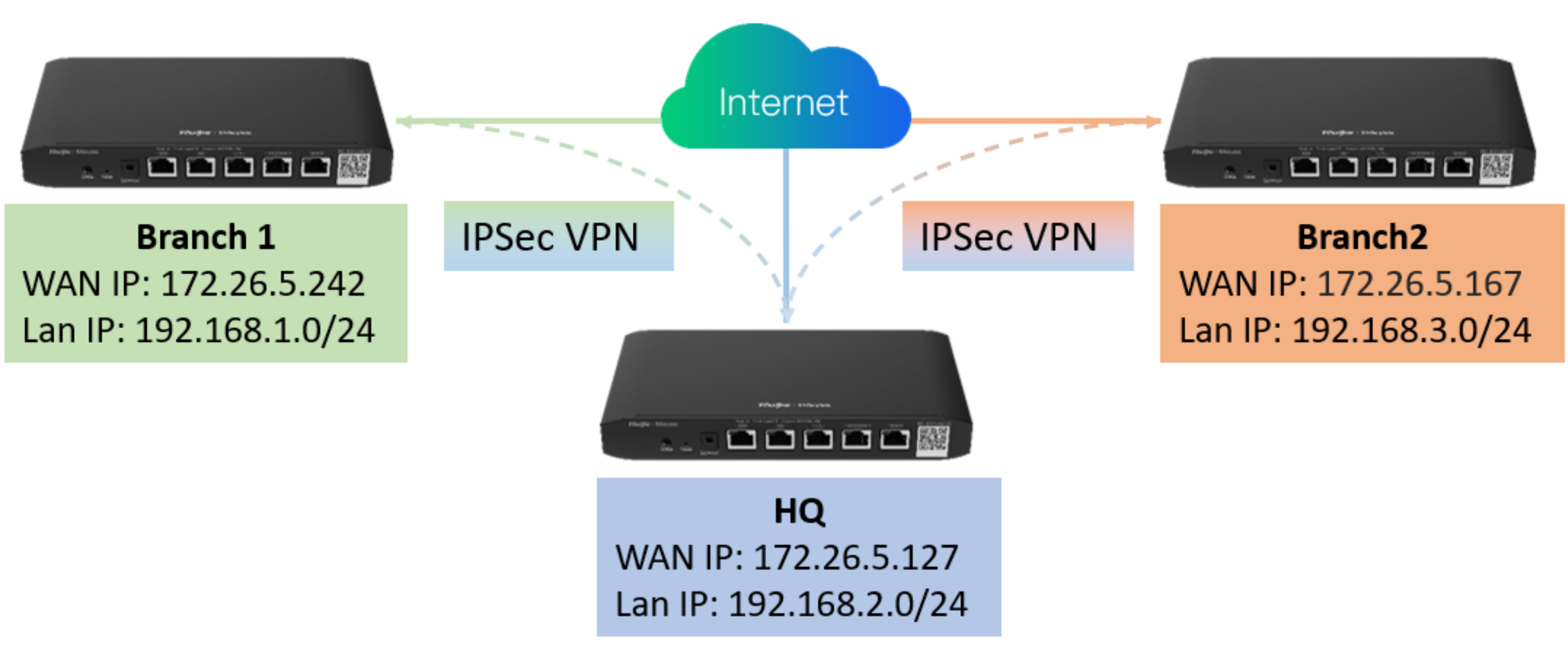
How to realize the inter-communication among the branches by establishing the IPsec VPN on Reyee EG?

I. Applicable Scenario

IPSec VPNs are established between the three Reyee EGs so that the two branches can access resources at the headquarters and communicate with each other.

II. Topology



III. Key Points

1. The Intranet segments between the HQ and two branches can be summarized into a larger network segments. For example, 192.168.1.0−3.0/24 can be grouped into 192.168.0.0/22 (192.168.0.1−192.168.3.254).
2. When configuring IPSec VPN on HQ and Branch devices, the configuration related to the HQ segment should be the summarized network segment, for example, 192.168.0.0/22

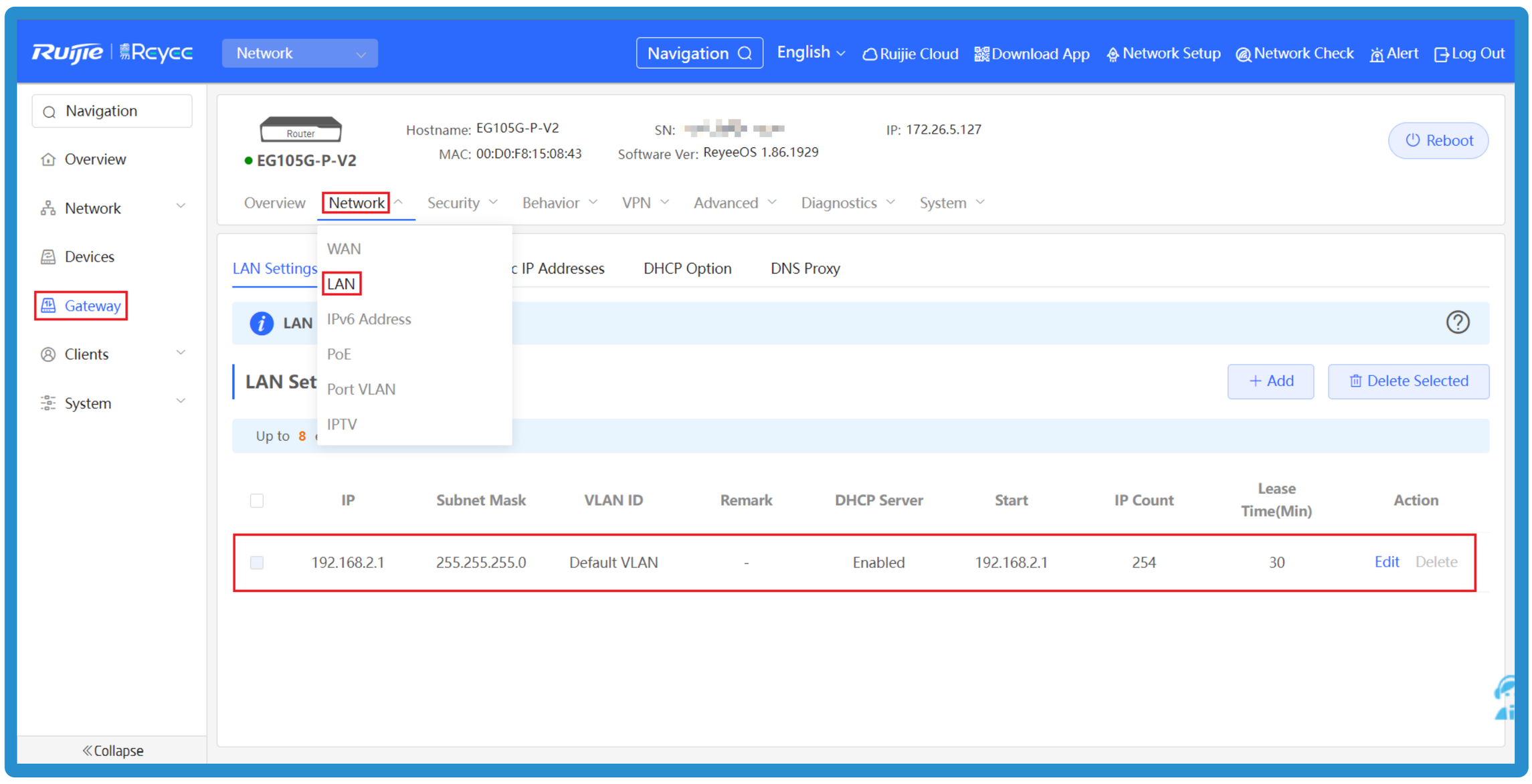
IV. Network Planning

1. Initial Configuration of Networks
2. Configure the intranet segments of three EGs
3. Establish the IPSec VPN among the branches and HQ
4. Connection Verification

