



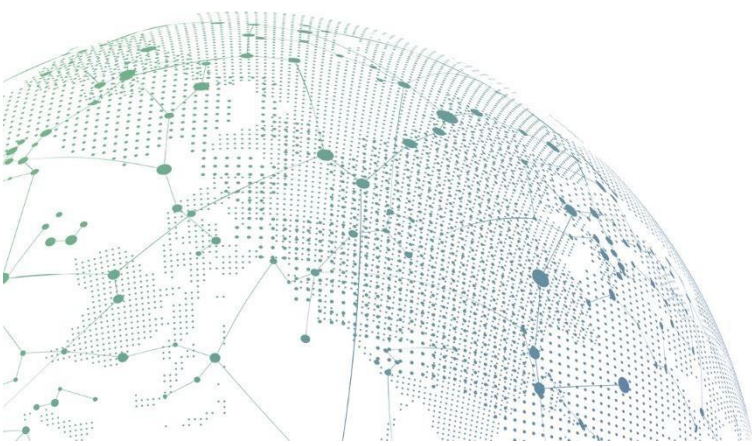
SANGFOR



NGAF

Panduan Konfigurasi IPSec VPN dengan CISCO

Versi 8.0.35



Data Perubahan

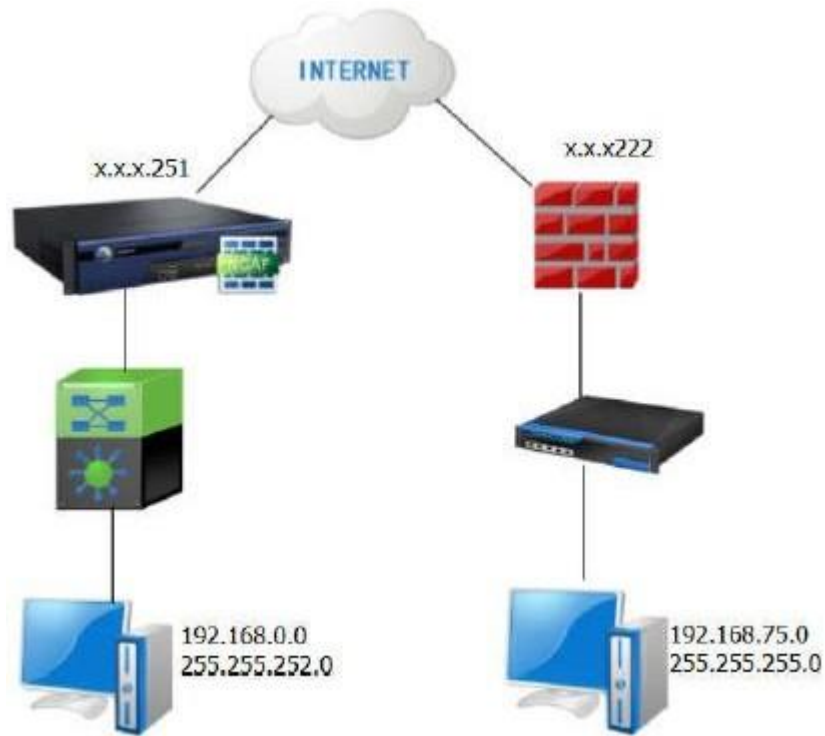
Date	Change Description
June 9 ,2021	Panduan Konfigurasi NGAF IPSec VPN dengan CISCO

DAFTAR ISI

BAB 1 Skenario Penerapan.....	1
BAB 2 Metoda Konfigurasi.....	2
BAB 3 Perhatian	8

BAB 1 Skenario Penerapan

Penerapan IPSec VPN pada NGAF dengan Produk lainnya seperti CISCO RV042:



Persyaratan:

1. Persyaratan pada NGAF dan produk lainnya seperti CISCO RV042. Kedua alat harus dapat saling berkomunikasi secara normal.

