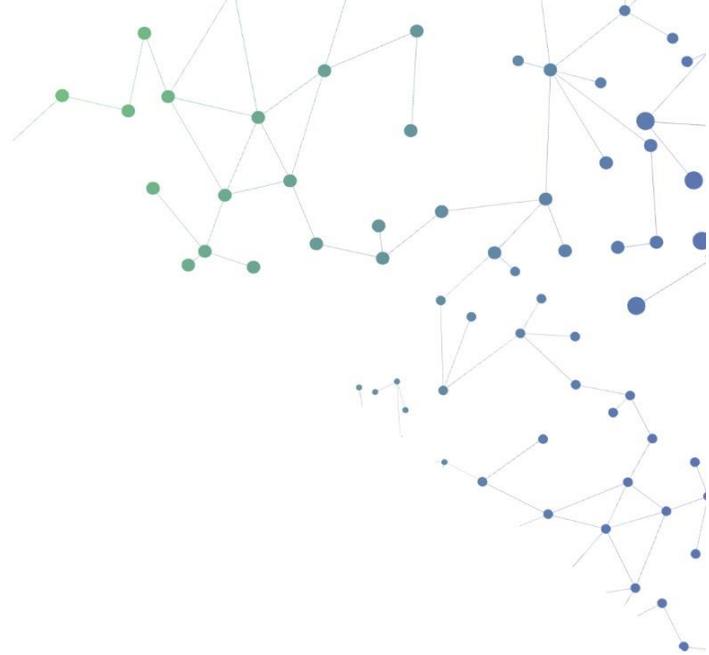




SANGFOR



NGAF

**SANGFOR VPN Configure In Route Mode
Guide**

Version 8.0.6

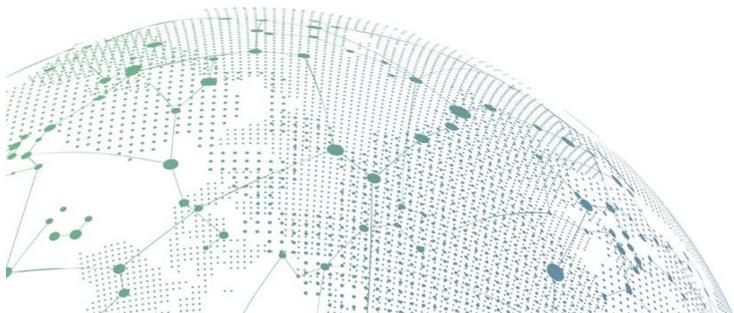


Table of Contents

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

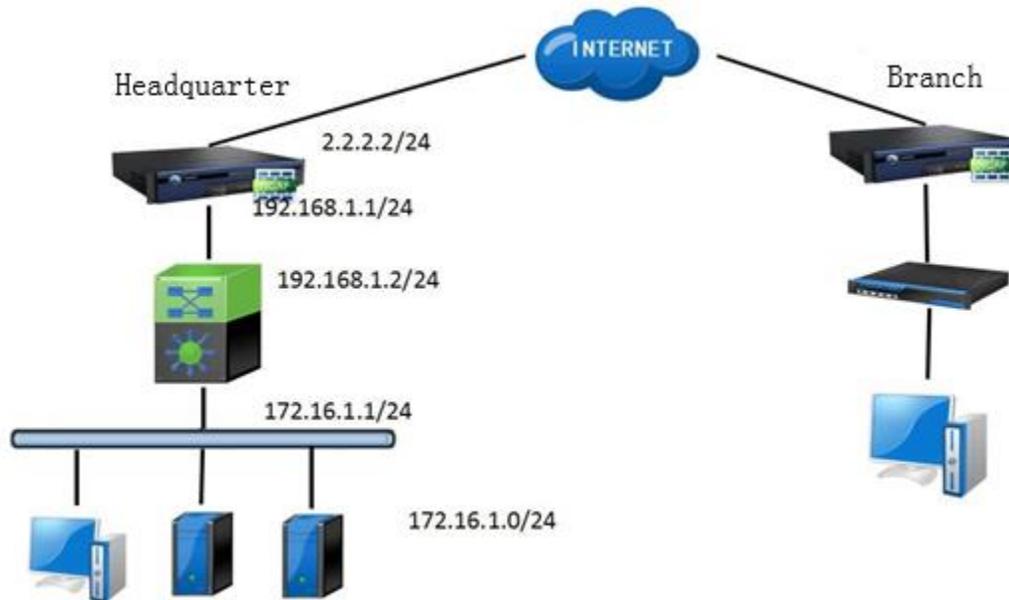
1 Function introduction

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:

Edit Physical Interface

Enable

Name: eth1
Description:
Type: Route (layer 3)
Added To Zone: LAN
Basic Attributes: Pingable
 WAN attribute
 IPsec VPN outgoing line: Line 1

Static DHCP PPPoE

Static IP: 192.168.1.1/24
Next-Hop IP:

Line Bandwidth

Outbound: 1024 Mbps
Inbound: 1024 Mbps

Link State Detection

Specify link state detection method(s).

Advanced

Configure link mode, MTU and MAC address.

The interface is being used by VPN settings. VPN s...

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

