



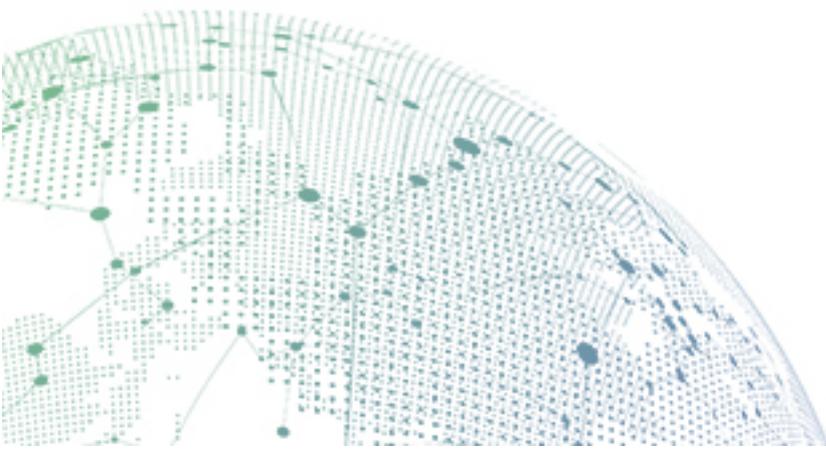
**SANGFOR**



# NGAF

## Transparent Mode Deployment Guide

Version 8.0.5



---

## Change Log

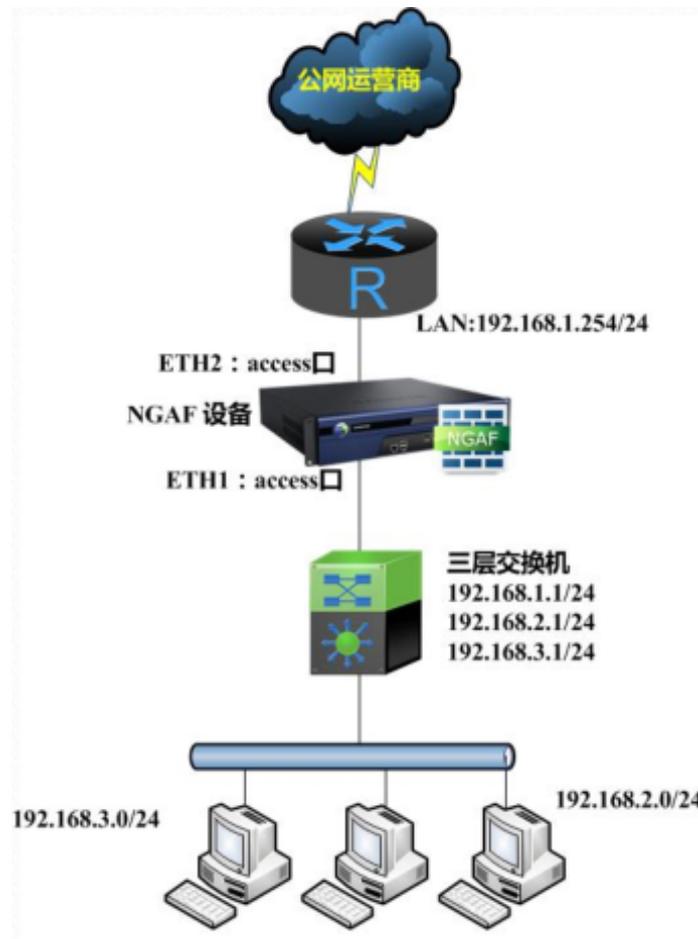
| Date            | Change Description              |
|-----------------|---------------------------------|
| October 9, 2018 | Version 8.0.5 document release. |
|                 |                                 |

---

# CONTENT

|                                       |    |
|---------------------------------------|----|
| Chapter 1 Applicable Environment..... | 4  |
| Chapter 2 Configuration Step .....    | 4  |
| Chapter 3 Precautions .....           | 12 |

