# Sangfor NGAF

## Bridge Mode Deployment Configuration Guide

| | |
|---|---|
| **Product Version** | 8.0.47 |
| **Document Version** | 01 |
| **Released on** | Sept. 07, 2022 |

## Disclaimer

Products, services or features described in this document, whether wholly or in part, may be 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.

# Technical Support

For technical support, please visit: https://www.sangfor.com/en/about-us/contact-us/technical-support

Send information about errors or any product related problem to tech.support@sangfor.com.

# About This Document

This document describes the configuration guide for bridge mode deployment of Sangfor Next Generation Application Firewall(NGAF).

# Intended Audience

This document is intended for:

- System Administrator
- Network Administrator

# Note Icons

| English Icon | Description |
|---|---|
|   | Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury. |
|   | Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury. |
|   | Indicates a hazardous situation, which if not avoided, could result in minor or moderate injury. |
|   | Indicates a hazardous situation, which if not avoided, could result in settings failing to take effect, equipment damage, or data loss.<br>NOTICE addresses practices not related to personal injury. |
|   | Calls attention to important information, best practices, and tips.<br>NOTE addresses information not related to personal injury or equipment damage. |

# Change Log

| Date | Change Description |
|---|---|
| Sept. 07, 2022 | This is the first release of this document. |

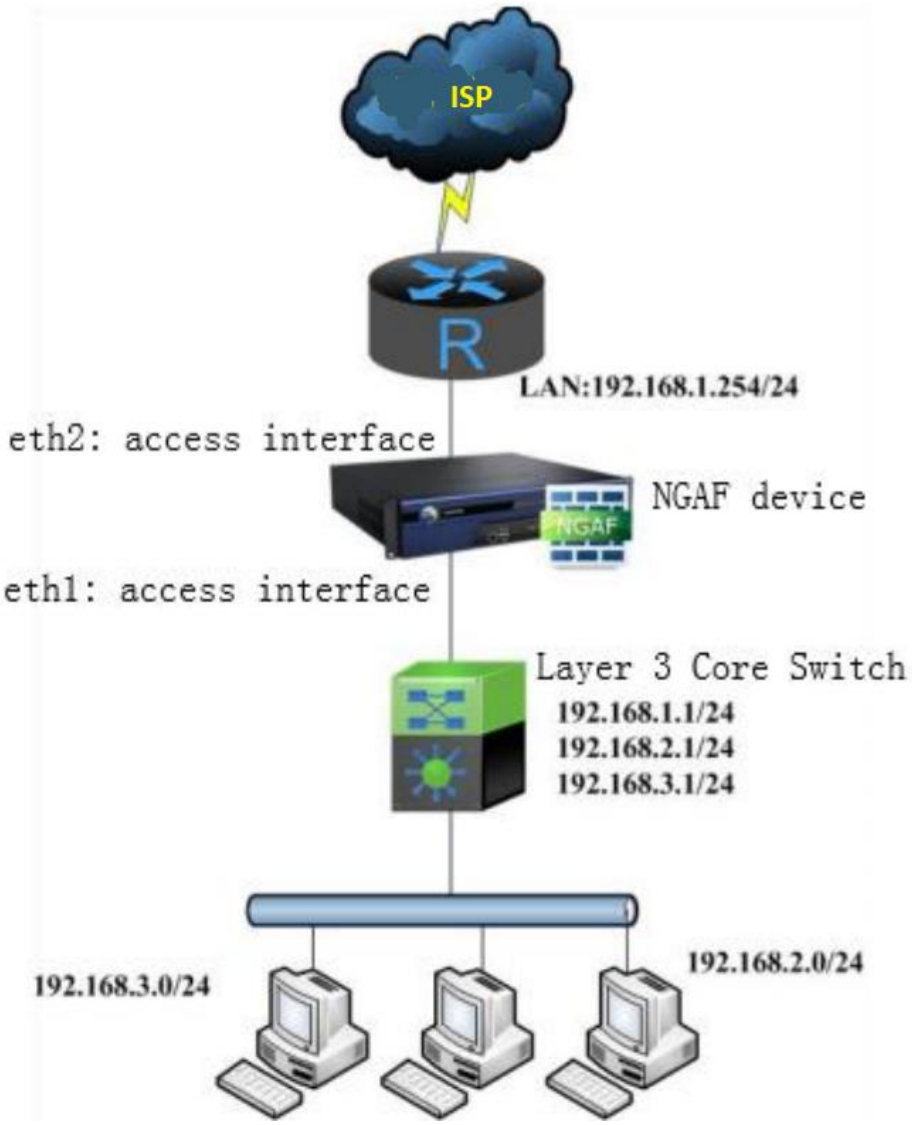
# Contents

# 1 Introduction

NGAF deploy in bridge mode belongs to a Layer 2 network device. Therefore, it can implement all the security functions of the firewall, such as Access control, bandwidth management, DNS mapping, etc. (except for the functions of the route interface).

