



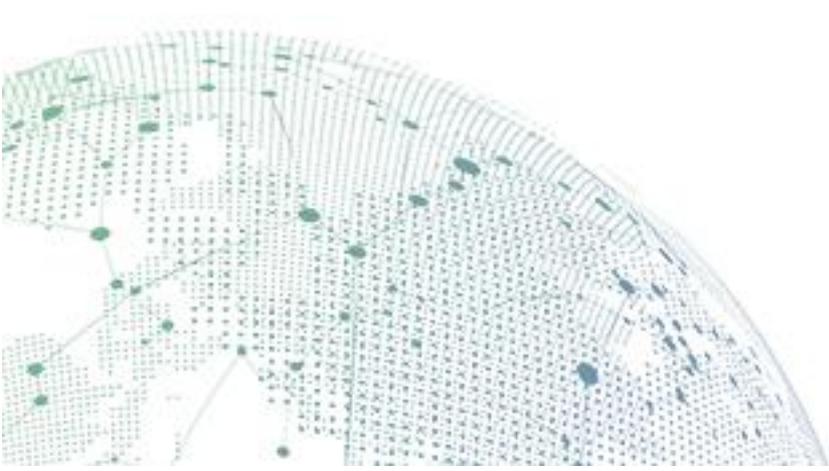
SANGFOR



NGAF

Route Mode Deployment Guide

Version 8.0.5



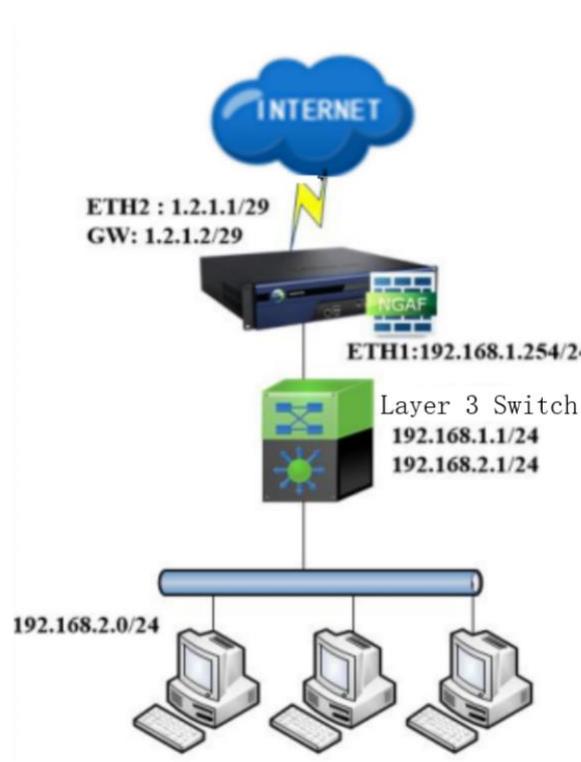
Change Log

Date	Change Description

CONTENT

Chapter 1 Applicable Scenario	4
Chapter 2 Configuration Steps	5
2.1 Configure Interfaces and Zone	5
2.2 Configure Route	8
2.3 NAT Configuration.....	9
2.4 Access Control.....	10

