SANGFOR

NGAF

Best Practices for Scenarios_Establish SangforVPN

Version 8.0.17

Change Log

Date	Change Description
July 31, 2020	Version 8.0.17 document release.
May 17, 2021	Document update.

CONTENT

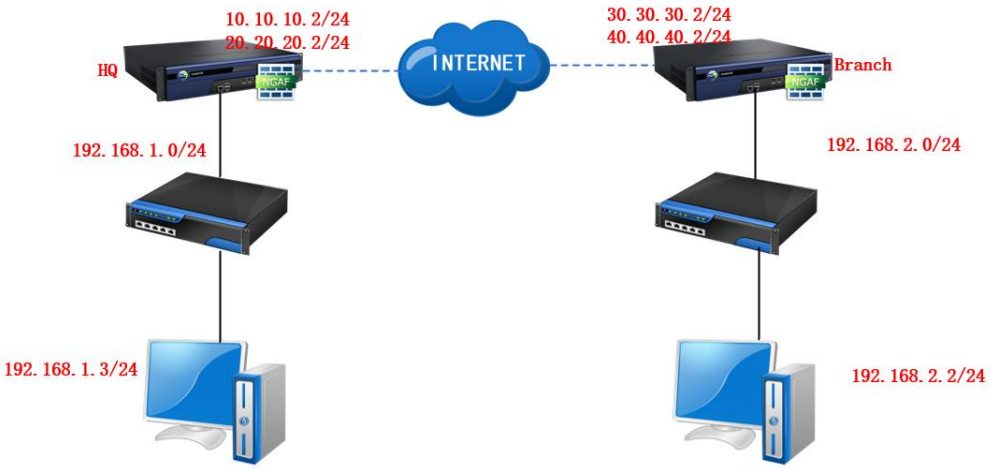
Chapter 1 Scenario

XX National Post Company has branches and stores in many places; now the customer's network requirements allow branches and stores to access the web services of the headquarters, while ensuring that data transmission is secure and encrypted.

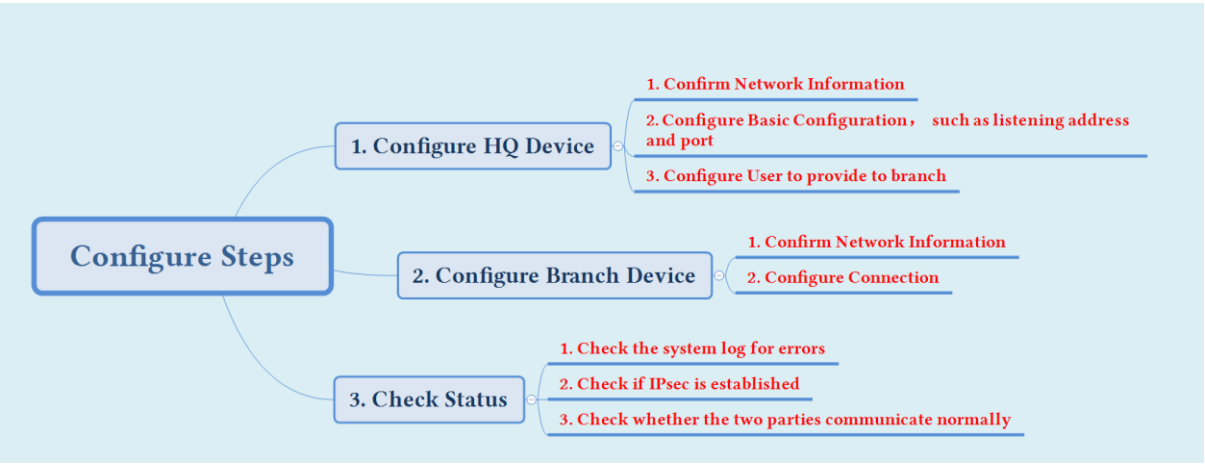
By analyzing the customer network, we can use SangforVPN to connect the headquarters and branch networks so that the branches can access the resources of the headquarters through SangforVPN.

SangforVPN requires at least one end to be accessible on the public network, that is, directly connected to the Internet. The customer's headquarters uses AF as the network exit and is a fixed IP, thus meeting the demand.

Check whether the network segments of the headquarters and branches conflict.

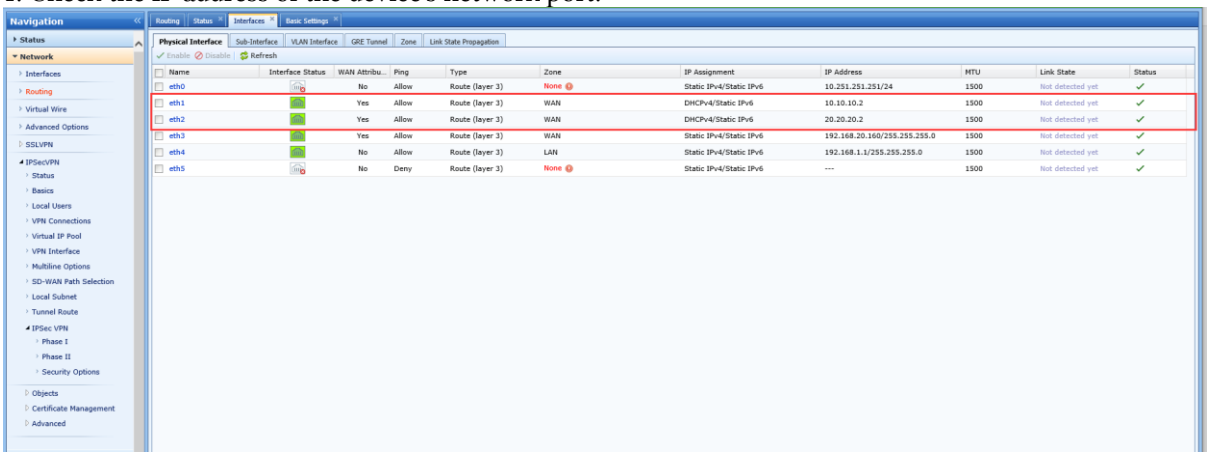


1.1 Configure Steps

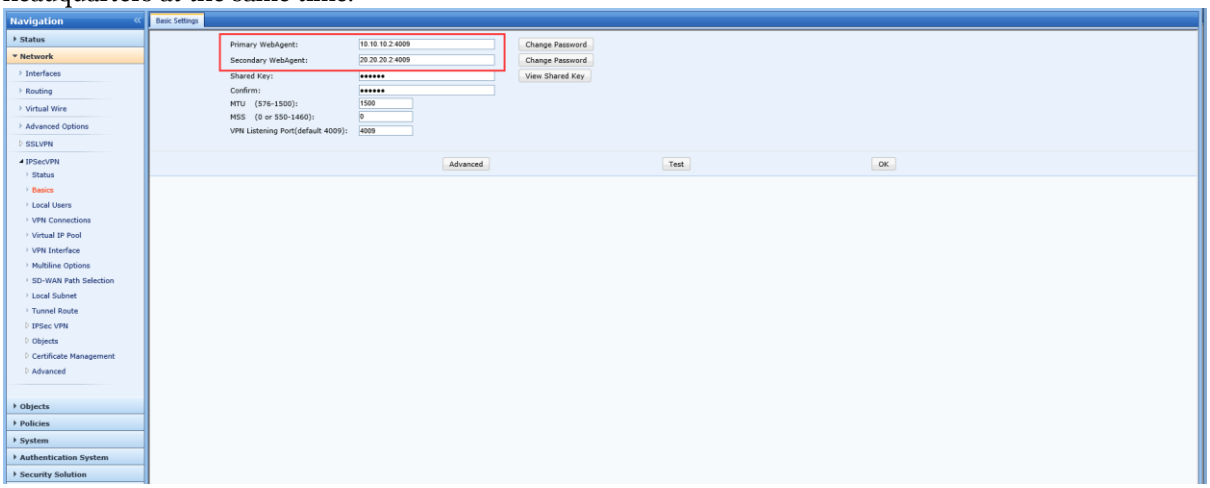


Chapter 2 Configure HQ AF

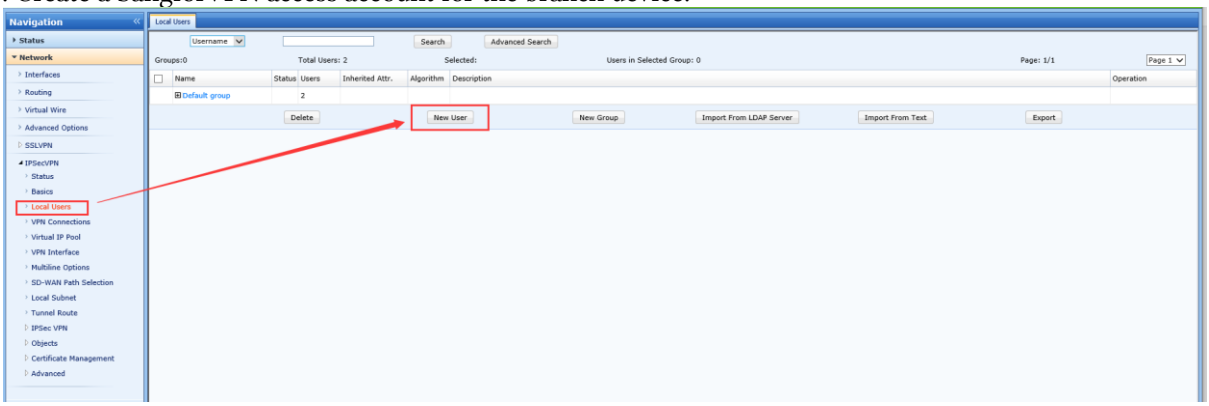
1. Check the IP address of the device's network port.

