

# 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:  ⓘ IP Address/Domain ⓘ Protocol: All ▼

Passthrough: ☐ Enable ☒ Disable

Status: ☒ Denied ☐ Allowed ⓘ


Turn On

Results (0)

Refresh

All protocols ▼ IP address, port 🔍

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

No.	Time Occurred	Src IP	Dst IP	Dst Port	Protocol	Inbound Interface	Outbound Interface	Status	Description	Operation	...
<div><p>No data available</p></div>											

# 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.

Troubleshooting

Status: Conducting precise traffic analysis

Method: Precise traffic analysis Global passthrough and an

This is recommended when individual network, service or application

Turn Off

Results (3)

Refresh

Status: All (3) Denied (3) Allowed (0) Whitelisted (0)

Note: Analyses are

No.	Time Occurred	Src IP	D
1	16:18:18	172.16.10.100	15
2	16:18:36	192.168.19.15	17
3	16:18:08	192.168.19.15	17

Packet Details

Time Accessed: 16:15:40 1/4 Previous Next

Description

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

Src IP: 172.16.10.100 Dst IP: 192.168.19.15

Src Port: 52788 Dst Port: 54120

Protocol: tcp Dst Domain Name: -

All protocols IP address, port

Operation	Operation	Operation
Denied	Application Control Policy	View
Denied	Application Control Policy	View
Denied	Application Control Policy	View

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.

### Troubleshooting

Status: Not conducting troubleshooting currently

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**

All protocols ▼ IP address, port 🔍

Status	Description	Operation	...
--------	-------------	-----------	-----