คู่มือองค์ความรู้

เรื่อง

การพัฒนาคลังข้อมูลสารสนเทศเศรษฐกิจอุตสาหกรรม

จัดทำโดย

คณะทำงานการพัฒนาคลังข้อมูลสารสนเทศเศรษฐกิจอุตสาหกรรม

คำนำ

สำนักงานเศรษฐกิจอุตสาหกรรม (สศอ.) เป็นหน่วยงานที่ทำหน้าที่เกี่ยวกับการเสนอแนะนโยบาย แผน ยุทธศาสตร์ มาตรการด้านการพัฒนาอุตสาหกรรมของประเทศในระดับมหภาคและอุตสาหกรรมรายสาขา รวมทั้งพัฒนาระบบเตือนภัยด้านอุตสาหกรรม เพื่อเป็นองค์กรชี้นำในการพัฒนาอุตสาหกรรมของประเทศให้เติบโตอย่างต่อเนื่องและยั่งยืน ส่งสัญญาณเตือนภัยทางอุตสาหกรรมอย่างถูกต้องและมีประสิทธิภาพ

สำหรับในปีงบประมาณ พ.ศ. 2553 สำนักงาน ก.พ.ร. กำหนดให้ส่วนราชการดำเนินการตามเกณฑ์คุณภาพการบริหารจัดการภาครัฐ PMQA ในหมวด 4 การวัด การวิเคราะห์และการจัดการความรู้ (IT 1-IT 7) เป็นหมวดบังคับ โดยเฉพาะ IT 7 การจัดการความรู้จะต้องมีองค์ความรู้ที่จำเป็นต่อการปฏิบัติราชการตามประเด็นยุทธศาสตร์ 3 องค์ความรู้ คณะทำงานจัดทำความรู้ในการพัฒนาคลังข้อมูลสารสนเทศเศรษฐกิจอุตสาหกรรม สำนักงานเศรษฐกิจอุตสาหกรรม ประจำปีงบประมาณ พ.ศ. 2553 ได้จัดทำคู่มือการพัฒนาคลังข้อมูลสารสนเทศเศรษฐกิจอุตสาหกรรม ซึ่งเป็นความรู้ตามประเด็นยุทธศาสตร์ที่ 2 ขึ้น เพื่อใช้เป็นคู่มือการปฏิบัติงาน (Working Manual) สำหรับเจ้าหน้าที่ สศอ. และผู้ที่สนใจทั่วไป โดยคู่มือประกอบด้วยเนื้อหา 5 ส่วน ได้แก่ ส่วนที่ 1 บทนำ ส่วนที่ 2 การรวบรวมความต้องการและศึกษาข้อมูล ส่วนที่ 3 การออกแบบระบบคลังข้อมูลสารสนเทศเศรษฐกิจอุตสาหกรรม ส่วนที่ 4 การพัฒนาระบบคลังข้อมูลสารสนเทศเศรษฐกิจอุตสาหกรรม ส่วนสุดท้าย ภาคผนวก

คณะผู้จัดทำ หวังเป็นอย่างยิ่งว่า คู่มือเล่มนี้จะเป็นประโยชน์ต่อเจ้าหน้าที่ สศอ. และผู้ที่สนใจทั่วไปนำไปใช้เป็นแนวทางในปฏิบัติการทำงานได้อย่างถูกต้องและมีประสิทธิภาพ ทั้งนี้หากมีข้อผิดพลาดประการใด ขออภัยมา ณ ที่นี้ด้วย

คณะทำงานจัดทำความรู้ในการพัฒนาคลังข้อมูล

สารสนเทศเศรษฐกิจอุตสาหกรรม

สำนักงานเศรษฐกิจอุตสาหกรรม (สศอ.)

สารบัญ

		หน้า
บทที่ 1	บทนำ	1
บทที่ 2	การรวบรวมความต้องการและศึกษาข้อมูล	3
บทที่ 3	การออกแบบระบบคลังข้อมูลประกอบ	5
บทที่ 4	การพัฒนาระบบคลังข้อมูลสารสนเทศเศรษฐกิจอุตสาหกรรม	7
ภาคผนวก ก:		**13**
	เทคโนโลยี VPN คืออะไร	13
	ส่วนประกอบที่ใช้ในการสถาปัตยกรรมแบบ VPN	25
	ข้อดี และข้อเสียของ VPN	30

บทที่ 1

บทนำ

กระทรวงอุตสาหกรรมได้เสนอเรื่องต่อคณะรัฐมนตรีเมื่อวันที่ 26 มิถุนายน 2533 ขอปรับปรุงฐานะของกองเศรษฐกิจอุตสาหกรรม สำนักงานปลัดกระทรวงอุตสาหกรรมให้เป็นสำนักงานเทียบเท่ากรม เพื่อเพิ่มขีดความสามารถในการปฏิบัติงานนโยบายและแผนพัฒนาอุตสาหกรรมให้มีประสิทธิภาพยิ่งขึ้น และคณะรัฐมนตรีได้มีมติเห็นชอบ ในการจัดตั้งสำนักงานเศรษฐกิจอุตสาหกรรม โดยให้โอนงานของสำนักงานพัฒนาอุตสาหกรรมหลัก สำนักงานปลัด กระทรวงอุตสาหกรรมมารวมเข้าด้วยกันตามพระราชบัญญัติปรับปรุงกระทรวง ทบวง กรม พ.ศ. 2534 และพระราชบัญญัติโอนอำนาจหน้าที่ และกิจการบริหารงานบางส่วนของสำนักงานปลัดกระทรวงอุตสาหกรรม (กองเศรษฐกิจ อุตสาหกรรม และสำนักงานพัฒนาอุตสาหกรรมหลัก) กระทรวงอุตสาหกรรม ไปเป็นของสำนักงานเศรษฐกิจอุตสาหกรรม กระทรวงอุตสาหกรรม พ.ศ.2534 โดยได้ประกาศในราชกิจจานุเบกษา เล่ม 108 ตอนที่ 156 ลงวันที่ 4 กันยายน พ.ศ. 2534 โดยให้มีผลใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษา ดังนั้นจึงได้ถือเอา วันที่ 5 กันยายน 2534 เป็นวันก่อตั้ง สศอ. ตั้งแต่นั้นมา

อำนาจหน้าที่

1. บริหารราชการทั่วไปของสำนักงานเศรษฐกิจอุตสาหกรรม และราชการที่มิได้กำหนดให้เป็นอำนาจหน้าที่ ของส่วนราชการใดในสังกัดกระทรวงโดยเฉพาะ
2. เสนอแนะนโยบายของกระทรวงให้สอดคล้องกับแผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ และนโยบายของรัฐบาลรวมทั้งการจัดทำแผนแม่บทประสานแผนปฏิบัติงานละเสนอนโยบายในการก่อตั้งและจัดสรรงบประมาณประจำปีของหน่วยงานในสังกัดกระทรวง
3. กำกับ เร่งรัด ติดตาม และประเมินผลการปฏิบัติงานตามแผนงานและโครงการของหน่วยงานในสังกัด กระทรวง
4. จัดทำรายงานภาวะเศรษฐกิจอุตสาหกรรมสาขาต่าง ๆ เพื่อเป็นพื้นฐานในการกำหนดนโยบายและวางแผน การพัฒนาอุตสาหกรรม และหาวิธีการแก้ปัญหาหรือพัฒนาเทคโนโลยีอุตสาหกรรมในสาขาต่าง ๆ
5. กำหนดนโยบายในการสำรวจการเก็บรักษาและการใช้ประโยชน์ข้อมูลของหน่วยงานในสังกัดกระทรวง และทำหน้าที่เป็นศูนย์ข้อมูลของกระทรวง
6. ปฏิบัติการอื่นใดตามที่กฎหมายกำหนดให้เป็นหน้าที่ของสำนักงานเศรษฐกิจอุตสาหกรรม

สถานที่ตั้ง สศอ.

เริ่มแรกอาศัยที่อยู่อาคารนารายณ์ ของกระทรวงอุตสาหกรรมเป็นที่ทำการตั้งแต่เดือนเมษายน 2535 - พฤษภาคม 2537 เมื่อกรมโรงงานอุตสาหกรรมได้สร้างอาคารใหม่เสร็จสิ้นแล้วจึงได้ย้ายที่ทำการมาอาศัยตึกกรมโรงงานอุตสาหกรรมอยู่ชั่วคราวตั้งแต่ พฤษภาคม 2537 - ตุลาคม 2543 แล้วจึงได้ย้ายเข้ามาอยู่อาคารของ สศอ. เอง ซึ่งตั้งอยู่ในบริเวณกระทรวงอุตสาหกรรม ระหว่างกรมทรัพยากรธรณี และกรมส่งเสริมอุตสาหกรรม ตั้งแต่เดือนตุลาคม 2543 เป็นต้นมาจนถึงปัจจุบัน โดยแบ่งโครงสร้างการบริหารราชการของ สศอ. ดังนี้

สำนักวิจัยเศรษฐกิจอุตสาหกรรม : อำนาจหน้าที่ความรับผิดชอบ

- จัดหาและรวบรวมข้อมูลเศรษฐกิจมหภาค และเป็นหน่วยสารสนเทศเชิงลึกของกระทรวง รวมถึงการเชื่อมโยงเครือข่ายข้อมูลกับหน่วยงานอื่นที่เกี่ยวข้อง
- วิเคราะห์ และวิจัยประเด็นทางเศรษฐกิจที่มีผลต่อการพัฒนาอุตสาหกรรมของประเทศ และติดตามสถานการณ์ รวมทั้งคาดการณ์แนวโน้มและเตือนภัยภาคอุตสาหกรรมโดยรวม
- พัฒนาเครื่องมือทางเศรษฐศาสตร์เพื่อสนับสนุนการศึกษาวิเคราะห์และวิจัยทางเศรษฐกิจอุตสาหกรรม
- ปฏิบัติงานร่วมหรือสนับสนุนการปฏิบัติงานของหน่วยงานอื่นที่เกี่ยวข้อง หรือที่ได้รับมอบหมาย

บทที่ 2

การรวบรวมความต้องการและศึกษาข้อมูล

โครงข่ายคลังข้อมูลเศรษฐกิจอุตสาหกรรม

เนื่องจากสำนักงานเศรษฐกิจอุตสาหกรรม มีหน้าที่ในการวางนโยบาย แผนยุทธศาสตร์ การพัฒนาอุตสาหกรรม และยังมีหน้าที่จัดทำสารสนเทศเศรษฐกิจอุตสาหกรรม ระบบเตือนภัยอุตสาหกรรมที่ทันสมัย เชื่อถือได้ และเชื่อมโยงกับหน่วยงานที่เกี่ยวข้อง และยังให้บริการเผยแพร่ข้อมูล สร้างความเข้มแข็งให้เป็นองค์กรแห่งความความรู้ด้านเศรษฐกิจอุตสาหกรรม การดำเนินการจัดการข้อมูลจึงเป็นสิ่งจำเป็น และสำคัญในการที่จะมาช่วยในการทำสถิติ และดัชนีอุตสาหกรรมต่าง ๆ เพื่อให้ได้ข้อมูลที่มีประสิทธิภาพ นำไปวิเคราะห์ข้อมูลเชิงลึกในด้านต่าง ๆ และสามารถนำเสนอต่อผู้บริหารของกระทรวงอุตสาหกรรมเพื่อช่วยในการบริหารงานจัดการข้อมูลอุตสาหกรรมได้

สำนักงานเศรษฐกิจอุตสาหกรรมจึงมีแนวคิดที่จะทำการรวบรวมข้อมูลเศรษฐกิจอุตสาหกรรมจากหน่วยงานต่าง ๆ เพื่อนำมาวิเคราะห์ และจัดทำอุตสาหกรรมรายสาขา โดยข้อมูลที่ได้จะต้องเป็นข้อมูลที่ถูกต้อง และทันเวลา อีกทั้งยังต้องมีความสะดวก รวดเร็ว ในการรวบรวม จัดเก็บ วิเคราะห์ และใช้งาน

2. การรวบรวมความต้องการและศึกษาข้อมูล

2.1 การกำหนดกรอบและคัดเลือกข้อมูล

เนื่องจากการรวบรวมข้อมูลจากสถาบันและหน่วยงานต่าง ๆ จะเป็นการทำงานแบบอัตโนมัติ มีความสะดวก รวดเร็วในการรวบรวม และยังมีระบบรักษาความปลอดภัยของข้อมูล จึงนำเสนอโครงข่ายข้อมูลที่มีระบบการรักษาความปลอดภัยของข้อมูลสูง โดยใช้เครือข่าย Internet เป็นเส้นทางรวบรวมข้อมูล ซึ่งมีการใช้เทคโนโลยี VPN (Virtual Private Network) หรือเรียกว่าเครือข่ายส่วนตัวเสมือน โดย VPN จะทำให้การเชื่อมโยงสื่อสารในโครงข่าย Internet มีความปลอดภัยเสมือนมีการใช้โครงข่ายที่เป็น Intranet หรือสายเช่าสัญญาณเฉพาะโครงข่าย เพราะมีการเข้ารหัสข้อมูลที่มีการส่งจากต้นทางไปยังปลายทาง โดยเส้นทางจะถูกสร้างในลักษณะคล้ายอุโมงค์จากต้นทางไปถึงปลายทาง ทำให้ผู้ไม่มีสิทธิไม่สามารถเข้าถึงข้อมูลได้

