ระบบเครือข่ายเสมือส่วนตัว VPN

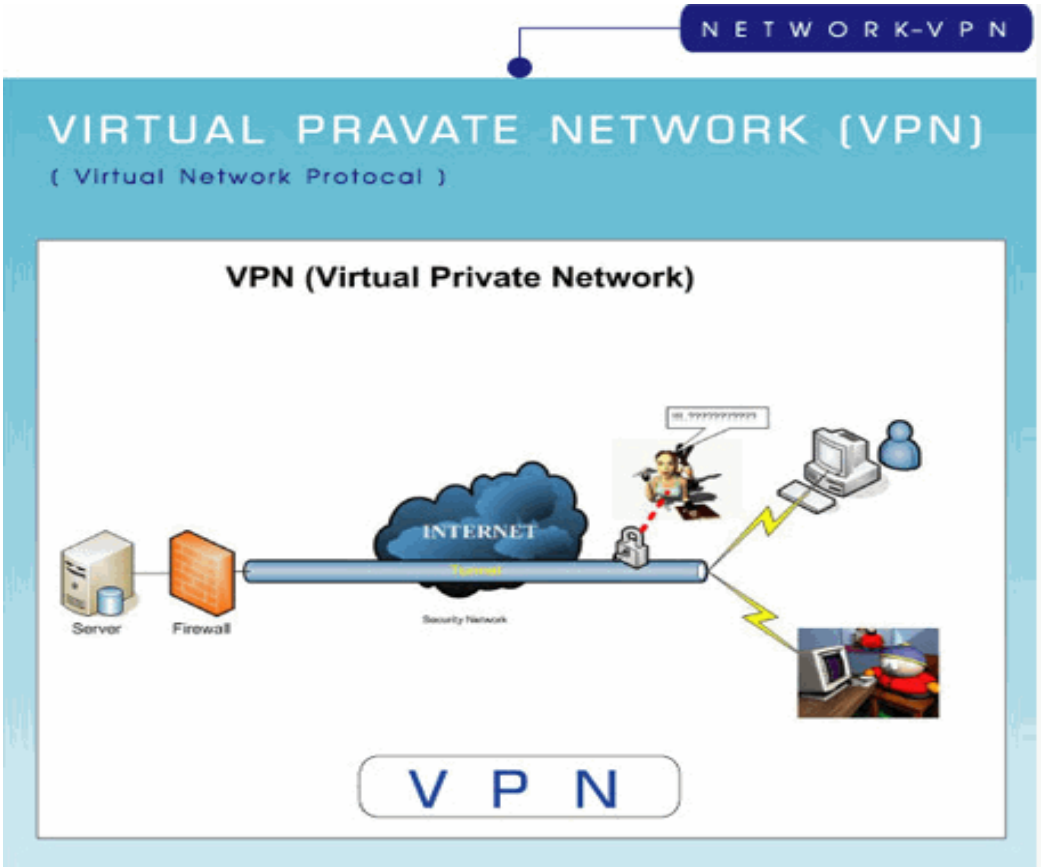
1.ทำความรู้จักกับระบบเครือข่ายเสมือนส่วนตัว VPN (Virtual Private Network)

Virtual Private Network (VPN) หมายถึง เครือข่ายเสมือนส่วนตัวที่ทำงานโดยใช้โครงสร้างของเครือข่ายสาธารณะ หรืออาจจะวิ่งบนเครือข่ายไอพีก็ได้แต่ยังสามารถคงความเป็นเครือข่ายเฉพาะขององค์กรได้ด้วยการเข้ารหัสข้อมูลก่อนส่งเพื่อให้ข้อมูลมีความปลอดภัยมากขึ้น

-VPN ถูกนำมาใช้กับองค์กรขนาดใหญ่ที่มีสาขาอยู่ตามที่ต่างๆและต้องการต่อเชื่อมเข้าหากันโดยยังคงสามารถรักษาเครือข่ายให้ใช้ได้เฉพาะคนภายในองค์กรหรือคนที่เกี่ยวข้องด้วย

