การศึกษาความเป็นไปได้ในการนำเครือข่าย VPN มาใช้ในบริษัทและสาขาต่าง ๆ

FEASIBILITY STUDY OF VIRTUAL PRIVATE NETWORK FOR A CORPORATE AND ITS BRANCHES.

โดย

นาย บงการ ช้างเสวก

รหัส 44067627

อาจารย์ที่ปรึกษา

อาจารย์อัครินทร์ คุณกิตติ

รายงานนี้เป็นส่วนหนึ่งของวิชาโครงการศึกษากรณีพิเศษ
หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
ภาคเรียนที่ 1 ปีการศึกษา 2546
คณะเทคโนโลยีสารสนเทศ
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ชื่อหัวข้อ	การศึกษาความเป็นไปได้ในการนำเครือข่าย VPN มาใช้ในบริษัทและสาขาต่าง ๆ
นักศึกษา	นายบงการ ช้างเสวก
อาจารย์ที่ปรึกษา	อ.อัครินทร์ คุณกิตติ
ระดับการศึกษา	วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
แขนงวิชา	การจัดการเทคโนโลยีสารสนเทศ
ปีการศึกษา	2546

บทคัดย่อ

การศึกษาความเป็นไปได้ในการนำเครือข่าย VPN มาใช้ในการติดต่อสื่อสารภายในบริษัทฯเพื่อทำการเชื่อมต่อสำนักงานสาขาให้สามารถใช้งานระบบงานของสำนักงานใหญ่ผ่านเครือข่ายอินเตอร์เน็ต ครอบคลุมไปถึงการให้บริการแก่ผู้บริหารภายในและภายนอก (ผู้บริหารจากบริษัทฯในเครือ ที่มีความจำเป็นต้องเข้ามาสืบค้นข้อมูลภายใน) ที่จำเป็นต้องเดินทางออกไปทำงานนอกบริษัทฯ ให้สามารถเข้ามาตรวจสอบข้อมูลข่าวสารต่าง ๆ ภายในบริษัทฯได้โดยผ่านระบบเครือข่ายอินเตอร์เน็ต โดยได้สรุปแนวทางเลือกออกเป็น 2 แนวทางได้แก่ ทางเลือกที่ 1. การทำอุโมงค์ VPN ด้วยฮาร์ดแวร์ ทางเลือกที่ 2. การทำอุโมงค์ VPN ด้วยซอร์ฟแวร์ โดยการศึกษานี้เป็นการศึกษาความเป็นไปได้ในทางการเงินด้วยปัจจัยสำคัญที่ช่วยในการตัดสินใจเลือกโครงการ ได้แก่ มูลค่าการลงทุนเริ่มต้น ค่าใช้จ่ายโครงการ อัตราผลตอบแทนต่อทรัพย์สิน อัตราผลตอบแทนต่อการลงทุน ระยะเวลาการคุ้มทุน และผลตอบแทนภายใน โดยจากการวิเคราะห์ผลสรุปในทั้งสองแนวทางนั้นมีความแตกต่างกันน้อยมากหรือประมาณ 1-4 % ทำให้การสรุปเลือกแนวทางเลือกที่ 1 การทำอุโมงค์ VPN ด้วยฮาร์ดแวร์เนื่องจากทางเลือกที่ 1 ให้ผลตอบแทนสุทธิสูงกว่าทางเลือกที่ 2 อยู่ 19% และมีค่าใช้จ่ายในการบริหารงานที่ต่ำกว่าในทางเลือกที่ 2

Title	Feasibility Study of Virtual Private Network for a Corporate and its branches.
Student	Mr. Bongkarn Changsewok
Advisor	Mr. Akharin Khunkitti
Level of Study	Master of Science in Information Technology
Major	Information Technology Management
Academic Year	2003

ABSTRACT

Feasibility Study of VPN Implementation in enterprise corporate. VPN implement for connect corporate branches to access main office network thru Internet access with more security to serve corporate's management and employee who need to access corporate's network when they're working out of office. In this case studying include of study the corporate vision and readily, comparison between many types of VPN implementation to match with corporate requirement and recently network with 2 choices between 1. VPN Hardware 2. VPN Software , And study the economics feasibility with the important decision making factor, which are capital expenditure, cost of operation and maintenance, estimate revenue payback period and internal rate return. Finally shall be utilized the result of this feasibility study is analyzed of the VPN type. And after analytical VPN Hardware give the benefit more than VPN Software and less expenses.

กิตติกรรมประกาศ

โครงการศึกษากรณีพิเศษฉบับนี้ สำเร็จลุล่วงไปได้ด้วยการให้คำปรึกษาอย่างดียิ่งของอาจารย์อัครินทร์ คุณกิตติ อาจารย์ที่ปรึกษาโครงการ และอาจารผู้ควบคุมการสอบทุกท่านที่ได้ให้คำปรึกษาและแก้ไขจุดบกพร่องของโครงการจำสำเร็จเป็นรายงานฉบับสมบูรณ์ขึ้นมาได้ ผู้จัดทำขอกราบขอบพระคุณเป็นอย่างสูงมา ณ โอกาสนี้

ขอขอบพระคุณบริษัท อาร์มสตรอง รับเบอร์ แอนด์ เคมิคัลโปรดักส์ จำกัดที่ให้โอกาสผู้จัดทำได้ทำงานในส่วนงานที่มีความสำคัญในการพัฒนาระบบ และเป็นต้นแบบในการศึกษาโครงการศึกษากรณีพิเศษฉบับนี้ รวมถึงผู้ร่วมงานทุกท่านที่ได้ทำงานอย่างเต็มความสามารถเพื่อช่วยแบ่งเบาภาระในงานประจำของผู้จัด

โดยท้ายสุดนี้ผู้จัดทำขอน้อมระลึกถึงพระคุณของบิดามารดาที่ได้ให้การเลียงดูและอบรมอย่างดี ขอระลึกถึงพระคุณของครูอาจารย์ทุกท่านที่ถ่ายถอดความรู้ให้ได้มาใช้ในการศึกษา หากเกิดข้อพกพร่องประการใดในโครงการศึกษาพิเศษนี้ผู้จัดทำขอน้อมรับไว้เป็นบทเรียนแก่ตนเองต่อไป

บงการ ช้างเสวก

สารบัญ

หน้า

สารบัญ (ต่อ)

สารบัญตาราง

หน้า

สารบัญภาพ

หน้า

บทที่ 1
บทนำ

บริษัท อาร์มสตรอง รับเบอร์ แอนด์ เคมิคัล โปรดักส์ จำกัด ก่อตั้งในปี 2537 เป็นบริษัทฯร่วมลงทุนระหว่างประเทศไทย สิงคโปร์ และญี่ปุ่น มีบริษัทฯแม่ ตั้งอยู่ที่ประเทศสิงคโปร์ โดยดำเนินกิจการเกี่ยวกับ การผลิตชิ้นส่วนอิเลคทรอนิกส์ ที่ใช้วัตถุดิบจากยาง ฟองน้ำ และโลหะ โดยมีการขายสินค้าให้ทั้งภายในและภายนอกประเทศ รวมทั้งยังมีการสั่งซื้อวัตถุดิบทั้งภายในและภายนอกประเทศ

