

#Troubleshooting# Troubleshoot internet access with NSF as firewall

***Product:** NSF

***Version:** 8.0.85

***1. Introduction**

1.1 User Scenario

Replacing a firewall in an existing network environment can be a challenge. In this guide, we will see what the possible solutions are in case there is no internet connectivity after the adoption of Sangfor NSF.

1.2 Requirements

1. Sangfor NSF updated to the latest release.

***2. Troubleshoot Guide**

In this troubleshooting guide, we will show what to check if users behind Sangfor NSF cannot go to the internet (regardless of the configuration mode).

2.1 Sangfor NSF configured as Route mode

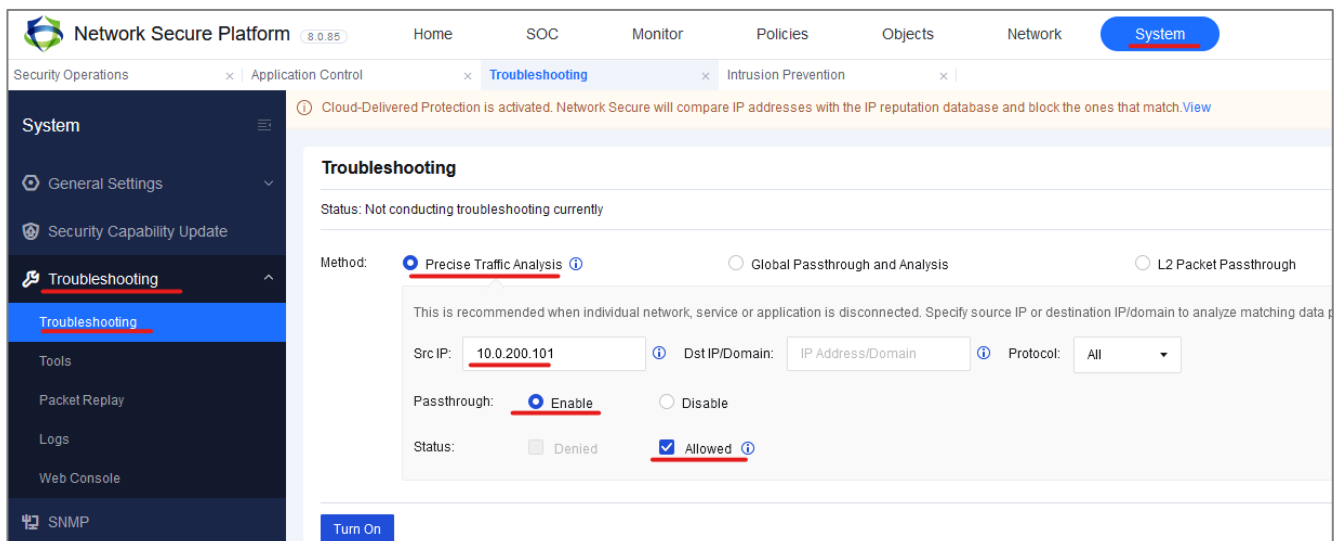
If you have deployed Sangfor NSF as route mode and configured the intranet LAN as Layer 3, the LAN PCs' gateway is set to the LAN interface of the NSF.

If you're unable to ping the LAN interface, verify if there are any restrictions configured for the PC's IP in the switch, or if the VLAN interface of the PC connected to the switch has been incorrectly configured. Also, check if an Access Control List (ACL) has been set up in the switch to prevent the PC IP from accessing the external network.

Instead, if you configure your intranet LAN as Layer 3 on NSF and if an intranet user is unable to access the internet in a Layer 3 environment, you can use the PC that is unable to access the

internet to ping the switch core IP. If the ping is unsuccessful, check this section for any issues with the switch core that the pc is connected to. If the switch core IP address is pingable, then proceed to ping the LAN interface of the NSF.

