.
3	이 줄의 첫 번째 비트는 헤더가 아카이브 타임스탬프를 포함하는 확장 헤더임을 나타내는 플래그입니다. 그다음 15비트는 이벤트가 탐지된 도메인의 네트워크 맵 ID를 포함하는 선택적 필드입니다. 해당 줄의 나머지 비트는 레코드 유형 값 400(침입 이벤트 레코드)을 나타냅니다.
4	이 줄은 다음에 오는 이벤트 레코드의 길이가 278바이트임을 나타냅니다.
5	이 줄은 이벤트가 저장된 타임스탬프입니다. 여기서 이벤트는 2014년 7월 2일 수요일 오후 4시 11분 27초에 저장되었습니다.
6	이 줄은 나중에 사용하기 위해 예약되었으며 0으로 채워져 있습니다.
7	이 줄은 블록 유형이 45(5.4 이상 버전용 침입 이벤트 레코드의 블록 유형)임을 나타냅니다.
8	이 줄은 데이터 블록의 길이가 278바이트임을 나타냅니다.
9	이 줄은 이벤트가 센서 번호 5에서 수집되었음을 나타냅니다.
10	이 줄은 이벤트 ID 번호가 65580임을 나타냅니다.
11	이 줄은 이벤트가 1404317489초에 발생했음을 나타냅니다.
12	이 줄은 이벤트가 46542마이크로초에 발생했음을 나타냅니다.
13	이 줄은 규칙 ID 번호가 4임을 나타냅니다.
14	이 줄은 이벤트가 생성기 ID 번호 119(규칙 엔진)에서 탐지되었음을 나타냅니다.
15	이 줄은 규칙 수정 번호가 1임을 나타냅니다.
16	이 줄은 분류 ID 번호가 1임을 나타냅니다.
17	이 줄은 우선순위 ID 번호가 3임을 나타냅니다.
18	이 줄은 소스 IP 주소가 10.5.61.220임을 나타냅니다. 이 필드에는 IPv4 또는 IPv6 주소가 포함될 수 있습니다.
19	이 줄은 대상 IP 주소가 10.5.56.133임을 나타냅니다. 이 필드에는 IPv4 또는 IPv6 주소가 포함될 수 있습니다.
20	이 줄의 첫 2바이트는 소스 포트 번호가 33018임을 나타내고 다음 2바이트는 대상 포트 번호가 8080임을 나타냅니다.
21	이 줄의 첫 번째 바이트는 이벤트에 사용된 프로토콜이 TCP(6)임을 나타냅니다. 두 번째 바이트는 영향 플래그인데, 두 번째 비트가 1이므로 해당 이벤트는 빨간색(취약함)입니다. 그리고 소스 또는 대상 호스트가 시스템이 모니터링하는 네트워크에 있고, 네트워크 맵에 있으며, 이벤트에 나와 있는 포트에서 서버를 실행하고 있는 것입니다. 또한 두 번째 플래그와 세 번째 플래그가 1이므로 이 이벤트는 잠재적으로 취약한 주황색 이벤트입니다. 이 줄의 세 번째 바이트는 영향인데, 여기서 영향은 이벤트가 주황색(잠재적으로 취약함)임을 나타내는 2입니다. 마지막 바이트는 이벤트가 차단되지 않았음을 나타냅니다.
22	이 줄에는 MPLS 레이블(있는 경우)이 포함됩니다.
23	이 줄의 첫 2바이트는 VLAN ID가 0임을 나타냅니다. 그리고 마지막 2바이트는 예약 바이트이며 0으로 설정됩니다.

숫자	설명
24	이 줄은 침입 정책의 고유 ID 번호를 포함합니다.
25	이 줄은 사용자의 내부 ID 번호를 포함합니다. 여기서는 해당하는 사용자가 없으므로 해당 줄의 값은 모두 0입니다.
26	이 줄은 웹 애플리케이션의 내부 ID 번호(847)를 포함합니다.
27	이 줄은 클라이언트 애플리케이션의 내부 ID 번호(2000000676)를 포함합니다.
28	이 줄은 애플리케이션 프로토콜의 내부 ID 번호(676)를 포함합니다.
29	이 줄은 액세스 제어 규칙의 고유 식별자(1)를 포함합니다.
30	이 줄은 액세스 제어 정책의 고유 식별자를 포함합니다.
31	이 줄은 인그레스 인터페이스의 고유 식별자를 포함합니다.
32	이 줄은 이그레스(egress) 인터페이스의 고유 식별자를 포함합니다. 이 이벤트는 차단되었기 때문입니다.
33	이 줄은 인그레스 보안 영역의 고유 식별자를 포함합니다.
34	이 줄은 이그레스(egress) 보안 영역의 고유 식별자를 포함합니다.
35	이 줄은 침입 이벤트와 관련된 연결 이벤트의 Unix 타임스탬프를 포함합니다.
36	이 줄의 첫 2바이트는 연결 이벤트를 생성한 매니지드 디바이스에 있는 Snort 인스턴스의 숫자 ID를 나타냅니다. 나머지 2바이트는 1초 이내에 발생하는 연결 이벤트를 구별하는 데 사용되는 값을 나타냅니다.
37	이 줄의 첫 2바이트는 소스 호스트의 국가 코드를 나타냅니다. 그리고 나머지 2바이트는 대상 호스트의 국가 코드를 나타냅니다.
38	이 줄의 첫 2바이트는 이 이벤트와 관련된 보안 침해의 ID 번호를 포함합니다. 그리고 나머지 2바이트는 트래픽이 통과한 보안 상황(가상 방화벽)의 ID 번호 시작 부분을 포함합니다.
39	이 줄은 트래픽이 통과한 보안 상황(가상 방화벽)의 ID 번호 나머지 부분을 포함합니다.
40	이 줄의 첫 2바이트는 트래픽이 통과한 보안 상황(가상 방화벽)의 마지막 2바이트를 포함합니다. 그리고 두 번째 2바이트는 SSL 서버 인증서(SSL을 사용한 경우)의 SHA1 해시 시작 부분을 포함합니다.
41	이 줄은 SSL 서버 인증서(SSL을 사용한 경우)의 SHA1 해시 나머지 부분을 포함합니다.
42	이 줄의 첫 2바이트는 SSL 서버 인증서의 SHA1 해시에서 마지막 2바이트를 포함합니다. 두 번째 2바이트는 실제로 수행한 SSL 작업을 포함합니다. 이 연결에서는 SSL이 사용되지 않았으므로 해당 값은 0입니다.
43	이 줄의 첫 2바이트는 SSL 플로우 상태를 포함합니다. 이 연결에서는 SSL이 사용되지 않았으므로 해당 값은 0입니다. 두 번째 2바이트는 이 이벤트와 관련된 네트워크 분석 정책 UUID의 첫 2바이트를 포함합니다.
44	이 줄은 이 이벤트와 관련된 네트워크 분석 정책 UUID의 나머지 부분을 포함합니다.

침입 영향 알림 예시

다음 다이어그램에는 예시 침입 영향 알림 레코드가 나와 있습니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	1	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	1	0	0	1	0	0	0	1	0	1	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
9	0	1	0	0	0	0	0	1	1	0	0	1	1	0	1	1	0	1	1	0	1	1	1	1	0	0	1	0	1	0	0	
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
11	1	0	1	0	1	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	1	1	0
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0
15	0	1	0	1	0	1	1	0	0	1	1	1	0	1	0	1	0	1	1	0	1	1	0	0	0	1	1	0	1	1	1	0
	0	1	1	0	0	1	0	1	0	1	1	1	0	0	1	0	0	1	1	0	0	0	0	1	0	1	1	0	0	0	1	0
	0	1	1	0	1	1	0	0	0	1	1	0	0	1	0	1																

위의 예시에는 다음과 같은 정보가 표시되어 있습니다.

숫자	설명
1	이 줄의 첫 2바이트는 표준 헤더 값 1을 나타냅니다. 두 번째 2바이트는 메시지가 데이터 메시지(메시지 유형 4)임을 나타냅니다.
2	이 줄은 다음에 오는 메시지의 길이가 58바이트임을 나타냅니다.
3	이 줄의 첫 번째 비트는 헤더가 아카이브 타임스탬프를 포함하는 확장 헤더가 아님을 나타내는 플래그입니다. 그다음 15비트는 이벤트가 탐지된 도메인의 네트워크 맵 ID를 포함하는 선택적 필드입니다. 해당 줄의 나머지 비트는 레코드 유형 값 9(침입 영향 알림 레코드)를 나타냅니다.
4	이 줄은 다음에 오는 데이터의 길이가 50바이트임을 나타냅니다.
5	이 줄의 값은 침입 영향 알림 데이터 블록이 뒤에 옴을 나타내는 20입니다.
6	이 줄은 영향 알림 블록 헤더를 포함한 영향 알림 블록의 길이가 50바이트임을 나타냅니다.
7	이 줄은 이벤트 ID 번호가 201256임을 나타냅니다.
8	이 줄은 이벤트가 디바이스 번호 2에서 수집되었음을 나타냅니다.
9	이 줄은 이벤트가 1087223700초에 발생했음을 나타냅니다.
10	이 줄은 이벤트와 관련된 영향 레벨이 1(빨간색, 취약함)임을 나타냅니다.
11	이 줄은 위반 이벤트와 관련된 IP 주소가 172.16.1.22임을 나타냅니다.
12	이 줄은 위반과 관련된 대상 IP 주소가 없음을 나타냅니다(값이 0으로 설정됨).
13	이 줄은 문자열 블록 길이와 텍스트 문자열(여기서는 영향 이름이 포함된 문자열)을 포함하는 문자열 블록이 뒤에 옴을 나타냅니다. 문자열 블록에 대한 자세한 정보는 문자열 데이터 블록, 페이지 3-61의 내용을 참조하십시오.
14	이 줄은 문자열 블록 표시기와 길이를 포함한 문자열 블록의 총 길이가 18바이트임을 나타냅니다. 여기에는 영향 설명의 10바이트와 문자열 헤더의 8바이트가 포함됩니다.
15	이 줄은 영향 설명이 "Vulnerable(취약함)"임을 나타냅니다.

패킷 레코드 예시

다음 다이어그램에는 예시 패킷 레코드가 나와 있습니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	1	1	1	0	1
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	1	0	1	0	1
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	1	1	1	0	1	1	0	1	1	0	0	1	1	0
7	0	0	1	1	1	1	1	1	0	0	0	0	0	1	0	0	0	1	1	1	1	1	1	1	0	1	1	1	0	0	1	0
8	0	0	1	1	1	1	1	1	0	0	0	0	0	1	0	0	0	1	1	1	1	1	1	1	0	1	1	1	0	1	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	0	0	0	0	1	1	0	0	1	1	1	0	1
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	1	1	1	0	0	1
12	0	0	1	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	0	0	0	0	0	0	1	1	0	0	0	0		
	0	0	1	1	0	0	0	0	1	1	0	0	0	0	0	0	1	1	1	0	1	0	0	0	1	0	0	0	0	0		

위의 예시에는 다음과 같은 패킷 정보가 표시되어 있습니다.

숫자	설명
1	이 줄의 첫 2바이트는 표준 헤더 값 1을 나타냅니다. 두 번째 2바이트는 메시지가 데이터 메시지(메시지 유형 4)임을 나타냅니다.
2	이 줄은 다음에 오는 메시지의 길이가 989바이트임을 나타냅니다.
3	이 줄의 첫 번째 비트는 헤더가 아카이브 타임스탬프를 포함하는 확장 헤더가 아님을 나타내는 플래그입니다. 그다음 15비트는 이벤트가 탐지된 도메인의 네트워크 맵 ID를 포함하는 선택적 필드입니다. 해당 줄의 나머지 비트는 레코드 유형 값 2(패킷 레코드)를 나타냅니다.
4	이 줄은 다음에 오는 패킷 레코드의 길이가 981바이트임을 나타냅니다.
5	이 줄은 이벤트가 디바이스 번호 3에서 수집되었음을 나타냅니다.
6	이 줄은 이벤트 ID 번호가 195430임을 나타냅니다.
7	이 줄은 이벤트가 10572378초에 발생했음을 나타냅니다.
8	이 줄은 패킷이 10572380초에 수집되었음을 나타냅니다.
9	이 줄은 패킷이 254365마이크로초에 수집되었음을 나타냅니다.
10	이 줄은 링크 유형이 1(이더넷 계층)임을 나타냅니다.
11	이 줄은 다음에 오는 패킷 데이터의 길이가 953바이트임을 나타냅니다.
12	이 줄과 다음 줄에는 실제 페이로드 데이터가 표시됩니다. 실제 데이터는 953바이트이지만 이 예시에서는 잘렸습니다.

분류 레코드 예시

다음 다이어그램에는 예시 분류 레코드가 나와 있습니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	1	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	1
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	1	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	1	1	1	0	1	0	0	0	1	1	1	0	0	1	0
	0	1	1	0	1	1	1	1	0	1	1	0	1	0	1	0	0	1	1	0	0	0	0	1	0	1	1	0	1	1	1	0
	0	0	1	0	1	1	0	1	0	1	1	0	0	0	0	1	0	1	1	0	0	0	1	1	0	1	1	1	0	1	0	0
	0	1	1	0	1	0	0	1	0	1	1	1	0	1	1	0	0	1	1	0	1	0	0	1	0	1	1	1	0	1	0	0
7	0	1	1	1	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	1	0	1	0	0	0	0	0	1
	0	0	1	0	0	0	0	0	0	1	0	0	1	1	1	0	0	1	1	0	0	1	0	1	0	1	1	1	0	1	0	0
	0	1	1	1	0	1	1	1	0	1	1	0	1	1	1	1	0	1	1	1	0	0	1	0	0	1	1	0	1	0	1	1
	0	0	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	1	1	1	0	0	1	0	0	1	1	0	1	1	1	1
	0	1	1	0	1	0	1	0	0	1	1	0	0	0	0	1	0	1	1	0	1	1	1	0	0	0	1	0	0	0	0	0
	0	1	1	1	0	1	1	1	0	1	1	0	0	0	0	1	0	1	1	1	0	0	1	1	0	0	1	0	0	0	0	0
	0	1	0	0	0	1	0	0	0	1	1	0	0	1	0	1	0	1	1	1	0	1	0	0	0	1	1	0	0	1	0	1
	0	1	1	0	0	0	1	1	0	1	1	1	0	1	0	0	0	1	1	0	0	1	0	1	0	1	1	0	0	1	0	0
8	1	0	0	1	1	1	0	1	1	1	0	0	0	1	1	0	0	0	0	0	0	1	0	1	1	1	1	0	1	0	0	0
	1	1	0	0	1	0	1	1	1	0	1	0	0	0	1	0	0	0	0	1	0	0	0	1	1	1	0	1	1	0	0	1
	1	0	0	0	1	0	0	1	1	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0
	0	1	0	1	0	1	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	1
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

위의 예시에는 다음과 같은 이벤트 정보가 표시되어 있습니다.

숫자	설명
1	이 줄의 첫 2바이트는 표준 헤더 값 1을 나타냅니다. 두 번째 2바이트는 메시지가 데이터 메시지(메시지 유형 4)임을 나타냅니다.
2	이 줄은 다음에 오는 메시지의 길이가 92바이트임을 나타냅니다.
3	이 줄의 첫 번째 비트는 헤더가 아카이브 타임스탬프를 포함하는 확장 헤더가 아님을 나타내는 플래그입니다. 그다음 15비트는 이벤트가 탐지된 도메인의 네트워크 맵 ID를 포함하는 선택적 필드입니다. 해당 줄의 나머지 비트는 레코드 유형 값 67(분류 레코드)을 나타냅니다.
4	이 줄은 다음에 오는 분류 레코드의 길이가 84바이트임을 나타냅니다.
5	이 줄은 분류 ID가 35임을 나타냅니다.
6	이 줄의 첫 2바이트는 뒤에 오는 분류 이름의 길이가 15바이트임을 나타냅니다. 두 번째 2바이트에서는 분류 이름 자체(여기서는 "trojan-activity")가 시작됩니다.
7	이 줄의 첫 2바이트에는 줄 6에 설명된 분류 이름이 계속 표시됩니다. 이 줄의 다음 2바이트는 뒤에 오는 분류 설명의 길이가 29바이트임을 나타냅니다. 나머지 바이트에서는 분류 설명(여기서는 `"A Network Trojan was Detected."`)이 시작됩니다.
8	이 줄은 분류의 고유 식별자 역할을 하는 분류 ID 번호를 나타냅니다.
9	이 줄은 분류 수정의 고유 식별자 역할을 하는 분류 수정 ID 번호를 나타냅니다. 여기서는 분류 수정이 없으므로 해당 값이 null입니다.

우선순위 레코드 예시

다음 예시에는 샘플 우선순위 레코드가 표시되어 있습니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	1	0	1	0	0	0	0	1	1	0	1	0	0	1
	0	1	1	0	0	1	1	1	0	1	1	0	1	0	0	0																

위의 예시에는 다음과 같은 이벤트 정보가 표시되어 있습니다.

숫자	설명
1	이 줄의 첫 2바이트는 표준 헤더 값 1을 나타냅니다. 두 번째 2바이트는 메시지가 데이터 메시지(메시지 유형 4)임을 나타냅니다.
2	이 줄은 다음에 오는 메시지가 16바이트임을 나타냅니다.
3	이 줄은 레코드 유형 값 4(우선순위 레코드)를 나타냅니다.
4	이 줄은 다음에 오는 우선순위 레코드의 길이가 8바이트임을 나타냅니다.
5	이 줄은 우선순위 ID가 1임을 나타냅니다.
6	이 줄의 첫 2바이트는 우선순위 이름에 4바이트가 포함되어 있음을 나타냅니다. 두 번째 2바이트와 다음 줄의 2바이트에는 우선순위 이름 자체인 "high(높음)"가 표시됩니다.

규칙 메시지 레코드 예시

다음 예시에는 샘플 규칙 레코드가 표시되어 있습니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	0	1
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	1	0	1	1	0	1	0	0	1	0	1
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	1	0	1	1	0	1	0	0	1	0	1
9	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	1	1	0	1	1	0	1	1	0	0	0	1	1	0	1	1	1
	0	0	1	0	0	1	1	1	0	0	1	1	1	0	0	1	0	0	1	0	0	1	1	0	0	0	0	1	1	1	1	1
	0	0	0	1	0	0	0	1	1	1	1	0	0	0	1	1	1	0	1	1	0	0	0	0	0	0	0	0	0	1	0	0	1
	1	0	0	0	0	1	0	0	1	0	0	0	1	1	1	1	0	1	1	0	1	0	0	1	1	1	1	0	0	0	1	1
10	0	1	1	0	1	1	0	1	1	1	0	1	0	0	1	0	1	0	1	1	0	1	1	0	0	0	1	1	0	1	1	1
	0	0	1	0	1	0	1	0	1	0	1	0	0	1	0	1	0	0	1	0	0	1	1	0	0	0	0	1	1	1	1	1
	0	0	0	1	0	0	0	1	1	1	1	0	0	0	1	1	1	0	1	1	0	0	0	0	0	0	0	0	0	1	0	0	1

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	1	0	0	0	0	1	0	0	1	0	0	0	1	1	1	1	0	1	1	0	1	0	0	1	1	1	1	0	0	0	1	1
11	0	1	1	0	1	1	0	1	1	1	0	1	0	0	1	0	0	1	0	0	0	0	0	1	0	1	0	1	0	0	0	0
	0	1	0	1	0	0	0	0	0	0	1	0	1	1	0	1	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	1
	0	1	0	1	0	1	0	0	0	1	0	0	0	1	0	1	0	1	0	0	0	0	1	1	0	1	0	1	0	1	0	0
	0	0	1	0	0	0	0	0	0	1	0	0	0	1	0	0	0	1	0	0	1	1	1	0	0	1	0	1	0	0	1	1
	0	0	1	0	0	0	0	0	0	1	1	1	0	0	1	0	0	1	1	0	0	1	0	1	0	1	1	1	0	0	0	1
	0	1	1	1	0	1	0	1	0	1	1	0	0	1	0	1	0	1	1	1	0	0	1	1	0	1	1	1	0	1	0	0
	0	0	1	0	0	0	0	0	0	1	1	0	0	1	1	0	0	1	1	0	1	1	1	1	0	1	1	1	0	0	1	0
	0	0	1	0	0	0	0	0	0	1	1	1	0	0	0	0	0	1	1	0	1	1	1	1	0	1	1	1	0	1	0	0
	0	1	1	0	0	1	0	1	0	1	1	0	1	1	1	0	0	1	1	1	0	1	0	0	0	1	1	0	1	0	0	1
	0	1	1	0	0	0	0	0	1	0	1	1	0	1	1	0	0	0	0	1	0	0	0	0	0	1	1	0	1	1	0	1
	0	1	1	0	0	0	0	1	0	1	1	0	1	1	0	0	0	1	1	1	0	1	1	1	0	1	1	0	0	0	0	1
	0	1	1	1	0	0	1	0	0	1	1	0	0	1	0	1	0	0	1	0	0	0	0	0	0	1	0	1	0	0	1	1
	0	1	1	0	0	0	0	1	0	1	1	0	0	1	1	0	0	1	1	0	0	1	0	1	0	1	0	0	0	1	1	1
	0	1	1	1	0	1	0	1	0	1	1	0	0	0	0	1	0	1	1	1	0	0	1	0	0	1	1	0	0	1	0	0
	0	0	1	0	0	0	0	0	0	1	1	1	0	1	0	0	0	1	1	0	0	1	1	1	0	0	1	0	0	0	0	0
	0	1	1	0	0	1	0	0	0	1	1	0	1	1	1	1	0	1	1	0	1	1	0	1	0	1	1	0	0	0	0	1
	0	1	1	0	1	0	0	1	0	1	1	0	1	1	1	0	0	0	1	0	0	0	0	0	0	0	1	1	0	0	1	1
	0	0	1	1	0	1	1	0	0	0	1	1	0	0	0	0	0	0	1	0	1	1	1	0	0	1	1	0	0	0	1	1
	0	1	1	0	1	1	1	0																								

위의 예시에는 다음과 같은 이벤트 정보가 표시되어 있습니다.

숫자	설명
1	이 줄의 첫 2바이트는 표준 헤더 값 1을 나타냅니다. 두 번째 2바이트는 메시지가 데이터 메시지(메시지 유형 4)임을 나타냅니다.
2	이 줄은 다음에 오는 메시지가 129바이트임을 나타냅니다.
3	이 줄의 첫 번째 비트는 헤더가 아카이브 타임스탬프를 포함하는 확장 헤더가 아님을 나타내는 플래그입니다. 그다음 15비트는 이벤트가 탐지된 도메인의 네트워크 맵 ID를 포함하는 선택적 필드입니다. 해당 줄의 나머지 비트는 레코드 유형 값 66(규칙 메시지 레코드)을 나타냅니다.
4	이 줄은 다음에 오는 규칙 메시지 레코드의 길이가 121바이트임을 나타냅니다.
5	이 줄은 생성기 ID 번호가 1(규칙 엔진)임을 나타냅니다.
6	이 줄은 규칙 ID 번호가 28069임을 나타냅니다.
7	이 줄은 규칙 수정 번호가 1임을 나타냅니다.
8	이 줄은 Firepower System에 렌더링된 규칙 ID 번호가 28069임을 나타냅니다.
9	이 줄의 첫 2바이트는 규칙 텍스트 이름에 71바이트가 포함되어 있음을 나타냅니다. 두 번째 2바이트에서는 규칙의 고유 식별자 번호가 시작됩니다.
10	이 줄의 첫 2바이트에서는 규칙의 고유 식별자 번호가 끝납니다. 그다음 2바이트에서는 규칙 수정의 고유 식별자 번호가 시작됩니다.
11	이 줄의 첫 2바이트에서는 규칙 수정의 고유 식별자 번호가 끝납니다. 두 번째 2바이트에서는 규칙 메시지 자체의 텍스트가 시작됩니다. 전송된 규칙 메시지의 전체 텍스트는 `APP-DETECT DNS request for potential malware SafeGuard to domain 360.cn` 입니다.

6.1.x 버전용 연결 통계 데이터 블록 예시

다음 다이어그램에 예시 연결 통계 레코드가 나와 있습니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	0	0	1	1	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	1	1
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	1	1	1	1	0	0
5	0	1	0	1	0	1	1	1	1	1	1	1	1	0	1	1	1	0	0	0	1	1	1	0	0	0	1	1	0	1	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	0	1	0	1	1
14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
15	1	1	0	1	0	0	0	1	1	0	0	0	0	1	0	0	1	1	1	1	1	0	1	1	0	1	0	1	0	1	1	1
16	0	0	0	0	1	0	0	0	1	0	1	1	1	0	1	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	1	1
19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	1	0	0
20	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
21	0	1	0	1	1	0	0	1	1	1	1	0	0	1	0	0	0	1	0	1	0	0	0	0	0	1	0	1	1	1	0	0
	0	1	0	0	0	1	0	0	1	0	0	1	0	0	1	1	0	0	0	1	0	0	0	1	1	1	1	0	0	1	1	0
	1	0	1	0	0	1	1	0	0	0	1	0	1	1	0	1	1	1	1	1	0	0	0	1	1	1	0	1	1	1	0	1
	1	1	1	1	0	1	1	1	0	0	1	1	0	0	0	1	1	0	1	0	1	0	0	0	0	1	0	1	1	1	1	0
22	0	1	1	0	0	0	0	0	1	1	0	1	0	1	0	1	0	0	0	0	1	1	0	0	1	0	0	0	0	0	0	0
	0	1	0	0	0	1	0	0	1	0	0	1	0	0	1	1	0	0	0	1	0	0	0	1	1	1	1	0	0	1	1	0
	1	0	0	1	1	0	0	0	0	1	0	0	0	0	1	1	1	0	0	0	0	1	0	0	1	1	0	1	1	0	0	0
	1	1	0	1	0	1	1	0	1	0	1	0	0	0	1	1	1	1	1	0	0	0	0	0	0	0	0	0	1	0	0	0

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
23	0	1	0	1	1	0	0	1	1	0	0	1	0	0	0	1	0	0	1	0	0	1	1	0	1	1	0	1	1	1	1	0
	0	1	0	0	0	1	0	0	1	0	0	1	0	0	1	1	0	0	0	1	0	0	0	1	1	1	1	0	0	1	1	0
	1	0	1	0	0	1	1	0	0	0	1	0	1	1	0	1	1	1	1	1	0	0	0	1	1	1	0	1	1	1	1	1
	1	1	1	1	0	1	1	1	0	0	1	1	0	0	0	1	1	0	1	0	1	0	0	0	0	1	0	1	1	1	1	0
24	0	1	1	0	0	0	0	0	1	0	0	0	1	1	0	1	0	1	1	0	1	1	0	0	1	1	1	1	0	1	0	0
	0	1	0	0	0	1	0	0	1	0	0	1	0	0	1	1	0	0	0	1	0	0	0	1	1	1	1	0	0	1	1	0
	1	0	0	1	1	0	0	0	0	1	0	0	0	0	1	1	1	0	0	0	0	1	0	0	1	1	0	1	1	0	0	0
	1	1	0	1	0	1	1	0	1	0	1	0	0	0	1	1	1	1	1	0	0	0	0	0	0	0	0	0	1	0	0	0
25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	1	0	1	0	1	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	1	0	1
26	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	0	1	0	0	1	0	0	0	0	0	1	1	0	0	0	0	1	0	0	1	0	1	0	1	1	1	1	1	0	1	0	0
27	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
28	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	1	0	1	0	1	1	1	1	1	1	0	1	0	0	1	1	1	0	0	0	0	1	1	1	0	0	1	1	1	0	1
29	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	1	0	0	1	1
30	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
31	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
32	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	1	0	1	0	1	1	0	0	0	0	1	0	1	0
33	0	0	0	0	0	0	0	1	1	0	1	1	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
34	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
35	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	0	1	1	1	0	0
36	0	1	1	1	0	0	1	1	0	1	0	1	0	1	1	1	1	1	1	1	1	0	1	1	1	0	0	0	1	1	1	0
37	0	0	1	1	0	0	1	1	0	1	0	1	0	1	1	1	1	1	1	1	1	0	1	1	1	0	0	0	1	1	1	0
38	0	0	1	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
39	0	0	0	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
40	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0
41	1	1	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
42	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
43	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
44	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
45	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
46	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
47	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
48	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
49	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
50	0	1	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
51	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
52	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1
53	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
54	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
55	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
56	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
57	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
58	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
59	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
60	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
61	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
62	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
63	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
65	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
66	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
67	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
68	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
69	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0
70	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
71	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
72	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
73	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
74	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
75	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
76	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
77	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
78	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
79	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
80	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
81	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
82	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
83	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
84	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
85	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
86	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
87	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
88	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
89	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
90	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
91	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
92	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
93	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
94	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
95	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
96	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	1	0	0	1	1	1	0	0	1	1	1	1	0	0	0	1	1	0	0	1	0	1	1	0	1	1	1	0	0	0	0
	0	1	1	1	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0	1	0	0	0	1	1	1	1	0	0	1	1	0
	1	0	1	0	1	0	0	1	1	0	0	1	1	0	1	1	1	1	0	0	1	1	0	1	1	0	1	1	0	0	0	1
97	1	0	0	1	1	1	0	0	1	0	1	1	0	1	0	1	0	1	0	1	0	0	1	1	1	1	1	1	1	1	0	1
98	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
99	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
101	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
102	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
103	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
104	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
105	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
106	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
107	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0								

위의 예시에는 다음과 같은 이벤트 정보가 표시되어 있습니다.

숫자	설명
1	이 줄의 첫 2바이트는 표준 헤더 값 1을 나타냅니다. 두 번째 2바이트는 메시지가 데이터 메시지(메시지 유형 4)임을 나타냅니다.
2	이 줄은 다음에 오는 메시지의 길이가 716바이트임을 나타냅니다.
3	이 줄의 첫 번째 비트는 헤더가 아카이브 타임스탬프를 포함하는 확장 헤더임을 나타내는 플래그입니다. 그다음 15비트는 이벤트가 탐지된 도메인의 네트워크 맵 ID를 포함하는 선택적 필드입니다. 해당 줄의 나머지 비트는 레코드 유형 값 71(연결 통계 레코드)을 나타냅니다.
4	이 줄은 다음에 오는 이벤트 레코드의 길이가 700바이트임을 나타냅니다.
5	이 줄은 이벤트가 저장된 타임스탬프입니다. 여기서 이벤트는 2016년 10월 10일 월요일 오전 8시 48분 52초에 저장되었습니다.
6	이 줄은 나중에 사용하기 위해 예약되었으며 0으로 채워져 있습니다.
7	이 줄에서는 검색 이벤트를 생성한 디바이스의 ID 번호를 제공합니다. 디바이스 ID는 1입니다.
8	이 줄은 레거시(IPv4) IP 주소용이며, 채워지지 않으므로 0만 포함합니다. IPv4 주소는 IPv6 필드에 저장됩니다.
9	이 줄은 이벤트와 관련된 호스트의 MAC 주소를 포함합니다. MAC 주소는 00:00:00:00:00:00입니다.
10	이 줄의 첫 16비트는 MAC 주소의 나머지 부분을 포함합니다. 그다음 8비트는 호스트에 IPv6 주소가 있는지를 나타내는 플래그입니다. 마지막 8비트는 비어 있으며 나중에 사용하기 위해 예약되어 있습니다.
11	이 줄은 이벤트가 발생한 시간의 Unix 타임스탬프를 포함합니다.
12	이 줄은 이벤트 마이크로초를 포함합니다. 여기서 해당 값은 0입니다.
13	이 줄은 이벤트 유형을 포함합니다. 여기서 유형은 1003입니다.
14	이 줄은 이벤트 하위 유형을 포함합니다. 여기서 이벤트 하위 유형은 1이고 이벤트 유형은 1003이므로 해당 이벤트는 연결 통계 이벤트입니다.
15	이 줄은 파일 번호용으로 사용되며 내부 전용입니다.
16	이 줄은 파일 위치용으로 사용되며 내부 전용입니다.
17	이 줄은 IPv6 주소를 포함합니다. Has IPv6(IPv6 있음) 플래그가 설정되어 있으면 이 필드가 있으며 사용됩니다. 여기서 이 줄에는 IPv6 주소 0:3eb:0:1:d184:fb57:8ba:c00이 포함되어 있습니다.
18	이 줄은 블록 유형을 포함합니다. 여기서 해당 값은 연결 통계 데이터 블록 유형을 나타내는 163입니다.
19	이 줄은 데이터 블록 길이를 포함합니다. 여기서 해당 값은 데이터 644바이트가 포함되어 있음을 나타냅니다.
20	이 줄에서는 검색 이벤트를 생성한 디바이스의 ID 번호를 제공합니다. 디바이스 ID는 1입니다.
21	이 줄에는 인그레스 보안 영역이 포함됩니다. 여기서 해당 영역은 59e4505c-4493-11e6-a62d-f1dff731a85입니다.
22	이 줄에는 이그레스(egress) 보안 영역이 포함됩니다. 여기서 해당 영역은 60d50c80-4493-11e6-9843-84d8d6a3e008입니다.

숫자	설명
23	이 줄에는 인그레스 인터페이스가 포함됩니다. 여기서 해당 인터페이스는 599126de-4493-11e6-a62d-f1dff731a85e입니다.
24	이 줄에는 이그레스(egress) 인터페이스가 포함됩니다. 여기서 해당 인터페이스는 608d6cf4-4493-11e6-9843-84d8d6a3e008입니다.
25	이 줄은 연결 이벤트에 설명된 세션을 시작한 호스트의 IP 주소를 포함합니다. 이 IP 주소는 172.16.3.5입니다.
26	이 줄은 이벤트를 시작한 호스트에 응답한 호스트의 IP 주소를 포함합니다. 이 IP 주소는 72.48.149.244입니다.
27	요청이 생성된 프록시를 사용하는 호스트의 IP 주소입니다. 이 예시에서 해당 주소는 비어 있습니다.
28	이 줄은 트리거된 상관관계 이벤트와 연결되어 있는 규칙의 수정 번호를 포함합니다. 여기서 수정 번호는 00000000-0000-0000-0000-000057e9c39d입니다.
29	이 줄은 이벤트를 트리거한 규칙의 내부 식별자를 포함합니다. 이 규칙은 268439603입니다.
30	이 줄은 이벤트를 트리거한 터널 규칙의 내부 식별자를 포함합니다. 이 이벤트는 터널 규칙에 의해 트리거되지 않았으므로 해당 값은 0입니다.
31	이 줄의 첫 2바이트는 규칙으로 지정된 작업을 포함합니다. 여기서 해당 값은 Block(차단) 작업을 나타내는 4입니다. 마지막 2바이트는 규칙 이유를 포함합니다. 여기서 이유는 Intrusion Block(침입 차단)을 의미하는 64입니다.
32	첫 2바이트는 규칙 이유의 나머지 부분을 포함합니다. 두 번째 2바이트는 이니시에이터 호스트에서 사용하는 포트(43786)를 포함합니다.
33	이 줄의 첫 2바이트는 응답자 포트(443)를 포함합니다. 나머지 2바이트는 TCP 플래그를 포함합니다.
34	이 줄의 첫 번째 바이트는 프로토콜(6)을 포함합니다. 이 값은 이벤트가 TCP에서 발생했음을 나타냅니다. 나머지 24비트는 Netflow 소스의 IP 주소 첫 부분(00000000-0000-0000-0000-000000000000)을 포함합니다.
35	이 줄의 첫 번째 바이트는 Netflow 소스의 마지막 8비트를 포함합니다. 다음 2바이트는 이벤트를 생성한 Snort 인스턴스의 식별자(7)를 포함합니다. 나머지 바이트는 연결 카운터를 포함합니다.
36	이 줄의 첫 바이트는 연결 카운터의 나머지 부분을 포함합니다. 마지막 24비트는 세션에서 교환된 첫 번째 패킷의 Unix 타임스탬프 시작 부분을 포함합니다. 이 타임스탬프는 2016년 10월 10일 월요일 오전 8시 48분 51초를 나타내는 1476103731입니다.
37	첫 번째 바이트는 첫 번째 패킷 타임스탬프의 나머지 부분을 포함합니다. 나머지 3바이트는 세션에서 교환할 마지막 패킷의 타임스탬프를 포함합니다. 이 타임스탬프 역시 2016년 10월 10일 월요일 오전 8시 48분 51초이므로, 세션의 지속시간은 1초 미만입니다.
38	이 줄의 첫 번째 바이트는 마지막 패킷 타임스탬프의 마지막 8비트를 포함합니다. 나머지 24비트는 이벤트를 시작한 호스트가 전송한 패킷 수(여기서는 13개)를 포함합니다.
39	이 줄의 첫 번째 바이트는 이니시에이터에서 전송한 패킷 수의 나머지 부분입니다. 다음 24비트는 응답자가 전송한 패킷 수(여기서는 0)를 포함합니다.
40	이 줄의 첫 번째 바이트는 응답자에서 전송한 패킷 수의 나머지 부분입니다. 다음 24비트는 이니시에이터가 전송한 바이트 수(여기서는 1743)를 포함합니다.

숫자	설명
41	첫 번째 바이트는 이니시에이터 전송 바이트의 마지막 부분이며, 나머지 24비트에서는 응답자 전송 바이트(여기서는 0)가 시작됩니다.
42	첫 번째 바이트는 응답자 전송 바이트의 마지막 부분이며, 나머지 24비트에서는 삭제된 이니시에이터 패킷(여기서는 0)이 시작됩니다.
43	첫 번째 바이트는 삭제된 이니시에이터 패킷의 마지막 부분이며, 나머지 24비트에서는 삭제된 응답자 패킷(여기서는 0)이 시작됩니다.
44	첫 번째 바이트는 삭제된 응답자 패킷의 마지막 부분이며, 나머지 24비트에서는 삭제된 이니시에이터 바이트(여기서는 0)가 시작됩니다.
45	첫 번째 바이트는 삭제된 이니시에이터 바이트의 마지막 부분이며, 나머지 24비트에서는 삭제된 응답자 바이트(여기서는 0)가 시작됩니다.
46	첫 번째 바이트는 삭제된 응답자 바이트의 마지막 부분이며, 나머지 24비트에서는 속도 제한이 적용되는 인터페이스의 이름(여기서는 00000000-0000-0000-0000-000000000000)이 시작됩니다.
47	이 줄의 첫 번째 바이트는 QOS 적용 인터페이스의 나머지 부분입니다. 나머지 부분은 연결에 적용된 QOS 규칙입니다. 이 인터페이스에는 QOS 규칙이 적용되지 않았으므로 ID는 0입니다.
48	이 줄의 첫 번째 바이트는 QOS 규칙 ID의 나머지 부분입니다. 그리고 나머지 부분은 트래픽을 생성한 호스트에 마지막으로 로그인한 사용자의 ID 번호인 16466입니다.
49	이 줄의 첫 번째 바이트는 사용자 ID의 나머지 부분입니다. 그리고 나머지 부분은 연결에 사용된 애플리케이션 프로토콜의 ID입니다. 여기서 해당 ID는 HTTPS 연결을 나타내는 1122입니다.
50	이 줄의 첫 번째 바이트는 애플리케이션 프로토콜 ID의 나머지 부분입니다. 그리고 나머지 부분은 URL 카테고리입니다.
51	이 줄의 첫 번째 바이트는 URL 카테고리의 나머지 부분입니다. 그리고 나머지 부분은 URL 평판입니다. 여기서 평판은 "Risk Unknown(위험 알 수 없음)"을 의미하는 0입니다.
52	이 줄의 첫 번째 바이트는 URL 평판의 나머지 부분입니다. 그리고 나머지 부분은 클라이언트 애플리케이션 ID입니다. 여기서 ID는 "SSL Client(SSL 클라이언트)"를 의미하는 1296입니다.
53	이 줄의 첫 번째 바이트는 클라이언트 애플리케이션 ID의 나머지 부분입니다. 그리고 나머지 부분은 웹 애플리케이션 ID입니다. 여기서 ID는 "Unknown(알 수 없음)"을 의미하는 0입니다.
54	이 줄의 첫 번째 바이트는 웹 애플리케이션 ID의 나머지 부분입니다. 이 줄의 나머지 부분에서는 블록 유형 0이 시작됩니다(문자열 블록 유형이 시작됨을 나타냄).
55	이 줄의 첫 번째 바이트는 문자열 블록 유형의 나머지 부분입니다. 그리고 나머지 부분은 블록 길이입니다. 이 길이는 클라이언트 애플리케이션 URL에 헤더와 길이를 포함하여 8바이트가 들어 있음을 나타내는데, 이는 클라이언트 애플리케이션 URL에 데이터가 없다는 의미입니다.
56	이 줄의 첫 번째 바이트는 문자열 블록 길이의 나머지 부분입니다. 여기서는 클라이언트 애플리케이션 URL에 데이터가 없으므로 이 줄의 나머지 부분은 블록 유형 0으로 시작됩니다(NetBIOS 이름에 대한 문자열 블록 유형이 시작됨을 나타냄).
57	이 줄의 첫 번째 바이트는 문자열 블록 유형의 나머지 부분입니다. 그리고 나머지 부분은 블록 길이입니다. 이 길이는 NetBIOS 이름에 헤더와 길이를 포함하여 8바이트가 들어 있음을 나타내는데, 이는 NetBIOS 이름에 데이터가 없다는 의미입니다.

숫자	설명
58	이 줄의 첫 번째 바이트는 문자열 블록 길이의 나머지 부분입니다. 여기서는 NetBIOS에 데이터가 없으므로 이 줄의 나머지 부분은 블록 유형 0으로 시작됩니다(클라이언트 애플리케이션 버전에 대한 문자열 블록 유형이 시작됨을 나타냄).
59	이 줄의 첫 번째 바이트는 문자열 블록 유형의 나머지 부분입니다. 그리고 나머지 부분은 블록 길이입니다. 이 길이는 클라이언트 애플리케이션 버전에 헤더와 길이를 포함하여 8바이트가 들어 있음을 나타내는데, 이는 클라이언트 애플리케이션 버전에 데이터가 없다는 의미입니다.
60	이 줄에는 클라이언트 애플리케이션 버전 블록 길이의 나머지 바이트를 포함합니다. 마지막 3바이트는 연결 이벤트와 관련된 첫 번째 모니터 규칙의 ID인 268439553입니다.
61	이 줄은 첫 번째 모니터 규칙 ID의 마지막 바이트를 포함합니다. 나머지 3바이트는 두 번째 모니터 규칙의 ID(0)입니다.
62	이 줄은 두 번째 모니터 규칙 ID의 마지막 바이트를 포함합니다. 나머지 3바이트는 세 번째 모니터 규칙의 ID(0)입니다.
63	이 줄은 세 번째 모니터 규칙 ID의 마지막 바이트를 포함합니다. 나머지 3바이트는 네 번째 모니터 규칙의 ID(0)입니다.
64	이 줄은 네 번째 모니터 규칙 ID의 마지막 바이트를 포함합니다. 나머지 3바이트는 다섯 번째 모니터 규칙의 ID(0)입니다.
65	이 줄은 여섯 번째 모니터 규칙 ID의 마지막 바이트를 포함합니다. 나머지 3바이트는 일곱 번째 모니터 규칙의 ID(0)입니다.
66	이 줄은 일곱 번째 모니터 규칙 ID의 마지막 바이트를 포함합니다. 나머지 3바이트는 여덟 번째 모니터 규칙의 ID(0)입니다.
67	이 줄은 여덟 번째 모니터 규칙 ID의 마지막 바이트를 포함합니다. 이 줄의 두 번째 바이트는 소스 또는 대상 IP 주소가 IP 블랙리스트와 일치했는지를 나타냅니다. 이 줄의 세 번째 바이트는 IP 블랙리스트와 일치한 IP 계층입니다. 마지막 바이트에서는 파일 이벤트 개수(0)가 시작됩니다.
68	이 줄의 첫 번째 바이트는 나머지 파일 이벤트 개수입니다. 다음 2바이트는 침입 이벤트 개수를 포함합니다. 마지막 바이트는 이니시에이터 국가를 포함합니다. 여기서 해당 국가는 "unknown(알 수 없음)"을 의미하는 0입니다.
69	이 줄의 첫 번째 바이트는 이니시에이터 국가의 두 번째 바이트입니다. 다음 2바이트는 응답자 국가(840)입니다. 마지막 바이트에서는 원래 클라이언트 국가가 시작됩니다. 여기서 해당 국가는 "unknown(알 수 없음)"을 의미하는 0입니다.
70	이 줄의 첫 번째 바이트는 원래 클라이언트 국가의 끝부분입니다. 다음 2바이트는 IOC 번호(0)입니다. 마지막 바이트는 소스 자동 시스템의 첫 바이트(0)입니다.
71	이 줄의 첫 3바이트는 소스 자동 시스템입니다. 마지막 바이트는 대상 자동 시스템의 첫 바이트(0)입니다.
72	이 줄의 첫 3바이트는 대상 자동 시스템입니다. 마지막 바이트는 입력 인터페이스의 SNMP 색인(0)입니다.
73	이 줄의 첫 번째 바이트는 입력 인터페이스의 SNMP 색인입니다. 다음 2바이트는 출력 인터페이스의 SNMP 색인(0)입니다. 이 줄의 마지막 바이트는 들어오는 인터페이스의 서비스 유형 설정(0)입니다.
74	이 줄의 첫 번째 바이트는 나가는 인터페이스의 서비스 유형 설정(0)입니다. 두 번째 바이트는 소스 마스크(0)입니다. 세 번째 바이트는 대상 마스크(0)입니다. 마지막 바이트는 트래픽이 통과한 보안 상황의 ID 번호 시작 부분입니다. 여기서 보안 상황은 00000000-0000-0000-0000-000000000000입니다.

숫자	설명
75	이 줄의 첫 3바이트는 보안 상황의 나머지 부분입니다. 마지막 바이트는 VLAN ID(0) 입니다.
76	첫 번째 바이트는 VLAN ID입니다. 마지막 3바이트에서는 값이 0인 문자열 블록이 시작됩니다. 이 문자열 블록은 참조된 호스트의 이름을 포함합니다.
77	첫 번째 바이트는 문자열 블록 유형의 나머지 부분입니다. 마지막 3바이트는 블록 유형과 길이를 포함한 문자열 블록의 총 길이입니다. 여기서 해당 길이는 8바이트인데, 이는 참조된 호스트가 없으므로 문자열 블록에 데이터가 없다는 의미입니다.
78	첫 번째 바이트는 문자열 블록 길이의 나머지 부분입니다. 마지막 3바이트에서는 값이 0인 문자열 블록이 시작됩니다. 이 문자열 블록은 사용자 에이전트를 포함합니다.
79	첫 번째 바이트는 문자열 블록 유형의 나머지 부분입니다. 마지막 3바이트는 블록 유형과 길이를 포함한 문자열 블록의 총 길이입니다. 여기서 해당 길이는 8바이트인데, 이는 사용자 에이전트가 없으므로 문자열 블록에 데이터가 없다는 의미입니다.
80	첫 번째 바이트는 문자열 블록 길이의 나머지 부분입니다. 마지막 3바이트에서는 값이 0인 문자열 블록이 시작됩니다. 이 문자열 블록은 HTTP 참조 페이지를 포함합니다.
81	첫 번째 바이트는 문자열 블록 유형의 나머지 부분입니다. 마지막 3바이트는 블록 유형과 길이를 포함한 문자열 블록의 총 길이입니다. 여기서 해당 길이는 8바이트인데, 이는 HTTP 참조 페이지가 없으므로 문자열 블록에 데이터가 없다는 의미입니다.
82	이 줄의 첫 번째 바이트는 문자열 블록 길이의 마지막 부분을 포함합니다. 마지막 3바이트는 SSL 인증서 핑거프린트(00000000000000000000)를 포함합니다.
83	이 줄의 첫 번째 바이트는 SSL 인증서 핑거프린트 ID의 마지막 부분을 포함합니다. 이 줄의 나머지 부분은 SSL 정책 ID(00000000-0000-0000-0000-000000000000)를 포함합니다.
84	이 줄의 첫 번째 바이트는 SSL 정책 ID의 끝부분입니다. 나머지 3바이트는 SSL 규칙 ID(0)입니다.
85	이 줄의 첫 번째 바이트는 SSL 규칙 ID의 나머지 부분입니다. 다음 2바이트는 SSL 암호 그룹입니다. 여기서 해당 값은 TLS_NULL_WITH_NUL_NULL을 의미하는 0입니다. 마지막 바이트는 SSL 버전(0)입니다.
86	이 줄은 SSL 서버 인증서 상태를 포함합니다. 여기서 해당 값은 Not Checked(확인되지 않음)를 의미하는 0입니다.
87	이 줄의 첫 2바이트는 SSL 실제 작업입니다. 여기서 해당 값은 Unknown(알 수 없음)을 의미하는 0입니다. 다음 2바이트는 SSL 예상 작업입니다. 여기서 해당 값은 Unknown(알 수 없음)을 의미하는 0입니다.
88	이 줄의 첫 2바이트는 SSL 플로우 상태입니다. 여기서 해당 값은 Unknown(알 수 없음)을 의미하는 0입니다. 다음 2바이트는 SSL 플로우 오류입니다. 여기서 해당 값은 Unknown(알 수 없음)을 의미하는 0입니다.
89	이 줄의 첫 2바이트는 SSL 플로우 오류의 나머지 부분입니다. 다음 2바이트는 SSL 플로우 메시지(0)입니다.
90	이 줄의 첫 2바이트는 SSL 플로우 메시지입니다. 다음 2바이트는 SSL 플로우 플래그(0)입니다.
91	이 줄의 첫 2바이트는 SSL 플로우 플래그의 나머지 부분입니다. 다음 2바이트에서는 SSL 서버 이름에 대한 문자열 블록(유형 0)이 시작됩니다.
92	이 줄의 첫 2바이트에서는 문자열 블록 유형이 끝나며, 다음 2바이트에는 문자열 블록 길이가 포함됩니다. 여기서는 블록 유형과 길이를 포함한 블록 길이가 8이므로 문자열 블록에 데이터가 포함되어 있지 않은 것입니다.

숫자	설명
93	첫 2바이트는 문자열 블록 길이의 나머지 부분을 포함합니다. 다음 2바이트는 SSL URL 카테고리를 포함합니다. 여기서 해당 값은 Unknown(알 수 없음)을 의미하는 0입니다.
94	이 줄의 첫 2바이트는 SSL URL 카테고리의 나머지 부분을 포함합니다. 다음 2바이트에서는 SSL 세션 ID(00000000000000000000000000000000)가 시작됩니다.
95	이 줄의 첫 번째 바이트는 SSL 세션 ID의 끝부분을 포함합니다. 다음 바이트는 SSL 세션 ID의 길이(0)를 포함합니다. 다음 2바이트에서는 SSL 티켓 ID(00000000000000000000)가 시작됩니다.
96	이 줄의 첫 2바이트는 SSL 티켓 ID의 끝부분을 포함합니다. 세 번째 바이트는 SSL 티켓 ID 길이(0)를 포함합니다. 마지막 바이트에서는 네트워크 분석 정책 수정(4e78cb70-7842-11e6-a99b-cdb19cb553fd)이 시작됩니다.
97	이 줄의 첫 3바이트는 네트워크 분석 정책 수정의 끝부분을 포함합니다. 마지막 바이트에서는 엔드포인트 프로파일 ID(0)가 시작됩니다.
98	이 줄의 첫 3바이트는 엔드포인트 프로파일 ID입니다. 나머지 바이트에서는 보안 그룹 ID(0)가 시작됩니다.
99	이 줄의 첫 3바이트는 보안 그룹 ID입니다. 나머지 바이트에서는 위치 IPv6(인터페이스가 ISE와 통신하는 데 사용하는 IP 주소)이 시작됩니다. 여기서 해당 주소는 비어 있습니다.
100	이 줄의 첫 3바이트는 위치 IPv6의 끝부분입니다. 나머지 바이트에서는 HTTP 응답이 시작됩니다. 여기서 해당 값은 HTTP 응답이 없었음을 의미하는 0입니다.
101	이 줄의 첫 3바이트는 HTTP 응답의 끝부분입니다. 나머지 바이트에서는 DNS 쿼리에 대한 문자열 블록(유형 0)이 시작됩니다.
102	첫 3바이트에서는 문자열 블록 유형이 완료됩니다. 나머지 바이트는 문자열 블록 길이를 포함합니다. 여기서는 블록 유형과 길이를 포함한 길이가 8바이트인데, 이는 DNS 쿼리에 데이터가 없다는 의미입니다.
103	첫 3바이트에서는 문자열 블록 길이가 끝납니다. 이 줄의 나머지 바이트에서는 DNS 레코드 유형(71)이 시작됩니다.
104	이 줄의 첫 번째 바이트에서는 DNS 레코드 유형이 끝납니다. 다음 2바이트는 DNS 응답 유형(0)입니다. 마지막 바이트에서는 DNS TTL이 시작됩니다.
105	이 줄의 첫 3바이트는 DNS TTL입니다. 마지막 바이트에서는 싱크홀 UUID(00000000-0000-0000-0000-000000000000)가 시작됩니다.
106	이 줄의 첫 3바이트에서는 싱크홀 UUID가 끝납니다. 마지막 바이트에서는 보안 인텔리전스 목록(0)이 시작됩니다.
107	이 줄의 첫 3바이트에서는 보안 인텔리전스 목록이 시작됩니다. 마지막 바이트에서는 두 번째 보안 인텔리전스 목록(0)이 시작됩니다.

5.1 이상 버전 사용자 이벤트 예시

다음 다이어그램에 예시 사용자 이벤트 레코드가 나와 있습니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	1	0	0	1
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	1	1	1
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0	1
5	0	1	0	1	0	0	1	1	0	0	1	1	0	0	0	0	0	1	1	1	1	1	0	0	0	0	1	0	1	0	0	1
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
11	0	1	0	1	0	0	1	0	1	1	1	0	1	1	1	1	1	1	1	1	0	0	0	1	0	1	1	1	0	0	1	1
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	0	1	1	0	0	1	0	0	1	1	1	1
13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	0	1	1	0	0
14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
15	0	1	1	1	0	0	1	1	1	1	1	1	0	0	0	1	1	1	1	0	1	1	1	1	0	1	0	1	0	0	1	0
16	0	0	0	1	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	0	0	0	0	1	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	1	1	1	1	0	1	1	1	1	0	0	0
18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1
19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	1
20	0	1	0	1	0	0	1	0	1	1	1	0	1	1	1	1	1	1	1	1	0	0	0	1	0	1	1	1	0	0	1	1

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
24	0	0	1	0	0	0	0	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	0	0	0	0	1	1	0	0	0	1
	0	1	0	0	0	0	0	0	0	0	1	1	0	0	0	1	0	0	1	1	0	0	0	0	0	0	1	0	1	1	1	0
	0	0	1	1	0	1	0	0	0	0	1	0	1	1	1	0	0	0	1	1	0	0	0	1	0	0	1	1	0	0	0	1
	0	0	1	0	1	1	1	0	0	0	1	1	0	0	0	1	0	0	1	1	0	1	1	1	0	0	1	1	0	1	0	1
25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1
26	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	0	1	0	1	0
27	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
28	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
29	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	0	0	0	0	1	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	1	1	1	1	0	1	1	1	1	0	0	0
30	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
31	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0																								

위의 예시에는 다음과 같은 정보가 표시되어 있습니다.

숫자	설명
1	이 줄의 첫 2바이트는 표준 헤더 값 `1`을 나타냅니다. 두 번째 2바이트는 메시지가 데이터 메시지(메시지 유형 4)임을 나타냅니다.
2	이 줄은 다음에 오는 메시지의 길이가 `153`바이트임을 나타냅니다.
3	이 줄의 첫 번째 비트는 헤더가 아카이브 타임스탬프를 포함하는 확장 헤더임을 나타내는 플래그입니다. 그다음 15비트는 이벤트가 탐지된 도메인의 네트워크 맵 ID를 포함하는 선택적 필드입니다. 해당 줄의 나머지 비트는 레코드 유형 값 `95`(사용자 정보 업데이트 메시지 블록)를 나타냅니다.
4	이 줄은 다음에 오는 데이터의 길이가 `137`바이트임을 나타냅니다.

숫자	설명
5	이 줄은 아카이브 타임스탬프를 포함합니다. 비트 23이 설정되었으므로 이 줄이 포함됩니다. 타임스탬프는 1970년 1월 1일 이후의 초 단위 시간으로 저장된 Unix 타임스탬프입니다. 여기서 타임스탬프는 1,391,789,354(2014년 2월 3일 월요일 오후 7시 43분 49초)입니다.
6	이 줄은 0을 포함하며 나중에 사용하기 위해 예약됩니다.
7	이 줄은 탐지 엔진 ID가 3임을 나타냅니다.
8	이 줄은 레거시(IPv4) IP 주소용이며, 채워지지 않으므로 0만 포함합니다. IPv4 주소는 IPv6 필드에 저장됩니다.
9	이 줄은 이벤트와 관련된 MAC 주소를 포함합니다. 여기서는 MAC 주소가 없으므로 해당 줄은 0을 포함합니다.
10	이 줄의 앞쪽 절반은 MAC 주소의 나머지 부분(모두 0)입니다. 그다음 바이트는 IPv6 주소의 유무를 나타냅니다. 이 줄의 마지막 바이트는 나중에 사용하기 위해 예약되며 0을 포함합니다.
11	이 줄은 시스템이 이벤트를 생성한 UNIX 타임스탬프(1970년 1월 1일 이후의 초 단위 시간)를 포함합니다.
12	이 줄은 시스템이 이벤트를 생성한 마이크로초(100만분의 1초) 단위의 증분 시간을 포함합니다.
13	이 줄은 이벤트 유형을 포함합니다. 여기서 해당 값은 사용자 수정 메시지를 나타내는 1004입니다.
14	이 줄은 이벤트 하위 유형을 포함합니다. 여기서 해당 값은 사용자 로그인 이벤트를 나타내는 2입니다.
15	이 줄은 직렬 파일 번호를 포함합니다. 이 필드는 내부용이므로 무시해도 됩니다.
16	이 줄은 직렬 파일에서 이벤트의 위치를 포함합니다. 이 필드는 내부용이므로 무시해도 됩니다.
17	이 줄은 IPv6 주소를 포함합니다. Has IPv6(IPv6 있음) 플래그가 설정되어 있으면 이 필드가 있으며 사용됩니다. 그러나 여기서는 IPv4 주소 10.4.15.120이 포함됩니다.
18	이 줄에서는 사용자 로그인 정보 데이터 블록(블록 유형 127로 표시됨)이 시작됩니다.
19	이 줄은 다음에 오는 블록의 길이가 81바이트임을 나타냅니다.
20	이 줄은 사용자 로그인 타임스탬프가 1,391,456,7임을 나타냅니다. 이는 해당 이벤트가 2014년 10월 3일 월요일 오후 7시 43분 47초(GMT)에 생성되었다는 의미입니다.
21	이 줄은 레거시(IPv4) IP 주소용이며, 채워지지 않으므로 0만 포함합니다. IPv4 주소는 IPv6 필드에 저장됩니다.
22	이 줄은 문자열 블록 길이와 텍스트 문자열(여기서는 사용자 이름이 포함된 문자열)을 포함하는 문자열 블록이 뒤에 옴을 나타냅니다. 문자열 블록에 대한 자세한 정보는 문자열 데이터 블록, 페이지 3-61의 내용을 참조하십시오.
23	이 줄은 문자열 블록의 데이터 길이가 16바이트임을 나타냅니다.
24	이 줄은 사용자의 이름이 "301@10.4.11.175"임을 나타냅니다.
25	이 줄은 사용자의 ID 번호를 나타냅니다.
26	이 줄은 로그인 정보가 파생된 연결에서 사용되는 애플리케이션 프로토콜의 애플리케이션 ID를 나타냅니다.

숫자	설명
27	이 줄은 문자열 블록 길이와 텍스트 문자열(여기서는 이메일 주소가 포함된 문자열)을 포함하는 문자열 블록이 뒤에 옴을 나타냅니다. 문자열 블록에 대한 자세한 정보는 문자열 데이터 블록, 페이지 3-61의 내용을 참조하십시오.
28	이 줄은 문자열 블록의 데이터 길이가 0바이트임을 나타냅니다. 이 사용자와 관련된 이메일 주소가 없기 때문입니다.
29	이 줄은 로그인 중인 사용자가 탐지된 호스트의 IP 주소를 포함합니다.
30	첫 번째 바이트는 로그인 유형을 포함합니다. 이 줄의 나머지 부분은 문자열 블록 길이와 텍스트 문자열(여기서는 로그인을 보고하는 Active Directory 서버의 이름이 포함된 문자열)을 포함하는 문자열 블록이 뒤에 옴을 나타냅니다. 문자열 블록에 대한 자세한 정보는 문자열 데이터 블록, 페이지 3-61의 내용을 참조하십시오.
31	이 줄의 첫 번째 바이트에서는 문자열 데이터 블록이 완료됩니다. 그리고 이 줄의 나머지 부분은 문자열 블록의 데이터 길이가 0바이트임을 나타냅니다. 이 로그인과 관련된 Active Directory 서버가 없기 때문입니다.

검색 데이터 구조 예시

이 섹션에는 eStreamer에서 검색 이벤트에 대해 전송할 수 있는 데이터 구조의 예시가 포함되어 있습니다. 제공되는 예시는 다음과 같습니다.

새 네트워크 프로토콜 메시지 예시

다음 다이어그램에 3.0 이상 버전의 새 네트워크 프로토콜 메시지 샘플이 나와 있습니다.

바이트	0								1								2								3								
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
헤더 버전 1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	이벤트 메시지(4)가 포함된 표준 메시지 헤더 시작
메시지 길이(49B)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	
새 NW 프로토콜 메시지(13)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	
메시지 길이(41B)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	0	1	0	
탐지 엔진 ID(2)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	

바이트	0	1	2	3	
비트	0 1 2 3 4 5 6 7	8 9 10 11 12 13 14 15	16 17 18 19 20 21 22 23	24 25 26 27 28 29 30 31	
IP(192.168.1.10)	1 1 0 0 0 0 0 0	1 0 1 0 1 0 0 0	0 0 0 0 0 0 0 1	0 0 0 0 1 0 1 0	
MAC 주소(없음)	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	
	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	예약된 바이트(0)
Unix 초 (1047242787)	0 0 1 1 1 1 1 0	0 1 1 0 1 0 1 1	1 0 1 0 1 0 0 0	0 0 1 0 0 0 1 1	
Unix 밀리초 (973208)	0 0 0 0 0 0 0 0	0 0 0 0 1 1 1 0	1 1 0 1 1 0 0 1	1 0 0 1 1 0 0 0	
예약된 바이트 (0)	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 1 1	1 1 1 0 1 0 0 0	이벤트 유형 1000 - 신규
이벤트 하위 유형 4 - 새 전송 프로토콜	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 1 0 0	
파일 번호	0 1 0 0 0 0 0 0	0 1 0 0 0 1 1 1	1 0 0 0 1 0 0 1	1 1 0 1 0 0 0 1	
파일 위치	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 1	1 0 0 0 0 0 0 0	표준 메시지 헤더 끝
프로토콜 (6-TCP)	0 0 0 0 0 1 1 0				

새 TCP 서버 메시지 예시

다음 다이어그램에 3.0 버전의 새 TCP 서버 메시지 샘플이 나와 있습니다.

바이트	0	1	2	3	
비트	0 1 2 3 4 5 6 7	8 9 10 11 12 13 14 15	16 17 18 19 20 21 22 23	24 25 26 27 28 29 30 31	
헤더 버전 1	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 1	0 0 0 0 0 0 0 0	0 0 0 0 0 1 0 0	이벤트 메시지(4)가 포함된 표준 메시지 헤더 시작
메시지 길이 (256B)	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 1	0 0 0 0 0 0 0 0	
새 TCP 서비스 메시지(11)	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 1 0 1 1	

바이트	0	1	2	3	
비트	0 1 2 3 4 5 6 7	8 9 10 11 12 13 14 15	16 17 18 19 20 21 22 23	24 25 26 27 28 29 30 31	
메시지 길이 (248B)	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	1 1 1 1 1 0 0 0	
탐지 엔진 ID(2)	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 1 0	
IP(192.168.1.10)	1 1 0 0 0 0 0 0	1 0 1 0 1 0 0 0	0 0 0 0 0 0 0 1	0 0 0 0 1 0 1 0	
MAC 주소(없음)	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	
	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	예약된 바이트(0)
Unix 초 (1047242787)	0 0 1 1 1 1 1 0	0 1 1 0 1 0 1 1	1 0 1 0 1 0 0 0	0 0 1 0 0 0 1 1	
Unix 밀리초 (973208)	0 0 0 0 0 0 0 0	0 0 0 0 1 1 1 0	1 1 0 1 1 0 0 1	1 0 0 1 1 0 0 0	
예약된 바이트 (0)	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 1 1	1 1 1 0 1 0 0 0	이벤트 유형 1000 - 신규
이벤트 하위 유형 2 - 새 호스트	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 1 0	
파일 번호	0 1 0 0 0 0 0 0	0 1 0 0 0 1 1 1	1 0 0 0 1 0 0 1	1 1 0 1 0 0 0 1	
파일 위치	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	1 1 0 0 0 0 0 0	표준 메시지 헤더 끝
서버 블록 헤더 (12)	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 1 1 0 0	서버 데이터 블록 시작
서버 길이 (208B)	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	1 1 0 1 0 0 0 0	
서버 포트(80)	0 0 0 0 0 0 0 0	0 1 0 1 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	적중 수
적중 수(1)	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 1	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	문자열 블록 헤더
문자열 블록 헤더(0)	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	문자열 블록 길이
문자열 블록 길이(13B)	0 0 0 0 0 0 0 0	0 0 0 0 1 1 0 1	0 1 1 0 1 0 0 0	0 1 1 1 0 1 0 0	
서버 이름 (`https`)	0 1 1 1 0 1 0 0	0 1 1 1 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	문자열 블록 헤더

바이트	0								1								2								3								
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
문자열 블록 헤더(0)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	문자열 블록 길이
문자열 블록 길이(15B)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	1	0	0	0	0	0	1	
서버 벤더 (Apache + null 바이트)	0	1	1	1	0	0	0	0	0	1	1	0	0	0	0	1	0	1	1	0	0	0	1	1	0	1	1	0	1	0	0	0	
	0	1	1	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	문자열 블록 헤더
문자열 블록 헤더(0)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	문자열 블록 길이
문자열 길이 (8-제품 없음)	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	문자열 블록 헤더
문자열 블록 헤더(0)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	문자열 블록 길이
문자열 블록 길이(22B)	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	0	0	1	1	0	0	0	1	0	0	1	0	1	1	1	0	
버전 - 1.3.26(Unix)	0	0	1	1	0	0	1	1	0	0	1	0	1	1	1	0	0	0	1	1	0	0	1	0	0	0	1	1	0	1	1	0	
	0	0	1	0	0	0	0	0	0	0	1	0	1	0	0	0	0	1	0	1	0	1	0	1	0	1	1	0	1	1	1	0	
	0	1	1	0	1	0	0	1	0	1	1	1	1	0	0	0	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	
목록 블록 헤더 (11)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	하위 서버 목록 시작
목록 블록 크기 (94B)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	1	1	0	
하위 서버 헤더 (1)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	하위 서버 블록 시작
하위 서버 길이 (46B)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	1	0	
문자열 블록 헤더(0)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
문자열 길이 (16B)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	
하위 서버 이름 - mod_ssl	0	1	1	0	1	1	0	1	0	1	1	0	1	1	1	1	0	1	1	0	0	1	0	0	0	1	0	1	1	1	1	1	
	0	1	1	1	0	0	1	1	0	1	1	1	0	0	1	1	0	1	1	0	1	1	0	0	0	0	0	0	0	0	0	0	

바이트	0								1								2								3								
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
문자열 블록 헤더(0)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
문자열 블록 길이(8B)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	(하위 유형 벤더 없음)
문자열 블록 헤더(0)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
문자열 블록 길이(14B)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	
하위 서버 버전 - 2.8.9 + null 문자	0	0	1	1	0	0	1	0	0	0	1	0	1	1	1	0	0	0	1	1	1	0	0	0	0	0	1	0	1	1	1	0	하위 서버 블록 끝
	0	0	1	1	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	하위 서버 블록 시작
하위 서버 헤더(1)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	하위서버 길이
하위 서버 길이(48B)	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	문자열 블록 헤더
문자열 블록 헤더(0)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	문자열 블록 크기
문자열 블록 크기(16B)	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	0	0	1	1	1	1	0	1	1	1	0	0	0	0	
하위 서버 이름 - OpenSSL	0	1	1	0	0	1	0	1	0	1	1	0	1	1	1	0	0	1	0	1	0	0	1	1	0	1	0	1	0	0	1	1	
	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	문자열 블록 헤더
문자열 블록 헤더(0)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	문자열 데이터 길이
문자열 길이(8-벤더 없음)	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	문자열 블록 헤더
문자열 블록 헤더(0)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	문자열 블록 길이
문자열 블록 길이(16B)	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	1	0	0	0	0	0	1	0	1	1	1	0		

바이트	0								1								2								3								
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
하위 서버 버전 - 0.9.6.d + null 바이트	0	0	1	1	1	0	0	1	0	0	1	0	1	1	1	0	0	0	1	1	0	1	1	0	0	0	1	0	1	1	1	0	하위 서버 블록 끝
	0	1	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	신뢰도 %
신뢰도 %(100)	0	0	0	0	0	0	0	0	0	1	1	0	0	1	0	0	0	0	1	1	1	1	1	0	0	1	1	0	1	0	1	1	마지막 사용
마지막 사용 (1047242787)	1	0	1	0	1	0	0	0	0	0	1	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Blob 데이터 블록
Blob 데이터 블록(10)	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Blob 데이터 길이
Blob 데이터 길이(22B)	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	0	1	0	0	1	0	0	0	0	1	0	1	0	1	0	0	
서버 배너 (HTTP/1.1 414 요청) - 예: 단축형 서버 배너, 대개 256B	0	1	0	1	0	1	0	0	0	1	0	1	0	0	0	0	0	0	1	0	1	1	1	1	0	0	1	1	0	0	0	1	
	0	0	1	0	1	1	1	0	0	0	1	1	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	1	1	0	1	0	0	
	0	0	1	1	0	0	0	1	0	0	1	1	0	1	0	0	0	0	1	0	0	0	0	0	0	0	1	0	1	0	0	1	0	
	0	1	1	0	0	1	0	1	0	1	1	1	0	0	0	1	0	1	1	1	0	1	0	1	0	1	1	0	0	1	0	1	서버 데이터 블록 끝

레거시 데이터 구조 이해

이 부록에는 eStreamer가 이전 버전 Firepower System 제품에서 지원하는 데이터 구조에 대한 정보가 포함되어 있습니다.

클라이언트가 이전 버전 형식의 데이터를 요청하도록 설정된 비트를 포함하는 이벤트 스트림 요청을 사용하는 경우 이 부록의 정보를 참조하여 수신되는 데이터 메시지의 데이터 구조를 식별할 수 있습니다.

5.0 이전 버전에서는 개별 탐지 엔진에 ID가 할당되었습니다. 버전 5.0에서는 디바이스에 ID가 할당되었습니다. 버전에 따라 데이터 구조는 이러한 ID 할당을 반영합니다.

참고 이 부록에서는 Firepower System 4.9 이상 버전의 데이터 구조만 설명합니다. 그 이전 데이터 구조 버전의 구조에 대한 문서가 필요한 경우 Cisco 고객 지원에 문의하십시오.

자세한 내용은 다음 섹션을 참조하십시오.

레거시 침입 데이터 구조

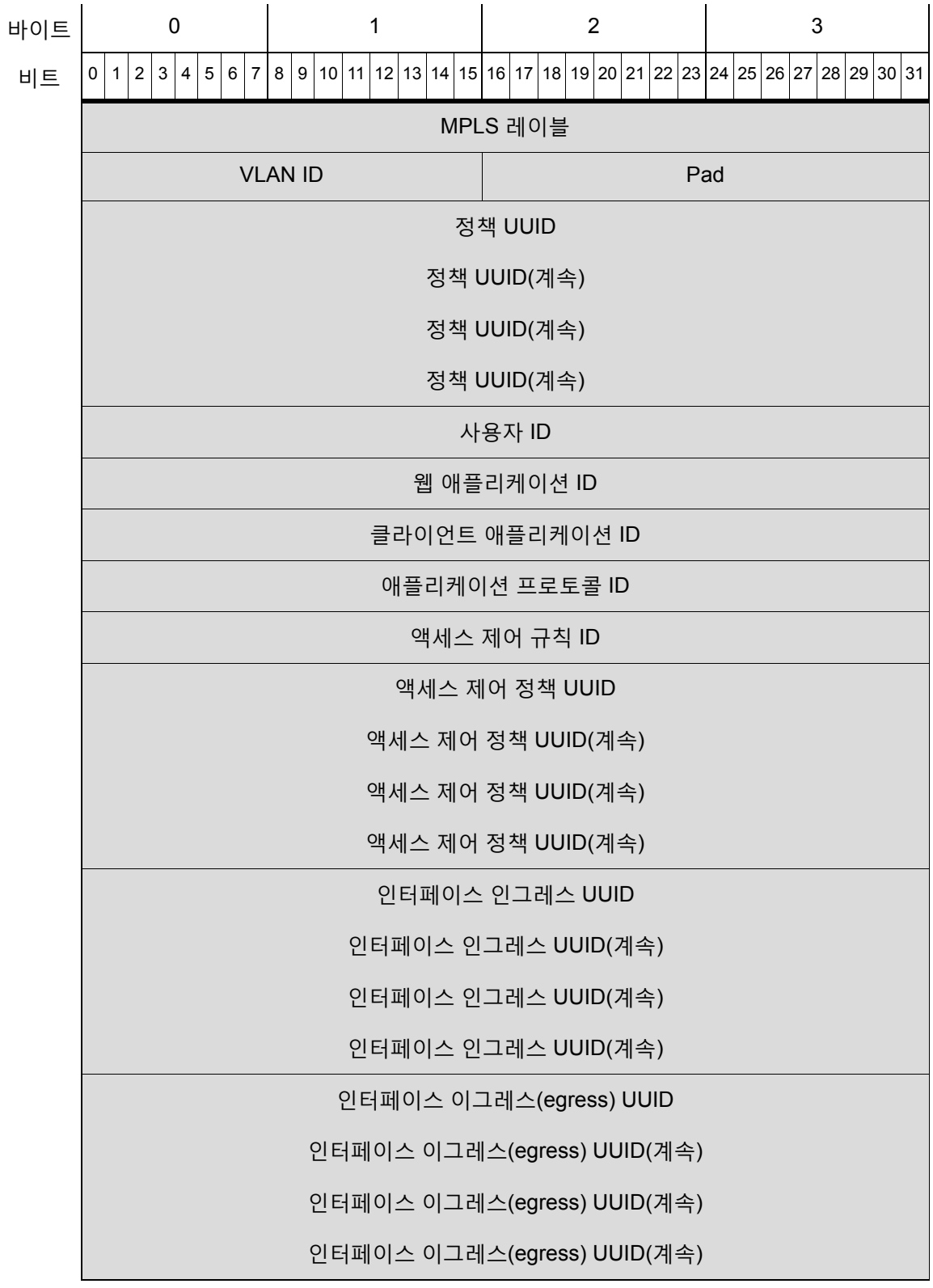
5.0.x~5.1 버전용 침입 이벤트(IPv4) 레코드

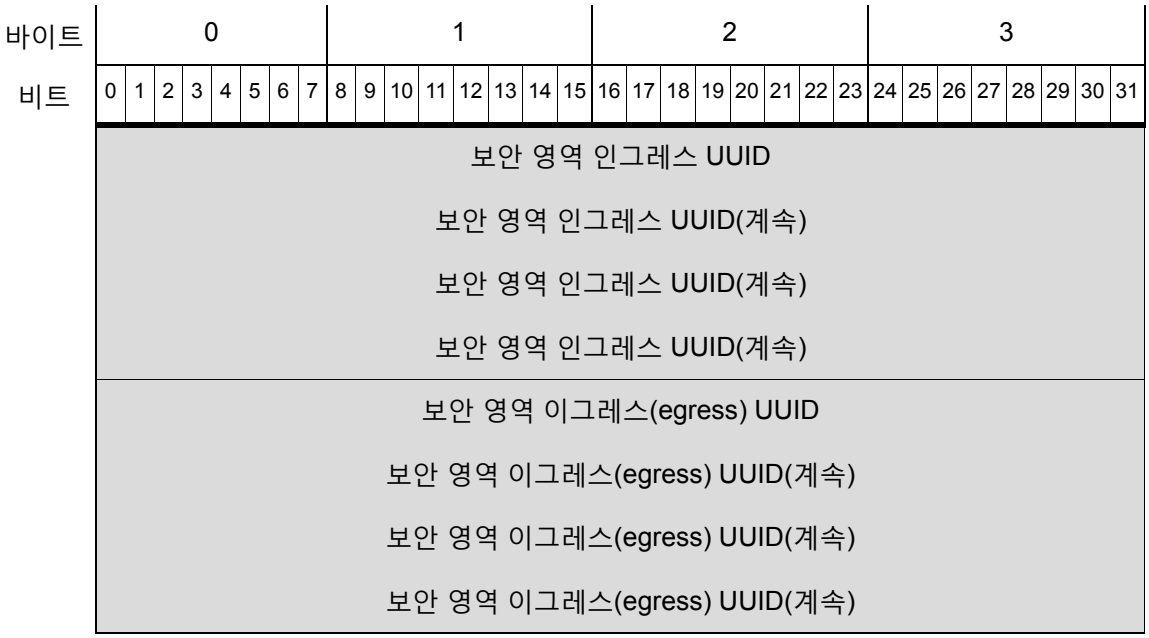
다음 그림에서 침입 이벤트(IPv4) 레코드의 필드는 음영으로 표시되어 있습니다. 레코드 유형은 207입니다.

요청 메시지에서 침입 이벤트 플래그나 확장 요청 플래그를 설정하여 침입 이벤트 레코드를 요청합니다. 요청 플래그, 페이지 2-12 및 확장 요청 제출, 페이지 2-4의 내용을 참조하십시오.

버전 5.0.x~5.1 침입 이벤트의 경우 이벤트 ID, 매니지드 디바이스 ID 및 이벤트 초가 결합되어 고유 식별자가 생성됩니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
헤더 버전(1)																	메시지 유형(4)															
메시지 길이																																
네트워크 맵 ID																	레코드 유형(207)															
레코드 길이																																
eStreamer 서버 타임스탬프(이벤트에서 비트 23이 설정된 경우에 한함)																																
이후 사용을 위해 예약됨(이벤트에서 비트 23이 설정된 경우에 한함)																																
디바이스 ID																																
이벤트 ID																																
이벤트 초																																
이벤트 마이크로초																																
규칙 ID(서명 ID)																																
생성자 ID																																
규칙 수정																																
분류 ID																																
우선순위 ID																																
소스 IPv4 주소																																
대상 IPv4 주소																																
소스 포트																	대상 포트															
IP 프로토콜 ID									영향 플래그								영향								차단됨							


바이트
0
1
2
3
비트
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
MPLS 레이블
VLAN ID
Pad
정책 UUID
정책 UUID(계속)
정책 UUID(계속)
정책 UUID(계속)
사용자 ID
웹 애플리케이션 ID
클라이언트 애플리케이션 ID
애플리케이션 프로토콜 ID
액세스 제어 규칙 ID
액세스 제어 정책 UUID
액세스 제어 정책 UUID(계속)
액세스 제어 정책 UUID(계속)
액세스 제어 정책 UUID(계속)
인터페이스 인그레스 UUID
인터페이스 인그레스 UUID(계속)
인터페이스 인그레스 UUID(계속)
인터페이스 인그레스 UUID(계속)
인터페이스 이그레스(egress) UUID
인터페이스 이그레스(egress) UUID(계속)
인터페이스 이그레스(egress) UUID(계속)
인터페이스 이그레스(egress) UUID(계속)



다음 표에는 각 침입 이벤트 레코드 데이터 필드에 대한 설명이 나와 있습니다.

표 B-1 침입 이벤트(IPv4) 레코드 필드

필드	데이터 유형	설명
디바이스 ID	unit32	탐지 중인 매니지드 디바이스의 ID 번호를 포함합니다. 버전 3 또는 4 메타데이터를 요청하면 매니지드 디바이스 이름을 가져올 수 있습니다. 자세한 정보는 매니지드 디바이스 레코드 메타데이터, 페이지 3-35의 내용을 참조하십시오.
이벤트 ID	uint32	이벤트 ID 번호입니다.
이벤트 초	uint32	이벤트가 탐지된 UNIX 타임스탬프(1970년 1월 1일 이후의 초 단위 시간)입니다.
이벤트 마이크로초	uint32	이벤트 탐지 타임스탬프의 마이크로초(100만분의 1초) 단위 증분 시간입니다.
규칙 ID(서명 ID)	uint32	이벤트와 일치하는 규칙 ID 번호입니다.
생성자 ID	uint32	이벤트를 생성한 Firepower System 전처리기의 ID 번호입니다.
규칙 수정	uint32	규칙 수정 번호입니다.
분류 ID	uint32	이벤트 분류 메시지의 ID 번호입니다.
우선순위 ID	uint32	이벤트와 관련된 우선순위의 ID 번호입니다.
소스 IPv4 주소	uint8[4]	이벤트에 사용된 소스 IPv4 주소(주소 옥텟 형식)입니다.
대상 IPv4 주소	uint8[4]	이벤트에 사용된 대상 IPv4 주소(주소 옥텟 형식)입니다.
소스 포트	uint16	이벤트 프로토콜 유형이 TCP 또는 UDP인 경우 소스 포트 번호입니다.
대상 포트	uint16	이벤트 프로토콜 유형이 TCP 또는 UDP인 경우 대상 포트 번호입니다.

표 B-1 침입 이벤트(IPv4) 레코드 필드 (계속)

필드	데이터 유형	설명
IP 프로토콜 번호	uint8	IANA에서 지정한 프로토콜 번호입니다. 예를 들면 다음과 같습니다. • 0 - IP • 1 - ICMP • 6 - TCP • 17 - UDP
영향 플래그	bits[8]	이벤트의 영향 플래그 값입니다. 하위 8비트가 영향 레벨을 나타냅니다. 값은 다음과 같습니다. • 0x01(비트 0) - 소스 또는 대상 호스트가 시스템에서 모니터링하는 네트워크에 있습니다. • 0x02(비트 1) - 소스 또는 대상 호스트가 네트워크 맵에 있습니다. • 0x04(비트 2) - 소스 또는 대상 호스트가 이벤트의 포트에서 서버를 실행 중이거나(TCP 또는 UDP인 경우) IP 프로토콜을 사용합니다. • 0x08(비트 3) - 이벤트의 소스 또는 대상 호스트 운영 체제에 매핑된 취약점이 있습니다. • 0x10(비트 4) - 이벤트에서 탐지된 서버에 매핑된 취약점이 있습니다. • 0x20(비트 5) - 이벤트로 인해 매니지드 디바이스에서 세션이 삭제되었습니다(디바이스가 인라인, 스위치드 또는 라우티드 구축에서 실행 중인 경우에만 사용됨). Firepower System 웹 인터페이스의 차단 상태에 해당합니다. • 0x40(비트 6) - 이 이벤트를 생성한 규칙에 영향 플래그를 빨간색으로 설정하는 규칙 메타데이터가 있습니다. 소스 또는 대상 호스트가 바이러스, 트로이 목마, 기타 악성 소프트웨어에 감염되었을 가능성이 있습니다. • 0x80(비트 7) - 이벤트에서 탐지된 클라이언트에 매핑된 취약점이 있습니다. 다음 영향 레벨 값은 방어 센터의 특정 우선순위에 매핑됩니다. x는 값이 0 또는 1일 수 있음을 나타냅니다. • (0, 알 수 없음): 00X00000 • 빨간색(1, 취약함): XXXX1XXX, XXX1XXXX, X1XXXXXX, 1XXXXXXX • 주황색(2, 잠재적으로 취약함): 00X00111 • 노란색(3, 현재 취약하지 않음): 00X00011 • 파란색(4, 알 수 없는 대상): 00X00001

표 B-1 침입 이벤트(IPv4) 레코드 필드 (계속)

필드	데이터 유형	설명
영향	uint8	이벤트의 영향 플래그 값입니다. 값은 다음과 같습니다. • 1 - 빨간색(취약함) • 2 - 주황색(잠재적으로 취약함) • 3 - 노란색(현재 취약하지 않음) • 4 - 파란색(알 수 없는 대상) • 5 - 회색(알 수 없는 영향)
차단됨	uint8	이벤트가 차단되었는지를 나타내는 값입니다. • 0 - 차단되지 않음 • 1 - 차단 • 2 - 차단 대상이지만 컨피그레이션에서 허용하지 않음
MPLS 레이블	uint32	MPLS 레이블입니다.
VLAN ID	uint16	패킷이 생성된 VLAN의 ID를 나타냅니다.
Pad	uint16	이후 사용을 위해 예약됩니다.
정책 UUID	uint8[16]	침입 정책의 고유 식별자 역할을 하는 정책 ID 번호입니다.
사용자 ID	uint32	해당하는 경우 사용자의 내부 ID 번호입니다.
웹 애플리케이션 ID	uint32	해당하는 경우 웹 애플리케이션의 내부 ID 번호입니다.
클라이언트 애플리케이션 ID	uint32	해당하는 경우 클라이언트 애플리케이션의 내부 ID 번호입니다.
애플리케이션 프로토콜 ID	uint32	해당하는 경우 애플리케이션 프로토콜의 내부 ID 번호입니다.
액세스 제어 규칙 ID	uint32	액세스 제어 규칙의 고유 식별자 역할을 하는 규칙 ID 번호입니다.
액세스 제어 정책 UUID	uint8[16]	액세스 제어 정책의 고유 식별자 역할을 하는 정책 ID 번호입니다.
인그레스 인터페이스 UUID	uint8[16]	인그레스 인터페이스의 고유 식별자 역할을 하는 인터페이스 ID 번호입니다.
이그레스(egress) 인터페이스 UUID	uint8[16]	이그레스(egress) 인터페이스의 고유 식별자 역할을 하는 인터페이스 ID 번호입니다.
인그레스 보안 영역 UUID	uint8[16]	인그레스 보안 영역의 고유 식별자 역할을 하는 영역 ID 번호입니다.
이그레스(egress) 보안 영역 UUID	uint8[16]	이그레스(egress) 보안 영역의 고유 식별자 역할을 하는 영역 ID 번호입니다.

5.0.x~5.1 버전용 침입 이벤트(IPv6) 레코드

다음 그림에서 침입 이벤트(IPv6) 레코드의 필드는 음영으로 표시되어 있습니다. 레코드 유형은 208입니다.

요청 메시지에서 침입 이벤트 플래그나 확장 요청 플래그를 설정하여 침입 이벤트 레코드를 요청합니다. 요청 플래그, 페이지 2-12 및 확장 요청 제출, 페이지 2-4의 내용을 참조하십시오.

버전 5.0.x~5.1 침입 이벤트의 경우 이벤트 ID, 매니지드 디바이스 ID 및 이벤트 초가 결합되어 고유 식별자가 생성됩니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
헤더 버전(1)																	메시지 유형(4)															
메시지 길이																																
네트워크 맵 ID																	레코드 유형(208)															
레코드 길이																																
eStreamer 서버 타임스탬프(이벤트에서 비트 23이 설정된 경우에 한함)																																
이후 사용을 위해 예약됨(이벤트에서 비트 23이 설정된 경우에 한함)																																
디바이스 ID																																
이벤트 ID																																
이벤트 초																																
이벤트 마이크로초																																
규칙 ID(서명 ID)																																
생성자 ID																																
규칙 수정																																
분류 ID																																
우선순위 ID																																
소스 IPv6 주소																																
소스 IPv6 주소(계속)																																
소스 IPv6 주소(계속)																																
소스 IPv6 주소(계속)																																

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
대상 IPv6 주소																																
대상 IPv6 주소(계속)																																
대상 IPv6 주소(계속)																																
대상 IPv6 주소(계속)																																
소스 포트/ICMP 유형																	대상 포트/ICMP 코드															
IP 프로토콜 ID									영향 플래그								영향								차단됨							
MPLS 레이블																																
VLAN ID																	Pad															
정책 UUID																																
정책 UUID(계속)																																
정책 UUID(계속)																																
정책 UUID(계속)																																
사용자 ID																																
웹 애플리케이션 ID																																
클라이언트 애플리케이션 ID																																
애플리케이션 프로토콜 ID																																
액세스 제어 규칙 ID																																
액세스 제어 정책 UUID																																
액세스 제어 정책 UUID(계속)																																
액세스 제어 정책 UUID(계속)																																
액세스 제어 정책 UUID(계속)																																
인터페이스 인그레스 UUID																																
인터페이스 인그레스 UUID(계속)																																
인터페이스 인그레스 UUID(계속)																																
인터페이스 인그레스 UUID(계속)																																

다음 표에는 각 침입 이벤트 레코드 데이터 필드에 대한 설명이 나와 있습니다.

표 B-2 침입 이벤트(IPv6) 레코드 필드

필드	데이터 유형	설명
디바이스 ID	unit32	탐지 중인 디바이스의 ID 번호를 포함합니다. 버전 3 또는 4 메타데이터를 요청하면 매니지드 디바이스 이름을 가져올 수 있습니다. 자세한 정보는 매니지드 디바이스 레코드 메타데이터, 페이지 3-35의 내용을 참조하십시오.
이벤트 ID	uint32	이벤트 ID 번호입니다.
이벤트 초	uint32	이벤트가 탐지된 UNIX 타임스탬프(1970년 1월 1일 이후의 초 단위 시간)입니다.
이벤트 마이크로초	uint32	이벤트 탐지 타임스탬프의 마이크로초(100만분의 1초) 단위 증분 시간입니다.
규칙 ID(서명 ID)	uint32	이벤트와 일치하는 규칙 ID 번호입니다.
생성자 ID	uint32	이벤트를 생성한 Firepower System 전처리기의 ID 번호입니다.
규칙 수정	uint32	규칙 수정 번호입니다.
분류 ID	uint32	이벤트 분류 메시지의 ID 번호입니다.
우선순위 ID	uint32	이벤트와 관련된 우선순위의 ID 번호입니다.

표 B-2 침입 이벤트(IPv6) 레코드 필드 (계속)

필드	데이터 유형	설명
소스 IPv6 주소	uint8[16]	이벤트에 사용된 소스 IPv6 주소(주소 옥텟 형식)입니다.
대상 IPv6 주소	uint8[16]	이벤트에 사용된 대상 IPv6 주소(주소 옥텟 형식)입니다.
소스 포트/ ICMP 유형	uint16	이벤트 프로토콜 유형이 TCP 또는 UDP인 경우 소스 포트 번호입니다. 프로토콜 유형이 ICMP인 경우 ICMP 유형을 나타냅니다.
대상 포트/ ICMP 코드	uint16	이벤트 프로토콜 유형이 TCP 또는 UDP인 경우 대상 포트 번호입니다. 프로토콜 유형이 ICMP인 경우 ICMP 코드를 나타냅니다.
IP 프로토콜 번호	uint8	IANA에서 지정한 프로토콜 번호입니다. 예를 들면 다음과 같습니다. • 0 - IP • 1 - ICMP • 6 - TCP • 17 - UDP

표 B-2 침입 이벤트(IPv6) 레코드 필드 (계속)

필드	데이터 유형	설명
영향 플래그	bits[8]	이벤트의 영향 플래그 값입니다. 하위 8비트가 영향 레벨을 나타냅니다. 값은 다음과 같습니다. • 0x01(비트 0) - 소스 또는 대상 호스트가 시스템에서 모니터링하는 네트워크에 있습니다. • 0x02(비트 1) - 소스 또는 대상 호스트가 네트워크 맵에 있습니다. • 0x04(비트 2) - 소스 또는 대상 호스트가 이벤트의 포트에서 서버를 실행 중이거나(TCP 또는 UDP인 경우) IP 프로토콜을 사용합니다. • 0X08(비트 3) - 이벤트의 소스 또는 대상 호스트 운영 체제에 매핑된 취약점이 있습니다. • 0x10(비트 4) - 이벤트에서 탐지된 서버에 매핑된 취약점이 있습니다. • 0x20(비트 5) - 이벤트로 인해 매니지드 디바이스에서 세션이 삭제되었습니다(디바이스가 인라인, 스위치드 또는 라우티드 구축에서 실행 중인 경우에만 사용됨). Firepower System 웹 인터페이스의 차단 상태에 해당합니다. • 0x40(비트 6) - 이 이벤트를 생성한 규칙에 영향 플래그를 빨간색으로 설정하는 규칙 메타데이터가 있습니다. 소스 또는 대상 호스트가 바이러스, 트로이 목마, 기타 악성 소프트웨어에 감염되었을 가능성이 있습니다. • 0x80(비트 7) - 이벤트에서 탐지된 클라이언트에 매핑된 취약점이 있습니다. 다음 영향 레벨 값은 방어 센터의 특정 우선순위에 매핑됩니다. x는 값이 0 또는 1일 수 있음을 나타냅니다. • (0, 알 수 없음): 00X00000 • 빨간색(1, 취약함): XXXX1XXX, XXX1XXXX, X1XXXXXX, 1XXXXXXX • 주황색(2, 잠재적으로 취약함): 00X00111 • 노란색(3, 현재 취약하지 않음): 00X00011 • 파란색(4, 알 수 없는 대상): 00X00001
영향	uint8	이벤트의 영향 플래그 값입니다. 값은 다음과 같습니다. • 1 - 빨간색(취약함) • 2 - 주황색(잠재적으로 취약함) • 3 - 노란색(현재 취약하지 않음) • 4 - 파란색(알 수 없는 대상) • 5 - 회색(알 수 없는 영향)

표 B-2 침입 이벤트(IPv6) 레코드 필드 (계속)

필드	데이터 유형	설명
차단됨	uint8	이벤트가 차단되었는지를 나타내는 값입니다. • 0 - 차단되지 않음 • 1 - 차단 • 2 - 차단 대상이지만 컨피그레이션에서 허용하지 않음
MPLS 레이블	uint32	MPLS 레이블입니다. 4.9 이상 버전의 이벤트에만 적용됩니다.
VLAN ID	uint16	패킷이 생성된 VLAN의 ID를 나타냅니다. 4.9 이상 버전의 이벤트에만 적용됩니다.
Pad	uint16	이후 사용을 위해 예약됩니다.
정책 UUID	uint8[16]	침입 정책의 고유 식별자 역할을 하는 정책 ID 번호입니다.
사용자 ID	uint32	해당하는 경우 사용자의 내부 ID 번호입니다.
웹 애플리케이션 ID	uint32	해당하는 경우 웹 애플리케이션의 내부 ID 번호입니다.
클라이언트 애플리케이션 ID	uint32	해당하는 경우 클라이언트 애플리케이션의 내부 ID 번호입니다.
애플리케이션 프로토콜 ID	uint32	해당하는 경우 애플리케이션 프로토콜의 내부 ID 번호입니다.
액세스 제어 규칙 ID	uint32	액세스 제어 규칙의 고유 식별자 역할을 하는 규칙 ID 번호입니다.
액세스 제어 정책 UUID	uint8[16]	액세스 제어 정책의 고유 식별자 역할을 하는 정책 ID 번호입니다.
인그레스 인터페이스 UUID	uint8[16]	인그레스 인터페이스의 고유 식별자 역할을 하는 인터페이스 ID 번호입니다.
이그레스(egress) 인터페이스 UUID	uint8[16]	이그레스(egress) 인터페이스의 고유 식별자 역할을 하는 인터페이스 ID 번호입니다.
인그레스 보안 영역 UUID	uint8[16]	인그레스 보안 영역의 고유 식별자 역할을 하는 영역 ID 번호입니다.
이그레스(egress) 보안 영역 UUID	uint8[16]	이그레스(egress) 보안 영역의 고유 식별자 역할을 하는 영역 ID 번호입니다.

5.2.x 버전용 침입 이벤트 레코드

다음 그림에서 침입 이벤트 레코드의 필드는 음영으로 표시되어 있습니다. 계열 2 데이터 블록 집합에서 레코드 유형은 400이고 블록 유형은 34입니다.

5.2.x 침입 이벤트는 eStreamer에서 확장 요청을 통해서만 요청할 수 있습니다. 이렇게 하려면 스트림 요청 메시지에서 이벤트 유형 코드 12, 버전 코드 5를 요청합니다. 확장 요청 제출에 대한 자세한 정보는 확장 요청 제출, 페이지 2-4의 내용을 참조하십시오.

버전 5.2.x 침입 이벤트의 경우 이벤트 ID, 매니지드 디바이스 ID 및 이벤트 초가 결합되어 고유 식별자가 생성됩니다. 그리고 연결 초, 연결 인스턴스 및 연결 카운터가 결합되어 침입 이벤트와 관련된 연결 이벤트의 고유 식별자가 생성됩니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
헤더 버전(1)																	메시지 유형(4)															
메시지 길이																																
네트워크 맵 ID																	레코드 유형(400)															
레코드 길이																																
eStreamer 서버 타임스탬프(이벤트에서 비트 23이 설정된 경우에 한함)																																
이후 사용을 위해 예약됨(이벤트에서 비트 23이 설정된 경우에 한함)																																
블록 유형(34)																																
블록 길이																																
디바이스 ID																																
이벤트 ID																																
이벤트 초																																
이벤트 마이크로초																																
규칙 ID(서명 ID)																																
생성자 ID																																
규칙 수정																																
분류 ID																																
우선순위 ID																																
소스 IP 주소																																
소스 IP 주소(계속)																																
소스 IP 주소(계속)																																
소스 IP 주소(계속)																																

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
대상 IP 주소																																
대상 IP 주소(계속)																																
대상 IP 주소(계속)																																
대상 IP 주소(계속)																																
소스 포트 또는 ICMP 유형																	대상 포트 또는 ICMP 코드															
IP 프로토콜 ID									영향 플래그								영향								차단됨							
MPLS 레이블																																
VLAN ID																	Pad															
정책 UUID																																
정책 UUID(계속)																																
정책 UUID(계속)																																
정책 UUID(계속)																																
사용자 ID																																
웹 애플리케이션 ID																																
클라이언트 애플리케이션 ID																																
애플리케이션 프로토콜 ID																																
액세스 제어 규칙 ID																																
액세스 제어 정책 UUID																																
액세스 제어 정책 UUID(계속)																																
액세스 제어 정책 UUID(계속)																																
액세스 제어 정책 UUID(계속)																																
인터페이스 인그레스 UUID																																
인터페이스 인그레스 UUID(계속)																																
인터페이스 인그레스 UUID(계속)																																
인터페이스 인그레스 UUID(계속)																																

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
인터페이스 이그레스(egress) UUID																																
인터페이스 이그레스(egress) UUID(계속)																																
인터페이스 이그레스(egress) UUID(계속)																																
인터페이스 이그레스(egress) UUID(계속)																																
보안 영역 인그레스 UUID																																
보안 영역 인그레스 UUID(계속)																																
보안 영역 인그레스 UUID(계속)																																
보안 영역 인그레스 UUID(계속)																																
보안 영역 이그레스(egress) UUID																																
보안 영역 이그레스(egress) UUID(계속)																																
보안 영역 이그레스(egress) UUID(계속)																																
보안 영역 이그레스(egress) UUID(계속)																																
연결 타임스탬프																																
연결 인스턴스 ID																	연결 카운터															
소스 국가																	대상 국가															

다음 표에는 각 침입 이벤트 레코드 데이터 필드에 대한 설명이 나와 있습니다.

표 B-3 5.2.x 버전용 침입 이벤트 레코드 필드

필드	데이터 유형	설명
블록 유형	unint32	침입 이벤트 데이터 블록을 시작합니다. 이 값은 항상 34입니다.
블록 길이	unint32	침입 이벤트 데이터 블록의 총 바이트 수입니다. 여기에는 침입 이벤트 블록 유형 및 길이 필드의 8바이트에 그 뒤의 데이터 바이트 수를 더한 값이 포함됩니다.
디바이스 ID	unit32	탐지 중인 매니지드 디바이스의 ID 번호를 포함합니다. 버전 3 또는 4 메타데이터를 요청하면 매니지드 디바이스 이름을 가져올 수 있습니다. 자세한 정보는 매니지드 디바이스 레코드 메타데이터, 페이지 3-35의 내용을 참조하십시오.
이벤트 ID	uint32	이벤트 ID 번호입니다.

