



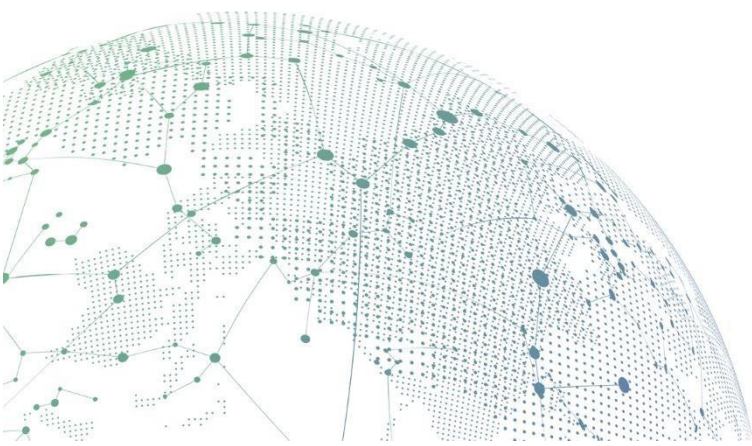
SANGFOR



NGAF

IPSec VPN with CISCO Configuration Guide

Version 8.0.35



Change Log

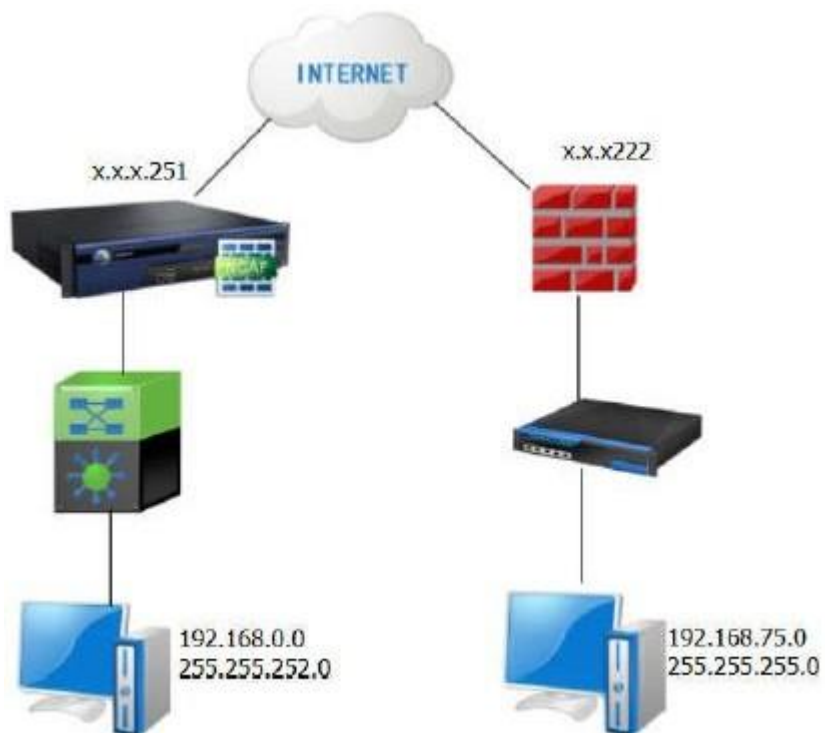
Date	Change Description
June 9 ,2021	NGAF IPSec VPN with CISCO Configuration Guide

CONTENT

Chapter 1 Application Scenario.....	1
Chapter 2 Configuration Method.....	2
Chapter 3 Precautions	8

Chapter 1 Application Scenario

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



Requirement:

1. Require an NGAF device and a third-party device such as the 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.



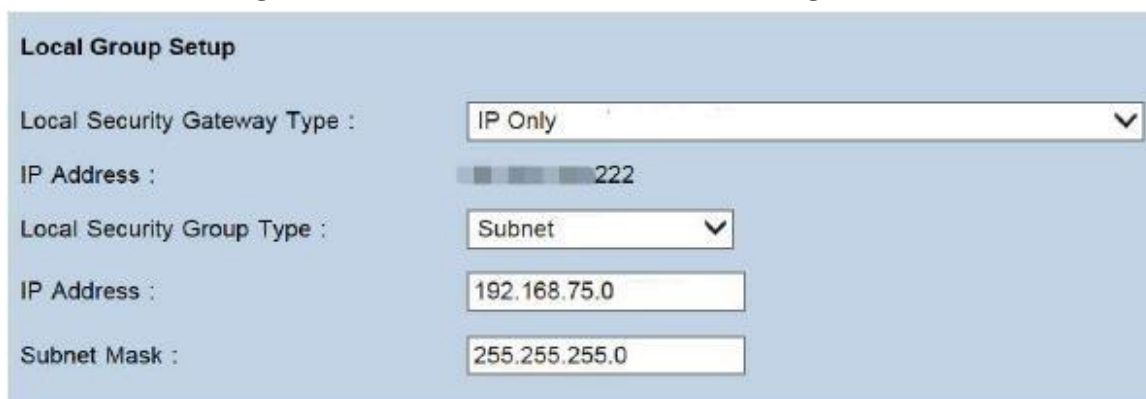
- 2) Select the corresponding WAN interface, configure the name of the policy.



A screenshot of the 'Gateway To Gateway' configuration page. The title is 'Gateway To Gateway'. Below it is the section 'Add a New Tunnel'. The form contains the following fields:

- Tunnel No.: 1
- Tunnel Name: TOSH
- Interface: WAN1 (selected from a dropdown menu)
- Enable:

- 3) Configure the connection mode and subnet range



A screenshot of the 'Local Group Setup' configuration page. The title is 'Local Group Setup'. The form contains the following fields:

- Local Security Gateway Type: IP Only (selected from a dropdown menu)
- IP Address: [IP address field] 222
- Local Security Group Type: Subnet (selected from a dropdown menu)
- IP Address: 192.168.75.0
- Subnet Mask: 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

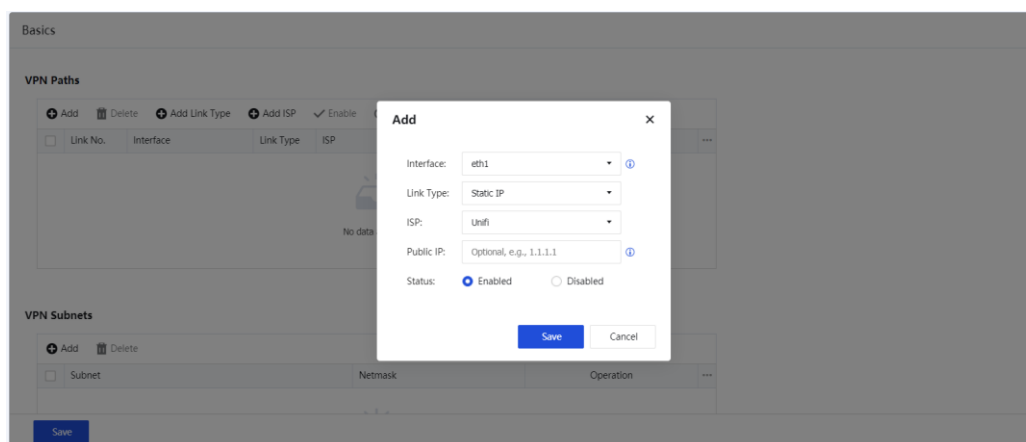
Phase 2 SA Life Time : 28000 seconds

Preshared Key : [Redacted]

