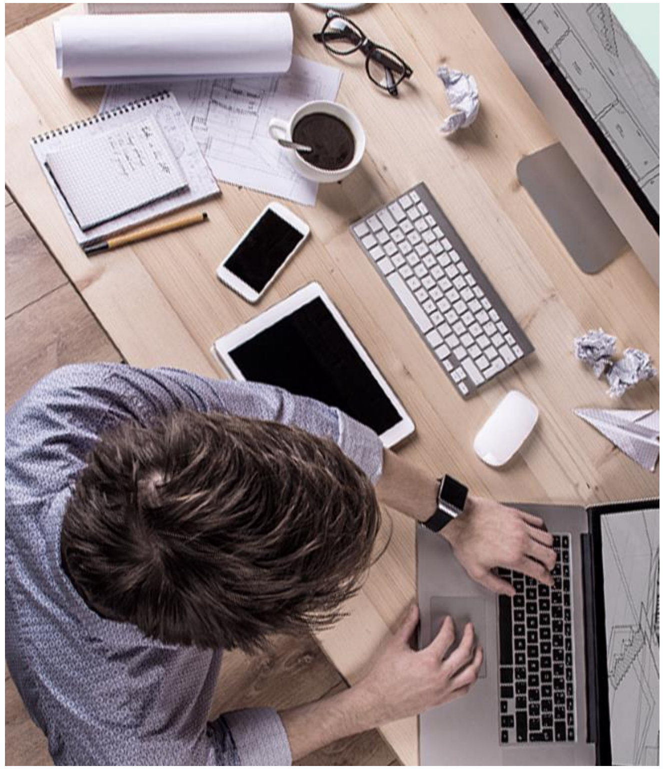
SANGFOR

Sangfor NSF V8.0.85 Associate

Deployment



1 Introduction

2 Route mode

3 Bridge mode

4 Virtual wire mode

5 Mirror Mode

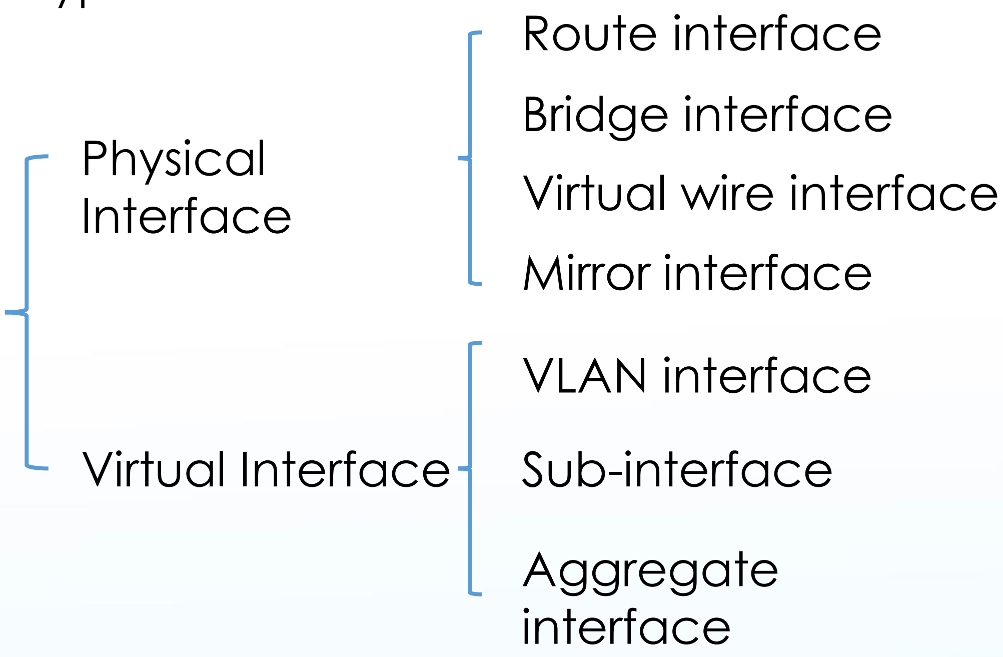
6 Mixed mode

PART 1 Introduction

Deployment Introduction

In order to make NSF adopt various scenario and improve the network expandability of NSF, there is no definite deployment of NSF to choose, it depends on the attributes of each network port.

Interface type:

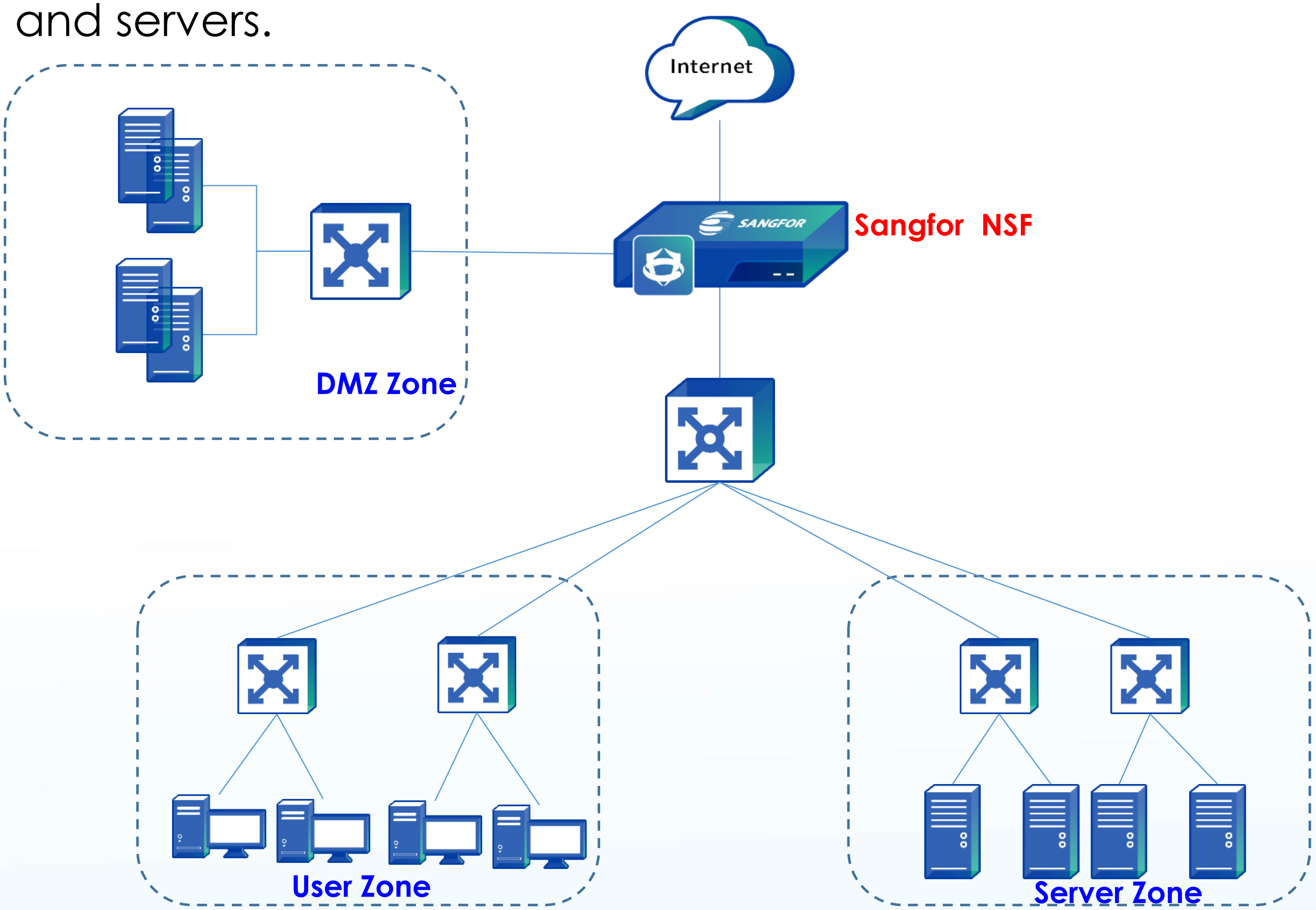


- Physical Interface
  - Route interface
  - Bridge interface
  - Virtual wire interface
  - Mirror interface
- Virtual Interface
  - VLAN interface
  - Sub-interface
  - Aggregate interface

PART 2 Route mode

Route Mode

Customer requirements: The existing topology is shown in the figure below. Use NSF to replace the existing firewall deployed at the egress to achieve security protection for intranet users and servers.



Route Mode - Requirement Analysis

What preparatory work do we need to do before deployment?

1. Interface configuration of existing devices
2. Intranet segment planning, to configure return packet routing
3. Whether there are servers to be NAT
4. Whether intranet users need proxy to access Internet
5. Access control for internal and external networks
6. Security policy configuration to achieve user requirements
7. Is the topology complete

Route Mode – Configuration Ideas

1. Configure the interface address and define the zone corresponding to the interface.

In **Network** > **Interfaces** > **Physical Interfaces**, select the interface and configure the interface type, zone, basic attributes, and IP address.

2. Configure routing.

In **Network** > **Routing**, add a new static route, configure the default route or return packet route.

3. Configure SNAT.

In **Policy > NAT**, add a new source NAT.

4. Configure DNAT.

In **Policy > NAT**, add a new destination or bidirectional NAT.

5. Configure the application control policy, put through the intranet user Internet access rights.

In **Policy > Access Control** > **Application Control**, add a new application control policy to release the data access rights from LAN to WAN.

