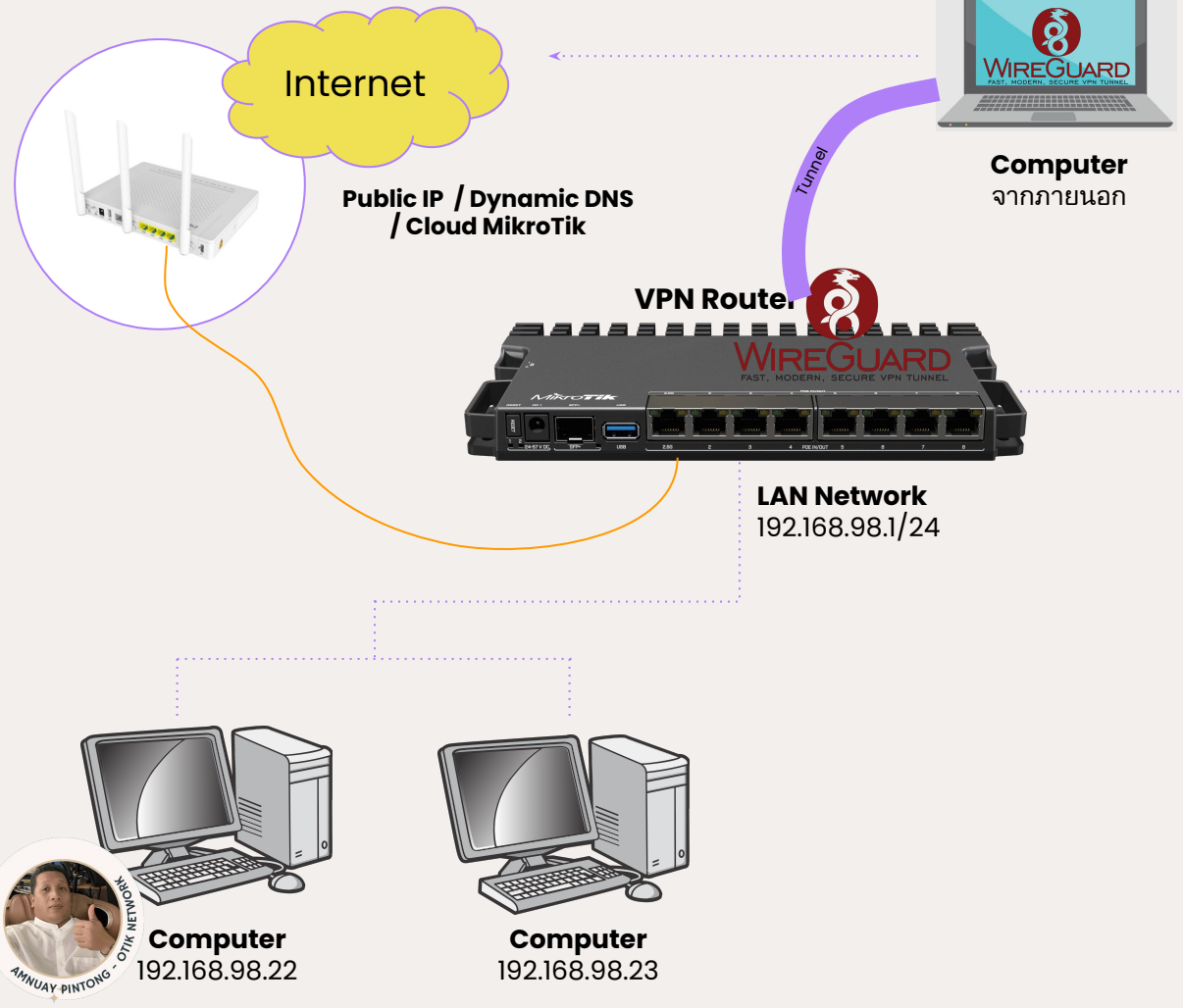
Site to Site

WireGuard

ROS7 & Windows

Client to Site

WIREGUARD
FAST, MODERN, SECURE VPN TUNNEL


Internet
Public IP / Dynamic DNS
/ Cloud MikroTik
Tunnel
Computer
จากภายนอก
VPN Router
WireGuard
FAST, MODERN, SECURE VPN TUNNEL
LAN Network
192.168.98.1/24
ACCOUNTING SYSTEM
(Express, WinSpeed, อื่นๆ)
192.168.98.4
ShareData Center
(แชร์ไฟล์กลาง)
192.168.98.31
Computer
192.168.98.22
Computer
192.168.98.23
AMNUAY PINTONG - OTIK NETWORK
WireGuard
FAST, MODERN, SECURE VPN TUNNEL

VPN?