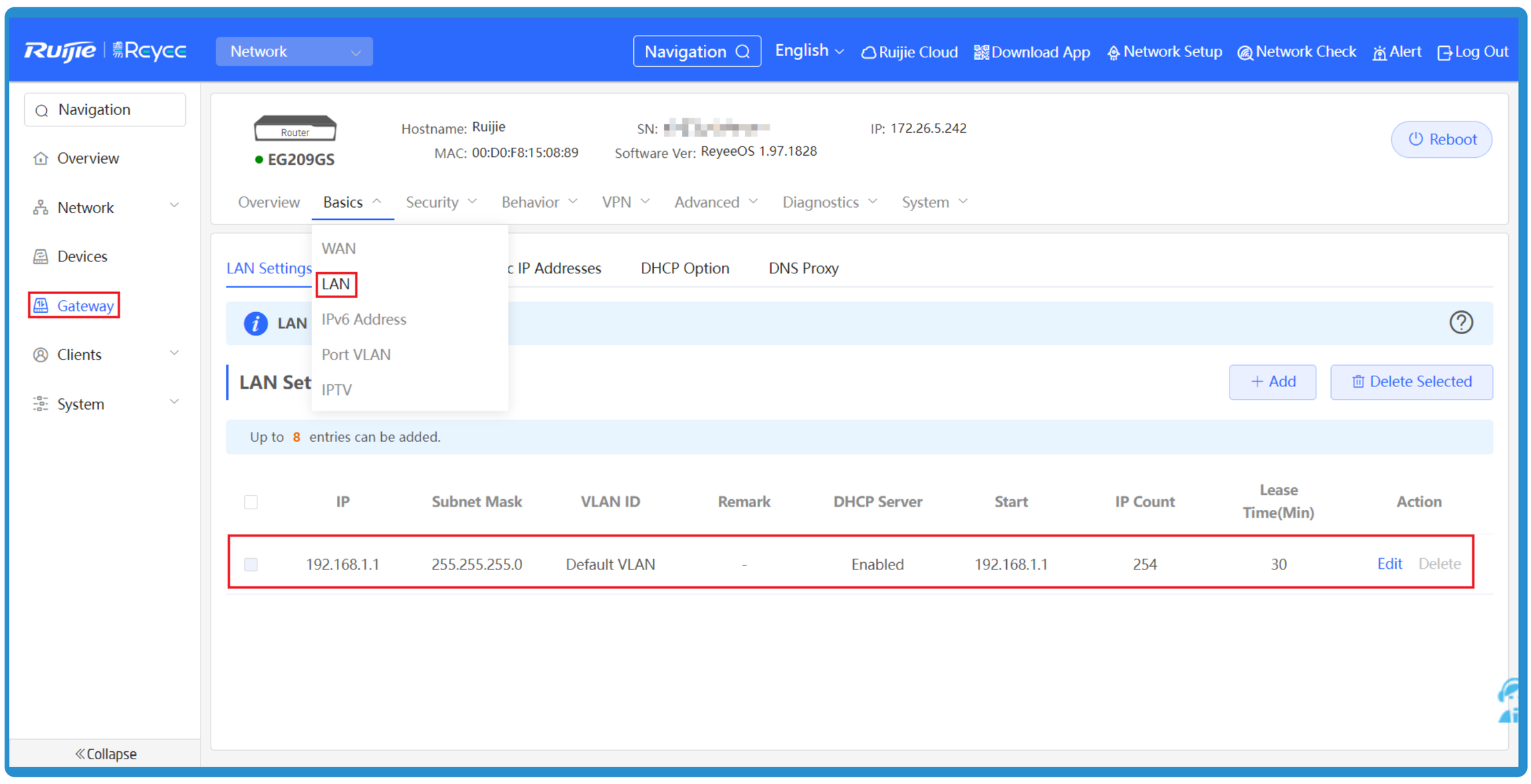
V. Configuration Steps

1 Configure the intranet segments of three EGs.

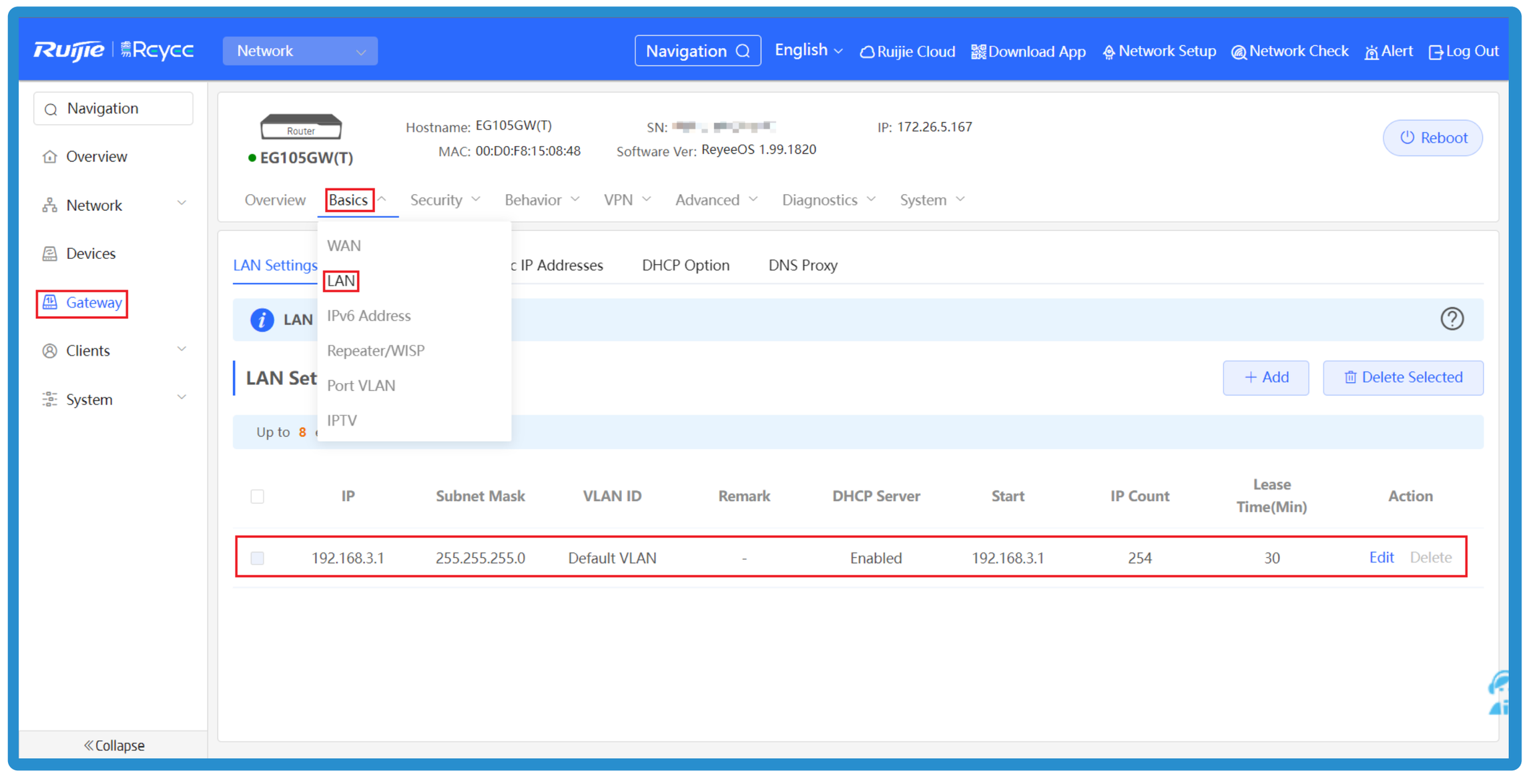
(1) Configure the intranet segments of HQ as 192.168.2.0/24



