How To Guide:

Site-to-Site VPN Bonding

Introduction

This article outlines general procedures for configuring site-to-site VPN bonding and failover based on the diagram example of site-to-site VPN network in the following page.

Diagram Example

Branch:

Port 1:
WAN 1: example_1
IP: 203.67.222.40, Subnet: 203.67.222.40/30, GW:203.67.222.1

Port 2:
WAN 2: example_2
IP: 100.100.100.6, Subnet:100.100.100.0/29, GW:100.100.100.1

Port 4:
Branch LAN: 10.168.1.0/24, Interface: 10.168.1.254

HQ:

Port 1:
WAN 1: hq_1
IP: 103.67.222.47, Subnet: 103.67.222.40/29, GW:103.67.222.41

Port 2:
WAN 2: hq_2
IP: 118.169.192.20, Subnet: 118.169.192.20/30, GW:118.169.192.21

Port 4:
HQ LAN: 20.20.20.0/24, Interface: 20.20.20.254

Requirement

In this case, the solution is requested to:

1. Ensure site-to-site VPN connectivity when/if any one of WAN links fails.

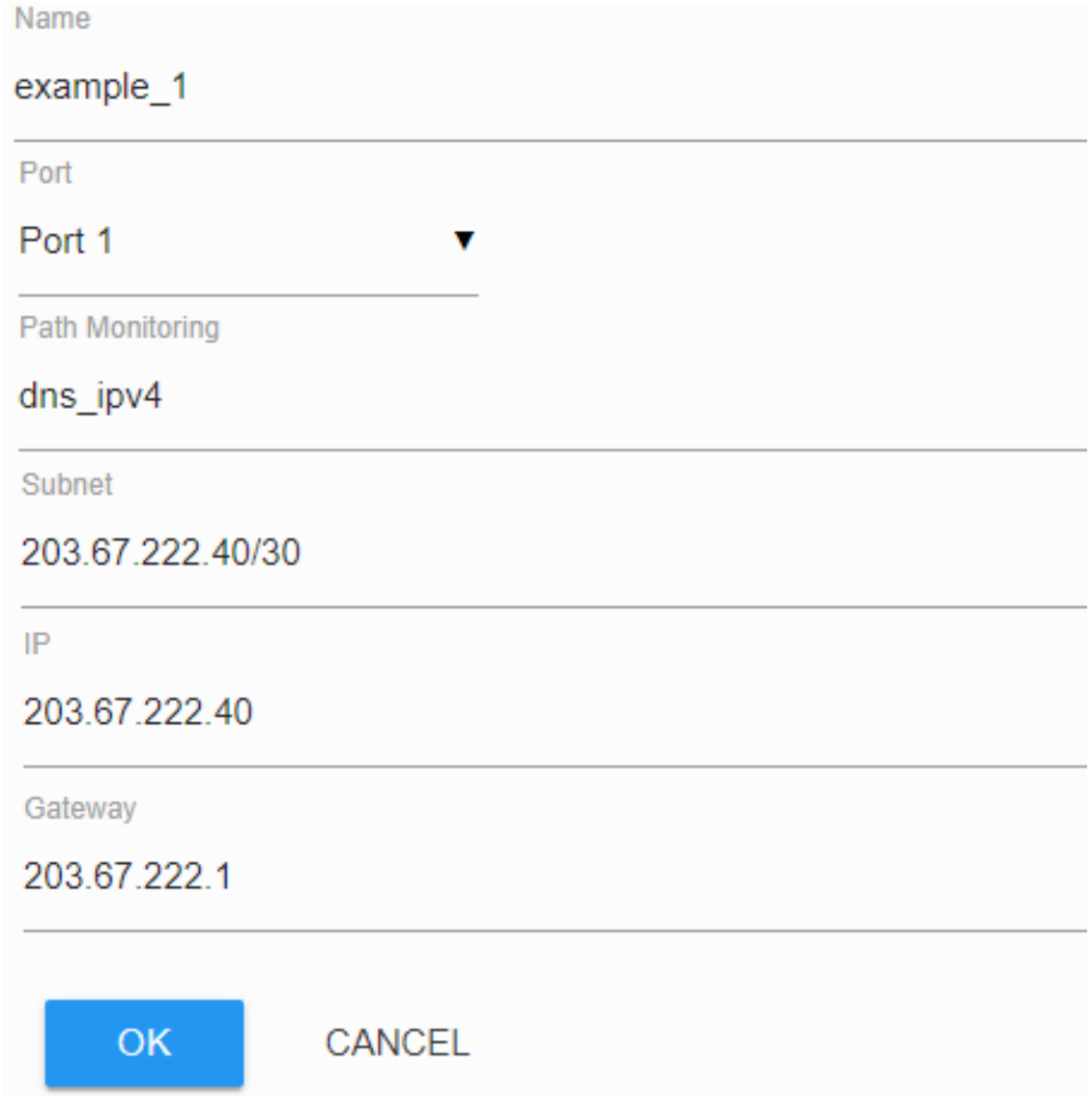
2. Highly utilize site-to-site network bandwidth by distributing VPN traffic across all available paths at both ends.

