SANGFOR

NGAF

Best Practices for Scenarios_Establish IPsecVPN

Version 8.0.17

Change Log

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

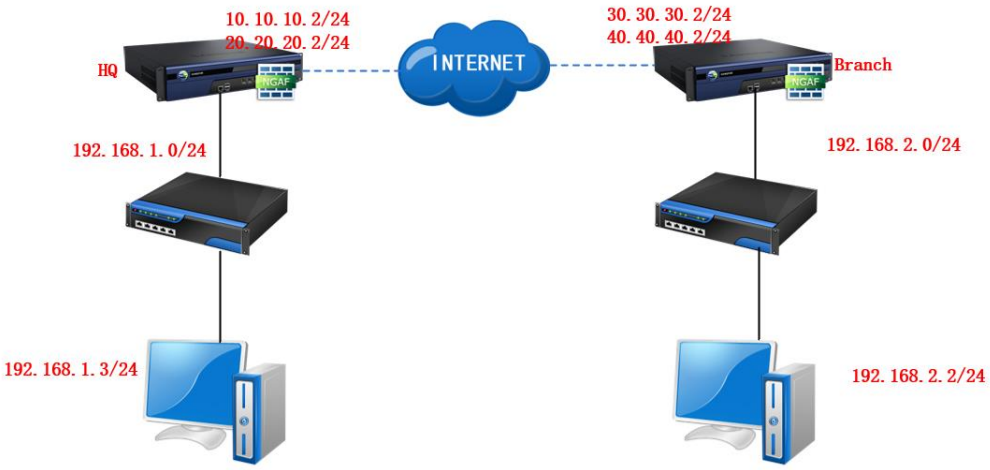
CONTENT

Chapter 1 Scenario

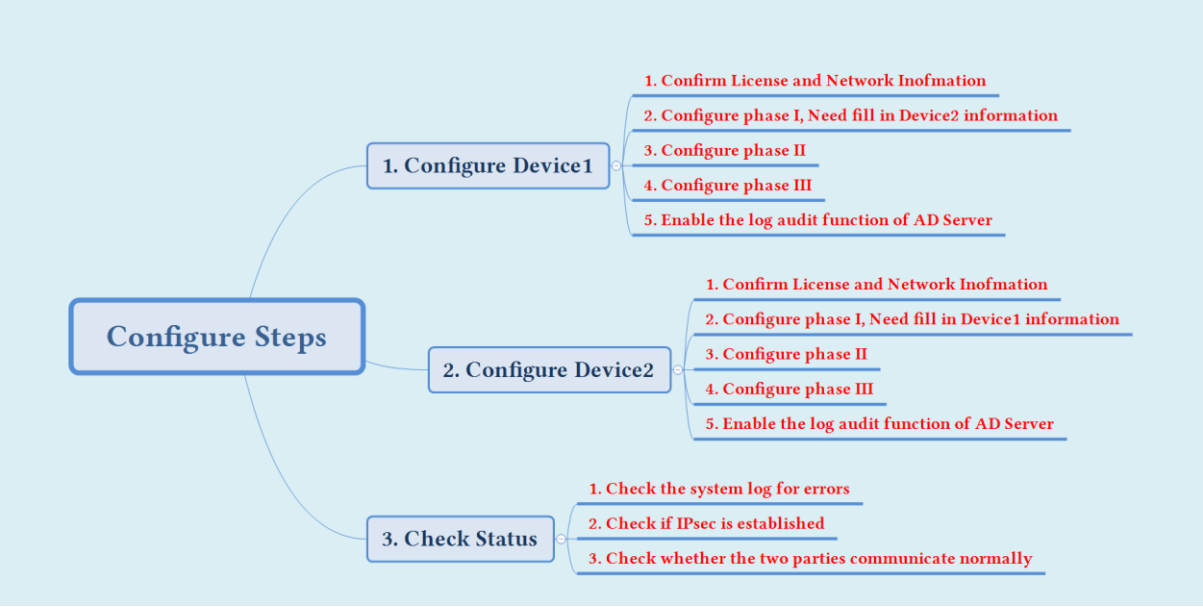
XX National Postal Company has branches and stores in various provinces and cities. Now the customer's network requirements allow branches and stores to access the web services of the headquarters, while ensuring that data transmission is secure and encrypted. The customer's business system is mainly located in the headquarters, and has long been faced with hacker attacks and various security issues. The customer has been using a certain manufacturer's firewall device for many years, but cannot defend against hacker attacks. In order to obtain better security protection capabilities, the customer decided to replace the original security device in the headquarters with Sangfor device. However, there are many customer branches, and it is difficult to replace all branch equipment at one time without affecting the network. Therefore, the branch will not replace the original device temporarily. Because the branch device is not a Sangfor device, so it can only establish a standard IPsecVPN solution and cannot use SangforVPN.

About IPsecVPN: Standard IPSEC VPN connection can only be used in main mode when both ends have a fixed public IP and no NAT. It is recommended to use aggressive mode connection when either party has a dynamic IP address or NAT.

The current environment branches and headquarters are static IP, so choose to use the main mode. This article takes NGAF as an example in both the branch and the headquarters.

