SANGFOR

IPsec VPN

IPsec VPN standard configuration guide

Change Log

Date	Change Description
August 19, 2019	Sangfor IPsec VPN standard configuration guide.

CONTENT

Chapter 1 Content requirements

Note: If the whole document only has 1 chapter, this title can be omitted.

1 Document title

1.1 Technical Documents

SANGFOR_IPSECVPN _ STANDARD_CONFIGARATION_GUIDE_201908919

2 Product Version

Every document should be written with the latest product version unless special instructions.

DLAN Version 5.0 and above.

3 Preparation

3.1 Conditional Inspection

Before doing standard IPSEC, it needs to confirm the following condition:
(1) The Sangfor standard IPSEC follows the international standard IPSEC VPN protocol, as long as the peer VPN is also used the standard IPSEC protocol, then we able to use VPN connection with the peer.
(2) Sangfor equipment and third-party equipment for VPN connection, it need authorization to connect, whether there is authorization it can be queried in the licensing in the device WEBUI.
(3) If the Sangfor device is deployed in single-arm mode, to do standard IPSEC, check the DLAN version of the Sangfor device.
This is DLAN 5.0 or above. If not, contact the vendor to evaluate if it can be upgraded.

3.2 Environment Confirmation

Standard IPSEC connection, there are two modes, the Main mode, the Aggressive mode, then under what situation should choose the corresponding connection mode, will make a detailed introduction below:

1. If there is a NAT environment on both sides of the VPN device, you must use the aggressive mode.
    a. If both parties are static ip, there is no NAT environment, then you can be aggressive mode or main mode!
    b. If only one party is ADSL, there is no NAT environment,

       If the traffic is sent from ADSL to the static ip intranet, then either use the aggressive or main mode!

       If the traffic is sent from the static ip intranet to the ADSL intranet, then must applied the shell for ADSL, make sure the static ip site must enable the domain name of the connection ADSL!
    c. If both parties are ADSL, there must be a domain name for deploying shells to ensure that one site can connect through the domain name to another site VPN!

    (PS: ADSL may be obtained from the operator's private network address, if the operator has NAT, then must be connected in aggressive mode)
2. Sangfor VPN main mode default only supports ip address as ID! Sangfor VPN aggressive mode only supports FQDN as id by default (but DLAN 5.x and above aggressive mode can support IP address as the ID)

3. Sangfor VPN only supports Policy-based IPsec, does not support Route-based ipsec (route-based IPsec: IPsec is based on GRE tunnel)
4. Sangfor VPN only supports the second phase is to use Tunnel mode, does not support Transport mode!
5. Sangfor vpn only supports the first phase is to use the protocol version of IKE version 1, does not support IKE version version 2!

4 Configuration Guide

4.1 Main mode connection case

For example, in one of the following cases:

A company headquarters is a Sangfor device as a gateway.

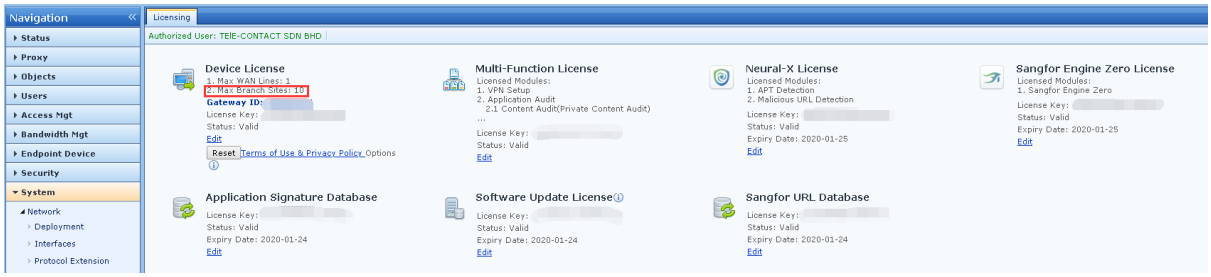
Gateway mode deployment, static public network IP 1.1.1.1 the intranet has a network segment of 192.168.1.0/24. The customer has a branch office, which is a peer Firewall to export, static public network IP 2.2.2.2 the intranet has a network segment of 192.168.2.0/24. Currently customer requirements require Sangfor device to be connected to the peer firewall for vpn connection. Implement the intranet 192.168.1.0 network segment can communicate with 192.168.2.0 network segment.

