Erkennen von gefälschten E-Mail-Nachrichten auf der ESA und Erstellen von Ausnahmen

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie E-Mail-Spoofing auf der Cisco ESA gesteuert wird und wie Ausnahmen für Benutzer erstellt werden, die gefälschte E-Mails senden dürfen.

Voraussetzungen

Anforderungen

Ihre E-Mail Security Appliance (ESA) muss eingehende und ausgehende E-Mails verarbeiten und eine Standardkonfiguration von RELAYLIST verwenden, um Nachrichten als ausgehende Nachrichten zu kennzeichnen.

Verwendete Komponenten

Zu den spezifischen Komponenten gehören:

- Dictionary: wird zum Speichern aller internen Domänen verwendet.
- Nachrichtenfilter : wird verwendet, um die Logik zur Erkennung gefälschter E-Mails zu verarbeiten und einen Header einzufügen, auf den Content-Filter reagieren können.
- Policy Quarantine (Richtlinienquarantäne): wird verwendet, um Duplikate gefälschter E-Mails vorübergehend zu speichern. Fügen Sie die IP-Adresse der freigegebenen Nachrichten zu MY_TRUSTED_SPOOF_HOSTS hinzu, um zu verhindern, dass künftige Nachrichten von diesem Absender in die Richtlinienquarantäne gelangen.
- MY_TRUSTED_SPOOF_HOSTS: Liste, die auf Ihre vertrauenswürdigen sendenden IP-Adressen verweist. Wenn Sie dieser Liste eine IP-Adresse eines Absenders hinzufügen, wird die Quarantäne übersprungen, und der Absender kann die Nachricht fälschen. Sie platzieren vertrauenswürdige

Absender in Ihrer Absendergruppe MY_TRUSTED_SPOOF_HOSTS, sodass gefälschte Nachrichten von diesen Absendern nicht in Quarantäne gestellt werden.
- RELAYLIST: Liste zur Authentifizierung von IP-Adressen, die weitergeleitet werden dürfen, oder zum Senden ausgehender E-Mails. Wenn die E-Mail über diese Absendergruppe zugestellt wird, wird davon ausgegangen, dass es sich bei der Nachricht nicht um eine gefälschte Nachricht handelt.

Hinweis: Wenn eine Absendergruppe anders als MY_TRUSTED_SPOOF_HOSTS oder RELAYLIST bezeichnet wird, müssen Sie den Filter mit dem entsprechenden Absendergruppennamen ändern. Wenn Sie mehrere Listener haben, haben Sie auch mehr als einen MY_TRUSTED_SPOOF_HOSTS.

Die Informationen in diesem Dokument basieren auf der ESA mit einer beliebigen AsyncOS-Version.

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

Spoofing ist auf der Cisco ESA standardmäßig aktiviert. Es gibt mehrere triftige Gründe, warum Sie es anderen Domains erlauben, in Ihrem Namen zu senden. Ein gängiges Beispiel hierfür ist, dass der ESA-Administrator gefälschte E-Mails kontrollieren möchte, indem gefälschte Nachrichten in Quarantäne gestellt werden, bevor sie zugestellt werden.

Um eine bestimmte Aktion auszuführen, wie z. B. Quarantäne bei gefälschten E-Mails, müssen Sie zuerst gefälschte E-Mails erkennen.

Was ist E-Mail-Spoofing

Bei E-Mail-Spoofing handelt es sich um die Fälschung eines E-Mail-Headers, sodass die Nachricht von einer anderen Person oder einem anderen Ort als der tatsächlichen Quelle stammt. E-Mail-Spoofing ist eine Taktik, die in Phishing- und Spam-Kampagnen verwendet wird, da die Wahrscheinlichkeit höher ist, dass eine E-Mail geöffnet wird, wenn sie glaubt, von einer legitimen Quelle gesendet worden zu sein.

So erkennen Sie gefälschte E-Mails

Sie möchten alle Nachrichten filtern, die einen Umschlagabsender (Mail-From) und einen freundlichen Absender-Header (From) haben, der eine Ihrer eigenen eingehenden Domänen in der E-Mail-Adresse enthält.