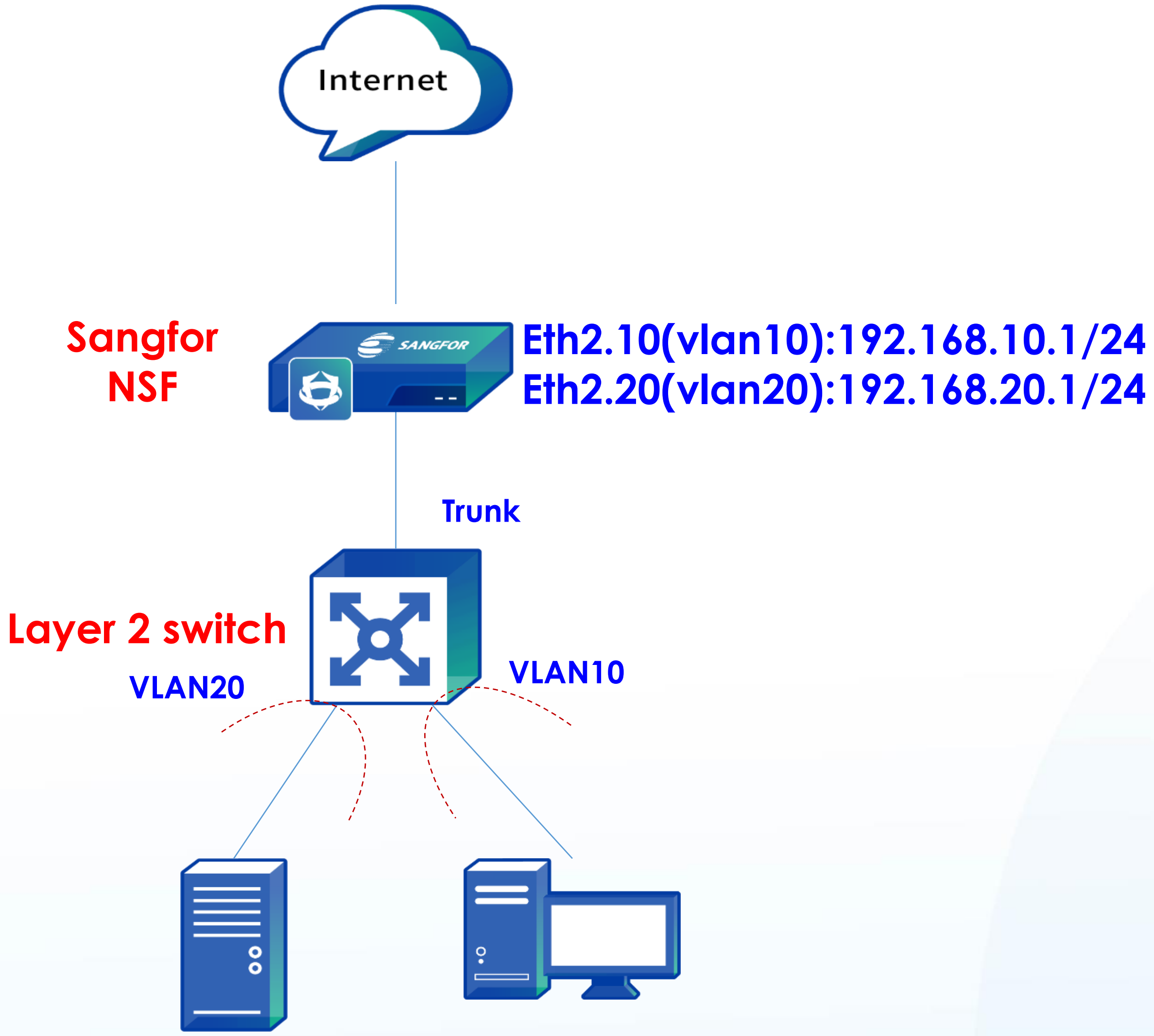
6. Configure Network security protection policies.

Such as: business protection policy, user protection policy, etc.

Single-arm Route (Trunk)

Single-arm routing refers to the interconnection between different VLANs (virtual LANs) that were originally isolated from each other by configuring a sub-interface (logical interface, there is no real physical interface) on one interface of the router. The opposite interface of LAN is Trunk.

Note: You can set Lan interface as a route, and then set the corresponding sub-interface.


Internet
Sangfor NSF
Eth2.10(vlan10):192.168.10.1/24
Eth2.20(vlan20):192.168.20.1/24
Trunk
Layer 2 switch
VLAN20
VLAN10

Single-arm Route – Configuration Ideas

1. Configure the interface address and define the zone corresponding to the interface.

In **Network** > **Interfaces** > **Physical Interfaces**, select the interface and configure the interface type, zone, basic attributes, and IP address.

2. Configure routing.

In **Network** > **Routing**, add a new static route, configure the default route or return packet route.

3. Configure SNAT.

In **Policy > NAT**, add a new source NAT.

4. Configure DNAT.

In **Policy > NAT**, add a new destination or bidirectional NAT.

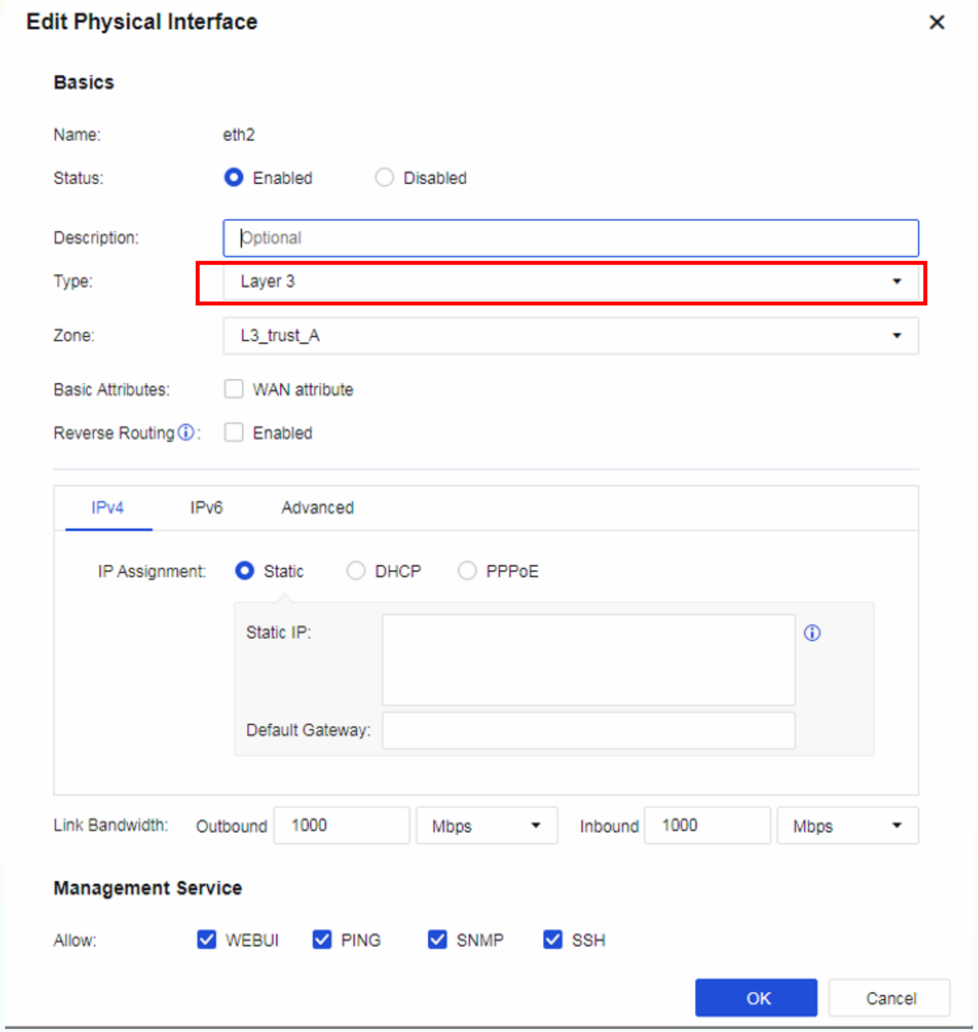
5. Configure the application control policy, put through the intranet user Internet access rights.

In **Policy > Access Control** > **Application Control**, add a new application control policy to release the data access rights from LAN to WAN.

6. Configure Network security protection policies.

Such as: business protection policy, user protection policy, etc.

Single-arm Route (trunk)



Edit Physical Interface ×

Basics

Name: eth2

Status: ● Enabled ○ Disabled

Description: Optional

Type: Layer 3

Zone: L3_trust_A

Basic Attributes: □ WAN attribute

Reverse Routing ⓘ: □ Enabled

IPv4 | IPv6 | Advanced

IP Assignment: ● Static ○ DHCP ○ PPPoE

Static IP:

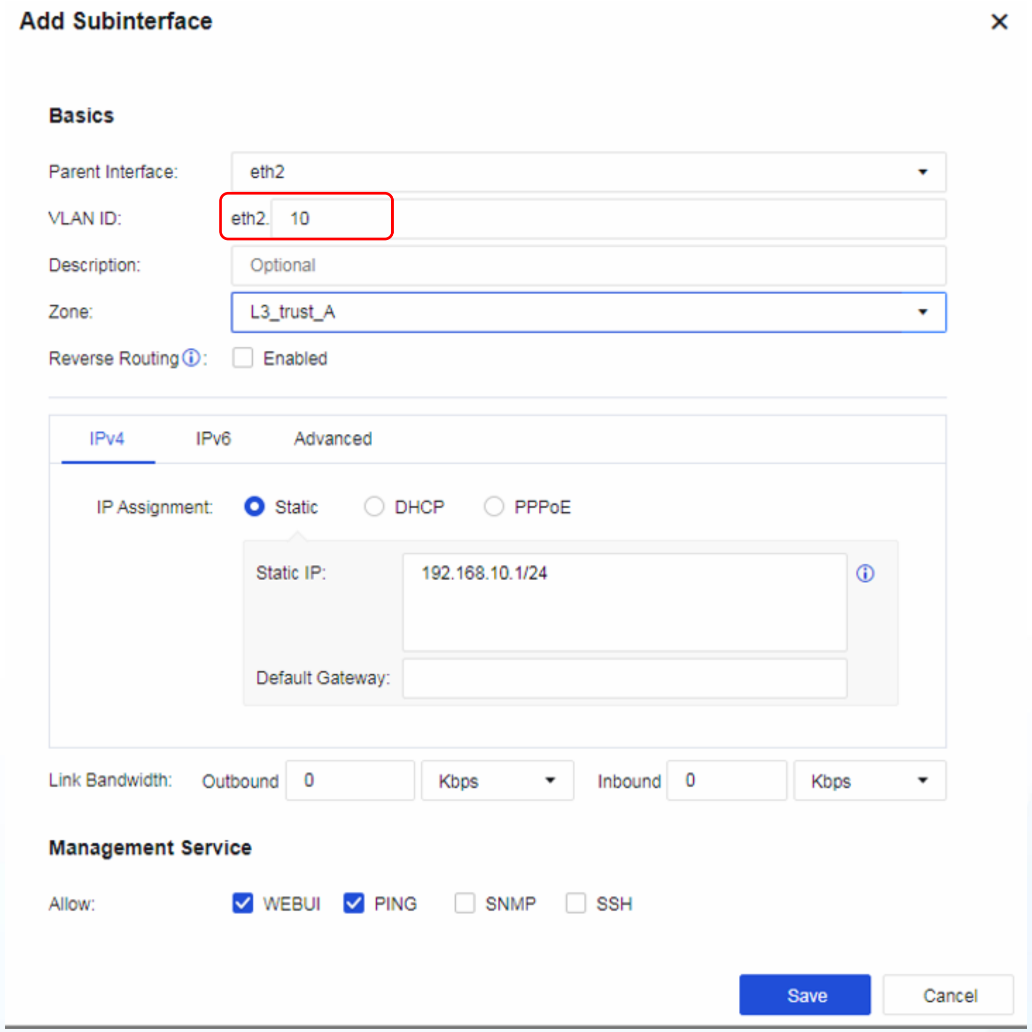
Default Gateway:

Link Bandwidth: Outbound 1000 Mbps Inbound 1000 Mbps

Management Service

Allow: ☑ WEBUI ☑ PING ☑ SNMP ☑ SSH

OK | Cancel



Add Subinterface ×

Basics

Parent Interface: eth2

VLAN ID: eth2. 10

Description: Optional

Zone: L3_trust_A

Reverse Routing ⓘ: □ Enabled

IPv4 | IPv6 | Advanced

IP Assignment: ● Static ○ DHCP ○ PPPoE

Static IP: 192.168.10.1/24

Default Gateway:

Link Bandwidth: Outbound 0 Kbps Inbound 0 Kbps

Management Service

Allow: ☑ WEBUI ☑ PING □ SNMP □ SSH

Save | Cancel

Route Mode Summary

1. In this deployment, the NSF is located between the internal network and the external network and is responsible for routing and addressing in the internal network and the external network, which is equivalent to a router. The upstream and downstream interfaces connected to the internal and external networks work at Layer 3 and need to be configured with IP addresses of different network segments.

2. This deployment supports more security features, such as NAT, policy routing, dynamic routing protocols (OSPF, BGP, RIP), and more.

3. It requires modification of the original network topology, which is a big changes to the existing environment.

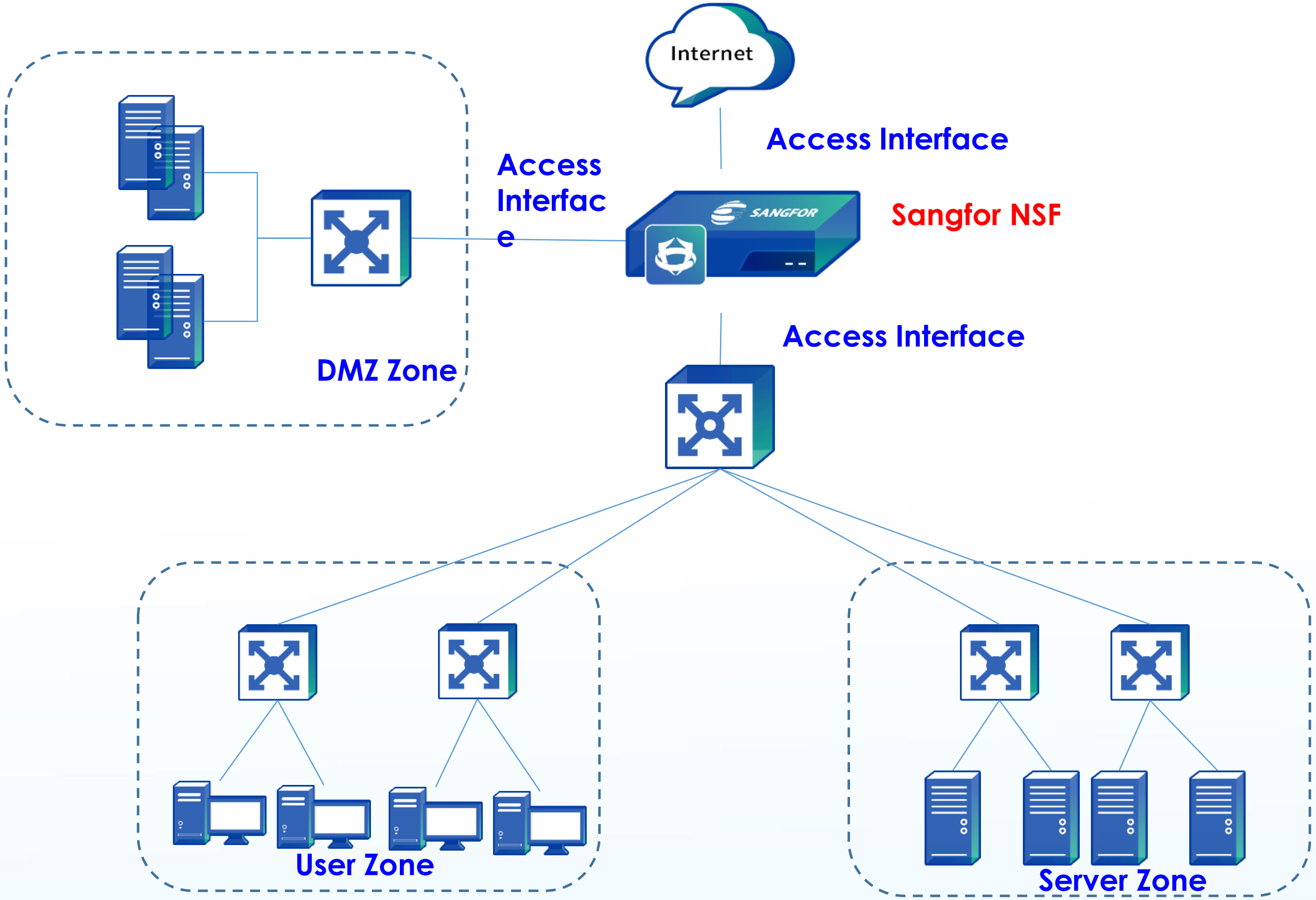
4. It is generally deployed in locations where routing and forwarding are required, such as egress routers or replacing existing routers, old firewalls, and other scenarios.

PART 3

Bridge mode

Bridge Mode

Customer requirement: Deploy an Network Secure device for security protection, but without changing the existing network environment.



Bridge Mode

What preparatory work do we need to do before deployment?

1. Define Interface
2. Define Management IP
3. Configure routing, generally the default route is used for NSF Internet access, and the return packet route is used for manage NSF
4. No need to configure NAT
5. Access control for internal and external networks
6. Security policy configuration to achieve user requirements

Bridge Mode – Configuration Ideas

1. Configure the interface address and define the zone corresponding to the interface.

In **Network** > **Interfaces** > **Physical Interfaces**, select the interface and configure the interface type, zone, basic attributes such as Access or Trunk.

2. Configure Management Interface.

In **Network** > **Interfaces** > **Physical Interfaces**, select the interface or VLAN Interface and configure the management interface IP

3. Configure Route.

In **Network > Routes**, configure the default route and return packet route.

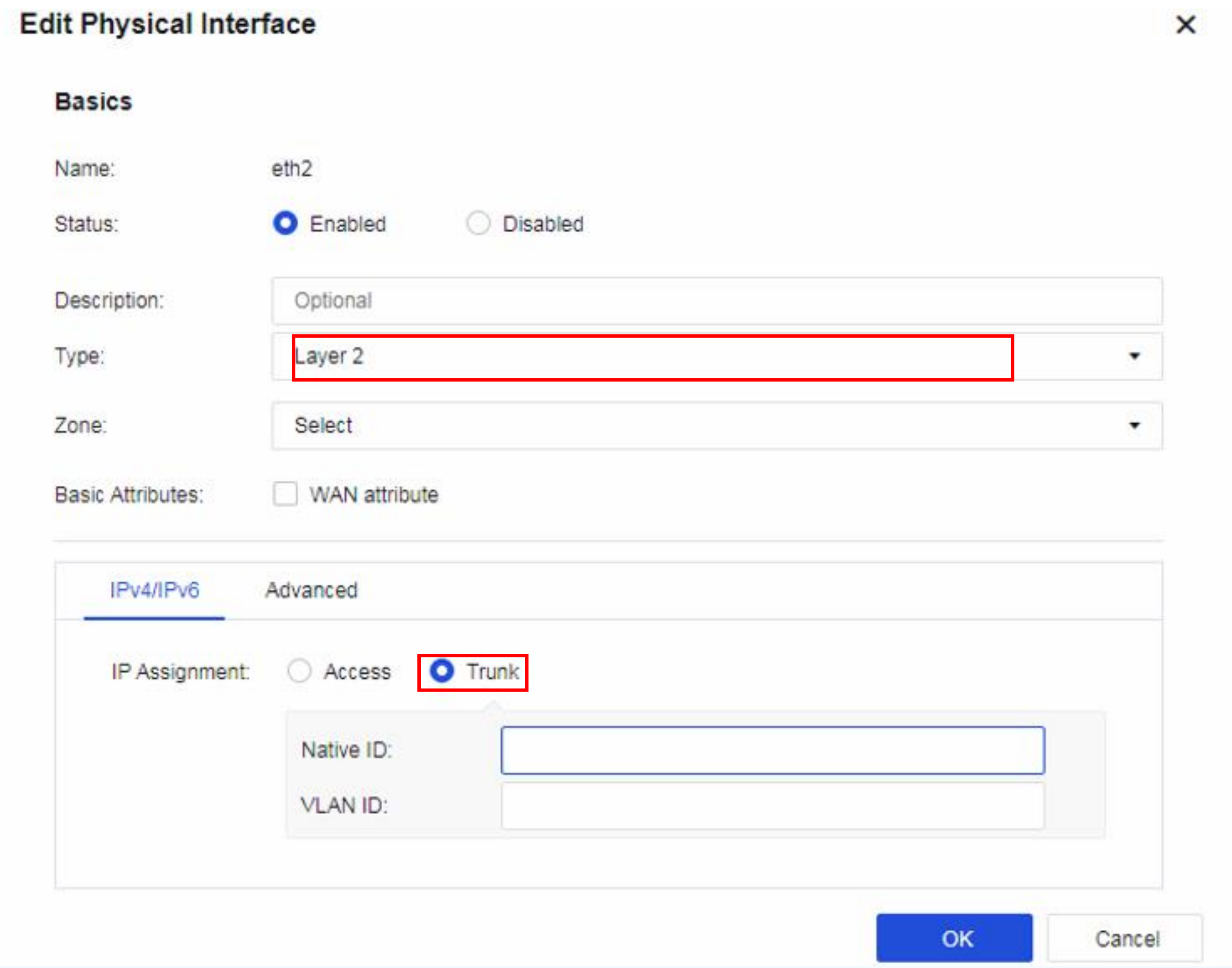
5. Configure the application control policy, put through the intranet user Internet access rights.

