

Virtual Private Network (VPN)



Bangkok Medical Software Co., Ltd.
www.hosxp.net



OpenVPN

- ทำไมต้องทำ **VPN** ?
- และทำไมต้องใช้ **OpenVPN**
- ทำแล้วได้ประโยชน์อย่างไร ?
- แล้วต้องทำทุกที่หรือเปล่า ?



Virtual Private Network

Virtual Private Network คือเครือข่ายส่วนบุคคลเสมือน หมายถึง ระบบเครือข่ายส่วนบุคคลที่สร้างโดยใช้เครือข่ายสาธารณะ เป็นการขยายเครือข่ายส่วนบุคคลโดยใช้ประโยชน์จากเครือข่ายสาธารณะ อย่างเช่นเครือข่ายอินเทอร์เน็ต มุมมองของผู้ใช้แล้วจะเป็นการเชื่อมต่อระหว่างจุดต่อจุดระหว่างเครื่องคอมพิวเตอร์ผู้ใช้งานกับเซิร์ฟเวอร์ภายในองค์กร โดยที่การเชื่อมต่อนั้นจะมีความปลอดภัยเนื่องจากการเข้ารหัสข้อมูลซึ่งสามารถสรุปคร่าว ๆ ได้ดังนี้



ประเภท VPN

VPN มี 3 ประเภท โดยขึ้นกับลักษณะการใช้งาน

- **Access VPN (Host-to-Net VPN)**
- **Intranet VPN (Site-to-Site VPN)**
- **Extranet VPN**



VPN Tunneling Protocol

- PPTP (Point to Point Tunneling Protocol)
- L2TP (Layer 2 Tunneling Protocol)
- IPSec (IP Security) เป็นการเข้ารหัสข้อมูล **Layer 3**
- SSL/TLS เป็นการเข้ารหัสข้อมูล **Layer 4** โดยใช้เทคโนโลยี SSL



VPN (tun/tap)

- VPN แบบ tun/tap ได้แก่ OpenVPN, Vtune, tinc และ CIPE OpenVPN ซึ่งเป็น Open Source VPN ที่ทำงานบนโปรโตคอล SSL (Secure Socket Layer)



OpenVPN

OpenVPN เป็นการสร้างเครือข่ายส่วนตัวเสมือน (**Virtual Private Network** หรือ **VPN**) ที่ทำให้ผู้ใช้งานเครือข่ายสามารถส่งข้อมูลหากันได้โดยรู้สึกว่กำลังสื่อสารกันภายในเครือข่ายเดียวกัน อีกทั้งยังมีความปลอดภัย โดยที่ **OpenVPN** รองรับการอัปเดตที่มการเข้ารหัสที่หลากหลาย



อีกทั้ง **OpenVPN** ยังสามารถใช้งานแบบ **Cross platform** ได้ กล่าวคือ **OpenVPN** รองรับระบบปฏิบัติการมากมาย ไม่ว่าจะเป็น **Linux, Windows XP, Windows Vista, OpenBSD, FreeBSD, Mac OS, และ Solaris** การติดตั้งเหมือนการใช้งานแอปพลิเคชันทั่วไปที่ทำงานร่วมกับ **SSL** ซึ่งมีผลให้การติดตั้งไม่ยุ่งยาก



แนวคิดของ OpenVPN

แนวคิดของการสร้าง **VPN** โดยใช้ **OpenVPN** แบบ **Static key** นั่นคือการเข้ารหัสข้อมูลด้วย **Symmetric key** ระหว่างเครื่องที่มีการเชื่อมต่อกัน โดยใน **OpenVPN** กำหนดให้เครื่องหนึ่งเรียกว่า **server** และอีกเครื่องเรียกว่า **client**

นั่นหมายความว่าก่อนที่จะมีการสร้าง **VPN** ระหว่าง **server** กับ **client** นั้นจะต้องมีการสร้าง **static key** ที่เครื่องใดเครื่องหนึ่ง (ในที่นี้คือ **server**) และกระจาย **static key** นั้นไปให้อีกเครื่อง (**client**) หลังจากนั้นทั้งสองจึงใช้ **static key** ในการเข้ารหัส **packet** ที่ส่งไปมาระหว่างกัน



การเชื่อมต่อ **VPN** ด้วย **OpenVPN** จะกระทำผ่าน **interface** ใหม่ที่ชื่อว่า **tunnel interface** โดยที่เมื่อมีการสร้าง **VPN** เรียบร้อยแล้วจะมี **interface** ที่ชื่อ **tun0** และมี **IP address** ที่อยู่ในอีก **subnet** หนึ่งซึ่ง **interface** นี้จะทำการเข้ารหัสข้อความและส่งไปยังอีกฝั่งหนึ่งผ่าน **physical interface**