PPTP VPN | OPEN VPN | SSTP VPN | IPSEC VPN | L2TP VPN | WIREGUARD VPN...

VPN คืออะไร?

คำจำกัดความ:

VPN (Virtual Private Network) คือเครือข่ายเสมือนที่ช่วยสร้างการเชื่อมต่อที่ปลอดภัยและเข้ารหัสระหว่างอุปกรณ์ของคุณและเซิร์ฟเวอร์ระยะไกลผ่านอินเทอร์เน็ต

WIREGUARD
FAST, MODERN, SECURE VPN TUNNEL

VPN คืออะไร? วัตถุประสงค์:

- ปกป้องข้อมูลจากการถูกดักจับ
- มอบความเป็นส่วนตัวออนไลน์ด้วยการซ่อน IP Address
- ช่วยให้เข้าถึงทรัพยากรเครือข่ายเหมือนอยู่ในเครือข่ายเดียวกัน

WIREGUARD
FAST, MODERN, SECURE VPN TUNNEL

VPN คืออะไร? การทำงาน:

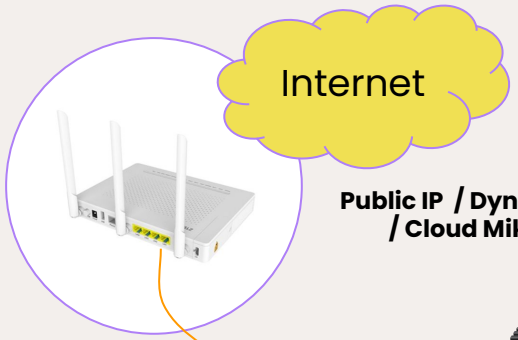
- อุปกรณ์ของคุณเชื่อมต่อกับเซิร์ฟเวอร์ VPN
- ข้อมูลจะถูกเข้ารหัสและส่งไปยังเซิร์ฟเวอร์อย่างปลอดภัย
- เซิร์ฟเวอร์ทำหน้าที่เป็นตัวกลางระหว่างคุณกับอินเทอร์เน็ต

WIREGUARD
FAST, MODERN, SECURE VPN TUNNEL

VPN คืออะไร? ตัวอย่างการใช้งาน:

- การทำงานระยะไกลที่ปลอดภัย
- การเข้าถึงเนื้อหาที่มีข้อจำกัดทางภูมิศาสตร์
- ปกป้องข้อมูลสำคัญขณะใช้งาน Wi-Fi สาธารณะ

WIREGUARD
FAST, MODERN, SECURE VPN TUNNEL

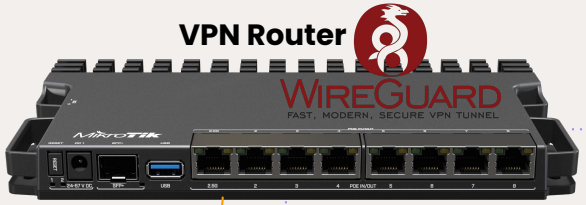


Public IP / Dynamic DNS / Cloud MikroTik

Computer
จากภายนอก

ACCOUNTING SYSTEM
(Express, WinSpeed, อื่นๆ)
192.168.98.4

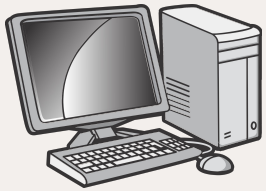
VPN Router



LAN Network
192.168.98.1/24

ShareData Center
(แชร์ไฟล์กลาง)
192.168.98.31

Computer
192.168.98.22



Computer
192.168.98.23

WIREGUARD
FAST, MODERN, SECURE VPN TUNNEL

Introduction

What is WireGuard?