Configuring Site-to-Site VPN Bonding

Follow the steps below to configure site-to-site VPN bonding on the branch appliance with the IP details given:

1. *WAN > ADD*
2. *LAN > ADD*
3. *System > Keys > XBond (make sure the XBond keys match.)*
4. *Object > XBond > ADD*
5. *Policy Routing > ADD*

WAN > ADD > Static



WAN > ADD > Static

Name

example_2

Port

Port 2 ▼

Path Monitoring

dns_ipv4 ▼

Subnet

100.100.100.0/29

IP

100.100.100.6

Gateway

100.100.100.1

OK CANCEL

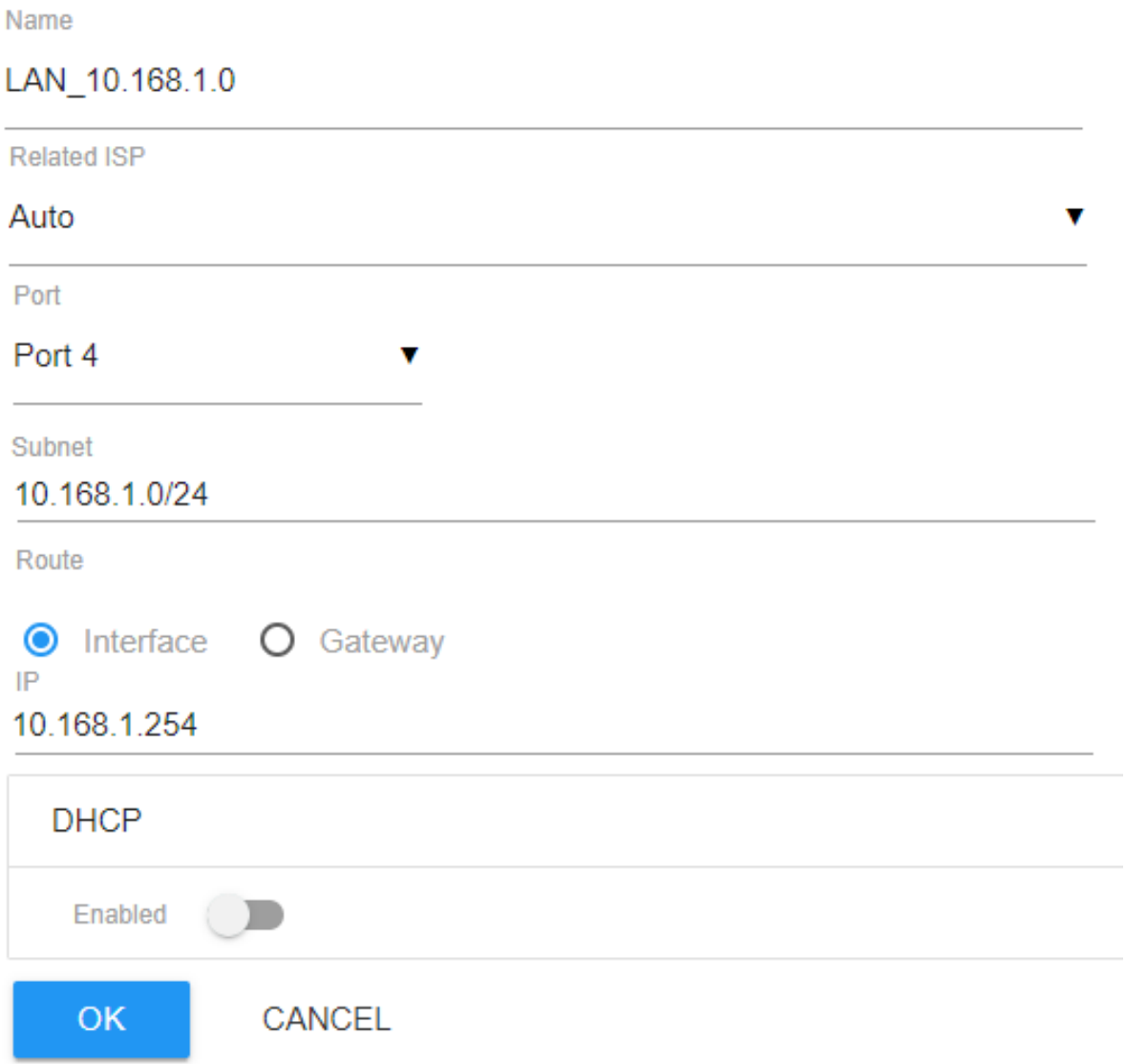
WAN configuration is done as follows:

WAN

ADD DELETE

Status	Type	Name	Port	Interface	Subnet	IP	Gateway
✓	Static	example_1	Port 1	eth0_6	203.67.222.40/30	203.67.222.40	203.67.222.1
✓	Static	example_2	Port 2	eth1_2	100.100.100.0/29	100.100.100.6	100.100.100.1

