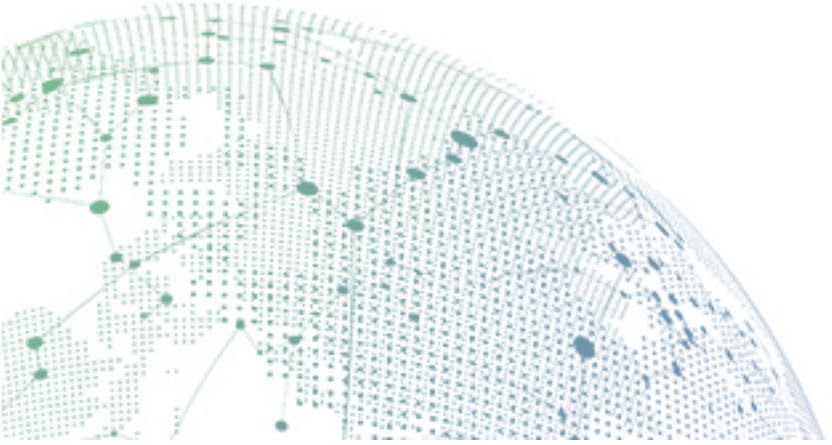
SANGFOR

NGAF

Transparent Mode Deployment Guide

Version 8.0.5

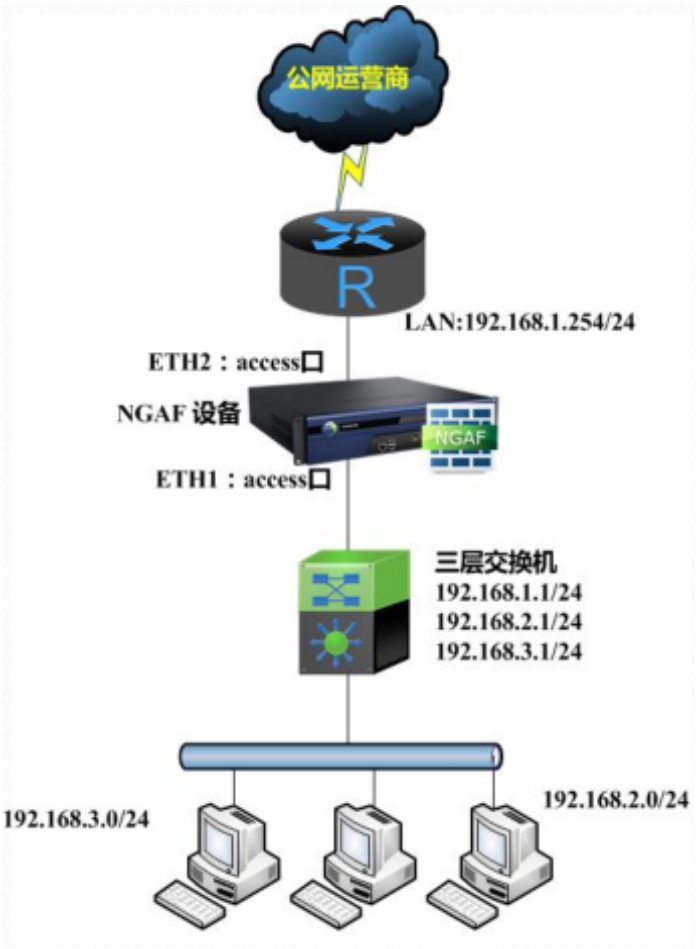


Change Log

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

CONTENT

Chapter 1 Applicable Environment

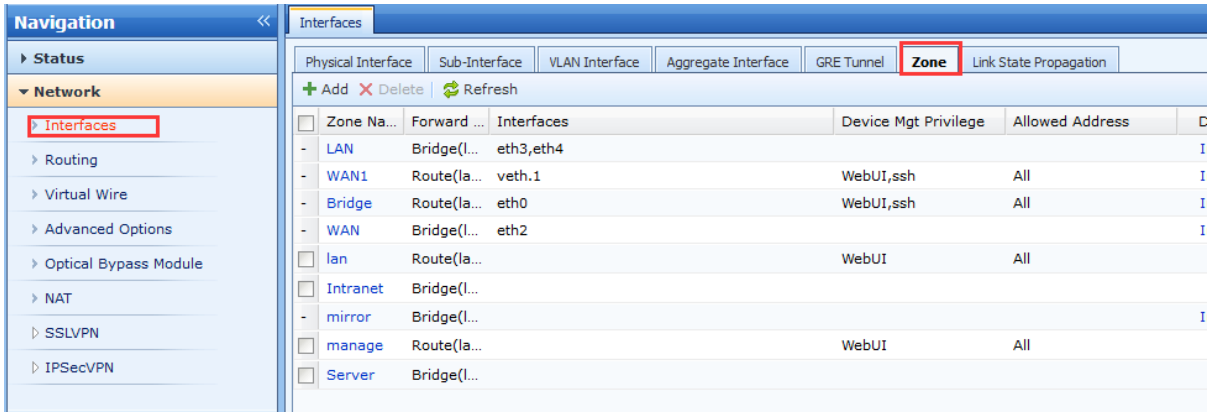


When user need to apply firewall and does not change their network environment.