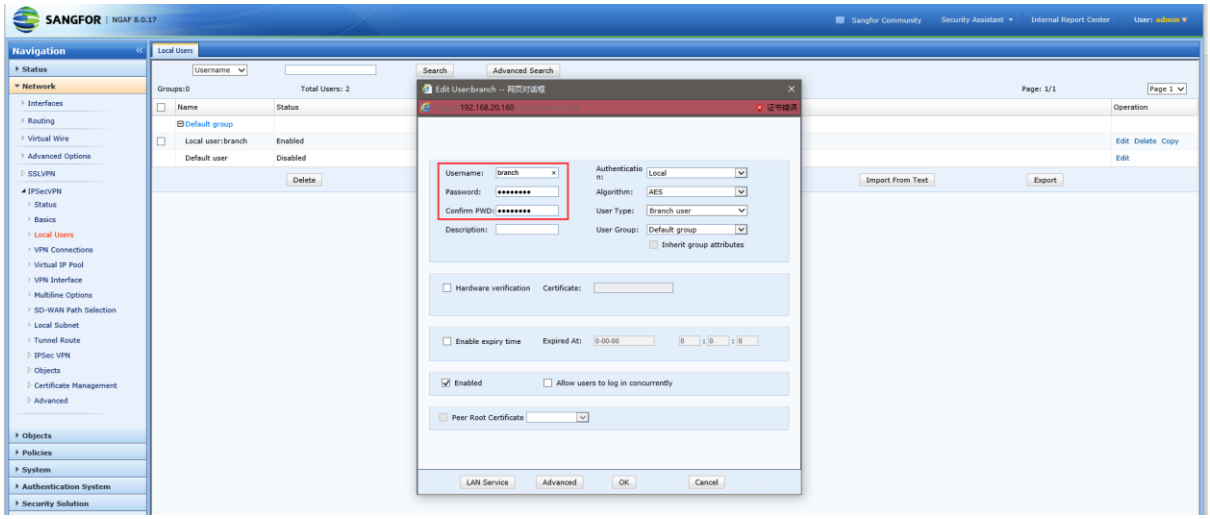


2. Configure the primary webagent and secondary webagent according to the address of the device network port; at the same time, configure the port to be 4009 when writing webagent, which is the default listening port of SangforVPN. If you need to fill it out, you need to fill it out at the branch and headquarters at the same time.