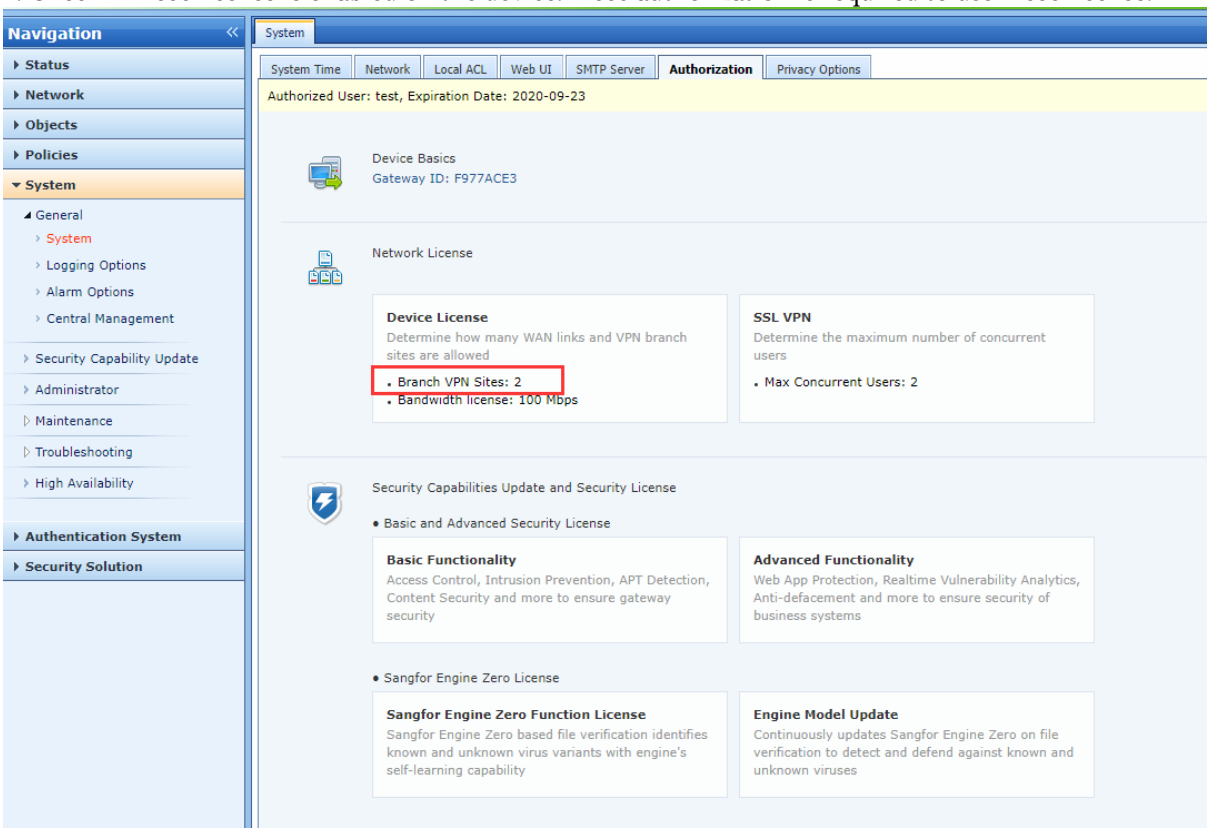


1.1 Configure Steps

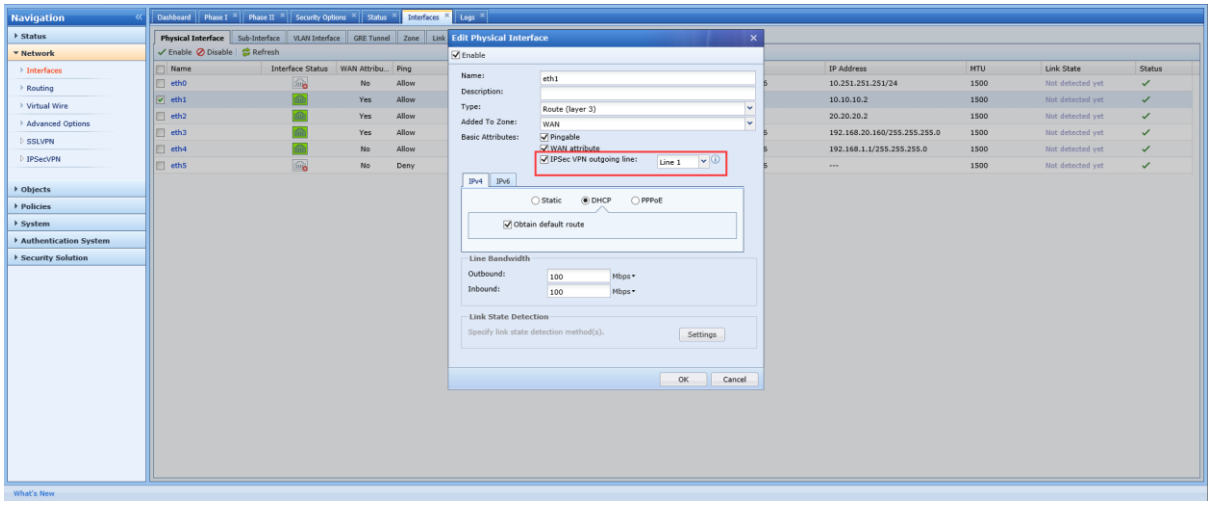


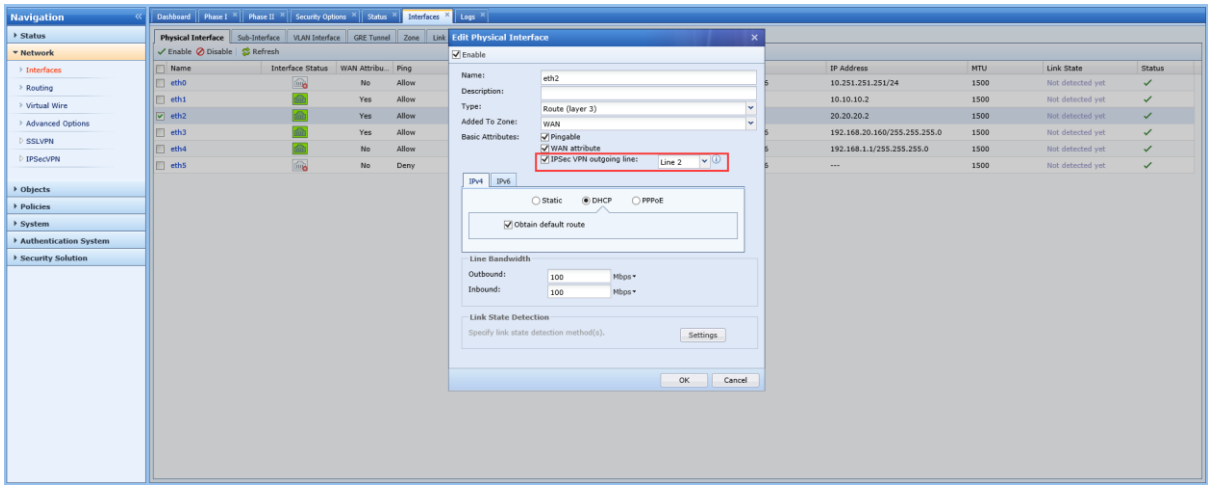
Chapter 2 Configure HQ Device A

1. Check if IPsec license is enabled on the device. IPsec authorization is required to use IPsec license.

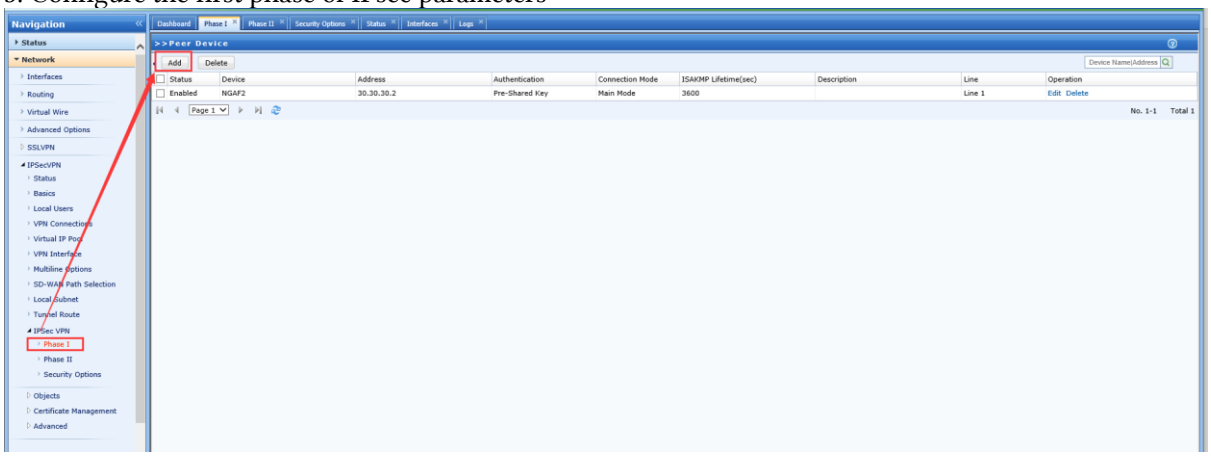


2. Choose a WAN port as the IPsecVPN outgoing interface and designate it as a line.

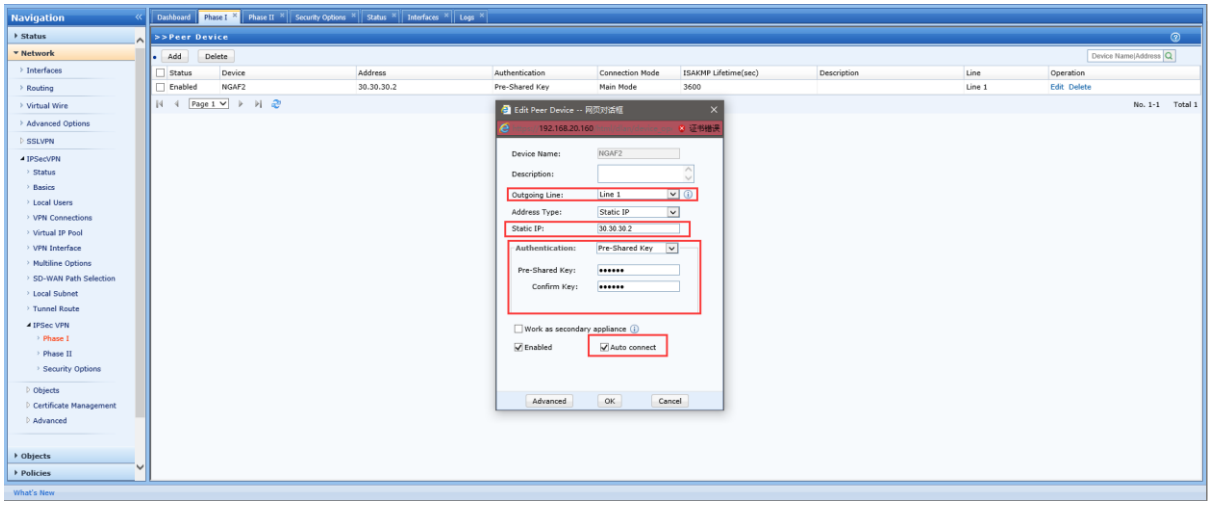




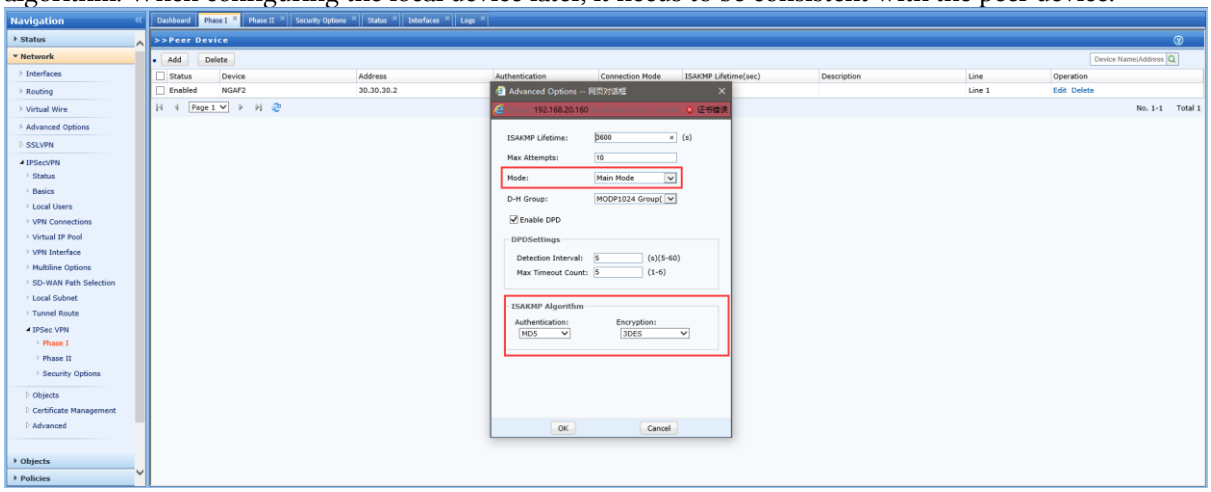
3. Configure the first phase of IPsec parameters



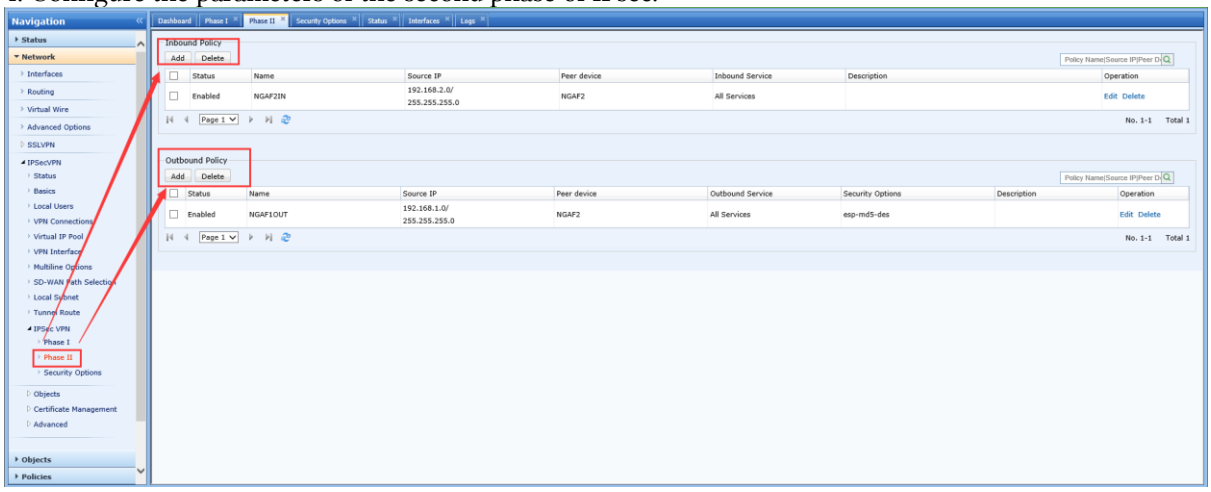
Need to select the exit line, for example, line 1 as the main line, here select line 1 as the line established by IPsecVPN. Fill in the IP of the branch device and the shared key; name the peer device, for example, name the peer device NGAF2.



