Häufig gestellte Fragen zur ESA: Wie kann ich die ESA Anti-Spam-Funktion testen?

Inhalt

Einführung

Dieses Dokument beschreibt, wie die Anti-Spam-Funktion der Cisco E-Mail Security Appliance (ESA) getestet wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco ESA
- AsyncOS
- Cisco ESA Anti-Spam-Funktion

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf allen Versionen von AsyncOS.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Wie kann ich die ESA Anti-Spam-Funktion testen?

Um die Funktionalität der ESA Anti-Spam-Funktion zu testen, erstellen Sie über TELNET oder Ihren E-Mail-Client (Microsoft Outlook, Eudora, Thunderbird, Lotus Notes) eine neue Nachricht, und fügen Sie einen der folgenden Header ein:

- X-Advertisement: Verdächtig
- X-Advertisement: Spam
- X-Advertisement: Marketing

Sie können die Nachricht dann über die ESA mit aktivierter Anti-Spam-Funktion senden und die Ergebnisse überwachen.

Anti-Spam mit TELNET testen

Dieser Abschnitt enthält ein Beispiel, in dem veranschaulicht wird, wie eine Testnachricht manuell über das allgemein verfügbare TELNET-Dienstprogramm erstellt wird.

Verwenden Sie die Informationen im nächsten Beispiel, um eine Testnachricht über TELNET zu erstellen. Geben Sie die Informationen in **Fettschrift ein**, und der Server sollte wie folgt antworten:

```
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
```

Überprüfen Sie die **mail_logs** und das Ergebnis der Anti-Spam-Prüfung, um sicherzustellen, dass die Nachricht wie geschrieben behandelt wird. Wie im vorherigen Beispiel gezeigt, erkennt die Richtlinie für eingehende E-Mails, dass die E-Mail Marketing lautet:

```
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
```

Fehlerbehebung

Wenn die Nachricht nicht als Spam, vermuteter Spam oder Marketing erkannt wird, überprüfen Sie die **Mail-Richtlinien > Richtlinien für eingehende E-Mails** oder **Mail-Policys > Richtlinien für ausgehende E-Mails**. Wählen Sie den Standard-Policy- oder Policy-Namen aus, und klicken Sie auf den Hyperlink in der Spalte Anti-Spam, um die Anti-Spam-Einstellungen und die Konfiguration für die Richtlinie zu überprüfen.

Cisco empfiehlt, die **Einstellungen für positiv identifizierten Spam**, die **Einstellungen für vermuteten Spam** und/oder die **Marketing-E-Mail-Einstellungen** wie gewünscht zu aktivieren.