# Chapter 1 Applicable Environment

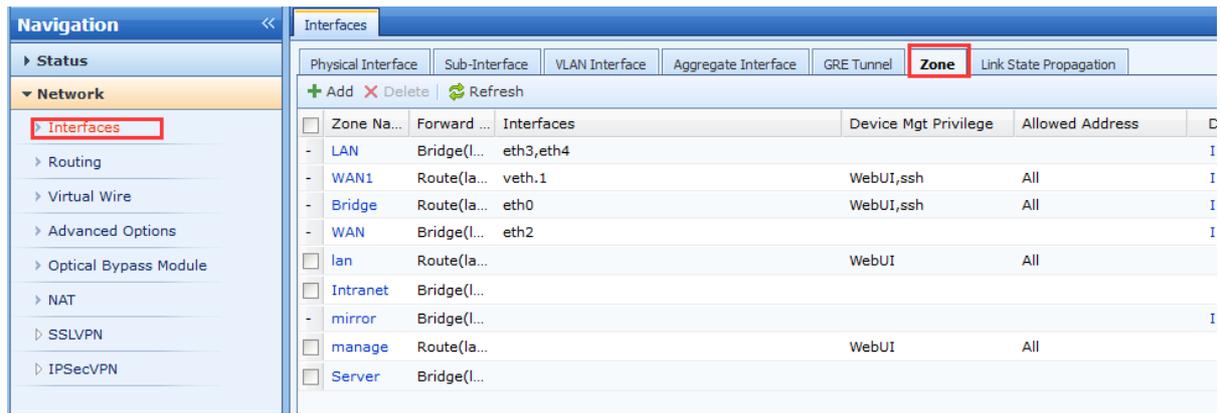


When user need to apply firewall and does not change their network environment.