Minimum Preshared Key Complexity : Enable

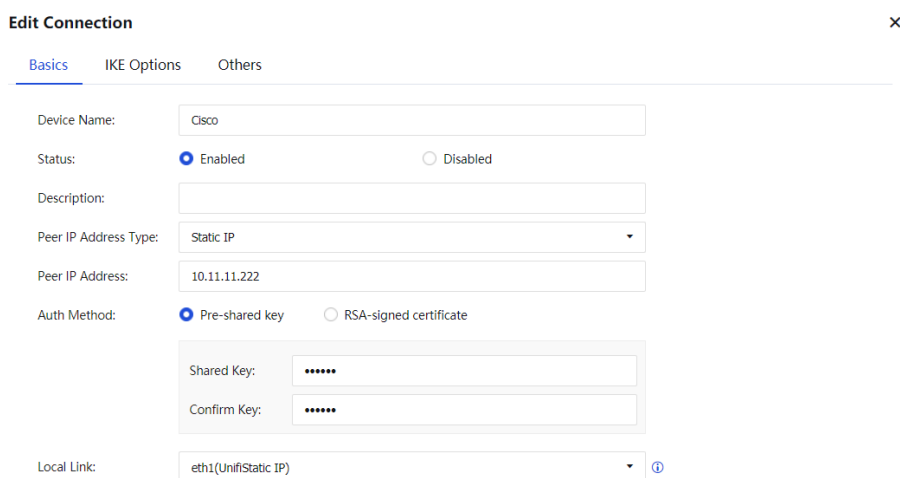
2. NGAF configuration

1) Go to **Network > IPsec VPN > Basic Settings** to configure the VPN Paths.



Note: if your device is deployed in route mode or single-arm mode and the WAN interface has not been configured with a public IP address, you need to configure the public IP of front device in the Public IP section.

2) In **Network > IPsec VPN > Third-Party Connection** to configure the IPsec VPN parameter.



- Under **Encrypted Traffic**, click **Add** button to add Local and Peer IP Address configuration.

Add Encrypted Traffic ✕

Local IP Address: ⓘ

Local Intranet Service:

Peer IP Address: ⓘ

Peer Intranet Service:

Phase 2 Proposal: ⓘ

Protocol	Encryption Algorithm	Auth Algorithm	Perfect Forward Secrecy	Operation	...
ESP	AES	SHA1	-None-	Delete	
ESP	AES256	SHA1	-None-	Delete	
ESP	DES	SHA1	-None-	Delete	

- After adding the Local IP Address and Peer IP Address, choose the Phase 2 proposal that matches with the peer device and click the **Add** button.

Add Encrypted Traffic ✕

Local Intranet Service:

Peer IP Address: ⓘ

Peer Intranet Service:

Phase 2 Proposal: ⓘ

Protocol	Encryption Algorithm	Auth Algorithm	Perfect Forward Secrecy	Operation	...
ESP	3DES	MD5	-None-	Delete	

1/16 entries ⓘ

Route Priority: (1-256) ⓘ

NGAF Configuration Guide Version

Add Connection

Auth Method: Pre-shared key RSA-signed certificate

Shared Key:

Confirm Key:

Local Link:

Encrypted Traffic

<input type="checkbox"/>	Local IP Address	Local Intranet Service	Peer IP Address	Peer Intranet Service	Phase 2 Proposal	Route Priority	Opera
<input type="checkbox"/>	192.168.0.0/24	All Services	192.168.75.0/24	All Services	ESP/ MD5-3DES/ None	128	Edit

5) Then go to **IKE Options**, configure the phase 1 IKE configuration.

Add Connection

Basics **IKE Options** Others

IKE Version: IKEv1 IKEv2 ⓘ

Mode: Main mode Aggressive mode

Initiate Connection: Enable Disable

Local ID Type:

Local ID:

Peer ID Type:

Peer ID:

IKE SA Timeout(s):

DH Group:

DPD: Enable Disable ⓘ

NGAF Configuration Guide Version

Add Connection ✕

DH Group:

DPD: Enable Disable ⓘ

NAT-T: Enable Disable ⓘ

Detection Interval and Max Attempts below are only applicable when DPD or NAT-T is enabled.

Detection Interval(s):

Max Attempts:

Phase 1 Proposal:

Encryption Algorithm	Auth Algorithm	Operation	...
3DES	MD5	Delete	

1/16 entries ⓘ

6) Lastly, go to **Others** to configure Phase 2 SA Timeout.

Add Connection ✕

Basics IKE Options Others

Max Attempts: ⓘ

IPSec SA Timeout(s):

Expiration Time: Enable Disable

Chapter 3 Precautions

1. Make sure local and peer device settings are consistent.
2. Ensure the UDP500 and UDP4500 between two devices can communicate normally, or else unable to connect.
3. The lifetime for phase one and phase two is recommended to use 28800 seconds. If the lifetime uses 3600 seconds, it will be ended very fast.
4. When testing in LAN, the source IP and the destination IP must match the Local and Peer IP configured in **Encrypted Traffic, otherwise**, the data cannot enter the VPN tunnel.
5. Bridge mode does not support IPsec VPN.
6. Before configuring IPsec VPN on NGAF, you need to Go to **Network> IPsec VPN> Status** to enable VPN service.
7. 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