Spoofing für bestimmte Absender zulassen

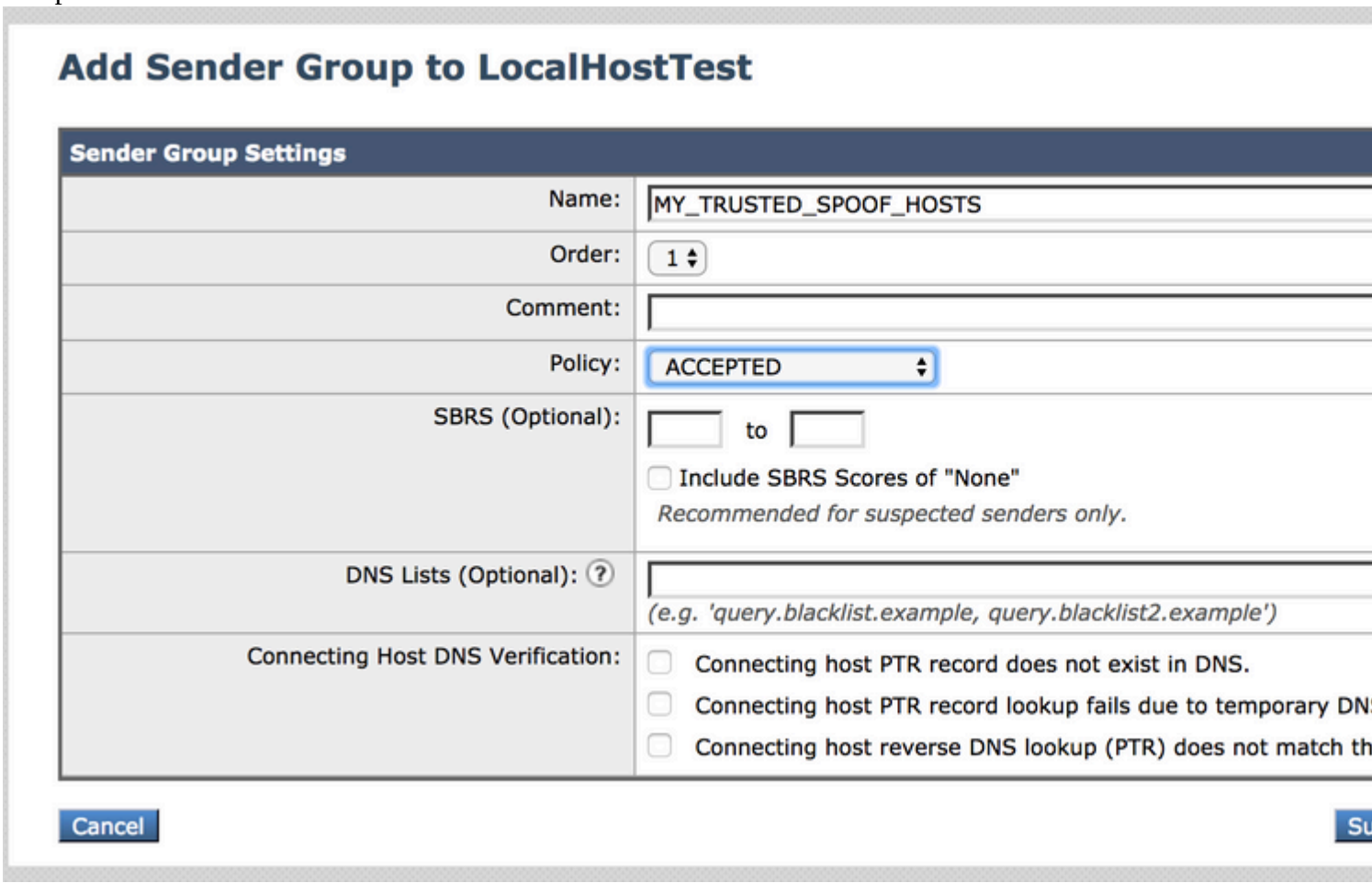
Wenn Sie den in diesem Artikel bereitgestellten Nachrichtenfilter implementieren, werden gefälschte Nachrichten mit einem Header gekennzeichnet, und der Inhaltsfilter wird verwendet, um Maßnahmen für den Header zu ergreifen. Um eine Ausnahme hinzuzufügen, fügen Sie einfach die Absender-IP zu MY_TRUSTED_SPOOF_HOSTS hinzu.