3.1.1 Preparation:

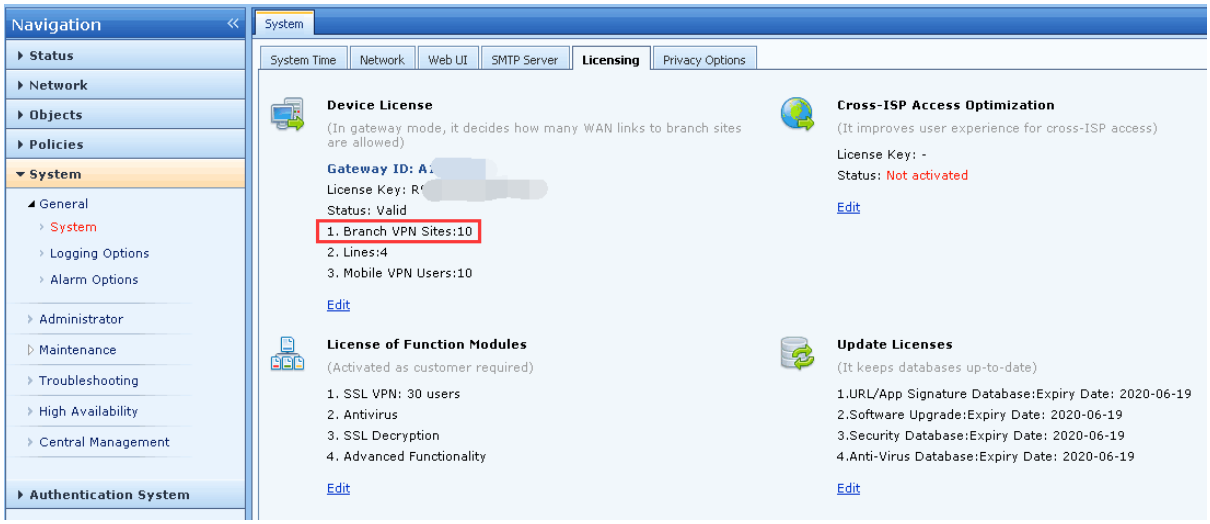
(1) Confirm that the VPN of peer firewall is a standard IPSEC protocol and can be connect.

(2) Confirm that the Sangfor device has the license for standard IPSEC connection. As shown in the figure below, there is no authorization, this need enable the licensing. Authorize relevant local market personnel to contact.

