บทที่ 9

Virtual Private Network

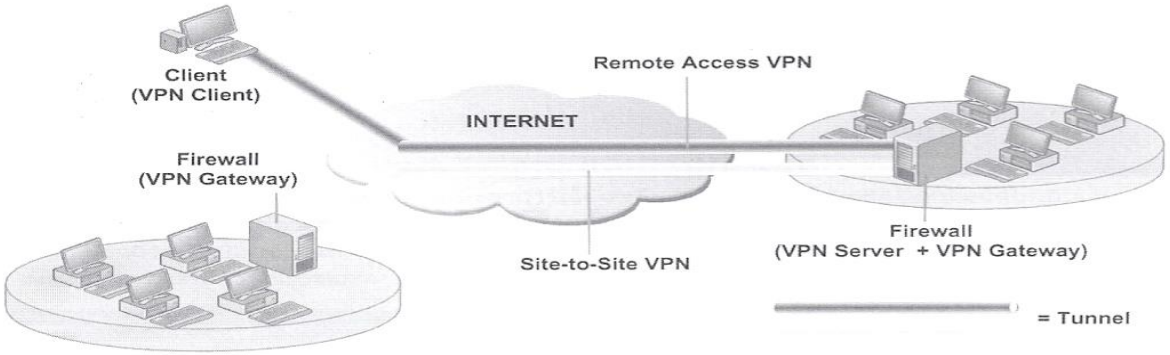
VPN (Virtual Private Network)

VPN หรือ Virtual Private Network คือการสร้างเครือข่ายเสมือนส่วนบุคคลขึ้นมาบนเครือข่ายที่ใช้งานอยู่จริง ซึ่งมักจะเป็นเครือข่ายสาธารณะ เช่น อินเทอร์เน็ต เป็นต้น เครื่องหรือระบบเครือข่ายที่เชื่อมต่อกันด้วย VPN จะเสมือนหนึ่งว่าอยู่ในเครือข่ายหรือระบบ LAN เดียวกันหรืออธิบายอีกนัยหนึ่งคือเปรียบเสมือนมีท่อสำหรับรับส่งข้อมูลที่มองไม่เห็นเชื่อมถึงกันอยู่นั่นเองท่อรับส่งข้อมูลดังกล่าวนี้ในทาง LAN จะเรียกว่า Tunnel ที่แปลว่าอุโมงค์นั่นเอง

อย่างไรก็ตามในเชิงเทคนิคแล้ว VPN ก็คือเทคนิคที่ใช้ในการสร้างช่องทางการลำเลียงข้อมูลที่ปลอดภัยขึ้นระหว่างต้นทางและปลายทาง โดยอาศัยเทคนิคที่ใช้ในการสร้างช่องทางการลำเลียงข้อมูลที่ปลอดภัยขึ้นระหว่างต้นทางและปรายทาง โดยอาศัยเทคนิคการเข้ารหัสข้อมูล (Encryption) เพื่อป้องกันไม่ให้ข้อมูลที่ถูกดักหรือขโมยระหว่างทางถูกนำไปถอดรหัสหรือนำไปใช้ประโยชน์ต่อได้ นอกจากนี้ยังประกอบไปด้วยเทคนิคการป้องกันการปลอมแปลงข้อมูล การตรวจยืนยันตัวผู้ใช้ และการตรวจยืนยันตัวระหว่างต้นทางและปลายทางเพื่อป้องกันการสวมรอย

ประเภทของ VPN

VPN แบ่งออกเป็น 2 ประเภทตามลักษณะของการใช้งาน คือ Remote Access VPN และ Site-to-site VPN ดังมีรายละเอียดดังนี้



รูปที่ 9.1 VPN

ที่มา : คู่มือดูแลระบบ Network ฉบับมืออาชีพ, 2551 : 334

Remote Access VPN

Remote Access VPN คือ การเชื่อมต่อ VPN จากเครื่องคอมพิวเตอร์เดี่ยวๆ ที่อยู่ภายนอก หรืออินเทอร์เน็ตเข้ากับระบบ LAN ภายใน (หรือที่เรียกว่า Client-to-LAN หรือ Client-to Gateway) โดยผ่านอุปกรณ์ที่เรียก VPN Server ซึ่งในกรณีนี้ตัวอุปกรณ์ Firewall ทั่วๆ ไปมักจะมีความสามารถเป็น VPN Server ได้ในตัว อย่างไรก็ตามในตัวระบบปฏิบัติการทั่วๆ ไป เช่น Windows หรือ Linux ก็มีความสามารถเป็น VPN Server ได้ด้วยเช่นกัน เครื่องคอมพิวเตอร์ภายนอกจะต้องได้การติดตั้งโปรแกรมหรือซอฟแวร์ที่เรียกว่า VPN Client ซึ่งมักจะติดมาให้กับชุดอุปกรณ์ของ Firewall อยู่แล้วแต่ในกรณีของระบบ ปฏิบัติการ Windows รุ่นปัจจุบันก็มักจะมีความสามารถในการเชื่อมต่อ Remote Access VPN ได้ในตัวโดยไม่ต้องติดตั้งซอฟต์แวร์หรือโปรแกรมเพิ่ม แต่ก็ต้องตั้งค่าให้ถูกต้องด้วย สำหรับโปรโตคอลที่ใช้ในการเชื่อมต่อ Remote Access VPN ได้แก่ PPTP , L2F , L2TP , L2TP/IPSec และ IPSec

