



NGAF

Mix Mode Deployment Guide

Version 8.0.5

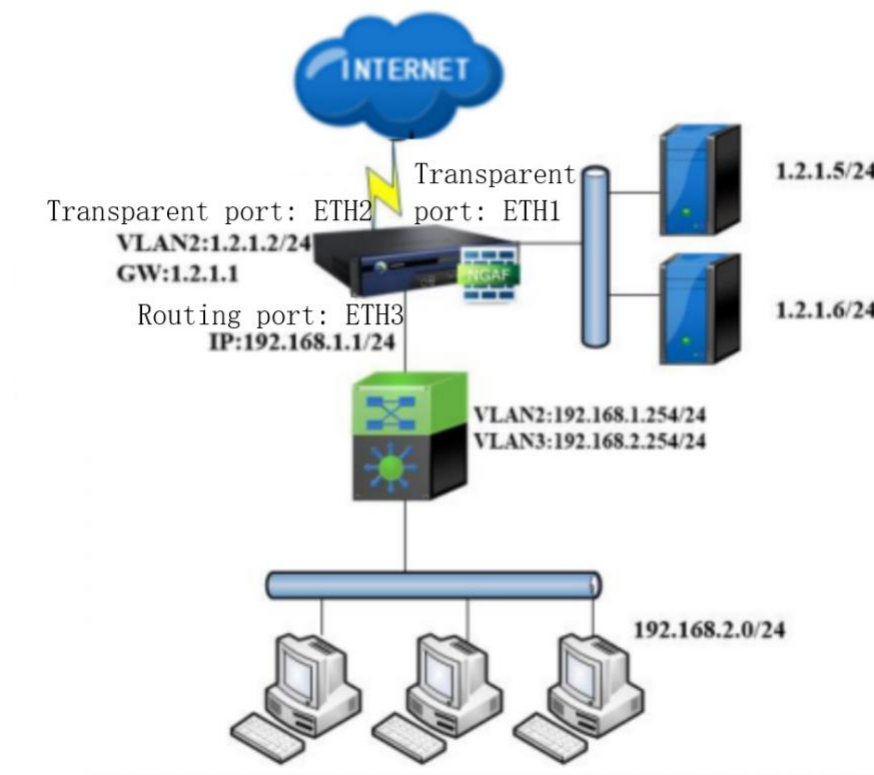
Change Log

Date	Change Description
	Version 8.0.5 document release.

CONTENT

Chapter 1 Applicable Scenario	4
Chapter 2 Configuration Steps	5
2.1 Configure Interfaces and Zone	5
2.2 Configure Route	11
2.3 NAT Configuration.....	12
2.4 Access Control.....	13