LAN > ADD

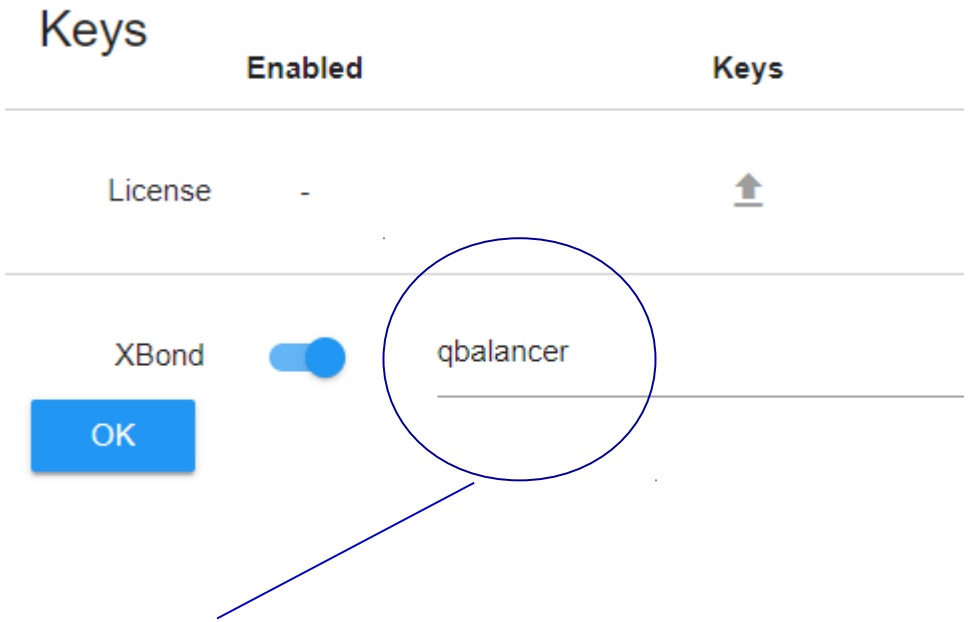

Name
LAN_10.168.1.0
Related ISP
Auto
Port
Port 4
Subnet
10.168.1.0/24
Route
Interface
Gateway
IP
10.168.1.254
DHCP
Enabled
OK
CANCEL

LAN

LAN configuration is done as follows:

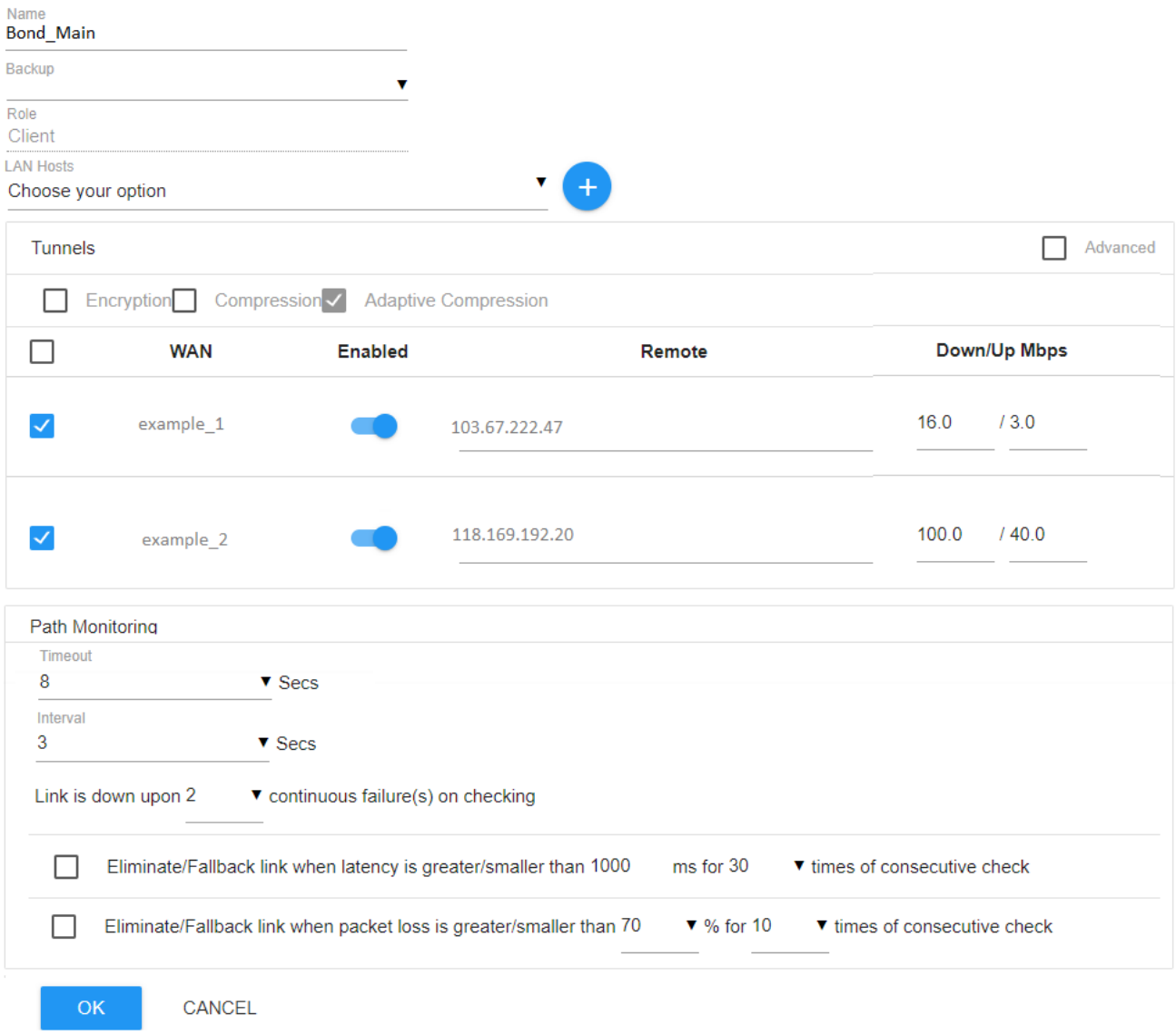
System > Keys > XBond

For ***XBond***, there are ***client*** and ***server***. The ***XBond client*** will automatically connect the ***XBond server*** to create XBond bonding tunnels, and the keys on both ends have to be symmetrically set.



