Rileva i messaggi di posta elettronica oggetto di spoofing sull'ESA e crea eccezioni

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Premesse](#)
[Che cos'è lo spoofing della posta elettronica](#)
[Come rilevare le e-mail falsificate](#)
[Come consentire lo spoofing per mittenti specifici](#)
[Configurazione](#)
[Crea un dizionario](#)
[Creare un filtro messaggi](#)
[Aggiungi eccezioni spoof a MY_TRUSTED_SPOOF_HOSTS](#)
[Verifica](#)
[Verifica che i messaggi di spoofing siano in quarantena](#)
[Verifica recapito messaggi di eccezione spoof](#)
[Informazioni correlate](#)

Introduzione

Questo documento descrive come controllare lo spoofing delle e-mail su Cisco ESA e come creare eccezioni per gli utenti autorizzati a inviare e-mail oggetto di spoofing.

Prerequisiti

Requisiti

Email Security Appliance (ESA) deve elaborare i messaggi di posta in arrivo e in uscita e utilizzare una configurazione standard di RELAYLIST per contrassegnare i messaggi come in uscita.

Componenti usati

I componenti specifici utilizzati comprendono:

- Dizionario: utilizzato per archiviare tutti i domini interni.
- Filtro messaggi : utilizzato per gestire la logica di rilevamento dei messaggi di posta elettronica falsificati e per inserire un'intestazione su cui i filtri contenuti possono agire.
- Quarantena criteri: utilizzato per archiviare temporaneamente i duplicati di messaggi di posta elettronica falsificati. Prendere in considerazione l'aggiunta dell'indirizzo IP dei messaggi rilasciati a MY_TRUSTED_SPOOF_HOSTS per impedire che i futuri messaggi provenienti da questo mittente vengano messi in quarantena.
- MY_TRUSTED_SPOOF_HOSTS: elenco in cui fare riferimento agli indirizzi IP di invio attendibili. L'aggiunta di un indirizzo IP di un mittente all'elenco ignora la quarantena e consente al mittente di eseguire lo spoof. I mittenti attendibili vengono inseriti nel gruppo di mittenti MY_TRUSTED_SPOOF_HOSTS in modo che i messaggi oggetto di spoofing di questi mittenti non

vengano messi in quarantena.
- RELAYLIST: elenco per autenticare gli indirizzi IP a cui è consentito l'inoltro o l'invio di e-mail in uscita. Se l'e-mail viene recapitata tramite questo gruppo di mittenti, si presume che il messaggio non sia un messaggio oggetto di spoofing.

Nota: se uno dei due gruppi di mittenti è denominato in modo diverso da MY_TRUSTED_SPOOF_HOSTS o RELAYLIST, è necessario modificare il filtro con il nome del gruppo di mittenti corrispondente. Inoltre, se si hanno più listener, si ha anche più di un MY_TRUSTED_SPOOF_HOSTS.

Le informazioni di questo documento si basano sull'ESA con qualsiasi versione AsyncOS.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Lo spoofing è abilitato per impostazione predefinita su Cisco ESA. Esistono diversi motivi validi per consentire l'invio di altri domini per conto dell'utente. Un esempio comune: l'amministratore ESA vuole controllare le e-mail contraffatte mettendo in quarantena i messaggi contraffatti prima che vengano consegnati.

Per eseguire un'azione specifica, ad esempio la quarantena di messaggi di posta elettronica falsificati, è necessario innanzitutto rilevare tali messaggi.

Che cos'è lo spoofing della posta elettronica

Lo spoofing delle e-mail è la falsificazione di un'intestazione e-mail in modo che il messaggio sembri provenire da una persona o da un luogo diverso dalla fonte effettiva. Lo spoofing delle e-mail è una tattica utilizzata nelle campagne di phishing e spam perché è più probabile che le persone aprano un'e-mail quando pensano che sia stata inviata da una fonte legittima.

Come rilevare le e-mail falsificate

Si desidera filtrare tutti i messaggi con un mittente di busta (Da-Posta) e un'intestazione Inviato da (Da) contenenti uno dei propri domini in arrivo nell'indirizzo di posta elettronica.

