# Detecte mensagens de Email falsificado no ESA e crie exceções para os remetentes que são permitidos ao spoof

## Índice



## Introdução

Este documento descreve como controlar a falsificação do email na ferramenta de segurança do email de Cisco (ESA) e como criar exceções para os usuários permitidos enviar email falsificado.

## Pré-requisitos

### Requisitos

Seu ESA deve processar correios entrantes e que parte, e deve usar uma configuração padrão de RELAYLIST para embandeirar mensagens como que parte.

### Componentes Utilizados

A informação neste documento é baseada no ESA com toda a versão de AsyncOS. As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Os componentes específicos usados incluem:

- Dicionário: usado para armazenar todos seus domínios internos.
- Filtro da mensagem: usado para segurar a lógica de detectar o email falsificado e de introduzir um encabeçamento em que os filtros satisfeitos possam atuar.
- Quarentena da política: usado para armazenar temporariamente duplicartes de email falsificado. Considere adicionar o endereço IP de Um ou Mais Servidores Cisco ICM NT de mensagens liberadas ao MY_TRUSTED_SPOOF_HOSTS para impedir mensagens futura deste remetente de incorporar a quarentena da política.
- MY_TRUSTED_SPOOF_HOSTS: aliste provendo seus endereços IP de Um ou Mais Servidores Cisco ICM NT de emissão confiados. Adicionar um endereço IP de Um ou Mais Servidores Cisco ICM NT de um remetente a esta lista saltará a quarentena e permitirá o remetente ao spoof. Nós estamos colocando remetentes confiados em seu grupo do remetente MY_TRUSTED_SPOOF_HOSTS de modo que as mensagens falsificado destes remetentes não quarantined.
- RELAYLIST: aliste para os endereços IP de Um ou Mais Servidores Cisco ICM NT de autenticação que são permitidos retransmitir, ou envie o email de partida. Se o email está sendo entregado através deste grupo do remetente a suposição é que a mensagem não é uma mensagem falsificado.

  **Note**: Se o grupo do remetente é chamado algo diferente do que MY_TRUSTED_SPOOF_HOSTS ou RELAYLIST, você terá que alterar o filtro com o nome do grupo correspondente do remetente. Também, se você tem ouvintes múltiplos, você pode igualmente ter mais de um MY_TRUSTED_SPOOF_HOSTS.

# Informações de Apoio

A falsificação é permitida à revelia em Cisco ESA. Há diversos, motivos válidos para permitir que outros domínios enviem sobre seu interesse.  Um exemplo comum,
administrador ESA pode querer a controlar email falsificado quarantining mensagens falsificado antes que estejam entregadas.

Para tomar uma ação específica tal como a quarentena no email falsificado, você deve primeiramente detectar o email falsificado.

## Que é falsificação do email?

A falsificação do email é a falsificação de um encabeçamento do email de modo que a mensagem pareça ter originado de alguém ou em algum lugar a não ser o origem real. A falsificação do email é uma tática usada no phishing e as campanhas do Spam porque os povos são mais prováveis abrir um email quando o pensam foram enviadas por uma fonte legítima.

## Como detectar o email falsificado?

Você quererá filtrar todas as mensagens que tiverem um remetente do envelope (Correio-de) e “amigável” (de) do encabeçamento que contém um de seus próprios domínios entrantes no endereço email.

