Identifique e permita server deficientes do correio da contagem da reputação de SenderBase (SBR)

Índice

Introdução

Este artigo descreve como identificar e para permitir temporariamente server do correio com reputação deficiente de SenderBase marcar (SBR) através da ferramenta de segurança do email (ESA).

Informações de Apoio

A filtração da reputação do remetente é a primeira camada de proteção do Spam, permitindo que você controle as mensagens que vêm através do gateway de e-mail baseado na fiabilidade do remetente como determinada por SBR. Os servidores de e-mail com SBR deficientes podem ter suas conexões rejeitadas, ou suas mensagens saltadas, com base em suas preferências.

Problema

Um mail server conecta ao ESA e é relatado porque os SBR deficientes e os email são atrasado devido a uma resposta de 554 S TP recebida pelo server de conexão.

Resposta da amostra 554:

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

Solução

Identifique o mail server deficiente SBR

Use o comando line interface(cli) porque o rastreamento de mensagem das interfaces gráficas de usuário (GUI) não grava conexões rejeitadas à revelia.

> Nota: O seguimento de conexões rejeitadas pode ser permitido em **serviços > em rastreamento de mensagem do > segurança GUI > permite "a manipulação rejeitada da conexão"**

Use o **grep** contra o domínio a fim puxar todos os dados de registro relacionados contra esse domínio. Para esta saída, o domínio do exemplo usado é *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
```

Então **grep a** conexão recebida ID (ICID) para extrair a informação do host de correio. O ICID está registrando é usado a fim revelar toda a informação como: enviando o endereço IP de Um ou Mais Servidores Cisco ICM NT do host, o DNS verificou o hostname (se disponível), sendergroup que combina e os SBR associados marcam:

```
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
```

Permita o mail server deficiente SBR com o ESA

1. Do GUI, navegue **para enviar políticas > vista geral do CHAPÉU**.
2. O clique **adiciona o grupo do remetente…**
3. Nomeie o grupo do remetente com um nome significativo.
4. Selecione a ordem de modo que esteja acima do grupo do remetente da LISTA NEGRA.
5. Selecione uma ou outra política do correio, **ACEITADA** ou **ESTRANGULADA**.
6. Saa de todos campos restantes vazios.
7. O clique **submete e adiciona remetentes**
8. Adicionar o endereço IP de Um ou Mais Servidores Cisco ICM NT ou o nome de host DNS dos host afetados como ficado situado do comando grep.
9. O clique **submete-se**
10. Reveja a vista geral do CHAPÉU e assegure-se de que o grupo novo do remetente esteja pedido corretamente.
11. Finalmente, o clique **compromete** para salvar todas as alterações de configuração.

Para o endereço do remetente, os seguintes formatos são permitidos:

- Endereços do IPv6 tais como 2001:420:80:1::5

- Endereços do IPv4 tais como 10.1.1.0
- Sub-redes do IPv4 ou do IPv6 tais como 10.1.1.0/24, 2001:db8::/32
- Escalas de endereço do IPv4 ou do IPv6 tais como 10.1.1.10-20, 10.1.1-5, ou 2001:db8::1-2001:db8::10
- Nomes de host tais como example.com
- Nomes de host parciais tais como .example.com.

No exemplo como mostrado acima, a fim permitir todo o outro término da informação do mail server com *test.com*, isto seria configurado como:

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

Informações Relacionadas

Sobre Cisco SenderBase