(2) Configure the intranet segments of Branch 1 as 192.168.1.0/24



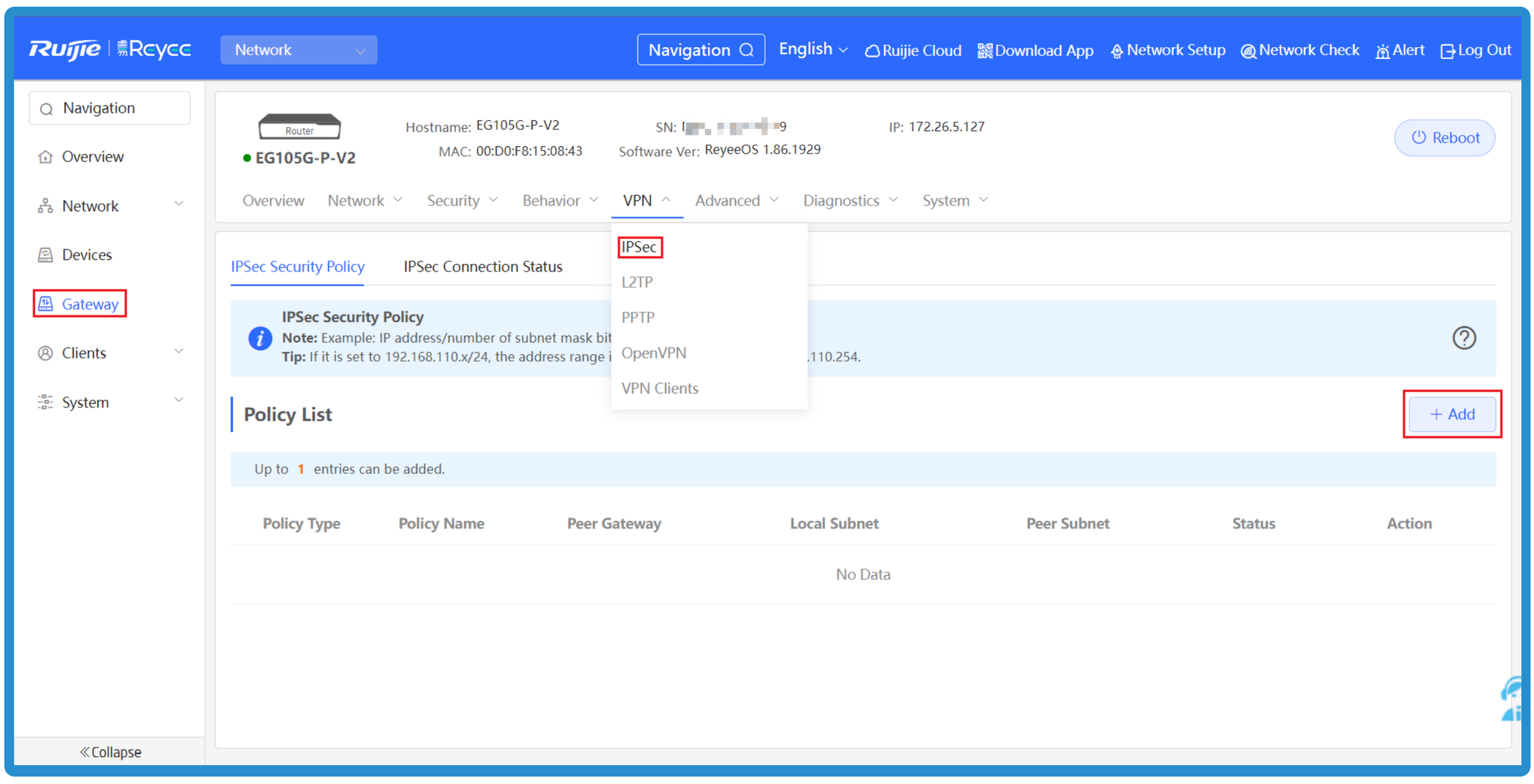
(3) Configure the intranet segments of Branch 2 as 192.168.3.0/24



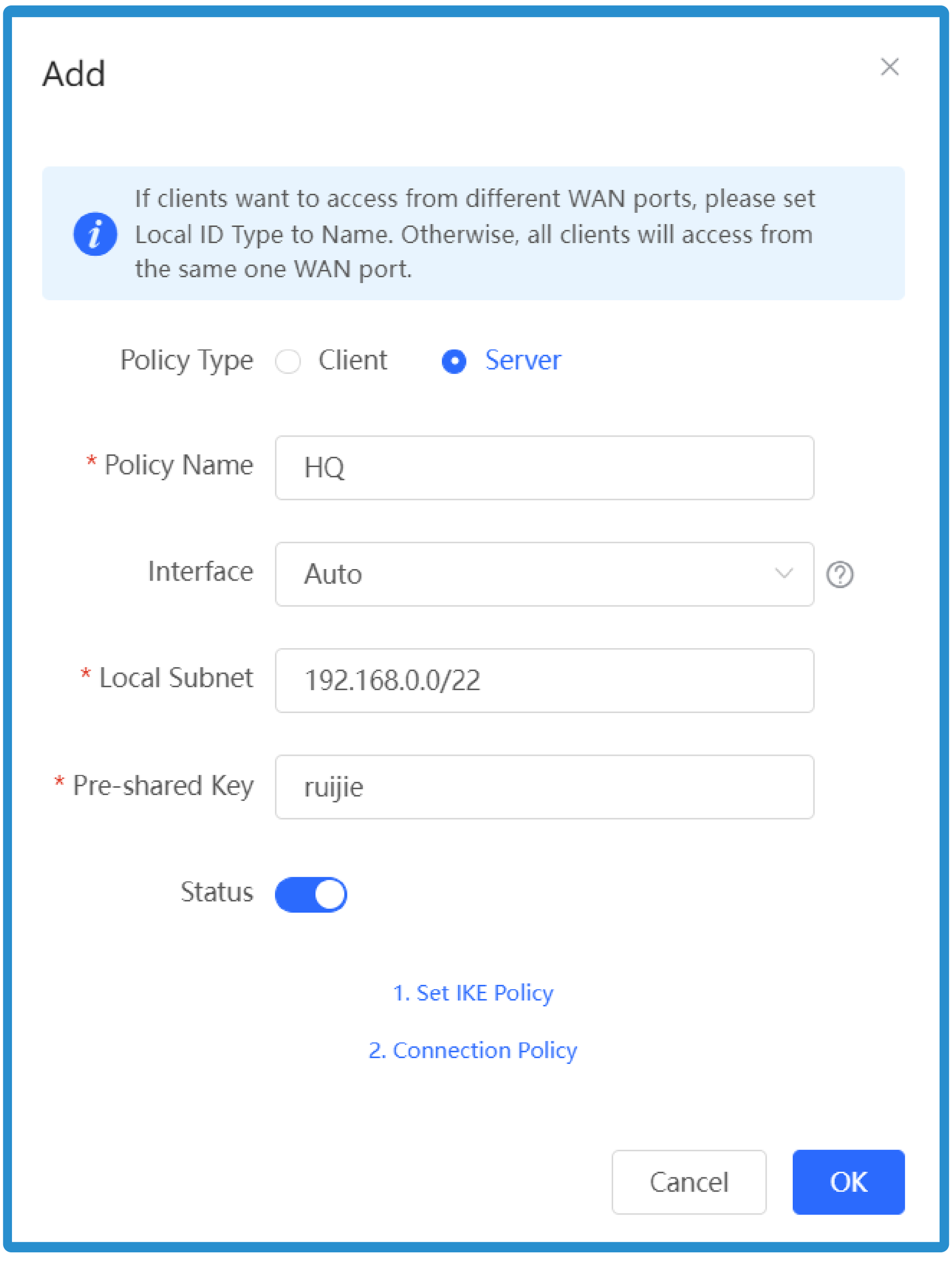
IV. Configuration Steps

② Establish the IPSec VPN among the HQ and two Branches.