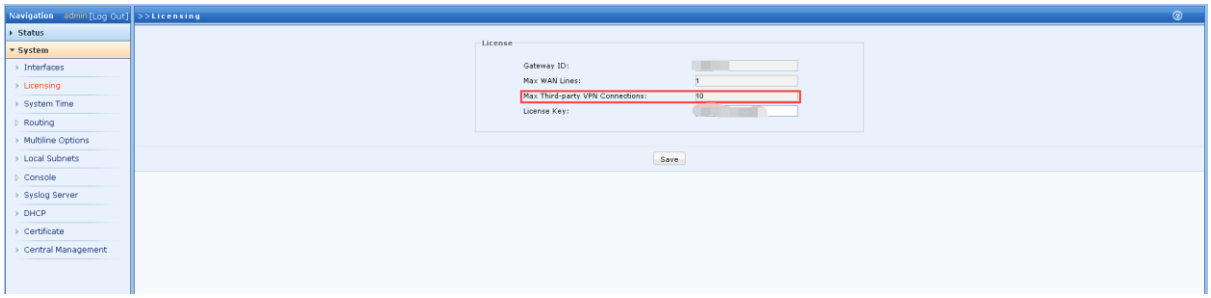
IAM



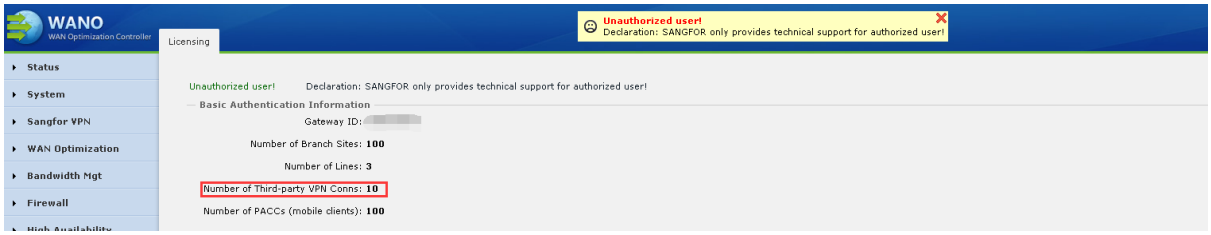
NGAF



MIG



WANO



VPN connection can be performed after the authorization is completed.

4.1.1 Mode Selection

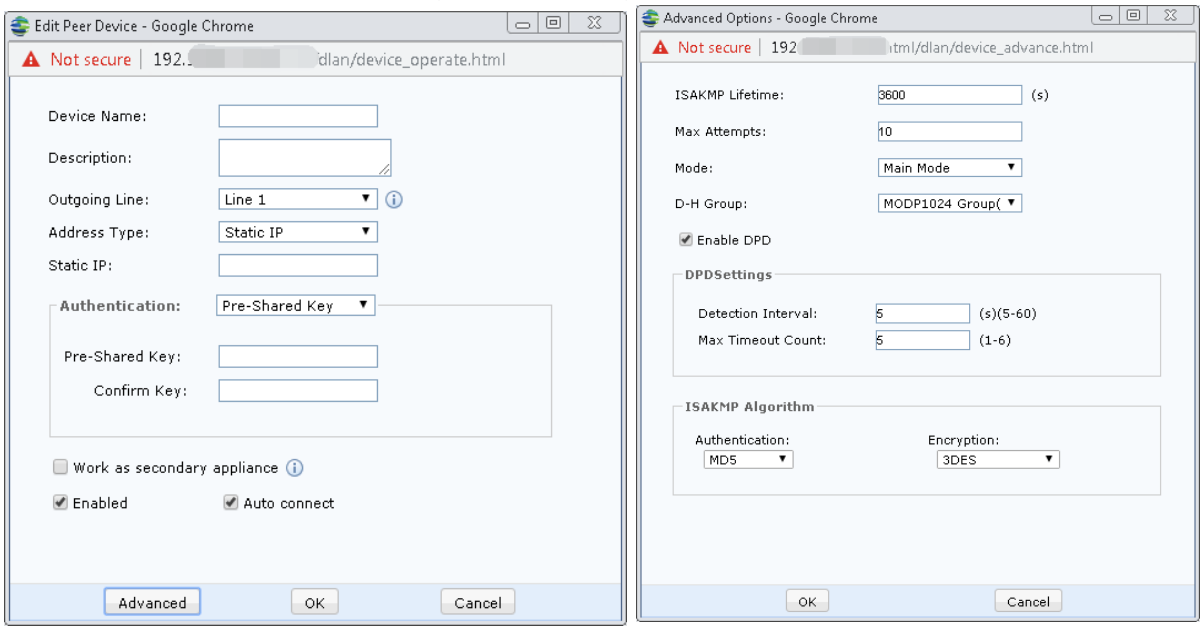
The customer's environment does not have a NAT environment. Both parties have a static public IP address, and both parties have public IP addresses. Underneath, you can choose either the main mode or the aggressive mode. In this case, the main mode is selected for connection.

4.1.2 Configuration Implementation

Configure on the Sangfor device according to the specific needs of the customer. The specific configuration is shown below:

The first phase of the configuration:

IAM, NGAF, MIG, and WANO is using the same configuration interface.



