SANGFOR

NGAF

Route Mode Deployment Guide

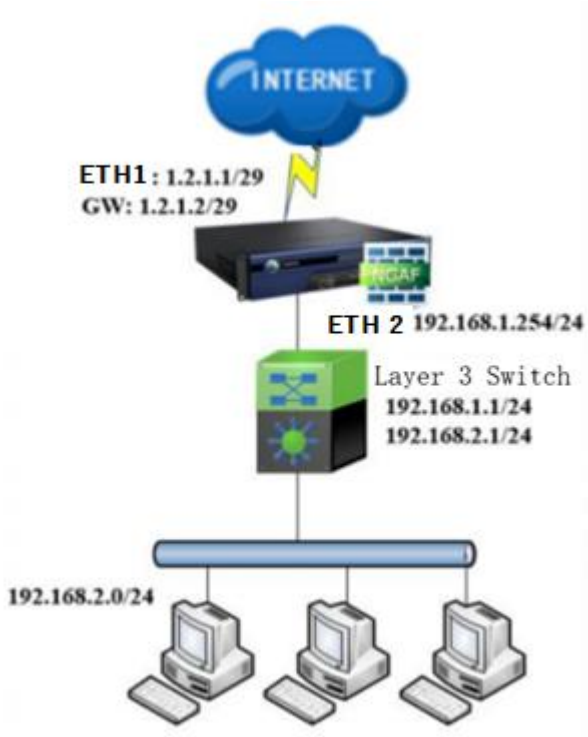
Version 8.0.35

Change Log

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

Contents

Chapter 1 Applicable Scenario



This deployment is suit on those environments which require Sangfor NGAF deploy as network gateway or replace gateway router.

Chapter 2 Configuration Steps

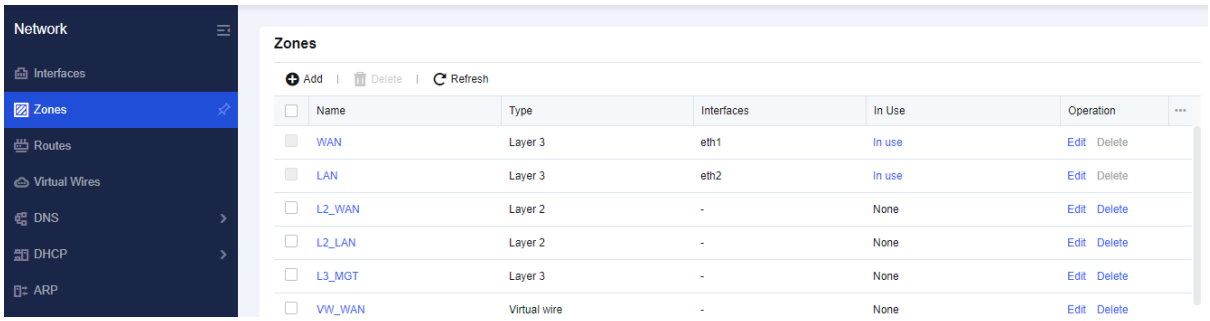
2.1 Configure Interfaces and Zone

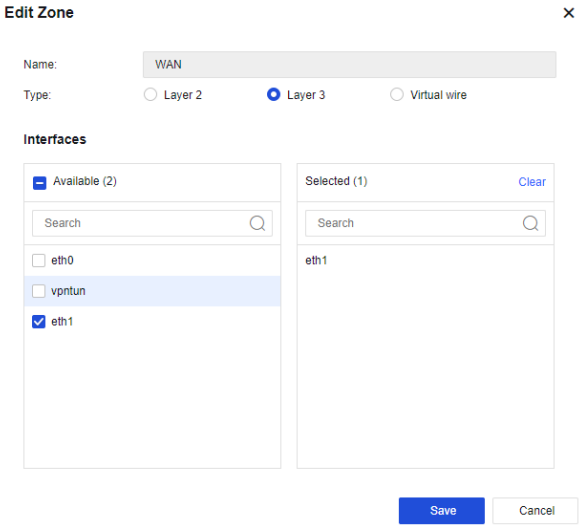
1. Zone Configuration:

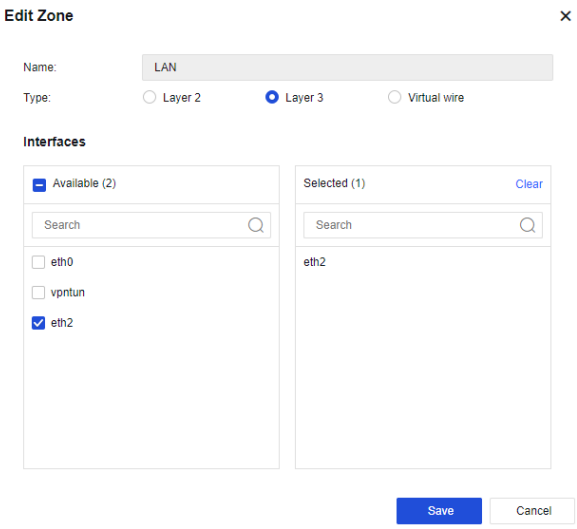
Access **Network > Zones** to add or modify the zone configuration.

Name: WAN / LAN

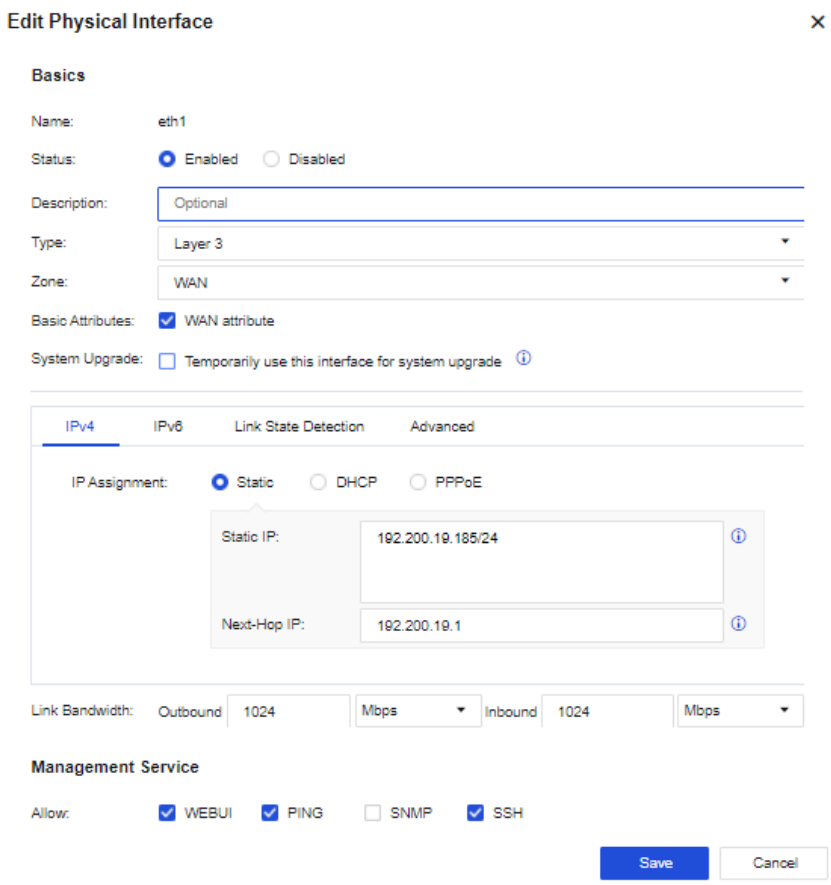
Forward Mode: Route (Layer 3)

