

คู่มือการตั้งค่าและใช้งาน VPN บน Fortinet FortiGate 200F

สำหรับผู้ดูแลระบบเครือข่ายของหน่วยงานภาครัฐและโรงพยาบาล

☐ ส่วนที่ 1: ประเภทของ VPN ที่ FortiGate รองรับ

1. SSL VPN (Remote Access): สำหรับให้ผู้ใช้ภายนอกเชื่อมต่อเข้าสู่ระบบภายในผ่าน FortiClient หรือ Web Portal
2. IPSec VPN (Site-to-Site): สำหรับเชื่อมต่อระหว่างสำนักงาน/โรงพยาบาล 2 แห่งเข้าหากันผ่านอินเทอร์เน็ต

☐ ส่วนที่ 2: ขั้นตอนการตั้งค่า SSL VPN (Remote Access)

1. เปิดใช้งาน SSL VPN: ไปที่เมนู VPN ☐ SSL-VPN Settings ☐ Listen on Interface: wan1, Port: 10443
2. ตั้งค่า SSL-VPN Portal: VPN ☐ SSL-VPN Portals ☐ Full_Access ☐ IP Range 10.10.10.1-10.10.10.50
3. สร้าง User & Group: User ☐ Add User / Group ☐ SSLVPN_Users
4. สร้าง Firewall Policy: ssl.root ☐ internal, Source: SSLVPN_Users, Destination: All
5. ทดสอบผ่าน FortiClient VPN ☐ Remote Gateway: 203.154.xxx.xxx:10443 ☐ Connect

☐ แผนภาพโครงสร้าง SSL VPN และ IPSec VPN

FortiGate 200F VPN Setup (ฉบับสมบูรณ์)

1. SSL VPN (Remote Access)



1. ตรวจสอบการตั้งค่า SSL VPN → VPN → SSL-V Settings
2. Listen on Interface: WAN
3. Listen Port: 10443
4. Server Certificate (Certificates)
3. บนเครื่อง กราฟิก บรอนซ์ เรกบดง → User Definition Add User
4. Tunnel Mode ติดสลับ
5. Assign an IP Range 10.10.10.1–10.10.10.50
6. DNS Server IP
4. เตรียมสาขาขมรก → SSLVPN_Users รายให้เดา SSLVINues
1. Policy & Objects → IPv4 Policy → Add New
2. Incoming Interface: ssl.root, Outgoing Interface: internal
3. Source: SSLVPN_Users, Destination: All, Action: ACCEPT
5. ทบท FortiClient

2. IPSec VPN (Site-to-Site)



☐ ส่วนที่ 3: ขั้นตอนการตั้งค่า IPSec VPN (Site-to-Site)

ตัวอย่างการเชื่อมต่อระหว่างสำนักงานใหญ่ (HQ) ☐ โรงพยาบาลชุมชน (Branch)

HQ IP WAN: 203.154.10.1 / LAN: 192.168.1.0/24

Branch IP WAN: 203.154.20.1 / LAN: 192.168.2.0/24

1. สร้าง Phase 1: VPN ☐ IPSec Tunnels ☐ Custom ☐ ตั้งค่า Remote Gateway, Pre-shared Key
2. สร้าง Phase 2: ระบุ Local/Remote Subnet และ Encryption
3. เพิ่ม Firewall Policy: LAN ☐ VPN และ VPN ☐ LAN
4. เพิ่ม Static Route: ปลายทาง 192.168.2.0/24 ผ่าน Tunnel

☐ ส่วนที่ 4: ตรวจสอบสถานะและคำสั่ง CLI

ใช้คำสั่งต่อไปนี้เพื่อตรวจสอบสถานะ VPN:

diagnose vpn tunnel list

diagnose vpn ike gateway list

☐ เคล็ดลับเพิ่มเติม

- ใช้ FortiAnalyzer หรือ FortiCloud ตรวจสอบการเชื่อมต่อ VPN และ Log
- ตรวจสอบ MTU และ Split Tunnel หากผู้ใช้บางรายเชื่อมต่อได้แต่ใช้งานช้า

จัดทำโดย: ผู้เชี่ยวชาญระบบเครือข่ายและความปลอดภัย Fortinet

สำหรับการใช้งานภายในสำนักงานสาธารณสุขจังหวัดตราด และโรงพยาบาลชุมชนในสังกัด