ESA FAQ: Como posso eu testar a característica do Anti-Spam ESA?

Índice

Introdução

Este documento descreve como testar Cisco envia por correio eletrónico a característica do Anti-Spam da ferramenta de segurança (ESA).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

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

Componentes Utilizados

A informação neste documento é baseada em todas as versões de AsyncOS.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Como posso eu testar a característica do Anti-Spam ESA?

A fim testar a funcionalidade da característica do Anti-Spam ESA, crie uma mensagem nova através de TELNET ou seu cliente de e-mail (Microsoft outlook, Eudora, Thunderbird, Lotus Notes) e inserção uma destes encabeçamentos:

- X-propaganda: Suspeito
- X-propaganda: Spam
- X-propaganda: Mercado

Você pode então enviar a mensagem com o ESA com a característica do Anti-Spam permitida e monitorar os resultados.

Teste o Anti-Spam com TELNET

Esta seção fornece um exemplo que mostre como criar manualmente um mensagem de teste através do utilitário Telnet amplamente disponível.

Use a informação no exemplo seguinte a fim criar um mensagem de teste com TELNET. Incorpore a informação mostrada em corajoso, e o server deve responder como mostrado:

```
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
```

Reveja os mail_logs e verifique o resultado da exploração do anti-Spam a fim assegurar que a mensagem está tratada como escrita. Conforme o exemplo anterior, a política de entrada do correio do padrão detecta que o correio está introduzindo no mercado:

```
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

Se a mensagem não é detectada como o Spam, o Spam suspeitado, ou o mercado, reveja o **correio Polcies > políticas do correio recebido** ou **políticas do correio > políticas que parte do correio**. Escolha o nome da política padrão ou da política, e clique o hiperlink o na coluna do Anti-Spam a fim verificar os ajustes e a configuração do Anti-Spam para a política.

Cisco recomenda que você permite os **ajustes Positivo-identificados do Spam**, os **ajustes suspeitados do Spam**, e/ou os **ajustes do email do mercado** como desejados.