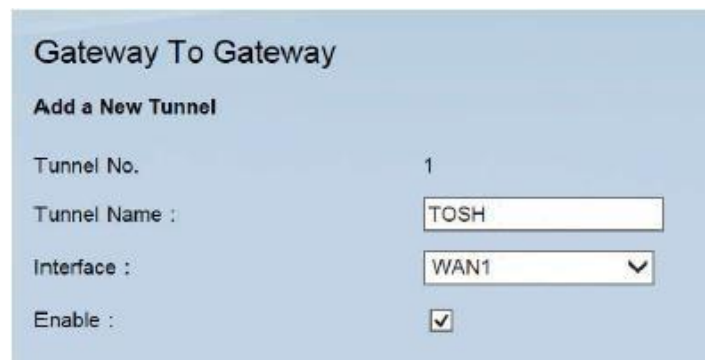
BAB 2 Metoda Konfigurasi

1. Konfigurasi pada CISCO

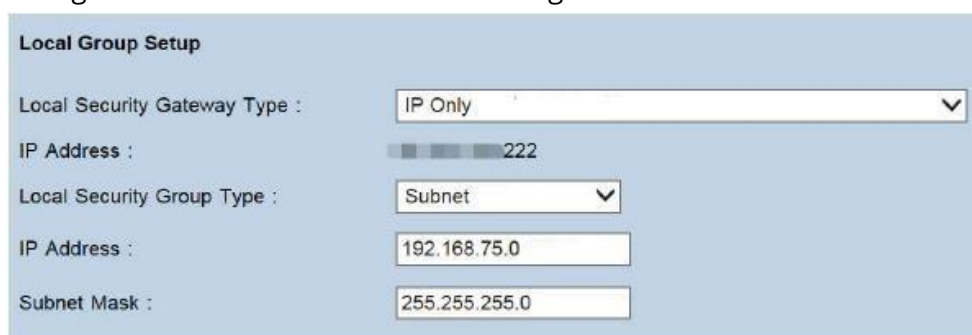
- 1) Pilih mode koneksi “gateway to gateway”.



- 2) Pilih interface sehubungan dengan WAN, konfigurasi nama dari policy.

A screenshot of the 'Gateway To Gateway' configuration page. The page has a light blue header with the title 'Gateway To Gateway'. Below the title is a section 'Add a New Tunnel'. The form contains the following 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) Konfigurasi mode koneksi dan subnet range

A screenshot of the 'Local Group Setup' configuration page. The page has a light blue header with the title 'Local Group Setup'. The form contains the following 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

IP by DNS Resolved

Remote Security Group Type : Subnet ▼

IP Address : 192.168.0.0

Subnet Mask : 255.255.252.0

4) Konfigurasi parameter dari “phase one” dan “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 ▼

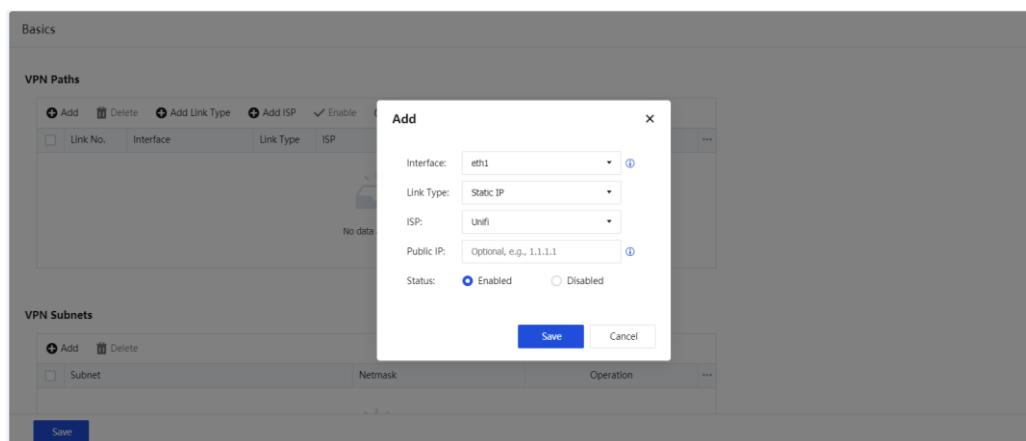
Phase 2 SA Life Time : 28000 seconds

Preshared Key :

