SANGFOR

IAM

Port Mapping(DNAT) Failure Troubleshooting Guide

Version 12.0.18

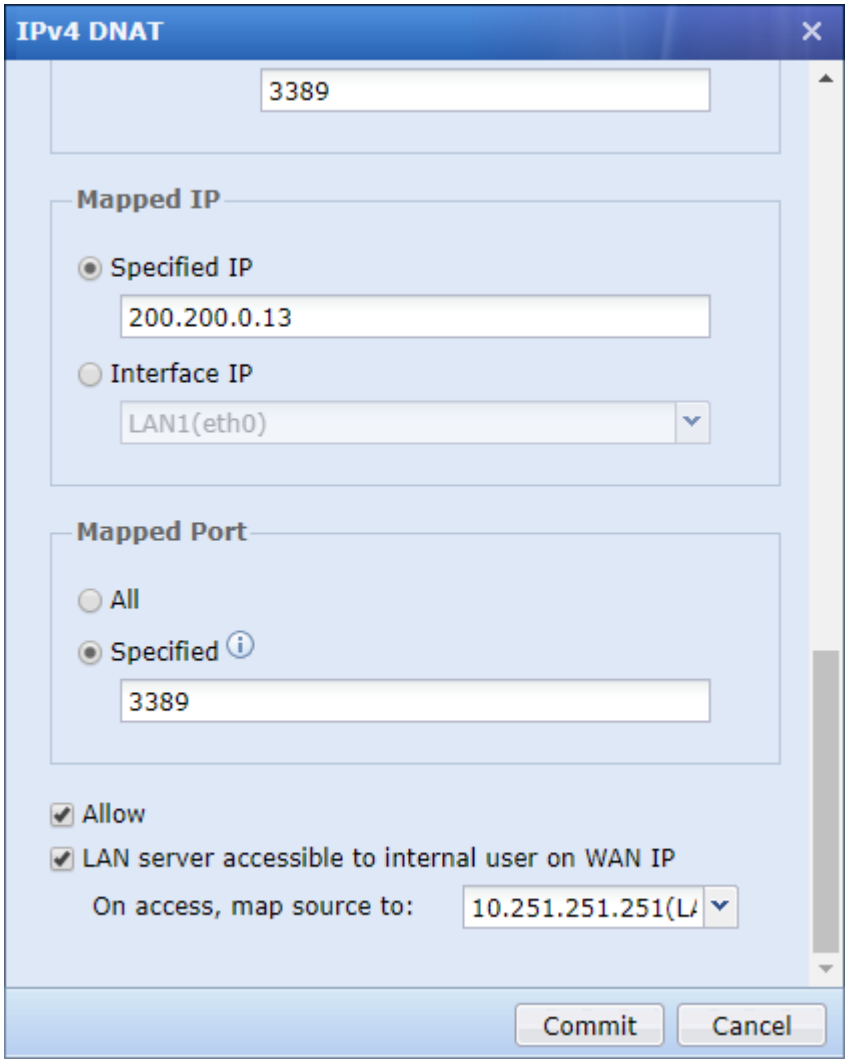
Change Log

Date	Change Description
May 18, 2019	Version 12.0.18 document release.

