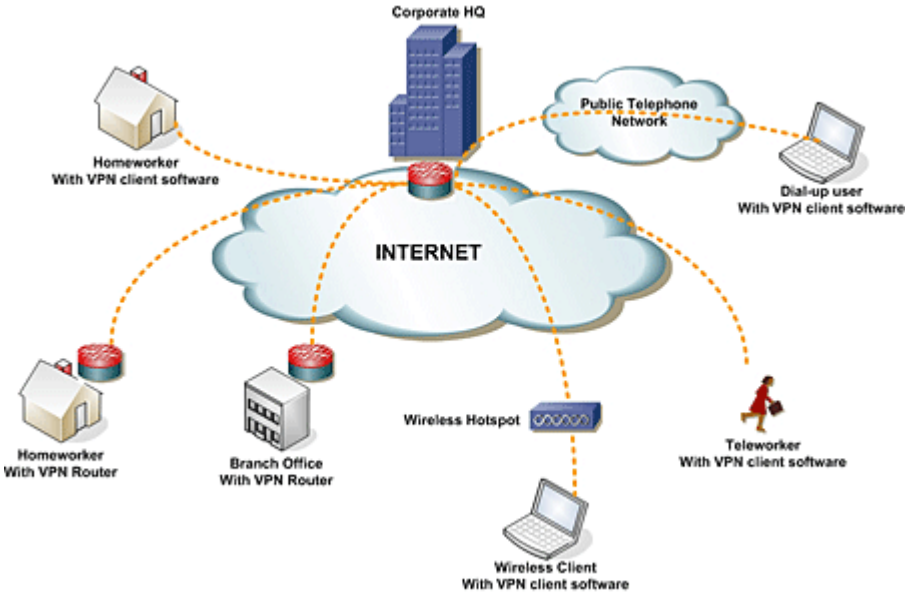
VPN (Virtual Private Network)

นายเกรียงศักดิ์นามโคตร (Mr.Jodoi) เรียบเรียง

VPN หรือ Virtual Private Network หมายถึง เครือข่ายเสมือนส่วนตัว ที่ทำงานโดยใช้โครงสร้างของเครือข่ายสาธารณะ หรืออาจจะวิ่งบนเครือข่าย IP ก็ได้แต่ยังสามารถคงความเป็นเครือข่ายเฉพาะขององค์กรได้ ด้วยการเข้ารหัสแพ็กเก็ตก่อนส่ง เพื่อให้ข้อมูล มีความปลอดภัยมากขึ้น สรุปง่ายๆคือต้องมีความเป็นส่วนตัวและมีความปลอดภัยนั่นเอง ดังรูปด้านล่าง



ไม่ว่าเราจะอยู่ที่ใดก็เสมือนนั่งทำงานอยู่ที่ HQ (สำนักงานใหญ่ของบริษัท) สามารถใช้งาน printer , ส่ง e-mail หรือใช้โทรศัทพ์ภายในได้

VPN จะครอบคลุมทั้งอุปกรณ์ฮาร์ดแวร์(เช่น Gateway Box , Router, Firewall) ,และซอฟต์แวร์ (VPN Server บน Windows Server, VPN Server บน Linux Server หรือ Application VPN) การเข้ารหัสแพ็กเก็ต เพื่อทำให้ข้อมูล มีความปลอดภัยนั้น ก็มีอยู่หลายกลไกด้วยกัน ซึ่งวิธีเข้ารหัสข้อมูล (encryption) จะทำกันที่เลเยอร์ 2 คือ Data Link Layer หรือที่เรียกกันว่า tunneling protocols ซึ่ง tunneling protocols ที่อยู่ใน Layer 2 ได้แก่

