502/504个GATEWAY_TIMEOUT错误，当浏览对某些站点时

目录

问题：

当浏览对某些站点时，为什么看到502/504个GATEWAY_TIMEOUT错误？

症状：当浏览到某些网站时，用户接收从思科WSA的502个或504个网关超时错误

当浏览到网站时，用户接收502个或504个网关超时错误。访问日志将显示'NONE/504或'NONE/502

示例访问记录行：

1233658928.496 153185个10.10.70.50 **NONE/504** 1729 GET http://www.example.com/ -直接 www.example.com - .....

有许多原因为什么WSA可能返回一个502个或504个网关超时错误。虽然这些错误反应是类似的，了解他们之间的细微的区别是重要的。

这是方案的种类的一些示例可能发生：

- **502** ：WSA尝试建立TCP连接用Web服务器，但是未接收SYN/ACK。
- **504** ：WSA接收终止连接用Web服务器的TCP重置(RST)。
- **504** ：WSA从要求的服务不得到答复在通信用Web服务器之前，例如DNS失败。
- **504** ：WSA建立了TCP连接用Web服务器并且发送GET请求，但是WSA从未接收HTTP响应。

下面每个方案和更多详细信息示例关于潜在问题：

502 ：WSA尝试建立TCP连接用Web服务器，但是未接收SYN/ACK。
如果Web服务器不响应到WSA的SYN数据包，在一定数量的尝试以后，客户端将发送一个502个网关超时错误。 此的典型的原因是： **1.**Web服务器或Web服务器网络有问题。 **2.**在WSA网络的一个网络问题防止SYN数据包到互联网。 **3.**防火墙或类似设备下降WSA SYN数据包或Web服务器的SYN/ACK **4.** IP伪装在WSA启用，但是没有适当地配置(没有返回路径重定向) **故障排除步骤：**

如果WSA能ICMP Ping Web服务器，第一步将验证。通过使用以下CLI命令，这可以执行：
WSA> *ping www.example.com*
如果ping发生故障，不意味着服务器发生故障。可能含义ICMP数据包在路径阻拦某处。如果ping成功，则我们能肯定知道WSA有一个基本layer3级别连接到Web服务器。
如果WSA有能力建立在端口80的TCP连接对Web服务器， telnet测验将验证。请参阅说明进一步在此条款为执行telnet测验。

网络问题或防火墙块
如果ping是成功，但是telnet出故障，有一种好可能性一个过滤设备，例如防火墙，防止此流量获得通过网络。推荐防火墙日志和数据包捕获从防火墙对于更详细的资料分析。
IP伪装enable (event)，但是不适当地配置
如果明确地代理通过WSA或telnet测验是成功的，这显示WSA能通信直接地到Web服务器，但是，当客户端代理通过与IP伪装的WSA，有问题。

没有客户端IP伪装：
- WSA发送SYN到Web服务器使用其自己的IP地址作为来源。当数据包回来时，去直接地WSA。

使用客户端IP伪装：
- WSA发送SYN，反而，使用客户端IP作为来源。没有一特殊网络设置，返回信息包将发送给客户端而不是WSA。
- 为了使用伪装的客户端IP，用一个非常详细的方式必须配置网络为了实现数据包适当地重定向。如果Web服务器返回路径信息包被发送给客户端而不是WSA， WSA不会看到服务器SYN/ACK并且发送一个502个网关超时错误回到客户端。

504 ：WSA接收终止连接用Web服务器的TCP重置(RST)。

如果WSA收到在其上行连接的一TCP重置数据包对Web服务器， WSA将发送一个504个网关超时错误给客户端。

此的典型的原因是：
1.思科Layer4流量监控(L4TM)阻塞从连接Web服务器的WSA代理。
2.防火墙、IDS、IPS，或者其他包侦测设备阻塞WSA。

故障排除步骤：
首先请确定TCP RST是否来自自L4TM或另一个设备。
如果L4TM阻塞此流量，流量在GUI报告将出现在“***箴言报下- > L4流量监控***”。否则， RST来自一个不同的设备。
阻塞的L4TM ：
推荐，如果L4TM是阻塞，请勿阻塞在端口WSA代理也运作。有此的多个原因：
1.WSA代理提供一友好错误消息一旦问题，而不是重置连接的TCP。当他们阻塞，这将帮助限制从最终用户的混乱。
2.WSA代理有能力扫描和阻塞特定内容，而L4TM阻塞匹配一个列入黑名单的IP地址的所有流量。
为了配置L4TM不阻塞在代理端口，请去“***GUI - > Security服务- > L4流量监控***”。
如果站点是已知坏网站，但是有原因为什么应该允许流量，站点可以是白色列出的在：
“***GUI - > Web安全经理- > L4流量监控- >请允许列表***”

阻塞的防火墙/IDS/IPS ：
如果在网络的另一个设备阻塞从连接的WSA到Web服务器，推荐分析以下：
1.防火墙块日志

2.在问题期间的入口/出口数据包捕获

块日志可能迅速确认设备是否阻塞WSA。有时防火墙、IPS或者IDS将阻塞流量和不会记录它适当地。如果这是实际情形，证明的唯一方法TCP RST来自的地方，是获取入口和出口捕获从设备。如果RST被派出入口接口，并且数据包没有游遍输出侧，安全设备确实是原因。

504 ：WSA建立了TCP连接用Web服务器并且发送GET请求，但是WSA从未接收HTTP响应。

如果WSA发送HTTP GET，但是从未收到答复，将发送一个504个网关超时错误给客户端。

此的典型的原因是：

- 防火墙， IDS， IPS，或者其他包侦测设备允许TCP连接，但是阻塞从到达Web服务器的HTTP内容。在这种情况下，种类HTTP数据阻塞的telnet测验可能帮助隔离。

防火墙块日志是否可能迅速确认/设备为什么阻塞WSA。有时防火墙、IPS或者IDS将阻塞流量和不会记录它适当地。如果这是实际情形，证明的唯一方法TCP RST来自的地方，是获取入口和出口捕获从设备。如果RST被派出入口接口，并且数据包没有游遍输出侧，安全设备确实是原因。

测试连接用一Web服务器使用telnet

从WSA CLI，请运行**Telnet命令**：

WSA> **telnet**
请选择请建立接口您要远程登录。
1. 自动
2. 管理(192.168.15.200/24 ：wsa.hostname.com)
3. P1 (192.168.113.199/24 ：data.com)
3 [1]>

输入远程主机名或IP地址。
[]> www.example.com

输入远程端口。
80 [25]>

尝试10.3.2.99…
连接对www.example.com。
转义字符是'^]'。

Note:"用红色连接"消息，表明TCP成功设立在WSA和Web服务器之间。

HTTP请求可能通过此远程登录会话手工发送。下列是可以在"已连接"消息以后被键入的示例请求：

GET http://www.example.com HTTP/1.1
主机：www.example.com
{回车}

Note:确保添加额外的回车在末端，否则服务器不会回答请求。