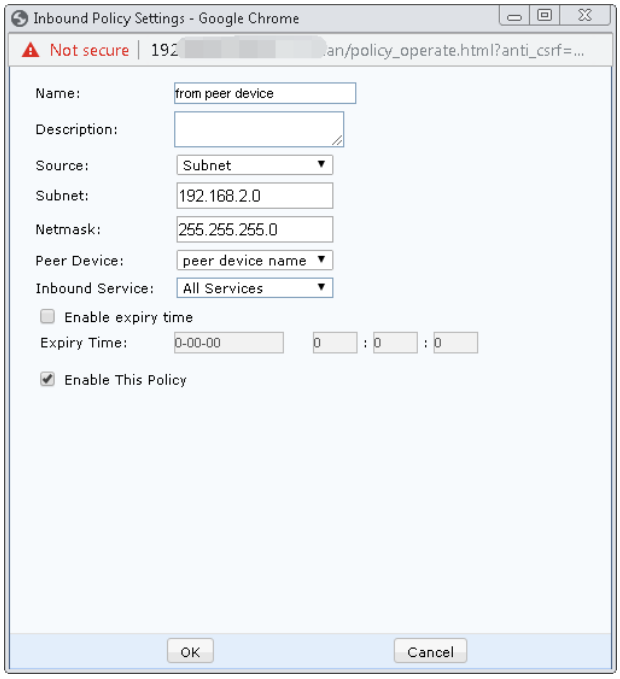
Device Name	**:**	**Peer device name**
Static IP	**:**	**Peer device public IP**
Pre-Share Key	**:**	**Same as peer device configured**
Confirm Key	**:**	**Same as peer device configured**

Make sure every setting is same as the peer device.

The second phase of the configuration:

First establish an inbound policy. This inbound policy is for the network segment that peer want to access. If there are several network segments fill in several policies, in this case, peer have only one network segment with a 192.168.2.0/24. At this time establish an inbound policy can be used. The specific configuration looks at the following figure:

IAM, NGAF, MIG, and WANO is using the same configuration interface.

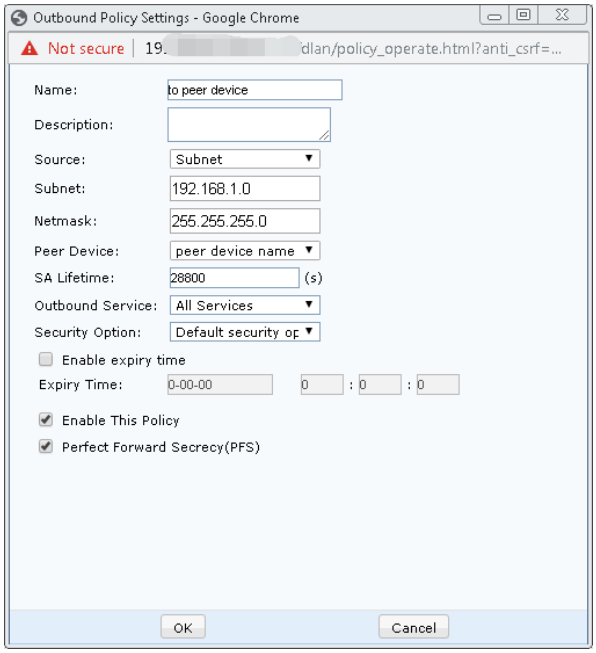


Subnet/Netmask : Peer device local subnet

Peer Device : Peer device created at phase 1

Then you can establish an outbound policy. This outbound policy defines what network segments are to be accessed by the local network segment, if there are several network segments fill in several policies. The specific configuration is as follows:

IAM, NGAF, MIG, and WANO is using the same configuration interface.



Subnet/Netmask : Local subnet

Peer Device : Peer device created at phase 1

Perfect Forward Secrecy(PFS) : Same as peer device.

The second phase of the security option selects the default Security option, which reads as follows:

IAM, NGAF, MIG, and WANO is using pretty much same interface.

At this point, the configuration of the Sangfor device is done. If the third party has already been configured, it will see the connections that are already connected in DLAN allowed status;

The rest is the configuration of the peer. The configuration of each vendor may be slightly different. The configuration of the peer is according to their manufacturer configuration requirement.

5 Precautions

(1) The Sangfor standard IPSEC needs to be authorized. For specific authorization, you can contact sale team for consultation.

(2) If the VPN configuration is not connected after the configuration is completed, you can go to the system log to see if there is any error, modify the configuration according to the error message

(3) When doing standard IPSEC interconnection, the equipment of the peer manufacturer should pay attention between the VPN and the LAN allow in the firewall rules.