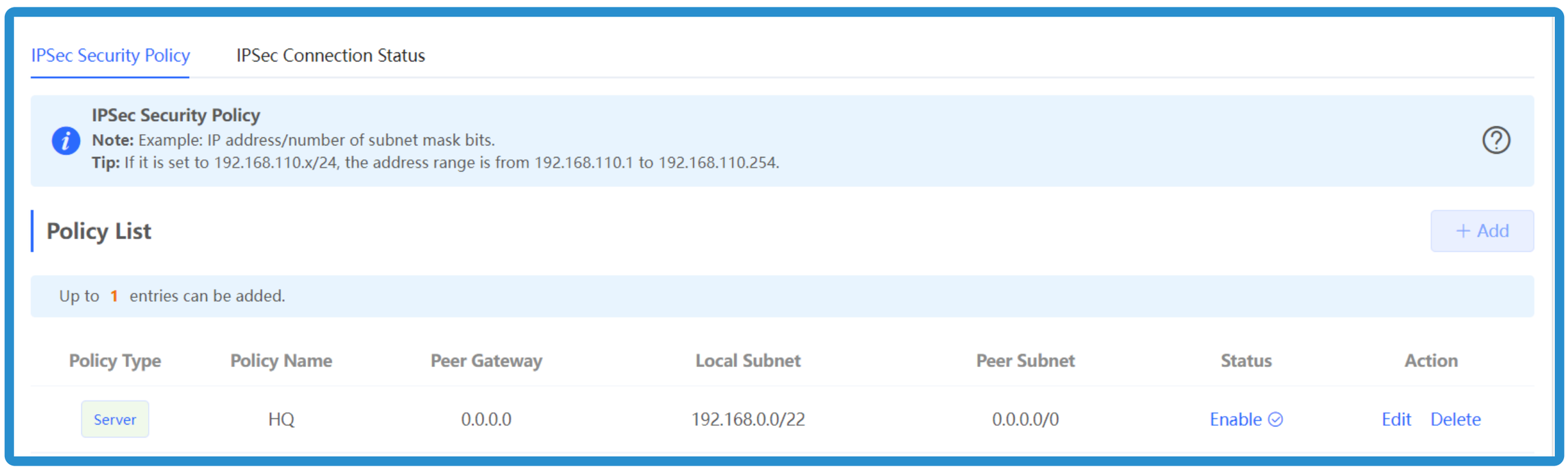
(1) HQ:



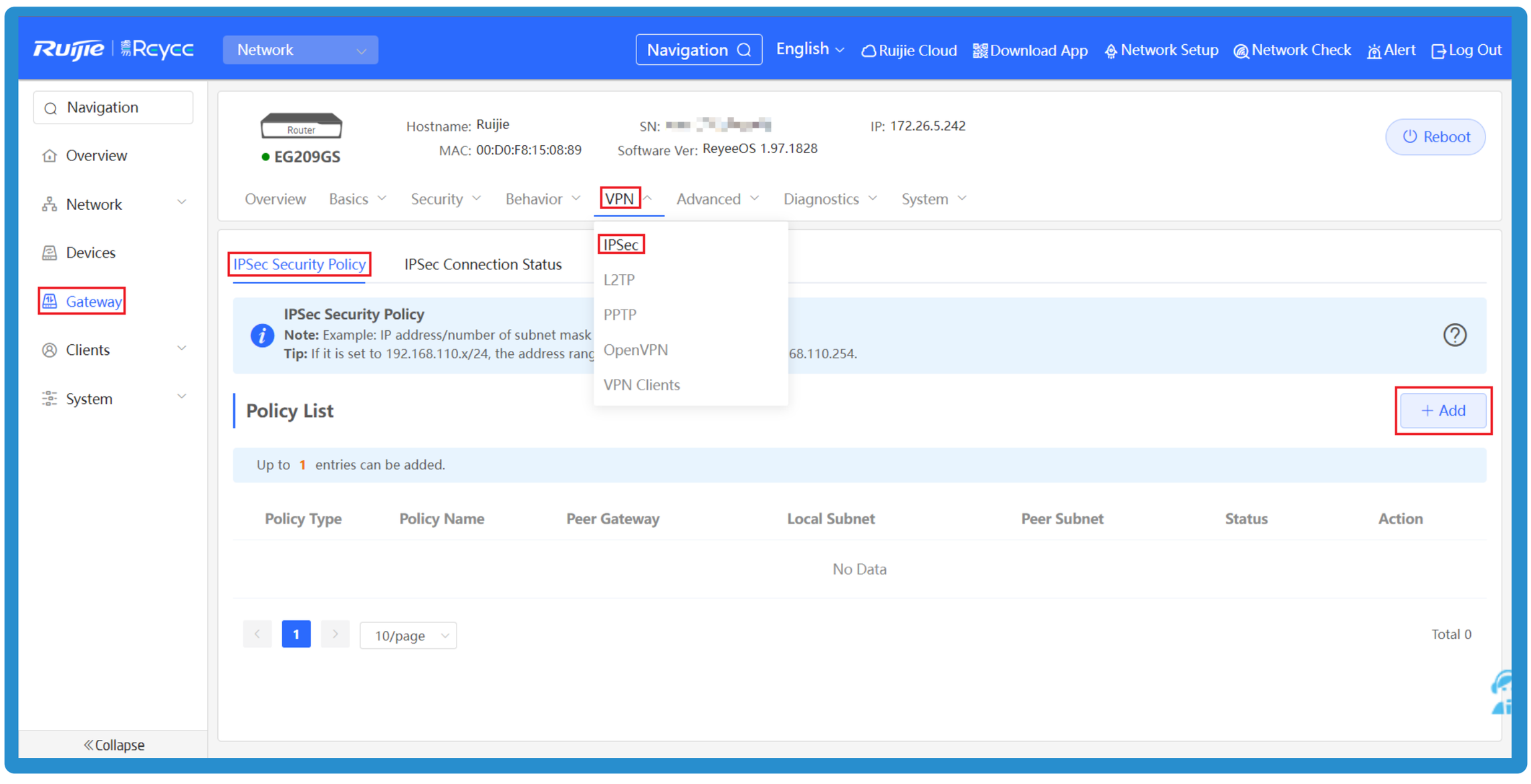
Configure the local subnet of HQ as 192.168.0.0/22



