Bounce berichten met "552 #5.3.4 berichtgrootte overschrijdt limiet"

Inhoud

Inleiding

Dit document beschrijft berichten die zijn verworpen en verzonden vanwege grote kopregels in de Cisco e-mail security applicatie (ESA).

Bounce berichten met "552 #5.3.4 berichtgrootte overschrijdt limiet"

Wanneer een host probeert post te verzenden met een grote header, kan het ESA deze versturen. De eindgebruiker kan een van de volgende foutmeldingen zien:

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

In andere gevallen kan de host hetzelfde bericht blijven herhalen.

Er is een limiet van 1000 regels voor de berichtkop. Als de veldnamenlengte meer dan 1000 regels bedraagt, verstuurt de ESA het bericht *"552 #5.3.4 berichtkopgrootte overschrijdt"* naar de verzendende host.

Sommige hosts negeren dit bericht en blijven gegevens verzenden. De ESA interpreteert deze gegevens als opdrachten voor het midden- en kleinbedrijf en retourneert "*opdracht 500 #5.5.1 niet herkend*" voor elke regel.

Na het overschrijden van de limiet van 4 slechte opdrachten terugkeert ESA dan het bericht, "*421 overschreden slechte limiet*"*, en laat de verbinding vallen*.

Deze instelling kan alleen op CLI worden gewijzigd:

```
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]>
```

Als er wijzigingen of updates worden aangebracht, keert u terug naar de hoofdprompt van CLI en voert u de wijzigingen op en voert u deze uit.

Gerelateerde informatie

- Cisco e-mail security applicatie - eindgebruikershandleidingen
- Technische ondersteuning en documentatie – Cisco Systems