防火墙外网口如何改MTU和TCP MSS值

虚拟分片重组 **余振华** 2021-04-16 发表

问题描述

防火墙外网口如何改MTU和TCP MSS值?

解决方法

MTU是数据链路层的概念，表示接口的最大传输单元，一般情况下指的是接口所能传输IP报文的最大长度。
默认以太网接口MTU为1500，那么传输长度为1490大小的IP报文完全没有问题；
但是VPN隧道携带了一层层封装，比如IPsec报文：
这样就会导致封装过后的新IP报文长度可能会大于接口的MTU值， IPsec为了确保传输报文不大于物理接口的MTU值，所以规定了隧道自己的MTU值，即Path MTU，即要求被封装的报文长度不能大于这个值，否则将被分片处理。Path MTU在ipsec sa中可以看到，这个值不是固定的，因为每个隧道使用的模式和算法不同。
但很多业务类型是基于TCP的，TCP的IP报文header通常明确指定了本报文不能给分片（Don't fragment）。
这样的话，就必须使得载荷为TCP业务的IP报文长度必须小于Path MTU，否则将被IPsec隧道丢弃，MTU check failure会一直增长。
IP报文不可以被分片，但是TCP 报文可以。TCP三次握手的时候，头部会有协商MSS（Maximum segment size）的选项，在一长串网络设备中，以设置最小的MSS来传输TCP报文。
所以我们需要将TCP MSS调小以保证TCP报文长度变小，这样IP报文长度也会变小，经过IPsec隧道时就不会被隧道MTU限制。
TCP MSS设置为多少合适呢，由于TCP业务报文的IP头和TCP头长度都是20字节，那么IP场景下；TCP MSS = Path MTU – IP Header – TCP Header = Path MTU – 40.
比如Path = 1428，那么在内外网口下设置TCP MSS为1388就可以，小一点也没关系，但是不能太小，否则TCP报文重组也会消耗一定性能。
综上，不能调整接口MTU！要调整只能调整TCP MSS。