- A modern, secure VPN protocol.
  - Lightweight and efficient.
- Why Use WireGuard?
  - Simplicity and speed.
  - Cross-platform compatibility.

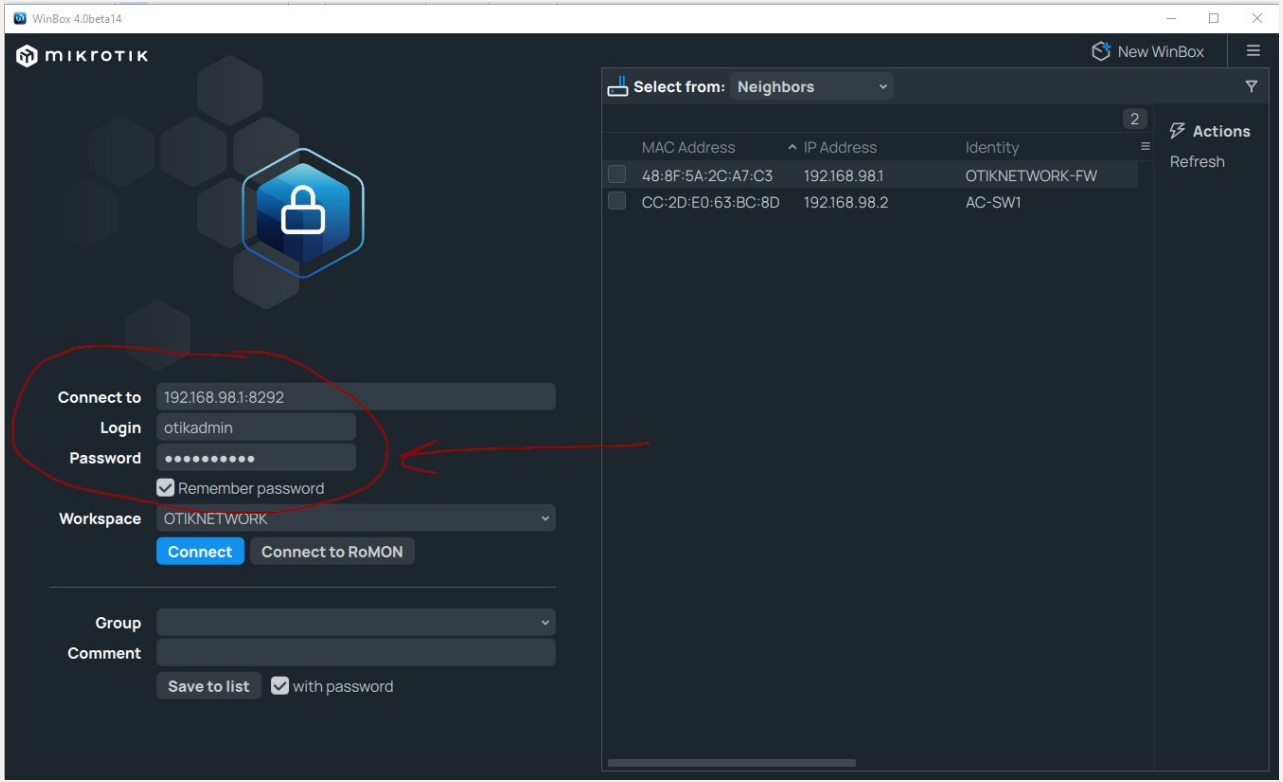
WIREGUARD
FAST, MODERN, SECURE VPN TUNNEL

Requirements

- **Hardware and Software Needed:**
  - MikroTik RouterOS (v7.1 or later).
  - Windows 10/11 client.
  - Network details (IP addresses, subnets).
- **Applications:**
  - WireGuard app for Windows.

WIREGUARD
FAST, MODERN, SECURE VPN TUNNEL

Login MikroTik



Connect to your MikroTik

Configuring MikroTik

Step 1: Enable WireGuard Interface

- Open WinBox/WebFig.
- Go to Interfaces > WireGuard.
- Add a new interface:
  - Name: wg0.
  - Generate Public Key.
  - Assign an IP (e.g., 192.168.88.1/24).

