Detecteer spoofed e-mailberichten op de ESA en maak uitzonderingen

Inhoud

Inleiding

Dit document beschrijft hoe u e-mailspoofing op de Cisco ESA kunt controleren en hoe u uitzonderingen kunt maken voor de gebruikers die spoofed e-mails mogen verzenden.

Voorwaarden

Vereisten

Uw e-mail security applicatie (ESA) moet zowel inkomende als uitgaande e-mails verwerken en een standaardconfiguratie van RELAYLIST gebruiken om berichten als uitgaand te markeren.

Gebruikte componenten

Specifieke componenten die worden gebruikt, zijn onder meer:

- Woordenboek: gebruikt om al uw interne domeinen op te slaan.
- Berichtfilter: gebruikt om de logica te verwerken om gespoofde e-mail te detecteren en een header in te voegen waar inhoudsfilters op kunnen reageren.
- Policy Quarantaine: gebruikt om duplicaten van gespoofde e-mails tijdelijk op te slaan. Overweeg om het IP-adres van vrijgegeven berichten toe te voegen aan MY_TRUSTED_SPOOF_HOSTS om te voorkomen dat toekomstige berichten van deze afzender de beleidsquarantaine ingaan.
- MY_TRUSTED_SPOOF_HOSTS: lijst om uw vertrouwde verzendende IP-adressen te raadplegen. Door een IP-adres van een afzender aan deze lijst toe te voegen, wordt de quarantaine overgeslagen en krijgt de afzender een parodie. U plaatst vertrouwde afzenders in uw MY_TRUSTED_SPOOF_HOSTS afzendergroep zodat gespoofde berichten van deze afzenders niet in quarantaine worden geplaatst.

- RELAYLIST: lijst om IP-adressen te verifiëren die uitgaande e-mail mogen doorgeven of verzenden. Als de e-mail via deze afzendergroep wordt geleverd, wordt aangenomen dat het bericht geen spoofed bericht is.

Opmerking: Als een van de afzendergroepen iets anders wordt genoemd dan MY_TRUSTED_SPOOF_HOSTS of RELAYLIST, moet u het filter wijzigen met de corresponderende afzendergroepnaam. Ook, als je meerdere luisteraars hebt, heb je ook meer dan één MY_TRUSTED_SPOOF_HOSTS.

De informatie in dit document is gebaseerd op de ESA met elke AsyncOS-versie.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Spoofing is standaard ingeschakeld op de Cisco ESA. Er zijn verschillende, geldige redenen om andere domeinen toe te staan om namens u te verzenden. Eén veelvoorkomend voorbeeld: ESA-beheerder wil gespoofde e-mails controleren door gespoofde berichten in quarantaine te plaatsen voordat ze worden afgeleverd.

Om een specifieke actie te ondernemen, zoals quarantaine op gespoofde e-mail, moet u eerst gespoofde e-mail detecteren.

Wat is e-mailspoofing

E-mailspoofing is de vervalsing van een e-mailheader, zodat het bericht afkomstig lijkt te zijn van iemand of ergens anders dan de werkelijke bron. E-mailspoofing is een tactiek die wordt gebruikt in phishing- en spamcampagnes, omdat mensen eerder geneigd zijn een e-mail te openen als ze denken dat deze is verstuurd door een legitieme bron.

Hoe spoofed email te detecteren

U wilt alle berichten filteren die een envelopzender (Mail-From) en vriendelijk van (From) header hebben die een van uw eigen inkomende domeinen in het e-mailadres bevatten.

Spoofing toestaan voor specifieke afzenders

Wanneer u de berichtfilter implementeert die binnen dit artikel wordt geboden, worden spoofed berichten gelabeld met een header en wordt de inhoudsfilter gebruikt om actie te ondernemen op de header. Om een uitzondering toe te voegen, voeg eenvoudig de afzender IP aan MY_TRUSTED_SPOOF_HOSTS toe.