Konfigurieren

Absendergruppe erstellen

1. Navigieren Sie in der ESA-GUI zu **Mail Policies > HAT Overview**
2. Klicken Sie auf **Hinzufügen**
3. Geben Sie im Feld Name den Namen **MY_TRUSTED_SPOOF_HOSTS an**.
4. Geben Sie im Feld "Order" (Bestellung) den Wert **1 an**.
5. Geben Sie im Feld Policy (Richtlinie) den Wert **ACCEPTED (AKZEPTIERT)** an.
6. Klicken Sie auf **Senden**, um die Änderungen zu speichern.
7. Klicken Sie abschließend auf **Änderungen bestätigen**, um die Konfiguration zu speichern.

Beispiel:

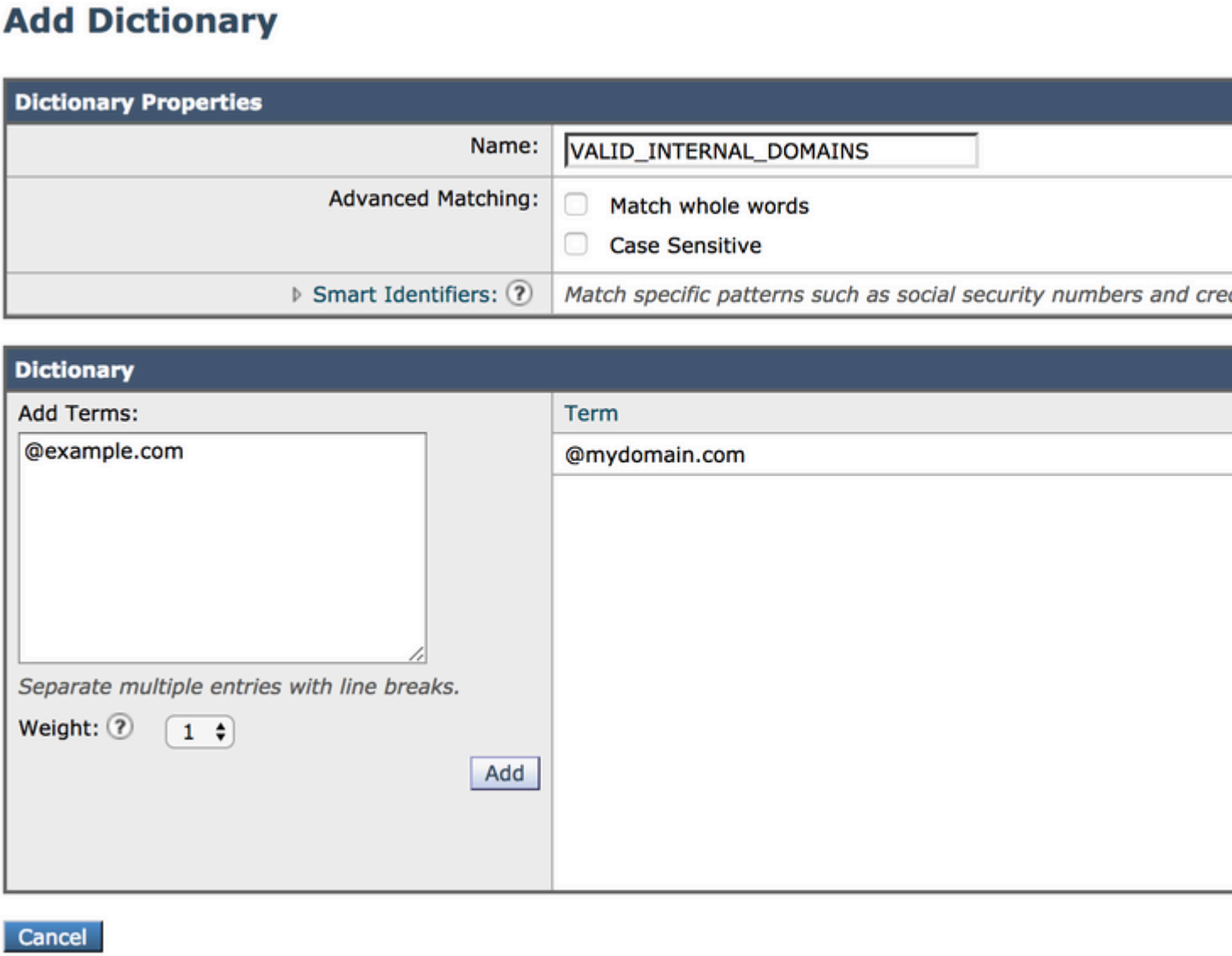


Dictionary erstellen

Erstellen Sie ein Dictionary für alle Domänen, für die Sie Spoofing auf der ESA deaktivieren möchten:

1. Navigieren Sie in der ESA-GUI zu **Mail-Policys > Wörterbücher.**
2. Klicken Sie auf **Dictionary hinzufügen.**
3. Geben Sie im Feld Name den Namen 'VALID_INTERNAL_DOMAINS' an, damit das Kopieren und Einfügen des Nachrichtenfilters fehlerfrei erfolgt.
