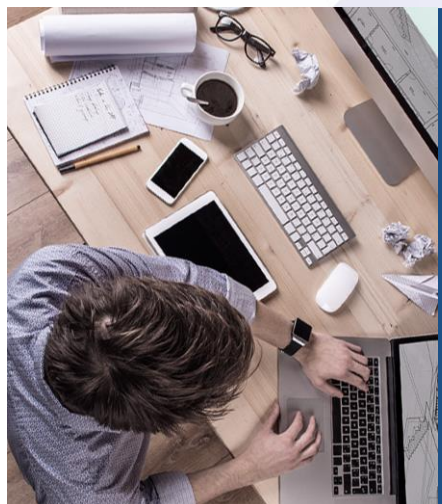




Sangfor NGAF v8.0.47 Associate

Basic Network Configuration





1 Interface

2 Routing

3 NAT

1 Interface



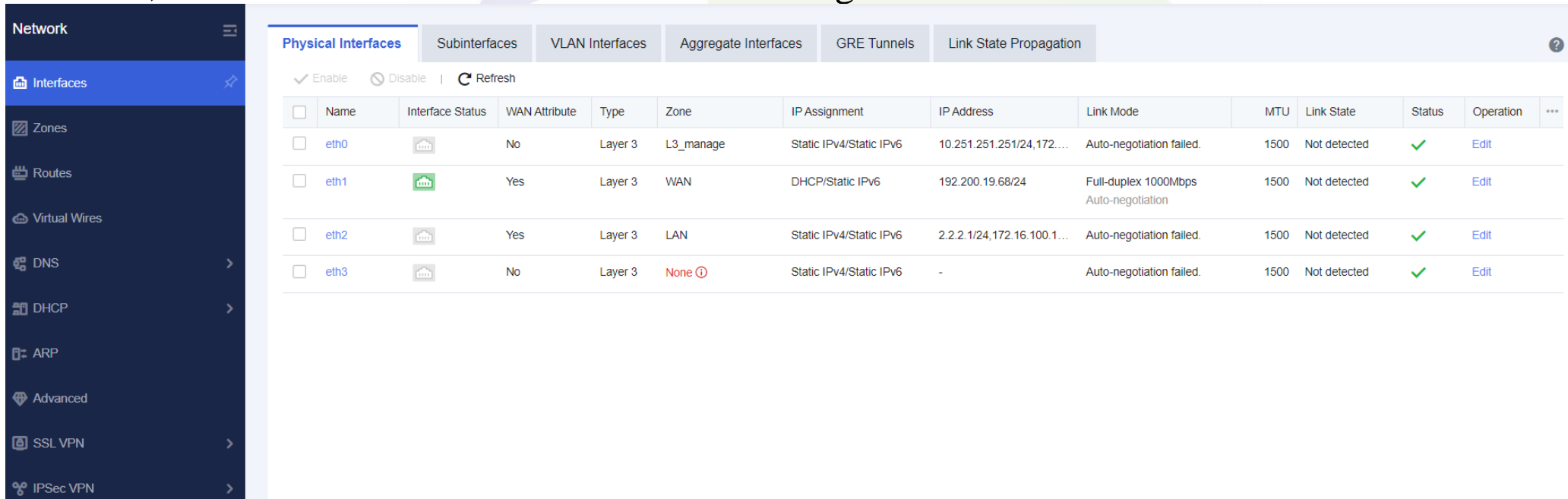
SANGFOR
深信服科技





Physical Interface

NGAF interfaces 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.



	Name	Interface Status	WAN Attribute	Type	Zone	IP Assignment	IP Address	Link Mode	MTU	Link State	Status	Operation	...
<input type="checkbox"/>	eth0		No	Layer 3	L3_manage	Static IPv4/Static IPv6	10.251.251.251/24,172....	Auto-negotiation failed.	1500	Not detected	✓	Edit	
<input type="checkbox"/>	eth1		Yes	Layer 3	WAN	DHCP/Static IPv6	192.200.19.68/24	Full-duplex 1000Mbps Auto-negotiation	1500	Not detected	✓	Edit	
<input type="checkbox"/>	eth2		Yes	Layer 3	LAN	Static IPv4/Static IPv6	2.2.2.1/24,172.16.100.1...	Auto-negotiation failed.	1500	Not detected	✓	Edit	
<input type="checkbox"/>	eth3		No	Layer 3	None ⓘ	Static IPv4/Static IPv6	-	Auto-negotiation failed.	1500	Not detected	✓	Edit	

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.

Edit Phy Edit Phy Edit Physical Interface

X



Basic	Basics	Basics
Name:	Name:	Name: eth1
Status:	Status:	Status: <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Description:	Description:	Description: Optional
Type:	Type:	Type: Layer 3
Zone:	Zone:	Zone: WAN
Basic Attributes:	Basic Attributes:	Basic Attributes: <input checked="" type="checkbox"/> WAN attribute
System Upgrade:	System Upgrade:	System Upgrade: <input type="checkbox"/> Temporarily use this interface for system upgrade i

IPv4 IPv6 Link State Detection Advanced

Link Mode: Auto-negotiation

MTU: 1500 [i](#)

MAC Address: 00:0C:29:3F:86:09 [Restore Default MAC](#)

Link Bandwidth: Outbound 1024 Mbps Inbound 1024 Mbps

Management Service

Save

Cancel

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'

Advanced Options

Handshake Time (secs):

Timeout (secs):

Max Attempts:

Others:

- ☒ Auto dial-up
- ☒ Add default route
- ☒ Taken as preferred DNS server

Save

Cancel

Edit Physical Interface

Type: Layer 3

Zone: WAN

Basic Attributes: ☒ WAN attribute

System Upgrade: ☐ Temporarily use this interface for system upgrade ⓘ

IPv4 IPv6 Link State Detection Advanced

IP Assignment: ☐ Static ☐ DHCP ☒ PPPoE

Status: ❗ Disconnected | [View](#)

Username:

Password:

Connect

Advanced

Link Bandwidth: Outbound Mbps Inbound Mbps

Management Service

Allow: ☒ WEBUI ☒ PING ☐ SNMP ☒ SSH

Save

Cancel



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.

Edit Physical Interface



Basics

Name: eth0

Status: ☒ Enabled ☐ Disabled

Description: Manage interface

Type: Layer 3

Zone: Select

Basic Attributes: ☐ WAN attribute

System Upgrade: ☐ Temporarily use this interface for system upgrade [i](#)

IPv4 IPv6 Link State Detection Advanced

IP Assignment: ☒ Static ☐ DHCP ☐ PPPoE

Static IP: 10.251.251.251/24 [i](#)

Next-Hop IP: [i](#)

Link Bandwidth: Outbound 8 Mbps Inbound 8 Mbps

Save Cancel

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.

Edit Physical

Edit Physical Interface

X

Basics

Basics

Name:

Name:

eth0

Status:

Status:

☒ Enabled ☐ Disabled

Description:

Description:

Manage interface

Type:

Type:

Layer 2

Zone:

Zone:

Select

Basic Attribute:

Basic Attributes:

☐ WAN attribute

IPv4/IPv6

Advanced

Link Mode:

Auto-negotiation

MTU:

1500

i

MAC Address:

00:0C:29:3F:86:FF

Restore Default MAC

Save

Cancel

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.

Edit Physical Interface

Basics

Name: eth0

Status: ☒ Enabled ☐ Disabled

Description: Manage interface

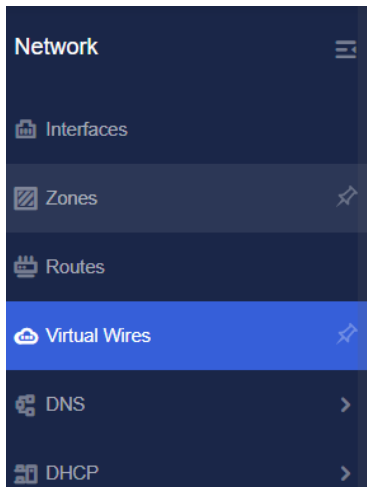
Type: Virtual wire

Zone: Select

Interface Pair 1: eth0

Interface Pair 2: Select

Basic Attributes: ☐ WAN attribute



Virtual Wires

[+ Add](#) | [Delete](#) | [Refresh](#)

<input type="checkbox"/>	Name	Interface Pair 1	Interface Pair 2	Description	Operation	...
<input type="checkbox"/>	Virtual1	eth2	eth3	-	Edit	Delete

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.

Edit Physical Interface

Basics

Name: eth4

Status: ☒ Enabled ☐ Disabled

Description: Optional

Type: Mirror

Zone: Mirror_A

Traffic Statistics: ☒ Enable

Network Objects: Private Network Segment

Save

Cancel

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.

Add Aggregate Interface

Basic Settings

Name: aggr. 1-4 Maximum support to 4

Description: Optional

Type: Layer 3 Don't support mirror port

Zone: Select

Work Mode: Active-passive

Basic Attributes: ☐ WAN attribute

System Upgrade: ☐ Temporarily use this interface for system upgrade i

Select Member Interfaces i

Available (2)

Search Q

☐ eth1

☐ eth2

Selected (0) Clear

Save Cancel

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.

Add Subinterface

Basics

Physical Interfaces:

eth2

Select which route interface

VLAN ID:

eth2

2

Configure VLAN ID

Description:

Optional

Zone:

Select

System Upgrade:

☐ Temporarily use this interface for system upgrade ⓘ

Network

Link State Detection

Advanced

IP Assignment:

☒ Static

☐ DHCP

☐ PPPoE

Static IP:

Optional ⓘ

Next-Hop IP:

Optional

Management Service

Allow:

☒

WEBUI

☒

PING

☐

SNMP

☐

SSH

Save

Cancel

VLAN interface

VLAN Interface:

Create IP address for VLAN, this is logical interface.

Add VLAN Interface

Basics

VLAN ID: → ⓘ

Description:

Zone:

System Upgrade: ☐ Temporarily use this interface for system upgrade ⓘ

IPv4

IPv6

Link State Detection

Advanced

IP Assignment:

☒ Static

☐ DHCP

Static IP:

ⓘ

Next-Hop IP:

Management Service

Allow:



