

Content-Filter verwenden, um E-Mails an die Spam-Quarantäne in der ESA weiterzuleiten

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird die Konfiguration zum Umleiten von E-Mails, die nicht als Spam markiert sind, in die Spam-Quarantäne beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, sich mit folgenden Themen vertraut zu machen:

- Cisco Secure Email Gateway (SEG/ESA)
- Kenntnisse zu Content-Filtern
- Wissen in Quarantäne
- Wissen über die Spam-Quarantäne

Verwendete Komponenten

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

- E-Mail Security Appliance

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

Der Zweck der Spam-Quarantäne besteht darin, als Spam markierte E-Mails in Quarantäne zu stellen. In Bezug auf Ihre Unternehmensanforderungen können Sie jedoch E-Mails, die nicht als

Spam klassifiziert sind, an die Spam-Quarantäne umleiten.

Achtung: Stellen Sie sicher, dass Sie mit dem Quarantänezugriff für Endbenutzer vertraut sind.

Konfigurieren

Erstellen Sie den Content-Filter auf der ESA:

1. Navigieren Sie zu **Mail Policies > Incoming/Outgoing content filters**
2. Klicken Sie auf **Add Filter**
3. Filter benennen
4. Bedingung gewünscht und hinzugefügt
5. Klicken Sie auf **Add Action**
6. Auswählen **Add/Edit Header**
7. Nutzung **x-IronPort-Quarantine** für die **Header Name** Wertschöpfungsfield
8. **Submit** und **Commit**

Wie in der Abbildung dargestellt:

The screenshot shows the 'Add Action' configuration window. On the left is a list of actions, with 'Add/Edit Header' selected and highlighted. The main area is titled 'Add/Edit Header' and contains the following fields and options:

- Header Name:** A text input field containing 'x-IronPort-Quarantine'. Below it is the label 'New Header Name or Existing Header'.
- Specify Value for New Header (optional):** A radio button that is selected, followed by an empty text input field.
- Prepend to the Value of Existing Header:** A radio button, followed by an empty text input field.
- Append to the Value of Existing Header:** A radio button, followed by an empty text input field.
- Search & Replace from the Value of Existing Header:** A radio button, followed by a 'Search for:' text input field with an asterisk and a 'Replace with:' text input field. Below these is the instruction 'Leave blank to remove searched text from value.'

Inhaltsfilteraktion zum

Hinzufügen eines Headers

Wenden Sie diesen Filter abschließend auf die gewünschte Mail-Policy für ein- und ausgehenden Datenverkehr an.

Zugehörige Informationen

- [Endanwenderanleitungen ESA](#)

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.