Come consentire lo spoofing per mittenti specifici

Quando si implementa il filtro messaggi fornito in questo articolo, i messaggi oggetto di spoofing vengono contrassegnati con un'intestazione e il filtro contenuti viene utilizzato per eseguire un'azione sull'intestazione. Per aggiungere un'eccezione, è sufficiente aggiungere l'indirizzo IP del mittente a MY_TRUSTED_SPOOF_HOSTS.

Configurazione

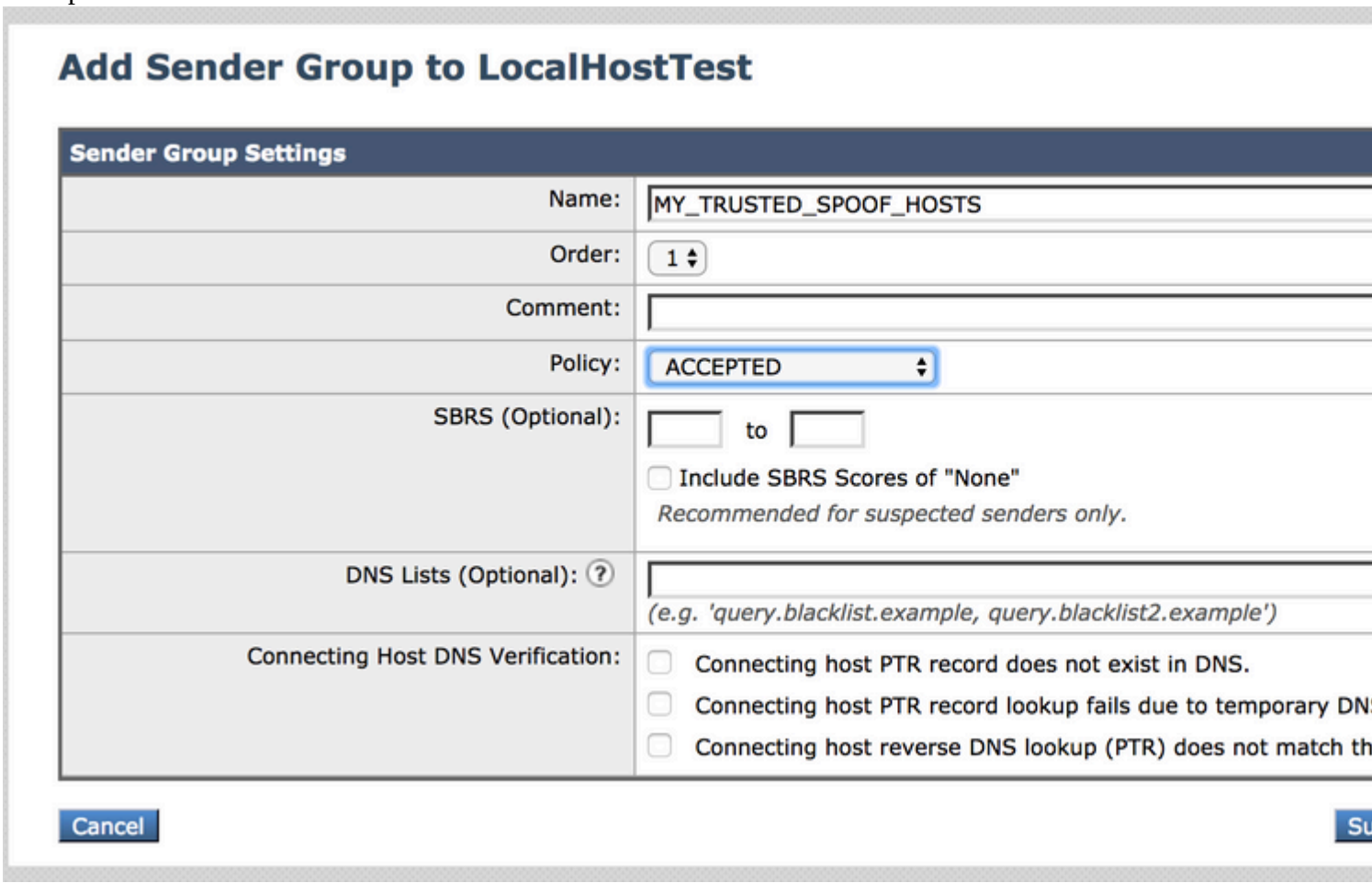
Crea un gruppo di mittenti

1. Dalla GUI dell'ESA, selezionare **Mail Policies > HAT Overview (Policy di posta > Panoramica**

HAT)

