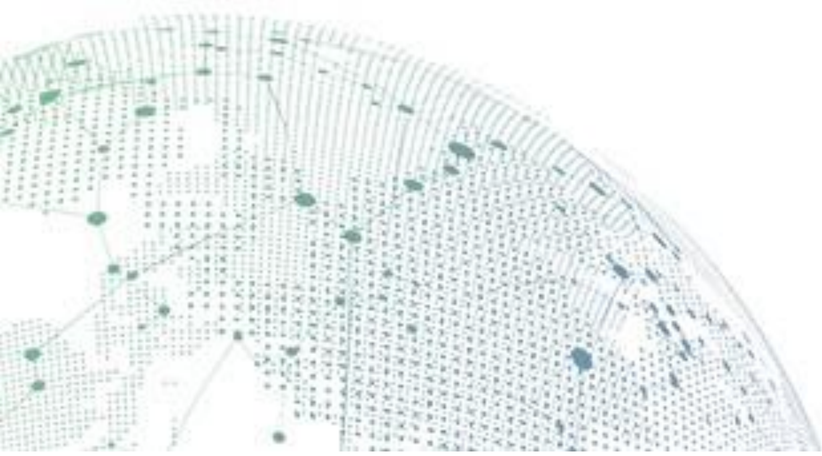
NGAF

DNAT Troubleshooting

Version 8.0.6



Change Log

Date	Change Description
May 8, 2019	DNAT Troubleshooting

Content

Chapter 1 Application scenario 1

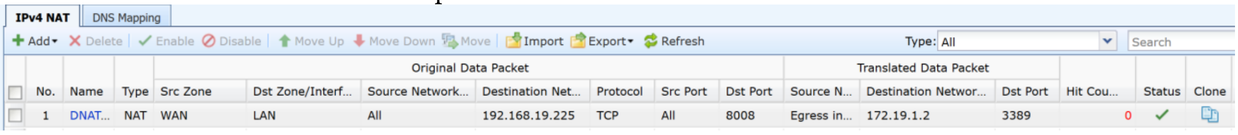
Chapter 2 Troubleshooting methods...1

Chapter 1 Application scenario

DNAT is configured but the business cannot be accessed normally.

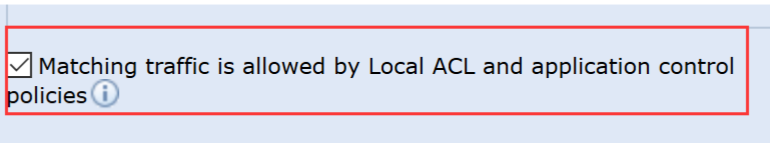
Chapter 2 Troubleshooting methods

1. Go to **Policies** > **NAT** check if the basic configuration is correct, The **Src Zone** selects the **WAN** because the accessed packets come from the public network, The **Dst Zone** of the **Original Data Packet** is the server zone. The **Destination Network** of the **Orginal Data Packet** is the WAN IP of NAGF.The **Destination IP** of the **Translated Data Packet** is the real IP of the server. The **Dst Port** of the Translated Data Packet is the service port.



				Original Data Packet						Translated Data Packet					
□	No.	Name	Type	Src Zone	Dst Zone/Interf...	Source Network...	Destination Net...	Protocol	Src Port	Dst Port	Source N...	Destination Networ...	Dst Port	Hit Cou...	Status	Clone
□	1	DNAT...	NAT	WAN	LAN	All	192.168.19.225	TCP	All	8008	Egress in...	172.19.1.2	3389	0	✓	

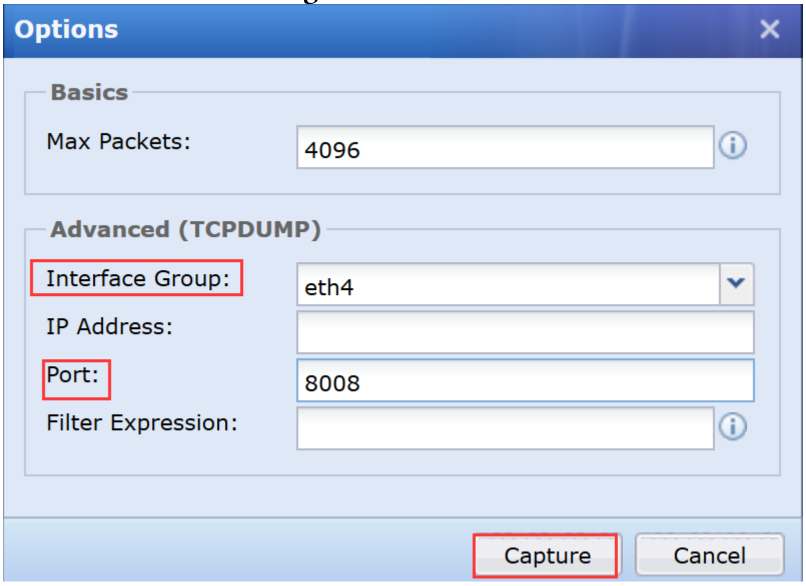
2. Go to **Policies** > **NAT** **Edit NAT** Rule as follows,Matching traffic allowed by Local ACL and application control policies.



☑ Matching traffic is allowed by Local ACL and application control policies

3. Test to confirm that the public network IP of NGAF can be accessed normally. If the service uses TCP port ,Use the **telnet** command on other public network computers to test whether the port can pass.

4. Go to **System** > **Troubleshooting** > **Capture Packets** select **Options** capture packet. Pay attention to select the WAN interface and **Dst Port** of **Orginal Data Packet**.



Basics

Max Packets: 4096

Advanced (TCPDUMP)

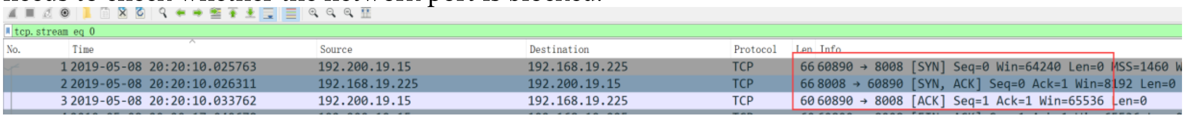
Interface Group: eth4

IP Address:

Port: 8008

Filter Expression:

5. Analyze packets using **wireshark** software, Wireshark can be downloaded on google. Normal packet we can see a TCP three-way handshake as shown below. If the first SYN request in the packet cannot be found in the packet, It must be that the intermediate network device intercepts the data packet and needs to check whether the network port is blocked.



```
tcp.stream eq 0
No.   Time                        Source           Destination      Protocol  Len Info
    1 2019-05-08 20:20:10.025763  192.200.19.15    192.168.19.225   TCP        66 60890 → 8008 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 W
    2 2019-05-08 20:20:10.026311  192.168.19.225   192.200.19.15    TCP        66 8008 → 60890 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0
    3 2019-05-08 20:20:10.033762  192.200.19.15    192.168.19.225   TCP        60 60890 → 8008 [ACK] Seq=1 Ack=1 Win=65536 Len=0
```

6. Go to **System** > **Troubleshooting** > **Web Consle** use the **ping** or **telnet** command to test whether the NGAF to the server network is normal.

7. Capture packets in the server Zone of Interface, Compare the server zone and WAN packets for abnormalities.

SANGFOR

Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.The information in this document is subject to change without notice. To obtain the latest version, contact the international service center of SANGFOR Technologies Inc