1) Layer 2 Forwarding (L2F) tunneling protocol นี้ Cisco เป็นผู้คิดค้นขึ้นมา
2) Point-to-Point Tunneling Protocol (PPTP) tunneling protocol นี้ Microsoft เป็นผู้คิดค้นขึ้นมา
3) Layer 2 Tunneling Protocol (L2TP) tunneling protocol นี้ Microsoft และ Cisco เป็นผู้คิดค้นขึ้นมาเพื่อใช้แทน L2F และ PPTP เป็นการรวมทั้ง 2 tunneling protocol เข้าด้วยกัน

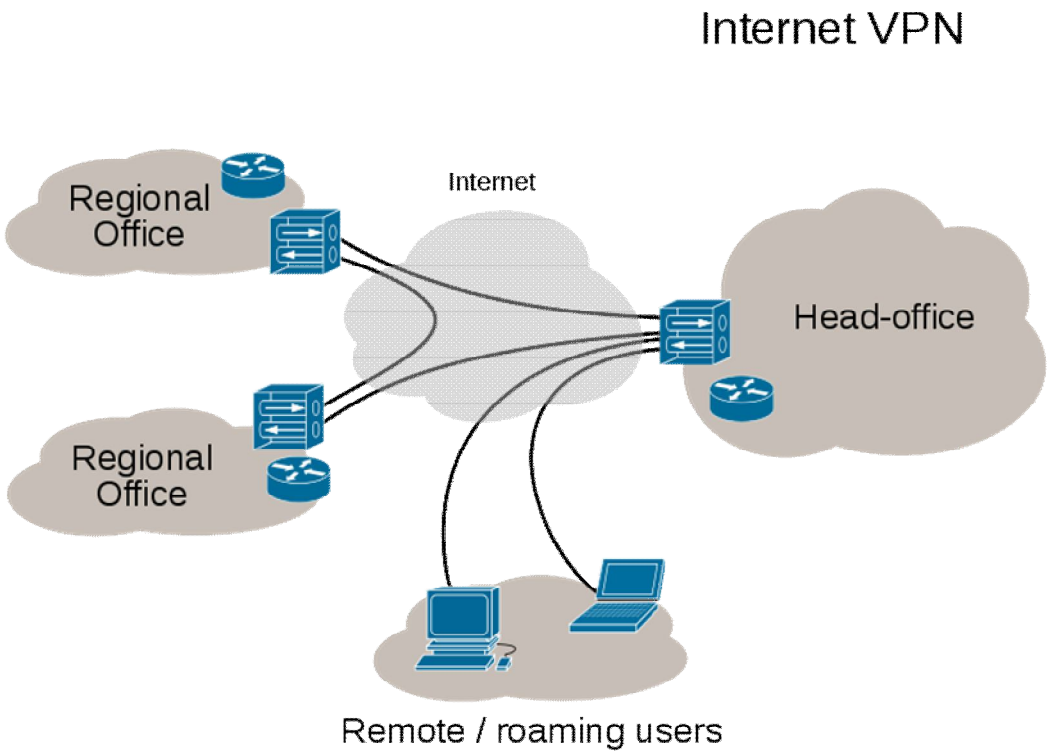
4) Generic Routing Encapsulation (GRE) เป็น tunneling protocol ที่เปิดโอกาสให้ product อื่นที่ไม่ใช่ Cisco สามารถทำ VPN บน IP tunnels ได้

ข้อด้วยของ tunneling protocols ใน Layer 2 คือช้าและสามารถโดนโขมยข้อมูลหรือโดน hack ได้

ปัจจุบัน มีการเข้ารหัสใน IP Layer (Layer 3) ได้แก่

1) IPSec (IP Security) เป็น tunneling protocol ตามมาตรฐานของหน่วยงาน IETF
2) SSL VPN เป็น tunneling protocol ที่พัฒนาโดย Netscape Corporation เป็นการทำ VPN ผ่าน Web Browser ผ่านพอร์ต 443

ข้อดีของ tunneling protocols ใน Layer 3 คือเร็วกว่า และปลอดภัยกว่า tunneling protocols ใน Layer 2 และถ้าเป็นอุปกรณ์ทางด้าน Network ที่ออกมาใหม่ไม่ว่าจะเป็น Router หรือ Firewall จะมี tunneling protocols ใน Layer 3 ไม่ว่าจะเป็น IPSec หรือ SSL VPN มาด้วยเสมอ