Chapter 1 Applicable Scenario



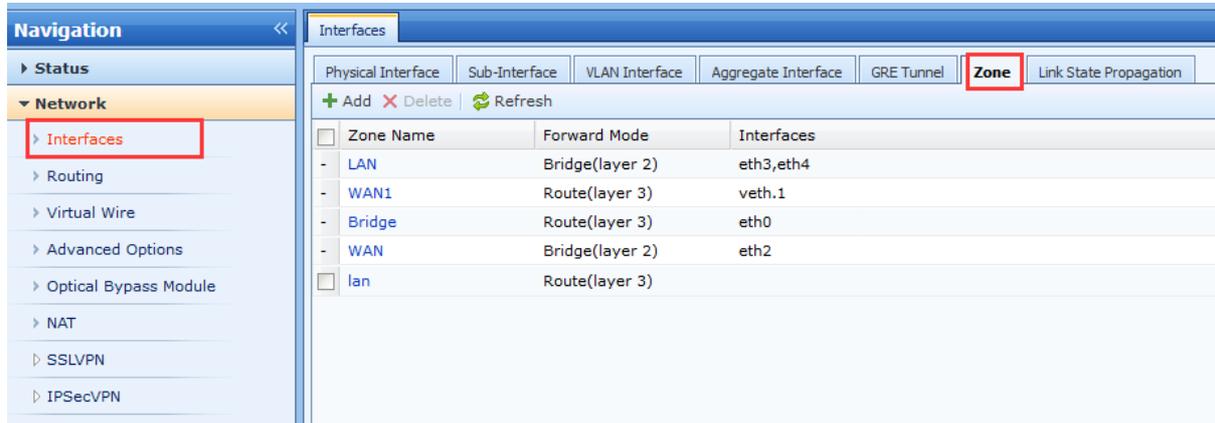
This deployment is suitable for those environments which require Sangfor NGAF to be their gateway or router.

Chapter 2 Configuration Steps

2.1 Configure Interfaces and Zone

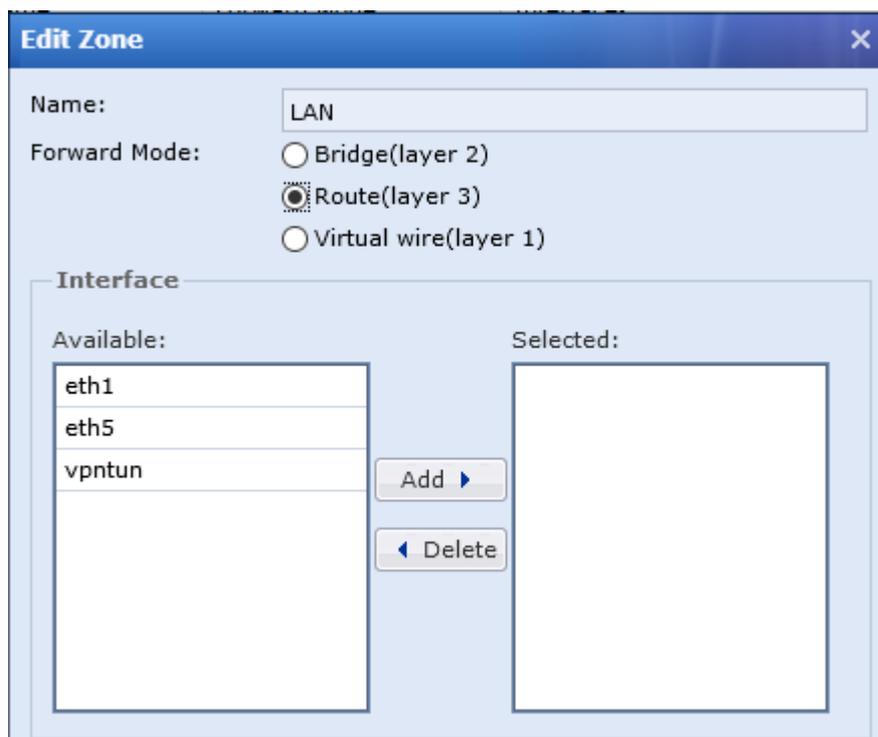
1. Interface / Zone Configuration:

Modify "Network" → "Zone or Interface" → "Add" to add or modify the zone and interface configuration.