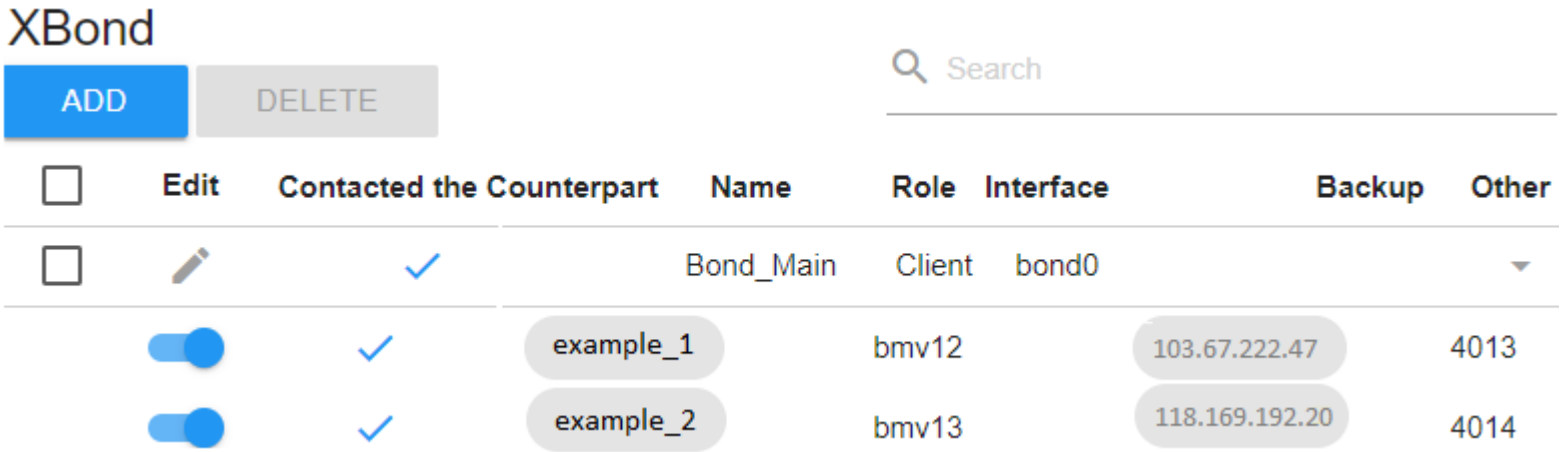
The is the user-defined key for ***XBond***.

