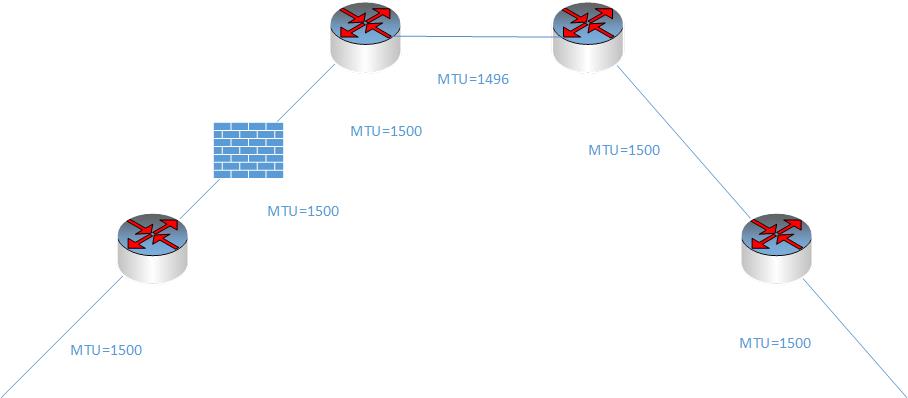
# 1、问题

在实际环境中，往往出现在某个链路上MTU不规范，比正常的MTU(1500)要小。从理论上讲，出现这种情况后，应由路由器发送ICMP告知发送端调整MTU。但是由于网络比较复杂，该告知无法到达发送者。

如下图所示，中间路由器的通路的MTU为1496。这导致网络两侧设备通讯时，小包可以通过，但是大包无法通过。现象就是可以ping通，但是无法下载数据或者打开页面。



# 解决方案

防火墙可以调整TCP通讯的MSS值，使得链路两端的设备通讯时不发送MTU为1500的数据包，从而避免丢包事件。

MTU: Maxitum Transmission Unit 最大传输单元  
MSS: Maxitum Segment Size 最大分段大小

由于以太网EthernetII最大的数据帧是1518Bytes这样，刨去以太网帧的帧头（DMAC目的地址MAC48bit=6Bytes+SMAC源MAC地址48bit=6Bytes+Type域2bytes）14Bytes和帧尾CRC校验部分4Bytes（这个部门有时候大家也把它叫做FCS），那么剩下承载上层协议的地方也就是Data域最大就只能有1500Bytes. 这个值我们就把它称之为MTU。

MSS就是TCP数据包每次能够传输的最大数据分段。为了达到最佳的传输效能

TCP协议在建立连接的时候通常要协商双方的MSS值，这个值TCP协议在实现的

时候往往用MTU值代替（需要减去IP数据包包头的大小20Bytes和TCP数据段的包头20Bytes）所以往往MSS为1460。通讯双方会根据双方提供的MSS值得最小值确定为这次连接的最大MSS值。

也就是说，在上图的案例中MTU值为1496，那么我们可以通过调整MSS为1496-40=1456， 来达到调整发包大小满足MTU的要求。

具体设置方法如下：

define firewall policy

edit xxx

set tcp-mss-sender 1456

set tcp-mss-receiver 1456

end

当然如果不清楚中间链路的具体MTU，可以再往小处调整。该方法的缺点是需要调整所有的策略。