สรุปความหมาย ได้ดังนี้

- เทคโนโลยี VPN จะทำการเชื่อมต่อองค์ประกอบข้อมูลและทรัพยากรต่างๆ ของระบบเครือข่ายหนึ่ง ให้เข้ากับระบบเครือข่ายหนึ่ง
- เทคโนโลยี VPN จะทำงานโดยยอมให้ผู้ใช้งานสร้างท่ออุโมงค์ เสมือนเพื่อใช้ในการรับส่งข้อมูลผ่านระบบเครือข่ายอินเตอร์เน็ต
- ส่วนประกอบที่สำคัญหรือหัวใจหลักในการทำ VPN ก็คือการใช้งานอินเตอร์เน็ต



ข้อดีของระบบ VPN

1. **ประหยัดค่าใช้จ่าย**

การสร้างวงจรเสมือนจริงผ่านเครือข่าย Internet ใช้หลักการให้เครือข่ายย่อยเชื่อมกับ Internet ที่ท้องถิ่น ซึ่งจะเสียค่าเช่าวงจรเฉพาะท้องถิ่น และค่าบริการ Internet เท่านั้น (ในองค์กรที่มีหลายสาขา จึงไม่จำเป็นต้องเช่า Leased Line หลายสายอีกต่อไป) การสร้าง VPN ยังทำได้กับเครือข่ายขนาดเล็กที่ใดก็ได้ โดยต้องมีระบบเครือข่ายที่รองรับ คือ ต้องมี Router ที่สนับสนุน Protocol แบบ VPN ได้ จากการศึกษาของ IDC พบว่า VPN สามารถลดค่าใช้จ่ายในการเชื่อมต่อแบบ WAN ได้ราว 40 %

2. **มีการรักษาความปลอดภัยของข้อมูล**

การสร้างวงจรเสมือนจริง ผ่านเครือข่ายสาธารณะ มีจุดเด่นคือ Router ต้นทาง และ Router ปลายทางของเครือข่ายที่สร้างวงจรเสมือนจริงนี้ จะทำการเข้ารหัสข้อมูลและบีบอัดข้อมูลเข้าไว้ใน Packet IP ทำให้ข้อมูลที่วิ่งไปในเครือข่าย Internet ได้รับการป้องกัน ซึ่งถ้ามีใครแอบดักข้อมูล หรือ IP Packet ไปได้ ก็ได้ข้อมูลที่เข้ารหัสยาก ซึ่งยากต่อการถอดรหัส เพราะเป็นรหัสที่ต้องการคีย์ถอดรหัส รวมถึงมีการสร้างอุโมงค์สื่อสาร (Tunneling) การพิสูจน์บุคคล หรือการจำกัดสิทธิ์ในการเชื่อมต่อ

สามารถสรุปวิธีการที่นำมาใช้ เพื่อให้ VPN มีความสามารถในการรักษาและดูแลเครือข่ายและข้อมูลให้ปลอดภัยมากขึ้น ได้ดังนี้

2.1) Firewall จะเป็นการติดตั้งตัวกั้นกลางระหว่าง network ของเรากับ Internet โดยตัว Firewall จะสามารถจำกัดจำนวนของ port รวมทั้งลักษณะของ packet และ protocol ที่จะมาใช้งาน

2..2) Encryption (การเข้ารหัส) เป็นกระบวนการที่นำข้อมูลจากเครื่องคอมพิวเตอร์หนึ่งเครื่องไปทำการเข้ารหัสก่อนที่จะส่งไปยังเครือข่ายคอมพิวเตอร์อื่น

2.3) IPSec หรือ Internet Protocol Security Protocol เป็นการเข้ารหัสที่ช่วยให้ระบบรักษาความปลอดภัยทำงานได้ดียิ่งขึ้น เช่น การเข้ารหัสแบบ Algorithm และการตรวจสอบผู้ใช้ โดยทั่วไป IPSec มีการเข้ารหัส 2 แบบด้วยกันคือ

- tunnel จะทำการเข้ารหัสทั้งหัวของข้อความ (header) และข้อมูลในแต่ละ Packet (payload of each packet)
- transport จะเข้ารหัสเฉพาะตัวข้อมูลเท่านั้น