Chapter 1 Applicable Scenario



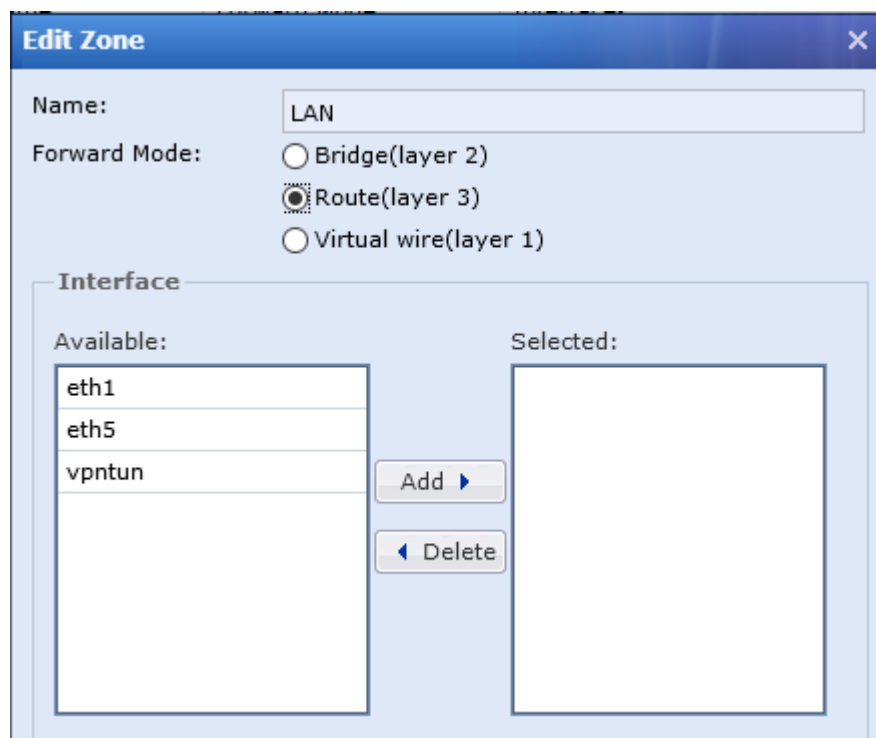
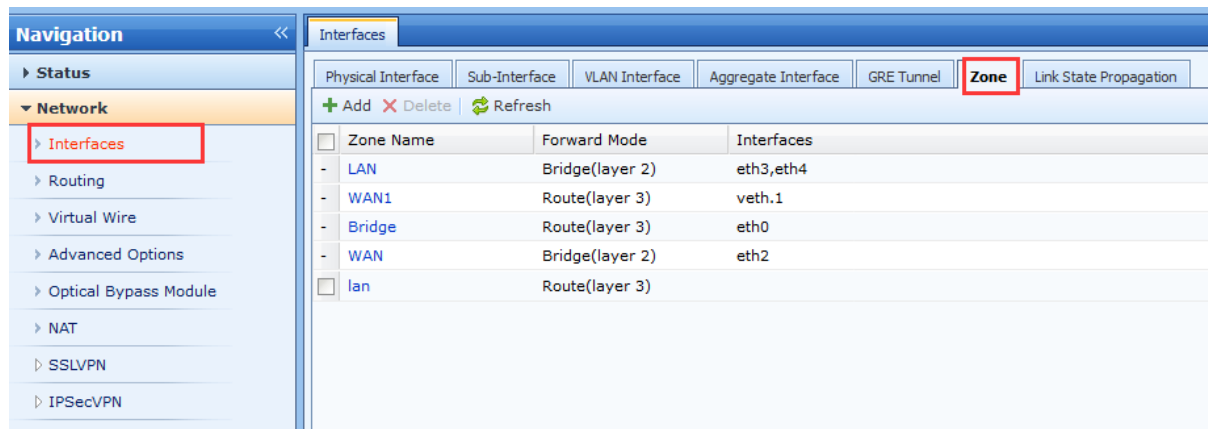
Configure SANGFOR NGAF WAN port as route mode, LAN use proxy to access internet, Intranet will provide public IP for users and servers. To allow user to access server by using public IP to access server farm, not using port mapping.

Chapter 2 Configuration Steps

2.1 Configure Interfaces and Zone

1. Interface / Zone Configuration:

Modify "Network" → "Interfaces" → "Zone" → "Add", to add zone and physical interface correspondingly,



Edit Zone [X]

Name:

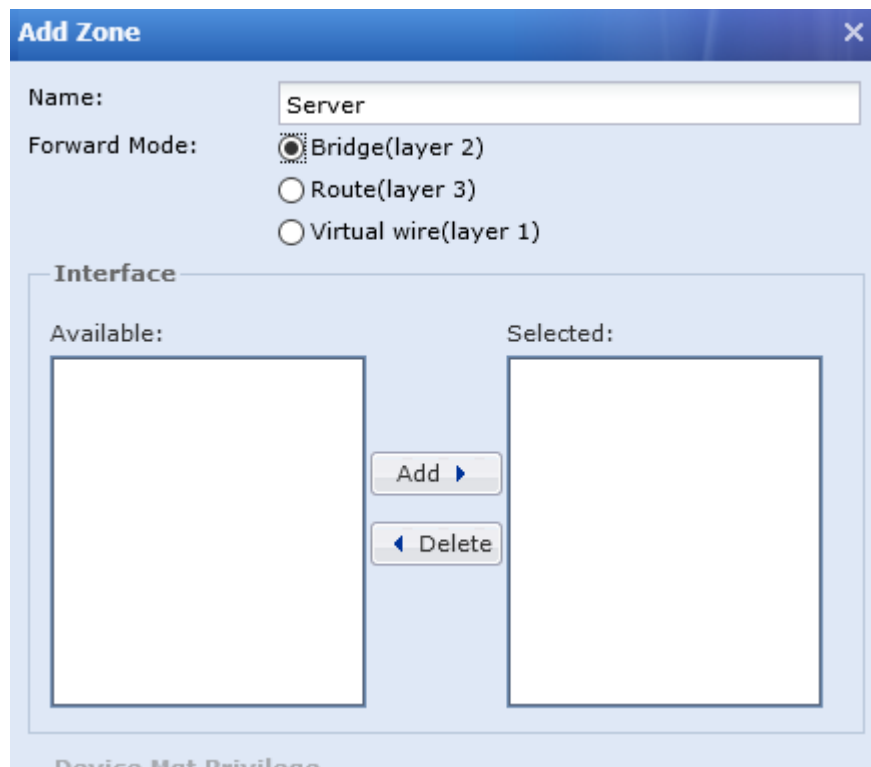
Forward Mode: ☐ Bridge(layer 2)
☒ Route(layer 3)
☐ Virtual wire(layer 1)

