SANGFOR

NGAF

SANGFOR VPN Configure In Route Mode Guide

Version 8.0.6

Table of Contents

1 Function introduction 1
2 Application scenarios 1
3 Description of necessary conditions 2
4 Configuration ideas 2
5 Configuration and screenshot 3
5.1 Configuring VPN 3
5.1.1 Headquarter configuration 3
5.1.2 Branch Configuration 8
6 Precautions 9

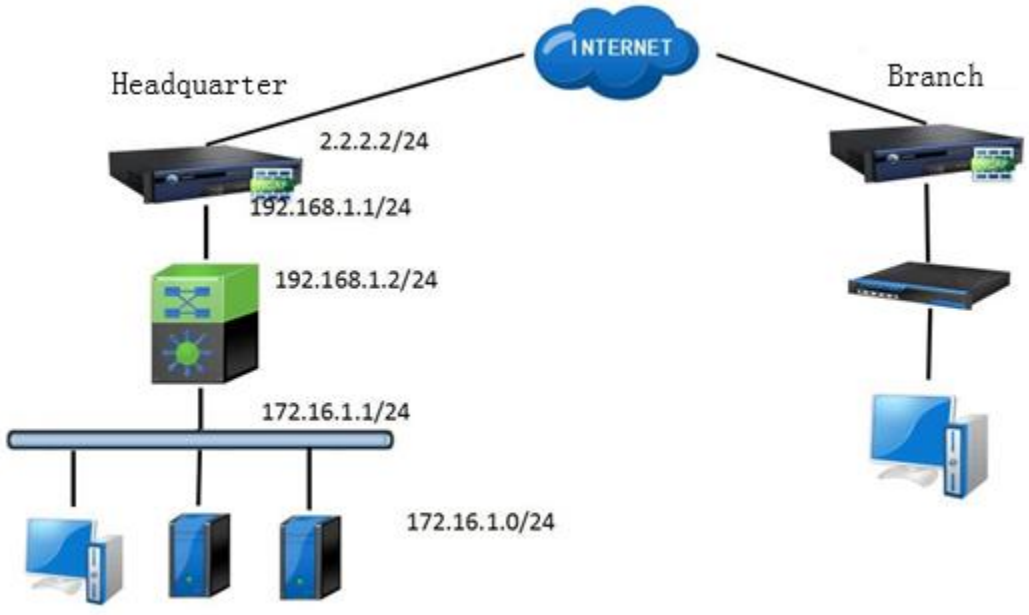
1 Function introduction

The full name of VPN is Virtual Private Network. VPN is defined as establishing a temporary and secure connection over a public network (normally through Internet), a secure and stable tunnel through a chaotic public network. By using this tunnel, you can encrypt data several times to achieve the purpose of using Internet safely. A virtual private network is an extension of an intranet. Virtual private networks help to remote users, corporate branches, business partners, and suppliers establish trusted and secure connections to the company's intranet for secure extranet virtual private networks that connect to business partners and users. VPN mainly uses tunnel technology, encryption technology, decryption technology, key management technology and user and device identity authentication technology.

2 Application scenarios

SANGFOR VPN application scenario:

1. Applicable users to use Windows computer to access SANGFOR VPN access application system for remote office.
2. Applicable to establish a SANGFOR VPN connection between headquarters and branches to connect headquarter network and branch network.



Topology diagram:

Headquarter:

1. NGAF device deployed in route mode on the internal network above Layer 3 switch. The internal network port eth1 is connected to the internal network switch and he eth2 is connected to the public network.

   Eth1 : 192.168.1.1/24

Eth2 : 2.2.2.2/24

Uplink Port of Layer 3 switch :172.16.1.0/24

2. The Layer 3 switch connected to the internal network, the internal network segment is 172.16.1.0/24.

Branch:

1. Branch NGAF gateway is deployed at the egress and the eth1 is the intranet port 10.10.10.1/24.
2. The internal network switch is a Layer 2 switch. The gateway of the internal network PC points to the LAN port of the NGAF. The network segment is 10.10.10.0/24.