In **Policy > Access Control** > **Application Control**, add a new application control policy to release the data access rights from LAN to WAN.

6. Configure Network security protection policies.

Such as: business protection policy, user protection policy, etc.

Bridge Mode (Trunk)



Edit Physical Interface

Basics

Name: eth2

Status: ● Enabled ○ Disabled

Description: Optional

Type: Layer 2

Zone: Select

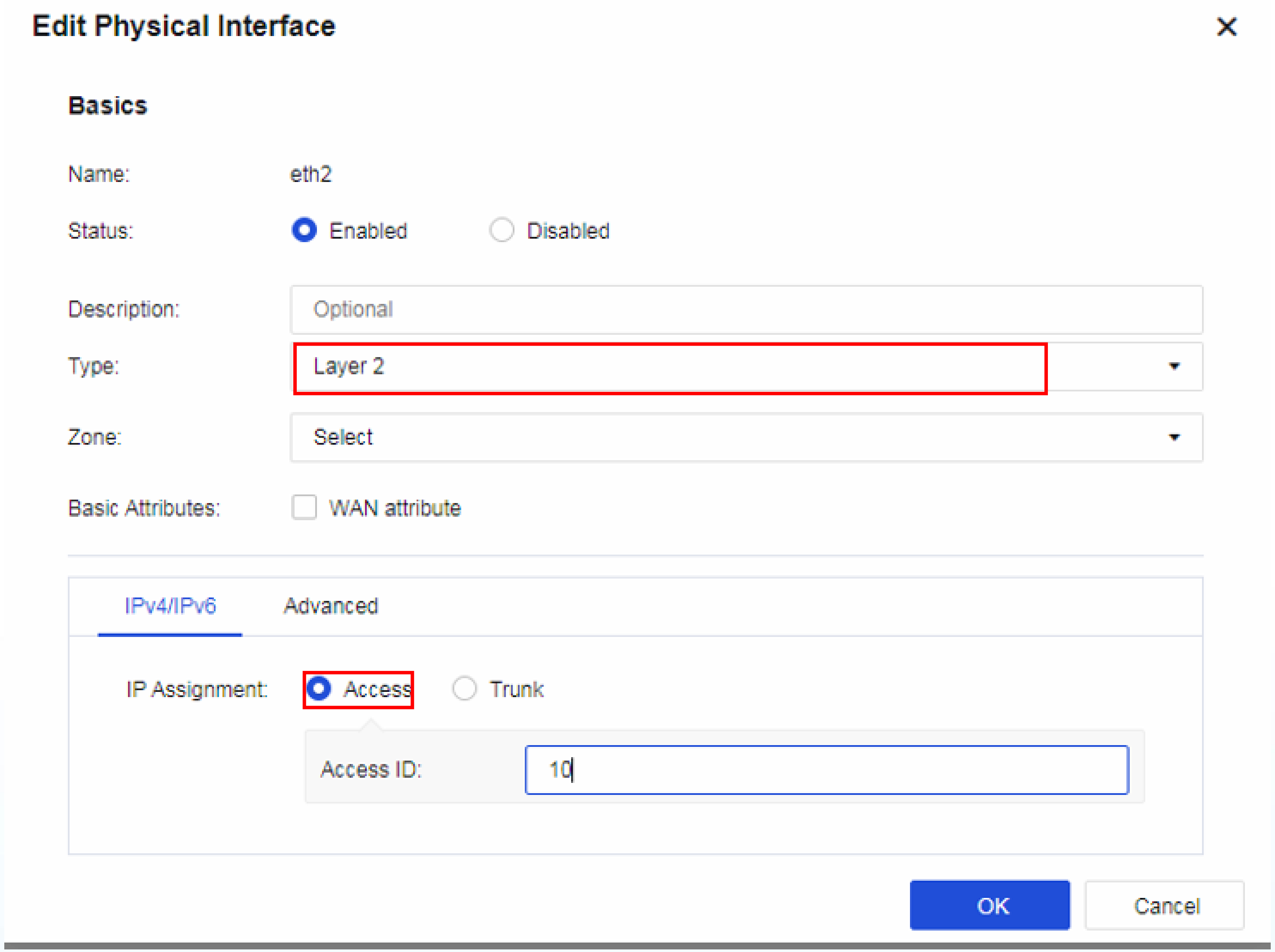
Basic Attributes: □ WAN attribute

IP Assignment: ○ Access ● Trunk

Native ID:

VLAN ID:

Bridge Mode (access)



Edit Physical Interface

Basics

Name: eth2

Status: ● Enabled ○ Disabled

Description: Optional

Type: Layer 2

Zone: Select

Basic Attributes: □ WAN attribute

IP Assignment: ● Access ○ Trunk

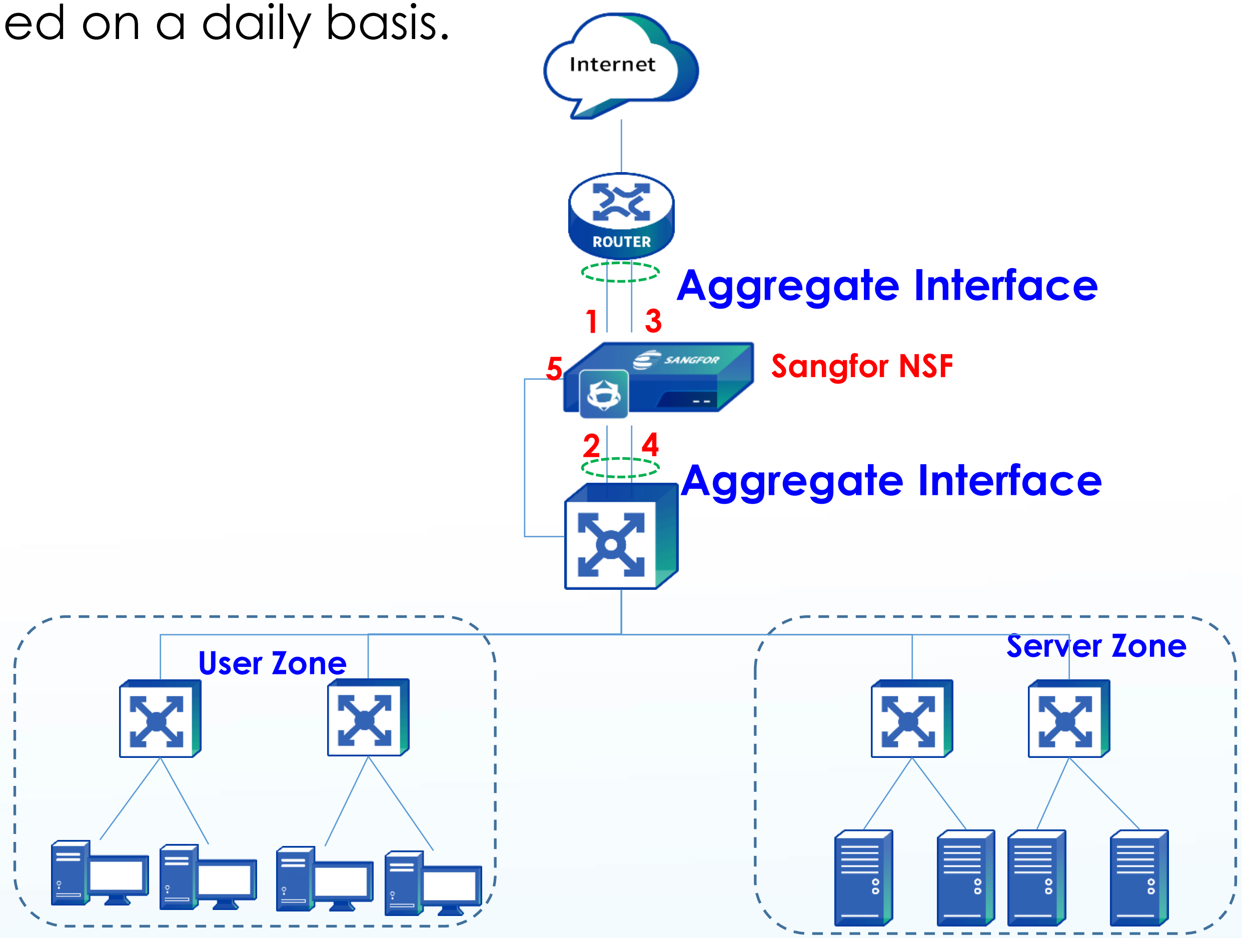
Access ID: 10

PART 4

Virtual wire mode

Virtual Wire Mode

User requirements: Router and switch configure aggregate port, requiring transparent deployment of NSF device which is the data coming in from interface 1 and outgoing from interface 2. No longer forwarded packets to other interfaces. At the same time, the firewall device can be managed on a daily basis.



Virtual Wire Mode

Virtual wire deployments are another special case of transparent deployments:

1. Like bridge deployment, the interfaces are Layer 2 interfaces, but are defined as virtual network interfaces.

2. The virtual network interfaces must exist in pairs. When forwarding packets, there is no need to check the MAC table and it is forwarded directly from the virtual wire paired interface.

3. The forwarding performance of the virtual wire interface is higher than the bridge interface, and the virtual wire interface deployment is recommended for single-input, single-output bridge environments.

Virtual Wire Mode – Configuration Ideas

1. Configure the interface address and define the zone corresponding to the interface.

In **Network** > **Interfaces** > **Physical Interfaces**, select the interface and configure the interface type, zone and interface pair.

2. Configure Management Interface.

In **Network** > **Interfaces** > **Physical Interfaces**, select the interface and configure the management interface IP

3. Configure Route.

In **Network > Routes**, configure the default route and return packet route.

