



# Sangfor NGAF

## NAT Configuration Guide

<b>Product Version</b>	8.0.35
<b>Document Version</b>	01
<b>Released on</b>	July. 12, 2021



Copyright © Sangfor Technologies Inc. 2021. All rights reserved.

Unless otherwise stated or authorized, Sangfor Technologies Inc. (hereinafter referred to as "Sangfor") and its affiliates reserve all intellectual property rights, including but not limited to copyrights, trademarks, patents, and trade secrets, and related rights to text, images, pictures, photographs, audio, videos, charts, colors, and layouts as presented in or concerning this document and content therein. Without prior written consent of Sangfor, this document and content therein must not be reproduced, forwarded, adapted, modified or displayed or distributed by any other means for any purpose.

## **Disclaimer**

Products, services or features described in this document, whether wholly or in part, maybe not within your purchase scope or usage scope. The products, services or features you purchase must be subject to the commercial contract and terms as agreed by you and Sangfor. Unless otherwise provided in the contract, Sangfor disclaims warranties of any kind, either express or implied, for the content of this document.

Due to product version upgrades or other reasons, the content of this document will be updated from time to time. Unless otherwise agreed, this document is used for reference only, and all statements, information, and recommendations therein do not constitute any express or implied warranties.

## Change Log

Date	Change Description
July. 12, 2021	This is the first release of this document.

# Contents

Change Log.....	1
1 Introduction.....	3
1.1 Abbreviations and conventions .....	3
1.2 Feedback .....	3
2 Scenario .....	4
3 Network Topology .....	4
4 Application Scenes.....	4
4.1 Source NAT .....	4
4.2 Destination NAT .....	6
4.3 Bidirectional NAT .....	8
5 Precautions.....	10

# 1 Introduction

## 1.1 Abbreviations and conventions

NGAF in this article refers to the SANGFOR NGAF device.

## 1.2 Feedback

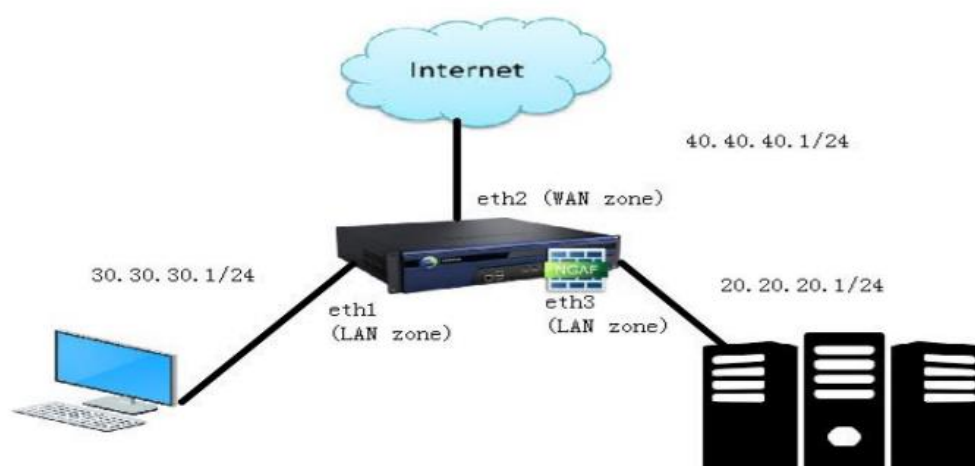
If you find any questions about this document, please feel free to give us feedback, email: [tech.support@sangfor.com](mailto:tech.support@sangfor.com).

## 2 Scenario

Network Address Translation includes **Source NAT**, **Destination NAT** and **Bidirectional NAT**.

- The main purposes of **Source NAT** are to act as agent for intranet user to access Internet by translating source IP address to public IP address.
- The main purpose of **Destination NAT** is to advertise and promote the internal server to public network by translating the destination IP address to private IP address.
- **Bidirectional NAT** is to allow intranet users to access internal server via public IP address or domain name of the internal server.

## 3 Network Topology



## 4 Application Scenes

### 4.1 Source NAT

Requirements: Agent for intranet users to access Internet

Explanations for configuration:

- Step 1.** Ensure that the direction of data flow which needs address translation is correct.

**Step 2.** Under **Policies > NAT**, click **Add** button and choose the type as **Source NAT** to define new SNAT rule.

**Add NAT Policy**

LAN Zone  
L3\_trust\_A  
Internal Host  
internal

Access Public Host

Public Zone  
L3\_untrust\_A  
Public Host  
All

Translated Src IP  
Outbound Interface

NGAF

Type:  Source NAT  Destination NAT  Bidirectional NAT

**Basics**

Name: SNAT

Status:  Enabled  Disabled

Description: Optional

Move To: Top

Schedule: All week

**Original Data Packet**

Src Zone: L3\_trust\_A

Src Address: internal

Dst Zone/Interface:  Zone  Interface  
L3\_untrust\_A

Dst Address: All

Services: any

**Translated Data Packet**

Translate Src IP To: Outbound Interface

Translate Dst IP To: Untranslated

Translate Dst Port To: Untranslated

Save and Copy Save Cancel

**Src Zone:** Zone where the users need to access Internet.

**Src Address:** IP addresses or IP range of users who need to access Internet.

**Dst Zone/Interface:** Destination zone or interface that needed to be accessed.

**Dst Address:** IP group that wants to access Internet. By default, it is filled with "All" and it can be changed manually.