2.2 การกำหนดกรอบข้อมูลและศึกษาความสัมพันธ์ มีรายละเอียดการดำเนินการดังนี้

- กำหนดรูปแบบและวิธีการในการรวบรวมข้อมูล พร้อมสร้างมาตรฐานในการแลกเปลี่ยนข้อมูลระหว่างสำนักงานเศรษฐกิจอุตสาหกรรมกับหน่วยงานต่าง ๆ ให้มีรูปแบบเดียวกัน
- จัดทำคลังข้อมูลสำหรับเก็บข้อมูล โดยการสร้างระบบการรวบรวมข้อมูลจากหน่วยงานต่างๆ เข้ามายังสำนักงานเศรษฐกิจอุตสาหกรรมโดยอัตโนมัติ
- นำเข้าข้อมูลที่รวบรวมมา โดยผ่านกระบวนการลดความซ้ำซ้อนของข้อมูล ก่อนที่จะจัดเก็บลงฐานข้อมูลกลางฐาน
- กำหนดขอบเขตในการให้บริการข้อมูลแก่สถาบันต่างๆ หรือหน่วยงานต่าง ๆ

บทที่ 3

การออกแบบระบบคลังข้อมูลสารสนเทศเศรษฐกิจอุตสาหกรรม

3. การออกแบบระบบคลังข้อมูลสารสนเทศเศรษฐกิจอุตสาหกรรม

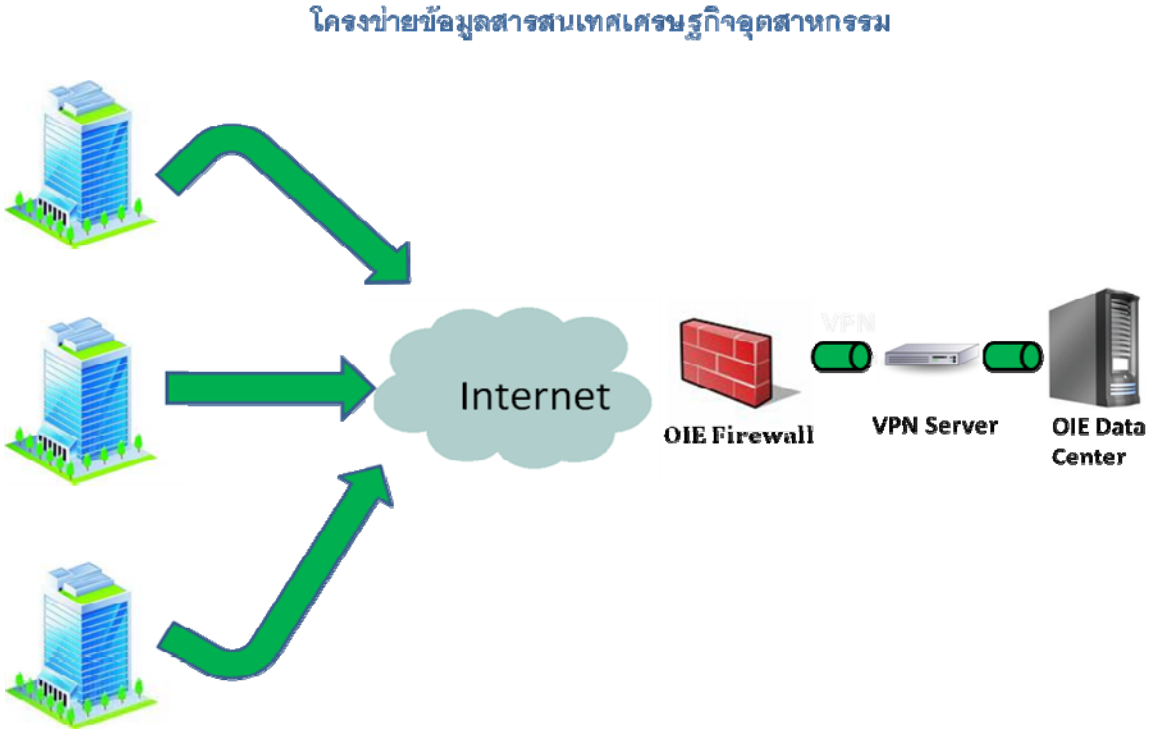
3.1 การออกโครงสร้างฐานข้อมูลกลาง

สถาปัตยกรรมโครงข่ายการเชื่อมโยงข้อมูล

โครงข่ายเชื่อมโยงข้อมูล เป็นโครงสร้างเครือข่ายที่ทำการเชื่อมโยงระหว่างคลังข้อมูลเศรษฐกิจอุตสาหกรรม กับฐานข้อมูลจากหน่วยงานต่าง ๆ เพื่อทำการรวบรวมข้อมูลที่จำเป็นมาเก็บไว้ที่คลังข้อมูล โดยโครงข่ายเชื่อมโยงข้อมูลประกอบด้วย 2 ส่วนหลัก ๆ คือ

- โครงข่าย คือ network ที่ทำการเชื่อมโยงระหว่างฐานข้อมูลกลางกับหน่วยงานต่าง ๆ โดยใช้เครือข่าย Internet เพราะในปัจจุบันเครือข่าย Internet มีการใช้งานอย่างแพร่หลาย ทุกหน่วยงานมีการใช้งาน Internet อยู่แล้วไม่จำเป็นต้องลงทุนสร้าง network ที่เป็น Intranet หรือสายเช่าสัญญาณเฉพาะโครงข่ายที่ค่าใช้จ่ายสูงกว่า
- ระบบรักษาความปลอดภัยโครงข่าย คือ การรักษาความปลอดภัยของข้อมูลในโครงข่าย ไม่ให้บุคคลภายนอกที่ไม่ได้รับอนุญาตทำการเข้าถึงข้อมูลที่มีการส่งในโครงข่าย เพราะเครือข่าย Internet เป็นเครือข่ายสาธารณะการเข้าถึงข้อมูลสามารถทำได้โดยงาน ดังนั้นจึงต้องมีการรักษาความปลอดภัยในโครงข่ายโดยการใช้เทคโนโลยีที่เรียกว่า VPN (Virtual Private Network) หรือเรียกว่าเครือข่ายส่วนตัวเสมือน ซึ่ง VPN จะทำให้การเชื่อมโยงสื่อสารในโครงข่าย Internet มีความปลอดภัยเสมือนมีการใช้โครงข่ายที่เป็น Intranet หรือสายเช่าสัญญาณเฉพาะโครงข่าย เพราะมีการเข้ารหัสข้อมูลที่มีการส่งจากต้นทางไปยังปลายทาง โดยเส้นทางจะถูกสร้างในลักษณะคล้ายอุโมงค์จากต้นทางไปถึงปลายทาง ทำให้ผู้ไม่มีสิทธิไม่สามารถเข้าถึงข้อมูลได้

3.2 การออกแบบโครงข่ายเชื่อมโยงข้อมูล



อุปกรณ์ Hardware ที่ใช้

1. เครื่องคอมพิวเตอร์แม่ข่าย HP รุ่น DL380G6 ทำหน้าที่เป็น Database server รวบรวมข้อมูลจากหน่วยงานต่าง ๆ มาเก็บไว้ในฐานข้อมูล
2. อุปกรณ์ตรวจสอบและป้องกันการบุกรุกของระบบเครือข่าย CISCO รุ่น ASA5510 ทำหน้าที่เป็นอุปกรณ์แม่ข่ายของเครือข่ายส่วนตัวเสมือน (VPN Server)

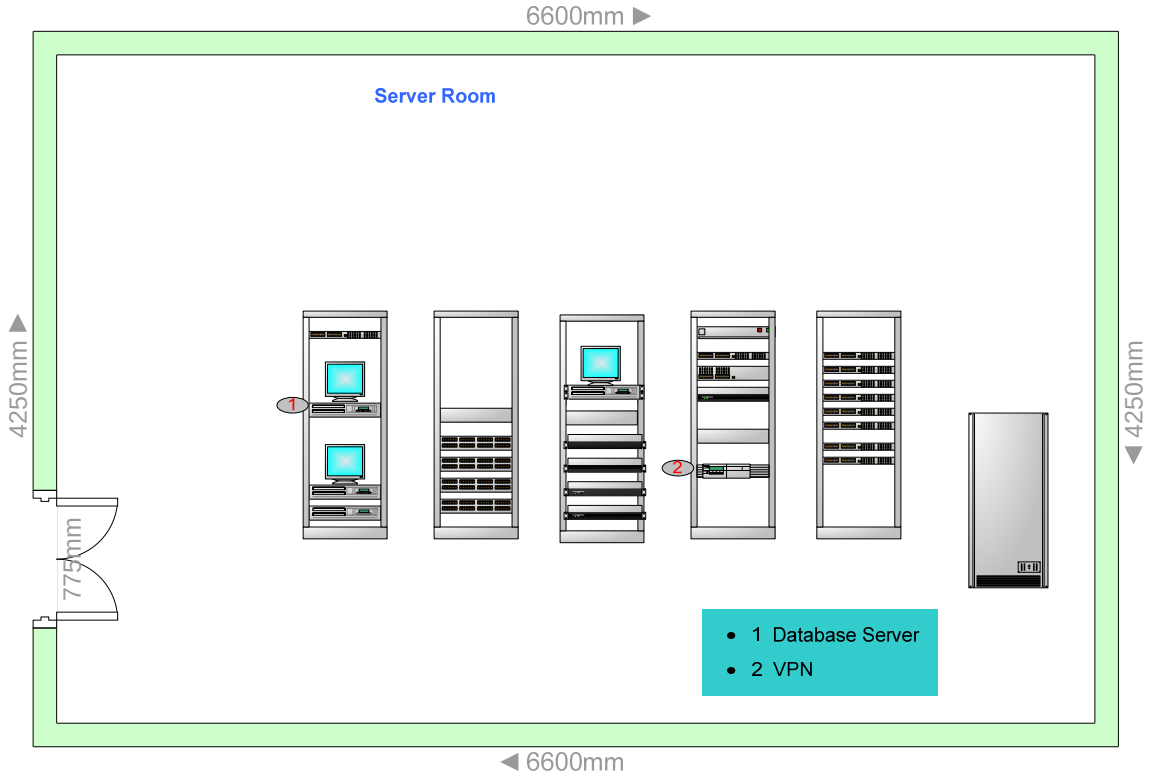
บทที่ 4

การพัฒนาระบบคลังข้อมูลสารสนเทศเศรษฐกิจอุตสาหกรรม

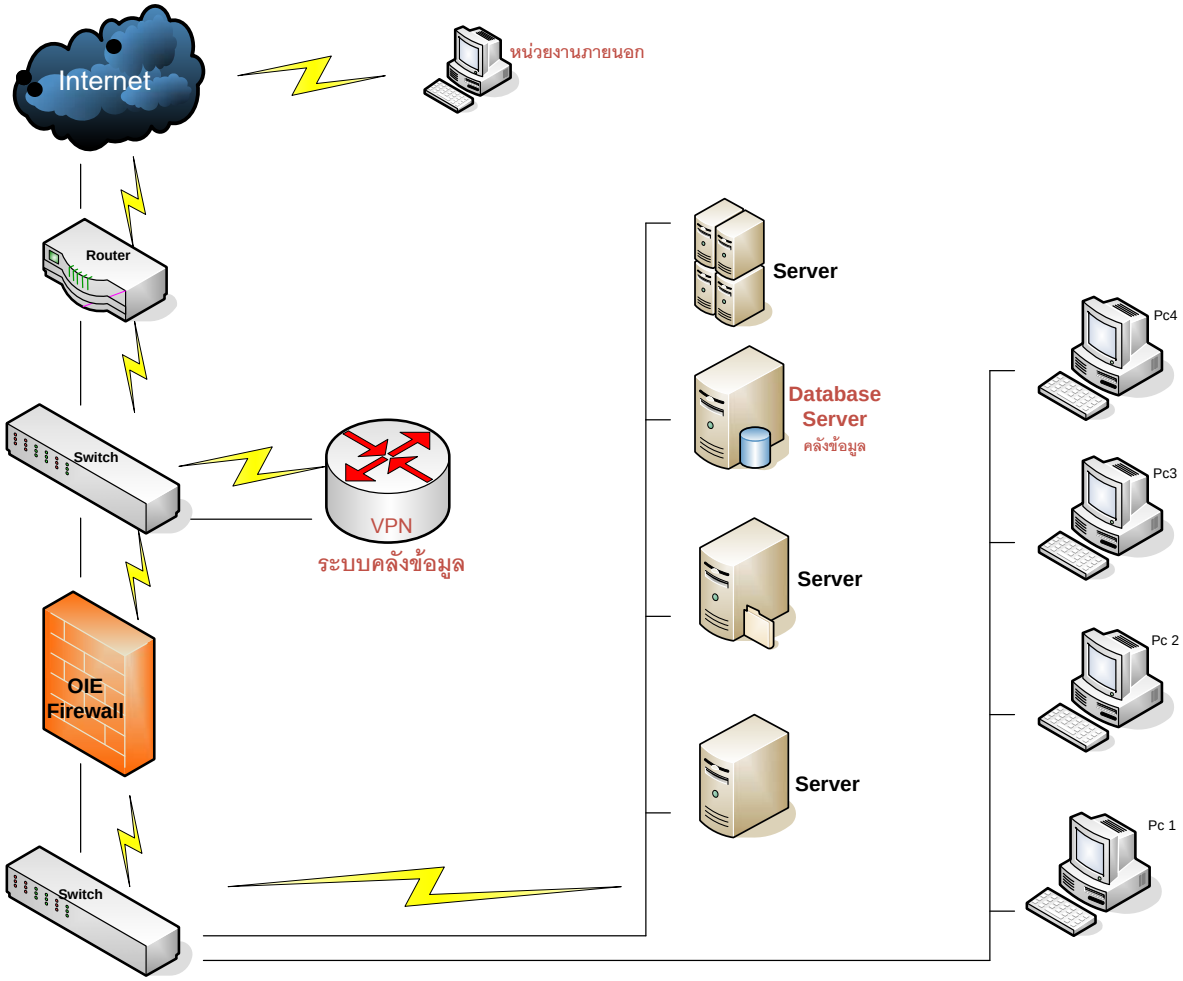
4.1 การพัฒนาระบบรวบรวมข้อมูลและการติดตั้งระบบคลังข้อมูลสารสนเทศเศรษฐกิจอุตสาหกรรม