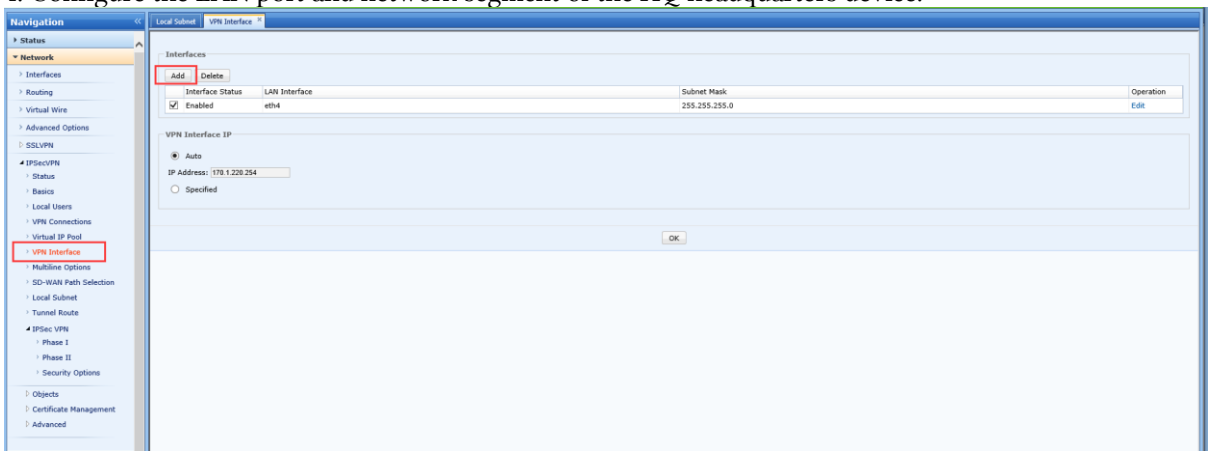


3. Create a SangforVPN access account for the branch device.

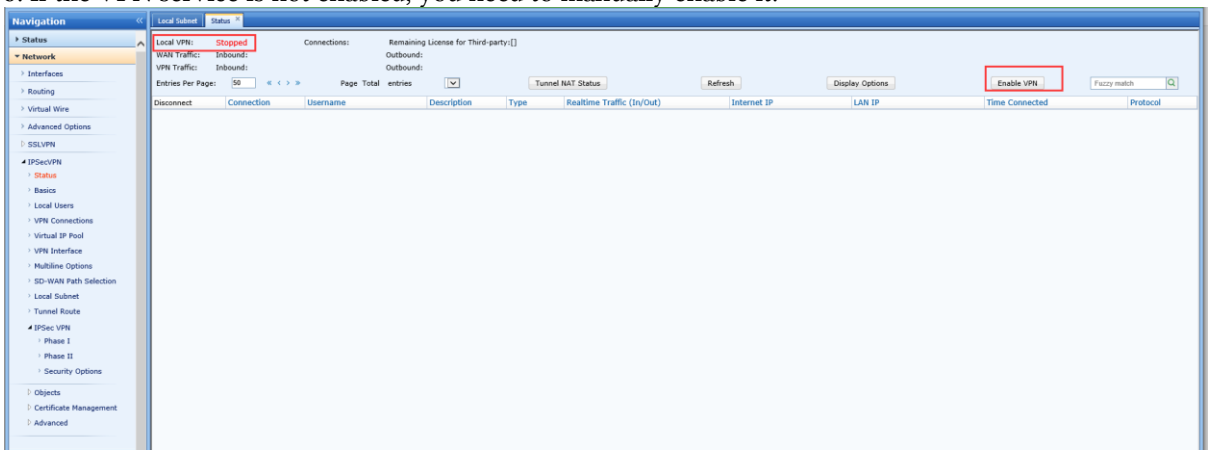




4. Configure the LAN port and network segment of the HQ headquarters device.

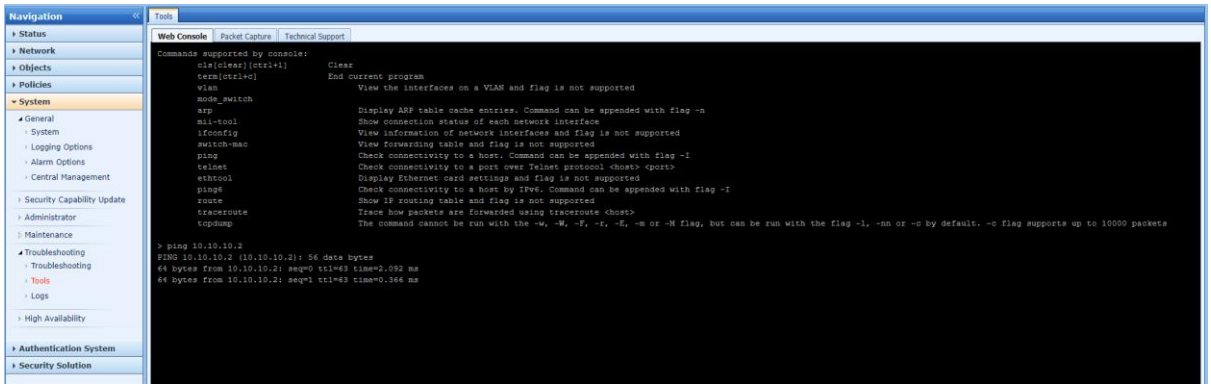


5. If the VPN service is not enabled, you need to manually enable it.

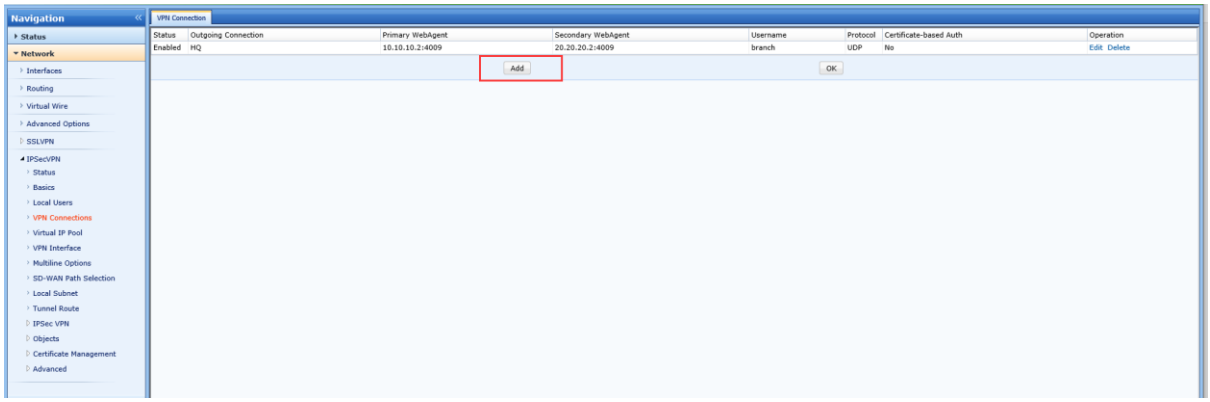


Chapter 3 Configure Branch AF

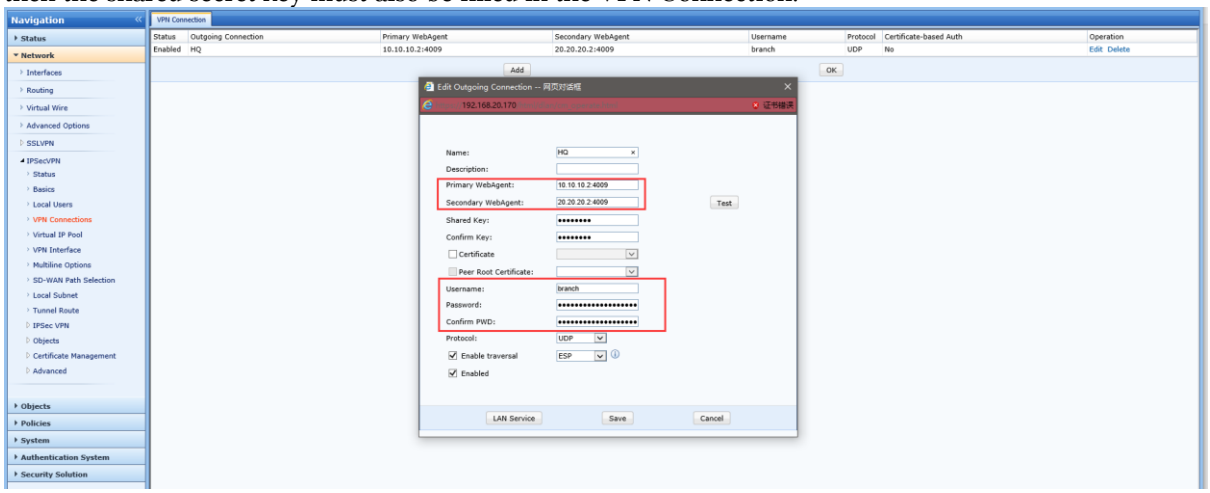
1. Check whether it can communicate with the headquarters device.



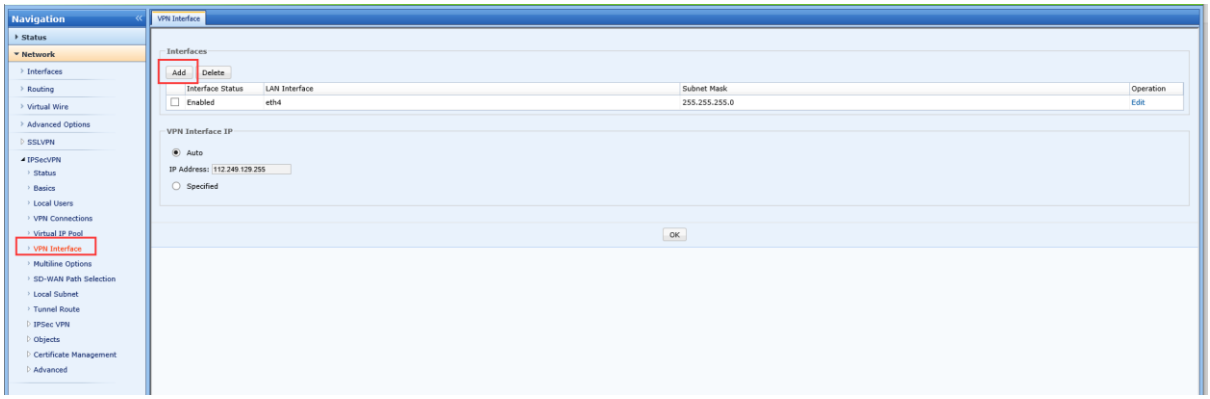
2. Configure VPN Connection.



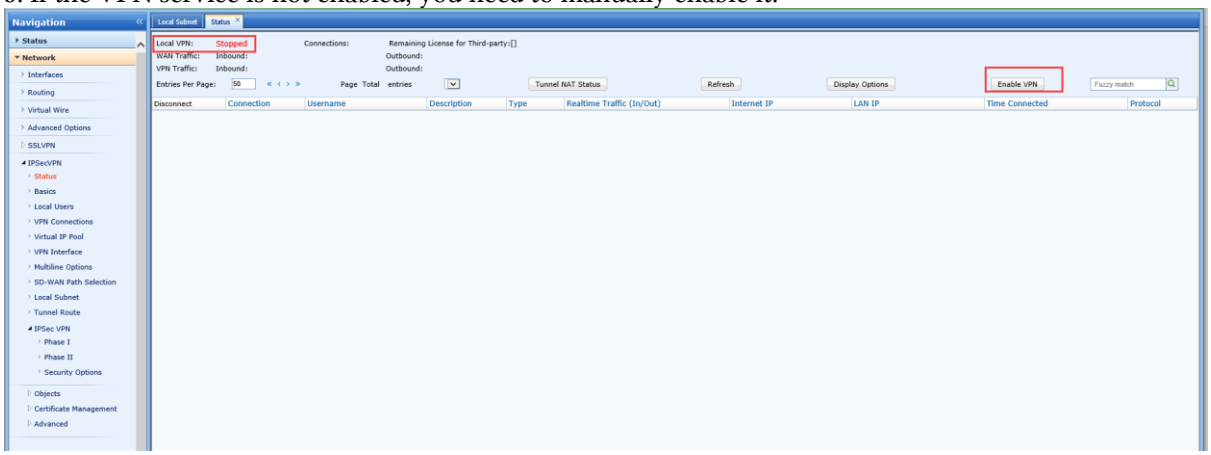
3. Fill in the primary and secondary webagent configured on the HQ device and fill in the port. At the same time, configure the user name and password. If the shared secret key is filled in on the HQ device, then the shared secret key must also be filled in the VPN Connection.



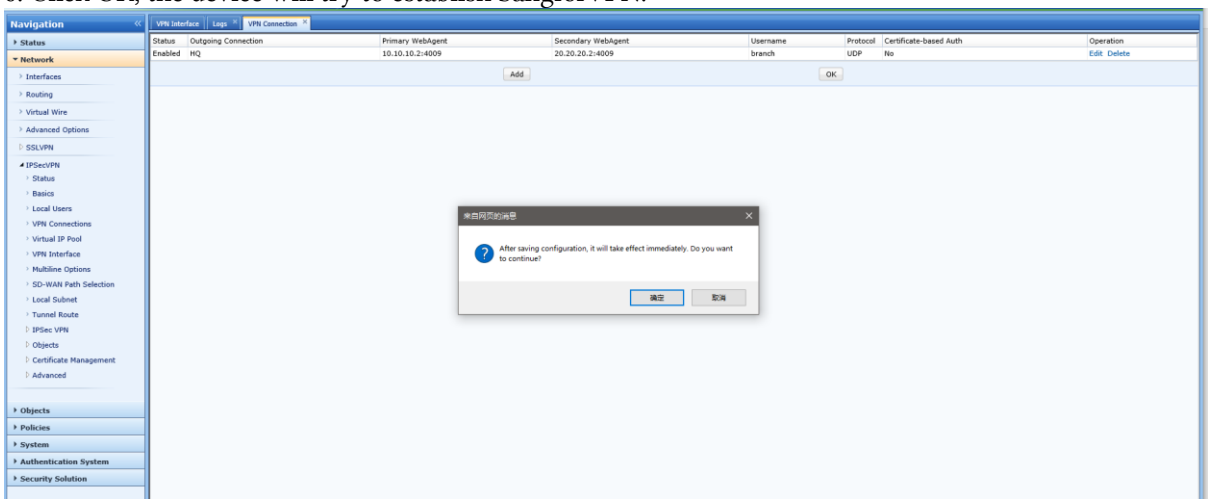
4. Configure the VPN interface, specify the LAN port of the branch device and the network segment directly connected to the LAN port.