표 B-3 5.2.x 버전용 침입 이벤트 레코드 필드 (계속)

필드	데이터 유형	설명
이벤트 초	uint32	이벤트가 탐지된 UNIX 타임스탬프(1970년 1월 1일 이후의 초 단위 시간)입니다.
이벤트 마이크로초	uint32	이벤트 탐지 타임스탬프의 마이크로초(100만분의 1초) 단위 증분 시간입니다.
규칙 ID(서명 ID)	uint32	이벤트와 일치하는 규칙 ID 번호입니다.
생성자 ID	uint32	이벤트를 생성한 Firepower System 전처리기의 ID 번호입니다.
규칙 수정	uint32	규칙 수정 번호입니다.
분류 ID	uint32	이벤트 분류 메시지의 ID 번호입니다.
우선순위 ID	uint32	이벤트와 관련된 우선순위의 ID 번호입니다.
소스 IP 주소	uint8[16]	이벤트에 사용된 소스 IPv4 또는 IPv6 주소입니다.
대상 IP 주소	uint8[16]	이벤트에 사용된 대상 IPv4 또는 IPv6 주소입니다.
소스 포트 또는 ICMP 유형	uint16	이벤트 프로토콜 유형이 TCP 또는 UDP인 경우 소스 포트 번호이거나, ICMP 트래픽에 의해 이벤트가 발생한 경우 ICMP 유형입니다.
대상 포트 또는 ICMP 코드	uint16	이벤트 프로토콜 유형이 TCP 또는 UDP인 경우 대상 포트 번호이거나, ICMP 트래픽에 의해 이벤트가 발생한 경우 ICMP 코드입니다.
IP 프로토콜 번호	uint8	IANA에서 지정한 프로토콜 번호입니다. 예를 들면 다음과 같습니다. • 0 - IP • 1 - ICMP • 6 - TCP • 17 - UDP

표 B-3 5.2.x 버전용 침입 이벤트 레코드 필드 (계속)

필드	데이터 유형	설명
영향 플래그	bits[8]	이벤트의 영향 플래그 값입니다. 하위 8비트가 영향 레벨을 나타냅니다. 값은 다음과 같습니다. • 0x01(비트 0) - 소스 또는 대상 호스트가 시스템에서 모니터링하는 네트워크에 있습니다. • 0x02(비트 1) - 소스 또는 대상 호스트가 네트워크 맵에 있습니다. • 0x04(비트 2) - 소스 또는 대상 호스트가 이벤트의 포트에서 서버를 실행 중이거나(TCP 또는 UDP인 경우) IP 프로토콜을 사용합니다. • 0X08(비트 3) - 이벤트의 소스 또는 대상 호스트 운영 체제에 매핑된 취약점이 있습니다. • 0x10(비트 4) - 이벤트에서 탐지된 서버에 매핑된 취약점이 있습니다. • 0x20(비트 5) - 이벤트로 인해 매니지드 디바이스에서 세션이 삭제되었습니다(디바이스가 인라인, 스위치드 또는 라우티드 구축에서 실행 중인 경우에만 사용됨). Firepower System 웹 인터페이스의 차단 상태에 해당합니다. • 0x40(비트 6) - 이 이벤트를 생성한 규칙에 영향 플래그를 빨간색으로 설정하는 규칙 메타데이터가 있습니다. 소스 또는 대상 호스트가 바이러스, 트로이 목마, 기타 악성 소프트웨어에 감염되었을 가능성이 있습니다. • 0x80(비트 7) - 이벤트에서 탐지된 클라이언트에 매핑된 취약점이 있습니다. (5.0 이상 버전만 해당) 다음 영향 레벨 값은 방어 센터의 특정 우선순위에 매핑됩니다. x는 값이 0 또는 1일 수 있음을 나타냅니다. • (0, 알 수 없음): 00X00000 • 빨간색(1, 취약함): XXXX1XXX, XXX1XXXX, X1XXXXXX, 1XXXXXXX (5.0 이상 버전만 해당) • 주황색(2, 잠재적으로 취약함): 00X0011X • 노란색(3, 현재 취약하지 않음): 00X0001X • 파란색(4, 알 수 없는 대상): 00X00001
영향	uint8	이벤트의 영향 플래그 값입니다. 값은 다음과 같습니다. • 1 - 빨간색(취약함) • 2 - 주황색(잠재적으로 취약함) • 3 - 노란색(현재 취약하지 않음) • 4 - 파란색(알 수 없는 대상) • 5 - 회색(알 수 없는 영향)

표 B-3 5.2.x 버전용 침입 이벤트 레코드 필드 (계속)

필드	데이터 유형	설명
차단됨	uint8	이벤트가 차단되었는지를 나타내는 값입니다. • 0 - 차단되지 않음 • 1 - 차단 • 2 - 차단 대상이지만 컨피그레이션에서 허용하지 않음
MPLS 레이블	uint32	MPLS 레이블입니다.
VLAN ID	uint16	패킷이 생성된 VLAN의 ID를 나타냅니다.
Pad	uint16	이후 사용을 위해 예약됩니다.
정책 UUID	uint8[16]	침입 정책의 고유 식별자 역할을 하는 정책 ID 번호입니다.
사용자 ID	uint32	해당하는 경우 사용자의 내부 ID 번호입니다.
웹 애플리케이션 ID	uint32	해당하는 경우 웹 애플리케이션의 내부 ID 번호입니다.
클라이언트 애플리케이션 ID	uint32	해당하는 경우 클라이언트 애플리케이션의 내부 ID 번호입니다.
애플리케이션 프로토콜 ID	uint32	해당하는 경우 애플리케이션 프로토콜의 내부 ID 번호입니다.
액세스 제어 규칙 ID	uint32	액세스 제어 규칙의 고유 식별자 역할을 하는 규칙 ID 번호입니다.
액세스 제어 정책 UUID	uint8[16]	액세스 제어 정책의 고유 식별자 역할을 하는 정책 ID 번호입니다.
인그레스 인터페이스 UUID	uint8[16]	인그레스 인터페이스의 고유 식별자 역할을 하는 인터페이스 ID 번호입니다.
이그레스 (egress) 인터페이스 UUID	uint8[16]	이그레스(egress) 인터페이스의 고유 식별자 역할을 하는 인터페이스 ID 번호입니다.
인그레스 보안 영역 UUID	uint8[16]	인그레스 보안 영역의 고유 식별자 역할을 하는 영역 ID 번호입니다.
이그레스 (egress) 보안 영역 UUID	uint8[16]	이그레스(egress) 보안 영역의 고유 식별자 역할을 하는 영역 ID 번호입니다.
연결 타임스탬프	uint32	침입 이벤트와 관련된 연결 이벤트의 UNIX 타임스탬프(1970년 1월 1일 이후의 초 단위 시간)입니다.
연결 인스턴스 ID	uint16	연결 이벤트를 생성한 매니지드 디바이스에 있는 Snort 인스턴스의 숫자 ID입니다.
연결 카운터	uint16	1초 이내에 발생하는 연결 이벤트를 구별하는 데 사용되는 값입니다.
소스 국가	uint16	소스 호스트의 국가 코드입니다.
대상 국가	uint16	대상 호스트의 국가 코드입니다.

5.3 버전용 침입 이벤트 레코드

다음 그림에서 침입 이벤트 레코드의 필드는 음영으로 표시되어 있습니다. 계열 2 데이터 블록 집합에서 레코드 유형은 400이고 블록 유형은 41입니다.

5.3 침입 이벤트는 eStreamer에서 확장 요청을 통해서만 요청할 수 있습니다. 이렇게 하려면 스트림 요청 메시지에서 이벤트 유형 코드 12, 버전 코드 6을 요청합니다. 확장 요청 제출에 대한 자세한 정보는 확장 요청 제출, 페이지 2-4의 내용을 참조하십시오.

버전 5.3 침입 이벤트의 경우 이벤트 ID, 매니지드 디바이스 ID 및 이벤트 초가 결합되어 고유 식별자가 생성됩니다. 그리고 연결 초, 연결 인스턴스 및 연결 카운터가 결합되어 침입 이벤트와 관련된 연결 이벤트의 고유 식별자가 생성됩니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
헤더 버전(1)																	메시지 유형(4)															
메시지 길이																																
네트워크 맵 ID																	레코드 유형(400)															
레코드 길이																																
eStreamer 서버 타임스탬프(이벤트에서 비트 23이 설정된 경우에 한함)																																
이후 사용을 위해 예약됨(이벤트에서 비트 23이 설정된 경우에 한함)																																
블록 유형(41)																																
블록 길이																																
디바이스 ID																																
이벤트 ID																																
이벤트 초																																
이벤트 마이크로초																																
규칙 ID(서명 ID)																																
생성자 ID																																
규칙 수정																																
분류 ID																																
우선순위 ID																																

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
소스 IP 주소																																
소스 IP 주소(계속)																																
소스 IP 주소(계속)																																
소스 IP 주소(계속)																																
대상 IP 주소																																
대상 IP 주소(계속)																																
대상 IP 주소(계속)																																
대상 IP 주소(계속)																																
소스 포트 또는 ICMP 유형																	대상 포트 또는 ICMP 코드															
IP 프로토콜 ID									영향 플래그								영향								차단됨							
MPLS 레이블																																
VLAN ID																	Pad															
정책 UUID																																
정책 UUID(계속)																																
정책 UUID(계속)																																
정책 UUID(계속)																																
사용자 ID																																
웹 애플리케이션 ID																																
클라이언트 애플리케이션 ID																																
애플리케이션 프로토콜 ID																																
액세스 제어 규칙 ID																																
액세스 제어 정책 UUID																																
액세스 제어 정책 UUID(계속)																																
액세스 제어 정책 UUID(계속)																																
액세스 제어 정책 UUID(계속)																																

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
인터페이스 인그레스 UUID																																
인터페이스 인그레스 UUID(계속)																																
인터페이스 인그레스 UUID(계속)																																
인터페이스 인그레스 UUID(계속)																																
인터페이스 이그레스(egress) UUID																																
인터페이스 이그레스(egress) UUID(계속)																																
인터페이스 이그레스(egress) UUID(계속)																																
인터페이스 이그레스(egress) UUID(계속)																																
보안 영역 인그레스 UUID																																
보안 영역 인그레스 UUID(계속)																																
보안 영역 인그레스 UUID(계속)																																
보안 영역 인그레스 UUID(계속)																																
보안 영역 이그레스(egress) UUID																																
보안 영역 이그레스(egress) UUID(계속)																																
보안 영역 이그레스(egress) UUID(계속)																																
보안 영역 이그레스(egress) UUID(계속)																																
연결 타임스탬프																																
연결 인스턴스 ID																	연결 카운터															
소스 국가																	대상 국가															
IOC 번호																																

다음 표에는 각 침입 이벤트 레코드 데이터 필드에 대한 설명이 나와 있습니다.

표 B-4 5.3 버전용 침입 이벤트 레코드 필드

필드	데이터 유형	설명
블록 유형	unint32	침입 이벤트 데이터 블록을 시작합니다. 이 값은 항상 34입니다.
블록 길이	unint32	침입 이벤트 데이터 블록의 총 바이트 수입니다. 여기에는 침입 이벤트 블록 유형 및 길이 필드의 8바이트에 그 뒤의 데이터 바이트 수를 더한 값이 포함됩니다.
디바이스 ID	unit32	탐지 중인 매니지드 디바이스의 ID 번호를 포함합니다. 버전 3 또는 4 메타데이터를 요청하면 매니지드 디바이스 이름을 가져올 수 있습니다. 자세한 정보는 매니지드 디바이스 레코드 메타데이터, 페이지 3-35의 내용을 참조하십시오.
이벤트 ID	uint32	이벤트 ID 번호입니다.
이벤트 초	uint32	이벤트가 탐지된 UNIX 타임스탬프(1970년 1월 1일 이후의 초 단위 시간)입니다.
이벤트 마이크로초	uint32	이벤트 탐지 타임스탬프의 마이크로초(100만분의 1초) 단위 증분 시간입니다.
규칙 ID(서명 ID)	uint32	이벤트와 일치하는 규칙 ID 번호입니다.
생성자 ID	uint32	이벤트를 생성한 Firepower System 전처리기의 ID 번호입니다.
규칙 수정	uint32	규칙 수정 번호입니다.
분류 ID	uint32	이벤트 분류 메시지의 ID 번호입니다.
우선순위 ID	uint32	이벤트와 관련된 우선순위의 ID 번호입니다.
소스 IP 주소	uint8[16]	이벤트에 사용된 소스 IPv4 또는 IPv6 주소입니다.
대상 IP 주소	uint8[16]	이벤트에 사용된 대상 IPv4 또는 IPv6 주소입니다.
소스 포트 또는 ICMP 유형	uint16	이벤트 프로토콜 유형이 TCP 또는 UDP인 경우 소스 포트 번호이거나, ICMP 트래픽에 의해 이벤트가 발생한 경우 ICMP 유형입니다.
대상 포트 또는 ICMP 코드	uint16	이벤트 프로토콜 유형이 TCP 또는 UDP인 경우 대상 포트 번호이거나, ICMP 트래픽에 의해 이벤트가 발생한 경우 ICMP 코드입니다.
IP 프로토콜 번호	uint8	IANA에서 지정한 프로토콜 번호입니다. 예를 들면 다음과 같습니다. • 0 - IP • 1 - ICMP • 6 - TCP • 17 - UDP

표 B-4 5.3 버전용 침입 이벤트 레코드 필드 (계속)

필드	데이터 유형	설명
영향 플래그	bits[8]	이벤트의 영향 플래그 값입니다. 하위 8비트가 영향 레벨을 나타냅니다. 값은 다음과 같습니다. • 0x01(비트 0) - 소스 또는 대상 호스트가 시스템에서 모니터링하는 네트워크에 있습니다. • 0x02(비트 1) - 소스 또는 대상 호스트가 네트워크 맵에 있습니다. • 0x04(비트 2) - 소스 또는 대상 호스트가 이벤트의 포트에서 서버를 실행 중이거나(TCP 또는 UDP인 경우) IP 프로토콜을 사용합니다. • 0X08(비트 3) - 이벤트의 소스 또는 대상 호스트 운영 체제에 매핑된 취약점이 있습니다. • 0x10(비트 4) - 이벤트에서 탐지된 서버에 매핑된 취약점이 있습니다. • 0x20(비트 5) - 이벤트로 인해 매니지드 디바이스에서 세션이 삭제되었습니다(디바이스가 인라인, 스위치드 또는 라우티드 구축에서 실행 중인 경우에만 사용됨). Firepower System 웹 인터페이스의 차단 상태에 해당합니다. • 0x40(비트 6) - 이 이벤트를 생성한 규칙에 영향 플래그를 빨간색으로 설정하는 규칙 메타데이터가 있습니다. 소스 또는 대상 호스트가 바이러스, 트로이 목마, 기타 악성 소프트웨어에 감염되었을 가능성이 있습니다. • 0x80(비트 7) - 이벤트에서 탐지된 클라이언트에 매핑된 취약점이 있습니다. (5.0 이상 버전만 해당) 다음 영향 레벨 값은 방어 센터의 특정 우선순위에 매핑됩니다. x는 값이 0 또는 1일 수 있음을 나타냅니다. • (0, 알 수 없음): 00X00000 • 빨간색(1, 취약함): XXXX1XXX, XXX1XXXX, X1XXXXXX, 1XXXXXXX (5.0 이상 버전만 해당) • 주황색(2, 잠재적으로 취약함): 00X0011X • 노란색(3, 현재 취약하지 않음): 00X0001X • 파란색(4, 알 수 없는 대상): 00X00001
영향	uint8	이벤트의 영향 플래그 값입니다. 값은 다음과 같습니다. • 1 - 빨간색(취약함) • 2 - 주황색(잠재적으로 취약함) • 3 - 노란색(현재 취약하지 않음) • 4 - 파란색(알 수 없는 대상) • 5 - 회색(알 수 없는 영향)

표 B-4 5.3 버전용 침입 이벤트 레코드 필드 (계속)

필드	데이터 유형	설명
차단됨	uint8	이벤트가 차단되었는지를 나타내는 값입니다. • 0 - 차단되지 않음 • 1 - 차단 • 2 - 차단 대상이지만 컨피그레이션에서 허용하지 않음
MPLS 레이블	uint32	MPLS 레이블입니다.
VLAN ID	uint16	패킷이 생성된 VLAN의 ID를 나타냅니다.
Pad	uint16	이후 사용을 위해 예약됩니다.
정책 UUID	uint8[16]	침입 정책의 고유 식별자 역할을 하는 정책 ID 번호입니다.
사용자 ID	uint32	해당하는 경우 사용자의 내부 ID 번호입니다.
웹 애플리케이션 ID	uint32	해당하는 경우 웹 애플리케이션의 내부 ID 번호입니다.
클라이언트 애플리케이션 ID	uint32	해당하는 경우 클라이언트 애플리케이션의 내부 ID 번호입니다.
애플리케이션 프로토콜 ID	uint32	해당하는 경우 애플리케이션 프로토콜의 내부 ID 번호입니다.
액세스 제어 규칙 ID	uint32	액세스 제어 규칙의 고유 식별자 역할을 하는 규칙 ID 번호입니다.
액세스 제어 정책 UUID	uint8[16]	액세스 제어 정책의 고유 식별자 역할을 하는 정책 ID 번호입니다.
인그레스 인터페이스 UUID	uint8[16]	인그레스 인터페이스의 고유 식별자 역할을 하는 인터페이스 ID 번호입니다.
이그레스(egress) 인터페이스 UUID	uint8[16]	이그레스(egress) 인터페이스의 고유 식별자 역할을 하는 인터페이스 ID 번호입니다.
인그레스 보안 영역 UUID	uint8[16]	인그레스 보안 영역의 고유 식별자 역할을 하는 영역 ID 번호입니다.
이그레스(egress) 보안 영역 UUID	uint8[16]	이그레스(egress) 보안 영역의 고유 식별자 역할을 하는 영역 ID 번호입니다.
연결 타임스탬프	uint32	침입 이벤트와 관련된 연결 이벤트의 UNIX 타임스탬프(1970년 1월 1일 이후의 초 단위 시간)입니다.
연결 인스턴스 ID	uint16	연결 이벤트를 생성한 매니지드 디바이스에 있는 Snort 인스턴스의 숫자 ID입니다.
연결 카운터	uint16	1초 이내에 발생하는 연결 이벤트를 구별하는 데 사용되는 값입니다.
소스 국가	uint16	소스 호스트의 국가 코드입니다.
대상 국가	uint16	대상 호스트의 국가 코드입니다.
IOC 번호	uint16	이 이벤트와 관련된 보안 침해의 ID 번호입니다.

5.1.1.x 버전용 침입 이벤트 레코드

다음 그림에서 침입 이벤트 레코드의 필드는 음영으로 표시되어 있습니다. 레코드 유형은 400이고 블록 유형은 25입니다.

5.1.1.x 침입 이벤트는 eStreamer에서 확장 요청을 통해서만 요청할 수 있습니다. 이렇게 하려면 스트림 요청 메시지에서 이벤트 유형 코드 12, 버전 코드 4를 요청합니다. 확장 요청 제출에 대한 자세한 정보는 확장 요청 제출, 페이지 2-4의 내용을 참조하십시오.

버전 5.1.1.x 침입 이벤트의 경우 이벤트 ID, 매니지드 디바이스 ID 및 이벤트 초가 결합되어 고유 식별자가 생성됩니다. 그리고 연결 초, 연결 인스턴스 및 연결 카운터가 결합되어 침입 이벤트와 관련된 연결 이벤트의 고유 식별자가 생성됩니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
헤더 버전(1)																	메시지 유형(4)															
메시지 길이																																
네트워크 맵 ID																	레코드 유형(400)															
레코드 길이																																
eStreamer 서버 타임스탬프(이벤트에서 비트 23이 설정된 경우에 한함)																																
이후 사용을 위해 예약됨(이벤트에서 비트 23이 설정된 경우에 한함)																																
블록 유형(25)																																
블록 길이																																
디바이스 ID																																
이벤트 ID																																
이벤트 초																																
이벤트 마이크로초																																
규칙 ID(서명 ID)																																
생성자 ID																																
규칙 수정																																
분류 ID																																
우선순위 ID																																

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
소스 IP 주소																																
소스 IP 주소(계속)																																
소스 IP 주소(계속)																																
소스 IP 주소(계속)																																
대상 IP 주소																																
대상 IP 주소(계속)																																
대상 IP 주소(계속)																																
대상 IP 주소(계속)																																
소스 포트/ICMP 유형																	대상 포트/ICMP 코드															
IP 프로토콜 ID									영향 플래그								영향								차단됨							
MPLS 레이블																																
VLAN ID																	Pad															
정책 UUID																																
정책 UUID(계속)																																
정책 UUID(계속)																																
정책 UUID(계속)																																
사용자 ID																																
웹 애플리케이션 ID																																
클라이언트 애플리케이션 ID																																
애플리케이션 프로토콜 ID																																
액세스 제어 규칙 ID																																
액세스 제어 정책 UUID																																
액세스 제어 정책 UUID(계속)																																
액세스 제어 정책 UUID(계속)																																
액세스 제어 정책 UUID(계속)																																

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
인터페이스 인그레스 UUID																																
인터페이스 인그레스 UUID(계속)																																
인터페이스 인그레스 UUID(계속)																																
인터페이스 인그레스 UUID(계속)																																
인터페이스 이그레스(egress) UUID																																
인터페이스 이그레스(egress) UUID(계속)																																
인터페이스 이그레스(egress) UUID(계속)																																
인터페이스 이그레스(egress) UUID(계속)																																
보안 영역 인그레스 UUID																																
보안 영역 인그레스 UUID(계속)																																
보안 영역 인그레스 UUID(계속)																																
보안 영역 인그레스 UUID(계속)																																
보안 영역 이그레스(egress) UUID																																
보안 영역 이그레스(egress) UUID(계속)																																
보안 영역 이그레스(egress) UUID(계속)																																
보안 영역 이그레스(egress) UUID(계속)																																
연결 타임스탬프																																
연결 인스턴스 ID																	연결 카운터															

다음 표에는 각 침입 이벤트 레코드 데이터 필드에 대한 설명이 나와 있습니다.

표 B-5 5.1.1 버전용 침입 이벤트 레코드 필드

필드	데이터 유형	설명
블록 유형	unint32	침입 이벤트 데이터 블록을 시작합니다. 이 값은 항상 25입니다.
블록 길이	unint32	침입 이벤트 데이터 블록의 총 바이트 수입니다. 여기에는 침입 이벤트 블록 유형 및 길이 필드의 8바이트에 그 뒤의 데이터 바이트 수를 더한 값이 포함됩니다.
디바이스 ID	unit32	탐지 중인 매니지드 디바이스의 ID 번호를 포함합니다. 버전 3 또는 4 메타데이터를 요청하면 매니지드 디바이스 이름을 가져올 수 있습니다. 자세한 정보는 매니지드 디바이스 레코드 메타데이터, 페이지 3-35의 내용을 참조하십시오.
이벤트 ID	uint32	이벤트 ID 번호입니다.
이벤트 초	uint32	이벤트가 탐지된 UNIX 타임스탬프(1970년 1월 1일 이후의 초 단위 시간)입니다.
이벤트 마이크로초	uint32	이벤트 탐지 타임스탬프의 마이크로초(100만분의 1초) 단위 증분 시간입니다.
규칙 ID(서명 ID)	uint32	이벤트와 일치하는 규칙 ID 번호입니다.
생성자 ID	uint32	이벤트를 생성한 Firepower System 전처리기의 ID 번호입니다.
규칙 수정	uint32	규칙 수정 번호입니다.
분류 ID	uint32	이벤트 분류 메시지의 ID 번호입니다.
우선순위 ID	uint32	이벤트와 관련된 우선순위의 ID 번호입니다.
소스 IP 주소	uint8[16]	이벤트에 사용된 소스 IPv4 또는 IPv6 주소입니다.
대상 IP 주소	uint8[16]	이벤트에 사용된 대상 IPv4 또는 IPv6 주소입니다.
소스 포트/ ICMP 유형	uint16	이벤트 프로토콜 유형이 TCP 또는 UDP인 경우 소스 포트 번호이거나, ICMP 트래픽에 의해 이벤트가 발생한 경우 ICMP 유형입니다.
대상 포트/ ICMP 코드	uint16	이벤트 프로토콜 유형이 TCP 또는 UDP인 경우 대상 포트 번호이거나, ICMP 트래픽에 의해 이벤트가 발생한 경우 ICMP 코드입니다.
IP 프로토콜 번호	uint8	IANA에서 지정한 프로토콜 번호입니다. 예를 들면 다음과 같습니다. • 0 - IP • 1 - ICMP • 6 - TCP • 17 - UDP

표 B-5 5.1.1 버전용 침입 이벤트 레코드 필드 (계속)

필드	데이터 유형	설명
영향 플래그	bits[8]	이벤트의 영향 플래그 값입니다. 하위 8비트가 영향 레벨을 나타냅니다. 값은 다음과 같습니다. • 0x01(비트 0) - 소스 또는 대상 호스트가 시스템에서 모니터링하는 네트워크에 있습니다. • 0x02(비트 1) - 소스 또는 대상 호스트가 네트워크 맵에 있습니다. • 0x04(비트 2) - 소스 또는 대상 호스트가 이벤트의 포트에서 서버를 실행 중이거나(TCP 또는 UDP인 경우) IP 프로토콜을 사용합니다. • 0X08(비트 3) - 이벤트의 소스 또는 대상 호스트 운영 체제에 매핑된 취약점이 있습니다. • 0x10(비트 4) - 이벤트에서 탐지된 서버에 매핑된 취약점이 있습니다. • 0x20(비트 5) - 이벤트로 인해 매니지드 디바이스에서 세션이 삭제되었습니다(디바이스가 인라인, 스위치드 또는 라우티드 구축에서 실행 중인 경우에만 사용됨). Firepower System 웹 인터페이스의 차단 상태에 해당합니다. • 0x40(비트 6) - 이 이벤트를 생성한 규칙에 영향 플래그를 빨간색으로 설정하는 규칙 메타데이터가 있습니다. 소스 또는 대상 호스트가 바이러스, 트로이 목마, 기타 악성 소프트웨어에 감염되었을 가능성이 있습니다. • 0x80(비트 7) - 이벤트에서 탐지된 클라이언트에 매핑된 취약점이 있습니다. 다음 영향 레벨 값은 방어 센터의 특정 우선순위에 매핑됩니다. x는 값이 0 또는 1일 수 있음을 나타냅니다. • (0, 알 수 없음): 00X00000 • 빨간색(1, 취약함): XXXX1XXX, XXX1XXXX, X1XXXXXX, 1XXXXXXX • 주황색(2, 잠재적으로 취약함): 00X00111 • 노란색(3, 현재 취약하지 않음): 00X00011 • 파란색(4, 알 수 없는 대상): 00X00001
영향	uint8	이벤트의 영향 플래그 값입니다. 값은 다음과 같습니다. • 1 - 빨간색(취약함) • 2 - 주황색(잠재적으로 취약함) • 3 - 노란색(현재 취약하지 않음) • 4 - 파란색(알 수 없는 대상) • 5 - 회색(알 수 없는 영향)

표 B-5 5.1.1 버전용 침입 이벤트 레코드 필드 (계속)

필드	데이터 유형	설명
차단됨	uint8	이벤트가 차단되었는지를 나타내는 값입니다. • 0 - 차단되지 않음 • 1 - 차단 • 2 - 차단 대상이지만 컨피그레이션에서 허용하지 않음
MPLS 레이블	uint32	MPLS 레이블입니다.
VLAN ID	uint16	패킷이 생성된 VLAN의 ID를 나타냅니다.
Pad	uint16	이후 사용을 위해 예약됩니다.
정책 UUID	uint8[16]	침입 정책의 고유 식별자 역할을 하는 정책 ID 번호입니다.
사용자 ID	uint32	해당하는 경우 사용자의 내부 ID 번호입니다.
웹 애플리케이션 ID	uint32	해당하는 경우 웹 애플리케이션의 내부 ID 번호입니다.
클라이언트 애플리케이션 ID	uint32	해당하는 경우 클라이언트 애플리케이션의 내부 ID 번호입니다.
애플리케이션 프로토콜 ID	uint32	해당하는 경우 애플리케이션 프로토콜의 내부 ID 번호입니다.
액세스 제어 규칙 ID	uint32	액세스 제어 규칙의 고유 식별자 역할을 하는 규칙 ID 번호입니다.
액세스 제어 정책 UUID	uint8[16]	액세스 제어 정책의 고유 식별자 역할을 하는 정책 ID 번호입니다.
인그레스 인터페이스 UUID	uint8[16]	인그레스 인터페이스의 고유 식별자 역할을 하는 인터페이스 ID 번호입니다.
이그레스(egress) 인터페이스 UUID	uint8[16]	이그레스(egress) 인터페이스의 고유 식별자 역할을 하는 인터페이스 ID 번호입니다.
인그레스 보안 영역 UUID	uint8[16]	인그레스 보안 영역의 고유 식별자 역할을 하는 영역 ID 번호입니다.
이그레스(egress) 보안 영역 UUID	uint8[16]	이그레스(egress) 보안 영역의 고유 식별자 역할을 하는 영역 ID 번호입니다.
연결 타임스탬프	uint32	침입 이벤트와 관련된 연결 이벤트의 UNIX 타임스탬프(1970년 1월 1일 이후의 초 단위 시간)입니다.
연결 인스턴스 ID	uint16	연결 이벤트를 생성한 매니지드 디바이스에 있는 Snort 인스턴스의 숫자 ID입니다.
연결 카운터	uint16	1초 이내에 발생하는 연결 이벤트를 구별하는 데 사용되는 값입니다.

5.3.1 버전용 침입 이벤트 레코드

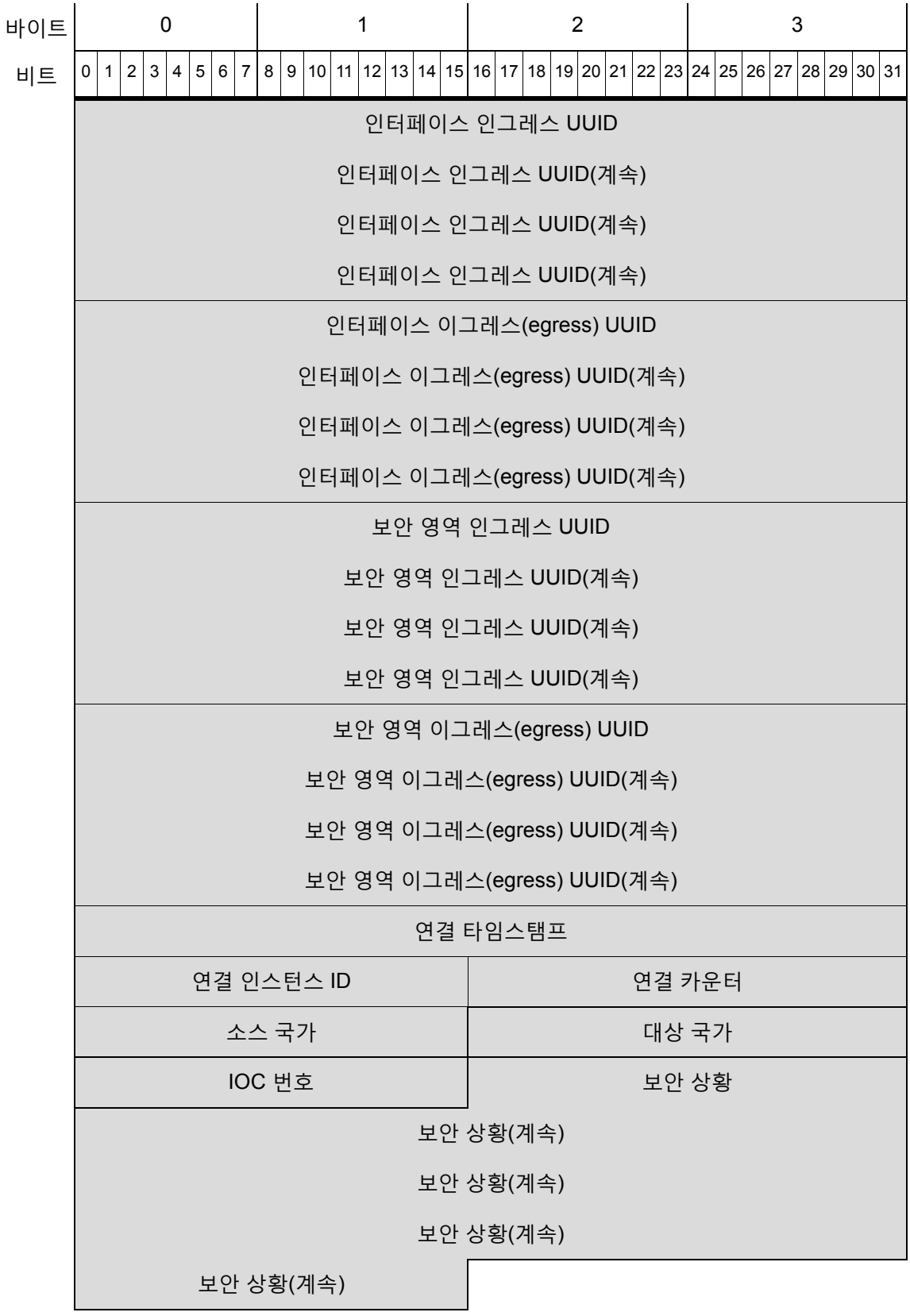
다음 그림에서 침입 이벤트 레코드의 필드는 음영으로 표시되어 있습니다. 계열 2 데이터 블록 집합에서 레코드 유형은 400이고 블록 유형은 42입니다.

5.3.1 침입 이벤트는 eStreamer에서 확장 요청을 통해서만 요청할 수 있습니다. 이렇게 하려면 스트림 요청 메시지에서 이벤트 유형 코드 12, 버전 코드 7을 요청합니다. 확장 요청 제출에 대한 자세한 정보는 확장 요청 제출, 페이지 2-4의 내용을 참조하십시오.

버전 5.3.1 침입 이벤트의 경우 이벤트 ID, 매니지드 디바이스 ID 및 이벤트 초가 결합되어 고유 식별자가 생성됩니다. 그리고 연결 초, 연결 인스턴스 및 연결 카운터가 결합되어 침입 이벤트와 관련된 연결 이벤트의 고유 식별자가 생성됩니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
헤더 버전(1)																	메시지 유형(4)															
메시지 길이																																
네트워크 맵 ID																	레코드 유형(400)															
레코드 길이																																
eStreamer 서버 타임스탬프(이벤트에서 비트 23이 설정된 경우에 한함)																																
이후 사용을 위해 예약됨(이벤트에서 비트 23이 설정된 경우에 한함)																																
블록 유형(42)																																
블록 길이																																
디바이스 ID																																
이벤트 ID																																
이벤트 초																																
이벤트 마이크로초																																
규칙 ID(서명 ID)																																
생성자 ID																																
규칙 수정																																
분류 ID																																
우선순위 ID																																

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
소스 IP 주소																																
소스 IP 주소(계속)																																
소스 IP 주소(계속)																																
소스 IP 주소(계속)																																
대상 IP 주소																																
대상 IP 주소(계속)																																
대상 IP 주소(계속)																																
대상 IP 주소(계속)																																
소스 포트 또는 ICMP 유형																	대상 포트 또는 ICMP 코드															
IP 프로토콜 ID									영향 플래그								영향								차단됨							
MPLS 레이블																																
VLAN ID																	Pad															
정책 UUID																																
정책 UUID(계속)																																
정책 UUID(계속)																																
정책 UUID(계속)																																
사용자 ID																																
웹 애플리케이션 ID																																
클라이언트 애플리케이션 ID																																
애플리케이션 프로토콜 ID																																
액세스 제어 규칙 ID																																
액세스 제어 정책 UUID																																
액세스 제어 정책 UUID(계속)																																
액세스 제어 정책 UUID(계속)																																
액세스 제어 정책 UUID(계속)																																


바이트
0
1
2
3
비트
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
인터페이스 인그레스 UUID
인터페이스 인그레스 UUID(계속)
인터페이스 인그레스 UUID(계속)
인터페이스 인그레스 UUID(계속)
인터페이스 이그레스(egress) UUID
인터페이스 이그레스(egress) UUID(계속)
인터페이스 이그레스(egress) UUID(계속)
인터페이스 이그레스(egress) UUID(계속)
보안 영역 인그레스 UUID
보안 영역 인그레스 UUID(계속)
보안 영역 인그레스 UUID(계속)
보안 영역 인그레스 UUID(계속)
보안 영역 이그레스(egress) UUID
보안 영역 이그레스(egress) UUID(계속)
보안 영역 이그레스(egress) UUID(계속)
보안 영역 이그레스(egress) UUID(계속)
연결 타임스탬프
연결 인스턴스 ID
연결 카운터
소스 국가
대상 국가
IOC 번호
보안 상황
보안 상황(계속)
보안 상황(계속)
보안 상황(계속)
보안 상황(계속)

다음 표에는 각 침입 이벤트 레코드 데이터 필드에 대한 설명이 나와 있습니다.

표 B-6 5.3.1 버전용 침입 이벤트 레코드 필드

필드	데이터 유형	설명
블록 유형	unint32	침입 이벤트 데이터 블록을 시작합니다. 이 값은 항상 42입니다.
블록 길이	unint32	침입 이벤트 데이터 블록의 총 바이트 수입니다. 여기에는 침입 이벤트 블록 유형 및 길이 필드의 8바이트에 그 뒤의 데이터 바이트 수를 더한 값이 포함됩니다.
디바이스 ID	unit32	탐지 중인 매니지드 디바이스의 ID 번호를 포함합니다. 버전 3 또는 4 메타데이터를 요청하면 매니지드 디바이스 이름을 가져올 수 있습니다. 자세한 정보는 매니지드 디바이스 레코드 메타데이터, 페이지 3-35의 내용을 참조하십시오.
이벤트 ID	uint32	이벤트 ID 번호입니다.
이벤트 초	uint32	이벤트가 탐지된 UNIX 타임스탬프(1970년 1월 1일 이후의 초 단위 시간)입니다.
이벤트 마이크로초	uint32	이벤트 탐지 타임스탬프의 마이크로초(100만분의 1초) 단위 증분 시간입니다.
규칙 ID(서명 ID)	uint32	이벤트와 일치하는 규칙 ID 번호입니다.
생성자 ID	uint32	이벤트를 생성한 Firepower System 전처리기의 ID 번호입니다.
규칙 수정	uint32	규칙 수정 번호입니다.
분류 ID	uint32	이벤트 분류 메시지의 ID 번호입니다.
우선순위 ID	uint32	이벤트와 관련된 우선순위의 ID 번호입니다.
소스 IP 주소	uint8[16]	이벤트에 사용된 소스 IPv4 또는 IPv6 주소입니다.
대상 IP 주소	uint8[16]	이벤트에 사용된 대상 IPv4 또는 IPv6 주소입니다.
소스 포트 또는 ICMP 유형	uint16	이벤트 프로토콜 유형이 TCP 또는 UDP인 경우 소스 포트 번호이거나, ICMP 트래픽에 의해 이벤트가 발생한 경우 ICMP 유형입니다.
대상 포트 또는 ICMP 코드	uint16	이벤트 프로토콜 유형이 TCP 또는 UDP인 경우 대상 포트 번호이거나, ICMP 트래픽에 의해 이벤트가 발생한 경우 ICMP 코드입니다.
IP 프로토콜 번호	uint8	IANA에서 지정한 프로토콜 번호입니다. 예를 들면 다음과 같습니다. • 0 - IP • 1 - ICMP • 6 - TCP • 17 - UDP

표 B-6 5.3.1 버전용 침입 이벤트 레코드 필드 (계속)

필드	데이터 유형	설명
영향 플래그	bits[8]	이벤트의 영향 플래그 값입니다. 하위 8비트가 영향 레벨을 나타냅니다. 값은 다음과 같습니다. • 0x01(비트 0) - 소스 또는 대상 호스트가 시스템에서 모니터링하는 네트워크에 있습니다. • 0x02(비트 1) - 소스 또는 대상 호스트가 네트워크 맵에 있습니다. • 0x04(비트 2) - 소스 또는 대상 호스트가 이벤트의 포트에서 서버를 실행 중이거나(TCP 또는 UDP인 경우) IP 프로토콜을 사용합니다. • 0x08(비트 3) - 이벤트의 소스 또는 대상 호스트 운영 체제에 매핑된 취약점이 있습니다. • 0x10(비트 4) - 이벤트에서 탐지된 서버에 매핑된 취약점이 있습니다. • 0x20(비트 5) - 이벤트로 인해 매니지드 디바이스에서 세션이 삭제되었습니다(디바이스가 인라인, 스위치드 또는 라우티드 구축에서 실행 중인 경우에만 사용됨). Firepower System 웹 인터페이스의 차단 상태에 해당합니다. • 0x40(비트 6) - 이 이벤트를 생성한 규칙에 영향 플래그를 빨간색으로 설정하는 규칙 메타데이터가 있습니다. 소스 또는 대상 호스트가 바이러스, 트로이 목마, 기타 악성 소프트웨어에 감염되었을 가능성이 있습니다. • 0x80(비트 7) - 이벤트에서 탐지된 클라이언트에 매핑된 취약점이 있습니다. (5.0 이상 버전만 해당) 다음 영향 레벨 값은 방어 센터의 특정 우선순위에 매핑됩니다. `x`는 값이 0 또는 1일 수 있음을 나타냅니다. • (0, 알 수 없음): `00X00000` • 빨간색(1, 취약함): `XXXX1XXX, XXX1XXXX, X1XXXXXX, 1XXXXXXX` (5.0 이상 버전만 해당) • 주황색(2, 잠재적으로 취약함): `00X0011X` • 노란색(3, 현재 취약하지 않음): `00X0001X` • 파란색(4, 알 수 없는 대상): `00X00001`
영향	uint8	이벤트의 영향 플래그 값입니다. 값은 다음과 같습니다. • `1` - 빨간색(취약함) • `2` - 주황색(잠재적으로 취약함) • `3` - 노란색(현재 취약하지 않음) • `4` - 파란색(알 수 없는 대상) • `5` - 회색(알 수 없는 영향)

표 B-6 5.3.1 버전용 침입 이벤트 레코드 필드 (계속)

필드	데이터 유형	설명
차단됨	uint8	이벤트가 차단되었는지를 나타내는 값입니다. • 0 - 차단되지 않음 • 1 - 차단 • 2 - 차단 대상이지만 컨피그레이션에서 허용하지 않음
MPLS 레이블	uint32	MPLS 레이블입니다.
VLAN ID	uint16	패킷이 생성된 VLAN의 ID를 나타냅니다.
Pad	uint16	이후 사용을 위해 예약됩니다.
정책 UUID	uint8[16]	침입 정책의 고유 식별자 역할을 하는 정책 ID 번호입니다.
사용자 ID	uint32	해당하는 경우 사용자의 내부 ID 번호입니다.
웹 애플리케이션 ID	uint32	해당하는 경우 웹 애플리케이션의 내부 ID 번호입니다.
클라이언트 애플리케이션 ID	uint32	해당하는 경우 클라이언트 애플리케이션의 내부 ID 번호입니다.
애플리케이션 프로토콜 ID	uint32	해당하는 경우 애플리케이션 프로토콜의 내부 ID 번호입니다.
액세스 제어 규칙 ID	uint32	액세스 제어 규칙의 고유 식별자 역할을 하는 규칙 ID 번호입니다.
액세스 제어 정책 UUID	uint8[16]	액세스 제어 정책의 고유 식별자 역할을 하는 정책 ID 번호입니다.
인그레스 인터페이스 UUID	uint8[16]	인그레스 인터페이스의 고유 식별자 역할을 하는 인터페이스 ID 번호입니다.
이그레스(egress) 인터페이스 UUID	uint8[16]	이그레스(egress) 인터페이스의 고유 식별자 역할을 하는 인터페이스 ID 번호입니다.
인그레스 보안 영역 UUID	uint8[16]	인그레스 보안 영역의 고유 식별자 역할을 하는 영역 ID 번호입니다.
이그레스(egress) 보안 영역 UUID	uint8[16]	이그레스(egress) 보안 영역의 고유 식별자 역할을 하는 영역 ID 번호입니다.
연결 타임스탬프	uint32	침입 이벤트와 관련된 연결 이벤트의 UNIX 타임스탬프(1970년 1월 1일 이후의 초 단위 시간)입니다.
연결 인스턴스 ID	uint16	연결 이벤트를 생성한 매니지드 디바이스에 있는 Snort 인스턴스의 숫자 ID입니다.
연결 카운터	uint16	1초 이내에 발생하는 연결 이벤트를 구별하는 데 사용되는 값입니다.

표 B-6 5.3.1 버전용 침입 이벤트 레코드 필드 (계속)

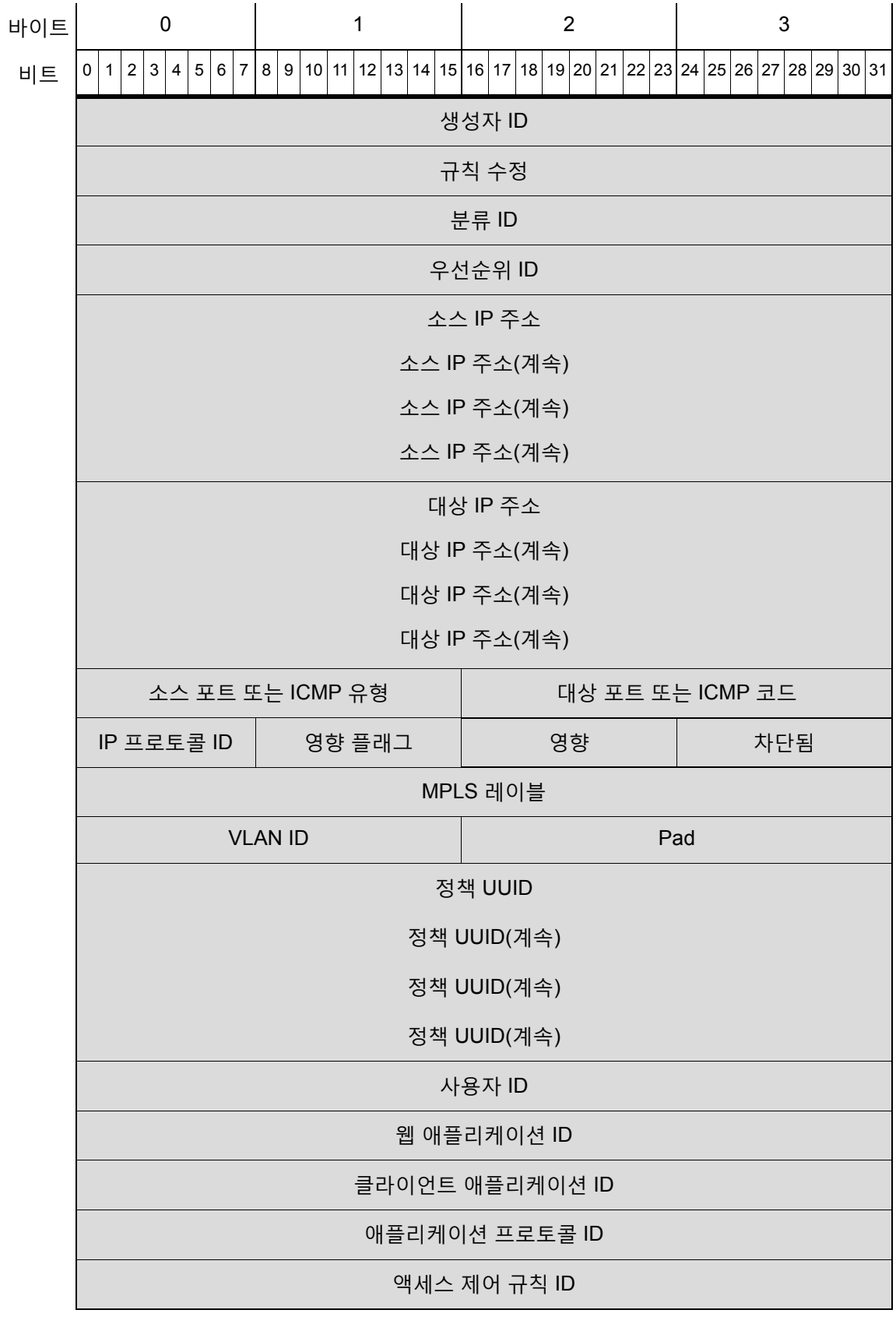
필드	데이터 유형	설명
소스 국가	uint16	소스 호스트의 국가 코드입니다.
대상 국가	uint16	대상 호스트의 국가 코드입니다.
IOC 번호	uint16	이 이벤트와 관련된 보안 침해의 ID 번호입니다.
보안 상황	uint8(16)	트래픽이 통과한 보안 상황(가상 방화벽)의 ID 번호입니다. 이 필드는 다중 컨텍스트 모드의 ASA FirePOWER 디바이스에 대해서만 채워집니다.

5.4.x 버전용 침입 이벤트 레코드

다음 그림에서 침입 이벤트 레코드의 필드는 음영으로 표시되어 있습니다. 계열 2 데이터 블록 집합에서 레코드 유형은 400이고 블록 유형은 45입니다. 이는 블록 유형 42를 대체하며 블록 유형 60으로 대체됩니다. SSL 지원 및 네트워크 분석 정책용 필드가 추가되었습니다.

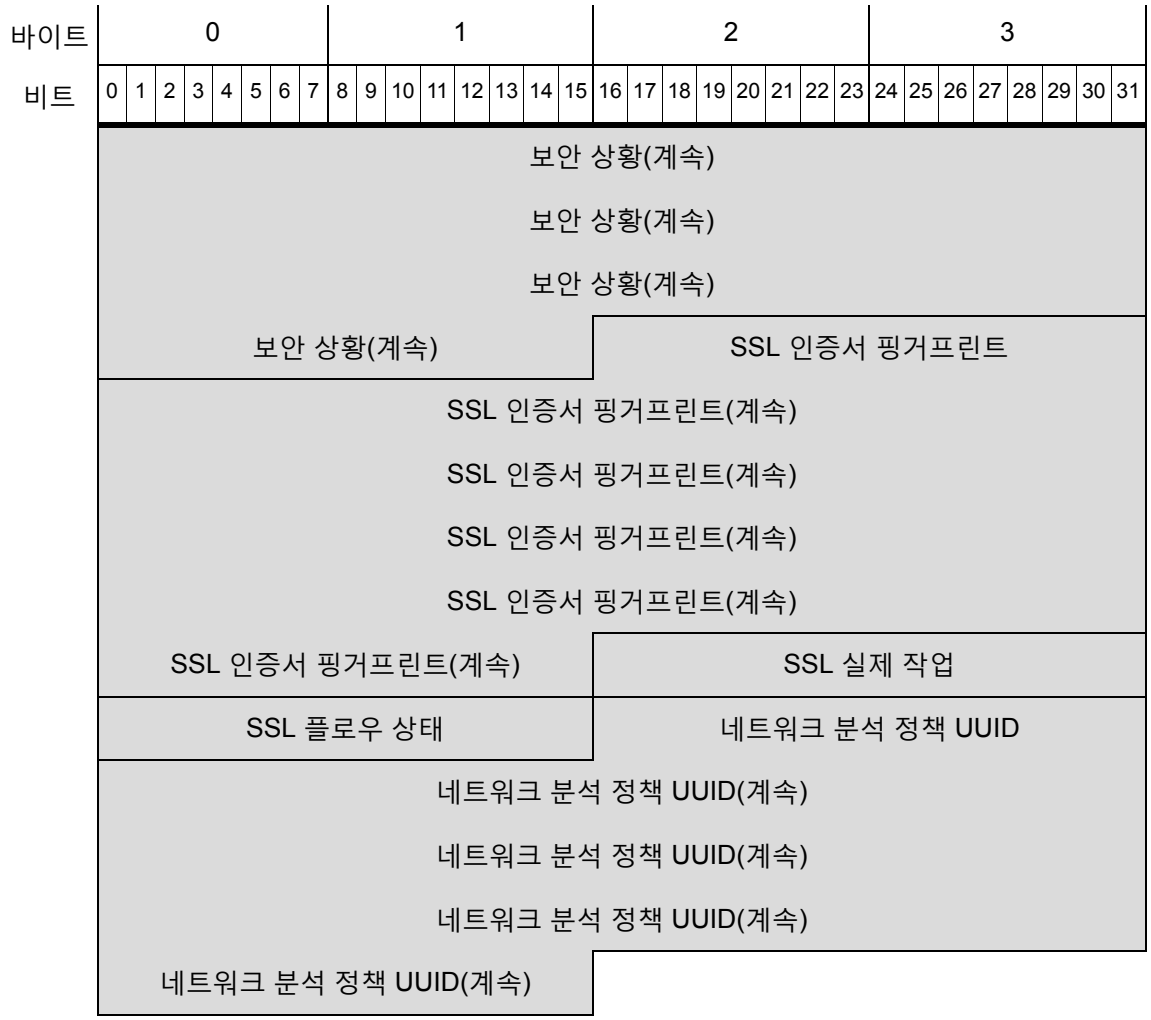
5.4.x 침입 이벤트는 eStreamer에서 확장 요청을 통해서만 요청할 수 있습니다. 이렇게 하려면 스트림 요청 메시지에서 이벤트 유형 코드 12, 버전 코드 8를 요청합니다. 확장 요청 제출에 대한 자세한 정보는 확장 요청 제출, 페이지 2-4의 내용을 참조하십시오.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
헤더 버전(1)																	메시지 유형(4)															
메시지 길이																																
네트워크 맵 ID																	레코드 유형(400)															
레코드 길이																																
eStreamer 서버 타임스탬프(이벤트에서 비트 23이 설정된 경우에 한함)																																
이후 사용을 위해 예약됨(이벤트에서 비트 23이 설정된 경우에 한함)																																
블록 유형(45)																																
블록 길이																																
디바이스 ID																																
이벤트 ID																																
이벤트 초																																
이벤트 마이크로초																																
규칙 ID(서명 ID)																																



바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
생성자 ID																																
규칙 수정																																
분류 ID																																
우선순위 ID																																
소스 IP 주소 소스 IP 주소(계속) 소스 IP 주소(계속) 소스 IP 주소(계속)																																
대상 IP 주소 대상 IP 주소(계속) 대상 IP 주소(계속) 대상 IP 주소(계속)																																
소스 포트 또는 ICMP 유형																	대상 포트 또는 ICMP 코드														
IP 프로토콜 ID									영향 플래그								영향								차단됨							
MPLS 레이블																																
VLAN ID																	Pad															
정책 UUID 정책 UUID(계속) 정책 UUID(계속) 정책 UUID(계속)																																
사용자 ID																																
웹 애플리케이션 ID																																
클라이언트 애플리케이션 ID																																
애플리케이션 프로토콜 ID																																
액세스 제어 규칙 ID																																

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
액세스 제어 정책 UUID																																
액세스 제어 정책 UUID(계속)																																
액세스 제어 정책 UUID(계속)																																
액세스 제어 정책 UUID(계속)																																
인터페이스 인그레스 UUID																																
인터페이스 인그레스 UUID(계속)																																
인터페이스 인그레스 UUID(계속)																																
인터페이스 인그레스 UUID(계속)																																
인터페이스 이그레스(egress) UUID																																
인터페이스 이그레스(egress) UUID(계속)																																
인터페이스 이그레스(egress) UUID(계속)																																
인터페이스 이그레스(egress) UUID(계속)																																
보안 영역 인그레스 UUID																																
보안 영역 인그레스 UUID(계속)																																
보안 영역 인그레스 UUID(계속)																																
보안 영역 인그레스 UUID(계속)																																
보안 영역 이그레스(egress) UUID																																
보안 영역 이그레스(egress) UUID(계속)																																
보안 영역 이그레스(egress) UUID(계속)																																
보안 영역 이그레스(egress) UUID(계속)																																
연결 타임스탬프																																
연결 인스턴스 ID																	연결 카운터															
소스 국가																	대상 국가															
IOC 번호																	보안 상황															



다음 표에는 각 침입 이벤트 레코드 데이터 필드에 대한 설명이 나와 있습니다.

표 B-7 5.4.x 버전용 침입 이벤트 레코드 필드

필드	데이터 유형	설명
블록 유형	unint32	침입 이벤트 데이터 블록을 시작합니다. 이 값은 항상 45입니다.
블록 길이	unint32	침입 이벤트 데이터 블록의 총 바이트 수입니다. 여기에는 침입 이벤트 블록 유형 및 길이 필드의 8바이트에 그 뒤의 데이터 바이트 수를 더한 값이 포함됩니다.
디바이스 ID	unit32	탐지 중인 매니지드 디바이스의 ID 번호를 포함합니다. 버전 3 또는 4 메타데이터를 요청하면 매니지드 디바이스 이름을 가져올 수 있습니다. 자세한 정보는 매니지드 디바이스 레코드 메타데이터, 페이지 3-35의 내용을 참조하십시오.
이벤트 ID	uint32	이벤트 ID 번호입니다.
이벤트 초	uint32	이벤트가 탐지된 UNIX 타임스탬프(1970년 1월 1일 이후의 초 단위 시간)입니다.

표 B-7 5.4.x 버전용 침입 이벤트 레코드 필드 (계속)

필드	데이터 유형	설명
이벤트 마이크로초	uint32	이벤트 탐지 타임스탬프의 마이크로초(100만분의 1초) 단위 증분 시간입니다.
규칙 ID(서명 ID)	uint32	이벤트와 일치하는 규칙 ID 번호입니다.
생성자 ID	uint32	이벤트를 생성한 Firepower System 전처리기의 ID 번호입니다.
규칙 수정	uint32	규칙 수정 번호입니다.
분류 ID	uint32	이벤트 분류 메시지의 ID 번호입니다.
우선순위 ID	uint32	이벤트와 관련된 우선순위의 ID 번호입니다.
소스 IP 주소	uint8[16]	이벤트에 사용된 소스 IPv4 또는 IPv6 주소입니다.
대상 IP 주소	uint8[16]	이벤트에 사용된 대상 IPv4 또는 IPv6 주소입니다.
소스 포트 또는 ICMP 유형	uint16	이벤트 프로토콜 유형이 TCP 또는 UDP인 경우 소스 포트 번호이거나, ICMP 트래픽에 의해 이벤트가 발생한 경우 ICMP 유형입니다.
대상 포트 또는 ICMP 코드	uint16	이벤트 프로토콜 유형이 TCP 또는 UDP인 경우 대상 포트 번호이거나, ICMP 트래픽에 의해 이벤트가 발생한 경우 ICMP 코드입니다.
IP 프로토콜 번호	uint8	IANA에서 지정한 프로토콜 번호입니다. 예를 들면 다음과 같습니다. • 0 - IP • 1 - ICMP • 6 - TCP • 17 - UDP

표 B-7 5.4.x 버전용 침입 이벤트 레코드 필드 (계속)

필드	데이터 유형	설명
영향 플래그	bits[8]	이벤트의 영향 플래그 값입니다. 하위 8비트가 영향 레벨을 나타냅니다. 값은 다음과 같습니다. • 0x01(비트 0) - 소스 또는 대상 호스트가 시스템에서 모니터링하는 네트워크에 있습니다. • 0x02(비트 1) - 소스 또는 대상 호스트가 네트워크 맵에 있습니다. • 0x04(비트 2) - 소스 또는 대상 호스트가 이벤트의 포트에서 서버를 실행 중이거나(TCP 또는 UDP인 경우) IP 프로토콜을 사용합니다. • 0x08(비트 3) - 이벤트의 소스 또는 대상 호스트 운영 체제에 매핑된 취약점이 있습니다. • 0x10(비트 4) - 이벤트에서 탐지된 서버에 매핑된 취약점이 있습니다. • 0x20(비트 5) - 이벤트로 인해 매니지드 디바이스에서 세션이 삭제되었습니다(디바이스가 인라인, 스위치드 또는 라우티드 구축에서 실행 중인 경우에만 사용됨). Firepower System 웹 인터페이스의 차단 상태에 해당합니다. • 0x40(비트 6) - 이 이벤트를 생성한 규칙에 영향 플래그를 빨간색으로 설정하는 규칙 메타데이터가 있습니다. 소스 또는 대상 호스트가 바이러스, 트로이 목마, 기타 악성 소프트웨어에 감염되었을 가능성이 있습니다. • 0x80(비트 7) - 이벤트에서 탐지된 클라이언트에 매핑된 취약점이 있습니다. (5.0 이상 버전만 해당) 다음 영향 레벨 값은 방어 센터의 특정 우선순위에 매핑됩니다. `x`는 값이 0 또는 1일 수 있음을 나타냅니다. • 회색(0, 알 수 없음): `00X00000` • 빨간색(1, 취약함): `XXXX1XXX`, `XXX1XXXX`, `X1XXXXXX`, `1XXXXXXX` (5.0 이상 버전만 해당) • 주황색(2, 잠재적으로 취약함): `00X0011X` • 노란색(3, 현재 취약하지 않음): `00X0001X` • 파란색(4, 알 수 없는 대상): `00X00001`
영향	uint8	이벤트의 영향 플래그 값입니다. 값은 다음과 같습니다. • `1` - 빨간색(취약함) • `2` - 주황색(잠재적으로 취약함) • `3` - 노란색(현재 취약하지 않음) • `4` - 파란색(알 수 없는 대상) • `5` - 회색(알 수 없는 영향)

표 B-7 5.4.x 버전용 침입 이벤트 레코드 필드 (계속)

필드	데이터 유형	설명
차단됨	uint8	이벤트가 차단되었는지를 나타내는 값입니다. • 0 - 차단되지 않음 • 1 - 차단 • 2 - 차단 대상이지만 컨피그레이션에서 허용하지 않음
MPLS 레이블	uint32	MPLS 레이블입니다.
VLAN ID	uint16	패킷이 생성된 VLAN의 ID를 나타냅니다.
Pad	uint16	이후 사용을 위해 예약됩니다.
정책 UUID	uint8[16]	침입 정책의 고유 식별자 역할을 하는 정책 ID 번호입니다.
사용자 ID	uint32	해당하는 경우 사용자의 내부 ID 번호입니다.
웹 애플리케이션 ID	uint32	해당하는 경우 웹 애플리케이션의 내부 ID 번호입니다.
클라이언트 애플리케이션 ID	uint32	해당하는 경우 클라이언트 애플리케이션의 내부 ID 번호입니다.
애플리케이션 프로토콜 ID	uint32	해당하는 경우 애플리케이션 프로토콜의 내부 ID 번호입니다.
액세스 제어 규칙 ID	uint32	액세스 제어 규칙의 고유 식별자 역할을 하는 규칙 ID 번호입니다.
액세스 제어 정책 UUID	uint8[16]	액세스 제어 정책의 고유 식별자 역할을 하는 정책 ID 번호입니다.
인그레스 인터페이스 UUID	uint8[16]	인그레스 인터페이스의 고유 식별자 역할을 하는 인터페이스 ID 번호입니다.
이그레스(egress) 인터페이스 UUID	uint8[16]	이그레스(egress) 인터페이스의 고유 식별자 역할을 하는 인터페이스 ID 번호입니다.
인그레스 보안 영역 UUID	uint8[16]	인그레스 보안 영역의 고유 식별자 역할을 하는 영역 ID 번호입니다.
이그레스(egress) 보안 영역 UUID	uint8[16]	이그레스(egress) 보안 영역의 고유 식별자 역할을 하는 영역 ID 번호입니다.
연결 타임스탬프	uint32	침입 이벤트와 관련된 연결 이벤트의 UNIX 타임스탬프(1970년 1월 1일 이후의 초 단위 시간)입니다.
연결 인스턴스 ID	uint16	연결 이벤트를 생성한 매니지드 디바이스에 있는 Snort 인스턴스의 숫자 ID입니다.
연결 카운터	uint16	1초 이내에 발생하는 연결 이벤트를 구별하는 데 사용되는 값입니다.
소스 국가	uint16	소스 호스트의 국가 코드입니다.
대상 국가	uint16	대상 호스트의 국가 코드입니다.
IOC 번호	uint16	이 이벤트와 관련된 보안 침해의 ID 번호입니다.

표 B-7 5.4.x 버전용 침입 이벤트 레코드 필드 (계속)

필드	데이터 유형	설명
보안 상황	uint8[16]	트래픽이 통과한 보안 상황(가상 방화벽)의 ID 번호입니다. 이 필드는 다중 컨텍스트 모드의 ASA FirePOWER 디바이스에 대해서만 채워집니다.
SSL 인증서 핑거프린트	uint8[20]	SSL 서버 인증서의 SHA1 해시입니다.
SSL 실제 작업	uint16	SSL 규칙에 기반한 연결에서 수행된 작업입니다. 규칙에 명시된 작업이 가능하지 않을 수도 있으므로, 이는 예상 작업과 다를 수 있습니다. 가능한 값은 다음과 같습니다. • 0 - '알 수 없음' • 1 - '암호 해독 안 함' • 2 - '차단' • 3 - '차단 및 재설정' • 4 - '암호 해독(알려진 키)' • 5 - '암호 해독(키 교체)' • 6 - '암호 해독(재서명)'

표 B-7 5.4.x 버전용 침입 이벤트 레코드 필드 (계속)

필드	데이터 유형	설명
SSL 플로우 상태	uint16	SSL 플로우의 상태입니다. 이 값은 작업을 수행한 이유 또는 오류 메시지가 표시된 이유를 설명합니다. 가능한 값은 다음과 같습니다. • 0 - '알 수 없음' • 1 - '일치하지 않음' • 2 - '성공' • 3 - '캐시되지 않은 세션' • 4 - '알 수 없는 암호 그룹' • 5 - '지원되지 않는 암호 그룹' • 6 - '지원되지 않는 SSL 버전' • 7 - 'SSL 압축 사용됨' • 8 - '패시브 모드에서 세션 암호 해독 불가' • 9 - '핸드셰이크 오류' • 10 - '암호 해독 오류' • 11 - '서버 이름 카테고리 조회 보류 중' • 12 - '공용 이름 카테고리 조회 보류 중' • 13 - '내부 오류' • 14 - '네트워크 파라미터 사용 불가' • 15 - '유효하지 않은 서버 인증서 핸들' • 16 - '서버 인증서 핑거프린트 사용 불가' • 17 - '주체 DN을 캐시할 수 없음' • 18 - '발급자 DN을 캐시할 수 없음' • 19 - '알 수 없는 SSL 버전' • 20 - '외부 인증서 목록 사용 불가' • 21 - '외부 인증서 핑거프린트 사용 불가' • 22 - '내부 인증서 목록이 유효하지 않음' • 23 - '내부 인증서 목록 사용 불가' • 24 - '내부 인증서 사용 불가' • 25 - '내부 인증서 핑거프린트 사용 불가' • 26 - '서버 인증서 검증 사용 불가' • 27 - '서버 인증서 검증 장애' • 28 - '유효하지 않은 작업'
네트워크 분석 정책 UUID	uint8[16]	침입 이벤트를 생성한 네트워크 분석 정책의 UUID입니다.

침입 영향 알림 데이터

침입 영향 알림 이벤트에는 영향 이벤트에 대한 정보가 포함됩니다. 침입 이벤트를 시스템 네트워크 맵 데이터에 비교하여 영향을 확인할 때 이 이벤트가 전송됩니다. 이 이벤트는 레코드 유형이 9인 표준 레코드 헤더를 사용하며, 그 뒤에는 계열 1 블록 그룹에서 데이터 블록 유형이 20인 침입 영향 알림 데이터 블록이 옵니다. 영향 알림 데이터 블록은 계열 1 데이터 블록 유형입니다. 계열 1 데이터 블록에 대한 자세한 정보는 검색(계열 1) 블록 이해, 페이지 4-63의 내용을 참조하십시오.

요청 메시지의 Flags(플래그) 필드에서 비트 5를 설정해야 eStreamer에서 침입 영향 이벤트를 전송하도록 요청할 수 있습니다. 요청 메시지에 대한 자세한 정보는 이벤트 스트림 요청 메시지 형식, 페이지 2-10의 내용을 참조하십시오. 이러한 경고의 버전 1은 IPv4만 처리합니다. 5.3에 도입된 버전 2는 IPv4와 함께 IPv6 이벤트도 처리합니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	헤더 버전(1)																메시지 유형(4)															
	메시지 길이																															
	네트워크 맵 ID																레코드 유형(9)															
	레코드 길이																															
	침입 영향 알림 블록 유형(20)																															
	침입 영향 알림 블록 길이																															
	이벤트 ID																															
	디바이스 ID																															
	이벤트 초																															
	영향																															
	소스 IP 주소																															
	대상 IP 주소																															
영향 설명	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	설명...																															

다음 표에는 영향 이벤트의 각 데이터 필드에 대한 설명이 나와 있습니다.

표 B-8 영향 이벤트 데이터 필드

필드	데이터 유형	설명
침입 영향 알림 블록 유형	uint32	침입 영향 알림 데이터 블록이 뒤에 옴을 나타냅니다. 이 필드의 값은 항상 20입니다. 침입 이벤트 및 메타 데이터 레코드 유형, 페이지 3-1의 내용을 참조하십시오.
침입 영향 알림 블록 길이	uint32	침입 영향 알림 데이터 블록의 길이를 나타냅니다. 여기에는 해당 블록 뒤에 오는 모든 데이터와 침입 영향 알림 블록 유형 및 길이의 8바이트가 포함됩니다.
이벤트 ID	uint32	이벤트 ID 번호를 나타냅니다.
디바이스 ID	uint32	매니지드 디바이스 ID 번호를 나타냅니다.
이벤트 초	uint32	이벤트가 탐지된 초 단위 시간(1970년 1월 1일 이후)을 나타냅니다.
영향	bits[8]	이벤트의 영향 플래그 값입니다. 하위 8비트가 영향 레벨을 나타냅니다. 값은 다음과 같습니다. • 0x01(비트 0) - 소스 또는 대상 호스트가 시스템에서 모니터링하는 네트워크에 있습니다. • 0x02(비트 1) - 소스 또는 대상 호스트가 네트워크 맵에 있습니다. • 0x04(비트 2) - 소스 또는 대상 호스트가 이벤트의 포트에서 서버를 실행 중이거나(TCP 또는 UDP인 경우) IP 프로토콜을 사용합니다. • 0X08(비트 3) - 이벤트의 소스 또는 대상 호스트 운영 체제에 매핑된 취약점이 있습니다. • 0x10(비트 4) - 이벤트에서 탐지된 서버에 매핑된 취약점이 있습니다. • 0x20(비트 5) - 이벤트로 인해 매니지드 디바이스에서 세션이 삭제되었습니다(디바이스가 인라인, 스위치드 또는 라우티드 구축에서 실행 중인 경우에만 사용됨). Firepower System 웹 인터페이스의 차단 상태에 해당합니다. • 0x40(비트 6) - 이 이벤트를 생성한 규칙에 영향 플래그를 빨간색으로 설정하는 규칙 메타데이터가 있습니다. 소스 또는 대상 호스트가 바이러스, 트로이 목마, 기타 악성 소프트웨어에 감염되었을 가능성이 있습니다. • 0x80(비트 7) - 이벤트에서 탐지된 클라이언트에 매핑된 취약점이 있습니다. (5.0 이상 버전만 해당) 다음 영향 레벨 값은 방어 센터의 특정 우선순위에 매핑됩니다. X는 값이 0 또는 1일 수 있음을 나타냅니다. • (0, 알 수 없음): 00X00000 • 빨간색(1, 취약함): XXXX1XXX, XXX1XXXX, X1XXXXXX, 1XXXXXXX (5.0 이상 버전만 해당) • 주황색(2, 잠재적으로 취약함): 00X0011X • 노란색(3, 현재 취약하지 않음): 00X0001X • 파란색(4, 알 수 없는 대상): 00X00001

표 B-8 영향 이벤트 데이터 필드 (계속)

필드	데이터 유형	설명
소스 IP 주소	uint8[4]	영향 이벤트와 관련된 호스트의 IP 주소(IP 주소 옥텟 형식)입니다.
대상 IP 주소	uint8[4]	해당하는 경우 영향 이벤트와 관련된 호스트의 대상 IP 주소(IP 주소 옥텟 형식)입니다. 대상 IP 주소가 없으면 이 값은 0입니다.
문자열 블록 유형	uint32	영향 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0으로 설정됩니다. 문자열 블록에 대한 자세한 정보는 문자열 데이터 블록, 페이지 4-72의 내용을 참조하십시오.
문자열 블록 길이	uint32	이벤트 설명 문자열 블록의 바이트 수입니다. 여기에는 문자열 블록 유형의 4바이트 + 문자열 블록 길이의 4바이트 + 설명의 바이트 수가 포함됩니다.
설명	string	영향 이벤트의 설명입니다.

레거시 악성코드 이벤트 데이터 구조

5.1 버전용 악성코드 이벤트 데이터 블록

eStreamer 서비스는 악성코드 이벤트 데이터 블록을 사용하여 악성코드 이벤트에 대한 정보를 저장합니다. 이러한 이벤트에는 클라우드 내에서 탐지 또는 격리된 악성코드, 탐지 방법, 악성코드의 영향을 받은 호스트 및 사용자에 대한 정보가 포함됩니다. 계열 2 블록 그룹에서 악성코드 이벤트 데이터 블록의 블록 유형은 16입니다. 이벤트 버전이 1이고 이벤트 코드가 101인 요청 메시지에서 악성코드 이벤트 플래그(Request Flags(요청 플래그) 필드의 비트 30)를 설정하여 악성코드 이벤트 레코드의 일부분으로 이벤트를 요청합니다.

다음 그림에 악성코드 이벤트 데이터 블록의 구조가 나와 있습니다.

바이트	0				1				2				3			
비트	0 1 2 3 4 5 6 7				8 9 10 11 12 13 14 15				16 17 18 19 20 21 22 23				24 25 26 27 28 29 30 31			
	악성코드 이벤트 블록 유형(16)															
	악성코드 이벤트 블록 길이															
	에이전트 UUID															
	에이전트 UUID(계속)															
	에이전트 UUID(계속)															
	에이전트 UUID(계속)															
	클라우드 UUID															
	클라우드 UUID(계속)															
	클라우드 UUID(계속)															
	클라우드 UUID(계속)															
	타임스탬프															
	이벤트 유형 ID															
	이벤트 하위 유형 ID				호스트 IP 주소											
탐지 이름	호스트 IP 주소(계속)				탐지기 ID				문자열 블록 유형(0)							
	문자열 블록 유형(0)(계속)								문자열 블록 길이							
	문자열 블록 길이(계속)								탐지 이름...							
사용자	문자열 블록 유형(0)															
	문자열 블록 길이															
	사용자...															
파일 이름	문자열 블록 유형(0)															
	문자열 블록 길이															
	파일 이름...															

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
파일 경로	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	파일 경로...																															
파일 SHA 해시	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	파일 SHA 해시...																															
	파일 크기																															
	파일 유형								파일 타임스탬프																							
상위 파일 이름	파일 타임스탬프(계속)								문자열 블록 유형(0)																							
	문자열 블록 유형(0)(계속)								문자열 블록 길이																							
	문자열 블록 길이(계속)								상위 파일 이름...																							
상위 파일 SHA 해시	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	상위 파일 SHA 해시...																															
이벤트 설명	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	이벤트 설명...																															

다음 표에는 악성코드 이벤트 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 B-9 악성코드 이벤트 데이터 블록 필드

필드	데이터 유형	설명
악성코드 이벤트 블록 유형	uint32	악성코드 이벤트 데이터 블록을 시작합니다. 이 값은 항상 16입니다.
악성코드 이벤트 블록 길이	uint32	악성코드 이벤트 데이터 블록의 총 바이트 수입니다. 여기에는 악성코드 이벤트 블록 유형 및 길이 필드의 8바이트에 그 뒤의 데이터 바이트 수를 더한 값이 포함됩니다.
에이전트 UUID	uint8[16]	악성코드를 보고하는 AMP for Endpoints 에이전트의 내부 고유 ID입니다.
클라우드 UUID	uint8[16]	악성코드 이벤트가 시작된 악성코드 인식 네트워크의 내부 고유 ID입니다.
타임스탬프	uint32	악성코드 이벤트 생성 타임스탬프입니다.
이벤트 유형 ID	uint32	악성코드 이벤트 유형의 내부 ID입니다.
이벤트 하위 유형 ID	uint8	악성코드를 탐지하도록 유도한 작업의 내부 ID입니다.
호스트 IP 주소	uint32	악성코드 이벤트와 관련된 호스트 IP 주소입니다.
탐지기 ID	uint8	악성코드를 탐지한 탐지 기술의 내부 ID입니다.
문자열 블록 유형	uint32	탐지 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	탐지 이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Detection Name(탐지 이름) 필드의 바이트 수를 더한 값이 포함됩니다.
탐지 이름	string	탐지 또는 격리된 악성코드의 이름입니다.
문자열 블록 유형	uint32	사용자 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	사용자 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 User(사용자) 필드의 바이트 수를 더한 값이 포함됩니다.
사용자	string	Cisco 에이전트가 설치되어 있으며 악성코드 이벤트가 발생한 컴퓨터의 사용자입니다. 이러한 사용자는 사용자 검색에 연결되지 않습니다.
문자열 블록 유형	uint32	파일 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	파일 이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 File Name(파일 이름) 필드의 바이트 수를 더한 값이 포함됩니다.
파일 이름	string	탐지 또는 격리된 파일의 이름입니다.
문자열 블록 유형	uint32	파일 경로가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.

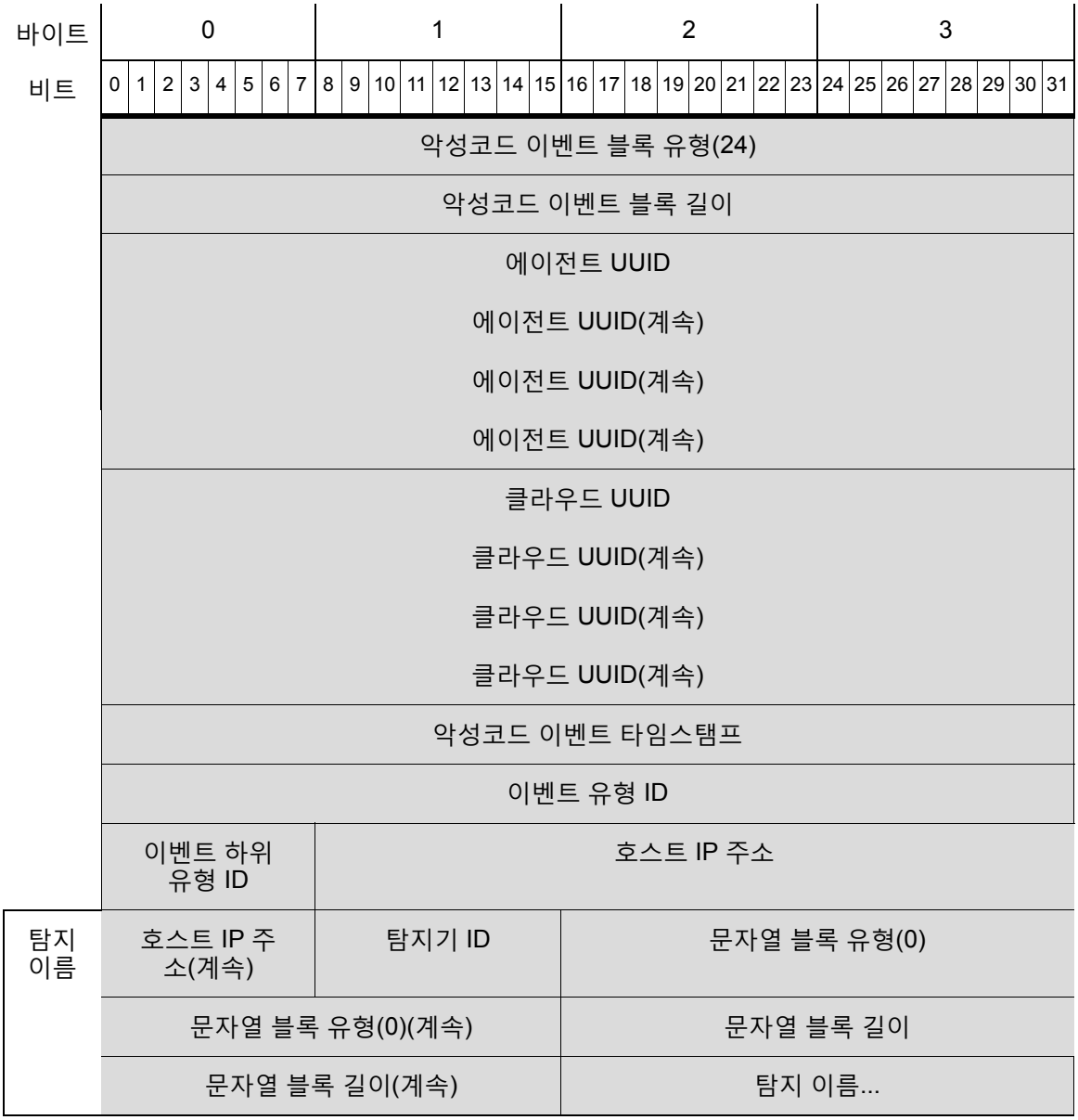
표 B-9 악성코드 이벤트 데이터 블록 필드 (계속)

필드	데이터 유형	설명
문자열 블록 길이	uint32	파일 경로 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 File Path(파일 경로) 필드의 바이트 수를 더한 값이 포함됩니다.
파일 경로	string	탐지 또는 격리된 파일의 파일 경로이며, 파일 이름은 포함되지 않습니다.
문자열 블록 유형	uint32	파일 SHA 해시가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	파일 SHA 해시 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 File SHA Hash(파일 SHA 해시) 필드의 바이트 수를 더한 값이 포함됩니다.
파일 SHA 해시	string	탐지 또는 격리된 파일의 SHA-256 해시 값입니다.
파일 크기	uint32	탐지 또는 격리된 파일의 바이트 크기입니다.
파일 유형	uint8	탐지 또는 격리된 파일의 파일 유형입니다.
파일 타임스탬프	uint32	탐지 또는 격리된 파일의 생성 타임스탬프입니다.
문자열 블록 유형	uint32	상위 파일 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	상위 파일 이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Parent File Name(상위 파일 이름) 필드의 바이트 수를 더한 값이 포함됩니다.
상위 파일 이름	string	탐지가 발생했을 때 탐지 또는 격리된 파일에 액세스한 파일의 이름입니다.
문자열 블록 유형	uint32	상위 파일 SHA 해시가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	상위 파일 SHA 해시 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Parent File SHA Hash(상위 파일 SHA 해시) 필드의 바이트 수를 더한 값이 포함됩니다.
상위 파일 SHA 해시	string	탐지가 발생했을 때 탐지 또는 격리된 파일에 액세스한 상위 파일의 SHA-256 해시 값입니다.
문자열 블록 유형	uint32	이벤트 설명이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	이벤트 설명 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Event Description(이벤트 설명) 필드의 바이트 수를 더한 값이 포함됩니다.
이벤트 설명	string	이벤트 유형과 관련된 추가 이벤트 정보입니다.

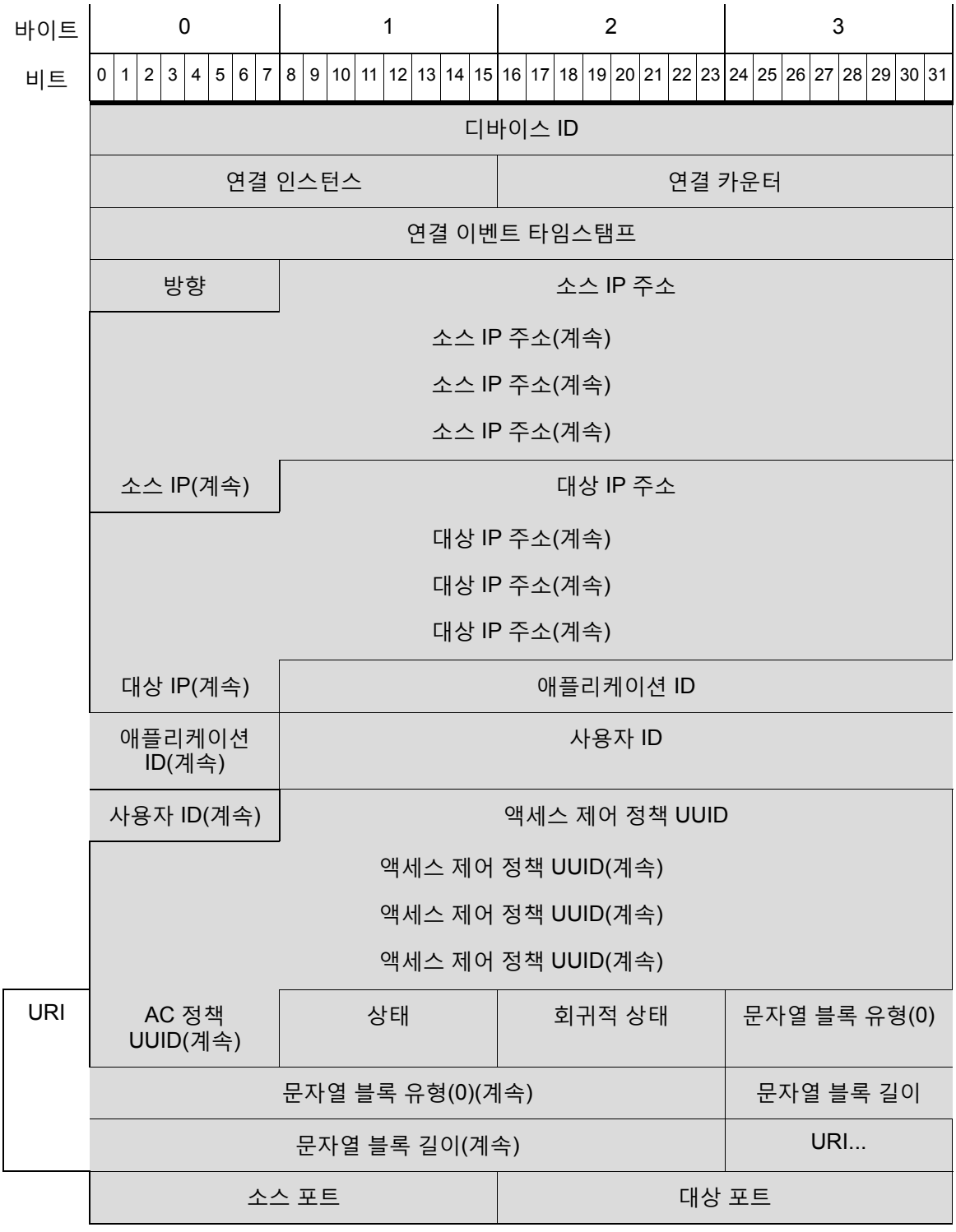
5.1.1.x 버전용 악성코드 이벤트 데이터 블록

eStreamer 서비스는 악성코드 이벤트 데이터 블록을 사용하여 악성코드 이벤트에 대한 정보를 저장합니다. 이러한 이벤트에는 클라우드 내에서 탐지 또는 격리된 악성코드, 탐지 방법, 악성코드의 영향을 받은 호스트 및 사용자에 대한 정보가 포함됩니다. 계열 2 블록 그룹에서 악성코드 이벤트 데이터 블록의 블록 유형은 24입니다. 이벤트 버전이 2이고 이벤트 코드가 101인 요청 메시지에서 악성코드 이벤트 플래그(Request Flags(요청 플래그) 필드의 비트 30)를 설정하여 악성코드 이벤트 레코드의 일부분으로 이벤트를 요청합니다.

다음 그림에 악성코드 이벤트 데이터 블록의 구조가 나와 있습니다.



바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
사용자	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	사용자...																															
파일 이름	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	파일 이름...																															
파일 경로	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	파일 경로...																															
파일 SHA 해시	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	파일 SHA 해시...																															
	파일 크기																															
	파일 유형								파일 타임스탬프																							
상위 파일 이름	파일 타임스탬프(계속)								문자열 블록 유형(0)																							
	문자열 블록 유형(0)(계속)								문자열 블록 길이																							
	문자열 블록 길이(계속)								상위 파일 이름...																							
상위 파일 SHA 해시	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	상위 파일 SHA 해시...																															
이벤트 설명	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	이벤트 설명...																															



다음 표에는 악성코드 이벤트 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 B-10 5.1.1.x 버전용 악성코드 이벤트 데이터 블록 필드

필드	데이터 유형	설명
악성코드 이벤트 블록 유형	uint32	악성코드 이벤트 데이터 블록을 시작합니다. 이 값은 항상 24입니다.
악성코드 이벤트 블록 길이	uint32	악성코드 이벤트 데이터 블록의 총 바이트 수입니다. 여기에는 악성코드 이벤트 블록 유형 및 길이 필드의 8바이트에 그 뒤의 데이터 바이트 수를 더한 값이 포함됩니다.
에이전트 UUID	uint8[16]	악성코드를 보고하는 AMP for Endpoints 에이전트의 내부 고유 ID입니다.
클라우드 UUID	uint8[16]	악성코드 이벤트가 시작된 악성코드 인식 네트워크의 내부 고유 ID입니다.
악성코드 이벤트 타임스탬프	uint32	악성코드 이벤트 생성 타임스탬프입니다.
이벤트 유형 ID	uint32	악성코드 이벤트 유형의 내부 ID입니다.
이벤트 하위 유형 ID	uint8	악성코드를 탐지하도록 유도한 작업의 내부 ID입니다.
호스트 IP 주소	uint32	악성코드 이벤트와 관련된 호스트 IP 주소입니다.
탐지기 ID	uint8	악성코드를 탐지한 탐지 기술의 내부 ID입니다.
문자열 블록 유형	uint32	탐지 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	탐지 이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Detection Name(탐지 이름) 필드의 바이트 수를 더한 값이 포함됩니다.
탐지 이름	string	탐지 또는 격리된 악성코드의 이름입니다.
문자열 블록 유형	uint32	사용자 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	사용자 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 User(사용자) 필드의 바이트 수를 더한 값이 포함됩니다.
사용자	string	Cisco 에이전트가 설치되어 있으며 악성코드 이벤트가 발생한 컴퓨터의 사용자입니다. 이러한 사용자는 사용자 검색에 연결되지 않습니다.
문자열 블록 유형	uint32	파일 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	파일 이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 File Name(파일 이름) 필드의 바이트 수를 더한 값이 포함됩니다.
파일 이름	string	탐지 또는 격리된 파일의 이름입니다.
문자열 블록 유형	uint32	파일 경로가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.

표 B-10 5.1.1.x 버전용 악성코드 이벤트 데이터 블록 필드 (계속)

필드	데이터 유형	설명
문자열 블록 길이	uint32	파일 경로 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 File Path(파일 경로) 필드의 바이트 수를 더한 값이 포함됩니다.
파일 경로	string	탐지 또는 격리된 파일의 파일 경로이며, 파일 이름은 포함되지 않습니다.
문자열 블록 유형	uint32	파일 SHA 해시가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	파일 SHA 해시 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 File SHA Hash(파일 SHA 해시) 필드의 바이트 수를 더한 값이 포함됩니다.
파일 SHA 해시	string	탐지 또는 격리된 파일의 SHA-256 해시 값이 렌더링된 문자열입니다.
파일 크기	uint32	탐지 또는 격리된 파일의 바이트 크기입니다.
파일 유형	uint8	탐지 또는 격리된 파일의 파일 유형입니다.
파일 타임스탬프	uint32	탐지 또는 격리된 파일이 생성된 UNIX 타임스탬프(1970년 1월 1일 이후의 초 단위 시간)입니다.
문자열 블록 유형	uint32	상위 파일 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	상위 파일 이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Parent File Name(상위 파일 이름) 필드의 바이트 수를 더한 값이 포함됩니다.
상위 파일 이름	string	탐지가 발생했을 때 탐지 또는 격리된 파일에 액세스한 파일의 이름입니다.
문자열 블록 유형	uint32	상위 파일 SHA 해시가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	상위 파일 SHA 해시 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Parent File SHA Hash(상위 파일 SHA 해시) 필드의 바이트 수를 더한 값이 포함됩니다.
상위 파일 SHA 해시	string	탐지가 발생했을 때 탐지 또는 격리된 파일에 액세스한 상위 파일의 SHA-256 해시 값입니다.
문자열 블록 유형	uint32	이벤트 설명이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	이벤트 설명 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Event Description(이벤트 설명) 필드의 바이트 수를 더한 값이 포함됩니다.
이벤트 설명	string	이벤트 유형과 관련된 추가 이벤트 정보입니다.
디바이스 ID	uint32	이벤트를 생성한 디바이스의 ID입니다.

표 B-10 5.1.1.x 버전용 악성코드 이벤트 데이터 블록 필드 (계속)

필드	데이터 유형	설명
연결 인스턴스	uint16	이벤트를 생성한 디바이스의 Snort 인스턴스입니다. 이 이벤트를 연결 또는 IDS 이벤트와 연결하는 데 사용됩니다.
연결 카운터	uint16	1초 이내에 발생하는 연결 이벤트를 구별하는 데 사용되는 값입니다.
연결 이벤트 타임스탬프	uint32	연결 이벤트의 타임스탬프입니다.
방향	uint8	파일이 업로드되었는지 아니면 다운로드되었는지를 나타냅니다. 다음과 같은 값을 사용할 수 있습니다. • 1 - 다운로드 • 2 - 업로드 현재 이 값은 프로토콜에 따라 달라집니다(예: 연결이 HTTP인 경우 다운로드임).
소스 IP 주소	uint8[16]	연결 소스의 IPv4 또는 IPv6 주소입니다.
대상 IP 주소	uint8[16]	연결 대상의 IPv4 또는 IPv6 주소입니다.
애플리케이션 ID	uint32	파일 전송을 사용하여 애플리케이션에 매핑되는 ID 번호입니다.
사용자 ID	uint32	시스템이 식별한 대상 호스트에 로그인하는 사용자의 ID 번호입니다.
액세스 제어 정책 UUID	uint8[16]	이벤트를 트리거한 액세스 제어 정책의 고유 식별자 역할을 하는 ID 번호입니다.
상태	uint8	파일의 악성코드 상태입니다. 가능한 값은 다음과 같습니다. • 1 - CLEAN - 파일이 정상 상태이며 악성코드가 포함되어 있지 않습니다. • 2 - UNKNOWN - 파일에 악성코드가 포함되어 있는지 알 수 없습니다. • 3 - MALWARE - 파일에 악성코드가 포함되어 있습니다. • 4 - CACHE_MISS - 소프트웨어가 Cisco 클라우드에 상태 요청을 보낼 수 없습니다. • 5 - NO_CLOUD_RESP - Cisco 클라우드 서비스가 요청에 응답하지 않았습니다.
회귀적 상태	uint8	상태가 업데이트된 경우 파일의 상태입니다. 상태가 업데이트되지 않은 경우 이 필드에는 Disposition(상태) 필드와 동일한 값이 포함됩니다. 가능한 값은 Disposition(상태) 필드와 동일합니다.
문자열 블록 유형	uint32	URI가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	URI 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 URI 필드의 바이트 수를 더한 값이 포함됩니다.

표 B-10 5.1.1.x 버전용 악성코드 이벤트 데이터 블록 필드 (계속)

필드	데이터 유형	설명
URI	string	연결의 URI입니다.
소스 포트	uint16	연결 소스의 포트 번호입니다.
대상 포트	uint16	연결 대상의 포트 번호입니다.

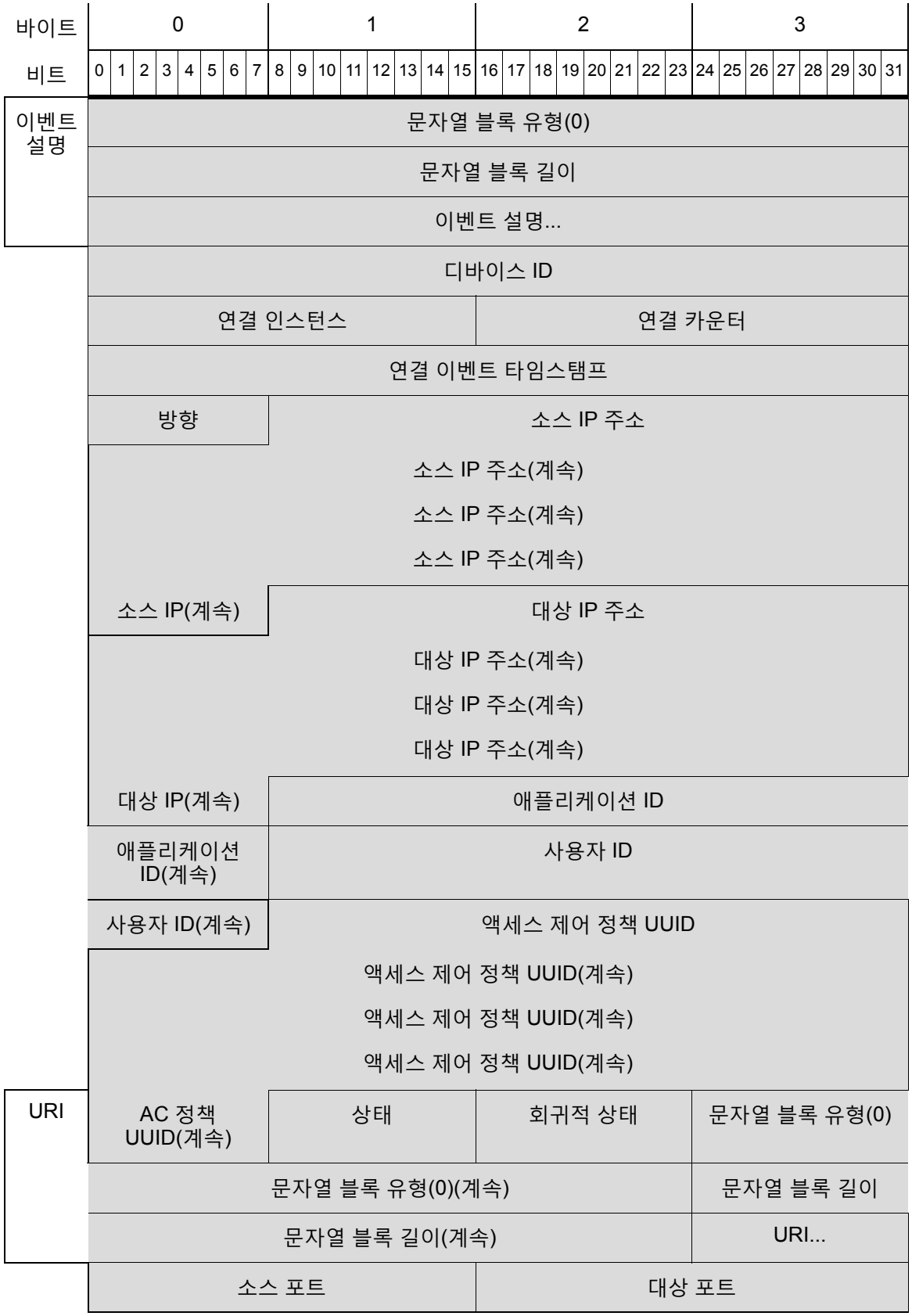
5.2.x 버전용 악성코드 이벤트 데이터 블록

eStreamer 서비스는 악성코드 이벤트 데이터 블록을 사용하여 악성코드 이벤트에 대한 정보를 저장합니다. 이러한 이벤트에는 클라우드 내에서 탐지 또는 격리된 악성코드, 탐지 방법, 악성코드의 영향을 받은 호스트 및 사용자에 대한 정보가 포함됩니다. 계열 2 블록 그룹에서 악성코드 이벤트 데이터 블록의 블록 유형은 33입니다. 이벤트 버전이 3이고 이벤트 코드가 101인 요청 메시지에서 악성코드 이벤트 플래그(Request Flags(요청 플래그) 필드의 비트 30)를 설정하여 악성코드 이벤트 레코드의 일부분으로 이벤트를 요청합니다.

다음 그림에 악성코드 이벤트 데이터 블록의 구조가 나와 있습니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
악성코드 이벤트 블록 유형(33)																																
악성코드 이벤트 블록 길이																																
에이전트 UUID																																
에이전트 UUID(계속)																																
에이전트 UUID(계속)																																
에이전트 UUID(계속)																																
클라우드 UUID																																
클라우드 UUID(계속)																																
클라우드 UUID(계속)																																
클라우드 UUID(계속)																																
악성코드 이벤트 타임스탬프																																
이벤트 유형 ID																																

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
탐지 이름	이벤트 하위 유형 ID								탐지기 ID								문자열 블록 유형(0)															
	문자열 블록 유형(0)(계속)																문자열 블록 길이															
	문자열 블록 길이(계속)																탐지 이름...															
사용자	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	사용자...																															
파일 이름	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	파일 이름...																															
파일 경로	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	파일 경로...																															
파일 SHA 해시	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	파일 SHA 해시...																															
	파일 크기																															
	파일 유형																															
	파일 타임스탬프																															
상위 파일 이름	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	상위 파일 이름...																															
상위 파일 SHA 해시	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	상위 파일 SHA 해시...																															


바이트
0
1
2
3
비트
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
이벤트 설명
문자열 블록 유형(0)
문자열 블록 길이
이벤트 설명...
디바이스 ID
연결 인스턴스
연결 카운터
연결 이벤트 타임스탬프
방향
소스 IP 주소
소스 IP 주소(계속)
소스 IP 주소(계속)
소스 IP 주소(계속)
소스 IP(계속)
대상 IP 주소
대상 IP 주소(계속)
대상 IP 주소(계속)
대상 IP 주소(계속)
대상 IP(계속)
애플리케이션 ID
애플리케이션 ID(계속)
사용자 ID
사용자 ID(계속)
액세스 제어 정책 UUID
액세스 제어 정책 UUID(계속)
액세스 제어 정책 UUID(계속)
액세스 제어 정책 UUID(계속)
URI
AC 정책 UUID(계속)
상태
회귀적 상태
문자열 블록 유형(0)
문자열 블록 유형(0)(계속)
문자열 블록 길이
문자열 블록 길이(계속)
URI...
소스 포트
대상 포트

다음 표에는 악성코드 이벤트 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 B-11 5.2.x 버전용 악성코드 이벤트 데이터 블록 필드

필드	데이터 유형	설명
악성코드 이벤트 블록 유형	uint32	악성코드 이벤트 데이터 블록을 시작합니다. 이 값은 항상 33입니다.
악성코드 이벤트 블록 길이	uint32	악성코드 이벤트 데이터 블록의 총 바이트 수입니다. 여기에는 악성코드 이벤트 블록 유형 및 길이 필드의 8바이트에 그 뒤의 데이터 바이트 수를 더한 값이 포함됩니다.
에이전트 UUID	uint8[16]	악성코드를 보고하는 AMP for Endpoints 에이전트의 내부 고유 ID입니다.
클라우드 UUID	uint8[16]	악성코드 이벤트가 시작된 악성코드 인식 네트워크의 내부 고유 ID입니다.
악성코드 이벤트 타임스탬프	uint32	악성코드 이벤트 생성 타임스탬프입니다.
이벤트 유형 ID	uint32	악성코드 이벤트 유형의 내부 ID입니다.
이벤트 하위 유형 ID	uint8	악성코드를 탐지하도록 유도한 작업의 내부 ID입니다.
탐지기 ID	uint8	악성코드를 탐지한 탐지 기술의 내부 ID입니다.
문자열 블록 유형	uint32	탐지 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	탐지 이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Detection Name(탐지 이름) 필드의 바이트 수를 더한 값이 포함됩니다.
탐지 이름	string	탐지 또는 격리된 악성코드의 이름입니다.
문자열 블록 유형	uint32	사용자 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	사용자 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 User(사용자) 필드의 바이트 수를 더한 값이 포함됩니다.
사용자	string	Cisco 에이전트가 설치되어 있으며 악성코드 이벤트가 발생한 컴퓨터의 사용자입니다. 이러한 사용자는 사용자 검색에 연결되지 않습니다.

표 B-11 5.2.x 버전용 악성코드 이벤트 데이터 블록 필드 (계속)

필드	데이터 유형	설명
문자열 블록 유형	uint32	파일 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	파일 이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 File Name(파일 이름) 필드의 바이트 수를 더한 값이 포함됩니다.
파일 이름	string	탐지 또는 격리된 파일의 이름입니다.
문자열 블록 유형	uint32	파일 경로가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	파일 경로 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 File Path(파일 경로) 필드의 바이트 수를 더한 값이 포함됩니다.
파일 경로	string	탐지 또는 격리된 파일의 파일 경로이며, 파일 이름은 포함되지 않습니다.
문자열 블록 유형	uint32	파일 SHA 해시가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	파일 SHA 해시 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 File SHA Hash(파일 SHA 해시) 필드의 바이트 수를 더한 값이 포함됩니다.
파일 SHA 해시	string	탐지 또는 격리된 파일의 SHA-256 해시 값이 렌더링된 문자열입니다.
파일 크기	uint32	탐지 또는 격리된 파일의 바이트 크기입니다.
파일 유형	uint8	탐지 또는 격리된 파일의 파일 유형입니다.
파일 타임스탬프	uint32	탐지 또는 격리된 파일이 생성된 UNIX 타임스탬프(1970년 1월 1일 이후의 초 단위 시간)입니다.
문자열 블록 유형	uint32	상위 파일 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	상위 파일 이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Parent File Name(상위 파일 이름) 필드의 바이트 수를 더한 값이 포함됩니다.
상위 파일 이름	string	탐지가 발생했을 때 탐지 또는 격리된 파일에 액세스한 파일의 이름입니다.
문자열 블록 유형	uint32	상위 파일 SHA 해시가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	상위 파일 SHA 해시 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Parent File SHA Hash(상위 파일 SHA 해시) 필드의 바이트 수를 더한 값이 포함됩니다.
상위 파일 SHA 해시	string	탐지가 발생했을 때 탐지 또는 격리된 파일에 액세스한 상위 파일의 SHA-256 해시 값입니다.