การติดตั้งอุปกรณ์ Hardware

มีดำเนินการสำรวจจุดติดตั้งอุปกรณ์ Hardware ที่ศูนย์สารสนเทศเศรษฐกิจอุตสาหกรรม ชั้น 4 อาคารสำนักงานเศรษฐกิจอุตสาหกรรม โดยมีจุดติดตั้งตามแผนภาพที่แสดงดังนี้



รูปแบบการติดตั้ง



ขั้นตอนการติดตั้งโครงข่ายคลังข้อมูล

การติดตั้งโครงข่ายคลังข้อมูลที่มีการเชื่อมโยงกันระหว่างสำนักงานเศรษฐกิจอุตสาหกรรม กับหน่วยงานต่าง ๆ สามารถแบ่งการติดตั้งได้เป็น 3 ส่วนใหญ่ ๆ คือ

1. การติดตั้งส่วนเครือข่ายส่วนตัวเสมือน (VPN) เป็นการติดตั้งอุปกรณ์แม่ข่ายของเครือข่ายส่วนตัวเสมือนที่เครือข่ายภายในของสำนักงานเศรษฐกิจอุตสาหกรรม โดยมีขั้นตอนการติดตั้งดังนี้

1.1 ติดตั้งอุปกรณ์แม่ข่ายของเครือข่ายส่วนตัวเสมือนที่ห้อง Server ศูนย์สารสนเทศเศรษฐกิจอุตสาหกรรม

1.2 Setup IP Address ให้กับ VPN Server เพื่อให้เครือข่ายภายในของสำนักงานเศรษฐกิจอุตสาหกรรมสามารถมองเห็น VPN Server ได้

1.3 Setup อุปกรณ์ Router ของสำนักงานเศรษฐกิจอุตสาหกรรมให้ทำการ Forward Port มาที่ VPN Server เมื่อมีการติดต่อมาจากเครื่องภายนอกจาก Port ที่กำหนด

1.4 Setup ให้ VPN Server ทำการส่ง Syslog ไปที่ Server ที่ทำการเก็บ Log files

2. การติดตั้งส่วนเครื่องคอมพิวเตอร์แม่ข่าย เป็นการติดตั้งอุปกรณ์คอมพิวเตอร์ที่ทำหน้าที่เป็น Database Server โดยมีระบบรวบรวมข้อมูล และ Database อยู่บนเครื่องเดียวกัน ซึ่งมีขั้นตอนการติดตั้งดังนี้

2.1 ติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายที่ห้อง Server ศูนย์สารสนเทศเศรษฐกิจอุตสาหกรรม พร้อมทั้ง Set IP Address เพื่อให้เครือข่ายภายในของสำนักงานเศรษฐกิจอุตสาหกรรมสามารถมองเห็นเครื่องคอมพิวเตอร์แม่ข่ายได้

2.2 ติดตั้งระบบปฏิบัติการ Windows Server 2008 R2 พร้อมทั้ง SQL Server 2008 R2 บนเครื่องคอมพิวเตอร์แม่ข่าย

2.3 ติดตั้งระบบรวบรวมข้อมูลบนเครื่องคอมพิวเตอร์แม่ข่าย

2.4 Setup การเชื่อมต่อ VPN โดยการติดต่อไปที่ VPN Server เพื่อติดตั้งโมดูลสำหรับเชื่อมต่อเครือข่ายส่วนตัวเสมือน

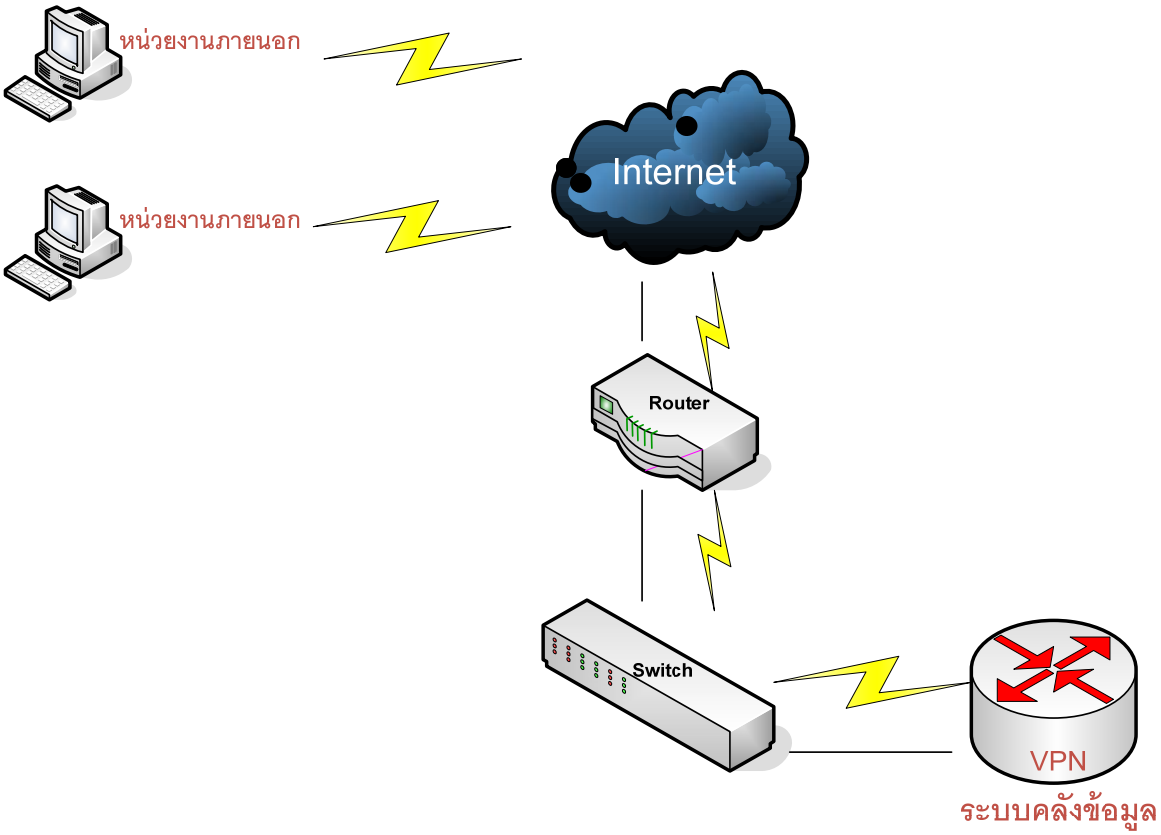
3. การติดตั้งส่วนเครื่องคอมพิวเตอร์ลูกข่าย เป็นการติดตั้งคอมพิวเตอร์ที่อยู่ตามหน่วยงานต่าง ๆ ให้ทำการส่งข้อมูลกลับมาที่สำนักงานเศรษฐกิจอุตสาหกรรม

3.1 ติดตั้งระบบส่งข้อมูลเพื่อทำการดึงข้อมูลจากฐานข้อมูลของหน่วยงานแปลงเป็น Format XML ในรูปแบบมาตรฐานเพื่อส่งข้อมูลให้กับระบบรวบรวมข้อมูลบนเครื่องคอมพิวเตอร์แม่ข่าย

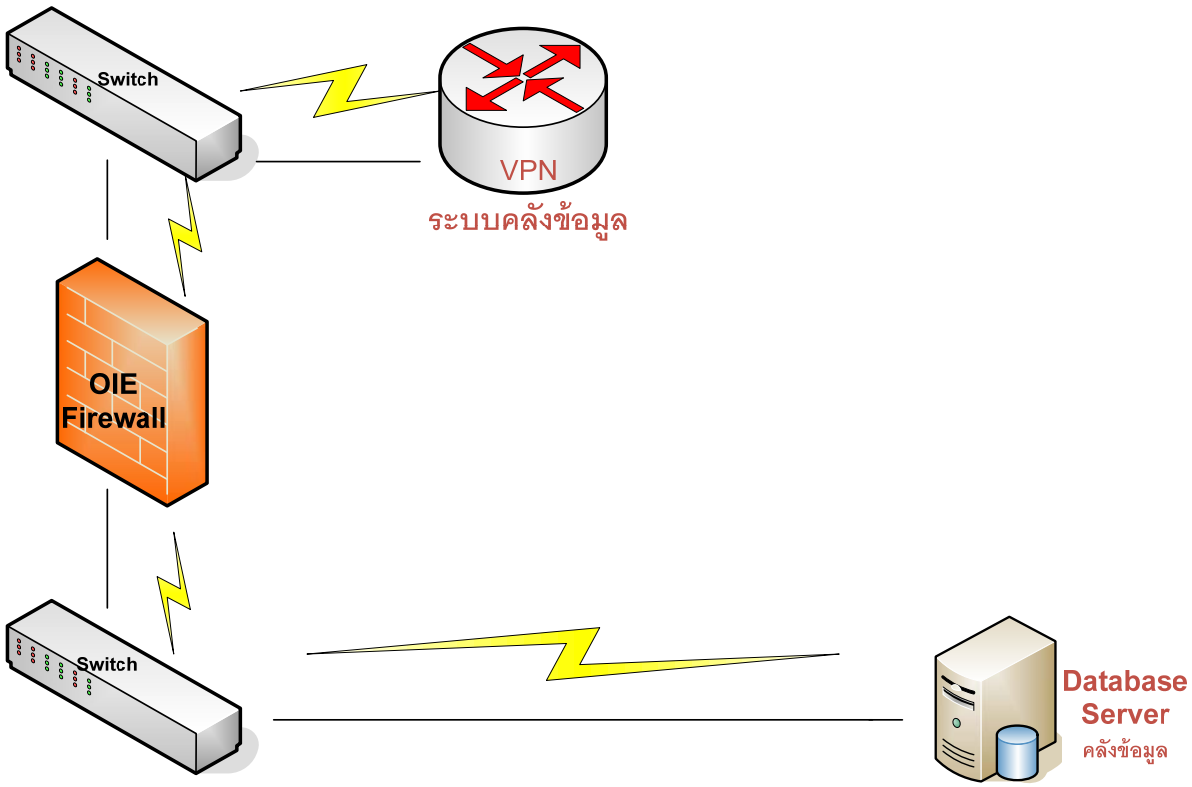
3.2 4 Setup การเชื่อมต่อ VPN โดยการติดต่อไปที่ VPN Server เพื่อติดตั้งโมดูลสำหรับเชื่อมต่อเครือข่ายส่วนตัวเสมือน

ขั้นตอนการทำงานของโครงข่าย

1. หน่วยงานภายนอกสามารถติดต่อเข้าสู่ VPN ที่เป็นโครงข่ายของระบบคลังข้อมูลเศรษฐกิจอุตสาหกรรมผ่านทางเครือข่าย Internet ของหน่วยงานเอง



2. เครื่อง Database Server ของระบบคลังข้อมูลเศรษฐกิจอุตสาหกรรมทำการติดต่อเข้าสู่ระบบ VPN โดยผ่านเครือข่าย Lan ภายในของสำนักงานเศรษฐกิจอุตสาหกรรม โดยเครื่อง Database Server นี้ไม่จำเป็นที่ต้องออก Internet ได้



3. เมื่อหน่วยงานภายนอก และ Database Server ทำการติดต่อเข้าสู่ระบบ VPN ของระบบคลังข้อมูลเศรษฐกิจอุตสาหกรรมเรียบร้อยแล้วการเชื่อมต่อของโครงข่ายระบบจึงจะเสร็จสมบูรณ์ เสมือนมีการเชื่อมต่ออยู่ในวง Network ภายใน

