SANGFOR

IAM

Open Authentication Troubleshooting Guide

Version 12.0.18

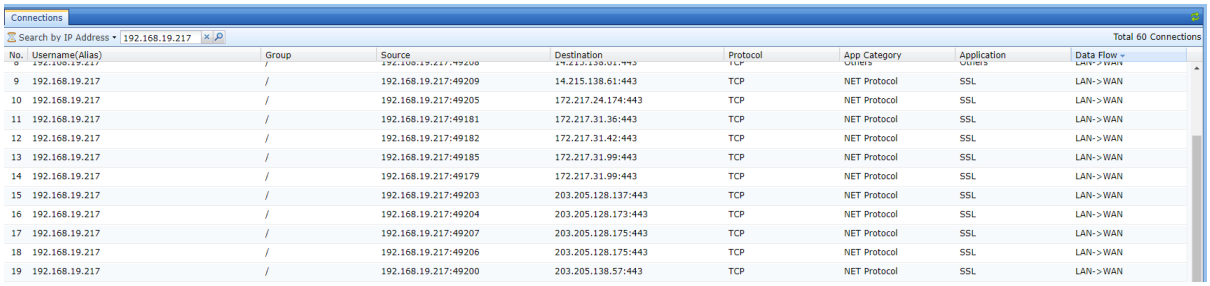
Change Log

Date	Change Description
May 30, 2019	Version 12.0.18 document release.

CONTENT

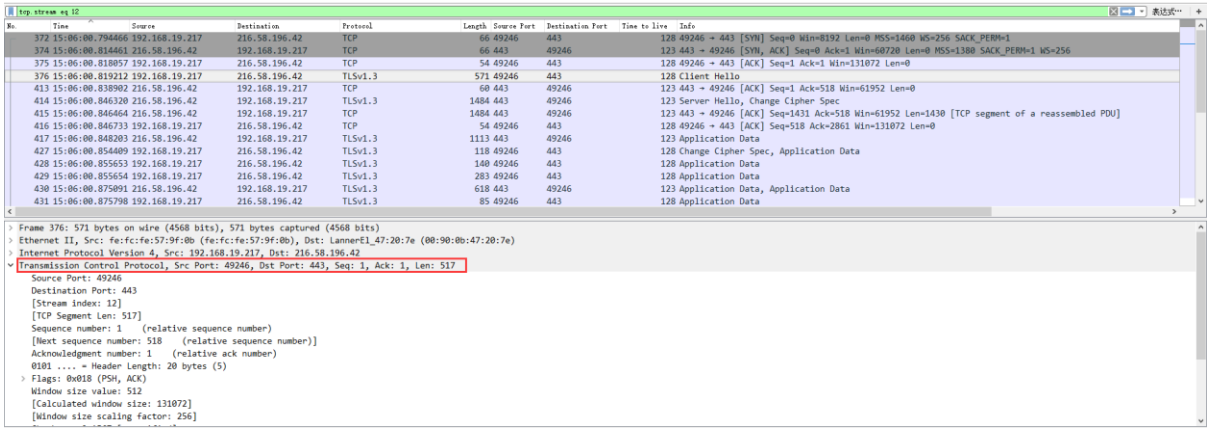
Chapter 1 Use Open Authentication but no users in Online Users

- Check if there is a test ip connection on the IAM and if the traffic is bidirectional.



