

Troubleshooting(software bypass)

When we have problems but we do not know what went wrong, we can start bypass/packet drop list. Through filtered packets, we can know which policy may gone wrong.

Path: System > Troubleshooting > Troubleshooting

Troubleshooting ?

Status: Not conducting troubleshooting currently

Method: Precise traffic analysis ⓘ Global passthrough and analysis L2 packet passthrough

This is recommended when individual network, service or application is disconnected. Specify source IP or destination IP/domain name to analyze matching data packets and locate issues precisely.

Src IP: ⓘ Dst IP/Domain Name: ⓘ Protocol: ▼

Passthrough: Enable Disable

Status: Denied Allowed ⓘ

Turn On

Results (0)

Status:

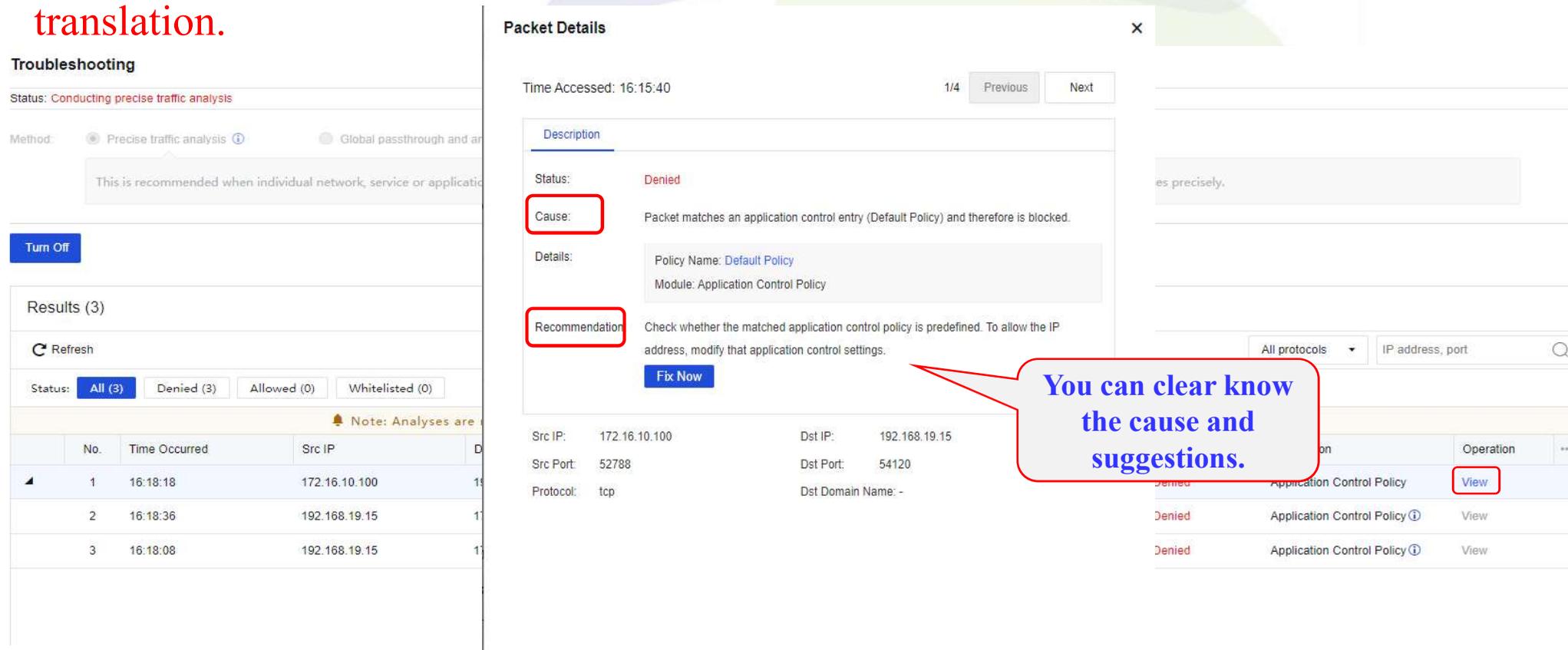
No.	Time Occurred	Src IP	Dst IP	Dst Port	Protocol	Inbound Interface	Outbound Interface	Status	Description	Operation	...
 No data available											

Troubleshooting(software bypass)

Precise traffic analysis

Specify src and dst IP, or dst domain name to analyze matching data packets and locate issues precisely.