นอกจากนี้ อุปกรณ์ตรวจสอบและป้องกันการบุกรุกของระบบเครือข่าย ยี่ห้อ CISCO รุ่น ASA5510 ที่ทำหน้าที่เป็น VPN Server ยังมีระบบจัดเก็บ Log Files ภายในอุปกรณ์เองและยังสามารถส่ง Logs ต่อไปให้ยัง Server ที่เก็บ Logs ในรูปแบบของ Syslog ที่เป็นมาตรฐานทั่วไปได้อีกด้วย

ภาคผนวก ก

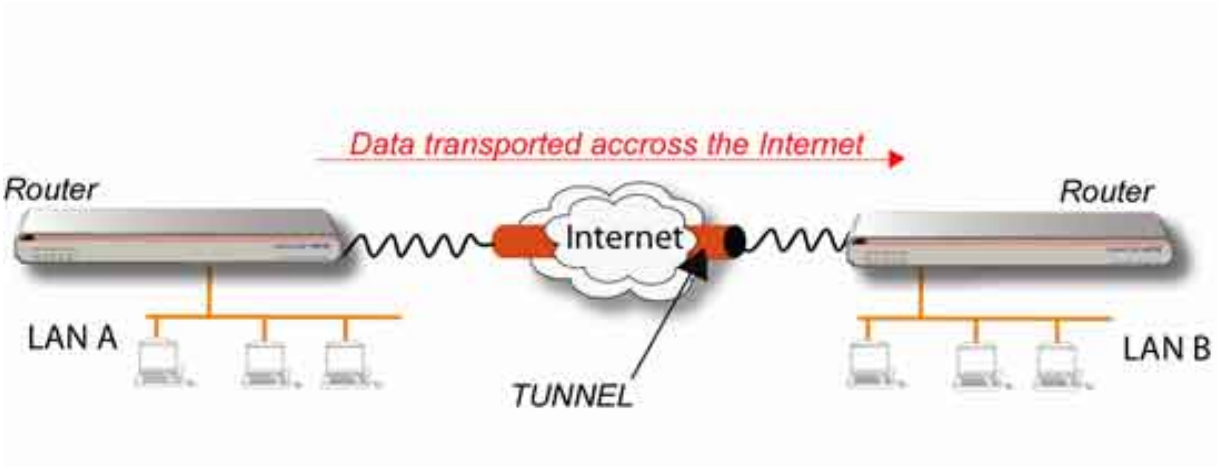
เทคโนโลยี VPN คืออะไร

VPN ย่อมาจาก Virtual Private Network เป็นเทคโนโลยีการเชื่อมต่อเครือข่ายนอกอาคาร (WAN - Wide Area Network) เป็นระบบเครือข่ายภายในองค์กร ซึ่งเชื่อมเครือข่ายในแต่ละสาขาเข้าด้วยกัน โดยอาศัย Internet เป็นตัวกลาง มีการทำ Tunneling หรือการสร้างอุโมงค์เสมือนไว้รับส่งข้อมูล มีระบบเข้ารหัสป้องกันการลักลอบใช้ข้อมูล เหมาะสำหรับองค์กรขนาดใหญ่ซึ่งต้องการความคล่องตัวในการติดต่อรับส่งข้อมูลระหว่างสาขา มีประสิทธิภาพเช่นเดียวกับ Private Network นอกจากนี้ยังสามารถกำหนดหมายเลข IP เป็นเครือข่ายเดียวกัน ทำให้สามารถ login เข้ามาใช้เครือข่ายภายในองค์กรได้ทุกสถานที่ ไม่จำเป็นต้องอยู่ในที่ทำงาน

PN : Private Network คือเครือข่ายภายในของแต่ละองค์กร, Private Network เกิดจากการที่องค์กรต้องการเชื่อมเครือข่ายของแต่ละสาขาเข้าด้วยกัน (กรณีพวกที่เชื่อมต่อด้วย TCP / IP เลขที่ IP ก็จะกำหนดเป็น 10.xxx.xxx.xxx หรือ 192.168.xxx.xxx หรือ 172.16.xxx.xxx) ในสมัยก่อนจะทำการเชื่อมต่อด้วย leased line หลังจากที่เกิดการเติบโตของการใช้งาน Internet และการพัฒนาเทคโนโลยีที่เกี่ยวข้อง การปรับปรุงในเรื่อง ความเร็วของการเชื่อมต่อ ทำให้เกิดแนวคิดในการแทนที่ leased line หรือ Frame Relay ซึ่งมีราคาแพง ด้วย Internet ที่มีราคาถูกกว่า แล้วตั้งชื่อว่า Virtual Private Network

และจากการที่มีคนได้กำหนดความหมายของ VPN เป็นภาษาอังกฤษไว้ว่า "VPN is Private Communications Network Existing within a Shared or Public network Especially the Internet" จะสามารถสรุปความหมาย ได้ดังนี้

- เทคโนโลยี VPN จะทำการเชื่อมต่อองค์ประกอบข้อมูลและทรัพยากรต่างๆ ของระบบเครือข่ายหนึ่ง ให้เข้ากับระบบเครือข่ายหนึ่ง
- เทคโนโลยี VPN จะทำงานโดยยอมให้ผู้ใช้งานสร้างท่ออุโมงค์ เสมือนเพื่อใช้ในการรับส่งข้อมูลผ่านระบบ เครือข่ายอินเตอร์เน็ต
- ส่วนประกอบที่สำคัญหรือหัวใจหลักในการทำ VPN ก็คือการใช้งานอินเตอร์เน็ต



เทคโนโลยี วีพีเอ็นเปรียบเสมือนการสร้างอุโมงค์เพื่อการสื่อสาร

ทำไมถึงต้องใช้ VPN ?

เนื่องจากปัจจุบันการติดต่อสื่อสารถือว่าเป็นสิ่งที่มีความจำเป็นมากขึ้นเรื่อยๆ โดยถ้าเราต้องการการเชื่อมต่อที่มีประสิทธิภาพ มีความปลอดภัยระหว่าง Network บริการที่ดีที่สุดคือ การเช่าสายสัญญาณ (leased line) ซึ่งจะทำการเชื่อมต่อระบบเน็ตเวิร์คของเราด้วยการใช้สายสัญญาณตรงสู่ปลายทาง ทำให้มีความปลอดภัยสูงเพราะไม่ต้องมีการใช้สื่อกลางร่วมกับผู้อื่น และมีความเร็วคงที่ แต่การเช่าสายสัญญาณนั้นข้อเสียคือ ค่าใช้จ่ายในการใช้บริการนั้นสูงมาก เมื่อเทียบกับความเร็วที่ได้รับ ซึ่งองค์กรขนาดเล็กนั้นคงไม่สามารถทำได้

เทคโนโลยี VPN ได้เข้ามาเป็นอีกทางเลือกหนึ่ง เนื่องจากได้ใช้สื่อกลางคือ Internet ที่มีการติดตั้งอยู่อย่างแพร่หลายเข้ามาสร้างระบบเน็ตเวิร์คจำลอง โดยมีการสร้างอุโมงค์ข้อมูล (Tunnel) เชื่อมต่อกันระหว่างต้นทางกับปลายทาง ทำให้เสมือนว่าเป็นระบบเน็ตเวิร์คเดียวกัน สามารถส่งข้อมูลต่างๆที่ระบบเน็ตเวิร์คทำได้ โดยข้อมูลที่ส่งนั้นจะถูกส่งผ่านไปในอุโมงค์ข้อมูล ทำให้มีความปลอดภัยสูง ใกล้เคียงกับ leased line แต่ค่าใช้จ่ายในการทำ VPN นั้นต่ำกว่าการเช่าสายสัญญาณมาก

VPN Architecture

สามารถแบ่งได้ออกเป็น 3 ชนิด คือ Remote access VPN, Intranet VPN และ Extranet VPN

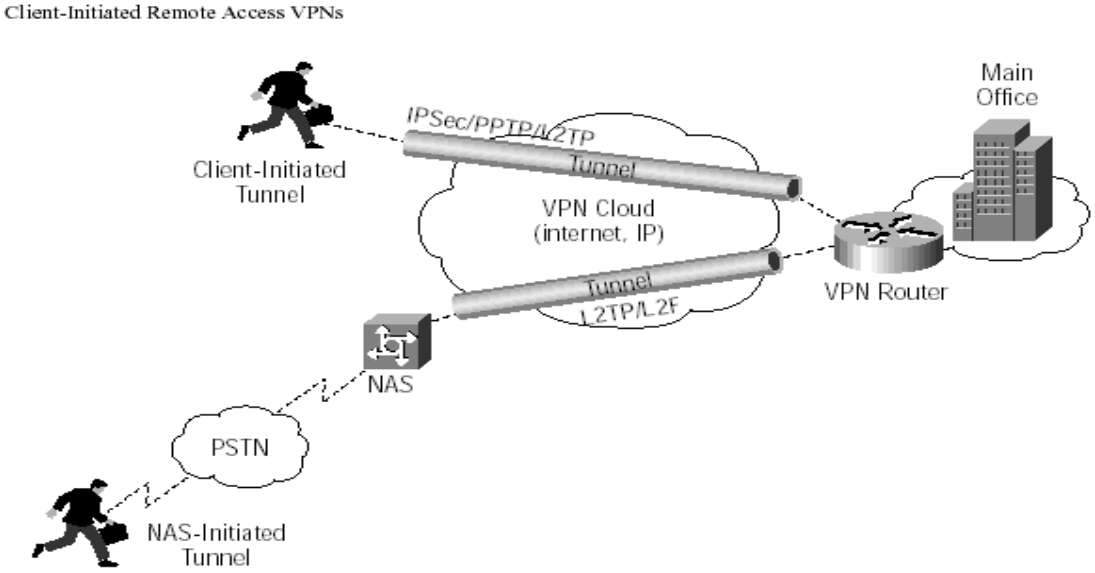
Remote access VPN

สามารถทำการเชื่อมต่อระหว่าง Users ที่ไม่ได้อยู่ที่องค์กร เข้ากับ Server โดยผ่านทาง ISP (Internet Services Provider), Remote access VPN ยังอนุญาตให้ Users สามารถเชื่อมต่อกับตัวองค์กรเมื่อไหร่ก็ได้ตามที่ต้องการ โดยที่ Users จะทำการเชื่อมต่อผ่านทาง ISP ที่รองรับเทคโนโลยี VPN เมื่อ VPN devices ของ ISP ยอมรับการ Login ของ Users แล้ว จะทำการสร้าง Tunnel ไปยัง VPN devices ทางฝั่ง Office ขององค์กร จากนั้นจะทำการส่ง Packets ผ่านทาง Internet

<u>ข้อดีของ Remote access VPN ได้แก่</u>

- ลดต้นทุนจากจัดซื้ออุปกรณ์พวก Modem หรือ อุปกรณ์ Server ปลายทาง
- สามารถเพิ่มจำนวนได้มาก และ เพิ่ม Users ใหม่ ได้ง่าย
- ลดรายจ่ายจากการสื่อสารทางไกล

รูปแสดง Remote Access VPN



Intranet VPN

Intranet VPN จะเป็นการสร้าง Virtual circuit ระหว่าง Office สาขาต่างๆ ขององค์กร เข้ากับ ตัวองค์กร หรือว่า ระหว่างสาขาต่างๆ ของ Office เข้าด้วยกัน จากเดิมที่ทำการเชื่อมต่อโดยใช้ Leased Line หรือ Frame relay จะมีราคาสูง หากใช้ Intranet VPN จะเป็นการประหยัดค่าใช้จ่ายมากกว่า

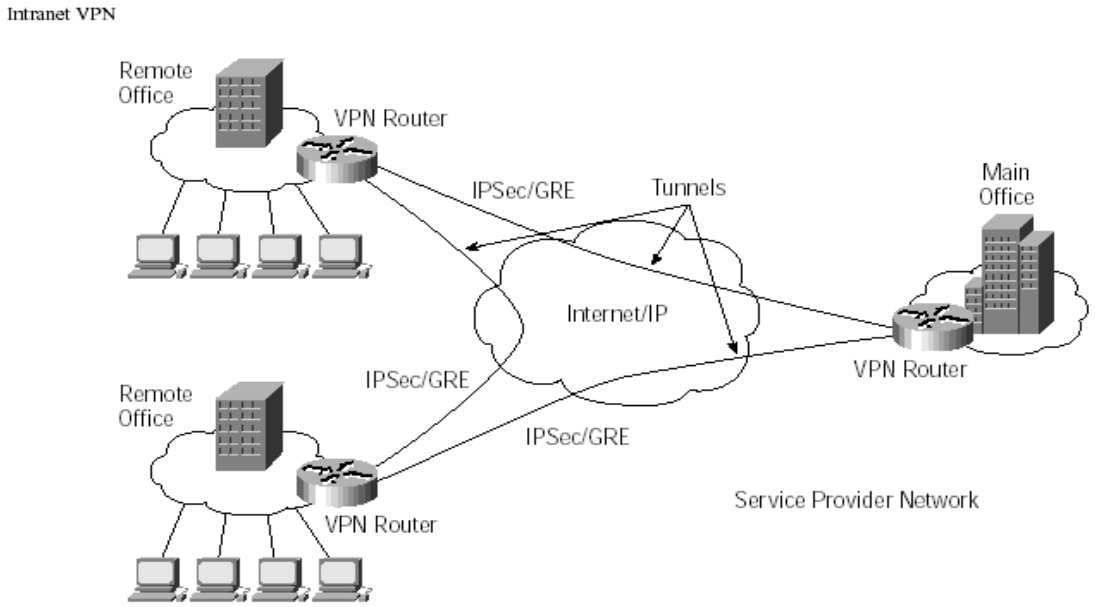
สิ่งสำคัญของ Intranet VPN ก็คือ การ Encryption ข้อมูลที่ต้องมีประสิทธิภาพ เพื่อปกป้องข้อมูลระหว่างที่ส่งผ่านระบบเครือข่าย สิ่งสำคัญอีกอย่างหนึ่งก็คือ ต้องให้ความสำคัญกับ Applications ประเภท Sale และ Customer ,Database Management, Document Exchange, Financial Transactions และ Inventory Database Management