No.	Username(Alias)	Group	Source	Destination	Protocol	App Category	Application	Data Flow
9	192.168.19.217	/	192.168.19.217:49209	14.215.138.61:443	TCP	NET Protocol	SSL	LAN->WAN
10	192.168.19.217	/	192.168.19.217:49205	172.217.24.174:443	TCP	NET Protocol	SSL	LAN->WAN
11	192.168.19.217	/	192.168.19.217:49181	172.217.31.36:443	TCP	NET Protocol	SSL	LAN->WAN
12	192.168.19.217	/	192.168.19.217:49182	172.217.31.42:443	TCP	NET Protocol	SSL	LAN->WAN
13	192.168.19.217	/	192.168.19.217:49185	172.217.31.99:443	TCP	NET Protocol	SSL	LAN->WAN
14	192.168.19.217	/	192.168.19.217:49179	172.217.31.99:443	TCP	NET Protocol	SSL	LAN->WAN
15	192.168.19.217	/	192.168.19.217:49203	203.205.128.137:443	TCP	NET Protocol	SSL	LAN->WAN
16	192.168.19.217	/	192.168.19.217:49204	203.205.128.173:443	TCP	NET Protocol	SSL	LAN->WAN
17	192.168.19.217	/	192.168.19.217:49207	203.205.128.175:443	TCP	NET Protocol	SSL	LAN->WAN
18	192.168.19.217	/	192.168.19.217:49206	203.205.128.175:443	TCP	NET Protocol	SSL	LAN->WAN
19	192.168.19.217	/	192.168.19.217:49200	203.205.138.57:443	TCP	NET Protocol	SSL	LAN->WAN

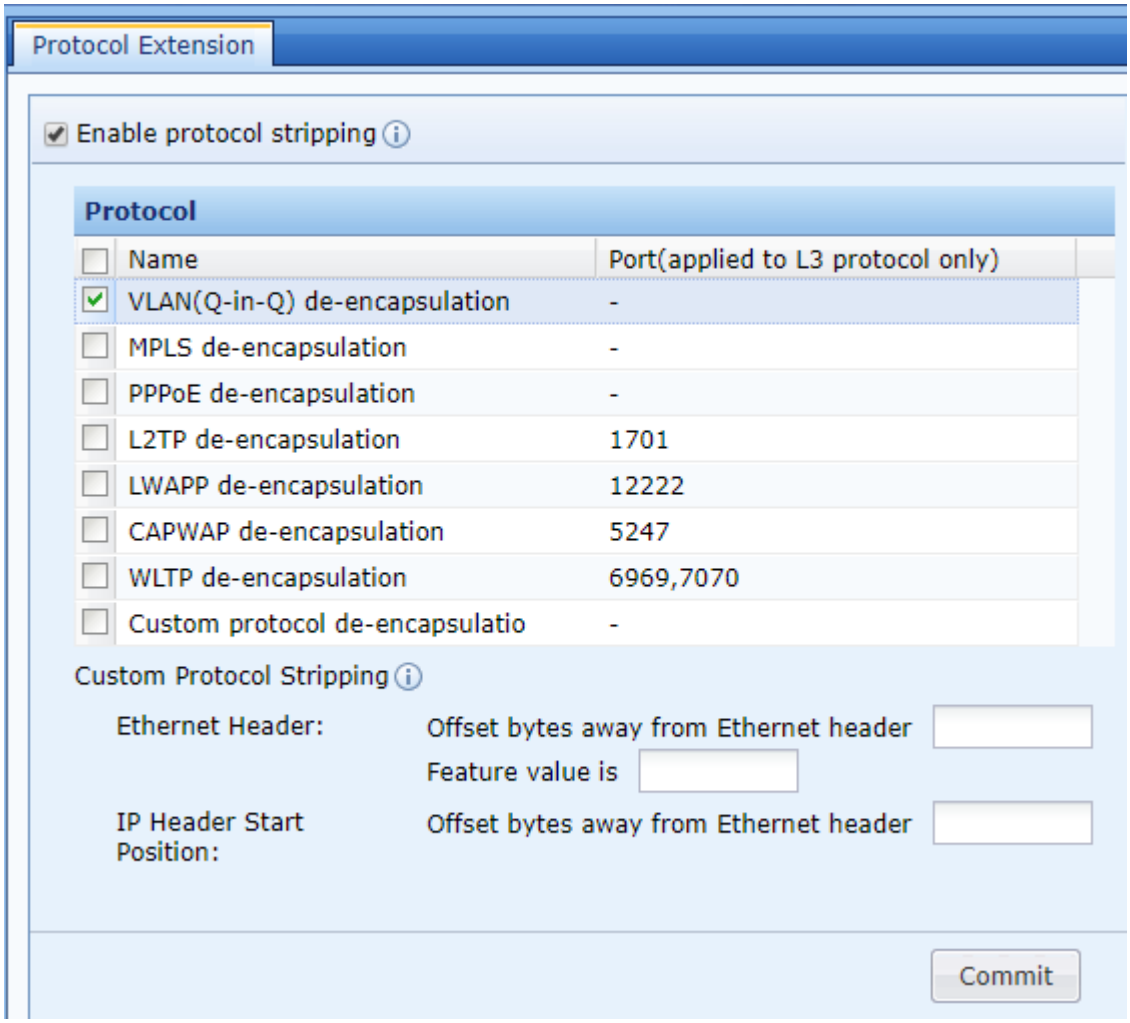
- Check whether the data packet has a TCP protocol packet, and there is no TCP protocol packet. Then, if Open Authentication is configured, the IP of the PC will not appear in **Online Users**.