# 2 Scenario

The firewall security feature needs to be implemented without changing the current network environment of the customer.



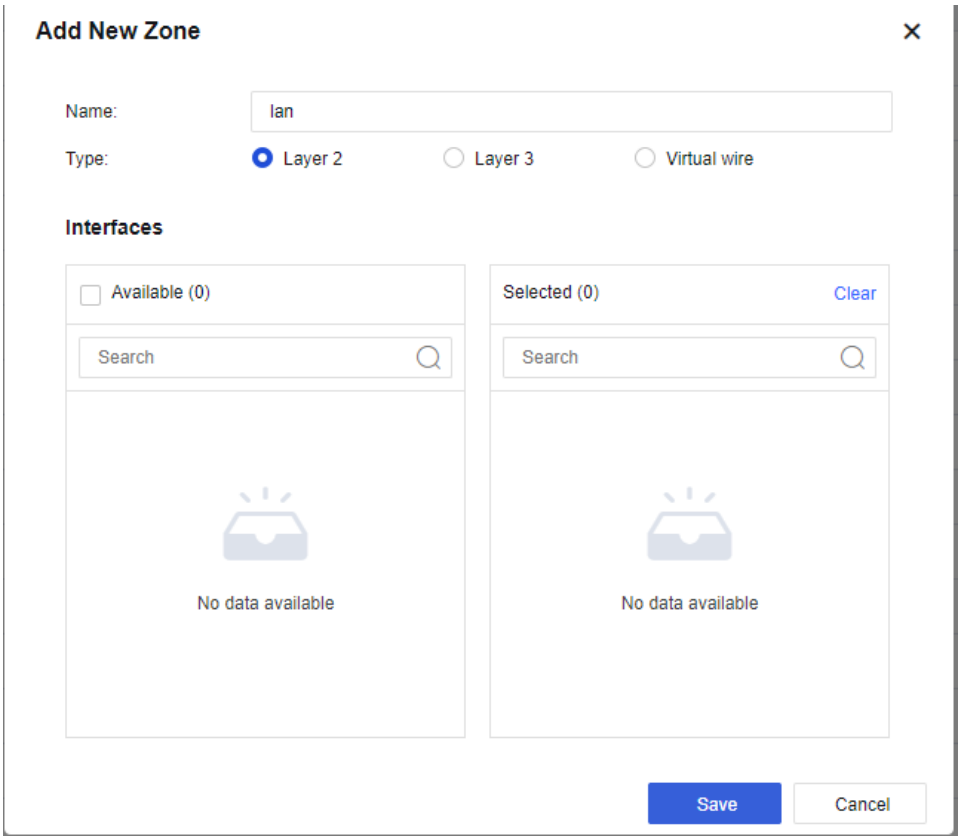
# 3 Preparation

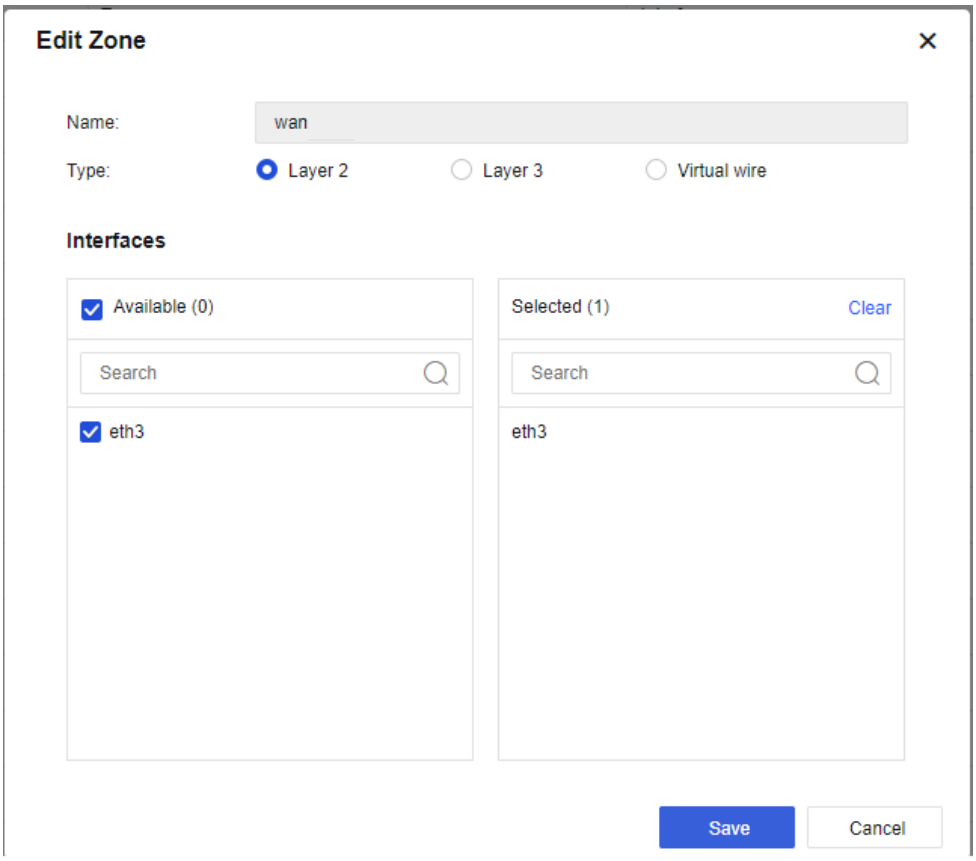
1. A designated network topology environment.
