

## IPSec Road Warrior / Mobile Client

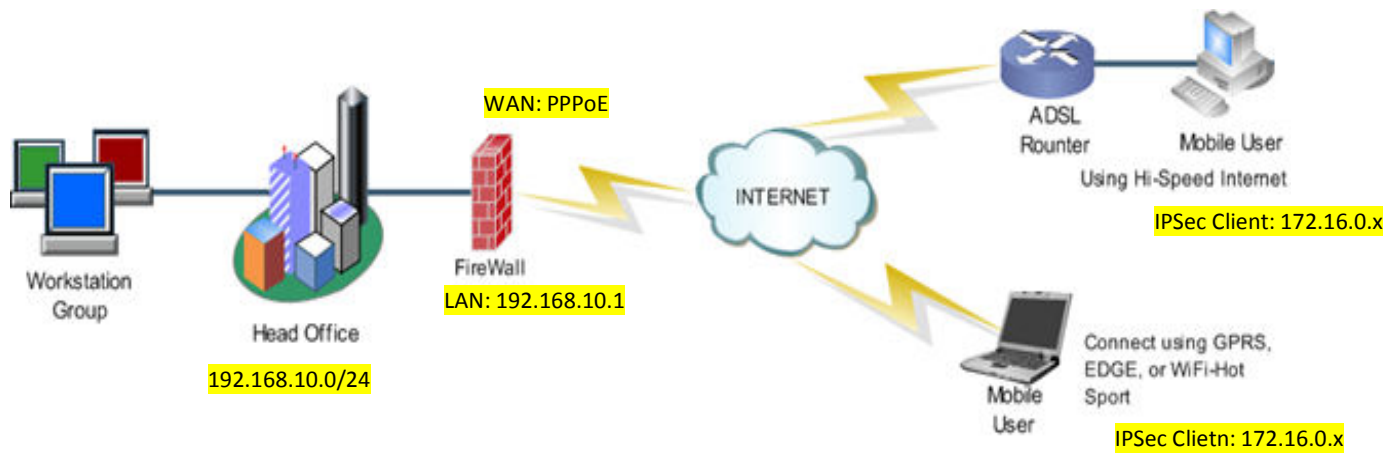
Sunday, November 07, 2010  
11:51 PM

### ! ข้อกำหนดเบื้องต้น

- ADSL Modem - Bridge Mode
- ลงทะเบียน Dynamic DNS
- Non-Overlapping IP Address

### ! ขั้นตอนการติดตั้ง

- ติดตั้ง LAN Interface
- ติดตั้ง WAN Interface
- ติดตั้ง Dynamic DNS Client
- Enable IPSec Tunnels
  - Allow Mobile Client
  - Phase 1 Configuration
  - Phase 2 Configuration
  - Pre-shared Keys
- สร้าง IPSec Firewall Rules
- สร้าง Static Routes
- Mobile IPSec Configuratin
  - Shrew Soft VPN Client [www.shrew.net](http://www.shrew.net)



# IPsec Road Warrior/Mobile Client How-To

---

Road Warrior หรือ Mobile IPsec Client มีเทคนิคการติดตั้งและใช้งานได้ง่ายๆ แต่ที่ส่วนที่สำคัญคือต้องแน่ใจว่าการกำหนดค่าต่างๆ ทั้ง Server & Client จะต้องสัมพันธ์กัน โดยมีขั้นตอนดังต่อไปนี้

## pfSense Configuration

1. ที่หน้าจอ WebGUI ไปที่ VPN > IPsec, Tunnels

- Check Enable IPsec
- Save

2. ที่แท็บ VPN > IPsec, Mobile Clients

เลือก Allow Mobile Clients และกำหนดค่าต่างๆ ดังต่อไปนี้

Phase 1 Proposal (authentication):

- Negotiation Mode : Aggressive
- Server Identifier : My IP Address
- Encryption Algorithm : 3DES
- Hash Algorithm : SHA1
- DH Key Group : 2
- Lifetime : 86400
- Authentication Method : Pre-Shared Key

Phase 2 Proposal (SA/Key Exchange)

- Protocol : ESP
- Encryption Algorithms : 3DES, Blowfish, CAST128, Rijndael (AES)
- Hash Algorithms : SHA1, MD5
- PFS Key Group : Off
- Lifetime : 3600
- คลิก Save

### 3. ทำการสร้าง Pre-Shared Keys

- คลิกที่แท็บ VPN > IPsec, Pre-Shared Keys
- คลิกเครื่องหมาย "+" เพื่อทำการสร้าง PSK ใหม่
- Identifier : ใส่ E-mail address, เช่น yourname@yourdomain.com
- Pre-shared Key : กำหนดรหัสผ่าน ควรประกอบไปด้วย ตัวหนังสือ เล็ก-ใหญ่ และ สัญลักษณ์ต่าง ๆ
- คลิก Save

### 4. สร้าง Firewall Rules > IPsec

IPsec - Firewall Rules	
Action	Pass
Interface	IPSEC
Protocol	Any
Source	Any
Source OS	Any
Destination	Any
Log	Check
Gateway	Default
Description	Allow all traffic pass IPsec VPN

### 5. สร้าง Static Route เพื่อให้ LAN Subnet ของ Server สามารถ Routing ไปยัง LAN Subnet ของ Mobile Client ได้อย่างถูกต้อง

ทำการตรวจสอบ Service โดยไปที่ Status > Services ต้องแน่ใจว่า IPsec/Racoon service กำลังทำงานอยู่

## Client Configuration

สำหรับ Mobile IPsec Client ตามตัวอย่างนี้จะใช้โปรแกรม Shrew Soft VPN Client ซึ่ง เป็น Freeware รองรับการเชื่อมต่อ IPsec มาตรฐานเป็นอย่างดี สามารถ Download ได้ที่ [www.shrew.net](http://www.shrew.net)

Shrew Soft Client Config:

### 1. General Tab:

- Host: <ใส่ WAN IP ของ pfSense Box หรือ Host เช่น sitea.dyndns.biz>
- Port: 500
- Auto Configuration: Disabled
- Adapter: Use virtual adapter and assigned address
- Address: (ใส่ random range ที่เราไม่ได้ใช้งาน เช่น 172.16.0.x)
- Netmask: 255.255.255.0

### 2. Client Tab:

- ไม่ต้องเปลี่ยนแปลงค่าใดๆ

### 3. Name Resolution Tab:

- Uncheck Enable WINS
- Uncheck Enable DNS

### 4. Authentication Tab:

- Authentication Method: Mutual PSK
- Local Identity:  
Type: Key Identifier  
Key ID: E-mail address
- Remote Identity:  
Identification Type: IP Address  
 Use Discovered remote host address
- Credentials:  
Pre Shared Key: (PSK on server for this e-mail address)

### 5. Phase 1:

- Exchange Type: aggressive
- DH Exchange: Group 2
- Cipher Algorithm: 3DES
- Hash Algorithm: SHA1

- Key Life Time: 86400

#### 6. Phase 2:

- Transform Algorithm: esp-3des
- HMAC Algorithm: SHA1
- PFS: DisabledCompress: disabled
- Compress Algorithm: disabled
- Key Life Time: 3600
- Key Life Data Limit: 0

#### 7. Policy:

- UNCHECK Obtain Topology Automatically
- Click Add
- Type: Include
- Address: (ใส่ Network ด้านหลัง pfSense Box ที่เราต้องการ Access เช่น 192.168.10.0)
- Netmask: 255.255.255.0 (หรือ Netmask ใดๆ สำหรับ network นั้น)