Routing – Policy Route

Supported Devices

ZyWALL 110
ZyWALL 310
ZyWALL 1100
USG 40*
USG40W*
USG60
USG60W
USG110
USG210
USG310
USG1100
USG1900
USG20-VPN**
USG20W-VPN**
USG2200-VPN

** OPT port can be configured to function as a secondary WAN.*

*** SFP port can be configured to function as a secondary WAN.*

Overview

Use policy routes to override the ZyWALL/USG's default routing behavior in order to send packets through the appropriate interface and/or VPN tunnel(s).

Traditionally, routing is based on the destination address only and the ZyWALL/USG takes the shortest path to forward a packet. IP Policy Routing provides a mechanism to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator. Policy-based routing is applied to incoming packets on a per interface bases, prior to the normal routing.

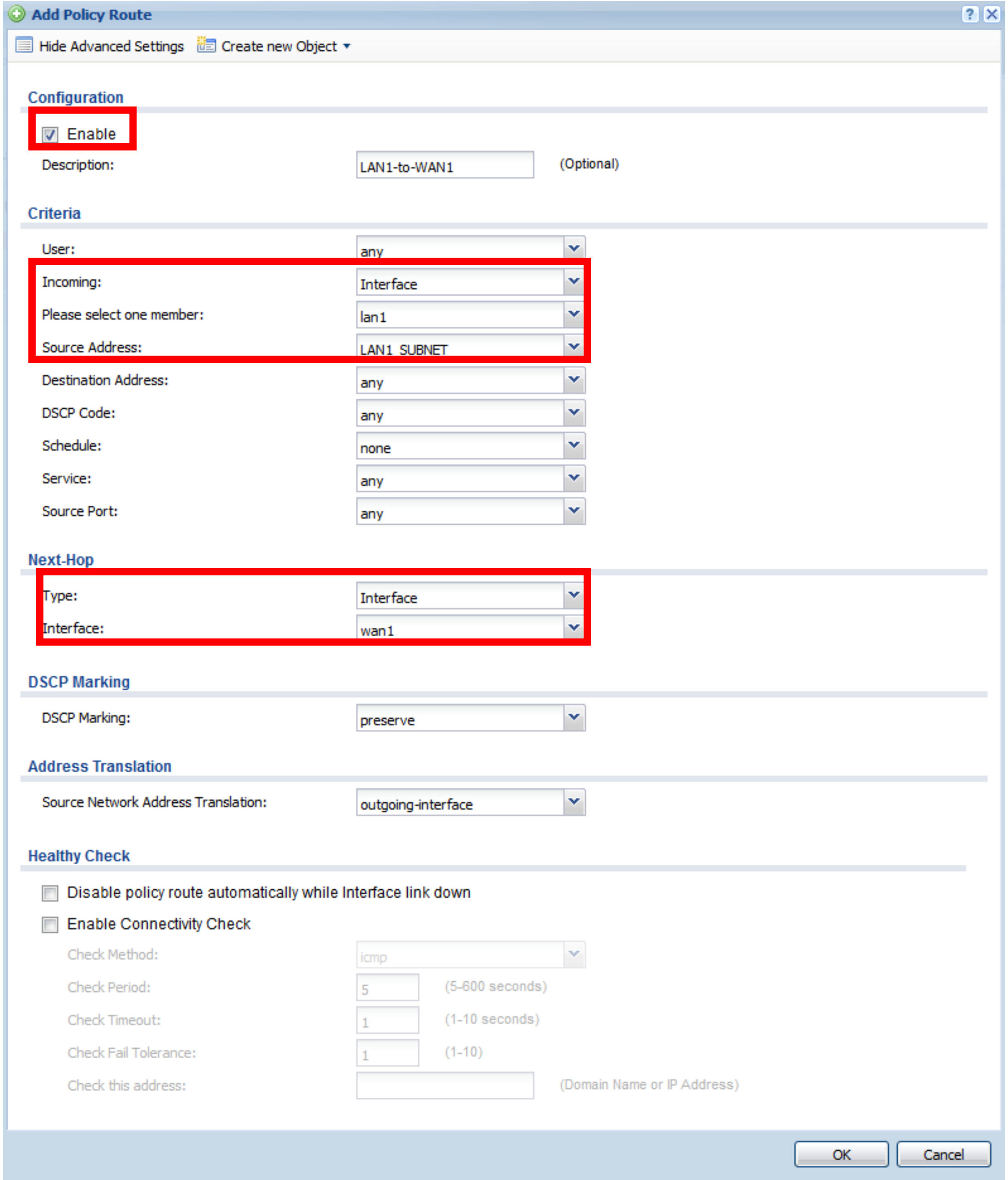
Routing Rules

Below are some examples policy routes for some of the most common scenarios.