Objects > XBond > ADD

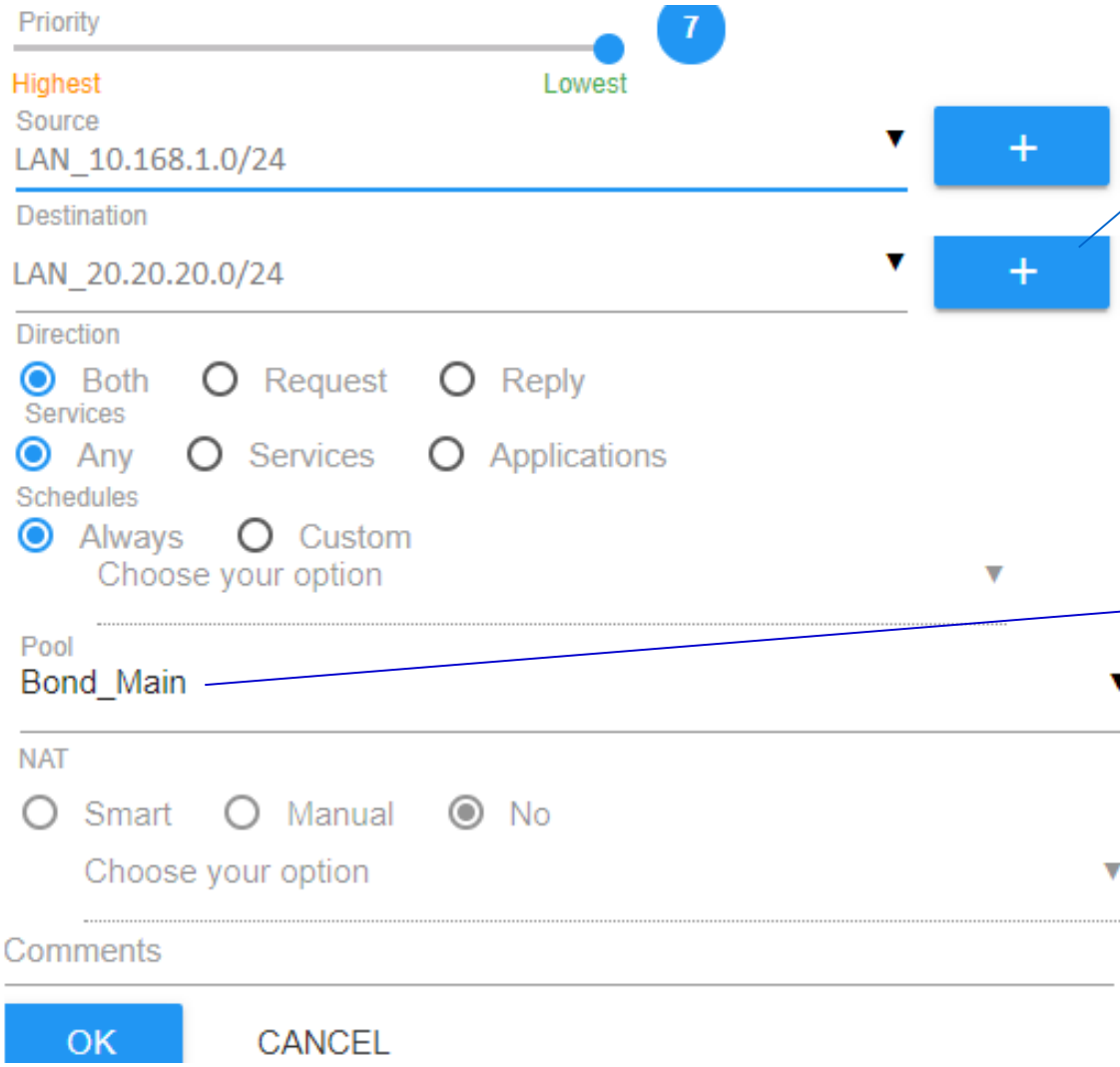


Objects > XBond

Configuration for XBond on the ***Branch*** appliance is done as follows:



Policy Routing > ADD

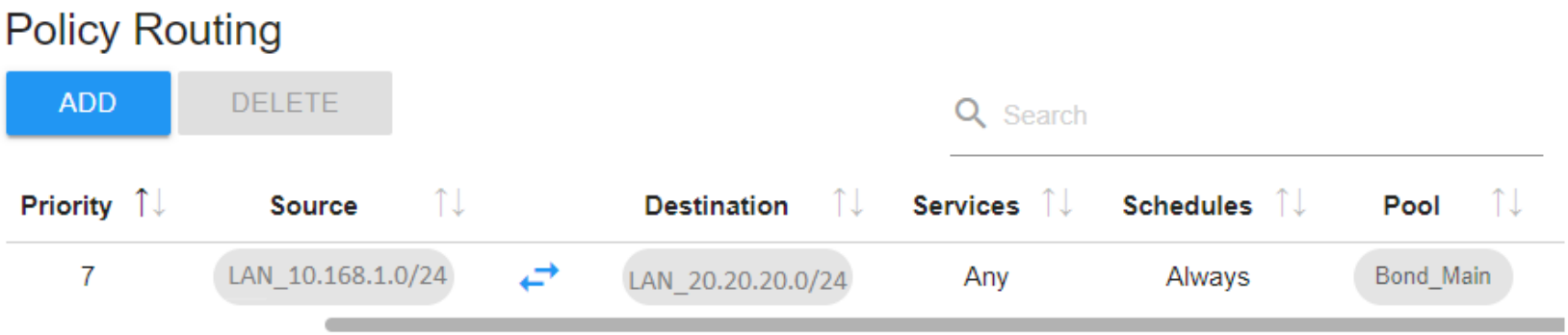


Add HQ subnet here for site-to-site policy routing.

Choose the XBond newly created.

Policy Routing

Policy Routing for VPN bonding on the Branch appliance is done as follows:



Follow the steps below to configure site-to-site VPN bonding on the HQ appliance:

