

ESA에서 CEF 로그 항목 및 CEF 헤더 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[구성](#)

[CEF 로그 항목](#)

[수신/발신 콘텐츠 필터 추가](#)

[통합 이벤트 로그 서브스크립션에 CEF 로그 항목 추가](#)

[CEF 헤더](#)

[기록할 CEF 헤더를 추가합니다.](#)

[통합 이벤트 로그 서브스크립션에 CEF 로그 항목 추가](#)

[관련 정보](#)

소개

이 문서에서는 Cisco SEG(Secure Email Gateway)의 CEF(Common Event Format) 로그 항목 및 헤더에 대한 컨피그레이션을 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 항목에 대한 지식을 권장합니다.

- Cisco Secure Email Gateway/Email Security Appliance(SEG/ESA)
- 콘텐츠 필터 지식
- 로그 서브스크립션 정보

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Email Security Appliance 버전 14.3

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

Consolidated Event Logs(통합 이벤트 로그)는 각 메시지 이벤트를 단일 로그 라인으로 요약합니다. 분석을 위해 SIEM(Security Information and Event Management) 공급업체 또는 애플리케이션으로 전송되는 데이터(로그 정보)의 바이트 수를 줄이려면 이 로그 유형을 사용합니다. 로그는 대부분의 SIEM 공급업체에서 널리 사용하는 CEF 로그 메시지 형식입니다.

CEF Log Entry(CEF 로그 항목) 및 CEF Headers(CEF 헤더)가 추가되어 메일 이벤트를 추적 및 구성하는 데 필요한 추가 정보를 제공합니다.

구성

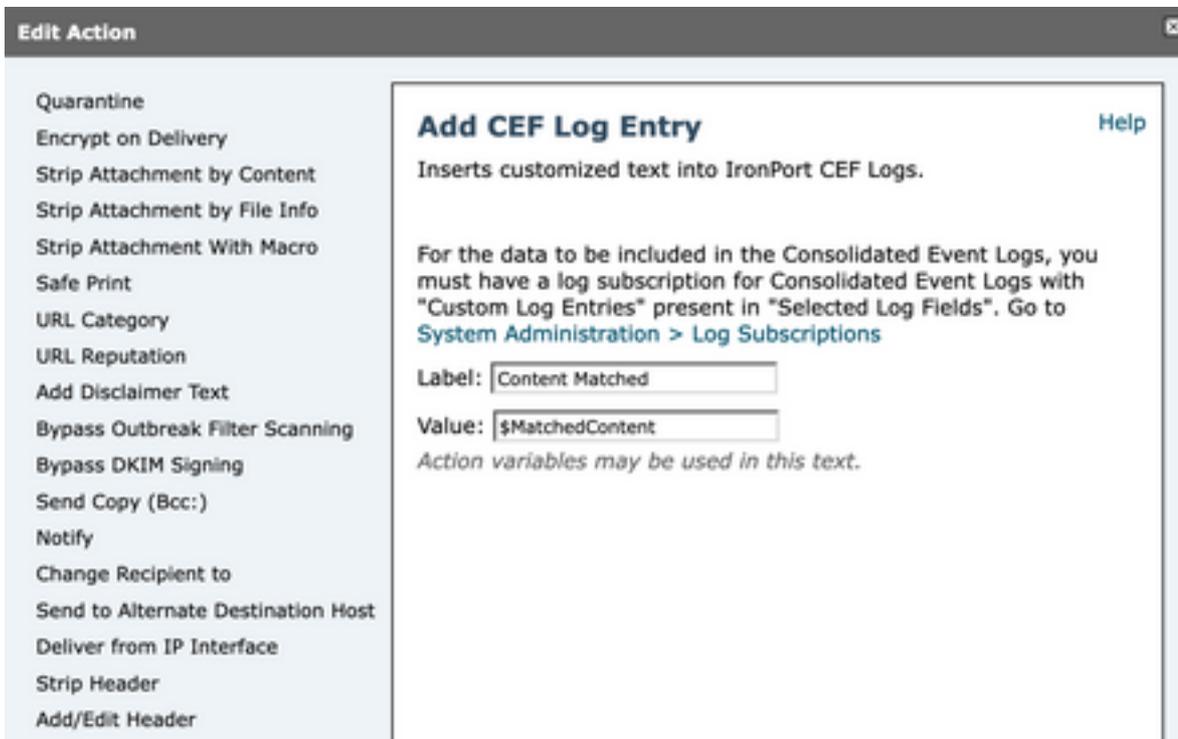
CEF 로그 항목

수신/발신 콘텐츠 필터 추가

먼저 ESA에서 콘텐츠 필터를 생성합니다.