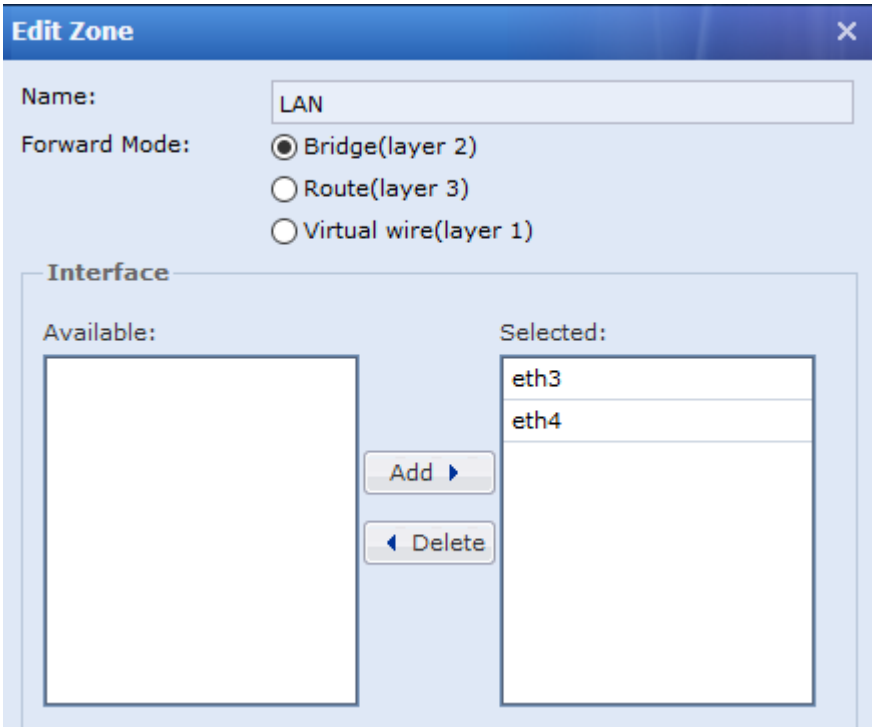
Chapter 2 Configuration Step

2.1 Configure Zone for LAN, WAN and management

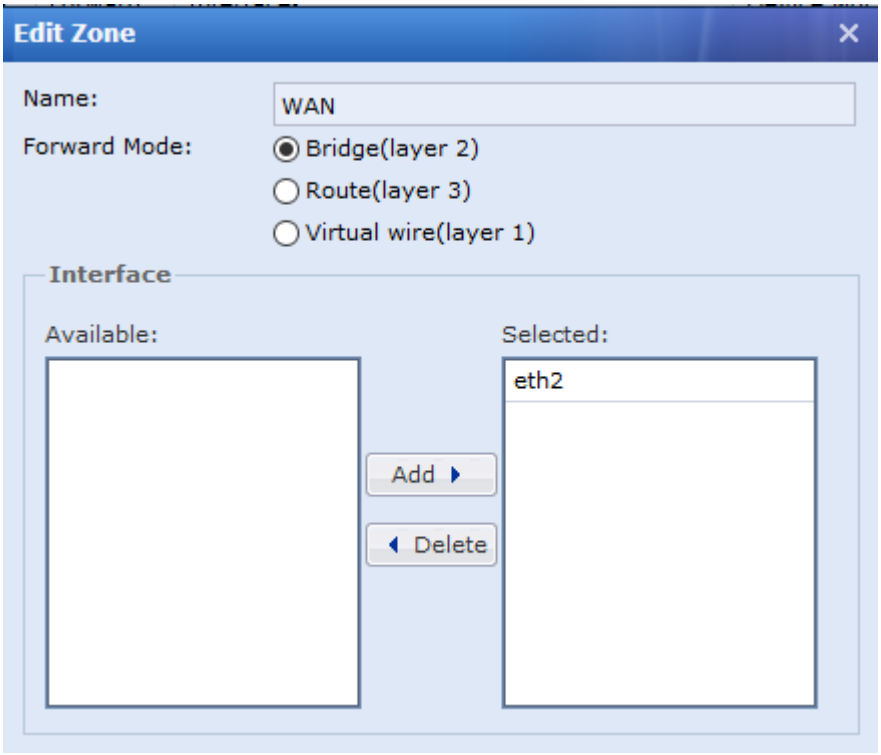
Go to [Network]→[Interfaces]-[Physical Interfaces]