표 B-11 5.2.x 버전용 악성코드 이벤트 데이터 블록 필드 (계속)

필드	데이터 유형	설명
문자열 블록 유형	uint32	이벤트 설명이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	이벤트 설명 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Event Description(이벤트 설명) 필드의 바이트 수를 더한 값이 포함됩니다.
이벤트 설명	string	이벤트 유형과 관련된 추가 이벤트 정보입니다.
디바이스 ID	uint32	이벤트를 생성한 디바이스의 ID입니다.
연결 인스턴스	uint16	이벤트를 생성한 디바이스의 Snort 인스턴스입니다. 이벤트를 연결 또는 IDS 이벤트와 연결하는 데 사용됩니다.
연결 카운터	uint16	1초 이내에 발생하는 연결 이벤트를 구별하는 데 사용되는 값입니다.
연결 이벤트 타임스탬프	uint32	연결 이벤트의 타임스탬프입니다.
방향	uint8	파일이 업로드되었는지 아니면 다운로드되었는지를 나타냅니다. 다음과 같은 값을 사용할 수 있습니다. • 1 - 다운로드 • 2 - 업로드 현재 이 값은 프로토콜에 따라 달라집니다(예: 연결이 HTTP인 경우 다운로드임).
소스 IP 주소	uint8[16]	연결 소스의 IPv4 또는 IPv6 주소입니다.
대상 IP 주소	uint8[16]	연결 대상의 IPv4 또는 IPv6 주소입니다.
애플리케이션 ID	uint32	파일 전송을 사용하여 애플리케이션에 매핑되는 ID 번호입니다.
사용자 ID	uint32	시스템이 식별한 대상 호스트에 로그인하는 사용자의 ID 번호입니다.
액세스 제어 정책 UUID	uint8[16]	이벤트를 트리거한 액세스 제어 정책의 고유 식별자 역할을 하는 ID 번호입니다.
상태	uint8	파일의 악성코드 상태입니다. 가능한 값은 다음과 같습니다. • 1 - CLEAN - 파일이 정상 상태이며 악성코드가 포함되어 있지 않습니다. • 2 - NEUTRAL - 파일에 악성코드가 포함되어 있는지 알 수 없습니다. • 3 - MALWARE - 파일에 악성코드가 포함되어 있습니다. • 4 - CACHE_MISS - 소프트웨어가 Cisco 클라우드에 상태 요청을 보낼 수 없거나 Cisco 클라우드 서비스가 요청에 응답하지 않았습니다.

표 B-11 5.2.x 버전용 악성코드 이벤트 데이터 블록 필드 (계속)

필드	데이터 유형	설명
회귀적 상태	uint8	상태가 업데이트된 경우 파일의 상태입니다. 상태가 업데이트되지 않은 경우 이 필드에는 Disposition(상태) 필드와 동일한 값이 포함됩니다. 가능한 값은 Disposition(상태) 필드와 동일합니다.
문자열 블록 유형	uint32	URI가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	URI 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 URI 필드의 바이트 수를 더한 값이 포함됩니다.
URI	string	연결의 URI입니다.
소스 포트	uint16	연결 소스의 포트 번호입니다.
대상 포트	uint16	연결 대상의 포트 번호입니다.
소스 국가	uint16	소스 호스트의 국가 코드입니다.
대상 국가	uint16	대상 호스트의 국가 코드입니다.
웹 애플리케이션 ID	uint32	해당하는 경우 탐지된 웹 애플리케이션의 내부 ID 번호입니다.
클라이언트 애플리케이션 ID	uint32	해당하는 경우 탐지된 클라이언트 애플리케이션의 내부 ID 번호입니다.
작업	uint8	파일 유형을 기반으로 파일에 조취를 취합니다. 다음과 같은 값을 사용할 수 있습니다. • 1 - 탐지 • 2 - 차단 • 3 - 악성코드 클라우드 조회 • 4 - 악성코드 차단 • 5 - 악성코드 화이트리스트 추가
프로토콜	uint8	사용자가 지정한 IANA 프로토콜 번호입니다. 예를 들면 다음과 같습니다. • 1 - ICMP • 4 - IP • 6 - TCP • 17 - UDP 현재는 TCP만 설정 가능합니다.

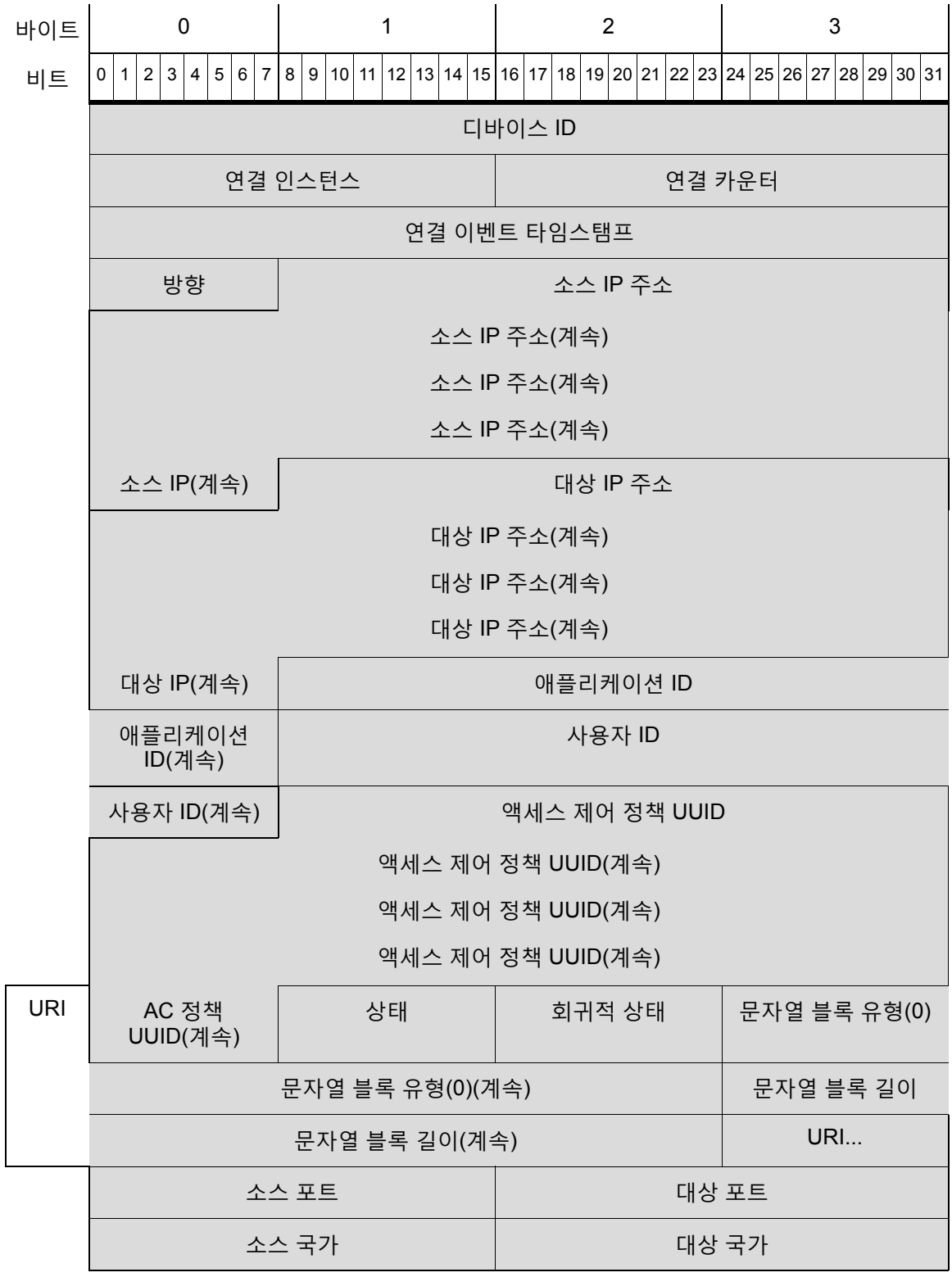
5.3 버전용 악성코드 이벤트 데이터 블록

eStreamer 서비스는 악성코드 이벤트 데이터 블록을 사용하여 악성코드 이벤트에 대한 정보를 저장합니다. 이러한 이벤트에는 클라우드 내에서 탐지 또는 격리된 악성코드, 탐지 방법, 악성코드의 영향을 받은 호스트 및 사용자에 대한 정보가 포함됩니다. 계열 2 블록 그룹에서 악성코드 이벤트 데이터 블록의 블록 유형은 35입니다. 이벤트 버전이 4이고 이벤트 코드가 101인 요청 메시지에서 악성코드 이벤트 플래그(Request Flags(요청 플래그) 필드의 비트 30)를 설정하여 악성코드 이벤트 레코드의 일부분으로 이벤트를 요청합니다.

다음 그림에 악성코드 이벤트 데이터 블록의 구조가 나와 있습니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
악성코드 이벤트 블록 유형(35)																																
악성코드 이벤트 블록 길이																																
에이전트 UUID																																
에이전트 UUID(계속)																																
에이전트 UUID(계속)																																
에이전트 UUID(계속)																																
클라우드 UUID																																
클라우드 UUID(계속)																																
클라우드 UUID(계속)																																
클라우드 UUID(계속)																																
악성코드 이벤트 타임스탬프																																
이벤트 유형 ID																																
이벤트 하위 유형 ID																																
탐지 이름	탐지기 ID								문자열 블록 유형(0)																							
	문자열 블록 유형(0)(계속)								문자열 블록 길이																							
	문자열 블록 길이(계속)								탐지 이름...																							

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
사용자	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	사용자...																															
파일 이름	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	파일 이름...																															
파일 경로	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	파일 경로...																															
파일 SHA 해시	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	파일 SHA 해시...																															
	파일 크기																															
	파일 유형																															
	파일 타임스탬프																															
상위 파일 이름	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	상위 파일 이름...																															
상위 파일 SHA 해시	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	상위 파일 SHA 해시...																															
이벤트 설명	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	이벤트 설명...																															


바이트
0
1
2
3
비트
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
디바이스 ID
연결 인스턴스
연결 카운터
연결 이벤트 타임스탬프
방향
소스 IP 주소
소스 IP 주소(계속)
소스 IP 주소(계속)
소스 IP 주소(계속)
소스 IP(계속)
대상 IP 주소
대상 IP 주소(계속)
대상 IP 주소(계속)
대상 IP 주소(계속)
대상 IP(계속)
애플리케이션 ID
애플리케이션 ID(계속)
사용자 ID
사용자 ID(계속)
액세스 제어 정책 UUID
액세스 제어 정책 UUID(계속)
액세스 제어 정책 UUID(계속)
액세스 제어 정책 UUID(계속)
URI
AC 정책 UUID(계속)
상태
회귀적 상태
문자열 블록 유형(0)
문자열 블록 유형(0)(계속)
문자열 블록 길이
문자열 블록 길이(계속)
URI...
소스 포트
대상 포트
소스 국가
대상 국가

다음 표에는 악성코드 이벤트 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 B-12 5.3 버전용 악성코드 이벤트 데이터 블록 필드

필드	데이터 유형	설명
악성코드 이벤트 블록 유형	uint32	악성코드 이벤트 데이터 블록을 시작합니다. 이 값은 항상 35입니다.
악성코드 이벤트 블록 길이	uint32	악성코드 이벤트 데이터 블록의 총 바이트 수입니다. 여기에는 악성코드 이벤트 블록 유형 및 길이 필드의 8바이트에 그 뒤의 데이터 바이트 수를 더한 값이 포함됩니다.
에이전트 UUID	uint8[16]	악성코드를 보고하는 AMP for Endpoints 에이전트의 내부 고유 ID입니다.
클라우드 UUID	uint8[16]	악성코드 이벤트가 시작된 악성코드 인식 네트워크의 내부 고유 ID입니다.
악성코드 이벤트 타임스탬프	uint32	악성코드 이벤트 생성 타임스탬프입니다.
이벤트 유형 ID	uint32	악성코드 이벤트 유형의 내부 ID입니다.
이벤트 하위 유형 ID	uint32	악성코드를 탐지하도록 유도한 작업의 내부 ID입니다.
탐지기 ID	uint8	악성코드를 탐지한 탐지 기술의 내부 ID입니다.
문자열 블록 유형	uint32	탐지 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	탐지 이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Detection Name(탐지 이름) 필드의 바이트 수를 더한 값이 포함됩니다.
탐지 이름	string	탐지 또는 격리된 악성코드의 이름입니다.
문자열 블록 유형	uint32	사용자 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	사용자 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 User(사용자) 필드의 바이트 수를 더한 값이 포함됩니다.
사용자	string	Cisco 에이전트가 설치되어 있으며 악성코드 이벤트가 발생한 컴퓨터의 사용자입니다. 이러한 사용자는 사용자 검색에 연결되지 않습니다.

표 B-12 5.3 버전용 악성코드 이벤트 데이터 블록 필드 (계속)

필드	데이터 유형	설명
문자열 블록 유형	uint32	파일 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	파일 이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 File Name(파일 이름) 필드의 바이트 수를 더한 값이 포함됩니다.
파일 이름	string	탐지 또는 격리된 파일의 이름입니다.
문자열 블록 유형	uint32	파일 경로가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	파일 경로 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 File Path(파일 경로) 필드의 바이트 수를 더한 값이 포함됩니다.
파일 경로	string	탐지 또는 격리된 파일의 파일 경로이며, 파일 이름은 포함되지 않습니다.
문자열 블록 유형	uint32	파일 SHA 해시가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	파일 SHA 해시 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 File SHA Hash(파일 SHA 해시) 필드의 바이트 수를 더한 값이 포함됩니다.
파일 SHA 해시	string	탐지 또는 격리된 파일의 SHA-256 해시 값이 렌더링된 문자열입니다.
파일 크기	uint32	탐지 또는 격리된 파일의 바이트 크기입니다.
파일 유형	uint8	탐지 또는 격리된 파일의 파일 유형입니다. 이 필드의 의미가 이 이벤트와 함께 메타데이터에 포함되어 전송됩니다. 자세한 정보는 AMP for Endpoints 파일 유형 메타데이터, 페이지 3-42의 내용을 참조하십시오.
파일 타임스탬프	uint32	탐지 또는 격리된 파일이 생성된 UNIX 타임스탬프(1970년 1월 1일 이후의 초 단위 시간)입니다.
문자열 블록 유형	uint32	상위 파일 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	상위 파일 이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Parent File Name(상위 파일 이름) 필드의 바이트 수를 더한 값이 포함됩니다.
상위 파일 이름	string	탐지가 발생했을 때 탐지 또는 격리된 파일에 액세스한 파일의 이름입니다.
문자열 블록 유형	uint32	상위 파일 SHA 해시가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.

표 B-12 5.3 버전용 악성코드 이벤트 데이터 블록 필드 (계속)

필드	데이터 유형	설명
문자열 블록 길이	uint32	상위 파일 SHA 해시 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Parent File SHA Hash(상위 파일 SHA 해시) 필드의 바이트 수를 더한 값이 포함됩니다.
상위 파일 SHA 해시	string	탐지가 발생했을 때 탐지 또는 격리된 파일에 액세스한 상위 파일의 SHA-256 해시 값입니다.
문자열 블록 유형	uint32	이벤트 설명이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	이벤트 설명 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Event Description(이벤트 설명) 필드의 바이트 수를 더한 값이 포함됩니다.
이벤트 설명	string	이벤트 유형과 관련된 추가 이벤트 정보입니다.
디바이스 ID	uint32	이벤트를 생성한 디바이스의 ID입니다.
연결 인스턴스	uint16	이벤트를 생성한 디바이스의 Snort 인스턴스입니다. 이벤트를 연결 또는 IDS 이벤트와 연결하는 데 사용됩니다.
연결 카운터	uint16	1초 이내에 발생하는 연결 이벤트를 구별하는 데 사용되는 값입니다.
연결 이벤트 타임스탬프	uint32	연결 이벤트의 타임스탬프입니다.
방향	uint8	파일이 업로드되었는지 아니면 다운로드되었는지를 나타냅니다. 다음과 같은 값을 사용할 수 있습니다. • 1 - 다운로드 • 2 - 업로드 현재 이 값은 프로토콜에 따라 달라집니다(예: 연결이 HTTP인 경우 다운로드임).
소스 IP 주소	uint8[16]	연결 소스의 IPv4 또는 IPv6 주소입니다.
대상 IP 주소	uint8[16]	연결 대상의 IPv4 또는 IPv6 주소입니다.
애플리케이션 ID	uint32	파일 전송을 사용하여 애플리케이션에 매핑되는 ID 번호입니다.
사용자 ID	uint32	시스템이 식별한 대상 호스트에 로그인하는 사용자의 ID 번호입니다.
액세스 제어 정책 UUID	uint8[16]	이벤트를 트리거한 액세스 제어 정책의 고유 식별자 역할을 하는 ID 번호입니다.

표 B-12 5.3 버전용 악성코드 이벤트 데이터 블록 필드 (계속)

필드	데이터 유형	설명
상태	uint8	파일의 악성코드 상태입니다. 가능한 값은 다음과 같습니다. • 1 - CLEAN - 파일이 정상 상태이며 악성코드가 포함되어 있지 않습니다. • 2 - UNKNOWN - 파일에 악성코드가 포함되어 있는지 알 수 없습니다. • 3 - MALWARE - 파일에 악성코드가 포함되어 있습니다. • 4 - UNAVAILABLE - 소프트웨어가 Cisco 클라우드에 상태 요청을 보낼 수 없거나 Cisco 클라우드 서비스가 요청에 응답하지 않았습니다. • 5 - CUSTOM SIGNATURE - 파일이 사용자가 정의한 해시와 일치하며 사용자가 지정한 방식으로 처리됩니다.
회귀적 상태	uint8	상태가 업데이트된 경우 파일의 상태입니다. 상태가 업데이트되지 않은 경우 이 필드에는 Disposition(상태) 필드와 동일한 값이 포함됩니다. 가능한 값은 Disposition(상태) 필드와 동일합니다.
문자열 블록 유형	uint32	URI가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	URI 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 URI 필드의 바이트 수를 더한 값이 포함됩니다.
URI	string	연결의 URI입니다.
소스 포트	uint16	연결 소스의 포트 번호입니다.
대상 포트	uint16	연결 대상의 포트 번호입니다.
소스 국가	uint16	소스 호스트의 국가 코드입니다.
대상 국가	uint16	대상 호스트의 국가 코드입니다.
웹 애플리케이션 ID	uint32	해당하는 경우 탐지된 웹 애플리케이션의 내부 ID 번호입니다.
클라이언트 애플리케이션 ID	uint32	해당하는 경우 탐지된 클라이언트 애플리케이션의 내부 ID 번호입니다.
작업	uint8	파일 유형을 기반으로 파일에 조취를 취합니다. 다음과 같은 값을 사용할 수 있습니다. • 1 - 탐지 • 2 - 차단 • 3 - 악성코드 클라우드 조회 • 4 - 악성코드 차단 • 5 - 악성코드 화이트리스트 추가

표 B-12 5.3 버전용 악성코드 이벤트 데이터 블록 필드 (계속)

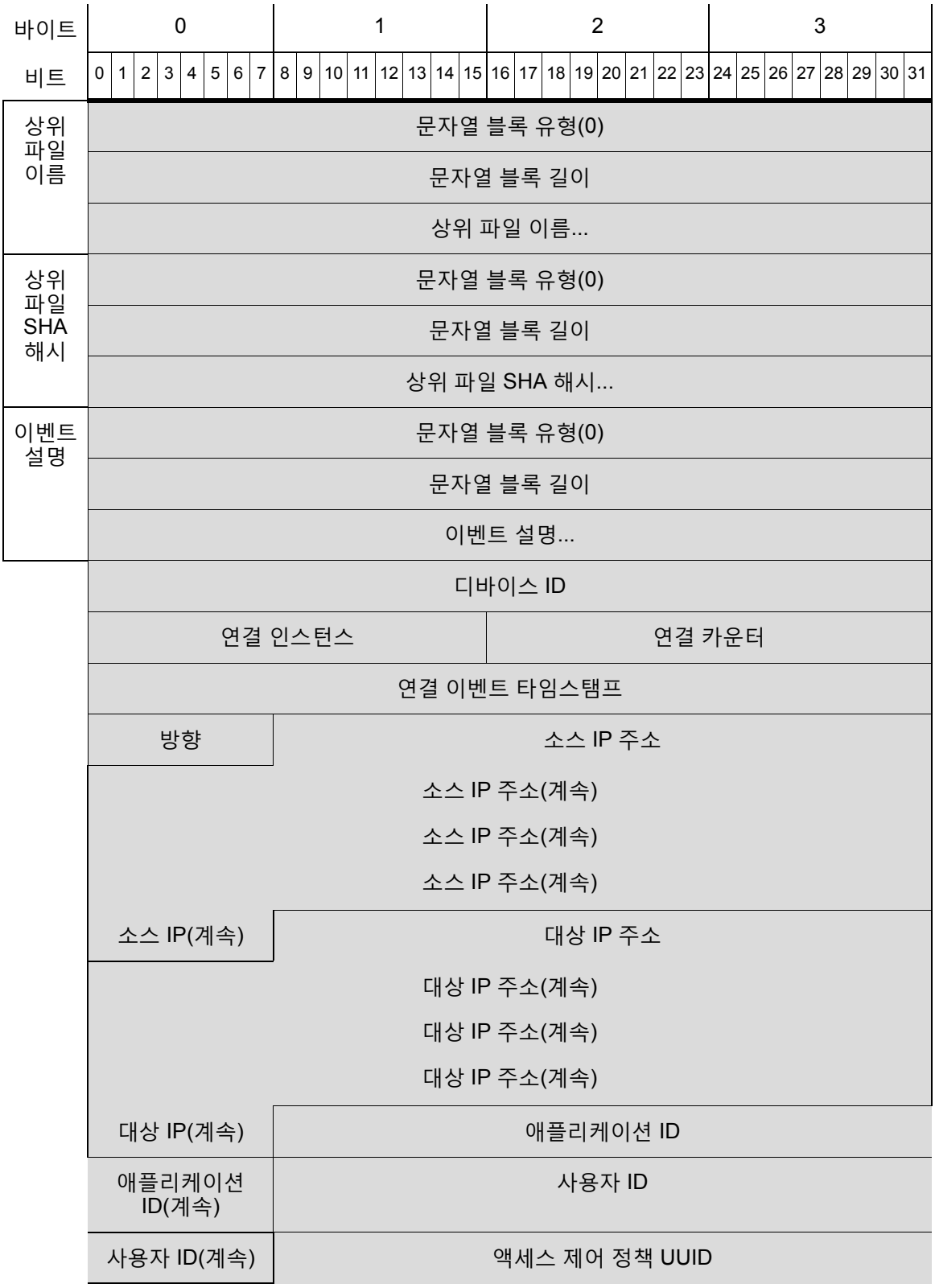
필드	데이터 유형	설명
프로토콜	uint8	사용자가 지정한 IANA 프로토콜 번호입니다. 예를 들면 다음과 같습니다. • 1 - ICMP • 4 - IP • 6 - TCP • 17 - UDP 현재는 TCP만 설정 가능합니다.
위협 점수	uint8	동적 분석 과정에서 관찰된 잠재적으로 악의적인 동작을 기준으로 한 0부터 100까지의 숫자 값입니다.
IOC 번호	uint16	이 이벤트와 관련된 보안 침해의 ID 번호입니다.

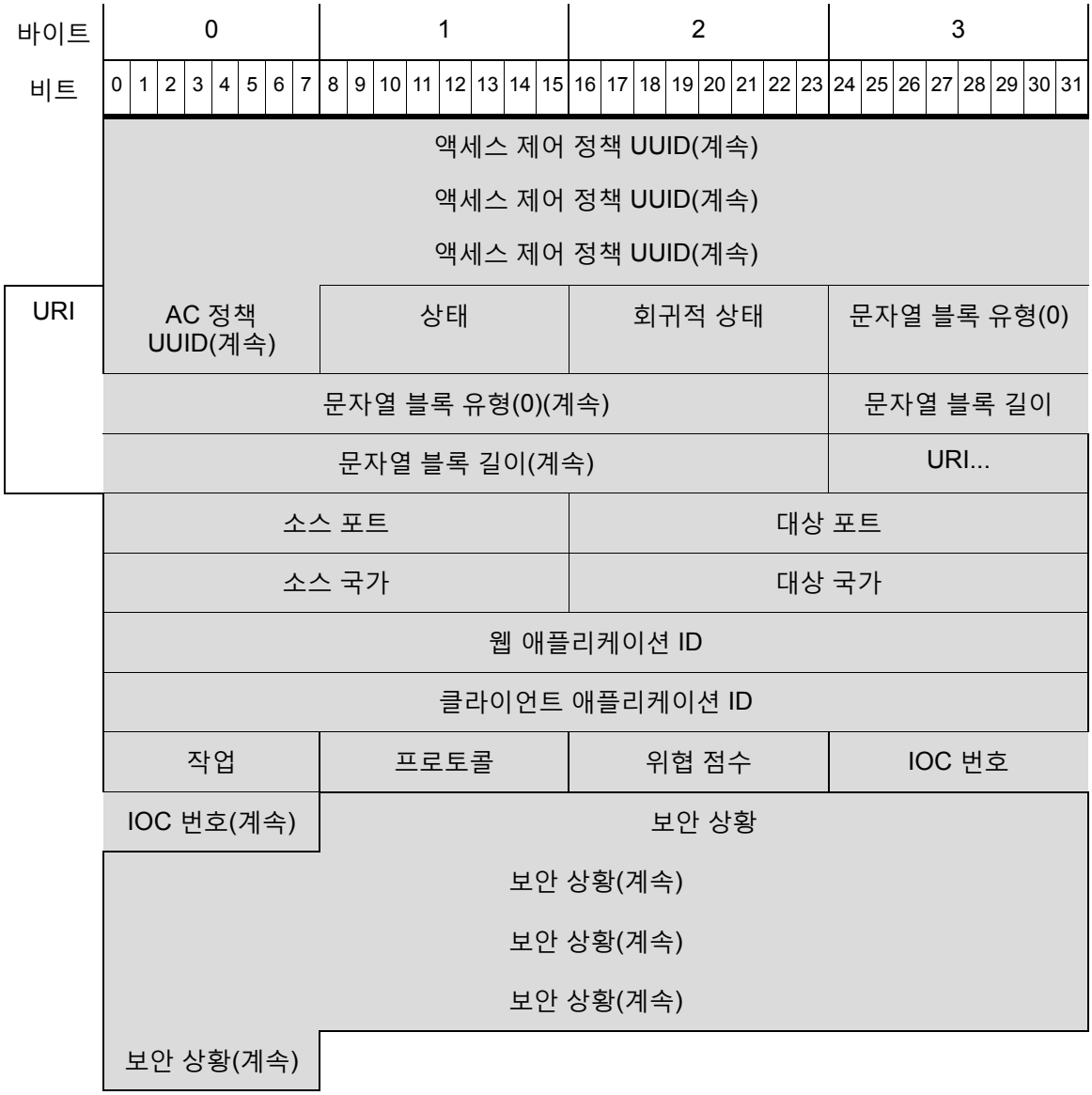
5.3.1 버전용 악성코드 이벤트 데이터 블록

eStreamer 서비스는 악성코드 이벤트 데이터 블록을 사용하여 악성코드 이벤트에 대한 정보를 저장합니다. 이러한 이벤트에는 클라우드 내에서 탐지 또는 격리된 악성코드, 탐지 방법, 악성코드의 영향을 받은 호스트 및 사용자에 대한 정보가 포함됩니다. 계열 2 블록 그룹에서 악성코드 이벤트 데이터 블록의 블록 유형은 44입니다. 이는 블록 35를 대체합니다. 이벤트 버전이 5이고 이벤트 코드가 101인 요청 메시지에서 악성코드 이벤트 플래그(Request Flags(요청 플래그) 필드의 비트 30)를 설정하여 악성코드 이벤트 레코드의 일부분으로 이벤트를 요청합니다.

다음 그림에 악성코드 이벤트 데이터 블록의 구조가 나와 있습니다.


바이트
0
1
2
3
비트
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
악성코드 이벤트 타임스탬프
이벤트 유형 ID
이벤트 하위 유형 ID
탐지 이름
탐지기 ID
문자열 블록 유형(0)
문자열 블록 유형(0)(계속)
문자열 블록 길이
문자열 블록 길이(계속)
탐지 이름...
사용자
문자열 블록 유형(0)
문자열 블록 길이
사용자...
파일 이름
문자열 블록 유형(0)
문자열 블록 길이
파일 이름...
파일 경로
문자열 블록 유형(0)
문자열 블록 길이
파일 경로...
파일 SHA 해시
문자열 블록 유형(0)
문자열 블록 길이
파일 SHA 해시...
파일 크기
파일 유형
파일 타임스탬프


바이트
0
1
2
3
비트
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
상위 파일 이름
문자열 블록 유형(0)
문자열 블록 길이
상위 파일 이름...
상위 파일 SHA 해시
문자열 블록 유형(0)
문자열 블록 길이
상위 파일 SHA 해시...
이벤트 설명
문자열 블록 유형(0)
문자열 블록 길이
이벤트 설명...
디바이스 ID
연결 인스턴스
연결 카운터
연결 이벤트 타임스탬프
방향
소스 IP 주소
소스 IP 주소(계속)
소스 IP 주소(계속)
소스 IP 주소(계속)
소스 IP(계속)
대상 IP 주소
대상 IP 주소(계속)
대상 IP 주소(계속)
대상 IP 주소(계속)
대상 IP(계속)
애플리케이션 ID
애플리케이션 ID(계속)
사용자 ID
사용자 ID(계속)
액세스 제어 정책 UUID



다음 표에는 악성코드 이벤트 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 B-13 5.3.1 버전용 악성코드 이벤트 데이터 블록 필드

필드	데이터 유형	설명
악성코드 이벤트 블록 유형	uint32	악성코드 이벤트 데이터 블록을 시작합니다. 이 값은 항상 44입니다.
악성코드 이벤트 블록 길이	uint32	악성코드 이벤트 데이터 블록의 총 바이트 수입니다. 여기에는 악성코드 이벤트 블록 유형 및 길이 필드의 8바이트에 그 뒤의 데이터 바이트 수를 더한 값이 포함됩니다.
에이전트 UUID	uint8[16]	악성코드를 보고하는 AMP for Endpoints 에이전트의 내부 고유 ID입니다.
클라우드 UUID	uint8[16]	악성코드 이벤트가 시작된 Cisco Advanced Malware Protection 클라우드의 내부 고유 ID입니다.

표 B-13 5.3.1 버전용 악성코드 이벤트 데이터 블록 필드 (계속)

필드	데이터 유형	설명
악성코드 이벤트 타임스탬프	uint32	악성코드 이벤트 생성 타임스탬프입니다.
이벤트 유형 ID	uint32	악성코드 이벤트 유형의 내부 ID입니다.
이벤트 하위 유형 ID	uint32	악성코드를 탐지하도록 유도한 작업의 내부 ID입니다.
탐지기 ID	uint8	악성코드를 탐지한 탐지 기술의 내부 ID입니다.
문자열 블록 유형	uint32	탐지 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	탐지 이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Detection Name(탐지 이름) 필드의 바이트 수를 더한 값이 포함됩니다.
탐지 이름	string	탐지 또는 격리된 악성코드의 이름입니다.
문자열 블록 유형	uint32	사용자 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	사용자 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 User(사용자) 필드의 바이트 수를 더한 값이 포함됩니다.
사용자	string	Cisco 에이전트가 설치되어 있으며 악성코드 이벤트가 발생한 컴퓨터의 사용자입니다. 이러한 사용자는 사용자 검색에 연결되지 않습니다.
문자열 블록 유형	uint32	파일 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	파일 이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 File Name(파일 이름) 필드의 바이트 수를 더한 값이 포함됩니다.
파일 이름	string	탐지 또는 격리된 파일의 이름입니다.
문자열 블록 유형	uint32	파일 경로가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	파일 경로 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 File Path(파일 경로) 필드의 바이트 수를 더한 값이 포함됩니다.
파일 경로	string	탐지 또는 격리된 파일의 파일 경로이며, 파일 이름은 포함되지 않습니다.
문자열 블록 유형	uint32	파일 SHA 해시가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	파일 SHA 해시 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 File SHA Hash(파일 SHA 해시) 필드의 바이트 수를 더한 값이 포함됩니다.
파일 SHA 해시	string	탐지 또는 격리된 파일의 SHA-256 해시 값이 렌더링된 문자열입니다.

표 B-13 5.3.1 버전용 악성코드 이벤트 데이터 블록 필드 (계속)

필드	데이터 유형	설명
파일 크기	uint32	탐지 또는 격리된 파일의 바이트 크기입니다.
파일 유형	uint8	탐지 또는 격리된 파일의 파일 유형입니다. 이 필드의 의미가 이 이벤트와 함께 메타데이터에 포함되어 전송됩니다. 자세한 정보는 AMP for Endpoints 파일 유형 메타데이터, 페이지 3-42의 내용을 참조하십시오.
파일 타임스탬프	uint32	탐지 또는 격리된 파일이 생성된 UNIX 타임스탬프(1970년 1월 1일 이후의 초 단위 시간)입니다.
문자열 블록 유형	uint32	상위 파일 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	상위 파일 이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Parent File Name(상위 파일 이름) 필드의 바이트 수를 더한 값이 포함됩니다.
상위 파일 이름	string	탐지가 발생했을 때 탐지 또는 격리된 파일에 액세스한 파일의 이름입니다.
문자열 블록 유형	uint32	상위 파일 SHA 해시가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	상위 파일 SHA 해시 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Parent File SHA Hash(상위 파일 SHA 해시) 필드의 바이트 수를 더한 값이 포함됩니다.
상위 파일 SHA 해시	string	탐지가 발생했을 때 탐지 또는 격리된 파일에 액세스한 상위 파일의 SHA-256 해시 값입니다.
문자열 블록 유형	uint32	이벤트 설명이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	이벤트 설명 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Event Description(이벤트 설명) 필드의 바이트 수를 더한 값이 포함됩니다.
이벤트 설명	string	이벤트 유형과 관련된 추가 이벤트 정보입니다.
디바이스 ID	uint32	이벤트를 생성한 디바이스의 ID입니다.
연결 인스턴스	uint16	이벤트를 생성한 디바이스의 Snort 인스턴스입니다. 이벤트를 연결 또는 IDS 이벤트와 연결하는 데 사용됩니다.
연결 카운터	uint16	1초 이내에 발생하는 연결 이벤트를 구별하는 데 사용되는 값입니다.
연결 이벤트 타임스탬프	uint32	연결 이벤트의 타임스탬프입니다.

표 B-13 5.3.1 버전용 악성코드 이벤트 데이터 블록 필드 (계속)

필드	데이터 유형	설명
방향	uint8	파일이 업로드되었는지 아니면 다운로드되었는지를 나타냅니다. 다음과 같은 값을 사용할 수 있습니다. • 1 - 다운로드 • 2 - 업로드 현재 이 값은 프로토콜에 따라 달라집니다(예: 연결이 HTTP인 경우 다운로드임).
소스 IP 주소	uint8[16]	연결 소스의 IPv4 또는 IPv6 주소입니다.
대상 IP 주소	uint8[16]	연결 대상의 IPv4 또는 IPv6 주소입니다.
애플리케이션 ID	uint32	파일 전송을 사용하여 애플리케이션에 매핑되는 ID 번호입니다.
사용자 ID	uint32	시스템이 식별한 대상 호스트에 로그인하는 사용자의 ID 번호입니다.
액세스 제어 정책 UUID	uint8[16]	이벤트를 트리거한 액세스 제어 정책의 고유 식별자 역할을 하는 ID 번호입니다.
상태	uint8	파일의 악성코드 상태입니다. 가능한 값은 다음과 같습니다. • 1 - CLEAN - 파일이 정상 상태이며 악성코드가 포함되어 있지 않습니다. • 2 - UNKNOWN - 파일에 악성코드가 포함되어 있는지 알 수 없습니다. • 3 - MALWARE - 파일에 악성코드가 포함되어 있습니다. • 4 - UNAVAILABLE - 소프트웨어가 Cisco 클라우드에 상태 요청을 보낼 수 없거나 Cisco 클라우드 서비스가 요청에 응답하지 않았습니다. • 5 - CUSTOM SIGNATURE - 파일이 사용자가 정의한 해시와 일치하며 사용자가 지정한 방식으로 처리됩니다.
회귀적 상태	uint8	상태가 업데이트된 경우 파일의 상태입니다. 상태가 업데이트되지 않은 경우 이 필드에는 Disposition(상태) 필드와 동일한 값이 포함됩니다. 가능한 값은 Disposition(상태) 필드와 동일합니다.
문자열 블록 유형	uint32	URI가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	URI 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 URI 필드의 바이트 수를 더한 값이 포함됩니다.
URI	string	연결의 URI입니다.
소스 포트	uint16	연결 소스의 포트 번호입니다.
대상 포트	uint16	연결 대상의 포트 번호입니다.
소스 국가	uint16	소스 호스트의 국가 코드입니다.

표 B-13 5.3.1 버전용 악성코드 이벤트 데이터 블록 필드 (계속)

필드	데이터 유형	설명
대상 국가	uint16	대상 호스트의 국가 코드입니다.
웹 애플리케이션 ID	uint32	해당하는 경우 탐지된 웹 애플리케이션의 내부 ID 번호입니다.
클라이언트 애플리케이션 ID	uint32	해당하는 경우 탐지된 클라이언트 애플리케이션의 내부 ID 번호입니다.
작업	uint8	파일 유형을 기반으로 파일에 조취를 취합니다. 다음과 같은 값을 사용할 수 있습니다. • 1 - 탐지 • 2 - 차단 • 3 - 악성코드 클라우드 조회 • 4 - 악성코드 차단 • 5 - 악성코드 화이트리스트 추가
프로토콜	uint8	사용자가 지정한 IANA 프로토콜 번호입니다. 예를 들면 다음과 같습니다. • 1 - ICMP • 4 - IP • 6 - TCP • 17 - UDP 현재는 TCP만 설정 가능합니다.
위협 점수	uint8	동적 분석 과정에서 관찰된 잠재적으로 악의적인 동작을 기준으로 한 0부터 100까지의 숫자 값입니다.
IOC 번호	uint16	이 이벤트와 관련된 보안 침해의 ID 번호입니다.
보안 상황	uint8(16)	트래픽이 통과한 보안 상황(가상 방화벽)의 ID 번호입니다. 이 필드는 다중 컨텍스트 모드의 ASA FirePOWER 디바이스에 대해서만 채워집니다.

5.4.x 버전용 악성코드 이벤트 데이터 블록

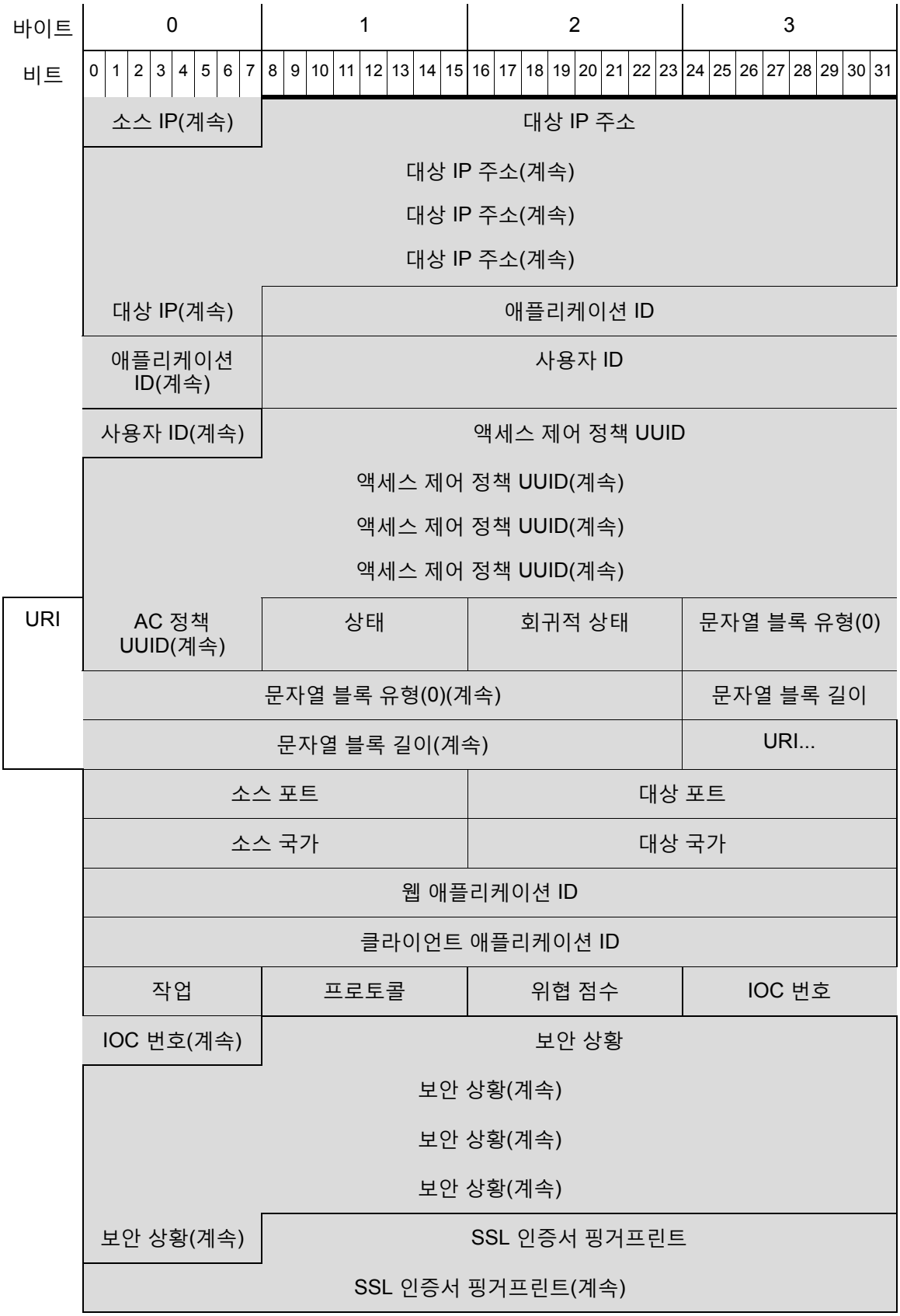
eStreamer 서비스는 악성코드 이벤트 데이터 블록을 사용하여 악성코드 이벤트에 대한 정보를 저장합니다. 이러한 이벤트에는 클라우드 내에서 탐지 또는 격리된 악성코드, 탐지 방법, 악성코드의 영향을 받은 호스트 및 사용자에 대한 정보가 포함됩니다. 계열 2 블록 그룹에서 악성코드 이벤트 데이터 블록의 블록 유형은 47입니다. 이는 블록 유형 44를 대체하며 블록 유형 62로 대체됩니다. SSL 및 파일 아카이브 지원용 필드가 추가되었습니다.

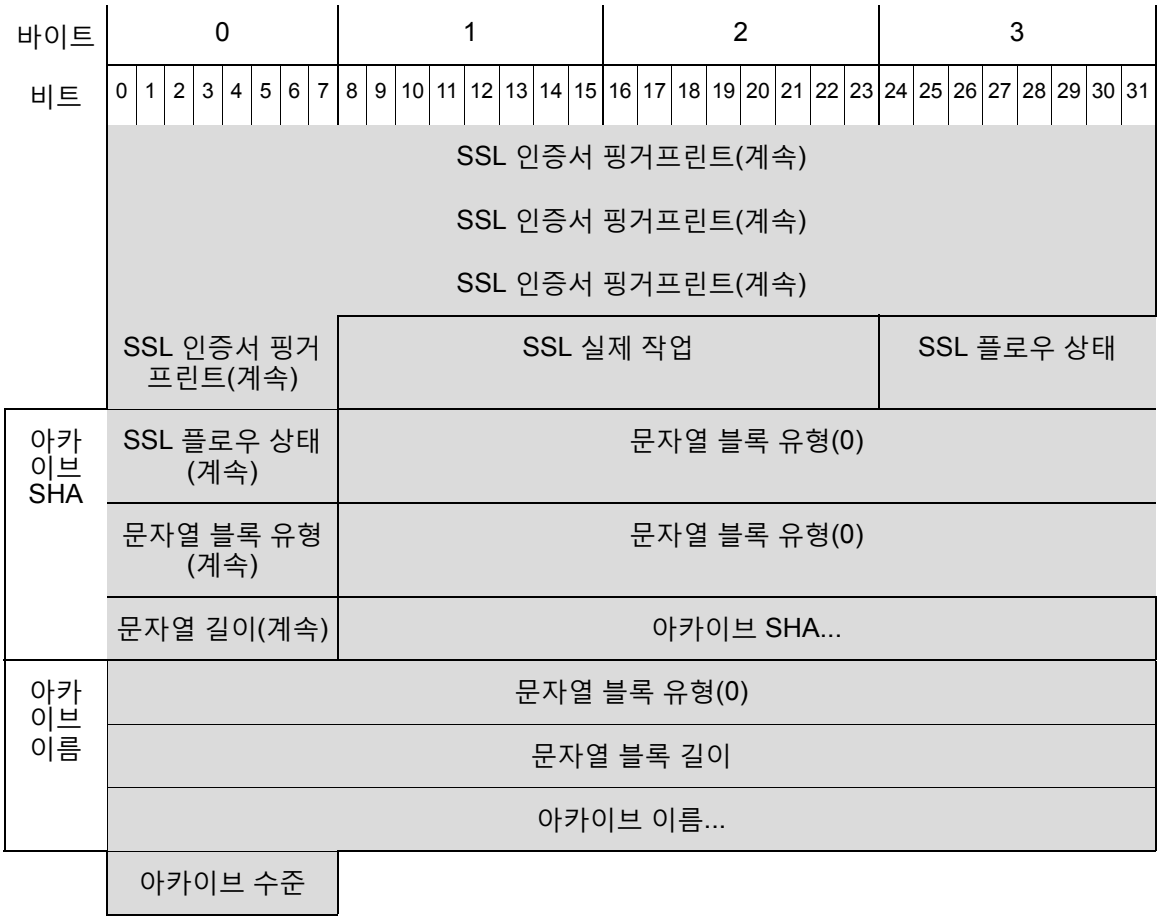
이벤트 버전이 6이고 이벤트 코드가 101인 요청 메시지에서 악성코드 이벤트 플래그(Request Flags(요청 플래그) 필드의 비트 30)를 설정하여 악성코드 이벤트 레코드의 일부분으로 이벤트를 요청합니다.

다음 그림에 악성코드 이벤트 데이터 블록의 구조가 나와 있습니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
악성코드 이벤트 블록 유형(47)																																
악성코드 이벤트 블록 길이																																
에이전트 UUID																																
에이전트 UUID(계속)																																
에이전트 UUID(계속)																																
에이전트 UUID(계속)																																
클라우드 UUID																																
클라우드 UUID(계속)																																
클라우드 UUID(계속)																																
클라우드 UUID(계속)																																
악성코드 이벤트 타임스탬프																																
이벤트 유형 ID																																
이벤트 하위 유형 ID																																
탐지 이름	탐지기 ID								문자열 블록 유형(0)																							
	문자열 블록 유형(0)(계속)								문자열 블록 길이																							
	문자열 블록 길이(계속)								탐지 이름...																							
사용자	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	사용자...																															
파일 이름	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	파일 이름...																															


바이트
0
1
2
3
비트
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
파일 경로
문자열 블록 유형(0)
문자열 블록 길이
파일 경로...
파일 SHA 해시
문자열 블록 유형(0)
문자열 블록 길이
파일 SHA 해시...
파일 크기
파일 유형
파일 타임스탬프
상위 파일 이름
문자열 블록 유형(0)
문자열 블록 길이
상위 파일 이름...
상위 파일 SHA 해시
문자열 블록 유형(0)
문자열 블록 길이
상위 파일 SHA 해시...
이벤트 설명
문자열 블록 유형(0)
문자열 블록 길이
이벤트 설명...
디바이스 ID
연결 인스턴스
연결 카운터
연결 이벤트 타임스탬프
방향
소스 IP 주소
소스 IP 주소(계속)
소스 IP 주소(계속)
소스 IP 주소(계속)


바이트
0
1
2
3
비트
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
소스 IP(계속)
대상 IP 주소
대상 IP 주소(계속)
대상 IP 주소(계속)
대상 IP 주소(계속)
대상 IP(계속)
애플리케이션 ID
애플리케이션 ID(계속)
사용자 ID
사용자 ID(계속)
액세스 제어 정책 UUID
액세스 제어 정책 UUID(계속)
액세스 제어 정책 UUID(계속)
액세스 제어 정책 UUID(계속)
URI
AC 정책 UUID(계속)
상태
회귀적 상태
문자열 블록 유형(0)
문자열 블록 유형(0)(계속)
문자열 블록 길이
문자열 블록 길이(계속)
URI...
소스 포트
대상 포트
소스 국가
대상 국가
웹 애플리케이션 ID
클라이언트 애플리케이션 ID
작업
프로토콜
위협 점수
IOC 번호
IOC 번호(계속)
보안 상황
보안 상황(계속)
보안 상황(계속)
보안 상황(계속)
보안 상황(계속)
SSL 인증서 핑거프린트
SSL 인증서 핑거프린트(계속)



다음 표에는 악성코드 이벤트 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 B-14 5.4.x 버전용 악성코드 이벤트 데이터 블록 필드

필드	데이터 유형	설명
악성코드 이벤트 블록 유형	uint32	악성코드 이벤트 데이터 블록을 시작합니다. 이 값은 항상 47입니다.
악성코드 이벤트 블록 길이	uint32	악성코드 이벤트 데이터 블록의 총 바이트 수입니다. 여기에는 악성코드 이벤트 블록 유형 및 길이 필드의 8바이트에 그 뒤의 데이터 바이트 수를 더한 값이 포함됩니다.
에이전트 UUID	uint8[16]	악성코드를 보고하는 AMP for Endpoints 에이전트의 내부 고유 ID입니다.
클라우드 UUID	uint8[16]	악성코드 이벤트가 시작된 Cisco Advanced Malware Protection 클라우드의 내부 고유 ID입니다.
악성코드 이벤트 타임스탬프	uint32	악성코드 이벤트 생성 타임스탬프입니다.
이벤트 유형 ID	uint32	악성코드 이벤트 유형의 내부 ID입니다.
이벤트 하위 유형 ID	uint32	악성코드를 탐지하도록 유도한 작업의 내부 ID입니다.
탐지기 ID	uint8	악성코드를 탐지한 탐지 기술의 내부 ID입니다.

표 B-14 5.4.x 버전용 악성코드 이벤트 데이터 블록 필드 (계속)

필드	데이터 유형	설명
문자열 블록 유형	uint32	탐지 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	탐지 이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Detection Name(탐지 이름) 필드의 바이트 수를 더한 값이 포함됩니다.
탐지 이름	string	탐지 또는 격리된 악성코드의 이름입니다.
문자열 블록 유형	uint32	사용자 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	사용자 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 User(사용자) 필드의 바이트 수를 더한 값이 포함됩니다.
사용자	string	Cisco 에이전트가 설치되어 있으며 악성코드 이벤트가 발생한 컴퓨터의 사용자입니다. 이러한 사용자는 사용자 검색에 연결되지 않습니다.
문자열 블록 유형	uint32	파일 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	파일 이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 File Name(파일 이름) 필드의 바이트 수를 더한 값이 포함됩니다.
파일 이름	string	탐지 또는 격리된 파일의 이름입니다.
문자열 블록 유형	uint32	파일 경로가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	파일 경로 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 File Path(파일 경로) 필드의 바이트 수를 더한 값이 포함됩니다.
파일 경로	string	탐지 또는 격리된 파일의 파일 경로이며, 파일 이름은 포함되지 않습니다.
문자열 블록 유형	uint32	파일 SHA 해시가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	파일 SHA 해시 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 File SHA Hash(파일 SHA 해시) 필드의 바이트 수를 더한 값이 포함됩니다.
파일 SHA 해시	string	탐지 또는 격리된 파일의 SHA-256 해시 값이 렌더링된 문자열입니다.
파일 크기	uint32	탐지 또는 격리된 파일의 바이트 크기입니다.
파일 유형	uint8	탐지 또는 격리된 파일의 파일 유형입니다. 이 필드의 의미가 이 이벤트와 함께 메타데이터에 포함되어 전송됩니다. 자세한 정보는 AMP for Endpoints 파일 유형 메타데이터, 페이지 3-42의 내용을 참조하십시오.

표 B-14 5.4.x 버전용 악성코드 이벤트 데이터 블록 필드 (계속)

필드	데이터 유형	설명
파일 타임스탬프	uint32	탐지 또는 격리된 파일이 생성된 UNIX 타임스탬프(1970년 1월 1일 이후의 초 단위 시간)입니다.
문자열 블록 유형	uint32	상위 파일 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	상위 파일 이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Parent File Name(상위 파일 이름) 필드의 바이트 수를 더한 값이 포함됩니다.
상위 파일 이름	string	탐지가 발생했을 때 탐지 또는 격리된 파일에 액세스한 파일의 이름입니다.
문자열 블록 유형	uint32	상위 파일 SHA 해시가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	상위 파일 SHA 해시 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Parent File SHA Hash(상위 파일 SHA 해시) 필드의 바이트 수를 더한 값이 포함됩니다.
상위 파일 SHA 해시	string	탐지가 발생했을 때 탐지 또는 격리된 파일에 액세스한 상위 파일의 SHA-256 해시 값입니다.
문자열 블록 유형	uint32	이벤트 설명이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	이벤트 설명 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Event Description(이벤트 설명) 필드의 바이트 수를 더한 값이 포함됩니다.
이벤트 설명	string	이벤트 유형과 관련된 추가 이벤트 정보입니다.
디바이스 ID	uint32	이벤트를 생성한 디바이스의 ID입니다.
연결 인스턴스	uint16	이벤트를 생성한 디바이스의 Snort 인스턴스입니다. 이벤트를 연결 또는 IDS 이벤트와 연결하는 데 사용됩니다.
연결 카운터	uint16	1초 이내에 발생하는 연결 이벤트를 구별하는 데 사용되는 값입니다.
연결 이벤트 타임스탬프	uint32	연결 이벤트의 타임스탬프입니다.
방향	uint8	파일이 업로드되었는지 아니면 다운로드되었는지를 나타냅니다. 다음과 같은 값을 사용할 수 있습니다. • 1 - 다운로드 • 2 - 업로드 현재 이 값은 프로토콜에 따라 달라집니다(예: 연결이 HTTP인 경우 다운로드임).
소스 IP 주소	uint8[16]	연결 소스의 IPv4 또는 IPv6 주소입니다.
대상 IP 주소	uint8[16]	연결 대상의 IPv4 또는 IPv6 주소입니다.
애플리케이션 ID	uint32	파일 전송을 사용하여 애플리케이션에 매핑되는 ID 번호입니다.

표 B-14 5.4.x 버전용 악성코드 이벤트 데이터 블록 필드 (계속)

필드	데이터 유형	설명
사용자 ID	uint32	시스템이 식별한 대상 호스트에 로그인하는 사용자의 ID 번호입니다.
액세스 제어 정책 UUID	uint8[16]	이벤트를 트리거한 액세스 제어 정책의 고유 식별자 역할을 하는 ID 번호입니다.
상태	uint8	파일의 악성코드 상태입니다. 가능한 값은 다음과 같습니다. • 1 - CLEAN - 파일이 정상 상태이며 악성코드가 포함되어 있지 않습니다. • 2 - UNKNOWN - 파일에 악성코드가 포함되어 있는지 알 수 없습니다. • 3 - MALWARE - 파일에 악성코드가 포함되어 있습니다. • 4 - UNAVAILABLE - 소프트웨어가 Cisco 클라우드에 상태 요청을 보낼 수 없거나 Cisco 클라우드 서비스가 요청에 응답하지 않았습니다. • 5 - CUSTOM SIGNATURE - 파일이 사용자가 정의한 해시와 일치하며 사용자가 지정한 방식으로 처리됩니다.
회귀적 상태	uint8	상태가 업데이트된 경우 파일의 상태입니다. 상태가 업데이트되지 않은 경우 이 필드에는 Disposition(상태) 필드와 동일한 값이 포함됩니다. 가능한 값은 Disposition(상태) 필드와 동일합니다.
문자열 블록 유형	uint32	URI가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	URI 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 URI 필드의 바이트 수를 더한 값이 포함됩니다.
URI	string	연결의 URI입니다.
소스 포트	uint16	연결 소스의 포트 번호입니다.
대상 포트	uint16	연결 대상의 포트 번호입니다.
소스 국가	uint16	소스 호스트의 국가 코드입니다.
대상 국가	uint16	대상 호스트의 국가 코드입니다.
웹 애플리케이션 ID	uint32	해당하는 경우 탐지된 웹 애플리케이션의 내부 ID 번호입니다.
클라이언트 애플리케이션 ID	uint32	해당하는 경우 탐지된 클라이언트 애플리케이션의 내부 ID 번호입니다.

표 B-14 5.4.x 버전용 악성코드 이벤트 데이터 블록 필드 (계속)

필드	데이터 유형	설명
작업	uint8	파일 유형을 기반으로 파일에 조취를 취합니다. 다음과 같은 값을 사용할 수 있습니다. • 1 - 탐지 • 2 - 차단 • 3 - 악성코드 클라우드 조회 • 4 - 악성코드 차단 • 5 - 악성코드 화이트리스트 추가 • 6 - 클라우드 조회 시간 초과 • 7 - 맞춤형 탐지 • 8 - 맞춤형 탐지 차단 • 9 - 아카이브 차단(수준 초과됨) • 10 - 아카이브 차단(암호화됨) • 11 - 아카이브 차단(검사하지 못함)
프로토콜	uint8	사용자가 지정한 IANA 프로토콜 번호입니다. 예를 들면 다음과 같습니다. • 1 - ICMP • 4 - IP • 6 - TCP • 17 - UDP 현재는 TCP만 설정 가능합니다.
위협 점수	uint8	동적 분석 과정에서 관찰된 잠재적으로 악의적인 동작을 기준으로 한 0부터 100까지의 숫자 값입니다.
IOC 번호	uint16	이 이벤트와 관련된 보안 침해의 ID 번호입니다.
보안 상황	uint8(16)	트래픽이 통과한 보안 상황(가상 방화벽)의 ID 번호입니다. 이 필드는 다중 컨텍스트 모드의 ASA FirePOWER 디바이스에 대해서만 채워집니다.
SSL 인증서 핑거프린트	uint8[20]	SSL 서버 인증서의 SHA1 해시입니다.
SSL 실제 작업	uint16	SSL 규칙에 기반한 연결에서 수행된 작업입니다. 규칙에 명시된 작업이 가능하지 않을 수도 있으므로, 이는 예상 작업과 다를 수 있습니다. 가능한 값은 다음과 같습니다. • 0 - '알 수 없음' • 1 - '암호 해독 안 함' • 2 - '차단' • 3 - '차단 및 재설정' • 4 - '암호 해독(알려진 키)' • 5 - '암호 해독(키 교체)' • 6 - '암호 해독(재서명)'

표 B-14 5.4.x 버전용 악성코드 이벤트 데이터 블록 필드 (계속)

필드	데이터 유형	설명
SSL 플로우 상태	uint16	SSL 플로우의 상태입니다. 이 값은 작업을 수행한 이유 또는 오류 메시지가 표시된 이유를 설명합니다. 가능한 값은 다음과 같습니다. • 0 - '알 수 없음' • 1 - '일치하지 않음' • 2 - '성공' • 3 - '캐시되지 않은 세션' • 4 - '알 수 없는 암호 그룹' • 5 - '지원되지 않는 암호 그룹' • 6 - '지원되지 않는 SSL 버전' • 7 - 'SSL 압축 사용됨' • 8 - '패시브 모드에서 세션 암호 해독 불가' • 9 - '핸드셰이크 오류' • 10 - '암호 해독 오류' • 11 - '서버 이름 카테고리 조회 보류 중' • 12 - '공용 이름 카테고리 조회 보류 중' • 13 - '내부 오류' • 14 - '네트워크 파라미터 사용 불가' • 15 - '유효하지 않은 서버 인증서 핸들' • 16 - '서버 인증서 핑거프린트 사용 불가' • 17 - '주체 DN을 캐시할 수 없음' • 18 - '발급자 DN을 캐시할 수 없음' • 19 - '알 수 없는 SSL 버전' • 20 - '외부 인증서 목록 사용 불가' • 21 - '외부 인증서 핑거프린트 사용 불가' • 22 - '내부 인증서 목록이 유효하지 않음' • 23 - '내부 인증서 목록 사용 불가' • 24 - '내부 인증서 사용 불가' • 25 - '내부 인증서 핑거프린트 사용 불가' • 26 - '서버 인증서 검증 사용 불가' • 27 - '서버 인증서 검증 장애' • 28 - '유효하지 않은 작업'
문자열 블록 유형	uint32	아카이브 SHA가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	아카이브 SHA 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 침입 정책 이름의 바이트 수를 더한 값이 포함됩니다.

표 B-14 5.4.x 버전용 악성코드 이벤트 데이터 블록 필드 (계속)

필드	데이터 유형	설명
아카이브 SHA	string	파일이 포함된 상위 아카이브의 SHA1 해시입니다.
문자열 블록 유형	uint32	아카이브 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	아카이브 이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 침입 정책 이름의 바이트 수를 더한 값이 포함됩니다.
아카이브 이름	string	상위 아카이브의 이름입니다.
아카이브 수준	uint8	파일이 중첩된 계층의 수입니다. 예를 들어 텍스트 파일이 zip 아카이브에 들어 있는 경우 이 항목의 값은 1입니다.

레거시 검색 데이터 구조

레거시 검색 이벤트 헤더

5.0~5.1.1.x 버전용 검색 이벤트 헤더

검색 및 연결 이벤트 메시지에는 검색 이벤트 헤더가 포함됩니다. 이 헤더는 이벤트의 유형과 하위 유형, 이벤트가 발생한 시간과 디바이스, 그리고 메시지의 이벤트 데이터 구조에 대한 정보를 전달합니다. 이 헤더 뒤에는 실제 호스트 검색, 사용자 또는 연결 이벤트 데이터가 옵니다. 구조는 이벤트 유형별 호스트 검색 구조, 페이지 4-44에 설명되어 있는 각 이벤트 유형/하위 유형 값과 연결됩니다.

검색 이벤트 헤더의 이벤트 유형 및 이벤트 하위 유형 필드는 전송된 이벤트 메시지의 구조를 식별합니다. 이벤트 데이터 블록의 구조가 확인되면 프로그램이 메시지를 적절하게 구문 분석할 수 있습니다.

다음 다이어그램에서 음영으로 표시된 행은 검색 이벤트 헤더의 형식을 나타냅니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	헤더 버전(1)																메시지 유형(4)															
	메시지 길이																															
	네트워크 맵 ID																레코드 유형															
	레코드 길이																															
	eStreamer 서버 타임스탬프(이벤트에서 비트 23이 설정된 경우에 한함)																															
	이후 사용을 위해 예약됨(이벤트에서 비트 23이 설정된 경우에 한함)																															
검색 이벤트 헤더	디바이스 ID																															
	IP 주소																															
	MAC 주소																															
	MAC 주소(계속)																이후 사용을 위해 예약됨															
	이벤트 초																															
	이벤트 마이크로초																															
	예약됨(내부)								이벤트 유형																							
	이벤트 하위 유형																															
	파일 번호(내부 전용)																															
	파일 위치(내부 전용)																															

다음 표에는 검색 이벤트 헤더에 대한 설명이 나와 있습니다.

표 B-15 검색 이벤트 헤더 필드

필드	데이터 유형	설명
디바이스 ID	uint32	검색 이벤트를 생성한 디바이스의 ID 번호입니다. 버전 3 및 4 메타데이터를 요청하면 디바이스의 메타데이터를 가져올 수 있습니다. 자세한 정보는 매니지드 디바이스 레코드 메타데이터, 페이지 3-35의 내용을 참조하십시오.
IP 주소	uint32	이벤트와 관련된 호스트의 IP 주소입니다.
MAC 주소	uint8[6]	이벤트와 관련된 호스트의 MAC 주소입니다.

표 B-15 검색 이벤트 헤더 필드 (계속)

필드	데이터 유형	설명
이후 사용을 위해 예약됨	byte[2]	값이 0으로 설정된 2바이트 패딩입니다.
이벤트 초	uint32	시스템에서 이벤트를 생성한 UNIX 타임스탬프(1970년 1월 1일 이후의 초 단위 시간)입니다.
이벤트 마이크로초	uint32	시스템이 이벤트를 생성한 마이크로초(100만분의 1초) 단위의 증분 시간입니다.
예약됨(내부)	byte	Cisco의 내부 데이터이므로 무시해도 됩니다.
이벤트 유형	uint32	이벤트 유형(새 이벤트의 경우 1000, 변경 이벤트의 경우 1001, 사용자 입력 이벤트의 경우 1002, 전체 호스트 프로파일의 경우 1050)입니다. 사용 가능한 이벤트 유형의 목록은 이벤트 유형별 호스트 검색 구조, 페이지 4-44의 내용을 참조하십시오.
이벤트 하위 유형	uint32	이벤트 하위 유형입니다. 사용 가능한 이벤트 하위 유형의 목록은 이벤트 유형별 호스트 검색 구조, 페이지 4-44의 내용을 참조하십시오.
파일 번호	byte[4]	직렬 파일 번호입니다. 이 필드는 Cisco 내부용이므로 무시해도 됩니다.
파일 위치	byte[4]	직렬 파일에서 이벤트의 위치입니다. 이 필드는 Cisco 내부용이므로 무시해도 됩니다.

레거시 서버 데이터 블록

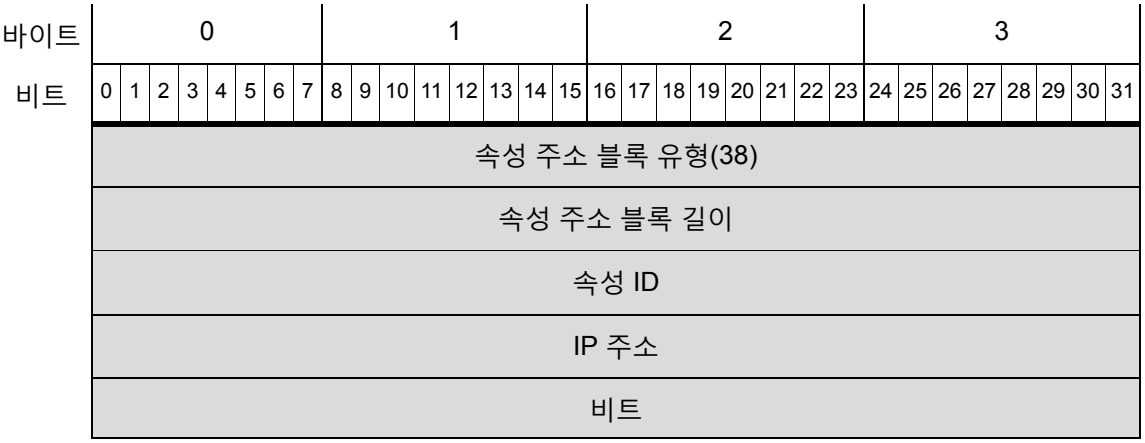
자세한 내용은 다음 섹션을 참조하십시오.

- 5.0~5.1.1.x 버전용 속성 주소 데이터 블록, 페이지 B-92

5.0~5.1.1.x 버전용 속성 주소 데이터 블록

속성 주소 데이터 블록은 속성 목록 항목을 포함하며 속성 정의 데이터 블록 내에서 사용됩니다. 이 블록의 블록 유형은 38입니다.

다음 다이어그램에 속성 주소 데이터 블록의 기본 구조가 나와 있습니다.



다음 표에는 속성 주소 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 B-16 속성 주소 데이터 블록 필드

필드	데이터 유형	설명
속성 주소 블록 유형	uint32	속성 주소 데이터 블록을 시작합니다. 이 값은 항상 38입니다.
속성 주소 블록 길이	uint32	속성 주소 데이터 블록의 바이트 수입니다. 여기에는 속성 주소 블록 유형 및 길이의 8바이트에 그 뒤의 속성 주소 데이터 바이트 수를 더한 값이 포함됩니다.
속성 ID	uint32	해당하는 경우 영향을 받는 속성의 ID 번호입니다.
IP 주소	uint8[4]	주소가 자동으로 할당된 경우 호스트의 IP 주소(IP 주소 옥텟 형식)입니다.
비트	uint32	IP 주소가 자동으로 할당된 경우 넷마스크를 계산하는 데 사용되는 주요 비트를 포함합니다.

레거시 클라이언트 애플리케이션 데이터 블록

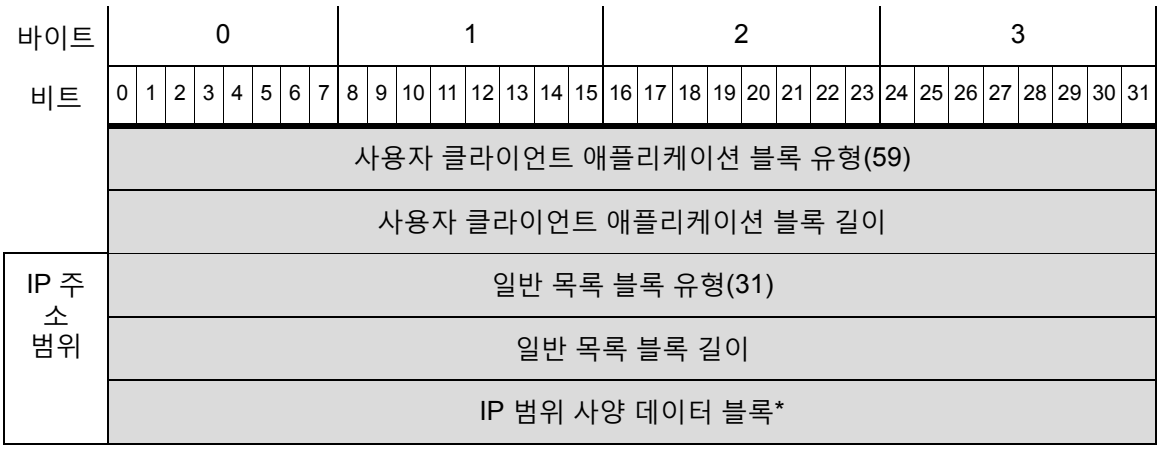
자세한 내용은 다음 섹션을 참조하십시오.

- 5.0~5.1 버전용 사용자 클라이언트 애플리케이션 데이터 블록, 페이지 B-93

5.0~5.1 버전용 사용자 클라이언트 애플리케이션 데이터 블록

사용자 클라이언트 애플리케이션 데이터 블록에는 클라이언트 애플리케이션 데이터의 소스에 대한 정보, 데이터를 추가한 사용자의 ID 번호 및 IP 주소 범위 데이터 블록 목록이 포함됩니다. 사용자 클라이언트 애플리케이션 데이터 블록의 블록 유형은 59입니다.

다음 다이어그램에 사용자 클라이언트 애플리케이션 데이터 블록의 기본 구조가 나와 있습니다.



	애플리케이션 프로토콜 ID
	클라이언트 애플리케이션 ID
버전	문자열 블록 유형(0)
	문자열 블록 길이
	버전...

다음 표에는 사용자 클라이언트 애플리케이션 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 B-17 사용자 클라이언트 애플리케이션 데이터 블록 필드

필드	바이트 수	설명
사용자 클라이언트 애플리케이션 블록 유형	uint32	사용자 클라이언트 애플리케이션 데이터 블록을 시작합니다. 이 값은 항상 138입니다.
사용자 클라이언트 애플리케이션 블록 길이	uint32	사용자 클라이언트 애플리케이션 데이터 블록의 총 바이트 수입니다. 여기에는 사용자 클라이언트 애플리케이션 블록 유형 및 길이 필드의 8바이트에 그 뒤의 사용자 클라이언트 애플리케이션 데이터 바이트 수를 더한 값이 포함됩니다.
일반 목록 블록 유형	uint32	IP 주소 범위 데이터를 전달하는 IP 범위 사양 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 IP 범위 사양 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
IP 범위 사양 데이터 블록*	variable	사용자 입력의 IP 주소 범위에 대한 정보가 포함된 IP 범위 사양 데이터 블록입니다. 이 데이터 블록에 대한 설명은 표 4-58사용자 서버 데이터 블록 필드, 페이지 4-105의 내용을 참조하십시오.
애플리케이션 프로토콜 ID	uint32	해당하는 경우 애플리케이션 프로토콜의 내부 ID 번호입니다.
클라이언트 애플리케이션 ID	uint32	해당하는 경우 탐지된 클라이언트 애플리케이션의 내부 ID 번호입니다.
문자열 블록 유형	uint32	클라이언트 애플리케이션 버전이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	클라이언트 애플리케이션 버전 문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이 필드의 값에 버전의 바이트 수를 더한 값이 포함됩니다.
버전	string	클라이언트 애플리케이션 버전입니다.

레거시 스캔 결과 데이터 블록

자세한 내용은 다음 섹션을 참조하십시오.

- 5.0~5.1.1.x 버전용 스캔 결과 데이터 블록, 페이지 B-95
- 5.0.x 버전용 사용자 제품 데이터 블록, 페이지 B-97
- 5.x 버전용 사용자 정보 데이터 블록, 페이지 B-117

5.0~5.1.1.x 버전용 스캔 결과 데이터 블록

스캔 결과 데이터 블록은 취약점을 설명하며 스캔 결과 추가 이벤트(이벤트 유형 1002, 하위 유형 11) 내에서 사용됩니다. 스캔 결과 데이터 블록의 블록 유형은 102입니다.

다음 다이어그램에 스캔 결과 데이터 블록의 형식이 나와 있습니다.

다음 표에는 스캔 결과 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 B-18 스캔 결과 데이터 블록 필드

필드	데이터 유형	설명
스캔 결과 블록 유형	uint32	스캔 결과 데이터 블록을 시작합니다. 이 값은 항상 102입니다.
스캔 결과 블록 길이	uint32	취약점 스캔 데이터 블록의 바이트 수입니다. 여기에는 취약점 스캔 블록 유형 및 길이 필드의 8바이트에 그 뒤의 취약점 스캔 데이터 바이트 수를 더한 값이 포함됩니다.
사용자 ID	uint32	스캔 결과를 가져왔거나 스캔 결과가 생성된 스캔을 실행한 사용자의 사용자 ID 번호를 포함합니다.
스캔 유형	uint32	결과가 시스템에 추가된 방법을 나타냅니다.
IP 주소	uint32	결과에서 취약점의 영향을 받는 호스트의 IP 주소(IP 주소 옥텟 형식)입니다.
포트	uint16	결과에서 취약점의 영향을 받는 하위 서버가 사용하는 포트입니다.
프로토콜	uint16	IANA 프로토콜 번호입니다. 예를 들면 다음과 같습니다. • 1 - ICMP • 4 - IP • 6 - TCP • 17 - UDP
플래그	uint16	예약됨
목록 블록 유형	uint32	전송 취약점 스캔 데이터를 전달하는 취약점 스캔 데이터 블록으로 구성된 목록 데이터 블록을 시작합니다. 이 값은 항상 11입니다.
목록 블록 길이	uint32	목록의 바이트 수입니다. 이 수에는 목록 블록 유형 및 길이 필드의 8바이트에 캡슐화된 모든 취약점 스캔 데이터 블록을 더한 값이 포함됩니다. 이 필드 뒤에는 취약점 스캔 데이터 블록이 없을 수도 있고 하나 이상 올 수도 있습니다.
취약점 스캔 블록 유형	uint32	스캔 중에 탐지된 취약점을 설명하는 취약점 스캔 데이터 블록을 시작합니다. 이 값은 항상 109입니다.
취약점 스캔 블록 길이	uint32	취약점 스캔 데이터 블록의 바이트 수입니다. 여기에는 취약점 스캔 블록 유형 및 길이 필드의 8바이트에 그 뒤의 취약점 스캔 데이터 바이트 수를 더한 값이 포함됩니다.
취약점 데이터	string	각 취약점과 관련된 정보입니다.
목록 블록 유형	uint32	전송 취약점 스캔 데이터를 전달하는 취약점 스캔 데이터 블록으로 구성된 목록 데이터 블록을 시작합니다. 이 값은 항상 11입니다.
목록 블록 길이	uint32	목록의 바이트 수입니다. 이 수에는 목록 블록 유형 및 길이 필드의 8바이트에 캡슐화된 모든 취약점 스캔 데이터 블록을 더한 값이 포함됩니다. 이 필드 뒤에는 취약점 스캔 데이터 블록이 없을 수도 있고 하나 이상 올 수도 있습니다.
일반 스캔 결과 블록 유형	uint32	스캔 중에 탐지된 서버 및 운영 체제 데이터를 설명하는 일반 스캔 결과 데이터 블록을 시작합니다. 이 값은 항상 108입니다.

표 B-18 스캔 결과 데이터 블록 필드 (계속)

필드	데이터 유형	설명
일반 스캔 결과 블록 길이	uint32	일반 스캔 결과 데이터 블록의 바이트 수입니다. 여기에는 일반 스캔 결과 블록 유형 및 길이 필드의 8바이트에 그 뒤의 스캔 결과 데이터 바이트 수를 더한 값이 포함됩니다.
일반 스캔 결과 데이터	string	각 스캔 결과와 관련된 정보입니다.
일반 목록 블록 유형	uint32	서드파티 애플리케이션의 호스트 입력 데이터를 전달하는 사용자 제품 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 사용자 제품 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
사용자 제품 데이터 블록*	variable	호스트 입력 데이터를 포함하는 사용자 제품 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 사용자 제품 데이터 블록, 페이지 4-171의 내용을 참조하십시오.

5.0.x 버전용 사용자 제품 데이터 블록

사용자 제품 데이터 블록은 서드파티 애플리케이션에서 가져온 호스트 입력 데이터(서드파티 애플리케이션 문자열 매핑 포함)를 전달합니다. 이 데이터 블록은 6.0.x 버전용 연결 통계 데이터 블록, 페이지 B-194 및 사용자 서버 및 운영 체제 메시지, 페이지 4-58에서 사용됩니다. 사용자 제품 데이터 블록의 블록 유형은 4.10.x 버전의 경우 65, 5.0~5.0.x 버전의 경우 118입니다. 블록 유형의 구조는 동일합니다.

참고 다음 다이어그램에서 데이터 블록 이름 옆에 있는 별표(*)는 데이터 블록 인스턴스가 여러 개 나올 수 있음을 나타냅니다.

다음 다이어그램에 사용자 제품 데이터 블록의 형식이 나와 있습니다.


바이트
0
1
2
3
비트
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
IP주소 범위
일반 목록 블록 유형(31)
일반 목록 블록 길이
IP 범위 사양 데이터 블록*
포트
프로토콜
사용자 제품 삭제
맞춤형 벤더 문자열
문자열 블록 유형(0)
문자열 블록 길이
맞춤형 벤더 문자열...
맞춤형 제품 문자열
문자열 블록 유형(0)
문자열 블록 길이
맞춤형 제품 문자열...
맞춤형 버전 문자열
문자열 블록 유형(0)
문자열 블록 길이
맞춤형 버전 문자열...
소프트웨어 ID
서버 ID
벤더 ID
제품 ID
주 버전 문자열
문자열 블록 유형(0)
문자열 블록 길이
주 버전 문자열...
부 버전 문자열
문자열 블록 유형(0)
문자열 블록 길이
부 버전 문자열...

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
수정 문자열	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	수정 문자열...																															
끝 주 버전 문자열	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	끝 주 버전 문자열...																															
끝 부 버전 문자열	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	끝 부 버전 문자열...																															
끝 수정 문자열	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	끝 수정 문자열...																															
빌드 문자열	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	빌드 문자열...																															
패치 문자열	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	패치 문자열...																															
확장 문자열	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	확장 문자열...																															

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
OS UUID	운영 체제 UUID																															
	운영 체제 UUID(계속)																															
	운영 체제 UUID(계속)																															
	운영 체제 UUID(계속)																															
수정 목록	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
	수정 목록 데이터 블록*																															

다음 표에는 사용자 제품 데이터 블록의 구성 요소에 대한 설명이 나와 있습니다.

표 B-19 4.10.x, 5.0~5.0.x 버전용 사용자 제품 데이터 블록 필드

필드	데이터 유형	설명
사용자 제품 데이터 블록 유형	uint32	사용자 제품 데이터 블록을 시작합니다. 이 값은 4.10.x 버전의 경우 65, 5.0~5.0.x 버전의 경우 118입니다.
사용자 제품 블록 길이	uint32	사용자 제품 데이터 블록의 총 바이트 수입니다. 여기에는 사용자 제품 블록 유형 및 길이 필드의 8바이트에 그 뒤의 사용자 제품 데이터 바이트 수를 더한 값이 포함됩니다.
소스 ID	uint32	데이터를 가져온 소스의 ID 번호입니다.
소스 유형	uint32	데이터를 제공한 소스의 소스 유형입니다.
일반 목록 블록 유형	uint32	IP 주소 범위 데이터를 전달하는 IP 범위 사양 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 IP 범위 사양 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
IP 범위 사양 데이터 블록*	variable	사용자 입력의 IP 주소 범위에 대한 정보가 포함된 IP 범위 사양 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.2 이상 버전용 IP 주소 범위 데이터 블록, 페이지 4-96의 내용을 참조하십시오.
포트	uint16	사용자가 지정한 포트입니다.
프로토콜	uint16	사용자가 지정한 IANA 프로토콜 번호입니다. 예를 들면 다음과 같습니다. • 1 - ICMP • 4 - IP • 6 - TCP • 17 - UDP

표 B-19 4.10.x, 5.0~5.0.x 버전용 사용자 제품 데이터 블록 필드 (계속)

필드	데이터 유형	설명
사용자 제품 삭제	uint32	사용자 OS 정의가 호스트에서 삭제되었는지를 나타냅니다. • 0 - 아니요 • 1 - 예
문자열 블록 유형	uint32	사용자 입력에 지정된 맞춤형 벤더 이름을 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	맞춤형 벤더 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 벤더 이름의 바이트 수를 더한 값이 포함됩니다.
맞춤형 벤더 이름	string	사용자 입력에 지정된 맞춤형 벤더 이름입니다.
문자열 블록 유형	uint32	사용자 입력에 지정된 맞춤형 제품 이름을 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	맞춤형 제품 이름 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 제품 이름의 바이트 수를 더한 값이 포함됩니다.
맞춤형 제품 이름	string	사용자 입력에 지정된 맞춤형 제품 이름입니다.
문자열 블록 유형	uint32	사용자 입력에 지정된 맞춤형 버전을 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	맞춤형 버전 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 버전의 바이트 수를 더한 값이 포함됩니다.
맞춤형 버전	string	사용자 입력에 지정된 맞춤형 버전입니다.
소프트웨어 ID	uint32	Cisco 데이터베이스 내 서버 또는 운영 체제의 특정 수정에 대한 식별자입니다.
서버 ID	uint32	사용자 입력에 지정된 호스트 서버의 애플리케이션 프로토콜에 대한 Cisco 애플리케이션 식별자입니다.
벤더 ID	uint32	지정한 서드파티 운영 체제가 Cisco 3D 운영 체제 정의에 매핑될 때 해당 서드파티 운영 체제의 벤더 식별자입니다.
제품 ID	uint32	지정한 서드파티 운영 체제 문자열이 Cisco 3D 운영 체제 정의에 매핑될 때 해당 서드파티 운영 체제 문자열의 제품 ID 문자열입니다.
문자열 블록 유형	uint32	사용자 입력의 서드파티 운영 체제 문자열이 매핑되는 Cisco 3D 운영 체제 정의의 주 버전 번호가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	주 버전 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 버전의 바이트 수를 더한 값이 포함됩니다.
주 버전	string	서드파티 운영 체제 문자열이 매핑되는 Cisco 3D 운영 체제 정의의 주 버전입니다.
문자열 블록 유형	uint32	서드파티 운영 체제 문자열이 매핑되는 Cisco 3D 운영 체제 정의의 부 버전 번호가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.

표 B-19 4.10.x, 5.0~5.0.x 버전용 사용자 제품 데이터 블록 필드 (계속)

필드	데이터 유형	설명
문자열 블록 길이	uint32	부 버전 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 버전의 바이트 수를 더한 값이 포함됩니다.
부 버전	string	사용자 입력의 서드파티 운영 체제 문자열이 매핑되는 Cisco 3D 운영 체제 정의의 부 버전 번호입니다.
문자열 블록 유형	uint32	사용자 입력의 서드파티 운영 체제 문자열이 매핑되는 Cisco 운영 체제 정의의 수정 번호가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	수정 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 수정 번호의 바이트 수를 더한 값이 포함됩니다.
수정	string	사용자 입력의 서드파티 운영 체제 문자열이 매핑되는 Cisco 3D 운영 체제 정의의 수정 번호입니다.
문자열 블록 유형	uint32	서드파티 운영 체제 문자열이 매핑되는 Cisco 3D 운영 체제 정의의 마지막 주 버전이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	끝 주 버전 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 버전의 바이트 수를 더한 값이 포함됩니다.
끝 주 버전	string	사용자 입력의 서드파티 운영 체제 문자열이 매핑되는 Cisco 3D 운영 체제 정의의 주 버전 번호 범위에서 마지막 버전 번호입니다.
문자열 블록 유형	uint32	서드파티 운영 체제 문자열이 매핑되는 Cisco 3D 운영 체제 정의의 마지막 부 버전이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	끝 부 버전 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 버전의 바이트 수를 더한 값이 포함됩니다.
끝 부 버전	string	사용자 입력의 서드파티 운영 체제 문자열이 매핑되는 Cisco 3D 운영 체제 정의의 부 버전 번호 범위에서 마지막 버전 번호입니다.
문자열 블록 유형	uint32	서드파티 운영 체제 문자열이 매핑되는 Cisco 3D 운영 체제 정의의 마지막 수정 번호가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	끝 수정 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 수정 번호의 바이트 수를 더한 값이 포함됩니다.
끝 수정	string	사용자 입력의 서드파티 운영 체제 문자열이 매핑되는 Cisco 3D 운영 체제 정의의 수정 번호 범위에서 마지막 수정 번호입니다.
문자열 블록 유형	uint32	서드파티 운영 체제 문자열이 매핑되는 Cisco 3D 운영 체제의 빌드 번호가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	빌드 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 빌드 번호의 바이트 수를 더한 값이 포함됩니다.

표 B-19 4.10.x, 5.0~5.0.x 버전용 사용자 제품 데이터 블록 필드 (계속)

필드	데이터 유형	설명
빌드	string	사용자 입력의 서드파티 운영 체제 문자열이 매핑되는 Cisco 3D 운영 체제의 빌드 번호입니다.
문자열 블록 유형	uint32	서드파티 운영 체제 문자열이 매핑되는 Cisco 3D 운영 체제의 패치 번호가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	패치 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 패치 번호의 바이트 수를 더한 값이 포함됩니다.
패치	string	사용자 입력의 서드파티 운영 체제 문자열이 매핑되는 Cisco 3D 운영 체제의 패치 번호입니다.
문자열 블록 유형	uint32	서드파티 운영 체제 문자열이 매핑되는 Cisco 3D 운영 체제의 확장 번호가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	확장 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 확장 번호의 바이트 수를 더한 값이 포함됩니다.
확장	string	사용자 입력의 서드파티 운영 체제 문자열이 매핑되는 Cisco 3D 운영 체제의 확장 번호입니다.
UUID	uint8 [x16]	운영 체제의 고유 ID 번호를 포함합니다.
일반 목록 블록 유형	uint32	지정한 IP 주소 범위의 호스트에 적용된 수정과 관련한 사용자 입력 데이터를 전달하는 수정 목록 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 수정 목록 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
수정 목록 데이터 블록*	variable	호스트에 적용된 수정에 대한 정보를 포함하는 수정 목록 데이터 블록입니다. 이 데이터 블록에 대한 설명은 수정 목록 데이터 블록, 페이지 4-103의 내용을 참조하십시오.

레거시 사용자 로그인 데이터 블록

자세한 내용은 다음 섹션을 참조하십시오.

- 5.0~5.0.2 버전용 사용자 로그인 정보 데이터 블록, 페이지 B-104
- 5.1~5.4.x 버전용 사용자 로그인 정보 데이터 블록, 페이지 B-105
- 6.0.x 버전용 사용자 로그인 정보 데이터 블록, 페이지 B-107
- 6.1.x 버전용 사용자 로그인 정보 데이터 블록, 페이지 B-110
- 5.x 버전용 사용자 정보 데이터 블록, 페이지 B-117

5.0~5.0.2 버전용 사용자 로그인 정보 데이터 블록

사용자 로그인 정보 데이터 블록은 사용자 정보 업데이트 메시지에 사용되며 탐지된 사용자의 로그인 정보 변경 사항을 전달합니다. 자세한 정보는 사용자 정보 업데이트 메시지 블록, 페이지 4-62의 내용을 참조하십시오.

사용자 로그인 정보 데이터 블록의 블록 유형은 5.0~5.0.2 버전의 경우 121입니다.

아래 그림에 사용자 로그인 정보 데이터 블록의 형식이 나와 있습니다.

다음 표에는 사용자 로그인 정보 데이터 블록의 구성 요소에 대한 설명이 나와 있습니다.

표 B-20 5.0~5.0.2 버전용 사용자 로그인 정보 데이터 블록 필드

필드	데이터 유형	설명
사용자 로그인 정보 블록 유형	uint32	사용자 로그인 정보 데이터 블록을 시작합니다. 5.0~5.0.2 버전의 경우 이 값은 121입니다.
사용자 로그인 정보 블록 길이	uint32	사용자 로그인 정보 데이터 블록의 총 바이트 수입니다. 여기에는 사용자 로그인 정보 블록 유형 및 길이 필드의 8바이트에 그 뒤의 사용자 로그인 정보 데이터 바이트 수를 더한 값이 포함됩니다.
타임스탬프	uint32	이벤트의 타임스탬프입니다.

표 B-20 5.0~5.0.2 버전용 사용자 로그인 정보 데이터 블록 필드 (계속)

필드	데이터 유형	설명
IP 주소	uint8[4]	로그인 중인 사용자가 탐지된 호스트의 IP 주소(IP 주소 옥텟 형식)입니다.
문자열 블록 유형	uint32	사용자의 사용자 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	사용자 이름 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 사용자 이름의 바이트 수를 더한 값이 포함됩니다.
사용자 이름	string	사용자의 사용자 이름입니다.
사용자 ID	uint32	사용자의 ID 번호입니다.
애플리케이션 ID	uint32	로그인 정보가 파생된 연결에서 사용되는 애플리케이션 프로토콜의 애플리케이션 ID입니다.
문자열 블록 유형	uint32	사용자의 이메일 주소가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	이메일 주소 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 이메일 주소의 바이트 수를 더한 값이 포함됩니다.
이메일	string	사용자의 이메일 주소입니다.

5.1~5.4.x 버전용 사용자 로그인 정보 데이터 블록

사용자 로그인 정보 데이터 블록은 사용자 정보 업데이트 메시지에 사용되며 탐지된 사용자의 로그인 정보 변경 사항을 전달합니다. 자세한 정보는 사용자 계정 업데이트 메시지 데이터 블록, 페이지 4-180의 내용을 참조하십시오.

계열 1 블록 그룹에서 사용자 로그인 정보 데이터 블록의 블록 유형은 4.7~4.10.x 버전의 경우 73, 5.0~5.0.2 버전의 경우 121, 5.1~5.4.x 버전의 경우 127입니다.

아래 그림에 사용자 로그인 정보 데이터 블록의 형식이 나와 있습니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	사용자 ID																															
	애플리케이션 ID																															
이메일	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	이메일...																															
	IPv6 주소 IPv6 주소(계속) IPv6 주소(계속) IPv6 주소(계속)																															
보고자	로그인 유형								문자열 블록 유형(0)																							
	문자열 블록 유형(0)(계속)								문자열 블록 길이																							
	문자열 블록 길이								보고자...																							

다음 표에는 사용자 로그인 정보 데이터 블록의 구성 요소에 대한 설명이 나와 있습니다.

표 B-21 사용자 로그인 정보 데이터 블록 필드

필드	데이터 유형	설명
사용자 로그인 정보 블록 유형	uint32	사용자 로그인 정보 데이터 블록을 시작합니다. 5.1 이상 버전의 경우 이 값은 127입니다.
사용자 로그인 정보 블록 길이	uint32	사용자 로그인 정보 데이터 블록의 총 바이트 수입니다. 여기에는 사용자 로그인 정보 블록 유형 및 길이 필드의 8바이트에 그 뒤의 사용자 로그인 정보 데이터 바이트 수를 더한 값이 포함됩니다.
타임스탬프	uint32	이벤트의 타임스탬프입니다.
IPv4 주소	uint32	이 필드는 예약되지만 더 이상 내용이 입력되지는 않습니다. IPv4 주소는 IPv6 Address(IPv6 주소) 필드에 저장됩니다. 자세한 정보는 IP 주소, 페이지 1-5의 내용을 참조하십시오.
문자열 블록 유형	uint32	사용자의 사용자 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	사용자 이름 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 사용자 이름의 바이트 수를 더한 값이 포함됩니다.

표 B-21 사용자 로그인 정보 데이터 블록 필드 (계속)

필드	데이터 유형	설명
사용자 이름	string	사용자의 사용자 이름입니다.
사용자 ID	uint32	사용자의 ID 번호입니다.
애플리케이션 ID	uint32	로그인 정보가 파생된 연결에서 사용되는 애플리케이션 프로토콜의 애플리케이션 ID입니다.
문자열 블록 유형	uint32	사용자의 이메일 주소가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	이메일 주소 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 이메일 주소의 바이트 수를 더한 값이 포함됩니다.
이메일	string	사용자의 이메일 주소입니다.
IPv6 주소	uint8[16]	로그인 중인 사용자가 탐지된 호스트의 IPv6 주소(IP 주소 옥텟 형식)입니다.
로그인 유형	uint8	탐지된 사용자 로그인의 유형입니다.
문자열 블록 유형	uint32	보고자 값이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	보고자 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 Reported By(보고자) 필드의 바이트 수를 더한 값이 포함됩니다.
보고자	string	로그인을 보고하는 Active Directory 서버의 이름입니다.

6.0.x 버전용 사용자 로그인 정보 데이터 블록

사용자 로그인 정보 데이터 블록은 사용자 정보 업데이트 메시지에 사용되며 탐지된 사용자의 로그인 정보 변경 사항을 전달합니다. 자세한 정보는 사용자 계정 업데이트 메시지 데이터 블록, 페이지 4-180의 내용을 참조하십시오.

사용자 로그인 정보 데이터 블록의 블록 유형은 6.0.x 버전의 경우 159입니다. 이 데이터 블록에는 새 ISE 통합 엔드포인트 프로파일, 보안 인텔리전스 필드가 포함되어 있습니다.

계열 1 블록 그룹에서 사용자 로그인 정보 데이터 블록의 블록 유형은 4.7~4.10.x 버전의 경우 73, 5.0~5.0.2 버전의 경우 121, 5.1 이상 버전의 경우 127입니다. 자세한 정보는 5.1~5.4.x 버전용 사용자 로그인 정보 데이터 블록, 페이지 B-105의 내용을 참조하십시오.

아래 그림에 사용자 로그인 정보 데이터 블록의 형식이 나와 있습니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
사용자 이름	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	사용자 이름...																															
도메인	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	도메인...																															
	사용자 ID																															
	영역 ID																															
	엔드포인트 프로파일 ID																															
	보안 그룹 ID																															
	프로토콜																															
이메일	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	이메일...																															
	IPv6 주소 IPv6 주소(계속) IPv6 주소(계속) IPv6 주소(계속)																															
	위치 IPv6 주소 위치 IPv6 주소(계속) 위치 IPv6 주소(계속) 위치 IPv6 주소(계속)																															
보고자	로그인 유형								인증 유형								문자열 블록 유형(0)															
	문자열 블록 유형(0)(계속)																문자열 블록 길이															
	문자열 블록 길이(계속)																보고자...															

다음 표에는 사용자 로그인 정보 데이터 블록의 구성 요소에 대한 설명이 나와 있습니다.

표 B-22 사용자 로그인 정보 데이터 블록 필드

필드	데이터 유형	설명
사용자 로그인 정보 블록 유형	uint32	사용자 로그인 정보 데이터 블록을 시작합니다. 6.0.x 버전의 경우 이 값은 159입니다.
사용자 로그인 정보 블록 길이	uint32	사용자 로그인 정보 데이터 블록의 총 바이트 수입니다. 여기에는 사용자 로그인 정보 블록 유형 및 길이 필드의 8바이트에 그 뒤의 사용자 로그인 정보 데이터 바이트 수를 더한 값이 포함됩니다.
타임스탬프	uint32	이벤트의 타임스탬프입니다.
IPv4 주소	uint32	이 필드는 예약되지만 더 이상 내용이 입력되지는 않습니다. IPv4 주소는 IPv6 Address(IPv6 주소) 필드에 저장됩니다. 자세한 정보는 IP 주소, 페이지 1-5의 내용을 참조하십시오.
문자열 블록 유형	uint32	사용자의 사용자 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	사용자 이름 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 사용자 이름의 바이트 수를 더한 값이 포함됩니다.
사용자 이름	string	사용자의 사용자 이름입니다.
문자열 블록 유형	uint32	도메인이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	사용자 이름 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 도메인의 바이트 수를 더한 값이 포함됩니다.
도메인	string	사용자가 로그인한 도메인입니다.
사용자 ID	uint32	사용자의 ID 번호입니다.
영역 ID	uint32	ID 영역에 해당하는 정수 ID입니다.
엔드포인트 프로파일 ID	uint32	연결 엔드포인트에서 사용하는 디바이스 유형의 ID 번호입니다. 각 DC에 대해 고유하며 메타데이터에서 확인 가능합니다.
보안 그룹 ID	uint32	네트워크 트래픽 그룹의 ID 번호입니다.
프로토콜	uint32	사용자를 탐지하거나 보고하는 데 사용되는 프로토콜입니다. 가능한 값은 다음과 같습니다. • 165 - FTP • 426 - SIP • 547 - AOL Instant Messenger • 683 - IMAP • 710 - LDAP • 767 - NTP • 773 - Oracle Database • 788 - POP3 • 1755 - MDNS

표 B-22 사용자 로그인 정보 데이터 블록 필드 (계속)

필드	데이터 유형	설명
문자열 블록 유형	uint32	사용자의 이메일 주소가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	이메일 주소 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 이메일 주소의 바이트 수를 더한 값이 포함됩니다.
이메일	string	사용자의 이메일 주소입니다.
IPv6 주소	uint8[16]	로그인 중인 사용자가 탐지된 호스트의 IPv6 주소(IP 주소 옥텟 형식)입니다.
위치 IPv6 주소	uint8[16]	사용자가 가장 최근에 로그인한 IP 주소입니다. IPv4 또는 IPv6 주소일 수 있습니다.
로그인 유형	uint8	탐지된 사용자 로그인의 유형입니다.
인증 유형	uint8	사용자가 사용한 인증의 유형입니다. 값은 다음 중 하나일 수 있습니다. • 0 - 인증 필요 없음 • 1 - 패시브 인증, AD 에이전트 또는 ISE 세션 • 2 - 종속 포털 정상 인증 • 3 - 종속 포털 게스트 인증 • 4 - 종속 포털 인증 장애
문자열 블록 유형	uint32	보고자 값이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	보고자 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 Reported By(보고자) 필드의 바이트 수를 더한 값이 포함됩니다.
보고자	string	로그인을 보고하는 Active Directory 서버의 이름입니다.

6.1.x 버전용 사용자 로그인 정보 데이터 블록

계열 1 블록 그룹에서 사용자 로그인 정보 데이터 블록의 블록 유형은 6.1 이상 버전의 경우 165입니다. 이 데이터 블록은 새로운 포트 및 터널링 필드를 포함하며, 이는 블록 유형 159를 대체합니다. 자세한 정보는 6.0.x 버전용 사용자 로그인 정보 데이터 블록, 페이지 B-107의 내용을 참조하십시오. 이는 블록 유형 167로 대체됩니다.

아래 그림에 사용자 로그인 정보 데이터 블록의 형식이 나와 있습니다.


바이트
0
1
2
3
비트
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
사용자 로그인 정보 블록 유형(165)
사용자 로그인 정보 블록 길이
타임스탬프
IPv4 주소
사용자 이름
문자열 블록 유형(0)
문자열 블록 길이
사용자 이름...
도메인
문자열 블록 유형(0)
문자열 블록 길이
도메인...
사용자 ID
영역 ID
엔드포인트 프로파일 ID
보안 그룹 ID
프로토콜
포트
범위 시작
시작 포트
종료 포트
이메일
문자열 블록 유형(0)
문자열 블록 길이
이메일...
IPv6 주소
IPv6 주소(계속)
IPv6 주소(계속)
IPv6 주소(계속)

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	위치 IPv6 주소 위치 IPv6 주소(계속) 위치 IPv6 주소(계속) 위치 IPv6 주소(계속)																															
보고자	로그인 유형								인증 유형								문자열 블록 유형(0)															
	문자열 블록 유형(0)(계속)																문자열 블록 길이															
	문자열 블록 길이(계속)																보고자...															

다음 표에는 사용자 로그인 정보 데이터 블록의 구성 요소에 대한 설명이 나와 있습니다.

표 B-23 사용자 로그인 정보 데이터 블록 필드

필드	데이터 유형	설명
사용자 로그인 정보 블록 유형	uint32	사용자 로그인 정보 데이터 블록을 시작합니다. 6.1 이상 버전의 경우 이 값은 165입니다.
사용자 로그인 정보 블록 길이	uint32	사용자 로그인 정보 데이터 블록의 총 바이트 수입니다. 여기에는 사용자 로그인 정보 블록 유형 및 길이 필드의 8바이트에 그 뒤의 사용자 로그인 정보 데이터 바이트 수를 더한 값이 포함됩니다.
타임스탬프	uint32	이벤트의 타임스탬프입니다.
IPv4 주소	uint32	이 필드는 예약되지만 더 이상 내용이 입력되지는 않습니다. IPv4 주소는 IPv6 Address(IPv6 주소) 필드에 저장됩니다. 자세한 정보는 IP 주소, 페이지 1-5의 내용을 참조하십시오.
문자열 블록 유형	uint32	사용자의 사용자 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	사용자 이름 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 사용자 이름의 바이트 수를 더한 값이 포함됩니다.
사용자 이름	string	사용자의 사용자 이름입니다.
문자열 블록 유형	uint32	도메인이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	사용자 이름 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 도메인의 바이트 수를 더한 값이 포함됩니다.
도메인	string	사용자가 로그인한 도메인입니다.
사용자 ID	uint32	사용자의 ID 번호입니다.