1. 이동 Mail Policies > Incoming/Outgoing content filters
2. 클릭 Add Filter
3. 필터 이름 지정
4. 원하는 조건 추가
5. 클릭 Add Action
6. 선택 Add CEF Log Entry
7. 레이블의 이름을 지정하고 Action Variables 값 상자
8. Submit and Commit

이 문서에서는 \$MatchedContent 그림과 같은 작업 변수:



로그 항목 작업

콘텐츠 필터의 CEF

통합 이벤트 로그 서브스크립션에 CEF 로그 항목 추가

다음으로, 이전에 생성한 CEF 로그 항목을 추가하려면 Consolidated Event Log Subscription을 생

성하거나 수정합니다.

1. 이동 **System Administration > Log Subscriptions**
2. 통합 이벤트 로그 추가 또는 선택
3. 선택 **Custom Log Entries** 을 클릭하고 **Add**
4. **Submit and Commit**

Log Subscription

Log Type: Consolidated Event Logs

Log Name: CEF_test
(will be used to name the log directory)

Log Fields:

Available Log Fields:

- AV Verdict
- Content Filters Verdict
- Custom Log Headers
- DANE Host
- DANE Status
- DCID Timestamp
- DMA IP
- DKIM Verdict
- DLP Verdict
- DMARC Verdict
- Data IP
- File(s) Details
- Friendly From
- Graymail Verdict
- SCID Timestamp
- Listener Name
- Mail Direction

Selected Log Fields:

- Serial Number
- MID
- SCID
- DCID
- Custom Log Entries

Buttons: Add >, < Remove, Move Up, Move Down

립션의 사용자 지정 로그 항목

CEF 로그 서브스크

CEF 헤더

기록할 CEF 헤더를 추가합니다.

먼저 ESA에 CEF 헤더를 추가합니다

1. 이동 **System Administration > Logs Subscription**
2. 클릭 **Edit Settings** 전역 설정에서
3. CEF Headers 아래에서 기록할 헤더를 나열합니다
4. **Submit and Commit**

Log Subscriptions Global Settings

Mode --Cluster: Hosted_Cluster

Change Mode...

Centralized Management Options

Edit Global Settings

System metrics frequency: 60 seconds

Logging Options:

- Message-ID headers in Mail Logs
- Original subject header of each message
- Remote response text in Mail Logs

Headers (Optional): List any headers you want to record in the log files:

- X-IronPort-Anti-Spam-Result, To, From, Reply-To, Sender, X-IronPort-Anti-Spam-Result

CEF Headers (Optional): List any headers you want to record in the CEF log files:

- Message-ID, Mime-version, Content-type, Content-disposition, Content-transfer-encoding, Thread-Topic, Thread-Index, X-IronPort-Anti-Spam-Result, To, From, Reply-To, Sender

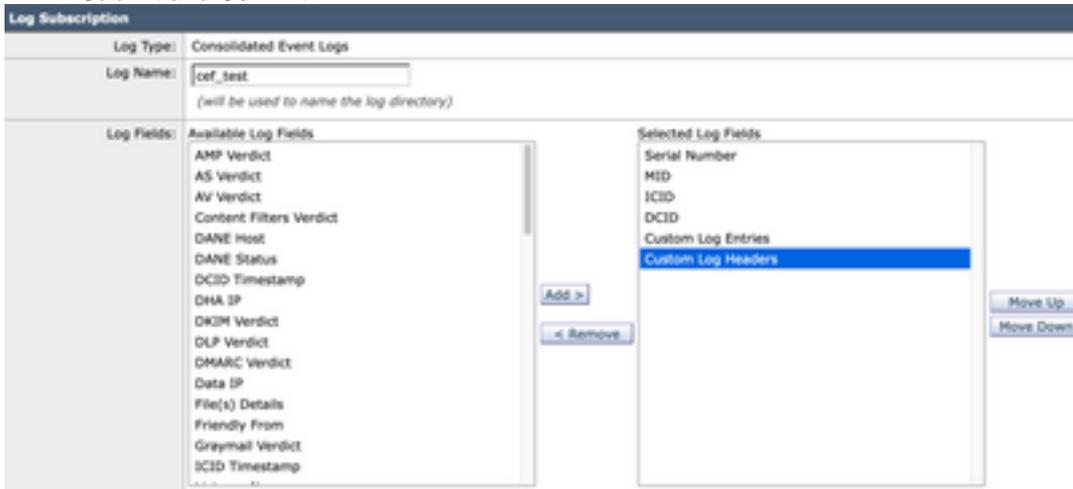
Buttons: Cancel, Submit

CEF 헤더 컨피그레이션

통합 이벤트 로그 서브스크립션에 CEF 로그 항목 추가

그런 다음 통합 이벤트 로그 서브스크립션을 생성하거나 수정하여 이전에 기록된 CEF 헤더를 추가합니다.

1. 이동 System Administration > Logs Subscription
2. 통합 이벤트 로그 추가 또는 선택
3. 선택 Custom Log Entries 을 클릭하고 Add
4. Submit and Commit



CEF 로그 헤더

CEF 로그 서브스크립션의

관련 정보

- [최종 사용자 설명서 ESA 14.3](#)
- [릴리스 정보 ESA 14.3](#)
- [Technical Support - Cisco Systems](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.