Q-Balancer®

How To Guide:

Site-to-Site VPN Load Balancing with TMV Tunnels

Introduction

VPN load balancing enables site-to-site traffic to be distributed based on IP or session across multiple VPN tunnels.

This article outlines the configuration of TMV tunnel, which is terminated on the appliances at both ends, and their relevant routing policy.

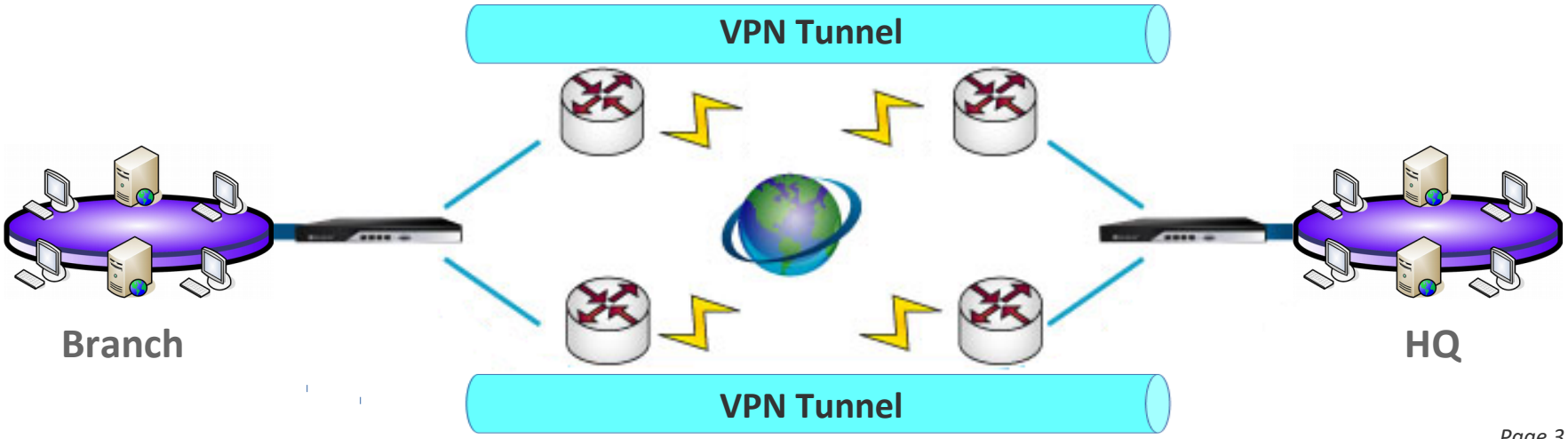
Diagram Example

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 configuration is required to:

> Failover site-to-site access to the remaining active path in case one of WAN links failed.

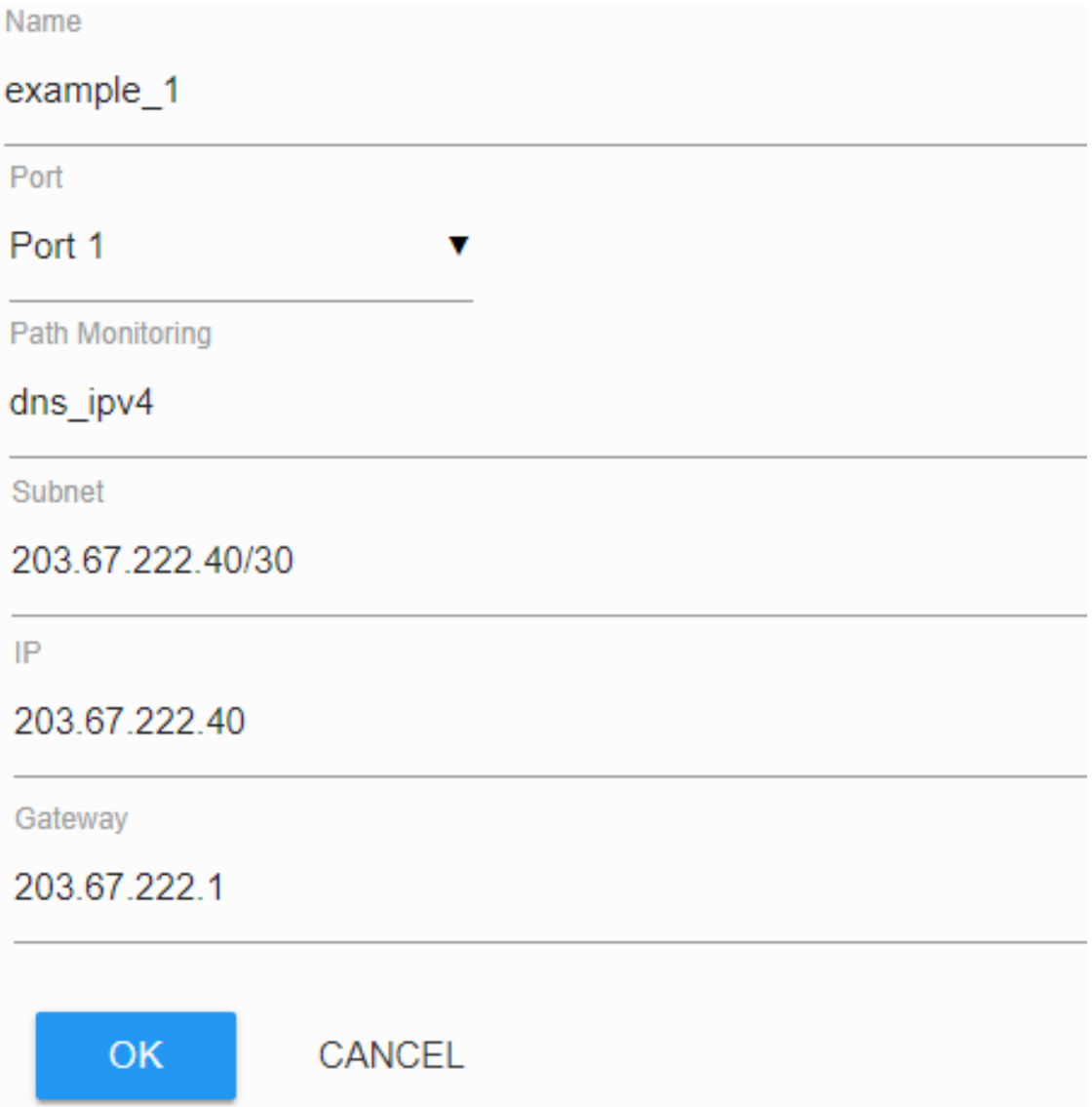
> Load Balance site-to-site traffic across all available tunnels.