Step 2: Create Peer Configuration

- Go to Interfaces > WireGuard > Peers.
- Add a peer:
  - Public Key: From the Windows client.
  - Allowed IPs: 192.168.88.2/32.

WIREGUARD
FAST, MODERN, SECURE VPN TUNNEL

MikroTik Firewall Rules

1. Allow UDP traffic on port 51820:

```
/ip firewall filter
add chain=input action=accept protocol=udp
dst-port=51820
```

2. Ensure routing is set up for the WireGuard subnet.

WIREGUARD
FAST, MODERN, SECURE VPN TUNNEL

Configuring Windows Client

Step 1: Install WireGuard

- Download from WireGuard Official Site.
- Install and open the application.

Step 2: Configure Interface

- Generate keys in the WireGuard app.
- Set up the interface:
  - Private Key: Generated by the app.
  - Address: 192.168.88.2/24.
  - DNS (Optional): 8.8.8.8.

Step 3: Configure Peer

- Add a new peer configuration:
- **Public Key**: MikroTik's key.
- **Endpoint**: MikroTik's public IP and port (203.0.113.1:51820).
- **Allowed IPs**:
  - Full tunnel: 0.0.0.0/0, ::/0.
  - Split tunnel: Specific subnets (e.g., 192.168.88.0/24).
  - Persistent Keepalive: 25 (optional for NAT traversal).

WIREGUARD
FAST, MODERN, SECURE VPN TUNNEL

Full Tunnel vs. Split Tunnel in VPN

Full Tunnel

- Definition: All network traffic from the client is routed through the VPN.
- Allowed IPs Configuration: 0.0.0.0/0, ::/0.
- Use Case:
  - Provides maximum privacy and security by routing all traffic through the VPN server.
  - Ideal for public Wi-Fi connections or environments where privacy is a priority.
- Advantages:
  - Ensures complete encryption of all traffic.
  - Hides all client activity from the local network.
- Disadvantages:
  - Increased bandwidth usage on the VPN server.
  - May result in slower internet speeds due to the extra routing.

WIREGUARD
FAST, MODERN, SECURE VPN TUNNEL

Full Tunnel vs. Split Tunnel in VPN

Split Tunnel

- Definition: Only specific network traffic is routed through the VPN, while the rest accesses the internet directly.
- Allowed IPs Configuration: Specific subnets (e.g., 192.168.88.0/24).
- Use Case:
  - Useful for accessing remote network resources (e.g., internal servers) while using local internet for other tasks.
  - Reduces load on the VPN server.
- Advantages:
  - Improved internet speed for non-VPN traffic.
  - Reduced VPN server bandwidth usage.
- Disadvantages:
  - Some traffic may not be encrypted, reducing privacy.
  - Requires careful configuration to avoid exposing sensitive data.

WIREGUARD
FAST, MODERN, SECURE VPN TUNNEL

WireGuard Client Configuration Parameters

Interface Configuration

- Private Key: Generated by the client.
- Address: 192.168.88.2/24.
- DNS: 8.8.8.8 (optional).

Peer Configuration

- Public Key: From MikroTik.
- Endpoint: MikroTik's public IP and port (203.0.113.1:51820).
- Allowed IPs:
  - Full tunnel: 0.0.0.0/0, ::/0.
  - Split tunnel: Specific subnets.
- Persistent Keepalive: 25 (optional).

WIREGUARD
FAST, MODERN, SECURE VPN TUNNEL

Example Configuration

[Interface]
PrivateKey = <Client_Private_Key>
Address = 192.168.88.2/24
DNS = 8.8.8.8

[Peer]
PublicKey = <MikroTik_Public_Key>
Endpoint = 203.0.113.1:51820
AllowedIPs = 0.0.0.0/0, ::/0
PersistentKeepalive = 25

Full Tunnel

[Interface]
PrivateKey = <Client_Private_Key>
Address = 192.168.88.2/24
DNS = 8.8.8.8

[Peer]
PublicKey = <MikroTik_Public_Key>
Endpoint = 203.0.113.1:51820
AllowedIPs = 192.168.88.0/24,10.2.2.0/24
PersistentKeepalive = 25

Split Tunnel

Testing

WIREGUARD VPN...

