SANGFOR

NGAF
IPSec VPN with CISCO Configuration Guide

Version 8.0.8

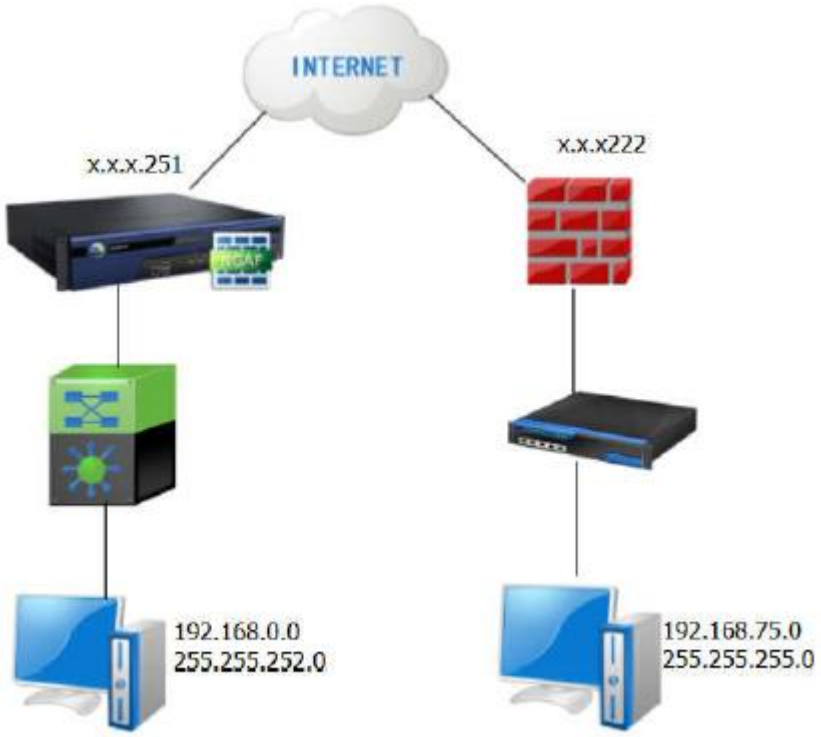
Change Log

Date	Change Description
Nov 25,2019	NGAF IPSec VPN with CISCO Configuration Guide

CONTENT

Chapter 1 Application Scenario

Establish IPSec VPN on NGAF and a third party device like CISCO RV042:



Requirement:

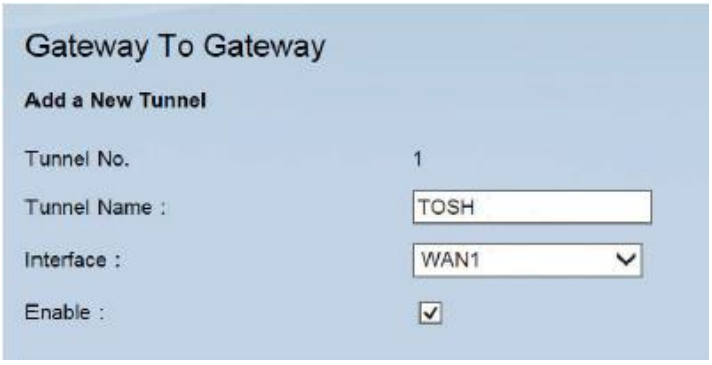
1. Require a NGAF device and a third party device such as CISCO RV042 device. Both of the device must be able to communicate normally.

