ESA FAQ: ¿Cómo puedo probar la característica del Anti-Spam ESA?

Contenido

Introducción

Este documento describe cómo probar la característica del Anti-Spam del dispositivo de seguridad del correo electrónico de Cisco (ESA).

Prerequisites

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco ESA
- AsyncOS
- Característica del Anti-Spam de Cisco ESA

Componentes Utilizados

La información en este documento se basa en todas las versiones de AsyncOS.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

¿Cómo puedo probar la característica del Anti-Spam ESA?

Para probar las funciones de la característica del Anti-Spam ESA, cree un nuevo mensaje vía TELNET o su cliente de correo electrónico (Microsoft Outlook, Eudora, Thunderbird, Lotus Notes) y el separador de millares uno de estas encabezados:

- X-anuncio: Sospechoso
- X-anuncio: Spam
- X-anuncio: Comercialización

Usted puede después enviar el mensaje con el ESA con la característica del Anti-Spam habilitada y monitorear los resultados.

Pruebe el Anti-Spam con TELNET

Esta sección proporciona un ejemplo que muestre cómo crear manualmente un mensaje de prueba vía la utilidad Telnet ancho-disponible.

Utilice la información en el próximo ejemplo para crear un mensaje de prueba a través de TELNET. Ingrese la información mostrada en intrépido, y el servidor debe responder como se muestra:

```
telnet hostname.example.com 25

220 hostname.example.com ESMTP
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
```

Revise los mail_logs y verifique el resultado de la exploración del anti-Spam para asegurar que el mensaje esté tratado según lo escrito. Según el ejemplo anterior, la directiva entrante predeterminada del correo detecta que el correo está comercializando:

```
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
```

Troubleshooting

Si el mensaje no se detecta como el Spam, el Spam sospechoso, o comercialización, revise el **correo Polcies >** las **directivas del correo entrante** o las **directivas del correo > las directivas salientes del correo**. Elija el nombre de la política predeterminada o de la directiva, y haga clic el enlace hipertexto en el columna del Anti-Spam para verificar las configuraciones y la configuración del Anti-Spam para la directiva.

Cisco recomienda que usted habilita las **configuraciones Positivo-identificadas del Spam**, las **configuraciones sospechosas del Spam**, y/o las **configuraciones del correo electrónico del márketing** según lo deseado.