2. Fare clic su **Aggiungi.**
3. Nel campo Nome, specificare **MY_TRUSTED_SPOOF_HOSTS**.
4. Nel campo Ordine, specificare **1**.
5. Per il campo Criterio, specificare **ACCETTATO**.
6. Fare clic su **Invia** per salvare le modifiche.
7. Infine, fare clic su **Commit delle modifiche** per salvare la configurazione

Esempio:

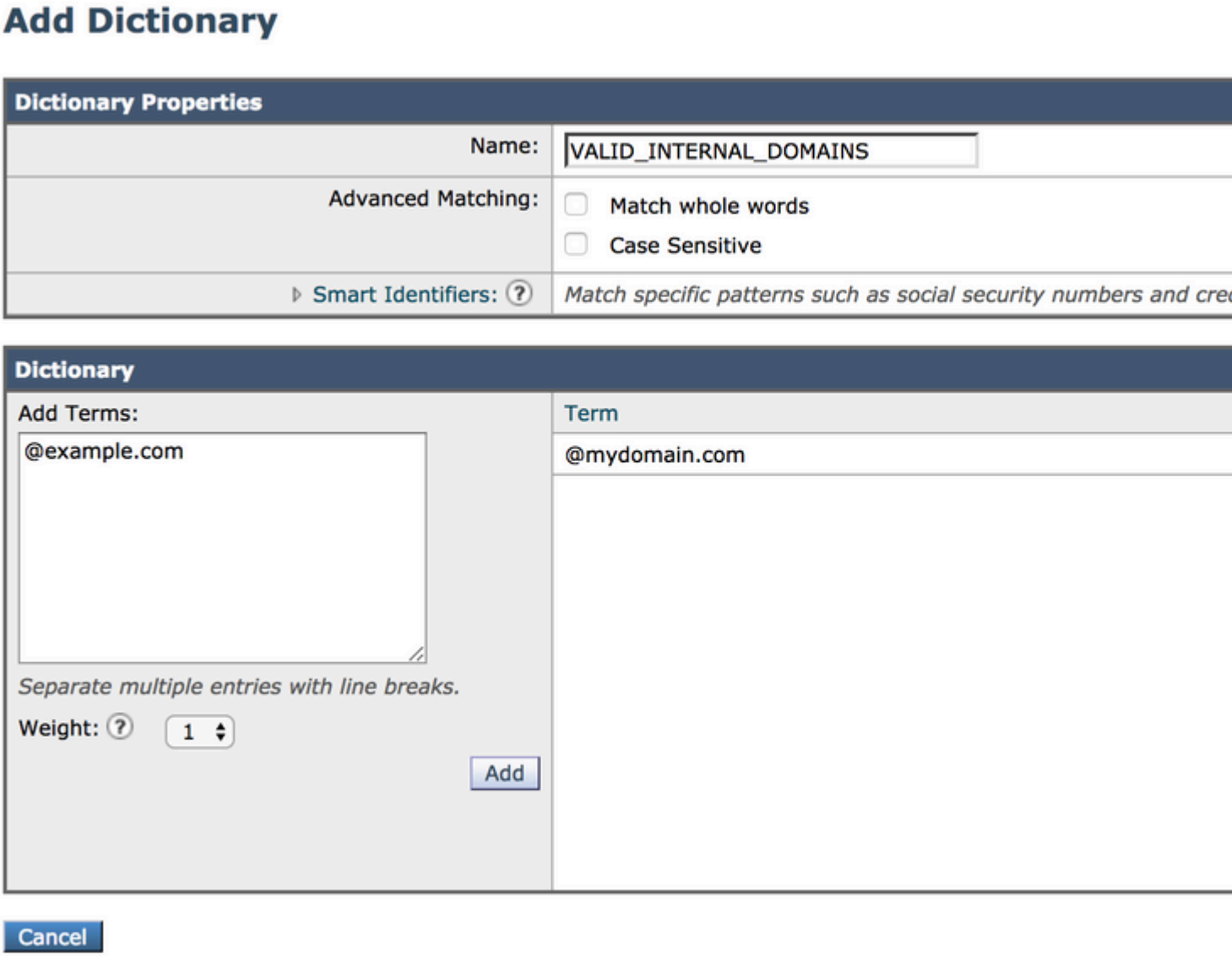


Crea un dizionario

Creare un dizionario per tutti i domini per i quali si desidera disattivare lo spoofing sull'ESA:

1. Dalla GUI dell'ESA, selezionare **Mail Policies > Dictionaries** (Policy di posta > Dizionari).
2. Fare clic su **Aggiungi dizionario.**
3. Nel campo Nome, specificare 'VALID_INTERNAL_DOMAINS' per rendere il filtro messaggi privo di errori durante la copia e l'incollamento.
4. In aggiungi termini aggiungere tutti i domini che si desidera rilevare lo spoofing. Immettere il dominio preceduto dal simbolo @, quindi fare clic su **add** (aggiungi).
5. Assicurarsi che la casella di controllo **Corrispondenza parole intere** sia deselezionata.
6. Fare clic su **Invia** per salvare le modifiche apportate al dizionario.
7. Infine, fare clic su **Commit delle modifiche** per salvare la configurazione.

Esempio:



Creare un filtro messaggi

Successivamente, è necessario creare un filtro messaggi per utilizzare il dizionario appena creato, "VALID_INTERNAL_DOMAINS"**:**

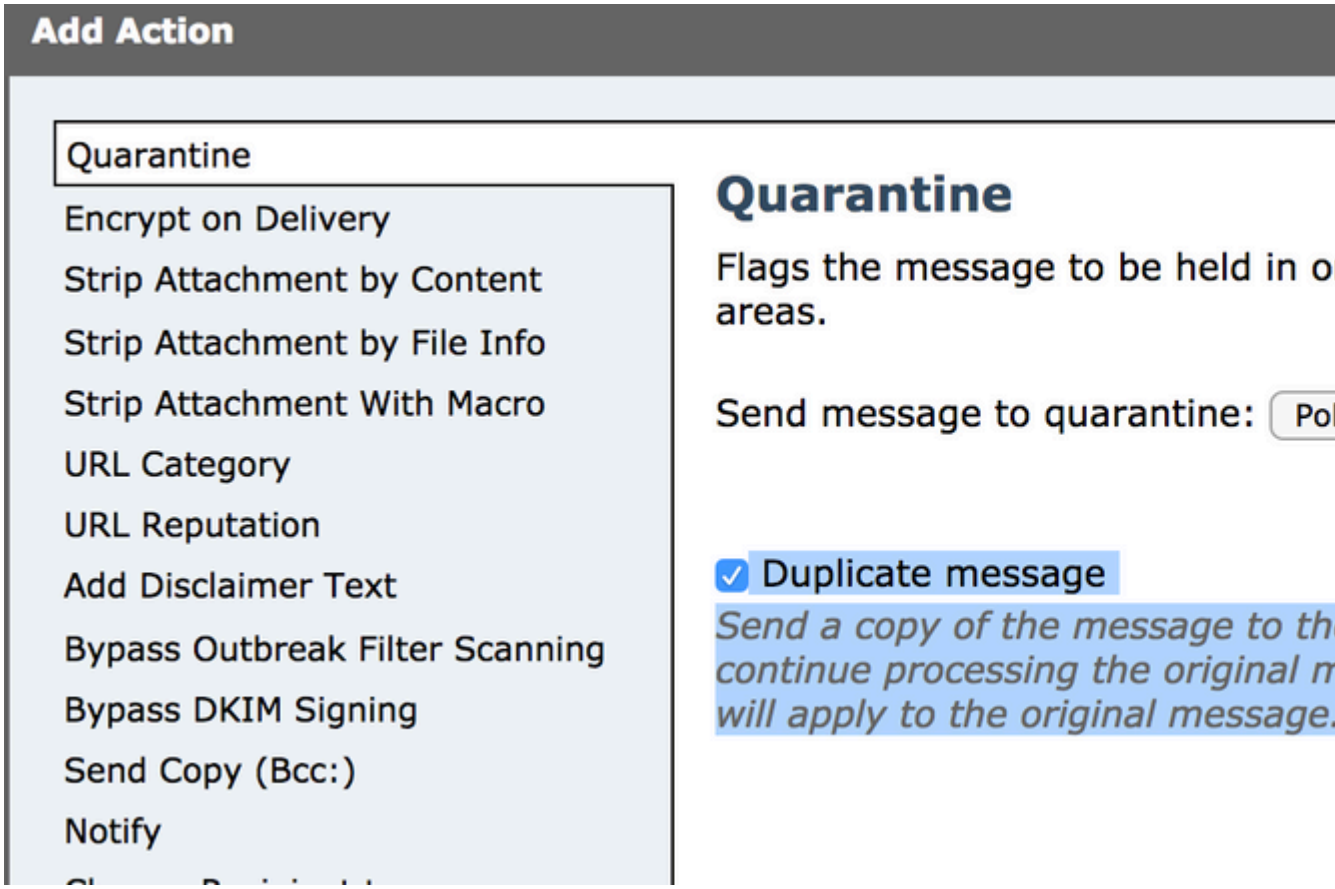
1. connettersi all'interfaccia della riga di comando (CLI) dell'ESA.
2. Eseguire il comando **Filtri.**
3. Eseguire il comando **New** per creare un nuovo filtro messaggi.
4. Copiare e incollare questo esempio di filtro, apportando le modifiche necessarie ai nomi effettivi del gruppo di mittenti:

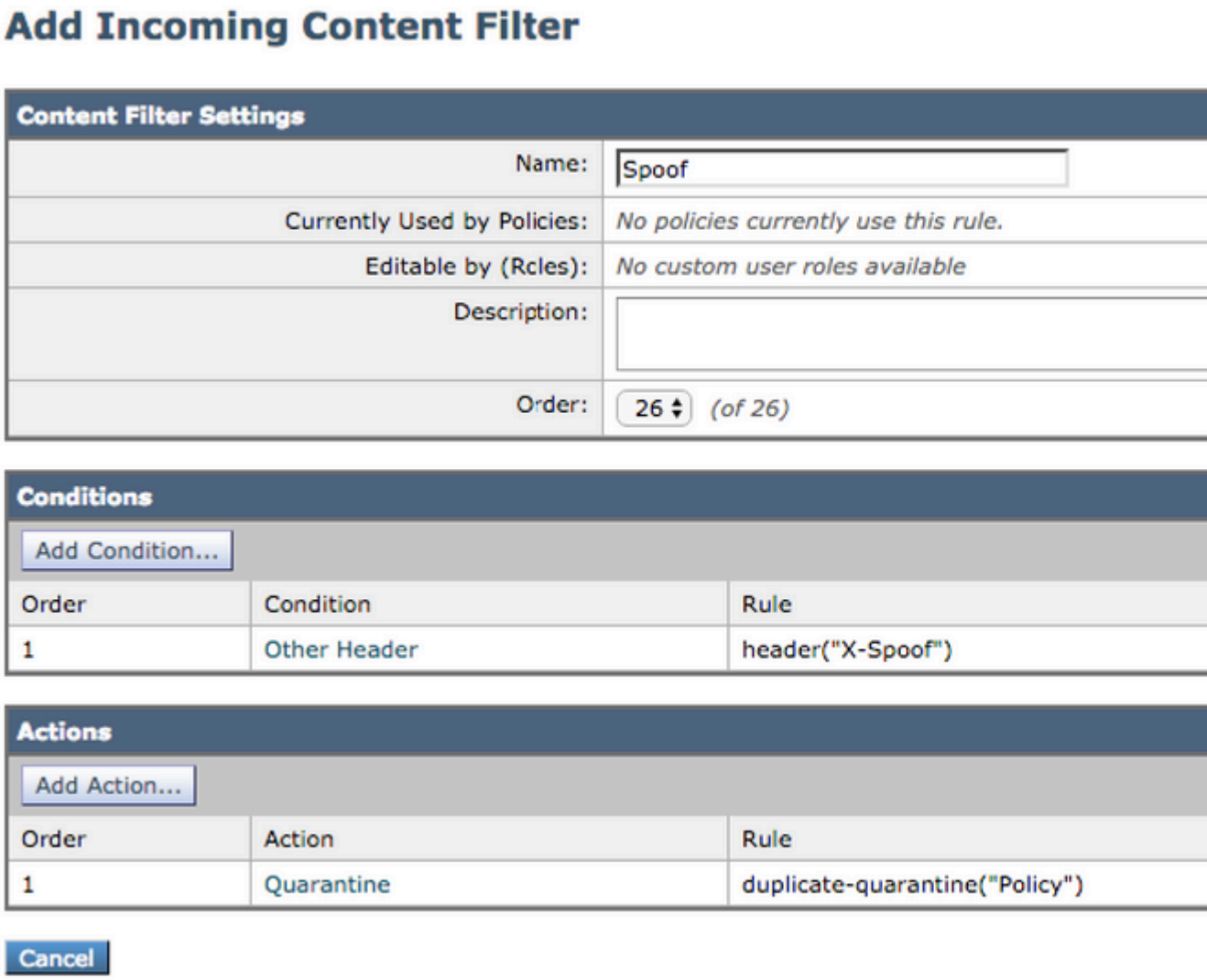
```
mark_spoofed_messages:
if(
     (mail-from-dictionary-match("VALID_INTERNAL_DOMAINS", 1))
 OR  (header-dictionary-match("VALID_INTERNAL_DOMAINS","From", 1)))
 AND ((sendergroup != "RELAYLIST")
 AND (sendergroup != "MY_TRUSTED_SPOOF_HOSTS")
  )
{
```

