

Was kann dazu führen, dass das SMTP-Banner verzögert wird?

Inhalt

[Frage:](#)
[DNS-Probleme](#)
[Hohe CPU-Auslastung](#)

[Ressourcenschonungsmodus](#)
[Firewalls](#)

Frage:

Was kann dazu führen, dass das SMTP-Banner verzögert wird?

Wenn Sie in der Regel von telnet zu Port 25 eines Mailserver wechseln, erhalten Sie das SMTP-Banner sehr schnell. Hier einige Beispiele für SMTP-Banner:

```
220 host.example.com ESMTP
554 host.example.com
Manchmal kommt es zu Verzögerungen, und Sie erhalten lediglich die
Verbindungsinformationen in Ihrem Display. Hier ein Beispiel:
host.example.com> telnet 10.92.152.18 25
Versuchen Sie, 10.92.152.18..
Mit host.example.com verbunden.
Escape-Zeichen ist '^]'.
```

Beachten Sie, dass das Banner in diesem Beispiel fehlt. Nach einiger Zeit sollte das Banner endlich in der nächsten Zeile angezeigt werden. Dieser Artikel behandelt diese spezielle Situation. Es gibt vier gemeinsame Ursachen: **DNS-Probleme, hohe CPU-Auslastung, Ressourcenschonungsmodus und Firewalls.**

DNS-Probleme

Die häufigste Ursache für die Verzögerung des SMTP-Banners ist, dass die DNS-Suche länger als normal oder zeitlich abgelaufen war. Es gibt drei Suchvorgänge zwischen der Verbindung und der Banneranzeige: eine umgekehrte DNS- (oder PTR-Datensatz-) Suche, dann eine Vorwärts- (oder A-Datensatz-) Suche des im PTR-Datensatz angegebenen Hostnamens und anschließend eine SenderBase-Suche, um die SBRS (SenderBase Reputation Score) des verbindenden Hosts abzurufen.

Mit diesen Suchvorgängen wird bestimmt, zu welcher Absendergruppe der verbindende Host gehört. Dadurch wird festgelegt, welche Mail Flow-Richtlinie verwendet wird und ob E-Mails von diesem Host akzeptiert werden. Dies wirkt sich darauf aus, welches E-Mail-Banner ggf. gesendet wird. Daher ist es wichtig, dass diese Suchvorgänge vor der Bannerübergabe durchgeführt werden.

Um festzustellen, ob es sich um ein DNS-Problem handelt, müssen Sie sich in der Befehlszeile (CLI) der ESA anmelden und den Befehl nslookup verwenden. Dies ist von der Appliance aus wichtig, damit Sie aus ihrer Perspektive arbeiten. Zuerst müssen Sie die IP-Adresse kennen, die versucht, eine Verbindung herzustellen. Sie können Mail_logs oder Message Tracking verwenden, um die IP-Adresse abzurufen.

Sobald Sie die IP-Adresse kennen, können Sie mit nslookup zum Testen beginnen. Achten Sie darauf, zu zählen, wie viele Sekunden für jeden dieser Schritte benötigt werden.

DNS-Suchvorgänge! Zunächst die umgekehrte DNS-Suche:

```
host.example.com> nslookup 10.92.152.18
PTR= host.example.com TTL=2h 35m 43s
```

Suchen Sie anschließend den Hostnamen, der bei der umgekehrten DNS-Suche zurückgegeben wurde, wie folgt:

```
host.example.com> nslookup host.example.com
A = 10,92,152,18 TTL = 2 Std. 34 m 16 s
```

Wenn die Gesamtzeit für diese beiden Suchläufe ungefähr mit der Verspätung des Banners übereinstimmt, haben Sie die Ursache gefunden und möchten die DNS-Situation weiter prüfen. Die nächsten Schritte können das Testen anderer IP-Adressen aus verschiedenen Netzwerken umfassen. Dadurch erfahren Sie, ob das Problem auf bestimmte Hosts oder Netzwerke beschränkt ist oder ob ein allgemeineres DNS-Problem vorliegt.

Hohe CPU-Auslastung

Eine weitere mögliche Ursache für die Verzögerung des SMTP-Banners ist eine sehr hohe CPU-Auslastung.

Bei starker Auslastung eines Systems dauert alles länger. Sie können dies überprüfen, indem Sie auf der Registerkarte Monitor auf die Seite Systemstatus klicken oder den CLI-Befehl 'status detail' verwenden. In beiden Fällen werden die CPU-Nutzungsstatistiken im Abschnitt Messwerte angezeigt. Hier ein Beispiel:

```
CPU-Auslastung
Insgesamt 67 %
MGA 16 %
FALL 46 %
Brightmail AntiSpam 0 %
AntiVirus 0 %
Reporting 4 %
Quarantäne 0 %
```

Wenn die Gesamtsumme sehr hoch ist (95 % oder höher) und für mehrere Minuten hoch bleibt, ist

die CPU-Auslastung wahrscheinlich die Ursache für

Verzögerungen beim SMTP-Banner.

Ressourcenschonungsmodus

Eine weitere mögliche Ursache für die SMTP-Bannerverzögerung ist, dass das System in den Ressourcenschonungsmodus gewechselt ist. In diesem Modus schützt sich das System, indem es den Fluss der E-Mail-Akzeptanz verlangsamt. Dies geschieht, indem jede SMTP-Antwort, die gesendet wird, absichtlich verzögert wird. Um festzustellen, ob sich das System im Ressourcenschonungsmodus befindet, gehen Sie zur Seite Systemstatus auf der Registerkarte Monitor, oder verwenden Sie den CLI-Befehl 'status detail'. Suchen Sie im Abschnitt Messanzeigen nach der Zeile Ressourceneinsparung.

Hier ein Beispiel:

```
Ressourceneinsparung 0
```

Jede Nicht-Null-Zahl bedeutet, dass das System versucht, sich zu schützen, indem es SMTP-Antworten verlangsamt. Weitere Informationen zur Ressourceneinsparung finden Sie hier:

[Was ist der Ressourcenschonungsmodus?](#)

Firewalls

Die letzte häufige Ursache für SMTP-Bannerverzögerungen sind SMTP-fähige Firewalls. Diese Funktion, z. B. Durchführen von SMTP-Fixups oder Durchführen von Sicherheits-Scans für alle SMTP-Inhalte. Manchmal verzögert eine Firewall das Banner während der Prüfung und kann den Inhalt des SMTP-Banners ändern. Im Folgenden sehen Sie ein Beispiel für eine beliebige Firewall, die das SMTP-Banner ändert:

```
220
*****02*****
*****
0 *****2*****200**0*****0*00
```