표 B-23 사용자 로그인 정보 데이터 블록 필드 (계속)

필드	데이터 유형	설명
영역 ID	uint32	ID 영역에 해당하는 정수 ID입니다.
엔드포인트 프로파일 ID	uint32	연결 엔드포인트에서 사용하는 디바이스 유형의 ID 번호입니다. 각 DC에 대해 고유하며 메타데이터에서 확인 가능합니다.
보안 그룹 ID	uint32	네트워크 트래픽 그룹의 ID 번호입니다.
프로토콜	uint32	사용자를 탐지하거나 보고하는 데 사용되는 프로토콜입니다. 가능한 값은 다음과 같습니다. • 165 - FTP • 426 - SIP • 547 - AOL Instant Messenger • 683 - IMAP • 710 - LDAP • 767 - NTP • 773 - Oracle Database • 788 - POP3 • 1755 - MDNS
포트	uint16	사용자가 탐지된 포트 번호입니다.
범위 시작	uint16	TS 에이전트에서 사용하는 포트 범위의 시작 포트입니다.
시작 포트	uint16	개별 사용자에게 할당된 TS 에이전트 범위의 시작 포트입니다.
종료 포트	uint16	개별 사용자에게 할당된 TS 에이전트 범위의 종료 포트입니다.
문자열 블록 유형	uint32	사용자의 이메일 주소가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	이메일 주소 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 이메일 주소의 바이트 수를 더한 값이 포함됩니다.
이메일	string	사용자의 이메일 주소입니다.
IPv6 주소	uint8[16]	로그인 중인 사용자가 탐지된 호스트의 IPv6 주소(IP 주소 옥텟 형식)입니다.
위치 IPv6 주소	uint8[16]	사용자가 가장 최근에 로그인한 IP 주소입니다. IPv4 또는 IPv6 주소일 수 있습니다.
로그인 유형	uint8	탐지된 사용자 로그인의 유형입니다.
인증 유형	uint8	사용자가 사용한 인증의 유형입니다. 값은 다음 중 하나일 수 있습니다. • 0 - 인증 필요 없음 • 1 - 패시브 인증, AD 에이전트 또는 ISE 세션 • 2 - 종속 포털 정상 인증 • 3 - 종속 포털 게스트 인증 • 4 - 종속 포털 인증 장애

표 B-23 사용자 로그인 정보 데이터 블록 필드 (계속)

필드	데이터 유형	설명
문자열 블록 유형	uint32	보고자 값이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	보고자 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 Reported By(보고자) 필드의 바이트 수를 더한 값이 포함됩니다.
보고자	string	로그인을 보고하는 Active Directory 서버의 이름입니다.

6.1.x 버전용 사용자 로그인 정보 데이터 블록

사용자 로그인 정보 데이터 블록은 사용자 정보 업데이트 메시지에 사용되며 탐지된 사용자의 로그인 정보 변경 사항을 전달합니다. 자세한 정보는 사용자 정보 업데이트 메시지 블록, 페이지 4-62의 내용을 참조하십시오.

계열 1 블록 그룹에서 사용자 로그인 정보 데이터 블록의 블록 유형은 6.1.x 버전의 경우 165입니다. 이 데이터 블록은 새로운 포트 및 터널링 필드를 포함하며, 이는 블록 유형 159를 대체합니다. 이는 블록 유형 167로 대체됩니다. 자세한 정보는 6.0.x 버전용 사용자 로그인 정보 데이터 블록, 페이지 B-107의 내용을 참조하십시오.

아래 그림에 사용자 로그인 정보 데이터 블록의 형식이 나와 있습니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	엔드포인트 프로파일 ID																															
	보안 그룹 ID																															
	프로토콜																															
	포트																범위 시작															
	시작 포트																종료 포트															
이메일	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	이메일...																															
	IPv6 주소 IPv6 주소(계속) IPv6 주소(계속) IPv6 주소(계속)																															
	위치 IPv6 주소 위치 IPv6 주소(계속) 위치 IPv6 주소(계속) 위치 IPv6 주소(계속)																															
보고자	로그인 유형								인증 유형								문자열 블록 유형(0)															
	문자열 블록 유형(0)(계속)																문자열 블록 길이															
	문자열 블록 길이(계속)																보고자...															
도메인	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	설명...																															

다음 표에는 사용자 로그인 정보 데이터 블록의 구성 요소에 대한 설명이 나와 있습니다.

표 B-24 사용자 로그인 정보 데이터 블록 필드

필드	데이터 유형	설명
사용자 로그인 정보 블록 유형	uint32	사용자 로그인 정보 데이터 블록을 시작합니다. 6.2 이상 버전의 경우 이 값은 165입니다.
사용자 로그인 정보 블록 길이	uint32	사용자 로그인 정보 데이터 블록의 총 바이트 수입니다. 여기에는 사용자 로그인 정보 블록 유형 및 길이 필드의 8바이트에 그 뒤의 사용자 로그인 정보 데이터 바이트 수를 더한 값이 포함됩니다.
타임스탬프	uint32	이벤트의 타임스탬프입니다.
IPv4 주소	uint32	이 필드는 예약되지만 더 이상 내용이 입력되지는 않습니다. IPv4 주소는 IPv6 Address(IPv6 주소) 필드에 저장됩니다. 자세한 정보는 IP 주소, 페이지 1-5의 내용을 참조하십시오.
문자열 블록 유형	uint32	사용자의 사용자 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	사용자 이름 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 사용자 이름의 바이트 수를 더한 값이 포함됩니다.
사용자 이름	string	사용자의 사용자 이름입니다.
문자열 블록 유형	uint32	도메인이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	사용자 이름 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 도메인의 바이트 수를 더한 값이 포함됩니다.
도메인	string	사용자가 로그인한 도메인입니다.
사용자 ID	uint32	사용자의 ID 번호입니다.
영역 ID	uint32	ID 영역에 해당하는 정수 ID입니다.
엔드포인트 프로파일 ID	uint32	연결 엔드포인트에서 사용하는 디바이스 유형의 ID 번호입니다. 각 DC에 대해 고유하며 메타데이터에서 확인 가능합니다.
보안 그룹 ID	uint32	네트워크 트래픽 그룹의 ID 번호입니다.
프로토콜	uint32	사용자를 탐지하거나 보고하는 데 사용되는 프로토콜입니다. 가능한 값은 다음과 같습니다. • 165 - FTP • 426 - SIP • 547 - AOL Instant Messenger • 683 - IMAP • 710 - LDAP • 767 - NTP • 773 - Oracle Database • 788 - POP3 • 1755 - MDNS
포트	uint16	사용자가 탐지된 포트 번호입니다.

표 B-24 사용자 로그인 정보 데이터 블록 필드 (계속)

필드	데이터 유형	설명
범위 시작	uint16	TS 에이전트에서 사용하는 포트 범위의 시작 포트입니다.
시작 포트	uint16	개별 사용자에게 할당된 TS 에이전트 범위의 시작 포트입니다.
종료 포트	uint16	개별 사용자에게 할당된 TS 에이전트 범위의 종료 포트입니다.
문자열 블록 유형	uint32	사용자의 이메일 주소가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	이메일 주소 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 이메일 주소의 바이트 수를 더한 값이 포함됩니다.
이메일	string	사용자의 이메일 주소입니다.
IPv6 주소	uint8[16]	로그인 중인 사용자가 탐지된 호스트의 IPv6 주소(IP 주소 옥텟 형식)입니다.
위치 IPv6 주소	uint8[16]	사용자가 가장 최근에 로그인한 IP 주소입니다. IPv4 또는 IPv6 주소일 수 있습니다.
로그인 유형	uint8	탐지된 사용자 로그인의 유형입니다.
인증 유형	uint8	사용자가 사용한 인증의 유형입니다. 값은 다음 중 하나일 수 있습니다. • 0 - 인증 필요 없음 • 1 - 패시브 인증, AD 에이전트 또는 ISE 세션 • 2 - 종속 포털 정상 인증 • 3 - 종속 포털 게스트 인증 • 4 - 종속 포털 인증 장애
문자열 블록 유형	uint32	보고자 값이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	보고자 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 Reported By(보고자) 필드의 바이트 수를 더한 값이 포함됩니다.
보고자	string	로그인을 보고하는 Active Directory 서버의 이름입니다.

5.x 버전용 사용자 정보 데이터 블록

사용자 정보 데이터 블록은 사용자 수정 메시지에서 사용되며 탐지, 제거 또는 삭제된 사용자에 대한 정보를 전달합니다. 자세한 정보는 사용자 수정 메시지, 페이지 4-62의 내용을 참조하십시오.

계열 1 블록 그룹에서 사용자 정보 데이터 블록의 블록 유형은 4.7~4.10.x 버전의 경우 75, 5.x 버전의 경우 120입니다. 블록 유형 75와 120의 구조는 동일합니다.

다음 다이어그램에 사용자 정보 데이터 블록의 형식이 나와 있습니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	사용자 정보 블록 유형(75 | 120)																															
	사용자 정보 블록 길이																															
	사용자 ID																															
사용자 이름	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	사용자 이름...																															
	프로토콜																															
이름	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	이름...																															
성	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	성...																															
이메일	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	이메일...																															
부서	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	부서...																															
전화	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	전화...																															

다음 표에는 사용자 정보 데이터 블록의 구성 요소에 대한 설명이 나와 있습니다.

표 B-25 사용자 정보 데이터 블록 필드

필드	데이터 유형	설명
사용자 정보 블록 유형	uint32	사용자 정보 데이터 블록을 시작합니다. 이 값은 4.7~4.10.x 버전의 경우 75, 5.0 이상 버전의 경우 120입니다.
사용자 정보 블록 길이	uint32	사용자 정보 데이터 블록의 총 바이트 수입니다. 여기에는 사용자 정보 블록 유형 및 길이 필드의 8바이트에 그 뒤의 사용자 정보 데이터 바이트 수를 더한 값이 포함됩니다.
사용자 ID	uint32	사용자의 ID 번호입니다.
문자열 블록 유형	uint32	사용자의 사용자 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	사용자 이름 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 사용자 이름의 바이트 수를 더한 값이 포함됩니다.
사용자 이름	string	사용자의 사용자 이름입니다.
프로토콜	uint32	사용자 정보를 포함하는 패킷의 프로토콜입니다.
문자열 블록 유형	uint32	사용자의 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	이름 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 이름의 바이트 수를 더한 값이 포함됩니다.
이름	string	사용자의 이름입니다.
문자열 블록 유형	uint32	사용자의 성이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	사용자 성 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 성의 바이트 수를 더한 값이 포함됩니다.
성	string	사용자의 성입니다.
문자열 블록 유형	uint32	사용자의 이메일 주소가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	이메일 주소 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 이메일 주소의 바이트 수를 더한 값이 포함됩니다.
이메일	string	사용자의 이메일 주소입니다.
문자열 블록 유형	uint32	사용자의 부서가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	부서 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 부서의 바이트 수를 더한 값이 포함됩니다.
부서	string	사용자의 부서입니다.

표 B-25 사용자 정보 데이터 블록 필드 (계속)

필드	데이터 유형	설명
문자열 블록 유형	uint32	사용자의 전화번호가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	전화번호 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 전화번호의 바이트 수를 더한 값이 포함됩니다.
전화	string	사용자의 전화번호입니다.

레거시 호스트 프로파일 데이터 블록

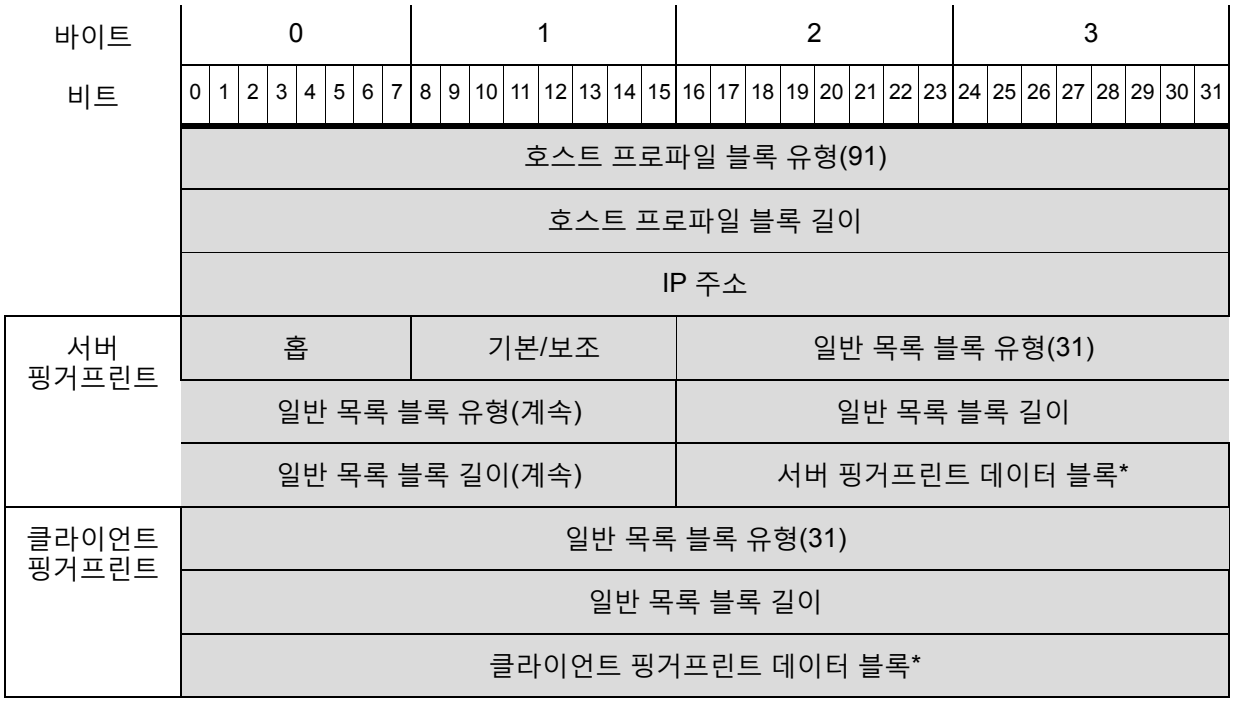
자세한 내용은 다음 섹션을 참조하십시오.

- 5.0~5.0.2 버전용 호스트 프로파일 데이터 블록, 페이지 B-120

5.0~5.0.2 버전용 호스트 프로파일 데이터 블록

다음 다이어그램에 5.0~5.0.2 버전의 호스트 프로파일 데이터 블록 형식이 나와 있습니다. 호스트 프로파일 데이터 블록은 호스트 임계성 값은 포함하지 않지만 VLAN 유무 표시기는 포함합니다. 그리고 호스트 프로파일 데이터 블록은 호스트의 NetBIOS 이름을 전달할 수 있습니다. 이 호스트 프로파일 데이터 블록의 블록 유형은 91입니다.

참고 이 다이어그램에서 블록 유형 필드 옆에 있는 별표(*)는 메시지가 계열 1 데이터 블록 인스턴스를 포함하지 않을 수도 있고 하나 이상 포함할 수도 있음을 나타냅니다.



바이트	0								1								2								3								
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
SMB 핑거프린트	일반 목록 블록 유형(31)																																
	일반 목록 블록 길이																																
	SMB 핑거프린트 데이터 블록*																																
DHCP 핑거프린트	일반 목록 블록 유형(31)																																
	일반 목록 블록 길이																																
	DHCP 핑거프린트 데이터 블록*																																
	목록 블록 유형(11)																																TCP 서버 목록
	목록 블록 길이																																
TCP 서버 블록*	서버 블록 유형(36)																																
	서버 블록 길이																																
	TCP 서버 데이터...																																
	목록 블록 유형(11)																																UDP 서버 목록
	목록 블록 길이																																
UDP 서버 블록*	서버 블록 유형(36)*																																
	서버 블록 길이																																
	UDP 서버 데이터...																																
	목록 블록 유형(11)																																네트워크 프로토콜 목록
	목록 블록 길이																																
네트워크 프로토콜 블록*	프로토콜 블록 유형(4)*																																
	프로토콜 블록 길이																																
	네트워크 프로토콜 데이터...																																


바이트
0
1
2
3
비트
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
목록 블록 유형(11)
목록 블록 길이
프로토콜 블록 유형(4)*
프로토콜 블록 길이
전송 프로토콜 데이터...
전송 프로토콜 목록
전송 프로토콜 블록*
목록 블록 유형(11)
목록 블록 길이
MAC 주소 블록 유형(95)*
MAC 주소 블록 길이
MAC 주소 데이터...
MAC 주소 목록
MAC 주소 블록*
호스트 마지막 확인
호스트 유형
VLAN 유무
VLAN ID
VLAN 유형
VLAN 우선순위
일반 목록 블록 유형(31)
일반 목록 블록 유형(계속)
일반 목록 블록 길이
일반 목록 블록 길이(계속)
클라이언트 애플리케이션 블록 유형(112)*
클라이언트 애플리케이션 블록 유형(29)*(계속)
클라이언트 애플리케이션 블록 길이
클라이언트 애플리케이션 블록 길이(계속)
클라이언트 애플리케이션 데이터...
클라이언트 애플리케이션 목록
클라이언트 앱 데이터
문자열 블록 유형(0)
문자열 블록 길이
NetBIOS 문자열 데이터...
NetBIOS 이름

다음 표에는 4.9~5.0.2 버전에서 반환되는 호스트 프로파일 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 B-26 5.0~5.0.2 버전용 호스트 프로파일 데이터 블록 필드

필드	데이터 유형	설명
호스트프로파일 블록 유형	uint32	4.9~5.0.2 버전용 호스트 프로파일 데이터 블록을 시작합니다. 이 데이터 블록의 블록 유형은 91입니다.
호스트프로파일 블록 길이	uint32	호스트 프로파일 데이터 블록의 바이트 수입니다. 여기에는 호스트 프로파일 블록 유형 및 길이 필드의 8바이트에 그 뒤의 호스트 프로파일 데이터에 포함된 바이트 수를 더한 값이 포함됩니다.
IP 주소	uint8[4]	프로파일에서 설명하는 호스트의 IP 주소(IP 주소 옥텟 형식)입니다.
홉	uint8	호스트에서 디바이스로의 홉 수입니다.
기본/보조	uint8	호스트가 호스트를 탐지한 디바이스의 기본 네트워크에 있는지 아니면 보조 네트워크에 있는지를 나타냅니다. • 0 - 호스트가 기본 네트워크에 있습니다. • 1 - 호스트가 보조 네트워크에 있습니다.
일반 목록 블록 유형	uint32	서버 핑거프린트를 사용하여 식별된 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
운영 체제 핑거프린트(서버 핑거프린트) 데이터 블록*	variable	서버 핑거프린트를 사용하여 식별된 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.0~5.0.2 버전용 운영 체제 핑거프린트 데이터 블록, 페이지 B-127의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	클라이언트 핑거프린트를 사용하여 식별된 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
운영 체제 핑거프린트(클라이언트 핑거프린트) 데이터 블록*	variable	클라이언트 핑거프린트를 사용하여 식별된 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.0~5.0.2 버전용 운영 체제 핑거프린트 데이터 블록, 페이지 B-127의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	SMB 핑거프린트를 사용하여 식별된 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
운영 체제 핑거프린트(SMB 핑거프린트) 데이터 블록*	variable	SMB 핑거프린트를 사용하여 식별된 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.0~5.0.2 버전용 운영 체제 핑거프린트 데이터 블록, 페이지 B-127의 내용을 참조하십시오.

표 B-26 5.0~5.0.2 버전용 호스트 프로파일 데이터 블록 필드 (계속)

필드	데이터 유형	설명
일반 목록 블록 유형	uint32	DHCP 핑거프린트를 사용하여 식별된 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
운영 체제 핑거프린트(DHCP 핑거프린트) 데이터 블록*	variable	DHCP 핑거프린트를 사용하여 식별된 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.0~5.0.2 버전용 운영 체제 핑거프린트 데이터 블록, 페이지 B-127의 내용을 참조하십시오.
목록 블록 유형	uint32	TCP 서버 데이터를 전달하는 서버 데이터 블록으로 구성된 목록 데이터 블록을 시작합니다. 이 값은 항상 11입니다.
목록 블록 길이	uint32	목록의 바이트 수입니다. 이 수에는 목록 블록 유형 및 길이 필드의 8바이트에 캡슐화된 모든 서버 데이터 블록을 더한 값이 포함됩니다. 이 필드 뒤에는 서버 데이터 블록이 없을 수도 있고 하나 이상 올 수도 있습니다.
서버 블록 유형	uint32	서버 데이터 블록을 시작합니다. 이 값은 항상 89입니다.
서버 블록 길이	uint32	서버 데이터 블록의 바이트 수입니다. 여기에는 서버 블록 유형 및 길이 필드의 8바이트에 그 뒤의 TCP 서버 데이터 바이트 수를 더한 값이 포함됩니다.
TCP 서버 데이터	variable	이전 버전 제품에 설명되어 있는 TCP 서버를 설명하는 데이터 필드입니다.
목록 블록 유형	uint32	UDP 서버 데이터를 전달하는 서버 데이터 블록으로 구성된 목록 데이터 블록을 시작합니다. 이 값은 항상 11입니다.
목록 블록 길이	uint32	목록의 바이트 수입니다. 이 수에는 목록 블록 유형 및 길이 필드의 8바이트에 캡슐화된 모든 서버 데이터 블록을 더한 값이 포함됩니다. 이 필드 뒤에는 서버 데이터 블록이 없을 수도 있고 하나 이상 올 수도 있습니다.
서버 블록 유형	uint32	UDP 서버를 설명하는 서버 데이터 블록을 시작합니다. 이 값은 항상 89입니다.
서버 블록 길이	uint32	서버 데이터 블록의 바이트 수입니다. 여기에는 서버 블록 유형 및 길이 필드의 8바이트에 그 뒤의 UDP 서버 데이터 바이트 수를 더한 값이 포함됩니다.
UDP 서버 데이터	variable	이전 버전 제품에 설명되어 있는 UDP 서버를 설명하는 데이터 필드입니다.
목록 블록 유형	uint32	네트워크 프로토콜 데이터를 전달하는 프로토콜 데이터 블록으로 구성된 목록 데이터 블록을 시작합니다. 이 값은 항상 11입니다.

표 B-26 5.0~5.0.2 버전용 호스트 프로파일 데이터 블록 필드 (계속)

필드	데이터 유형	설명
목록 블록 길이	uint32	목록의 바이트 수입니다. 이 수에는 목록 블록 유형 및 길이 필드의 8바이트에 캡슐화된 모든 프로토콜 데이터 블록을 더한 값이 포함됩니다. 이 필드 뒤에는 프로토콜 데이터 블록이 없을 수도 있고 하나 이상 올 수도 있습니다.
프로토콜 블록 유형	uint32	네트워크 프로토콜을 설명하는 프로토콜 데이터 블록을 시작합니다. 이 값은 항상 4입니다.
프로토콜 블록 길이	uint32	프로토콜 데이터 블록의 바이트 수입니다. 여기에는 프로토콜 블록 유형 및 길이 필드의 8바이트에 그 뒤의 프로토콜 데이터 바이트 수를 더한 값이 포함됩니다.
네트워크 프로토콜 데이터	uint16	프로토콜 데이터 블록, 페이지 4-77에 설명되어 있는 네트워크 프로토콜 번호가 포함된 데이터 필드입니다.
목록 블록 유형	uint32	전송 프로토콜 데이터를 전달하는 프로토콜 데이터 블록으로 구성된 목록 데이터 블록을 시작합니다. 이 값은 항상 11입니다.
목록 블록 길이	uint32	목록의 바이트 수입니다. 이 수에는 목록 블록 유형 및 길이 필드의 8바이트에 캡슐화된 모든 프로토콜 데이터 블록을 더한 값이 포함됩니다. 이 필드 뒤에는 전송 프로토콜 데이터 블록이 없을 수도 있고 하나 이상 올 수도 있습니다.
프로토콜 블록 유형	uint32	전송 프로토콜을 설명하는 프로토콜 데이터 블록을 시작합니다. 이 값은 항상 4입니다.
프로토콜 블록 길이	uint32	프로토콜 데이터 블록의 바이트 수입니다. 여기에는 프로토콜 블록 유형 및 길이의 8바이트에 그 뒤의 프로토콜 데이터 바이트 수를 더한 값이 포함됩니다.
전송 프로토콜 데이터	variable	프로토콜 데이터 블록, 페이지 4-77에 설명되어 있는 전송 프로토콜 번호가 포함된 데이터 필드입니다.
목록 블록 유형	uint32	MAC 주소 데이터 블록으로 구성된 목록 데이터 블록을 시작합니다. 이 값은 항상 11입니다.
목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 MAC 주소 데이터 블록을 포함한 목록의 바이트 수입니다.
호스트 MAC 주소 블록 유형	uint32	호스트 MAC 주소 데이터 블록을 시작합니다. 이 값은 항상 95입니다.
호스트 MAC 주소 블록 길이	uint32	호스트 MAC 주소 데이터 블록의 바이트 수입니다. 여기에는 호스트 MAC 블록 유형 및 길이 필드의 8바이트에 그 뒤의 호스트 MAC 주소 데이터 바이트 수를 더한 값이 포함됩니다.
호스트 MAC 주소 데이터	variable	4.9 이상 버전용 호스트 MAC 주소, 페이지 4-117에 설명되어 있는 호스트 MAC 주소 데이터 필드입니다.
호스트 마지막 확인	uint32	시스템이 호스트 활동을 마지막으로 탐지한 시간을 나타내는 UNIX 타임스탬프입니다.

표 B-26 5.0~5.0.2 버전용 호스트 프로파일 데이터 블록 필드 (계속)

필드	데이터 유형	설명
호스트 유형	uint32	호스트 유형을 나타냅니다. 다음 값이 표시될 수 있습니다. • 0 - 호스트 • 1 - 라우터 • 2 - 브리지 • 3 - NAT 디바이스 • 4 - LB(로드 밸런서)
VLAN 유무	uint8	VLAN의 유무를 나타냅니다. • 0 - 예 • 1 - 아니요
VLAN ID	uint16	호스트가 구성원으로 포함된 VLAN을 나타내는 VLAN ID 번호입니다.
VLAN 유형	uint8	VLAN 태그에 캡슐화된 패킷 유형입니다.
VLAN 우선순위	uint8	VLAN 태그에 포함된 우선순위 값입니다.
일반 목록 블록 유형	uint32	클라이언트 애플리케이션 데이터를 전달하는 클라이언트 애플리케이션 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 클라이언트 애플리케이션 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
클라이언트 애플리케이션 블록 유형	uint32	클라이언트 애플리케이션 블록을 시작합니다. 이 값은 항상 5입니다.
클라이언트 애플리케이션 블록 길이	uint32	클라이언트 애플리케이션 블록의 바이트 수입니다. 여기에는 클라이언트 애플리케이션 블록 유형 및 길이 필드의 8바이트에 그 뒤의 클라이언트 애플리케이션 데이터 바이트 수를 더한 값이 포함됩니다.
클라이언트 애플리케이션 데이터	variable	5.0 이상 버전용 호스트 클라이언트 애플리케이션 데이터 블록, 페이지 4-156에 설명되어 있는 클라이언트 애플리케이션을 설명하는 클라이언트 애플리케이션 데이터 필드입니다.
문자열 블록 유형	uint32	NetBIOS 이름에 대한 문자열 데이터 블록을 시작합니다. 이 값은 문자열 데이터를 나타내는 0으로 설정됩니다.
문자열 블록 길이	uint32	NetBIOS 이름 데이터 블록의 바이트 수를 나타냅니다. 여기에는 문자열 블록 유형 및 길이의 8바이트에 NetBIOS 이름의 바이트 수를 더한 값이 포함됩니다.
NetBIOS 문자열 데이터	variable	호스트 프로파일에 설명되어 있는 호스트의 NetBIOS 이름을 포함합니다.

레거시 OS 핑거프린트 데이터 블록

자세한 내용은 다음 섹션을 참조하십시오.

- 5.0~5.0.2 버전용 운영 체제 핑거프린트 데이터 블록, 페이지 B-127

5.0~5.0.2 버전용 운영 체제 핑거프린트 데이터 블록

운영 체제 핑거프린트 데이터 블록의 블록 유형은 87입니다. 이 블록은 핑거프린트 UUID(범용 고유 식별자)와 핑거프린트 유형, 핑거프린트 소스 유형 및 핑거프린트 소스 ID를 포함합니다. 다음 다이어그램에 5.0~5.0.2 버전용 운영 체제 핑거프린트 데이터 블록의 형식이 나와 있습니다.

다음 표에는 운영 체제 핑거프린트 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 B-27 운영 체제 핑거프린트 데이터 블록 필드

필드	데이터 유형	설명
운영 체제 핑거프린트 데이터 블록 유형	uint32	운영 체제 데이터 블록을 시작합니다. 이 값은 항상 87입니다.
운영 체제 데이터 블록 길이	uint32	운영 체제 핑거프린트 데이터 블록의 바이트 수입니다. 이 값은 항상 41(데이터 블록 유형 및 길이 필드의 8바이트 + 핑거프린트 UUID 값의 16바이트 + 핑거프린트 유형의 4바이트 + 핑거프린트 소스 유형의 4바이트 + 핑거프린트 소스 ID의 4바이트 + 마지막 확인 값의 4바이트 + TTL 차이의 1바이트)이어야 합니다.
핑거프린트 UUID	uint8[16]	운영 체제의 고유 식별자 역할을 하는 옥텟 형식의 핑거프린트 ID 번호입니다. 핑거프린트 UUID는 VDB(취약점 데이터베이스)의 운영 체제 이름, 벤더 및 버전에 매핑됩니다.
핑거프린트 유형	uint32	핑거프린트의 유형을 나타냅니다.

표 B-27 운영 체제 핑거프린트 데이터 블록 필드 (계속)

필드	데이터 유형	설명
핑거프린트소스 유형	uint32	운영 체제 핑거프린트를 제공한 소스의 유형(예: 사용자 또는 스캐너)을 나타냅니다.
핑거프린트 소스 ID	uint32	운영 체제 핑거프린트를 제공한 소스의 ID를 나타냅니다.
마지막 확인	uint32	트래픽에서 핑거프린트가 마지막으로 확인된 시간을 나타냅니다.
TTL 차이	uint8	핑거프린트의 TTL 값과 호스트 핑거프린트를 생성하는 데 사용되는 패킷에서 확인된 TTL 값 간 차이를 나타냅니다.

레거시 연결 데이터 구조

자세한 내용은 다음 섹션을 참조하십시오.

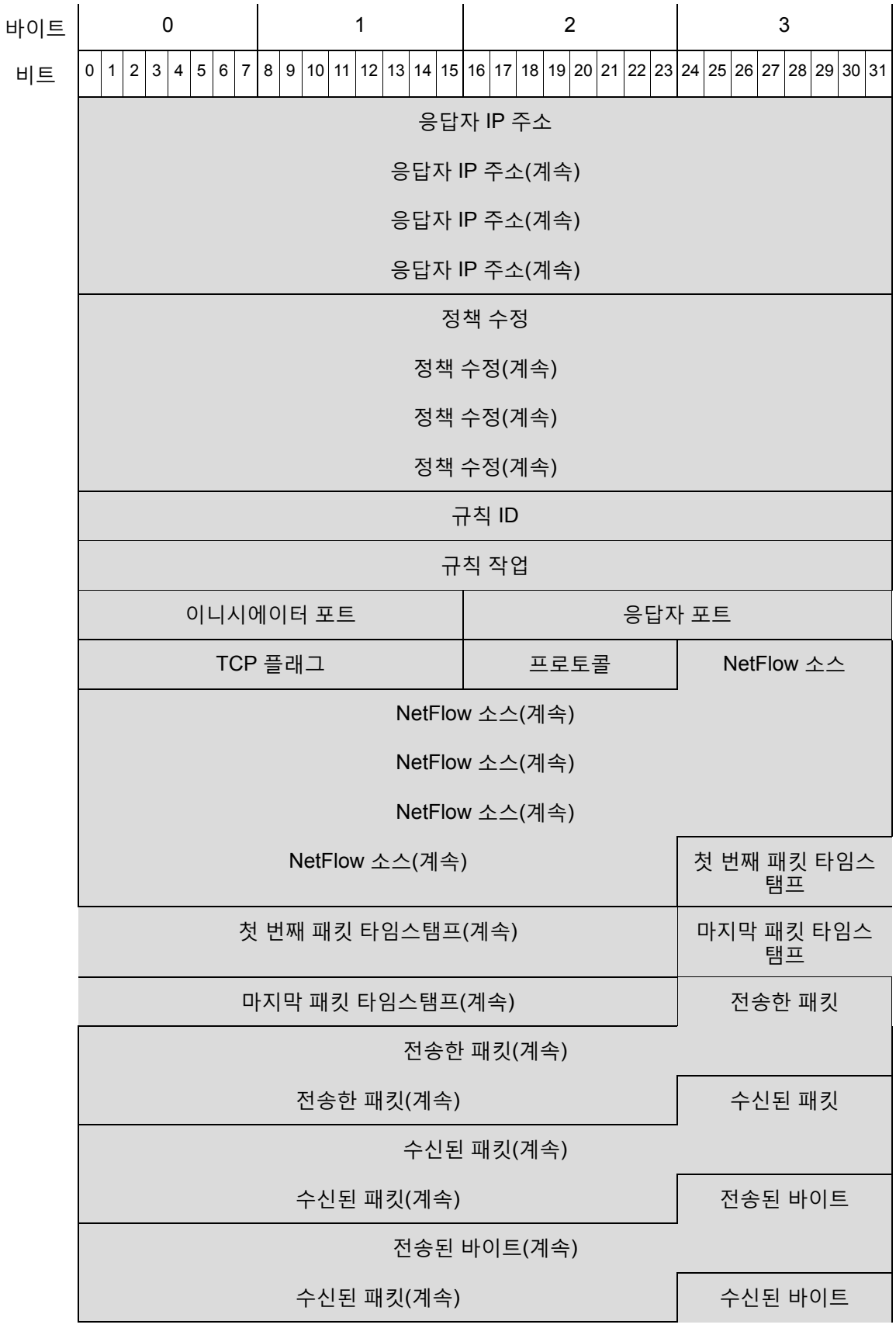
5.0~5.0.2 버전용 연결 통계 데이터 블록

연결 통계 데이터 블록은 연결 데이터 메시지에 사용됩니다. 5.0~5.0.2 버전용 연결 통계 데이터 블록의 블록 유형은 115입니다.

연결 통계 데이터 메시지에 대한 자세한 정보는 연결 통계 데이터 메시지, 페이지 4-54의 내용을 참조하십시오.

다음 다이어그램에 5.0~5.0.2 버전의 연결 통계 데이터 블록 형식이 나와 있습니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
연결 데이터 블록 유형(115)																																
연결 데이터 블록 길이																																
디바이스 ID																																
인그레스 영역 인그레스 영역(계속) 인그레스 영역(계속) 인그레스 영역(계속)																																
이그레스(egress) 영역 이그레스(egress) 영역(계속) 이그레스(egress) 영역(계속) 이그레스(egress) 영역(계속)																																
인그레스 인터페이스 인그레스 인터페이스(계속) 인그레스 인터페이스(계속) 인그레스 인터페이스(계속)																																
이그레스(egress) 인터페이스 이그레스(egress) 인터페이스(계속) 이그레스(egress) 인터페이스(계속) 이그레스(egress) 인터페이스(계속)																																
이니시에이터 IP 주소 이니시에이터 IP 주소(계속) 이니시에이터 IP 주소(계속) 이니시에이터 IP 주소(계속)																																


바이트
0
1
2
3
비트
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
응답자 IP 주소
응답자 IP 주소(계속)
응답자 IP 주소(계속)
응답자 IP 주소(계속)
정책 수정
정책 수정(계속)
정책 수정(계속)
정책 수정(계속)
규칙 ID
규칙 작업
이니시에이터 포트
응답자 포트
TCP 플래그
프로토콜
NetFlow 소스
NetFlow 소스(계속)
NetFlow 소스(계속)
NetFlow 소스(계속)
NetFlow 소스(계속)
첫 번째 패킷 타임스탬프
첫 번째 패킷 타임스탬프(계속)
마지막 패킷 타임스탬프
마지막 패킷 타임스탬프(계속)
전송한 패킷
전송한 패킷(계속)
전송한 패킷(계속)
수신된 패킷
수신된 패킷(계속)
수신된 패킷(계속)
전송된 바이트
전송된 바이트(계속)
수신된 패킷(계속)
수신된 바이트

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	수신된 바이트(계속)																															
	수신된 바이트(계속)																								사용자 ID							
	사용자 ID(계속)																								애플리케이션 프로토콜 ID							
	애플리케이션 프로토콜 ID(계속)																								URL 카테고리							
	URL 카테고리(계속)																								URL 평판							
	URL 평판(계속)																								클라이언트 애플리케이션 ID							
	클라이언트 애플리케이션 ID(계속)																								웹 애플리케이션 ID							
	웹 애플리케이션 ID(계속)																								문자열 블록 유형(0)							
클라이언트 앱 URL	문자열 블록 유형(계속)																								문자열 블록 길이							
	문자열 블록 길이(계속)																								클라이언트 애플리케이션 URL...							
NetBIOS 이름	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	NetBIOS 이름...																															
클라이언트 애플리케이션 버전	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	클라이언트 애플리케이션 버전...																															

다음 표에는 5.0~5.0.2 버전용 연결 통계 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 B-28 5.0~5.0.2 버전용 연결 통계 데이터 블록 필드

필드	데이터 유형	설명
연결 통계 데이터 블록 유형	uint32	5.0~5.0.2 버전용 연결 통계 데이터 블록을 시작합니다. 값은 항상 115입니다.
연결 통계 데이터 블록 길이	uint32	연결 통계 데이터 블록의 바이트 수입니다. 여기에는 연결 통계 블록 유형 및 길이 필드의 8바이트에 그 뒤의 연결 데이터 바이트 수를 더한 값이 포함됩니다.
디바이스 ID	uint32	연결 이벤트를 탐지한 디바이스입니다.

표 B-28 5.0~5.0.2 버전용 연결 통계 데이터 블록 필드 (계속)

필드	데이터 유형	설명
인그레스 영역	uint8[16]	정책 위반을 트리거한 이벤트의 인그레스 보안 영역입니다.
이그레스 (egress) 영역	uint8[16]	정책 위반을 트리거한 이벤트의 이그레스(egress) 보안 영역입니다.
인그레스 인터페이스	uint8[16]	인바운드 트래픽용 인터페이스입니다.
이그레스 (egress) 인터페이스	uint8[16]	아웃바운드 트래픽용 인터페이스입니다.
이니시에이터 IP 주소	uint8[16]	연결 이벤트에서 설명하는 세션을 시작한 호스트의 IP 주소(IP 주소 옥텟 형식)입니다.
응답자 IP 주소	uint8[16]	시작 호스트에 응답한 호스트의 IP 주소(IP 주소 옥텟 형식)입니다.
정책 수정	uint8[16]	해당하는 경우 트리거된 상관관계와 관련된 규칙의 수정 번호입니다.
규칙 ID	uint32	해당하는 경우 이벤트를 트리거한 규칙의 내부 식별자입니다.
규칙 작업	uint32	해당 규칙(허용, 차단 등)에 대해 사용자 인터페이스에서 선택한 작업입니다.
이니시에이터 포트	uint16	시작 호스트에 사용되는 포트입니다.
응답자 포트	uint16	응답 호스트에 사용되는 포트입니다.
TCP 플래그	uint16	연결 이벤트에 대한 모든 TCP 플래그를 나타냅니다.
프로토콜	uint8	IANA에서 지정한 프로토콜 번호입니다.
NetFlow 소스	uint8[16]	연결에 대한 데이터를 내보낸 NetFlow 지원 디바이스의 IP 주소입니다.
첫 번째 패킷 타임스탬프	uint32	세션에서 첫 번째 패킷이 교환된 날짜의 시간의 UNIX 타임스탬프입니다.
마지막 패킷 타임스탬프	uint32	세션에서 마지막 패킷이 교환된 날짜의 시간의 UNIX 타임스탬프입니다.
전송한 패킷	uint64	시작 호스트에서 전송한 패킷 수입니다.
수신된 패킷	uint64	응답 호스트에서 전송한 패킷 수입니다.
전송된 바이트	uint64	시작 호스트에서 전송한 바이트 수입니다.
수신된 바이트	uint64	응답 호스트에서 전송한 바이트 수입니다.
사용자 ID	uint32	트래픽을 생성한 호스트에 마지막으로 로그인한 사용자의 내부 ID 번호입니다.
애플리케이션 프로토콜 ID	uint32	애플리케이션 프로토콜의 애플리케이션 ID입니다.
URL 카테고리	uint32	URL 카테고리의 내부 ID 번호입니다.
URL 평판	uint32	URL 평판의 내부 ID 번호입니다.
클라이언트 애플리케이션 ID	uint32	해당하는 경우 탐지된 클라이언트 애플리케이션의 내부 ID 번호입니다.

표 B-28 5.0~5.0.2 버전용 연결 통계 데이터 블록 필드 (계속)

필드	데이터 유형	설명
웹 애플리케이션 ID	uint32	해당하는 경우 탐지된 웹 애플리케이션의 내부 ID 번호입니다.
문자열 블록 유형	uint32	클라이언트 애플리케이션 URL에 대한 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	클라이언트 애플리케이션 URL 문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이 필드의 8바이트에 클라이언트 애플리케이션 URL 문자열의 바이트 수를 더한 값이 포함됩니다.
클라이언트 애플리케이션 URL	string	해당하는 경우 클라이언트 애플리케이션이 액세스한 URL입니다. 예를 들면 `/files/index.html`과 같습니다.
문자열 블록 유형	uint32	호스트 NetBIOS 이름에 대한 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이 필드의 8바이트에 NetBIOS 이름 문자열의 바이트 수를 더한 값이 포함됩니다.
NetBIOS 이름	string	호스트 NetBIOS 이름 문자열입니다.
문자열 블록 유형	uint32	클라이언트 애플리케이션 버전에 대한 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	클라이언트 애플리케이션 버전에 대한 문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이의 8바이트에 버전의 바이트 수를 더한 값이 포함됩니다.
클라이언트 애플리케이션 버전	string	클라이언트 애플리케이션 버전입니다.

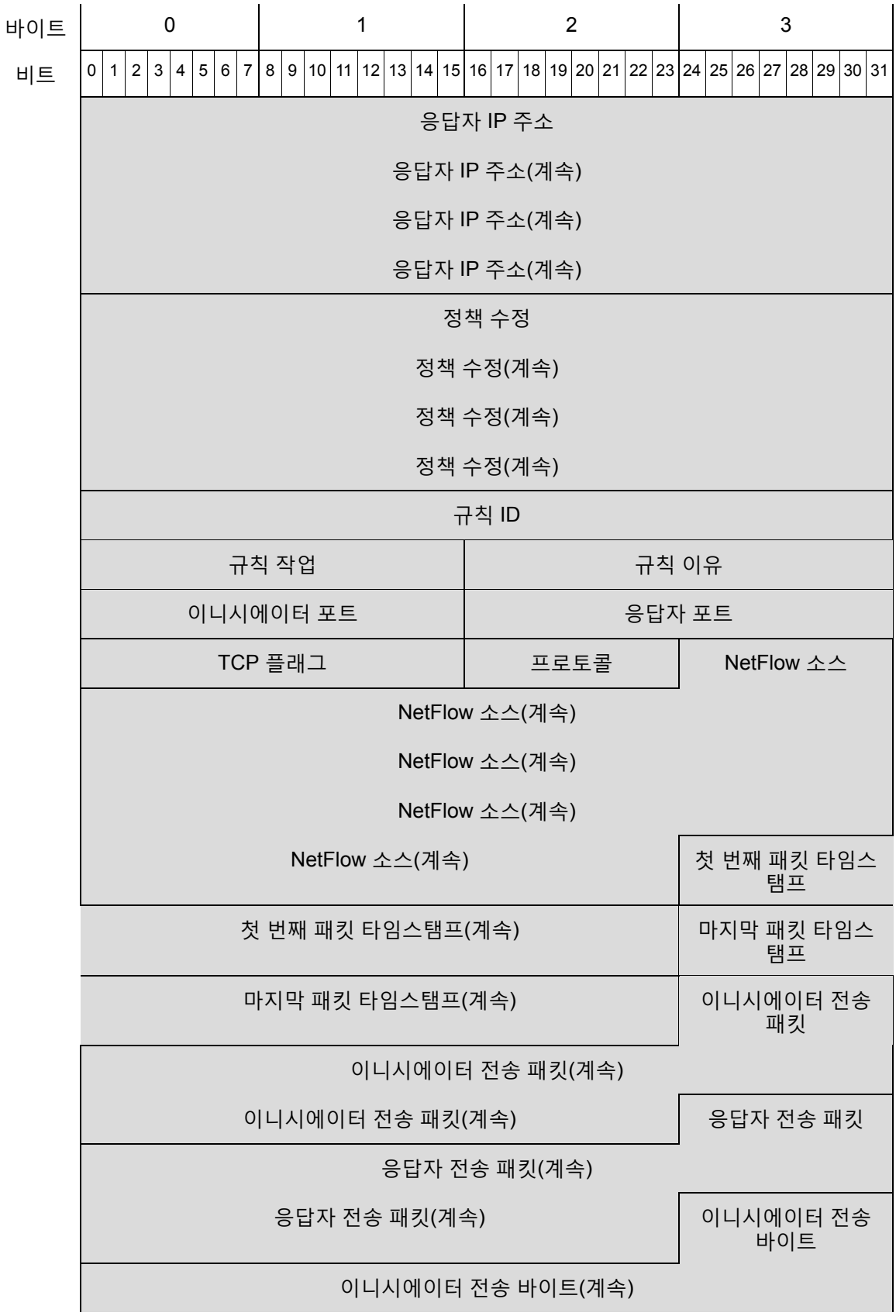
5.1 버전용 연결 통계 데이터 블록

연결 통계 데이터 블록은 연결 데이터 메시지에 사용됩니다. 5.0.2 버전과 비교할 때 5.1 버전에서 변경된 연결 데이터 블록 관련 사항으로는 5.1에 도입된 컨피그레이션 파라미터를 포함하는 새 필드(규칙 작업 이유, 모니터 규칙, 보안 인텔리전스 소스/대상, 보안 인텔리전스 계층)가 추가된 점이 포함됩니다. 5.1 버전용 연결 통계 데이터 블록의 블록 유형은 126입니다.

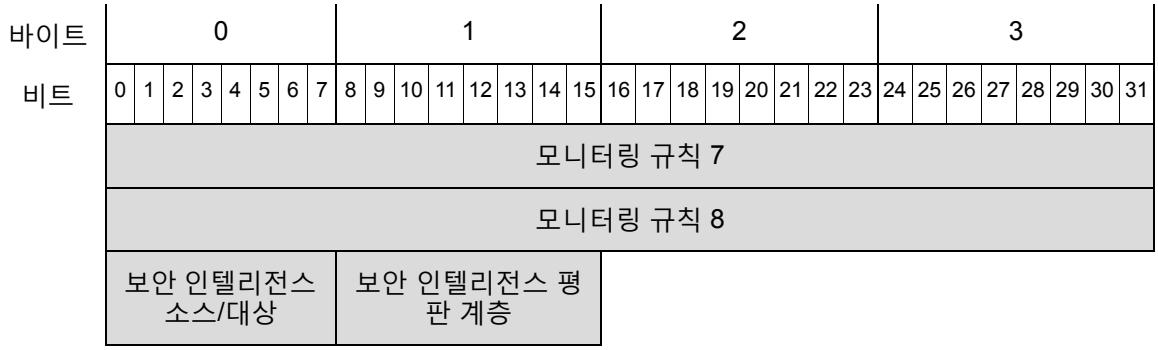
연결 통계 데이터 메시지에 대한 자세한 정보는 연결 통계 데이터 메시지, 페이지 4-54의 내용을 참조하십시오.

다음 다이어그램에 5.1 버전의 연결 통계 데이터 블록 형식이 나와 있습니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
연결 데이터 블록 유형(126)																																
연결 데이터 블록 길이																																
디바이스 ID																																
인그레스 영역 인그레스 영역(계속) 인그레스 영역(계속) 인그레스 영역(계속)																																
이그레스(egress) 영역 이그레스(egress) 영역(계속) 이그레스(egress) 영역(계속) 이그레스(egress) 영역(계속)																																
인그레스 인터페이스 인그레스 인터페이스(계속) 인그레스 인터페이스(계속) 인그레스 인터페이스(계속)																																
이그레스(egress) 인터페이스 이그레스(egress) 인터페이스(계속) 이그레스(egress) 인터페이스(계속) 이그레스(egress) 인터페이스(계속)																																
이니시에이터 IP 주소 이니시에이터 IP 주소(계속) 이니시에이터 IP 주소(계속) 이니시에이터 IP 주소(계속)																																


바이트
0
1
2
3
비트
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
응답자 IP 주소
응답자 IP 주소(계속)
응답자 IP 주소(계속)
응답자 IP 주소(계속)
정책 수정
정책 수정(계속)
정책 수정(계속)
정책 수정(계속)
규칙 ID
규칙 작업
규칙 이유
이니시에이터 포트
응답자 포트
TCP 플래그
프로토콜
NetFlow 소스
NetFlow 소스(계속)
NetFlow 소스(계속)
NetFlow 소스(계속)
NetFlow 소스(계속)
첫 번째 패킷 타임스탬프
첫 번째 패킷 타임스탬프(계속)
마지막 패킷 타임스탬프
마지막 패킷 타임스탬프(계속)
이니시에이터 전송 패킷
이니시에이터 전송 패킷(계속)
이니시에이터 전송 패킷(계속)
응답자 전송 패킷
응답자 전송 패킷(계속)
응답자 전송 패킷(계속)
이니시에이터 전송 바이트
이니시에이터 전송 바이트(계속)

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	이니시에이터 전송 바이트(계속)																								응답자 전송 바이트							
	응답자 전송 바이트(계속)																															
	응답자 전송 바이트(계속)																								사용자 ID							
	사용자 ID(계속)																								애플리케이션 프로토콜 ID							
	애플리케이션 프로토콜 ID(계속)																								URL 카테고리							
	URL 카테고리(계속)																								URL 평판							
	URL 평판(계속)																								클라이언트 애플리케이션 ID							
	클라이언트 애플리케이션 ID(계속)																								웹 애플리케이션 ID							
	웹 애플리케이션 ID(계속)																								문자열 블록 유형(0)							
클라이언트 앱 URL	문자열 블록 유형(계속)																								문자열 블록 길이							
	문자열 블록 길이(계속)																								클라이언트 애플리케이션 URL...							
NetBIOS 이름	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	NetBIOS 이름...																															
클라이언트 애플리케이션 버전	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	클라이언트 애플리케이션 버전...																															
	모니터링 규칙 1																															
	모니터링 규칙 2																															
	모니터링 규칙 3																															
	모니터링 규칙 4																															
	모니터링 규칙 5																															
	모니터링 규칙 6																															



다음 표에는 5.1 버전용 연결 통계 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 B-29 5.1 버전용 연결 통계 데이터 블록 필드

필드	데이터 유형	설명
연결 통계 데이터 블록 유형	uint32	5.1 버전용 연결 통계 데이터 블록을 시작합니다. 값은 항상 126입니다.
연결 통계 데이터 블록 길이	uint32	연결 통계 데이터 블록의 바이트 수입니다. 여기에는 연결 통계 블록 유형 및 길이 필드의 8바이트에 그 뒤의 연결 데이터 바이트 수를 더한 값이 포함됩니다.
디바이스 ID	uint32	연결 이벤트를 탐지한 디바이스입니다.
인그레스 영역	uint8[16]	정책 위반을 트리거한 이벤트의 인그레스 보안 영역입니다.
이그레스 (egress) 영역	uint8[16]	정책 위반을 트리거한 이벤트의 이그레스(egress) 보안 영역입니다.
인그레스 인터페이스	uint8[16]	인바운드 트래픽용 인터페이스입니다.
이그레스 (egress) 인터페이스	uint8[16]	아웃바운드 트래픽용 인터페이스입니다.
이니시에이터 IP 주소	uint8[16]	연결 이벤트에서 설명하는 세션을 시작한 호스트의 IP 주소(IP 주소 옥텟 형식)입니다.
응답자 IP 주소	uint8[16]	시작 호스트에 응답한 호스트의 IP 주소(IP 주소 옥텟 형식)입니다.
정책 수정	uint8[16]	해당하는 경우 트리거된 상관관계와 관련된 규칙의 수정 번호입니다.
규칙 ID	uint32	해당하는 경우 이벤트를 트리거한 규칙의 내부 식별자입니다.
규칙 작업	uint16	해당 규칙(허용, 차단 등)에 대해 사용자 인터페이스에서 선택한 작업입니다.
규칙 이유	uint16	규칙이 이벤트를 트리거한 이유입니다.
이니시에이터 포트	uint16	시작 호스트에 사용되는 포트입니다.
응답자 포트	uint16	응답 호스트에 사용되는 포트입니다.
TCP 플래그	uint16	연결 이벤트에 대한 모든 TCP 플래그를 나타냅니다.
프로토콜	uint8	IANA에서 지정한 프로토콜 번호입니다.

표 B-29 5.1 버전용 연결 통계 데이터 블록 필드 (계속)

필드	데이터 유형	설명
NetFlow 소스	uint8[16]	연결에 대한 데이터를 내보낸 NetFlow 지원 디바이스의 IP 주소입니다.
첫 번째 패킷 타임스탬프	uint32	세션에서 첫 번째 패킷이 교환된 날짜의 시간의 UNIX 타임스탬프입니다.
마지막 패킷 타임스탬프	uint32	세션에서 마지막 패킷이 교환된 날짜의 시간의 UNIX 타임스탬프입니다.
이니시에이터 전송 패킷	uint64	시작 호스트에서 전송한 패킷 수입니다.
응답자 전송 패킷	uint64	응답 호스트에서 전송한 패킷 수입니다.
이니시에이터 전송 바이트	uint64	시작 호스트에서 전송한 바이트 수입니다.
응답자 전송 바이트	uint64	응답 호스트에서 전송한 바이트 수입니다.
사용자 ID	uint32	트래픽을 생성한 호스트에 마지막으로 로그인한 사용자의 내부 ID 번호입니다.
애플리케이션 프로토콜 ID	uint32	애플리케이션 프로토콜의 애플리케이션 ID입니다.
URL 카테고리	uint32	URL 카테고리의 내부 ID 번호입니다.
URL 평판	uint32	URL 평판의 내부 ID 번호입니다.
클라이언트 애플리케이션 ID	uint32	해당하는 경우 탐지된 클라이언트 애플리케이션의 내부 ID 번호입니다.
웹 애플리케이션 ID	uint32	해당하는 경우 탐지된 웹 애플리케이션의 내부 ID 번호입니다.
문자열 블록 유형	uint32	클라이언트 애플리케이션 URL에 대한 문자열 데이터 블록을 시작합니다. 이 값은 항상 `0`입니다.
문자열 블록 길이	uint32	클라이언트 애플리케이션 URL 문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이 필드의 8바이트에 클라이언트 애플리케이션 URL 문자열의 바이트 수를 더한 값이 포함됩니다.
클라이언트 애플리케이션 URL	string	해당하는 경우 클라이언트 애플리케이션이 액세스한 URL입니다. 예를 들면 `/files/index.html`과 같습니다.
문자열 블록 유형	uint32	호스트 NetBIOS 이름에 대한 문자열 데이터 블록을 시작합니다. 이 값은 항상 `0`입니다.
문자열 블록 길이	uint32	문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이 필드의 8바이트에 NetBIOS 이름 문자열의 바이트 수를 더한 값이 포함됩니다.
NetBIOS 이름	string	호스트 NetBIOS 이름 문자열입니다.
문자열 블록 유형	uint32	클라이언트 애플리케이션 버전에 대한 문자열 데이터 블록을 시작합니다. 이 값은 항상 `0`입니다.
문자열 블록 길이	uint32	클라이언트 애플리케이션 버전에 대한 문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이의 8바이트에 버전의 바이트 수를 더한 값이 포함됩니다.

표 B-29 5.1 버전용 연결 통계 데이터 블록 필드 (계속)

필드	데이터 유형	설명
클라이언트 애플리케이션 버전	string	클라이언트 애플리케이션 버전입니다.
모니터링 규칙 1	uint32	연결 이벤트와 관련된 첫 번째 모니터 규칙의 ID입니다.
모니터링 규칙 2	uint32	연결 이벤트와 관련된 두 번째 모니터 규칙의 ID입니다.
모니터링 규칙 3	uint32	연결 이벤트와 관련된 세 번째 모니터 규칙의 ID입니다.
모니터링 규칙 4	uint32	연결 이벤트와 관련된 네 번째 모니터 규칙의 ID입니다.
모니터링 규칙 5	uint32	연결 이벤트와 관련된 다섯 번째 모니터 규칙의 ID입니다.
모니터링 규칙 6	uint32	연결 이벤트와 관련된 여섯 번째 모니터 규칙의 ID입니다.
모니터링 규칙 7	uint32	연결 이벤트와 관련된 일곱 번째 모니터 규칙의 ID입니다.
모니터링 규칙 8	uint32	연결 이벤트와 관련된 여덟 번째 모니터 규칙의 ID입니다.
보안 인텔리전스 소스/대상	uint8	소스 또는 대상 IP 주소가 IP 블랙리스트와 일치했는지를 나타냅니다.
보안 인텔리전스 계층	uint8	IP 블랙리스트와 일치한 IP 계층입니다.

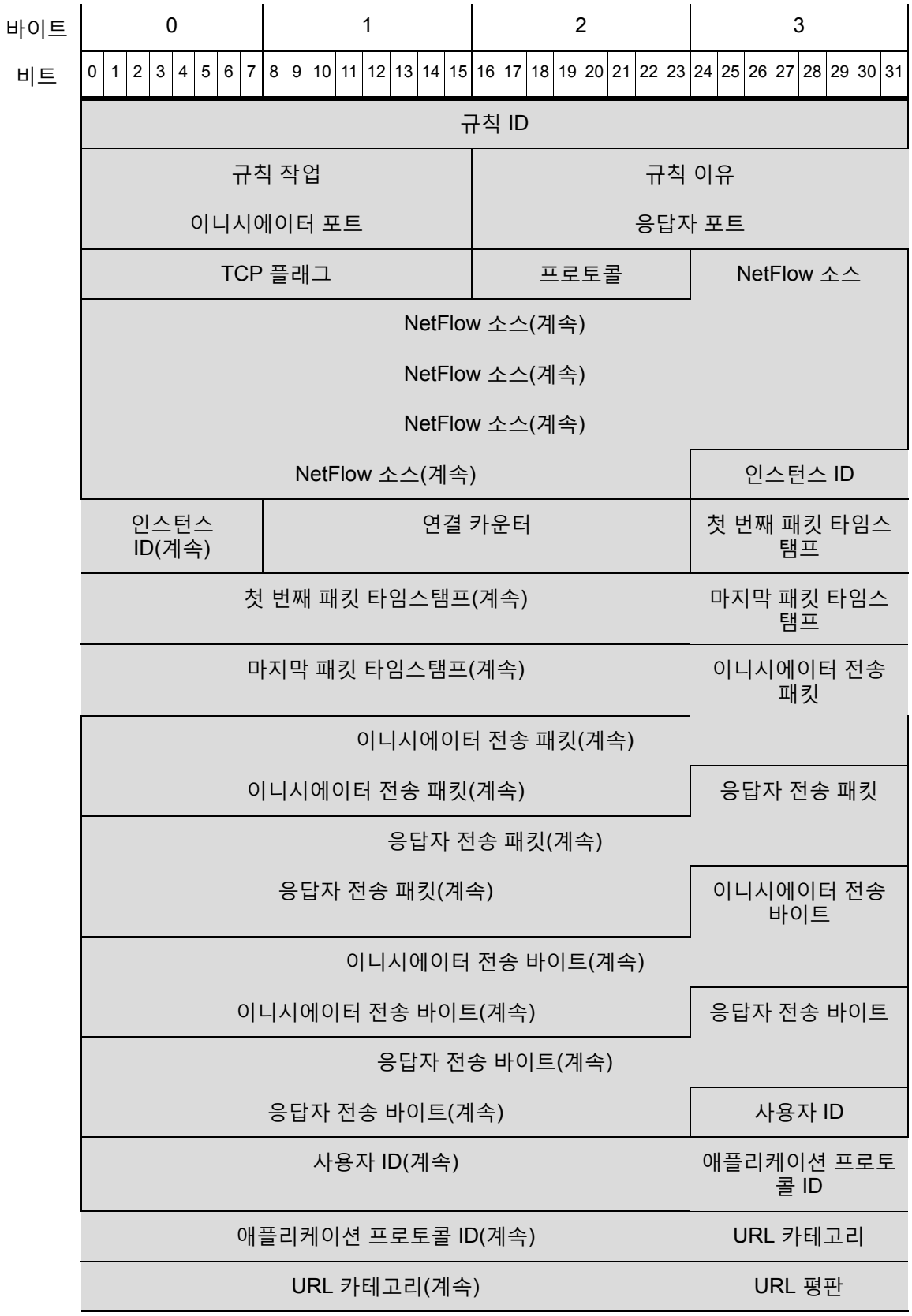
5.2.x 버전용 연결 통계 데이터 블록

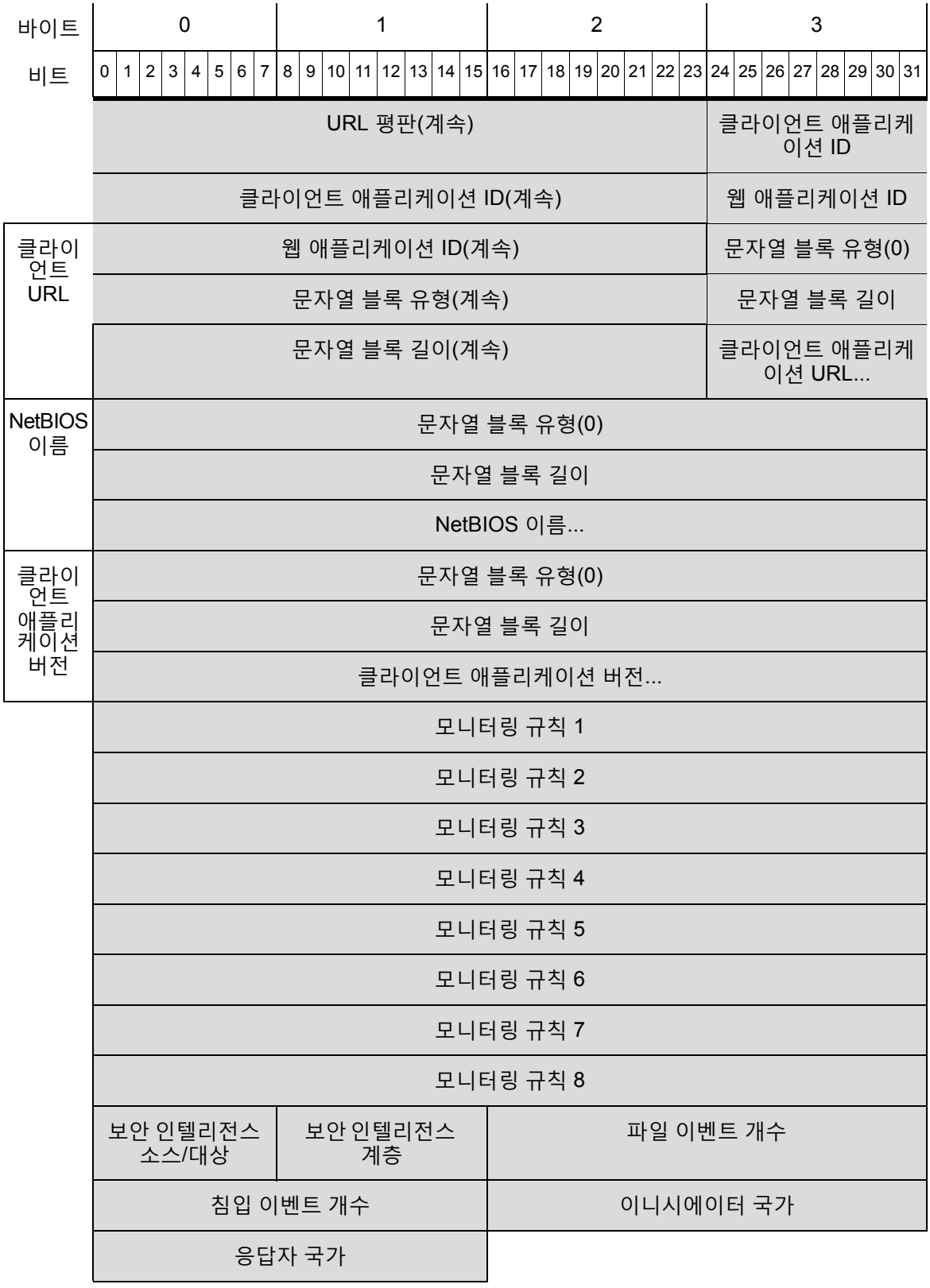
연결 통계 데이터 블록은 연결 데이터 메시지에 사용됩니다. 5.1.1 버전과 비교할 때 5.2 버전에서 변경된 연결 데이터 블록 관련 사항으로는 지리위치를 지원하기 위해 새 필드가 추가된 점이 포함됩니다. 계열 1 블록 그룹에서 5.2.x 버전용 연결 통계 데이터 블록의 블록 유형은 144입니다. 이는 블록 유형 137(5.1.1.x 버전용 연결 통계 데이터 블록, 페이지 B-148)의 사용을 중단합니다.

연결 통계 데이터 메시지에 대한 자세한 정보는 연결 통계 데이터 메시지, 페이지 4-54의 내용을 참조하십시오.

다음 다이어그램에 5.2.x 버전의 연결 통계 데이터 블록 형식이 나와 있습니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
이그레스(egress) 영역																																
이그레스(egress) 영역(계속)																																
이그레스(egress) 영역(계속)																																
이그레스(egress) 영역(계속)																																
인그레스 인터페이스																																
인그레스 인터페이스(계속)																																
인그레스 인터페이스(계속)																																
인그레스 인터페이스(계속)																																
이그레스(egress) 인터페이스																																
이그레스(egress) 인터페이스(계속)																																
이그레스(egress) 인터페이스(계속)																																
이그레스(egress) 인터페이스(계속)																																
이니시에이터 IP 주소																																
이니시에이터 IP 주소(계속)																																
이니시에이터 IP 주소(계속)																																
이니시에이터 IP 주소(계속)																																
응답자 IP 주소																																
응답자 IP 주소(계속)																																
응답자 IP 주소(계속)																																
응답자 IP 주소(계속)																																
정책 수정																																
정책 수정(계속)																																
정책 수정(계속)																																
정책 수정(계속)																																


바이트
0
1
2
3
비트
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
규칙 ID
규칙 작업
규칙 이유
이니시에이터 포트
응답자 포트
TCP 플래그
프로토콜
NetFlow 소스
NetFlow 소스(계속)
NetFlow 소스(계속)
NetFlow 소스(계속)
NetFlow 소스(계속)
인스턴스 ID
인스턴스 ID(계속)
연결 카운터
첫 번째 패킷 타임스탬프
첫 번째 패킷 타임스탬프(계속)
마지막 패킷 타임스탬프
마지막 패킷 타임스탬프(계속)
이니시에이터 전송 패킷
이니시에이터 전송 패킷(계속)
이니시에이터 전송 패킷(계속)
응답자 전송 패킷
응답자 전송 패킷(계속)
응답자 전송 패킷(계속)
이니시에이터 전송 바이트
이니시에이터 전송 바이트(계속)
이니시에이터 전송 바이트(계속)
응답자 전송 바이트
응답자 전송 바이트(계속)
응답자 전송 바이트(계속)
사용자 ID
사용자 ID(계속)
애플리케이션 프로토콜 ID
애플리케이션 프로토콜 ID(계속)
URL 카테고리
URL 카테고리(계속)
URL 평판


바이트
0
1
2
3
비트
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
URL 평판(계속)
클라이언트 애플리케이션 ID
클라이언트 애플리케이션 ID(계속)
웹 애플리케이션 ID
클라이언트 URL
웹 애플리케이션 ID(계속)
문자열 블록 유형(0)
문자열 블록 유형(계속)
문자열 블록 길이
문자열 블록 길이(계속)
클라이언트 애플리케이션 URL...
NetBIOS 이름
문자열 블록 유형(0)
문자열 블록 길이
NetBIOS 이름...
클라이언트 애플리케이션 버전
문자열 블록 유형(0)
문자열 블록 길이
클라이언트 애플리케이션 버전...
모니터링 규칙 1
모니터링 규칙 2
모니터링 규칙 3
모니터링 규칙 4
모니터링 규칙 5
모니터링 규칙 6
모니터링 규칙 7
모니터링 규칙 8
보안 인텔리전스 소스/대상
보안 인텔리전스 계층
파일 이벤트 개수
침입 이벤트 개수
이니시에이터 국가
응답자 국가

다음 표에는 5.2.x 버전용 연결 통계 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 B-30 5.2.x 버전용 연결 통계 데이터 블록 필드

필드	데이터 유형	설명
연결 통계 데이터 블록 유형	uint32	5.2.x 버전용 연결 통계 데이터 블록을 시작합니다. 값은 항상 144입니다.
연결 통계 데이터 블록 길이	uint32	연결 통계 데이터 블록의 바이트 수입니다. 여기에는 연결 통계 블록 유형 및 길이 필드의 8바이트에 그 뒤의 연결 데이터 바이트 수를 더한 값이 포함됩니다.
디바이스 ID	uint32	연결 이벤트를 탐지한 디바이스입니다.
인그레스 영역	uint8[16]	정책 위반을 트리거한 이벤트의 인그레스 보안 영역입니다.
이그레스(egress) 영역	uint8[16]	정책 위반을 트리거한 이벤트의 이그레스(egress) 보안 영역입니다.
인그레스 인터페이스	uint8[16]	인바운드 트래픽용 인터페이스입니다.
이그레스(egress) 인터페이스	uint8[16]	아웃바운드 트래픽용 인터페이스입니다.
이니시에이터 IP 주소	uint8[16]	연결 이벤트에서 설명하는 세션을 시작한 호스트의 IP 주소(IP 주소 옥텟 형식)입니다.
응답자 IP 주소	uint8[16]	시작 호스트에 응답한 호스트의 IP 주소(IP 주소 옥텟 형식)입니다.
정책 수정	uint8[16]	해당하는 경우 트리거된 상관관계와 관련된 규칙의 수정 번호입니다.
규칙 ID	uint32	해당하는 경우 이벤트를 트리거한 규칙의 내부 식별자입니다.
규칙 작업	uint16	해당 규칙(허용, 차단 등)에 대해 사용자 인터페이스에서 선택한 작업입니다.
규칙 이유	uint16	규칙이 이벤트를 트리거한 이유입니다.
이니시에이터 포트	uint16	시작 호스트에 사용되는 포트입니다.
응답자 포트	uint16	응답 호스트에 사용되는 포트입니다.
TCP 플래그	uint16	연결 이벤트에 대한 모든 TCP 플래그를 나타냅니다.
프로토콜	uint8	IANA에서 지정한 프로토콜 번호입니다.
NetFlow 소스	uint8[16]	연결에 대한 데이터를 내보낸 NetFlow 지원 디바이스의 IP 주소입니다.
인스턴스 ID	uint16	이벤트를 생성한 매니지드 디바이스의 Snort 인스턴스의 숫자 ID입니다.
연결 카운터	uint16	1초 이내에 발생하는 연결 이벤트를 구별하는 데 사용되는 값입니다.
첫 번째 패킷 타임스탬프	uint32	세션에서 첫 번째 패킷이 교환된 날짜의 시간의 UNIX 타임스탬프입니다.
마지막 패킷 타임스탬프	uint32	세션에서 마지막 패킷이 교환된 날짜의 시간의 UNIX 타임스탬프입니다.
이니시에이터 전송 패킷	uint64	시작 호스트에서 전송한 패킷 수입니다.

표 B-30 5.2.x 버전용 연결 통계 데이터 블록 필드 (계속)

필드	데이터 유형	설명
응답자 전송 패킷	uint64	응답 호스트에서 전송한 패킷 수입니다.
이니시에이터 전송 바이트	uint64	시작 호스트에서 전송한 바이트 수입니다.
응답자 전송 바이트	uint64	응답 호스트에서 전송한 바이트 수입니다.
사용자 ID	uint32	트래픽을 생성한 호스트에 마지막으로 로그인한 사용자의 내부 ID 번호입니다.
애플리케이션 프로토콜 ID	uint32	애플리케이션 프로토콜의 애플리케이션 ID입니다.
URL 카테고리	uint32	URL 카테고리의 내부 ID 번호입니다.
URL 평판	uint32	URL 평판의 내부 ID 번호입니다.
클라이언트 애플리케이션 ID	uint32	해당하는 경우 탐지된 클라이언트 애플리케이션의 내부 ID 번호입니다.
웹 애플리케이션 ID	uint32	해당하는 경우 탐지된 웹 애플리케이션의 내부 ID 번호입니다.
문자열 블록 유형	uint32	클라이언트 애플리케이션 URL에 대한 문자열 데이터 블록을 시작합니다. 이 값은 항상 `0`입니다.
문자열 블록 길이	uint32	클라이언트 애플리케이션 URL 문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이 필드의 8바이트에 클라이언트 애플리케이션 URL 문자열의 바이트 수를 더한 값이 포함됩니다.
클라이언트 애플리케이션 URL	string	해당하는 경우 클라이언트 애플리케이션이 액세스한 URL입니다. 예를 들면 `/files/index.html`과 같습니다.
문자열 블록 유형	uint32	호스트 NetBIOS 이름에 대한 문자열 데이터 블록을 시작합니다. 이 값은 항상 `0`입니다.
문자열 블록 길이	uint32	문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이 필드의 8바이트에 NetBIOS 이름 문자열의 바이트 수를 더한 값이 포함됩니다.
NetBIOS 이름	string	호스트 NetBIOS 이름 문자열입니다.
문자열 블록 유형	uint32	클라이언트 애플리케이션 버전에 대한 문자열 데이터 블록을 시작합니다. 이 값은 항상 `0`입니다.
문자열 블록 길이	uint32	클라이언트 애플리케이션 버전에 대한 문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이의 8바이트에 버전의 바이트 수를 더한 값이 포함됩니다.
클라이언트 애플리케이션 버전	string	클라이언트 애플리케이션 버전입니다.
모니터링 규칙 1	uint32	연결 이벤트와 관련된 첫 번째 모니터 규칙의 ID입니다.
모니터링 규칙 2	uint32	연결 이벤트와 관련된 두 번째 모니터 규칙의 ID입니다.
모니터링 규칙 3	uint32	연결 이벤트와 관련된 세 번째 모니터 규칙의 ID입니다.
모니터링 규칙 4	uint32	연결 이벤트와 관련된 네 번째 모니터 규칙의 ID입니다.
모니터링 규칙 5	uint32	연결 이벤트와 관련된 다섯 번째 모니터 규칙의 ID입니다.
모니터링 규칙 6	uint32	연결 이벤트와 관련된 여섯 번째 모니터 규칙의 ID입니다.

표 B-30 5.2.x 버전용 연결 통계 데이터 블록 필드 (계속)

필드	데이터 유형	설명
모니터링 규칙 7	uint32	연결 이벤트와 관련된 일곱 번째 모니터 규칙의 ID입니다.
모니터링 규칙 8	uint32	연결 이벤트와 관련된 여덟 번째 모니터 규칙의 ID입니다.
보안 인텔리전스 소스/대상	uint8	소스 또는 대상 IP 주소가 IP 블랙리스트와 일치했는지를 나타냅니다.
보안 인텔리전스 계층	uint8	IP 블랙리스트와 일치한 IP 계층입니다.
파일 이벤트 개수	uint16	1초 이내에 발생하는 파일 이벤트를 구별하는 데 사용되는 값입니다.
침입 이벤트 개수	uint16	1초 이내에 발생하는 침입 이벤트를 구별하는 데 사용되는 값입니다.
이니시에이터 국가	uint16	시작 호스트의 국가 코드입니다.
응답자 국가	uint16	응답 호스트의 국가 코드입니다.

5.0~5.1 버전용 연결 청크 데이터 블록

연결 청크 데이터 블록은 NetFlow 디바이스가 탐지한 연결 데이터를 전달합니다. 연결 청크 데이터 블록의 블록 유형은 4.10.1 이전 버전의 경우 66, 5.0~5.1 버전의 경우 119입니다.

다음 다이어그램에 연결 청크 데이터 블록의 형식이 나와 있습니다.

다음 표에는 연결 청크 데이터 블록의 구성 요소에 대한 설명이 나와 있습니다.

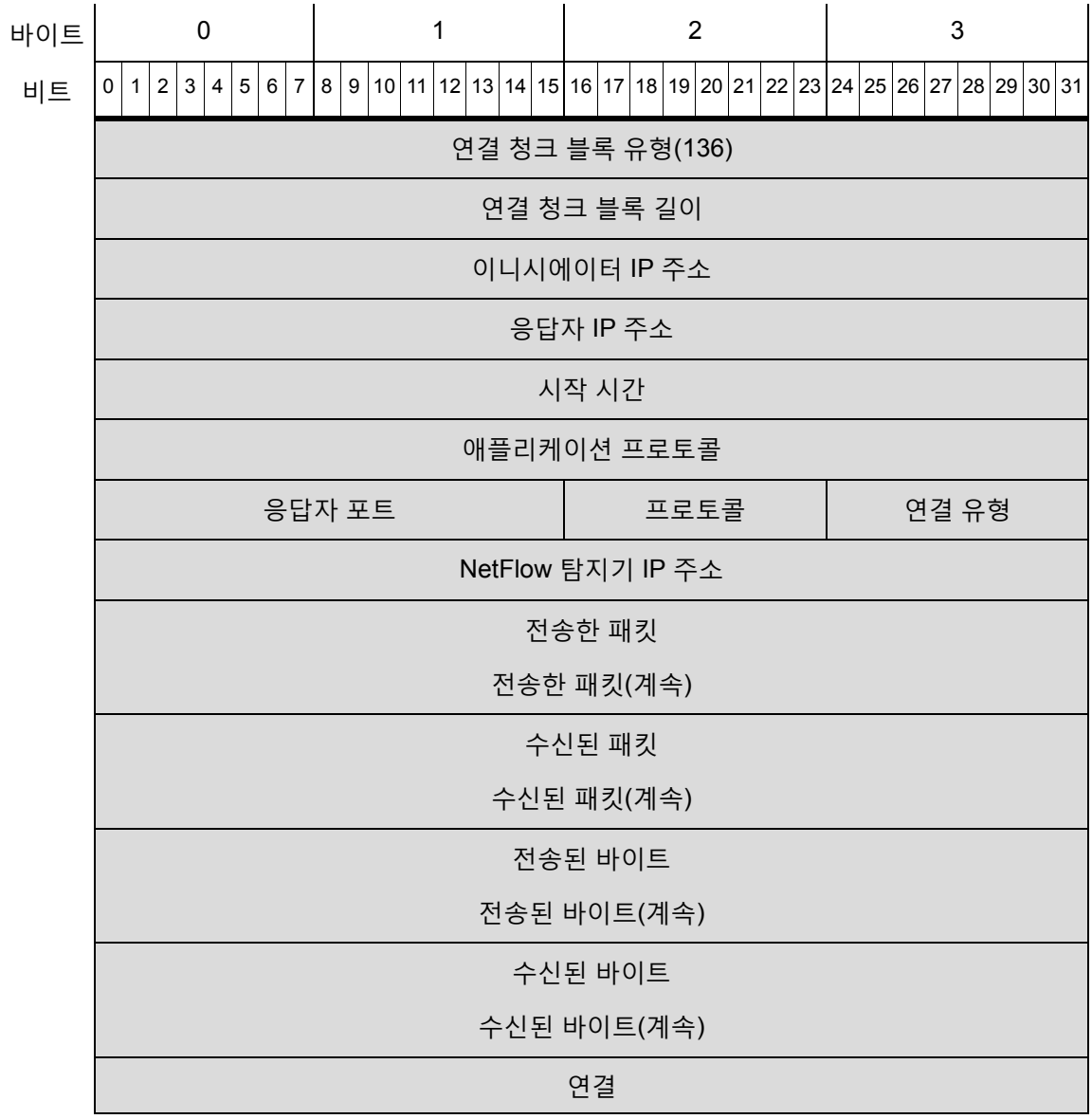
표 B-31 연결 청크 데이터 블록 필드

필드	데이터 유형	설명
연결 청크 블록 유형	uint32	연결 청크 데이터 블록을 시작합니다. 이 값은 4.10.1 이전 버전의 경우 66, 5.0 버전의 경우 119입니다.
연결 청크 블록 길이	uint32	연결 청크 데이터 블록의 총 바이트 수입니다. 여기에는 연결 청크 블록 유형 및 길이 필드의 8바이트에 그 뒤의 연결 청크 데이터 바이트 수를 더한 값이 포함됩니다.
이니시에이터 IP 주소	uint8[4]	연결을 시작한 호스트의 IP 주소(IP 주소 옥텟 형식)입니다.
응답자 IP 주소	uint8[4]	연결에 응답하는 호스트의 IP 주소(IP 주소 옥텟 형식)입니다.
시작 시간	uint32	연결 청크의 시작 시간입니다.
애플리케이션 ID	uint32	연결에 사용된 애플리케이션 프로토콜의 애플리케이션 ID 번호입니다.
응답자 포트	uint16	연결 청크의 응답자가 사용하는 포트입니다.
프로토콜	uint8	사용자 정보를 포함하는 패킷의 프로토콜입니다.
연결 유형	uint8	연결의 유형입니다.
소스 디바이스 IP 주소	uint8[4]	연결을 탐지한 NetFlow 디바이스의 IP 주소(IP 주소 옥텟 형식)입니다.
전송한 패킷	uint32	연결 청크에서 보낸 패킷의 수입니다.
수신된 패킷	uint32	연결 청크에서 받은 패킷의 수입니다.
전송된 바이트	uint32	연결 청크에서 보낸 바이트 수입니다.
수신된 바이트	uint32	연결 청크에서 받은 바이트 수입니다.
연결	uint32	연결 청크에서 실행된 세션의 수입니다.

5.1.1~6.0.x 버전용 연결 청크 데이터 블록

연결 청크 데이터 블록은 연결 데이터를 전달하며 5분 동안 누적된 연결 로그 데이터를 저장합니다. 계열 1 블록 그룹에서 연결 청크 데이터 블록의 블록 유형은 136입니다. 이는 블록 유형 119를 대체합니다.

다음 다이어그램에 연결 청크 데이터 블록의 형식이 나와 있습니다.



다음 표에는 연결 청크 데이터 블록의 구성 요소에 대한 설명이 나와 있습니다.

표 B-32 연결 청크 데이터 블록 필드

필드	데이터 유형	설명
연결 청크 블록 유형	uint32	연결 청크 데이터 블록을 시작합니다. 이 값은 항상 136입니다.
연결 청크 블록 길이	uint32	연결 청크 데이터 블록의 총 바이트 수입니다. 여기에는 연결 청크 블록 유형 및 길이 필드의 8바이트에 그 뒤의 연결 청크 데이터 바이트 수를 더한 값이 포함됩니다.
이니시에이터 IP 주소	uint8(4)	이 연결 유형의 이니시에이터 IP 주소입니다. 이 주소는 응답자 IP 주소와 함께 동일한 연결을 식별하는 데 사용됩니다.
응답자 IP 주소	uint8(4)	이 연결 유형의 응답자 IP 주소입니다. 이 주소는 이니시에이터 IP 주소와 함께 동일한 연결을 식별하는 데 사용됩니다.
시작 시간	uint32	연결 청크의 시작 시간입니다.
애플리케이션 프로토콜	uint32	연결에 사용된 프로토콜의 ID 번호입니다.
응답자 포트	uint16	연결 청크의 응답자가 사용하는 포트입니다.
프로토콜	uint8	사용자 정보를 포함하는 패킷의 프로토콜입니다.
연결 유형	uint8	연결의 유형입니다.
NetFlow 탐지기 IP 주소	uint8[4]	연결을 탐지한 NetFlow 디바이스의 IP 주소(IP 주소 옥텟 형식)입니다.
전송한 패킷	uint64	연결 청크에서 보낸 패킷의 수입니다.
수신된 패킷	uint64	연결 청크에서 받은 패킷의 수입니다.
전송된 바이트	uint64	연결 청크에서 보낸 바이트 수입니다.
수신된 바이트	uint64	연결 청크에서 받은 바이트 수입니다.
연결	uint32	5분 동안의 연결 수입니다.

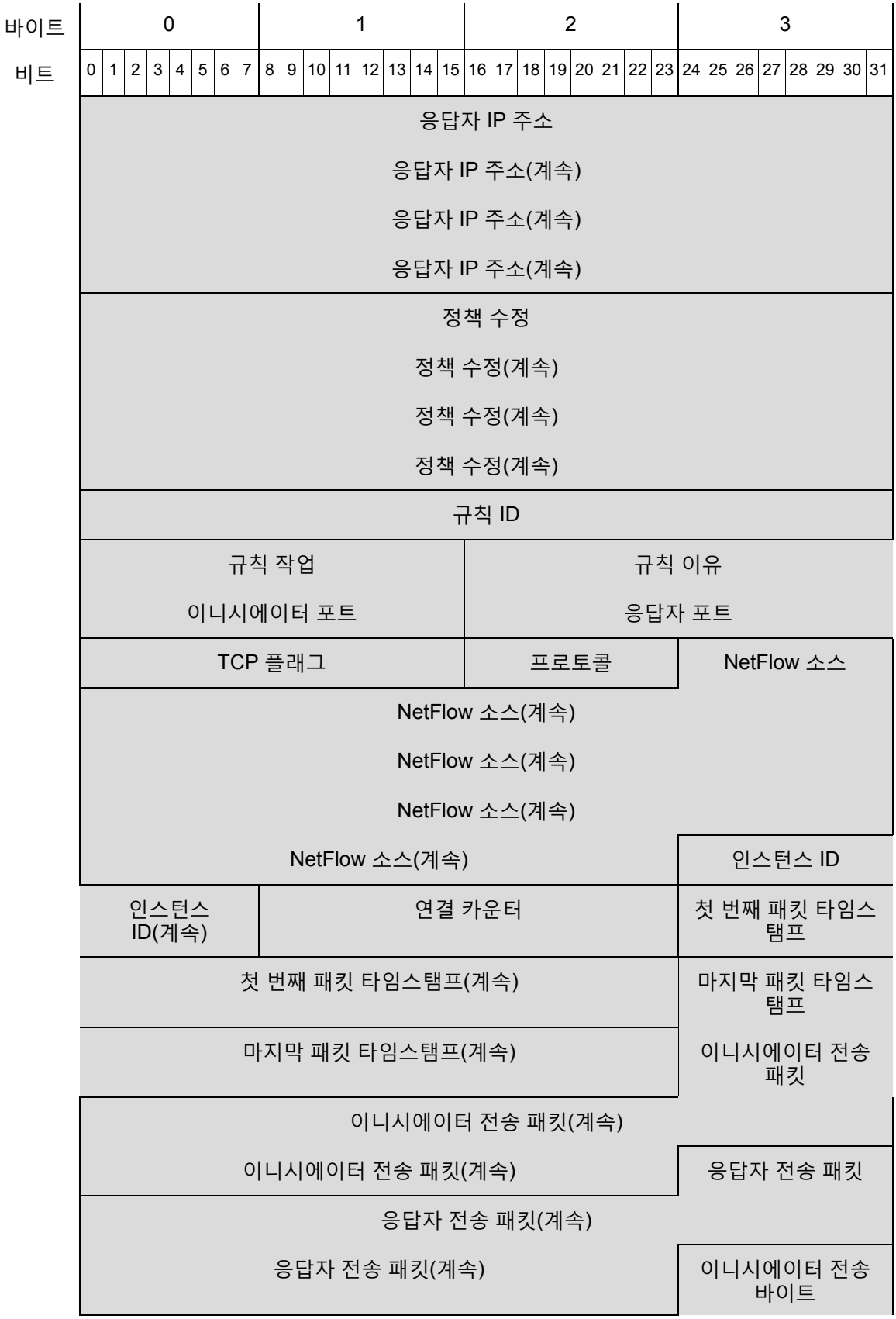
5.1.1.x 버전용 연결 통계 데이터 블록

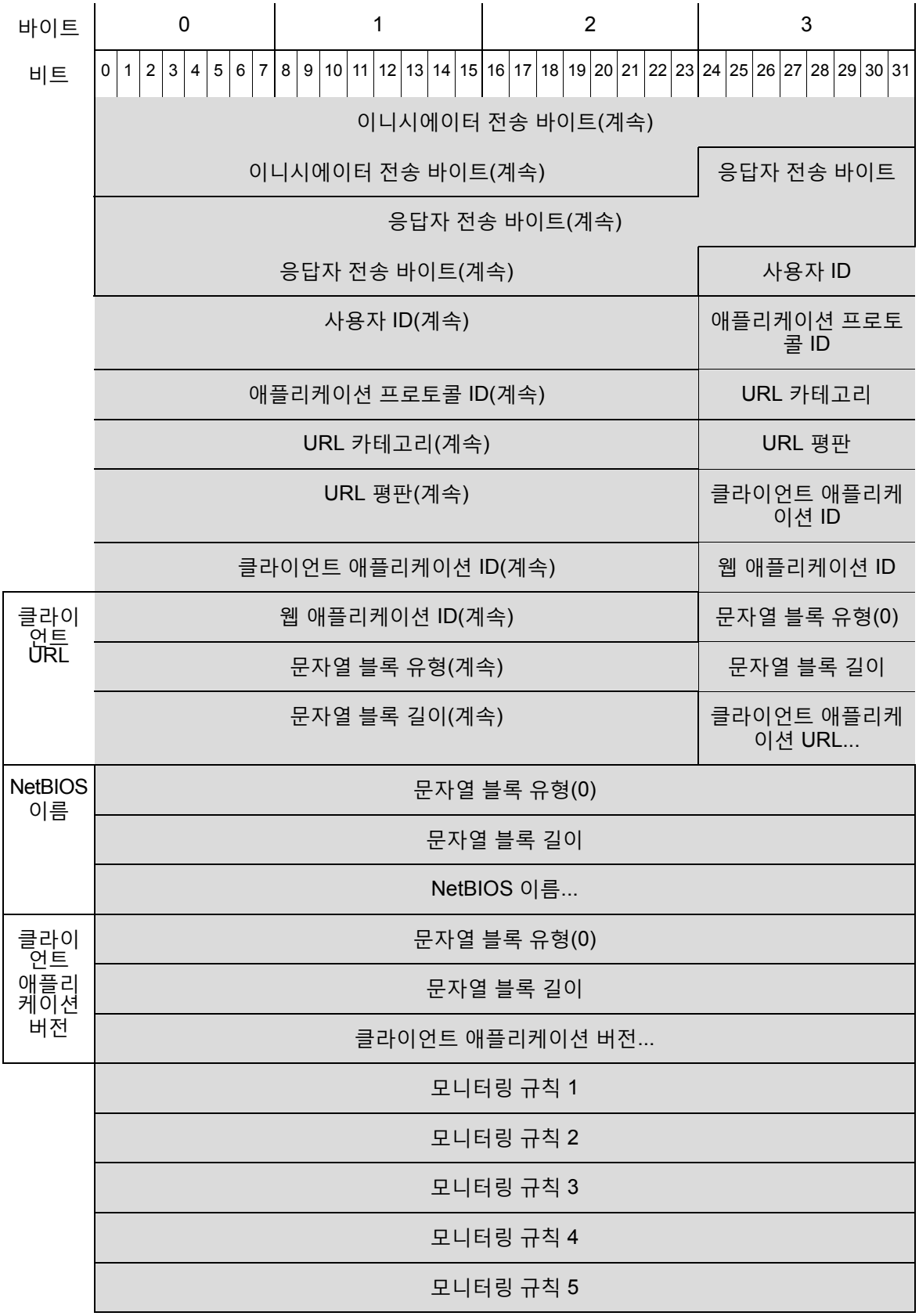
연결 통계 데이터 블록은 연결 데이터 메시지에 사용됩니다. 5.1 버전과 비교할 때 5.1.1 버전에서 변경된 연결 데이터 블록 관련 사항으로는 침입 이벤트를 식별하기 위해 새 필드가 추가된 점이 포함됩니다. 5.1.1.x 버전용 연결 통계 데이터 블록의 블록 유형은 137입니다. 이는 블록 유형 126(5.1 버전용 연결 통계 데이터 블록, 페이지 B-133)의 사용을 중단합니다.

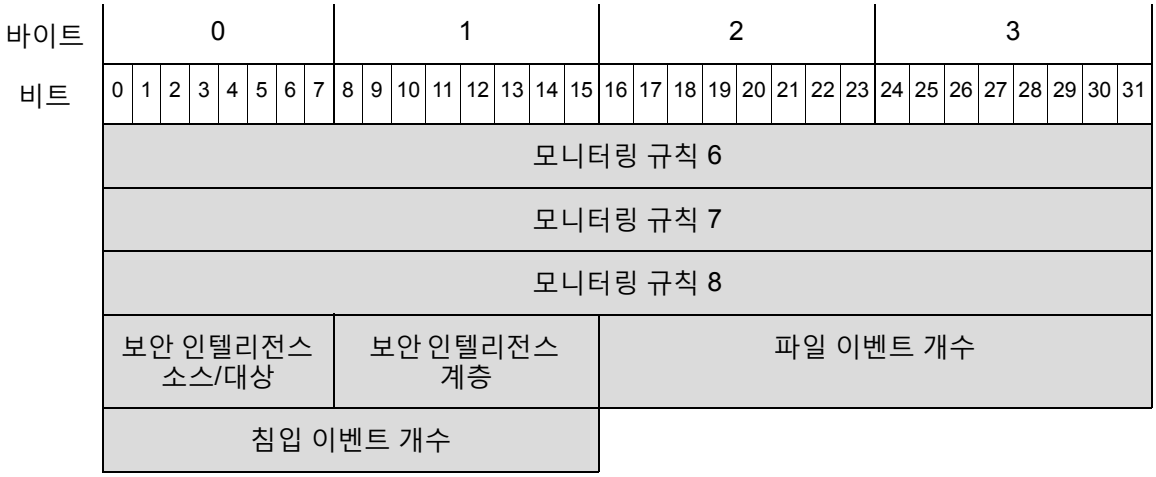
연결 통계 데이터 메시지에 대한 자세한 정보는 연결 통계 데이터 메시지, 페이지 4-54의 내용을 참조하십시오.

다음 다이어그램에 5.1.1 버전의 연결 통계 데이터 블록 형식이 나와 있습니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
연결 데이터 블록 유형(137)																																
연결 데이터 블록 길이																																
디바이스 ID																																
인그레스 영역																																
인그레스 영역(계속)																																
인그레스 영역(계속)																																
인그레스 영역(계속)																																
이그레스(egress) 영역																																
이그레스(egress) 영역(계속)																																
이그레스(egress) 영역(계속)																																
이그레스(egress) 영역(계속)																																
인그레스 인터페이스																																
인그레스 인터페이스(계속)																																
인그레스 인터페이스(계속)																																
인그레스 인터페이스(계속)																																
이그레스(egress) 인터페이스																																
이그레스(egress) 인터페이스(계속)																																
이그레스(egress) 인터페이스(계속)																																
이그레스(egress) 인터페이스(계속)																																
이니시에이터 IP 주소																																
이니시에이터 IP 주소(계속)																																
이니시에이터 IP 주소(계속)																																
이니시에이터 IP 주소(계속)																																


바이트
0
1
2
3
비트
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
응답자 IP 주소
응답자 IP 주소(계속)
응답자 IP 주소(계속)
응답자 IP 주소(계속)
정책 수정
정책 수정(계속)
정책 수정(계속)
정책 수정(계속)
규칙 ID
규칙 작업
규칙 이유
이니시에이터 포트
응답자 포트
TCP 플래그
프로토콜
NetFlow 소스
NetFlow 소스(계속)
NetFlow 소스(계속)
NetFlow 소스(계속)
NetFlow 소스(계속)
인스턴스 ID
인스턴스 ID(계속)
연결 카운터
첫 번째 패킷 타임스탬프
첫 번째 패킷 타임스탬프(계속)
마지막 패킷 타임스탬프
마지막 패킷 타임스탬프(계속)
이니시에이터 전송 패킷
이니시에이터 전송 패킷(계속)
이니시에이터 전송 패킷(계속)
응답자 전송 패킷
응답자 전송 패킷(계속)
응답자 전송 패킷(계속)
이니시에이터 전송 바이트


바이트
0
1
2
3
비트
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
이니시에이터 전송 바이트(계속)
이니시에이터 전송 바이트(계속)
응답자 전송 바이트
응답자 전송 바이트(계속)
응답자 전송 바이트(계속)
사용자 ID
사용자 ID(계속)
애플리케이션 프로토콜 ID
애플리케이션 프로토콜 ID(계속)
URL 카테고리
URL 카테고리(계속)
URL 평판
URL 평판(계속)
클라이언트 애플리케이션 ID
클라이언트 애플리케이션 ID(계속)
웹 애플리케이션 ID
클라이언트 URL
웹 애플리케이션 ID(계속)
문자열 블록 유형(0)
문자열 블록 유형(계속)
문자열 블록 길이
문자열 블록 길이(계속)
클라이언트 애플리케이션 URL...
NetBIOS 이름
문자열 블록 유형(0)
문자열 블록 길이
NetBIOS 이름...
클라이언트 애플리케이션 버전
문자열 블록 유형(0)
문자열 블록 길이
클라이언트 애플리케이션 버전...
모니터링 규칙 1
모니터링 규칙 2
모니터링 규칙 3
모니터링 규칙 4
모니터링 규칙 5



다음 표에는 5.1.1.x 버전용 연결 통계 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 B-33 5.1.1.x 버전용 연결 통계 데이터 블록 필드

필드	데이터 유형	설명
연결 통계 데이터 블록 유형	uint32	5.1.1.x 버전용 연결 통계 데이터 블록을 시작합니다. 값은 항상 137입니다.
연결 통계 데이터 블록 길이	uint32	연결 통계 데이터 블록의 바이트 수입니다. 여기에는 연결 통계 블록 유형 및 길이 필드의 8바이트에 그 뒤의 연결 데이터 바이트 수를 더한 값이 포함됩니다.
디바이스 ID	uint32	연결 이벤트를 탐지한 디바이스입니다.
인그레스 영역	uint8[16]	정책 위반을 트리거한 이벤트의 인그레스 보안 영역입니다.
이그레스 (egress) 영역	uint8[16]	정책 위반을 트리거한 이벤트의 이그레스(egress) 보안 영역입니다.
인그레스 인터페이스	uint8[16]	인바운드 트래픽용 인터페이스입니다.
이그레스 (egress) 인터페이스	uint8[16]	아웃바운드 트래픽용 인터페이스입니다.
이니시에이터 IP 주소	uint8[16]	연결 이벤트에서 설명하는 세션을 시작한 호스트의 IP 주소(IP 주소 옥텟 형식)입니다.
응답자 IP 주소	uint8[16]	시작 호스트에 응답한 호스트의 IP 주소(IP 주소 옥텟 형식)입니다.
정책 수정	uint8[16]	해당하는 경우 트리거된 상관관계와 관련된 규칙의 수정 번호입니다.
규칙 ID	uint32	해당하는 경우 이벤트를 트리거한 규칙의 내부 식별자입니다.
규칙 작업	uint16	해당 규칙(허용, 차단 등)에 대해 사용자 인터페이스에서 선택한 작업입니다.
규칙 이유	uint16	규칙이 이벤트를 트리거한 이유입니다.
이니시에이터 포트	uint16	시작 호스트에 사용되는 포트입니다.

표 B-33 5.1.1.x 버전용 연결 통계 데이터 블록 필드 (계속)

필드	데이터 유형	설명
응답자 포트	uint16	응답 호스트에 사용되는 포트입니다.
TCP 플래그	uint16	연결 이벤트에 대한 모든 TCP 플래그를 나타냅니다.
프로토콜	uint8	IANA에서 지정한 프로토콜 번호입니다.
NetFlow 소스	uint8[16]	연결에 대한 데이터를 내보낸 NetFlow 지원 디바이스의 IP 주소입니다.
인스턴스 ID	uint16	이벤트를 생성한 매니지드 디바이스의 Snort 인스턴스의 숫자 ID입니다.
연결 카운터	uint16	1초 이내에 발생하는 연결 이벤트를 구별하는 데 사용되는 값입니다.
첫 번째 패킷 타임스탬프	uint32	세션에서 첫 번째 패킷이 교환된 날짜의 시간의 UNIX 타임스탬프입니다.
마지막 패킷 타임스탬프	uint32	세션에서 마지막 패킷이 교환된 날짜의 시간의 UNIX 타임스탬프입니다.
이니시에이터 전송 패킷	uint64	시작 호스트에서 전송한 패킷 수입니다.
응답자 전송 패킷	uint64	응답 호스트에서 전송한 패킷 수입니다.
이니시에이터 전송 바이트	uint64	시작 호스트에서 전송한 바이트 수입니다.
응답자 전송 바이트	uint64	응답 호스트에서 전송한 바이트 수입니다.
사용자 ID	uint32	트래픽을 생성한 호스트에 마지막으로 로그인한 사용자의 내부 ID 번호입니다.
애플리케이션 프로토콜 ID	uint32	애플리케이션 프로토콜의 애플리케이션 ID입니다.
URL 카테고리	uint32	URL 카테고리의 내부 ID 번호입니다.
URL 평판	uint32	URL 평판의 내부 ID 번호입니다.
클라이언트 애플리케이션 ID	uint32	해당하는 경우 탐지된 클라이언트 애플리케이션의 내부 ID 번호입니다.
웹 애플리케이션 ID	uint32	해당하는 경우 탐지된 웹 애플리케이션의 내부 ID 번호입니다.
문자열 블록 유형	uint32	클라이언트 애플리케이션 URL에 대한 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	클라이언트 애플리케이션 URL 문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이 필드의 8바이트에 클라이언트 애플리케이션 URL 문자열의 바이트 수를 더한 값이 포함됩니다.
클라이언트 애플리케이션 URL	string	해당하는 경우 클라이언트 애플리케이션이 액세스한 URL입니다. 예를 들면 /files/index.html과 같습니다.
문자열 블록 유형	uint32	호스트 NetBIOS 이름에 대한 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.

표 B-33 5.1.1.x 버전용 연결 통계 데이터 블록 필드 (계속)

필드	데이터 유형	설명
문자열 블록 길이	uint32	문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이 필드의 8바이트에 NetBIOS 이름 문자열의 바이트 수를 더한 값이 포함됩니다.
NetBIOS 이름	string	호스트 NetBIOS 이름 문자열입니다.
문자열 블록 유형	uint32	클라이언트 애플리케이션 버전에 대한 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	클라이언트 애플리케이션 버전에 대한 문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이의 8바이트에 버전의 바이트 수를 더한 값이 포함됩니다.
클라이언트 애플리케이션 버전	string	클라이언트 애플리케이션 버전입니다.
모니터링 규칙 1	uint32	연결 이벤트와 관련된 첫 번째 모니터 규칙의 ID입니다.
모니터링 규칙 2	uint32	연결 이벤트와 관련된 두 번째 모니터 규칙의 ID입니다.
모니터링 규칙 3	uint32	연결 이벤트와 관련된 세 번째 모니터 규칙의 ID입니다.
모니터링 규칙 4	uint32	연결 이벤트와 관련된 네 번째 모니터 규칙의 ID입니다.
모니터링 규칙 5	uint32	연결 이벤트와 관련된 다섯 번째 모니터 규칙의 ID입니다.
모니터링 규칙 6	uint32	연결 이벤트와 관련된 여섯 번째 모니터 규칙의 ID입니다.
모니터링 규칙 7	uint32	연결 이벤트와 관련된 일곱 번째 모니터 규칙의 ID입니다.
모니터링 규칙 8	uint32	연결 이벤트와 관련된 여덟 번째 모니터 규칙의 ID입니다.
보안 인텔리전스 소스/대상	uint8	소스 또는 대상 IP 주소가 IP 블랙리스트와 일치했는지를 나타냅니다.
보안 인텔리전스 계층	uint8	IP 블랙리스트와 일치한 IP 계층입니다.
파일 이벤트 개수	uint16	1초 이내에 발생하는 파일 이벤트를 구별하는 데 사용되는 값입니다.
침입 이벤트 개수	uint16	1초 이내에 발생하는 침입 이벤트를 구별하는 데 사용되는 값입니다.