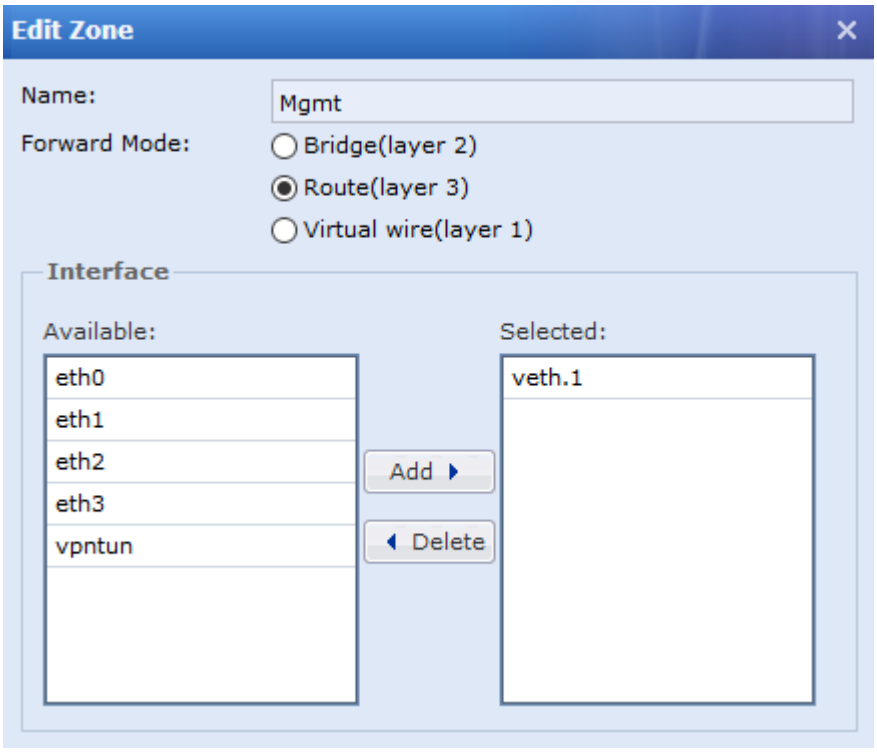
Configuration for LAN zone



Configuration for WAN zone



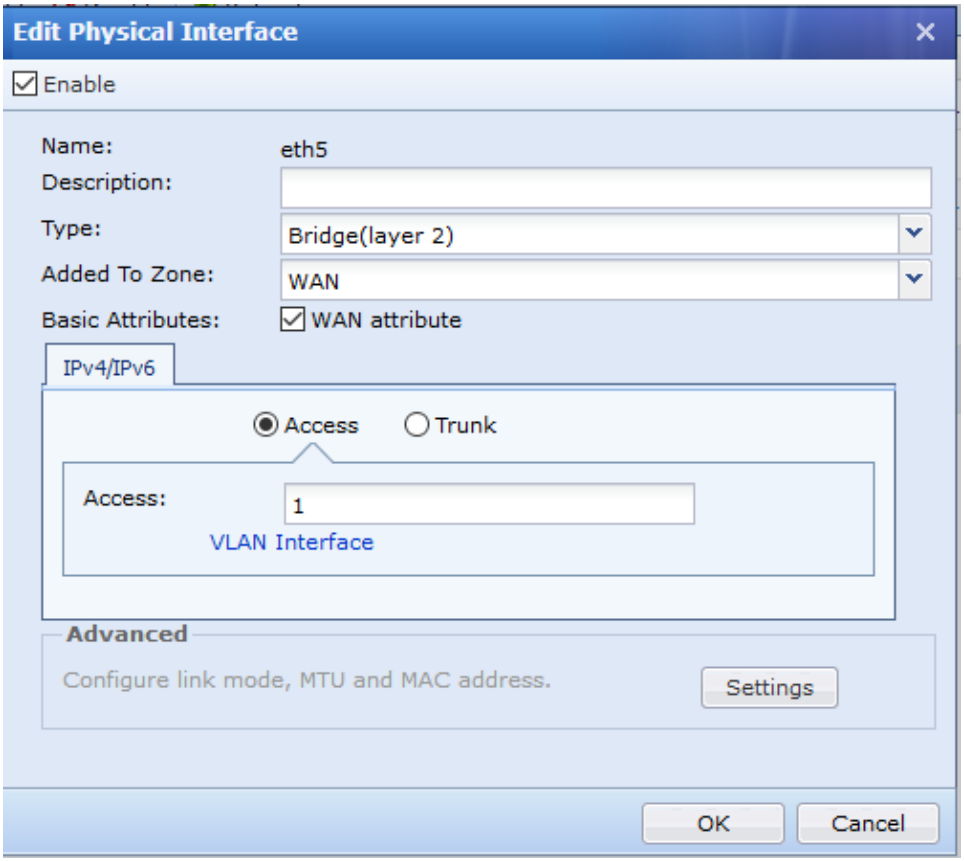
Configuration for Management zone



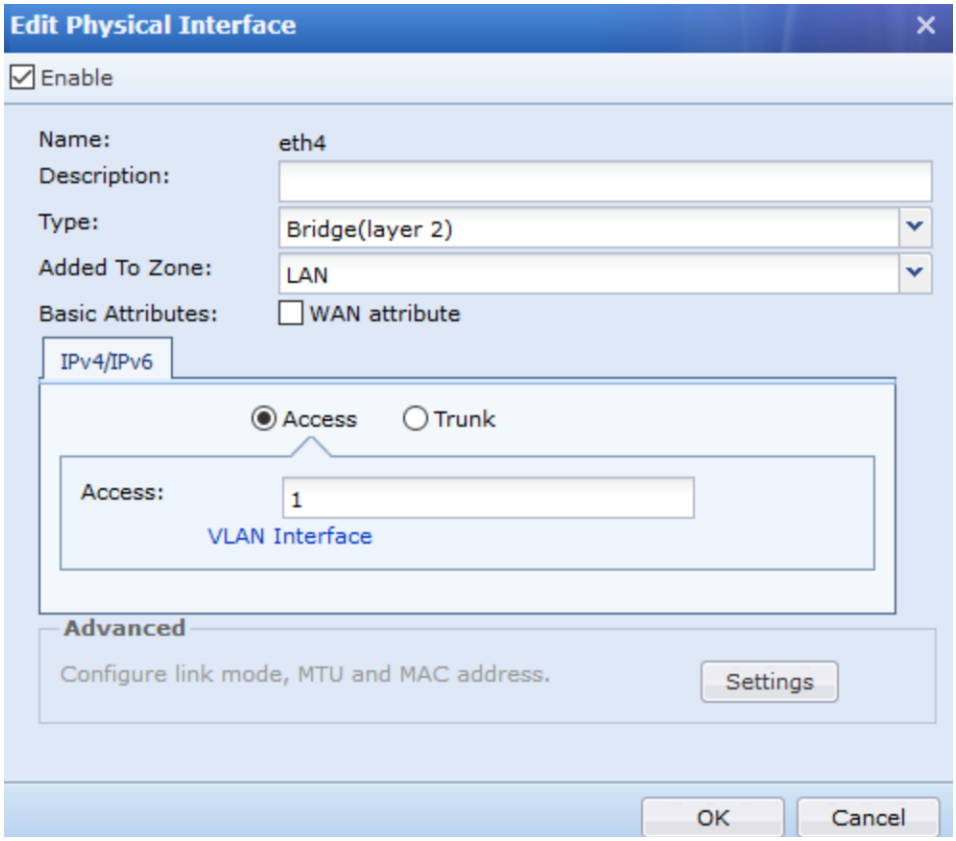
2.2 Interface Configuration

