



SANGFOR



NGAF IPSec VPN with CISCO Configuration Guide

Version 8.0.8



Change Log

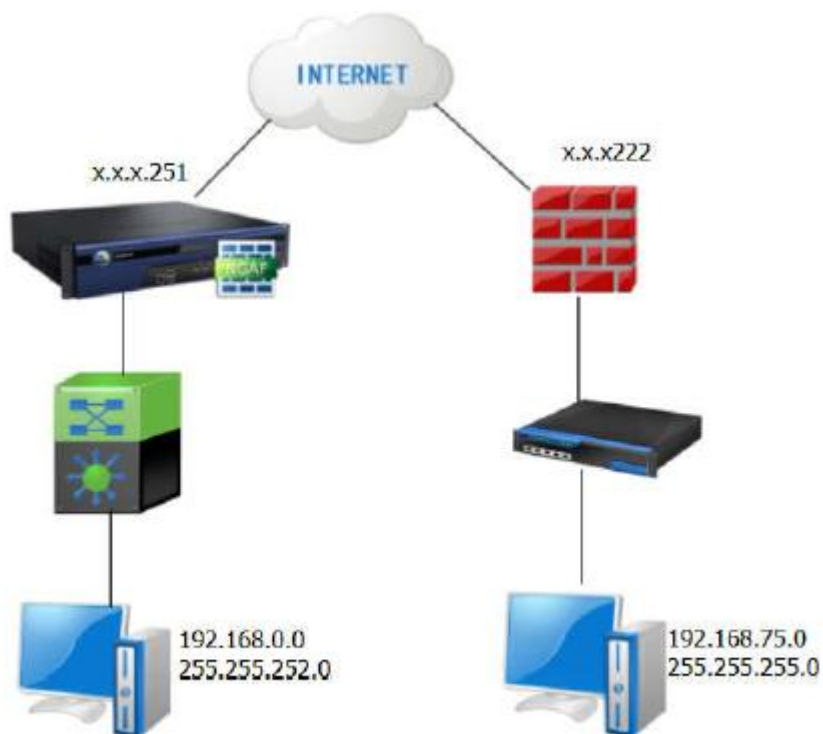
Date	Change Description
Nov 25,2019	NGAF IPSec VPN with CISCO Configuration Guide

CONTENT

Chapter 1 Application Scenario	1
Chapter 2 Configuration Method.....	2
Chapter 3 Precautions	6

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

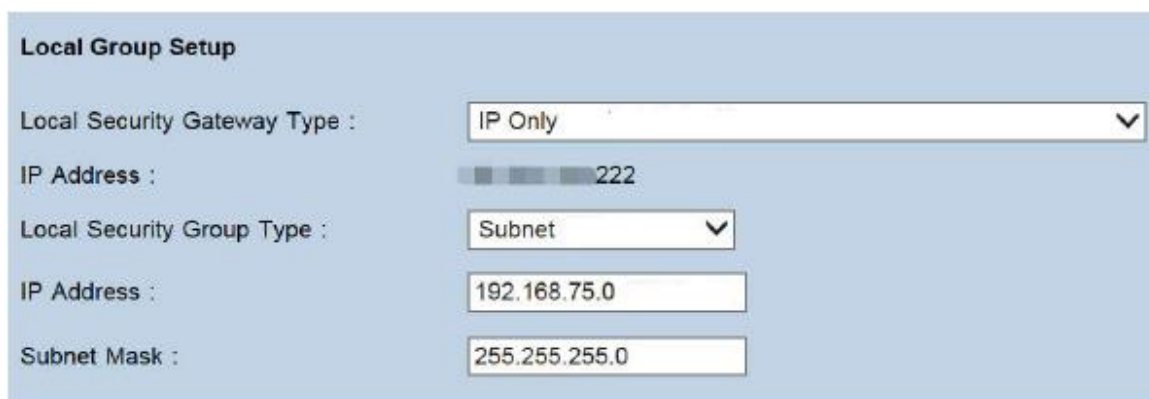
- 1) Select gateway to gateway connection mode.



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

A screenshot of the 'Gateway To Gateway' configuration page. The page has a title 'Gateway To Gateway' and a sub-header 'Add a New Tunnel'. Below this, there are four fields: 'Tunnel No.' with the value '1', 'Tunnel Name' with the value 'TOSH', 'Interface' with a dropdown menu showing 'WAN1', and 'Enable' with a checked checkbox.