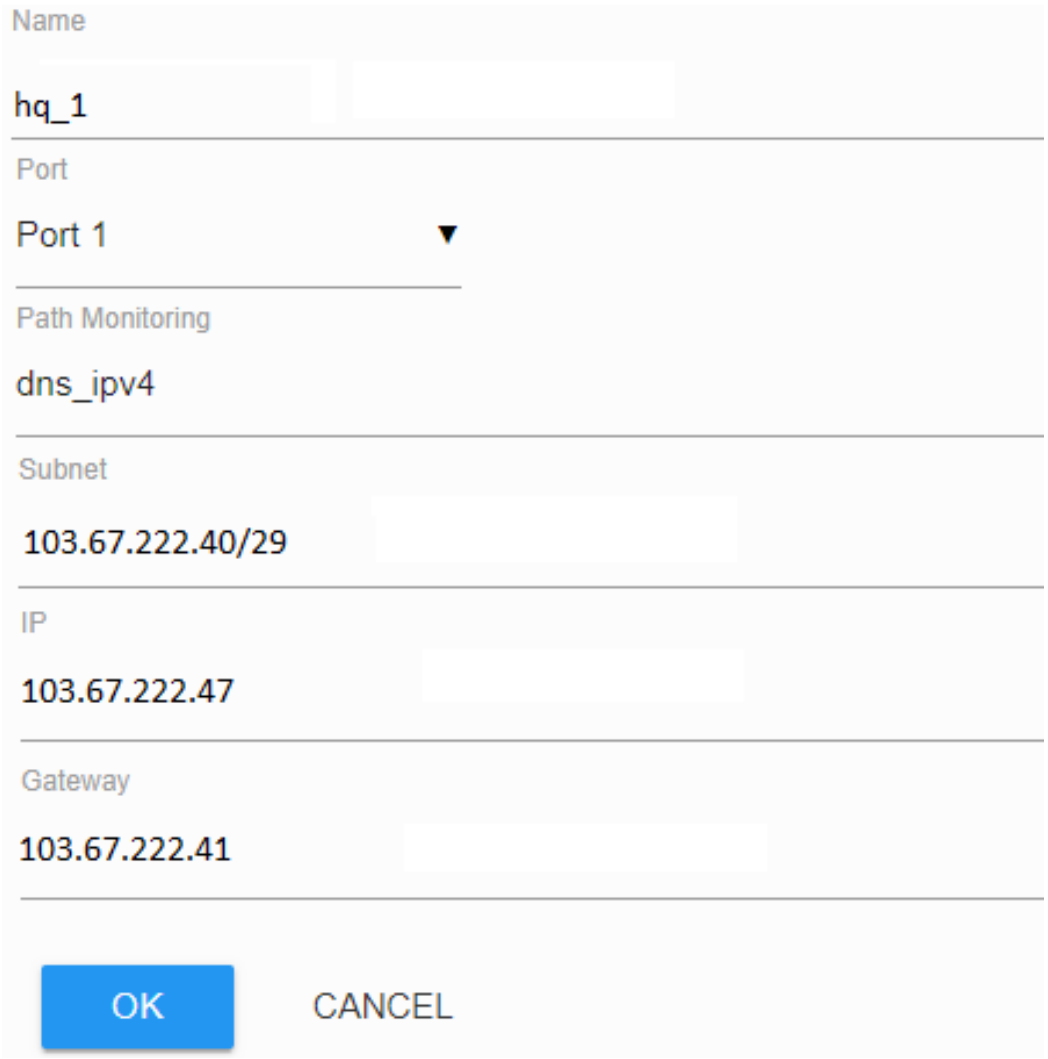
1. WAN > ADD > Static

2. LAN > ADD

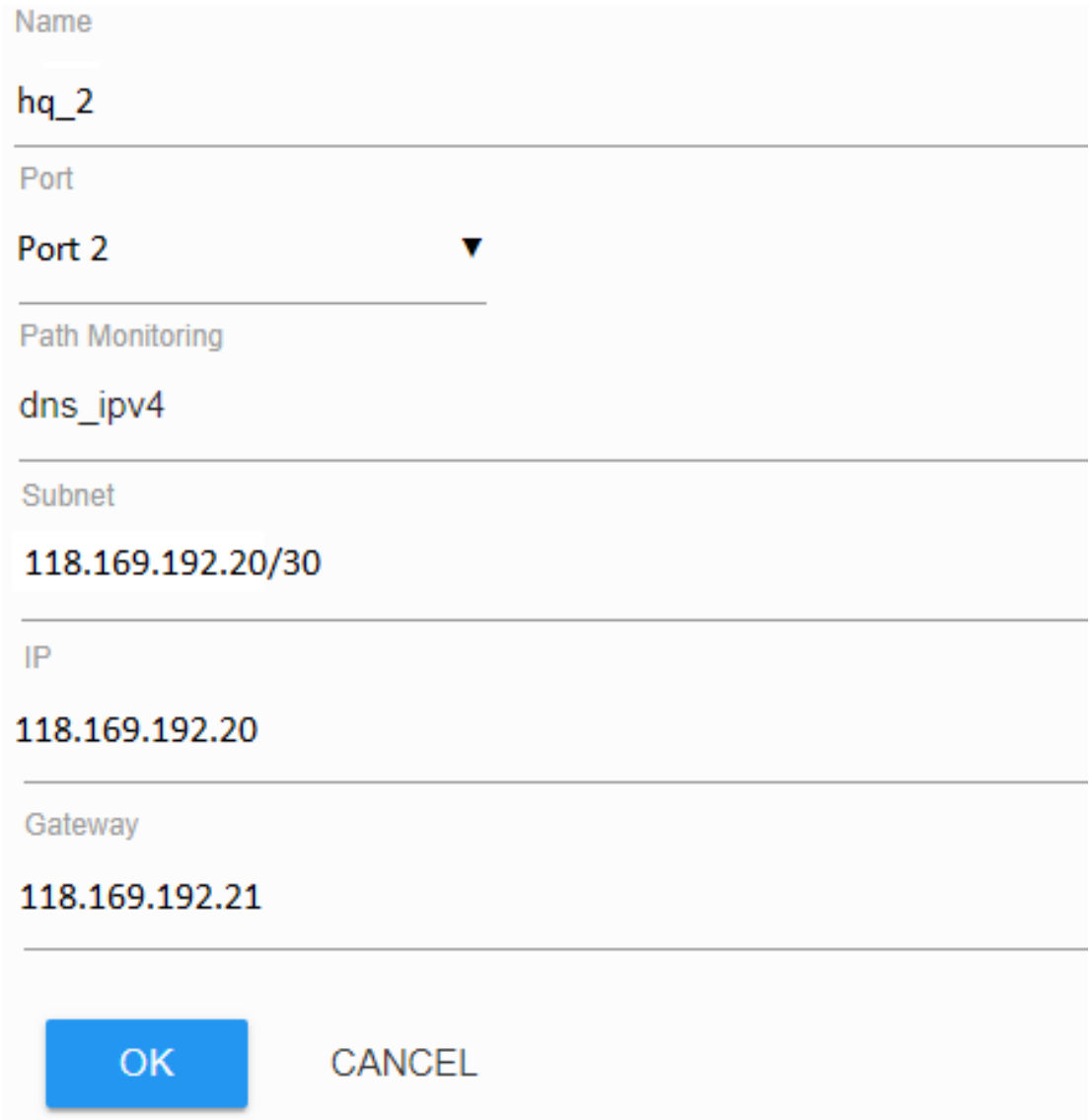
3. Object > XBond (Generated automatically)