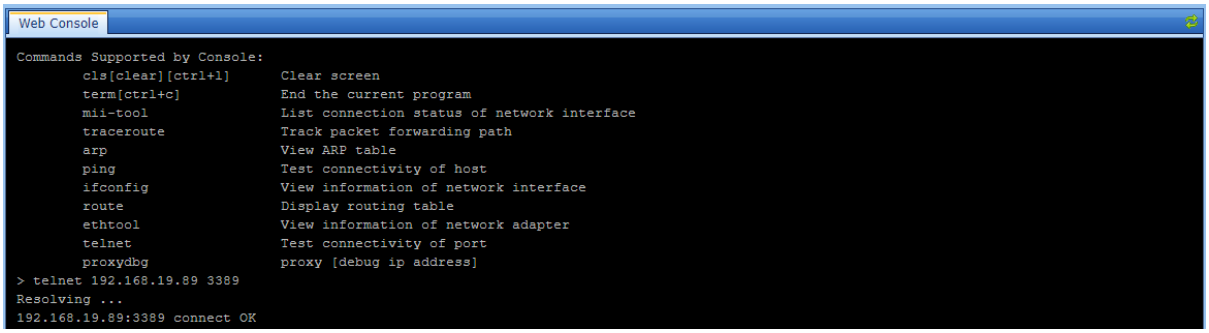
CONTENT

1 Basic troubleshooting

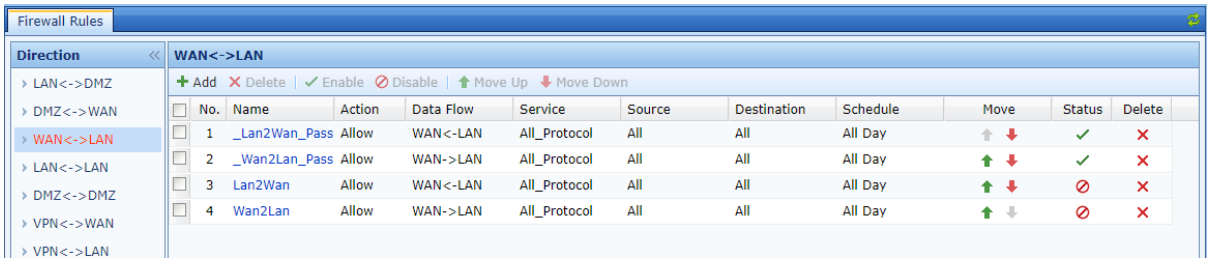
- Check whether the configuration is correct, for example, whether the Destination IP address is incorrectly configured, the port configuration is incorrect, and whether "**Allow**" is checked.



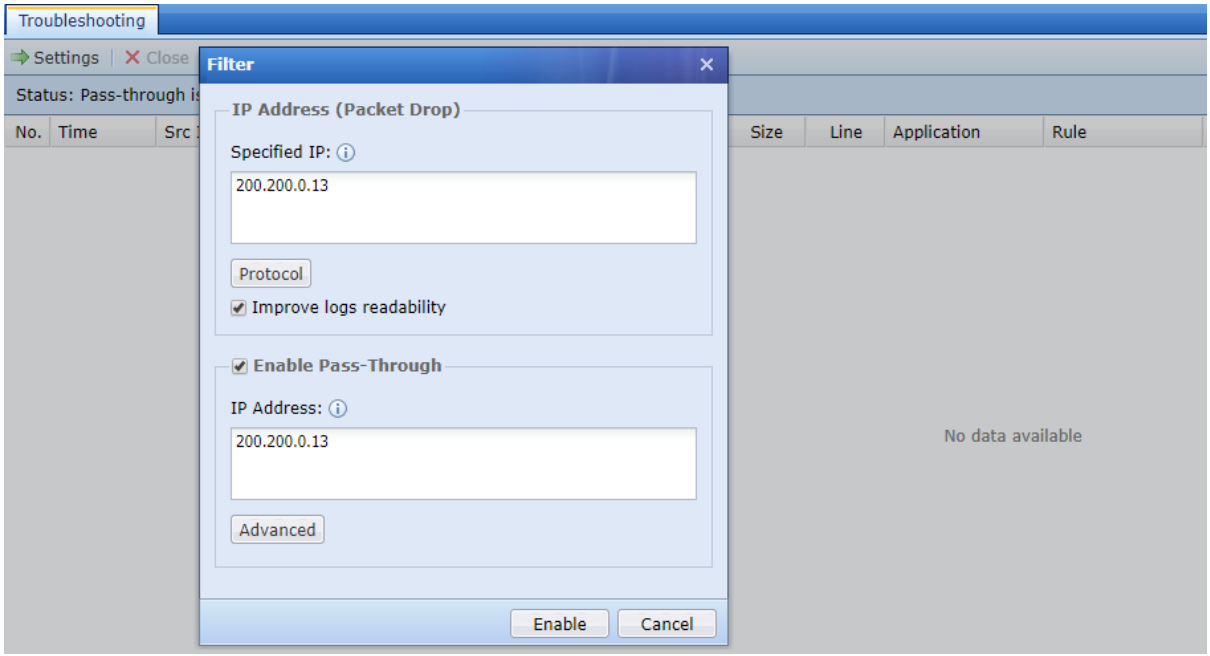
- When there are multiple DNAT RULEs, check for configuration conflicts: The priority of DNAT RULE is matched from top to bottom.
- Check whether IAM able to access the intranet server. If it is a TCP port, you can test the connectivity of the intranet server port on the IAM. If unable to access, check whether the route is configured correctly, and check other devices have intercepted the related data, or the server does not provide services.

