Sangfor NGAF Configuration Guide

DNS Proxy and DNS Transparent Proxy

Product Version	8.0.35
Document Version	01
Released on	Jun. 07, 2021

Change Log

Date	Change Description
Jun. 07, 2021	This is the first release of this document.

Contents

1 Introduction

1.1 Abbreviations and conventions

NGAF in this article refers to the SANGFOR NGAF device.

1.2 Feedback

If you find any questions of this documents, please feel free to give us feedback, email: tech.support@sangfor.com.

2 DNS Proxy

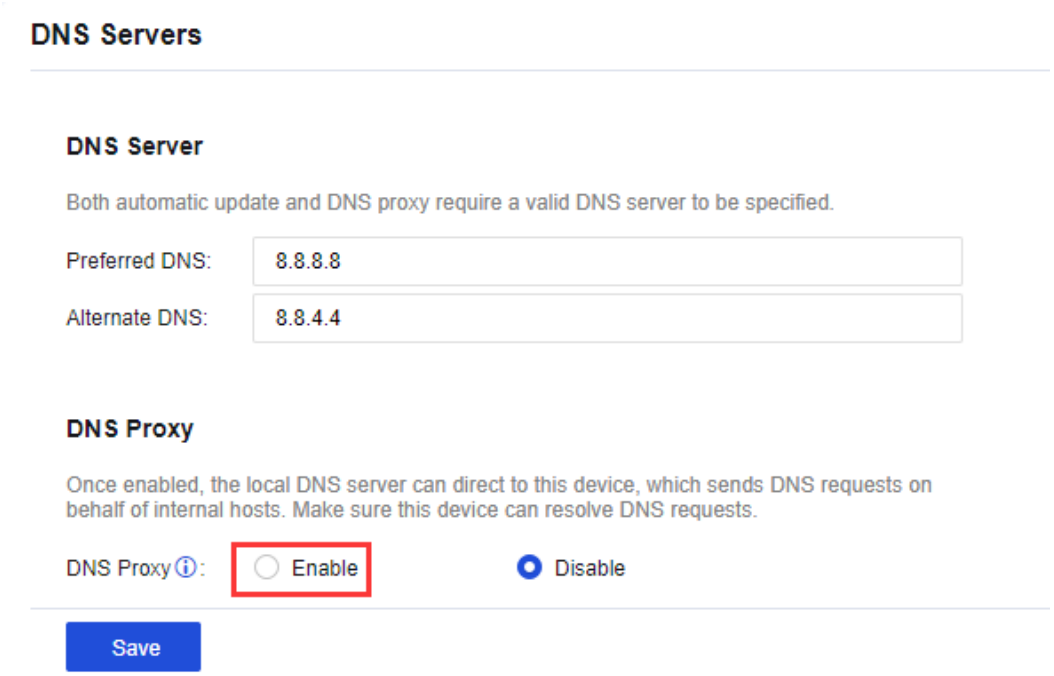
2.1 Scenario

DNS proxy is mainly configured on the gateway device, and the gateway sends DNS requests to the domain name server instead of the intranet host. It is mainly used in the case that sometimes the DNS server address cannot be configured in the intranet network or the user is not clear about the DNS server address, and the DNS address is directly filled in as the gateway address for the convenience of the user.

Test environment is shown as below:

2.2 Configuration Steps

Step 1. Login to NGAF web console, go to **Networks** > **DNS** > **DNS Servers.** Enable the DNS proxy option as shown in figure below.