Site-to-Site VPN

Site-to-Sire VPN คือการเชื่อมต่อ VPN ระหว่างระบบ LAN 2 ระบบเข้าด้วยกัน (หรือที่เรียกว่า LAN-to-LAN หรือ Gateway-to-Gateway) โดยอาศัยอุปกรณ์ที่เรียกว่า VPN Gateway ที่ติดตั้งไว้ในระบบ LAN ทั้ง 2 ฝั่ง เป็นตัวเชื่อมต่ออุปกรณ์ Firewall โดยทั่วๆ ไปจะมีความสามารถในการทำตัวเป็น VPN Gateway ได้ ตัวอย่างเช่น การเชื่อมต่อระบบ LAN ระหว่างสาขา และสำนักงานใหญ่เข้าด้วยกันโดยอาศัยการทำงาน Site-to-site VPN ผ่านอินเตอร์เน็ต การสร้างท่อรับส่งข้อมูลหรือ Tunnel จะเกิดขึ้นระหว่าง VPN Gateway เท่านั้น เครื่องลูกข่ายภายในระบบ LAN แต่ละฝั่งจะสามารถติดต่อสื่อสารกับอีกฝั่งหนึ่งได้โดยไม่ต้องติดตั้งซอฟต์แวร์หรือตั้งค่าใดๆ ในเครื่องเพิ่ม อธิบายง่ายๆ ก็คือเครื่องลูกข่ายจะไม่รับรู้ว่ามีการเชื่อมต่อระหว่างระบบ LAN ทั้งสองฝั่งด้วย VPN กันอยู่ สำหรับโปรโตคอลที่สามารถใช้ในการทำงาน Site-to-Site VPN ก็คือ PPTP , L2F , L2TP , L2TP/IPSec และ IPSec(Tunnel mode) แต่ที่เป็นมาตรฐานและนิยมใช้กันโดยทั่วไปคือ IPSec

ความสามารถจริงแล้วการเชื่อมต่อแบบ Site-to-Site โดยไม่ผ่าน VPN นั้น สามารถทำได้โดยการเชื่อมผ่าน Leased Line หรือ Frame Relay แต่เนื่องจากต้องเสียค่าใช้จ่ายหรือค่าบริการที่ค่อนข้างสูง ดังนั้นจึงเป็นที่มาของ Site-to-Site VPN นั้นเอง จุดเด่นของ Site-to-Site VPN ก็คือค่าใช้จ่ายต่ำ ในขณะที่ได้ความปลอดภัยของข้อมูลในระดับสูงหรืออาจเทียบเท่ากับ Leased Line หรือ Frame Relay ได้ แต่ก็ต้องขึ้นอยู่

กับเทคโนโลยี VPN ที่เลือกใช้ด้วย สำหรับจุดอ่อนก็คือเรื่องของความเร็วในการรับส่งข้อมูลที่อาจจะเทียบเท่า Leased Line หรือ Frame Relay ไม่ได้

Remote Access VPN

ในที่นี้จะอธิบายเฉพาะ Remote Access VPN ซึ่งเป็น VPN ประเภทที่ใช้กันอยู่ทั่วไปเป็นส่วนใหญ่ สำหรับ Site-to-Site VPN ซึ่งเป็นประเภทที่ใช้น้อยกว่านั้นจะไม่อธิบาย รายละเอียดของ Remote Access VPN มีดังต่อไปนี้

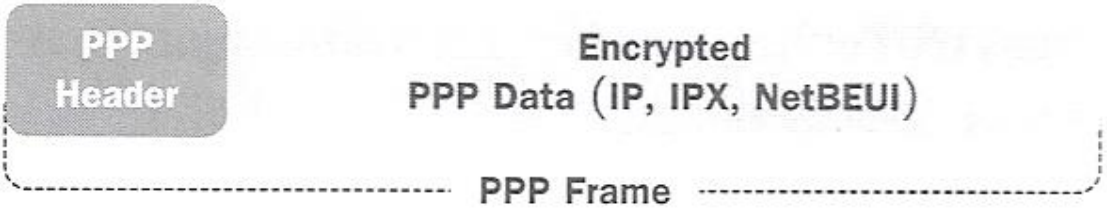
Compulsory และ Voluntary Tunnel

ในกรณีของ Remote Access VPN นั้นเครื่องลูกข่ายสามารถที่จะสร้างท่อรับส่งข้อมูลสำหรับ Tunnel ได้ใน 2 ลักษณะตามการใช้งาน ได้แก่

- Compulsory Tunnel (หรือ Mandatory Tunnel) คือการเชื่อมต่อ Remote Access VPN โดยวิธีการหมุนโมเด็มผ่ายสายโทรศัพท์จากเครื่องลูกข่ายไปยังอุปกรณ์ Remote Access Server (RAS) ที่มักจะตั้งอยู่ในที่ทำการของผู้ให้บริการอินเตอร์เน็ต การสร้างท่อรับส่งข้อมูล หรือ Tunnel จะเกิดขึ้นระหว่างอุปกรณ์ RAS และ VPN SERVER เท่านั้น การใช้งาน VPN ในลักษณะนี้มักจะเป็นบริการพิเศษของผู้ให้บริการอินเตอร์เน็ตที่หากต้องการใช้ก็ต้องเสียค่าบริการเพิ่ม
- Voluntary Tunnel คือการเชื่อมต่อ Remote Access VPN โดยที่การสร้างท่อรับส่งข้อมูลหรือ Tunnel เกิดขึ้นตั้งแต่เครื่องลูกข่ายจนถึงตัว VPN Server เลย เครื่องลูกข่ายสามารถเชื่อมต่ออินเทอร์เน็ตโดยการหมุนโมเด็ม, ADSL หรือแชร์อินเทอร์เน็ตจากระบบ LAN ภายในองค์กรก็ได้ การใช้งาน Remote Access VPNในปัจจุบันส่วนใหญ่จะเป็นแบบนี้เนื่องจากไม่ต้องสนใจว่าอุปกรณ์ RAS ของผู้ให้บริการอินเทอร์เน็ตจะสนับสนุนการเชื่อมต่อกับ VPN Server ได้หรือไม่

PPP (Point-to-Point Protocol)