2. An NGAF device.

# 4 Configuration

## 4.1 Interface/ Zone

1. Navigate to **Network > Zone > Add**, add LAN, WAN, and Management zone as the figure below:

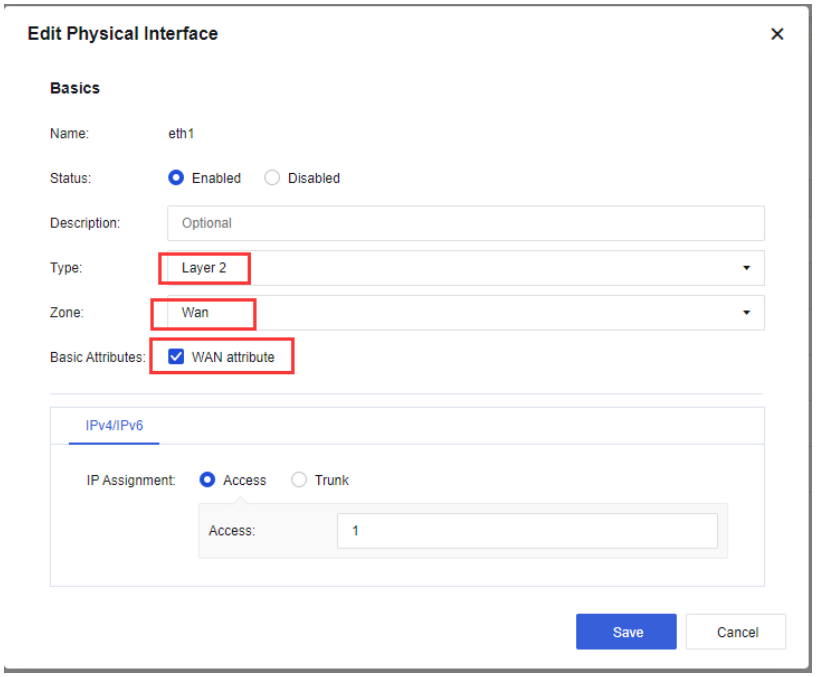





**NOTE**

Management is Layer 3 ZONE.