Routing Internal Traffic Through Specific WAN

Depending on your implementation of the ZyXEL router, you may be using multiple internet connections and multiple internal networks (LAN1 and Guest for example). To optimize the internal networks (LAN1) performance you may want to force this traffic through the faster most reliable internet connection while guest use a slower internet connection. This can be achieved by creating two policy routes, one to send traffic out the fast internet connection and the second to send the guest traffic out the slower connection.

For this example WAN1 is the fast connection and WAN2 is the slower internet connection.



Configuration

☑ Enable

Description:	LAN1-to-WAN1	(Optional)

Criteria

User:	any
Incoming:	Interface
Please select one member:	lan1
Source Address:	LAN1_SUBNET
Destination Address:	any
DSCP Code:	any
Schedule:	none
Service:	any
Source Port:	any

Next-Hop

Type:	Interface
Interface:	wan1

DSCP Marking

DSCP Marking:	preserve

Address Translation

Source Network Address Translation:	outgoing-interface

Healthy Check

□ Disable policy route automatically while Interface link down

□ Enable Connectivity Check

Check Method:	icmp	
Check Period:	5	(5-600 seconds)
Check Timeout:	1	(1-10 seconds)
Check Fail Tolerance:	1	(1-10)
Check this address:		(Domain Name or IP Address)

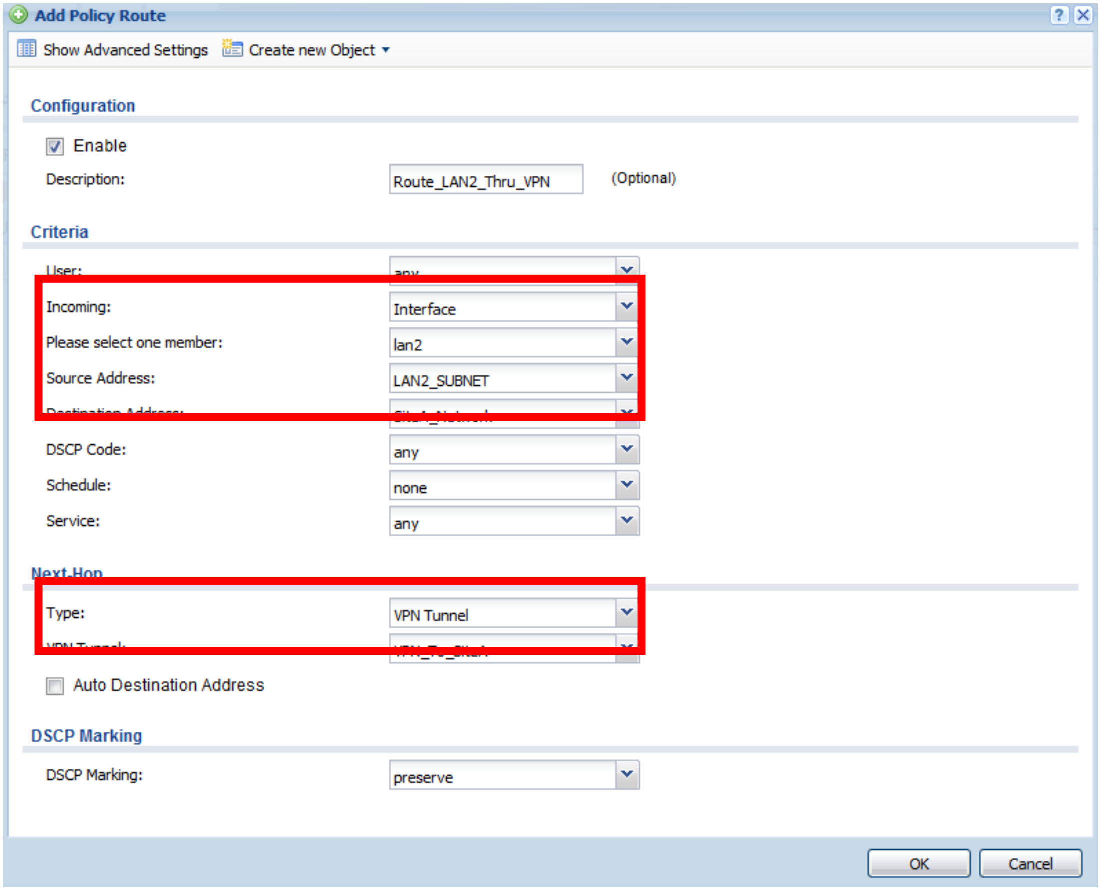
Note: Check the "Disable policy route automatically while Interface link down" to have the route disable automatically if WAN is down and use the live connection for backup.*