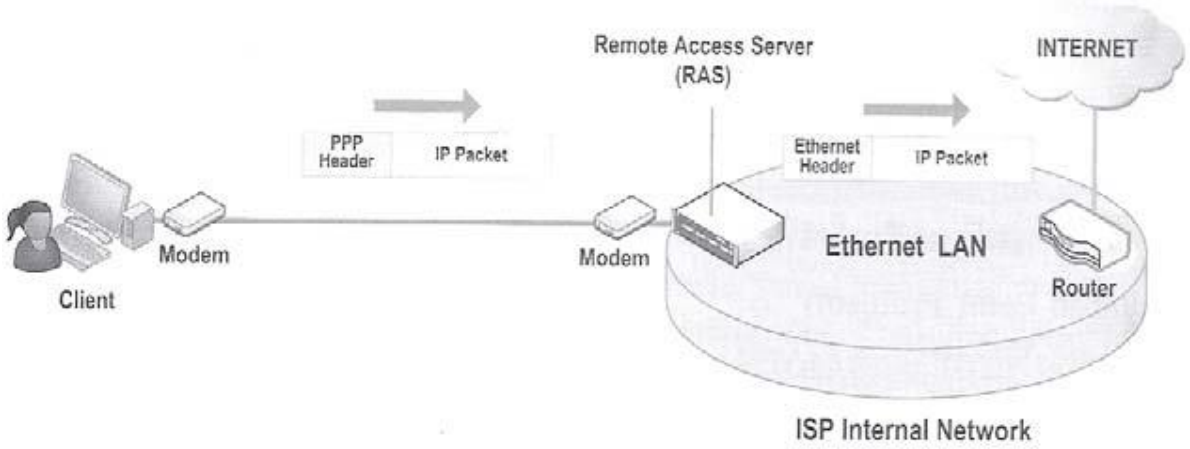
PPP คือ โปโตคอลที่เอื้ออำนวยให้เครื่องลูกข่ายสามารถเชื่อมต่อหรือเข้าถึงระบบเครือข่ายภายในองค์กรได้จากระยะไกล (Remote Access) ด้วยวิธีการหมุนโมเด็มผ่านสายโทรศัพท์ (Dial-up) ภายในตัวโปโตคอล PPP นั้นจะมีกลไกการรักษาความปลอดภัยของข้อมูลพร้อมสรรพในตัวมันเอง เช่น การตรวจยืนยันตัวผู้ใช้ (User Authentication) และ การเข้ารหัสข้อมูล (Encryption) เป็นต้น



รูปที่ 9.2 โครงสร้างของโปรโตคอล PPP

ที่มา : คู่มือดูแลระบบ Network ฉบับมืออาชีพ, 2551 : 336

โครงสร้างของโปรโตคอล PPP นั้นสามารถบรรจุแพ็กเก็ตของโปรโตคอลในระดับที่สูงกว่าไว้ภายในตัวได้ เช่น IP, IPX และ NetBEUI เป็นต้น ดังแสดงในรูปที่ 9.2 ซึ่งในกรณีนี้ PPP จะทำหน้าที่ขนถ่ายแพ็กเก็ตของโปรโตคอลในระดับสูงเหล่านั้นให้ไปถึงอุปกรณ์ RAS จะทำการถอดโครงสร้างส่วนหัว (Header) ของ PPP ออกให้เหลือเฉพาะเนื้อข้อมูล (Data) ซึ่งก็คือแพ็กเก็ตของโปรโตคอลระดับสูงที่บรรจุอยู่ข้างใน จากนั้นจึงส่งต่อเข้าไปยังระบบ LAN ภายในองค์กรเพื่อให้แพ็กเก็ตนั้นไปถึงเครื่องปลายทางได้



รูปที่ 9.3 การใช้งานอินเทอร์เน็ตโดยวิธีหมุนโมเด็ม

ที่มา : คู่มือดูแลระบบ Network ฉบับมืออาชีพ, 2551 : 336

สำหรับกลไกการรักษาความปลอดภัยของข้อมูลของ PPP นั้นจะประกอบด้วย การตรวจยืนยันตัวผู้ใช้ (User Authentication) ที่กระทำโดยฝั่งที่เป็นอุปกรณ์ RAS และ การเข้ารหัสข้อมูล (Encryption) ระหว่างต้นทางและปลายทาง โดยทั่วไปในระบบปฏิบัติการ Windows รุ่นใหม่ๆ นั้นจะมีความสามารถในการเชื่อมต่อกับอุปกรณ์ RAS หรือสามารถทำตัวเป็น RAS ได้ในตัวแต่ก็ต้องตั้งค่าให้ถูกต้องด้วย

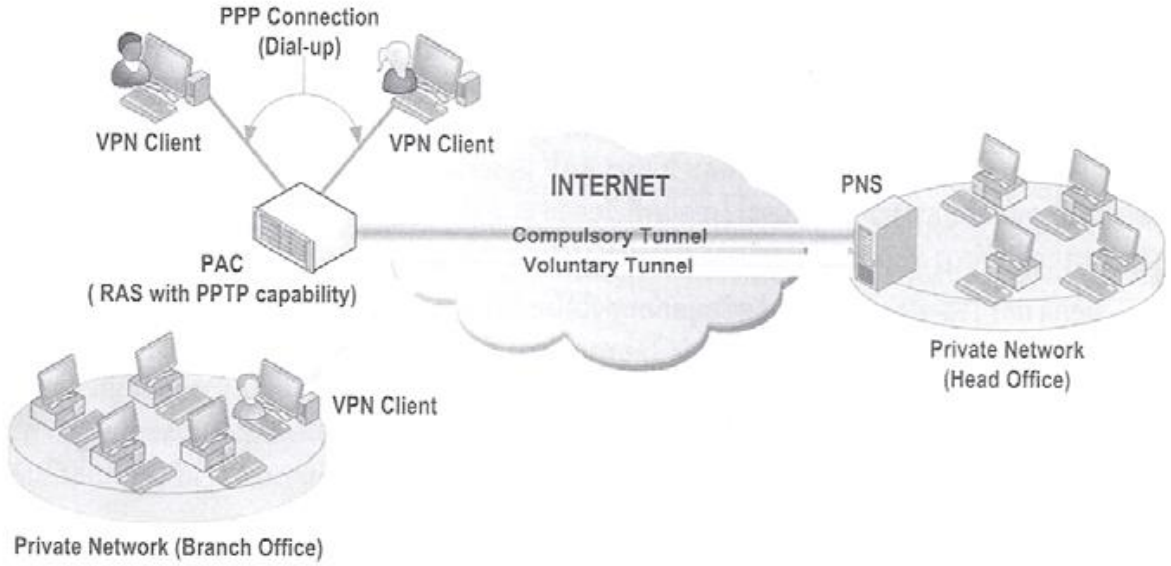
PPP และหลักการทำงานของ VPN

ดังที่ได้อธิบายไปแล้วว่า PPP คือโปรโตคอลที่มีการรักษาความปลอดภัยของข้อมูลพร้อมสรรพในตัวมันเอง เช่น การตรวจยืนยันตัวผู้ใช้ และ การเข้ารหัสข้อมูล ดังนั้นจึงเหมาะที่จะนำมาใช้ในการขนถ่ายข้อมูลผ่านอินเทอร์เน็ตหรือเครือข่าย IP แต่เนื่องจาก PPP ถูกออกแบบมาให้ทำงานเฉพาะการเชื่อมต่อผ่านโมเด็มและสายโทรศัพท์เท่านั้น หากสามารถทำให้ PPP สามารถเดินทางข้ามเครือข่ายอินเทอร์เน็ตหรือเครือข่าย IP ประเภทต่างๆ เช่นระบบ LAN ได้ก็จะเป็นการเพิ่มขอบเขตการทำงานของ PPP ออกไปได้ ดังนั้น วิธีการและทั้งหมดที่อธิบายไปข้างต้นก็คือหลักการทำงานของ VPN นั่นเอง