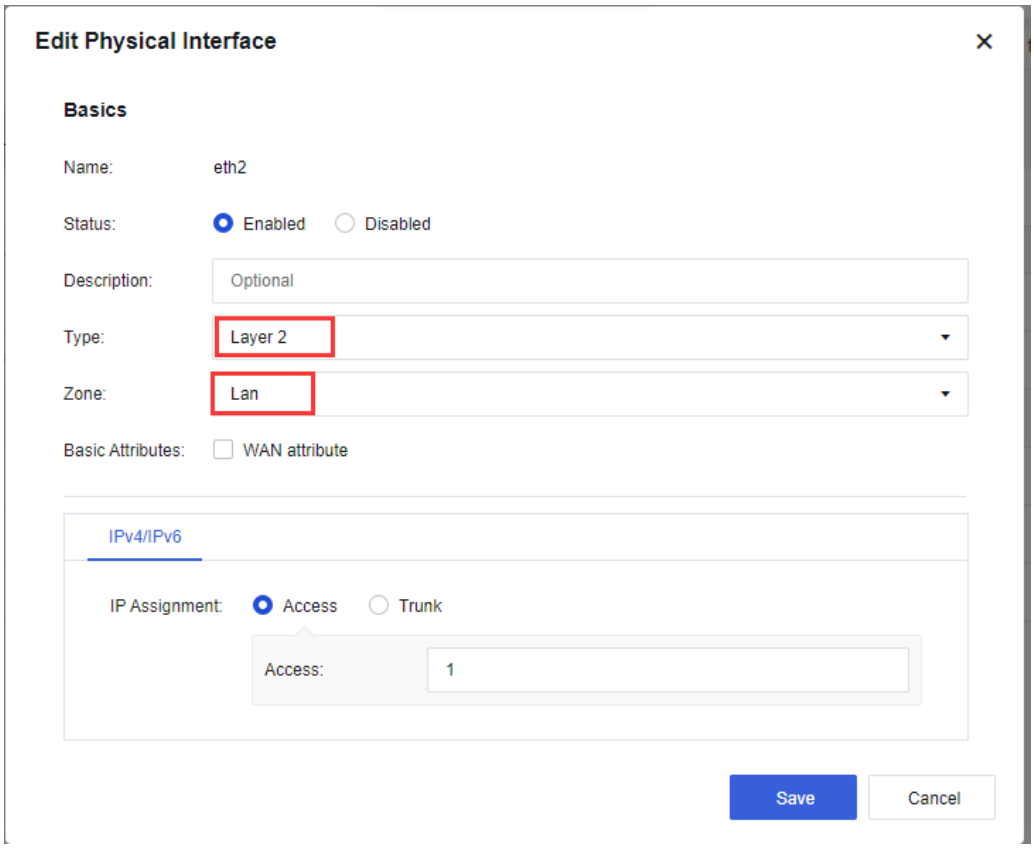
2. Navigate to **Network > Interfaces > Physical Interface,** select the interface and configure the WAN interface as shown in the figure below:



**NOTE**

The connection type is **Access** or **Trunk**. Generally, the Access interface belongs to VLAN 1 and can be modified or set to other VLANs. However, the two interfaces of the device must be in the same VLAN. In Trunk mode, native 1-1000 does not need to modify. Users can set the VLAN range to the VLAN number that needs to be penetrated by the device.

