业务报文长度超过sslvpn ac口MTU导致被丢包，sslvpn拨号后网页打不开

SSL VPN　李瑞　2024-01-09 发表

组网及说明

inode----SSLVPN gateway ----server

告警信息

不涉及

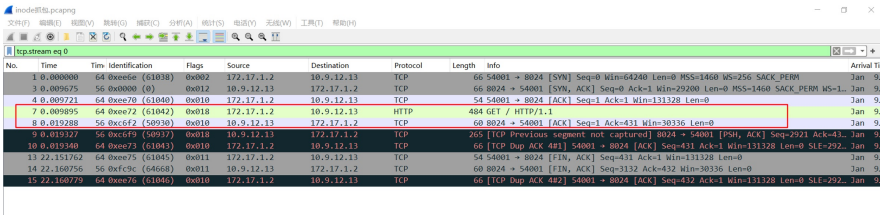
问题描述

现网配置sslvpn的ip接入，内网服务器可以ping通，但是打开http网页失败，浏览器网页没有报错，就是一直在加载的状态，最后失败

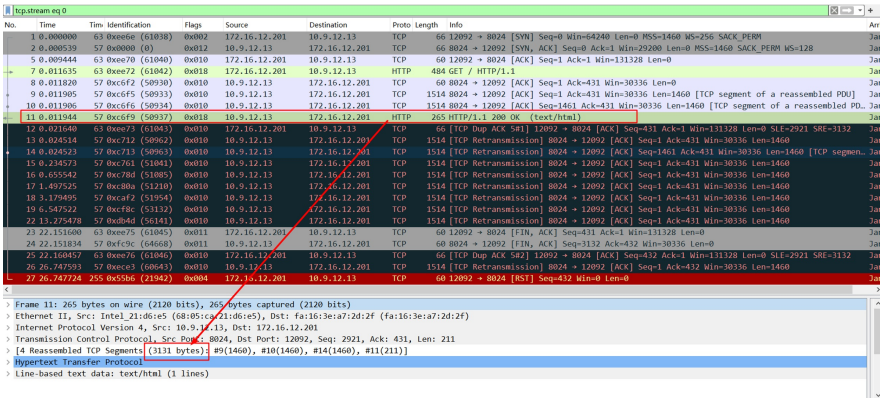
过程分析

inode网卡、防火墙抓包对比，发现大包被防火墙丢了

inode抓包



FW抓包：



SSLVPN-AC1接口的mtu固定且无法改变，随着版本的升级，AC口的MTU会改变：

[sslvpn]dis interface SSLVPN-AC 1
SSLVPN-AC1
Current state: UP
Line protocol state: UP
Description: SSLVPN-AC1 Interface
Bandwidth: 10000000 kbps
Maximum transmission unit: 1359
Internet address: 172.17.1.1/24 (Primary)
Link layer protocol is SSLVPN
Last clearing of counters: Never
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 78277 packets, 9093624 bytes, 0 drops
Output: 75539 packets, 51043445 bytes, 0 drops

当现网报文的长度超过AC口的大小时，会被AC口丢弃导致报文被丢

解决方法

观察到现场被丢的报文是HTTP协议，可以改小内网口（注意不是AC口的TCP MSS）的TCP MSS小于AC口的MTU防止被AC口卡MTU