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

Assign one interface for WAN attribute and WAN zone

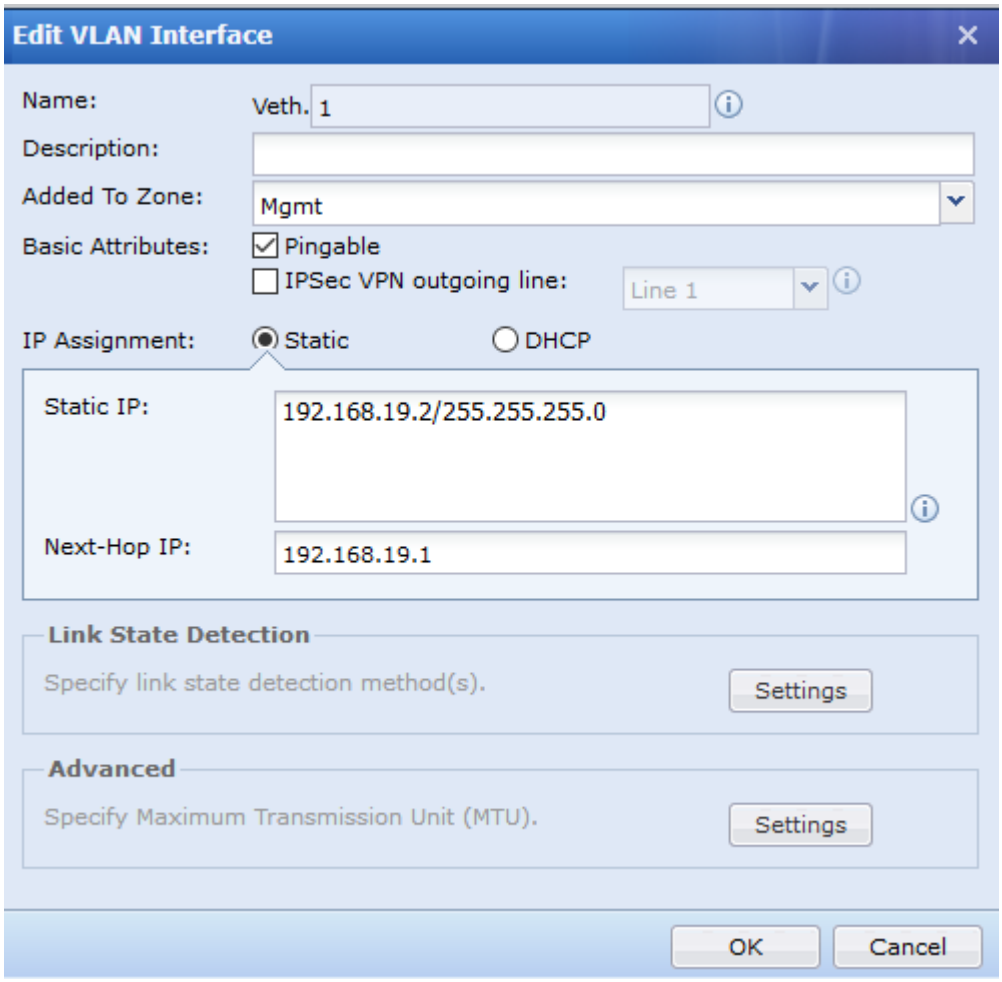


Assign another interface for LAN zone



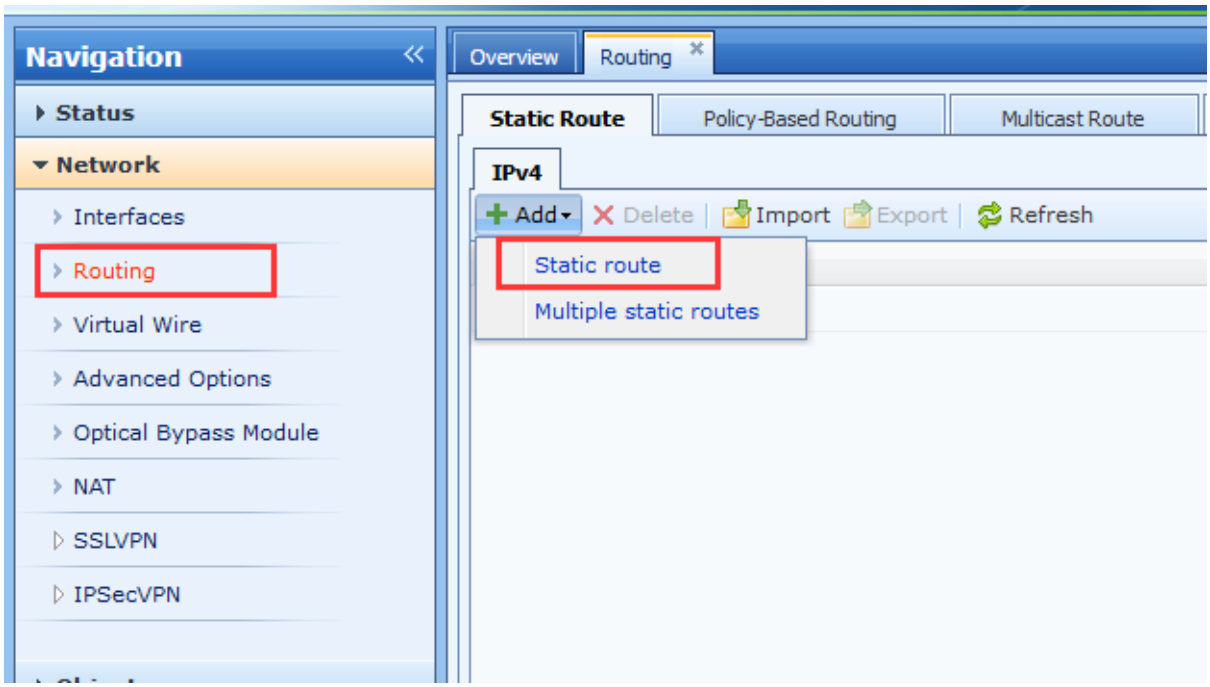