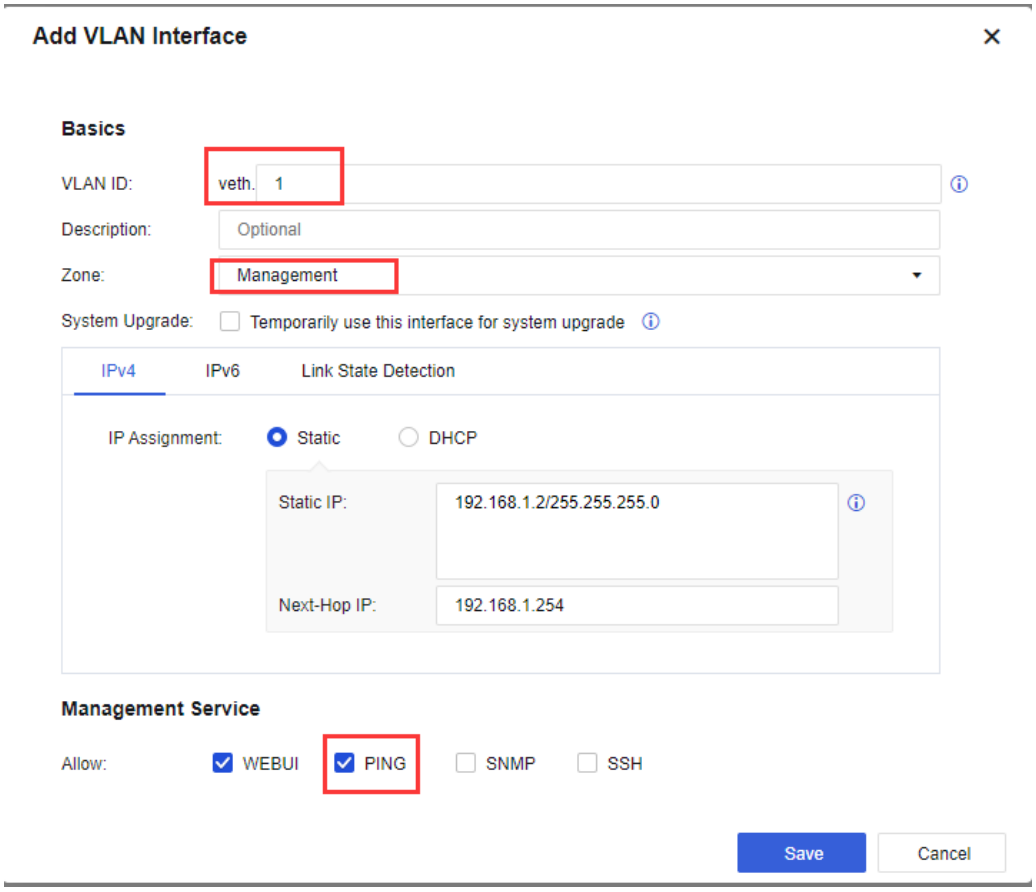
3. Navigate to **Network > Interfaces > Physical Interface,** select the interface and configure as LAN interface as shown in the figure below:




**NOTE**

The connection type is **Access** or **Trunk**. Generally, the Access interface belongs to VLAN 1 and can be modified or set to other VLANs. However, the two interfaces of the device must be in the same VLAN. In Trunk mode, native 1-1000 does not need to modify. Users can set the VLAN range to the VLAN number that needs to be penetrated by the device.