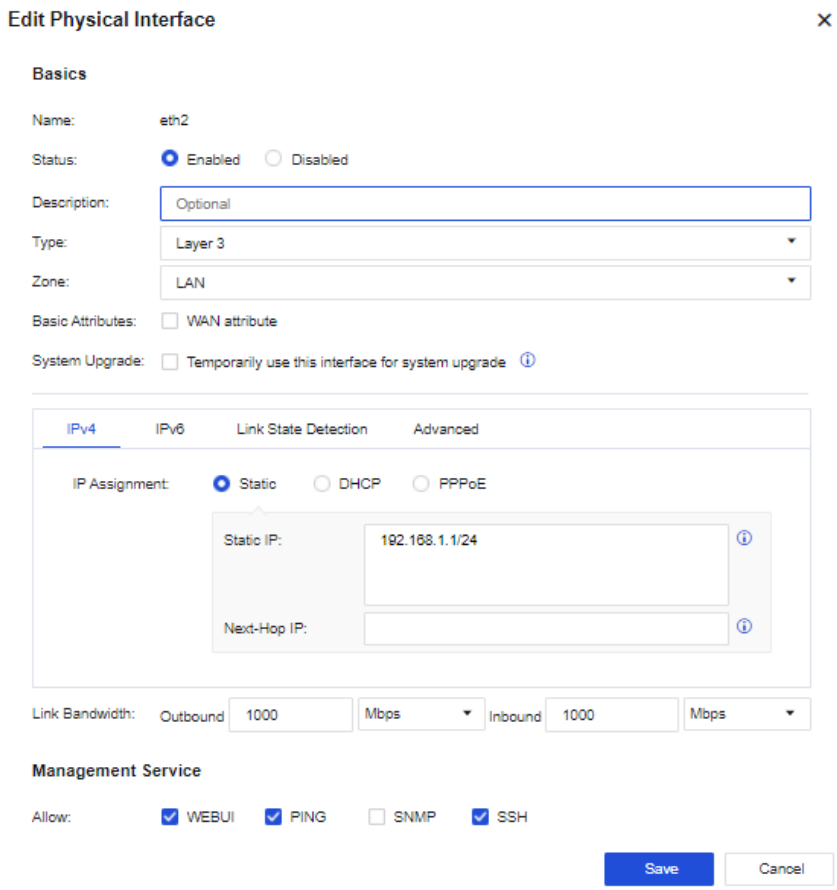






2. Access to **Network** > **Interfaces** to configure eth 1 and eth2 as WAN and LAN interface as figure shown below:

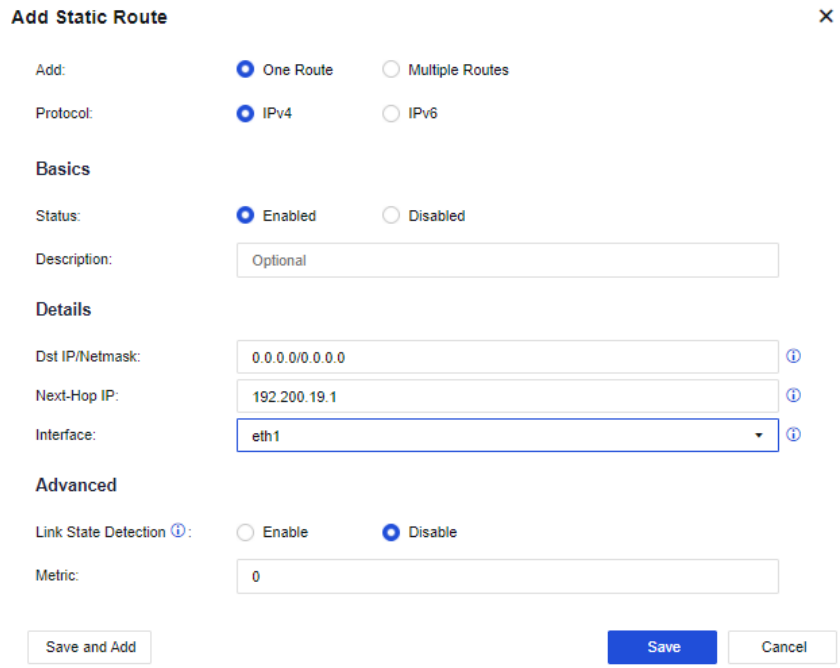




2.2 Configure Route

2.2.1 Configure Default Route