ปกติแล้ว VPN ถูกนำมาใช้กับองค์กรขนาดใหญ่ ที่มีสาขาอยู่ตามที่ต่างๆ และต้องการต่อเชื่อมเข้าหากัน โดยยังคงสามารถรักษาเครือข่ายให้ใช้ได้เฉพาะ คนภายในองค์กร หรือคนที่เกี่ยวข้องด้วย เช่น ลูกค้า, ซัพพลายเออร์ หรือ คู่ค่า เป็นต้น

นอกจากนี้แล้ว กลไกในการสร้างโครงข่าย VPN อีกประเภทหนึ่ง คือ MPLS (Multiprotocal Label Switch) เป็นวิธีในการส่งแพ็กเก็ต โดยการใส่label ที่ส่วนหัว ของข้อความ

และค่อยเข้ารหัสข้อมูล จากนั้น จึงส่งไปยังจุดหมายปลายทาง เมื่อถึงปลายทาง ก็จะถอดรหัสที่ส่วนหัวออก วิธีการนี้ ช่วยให้ผู้วางระบบเครือข่าย สามารถแบ่ง Virtual LAN เป็นวงย่อย ให้เป็นเครือข่ายเดียวกันได้ตัวอย่างเช่น บริษัท A ก็จะได้VPN label A ที่หัวข้อความ ของทุกแพ็กเก็ต บริษัท B ได้รหัสที่หัวข้อความเป็น B เพื่อส่งข้อมูล ข้อมูลที่ส่งออกไป ก็จะวิ่งไปหาปลายทางตาม Label ของตนซึ่งผู้วางระบบ สามารถเพิ่มกลุ่มในวง VLAN ได้อย่างไม่จำกัด

<u>บริการ VPN แบ่งออกเป็น 3 รูปแบบ</u>

1. Remote access VPNs : เป็นรูปแบบในการเข้าถึงเครือข่าย VPN จากอุปกรณ์เคลื่อนที่ต่างๆ ซึ่งสามารถเข้าถึงเครือข่ายได้ โดยเป็นการเข้าถึงจากไคลเอ็นต์ใดๆ ก็ได้ โดยอาศัย ผู้ให้บริการอินเทอร์เน็ต เป็นตัวกลาง ในการติดต่อ ซึ่งจะมีการเข้ารหัสในการ ส่งสัญญาณจากเครื่องไคลเอ็นต์ไปยัง VPN Server หรือสรุปคือ ต้องมี VPN Server 1 ตัว และเครื่อง Client ที่ต้องการติดต่อต้องมีการติดตั้ง VPN Client ไว้ที่อุปกรณ์ รูปแบบนี้จะเหมาะกับ ลักษณะการทำงานแบบ Mobile User เช่น พนักงานฝ่ายขายหรือวิศวกรที่เดินทางไปต่างจังหวัดบ่อยๆ

2. Site-to-site VPNs หรือ Intranet VPN: เป็นรูปแบบในการเข้าถึงเครือข่าย VPN ที่ใช้เฉพาะภายในองค์กรเท่านั้น อาทิ การต่อเชื่อมเครือข่าย ระหว่างสำนักงานใหญ่ในกรุงเทพฯ และสาขาย่อยในต่างจังหวัดเสมือนกับ การทดแทน การเช่าวงจรลีสไลน์ ระหว่าง กรุงเทพกับต่างจังหวัด โดยที่แต่ละสาขาสามารถ ต่อเชื่อมเข้ากับ ผู้ให้บริการอินเทอร์เน็ต ในท้องถิ่นของตน เพื่อเชื่อมเข้าโครงข่าย VPN ขององค์กรอีกทีหนึ่ง หรือสรุปก็คือ ต้องให้ Router หรืออุปกรณ์ 2 ฝั่ง ทำ VPN แบบ Site-to-site ถึงกัน โดย เครื่องของ Client ไม่ต้องทำอะไร ปัจจุบันเป็นที่นิยมมาก ยกตัวอย่าง มีบริษัทที่มี ADSL ในพื้นที่เช่น เชียงใหม่กับ กรุงเทพฯ และ ADSL Router เป็นรุ่นที่มีฟังก์ชัน VPN Site-to-site ทำให้ทั้ง 2 สาขาใช้งานภายในได้แบบประหยัดค่าใช้จ่ายมากๆ ไม่ว่าจะเป็น Data,voice หรือ video เป็นต้น

