As mensagens de salto com tamanho do cabeçalho da mensagem "552 #5.3.4 excedem o limite”

Índice

[Introdução](#)
[As mensagens de salto com tamanho do cabeçalho da mensagem "552 #5.3.4 excedem o limite”](#)
[Informações Relacionadas](#)

Introdução

Este documento descreve as mensagens rejeitadas e saltou devido aos grandes encabeçamentos na ferramenta de segurança do email de Cisco (ESA).

As mensagens de salto com tamanho do cabeçalho da mensagem "552 #5.3.4 excedem o limite”

Quando um host tenta enviar o correio com um grande encabeçamento, o ESA pode rejeitá-lo. O utilizador final pode ver um dos seguintes Mensagens de Erro:

```
"552 #5.3.4 message header size exceeds limit"
"500 #5.5.1 command not recognized"
"421 Exceeded bad SMTP command limit"
```

Em outros casos, o host pode manter-se experimentar de novo a mesma mensagem.

Há um limite 1000-line para o cabeçalho da mensagem. Quando o comprimento de cabeçalho excede 1000 linhas, o ESA envia o *tamanho do cabeçalho da mensagem da* mensagem *"552 #5.3.4 excede o limite” ao* host de emissão.

Alguns anfitriões podem ignorar esta mensagem e continuar a enviar dados. O ESA interpreta estes dados como o S TP comanda, e retornos, “o *comando 500 #5.5.1 não reconhecido*” para cada linha.

Após ter ultrapassado o limite de 4 comandos ruins S TP, o ESA retorna então a mensagem, “*421 excedeu o limite ruim do comando S TP*”, e deixa cair a conexão.

Este ajuste pode ser mudado no CLI somente:

```
myesa.local> listenerconfig
```

```
Currently configured listeners:
1. listener_myesa.local (on Management, 192.168.0.199) SMTP TCP Port 25 Public

Choose the operation you want to perform:
- NEW - Create a new listener.
- EDIT - Modify a listener.
- DELETE - Remove a listener.
- SETUP - Change global settings.
[]> setup

Enter the global limit for concurrent connections to be allowed across
all listeners.
[50]>

Listener istener_myesa.local Policy $TRUSTED max concurrency value of 300
will be limited to 50 by this concurrency setting.
Enter the global limit for concurrent TLS connections to be allowed across
all listeners.
[100]>

Concurrent TLS connections value of 100 will be limited to 50 by the global
limit for concurrent connections.

Enter the maximum number of message header lines. 0 indicates no limit.
[1000]>

Enter the rate at which injection control counters are reset.
[1h]>

Enter the timeout for unsuccessful inbound connections.
[5m]>

Enter the maximum connection time for inbound connections.
[15m]>

What hostname should Received: headers be stamped with?
1. The hostname of the Virtual Gateway(tm) used for delivering the message
2. The hostname of the interface the message is received on
[2]>

The system will always add a Message-ID header to outgoing messages that don't
already have one. Would you like to do the same for incoming messages? (Not
recommended.) [N]>

By default connections with a HAT REJECT policy will be closed with a banner
message at the start of the SMTP conversation. Would you like to do the rejection
at the message recipient level instead for more
detailed logging of rejected mail? [N]>
```

Se algum muda ou as atualizações estão feitas, retorne por favor à alerta principal CLI e a corrida **compromete** para salvar e executar as mudanças.

Informações Relacionadas

- Cisco envia por correio eletrónico a ferramenta de segurança - Guias do utilizador final
- Suporte Técnico e Documentação - Cisco Systems