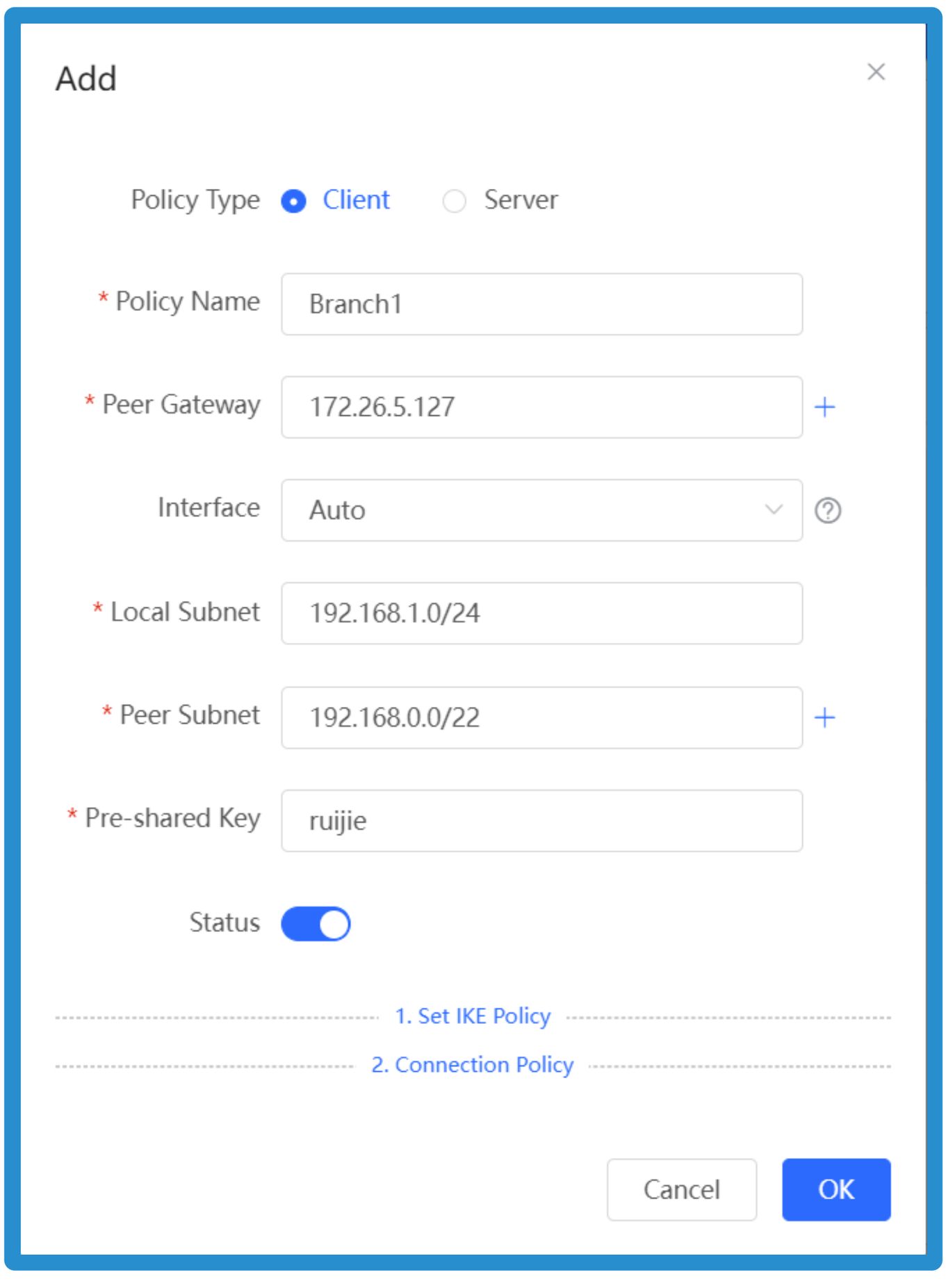
IV. Configuration Steps



(2) Branch 1

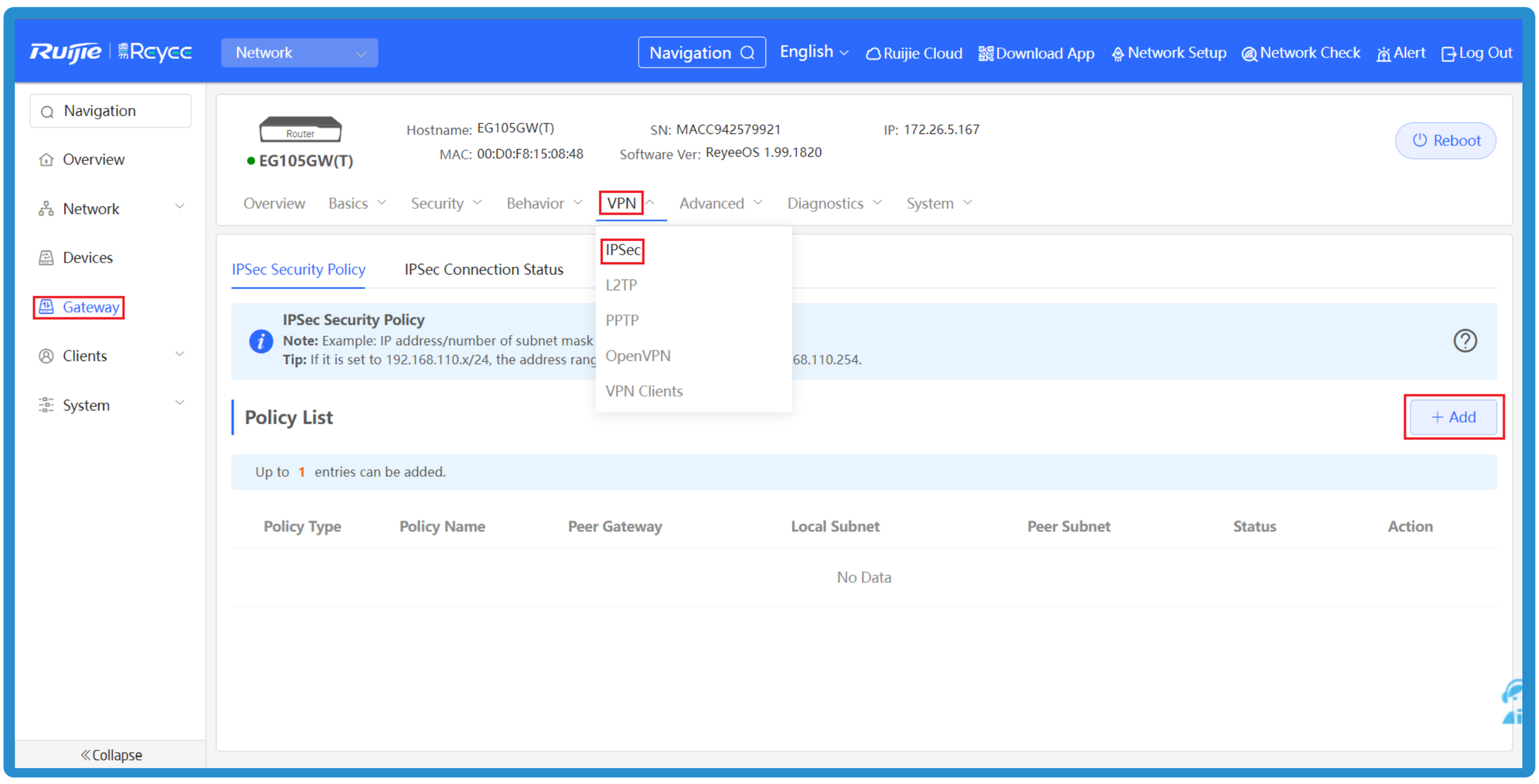


Configure the local subnet of Branch 1 as 192.168.1.0/24 and the peer subnet as 168.0.0/22

