# Que pode fazer com que o banner do SMTP seja atrasado?

## Índice

Pergunta:
Edições DNS
Uso da alta utilização da CPU

Modo da conservação do recurso
Firewall

## Pergunta:

Que pode fazer com que o banner do SMTP seja atrasado?

Tipicamente quando você telnet à porta 25 de um mail server, você obterá o banner do SMTP muito rapidamente. Estão aqui os exemplos dos banner do SMTP:

```
220 host.example.com ESMTP
554 host.example.com
Às vezes há um atraso e tudo que você obtém é a informação de conexão em
seu indicador. Aqui está um exemplo:
host.example.com > telnet 10.92.152.18 25
Tentando 10.92.152.18…
Conectado a host.example.com.
O caractere de escape é "^]".
```

Note que a bandeira falta neste exemplo. Depois que alguma hora passa, a bandeira deve finalmente ser indicada na linha seguinte. Este artigo endereça esta situação específica. Há quatro causas comum que nós discutiremos: **Edições DNS, uso da alta utilização da CPU, modo da conservação do recurso e Firewall**.

### Edições DNS

A maioria de causa comum do banner do SMTP que está sendo atrasado é que as pesquisas de DNS tomaram mais por muito tempo do que normal ou cronometrada para fora. Há três consultas que acontecem entre a conexão e o indicador da bandeira: uma consulta reversa registro DNS (ou PTR), então registro dianteiro (ou A) uma consulta do hostname dado no registro PTR, e uma consulta de SenderBase para obter então os SBR do host de conexão (contagem da reputação de SenderBase).

Estas consultas são usadas para determinar que grupo do remetente o host de conexão pertence. Isto determina que política do fluxo de correio é usada e se o correio será aceitado deste host. Isto afeta que bandeira do correio, eventualmente, será enviada. É por isso é crítico para estas consultas acontecer antes que a bandeira esteja dada.

Para determinar se a edição é DNS relativo, você precisará de registrar na linha de comando (CLI) do ESA e de usar o comando nslookup. É importante fazer isto do dispositivo próprio assim que você está trabalhando de sua perspectiva. Primeiramente você precisará de conhecer o endereço IP de Um ou Mais Servidores Cisco ICM NT que está tentando conectar. Você pode querer usar os mail_logs ou o rastreamento de mensagem para obter o endereço IP de Um ou Mais Servidores Cisco ICM NT.

Uma vez que você conhece o IP, você pode começar usar o nslookup para testar. Seja certo contar quantos segundos toma para cada um destes

Pesquisas de DNS! Primeiramente a pesquisa de DNS reversa:

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

Faça então uma consulta no hostname que voltou na pesquisa de DNS reversa, como assim:

```
host.example.com > nslookup host.example.com
A=10.92.152.18 TTL=2h 34m 16s
```

Se o tempo total para estas duas consultas combina aproximadamente quanto tempo a bandeira está atrasada, você encontrou a causa e querê-la-á rever mais a situação DNS. As próximas etapas podiam incluir o teste de outros endereços IP de Um ou Mais Servidores Cisco ICM NT das redes diferentes. Isto dir-lhe-á se a edição está isolada aos anfitriões ou às redes específicas, ou se há uma edição mais geral DNS.

## Uso da alta utilização da CPU

Uma outra causa possível do atraso do banner do SMTP é muito uso da alta utilização da CPU.

Quando um sistema está sob a carga pesada, tudo toma mais por muito tempo para acontecer. Você pode verificar este indo à página do status de sistema da aba do monitor, ou usando do “o comando CLI do detalhe estado”. Ambos dão as estatísticas do USO de CPU na seção dos calibres. Aqui está um exemplo:

```
Utilização da CPU
Total 67%
MGA 16%
CASO 46%
Brightmail AntiSpam 0%
AntiVirus 0%
Relatando 4%
Quarentena 0%
```

Se o total é muito alto (95% ou mais alto) e continua a permanecer alto por diversos minutos, o USO de CPU é provável a causa de

os atrasos do banner do SMTP.

## Modo da conservação do recurso

Uma outra causa possível do atraso do banner do SMTP é que o sistema entrou no modo da conservação do recurso. Neste modo, o sistema protege-se retardando o fluxo da aceitação do correio. Faz este intencionalmente atrasando cada resposta que S TP envia. Para determinar se o sistema reage do modo da conservação do recurso, vá à página do status de sistema da aba do monitor, ou pelo uso do “o comando CLI do detalhe estado”. Procure a linha da conservação do recurso na seção dos calibres.

Aqui está um exemplo:

```
Conservação 0 do recurso
```

Todo o número diferente de zero significa que o sistema está tentando se proteger retardando respostas S TP. Você pode aprender mais sobre a conservação do recurso aqui:

Que é modo da conservação do recurso?

## Firewall

A última causa comum de atrasos do banner do SMTP é os Firewall que são S TP ciente. Estes caracterizam como “reparares de execução S TP ou a Segurança running faz a varredura em todo o índice S TP. Às vezes um Firewall pode atrasar a bandeira quando fizer a varredura e alterar possivelmente do índice do banner do SMTP. Está aqui um exemplo de um Firewall popular que altera o banner do SMTP:

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