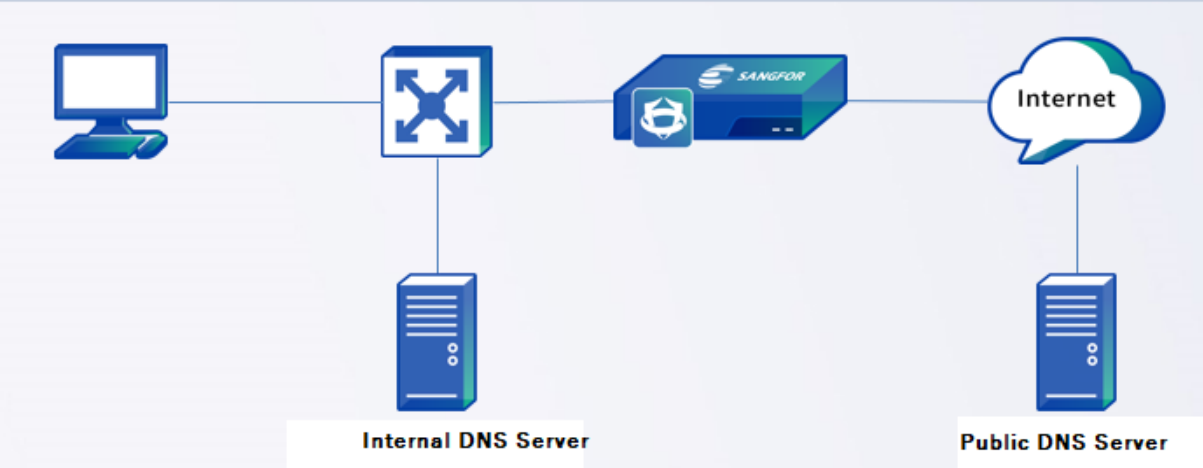


3 DNS Transparent Proxy

3.1 Scenario

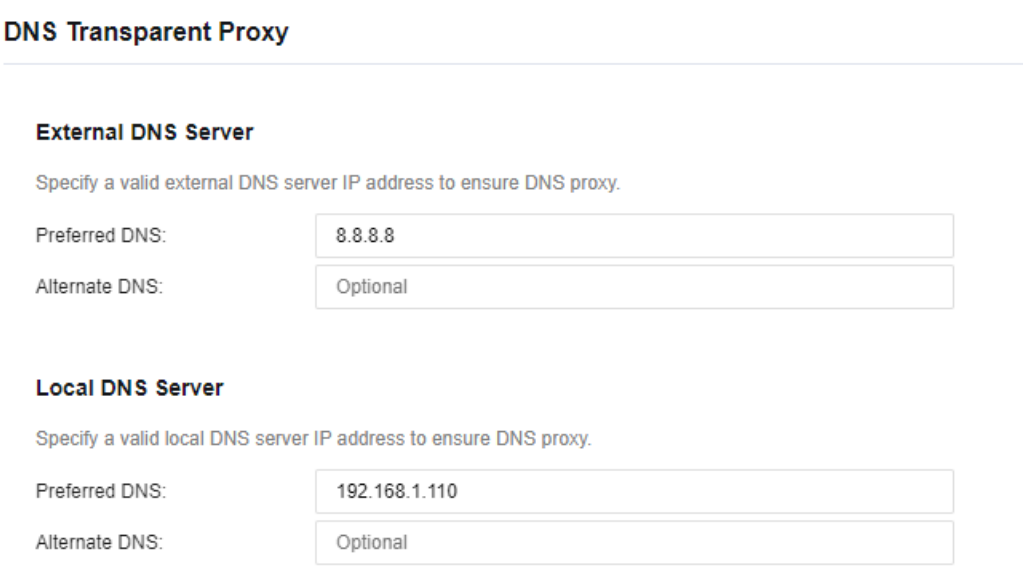
DNS transparent proxy is configured on the gateway device, and the gateway intercepts the DNS request from the intranet host and then sends the DNS request to its own configured domain name server, which has the following two main scenarios.

- Setting arbitrary DNS addresses for the convenience of intranet users who are not aware of the DNS server addresses.
- Sending DNS requests to the DNS servers specified by the gateway, which can be combined with policy routing for routing, etc.