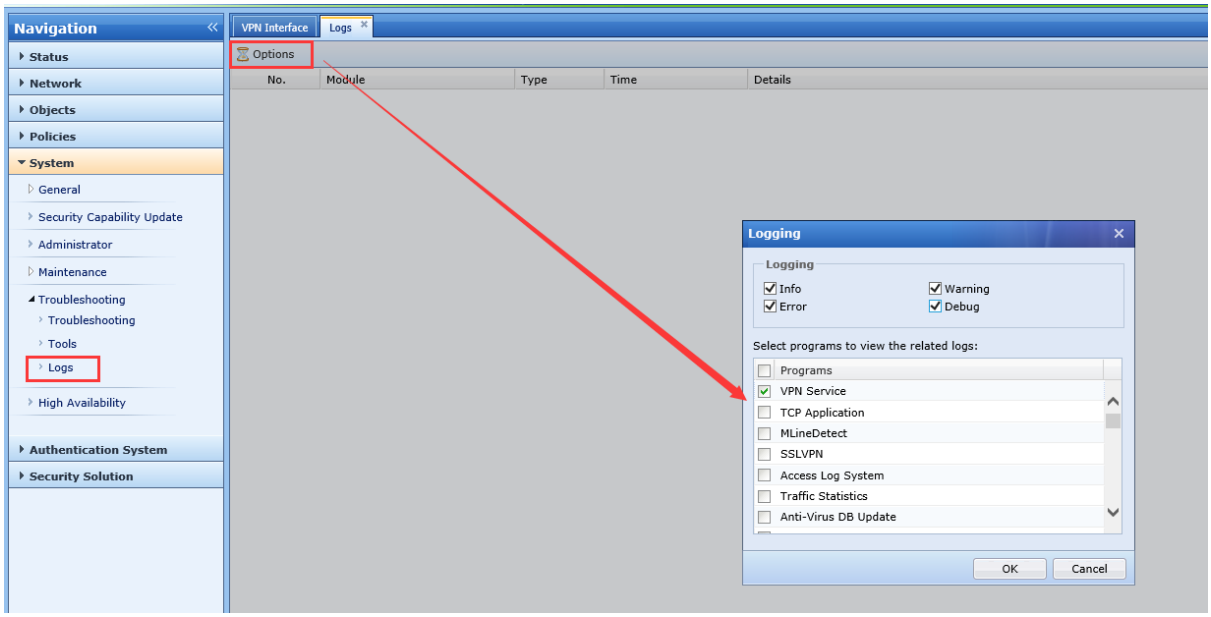
5. If the VPN service is not enabled, you need to manually enable it.

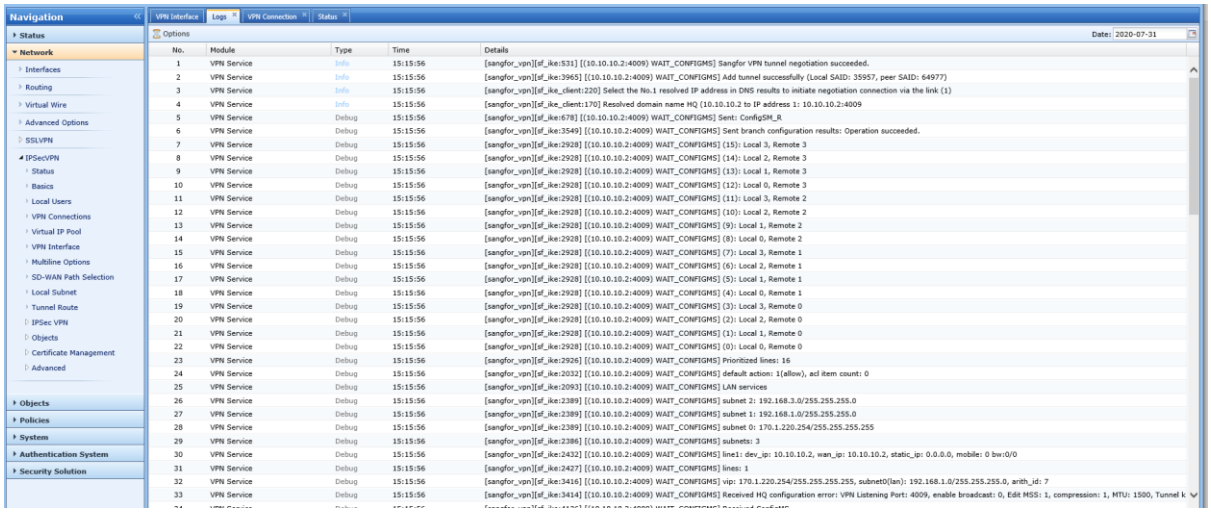


6. Click OK, the device will try to establish SangforVPN.

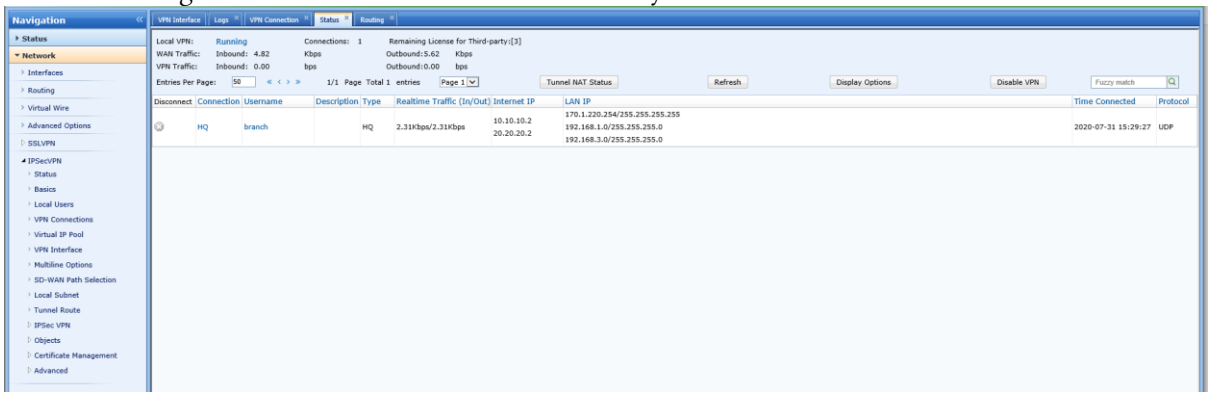


7. Check the system log, check whether there is an error log during the VPN establishment process.





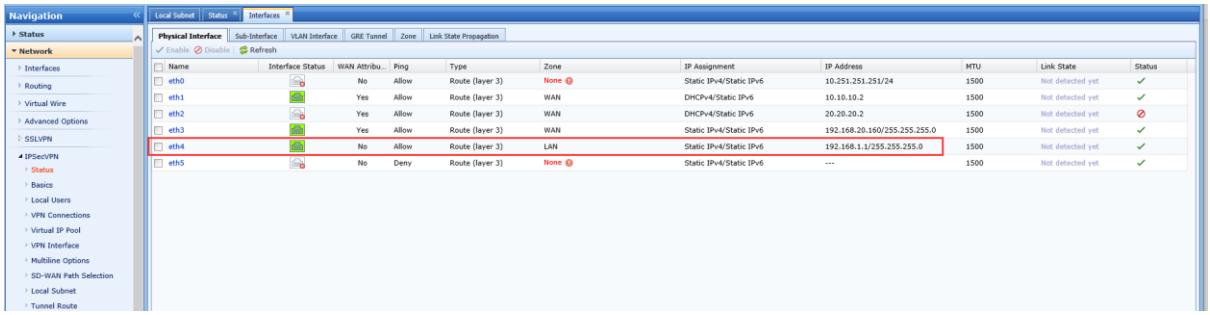
8. Check the status, click Refresh, and check whether there are tunnel related parameters. If there are, it means that SangforVPN has been established successfully.



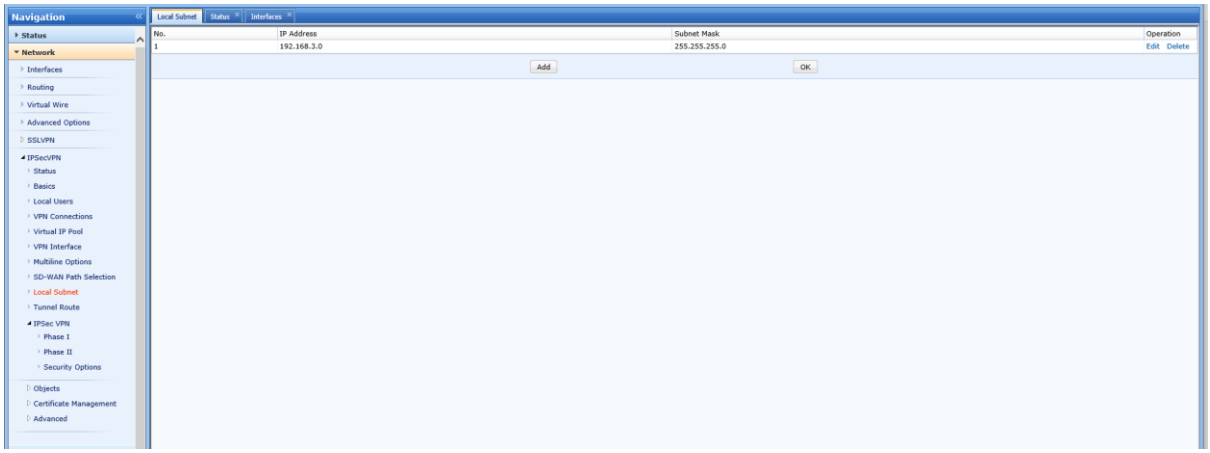
9. If the headquarters and branches are in a three-tier environment, that is, there are other network segments in the LAN area, then the internal network segments need to be published on the headquarters and branches.

