NGAF

Best Practices for Configuration_Establish SangforVPN

Version 8.0.35

Change Log

Date	Change Description
May 5, 2021	Document release.
May 17, 2021	Document update.

CONTENT

Chapter 1 Content Requirements

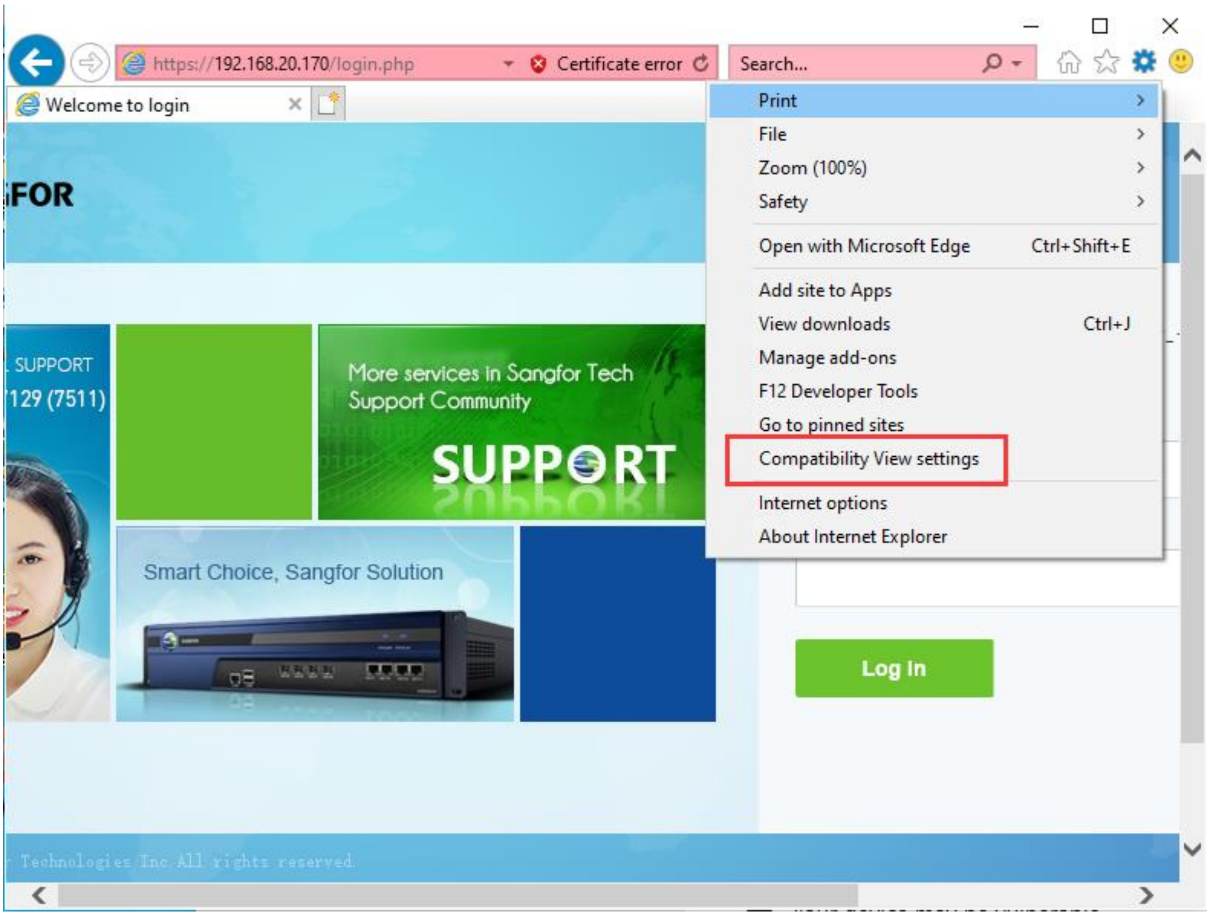
Related documents:

Best Practices for Configuration usually include selection of deployment mode, configuration ideas, information collection, function limitations, version differences. Regarding ***Establish SangforVPN***, if you want to learn about general POC scenarios and detailed configuration steps, please refer to the following link:

https://community.sangfor.com/plugin.php?id=sangfor_databases:index&mod=viewdatabase&tid=4598

1.1 Basic

1. If any end uses 8.0.26 and previous version. It is recommended to use IE browser to configure VPN related functions and enable the browser compatibility adaptation function.