Configuring VPN Load Balancing on the Branch Office Appliance

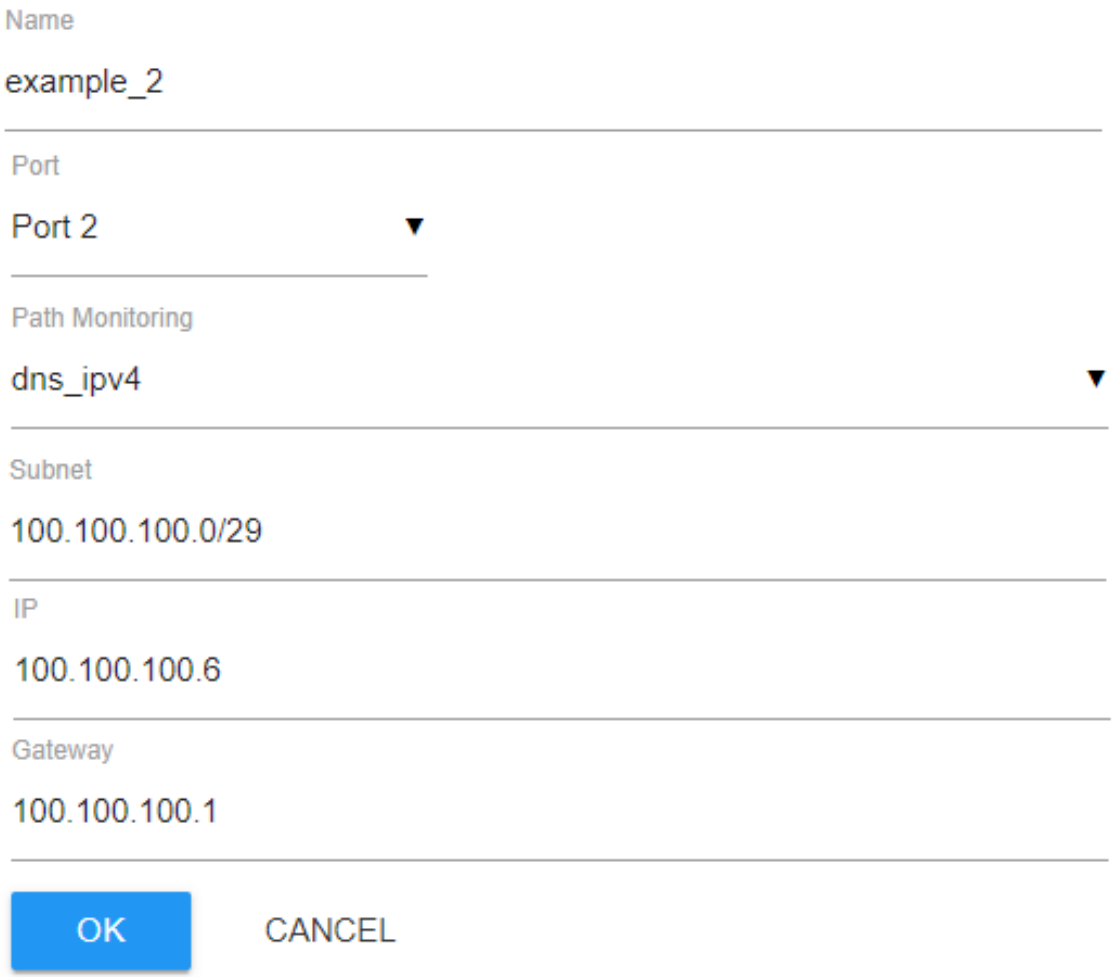
Follow the steps below to configure site-to-site VPN load balancing on the branch appliance with the IP details given:

1. *WAN > ADD*
2. *LAN > ADD*
3. *Tunnels > ADD*
4. *Object > DPS > ADD*
5. *Policy Routing > ADD*