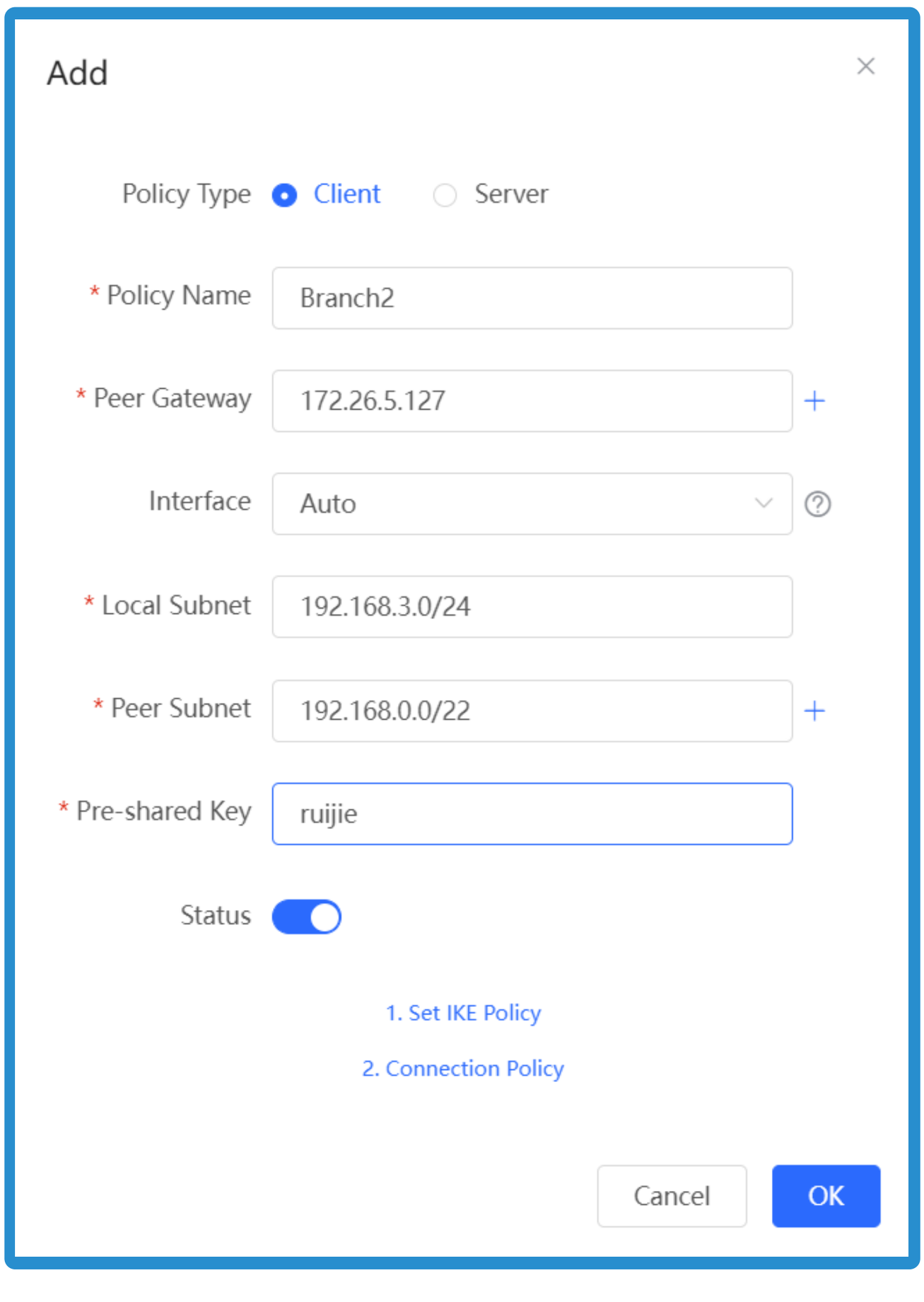


IV. Configuration Steps

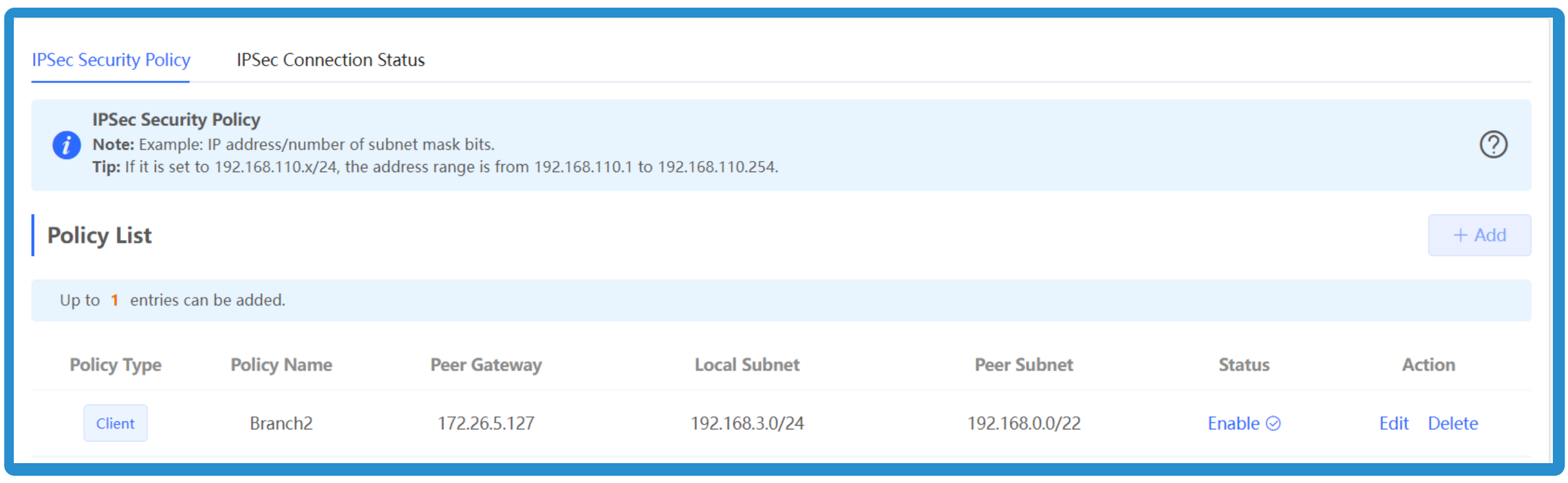
(3) Branch 2



Configure the local Subnet of Branch 1 as 192.168.3.0/24, and the peer subnet as 193.168.0.0/22