ในปัจจุบันบริษัทฯมีสำนักงานอยู่ใน 3 จังหวัด คือ จังหวัดสมุทรปราการ จังหวัดปราจีนบุรี และจังหวัดอยุธยา โดยในปัจจุบันได้มีการเชื่อมต่อระบบเครือข่ายระหว่างสำนักงานสมุทรปราการ ปราจีนบุรี และจังหวัดอยุธยา เข้าด้วยกัน โดยใช้วงจรเช่า 128Kbps และ 64Kbps ตามลำดับ เพื่อทำการสื่อสารข้อมูลสารสนเทศ และมีการเชื่อมต่อระบบเครือข่ายภายในเข้ากับเครือข่ายอินเทอร์เน็ตโดยการใช้สัญญาณดาวเทียม 256/128Kbps และ สายสัญญาณเช่า 64Kbps โดยทั่วไปข้อมูลสารสนเทศที่ใช้สื่อสารระหว่างสำนักงานทั้งสองแห่งจะเป็นการรับส่งจดหมายอิเลคทรอนิกส์ ระบบฐานข้อมูล และการใช้โทรศัพท์บนเครือข่าย IP Network

ในปัจจุบันเครือข่ายอินเทอร์เน็ตได้เข้ามามีบทบาทเป็นอย่างมากในบริษัทฯ โดยใช้ในการรับส่งอิเลคทรอนิกส์เมล์ ใช้ในการค้นหาข้อมูลข่าวสารเพื่อนำมาใช้ในการสนับสนุนการทำงานของบริษัทฯรวมทั้งยังนำมาเพื่อทำ Supply Chain Management ทางฝ่ายบริหารจึงมีความต้องการให้มีการสื่อสารข้อมูลและเผยแพร่ข้อมูลสารสนเทศที่ใช้กันภายในบริษัทฯ ให้ทางบริษัทฯแม่ที่ประเทศ สิงคโปร์และสำนักงานสาขาที่ประเทศ มาเลเซีย อินโดนีเซีย และจีน ได้รับทราบ นอกเหนือจากการส่งจดหมายอิเลคทรอนิกส์ โดยมอบหมายให้แผนกสารสนเทศทำการศึกษาถึงความเป็นไปได้ในการวางแผนติดตั้งระบบเครือข่ายที่สามารถสื่อสารข้อมูลผ่านเครือข่ายอินเทอร์เน็ตได้อย่างปลอดภัยและคุ้มค่าการลงทุน

ทางแผนกสารสนเทศได้มองเห็นว่าการสื่อสารข้อมูลต่าง ๆ ผ่านเครือข่ายอินเทอร์เน็ตนั้นเป็นการสื่อสารที่ไม่มีความปลอดภัยเลยเนื่องจากการสื่อสารส่วนมากเป็นในรูปแบบข้อความ(Plain Text) จึงได้คิดที่จะนำเทคโนโลยีเครือข่ายเสมือนส่วนตัว หรือที่รู้จักกันในชื่อ VPN (Virtual Private Network) เข้ามาใช้ เนื่องจากเห็นว่าการส่งข้อมูลผ่านเครือข่าย VPN ไป

บนเครือข่ายอินเทอร์เน็ตนั้นมีความปลอดภัยที่ค่อนข้างสูง และยังมีรูปแบบการเชื่อมต่อในหลายรูปแบบ จึงทำให้เทคโนโลยี VPN น่าจะเป็นเทคโนโลยีที่เหมาะสมที่สุดในการนำมาใช้งานเพื่อตอบสนองความต้องการและนโยบายผู้บริหาร

1.1 วัตถุประสงค์การศึกษา

1. เพื่อศึกษาข้อมูลที่ทำการทางบริษัทฯใช้ในการสื่อสารระหว่างสำนักงานในประเทศกับบริษัทฯแม่ที่สิงคโปร์
2. เพื่อศึกษาความรูปแบบของเครือข่าย VPN แบบต่าง ๆ
3. เพื่อศึกษาความเป็นไปได้ในการนำเทคโนโลยีเครือข่าย VPN เข้ามาใช้ในการสื่อสารข้อมูลผ่านเครือข่ายอินเทอร์เน็ต
4. เพื่อศึกษาวิธีการติดตั้งเครือข่าย VPN
5. เพื่อเสนอแนะแผนงาน และ กลยุทธ์การดำเนินงานการติดตั้งเครือข่าย VPN ระหว่างสำนักงานสาขาต่าง ๆ

1.2 ขอบเขตในการศึกษา

1. ศึกษาเฉพาะในส่วนที่เป็นการเชื่อมต่อระหว่างสำนักงานในประเทศเชื่อมต่อกับสำนักงานใหญ่ที่ประเทศสิงคโปร์เพื่อเป็นแนวทางให้กับสำนักงานอื่น ๆ ต่อไป
2. ศึกษาเฉพาะความเป็นไปได้ในส่วนที่มีความสำคัญในการตัดสินใจดำเนินงานโครงการของผู้บริหาร
    - ความเป็นไปได้ทางเทคนิคตามวิธีการพัฒนาโครงการด้านระบบสารสนเทศ ได้แก่ HARDWARE, SOFTWARE, NETWORKING และ ระบบข้อมูลต่าง ๆที่มีความจำเป็นในการสื่อสารผ่านเครือข่าย VPN
    - ความเป็นไปได้ทางเศรษฐศาสตร์ และการเงิน ได้แก่ การทำ Cash Flow Analysis, Net Present Value (NPV), Benefit/Cost Ratio, Internal Rate of Return (IRR), Pay back Period , Return on Investment

3. เสนอแนะแนวทาง แผนงาน กลยุทธ์ในการดำเนินงาน และ งบประมาณ ในการดำเนินงานในการบริหารโครงการ รวมทั้งข้อเสนอแนะในการดำเนินงานด้านอื่น ๆ ในการพัฒนาโครงการในระยะต่อ ๆ ไป

1.3 วิธีการศึกษา

1. ศึกษารูปแบบและวิธีการทำงานขั้นพื้นฐานของเครือข่าย VPN
2. ศึกษาเครือข่ายคอมพิวเตอร์ภายในของบริษัทฯเพื่อทำการศึกษาหารูปแบบของเครือข่าย VPN ที่เหมาะสม
3. ศึกษารูปแบบของข้อมูลที่จะทำการสื่อสารผ่านเครือข่าย VPN เพื่อพิจารณาคัดเลือกข้อมูลที่สำคัญ ๆ
4. วิเคราะห์ทางการเงินและผลตอบแทนทางการเงิน ตามหลักวิธีการทางเศรษฐศาสตร์

1.4 ประโยชน์ที่คาดว่าจะได้รับ

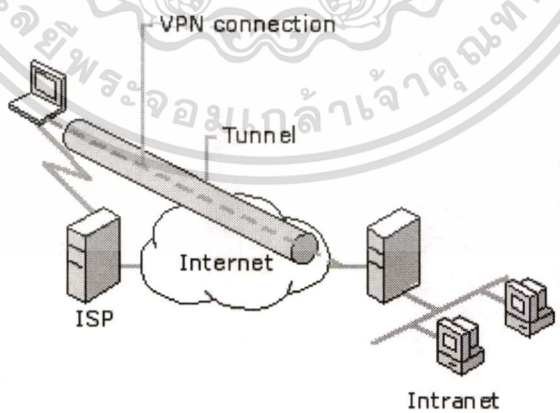
1. เพื่อช่วยให้ผู้บริหารได้มีข้อมูลเพื่อการตัดสินใจในการวางแผนดำเนินโครงการ การนำเครือข่าย VPN มาใช้ในบริษัทฯและสาขาต่าง ๆ รวมทั้งเป็นแนวทางการวิเคราะห์โครงการด้านสารสนเทศของบริษัทฯด้านต่าง ๆ ของบริษัทฯในโอกาสต่อไป
2. เพื่อช่วยในเครือข่ายที่จะทำการติดตั้งได้คุ้มค่าต่อการลงทุน และ ตรงตามความต้องการของผู้ใช้งานระบบ
3. ช่องทางการสื่อสารข้อมูลให้กับผู้บริหารและพนักงานที่ต้องทำงานนอกสถานที่ให้สามารถรับรู้ข่าวสารและสารสนเทศภายในได้จากทุก ๆ สถานที่ที่สามารถเชื่อมต่อเข้าเครือข่ายอินเทอร์เน็ตได้
4. เพิ่มประสิทธิภาพในการดูแลรักษาระบบสารสนเทศภายในโดยสามารถเข้ามาตรวจสอบและแก้ไขข้อผิดพลาดของระบบภายในจากภายนอกได้อย่างปลอดภัย
5. สามารถเพิ่มช่องทางการค้นหาข้อมูลจากระบบภายในของสำนักงานแต่ละสาขาได้นอกจากทางอิเลคทรอนิกส์เมล์
6. ลดค่าใช้จ่ายในการเช่าสายสัญญาณ LEASED LINE ซึ่งมีค่าใช้จ่ายที่สูงมากเมื่อเปรียบเทียบกับการใช้งานผ่านเครือข่ายอินเทอร์เน็ตถึงแม้ว่าประสิทธิภาพจะไม่สามารถนำมาเทียบกับการเช่าสัญญาณ LEASED LINE