- 3) Configure the connection mode and subnet range

A screenshot of the 'Local Group Setup' configuration page. The page has a title 'Local Group Setup'. Below this, there are five fields: 'Local Security Gateway Type' with a dropdown menu showing 'IP Only', 'IP Address' with a value of '222', 'Local Security Group Type' with a dropdown menu showing 'Subnet', 'IP Address' with the value '192.168.75.0', and 'Subnet Mask' with the value '255.255.255.0'.

Remote Group Setup

Remote Security Gateway Type : IP Only

IP Address : 251

Remote Security Group Type : Subnet

IP Address : 192.168.0.0

Subnet Mask : 255.255.252.0

4) Parameter configuration of phase one and phase two

IPSec Setup

Keying Mode : IKE with Preshared key

Phase 1 DH Group : Group 2 - 1024 bit

Phase 1 Encryption : 3DES

Phase 1 Authentication : MD5

Phase 1 SA Life Time : 3600 seconds

Perfect Forward Secrecy : ☐

Phase 2 DH Group : Group 2 - 1024 bit

Phase 2 Encryption : 3DES

Phase 2 Authentication : MD5

Phase 2 SA Life Time : 28000 seconds

Preshared Key :

Minimum Preshared Key Complexity : ☐ Enable

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.

Edit Physical Interface

☒ Enable

Name: eth1

Description:

Type: Route (layer 3)

Added To Zone: L3_untrust_A

Basic Attributes:

- ☒ Pingable
- ☒ WAN attribute
- ☒ IPsec VPN outgoing line: Line 1

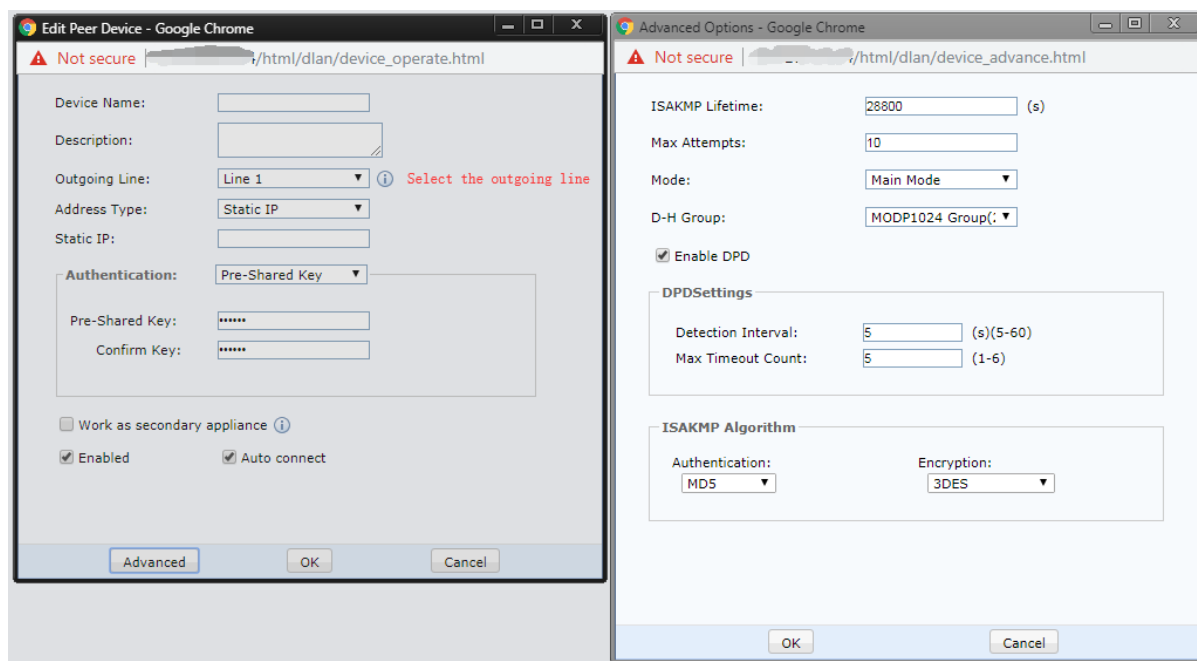
Need to correspond with phase one line

IPv4 IPv6

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

Copyright © SANGFOR Technologies Inc. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of SANGFOR Technologies Inc.

SANGFOR is the trademark of SANGFOR Technologies Inc. All other trademarks and trade names mentioned in this document are the property of their respective holders.

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