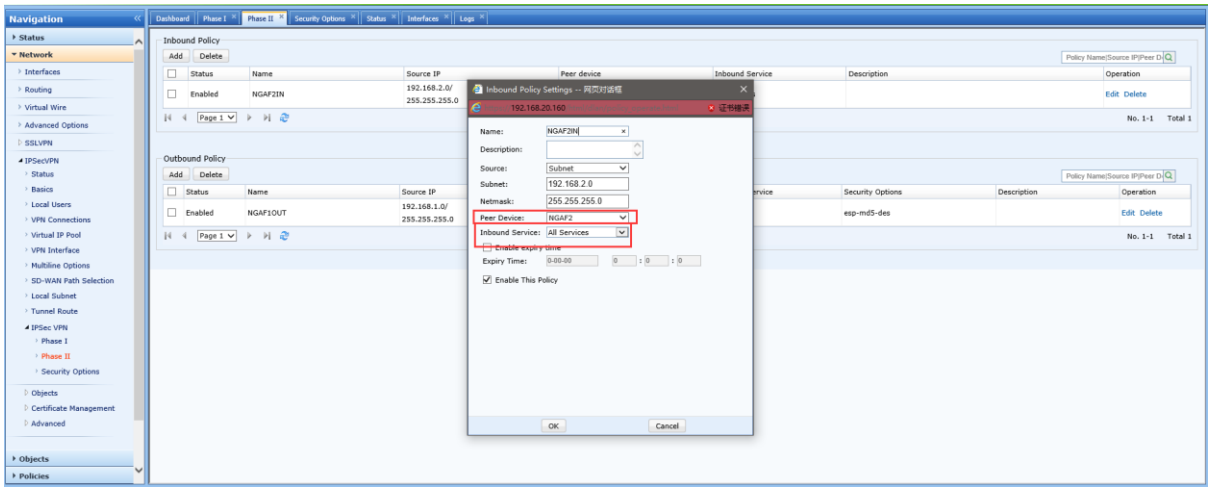
Click "Advanced", select the main mode, and confirm the authentication algorithm and encryption algorithm. When configuring the local device later, it needs to be consistent with the peer device.



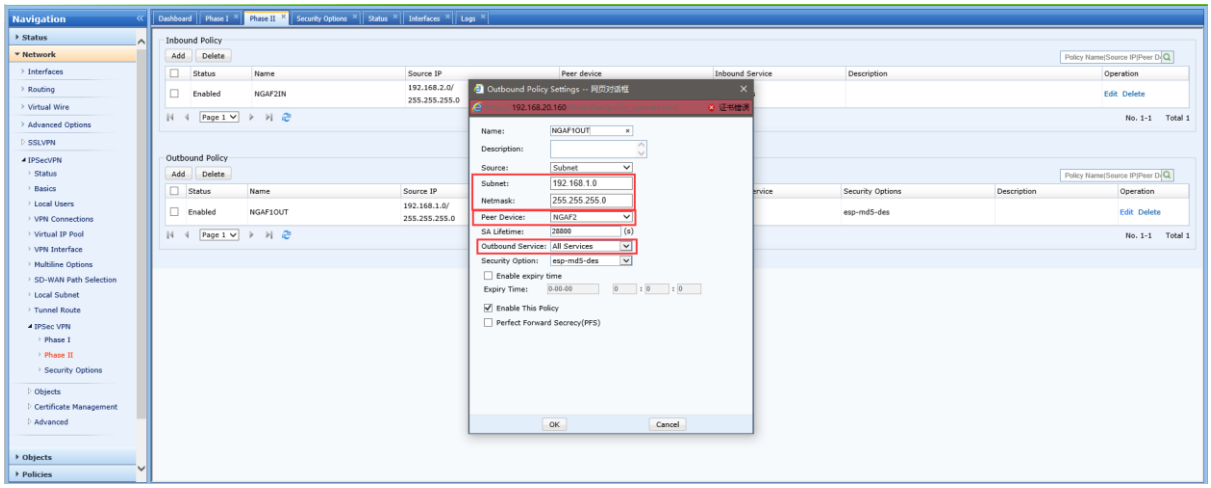
4. Configure the parameters of the second phase of IPsec.



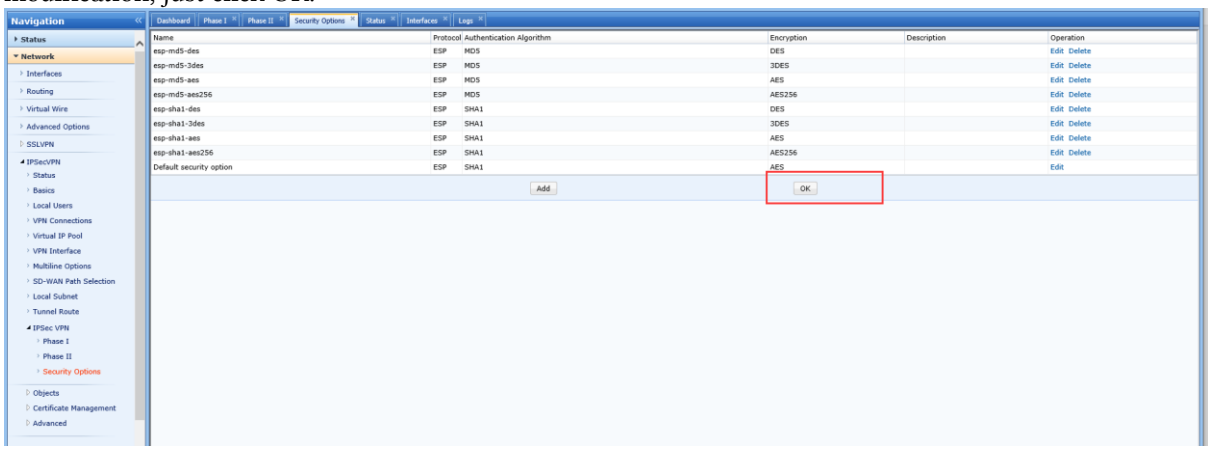
The Inbound Policy fills in the intranet network segment of the branch, which means that compared to the current device, which network segment of the branch data packets need to transport to the VPN tunnel of the device so that the current device can establish the route to return packet, and the peer device selects the NGAF2 device we named in the first stage. Inbound Service usually needs to be selected as "All Services", and the default option is "All TCP Services". If the default option is used, the ping test will fail for only TCP Services are allowed to enter the VPN tunnel.



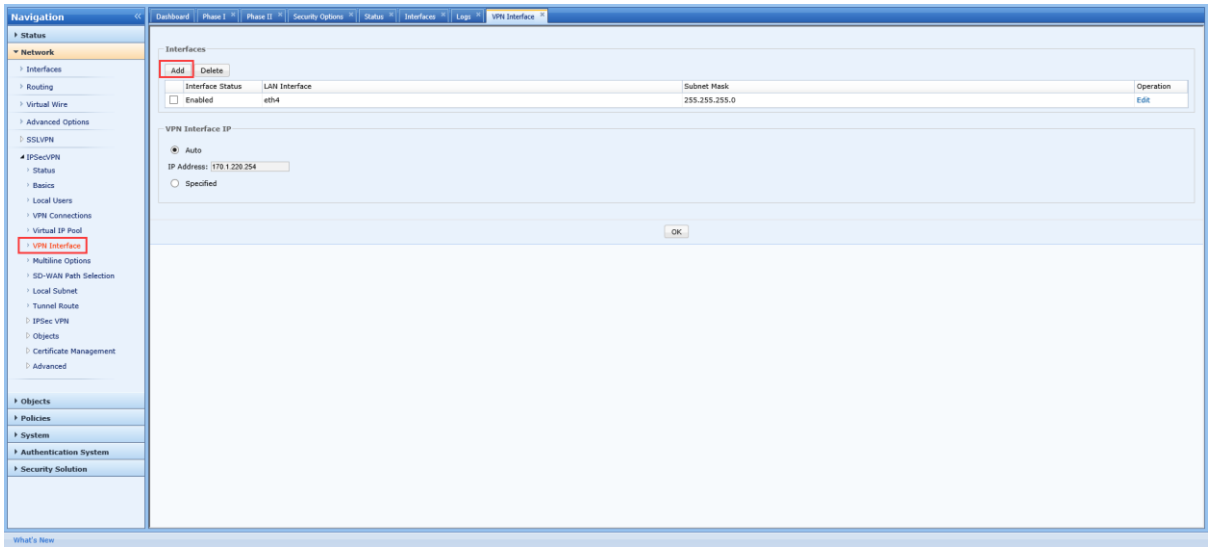
Outbound Policy means to advertise the internal network segment of the current device so that the peer device can establish route to return packets. Outbound Service usually needs to be selected as "All Services", and the default option is "All TCP Services". If the default option is used, the ping test will fail for UDP traffic cannot enter the VPN tunnel.



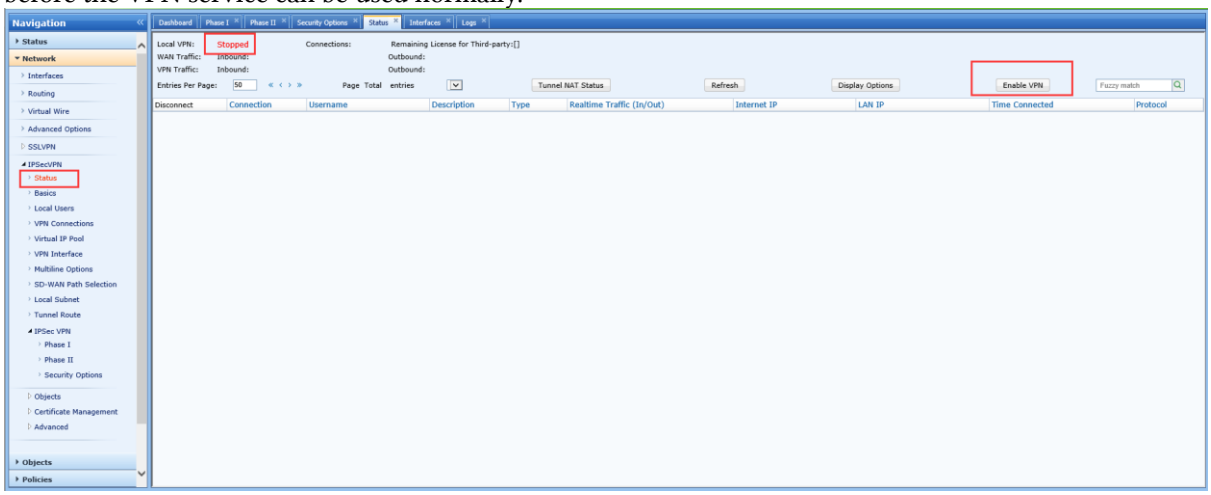
5. Configure the third stage of IPsec. The third stage is usually the encryption algorithm, usually without modification, just click OK.