Chapter 2 Configuration Method

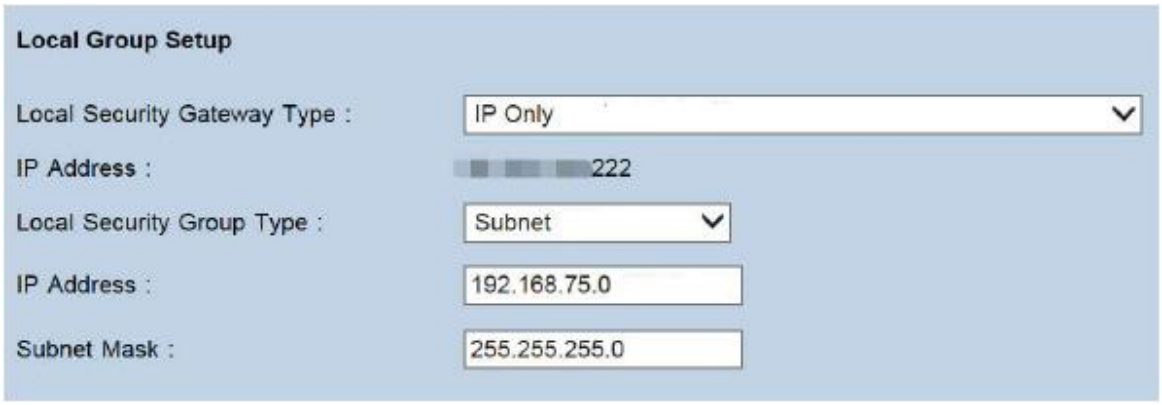
1. CISCO configuration

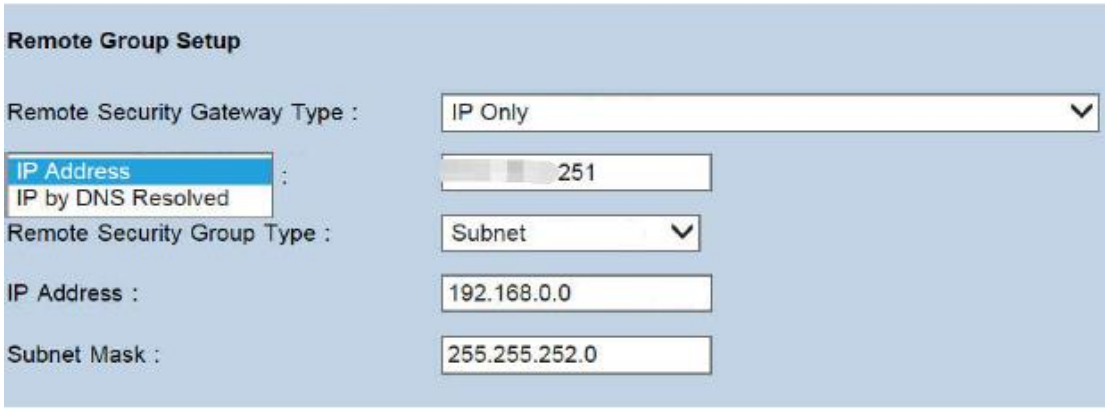
   1) Select gateway to gateway connection mode.

   2) Select the corresponding WAN interface, configure the name of policy.

