

คู่มือการตั้งค่า IPsec VPN บน Mac OS

ด้วยโปรแกรม FortiClient VPN

การเชื่อมต่อ RMUTT-IPsec

1. บทนำและวัตถุประสงค์

เอกสารฉบับนี้จัดทำขึ้นเพื่อใช้เป็นคู่มืออ้างอิงสำหรับการตั้งค่าการเชื่อมต่อ IPsec VPN ผ่านโปรแกรม FortiClient สำหรับผู้ใช้งานที่ต้องการเชื่อมต่อเข้าสู่เครือข่ายภายในองค์กรจากภายนอกอย่างปลอดภัย

ข้อกำหนดเบื้องต้น (Prerequisites)

- ติดตั้งโปรแกรม FortiClient เรียบร้อยแล้วบนเครื่องคอมพิวเตอร์
- มีข้อมูล Remote Gateway (Server Address) ของหน่วยงาน
- มี Pre-shared Key (รหัสลับที่ใช้ร่วมกันระหว่างไคลเอนต์และเกตเวย์) ที่ได้รับจากผู้ดูแลระบบ
- มีบัญชีผู้ใช้งาน (Username/Password) สำหรับ Authentication (EAP) ในการล็อกอินเข้าใช้งาน VPN
- เครื่องคอมพิวเตอร์เชื่อมต่ออินเทอร์เน็ตได้ปกติ และไม่มีไฟร์วอลล์ปิดกั้นพอร์ต UDP 500 / 4500
- Download** https://drive.google.com/file/d/1W0gnN_WwqoWsZaU-ajdJJJe6pwlN5GzrG/view?usp=sharing

2. ขั้นตอนการตั้งค่า

2.1 การสร้างการเชื่อมต่อและระบุ Remote Gateway

ขั้นตอนที่ 1 เปิดโปรแกรม FortiClient แล้วไปที่เมนู REMOTE ACCESS ทางด้านซ้ายมือ

ขั้นตอนที่ 2 เลือกแท็บ IPsec VPN แล้วกดเพิ่มการเชื่อมต่อใหม่ (Add a new connection) เพื่อเปิดหน้าต่าง EDIT VPN

ขั้นตอนที่ 3 กรอกข้อมูลตามรายละเอียดด้านล่าง:

ADD VPN

SSL VPN | **IPsec VPN** | XML

Connection Name: RMUTT-IPSec

Description:

Remote Gateway: 202.44.130.19

+ Add Gateway

Authentication Method: Pre-shared Key

Authentication (EAP): ☒ Prompt on login ☐ Save login ☐ Disable

Single Sign On: ☐ Enable Single Sign On (SSO) for VPN Tunnel

VPN Settings

IKE: ☐ Version1 [Unsupported] ☒ Version2

Address Assignment: ☒ Mode Config ☐ Manually Set [Unsupported]

☐ DHCP over IPsec [Unsupported]

Cancel Save

ตารางที่ 1: ข้อมูลการเชื่อมต่อพื้นฐาน

พารามิเตอร์	ค่าที่กำหนด
Connection Name	RMUTT-IPSec
Description	(เว้นว่างได้)
Remote Gateway	202.44.130.19
Authentication Method	Pre-shared key
Pre-shared Key	IPSEC@RMUTT@2026\$
Authentication (EAP)	Prompt on login

พารามิเตอร์	ค่าที่กำหนด
Failover SSL VPN	[None]
Single Sign-On (SSO)	ไม่เปิดใช้งาน (Disable)

2.2 การตั้งค่า VPN Settings

ขั้นตอนที่ 4 เลื่อนลงมาที่ส่วน VPN Settings แล้วตรวจสอบ/กำหนดค่าดังนี้:

VPN Settings

IKE
☐ Version1 [Unsupported]
☒ Version2

Address Assignment
☒ Mode Config
☐ Manually Set [Unsupported]

☐ DHCP over IPsec [Unsupported]

Encapsulation
☒ IKE UDP Port
☐ IPsec over TCP

☐ Auto (UDP fallback TCP)

IKE UDP Port

ตารางที่ 2: VPN Settings

พารามิเตอร์	ค่าที่กำหนด
IKE	Version 2
Address Assignment	Mode Config
Encapsulation	IKE UDP Port
IKE UDP Port	4500

*ค่าที่เหลือตั้งแต่ข้อ 2.3 โดยปกติจะเป็นค่า default ไม่จำเป็นต้องตั้งค่าใดๆอีก แต่หาก VPN ไม่ได้ให้ตรวจสอบว่า ค่า default ตรงกับเอกสารนี้หรือไม่