Interface

Available:		Selected:
eth1	<input type="button" value="Add >"/> <input type="button" value="Delete <"/>	
eth5		
vpntun		

Name: WAN / LAN

Forward Mode: Route (Layer 3)



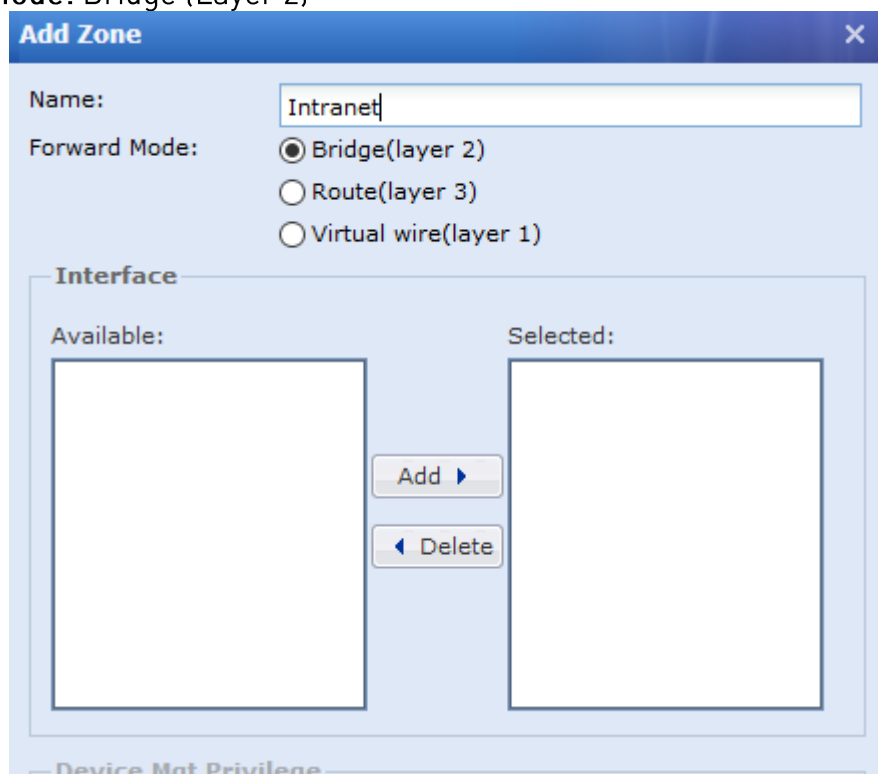
The image shows a Windows-style dialog box titled "Add Zone" with a close button (X) in the top right corner. It contains the following fields and options:

- Name:** A text input field containing the word "Server".
- Forward Mode:** Three radio button options:
 - ☒ Bridge(layer 2)
 - ☐ Route(layer 3)
 - ☐ Virtual wire(layer 1)
- Interface:** A section containing two empty rectangular boxes labeled "Available:" and "Selected:". Between these boxes are two buttons: "Add ►" and "◄ Delete".

At the bottom of the dialog, there is a faint label "Device Not Privileged".

Name: Server

Forward Mode: Bridge (Layer 2)



The image shows a second instance of the "Add Zone" dialog box. It contains the following fields and options:

- Name:** A text input field containing the word "Intranet".
- Forward Mode:** Three radio button options:
 - ☒ Bridge(layer 2)
 - ☐ Route(layer 3)
 - ☐ Virtual wire(layer 1)
- Interface:** A section containing two empty rectangular boxes labeled "Available:" and "Selected:". Between these boxes are two buttons: "Add ►" and "◄ Delete".

At the bottom of the dialog, there is a faint label "Device Not Privileged".

