



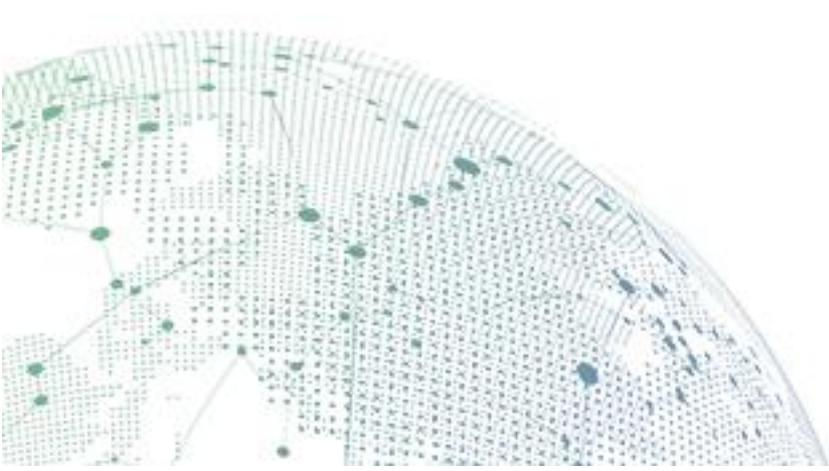
**SANGFOR**



# **NGAF**

## **Route Mode Deployment Guide**

Version 8.0.35



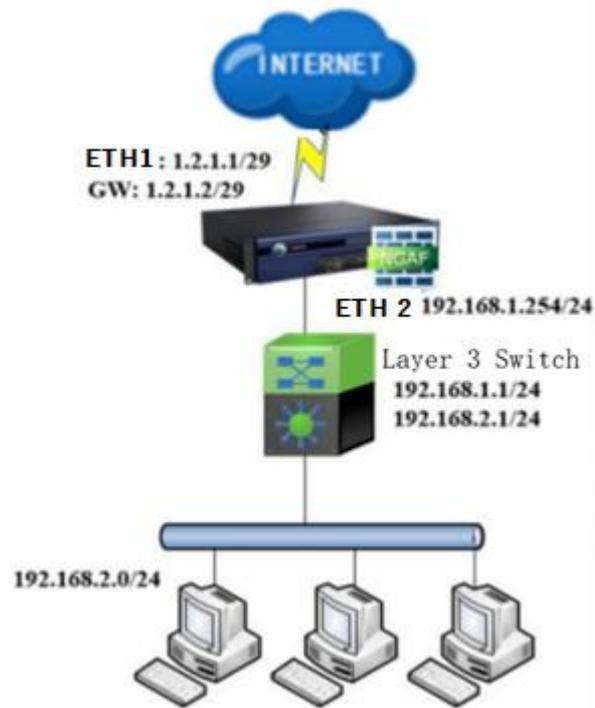
## Change Log

Date	Change Description
14/6/2021	Update document to NGAF v8035

## Contents

<b>Chapter 1 Applicable Scenario</b>	<b>4</b>
<b>Chapter 2 Configuration Steps</b>	<b>5</b>
2.1 Configure Interfaces and Zone .....	5
2.2 Configure Route .....	7
2.2.1 Configure Default Route	7
2.3 NAT Configuration .....	8
2.4 Access Control .....	10
2.5 Result .....	11

# Chapter 1 Applicable Scenario



This deployment is suitable for those environments which require Sangfor NGAF to be deployed as a network gateway or to replace a gateway router.

# Chapter 2 Configuration Steps

## 2.1 Configure Interfaces and Zone

### 1. Zone Configuration:

Access **Network > Zones** to add or modify the zone configuration.

Name: WAN / LAN

Forward Mode: Route (Layer 3)

<input type="checkbox"/>	Name	Type	Interfaces	In Use	Operation	...
<input checked="" type="checkbox"/>	WAN	Layer 3	eth1	In use	Edit Delete	
<input checked="" type="checkbox"/>	LAN	Layer 3	eth2	In use	Edit Delete	
<input type="checkbox"/>	L2_WAN	Layer 2	-	None	Edit Delete	
<input type="checkbox"/>	L2_LAN	Layer 2	-	None	Edit Delete	
<input type="checkbox"/>	L3_MGT	Layer 3	-	None	Edit Delete	
<input type="checkbox"/>	VW_WAN	Virtual wire	-	None	Edit Delete	

**Edit Zone** ×

Name:

Type:  Layer 2  Layer 3  Virtual wire

**Interfaces**

Available (2)	Selected (1)
<input type="checkbox"/> eth0	<input type="checkbox"/> eth0
<input type="checkbox"/> vptun	<input type="checkbox"/> vptun
<input checked="" type="checkbox"/> eth1	<input checked="" type="checkbox"/> eth1

**Edit Zone** ×

Name:

Type:  Layer 2  Layer 3  Virtual wire

**Interfaces**

Available (2)	Selected (1)
<input type="checkbox"/> eth0	<input type="checkbox"/> eth0
<input type="checkbox"/> vptun	<input type="checkbox"/> vptun
<input checked="" type="checkbox"/> eth2	<input checked="" type="checkbox"/> eth2

