

# 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

No.	Time	Time Identification	Flags	Source	Destination	Protocol	Length	Info	Actual Ti
1	0.000000	64 0ee0e6 (61038)	0x002	172.17.1.2	10.9.12.13	TCP	66	54801 → 8024 [SYN] Seq=0 Min=64240 Len=0 MSS=1460 WS=256 SACK_PERM	Jan 9
3	0.009575	56 0x0000 (0)	0x012	10.9.12.13	172.17.1.2	TCP	66	8024 → 54801 [SYN, ACK] Seq=0 Ack=1 Min=29280 Len=0 MSS=1460 SACK_PERM WS=1	Jan 9
4	0.009721	64 0ee0e6 (61040)	0x010	172.17.1.2	10.9.12.13	TCP	54	54801 → 8024 [ACK] Seq=1 Ack=1 Min=131328 Len=0	Jan 9
7	0.009895	64 0ee0e7 (61042)	0x018	172.17.1.2	10.9.12.13	HTTP	484	GET / HTTP/1.1	Jan 9
8	0.012988	56 0xc6f2 (58930)	0x010	10.9.12.13	172.17.1.2	TCP	60	8024 → 54801 [ACK] Seq=1 Ack=431 Min=30336 Len=0	Jan 9
9	0.019127	56 0xc6f9 (58937)	0x018	10.9.12.13	172.17.1.2	TCP	265	[TCP Previous segment not captured] 8024 → 54801 [PSH, ACK] Seq=2921 Ack=431	Jan 9
10	0.019340	64 0ee0e7 (61043)	0x010	172.17.1.2	10.9.12.13	TCP	66	[TCP Dup ACK 481] 54801 → 8024 [ACK] Seq=431 Ack=1 Min=131328 Len=0 SLE=2921	Jan 9
13	22.151762	64 0ee0e7 (61045)	0x011	172.17.1.2	10.9.12.13	TCP	54	54801 → 8024 [FIN, ACK] Seq=431 Ack=1 Min=131328 Len=0	Jan 9
14	22.168750	56 0xf6c3 (64608)	0x011	10.9.12.13	172.17.1.2	TCP	60	8024 → 54801 [FIN, ACK] Seq=3132 Ack=432 Min=30336 Len=0	Jan 9
17	22.169777	64 0ee0e6 (61046)	0x010	172.17.1.2	10.9.12.13	TCP	66	[TCP Dup ACK 422] 54801 → 8024 [ACK] Seq=432 Ack=1 Min=131328 Len=0 SLE=2921	Jan 9