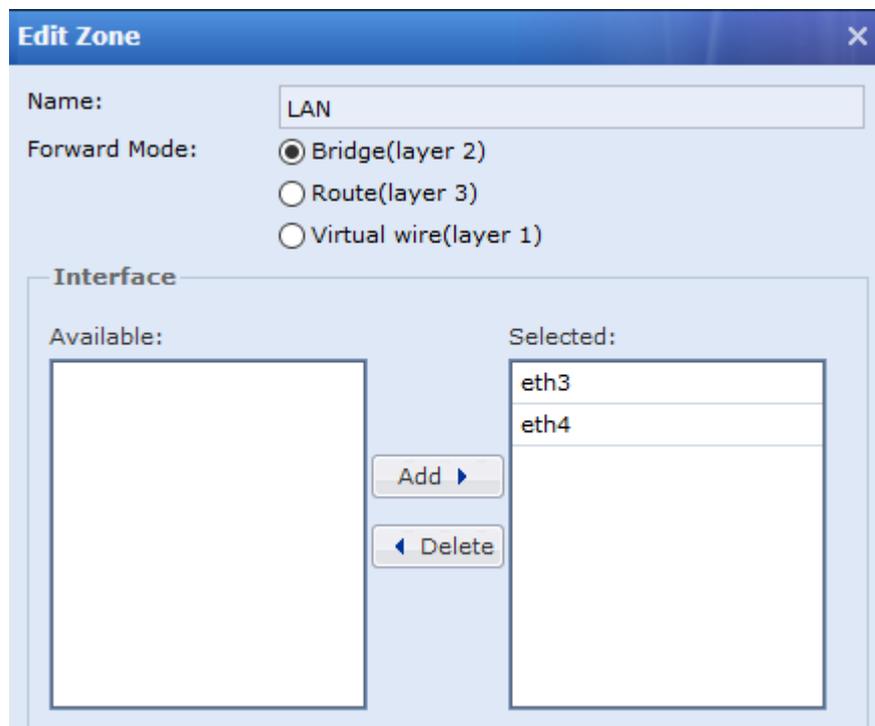
## Chapter 2 Configuration Step

### 2.1 Configure Zone for LAN, WAN and management

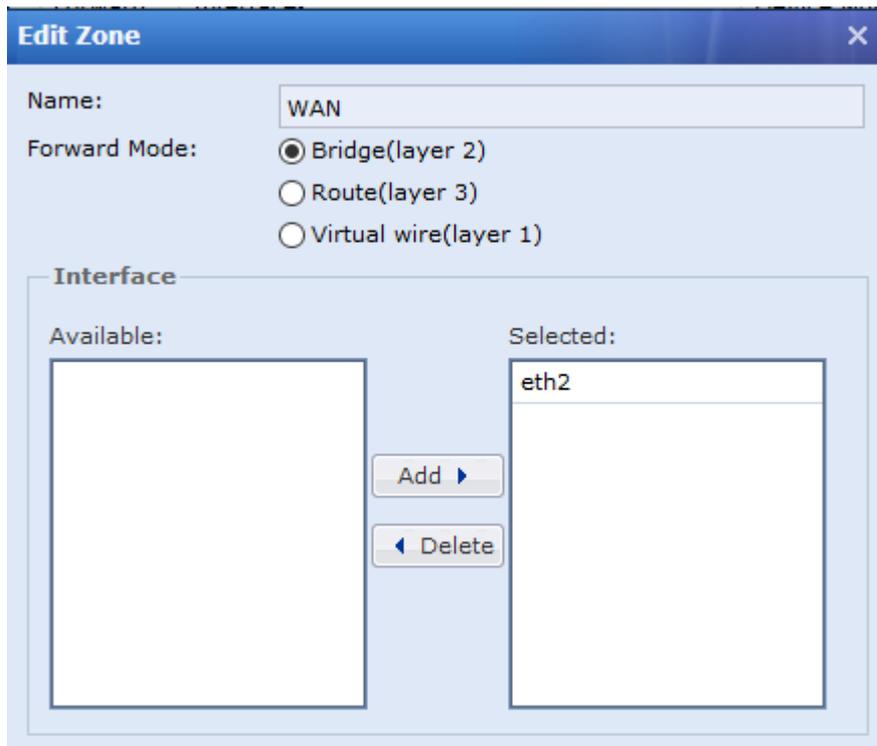
Go to [Network]→[Interfaces]-[Physical Interfaces]



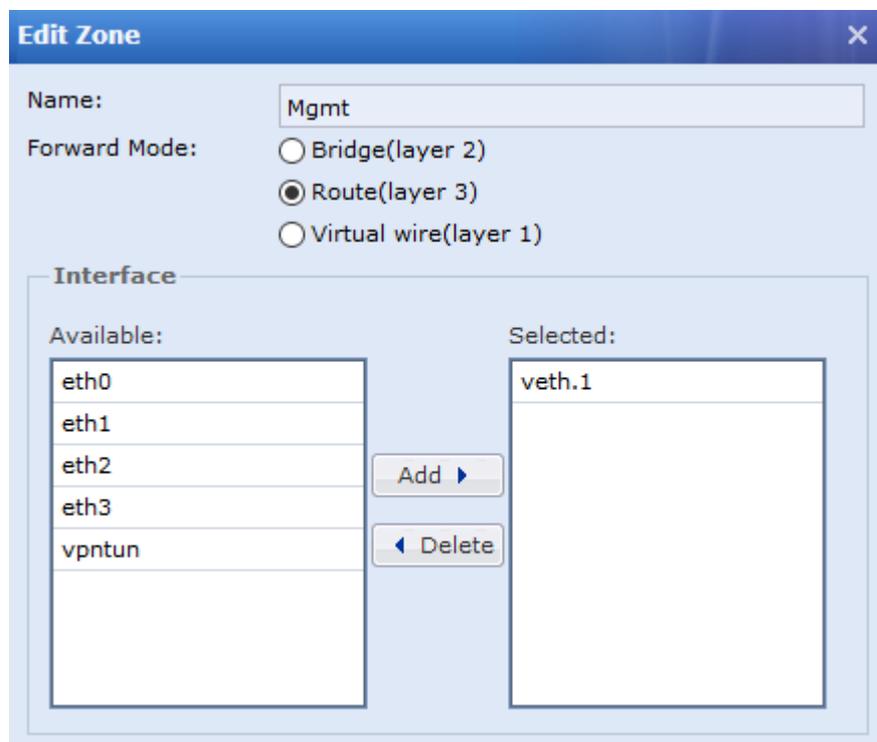
Configuration for LAN zone



Configuration for WAN zone



Configuration for Management zone



## 2.2 Interface Configuration

---

Go to [Network]→[Interfaces]-[Physical Interfaces].