Name: Intranet

Forward Mode: Bridge (Layer 2)

2. Configure "Network" → "Interfaces" → "Physical Interface", click the interface which will be your intranet interface for example eth 2. As image shown below:

The screenshot shows the 'Edit Physical Interface' window for interface 'eth2'. The window has a title bar with a close button. Below the title bar is a section with a checked 'Enable' checkbox. The main configuration area includes fields for 'Name' (eth2), 'Description' (abc), 'Type' (Bridge(layer 2)), and 'Added To Zone' (Intranet). There is a 'Basic Attributes' section with a 'WAN attribute' checkbox. Below this is a tabbed interface with 'IPv4/IPv6' selected. The 'Access' tab is active, showing radio buttons for 'Access' (selected) and 'Trunk'. Below the radio buttons is a field for 'Access' with the value '2' and a label 'VLAN Interface'.

3. Configure "Network" → "Interfaces" → "Physical Interface", click the interface which will be your server interface for example eth 1. As image shown below:

The screenshot shows the 'Edit Physical Interface' window for interface 'eth1'. The window has a title bar with a close button. Below the title bar is a section with a checked 'Enable' checkbox. The main configuration area includes fields for 'Name' (eth1), 'Description' (empty), 'Type' (Bridge(layer 2)), and 'Added To Zone' (Server). There is a 'Basic Attributes' section with a 'WAN attribute' checkbox. Below this is a tabbed interface with 'IPv4/IPv6' selected. The 'Access' tab is active, showing radio buttons for 'Access' (selected) and 'Trunk'. Below the radio buttons is a field for 'Access' with the value '2' and a label 'VLAN Interface'.

4. Configure "Network" —> "Interfaces" —> "Physical Interface", click the interface which will be your LAN interface for example eth 3. As image shown below:

The screenshot shows the 'Edit Physical Interface' configuration window for interface 'eth3'. The window has a blue header bar with the title 'Edit Physical Interface' and a close button (X). Below the header, there is a section with a checked 'Enable' checkbox. The main configuration area is divided into several sections:

- Name:** eth3
- Description:** (empty text field)
- Type:** Route(layer 3) (dropdown menu)
- Added To Zone:** lan (dropdown menu)
- Basic Attributes:**
 - ☒ Pingable
 - ☐ WAN attribute
 - ☐ IPsec VPN outgoing line: Line 1 (dropdown menu with an info icon)

Below the basic attributes, there is a tabbed interface with the 'IPv4' tab selected. Inside the IPv4 tab, there are three radio buttons: 'Static' (selected), 'DHCP', and 'PPPoE'. Below these, there is a section for static IP configuration:

- Static IP:** 192.168.1.1/24 (text field with an info icon)
- Next-Hop IP:** (empty text field with an info icon)

At the bottom of the window, there is a section titled 'Line Bandwidth' with two rows:

- Outbound:** 1024 Mbps (text field with a dropdown arrow)
- Inbound:** 1024 Mbps (text field with a dropdown arrow)

5. Configure "Network"—>"Interfaces"—>"Physical Interface", click the interface which will be your LAN interface for example eth 3. As image shown below:

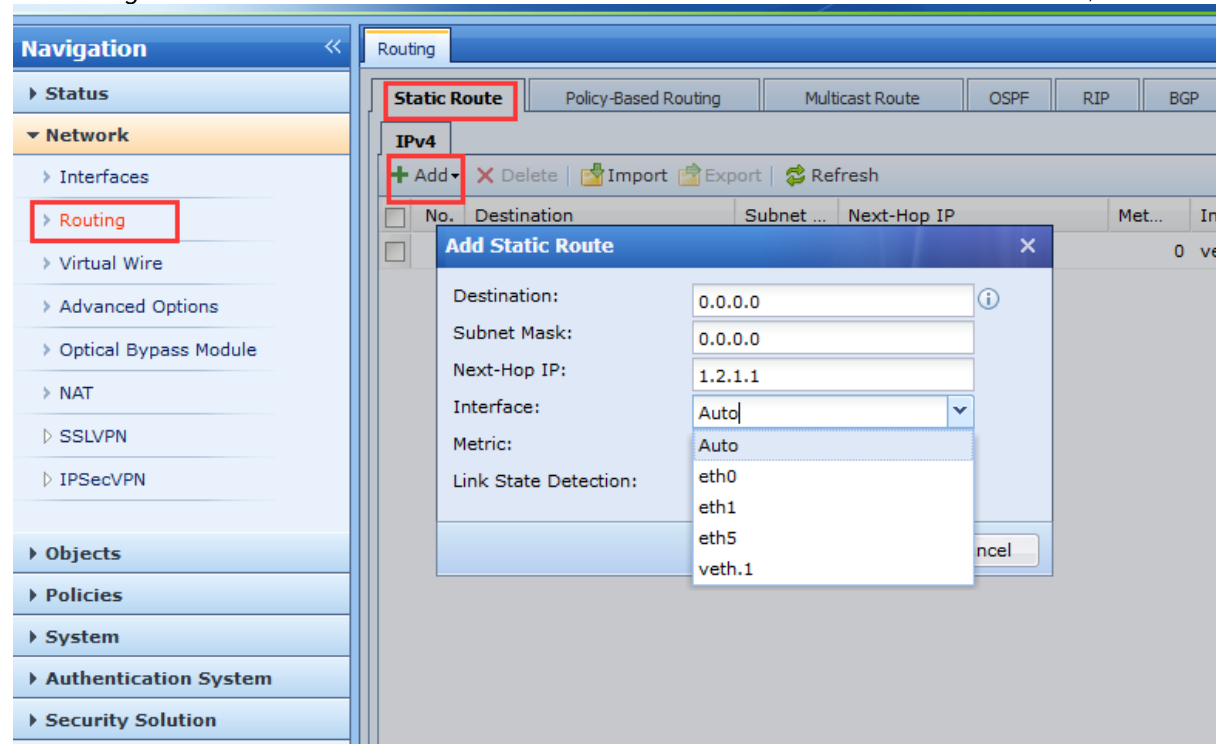
The screenshot shows the 'Add VLAN Interface' configuration window. The fields are as follows:

- Name:** Veth. 2
- Description:** (empty)
- Added To Zone:** WAN1
- Basic Attributes:**
 - ☒ Pingable
 - ☐ IPsec VPN outgoing line: Line 1
- IP Assignment:** Static (selected), DHCP (unselected)
- Static IP:** 1.2.1.2/24
- Next-Hop IP:** 1.2.1.1
- Link State Detection:** Specify link state detection method(s). [Settings]

2.2 Configure Route

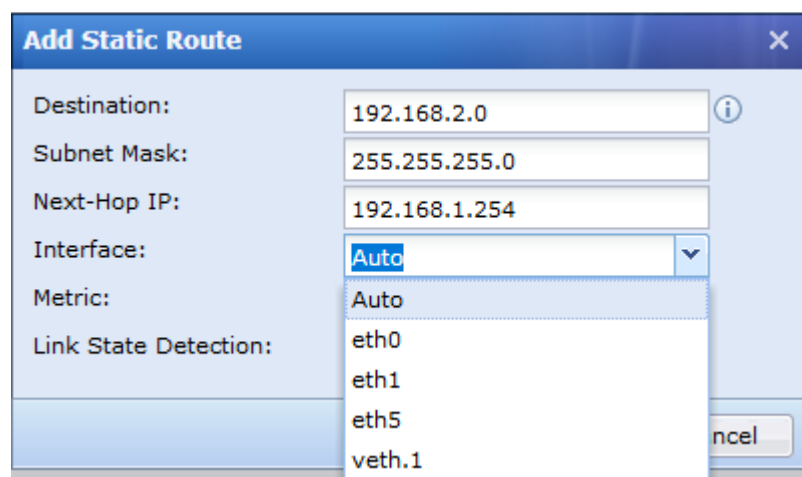
Default Route

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



This static route configuration will allow user's network environment to have a smooth and well in and out traffic flow.

Static Route for Packets coming back



This configuration is to allow packet to route back to user's environment with specified static route.

2.3 NAT Configuration

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

The screenshot shows the 'Add Source NAT Rule' dialog box. It has a title bar with a close button. The dialog is divided into several sections:

- Enable:** A checkbox labeled 'Enable' is checked.
- Name:** A text field containing 'Proxy'.
- Description:** An empty text field.
- Move To:** A dropdown menu showing 'above entry No.' and a text field with '1'.
- Source:**
 - Zone:** A dropdown menu showing 'lan'.
 - Network Objects:** A dropdown menu showing 'All'.
- Destination:**
 - Zone/Interface:** Two radio buttons: 'Zone' (selected) and 'Interface'. Below 'Zone' is a dropdown menu showing 'WAN1'. Below 'Interface' is a dropdown menu showing 'eth0'.
 - 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 dialog are three buttons: 'Save and Add', 'OK', and 'Cancel'.

SNAT configuration will allow network to route the packets to public.

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

Default Access Control policy will deny all the service 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