**Service:** Service that users used to access Internet. It can be changed manually according to the need.

**Translate Src IP To:** To specify IP addresses from intranet to be translated to which outgoing interface. Normally, the "Outbound interface" is chosen.

## 4.2 Destination NAT

Requirements: When users from WAN need to access an internal server or when there is an internal server that is needed to be advertised or promoted to the Internet such as a web server.

Explanations for configuration:

**Step 1.** Ensure that the direction of data flow which needs address translation is correct.

**Step 2.** Go to **Policies > NAT**, click **Add** button and choose the type as **Destination NAT** to define new DNAT rule.

**Add NAT Policy**

Public Zone  
L3\_untrust\_A

Public Host  
All

Dst IP-Port  
40.40.40.1:0-65535

Access Internal Server

Internal Servers  
20.20.20.1

NGAF

Type:  Source NAT  Destination NAT  Bidirectional NAT

**Basics**

Name: DNAT

Status:  Enabled  Disabled

Description: Optional

Move To: Top

Schedule: All week

**Original Data Packet**

Src Zone: L3\_untrust\_A

Src Address: All

Destination:  IP Address  Network Objects

40.40.40.1

Services: any

**Translated Data Packet**

Translate Src IP To: Untranslated

Translate Dst IP To: IP Address

IP Address: 20.20.20.1

Translate Port To: Usually internal server port

**To make NAT policy work, please configure local ACL or application control policy.**

Allow:  Add ACL policy automatically  Add ACL policy manually

Save and Copy Save Cancel

**Src Zone:** Zone where data transmission is initiated. Normally, it is a WAN area.

**Src Address:** IP addresses or IP range of users who need to access the server. Normally it is "All".

**Destination:** Public IP address or Public IP group used to access the server. The public IP need to be configured in WAN interface.

**Service:** Service is used when users from WAN access to the internal server. It



can be changed manually according to the need.

**Translate Dst IP To:** The options include **IP Address**, **IP range**, **Network Objects** and **Unchanged**. Normally, **IP Address** is chosen and it can be changed manually.

**IP Address:** IP address of the internal server.

**Translate Port To:** This option is used to translate port to the actual port that the server provides service. Leave it empty if the port same as **Service** you selected.

## 4.3 Bidirectional NAT

Requirements: Intranet users want to access internal server via public IP address.

Explanations for configuration:

- Step 1.** Ensure that the direction of data flow which needs address translation is correct.
- Step 2.** Go to **Policies > NAT**, then click **Add** button and choose type as **Bidirectional NAT** to define new BNAT.

**Add NAT Policy** X

Type:  Source NAT  Destination NAT  Bidirectional NAT

**Basics**

Name:

Status:  Enabled  Disabled

Description:

Move To:  ⓘ

Schedule:

**Original Data Packet**

Src Zone:

Src Address:

Destination:  IP Address  Network Objects

ⓘ

Services:

**Translated Data Packet**

Translate Src IP To:

Translate Dst IP To:

IP Address:

Translate Port To:

ⓘ To make NAT policy work, please configure local ACL or application control policy.

Allow:  Add ACL policy automatically  Add ACL policy manually

**Src Zone:** Zone where the users need to access the internal server.

**Src Address:** IP address or the IP range of the users that need to access the internal server.

**Destination:** IP address or Network Object of internal server that needed to be accessed.

**Service:** Service is used when users from WAN access to the internal server. It can be changed manually according to the need.

**Translation Src IP To:** To specify the outgoing interface's IP address that the intranet users' IP addresses would be translated to. Normally, it is configured to "Egress interface".

**Translate Dst IP To:** The options include **IP Address**, **IP range**, **Network Objects** and **Unchanged**. Normally, **IP Address** is chosen and it can be changed manually.

**IP Address:** IP address of internal server.

**Translate Port To:** This option is used to translate port to the actual port that the server provides service. Leave it empty if the port same as **Service** you selected.

## 5 Precautions

1. NGAF must be able to communicate with the server's port but not only able to ping the server.
2. Ensure that the ISP does not block the port of the server. It could be verified by capturing request packets from testing source IP at WAN interface.
3. Bidirectional NAT will translate both the source and destination IP, therefore the filtering rule when capturing packets at server zone can only be server's IP address.
4. Ensure that NGAF device can access Internet and access policy must allow.
5. Intranet PC must be able to access NGAF's LAN interface.