โปรโตคอลที่ใช้สำหรับ VPN

PPTP (Point-to-Point Tunneling Protocol)

PPTP (Point-to-Point Tunneling Protocol) คือโปรโตคอลที่ใช้สำหรับการทำ VPN ในรุ่นแรกๆ และยังใช้กันอยู่ในปัจจุบัน พัฒนาขึ้นโดยบริษัทไมโครซอฟท์ โดยทั่วไปมักใช้สำหรับการเชื่อมต่อเครื่องลูกข่ายเดี่ยวๆ จากระบบเครือข่ายภายนอกหรืออินเทอร์เน็ตเข้าสู่ระบบ LAN ภายในบริษัทหรือที่เรียกว่า Remote Access VPN (Client-to-LAN) โดยสามารถสนับสนุนการสร้างท่อรับส่งข้อมูลหรือ Tunnel ได้ทั้งแบบ Compulsory Tunnel และ Voluntary Tunnel

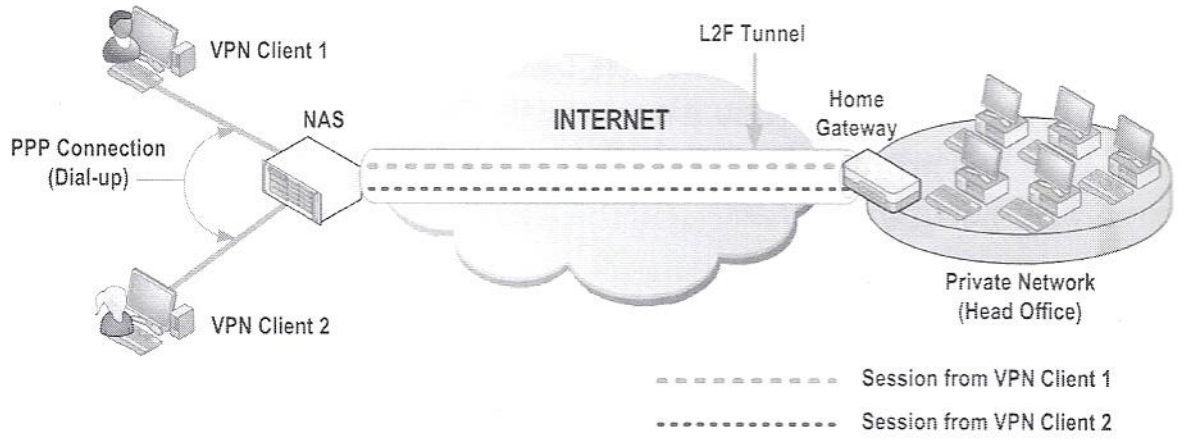


รูปที่ 9.4 PPTP โปรโตคอล

ที่มา : คู่มือดูแลระบบ Network ฉบับมืออาชีพ, 2551 : 338

L2F (Layer 2 Forwarding)

L2F คือโปรโตคอลที่พัฒนาโดยบริษัท Cisco Systems เพื่อใช้ทำ Remote Access VPN ในอุปกรณ์ยี่ห้อ Cisco เช่น Router หรือ Firewall เป็นหลัก ท่อหรือ Tunnel ที่สร้างขึ้นจะอยู่ระหว่างอุปกรณ์ NAS ซึ่งก็คืออุปกรณ์ RAS ที่มีความสามารถในการเชื่อมต่อกับอุปกรณ์ Cisco ที่ทำหน้าที่เป็น VPN Server จะเรียกว่า Home Gateway ดังแสดงในรูปที่ 9.5



รูปที่ 9.5 L2F โปรโตคอล

ที่มา : คู่มือดูแลระบบ Network ฉบับมืออาชีพ, 2551 : 341

L2F จะสนับสนุนการทำ Remote Access VPN แบบ Compusory Tunnel เท่านั้นกล่าวคือการสร้างท่อรับส่งข้อมูลหรือ Tunnel นั้น จะเกิดขึ้นระหว่างอุปกรณ์ NAS และ Home Gateway เท่านั้น ระหว่างเครื่องลูกข่ายและ NAS จะเป็นการเชื่อมต่อตามปกติ ภายในท่อรับส่งข้อมูลสามารถรองรับการขนถ่ายข้อมูลจากเครื่องลูกข่ายได้หลายเครื่องพร้อมกัน

L2F ทำงานในระดับ Data Link Layar หรือ Layar 2 ของดมเดล OSI สามารถขนถ่ายได้ทั้ง PPP และ SLIP ซึ่งเป็นโปรโตคอลที่ใช้งานบนสายโทรศัพท์หรือโมเด็มในรุ่นแรกๆ แต่ปัจจุบันถูกแทนที่โดย PPP ไปแล้ว

ใน PPTP นั่นจะมีการเปิดคอนเน็คชั่นแบบ TCP เพิ่มอีก 1 คอนเน็คชั่นที่เรียกว่า PPTP Control Connection โดยผ่านพอร์ต 1723 เพื่อใช้สำหรับแลกเปลี่ยนข้อมูลที่ใช้ควบคุมการทำงานของท่อรับส่งข้อมูล แต่สำหรับใน L2F นั้นจะอาศัยการแลกเปลี่ยนข้อมูลที่ใช้ควบคุมการทำงานโดยใช้ช่องทางเดียวกัน

กับการส่งข้อมูลปกติภายในท่อที่สร้างขึ้นนั่นเอง อธิบายอีกนัยหนึ่งคือ L2F จะอาศัยโปรโตคอล UDP ผ่านพอร์ต 1701 ในการสร้างท่อรับส่งข้อมูลหรือ Tunnel พร้อมกับการขนถ่ายข้อมูลภายในท่อ ดังนั้นการเชื่อมต่อผ่าน Firewall จึงต้องเปิดพอร์ต UDP หมายเลข 1701 ด้วย