4. Policy Routing > ADD

WAN > ADD > Static



WAN > ADD > Static



WAN

WAN configuration is done as follows:

Status	Type	Name	Port	Interface	Subnet	IP	Gateway
✓	Static	hq_1	Port 1	eth0_9	103.67.222.40/29	103.67.222.47	103.67.222.41
✓	Static	hq_2	Port 2	eth1_10	118.169.192.20/30	118.169.192.20	118.169.192.21

LAN > ADD

Name

LAN_20.20.20.0/24

Related ISP

Auto

Port

Port 4

Subnet

20.20.20.0/24

Route

Interface Gateway

IP

20.20.20.254

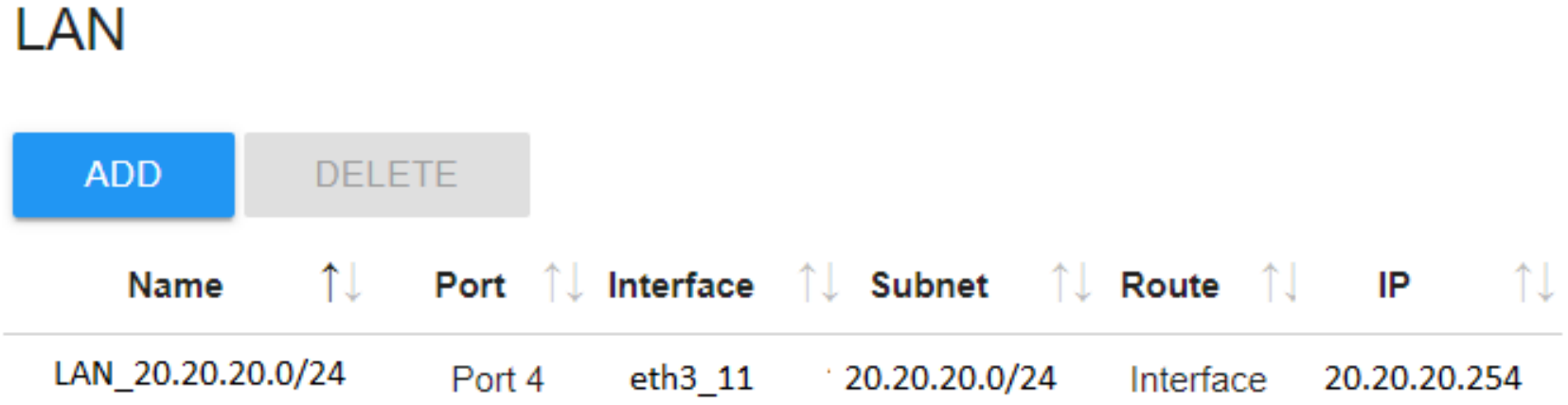
DHCP

Enabled

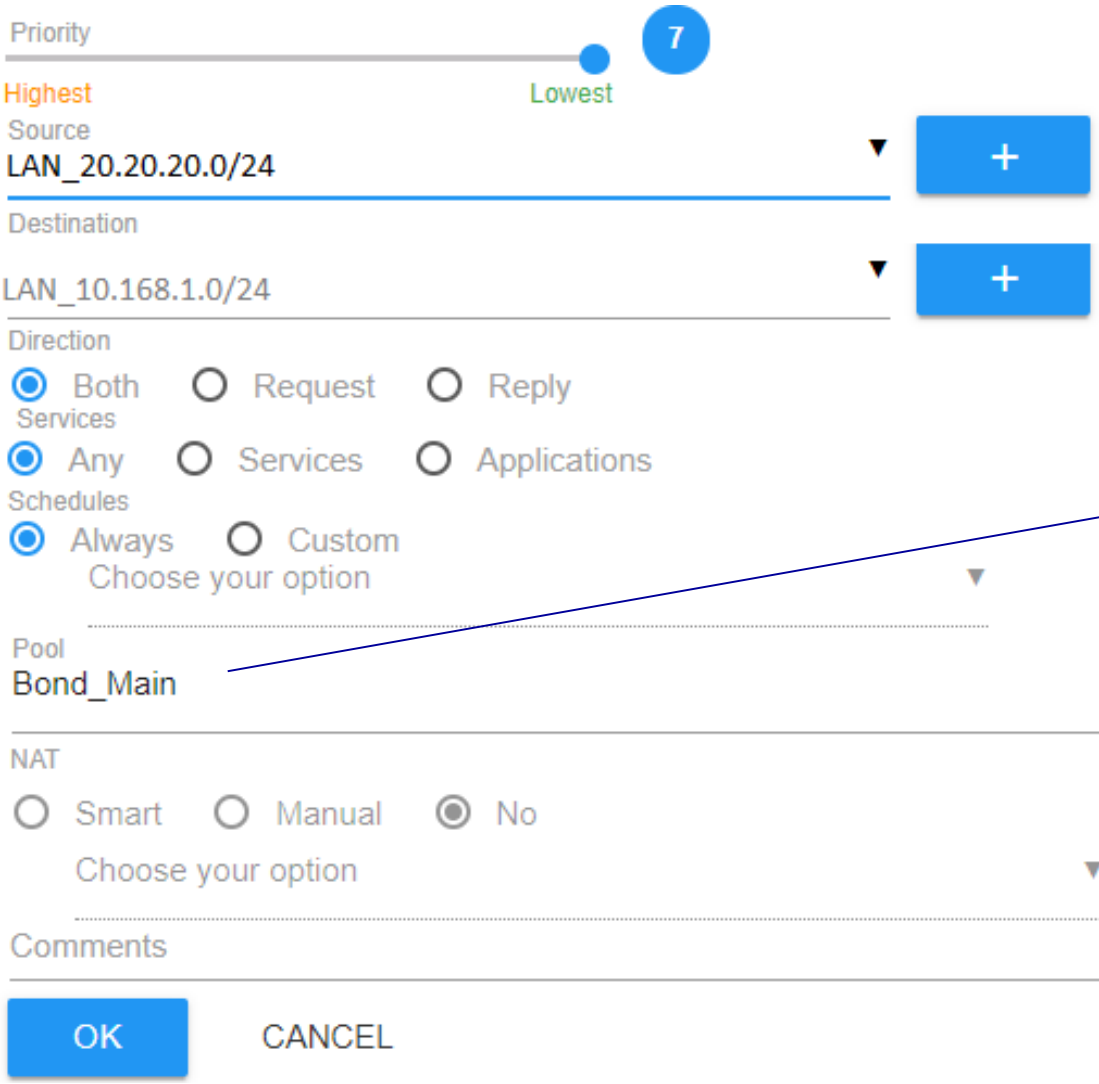