Testing the Connection

Steps to Verify:

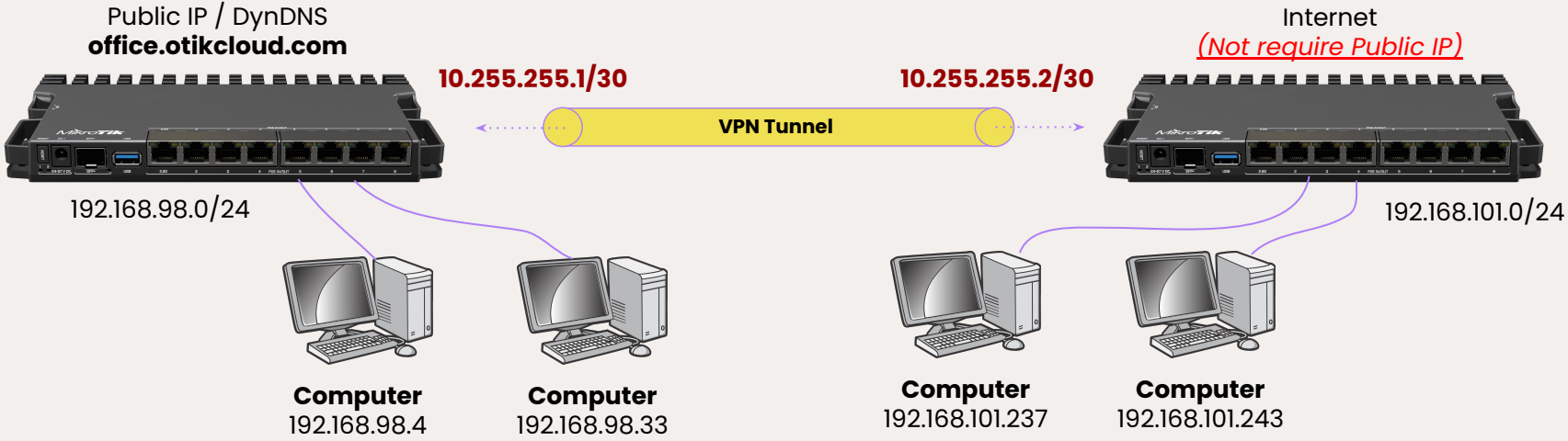
- Ping MikroTik's WireGuard IP (192.168.88.1).
- Check routing and firewall if issues occur.

Common Issues:

- Incorrect keys.
- Firewall blocking traffic.

WIREGUARD
FAST, MODERN, SECURE VPN TUNNEL

Site To Site VPN



WIREGUARD
FAST, MODERN, SECURE VPN TUNNEL

การออกแบบระบบ (Network Design Example)

ฝั่ง HQ (Headquarters)

- Public IP (หรือ DDNS): office.otikcloud.com (สมมติพอร์ต WireGuard เป็น 7443)
- Local Networks: 192.168.98.0/24
- WireGuard IP (ท่อ VPN): 10.255.255.1/30

ฝั่ง Branch (สาขา)

- Public IP: ไม่จำเป็นต้องมี (เป็นเน็ตบ้านทั่วไปหรืออยู่หลัง NAT ก็ได้)
- Local Networks: 192.168.101.0/24
- WireGuard IP (ท่อ VPN): 10.255.255.2/30

ขั้นตอนการคอนฟิกในแต่ละฝั่ง

Headquarters

ฝั่งที่ 1: การคอนฟิกที่ HQ (Headquarters)

1. สร้างอินเทอร์เฟซ WireGuard (ขารับ)

ไปที่เมนู WireGuard -> แท็บ WireGuard -> กด + (Add New)

- Name: wg-site-to-branch
- Listen Port: 7443 (เปิดพอร์ตนี้ที่ Firewall ขา WAN ของ HQ ด้วยเพื่อให้ Branch วิ่งเข้ามาได้)
- *เมื่อกด Apply ระบบจะเจนเนอเรต Public Key ของ HQ ออกมา ให้ก๊อปปี้เก็บไว้ไปใส่ฝั่ง Branch*

