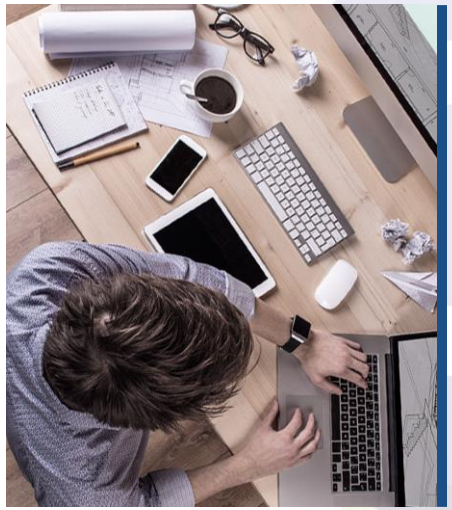
Sangfor NGAF v8.0.47 Associate

Basic Network Configuration



1. Interface
2. Routing
3. NAT

1 Interface

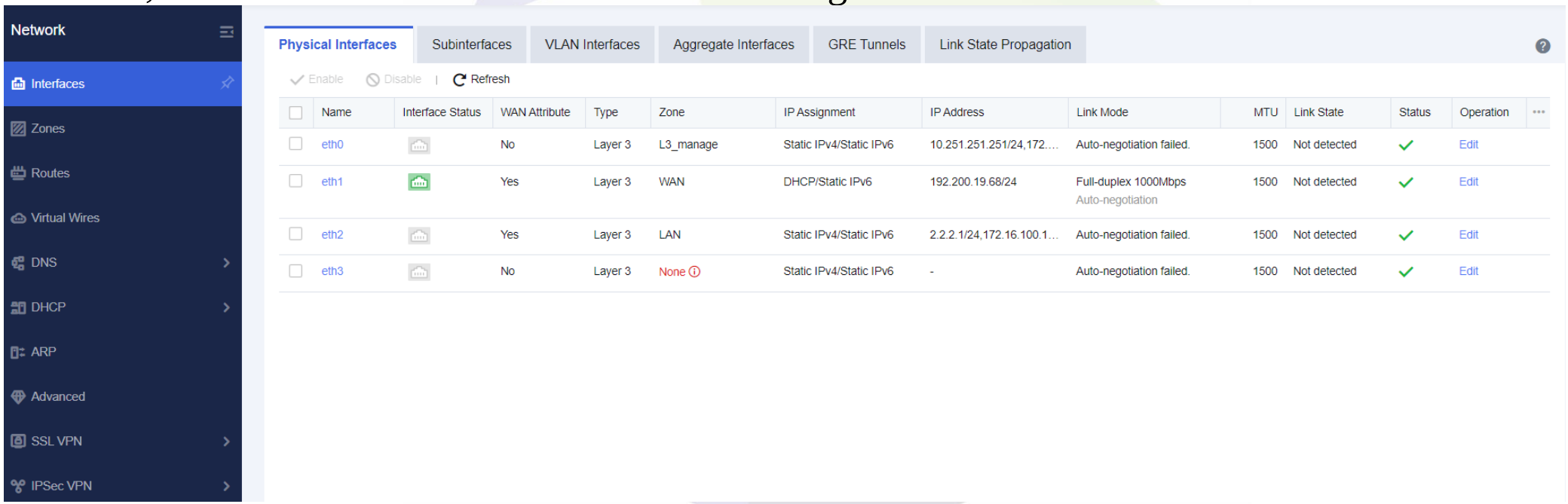
SANGFOR
深信服科技

Physical Interface

NGAF interfaces are correspond with the physical panel.

Eth0 is the management interface.

Physical interface can define physical interface as route, bridge, Virtual Wire and mirror interface, the first three kinds of interface can configure as WAN attribute.



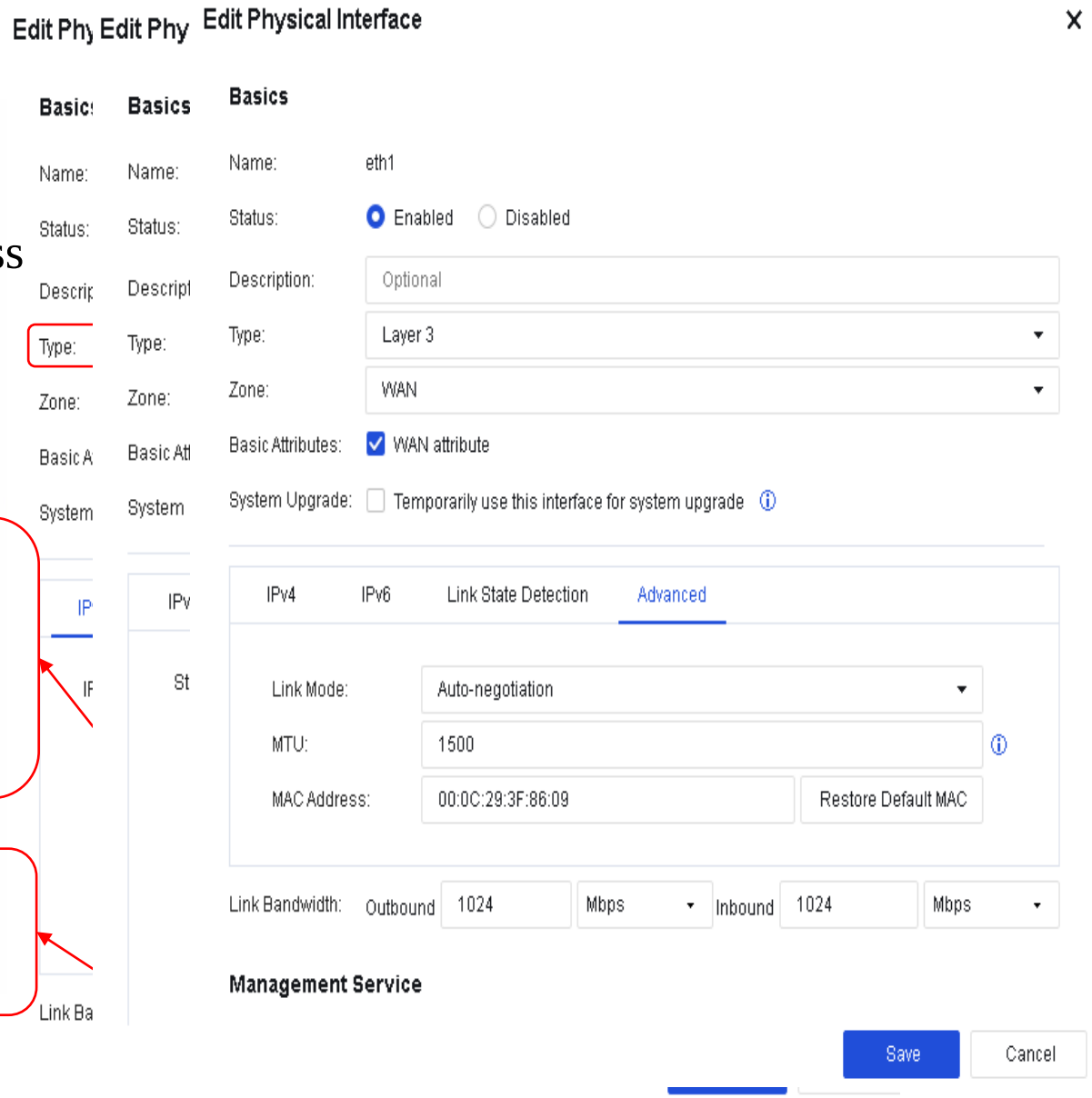
Physical interface can’t delete or add, it depends on the model.

Route Interface

Route interface:
Must configure a IP address for routing purpose.

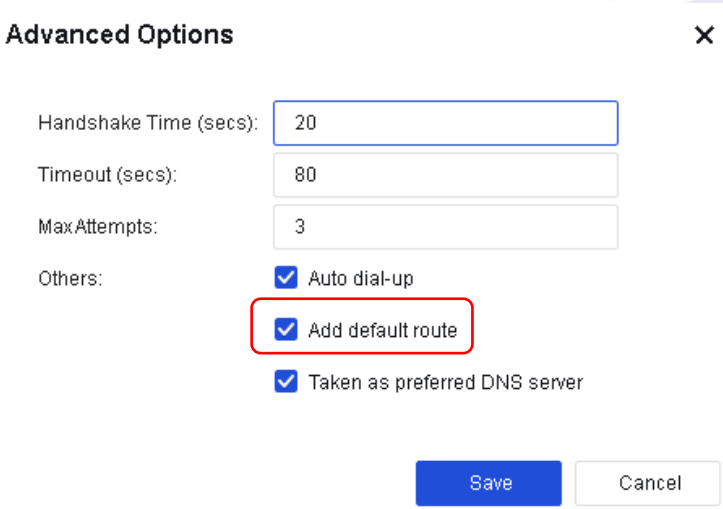
Configure next hop IP , for link state detection and it won't automatically create 0.0.0.0 default route, need to manually create.

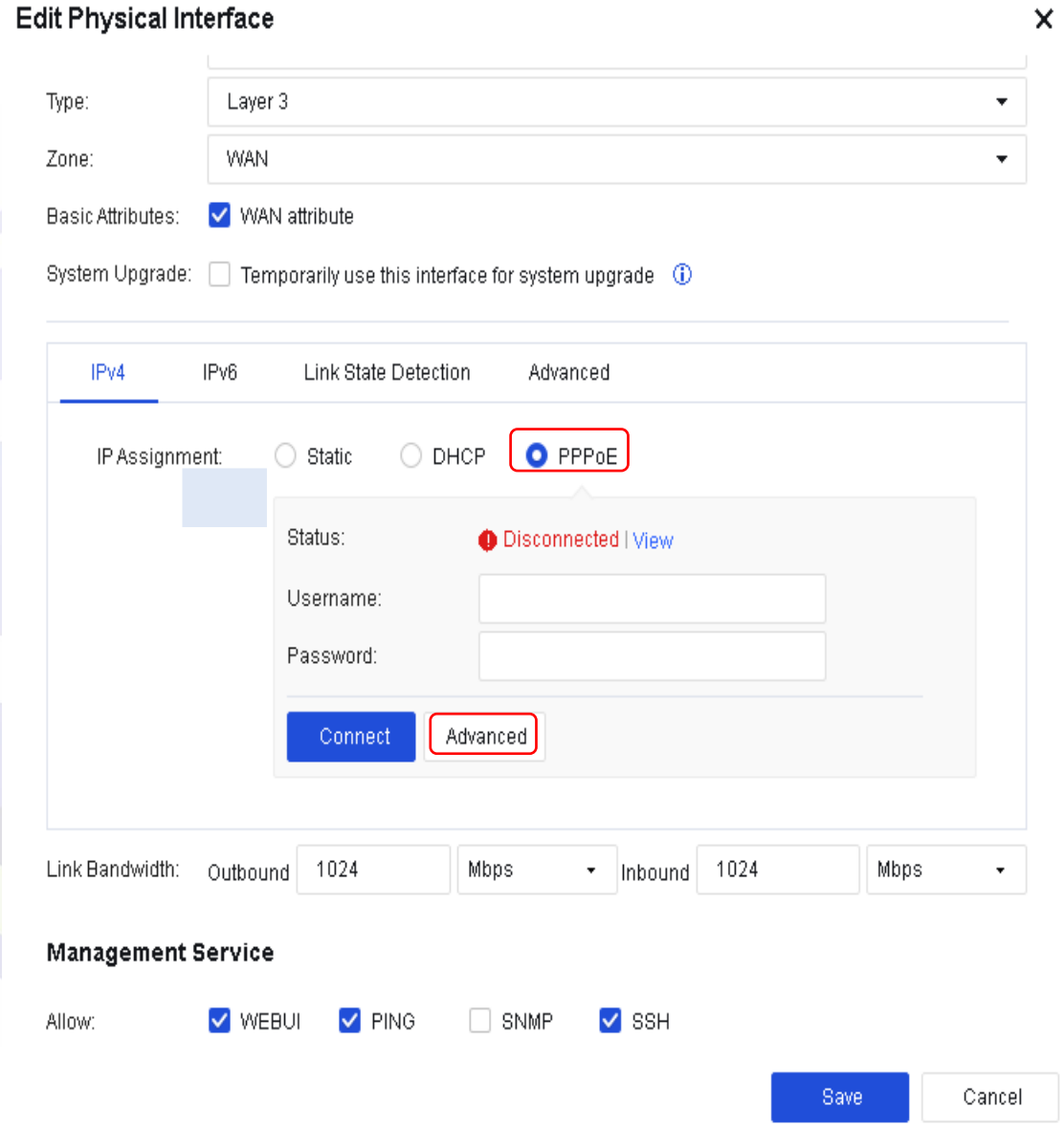
Bandwidth of the interface, this is not related with BM and use for Link Load balance.



Route Interface

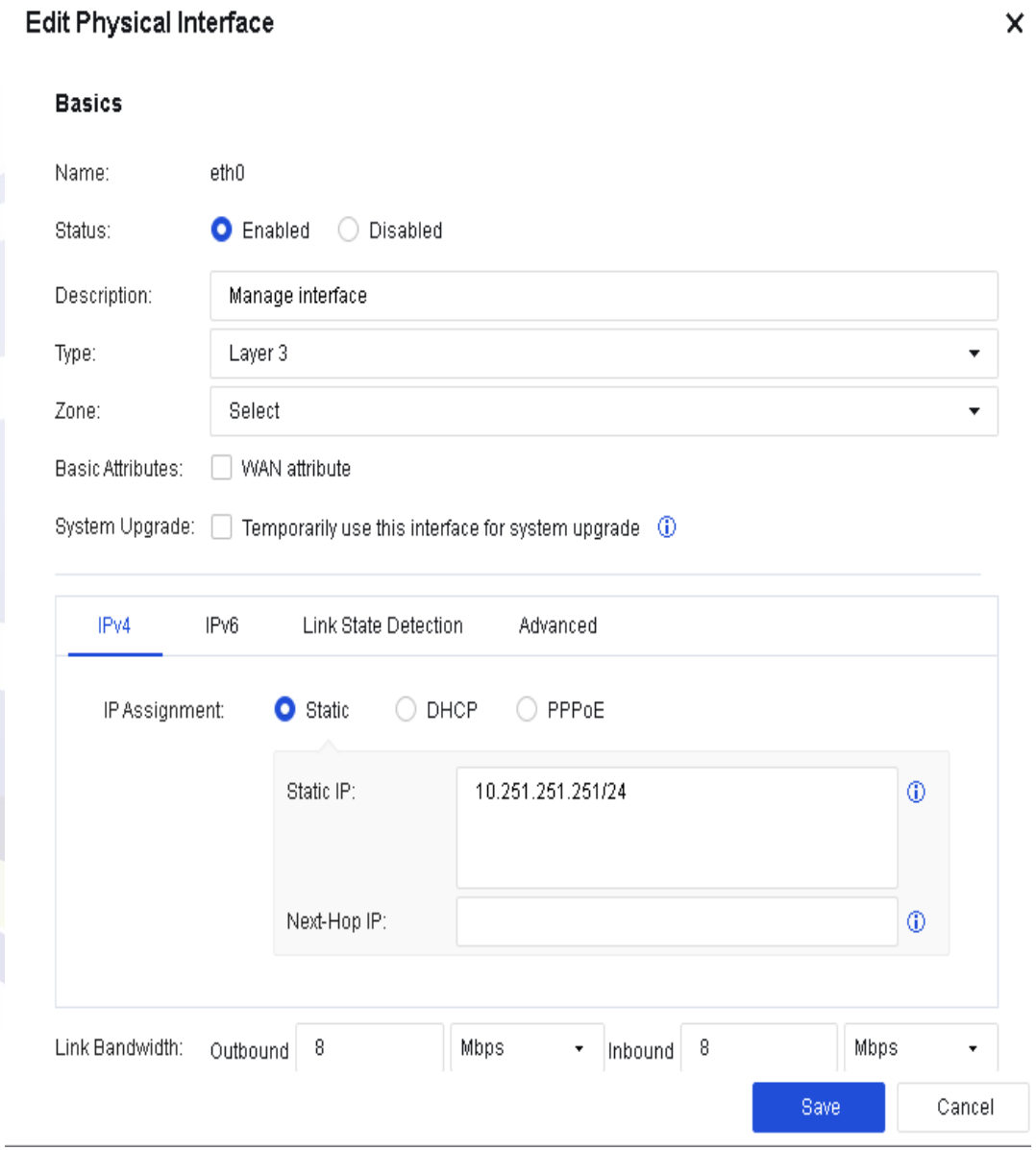
If the interface set as a route mode and the IP Assignment is the PPPoE, it needs to enable the option ‘obtain default route’





Route Interface

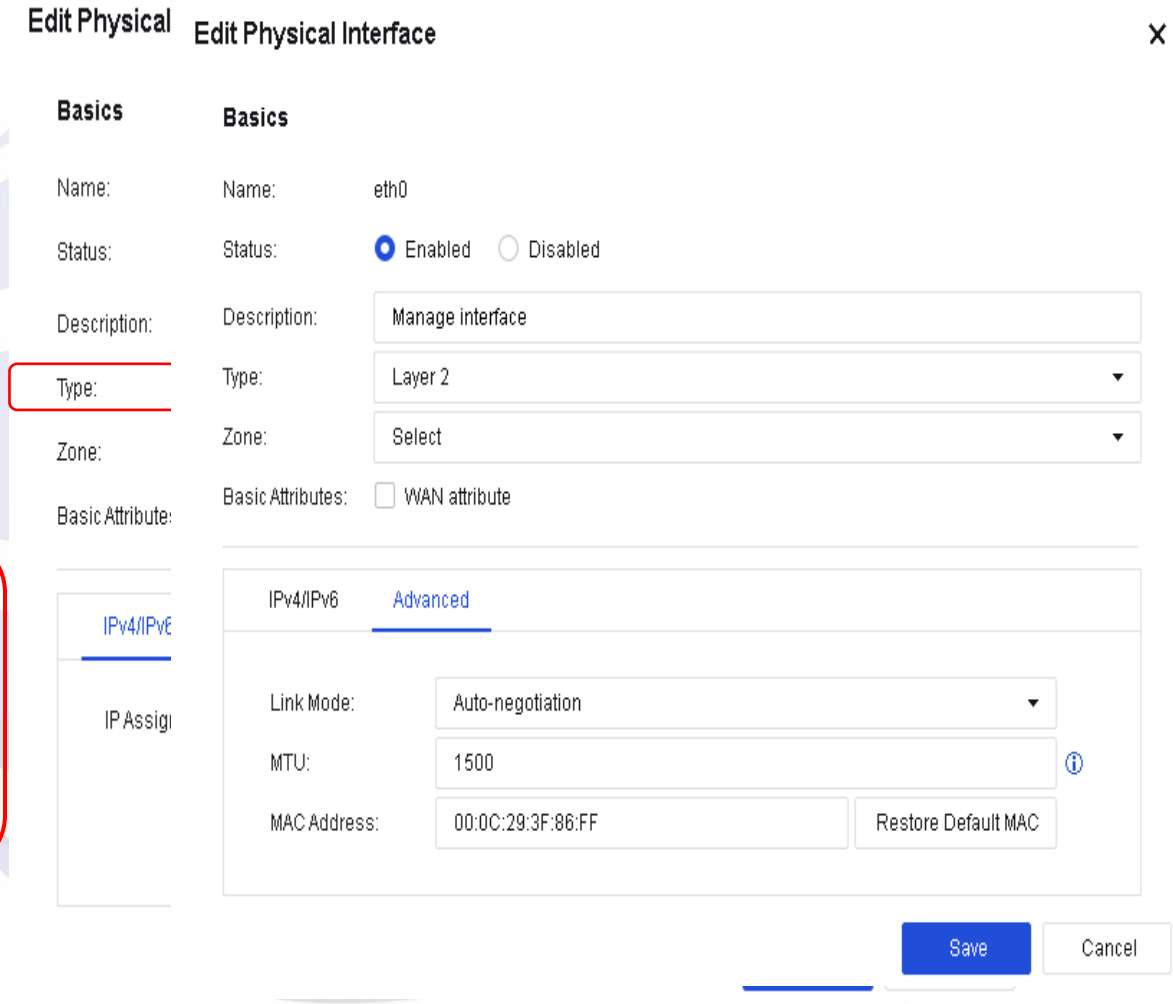
Manage interface:
Eth0 is permanent manage interface and type will be route interface, IP is 10.251.251.251/24. The Interface type cannot be change. The management IP can be change after version 8.0.13 but cannot be delete.