L2F จะใช้วิธีการตรวจยืนยันตัวผู้ใช้เช่นเดียวกับ PPTP นั่นคือจะไปอาศัยกลไกภายในตัวของ PPP เอง แต่ก็ยังสามารถเลือกใช้การตรวจยืนยันตัวผู้ใช้ด้วยวิธีอื่นๆ ได้อีก เช่น TACACS+ และ RADIUS สำหรับการเข้ารหัสข้อมูลนั้นก็ใช้วิธีเดียวกันกับที่ใช้ใน PPTP ในปัจจุบัน L2F ไม่นิยมใช้กันแล้วเพราะถูกแทนที่โดย L2TP และ IPSec ที่จะอธิบายต่อไป

L2TP (Layer 2 Tunneling Protocol)

L2TP (Layer 2 Tunneling Protocol) คือโปรโตคอลที่เกิดจากการนำเอาข้อดีของ PPTPและ L2F มาผสมกัน แต่ค่อนข้างจะเอนเอียงไปทาง L2F มากหน่อย และยังคงใช้หลักการเดิมคือการขนถ่ายแพ็กเก็ตของ PPP ให้สามารถเดินทางผ่านเครือข่ายอินเทอร์เน็ตหรือระบบเครือข่ายแบบ IP นั่นเอง ดังนั้นการเข้ารหัสข้อมูลและการตรวจยืนยันตัวผู้ใช้ยังคงใช้กลไกภายในตัว PPP เองอยู่เช่นเดียวกับ PPTP และ L2F

ใน L2TP นั้นจะนิยมเรียกอุปกรณ์ VPN Server ว่า LNS (L2TP Network Server) และเรียกอุปกรณ์หรือเครื่องที่เชื่อมต่อกับ VPN Server ว่า LAC (L2TP Access Concentrator) โดยที่ LAC นั้นจะหมายถึงอุปกรณ์ Remote Access Server ที่มีความสามารถในการติดต่อกับ LNS ด้วยโปรโตคอล L2TP ได้โดยตรงนั่นเอง

L2TP/IPSec

L2TP/IPSec (อ่านว่า L2TP over IPSec) คือการผสมผสานระหว่าง L2TP และ IPSec ที่ทำงานในแบบ Transport Mode ทั้งนี้ก็เนื่องจากว่ากลไกการรักษาความปลอดภัยของข้อมูลภายในตัวของ PPP นั้นยังจัดอยู่ในระดับที่ไม่ค่อยปลอดภัยมากนัก การนำ IPSec มาช่วยในเรื่องของการเข้ารหัสข้อมูลและการตรวจยืนยันแหล่งที่มาของแพ็กเก็ตให้กับ L2TP จึงช่วยแก้ปัญหาดังกล่าวข้างต้น ประกอบกับภายในตัวของ L2TP เองนั้นก็ยังมีความสามารถในการตรวจยืนยันตัวผู้ใช้ด้วยรหัสผู้ใช้และรหัสผ่านที่ติดมากับแพ็กเก็ตของ PPP ที่บรรจุอยู่ข้างในด้วย ดังนั้น L2TP/IPSec จึงนับเป็นโปรโตคอลที่ให้ความปลอดภัยของข้อมูลสูง

มาก อย่างไรก็ตามข้อเสียของ L2TP/IPSec ก็คือไม่สามารถทำงานผ่านอุปกรณ์ NAT โดยทั่วๆ ไปได้ ซึ่งข้อเสียนี้ก็เป็นข้อเสียเดียวกันกับ IPSec นั่นเอง

ในระบบปฏิบัติการ Windows นั้น ตัว VPN Client จะสนับสนุนการทำ Remote Access VPN โดยผ่าน L2TP/IPSec โดยอัตโนมัติ แต่ถ้าคุณต้องการใช้ L2TP เพียวๆ โดยไม่มี IPSec เข้ามาช่วยก็สามารถทำได้โดยการแก้ไขข้อมูลใน Registry รายละเอียดสามารถศึกษาได้จากบทความ support.microsoft.com /kb/310109 ในเว็บไซต์ของไมโครซอฟต์

IPSec (IP Security)

IPSec (IP Security) เป็นโปรโตคอลที่ใช้ในการปกป้องข้อมูลในแพ็กเก็ตของ IP ให้ปลอดภัยจากการถูกดักอ่านข้อมูลภายในแพ็กเก็ตและการปลอมแปลงแพ็กเก็ต สำหรับเทคนิคที่ใช้ใน IPSec ประกอบด้วย การเข้ารหัสข้อมูล (Encryption) การป้องกันการแก้ไขหรือปลอมแปลงแพ็กเก็ต และการตรวจยืนยันแหล่งที่มาของแพ็กเก็ต (Authentication) เป็นต้น โดยทั่วไปแพ็กเก็ตของ IP มักจะบรรจุโปรโตคอลในระดับสูงขึ้นไปไว้ภายใน เช่น TCP หรือ UDP เป็นต้น ดังนั้น โปรโตคอลเหล่านี้จะได้รับการปกป้องโดย IPSec ไปด้วย IPSec จะทำงานในระดับ Layer 3 หรือ Network Layer ของโมเดล OSI ซึ่งเป็นระดับเดียวกับ IP และเนื่องจาก IPSec จะอาศัยกลไกการปกป้องข้อมูลที่ออกแบบไว้ในมาตรฐานของ TCP/IP เอง ดังนั้นมันจึงใช้งานได้เฉพาะในเครือข่ายแบบ IP เท่านั้น ในปัจจุบันผู้ผลิตอุปกรณ์ Firewall หรือ VPN โดยส่วนใหญ่จะสนับสนุนการทำ VPN โดยใช้ IPSec กันเป็นหลัก โดยสามารถใช้งานได้ทั้งในแบบ Site-to-Site และ Remote Access VPN

ส่วนประกอบของ IPSec

IPSec ประกอบด้วยโปรโตคอลย่อยอื่นๆ อีกหลายตัวที่ทำงานร่วมกัน แต่ที่สำคัญและขาดไม่ได้

