CEF-Protokolleintrag und CEF-Header in der ESA konfigurieren

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration für CEF-Protokolleinträge und -Header (Common Event Format) für Cisco Secure Email Gateway (SEG) beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, sich mit folgenden Themen vertraut zu machen:

- Cisco Secure Email Gateway/E-Mail Security Appliance (SEG/ESA)
- Kenntnisse zu Content-Filtern
- Kenntnisse zu Protokoll-Abonnements

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Email Security Appliance Version 14.3

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

Die konsolidierten Ereignisprotokolle fassen jedes Nachrichtenereignis in einer einzigen Protokollzeile zusammen. Verwenden Sie diesen Protokolltyp, um die Anzahl der Byte an Daten (Protokollinformationen) zu reduzieren, die zur Analyse an einen SIEM-Anbieter (Security Information and Event Management) oder eine SIEM-Anwendung gesendet werden. Die Protokolle haben das CEF-Protokollnachrichtenformat, das von den meisten SIEM-Anbietern häufig verwendet wird.

CEF-Protokolleintrag und CEF-Header werden hinzugefügt, um zusätzliche Informationen zum Nachverfolgen und Organisieren von E-Mail-Ereignissen bereitzustellen.

Konfigurieren

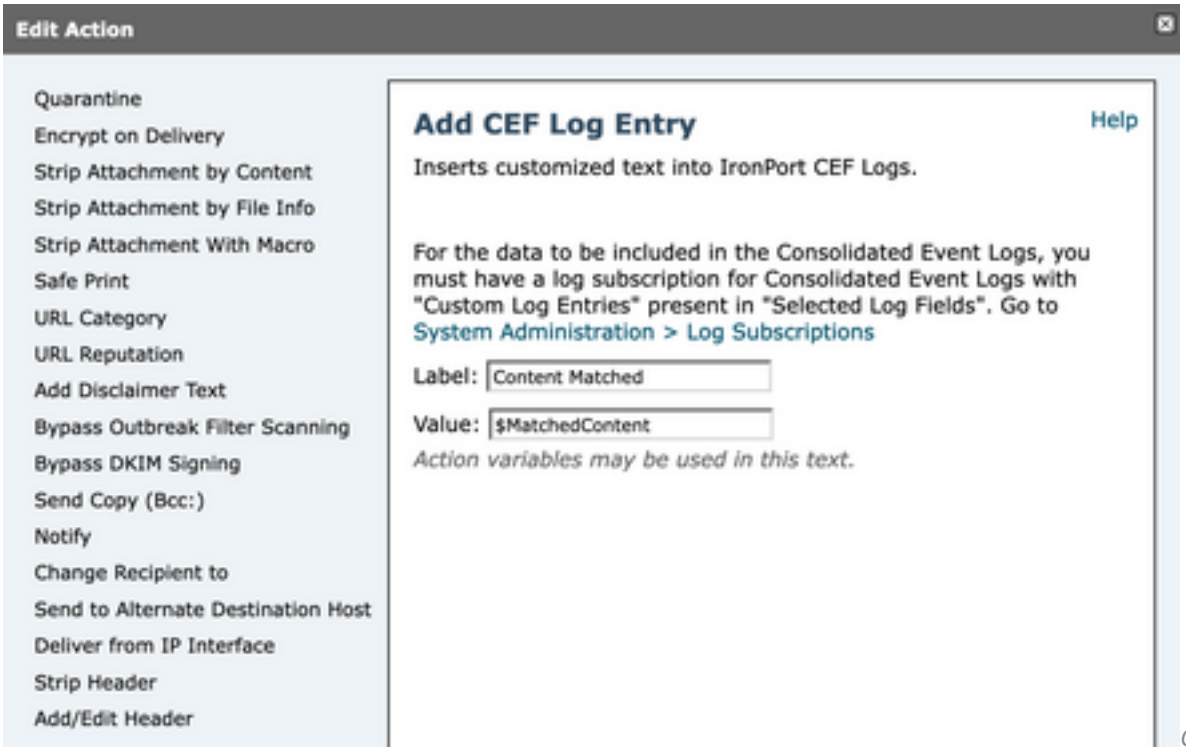
CEF-Protokolleintrag

Hinzufügen des eingehenden/ausgehenden Content-Filters

Erstellen Sie zunächst den Content-Filter auf der ESA:

1. Gehe zu **Mail Policies > Incoming/Outgoing content filters**
2. Klicken Sie in **Add Filter**
3. Filter benennen
4. Bedingung hinzugefügt
5. Klicken Sie in **Add Action**
6. Auswählen **Add CEF Log Entry**
7. Benennen Sie das Label, und verwenden Sie **Action Variables** für das Wertfeld
8. **Submit and Commit**

Dieses Dokumentationsbeispiel verwenden wir **$MatchedContent** Aktionsvariable, wie im Bild gezeigt:



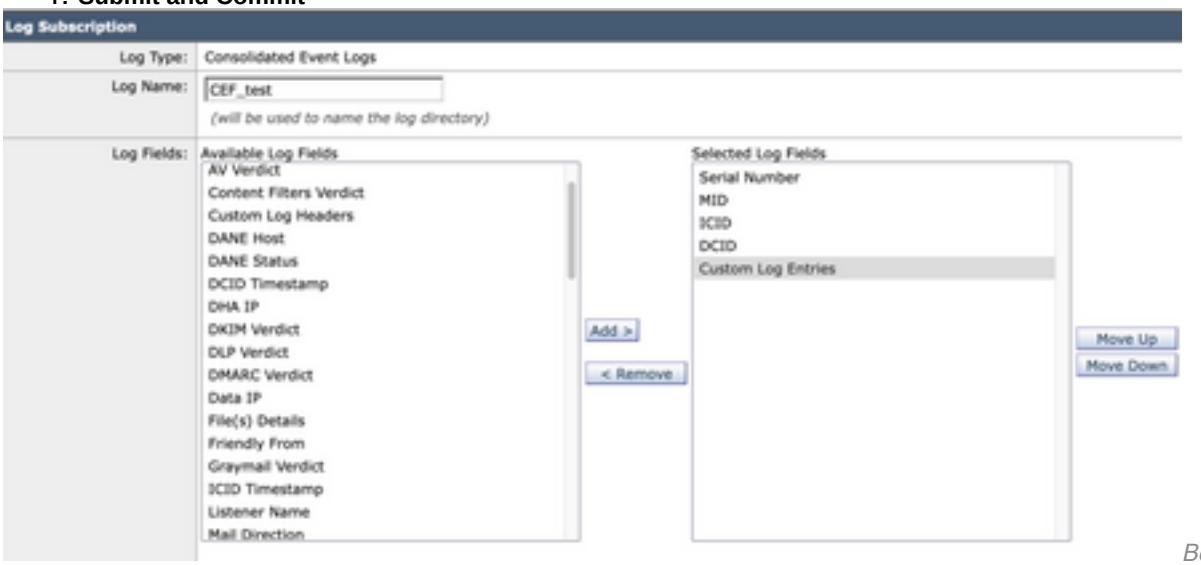
CEF-

Protokolleintragsaktion in Content-Filtern

Hinzufügen eines CEF-Protokolleintrags im Abonnement für das konsolidierte Ereignisprotokoll

Erstellen oder ändern Sie anschließend das Consolidated Event Log Subscription, um den zuvor erstellten CEF-Protokolleintrag hinzuzufügen:

1. Gehe zu **System Administration > Log Subscriptions**
2. Hinzufügen oder Auswählen der konsolidierten Ereignisprotokolle
3. Auswählen **Custom Log Entries** und klicke auf **Add**
4. **Submit and Commit**



