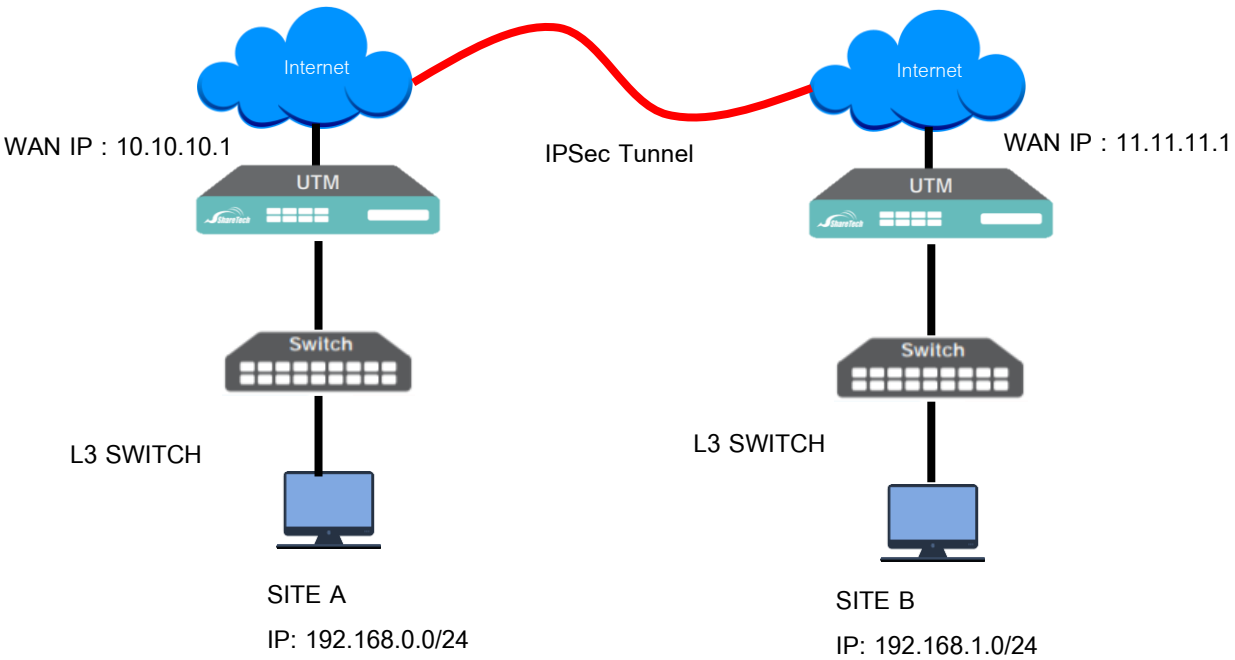
IPSec VPN



IPSec VPN เป็น VPN แบบ Site to Site คือต้องมีอุปกรณ์สองตัวมาเชื่อมต่อกัน โดยเครื่องคอมพิวเตอร์ ทั้งสอง Site ไม่ต้อง Setup ใดๆทั้งสิ้น จะง่ายต่อการใช้งานและมีความปลอดภัยสูง

Support : support.th@nit.co.th
Sales : rung@nit.co.th
Mobile : 081=985-6916
Web : www.netinfortech.co.th
Line : nit.sharetech

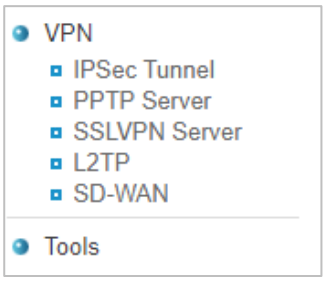
การ Setting จะต้องทำการ Setting ให้เหมือนกันทั้ง 2 Site ดัง ดังนั้นเราต้องกำหนดค่าต่างๆ ขึ้นมาก่อนทั้งสอง Site เพื่อป้องกันการผิดพลาด ตัวอย่างตาม ตารางด้านล่าง

	Site A	Site B
WAN IP	10.10.10.1	11.11.11.1
LAN Subnet	192.168.0.0/24	192.168.1.0/24
IKE Setting (Phase 1)		
IKE	V1	V1
Connection Type	Main	Main
Preshare Key	123456789	123456789
ISAKMP / DH Group	AES / SHA-1 Group 2	AES / SHA-1 Group 2
IKE SA Lifetime	3	3
IPSec Setting (Phase 2)		
IPSec	AES/SHA-1	AES/SHA-1
Perfect Forward Secrecy (PFS)	No	No
IPSec SA Lifetime	3	3