2. Access to **Network > Interfaces** to configure eth 1 and eth2 as WAN and LAN interface as figure shown below:

**Edit Physical Interface** ✕

**Basics**

Name: eth1

Status:  Enabled  Disabled

Description: Optional

Type: Layer 3

Zone: WAN

Basic Attributes:  WAN attribute

System Upgrade:  Temporarily use this interface for system upgrade ⓘ

---

**IPv4** | IPv6 | Link State Detection | Advanced

IP Assignment:  Static  DHCP  PPPoE

Static IP: 192.200.19.185/24 ⓘ

Next-Hop IP: 192.200.19.1 ⓘ

Link Bandwidth: Outbound 1024 Mbps Inbound 1024 Mbps

**Management Service**

Allow:  WEBUI  PING  SNMP  SSH

## Edit Physical Interface



### Basics

Name: eth2

Status:  Enabled  Disabled

Description: Optional

Type: Layer 3

Zone: LAN

Basic Attributes:  WAN attribute

System Upgrade:  Temporarily use this interface for system upgrade

IPv4 IPv6 Link State Detection Advanced

IP Assignment:  Static  DHCP  PPPoE

Static IP: 192.168.1.1/24

Next-Hop IP:

Link Bandwidth: Outbound 1000 Mbps Inbound 1000 Mbps

### Management Service

Allow:  WEBUI  PING  SNMP  SSH

Save Cancel

## 2.2 Configure Route

### 2.2.1 Configure Default Route

1. Access to **Network > Routes > Static Routes**. Click **Add** to add new default route in NGAF as shown in figure below:

### Add Static Route



Add:  One Route  Multiple Routes

Protocol:  IPv4  IPv6

Basics

Status:  Enabled  Disabled

Description: Optional

Details

Dst IP/Netmask: 0.0.0.0/0.0.0.0

Next-Hop IP: 192.200.19.1

Interface: eth1

Advanced

Link State Detection :  Enable  Disable

Metric: 0

Save and Add Save Cancel

## 2.2.2 Configure Return Route

Return Route for 192.168.2.0/24 Segment

1. Access to **Network** > **Routes** > **Static Routes**. Click **Add** to add new return route in NGAF as shown in figure below:

### Add Static Route ✕

Add:  One Route  Multiple Routes

Protocol:  IPv4  IPv6

**Basics**

Status:  Enabled  Disabled

Description:

**Details**

Dst IP/Netmask:  ⓘ

Next-Hop IP:  ⓘ

Interface:  ⓘ

**Advanced**

Link State Detection ⓘ:  Enable  Disable

Metric:

## 2.3 NAT Configuration

1. Go to **Policies** > **NAT**. Click **Add** and select **Source NAT** to configure SNAT for internal device access internet as image shown below:

## Edit NAT Policy

✕



Type:  Source NAT  Destination NAT  Bidirectional NAT

### Basics

Name:

Status:  Enabled  Disabled

Description:

Schedule:

### Original Data Packet

Src Zone:

Src Address:

Dst Zone/Interface:  Zone  Interface

Dst Address:

Services:

### Translated Data Packet

Translate Src IP To:

Translate Dst IP To:

Translate Dst Port To:

Save

Cancel

## 2.4 Access Control

Configure application control policy to allow the internal to access internet.

1. Go to Policies > Access control > Application control to configure an allow policy as figure shown below:

### Edit Application Control Policy ×

**Basics**

Name:

Status:  Enabled  Disabled

Description:

Policy Group:

Tag:

**Source**

Src Zone:

Src Address:  Network Objects  User/Group

**Destination**

Dst Zone:

Dst Address:

Services:

Applications:

**Others**

Action:  Allow  Deny

### NOTICE

By default, NGAF pre configured an Application Control policy to deny all the service and user need to manually to allow the certain service. User can configure other policy based on their needs as well.

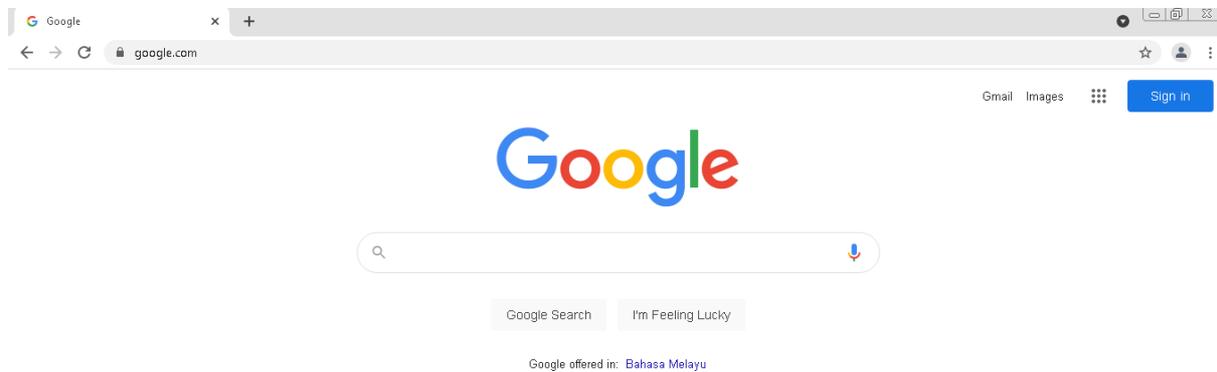
## 2.5 Result

1. Access to one of the PC to do some ping test and use browser to access website.

```
C:\Users\...>ping google.com

Pinging google.com [172.217.31.46] with 32 bytes of data:
Reply from 172.217.31.46: bytes=32 time=20ms TTL=117
Reply from 172.217.31.46: bytes=32 time=20ms TTL=117
Reply from 172.217.31.46: bytes=32 time=20ms TTL=117
Reply from 172.217.31.46: bytes=32 time=19ms TTL=117

Ping statistics for 172.217.31.46:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 19ms, Maximum = 20ms, Average = 19ms
```





Copyright © SANGFOR Technologies Inc. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of SANGFOR Technologies Inc.

SANGFOR is the trademark of SANGFOR Technologies Inc. All other trademarks and trade names mentioned in this document are the property of their respective holders. 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