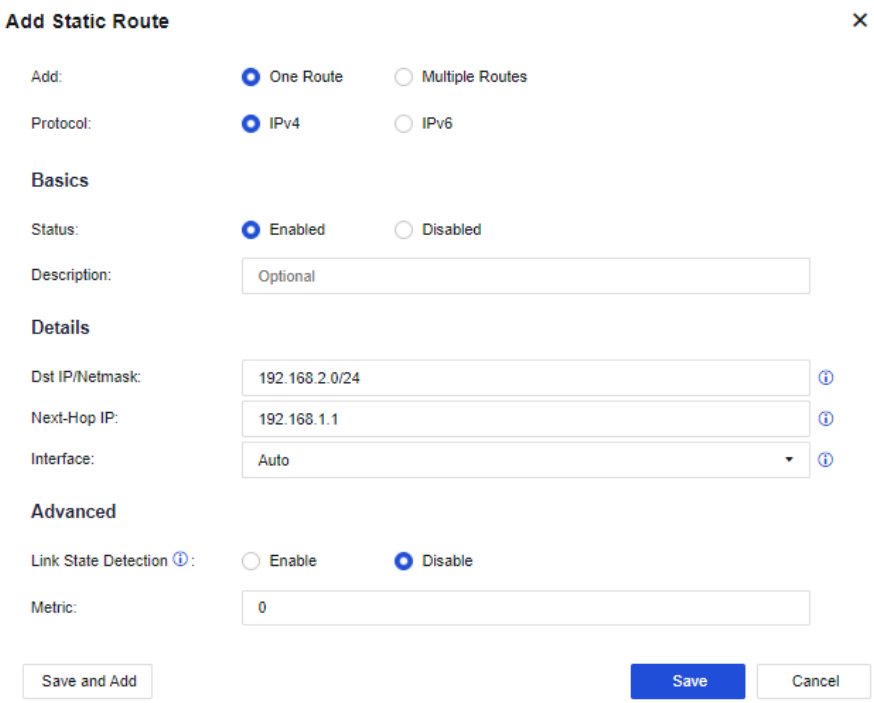
1. Access to **Network** > **Routes** > **Static Routes**. Click **Add** to add new default route in NGAF as shown in figure below:



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:



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: SNAT

Status: Enabled | Disabled

Description: Optional

Schedule: All week

Original Data Packet

Src Zone: LAN

Src Address: Internal

Dst Zone/Interface: Zone | Interface

WAN

Dst Address: All

Services: any

Translated Data Packet

Translate Src IP To: Outbound Interface

Translate Dst IP To: Untranslated

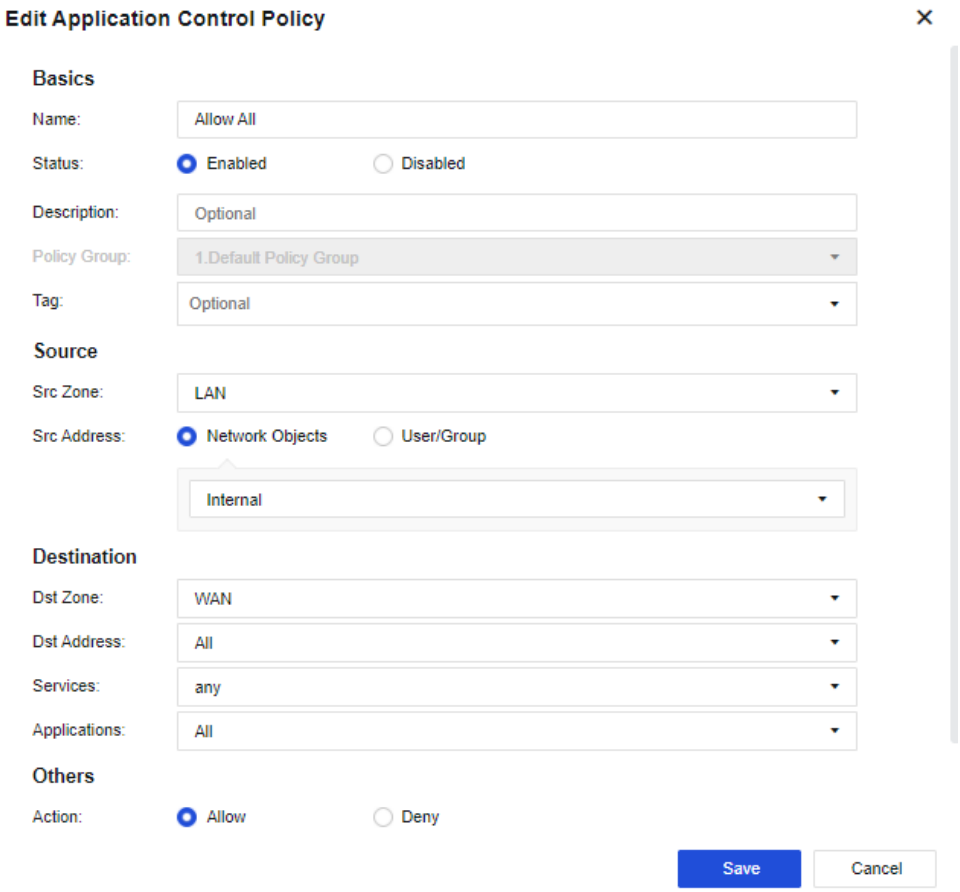
Translate Dst Port To: Untranslated

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:

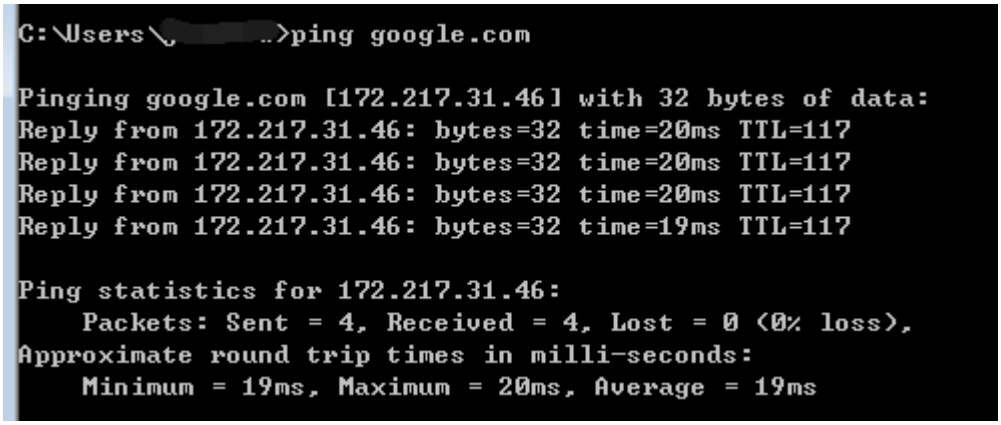


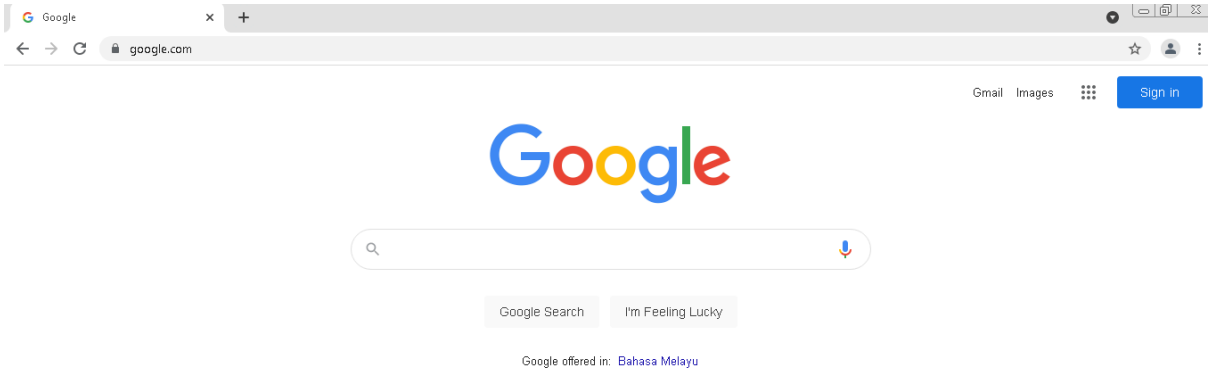
NOTICE

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.





SANGFOR