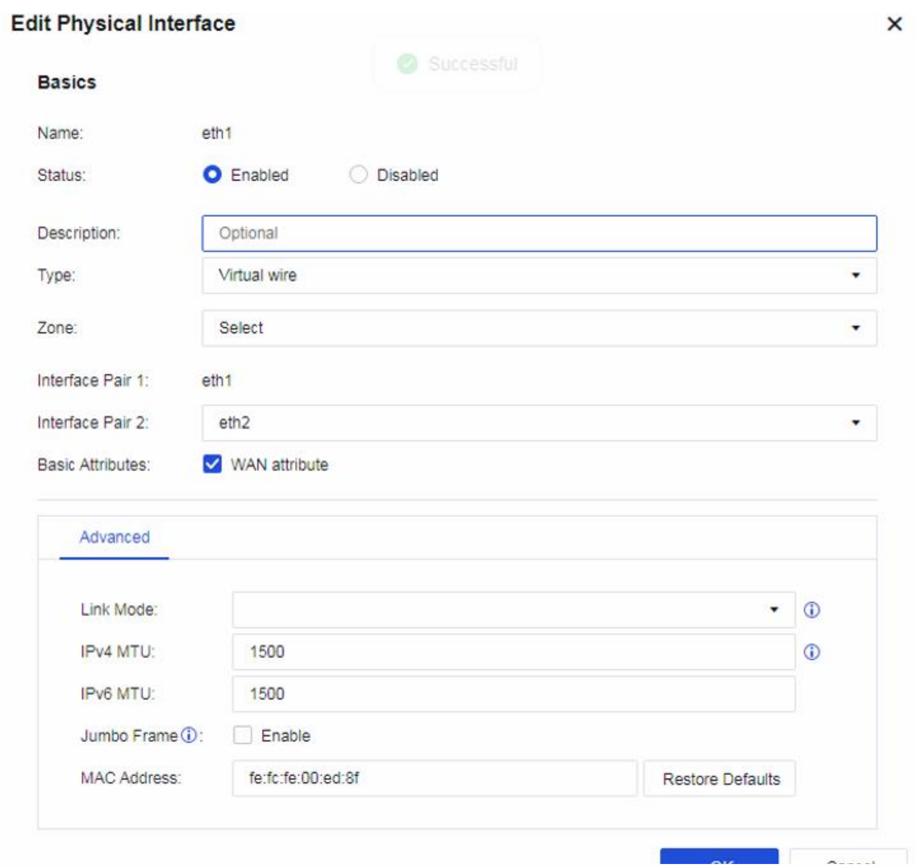
5. Configure the application control policy, put through the intranet user Internet access rights.

In **Policy > Access Control** > **Application Control**, add a new application control policy to release the data access rights from LAN to WAN.

6. Configure Network security protection policies.

Such as: business protection policy, user protection policy, etc.

Virtual Wire Mode



Edit Physical Interface

Successful

Basics

Name: eth1

Status: ● Enabled ○ Disabled

Description: Optional

Type: Virtual wire

Zone: Select

Interface Pair 1: eth1

Interface Pair 2: eth2

Basic Attributes: ☑ WAN attribute

Advanced

Link Mode:

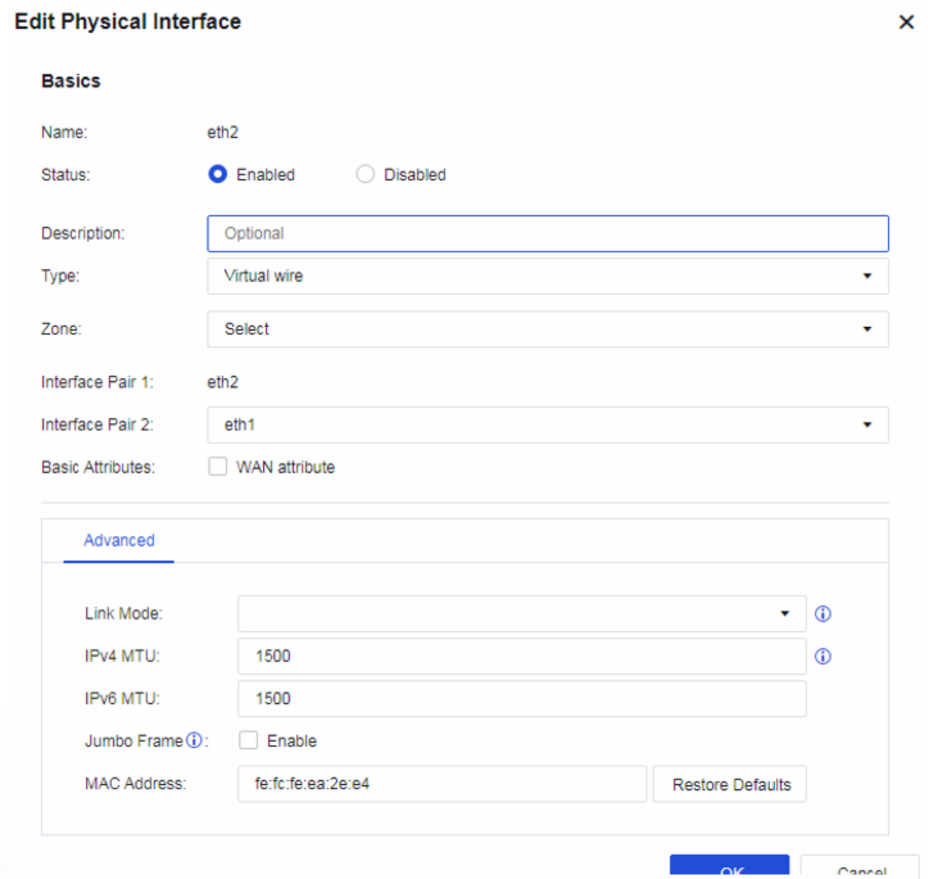
IPv4 MTU: 1500

IPv6 MTU: 1500

Jumbo Frame: □ Enable

MAC Address: fe:fc:fe:00:ed:8f

Restore Defaults



Edit Physical Interface

Basics

Name: eth2

Status: ● Enabled ○ Disabled

Description: Optional

Type: Virtual wire

Zone: Select

Interface Pair 1: eth2

Interface Pair 2: eth1

Basic Attributes: □ WAN attribute

Advanced

Link Mode:

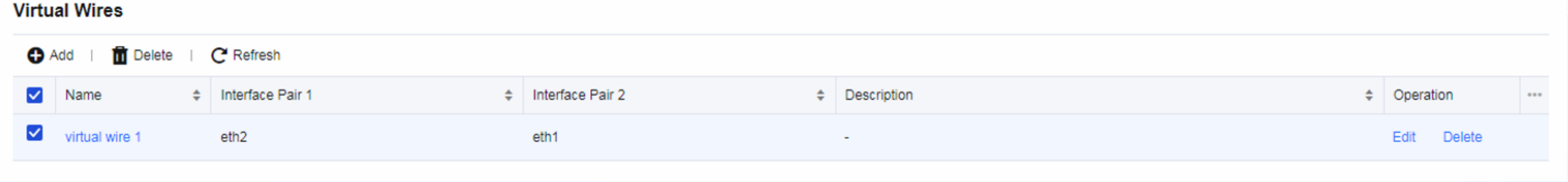
IPv4 MTU: 1500

IPv6 MTU: 1500

Jumbo Frame: □ Enable

MAC Address: fe:fc:fe:ea:2e:e4

Restore Defaults



Virtual Wires

Add | Delete | Refresh

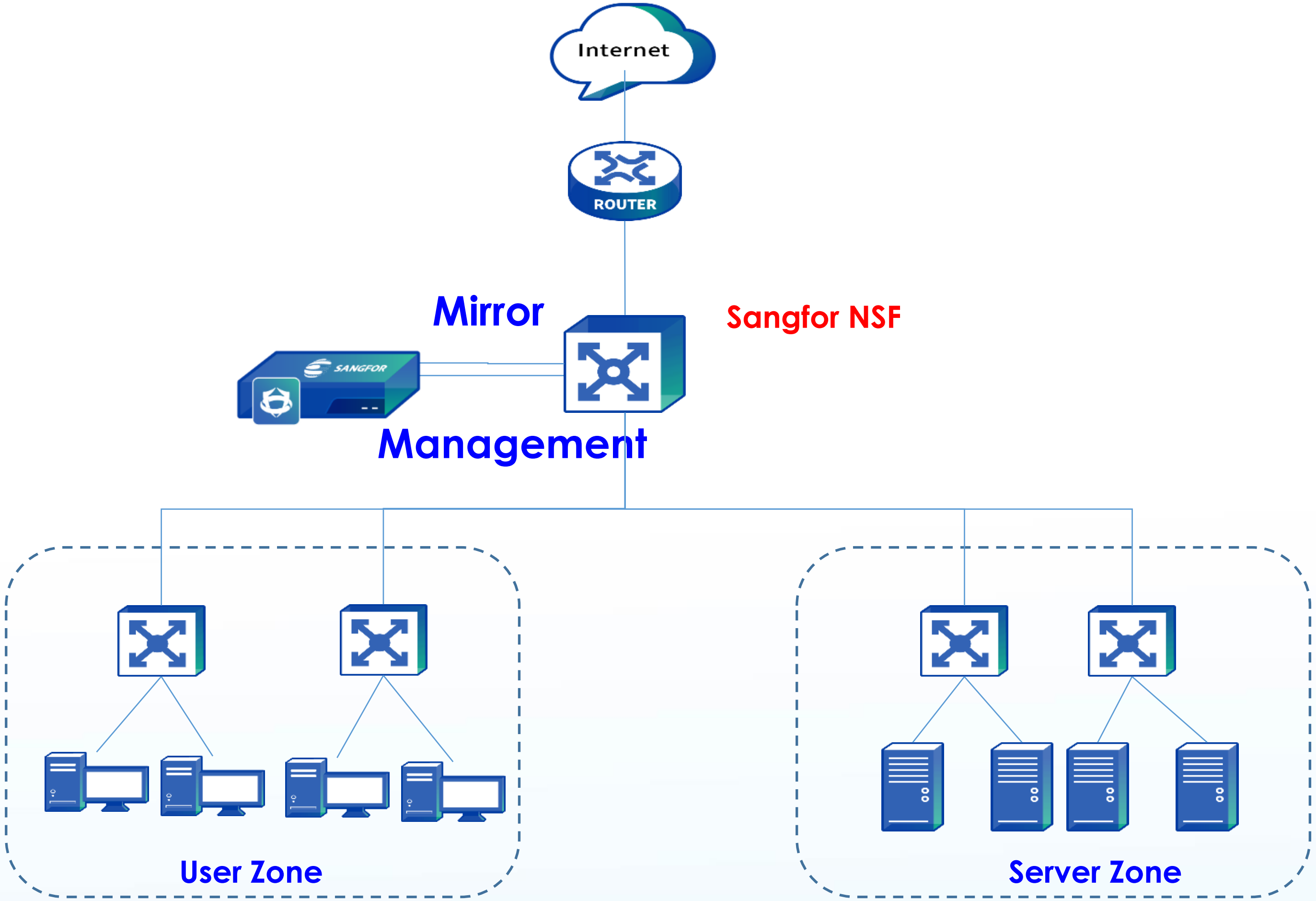
☑	Name	Interface Pair 1	Interface Pair 2	Description	Operation
☑	virtual wire 1	eth2	eth1	-	Edit Delete

PART 5

Mirror mode

Mirror mode

Requirements: Detect the network risk but don’t interrupt the network.