Assign one interface for WAN attribute and WAN zone

**Edit Physical Interface** [X]

Enable

Name: eth5

Description: [ ]

Type: Bridge(layer 2) [v]

Added To Zone: WAN [v]

Basic Attributes:  WAN attribute

IPv4/IPv6

Access  Trunk

Access: 1  
VLAN Interface

**Advanced**  
Configure link mode, MTU and MAC address. [Settings]

[OK] [Cancel]

Assign another interface for LAN zone

**Edit Physical Interface** [X]

Enable

Name: eth4

Description: [Empty]

Type: Bridge(layer 2) [v]

Added To Zone: LAN [v]

Basic Attributes:  WAN attribute

IPv4/IPv6

Access  Trunk

Access: 1  
VLAN Interface

**Advanced**  
Configure link mode, MTU and MAC address. [Settings]

[OK] [Cancel]

## 2.3 VLAN Configuration

Create a VLAN interface and add to management zone

**Edit VLAN Interface** ✕

Name: Veth. 1 (i)

Description:

Added To Zone: Mgmt ▼

Basic Attributes:  Pingable  
 IPsec VPN outgoing line: Line 1 ▼ (i)

IP Assignment:  Static  DHCP

Static IP: 192.168.19.2/255.255.255.0 (i)

Next-Hop IP: 192.168.19.1

---

**Link State Detection**

Specify link state detection method(s). Settings

---

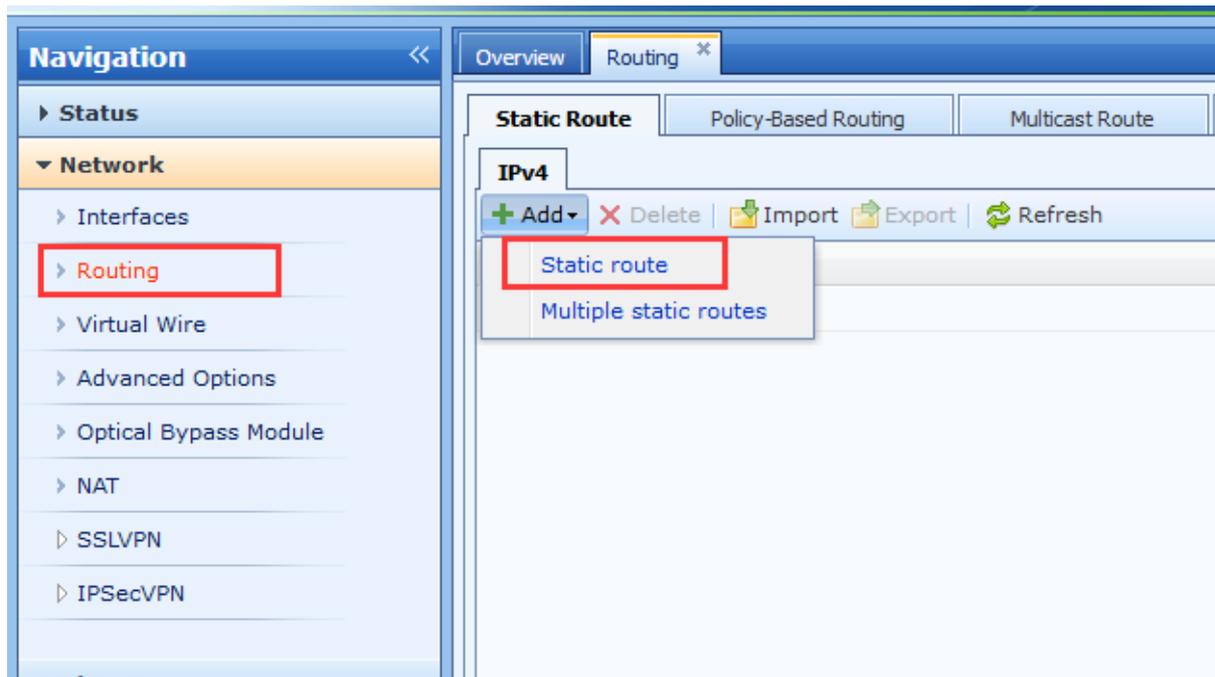
**Advanced**

Specify Maximum Transmission Unit (MTU). Settings

OK Cancel

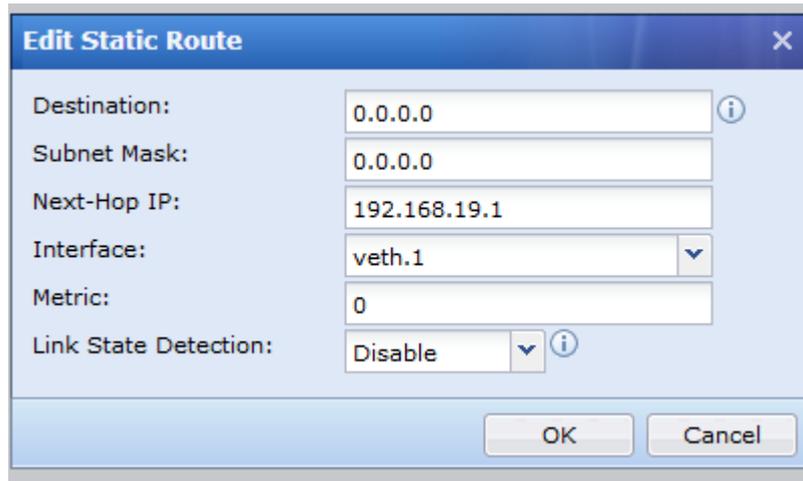
## 2.4 Routing Configuration

Configure it from [Network]→[Routing]→[Static Route]→[Add]→[Static Route] as image shown below:



Insert destination address, subnet mask, next hop IP and choose an interface for VLAN.

---



**Edit Static Route**

Destination: 0.0.0.0