WAN > ADD > Static



WAN > ADD > Static



WAN

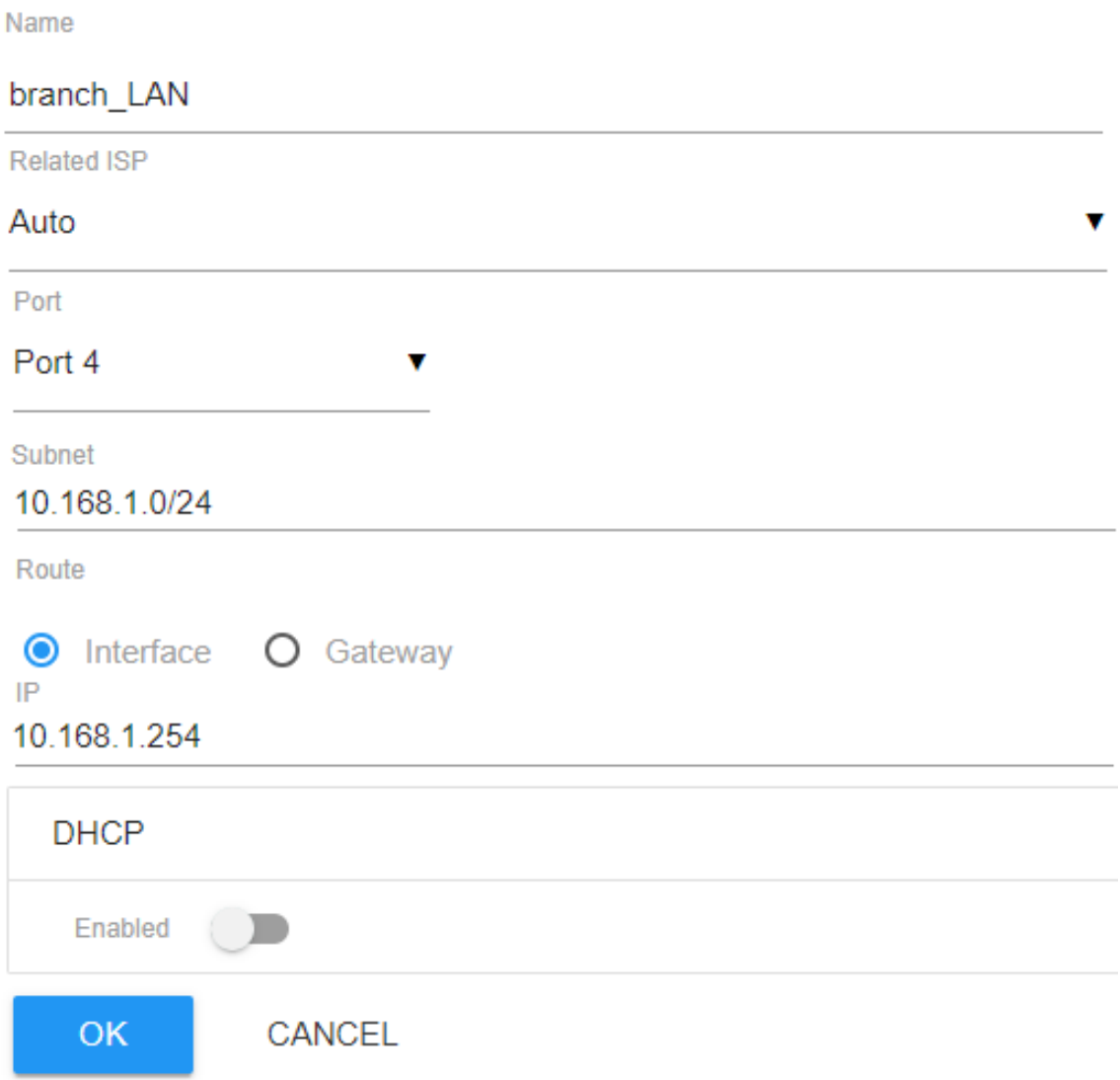
WAN configuration on the branch office appliance is done as follows:

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

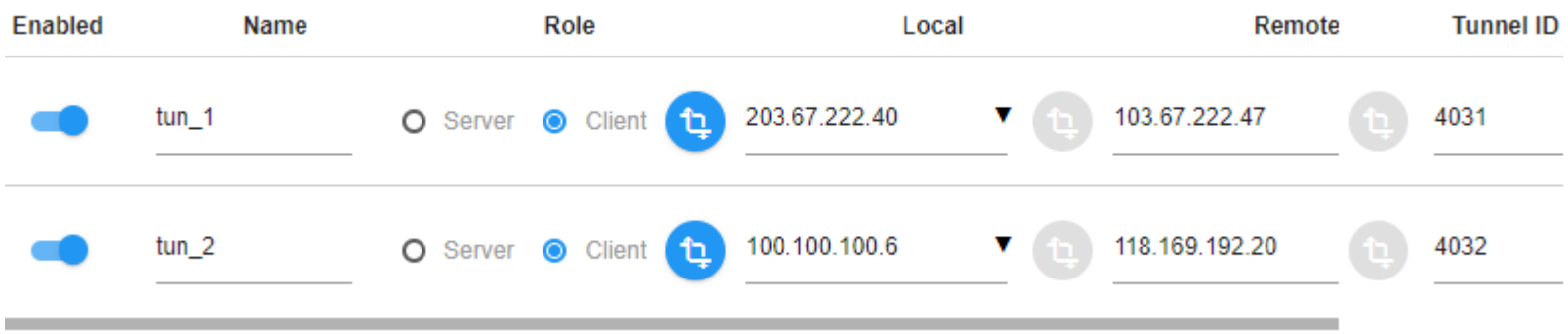

Name
branch_LAN
Related ISP
Auto
Port
Port 4
Subnet
10.168.1.0/24
Route
Interface
Gateway
IP
10.168.1.254
DHCP
Enabled
OK
CANCEL

LAN

LAN configuration on the branch office appliance is done as follows:

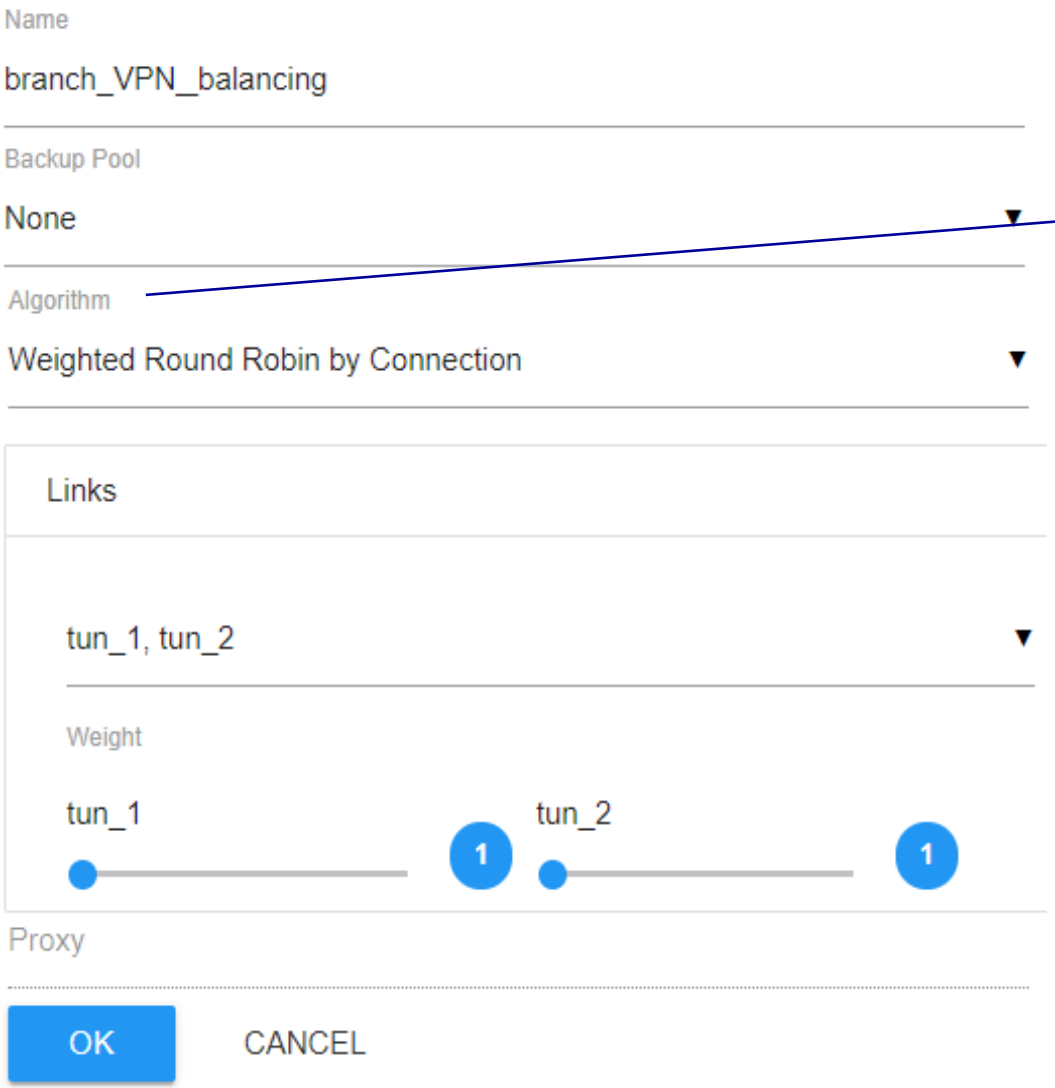
Tunnels > ADD

For ***TMV Tunnels***, there are 2 ***Roles***, ***client*** and ***server***. The ***TMV Client*** will automatically connect the ***TMV server*** to create tunnels, and the ***Tunnel ID*** on both ends have to be the same. Adding ***TMV*** on the branch appliance is done as follows:



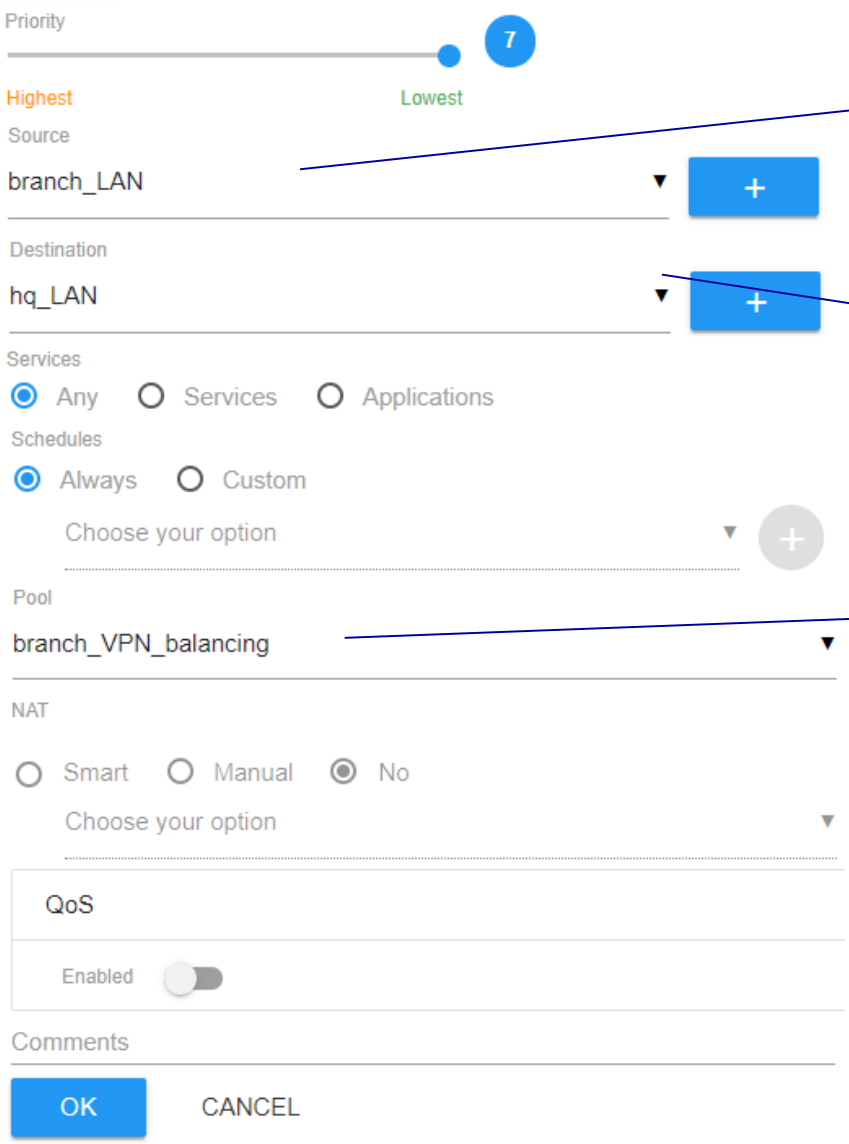
Objects > DPS > ADD

Adding a ***DPS*** object for ***TMV*** tunnels on the branch appliance:



Note: All algorithms are applicable for VPN load balancing.

Policy Routing > ADD



Set branch subnet here for site-to-site policy routing.

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

Choose the DPS newly created for TMV.

Policy Routing

Policy Routing for VPN load balancing on the branch appliance is done as follows:

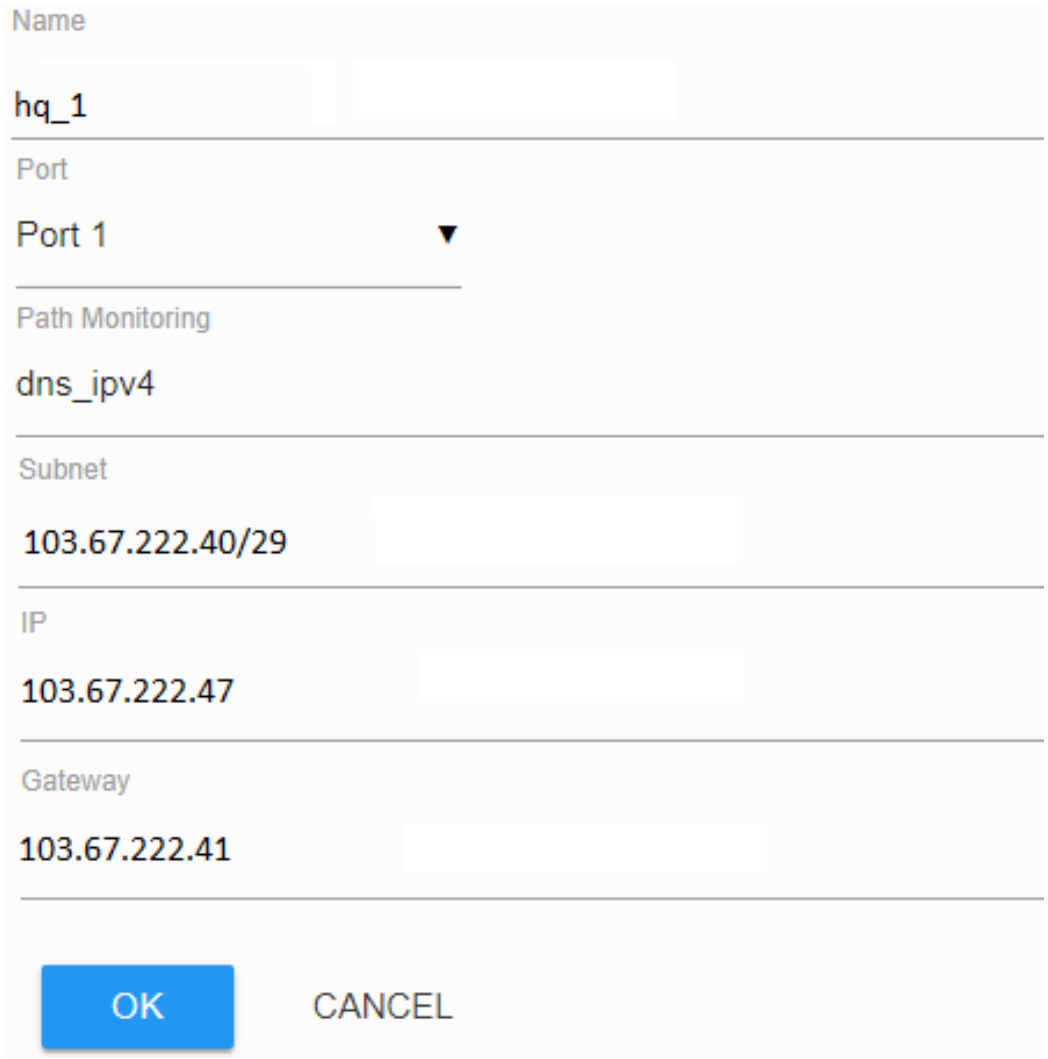
branch_LAN	⇄	hq_LAN	Any	Always	branch_VPN_balancing	No	-

Configuring VPN Load Balancing on the HQ Office Appliance

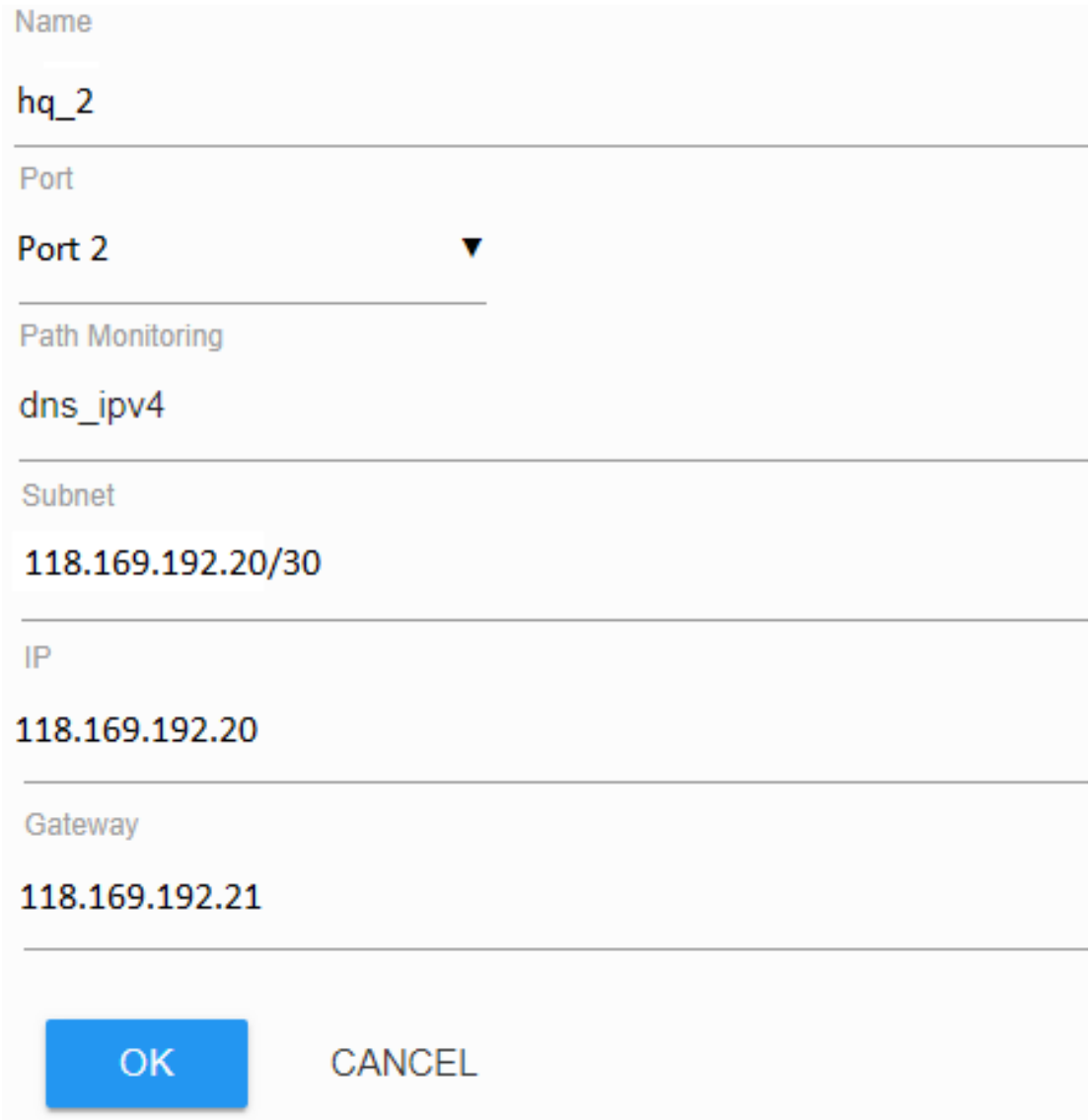
Follow the steps below to configure site-to-site VPN load balancing on the HQ office appliance with the IP details given:

1. *WAN > ADD*
2. *LAN > ADD*
3. *Tunnels > ADD*
4. *Object > DPS > ADD*
5. *Policy Routing > ADD*

WAN > ADD > Static

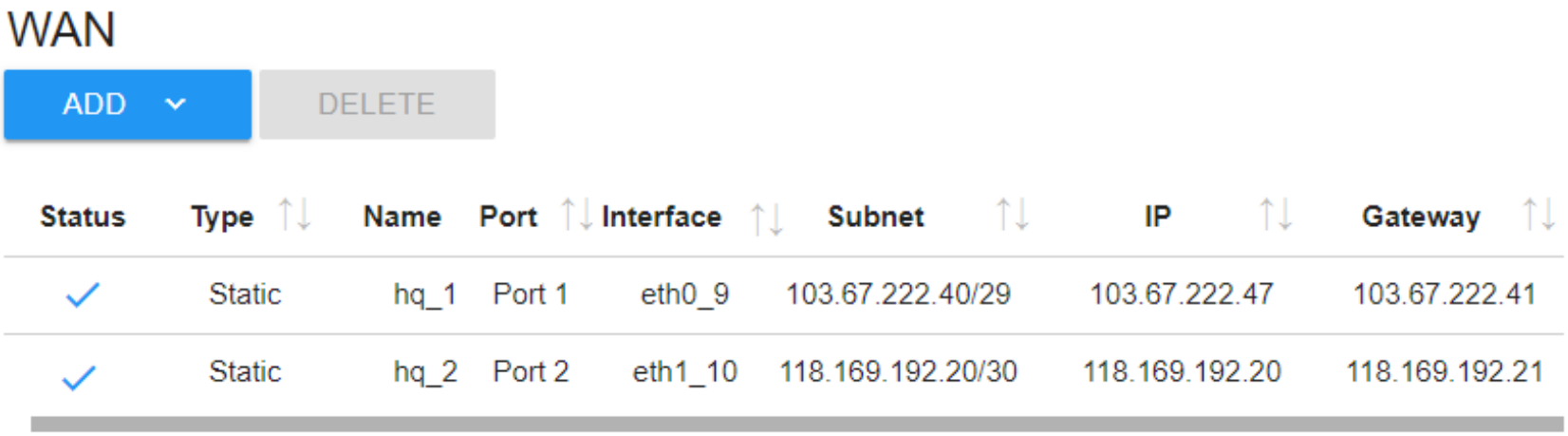


WAN > ADD > Static

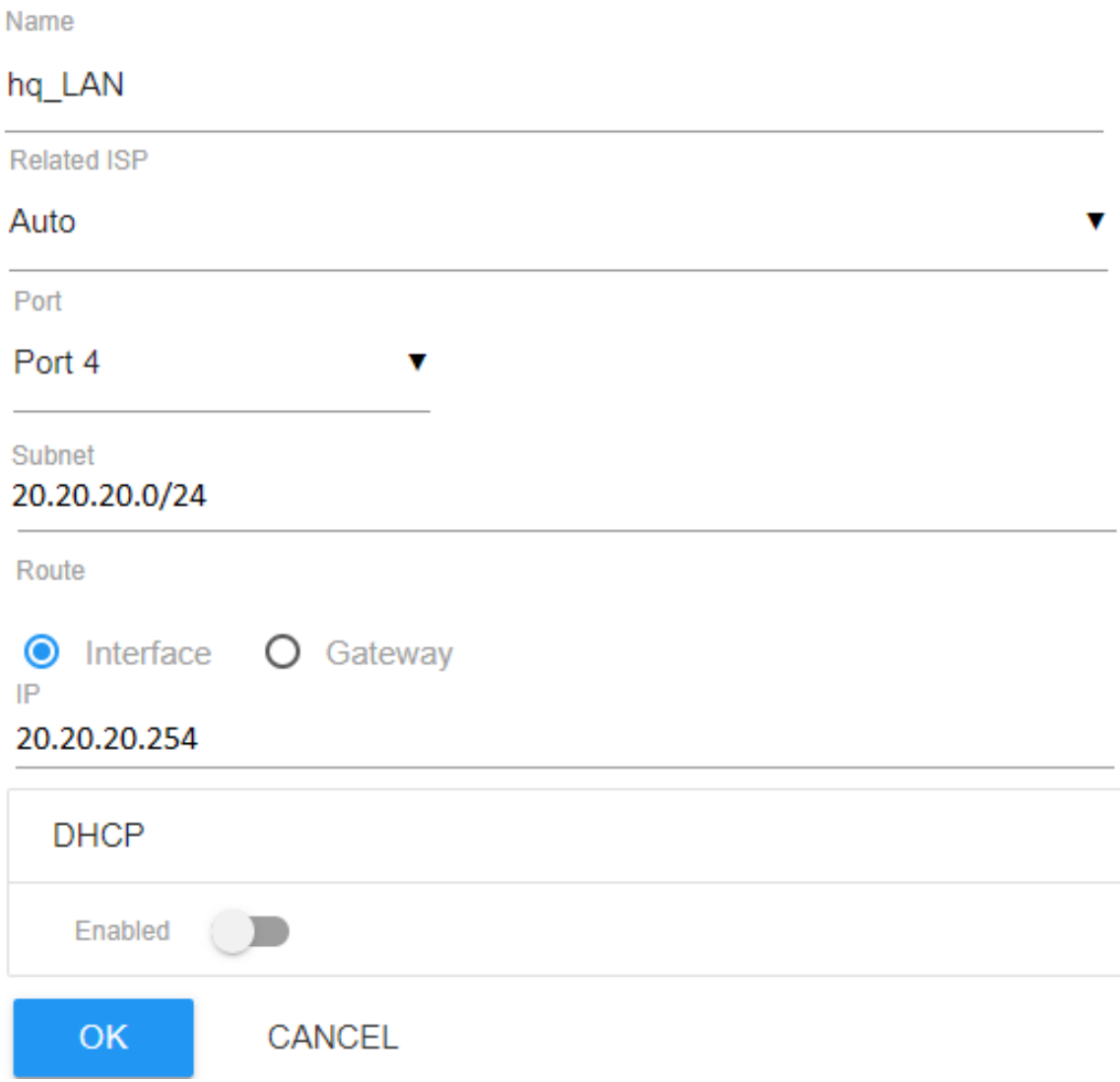


WAN

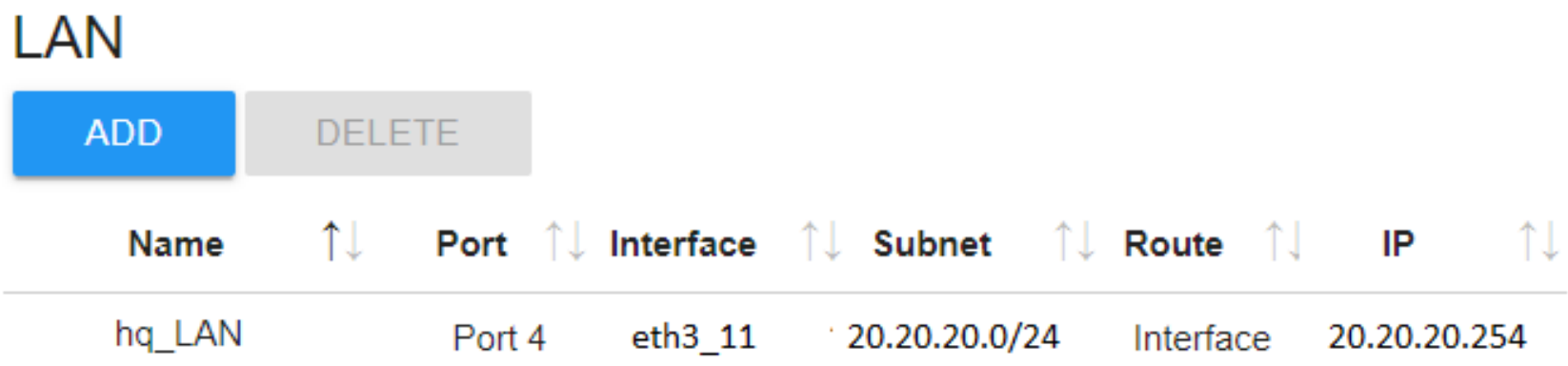
