What can cause the SMTP banner to be delayed?

Document ID: 118016

Contributed by Jackie Fleming and Enrico Werner Cisco TAC Engineers.
Jul 18, 2014

Contents

Question:

What can cause the SMTP banner to be delayed?

Typically when you telnet to port 25 of a mail server, you will get the SMTP banner very quickly. Here are examples of SMTP banners:

220 host.example.com ESMTP
554 host.example.com
Sometimes there is a delay and all you get is the connection information in your display. Here is an example:
host.example.com> telnet 10.92.152.18 25
Trying 10.92.152.18...
Connected to host.example.com.
Escape character is '^]'.

Note that the banner is missing in this example. After some time passes, the banner should finally be displayed on the next line. This article addresses this specific situation. There are four common causes we will discuss: ***DNS Issues, High CPU Usage, Resource Conservation mode and Firewalls***.

DNS Issues

The most common cause of the SMTP banner being delayed is that the DNS lookups took longer than normal or timed out. There are three lookups that happen between the connect and the banner display: a reverse DNS (or PTR record) lookup, then a forward (or A record) lookup of the hostname given in the PTR record, and then a SenderBase lookup to get the connecting host's SBRS (SenderBase Reputation Score).

These lookups are used to determine which Sender Group the connecting host belongs to. This determines what Mail Flow Policy is used and if mail will be accepted from this host. This affects what mail banner, if any, will be sent. That is why it is critical for these lookups to happen before the banner is given.

To determine if the issue is DNS related, you will need to log into the command line (CLI) of the ESA and use the nslookup command. It is important to do this from the appliance itself so you are working from its perspective. First you will need to know the IP address that is trying to connect. You may want to use the mail_logs or Message Tracking to get the IP address.

Once you know the IP, you can start using nslookup to test. Be sure to count how many seconds it takes for each of these

DNS lookups! First the reverse DNS lookup:

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

Then do a lookup on the hostname that came back on the reverse DNS lookup, like so:

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

If the total time for these two lookups approximately matches how long the banner is delayed, you have found the cause and will want to review the DNS situation further. The next steps could include testing other IP addresses from different networks. This will tell you if the issue is isolated to specific hosts or networks, or if there is a more general DNS issue.

High CPU Usage

Another possible cause of the SMTP banner delay is very high CPU usage.

When a system is under heavy load, everything takes longer to happen. You can check this by going to the System Status page of the Monitor tab, or by using the 'status detail' CLI command. Both of these will give the CPU usage statistics in the Gages section. Here is an example:

CPU Utilization
Total 67%
MGA 16%
CASE 46%
Brightmail AntiSpam 0%
AntiVirus 0%
Reporting 4%
Quarantine 0%

If the Total is very high (95% or higher) and continues to remain high for several minutes, CPU usage is likely the cause of

the SMTP banner delays.

Resource Conservation mode

Another possible cause of the SMTP banner delay is that the system has entered Resource Conservation mode. In this mode, the system protects itself by slowing down the flow of mail acceptance. It does this by intentionally delaying each SMTP response it sends. To determine if the system is in Resource Conservation mode, go to the System Status page of the Monitor tab, or by use the 'status detail' CLI command. Look for

the Resource Conservation line in the Gages section.

Here is an example:

Resource Conservation 0

Any non−zero number means the system is trying to protect itself by slowing SMTP responses. You can learn more about Resource Conservation here:

What is resource conservation mode?

Firewalls

The last common cause of SMTP banner delays are firewalls that are SMTP aware. These feature such as performing 'SMTP fixup' or running security scans on all SMTP content. Sometimes a firewall may delay the banner while it scans and possibly modifies the content of the SMTP banner. Here is an example of a popular firewall altering the SMTP banner:

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

Updated: Jul 18, 2014 Document ID: 118016