โครงสร้างของ IP WAN ใช้ IPSec หรือ GRE ทำการสร้าง Tunnel ที่มีความปลอดภัย ระหว่างเครือข่าย

<u>ข้อดีของ Intranet VPN ก็คือ</u>

- ลดค่าใช้จ่ายจาก WAN Bandwidth, ใช้ WAN Bandwidth ได้อย่างมีประสิทธิภาพ
- Topologies ที่ยืดหยุ่น
- หลีกเลี่ยงการเกิด Congestion โดยการใช้ Bandwidth management traffic shaping

รูปแสดง Intranet VPN

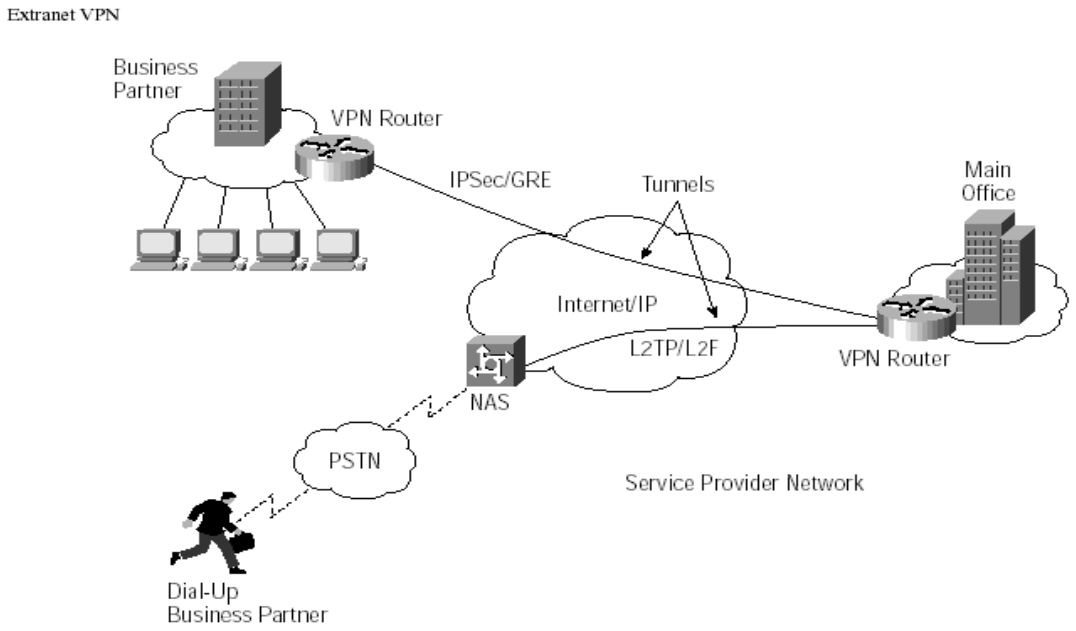


Extranet VPN

Extranet VPN เป็นที่รู้จักกันในชื่อ Internet-based VPN, Concept ของการติดตั้ง Extranet VPN นั้นเหมือนกับ Intranet VPN ส่วนที่ต่างกันก็คือ Users, Extranet VPN จะสร้างไว้เพื่อ Users ประเภทลูกค้า, ผู้ผลิต, องค์กรต่างองค์กรที่ต้องการเชื่อมต่อกัน หรือว่าองค์กรที่มีหลายสาขา

Internet Security Protocol (IPSec) ถูกใช้โดยยอมรับเป็นมาตรฐานของ Extranet VPN

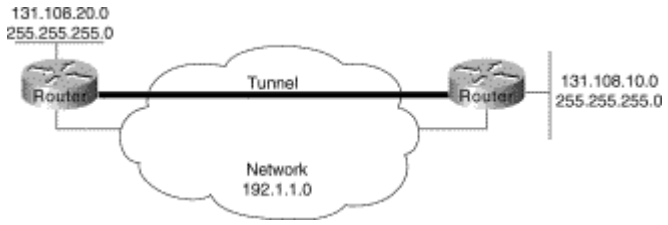
รูปแสดง Extranet VPN



Tunneling

การทำงานหลักๆของ VPN ก็คือการส่งข้อมูลผ่านอุโมงค์ข้อมูล (Tunnel) ไปสู่ระบบเน็ตเวิร์คปลายทาง เนื่องจากอุโมงค์ข้อมูลที่สร้างขึ้นนั้นสร้างผ่านระบบอินเตอร์เน็ต (Internet) และการส่งข้อมูลต้องมีการจัดการ Packet ต่างๆให้ผ่านไปตามอุโมงค์อย่างถูกต้อง การสร้าง Tunnel นั้นประกอบด้วย รูปแบบโปรโตคอล (Protocol) 3 แบบ คือ

- Carrier protocol
- Encapsulating protocol
- Passenger Protocol



Carrier protocol

เป็นโปรโตคอลที่ระบบเน็ตเวิร์ค จะใช้ส่งข้อมูลผ่านอุโมงค์ โดยจะเป็นตัวส่ง Encapsulate โปรโตคอลไปยังปลายทาง

Encapsulating protocol

เป็นโปรโตคอลที่ทำการห่อหุ้มข้อมูลที่จะส่งไว้ ข้อมูลที่ถูกส่งทั้งหมดจะถูกใส่ผ่าน Packet ของโปรโตคอลต่างๆ โปรโตคอลที่มีการใช้งานได้แก่

- **GRE**

GRE ย่อมากจาก Generic routing encapsulation ซึ่งเป็น encapsulating protocol พื้นฐานโดยจะทำหน้าที่ห่อ Packet ของ passenger โปรโตคอลไว้เพื่อที่จะส่งผ่านอุโมงค์ข้อมูล GRE จะเพิ่มข้อมูลในส่วนของชนิดของ Packet ที่ได้ Encapsulate และข้อมูลเกี่ยวกับ Connection ระหว่างทั้งสองระบบด้วย ส่วนใหญ่ GRE นั้นจะใช้ในการใช้งานแบบ VPN ระหว่าง site-to-site

- **PPTP**

PPTP หรือ Point to Point Tunneling Protocols เป็นโปรโตคอลแรกสุดที่ออกมา โดยจะกล่าวถึงมาตรฐานการ Encryption และ Authentication ซึ่งพัฒนาจากบริษัทต่างๆ โดยมี Microsoft และ 3Com ได้ร่วมอยู่ด้วย ดังนั้นจึงเป็นโปรโตคอลที่เป็น Default ของวินโดว์ที่จะใช้งาน VPN ซึ่งโปรโตคอลนี้ มีพื้นฐานอยู่บน PPP ทำให้โปรแกรมที่ใช้โปรโตคอลนี้ เป็นการเชื่อมต่อในลักษณะคอมพิวเตอร์เครื่องเดียวทำการเชื่อมวีพีเอ็นต่อไปยังระบบเน็ตเวิร์กที่รองรับการใช้งาน PPTP นั้นมีข้อดีคือความสะดวกในการนำมาใช้งานที่ไม่ต้องมีการลงทุนทั้งในด้าน software และ hardware มากนัก แต่ในด้านความปลอดภัยนั้น ถือว่ายังด้อยกว่า IPsec ที่ออกมาทีหลังอยู่ โดยมีข้อดีและข้อเสียที่สรุปได้ดังนี้คือ

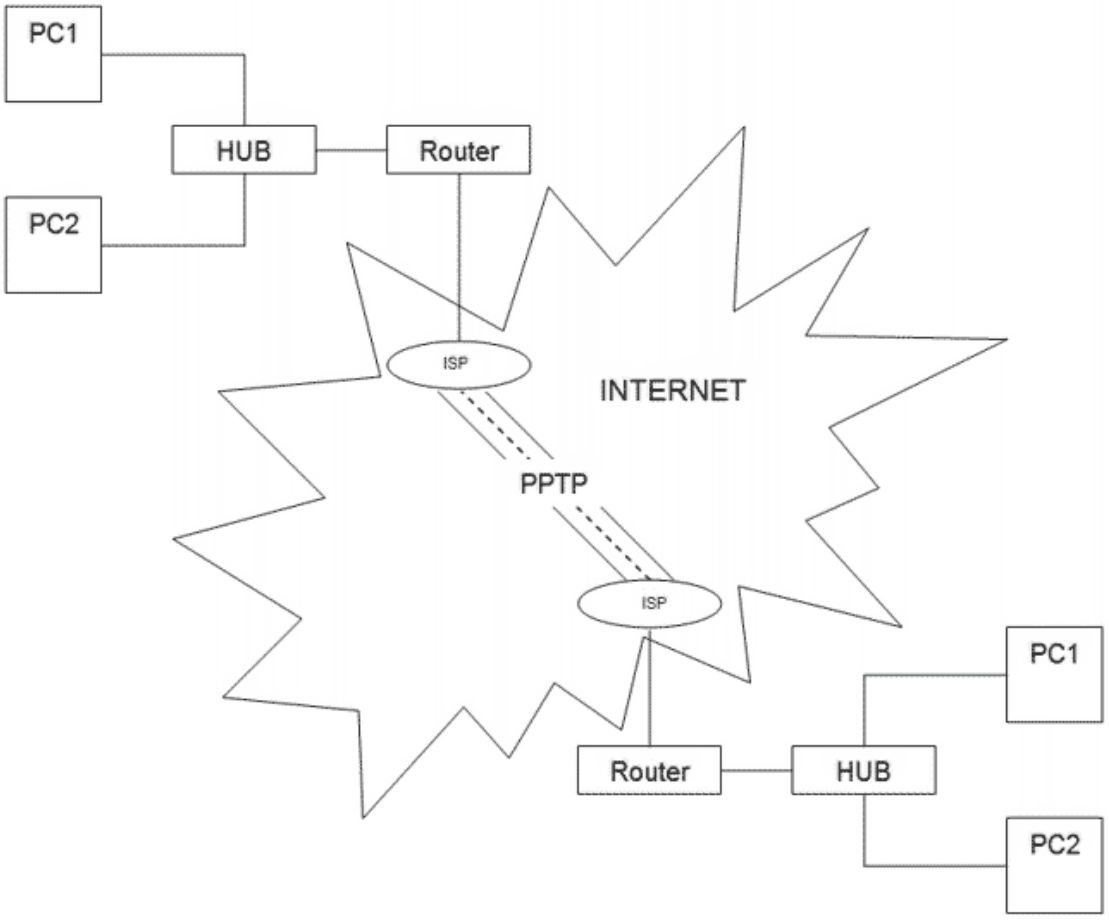
ข้อดีของโปรโตคอล PPTP

- ใช้โอเวอร์เฮดในการทำงานน้อย

- สามารถใช้ได้กับทุกระบบปฏิบัติการ ต้องการเพียงแค่ PPTP Client เท่านั้น
- สามารถใช้งานผ่าน NAT ได้

ข้อเสียของโปรโตคอล PPTP

- การเข้ารหัสของ PPTP จะเริ่มหลังจากการทำ authenticate ดังนั้นในระหว่างนั้นอาจถูกดักอ่านข้อมูลได้
- การ authenticate ของ PPTP จะทำในระดับผู้ใช้เพียงระดับเดียวเท่านั้น อาจทำให้ระดับความปลอดภัยต่ำ



- **L2F**

คือ Layer Two Forwarding ซึ่งมีลักษณะการทำงานที่คล้ายกับ PPTP คือ จะสร้าง Tunnel ห่อหุ้ม PPP ไว้ แต่จะแตกต่างกันตรงที่ PPTP นั้นเป็นการทำงานที่เลเยอร์ที่ 3 ส่วน L2F จะทำงานที่เลเยอร์ที่ 2 แทน โดยใช้พวกเฟรมรีเลย์หรือ ATM ใช้ในการทำ Tunnel

- **L2TP**

L2PT ย่อมาจาก Layer 2 Tunneling Protocol ซึ่งพัฒนามาจากโปรโตคอล PPTP และ L2F โดยสามารถที่จะหุ้ม Protocol อื่นๆนอกจาก TCP/IP เช่น IPX, SNA และ AppleTalk ไว้ในซอง แล้วใช้บริการของ TCP/IP ในการส่งผ่าน Internet อย่างไรก็ตาม L2TP นั้น ไม่มีความสามารถในการเข้ารหัสข้อมูลภายในตัวเอง ทำให้ต้องใช้บริการการเข้ารหัสจาก Protocol ตัวอื่น เช่น L2TP/IPSec Protocol ก็ใช้ L2TP ร่วมกับ IPSec โดยที่ใช้ IPSec ในการเข้ารหัสข้อมูล