3. Extranet VPN: เป็นรูปแบบในการเข้าถึงเครือข่าย ที่คล้ายกับ Intranet VPN แต่มีการขยายวงออกไป ยังกลุ่มลูกค้า ซัพพลายเออร์ และพาร์ตเนอร์ เพื่อให้ใช้เครือข่ายได้ จุดสำคัญอย่างหนึ่ง ในการเลือกติดตั้ง VPN คือการเลือก ผู้ให้บริการอินเทอร์เน็ต ที่วางระบบรักษาความปลอดภัยเป็นอย่างดี มีส่วนอย่างมาก ในการส่งข้อมูลบน VPN ให้ปลอดภัยมากยิ่งขึ้น เพราะถ้า ไอเอสพี มีระบบรักษาความปลอดภัย ที่รัดกุม ก็จะช่วยให้ ข้อมูลที่ส่งมา มีความปลอดภัยมากขึ้น Extranet VPN อาจจะเปิดให้ใช้งานได้แค่บางเมนูเท่านั้น ต้องเน้นเรื่องของความเป็นส่วนตัว

ประโยชน์ที่ได้รับจาก VPN

ประโยชน์ของ การติดตั้งเครือข่ายแบบ VPN จะช่วยองค์กร ประหยัดค่าใช้จ่าย เพราะไม่ว่าผู้ใช้องค์กร จะอยู่ที่ใดในโลก ก็สามารถเข้าถึง เครือข่าย VPN ของตนได้ โดยการต่อเชื่อม เข้ากับ ผู้ให้บริการท้องถิ่นนั้นๆ ทำให้ช่วยลด ค่าใช้จ่าย ในการติดต่อสื่อสาร และสามารถ ลดค่าใช้จ่ายในส่วนของ การดูแลรักษาระบบอีกด้วย นอกจากนี้ ระบบเครือข่าย VPN ยังสามารถ ให้ความคล่องตัวในการเปลี่ยนแปลง เช่น การขยายเครือข่าย ในอนาคตนอกจากนี้แล้ว ในแง่ของ ผู้ให้บริการอินเทอร์เน็ต การออกบริการ VPN ก็เป็นอีกทางเลือกหนึ่ง ที่ช่วยให้ ลูกค้าของไอเอสพี ประหยัดค่าใช้จ่าย และสะดวกสบายมากขึ้น

สำหรับหน่วยงานที่มีงบประมาณน้อย ผมขอเสนอตัวนี้ครับ **OpenVPN** ซึ่งเป็นของ free และเป็นopen source สามารถติดตั้งได้ทั้งบน Windows และ Linux ติดตั้งได้ทั้งแบบ Remote access VPNs และ Site-to-site VPNs สะดวกและประหยัดค่าใช้จ่าย แต่ต้องมีความรู้พอสมควร

หวังว่าบทความนี้คงจะก่อให้เกิดประโยชน์ไม่มากก็น้อยสำหรับผู้ที่ทำงานอยู่ในแวดวงไอทีนะครับ

แหล่งข้อมูลอ้างอิง

http://en.wikipedia.org/wiki/Virtual_private_network

http://en.wikipedia.org/wiki/OpenVPN

http://www.cisco.com

สนับสนุนโดย http://www.jodoi.com