Mirror Mode – Configuration Ideas

1. Configure the interface address and define the zone corresponding to the interface.

In **Network** > **Interfaces** > **Physical Interfaces**, select the interface and configure the interface type, zone traffic statistic and network object.

2. Configure Management Interface.

In **Network** > **Interfaces** > **Physical Interfaces**, select the interface and configure the management interface IP

3. Configure Route.

In **Network > Routes**, configure the default route.

5. Configure the TCP reset message in mirror mode

In **System > General Setting**> **Network**, enable the **Send a TCP reset message in mirror mode to deny a request**.

6. Configure Network security protection policies.

Such as: business protection policy, user protection policy, etc.

Mirror Mode

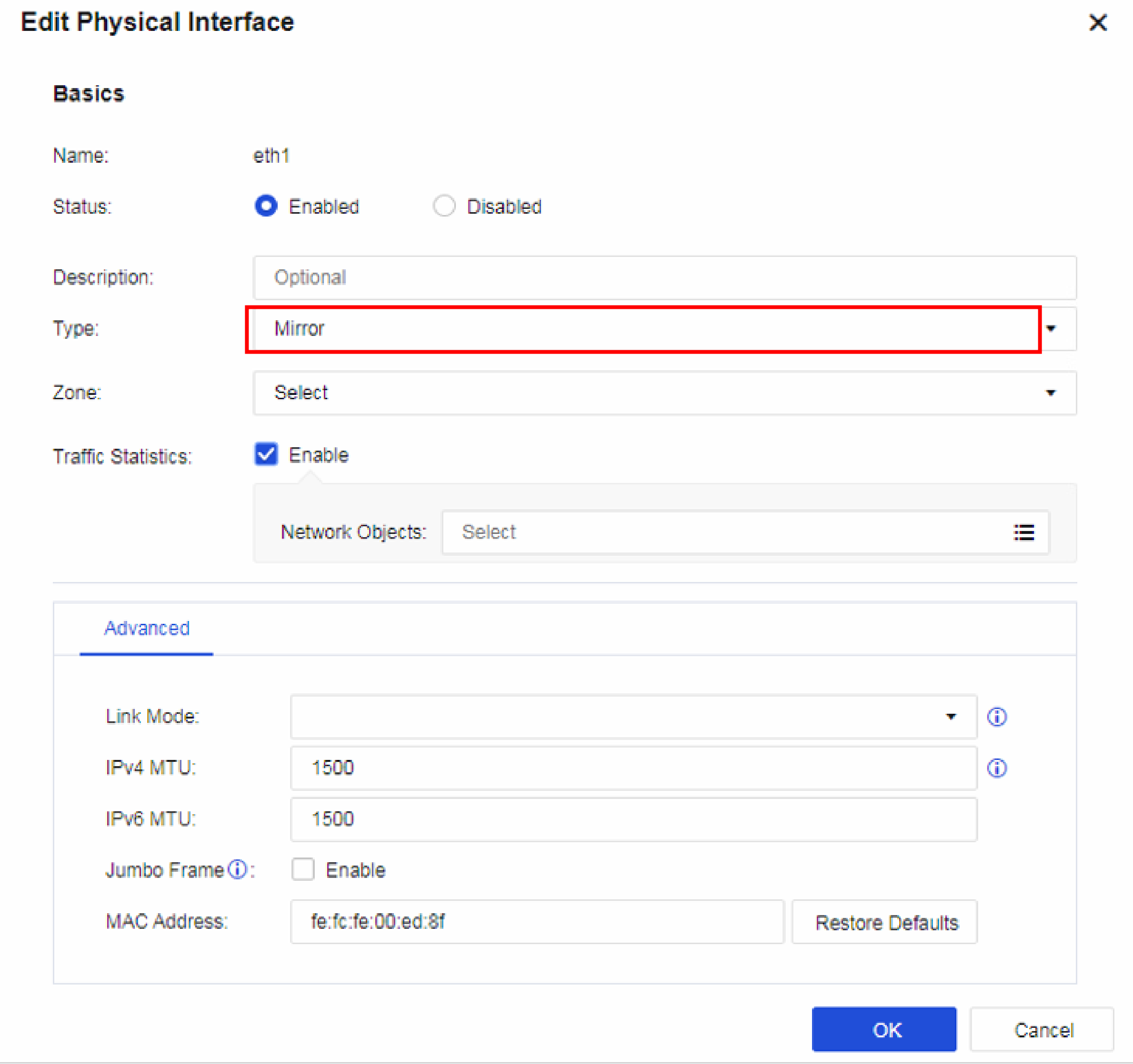
1. The device is mounted on the existing network without affecting the existing network structure. By using port mirroring technology mirrors traffic to the NSF, achieve analysis and processing of packets.

2. A separate management interface is required to manage the device.

3. Configure the TCP reset message in mirror mode.

4. The only features supported by bypass deployment are:
   1. APT
   2. PVS
   3. WAF
   4. IPS
   5. DLP

Mirror mode



Edit Physical Interface

Basics

Name: eth1

Status: ● Enabled ○ Disabled

Description: Optional

Type: Mirror

Zone: Select

Traffic Statistics: ☑ Enable

Network Objects: Select

Advanced

Link Mode:

IPv4 MTU: 1500

IPv6 MTU: 1500

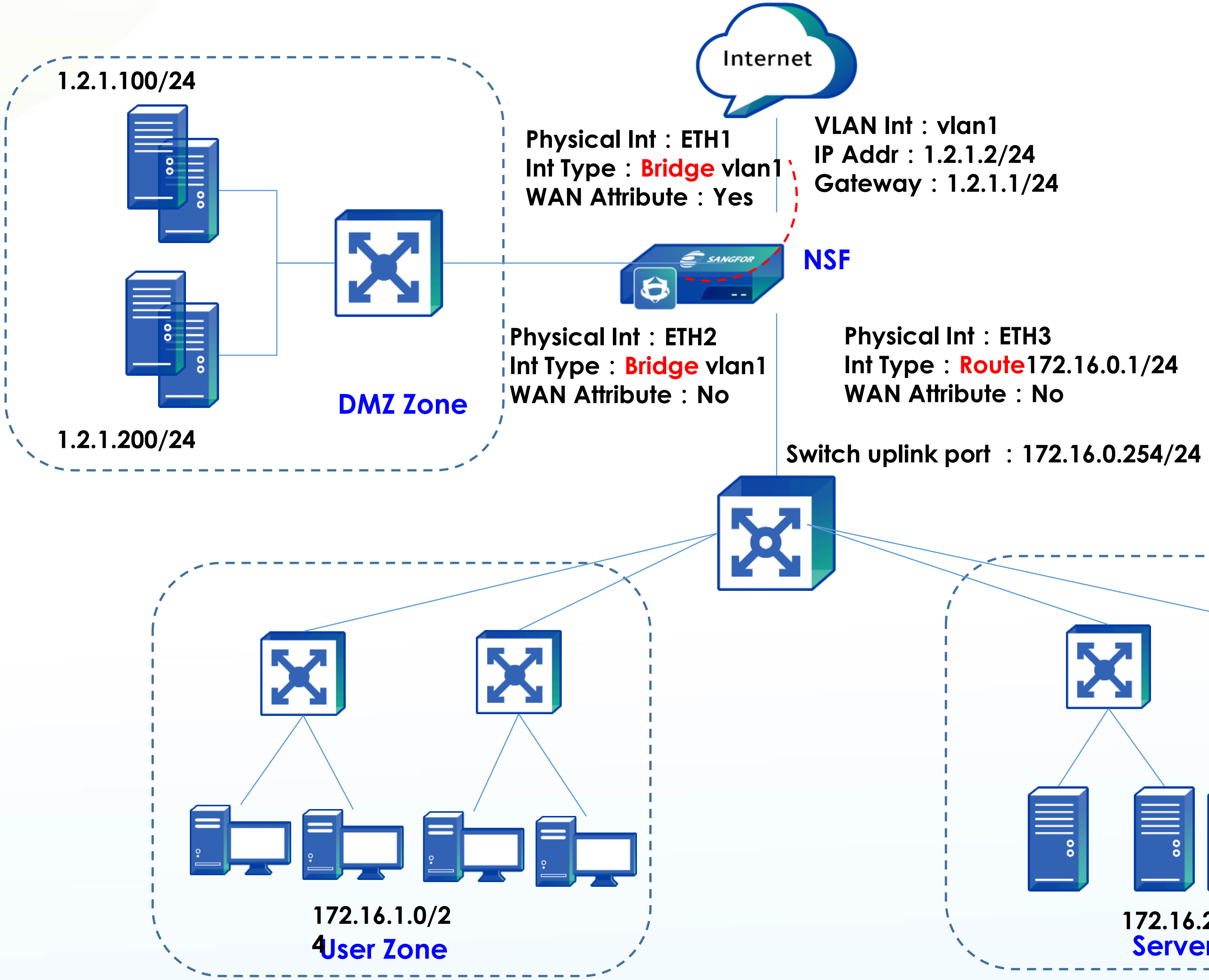
Jumbo Frame: □ Enable

MAC Address: fe:fc:fe:00:ed:8f

PART 6

Mixed mode

Mixed Mode Case Study



Requirement:
Customer have a server farm and all server configure Public IP as IP address. Internal user configure as Private IP address and through NAT to access internet. NSF need to deploy as a internet Gateway to protect Server and internal user.

Recommendations:
Deploy as Mixed mode(gateway mode + bridge mode). NSF connect internet and server by bridge(access) interface , internal user connect to route interface.