HQ:

The LAN area is directly connected to the network segment 192.168.1.0/24. Actually, a three-layer switch is connected below and there is a network segment 192.168.3.0/24.

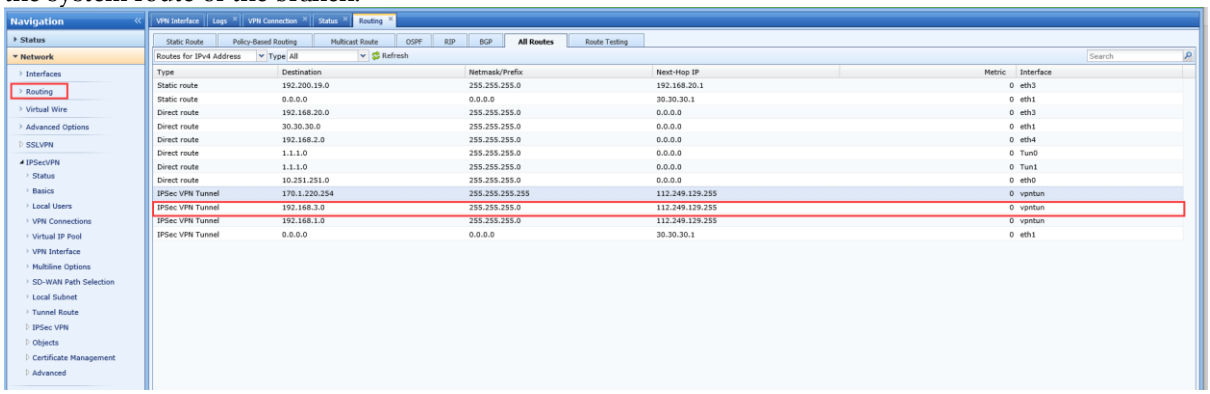


Need to fill in 192.168.3.0/24 in the local subnet



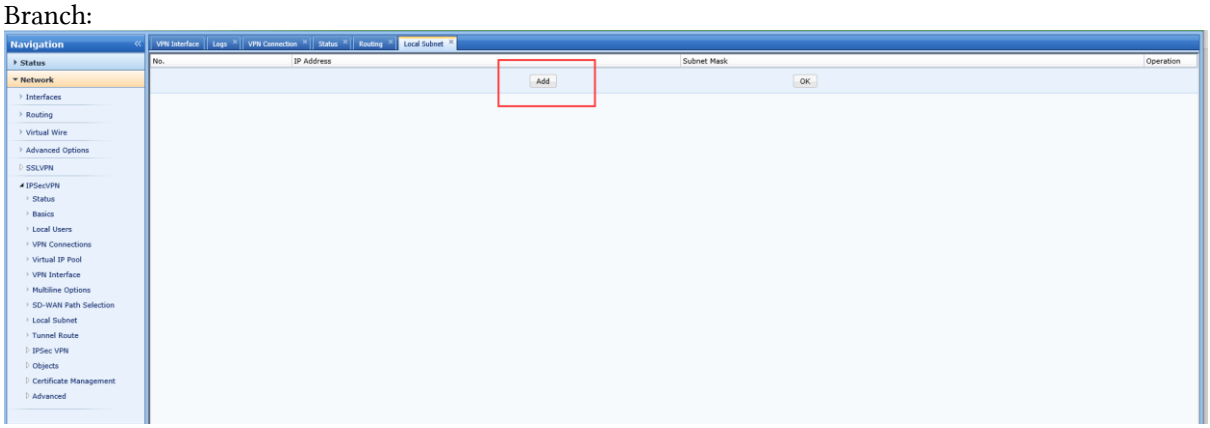
Branch:

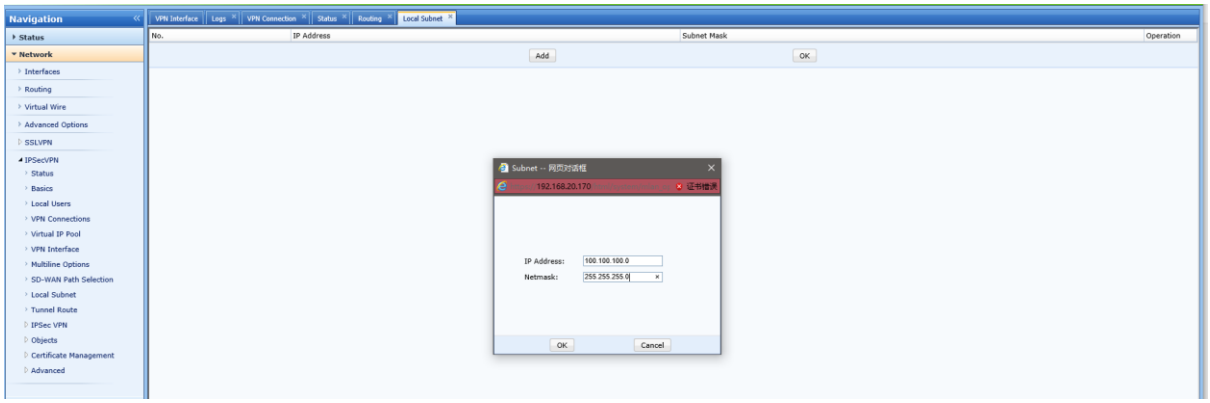
After the headquarters publishes the subnet 192.168.3.0/24, the route of 192.168.3.0/24 can be queried in the system route of the branch.

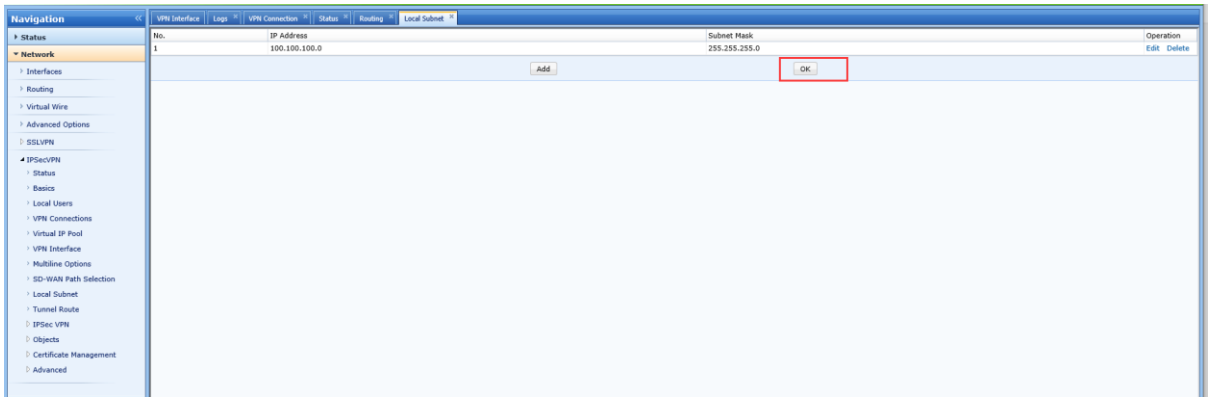


10. If there is an internal network segment in the branch, you need to configure the local subnet to publish the internal network segment.

Branch:

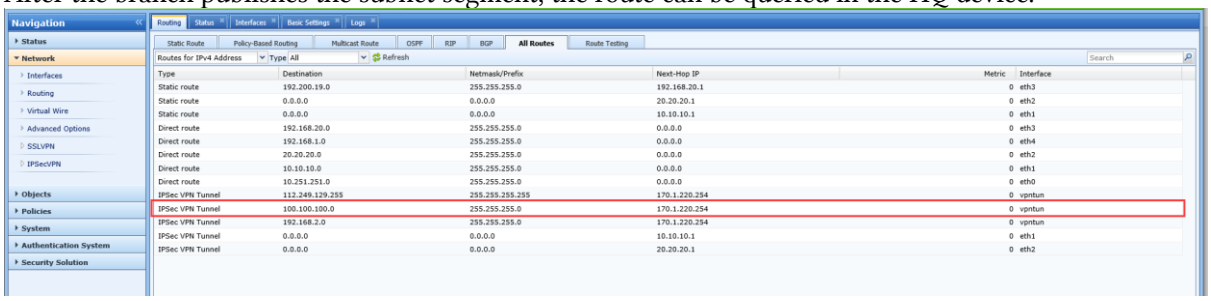






HQ:

After the branch publishes the subnet segment, the route can be queried in the HQ device.