Subnet Mask: 0.0.0.0

Next-Hop IP: 192.168.19.1

Interface: veth.1

Metric: 0

Link State Detection: Disable

OK Cancel

If you need other static route in your network then you can proceed it in the same section here as well.

## 2.5 Application Control Policy

**Navigation** <<

- ▶ Status
- ▶ Network
- ▶ Objects
- ▼ Policies
  - ▲ Access Control
    - ▶ **Application Control**
    - ▶ Country Blocking
    - ▶ Connection Control
  - ▲ Network Security
    - ▶ Policies
    - ▶ Anti-DoS/DDoS
    - ▶ ARP Spoofing Prevention
  - ▶ Decryption
  - ▶ Bandwidth Management
  - ▶ Configuration Wizard
  - ▶ Blacklist/Whitelist

Overview Application Control ✕

+ Add ✕ Delete | ✓ Enable ⓧ Disable | ↑ Move Up

| <input type="checkbox"/> | Priority | Name           | Group         |
|--------------------------|----------|----------------|---------------|
| <input type="checkbox"/> | 1        | block p2p      | Default group |
| <input type="checkbox"/> | 2        | Allow          | Default group |
| -                        | 3        | Default Policy | -             |

**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.

---

## Chapter 3 Precautions

Transparent deployment mode is standing between 2nd and 3rd layer. But adding policy will only allows 3rd layer to 3rd layer zone to work. It will not working if user set policy for 2nd layer to 3rd later. Besides, configuration for routing is allow device to have internet access and update their database automatically.



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