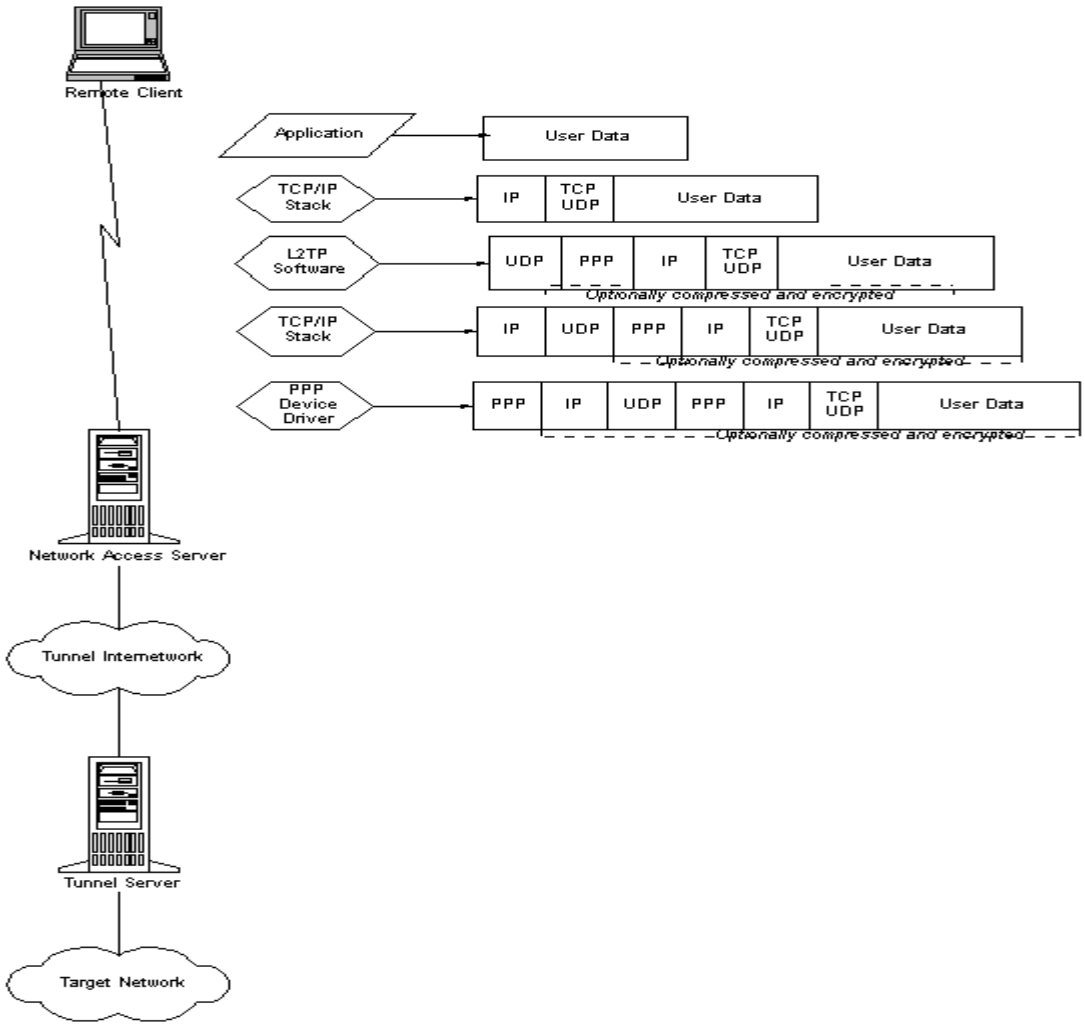
นอกจากนั้น L2TP ยังสนับสนุนการทำ Tunnel หลาย ๆ อันพร้อมกันบนไคลเอ็นต์เพียงตัวเดียว ซึ่งคุณสมบัตินี้ยิ่งทวีความสำคัญมากขึ้นในอนาคต เมื่อทันแนลสามารถสนับสนุนการจองแบนด์วิดธ์และ QoS

ข้อดีของ L2TP with IPSec

- การ authenticate ของ L2TP with IPSec ทำทั้งในระดับผู้ใช้และในระดับโฮสต์โดยการตรวจสอบ Certificate ของโฮสต์
- IPSec ให้ความปลอดภัยในด้านของความถูกต้องและความลับของข้อมูลเป็นอย่างดี

ข้อเสียของ L2TP

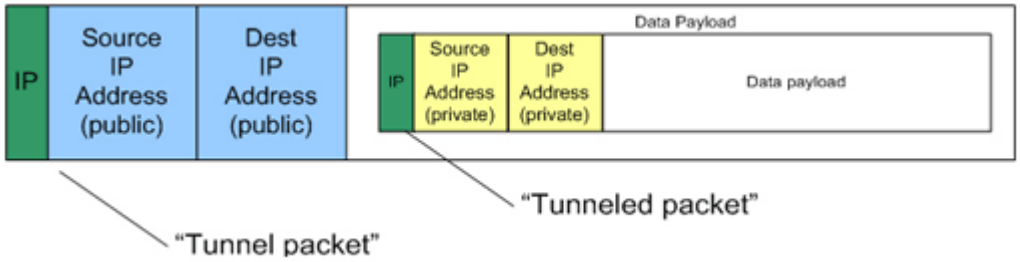
- จำเป็นต้องมี Certificate เพราะ IPSec จะต้องทำการแลกเปลี่ยน Key เพื่อการเข้ารหัสข้อมูล
- ไม่สามารถใช้งานกับระบบปฏิบัติการรุ่นเก่าตั้งแต่ Windows98 ลงไป
- ไม่สามารถใช้งานผ่าน NAT ได้



- **IPSec**

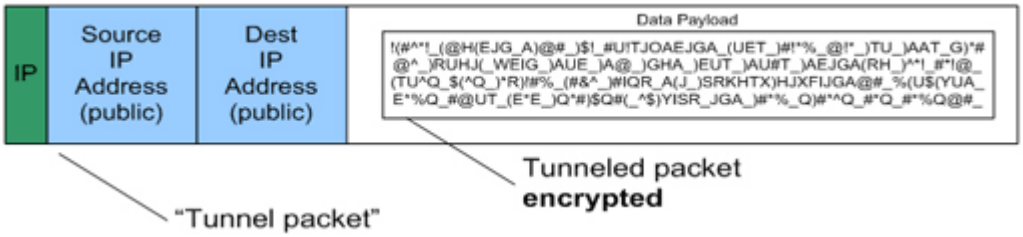
IP Security เป็นการรวม Protocol หลายๆอันมาไว้ด้วยกัน ซึ่งปัจจุบันนั้นมีความนิยมเนื่องจากมีความสามารถทางด้านความปลอดภัยสูง ซึ่งจะทำงานที่ Layer ที่ 3 โดยการทำงานนั้น IPSec จะมีการเข้ารหัส 2 แบบด้วยกันคือ

  - Transport mode คือ จะมีการเข้ารหัสเฉพาะส่วนของข้อมูล แต่ส่วนของ Header จะยังไม่มีการเข้ารหัส ซึ่งใน Mode นี้โดยส่วนมากจะนำไปทำงานร่วมกับโปรโตคอลอื่นๆ เช่น ร่วมกับโปรโตคอล L2TP



Transport Mode

- Tunnel mode จะเป็นการเข้ารหัสทั้งส่วนของข้อมูลและ Header ซึ่งทำให้ข้อมูลมีความปลอดภัยสูงขึ้น



Tunnel Mode

นอกจากนี้แล้ว โปรแกรมประเภท VPN Client บางตัวนั้นได้มีการสร้าง Protocol ของตัวเองขึ้นมาใช้งานด้วย เช่นโปรแกรม CIPE เป็นต้น

- **MPLS**

คือ Multiprotocol Label Switching เป็นเทคโนโลยีที่เพิ่งเกิดขึ้น มีการทำงานในรูปแบบเดียวกันกับข้อมูลต่างๆ ที่มีการส่งผ่านไปมาในระบบเครือข่าย โดยจะมีการติดเครื่องหมาย (Label) ให้กับแต่ละหน่วยของแพ็คเก็ท (Packet) เพื่อที่จะบอกอุปกรณ์เครือข่าย อย่างเช่นเราเตอร์และสวิสท์ ให้ทำการส่งข้อมูลไปในทิศทาง และรูปแบบที่กำหนดไว้ และสำหรับข้อมูลที่มีความสำคัญมาก ก็จะได้รับการส่งแบบพิเศษกว่าข้อมูลอื่นๆ

ปัจจุบันโปรโตคอล MPLS กำลังได้รับ ความนิยมเป็นอย่างมาก เนื่องจากลงทุนน้อยกว่า VPN แบบเดิมที่ต้องติดตั้งจุดต่อจุด ทำให้ผู้ใช้สามารถเชื่อมต่อข้อมูลได้หลายจุดโดยไม่ต้องติดตั้งอุปกรณ์เป็น จำนวนมาก โดยปัจจุบันผู้ให้บริการรายใหญ่มักเลือกใช้โปรโตคอล MPLS เนื่องจากสามารถรองรับการเพิ่มขยายจำนวนผู้ใช้ และบริการเสริมใหม่ๆ ในอนาคต

Passenger Protocol

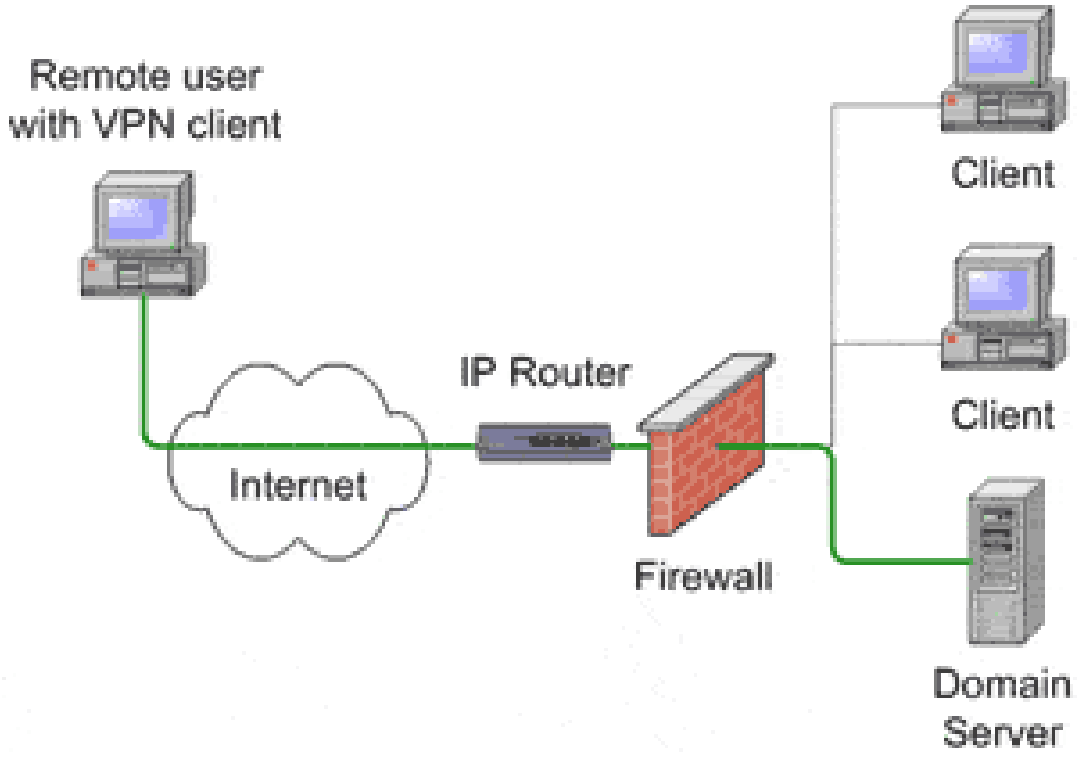
เป็นข้อมูลที่ถูกส่งออกไป หรือ ข้อมูลต้นฉบับนั่นเอง โปรโตคอลเหล่านี้ เช่น IPX, NetBeui, IP ซึ่งบางอันนั้นไม่สามารถส่งไปบนอินเตอร์เน็ตได้ แต่เนื่องจากเราเป็นการสร้างระบบ virtual network ทำให้ปลายทางเสมือนเป็นเน็ตเวิร์คเดียวกัน ทำให้สามารถทำสิ่งต่างๆที่ระบบเน็ตเวิร์คทำได้

ความปลอดภัยในระบบ VPN

การจะทำให้ระบบ VPN ปลอดภัยนั้น ประกอบไปด้วยหลายๆวิธีที่สามารถทำได้ โดยในที่นี้จะกล่าวถึงวิธีดังต่อไปนี้