11. At the PC192.168.2.2 of the branch intranet, try to ping the server 192.168.1.3 of the headquarters intranet, and the verification is successful.

```
C:\Users\Sangfor>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::28d4:32aa:17e3:7bc0%11
   IPv4 Address. . . . . . . . . . . : 192.168.2.2
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.2.1

C:\Users\Sangfor>ping 192.168.1.3 -t

Pinging 192.168.1.3 with 32 bytes of data:
Reply from 192.168.1.3: bytes=32 time=2ms TTL=126
Reply from 192.168.1.3: bytes=32 time=1ms TTL=126
```

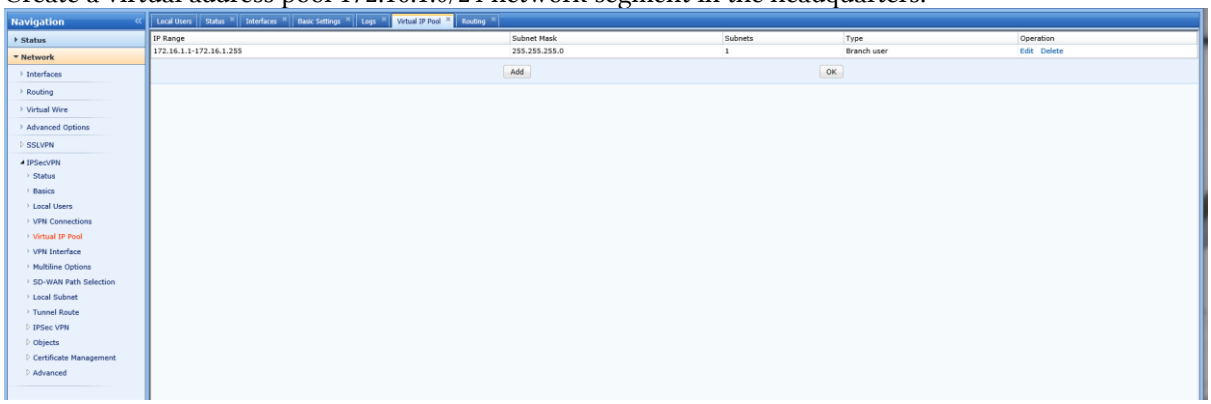
Chapter 4 Advanced Configuration

4.1 Tunnel NAT Scenario

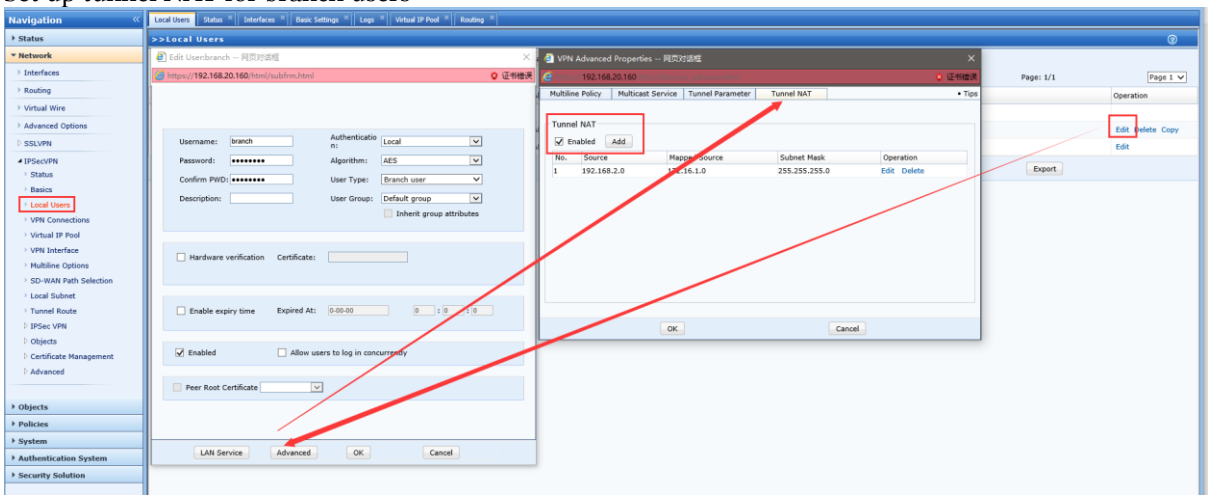
A large number of branches and stores of some customers. In this case, different branches may use the same network segment. For example, the internal networks of Branch1 and Branch2 both have the 192.168.2.0/24 network segment, so when Branch1 and Branch2 access the headquarters resources Cause an address conflict. For this use scenario, it is recommended to use the tunnel NAT function. Tunnel NAT is to convert the source IP of the request from the branch with the address conflict to the headquarters to other network segments, so that normal communication can be achieved.

1. For example, convert the source network segment 192.168.2.0/24 of the branch of Branch1 to the headquarters of 172.16.1.0/24, so that Branch1 can access the headquarters and Branch2 can directly access the services of the headquarters through the VPN tunnel.

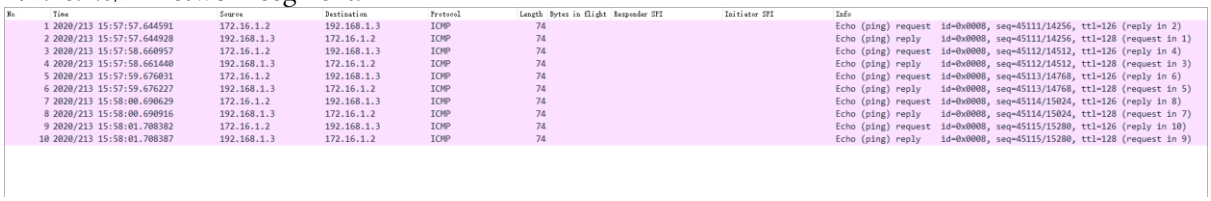
Create a virtual address pool 172.16.1.0/24 network segment in the headquarters.