Bridge Interface

Bridge Interface:
Bridge interface like normal switch port , doesn't need a IP address, not support routing.
It transfer data based on MAC address

Some of the feature need configure interface as WAN attribute.
Take note: If interface configure as bridge with WAN attribute , reverse cable connection will cause WAN Attribute not working.

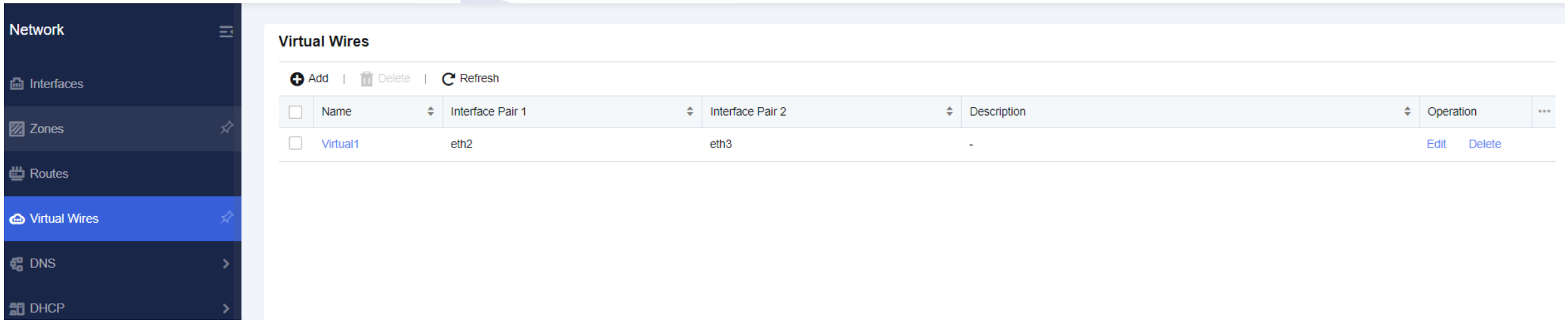


Virtual Wire Interface

Virtual wire interface:

Like a normal switch port , doesn't need to configure any IP address, doesn't support routing, data transmit also doesn't refer to MAC address list, it will also transmit to the other interface.

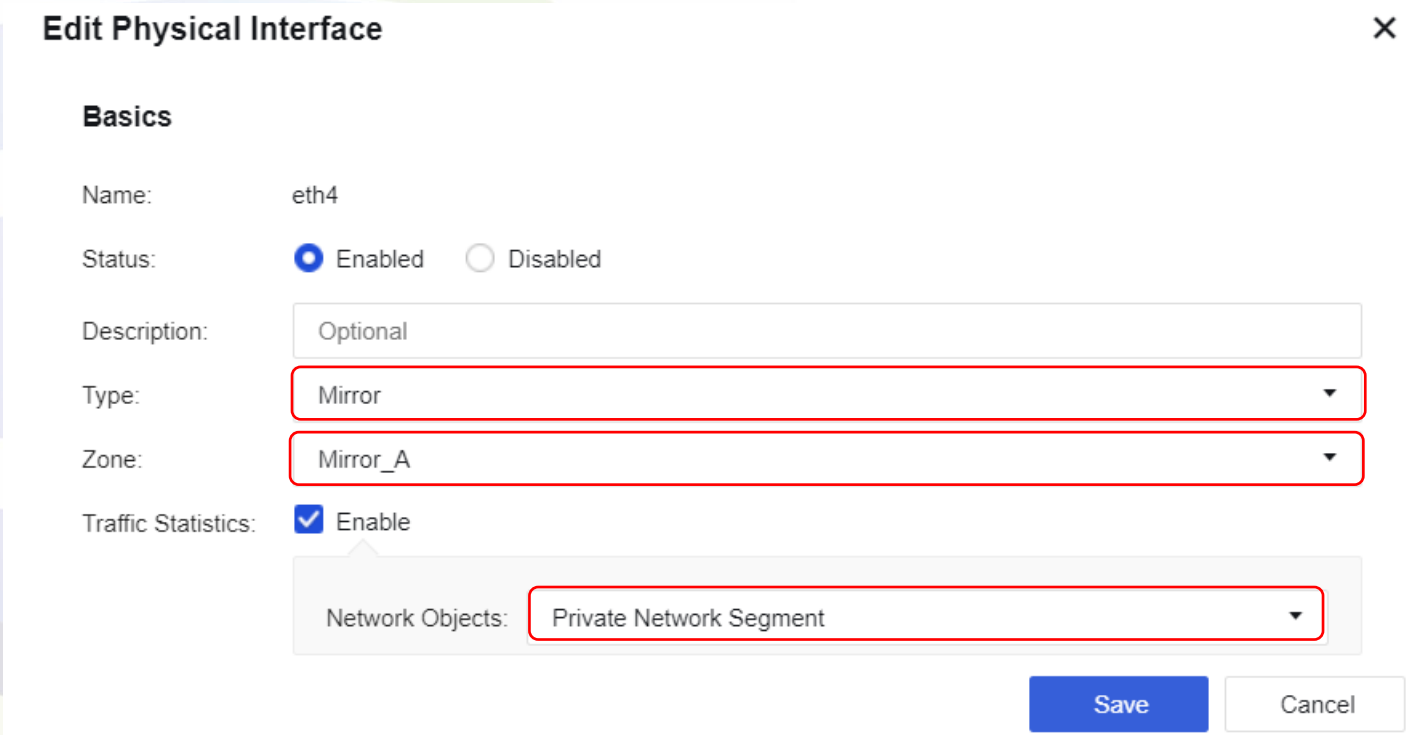
Virtual Wire interface transmission performance is higher than bridge interface.



Mirror Interface

Mirror Interface:
The mirroring interface cannot be configured with an IP address and does not support data forwarding。It is only used to receive mirrored data from external mirrors.

Note: Mirror interface can be configured more than one. Choose according to the actual business scenario of the site that needs to receive data.



Aggregate interface

Aggregate Interface is a logical interface, not a physical interface, combined with multi Ethernet interfaces.

Four work mode:

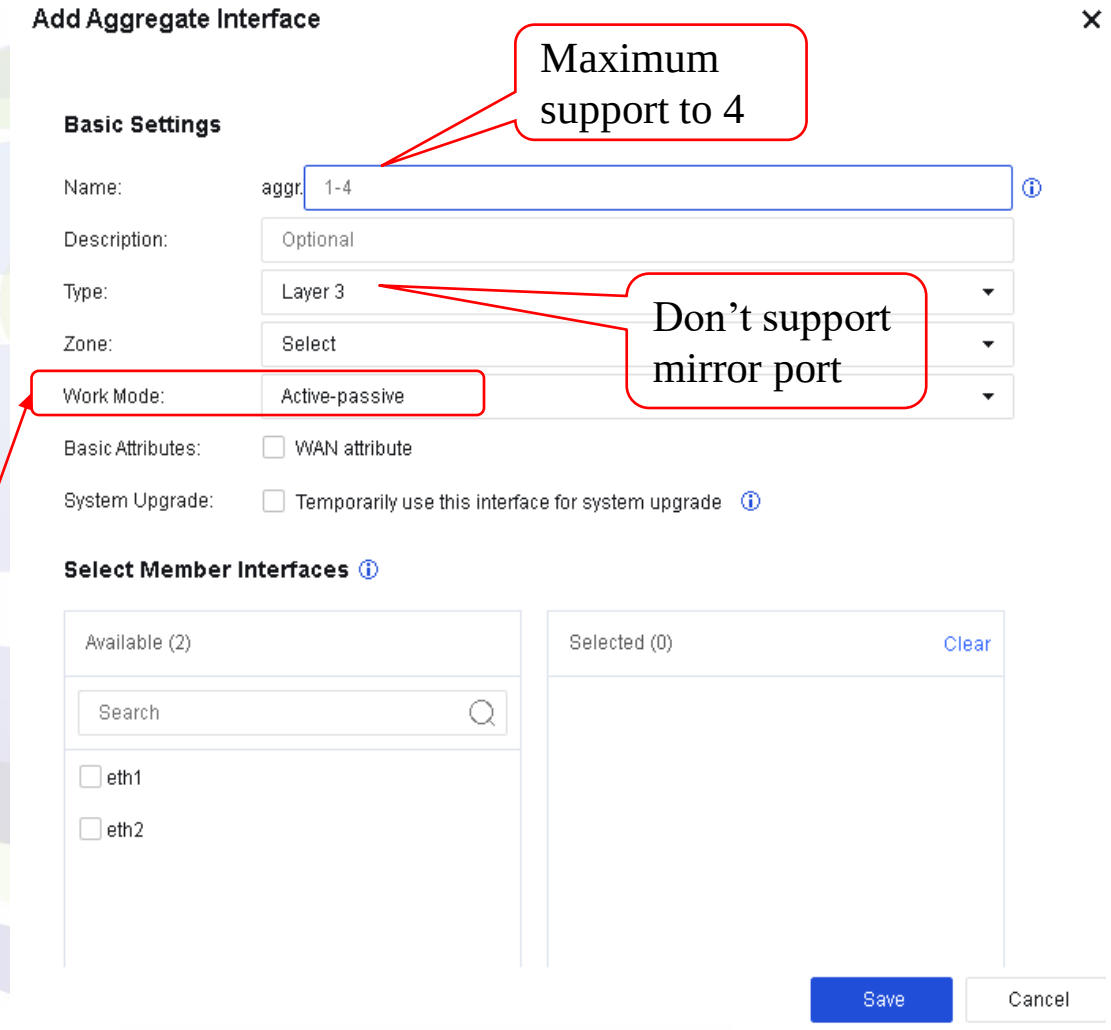
Load balance --hash: packet transmission depends on the hash value of source and destination IP / MAC

Load balance --RR: packet transmit to each interface evenly

Standby mode - take the largest number eth-based interface transceiver package, the rest is prepared Interface

LACP --can support LACP protocol with the standard IEEE 802.3ad.

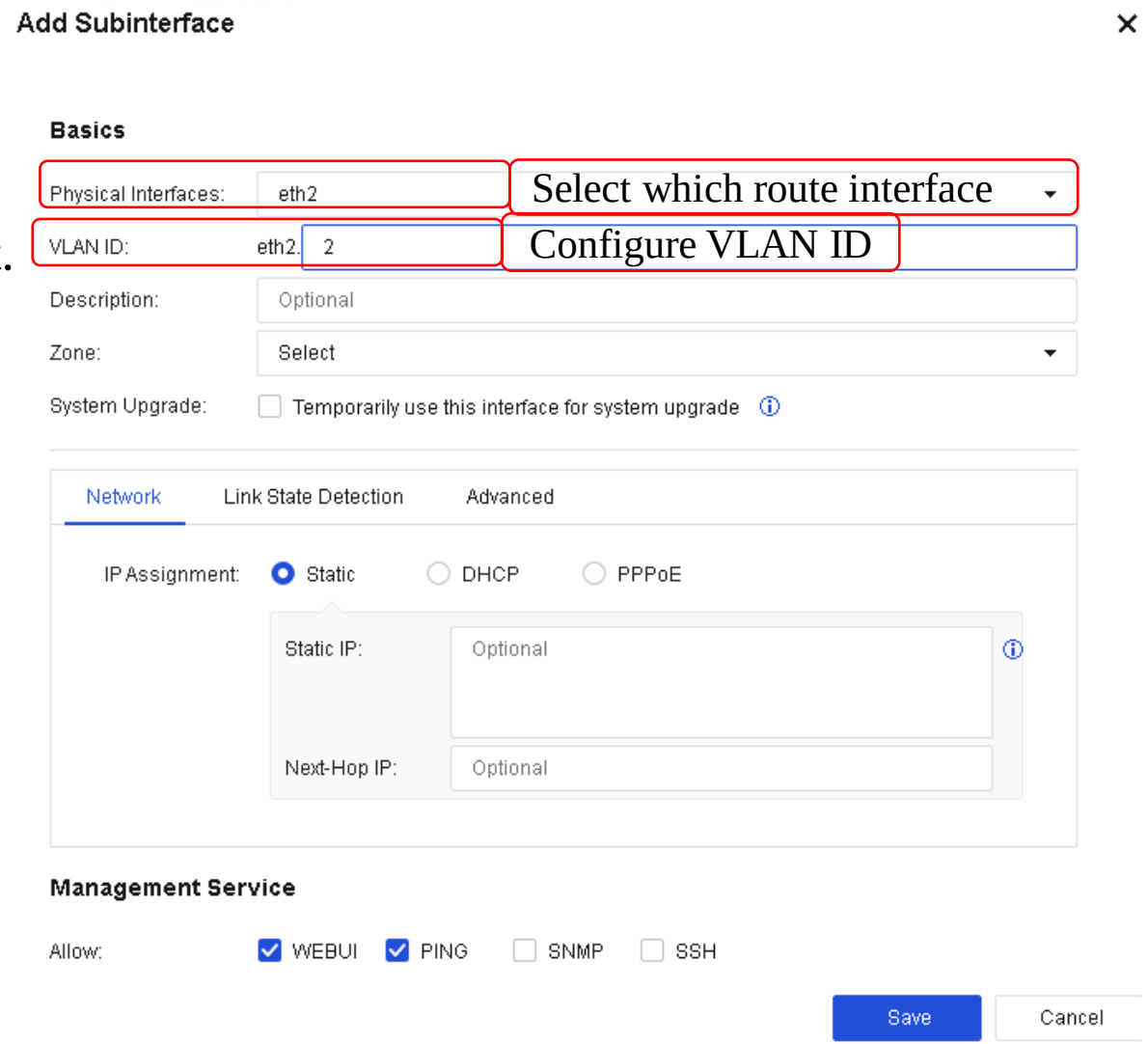
Noted: If the LACP mode of both ports of the device is in passive mode, the aggregation relationship cannot be established.



Sub-Interface

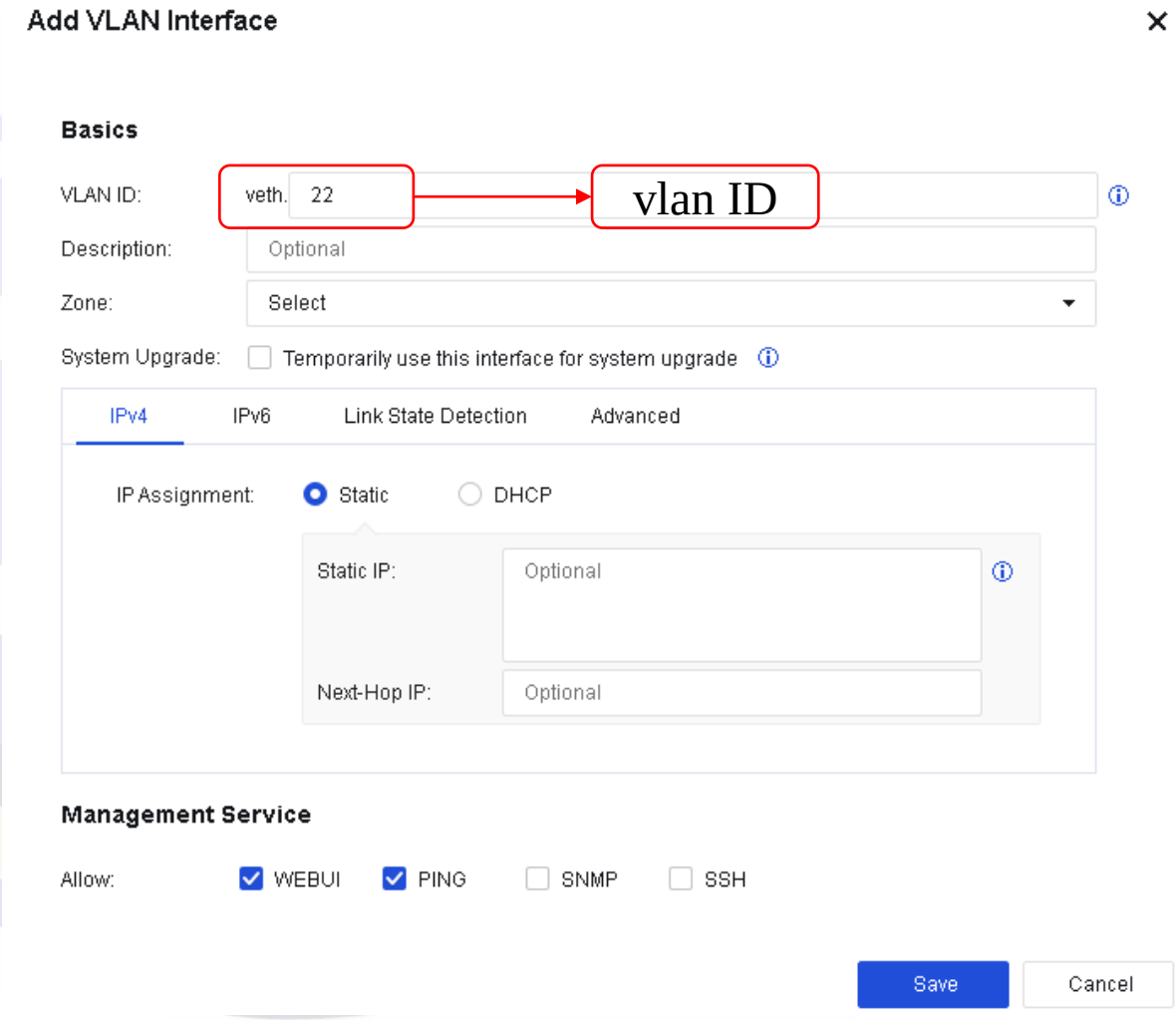
Sub interface:
Sub interface apply on when route interface connect on VLAN TRUNK port.