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.Compared with standard IPSEC VPN, SANGFOR VPN has the following advantages:

Support the public network environment where both ends are non-fixed IP

VPN multi-line multiplexing technology to achieve load balancing and backup of VPN links

VPN dedicated line technology to realize the isolation between VPN network and public network

Inter-tunnel routing technology, branch users go online through the headquarters, realizing unified management and control of the headquarters

NAT technology between tunnels to solve the problem of IP conflicts in multiple branch network segments

Flow control technology in the tunnel to realize reasonable bandwidth allocation

1.2 Confirm the Requirements and Deployment

1. Confirm whether the user name and password filled in for the connection management of the branch device are consistent with the user name and password configured by the user management of the headquarters device, and confirm that the webagent address filled in by the branch device is consistent with that of the headquarters device

2. Multi-IP scenarios in the headquarters

To confirm whether the format is correct, click the test button during connection management configuration (PS: the test only verifies the format, not connectivity);

3. There are scenarios where the headquarters equipment is both the headquarters and branch roles

The main and backup webagent configuration of the access branch must be exactly the same as that of the headquarters (including format, IP, port);

4. Scenario of single-armed headquarters equipment

1) Whether the egress network device has port mapping for UDP and TCP for port 4009 (assuming that the VPN port is the default unmodified; assuming that the default port is modified, use UDP to establish the VPN, the egress gateway device must do symmetric port mapping); Use telnet to test whether the 4009 port of the IP address of the headquarters' public network can be connected to the computer on the Internet (only TCP port is applicable, UDP is not suitable)

2) Single-arm scenario export mapping needs to be mapped to single-arm multi-line IP, but cannot be mapped to lan port IP;

3) For dlan620 and above, in the single-arm scenario, if multiple lines are enabled, the Internet IP needs to be bound to the real line public network IP on the multiple lines;

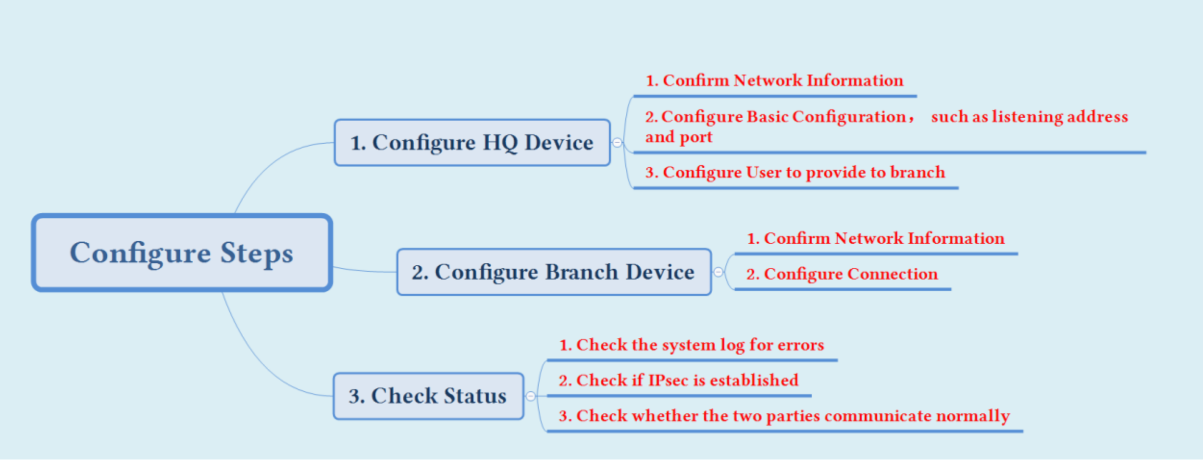
5. When the headquarters egress gateway device or the headquarters device is used as the egress gateway and uses PPPoE dial-up to access the Internet

One thing to note is that PPPoE cannot obtain the IP reserved by the operator. The address obtained by PPPoE can be changed, but it must be a public IP address. If you encounter this environment, please contact the operator to apply for a direct public IP instead of a private IP

6. Confirm whether the branch device can access the Internet and whether the connectivity to the external network is normal. Telnet on the branch device to test the connectivity to port 4009 of the headquarters device

1.3 Best Practices for Configuration

1.3.1 Configuration Steps


Configure Steps
1. Configure HQ Device
1. Confirm Network Information
2. Configure Basic Configuration， such as listening address and port
3. Configure User to provide to branch
2. Configure Branch Device
1. Confirm Network Information
2. Configure Connection
3. Check Status
1. Check the system log for errors
2. Check if IPsec is established
3. Check whether the two parties communicate normally

3.Compared with standard IPSEC VPN, SANGFOR VPN has the following advantages:

Support the public network environment where both ends are non-fixed IP

VPN multi-line multiplexing technology to achieve load balancing and backup of VPN links

VPN dedicated line technology to realize the isolation between VPN network and public network

Inter-tunnel routing technology, branch users go online through the headquarters, realizing unified management and control of the headquarters

NAT technology between tunnels to solve the problem of IP conflicts in multiple branch network segments

Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.The information in this document is subject to change without notice. To obtain the latest version, contact the international service center of SANGFOR Technologies Inc