2.3 VLAN Configuration

Create a VLAN interface and add to management zone

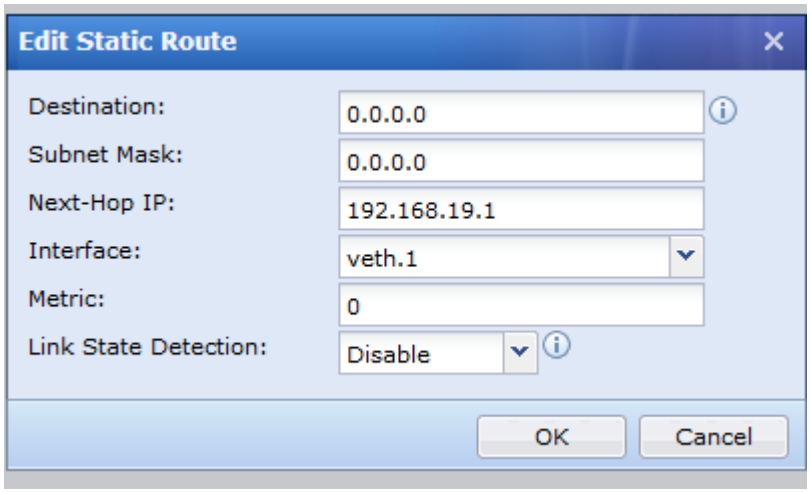

Edit VLAN Interface
Name:
Veth. 1
Description:
Added To Zone:
Mgmt
Basic Attributes:
Pingable
IPSec VPN outgoing line:
Line 1
IP Assignment:
Static
DHCP
Static IP:
192.168.19.2/255.255.255.0
Next-Hop IP:
192.168.19.1
Link State Detection
Specify link state detection method(s).
Settings
Advanced
Specify 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:

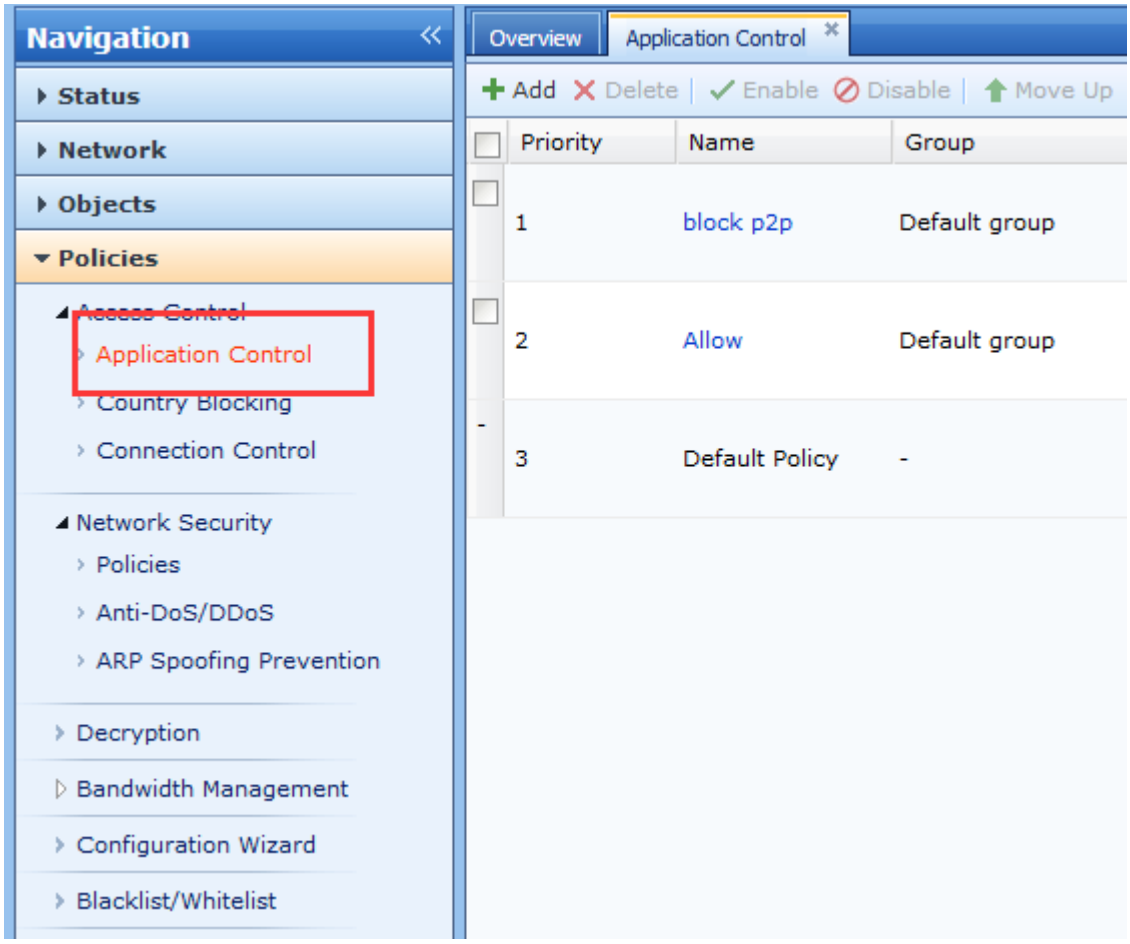


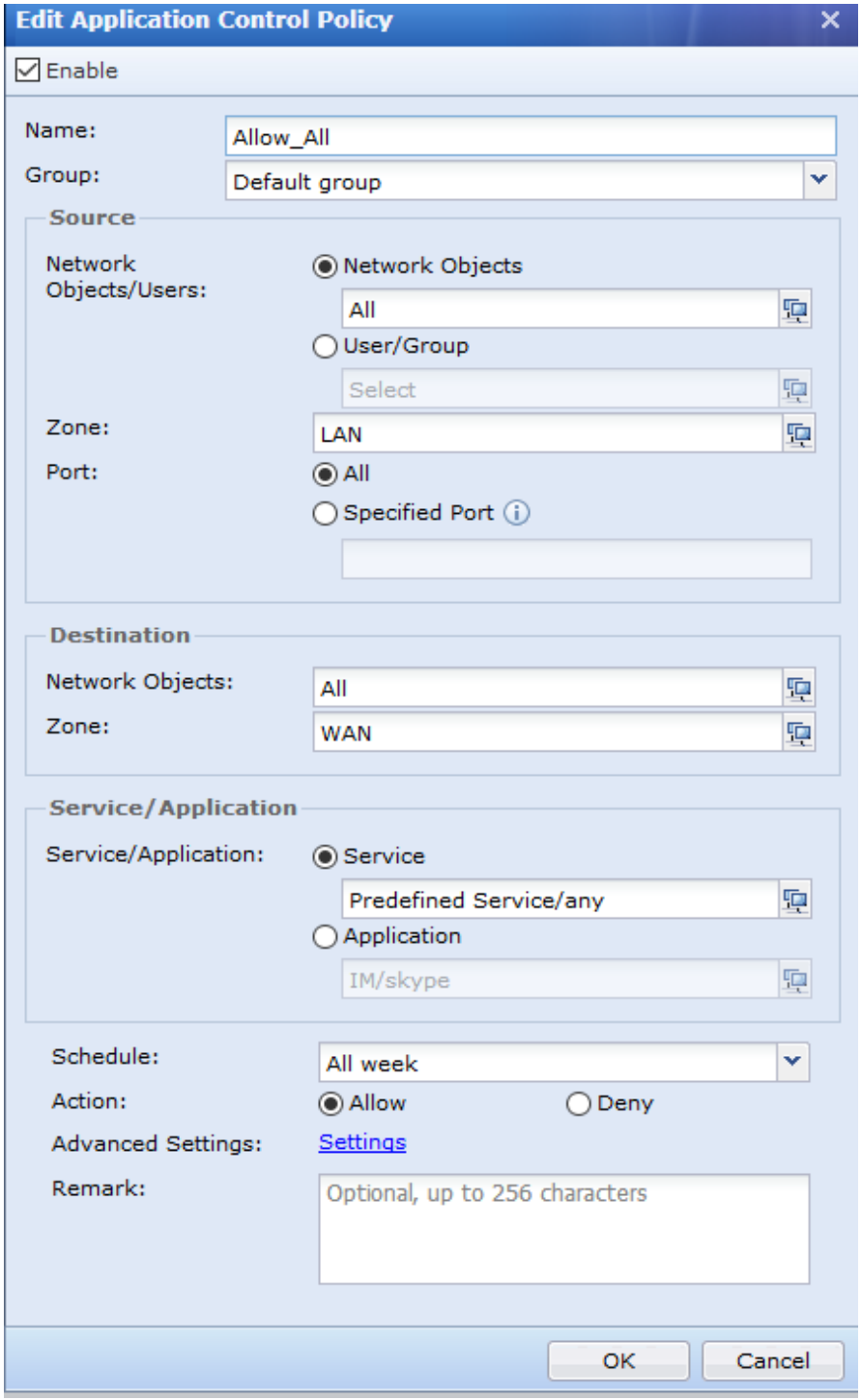
Insert destination address, subnet mask, next hop IP and choose an interface for VLAN.



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
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
Priority
Name
Group
1
block p2p
Default group
2
Allow
Default group
3
Default Policy
-



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.

SANGFOR