WEBUI



PING



SNMP



SSH

Save

Cancel

Interface Precautions

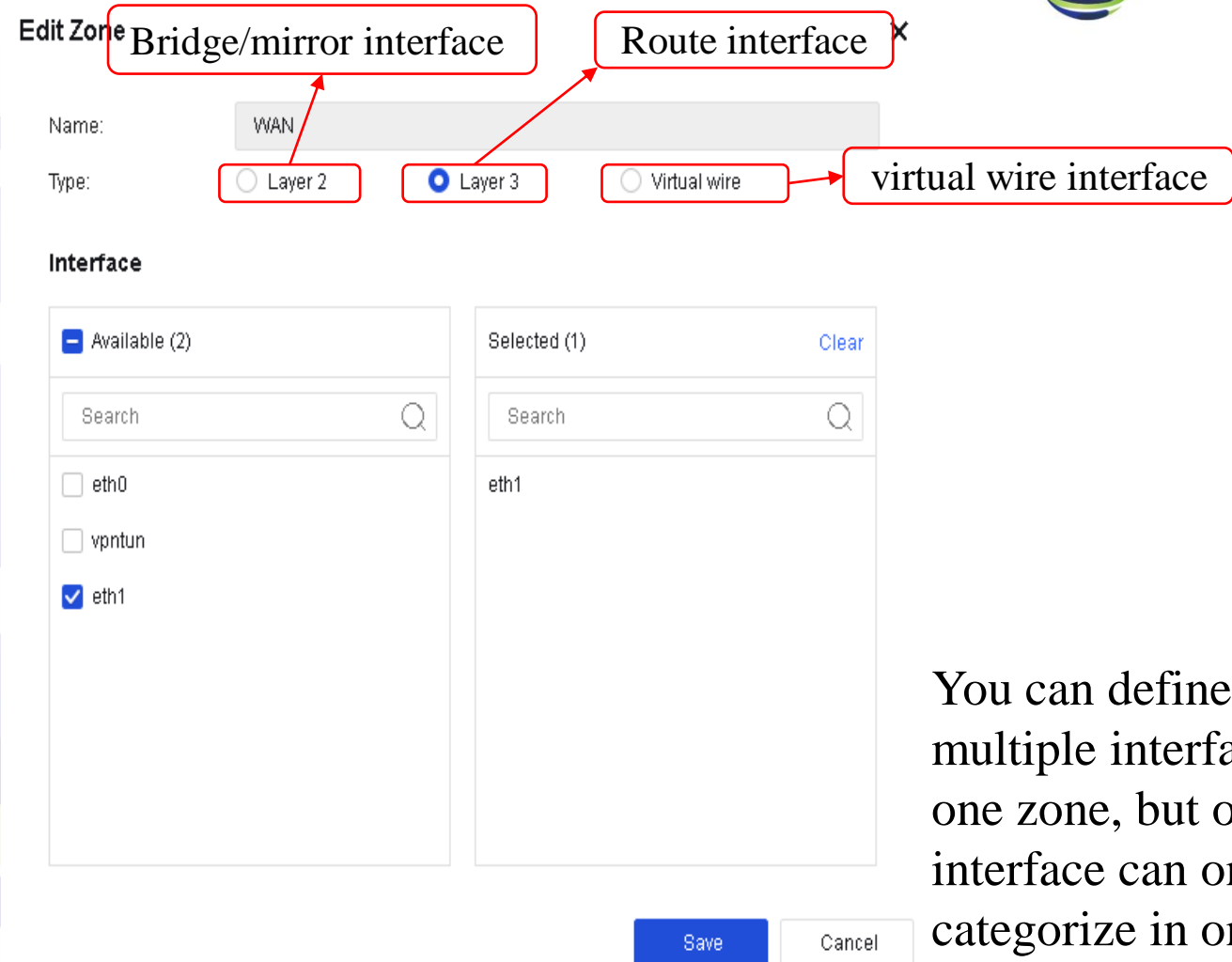
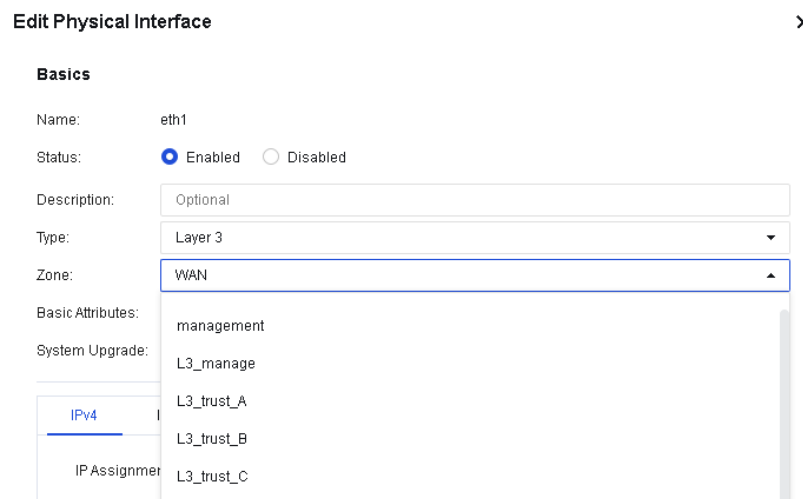
1. NGAF can support multiple WAN attribute interface.
2. Management interface does not support configure as bridge or virtual wire interface. If customer wants to deploy as double bridge , then the device must have at least 5 physical interface.
3. A route interface can add in multiple sub-interface,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

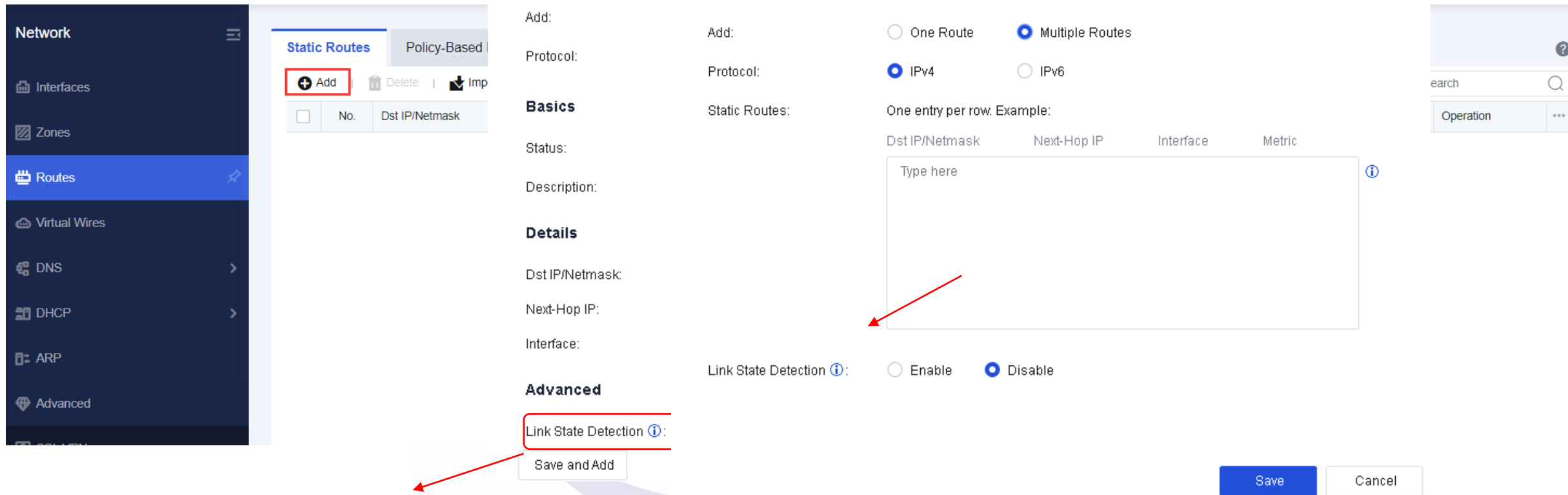
2 Routing



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.



Network

- Interfaces
- Zones
- Routes**
- Virtual Wires
- DNS
- DHCP
- ARP
- Advanced

Static Routes Policy-Based

+ Add Delete Imp

No. Dst IP/Netmask

Basics

Add:

Protocol:

Status:

Description:

Details

Dst IP/Netmask:

Next-Hop IP:

Interface:

Advanced

Link State Detection ⓘ:

Save and Add

One Route Multiple Routes

IPv4 IPv6

Static Routes:

One entry per row. Example:

Dst IP/Netmask	Next-Hop IP	Interface	Metric
Type here ⓘ			

Link State Detection ⓘ: Enable Disable

Save Cancel

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.

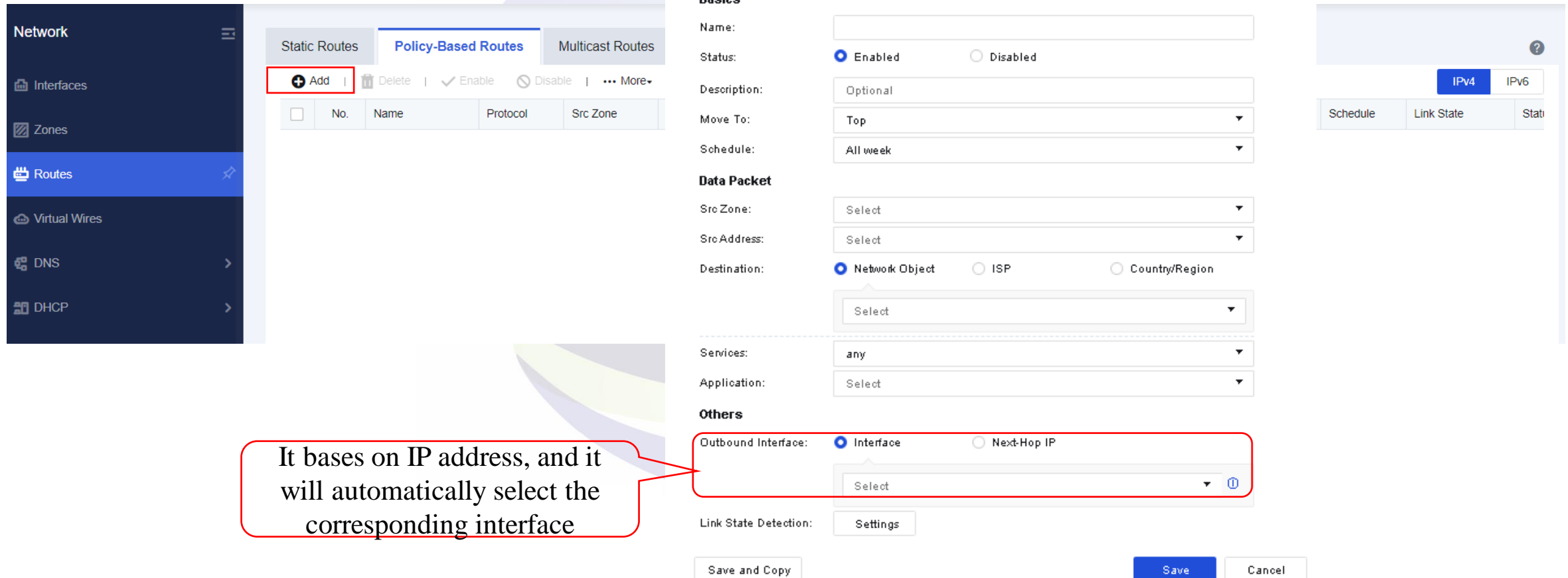
PBR common scenario:

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.



The screenshot displays the Sangfor Network Management System interface. On the left, a sidebar menu shows 'Network' with sub-items: Interfaces, Zones, Routes (highlighted), Virtual Wires, DNS, and DHCP. The main panel is titled 'Policy-Based Routes' and includes tabs for 'Static Routes', 'Policy-Based Routes', and 'Multicast Routes'. Below the tabs, there's a table with columns: No., Name, Protocol, and Src Zone. A red box highlights the '+ Add' button. To the right, a modal window titled 'Add Policy-Based Route' is open. It contains several sections: 'Route Type' (Source-based route selected), 'Protocol' (IPv4 selected), 'Basics' (Name, Status: Enabled, Description: Optional, Move To: Top, Schedule: All week), 'Data Packet' (Src Zone, Src Address, Destination: Network Object selected, Services: any, Application: Select), and 'Others' (Outbound Interface: Interface selected, Next-Hop IP, Link State Detection: Settings). A red box highlights the 'Outbound Interface' section. At the bottom of the modal, there are buttons for 'Save and Copy', 'Save', and 'Cancel'. A red callout bubble points to the 'Outbound Interface' section with the text: 'It bases on IP address, and it will automatically select the corresponding interface'.