3 Description of necessary conditions

1. One NGAF device and number of mobile users.
2. Another SANGFOR device.

4 Configuration ideas

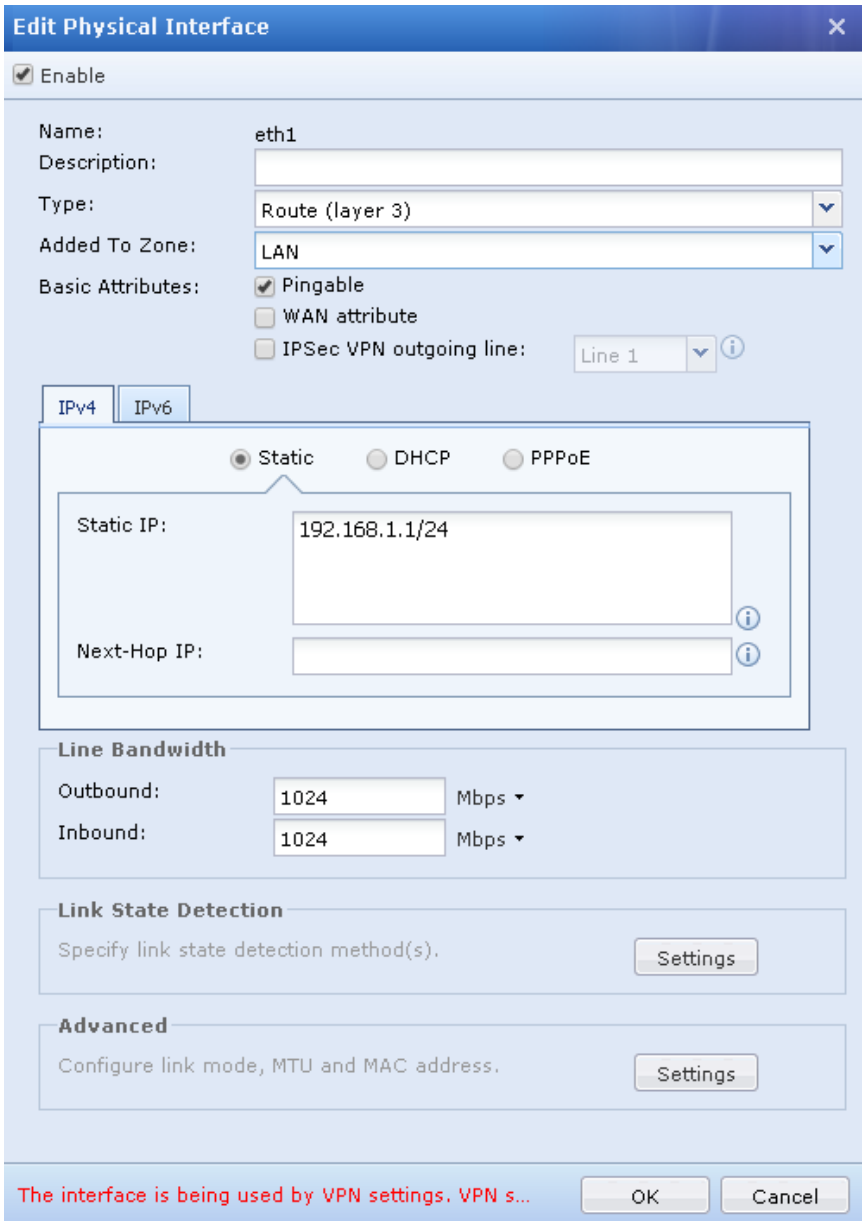
1. Configure the VPN configuration in the NGAF device WEB console.
2. You need to configure the VPN configuration in the SANGFOR device on peer end.