- **Firewalls**

เป็นการสร้างความปลอดภัยระว่างระบบเน็ตเวิร์คกับอินเตอร์เน็ต โดย Firewalls จะเป็นตัวควบคุมการเปิด-ปิด Portsต่างๆ ซึ่งสามารถทำให้เราควบคุมได้ว่าต้องการให้ Protocols ไหนสามารถใช้งานได้บ้าง Packet ที่เข้ามานั้นจะอนุญาตให้ผ่านหรือไม่ และจะปิด port ที่ไม่ได้ใช้งานไว้ สามารถป้องกันการบุกรุกจากพอร์ทที่ไม่ได้ใช้งานได้



- **Encryption**

Encryption คือ การเข้ารหัสของข้อมูลที่จะทำการส่งไปยังคอมพิวเตอร์เครื่องอื่น ซึ่งเมื่อข้อมูลที่ผ่านการ Encrypt ถูกส่งไปถึงผู้รับ ผู้รับจะต้องทำการ Decode เพื่อให้ได้ข้อมูลที่ผู้ส่งต้องการส่งคืนมา จะทำให้ข้อมูลมีความปลอดภัยเพราะระหว่างทางนั้นถ้าผู้อื่นได้รับข้อมูลไปก็ไม่สามารถรู้ได้ว่าข้อมูลนั้นเป็นอะไร การ Encrypt นั้นสามารถแบ่งออกได้เป็น 2 ลักษณะ คือ

- Symmetric-key encryption

ในแต่ละเครื่องจะมี Code เฉพาะในการใช้เข้ารหัสข้อมูลก่อนที่จะส่งไปให้อีกเครื่องหนึ่ง การใช้ Symmetric-key เราต้องรู้ว่าเราจะส่งข้อมูลไปที่เครื่องไหนและเราต้องทำการลง key เดียวกันไว้ในเครื่องที่เราต้องการส่งไปด้วย ทำให้ key นี้จะรู้กันแค่ผู้ส่งและผู้รับเท่านั้น เพื่อที่จะทำการ Encrypt และ Decode ได้ถูกต้อง และผู้อื่นก็จะถอดรหัสข้อมูลได้

- Public-key encryption

การใช้งานจะเป็นการทำงานร่วมกันระหว่าง Public key และ Private key โดย Public key นั้นจะถูกให้ไปในคอมพิวเตอร์ที่ต้องการจะติดต่อกับเครื่องเรา ซึ่งผู้ที่รู้ key เป็นกลุ่มของคอมพิวเตอร์ต่างกับ Symmetric ที่เป็น key สำหรับ 2 เครื่อง สำหรับการ Decode นั้น จะใช้ Public key ร่วมกับ Private key ที่ต่างกันในแต่ละเครื่อง โดย Public key ที่เป็นที่นิยมใช้งานคือ Pretty Good Privacy (PGP) ซึ่งสามารถจะ Encrypt ข้อมูลได้ทุกชนิดที่ต้องการส่ง

- **IPSec**

เป็น โปรโตคอลที่มีความปลอดภัยเมื่อนำมาใช้งานในการส่งข้อมูลผ่าน VPN ซึ่งลักษณะของโปรโตคอล IPSec นี้ได้อธิบายไว้แล้วในหัวข้อ Encapsulation protocol ในเรื่องของ Tunnel ที่ผ่านมา

- **AAA Server**

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

- คุณเป็นใคร Who you are (authentication)
- คุณได้รับอนุญาตให้ทำอะไรบ้าง What you are allowed to do (authorization)
- คุณทำอะไรไปบ้าง What you actually do (accounting)

ส่วนประกอบที่ใช้ในการสถาปัตยกรรมแบบ VPN

ส่วนประกอบที่ใช้นั้นแบ่งออกเป็น 2 ประเภท คือ Hardware และ Software

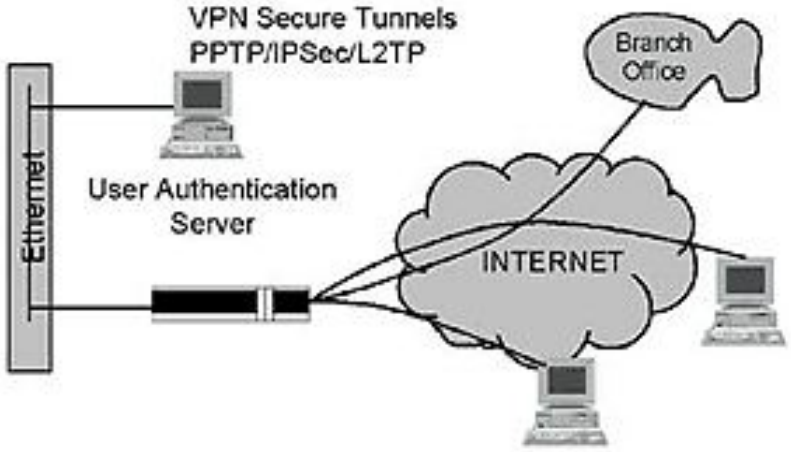
รูปแบบ Hardware-Based VPN

1. Router สามารถแบ่งออกเป็น 2 แบบ ได้แก่

1.1) เพิ่มซอฟต์แวร์เข้าไปที่ตัว Router เพื่อเพิ่มกระบวนการ เข้ารหัส/ถอดรหัส ข้อมูลที่จะวิ่งผ่าน Router ลักษณะนี้เป็นการติดตั้งซอฟต์แวร์เข้าไปที่ชิป ซึ่งอาจเป็นไปในรูปแบบของ NVRAM (Non-Volatile RAM) หรืออาจเป็นชุดของ Flash Memory ก็เป็นได้ ระบบนี้มีข้อดีตรงที่สามารถอัพเกรดการทำงานของซอฟต์แวร์ได้

1.2) เพิ่มการ์ดเข้าไปที่ตัวแท่นเครื่องของ Router ซึ่งอาจเป็นไปในรูปแบบของโมดูลเล็ก ๆ ภายในตัว Router หรือไม่ก็เป็นแบบโมดูลที่ติดตั้งบน Router แบบ Chassis (Router ที่สามารถถอดหรือใส่แผงวงจรได้โดยตรง) รูปแบบนี้เป็นการใช้โมดูลที่เสริมเข้ามาเพื่อทำงานร่วมกับซีพียูบน Router โดยตรง

ผู้ผลิตบางรายได้ผลิต Router ที่เป็นแบบโมดูลให้สามารถถอดเปลี่ยนแผงวงจรได้โดยไม่ต้องปิดเครื่อง อีกทั้งมีระบบที่เรียกว่า Redundancy กล่าวคือ หากพบว่ามีปัญหาที่แผงวงจรใดก็จะมีแผงวงจรอีกแผงหนึ่งที่ติดตั้งประกบคู่อยู่แล้วทำงานแทนได้ทันที ดังนั้นการเพิ่มเติมโมดูล VPN เข้าไปที่ Router สามารถทำได้โดยไม่ต้องปิดเครื่อง ทำให้งานขององค์กรไม่สะดุด

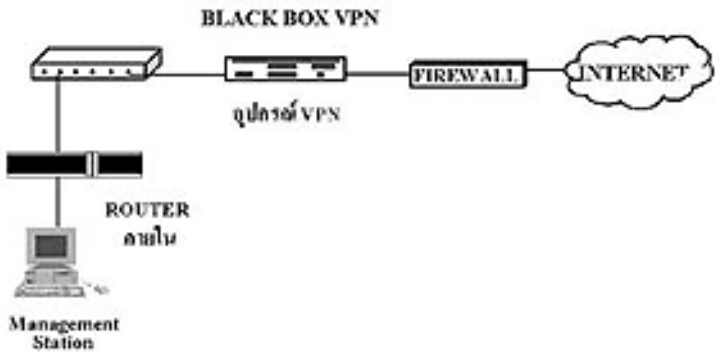


2. Black Box

ส่วนใหญ่จะมีรูปร่างคล้ายกับคอมพิวเตอร์เครื่องหนึ่ง หรือไม่ก็เป็นลักษณะคล้ายกับอุปกรณ์ Switching Hub หรือ Router อย่างใดอย่างหนึ่ง ซึ่งอุปกรณ์นี้จะมีการติดตั้งซอฟต์แวร์ที่ใช้สร้างอุโมงค์เชื่อมต่อและเข้ารหัสข้อมูลข่าวสารในอุโมงค์ ขณะที่ยังมีบางผลิตภัณฑ์มาพร้อมกับซอฟต์แวร์ที่ทำงานบน Desktop PC ของ Client เพื่อใช้บริหารจัดการกับอุปกรณ์ Black Box นี้ ทำให้ท่านสามารถจัดตั้ง Configuration ผ่านทาง Web Browser ได้อีกด้วย

Black Box VPN เป็นอุปกรณ์แยกต่างหากที่สนับสนุนการเข้ารหัสในหลายรูปแบบ เช่น 40 Bit DES (มาตรฐานสำหรับนานาชาติ) และ 3DES สำหรับอเมริกาและแคนาดา เชื่อกันว่าผลิตภัณฑ์ VPN ในรูปแบบ Black Box นี้ทำงานได้เร็วกว่า Software VPN แน่นอน เนื่องจากตัวโปรเซสเซอร์ที่ถูกออกแบบมาทำหน้าที่ดูแลการทำงานของ VPN เป็นการเฉพาะ โดยจะสร้างอุโมงค์ได้หลาย ๆ อุโมงค์ รวมทั้งการเข้ารหัสและการถอดรหัสได้อย่างรวดเร็ว อย่างไรก็ดี จะทำงานโดยอาศัย Black Box เพียงลำพังไม่ได้ เนื่องจากระบบนี้ไม่มีส่วนของการบริหารจัดการโดยตรง อีกทั้งการจัดตั้ง Configuration ต่าง ๆ เช่น การกำหนดกติกาของการพิสูจน์สิทธิ (Authentication) จำเป็นต้องใช้คอมพิวเตอร์อีกตัวหนึ่ง รวมทั้งการอ่านค่าต่าง ๆ ที่มีการบันทึกไว้ก็ต้องอ่านจากคอมพิวเตอร์เช่นกัน

ปกติอุปกรณ์ Black Box VPN จะติดตั้งไว้ด้านหลังของ Firewall เสมอ เนื่องจาก Firewall มีประสิทธิภาพในการป้องกันการก้าวล่วงเข้ามาใช้งานในองค์กรได้ดี แต่ไม่สามารถป้องกันข้อมูลที่วิ่งเข้าวิ่งออกระหว่างองค์กรกับผู้ใช้งาน และในทางกลับกัน VPN ไม่สามารถป้องกันการโจมตีจากผู้หวังดีแต่ประสงค์ร้ายที่อาจสร้างความเสียหายแก่เครือข่ายของท่าน ดังนั้นการจัดตั้งค่าใน Firewall จึงต้องระมัดระวังการทำงานของ VPN ด้วย เนื่องจาก Firewall จะต้องตรวจสอบ Packet ต่าง ๆ ที่วิ่งเข้าวิ่งออก ดังนั้นท่านต้องทำให้มั่นใจว่า Firewall จะยอมให้เฉพาะ Packet ที่ผ่านการเข้ารหัสจาก VPN สามารถผ่านสู่ระบบได้ตามปกติ ดังรูป



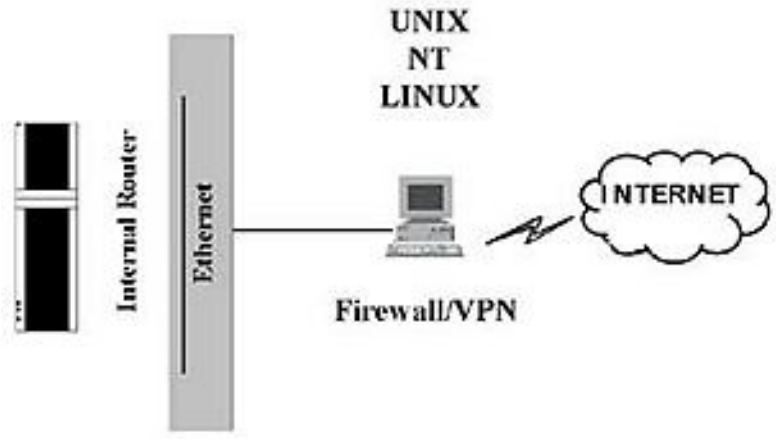
รูปแบบ Firewall-Based VPN

Firewall-Based VPN ดูเหมือนจะเป็นรูปแบบ VPN ที่เป็นปกติธรรมดาและนิยมใช้แพร่หลายมากที่สุด มีผู้ผลิตจำนวนไม่น้อยที่เสนอรูปแบบการเชื่อมต่อแบบนี้ อย่างไรก็ตามมิได้หมายความว่าลักษณะนี้เป็นรูปแบบที่ดีที่สุด เพียงแต่องค์กรส่วนใหญ่ที่เชื่อมต่อกับอินเทอร์เน็ตส่วนใหญ่จะมีไฟร์วอลล์อยู่แล้ว ดังนั้น การเพิ่มซอฟต์แวร์ที่เกี่ยวกับการเข้ารหัสข้อมูล รวมถึงซอฟต์แวร์ที่เกี่ยวข้องเข้าไปยังตัวไฟร์วอลล์ก็สามารถดำเนินงานได้ทันที