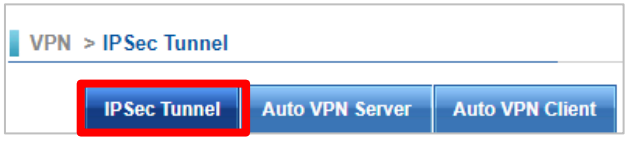
ขั้นตอนแรกให้เข้าไป Setting ที่ Site A ก่อน

Site A (IPSec VPN Setting)

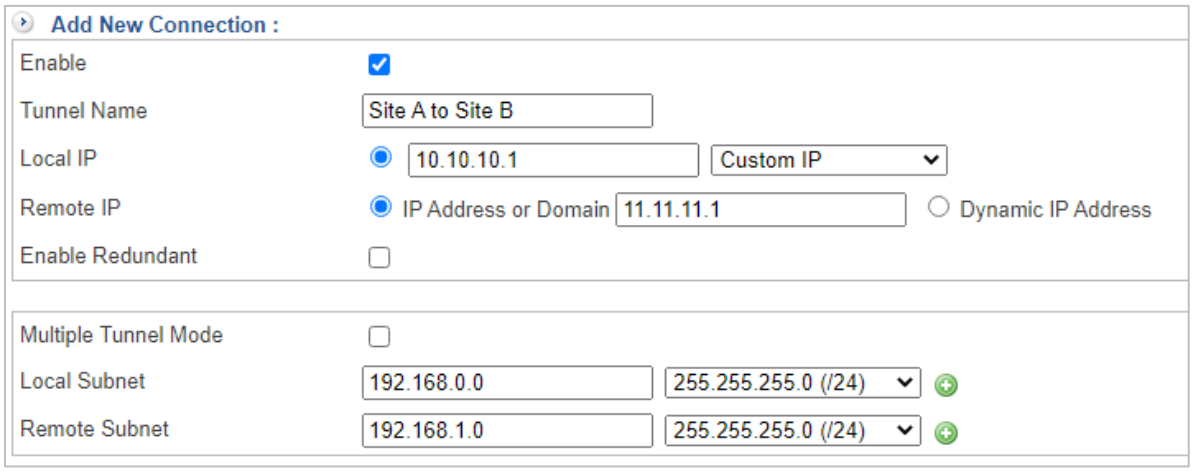
1.เข้าเมนู VPN



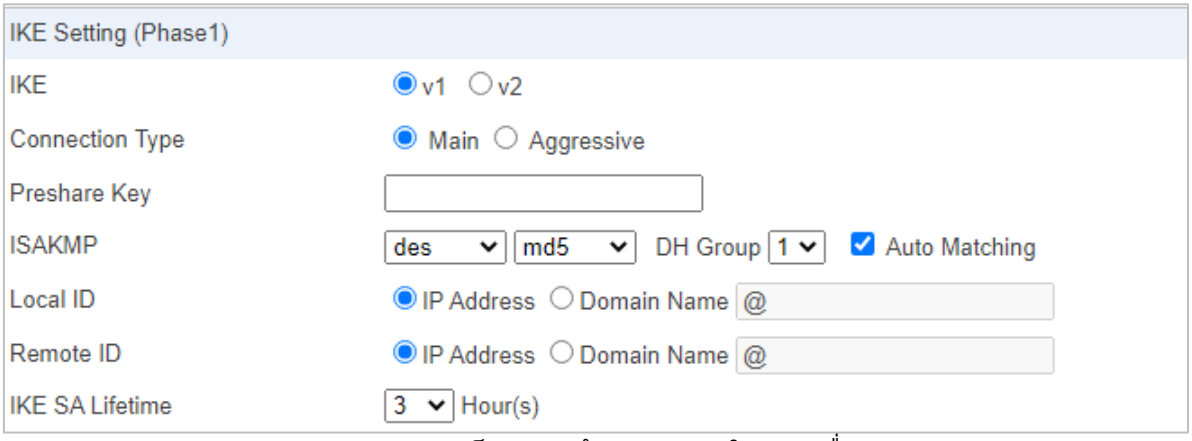
2.เลือกเมนูย่อย IPSec Tunnel



3.กดปุ่ม Add เพื่อสร้าง Tunnel หลังจากนั้นให้กำหนดค่าตาม ตารางที่เรากำหนดไว้

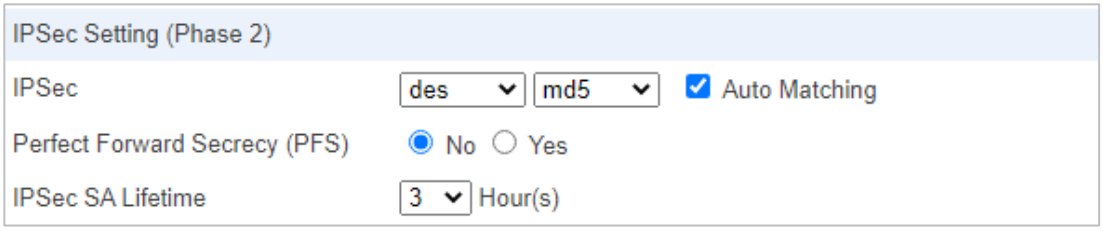


- Enable ให้คลิกถูก
- Tunnel Name ให้ใส่ชื่อของ Tunnel ที่สื่อความหมาย
- Local IP เป็น WAN IP Address ของ Site A ต.ย 10.10.10.1
- Remote IP เป็น WAN IP Address ของ Site B ต.ย 11.11.11.1
- Local Subnet ให้ใส่ LAN IP Subnet ของ Site A ต.ย 192.168.0.0 เลือก Netmask เป็น 255.255.255.0(/24) หรือตามที่ใช้งานจริง
- Remote Subnet ให้ใส่ LAN IP Subnet ของ Site B ต.ย 192.168.1.0 เลือก Netmask เป็น 255.255.255.0(/24) หรือตามที่ใช้งานจริง