Sub interface is logical interface and can only add under route interface.



VLAN interface

VLAN Interface:
Create IP address for VLAN, this is logical interface.



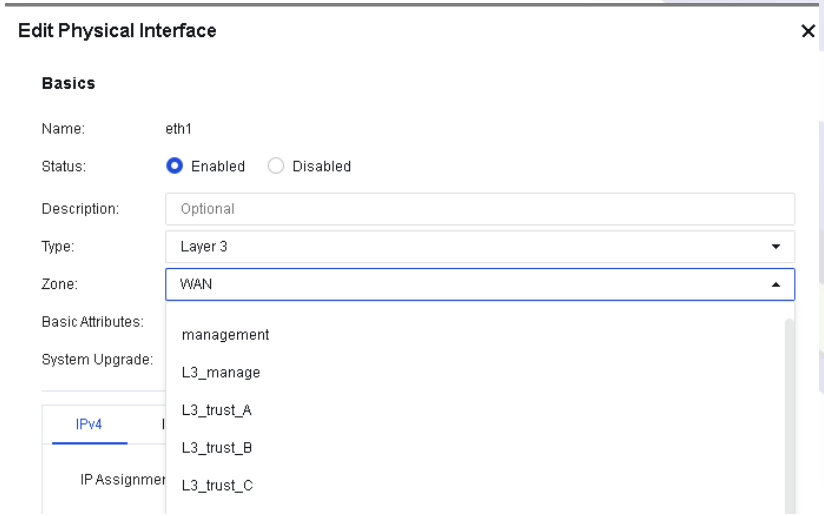
Interface Precautions

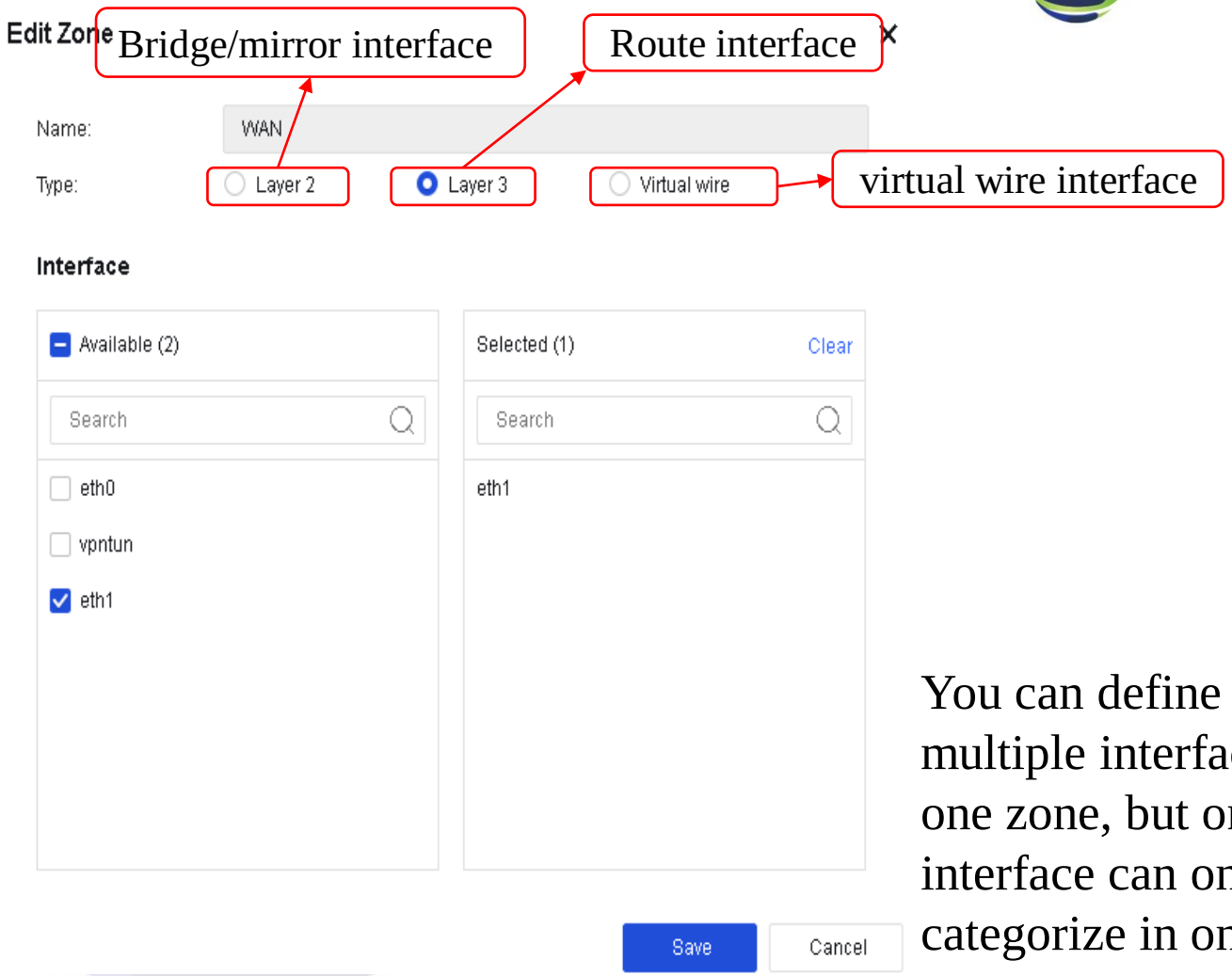
1. NGAF can support multiple WAN attribute interface.
2. Management interface does not support configure as bridge or virtual wire interface. If customer wants to deploy as double bridge , then the device must have at least 5 physical interface.
3. A route interface can add in multiple sub-interface, route interface IP address & sub-interface IP address can’t conflict.
4. Only physical interface support IPv6.

Zone

Zone:
Use for defining & categorizing interface, policy are based on the zone.

You can add into the zone at the interface page.





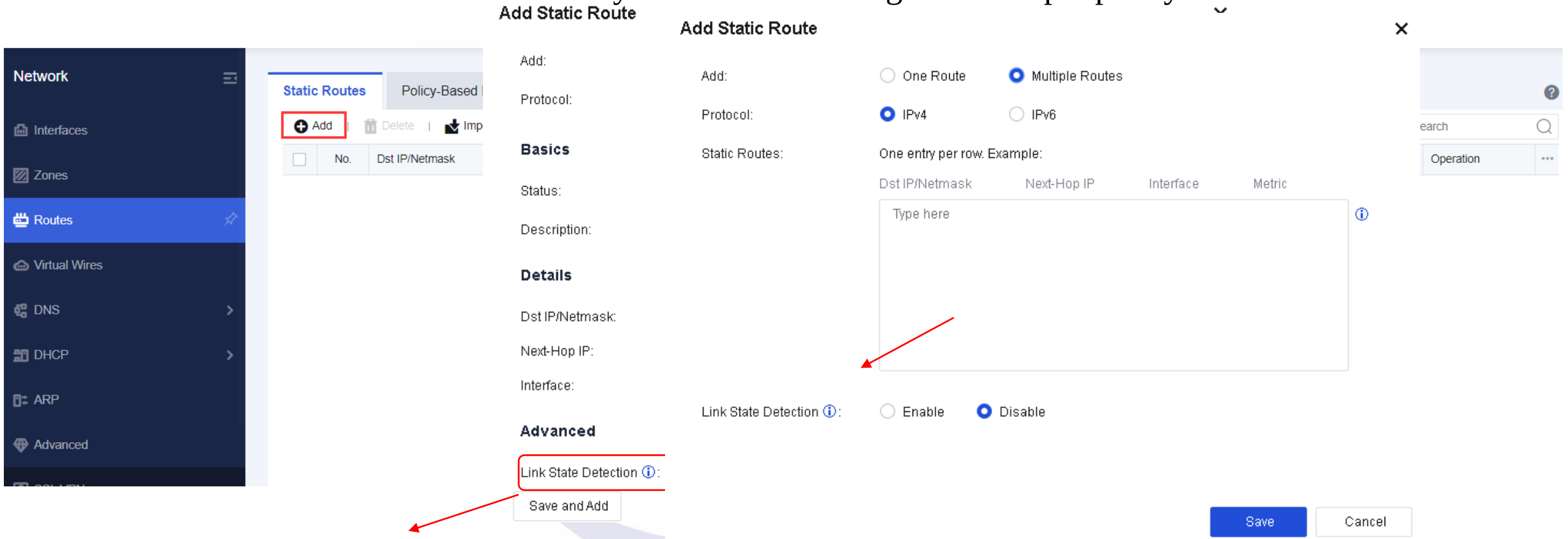
You can define multiple interface in one zone, but one interface can only categorize in one zone.

2 Routing

SANGFOR
深信服科技

Static Route

NGAF Static route need add in manually and can add in single or multiple policy in one time.



If enabled, status of the static route will be set to invalid and the route entry will be deleted from the corresponding routing table when link on the selected interface fails (determined by either Ping or DNS lookup).
It is recommended if this route is a floating static route.
Note: Make sure link state detection is enabled for the selected interface.

Multiple static routes is one entry per row and please follow the instruction and sample.

Policy-Based Routing

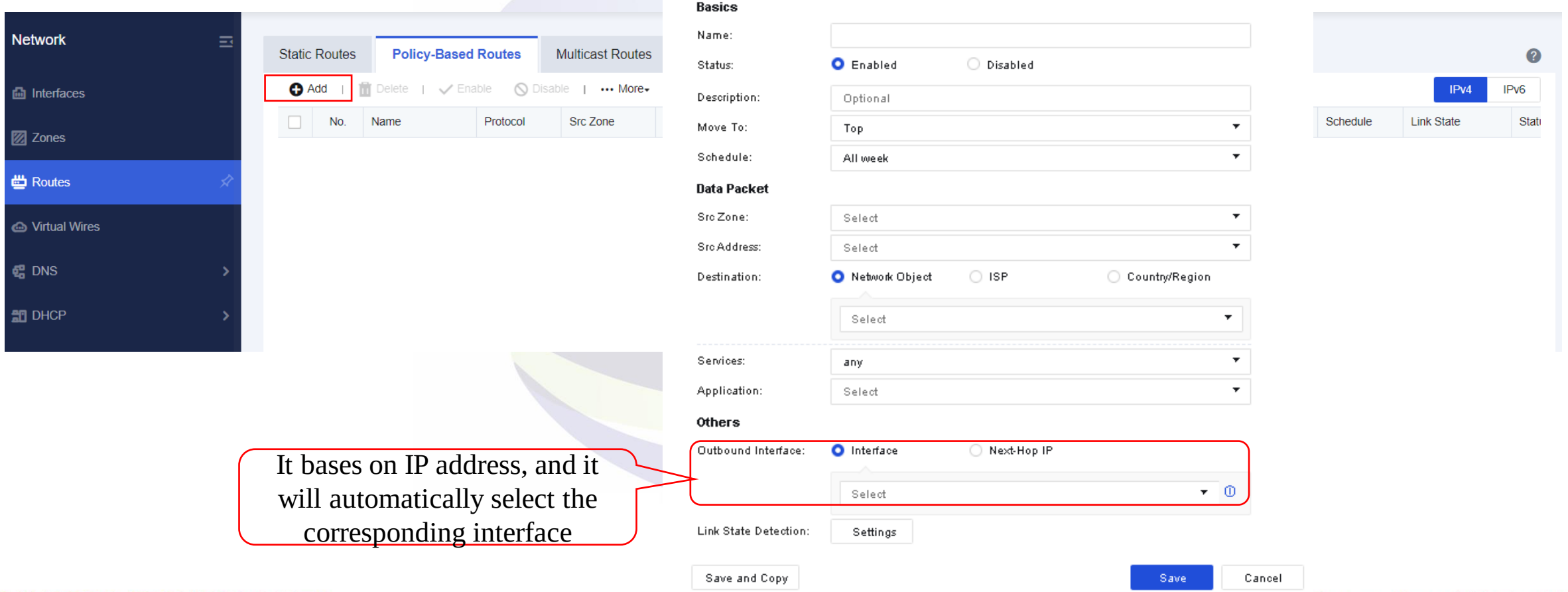
NGAF policy-based routing mainly for multi-WAN line, based on source/destination IP, port, and application to route traffic.

PBR common scenario:

1. Source based routing: Base on source IP address and protocol to select interface or next hop. Can achieve different network range of internal user access to internet via different WAN line.
2. Line load balance routing: Device have more than one WAN line, policy route can base on bandwidth proportion, weighted minimum bandwidth to select interface policy.
3. Application: Base on application to select WAN line.

Policy-Based Routing

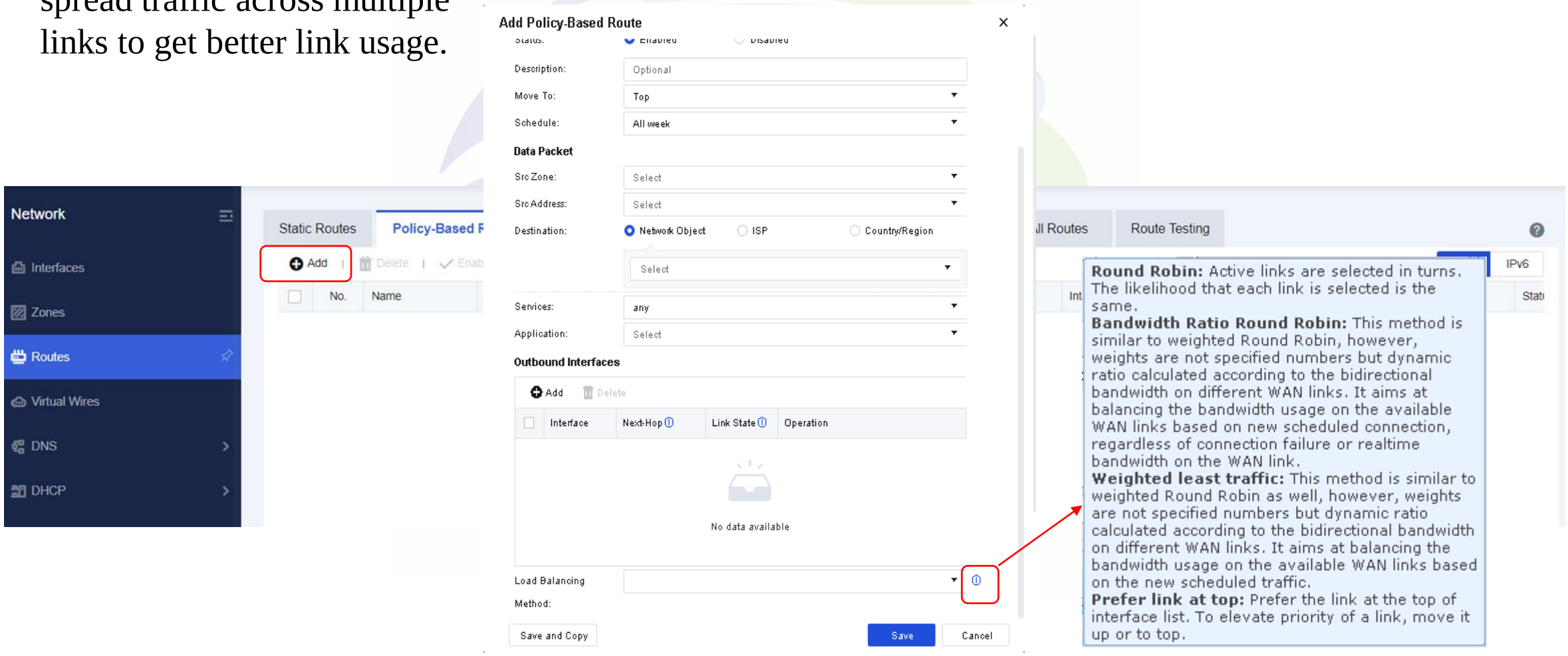
Source-Based Route:
Based on source IP address and protocol to select interface or next hop IP address.