WAN configuration on the HQ office appliance is done as follows:



LAN > ADD

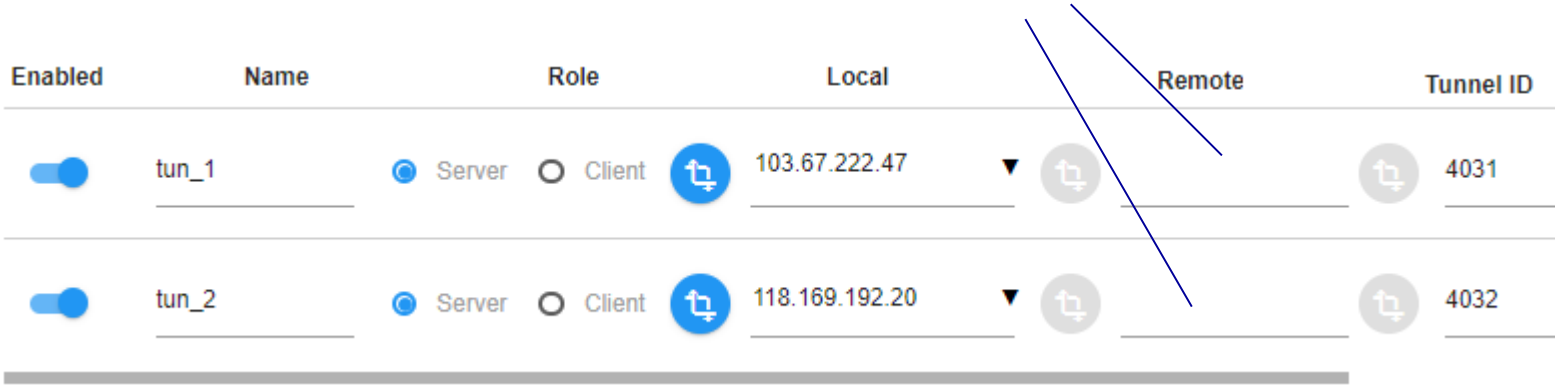

Name
hq_LAN
Related ISP
Auto
Port
Port 4
Subnet
20.20.20.0/24
Route
Interface
Gateway
IP
20.20.20.254
DHCP
Enabled
OK
CANCEL

LAN configuration on the HQ office appliance is done as follows:



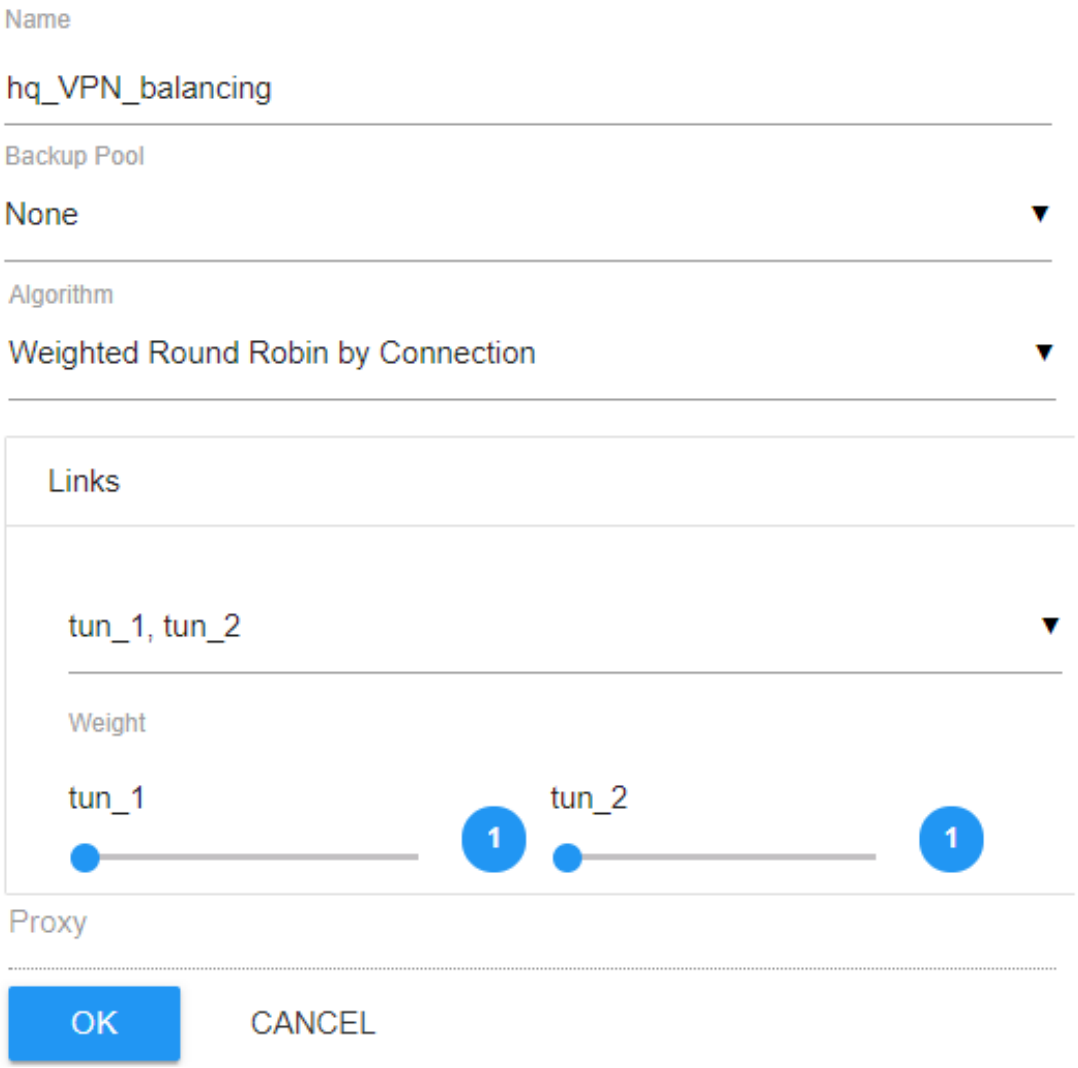
Tunnels > ADD

leave the fields blank.

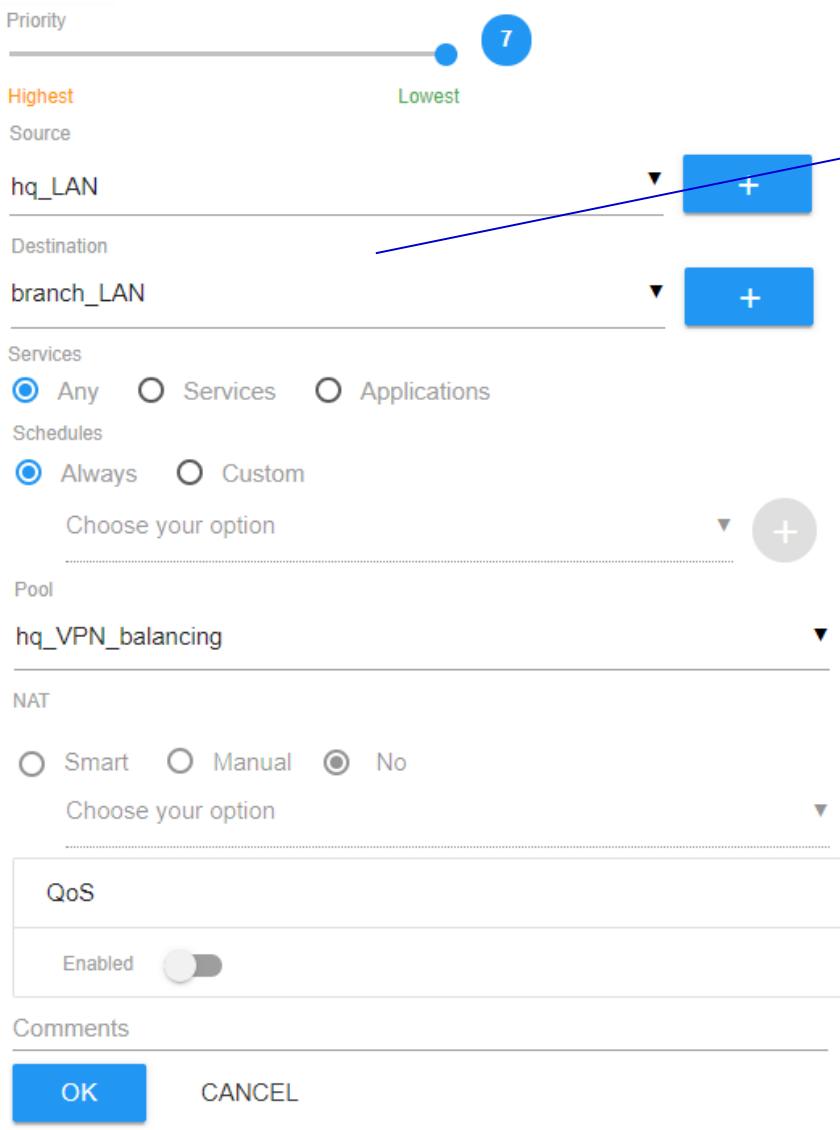


Objects > DPS > ADD

Adding a ***DPS*** object for ***TMV*** tunnels on the HQ appliance:



Policy Routing > ADD



Set branch subnet here for policy routing.

Policy Routing

Policy Routing for site-to-site VPN load balancing on the HQ office appliance is done as follows:

hq_LAN	⇄	branch_LAN	Any	Always	hq_VPN_balancing	No

Done!

Check if it works. For example, on the LAN hosts at branch office run the command PING to the hosts at HQ office.