อย่างไรก็ดี IPSec จะใช้ได้กับระบบ อุปกรณ์ และ Firewall ของแต่ละเครือข่ายที่มีการติดตั้งระบบความปลอดภัยที่เหมือนกันเท่านั้น

3. **มีความยืดหยุ่นสูง**

โดยเฉพาะอย่างยิ่งในกรณีการทำ Remote Access ให้ผู้ใช้ติดต่อเข้ามาใช้งานเครือข่ายจากนอกสถานที่ เช่น พวกผู้บริหาร หรือฝ่ายขาย ที่ออกไปทำงานนอกสถานที่สามารถเชื่อมต่อเข้าเครือข่ายของบริษัท เพื่อเช็คข่าว อ่านเมล์ หรือใช้งานโปรแกรม เพื่อเรียกดูข้อมูล เป็นต้น การใช้ VPN สามารถ login เข้าสู่ ระบบงานของบริษัทโดยใช้โปรแกรมจำพวก VPN Client เช่น Secureremote ของบริษัท Checkpoint เป็นต้น วิธีการอย่างนี้ทำให้เกิดความคล่องตัวในการทำงานเป็นอย่างมาก และยังสามารถขยาย Bandwidth ในการใช้งาน VPN ได้อย่างไม่ยุ่งยากอีกด้วย

4**. จัดการและดูแลได้ง่าย**

การบริหารและการจัดการเครือข่าย ทำได้ดีและสะดวกต่อการขยายและวางแผนการขยาย โดยเน้นการสนับสนุนการทำงาน และการดูแลได้อย่างมีประสิทธิภาพ

5. **สามารถกำหนดหมายเลข IP เป็นเครือข่ายเดียวกันได้**

การแยกเครือข่าย 2 เครือข่าย ระบบ IPจะต้องแยกกัน แต่การสร้าง VPN จะทำให้ 2 เครือข่ายนี้เสมือนเป็นเครือข่ายเดียวกัน ดังนั้นจึงใช้หมายเลข IP และ Domain เดียวกันได้

6. **ประสิทธิภาพการรับส่งข้อมูล**

เทียบเท่ากับการเช่า Leased Line เชื่อมโยงสาขาโดยตรง

7. สามารถเข้ามาใช้งานระบบได้ทุกที่ทั่วโลก ถ้าเชื่อมเข้ากับอินเตอร์เน็ต

<u>2.ทำไมต้องใช้ระบบเครือข่ายเสมือนส่วนตัว VPN (Virtual Private Network)</u>

เนื่องจากปัจจุบันการติดต่อสื่อสารถือว่าเป็นสิ่งที่มีความจำเป็นมากขึ้นเรื่อยๆ โดยถ้าเราต้องการการเชื่อมต่อที่มีประสิทธิภาพ มีความปลอดภัยระหว่าง Network บริการที่ดีที่สุดคือ การเช่าสายสัญญาณ (leased line) ซึ่งจะทำการเชื่อมต่อระบบเน็ตเวิร์คของเราด้วยการใช้สายสัญญาณตรงสู่ปลายทาง ทำให้มีความปลอดภัยสูงเพราะไม่ต้องมีการใช้สื่อกลางร่วมกับผู้อื่น และมีความเร็วคงที่ แต่การเช่าสาสัญญาณนั้นใช้ข้อเสียคือ ค่าใช้จ่ายในการใช้บริการนั้นสูงมาก เมื่อเทียบกับความเร็วที่ได้รับ ซึ่งบริษัทขนาดเล็กนั้นคงไม่สามารถทำได้

เทคโนโลยี VPN ได้เข้ามาเป็นอีกทางเลือกหนึ่ง เนื่องจากได้ใช้สื่อกลางคือ Internet ที่มีการติดตั้งอยู่อย่างแพร่หลายเข้ามาสร้างระบบเน็ตเวิร์คจำลอง โดยมีการสร้างอุโมงค์ข้อมูล (Tunnel) เชื่อมต่อกันระหว่างต้นทางกับปลายทาง ทำให้เสมือนว่าเป็นระบบเน็ตเวิร์คเดียวกัน สามารถส่งข้อมูลต่างๆที่ระบบเน็ตเวิร์คทำ

