

SMTP 배너를 지연시킬 수 있는 원인은 무엇입니까?

목차

[질문:](#)
[DNS 문제](#)
[높은 CPU 사용량](#)

[리소스 절약 모드](#)
[방화벽](#)

질문:

SMTP 배너를 지연시킬 수 있는 원인은 무엇입니까?

일반적으로 메일 서버의 포트 25에 텔넷할 때 SMTP 배너를 매우 빠르게 얻을 수 있습니다.다음은 SMTP 배너의 예입니다.

```
220 host.example.com ESMTP
554 host.example.com

host.example.com> telnet 10.92.152.18 25
10.92.152.18...
host.example.com .
 '^] '.
```

이 예에서는 배너가 없습니다.시간이 지나면 배너가 다음 행에 표시됩니다.이 문서에서는 이러한 구체적인 상황을 다룹니다.다음과 같은 네 가지 일반적인 원인이 있습니다.**DNS 문제, 높은 CPU 사용량, 리소스 절약 모드 및 방화벽.**

DNS 문제

SMTP 배너가 지연되는 가장 일반적인 원인은 DNS 조회가 평소보다 오래 걸리거나 시간 초과되었기 때문입니다.연결과 배너 표시 간에는 다음과 같은 세 가지 조회가 있습니다.역방향 DNS(또는 PTR 레코드) 조회, PTR 레코드에 지정된 호스트 이름의 정방향(또는 A 레코드) 조회, 연결된 호스트의 SBR(SenderBase Reputation Score)를 얻기 위한 SenderBase 조회

이러한 조회는 연결 호스트가 속한 발신자 그룹을 확인하는 데 사용됩니다.Mail Flow Policy가 사용되는 항목과 이 호스트에서 메일을 수락할지 여부를 결정합니다.이는 전송되는 메일 배너가 있는 경우 영향을 미칩니다.따라서 배너가 제공되기 전에 이러한 조회가 반드시 이루어져야 합니다.

DNS 관련 문제인지 확인하려면 ESA의 CLI(Command Line)에 로그인하고 nslookup 명령을 사용해야 합니다. 어플라이언스 자체에서 이 작업을 수행하는 것이 중요합니다. 따라서 어플라이언스의 관점에서 작업을 수행해야 합니다. 먼저 연결하려는 IP 주소를 알아야 합니다. mail_logs 또는 Message Tracking을 사용하여 IP 주소를 가져올 수 있습니다.

IP를 알게 되면 nslookup을 사용하여 테스트할 수 있습니다. 각 작업에 걸리는 시간은 몇 초인지 확인하십시오.

DNS 조회! 먼저 역방향 DNS 조회:

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

그런 다음 다음과 같이 역방향 DNS 조회에서 반환된 호스트 이름을 조회합니다.

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

이 두 조회의 총 시간이 배너의 지연 시간과 대략 일치하면 원인을 찾았으며 DNS 상황을 더 자세히 검토하고자 합니다. 다음 단계는 서로 다른 네트워크에서 다른 IP 주소를 테스트하는 것을 포함할 수 있습니다. 이렇게 하면 문제가 특정 호스트 또는 네트워크로 격리되는지 아니면 일반적인 DNS 문제가 있는지 알 수 있습니다.

높은 CPU 사용량

SMTP 배너 지연의 또 다른 가능한 원인은 CPU 사용량이 매우 많습니다.

시스템이 과부하가 높을 때 모든 작업이 더 오래 걸립니다. Monitor 탭의 System Status(시스템 상태) 페이지로 이동하거나 'status detail' CLI 명령을 사용하여 이를 확인할 수 있습니다. 이 두 가지 모두 Gauges(게이지) 섹션의 CPU 사용량 통계를 제공합니다. 예를 들면 다음과 같습니다.

```
CPU
 67%
MGA 16%
 46%
Brightmail AntiSpam 0%
 0%
 4%
 0%
```

Total(합계)이 매우 높음(95% 이상)이고 몇 분 동안 계속 높은 상태를 유지하는 경우 CPU 사용량이 원인일 가능성이 높습니다.

SMTP 배너 지연.

리소스 절약 모드

SMTP 배너 지연의 또 다른 가능한 원인은 시스템이 리소스 절약 모드로 들어갔기 때문입니다. 이 모드에서는 메일 수락 흐름을 늦춰 스스로를 보호합니다. 이는 보내는 각 SMTP 응답을 의도적으로

지연시켜 수행합니다.시스템이 리소스 보존 모드인지 확인하려면 Monitor(모니터) 탭의 System Status(시스템 상태) 페이지로 이동하거나 'status detail' CLI 명령을 사용합니다.게이지(Gauges) 섹션에서 리소스 절약 라인을 찾습니다.

예를 들면 다음과 같습니다.

0

0이 아닌 숫자는 시스템이 SMTP 응답을 지연시켜 스스로를 보호하려고 함을 의미합니다. Resource Conservation에 대한 자세한 내용은 여기에서 확인할 수 있습니다.

[리소스 보존 모드란 무엇입니까?](#)

방화벽

SMTP 배너 지연의 마지막 일반적인 원인은 SMTP를 인식하는 방화벽입니다.이러한 기능(예: 'SMTP 수정' 수행 또는 모든 SMTP 콘텐츠에 대한 보안 검사 실행)때로는 방화벽이 SMTP 배너를 스캔하는 동안 배너를 지연시키고 SMTP 배너의 콘텐츠를 수정할 수 있습니다.다음은 SMTP 배너를 변경하는 일반적인 방화벽의 예입니다.

220

0 *****200**0*****0*0