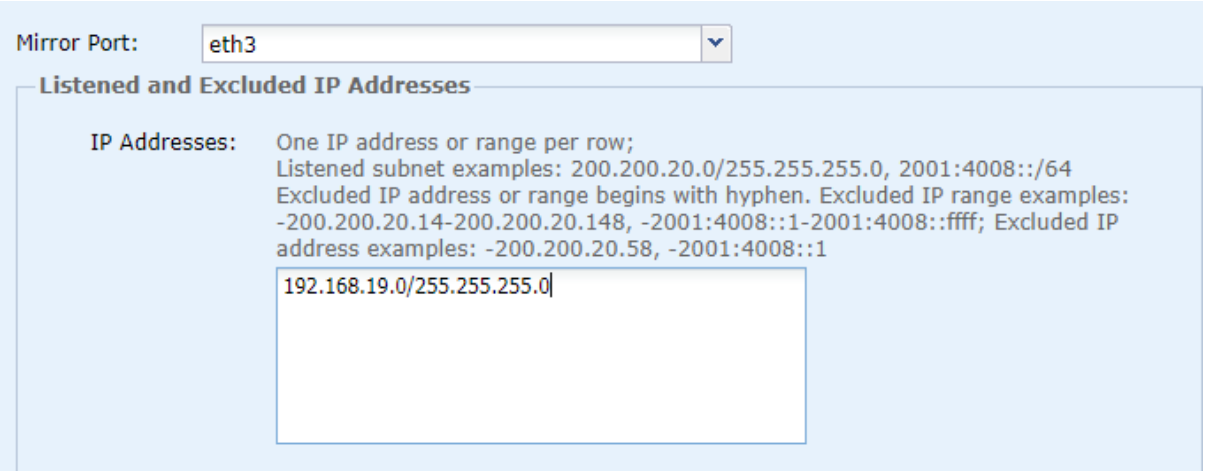
No.	Time	Source	Destination	Protocol	Length	Source Port	Destination Port	Time to live	Info
372	15:06:00.794466	192.168.19.217	216.58.196.42	TCP	66	49246	443	128	49246 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
374	15:06:00.814461	216.58.196.42	192.168.19.217	TCP	66	443	49246	123	443 → 49246 [SYN, ACK] Seq=0 Ack=1 Win=60720 Len=0 MSS=1380 SACK_PERM=1 WS=256
375	15:06:00.818057	192.168.19.217	216.58.196.42	TCP	54	49246	443	128	49246 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
376	15:06:00.819212	192.168.19.217	216.58.196.42	TLSv1.3	571	49246	443	128	Client Hello
413	15:06:00.838902	216.58.196.42	192.168.19.217	TCP	60	443	49246	123	443 → 49246 [ACK] Seq=1 Ack=518 Win=61952 Len=0
414	15:06:00.846320	216.58.196.42	192.168.19.217	TLSv1.3	1484	443	49246	123	Server Hello, Change Cipher Spec
415	15:06:00.846464	216.58.196.42	192.168.19.217	TCP	1484	443	49246	123	443 → 49246 [ACK] Seq=1431 Ack=518 Win=61952 Len=1430 [TCP segment of a reassembled PDU]
416	15:06:00.846733	192.168.19.217	216.58.196.42	TCP	54	49246	443	128	49246 → 443 [ACK] Seq=518 Ack=2861 Win=131072 Len=0
417	15:06:00.848203	216.58.196.42	192.168.19.217	TLSv1.3	1113	443	49246	123	Application Data
427	15:06:00.854409	192.168.19.217	216.58.196.42	TLSv1.3	118	49246	443	128	Change Cipher Spec, Application Data
428	15:06:00.855653	192.168.19.217	216.58.196.42	TLSv1.3	140	49246	443	128	Application Data
429	15:06:00.855654	192.168.19.217	216.58.196.42	TLSv1.3	283	49246	443	128	Application Data
430	15:06:00.875091	216.58.196.42	192.168.19.217	TLSv1.3	618	443	49246	123	Application Data, Application Data
431	15:06:00.875798	192.168.19.217	216.58.196.42	TLSv1.3	85	49246	443	128	Application Data

```
> Frame 376: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits)
> Ethernet II, Src: fe:fc:fe:57:9f:0b (fe:fc:fe:57:9f:0b), Dst: LannerEl_47:20:7e (00:90:0b:47:20:7e)
> Internet Protocol Version 4, Src: 192.168.19.217, Dst: 216.58.196.42
v Transmission Control Protocol, Src Port: 49246, Dst Port: 443, Seq: 1, Ack: 1, Len: 517
    Source Port: 49246
    Destination Port: 443
    [Stream index: 12]
    [TCP Segment Len: 517]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 518    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window size value: 512
    [Calculated window size: 131072]
    [Window size scaling factor: 256]
```