1. Encapsulated Security Payload (ESP) คือโปรโตคอลที่ใช้ในการเข้ารหัสข้อมูลโดยใช้หลักการของ Symmetric Cryptography หรือการใช้กุญแจการเข้าและการถอดรหัสร่วมกันทั้งต้นทางและปลายทาง แพ็กเก็ตของ IP ที่ต้องการความปลอดภัยของข้อมูลสามารถใช้ ESP ในการเข้ารหัสข้อมูลก่อนส่งได้ แต่ขอบเขตการปกป้องข้อมูลในแพ็กเก็ตนั้นจะมีผลเฉพาะในส่วนของเนื้อข้อมูล (IP Data) ของแพ็กเก็ตเท่านั้น

2. Authentication Header (AH) คือโปรโตคอลที่ใช้ในการป้องกันการแก้ไขหรือปลอมแปลงแพ็กเก็ต โดยอาศัยการคำนวณค่า Checksum ซึ่งได้จากการนำเอาข้อมูลจากโครงสร้างส่วนหัวและเนื้อข้อมูลของแพ็กเก็ตพร้อมด้วยกุญแจการเข้ารหัสมาเข้าสูตรการคำนวณทางคณิตศาสตร์แล้วนำค่าที่ได้ไปบันทึกไว้ในโครงสร้างส่วนหัวของแพ็กเก็ตเพื่อให้ทั้งต้นทางและปลายทางสามารถใช้ในการตรวจสอบว่าแพ็กเก็ตที่ได้รับมานั้นไม่ได้ผ่านการปลอมแปลงมา และเนื่องจาก AH ใช้ทั้งข้อมูลในโครงสร้างส่วนหัวและเนื้อข้อมูลของแพ็กเก็ตมาคำนวณค่าChecksum ดังนั้นขอบเขตการปกป้องข้อมูลจะมีผลครอบคลุมทุกส่วนของแพ็กเก็ตด้วย

3. Internet Key Exchange (IKE) Protocol คือโปรโตคอลที่ใช้ในการตกลงรายละเอียดหรือวิธีการที่จะใช้ในการสร้างช่องทางการสื่อสารที่ปลอดภัยขึ้นระหว่างต้นทางและปลายทาง การทำงานของ IKE จะแบ่งออกเป็น 2 ขั้นตอน ดังนี้

3.1. Phase 1 เป็นการตกลงรายละเอียดหรือวิธีการที่จะใช้ในการสร้างช่องทางการสื่อสารที่ปลอดภัยขึ้นระหว่างต้นทางและปลายทาง เช่น วิธีการเข้ารหัสข้อมูล วิธีการป้องกันการแก้ไขหรือปลอมแปลงแพ็กเก็ต การสร้างกุญแจการเข้ารหัสข้อมูลที่จะใช้ร่วมกัน และวิธีการตรวจยืนยันตัวระหว่างกัน เป็นต้น ช่องทางการสื่อสารที่สร้างขึ้นในขั้นตอนนี้ยังถูกใช้งานต่อเนื่องในขั้นตอนที่ 2 ด้วย สำหรับวิธีการตรวจยืนยันตัวระหว่างกันนั้นแบ่งออกได้เป็น 3 วิธีหลักๆ คือ

1. Pre-shared Key คือการกำหนดรหัสลับซึ่งคล้ายๆ กับรหัสผ่านเพื่อให้ต้นทางและปลายทางใช้ในการยืนยันตัวระหว่างกัน

2. Digital Signature คือการที่ฝั่งต้นทางใช้ Private Key ของตัวเองซึ่งถูกเก็บเป็นความลับไว้มาทดลองเข้ารหัสข้อมูลเพื่อส่งไปให้ปลายทางทดลองถอดรหัสด้วย Public Key ที่เผยแพร่ไว้ โดยฝั่งต้นทางเพื่อให้ใช้คู่กัน หากปลายทางสามารถถอดรหัสได้ก็แสดงว่าข้อมูลที่ได้รับนั้นมาจากต้นทางที่

3. Self Signed certificate คือการใช้เทคนิคและวิธีการของ Digital Certificate นั่นเอง แต่ที่ต่างกันคือ Self Signed Certificate นั้นจะออกโดยผู้ดูแลระบบเพื่อใช้ภายในองค์กรเอง ทำให้ประหยัดค่าใช้จ่ายในการขอมี และยังสะดวกในการบริการอีกด้วย

3.2. Phase 2 เป็นการตกลงรายละเอียดหรือวิธีการที่ใช้ในการปกป้องระหว่างต้นทางและปลายทาง เพื่อใช้ในการทำงานของโปรโตคอล ESP และ AH โดยอาศัยช่องทางการสื่อสารที่สื่อสารขึ้นในขั้นตอนนี้จะมีการตกลงระหว่างต้นทางและปลายทางเพื่อสร้างกุญแจการเข้ารหัสข้อมูลสำหรับ ESP และ AH ที่ใช้ร่วมกันทั้งสองฝ่ายขึ้นใหม่จำนวน 2 ชุด โดยชุดที่ 1 ใช้สำหรับการส่งข้อมูล และ ชุดที่ 2 ใช้สำหรับการรับข้อมูล กุญแจเข้ารหัสดังกล่าวนี้จะหมดอายุภายในเวลาสั้นๆ และต้องมีการสร้างขึ้นใหม่อยู่เป็นระยะๆ ตลอดการสื่อสารทั้งนี้เพื่อเป็นการเพิ่มความปลอดภัยของข้อมูลให้มากยิ่งขึ้นนั่นเอง