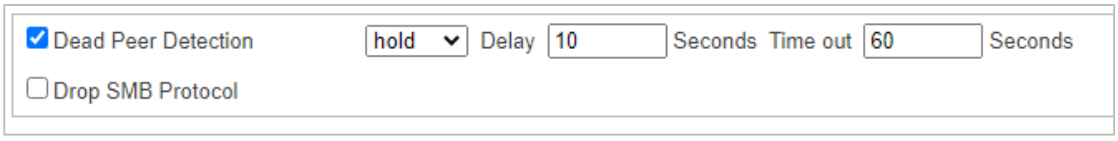


- IKE Setting (Phase 1) เป็นการสร้างช่องทางในการเชื่อมต่อระหว่าง Site A กับ B
  - IKE ให้เลือก V1
  - Connection Type ให้เลือก Main

- Preshare Key ให้ใส่ตามที่กำหนด เช่น 123456789
- ISAKMP ให้เลือกตามที่เรากำหนดไว้เช่น AES/SHA-1 DH Group 2
- IKE SA Lifetime เลือก 3 Hour(s) เป็นการกำหนดเวลาของการเชื่อมต่อว่าเชื่อมต่อไปนานกี่ชั่วโมง ถึงจะทำการสร้างการเชื่อมต่อใหม่ เพราะถ้ากำหนดไว้หลายชั่วโมงอาจจะทำให้โดน Attack ได้ค่าที่เหมาะ (1-8 Hour)



- IPSec Setting (Phase 2) เป็นขั้นตอนการเข้ารหัสข้อมูล (Encryption) หลังจากที่มีการสร้าง Tunnel ใน Phase 1 เรียบร้อยแล้ว
  - IPSec เลือก AES/SHA-1
  - Perfect Forward Secrecy (PFS) เลือก No
  - IPSec SA Lifetime เลือก 3 Hour(s) เป็นการหมดอายุของการ Encryption



