IAM

Failing to audit online behavior under bypass mode Troubleshooting Guide

Version 12.0.18

Change Log

Date	Change Description
April 2, 2019	Version 12.0.18 document release.

CONTENT

Chapter 1 Basic Check 1
1 Definition 1
2 Configuration check 1
3 Check line connection 1
Chapter 2 Advanced troubleshooting 1
1 Check if data is mirrored to IAM in both directions 1
2 Check if there is a multi-layer protocol 2

Chapter 1 Basic Check

1 Definition

- Confirm that the device's Listened and Excluded IP Addresses and Listened Servers are configured correctly.
- In bypass mode, any address will match one of the three regions of Listened and Excluded IP Addresses (LI), Listened Servers (LIS), and Listened and Excluded IP Addresses and Listed Servers (Others).

The communication between (LI) and (LIS) is LAN->WAN

The communication between (LI) and (Others) is LAN->WAN

Communication between (LIS) and (Others) is LAN->WAN

Among them (LI) and (LIS) may overlap. If the source IP is both (LI), no match (LIS) is LAN->LAN.

If the source IP is (LIS), there is no match (LI) that is also LAN->LAN.

The device only recognizes and audits the LAN->WAN data. So Listened and Excluded IP Addresses cannot be configured for all network segments.

2 Configuration check

- 11.0 and newer versions require a mirror port to be specified in the Network Configuration Wizard.
- Whether to add a network segment or IP to Global Exclusion.
- Confirm that Databasee is updated to the latest, whether Custom Application or URL Database is configured.

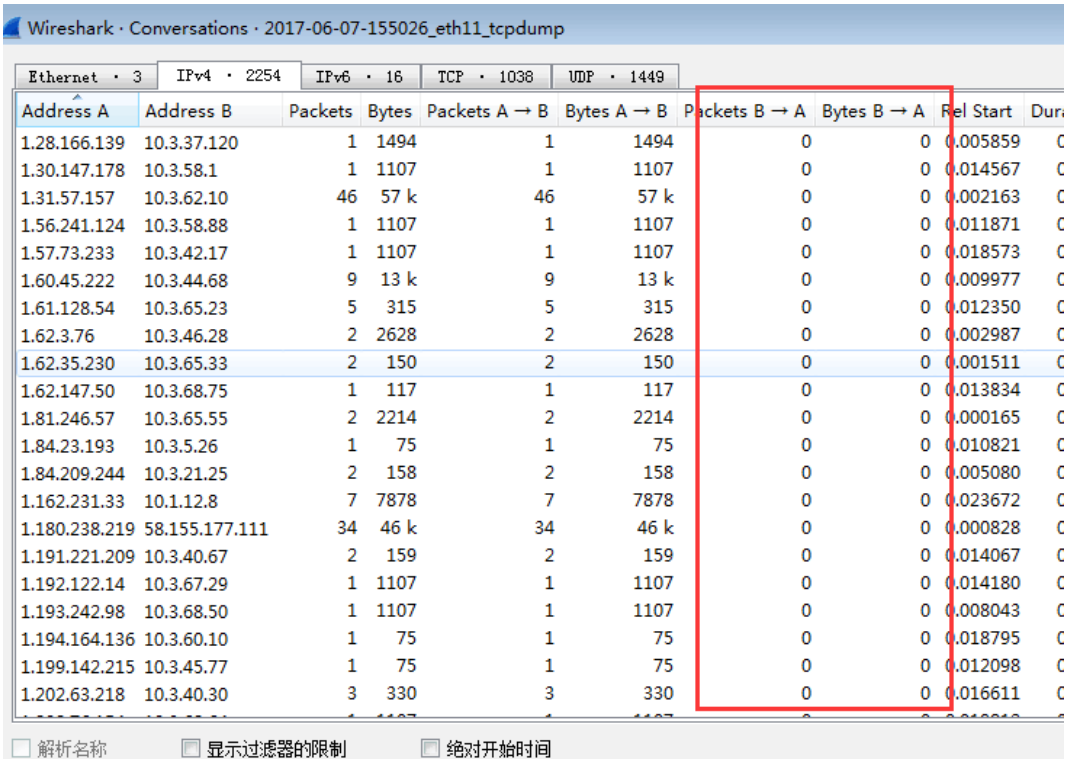
3 Check line connection

Confirm that the wiring is correct, and whether the switch mirrors the traffic to the IAM.