5.3 버전용 연결 통계 데이터 블록

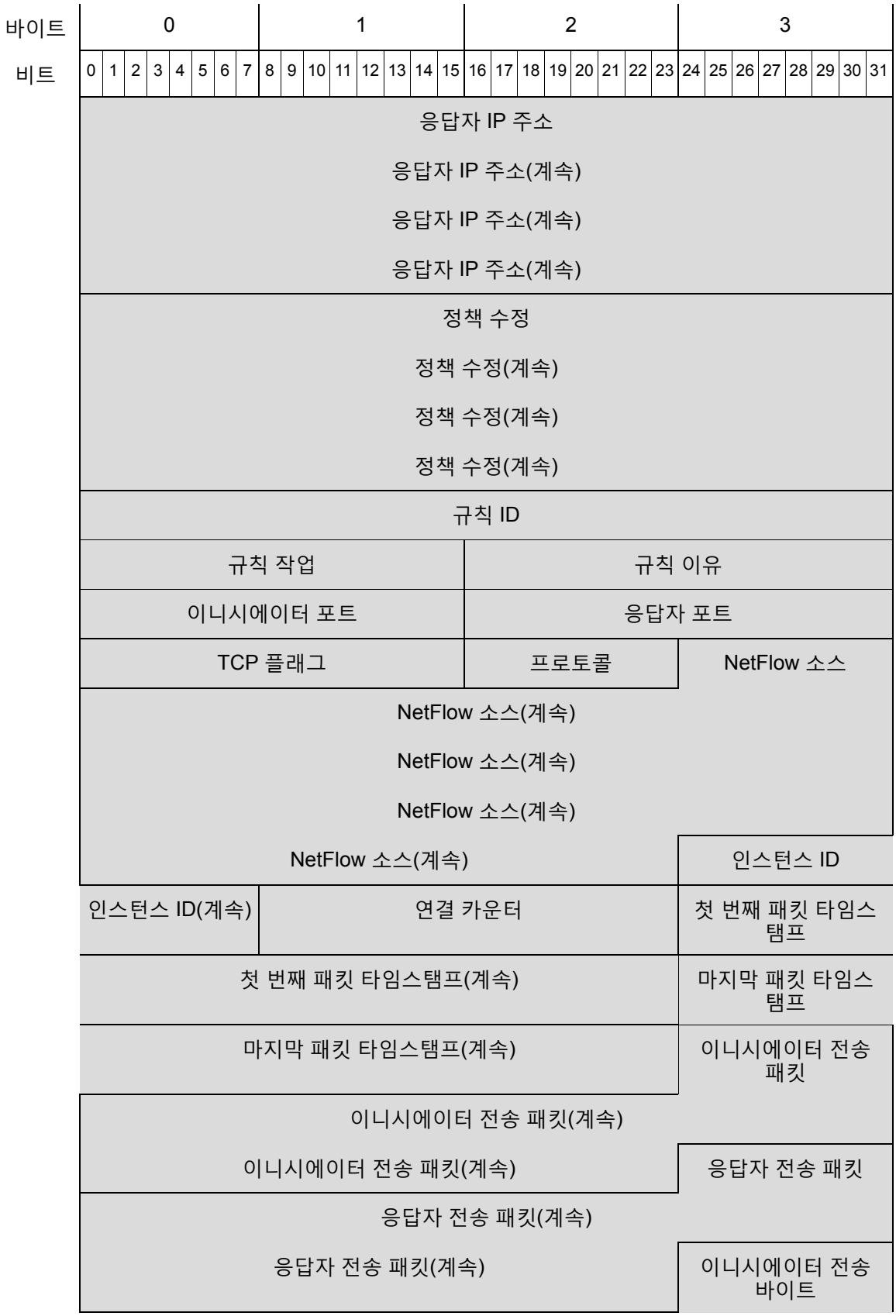
연결 통계 데이터 블록은 연결 데이터 메시지에 사용됩니다. 5.2.x 버전과 비교할 때 5.3 버전에서 변경된 연결 데이터 블록 관련 사항으로는 NetFlow 정보용 새 필드가 추가된 점이 포함됩니다. 계열 1 블록 그룹에서 5.3 버전용 연결 통계 데이터 블록의 블록 유형은 152입니다. 이는 블록 유형 144(5.2.x 버전용 연결 통계 데이터 블록, 페이지 B-139)의 사용을 중단합니다.

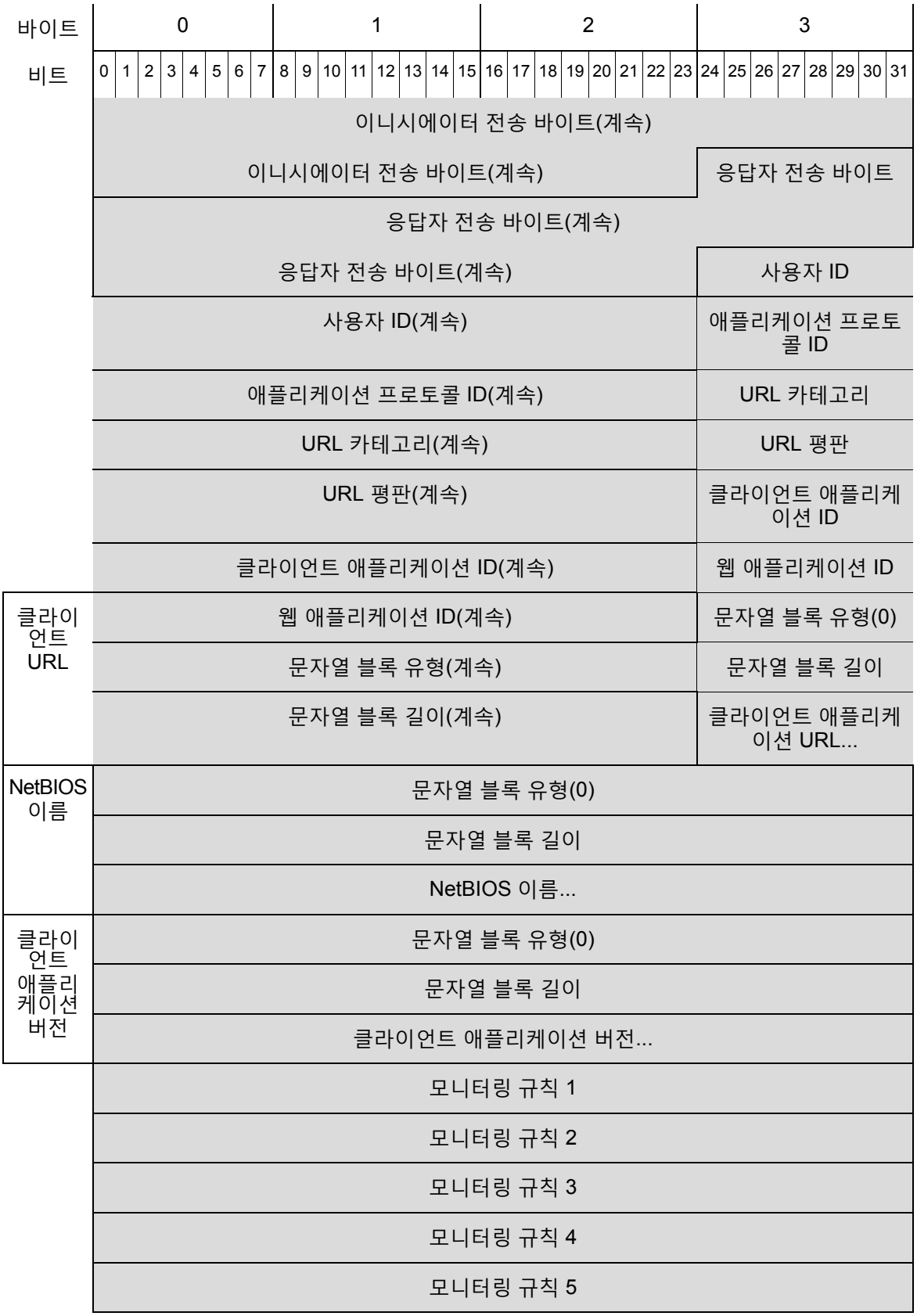
이벤트 버전이 10이고 이벤트 코드가 71인 요청 메시지에서 확장 이벤트 플래그(Request Flags(요청 플래그) 필드의 비트 30)를 설정하여 연결 이벤트 레코드를 요청합니다. 요청 플래그, 페이지 2-12의 내용을 참조하십시오. 비트 23을 활성화하면 레코드에 확장 이벤트 헤더가 포함됩니다.

연결 통계 데이터 메시지에 대한 자세한 정보는 연결 통계 데이터 메시지, 페이지 4-54의 내용을 참조하십시오.

다음 다이어그램에 5.3 이상 버전의 연결 통계 데이터 블록 형식이 나와 있습니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
연결 데이터 블록 유형(152)																																
연결 데이터 블록 길이																																
디바이스 ID																																
인그레스 영역																																
인그레스 영역(계속)																																
인그레스 영역(계속)																																
인그레스 영역(계속)																																
이그레스(egress) 영역																																
이그레스(egress) 영역(계속)																																
이그레스(egress) 영역(계속)																																
이그레스(egress) 영역(계속)																																
인그레스 인터페이스																																
인그레스 인터페이스(계속)																																
인그레스 인터페이스(계속)																																
인그레스 인터페이스(계속)																																
이그레스(egress) 인터페이스																																
이그레스(egress) 인터페이스(계속)																																
이그레스(egress) 인터페이스(계속)																																
이그레스(egress) 인터페이스(계속)																																
이니시에이터 IP 주소																																
이니시에이터 IP 주소(계속)																																
이니시에이터 IP 주소(계속)																																
이니시에이터 IP 주소(계속)																																


바이트
0
1
2
3
비트
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
응답자 IP 주소
응답자 IP 주소(계속)
응답자 IP 주소(계속)
응답자 IP 주소(계속)
정책 수정
정책 수정(계속)
정책 수정(계속)
정책 수정(계속)
규칙 ID
규칙 작업
규칙 이유
이니시에이터 포트
응답자 포트
TCP 플래그
프로토콜
NetFlow 소스
NetFlow 소스(계속)
NetFlow 소스(계속)
NetFlow 소스(계속)
NetFlow 소스(계속)
인스턴스 ID
인스턴스 ID(계속)
연결 카운터
첫 번째 패킷 타임스탬프
첫 번째 패킷 타임스탬프(계속)
마지막 패킷 타임스탬프
마지막 패킷 타임스탬프(계속)
이니시에이터 전송 패킷
이니시에이터 전송 패킷(계속)
이니시에이터 전송 패킷(계속)
응답자 전송 패킷
응답자 전송 패킷(계속)
응답자 전송 패킷(계속)
이니시에이터 전송 바이트


바이트
0
1
2
3
비트
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
이니시에이터 전송 바이트(계속)
이니시에이터 전송 바이트(계속)
응답자 전송 바이트
응답자 전송 바이트(계속)
응답자 전송 바이트(계속)
사용자 ID
사용자 ID(계속)
애플리케이션 프로토콜 ID
애플리케이션 프로토콜 ID(계속)
URL 카테고리
URL 카테고리(계속)
URL 평판
URL 평판(계속)
클라이언트 애플리케이션 ID
클라이언트 애플리케이션 ID(계속)
웹 애플리케이션 ID
클라이언트 URL
웹 애플리케이션 ID(계속)
문자열 블록 유형(0)
문자열 블록 유형(계속)
문자열 블록 길이
문자열 블록 길이(계속)
클라이언트 애플리케이션 URL...
NetBIOS 이름
문자열 블록 유형(0)
문자열 블록 길이
NetBIOS 이름...
클라이언트 애플리케이션 버전
문자열 블록 유형(0)
문자열 블록 길이
클라이언트 애플리케이션 버전...
모니터링 규칙 1
모니터링 규칙 2
모니터링 규칙 3
모니터링 규칙 4
모니터링 규칙 5

다음 표에는 5.3 버전용 연결 통계 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 B-34 5.3 이상 버전용 연결 통계 데이터 블록 필드

필드	데이터 유형	설명
연결 통계 데이터 블록 유형	uint32	5.3 버전용 연결 통계 데이터 블록을 시작합니다. 값은 항상 152입니다.
연결 통계 데이터 블록 길이	uint32	연결 통계 데이터 블록의 바이트 수입니다. 여기에는 연결 통계 블록 유형 및 길이 필드의 8바이트에 그 뒤의 연결 데이터 바이트 수를 더한 값이 포함됩니다.
디바이스 ID	uint32	연결 이벤트를 탐지한 디바이스입니다.
인그레스 영역	uint8[16]	정책 위반을 트리거한 이벤트의 인그레스 보안 영역입니다.
이그레스 (egress) 영역	uint8[16]	정책 위반을 트리거한 이벤트의 이그레스(egress) 보안 영역입니다.
인그레스 인터페이스	uint8[16]	인바운드 트래픽용 인터페이스입니다.
이그레스 (egress) 인터페이스	uint8[16]	아웃바운드 트래픽용 인터페이스입니다.
이니시에이터 IP 주소	uint8[16]	연결 이벤트에서 설명하는 세션을 시작한 호스트의 IP 주소(IP 주소 옥텟 형식)입니다.
응답자 IP 주소	uint8[16]	시작 호스트에 응답한 호스트의 IP 주소(IP 주소 옥텟 형식)입니다.

표 B-34 5.3 이상 버전용 연결 통계 데이터 블록 필드 (계속)

필드	데이터 유형	설명
정책 수정	uint8[16]	해당하는 경우 트리거된 상관관계와 관련된 규칙의 수정 번호입니다.
규칙 ID	uint32	해당하는 경우 이벤트를 트리거한 규칙의 내부 식별자입니다.
규칙 작업	uint16	해당 규칙(허용, 차단 등)에 대해 사용자 인터페이스에서 선택한 작업입니다.
규칙 이유	uint16	규칙이 이벤트를 트리거한 이유입니다.
이니시에이터 포트	uint16	시작 호스트에 사용되는 포트입니다.
응답자 포트	uint16	응답 호스트에 사용되는 포트입니다.
TCP 플래그	uint16	연결 이벤트에 대한 모든 TCP 플래그를 나타냅니다.
프로토콜	uint8	IANA에서 지정한 프로토콜 번호입니다.
NetFlow 소스	uint8[16]	연결에 대한 데이터를 내보낸 NetFlow 지원 디바이스의 IP 주소입니다.
인스턴스 ID	uint16	이벤트를 생성한 매니지드 디바이스의 Snort 인스턴스의 숫자 ID입니다.
연결 카운터	uint16	1초 이내에 발생하는 연결 이벤트를 구별하는 데 사용되는 값입니다.
첫 번째 패킷 타임스탬프	uint32	세션에서 첫 번째 패킷이 교환된 날짜의 시간의 UNIX 타임스탬프입니다.
마지막 패킷 타임스탬프	uint32	세션에서 마지막 패킷이 교환된 날짜의 시간의 UNIX 타임스탬프입니다.
이니시에이터 전송 패킷	uint64	시작 호스트에서 전송한 패킷 수입니다.
응답자 전송 패킷	uint64	응답 호스트에서 전송한 패킷 수입니다.
이니시에이터 전송 바이트	uint64	시작 호스트에서 전송한 바이트 수입니다.
응답자 전송 바이트	uint64	응답 호스트에서 전송한 바이트 수입니다.
사용자 ID	uint32	트래픽을 생성한 호스트에 마지막으로 로그인한 사용자의 내부 ID 번호입니다.
애플리케이션 프로토콜 ID	uint32	애플리케이션 프로토콜의 애플리케이션 ID입니다.
URL 카테고리	uint32	URL 카테고리의 내부 ID 번호입니다.
URL 평판	uint32	URL 평판의 내부 ID 번호입니다.
클라이언트 애플리케이션 ID	uint32	해당하는 경우 탐지된 클라이언트 애플리케이션의 내부 ID 번호입니다.
웹 애플리케이션 ID	uint32	해당하는 경우 탐지된 웹 애플리케이션의 내부 ID 번호입니다.
문자열 블록 유형	uint32	클라이언트 애플리케이션 URL에 대한 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.

표 B-34 5.3 이상 버전용 연결 통계 데이터 블록 필드 (계속)

필드	데이터 유형	설명
문자열 블록 길이	uint32	클라이언트 애플리케이션 URL 문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이 필드의 8바이트에 클라이언트 애플리케이션 URL 문자열의 바이트 수를 더한 값이 포함됩니다.
클라이언트 애플리케이션 URL	string	해당하는 경우 클라이언트 애플리케이션이 액세스한 URL입니다. 예를 들면 `/files/index.html`과 같습니다.
문자열 블록 유형	uint32	호스트 NetBIOS 이름에 대한 문자열 데이터 블록을 시작합니다. 이 값은 항상 `0`입니다.
문자열 블록 길이	uint32	문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이 필드의 8바이트에 NetBIOS 이름 문자열의 바이트 수를 더한 값이 포함됩니다.
NetBIOS 이름	string	호스트 NetBIOS 이름 문자열입니다.
문자열 블록 유형	uint32	클라이언트 애플리케이션 버전에 대한 문자열 데이터 블록을 시작합니다. 이 값은 항상 `0`입니다.
문자열 블록 길이	uint32	클라이언트 애플리케이션 버전에 대한 문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이의 8바이트에 버전의 바이트 수를 더한 값이 포함됩니다.
클라이언트 애플리케이션 버전	string	클라이언트 애플리케이션 버전입니다.
모니터링 규칙 1	uint32	연결 이벤트와 관련된 첫 번째 모니터 규칙의 ID입니다.
모니터링 규칙 2	uint32	연결 이벤트와 관련된 두 번째 모니터 규칙의 ID입니다.
모니터링 규칙 3	uint32	연결 이벤트와 관련된 세 번째 모니터 규칙의 ID입니다.
모니터링 규칙 4	uint32	연결 이벤트와 관련된 네 번째 모니터 규칙의 ID입니다.
모니터링 규칙 5	uint32	연결 이벤트와 관련된 다섯 번째 모니터 규칙의 ID입니다.
모니터링 규칙 6	uint32	연결 이벤트와 관련된 여섯 번째 모니터 규칙의 ID입니다.
모니터링 규칙 7	uint32	연결 이벤트와 관련된 일곱 번째 모니터 규칙의 ID입니다.
모니터링 규칙 8	uint32	연결 이벤트와 관련된 여덟 번째 모니터 규칙의 ID입니다.
보안 인텔리전스 소스/대상	uint8	소스 또는 대상 IP 주소가 IP 블랙리스트와 일치했는지를 나타냅니다.
보안 인텔리전스 계층	uint8	IP 블랙리스트와 일치한 IP 계층입니다.
파일 이벤트 개수	uint16	1초 이내에 발생하는 파일 이벤트를 구별하는 데 사용되는 값입니다.
침입 이벤트 개수	uint16	1초 이내에 발생하는 침입 이벤트를 구별하는 데 사용되는 값입니다.
이니시에이터 국가	uint16	시작 호스트의 국가 코드입니다.
응답자 국가	uint16	응답 호스트의 국가 코드입니다.
IOC 번호	uint16	이 이벤트와 관련된 보안 침해의 ID 번호입니다.
소스 자동 시스템	uint32	소스의 AS 번호(원본 또는 피어)입니다.

표 B-34 5.3 이상 버전용 연결 통계 데이터 블록 필드 (계속)

필드	데이터 유형	설명
대상 자동 시스템	uint32	대상의 AS 번호(원본 또는 피어)입니다.
SNMP 입력	uint16	입력 인터페이스의 SNMP 인덱스입니다.
SNMP 출력	uint16	출력 인터페이스의 SNMP 인덱스입니다.
소스 TOS	uint8	들어오는 인터페이스에 대한 서비스 유형 바이트 설정입니다.
대상 TOS	uint8	나가는 인터페이스에 대한 서비스 유형 바이트 설정입니다.
소스 마스크	uint8	소스 주소 접두사 마스크입니다.
대상 마스크	uint8	대상 주소 접두사 마스크입니다.

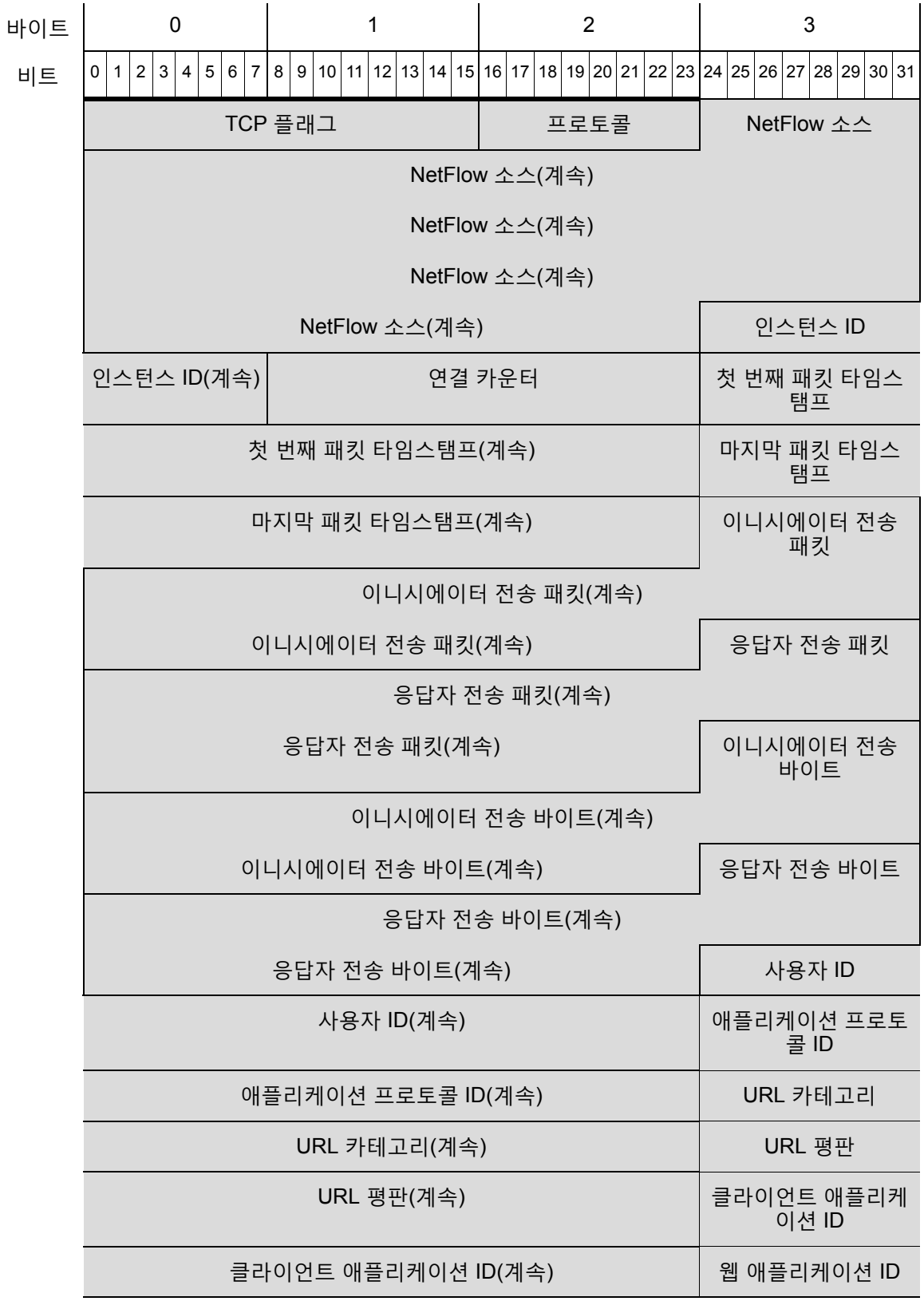
5.3.1 버전용 연결 통계 데이터 블록

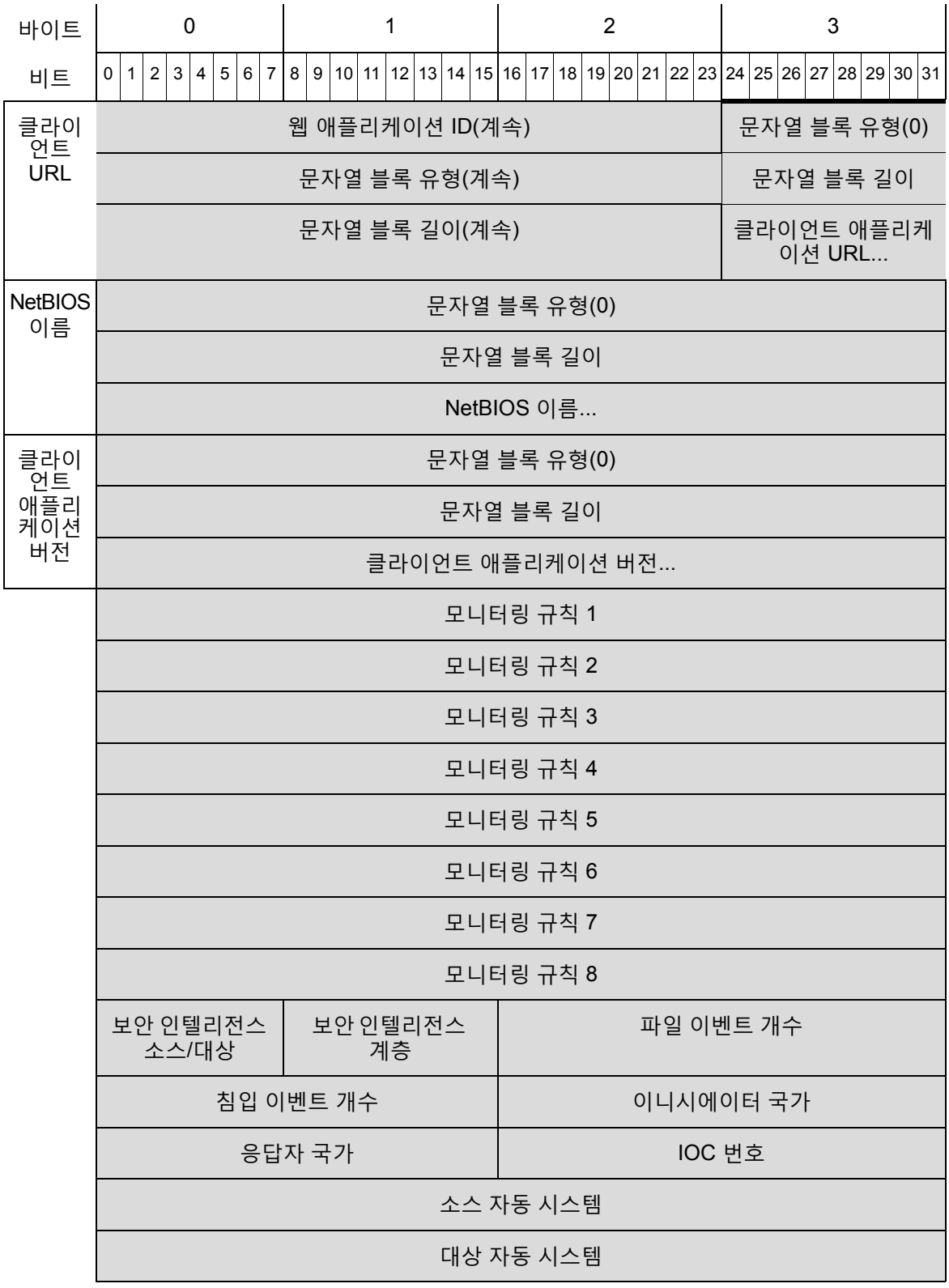
연결 통계 데이터 블록은 연결 데이터 메시지에 사용됩니다. 5.3 버전과 비교할 때 5.3.1 버전에서 변경된 사항은 보안 상황 필드가 추가되었다는 것뿐입니다. 계열 1 블록 그룹에서 5.3.1 버전용 연결 통계 데이터 블록의 블록 유형은 154입니다. 이는 블록 유형 152(5.3 버전용 연결 통계 데이터 블록, 페이지 B-154)의 사용을 중단합니다.

이벤트 버전이 11이고 이벤트 코드가 71인 요청 메시지에서 확장 이벤트 플래그(Request Flags(요청 플래그) 필드의 비트 30)를 설정하여 연결 이벤트 레코드를 요청합니다. 요청 플래그, 페이지 2-12의 내용을 참조하십시오. 비트 23을 활성화하면 레코드에 확장 이벤트 헤더가 포함됩니다. 연결 통계 데이터 메시지에 대한 자세한 정보는 연결 통계 데이터 메시지, 페이지 4-54의 내용을 참조하십시오.

다음 다이어그램에 5.3.1 버전의 연결 통계 데이터 블록 형식이 나와 있습니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
이그레스(egress) 영역(계속)																																
인그레스 인터페이스																																
인그레스 인터페이스(계속)																																
인그레스 인터페이스(계속)																																
인그레스 인터페이스(계속)																																
이그레스(egress) 인터페이스																																
이그레스(egress) 인터페이스(계속)																																
이그레스(egress) 인터페이스(계속)																																
이그레스(egress) 인터페이스(계속)																																
이니시에이터 IP 주소																																
이니시에이터 IP 주소(계속)																																
이니시에이터 IP 주소(계속)																																
이니시에이터 IP 주소(계속)																																
응답자 IP 주소																																
응답자 IP 주소(계속)																																
응답자 IP 주소(계속)																																
응답자 IP 주소(계속)																																
정책 수정																																
정책 수정(계속)																																
정책 수정(계속)																																
정책 수정(계속)																																
규칙 ID																																
규칙 작업																	규칙 이유															
이니시에이터 포트																	응답자 포트															


바이트
0
1
2
3
비트
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
TCP 플래그
프로토콜
NetFlow 소스
NetFlow 소스(계속)
NetFlow 소스(계속)
NetFlow 소스(계속)
NetFlow 소스(계속)
인스턴스 ID
인스턴스 ID(계속)
연결 카운터
첫 번째 패킷 타임스탬프
첫 번째 패킷 타임스탬프(계속)
마지막 패킷 타임스탬프
마지막 패킷 타임스탬프(계속)
이니시에이터 전송 패킷
이니시에이터 전송 패킷(계속)
이니시에이터 전송 패킷(계속)
응답자 전송 패킷
응답자 전송 패킷(계속)
응답자 전송 패킷(계속)
이니시에이터 전송 바이트
이니시에이터 전송 바이트(계속)
이니시에이터 전송 바이트(계속)
응답자 전송 바이트
응답자 전송 바이트(계속)
응답자 전송 바이트(계속)
사용자 ID
사용자 ID(계속)
애플리케이션 프로토콜 ID
애플리케이션 프로토콜 ID(계속)
URL 카테고리
URL 카테고리(계속)
URL 평판
URL 평판(계속)
클라이언트 애플리케이션 ID
클라이언트 애플리케이션 ID(계속)
웹 애플리케이션 ID


바이트
0
1
2
3
비트
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
클라이언트 URL
웹 애플리케이션 ID(계속)
문자열 블록 유형(0)
문자열 블록 유형(계속)
문자열 블록 길이
문자열 블록 길이(계속)
클라이언트 애플리케이션 URL...
NetBIOS 이름
문자열 블록 유형(0)
문자열 블록 길이
NetBIOS 이름...
클라이언트 애플리케이션 버전
문자열 블록 유형(0)
문자열 블록 길이
클라이언트 애플리케이션 버전...
모니터링 규칙 1
모니터링 규칙 2
모니터링 규칙 3
모니터링 규칙 4
모니터링 규칙 5
모니터링 규칙 6
모니터링 규칙 7
모니터링 규칙 8
보안 인텔리전스 소스/대상
보안 인텔리전스 계층
파일 이벤트 개수
침입 이벤트 개수
이니시에이터 국가
응답자 국가
IOC 번호
소스 자동 시스템
대상 자동 시스템

다음 표에는 5.3.1 버전용 연결 통계 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 B-35 5.3.1 버전용 연결 통계 데이터 블록 필드

필드	데이터 유형	설명
연결 통계 데이터 블록 유형	uint32	5.3.1 이상 버전용 연결 통계 데이터 블록을 시작합니다. 값은 항상 154입니다.
연결 통계 데이터 블록 길이	uint32	연결 통계 데이터 블록의 바이트 수입니다. 여기에는 연결 통계 블록 유형 및 길이 필드의 8바이트에 그 뒤의 연결 데이터 바이트 수를 더한 값이 포함됩니다.
디바이스 ID	uint32	연결 이벤트를 탐지한 디바이스입니다.
인그레스 영역	uint8[16]	정책 위반을 트리거한 이벤트의 인그레스 보안 영역입니다.
이그레스 (egress) 영역	uint8[16]	정책 위반을 트리거한 이벤트의 이그레스(egress) 보안 영역입니다.
인그레스 인터페이스	uint8[16]	인바운드 트래픽용 인터페이스입니다.
이그레스 (egress) 인터페이스	uint8[16]	아웃바운드 트래픽용 인터페이스입니다.
이니시에이터 IP 주소	uint8[16]	연결 이벤트에서 설명하는 세션을 시작한 호스트의 IP 주소(IP 주소 옥텟 형식)입니다.
응답자 IP 주소	uint8[16]	시작 호스트에 응답한 호스트의 IP 주소(IP 주소 옥텟 형식)입니다.
정책 수정	uint8[16]	해당하는 경우 트리거된 상관관계와 관련된 규칙의 수정 번호입니다.
규칙 ID	uint32	해당하는 경우 이벤트를 트리거한 규칙의 내부 식별자입니다.
규칙 작업	uint16	해당 규칙(허용, 차단 등)에 대해 사용자 인터페이스에서 선택한 작업입니다.
규칙 이유	uint16	규칙이 이벤트를 트리거한 이유입니다.

표 B-35 5.3.1 버전용 연결 통계 데이터 블록 필드 (계속)

필드	데이터 유형	설명
이니시에이터 포트	uint16	시작 호스트에 사용되는 포트입니다.
응답자 포트	uint16	응답 호스트에 사용되는 포트입니다.
TCP 플래그	uint16	연결 이벤트에 대한 모든 TCP 플래그를 나타냅니다.
프로토콜	uint8	IANA에서 지정한 프로토콜 번호입니다.
NetFlow 소스	uint8[16]	연결에 대한 데이터를 내보낸 NetFlow 지원 디바이스의 IP 주소입니다.
인스턴스 ID	uint16	이벤트를 생성한 매니지드 디바이스의 Snort 인스턴스의 숫자 ID입니다.
연결 카운터	uint16	1초 이내에 발생하는 연결 이벤트를 구별하는 데 사용되는 값입니다.
첫 번째 패킷 타임스탬프	uint32	세션에서 첫 번째 패킷이 교환된 날짜의 시간의 UNIX 타임스탬프입니다.
마지막 패킷 타임스탬프	uint32	세션에서 마지막 패킷이 교환된 날짜의 시간의 UNIX 타임스탬프입니다.
이니시에이터 전송 패킷	uint64	시작 호스트에서 전송한 패킷 수입니다.
응답자 전송 패킷	uint64	응답 호스트에서 전송한 패킷 수입니다.
이니시에이터 전송 바이트	uint64	시작 호스트에서 전송한 바이트 수입니다.
응답자 전송 바이트	uint64	응답 호스트에서 전송한 바이트 수입니다.
사용자 ID	uint32	트래픽을 생성한 호스트에 마지막으로 로그인한 사용자의 내부 ID 번호입니다.
애플리케이션 프로토콜 ID	uint32	애플리케이션 프로토콜의 애플리케이션 ID입니다.
URL 카테고리	uint32	URL 카테고리의 내부 ID 번호입니다.
URL 평판	uint32	URL 평판의 내부 ID 번호입니다.
클라이언트 애플리케이션 ID	uint32	해당하는 경우 탐지된 클라이언트 애플리케이션의 내부 ID 번호입니다.
웹 애플리케이션 ID	uint32	해당하는 경우 탐지된 웹 애플리케이션의 내부 ID 번호입니다.
문자열 블록 유형	uint32	클라이언트 애플리케이션 URL에 대한 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	클라이언트 애플리케이션 URL 문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이 필드의 8바이트에 클라이언트 애플리케이션 URL 문자열의 바이트 수를 더한 값이 포함됩니다.
클라이언트 애플리케이션 URL	string	해당하는 경우 클라이언트 애플리케이션이 액세스한 URL입니다. 예를 들면 /files/index.html과 같습니다.

표 B-35 5.3.1 버전용 연결 통계 데이터 블록 필드 (계속)

필드	데이터 유형	설명
문자열 블록 유형	uint32	호스트 NetBIOS 이름에 대한 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이 필드의 8바이트에 NetBIOS 이름 문자열의 바이트 수를 더한 값이 포함됩니다.
NetBIOS 이름	string	호스트 NetBIOS 이름 문자열입니다.
문자열 블록 유형	uint32	클라이언트 애플리케이션 버전에 대한 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	클라이언트 애플리케이션 버전에 대한 문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이의 8바이트에 버전의 바이트 수를 더한 값이 포함됩니다.
클라이언트 애플리케이션 버전	string	클라이언트 애플리케이션 버전입니다.
모니터링 규칙 1	uint32	연결 이벤트와 관련된 첫 번째 모니터 규칙의 ID입니다.
모니터링 규칙 2	uint32	연결 이벤트와 관련된 두 번째 모니터 규칙의 ID입니다.
모니터링 규칙 3	uint32	연결 이벤트와 관련된 세 번째 모니터 규칙의 ID입니다.
모니터링 규칙 4	uint32	연결 이벤트와 관련된 네 번째 모니터 규칙의 ID입니다.
모니터링 규칙 5	uint32	연결 이벤트와 관련된 다섯 번째 모니터 규칙의 ID입니다.
모니터링 규칙 6	uint32	연결 이벤트와 관련된 여섯 번째 모니터 규칙의 ID입니다.
모니터링 규칙 7	uint32	연결 이벤트와 관련된 일곱 번째 모니터 규칙의 ID입니다.
모니터링 규칙 8	uint32	연결 이벤트와 관련된 여덟 번째 모니터 규칙의 ID입니다.
보안 인텔리전스 소스/대상	uint8	소스 또는 대상 IP 주소가 IP 블랙리스트와 일치했는지를 나타냅니다.
보안 인텔리전스 계층	uint8	IP 블랙리스트와 일치한 IP 계층입니다.
파일 이벤트 개수	uint16	1초 이내에 발생하는 파일 이벤트를 구별하는 데 사용되는 값입니다.
침입 이벤트 개수	uint16	1초 이내에 발생하는 침입 이벤트를 구별하는 데 사용되는 값입니다.
이니시에이터 국가	uint16	시작 호스트의 국가 코드입니다.
응답자 국가	uint16	응답 호스트의 국가 코드입니다.
IOC 번호	uint16	이 이벤트와 관련된 보안 침해의 ID 번호입니다.
소스 자동 시스템	uint32	소스의 AS 번호(원본 또는 피어)입니다.
대상 자동 시스템	uint32	대상의 AS 번호(원본 또는 피어)입니다.
SNMP 입력	uint16	입력 인터페이스의 SNMP 인덱스입니다.
SNMP 출력	uint16	출력 인터페이스의 SNMP 인덱스입니다.
소스 TOS	uint8	들어오는 인터페이스에 대한 서비스 유형 바이트 설정입니다.
대상 TOS	uint8	나가는 인터페이스에 대한 서비스 유형 바이트 설정입니다.

표 B-35 5.3.1 버전용 연결 통계 데이터 블록 필드 (계속)

필드	데이터 유형	설명
소스 마스크	uint8	소스 주소 접두사 마스크입니다.
대상 마스크	uint8	대상 주소 접두사 마스크입니다.
보안 상황	uint8(16)	트래픽이 통과한 보안 상황(가상 방화벽)의 ID 번호입니다. 이 필드는 다중 컨텍스트 모드의 ASA FirePOWER 디바이스에 대해서만 채워집니다.

5.4 버전용 연결 통계 데이터 블록

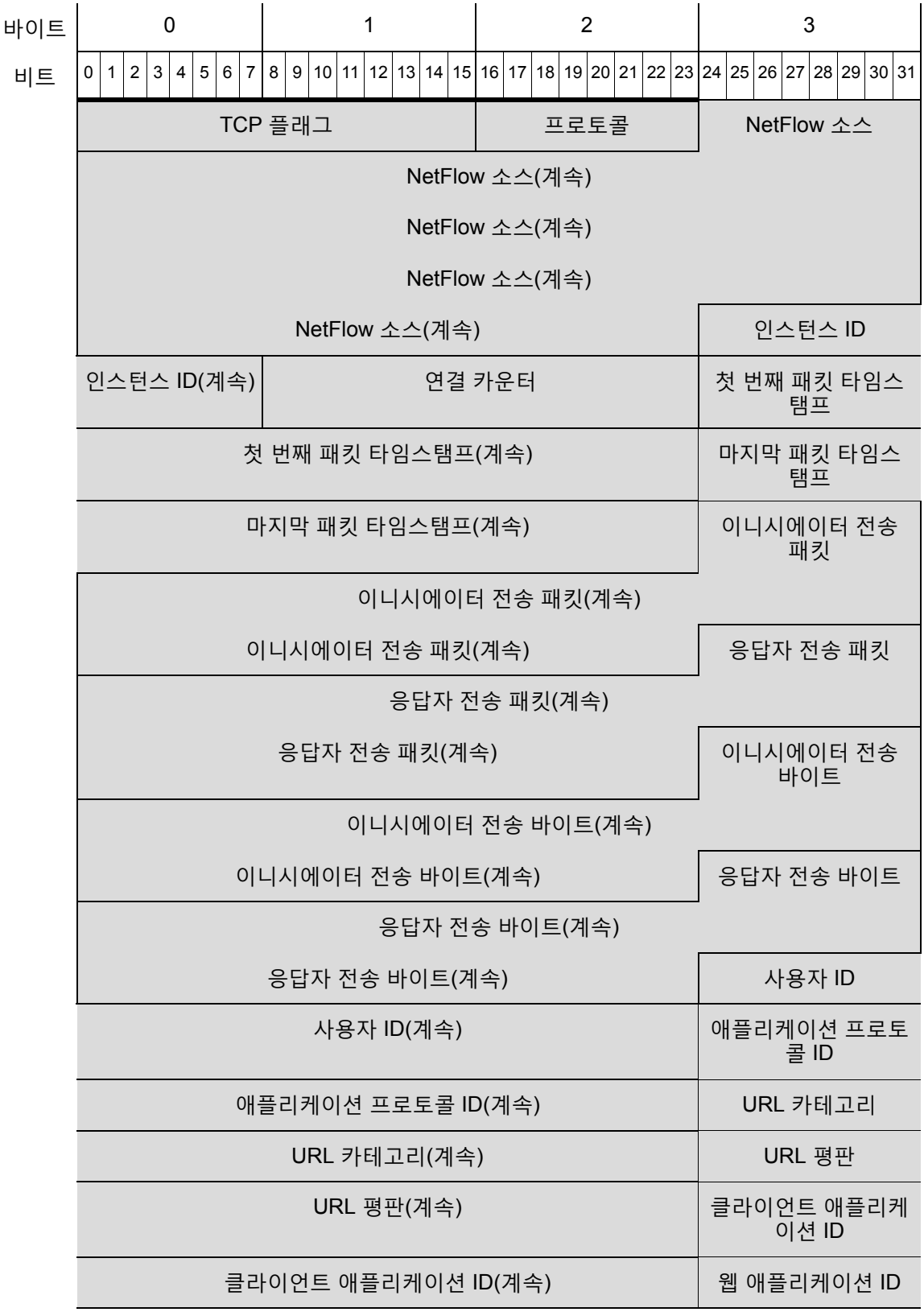
연결 통계 데이터 블록은 연결 데이터 메시지에 사용됩니다. 5.4 버전용 연결 통계 데이터 블록에는 새 필드가 여러 개 추가되었습니다. SSL 연결, HTTP 리디렉션 및 네트워크 분석 정책용 필드가 추가되었습니다. 계열 1 블록 그룹에서 5.4 버전용 연결 통계 데이터 블록의 블록 유형은 155입니다. 이는 블록 유형 154(5.3.1 버전용 연결 통계 데이터 블록, 페이지 B-161)의 사용을 중단합니다.

이벤트 버전이 12이고 이벤트 코드가 71인 요청 메시지에서 확장 이벤트 플래그(Request Flags(요청 플래그) 필드의 비트 30)를 설정하여 연결 이벤트 레코드를 요청합니다. 요청 플래그, 페이지 2-12의 내용을 참조하십시오. 비트 23을 활성화하면 레코드에 확장 이벤트 헤더가 포함됩니다.

연결 통계 데이터 메시지에 대한 자세한 정보는 연결 통계 데이터 메시지, 페이지 4-54의 내용을 참조하십시오.

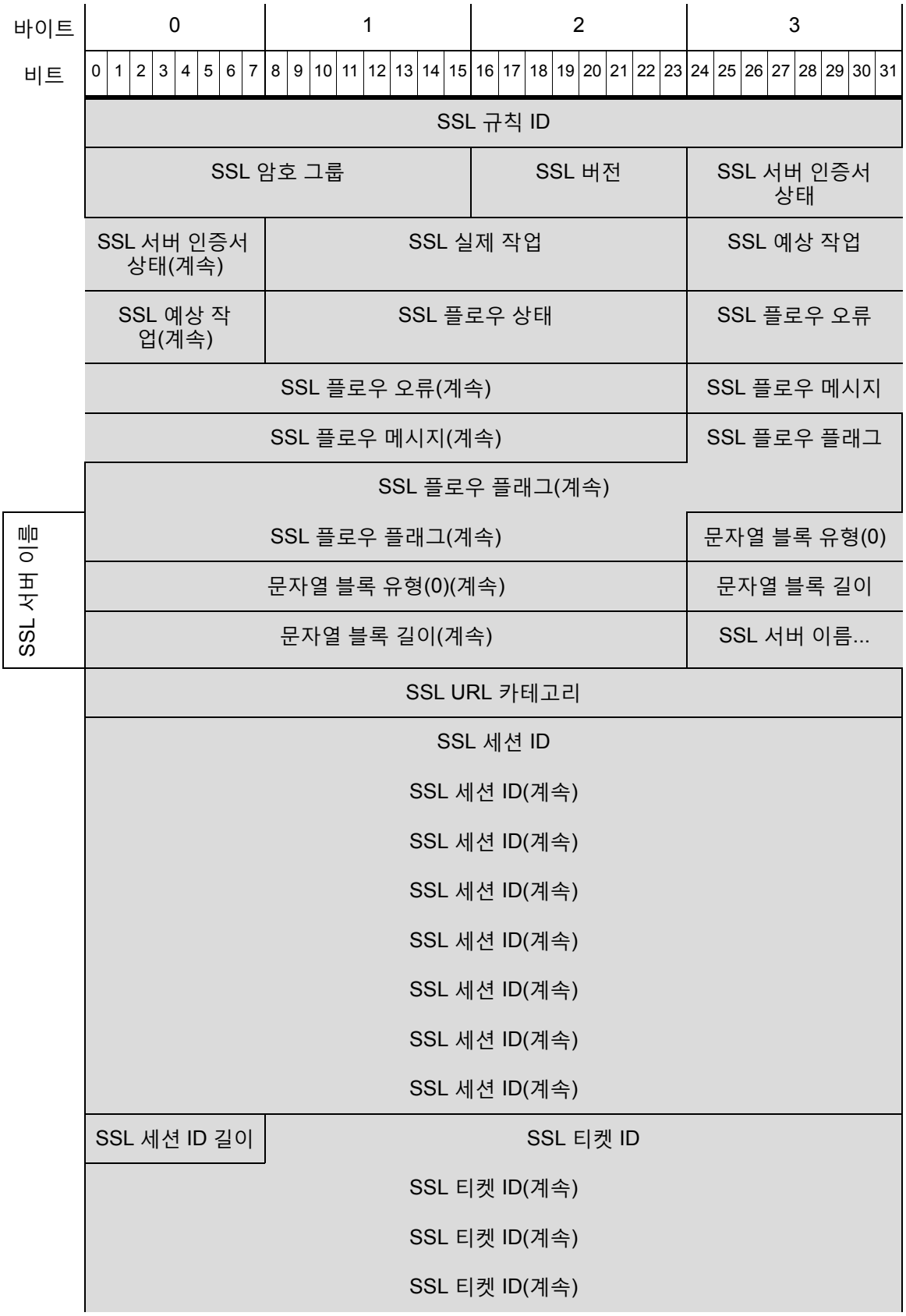
다음 다이어그램에 5.4 버전의 연결 통계 데이터 블록 형식이 나와 있습니다.

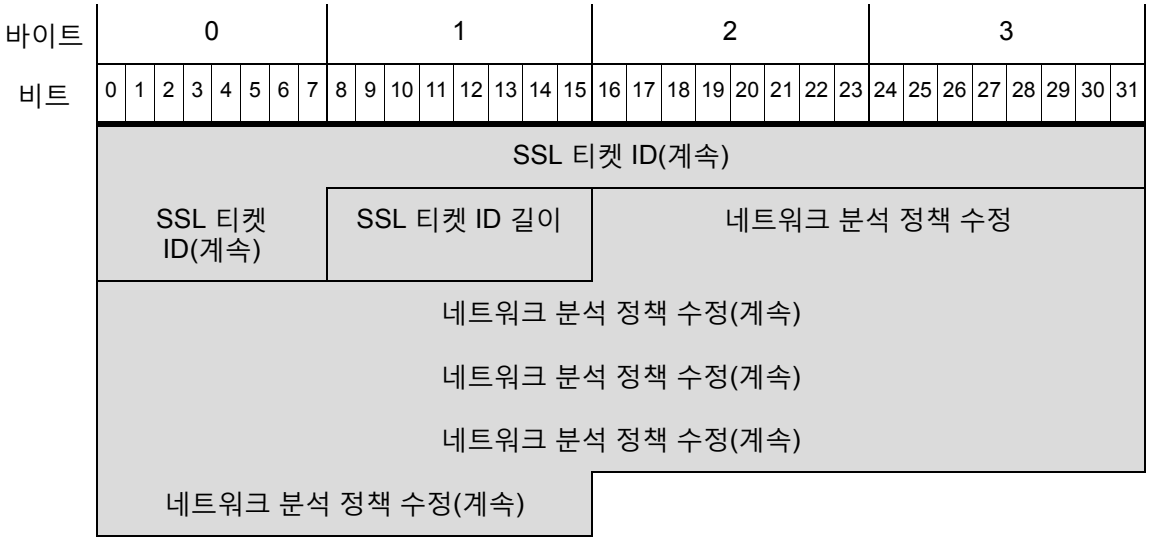
바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
인그레스 인터페이스																																
인그레스 인터페이스(계속)																																
인그레스 인터페이스(계속)																																
인그레스 인터페이스(계속)																																
이그레스(egress) 인터페이스																																
이그레스(egress) 인터페이스(계속)																																
이그레스(egress) 인터페이스(계속)																																
이그레스(egress) 인터페이스(계속)																																
이니시에이터 IP 주소																																
이니시에이터 IP 주소(계속)																																
이니시에이터 IP 주소(계속)																																
이니시에이터 IP 주소(계속)																																
응답자 IP 주소																																
응답자 IP 주소(계속)																																
응답자 IP 주소(계속)																																
응답자 IP 주소(계속)																																
정책 수정																																
정책 수정(계속)																																
정책 수정(계속)																																
정책 수정(계속)																																
규칙 ID																																
규칙 작업																	규칙 이유															
이니시에이터 포트																	응답자 포트															


바이트
0
1
2
3
비트
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
TCP 플래그
프로토콜
NetFlow 소스
NetFlow 소스(계속)
NetFlow 소스(계속)
NetFlow 소스(계속)
NetFlow 소스(계속)
인스턴스 ID
인스턴스 ID(계속)
연결 카운터
첫 번째 패킷 타임스탬프
첫 번째 패킷 타임스탬프(계속)
마지막 패킷 타임스탬프
마지막 패킷 타임스탬프(계속)
이니시에이터 전송 패킷
이니시에이터 전송 패킷(계속)
이니시에이터 전송 패킷(계속)
응답자 전송 패킷
응답자 전송 패킷(계속)
응답자 전송 패킷(계속)
이니시에이터 전송 바이트
이니시에이터 전송 바이트(계속)
이니시에이터 전송 바이트(계속)
응답자 전송 바이트
응답자 전송 바이트(계속)
응답자 전송 바이트(계속)
사용자 ID
사용자 ID(계속)
애플리케이션 프로토콜 ID
애플리케이션 프로토콜 ID(계속)
URL 카테고리
URL 카테고리(계속)
URL 평판
URL 평판(계속)
클라이언트 애플리케이션 ID
클라이언트 애플리케이션 ID(계속)
웹 애플리케이션 ID


바이트
0
1
2
3
비트
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
클라이언트 URL
웹 애플리케이션 ID(계속)
문자열 블록 유형(0)
문자열 블록 유형(계속)
문자열 블록 길이
문자열 블록 길이(계속)
클라이언트 애플리케이션 URL...
NetBIOS 이름
문자열 블록 유형(0)
문자열 블록 길이
NetBIOS 이름...
클라이언트 애플리케이션 버전
문자열 블록 유형(0)
문자열 블록 길이
클라이언트 애플리케이션 버전...
모니터링 규칙 1
모니터링 규칙 2
모니터링 규칙 3
모니터링 규칙 4
모니터링 규칙 5
모니터링 규칙 6
모니터링 규칙 7
모니터링 규칙 8
보안 인텔리전스 소스/대상
보안 인텔리전스 계층
파일 이벤트 개수
침입 이벤트 개수
이니시에이터 국가
응답자 국가
IOC 번호
소스 자동 시스템
대상 자동 시스템


바이트
0
1
2
3
비트
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
SNMP 입력
SNMP 출력
소스 TOS
대상 TOS
소스 마스크
대상 마스크
보안 상황
보안 상황(계속)
보안 상황(계속)
보안 상황(계속)
참조된 호스트
VLAN ID
문자열 블록 유형(0)
문자열 블록 유형(0)(계속)
문자열 블록 길이
문자열 블록 길이(계속)
참조된 호스트...
사용자 에이전트
문자열 블록 유형(0)
문자열 블록 길이
사용자 에이전트...
HTTP 참조 페이지
문자열 블록 유형(0)
문자열 블록 길이
HTTP 참조 페이지...
SSL 인증서 핑거프린트
SSL 인증서 핑거프린트(계속)
SSL 인증서 핑거프린트(계속)
SSL 인증서 핑거프린트(계속)
SSL 인증서 핑거프린트(계속)
SSL 정책 ID
SSL 정책 ID(계속)
SSL 정책 ID(계속)
SSL 정책 ID(계속)


바이트
0
1
2
3
비트
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
SSL 규칙 ID
SSL 암호 그룹
SSL 버전
SSL 서버 인증서 상태
SSL 서버 인증서 상태(계속)
SSL 실제 작업
SSL 예상 작업
SSL 예상 작업(계속)
SSL 플로우 상태
SSL 플로우 오류
SSL 플로우 오류(계속)
SSL 플로우 메시지
SSL 플로우 메시지(계속)
SSL 플로우 플래그
SSL 플로우 플래그(계속)
SSL 플로우 플래그(계속)
문자열 블록 유형(0)
문자열 블록 유형(0)(계속)
문자열 블록 길이
문자열 블록 길이(계속)
SSL 서버 이름...
SSL 서버 이름
SSL URL 카테고리
SSL 세션 ID
SSL 세션 ID(계속)
SSL 세션 ID(계속)
SSL 세션 ID(계속)
SSL 세션 ID(계속)
SSL 세션 ID(계속)
SSL 세션 ID(계속)
SSL 세션 ID(계속)
SSL 세션 ID 길이
SSL 티켓 ID
SSL 티켓 ID(계속)
SSL 티켓 ID(계속)
SSL 티켓 ID(계속)



다음 표에는 5.4 이상 버전용 연결 통계 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 B-36 5.4 이상 버전용 연결 통계 데이터 블록 필드

필드	데이터 유형	설명
연결 통계 데이터 블록 유형	uint32	5.4 이상 버전용 연결 통계 데이터 블록을 시작합니다. 값은 항상 155입니다.
연결 통계 데이터 블록 길이	uint32	연결 통계 데이터 블록의 바이트 수입니다. 여기에는 연결 통계 블록 유형 및 길이 필드의 8바이트에 그 뒤의 연결 데이터 바이트 수를 더한 값이 포함됩니다.
디바이스 ID	uint32	연결 이벤트를 탐지한 디바이스입니다.
인그레스 영역	uint8[16]	정책 위반을 트리거한 이벤트의 인그레스 보안 영역입니다.
이그레스 (egress) 영역	uint8[16]	정책 위반을 트리거한 이벤트의 이그레스(egress) 보안 영역입니다.
인그레스 인터페이스	uint8[16]	인바운드 트래픽용 인터페이스입니다.
이그레스 (egress) 인터페이스	uint8[16]	아웃바운드 트래픽용 인터페이스입니다.
이니시에이터 IP 주소	uint8[16]	연결 이벤트에서 설명하는 세션을 시작한 호스트의 IP 주소(IP 주소 옥텟 형식)입니다.
응답자 IP 주소	uint8[16]	시작 호스트에 응답한 호스트의 IP 주소(IP 주소 옥텟 형식)입니다.
정책 수정	uint8[16]	해당하는 경우 트리거된 상관관계와 관련된 규칙의 수정 번호입니다.
규칙 ID	uint32	해당하는 경우 이벤트를 트리거한 규칙의 내부 식별자입니다.
규칙 작업	uint16	해당 규칙(허용, 차단 등)에 대해 사용자 인터페이스에서 선택한 작업입니다.
규칙 이유	uint16	규칙이 이벤트를 트리거한 이유입니다.

표 B-36 5.4 이상 버전용 연결 통계 데이터 블록 필드 (계속)

필드	데이터 유형	설명
이니시에이터 포트	uint16	시작 호스트에 사용되는 포트입니다.
응답자 포트	uint16	응답 호스트에 사용되는 포트입니다.
TCP 플래그	uint16	연결 이벤트에 대한 모든 TCP 플래그를 나타냅니다.
프로토콜	uint8	IANA에서 지정한 프로토콜 번호입니다.
NetFlow 소스	uint8[16]	연결에 대한 데이터를 내보낸 NetFlow 지원 디바이스의 IP 주소입니다.
인스턴스 ID	uint16	이벤트를 생성한 매니지드 디바이스의 Snort 인스턴스의 숫자 ID입니다.
연결 카운터	uint16	1초 이내에 발생하는 연결 이벤트를 구별하는 데 사용되는 값입니다.
첫 번째 패킷 타임스탬프	uint32	세션에서 첫 번째 패킷이 교환된 날짜의 시간의 UNIX 타임스탬프입니다.
마지막 패킷 타임스탬프	uint32	세션에서 마지막 패킷이 교환된 날짜의 시간의 UNIX 타임스탬프입니다.
이니시에이터 전송 패킷	uint64	시작 호스트에서 전송한 패킷 수입니다.
응답자 전송 패킷	uint64	응답 호스트에서 전송한 패킷 수입니다.
이니시에이터 전송 바이트	uint64	시작 호스트에서 전송한 바이트 수입니다.
응답자 전송 바이트	uint64	응답 호스트에서 전송한 바이트 수입니다.
사용자 ID	uint32	트래픽을 생성한 호스트에 마지막으로 로그인한 사용자의 내부 ID 번호입니다.
애플리케이션 프로토콜 ID	uint32	애플리케이션 프로토콜의 애플리케이션 ID입니다.
URL 카테고리	uint32	URL 카테고리의 내부 ID 번호입니다.
URL 평판	uint32	URL 평판의 내부 ID 번호입니다.
클라이언트 애플리케이션 ID	uint32	해당하는 경우 탐지된 클라이언트 애플리케이션의 내부 ID 번호입니다.
웹 애플리케이션 ID	uint32	해당하는 경우 탐지된 웹 애플리케이션의 내부 ID 번호입니다.
문자열 블록 유형	uint32	클라이언트 애플리케이션 URL에 대한 문자열 데이터 블록을 시작합니다. 이 값은 항상 `0`입니다.
문자열 블록 길이	uint32	클라이언트 애플리케이션 URL 문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이 필드의 8바이트에 클라이언트 애플리케이션 URL 문자열의 바이트 수를 더한 값이 포함됩니다.
클라이언트 애플리케이션 URL	string	해당하는 경우 클라이언트 애플리케이션이 액세스한 URL입니다. 예를 들면 `/files/index.html`과 같습니다.

표 B-36 5.4 이상 버전용 연결 통계 데이터 블록 필드 (계속)

필드	데이터 유형	설명
문자열 블록 유형	uint32	호스트 NetBIOS 이름에 대한 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이 필드의 8바이트에 NetBIOS 이름 문자열의 바이트 수를 더한 값이 포함됩니다.
NetBIOS 이름	string	호스트 NetBIOS 이름 문자열입니다.
문자열 블록 유형	uint32	클라이언트 애플리케이션 버전에 대한 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	클라이언트 애플리케이션 버전에 대한 문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이의 8바이트에 버전의 바이트 수를 더한 값이 포함됩니다.
클라이언트 애플리케이션 버전	string	클라이언트 애플리케이션 버전입니다.
모니터링 규칙 1	uint32	연결 이벤트와 관련된 첫 번째 모니터 규칙의 ID입니다.
모니터링 규칙 2	uint32	연결 이벤트와 관련된 두 번째 모니터 규칙의 ID입니다.
모니터링 규칙 3	uint32	연결 이벤트와 관련된 세 번째 모니터 규칙의 ID입니다.
모니터링 규칙 4	uint32	연결 이벤트와 관련된 네 번째 모니터 규칙의 ID입니다.
모니터링 규칙 5	uint32	연결 이벤트와 관련된 다섯 번째 모니터 규칙의 ID입니다.
모니터링 규칙 6	uint32	연결 이벤트와 관련된 여섯 번째 모니터 규칙의 ID입니다.
모니터링 규칙 7	uint32	연결 이벤트와 관련된 일곱 번째 모니터 규칙의 ID입니다.
모니터링 규칙 8	uint32	연결 이벤트와 관련된 여덟 번째 모니터 규칙의 ID입니다.
보안 인텔리전스 소스/대상	uint8	소스 또는 대상 IP 주소가 IP 블랙리스트와 일치했는지를 나타냅니다.
보안 인텔리전스 계층	uint8	IP 블랙리스트와 일치한 IP 계층입니다.
파일 이벤트 개수	uint16	1초 이내에 발생하는 파일 이벤트를 구별하는 데 사용되는 값입니다.
침입 이벤트 개수	uint16	1초 이내에 발생하는 침입 이벤트를 구별하는 데 사용되는 값입니다.
이니시에이터 국가	uint16	시작 호스트의 국가 코드입니다.
응답자 국가	uint16	응답 호스트의 국가 코드입니다.
IOC 번호	uint16	이 이벤트와 관련된 보안 침해의 ID 번호입니다.
소스 자동 시스템	uint32	소스의 AS 번호(원본 또는 피어)입니다.
대상 자동 시스템	uint32	대상의 AS 번호(원본 또는 피어)입니다.
SNMP 입력	uint16	입력 인터페이스의 SNMP 인덱스입니다.
SNMP 출력	uint16	출력 인터페이스의 SNMP 인덱스입니다.
소스 TOS	uint8	들어오는 인터페이스에 대한 서비스 유형 바이트 설정입니다.
대상 TOS	uint8	나가는 인터페이스에 대한 서비스 유형 바이트 설정입니다.

표 B-36 5.4 이상 버전용 연결 통계 데이터 블록 필드 (계속)

필드	데이터 유형	설명
소스 마스크	uint8	소스 주소 접두사 마스크입니다.
대상 마스크	uint8	대상 주소 접두사 마스크입니다.
보안 상황	uint8(16)	트래픽이 통과한 보안 상황(가상 방화벽)의 ID 번호입니다. 이 필드는 다중 컨텍스트 모드의 ASA FirePOWER 디바이스에 대해서만 채워집니다.
VLAN ID	uint16	호스트가 구성원으로 포함된 VLAN을 나타내는 VLAN ID 번호입니다.
문자열 블록 유형	uint32	참조된 호스트 이름을 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	참조된 호스트 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Referenced Host(참조된 호스트) 필드의 바이트 수를 더한 값이 포함됩니다.
참조된 호스트	string	HTTP 또는 DNS로 제공되는 호스트 이름 정보입니다.
문자열 블록 유형	uint32	사용자 에이전트를 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	사용자 에이전트 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 User Agent(사용자 에이전트) 필드의 바이트 수를 더한 값이 포함됩니다.
사용자 에이전트	string	세션에서 UserAgent 헤더 필드의 정보입니다.
문자열 블록 유형	uint32	HTTP 참조 페이지를 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	HTTP 참조 페이지 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 HTTP Referer(HTTP 참조 페이지) 필드의 바이트 수를 더한 값이 포함됩니다.
HTTP 참조 페이지	string	페이지가 생성된 사이트입니다. HTTP 트래픽의 참조 페이지 헤더 정보에서 찾을 수 있습니다.
SSL 인증서 핑거프린트	uint8[20]	SSL 서버 인증서의 SHA1 해시입니다.
SSL 정책 ID	uint8[16]	연결을 처리한 SSL 정책의 ID 번호입니다.
SSL 규칙 ID	uint32	연결을 처리한 SSL 규칙 또는 기본 동작의 ID 번호입니다.
SSL 암호 그룹	uint16	SSL 연결에서 사용되는 암호화 그룹입니다. 값은 10진수 형식으로 저장됩니다. 값으로 지정되는 암호 그룹은 `www.iana.org/assignments/tls-parameters/tls-parameters.xhtml`을 참조하십시오.
SSL 버전	uint8	연결을 암호화하는 데 사용된 SSL 또는 TLS 프로토콜 버전입니다.

표 B-36 5.4 이상 버전용 연결 통계 데이터 블록 필드 (계속)

필드	데이터 유형	설명
SSL 서버 인증서 상태	uint16	SSL 인증서의 상태입니다. 가능한 값은 다음과 같습니다. • 0 - 확인되지 않음 - 서버 인증서 상태를 평가하지 않았습니다. • 1 - 알 수 없음 - 서버 인증서 상태를 확인할 수 없습니다. • 2 - 유효 - 서버 인증서가 유효합니다. • 4 - 자체 서명 - 서버 인증서가 자체 서명되었습니다. • 16 - 유효하지 않은 발급자 - 서버 인증서의 발급자가 유효하지 않습니다. • 32 - 유효하지 않은 서명 - 서버 인증서의 서명이 유효하지 않습니다. • 64 - 만료됨 - 서버 인증서가 만료되었습니다. • 128 - 아직 유효하지 않음 - 서버 인증서가 아직 유효하지 않습니다. • 256 - 해지됨 - 서버 인증서가 해지되었습니다.
SSL 실제 작업	uint16	SSL 규칙에 기반한 연결에서 수행된 작업입니다. 규칙에 명시된 작업이 가능하지 않을 수도 있으므로, 이는 예상 작업과 다를 수 있습니다. 가능한 값은 다음과 같습니다. • 0 - '알 수 없음' • 1 - '암호 해독 안 함' • 2 - '차단' • 3 - '차단 및 재설정' • 4 - '암호 해독(알려진 키)' • 5 - '암호 해독(키 교체)' • 6 - '암호 해독(재서명)'
SSL 예상 작업	uint16	SSL 규칙에 기반한 연결에서 수행해야 하는 작업입니다. 가능한 값은 다음과 같습니다. • 0 - '알 수 없음' • 1 - '암호 해독 안 함' • 2 - '차단' • 3 - '차단 및 재설정' • 4 - '암호 해독(알려진 키)' • 5 - '암호 해독(키 교체)' • 6 - '암호 해독(재서명)'

표 B-36 5.4 이상 버전용 연결 통계 데이터 블록 필드 (계속)

필드	데이터 유형	설명
SSL 플로우 상태	uint16	SSL 플로우의 상태입니다. 이 값은 작업을 수행한 이유 또는 오류 메시지가 표시된 이유를 설명합니다. 가능한 값은 다음과 같습니다. • 0 - '알 수 없음' • 1 - '일치하지 않음' • 2 - '성공' • 3 - '캐시되지 않은 세션' • 4 - '알 수 없는 암호 그룹' • 5 - '지원되지 않는 암호 그룹' • 6 - '지원되지 않는 SSL 버전' • 7 - 'SSL 압축 사용됨' • 8 - '패시브 모드에서 세션 암호 해독 불가' • 9 - '핸드셰이크 오류' • 10 - '암호 해독 오류' • 11 - '서버 이름 카테고리 조회 보류 중' • 12 - '공용 이름 카테고리 조회 보류 중' • 13 - '내부 오류' • 14 - '네트워크 파라미터 사용 불가' • 15 - '유효하지 않은 서버 인증서 핸들' • 16 - '서버 인증서 핑거프린트 사용 불가' • 17 - '주체 DN을 캐시할 수 없음' • 18 - '발급자 DN을 캐시할 수 없음' • 19 - '알 수 없는 SSL 버전' • 20 - '외부 인증서 목록 사용 불가' • 21 - '외부 인증서 핑거프린트 사용 불가' • 22 - '내부 인증서 목록이 유효하지 않음' • 23 - '내부 인증서 목록 사용 불가' • 24 - '내부 인증서 사용 불가' • 25 - '내부 인증서 핑거프린트 사용 불가' • 26 - '서버 인증서 검증 사용 불가' • 27 - '서버 인증서 검증 장애' • 28 - '유효하지 않은 작업'
SSL 플로우 오류	uint32	자세한 SSL 오류 코드입니다. 이러한 값은 지원용으로 필요할 수 있습니다.

표 B-36 5.4 이상 버전용 연결 통계 데이터 블록 필드 (계속)

필드	데이터 유형	설명
SSL 플로우 메시지	uint32	SSL 핸드셰이크 도중 클라이언트와 서버 간에 교환된 메시지입니다. 자세한 내용은 http://tools.ietf.org/html/rfc5246을 참조하십시오. • 0x00000001 — NSE_MT__HELLO_REQUEST • 0x00000002 — NSE_MT__CLIENT_ALERT • 0x00000004 — NSE_MT__SERVER_ALERT • 0x00000008 — NSE_MT__CLIENT_HELLO • 0x00000010 — NSE_MT__SERVER_HELLO • 0x00000020 — NSE_MT__SERVER_CERTIFICATE • 0x00000040 — NSE_MT__SERVER_KEY_EXCHANGE • 0x00000080 — NSE_MT__CERTIFICATE_REQUEST • 0x00000100 — NSE_MT__SERVER_HELLO_DONE • 0x00000200 — NSE_MT__CLIENT_CERTIFICATE • 0x00000400 — NSE_MT__CLIENT_KEY_EXCHANGE • 0x00000800 — NSE_MT__CERTIFICATE_VERIFY • 0x00001000 — NSE_MT__CLIENT_CHANGE_CIPHER_SPEC • 0x00002000 — NSE_MT__CLIENT_FINISHED • 0x00004000 — NSE_MT__SERVER_CHANGE_CIPHER_SPEC • 0x00008000 — NSE_MT__SERVER_FINISHED • 0x00010000 — NSE_MT__NEW_SESSION_TICKET • 0x00020000 — NSE_MT__HANDSHAKE_OTHER • 0x00040000 — NSE_MT__APP_DATA_FROM_CLIENT • 0x00080000 — NSE_MT__APP_DATA_FROM_SERVER
SSL 플로우 플래그	uint64	암호화된 연결에 대한 디버깅 레벨 플래그입니다. 가능한 값은 다음과 같습니다. • 0x00000001 - NSE_FLOW__VALID - 다른 필드를 유효하게 만들려면 설정해야 함 • 0x00000002 - NSE_FLOW__INITIALIZED - 처리 준비가 완료된 내부 구조 • 0x00000004 - NSE_FLOW__INTERCEPT - SSL 세션이 중단됨
문자열 블록 유형	uint32	SSL 서버 이름을 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	SSL 서버 이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 SSL Server Name(SSL 서버 이름) 필드의 바이트 수를 더한 값이 포함됩니다.

표 B-36 5.4 이상 버전용 연결 통계 데이터 블록 필드 (계속)

필드	데이터 유형	설명
SSL 서버 이름	string	SSL Client Hello의 서버 이름 표시에서 제공된 이름입니다.
SSL URL 카테고리	uint32	서버 이름 및 인증서 일반 이름에서 확인된 플로우의 카테고리입니다.
SSL 세션 ID	uint8[32]	클라이언트와 서버가 세션 재사용에 동의하는 경우 SSL 핸드셰이크 중에 사용되는 세션 ID의 값입니다.
SSL 세션 ID 길이	uint8	SSL 세션 ID의 길이입니다. 세션 ID는 32바이트를 초과할 수는 없으며 32바이트보다 작을 수는 있습니다.
SSL 티켓 ID	uint8[20]	클라이언트와 서버가 세션 티켓 사용에 동의하는 경우 사용되는 세션 티켓의 해시입니다.
SSL 티켓 ID 길이	uint8	SSL 티켓 ID의 길이입니다. 티켓 ID는 20바이트를 초과할 수는 없으며 20바이트보다 작을 수는 있습니다.
네트워크 분석 정책 수정	uint8[16]	연결 이벤트와 관련된 네트워크 분석 정책의 수정 버전입니다.

5.4.1 버전용 연결 통계 데이터 블록

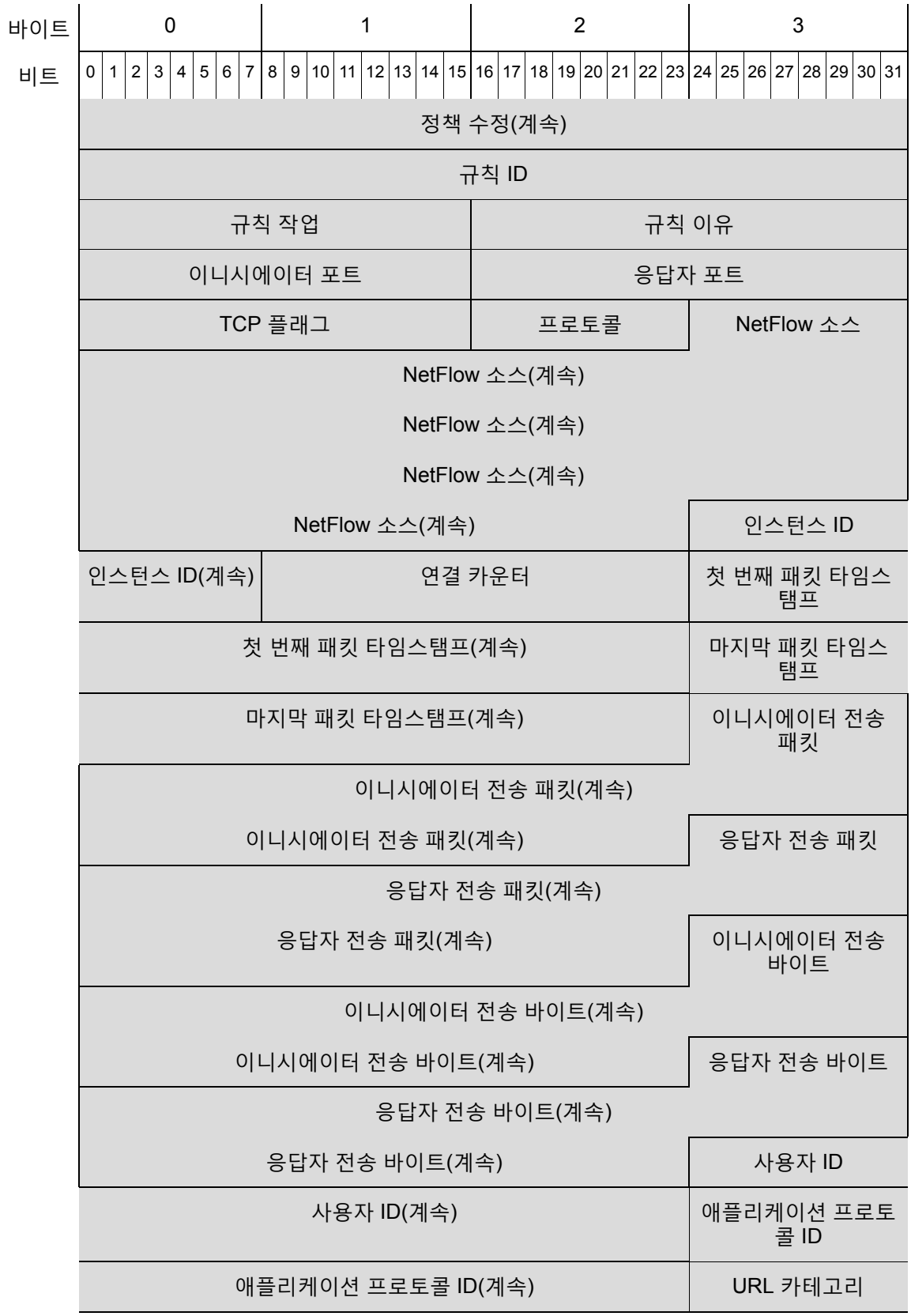
연결 통계 데이터 블록은 연결 데이터 메시지에 사용됩니다. 5.4 버전용 연결 통계 데이터 블록에는 새 필드가 여러 개 추가되었습니다. SSL 연결, HTTP 리디렉션 및 네트워크 분석 정책용 필드가 추가되었습니다. 계열 1 블록 그룹에서 5.4 이상 버전용 연결 통계 데이터 블록의 블록 유형은 157입니다. 이는 블록 유형 155(5.3.1 버전용 연결 통계 데이터 블록, 페이지 B-161)의 사용을 중단합니다.

이벤트 버전이 12이고 이벤트 코드가 71인 요청 메시지에서 확장 이벤트 플래그(Request Flags(요청 플래그) 필드의 비트 30)를 설정하여 연결 이벤트 레코드를 요청합니다. 요청 플래그, 페이지 2-12의 내용을 참조하십시오. 비트 23을 활성화하면 레코드에 확장 이벤트 헤더가 포함됩니다.

연결 통계 데이터 메시지에 대한 자세한 정보는 연결 통계 데이터 메시지, 페이지 4-54의 내용을 참조하십시오.

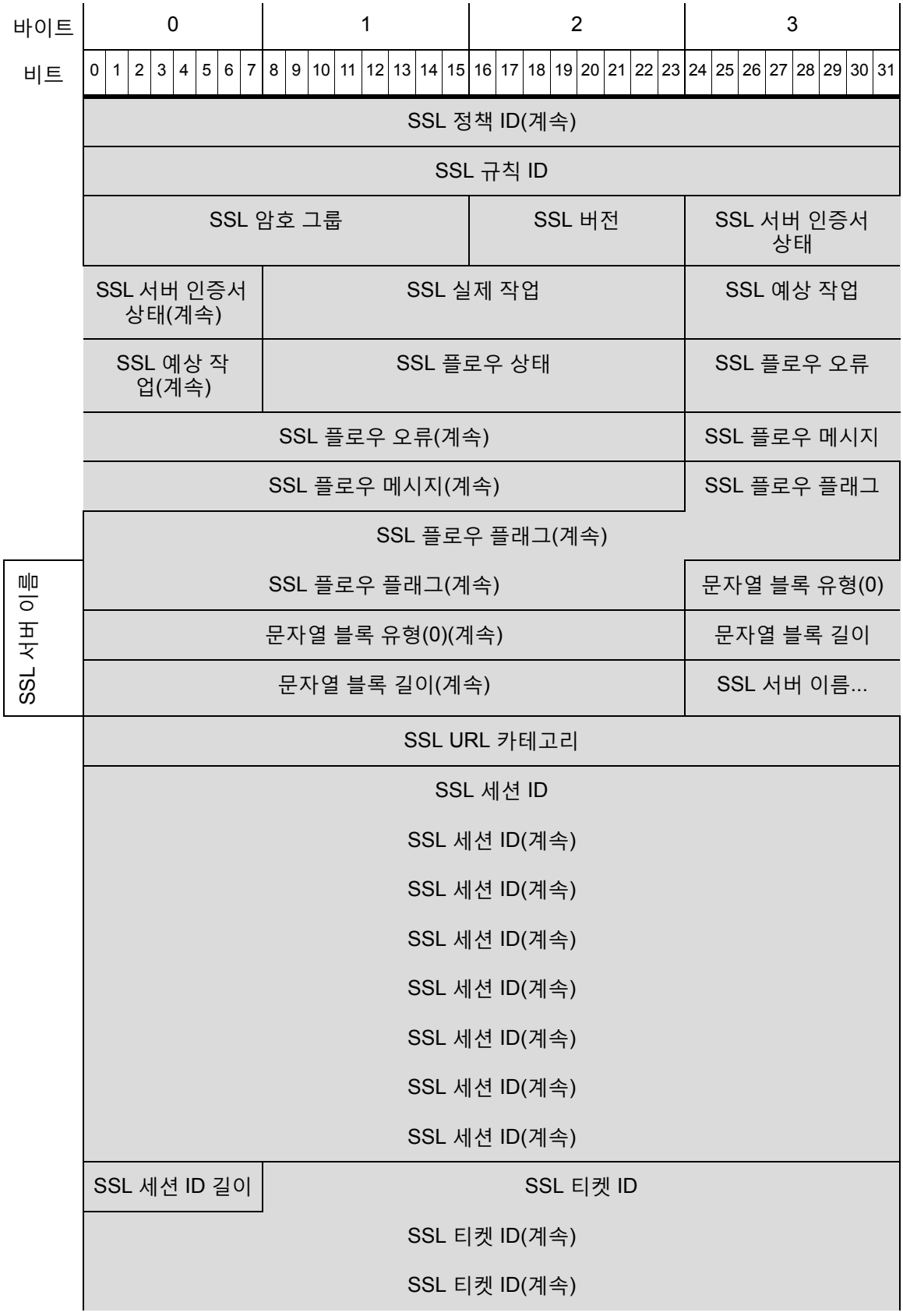
다음 다이어그램에 5.4 이상 버전의 연결 통계 데이터 블록 형식이 나와 있습니다.

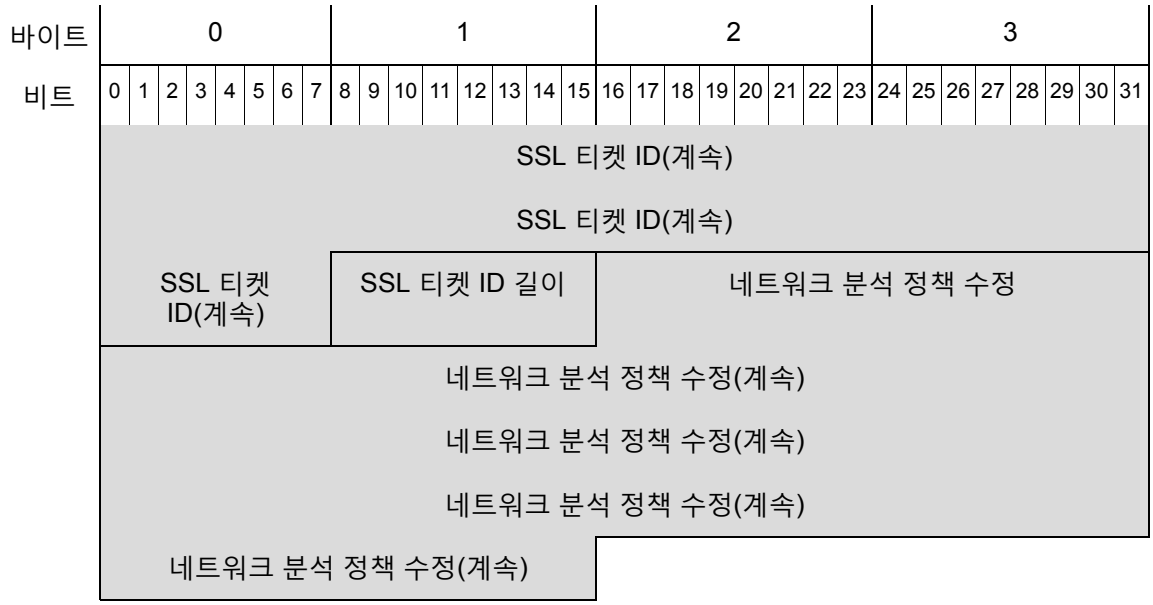
바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
인그레스 영역(계속)																																
이그레스(egress) 영역																																
이그레스(egress) 영역(계속)																																
이그레스(egress) 영역(계속)																																
이그레스(egress) 영역(계속)																																
인그레스 인터페이스																																
인그레스 인터페이스(계속)																																
인그레스 인터페이스(계속)																																
인그레스 인터페이스(계속)																																
이그레스(egress) 인터페이스																																
이그레스(egress) 인터페이스(계속)																																
이그레스(egress) 인터페이스(계속)																																
이그레스(egress) 인터페이스(계속)																																
이니시에이터 IP 주소																																
이니시에이터 IP 주소(계속)																																
이니시에이터 IP 주소(계속)																																
이니시에이터 IP 주소(계속)																																
응답자 IP 주소																																
응답자 IP 주소(계속)																																
응답자 IP 주소(계속)																																
응답자 IP 주소(계속)																																
정책 수정																																
정책 수정(계속)																																
정책 수정(계속)																																


바이트
0
1
2
3
비트
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
정책 수정(계속)
규칙 ID
규칙 작업
규칙 이유
이니시에이터 포트
응답자 포트
TCP 플래그
프로토콜
NetFlow 소스
NetFlow 소스(계속)
NetFlow 소스(계속)
NetFlow 소스(계속)
NetFlow 소스(계속)
인스턴스 ID
인스턴스 ID(계속)
연결 카운터
첫 번째 패킷 타임스탬프
첫 번째 패킷 타임스탬프(계속)
마지막 패킷 타임스탬프
마지막 패킷 타임스탬프(계속)
이니시에이터 전송 패킷
이니시에이터 전송 패킷(계속)
이니시에이터 전송 패킷(계속)
응답자 전송 패킷
응답자 전송 패킷(계속)
응답자 전송 패킷(계속)
이니시에이터 전송 바이트
이니시에이터 전송 바이트(계속)
이니시에이터 전송 바이트(계속)
응답자 전송 바이트
응답자 전송 바이트(계속)
응답자 전송 바이트(계속)
사용자 ID
사용자 ID(계속)
애플리케이션 프로토콜 ID
애플리케이션 프로토콜 ID(계속)
URL 카테고리

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	URL 카테고리(계속)																								URL 평판							
	URL 평판(계속)																								클라이언트 애플리케이션 ID							
	클라이언트 애플리케이션 ID(계속)																								웹 애플리케이션 ID							
클라이언트 URL	웹 애플리케이션 ID(계속)																								문자열 블록 유형(0)							
클라이언트 URL	문자열 블록 유형(계속)																								문자열 블록 길이							
클라이언트 URL	문자열 블록 길이(계속)																								클라이언트 애플리케이션 URL...							
NetBIOS 이름	문자열 블록 유형(0)																															
NetBIOS 이름	문자열 블록 길이																															
NetBIOS 이름	NetBIOS 이름...																															
클라이언트 애플리케이션 버전	문자열 블록 유형(0)																															
클라이언트 애플리케이션 버전	문자열 블록 길이																															
클라이언트 애플리케이션 버전	클라이언트 애플리케이션 버전...																															
	모니터링 규칙 1																															
	모니터링 규칙 2																															
	모니터링 규칙 3																															
	모니터링 규칙 4																															
	모니터링 규칙 5																															
	모니터링 규칙 6																															
	모니터링 규칙 7																															
	모니터링 규칙 8																															
	보안 인텔리전스 소스/대상								보안 인텔리전스 계층								파일 이벤트 개수															
	침입 이벤트 개수																이니시에이터 국가															
	응답자 국가																IOC 번호															


바이트
0
1
2
3
비트
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
소스 자동 시스템
대상 자동 시스템
SNMP 입력
SNMP 출력
소스 TOS
대상 TOS
소스 마스크
대상 마스크
보안 상황
보안 상황(계속)
보안 상황(계속)
보안 상황(계속)
참조된 호스트
VLAN ID
문자열 블록 유형(0)
문자열 블록 유형(0)(계속)
문자열 블록 길이
문자열 블록 길이(계속)
참조된 호스트...
사용자 에이전트
문자열 블록 유형(0)
문자열 블록 길이
사용자 에이전트...
HTTP 참조 페이지
문자열 블록 유형(0)
문자열 블록 길이
HTTP 참조 페이지...
SSL 인증서 핑거프린트
SSL 인증서 핑거프린트(계속)
SSL 인증서 핑거프린트(계속)
SSL 인증서 핑거프린트(계속)
SSL 인증서 핑거프린트(계속)
SSL 정책 ID
SSL 정책 ID(계속)
SSL 정책 ID(계속)


바이트
0
1
2
3
비트
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
SSL 정책 ID(계속)
SSL 규칙 ID
SSL 암호 그룹
SSL 버전
SSL 서버 인증서 상태
SSL 서버 인증서 상태(계속)
SSL 실제 작업
SSL 예상 작업
SSL 예상 작업(계속)
SSL 플로우 상태
SSL 플로우 오류
SSL 플로우 오류(계속)
SSL 플로우 메시지
SSL 플로우 메시지(계속)
SSL 플로우 플래그
SSL 플로우 플래그(계속)
SSL 서버 이름
SSL 플로우 플래그(계속)
문자열 블록 유형(0)
문자열 블록 유형(0)(계속)
문자열 블록 길이
문자열 블록 길이(계속)
SSL 서버 이름...
SSL URL 카테고리
SSL 세션 ID
SSL 세션 ID(계속)
SSL 세션 ID(계속)
SSL 세션 ID(계속)
SSL 세션 ID(계속)
SSL 세션 ID(계속)
SSL 세션 ID(계속)
SSL 세션 ID(계속)
SSL 세션 ID 길이
SSL 티켓 ID
SSL 티켓 ID(계속)
SSL 티켓 ID(계속)



다음 표에는 5.4 이상 버전용 연결 통계 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 B-37 5.4 이상 버전용 연결 통계 데이터 블록 필드

필드	데이터 유형	설명
연결 통계 데이터 블록 유형	uint32	5.4 이상 버전용 연결 통계 데이터 블록을 시작합니다. 값은 항상 157입니다.
연결 통계 데이터 블록 길이	uint32	연결 통계 데이터 블록의 바이트 수입니다. 여기에는 연결 통계 블록 유형 및 길이 필드의 8바이트에 그 뒤의 연결 데이터 바이트 수를 더한 값이 포함됩니다.
디바이스 ID	uint32	연결 이벤트를 탐지한 디바이스입니다.
인그레스 영역	uint8[16]	정책 위반을 트리거한 이벤트의 인그레스 보안 영역입니다.
이그레스(egress) 영역	uint8[16]	정책 위반을 트리거한 이벤트의 이그레스(egress) 보안 영역입니다.
인그레스 인터페이스	uint8[16]	인바운드 트래픽용 인터페이스입니다.
이그레스(egress) 인터페이스	uint8[16]	아웃바운드 트래픽용 인터페이스입니다.
이니시에이터 IP 주소	uint8[16]	연결 이벤트에서 설명하는 세션을 시작한 호스트의 IP 주소(IP 주소 옥텟 형식)입니다.
응답자 IP 주소	uint8[16]	시작 호스트에 응답한 호스트의 IP 주소(IP 주소 옥텟 형식)입니다.
정책 수정	uint8[16]	해당하는 경우 트리거된 상관관계와 관련된 규칙의 수정 번호입니다.
규칙 ID	uint32	해당하는 경우 이벤트를 트리거한 규칙의 내부 식별자입니다.

표 B-37 5.4 이상 버전용 연결 통계 데이터 블록 필드 (계속)

필드	데이터 유형	설명
규칙 작업	uint16	해당 규칙(허용, 차단 등)에 대해 사용자 인터페이스에서 선택한 작업입니다.
규칙 이유	uint16	규칙이 이벤트를 트리거한 이유입니다.
이니시에이터 포트	uint16	시작 호스트에 사용되는 포트입니다.
응답자 포트	uint16	응답 호스트에 사용되는 포트입니다.
TCP 플래그	uint16	연결 이벤트에 대한 모든 TCP 플래그를 나타냅니다.
프로토콜	uint8	IANA에서 지정한 프로토콜 번호입니다.
NetFlow 소스	uint8[16]	연결에 대한 데이터를 내보낸 NetFlow 지원 디바이스의 IP 주소입니다.
인스턴스 ID	uint16	이벤트를 생성한 매니지드 디바이스의 Snort 인스턴스의 숫자 ID입니다.
연결 카운터	uint16	1초 이내에 발생하는 연결 이벤트를 구별하는 데 사용되는 값입니다.
첫 번째 패킷 타임스탬프	uint32	세션에서 첫 번째 패킷이 교환된 날짜의 시간의 UNIX 타임스탬프입니다.
마지막 패킷 타임스탬프	uint32	세션에서 마지막 패킷이 교환된 날짜의 시간의 UNIX 타임스탬프입니다.
이니시에이터 전송 패킷	uint64	시작 호스트에서 전송한 패킷 수입니다.
응답자 전송 패킷	uint64	응답 호스트에서 전송한 패킷 수입니다.
이니시에이터 전송 바이트	uint64	시작 호스트에서 전송한 바이트 수입니다.
응답자 전송 바이트	uint64	응답 호스트에서 전송한 바이트 수입니다.
사용자 ID	uint32	트래픽을 생성한 호스트에 마지막으로 로그인한 사용자의 내부 ID 번호입니다.
애플리케이션 프로토콜 ID	uint32	애플리케이션 프로토콜의 애플리케이션 ID입니다.
URL 카테고리	uint32	URL 카테고리의 내부 ID 번호입니다.
URL 평판	uint32	URL 평판의 내부 ID 번호입니다.
클라이언트 애플리케이션 ID	uint32	해당하는 경우 탐지된 클라이언트 애플리케이션의 내부 ID 번호입니다.
웹 애플리케이션 ID	uint32	해당하는 경우 탐지된 웹 애플리케이션의 내부 ID 번호입니다.
문자열 블록 유형	uint32	클라이언트 애플리케이션 URL에 대한 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	클라이언트 애플리케이션 URL 문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이 필드의 8바이트에 클라이언트 애플리케이션 URL 문자열의 바이트 수를 더한 값이 포함됩니다.

표 B-37 5.4 이상 버전용 연결 통계 데이터 블록 필드 (계속)

필드	데이터 유형	설명
클라이언트 애플리케이션 URL	string	해당하는 경우 클라이언트 애플리케이션이 액세스한 URL입니다. 예를 들면 `/files/index.html`과 같습니다.
문자열 블록 유형	uint32	호스트 NetBIOS 이름에 대한 문자열 데이터 블록을 시작합니다. 이 값은 항상 `0`입니다.
문자열 블록 길이	uint32	문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이 필드의 8바이트에 NetBIOS 이름 문자열의 바이트 수를 더한 값이 포함됩니다.
NetBIOS 이름	string	호스트 NetBIOS 이름 문자열입니다.
문자열 블록 유형	uint32	클라이언트 애플리케이션 버전에 대한 문자열 데이터 블록을 시작합니다. 이 값은 항상 `0`입니다.
문자열 블록 길이	uint32	클라이언트 애플리케이션 버전에 대한 문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이의 8바이트에 버전의 바이트 수를 더한 값이 포함됩니다.
클라이언트 애플리케이션 버전	string	클라이언트 애플리케이션 버전입니다.
모니터링 규칙 1	uint32	연결 이벤트와 관련된 첫 번째 모니터 규칙의 ID입니다.
모니터링 규칙 2	uint32	연결 이벤트와 관련된 두 번째 모니터 규칙의 ID입니다.
모니터링 규칙 3	uint32	연결 이벤트와 관련된 세 번째 모니터 규칙의 ID입니다.
모니터링 규칙 4	uint32	연결 이벤트와 관련된 네 번째 모니터 규칙의 ID입니다.
모니터링 규칙 5	uint32	연결 이벤트와 관련된 다섯 번째 모니터 규칙의 ID입니다.
모니터링 규칙 6	uint32	연결 이벤트와 관련된 여섯 번째 모니터 규칙의 ID입니다.
모니터링 규칙 7	uint32	연결 이벤트와 관련된 일곱 번째 모니터 규칙의 ID입니다.
모니터링 규칙 8	uint32	연결 이벤트와 관련된 여덟 번째 모니터 규칙의 ID입니다.
보안 인텔리전스 소스/대상	uint8	소스 또는 대상 IP 주소가 IP 블랙리스트와 일치했는지를 나타냅니다.
보안 인텔리전스 계층	uint8	IP 블랙리스트와 일치한 IP 계층입니다.
파일 이벤트 개수	uint16	1초 이내에 발생하는 파일 이벤트를 구별하는 데 사용되는 값입니다.
침입 이벤트 개수	uint16	1초 이내에 발생하는 침입 이벤트를 구별하는 데 사용되는 값입니다.
이니시에이터 국가	uint16	시작 호스트의 국가 코드입니다.
응답자 국가	uint16	응답 호스트의 국가 코드입니다.
IOC 번호	uint16	이 이벤트와 관련된 보안 침해의 ID 번호입니다.
소스 자동 시스템	uint32	소스의 AS 번호(원본 또는 피어)입니다.
대상 자동 시스템	uint32	대상의 AS 번호(원본 또는 피어)입니다.
SNMP 입력	uint16	입력 인터페이스의 SNMP 인덱스입니다.
SNMP 출력	uint16	출력 인터페이스의 SNMP 인덱스입니다.
소스 TOS	uint8	들어오는 인터페이스에 대한 서비스 유형 바이트 설정입니다.

표 B-37 5.4 이상 버전용 연결 통계 데이터 블록 필드 (계속)

필드	데이터 유형	설명
대상 TOS	uint8	나가는 인터페이스에 대한 서비스 유형 바이트 설정입니다.
소스 마스크	uint8	소스 주소 접두사 마스크입니다.
대상 마스크	uint8	대상 주소 접두사 마스크입니다.
보안 상황	uint8(16)	트래픽이 통과한 보안 상황(가상 방화벽)의 ID 번호입니다. 이 필드는 다중 컨텍스트 모드의 ASA FirePOWER 디바이스에 대해서만 채워집니다.
VLAN ID	uint16	호스트가 구성원으로 포함된 VLAN을 나타내는 VLAN ID 번호입니다.
문자열 블록 유형	uint32	참조된 호스트 이름을 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	참조된 호스트 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Referenced Host(참조된 호스트) 필드의 바이트 수를 더한 값이 포함됩니다.
참조된 호스트	string	HTTP 또는 DNS로 제공되는 호스트 이름 정보입니다.
문자열 블록 유형	uint32	사용자 에이전트를 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	사용자 에이전트 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 User Agent(사용자 에이전트) 필드의 바이트 수를 더한 값이 포함됩니다.
사용자 에이전트	string	세션에서 UserAgent 헤더 필드의 정보입니다.
문자열 블록 유형	uint32	HTTP 참조 페이지를 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	HTTP 참조 페이지 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 HTTP Referer(HTTP 참조 페이지) 필드의 바이트 수를 더한 값이 포함됩니다.
HTTP 참조 페이지	string	페이지가 생성된 사이트입니다. HTTP 트래픽의 참조 페이지 헤더 정보에서 찾을 수 있습니다.
SSL 인증서 핑거프린트	uint8[20]	SSL 서버 인증서의 SHA1 해시입니다.
SSL 정책 ID	uint8[16]	연결을 처리한 SSL 정책의 ID 번호입니다.
SSL 규칙 ID	uint32	연결을 처리한 SSL 규칙 또는 기본 동작의 ID 번호입니다.
SSL 암호 그룹	uint16	SSL 연결에서 사용되는 암호화 그룹입니다. 값은 10진수 형식으로 저장됩니다. 값으로 지정되는 암호 그룹은 `www.iana.org/assignments/tls-parameters/tls-parameters.xhtml`을 참조하십시오.
SSL 버전	uint8	연결을 암호화하는 데 사용된 SSL 또는 TLS 프로토콜 버전입니다.

표 B-37 5.4 이상 버전용 연결 통계 데이터 블록 필드 (계속)

필드	데이터 유형	설명
SSL 서버 인증서 상태	uint16	SSL 인증서의 상태입니다. 가능한 값은 다음과 같습니다. • 0 - 확인되지 않음 - 서버 인증서 상태를 평가하지 않았습니다. • 1 - 알 수 없음 - 서버 인증서 상태를 확인할 수 없습니다. • 2 - 유효 - 서버 인증서가 유효합니다. • 4 - 자체 서명 - 서버 인증서가 자체 서명되었습니다. • 16 - 유효하지 않은 발급자 - 서버 인증서의 발급자가 유효하지 않습니다. • 32 - 유효하지 않은 서명 - 서버 인증서의 서명이 유효하지 않습니다. • 64 - 만료됨 - 서버 인증서가 만료되었습니다. • 128 - 아직 유효하지 않음 - 서버 인증서가 아직 유효하지 않습니다. • 256 - 해지됨 - 서버 인증서가 해지되었습니다.
SSL 실제 작업	uint16	SSL 규칙에 기반한 연결에서 수행된 작업입니다. 규칙에 명시된 작업이 가능하지 않을 수도 있으므로, 이는 예상 작업과 다를 수 있습니다. 가능한 값은 다음과 같습니다. • 0 - '알 수 없음' • 1 - '암호 해독 안 함' • 2 - '차단' • 3 - '차단 및 재설정' • 4 - '암호 해독(알려진 키)' • 5 - '암호 해독(키 교체)' • 6 - '암호 해독(재서명)'
SSL 예상 작업	uint16	SSL 규칙에 기반한 연결에서 수행해야 하는 작업입니다. 가능한 값은 다음과 같습니다. • 0 - '알 수 없음' • 1 - '암호 해독 안 함' • 2 - '차단' • 3 - '차단 및 재설정' • 4 - '암호 해독(알려진 키)' • 5 - '암호 해독(키 교체)' • 6 - '암호 해독(재서명)'

표 B-37 5.4 이상 버전용 연결 통계 데이터 블록 필드 (계속)

필드	데이터 유형	설명
SSL 플로우 상태	uint16	SSL 플로우의 상태입니다. 이 값은 작업을 수행한 이유 또는 오류 메시지가 표시된 이유를 설명합니다. 가능한 값은 다음과 같습니다. • 0 - '알 수 없음' • 1 - '일치하지 않음' • 2 - '성공' • 3 - '캐시되지 않은 세션' • 4 - '알 수 없는 암호 그룹' • 5 - '지원되지 않는 암호 그룹' • 6 - '지원되지 않는 SSL 버전' • 7 - 'SSL 압축 사용됨' • 8 - '패시브 모드에서 세션 암호 해독 불가' • 9 - '핸드셰이크 오류' • 10 - '암호 해독 오류' • 11 - '서버 이름 카테고리 조회 보류 중' • 12 - '공용 이름 카테고리 조회 보류 중' • 13 - '내부 오류' • 14 - '네트워크 파라미터 사용 불가' • 15 - '유효하지 않은 서버 인증서 핸들' • 16 - '서버 인증서 핑거프린트 사용 불가' • 17 - '주체 DN을 캐시할 수 없음' • 18 - '발급자 DN을 캐시할 수 없음' • 19 - '알 수 없는 SSL 버전' • 20 - '외부 인증서 목록 사용 불가' • 21 - '외부 인증서 핑거프린트 사용 불가' • 22 - '내부 인증서 목록이 유효하지 않음' • 23 - '내부 인증서 목록 사용 불가' • 24 - '내부 인증서 사용 불가' • 25 - '내부 인증서 핑거프린트 사용 불가' • 26 - '서버 인증서 검증 사용 불가' • 27 - '서버 인증서 검증 장애' • 28 - '유효하지 않은 작업'
SSL 플로우 오류	uint32	자세한 SSL 오류 코드입니다. 이러한 값은 지원용으로 필요할 수 있습니다.