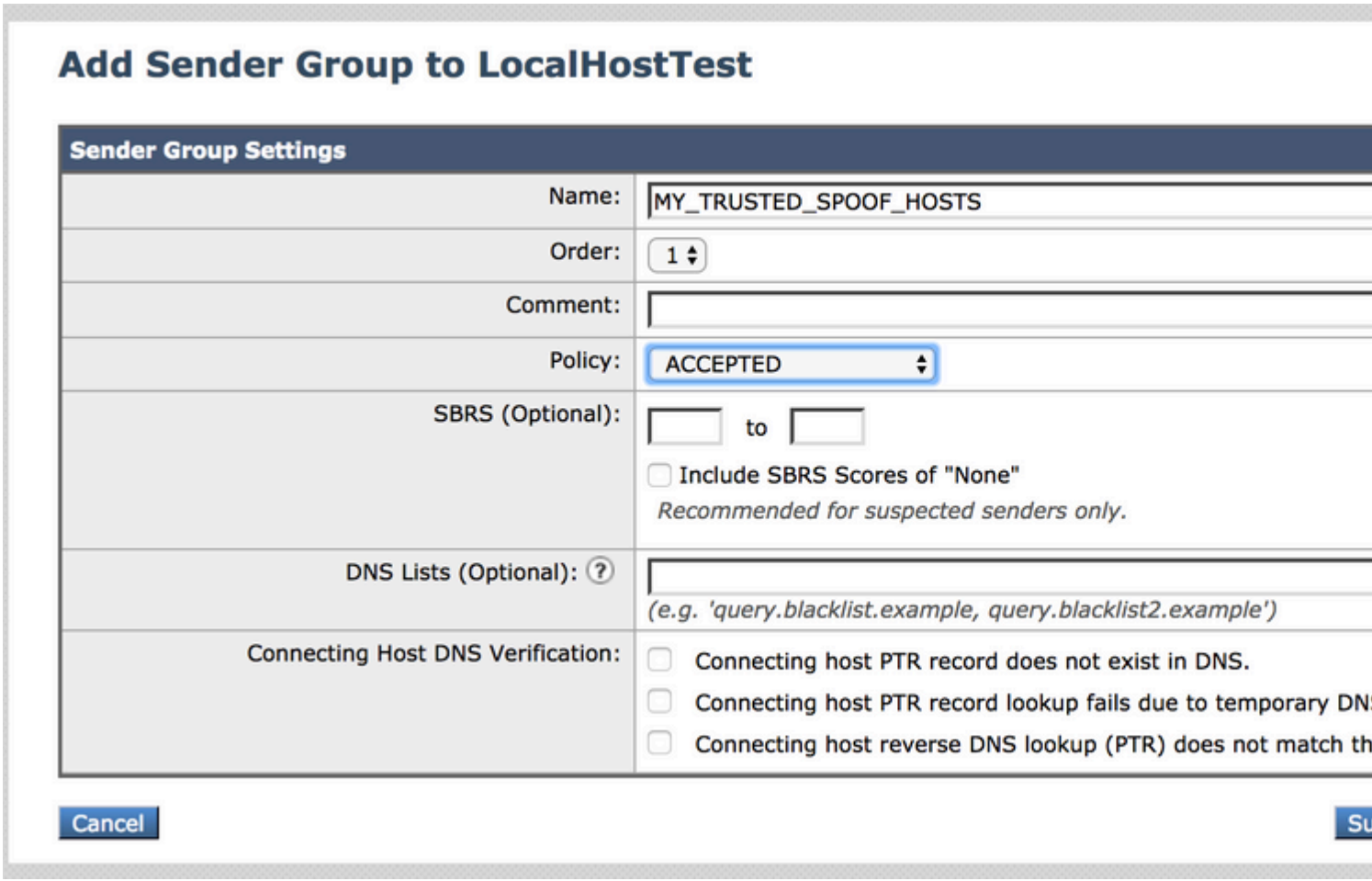
Configureren

Een sendergroep maken

1. Ga vanuit de ESA GUI naar **Mail Policies > HAT Overzicht**
2. Klik op de knop **Toevoegen.**
3. Specificeer in het veld Naam **MY_TRUSTED_SPOOF_HOSTS**.
4. Specificeer in het veld Volgorde **1**.