4. Navigate to **Network > Interfaces > VLAN interface > Add**, add a VLAN interface as shown in the figure below:



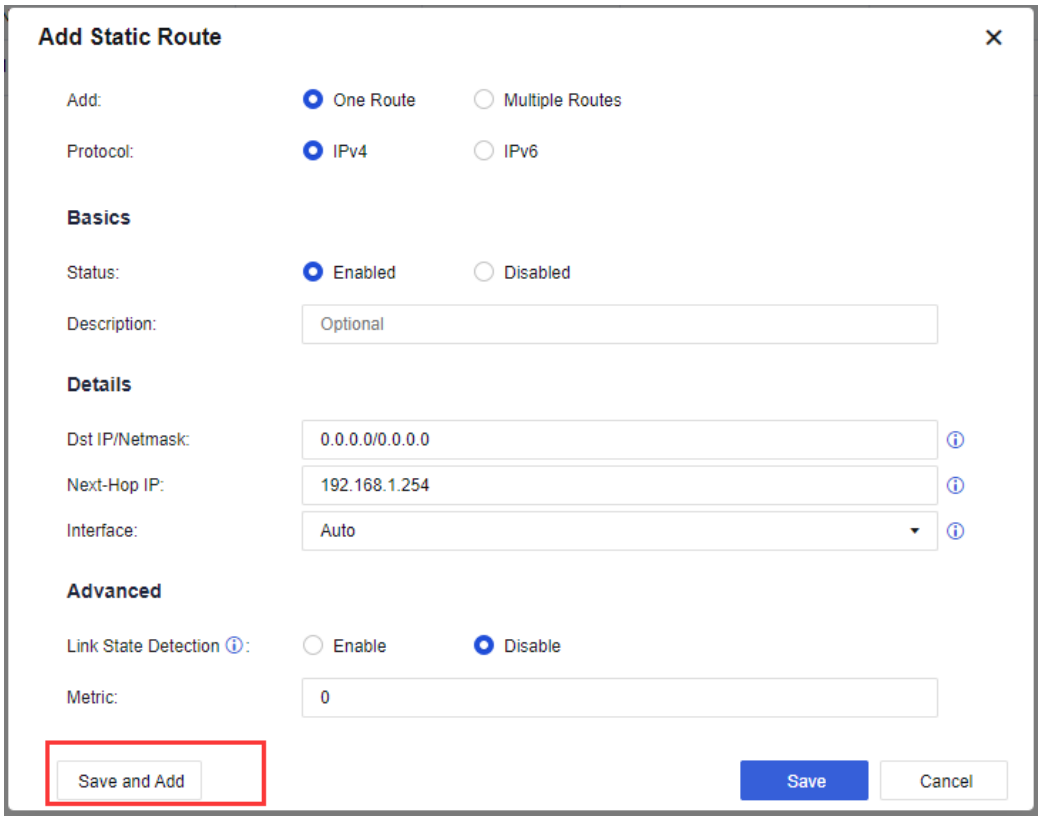

**NOTE**

**Link State Detection** is used to detect the quality of the link. The link detection method includes ARP probe, DNS lookup, and PING. The user is recommended to use PING and fill in the PING detection IP address.