It bases on IP address, and it will automatically select the corresponding interface

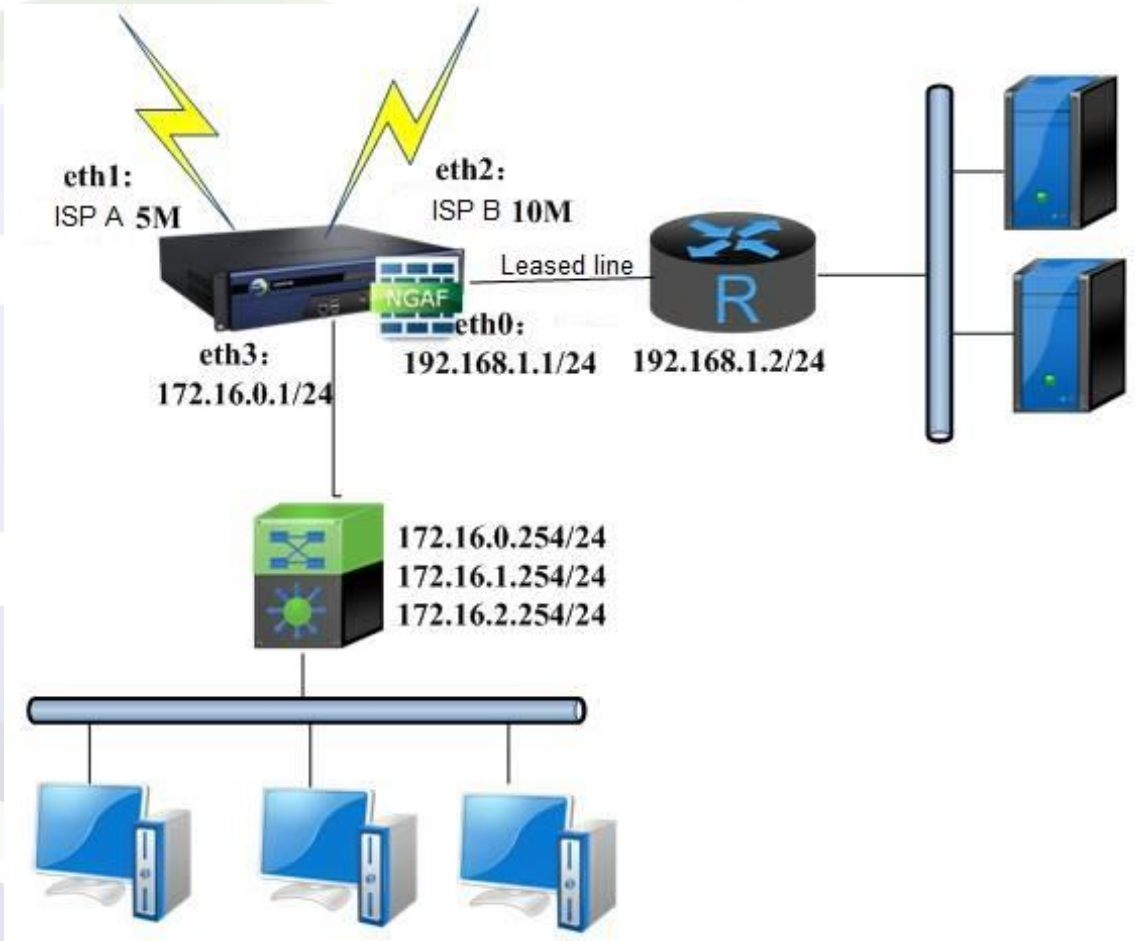
Policy-Based Routing

Link load-balancing route:
spread traffic across multiple links to get better link usage.



Policy-Based Routing Case Study

User scenario：
There are two ISP for internet.



User Requirement:
1. Internal user access to internet banking website (TCP 443) need go through ISP B.
2. Internal user access to internet need to select internet line base on bandwidth proportion left automatically.

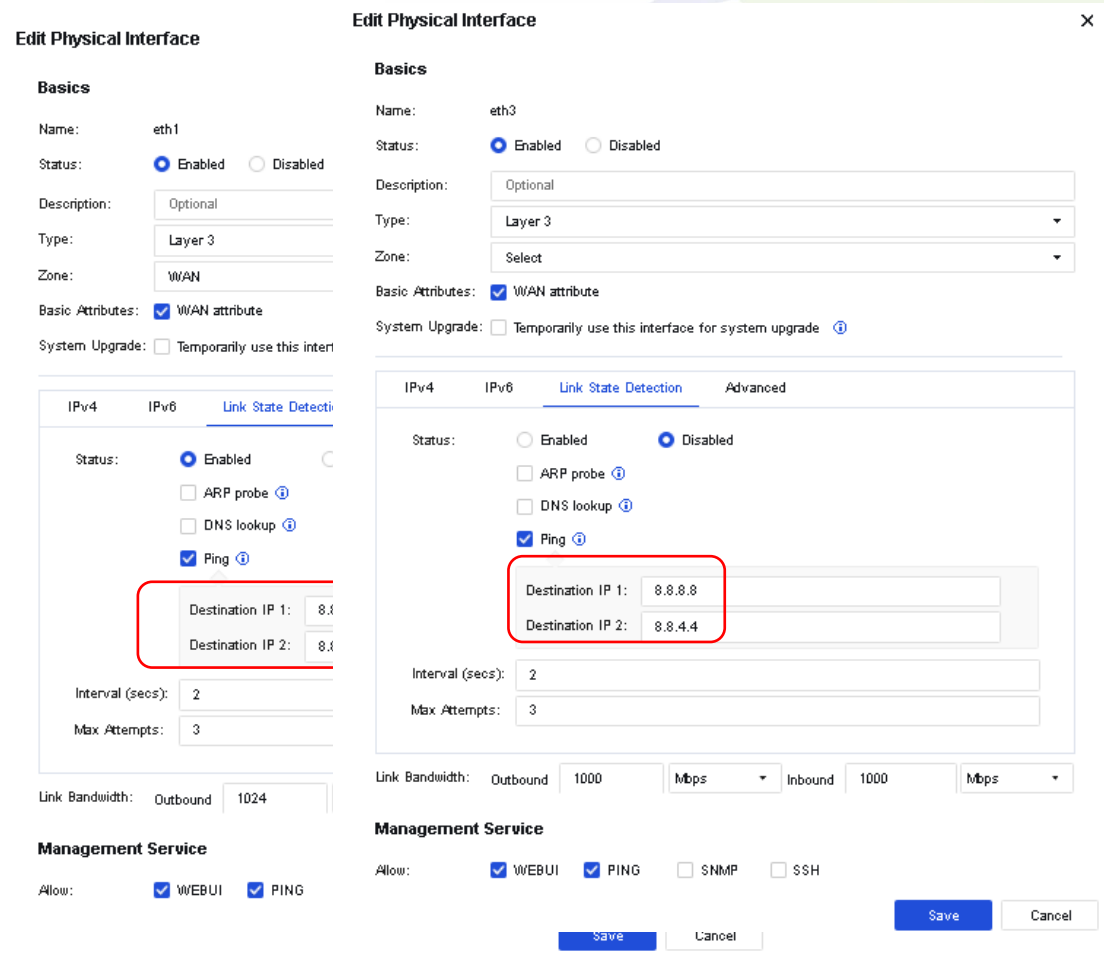
Policy-Based Routing Case Study

Configuration：

1. **Interface & Zone configuration：**
   - Interface that connect to internet which is Eth1 and Eth2 need configure as WAN attribute route interface, Next-Hop IP, line bandwidth and enable link state detection, add Eth1 and Eth2 in the WAN zone.
   - Define “LAN Zone” , configure eth3 to “LAN Zone”.
2. **Policy Route configuration**
   - Add source-base route, source select “LAN Zone”, destination IP select all, destination port: TCP 443, select interface eth2.
   - Add a load balance route, source “LAN Zone”, destination IP select all, interface select eth1 and eth2, load balance method select “weighted round robin”.
3. **Static Route configuration**
   - Add in a static route 0.0.0.0/0.0.0.0 , next hop IP point to eth2.
     (The purpose to add in static route is to prevent policy route failed , internal user still can access internet via static route.)

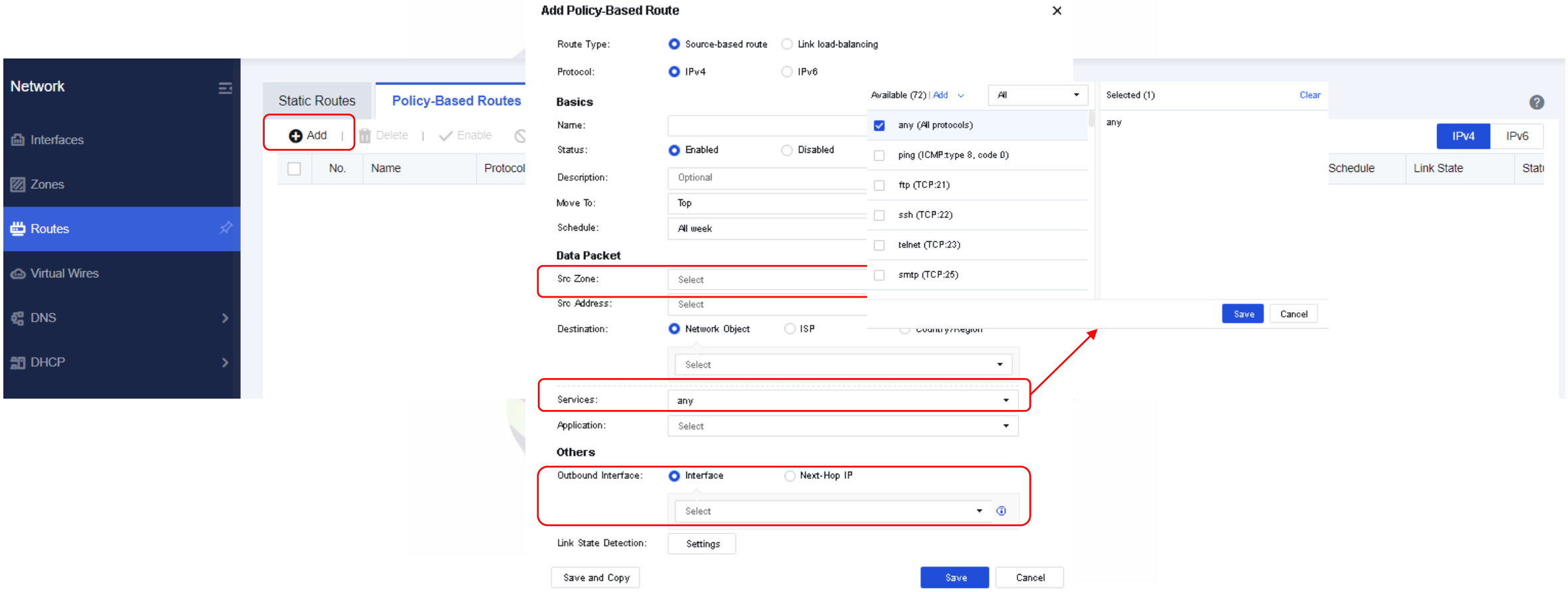
Policy-Based Routing Case Study

1. Interface & Zone configuration



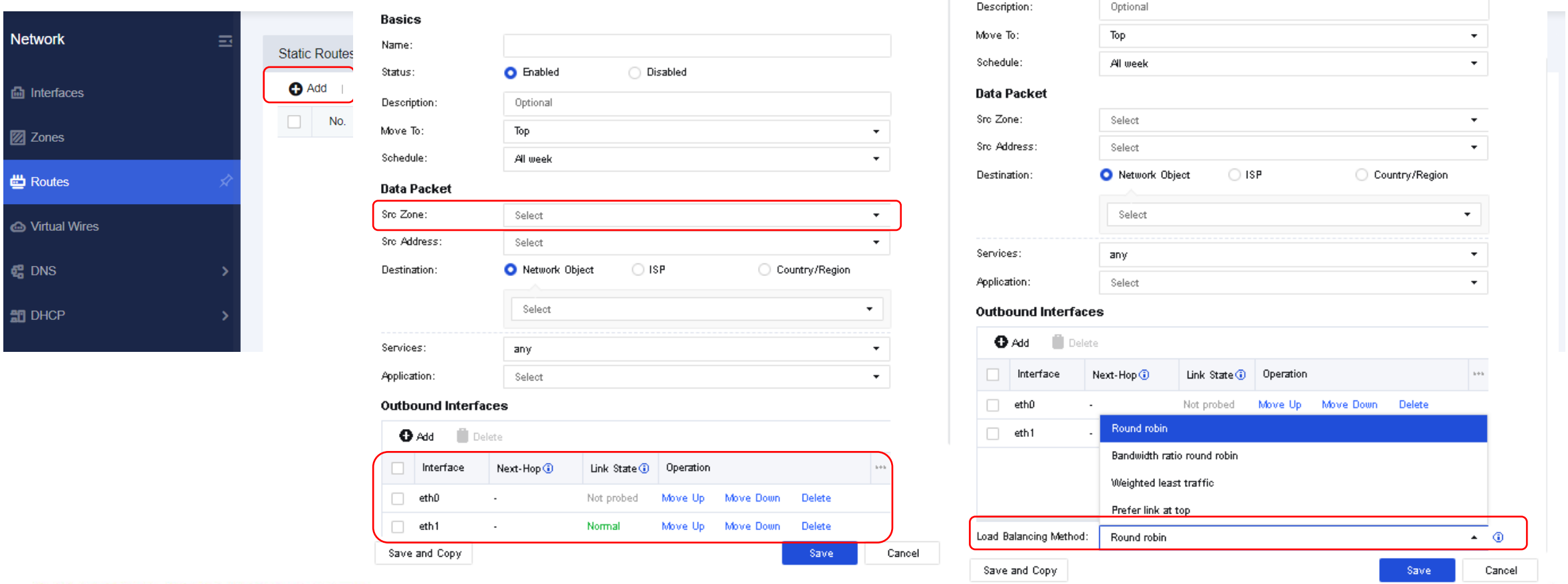
Policy-Based Routing Case Study

2.1 Add Source-based route



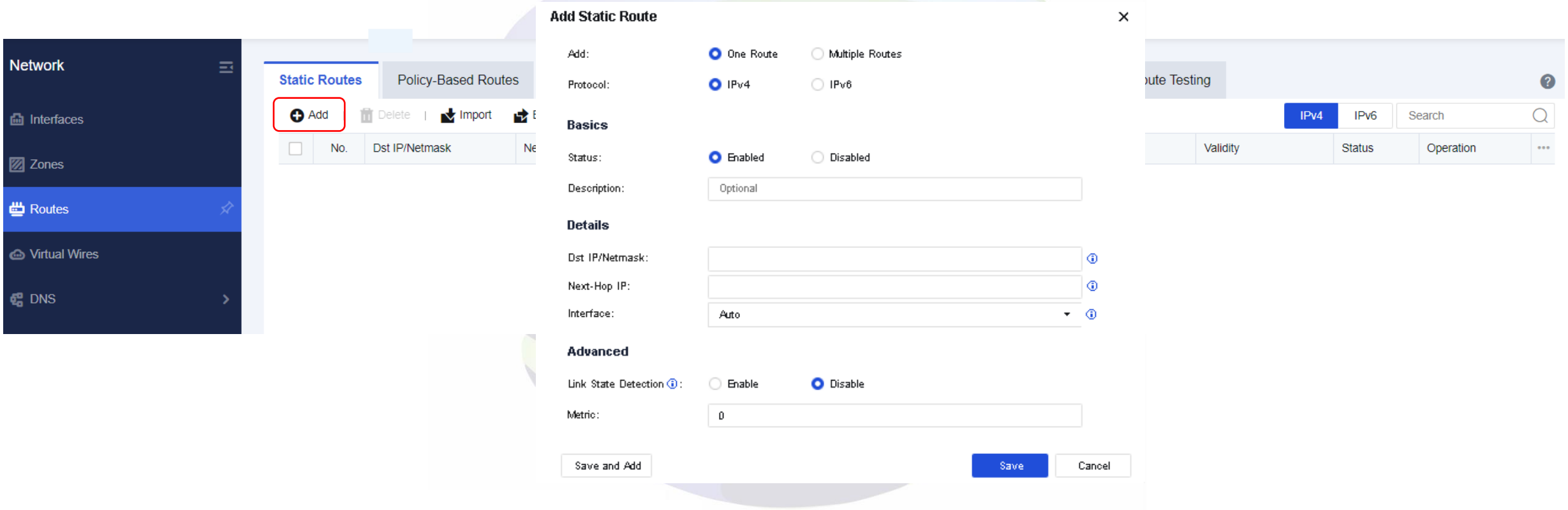
Policy-Based Routing Case Study

2.2 Add Link load-balancing route



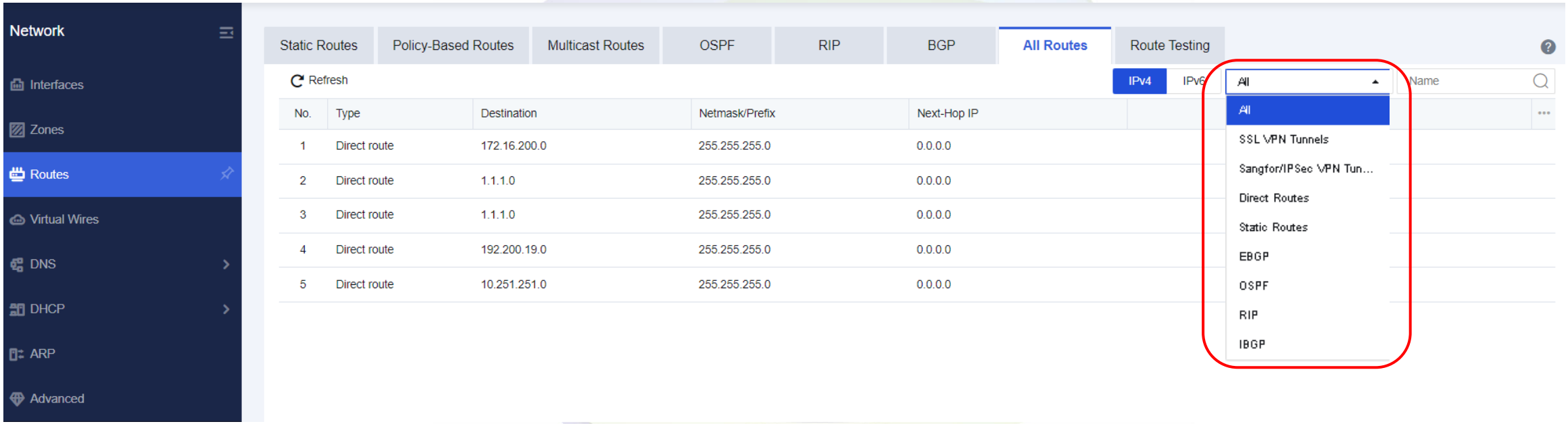
Policy-Based Routing Case Study

3. Add Static route



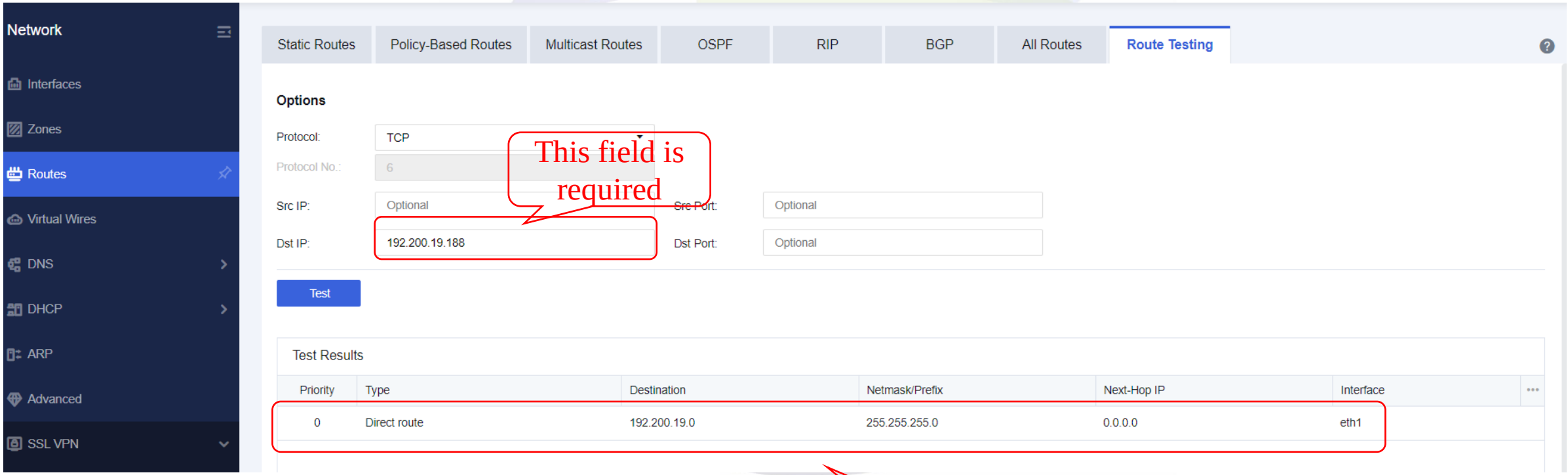
Display All routes

Display all routes.