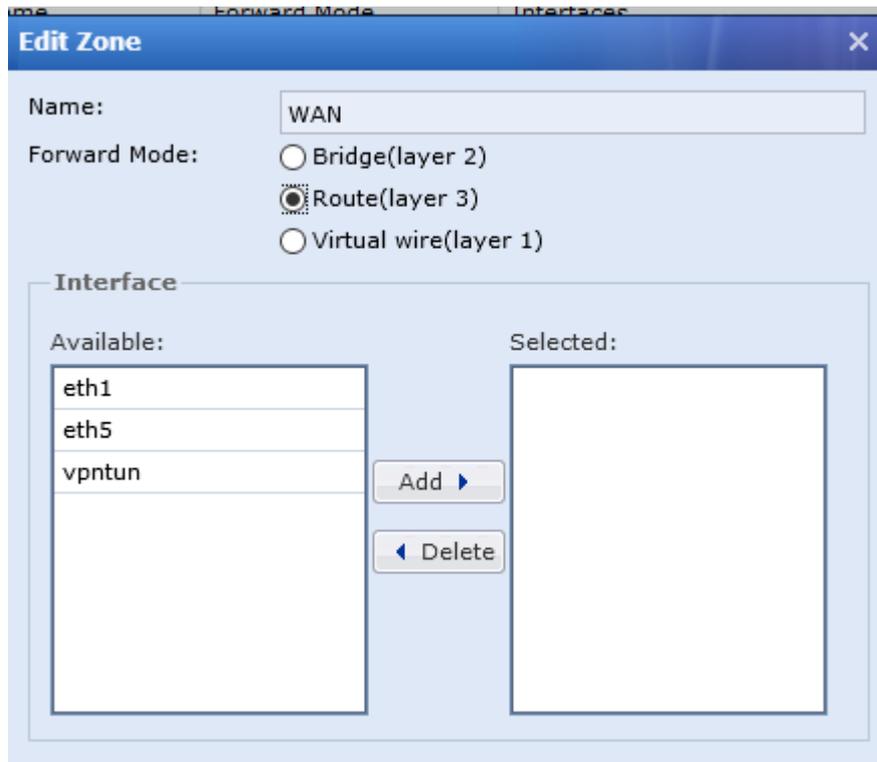


The screenshot shows a network configuration interface. On the left is a navigation pane with a tree view under 'Network'. The 'Interfaces' item is highlighted with a red box. The main area is titled 'Interfaces' and has several tabs: 'Physical Interface', 'Sub-Interface', 'VLAN Interface', 'Aggregate Interface', 'GRE Tunnel', 'Zone', and 'Link State Propagation'. The 'Zone' tab is selected and highlighted with a red box. Below the tabs are '+ Add', 'X Delete', and a refresh icon. A table lists existing zones:

Zone Name	Forward Mode	Interfaces
- LAN	Bridge(layer 2)	eth3,eth4
- WAN1	Route(layer 3)	veth.1
- Bridge	Route(layer 3)	eth0
- WAN	Bridge(layer 2)	eth2
<input type="checkbox"/> lan	Route(layer 3)	



The 'Edit Zone' dialog box is shown. It has a title bar with 'Edit Zone' and a close button. The 'Name' field contains 'LAN'. The 'Forward Mode' section has three radio buttons: 'Bridge(layer 2)', 'Route(layer 3)' (which is selected), and 'Virtual wire(layer 1)'. Below this is an 'Interface' section with two lists: 'Available:' and 'Selected:'. The 'Available:' list contains 'eth1', 'eth5', and 'vpntun'. There are 'Add' and 'Delete' buttons between the two lists.



Name: WAN / LAN

Forward Mode: Route (Layer 3)

2. Modify "Network" → "Zone or Interface" → "Add" to add or modify the zone and interface configuration

Configure eth 1 as LAN interface, make it pingable and assign an IP for it.

Edit Physical Interface

Enable

Name: eth1
Description:
Type: Route(layer 3)
Added To Zone: lan
Basic Attributes: Pingable
 WAN attribute
 IPSec VPN outgoing line: Line 1

IPv4

Static DHCP PPPoE

Static IP: 192.168.1.254/24
Next-Hop IP:

Configure eth 2 as WAN interface, make it pingable, WAN attribute and assign an IP for it.