4. Fügen Sie unter Begriffe hinzufügen alle Domänen hinzu, die Spoofing erkennen sollen. Geben Sie die Domäne mit einem @-Zeichen als Vorzeichen der Domäne ein, und klicken Sie auf **Hinzufügen**.
5. Stellen Sie sicher**,** dass das Kontrollkästchen **Ganze Wörter** zuordnen deaktiviert ist.
6. Klicken Sie auf **Senden**, um die Wörterbuchänderungen zu speichern.
7. Klicken Sie abschließend auf **Änderungen bestätigen**, um die Konfiguration zu speichern.

Beispiel:



Erstellen eines Nachrichtenfilters

Als Nächstes müssen Sie einen Nachrichtenfilter erstellen, um das soeben erstellte Wörterbuch "VALID_INTERNAL_DOMAINS" zu nutzen**:**

1. Stellen Sie eine Verbindung zur Befehlszeilenschnittstelle (CLI) der ESA her.
2. Führen Sie den Befehl **Filters (Filter) aus.**
3. Führen Sie den Befehl **Neu** aus, um einen neuen Nachrichtenfilter zu erstellen.
4. Kopieren Sie dieses Filterbeispiel, und fügen Sie es ein. Bearbeiten Sie ggf. die Namen der Absendergruppen:

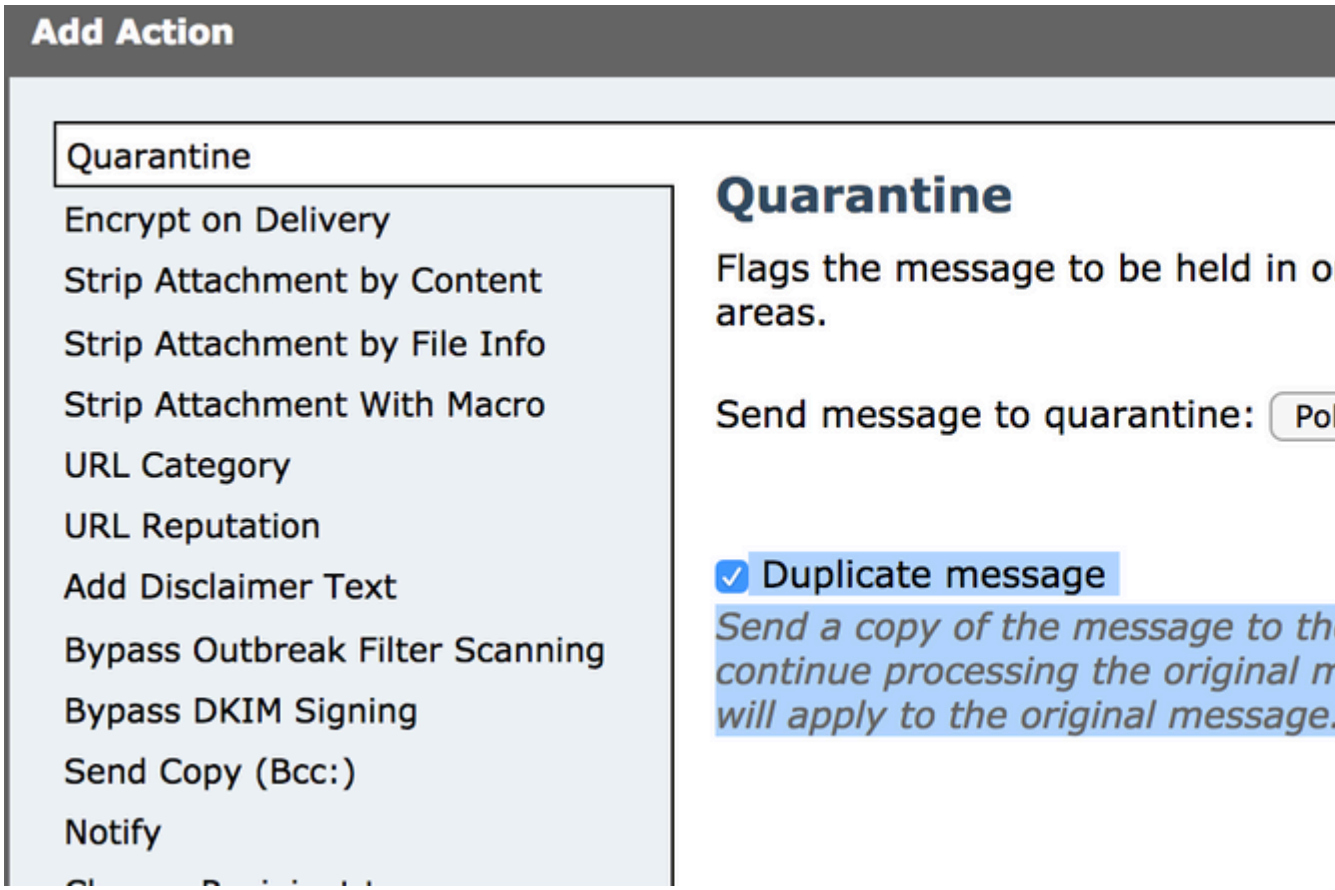
```
mark_spoofed_messages:
if(
     (mail-from-dictionary-match("VALID_INTERNAL_DOMAINS", 1))
 OR  (header-dictionary-match("VALID_INTERNAL_DOMAINS","From", 1)))
 AND ((sendergroup != "RELAYLIST")
 AND (sendergroup != "MY_TRUSTED_SPOOF_HOSTS")
  )
{
```