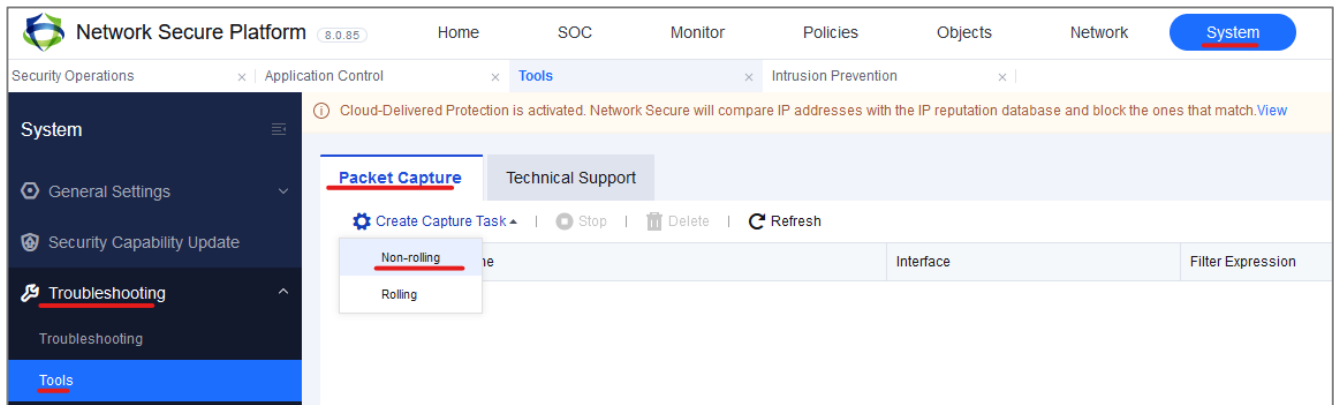
If you're able to log in, you can enable pass-through for the IP that cannot access the internet on the device. This will help you verify whether there is any policy blocking the IP from accessing the internet. To do this, navigate to: **System -> Troubleshooting -> Troubleshooting -> Precise Traffic Analysis** and configure the PC IP in the IP address field. Be careful not to configure the IP address in the excluded IP field. For example, if we have a PC with ip 10.0.200.101 we can enable traffic analysis as shown below:



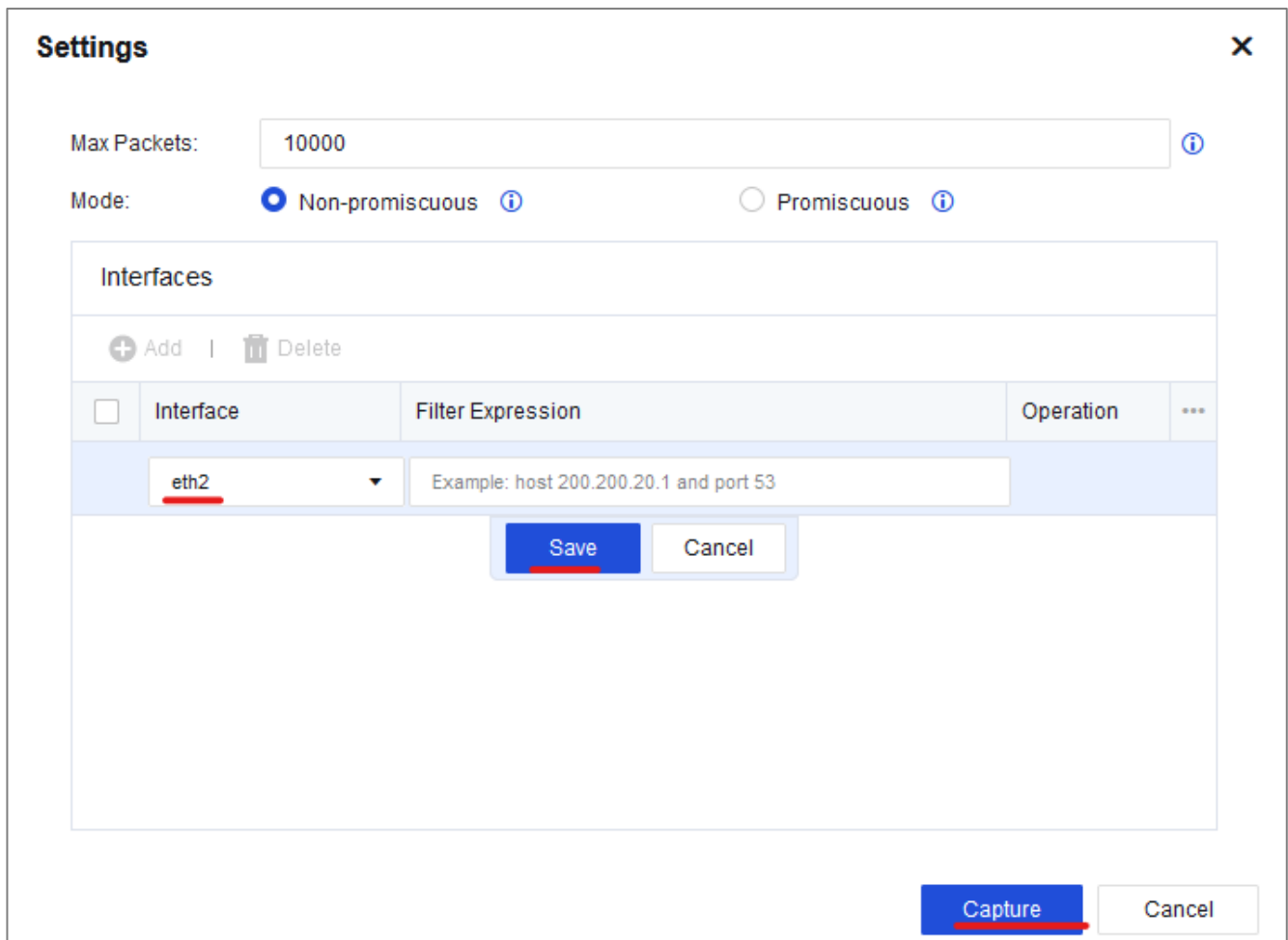
If you're still unable to access the internet after enabling pass-through, you can use **System -> Troubleshooting -> Tools -> Packet Capture** to capture the PC source IP in the LAN interface. Analyze the IP packets to verify whether the source IP packet has reached the LAN interface of the device or if other devices in the internal network have NATed the IP that cannot access the internet.