5. Specificeer in het veld Beleid **Geaccepteerd**.
6. Klik op **Indienen** om de wijzigingen op te slaan.
7. Klik tot slot op **Veranderingen vastleggen** om de configuratie op te slaan

Voorbeeld:

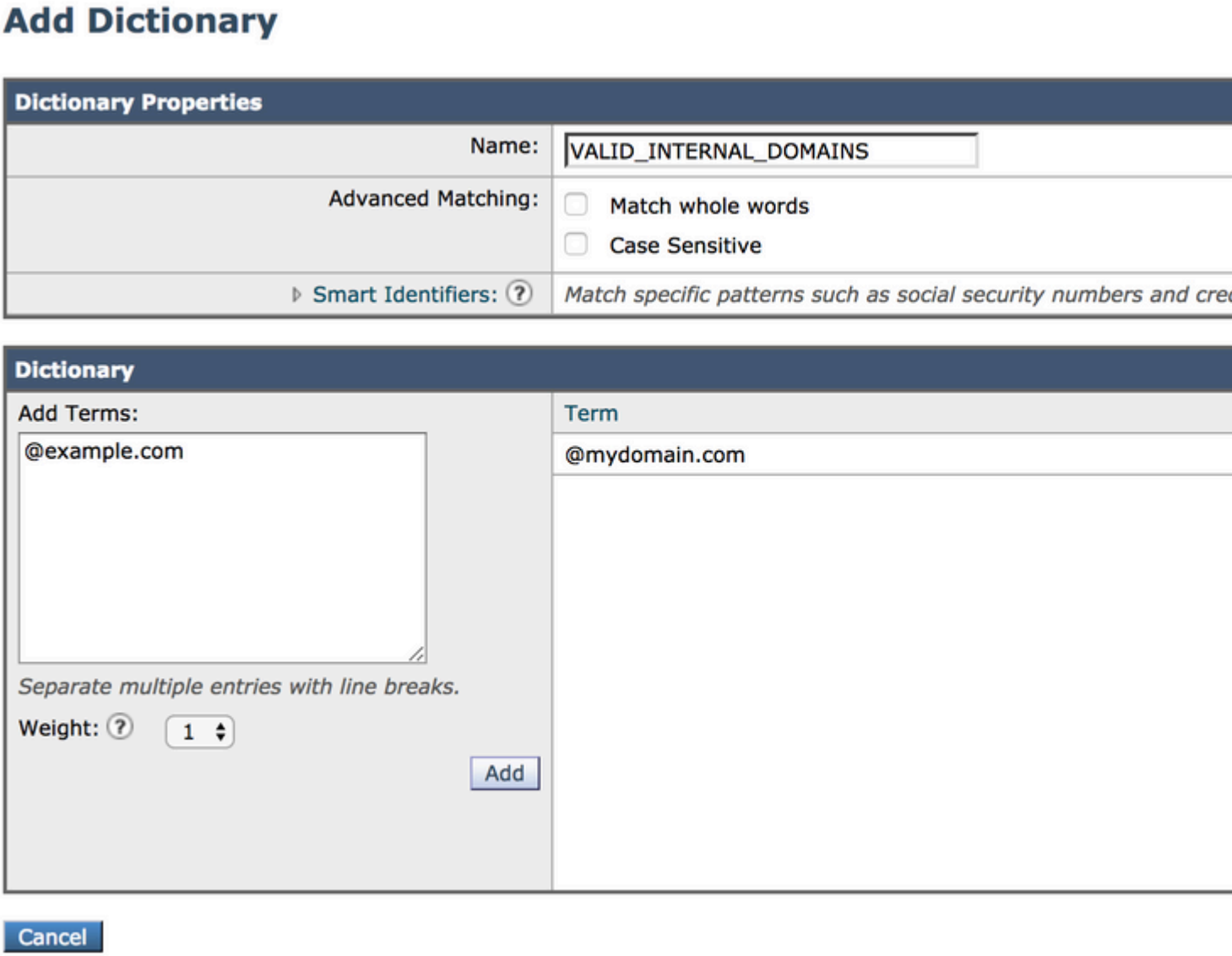


Een woordenboek maken

Maak een woordenboek voor alle domeinen die u wilt uitschakelen spoofing voor op de ESA:

1. Ga vanuit de ESA GUI naar **Mail Policies > Woordenboeken.**
2. Klik op de knop **Woordenboek toevoegen.**
3. Specificeer in het veld Naam 'GELDIG_INTERNE_DOMEINEN' om het kopiëren en plakken van het berichtfilter foutloos te laten verlopen.
4. Onder Add voorwaarden, voeg alle domeinen toe die u spoofing wilt detecteren. Voer het domein in met een @-teken dat het domein voorbereidt en klik op **Toevoegen**.
5. Zorg ervoor dat selectieteken voor **hele woorden** niet zijn ingeschakeld.
6. Klik op **Indienen** om de woordenboekwijzigingen op te slaan.
7. Klik tot slot op **Veranderingen vastleggen** om de configuratie op te slaan.

Voorbeeld:



Een berichtfilter maken

Vervolgens moet u een berichtfilter aanmaken om gebruik te kunnen maken van het woordenboek dat zojuist is aangemaakt, "GELDIG_INTERNE_DOMEINEN"**:**

1. Aansluiten op de opdrachtregelinterface (CLI) van de ESE.
2. Start de opdrachtfilters **.**
3. Voer de opdracht **Nieuw uit** om een nieuw berichtfilter te maken.
4. Kopieer en plak dit filtervoorbeeld, waarbij u indien nodig bewerkingen maakt voor uw feitelijke afzendergroepnamen:

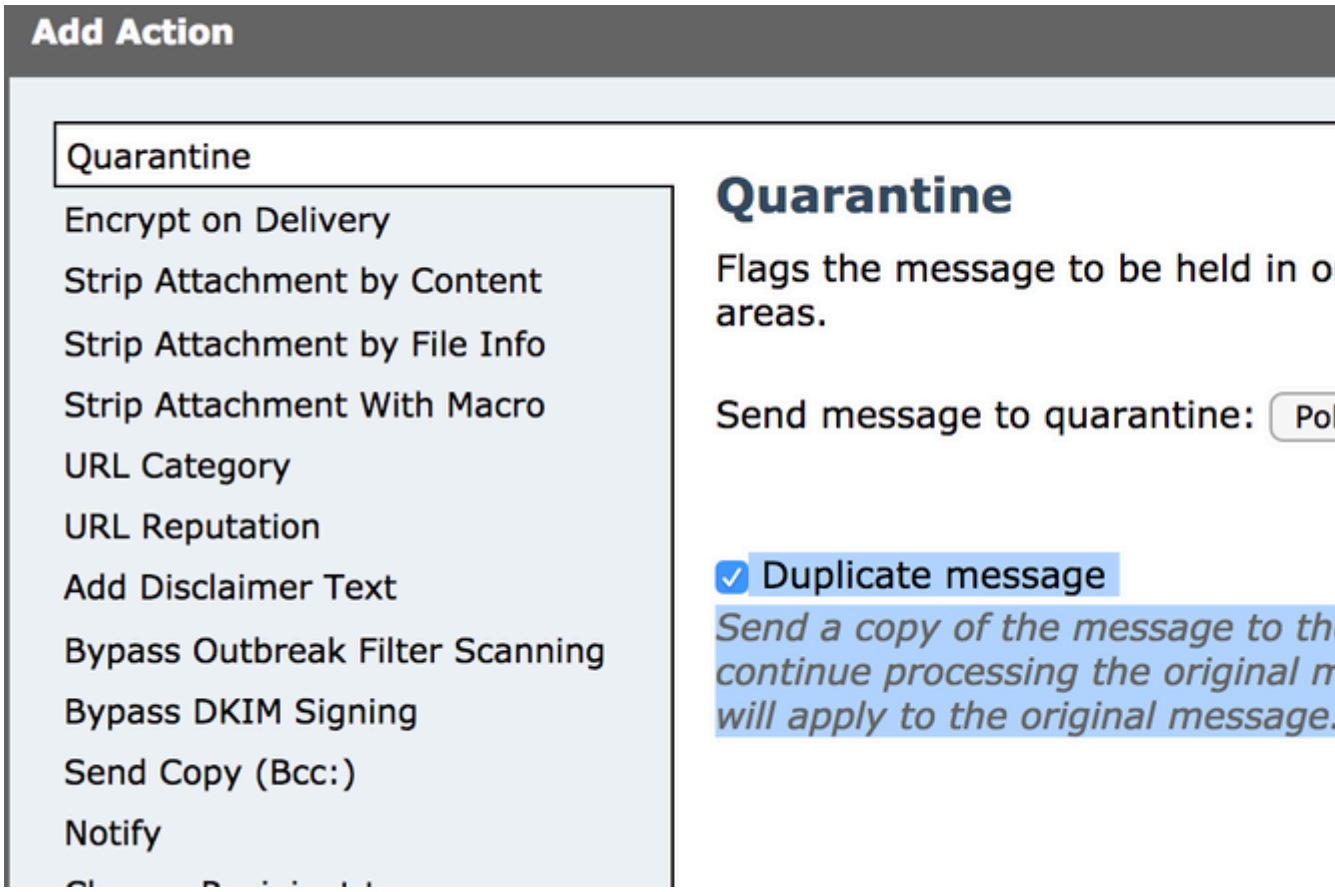
```
mark_spoofed_messages:
if(
     (mail-from-dictionary-match("VALID_INTERNAL_DOMAINS", 1))
 OR  (header-dictionary-match("VALID_INTERNAL_DOMAINS","From", 1)))
 AND ((sendergroup != "RELAYLIST")
 AND (sendergroup != "MY_TRUSTED_SPOOF_HOSTS")
  )
{
```

