识别并且提供恶劣的SenderBase名誉斯克尔(SBRS)邮件服务器

目录

简介

此条款描述如何通过电子邮件安全工具(ESA)识别和临时地允许有恶劣的SenderBase名誉的斯克尔(SBRS)邮件服务器。

背景信息

发送方名誉过滤是垃圾邮件保护第一块层，允许您控制通过根据发送方的可信赖性的电子邮件网关来如SBRS取决于的消息。 有恶劣的SBRS的电子邮件服务器能有他们的连接拒绝的，或者根据您的首选重新启动的，他们的消息。

问题

因为恶劣的SBRS和电子邮件延迟的归结于连接的服务器，接收的554 SMTP答复邮件服务器连接对ESA和报告。

示例554答复：

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

解决方案

识别可怜的SBRS邮件服务器

请使用命令行界面(CLI)，因为图形用户界面的(GUI)默认情况下消息跟踪不记录已拒绝连接。

> **注意**： 跟踪已拒绝连接可以启用在**GUI > Security Services>消息跟踪>enable "已拒绝连接处理"**

请使用**grep**域为了请求所有相关日志数据该域。 对于此输出，使用的示例域是*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
```

然后**grep**解压缩邮件主机信息的流入连接ID (ICID)。 ICID记录使用为了暴露所有信息例如： 发送主机IP地址， DNS验证主机名(若有)， sendergroup匹配和相关的SBRS分数：

```
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
```

通过ESA允许可怜的SBRS邮件服务器

1. 从GUI，请导航**邮寄策略>帽子概述**。
2. 单击**添加发送方组...**
3. 给出与一有意义的名称的发送方组。
4. 选择命令，以便它在黑名单发送方组上。
5. 选择任一项邮件策略，**接受**或**被节流**。
6. 空着其他字段。
7. 单击**提交并且添加发送方**
8. 添加IP地址或受影响的主机的DNS主机名如查找从grep命令。
9. 单击 **Submit**
10. 查看帽子概述并且保证新的发送方组正确地被定购。
11. 最后，请点击**进行**保存所有配置更改。

对于发送方地址，以下格式允许：

- IPv6地址例如2001:420:80:1::5
- IPv4地址例如10.1.1.0
- IPv4或IPv6子网例如10.1.1.0/24， 2001:db8::/32
- IPv4或IPv6地址范围例如10.1.1.10-20， 10.1.1-5或者2001:db8::1-2001:db8::10
- 主机名例如example.com
- 部分主机名例如.example.com。

在示例中如上所述，为了允许与*test.com的*其他邮件服务器信息结束，这将配置如下：

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

相关信息

关于思科SenderBase