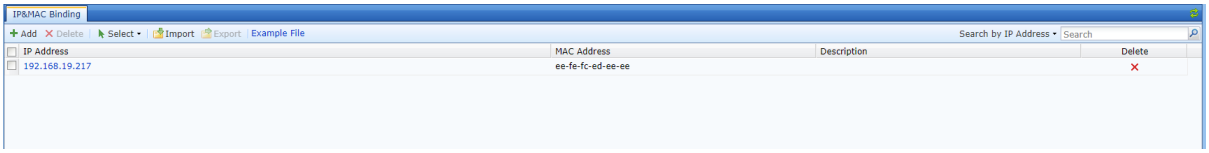
- Check whether there is a multi-layer protocol encapsulation, such as QinQ protocol encapsulation. If there is a protocol such as QinQ, you need to enable "**Protocol Extension**".

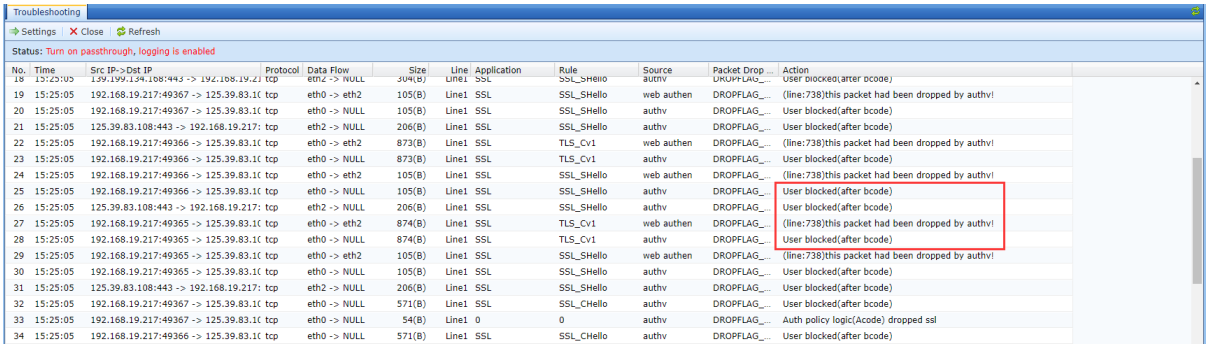


- If it is bypass mode, you need to check whether the IP address segment in Listened and Excluded IP Addresses is complete.