Route Testing

Route Testing contains SSL VPN Route/IPSEC VPN Route/Static Route/Policy-based Route/Dynamic Route.



Route Precautions

1. Route priority from high to low: VPN route > static route > policy-based route > default route.
2. NGAF 6.8 version above added the new Passive VPN Tunnel function. After enable the function, the routing priority will change to: static route / dynamic route > policy route > VPN route > default route.
3. Source-based route can be used to forward data from the device's non-WAN attribute interfaces by directly filling in the next hop of the route.
4. Link load-balancing route interface must enable the link state detection function to achieve automatic line failure switching
5. Policy route is read from top to bottom.

3 NAT

SANGFOR
深信服科技

Network Address Translation

NAT:

Network Address Translation (NAT) is a service that modifies address, port, or both types of information within network packets as they pass through a computer or network device.

Depends on different scenarios, NAT can be divided as three types:

- **Source network address translation**
- **Destination network address translation**
- **Bidirectional network address translation**
- **NAT64 or NAT46**

Network Address Translation

Source NAT:

Source NAT is when private IP address access to public IP address (internet), translate the private IP address to public IP address. We can have more than one private IP address translate to one public IP address.

Typical applicable scenario:

Device deploy as route mode and as a gateway to allow internal user access internet.

Destination NAT:

Destination NAT changes the destination address of packets passing through the route or firewall.

Typical applicable scenario:

DNAT is typically used when an external (public) host needs to initiate a session with an internal (private) host.

Bidirectional NAT:

Bidirectional NAT is indicate in one NAT rules translate source and destination address.

Typical applicable scenario:

Internal user want to access internal server via Public IP address.

Network Address Translation

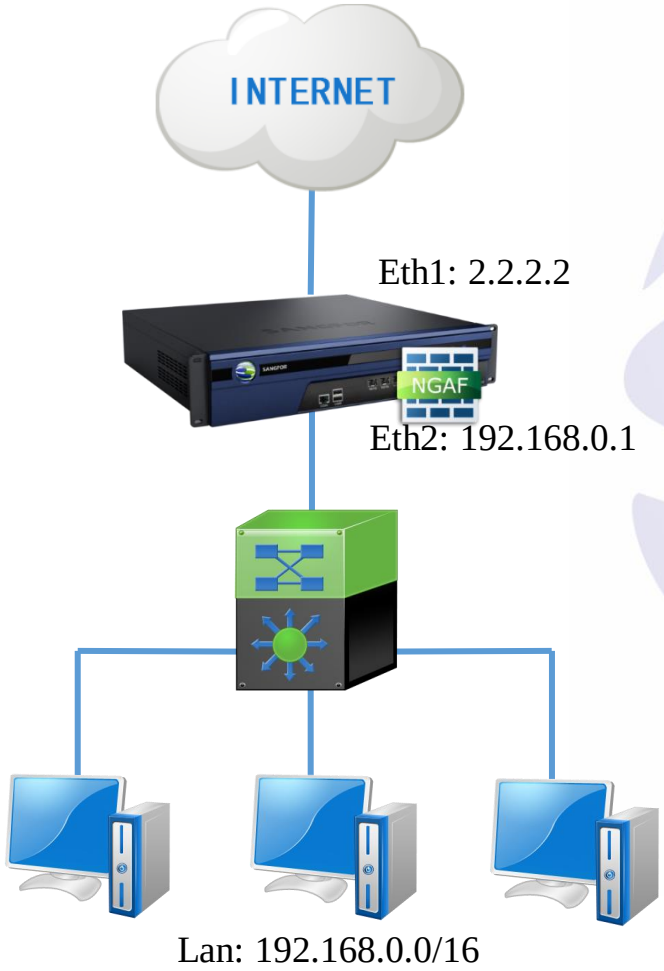
NAT64:

NAT64 is an IPv6 translation mechanism that facilitates communication between IPv6 and IPv4 hosts by using the form of Network Address Translation (NAT).

Typical applicable scenario:

The Intranet has an IPv4 server that now needs to be released to IPv6 addresses for access.

SNAT Case Study



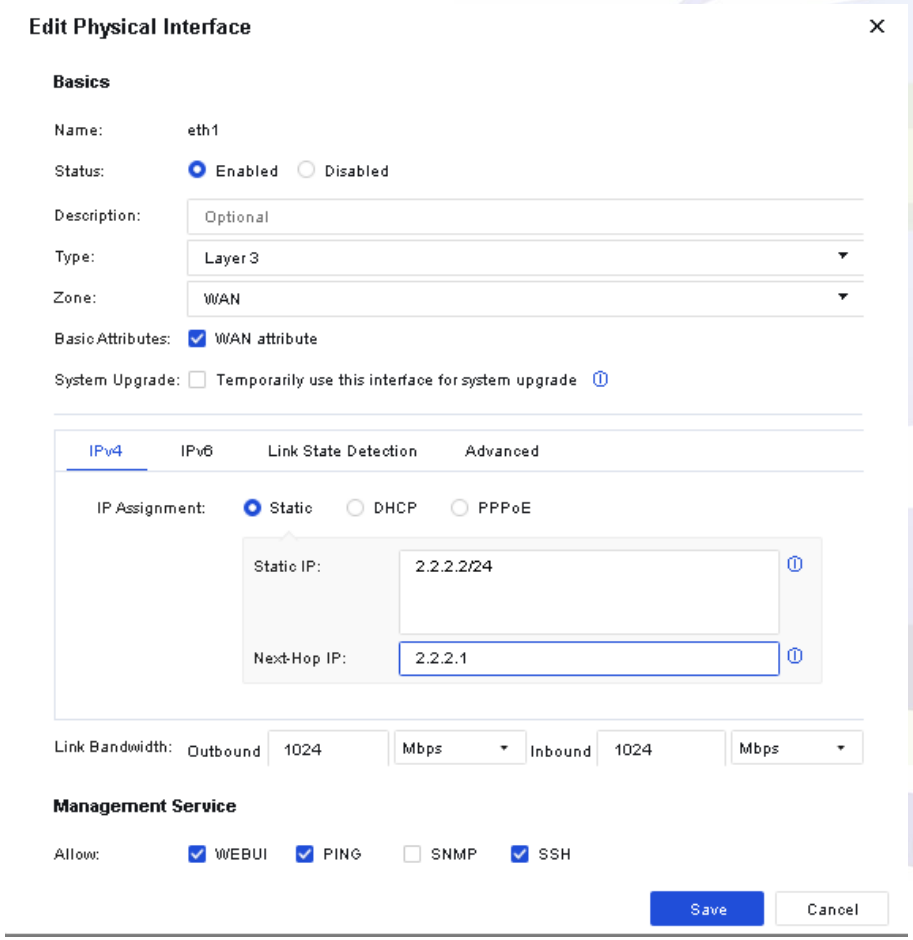
NGAF deploy as a internet gateway and connect a layer 3 switch. Internal network have PC and server.

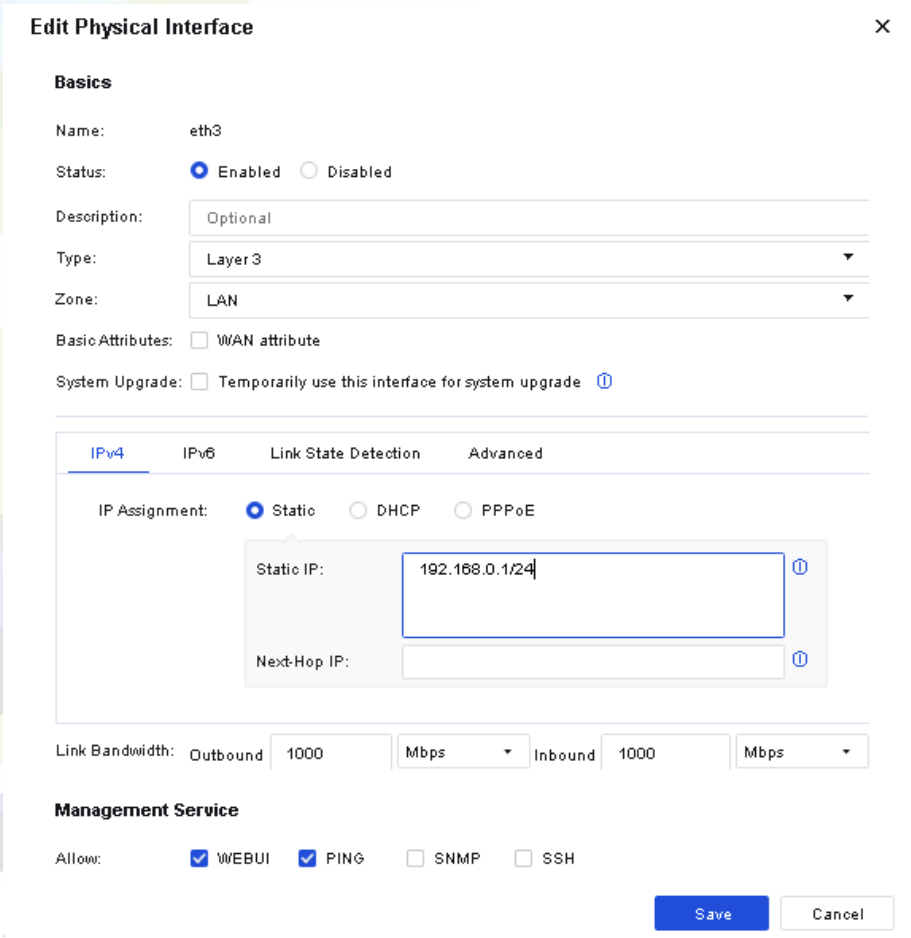
Requirement:
Internal PC and server need access internet by NGAF.

Solution: Configure SNAT on NGAF.

Source NAT Case Study

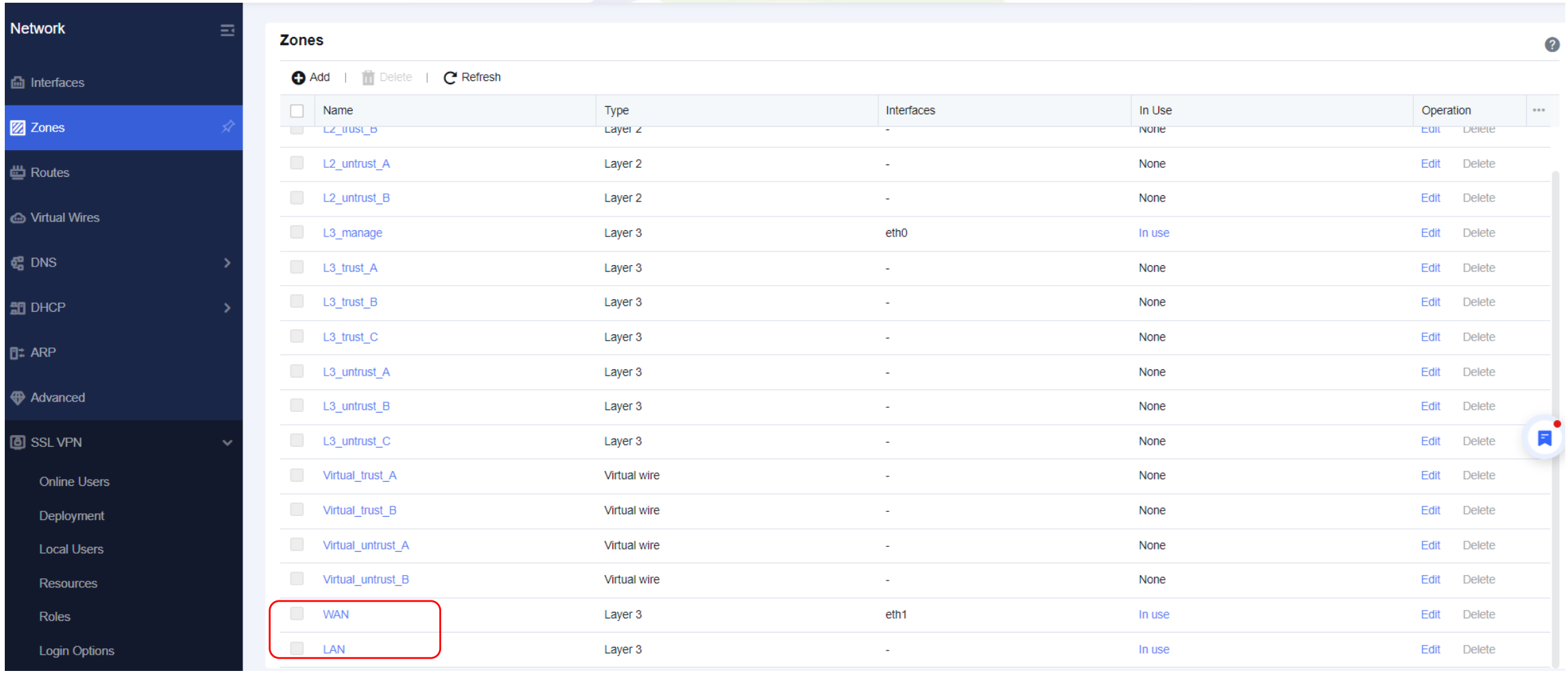
Step 1.1: Define interface, zone, route(omitted) and IP Group.





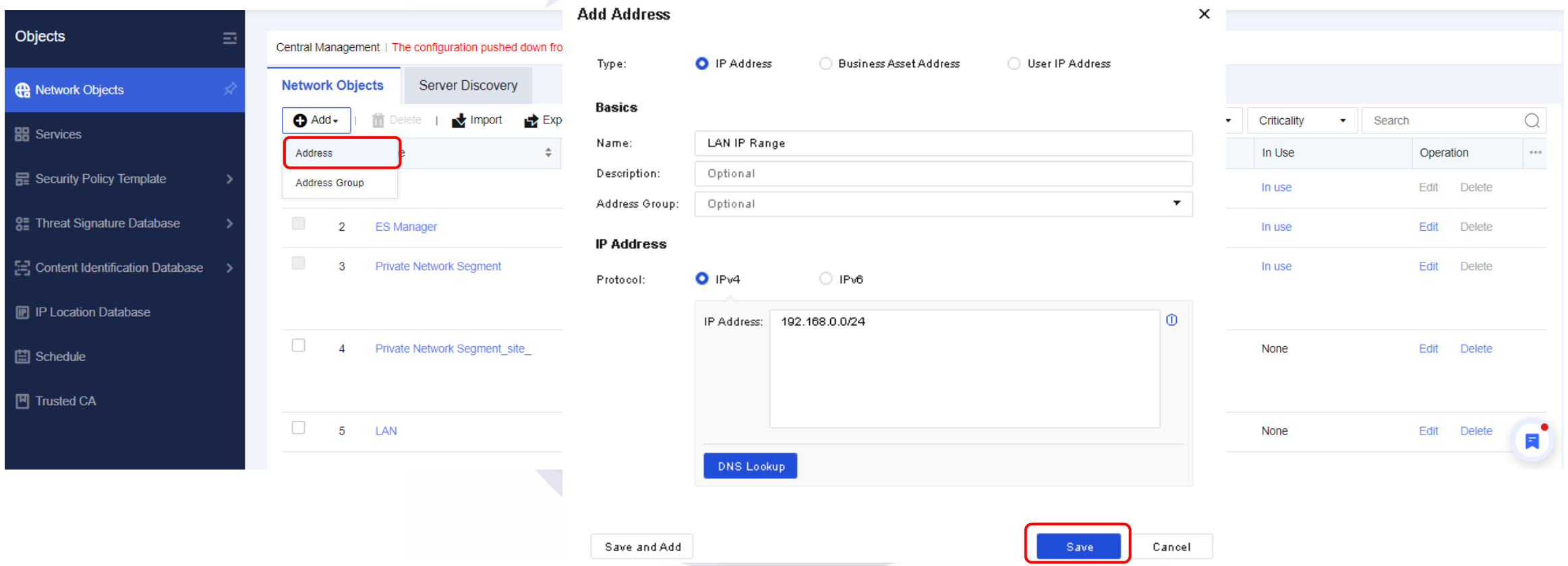
Source NAT Case Study

Step 1.2: Define interface, zone, route(omitted) and IP Group.



