잘못된 SBRS(SenderBase Reputation Score) 메일 서버 식별 및 허용

목차

소개

이 문서에서는 ESA(Email Security Appliance)를 통해 SBRS(SenderBase Reputation Score)가 낮은 메일 서버를 식별하고 임시로 허용하는 방법에 대해 설명합니다.

배경 정보

발신자 평판 필터링은 SBRS에 의해 결정된 발신자의 신뢰성에 따라 이메일 게이트웨이를 통해 전달되는 메시지를 제어할 수 있는 첫 번째 스팸 차단 계층입니다. SBRS가 부족한 이메일 서버는 사용자의 환경 설정에 따라 연결이 거부되거나 메시지가 반송될 수 있습니다.

문제

메일 서버는 ESA에 연결되며 SBRS가 불량으로 보고되고 연결 서버에서 수신한 554 SMTP 응답으로 인해 이메일이 지연됩니다.

샘플 554 응답:

```
-----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.
```

솔루션

불량 SBRS 메일 서버 식별

CLI(Command Line Interface)를 GUI(Graphical User Interface)의 메시지 추적에서 기본적으로 거부된 연결을 기록하지 않습니다.

> **참고:** 거부된 연결 추적은 **GUI > Security Services(보안 서비스) > Message Tracking(메시지 추적) > Enable "Rejected Connection Handling(거부된 연결 처리 사용)"에서 활성화할** 수 있습니다.

해당 도메인에 대해 모든 관련 로깅 데이터를 가져오려면 grep를 사용합니다. 이 출력의 경우 사용되는 예제 도메인은 *test.com입니다*.

```
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
```

그런 다음 ICID(Incoming Connection ID)에 grep 하여 메일 호스트 정보를 추출합니다. ICID는 호스트 IP 주소 전송, DNS 확인 호스트 이름(사용 가능한 경우), 발신자 그룹 일치, 관련 SBRS 점수 등의 모든 정보를 표시하기 위해 사용됩니다.

```
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
```

ESA를 통해 불량 SBRS 메일 서버 허용

1. GUI에서 Mail Policies(**메일 정책) > HAT overview(HAT 개요)로 이동합니다**.
2. 클릭 **발신자 그룹 추가...**
3. Sender Group의 이름을 의미 있는 이름으로 지정합니다.
4. BLACKLIST Sender Group(블랙리스트 발신자 그룹) 위에 오도록 주문을 선택합니다.
5. 메일 정책, ACCEPTED 또**는 THROTTLED를 선택합니다**.
6. 다른 모든 필드는 비워 둡니다.
7. 전송 **및 발신자 추가를 클릭합니다.**
8. grep 명령에 있는 영향받는 호스트의 IP 주소 또는 DNS 호스트 이름을 추가합니다.
9. Submit(제출)을 **클릭합니다.**
10. HAT 개요를 검토하고 새 Sender Group이 올바르게 주문되었는지 확인합니다.
11. 마지막으로 Commit을 클릭하여 모든 컨피그레이션 변경 사항을 저장합니다.

발신자 주소의 경우 다음 형식이 허용됩니다.

- 2001:420:80:1::5와 같은 IPv6 주소

- IPv4 주소(예: 10.1.1.0)
- IPv4 또는 IPv6 서브넷(예: 10.1.1.0/24, 2001:db8::/32)
- IPv4 또는 IPv6 주소 범위(예: 10.1.1.10-20, 10.1.1-5 또는 2001:db8::1-2001:db8::10)
- example.com과 같은 호스트 이름
- 부분 호스트 이름(예: .example.com)

위 예제에서 *test.com*으로 끝나는 다른 메일 서버 정보를 허용하기 위해 다음과 같이 구성되었을 수 있습니다.

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

관련 정보

Cisco SenderBase 정보