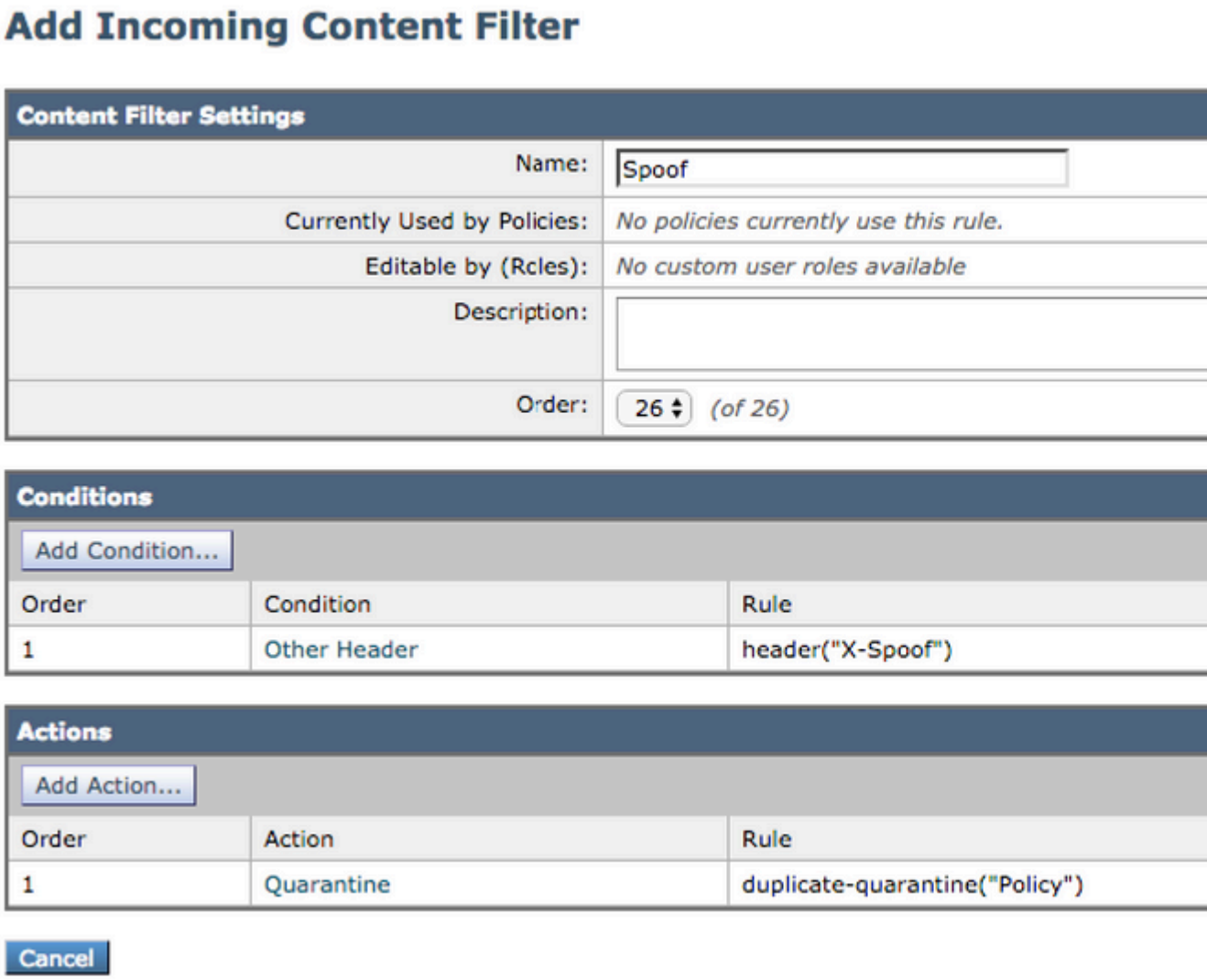
```
insert-header("X-Spoof", "");
}
```

5. Ga terug naar de CLI-prompt en voer **Commit** uit om de configuratie op te slaan.
6. Naar de **GUI** navigeren > **Postbeleid** > **Inkomende contentfilters**
7. Creëer Inkomende Content Filter dat actie onderneemt op de nepkop X-Spoof:

    1. Andere kop toevoegen
    2. Kop Naam: X-Spoof
    3. Kop bestaat radioknop