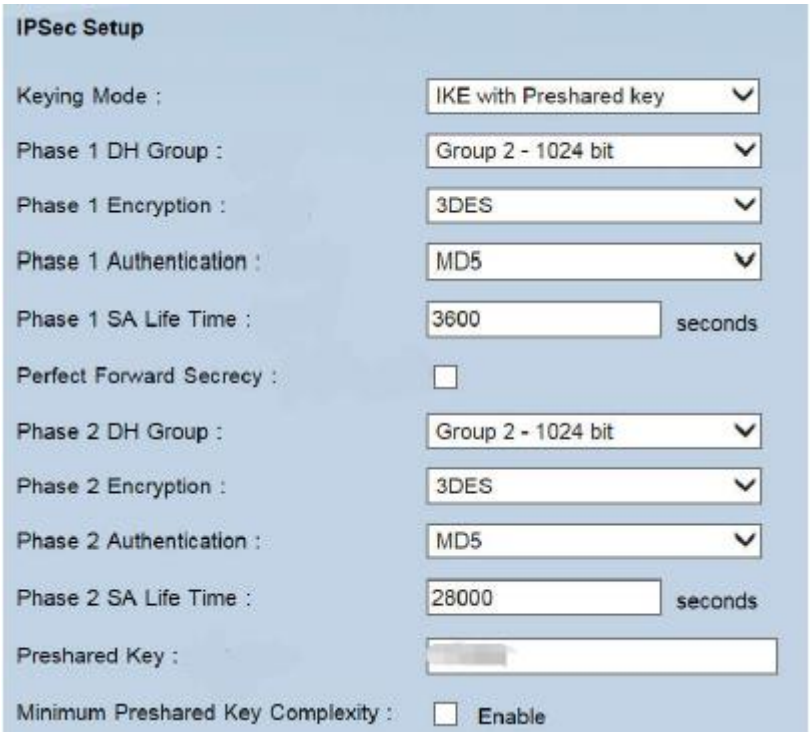


   3) Configure the connection mode and subnet range



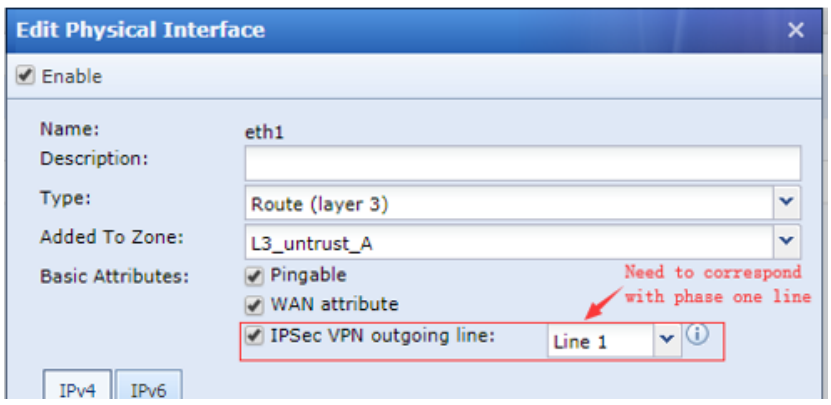


4) Parameter configuration of phase one and phase two



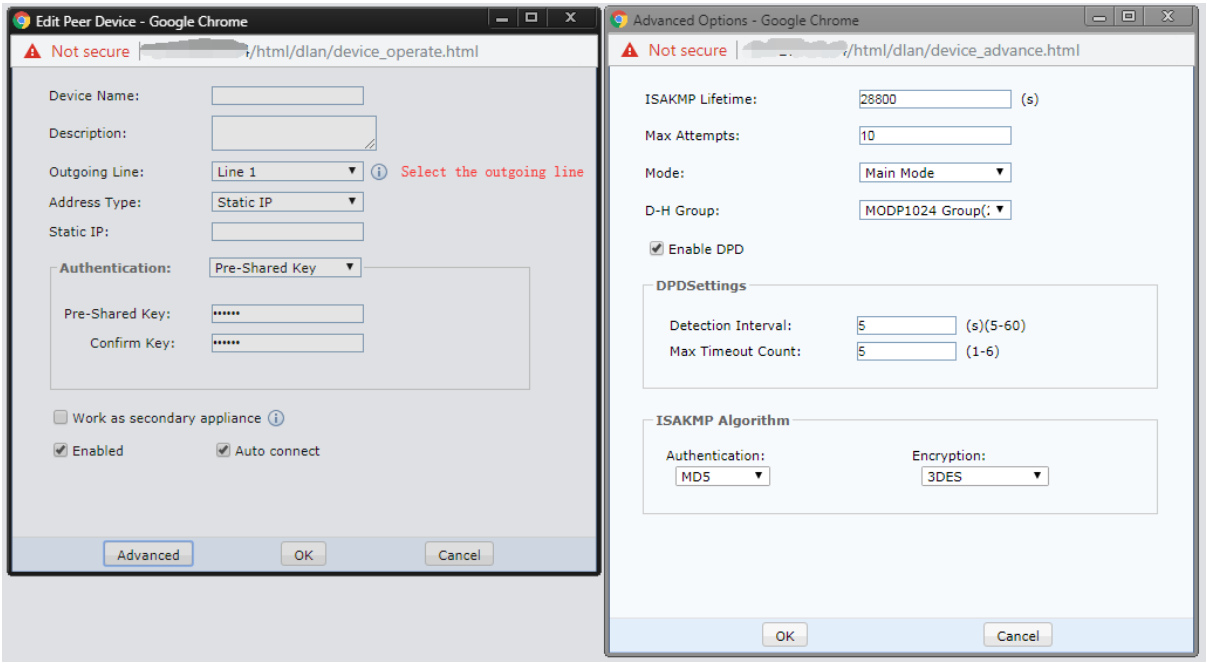
2. NGAF configuration

1) **Network > Interface** to configure the interface, tick IPSec VPN outgoing line (before version 6.8 does not have this module) or else the VPN service is unable function well.