Edit Physical Interface

Enable

Name: eth2
Description: abc
Type: Route(layer 3)
Added To Zone: lan
Basic Attributes: Pingable
 WAN attribute
 IPSec VPN outgoing line: Line 1

IPv4

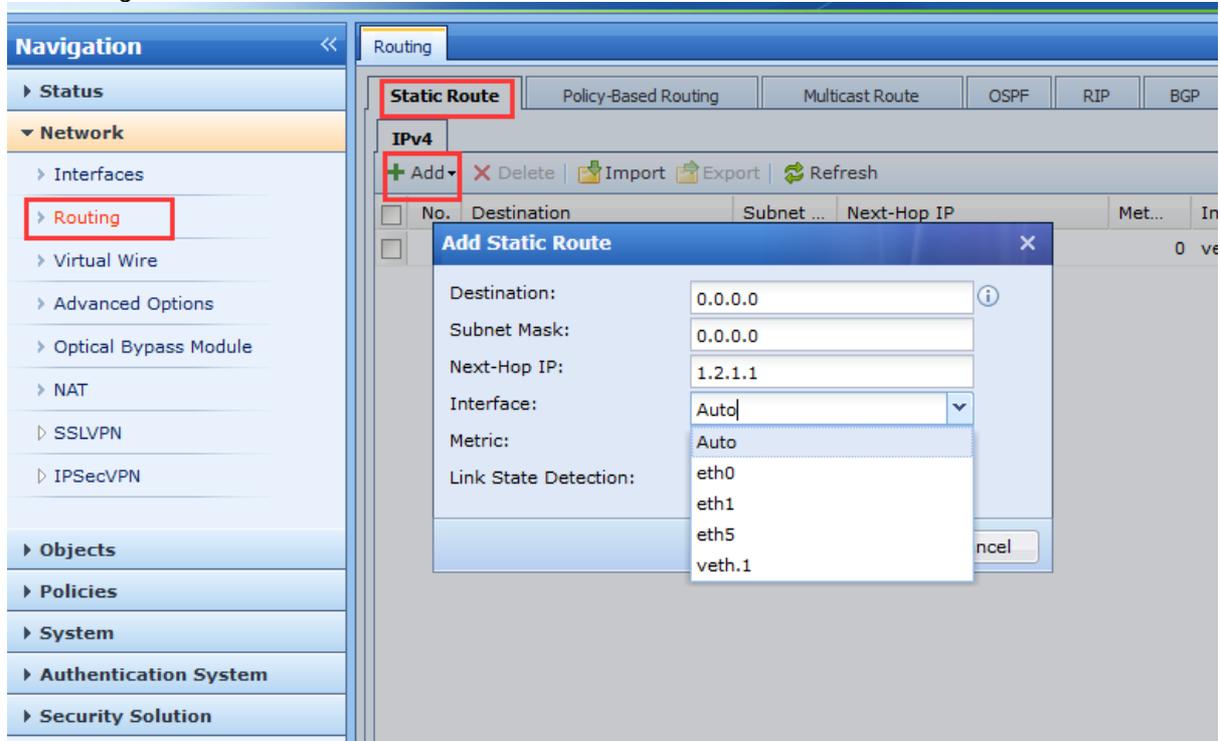
Static DHCP PPPoE

Static IP: 1.2.1.1/29
Next-Hop IP: 1.2.1.2

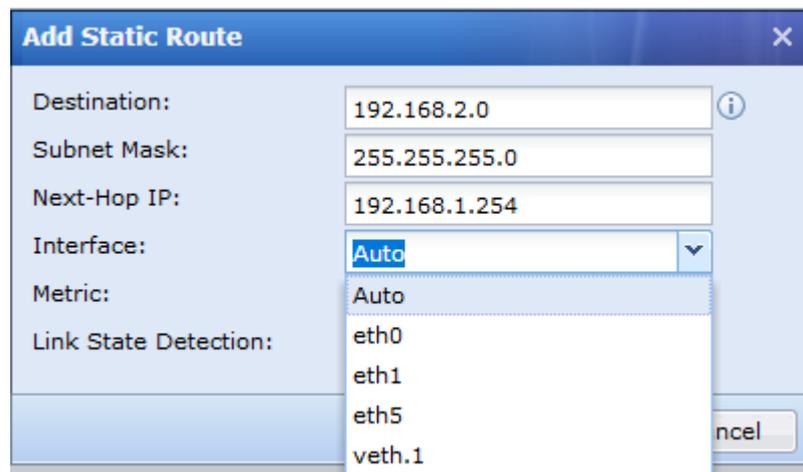
2.2 Configure Route

Default Route

1. Configure "Network" → "Route" → "Static Route" → "Add" → "Static Route",

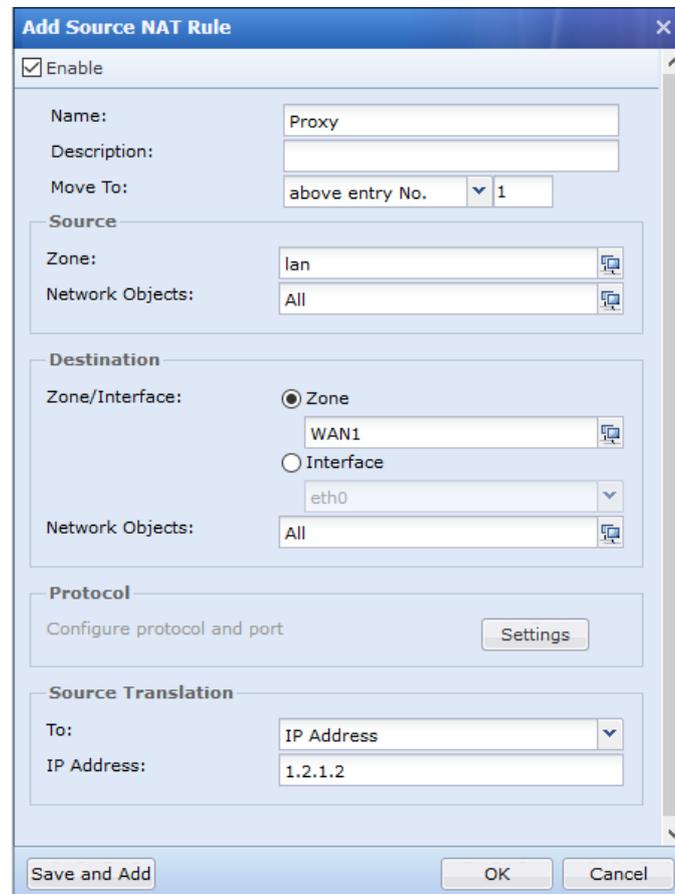


Static Route for Packets coming back



2.3 NAT Configuration

1. Configure "Firewall" → "NAT" → "Add" → "SNAT". As image shown below:



The screenshot shows the "Add Source NAT Rule" configuration window. The window is titled "Add Source NAT Rule" and has a close button (X) in the top right corner. It contains several sections for configuring the rule:

- Enable:** A checked checkbox labeled "Enable".
- Name:** A text field containing "Proxy".
- Description:** An empty text field.
- Move To:** A dropdown menu showing "above entry No." and a value of "1".
- Source:**
 - Zone:** A dropdown menu showing "lan".
 - Network Objects:** A dropdown menu showing "All".
- Destination:**
 - Zone/Interface:** Radio buttons for "Zone" (selected) and "Interface".
 - Zone/Interface:** A dropdown menu showing "WAN1" (under "Zone") and "eth0" (under "Interface").
 - Network Objects:** A dropdown menu showing "All".
- Protocol:** A section with the text "Configure protocol and port" and a "Settings" button.
- Source Translation:**
 - To:** A dropdown menu showing "IP Address".
 - IP Address:** A text field containing "1.2.1.2".

At the bottom of the window, there are three buttons: "Save and Add", "OK", and "Cancel".

2.4 Access Control

Edit Application Control Policy

Enable

Name:

Group:

Source

Network Objects/Users: Network Objects

User/Group

Zone:

Port: All
 Specified Port ⓘ

Destination

Network Objects:

Zone:

Service/Application

Service/Application: Service

Application

Schedule:

Action: Allow Deny

Advanced Settings: [Settings](#)

Remark:

OK Cancel

Attention: Default Access Control policy will deny all the service by default and user need to configure manually to allow the service. User can configure other policy based on their needs as well.



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