Chapter 2 Advanced troubleshooting

1 Check if data is mirrored to IAM in both directions

- Analyze whether the source IP address of the data packet conforms to the LAN->WAN direction. If the packet is configured to match the LAN->LAN or WAN->WAN direction, the device will not process the data.
- Grab a certain amount of data packets in the mirror port, save it as a file and download it using wireshark. If the data is unidirectionally mirrored to IAM, use the **[Statistics]-[Conversation]** function to see the result of the following figure.



Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Dur
1.28.166.139	10.3.37.120	1	1494	1	1494	0	0	0.005859	0
1.30.147.178	10.3.58.1	1	1107	1	1107	0	0	0.014567	0
1.31.57.157	10.3.62.10	46	57 k	46	57 k	0	0	0.002163	0
1.56.241.124	10.3.58.88	1	1107	1	1107	0	0	0.011871	0
1.57.73.233	10.3.42.17	1	1107	1	1107	0	0	0.018573	0
1.60.45.222	10.3.44.68	9	13 k	9	13 k	0	0	0.009977	0
1.61.128.54	10.3.65.23	5	315	5	315	0	0	0.012350	0
1.62.3.76	10.3.46.28	2	2628	2	2628	0	0	0.002987	0
1.62.35.230	10.3.65.33	2	150	2	150	0	0	0.001511	0
1.62.147.50	10.3.68.75	1	117	1	117	0	0	0.013834	0
1.81.246.57	10.3.65.55	2	2214	2	2214	0	0	0.000165	0
1.84.23.193	10.3.5.26	1	75	1	75	0	0	0.010821	0
1.84.209.244	10.3.21.25	2	158	2	158	0	0	0.005080	0
1.162.231.33	10.1.12.8	7	7878	7	7878	0	0	0.023672	0
1.180.238.219	58.155.177.111	34	46 k	34	46 k	0	0	0.000828	0
1.191.221.209	10.3.40.67	2	159	2	159	0	0	0.014067	0
1.192.122.14	10.3.67.29	1	1107	1	1107	0	0	0.014180	0
1.193.242.98	10.3.68.50	1	1107	1	1107	0	0	0.008043	0
1.194.164.136	10.3.60.10	1	75	1	75	0	0	0.018795	0
1.199.142.215	10.3.45.77	1	75	1	75	0	0	0.012098	0
1.202.63.218	10.3.40.30	3	330	3	330	0	0	0.016611	0

As can be seen from the above figure, the data packets are all in the A->B direction, and there is no data packet in the B->A direction.

In this case, you need to confirm whether the switch is mirrored separately. For example, the upstream mirror is connected to the eth0 port and the downstream mirror is connected to the eth2 port. If yes, you need to capture data analysis and confirmation of multiple network ports at the same time. The cleavage is not, contact the customer to check the mirror configuration of the switch.