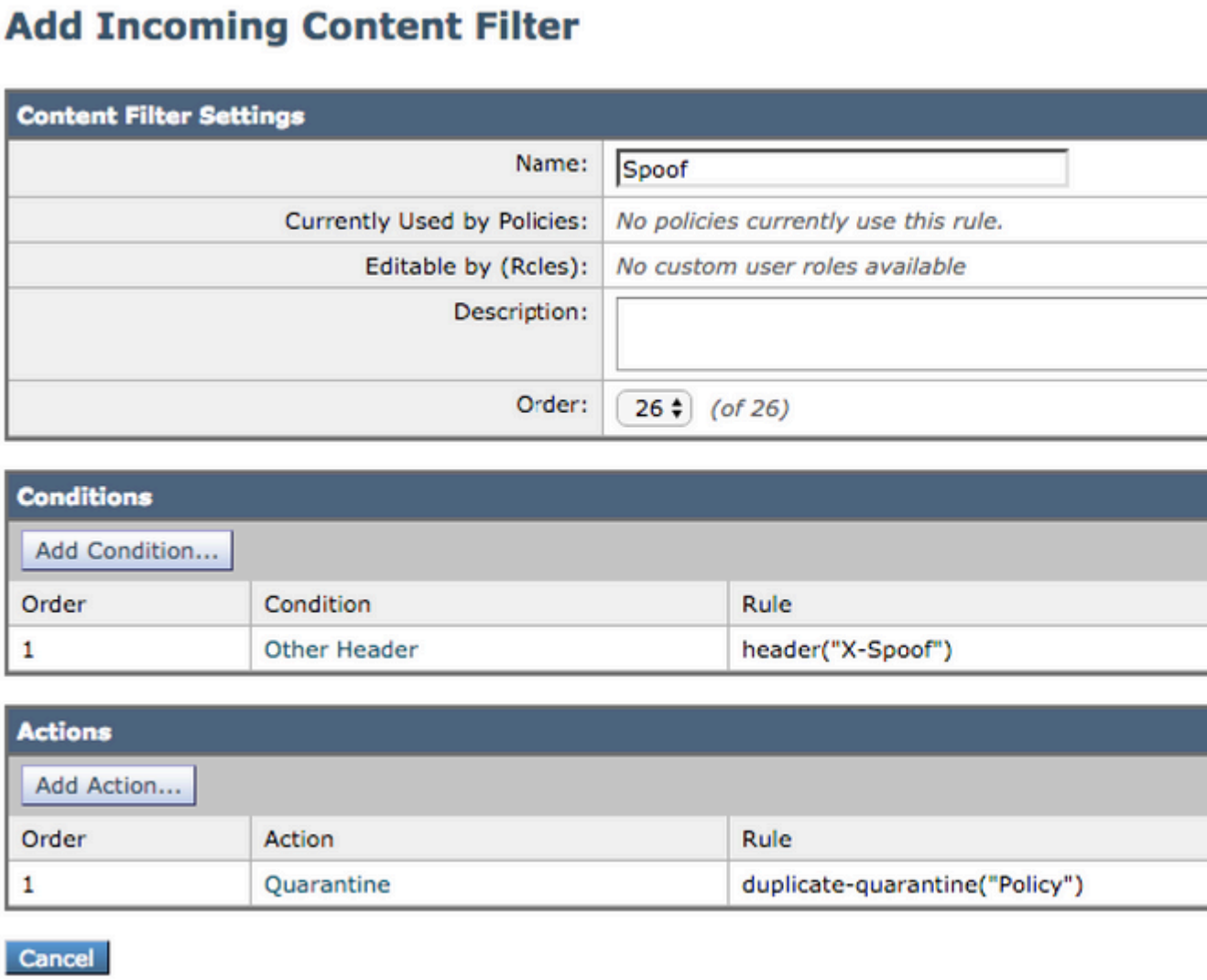
```
insert-header("X-Spoof", "");
}
```

5. Kehren Sie zur CLI-Eingabeaufforderung zurück, und führen Sie **Commit aus**, um die Konfiguration zu speichern.
6. Navigieren Sie zu **GUI > Mail-Policys > Filter für eingehende Inhalte.**
7. Erstellen Sie einen Filter für eingehende Inhalte, der Maßnahmen für den Spoofheader X-Spoof ausführt:

    1. Andere Kopfzeile hinzufügen
    2. Header-Name: X-Spoof
    3. Optionsfeld "Header vorhanden"
    4. Aktion hinzufügen: double-quarantine(Policy).

> **Hinweis**: Die hier gezeigte Funktion "Nachricht duplizieren" behält eine Kopie der Nachricht bei und sendet die ursprüngliche Nachricht weiter an den Empfänger.