6. Configure the internal network interface and network segment.

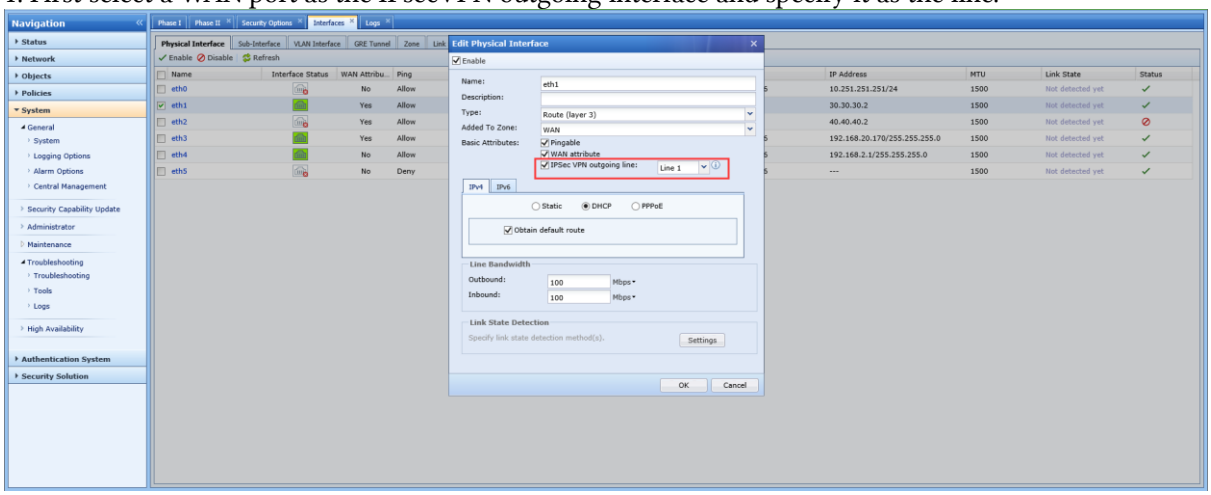


7. Enable the VPN service. The VPN service is turned off by default. You need to manually enable it before the VPN service can be used normally.

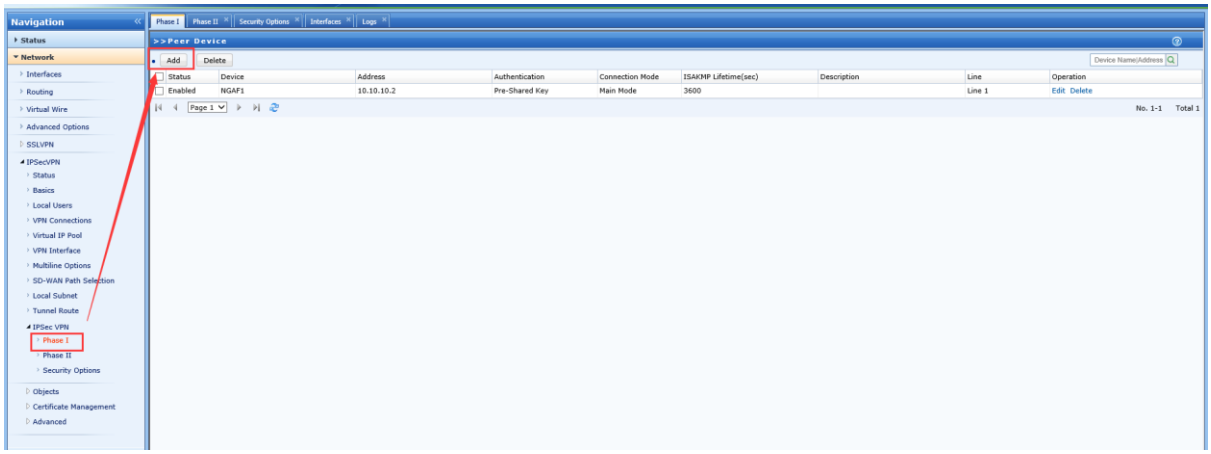


Chapter 3 Configure Branch Device B

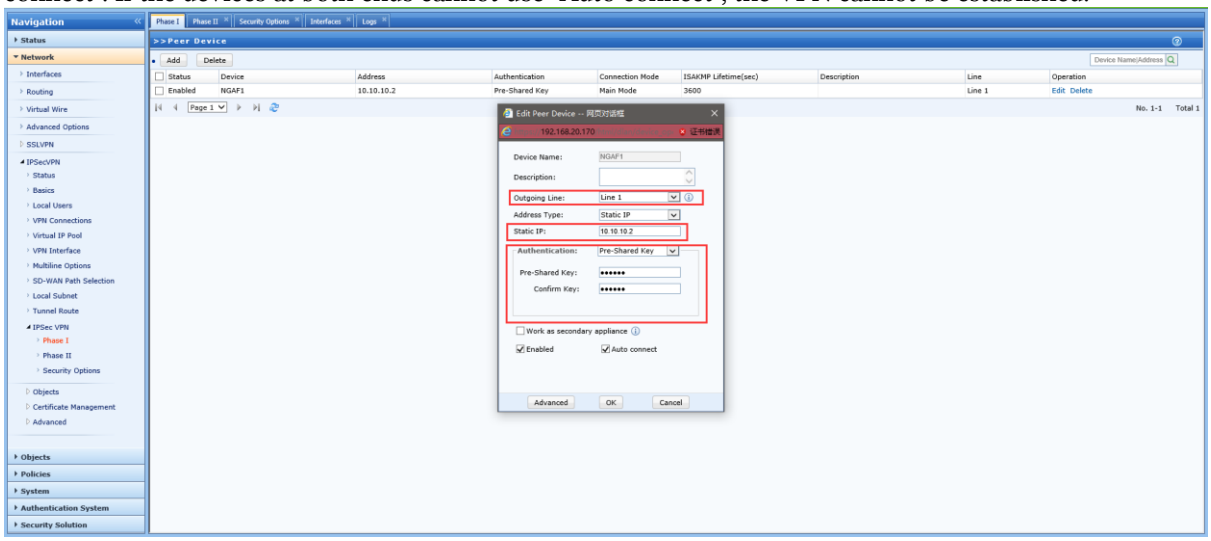
1. First select a WAN port as the IPsecVPN outgoing interface and specify it as the line.



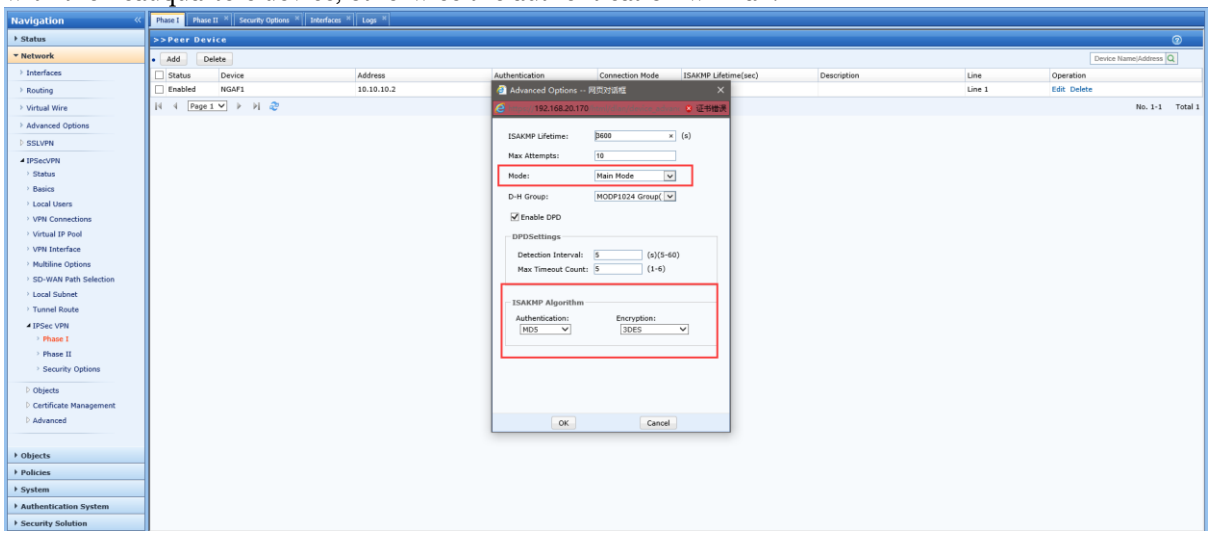
2. Configure the first phase of IPsec parameters.



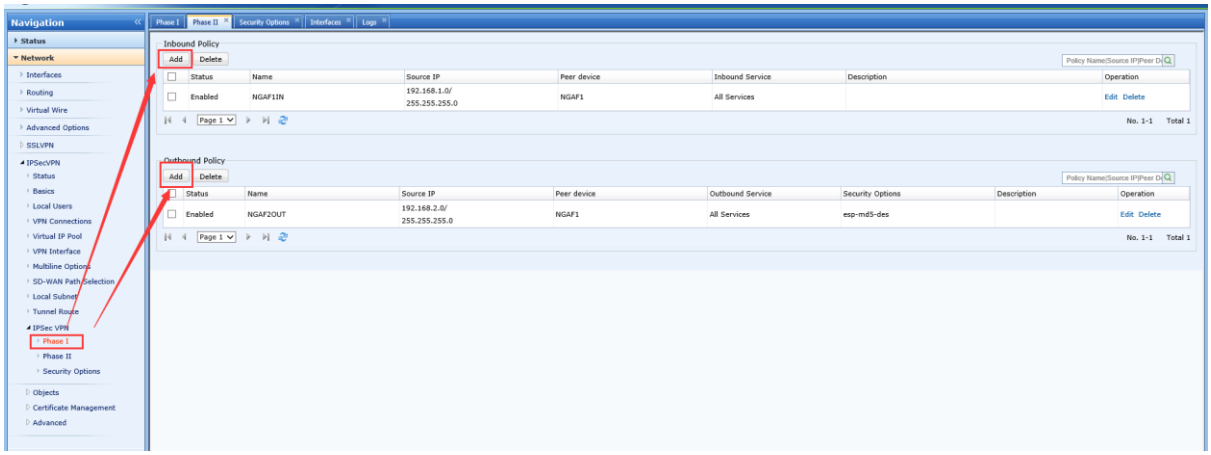
The configuration parameters include the IP and shared key of the headquarters. The shared key must be consistent with the shared key configured on the headquarters device. It should be noted that you generally need to select "Auto connect". At least one of the devices at both ends needs to enable "Auto connect". If the devices at both ends cannot use "Auto connect", the VPN cannot be established.