## Como permitir a falsificação para remetentes específicos?

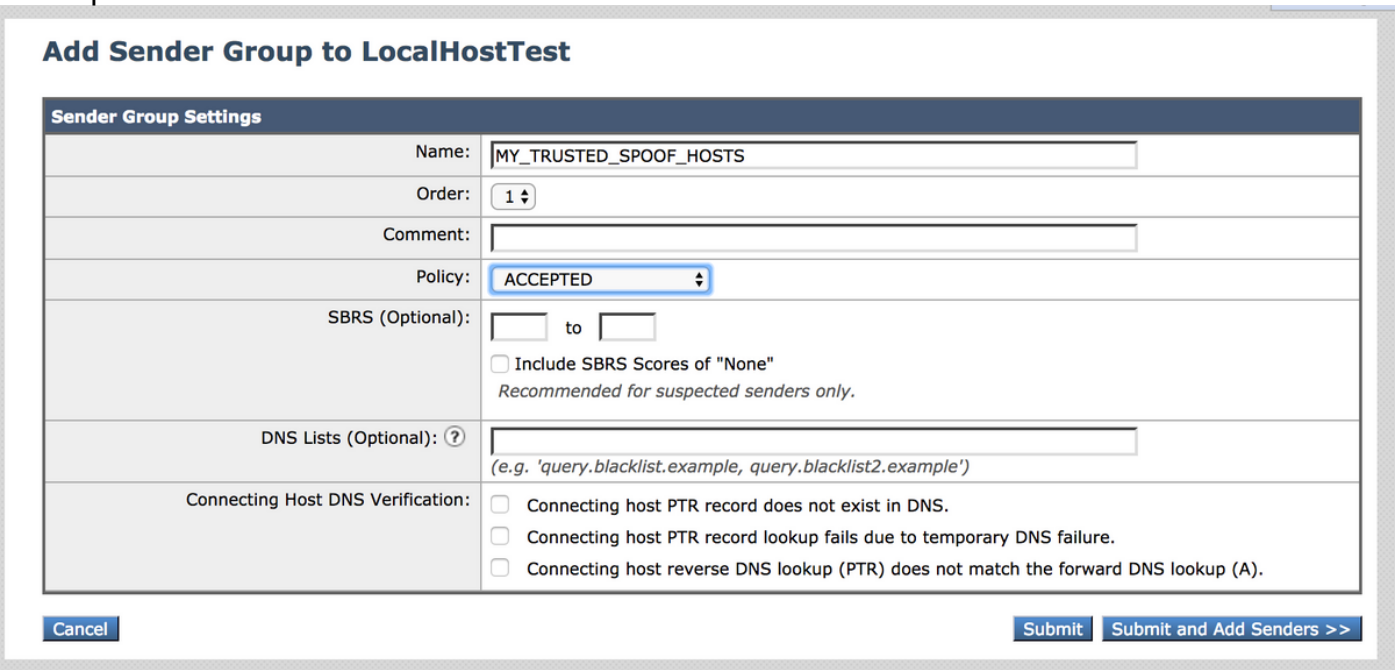
Ao executar o filtro da mensagem fornecido dentro deste artigo, as mensagens falsificado são etiquetadas com um encabeçamento, e o filtro satisfeito é usado para tomar a ação no encabeçamento. Para adicionar uma exceção, adicionar simplesmente o IP do remetente a MY_TRUSTED_SPOOF_HOSTS.

## Configurar

### Crie um Sendergroup

1. Do ESA GUI, navegue **para enviar políticas > vista geral do CHAPÉU**
2. Clique em Add.
3. No campo " nome " especifique **MY_TRUSTED_SPOOF_HOSTS**
4. No campo da “ordem” especifique **1**
5. Para o campo da “política”, especifique **ACEITADO**
6. O clique **submete-se** para salvar mudanças.
7. Finalmente, o clique **compromete mudanças** para salvar a configuração

Exemplo:

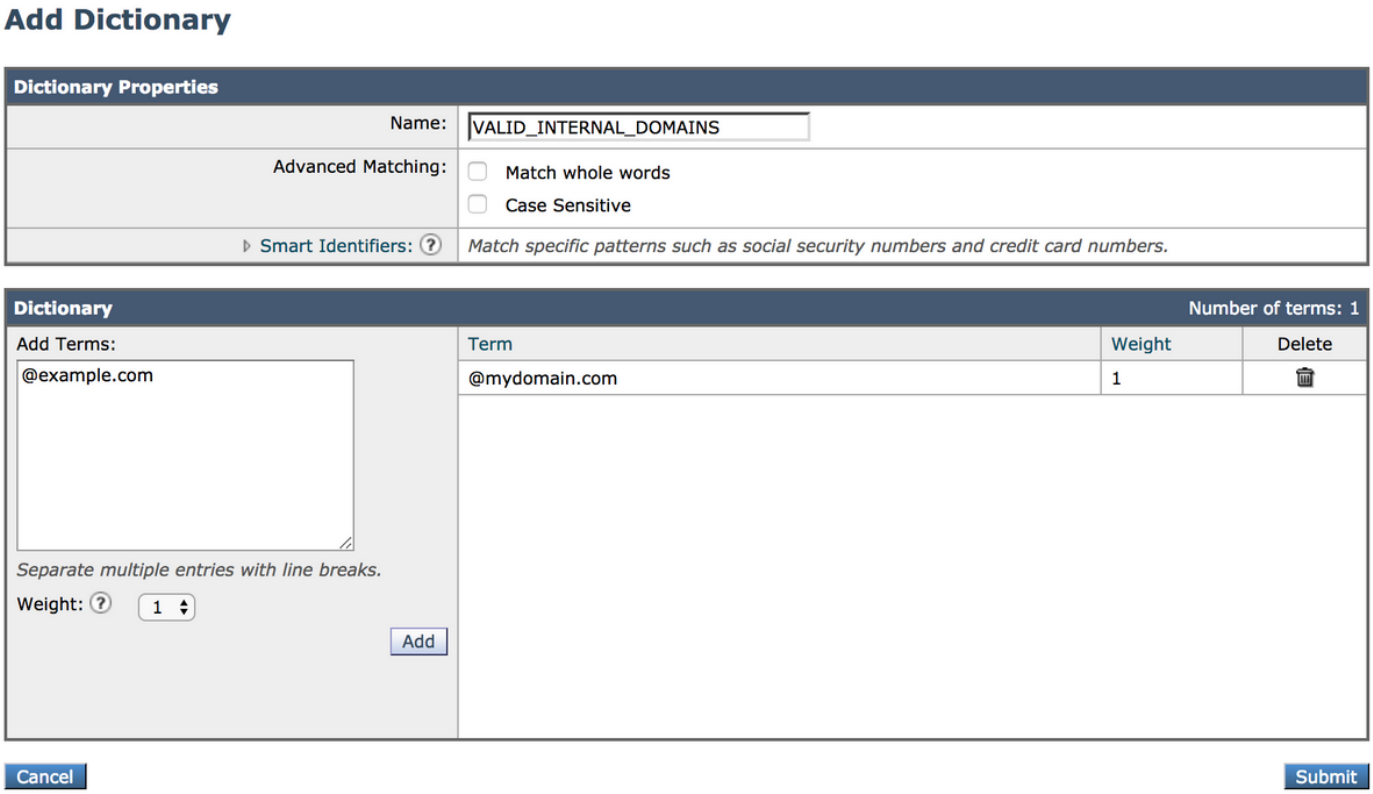



### Crie um dicionário

Crie um dicionário para todos os domínios que você quer desabilitar a falsificação para no ESA:

1. Do ESA GUI, navegue **para enviar políticas > dicionários.**
2. O clique **adiciona o dicionário.**
3. No campo " nome " especifique “VALID_INTERNAL_DOMAINS”, para fazer o copi e a cola do filtro da mensagem sem erros.
4. Sob “adicionar termos”, adicionam todos os domínios que você quer detectar a falsificação. Incorpore o domínio com @ um sinal que prepending o domínio e o clique adiciona.
5. Assegure-se de que do “a caixa de seleção das palavras inteiras fósforo” esteja desmarcada.
6. O clique **submete-se** para salvar as mudanças do dicionário.
7. Finalmente, o clique **compromete mudanças** para salvar a configuração

Exemplo:




## Crie um filtro da mensagem

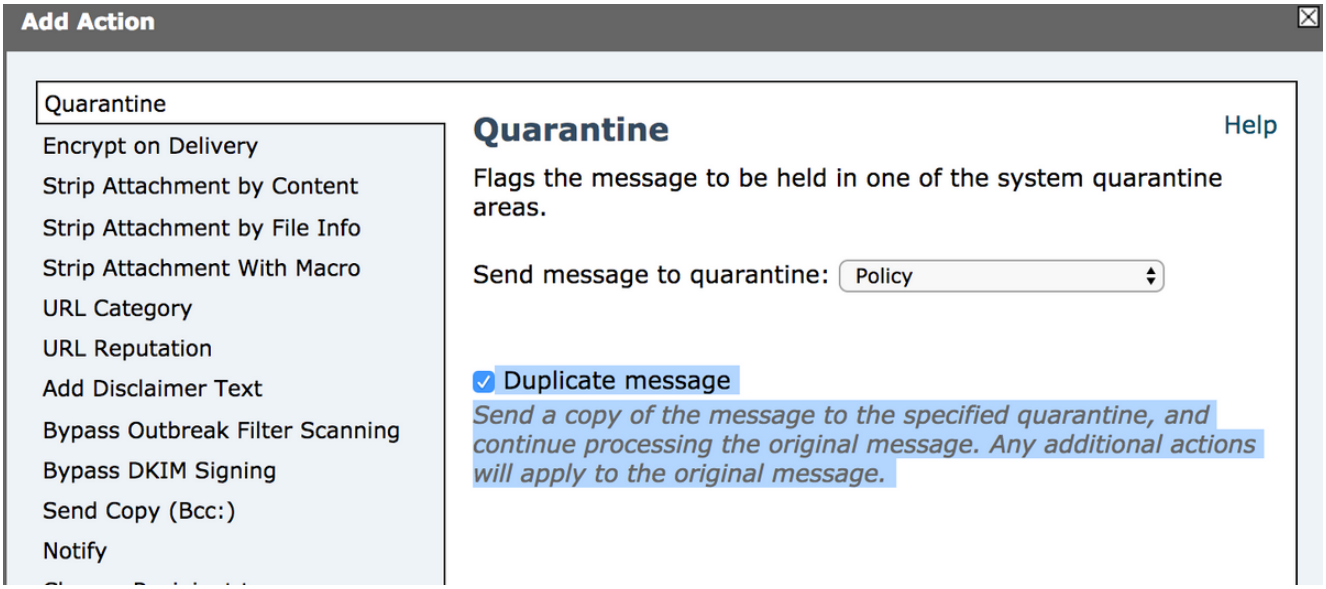
Em seguida, você precisará de criar um filtro da mensagem a fim leverage o dicionário apenas criado, “VALID_INTERNAL_DOMAINS”:

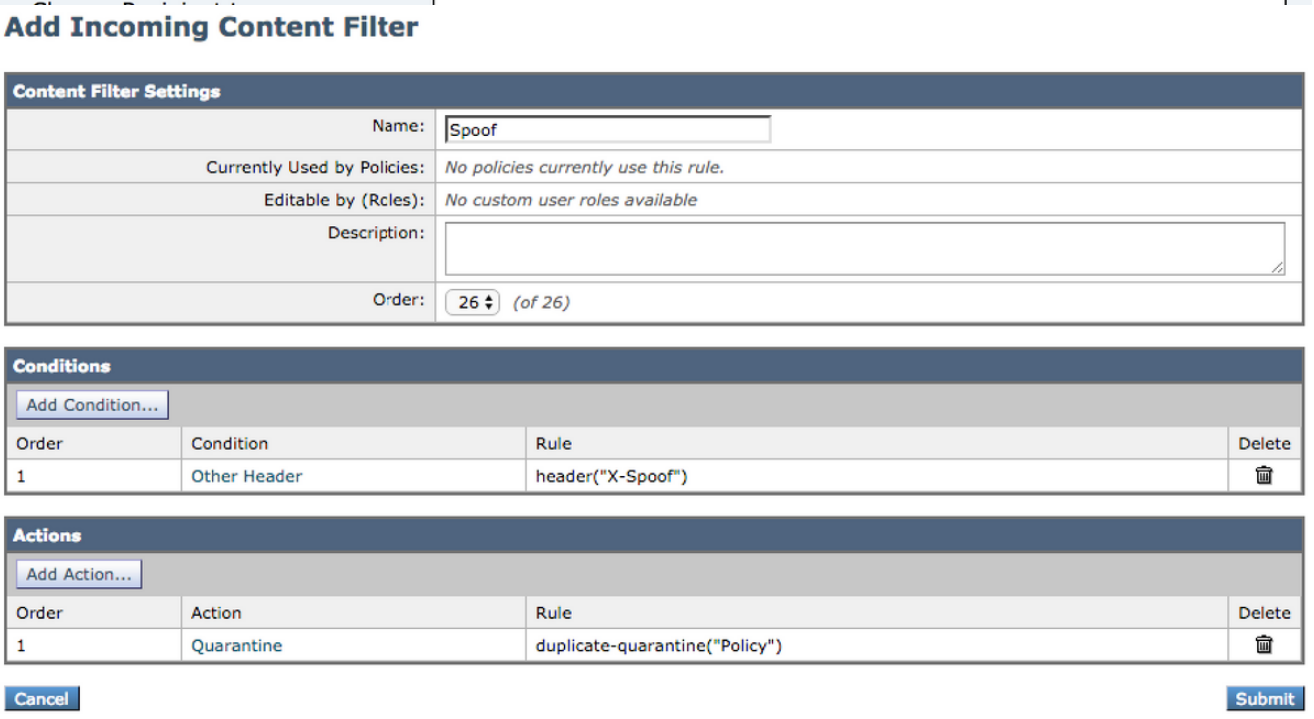
1. Conecte ao comando line interface(cli) do ESA.
2. Execute os **filtros do** comando.
3. Execute o comando new **criar um filtro novo da mensagem.**
4. A cópia e cola o seguinte exemplo do filtro, fazendo edita para seus nomes do grupo reais do remetente se necessário:

```
mark_spoofed_messages:
if(
(mail-from-dictionary-match("VALID_INTERNAL_DOMAINS", 1))
OR (header-dictionary-match("VALID_INTERNAL_DOMAINS","From", 1)))
AND ((sendergroup != "RELAYLIST")
AND (sendergroup != "MY_TRUSTED_SPOOF_HOSTS")
)
{
insert-header("X-Spoof", "");
}
```