Note: If NAT policy is set for application layer gateway, specify IP addresses before and after translation.



The screenshot displays the Sangfor Troubleshooting interface. On the left, the 'Troubleshooting' section shows the status 'Conducting precise traffic analysis' and the method 'Precise traffic analysis'. Below this, a 'Turn Off' button is visible. The 'Results (3)' section shows a table of denied traffic:

No.	Time Occurred	Src IP	Dst IP
1	16:18:18	172.16.10.100	192.168.19.15
2	16:18:36	192.168.19.15	172.16.10.100
3	16:18:08	192.168.19.15	172.16.10.100

The 'Packet Details' window is open, showing the following information:

- Time Accessed: 16:15:40
- Page: 1/4
- Status: Denied
- Cause: Packet matches an application control entry (Default Policy) and therefore is blocked.
- Details: Policy Name: Default Policy, Module: Application Control Policy
- Recommendation: Check whether the matched application control policy is predefined. To allow the IP address, modify that application control settings.
- Fix Now button

At the bottom of the packet details, the following information is displayed:

Src IP:	172.16.10.100	Dst IP:	192.168.19.15
Src Port:	52788	Dst Port:	54120
Protocol:	tcp	Dst Domain Name:	-

A callout box points to the 'Cause' and 'Recommendation' sections, stating: 'You can clear know the cause and suggestions.'

Troubleshooting(software bypass)

Global passthrough and analysis

Global passthrough will let all traffic direct passthrough NGAF

Troubleshooting ?

Status: Conducting global packet analysis

Method: Precise traffic analysis ⓘ Global passthrough and analysis L2 packet passthrough

Cautiously use this when network disconnection occurs and precise traffic analysis does not work effectively.

[Turn Off](#)

Results (9)

[Refresh](#) All protocols ▾ IP address, port 🔍

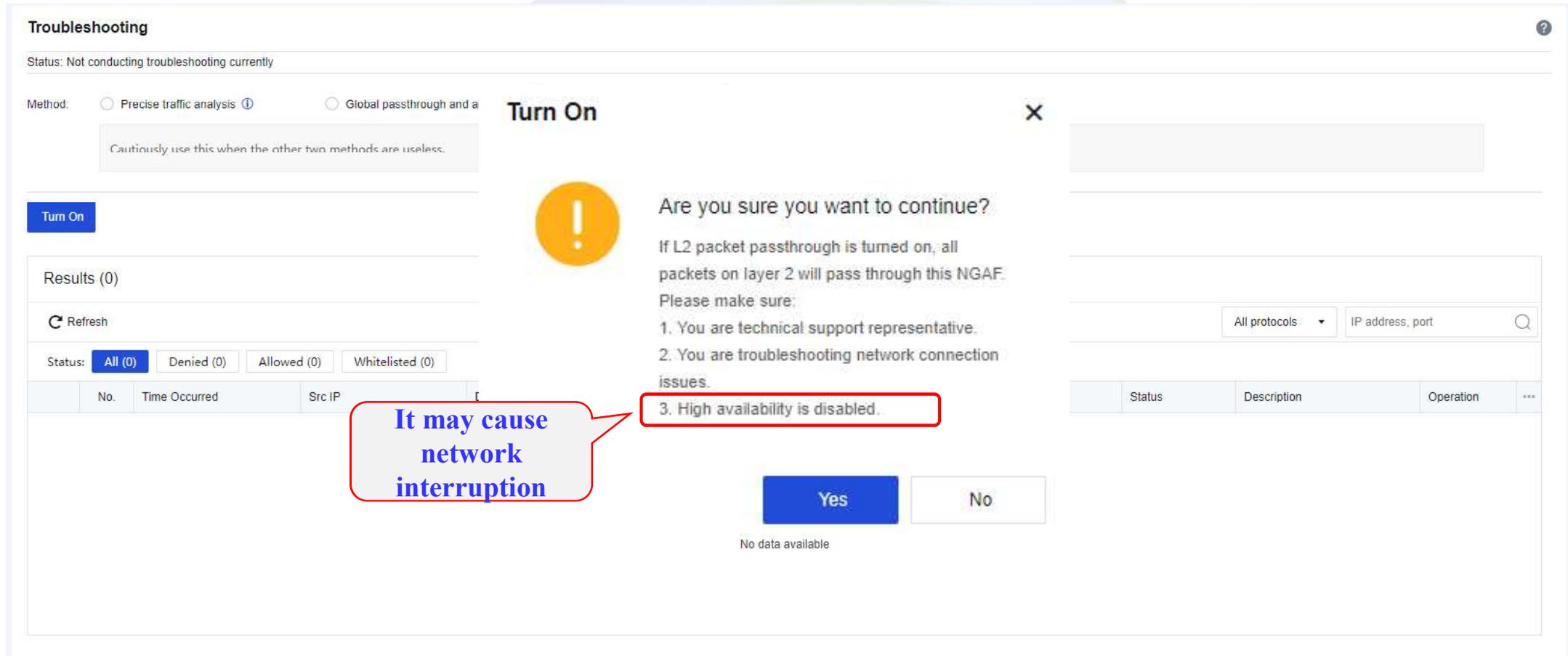
Status: All (9) Denied (9) Allowed (0) Whitelisted (0)