## FW抓包:

No.	Time	Time Identification	Flags	Source	Destination	Proto	Length	Info	Actual Ti
1	0.000000	63 0ee0e6 (61038)	0x002	172.16.12.201	10.9.12.13	TCP	66	12092 → 8024 [SYN] Seq=0 Min=64240 Len=0 MSS=1460 WS=256 SACK_PERM	Jan 9
2	0.000539	57 0x0000 (0)	0x012	10.9.12.13	172.16.12.201	TCP	66	8024 → 12092 [SYN, ACK] Seq=0 Ack=1 Min=29280 Len=0 MSS=1460 SACK_PERM WS=128	Jan 9
5	0.009444	63 0ee0e7 (61040)	0x010	172.16.12.201	10.9.12.13	TCP	60	12092 → 8024 [ACK] Seq=1 Ack=1 Min=131328 Len=0	Jan 9
7	0.011035	63 0ee0e7 (61042)	0x018	172.16.12.201	10.9.12.13	HTTP	484	GET / HTTP/1.1	Jan 9
8	0.011828	57 0xc6f2 (58930)	0x010	10.9.12.13	172.16.12.201	TCP	60	8024 → 12092 [ACK] Seq=1 Ack=431 Min=30336 Len=0	Jan 9
9	0.011905	57 0xc6f5 (58933)	0x010	10.9.12.13	172.16.12.201	TCP	1514	8024 → 12092 [ACK] Seq=1 Ack=431 Min=30336 Len=1460 [TCP segment of a reassembled PDU]	Jan 9
10	0.011906	57 0xc6f5 (58934)	0x010	10.9.12.13	172.16.12.201	TCP	1514	8024 → 12092 [ACK] Seq=1461 Ack=431 Min=30336 Len=1460 [TCP segment of a reassembled PDU]	Jan 9
11	0.011944	57 0xc6f9 (58937)	0x018	10.9.12.13	172.16.12.201	HTTP	265	HTTP/1.1 200 OK (text/html)	Jan 9
12	0.021040	63 0ee0e7 (61043)	0x010	172.16.12.201	10.9.12.13	TCP	66	[TCP Dup ACK 581] 12092 → 8024 [ACK] Seq=431 Ack=1 Min=131328 Len=0 SLE=2921 SRE=3132	Jan 9
13	0.024514	57 0xc712 (58962)	0x010	10.9.12.13	172.16.12.201	TCP	1514	[TCP Retransmission] 8024 → 12092 [ACK] Seq=1 Ack=431 Min=30336 Len=1460	Jan 9
14	0.024522	57 0xc713 (58963)	0x010	10.9.12.13	172.16.12.201	TCP	1514	[TCP Retransmission] 8024 → 12092 [ACK] Seq=1461 Ack=431 Min=30336 Len=1460 [TCP segment of a reassembled PDU]	Jan 9
15	0.234573	57 0xc701 (51041)	0x010	10.9.12.13	172.16.12.201	TCP	1514	[TCP Retransmission] 8024 → 12092 [ACK] Seq=1 Ack=431 Min=30336 Len=1460	Jan 9
16	0.255542	57 0xc70d (51085)	0x010	10.9.12.13	172.16.12.201	TCP	1514	[TCP Retransmission] 8024 → 12092 [ACK] Seq=1 Ack=431 Min=30336 Len=1460	Jan 9
17	1.497526	57 0xc80a (51210)	0x010	10.9.12.13	172.16.12.201	TCP	1514	[TCP Retransmission] 8024 → 12092 [ACK] Seq=1 Ack=431 Min=30336 Len=1460	Jan 9
18	3.170495	57 0xc8f2 (51564)	0x010	10.9.12.13	172.16.12.201	TCP	1514	[TCP Retransmission] 8024 → 12092 [ACK] Seq=1 Ack=431 Min=30336 Len=1460	Jan 9
19	6.547222	57 0xc8f6 (51312)	0x010	10.9.12.13	172.16.12.201	TCP	1514	[TCP Retransmission] 8024 → 12092 [ACK] Seq=1 Ack=431 Min=30336 Len=1460	Jan 9
22	13.273478	57 0xc8fd (56141)	0x010	10.9.12.13	172.16.12.201	TCP	1514	[TCP Retransmission] 8024 → 12092 [ACK] Seq=1 Ack=431 Min=30336 Len=1460	Jan 9
23	22.151600	63 0ee0e7 (61045)	0x011	172.16.12.201	10.9.12.13	TCP	60	12092 → 8024 [FIN, ACK] Seq=431 Ack=1 Min=131328 Len=0	Jan 9
24	22.151834	57 0xf6c3 (64608)	0x011	10.9.12.13	172.16.12.201	TCP	60	8024 → 12092 [FIN, ACK] Seq=3132 Ack=432 Min=30336 Len=0	Jan 9
25	22.160457	63 0ee0e6 (61046)	0x010	172.16.12.201	10.9.12.13	TCP	66	[TCP Dup ACK 582] 12092 → 8024 [ACK] Seq=432 Ack=1 Min=131328 Len=0 SLE=2921 SRE=3132	Jan 9
26	26.747593	57 0xc8c3 (60643)	0x010	10.9.12.13	172.16.12.201	TCP	1514	[TCP Retransmission] 8024 → 12092 [ACK] Seq=1 Ack=432 Min=30336 Len=1460	Jan 9
27	26.747728	256 0x0500 (21602)	0x004	172.16.12.201	10.9.12.13	TCP	60	12092 → 8024 [RST] Seq=432 Min=0 Len=0	Jan 9

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