5. Retorne à alerta principal CLI e a corrida **compromete** para salvar a configuração.
6. Navegue ao GUI > políticas do correio > filtros satisfeitos entrantes
7. Crie o filtro satisfeito entrante que toma a ação no X-spoof do encabeçamento do spoof: Adicionar a ação: duplicata-quarentena (“política ").

**Note**: A característica duplicada da mensagem mostrada aqui manterá uma cópia da mensagem, e continua a enviar o mensagem original ao receptor.




8. Ligue o filtro satisfeito às políticas do correio recebido em GUI > políticas do correio recebido de Policies> do correio
9. Submeta e comprometa mudanças

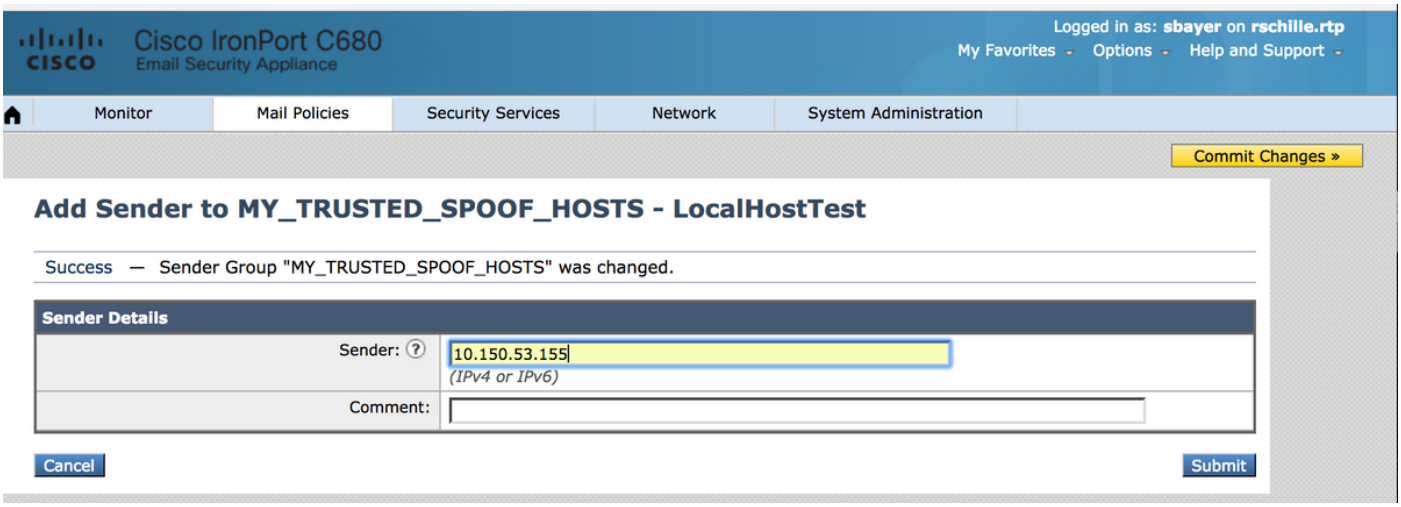
### Adicionar Spoof-exceções a MY_TRUSTED_SPOOF_HOSTS

Finalmente, você precisará de adicionar spoof-exceções (endereços IP de Um ou Mais Servidores Cisco ICM NT ou nomes de host) ao sendergroup MY_TRUSTED_SPOOF_HOSTS.