Create a second rule for the Guest network (whether it be LAN2, DMZ, a bridge interface or VLAN) using WAN2 for the Next-Hop.

Route Traffic Through VPN

The ZyXEL router unfortunately can only route one network subnet through the VPN or a range of consecutive IP addresses. If your network has a 192.168.1.0/24, a 172.16.0.0/24 and a 10.0.0.0/24 network subnets and need to route all three through a VPN, this would not be possible based on the VPN limitations of the ZyXEL security gateway. Creating a policy route to force traffic from the two other networks through the VPN tunnel would be a workaround.

The example below will route traffic from the LAN2 subnet destined for the remote subnet through the specified VPN tunnel.



Configuration

☑ Enable

Description: Route_LAN2_Thru_VPN (Optional)

Criteria

User: any

Incoming: Interface

Please select one member: lan2

Source Address: LAN2_SUBNET

Destination Address: SiteA_Network

DSCP Code: any

Schedule: none

Service: any

Next-Hop

Type: VPN Tunnel

VPN Tunnel: VPN_To_SiteA

☐ Auto Destination Address

DSCP Marking

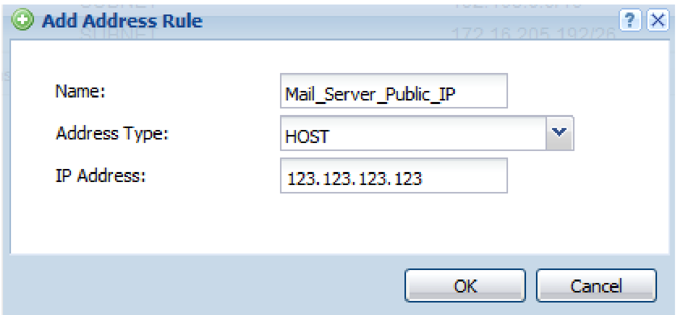
DSCP Marking: preserve

SNAT Routing

If you have multiple public IP addresses leased by the internet service provider and for instance you need the mail server to send out traffic using one of these addresses. You can create a policy route to send all traffic from the mail server out the WAN using a specific public IP on the leased block.

First an address object for the private mail server IP address and the public IP will need to be created under, **Configuration → Object → Address**.