Edit Physical Interface

Enable

Name: eth2

Description:

Type: Route (layer 3) ▼

Added To Zone: WAN ▼

Basic Attributes:

- Pingable
- WAN attribute
- IPSec VPN outgoing line: Line 1 ▼ ⓘ

IPv4 IPv6

Static DHCP PPPoE

Static IP: 2.2.2.2/24 ⓘ

Next-Hop IP: ⓘ

Line Bandwidth

Outbound: 1024 Mbps ▼

Inbound: 1024 Mbps ▼

Link State Detection

Specify link state detection method(s).

Advanced

Configure link mode, MTU and MAC address.

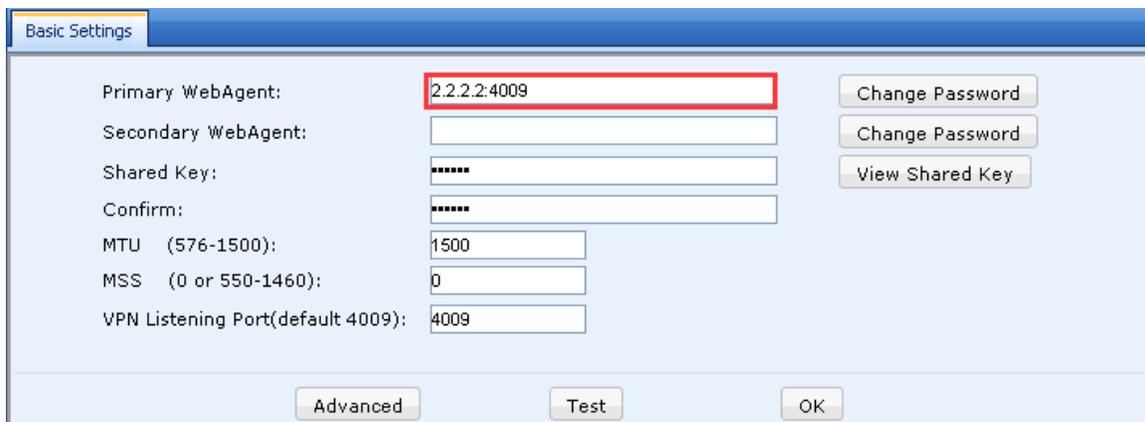
2. Go to **Network > Routing > Add > Static route**, add a packet return route. Destination write intranet network segment and next hop go to the uplink interface address of the Layer 3 Switch which shown in figure below:



Destination:	172.16.1.0
Subnet Mask:	255.255.255.0
Next-Hop IP:	192.168.1.2
Interface:	Auto
Metric:	0
Link State Detection:	Disable