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

5. Tornare al prompt della CLI principale ed eseguire **Commit** per salvare la configurazione.
6. Selezionare **GUI > Mail Policies > Incoming Content Filters** (Policy di posta > Filtri contenuti in arrivo)
7. Crea filtro contenuti in arrivo che esegue azioni sull'intestazione spoof X-Spoof:
    1. Aggiungi altra intestazione
    2. Nome intestazione: X-Spoof
    3. Pulsante di opzione Intestazione esistente
    4. Aggiungi azione: duplicate-quarantine(Policy).

> **Nota**: la funzione Duplica messaggio illustrata mantiene una copia del messaggio e continua a inviare il messaggio originale al destinatario.





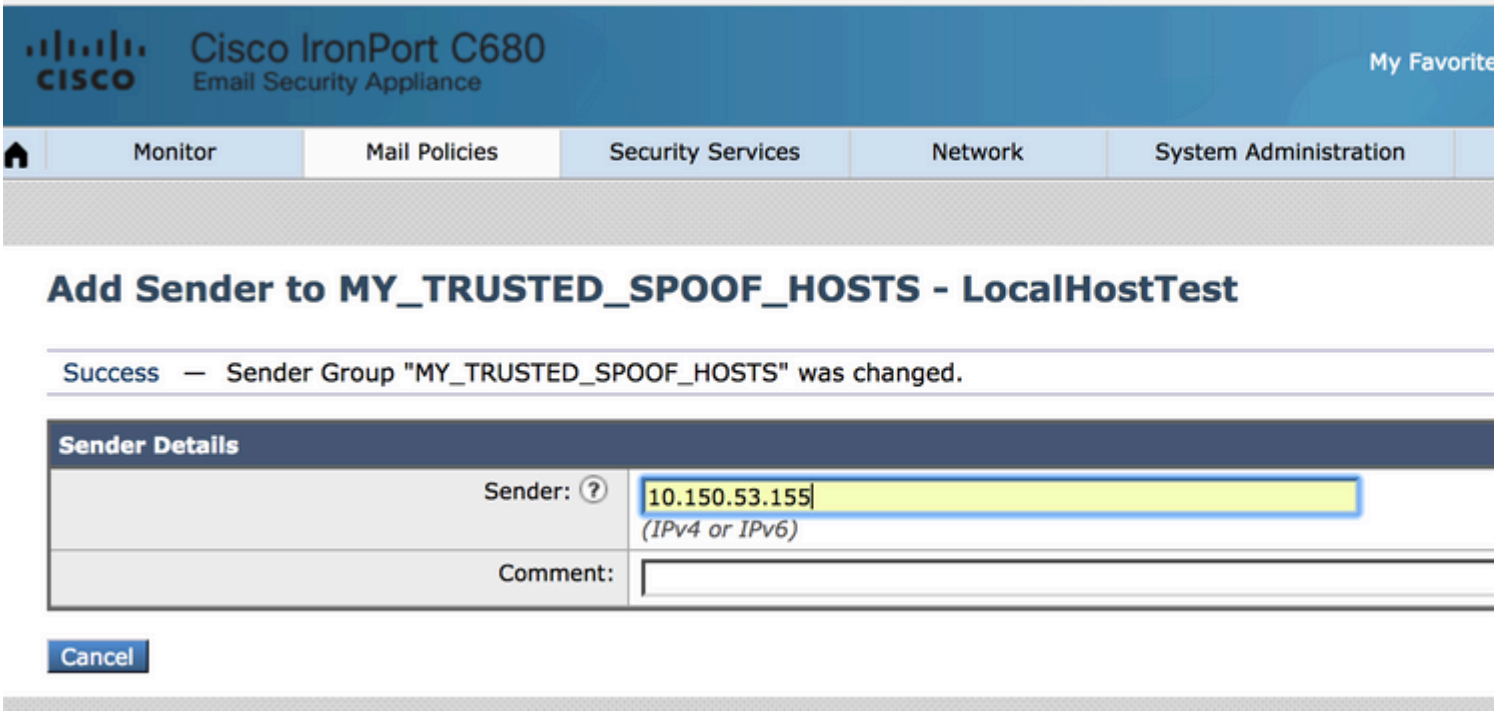
8. Collegare il filtro dei contenuti ai criteri della posta in arrivo dalla **GUI > Criteri di posta > Criteri posta in arrivo**.
9. Invia e conferma modifiche.