Network

- Interfaces
- Zones
- Routes**
- Virtual Wires
- DNS
- DHCP

Static Routes | **Policy-Based Routes** | Multicast Routes

+ Add | Delete | Enable | Disable | More

No.	Name	Protocol	Src Zone
-----	------	----------	----------

Add Policy-Based Route

Route Type: ☒ Source-based route ☐ Link load-balancing

Protocol: ☒ IPv4 ☐ IPv6

Basics

Name:

Status: ☒ Enabled ☐ Disabled

Description:

Move To:

Schedule:

Data Packet

Src Zone:

Src Address:

Destination: ☒ Network Object ☐ ISP ☐ Country/Region

Services:

Application:

Others

Outbound Interface: ☒ Interface ☐ Next-Hop IP

Link State Detection:

Save and Copy | Save | Cancel

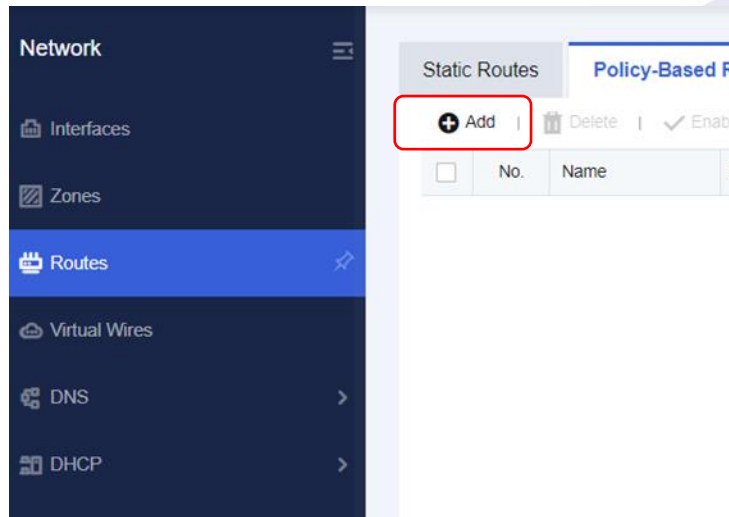
IPv4 | IPv6

Schedule | Link State | Status

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.



Add Policy-Based Route

Status: ☒ Enabled ☐ Disabled

Description:

Move To:

Schedule:

Data Packet

Src Zone:

Src Address:

Destination: ☒ Network Object ☐ ISP ☐ Country/Region

Services:

Application:

Outbound Interfaces

☒ Add ☐ Delete

Interface	Next-Hop ⓘ	Link State ⓘ	Operation
No data available			

Load Balancing Method:

Save and Copy Save Cancel

Round Robin: Active links are selected in turns. The likelihood that each link is selected is the same.

Bandwidth Ratio Round Robin: This method is similar to weighted Round Robin, however, weights are not specified numbers but dynamic ratio calculated according to the bidirectional bandwidth on different WAN links. It aims at balancing the bandwidth usage on the available WAN links based on new scheduled connection, regardless of connection failure or realtime bandwidth on the WAN link.

Weighted least traffic: This method is similar to weighted Round Robin as well, however, weights are not specified numbers but dynamic ratio calculated according to the bidirectional bandwidth on different WAN links. It aims at balancing the bandwidth usage on the available WAN links based on the new scheduled traffic.

Prefer link at top: Prefer the link at the top of interface list. To elevate priority of a link, move it up or to top.

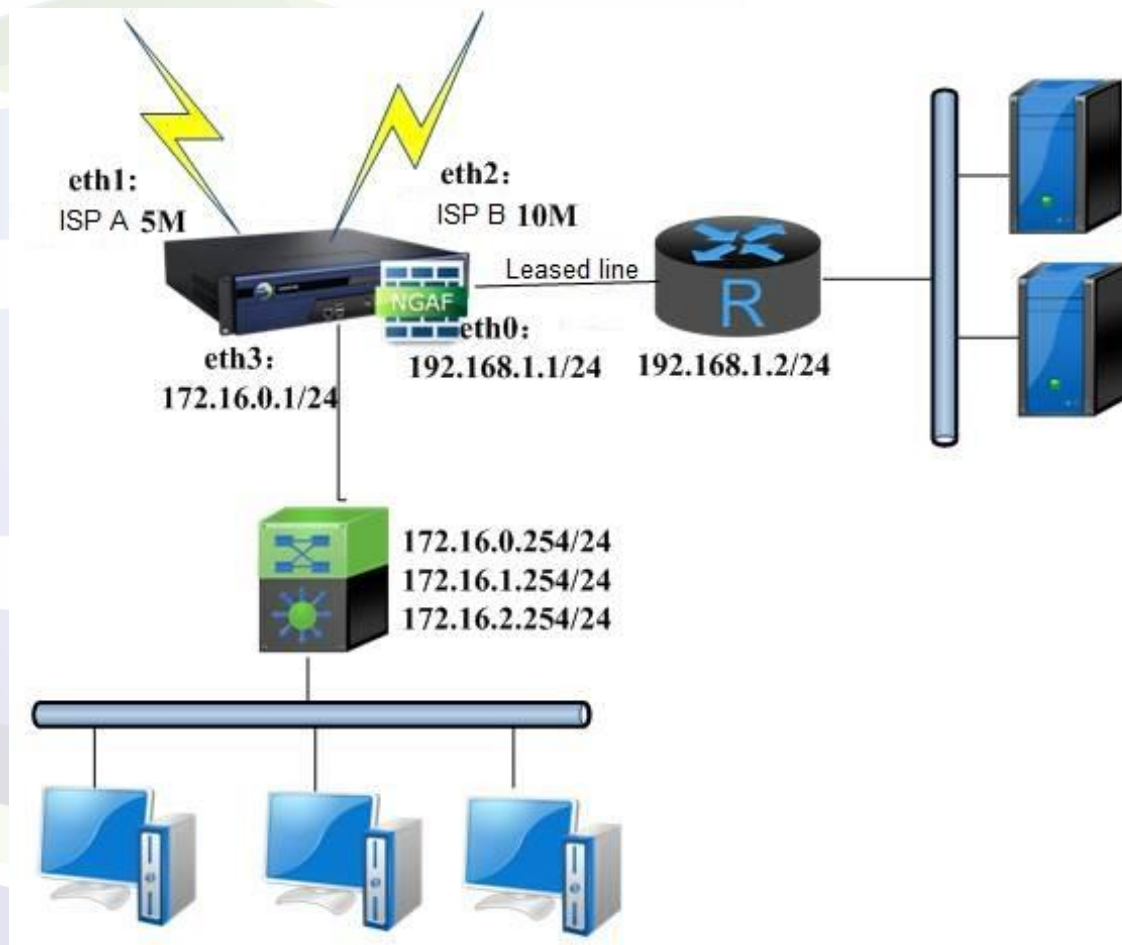
Policy-Based Routing Case Study

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

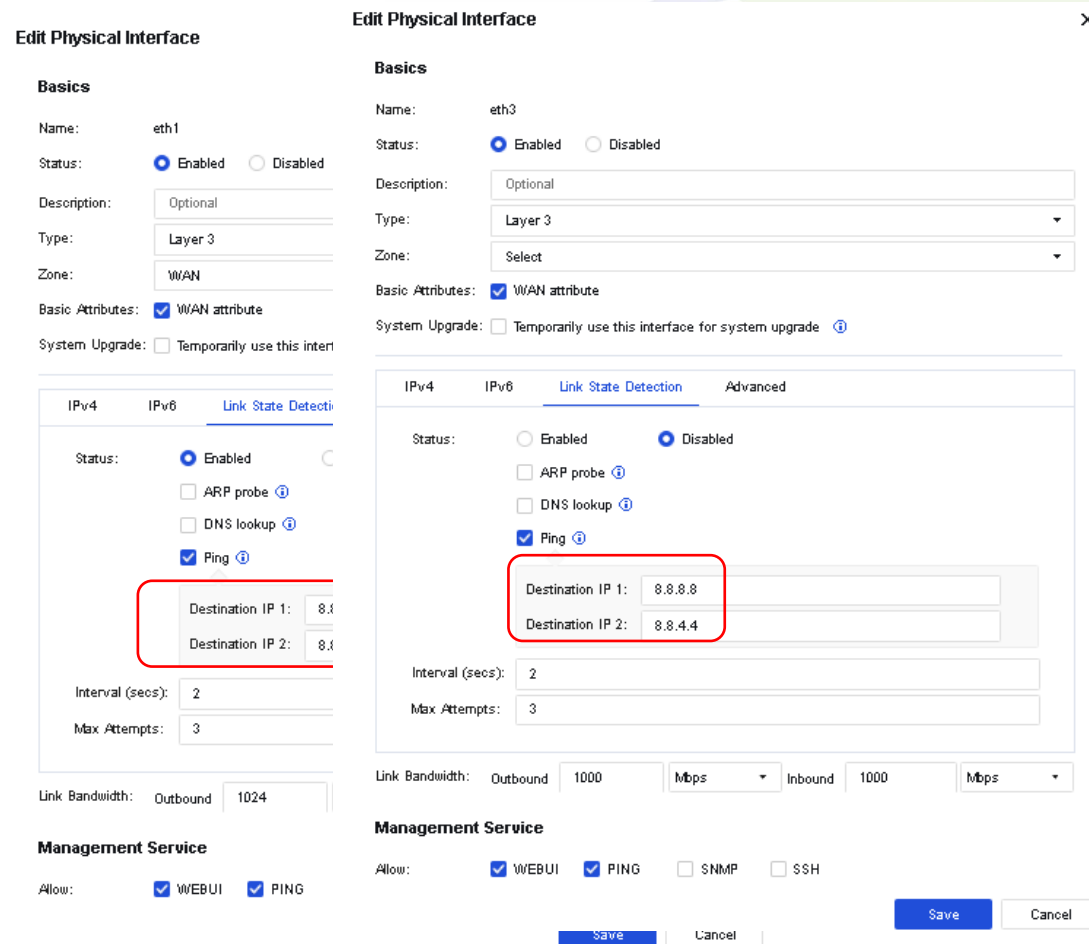
- Add source-base route, source select “LAN Zone”, destination IP select all, destination port: TCP 443, select interface eth2.
- Add a load balance route, source “LAN Zone”, destination IP select all, interface select eth1 and eth2, load balance method select “weighted round robin”.

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



The image displays two screenshots of the Sangfor firewall configuration interface, specifically the 'Edit Physical Interface' window.

Left Screenshot (Interface eth1):

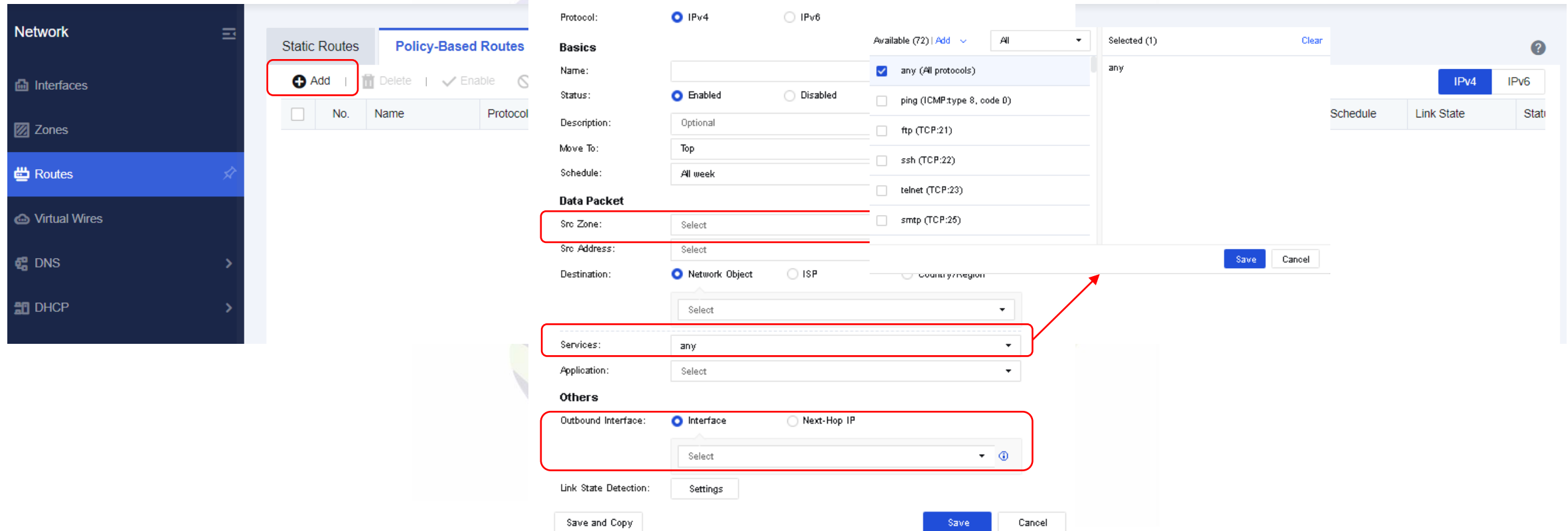
- Basics:**
 - Name: eth1
 - Status: ☒ Enabled ☐ Disabled
 - Description: Optional
 - Type: Layer 3
 - Zone: WAN
 - Basic Attributes: ☒ WAN attribute
 - System Upgrade: ☐ Temporarily use this interface for system upgrade
- Link State Detection:**
 - Status: ☒ Enabled ☐ Disabled
 - ☐ ARP probe
 - ☐ DNS lookup
 - ☒ Ping
 - Destination IP 1: 8.8.8.8
 - Destination IP 2: 8.8.4.4
 - Interval (secs): 2
 - Max Attempts: 3
- Link Bandwidth:** Outbound 1024
- Management Service:**
 - Allow: ☒ WEBUI ☒ PING