Public IP



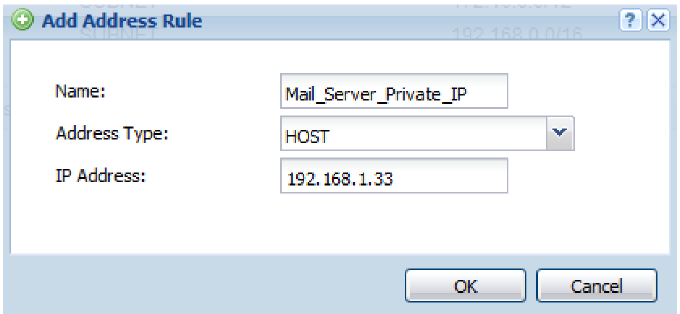
Add Address Rule

Name: Mail_Server_Public_IP

Address Type: HOST

IP Address: 123.123.123.123

Internal/Private IP



Add Address Rule

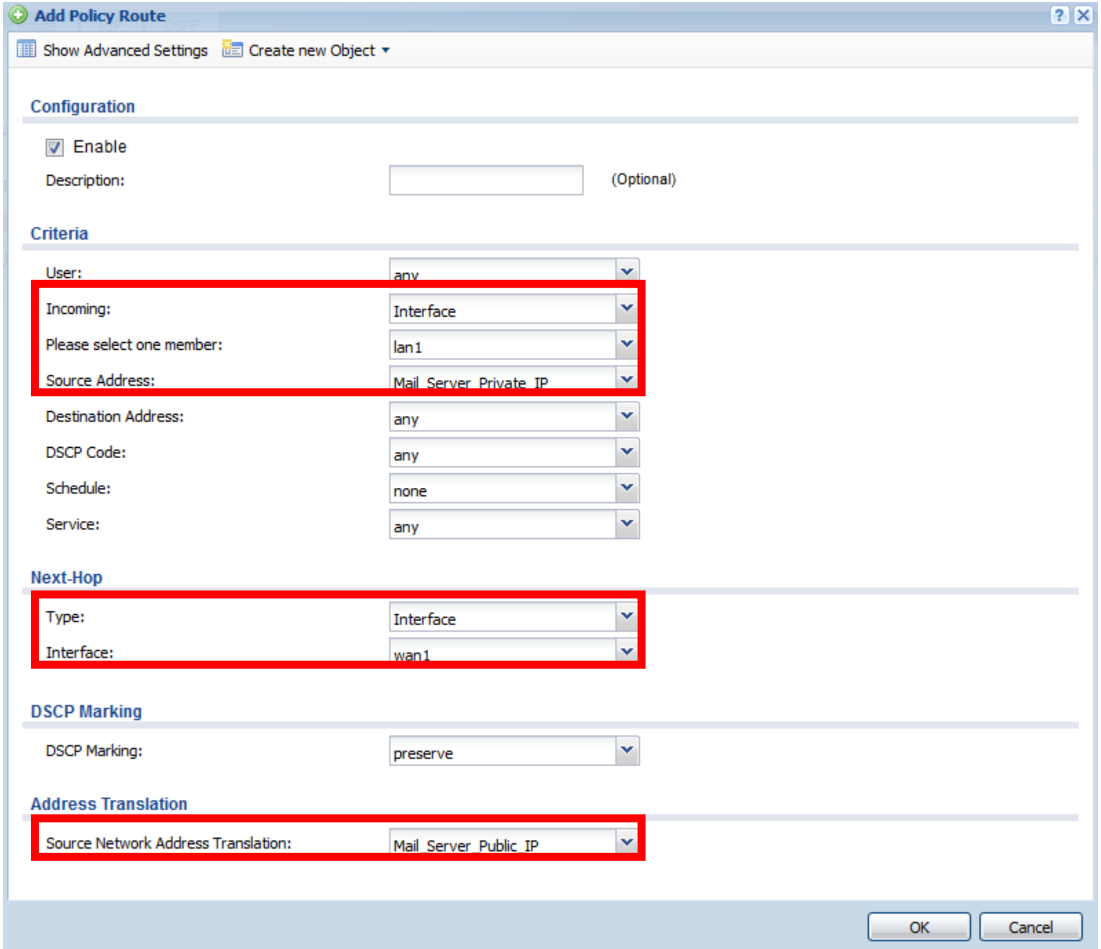
Name: Mail_Server_Private_IP

Address Type: HOST

IP Address: 192.168.1.33

To create the policy route to alter the public IP address the server will use to send traffic out to the internet go to, **Configuration → Network → Routing** and click the *Policy Route* tab.

- Select the incoming interface, this is the interface where the server is located.
- Source Address – Select the mail server private IP address object created previously.
- Next-Hop Type – Select Interface.
- Interface – Select the WAN connection the public IP belows to.
- Source Network Address Translation – Select the public IP address object created previously. This is the public IP address the mail server will use for outbound traffic.



Configuration

☑ Enable

Description: (Optional)

Criteria

User:	any
Incoming:	Interface
Please select one member:	lan1
Source Address:	Mail_Server_Private_IP
Destination Address:	any
DSCP Code:	any
Schedule:	none
Service:	any

Next-Hop

Type:	Interface
Interface:	wan1

DSCP Marking

DSCP Marking:	preserve

Address Translation

Source Network Address Translation:	Mail_Server_Public_IP