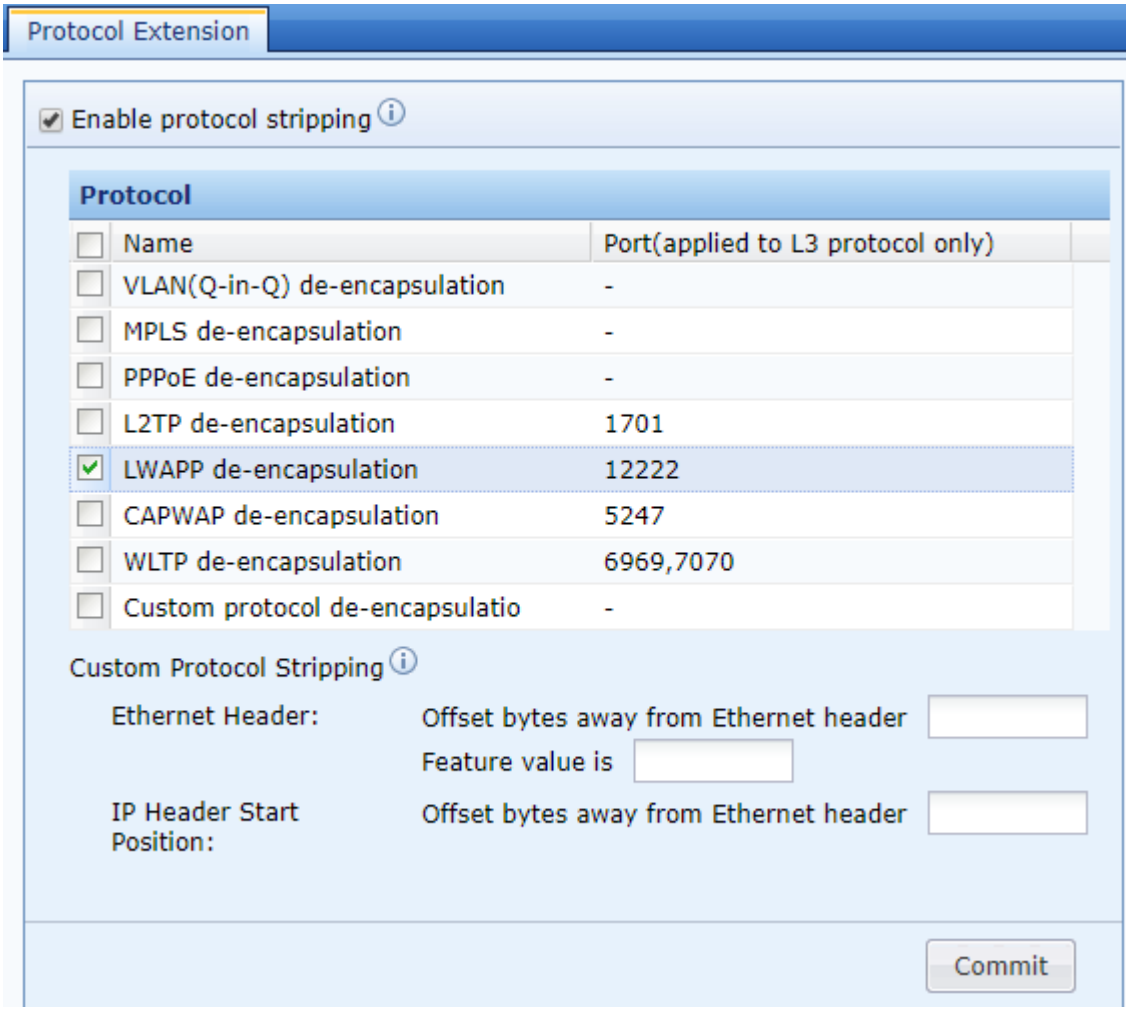
2 Check if there is a multi-layer protocol

Capture a certain amount of data packets in the mirror port, save them as files and download them, and use wireshark to analyze them. See if the packet has a protocol encapsulation.

```
Frame 1: 162 bytes on wire (1296 bits), 162 bytes captured (1296 bits)
Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
Internet Protocol Version 4, Src: 172.31.19.102, Dst: 221.176.215.21
User Datagram Protocol, Src Port: 12222 (12222), Dst Port: 12222 (12222)
LWAPP Encapsulated Packet
IEEE 802.11 QoS Data, Flags: .......T
Logical-Link Control
Internet Protocol Version 4, Src: 10.59.134.232, Dst: 111.62.242.42
Transmission Control Protocol, Src Port: 35561 (35561), Dst Port: http (80), Seq: 1, Ack: 1, Len: 0
```

For example, the packet shown in the above figure, it can be clearly seen that there is a protocol encapsulation. The upper layer IP is 172.31.19.220->221.176.215.21, and the lower layer IP is 10.59.134.232->11.62.242.42. The protocol encapsulation is lwapp.

In this case, you need to enable **[protocol stripping]** on the **[System]-[Network]-[Protocol Extension]** page of IAM.


Protocol Extension
Enable protocol stripping
Protocol
Name
Port(applied to L3 protocol only)
VLAN(Q-in-Q) de-encapsulation
-
MPLS de-encapsulation
-
PPPoE de-encapsulation
-
L2TP de-encapsulation
1701
LWAPP de-encapsulation
12222
CAPWAP de-encapsulation
5247
WLTP de-encapsulation
6969,7070
Custom protocol de-encapsulatio
-
Custom Protocol Stripping
Ethernet Header:
Offset bytes away from Ethernet header
Feature value is
IP Header Start Position:
Offset bytes away from Ethernet header
Commit