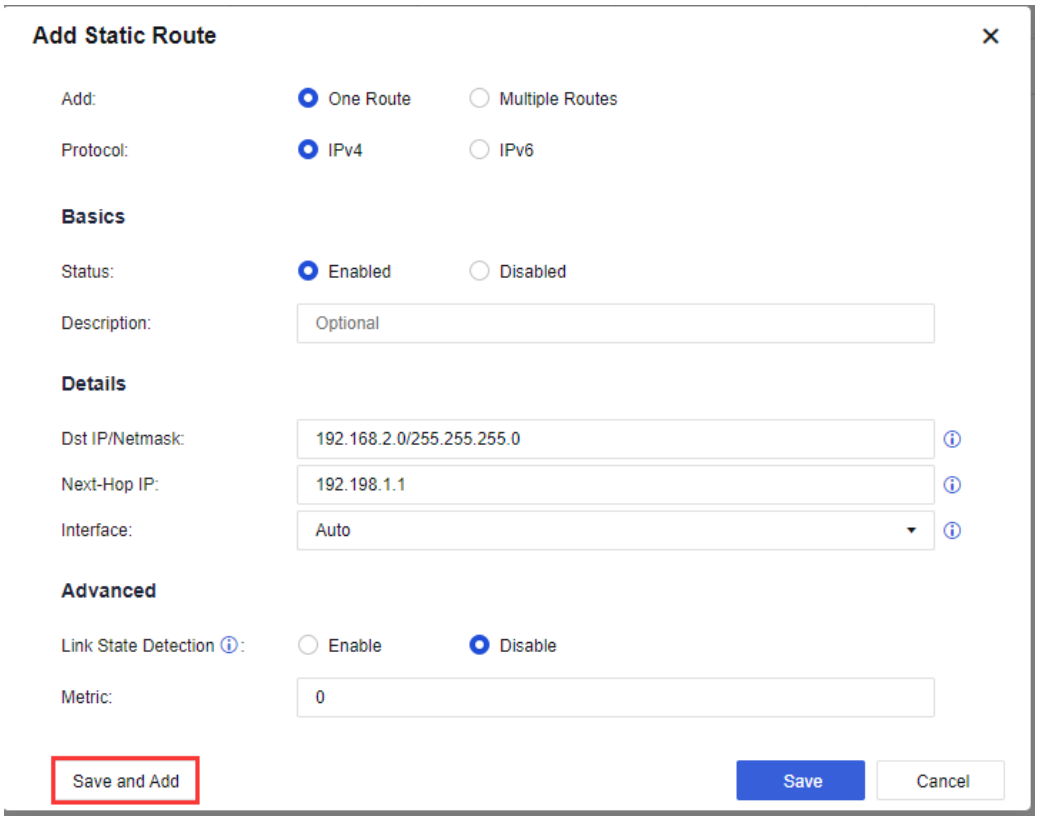
# 4.2 Routing

1. Navigate to **Network > Routes > Static Route > Add** to add a default route as shown in the figure below:

**Default Route:**




**Return Route:**

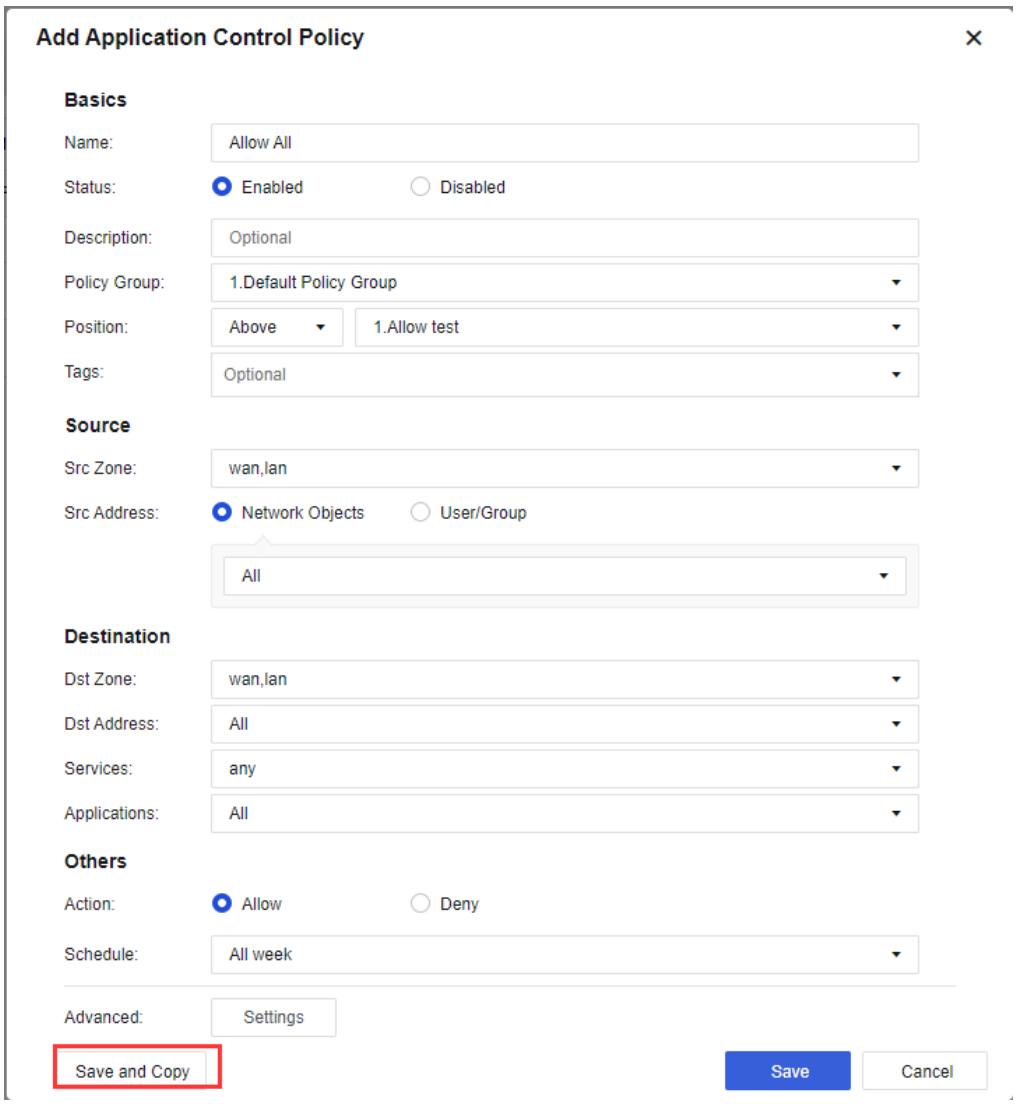


**NOTE**

**Destination IP** is the intranet user network segment. **Next-Hop IP** is the device's gateway.

# 4.3 Access Control Policy

1. Navigate to **Policies > Application Control > Policies > Add**, add an **Allow All** policy as shown in the figure below:




- **Policy Group:** Choose the default group.
- **Source:**
  - **Src Zone:** Select **WAN** and **LAN** zone.
  - **Src Address**: Select **Network Object** and **ALL**.
  - **Port: All** is selected by default.

- **Destination:**
  - **Dst Zone:** Select **WAN** and **LAN** zone.
  - **Dst Address:** Select **ALL**.
  - **Service:** Select **Any.**
  - **Application**: Select **All**.
- **Others:**
  - **Action**: Select **Allow**.

SANGFOR