OK CANCEL

LAN

LAN configuration is done as follows:



Policy Routing > ADD

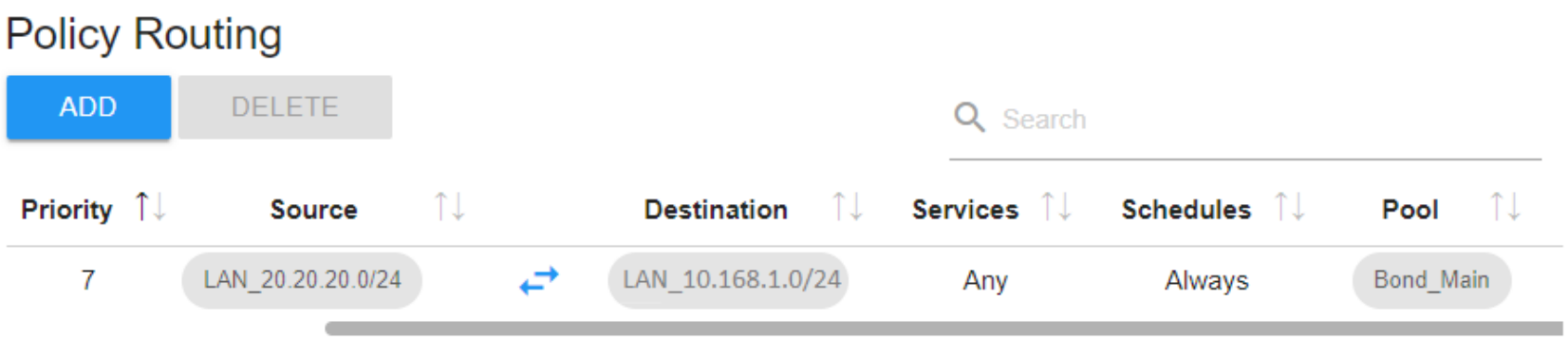


Add Branch subnet here for site-to-site policy routing.

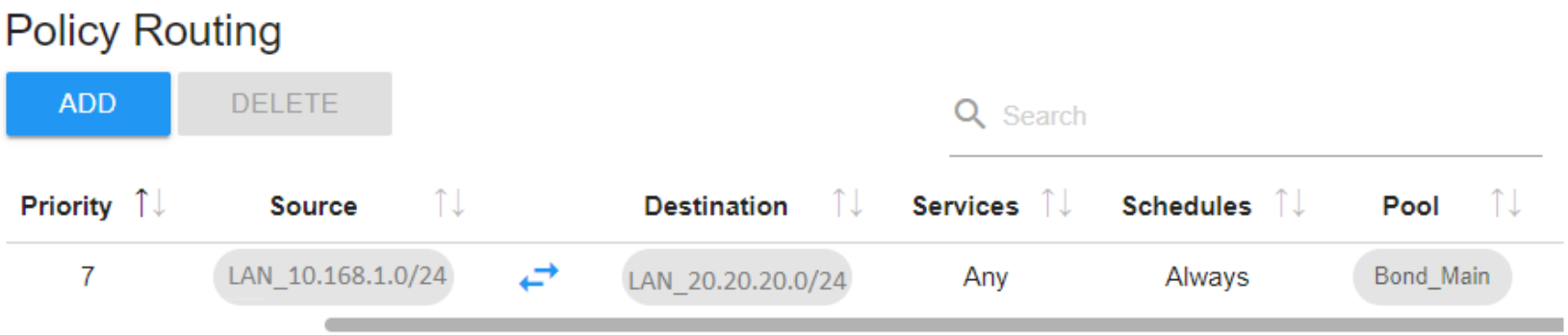
Select the XBond, which is automatically generated.

Policy Routing

Policy Routing for site-to-site VPN bonding on the ***HQ*** appliance is done as follows:



For your reference, the following is the policy route on the ***Branch*** appliance:



Done!

Check if the firewalls on both ends are able to ping one another now.