    4. Voeg actie toe: duplicate-quarantaine (beleid).

> **Opmerking**: de hier getoonde berichtenfunctie Dupliceren houdt een kopie van het bericht bij en blijft het oorspronkelijke bericht naar de ontvanger sturen.





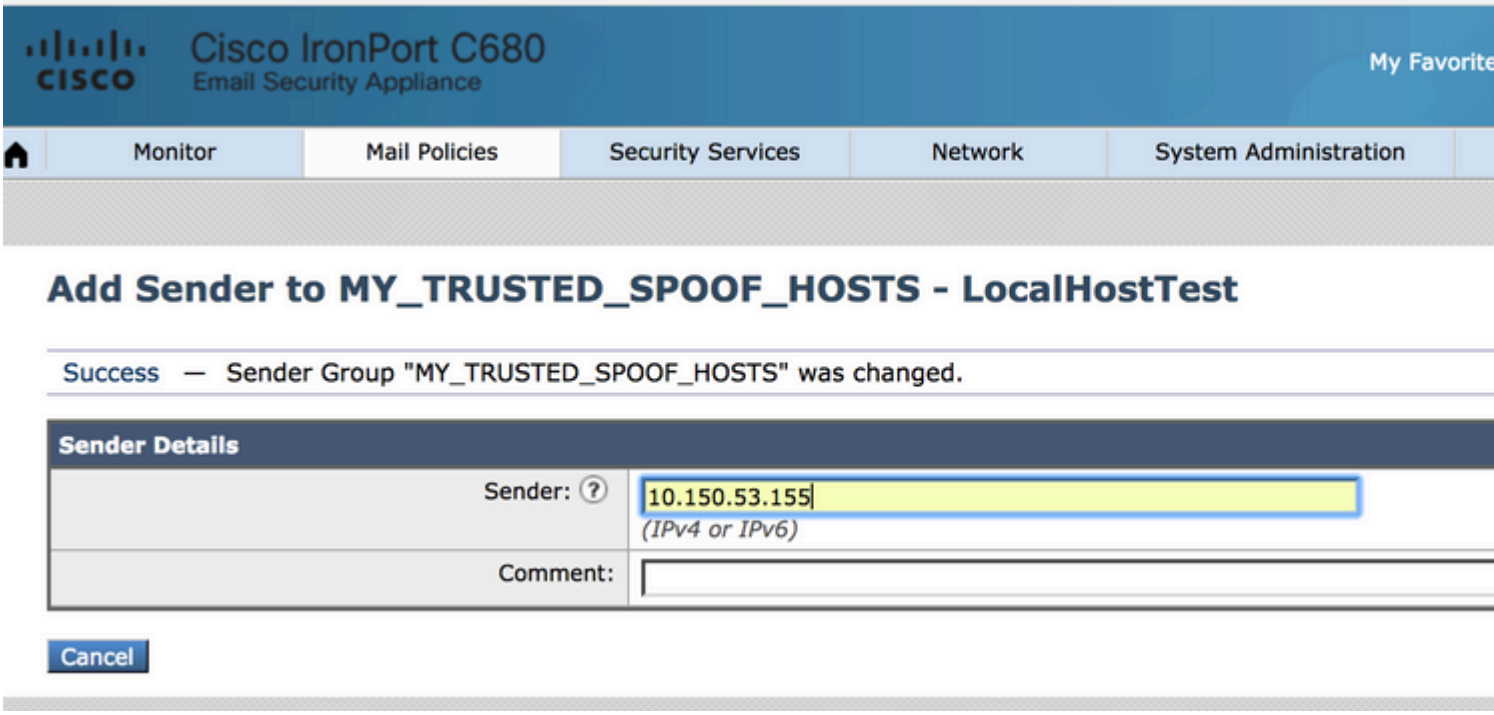
8. Koppel het filter voor inhoud aan het beleid voor inkomende e-mail op de **GUI-pagina** > **Postbeleid** > **Inkomende e-mail**.
9. Veranderingen verzenden en doorvoeren.