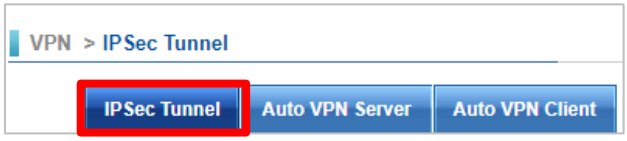
- ใช้ค่าตาม Default

4.กดปุ่ม Add เสร็จการ Setting ของ Site A ให้ไป Setting ที่ Site B

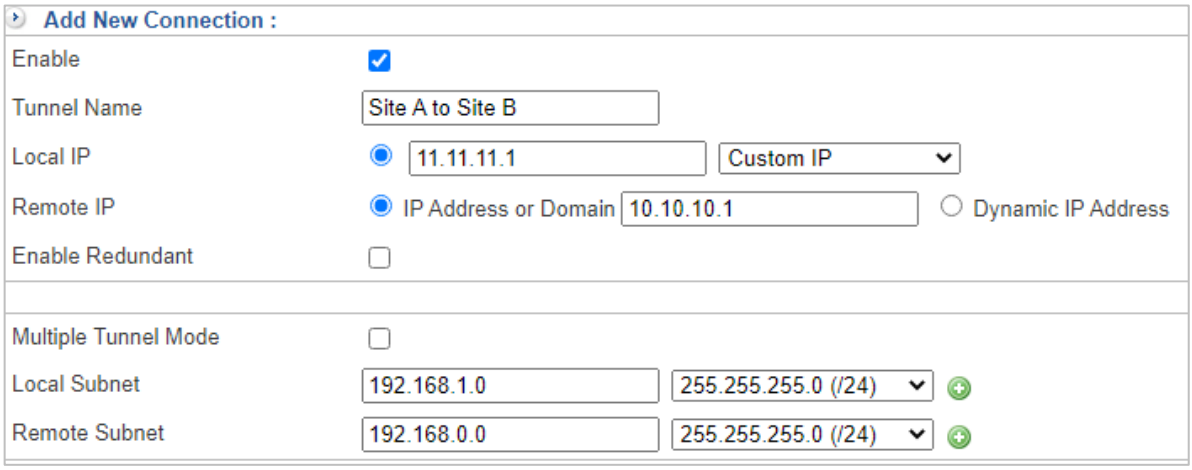
Site B (IPSec VPN Setting)

