Identifizieren und Zulassen schlechter SenderBase Reputation Score (SBRS)-Mail-Server

Inhalt

Einführung

In diesem Artikel wird beschrieben, wie E-Mail-Server mit schlechter SenderBase-Reputationsbewertung (SBRS) über die E-Mail-Security-Appliance (ESA) identifiziert und vorübergehend zugelassen werden.

Hintergrundinformationen

Die Filterung der Absenderreputation ist die erste Ebene des Spam-Schutzes, der es Ihnen ermöglicht, die Nachrichten, die über das E-Mail-Gateway gesendet werden, auf Basis der Vertrauenswürdigkeit des Absenders, wie vom SBRS bestimmt, zu steuern. Bei E-Mail-Servern mit schlechter SBRS können die Verbindungen abgelehnt oder die Nachrichten per Bounce zurückgesendet werden, je nach Ihren Präferenzen.

Problem

Ein Mailserver stellt eine Verbindung zur ESA her und wird als unzureichendes SBRS gemeldet, und E-Mails werden verzögert, da der Verbindungsserver eine SMTP-Antwort von 554 erhält.

Beispiel 554 Antwort:

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

Lösung

Identifizieren des schlechten SBRS-Mailservers

Verwenden Sie die Befehlszeilenschnittstelle (CLI), da die grafische Benutzeroberfläche (GUI)-Nachrichtenverfolgung abgelehnte Verbindungen standardmäßig nicht aufzeichnet.

> **Hinweis**: Die Nachverfolgung abgelehnter Verbindungen kann unter **GUI > Sicherheitsdienste > Nachrichtenverfolgung > Aktivieren "Abgelehnte Verbindungsbehandlung" aktiviert werden.**

Verwenden Sie **grep** gegen die Domäne, um alle zugehörigen Protokollierungsdaten für diese Domäne abzurufen. Für diese Ausgabe wird als Beispieldomäne *test.com* verwendet:

```
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
```

Grep the Incoming Connection ID (ICID) Then the mail host information. Die ICID-Protokollierung wird verwendet, um alle Informationen preiszugeben, z. B. die sendende Host-IP-Adresse, den für DNS verifizierten Hostnamen (falls vorhanden), die Absendergruppenzuordnung und den zugehörigen SBRS-Score:

```
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
```

Lassen Sie den schlechten SBRS-Mail-Server durch die ESA zu.

1. Navigieren Sie in der GUI zu **Mail Policies > HAT overview**.
2. Klicken **Absendergruppe hinzufügen..**
3. Geben Sie der Absendergruppe einen aussagekräftigen Namen.
4. Wählen Sie die Bestellung so aus, dass sie über der BLACKLIST-Absendergruppe liegt.
5. Wählen Sie entweder Mail-Policy, **ACCEPTED** oder **THROTTLED aus**.
6. Lassen Sie alle anderen Felder leer.
7. Klicken Sie auf **Senden und Absender hinzufügen.**
8. Fügen Sie entweder die IP-Adresse oder den DNS-Hostnamen des/der betroffenen Host(s)

über den Befehl grep ein.

9. Klicken Sie auf **Senden**
10. Überprüfen Sie die HAT-Übersicht, und stellen Sie sicher, dass die neue Absendergruppe korrekt bestellt wurde.
11. Klicken Sie abschließend auf **Commit (Übernehmen)**, um alle Konfigurationsänderungen zu speichern.

Für Absenderadressen sind die folgenden Formate zulässig:

- IPv6-Adressen wie 2001:420:80:1::5
- IPv4-Adressen wie 10.1.1.0
- IPv4- oder IPv6-Subnetze wie 10.1.1.0/24, 2001:db8::/32
- IPv4- oder IPv6-Adressbereiche wie 10.1.1.10-20, 10.1.1.1-5 oder 2001:db8::1-2001:db8::10
- Hostnamen wie beispiel.com
- Partielle Hostnamen, z. B. .example.com.

Im oben gezeigten Beispiel wäre dies wie folgt konfiguriert worden, um alle anderen Mail-Serverinformationen, die mit *test.com* enden, zuzulassen:

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

Zugehörige Informationen

Informationen zu Cisco SenderBase