7. เพิ่มความปลอดภัยของข้อมูลที่ทำการสื่อสารระหว่างสำนักงานต่าง ๆ เนื่องจากก่อนการ Implement เครือข่าย VPN นั้นเครือข่ายระหว่างประเทศนั้นส่งข้อมูลส่วนใหญ่ผ่านอินเทอร์เน็ตโดยการรับส่ง จดหมายอิเลคทรอนิกส์ ซึ่งการรับส่ง จดหมายอิเลคทรอนิกส์ ผ่านเครือข่ายอินเทอร์เน็ตโดยตรงนั้นสามารถที่จะดักจับข้อมูลแล้วนำมาตีความได้เพราะข้อมูลที่ผ่านเครือข่ายอินเทอร์เน็ตเป็นข้อความที่มิได้มีการเข้ารหัสแต่อย่างใด
8. ผลตอบแทนจากการอนุญาตให้เข้าใช้ระบบจากสำนักงานสาขาต่าง ประเทศ คือ มาเลเซีย อินโดนีเซีย และ จีน

บทที่ 2

รูปแบบของเครือข่าย VPN

เทคโนโลยีเครือข่าย VPN ถือได้ว่าเป็นเทคโนโลยีที่ช่วยเพิ่มประสิทธิภาพของการรับส่งข้อมูลในด้านความปลอดภัยของข้อมูลที่ต้องทำการขนส่งผ่านเครือข่ายสาธารณะอย่างเช่น เครือข่ายอินเทอร์เน็ตในปัจจุบัน โดยทำการประมาณช่องทางการขนส่งข้อมูลผ่านเครือข่ายสาธารณะให้เปรียบเสมือนเครือข่ายแบบ POINT-TO-POINT โดยทำการส่งข้อมูลเข้าระบบเครือข่ายสาธารณะหรือที่เรียกว่าการทำ TUN NELING โดยทั่วไปแล้วการทำ VPN นั้นมักนิยมทำการใน 2 เลเยอร์ คือใน เลเยอร์ 3 เน็ตเวิรค์ เลเยอร์ และ ในเลเยอร์ 2 หรือ ดาต้าลิงค์เลเยอร์ นอกจากนี้แล้ว กลไกในการสร้างเครือข่าย 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

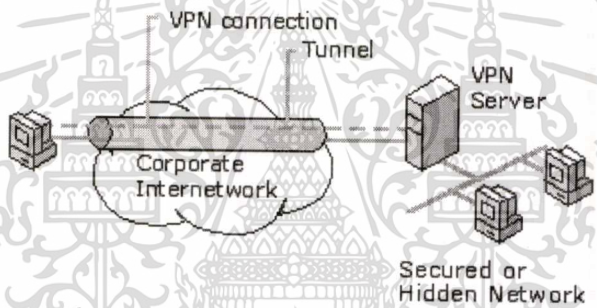


รูปที่ 2.1 การเชื่อมต่อ VPN

ในการแบ่งลักษณะการติดตั้งเครือข่าย VPN นั้นสามารถแบ่งออกได้หลายวิธีแต่วิธีที่นิยมกันโดยแบ่งตามการเข้ารหัสข้อมูลและการทำอุโมงค์ (Tunnel)

2.1 การเชื่อมต่อแบบ Client – to – Gateway

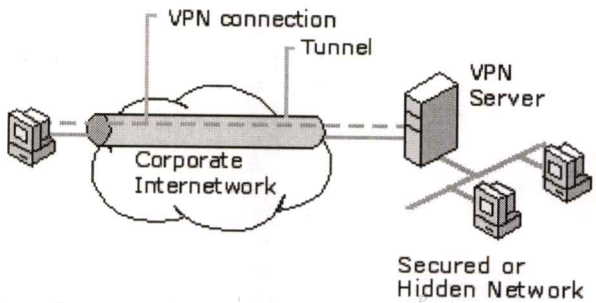
เป็นรูปแบบในการเข้าถึงเครือข่าย VPN จากอุปกรณ์เคลื่อนที่ต่างๆ ซึ่งสามารถเข้าถึงเครือข่ายได้ โดยเริ่มต้นจาก ผู้ใช้หมุนโมเด็ม ติดต่อมายังไอเอสพี และจากนั้นเครื่องของผู้ใช้ก็ทำการสร้าง Tunnel และเข้ารหัสข้อมูล ติดต่อกับเครื่อง VPN Server ของทางบริษัทฯ เพื่อส่งต่อข้อมูลไปยังเครื่องจุดหมายปลายทางซึ่งในรูปแบบนี้เหมาะสำหรับการใช้งานของผู้บริหารหรือพนักงานที่จำเป็นต้องเดินทางออกไปทำงานนอกบริษัทฯ บ่อย ๆ



รูปที่ 2.2 การเชื่อมต่อ VPN แบบ Client – to - Gateway

2.2 การเชื่อมต่อแบบ Gateway – to – Gateway

เป็นรูปแบบในการเข้าถึงเครือข่าย VPN ที่ใช้เฉพาะภายในบริษัทฯเท่านั้น อย่างเช่นการต่อเชื่อมเครือข่าย ระหว่างสำนักงานใหญ่ในกรุงเทพฯ และสาขาย่อย ในต่างจังหวัด เสมือนกับ การทดแทน การเช่าวงจร ระหว่าง กรุงเทพกับต่างจังหวัด โดยที่แต่ละสาขา สามารถต่อเชื่อมเข้ากับ ผู้ให้บริการอินเทอร์เน็ต ในท้องถิ่นของตน เพื่อเชื่อมเข้า เครือข่าย VPN ของบริษัทฯ อีกทีหนึ่ง

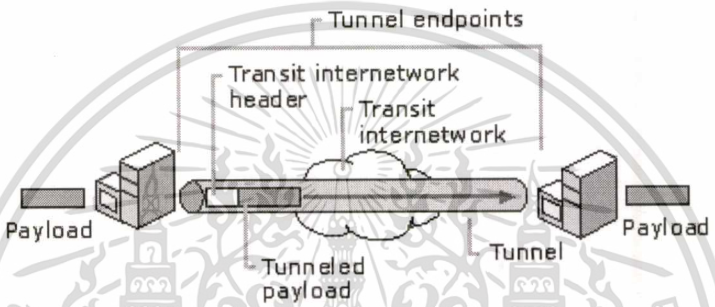


รูปที่ 2.3 การเชื่อมต่อ VPN แบบ Gateway – to – Gateway

2.3 โปรโตคอลพื้นฐานของระบบเครือข่าย VPN

การเชื่อมต่อเครือข่ายต่าง ๆ เข้าหากันโดยการใช้ VPN จำเป็นต้องมีโปรโตคอลพื้นฐานที่ทำหน้าที่ในการเข้ารหัสและทำ Tunnel ให้กับการเชื่อมต่อแต่ละครั้ง