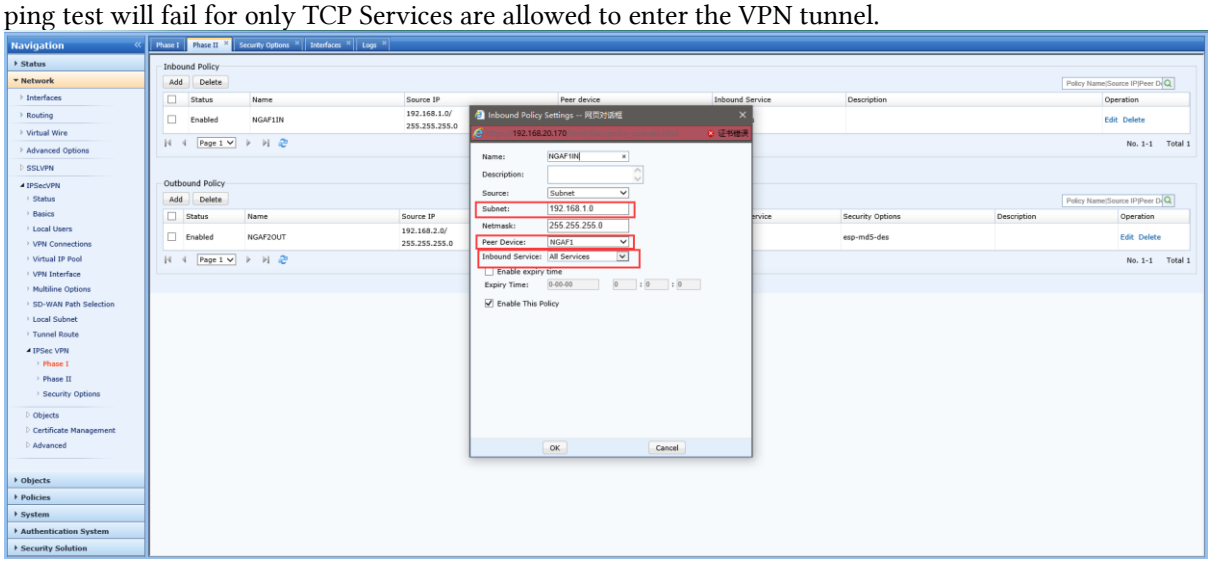
The mode, authentication algorithm, and encryption algorithm of the branch device must be consistent with the headquarters device, otherwise the authentication will fail.



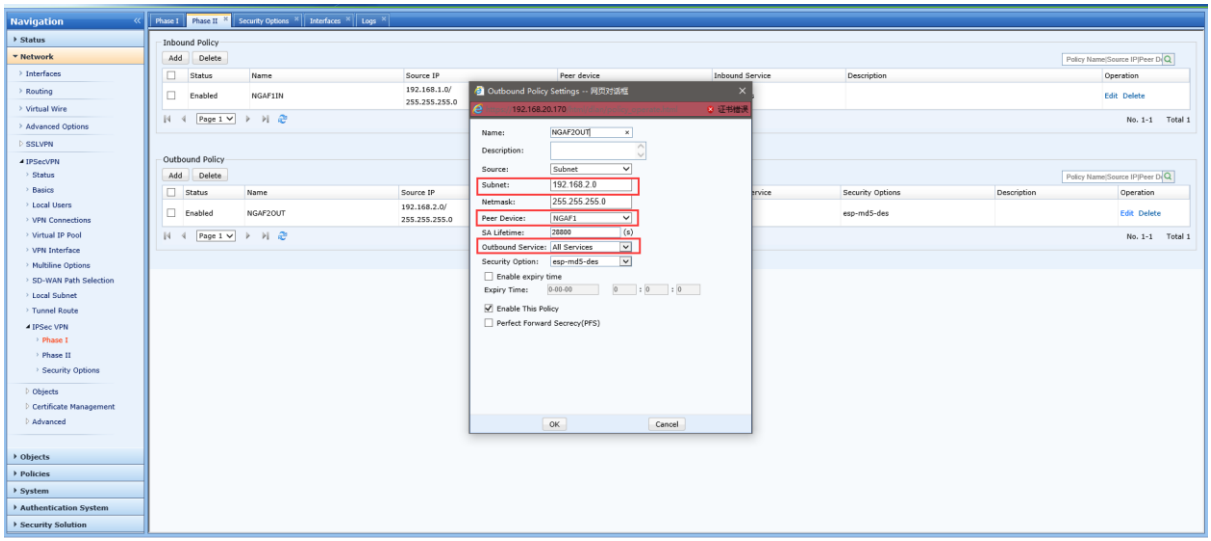
3. Configure IPsec Phase 2 parameters.



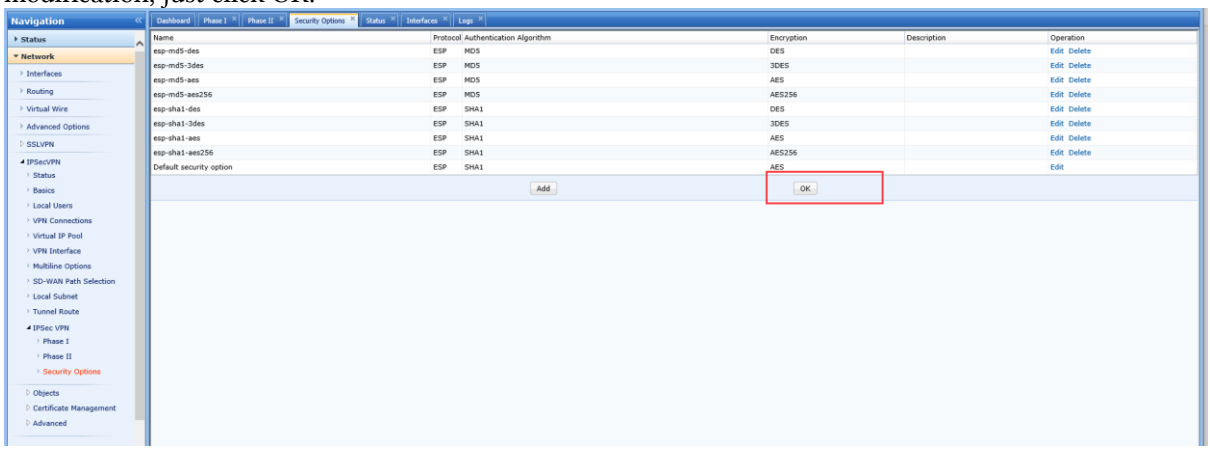
The Inbound Policy fills in the intranet network segment of the branch, which means that compared to the current device, which network segment of the branch data packets need to transport to the VPN tunnel of the device so that the current device can establish the route to return packet, and the peer device selects the NGAF1 device we named in the first stage. Inbound Service usually needs to be selected as "All Services", and the default option is "All TCP Services". If the default option is used, the ping test will fail for only TCP Services are allowed to enter the VPN tunnel.



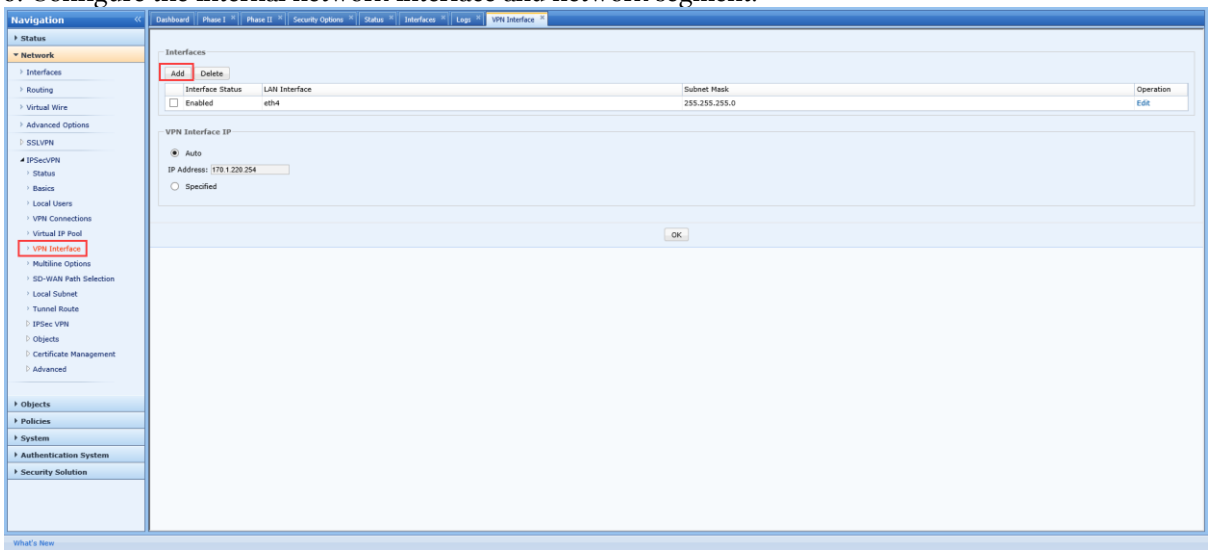
Outbound Policy means to advertise the internal network segment of the current device so that the peer device can establish route to return packets. Outbound Service usually needs to be selected as "All Services", and the default option is "All TCP Services". If the default option is used, the ping test will fail for UDP traffic cannot enter the VPN tunnel.



