ESA FAQ: Hoe kan ik het ESA Anti-Spam testen?

Inhoud

[Inleiding](#)
[Voorwaarden](#)
[Vereisten](#)
[Gebruikte componenten](#)
[Hoe kan ik het ESA Anti-Spam testen?](#)
[Anti-spam testen met TELNET](#)
[Problemen oplossen](#)

Inleiding

Dit document beschrijft hoe de Cisco e-mail security applicatie (ESA) moet worden getest voor de optie Anti-Spam.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco ESA
- AsyncOS
- Cisco ESA anti-Spam optie

Gebruikte componenten

De informatie in dit document is gebaseerd op alle versies van AsyncOS.

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 de potentiële impact van elke opdracht begrijpen.

Hoe kan ik het ESA Anti-Spam testen?

Om de functionaliteit van de ESA Anti-Spam optie te testen, moet u een nieuw bericht aanmaken via TELNET of uw e-mailclient (Microsoft Outlook, Eudora, Thunderbird, Lotus Notes) en een van deze kopregels invoegen:

- X-advertentie: verdenken
- X-advertentie: Spam
- X-advertentie: Marketing

U kunt het bericht vervolgens via het ESA verzenden met de Anti-Spam functie ingeschakeld en de resultaten controleren.

Anti-spam testen met TELNET

Deze sectie verschaft een voorbeeld dat toont hoe u handmatig een testbericht kunt maken via de algemeen beschikbare TELNET-voorziening.

Gebruik de informatie in het volgende voorbeeld om een testbericht door TELNET te maken. Voer de informatie in die **vet** wordt weergegeven en de server dient te reageren zoals wordt weergegeven:

```
telnet hostname.example.com 25

220 hostname.example.com ESMTP
ehlo localhost
250-hostname.example.com
250-8BITMIME
250 SIZE 10485760
mail from:




250 sender <sender@example.com> ok
rcpt to:




250 recipient <recipient@example.com> ok
data
354 go ahead
X-Advertisement: Marketing
from: sender@example.com
to: recipient@example.com
subject: test

test
.
250 ok:  Message 120 accepted
```

Controleer de **mail_logs** en controleer de resultaten van het anti-spam scannen om er zeker van te zijn dat het bericht op dezelfde manier wordt behandeld als geschreven. Zoals in het vorige voorbeeld, stelt het standaard inkomende postbeleid vast dat de post marketing is:

```
Thu Jun 26 22:21:56 2014 Info: New SMTP DCID 66 interface 172.11.1.111 address
 111.22.33.111 port 25
Thu Jun 26 22:21:58 2014 Info: DCID 66 TLS success protocol TLSv1 cipher
 RC4-SHA
Thu Jun 26 22:21:58 2014 Info: Delivery start DCID 66 MID 119 to RID [0]
Thu Jun 26 22:21:59 2014 Info: Message done DCID 66 MID 119 to RID [0]
Thu Jun 26 22:21:59 2014 Info: MID 119 RID [0] Response '2.0.0 s5R2LhnL014175
 Message accepted for delivery'
Thu Jun 26 22:21:59 2014 Info: Message finished MID 119 done
Thu Jun 26 22:22:04 2014 Info: DCID 66 close
Thu Jun 26 22:22:53 2014 Info: SDS_CLIENT: URL scanner enabled=0
Thu Jun 26 22:25:35 2014 Info: SLBL: Database watcher updated from snapshot
 20140627T022535-slbl.db.
Thu Jun 26 22:26:04 2014 Info: Start MID 120 ICID 426
Thu Jun 26 22:26:04 2014 Info: MID 120 ICID 426 From: <sender@example.com>
Thu Jun 26 22:26:10 2014 Info: MID 120 ICID 426 RID 0 To:
 <recipient@example.com>
Thu Jun 26 22:26:20 2014 Info: MID 120 Subject 'test'
Thu Jun 26 22:26:20 2014 Info: MID 120 ready 201 bytes from <sender@example.com>
Thu Jun 26 22:26:20 2014 Info: MID 120 matched all recipients for per-recipient
 policy DEFAULT in the inbound table
Thu Jun 26 22:26:21 2014 Info: MID 120 interim verdict using engine:
 CASE marketing
Thu Jun 26 22:26:21 2014 Info: MID 120 using engine: CASE marketing
Thu Jun 26 22:26:21 2014 Info: MID 120 interim AV verdict using Sophos CLEAN
Thu Jun 26 22:26:21 2014 Info: MID 120 antivirus negative
Thu Jun 26 22:26:21 2014 Info: Message finished MID 120 done
Thu Jun 26 22:26:21 2014 Info: MID 121 queued for delivery
Thu Jun 26 22:26:21 2014 Info: New SMTP DCID 67 interface 172.11.1.111 address
 111.22.33.111 port 25
Thu Jun 26 22:26:21 2014 Info: DCID 67 TLS success protocol TLSv1 cipher RC4-SHA
Thu Jun 26 22:26:21 2014 Info: Delivery start DCID 67 MID 121 to RID [0]
Thu Jun 26 22:26:22 2014 Info: Message done DCID 67 MID 121 to RID [0]
Thu Jun 26 22:26:22 2014 Info: MID 121 RID [0] Response '2.0.0 s5R2QQso009266
 Message accepted for delivery'
Thu Jun 26 22:26:22 2014 Info: Message finished MID 121 done
Thu Jun 26 22:26:27 2014 Info: DCID 67 close
```

Problemen oplossen

Als het bericht niet wordt herkend als spam-, verdachte spam- of marketingberichten, **dan** bekijkt u het **Mail-beleid > inkomende e-mailbeleid** of **postbeleid > Uitgaande postbeleid**. Kies de knop Default Policy of Policy Name en klik op de hyperlink in de kolom Anti-Spam om de instellingen en de configuratie van de stijl Anti-Spam te controleren.

Cisco raadt u aan de **positief geïdentificeerde** SSM**-instellingen**, de **vermoedelijke** SSM**-instellingen** en/of de **e-mailinstellingen voor het** in de handel brengen naar wens in te schakelen.