1.เข้าเมนู VPN

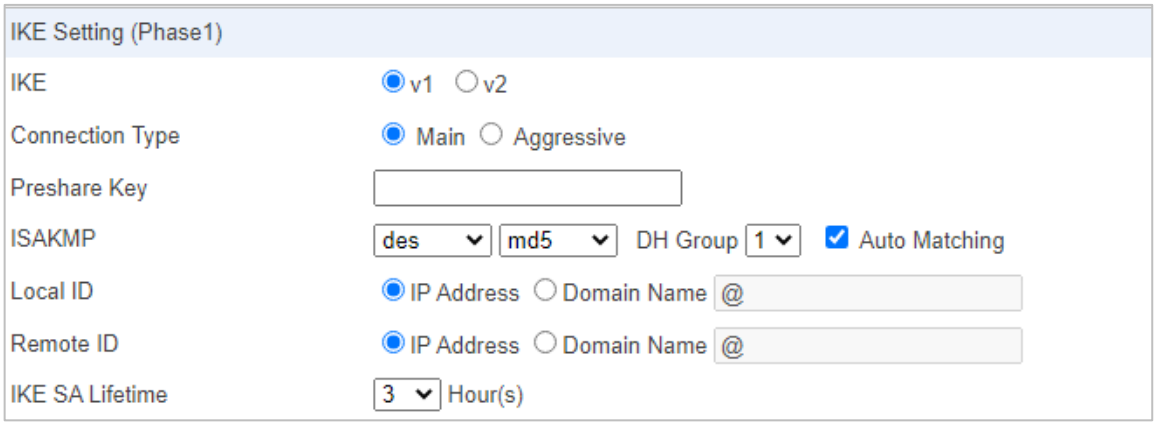
2.เลือกเมนูย่อย IPSec Tunnel



3.กดปุ่ม Add เพื่อสร้าง Tunnel หลังจากนั้นให้กำหนดค่าตาม ตารางที่เรากำหนดไว้

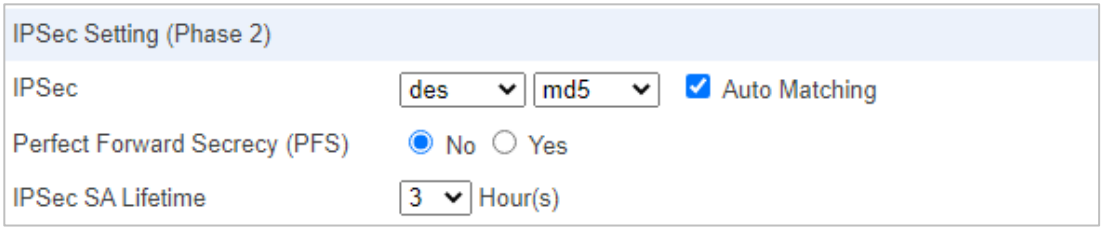


- Enable ให้คลิกถูก
- Tunnel Name ให้ใส่ชื่อของ Tunnel ที่สื่อความหมาย
- Local IP เป็น WAN IP Address ของ Site B ต.ย 11.1.11.1
- Remote IP เป็น WAN IP Address ของ Site A ต.ย 10.10.10.1
- Local Subnet ให้ใส่ LAN IP Subnet ของ Site B ต.ย 192.168.1.0 เลือก Netmask เป็น 255.255.255.0(/24) หรือตามที่ใช้งานจริง
- Remote Subnet ให้ใส่ LAN IP Subnet ของ Site A ต.ย 192.168.0.0 เลือก Netmask เป็น 255.255.255.0(/24) หรือตามที่ใช้งานจริง

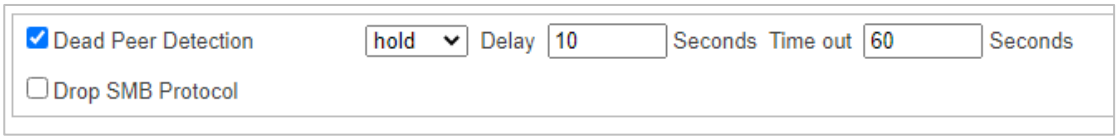


- IKE Setting (Phase 1) เป็นการสร้างช่องทางในการเชื่อมต่อระหว่าง Site A กับ B
  - IKE ให้เลือก V1
  - Connection Type ให้เลือก Main

- Preshare Key ให้ใส่ตามที่กำหนด เช่น 123456789
- ISAKMP ให้เลือกตามที่เรากำหนดไว้เช่น AES/SHA-1 DH Group 2
- IKE SA Lifetime เลือก 3 Hour(s) เป็นการกำหนดเวลาของการเชื่อมต่อว่าเชื่อมต่อไปนานกี่ชั่วโมง ถึงจะทำการสร้างการเชื่อมต่อใหม่ เพราะถ้ากำหนดไว้หลายชั่วโมงอาจจะทำให้โดน Attack ได้ค่าที่เหมาะ (1-8 Hour)



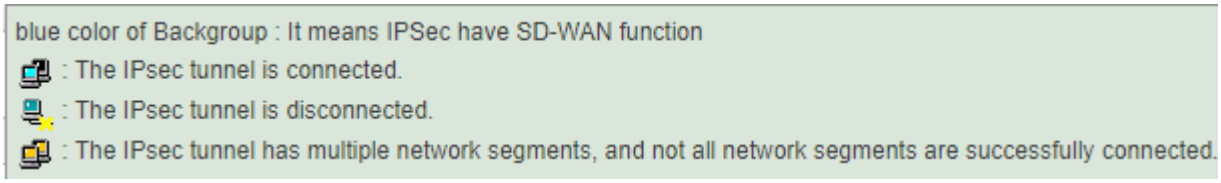
- IPSec Setting (Phase 2) เป็นขั้นตอนการเข้ารหัสข้อมูล (Encryption) หลังจากที่มีการสร้าง Tunnel ใน Phase 1 เรียบร้อยแล้ว
  - IPSec เลือก AES/SHA-1
  - Perfect Forward Secrecy (PFS) เลือก No
  - IPSec SA Lifetime เลือก 3 Hour(s) เป็นการหมดอายุของการ Encryption



- ใช้ค่าตาม Default

4.กดปุ่ม Add เสร็จการ Setting

เมื่อ Setting ทั้งสอง Site แล้ว IPSec VPN จะเริ่มดำเนินการเชื่อมต่อ ถ้า Setting ไม่ผิดที่ IPSec Tunnel จะแสดงสถานการณ์เชื่อมต่อ