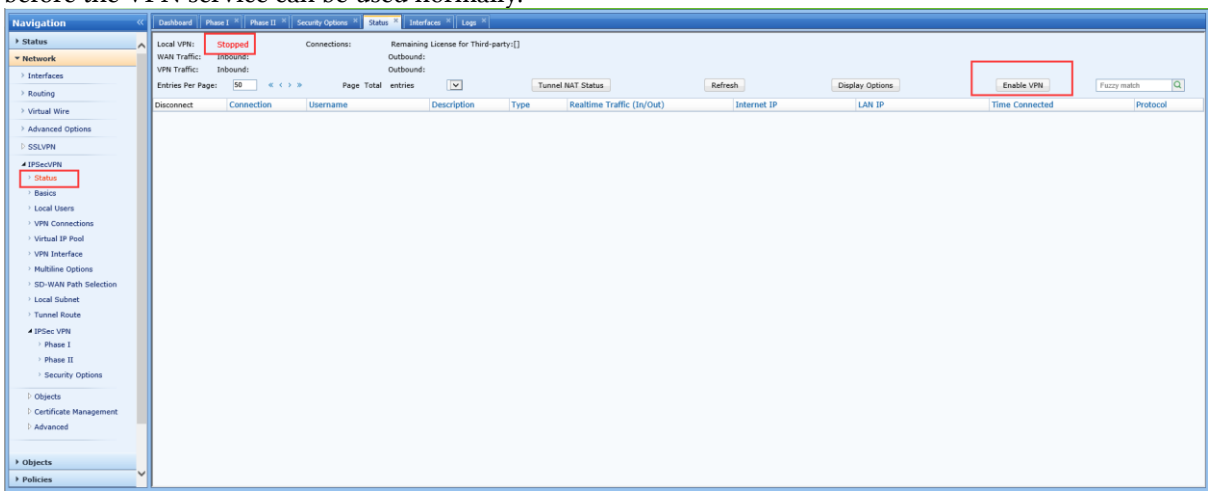
4. Configure the third stage of IPsec. The third stage is usually the encryption algorithm, usually without modification, just click OK.



5. Configure the internal network interface and network segment.

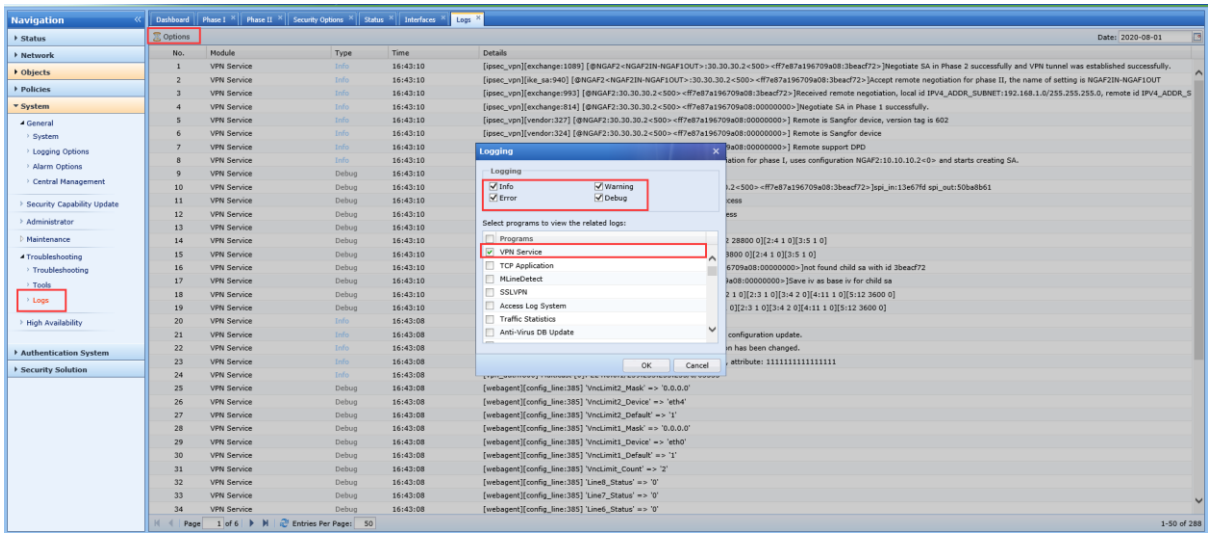


6. Enable the VPN service. The VPN service is turned off by default. You need to manually enable it before the VPN service can be used normally.



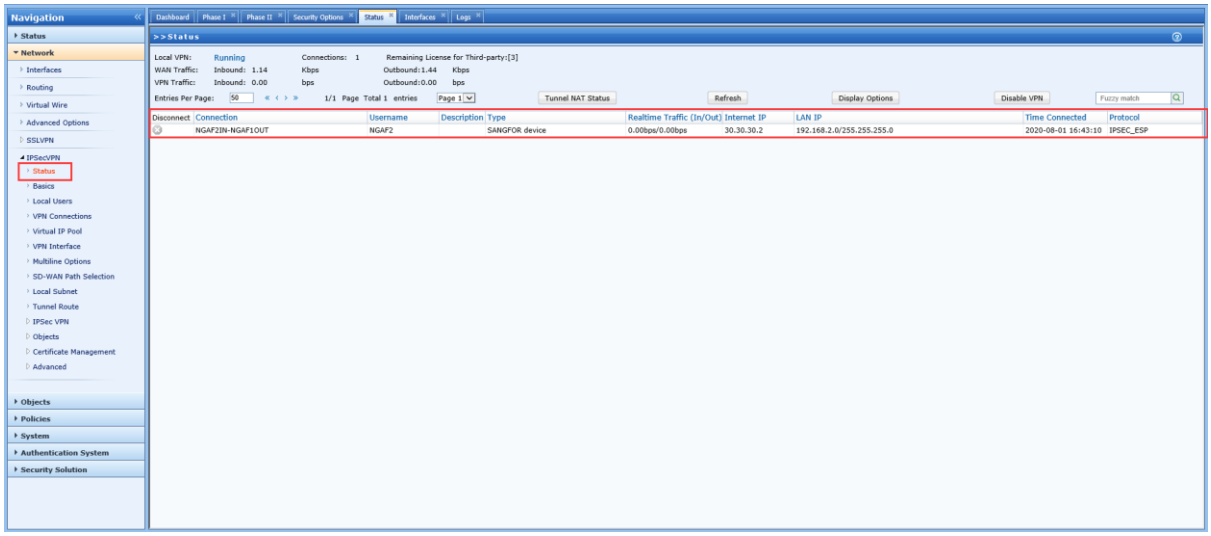
Chapter 4 Check IPsecVPN Status

1. Check the system logs corresponding to the VPN service on the headquarters device and branch device.

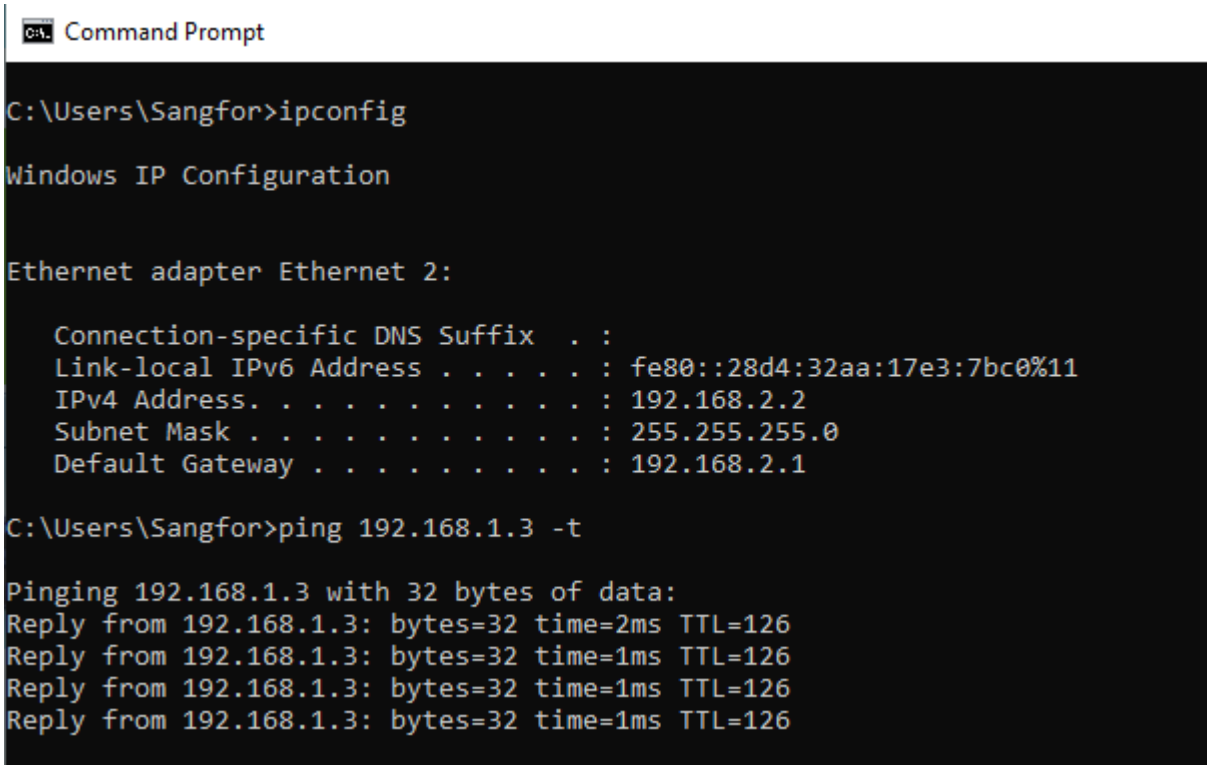


Check whether there is an error log and an alarm log. If there is an error log, you need to modify the relevant configuration according to the error log prompts.

2. Check the status of the VPN service. If the tunnel-related information can be queried, the VPN has been established successfully.

