Содержание

[Введение](#)
[Предварительные условия](#)
[Требования](#)
[Используемые компоненты](#)
[Как я могу протестировать функцию Защиты от спама ESA?](#)
[Протестируйте защиту от спама с TELNET](#)
[Устранение неполадок](#)

Введение

Этот документ описывает, как протестировать Cisco функция Защиты от спама Email Security Appliance (ESA).

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- ESA Cisco
- AsyncOS
- Функция Защиты от спама ESA Cisco

Используемые компоненты

Сведения в этом документе основываются на всех версиях AsyncOS.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Как я могу протестировать функцию Защиты от спама ESA?

Для тестирования функциональности функции Защиты от спама ESA создайте новое сообщение через TELNET или почтового клиента (Microsoft Outlook, Юдора, Thunderbird, Lotus Notes) и вставьте один из этих заголовков:

- **X-реклама: подозреваемый**

- X-реклама: спам
- X-реклама: маркетинг

Можно тогда передать сообщение через ESA с активированной опцией Для защиты от спама и контролировать результаты.

Протестируйте защиту от спама с TELNET

Этот раздел предоставляет пример, который показывает, как вручную создать тестовое сообщение через широко доступную служебную программу Telnet.

Используйте информацию в следующем примере для создания тестового сообщения через TELNET. Введите информацию, показанную **полужирным**, и сервер должен ответить как показано:

```
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
```

Рассмотрите **mail_logs** и проверьте результат сканирования защиты от спама, чтобы гарантировать, что сообщение рассматривается, как записано. Согласно предыдущему примеру, входящая почтовая политика по умолчанию обнаруживает, что Торгует почта:

```
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
```

Устранение неполадок

Если сообщение не обнаружено , поскольку Спам, Подозреваемый Спам, или Маркетинг, рассматривает **Почтовый Polcies> Политика Входящей почты** или **Почтовая Политика> Политика Исходящей почты**. Выберите Default Policy или Policy Name, и нажмите гиперссылку в столбец Anti-Spam для проверки параметров настройки Для защиты от спама и конфигурации для политики.

Cisco рекомендует включить **Положительно определенные Параметры настройки Спама**, **Подозреваемые Параметры настройки Спама** и/или **Торгующие Почтовые Параметры настройки** , как желаемый.