2.3.1 คุณสมบัติหลักของโปรโตคอล VPN



รูปที่ 2.4 รูปแบบการทำ TUNNELING

User Authentication. โปรโตคอลนั้นต้องสามารถทำการระบุสิทธิ์ให้กับ VPN Client ได้โดยตรงเมื่อทำการเชื่อมต่อเข้ากับ VPN Server และทั้งยังสามารถตรวจสอบการทำงานต่าง ๆ ของ VPN Client ได้ว่าทำงานใด ใครเป็นผู้ใช้ระบบและใช้งานเวลาใดถึงเวลาใด อย่างเช่น การใช้ EAP (Extensible Authentication Protocol) ในการเชื่อมต่อแบบ PPTP หรือการใช้ IKE (Internet Key Exchange) ในการเชื่อมต่อแบบ IPSec Tunnel Model

Address Management โปรโตคอลนั้นต้องสามารถกำหนดหมายเลขของเครื่องให้ VPN Client และเก็บ หมายเลข IP Address ที่เป็นหมายเลขภายในไว้ไม่ให้สามารถทำการอ่านได้ในเครือข่ายสาธารณะ เช่นการใช้การกำหนดหมายเลขแบบ NCP (Network control Protocol) ของการเชื่อมต่อด้วย L2TP

Data Encryption and Compression โปรโตคอลนั้นต้องทำให้ข้อมูลที่ถูกส่งผ่านเครือข่ายสาธารณะไม่สามารถอ่านโดยผู้ที่ไม่ได้รับสิทธิในการอ่านข้อมูลนั้น อย่างเช่นการใช้ MPPE (Microsoft Point to Point Encryption)

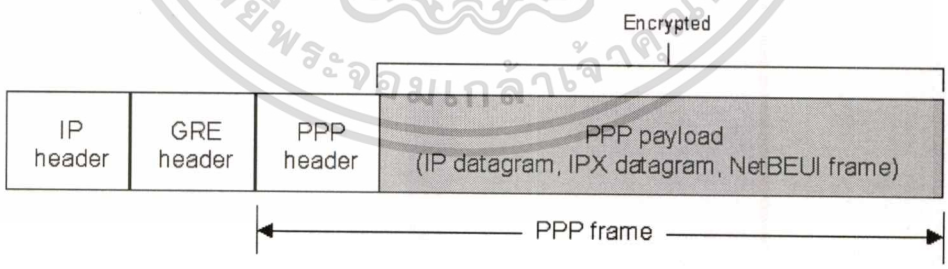
Key Management โปรโตคอลนั้นต้องทำการสร้างกุญแจเข้ารหัสข้อมูลที่ใหม่เสมอให้กับทั้งฝั่ง VPN Client และ VPN Server

Multiprotocol Support. โปรโตคอลนั้นควรสามารถทำการขนส่งข้อมูลที่ใช้โปรโตคอลที่มีการใช้งานทั่วไปได้ เช่น IP (Internet Protocol), IPX (Internetwork Packet Exchange)

โปรโตคอลที่ใช้ในการทำอุโมงค์ (TUNNELING) เพื่อเชื่อมต่อเครือข่าย VPN มีอยู่หลายโปรโตคอลแต่ในปัจจุบันที่ใช้กันทั่วไปมีอยู่ด้วยกัน 3 โปรโตคอล คือ

2.3.2 PPTP (Point to Point TUNNELING Protocol)

เป็นโปรโตคอลสำหรับสร้าง Tunnel ที่ใช้รับส่งข้อมูลผ่านเครือข่ายสาธารณะ เช่น อินเทอร์เน็ต พัฒนาขึ้นโดยกลุ่มบริษัท Microsoft, 3Com และ Ascend Communication โดย PPTP สามารถผนึกเฟรมของข้อมูลได้หลายชนิด เช่น IP, IPX หรือ NetBEUI แล้วส่งเฟรมเหล่านี้ผ่านเฟรม PPP ตามปกติ เมื่อตรวจดูข้อมูลที่ถูกส่งออกไปจะเสมือนกับการรับส่งเฟรม PPP ตามธรรมดาของคอมพิวเตอร์สองระบบ ซึ่งแท้ที่จริงแล้วข้อมูลที่รับส่งอาจจะเป็นเฟรม IP, IPX หรือ NetBEUI ที่คอมพิวเตอร์ทำการรับส่งข้อมูลกันจริงๆก็ได้ เมื่อใช้การเข้ารหัสและการลดข้อมูลเข้าไปอีก การรับส่งข้อมูลก็จะปลอดภัยมากยิ่งขึ้น PPTP จะใช้โปรโตคอล TCP(Transmission Control Protocol) ในการสร้าง Tunnel และแลกเปลี่ยนข้อมูลต่างๆที่เกี่ยวกับ Tunnel และใช้ PPP เป็นตัวรับส่งข้อมูลที่ต้องการติดต่อระหว่างผู้รับและผู้ส่ง

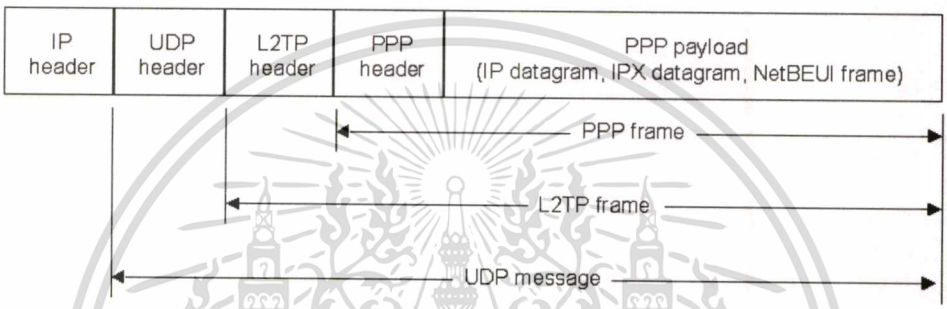


รูปที่ 2.5 ตัวอย่าง Packet ข้อมูลในแบบ PPTP

2.3.3 L2TP (Layer 2 TUNNELING Protocol)

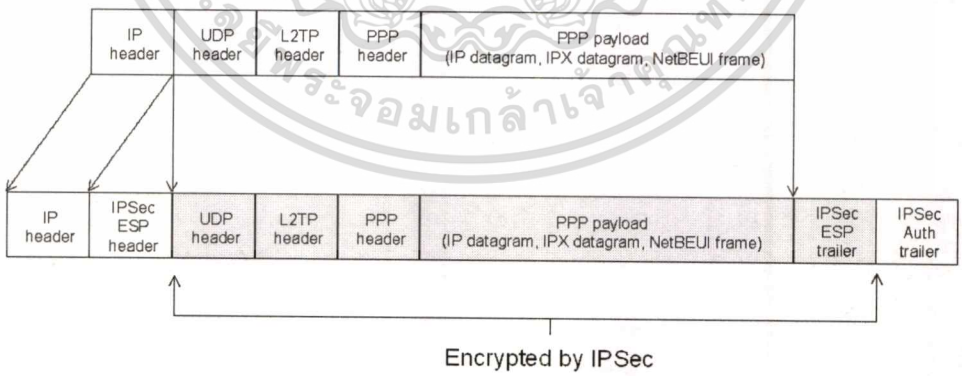
จะมีการทำงานคล้ายกับ PPTP แตกต่าง กันตรง L2TP จะใช้ User Datagram Protocol (UDP) ในการตกลงรายละเอียดในการรับส่งข้อมูลและสร้าง Tunnel แทนที่จะใช้ TCP ทำหน้าที่นี้ ส่วนเนื้อของข้อมูลจะรับส่งโดยใช้ UDP/PPP ผ่าน Tunnel ที่สร้างขึ้น แทนการใช้ TCP/IP ส่งไปกับ PPP ตามปกติ คุณสมบัติของ L2TP คือสามารถผนึกข้อมูลเฟรม PPP ทั้งหมด