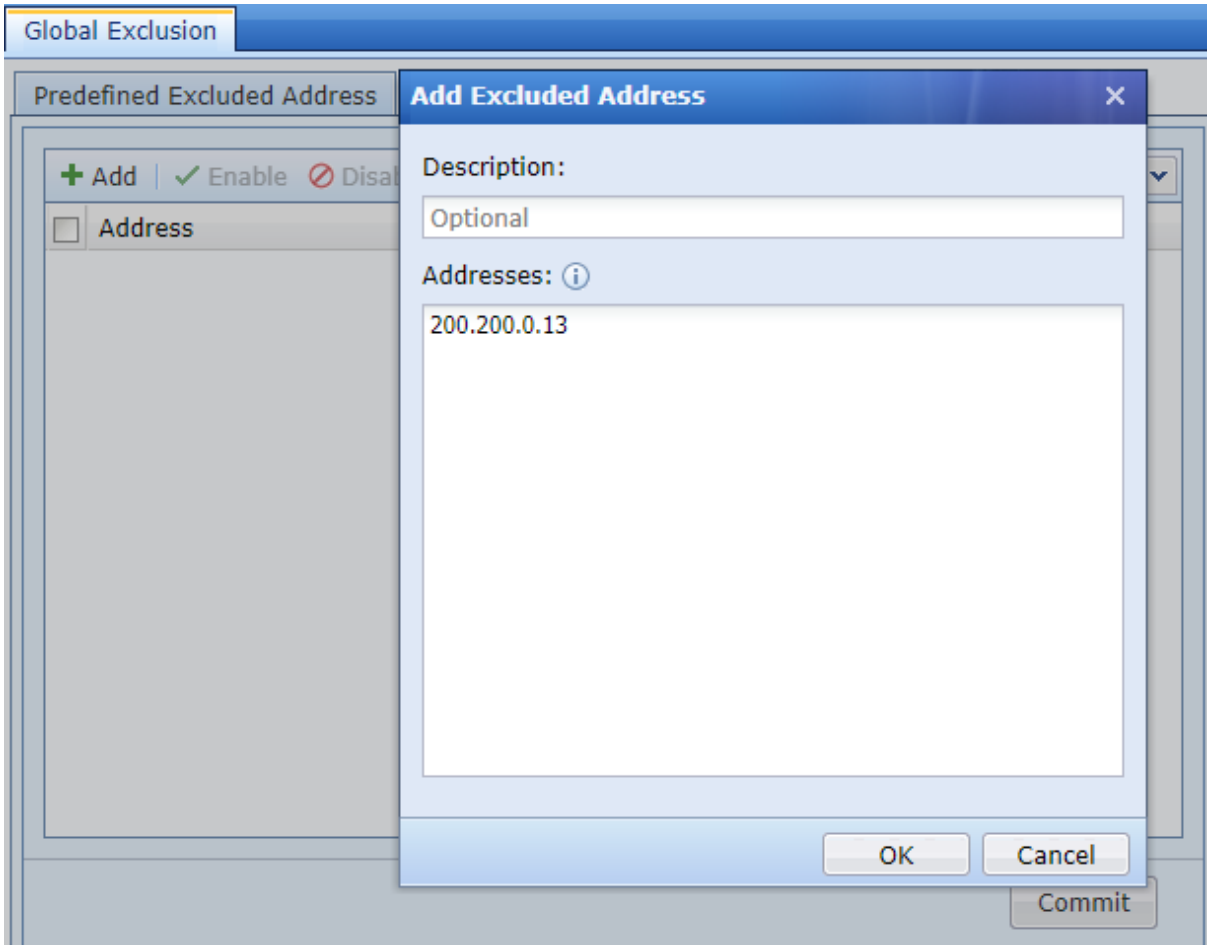


- If you check the configuration and find that "**Allow**" is not checked, you need to check whether the Firewall Rules are configured separately.