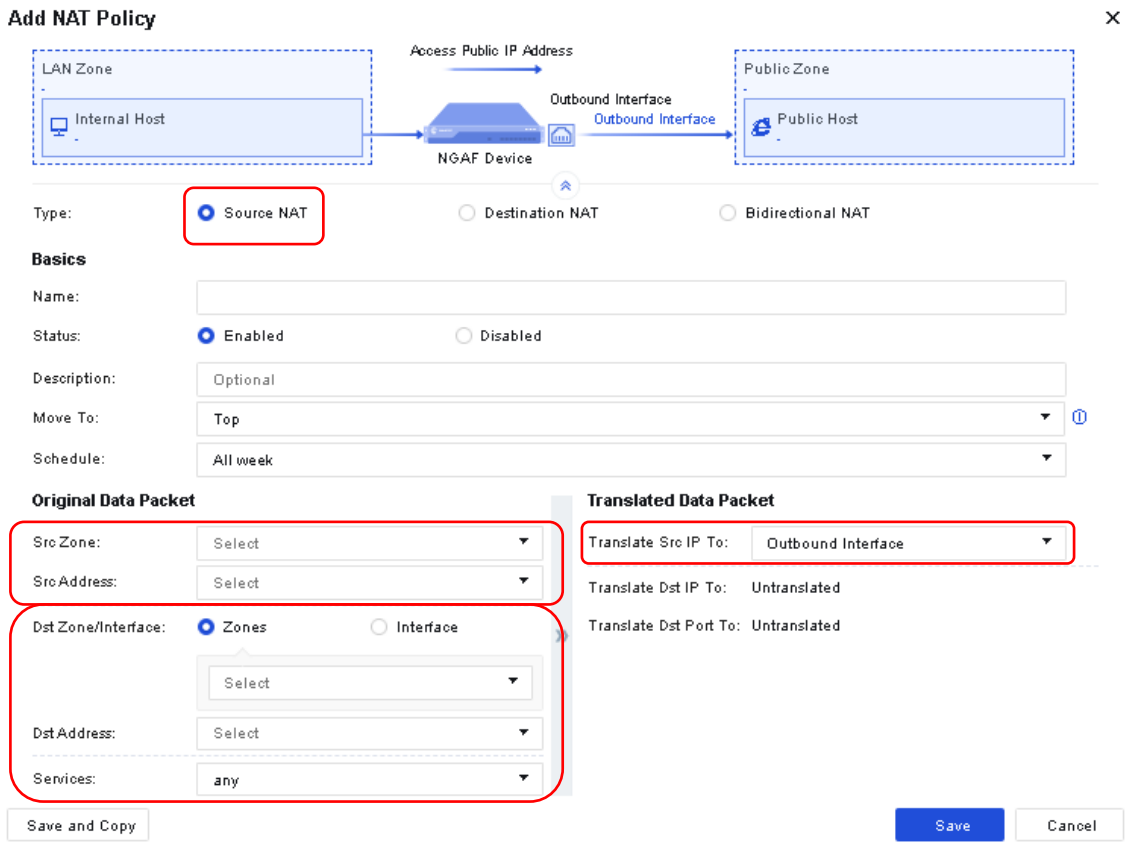
Source NAT Case Study

Step 1.3: Define interface, zone, route(omitted) and IP Group.

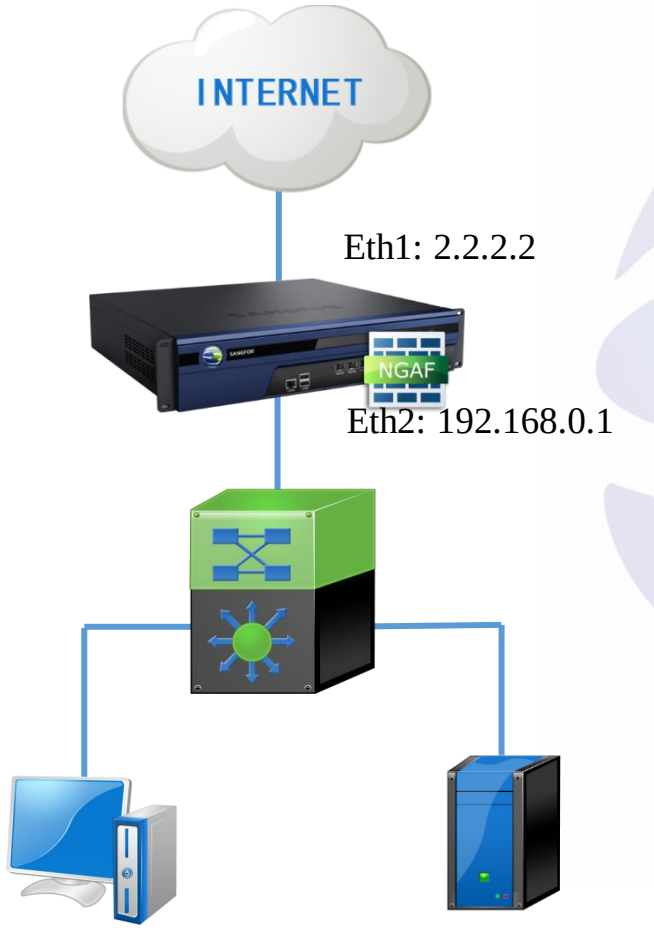


Source NAT Case Study

Step 2: Configure Source NAT.
Path: Policy > NAT



Destination NAT Case Study

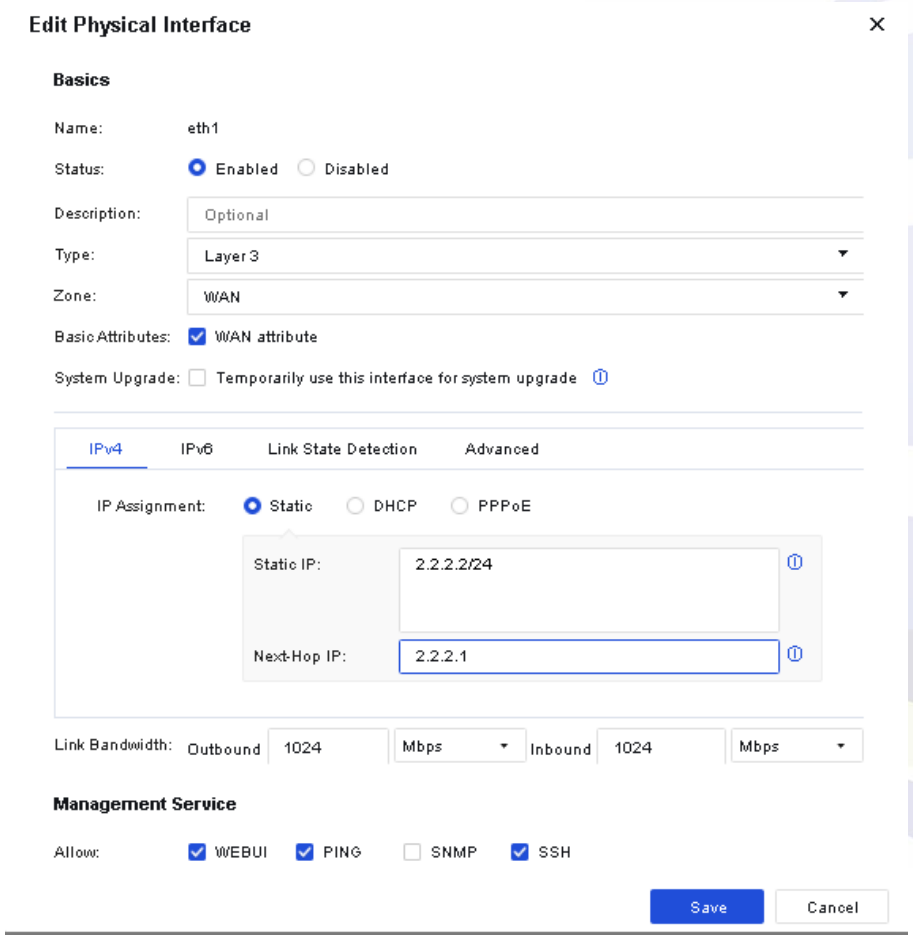


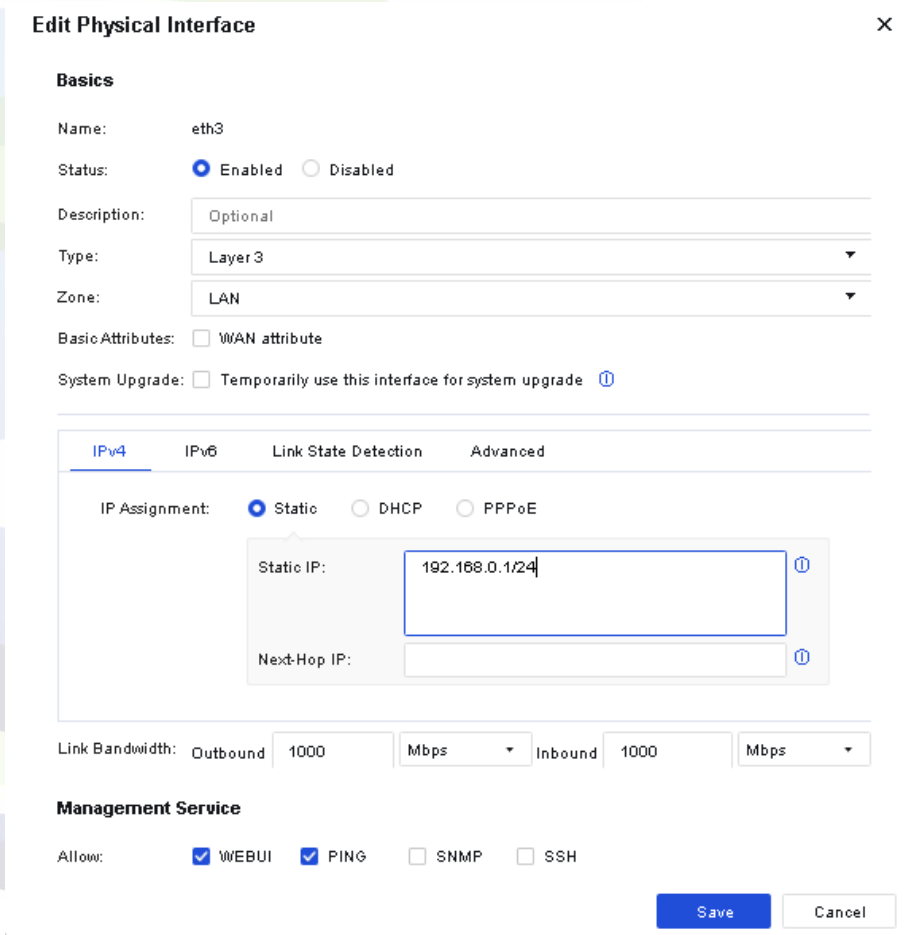
Requirement: NGAF deploy as internet gateway. Internal have a web server. Customer want to release web server to internet and external user can access web server by http://2.2.2.2.

Solution: Configure DNAT on NGAF.

Destination NAT Case Study

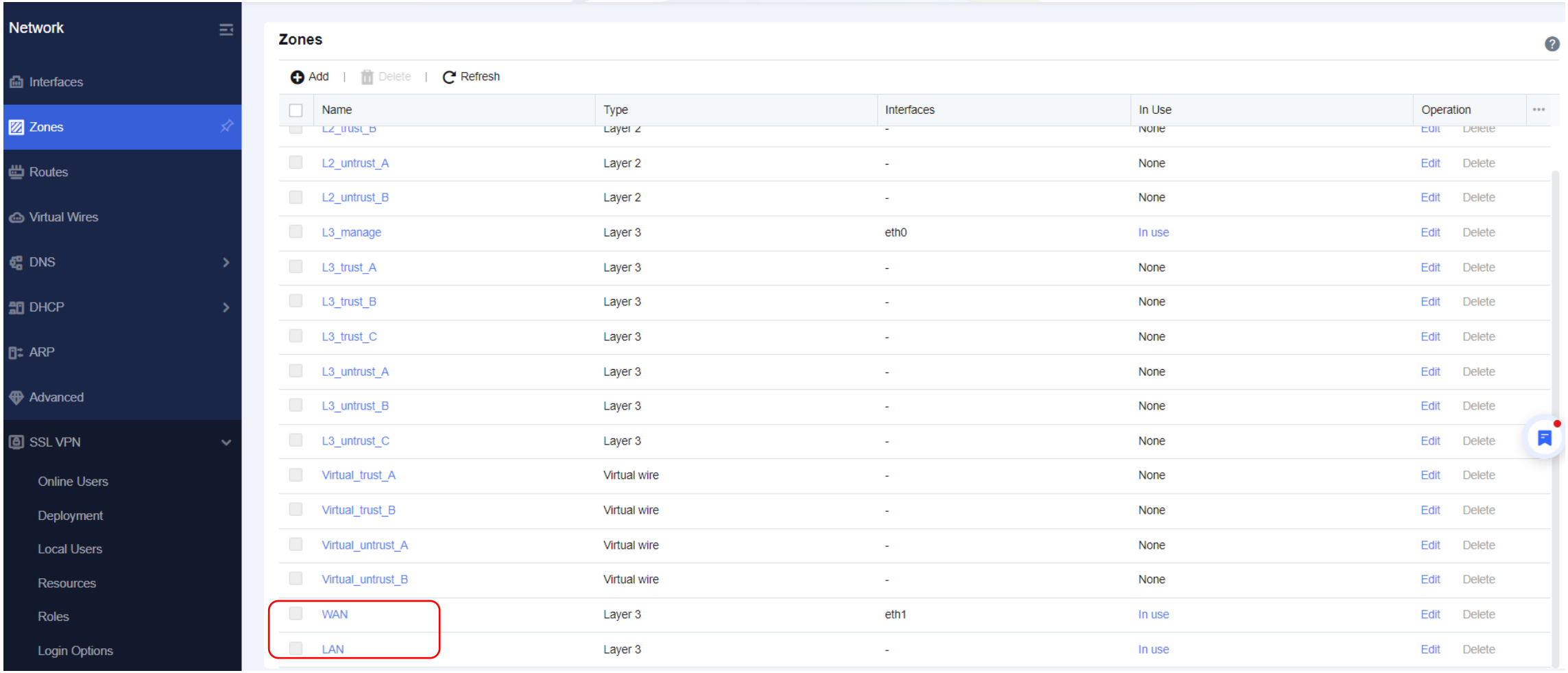
Step 1: Define interface, zone and route (omitted).