5 Configuration and screenshot

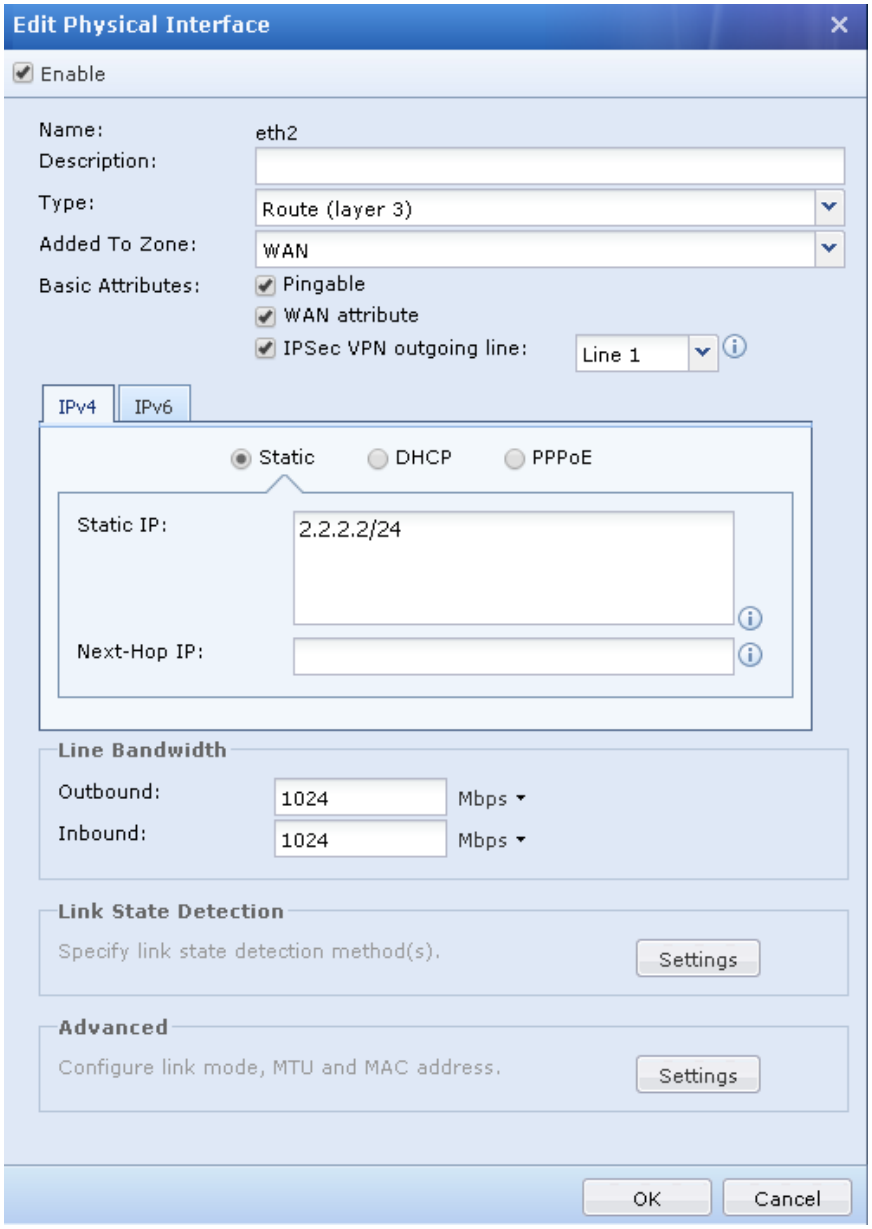
5.1 Configuring VPN

5.1.1 Headquarter configuration

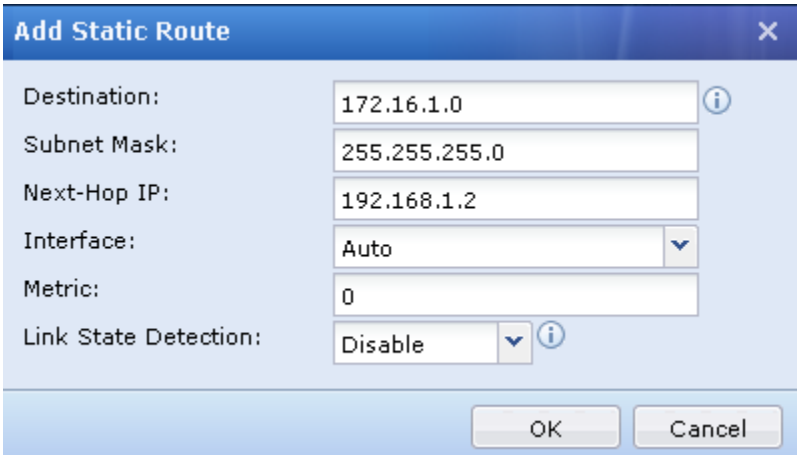
1. Go to Network > Interfaces > Physical Interface > eth1 as figure below:



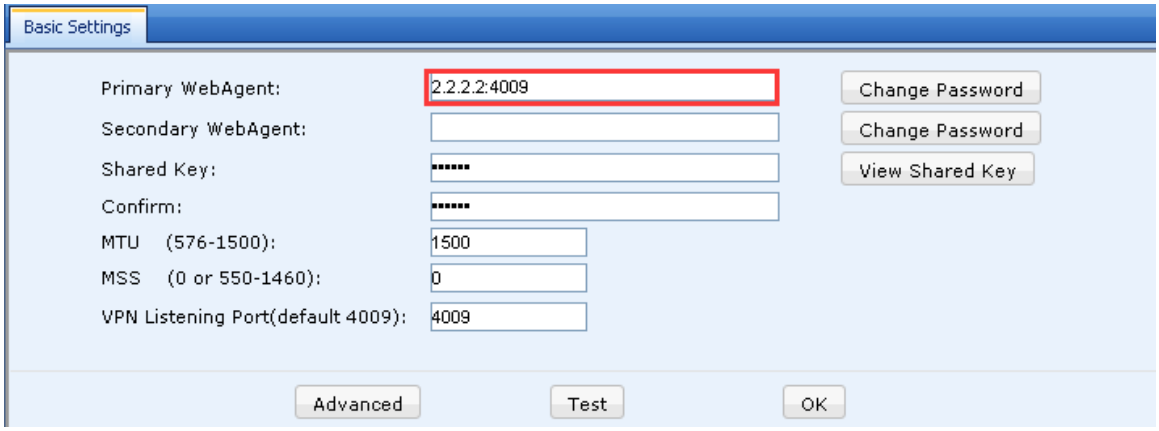
Go to Network > Interfaces > Physical Interface > eth2 as figure below:



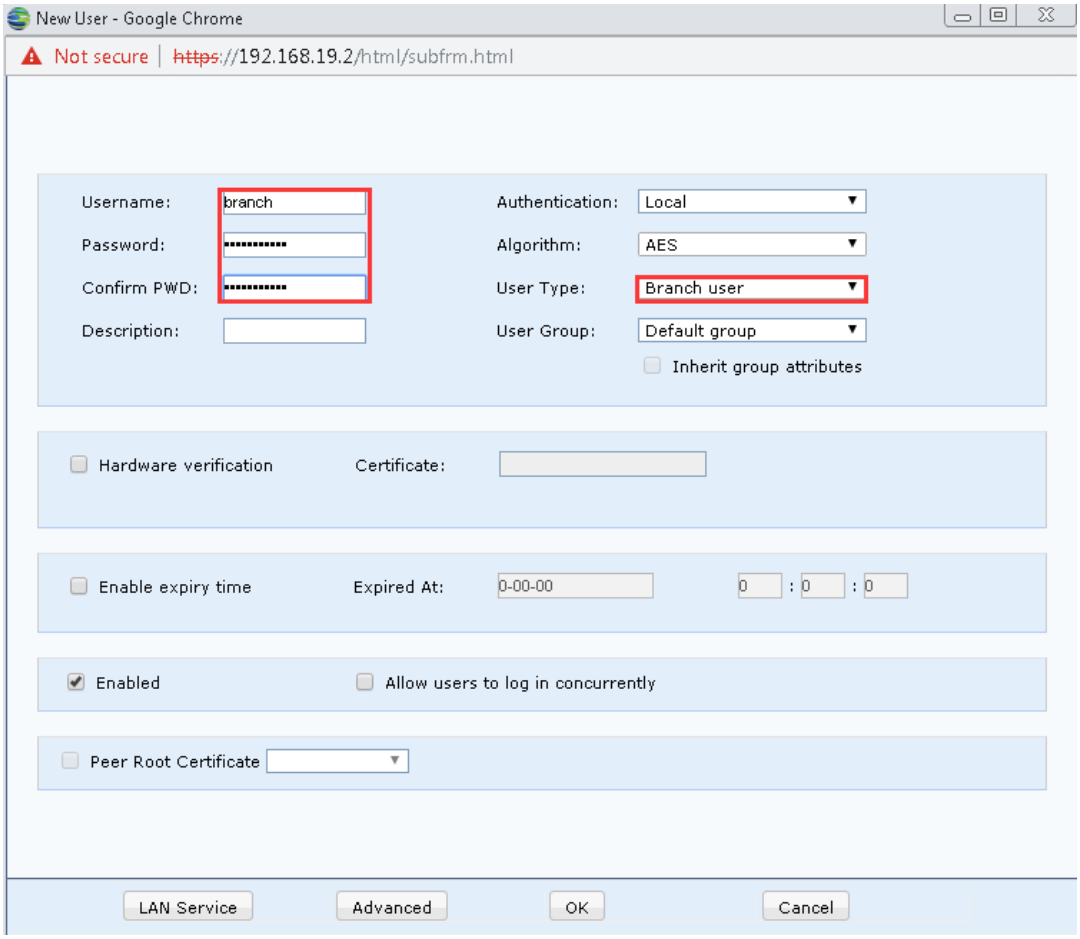
2. Go to **Network** > **Routing** > **Add** > **Static route,** add a packet return route. Destination write intranet network segment and next hop go to the uplink interface address of the Layer 3 Switch which shown in figure below:



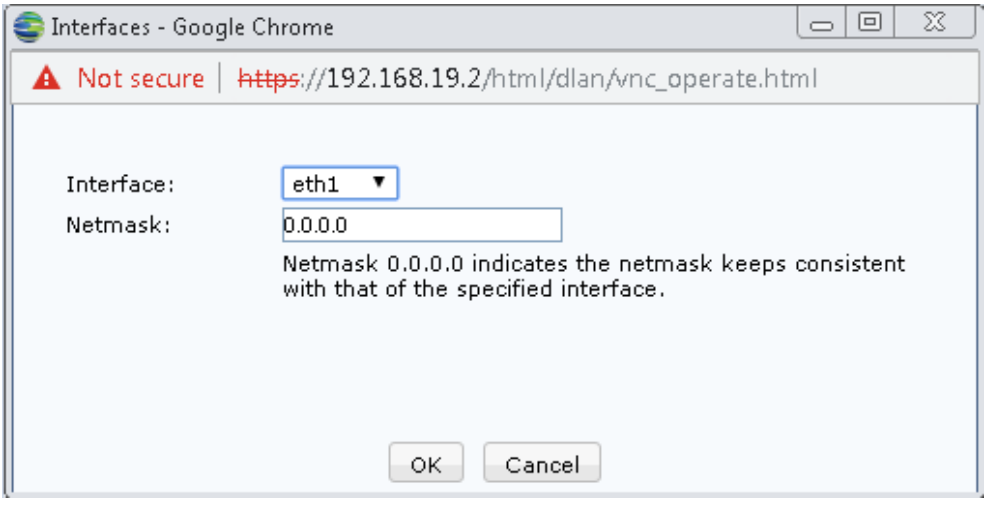
3. Go to **Network** > **IPSecVPN** > **Basics,** fill in the eth2 public address as figure below:



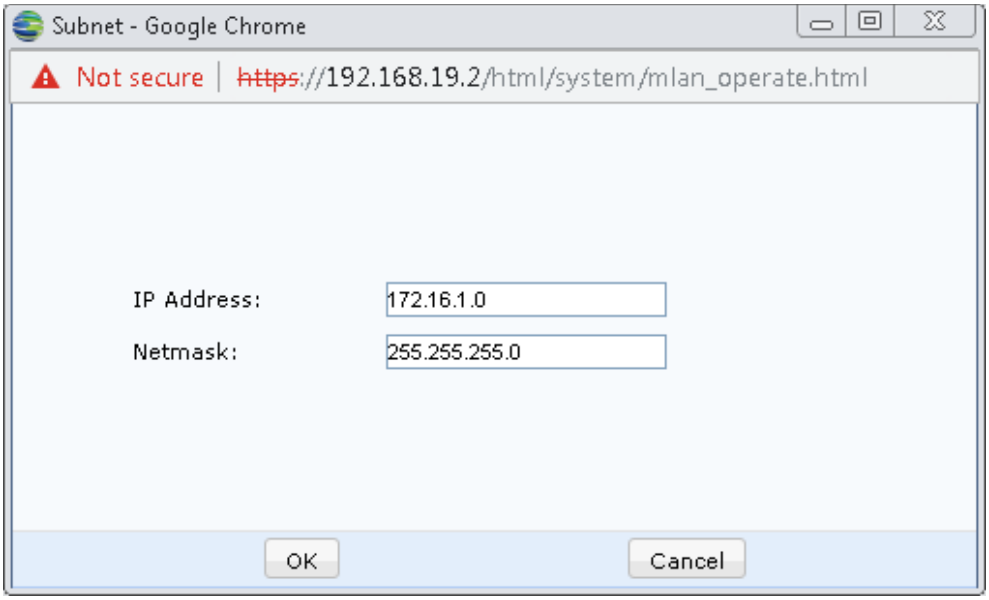
4. Go to Network > IPSecVPN > Local Users > New User, add a new user as figure below:



5. Go to **Network > IPSecVPN > VPN Interface,** add an LAN interface as figure below:

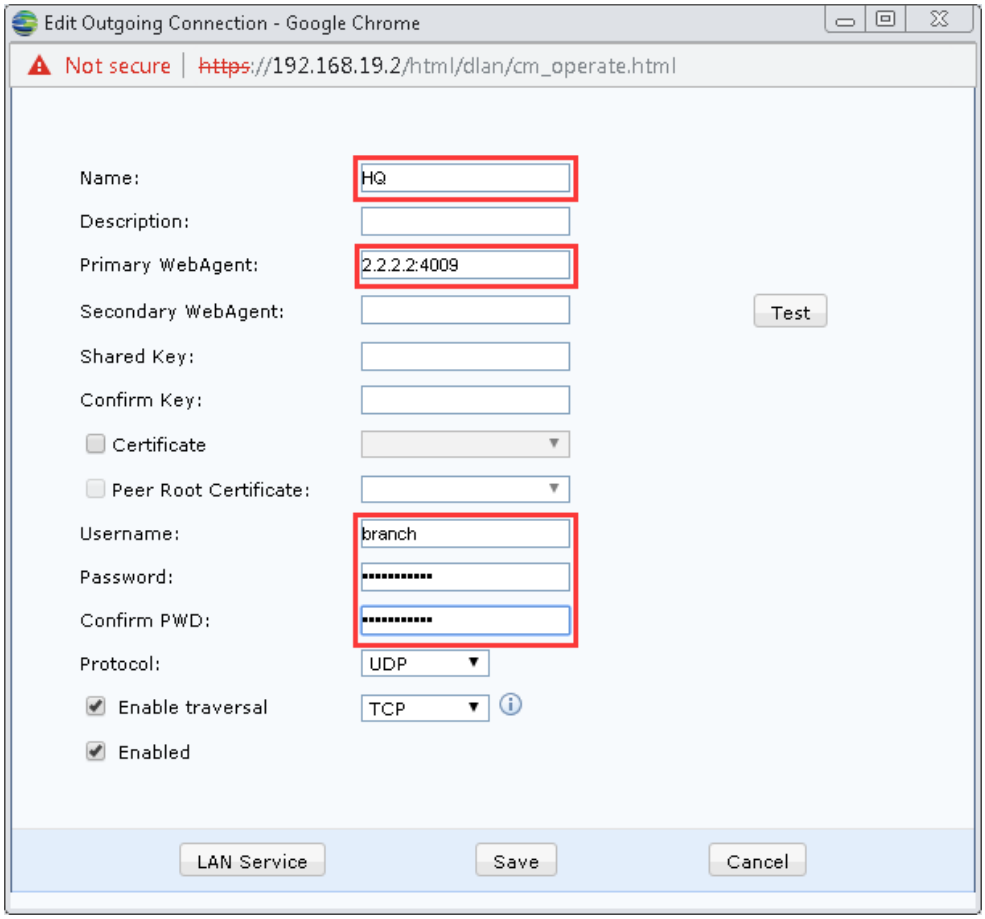


6. Go to Network > IPSecVPN > Local Subnet > Add, to LAN local subnet

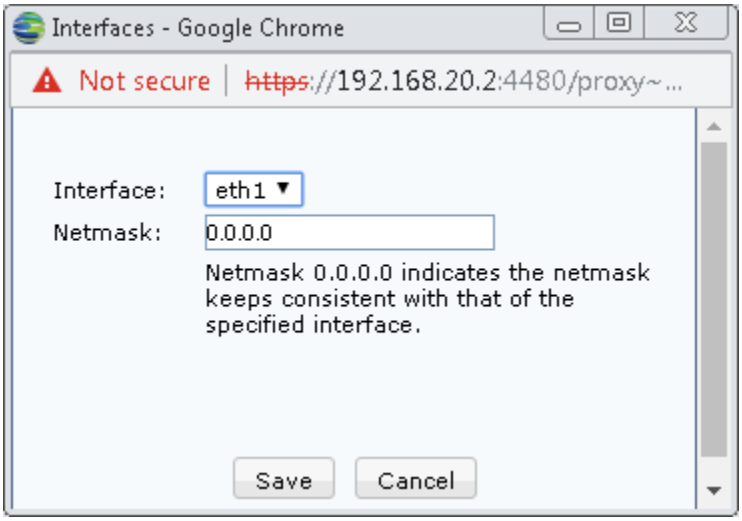


5.1.2 Branch Configuration

1. Go to **Network > IPSecVPN > VPN Connections,** fill in HQ webagent address and HQ local user as figure below:



2. Go to **Network > IPSecVPN > VPN Interface,** add an LAN interface as figure below:



6 Precautions

1. Branch and Headquarter need to configure VPN interface settings.
2. If you dont have a static public IP, need to request a WEBAGENT address.