ได้ โดยข้อมูลที่ส่งนั้นจะถูกส่งผ่านไปในอุโมงค์ข้อมูล ทำให้มีความปลอดภัยสูง ใกล้เคียงกับ leased line แต่ค่าใช้จ่ายในการทำ VPN นั้นต่ำกว่าการเช่าสายสัญญาณมาก

3.ความสามารถของระบบเครือข่ายเสมือนส่วนตัว VPN (Virtual Private Network)

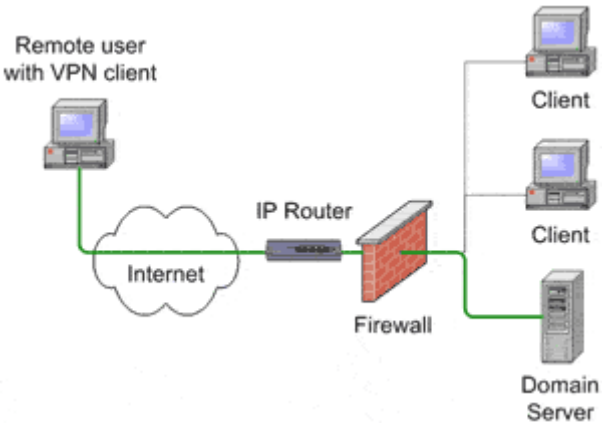
-การสร้างวงจรเสมือนจริงผ่านเครือข่าย Internet ใช้หลักการให้เครือข่ายย่อยเชื่อมกับ Internet ที่ท้องถิ่น ซึ่งจะเสียค่าเช่าวงจรเฉพาะท้องถิ่น และค่าบริการ Internet เท่านั้น ทำให้เราสามารถใช้งาน Internet ได้เหมือนเครือข่ายภายในองค์กรของเราเลย

- มีความปลอดภัยในการใช้งานค่อนข้างสูง

การจะทำให้ระบบ VPN ปลอดภัยนั้น ประกอบไปด้วยหลายๆวิธีที่สามารถทำได้ โดยในที่นี้จะกล่าวถึงวิธีดังต่อไปนี้

· **Firewalls**

เป็นการสร้างความปลอดภัยหระว่างระบบเน็ตเวิร์คกับอินเตอร์เน็ต โดย Firewalls จะเป็นตัวควบคุมการเปิด-ปิด Portsต่างๆ ซึ่งสามารถทำให้เราควบคุมได้ว่าต้องการให้ Protocols ไหนสามารถใช้งานได้บ้าง Packet ที่เข้ามานั้นจะอนุญาตให้ผ่านหรือไม่ และจะปิด port ทีไม่ได้ใช้งานไว้ สามารถป้องกันการบุกรุกจากพอร์ทที่ไม่ได้ใช้งานได้



· **Encryption**

Encryption คือ การเข้ารหัสของข้อมูลที่จะทำการส่งไปยังคอมพิวเตอร์เครื่องอื่น ซึ่งเมื่อข้อมูลที่ผ่านการ Encrypt ถูกส่งไปถึงผู้รับ ผู้รับจะต้องทำการ Decode เพื่อให้ได้ข้อมูลที่ผู้ส่งต้องการส่งคืนมา จะทำให้ข้อมูลมีความปลอดภัยเพราะระหว่างทางนั้นถ้าผู้อื่นได้รับข้อมูลไปก็ไม่สามารถรู้ได้ว่าข้อมูลนั้นเป็นอะไร

· **IPSec**

เป็น โปรโตคอลที่มีความปลอดภัยเมื่อนำมาใช้งานในการส่งข้อมูลผ่าน VPN

· **AAA Server**

AAA Server คือ Authenticate, Authorization และ Accounting server เป็นการเพิ่มความปลอดภัยในการใช้งานแบบ Remote-Access VPN ซึ่งเมื่อมีการเชื่อมต่อจาก Dial-up นั้นจะต้องผ่าน AAA Server ซึ่งจะมีการตรวจสอบกังนี้ คือ

คุณเป็นใคร Who you are (authentication)

คุณได้รับอนุญาตให้ทำอะไรบ้าง What you are allowed to do (authorization)

คุณทำอะไรไปบ้าง What you actually do (accounting)