For capturing the LAN interface (eth2 in our NSF) here are the steps:

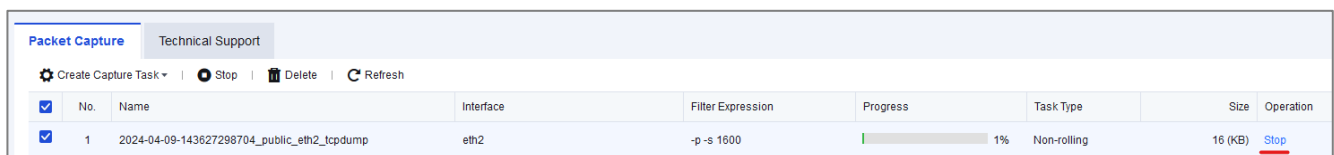
- 1) Start a non-rolling packet capture



2) Specify the LAN interface and click save and capture



3) After trying to connect to the internet from the intranet clients click stop capture.



4) After that download this traffic dump by selecting it and click download

Packet Capture		Technical Support						
<div> <div>Create Capture Task</div> <div>Stop</div> <div>Delete</div> <div>Refresh</div> </div>								
<input checked="" type="checkbox"/>	No.	Name	Interface	Filter Expression	Progress	Task Type	Size	Operation
<input checked="" type="checkbox"/>	1	2024-04-09-143627298704_public_eth2_tcpdump	eth2	-p -s 1600	Completed	Non-rolling	5.05 (MB)	Download Recapture

- 5) Use an external tool like Wireshark to analyze this file that contains traffic information to find out which type of traffic goes from intranet to firewall.

If the LAN interface is unable to capture the source IP, you should check if there are any Access Control List (ACL) restrictions on the source IP in the switch core.

If the LAN interface can capture the source IP, you should then capture the WAN interface for the PC to ping the destination IP.

This is to verify that the PC's IP address has been successfully translated. Please refer to the previous steps for specific configuration details.

In this document, the device's WAN interface is Eth1, and the LAN interface is Eth2. The PC's IP address is 10.0.200.101.

You need to verify whether the source IP in the packet has not been converted to a public IP.

Check if the PC's source IP has been added to the Source Network Address Translation (SNAT) of Network Address Translation (NAT).

2.2 Sangfor NSF configured as Bridge mode

If you have deployed Sangfor NSF as bridge mode and the intranet users cannot go to the Internet, I recommend enabling pass-through as described before to verify whether there is any policy blocking the IP from accessing the Internet.

If the internal network is still unable to access the Internet after enabling pass-through, you can use the packet capture method of the route mode to capture the PC's IP. This will help you verify whether the data packet is going through the NSF. If you're unable to capture the data packet of the PC, check whether there are any restrictions configured for the PC's IP in the switch, or if the VLAN interface of the PC connected to the switch has been incorrectly configured. Also, check if an Access Control List (ACL) has been set up in the switch to prevent the PC's IP from accessing the external network.

If you cannot bypass the NSF, check if there is any problem with the PC or other devices on the

internal network

***3. Precaution**

Please remember that once Layer 2 pass-through is enabled, only the basic network routing and forwarding capabilities are retained. The traffic no longer enters other functional modules like application control policies, security policies, etc.