คุณสมบัติของ OpenVPN

- ทำอุโมงค์แบบ **IP Frame** และแบบ **Ethernet Frame** ได้
- มีความปลอดภัยในระดับป้องกันทั้ง **Passive Attack** และ **Active Attack**
- ทำ **Load Balance** กรณีที่มี **VPN** เซิร์ฟเวอร์หลายตัว
- สนับสนุนการเข้ารหัสในรูปแบบ **Pre-shared Keys** และ **Certficated Keys**



- สนับสนุนการทำงานในรูปแบบ **HMAC Authentication**
- สนับสนุนการบีบอัดข้อมูลเพื่อลดปริมาณการจราจรบนเครือข่าย
- ทำ **DHCP** เพื่อแจกจ่ายไปยัง **VPN Client** ไม่ว่าจะเป็นการกำหนด **route, DNS, WINS** ซึ่งเหมาะกับการใช้งานแบบ **road-warrior**



- ทำอุโมงค์ผ่าน **NAT** ได้
- ไม่ต้องแก้ไข **kernel** โดยปกติ **kernel** ของลินุกซ์จะสนับสนุนการใช้งาน **tun/tap** อยู่แล้ว
- ใช้ได้หลากหลายแพลตฟอร์ม
- **OpenVPN** เป็น **GPL**



สิ่งที่ **OpenVPN** แตกต่างจาก **VPN** อื่นๆ

- **OpenVPN** สามารถทำงานได้หลายแพลตฟอร์ม ง่ายต่อการติดตั้ง รองรับการเชื่อมต่อจาก **client** ได้ในปริมาณมาก สามารถเซตให้ทำงานเป็น **DHCP** และ **NAT** ได้
- **OpenVPN** สามารถเลือกวิธีในการทำ **authenticate** ได้ตามความเหมาะสม
- **OpenVPN** สามารถบริหารจัดการได้ทั้งแบบ ส่วนกลางหรือระยะไกล โดยสามารถทำการบริหารจัดการโดยใช้ **GUI** ได้



- บน **Windows OS, OpenVPN** สามารถอ่าน **Certificates** และ **Private Keys** จาก **Smart cards** ได้(support the Windows Crypto API)
- **OpenVPN** มีความปลอดภัยในระดับป้องกันทั้ง **Passive Attack** และ **Active** •**OpenVPN** ถูกสร้างให้ใช้งานได้อย่างสะดวก ไม่ว่าจะใช้งานบน **Linux, Solaris, OpenBSD, FreeBSD, NetBSD, Mac OS X** และ **Windows 2000/XP** เพราะว่า **OpenVPN** ถูกออกแบบให้ **run** บน **user-space** ซึ่งไม่ขึ้นกับ **kernel**
- **OpenVPN** ถูกออกแบบให้มีความคงทนต่อความผิดพลาดต่างๆบน เครือข่ายอินเทอร์เน็ต(**unreliable network**)



การส่งข้อมูลผ่าน OpenVPN



UDP

TAP/TUN

Data Encryption



Server



UDP

TAP/TUN

Data Encryption



Client



ประโยชน์ที่ได้รับจาก VPN

- ช่วยองค์กรประหยัดค่าใช้จ่ายในการซื้อ **VPN**
- ก็สามารถเข้าถึงเครือข่าย **VPN** ของตนได้ไม่ว่าจะอยู่ที่ไหนก็ตาม
- ลดค่าใช้จ่ายในส่วนของการดูแลรักษาระบบ
- ระบบเครือข่าย **VPN** สามารถความคล่องตัวการเปลี่ยนแปลง เช่นการขยายเครือข่าย
- การรับส่งข้อมูลมีความปลอดภัยเพราะมีการเข้ารหัสข้อมูล



การทดสอบระบบ Datacenter

- Datacenter สสจ.น่าน
- Datacenter สสจ.กาญจนบุรี



ปัญหาและอุปสรรค

- ความรู้ในเรื่อง **OpenVPN**
- ระบบ **Server/Client** เครื่อง **Client** จะใช้เวลาในการติดตั้งทุกเครื่อง



Download

- ท่านสามารถ **Download** ไฟล์ **OpenVPN** ได้จาก <http://swupdate.openvpn.org/downloads/shield/openvpn-connect.msi>