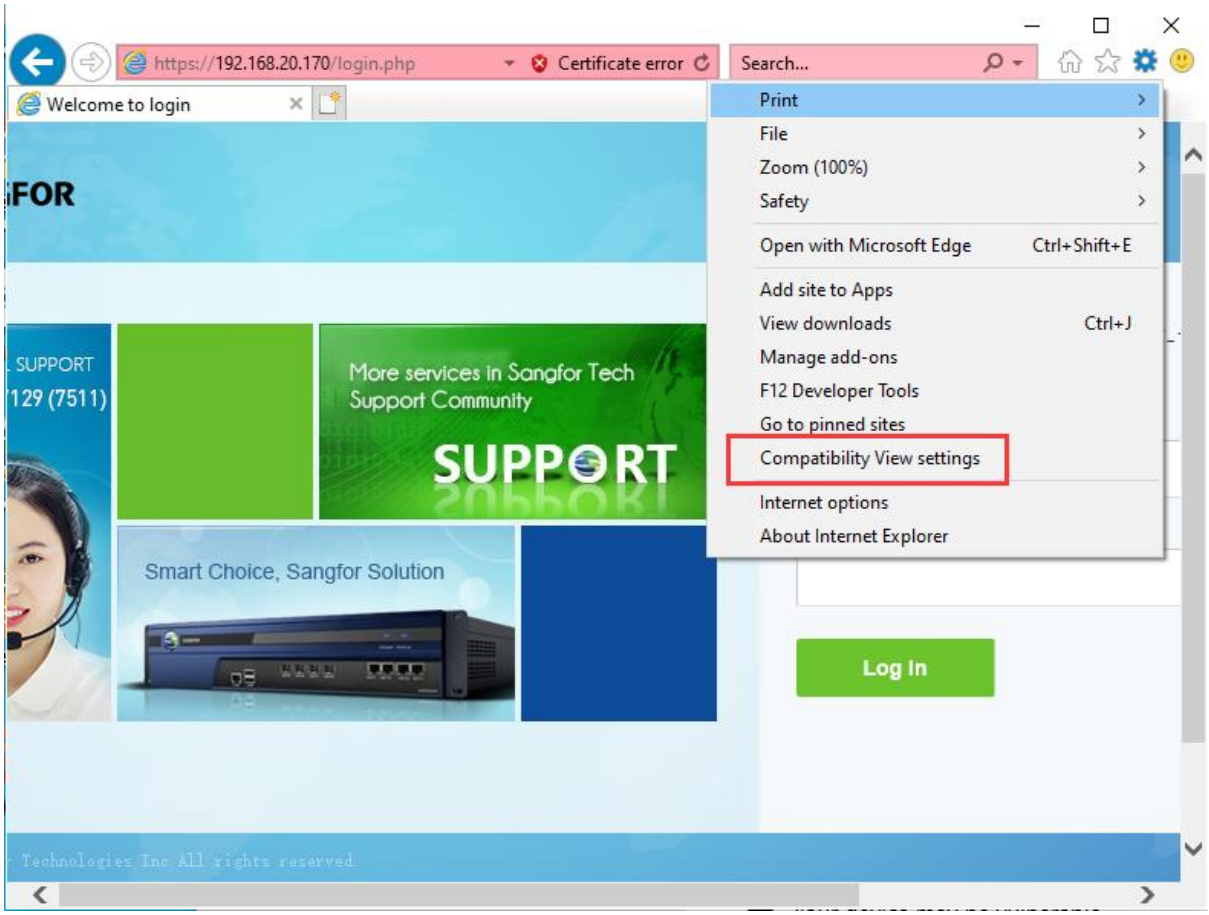


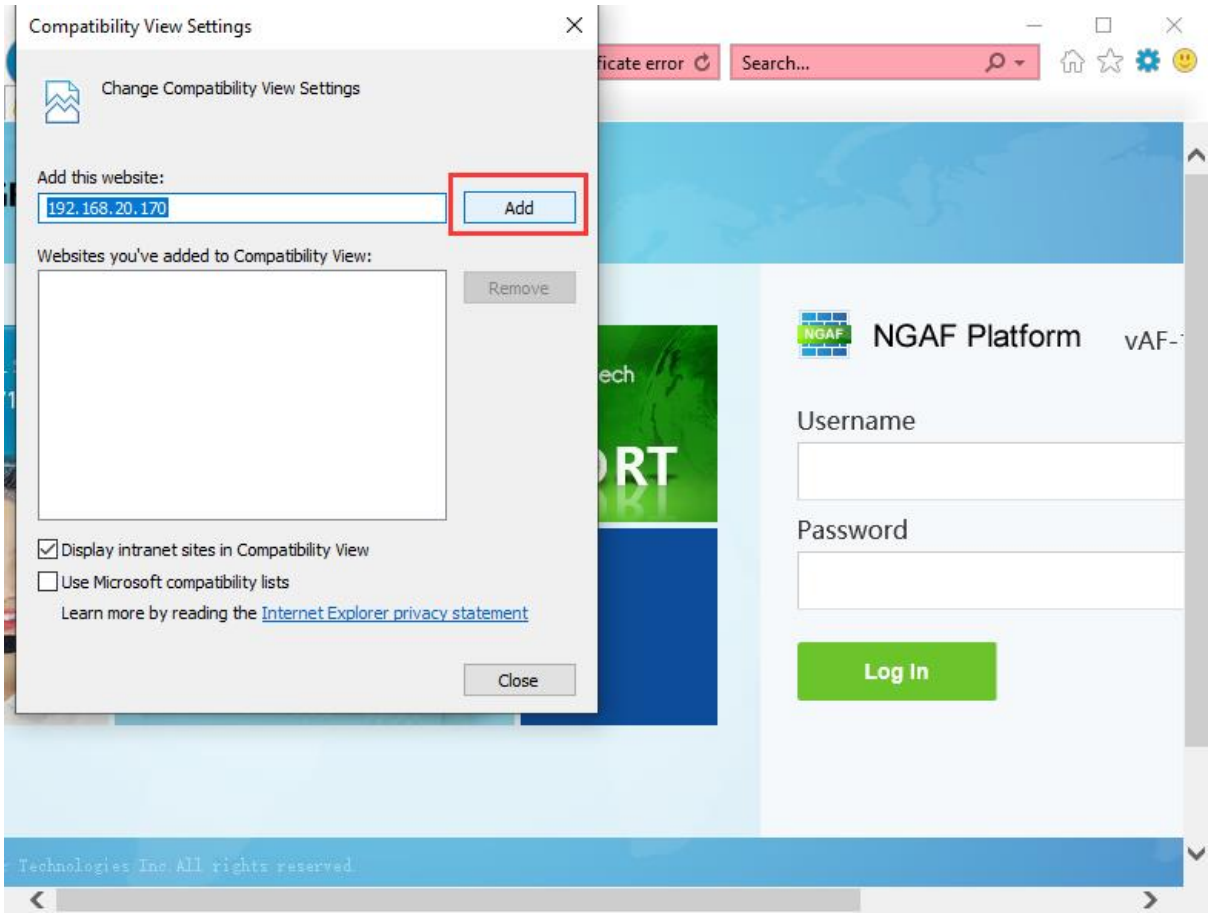
3. At the branch intranet PC, try to ping the headquarters intranet PC, and check whether the branch intranet PC192.168.2.2 can ping the headquarters intranet PC192.168.1.3. If you can ping, the communication is normal.