Right Screenshot (Interface eth3):

- Basics:**
 - Name: eth3
 - Status: ☒ Enabled ☐ Disabled
 - Description: Optional
 - Type: Layer 3
 - Zone: Select
 - Basic Attributes: ☒ WAN attribute
 - System Upgrade: ☐ Temporarily use this interface for system upgrade
- Link State Detection:**
 - Status: ☐ Enabled ☒ Disabled
 - ☐ ARP probe
 - ☐ DNS lookup
 - ☒ Ping
 - Destination IP 1: 8.8.8.8
 - Destination IP 2: 8.8.4.4
 - Interval (secs): 2
 - Max Attempts: 3
- Link Bandwidth:** Outbound 1000 Mbps, Inbound 1000 Mbps
- Management Service:**
 - Allow: ☒ WEBUI ☒ PING ☐ SNMP ☐ SSH

Policy-Based Routing Case Study

2.1 Add Source-based route



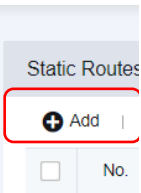
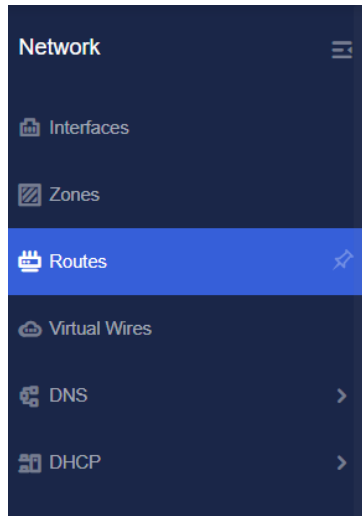
The screenshot displays the Sangfor Network Management System interface. On the left, a sidebar menu shows 'Network' with sub-items: Interfaces, Zones, Routes (highlighted), Virtual Wires, DNS, and DHCP. The main panel is divided into 'Static Routes' and 'Policy-Based Routes' tabs. The 'Policy-Based Routes' tab is active, showing a table with columns: No., Name, and Protocol. A red box highlights the '+ Add' button. The 'Add Policy-Based Route' dialog box is open, showing the following configuration:

- Route Type:** ☒ Source-based route, ☐ Link load-balancing
- Protocol:** ☒ IPv4, ☐ IPv6
- Basics:**
 - Name:** [Empty field]
 - Status:** ☒ Enabled, ☐ Disabled
 - Description:** [Optional]
 - Move To:** Top
 - Schedule:** All week
- Data Packet:**
 - Src Zone:** Select
 - Src Address:** Select
 - Destination:** ☒ Network Object, ☐ ISP
 - Services:** any (All protocols) [Selected]
 - Application:** Select
- Others:**
 - Outbound Interface:** ☒ Interface, ☐ Next-Hop IP
 - Link State Detection:** Settings

Buttons at the bottom include 'Save and Copy', 'Save', and 'Cancel'. A red arrow points from the 'Services' dropdown to the 'Selected (1)' list on the right, which contains 'any'.

Policy-Based Routing Case Study

2.2 Add Link load-balancing route



Add Policy-Based Route

Route Type: ☐ Source-based route ☒ Link load-balancing

Protocol: ☒ IPv4 ☐ IPv6

Basics

Name:

Status: ☒ Enabled ☐ Disabled

Description:

Move To:

Schedule:

Data Packet

Src Zone:

Src Address:

Destination: ☒ Network Object ☐ ISP ☐ Country/Region

Services:

Application:

Outbound Interfaces

<input type="checkbox"/>	Interface	Next-Hop	Link State	Operation
<input type="checkbox"/>	eth0	-	Not probed	Move Up Move Down Delete
<input type="checkbox"/>	eth1	-	Normal	Move Up Move Down Delete

Save and Copy Save Cancel

Add Policy-Based Route

Status: ☒ Enabled ☐ Disabled

Description:

Move To:

Schedule:

Data Packet

Src Zone:

Src Address:

Destination: ☒ Network Object ☐ ISP ☐ Country/Region

Services:

Application:

Outbound Interfaces

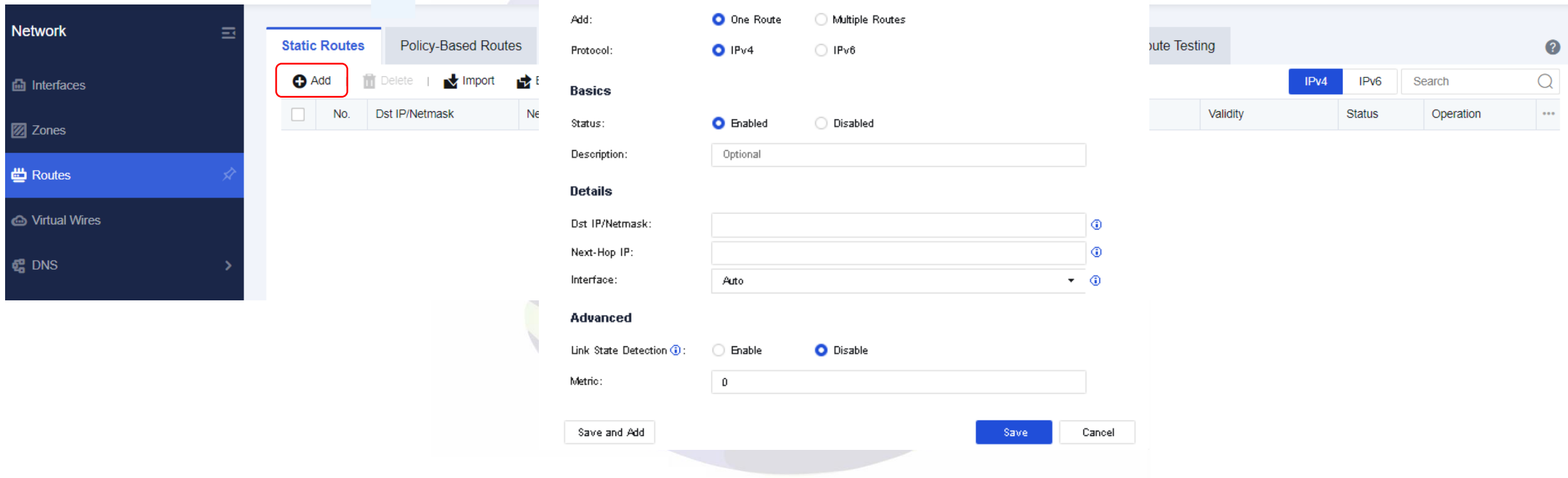
<input type="checkbox"/>	Interface	Next-Hop	Link State	Operation
<input type="checkbox"/>	eth0	-	Not probed	Move Up Move Down Delete
<input type="checkbox"/>	eth1	-	Round robin	Move Up Move Down Delete

Load Balancing Method:

Save and Copy Save Cancel

Policy-Based Routing Case Study

3. Add Static route



The screenshot displays the Sangfor Network Management System interface. On the left, a sidebar menu shows 'Network' with sub-items: Interfaces, Zones, Routes (highlighted), Virtual Wires, and DNS. The main panel is divided into 'Static Routes' and 'Policy-Based Routes' tabs. The 'Static Routes' tab is active, showing a table with columns: No., Dst IP/Netmask, and Ne. A red box highlights the '+ Add' button. The 'Add Static Route' dialog box is open, showing the following configuration:

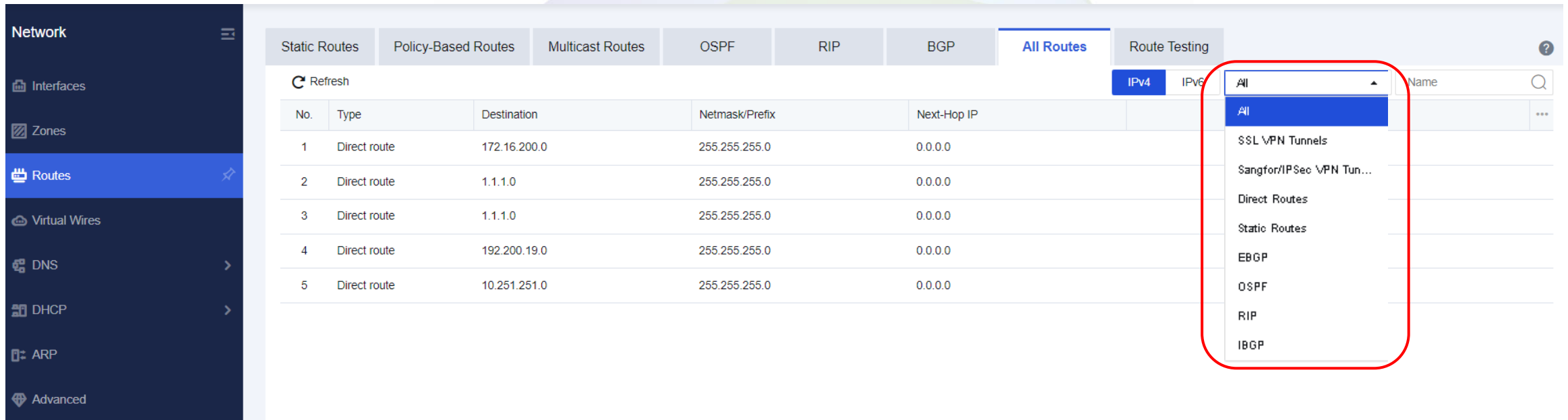
- Add:** ☒ One Route ☐ Multiple Routes
- Protocol:** ☒ IPv4 ☐ IPv6
- Basics**
 - Status:** ☒ Enabled ☐ Disabled
 - Description:** Optional
- Details**
 - Dst IP/Netmask:**
 - Next-Hop IP:**
 - Interface:** Auto
- Advanced**
 - Link State Detection:** ☐ Enable ☒ Disable
 - Metric:** 0

Buttons at the bottom of the dialog: Save and Add, Save, and Cancel.

On the right, a 'Route Testing' section is visible, featuring tabs for IPv4 and IPv6, a search bar, and a table with columns: Validity, Status, Operation, and a menu icon (***).

Display All routes

Display all routes.