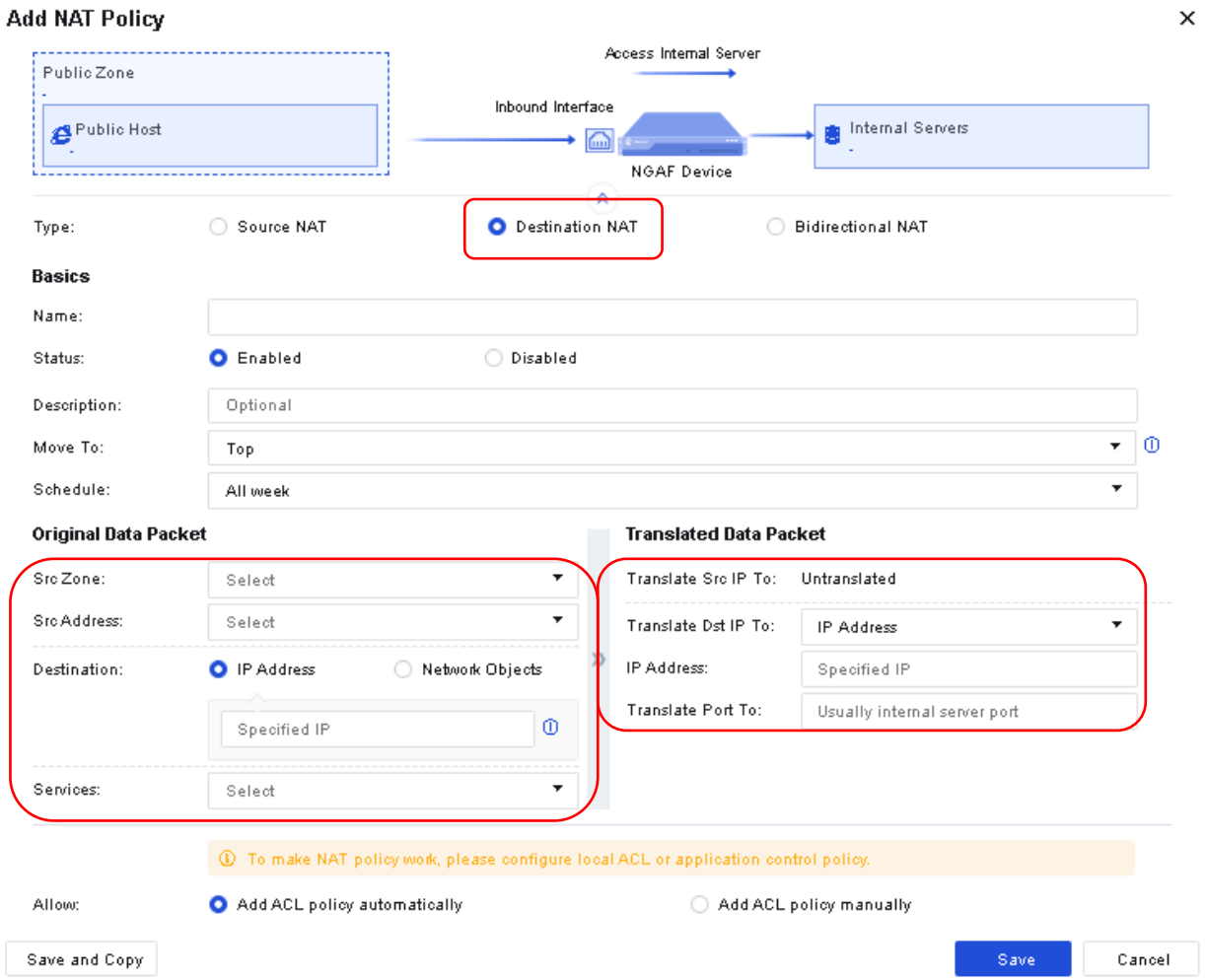
Destination NAT Case Study

Step 1.2: Define interface, zone and route (omitted).
Path: Network > Interface

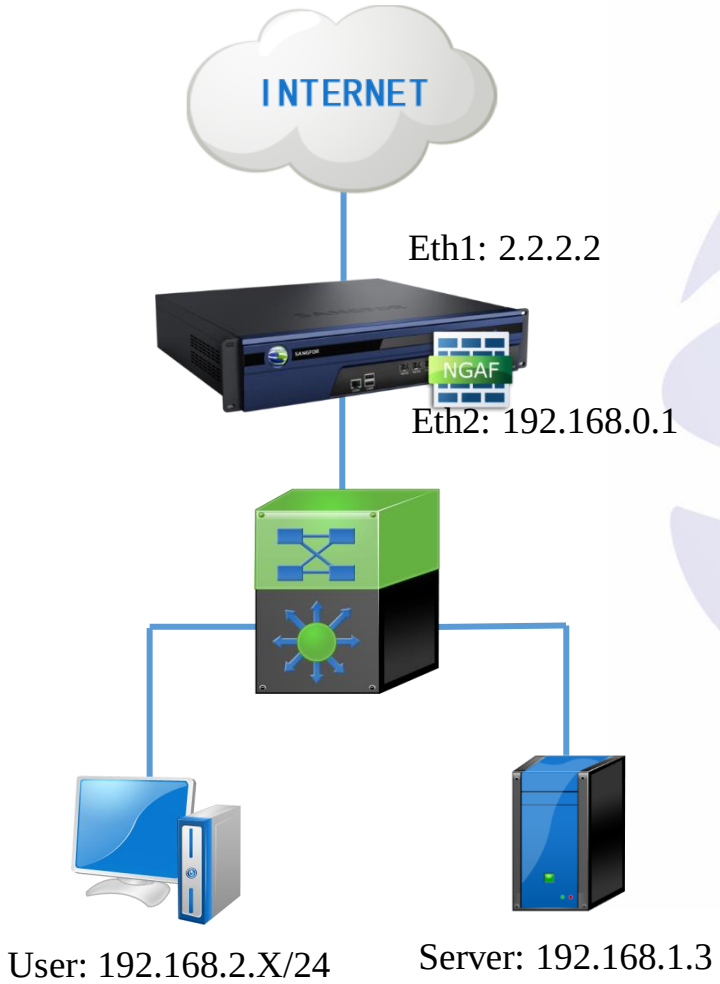


Network Address Translation

Step 2: Configure Destination NAT.
Path: Policy > NAT



Bidirectional NAT Case Study

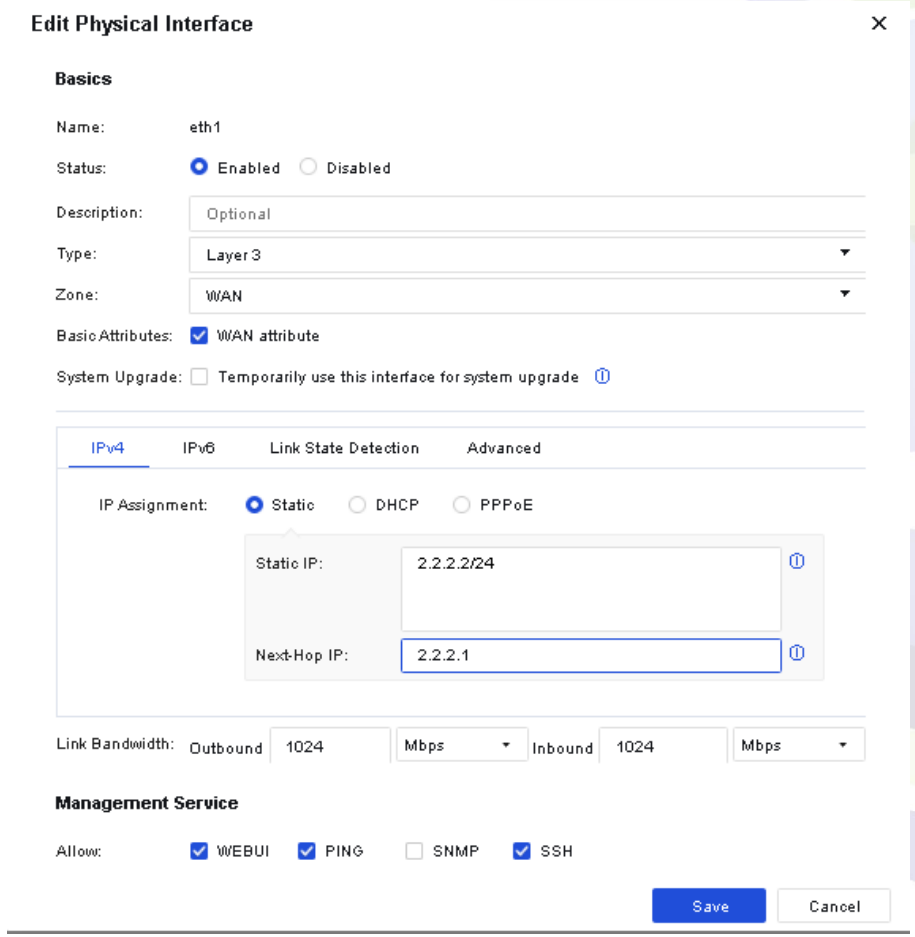


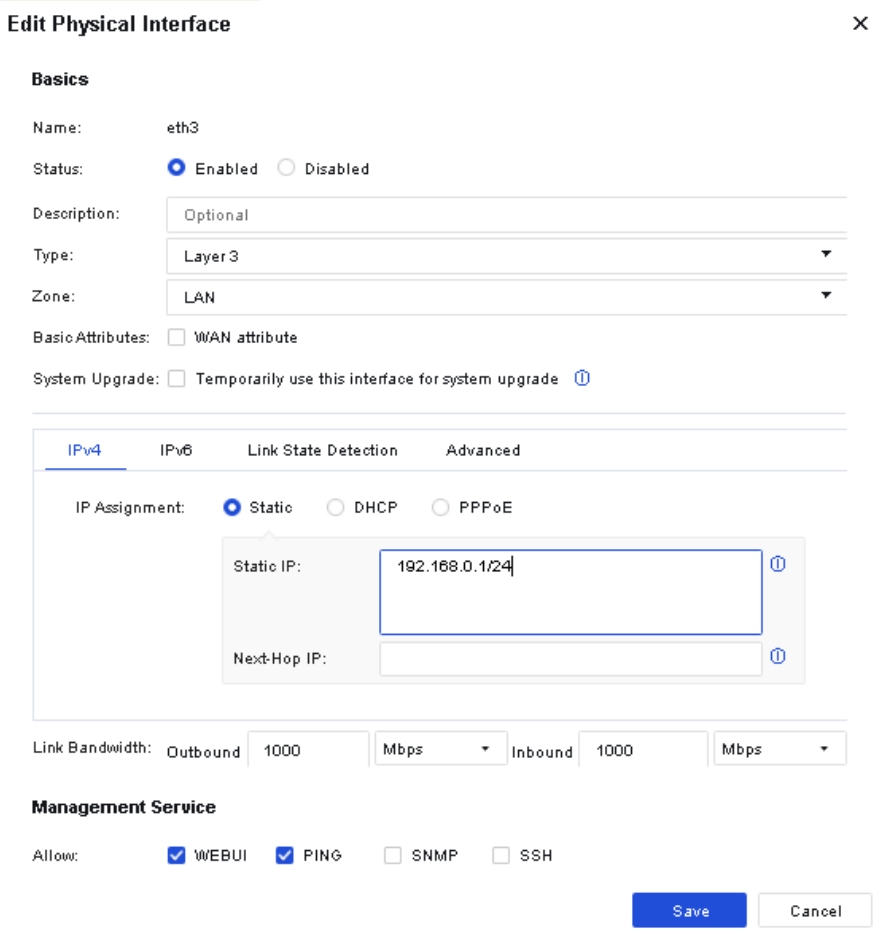
Requirement: NGFW deploy as internet gateway , internal have web server and customer had apply a domain name www.test.com and point to 2.2.2.2. Customer wants internal user to access web server via www.test.com.

Solution: Configure BNAT on NGAF.

Bidirectional NAT Case Study

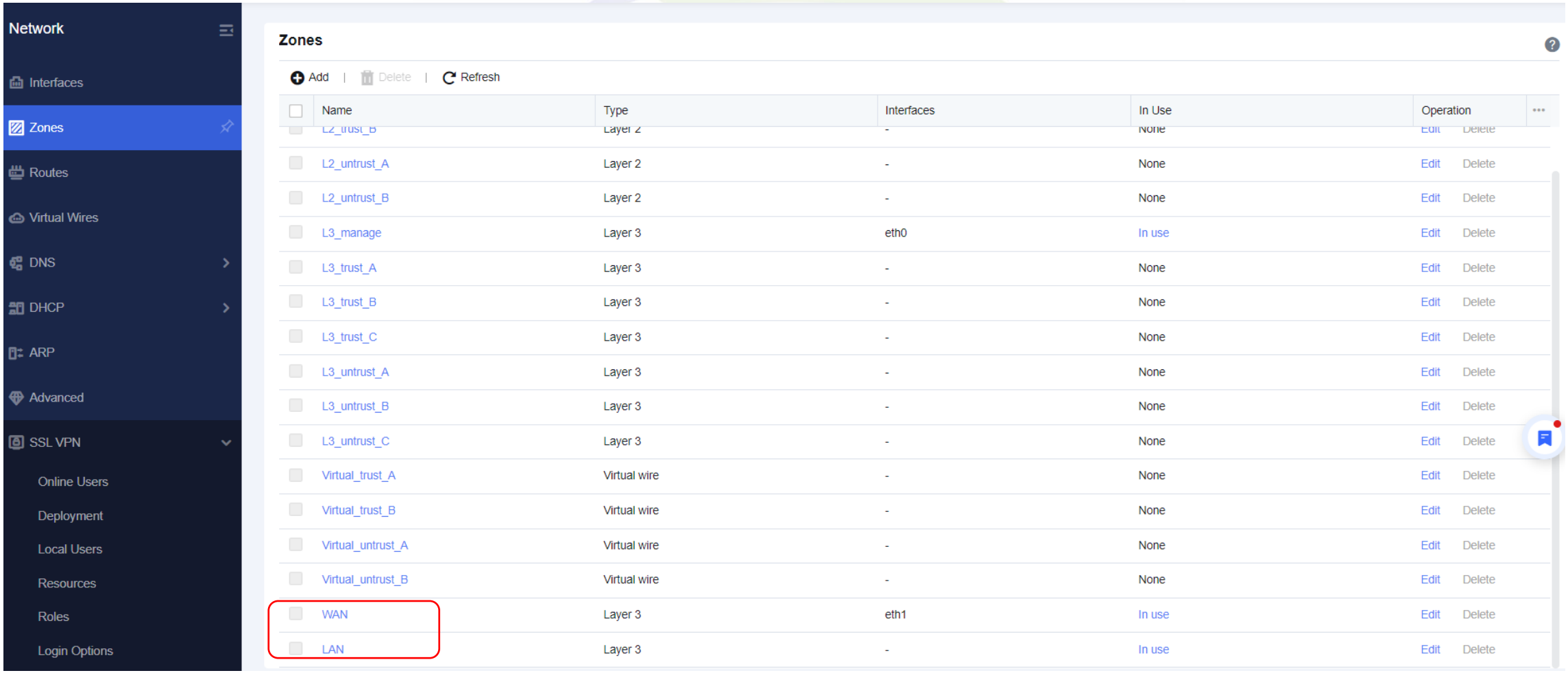
Step 1.1: Define interface, zone, route(omitted) and IP Group.





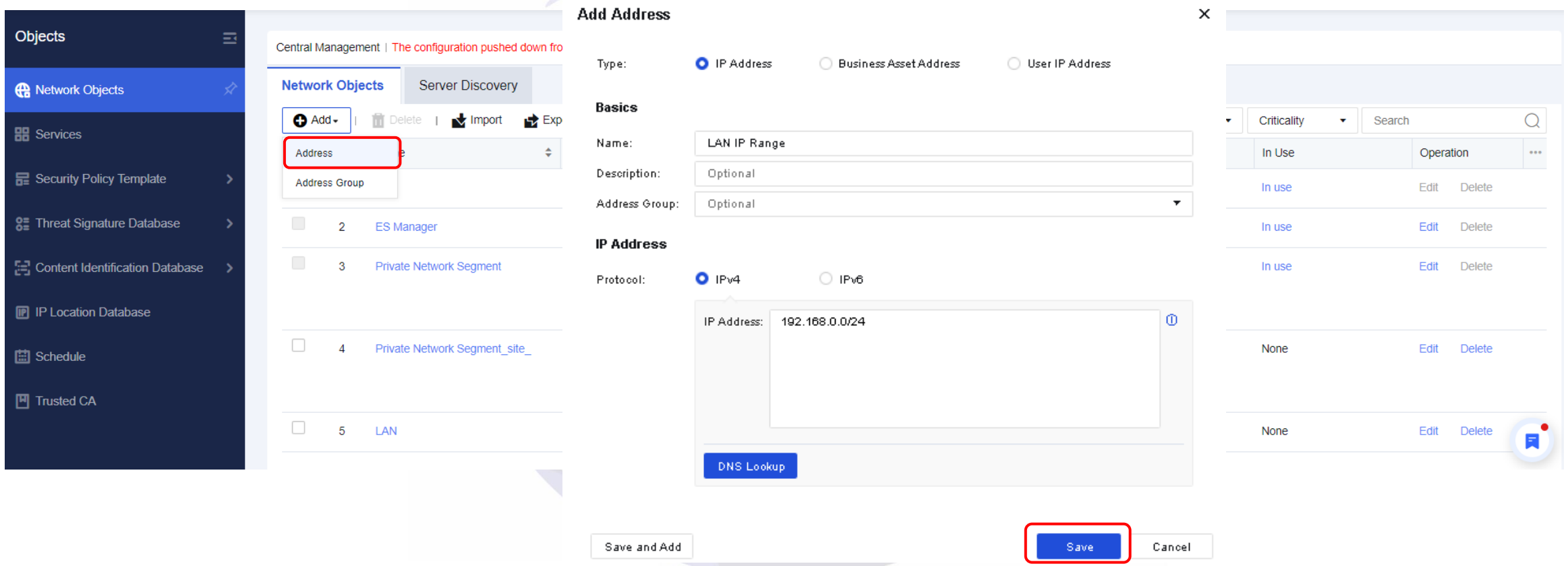
Bidirectional NAT Case Study

Step 1.2: Define interface, zone, route(omitted) and IP Group.



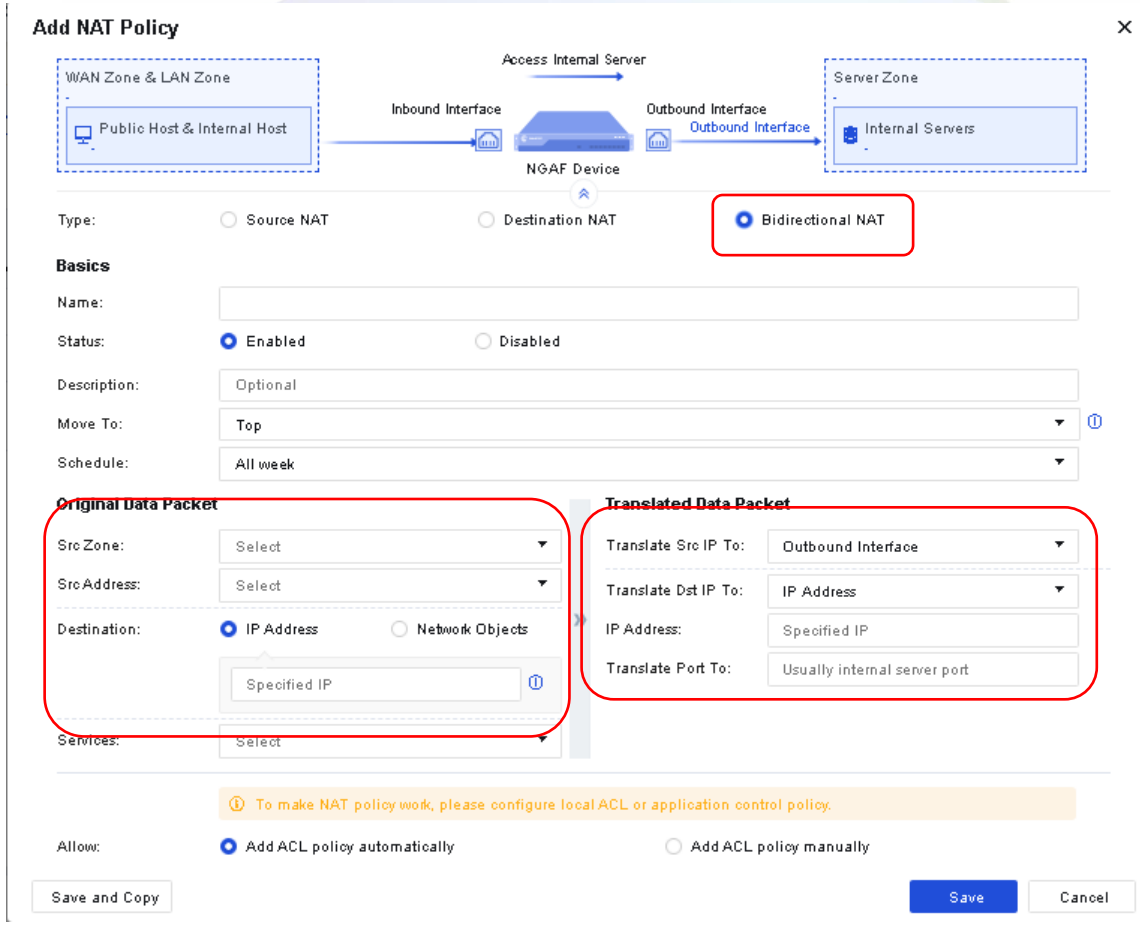
Bidirectional NAT Case Study

Step 1.3: Define interface, zone, route(omitted) and IP Group.