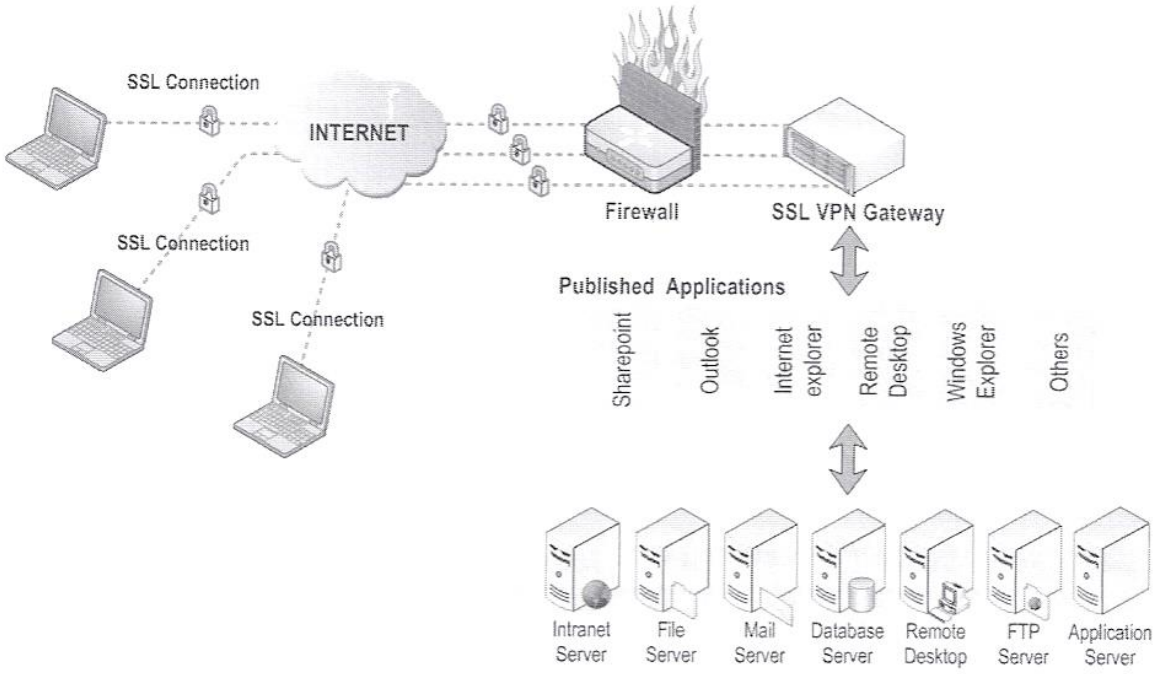
สรุปข้อดีข้อเสียของ IPSec

คุณสมบัติของ IPSec ที่เป็นจุดเด่นก็คือเรื่องของการเข้ารหัสข้อมูล การป้องกันการปลอมแปลงแพ็กเก็ตและการตรวจยืนยันแหล่งที่มาของแพ็กเก็ตได้ สามารถป้องการ Replay ได้ (การ Replay หมายถึงการแอบเก็บบันทึกแพ็กเก็ตที่เกิดจากการสื่อสารระหว่างเครื่อง 2 เครื่อง ไว้จากนั้นอาจมีการเปลี่ยนแปลงหรือแก้ไข)

SSL VPN (Secure Sockets Layer Virtual Private Network)

SSL VPN หรือมีชื่อเรียกอีกอย่างหนึ่งคือ SSL/TLS VPN โดยที่ SSL คือ Secure Socket Layer และ TLS คือ (Transport Layer Security) แต่ในที่นี้จะขอเรียกเป็น SSL VPN

SSL VPN คือเทคนิคที่เปิดโอกาสให้ผู้ใช้หรือเครื่องลูกข่ายที่อยู่ภายนอกหรืออินเตอร์เน็ตสามารถเข้าใช้งานแอพพลิเคชั่นภายในระบบ LAN ได้อย่างปลอดภัยโดยอาศัยโปรแกรมเว็บบราวเซอร์ควบคู่กับการเข้ารหัสข้อมูลด้วยเทคโนโลยีของ SSL นั่นเอง การใช้โปรแกรมเว็บบราวเซอร์ควบคู่กับเทคโนโลยีของ SSL นั่นเอง การใช้โปรแกรมเว็บบราวเซอร์ควบคู่กับเทคโนโลยีของ SSL นั้นไม่ใช่ของใหม่แต่อย่างใด เพียงแต่ว่าในอดีตนั้นมันถูกใช้เพื่อการทำธุรกิจหรือธุรกรรมผ่านอินเตอร์เน็ตเสียส่วนใหญ่ แต่ในปัจจุบันกลับได้รับความนิยมในการนำมาประยุกต์ใช้กับ Remote Access VPN ด้วย



รูปที่ 9.6 SSL VPN

ที่มา : คู่มือดูแลระบบ Network ฉบับมืออาชีพ, 2551 : 369

ข้อดีของ SSL VPN คือเครื่องลูกข่ายที่เชื่อมต่อผ่านอินเตอร์เน็ตจะไม่จำเป็นต้องติดตั้งโปรแกรม หรือซอร์ฟแวร์ประเภท VPN Client เหมือน IPSec หรือ PPTP แต่อย่างใด ขอเพียงมีโปรแกรมบราวเซอร์ในเครื่องก็สามารถใช้งานได้แล้ว นอกจากนี้ในฝั่งของVPN Server หรือ SSL VPN Gateway ที่อยู่หลังอุปกรณ์ก็ไม่ต้องมีการเซ็ตอัพ ให้ยุ่งยากแต่อย่างใด สามารถใช้งานงานผ่านอุปกรณ์ NAT ได้โดยไม่มีปัญหาเนื่องจากมันอาศัยโปรโตคอล HTTP และ HTTPS ในการทำงาน นอกจากนี้ยังสามารถหรือจำกัดโปรแกรมที่ต้องการเปิดให้ใช้ได้เป็นตัวๆ ไป หรือที่เราเรียกว่า Publish แทนที่จะเปิดให้เครื่องลูกข่ายสามารถมองเห็นหรือเข้าถึงได้ทั้งระบบเครือข่ายเหมือนในกรณีของ IPSes, PPTP หรือ L2TP

จุดอ่อนของ SSL VPN ก็คือการตรวจยืนยันตัว (Authentication) หรือการแสดงตนว่าเป็นเครื่องคอมพิวเตอร์ที่เป็นตัวจริงหรือไม่ใช่ เครื่องที่ปลอมแปลงขึ้นมานั้น มักจะกระทำแค่เพียงในฝั่งของเครื่องเซิร์ฟเวอร์ (เครื่องที่ทำหน้าที่ SSL VPN Gateway) เท่านั้น ซึ่งโดยทั่วไปจะใช้วิธีการจดทะเบียนเพื่อขอรับ SSL Certificate จากบริษัทหรือตัวแทน CA (Certificate Authority) แล้วนำมาติดตั้งลงในเครื่อง ในขณะที่ทางฝั่งเครื่องลูกข่ายนั้นมักจะใช้วิธีการตรวจยืนยันตัวโดยใช้รหัสผู้ใช้และรหัสผ่านซึ่งอาจเป็นช่องโหว่ในการถูกบุกรุกหรือโจมตีด้วยวิธี MIMT (Man-in-the-middle) Attack ได้