Network

- Interfaces
- Zones
- Routes**
- Virtual Wires
- DNS
- DHCP
- ARP
- Advanced

Static Routes Policy-Based Routes Multicast Routes OSPF RIP BGP **All Routes** Route Testing

Refresh

No.	Type	Destination	Netmask/Prefix	Next-Hop IP
1	Direct route	172.16.200.0	255.255.255.0	0.0.0.0
2	Direct route	1.1.1.0	255.255.255.0	0.0.0.0
3	Direct route	1.1.1.0	255.255.255.0	0.0.0.0
4	Direct route	192.200.19.0	255.255.255.0	0.0.0.0
5	Direct route	10.251.251.0	255.255.255.0	0.0.0.0

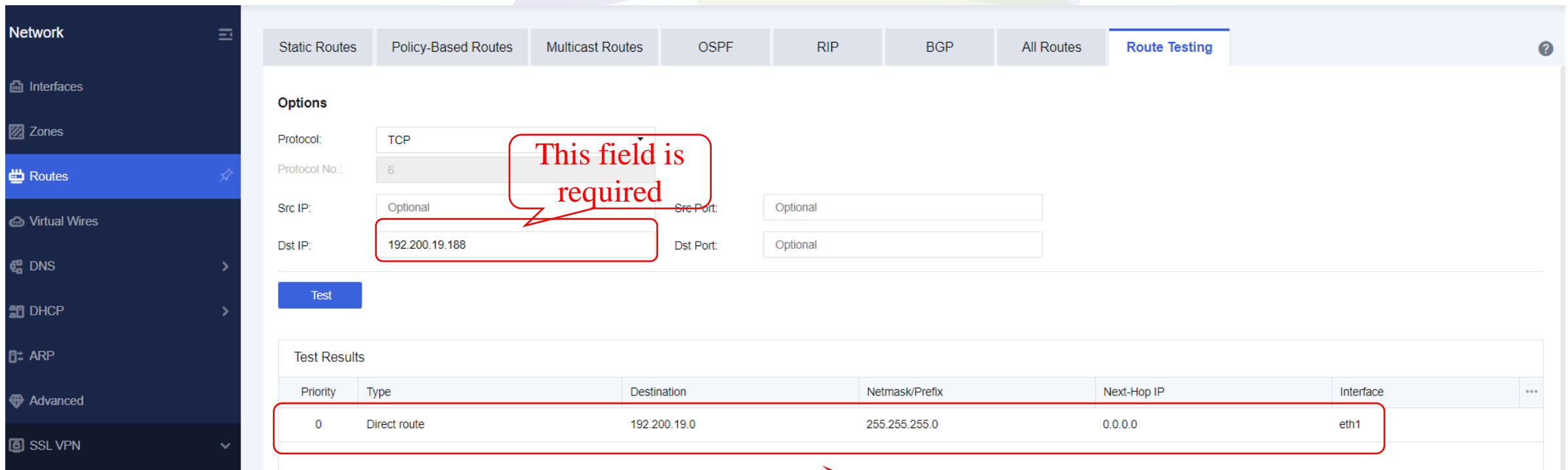
IPv4 IPv6

All

- All
- SSL VPN Tunnels
- Sangfor/IPSec VPN Tun...
- Direct Routes
- Static Routes
- EBGP
- OSPF
- RIP
- IBGP

Route Testing

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



The screenshot displays the SANGFOR NMS interface. On the left is a dark sidebar with a menu containing: Network, Interfaces, Zones, Routes (highlighted), Virtual Wires, DNS, DHCP, ARP, Advanced, and SSL VPN. The main content area has a top navigation bar with tabs: Static Routes, Policy-Based Routes, Multicast Routes, OSPF, RIP, BGP, All Routes, and Route Testing (active). Below the tabs is the 'Options' section with the following fields: Protocol (TCP), Protocol No. (6), Src IP (Optional), Dst IP (192.200.19.188), Src Port (Optional), and Dst Port (Optional). A red callout bubble points to the Dst IP field with the text 'This field is required'. Below the options is a blue 'Test' button. Underneath is the 'Test Results' section, which contains a table with the following data:

Priority	Type	Destination	Netmask/Prefix	Next-Hop IP	Interface	...
0	Direct route	192.200.19.0	255.255.255.0	0.0.0.0	eth1	

A red callout bubble points to the table with the text 'There are all matched routes, display by priority.'

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

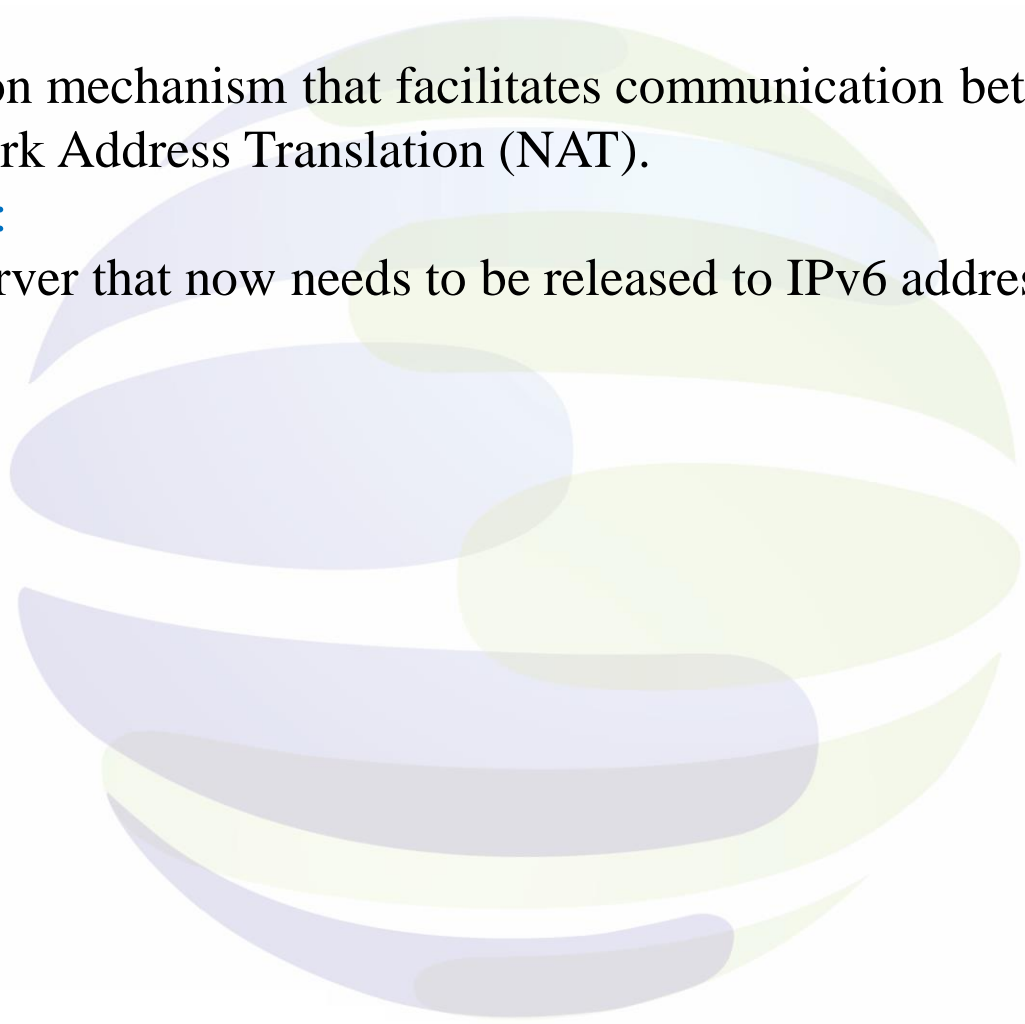


NAT64:

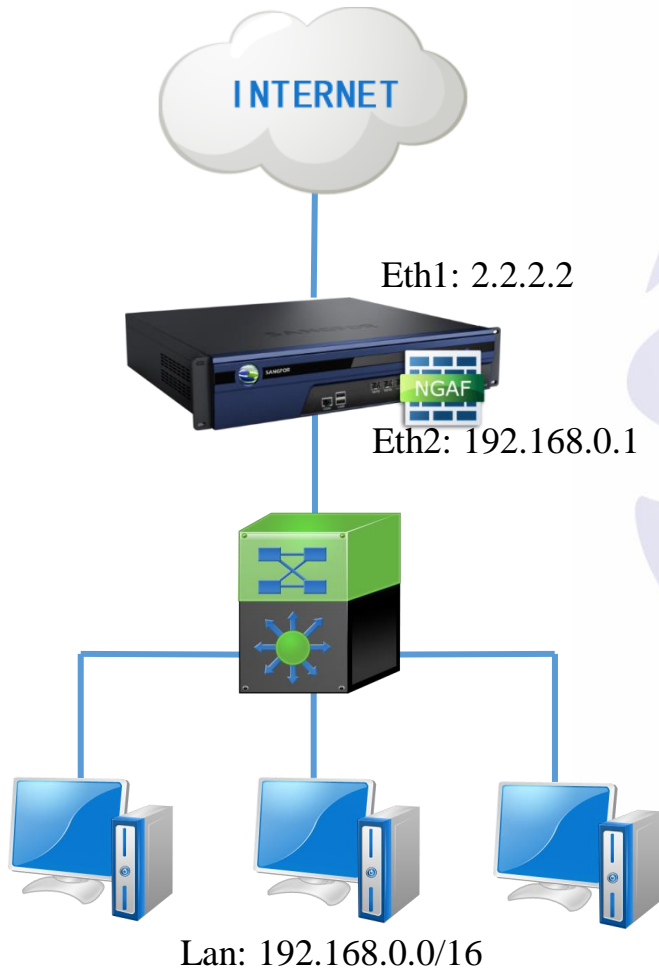
NAT64 is an IPv6 translation mechanism that facilitates communication between IPv6 and IPv4 hosts by using the form of Network Address Translation (NAT).

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.

Edit Physical Interface

Basics

Name:

eth1

Status:

Enabled

Disabled

Description:

Optional

Type:

Layer 3

Zone:

WAN

Basic Attributes:

WAN attribute

System Upgrade:

Temporarily use this interface for system upgrade

IPv4

IPv6

Link State Detection

Advanced

IP Assignment:

Static

DHCP

PPPoE

Static IP:

2.2.2.2/24

Next-Hop IP:

2.2.2.1

Link Bandwidth:

Outbound

1024

Mbps

Inbound

1024

Mbps

Management Service

Allow:

WEBUI

PING

SNMP

SSH

Save

Cancel

Edit Physical Interface

Basics

Name:

eth3

Status:

Enabled

Disabled

Description:

Optional

Type:

Layer 3

Zone:

LAN

Basic Attributes:

WAN attribute

System Upgrade:

Temporarily use this interface for system upgrade

IPv4

IPv6

Link State Detection

Advanced

IP Assignment:

Static

DHCP

PPPoE

Static IP:

192.168.0.1/24

Next-Hop IP:

Link Bandwidth:

Outbound

1000

Mbps

Inbound

1000

Mbps

Management Service

Allow:

WEBUI

PING

SNMP

SSH

Save

Cancel

Source NAT Case Study



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

Network

Interfaces

Zones

Routes

Virtual Wires

DNS

DHCP

ARP

Advanced

SSL VPN

Online Users

Deployment

Local Users

Resources

Roles

Login Options

Zones

+ Add

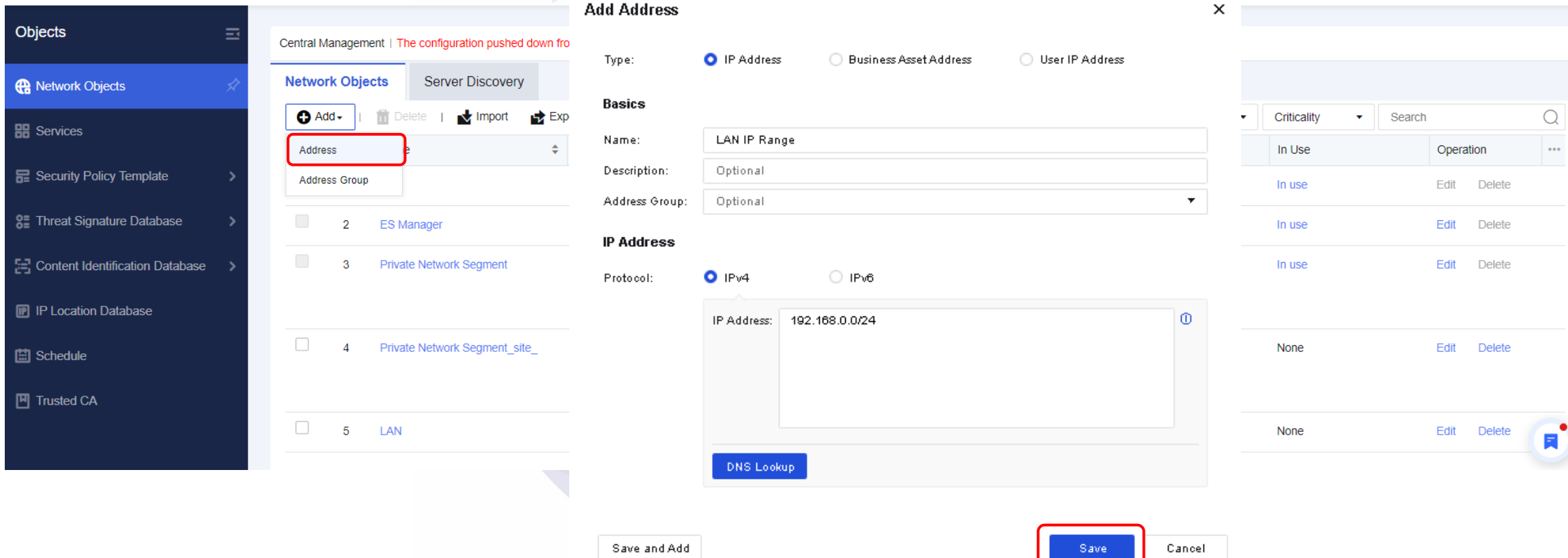
🗑 Delete

🔄 Refresh

<input type="checkbox"/>	Name	Type	Interfaces	In Use	Operation	...
<input type="checkbox"/>	L2_trust_B	Layer 2	-	none	Edit Delete	
<input type="checkbox"/>	L2_untrust_A	Layer 2	-	None	Edit Delete	
<input type="checkbox"/>	L2_untrust_B	Layer 2	-	None	Edit Delete	
<input type="checkbox"/>	L3_manage	Layer 3	eth0	In use	Edit Delete	
<input type="checkbox"/>	L3_trust_A	Layer 3	-	None	Edit Delete	
<input type="checkbox"/>	L3_trust_B	Layer 3	-	None	Edit Delete	
<input type="checkbox"/>	L3_trust_C	Layer 3	-	None	Edit Delete	
<input type="checkbox"/>	L3_untrust_A	Layer 3	-	None	Edit Delete	
<input type="checkbox"/>	L3_untrust_B	Layer 3	-	None	Edit Delete	
<input type="checkbox"/>	L3_untrust_C	Layer 3	-	None	Edit Delete	
<input type="checkbox"/>	Virtual_trust_A	Virtual wire	-	None	Edit Delete	
<input type="checkbox"/>	Virtual_trust_B	Virtual wire	-	None	Edit Delete	
<input type="checkbox"/>	Virtual_untrust_A	Virtual wire	-	None	Edit Delete	
<input type="checkbox"/>	Virtual_untrust_B	Virtual wire	-	None	Edit Delete	
<input type="checkbox"/>	WAN	Layer 3	eth1	In use	Edit Delete	
<input type="checkbox"/>	LAN	Layer 3	-	In use	Edit Delete	

Source NAT Case Study

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



The screenshot displays the Sangfor security management console interface. On the left, a sidebar menu lists various objects, with 'Network Objects' selected. The main panel shows the 'Add Address' dialog box, which is used to define a new IP address object. The dialog is divided into several sections:

- Basics:** Includes fields for Name (set to 'LAN IP Range'), Description (set to 'Optional'), and Address Group (set to 'Optional').
- IP Address:** Includes a Protocol section with 'IPv4' selected and 'IPv6' unselected. Below this is a large text area for the IP Address, currently containing '192.168.0.0/24'. A 'DNS Lookup' button is located below the text area.
- Buttons:** At the bottom of the dialog, there are three buttons: 'Save and Add', 'Save' (highlighted with a red box), and 'Cancel'.


On the right side of the console, a table displays a list of existing network objects. The table has columns for 'In Use', 'Operation', and 'Criticality'. The objects listed are:

In Use	Operation	Criticality
In use	Edit Delete	
In use	Edit Delete	
In use	Edit Delete	
None	Edit Delete	
None	Edit Delete	

Source NAT Case Study

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

Add NAT Policy ×



Type: ☒ Source NAT ☐ Destination NAT ☐ Bidirectional NAT

Basics

Name:

Status: ☒ Enabled ☐ Disabled

Description:

Move To: ⓘ

Schedule:

Original Data Packet

Src Zone:

Src Address:

Dst Zone/Interface: ☒ Zones ☐ Interface

Dst Address:

Services:

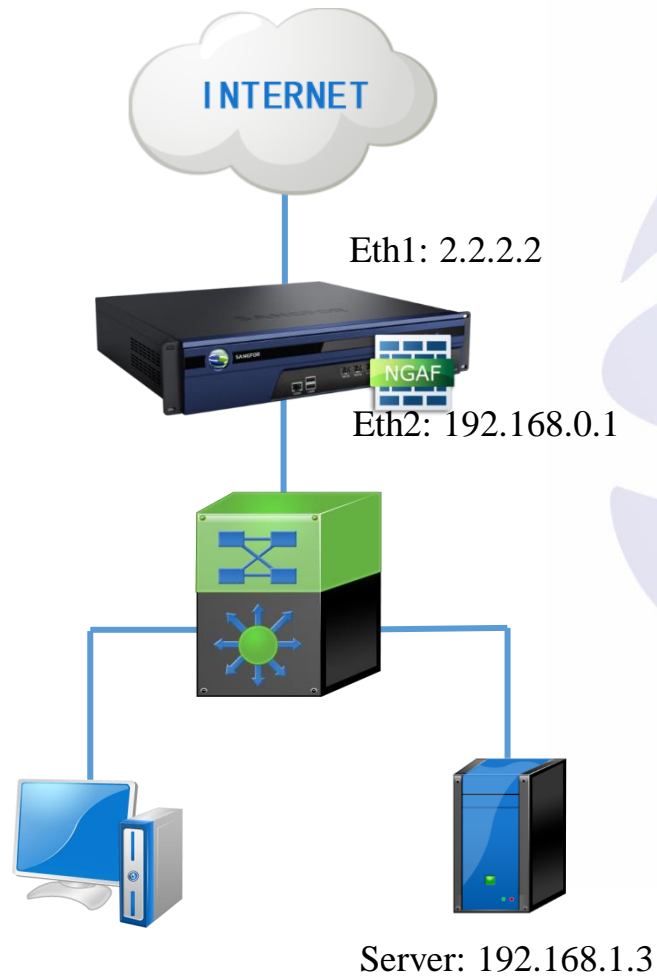
Translated Data Packet

Translate Src IP To:

Translate Dst IP To:

Translate Dst Port To:

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).

Edit Physical Interface

Basics

Name:eth1

Status:☒ Enabled ☐ Disabled

Description:Optional

Type:Layer 3

Zone:WAN

Basic Attributes:☒ WAN attribute

System Upgrade:☐ Temporarily use this interface for system upgrade ⓘ

IPv4IPv6Link State DetectionAdvanced

IP Assignment:☒ Static ☐ DHCP ☐ PPPoE

Static IP:2.2.2.2/24 ⓘ

Next-Hop IP:2.2.2.1 ⓘ

Link Bandwidth: Outbound1024MbpsInbound1024Mbps

Management Service

Allow:☒ WEBUI ☒ PING ☐ SNMP ☒ SSH

SaveCancel

Edit Physical Interface

Basics

Name:eth3

Status:☒ Enabled ☐ Disabled

Description:Optional

Type:Layer 3

Zone:LAN

Basic Attributes:☐ WAN attribute

System Upgrade:☐ Temporarily use this interface for system upgrade ⓘ

IPv4IPv6Link State DetectionAdvanced

IP Assignment:☒ Static ☐ DHCP ☐ PPPoE

Static IP:192.168.0.1/24 ⓘ

Next-Hop IP: ⓘ

Link Bandwidth: Outbound1000MbpsInbound1000Mbps

Management Service

Allow:☒ WEBUI ☒ PING ☐ SNMP ☐ SSH

SaveCancel

Destination NAT Case Study



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

Path: Network > Interface

Network

Interfaces

Zones

Routes

Virtual Wires

DNS

DHCP

ARP

Advanced

SSL VPN

Online Users

Deployment

Local Users

Resources

Roles

Login Options

Zones

+ Add

Delete

Refresh

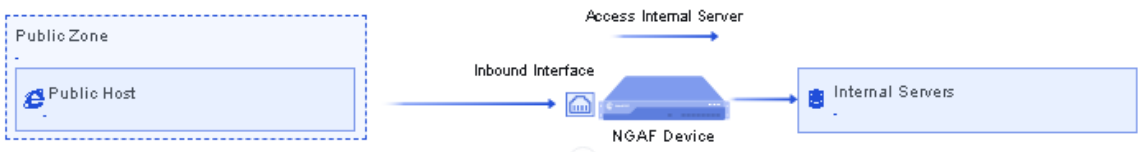
<input type="checkbox"/>	Name	Type	Interfaces	In Use	Operation	...
<input type="checkbox"/>	L2_trust_B	Layer 2	-	None	Edit Delete	
<input type="checkbox"/>	L2_untrust_A	Layer 2	-	None	Edit Delete	
<input type="checkbox"/>	L2_untrust_B	Layer 2	-	None	Edit Delete	
<input type="checkbox"/>	L3_manage	Layer 3	eth0	In use	Edit Delete	
<input type="checkbox"/>	L3_trust_A	Layer 3	-	None	Edit Delete	
<input type="checkbox"/>	L3_trust_B	Layer 3	-	None	Edit Delete	
<input type="checkbox"/>	L3_trust_C	Layer 3	-	None	Edit Delete	
<input type="checkbox"/>	L3_untrust_A	Layer 3	-	None	Edit Delete	
<input type="checkbox"/>	L3_untrust_B	Layer 3	-	None	Edit Delete	
<input type="checkbox"/>	L3_untrust_C	Layer 3	-	None	Edit Delete	
<input type="checkbox"/>	Virtual_trust_A	Virtual wire	-	None	Edit Delete	
<input type="checkbox"/>	Virtual_trust_B	Virtual wire	-	None	Edit Delete	
<input type="checkbox"/>	Virtual_untrust_A	Virtual wire	-	None	Edit Delete	
<input type="checkbox"/>	Virtual_untrust_B	Virtual wire	-	None	Edit Delete	
<input type="checkbox"/>	WAN	Layer 3	eth1	In use	Edit Delete	
<input type="checkbox"/>	LAN	Layer 3	-	In use	Edit Delete	

Network Address Translation

Step 2: Configure Destination NAT.