Voeg nep-uitzonderingen toe aan MY_TRUSTED_SPOOF_HOSTS

Tot slot moet je parodie-uitzonderingen (IP-adressen of hostnamen) toevoegen aan de my_TRUSTED_SPOOF_HOSTS sendergroup.

1. Navigeren via de web GUI: **Mail Policies** > **HAT Overzicht**
2. Klik en **open** de my_TRUSTED_SPOOF_HOSTS afzendergroep.
3. Klik op **Verzender toevoegen...** om een IP-adres, bereik, hostnaam of gedeeltelijke hostnaam toe te voegen.
4. Klik op **Indienen** om de wijzigingen in de afzender op te slaan.
5. Klik tot slot op **Veranderingen vastleggen** om de configuratie op te slaan.

Voorbeeld:



Verifiëren

Controleer of spoofed-berichten in quarantaine worden geplaatst

Verzend een testbericht dat één van uw domeinen als envelopafzender specificeert. Bevestig de filterwerking zoals verwacht door een berichtspoor op dat bericht uit te voeren. Het verwachte resultaat is dat het bericht in quarantaine wordt geplaatst omdat je nog geen uitzonderingen hebt gemaakt voor die afzenders die mogen parocheren.

<#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
```

Controleer of de spoedberichten met uitzondering van de regels worden afgeleverd

Spoof-Exception zenders zijn IP-adressen in uw afzendergroep(en) die in het filter hierboven worden genoemd.

RELAYLIST wordt genoemd omdat het door ESA wordt gebruikt om uitgaande post te verzenden. Berichten die door RELAYLIST worden verzonden zijn typisch uitgaande post, en zonder dit zou tot valse

positieven leiden, of uitgaande berichten die hierboven door de filter worden in quarantaine geplaatst.

Berichttraceringsvoorbeeld van een IP-adres dat is toegevoegd aan MY_TRUSTED_SPOOF_HOSTS met Spoof-Exception. De verwachte actie is leverantie en niet quarantaine. (Deze IP mag parodie vormen).

<#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
```

Gerelateerde informatie

- ESR-filtering van gespoofde post
- Beschermingsbewijs met verificatie afzender

Cisco interne informatie

Er is een functie verzoek bij het blootstellen van de RAT aan berichtfilters/inhoudsfilters om dit proces te vereenvoudigen:

Cisco bug-id CSCus49018 - ENH: blootstellen van RAT aan filteromstandigheden

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.