표 B-37 5.4 이상 버전용 연결 통계 데이터 블록 필드 (계속)

필드	데이터 유형	설명
SSL 플로우 메시지	uint32	SSL 핸드셰이크 도중 클라이언트와 서버 간에 교환된 메시지입니다. 자세한 내용은 http://tools.ietf.org/html/rfc5246을 참조하십시오. • 0x00000001 — NSE_MT__HELLO_REQUEST • 0x00000002 — NSE_MT__CLIENT_ALERT • 0x00000004 — NSE_MT__SERVER_ALERT • 0x00000008 — NSE_MT__CLIENT_HELLO • 0x00000010 — NSE_MT__SERVER_HELLO • 0x00000020 — NSE_MT__SERVER_CERTIFICATE • 0x00000040 — NSE_MT__SERVER_KEY_EXCHANGE • 0x00000080 — NSE_MT__CERTIFICATE_REQUEST • 0x00000100 — NSE_MT__SERVER_HELLO_DONE • 0x00000200 — NSE_MT__CLIENT_CERTIFICATE • 0x00000400 — NSE_MT__CLIENT_KEY_EXCHANGE • 0x00000800 — NSE_MT__CERTIFICATE_VERIFY • 0x00001000 — NSE_MT__CLIENT_CHANGE_CIPHER_SPEC • 0x00002000 — NSE_MT__CLIENT_FINISHED • 0x00004000 — NSE_MT__SERVER_CHANGE_CIPHER_SPEC • 0x00008000 — NSE_MT__SERVER_FINISHED • 0x00010000 — NSE_MT__NEW_SESSION_TICKET • 0x00020000 — NSE_MT__HANDSHAKE_OTHER • 0x00040000 — NSE_MT__APP_DATA_FROM_CLIENT • 0x00080000 — NSE_MT__APP_DATA_FROM_SERVER
SSL 플로우 플래그	uint64	암호화된 연결에 대한 디버깅 레벨 플래그입니다. 가능한 값은 다음과 같습니다. • 0x00000001 - NSE_FLOW__VALID - 다른 필드를 유효하게 만들려면 설정해야 함 • 0x00000002 - NSE_FLOW__INITIALIZED - 처리 준비가 완료된 내부 구조 • 0x00000004 - NSE_FLOW__INTERCEPT - SSL 세션이 중단됨
문자열 블록 유형	uint32	SSL 서버 이름을 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	SSL 서버 이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 SSL Server Name(SSL 서버 이름) 필드의 바이트 수를 더한 값이 포함됩니다.

표 B-37 5.4 이상 버전용 연결 통계 데이터 블록 필드 (계속)

필드	데이터 유형	설명
SSL 서버 이름	string	SSL Client Hello의 서버 이름 표시에서 제공된 이름입니다.
SSL URL 카테고리	uint32	서버 이름 및 인증서 일반 이름에서 확인된 플로우의 카테고리입니다.
SSL 세션 ID	uint8[32]	클라이언트와 서버가 세션 재사용에 동의하는 경우 SSL 핸드셰이크 중에 사용되는 세션 ID의 값입니다.
SSL 세션 ID 길이	uint8	SSL 세션 ID의 길이입니다. 세션 ID는 32바이트를 초과할 수는 없으며 32바이트보다 작을 수는 있습니다.
SSL 티켓 ID	uint8[20]	클라이언트와 서버가 세션 티켓 사용에 동의하는 경우 사용되는 세션 티켓의 해시입니다.
SSL 티켓 ID 길이	uint8	SSL 티켓 ID의 길이입니다. 티켓 ID는 20바이트를 초과할 수는 없으며 20바이트보다 작을 수는 있습니다.
네트워크 분석 정책 수정	uint8[16]	연결 이벤트와 관련된 네트워크 분석 정책의 수정 버전입니다.

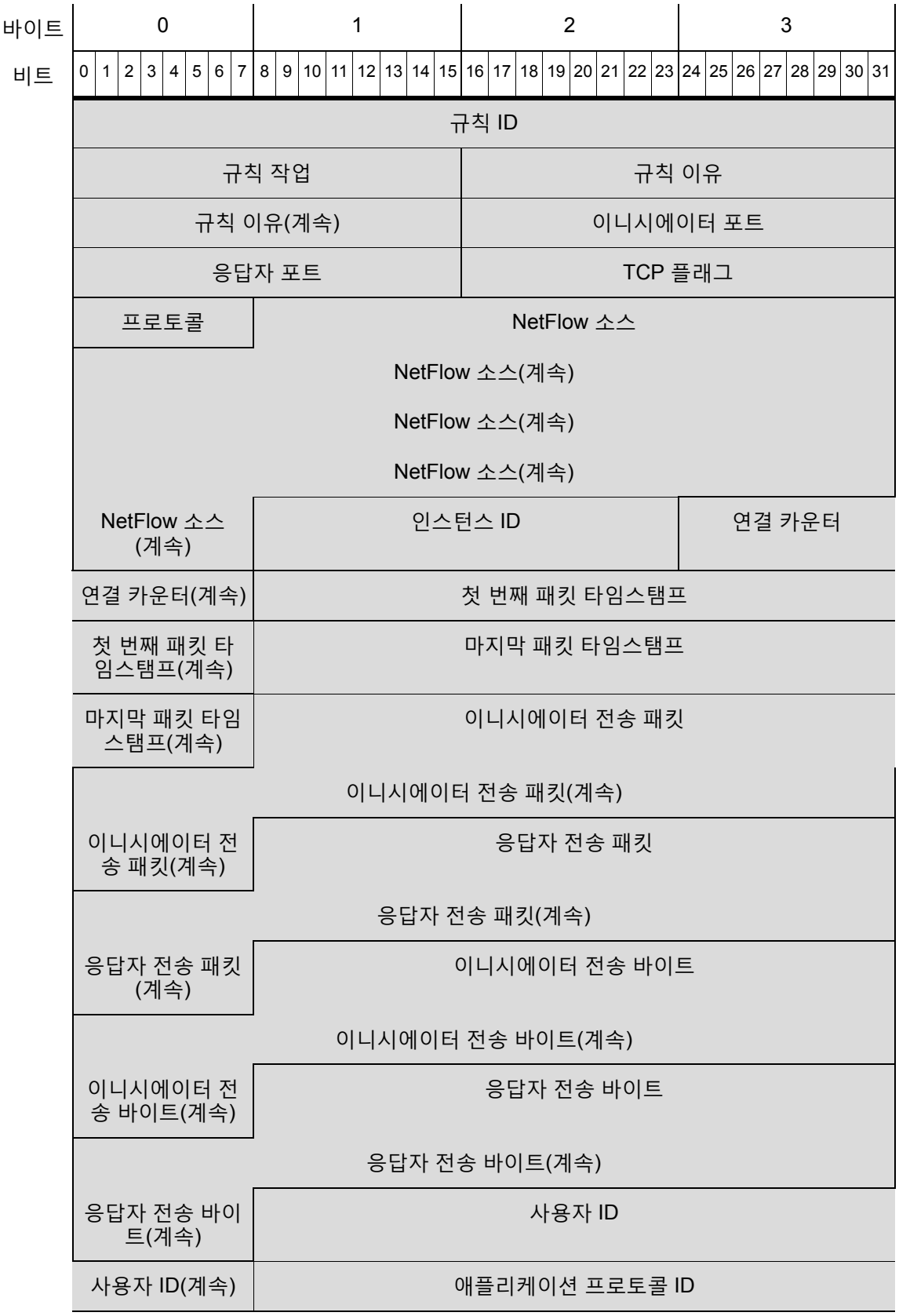
6.0.x 버전용 연결 통계 데이터 블록

연결 통계 데이터 블록은 연결 데이터 메시지에 사용됩니다. 6.0 버전용 연결 통계 데이터 블록에는 새 필드가 여러 개 추가되었습니다. ISE 통합 및 다중 네트워크 맵 지원을 위한 필드가 추가되었습니다. 계열 1 블록 그룹에서 6.0.x 버전용 연결 통계 데이터 블록의 블록 유형은 160입니다. 이는 블록 유형 157(5.4.1 버전용 연결 통계 데이터 블록, 페이지 B-181)을 대체합니다. DNS 조회 및 보안 인텔리전스를 지원하기 위해 새로운 필드가 추가되었습니다.

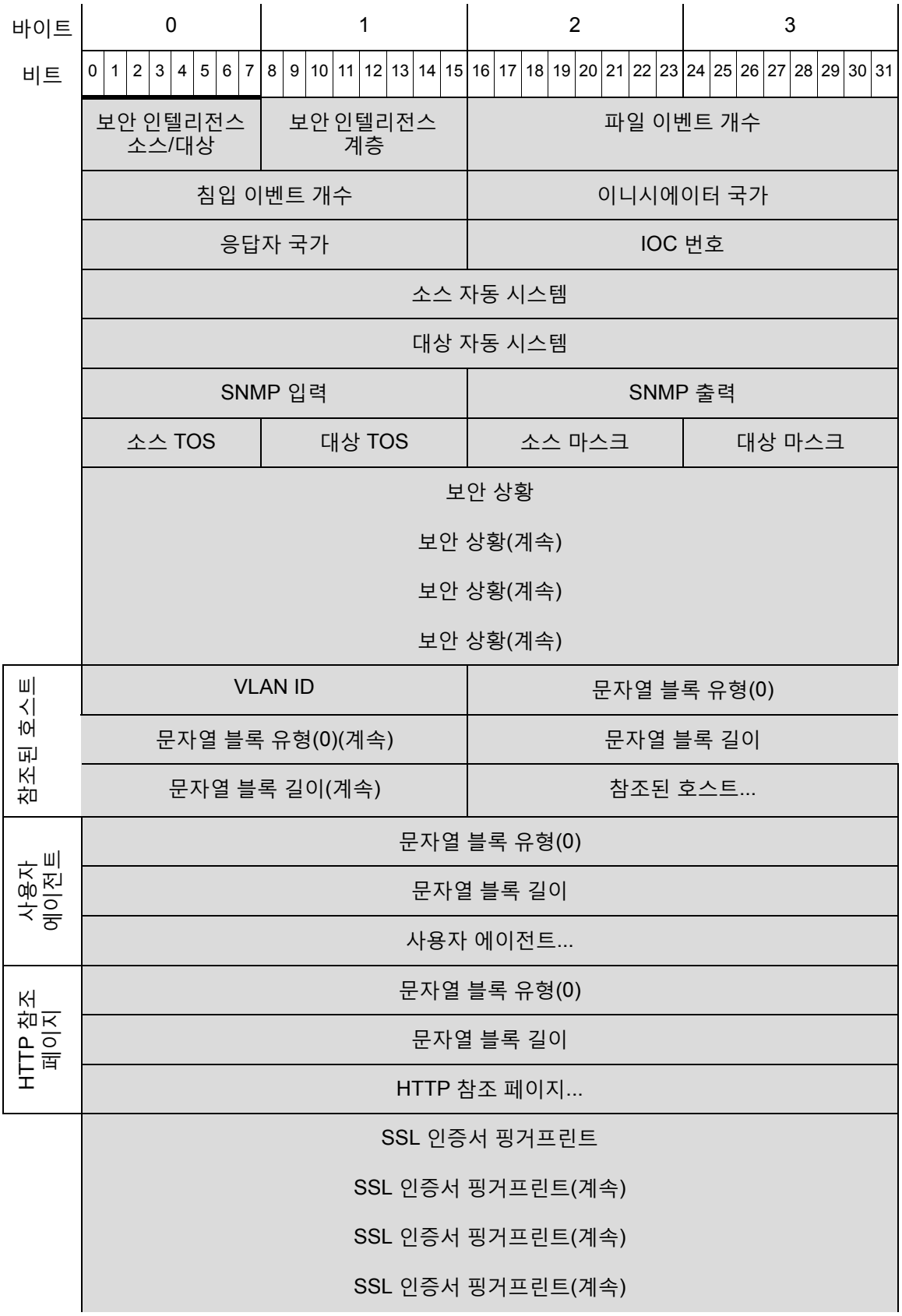
이벤트 버전이 13이고 이벤트 코드가 71인 요청 메시지에서 확장 이벤트 플래그(Request Flags(요청 플래그) 필드의 비트 30)를 설정하여 연결 이벤트 레코드를 요청합니다. 요청 플래그, 페이지 2-12의 내용을 참조하십시오. 비트 23을 활성화하면 레코드에 확장 이벤트 헤더가 포함됩니다.

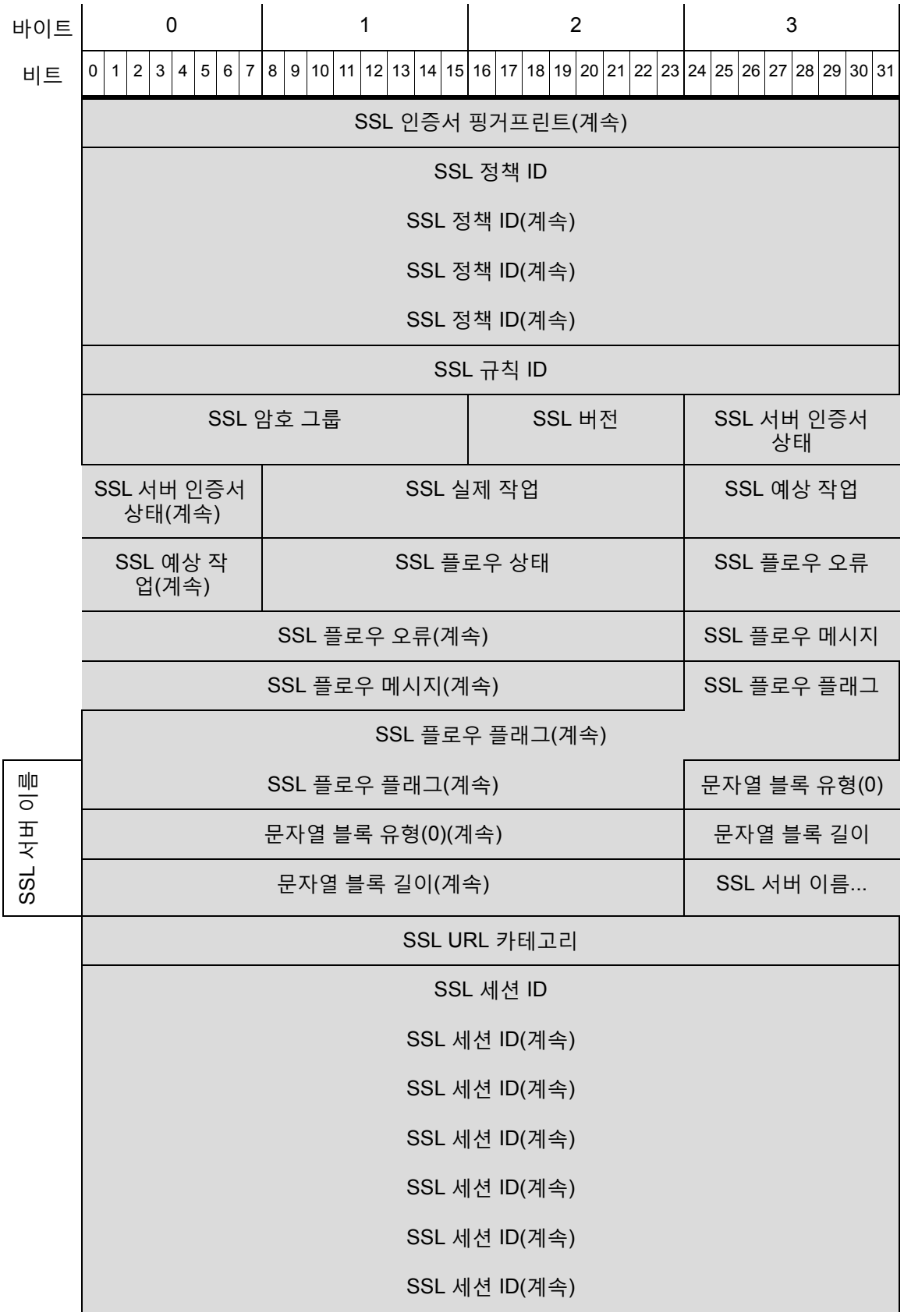
다음 다이어그램에 6.0.x 버전의 연결 통계 데이터 블록 형식이 나와 있습니다.

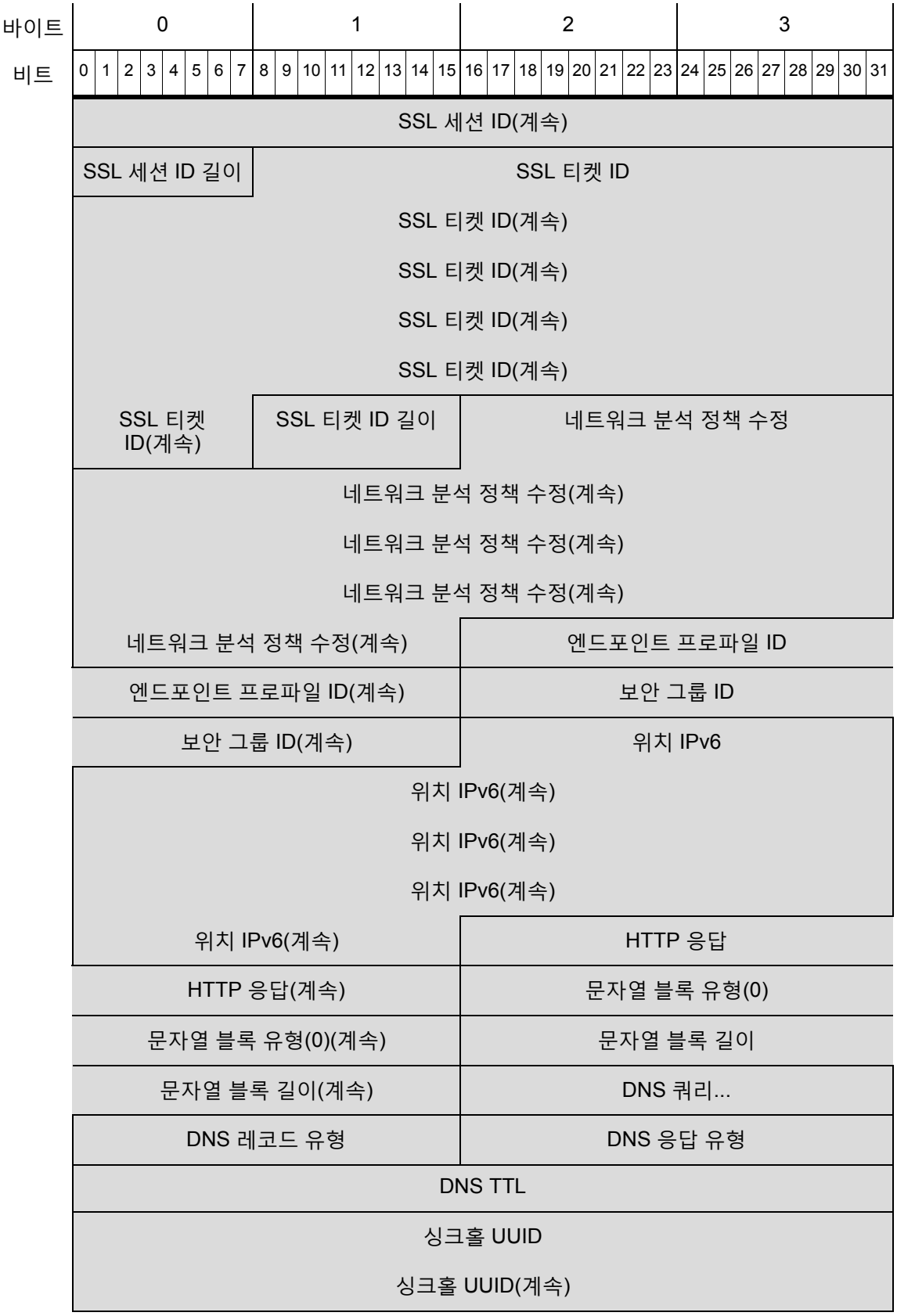
바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
이그레스(egress) 영역																																
이그레스(egress) 영역(계속)																																
이그레스(egress) 영역(계속)																																
이그레스(egress) 영역(계속)																																
인그레스 인터페이스																																
인그레스 인터페이스(계속)																																
인그레스 인터페이스(계속)																																
인그레스 인터페이스(계속)																																
이그레스(egress) 인터페이스																																
이그레스(egress) 인터페이스(계속)																																
이그레스(egress) 인터페이스(계속)																																
이그레스(egress) 인터페이스(계속)																																
이니시에이터 IP 주소																																
이니시에이터 IP 주소(계속)																																
이니시에이터 IP 주소(계속)																																
이니시에이터 IP 주소(계속)																																
응답자 IP 주소																																
응답자 IP 주소(계속)																																
응답자 IP 주소(계속)																																
응답자 IP 주소(계속)																																
정책 수정																																
정책 수정(계속)																																
정책 수정(계속)																																
정책 수정(계속)																																

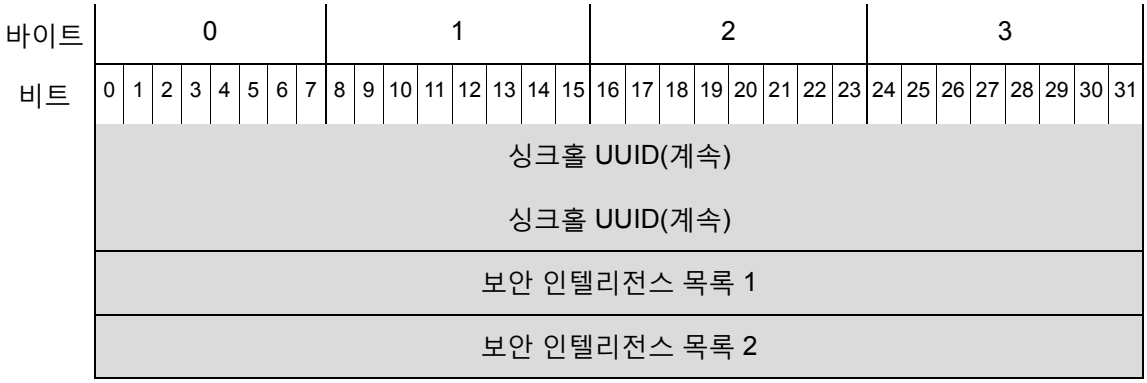

바이트
0
1
2
3
비트
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
규칙 ID
규칙 작업
규칙 이유
규칙 이유(계속)
이니시에이터 포트
응답자 포트
TCP 플래그
프로토콜
NetFlow 소스
NetFlow 소스(계속)
NetFlow 소스(계속)
NetFlow 소스(계속)
NetFlow 소스 (계속)
인스턴스 ID
연결 카운터
연결 카운터(계속)
첫 번째 패킷 타임스탬프
첫 번째 패킷 타임스탬프(계속)
마지막 패킷 타임스탬프
마지막 패킷 타임스탬프(계속)
이니시에이터 전송 패킷
이니시에이터 전송 패킷(계속)
이니시에이터 전송 패킷(계속)
응답자 전송 패킷
응답자 전송 패킷 (계속)
응답자 전송 패킷(계속)
이니시에이터 전송 바이트
이니시에이터 전송 바이트(계속)
이니시에이터 전송 바이트(계속)
응답자 전송 바이트
응답자 전송 바이트(계속)
사용자 ID
사용자 ID(계속)
애플리케이션 프로토콜 ID

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	애플리케이션 프로토콜 ID(계속)								URL 카테고리																							
	URL 카테고리(계속)								URL 평판																							
	URL 평판(계속)								클라이언트 애플리케이션 ID																							
	클라이언트 애플리케이션 ID(계속)								웹 애플리케이션 ID																							
클라이언트 URL	웹 애플리케이션 ID(계속)								문자열 블록 유형(0)																							
	문자열 블록 유형(계속)								문자열 블록 길이																							
	문자열 블록 길이(계속)								클라이언트 애플리케이션 URL...																							
NetBIOS 이름	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	NetBIOS 이름...																															
클라이언트 애플리케이션 버전	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	클라이언트 애플리케이션 버전...																															
	모니터링 규칙 1																															
	모니터링 규칙 2																															
	모니터링 규칙 3																															
	모니터링 규칙 4																															
	모니터링 규칙 5																															
	모니터링 규칙 6																															
	모니터링 규칙 7																															
	모니터링 규칙 8																															


바이트
0
1
2
3
비트
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
보안 인텔리전스 소스/대상
보안 인텔리전스 계층
파일 이벤트 개수
침입 이벤트 개수
이니시에이터 국가
응답자 국가
IOC 번호
소스 자동 시스템
대상 자동 시스템
SNMP 입력
SNMP 출력
소스 TOS
대상 TOS
소스 마스크
대상 마스크
보안 상황
보안 상황(계속)
보안 상황(계속)
보안 상황(계속)
참조된 호스트
VLAN ID
문자열 블록 유형(0)
문자열 블록 유형(0)(계속)
문자열 블록 길이
문자열 블록 길이(계속)
참조된 호스트...
사용자 에이전트
문자열 블록 유형(0)
문자열 블록 길이
사용자 에이전트...
HTTP 참조 페이지
문자열 블록 유형(0)
문자열 블록 길이
HTTP 참조 페이지...
SSL 인증서 핑거프린트
SSL 인증서 핑거프린트(계속)
SSL 인증서 핑거프린트(계속)
SSL 인증서 핑거프린트(계속)


바이트
0
1
2
3
비트
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
SSL 인증서 핑거프린트(계속)
SSL 정책 ID
SSL 정책 ID(계속)
SSL 정책 ID(계속)
SSL 정책 ID(계속)
SSL 규칙 ID
SSL 암호 그룹
SSL 버전
SSL 서버 인증서 상태
SSL 서버 인증서 상태(계속)
SSL 실제 작업
SSL 예상 작업
SSL 예상 작업(계속)
SSL 플로우 상태
SSL 플로우 오류
SSL 플로우 오류(계속)
SSL 플로우 메시지
SSL 플로우 메시지(계속)
SSL 플로우 플래그
SSL 플로우 플래그(계속)
SSL 플로우 플래그(계속)
문자열 블록 유형(0)
문자열 블록 유형(0)(계속)
문자열 블록 길이
문자열 블록 길이(계속)
SSL 서버 이름...
SSL 서버 이름
SSL URL 카테고리
SSL 세션 ID
SSL 세션 ID(계속)
SSL 세션 ID(계속)
SSL 세션 ID(계속)
SSL 세션 ID(계속)
SSL 세션 ID(계속)
SSL 세션 ID(계속)


바이트
0
1
2
3
비트
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
SSL 세션 ID(계속)
SSL 세션 ID 길이
SSL 티켓 ID
SSL 티켓 ID(계속)
SSL 티켓 ID(계속)
SSL 티켓 ID(계속)
SSL 티켓 ID(계속)
SSL 티켓 ID(계속)
SSL 티켓 ID 길이
네트워크 분석 정책 수정
네트워크 분석 정책 수정(계속)
네트워크 분석 정책 수정(계속)
네트워크 분석 정책 수정(계속)
네트워크 분석 정책 수정(계속)
엔드포인트 프로파일 ID
엔드포인트 프로파일 ID(계속)
보안 그룹 ID
보안 그룹 ID(계속)
위치 IPv6
위치 IPv6(계속)
위치 IPv6(계속)
위치 IPv6(계속)
위치 IPv6(계속)
HTTP 응답
HTTP 응답(계속)
문자열 블록 유형(0)
문자열 블록 유형(0)(계속)
문자열 블록 길이
문자열 블록 길이(계속)
DNS 쿼리...
DNS 레코드 유형
DNS 응답 유형
DNS TTL
싱크홀 UUID
싱크홀 UUID(계속)



다음 표에는 6.0.x 버전용 연결 통계 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 B-38 6.0.x 버전용 연결 통계 데이터 블록 필드

필드	데이터 유형	설명
연결 통계 데이터 블록 유형	uint32	6.0 이상 버전용 연결 통계 데이터 블록을 시작합니다. 값은 항상 160입니다.
연결 통계 데이터 블록 길이	uint32	연결 통계 데이터 블록의 바이트 수입니다. 여기에는 연결 통계 블록 유형 및 길이 필드의 8바이트에 그 뒤의 연결 데이터 바이트 수를 더한 값이 포함됩니다.
디바이스 ID	uint32	연결 이벤트를 탐지한 디바이스입니다.
인그레스 영역	uint8[16]	정책 위반을 트리거한 이벤트의 인그레스 보안 영역입니다.
이그레스(egress) 영역	uint8[16]	정책 위반을 트리거한 이벤트의 이그레스(egress) 보안 영역입니다.
인그레스 인터페이스	uint8[16]	인바운드 트래픽용 인터페이스입니다.
이그레스(egress) 인터페이스	uint8[16]	아웃바운드 트래픽용 인터페이스입니다.
이니시에이터 IP 주소	uint8[16]	연결 이벤트에서 설명하는 세션을 시작한 호스트의 IP 주소(IP 주소 옥텟 형식)입니다.
응답자 IP 주소	uint8[16]	시작 호스트에 응답한 호스트의 IP 주소(IP 주소 옥텟 형식)입니다.
정책 수정	uint8[16]	해당하는 경우 트리거된 상관관계와 관련된 규칙의 수정 번호입니다.
규칙 ID	uint32	해당하는 경우 이벤트를 트리거한 규칙의 내부 식별자입니다.
규칙 작업	uint16	해당 규칙(허용, 차단 등)에 대해 사용자 인터페이스에서 선택한 작업입니다.
규칙 이유	uint32	규칙이 이벤트를 트리거한 이유입니다.
이니시에이터 포트	uint16	시작 호스트에 사용되는 포트입니다.
응답자 포트	uint16	응답 호스트에 사용되는 포트입니다.
TCP 플래그	uint16	연결 이벤트에 대한 모든 TCP 플래그를 나타냅니다.
프로토콜	uint8	IANA에서 지정한 프로토콜 번호입니다.

표 B-38 6.0.x 버전용 연결 통계 데이터 블록 필드 (계속)

필드	데이터 유형	설명
NetFlow 소스	uint8[16]	연결에 대한 데이터를 내보낸 NetFlow 지원 디바이스의 IP 주소입니다.
인스턴스 ID	uint16	이벤트를 생성한 매니지드 디바이스의 Snort 인스턴스의 숫자 ID입니다.
연결 카운터	uint16	1초 이내에 발생하는 연결 이벤트를 구별하는 데 사용되는 값입니다.
첫 번째 패킷 타임스탬프	uint32	세션에서 첫 번째 패킷이 교환된 날짜의 시간의 UNIX 타임스탬프입니다.
마지막 패킷 타임스탬프	uint32	세션에서 마지막 패킷이 교환된 날짜의 시간의 UNIX 타임스탬프입니다.
이니시에이터 전송 패킷	uint64	시작 호스트에서 전송한 패킷 수입니다.
응답자 전송 패킷	uint64	응답 호스트에서 전송한 패킷 수입니다.
이니시에이터 전송 바이트	uint64	시작 호스트에서 전송한 바이트 수입니다.
응답자 전송 바이트	uint64	응답 호스트에서 전송한 바이트 수입니다.
사용자 ID	uint32	트래픽을 생성한 호스트에 마지막으로 로그인한 사용자의 내부 ID 번호입니다.
애플리케이션 프로토콜 ID	uint32	애플리케이션 프로토콜의 애플리케이션 ID입니다.
URL 카테고리	uint32	URL 카테고리의 내부 ID 번호입니다.
URL 평판	uint32	URL 평판의 내부 ID 번호입니다.
클라이언트 애플리케이션 ID	uint32	해당하는 경우 탐지된 클라이언트 애플리케이션의 내부 ID 번호입니다.
웹 애플리케이션 ID	uint32	해당하는 경우 탐지된 웹 애플리케이션의 내부 ID 번호입니다.
문자열 블록 유형	uint32	클라이언트 애플리케이션 URL에 대한 문자열 데이터 블록을 시작합니다. 이 값은 항상 `0`입니다.
문자열 블록 길이	uint32	클라이언트 애플리케이션 URL 문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이 필드의 8바이트에 클라이언트 애플리케이션 URL 문자열의 바이트 수를 더한 값이 포함됩니다.
클라이언트 애플리케이션 URL	string	해당하는 경우 클라이언트 애플리케이션이 액세스한 URL입니다. 예를 들면 `/files/index.html`과 같습니다.
문자열 블록 유형	uint32	호스트 NetBIOS 이름에 대한 문자열 데이터 블록을 시작합니다. 이 값은 항상 `0`입니다.
문자열 블록 길이	uint32	문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이 필드의 8바이트에 NetBIOS 이름 문자열의 바이트 수를 더한 값이 포함됩니다.
NetBIOS 이름	string	호스트 NetBIOS 이름 문자열입니다.

표 B-38 6.0.x 버전용 연결 통계 데이터 블록 필드 (계속)

필드	데이터 유형	설명
문자열 블록 유형	uint32	클라이언트 애플리케이션 버전에 대한 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	클라이언트 애플리케이션 버전에 대한 문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이의 8바이트에 버전의 바이트 수를 더한 값이 포함됩니다.
클라이언트 애플리케이션 버전	string	클라이언트 애플리케이션 버전입니다.
모니터링 규칙 1	uint32	연결 이벤트와 관련된 첫 번째 모니터 규칙의 ID입니다.
모니터링 규칙 2	uint32	연결 이벤트와 관련된 두 번째 모니터 규칙의 ID입니다.
모니터링 규칙 3	uint32	연결 이벤트와 관련된 세 번째 모니터 규칙의 ID입니다.
모니터링 규칙 4	uint32	연결 이벤트와 관련된 네 번째 모니터 규칙의 ID입니다.
모니터링 규칙 5	uint32	연결 이벤트와 관련된 다섯 번째 모니터 규칙의 ID입니다.
모니터링 규칙 6	uint32	연결 이벤트와 관련된 여섯 번째 모니터 규칙의 ID입니다.
모니터링 규칙 7	uint32	연결 이벤트와 관련된 일곱 번째 모니터 규칙의 ID입니다.
모니터링 규칙 8	uint32	연결 이벤트와 관련된 여덟 번째 모니터 규칙의 ID입니다.
보안 인텔리전스 소스/대상	uint8	소스 또는 대상 IP 주소가 IP 블랙리스트와 일치했는지를 나타냅니다.
보안 인텔리전스 계층	uint8	IP 블랙리스트와 일치한 IP 계층입니다.
파일 이벤트 개수	uint16	1초 이내에 발생하는 파일 이벤트를 구별하는 데 사용되는 값입니다.
침입 이벤트 개수	uint16	1초 이내에 발생하는 침입 이벤트를 구별하는 데 사용되는 값입니다.
이니시에이터 국가	uint16	시작 호스트의 국가 코드입니다.
응답자 국가	uint16	응답 호스트의 국가 코드입니다.
IOC 번호	uint16	이 이벤트와 관련된 보안 침해의 ID 번호입니다.
소스 자동 시스템	uint32	소스의 AS 번호(원본 또는 피어)입니다.
대상 자동 시스템	uint32	대상의 AS 번호(원본 또는 피어)입니다.
SNMP 입력	uint16	입력 인터페이스의 SNMP 인덱스입니다.
SNMP 출력	uint16	출력 인터페이스의 SNMP 인덱스입니다.
소스 TOS	uint8	들어오는 인터페이스에 대한 서비스 유형 바이트 설정입니다.
대상 TOS	uint8	나가는 인터페이스에 대한 서비스 유형 바이트 설정입니다.
소스 마스크	uint8	소스 주소 접두사 마스크입니다.
대상 마스크	uint8	대상 주소 접두사 마스크입니다.
보안 상황	uint8(16)	트래픽이 통과한 보안 상황(가상 방화벽)의 ID 번호입니다. 이 필드는 다중 컨텍스트 모드의 ASA FirePOWER 디바이스에 대해서만 채워집니다.

표 B-38 6.0.x 버전용 연결 통계 데이터 블록 필드 (계속)

필드	데이터 유형	설명
VLAN ID	uint16	호스트가 구성원으로 포함된 VLAN을 나타내는 VLAN ID 번호입니다.
문자열 블록 유형	uint32	참조된 호스트 이름을 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	참조된 호스트 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Referenced Host(참조된 호스트) 필드의 바이트 수를 더한 값이 포함됩니다.
참조된 호스트	string	HTTP 또는 DNS로 제공되는 호스트 이름 정보입니다.
문자열 블록 유형	uint32	사용자 에이전트를 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	사용자 에이전트 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 User Agent(사용자 에이전트) 필드의 바이트 수를 더한 값이 포함됩니다.
사용자 에이전트	string	세션에서 UserAgent 헤더 필드의 정보입니다.
문자열 블록 유형	uint32	HTTP 참조 페이지를 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	HTTP 참조 페이지 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 HTTP Referer(HTTP 참조 페이지) 필드의 바이트 수를 더한 값이 포함됩니다.
HTTP 참조 페이지	string	페이지가 생성된 사이트입니다. HTTP 트래픽의 참조 페이지 헤더 정보에서 찾을 수 있습니다.
SSL 인증서 핑거프린트	uint8[20]	SSL 서버 인증서의 SHA1 해시입니다.
SSL 정책 ID	uint8[16]	연결을 처리한 SSL 정책의 ID 번호입니다.
SSL 규칙 ID	uint32	연결을 처리한 SSL 규칙 또는 기본 동작의 ID 번호입니다.
SSL 암호 그룹	uint16	SSL 연결에서 사용되는 암호화 그룹입니다. 값은 10진수 형식으로 저장됩니다. 값으로 지정되는 암호 그룹은 `www.iana.org/assignments/tls-parameters/tls-parameters.xhtml`을 참조하십시오.
SSL 버전	uint8	연결을 암호화하는 데 사용된 SSL 또는 TLS 프로토콜 버전입니다.

표 B-38 6.0.x 버전용 연결 통계 데이터 블록 필드 (계속)

필드	데이터 유형	설명
SSL 서버 인증서 상태	uint16	SSL 인증서의 상태입니다. 가능한 값은 다음과 같습니다. • 0 - 확인되지 않음 - 서버 인증서 상태를 평가하지 않았습니다. • 1 - 알 수 없음 - 서버 인증서 상태를 확인할 수 없습니다. • 2 - 유효 - 서버 인증서가 유효합니다. • 4 - 자체 서명 - 서버 인증서가 자체 서명되었습니다. • 16 - 유효하지 않은 발급자 - 서버 인증서의 발급자가 유효하지 않습니다. • 32 - 유효하지 않은 서명 - 서버 인증서의 서명이 유효하지 않습니다. • 64 - 만료됨 - 서버 인증서가 만료되었습니다. • 128 - 아직 유효하지 않음 - 서버 인증서가 아직 유효하지 않습니다. • 256 - 해지됨 - 서버 인증서가 해지되었습니다.
SSL 실제 작업	uint16	SSL 규칙에 기반한 연결에서 수행된 작업입니다. 규칙에 명시된 작업이 가능하지 않을 수도 있으므로, 이는 예상 작업과 다를 수 있습니다. 가능한 값은 다음과 같습니다. • 0 - '알 수 없음' • 1 - '암호 해독 안 함' • 2 - '차단' • 3 - '차단 및 재설정' • 4 - '암호 해독(알려진 키)' • 5 - '암호 해독(키 교체)' • 6 - '암호 해독(재서명)'
SSL 예상 작업	uint16	SSL 규칙에 기반한 연결에서 수행해야 하는 작업입니다. 가능한 값은 다음과 같습니다. • 0 - '알 수 없음' • 1 - '암호 해독 안 함' • 2 - '차단' • 3 - '차단 및 재설정' • 4 - '암호 해독(알려진 키)' • 5 - '암호 해독(키 교체)' • 6 - '암호 해독(재서명)'

표 B-38 6.0.x 버전용 연결 통계 데이터 블록 필드 (계속)

필드	데이터 유형	설명
SSL 플로우 상태	uint16	SSL 플로우의 상태입니다. 이 값은 작업을 수행한 이유 또는 오류 메시지가 표시된 이유를 설명합니다. 가능한 값은 다음과 같습니다. • 0 - '알 수 없음' • 1 - '일치하지 않음' • 2 - '성공' • 3 - '캐시되지 않은 세션' • 4 - '알 수 없는 암호 그룹' • 5 - '지원되지 않는 암호 그룹' • 6 - '지원되지 않는 SSL 버전' • 7 - 'SSL 압축 사용됨' • 8 - '패시브 모드에서 세션 암호 해독 불가' • 9 - '핸드셰이크 오류' • 10 - '암호 해독 오류' • 11 - '서버 이름 카테고리 조회 보류 중' • 12 - '공용 이름 카테고리 조회 보류 중' • 13 - '내부 오류' • 14 - '네트워크 파라미터 사용 불가' • 15 - '유효하지 않은 서버 인증서 핸들' • 16 - '서버 인증서 핑거프린트 사용 불가' • 17 - '주체 DN을 캐시할 수 없음' • 18 - '발급자 DN을 캐시할 수 없음' • 19 - '알 수 없는 SSL 버전' • 20 - '외부 인증서 목록 사용 불가' • 21 - '외부 인증서 핑거프린트 사용 불가' • 22 - '내부 인증서 목록이 유효하지 않음' • 23 - '내부 인증서 목록 사용 불가' • 24 - '내부 인증서 사용 불가' • 25 - '내부 인증서 핑거프린트 사용 불가' • 26 - '서버 인증서 검증 사용 불가' • 27 - '서버 인증서 검증 장애' • 28 - '유효하지 않은 작업'
SSL 플로우 오류	uint32	자세한 SSL 오류 코드입니다. 이러한 값은 지원용으로 필요할 수 있습니다.

표 B-38 6.0.x 버전용 연결 통계 데이터 블록 필드 (계속)

필드	데이터 유형	설명
SSL 플로우 메시지	uint32	SSL 핸드셰이크 도중 클라이언트와 서버 간에 교환된 메시지입니다. 자세한 내용은 http://tools.ietf.org/html/rfc5246을 참조하십시오. • 0x00000001 — NSE_MT__HELLO_REQUEST • 0x00000002 — NSE_MT__CLIENT_ALERT • 0x00000004 — NSE_MT__SERVER_ALERT • 0x00000008 — NSE_MT__CLIENT_HELLO • 0x00000010 — NSE_MT__SERVER_HELLO • 0x00000020 — NSE_MT__SERVER_CERTIFICATE • 0x00000040 — NSE_MT__SERVER_KEY_EXCHANGE • 0x00000080 — NSE_MT__CERTIFICATE_REQUEST • 0x00000100 — NSE_MT__SERVER_HELLO_DONE • 0x00000200 — NSE_MT__CLIENT_CERTIFICATE • 0x00000400 — NSE_MT__CLIENT_KEY_EXCHANGE • 0x00000800 — NSE_MT__CERTIFICATE_VERIFY • 0x00001000 — NSE_MT__CLIENT_CHANGE_CIPHER_SPEC • 0x00002000 — NSE_MT__CLIENT_FINISHED • 0x00004000 — NSE_MT__SERVER_CHANGE_CIPHER_SPEC • 0x00008000 — NSE_MT__SERVER_FINISHED • 0x00010000 — NSE_MT__NEW_SESSION_TICKET • 0x00020000 — NSE_MT__HANDSHAKE_OTHER • 0x00040000 — NSE_MT__APP_DATA_FROM_CLIENT • 0x00080000 — NSE_MT__APP_DATA_FROM_SERVER
SSL 플로우 플래그	uint64	암호화된 연결에 대한 디버깅 레벨 플래그입니다. 가능한 값은 다음과 같습니다. • 0x00000001 - NSE_FLOW__VALID - 다른 필드를 유효하게 만들려면 설정해야 함 • 0x00000002 - NSE_FLOW__INITIALIZED - 처리 준비가 완료된 내부 구조 • 0x00000004 - NSE_FLOW__INTERCEPT - SSL 세션이 중단됨
문자열 블록 유형	uint32	SSL 서버 이름을 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	SSL 서버 이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 SSL Server Name(SSL 서버 이름) 필드의 바이트 수를 더한 값이 포함됩니다.

표 B-38 6.0.x 버전용 연결 통계 데이터 블록 필드 (계속)

필드	데이터 유형	설명
SSL 서버 이름	string	SSL Client Hello의 서버 이름 표시에서 제공된 이름입니다.
SSL URL 카테고리	uint32	서버 이름 및 인증서 일반 이름에서 확인된 플로우의 카테고리입니다.
SSL 세션 ID	uint8[32]	클라이언트와 서버가 세션 재사용에 동의하는 경우 SSL 핸드셰이크 중에 사용되는 세션 ID의 값입니다.
SSL 세션 ID 길이	uint8	SSL 세션 ID의 길이입니다. 세션 ID는 32바이트를 초과할 수는 없으며 32바이트보다 작을 수는 있습니다.
SSL 티켓 ID	uint8[20]	클라이언트와 서버가 세션 티켓 사용에 동의하는 경우 사용되는 세션 티켓의 해시입니다.
SSL 티켓 ID 길이	uint8	SSL 티켓 ID의 길이입니다. 티켓 ID는 20바이트를 초과할 수는 없으며 20바이트보다 작을 수는 있습니다.
네트워크 분석 정책 수정	uint8[16]	연결 이벤트와 관련된 네트워크 분석 정책의 수정 버전입니다.
엔드포인트 프로파일 ID	uint32	ISE가 식별한 연결 엔드포인트에서 사용하는 디바이스 유형의 ID 번호입니다. 각 DC에 대해 고유하며 메타데이터에서 확인 가능합니다.
보안 그룹 ID	uint32	정책을 기준으로 ISE가 사용자에게 할당하는 ID 번호입니다.
위치 IPv6	uint8[16]	ISE와 통신하는 인터페이스의 IP 주소입니다. IPv4 또는 IPv6일 수 있습니다.
HTTP 응답	uint32	HTTP 요청의 응답 코드입니다.
문자열 블록 유형	uint32	DNS 쿼리에 대한 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이 필드의 8바이트에 DNS 쿼리 문자열의 바이트 수를 더한 값이 포함됩니다.
DNS 쿼리	string	DNS 서버에 전송되는 쿼리의 콘텐츠입니다.
DNS 레코드 유형	uint16	DNS 레코드 유형에 해당하는 숫자 값입니다.

표 B-38 6.0.x 버전용 연결 통계 데이터 블록 필드 (계속)

필드	데이터 유형	설명
DNS 응답 유형	uint16	0 - NoError - 오류 없음 1 - FormErr - 형식 오류 2 - ServFail - 서버 장애 3 - NXDomain - 없는 도메인 4 - NotImp - 구현되지 않음 5 - Refused - 쿼리가 거부됨 6 - YXDomain - 이름이 없어야 하는데 있음 7 - YXRRSet - RR 설정이 없어야 하는데 있음 8 - NXRRSet - RR 설정이 있어야 하는데 없음 9 - NotAuth - 인증되지 않음 10 - NotZone - 이름이 영역에 포함되어 있지 않음 16 - BADSIG - TSIG 서명 장애 17 - BADKEY - 키가 인식되지 않음 18 - BADTIME - 서명이 기간을 벗어남 19 - BADMODE - 잘못된 TKEY 모드 20 - BADNAME - 중복 키 이름 21 - BADALG - 알고리즘이 지원되지 않음 22 - BADTRUNC - 잘못된 자르기 3841 - NXDOMAIN - 방화벽의 NXDOMAIN 응답 3842 - SINKHOLE - 방화벽의 싱크홀 응답
DNS TTL	uint32	DNS 응답의 초 단위 TTL(Time to Live)입니다.
싱크홀 UUID	uin8[16]	싱크홀 개체와 관련된 수정 UUID입니다.
보안 인텔리전스 목록 1	uint32	이벤트와 관련된 보안 인텔리전스 목록으로, 관련된 메타데이터의 보안 인텔리전스 목록에 매핑됩니다. 2개의 보안 인텔리전스 목록이 연결과 관련되어 있을 수 있습니다.
보안 인텔리전스 목록 2	uint32	이벤트와 관련된 보안 인텔리전스 목록으로, 관련된 메타데이터의 보안 인텔리전스 목록에 매핑됩니다. 2개의 보안 인텔리전스 목록이 연결과 관련되어 있을 수 있습니다.

6.1.x 버전용 연결 통계 데이터 블록

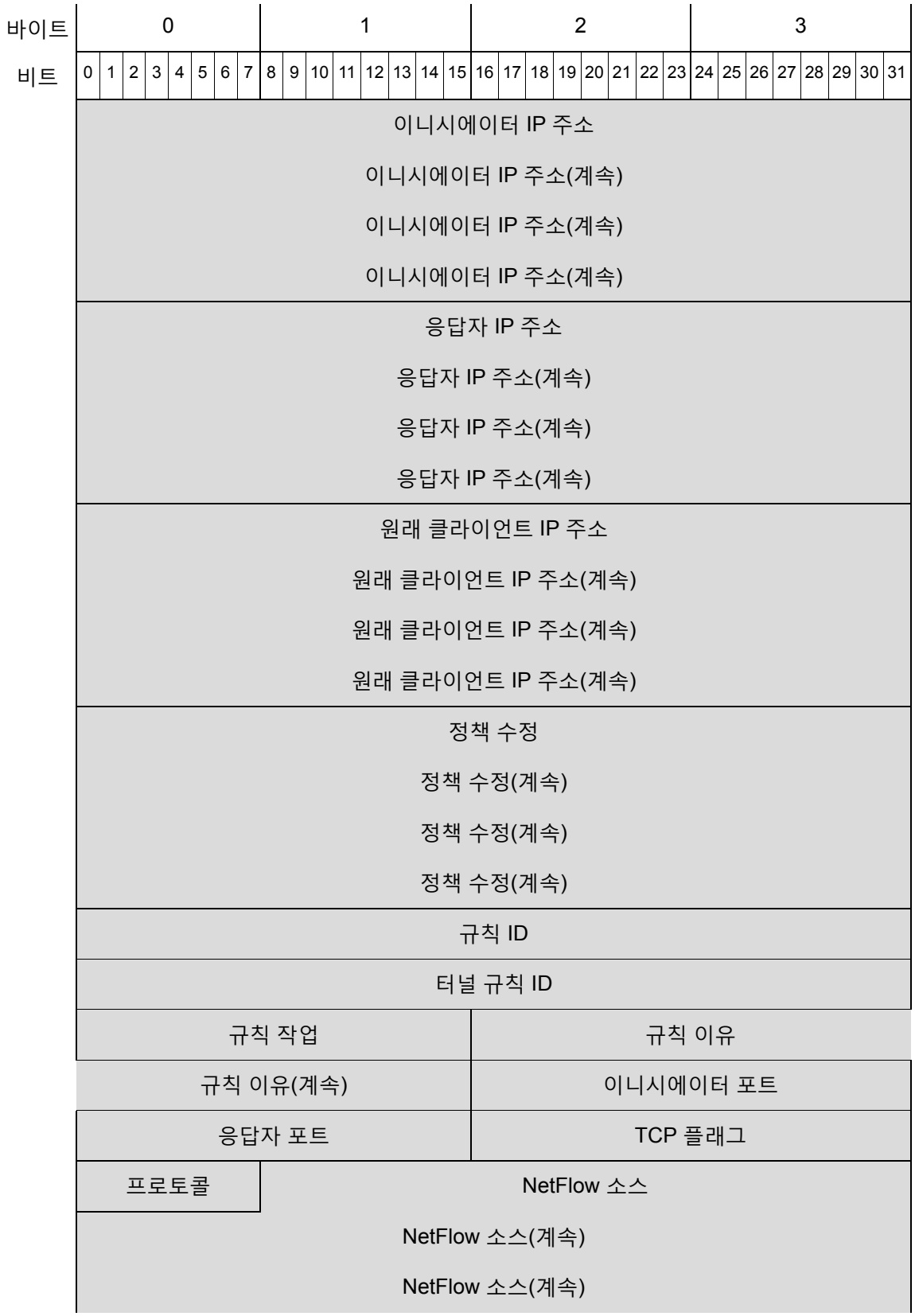
연결 통계 데이터 블록은 연결 데이터 메시지에 사용됩니다. 6.1.x 버전용 연결 통계 데이터 블록에는 새 필드가 여러 개 추가되었습니다. ISE 통합 및 다중 네트워크 맵 지원을 위한 필드가 추가되었습니다. 계열 1 블록 그룹에서 6.1 이상 버전용 연결 통계 데이터 블록의 블록 유형은 163입니다. 이는 블록 유형 160(6.0.x 버전용 연결 통계 데이터 블록, 페이지 B-194)을 대체합니다. DNS 조회 및 보안 인텔리전스를 지원하기 위해 새로운 필드가 추가되었습니다. 이는 블록 유형 168(6.2 이상 버전용 연결 통계 데이터 블록, 페이지 4-120)로 대체됩니다.

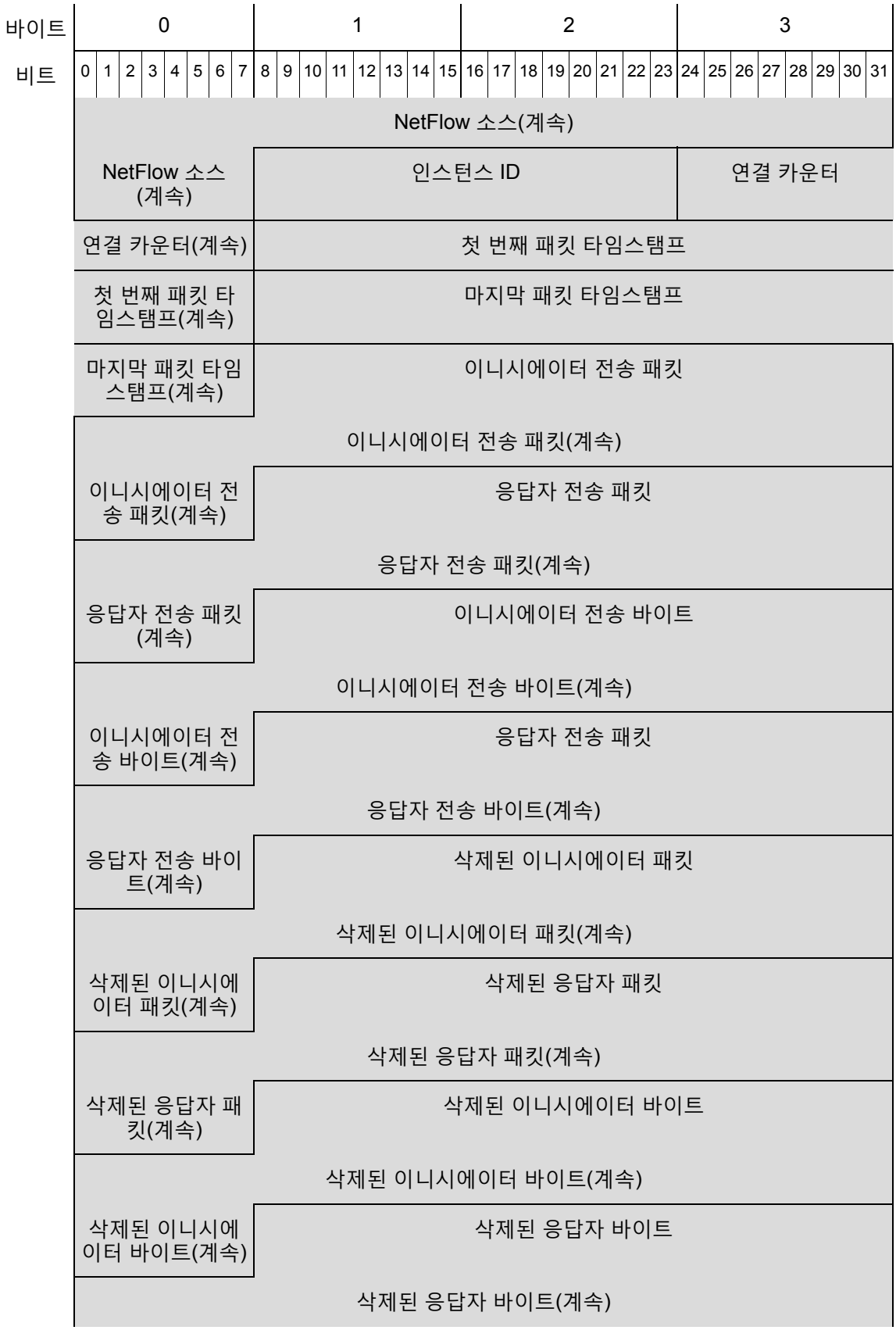
이벤트 버전이 13이고 이벤트 코드가 71인 요청 메시지에서 확장 이벤트 플래그(Request Flags(요청 플래그) 필드의 비트 30)를 설정하여 연결 이벤트 레코드를 요청합니다. 요청 플래그, 페이지 2-12의 내용을 참조하십시오. 비트 23을 활성화하면 레코드에 확장 이벤트 헤더가 포함됩니다.

연결 통계 데이터 메시지에 대한 자세한 정보는 연결 통계 데이터 메시지, 페이지 4-54의 내용을 참조하십시오.

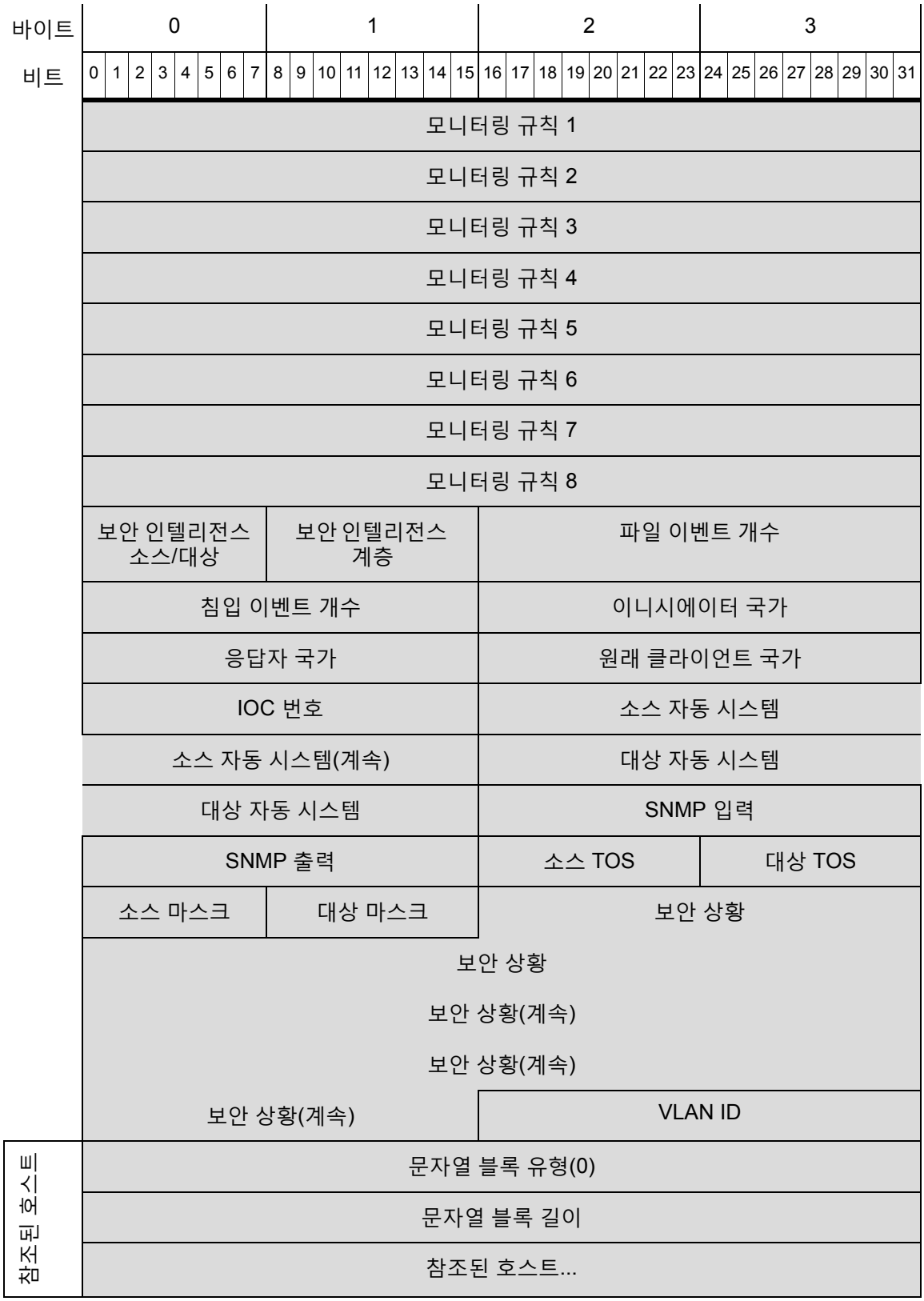
다음 다이어그램에 6.1 이상 버전의 연결 통계 데이터 블록 형식이 나와 있습니다.

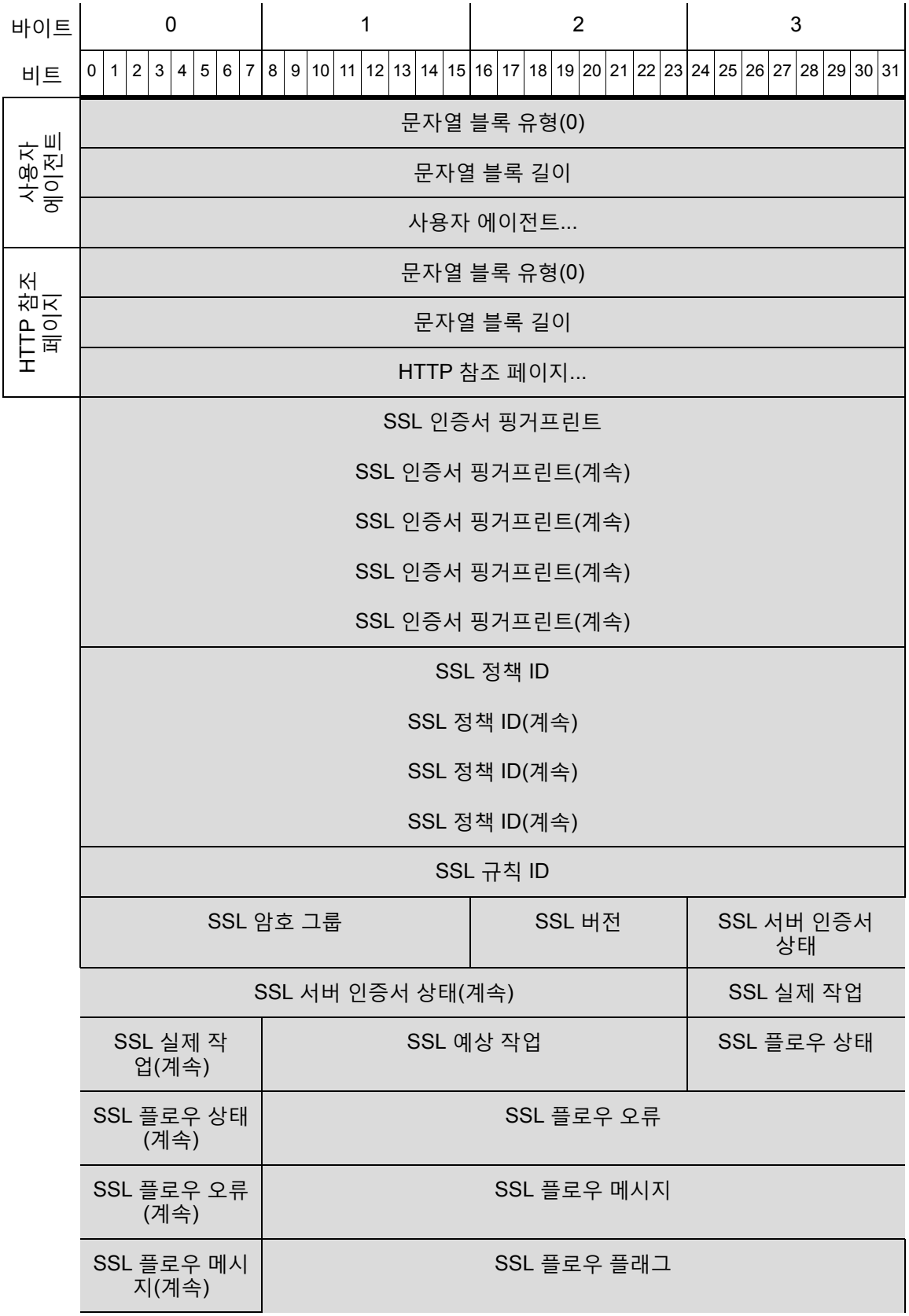
바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
연결 통계 데이터 블록 유형(163)																																
연결 통계 데이터 블록 길이																																
디바이스 ID																																
인그레스 영역 인그레스 영역(계속) 인그레스 영역(계속) 인그레스 영역(계속)																																
이그레스(egress) 영역 이그레스(egress) 영역(계속) 이그레스(egress) 영역(계속) 이그레스(egress) 영역(계속)																																
인그레스 인터페이스 인그레스 인터페이스(계속) 인그레스 인터페이스(계속) 인그레스 인터페이스(계속)																																
이그레스(egress) 인터페이스 이그레스(egress) 인터페이스(계속) 이그레스(egress) 인터페이스(계속) 이그레스(egress) 인터페이스(계속)																																

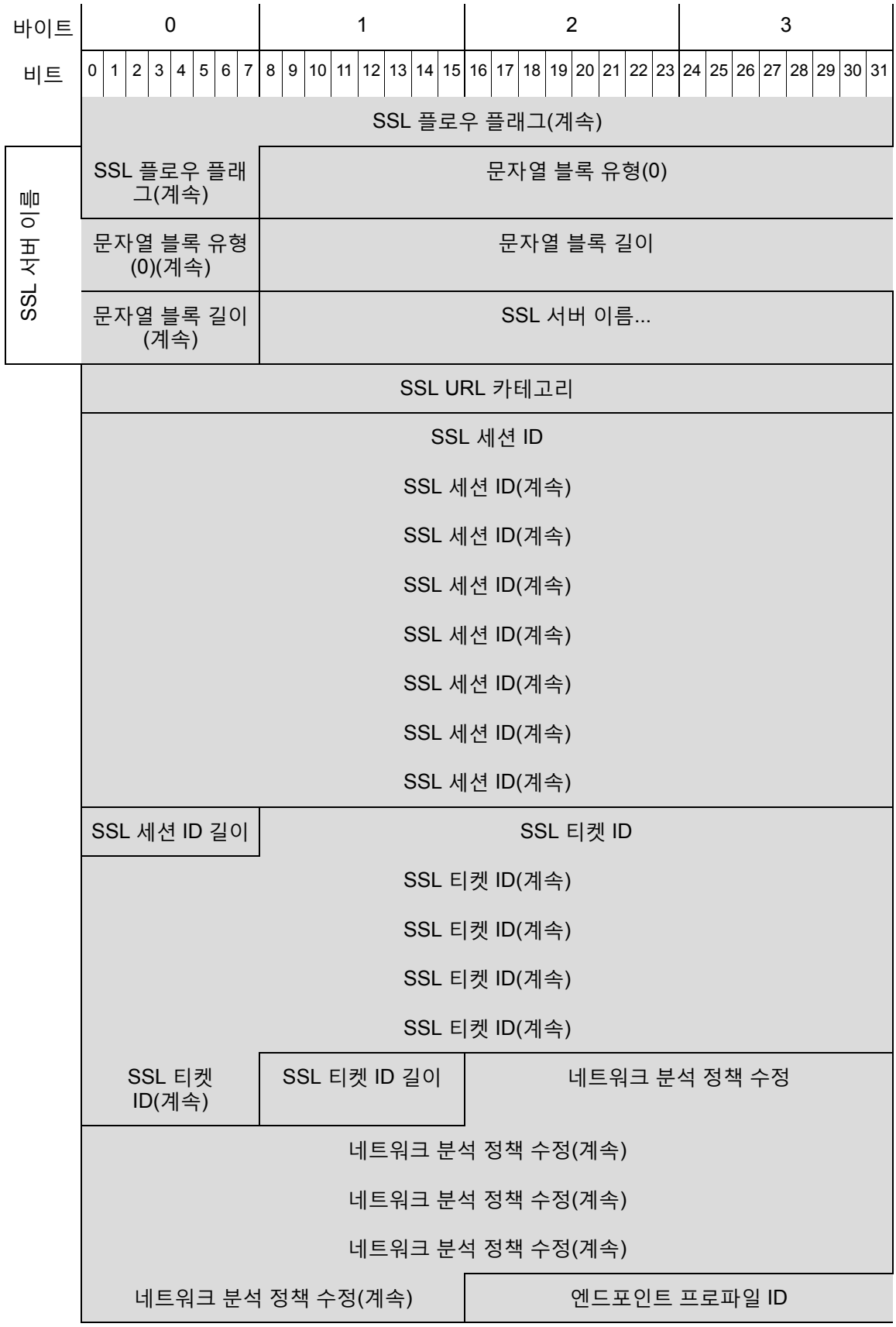

바이트
0
1
2
3
비트
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
이니시에이터 IP 주소
이니시에이터 IP 주소(계속)
이니시에이터 IP 주소(계속)
이니시에이터 IP 주소(계속)
응답자 IP 주소
응답자 IP 주소(계속)
응답자 IP 주소(계속)
응답자 IP 주소(계속)
원래 클라이언트 IP 주소
원래 클라이언트 IP 주소(계속)
원래 클라이언트 IP 주소(계속)
원래 클라이언트 IP 주소(계속)
정책 수정
정책 수정(계속)
정책 수정(계속)
정책 수정(계속)
규칙 ID
터널 규칙 ID
규칙 작업
규칙 이유
규칙 이유(계속)
이니시에이터 포트
응답자 포트
TCP 플래그
프로토콜
NetFlow 소스
NetFlow 소스(계속)
NetFlow 소스(계속)

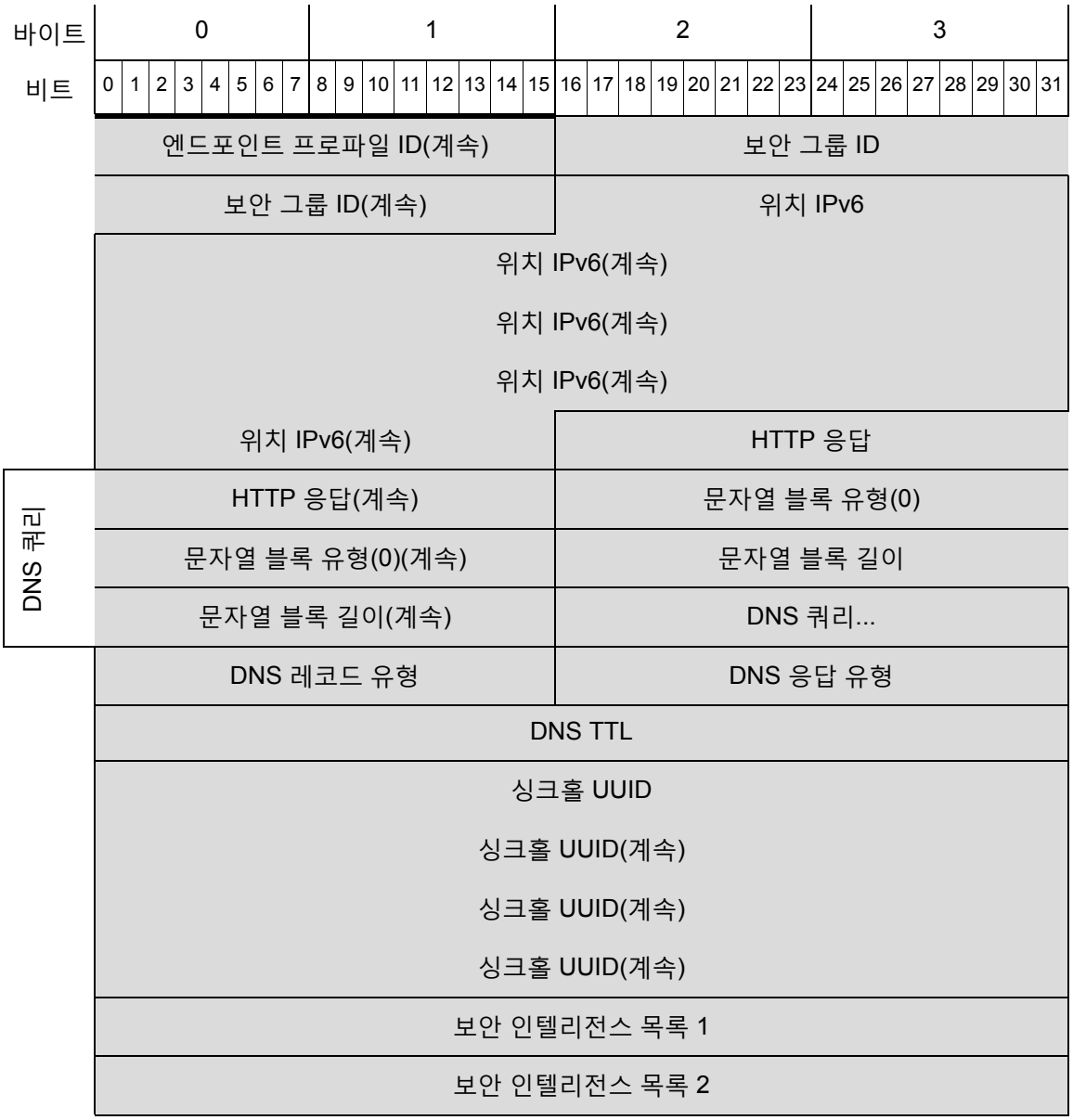

바이트
0
1
2
3
비트
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
NetFlow 소스(계속)
NetFlow 소스 (계속)
인스턴스 ID
연결 카운터
연결 카운터(계속)
첫 번째 패킷 타임스탬프
첫 번째 패킷 타임스탬프(계속)
마지막 패킷 타임스탬프
마지막 패킷 타임스탬프(계속)
이니시에이터 전송 패킷
이니시에이터 전송 패킷(계속)
응답자 전송 패킷
응답자 전송 패킷(계속)
이니시에이터 전송 바이트
이니시에이터 전송 바이트(계속)
응답자 전송 패킷
응답자 전송 바이트(계속)
삭제된 이니시에이터 패킷
삭제된 이니시에이터 패킷(계속)
삭제된 응답자 패킷
삭제된 응답자 패킷(계속)
삭제된 이니시에이터 바이트
삭제된 이니시에이터 바이트(계속)
삭제된 응답자 바이트
삭제된 응답자 바이트(계속)

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	삭제된 응답자 바이트(계속)								QOS 적용 인터페이스																							
	QOS 적용 인터페이스(계속)																															
	QOS 적용 인터페이스(계속)																															
	QOS 적용 인터페이스(계속)																															
	QoS 인터페이스(계속)								QOS 규칙 ID																							
	QOS 규칙 ID(계속)								사용자 ID																							
	사용자 ID(계속)								애플리케이션 프로토콜 ID																							
	애플리케이션 프로토콜 ID(계속)								URL 카테고리																							
	URL 카테고리(계속)								URL 평판																							
	URL 평판(계속)								클라이언트 애플리케이션 ID																							
	클라이언트 애플리케이션 ID(계속)								웹 애플리케이션 ID																							
클라이언트 URL	웹 애플리케이션 ID(계속)								문자열 블록 유형(0)																							
	문자열 블록 유형(계속)								문자열 블록 길이																							
	문자열 블록 길이(계속)								클라이언트 애플리케이션 URL...																							
NetBIOS 이름	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	NetBIOS 이름...																															
클라이언트 애플리케이션 버전	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	클라이언트 애플리케이션 버전...																															


바이트
0
1
2
3
비트
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
모니터링 규칙 1
모니터링 규칙 2
모니터링 규칙 3
모니터링 규칙 4
모니터링 규칙 5
모니터링 규칙 6
모니터링 규칙 7
모니터링 규칙 8
보안 인텔리전스 소스/대상
보안 인텔리전스 계층
파일 이벤트 개수
침입 이벤트 개수
이니시에이터 국가
응답자 국가
원래 클라이언트 국가
IOC 번호
소스 자동 시스템
소스 자동 시스템(계속)
대상 자동 시스템
대상 자동 시스템
SNMP 입력
SNMP 출력
소스 TOS
대상 TOS
소스 마스크
대상 마스크
보안 상황
보안 상황
보안 상황(계속)
보안 상황(계속)
보안 상황(계속)
VLAN ID
참조된 호스트
문자열 블록 유형(0)
문자열 블록 길이
참조된 호스트...


바이트
0
1
2
3
비트
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
사용자 에이전트
문자열 블록 유형(0)
문자열 블록 길이
사용자 에이전트...
HTTP 참조 페이지
문자열 블록 유형(0)
문자열 블록 길이
HTTP 참조 페이지...
SSL 인증서 핑거프린트
SSL 인증서 핑거프린트(계속)
SSL 인증서 핑거프린트(계속)
SSL 인증서 핑거프린트(계속)
SSL 인증서 핑거프린트(계속)
SSL 정책 ID
SSL 정책 ID(계속)
SSL 정책 ID(계속)
SSL 정책 ID(계속)
SSL 규칙 ID
SSL 암호 그룹
SSL 버전
SSL 서버 인증서 상태
SSL 서버 인증서 상태(계속)
SSL 실제 작업
SSL 실제 작업(계속)
SSL 예상 작업
SSL 플로우 상태
SSL 플로우 상태(계속)
SSL 플로우 오류
SSL 플로우 오류(계속)
SSL 플로우 메시지
SSL 플로우 메시지(계속)
SSL 플로우 플래그


바이트
0
1
2
3
비트
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
SSL 플로우 플래그(계속)
SSL 서버 블록
SSL 플로우 플래그(계속)
문자열 블록 유형(0)
문자열 블록 유형(0)(계속)
문자열 블록 길이
문자열 블록 길이(계속)
SSL 서버 이름...
SSL URL 카테고리
SSL 세션 ID
SSL 세션 ID(계속)
SSL 세션 ID(계속)
SSL 세션 ID(계속)
SSL 세션 ID(계속)
SSL 세션 ID(계속)
SSL 세션 ID(계속)
SSL 세션 ID(계속)
SSL 세션 ID 길이
SSL 티켓 ID
SSL 티켓 ID(계속)
SSL 티켓 ID(계속)
SSL 티켓 ID(계속)
SSL 티켓 ID(계속)
SSL 티켓 ID(계속)
SSL 티켓 ID 길이
네트워크 분석 정책 수정
네트워크 분석 정책 수정(계속)
네트워크 분석 정책 수정(계속)
네트워크 분석 정책 수정(계속)
네트워크 분석 정책 수정(계속)
엔드포인트 프로파일 ID



다음 표에는 6.1 이상 버전용 연결 통계 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 B-39 6.1 이상 버전용 연결 통계 데이터 블록 필드

필드	데이터 유형	설명
연결 통계 데이터 블록 유형	uint32	6.1.x 버전용 연결 통계 데이터 블록을 시작합니다. 값은 항상 163입니다.
연결 통계 데이터 블록 길이	uint32	연결 통계 데이터 블록의 바이트 수입니다. 여기에는 연결 통계 블록 유형 및 길이 필드의 8바이트에 그 뒤의 연결 데이터 바이트 수를 더한 값이 포함됩니다.
디바이스 ID	uint32	연결 이벤트를 탐지한 디바이스입니다.

표 B-39 6.1 이상 버전용 연결 통계 데이터 블록 필드 (계속)

필드	데이터 유형	설명
인그레스 영역	uint8[16]	정책 위반을 트리거한 이벤트의 인그레스 보안 영역입니다.
이그레스 (egress) 영역	uint8[16]	정책 위반을 트리거한 이벤트의 이그레스(egress) 보안 영역입니다.
인그레스 인터페이스	uint8[16]	인바운드 트래픽용 인터페이스입니다.
이그레스 (egress) 인터페이스	uint8[16]	아웃바운드 트래픽용 인터페이스입니다.
이니시에이터 IP 주소	uint8[16]	연결 이벤트에서 설명하는 세션을 시작한 호스트의 IP 주소(IP 주소 옥텟 형식)입니다.
응답자 IP 주소	uint8[16]	시작 호스트에 응답한 호스트의 IP 주소(IP 주소 옥텟 형식)입니다.
원래 클라이언트 IP 주소	uint8[16]	요청이 생성된 프록시를 사용하는 호스트의 IP 주소(IP 주소 옥텟 형식)입니다.
정책 수정	uint8[16]	해당하는 경우 트리거된 상관관계와 관련된 규칙의 수정 번호입니다.
규칙 ID	uint32	해당하는 경우 이벤트를 트리거한 규칙의 내부 식별자입니다.
터널 규칙 ID	uint32	해당하는 경우 이벤트를 트리거한 터널 규칙의 내부 식별자입니다.
규칙 작업	uint16	해당 규칙(허용, 차단 등)에 대해 사용자 인터페이스에서 선택한 작업입니다.
규칙 이유	uint32	규칙이 이벤트를 트리거한 이유입니다.
이니시에이터 포트	uint16	시작 호스트에 사용되는 포트입니다.
응답자 포트	uint16	응답 호스트에 사용되는 포트입니다.
TCP 플래그	uint16	연결 이벤트에 대한 모든 TCP 플래그를 나타냅니다.
프로토콜	uint8	IANA에서 지정한 프로토콜 번호입니다.
NetFlow 소스	uint8[16]	연결에 대한 데이터를 내보낸 NetFlow 지원 디바이스의 IP 주소입니다.
인스턴스 ID	uint16	이벤트를 생성한 매니지드 디바이스의 Snort 인스턴스의 숫자 ID입니다.
연결 카운터	uint16	1초 이내에 발생하는 연결 이벤트를 구별하는 데 사용되는 값입니다.
첫 번째 패킷 타임스탬프	uint32	세션에서 첫 번째 패킷이 교환된 날짜의 시간의 UNIX 타임스탬프입니다.
마지막 패킷 타임스탬프	uint32	세션에서 마지막 패킷이 교환된 날짜의 시간의 UNIX 타임스탬프입니다.
이니시에이터 전송 패킷	uint64	시작 호스트에서 전송한 패킷 수입니다.
응답자 전송 패킷	uint64	응답 호스트에서 전송한 패킷 수입니다.
이니시에이터 전송 바이트	uint64	시작 호스트에서 전송한 바이트 수입니다.

표 B-39 6.1 이상 버전용 연결 통계 데이터 블록 필드 (계속)

필드	데이터 유형	설명
응답자 전송 바이트	uint64	응답 호스트에서 전송한 바이트 수입니다.
삭제된 이니시에이터 패킷	uint64	속도 제한으로 인해 세션 이니시에이터에서 삭제된 패킷 수입니다.
삭제된 응답자 패킷	uint64	속도 제한으로 인해 세션 응답자에서 삭제된 패킷 수입니다.
삭제된 이니시에이터 바이트	uint64	속도 제한으로 인해 세션 이니시에이터에서 삭제된 바이트 수입니다.
삭제된 응답자 바이트	uint64	속도 제한으로 인해 세션 응답자에서 삭제된 바이트 수입니다.
QOS 적용 인터페이스	uint8[16]	속도가 제한되는 연결에서 속도 제한이 적용되는 인터페이스 이름입니다.
QOS 규칙 ID	uint32	해당하는 경우 연결에 적용된 QoS(Quality of Service) 규칙의 내부 ID 번호입니다.
사용자 ID	uint32	트래픽을 생성한 호스트에 마지막으로 로그인한 사용자의 내부 ID 번호입니다.
애플리케이션 프로토콜 ID	uint32	애플리케이션 프로토콜의 애플리케이션 ID입니다.
URL 카테고리	uint32	URL 카테고리의 내부 ID 번호입니다.
URL 평판	uint32	URL 평판의 내부 ID 번호입니다.
클라이언트 애플리케이션 ID	uint32	해당하는 경우 탐지된 클라이언트 애플리케이션의 내부 ID 번호입니다.
웹 애플리케이션 ID	uint32	해당하는 경우 탐지된 웹 애플리케이션의 내부 ID 번호입니다.
문자열 블록 유형	uint32	클라이언트 애플리케이션 URL에 대한 문자열 데이터 블록을 시작합니다. 이 값은 항상 `0`입니다.
문자열 블록 길이	uint32	클라이언트 애플리케이션 URL 문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이 필드의 8바이트에 클라이언트 애플리케이션 URL 문자열의 바이트 수를 더한 값이 포함됩니다.
클라이언트 애플리케이션 URL	string	해당하는 경우 클라이언트 애플리케이션이 액세스한 URL입니다. 예를 들면 `/files/index.html`과 같습니다.
문자열 블록 유형	uint32	호스트 NetBIOS 이름에 대한 문자열 데이터 블록을 시작합니다. 이 값은 항상 `0`입니다.
문자열 블록 길이	uint32	문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이 필드의 8바이트에 NetBIOS 이름 문자열의 바이트 수를 더한 값이 포함됩니다.
NetBIOS 이름	string	호스트 NetBIOS 이름 문자열입니다.
문자열 블록 유형	uint32	클라이언트 애플리케이션 버전에 대한 문자열 데이터 블록을 시작합니다. 이 값은 항상 `0`입니다.

표 B-39 6.1 이상 버전용 연결 통계 데이터 블록 필드 (계속)

필드	데이터 유형	설명
문자열 블록 길이	uint32	클라이언트 애플리케이션 버전에 대한 문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이의 8바이트에 버전의 바이트 수를 더한 값이 포함됩니다.
클라이언트 애플리케이션 버전	string	클라이언트 애플리케이션 버전입니다.
모니터링 규칙 1	uint32	연결 이벤트와 관련된 첫 번째 모니터 규칙의 ID입니다.
모니터링 규칙 2	uint32	연결 이벤트와 관련된 두 번째 모니터 규칙의 ID입니다.
모니터링 규칙 3	uint32	연결 이벤트와 관련된 세 번째 모니터 규칙의 ID입니다.
모니터링 규칙 4	uint32	연결 이벤트와 관련된 네 번째 모니터 규칙의 ID입니다.
모니터링 규칙 5	uint32	연결 이벤트와 관련된 다섯 번째 모니터 규칙의 ID입니다.
모니터링 규칙 6	uint32	연결 이벤트와 관련된 여섯 번째 모니터 규칙의 ID입니다.
모니터링 규칙 7	uint32	연결 이벤트와 관련된 일곱 번째 모니터 규칙의 ID입니다.
모니터링 규칙 8	uint32	연결 이벤트와 관련된 여덟 번째 모니터 규칙의 ID입니다.
보안 인텔리전스 소스/대상	uint8	소스 또는 대상 IP 주소가 IP 블랙리스트와 일치했는지를 나타냅니다.
보안 인텔리전스 계층	uint8	IP 블랙리스트와 일치한 IP 계층입니다.
파일 이벤트 개수	uint16	1초 이내에 발생하는 파일 이벤트를 구별하는 데 사용되는 값입니다.
침입 이벤트 개수	uint16	1초 이내에 발생하는 침입 이벤트를 구별하는 데 사용되는 값입니다.
이니시에이터 국가	uint16	시작 호스트의 국가 코드입니다.
응답자 국가	uint16	응답 호스트의 국가 코드입니다.
원래 클라이언트 국가	uint16	요청이 생성된 프록시를 사용하는 호스트의 국가 코드입니다.
IOC 번호	uint16	이 이벤트와 관련된 보안 침해의 ID 번호입니다.
소스 자동 시스템	uint32	소스의 AS 번호(원본 또는 피어)입니다.
대상 자동 시스템	uint32	대상의 AS 번호(원본 또는 피어)입니다.
SNMP 입력	uint16	입력 인터페이스의 SNMP 인덱스입니다.
SNMP 출력	uint16	출력 인터페이스의 SNMP 인덱스입니다.
소스 TOS	uint8	들어오는 인터페이스에 대한 서비스 유형 바이트 설정입니다.
대상 TOS	uint8	나가는 인터페이스에 대한 서비스 유형 바이트 설정입니다.
소스 마스크	uint8	소스 주소 접두사 마스크입니다.
대상 마스크	uint8	대상 주소 접두사 마스크입니다.
보안 상황	uint8(16)	트래픽이 통과한 보안 상황(가상 방화벽)의 ID 번호입니다. 이 필드는 다중 컨텍스트 모드의 ASA FirePOWER 디바이스에 대해서만 채워집니다.

표 B-39 6.1 이상 버전용 연결 통계 데이터 블록 필드 (계속)

필드	데이터 유형	설명
VLAN ID	uint16	호스트가 구성원으로 포함된 VLAN을 나타내는 VLAN ID 번호입니다.
문자열 블록 유형	uint32	참조된 호스트 이름을 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	참조된 호스트 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Referenced Host(참조된 호스트) 필드의 바이트 수를 더한 값이 포함됩니다.
참조된 호스트	string	HTTP 또는 DNS로 제공되는 호스트 이름 정보입니다.
문자열 블록 유형	uint32	사용자 에이전트를 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	사용자 에이전트 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 User Agent(사용자 에이전트) 필드의 바이트 수를 더한 값이 포함됩니다.
사용자 에이전트	string	세션에서 UserAgent 헤더 필드의 정보입니다.
문자열 블록 유형	uint32	HTTP 참조 페이지를 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	HTTP 참조 페이지 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 HTTP Referer(HTTP 참조 페이지) 필드의 바이트 수를 더한 값이 포함됩니다.
HTTP 참조 페이지	string	페이지가 생성된 사이트입니다. HTTP 트래픽의 참조 페이지 헤더 정보에서 찾을 수 있습니다.
SSL 인증서 핑거프린트	uint8[20]	SSL 서버 인증서의 SHA1 해시입니다.
SSL 정책 ID	uint8[16]	연결을 처리한 SSL 정책의 ID 번호입니다.
SSL 규칙 ID	uint32	연결을 처리한 SSL 규칙 또는 기본 동작의 ID 번호입니다.
SSL 암호 그룹	uint16	SSL 연결에서 사용되는 암호화 그룹입니다. 값은 10진수 형식으로 저장됩니다. 값으로 지정되는 암호 그룹은 www.iana.org/assignments/tls-parameters/tls-parameters.xhtml을 참조하십시오.
SSL 버전	uint8	연결을 암호화하는 데 사용된 SSL 또는 TLS 프로토콜 버전입니다.

표 B-39 6.1 이상 버전용 연결 통계 데이터 블록 필드 (계속)

필드	데이터 유형	설명
SSL 서버 인증서 상태	uint32	SSL 인증서의 상태입니다. 가능한 값은 다음과 같습니다. • 0 - 확인되지 않음 - 서버 인증서 상태를 평가하지 않았습니다. • 1 - 알 수 없음 - 서버 인증서 상태를 확인할 수 없습니다. • 2 - 유효 - 서버 인증서가 유효합니다. • 4 - 자체 서명 - 서버 인증서가 자체 서명되었습니다. • 16 - 유효하지 않은 발급자 - 서버 인증서의 발급자가 유효하지 않습니다. • 32 - 유효하지 않은 서명 - 서버 인증서의 서명이 유효하지 않습니다. • 64 - 만료됨 - 서버 인증서가 만료되었습니다. • 128 - 아직 유효하지 않음 - 서버 인증서가 아직 유효하지 않습니다. • 256 - 해지됨 - 서버 인증서가 해지되었습니다.
SSL 실제 작업	uint16	SSL 규칙에 기반한 연결에서 수행된 작업입니다. 규칙에 명시된 작업이 가능하지 않을 수도 있으므로, 이는 예상 작업과 다를 수 있습니다. 가능한 값은 다음과 같습니다. • 0 - '알 수 없음' • 1 - '암호 해독 안 함' • 2 - '차단' • 3 - '차단 및 재설정' • 4 - '암호 해독(알려진 키)' • 5 - '암호 해독(키 교체)' • 6 - '암호 해독(재서명)'
SSL 예상 작업	uint16	SSL 규칙에 기반한 연결에서 수행해야 하는 작업입니다. 가능한 값은 다음과 같습니다. • 0 - '알 수 없음' • 1 - '암호 해독 안 함' • 2 - '차단' • 3 - '차단 및 재설정' • 4 - '암호 해독(알려진 키)' • 5 - '암호 해독(키 교체)' • 6 - '암호 해독(재서명)'

표 B-39 6.1 이상 버전용 연결 통계 데이터 블록 필드 (계속)

필드	데이터 유형	설명
SSL 플로우 상태	uint16	SSL 플로우의 상태입니다. 이 값은 작업을 수행한 이유 또는 오류 메시지가 표시된 이유를 설명합니다. 가능한 값은 다음과 같습니다. • 0 - '알 수 없음' • 1 - '일치하지 않음' • 2 - '성공' • 3 - '캐시되지 않은 세션' • 4 - '알 수 없는 암호 그룹' • 5 - '지원되지 않는 암호 그룹' • 6 - '지원되지 않는 SSL 버전' • 7 - 'SSL 압축 사용됨' • 8 - '패시브 모드에서 세션 암호 해독 불가' • 9 - '핸드셰이크 오류' • 10 - '암호 해독 오류' • 11 - '서버 이름 카테고리 조회 보류 중' • 12 - '공용 이름 카테고리 조회 보류 중' • 13 - '내부 오류' • 14 - '네트워크 파라미터 사용 불가' • 15 - '유효하지 않은 서버 인증서 핸들' • 16 - '서버 인증서 핑거프린트 사용 불가' • 17 - '주체 DN을 캐시할 수 없음' • 18 - '발급자 DN을 캐시할 수 없음' • 19 - '알 수 없는 SSL 버전' • 20 - '외부 인증서 목록 사용 불가' • 21 - '외부 인증서 핑거프린트 사용 불가' • 22 - '내부 인증서 목록이 유효하지 않음' • 23 - '내부 인증서 목록 사용 불가' • 24 - '내부 인증서 사용 불가' • 25 - '내부 인증서 핑거프린트 사용 불가' • 26 - '서버 인증서 검증 사용 불가' • 27 - '서버 인증서 검증 장애' • 28 - '유효하지 않은 작업'
SSL 플로우 오류	uint32	자세한 SSL 오류 코드입니다. 이러한 값은 지원용으로 필요할 수 있습니다.

표 B-39 6.1 이상 버전용 연결 통계 데이터 블록 필드 (계속)

필드	데이터 유형	설명
SSL 플로우 메시지	uint32	SSL 핸드셰이크 도중 클라이언트와 서버 간에 교환된 메시지입니다. 자세한 내용은 http://tools.ietf.org/html/rfc5246을 참조하십시오. • 0x00000001 — NSE_MT__HELLO_REQUEST • 0x00000002 — NSE_MT__CLIENT_ALERT • 0x00000004 — NSE_MT__SERVER_ALERT • 0x00000008 — NSE_MT__CLIENT_HELLO • 0x00000010 — NSE_MT__SERVER_HELLO • 0x00000020 — NSE_MT__SERVER_CERTIFICATE • 0x00000040 — NSE_MT__SERVER_KEY_EXCHANGE • 0x00000080 — NSE_MT__CERTIFICATE_REQUEST • 0x00000100 — NSE_MT__SERVER_HELLO_DONE • 0x00000200 — NSE_MT__CLIENT_CERTIFICATE • 0x00000400 — NSE_MT__CLIENT_KEY_EXCHANGE • 0x00000800 — NSE_MT__CERTIFICATE_VERIFY • 0x00001000 — NSE_MT__CLIENT_CHANGE_CIPHER_SPEC • 0x00002000 — NSE_MT__CLIENT_FINISHED • 0x00004000 — NSE_MT__SERVER_CHANGE_CIPHER_SPEC • 0x00008000 — NSE_MT__SERVER_FINISHED • 0x00010000 — NSE_MT__NEW_SESSION_TICKET • 0x00020000 — NSE_MT__HANDSHAKE_OTHER • 0x00040000 — NSE_MT__APP_DATA_FROM_CLIENT • 0x00080000 — NSE_MT__APP_DATA_FROM_SERVER
SSL 플로우 플래그	uint64	암호화된 연결에 대한 디버깅 레벨 플래그입니다. 가능한 값은 다음과 같습니다. • 0x00000001 - NSE_FLOW__VALID - 다른 필드를 유효하게 만들려면 설정해야 함 • 0x00000002 - NSE_FLOW__INITIALIZED - 처리 준비가 완료된 내부 구조 • 0x00000004 - NSE_FLOW__INTERCEPT - SSL 세션이 중단됨
문자열 블록 유형	uint32	SSL 서버 이름을 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	SSL 서버 이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 SSL Server Name(SSL 서버 이름) 필드의 바이트 수를 더한 값이 포함됩니다.

표 B-39 6.1 이상 버전용 연결 통계 데이터 블록 필드 (계속)

필드	데이터 유형	설명
SSL 서버 이름	string	SSL Client Hello의 서버 이름 표시에서 제공된 이름입니다.
SSL URL 카테고리	uint32	서버 이름 및 인증서 일반 이름에서 확인된 플로우의 카테고리입니다.
SSL 세션 ID	uint8[32]	클라이언트와 서버가 세션 재사용에 동의하는 경우 SSL 핸드셰이크 중에 사용되는 세션 ID의 값입니다.
SSL 세션 ID 길이	uint8	SSL 세션 ID의 길이입니다. 세션 ID는 32바이트를 초과할 수는 없으며 32바이트보다 작을 수는 있습니다.
SSL 티켓 ID	uint8[20]	클라이언트와 서버가 세션 티켓 사용에 동의하는 경우 사용되는 세션 티켓의 해시입니다.
SSL 티켓 ID 길이	uint8	SSL 티켓 ID의 길이입니다. 티켓 ID는 20바이트를 초과할 수는 없으며 20바이트보다 작을 수는 있습니다.
네트워크 분석 정책 수정	uint8[16]	연결 이벤트와 관련된 네트워크 분석 정책의 수정 버전입니다.
엔드포인트 프로파일 ID	uint32	ISE가 식별한 연결 엔드포인트에서 사용하는 디바이스 유형의 ID 번호입니다. 각 DC에 대해 고유하며 메타데이터에서 확인 가능합니다.
보안 그룹 ID	uint32	정책을 기준으로 ISE가 사용자에게 할당하는 ID 번호입니다.
위치 IPv6	uint8[16]	ISE와 통신하는 인터페이스의 IP 주소입니다. IPv4 또는 IPv6일 수 있습니다.
HTTP 응답	uint32	HTTP 요청의 응답 코드입니다.
문자열 블록 유형	uint32	DNS 쿼리에 대한 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이 필드의 8바이트에 DNS 쿼리 문자열의 바이트 수를 더한 값이 포함됩니다.
DNS 쿼리	string	DNS 서버에 전송되는 쿼리의 콘텐츠입니다.
DNS 레코드 유형	uint16	DNS 레코드 유형에 해당하는 숫자 값입니다.
DNS 응답 유형	uint16	DNS 응답 유형에 해당하는 숫자 값입니다.
DNS TTL	uint32	DNS 응답의 초 단위 TTL(Time to Live)입니다.
싱크홀 UUID	uin8[16]	싱크홀 개체와 관련된 수정 UUID입니다.
보안 인텔리전스 목록 1	uint32	이벤트와 관련된 보안 인텔리전스 목록으로, 관련된 메타데이터의 보안 인텔리전스 목록에 매핑됩니다. 2개의 보안 인텔리전스 목록이 연결과 관련되어 있을 수 있습니다.
보안 인텔리전스 목록 2	uint32	이벤트와 관련된 보안 인텔리전스 목록으로, 관련된 메타데이터의 보안 인텔리전스 목록에 매핑됩니다. 2개의 보안 인텔리전스 목록이 연결과 관련되어 있을 수 있습니다.

레거시 파일 이벤트 데이터 구조

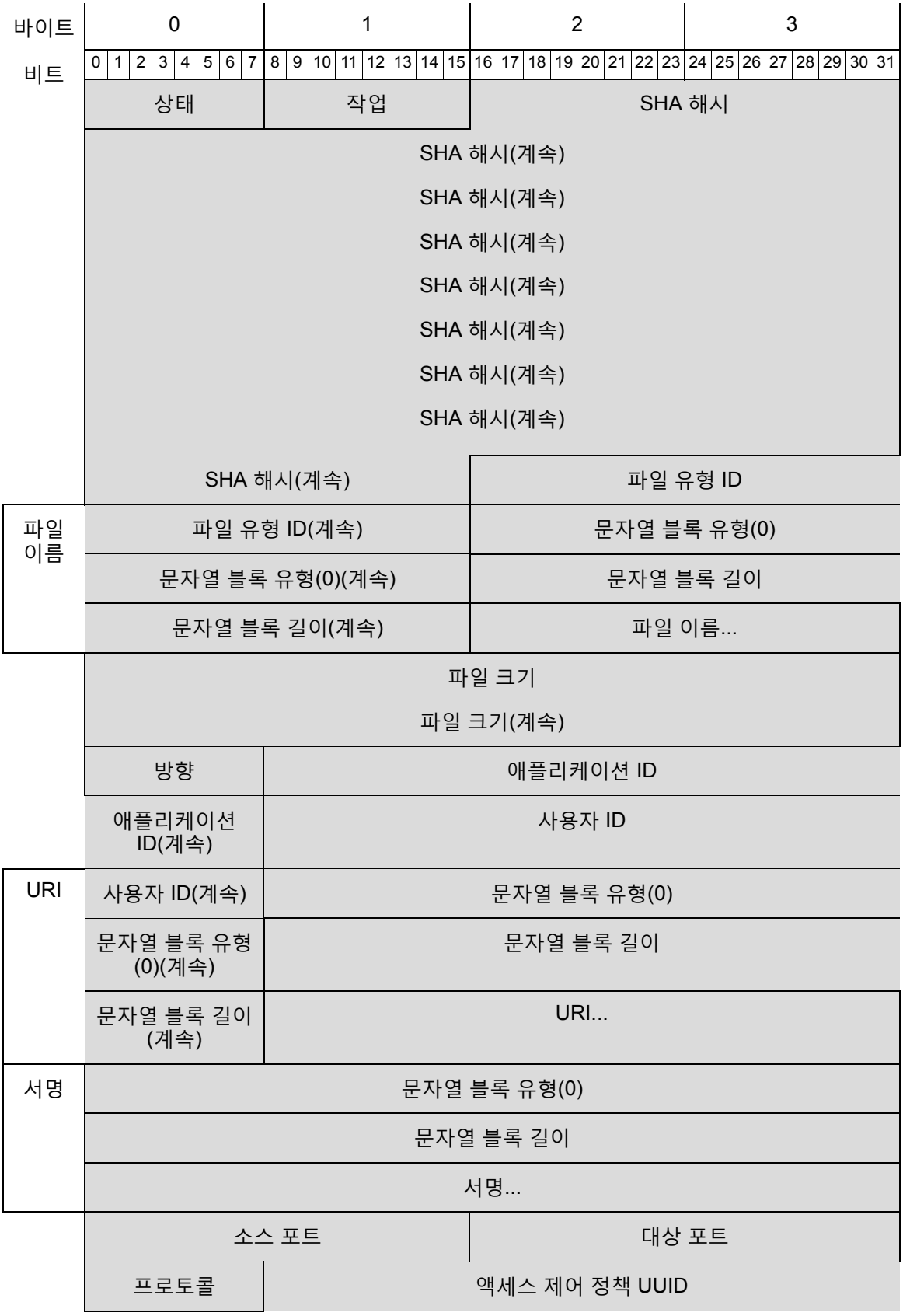
다음 항목에서는 기타 레거시 파일 이벤트 데이터 구조에 대해 설명합니다.