เชื่อมต่อสำเร็จ

เชื่อมต่อไม่สำเร็จ

IPSec จะแสดงว่าบาง Subnet ไม่สามารถเชื่อมต่อได้ สาเหตุ Network ของ Subnet นั้นหลุดหรือชนกันระหว่าง Site (Exp. มีการเชื่อมต่อ (Route) อยู่แล้ว)

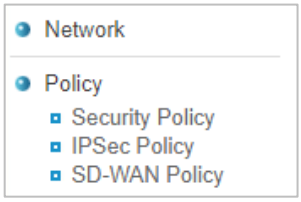
ข้อระมัดระวัง

การใช้งาน IPSec VPN จะไม่มี IP Subnet ซ้ำกันเด็ดขาด

ขั้นตอนถัดไป ถึงแม้นว่า Tunnel จะสามารถเชื่อมต่อกันได้แล้ว ก็ยังไม่สามารถรับส่งข้อมูลหากันระหว่าง Site ได้ จะต้องทำการสร้าง Policy อนุญาตให้รับส่งข้อมูลหากันได้ก่อน

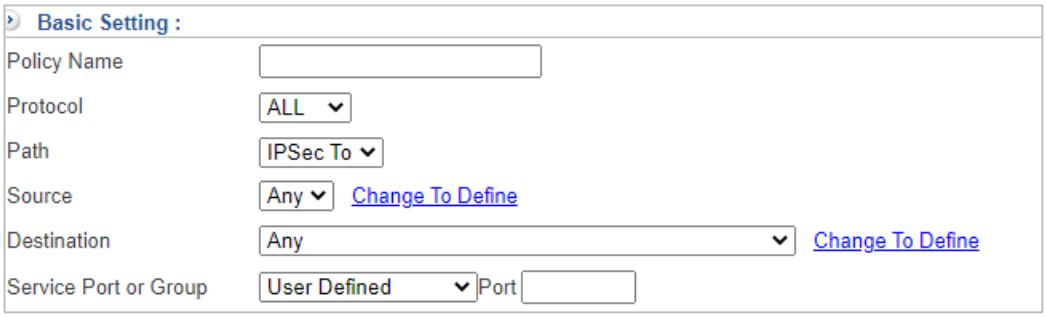
Policy

1.เข้าเมนู Policy



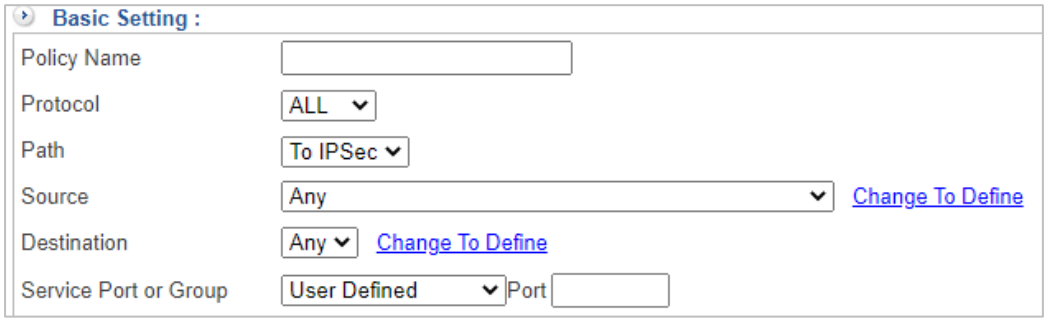
2.เลือก IPSec Policy และกดปุ่ม Add เพื่อสร้าง Policy ให้ทำการสร้าง 2 Policy

- อนุญาติจาก IPSec Tunnel เข้ามาที่ LAN



  - ใส่ Policy name
  - Path เลือก IPSec To ความหมายคืออนุญาตจาก IPSec ไป LAN
  - ถ้าไม่มีการกำหนดเงื่อนไขอื่นๆ เช่น ไปหากลุ่มของ LAN IP ให้กดปุ่ม Add

- อนุญาตจาก LAN ไปที่ IPSec Tunnel



  - ใส่ Policy name
  - Path เลือก IPSec To ความหมายคืออนุญาตจาก IPSec ไป LAN
  - ถ้าไม่มีการกำหนดเงื่อนไขอื่นๆ เช่น ไปหากลุ่มของ LAN IP ให้กดปุ่ม Add

เท่านี้ก็สามารถใช้งานรับส่งข้อมูลที่ปลอดภัยผ่าน IPSec VPN ได้แล้ว