Set up tunnel NAT for branch users

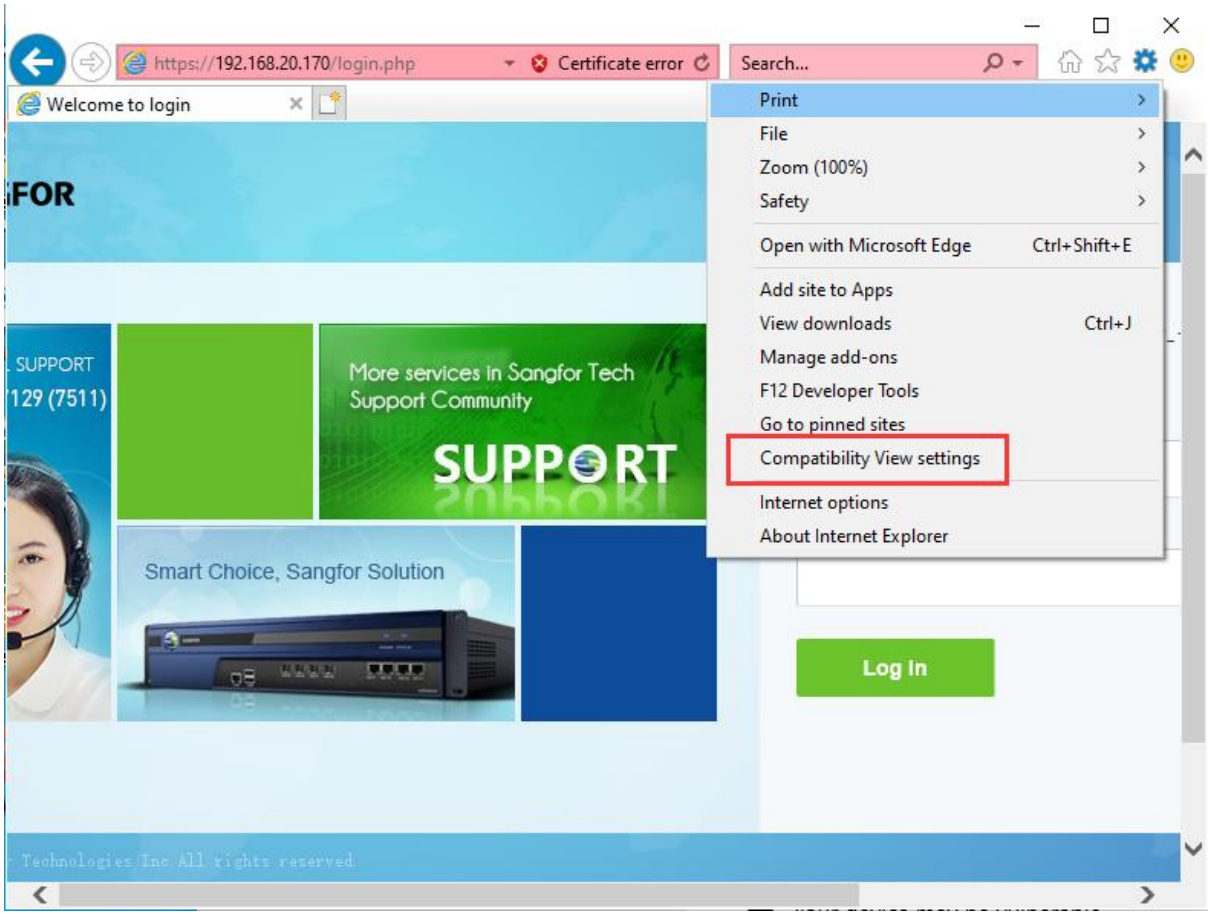


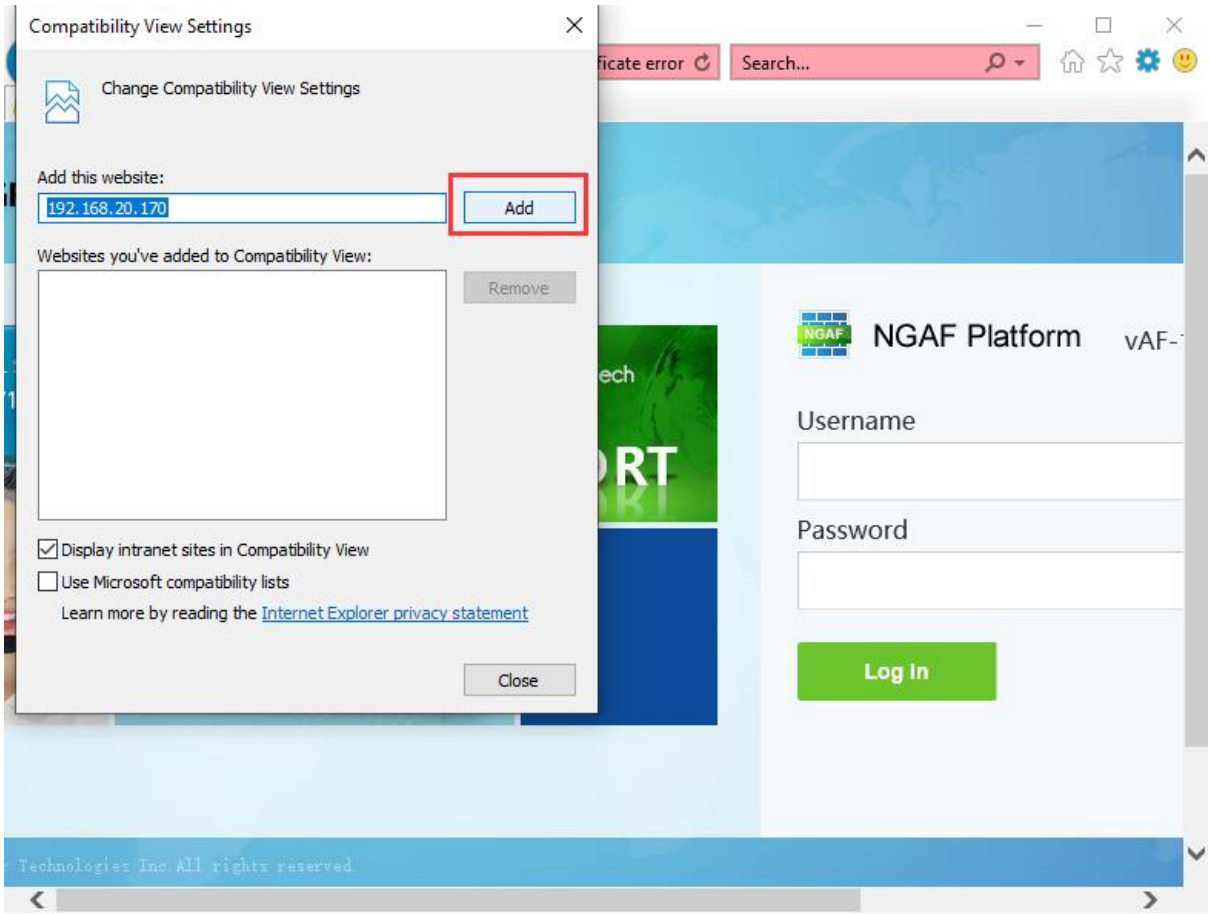
2. In the PC under the headquarters, you can see that the source IP has been converted to the IP of the 172.16.1.0/24 network segment.



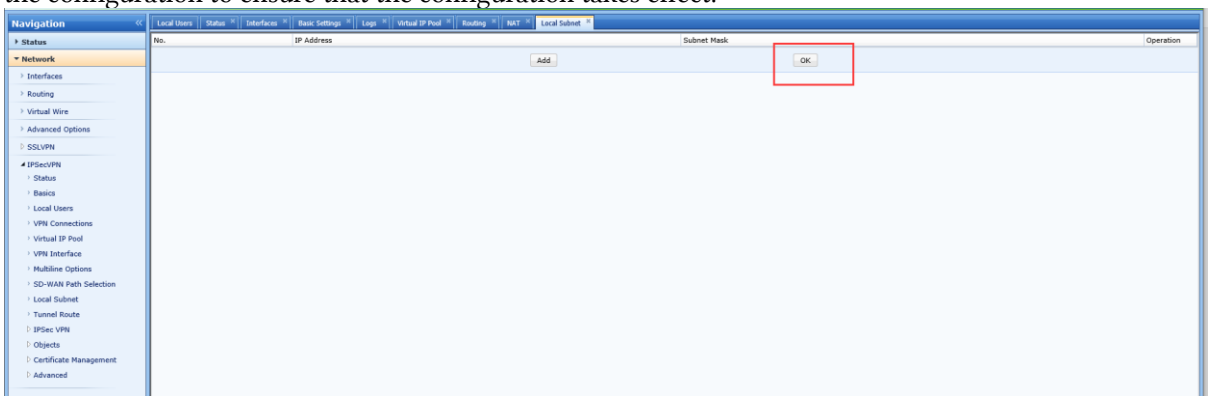
Chapter 5 Precaution

1. It is recommended to use IE browser to configure VPN related functions and enable the browser compatibility adaptation function.

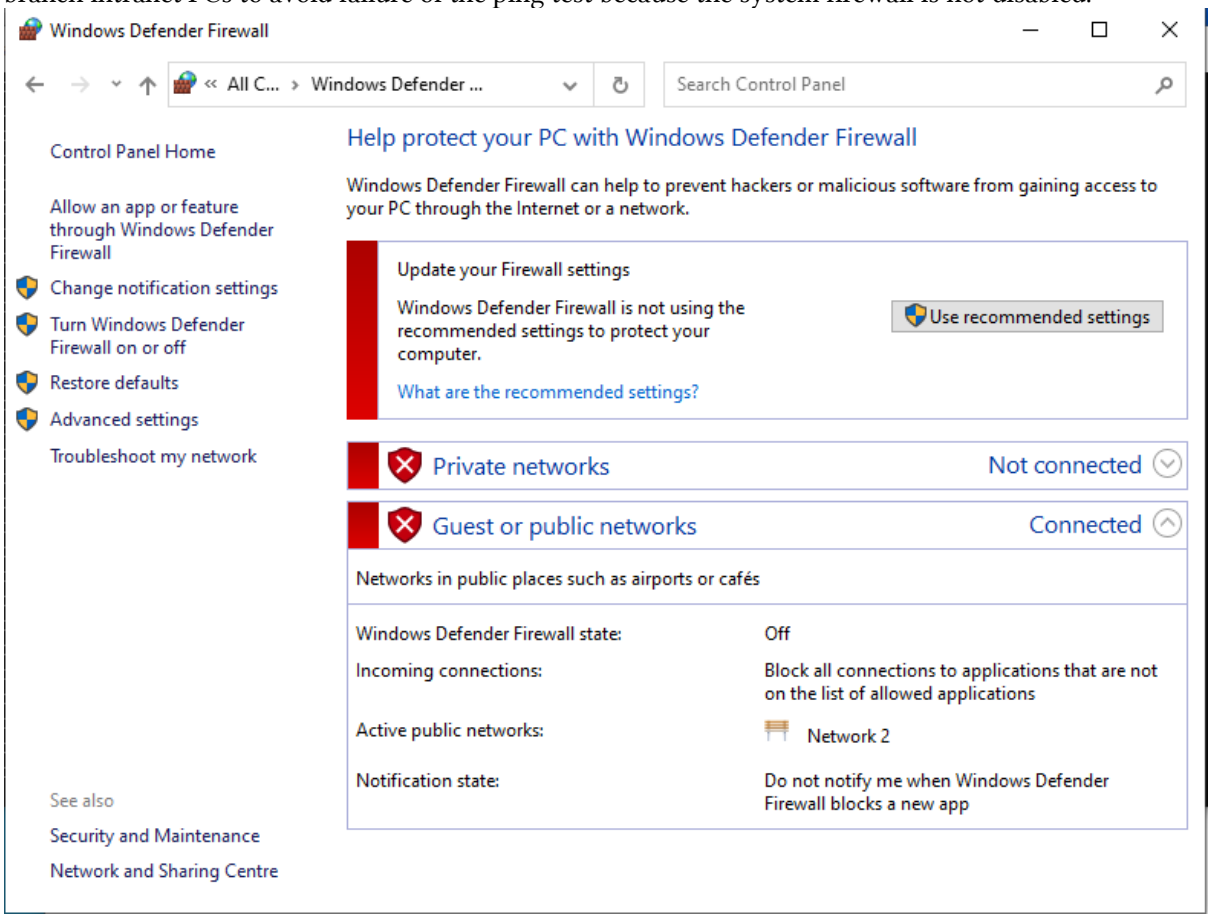

https://192.168.20.170/login.php
Certificate error
Search...
Welcome to login
Print
File
Zoom (100%)
Safety
Open with Microsoft Edge Ctrl+Shift+E
Add site to Apps
View downloads Ctrl+J
Manage add-ons
F12 Developer Tools
Go to pinned sites
Compatibility View settings
Internet options
About Internet Explorer
More services in Sangfor Tech Support Community
SUPPORT
Smart Choice, Sangfor Solution
Log In