Minimum Preshared Key Complexity : ☐ Enable

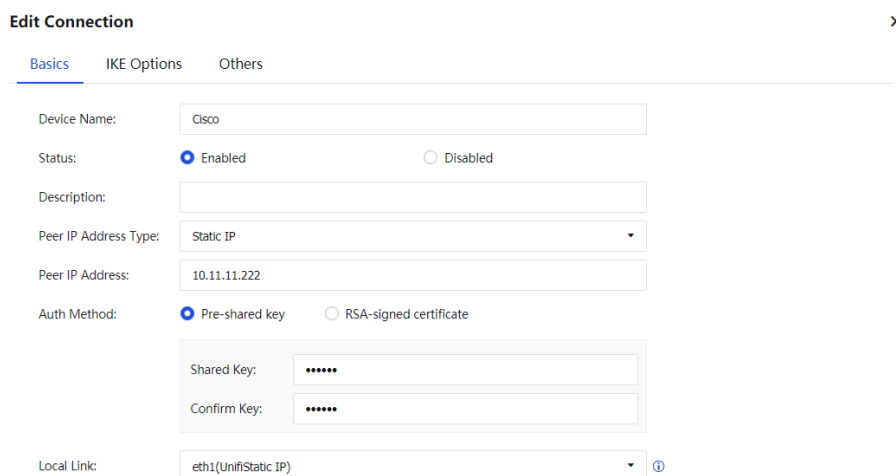
2. Konfigurasi pada NGAF

- 1) Pada **Network > IPsec VPN > Basic Settings** untuk konfigurasi VPN Path.



Note: Jika alat Anda menggunakan mode route mode atau single-arm dan interface WAN tidak menggunakan alamat IP Publik, Anda perlu mengkonfigurasi alamat IP Publik dari alat di depannya pada bagian alamat IP Publik.

- 2) Pada **Network > IPsec VPN > Third-Party Connection** untuk konfigurasi parameter IPsec VPN.



- 3) Pada **Encrypted Traffic**, klik tombol **Add** untuk menambahkan konfigurasi alamat IP Lokal dan Peer-nya.

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

- 4) Setelah ditambahkan alamat IP dan alamat IP Peer-nya, pilih "Phase 2 proposal" yang sesuai dengan alat peer-nya dengan mengklik tombol **Add**.

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) ⓘ

Add Connection

Auth Method: ☒ Pre-shared key ☐ RSA-signed certificate

Shared Key:

Confirm Key:

Local Link: eth1(unifiunifi) ⓘ

Encrypted Traffic

+ Add - Delete

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

Save

Cancel

5) Lalu ke bagian **IKE Options**, konfigurasi IKE phase 1.

Add Connection

Basics IKE Options OthersIKE Version: ☒ IKEv1 ☐ IKEv2 ⓘMode: ☒ Main mode ☐ Aggressive modeInitiate Connection: ☒ Enable ☐ Disable

Local ID Type: IP Address (IPv4_ADDR) ▾

Local ID:

Peer ID Type: IP Address (IPv4_ADDR) ▾

Peer ID:

IKE SA Timeout(s):

3600

DH Group:

group 2 ▾

DPD: ☒ Enable ☐ Disable ⓘ

Save

Cancel

Add Connection

DH Group: group 2 ▾

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):

30

Max Attempts:

5

Phase 1 Proposal:

3DES ▾

MD5 ▾

Add

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

1/16 entries ⓘ

Save

Cancel

6) Tahap terakhir, pada Others konfigur Phase 2 SA Timeout.

Add Connection ×

Basics IKE Options Others

Max Attempts:

ⓘ

IPSec SA Timeout(s):

Expiration Time:

☐ Enable ☒ Disable

Save

Cancel

BAB 3 Perhatian

1. Pastikan pengaturan pada lokal dan peer device secara konsisten
2. Pastikan UDP500 dan UDP4500 antara kedua alat dapat berkomunikasi dengan normal atau tidak dapat berkomunikasi.
3. Rekomendasi untuk lifetime adalah 28800 detik pada phase one dan phase two. Jika lifetime menggunakan 3600 detik, koneksi akan berakhir lebih cepat.
4. Sewaktu percobaan pada LAN, asal IP dan tujuan IP harus sesuai dengan lokal dan Peer IP yang dikonfigur dalam **Encrypted Traffic, otherwise**, atau data tidak akan dapat melalui VPN tunnel.
5. Mode Bridge tidak mendukung IPSec VPN.
6. Sebelum mengkonfigurasi IPSec VPN pada NGAF, Anda perlu mengaktifkan VPN Service pada **Network> IPsec VPN> Status**.
7. Pastikan NGAF memiliki lisensi untuk VPN.



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