

Como eu migro da quarentena local do Spam na ferramenta de segurança do email de Cisco (ESA) à quarentena central do Spam no dispositivo do Gerenciamento de segurança (S A)?

Índice

[Introdução](#)

[Como eu migro da quarentena local do Spam na ferramenta de segurança do email de Cisco \(ESA\) à quarentena central do Spam no dispositivo do Gerenciamento de segurança \(S A\)?](#)

[Hipóteses](#)

[Resumo da configuração](#)

[Procedimento](#)

Introdução

Este documento descreve como mover mensagens quarantined da quarentena local do Spam no ESA para a quarentena central do Spam no S A.

Como eu migro da quarentena local do Spam na ferramenta de segurança do email de Cisco (ESA) à quarentena central do Spam no dispositivo do Gerenciamento de segurança (S A)?

Hipóteses

A seguinte solução supõe que o dispositivo S A está configurado, de modo que o dispositivo ESA seja adicionado e a quarentena centralizada seja permitida.

Resumo da configuração

1. Enable centralizou a quarentena nos dispositivos ESA: Os serviços do > segurança GUI > o >Check da quarentena do Spam permitem a quarentena externo do Spam
2. Desabilite as quarentena locais: O GUI > o monitor > o Spam Quarantine> desmarcam permitem a quarentena do Spam
3. Submeta e comprometa mudanças.

4. Migre opcionalmente mensagens da quarentena de local à quarentena central através do processo abaixo.

Procedimento

No dispositivo ESA você precisaria de esvaziar a fila. Para esvaziar o workqueue:

Suspenda todos os ouvintes que usam o suspendlistener do comando CLI e escolha a opção "1. Tudo".

```
> suspendlistener
```

```
Choose the listener(s) you wish to suspend.  
Separate multiple entries with commas.
```

1. All
 2. Public
 3. Test
- ```
[*]> 1
```

Espera alguma hora até que a maioria de mensagens que pode entregar-se na fila da entrega estejam entregadas. (Você pode ver o número "de receptores ativos" na saída dos comandos status e dos tophosts).

```
>status
```

```
...
Gauges: Current
Connections
 Current Inbound Conn. 0
 Current Outbound Conn. 0
Queue
 Active Recipients 1
 Messages In Work Queue 0
 Kilobytes Used 85
 Kilobytes Free 71,303,083
 Messages In Quarantine
 Policy, Virus and Outbreak 10
 Kilobytes In Quarantine
 Policy, Virus and Outbreak 50
```

```
> tophosts
```

```
Sort results by:
```

1. Active Recipients
2. Connections Out
3. Delivered Recipients
4. Hard Bounced Recipients
5. Soft Bounced Events

```
[1]>1
```

```
Status as of: Mon Sep 29 13:09:53 2014 EDT
Hosts marked with '*' were down as of the last delivery attempt.
```

| # | Recipient Host | Active Recip. | Conn. Out | Deliv. Recip. | Soft Bounced | Hard Bounced |
|---|----------------|---------------|-----------|---------------|--------------|--------------|
| 1 | earthlink.net  | 1             | 0         | 2             | 0            | 0            |
| 2 | the.cpq.host   | 0             | 0         | 1             | 0            | 0            |

|   |                       |   |   |    |   |   |
|---|-----------------------|---|---|----|---|---|
| 3 | the.encryption.queue  | 0 | 0 | 14 | 0 | 0 |
| 4 | the.euq.queue         | 0 | 0 | 2  | 0 | 0 |
| 5 | the.euq.release.queue | 0 | 0 | 0  | 0 | 0 |

Se após 1-2 horas há ainda algumas mensagens na fila da entrega você precisaria de saltar estas mensagens usando os **bouncerecipients** do comando que escolhem a opção "3. Tudo" e a espera até a fila obtêm vazios.

> **bouncerecipients**

Please select how you would like to bounce messages:

1. By recipient host.
2. By Envelope From address.
3. All.

[1]> **3**

*Os remetentes de mensagens saltadas receberão a notificação que a mensagem não poderia ser entregue)*

Suspenda a entrega das mensagens usando o **suspenddel** do comando.

> **suspenddel**

Enter the number of seconds to wait before abruptly closing connections.

[30]>

Faça um backup de sua configuração através do **saveconfig** ou do **mailconfig** do comando como exige o cancelamento de suas rotas smtp e então as adicionar para trás mais tarde:

> **saveconfig**

Do you want to mask the password? Files with masked passwords cannot be loaded using loadconfig command. [Y]>

Através do GUI vão à rede - > as rotas S TP e removem todas as rotas smtp. (nota abaixo das rotas velhas porque você precisará das adicionar outra vez mais tarde). Ou, através da cópia do uso CLI para indicar então **claro** a remover.

> **smtproutes**

There are currently 4 routes configured.

Choose the operation you want to perform:

- NEW - Create a new route.
- EDIT - Edit destinations of an existing route.
- DELETE - Remove a route.
- PRINT - Display all routes.
- IMPORT - Import new routes from a file.
- EXPORT - Export all routes to a file.
- CLEAR - Remove all routes.

[ ]> **print**

..

[ ]> **clear**

Edite de “a rota smtp todos domínios restantes” e ajuste-a ao endereço IP de Um ou Mais Servidores Cisco ICM NT do dispositivo S A e à porta a **6025**.

```
>smtproutes
[]> edit
```

Enter the hostname you want to edit.  
[]> **ALL**

Choose the operation you want to perform:  
- ADD - Add new destination hosts.  
- REPLACE - Specify a new destination or set of destinations  
[]> **REPLACE**

Enter the destination hosts, separated by commas, which you want mail for ALL to be delivered.  
Enter USEDNS by itself to use normal DNS resolution for this route.  
Enter /dev/null by itself if you wish to discard the mail.  
Enclose in square brackets to force resolution via address (A) records, ignoring any MX records.  
[]> **mysma.com:6025**

Default route updated.

Verifique: Comprometa as mudanças e libere 2-3 mensagens do Spam de sua quarentena local como um teste.

```
> commit
```

Please enter some comments describing your changes:  
[]> changed default smtp route to point to SMA

Se as mensagens liberadas chegam corretamente à quarentena centralizada do Spam, libere o resto das mensagens.

As mensagens foram transferidas afinal ao dispositivo S A, restauram as rotas velhas das rotas S TP no dispositivo ESA.

Desabilite a quarentena local do Spam e permita a quarentena centralizada pelo contrário.

Recomece a operação normal no ESA usando o **resumo do** comando.

```
> resume
Mail delivery resumed.
```