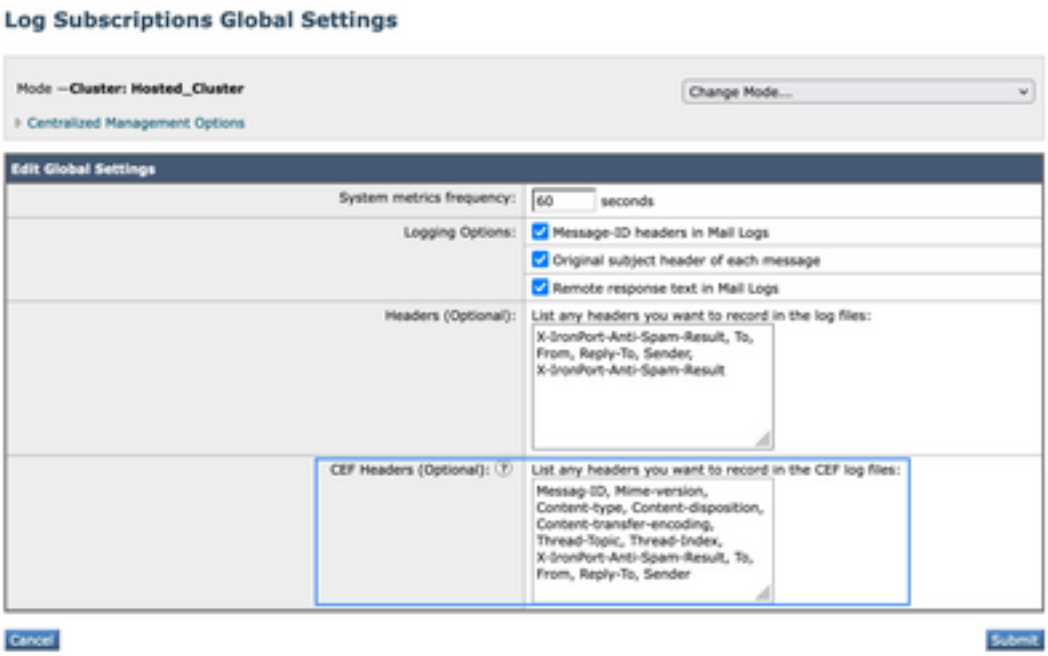
Benutzerdefinierte Protokolleinträge in CEF-Protokoll-Subscription

CEF-Header

Fügen Sie die zu protokollierenden CEF-Header hinzu:

Fügen Sie zunächst die CEF-Header in der ESA hinzu.

1. Gehe zu **System Administration > Logs Subscription**
2. Klicken Sie in **Edit Settings** unter Globale Einstellungen
3. Listen Sie unter CEF-Header die zu protokollierenden Header auf.
4. **Submit and Commit**

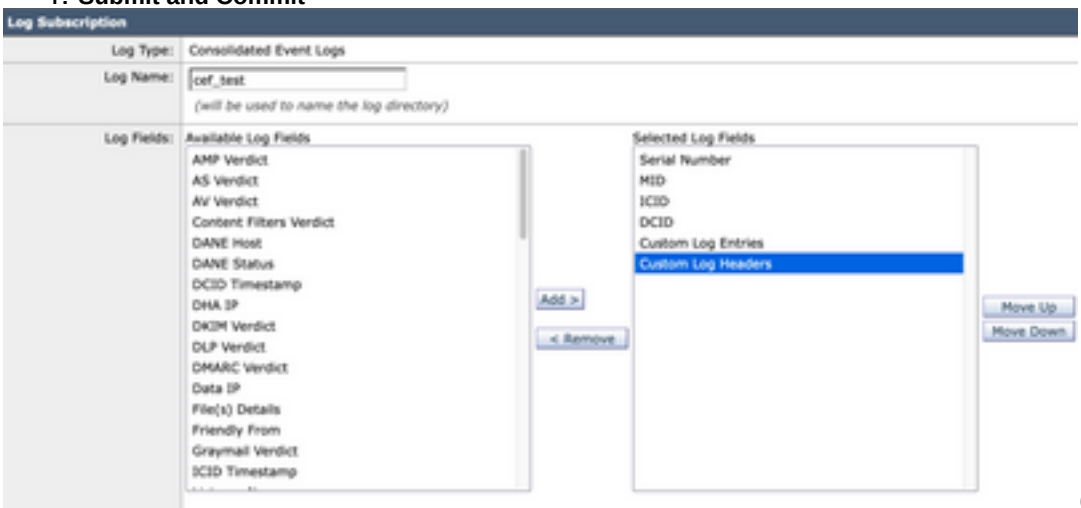


Konfiguration der CEF-Header

Hinzufügen eines CEF-Protokolleintrags im Abonnement für das konsolidierte Ereignisprotokoll

Erstellen oder ändern Sie anschließend das Abonnement für das konsolidierte Ereignisprotokoll, um die zuvor aufgezeichneten CEF-Header hinzuzufügen:

1. Gehe zu **System Administration > Logs Subscription**
2. Hinzufügen oder Auswählen der konsolidierten Ereignisprotokolle
3. Auswählen **Custom Log Entries** und klicke auf **Add**
4. **Submit and Commit**



CEF-Protokoll-Header in CEF-Protokoll-Subscription

Zugehörige Informationen

- Benutzerhandbuch ESVG 14.3
- Versionshinweise ESA 14.3
- Technischer Support – Cisco Systems

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.