Aggiungi eccezioni spoof a MY_TRUSTED_SPOOF_HOSTS

Infine, è necessario aggiungere eccezioni spoof (indirizzi IP o nomi host) al gruppo di mittenti MY_TRUSTED_SPOOF_HOSTS.

1. Navigare attraverso la GUI Web: **Mail Policies > HAT Overview (Policy di posta > Panoramica HAT)**
2. Fate clic su e **aprite** il gruppo di mittenti MY_TRUSTED_SPOOF_HOSTS.
3. Fare clic su **Aggiungi mittente...** per aggiungere un indirizzo IP, un intervallo, un nome host o un nome host parziale.
4. Fare clic su **Invia** per salvare le modifiche apportate al mittente.
5. Infine, fare clic su **Commit delle modifiche** per salvare la configurazione.

Esempio:



Verifica

Verifica che i messaggi di spoofing siano in quarantena

Invia un messaggio di prova specificando uno dei tuoi domini come mittente della busta. Verificare che il filtro funzioni come previsto eseguendo una traccia dei messaggi sul messaggio. Il risultato previsto è che il messaggio viene messo in quarantena perché non è stata ancora creata alcuna eccezione per i mittenti a cui è consentito lo spoofing.

<#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
```

Verifica recapito messaggi di eccezione spoof

I mittenti di eccezioni spoof sono indirizzi IP nei gruppi di mittenti a cui viene fatto riferimento nel filtro sopra riportato.

Si fa riferimento a RELAYLIST perché viene utilizzata dall'ESA per inviare la posta in uscita. I messaggi inviati da RELAYLIST sono in genere messaggi in uscita che, se non inclusi, creerebbero falsi positivi o

messaggi in uscita messi in quarantena dal filtro sopra indicato.

Esempio di verifica messaggi di un indirizzo IP di eccezione spoof aggiunto a MY_TRUSTED_SPOOF_HOSTS. L'azione prevista è il recapito e non la quarantena. (Questo indirizzo IP può essere contraffatto).

<#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 in
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
```

Informazioni correlate

- Filtro posta falsificata ESA
- Protezione da spoof mediante verifica mittente

Informazioni interne Cisco

Per semplificare questo processo, è necessario esporre la valutazione RAT ai filtri messaggi/contenuti:

ID bug Cisco CSCus49018 - ENH: esposizione della tabella di accesso del destinatario (RAT) per filtrare le condizioni

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).