ส่งไปในเครือข่ายอยู่ระดับล่างชนิดต่างๆ ได้ เช่น IP, X.25, Frame Relay หรือ ATM ทำให้ L2TP มีความคล่องตัวสูง เนื่องจากสามารถเลือกใช้เครือข่ายรับส่งข้อมูลระดับล่างได้หลายชนิดนั่นเอง ข้อมูลที่ส่งไปในท่อนี้อาจเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูล หรืออาจลดขนาดข้อมูลก่อนส่งด้วยก็ได้ คือ L2TP สามารถผนึกโปรโตคอลที่มีการรักษาความปลอดภัยในการรับส่งข้อมูล เช่น CHAP, PAP หรือ MS-CHAP ก็ได้ การสร้าง Tunnel ของ L2TP จะเกิดในระดับ Data Link Layer ในชั้นที่ 2 ของ OSI 7-Layer Model เช่นเดียวกับซอฟต์แวร์สำหรับการทำ TUNNELING ตัวอื่นๆ



รูปที่ 2.6 ตัวอย่าง Packet ข้อมูลในแบบ L2TP

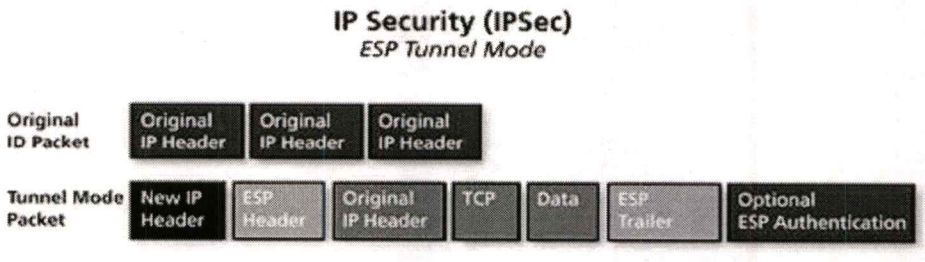
ในปัจจุบันได้นำเอาเทคโนโลยีการเข้ารหัสของ IPSec เข้ามาทำการเข้ารหัสข้อมูลให้กับเครือข่ายที่ใช้ L2TP โดยมักเรียกกันว่า L2TP/IPSec โดยหลังจากการเข้ารหัสแล้วชุดของข้อมูลจะได้ดังภาพ



รูปที่ 2.7 ตัวอย่าง Packet ข้อมูลในแบบ L2TP/IPSec

2.3.4 IPSec TUNNELING

เป็นการสร้าง Tunnel หรือท่อรับส่งข้อมูลอีกชนิดหนึ่งที่นับเป็นมาตรฐานในการรับส่งรับข้อมูลผ่านระบบเครือข่าย ที่พัฒนาขึ้นโดย Internet Engineering Task Force (IETF) ซึ่งกำหนดให้เฟรม IP ของข้อมูลที่ต้องการรับส่งถูกเข้ารหัสทั้งกลุ่ม (รวมทั้ง IP Address ด้วย) และเป็นข้อมูลของเฟรม IP ในชั้นถัดลงไป ข้อมูลทั้งหมดนี้จะถูกเข้าเข้ารหัสโดย Data Encryption Standard (DES) ซึ่งผู้รับและผู้ส่งจะใช้รหัสลับ ตัวเดียวกันในการเข้ารหัสและถอดรหัส ดังนั้นเข้ารหัสข้อมูลจำเป็นจะต้องส่งรหัสลับนี้ผ่านระบบเครือข่าย ไปให้ผู้รับเพื่อให้ในการถอดรหัสข้อมูลด้วย เพื่อให้การส่งรหัสลับนี้ผ่านระบบเครือข่ายปลอดภัย รหัสลับจะถูกเข้ารหัสโดยใช้ Diffie-Hellman เข้ารหัสในแบบ Asymmetric encryption คือมีการใช้รหัสลับสองตัวที่เรียกว่า Public Key และ Private Key ทำให้ผู้อื่นที่ดักข้อมูลในสายไม่สามารถอ่านรหัสลับนี้ได้ ทั้งผู้ลับและผู้ส่งจะใช้โปรโตคอลที่เรียกว่า Internet Key Exchange (IKE) ในการตกลงมาตรฐานการเข้ารหัสข้อมูล รวมถึงการส่งรหัสลับผ่านเครือข่าย ทำให้ IPSec มีความปลอดภัยจากการถูกผู้อื่นลักลอบดักข้อมูลในสายไปใช้ เมื่อส่งข้อมูลนี้ไปถึงปลายทาง ข้อมูลจะถูกถอดเฟรม IP ชั้นนอกออก เพื่อให้ได้ส่วนที่เป็นข้อมูลของชั้นแรกแล้วทำการถอดรหัสข้อมูลที่ได้รับนี้ให้กลับมาเป็นเฟรม IP ของข้อมูลเดิม โดยใช้รหัสลับที่ตกลงกันเอาไว้ ซึ่งจะเห็นว่าการทำงานจะเหมือนกับ PPTP นั่นเอง แต่ต่างกันตรงที่ว่าจะใช้การผนึกข้อมูลด้วยเฟรม IP ซ้อนสองชั้น โดยมีการเข้ารหัสข้อมูล IP ในชั้นแรก แทนการใช้ PPTP ในการรับส่งข้อมูลผ่าน Tunnel เท่านั้น เนื่องจาก IPSec เป็นมาตรฐานที่เสนอโดย Internet Engineering Task Force (IETF) ผู้ผลิตอุปกรณ์เครือข่ายและ ซอฟต์แวร์ระบบเครือข่าย ทั้งหลายก็จะพัฒนาผลิตภัณฑ์ของตนให้รองรับการทำงานของ IPSec นี้ คาดว่า IPSec จะค่อยๆแทนที่ TUNNELING Protocol อื่นๆที่มีอยู่ ในท้องตลาดปัจจุบันเช่น PPTP , L2F และ L2TP จนเหลือเป็นมาตรฐานเดียวในที่สุด



รูปที่ 2.8 ตัวอย่าง Packet ข้อมูลในแบบ IPSec TUNNELING

หลังจากที่ได้ศึกษาความสามารถและหลักการในการทำงาน วิธีการเข้ารหัส และรูปแบบในการติดต่อสื่อสารของเครือข่าย VPN แล้วจะสามารถช่วยให้วิเคราะห์เพื่อหารูปแบบในการวางระบบเครือข่าย VPN ให้เข้ากับความต้องการและการทำงานของบริษัทฯ ได้ดียิ่งขึ้นโดยเลือกเอามาตรฐานที่เป็นมาตรฐานใหม่แต่เริ่มแพร่หลายและสามารถหาอุปกรณ์ที่ใช้งานได้ง่ายอย่างการทำ IPSec TUNNELING มาเป็นตัวเลือกในการวางระบบเครือข่าย VPN ระหว่างสำนักงานจังหวัดสมุทรปราการและประเทศสิงคโปร์