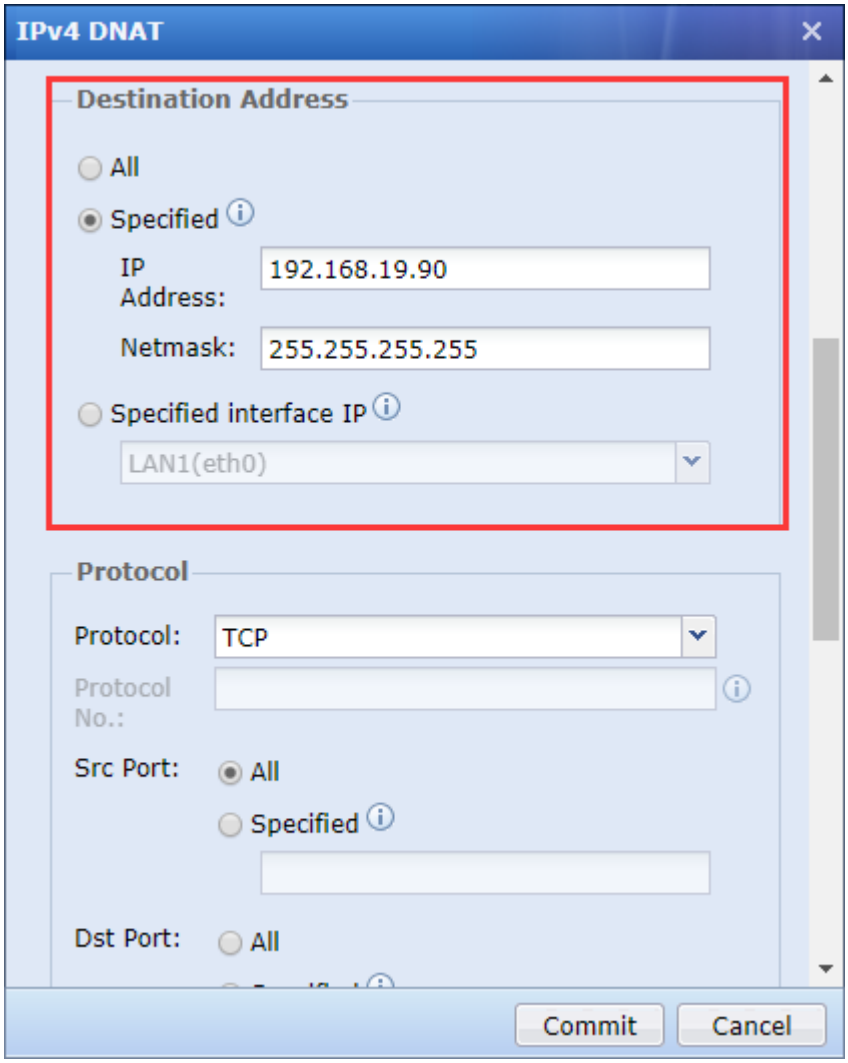
- Enable **Troubleshooting** and **Global Exclusion** to check whether IAM able communicate properly.



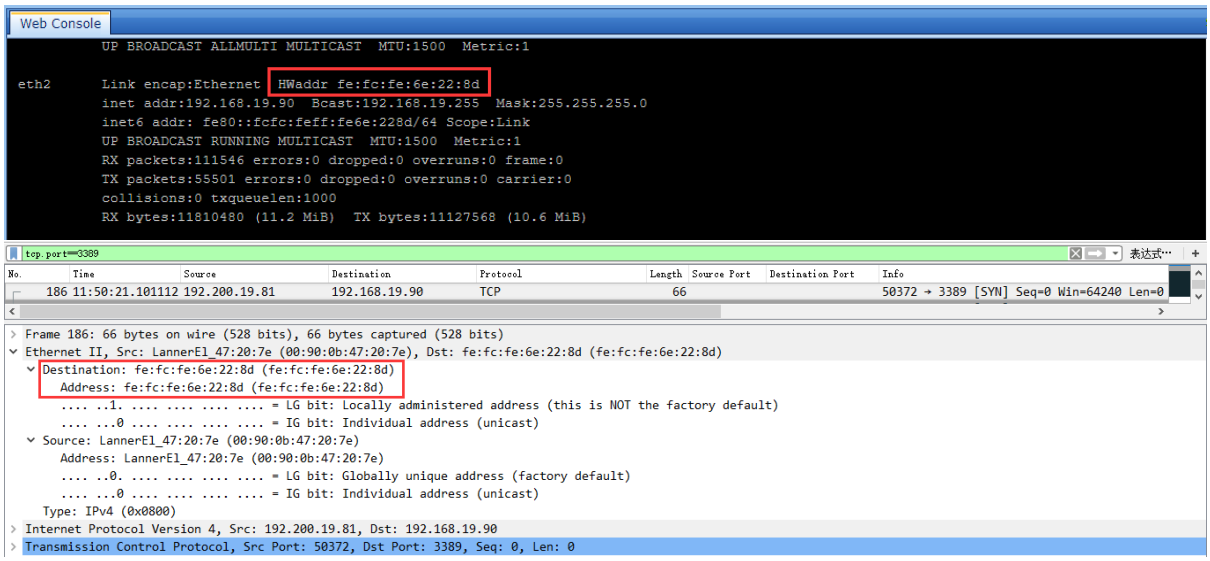


2 WAN->LAN direction DNAT rules do not take effect

- Capture and analyze: Check whether the "**Destination Address**" is configured properly on the IAM's WAN port, or check whether the packet has sent from external network to the IAM's WAN port's destination IP.