Path: Policy > NAT

Add NAT Policy ×



Type: ☐ Source NAT ☒ Destination NAT ☐ Bidirectional NAT

Basics

Name:

Status: ☒ Enabled ☐ Disabled

Description:

Move To: ⓘ

Schedule:

Original Data Packet

Src Zone:

Src Address:

Destination: ☒ IP Address ☐ Network Objects

ⓘ

Services:

Translated Data Packet

Translate Src IP To: Untranslated

Translate Dst IP To:

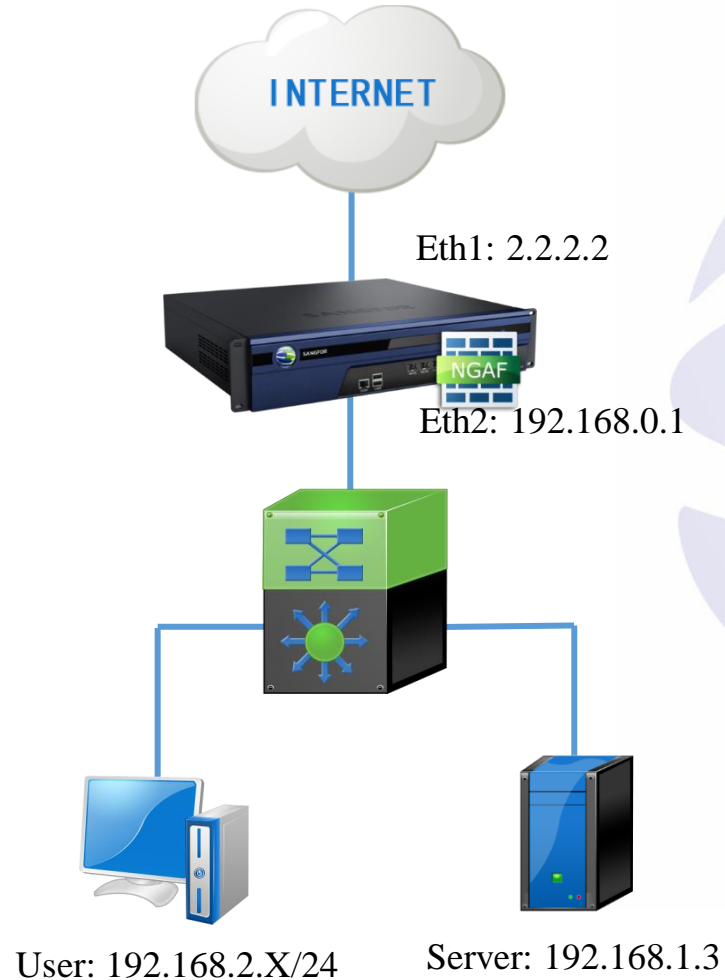
IP Address:

Translate Port To:

ⓘ To make NAT policy work, please configure local ACL or application control policy.

Allow: ☒ Add ACL policy automatically ☐ Add ACL policy manually

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.

Edit Physical Interface [X]

Basics

Name: eth1

Status: ☒ Enabled ☐ Disabled

Description: Optional

Type: Layer 3

Zone: WAN

Basic Attributes: ☒ WAN attribute

System Upgrade: ☐ Temporarily use this interface for system upgrade ⓘ

IPv4 | IPv6 | Link State Detection | Advanced

IP Assignment: ☒ Static ☐ DHCP ☐ PPPoE

Static IP: 2.2.2.2/24 ⓘ

Next-Hop IP: 2.2.2.1 ⓘ

Link Bandwidth: Outbound 1024 Mbps Inbound 1024 Mbps

Management Service

Allow: ☒ WEBUI ☒ PING ☐ SNMP ☒ SSH

Save **Cancel**

Edit Physical Interface [X]

Basics

Name: eth3

Status: ☒ Enabled ☐ Disabled

Description: Optional

Type: Layer 3

Zone: LAN

Basic Attributes: ☐ WAN attribute

System Upgrade: ☐ Temporarily use this interface for system upgrade ⓘ

IPv4 | IPv6 | Link State Detection | Advanced

IP Assignment: ☒ Static ☐ DHCP ☐ PPPoE

Static IP: 192.168.0.1/24 ⓘ

Next-Hop IP: ⓘ

Link Bandwidth: Outbound 1000 Mbps Inbound 1000 Mbps

Management Service

Allow: ☒ WEBUI ☒ PING ☐ SNMP ☐ SSH

Save **Cancel**

Bidirectional NAT Case Study



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

Network

Interfaces

Zones

Routes

Virtual Wires

DNS

DHCP

ARP

Advanced

SSL VPN

Online Users

Deployment

Local Users

Resources

Roles

Login Options

Zones

+ Add

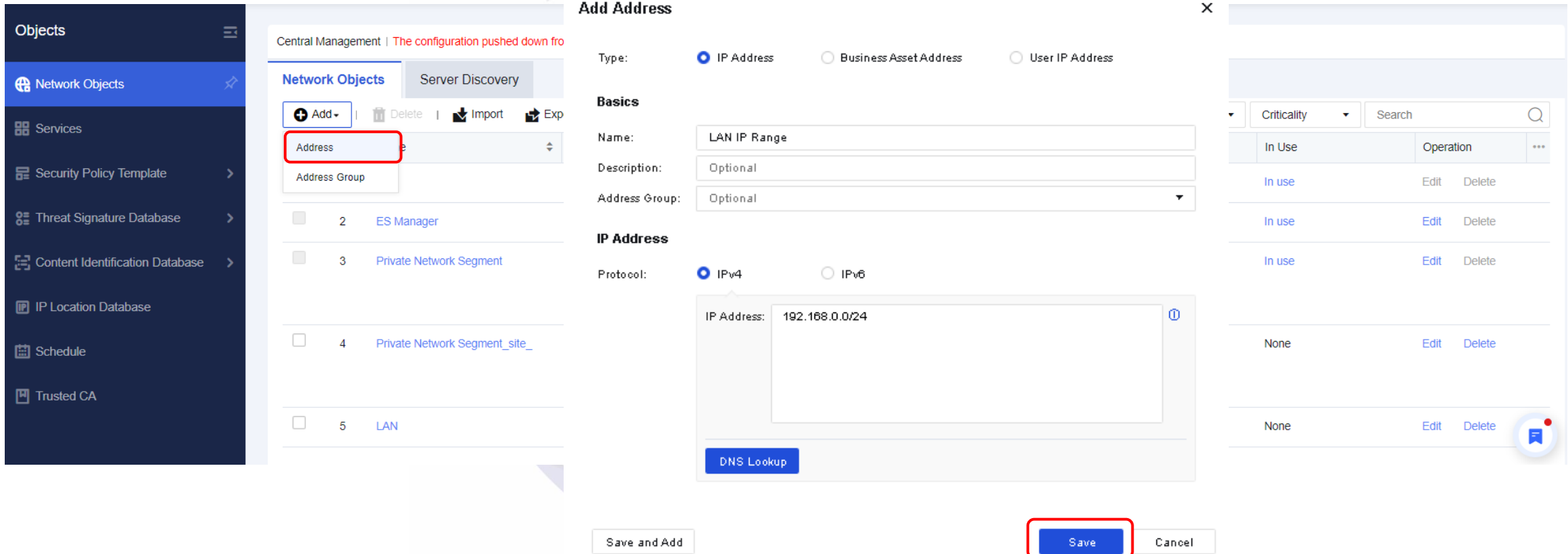
🗑 Delete

🔄 Refresh

<input type="checkbox"/>	Name	Type	Interfaces	In Use	Operation	...
<input type="checkbox"/>	L2_trust_B	Layer 2	-	None	Edit Delete	
<input type="checkbox"/>	L2_untrust_A	Layer 2	-	None	Edit Delete	
<input type="checkbox"/>	L2_untrust_B	Layer 2	-	None	Edit Delete	
<input type="checkbox"/>	L3_manage	Layer 3	eth0	In use	Edit Delete	
<input type="checkbox"/>	L3_trust_A	Layer 3	-	None	Edit Delete	
<input type="checkbox"/>	L3_trust_B	Layer 3	-	None	Edit Delete	
<input type="checkbox"/>	L3_trust_C	Layer 3	-	None	Edit Delete	
<input type="checkbox"/>	L3_untrust_A	Layer 3	-	None	Edit Delete	
<input type="checkbox"/>	L3_untrust_B	Layer 3	-	None	Edit Delete	
<input type="checkbox"/>	L3_untrust_C	Layer 3	-	None	Edit Delete	
<input type="checkbox"/>	Virtual_trust_A	Virtual wire	-	None	Edit Delete	
<input type="checkbox"/>	Virtual_trust_B	Virtual wire	-	None	Edit Delete	
<input type="checkbox"/>	Virtual_untrust_A	Virtual wire	-	None	Edit Delete	
<input type="checkbox"/>	Virtual_untrust_B	Virtual wire	-	None	Edit Delete	
<input type="checkbox"/>	WAN	Layer 3	eth1	In use	Edit Delete	
<input type="checkbox"/>	LAN	Layer 3	-	In use	Edit Delete	

Bidirectional NAT Case Study

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



The screenshot displays the Sangfor security management console interface. On the left, a sidebar menu lists various objects: Objects, Network Objects, Services, Security Policy Template, Threat Signature Database, Content Identification Database, IP Location Database, Schedule, and Trusted CA. The 'Network Objects' section is active, showing a list of objects including ES Manager, Private Network Segment, Private Network Segment_site_, and LAN. The 'Add Address' dialog box is open, showing the configuration for a new IP Address. The 'Type' is set to 'IP Address'. The 'Name' is 'LAN IP Range'. The 'Description' is 'Optional'. The 'Address Group' is 'Optional'. The 'Protocol' is set to 'IPv4'. The 'IP Address' field contains '192.168.0.0/24'. The 'Save' button is highlighted with a red box. A 'DNS Lookup' button is also visible. On the right, a table shows the status of the address group, with columns for 'In Use' and 'Operation'.

Add Address

Central Management | The configuration pushed down fro

Network Objects | Server Discovery

+ Add | Delete | Import | Exp

Address

Address Group

2 ES Manager

3 Private Network Segment

4 Private Network Segment_site_

5 LAN

Basics

Type: ☒ IP Address ☐ Business Asset Address ☐ User IP Address

Name: LAN IP Range

Description: Optional

Address Group: Optional

IP Address

Protocol: ☒ IPv4 ☐ IPv6

IP Address: 192.168.0.0/24

DNS Lookup


Save and Add Save Cancel

Criticality	Search	In Use	Operation	...
In use		Edit	Delete	
In use		Edit	Delete	
In use		Edit	Delete	
None		Edit	Delete	
None		Edit	Delete	

Bidirectional NAT Case Study

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

Add NAT Policy



Type: ☐ Source NAT ☐ Destination NAT ☒ Bidirectional NAT

Basics

Name:

Status: ☒ Enabled ☐ Disabled

Description:

Move To: ⓘ

Schedule:

Original Data Packet

Src Zone:

Src Address:

Destination: ☒ IP Address ☐ Network Objects

ⓘ

Services:

Translated Data Packet

Translate Src IP To:

Translate Dst IP To:

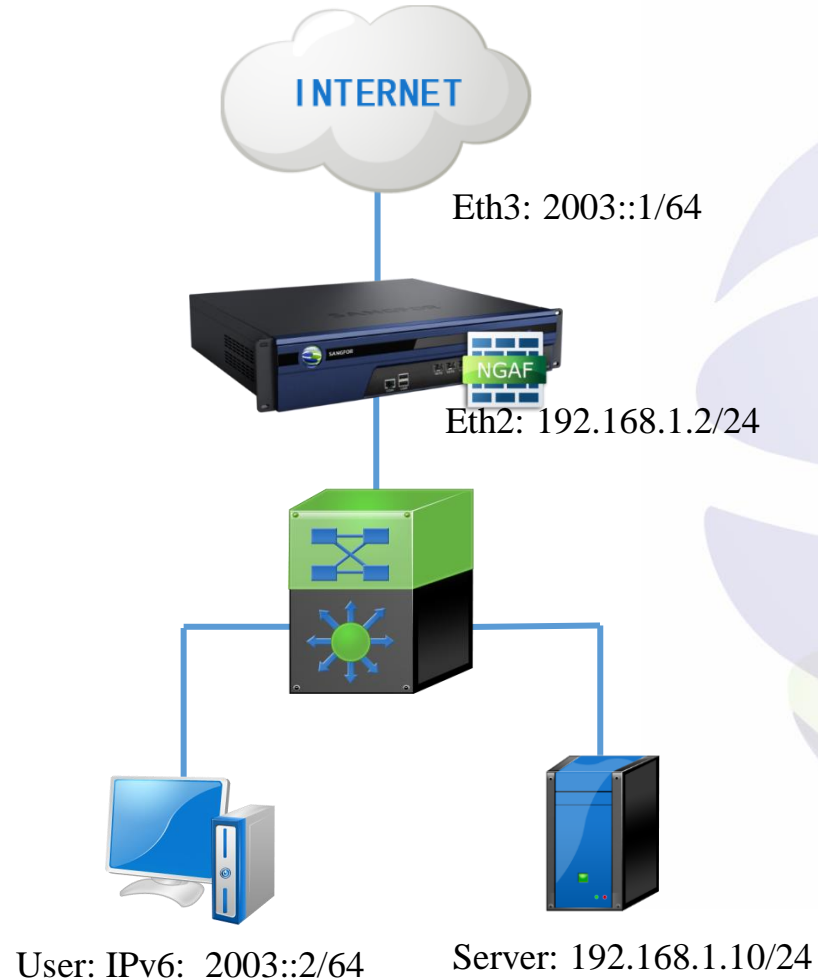
IP Address:

Translate Port To:

ⓘ To make NAT policy work, please configure local ACL or application control policy.