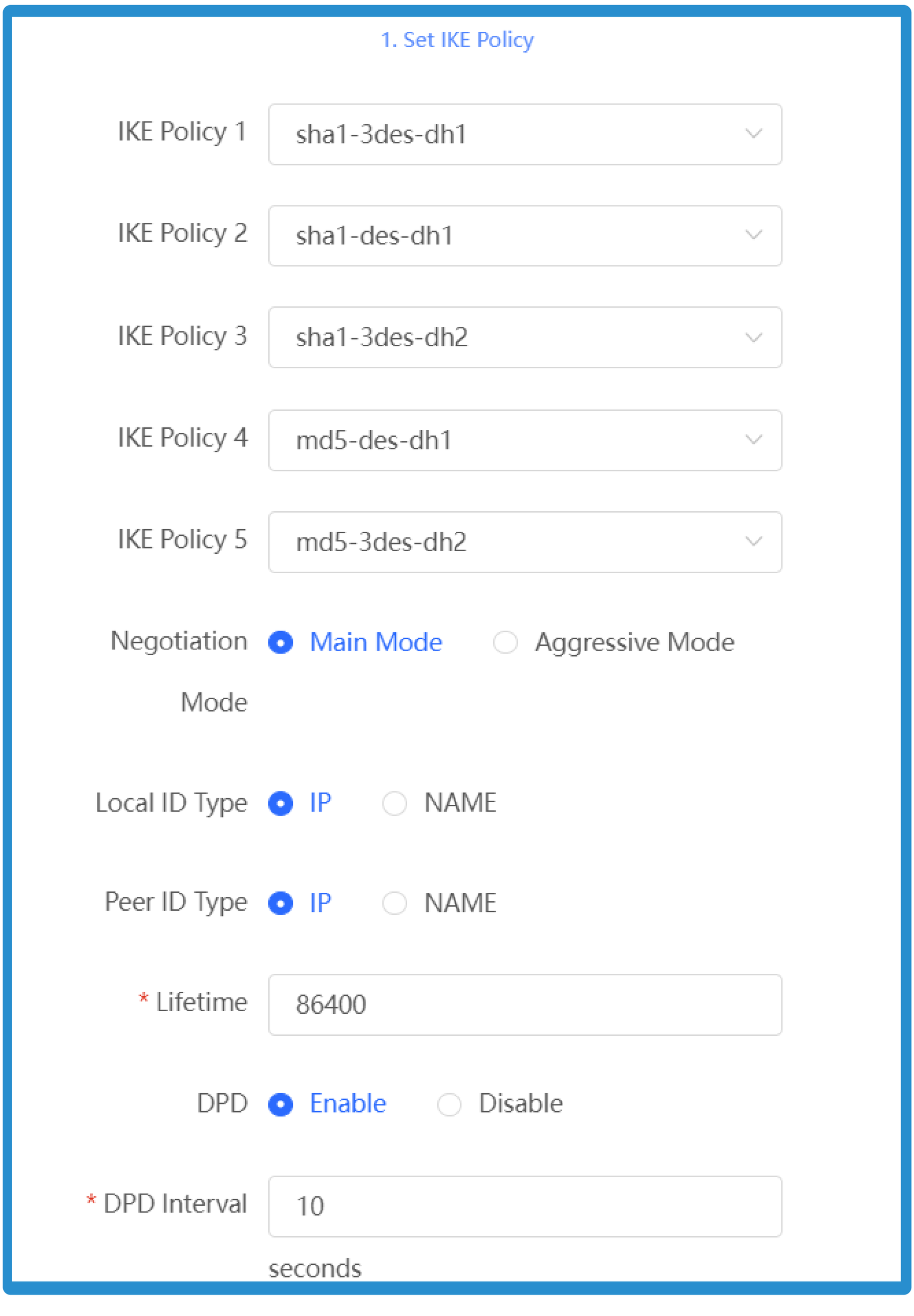
IV. Configuration Steps



Notice

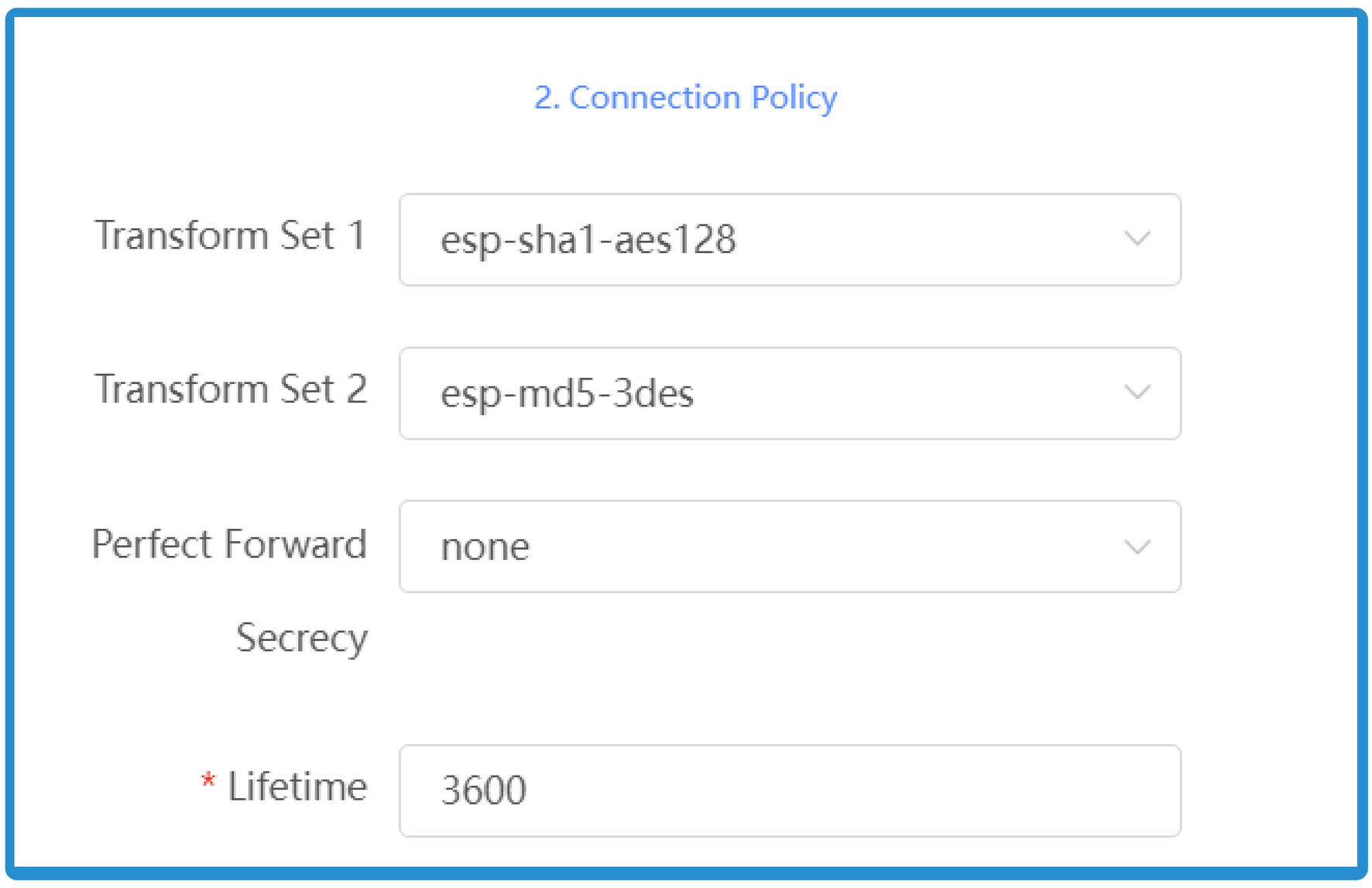
The IKE Policy and Transform of three EGs should be consistent

IKE Policy:



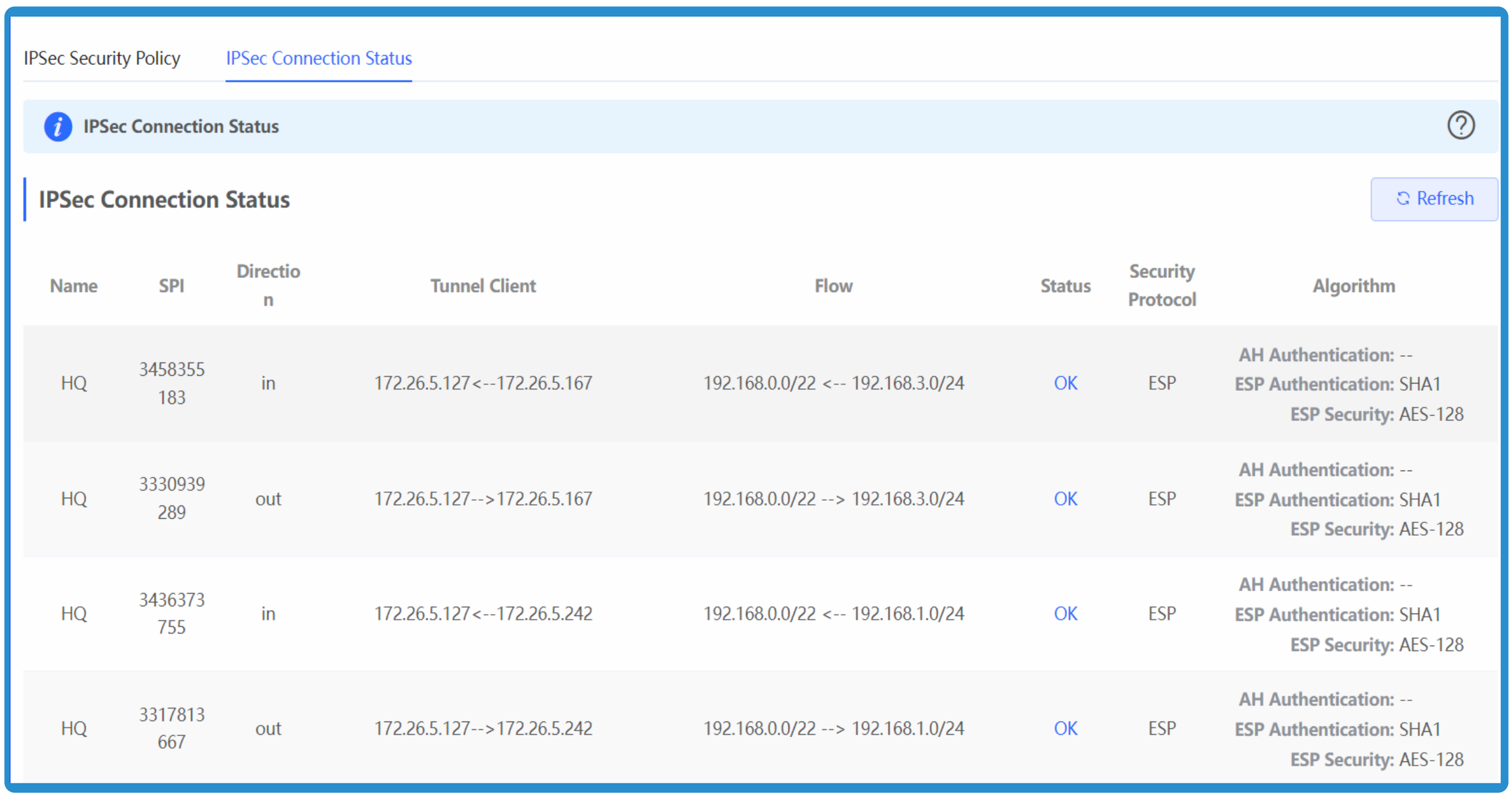
IV. Configuration Steps

Transform set:



3 Connection Check.

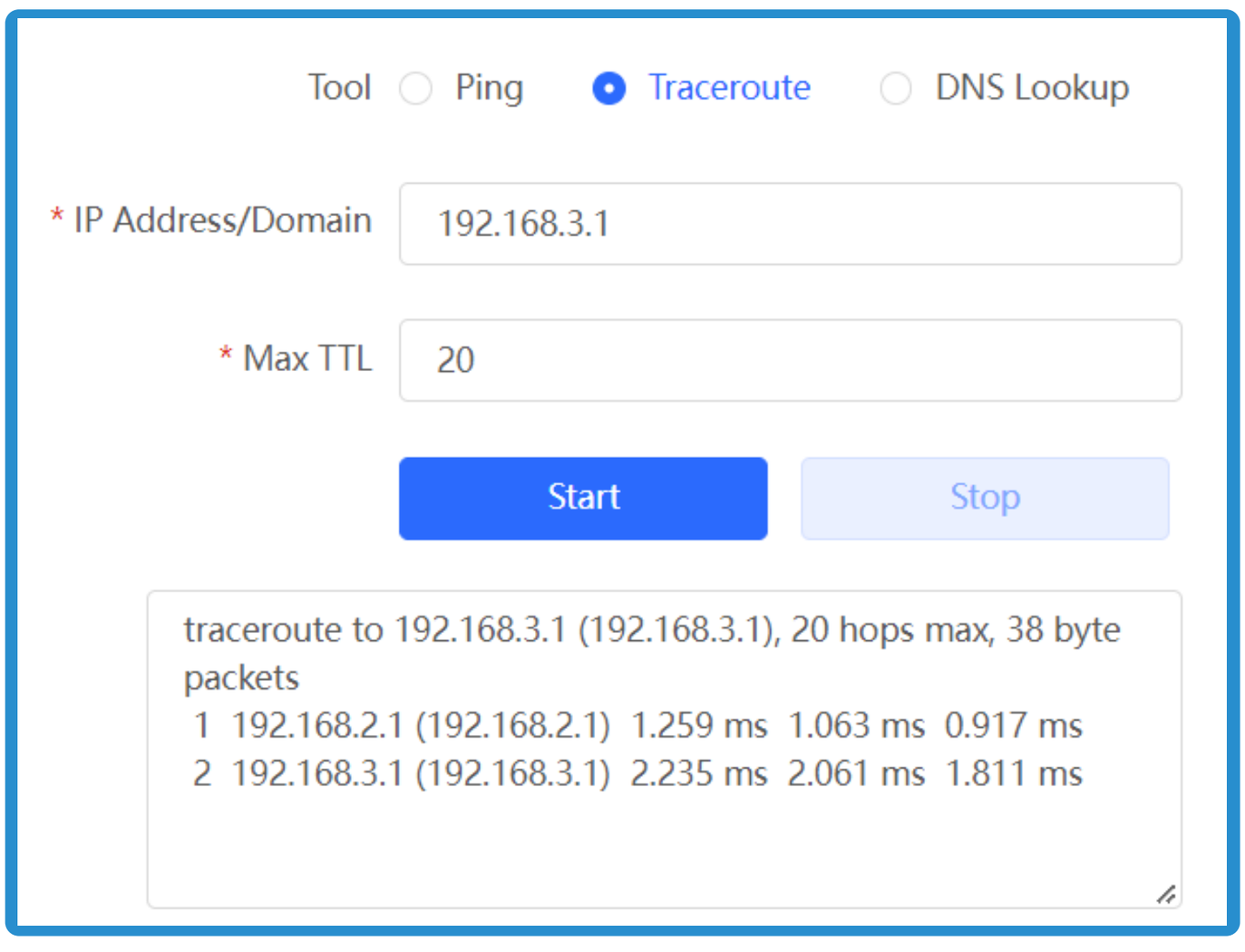
(1) Check the connection status on HQ: IPSec VPNs have been established successfully among two branches and HQ.



Name	SPI	Direction	Tunnel Client	Flow	Status	Security Protocol	Algorithm
HQ	3458355183	in	172.26.5.127<--172.26.5.167	192.168.0.0/22 <-- 192.168.3.0/24	OK	ESP	AH Authentication: -- ESP Authentication: SHA1 ESP Security: AES-128
HQ	3330939289	out	172.26.5.127-->172.26.5.167	192.168.0.0/22 --> 192.168.3.0/24	OK	ESP	AH Authentication: -- ESP Authentication: SHA1 ESP Security: AES-128
HQ	3436373755	in	172.26.5.127<--172.26.5.242	192.168.0.0/22 <-- 192.168.1.0/24	OK	ESP	AH Authentication: -- ESP Authentication: SHA1 ESP Security: AES-128
HQ	3317813667	out	172.26.5.127-->172.26.5.242	192.168.0.0/22 --> 192.168.1.0/24	OK	ESP	AH Authentication: -- ESP Authentication: SHA1 ESP Security: AES-128

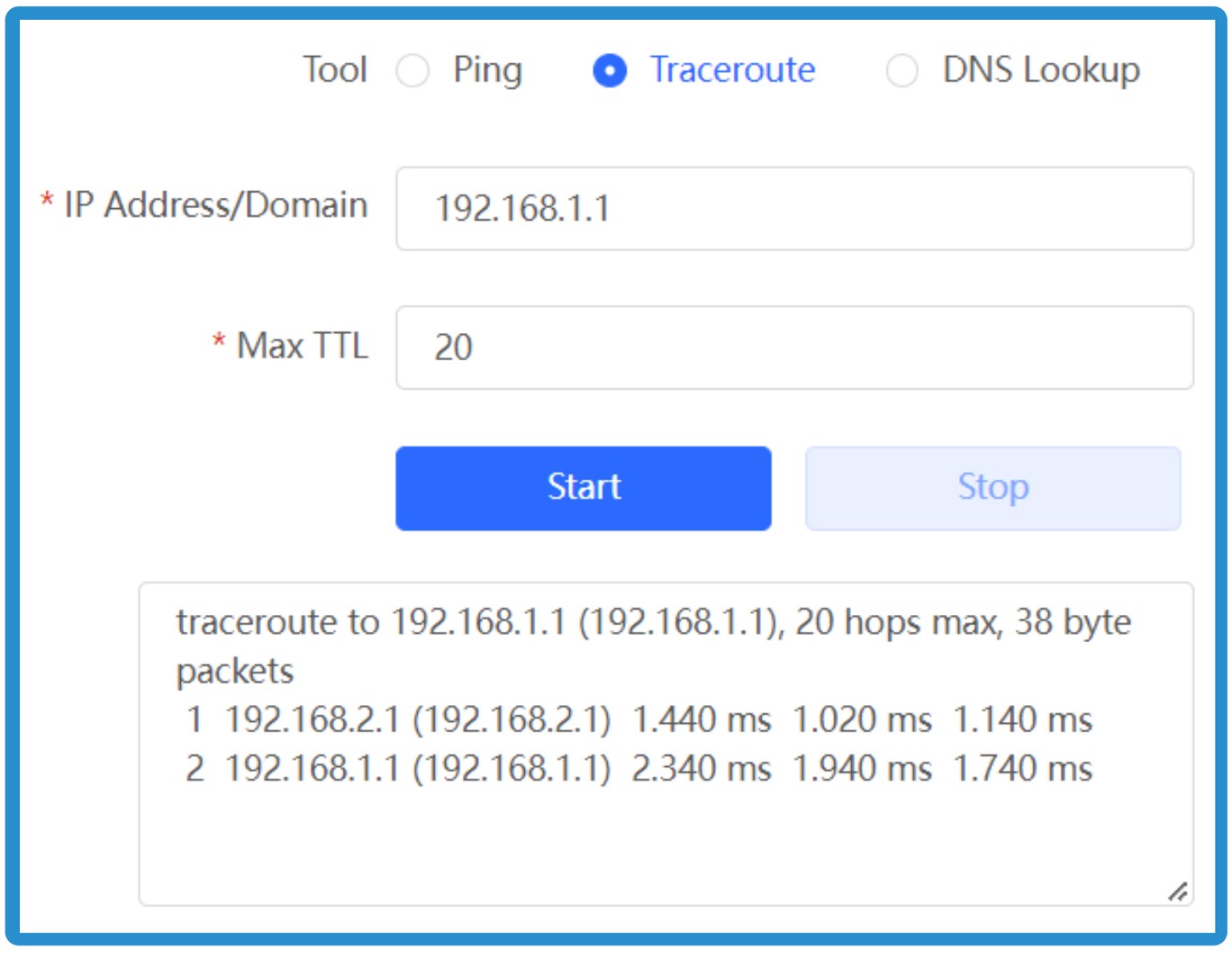
(2) Connection verification.

Branch 1 Traceroute Branch 2: Data from Branch 2 to branch 1 is transferred through HQ.



IV. Configuration Steps

Branch 2 Traceroute Branch 1: Data from Branch 1 to branch 2 is transferred through HQ.



Official Website ⋙ https://www.ruijienetworks.com

Community ⋙ https://community.ruijienetworks.com

Facebook ⋙ Ruijie Tech Support

YouTube ⋙ Ruijie Technical Support

Official Website

Community

Facebook

YouTube