

FOIRE AUX QUESTIONS ESA : Comment est-ce que je peux tester la caractéristique d'anti-Spam ESA ?

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Comment est-ce que je peux tester la caractéristique d'anti-Spam ESA ?](#)

[Anti-Spam de test avec TELNET](#)

[Dépannez](#)

Introduction

Ce document décrit comment tester la caractéristique d'anti-Spam des appareils de sécurité du courrier électronique de Cisco (ESA).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco ESA
- AsyncOS
- Caractéristique d'anti-Spam de Cisco ESA

[Composants utilisés](#)

Les informations dans ce document sont basées sur toutes les versions d'AsyncOS.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Comment est-ce que je peux tester la caractéristique d'anti-Spam ESA ?

Afin de tester la fonctionnalité de la caractéristique d'anti-Spam ESA, créez un nouveau message par l'intermédiaire de TELNET ou votre client de messagerie (Microsoft Outlook, Eudora, Thunderbird, Lotus Notes) et insérez une de ces en-têtes :

- **X-publicité : Suspect**
- **X-publicité : Spam**
- **X-publicité : Commercialisation**

Vous pouvez alors envoyer le message par l'ESA avec la fonction activée d'anti-Spam et surveiller les résultats.

Anti-Spam de test avec TELNET

Cette section fournit un exemple qui affiche comment créer manuellement un message-test par l'intermédiaire de l'utilitaire large-disponible de TELNET.

Employez les informations dans l'exemple suivant afin de créer un message-test par TELNET. Entrez dans l'information affichée en **gras**, et le serveur devrait répondre comme affiché :

```
telnet hostname.example.com 25
220 hostname.example.com ESMTF
ehlo localhost
250-hostname.example.com
250-8BITMIME
250 SIZE 10485760
mail from: <sender@example.com>
250 sender <sender@example.com> ok
rcpt to: <recipient@example.com>
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

Passez en revue les **mail_logs** et vérifiez les résultats de la lecture d'anti-Spam afin de s'assurer que le message est traité comme écrit. Selon l'exemple précédent, la stratégie d'arrivée par défaut de messagerie la détecte que la messagerie lance sur le marché :

```
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

Dépannez

Si le message n'est pas détecté comme Spam, Spam suspecté, ou commercialisation, passez en revue la **messagerie Polcies > des stratégies de messagerie entrante** ou **envoyez par mail les stratégies > les stratégies de mail sortant**. Choisissez la stratégie par défaut ou le nom de stratégie, et cliquez sur l'hyperlien dans la la colonne d'anti-Spam afin de vérifier les configurations et la configuration d'anti-Spam pour la stratégie.

Cisco recommande que vous activiez les **configurations Positif-identifiées de Spam**, les **configurations suspectées de Spam**, et/ou les **configurations d'email de vente** comme désirées.