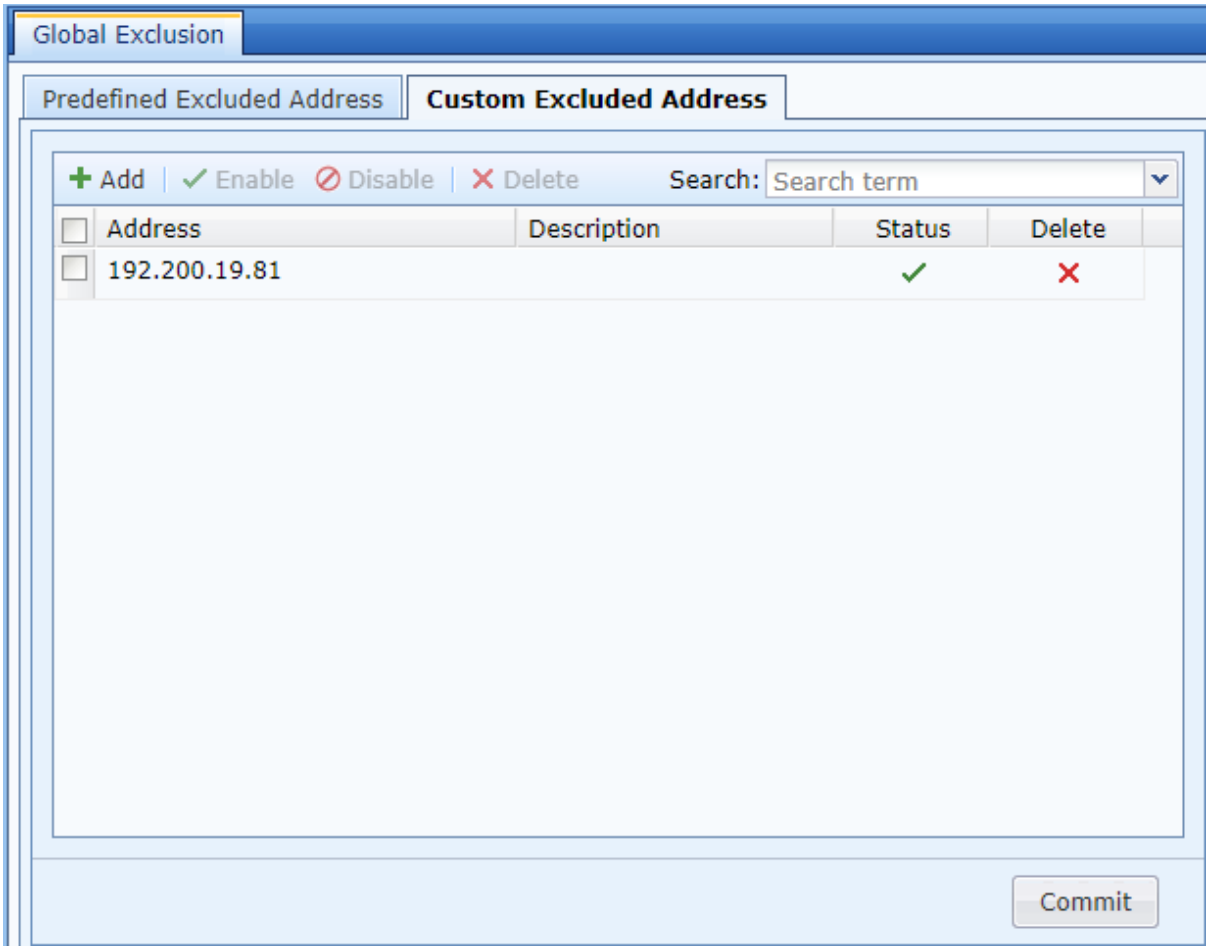


- Check if you have made the wrong IP/MAC binding, or turn on **Troubleshooting** to check for a drop log.