5.1.1.x 버전용 파일 이벤트

파일 이벤트는 네트워크를 통해 전송되는 파일에 대한 정보를 포함합니다. 이러한 정보로는 연결 정보, 파일이 악성코드인지 여부, 그리고 파일을 식별하는 특정 정보가 포함됩니다. 계열 2 블록 그룹에서 파일 이벤트의 블록 유형은 23입니다.

다음 그림에 파일 이벤트 데이터 블록의 구조가 나와 있습니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
파일 이벤트 블록 유형(23)																																
파일 이벤트 블록 길이																																
디바이스 ID																																
연결 인스턴스																	연결 카운터															
연결 타임스탬프																																
파일 이벤트 타임스탬프																																
소스 IP 주소 소스 IP 주소(계속) 소스 IP 주소(계속) 소스 IP 주소(계속)																																
대상 IP 주소 대상 IP 주소(계속) 대상 IP 주소(계속) 대상 IP 주소(계속)																																


바이트
0
1
2
3
비트
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
상태
작업
SHA 해시
SHA 해시(계속)
SHA 해시(계속)
SHA 해시(계속)
SHA 해시(계속)
SHA 해시(계속)
SHA 해시(계속)
SHA 해시(계속)
SHA 해시(계속)
파일 유형 ID
파일 이름
파일 유형 ID(계속)
문자열 블록 유형(0)
문자열 블록 유형(0)(계속)
문자열 블록 길이
문자열 블록 길이(계속)
파일 이름...
파일 크기
파일 크기(계속)
방향
애플리케이션 ID
애플리케이션 ID(계속)
사용자 ID
URI
사용자 ID(계속)
문자열 블록 유형(0)
문자열 블록 유형(0)(계속)
문자열 블록 길이
문자열 블록 길이(계속)
URI...
서명
문자열 블록 유형(0)
문자열 블록 길이
서명...
소스 포트
대상 포트
프로토콜
액세스 제어 정책 UUID

다음 표에는 파일 이벤트 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 B-40 파일 이벤트 데이터 블록 필드

필드	데이터 유형	설명
파일 이벤트 블록 유형	uint32	파일 이벤트 데이터 블록을 시작합니다. 이 값은 항상 23입니다.
파일 이벤트 블록 길이	uint32	파일 이벤트 블록의 총 바이트 수입니다. 여기에는 파일 이벤트 블록 유형 및 길이 필드의 8바이트에 그 뒤의 데이터 바이트 수를 더한 값이 포함됩니다.
디바이스 ID	uint32	이벤트를 생성한 디바이스의 ID입니다.
연결 인스턴스	uint16	이벤트를 생성한 디바이스의 Snort 인스턴스입니다. 이벤트를 연결 또는 침입 이벤트와 연결하는 데 사용됩니다.
연결 카운터	uint16	1초 이내에 발생하는 연결 이벤트를 구별하는 데 사용되는 값입니다.
연결 타임스탬프	uint32	관련 연결 이벤트의 UNIX 타임스탬프(1970년 1월 1일 이후의 초 단위 시간)입니다.
파일 이벤트 타임스탬프	uint32	파일 유형이 식별되고 파일 이벤트가 생성된 UNIX 타임스탬프(1970년 1월 1일 이후의 초 단위 시간)입니다.
소스 IP 주소	uint8[16]	연결 소스의 IPv4 또는 IPv6 주소입니다.
대상 IP 주소	uint8[16]	연결 대상의 IPv4 또는 IPv6 주소입니다.
상태	uint8	파일의 악성코드 상태입니다. 가능한 값은 다음과 같습니다. • 1 - CLEAN - 파일이 정상 상태이며 악성코드가 포함되어 있지 않습니다. • 2 - UNKNOWN - 파일에 악성코드가 포함되어 있는지 알 수 없습니다. • 3 - MALWARE - 파일에 악성코드가 포함되어 있습니다. • 4 - CACHE_MISS - 소프트웨어가 Cisco 클라우드에 상태 요청을 보낼 수 없습니다. • 5 - NO_CLOUD_RESP - Cisco 클라우드 서비스가 요청에 응답하지 않았습니다.

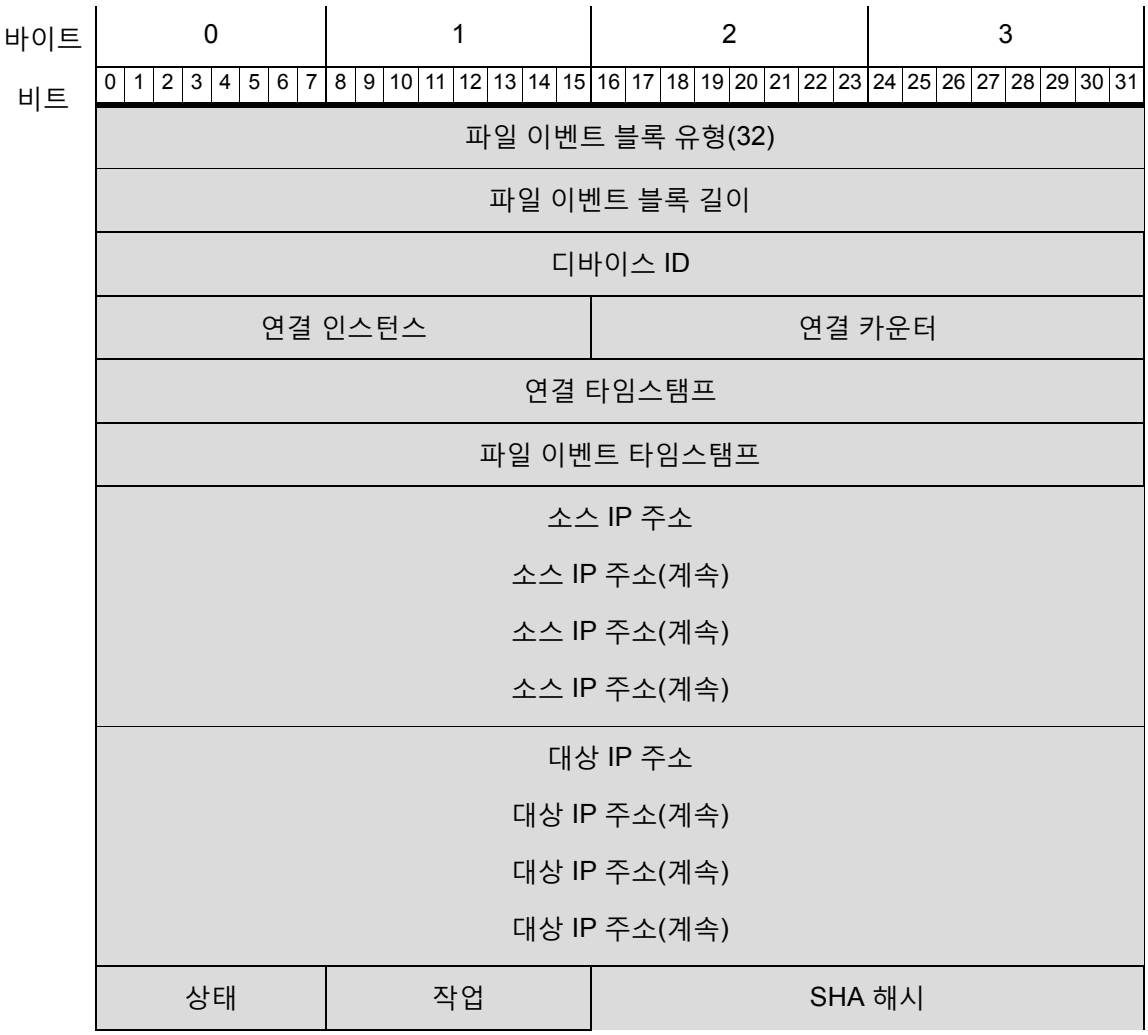
표 B-40 파일 이벤트 데이터 블록 필드 (계속)

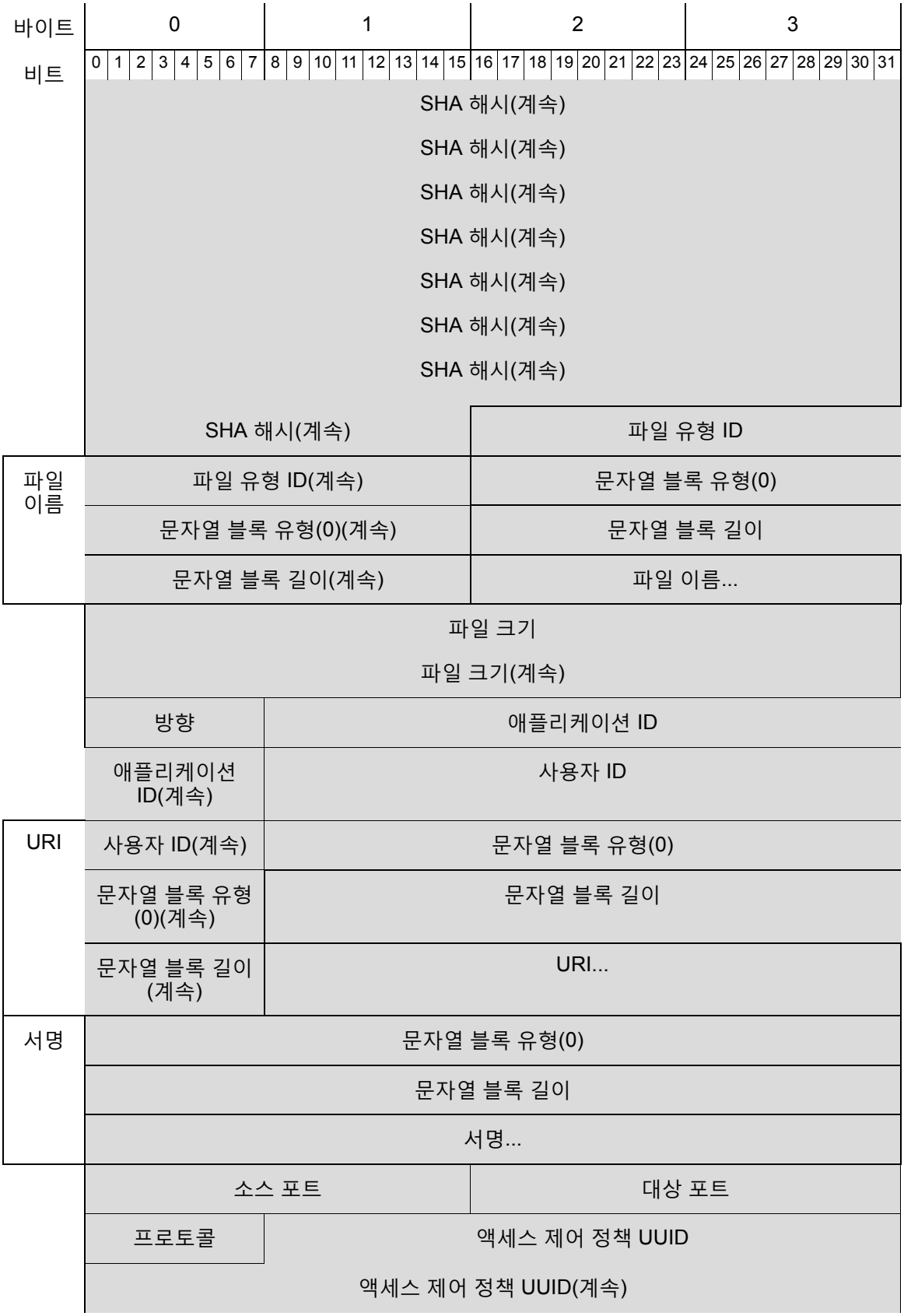
필드	데이터 유형	설명
작업	uint8	파일 유형을 기반으로 파일에 조취를 취합니다. 다음과 같은 값을 사용할 수 있습니다. • 1 - 탐지 • 2 - 차단 • 3 - 악성코드 클라우드 조회 • 4 - 악성코드 차단 • 5 - 악성코드 화이트리스트 추가
SHA 해시	uint8[32]	이진 형식으로 된 파일의 SHA-256 해시입니다.
파일 유형 ID	uint32	파일 유형에 매핑되는 ID 번호입니다.
파일 이름	string	파일의 이름입니다.
파일 크기	uint64	파일의 바이트 단위 크기입니다.
방향	uint8	파일이 업로드되었는지 아니면 다운로드되었는지를 나타내는 값입니다. 다음과 같은 값을 사용할 수 있습니다. • 1 - 다운로드 • 2 - 업로드 현재 이 값은 프로토콜에 따라 달라집니다(예: 연결이 HTTP인 경우 다운로드임).
애플리케이션 ID	uint32	파일 전송을 사용하여 애플리케이션에 매핑되는 ID 번호입니다.
사용자 ID	uint32	시스템이 식별한 대상 호스트에 로그인하는 사용자의 ID 번호입니다.
URI	string	연결의 URI(Uniform Resource Identifier)입니다.
서명	string	문자열 형식으로 된 파일의 SHA-256 해시입니다.
소스 포트	uint16	연결 소스의 포트 번호입니다.
대상 포트	uint16	연결 대상의 포트 번호입니다.
프로토콜	uint8	사용자가 지정한 IANA 프로토콜 번호입니다. 예를 들면 다음과 같습니다. • 1 - ICMP • 4 - IP • 6 - TCP • 17 - UDP 현재는 TCP만 설정 가능합니다.
액세스 제어 정책 UUID	uint8[16]	이벤트를 트리거한 액세스 제어 정책의 고유 식별자입니다.

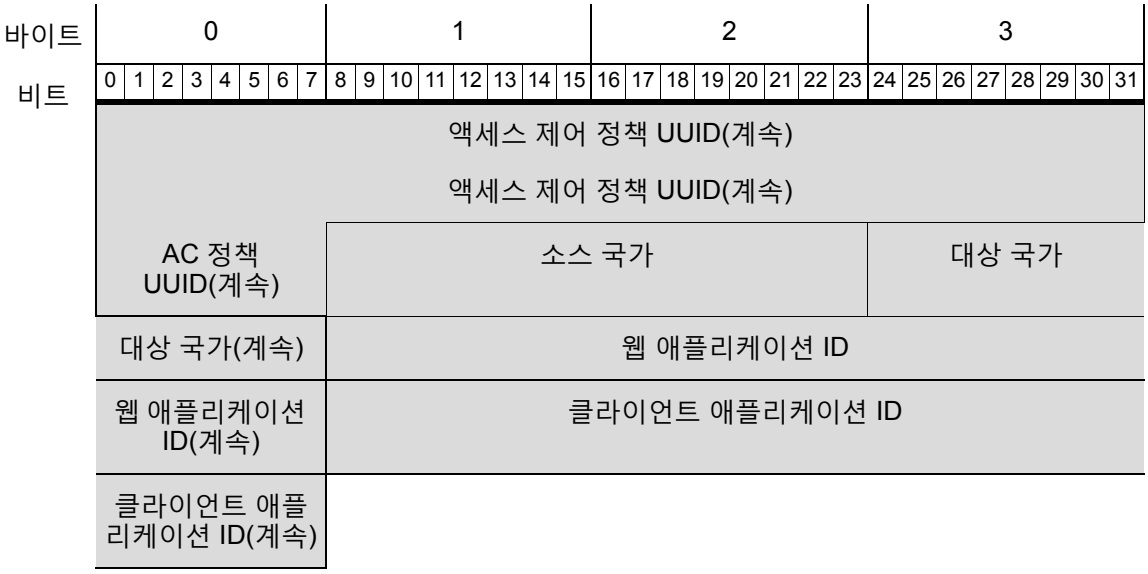
5.2.x 버전용 파일 이벤트

파일 이벤트는 네트워크를 통해 전송되는 파일에 대한 정보를 포함합니다. 이러한 정보로는 연결 정보, 파일이 악성코드인지 여부, 그리고 파일을 식별하는 특정 정보가 포함됩니다. 계열 2 블록 그룹에서 파일 이벤트의 블록 유형은 32입니다. 이는 블록 유형 23을 대체합니다. 소스 및 대상 국가와 클라이언트 및 웹 애플리케이션 인스턴스를 추적하기 위한 새 필드가 추가되었습니다.

다음 그림에 파일 이벤트 데이터 블록의 구조가 나와 있습니다.




바이트
0
1
2
3
비트
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
SHA 해시(계속)
SHA 해시(계속)
SHA 해시(계속)
SHA 해시(계속)
SHA 해시(계속)
SHA 해시(계속)
SHA 해시(계속)
SHA 해시(계속)
파일 유형 ID
파일 이름
파일 유형 ID(계속)
문자열 블록 유형(0)
문자열 블록 유형(0)(계속)
문자열 블록 길이
문자열 블록 길이(계속)
파일 이름...
파일 크기
파일 크기(계속)
방향
애플리케이션 ID
애플리케이션 ID(계속)
사용자 ID
URI
사용자 ID(계속)
문자열 블록 유형(0)
문자열 블록 유형(0)(계속)
문자열 블록 길이
문자열 블록 길이(계속)
URI...
서명
문자열 블록 유형(0)
문자열 블록 길이
서명...
소스 포트
대상 포트
프로토콜
액세스 제어 정책 UUID
액세스 제어 정책 UUID(계속)



다음 표에는 파일 이벤트 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 B-41 파일 이벤트 데이터 블록 필드

필드	데이터 유형	설명
파일 이벤트 블록 유형	uint32	파일 이벤트 데이터 블록을 시작합니다. 이 값은 항상 23입니다.
파일 이벤트 블록 길이	uint32	파일 이벤트 블록의 총 바이트 수입니다. 여기에는 파일 이벤트 블록 유형 및 길이 필드의 8바이트에 그 뒤의 데이터 바이트 수를 더한 값이 포함됩니다.
디바이스 ID	uint32	이벤트를 생성한 디바이스의 ID입니다.
연결 인스턴스	uint16	이벤트를 생성한 디바이스의 Snort 인스턴스입니다. 이벤트를 연결 또는 침입 이벤트와 연결하는 데 사용됩니다.
연결 카운터	uint16	1초 이내에 발생하는 연결 이벤트를 구별하는 데 사용되는 값입니다.
연결 타임스탬프	uint32	관련 연결 이벤트의 UNIX 타임스탬프(1970년 1월 1일 이후의 초 단위 시간)입니다.
파일 이벤트 타임스탬프	uint32	파일 유형이 식별되고 파일 이벤트가 생성된 UNIX 타임스탬프(1970년 1월 1일 이후의 초 단위 시간)입니다.
소스 IP 주소	uint8[16]	연결 소스의 IPv4 또는 IPv6 주소입니다.
대상 IP 주소	uint8[16]	연결 대상의 IPv4 또는 IPv6 주소입니다.

표 B-41 파일 이벤트 데이터 블록 필드 (계속)

필드	데이터 유형	설명
상태	uint8	파일의 악성코드 상태입니다. 가능한 값은 다음과 같습니다. • 1 - CLEAN - 파일이 정상 상태이며 악성코드가 포함되어 있지 않습니다. • 2 - NEUTRAL - 파일에 악성코드가 포함되어 있는지 알 수 없습니다. • 3 - MALWARE - 파일에 악성코드가 포함되어 있습니다. • 4 - CACHE_MISS - 소프트웨어가 Cisco 클라우드에 상태 요청을 보낼 수 없거나 Cisco 클라우드 서비스가 요청에 응답하지 않았습니다.
작업	uint8	파일 유형을 기반으로 파일에 조취를 취합니다. 다음과 같은 값을 사용할 수 있습니다. • 1 - 탐지 • 2 - 차단 • 3 - 악성코드 클라우드 조회 • 4 - 악성코드 차단 • 5 - 악성코드 화이트리스트 추가
SHA 해시	uint8[32]	이진 형식으로 된 파일의 SHA-256 해시입니다.
파일 유형 ID	uint32	파일 유형에 매핑되는 ID 번호입니다.
파일 이름	string	파일의 이름입니다.
파일 크기	uint64	파일의 바이트 단위 크기입니다.
방향	uint8	파일이 업로드되었는지 아니면 다운로드되었는지를 나타내는 값입니다. 다음과 같은 값을 사용할 수 있습니다. • 1 - 다운로드 • 2 - 업로드 현재 이 값은 프로토콜에 따라 달라집니다(예: 연결이 HTTP인 경우 다운로드임).
애플리케이션 ID	uint32	파일 전송을 사용하여 애플리케이션에 매핑되는 ID 번호입니다.
사용자 ID	uint32	시스템이 식별한 대상 호스트에 로그인하는 사용자의 ID 번호입니다.
URI	string	연결의 URI(Uniform Resource Identifier)입니다.
서명	string	문자열 형식으로 된 파일의 SHA-256 해시입니다.
소스 포트	uint16	연결 소스의 포트 번호입니다.
대상 포트	uint16	연결 대상의 포트 번호입니다.

표 B-41 파일 이벤트 데이터 블록 필드 (계속)

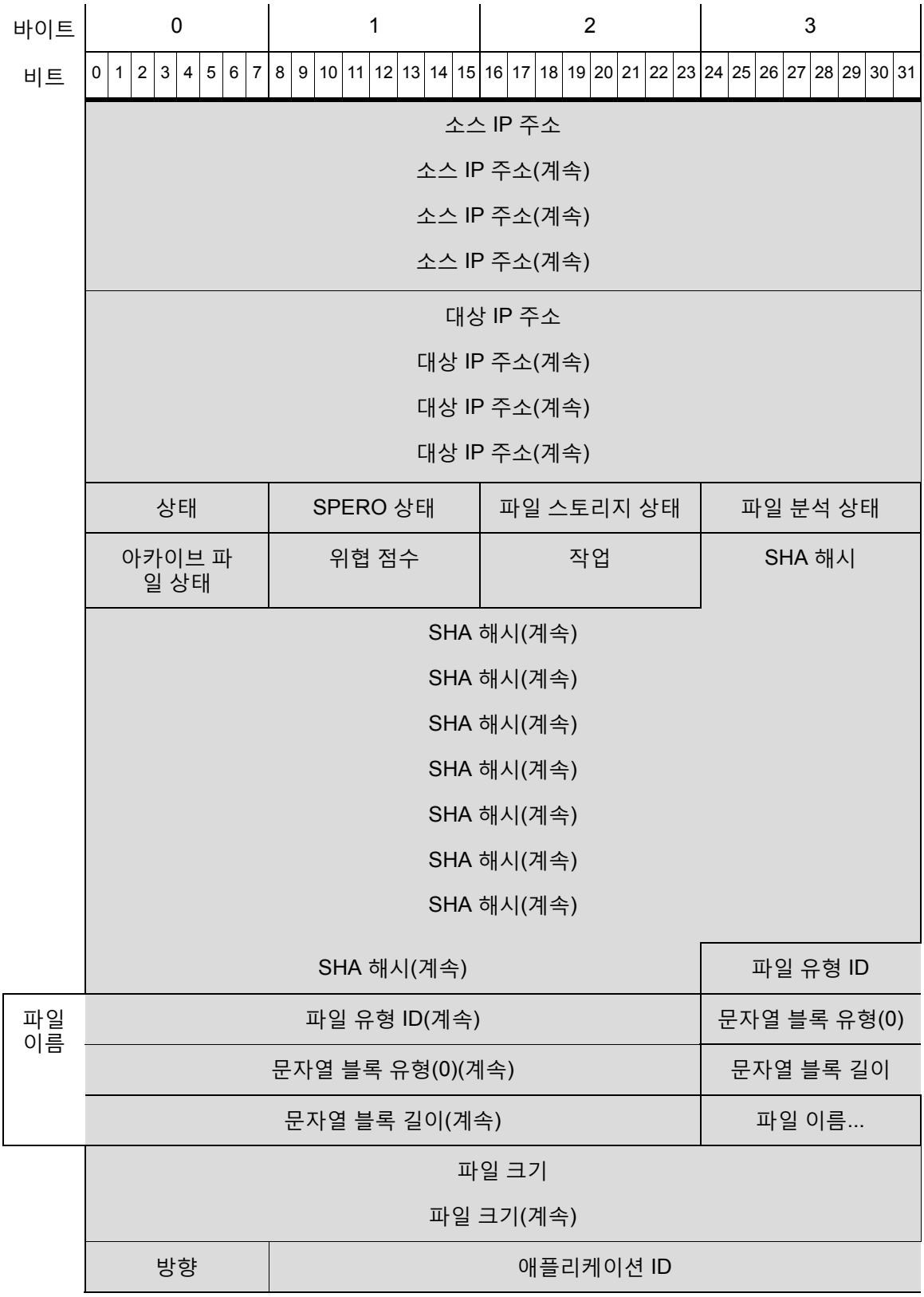
필드	데이터 유형	설명
프로토콜	uint8	사용자가 지정한 IANA 프로토콜 번호입니다. 예를 들면 다음과 같습니다. • 1 - ICMP • 4 - IP • 6 - TCP • 17 - UDP 현재는 TCP만 설정 가능합니다.
액세스 제어 정책 UUID	uint8[16]	이벤트를 트리거한 액세스 제어 정책의 고유 식별자입니다.
소스 국가	uint16	소스 호스트의 국가 코드입니다.
대상 국가	uint16	대상 호스트의 국가 코드입니다.
웹 애플리케이션 ID	uint32	해당하는 경우 웹 애플리케이션의 내부 ID 번호입니다.
클라이언트 애플리케이션 ID	uint32	해당하는 경우 클라이언트 애플리케이션의 내부 ID 번호입니다.

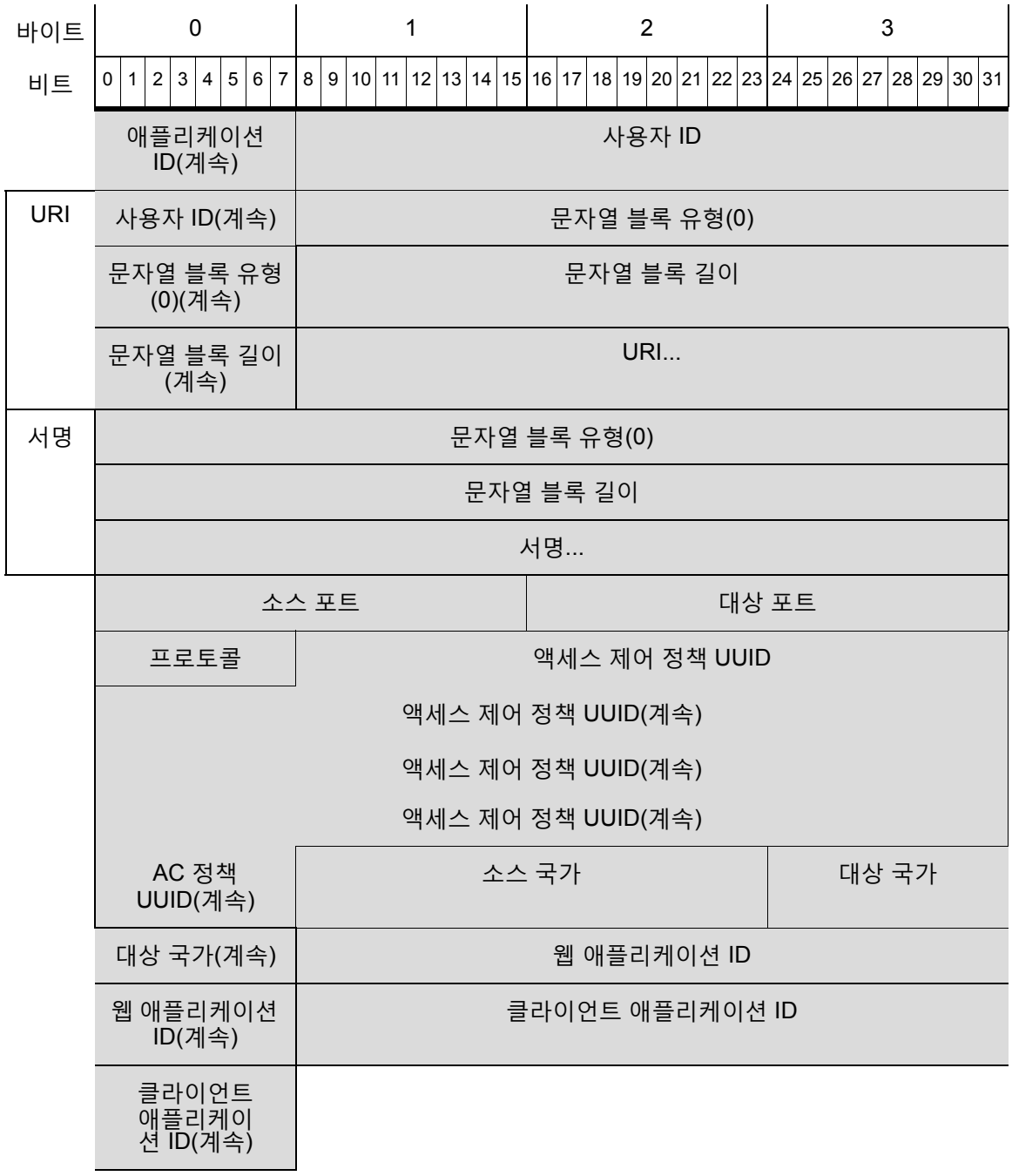
5.3 버전용 파일 이벤트

파일 이벤트는 네트워크를 통해 전송되는 파일에 대한 정보를 포함합니다. 이러한 정보로는 연결 정보, 파일이 악성코드인지 여부, 그리고 파일을 식별하는 특정 정보가 포함됩니다. 계열 2 블록 그룹에서 파일 이벤트의 블록 유형은 38입니다. 이는 블록 유형 32를 대체합니다. 동적 파일 분석 및 파일 스토리지를 추적하기 위한 새 필드가 추가되었습니다.

이벤트 버전이 3이고 이벤트 코드가 111인 요청 메시지에서 파일 이벤트 플래그(Request Flags(요청 플래그) 필드의 비트 30)를 설정하여 파일 이벤트 레코드를 요청합니다. 요청 플래그, 페이지 2-12의 내용을 참조하십시오. 비트 23을 활성화하면 레코드에 확장 이벤트 헤더가 포함됩니다.

다음 그림에 파일 이벤트 데이터 블록의 구조가 나와 있습니다.


바이트
0
1
2
3
비트
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
소스 IP 주소
소스 IP 주소(계속)
소스 IP 주소(계속)
소스 IP 주소(계속)
대상 IP 주소
대상 IP 주소(계속)
대상 IP 주소(계속)
대상 IP 주소(계속)
상태
SPERO 상태
파일 스토리지 상태
파일 분석 상태
아카이브 파일 상태
위협 점수
작업
SHA 해시
SHA 해시(계속)
SHA 해시(계속)
SHA 해시(계속)
SHA 해시(계속)
SHA 해시(계속)
SHA 해시(계속)
SHA 해시(계속)
SHA 해시(계속)
파일 유형 ID
파일 이름
파일 유형 ID(계속)
문자열 블록 유형(0)
문자열 블록 유형(0)(계속)
문자열 블록 길이
문자열 블록 길이(계속)
파일 이름...
파일 크기
파일 크기(계속)
방향
애플리케이션 ID



다음 표에는 파일 이벤트 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 B-42 파일 이벤트 데이터 블록 필드

필드	데이터 유형	설명
파일 이벤트 블록 유형	uint32	파일 이벤트 데이터 블록을 시작합니다. 이 값은 항상 23입니다.
파일 이벤트 블록 길이	uint32	파일 이벤트 블록의 총 바이트 수입니다. 여기에는 파일 이벤트 블록 유형 및 길이 필드의 8바이트에 그 뒤의 데이터 바이트 수를 더한 값이 포함됩니다.
디바이스 ID	uint32	이벤트를 생성한 디바이스의 ID입니다.
연결 인스턴스	uint16	이벤트를 생성한 디바이스의 Snort 인스턴스입니다. 이벤트를 연결 또는 침입 이벤트와 연결하는 데 사용됩니다.
연결 카운터	uint16	1초 이내에 발생하는 연결 이벤트를 구별하는 데 사용되는 값입니다.
연결 타임스탬프	uint32	관련 연결 이벤트의 UNIX 타임스탬프(1970년 1월 1일 이후의 초 단위 시간)입니다.
파일 이벤트 타임스탬프	uint32	파일 유형이 식별되고 파일 이벤트가 생성된 UNIX 타임스탬프(1970년 1월 1일 이후의 초 단위 시간)입니다.
소스 IP 주소	uint8[16]	연결 소스의 IPv4 또는 IPv6 주소입니다.
대상 IP 주소	uint8[16]	연결 대상의 IPv4 또는 IPv6 주소입니다.
상태	uint8	파일의 악성코드 상태입니다. 가능한 값은 다음과 같습니다. • 1 - CLEAN - 파일이 정상 상태이며 악성코드가 포함되어 있지 않습니다. • 2 - UNKNOWN - 파일에 악성코드가 포함되어 있는지 알 수 없습니다. • 3 - MALWARE - 파일에 악성코드가 포함되어 있습니다. • 4 - UNAVAILABLE - 소프트웨어가 Cisco 클라우드에 상태 요청을 보낼 수 없거나 Cisco 클라우드 서비스가 요청에 응답하지 않았습니다. • 5 - CUSTOM SIGNATURE - 파일이 사용자가 정의한 해시와 일치하며 사용자가 지정한 방식으로 처리됩니다.
SPERO 상태	uint8	파일 분석에 SPERO 서명이 사용되었는지를 나타냅니다. 값이 1, 2 또는 3이면 SPERO 분석이 사용된 것이고 그 외의 값이면 SPERO 분석이 사용되지 않은 것입니다.

표 B-42 파일 이벤트 데이터 블록 필드 (계속)

필드	데이터 유형	설명
파일 스토리지 상태	uint8	파일의 저장 상태입니다. 가능한 값은 다음과 같습니다. • 1 - 파일 저장됨 • 2 - 파일 저장됨 • 3 - 파일을 저장할 수 없음 • 4 - 파일을 저장할 수 없음 • 5 - 파일을 저장할 수 없음 • 6 - 파일을 저장할 수 없음 • 7 - 파일을 저장할 수 없음 • 8 - 파일 크기가 너무 큼 • 9 - 파일 크기가 너무 작음 • 10 - 파일을 저장할 수 없음 • 11 - 파일이 저장되지 않음(상태 사용 불가)
파일 분석 상태	uint8	동적 분석을 위해 파일이 제출되었는지 나타냅니다. 가능한 값은 다음과 같습니다. • 0 - 파일이 분석을 위해 전송되지 않음 • 1 - 분석을 위해 전송됨 • 2 - 분석을 위해 전송됨 • 4 - 분석을 위해 전송됨 • 5 - 전송하지 못함 • 6 - 전송하지 못함 • 7 - 전송하지 못함 • 8 - 전송하지 못함 • 9 - 파일 크기가 너무 작음 • 10 - 파일 크기가 너무 큼 • 11 - 분석을 위해 전송됨 • 12 - 분석 완료 • 13 - 장애(네트워크 문제) • 14 - 장애(속도 제한) • 15 - 장애(파일이 너무 큼) • 16 - 장애(파일 읽기 오류) • 17 - 장애(내부 라이브러리 오류) • 19 - 파일이 전송되지 않음(상태 사용 불가) • 20 - 장애(파일을 실행할 수 없음) • 21 - 장애(분석 시간 초과) • 22 - 분석을 위해 전송됨 • 23 - 파일이 지원되지 않음

표 B-42 파일 이벤트 데이터 블록 필드 (계속)

필드	데이터 유형	설명
아카이브 파일 상태	uint8	항상 0입니다.
위협 점수	uint8	동적 분석 과정에서 관찰된 잠재적으로 악의적인 동작을 기준으로 한 0부터 100까지의 숫자 값입니다.
작업	uint8	파일 유형을 기반으로 파일에 조취를 취합니다. 다음과 같은 값을 사용할 수 있습니다. • 1 - 탐지 • 2 - 차단 • 3 - 악성코드 클라우드 조회 • 4 - 악성코드 차단 • 5 - 악성코드 화이트리스트 추가
SHA 해시	uint8[32]	이진 형식으로 된 파일의 SHA-256 해시입니다.
파일 유형 ID	uint32	파일 유형에 매핑되는 ID 번호입니다. 이 필드의 의미가 이 이벤트와 함께 메타데이터에 포함되어 전송됩니다. 자세한 정보는 AMP for Endpoints 파일 유형 메타데이터, 페이지 3-42의 내용을 참조하십시오.
파일 이름	string	파일의 이름입니다.
파일 크기	uint64	파일의 바이트 단위 크기입니다.
방향	uint8	파일이 업로드되었는지 아니면 다운로드되었는지를 나타내는 값입니다. 다음과 같은 값을 사용할 수 있습니다. • 1 - 다운로드 • 2 - 업로드 현재 이 값은 프로토콜에 따라 달라집니다(예: 연결이 HTTP인 경우 다운로드임).
애플리케이션 ID	uint32	파일 전송을 사용하여 애플리케이션에 매핑되는 ID 번호입니다.
사용자 ID	uint32	시스템이 식별한 대상 호스트에 로그인하는 사용자의 ID 번호입니다.
URI	string	연결의 URI(Uniform Resource Identifier)입니다.
서명	string	문자열 형식으로 된 파일의 SHA-256 해시입니다.
소스 포트	uint16	연결 소스의 포트 번호입니다.
대상 포트	uint16	연결 대상의 포트 번호입니다.
프로토콜	uint8	사용자가 지정한 IANA 프로토콜 번호입니다. 예를 들면 다음과 같습니다. • 1 - ICMP • 4 - IP • 6 - TCP • 17 - UDP 현재는 TCP만 설정 가능합니다.

표 B-42 파일 이벤트 데이터 블록 필드 (계속)

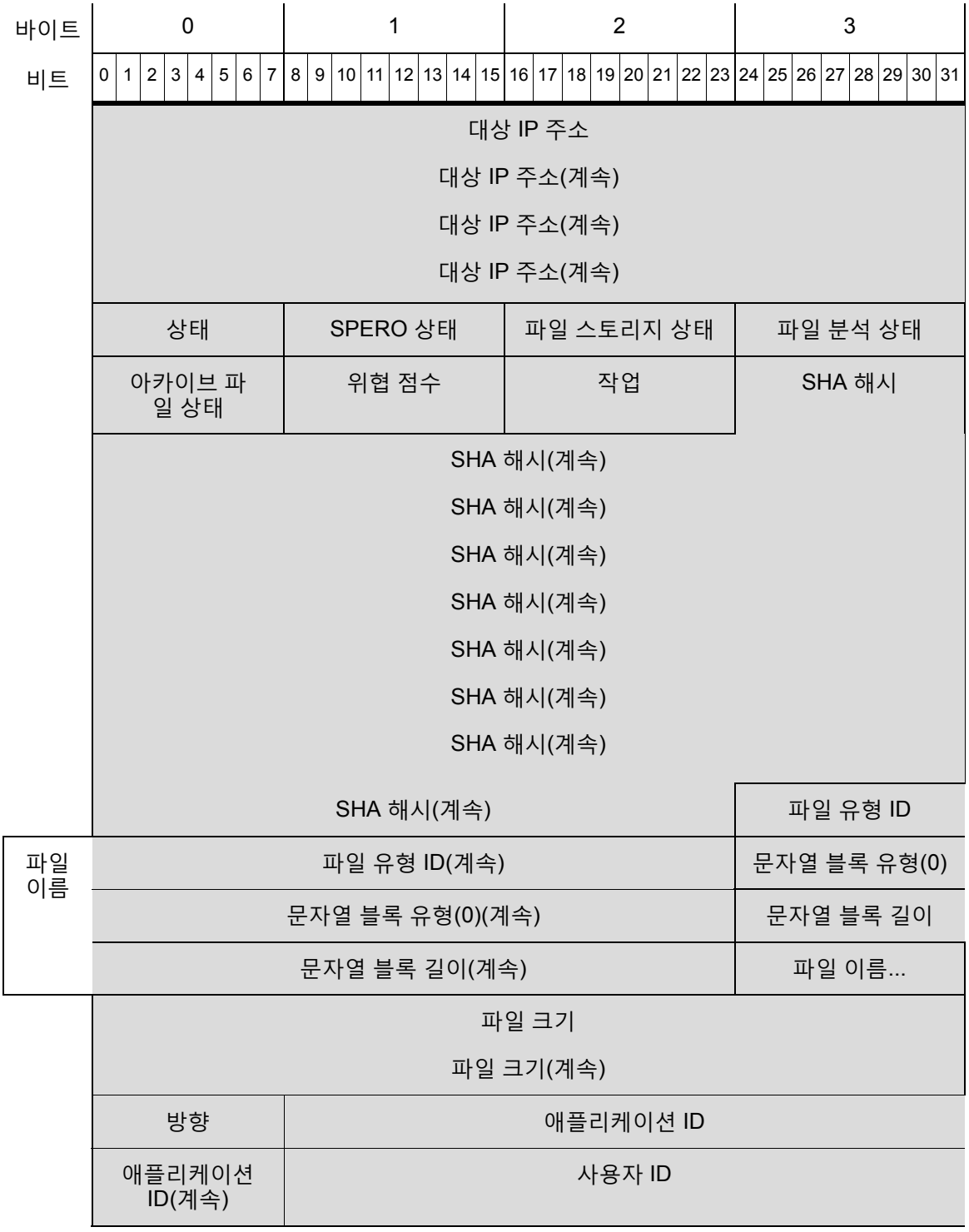
필드	데이터 유형	설명
액세스 제어 정책 UUID	uint8[16]	이벤트를 트리거한 액세스 제어 정책의 고유 식별자입니다.
소스 국가	uint16	소스 호스트의 국가 코드입니다.
대상 국가	uint16	대상 호스트의 국가 코드입니다.
웹 애플리케이션 ID	uint32	해당하는 경우 웹 애플리케이션의 내부 ID 번호입니다.
클라이언트 애플리케이션 ID	uint32	해당하는 경우 클라이언트 애플리케이션의 내부 ID 번호입니다.

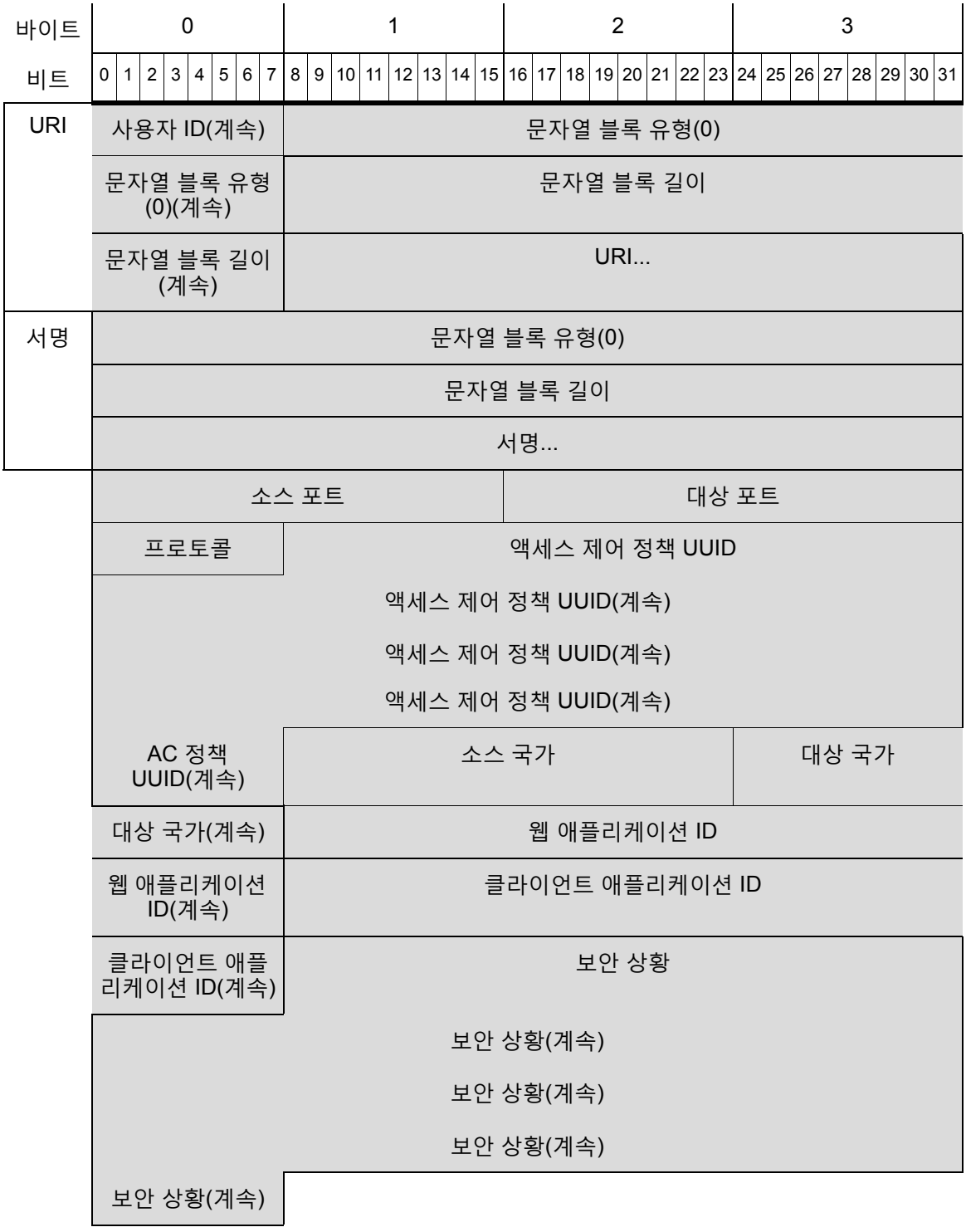
5.3.1 버전용 파일 이벤트

파일 이벤트는 네트워크를 통해 전송되는 파일에 대한 정보를 포함합니다. 이러한 정보로는 연결 정보, 파일이 악성코드인지 여부, 그리고 파일을 식별하는 특정 정보가 포함됩니다. 계열 2 블록 그룹에서 파일 이벤트의 블록 유형은 43입니다. 이는 블록 유형 38을 대체합니다. 보안 상황 필드가 추가되었습니다.

이벤트 버전이 4이고 이벤트 코드가 111인 요청 메시지에서 파일 이벤트 플래그(Request Flags(요청 플래그) 필드의 비트 30)를 설정하여 파일 이벤트 레코드를 요청합니다. 요청 플래그, 페이지 2-12의 내용을 참조하십시오. 비트 23을 활성화하면 레코드에 확장 이벤트 헤더가 포함됩니다.

다음 그림에 파일 이벤트 데이터 블록의 구조가 나와 있습니다.


바이트
0
1
2
3
비트
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
대상 IP 주소
대상 IP 주소(계속)
대상 IP 주소(계속)
대상 IP 주소(계속)
상태
SPERO 상태
파일 스토리지 상태
파일 분석 상태
아카이브 파일 상태
위협 점수
작업
SHA 해시
SHA 해시(계속)
SHA 해시(계속)
SHA 해시(계속)
SHA 해시(계속)
SHA 해시(계속)
SHA 해시(계속)
SHA 해시(계속)
SHA 해시(계속)
파일 유형 ID
파일 이름
파일 유형 ID(계속)
문자열 블록 유형(0)
문자열 블록 유형(0)(계속)
문자열 블록 길이
문자열 블록 길이(계속)
파일 이름...
파일 크기
파일 크기(계속)
방향
애플리케이션 ID
애플리케이션 ID(계속)
사용자 ID



다음 표에는 파일 이벤트 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 B-43 파일 이벤트 데이터 블록 필드

필드	데이터 유형	설명
파일 이벤트 블록 유형	uint32	파일 이벤트 데이터 블록을 시작합니다. 이 값은 항상 43입니다.
파일 이벤트 블록 길이	uint32	파일 이벤트 블록의 총 바이트 수입니다. 여기에는 파일 이벤트 블록 유형 및 길이 필드의 8바이트에 그 뒤의 데이터 바이트 수를 더한 값이 포함됩니다.
디바이스 ID	uint32	이벤트를 생성한 디바이스의 ID입니다.
연결 인스턴스	uint16	이벤트를 생성한 디바이스의 Snort 인스턴스입니다. 이벤트를 연결 또는 침입 이벤트와 연결하는 데 사용됩니다.
연결 카운터	uint16	1초 이내에 발생하는 연결 이벤트를 구별하는 데 사용되는 값입니다.
연결 타임스탬프	uint32	관련 연결 이벤트의 UNIX 타임스탬프(1970년 1월 1일 이후의 초 단위 시간)입니다.
파일 이벤트 타임스탬프	uint32	파일 유형이 식별되고 파일 이벤트가 생성된 UNIX 타임스탬프(1970년 1월 1일 이후의 초 단위 시간)입니다.
소스 IP 주소	uint8[16]	연결 소스의 IPv4 또는 IPv6 주소입니다.
대상 IP 주소	uint8[16]	연결 대상의 IPv4 또는 IPv6 주소입니다.
상태	uint8	파일의 악성코드 상태입니다. 가능한 값은 다음과 같습니다. • 1 - CLEAN - 파일이 정상 상태이며 악성코드가 포함되어 있지 않습니다. • 2 - UNKNOWN - 파일에 악성코드가 포함되어 있는지 알 수 없습니다. • 3 - MALWARE - 파일에 악성코드가 포함되어 있습니다. • 4 - UNAVAILABLE - 소프트웨어가 Cisco 클라우드에 상태 요청을 보낼 수 없거나 Cisco 클라우드 서비스가 요청에 응답하지 않았습니다. • 5 - CUSTOM SIGNATURE - 파일이 사용자가 정의한 해시와 일치하며 사용자가 지정한 방식으로 처리됩니다.
SPERO 상태	uint8	파일 분석에 SPERO 서명이 사용되었는지를 나타냅니다. 값이 1, 2 또는 3이면 SPERO 분석이 사용된 것이고 그 외의 값이면 SPERO 분석이 사용되지 않은 것입니다.

표 B-43 파일 이벤트 데이터 블록 필드 (계속)

필드	데이터 유형	설명
파일 스토리지 상태	uint8	파일의 저장 상태입니다. 가능한 값은 다음과 같습니다. • 1 - 파일 저장됨 • 2 - 파일 저장됨 • 3 - 파일을 저장할 수 없음 • 4 - 파일을 저장할 수 없음 • 5 - 파일을 저장할 수 없음 • 6 - 파일을 저장할 수 없음 • 7 - 파일을 저장할 수 없음 • 8 - 파일 크기가 너무 큼 • 9 - 파일 크기가 너무 작음 • 10 - 파일을 저장할 수 없음 • 11 - 파일이 저장되지 않음(상태 사용 불가)

표 B-43 파일 이벤트 데이터 블록 필드 (계속)

필드	데이터 유형	설명
파일 분석 상태	uint8	동적 분석을 위해 파일이 제출되었는지 나타냅니다. 가능한 값은 다음과 같습니다. • 0 - 파일이 분석을 위해 전송되지 않음 • 1 - 분석을 위해 전송됨 • 2 - 분석을 위해 전송됨 • 4 - 분석을 위해 전송됨 • 5 - 전송하지 못함 • 6 - 전송하지 못함 • 7 - 전송하지 못함 • 8 - 전송하지 못함 • 9 - 파일 크기가 너무 작음 • 10 - 파일 크기가 너무 큼 • 11 - 분석을 위해 전송됨 • 12 - 분석 완료 • 13 - 장애(네트워크 문제) • 14 - 장애(속도 제한) • 15 - 장애(파일이 너무 큼) • 16 - 장애(파일 읽기 오류) • 17 - 장애(내부 라이브러리 오류) • 19 - 파일이 전송되지 않음(상태 사용 불가) • 20 - 장애(파일을 실행할 수 없음) • 21 - 장애(분석 시간 초과) • 22 - 분석을 위해 전송됨 • 23 - 파일이 지원되지 않음 • 23 - 파일 전송 파일 용량 처리됨 - 분석을 위해 샌드박스로 파일을 제출할 수 없어서 파일 용량이 처리됨(센서에 저장됨) • 25 - 파일 전송 서버 제한됨 초과 용량 처리됨 - 서버의 속도 제한으로 인해 파일 용량이 처리됨 • 26 - 통신 장애 - 클라우드 연결 장애로 인해 파일 용량이 처리됨 • 27 - 전송되지 않음 - 컨피그레이션으로 인해 파일이 전송되지 않음 • 28 - 사전 클래스 불일치 - 사전 분류에서 파일의 임베디드 개체 또는 의심스러운 개체를 찾지 못하여 동적 분석을 위해 파일이 전송되지 않음 • 29 - 전송 샌드박스 프라이빗 클라우드로 전송됨 - 파일이 동적 분석을 위해 프라이빗 클라우드로 전송됨 • 30 - 전송 샌드박스 프라이빗 클라우드로 전송되지 않음 - 파일이 분석을 위해 프라이빗 클라우드로 전송되지 않음

표 B-43 파일 이벤트 데이터 블록 필드 (계속)

필드	데이터 유형	설명
아카이브 파일 상태	uint8	항상 0입니다.
위협 점수	uint8	동적 분석 과정에서 관찰된 잠재적으로 악의적인 동작을 기준으로 한 0부터 100까지의 숫자 값입니다.
작업	uint8	파일 유형을 기반으로 파일에 조취를 취합니다. 다음과 같은 값을 사용할 수 있습니다. • 1 - 탐지 • 2 - 차단 • 3 - 악성코드 클라우드 조회 • 4 - 악성코드 차단 • 5 - 악성코드 화이트리스트 추가
SHA 해시	uint8[32]	이진 형식으로 된 파일의 SHA-256 해시입니다.
파일 유형 ID	uint32	파일 유형에 매핑되는 ID 번호입니다. 이 필드의 의미가 이 이벤트와 함께 메타데이터에 포함되어 전송됩니다. 자세한 정보는 AMP for Endpoints 파일 유형 메타데이터, 페이지 3-42의 내용을 참조하십시오.
파일 이름	string	파일의 이름입니다.
파일 크기	uint64	파일의 바이트 단위 크기입니다.
방향	uint8	파일이 업로드되었는지 아니면 다운로드되었는지를 나타내는 값입니다. 다음과 같은 값을 사용할 수 있습니다. • 1 - 다운로드 • 2 - 업로드 현재 이 값은 프로토콜에 따라 달라집니다(예: 연결이 HTTP인 경우 다운로드임).
애플리케이션 ID	uint32	파일 전송을 사용하여 애플리케이션에 매핑되는 ID 번호입니다.
사용자 ID	uint32	시스템이 식별한 대상 호스트에 로그인하는 사용자의 ID 번호입니다.
URI	string	연결의 URI(Uniform Resource Identifier)입니다.
서명	string	문자열 형식으로 된 파일의 SHA-256 해시입니다.
소스 포트	uint16	연결 소스의 포트 번호입니다.
대상 포트	uint16	연결 대상의 포트 번호입니다.
프로토콜	uint8	사용자가 지정한 IANA 프로토콜 번호입니다. 예를 들면 다음과 같습니다. • 1 - ICMP • 4 - IP • 6 - TCP • 17 - UDP 현재는 TCP만 설정 가능합니다.

표 B-43 파일 이벤트 데이터 블록 필드 (계속)

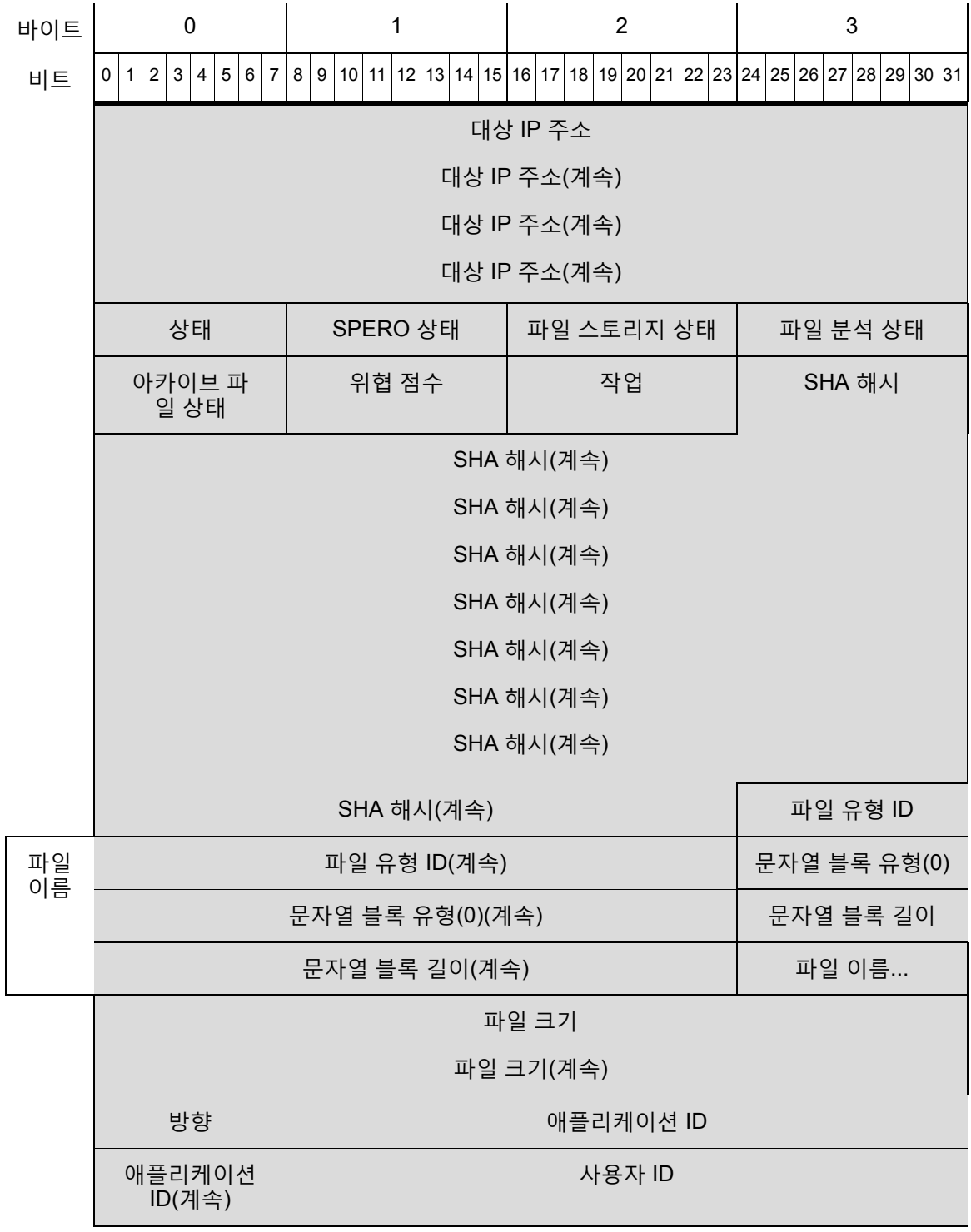
필드	데이터 유형	설명
액세스 제어 정책 UUID	uint8[16]	이벤트를 트리거한 액세스 제어 정책의 고유 식별자입니다.
소스 국가	uint16	소스 호스트의 국가 코드입니다.
대상 국가	uint16	대상 호스트의 국가 코드입니다.
웹 애플리케이션 ID	uint32	해당하는 경우 웹 애플리케이션의 내부 ID 번호입니다.
클라이언트 애플리케이션 ID	uint32	해당하는 경우 클라이언트 애플리케이션의 내부 ID 번호입니다.
보안 상황	uint8(16)	트래픽이 통과한 보안 상황(가상 방화벽)의 ID 번호입니다. 이 필드는 다중 컨텍스트 모드의 ASA FirePOWER 디바이스에 대해서만 채워집니다.

5.4.x 버전용 파일 이벤트

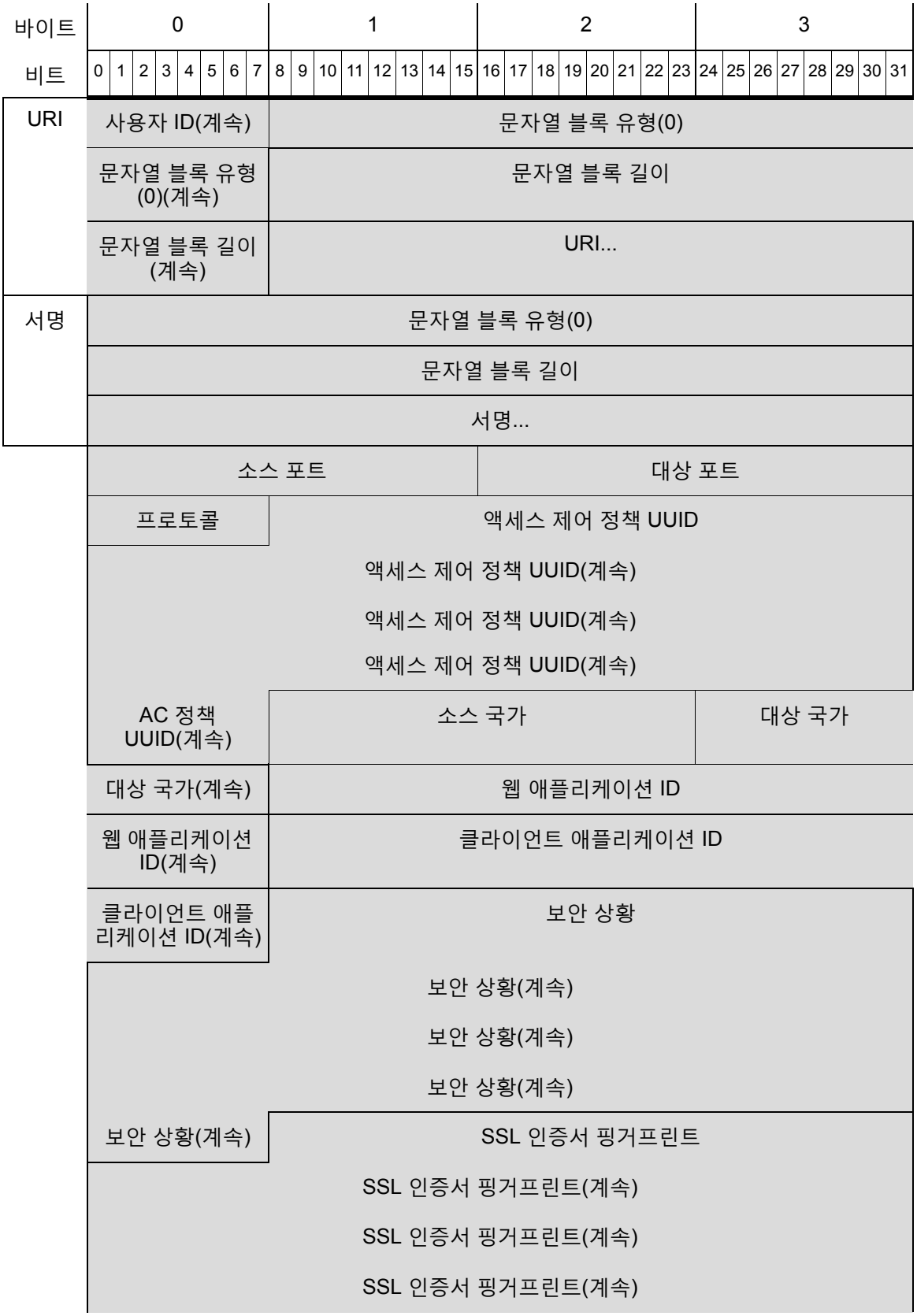
파일 이벤트는 네트워크를 통해 전송되는 파일에 대한 정보를 포함합니다. 이러한 정보로는 연결 정보, 파일이 악성코드인지 여부, 그리고 파일을 식별하는 특정 정보가 포함됩니다. 계열 2 블록 그룹에서 파일 이벤트의 블록 유형은 46입니다. 이는 블록 유형 43을 대체합니다. SSL 및 파일 아카이브 지원용 필드가 추가되었습니다.

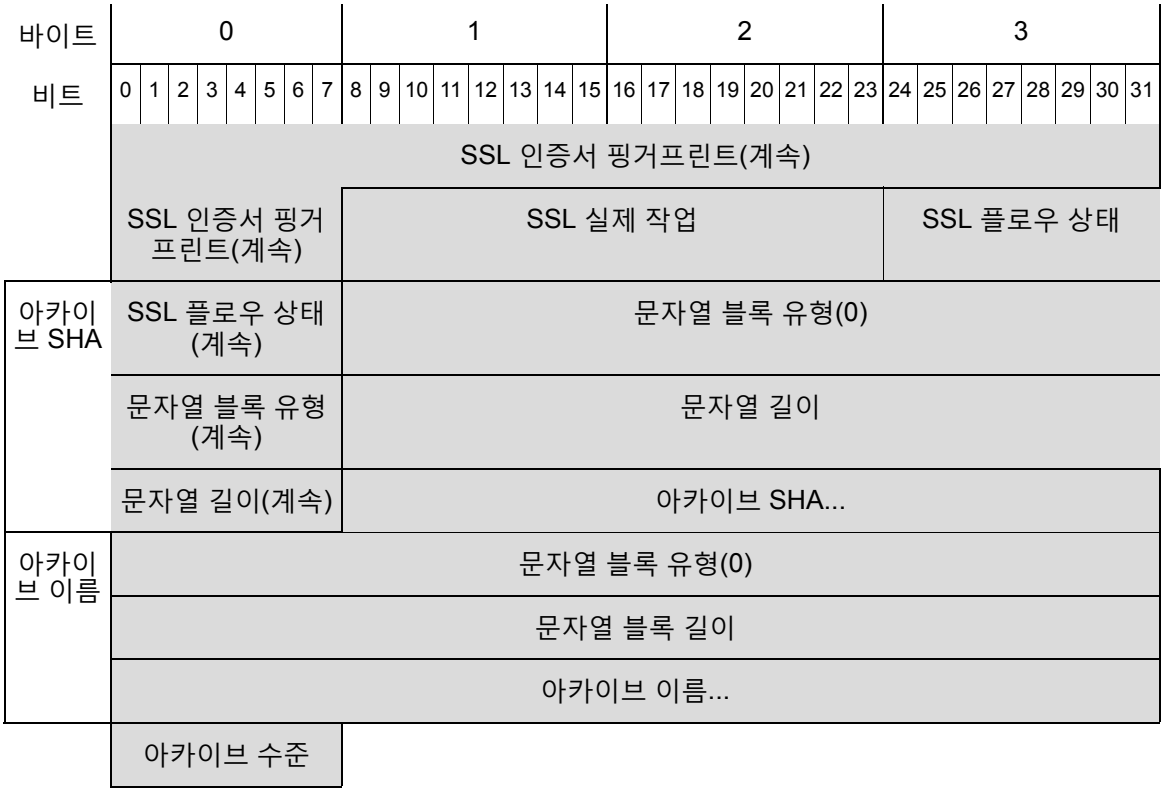
이벤트 버전이 5이고 이벤트 코드가 111인 요청 메시지에서 파일 이벤트 플래그(Request Flags(요청 플래그) 필드의 비트 30)를 설정하여 파일 이벤트 레코드를 요청합니다. 요청 플래그, 페이지 2-12의 내용을 참조하십시오. 비트 23을 활성화하면 레코드에 확장 이벤트 헤더가 포함됩니다.

다음 그림에 파일 이벤트 데이터 블록의 구조가 나와 있습니다.



바이트	0	1	2	3
비트	0 1 2 3 4 5 6 7	8 9 10 11 12 13 14 15	16 17 18 19 20 21 22 23	24 25 26 27 28 29 30 31
	대상 IP 주소			
	대상 IP 주소(계속)			
	대상 IP 주소(계속)			
	대상 IP 주소(계속)			
	상태	SPERO 상태	파일 스토리지 상태	파일 분석 상태
	아카이브 파일 상태	위협 점수	작업	SHA 해시
	SHA 해시(계속)			
	SHA 해시(계속)			
	SHA 해시(계속)			
	SHA 해시(계속)			
	SHA 해시(계속)			
	SHA 해시(계속)			
	SHA 해시(계속)			
	SHA 해시(계속)			파일 유형 ID
파일 이름	파일 유형 ID(계속)			문자열 블록 유형(0)
	문자열 블록 유형(0)(계속)			문자열 블록 길이
	문자열 블록 길이(계속)			파일 이름...
	파일 크기			
	파일 크기(계속)			
	방향	애플리케이션 ID		
	애플리케이션 ID(계속)	사용자 ID		


바이트
0
1
2
3
비트
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
URI
사용자 ID(계속)
문자열 블록 유형(0)
문자열 블록 유형(0)(계속)
문자열 블록 길이
문자열 블록 길이(계속)
URI...
서명
문자열 블록 유형(0)
문자열 블록 길이
서명...
소스 포트
대상 포트
프로토콜
액세스 제어 정책 UUID
액세스 제어 정책 UUID(계속)
액세스 제어 정책 UUID(계속)
액세스 제어 정책 UUID(계속)
AC 정책 UUID(계속)
소스 국가
대상 국가
대상 국가(계속)
웹 애플리케이션 ID
웹 애플리케이션 ID(계속)
클라이언트 애플리케이션 ID
클라이언트 애플리케이션 ID(계속)
보안 상황
보안 상황(계속)
보안 상황(계속)
보안 상황(계속)
보안 상황(계속)
SSL 인증서 핑거프린트
SSL 인증서 핑거프린트(계속)
SSL 인증서 핑거프린트(계속)
SSL 인증서 핑거프린트(계속)



다음 표에는 파일 이벤트 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 B-44 5.4.x 버전용 파일 이벤트 데이터 블록 필드

필드	데이터 유형	설명
파일 이벤트 블록 유형	uint32	파일 이벤트 데이터 블록을 시작합니다. 이 값은 항상 46입니다.
파일 이벤트 블록 길이	uint32	파일 이벤트 블록의 총 바이트 수입니다. 여기에는 파일 이벤트 블록 유형 및 길이 필드의 8바이트에 그 뒤의 데이터 바이트 수를 더한 값이 포함됩니다.
디바이스 ID	uint32	이벤트를 생성한 디바이스의 ID입니다.
연결 인스턴스	uint16	이벤트를 생성한 디바이스의 Snort 인스턴스입니다. 이벤트를 연결 또는 침입 이벤트와 연결하는 데 사용됩니다.
연결 카운터	uint16	1초 이내에 발생하는 연결 이벤트를 구별하는 데 사용되는 값입니다.
연결 타임스탬프	uint32	관련 연결 이벤트의 UNIX 타임스탬프(1970년 1월 1일 이후의 초 단위 시간)입니다.
파일 이벤트 타임스탬프	uint32	파일 유형이 식별되고 파일 이벤트가 생성된 UNIX 타임스탬프(1970년 1월 1일 이후의 초 단위 시간)입니다.
소스 IP 주소	uint8[16]	연결 소스의 IPv4 또는 IPv6 주소입니다.
대상 IP 주소	uint8[16]	연결 대상의 IPv4 또는 IPv6 주소입니다.

표 B-44 5.4.x 버전용 파일 이벤트 데이터 블록 필드 (계속)

필드	데이터 유형	설명
상태	uint8	파일의 악성코드 상태입니다. 가능한 값은 다음과 같습니다. • 1 - CLEAN - 파일이 정상 상태이며 악성코드가 포함되어 있지 않습니다. • 2 - UNKNOWN - 파일에 악성코드가 포함되어 있는지 알 수 없습니다. • 3 - MALWARE - 파일에 악성코드가 포함되어 있습니다. • 4 - UNAVAILABLE - 소프트웨어가 Cisco 클라우드에 상태 요청을 보낼 수 없거나 Cisco 클라우드 서비스가 요청에 응답하지 않았습니다. • 5 - CUSTOM SIGNATURE - 파일이 사용자가 정의한 해시와 일치하며 사용자가 지정한 방식으로 처리됩니다.
SPERO 상태	uint8	파일 분석에 SPERO 서명이 사용되었는지를 나타냅니다. 값이 1, 2 또는 3이면 SPERO 분석이 사용된 것이고 그 외의 값이면 SPERO 분석이 사용되지 않은 것입니다.
파일 스토리지 상태	uint8	파일의 저장 상태입니다. 가능한 값은 다음과 같습니다. • 1 - 파일 저장됨 • 2 - 파일 저장됨 • 3 - 파일을 저장할 수 없음 • 4 - 파일을 저장할 수 없음 • 5 - 파일을 저장할 수 없음 • 6 - 파일을 저장할 수 없음 • 7 - 파일을 저장할 수 없음 • 8 - 파일 크기가 너무 큼 • 9 - 파일 크기가 너무 작음 • 10 - 파일을 저장할 수 없음 • 11 - 파일이 저장되지 않음(상태 사용 불가)

표 B-44 5.4.x 버전용 파일 이벤트 데이터 블록 필드 (계속)

필드	데이터 유형	설명
파일 분석 상태	uint8	동적 분석을 위해 파일이 제출되었는지 나타냅니다. 가능한 값은 다음과 같습니다. • 0 - 파일이 분석을 위해 전송되지 않음 • 1 - 분석을 위해 전송됨 • 2 - 분석을 위해 전송됨 • 4 - 분석을 위해 전송됨 • 5 - 전송하지 못함 • 6 - 전송하지 못함 • 7 - 전송하지 못함 • 8 - 전송하지 못함 • 9 - 파일 크기가 너무 작음 • 10 - 파일 크기가 너무 큼 • 11 - 분석을 위해 전송됨 • 12 - 분석 완료 • 13 - 장애(네트워크 문제) • 14 - 장애(속도 제한) • 15 - 장애(파일이 너무 큼) • 16 - 장애(파일 읽기 오류) • 17 - 장애(내부 라이브러리 오류) • 19 - 파일이 전송되지 않음(상태 사용 불가) • 20 - 장애(파일을 실행할 수 없음) • 21 - 장애(분석 시간 초과) • 22 - 분석을 위해 전송됨 • 23 - 파일이 지원되지 않음

표 B-44 5.4.x 버전용 파일 이벤트 데이터 블록 필드 (계속)

필드	데이터 유형	설명
아카이브 파일 상태	uint8	검사 중인 아카이브의 상태입니다. 다음과 같은 값을 사용할 수 있습니다. • 0 - N/A - 파일을 아카이브로 검사하고 있지 않음 • 1 - 보류 중 - 아카이브를 검사하는 중 • 2 - 추출됨 - 문제없이 검사함 • 3 - 장애 발생함 - 시스템 자원이 부족하여 검사하지 못함 • 4 - 수준 초과됨 - 검사는 성공했으나 아카이브에서 중첩 검사 수준이 초과됨 • 5 - 암호화됨 - 검사가 일부분 성공함(아카이브가 암호화된 아카이브이거나 암호화된 아카이브를 포함함) • 6 - 검사 불가 - 검사가 일부분 성공함(파일이 손상되었거나 형식이 잘못되었을 수 있음)
위협 점수	uint8	동적 분석 과정에서 관찰된 잠재적으로 악의적인 동작을 기준으로 한 0부터 100까지의 숫자 값입니다.
작업	uint8	파일 유형을 기반으로 파일에 조취를 취합니다. 다음과 같은 값을 사용할 수 있습니다. • 1 - 탐지 • 2 - 차단 • 3 - 악성코드 클라우드 조회 • 4 - 악성코드 차단 • 5 - 악성코드 화이트리스트 추가 • 6 - 클라우드 조회 시간 초과 • 7 - 맞춤형 탐지 • 8 - 맞춤형 탐지 차단 • 9 - 아카이브 차단(수준 초과됨) • 10 - 아카이브 차단(암호화됨) • 11 - 아카이브 차단(검사하지 못함)
SHA 해시	uint8[32]	이진 형식으로 된 파일의 SHA-256 해시입니다.
파일 유형 ID	uint32	파일 유형에 매핑되는 ID 번호입니다. 이 필드의 의미가 이 이벤트와 함께 메타데이터에 포함되어 전송됩니다. 자세한 정보는 AMP for Endpoints 파일 유형 메타데이터, 페이지 3-42의 내용을 참조하십시오.
파일 이름	string	파일의 이름입니다.
파일 크기	uint64	파일의 바이트 단위 크기입니다.

표 B-44 5.4.x 버전용 파일 이벤트 데이터 블록 필드 (계속)

필드	데이터 유형	설명
방향	uint8	파일이 업로드되었는지 아니면 다운로드되었는지를 나타내는 값입니다. 다음과 같은 값을 사용할 수 있습니다. • 1 - 다운로드 • 2 - 업로드 현재 이 값은 프로토콜에 따라 달라집니다(예: 연결이 HTTP인 경우 다운로드임).
애플리케이션 ID	uint32	파일 전송을 사용하여 애플리케이션에 매핑되는 ID 번호입니다.
사용자 ID	uint32	시스템이 식별한 대상 호스트에 로그인하는 사용자의 ID 번호입니다.
URI	string	연결의 URI(Uniform Resource Identifier)입니다.
서명	string	문자열 형식으로 된 파일의 SHA-256 해시입니다.
소스 포트	uint16	연결 소스의 포트 번호입니다.
대상 포트	uint16	연결 대상의 포트 번호입니다.
프로토콜	uint8	사용자가 지정한 IANA 프로토콜 번호입니다. 예를 들면 다음과 같습니다. • 1 - ICMP • 4 - IP • 6 - TCP • 17 - UDP 현재는 TCP만 설정 가능합니다.
액세스 제어 정책 UUID	uint8[16]	이벤트를 트리거한 액세스 제어 정책의 고유 식별자입니다.
소스 국가	uint16	소스 호스트의 국가 코드입니다.
대상 국가	uint16	대상 호스트의 국가 코드입니다.
웹 애플리케이션 ID	uint32	해당하는 경우 웹 애플리케이션의 내부 ID 번호입니다.
클라이언트 애플리케이션 ID	uint32	해당하는 경우 클라이언트 애플리케이션의 내부 ID 번호입니다.
보안 상황	uint8(16)	트래픽이 통과한 보안 상황(가상 방화벽)의 ID 번호입니다. 이 필드는 다중 컨텍스트 모드의 ASA FirePOWER 디바이스에 대해서만 채워집니다.
SSL 인증서 핑거프린트	uint8[20]	SSL 서버 인증서의 SHA1 해시입니다.

표 B-44 5.4.x 버전용 파일 이벤트 데이터 블록 필드 (계속)

필드	데이터 유형	설명
SSL 실제 작업	uint16	SSL 규칙에 기반한 연결에서 수행된 작업입니다. 규칙에 명시된 작업이 가능하지 않을 수도 있으므로, 이는 예상 작업과 다를 수 있습니다. 가능한 값은 다음과 같습니다. • 0 - '알 수 없음' • 1 - '암호 해독 안 함' • 2 - '차단' • 3 - '차단 및 재설정' • 4 - '암호 해독(알려진 키)' • 5 - '암호 해독(키 교체)' • 6 - '암호 해독(재서명)'

표 B-44 5.4.x 버전용 파일 이벤트 데이터 블록 필드 (계속)

필드	데이터 유형	설명
SSL 플로우 상태	uint16	SSL 플로우의 상태입니다. 이 값은 작업을 수행한 이유 또는 오류 메시지가 표시된 이유를 설명합니다. 가능한 값은 다음과 같습니다. • 0 - '알 수 없음' • 1 - '일치하지 않음' • 2 - '성공' • 3 - '캐시되지 않은 세션' • 4 - '알 수 없는 암호 그룹' • 5 - '지원되지 않는 암호 그룹' • 6 - '지원되지 않는 SSL 버전' • 7 - 'SSL 압축 사용됨' • 8 - '패시브 모드에서 세션 암호 해독 불가' • 9 - '핸드셰이크 오류' • 10 - '암호 해독 오류' • 11 - '서버 이름 카테고리 조회 보류 중' • 12 - '공용 이름 카테고리 조회 보류 중' • 13 - '내부 오류' • 14 - '네트워크 파라미터 사용 불가' • 15 - '유효하지 않은 서버 인증서 핸들' • 16 - '서버 인증서 핑거프린트 사용 불가' • 17 - '주체 DN을 캐시할 수 없음' • 18 - '발급자 DN을 캐시할 수 없음' • 19 - '알 수 없는 SSL 버전' • 20 - '외부 인증서 목록 사용 불가' • 21 - '외부 인증서 핑거프린트 사용 불가' • 22 - '내부 인증서 목록이 유효하지 않음' • 23 - '내부 인증서 목록 사용 불가' • 24 - '내부 인증서 사용 불가' • 25 - '내부 인증서 핑거프린트 사용 불가' • 26 - '서버 인증서 검증 사용 불가' • 27 - '서버 인증서 검증 장애' • 28 - '유효하지 않은 작업'
문자열 블록 유형	uint32	아카이브 SHA가 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	아카이브 SHA 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 침입 정책 이름의 바이트 수를 더한 값이 포함됩니다.

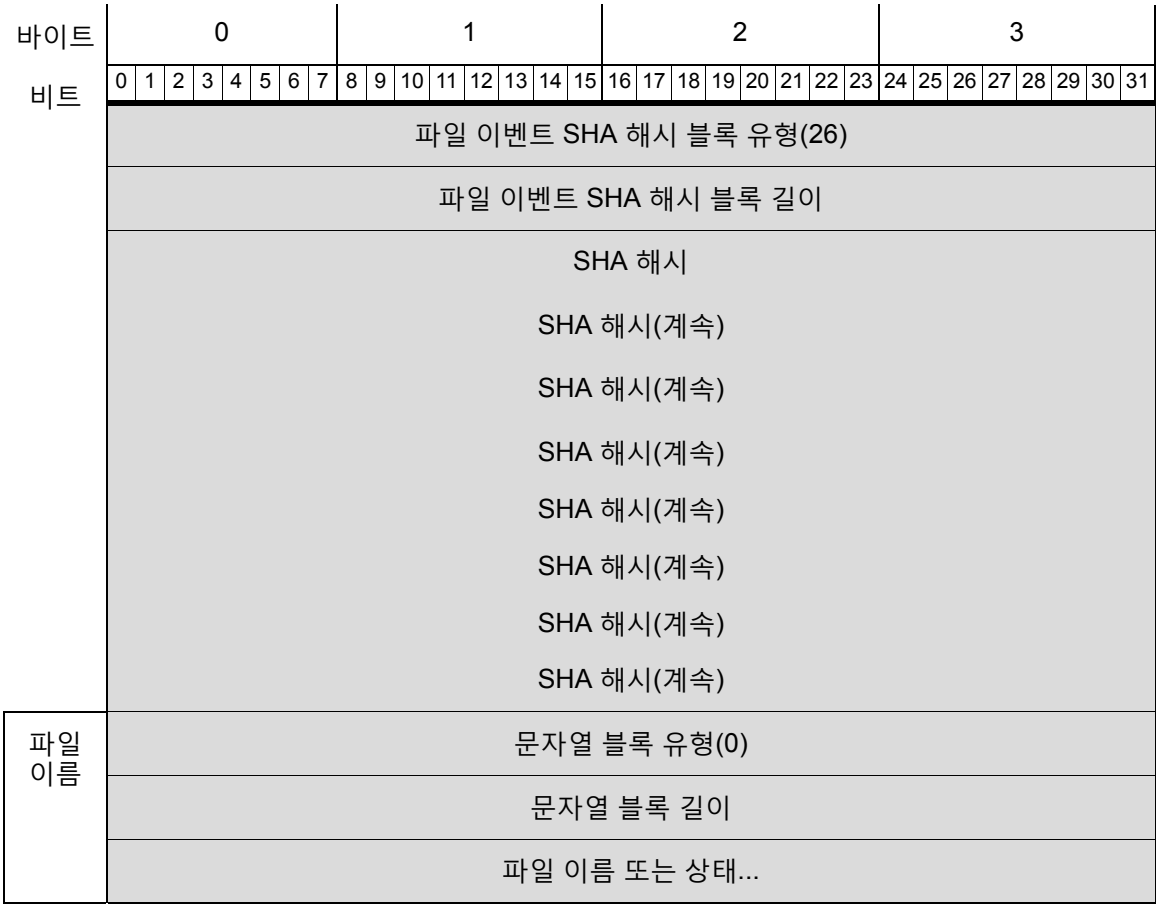
표 B-44 5.4.x 버전용 파일 이벤트 데이터 블록 필드 (계속)

필드	데이터 유형	설명
아카이브 SHA	string	파일이 포함된 상위 아카이브의 SHA1 해시입니다.
문자열 블록 유형	uint32	아카이브 이름이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	아카이브 이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 침입 정책 이름의 바이트 수를 더한 값이 포함됩니다.
아카이브 이름	string	상위 아카이브의 이름입니다.
아카이브 수준	uint8	파일이 중첩된 계층의 수입니다. 예를 들어 텍스트 파일이 zip 아카이브에 들어 있는 경우 이 항목의 값은 1입니다.

5.1.1~5.2.x 버전용 파일 이벤트 SHA 해시

eStreamer 서비스는 파일 이벤트 SHA 해시 데이터 블록을 사용하여 파일 SHA 해시의 매핑 메타데이터를 파일 이름에 포함합니다. 계열 2 데이터 블록 목록에서 이 블록의 블록 유형은 26입니다. 확장 요청(이벤트 코드 111)에서 파일 로그 이벤트를 요청했으며 비트 20을 설정하거나 이벤트 버전이 4이고 이벤트 코드가 21인 메타데이터를 요청하는 경우 이 블록 유형을 요청할 수 있습니다.

다음 다이어그램에 파일 이벤트 해시 데이터 블록의 구조가 나와 있습니다.



다음 표에는 파일 이벤트 SHA 해시 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 B-45 5.1.1~5.2.x 버전용 파일 이벤트 SHA 해시 데이터 블록 필드

필드	데이터 유형	설명
파일 이벤트 SHA 해시 블록 유형	uint32	파일 이벤트 SHA 해시 블록을 시작합니다. 이 값은 항상 26입니다.
파일 이벤트 SHA 해시 블록 길이	uint32	파일 이벤트 SHA 해시 블록의 총 바이트 수입니다. 여기에는 파일 이벤트 SHA 해시 블록 유형 및 길이 필드의 8바이트에 그 뒤의 데이터 바이트 수를 더한 값이 포함됩니다.
SHA 해시	uint8[32]	이진 형식으로 된 파일의 SHA-256 해시입니다.
문자열 블록 유형	uint32	파일과 관련된 설명 이름을 포함하는 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Name(이름) 필드의 바이트 수를 더한 값이 포함됩니다.
파일 이름 또는 상태	string	파일을 설명하는 이름 또는 상태입니다. 파일이 정상 상태이면 이 값은 Clean입니다. 파일 상태를 알 수 없는 경우 이 값은 Neutral입니다. 파일에 악성코드가 포함되어 있으면 파일 이름이 지정됩니다.

레거시 상관관계 이벤트 데이터 구조

다음 항목에서는 기타 레거시 상관관계(컴플라이언스) 데이터 구조에 대해 설명합니다.

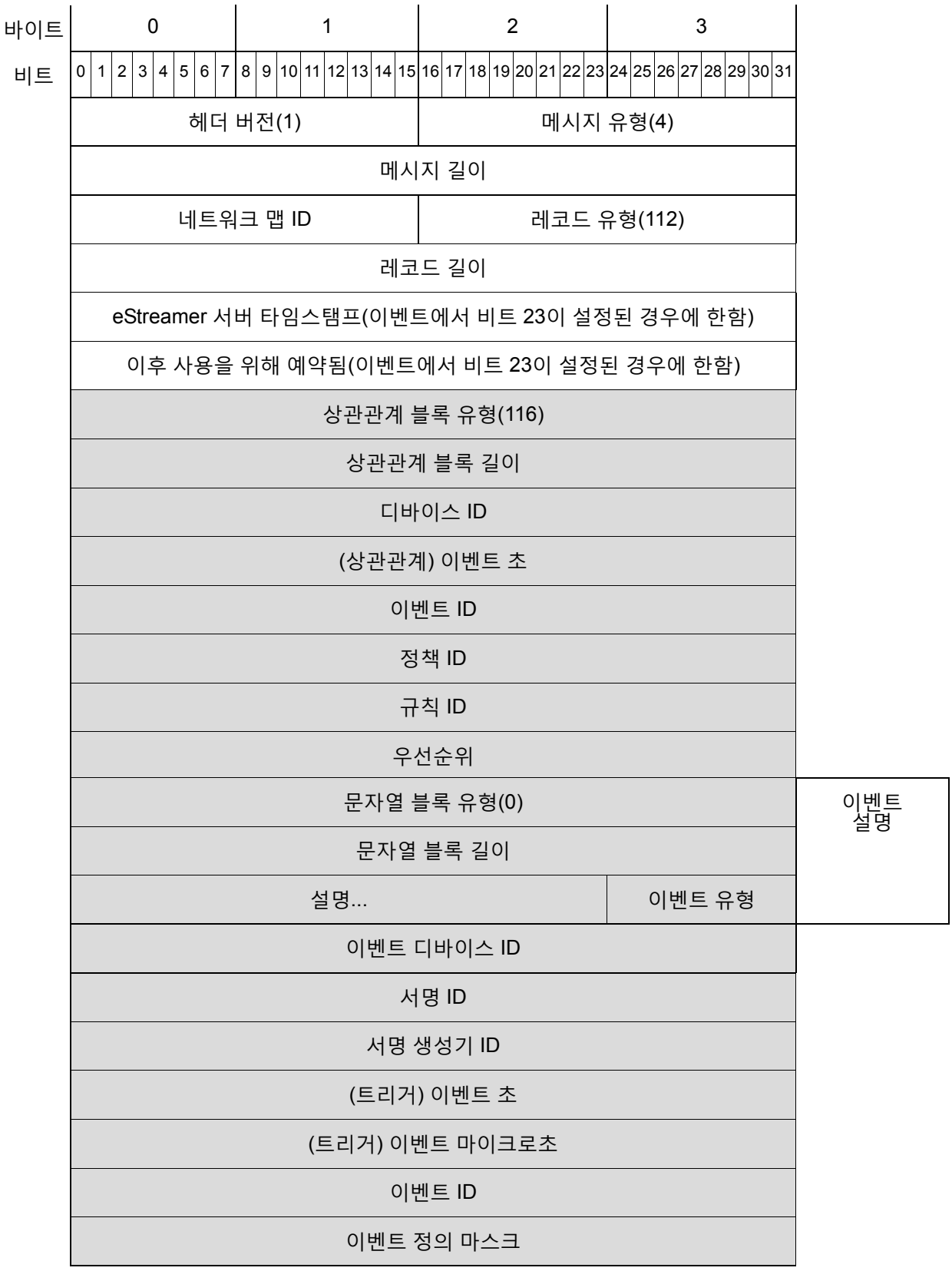
- 5.0~5.0.2 버전용 상관관계 이벤트, 페이지 B-258
- 5.1~5.3.x 버전용 상관관계 이벤트, 페이지 B-266

5.0~5.0.2 버전용 상관관계 이벤트

5.0 이전 버전에서는 명칭이 컴플라이언스 이벤트였던 상관관계 이벤트는 상관관계 정책 위반에 대한 정보를 포함합니다. 이 메시지는 표준 eStreamer 메시지 헤더를 사용하며 레코드 유형 112와 상관관계 데이터 블록 유형 116을 차례로 지정합니다. 데이터 블록 유형 116과 이전 버전인 블록 유형 107의 차이점은, 유형 116의 경우 관련된 보안 영역과 인터페이스에 대한 추가 정보를 포함한다는 것입니다.

5.0 상관관계 이벤트는 eStreamer에서 확장 요청을 통해서만 요청할 수 있습니다. 이렇게 하려면 스트림 요청 메시지에서 이벤트 유형 코드 31, 버전 코드 7을 요청합니다. 확장 요청 제출에 대한 자세한 정보는 확장 요청 제출, 페이지 2-4의 내용을 참조하십시오. 필요한 경우 초기 이벤트 스트림 요청 메시지의 플래그 필드에서 비트 23을 활성화하여 확장 이벤트 헤더를 포함할 수 있습니다. 플래그 필드에서 비트 20을 활성화하여 사용자 메타데이터를 포함할 수도 있습니다.

레코드 구조에는 계열 1 블록인 문자열 블록 유형이 포함됩니다. 계열 1 블록에 대한 자세한 정보는 검색(계열 1) 블록 이해, 페이지 4-63의 내용을 참조하십시오.


바이트
0
1
2
3
비트
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
헤더 버전(1)
메시지 유형(4)
메시지 길이
네트워크 맵 ID
레코드 유형(112)
레코드 길이
eStreamer 서버 타임스탬프(이벤트에서 비트 23이 설정된 경우에 한함)
이후 사용을 위해 예약됨(이벤트에서 비트 23이 설정된 경우에 한함)
상관관계 블록 유형(116)
상관관계 블록 길이
디바이스 ID
(상관관계) 이벤트 초
이벤트 ID
정책 ID
규칙 ID
우선순위
문자열 블록 유형(0)
문자열 블록 길이
설명...
이벤트 유형
이벤트 디바이스 ID
서명 ID
서명 생성기 ID
(트리거) 이벤트 초
(트리거) 이벤트 마이크로초
이벤트 ID
이벤트 정의 마스크
이벤트 설명


바이트
0
1
2
3
비트
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
이벤트 영향 플래그
IP 프로토콜
네트워크 프로토콜
소스 IP
소스 호스트 유형
소스 VLAN ID
소스 OS 핑거프린트 UUID
소스 OS 핑거프린트 UUID
소스 OS 핑거프린트 UUID(계속)
소스 OS 핑거프린트 UUID(계속)
소스 OS 핑거프린트 UUID(계속)
소스 OS 핑거프린트 UUID(계속)
소스 임계성
소스 임계성(계속)
소스 사용자 ID
소스 사용자 ID(계속)
소스 포트
소스 서버 ID
소스 서버 ID(계속)
대상 IP
대상 IP(계속)
대상 호스트 유형
대상 VLAN ID
대상 OS 핑거프린트 UUID
대상 OS 핑거프린트 UUID
대상 OS 핑거프린트 UUID(계속)
대상 OS 핑거프린트 UUID(계속)
대상 OS 핑거프린트 UUID(계속)
대상 OS 핑거프린트 UUID(계속)
대상 임계성
대상 사용자 ID
대상 포트
대상 서버 ID
대상 서버 ID(계속)
차단됨
인그레스 인터페이스 UUID
인그레스 인터페이스 UUID(계속)
인그레스 인터페이스 UUID(계속)
인그레스 인터페이스 UUID(계속)

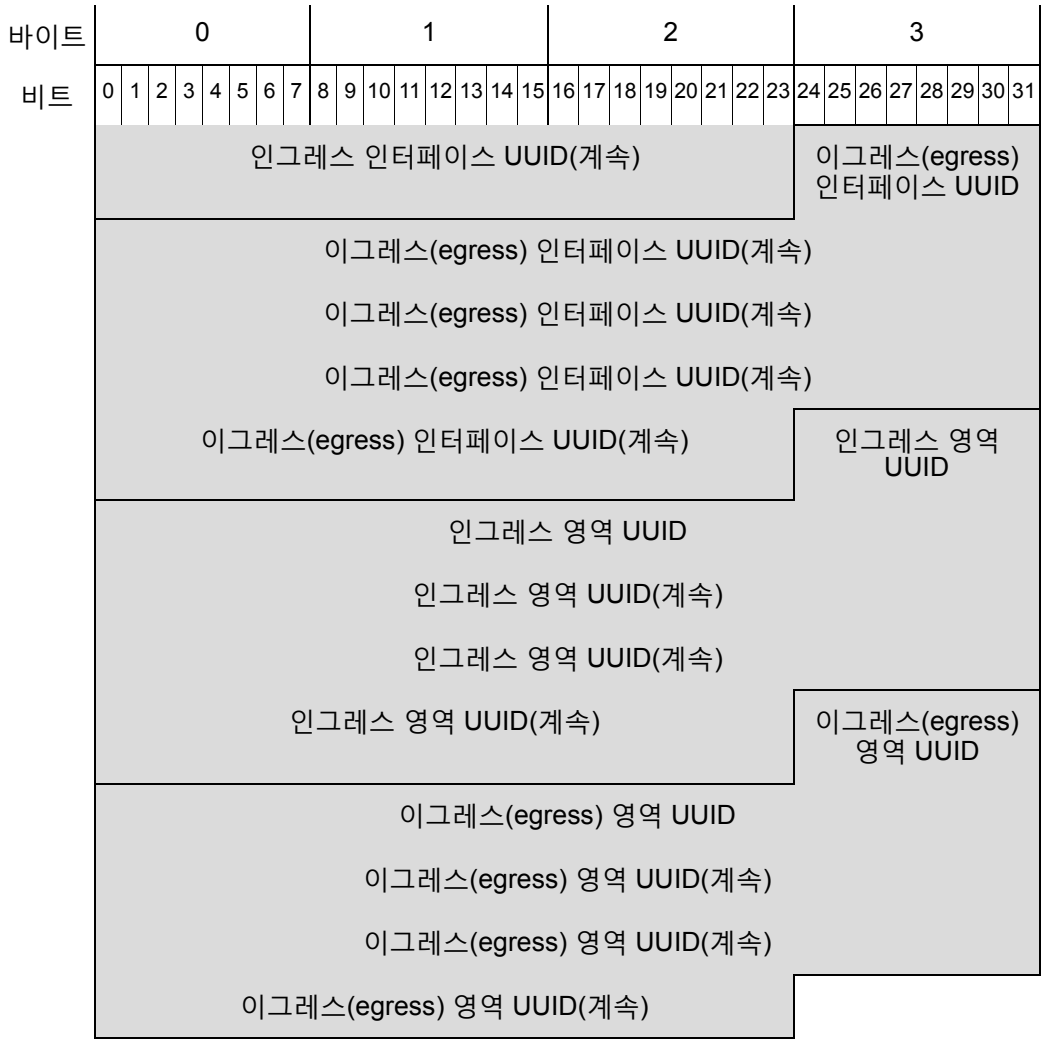


표 B-46 5.0~5.0.2 버전용 상관관계 이벤트 데이터 필드

필드	데이터 유형	설명
상관관계 블록 유형	uint32	상관관계 이벤트 데이터 블록이 뒤에 옴을 나타냅니다. 이 필드의 값은 항상 107입니다. 검색(계열 1) 블록 이해, 페이지 4-63의 내용을 참조하십시오.
상관관계 블록 길이	uint32	상관관계 데이터 블록의 길이입니다. 여기에는 상관관계 블록 유형의 8바이트에 그 뒤의 상관관계 데이터를 더한 값이 포함됩니다.
디바이스 ID	uint32	상관관계 이벤트를 생성한 매니지드 디바이스 또는 방어 센터의 내부 ID 번호입니다. 값 0은 방어 센터를 나타냅니다. 버전 3 메타데이터를 요청하면 매니지드 디바이스 이름을 가져올 수 있습니다. 자세한 정보는 매니지드 디바이스 레코드 메타데이터, 페이지 3-35의 내용을 참조하십시오.
(상관관계) 이벤트 초	uint32	상관관계 이벤트가 생성된 시간을 나타내는 UNIX 타임스탬프입니다(1970년 1월 1일 이후의 초 단위 시간).
이벤트 ID	uint32	상관관계 이벤트 ID 번호입니다.

표 B-46 5.0~5.0.2 버전용 상관관계 이벤트 데이터 필드 (계속)

필드	데이터 유형	설명
정책 ID	uint32	위반된 상관관계 정책의 ID 번호입니다 데이터베이스에서 정책 ID 번호를 가져오는 방법에 대한 자세한 정보는 서비스 레코드, 페이지 4-15의 내용을 참조하십시오.
규칙 ID	uint32	정책을 위반하는 방식으로 트리거된 상관관계 규칙의 ID 번호입니다. 데이터베이스에서 정책 ID 번호를 가져오는 방법에 대한 자세한 정보는 서비스 레코드, 페이지 4-15의 내용을 참조하십시오.
우선순위	uint32	이벤트에 할당된 우선순위입니다. 0에서 5 사이의 정숫값입니다.
문자열 블록 유형	uint32	상관관계 위반 이벤트 설명이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0으로 설정됩니다. 문자열 블록에 대한 자세한 정보는 문자열 데이터 블록, 페이지 4-72의 내용을 참조하십시오.
문자열 블록 길이	uint32	이벤트 설명 문자열 블록의 바이트 수입니다. 여기에는 문자열 블록 유형의 4바이트 + 문자열 블록 길이의 4바이트 + 설명의 바이트 수가 포함됩니다.
설명	string	상관관계 이벤트의 설명입니다.
이벤트 유형	uint8	상관관계 이벤트가 트리거된 원인(침입, 호스트 검색 또는 사용자 이벤트)을 나타냅니다. • 1 - 침입 • 2 - 호스트 검색 • 3 - 사용자
이벤트 디바이스 ID	uint32	상관관계 이벤트를 트리거한 이벤트가 생성된 디바이스의 ID 번호입니다. 버전 3 메타데이터를 요청하면 디바이스 이름을 가져올 수 있습니다. 자세한 정보는 매니지드 디바이스 레코드 메타데이터, 페이지 3-35의 내용을 참조하십시오.
서명 ID	uint32	이벤트가 침입 이벤트였던 경우 이벤트에 해당하는 규칙 ID 번호를 나타냅니다. 그렇지 않은 경우 값은 0입니다.
서명 생성기 ID	uint32	이벤트가 침입 이벤트였던 경우 해당 이벤트를 생성한 Firepower System 전처리기 또는 규칙 엔진의 ID 번호를 나타냅니다.
(트리거) 이벤트 초	uint32	상관관계 정책 규칙을 트리거한 이벤트의 시간을 나타내는 UNIX 타임스탬프입니다(1970년 1월 1일 이후의 초 단위 시간).
(트리거) 이벤트 마이크로초	uint32	이벤트가 탐지된 마이크로초(100만분의 1초) 단위의 증분 시간입니다.
이벤트 ID	uint32	디바이스에서 생성된 이벤트의 ID 번호입니다.
이벤트 정의 마스크	bits[32]	이 필드에 설정된 비트는 메시지에서 해당 필드 다음에 오는 필드 중 유효한 필드를 나타냅니다. 각 비트 값의 목록은 표 B-47(B-265 페이지)의 내용을 참조하십시오.