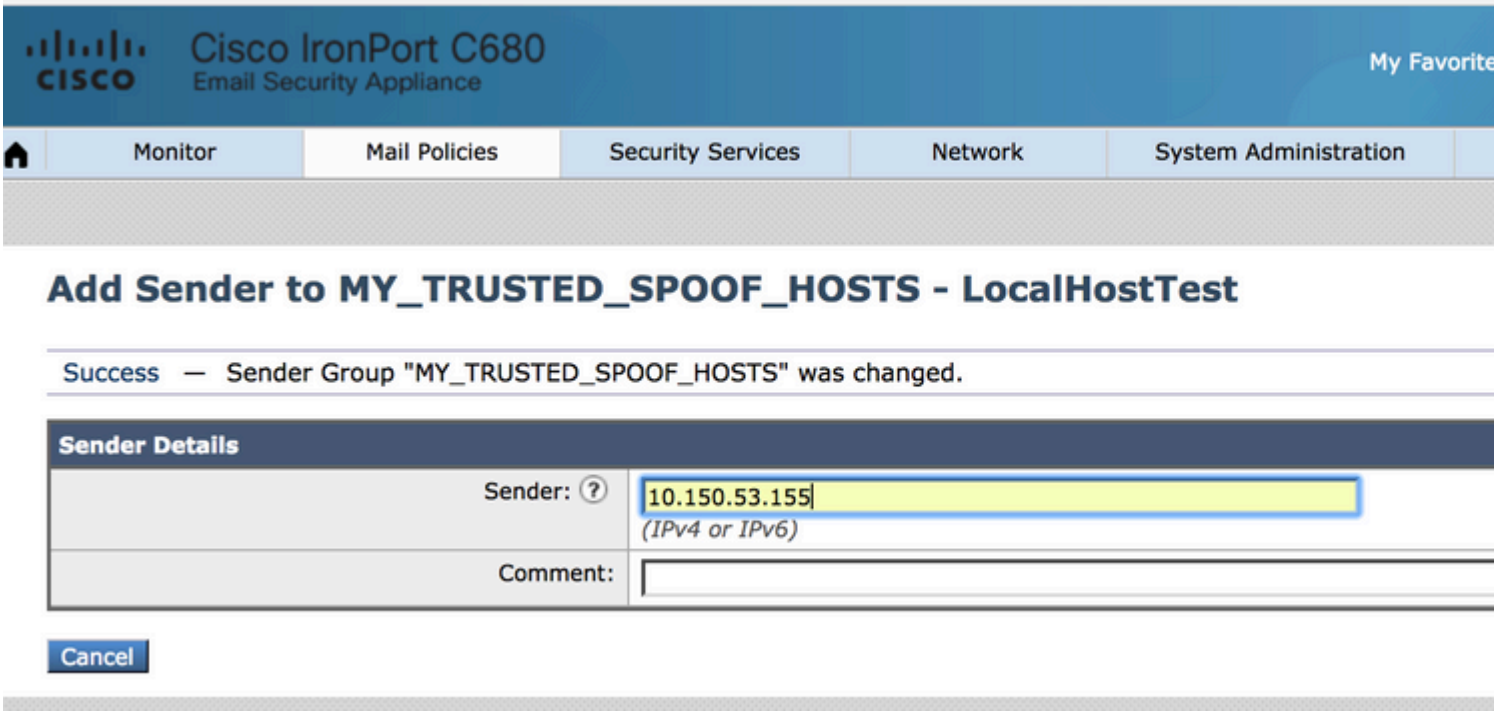
8. Verknüpfen Sie den Content-Filter mit Richtlinien für eingehende E-Mails unter **GUI > Mail-Richtlinien > Mail-Richtlinien für eingehende E-Mails**.
9. Senden und bestätigen Sie Änderungen.

Spoof-Ausnahmen zu MY_TRUSTED_SPOOF_HOSTS hinzufügen

Schließlich müssen Sie Spoofausnahmen (IP-Adressen oder Hostnamen) zur Absendergruppe MY_TRUSTED_SPOOF_HOSTS hinzufügen.

1. Navigieren über die Web-GUI: **Mail-Policys > HAT-Übersicht**
2. Klicken und **öffnen Sie** die Absendergruppe MY_TRUSTED_SPOOF_HOSTS.
3. Klicken Sie auf **Absender hinzufügen...** um eine IP-Adresse, einen Bereich, einen Hostnamen oder einen Teil des Hostnamens hinzuzufügen.
4. Klicken Sie auf **Senden**, um die Absenderänderungen zu speichern.
5. Klicken Sie abschließend auf **Änderungen bestätigen**, um die Konfiguration zu speichern.

Beispiel:



Überprüfung

Überprüfen, ob gefälschte Nachrichten in Quarantäne verschoben wurden

Senden Sie eine Testnachricht, in der Sie eine Ihrer Domänen als Umschlagabsender angeben. Überprüfen Sie, ob der Filter wie erwartet funktioniert, indem Sie eine Nachrichtenverfolgung für diese Nachricht durchführen. Das erwartete Ergebnis ist, dass die Nachricht in Quarantäne gestellt wird, da Sie noch keine Ausnahmen für die Absender erstellt haben, die Spoofing-Angriffe durchführen dürfen.

