

Content-Filter konfigurieren, um leere Betreff-E-Mails auszulösen

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Erstellen des Filters für eingehende Inhalte](#)

[Content-Filter zur Richtlinie für eingehende E-Mails hinzufügen](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie einen Content-Filter erstellen, um E-Mails mit einer leeren/leeren Betreffzeile zu identifizieren und Aktionen auszulösen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen.

- Cisco Secure Email Gateway (SEG/ESA)
- Kenntnisse zu Content-Filtern

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen.

- Cisco Secure Email Gateway (SEG/ESA) 14.0 und neuere Versionen

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 kennen.

Hintergrundinformationen

Je nach den Anforderungen Ihres Unternehmens können Sie Aktionen für Nachrichten auslösen, die über einen leeren Betreff-Header verfügen.

Konfigurieren

Erstellen des Filters für eingehende Inhalte

Erstellen Sie den Content-Filter in der ESA:

1. Navigieren Sie zu Mail-Policys > Filter für eingehende Inhalte.
2. Klicken Sie auf Filter hinzufügen.
3. Nennen Sie den Filter.
4. Verwenden Sie die Bedingung Betreff-Header.
5. Wählen Sie die Bedingung Equals aus.
6. Verwenden Sie diese Zeichen im Feld ^\$.
7. Klicken Sie auf OK.
8. Fügen Sie die Aktion entsprechend Ihrer Bequemlichkeit und Anforderungen hinzu.
9. Änderungen einsenden und bestätigen.

Edit Condition

- Message Body or Attachment
 - Message Body
 - URL Category
 - URL Reputation
 - Message Size
 - Message Language
 - Macro Detection
 - Attachment Content
 - Attachment File Info
 - Attachment Protection
- Subject Header**
- Other Header
 - Envelope Sender
 - Envelope Recipient
 - Receiving Listener
 - Remote IP/Hostname
 - Reputation Score
 - Domain Reputation
 - DKIM Authentication
 - Forged Email Detection
 - SPF Verification
 - S/MIME Gateway Message
 - S/MIME Gateway Verified
 - Duplicate Boundaries Verification
 - Geolocation

Subject Header [Help](#)

Does the subject header contain text that matches a specified pattern or match a term in a dictionary?

Subject Header:

Equals

Contains term in content dictionary:

TestFrom

Bedingung für Content-Filter

Beispiel für Content-Filter:

In diesem Beispiel für den Inhaltsfilter wird die Bedingung wie im Dokument beschrieben eingerichtet, und eine Aktion zum Hinzufügen eines Protokolleintrags wird ausgelöst, wenn ein eingehender Betreff-Header für E-Mails leer ist. Das Ergebnis wird in den Nachrichtenverfolgungsdetails protokolliert.

Edit Incoming Content Filter

Mode — Cluster: test Change Mode...

Centralized Management Options

Content Filter Settings

Name:	<input type="text" value="blank_subject"/>
Currently Used by Policies:	Default Policy
Description:	<input type="text"/>

Conditions

Order	Condition	Rule	Delete
1	Subject Header	subject == ""	<input type="button" value="Delete"/>

Actions

Order	Action	Rule	Delete
1	Add Log Entry	log-entry("Blank Subject")	<input type="button" value="Delete"/>

Beispiel für Content-Filter

Content-Filter zur Richtlinie für eingehende E-Mails hinzufügen

Nachdem Sie den Content-Filter in der ESA erstellt haben, müssen Sie sicherstellen, dass Sie ihn in Ihrer Mail-Richtlinie für eingehende E-Mails aktivieren.

1. Navigieren Sie in der ESA-GUI zu Mail-Policys > Mail-Policys für "Eingehend".
2. Wählen Sie die Richtlinie aus, mit der Ihr Content-Filter funktioniert. Verwenden Sie in diesem Fall die Standardrichtlinie.
3. Navigieren Sie zur 7. Spalte, die mit den Inhaltsfiltern verknüpft ist, und klicken Sie auf die Felder, die in dieser Spalte angezeigt werden.
4. Wählen Sie die Option Content-Filter aktivieren (Einstellungen anpassen) und dann den Content-Filter aus, den Sie in dieser Richtlinie aktivieren möchten.
5. Klicken Sie auf Senden und dann auf Änderungen bestätigen.

Zugehörige Informationen

- [Cisco Email Encryption-Benutzerhandbücher](#)

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.