2.3 การตั้งค่า Phase 1 (IKE Proposal และ DH Group)

ขั้นตอนที่ 5 กำหนดค่าการเข้ารหัสและการยืนยันตัวตนของ Phase 1 โดยระบบรองรับการเสนอค่าหลายชุด (Proposal) เพื่อให้ตรงกับฝั่งเกตเวย์อย่างน้อยหนึ่งชุด:

ตารางที่ 3: Phase 1 — IKE Proposal

พารามิเตอร์	ค่าที่กำหนด
Encryption (ชุดที่ 1)	AES128
Authentication (ชุดที่ 1)	SHA1
Encryption (ชุดที่ 2)	AES256
Authentication (ชุดที่ 2)	SHA256
DH Group	14
Key Life	86400 วินาที
Local ID	Optional (เว้นว่าง)

หมายเหตุ: DH Group 20 หมายถึง ECP384 (Elliptic Curve) ซึ่งให้ระดับความปลอดภัยสูงกว่ากลุ่มแบบ MODP ทั่วไป ควรเลือกให้ตรงกับที่ฝั่ง FortiGate (เกตเวย์ปลายทาง) กำหนดไว้

2.4 การตั้งค่า Dead Peer Detection

ขั้นตอนที่ 6 ตรวจสอบการตั้งค่าเพิ่มเติมก่อนเข้าสู่ Phase 2:

ตารางที่ 4: การตั้งค่าเพิ่มเติม

พารามิเตอร์	ค่าที่กำหนด
Local ID	Optional (เว้นว่าง)
Dead Peer Detection (DPD)	เปิดใช้งาน (Enable)

Dead Peer Detection (DPD) ใช้สำหรับตรวจสอบสถานะของอีกฝั่งของอุโมงค์ VPN อย่างต่อเนื่อง หากตรวจพบว่าอีกฝั่งไม่ตอบสนอง ระบบจะยกเลิกและสร้างการเชื่อมต่อใหม่โดยอัตโนมัติ

2.5 การตั้งค่า Phase 2 (IKE Proposal, Key Life, PFS)

ขั้นตอนที่ 7 กำหนดค่าการเข้ารหัสของ Phase 2 (ใช้สำหรับเข้ารหัสข้อมูลที่วิ่งผ่านอุโมงค์จริง) และกำหนดอายุของคีย์ (Key Life):

ตารางที่ 5: Phase 2 — IKE Proposal และ Key Life

พารามิเตอร์	ค่าที่กำหนด
Encryption (ชุดที่ 1)	AES128
Authentication (ชุดที่ 1)	SHA1
Encryption (ชุดที่ 2)	AES256
Authentication (ชุดที่ 2)	SHA256
Key Life (Seconds)	43200 วินาที (เปิดใช้งาน)
Key Life (KBytes)	5120 KB (ไม่เปิดใช้งาน)
Enable Replay Detection	เปิดใช้งาน
Enable Perfect Forward Secrecy (PFS)	เปิดใช้งาน

พารามิเตอร์	ค่าที่กำหนด
DH Group (PFS)	14

Perfect Forward Secrecy (PFS) ช่วยให้แต่ละเซสชันของ Phase 2 ใช้คีย์ที่คำนวณขึ้นใหม่โดยไม่ขึ้นกับคีย์ของ Phase 1 หากคีย์ใดคีย์หนึ่งรั่วไหลในภายหลัง จะไม่กระทบต่อเซสชันอื่นที่เข้ารหัสไว้ก่อนหน้านี้

ขั้นตอนที่ 8 เมื่อกำหนดค่าครบถ้วนแล้ว กดปุ่ม Save เพื่อบันทึกการตั้งค่า

ขั้นตอนที่ 9 กลับไปที่หน้ารายการ VPN Connection เลือกการเชื่อมต่อ RMUTT-IPSec แล้วกด Connect จากนั้นกรอก Username และ Password ตามที่ได้รับจากผู้ดูแลระบบเพื่อยืนยันตัวตน (EAP)

3. ตารางสรุปค่าพารามิเตอร์ทั้งหมด

สรุป Phase 1 และ Phase 2

พารามิเตอร์	ค่าที่กำหนด
IKE Version	2
Encapsulation / Port	IKE UDP Port 500
Phase 1 Encryption/Auth	AES128-SHA1, AES256-SHA256
Phase 1 DH Group	14
Phase 1 Key Life	86400 วินาที
Phase 2 Encryption/Auth	AES128-SHA1, AES256-SHA256
Phase 2 Key Life	43200 วินาที
PFS / DH Group	เปิดใช้งาน / กลุ่ม 14
Dead Peer Detection	เปิดใช้งาน