<#root>

```
Thu Apr 23 07:09:53 2015 Info: MID 102 ICID 9 RID 0 To: <xxxx_xxxx@domain.com>
Thu Apr 23 07:10:07 2015 Info: MID 102 Subject 'test1'
Thu Apr 23 07:10:07 2015 Info: MID 102 ready 177 bytes from <user_1@example.com>
Thu Apr 23 07:10:07 2015 Info: MID 102 matched all recipients for per-recipient policy DEFAULT in the in
Thu Apr 23 07:10:11 2015 Info: MID 102 interim verdict using engine: CASE spam negative
Thu Apr 23 07:10:11 2015 Info: MID 102 using engine: CASE spam negative
Thu Apr 23 07:10:11 2015 Info: MID 102 interim AV verdict using Sophos CLEAN
Thu Apr 23 07:10:11 2015 Info: MID 102 antivirus negative
```

Thu Apr 23 07:10:12 2015 Info: MID 102 quarantined to "Policy" (message filter:quarantine_spoofed_messag

```
Thu Apr 23 07:10:12 2015 Info: Message finished MID 102 done
```

Überprüfung der Zustellung von Spoof-Ausnahmemeldungen

Spoof-Exception-Absender sind IP-Adressen in der Absendergruppe(n), auf die im oben stehenden Filter verwiesen wird.

Auf RELAYLIST wird verwiesen, da sie von der ESA zum Senden ausgehender E-Mails verwendet wird. Bei Nachrichten, die von RELAYLIST gesendet werden, handelt es sich in der Regel um ausgehende E-

Mails. Wenn dies nicht berücksichtigt wird, kann es zu Fehlalarmen oder ausgehenden Nachrichten kommen, die durch den obigen Filter in Quarantäne gestellt werden.

Beispiel für die Nachrichtenverfolgung einer Spoof-Exception-IP-Adresse, die zu MY_TRUSTED_SPOOF_HOSTS hinzugefügt wurde. Die erwartete Aktion lautet "Zustellen" und nicht "Quarantäne". (Diese IP-Adresse darf getäuscht werden).

<#root>

```
Thu Apr 23 07:25:57 2015 Info: Start MID 108 ICID 11
Thu Apr 23 07:25:57 2015 Info: MID 108 ICID 11 From: <user_1@example.com>
Thu Apr 23 07:26:02 2015 Info: MID 108 ICID 11 RID 0 To: <user_xxxx@domain.com>
Thu Apr 23 07:26:10 2015 Info: MID 108 Subject 'test2'
Thu Apr 23 07:26:10 2015 Info: MID 108 ready 163 bytes from <user_1@example.com>
Thu Apr 23 07:26:10 2015 Info: MID 108 matched all recipients for per-recipient policy DEFAULT in the ir
Thu Apr 23 07:26:10 2015 Info: MID 108 interim AV verdict using Sophos CLEAN
Thu Apr 23 07:26:10 2015 Info: MID 108 antivirus negative
Thu Apr 23 07:26:10 2015 Info: MID 108 queued for delivery
Thu Apr 23 07:26:10 2015 Info: Delivery start DCID 16 MID 108 to RID [0]
Thu Apr 23 07:26:11 2015 Info: Message done DCID 16 MID 108 to RID [0]
Thu Apr 23 07:26:11 2015 Info: MID 108 RID [0] Response '2.0.0 t58EVG9N031598
```

Message accepted for delivery'

```
Thu Apr 23 07:26:11 2015 Info: Message finished MID 108 done
```

Zugehörige Informationen

- ESA-gefälschte Mail-Filterung
- Spoofschutz mit Absenderverifizierung

Interne Informationen von Cisco

Um diesen Prozess zu vereinfachen, wird eine Funktion angefordert, die die RAT Nachrichtenfiltern/Inhaltsfiltern aussetzt:

Cisco Bug-ID CSCus49018 - DE: Recipient Access Table (RAT) für Filterbedingungen verfügbar machen

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.