Firewall-Based VPN ปกติจะอยู่ในรูปแบบของซอฟต์แวร์ แต่ผู้ผลิตบางรายอาจเพิ่มประสิทธิภาพของ VPN เข้าไปในผลิตภัณฑ์ไฟร์วอลล์ของตน ซึ่งประสิทธิภาพการทำงานย่อมจะด้อยกว่าฮาร์ดแวร์อย่างแน่นอน อย่างไรก็ดีผู้ผลิตซอฟต์แวร์ VPN บางรายได้ผลิตซอฟต์แวร์ที่เป็น VPN แต่สามารถทำงานร่วมกับซอฟต์แวร์ไฟร์วอลล์ได้เป็นอย่างดี ซึ่งซอฟต์แวร์เหล่านี้ทำงานบนระบบปฏิบัติการต่าง ๆ เช่น UNIX, LINUX, Windows NT หรือ Windows 2000 เป็นต้น

รูปด้านล่าง แสดงลักษณะการเชื่อมต่อ VPN แบบที่นิยมใช้กันแพร่หลาย ซึ่งเรียกว่า Firewall-Based VPN รูปแบบนี้เป็นที่นิยมทั่วไปในหมู่องค์กรต่าง ๆ ดังนั้นการเพิ่มเติมซอฟต์แวร์ VPN เข้าไปจึงไม่ใช่เรื่องยาก เพียงแต่ว่าจะต้องเลือกโปรโตคอลที่ต้องการจะใช้ เช่น PPTP, L2TP หรือ IPSec เป็นต้น หากคิดว่า Firewall-Based VPN เป็นรูปแบบที่ต้องการ จะต้องพิจารณาผลิตภัณฑ์ไฟร์วอลล์ที่เหมาะสมและซอฟต์แวร์ VPN ที่นำมาใช้ร่วมกับไฟร์วอลล์นี้จะต้องส่งเสริมการทำงานซึ่งกันและกัน

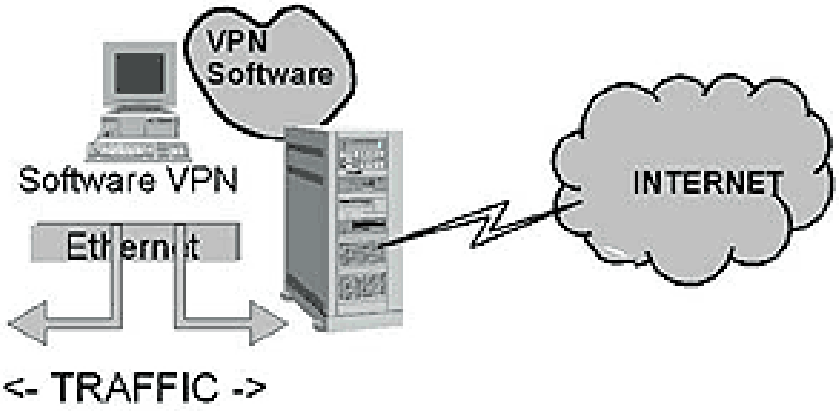
แสดงรูปแบบการเชื่อมต่อแบบ Firewall Based VPN



รูปแบบ Software-Based VPN

Software-Based VPN โดยแท้จริงแล้วเป็นซอฟต์แวร์ซึ่งทำหน้าที่จัดตั้งอุโมงค์การเชื่อมต่อ การเข้ารหัสและการถอดรหัสข้อมูลบนคอมพิวเตอร์ เป็นซอฟต์แวร์ที่ทำงานในลักษณะของไคลเอนต์และเซิร์ฟเวอร์ ตัวอย่างเช่น VPN ที่ใช้โปรโตคอล PPTP จะมีการติดตั้งซอฟต์แวร์เข้าไปที่เครื่องของไคลเอนต์และเชื่อมต่อกับเซิร์ฟเวอร์ที่ติดตั้งซอฟต์แวร์ VPN และจัดตั้งอุโมงค์เชื่อมต่อ VPN ขึ้น เมื่อเลือกใช้ซอฟต์แวร์ VPN จะต้องมีการขบวนการบริหารจัดการกับกุญแจรักษาความปลอดภัยที่ดี และเป็นไปได้ที่จะต้องการระบบการพิสูจน์สิทธิแบบที่เรียกว่า Certificate Authority การใช้ Software-Based VPN อาจต้องพิจารณากุญแจรักษาความปลอดภัยต่าง ๆ เช่น Public และ Private Key ลักษณะนี้คอมพิวเตอร์ทุกเครื่องไม่ว่าจะเป็นภายในหรือภายนอกองค์กรจะได้รับการพิสูจน์สิทธิก่อนจะส่งข้อมูลระหว่างกัน ซึ่งจะเห็นได้ว่าระบบซอฟต์แวร์ VPN นี้มีความยืดหยุ่นพอสมควร ยกตัวอย่างเช่น

รูปแสดงรูปแบบการเชื่อมต่อแบบ Software-Based VPN



ตัวอย่าง Software ที่ใช้ในการทำ VPN

1. Frees/Wan โปรแกรมที่ใช้ได้ในหลายระบบปฏิบัติการ ซึ่งเป็น Free ware ปัจจุบัน (09/48)ได้ออกถึง version 2.06 รายละเอียดเบื้องต้น มีดังนี้

Protocol: IPSEC

ระดับการเข้ารหัสข้อมูล (Encryption): ดีมาก

Authorization: X.509

ข้อดี : มีความน่าเชื่อถือ

ข้อเสีย : ติดตั้งยาก , มี Log file ขนาดใหญ่

2. OpenVPN เป็นโปรแกรม VPN แบบ Opensource ที่มีการใช้งานอย่างแพร่หลาย มีการใช้ SSL เพื่อเพิ่มความปลอดภัย มีการทำงานทั้ง Layer 2 และ 3 มีรายละเอียดดังนี้

Protocol: TLS + โปรโตคอลของโปรแกรม

ระดับการเข้ารหัสข้อมูล (Encryption): ดีมาก

Authorization: X.509

ข้อดี : ติดตั้งง่าย

ข้อเสีย : -

3. PoPToP เป็นโปรโตคอล ที่ใช้งาน tunnel แบบ GRE ที่มีมาให้กับ windows มีรายละเอียดดังนี้

Protocol: PPTP

ระดับการเข้ารหัสข้อมูล (Encryption): ดี แต่การทำ Authentication ไม่ดี

Authorization: X.509

ข้อดี : ใช้ Windows เป็นพื้นฐาน

ข้อเสีย : ใช้ Windows เป็นพื้นฐาน

4. Vtun เป็นโปรแกรมแบบ Opensource เช่นกัน ซึ่งเพิ่งจะพัฒนาขึ้นมาได้ไม่นานมากนัก โดยโปรแกรมนี้จะรองรับเฉพาะ บนระบบปฏิบัติการที่มีพื้นฐานมาจาก Unix มีรายละเอียดดังนี้

Protocol: ใช้โปรโตคอลแบบเฉพาะของโปรแกรม

ระดับการเข้ารหัสข้อมูล (Encryption): ไม่ดี

Authorization: SSH kludge

ข้อดี : น่าเชื่อถือ (สำหรับ 1 user)

ข้อเสีย : ต้องใช้ kludge script

ข้อดีและข้อเสียของ VPN

- **<u>ข้อดี</u>**

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) <u>Firewall</u> จะเป็นการติดตั้งตัวกั้นกลางระหว่าง network ของเรากับ Internet โดยตัว Firewall จะสามารถจำกัดจำนวนของ port รวมทั้งลักษณะของ packet และ protocol ที่จะมาใช้งาน

2..2) <u>Encryption</u> (การเข้ารหัส) เป็นกระบวนการที่นำข้อมูลจากเครื่องคอมพิวเตอร์หนึ่งเครื่องไปทำการเข้ารหัสก่อนที่จะส่งไปยังเครือข่ายคอมพิวเตอร์อื่น

2.3) <u>IPSec</u> 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 ที่ออกไปทำงานนอกสถานที่สามารถเชื่อมต่อเข้าเครือข่ายขององค์กร เพื่อเช็คข่าว อ่านเมล์ หรือใช้งานโปรแกรม เพื่อเรียกดูข้อมูล เป็นต้น การใช้ VPN สามารถ login เข้าสู่ ระบบงานขององค์กร โดยใช้โปรแกรมจำพวก 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

- **<u>ข้อเสีย</u>**

1. เทคโนโลยีที่สับสน

การตัดสินใจว่าจะนำเอาเทคโนโลยี VPN ชนิดใดมาใช้งานอาจเป็นเรื่องที่ค่อนข้างสับสน เนื่องจากการที่มีตัวเลือกมากมาย และการใช้มาตรฐาน VPN ที่แตกต่างกัน รวมทั้งการตีความเพื่อใช้งานที่ต่างกัน และปัญหาความสามารถในการทำงานร่วมกันระหว่างอุปกรณ์ VPN บางชนิดอาจทำให้เครือข่ายมีความซับซ้อนเพิ่มขึ้นได้

2. คุณภาพของการบริการ

VPN ทำงานอยู่บน Internet ซึ่งความเร็ว ,การเข้าถึง และคุณภาพ (Speed and access) เป็นเรื่องเหนือการควบคุมของผู้ดูแลเครือข่าย และเนื่องจากมีสัญญาณอาจเดินทางข้ามเครือข่ายจำนวนมาก ดังนั้นเมื่อมีการทำงานผ่านเครือข่าย IP ของผู้ให้บริการสื่อสารรายใดรายหนึ่ง ผู้ให้บริการรายนี้อาจไม่ทราบว่าสัญญาณเป็นแบบ IP VPN ดังนั้นจึงดำเนินการให้บริการที่คิดว่า "ดีที่สุด" เหมือนกับสัญญาณ IP อื่นๆ แทน

3. Technology ที่ต่างกัน

VPN มี technologies แตกต่างกันตามผู้ขายแต่ละราย โดยยังไม่มีมาตรฐานที่ใช้ร่วมกันอย่างแพร่หลายมากนัก ต้องมีการพัฒนาเพื่อรองรับ Protocol อื่นๆ นอกจาก Protocol ที่อยู่บนพื้นฐานของ IP

สรุป ข้อดี-ข้อเสีย

สถาปัตยกรรม	ข้อดี	ข้อเสีย
Hardware VPN	ประสิทธิภาพดี มีระบบรักษาความปลอดภัยที่ดี มีค่าใช้จ่ายน้อยสำหรับแพ็กเก็ตขนาดใหญ่ที่เข้ารหัสแล้ว บางผลิตภัณฑ์ให้การสนับสนุน Load Balancing	ความยืดหยุ่นจำกัด ราคาสูง ไม่สามารถเชื่อมต่อกับ ATM หรือระบบ FDDI ได้โดยตรง ส่วนใหญ่มีการเชื่อมต่อแบบฮาล์ฟดูเพล็กซ์ ต้องการรีบูตระบบใหม่ภายหลังการจัดตั้งคอนฟิกเสร็จสิ้น บางผลิตภัณฑ์มีปัญหาเกี่ยวกับประสิทธิภาพกับแพ็กเก็ตที่มีขนาดเล็ก (64 ไบต์) มีข้อจำกัดเมื่อทำงานกับ Subnet บางผลิตภัณฑ์ไม่มี NAT
Software VPN	สนับสนุนการทำงานบนหลากหลายระบบปฏิบัติการ ติดตั้งง่าย เหมาะสำหรับองค์กรทั่วไป	บางผลิตภัณฑ์มี NAT ที่ไม่ได้ประสิทธิภาพ บางทีก็ใช้ระบบการเข้ารหัสแบบเก่า ขาดคุณสมบัติในการบริหารจัดการระยะไกล ไม่มีระบบเฝ้าดูและตรวจสอบการทำงาน
Router-Base VPN	ใช้ฮาร์ดแวร์ เช่น Router ที่มีอยู่แล้ว มีระบบรักษาความปลอดภัยที่น่าเชื่อถือ ต้นทุนต่ำ หากใช้ Router ที่มีอยู่แล้ว	บางผลิตภัณฑ์อาจต้องการเพิ่มการ์ดอินเตอร์เฟส เพื่อการเข้ารหัสข้อมูลข่าวสารเพิ่มเติม มีปัญหาเรื่องประสิทธิภาพ ต้องการอัพเกรดเพื่อประสิทธิภาพที่ดีกว่า

สถาปัตยกรรม	ข้อดี	ข้อเสีย
Firewall-Based VPN	สามารถใช้กับหลากหลายระบบปฏิบัติการ รวมทั้งฮาร์ดแวร์หลายแบบ สามารถใช้อุปกรณ์ทางฮาร์ดแวร์ที่มีอยู่แล้ว บางผลิตภัณฑ์สนับสนุน Load Balancing รวมทั้ง IPSec	อาจมีปัญหาเกี่ยวกับระบบรักษาความปลอดภัย เนื่องจากระบบปฏิบัติการเข้ากันไม่ได้เต็มที่กับระบบพิสูจน์สิทธิแบบ RADIUS