VPN คืออะไร

นำเสนอเมื่อ 8 ต.ค. 2551

VPN หรือ **Virtual Private Network** หมายถึง เครือข่ายเสมือนส่วนตัว ที่ทำงานโดยใช้ โครงสร้างของเครือข่ายสาธารณะ หรืออาจจะวิ่งบน เครือข่ายไอพีก็ได้ แต่ยังสามารถ คงความเป็นเครือข่ายเฉพาะ ขององค์กรได้ ด้วยการ เข้ารหัสแพ็กเก็ตก่อนส่ง เพื่อให้ข้อมูล มีความปลอดภัยมากขึ้น

อย่างไรก็ดี คำว่า VPN จะครอบคลุมทั้งอุปกรณ์ฮาร์ดแวร์ (เช่น Gateway และ Router), ซอฟต์แวร์ และส่วนที่เป็นไฟร์วอลล์

การเข้ารหัสแพ็กเก็ต เพื่อทำให้ข้อมูล มีความปลอดภัยนั้น ก็มีอยู่หลายกลไกด้วยกัน ซึ่งวิธีเข้ารหัสข้อมูล (encryption) จะทำกันที่เลเยอร์ 2 คือ Data Link Layer แต่ปัจจุบัน มีการเข้ารหัสใน IP Layer โดยมักใช้เทคโนโลยี IPSec (IP Security)

ปกติแล้ว VPN ถูกนำมาใช้กับองค์กรขนาดใหญ่ ที่มีสาขาอยู่ตามที่ต่างๆ และต้องการ ต่อเชื่อมเข้าหากัน โดยยังคงสามารถ รักษาเครือข่ายให้ใช้ได้เฉพาะ คนภายในองค์กร หรือคนที่เกี่ยวข้องด้วย เช่น ลูกค้า, ซัพพลายเออร์ เป็นต้น

นอกจากนี้แล้ว กลไกในการสร้างโครงข่าย VPN อีกประเภทหนึ่ง คือ MPLS (Multiprotocal Label Switch) เป็นวิธีในการส่งแพ็กเก็ต โดยการใส่ label ที่ส่วนหัว ของข้อความ และค่อยเข้ารหัสข้อมูล จากนั้น จึงส่งไปยังจุดหมายปลายทาง เมื่อถึงปลายทาง ก็จะถอดรหัสที่ส่วนหัวออก วิธีการนี้ ช่วยให้ผู้วางระบบเครือข่าย สามารถแบ่ง Virtual LAN เป็นวงย่อย ให้เป็น เครือข่ายเดียวกันได้

ตัวอย่างเช่น บริษัท A ก็จะได้ VPN label A ที่หัวข้อความ ของทุกแพ็กเก็ต บริษัท B ได้รหัสที่หัวข้อความเป็น B เพื่อส่งข้อมูล ข้อมูลที่ส่งออกไป ก็จะวิ่งไปหาปลายทางตาม Label ของตน ซึ่งผู้วางระบบ สามารถเพิ่มกลุ่มในวง VLAN ได้อย่างไม่จำกัด

รูปแบบบริการ VPN

บริการ VPN แบ่งออกเป็น 3 รูปแบบ

1. Access VPN: เป็นรูปแบบในการเข้าถึงเครือข่าย VPN จากอุปกรณ์เคลื่อนที่ต่างๆ ซึ่งสามารถเข้าถึงเครือข่ายได้ใน 2 ลักษณะ โดยลักษณะแรก เป็นการเข้าถึงจากไคลเอ็นต์ใดๆ ก็ได้ โดยอาศัย ผู้ให้บริการอินเทอร์เน็ต เป็นตัวกลาง ในการติดต่อ ซึ่งจะมีการเข้ารหัสในการ ส่งสัญญาณ จากเครื่องไคลเอ็นต์ ไปยังไอเอสพี และลักษณะที่สอง เป็นการเข้าถึง จากเครื่องแอ็กเซสเซิร์ฟเวอร์ (Network Access Server-NAS) โดยเริ่มต้นจาก ผู้ใช้หมุนโมเด็ม ติดต่อมายังไอเอสพี และจากนั้น จะมีการเข้ารหัสข้อมูล และส่งต่อไปยังปลายทาง

2. Intranet VPN: เป็นรูปแบบในการเข้าถึงเครือข่าย VPN ที่ใช้เฉพาะภายในองค์กรเท่านั้น อาทิ การต่อเชื่อมเครือข่าย ระหว่างสำนักงานใหญ่ในกรุงเทพฯ และสาขาย่อย ในต่างจังหวัด เสมือนกับ การทดแทน การเช่าวงจรลีสไลน์ ระหว่าง กรุงเทพกับต่างจังหวัด โดยที่แต่ละสาขา สามารถ ต่อเชื่อมเข้ากับ ผู้ให้บริการอินเทอร์เน็ต ในท้องถิ่นของตน เพื่อเชื่อมเข้า โครงข่าย VPN ขององค์กรอีกทีหนึ่ง

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

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 ให้ความคล่องตัว ในการเปลี่ยนแปลง เช่น การขยายเครือข่าย ในอนาคต

นอกจากนี้แล้ว ในแง่ของ ผู้ให้บริการอินเทอร์เน็ต การออกบริการ VPN ก็เป็นอีกทางเลือกหนึ่ง ที่ช่วยให้ ลูกค้าของไอเอสพี ประหยัดค่าใช้จ่าย และสะดวกสบายมากขึ้น

แหล่งอ้างอิง : http://www.cisco.com