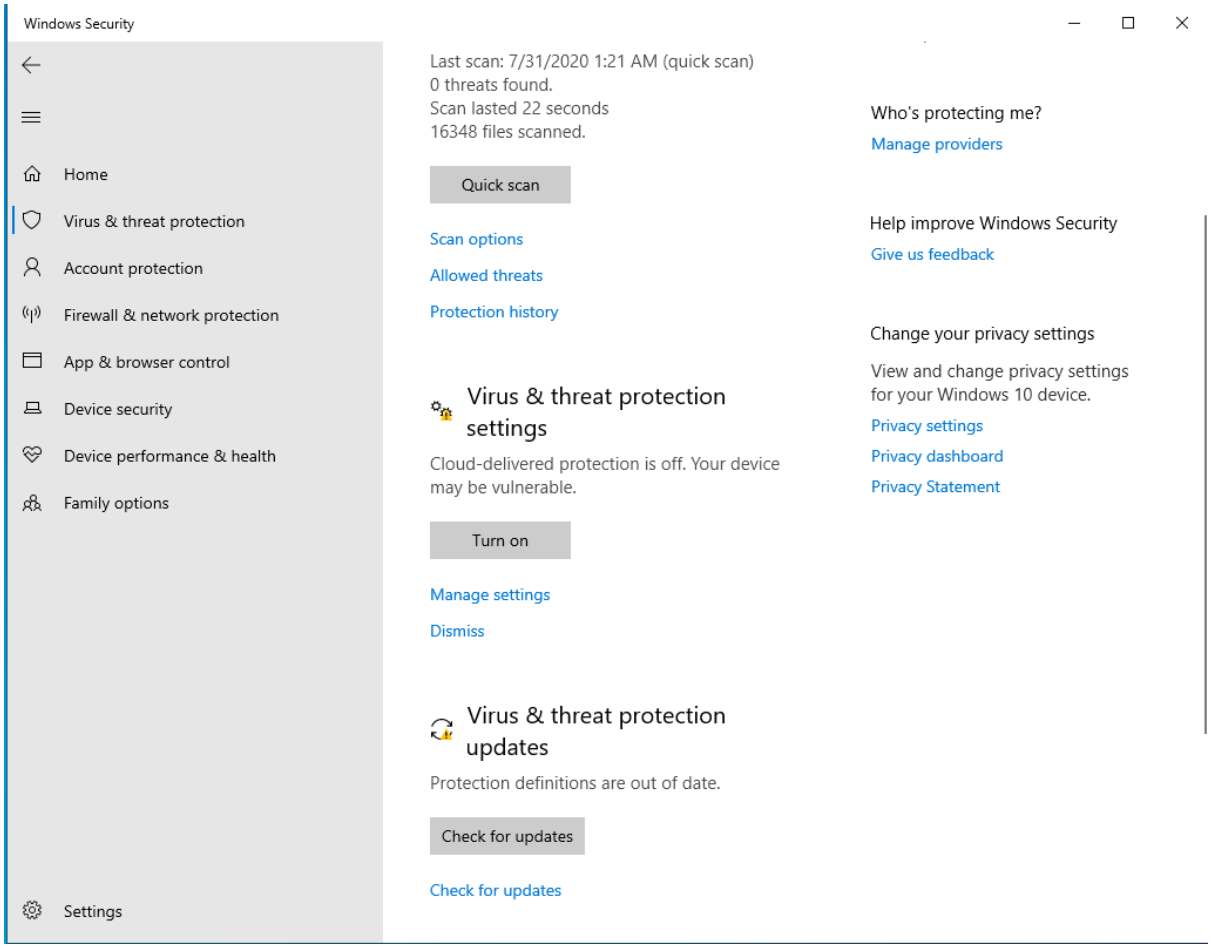

Compatibility View Settings
Change Compatibility View Settings
Add this website:
192.168.20.170
Add
Websites you've added to Compatibility View:
Remove
Display intranet sites in Compatibility View
Use Microsoft compatibility lists
Learn more by reading the Internet Explorer privacy statement
Close
NGAF Platform
Username
Password
Log In

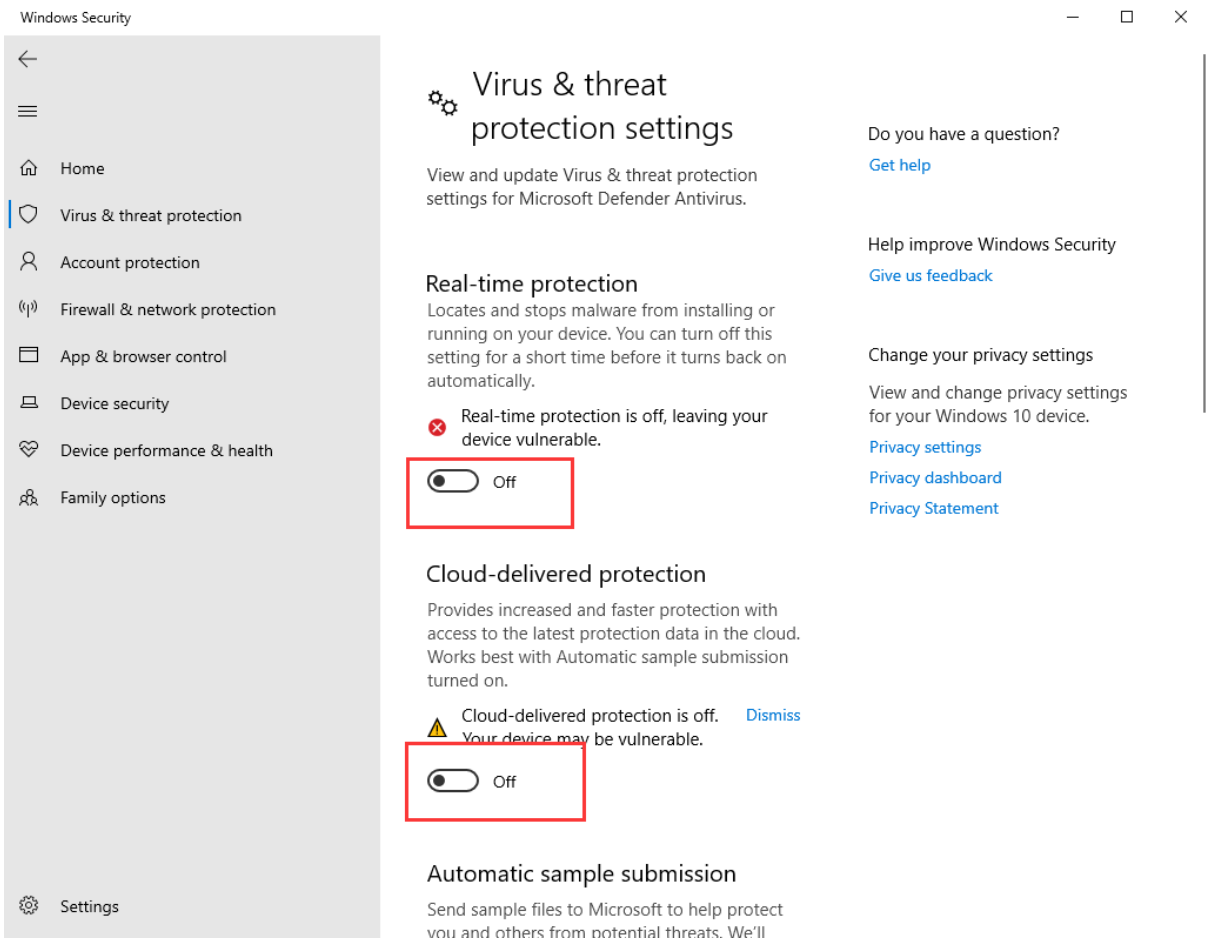
2. The VPN configuration has a large number of "OK" options, please be sure to click "OK" after finishing the configuration to ensure that the configuration takes effect.



3. When testing connectivity, it is recommended to turn off the system firewall of the headquarters and branch intranet PCs to avoid failure of the ping test because the system firewall is not disabled.




Windows Security
Home
Virus & threat protection
Account protection
Firewall & network protection
App & browser control
Device security
Device performance & health
Family options
Settings
Last scan: 7/31/2020 1:21 AM (quick scan)
0 threats found.
Scan lasted 22 seconds
16348 files scanned.
Quick scan
Scan options
Allowed threats
Protection history
Virus & threat protection settings
Cloud-delivered protection is off. Your device may be vulnerable.
Turn on
Manage settings
Dismiss
Virus & threat protection updates
Protection definitions are out of date.
Check for updates
Check for updates
Who's protecting me?
Manage providers
Help improve Windows Security
Give us feedback
Change your privacy settings
View and change privacy settings for your Windows 10 device.
Privacy settings
Privacy dashboard
Privacy Statement



4. Troubleshooting can be turned on for the test IP to avoid the interception of related data packets due to the NGAF policy configuration.