2. ผูก IP Address ให้ท่อ WireGuard

ไปที่ IP -> Addresses -> กด +

- Address: 10.255.255.1/30
- Interface: wg-site-to-branch

ฝั่งที่ 1: การคอนฟิกที่ HQ (Headquarters)

3. ตั้งค่า Peer (ระบุตัวตนและวงเน็ตเวิร์กของ Branch)

ไปที่เมนู WireGuard -> แท็บ Peers -> กด +

- Interface: wg-site-to-branch
- Public Key: *เอา Public Key ของฝั่ง Branch มาใส่*
- Endpoint / Endpoint Port: ปล่อยว่างไว้ (เพราะ HQ นั่งรอให้ Branch วิ่งเข้ามาหาเอง)
- Allowed Address: ใส่ IP ท่อ VPN ของ Branch และวงเน็ตเวิร์กภายในทั้งหมดของ Branch แยกด้วยเครื่องหมายจุลภาค (,)
    - ค่าที่ต้องใส่: 10.255.255.2/32, 192.168.101.0/24

4. ทำ Static Route เพื่อโยนทราฟฟิก

ไปที่ IP -> Routes -> กด + เพื่อบอกให้ HQ รู้ว่าถ้าจะไปหาเน็ตเวิร์กของ Branch ต้องวิ่งเข้าท่อนี้

- Route ที่ 1: * Dst. Address: 192.168.101.0/24
    - Interface : wg-site-to-branch
    - Gateway : 10.255.255.2

ขั้นตอนการคอนฟิกในแต่ละฝั่ง

Branch

ฝั่งที่ 2: การคอนฟิกที่ Branch (สาขา)

1. สร้างอินเทอร์เฟซ WireGuard (ขารุก)

ไปที่เมนู WireGuard -> แท็บ WireGuard -> กด + (Add New)

- Name: wg-site-to-hq
- Listen Port: ปล่อยตามที่ระบบสุ่มให้ได้เลย (เพราะเราเป็นฝ่ายวิ่งไปหา HQ)
- *เมื่อกด Apply ระบบจะเจนเนอเรต Public Key ของ Branch ออกมา ให้ก๊อปปี้ไปใส่ในข้อ 3 ของฝั่ง HQ*

2. ผูก IP Address ให้ท่อ WireGuard

ไปที่ IP -> Addresses -> กด +

- Address: 10.255.255.2/30
- Interface: wg-site-to-hq

ฝั่งที่ 2: การคอนฟิกที่ Branch (สาขา)

3. ตั้งค่า Peer (ชี้เป้าวิ่งไปหา HQ)

ไปที่เมนู WireGuard -> แท็บ Peers -> กด +

- Interface: wg-site-to-hq
- Public Key: *เอา Public Key ของฝั่ง HQ มาใส่*
- Endpoint: office.otikcloud.com (ใส่ IP หรือ Domain ของ HQ)
- Endpoint Port: 7433 (พอร์ตที่ HQ เปิดไว้)
- Allowed Address: ใส่ IP ท่อ VPN ของ HQ และวงเน็ตเวิร์กภายในทั้งหมดของ HQ
    - ค่าที่ต้องใส่: 10.255.255.1/32, 192.168.98.0/24
- Persistent Keepalive: 25 *(สำคัญมากสำหรับฝั่งสาขา เพื่อส่งแพ็กเก็ตไปเลี้ยงท่อ VPN ไม่ให้ Firewall ฝั่งเน็ตบ้านตัดพอร์ต)*

4. ทำ Static Route เพื่อโยนทราฟฟิก

ไปที่ IP -> Routes -> กด + เพื่อบอกฝั่ง Branch ว่าถ้าจะไปหาเน็ตเวิร์กของ HQ ให้วิ่งเข้าท่อนี้

- Route ที่ 1: * Dst. Address: 192.168.98.0/24
    - Interface : wg-site-to-hq
    - Gateway : 10.255.255.1

Demo

Testing the Connection

Steps to Verify:

- Ping MikroTik's WireGuard IP (192.168.98.1).
- Check routing and firewall if issues occur.

Common Issues:

- Incorrect keys.
- Firewall blocking traffic.

WIREGUARD
FAST, MODERN, SECURE VPN TUNNEL

THANKS!