🔔 Too many matches will be caused due to global passthrough. Denied packets are displayed preferentially. Try choosing a smaller scope.

No.	Time Occurred	Src IP	Dst IP	Dst Port	Protocol	Inbound Interface	Outbound Interface	Status	Description	Operation	...
1	16:12:12	172.16.10.100	192.168.19.15	8083	tcp	eth2	eth1	Denied	Application Control Policy	View	
2	16:12:12	192.168.19.15	172.16.10.100	52436	tcp	eth1	eth2	Denied	Application Control Policy ⓘ	View	
3	16:12:12	172.16.10.100	192.168.19.15	8083	tcp	eth2	eth1	Denied	Application Control Policy ⓘ	View	
4	16:12:13	172.16.10.100	192.168.19.15	8083	tcp	eth2	eth1	Denied	Application Control Policy ⓘ	View	
5	16:12:13	192.168.19.15	172.16.10.100	52436	tcp	eth1	eth2	Denied	Application Control Policy ⓘ	View	
6	16:12:13	172.16.10.100	192.168.19.15	8083	tcp	eth2	eth1	Denied	Application Control Policy ⓘ	View	
7	16:12:18	172.16.10.100	192.168.19.15	8083	tcp	eth2	eth1	Denied	Application Control Policy ⓘ	View	
8	16:12:18	192.168.19.15	172.16.10.100	52436	tcp	eth1	eth2	Denied	Application Control Policy ⓘ	View	
9	16:12:18	172.16.10.100	192.168.19.15	8083	tcp	eth2	eth1	Denied	Application Control Policy ⓘ	View	

Troubleshooting(software bypass)

Layer 2 pass-through is only effective for bridge mode. Virtual wire will only be effective if packets go through forwarding network interface.



The screenshot shows the 'Troubleshooting' section of a SANGFOR interface. The status is 'Not conducting troubleshooting currently'. Under 'Method', there are two radio buttons: 'Precise traffic analysis' (selected) and 'Global passthrough and a'. A warning box is present with the text 'Cautiously use this when the other two methods are useless.' Below this is a 'Turn On' button. A dialog box titled 'Turn On' is open, asking 'Are you sure you want to continue?'. It contains the text: 'If L2 packet passthrough is turned on, all packets on layer 2 will pass through this NGAF. Please make sure: 1. You are technical support representative. 2. You are troubleshooting network connection issues. 3. High availability is disabled.' The third point is highlighted with a red box. Below the dialog are 'Yes' and 'No' buttons. In the background, there is a table with columns 'No.', 'Time Occurred', and 'Src IP'. A red callout box points to the dialog with the text 'It may cause network interruption'.

Method: Precise traffic analysis ⓘ Global passthrough and a

Cautiously use this when the other two methods are useless.

Turn On

Results (0)

Refresh

Status: **All (0)** Denied (0) Allowed (0) Whitelisted (0)

No.	Time Occurred	Src IP
-----	---------------	--------

Turn On

Are you sure you want to continue?

If L2 packet passthrough is turned on, all packets on layer 2 will pass through this NGAF. Please make sure:

1. You are technical support representative.
2. You are troubleshooting network connection issues.
3. High availability is disabled.

Yes No

No data available

It may cause network interruption