บทที่ 3
การวิเคราะห์ความเป็นไปได้ทางเทคนิคของโครงการ

การศึกษาความเป็นไปได้ในการดำเนินโครงการ เพื่อช่วยในการตัดสินใจถึงความเป็นไปได้ของโครงการว่าจะสำเร็จไปได้ตามที่ต้องการหรือไม่ โดยจะทำการศึกษาใน 3 ลักษณะคือ การวิเคราะห์ความเป็นไปได้ในเชิงเทคนิค การวิเคราะห์ความเป็นไปได้ทางการเงิน และวิเคราะห์ความเป็นไปได้ในเชิงการปฏิบัติการ โดยในบทที่ 3 นี้จะเน้นไปที่การวิเคราะห์หาความเป็นไปได้ทางเทคนิคเป็นหลัก โดยจะศึกษารูปแบบการติดต่อสื่อสารปริมาณการสื่อสารของระบบ ตลอดจนเปรียบเทียบอุปกรณ์ที่จะทำหน้าที่ในการรองรับการทำงานของ VPN รูปแบบต่าง ๆ

ในปัจจุบันรูปแบบในการสื่อสารข้อมูลของบริษัทฯ นั้นมีแนวทางในการเข้าถึงได้เฉพาะในส่วนที่เป็นเครือข่ายภายในและในส่วนที่เป็นการรับส่ง E-MAIL จากภายนอกเท่านั้น แต่ในปัจจุบันนั้นมีผู้บริหารและพนักงานในหลาย ๆ ส่วนที่ไม่ได้ประจำในสำนักงานจึงเป็นการยากที่จะเข้าถึงเครือข่ายภายในนอกจากการรับรู้ผ่าน E-MAIL เท่านั้นอีกทั้งปัจจุบันฝ่ายสารสนเทศได้พัฒนาระบบในการเข้าถึงข้อมูลภายในผ่านอินทราเน็ทภายในบริษัทฯ จึงทำให้ผู้บริหารในส่วนต่าง ๆ ต้องการเข้าถึงข้อมูลบน อินทราเน็ทจากภายนอกบริษัทฯ แต่ต้องเป็นไปด้วยความปลอดภัย และข้อมูลไม่รั่วไหลไปภายนอก โดยกำหนดการเข้าถึงข้อมูลได้แบ่งออกเป็นการสื่อสารระหว่างสำนักงานระหว่างประเทศ และผู้ใช้งานทางไกลผ่านเครือข่ายอินเทอร์เน็ตสาธารณะ

3.1 การสื่อสารข้อมูลรูปแบบต่าง ๆภายในบริษัทฯ

การใช้งานข้อมูลสารสนเทศ ต่าง ๆ ในบริษัทฯนั้นแยกการใช้งานออกเป็น 2 ส่วน โดยแยกการเชื่อมต่อออกเป็น 2 รูปแบบคือ

- ส่วนที่ต้องทำงานนอกสถานที่แลผู้บริหารที่ต้องเดินทางไปต่างประเทศ
  1. จำนวนผู้บริหารและพนักงานที่ต้องทำงานนอกสถานที่ 10 ท่าน หากมีการเชื่อมต่อพร้อมกันคิดเป็น 10 การเชื่อมต่อ
  2. การรับส่งจดหมายอิเลคทรอนิกส์ ใช้โปรโตคอล TCP/IP, IMAP4, POP3, SMTP
  3. การตรวจสอบข้อมูลข่าวสารบริษัทฯผ่าน Website http://intranet.armstrong.co.th ใช้งานโปรโตคอล TCP/IP, HTTP, FTP

4. การทำ Remote Admin ของฝ่ายสารสนเทศ ใช้งาน โปรโตคอล TCP/IP, RDP

- ส่วนที่เป็นการเชื่อมต่อระหว่างสาขาย่อยและสาขาต่างประเทศ
  1. มีสำนักงานที่ต้องทำการเชื่อมต่ออยู่ 4 สำนักงาน ในแต่ละสำนักงานจะมีผู้บริหารเชื่อมต่อสำนักงานได้ 6 การเชื่อมต่อ
  2. การตรวจสอบสินค้าคงค้างในระบบผ่าน Website intranet.armstrong.co.th ใช้โปรโตคอล TCP/IP, HTTP, FTP
  3. การทำ Remote Admin ระหว่างสาขา ใช้โปรโตคอล TCP/IP, RDP
  4. การเข้าใช้งานระบบ ERP (Enterprise Resource Planning) ภายในสำนักงาน ใช้งานโปรโตคอล TCP/IP, Port 20001,20002
  5. การรับส่งจดหมายอิเลคทรอนิกส์ระหว่างสาขาในประเทศไทย 3 สาขา ใช้โปรโตคอล TCP/IP, IMAP4, POP3, SMTP

โดยการเชื่อมต่อทั้งหมดทั้งในแบบที่เป็น Remote Access และแบบที่เป็น Gateway to Gateway มีการเชื่อมต่อที่อนุญาตให้มากที่สุดทั้งหมด 34 การเชื่อมต่อ ซึ่งโดยทั่วไปแล้ว ประมาณการเชื่อมต่อแบบ Remote Access นั้นจะมีการเชื่อมต่อในเวลาเดียวกันน้อยมากคือมากที่สุดประมาณ 4 การเชื่อมต่อ แต่ในการเชื่อมต่อแบบที่เป็น Gateway to Gateway ทั้ง 4 สำนักงาน จะมีการเชื่อมต่อพร้อมกันประมาณไม่เกิน 3 การเชื่อมต่อในเวลาเดียวกันโดยรวมแล้วจะมีการเชื่อมต่อในพร้อมกันมากที่สุดประมาณ 16 การเชื่อมต่อ

3.2 รูปแบบของโปรโตคอลที่ต้องใช้งานผ่านเครือข่าย VPN

1) TCP/IP (Transmission Control Protocol / Internet Protocol)
2) IMAP4 (Internet Mail Application Protocol Version 4)
3) POP3 (Post Office Protocol Version 3)
4) SMTP(Simple Mail Transfer Protocol)
5) HTTP(Hyper Text Transfer Protocol)
6) FTP(File Transfer Protocol)
7) RDP(Remote Desktop Protocol)
8) TCP Port 20001 ARC1L Database
9) TCP Port 20002 CRP2 Database

หมายเหตุ : รายละเอียดในภาคผนวก ก.

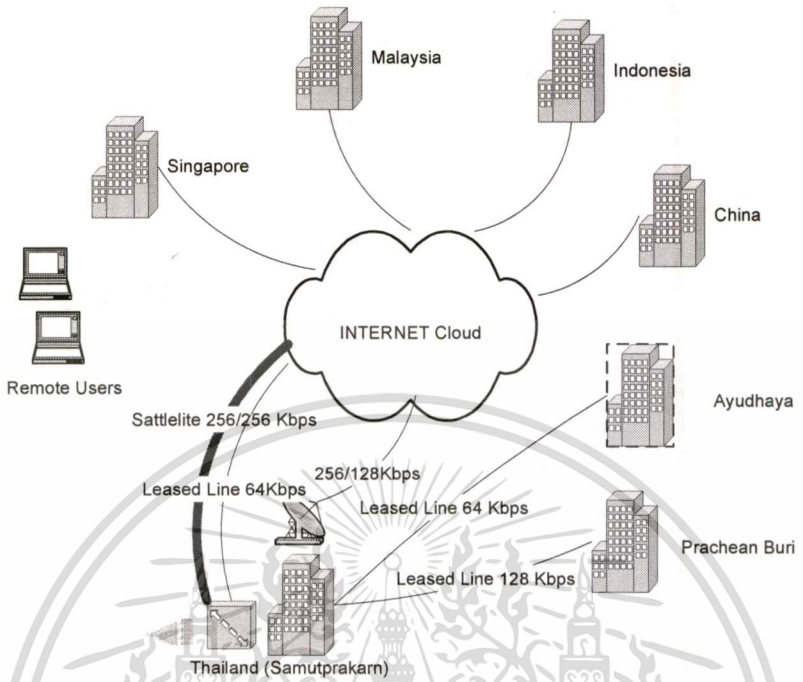
3.3 แนวคิดการนำเอาเทคโนโลยีเครือข่ายเสมือนส่วนตัวมาใช้ในการสื่อสารระหว่างสำนักงานสาขาต่าง ๆ