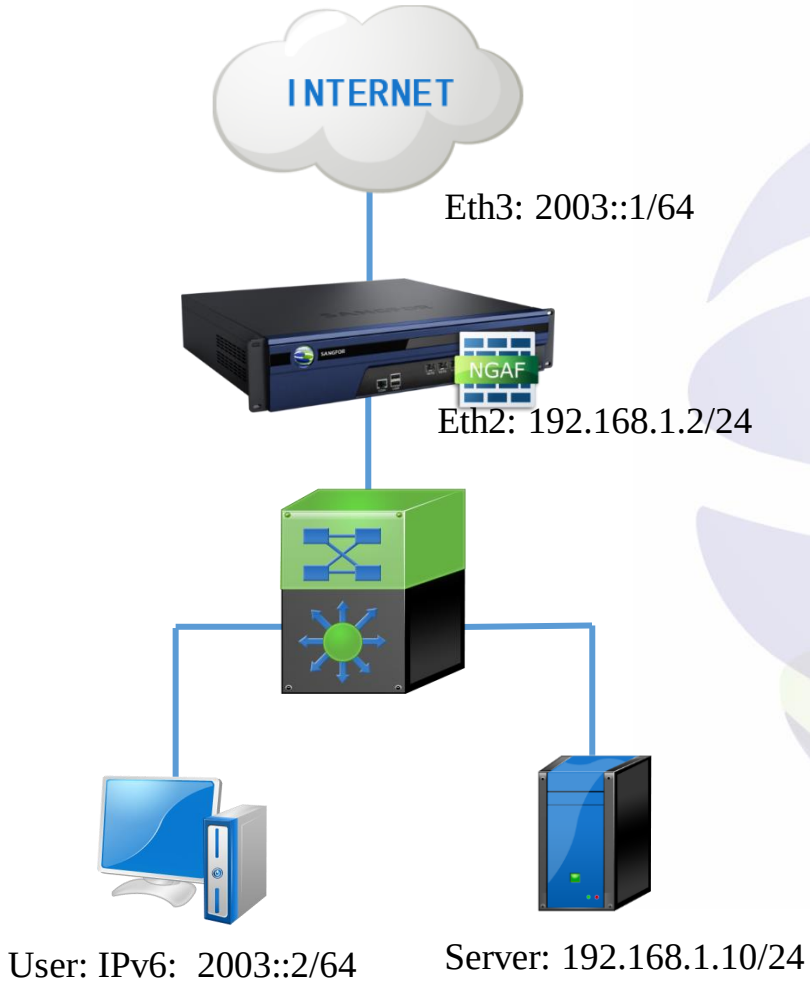


Bidirectional NAT Case Study

Step 2: Configure Bidirectional NAT.
Path: Policy > NAT



NAT64 Case Study



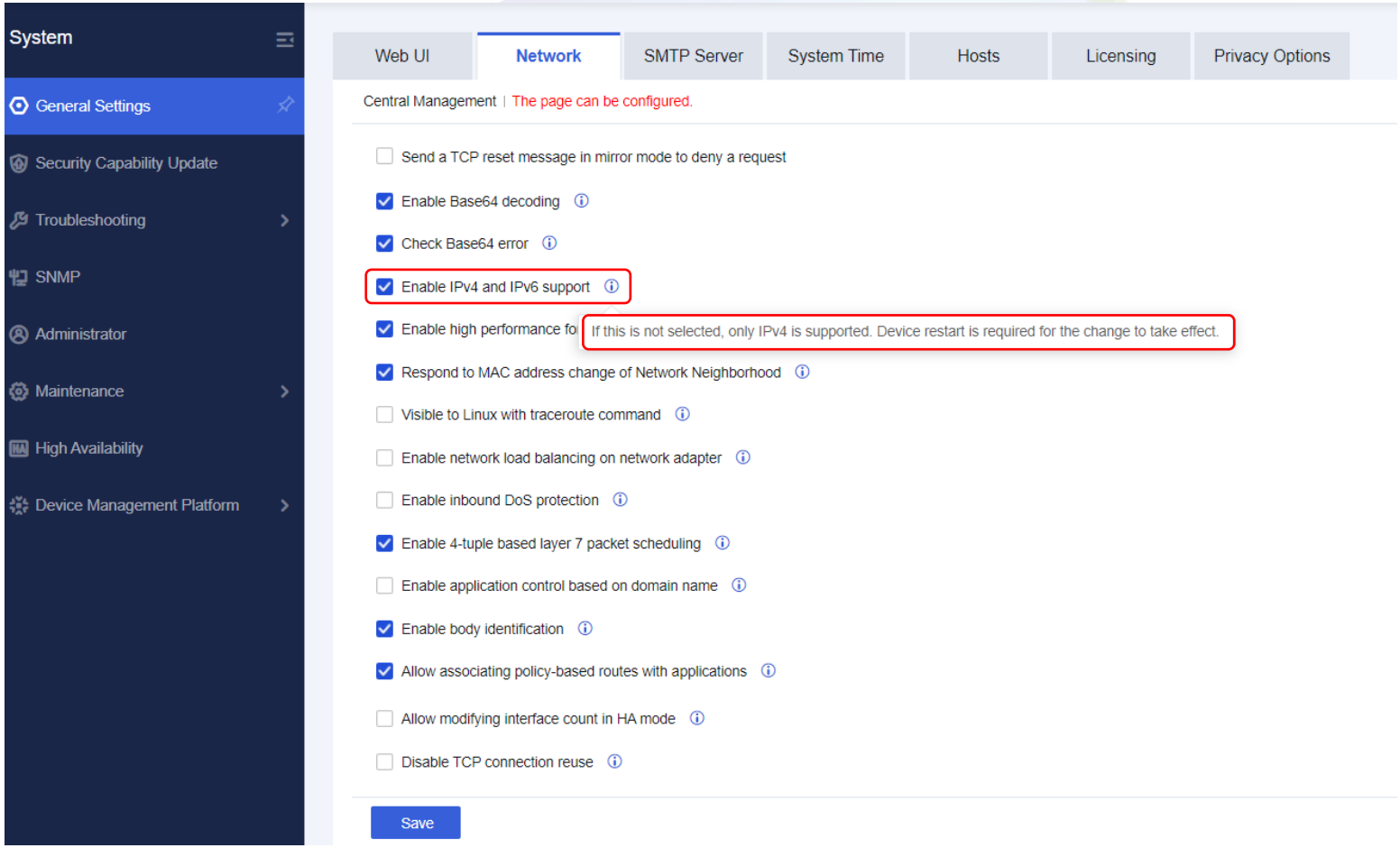
Requirement: LAN has an IPv4 server that now needs to be released to IPv6 addresses for access. IPv6 functionality involving NGAF is NAT's 6to4. At the same time, corresponding application layer protection should be done.

Solution: Configure DNAT 6 to 4.

NAT64 Case Study

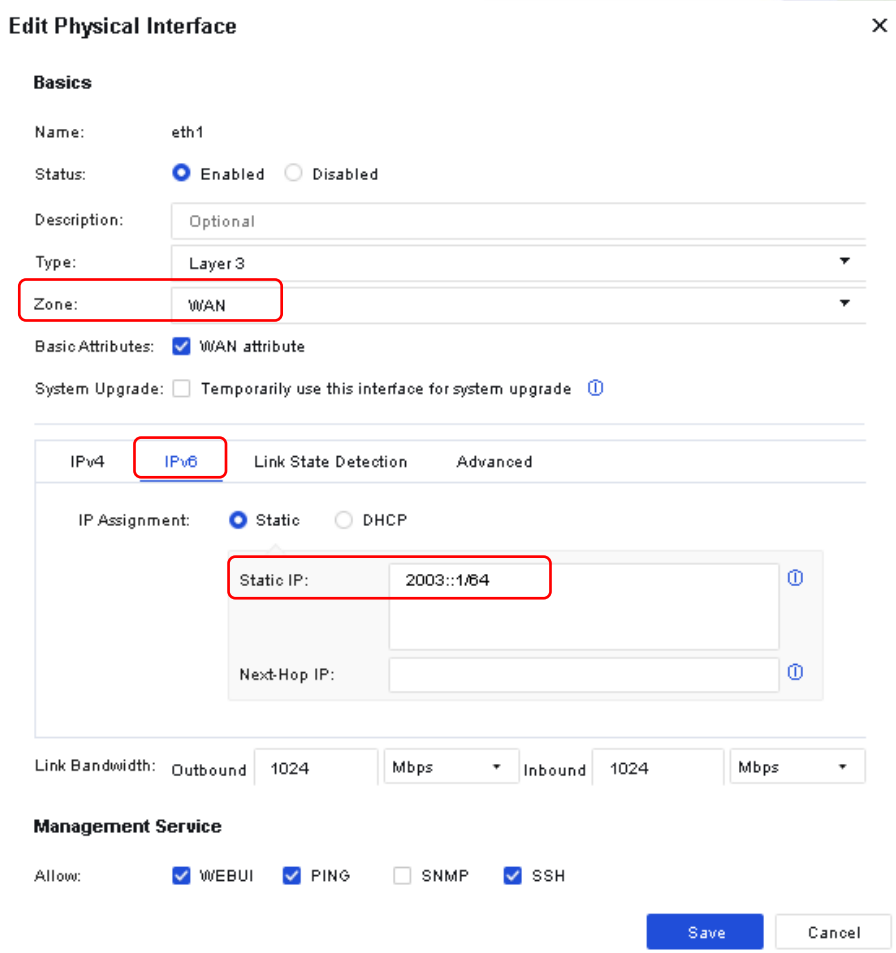
Step 4.1: Enable IPv6 and IPv4 support. IPv6 function is turned off by default. Please check “enable IPV4 and IPv6 support” in [System] - [General Settings] - [Network].

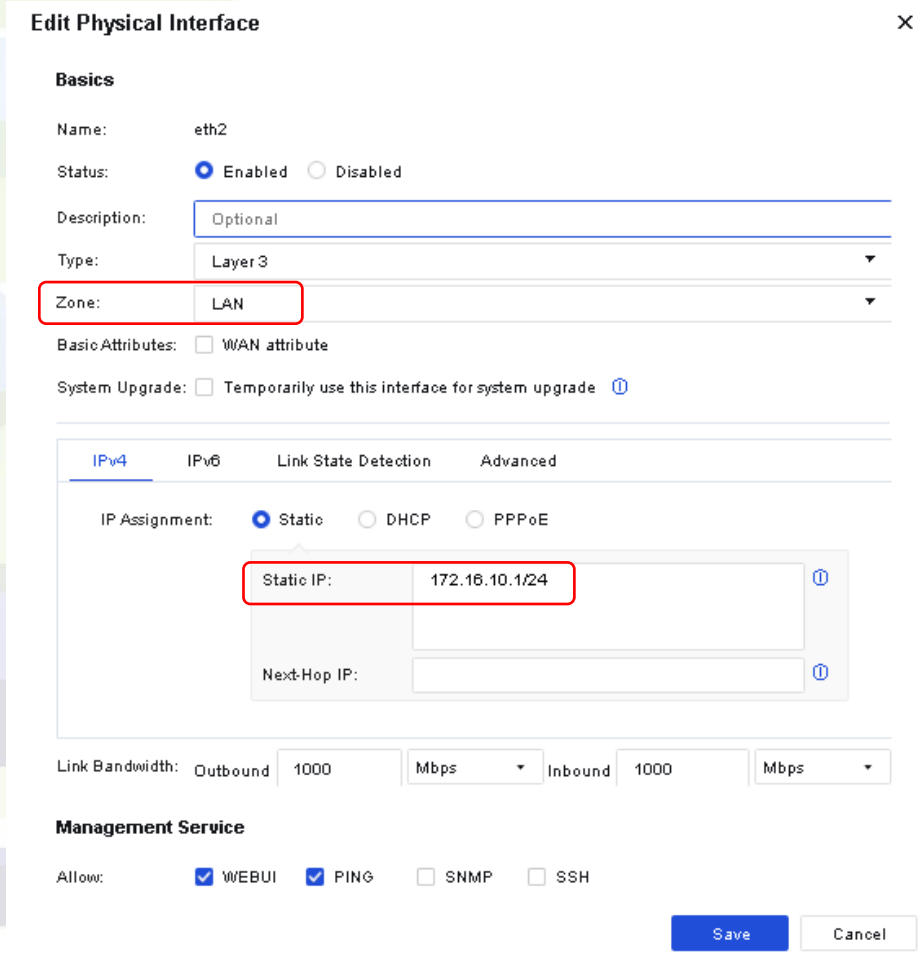
Turning on this function will restart the device.



NAT64 Case Study

Step 4.2: Define interface and zone.

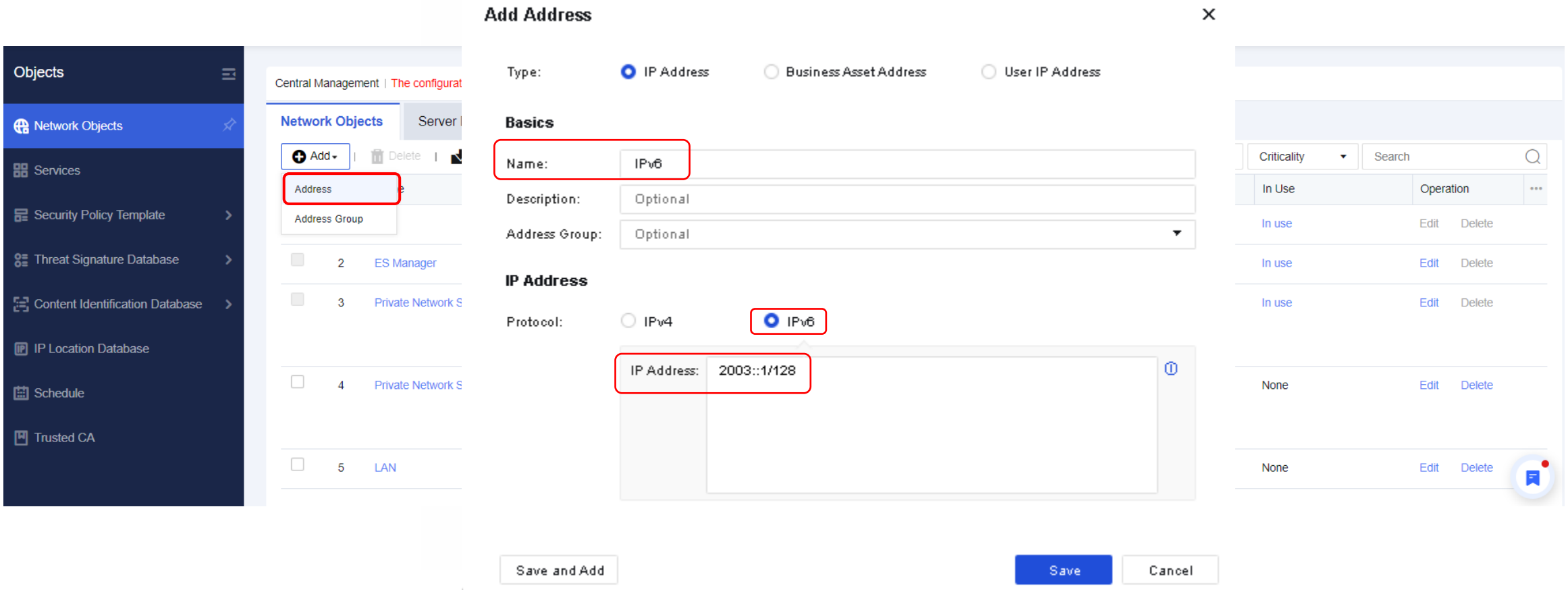




NAT64 Case Study

Step 4.3: Define Network object.

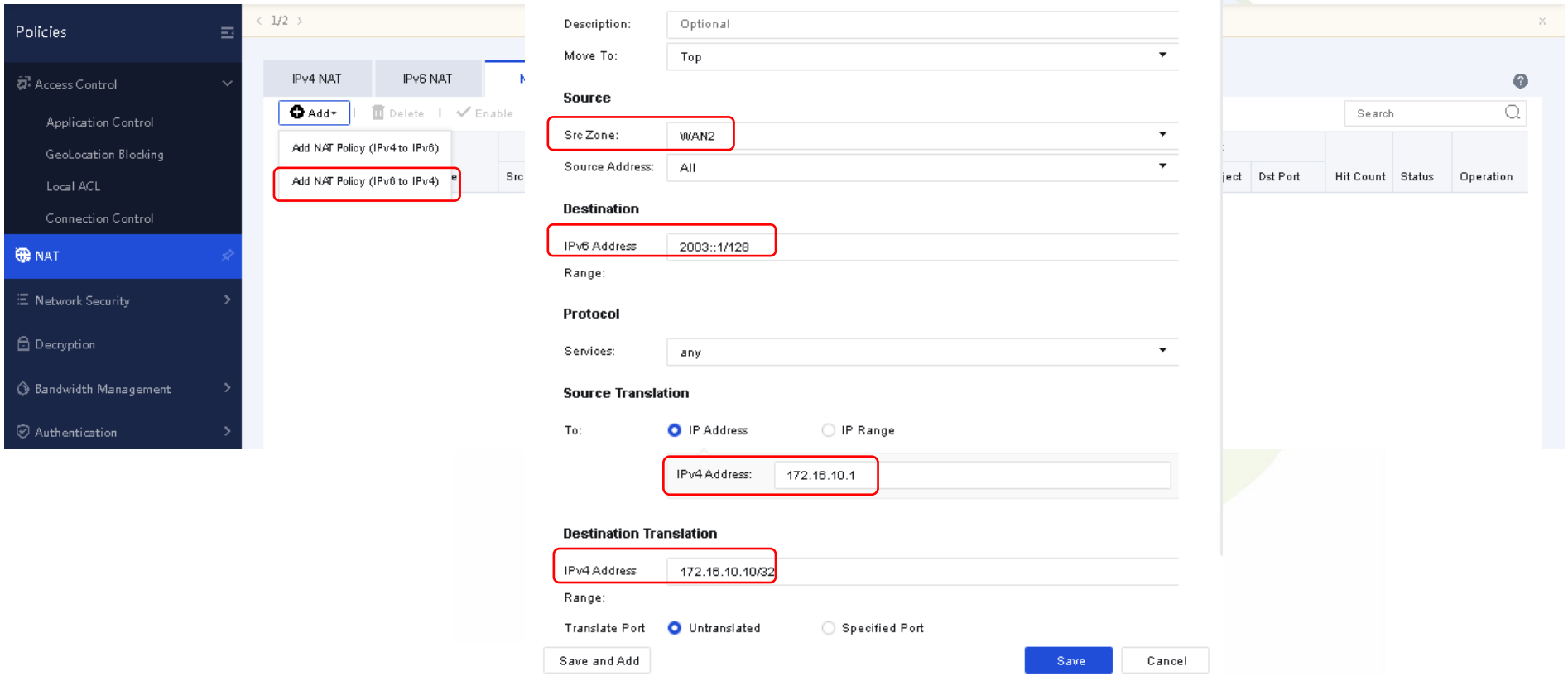
Path: Objects > Network Objects > Network Objects



NAT64 Case Study

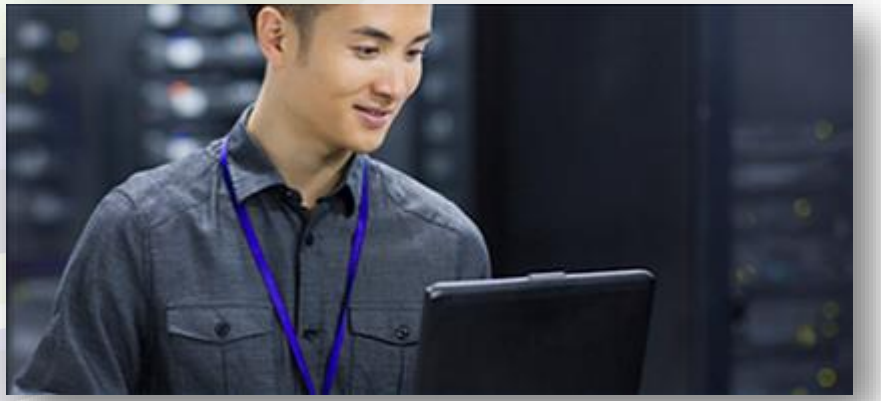
Step 4.3: Configure NAT64.

Path: Policy > NAT



Thank you !

tech.support@sangfor.com
community.sangfor.com



Sangfor Technologies (Headquarters)
Block A1, Nanshan iPark, No.1001
Xueyuan Road, Nanshan District,
Shenzhen, Guangdong Province,
P. R. China (518055)