

Bounce-Nachrichten mit "552 #5.3.4 Message-Header-Größe überschreitet Grenzwert"

Inhalt

[Einführung](#)

[Bounce-Nachrichten mit "552 #5.3.4 Message-Header-Größe überschreitet Grenzwert"](#)

[Zugehörige Informationen](#)

Einführung

In diesem Dokument werden die Nachrichten beschrieben, die aufgrund großer Header der Cisco E-Mail Security Appliance (ESA) abgelehnt und abgebrochen wurden.

Bounce-Nachrichten mit "552 #5.3.4 Message-Header-Größe überschreitet Grenzwert"

Wenn ein Host versucht, E-Mails mit einem großen Header zu senden, kann die ESA diese ablehnen. Möglicherweise wird dem Endbenutzer eine der folgenden Fehlermeldungen angezeigt:

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

In anderen Fällen versucht der Host möglicherweise weiterhin dieselbe Nachricht erneut.

Der Nachrichtenheader darf maximal 1000 Zeilen enthalten. Wenn die Headerlänge 1000 Zeilen überschreitet, sendet die ESA die Meldung *"552 #5.3.4 Message Header Size überschreitet Limit"* an den sendenden Host.

Einige Hosts ignorieren diese Nachricht möglicherweise und senden weiterhin Daten. Die ESA interpretiert diese Daten als SMTP-Befehle und gibt *"500 #5.5.1 Befehl nicht erkannt"* für jede Zeile zurück.

Nach Überschreiten der Obergrenze von vier fehlerhaften SMTP-Befehlen gibt die ESA die Meldung *"421 Overceeded bad SMTP command limit"* (421 überschritten die zulässige SMTP-Befehlsgrenze) zurück und beendet die Verbindung.

Diese Einstellung kann nur für die CLI geändert werden:

```
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 listener_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]>

Wenn Änderungen oder Aktualisierungen vorgenommen werden, kehren Sie zur CLI-Hauptaufforderung zurück, und führen Sie **commit aus**, um die Änderungen zu speichern und zu implementieren.

Zugehörige Informationen

- [Cisco Email Security Appliance - Benutzerhandbücher](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)