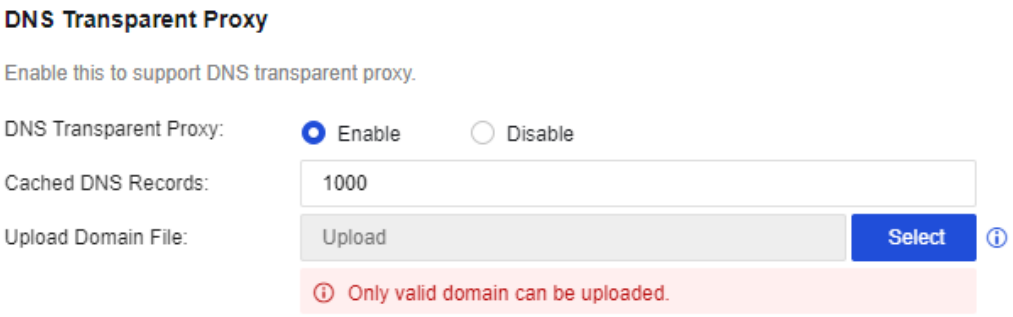


3.2 Configuration Steps

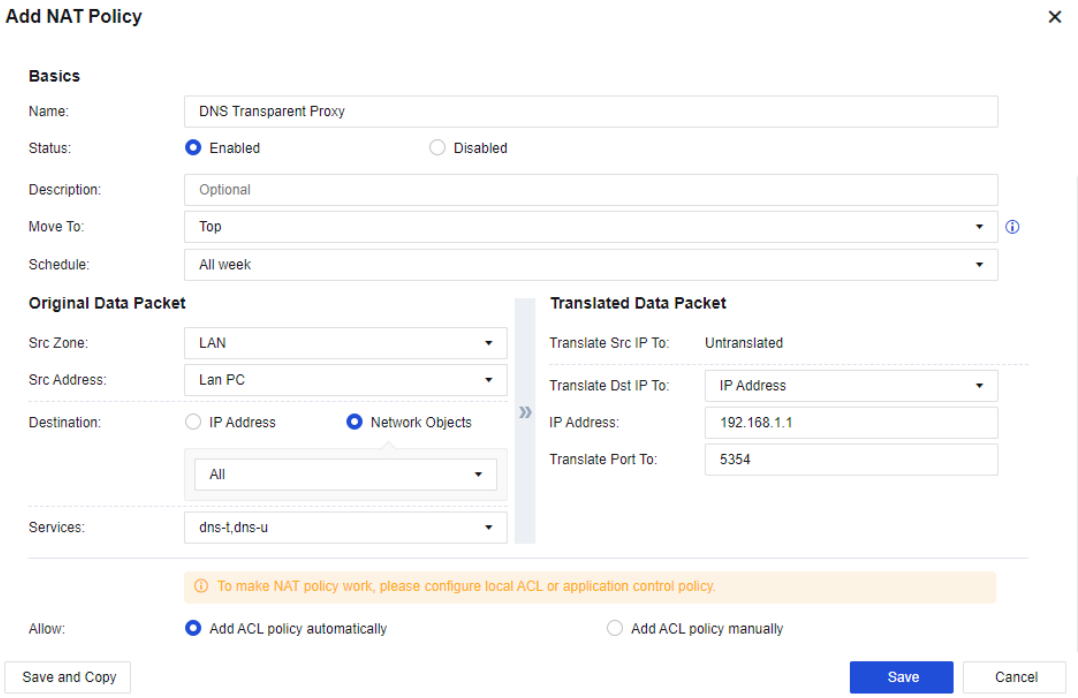
Step 1. Login to NGAF web console, go to **Networks** > **DNS** > **DNS Transparent Proxy.** Fill in the **External DNS Server** IP address and if there is an internal DNS server, fill in the IP address in **Local DNS Server.**



Step 2. **Enable** the DNS Transparent Proxy and fill in the DNS cache number in **Cached DNS Records**.



Step 3. Configure DNAT policy, **Policies** > **NAT** click **Add** to configure DNAT policy.



Original Data Packet

- **Src Zone**: select internal zone
- **Src Address**: select internal IP address/segment
- **Destination**: select Network Objects and select All
- **Services**: select TCP DNS and UDP DNS service

Translated Data Packet

- **IP Address**: fill in NGAF Lan interface IP address
- **Translate Port To**: Fill in port 5354

4 Precaution

i. The DNS server of the NGAF should be set up correctly to ensure that it can perform DNS resolution properly.

ii. DNS proxy and DNS transparent proxy not support in a bridge/virtual wire deployment environment.

iii. The DNS **uses TCP** Port **53** for zone transfers, for maintaining coherence between the DNS database and the server. The **UDP** port **53** is used when a client sends a query to the DNS server.

iv. DNS proxy use is **TCP** port **53**, NGAF's DNS proxy is open all for zone can access this port, such as NGAF deployment in the network gateway, it is recommended configure application control or Local ACL policy to deny block external unknown IP address access this port.

v. Require to configure a DNAT policy in order for DNS Transparent Proxy to work normally.

vi. The port used by the DNS transparent proxy is TCP port 5354.

vii. The DNS proxy requires the client to set DNS as the NGAF interface IP; the DNS transparent proxy does not require the client to set DNS as the NGAF interface IP.

viii. DNS transparent proxy will perform intranet lookup for DNS requests that are in the list of uploaded domain name files, and will perform extranet lookup for DNS requests that are not in the list of uploaded domain name file

SANGFOR