จากข้อมูลเบื้องต้นนั้นเราสามารถแบ่งแนวทางการติดตั้งเครือข่าย VPN ในบริษัทฯออกได้เป็น 4 แบบ คือ

- การติดตั้งการเชื่อมต่อแบบ Gateway to Gateway โดยใช้อุปกรณ์ที่ได้รับการออกแบบมาเพื่อใช้ในการติดตั้ง VPN โดยเฉพาะ
- การติดตั้งการเชื่อมต่อแบบ Gateway to Gateway โดยโดยการใช้ซอฟแวร์ทำ Tunnelling ให้กับ VPN
- การติดตั้งการเชื่อมต่อแบบ Client to Gateway โดยใช้อุปกรณ์ที่ได้รับการออกแบบมาเพื่อใช้ในการติดตั้ง VPN โดยเฉพาะ
- การติดตั้งการเชื่อมต่อแบบ Client to Gateway โดยโดยการใช้ซอฟแวร์ทำ Tunnelling ให้กับ VPN

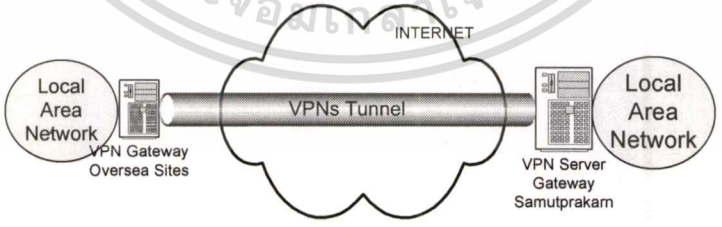
โดยในแต่ละแนวทางต้องเลือกโปรโตคอลในการทำ Tunnelling และเลือกรูปแบบในการเข้ารหัสข้อมูลให้กับการเครือข่าย VPN

จากข้อมูลที่ได้จากการศึกษาทั้งในส่วนของการเชื่อมต่อเครือข่ายและลักษณะการทำงานของโปรโตคอลแต่ละตัวที่มีความสำคัญต่อการใช้ระบบเครือข่าย VPN แล้วนั้นทำให้สามารถสรุปได้ว่าในรูปแบบของบริษัทฯที่มีพนักงานที่ต้องเดินทางไปทำงานนอกสถานที่ รวมทั้งผู้บริหารที่จำเป็นต้องมีการเดินทางไปต่างประเทศ และยังมีบริษัทฯที่เป็นสาขาต่าง ๆ ทั้งภายในและภายนอกประเทศทำให้สรุปได้ว่าระบบ VPN ที่เหมาะสมที่จะนำมาใช้ในบริษัทฯควรจะเป็นการเชื่อมต่อ VPN ทั้งสองแบบจะเป็นดังรูป



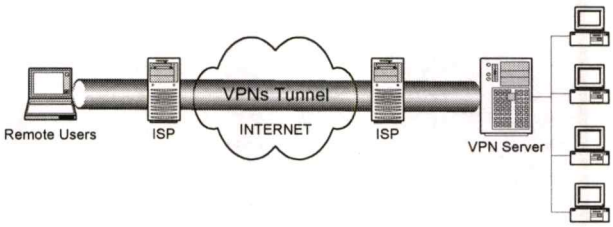
รูปที่ 3.1 การเชื่อมต่อเครือข่ายภายในผ่านเครือข่ายอินเทอร์เน็ตที่คาดว่าจะเป็นหลังจากการติดตั้ง VPN

โดยในส่วนที่เป็นสำนักงานสาขาต่าง ๆ จะเชื่อมต่อเข้าเครือข่ายอินเทอร์เน็ตประจำท้องถิ่นและทำการร้องขอการเชื่อมต่อ VPN ผ่าน VPN Gateway ของแต่ละสำนักงานเข้ามาที่ VPN Server Gateway สำนักงานจังหวัดสมุทรปราการเพื่อทำการเชื่อมต่อเครือข่ายของแต่ละสำนักงานเข้าด้วยกัน เป็นแบบ Gateway – to – Gateway ตามรูปด้านล่าง



รูปที่ 3.2 การเชื่อมต่อสำนักงานสาขา เข้ากับเครือข่าย VPN

และในส่วนของผู้บริหารและพนักงานที่ต้องเดินทางออกไปทำงานนอกสถานที่จะใช้การเชื่อมต่อจากอุปกรณ์เคลื่อนที่ของแต่ละบุคคลต่อไปยังผู้ให้บริการอินเทอร์เน็ตท้องถิ่นแล้วทำการสร้างการเชื่อมต่อ VPN ซึ่งจะจัดอยู่ในรูปแบบ Client – to – Gateway VPN. ดังรูปด้านล่าง



รูปที่ 3.3 การเชื่อมต่อสำหรับ Remote Users

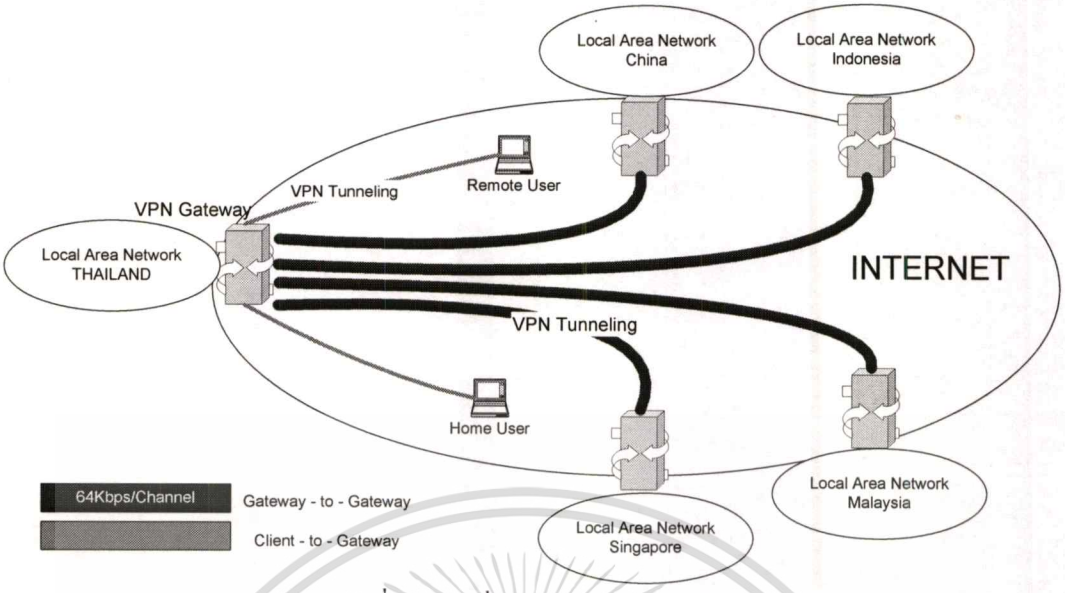
โดยในปัจจุบันนั้นอุปกรณ์และซอร์ฟแวร์ที่มีความสามารถในการทำ VPN TUNNELING นั้นมีความสามารถในการทำงานในทั้งสองแบบทำให้เราสามารถกำหนดทางเลือกที่จะนำมาวิเคราะห์เพื่อหาแนวทางการวางระบบเครือข่าย VPN ให้กับบริษัทฯ ได้ออกเป็น 2 แบบคือ