1. Navegue através da Web GUI: **Envie políticas > vista geral do CHAPÉU**
2. Clique e abra o grupo do remetente MY_TRUSTED_SPOOF_HOSTS.
3. Clique sobre “adicionam o remetente…” para adicionar um endereço IP de Um ou Mais Servidores Cisco ICM NT, uma escala, um nome de host, ou um nome de host parcial.

4. O clique **submete-se** para salvar as mudanças do remetente.
5. Finalmente, o clique **compromete mudanças** para salvar a configuração.

Exemplo:




## Verificar

### Verifique que as mensagens falsificado Quarantined

Envie um mensagem de teste que especifica um de seus domínios como o remetente do envelope. Valide o filtro está trabalhando como esperado executando uma trilha da mensagem nessa mensagem. O resultado esperado é que a mensagem obterá quarantined porque nós não criamos nenhuma exceções contudo para aqueles remetentes são permitidos que ao spoof.

```
Thu Apr 23 07:09:53 2015 Info: MID 102 ICID 9 RID 0 To: <test_user@domain.com>
Thu Apr 23 07:10:07 2015 Info: MID 102 Subject 'test1'
Thu Apr 23 07:10:07 2015 Info: MID 102 ready 177 bytes from <user_1@example.com>
Thu Apr 23 07:10:07 2015 Info: MID 102 matched all recipients for per-recipient policy DEFAULT
in the inbound table
Thu Apr 23 07:10:11 2015 Info: MID 102 interim verdict using engine: CASE spam negative
Thu Apr 23 07:10:11 2015 Info: MID 102 using engine: CASE spam negative
Thu Apr 23 07:10:11 2015 Info: MID 102 interim AV verdict using Sophos CLEAN
Thu Apr 23 07:10:11 2015 Info: MID 102 antivirus negative
Thu Apr 23 07:10:12 2015 Info: MID 102 quarantined to "Policy" (message
filter:quarantine_spoofed_messages)
Thu Apr 23 07:10:12 2015 Info: Message finished MID 102 done
```

### Verifique que mensagens da Spoof-exceção está sendo entregada

Os remetentes da “Spoof-exceção” são endereços IP de Um ou Mais Servidores Cisco ICM NT em seus grupos do remetente providos no filtro acima.

RELAYLIST é provido porque é usado pelo ESA para enviar o correio de partida. As mensagens que estão sendo enviadas por RELAYLIST são correio tipicamente de partida, e não incluir isto criaria falsos positivos, ou mensagens externa que estão sendo quarantined pelo filtro acima.

Exemplo do rastreamento de mensagem de um endereço IP de Um ou Mais Servidores Cisco ICM NT da “Spoof-exceção” que fosse a MY_TRUSTED_SPOOF_HOSTS. A ação prevista sido entrega e não quarantine. (Este IP é permitido ao spoof).

```
Thu Apr 23 07:25:57 2015 Info: Start MID 108 ICID 11
Thu Apr 23 07:25:57 2015 Info: MID 108 ICID 11 From: <user_1@example.com>
Thu Apr 23 07:26:02 2015 Info: MID 108 ICID 11 RID 0 To: <test_user@domain.com>
Thu Apr 23 07:26:10 2015 Info: MID 108 Subject 'test2'
Thu Apr 23 07:26:10 2015 Info: MID 108 ready 163 bytes from <user_1@example.com>
Thu Apr 23 07:26:10 2015 Info: MID 108 matched all recipients for per-recipient policy DEFAULT
in the inbound table
Thu Apr 23 07:26:10 2015 Info: MID 108 interim AV verdict using Sophos CLEAN
Thu Apr 23 07:26:10 2015 Info: MID 108 antivirus negative
Thu Apr 23 07:26:10 2015 Info: MID 108 queued for delivery
Thu Apr 23 07:26:10 2015 Info: Delivery start DCID 16 MID 108 to RID [0]
Thu Apr 23 07:26:11 2015 Info: Message done DCID 16 MID 108 to RID [0]
Thu Apr 23 07:26:11 2015 Info: MID 108 RID [0] Response '2.0.0 t58EVG9N031598 Message accepted
for delivery'
Thu Apr 23 07:26:11 2015 Info: Message finished MID 108 done
```

# Informações Relacionadas

- Filtração falsificado do correio ESA
- Proteção do spoof usando a verificação do remetente