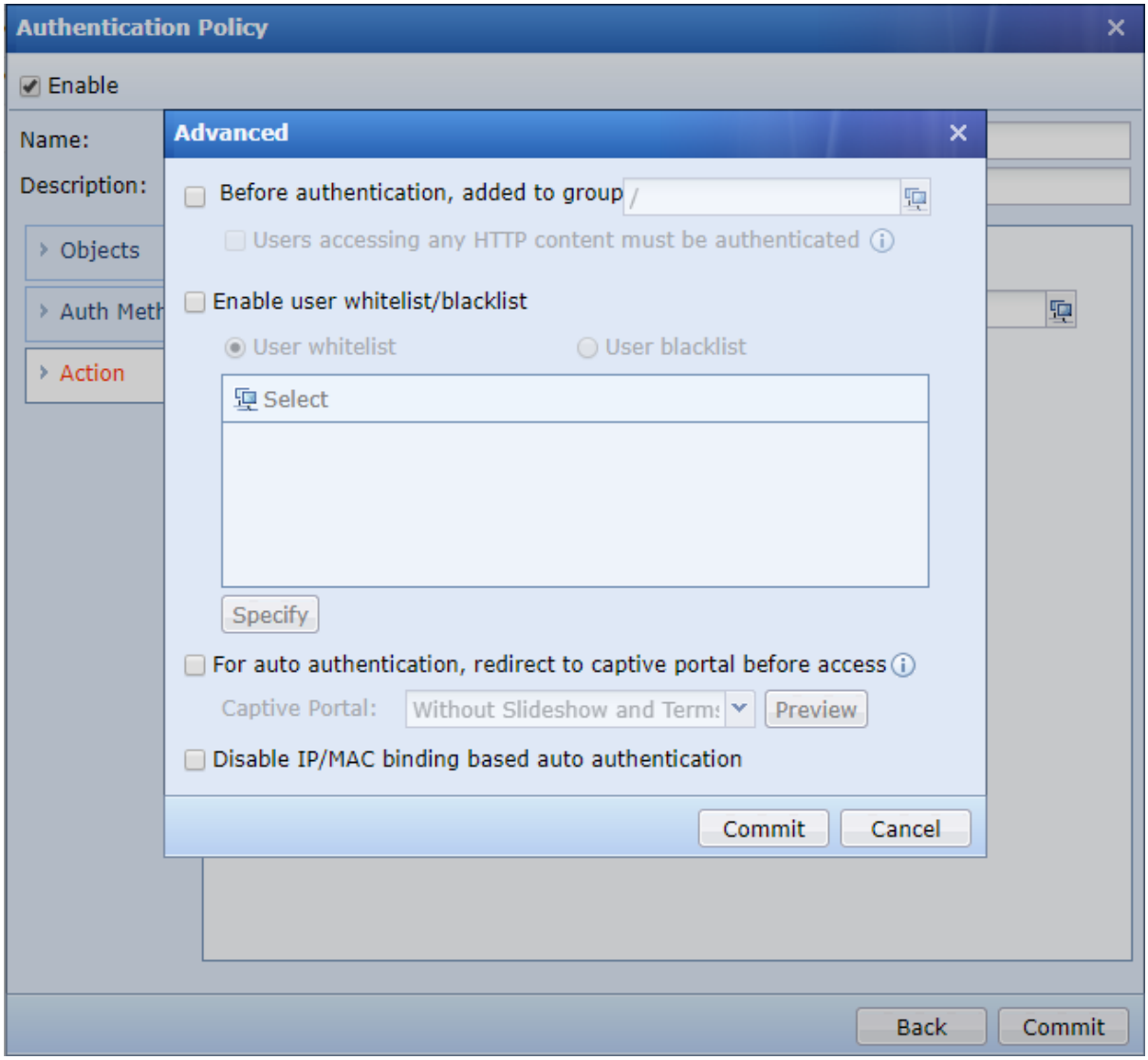




- Check if IP or network segment is added to **Global Exclusion**.



- Check whether a blacklist or whitelist is configured.



- Devices deployed in bridge mode need to check whether the network cable is reversed. If the network cable is connected and the "**Open auth for data flow from WAN to LAN interface**" is enabled, the IP of the intranet may not be online.