OK Cancel

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



Primary WebAgent:	2.2.2.2:4009	Change Password
Secondary WebAgent:		Change Password
Shared Key:	*****	View Shared Key
Confirm:	*****	
MTU (576-1500):	1500	
MSS (0 or 550-1460):	0	
VPN Listening Port(default 4009):	4009	

Advanced Test OK

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

New User - Google Chrome
Not secure | https://192.168.19.2/html/subfrm.html

Username: Authentication:
Password: Algorithm:
Confirm PWD: User Type:
Description: User Group:
 Inherit group attributes

Hardware verification Certificate:

Enable expiry time Expired At: : :

Enabled Allow users to log in concurrently

Peer Root Certificate

LAN Service Advanced OK Cancel

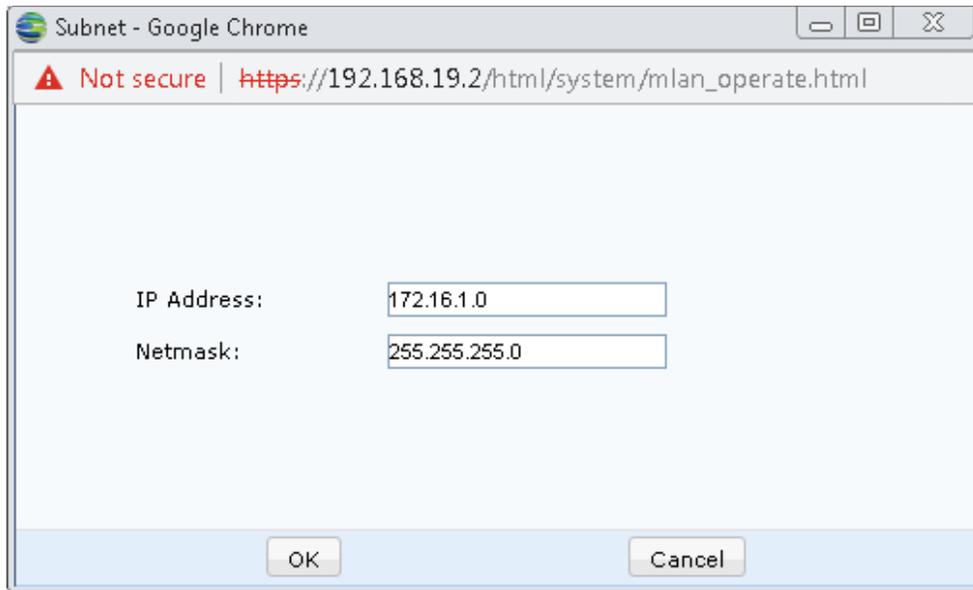
5. Go to Network > IPsecVPN > VPN Interface, add an LAN interface as figure below:

Interfaces - Google Chrome
Not secure | https://192.168.19.2/html/dlan/vnc_operate.html

Interface:
Netmask:
Netmask 0.0.0.0 indicates the netmask keeps consistent with that of the specified interface.

OK Cancel

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



The screenshot shows a web browser window titled "Subnet - Google Chrome". The address bar displays a "Not secure" warning and the URL "https://192.168.19.2/html/system/mlan_operate.html". The main content area contains a form with two input fields: "IP Address:" with the value "172.16.1.0" and "Netmask:" with the value "255.255.255.0". At the bottom of the form are "OK" and "Cancel" buttons.

5.1.2 Branch Configuration

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

Not secure | https://192.168.19.2/html/dlan/cm_operate.html

Name:

Description:

Primary WebAgent:

Secondary WebAgent:

Shared Key:

Confirm Key:

Certificate

Peer Root Certificate:

Username:

Password:

Confirm PWD:

Protocol:

Enable traversal

Enabled

Test

LAN Service Save Cancel

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

Not secure | <https://192.168.20.2:4480/proxy~...>

Interface:

Netmask:

Netmask 0.0.0.0 indicates the netmask keeps consistent with that of the specified interface.

Save Cancel

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.