- Capture and analyze: The destination MAC address of the data packet received by the IAM WAN port is the MAC address of the IAM's interface.



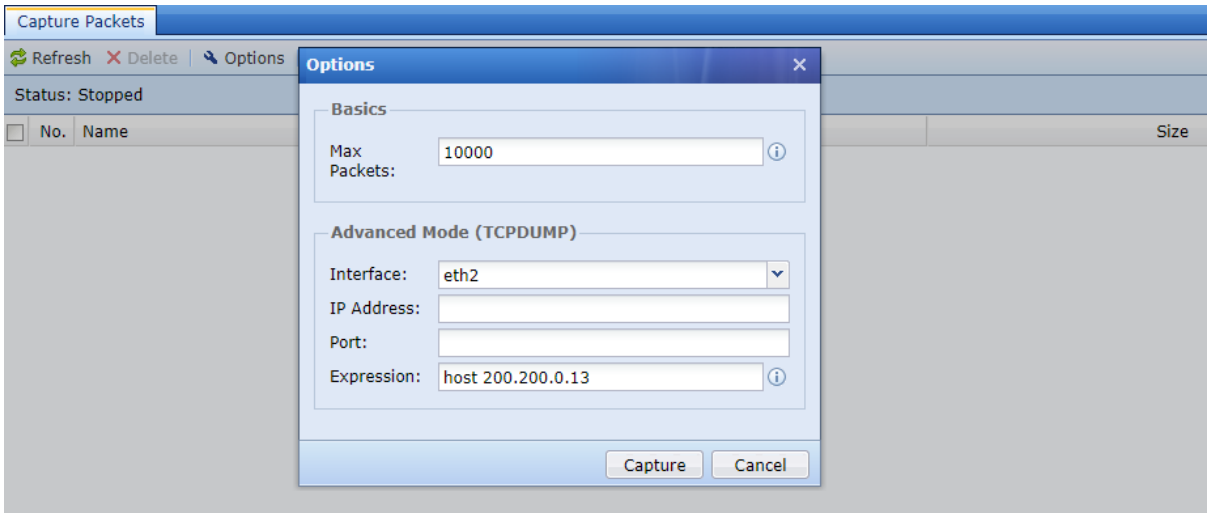
- Capture and analyze: Check whether the IAM LAN port has forwarding data to the server. If "**LAN server accessible to internal user on WAN IP**" is checked, please check whether the source IP address of the packet is translated.
- Capture the packet on the intranet server, confirm that the server has received the request packet,

and confirm that the server has reply packet.

- Capture packet analysis: Whether the server returned packets were sent to IAM. If the SNAT rule is not used, when the public network IP accesses the server and the server does not return the packet, it is necessary to confirm whether the gateway or the intranet switch route on the server will return the returned data to the IAM LAN port.
- If the external network is a mail server, the feedback email is unsuccessful. You need to pay attention to whether the internal network has a spam filtering system and whether "**LAN server accessible to internal user on WAN IP**" is checked. After the "**LAN server accessible to internal user on WAN IP**" is checked, the source IPs are all the same, and may be filtered by the spam filtering system to determine that the same IP sends too many emails.

3 LAN->LAN direction DNAT rules do not take effect

- Confirm that the WAN->LAN direction access is successful. If the DNAT rule in the WAN->LAN direction is in effect, then the network connectivity between IAM and the server is ruled out. You need to troubleshoot problems between PCs and devices.
- If the access in the WAN->LAN direction is not successful, check the WAN->LAN direction DNAT rule that does not take effect first.
- Capture the packet on the IAM's LAN port, and check whether the PC access to the public network IP/domain name packet through the IAM LAN port.
- Capture packets on the IAM LAN port to confirm whether the device has SNAT to access the server.
- Capture the packet on the server, confirm that the server has received the packet request, and confirm that the server has a reply packet.
- Capture packets on the IAM's LAN port and check whether the server's data packets are transmitted to the IAM's LAN port.



- Capture the packet on the IAM's LAN port and check if the IAM has returned the data to the PC.