識別並允許SenderBase信譽得分(SBRS)較差的郵件伺服器

目錄

簡介

本文描述如何通過郵件安全裝置(ESA)識別並暫時允許具有低SenderBase信譽得分(SBRS)的郵件伺服器。

背景資訊

發件人信譽過濾是垃圾郵件防護的第一層，允許您根據SBRS確定的發件人可信度來控制通過電子郵件網關的郵件。SBRS較差的電子郵件伺服器可能會根據您的首選項拒絕其連線或退回郵件。

問題

郵件伺服器連線到ESA，並報告為SBRS較差，並且由於連線伺服器收到的554 SMTP響應導致電子郵件延遲。

554響應示例：

```
-----Original Message-----
From: Mail Delivery System [mailto:Mailer-Daemon@example.domain.com]
Sent: 25 April 2013 23:23
To: user@companyx.com
Subject: Mail delivery failed: returning message to sender

This message was created automatically by mail delivery software.

A message that you sent could not be delivered to one or more of its
recipients. This is a permanent error. The following address(es) failed:

person@example.domain.com
SMTP error from remote mail server after initial connection:
host gatekeeper.companyx.com [195.195.195.1]: 554-gatekeeper1.companyx.com
554 Your access to this mail system has been rejected due to the sending
MTA's poor reputation. If you believe that this failure is in error, please
contact the intended recipient via alternate means.
```

解決方案

識別不良的SBRS郵件伺服器

使用命令列介面(CLI)作為圖形使用者介面(GUI)消息跟蹤預設情況下不記錄被拒絕的連線。

> **附註**： 可以在**GUI > Security Services > Message Tracking > Enable "Rejected Connection Handling"**處啟用被拒絕連線的跟蹤

對域使用**grep**，以提取該域的所有相關日誌記錄資料。 對於此輸出，使用的示例域為*test.com*:

```
myesa.local> grep "test.com" mail_logs

Info: New ICID 1512 to Management (10.0.0.1) from 198.51.100.1 connecting host reverse DNS
hostname: smtp1.

test.com


Info: MID 6531

ICID 1512 From: test@test.com
```

然後**grep**傳入連線ID(ICID)以提取郵件主機資訊。 ICID日誌記錄用於顯示所有資訊，例如：傳送主機IP地址、DNS驗證主機名（如果可用）、發件人組匹配和關聯的SBRS得分：

```
myesa.local> grep "ICID 1512" mail_logs


Tue Mar 10 12:04:29 2015 Info: New SMTP ICID 1512 interface Management (10.0.0.1) address
198.51.100.1 reverse dns host unknown verified smtp1.test.com
Tue Mar 10 12:04:29 2015 Info: ICID 1512 REJECT SG BLACKLIST match sbrs[-10:-3] SBRS -4.0
```

允許較差的SBRS郵件伺服器通過ESA

1. 在GUI中，導航到**Mail Policies > HAT overview**。
2. 按一下 **新增發件人組……**
3. 使用有意義的名稱為發件人組命名。
4. 選擇訂單，使其位於BLACKLIST發件人組上方。
5. 選擇郵件策略、**ACCEPTED**或**THROTTLED**。
6. 將所有其他欄位留空。
7. 按一下「提交並新增寄件者」
8. 根據grep命令新增受影響主機的IP地址或DNS主機名。
9. 按一下**Submit**
10. 檢查HAT概述並確保正確訂購新的發件人組。
11. 最後，按一下**Commit**儲存所有配置更改。

對於發件人地址，允許使用以下格式：

- IPv6地址，例如2001:420:80:1::5
- IPv4地址，如10.1.1.0
- IPv4或IPv6子網，例如10.1.1.0/24、2001:db8::/32
- IPv4或IPv6地址範圍，例如10.1.1.10-20、10.1.1-5或2001:db8::1-2001:db8::10

- 主機名，例如example.com
- 部分主機名，如.example.com。

在如上所示的示例中，為了允許以*test.com*結尾的任何其他郵件伺服器資訊，應將其配置為：

```
198.51.100.1
smtp1.test.com
.test.com
```

相關資訊

關於Cisco SenderBase