표 B-46 5.0~5.0.2 버전용 상관관계 이벤트 데이터 필드 (계속)

필드	데이터 유형	설명
이벤트 영향 플래그	bits[8]	이벤트의 영향 플래그 값입니다. 하위 8비트가 영향 레벨을 나타냅니다. 값은 다음과 같습니다. • 0x01(비트 0) - 소스 또는 대상 호스트가 시스템에서 모니터링하는 네트워크에 있습니다. • 0x02(비트 1) - 소스 또는 대상 호스트가 네트워크 맵에 있습니다. • 0x04(비트 2) - 소스 또는 대상 호스트가 이벤트의 포트에서 서버를 실행 중이거나(TCP 또는 UDP인 경우) IP 프로토콜을 사용합니다. • 0X08(비트 3) - 이벤트의 소스 또는 대상 호스트 운영 체제에 매핑된 취약점이 있습니다. • 0x10(비트 4) - 이벤트에서 탐지된 서버에 매핑된 취약점이 있습니다. • 0x20(비트 5) - 이벤트로 인해 매니지드 디바이스에서 세션이 삭제되었습니다(디바이스가 인라인, 스위치드 또는 라우티드 구축에서 실행 중인 경우에만 사용됨). Firepower System 웹 인터페이스의 차단 상태에 해당합니다. • 0x40(비트 6) - 이 이벤트를 생성한 규칙에 영향 플래그를 빨간색(비트 6)으로 설정하는 규칙 메타데이터가 있습니다. 소스 또는 대상 호스트가 바이러스, 트로이 목마, 기타 악성 소프트웨어에 감염되었을 가능성이 있습니다. • 0x80(비트 7) - 이벤트에서 탐지된 클라이언트에 매핑된 취약점이 있습니다. 다음 영향 레벨 값은 방어 센터의 특정 우선순위에 매핑됩니다. x는 값이 0 또는 1일 수 있음을 나타냅니다. • (0, 알 수 없음): 00X00000 • 빨간색(1, 취약함): XXXX1XXX, XXX1XXXX, X1XXXXXX, 1XXXXXXX • 주황색(2, 잠재적으로 취약함): 00X00111 • 노란색(3, 현재 취약하지 않음): 00X00011 • 파란색(4, 알 수 없는 대상): 00X00001
IP 프로토콜	uint8	해당하는 경우 이벤트와 관련된 IP 프로토콜의 식별자입니다.
네트워크 프로토콜	uint16	해당하는 경우 이벤트와 관련된 네트워크 프로토콜입니다.
소스 IP	uint8[4]	이벤트의 소스 호스트 IP 주소(IP 주소 옥텟 형식)입니다.
소스 호스트 유형	uint8	소스 호스트의 유형입니다. • 0 - 호스트 • 1 - 라우터 • 2 - 브리지
소스 VLAN ID	uint16	해당하는 경우 소스 호스트의 VLAN ID 번호입니다.

표 B-46 5.0~5.0.2 버전용 상관관계 이벤트 데이터 필드 (계속)

필드	데이터 유형	설명
소스 OS 핑거프린트 UUID	uint8[16]	소스 호스트 운영 체제의 고유 식별자 역할을 하는 핑거프린트 ID 번호입니다. 핑거프린트 ID에 매핑되는 값을 가져오는 방법에 대한 자세한 정보는 서비스 레코드, 페이지 4-15의 내용을 참조하십시오.
소스 임계성	uint16	소스 호스트의 사용자 정의 임계성 값입니다. • 0 - 없음 • 1 - 낮음 • 2 - 보통 • 3 - 높음
소스 사용자 ID	uint32	시스템이 식별한 소스 호스트에 로그인하는 사용자의 ID 번호입니다.
소스 포트	uint16	이벤트의 소스 포트입니다.
소스 서버 ID	uint32	소스 호스트에서 실행 중인 서버의 ID 번호입니다.
대상 IP 주소	uint8[4]	해당하는 경우 정책 위반과 관련된 대상 호스트의 IP 주소입니다. 대상 IP 주소가 없는 경우 이 값은 0입니다.
대상 호스트 유형	uint8	대상 호스트의 유형입니다. • 0 - 호스트 • 1 - 라우터 • 2 - 브리지
대상 VLAN ID	uint16	해당하는 경우 대상 호스트의 VLAN ID 번호입니다.
대상 OS 핑거프린트 UUID	uint8[16]	대상 호스트 운영 체제의 고유 식별자 역할을 하는 핑거프린트 ID 번호입니다. 핑거프린트 ID에 매핑되는 값을 가져오는 방법에 대한 자세한 정보는 서비스 레코드, 페이지 4-15의 내용을 참조하십시오.
대상 임계성	uint16	대상 호스트의 사용자 정의 임계성 값입니다. • 0 - 없음 • 1 - 낮음 • 2 - 보통 • 3 - 높음
대상 사용자 ID	uint32	시스템이 식별한 대상 호스트에 로그인하는 사용자의 ID 번호입니다.
대상 포트	uint16	이벤트의 대상 포트입니다.
대상 서비스 ID	uint32	소스 호스트에서 실행 중인 서버의 ID 번호입니다.

표 B-46 5.0~5.0.2 버전용 상관관계 이벤트 데이터 필드 (계속)

필드	데이터 유형	설명
차단됨	uint8	침입 이벤트를 트리거한 패킷에 발생한 상황을 나타내는 값입니다. • 0 - 침입 이벤트가 삭제되지 않음 • 1 - 침입 이벤트가 삭제됨(인라인/스위치드/라우티드 구축인 경우 삭제됨) • 2 - 이벤트를 트리거한 패킷이 삭제되었을 수 있음(침입 정책이 인라인, 스위치드 또는 라우티드 구축의 디바이스에 적용된 경우)
인그레스 인터페이스 UUID	uint8[16]	상관관계 이벤트와 관련된 인그레스 인터페이스의 고유 식별자 역할을 하는 인터페이스 ID입니다.
이그레스 (egress) 인터페이스 UUID	uint8[16]	상관관계 이벤트와 관련된 이그레스(egress) 인터페이스의 고유 식별자 역할을 하는 인터페이스 ID입니다.
인그레스 영역 UUID	uint8[16]	상관관계 이벤트와 관련된 인그레스 보안 영역의 고유 식별자 역할을 하는 영역 ID입니다.
이그레스 (egress) 영역 UUID	uint8[16]	상관관계 이벤트와 관련된 이그레스(egress) 보안 영역의 고유 식별자 역할을 하는 영역 ID입니다.

다음 표에는 각 이벤트 정의 마스크 값에 대한 설명이 나와 있습니다.

표 B-47 이벤트 정의 값

설명	마스크 값
Event Impact Flags(이벤트 영향 플래그)	0x00000001
IP Protocol(IP 프로토콜)	0x00000002
Network Protocol(네트워크 프로토콜)	0x00000004
Source IP(소스 IP)	0x00000008
Source Host Type(소스 호스트 유형)	0x00000010
Source VLAN ID(소스 VLAN ID)	0x00000020
Source Fingerprint ID(소스 지문 ID)	0x00000040
Source Criticality(소스 심각도)	0x00000080
Source Port(소스 포트)	0x00000100
Source Server(소스 서버)	0x00000200
Destination IP(목적지 IP)	0x00000400

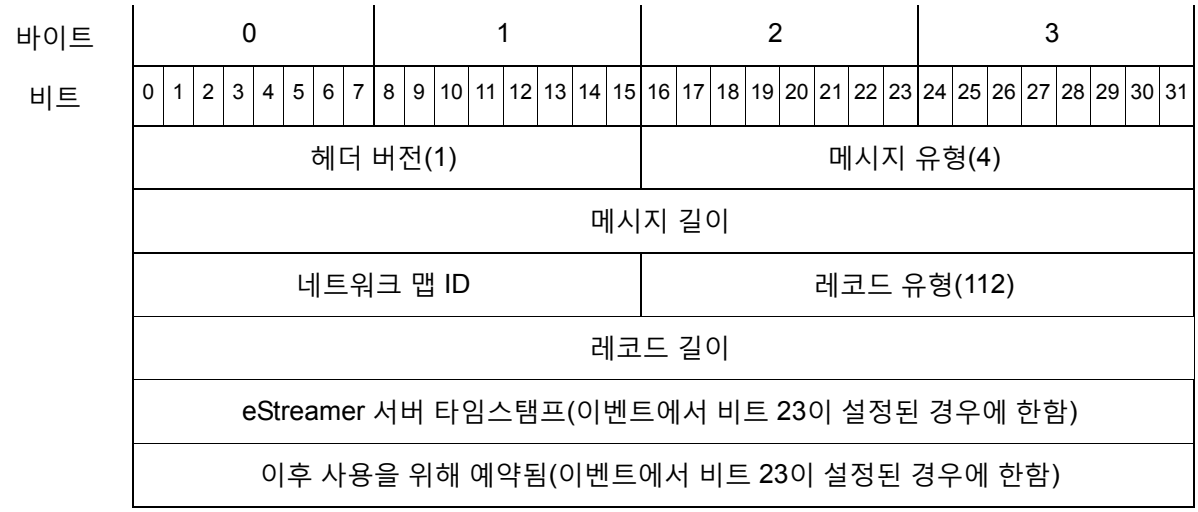
표 B-47 이벤트 정의 값 (계속)

설명	마스크 값
Destination Host Type(목적지 호스트 유형)	0x00000800
Destination VLAN ID(목적지 VLAN ID)	0x00001000
Destination Fingerprint ID(목적지 지문 ID)	0x00002000
Destination Criticality(목적지 심각도)	0x00004000
Destination Port(목적지 포트)	0x00008000
Destination Server(목적지 서버)	0x00010000
Source User(소스 사용자)	0x00020000
Destination User(목적지 사용자)	0x00040000

5.1~5.3.x 버전용 상관관계 이벤트

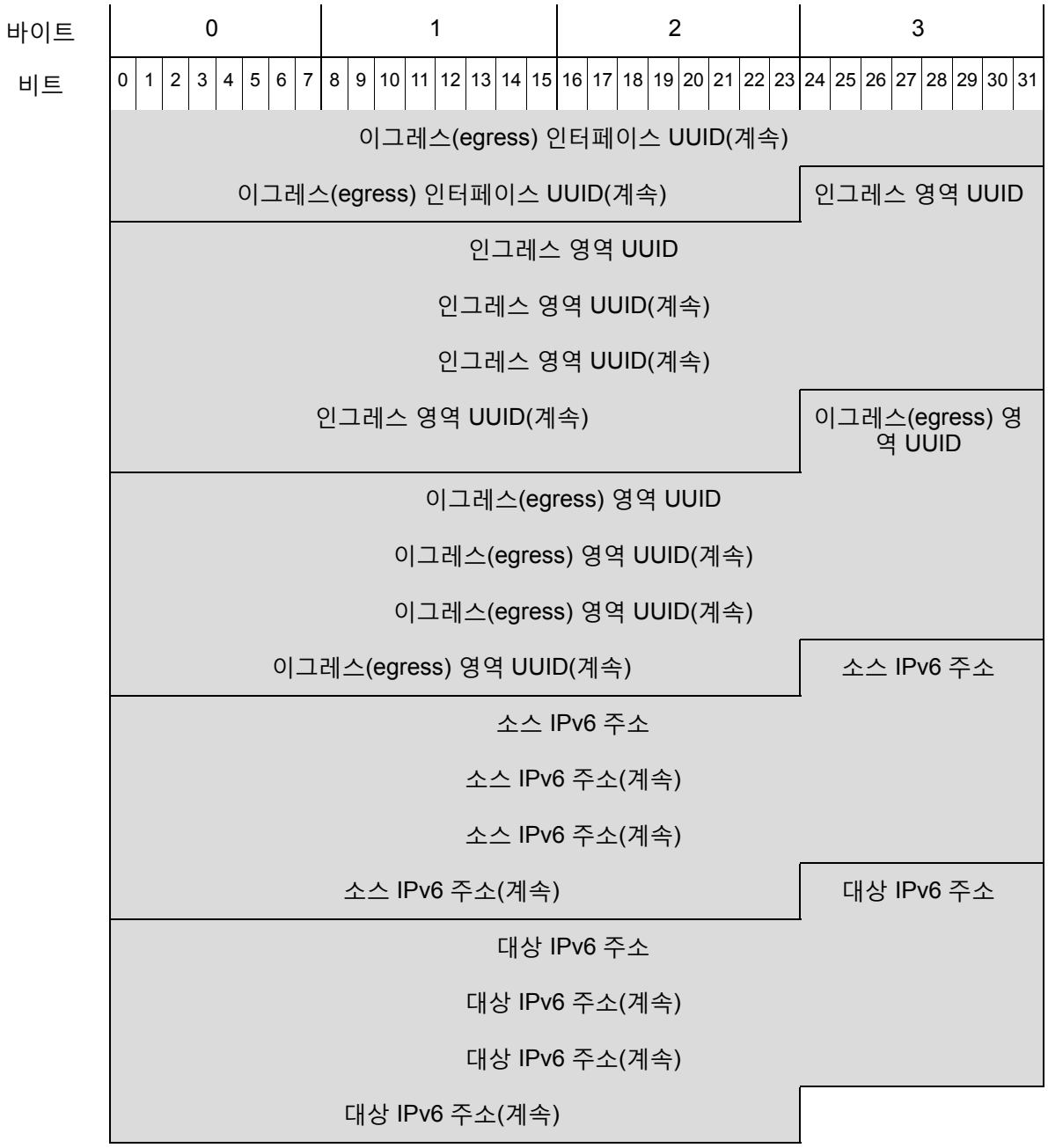
5.0 이전 버전에서는 명칭이 컴플라이언스 이벤트였던 상관관계 이벤트는 상관관계 정책 위반에 대한 정보를 포함합니다. 이 메시지는 표준 eStreamer 메시지 헤더를 사용하며 레코드 유형 112와 계열 1 데이터 블록 집합의 상관관계 데이터 블록 유형 128을 차례로 지정합니다. 데이터 블록 유형 128과 이전 버전인 블록 유형 116의 차이점은, 유형 128의 경우 IPv6 지원을 포함한다는 것입니다.

5.1~5.3.x 상관관계 이벤트는 eStreamer에서 확장 요청을 통해서만 요청할 수 있습니다. 이렇게 하려면 스트림 요청 메시지에서 이벤트 유형 코드 31, 버전 코드 8을 요청합니다. 확장 요청 제출에 대한 자세한 정보는 확장 요청 제출, 페이지 2-4의 내용을 참조하십시오. 필요한 경우 초기 이벤트 스트림 요청 메시지의 플래그 필드에서 비트 23을 활성화하여 확장 이벤트 헤더를 포함할 수 있습니다. 플래그 필드에서 비트 20을 활성화하여 사용자 메타데이터를 포함할 수도 있습니다.




바이트
0
1
2
3
비트
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
상관관계 블록 유형(128)
상관관계 블록 길이
디바이스 ID
(상관관계) 이벤트 초
이벤트 ID
정책 ID
규칙 ID
우선순위
문자열 블록 유형(0)
문자열 블록 길이
설명...
이벤트 유형
이벤트 설명
이벤트 디바이스 ID
서명 ID
서명 생성기 ID
(트리거) 이벤트 초
(트리거) 이벤트 마이크로초
이벤트 ID
이벤트 정의 마스크
이벤트 영향 플래그
IP 프로토콜
네트워크 프로토콜
소스 IP


바이트
0
1
2
3
비트
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
소스 호스트 유형
소스 VLAN ID
소스 OS 핑거프린트 UUID
소스 OS 핑거프린트 UUID
소스 OS 핑거프린트 UUID(계속)
소스 OS 핑거프린트 UUID(계속)
소스 OS 핑거프린트 UUID(계속)
소스 OS 핑거프린트 UUID(계속)
소스 임계성
소스 임계성(계속)
소스 사용자 ID
소스 사용자 ID(계속)
소스 포트
소스 서버 ID
소스 서버 ID(계속)
대상 IP
대상 IP(계속)
대상 호스트 유형
대상 VLAN ID
대상 OS 핑거프린트 UUID
대상 OS 핑거프린트 UUID
대상 OS 핑거프린트 UUID(계속)
대상 OS 핑거프린트 UUID(계속)
대상 OS 핑거프린트 UUID(계속)
대상 OS 핑거프린트 UUID(계속)
대상 임계성
대상 사용자 ID
대상 포트
대상 서버 ID
대상 서버 ID(계속)
차단됨
인그레스 인터페이스 UUID
인그레스 인터페이스 UUID(계속)
인그레스 인터페이스 UUID(계속)
인그레스 인터페이스 UUID(계속)
인그레스 인터페이스 UUID(계속)
이그레스(egress) 인터페이스 UUID
이그레스(egress) 인터페이스 UUID(계속)
이그레스(egress) 인터페이스 UUID(계속)



레코드 구조에는 계열 1 블록인 문자열 블록 유형이 포함됩니다. 계열 1 블록에 대한 자세한 정보는 검색(계열 1) 블록 이해, 페이지 4-63의 내용을 참조하십시오.

표 B-48 5.1~5.3.x 버전용 상관관계 이벤트 데이터 필드

필드	데이터 유형	설명
상관관계 블록 유형	uint32	상관관계 이벤트 데이터 블록이 뒤에 옴을 나타냅니다. 이 필드의 값은 항상 128입니다. 검색(계열 1) 블록 이해, 페이지 4-63의 내용을 참조하십시오.
상관관계 블록 길이	uint32	상관관계 데이터 블록의 길이입니다. 여기에는 상관관계 블록 유형의 8바이트에 그 뒤의 상관관계 데이터를 더한 값이 포함됩니다.
디바이스 ID	uint32	상관관계 이벤트를 생성한 매니지드 디바이스 또는 방어 센터의 내부 ID 번호입니다. 값 0은 방어 센터를 나타냅니다. 버전 3 메타데이터를 요청하면 매니지드 디바이스 이름을 가져올 수 있습니다. 자세한 정보는 매니지드 디바이스 레코드 메타데이터, 페이지 3-35의 내용을 참조하십시오.
(상관관계) 이벤트 초	uint32	상관관계 이벤트가 생성된 시간을 나타내는 UNIX 타임스탬프입니다(1970년 1월 1일 이후의 초 단위 시간).
이벤트 ID	uint32	상관관계 이벤트 ID 번호입니다.
정책 ID	uint32	위반된 상관관계 정책의 ID 번호입니다 데이터베이스에서 정책 ID 번호를 가져오는 방법에 대한 자세한 정보는 서비스 레코드, 페이지 4-15의 내용을 참조하십시오.
규칙 ID	uint32	정책을 위반하는 방식으로 트리거된 상관관계 규칙의 ID 번호입니다. 데이터베이스에서 정책 ID 번호를 가져오는 방법에 대한 자세한 정보는 서비스 레코드, 페이지 4-15의 내용을 참조하십시오.
우선순위	uint32	이벤트에 할당된 우선순위입니다. 0에서 5 사이의 정숫값입니다.
문자열 블록 유형	uint32	상관관계 위반 이벤트 설명이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0으로 설정됩니다. 문자열 블록에 대한 자세한 정보는 문자열 데이터 블록, 페이지 4-72의 내용을 참조하십시오.
문자열 블록 길이	uint32	이벤트 설명 문자열 블록의 바이트 수입니다. 여기에는 문자열 블록 유형의 4바이트 + 문자열 블록 길이의 4바이트 + 설명의 바이트 수가 포함됩니다.
설명	string	상관관계 이벤트의 설명입니다.
이벤트 유형	uint8	상관관계 이벤트가 트리거된 원인(침입, 호스트 검색 또는 사용자 이벤트)을 나타냅니다. • 1 - 침입 • 2 - 호스트 검색 • 3 - 사용자
이벤트 디바이스 ID	uint32	상관관계 이벤트를 트리거한 이벤트가 생성된 디바이스의 ID 번호입니다. 버전 3 메타데이터를 요청하면 디바이스 이름을 가져올 수 있습니다. 자세한 정보는 매니지드 디바이스 레코드 메타데이터, 페이지 3-35의 내용을 참조하십시오.
서명 ID	uint32	이벤트가 침입 이벤트였던 경우 이벤트에 해당하는 규칙 ID 번호를 나타냅니다. 그렇지 않은 경우 값은 0입니다.
서명 생성기 ID	uint32	이벤트가 침입 이벤트였던 경우 해당 이벤트를 생성한 Firepower System 전처리기 또는 규칙 엔진의 ID 번호를 나타냅니다.

표 B-48 5.1~5.3.x 버전용 상관관계 이벤트 데이터 필드 (계속)

필드	데이터 유형	설명
(트리거) 이벤트 초	uint32	상관관계 정책 규칙을 트리거한 이벤트의 시간을 나타내는 UNIX 타임스탬프입니다(1970년 1월 1일 이후의 초 단위 시간).
(트리거) 이벤트 마이크로초	uint32	이벤트가 탐지된 마이크로초(100만분의 1초) 단위의 증분 시간입니다.
이벤트 ID	uint32	Cisco 디바이스에서 생성된 이벤트의 ID 번호입니다.
이벤트 정의 마스크	bits[32]	이 필드에 설정된 비트는 메시지에서 해당 필드 다음에 오는 필드 중 유효한 필드를 나타냅니다. 각 비트 값의 목록은 표 B-47(B-265페이지)의 내용을 참조하십시오.
이벤트 영향 플래그	bits[8]	이벤트의 영향 플래그 값입니다. 하위 8비트가 영향 레벨을 나타냅니다. 값은 다음과 같습니다. • 0x01(비트 0) - 소스 또는 대상 호스트가 시스템에서 모니터링하는 네트워크에 있습니다. • 0x02(비트 1) - 소스 또는 대상 호스트가 네트워크 맵에 있습니다. • 0x04(비트 2) - 소스 또는 대상 호스트가 이벤트의 포트에서 서버를 실행 중이거나(TCP 또는 UDP인 경우) IP 프로토콜을 사용합니다. • 0x08(비트 3) - 이벤트의 소스 또는 대상 호스트 운영 체제에 매핑된 취약점이 있습니다. • 0x10(비트 4) - 이벤트에서 탐지된 서버에 매핑된 취약점이 있습니다. • 0x20(비트 5) - 이벤트로 인해 매니지드 디바이스에서 세션이 삭제되었습니다(디바이스가 인라인, 스위치드 또는 라우티드 구축에서 실행 중인 경우에만 사용됨). Firepower System 웹 인터페이스의 차단 상태에 해당합니다. • 0x40(비트 6) - 이 이벤트를 생성한 규칙에 영향 플래그를 빨간색으로 설정하는 규칙 메타데이터가 있습니다. 소스 또는 대상 호스트가 바이러스, 트로이 목마, 기타 악성 소프트웨어에 감염되었을 가능성이 있습니다. • 0x80(비트 7) - 이벤트에서 탐지된 클라이언트에 매핑된 취약점이 있습니다. (5.0 이상 버전만 해당) 다음 영향 레벨 값은 방어 센터의 특정 우선순위에 매핑됩니다. x는 값이 0 또는 1일 수 있음을 나타냅니다. • (0, 알 수 없음): 00X00000 • 빨간색(1, 취약함): XXXX1XXX, XXX1XXXX, X1XXXXXX, 1XXXXXXX (5.0 이상 버전만 해당) • 주황색(2, 잠재적으로 취약함): 00X0011X • 노란색(3, 현재 취약하지 않음): 00X0001X • 파란색(4, 알 수 없는 대상): 00X00001

표 B-48 5.1~5.3.x 버전용 상관관계 이벤트 데이터 필드 (계속)

필드	데이터 유형	설명
IP 프로토콜	uint8	해당하는 경우 이벤트와 관련된 IP 프로토콜의 식별자입니다.
네트워크 프로토콜	uint16	해당하는 경우 이벤트와 관련된 네트워크 프로토콜입니다.
소스 IP 주소	uint8[4]	이 필드는 예약되지만 더 이상 내용이 입력되지는 않습니다. 소스 IPv4 주소는 Source IPv6 Address(소스 IPv6 주소) 필드에 저장됩니다. 자세한 정보는 IP 주소, 페이지 1-5의 내용을 참조하십시오.
소스 호스트 유형	uint8	소스 호스트의 유형입니다. • 0 - 호스트 • 1 - 라우터 • 2 - 브리지
소스 VLAN ID	uint16	해당하는 경우 소스 호스트의 VLAN ID 번호입니다.
소스 OS 핑거프린트 UUID	uint8[16]	소스 호스트 운영 체제의 고유 식별자 역할을 하는 핑거프린트 ID 번호입니다. 핑거프린트 ID에 매핑되는 값을 가져오는 방법에 대한 자세한 정보는 서비스 레코드, 페이지 4-15의 내용을 참조하십시오.
소스 임계성	uint16	소스 호스트의 사용자 정의 임계성 값입니다. • 0 - 없음 • 1 - 낮음 • 2 - 보통 • 3 - 높음
소스 사용자 ID	uint32	시스템이 식별한 소스 호스트에 로그인하는 사용자의 ID 번호입니다.
소스 포트	uint16	이벤트의 소스 포트입니다.
소스 서버 ID	uint32	소스 호스트에서 실행 중인 서버의 ID 번호입니다.
대상 IP 주소	uint8[4]	이 필드는 예약되지만 더 이상 내용이 입력되지는 않습니다. 대상 IPv4 주소는 Destination IPv6 Address(대상 IPv6 주소) 필드에 저장됩니다. 자세한 정보는 IP 주소, 페이지 1-5의 내용을 참조하십시오.
대상 호스트 유형	uint8	대상 호스트의 유형입니다. • 0 - 호스트 • 1 - 라우터 • 2 - 브리지

표 B-48 5.1~5.3.x 버전용 상관관계 이벤트 데이터 필드 (계속)

필드	데이터 유형	설명
대상 VLAN ID	uint16	해당하는 경우 대상 호스트의 VLAN ID 번호입니다.
대상 OS 핑거프린트 UUID	uint8[16]	대상 호스트 운영 체제의 고유 식별자 역할을 하는 핑거프린트 ID 번호입니다. 핑거프린트 ID에 매핑되는 값을 가져오는 방법에 대한 자세한 정보는 서비스 레코드, 페이지 4-15의 내용을 참조하십시오.
대상 임계성	uint16	대상 호스트의 사용자 정의 임계성 값입니다. • 0 - 없음 • 1 - 낮음 • 2 - 보통 • 3 - 높음
대상 사용자 ID	uint32	시스템이 식별한 대상 호스트에 로그인하는 사용자의 ID 번호입니다.
대상 포트	uint16	이벤트의 대상 포트입니다.
대상 서비스 ID	uint32	소스 호스트에서 실행 중인 서버의 ID 번호입니다.
차단됨	uint8	침입 이벤트를 트리거한 패킷에 발생한 상황을 나타내는 값입니다. • 0 - 침입 이벤트가 삭제되지 않음 • 1 - 침입 이벤트가 삭제됨(인라인/스위치드/라우티드 구축인 경우 삭제됨) • 2 - 이벤트를 트리거한 패킷이 삭제되었을 수 있음(침입 정책이 인라인, 스위치드 또는 라우티드 구축의 디바이스에 적용된 경우)
인그레스 인터페이스 UUID	uint8[16]	상관관계 이벤트와 관련된 인그레스 인터페이스의 고유 식별자 역할을 하는 인터페이스 ID입니다.
이그레스(egress) 인터페이스 UUID	uint8[16]	상관관계 이벤트와 관련된 이그레스(egress) 인터페이스의 고유 식별자 역할을 하는 인터페이스 ID입니다.
인그레스 영역 UUID	uint8[16]	상관관계 이벤트와 관련된 인그레스 보안 영역의 고유 식별자 역할을 하는 영역 ID입니다.
이그레스(egress) 영역 UUID	uint8[16]	상관관계 이벤트와 관련된 이그레스(egress) 보안 영역의 고유 식별자 역할을 하는 영역 ID입니다.
소스 IPv6 주소	uint8[16]	이벤트의 소스 호스트 IP 주소(IPv6 주소 옥텟 형식)입니다.
대상 IPv6 주소	uint8[16]	이벤트의 대상 호스트 IP 주소(IPv6 주소 옥텟 형식)입니다.

레거시 호스트 데이터 구조

이러한 구조를 요청하려면 호스트 요청 메시지를 사용해야 합니다. 레거시 구조를 요청하려는 경우 호스트 요청 메시지에서 이전 형식을 사용해야 합니다. 자세한 정보는 호스트 요청 메시지 형식, 페이지 2-26의 내용을 참조하십시오.

다음 항목에서는 호스트 프로파일 및 전체 호스트 프로파일 구조를 비롯한 레거시 호스트 데이터 구조에 대해 설명합니다.

5.0~5.0.2 버전용 전체 호스트 프로파일 데이터 블록

5.0~5.0.2 버전용 전체 호스트 프로파일 데이터 블록에는 호스트 하나를 설명하는 전체 데이터 집합이 포함됩니다. 이 블록은 아래 그림에 나와 있는 형식으로 되어 있습니다. 해당 형식에 대한 설명은 다음 표에 나와 있습니다. 목록 데이터 블록을 제외하고는 캡슐화된 데이터 블록의 필드는 그림에 나와 있지 않습니다. 이러한 캡슐화된 데이터 블록에 대해서는 검색 및 연결 데이터 구조 이해, 페이지 4-1에서 별도로 설명합니다. 전체 호스트 프로파일 데이터 블록의 블록 유형 값은 111입니다.

참고 다음 다이어그램에서 블록 이름 옆에 있는 별표(*)는 데이터 블록 인스턴스가 여러 개 나올 수 있음을 나타냅니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
파생된 OS 핑거프린트	일반 목록 블록 길이(계속)								운영 체제 핑거프린트 블록 유형(130)*																							
	OS 핑거프린트 블록 유형(130)*(계속)								운영 체제 핑거프린트 블록 길이																							
	OS 핑거프린트 블록 길이(계속)								운영 체제 파생 핑거프린트 데이터...																							
	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
서버 핑거프린트	운영 체제 핑거프린트 블록 유형(130)*																															
	운영 체제 핑거프린트 블록 길이																															
	운영 체제 서버 핑거프린트 데이터...																															
	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
클라이언트 핑거프린트	운영 체제 핑거프린트 블록 유형(130)*																															
	운영 체제 핑거프린트 블록 길이																															
	운영 체제 클라이언트 핑거프린트 데이터...																															
	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
VDB 네이티브 핑거프린트 1	운영 체제 핑거프린트 블록 유형(130)*																															
	운영 체제 핑거프린트 블록 길이																															
	운영 체제 VDB 핑거프린트 데이터...																															
	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
VDB 네이티브 핑거프린트 2	운영 체제 핑거프린트 블록 유형(130)*																															
	운영 체제 핑거프린트 블록 길이																															
	운영 체제 VDB 핑거프린트 데이터...																															

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
사용자 핑거프린트	운영 체제 핑거프린트 블록 유형(130)*																															
	운영 체제 핑거프린트 블록 길이																															
	운영 체제 사용자 핑거프린트 데이터...																															
	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
스캔 핑거프린트	운영 체제 핑거프린트 블록 유형(130)*																															
	운영 체제 핑거프린트 블록 길이																															
	운영 체제 스캔 핑거프린트 데이터...																															
	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
애플리케이션 핑거프린트	운영 체제 핑거프린트 블록 유형(130)*																															
	운영 체제 핑거프린트 블록 길이																															
	운영 체제 애플리케이션 핑거프린트 데이터...																															
	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
충돌 핑거프린트	운영 체제 핑거프린트 블록 유형(130)*																															
	운영 체제 핑거프린트 블록 길이																															
	운영 체제 충돌 핑거프린트 데이터...																															
(TCP) 전체 서버 데이터	목록 블록 유형(11)...																															
	목록 블록 길이...																															
	(TCP) 전체 서버 데이터 블록(104)*																															

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
(UDP) 전체 서버 데이터	목록 블록 유형(11)																															
	목록 블록 길이																															
	(UDP) 전체 서버 데이터 블록(104)*																															
네트워크 프로토콜 데이터	목록 블록 유형(11)																															
	목록 블록 길이																															
	(네트워크) 프로토콜 데이터 블록(4)*																															
전송 프로토콜 데이터	목록 블록 유형(11)																															
	목록 블록 길이																															
	(전송) 프로토콜 데이터 블록(4)*																															
MAC 주소 데이터	목록 블록 유형(11)																															
	목록 블록 길이																															
	호스트 MAC 주소 데이터 블록(95)*																															
	마지막 확인																															
	호스트 유형																															
	비즈니스 임계성																VLAN ID															
	VLAN 유형								VLAN 우선순위								일반 목록 블록 유형(31)															
호스트 클라이언트 데이터	일반 목록 블록 유형(계속)																일반 목록 블록 길이															
	일반 목록 블록 길이(계속)																전체 호스트 클라이언트 애플리케이션 데이터 블록(112)*															
NetBIOS 이름	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	NetBIOS 이름 문자열...																															
메모 데이터	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	메모 문자열...																															

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
(VDB) 호스트 취약점	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
	(VDB) 호스트 취약점 데이터 블록(85)*																															
서드파티/VDB 호스트 취약점	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
	(서드파티/VDB) 호스트 취약점 데이터 블록(85)*																															
서드파티 스캔 호스트 취약점	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
	(서드파티 스캔) 원래 취약점 ID가 포함된 호스트 취약점 데이터 블록(85)*																															
속성 값 데이터	목록 블록 유형(11)																															
	목록 블록 길이																															
	속성값 데이터 블록*																															

다음 표에는 5.0~5.0.2 버전용 전체 호스트 프로파일 레코드의 구성 요소에 대한 설명이 나와 있습니다.

표 B-49 5.0~5.0.2 버전용 전체 호스트 프로파일 레코드 필드

필드	데이터 유형	설명
IP 주소	uint8[4]	호스트의 IP 주소(IP 주소 옥텟 형식)입니다.
홉	uint8	호스트에서 디바이스로의 네트워크 홉 수입니다.
일반 목록 블록 유형	uint32	기존 핑거프린트에서 호스트에 대해 파생된 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
운영 체제 파생 핑거프린트 데이터 블록*	variable	기존 핑거프린트에서 호스트에 대해 파생된 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 페이지 4-161의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	서버 핑거프린트를 사용하여 식별된 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.

표 B-49 5.0~5.0.2 버전용 전체 호스트 프로파일 레코드 필드 (계속)

필드	데이터 유형	설명
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
운영 체제 핑거프린트(서버 핑거프린트) 데이터 블록*	variable	서버 핑거프린트를 사용하여 식별된 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 페이지 4-161의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	클라이언트 핑거프린트를 사용하여 식별된 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
운영 체제 핑거프린트(클라이언트 핑거프린트) 데이터 블록*	variable	클라이언트 핑거프린트를 사용하여 식별된 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 페이지 4-161의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	Cisco VDB 핑거프린트를 사용하여 식별된 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
운영 체제 핑거프린트(VDB 네이티브 핑거프린트 1) 데이터 블록*	variable	Cisco VDB(취약점 데이터베이스)의 핑거프린트를 사용하여 식별된 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 페이지 4-161의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	Cisco VDB 핑거프린트를 사용하여 식별된 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
운영 체제 핑거프린트(VDB 네이티브 핑거프린트 2) 데이터 블록*	variable	Cisco VDB(취약점 데이터베이스)의 핑거프린트를 사용하여 식별된 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 페이지 4-161의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	사용자가 추가한 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
운영 체제 핑거프린트(사용자 핑거프린트) 데이터 블록*	variable	사용자가 추가한 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 페이지 4-161의 내용을 참조하십시오.

표 B-49 5.0~5.0.2 버전용 전체 호스트 프로파일 레코드 필드 (계속)

필드	데이터 유형	설명
일반 목록 블록 유형	uint32	취약점 스캐너가 추가한 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
운영 체제 핑거프린트(스캔 핑거프린트) 데이터 블록*	variable	취약점 스캐너가 추가한 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 페이지 4-161의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	애플리케이션이 추가한 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
운영 체제 핑거프린트(애플리케이션 핑거프린트) 데이터 블록*	variable	애플리케이션이 추가한 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 페이지 4-161의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	핑거프린트 충돌 해결을 통해 선택된 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
운영 체제 핑거프린트(충돌 핑거프린트) 데이터 블록*	variable	핑거프린트 충돌 해결을 통해 선택된 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 페이지 4-161의 내용을 참조하십시오.
목록 블록 유형	uint32	TCP 서비스 데이터를 전달하는 전체 서버 데이터 블록으로 구성된 목록 데이터 블록을 시작합니다. 이 값은 항상 11입니다.
목록 블록 길이	uint32	목록의 바이트 수입니다. 이 수에는 목록 블록 유형 및 길이 필드의 8바이트에 캡슐화된 모든 전체 서버 데이터 블록의 길이를 더한 값이 포함됩니다.
(TCP) 전체 서버 데이터 블록*	variable	호스트의 TCP 서비스에 대한 데이터를 전달하는 전체 서버 데이터 블록의 목록입니다. 이 데이터 블록에 대한 설명은 4.10.0 이상 버전용 전체 호스트 서버 데이터 블록, 페이지 4-140의 내용을 참조하십시오.
목록 블록 유형	uint32	UDP 서비스 데이터를 전달하는 전체 서버 데이터 블록으로 구성된 목록 데이터 블록을 시작합니다. 이 값은 항상 11입니다.
목록 블록 길이	uint32	목록의 바이트 수입니다. 이 수에는 목록 블록 유형 및 길이 필드의 8바이트에 캡슐화된 모든 전체 서버 데이터 블록의 길이를 더한 값이 포함됩니다.

표 B-49 5.0~5.0.2 버전용 전체 호스트 프로파일 레코드 필드 (계속)

필드	데이터 유형	설명
(UDP) 전체 서버 데이터 블록*	variable	호스트의 UDP 하위 서버에 대한 데이터를 전달하는 전체 서버 데이터 블록의 목록입니다. 이 데이터 블록에 대한 설명은 4.10.0 이상 버전용 전체 호스트 서버 데이터 블록, 페이지 4-140의 내용을 참조하십시오.
목록 블록 유형	uint32	네트워크 프로토콜 데이터를 전달하는 프로토콜 데이터 블록으로 구성된 목록 데이터 블록을 시작합니다. 이 값은 항상 11입니다.
목록 블록 길이	uint32	목록의 바이트 수입니다. 이 수에는 목록 블록 유형 및 길이 필드의 8바이트에 캡슐화된 모든 프로토콜 데이터 블록의 길이를 더한 값이 포함됩니다.
(네트워크) 프로토콜 데이터 블록*	variable	호스트의 네트워크 프로토콜에 대한 데이터를 전달하는 프로토콜 데이터 블록의 목록입니다. 이 데이터 블록에 대한 설명은 프로토콜 데이터 블록, 페이지 4-77의 내용을 참조하십시오.
목록 블록 유형	uint32	전송 프로토콜 데이터를 전달하는 프로토콜 데이터 블록으로 구성된 목록 데이터 블록을 시작합니다. 이 값은 항상 11입니다.
목록 블록 길이	uint32	목록의 바이트 수입니다. 이 수에는 목록 블록 유형 및 길이 필드의 8바이트에 캡슐화된 모든 프로토콜 데이터 블록의 길이를 더한 값이 포함됩니다.
(전송) 프로토콜 데이터 블록*	variable	호스트의 전송 프로토콜에 대한 데이터를 전달하는 프로토콜 데이터 블록의 목록입니다. 이 데이터 블록에 대한 설명은 프로토콜 데이터 블록, 페이지 4-77의 내용을 참조하십시오.
목록 블록 유형	uint32	MAC 주소 데이터 블록이 포함된 목록 데이터 블록을 시작합니다. 이 값은 항상 11입니다.
목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 호스트 MAC 주소 데이터 블록을 포함한 목록의 바이트 수입니다.
호스트 MAC 주소 데이터 블록*	variable	호스트 MAC 주소 데이터 블록의 목록입니다. 이 데이터 블록에 대한 설명은 4.9 이상 버전용 호스트 MAC 주소, 페이지 4-117의 내용을 참조하십시오.
마지막 확인	uint32	시스템이 호스트 활동을 마지막으로 탐지한 시간을 나타내는 UNIX 타임스탬프입니다.
호스트 유형	uint32	호스트 유형을 나타냅니다. 값은 다음과 같습니다. • 0 - 호스트 • 1 - 라우터 • 2 - 브리지 • 3 -NAT(Network Address Translation) 디바이스 • 4 - LB(로드 밸런서)
비즈니스 임계성	uint16	비즈니스에 대한 호스트의 임계성을 나타냅니다.
VLAN ID	uint16	호스트가 구성원으로 포함된 VLAN을 나타내는 VLAN ID 번호입니다.
VLAN 유형	uint8	VLAN 태그에 캡슐화된 패킷 유형입니다.
VLAN 우선순위	uint8	VLAN 태그에 포함된 우선순위 값입니다.

표 B-49 5.0~5.0.2 버전용 전체 호스트 프로파일 레코드 필드 (계속)

필드	데이터 유형	설명
일반 목록 블록 유형	uint32	클라이언트 애플리케이션 데이터를 전달하는 호스트 취약점 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 클라이언트 애플리케이션 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
전체 호스트 클라이언트 애플리케이션 데이터 블록*	variable	클라이언트 애플리케이션 데이터 블록의 목록입니다. 이 데이터 블록에 대한 설명은 5.0 이상 버전용 전체 호스트 클라이언트 애플리케이션 데이터 블록, 페이지 4-154의 내용을 참조하십시오.
문자열 블록 유형	uint32	호스트 NetBIOS 이름에 대한 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이 필드의 8바이트에 NetBIOS 이름 문자열의 바이트 수를 더한 값이 포함됩니다.
NetBIOS 이름	string	호스트 NetBIOS 이름 문자열입니다.
문자열 블록 유형	uint32	호스트 메모에 대한 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	메모 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 메모의 바이트 수를 더한 값이 포함됩니다.
메모	string	호스트에 대한 메모 호스트 속성의 콘텐츠를 포함합니다.
일반 목록 블록 유형	uint32	VDB 취약점 데이터를 전달하는 호스트 취약점 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
(VDB) 호스트 취약점 데이터 블록*	variable	Cisco VDB(취약점 데이터베이스)에서 식별된 취약점에 대한 호스트 취약점 데이터 블록의 목록입니다. 이 데이터 블록에 대한 설명은 4.9.0 이상 버전용 호스트 취약점 데이터 블록, 페이지 4-114의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	서드파티 취약점 스캔 데이터를 전달하는 호스트 취약점 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
(서드파티/VDB) 호스트 취약점 데이터 블록*	variable	Cisco VDB(취약점 데이터베이스)에 카탈로그화된 호스트 취약점에 대한 정보를 포함하며 서드파티 스캐너에서 제공한 호스트 취약점 데이터 블록입니다. 이 데이터 블록에 대한 설명은 4.9.0 이상 버전용 호스트 취약점 데이터 블록, 페이지 4-114의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	서드파티 취약점 스캔 데이터를 전달하는 호스트 취약점 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.

표 B-49 5.0~5.0.2 버전용 전체 호스트 프로파일 레코드 필드 (계속)

필드	데이터 유형	설명
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
(서드파티 스캔) 호스트 취약점 데이터 블록*	variable	서드파티 스캐너에서 제공한 호스트 취약점 데이터 블록입니다. 이러한 데이터 블록의 호스트 취약점 ID는 Cisco에서 탐지한 ID가 아니라 서드파티 스캐너 ID입니다. 이 데이터 블록에 대한 설명은 4.9.0 이상 버전용 호스트 취약점 데이터 블록, 페이지 4-114의 내용을 참조하십시오.
목록 블록 유형	uint32	속성 데이터를 전달하는 속성값 데이터 블록으로 구성된 목록 데이터 블록을 시작합니다. 이 값은 항상 11입니다.
목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 데이터 블록을 포함한 목록 데이터 블록의 바이트 수입니다.
속성값 데이터 블록*	variable	속성값 데이터 블록의 목록입니다. 이 목록의 데이터 블록에 대한 설명은 속성값 데이터 블록, 페이지 4-83의 내용을 참조하십시오.

5.1.1 버전용 전체 호스트 프로파일 데이터 블록

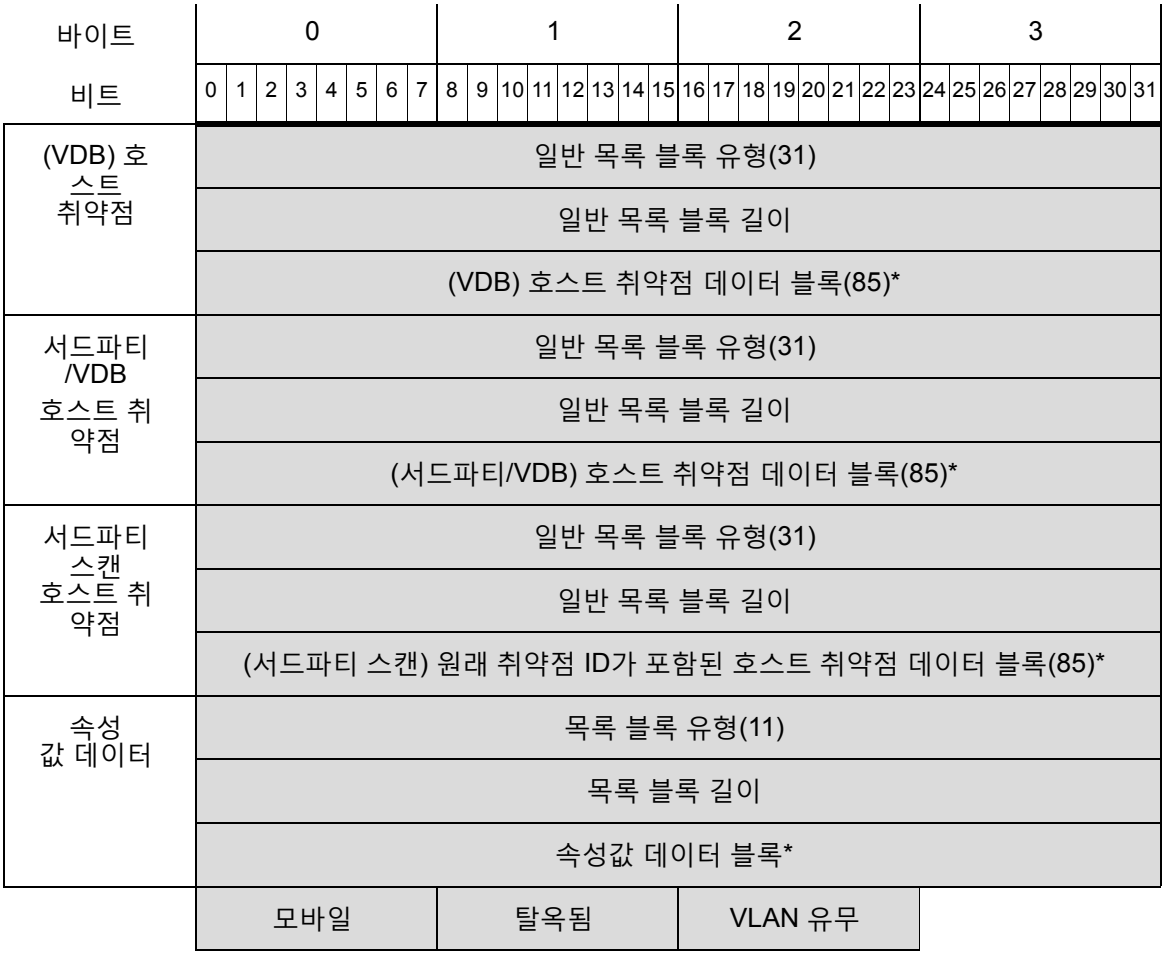
5.1.1 버전용 전체 호스트 프로파일 데이터 블록에는 호스트 하나를 설명하는 전체 데이터 집합이 포함됩니다. 이 블록은 아래 그림에 나와 있는 형식으로 되어 있습니다. 해당 형식에 대한 설명은 다음 표에 나와 있습니다. 목록 데이터 블록을 제외하고는 캡슐화된 데이터 블록의 필드는 그림에 나와 있지 않습니다. 이러한 캡슐화된 데이터 블록에 대해서는 검색 및 연결 데이터 구조 이해, 페이지 4-1에서 별도로 설명합니다. 전체 호스트 프로파일 데이터 블록의 블록 유형 값은 135입니다. 이는 데이터 블록 111의 사용을 중단합니다.

참고 다음 다이어그램에서 블록 이름 옆에 있는 별표(*)는 데이터 블록 인스턴스가 여러 개 나올 수 있음을 나타냅니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
파생된 OS 핑거프린트	일반 목록 블록 길이(계속)								운영 체제 핑거프린트 블록 유형(130)*																							
	OS 핑거프린트 블록 유형(130)*(계속)								운영 체제 핑거프린트 블록 길이																							
	OS 핑거프린트 블록 길이(계속)								운영 체제 파생 핑거프린트 데이터...																							
	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
서버 핑거프린트	운영 체제 핑거프린트 블록 유형(130)*																															
	운영 체제 핑거프린트 블록 길이																															
	운영 체제 서버 핑거프린트 데이터...																															
	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
클라이언트 핑거프린트	운영 체제 핑거프린트 블록 유형(130)*																															
	운영 체제 핑거프린트 블록 길이																															
	운영 체제 클라이언트 핑거프린트 데이터...																															
	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
VDB 네이티브 핑거프린트 1	운영 체제 핑거프린트 블록 유형(130)*																															
	운영 체제 핑거프린트 블록 길이																															
	운영 체제 VDB 핑거프린트 데이터...																															
	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
VDB 네이티브 핑거프린트 2	운영 체제 핑거프린트 블록 유형(130)*																															
	운영 체제 핑거프린트 블록 길이																															
	운영 체제 VDB 핑거프린트 데이터...																															

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
사용자 핑거프린트	운영 체제 핑거프린트 블록 유형(130)*																															
	운영 체제 핑거프린트 블록 길이																															
	운영 체제 사용자 핑거프린트 데이터...																															
	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
스캔 핑거프린트	운영 체제 핑거프린트 블록 유형(130)*																															
	운영 체제 핑거프린트 블록 길이																															
	운영 체제 스캔 핑거프린트 데이터...																															
	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
애플리케이션 핑거프린트	운영 체제 핑거프린트 블록 유형(130)*																															
	운영 체제 핑거프린트 블록 길이																															
	운영 체제 애플리케이션 핑거프린트 데이터...																															
	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
충돌 핑거프린트	운영 체제 핑거프린트 블록 유형(130)*																															
	운영 체제 핑거프린트 블록 길이																															
	운영 체제 충돌 핑거프린트 데이터...																															
(TCP) 전체 서버 데이터	목록 블록 유형(11)...																															
	목록 블록 길이...																															
	(TCP) 전체 서버 데이터 블록(104)*																															

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
(UDP) 전체 서버 데이터	목록 블록 유형(11)																															
	목록 블록 길이																															
	(UDP) 전체 서버 데이터 블록(104)*																															
네트워크 프로토콜 데이터	목록 블록 유형(11)																															
	목록 블록 길이																															
	(네트워크) 프로토콜 데이터 블록(4)*																															
전송 프로토콜 데이터	목록 블록 유형(11)																															
	목록 블록 길이																															
	(전송) 프로토콜 데이터 블록(4)*																															
MAC 주소 데이터	목록 블록 유형(11)																															
	목록 블록 길이																															
	호스트 MAC 주소 데이터 블록(95)*																															
	마지막 확인																															
	호스트 유형																															
	비즈니스 임계성																VLAN ID															
	VLAN 유형								VLAN 우선순위								일반 목록 블록 유형(31)															
호스트 클라이언트 데이터	일반 목록 블록 유형(계속)																일반 목록 블록 길이															
	일반 목록 블록 길이(계속)																전체 호스트 클라이언트 애플리케이션 데이터 블록(112)*															
NetBIOS 이름	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	NetBIOS 이름 문자열...																															
메모 데이터	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	메모 문자열...																															



다음 표에는 5.1.1 버전용 전체 호스트 프로파일 레코드의 구성 요소에 대한 설명이 나와 있습니다.

표 B-50 5.1.1 버전용 전체 호스트 프로파일 레코드 필드

필드	데이터 유형	설명
IP 주소	uint8[4]	호스트의 IP 주소(IP 주소 옥텟 형식)입니다.
홉	uint8	호스트에서 디바이스로의 네트워크 홉 수입니다.
일반 목록 블록 유형	uint32	기존 핑거프린트에서 호스트에 대해 파생된 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
운영 체제 파생 핑거프린트 데이터 블록*	variable	기존 핑거프린트에서 호스트에 대해 파생된 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 페이지 4-161의 내용을 참조하십시오.

표 B-50 5.1.1 버전용 전체 호스트 프로파일 레코드 필드 (계속)

필드	데이터 유형	설명
일반 목록 블록 유형	uint32	서버 핑거프린트를 사용하여 식별된 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
운영 체제 핑거프린트(서버 핑거프린트) 데이터 블록*	variable	서버 핑거프린트를 사용하여 식별된 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 페이지 4-161의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	클라이언트 핑거프린트를 사용하여 식별된 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
운영 체제 핑거프린트(클라이언트 핑거프린트) 데이터 블록*	variable	클라이언트 핑거프린트를 사용하여 식별된 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 페이지 4-161의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	Cisco VDB 핑거프린트를 사용하여 식별된 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
운영 체제 핑거프린트(VDB 네이티브 핑거프린트 1) 데이터 블록*	variable	Cisco VDB(취약점 데이터베이스)의 핑거프린트를 사용하여 식별된 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 페이지 4-161의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	Cisco VDB 핑거프린트를 사용하여 식별된 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
운영 체제 핑거프린트(VDB 네이티브 핑거프린트 2) 데이터 블록*	variable	Cisco VDB(취약점 데이터베이스)의 핑거프린트를 사용하여 식별된 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 페이지 4-161의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	사용자가 추가한 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.

표 B-50 5.1.1 버전용 전체 호스트 프로파일 레코드 필드 (계속)

필드	데이터 유형	설명
운영 체제 핑거프린트(사용자 핑거프린트) 데이터 블록*	variable	사용자가 추가한 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 페이지 4-161의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	취약점 스캐너가 추가한 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
운영 체제 핑거프린트(스캔 핑거프린트) 데이터 블록*	variable	취약점 스캐너가 추가한 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 페이지 4-161의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	애플리케이션이 추가한 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
운영 체제 핑거프린트(애플리케이션 핑거프린트) 데이터 블록*	variable	애플리케이션이 추가한 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 페이지 4-161의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	핑거프린트 충돌 해결을 통해 선택된 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
운영 체제 핑거프린트(충돌 핑거프린트) 데이터 블록*	variable	핑거프린트 충돌 해결을 통해 선택된 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 페이지 4-161의 내용을 참조하십시오.
목록 블록 유형	uint32	TCP 서비스 데이터를 전달하는 전체 서버 데이터 블록으로 구성된 목록 데이터 블록을 시작합니다. 이 값은 항상 11입니다.
목록 블록 길이	uint32	목록의 바이트 수입니다. 이 수에는 목록 블록 유형 및 길이 필드의 8바이트에 캡슐화된 모든 전체 서버 데이터 블록의 길이를 더한 값이 포함됩니다.
(TCP) 전체 서버 데이터 블록*	variable	호스트의 TCP 서비스에 대한 데이터를 전달하는 전체 서버 데이터 블록의 목록입니다. 이 데이터 블록에 대한 설명은 4.10.0 이상 버전용 전체 호스트 서버 데이터 블록, 페이지 4-140의 내용을 참조하십시오.
목록 블록 유형	uint32	UDP 서비스 데이터를 전달하는 전체 서버 데이터 블록으로 구성된 목록 데이터 블록을 시작합니다. 이 값은 항상 11입니다.

표 B-50 5.1.1 버전용 전체 호스트 프로파일 레코드 필드 (계속)

필드	데이터 유형	설명
목록 블록 길이	uint32	목록의 바이트 수입니다. 이 수에는 목록 블록 유형 및 길이 필드의 8바이트에 캡슐화된 모든 전체 서버 데이터 블록의 길이를 더한 값이 포함됩니다.
(UDP) 전체 서버 데이터 블록*	variable	호스트의 UDP 하위 서버에 대한 데이터를 전달하는 전체 서버 데이터 블록의 목록입니다. 이 데이터 블록에 대한 설명은 4.10.0 이상 버전용 전체 호스트 서버 데이터 블록, 페이지 4-140의 내용을 참조하십시오.
목록 블록 유형	uint32	네트워크 프로토콜 데이터를 전달하는 프로토콜 데이터 블록으로 구성된 목록 데이터 블록을 시작합니다. 이 값은 항상 11입니다.
목록 블록 길이	uint32	목록의 바이트 수입니다. 이 수에는 목록 블록 유형 및 길이 필드의 8바이트에 캡슐화된 모든 프로토콜 데이터 블록의 길이를 더한 값이 포함됩니다.
(네트워크) 프로토콜 데이터 블록*	variable	호스트의 네트워크 프로토콜에 대한 데이터를 전달하는 프로토콜 데이터 블록의 목록입니다. 이 데이터 블록에 대한 설명은 프로토콜 데이터 블록, 페이지 4-77의 내용을 참조하십시오.
목록 블록 유형	uint32	전송 프로토콜 데이터를 전달하는 프로토콜 데이터 블록으로 구성된 목록 데이터 블록을 시작합니다. 이 값은 항상 11입니다.
목록 블록 길이	uint32	목록의 바이트 수입니다. 이 수에는 목록 블록 유형 및 길이 필드의 8바이트에 캡슐화된 모든 프로토콜 데이터 블록의 길이를 더한 값이 포함됩니다.
(전송) 프로토콜 데이터 블록*	variable	호스트의 전송 프로토콜에 대한 데이터를 전달하는 프로토콜 데이터 블록의 목록입니다. 이 데이터 블록에 대한 설명은 프로토콜 데이터 블록, 페이지 4-77의 내용을 참조하십시오.
목록 블록 유형	uint32	MAC 주소 데이터 블록이 포함된 목록 데이터 블록을 시작합니다. 이 값은 항상 11입니다.
목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 호스트 MAC 주소 데이터 블록을 포함한 목록의 바이트 수입니다.
호스트 MAC 주소 데이터 블록*	variable	호스트 MAC 주소 데이터 블록의 목록입니다. 이 데이터 블록에 대한 설명은 4.9 이상 버전용 호스트 MAC 주소, 페이지 4-117의 내용을 참조하십시오.
마지막 확인	uint32	시스템이 호스트 활동을 마지막으로 탐지한 시간을 나타내는 UNIX 타임스탬프입니다.
호스트 유형	uint32	호스트 유형을 나타냅니다. 값은 다음과 같습니다. • 0 - 호스트 • 1 - 라우터 • 2 - 브리지 • 3 -NAT(Network Address Translation) 디바이스 • 4 - LB(로드 밸런서)
비즈니스 임계성	uint16	비즈니스에 대한 호스트의 임계성을 나타냅니다.
VLAN ID	uint16	호스트가 구성원으로 포함된 VLAN을 나타내는 VLAN ID 번호입니다.

표 B-50 5.1.1 버전용 전체 호스트 프로파일 레코드 필드 (계속)

필드	데이터 유형	설명
VLAN 유형	uint8	VLAN 태그에 캡슐화된 패킷 유형입니다.
VLAN 우선순위	uint8	VLAN 태그에 포함된 우선순위 값입니다.
일반 목록 블록 유형	uint32	클라이언트 애플리케이션 데이터를 전달하는 호스트 취약점 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 클라이언트 애플리케이션 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
전체 호스트 클라이언트 애플리케이션 데이터 블록*	variable	클라이언트 애플리케이션 데이터 블록의 목록입니다. 이 데이터 블록에 대한 설명은 5.0 이상 버전용 전체 호스트 클라이언트 애플리케이션 데이터 블록, 페이지 4-154의 내용을 참조하십시오.
문자열 블록 유형	uint32	호스트 NetBIOS 이름에 대한 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이 필드의 8바이트에 NetBIOS 이름 문자열의 바이트 수를 더한 값이 포함됩니다.
NetBIOS 이름	string	호스트 NetBIOS 이름 문자열입니다.
문자열 블록 유형	uint32	호스트 메모에 대한 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	메모 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 메모의 바이트 수를 더한 값이 포함됩니다.
메모	string	호스트에 대한 메모 호스트 속성의 콘텐츠를 포함합니다.
일반 목록 블록 유형	uint32	VDB 취약점 데이터를 전달하는 호스트 취약점 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
(VDB) 호스트 취약점 데이터 블록*	variable	Cisco VDB(취약점 데이터베이스)에서 식별된 취약점에 대한 호스트 취약점 데이터 블록의 목록입니다. 이 데이터 블록에 대한 설명은 4.9.0 이상 버전용 호스트 취약점 데이터 블록, 페이지 4-114의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	서드파티 취약점 스캔 데이터를 전달하는 호스트 취약점 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
(서드파티/VDB) 호스트 취약점 데이터 블록*	variable	Cisco VDB(취약점 데이터베이스)에 카탈로그화된 호스트 취약점에 대한 정보를 포함하며 서드파티 스캐너에서 제공한 호스트 취약점 데이터 블록입니다. 이 데이터 블록에 대한 설명은 4.9.0 이상 버전용 호스트 취약점 데이터 블록, 페이지 4-114의 내용을 참조하십시오.

표 B-50 5.1.1 버전용 전체 호스트 프로파일 레코드 필드 (계속)

필드	데이터 유형	설명
일반 목록 블록 유형	uint32	서드파티 취약점 스캔 데이터를 전달하는 호스트 취약점 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
(서드파티 스캔) 호스트 취약점 데이터 블록*	variable	서드파티 스캐너에서 제공한 호스트 취약점 데이터 블록입니다. 이러한 데이터 블록의 호스트 취약점 ID는 Cisco에서 탐지한 ID가 아니라 서드파티 스캐너 ID입니다. 이 데이터 블록에 대한 설명은 4.9.0 이상 버전용 호스트 취약점 데이터 블록, 페이지 4-114의 내용을 참조하십시오.
목록 블록 유형	uint32	속성 데이터를 전달하는 속성값 데이터 블록으로 구성된 목록 데이터 블록을 시작합니다. 이 값은 항상 11입니다.
목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 데이터 블록을 포함한 목록 데이터 블록의 바이트 수입니다.
속성값 데이터 블록*	variable	속성값 데이터 블록의 목록입니다. 이 목록의 데이터 블록에 대한 설명은 속성값 데이터 블록, 페이지 4-83의 내용을 참조하십시오.
모바일	uint8	운영 체제가 모바일 디바이스에서 실행되고 있는지를 나타내는 true-false 플래그입니다.
탈옥됨	uint8	모바일 디바이스의 운영 체제가 탈옥되었는지 나타내는 true-false 플래그입니다.
VLAN 유무	uint8	VLAN의 유무를 나타냅니다. • 0 - 예 • 1 - 아니요

5.2.x 버전용 전체 호스트 프로파일 데이터 블록

5.2.x 버전용 전체 호스트 프로파일 데이터 블록에는 호스트 하나를 설명하는 전체 데이터 집합이 포함됩니다. 이 블록은 아래 그림에 나와 있는 형식으로 되어 있습니다. 해당 형식에 대한 설명은 다음 표에 나와 있습니다. 목록 데이터 블록을 제외하고는 캡슐화된 데이터 블록의 필드는 그림에 나와 있지 않습니다. 이러한 캡슐화된 데이터 블록에 대해서는 검색 및 연결 데이터 구조 이해, 페이지 4-1에서 별도로 설명합니다. 전체 호스트 프로파일 데이터 블록의 블록 유형 값은 140입니다. 이는 이전 버전(블록 유형 135)을 대체합니다.

참고 다음 다이어그램에서 블록 이름 옆에 있는 별표(*)는 데이터 블록 인스턴스가 여러 개 나올 수 있음을 나타냅니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	전체 호스트 프로파일 데이터 블록(140)																															
	데이터 블록 길이																															
	호스트 ID 호스트 ID(계속) 호스트 ID(계속) 호스트 ID(계속)																															
IP 주소	목록 블록 유형(11)																															
	목록 블록 길이																															
	IP 주소 데이터 블록(143)*																															
	홉								일반 목록 블록 유형(31)																							
	일반 목록 블록 유형(계속)								일반 목록 블록 길이																							
파생된 OS 핑거프린트	일반 목록 블록 길이(계속)								운영 체제 핑거프린트 블록 유형(130)*																							
	OS 핑거프린트 블록 유형(130)*(계속)								운영 체제 핑거프린트 블록 길이																							
	OS 핑거프린트 블록 길이(계속)								운영 체제 파생 핑거프린트 데이터...																							
	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
서버 핑거프린트	운영 체제 핑거프린트 블록 유형(130)*																															
	운영 체제 핑거프린트 블록 길이																															
	운영 체제 서버 핑거프린트 데이터...																															
	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
클라이언트 핑거프린트	운영 체제 핑거프린트 블록 유형(130)*																															
	운영 체제 핑거프린트 블록 길이																															
	운영 체제 클라이언트 핑거프린트 데이터...																															
	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
VDB 네이티브 핑거프린트 1	운영 체제 핑거프린트 블록 유형(130)*																															
	운영 체제 핑거프린트 블록 길이																															
	운영 체제 VDB 핑거프린트 데이터...																															
	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
VDB 네이티브 핑거프린트 2	운영 체제 핑거프린트 블록 유형(130)*																															
	운영 체제 핑거프린트 블록 길이																															
	운영 체제 VDB 핑거프린트 데이터...																															
	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
사용자 핑거프린트	운영 체제 핑거프린트 블록 유형(130)*																															
	운영 체제 핑거프린트 블록 길이																															
	운영 체제 사용자 핑거프린트 데이터...																															
	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
스캔 핑거프린트	운영 체제 핑거프린트 블록 유형(130)*																															
	운영 체제 핑거프린트 블록 길이																															
	운영 체제 스캔 핑거프린트 데이터...																															
	일반 목록 블록 유형(31)																															

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	일반 목록 블록 길이																															
애플리케이션 핑거프린트	운영 체제 핑거프린트 블록 유형(130)*																															
	운영 체제 핑거프린트 블록 길이																															
	운영 체제 애플리케이션 핑거프린트 데이터...																															
충돌 핑거프린트	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
	운영 체제 핑거프린트 블록 유형(130)*																															
	운영 체제 핑거프린트 블록 길이																															
	운영 체제 충돌 핑거프린트 데이터...																															
모바일 핑거프린트	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
	운영 체제 핑거프린트 블록 유형(130)*																															
	운영 체제 핑거프린트 블록 길이																															
	운영 체제 모바일 핑거프린트 데이터...																															
IPv6 서버 핑거프린트	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
	운영 체제 핑거프린트 블록 유형(130)*																															
	운영 체제 핑거프린트 블록 길이																															
	운영 체제 IPv6 서버 핑거프린트 데이터...																															
IPv6 클라이언트 핑거프린트	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
	운영 체제 핑거프린트 블록 유형(130)*																															
	운영 체제 핑거프린트 블록 길이																															
	운영 체제 IPv6 클라이언트 핑거프린트 데이터...																															

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
IPv6 DHCP 핑거프린트	운영 체제 핑거프린트 블록 유형(130)*																															
	운영 체제 핑거프린트 블록 길이																															
	운영 체제 IPv6 DHCP 핑거프린트 데이터...																															
	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
사용자 에이전트 핑거프린트	운영 체제 핑거프린트 블록 유형(130)*																															
	운영 체제 핑거프린트 블록 길이																															
	운영 체제 사용자 에이전트 핑거프린트 데이터...																															
(TCP) 전체 서버 데이터	목록 블록 유형(11)...																															
	목록 블록 길이...																															
	(TCP) 전체 서버 데이터 블록(104)*																															
(UDP) 전체 서버 데이터	목록 블록 유형(11)																															
	목록 블록 길이																															
	(UDP) 전체 서버 데이터 블록(104)*																															
네트워크 프로토콜 데이터	목록 블록 유형(11)																															
	목록 블록 길이																															
	(네트워크) 프로토콜 데이터 블록(4)*																															
전송 프로토콜 데이터	목록 블록 유형(11)																															
	목록 블록 길이																															
	(전송) 프로토콜 데이터 블록(4)*																															

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
MAC 주소 데이터	목록 블록 유형(11)																															
	목록 블록 길이																															
	호스트 MAC 주소 데이터 블록(95)*																															
	마지막 확인																															
	호스트 유형																															
	비즈니스 임계성																VLAN ID															
	VLAN 유형								VLAN 우선순위								일반 목록 블록 유형(31)															
호스트 클라이언트 데이터	일반 목록 블록 유형(계속)																일반 목록 블록 길이															
	일반 목록 블록 길이(계속)																전체 호스트 클라이언트 애플리케이션 데이터 블록(112)*															
NetBios 이름 이름	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	NetBIOS 이름 문자열...																															
메모 데이터	문자열 블록 유형(0)																															
	문자열 블록 길이																															
	메모 문자열...																															
(VDB) 호스트 취약점	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
	(VDB) 호스트 취약점 데이터 블록(85)*																															
서드파티/VDB 호스트 취약점	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
	(서드파티/VDB) 호스트 취약점 데이터 블록(85)*																															
서드파티 스캔 호스트 취약점	일반 목록 블록 유형(31)																															
	일반 목록 블록 길이																															
	(서드파티 스캔) 원래 취약점 ID가 포함된 호스트 취약점 데이터 블록(85)*																															

다음 표에는 5.2.x 버전용 전체 호스트 프로파일 레코드의 구성 요소에 대한 설명이 나와 있습니다.

표 B-51 5.2.x 버전용 전체 호스트 프로파일 레코드 필드

필드	데이터 유형	설명
호스트 ID	uint8[16]	호스트의 고유 ID 번호로, UUID입니다.
목록 블록 유형	uint32	TCP 서비스 데이터를 전달하는 IP 주소 데이터 블록으로 구성된 목록 데이터 블록을 시작합니다. 이 값은 항상 11입니다.
목록 블록 길이	uint32	목록의 바이트 수입니다. 이 수에는 목록 블록 유형 및 길이 필드의 8바이트에 캡슐화된 모든 IP 주소 데이터 블록의 길이를 더한 값이 포함됩니다.
IP 주소	variable	호스트의 IP 주소와 각 IP 주소가 마지막으로 확인된 시간입니다. 이 데이터 블록에 대한 설명은 호스트 IP 주소 데이터 블록, 페이지 4-99의 내용을 참조하십시오.
홉	uint8	호스트에서 디바이스로의 네트워크 홉 수입니다.
일반 목록 블록 유형	uint32	기존 핑거프린트에서 호스트에 대해 파생된 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
운영 체제 파생 핑거프린트 데이터 블록*	variable	기존 핑거프린트에서 호스트에 대해 파생된 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 페이지 4-161의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	서버 핑거프린트를 사용하여 식별된 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
운영 체제 핑거프린트(서버 핑거프린트) 데이터 블록*	variable	서버 핑거프린트를 사용하여 식별된 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 페이지 4-161의 내용을 참조하십시오.

표 B-51 5.2.x 버전용 전체 호스트 프로파일 레코드 필드 (계속)

필드	데이터 유형	설명
일반 목록 블록 유형	uint32	클라이언트 핑거프린트를 사용하여 식별된 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
운영 체제 핑거프린트(클라이언트 핑거프린트) 데이터 블록*	variable	클라이언트 핑거프린트를 사용하여 식별된 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 페이지 4-161의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	Cisco VDB 핑거프린트를 사용하여 식별된 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
운영 체제 핑거프린트(VDB 네이티브 핑거프린트 1) 데이터 블록*	variable	Cisco VDB(취약점 데이터베이스)의 핑거프린트를 사용하여 식별된 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 페이지 4-161의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	Cisco VDB 핑거프린트를 사용하여 식별된 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
운영 체제 핑거프린트(VDB 네이티브 핑거프린트 2) 데이터 블록*	variable	Cisco VDB(취약점 데이터베이스)의 핑거프린트를 사용하여 식별된 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 페이지 4-161의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	사용자가 추가한 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
운영 체제 핑거프린트(사용자 핑거프린트) 데이터 블록*	variable	사용자가 추가한 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 페이지 4-161의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	취약점 스캐너가 추가한 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.

표 B-51 5.2.x 버전용 전체 호스트 프로파일 레코드 필드 (계속)

필드	데이터 유형	설명
운영 체제 핑거프린트(스캔 핑거프린트) 데이터 블록*	variable	취약점 스캐너가 추가한 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 페이지 4-161의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	애플리케이션이 추가한 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
운영 체제 핑거프린트(애플리케이션 핑거프린트) 데이터 블록*	variable	애플리케이션이 추가한 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 페이지 4-161의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	핑거프린트 충돌 해결을 통해 선택된 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
운영 체제 핑거프린트(충돌 핑거프린트) 데이터 블록*	variable	핑거프린트 충돌 해결을 통해 선택된 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 페이지 4-161의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	모바일 디바이스 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
운영 체제 핑거프린트(모바일) 데이터 블록*	variable	모바일 디바이스 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 페이지 4-161의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	IPv6 서버 핑거프린트를 사용하여 식별된 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
운영 체제 핑거프린트(IPv6 서버 핑거프린트) 데이터 블록*	variable	IPv6 서버 핑거프린트를 사용하여 식별된 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 페이지 4-161의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	IPv6 클라이언트 핑거프린트를 사용하여 식별된 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.

표 B-51 5.2.x 버전용 전체 호스트 프로파일 레코드 필드 (계속)

필드	데이터 유형	설명
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
운영 체제 핑거프린트(IPv6 클라이언트 핑거프린트) 데이터 블록*	variable	IPv6 클라이언트 핑거프린트를 사용하여 식별된 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 페이지 4-161의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	IPv6 DHCP 핑거프린트를 사용하여 식별된 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
운영 체제 핑거프린트(IPv6 DHCP) 데이터 블록*	variable	IPv6 DHCP 핑거프린트를 사용하여 식별된 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 페이지 4-161의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	사용자 에이전트 핑거프린트를 사용하여 식별된 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
운영 체제 핑거프린트(사용자 에이전트) 데이터 블록*	variable	사용자 에이전트 핑거프린트를 사용하여 식별된 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 페이지 4-161의 내용을 참조하십시오.
목록 블록 유형	uint32	TCP 서비스 데이터를 전달하는 전체 서버 데이터 블록으로 구성된 목록 데이터 블록을 시작합니다. 이 값은 항상 11입니다.
목록 블록 길이	uint32	목록의 바이트 수입니다. 이 수에는 목록 블록 유형 및 길이 필드의 8바이트에 캡슐화된 모든 전체 서버 데이터 블록의 길이를 더한 값이 포함됩니다.
(TCP) 전체 서버 데이터 블록*	variable	호스트의 TCP 서비스에 대한 데이터를 전달하는 전체 서버 데이터 블록의 목록입니다. 이 데이터 블록에 대한 설명은 4.10.0 이상 버전용 전체 호스트 서버 데이터 블록, 페이지 4-140의 내용을 참조하십시오.
목록 블록 유형	uint32	UDP 서비스 데이터를 전달하는 전체 서버 데이터 블록으로 구성된 목록 데이터 블록을 시작합니다. 이 값은 항상 11입니다.
목록 블록 길이	uint32	목록의 바이트 수입니다. 이 수에는 목록 블록 유형 및 길이 필드의 8바이트에 캡슐화된 모든 전체 서버 데이터 블록의 길이를 더한 값이 포함됩니다.
(UDP) 전체 서버 데이터 블록*	variable	호스트의 UDP 하위 서버에 대한 데이터를 전달하는 전체 서버 데이터 블록의 목록입니다. 이 데이터 블록에 대한 설명은 4.10.0 이상 버전용 전체 호스트 서버 데이터 블록, 페이지 4-140의 내용을 참조하십시오.

표 B-51 5.2.x 버전용 전체 호스트 프로파일 레코드 필드 (계속)

필드	데이터 유형	설명
목록 블록 유형	uint32	네트워크 프로토콜 데이터를 전달하는 프로토콜 데이터 블록으로 구성된 목록 데이터 블록을 시작합니다. 이 값은 항상 11입니다.
목록 블록 길이	uint32	목록의 바이트 수입니다. 이 수에는 목록 블록 유형 및 길이 필드의 8바이트에 캡슐화된 모든 프로토콜 데이터 블록의 길이를 더한 값이 포함됩니다.
(네트워크) 프로토콜 데이터 블록*	variable	호스트의 네트워크 프로토콜에 대한 데이터를 전달하는 프로토콜 데이터 블록의 목록입니다. 이 데이터 블록에 대한 설명은 프로토콜 데이터 블록, 페이지 4-77의 내용을 참조하십시오.
목록 블록 유형	uint32	전송 프로토콜 데이터를 전달하는 프로토콜 데이터 블록으로 구성된 목록 데이터 블록을 시작합니다. 이 값은 항상 11입니다.
목록 블록 길이	uint32	목록의 바이트 수입니다. 이 수에는 목록 블록 유형 및 길이 필드의 8바이트에 캡슐화된 모든 프로토콜 데이터 블록의 길이를 더한 값이 포함됩니다.
(전송) 프로토콜 데이터 블록*	variable	호스트의 전송 프로토콜에 대한 데이터를 전달하는 프로토콜 데이터 블록의 목록입니다. 이 데이터 블록에 대한 설명은 프로토콜 데이터 블록, 페이지 4-77의 내용을 참조하십시오.
목록 블록 유형	uint32	MAC 주소 데이터 블록이 포함된 목록 데이터 블록을 시작합니다. 이 값은 항상 11입니다.
목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 호스트 MAC 주소 데이터 블록을 포함한 목록의 바이트 수입니다.
호스트 MAC 주소 데이터 블록*	variable	호스트 MAC 주소 데이터 블록의 목록입니다. 이 데이터 블록에 대한 설명은 4.9 이상 버전용 호스트 MAC 주소, 페이지 4-117의 내용을 참조하십시오.
마지막 확인	uint32	시스템이 호스트 활동을 마지막으로 탐지한 시간을 나타내는 UNIX 타임스탬프입니다.
호스트 유형	uint32	호스트 유형을 나타냅니다. 값은 다음과 같습니다. • 0 - 호스트 • 1 - 라우터 • 2 - 브리지 • 3 -NAT(Network Address Translation) 디바이스 • 4 - LB(로드 밸런서)
비즈니스 임계성	uint16	비즈니스에 대한 호스트의 임계성을 나타냅니다.
VLAN ID	uint16	호스트가 구성원으로 포함된 VLAN을 나타내는 VLAN ID 번호입니다.
VLAN 유형	uint8	VLAN 태그에 캡슐화된 패킷 유형입니다.
VLAN 우선순위	uint8	VLAN 태그에 포함된 우선순위 값입니다.
일반 목록 블록 유형	uint32	클라이언트 애플리케이션 데이터를 전달하는 호스트 취약점 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.

표 B-51 5.2.x 버전용 전체 호스트 프로파일 레코드 필드 (계속)

필드	데이터 유형	설명
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 클라이언트 애플리케이션 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
전체 호스트 클라이언트 애플리케이션 데이터 블록*	variable	클라이언트 애플리케이션 데이터 블록의 목록입니다. 이 데이터 블록에 대한 설명은 5.0 이상 버전용 전체 호스트 클라이언트 애플리케이션 데이터 블록, 페이지 4-154의 내용을 참조하십시오.
문자열 블록 유형	uint32	호스트 NetBIOS 이름에 대한 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	문자열 데이터 블록의 바이트 수입니다. 여기에는 문자열 블록 유형 및 길이 필드의 8바이트에 NetBIOS 이름 문자열의 바이트 수를 더한 값이 포함됩니다.
NetBIOS 이름	string	호스트 NetBIOS 이름 문자열입니다.
문자열 블록 유형	uint32	호스트 메모에 대한 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	메모 문자열 데이터 블록의 바이트 수입니다. 여기에는 블록 유형 및 길이 필드의 8바이트에 메모의 바이트 수를 더한 값이 포함됩니다.
메모	string	호스트에 대한 메모 호스트 속성의 콘텐츠를 포함합니다.
일반 목록 블록 유형	uint32	VDB 취약점 데이터를 전달하는 호스트 취약점 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
(VDB) 호스트 취약점 데이터 블록*	variable	Cisco VDB(취약점 데이터베이스)에서 식별된 취약점에 대한 호스트 취약점 데이터 블록의 목록입니다. 이 데이터 블록에 대한 설명은 4.9.0 이상 버전용 호스트 취약점 데이터 블록, 페이지 4-114의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	서드파티 취약점 스캔 데이터를 전달하는 호스트 취약점 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
(서드파티/VDB) 호스트 취약점 데이터 블록*	variable	Cisco VDB(취약점 데이터베이스)에 카탈로그화된 호스트 취약점에 대한 정보를 포함하며 서드파티 스캐너에서 제공한 호스트 취약점 데이터 블록입니다. 이 데이터 블록에 대한 설명은 4.9.0 이상 버전용 호스트 취약점 데이터 블록, 페이지 4-114의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	서드파티 취약점 스캔 데이터를 전달하는 호스트 취약점 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.

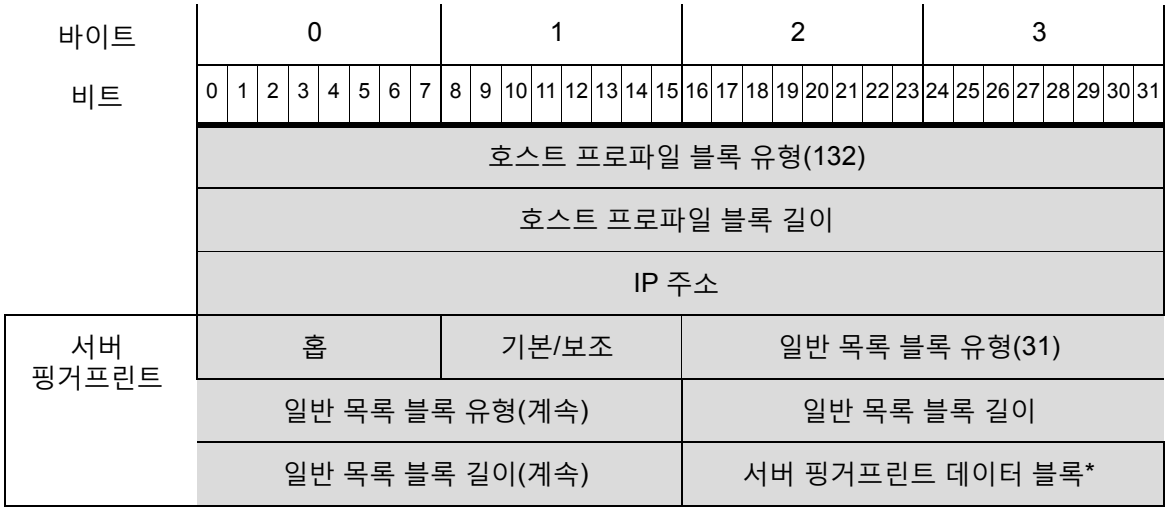
표 B-51 5.2.x 버전용 전체 호스트 프로파일 레코드 필드 (계속)

필드	데이터 유형	설명
(서드파티 스캔) 호스트 취약점 데이터 블록*	variable	서드파티 스캐너에서 제공한 호스트 취약점 데이터 블록입니다. 이러한 데이터 블록의 호스트 취약점 ID는 Cisco에서 탐지한 ID가 아니라 서드파티 스캐너 ID입니다. 이 데이터 블록에 대한 설명은 4.9.0 이상 버전용 호스트 취약점 데이터 블록, 페이지 4-114의 내용을 참조하십시오.
목록 블록 유형	uint32	속성 데이터를 전달하는 속성값 데이터 블록으로 구성된 목록 데이터 블록을 시작합니다. 이 값은 항상 11입니다.
목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 데이터 블록을 포함한 목록 데이터 블록의 바이트 수입니다.
속성값 데이터 블록*	variable	속성값 데이터 블록의 목록입니다. 이 목록의 데이터 블록에 대한 설명은 속성값 데이터 블록, 페이지 4-83의 내용을 참조하십시오.
모바일	uint8	운영 체제가 모바일 디바이스에서 실행되고 있는지를 나타내는 true-false 플래그입니다.
탈옥됨	uint8	모바일 디바이스의 운영 체제가 탈옥되었는지 나타내는 true-false 플래그입니다.

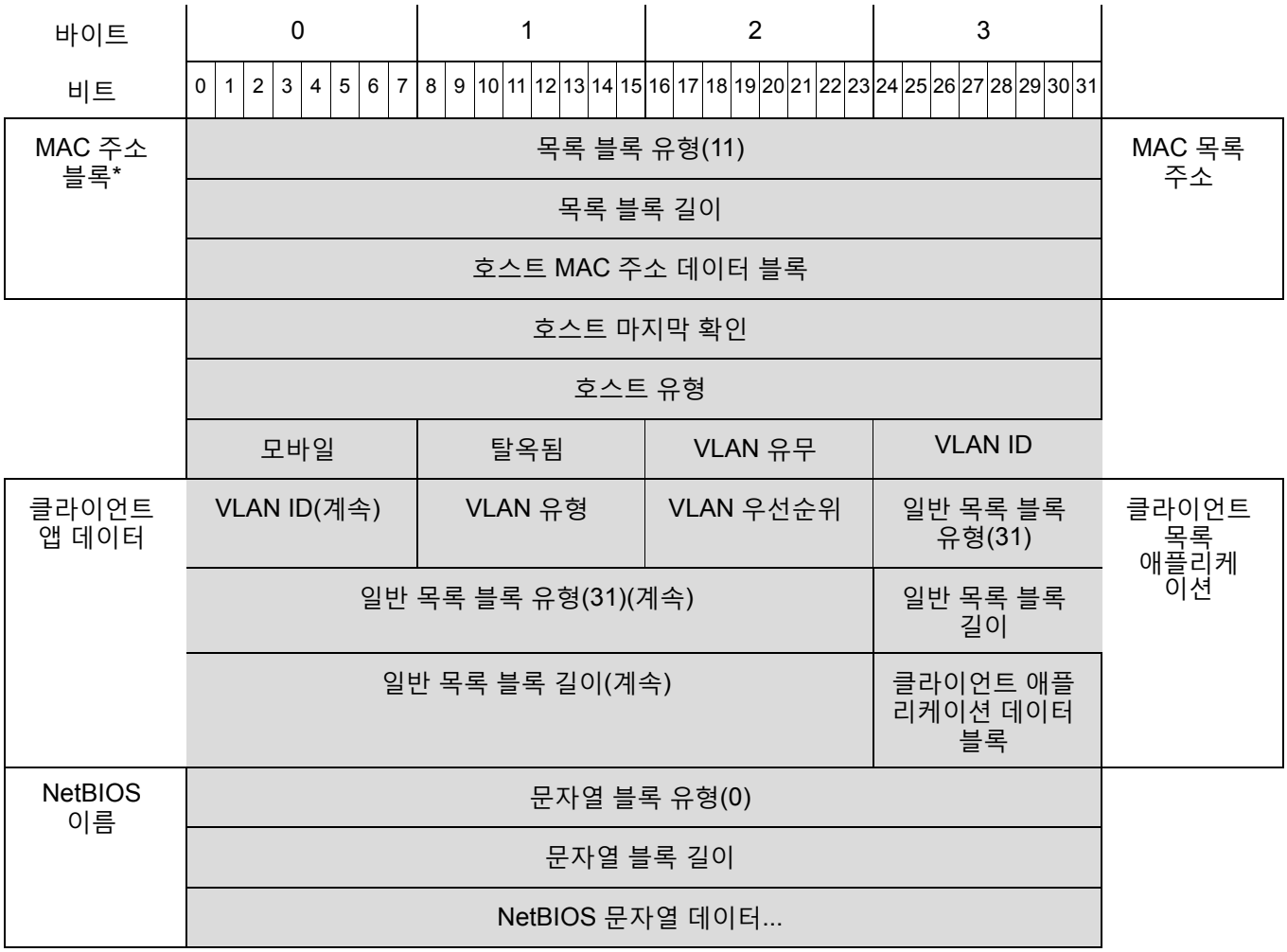
5.1.x 버전용 호스트 프로파일 데이터 블록

다음 다이어그램에 호스트 프로파일 데이터 블록의 형식이 나와 있습니다. 또한 이 데이터 블록은 호스트 임계성 값은 포함하지 않지만 VLAN 유무 표시기는 포함합니다. 그리고 이 데이터 블록은 호스트의 NetBIOS 이름을 전달할 수 있습니다. 호스트 프로파일 데이터 블록의 블록 유형은 132입니다.

참고 이 다이어그램에서 블록 유형 필드 옆에 있는 별표(*)는 메시지가 계열 1 데이터 블록 인스턴스를 포함하지 않을 수도 있고 하나 이상 포함할 수도 있음을 나타냅니다.



바이트	0								1								2								3									
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31		
클라이언트 핑거프린트	일반 목록 블록 유형(31)																																	
	일반 목록 블록 길이																																	
	클라이언트 핑거프린트 데이터 블록*																																	
SMB 핑거프린트	일반 목록 블록 유형(31)																																	
	일반 목록 블록 길이																																	
	SMB 핑거프린트 데이터 블록*																																	
DHCP 핑거프린트	일반 목록 블록 유형(31)																																	
	일반 목록 블록 길이																																	
	DHCP 핑거프린트 데이터 블록*																																	
모바일 디바이스 핑거프린트	일반 목록 블록 유형(31)																																	
	일반 목록 블록 길이																																	
	모바일 디바이스 핑거프린트 데이터 블록*																																	
TCP 서버 블록*	목록 블록 유형(11)																																TCP 목록 서버	
	목록 블록 길이																																	
	TCP 서버 데이터 블록																																	
UDP 서버 블록*	목록 블록 유형(11)																																UDP 목록 서버	
	목록 블록 길이																																	
	UDP 서버 데이터 블록																																	
네트워크 프로토콜 블록*	목록 블록 유형(11)																																네트워크 목록 프로토콜	
	목록 블록 길이																																	
	네트워크 프로토콜 데이터 블록																																	
전송 프로토콜 블록*	목록 블록 유형(11)																																전송 목록 프로토콜	
	목록 블록 길이																																	
	전송 프로토콜 데이터 블록																																	



다음 표에는 5.1.x 버전에서 반환되는 호스트 프로파일 데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 B-52 5.1.x 버전용 호스트 프로파일 데이터 블록 필드

필드	데이터 유형	설명
호스트프로파일 블록 유형	uint32	5.1.x 버전용 호스트 프로파일 데이터 블록을 시작합니다. 이 값은 항상 132입니다.
호스트프로파일 블록 길이	uint32	호스트 프로파일 데이터 블록의 바이트 수입니다. 여기에는 호스트 프로파일 블록 유형 및 길이 필드의 8바이트에 그 뒤의 호스트 프로파일 데이터에 포함된 바이트 수를 더한 값이 포함됩니다.
IP 주소	uint8[4]	프로파일에서 설명하는 호스트의 IP 주소(IP 주소 옥텟 형식)입니다.
홉	uint8	호스트에서 디바이스로의 홉 수입니다.

표 B-52 5.1.x 버전용 호스트 프로파일 데이터 블록 필드 (계속)

필드	데이터 유형	설명
기본/보조	uint8	호스트가 호스트를 탐지한 디바이스의 기본 네트워크에 있는지 아니면 보조 네트워크에 있는지를 나타냅니다. • 0 - 호스트가 기본 네트워크에 있습니다. • 1 - 호스트가 보조 네트워크에 있습니다.
일반 목록 블록 유형	uint32	서버 핑거프린트를 사용하여 식별된 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
운영 체제 핑거프린트(서버 핑거프린트) 데이터 블록*	variable	서버 핑거프린트를 사용하여 식별된 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 페이지 4-161의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	클라이언트 핑거프린트를 사용하여 식별된 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
운영 체제 핑거프린트(클라이언트 핑거프린트) 데이터 블록*	variable	클라이언트 핑거프린트를 사용하여 식별된 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 페이지 4-161의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	SMB 핑거프린트를 사용하여 식별된 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
운영 체제 핑거프린트(SMB 핑거프린트) 데이터 블록*	variable	SMB 핑거프린트를 사용하여 식별된 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 페이지 4-161의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	DHCP 핑거프린트를 사용하여 식별된 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
운영 체제 핑거프린트(DHCP 핑거프린트) 데이터 블록*	variable	DHCP 핑거프린트를 사용하여 식별된 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 페이지 4-161의 내용을 참조하십시오.
일반 목록 블록 유형	uint32	DHCP 핑거프린트를 사용하여 식별된 핑거프린트 데이터를 전달하는 운영 체제 핑거프린트 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.

표 B-52 5.1.x 버전용 호스트 프로파일 데이터 블록 필드 (계속)

필드	데이터 유형	설명
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 운영 체제 핑거프린트 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
운영 체제 핑거프린트(모바일 디바이스 핑거프린트)데이터 블록*	variable	모바일 디바이스 핑거프린트를 사용하여 식별된 호스트의 운영 체제에 대한 정보를 포함하는 운영 체제 핑거프린트 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.1 이상 버전용 운영 체제 핑거프린트 데이터 블록, 페이지 4-161의 내용을 참조하십시오.
목록 블록 유형	uint32	TCP 서버 데이터를 전달하는 서버 데이터 블록으로 구성된 목록 데이터 블록을 시작합니다. 이 값은 항상 11입니다.
목록 블록 길이	uint32	목록의 바이트 수입니다. 이 수에는 목록 블록 유형 및 길이 필드의 8바이트에 캡슐화된 모든 서버 데이터 블록을 더한 값이 포함됩니다. 이 필드 뒤에는 서버 데이터 블록이 없을 수도 있고 하나 이상 올 수도 있습니다.
TCP 서버 데이터 블록	variable	이전 버전 제품에 설명되어 있는 TCP 서버를 설명하는 호스트 서버 데이터 블록입니다.
목록 블록 유형	uint32	UDP 서버 데이터를 전달하는 서버 데이터 블록으로 구성된 목록 데이터 블록을 시작합니다. 이 값은 항상 11입니다.
목록 블록 길이	uint32	목록의 바이트 수입니다. 이 수에는 목록 블록 유형 및 길이 필드의 8바이트에 캡슐화된 모든 서버 데이터 블록을 더한 값이 포함됩니다. 이 필드 뒤에는 서버 데이터 블록이 없을 수도 있고 하나 이상 올 수도 있습니다.
UDP 서버 데이터 블록	uint32	이전 버전 제품에 설명되어 있는 UDP 서버를 설명하는 호스트 서버 데이터 블록입니다.
목록 블록 유형	uint32	네트워크 프로토콜 데이터를 전달하는 프로토콜 데이터 블록으로 구성된 목록 데이터 블록을 시작합니다. 이 값은 항상 11입니다.
목록 블록 길이	uint32	목록의 바이트 수입니다. 이 수에는 목록 블록 유형 및 길이 필드의 8바이트에 캡슐화된 모든 프로토콜 데이터 블록을 더한 값이 포함됩니다. 이 필드 뒤에는 프로토콜 데이터 블록이 없을 수도 있고 하나 이상 올 수도 있습니다.
네트워크 프로토콜 데이터 블록	uint32	네트워크 프로토콜을 설명하는 프로토콜 데이터 블록입니다. 이 데이터 블록에 대한 설명은 프로토콜 데이터 블록, 페이지 4-77의 내용을 참조하십시오.
목록 블록 유형	uint32	전송 프로토콜 데이터를 전달하는 프로토콜 데이터 블록으로 구성된 목록 데이터 블록을 시작합니다. 이 값은 항상 11입니다.
목록 블록 길이	uint32	목록의 바이트 수입니다. 이 수에는 목록 블록 유형 및 길이 필드의 8바이트에 캡슐화된 모든 프로토콜 데이터 블록을 더한 값이 포함됩니다. 이 필드 뒤에는 전송 프로토콜 데이터 블록이 없을 수도 있고 하나 이상 올 수도 있습니다.

표 B-52 5.1.x 버전용 호스트 프로파일 데이터 블록 필드 (계속)

필드	데이터 유형	설명
전송 프로토콜 데이터 블록	uint32	전송 프로토콜을 설명하는 프로토콜 데이터 블록입니다. 이 데이터 블록에 대한 설명은 프로토콜 데이터 블록, 페이지 4-77의 내용을 참조하십시오.
목록 블록 유형	uint32	MAC 주소 데이터 블록으로 구성된 목록 데이터 블록을 시작합니다. 이 값은 항상 11입니다.
목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 MAC 주소 데이터 블록을 포함한 목록의 바이트 수입니다.
호스트 MAC 주소 데이터 블록	uint32	호스트 MAC 주소를 설명하는 호스트 MAC 주소 데이터 블록입니다. 이 데이터 블록에 대한 설명은 4.9 이상 버전용 호스트 MAC 주소, 페이지 4-117의 내용을 참조하십시오.
호스트 마지막 확인	uint32	시스템이 호스트 활동을 마지막으로 탐지한 시간을 나타내는 UNIX 타임스탬프입니다.
호스트 유형	uint32	호스트 유형을 나타냅니다. 다음 값이 표시될 수 있습니다. • 0 - 호스트 • 1 - 라우터 • 2 - 브리지 • 3 - NAT 디바이스 • 4 - LB(로드 밸런서)
모바일	uint8	호스트가 모바일 디바이스인지를 나타내는 true-false 플래그입니다.
탈옥됨	uint8	호스트가 탈옥도 된 모바일 디바이스인지를 나타내는 true-false 플래그입니다.
VLAN 유무	uint8	VLAN의 유무를 나타냅니다. • 0 - 예 • 1 - 아니요
VLAN ID	uint16	호스트가 구성원으로 포함된 VLAN을 나타내는 VLAN ID 번호입니다.
VLAN 유형	uint8	VLAN 태그에 캡슐화된 패킷 유형입니다.
VLAN 우선순위	uint8	VLAN 태그에 포함된 우선순위 값입니다.
일반 목록 블록 유형	uint32	클라이언트 애플리케이션 데이터를 전달하는 클라이언트 애플리케이션 데이터 블록으로 구성된 일반 목록 데이터 블록을 시작합니다. 이 값은 항상 31입니다.
일반 목록 블록 길이	uint32	목록 헤더 및 캡슐화된 모든 클라이언트 애플리케이션 데이터 블록을 포함한 일반 목록 데이터 블록의 바이트 수입니다.
클라이언트 애플리케이션 데이터 블록	uint32	클라이언트 애플리케이션을 설명하는 클라이언트 애플리케이션 데이터 블록입니다. 이 데이터 블록에 대한 설명은 5.0 이상 버전용 전체 호스트 클라이언트 애플리케이션 데이터 블록, 페이지 4-154의 내용을 참조하십시오.

표 B-52 5.1.x 버전용 호스트 프로파일 데이터 블록 필드 (계속)

필드	데이터 유형	설명
문자열 블록 유형	uint32	NetBIOS 이름에 대한 문자열 데이터 블록을 시작합니다. 이 값은 문자열 데이터를 나타내는 0으로 설정됩니다.
문자열 블록 길이	uint32	NetBIOS 이름 데이터 블록의 바이트 수를 나타냅니다. 여기에는 문자열 블록 유형 및 길이의 8바이트에 NetBIOS 이름의 바이트 수를 더한 값이 포함됩니다.
NetBIOS 문자열 데이터	variable	호스트 프로파일에 설명되어 있는 호스트의 NetBIOS 이름을 포함합니다.

5.0~5.1.1.x 버전용 IP 범위 사양 데이터 블록

IP 범위 사양 데이터 블록은 IP 주소 범위를 전달하며 사용자 프로토콜, 사용자 클라이언트 애플리케이션, 주소 사양, 사용자 제품, 사용자 서버, 사용자 호스트, 사용자 취약점, 사용자 임계성 및 사용자 속성값 데이터 블록에 사용됩니다. IP 범위 사양 데이터 블록의 블록 유형은 61입니다.

다음 다이어그램에 IP 범위 사양 데이터 블록의 형식이 나와 있습니다.

다음 표에는 IP 범위 사양 데이터 블록의 구성 요소에 대한 설명이 나와 있습니다.

표 B-53 IP 범위 사양 데이터 블록 필드

필드	데이터 유형	설명
IP 범위 사양 블록 유형	uint32	IP 범위 사양 데이터 블록을 시작합니다. 이 값은 항상 61입니다.
IP 범위 사양 블록 길이	uint32	IP 범위 사양 데이터 블록의 총 바이트 수입니다. 여기에는 IP 범위 사양 블록 유형 및 길이 필드의 8바이트에 그 뒤의 IP 범위 사양 데이터 바이트 수를 더한 값이 포함됩니다.
IP 범위 사양 시작	uint32	IP 주소 범위의 시작 IP 주소입니다.
IP 범위 사양 끝	uint32	IP 주소 범위의 끝 IP 주소입니다.

액세스 제어 정책 규칙 이유 데이터 블록

eStreamer 서비스는 액세스 제어 규칙 정책 규칙 이유 데이터 블록을 사용하여 액세스 제어 정책 규칙 ID에 대한 정보를 포함합니다. 계열 2에서 이 데이터 블록의 블록 유형은 21입니다.

다음 다이어그램에 액세스 제어 정책 규칙 ID 메타데이터 블록의 구조가 나와 있습니다.

바이트	0								1								2								3							
비트	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	액세스 제어 정책 규칙 이유 데이터 블록 유형(21)																															
	액세스 제어 정책 규칙 이유 데이터 블록 길이																															
설명	이유																문자열 블록 유형(0)															
	문자열 블록 유형(0)(계속)																문자열 블록 길이															
	문자열 블록 길이(계속)																설명...															

다음 표에는 액세스 제어 정책 규칙 ID 메타데이터 블록의 필드에 대한 설명이 나와 있습니다.

표 B-54 액세스 제어 정책 규칙 이유 데이터 블록 필드

필드	데이터 유형	설명
액세스 제어 정책 규칙 이유 데이터 블록 유형	uint32	액세스 제어 정책 규칙 이유 데이터 블록을 시작합니다. 이 값은 항상 21입니다.
액세스 제어 정책 규칙 이유 데이터 블록 길이	uint32	액세스 제어 정책 규칙 이유 데이터 블록의 총 바이트 수입니다. 여기에는 액세스 제어 정책 규칙 이유 데이터 블록 유형 및 길이 필드의 8바이트에 그 뒤의 데이터 바이트 수를 더한 값이 포함됩니다.
이유	uint16	이벤트를 트리거한 규칙에 대한 이유 번호입니다.
문자열 블록 유형	uint32	액세스 제어 정책 규칙 이유의 설명이 포함된 문자열 데이터 블록을 시작합니다. 이 값은 항상 0입니다.
문자열 블록 길이	uint32	이름 문자열 데이터 블록에 포함된 바이트 수입니다. 여기에는 블록 유형과 헤더 필드의 8바이트에 Description(설명) 필드의 바이트 수를 더한 값이 포함됩니다.
설명	string	규칙에 대한 이유의 설명입니다.

색 인

숫자

B

E

I

M

N

O

T

U

V

ㄱ

ㄴ

ㄷ

ㅁ

ㅂ

ㅅ

ㅇ

ㅈ

ㅊ

ㅋ

ㅍ

ㅎ