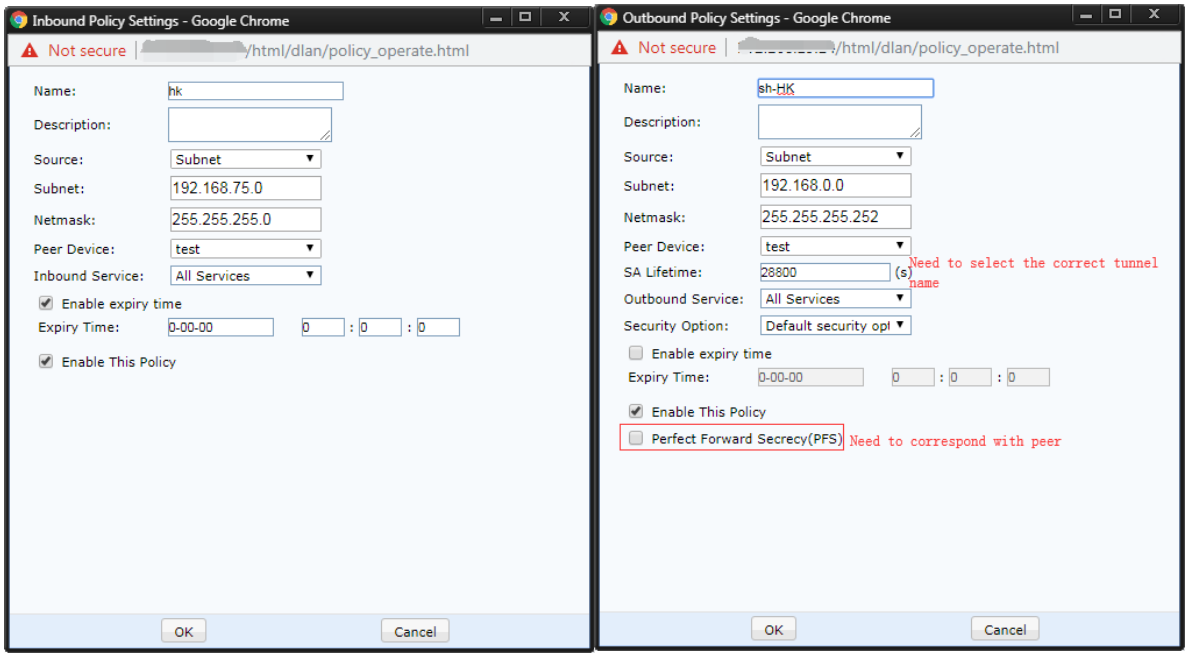


In **Network > IPSec VPN > VPN interface** add corresponding LAN interface. If the LAN interface is not added, the VPN service is also not able to function. (WAN interface with route mode should not be chosen as the VPN interface)

2) In **Network > IPSec VPN > Phase I** to configure the parameter.



3) In **Network** > **IPSec VPN** > **Phase II** to configure the inbound policy and outbound policy.



4) In **Network** > **IPSec VPN** > **Security Options** configure phase 2 authentication parameter.

Name	Protocol	Authentication Algorithm	Encryption	D
esp-md5-des	ESP	MD5	DES	
esp-md5-3des	ESP	MD5	3DES	
esp-md5-aes	ESP	MD5	AES	
esp-md5-aes256	ESP	MD5	AES256	
esp-sha1-des	ESP	SHA1	DES	
esp-sha1-3des	ESP	SHA1	3DES	
esp-sha1-aes	ESP	SHA1	AES	
esp-sha1-aes256	ESP	SHA1	AES256	
Default security option	ESP	SHA1	AES	

Add OK

Chapter 3 Precautions

1. Between two device's UDP500 and UDP4500 need to be ensure that they are able to communicate normally, or else unable to connect.
2. The lifetime for phase I and phase II is recommended to use 28800 seconds, if the lifetime use 3600 seconds it will be ended very fast.
3. When doing testing in LAN, the source IP and the destination IP must match the inbound and outbound, otherwise the data is not able to enter the VPN tunnel.
4. Bridge mode does not support third party connection.
5. Before configuring IPsec VPN on NGAF, you need to Go to **Network> IPsec VPN> Status** enable VPN service.
6. Make sure that NGAF has sufficient VPN License.

SANGFOR