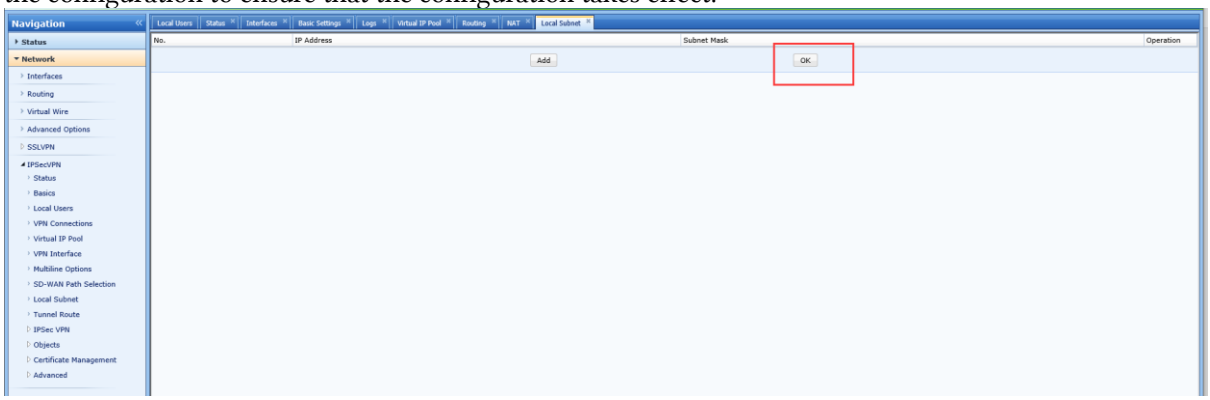
Chapter 5 Precaution

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

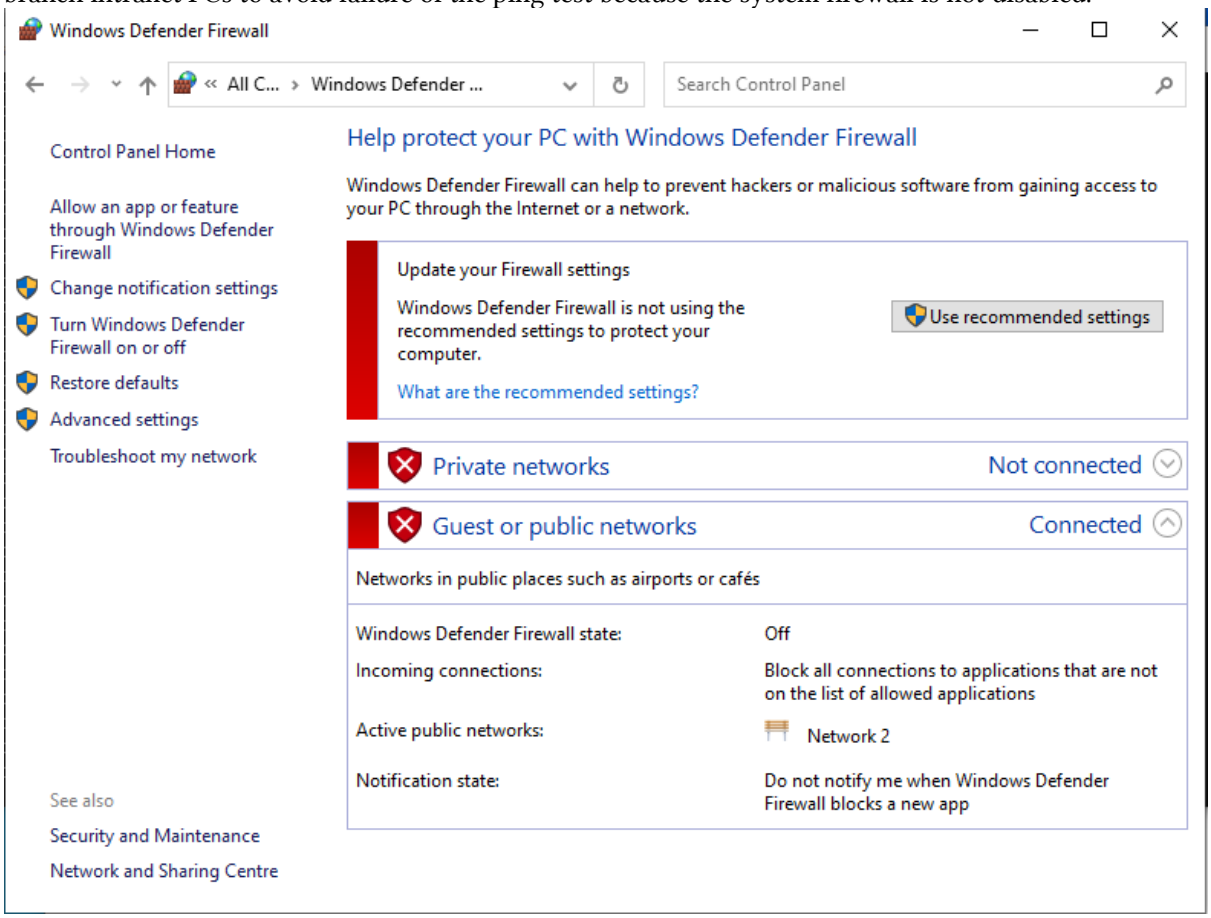

https://192.168.20.170/login.php
Certificate error
Search...
Welcome to login
Print
File
Zoom (100%)
Safety
Open with Microsoft Edge Ctrl+Shift+E
Add site to Apps
View downloads Ctrl+J
Manage add-ons
F12 Developer Tools
Go to pinned sites
Compatibility View settings
Internet options
About Internet Explorer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

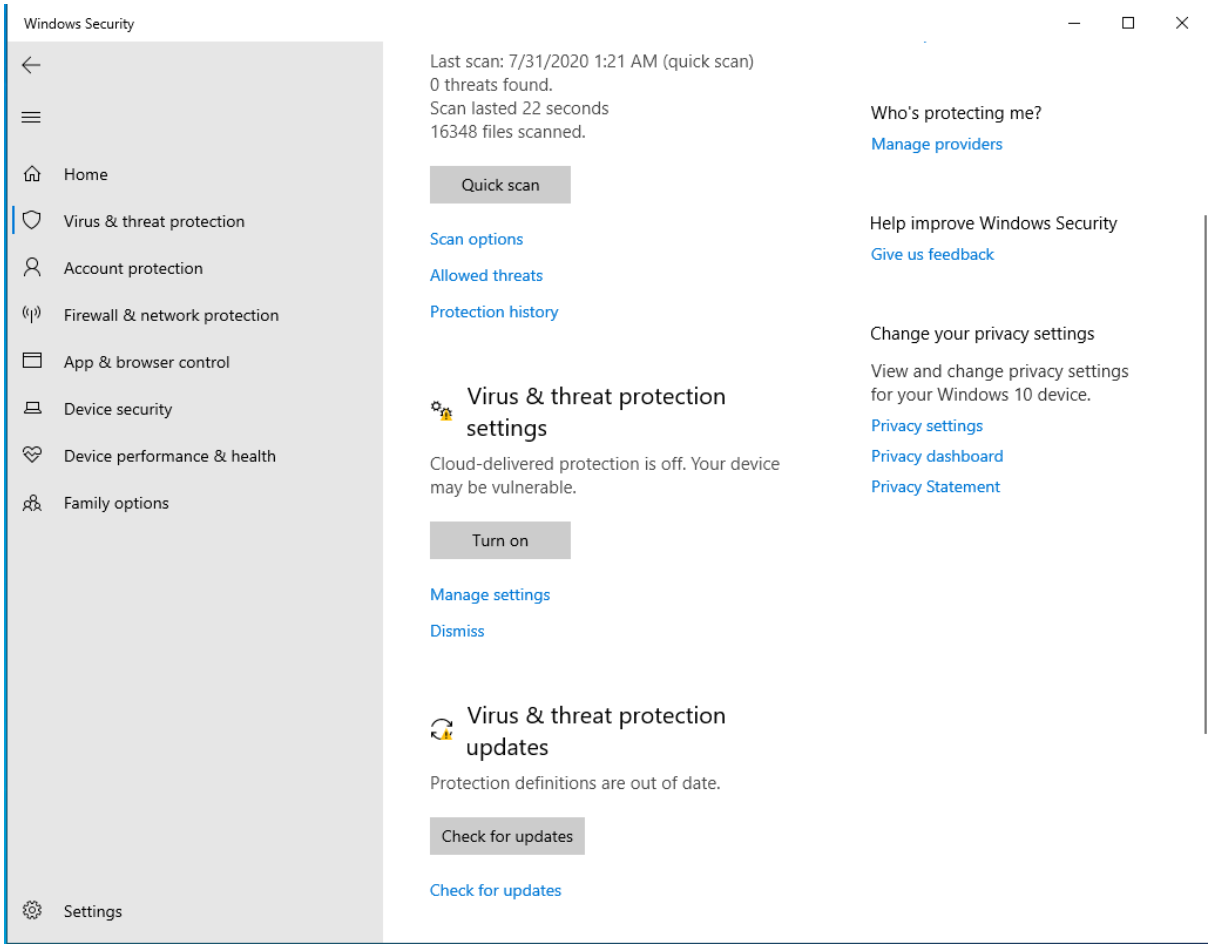

Compatibility View Settings
Change Compatibility View Settings
Add this website:
192.168.20.170
Add
Websites you've added to Compatibility View:
Remove
Display intranet sites in Compatibility View
Use Microsoft compatibility lists
Learn more by reading the Internet Explorer privacy statement
Close
NGAF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

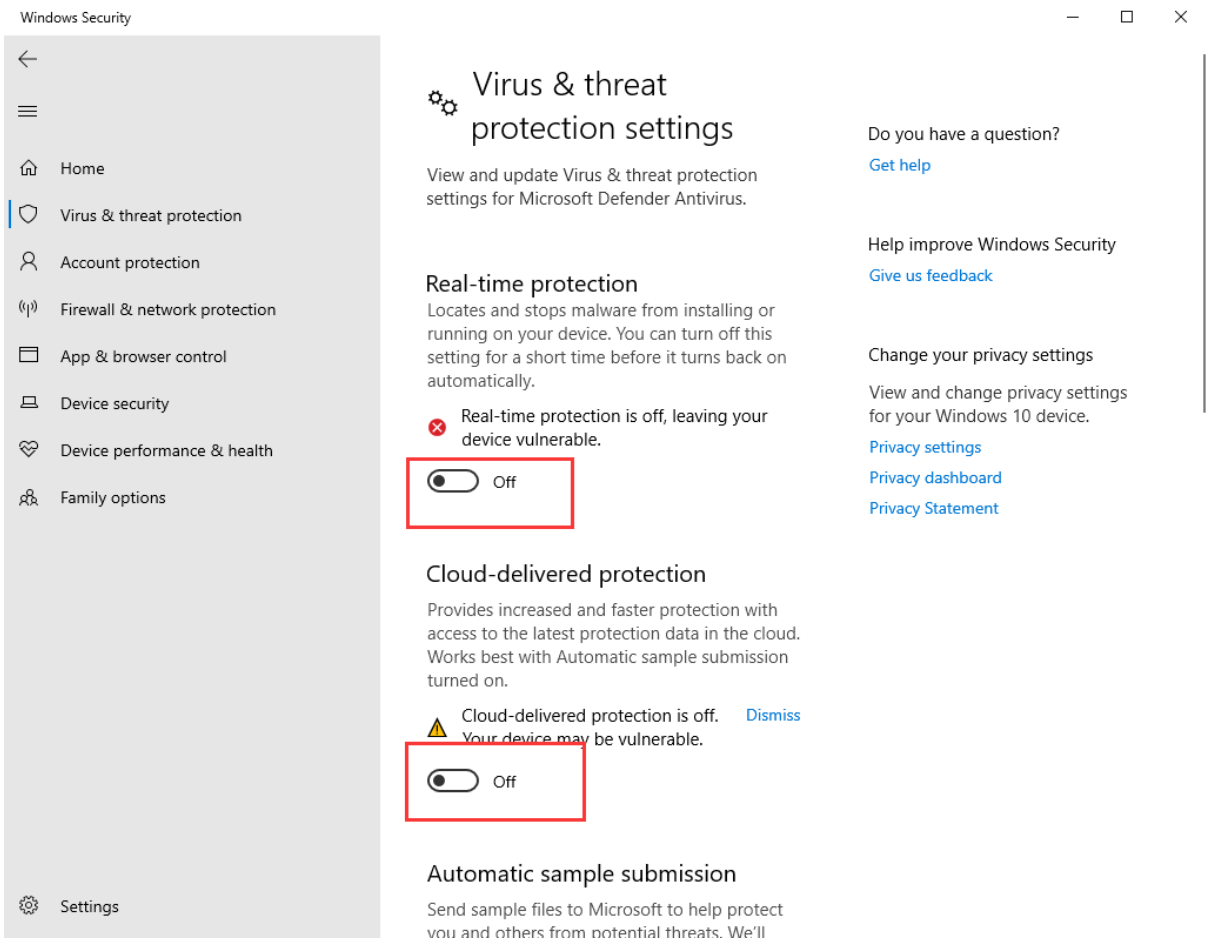
2. The VPN configuration has a large number of "OK" options, please be sure to click "OK" after finishing the configuration to ensure that the configuration takes effect.



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 enabled for the test IP to avoid interception of related data packets due to the NGAF policy configuration.