Allow: ☒ Add ACL policy automatically ☐ Add ACL policy manually

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.

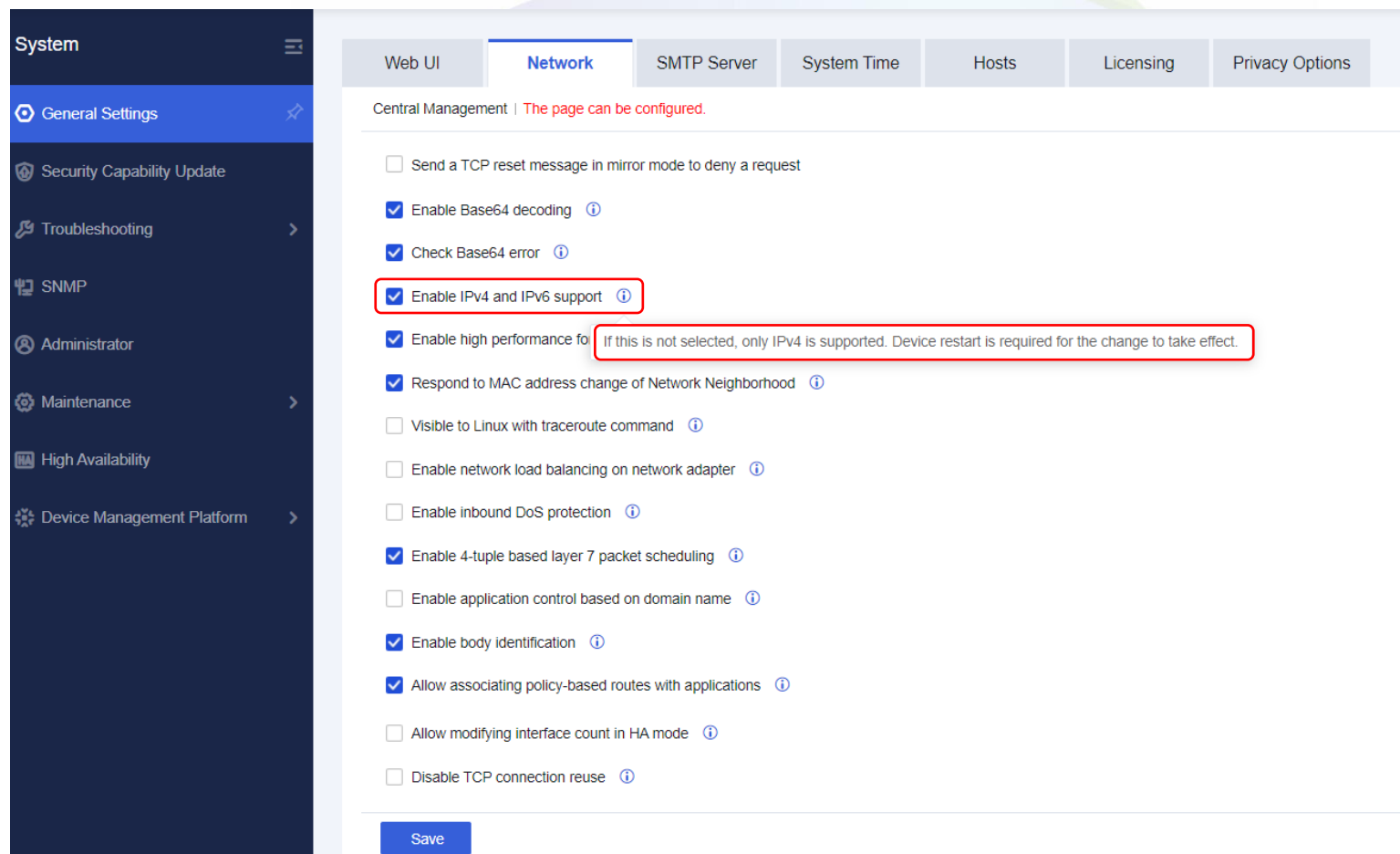
Solution: **Configure DNAT 6 to 4.**

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.

Edit Physical Interface

Basics

Name: eth1

Status: ☒ Enabled ☐ Disabled

Description: Optional

Type: Layer 3

Zone: WAN

Basic Attributes: ☒ WAN attribute

System Upgrade: ☐ Temporarily use this interface for system upgrade ⓘ

IPv4

IPv6

Link State Detection

Advanced

IP Assignment: ☒ Static ☐ DHCP

Static IP: 2003::1/64

Next-Hop IP:

Link Bandwidth: Outbound 1024 Mbps Inbound 1024 Mbps

Management Service

Allow: ☒ WEBUI ☒ PING ☐ SNMP ☒ SSH

Save

Cancel

Edit Physical Interface

Basics

Name: eth2

Status: ☒ Enabled ☐ Disabled

Description: Optional

Type: Layer 3

Zone: LAN

Basic Attributes: ☐ WAN attribute

System Upgrade: ☐ Temporarily use this interface for system upgrade ⓘ

IPv4

IPv6

Link State Detection

Advanced

IP Assignment: ☒ Static ☐ DHCP ☐ PPPoE

Static IP: 172.16.10.1/24

Next-Hop IP:

Link Bandwidth: Outbound 1000 Mbps Inbound 1000 Mbps

Management Service

Allow: ☒ WEBUI ☒ PING ☐ SNMP ☐ SSH

Save

Cancel

NAT64 Case Study

Step 4.3: Define Network object.

Path: Objects > Network Objects > Network Objects

Add Address ✕

Central Management | The configurat

Network Objects Server

+ Add 🗑️ Delete 📄 Address Group

☐ 2 ES Manager

☐ 3 Private Network S

☐ 4 Private Network S

☐ 5 LAN

Basics

Type: ☒ IP Address ☐ Business Asset Address ☐ User IP Address

Name: IPv6

Description: Optional

Address Group: Optional

IP Address

Protocol: ☐ IPv4 ☒ IPv6

IP Address: 2003::1/128

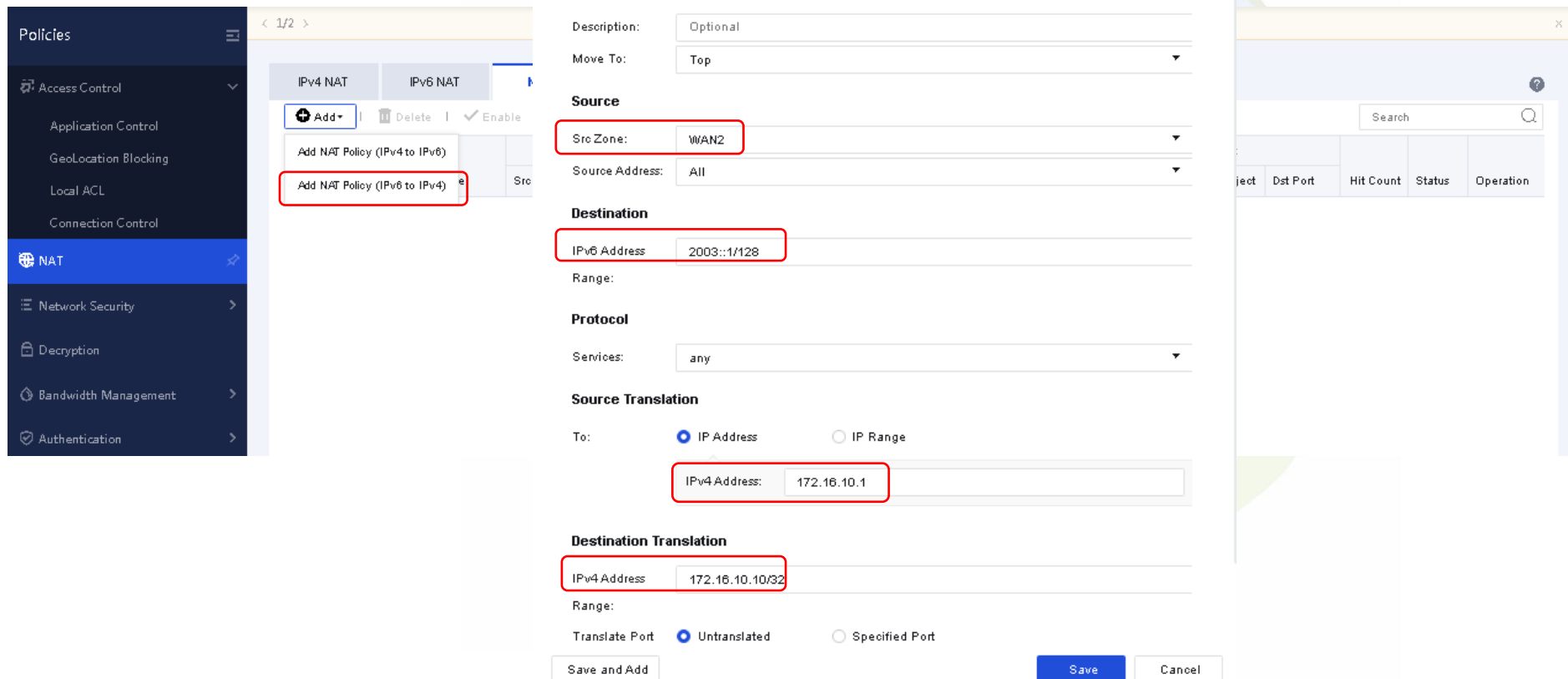
Save and Add Save Cancel

Table:

Criticality	Search	
In Use		Operation
In use		Edit Delete
In use		Edit Delete
In use		Edit Delete
None		Edit Delete
None		Edit Delete

NAT64 Case Study

Step 4.3: Configure NAT64.
Path: Policy > NAT



Add NAT Policy (IPv6 to IPv4)

Name: NAT64

Status: ☒ Enabled ☐ Disabled

Description: Optional

Move To: Top

Source

Src Zone: WAN2

Source Address: All

Destination

IPv6 Address: 2003::1/128

Range:

Protocol

Services: any

Source Translation

To: ☒ IP Address ☐ IP Range

IPv4 Address: 172.16.10.1

Destination Translation

IPv4 Address: 172.16.10.10/32

Range:

Translate Port: ☒ Untranslated ☐ Specified Port

Save and Add Save Cancel

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)