อย่างไรก็ตามหากต้องการใช้วิธีการตรวจยืนยันตัวของเครื่องลูกข่ายโดยใช้ SSL Certificate เหมือนทางฝั่งเซิร์ฟเวอร์นั้นก็สามารถทำได้เช่นกัน แต่ก็ต้องไปขอจดทะเบียน SSL Certificate กับ CA ให้กับเครื่องลูกข่ายแต่ละเครื่อง ซึ่งอาจเสียค่าใช้จ่ายและค่าดูแลรักษาเพิ่มอีกพอสมควร แต่ผู้ดูแลระบบสามารถเลี่ยงไปใช้วิธีที่เรียกว่า Self Signed Certificate หรือการออก SSL Certificate เพื่อใช้เองภายในองค์กร

SSL VPN นั้นมักจะถูกนำมาเปรียบเทียบกับ IPSec ซึ่งนิยมใช้กันเป็นส่วนใหญ่ในปัจจุบัน โดยมีข้อดีในแง่ที่ว่า ไม่ต้องติดตั้งซอฟต์แวร์หรือโปรแกรมใดๆ ในเครื่องขอเพียงมีโปรแกรมบราวเซอร์ในเครื่องก็พอ ทำให้ง่ายต่อการใช้งาน อีกทั้งยังช่วยลดปัญหาต่างๆ ที่อาจเกิดขึ้นจากการใช้งาน Remote Access VPN ผ่าน IPSec

โปรโตคอลของ VPN สมัยใหม่ๆ

Open VPN

ความหมายของคำว่า SSL VPN ตามที่ได้อธิบายไปแล้วข้างต้นนั้น ปัจจุบันมีหลายคนโต้แย้งว่า SSL VPN ไม่น่าจะจัดเป็นเทคโนโลยีของ VPN เลย และควรจะเรียกเป็น Application Gateway ซึ่งจัดเป็น Reverse Proxy Server ชนิดหนึ่งไปเลยมากกว่า แต่เนื่องจากมีผู้ผลิตหลายรายต่างก็เรียกผลิตภัณฑ์ของตนที่ทำงานในลักษณะของ Application Gateway ว่าเป็น SSL VPN Gateway กันไปหมดแล้ว จะด้วยความจงใจหรือเข้าใจผิดก็ตาม จึงทำให้เกิดความสับสนในกลุ่มผู้ใช้หรือผู้บริโภคไปทั่ว ประกอบกับในปัจจุบันยังมีซอฟต์แวร์ที่เป็น Open Source ตัวหนึ่งที่เรียกว่า Open VPN จะไม่ได้เกี่ยวข้องกับโปรแกรมเว็บบราวเซอร์เพื่อเน้นว่าเป็น “Clientless” แต่อย่างใด

Open VPN นั้นจะมีลักษณะหรือหลักการทำงานที่คล้ายคลึงกับ IPSec มากกว่า เครื่องลูกข่ายที่ต้องการเชื่อมต่อโดยใช้ Open VPN จะต้องติดตั้งซอฟต์แวร์ Open VPN Client เพิ่มเหมือนในกรณีของ IPSec และมีการสร้างท่อ (Tunnel) ระหว่างเครื่อง Open VPN Client และ Open VPN Server โดยใช้เทคนิคการเข้ารหัสของ SSL ซึ่งเป็นเทคนิคการเข้ารหัสในระดับ Transport Layer (เข้ารหัสเฉพาะในส่วนของเนื้อข้อมูลในแพ็กเก็ตของ TCP หรือ UDP) ดังนั้นมันจึงไม่มีปัญหาในการทำงานผ่านอุปกรณ์ NAT เหมือนดังกรณี IPSec สำหรับพอร์ตที่ใช้โดย Open VPN ในปัจจุบันจะใช้พอร์ต UDP 1194 เป็นพอร์ตมาตรฐาน (หรือสามารถตั้งเองโดยผู้ดูแลระบบได้) ดังนั้นในกรณีที่ต้องใช้ Open VPN Server อยู่ภายหลังอุปกรณ์ NAT หรือ Firewall ก็ต้องทำ Port mapping หรือเปิดพอร์ตให้ถูกต้องตรงกันไว้ด้วย

SSTP (Secure Socket Tunneling Protocol)

SSTP ก็คือโปรโตคอล VPN ตัวใหม่ของไมโครซอฟต์ ที่อาศัยโปรโตคอล HTTPS และเทคนิคของ SSL ในการเข้ารหัสข้อมูล เช่นเดียวกับ SSL VPN ดังนั้นบางคนจึงเรียก SSTP ว่า Microsoft SSL VPN เริ่มมีใช้กันใน Windows รุ่นใหม่ๆ เช่น Vista Service Pack 1 และ Windows Server 2008 สำหรับพอร์ตที่ใช้โดย SSTP ก็คือพอร์ต TCP 443 ที่ใช้โดยโปรโตคอล HTTPS นั่นเอง อย่างไรก็ตามในการใช้งาน SSTP เครื่องที่ทำหน้าที่เป็น VPN Server (SSTP VPN Server) จะไม่จำเป็นต้องติดตั้งหรือเปิดบริการเว็บเซิร์ฟเวอร์ IIS ไว้แต่อย่างใด เนื่องจากไม่เกี่ยวข้องกันอธิบายเพิ่มเติมคือ พอร์ต 443 ที่ใช้นั้นจะถูกจัดการโดยบริการ Routing and Remote Access Service ตัวใหม่ที่ใช้ใน Windows Server 2008 อย่างไรก็ตามตัว IIS และ Routing and Remote Access Service สามารถทำงานด้วยกันได้โดยไม่มีปัญหา SSTP ยังสามารถรองรับ IPv6 ด้วย คาดว่าในอนาคต SSTP คงจะมาแทนที่เทคโนโลยีของ VPN เดิมๆที่ใช้กันใน Windows รุ่นปัจจุบัน เช่น PPTP และ L2TP/IPSec เนื่องจากมันมีข้อดีคือ สามารถผ่านเข้าออกตัวอุปกรณ์ NAT หรือ Firewall ได้โดยไม่มีปัญหา