Mixed Mode Deployment Analysis

1. Since the servers all have public IP addresses, the interface eth1 of the AF device connecting to the public line and the interface eth2 connecting to the server group use transparent access interface and set the same VLAN ID. All users can access the server group directly through the public IP.

2. Add a new VLAN1 interface, assign a public IP address, and allocate the area to the external network area.

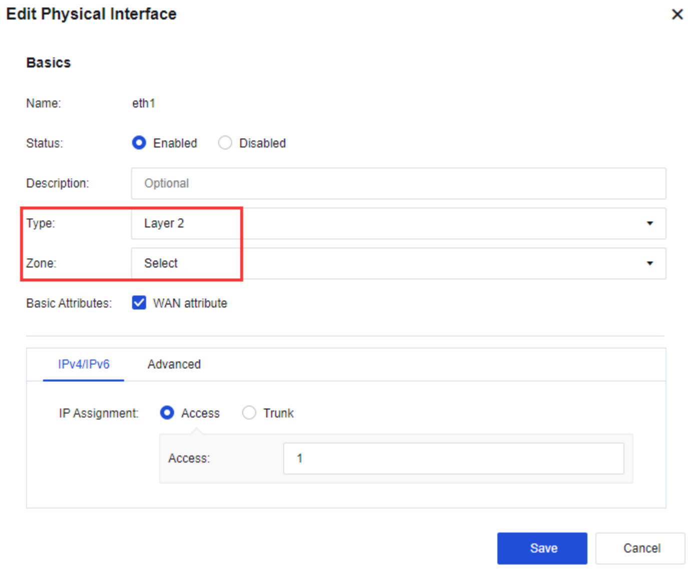
3. The eth3 of the NSF device is connected to the intranet using routing interface, set the IP address of the same network segment as the intranet switch, and set a static route to communicate with the intranet.

4. When an LAN user access Internet, the source IP address is translated to the IP address of the VLAN1 interface. When an LAN user access Internet, the source IP address is translated to the IP address of the VLAN1 interface. According to the requirement, divided into a layer 2 area to select the network port eth1 and eth2, divide two Layer 3 zone, where the external zone selects VLAN interface vlan1 and the internal zone selects interface eth3.

Mixed Mode Case Study

Configuration Step:

1. Configure interface eth1,eth2 and eth3:



Edit Physical Interface ×

Basics

Name: eth1

Status: ● Enabled ○ Disabled

Description: Optional

Type: Layer 2

Zone: Select

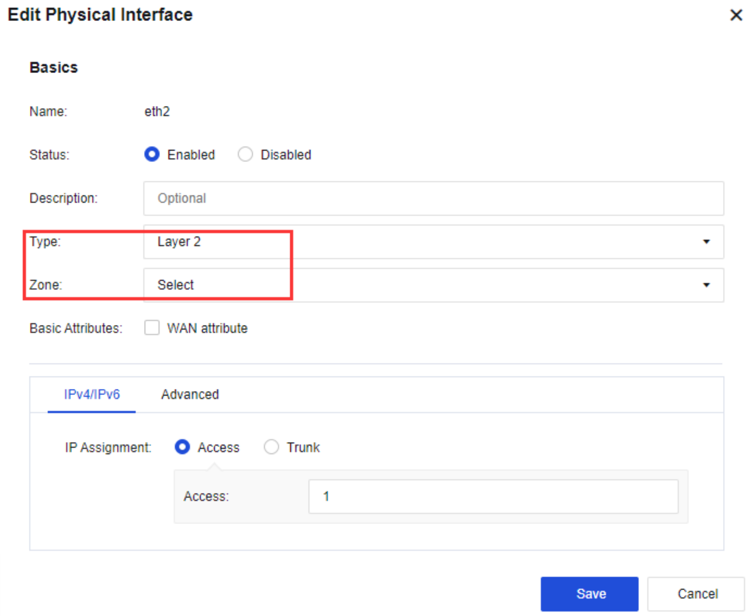
Basic Attributes: ☑ WAN attribute

IPv4/IPv6 | Advanced

IP Assignment: ● Access ○ Trunk

Access: 1

Save | Cancel



Edit Physical Interface ×

Basics

Name: eth2

Status: ● Enabled ○ Disabled

Description: Optional

Type: Layer 2

Zone: Select

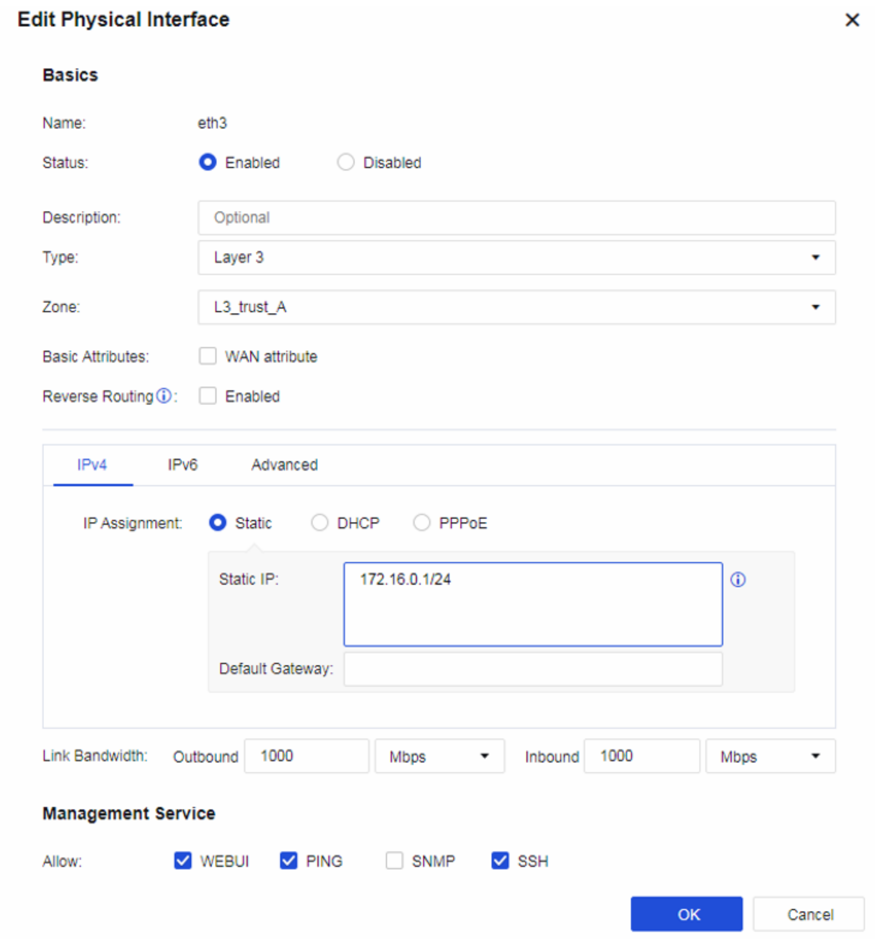
Basic Attributes: □ WAN attribute

IPv4/IPv6 | Advanced

IP Assignment: ● Access ○ Trunk

Access: 1

Save | Cancel



Edit Physical Interface ×

Basics

Name: eth3

Status: ● Enabled ○ Disabled

Description: Optional

Type: Layer 3

Zone: L3_trust_A

Basic Attributes: □ WAN attribute

Reverse Routing ⓘ: □ Enabled

IPv4 | IPv6 | Advanced

IP Assignment: ● Static ○ DHCP ○ PPPoE

Static IP: 172.16.0.1/24 ⓘ

Default Gateway:

Link Bandwidth: Outbound 1000 Mbps Inbound 1000 Mbps

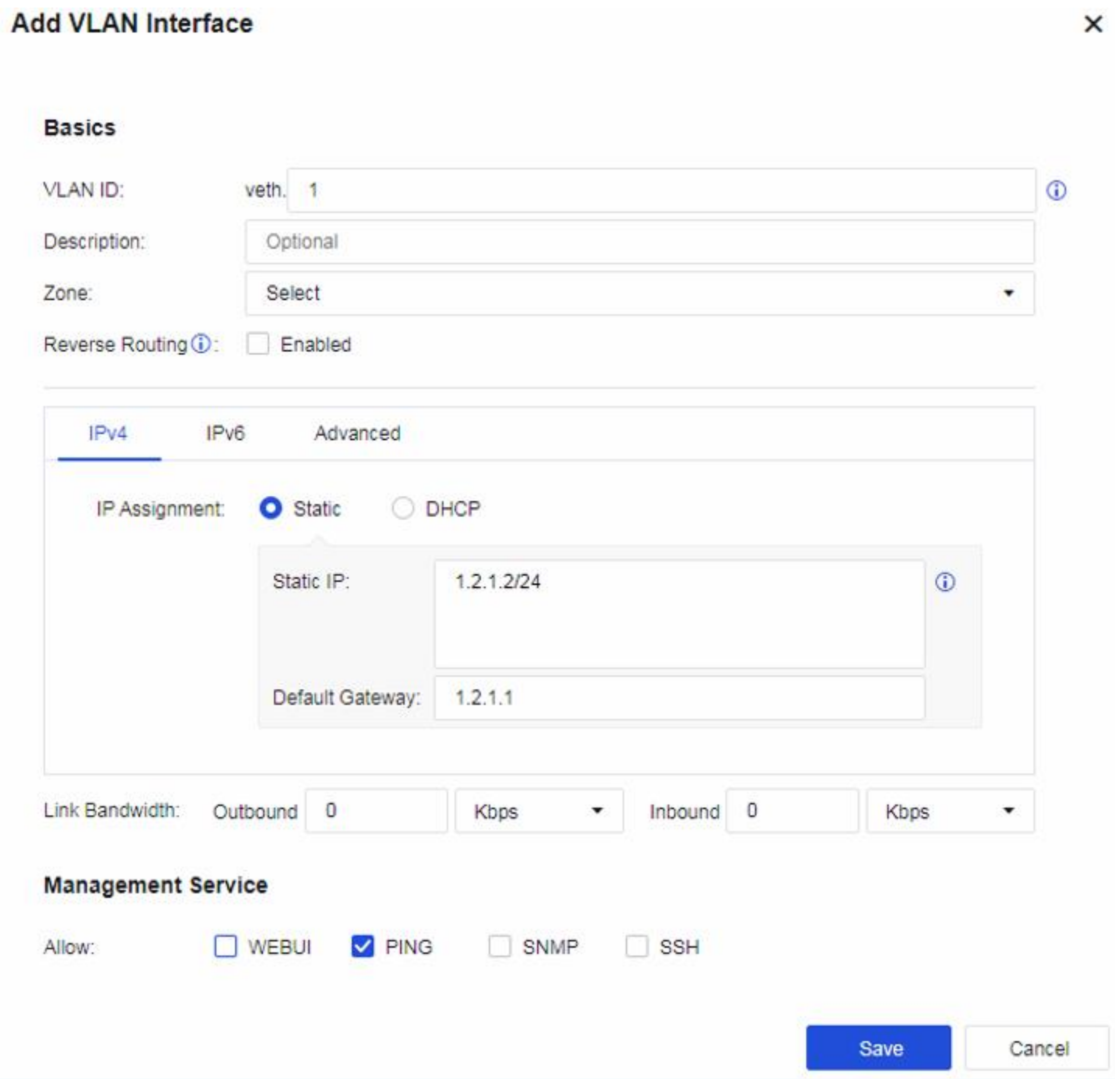
Management Service

Allow: ☑ WEBUI ☑ PING □ SNMP ☑ SSH

OK | Cancel

Mixed Mode Case Study

2. VLAN interface：



Add VLAN Interface

Basics

VLAN ID: veth. 1

Description: Optional

Zone: Select

Reverse Routing: □ Enabled

IP Assignment: ● Static ○ DHCP

Static IP: 1.2.1.2/24

Default Gateway: 1.2.1.1

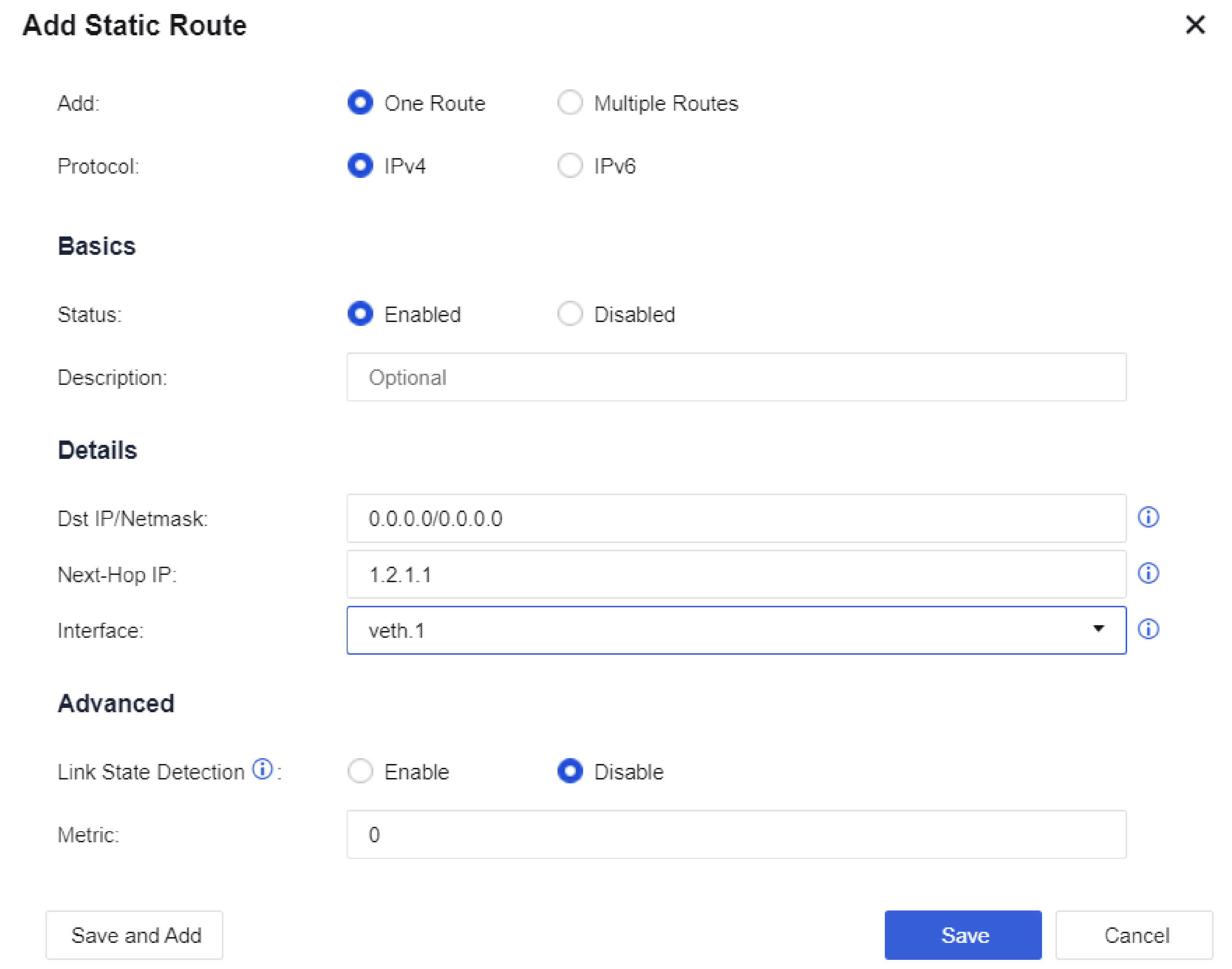
Link Bandwidth: Outbound 0 Kbps Inbound 0 Kbps

Management Service

Allow: □ WEBUI ☑ PING □ SNMP □ SSH

Mixed Mode Case Study

3. Route:



Add Static Route

Add: ● One Route ○ Multiple Routes

Protocol: ● IPv4 ○ IPv6

Basics

Status: ● Enabled ○ Disabled

Description: Optional

Details

Dst IP/Netmask: 0.0.0.0/0.0.0.0

Next-Hop IP: 1.2.1.1

Interface: veth.1

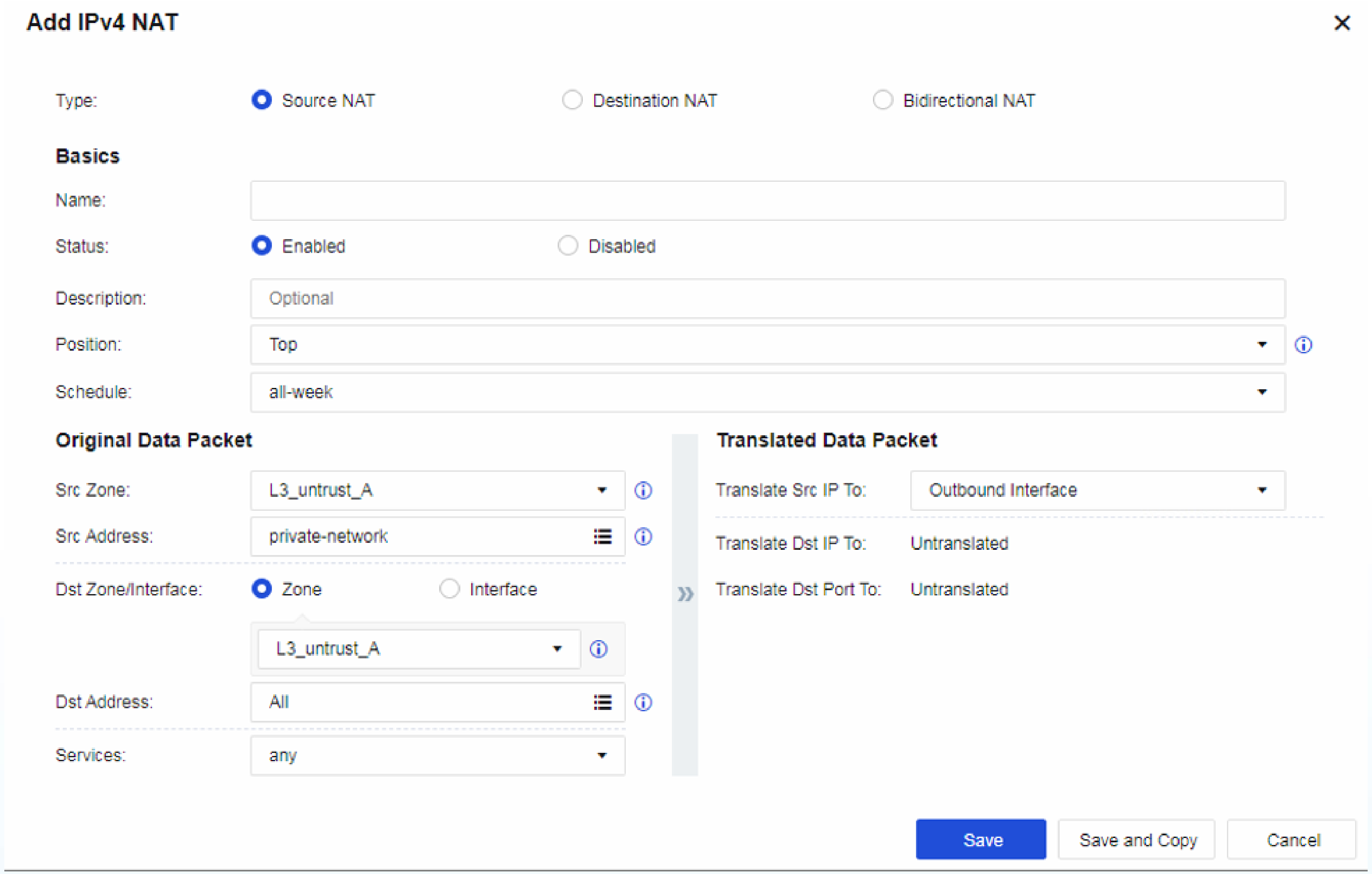
Advanced

Link State Detection: ○ Enable ● Disable

Metric: 0

Mixed Mode Case Study

4. Configure the IP group and source NAT.



Add IPv4 NAT

Type: ● Source NAT ○ Destination NAT ○ Bidirectional NAT

Basics

Name:

Status: ● Enabled ○ Disabled

Description: Optional

Position: Top

Schedule: all-week

Original Data Packet

Src Zone: L3_untrust_A

Src Address: private-network

Dst Zone/Interface: ● Zone ○ Interface

L3_untrust_A

Dst Address: All

Services: any

Translated Data Packet

Translate Src IP To: Outbound Interface

Translate Dst IP To: Untranslated

Translate Dst Port To: Untranslated

SANGFOR

THANK YOU

Technical Support Service

Email: tech.support@sangfor.com

Community: community.sangfor.com