(1) เครือข่าย VPN ที่ใช้อุปกรณ์ในการทำ VPN TUNNELING

(2) เครือข่าย VPN ที่ใช้ซอร์ฟแวร์ในการทำ VPN TUNNELING

3.4 การวางระบบเครือข่าย VPN และทางเลือกในการศึกษา

การเชื่อมต่อโดยรวมของเครือข่าย VPN ที่ทำการเชื่อมต่อ Remote User และสำนักงานสาขาต่างประเทศโดยสำนักงานประเทศไทยจะทำการติดตั้งสัญญาณ อินเตอร์เน็ตเพิ่มเติมจากที่มีอยู่เดิม Leased Line 64Kbps , Satellite 256/128 Kbps โดยเพิ่มการเชื่อมต่อแบบ Satellite 256/256 Kbps เพื่อเป็นการแบ่งสัญญาณออกเป็น 4 ช่อง ๆ ละ 64/64 Kbps โดยอุปกรณ์ที่เลือกใช้ในการทำ VPN Tunneling นั้นต้องสามารถทำการกำหนดปริมาณการส่งข้อมูลของแต่ละช่องทางได้ ซึ่งในแต่ละสำนักงานต้องไปทำการจัดสรรการใช้งานเครือข่าย VPN ของตนเองจากปริมาณ Bandwidth ที่กำหนดให้คือ 64Kbps



รูปที่ 3.4 การเชื่อมต่อโดยรวมของเครือข่าย VPN

ซึ่งหากเลือกการทำงาน Tunneling โดยการนำเอา ซอร์ฟแวร์มาใช้จะสามารถใช้ความสามารถในการทำ QOS (Quality of Service) ของซอร์ฟแวร์เหล่านั้นได้ แต่หากนำเอาฮาร์ดแวร์มาทำ tunneling ก็จำเป็นต้องเลือกหาอุปกรณ์ที่มีความสามารถในการทำ QOS ในแต่ละช่องสัญญาณของ VPN ได้

3.4.1 ทางเลือกที่ 1 การนำอุปกรณ์มาติดตั้งสำหรับการทำ Tunneling

ในแนวทางที่ 1 ได้เลือกใช้งานอุปกรณ์ของผู้ผลิต Symantec Gateway Security 5420 เพื่อใช้ในการเชื่อมต่อในส่วนของ ฝั่งจังหวัดสมุทรปราการเป็นอุปกรณ์ที่ทำหน้าที่เป็น Server ที่ให้บริการการเชื่อมต่อกับสำนักงานสาขาต่างประเทศ เนื่องจากสามารถให้บริการการการเชื่อมต่อได้กว่า 500 การเชื่อมต่อในขณะเดียวกันรวมทั้งยังมีความสามารถในการส่งผ่านข้อมูลได้ถึง 90 Megabit ต่อวินาที และในส่วนสำนักงานต่างประเทศจะทำการติดตั้งอุปกรณ์ Symantec Firewall/VPN Model 200 ซึ่งสามารถรองรับการทำงานได้พร้อมกันประมาณ 40 การเชื่อมต่อทำให้สามารถรองรับการใช้งานเครือข่ายได้ตามที่ต้องการ

ตารางที่ 3.1 แสดงอุปกรณ์ที่ใช้ในการทำ VPN Tunneling ในทางเลือกที่ 1

ประเภทอุปกรณ์	รายละเอียดอุปกรณ์
VPN Gateway ที่ติดตั้งเป็นศูนย์กลางการเชื่อมต่อที่ติดตั้งในประเทศไทย	Symantec Gateway Security Model 5420
VPN Gateway for Site ที่ติดตั้งไว้ในสำนักงานต่างประเทศ	Symantec Firewall/VPN Model 200

COMPARISON MODEL OF THE APPLIANCES

MODEL	5420	5440/5441	5460/5461
FEATURES			
Maximum Recommended Nodes	500	2500	4500
Stateful Thruput	200 Mbps	1.4 Gbps	1.8 Gbps
High-Availability Type	A/A, A/P, LB (A/A - Active/Active; A/P - Active/Passive; LB - Load Balancing)	A/A, A/P, LB (A/A - Active/Active; A/P - Active/Passive; LB - Load Balancing)	A/A, A/P, LB (A/A - Active/Active; A/P - Active/Passive; LB - Load Balancing)
Maximum Cluster Size	8	8	8
Full Inspection	95 Mbps	680 Mbps	730 Mbps
VPN 3DES Encryption	90 Mbps	400 Mbps	600 Mbps
VPN AES Encryption	30 Mbps	80 Mbps	90 Mbps
Memory	512 MB	1 GB	2 GB
Disk	40 GB	80 GB	80 GB
Rack space	1U	2U	2U
Fast Ethernet NIC	6	0	0
Gigabit NIC	0	6 (Model 5441 - has 2 copper and 4 SX Multi-Mode fiber ports)	8 (Model 5461 has 2 copper and 6 SX Multi-Mode fiber ports)
Connections per second	5000	11300	15300
Concurrent Connections	64,000	190,000	200,000

รูปที่ 3.5 รายละเอียดของอุปกรณ์ Symantec Gateway Security Model 5420,5440,5460

	MODEL 100	MODEL 200	MODEL 200R
Firewall	Yes	Yes	Yes
Gateway to Gateway VPN	Yes	Yes	Yes
Remote client to Gateway VPN	No	No	Yes
xDSL	Yes	Yes	Yes
Cable Modem	Yes	Yes	Yes
PPPoE	Yes	Yes	Yes
ISDN	Yes	Yes	Yes
T1	Yes	Yes	Yes
Recommended User Limit	25	40	40
	No License limitation	No License limitation	No License limitation
LAN Ports	4	8	8
WAN Ports	1	2	2
High Availability	Yes*	Yes*	Yes*
Load balancing	No	Yes	Yes

*With use of external modem and included Auto-Dial-Up Backup

รูปที่ 3.6 รายละเอียดของอุปกรณ์ Symantec FireWall/VPN Model 100,200,200R

3.4.2 ทางเลือกที่ 2 การติดตั้งซอร์ฟแวร์สำหรับการทำ Tunneling

ในทางเลือกที่ 2 การติดตั้งซอร์ฟแวร์สำหรับการทำ Tunneling โดยได้เลือกใช้ซอร์ฟแวร์ LINUX Red Had 8 ในการทำหน้าที่ในการเป็นระบบปฏิบัติการและใช้ IPTable ใน Red Had เพื่อทำ Tunneling สำหรับเครือข่าย VPN เนื่องจากเป็น Open Source และมีความสามารถในการทำ QOS (Quality of Service) โดยประสิทธิภาพในการทำ tunneling และประสิทธิภาพในการถ่ายโอนข้อมูลจะขึ้นอยู่กับประสิทธิภาพของเครื่องคอมพิวเตอร์ที่นำมาติดตั้งซอร์ฟแวร์ Red Had 8

ตารางที่ 3.2 แสดงอุปกรณ์และซอร์ฟแวร์ที่ใช้ในการทำ VPN Tunneling ในทางเลือกที่ 2

ประเภทอุปกรณ์	รายละเอียดอุปกรณ์
เครื่องคอมพิวเตอร์ที่ติดตั้งเป็นศูนย์กลางการเชื่อมต่อที่ติดตั้งในประเทศไทย	PENTIUM 4 2.4 GHz DDR RAM 1 GB BUS 400Mhz IDE 40GB
เครื่องคอมพิวเตอร์ที่ติดตั้งเป็นที่ติดตั้งไว้ในสำนักงานต่างประเทศ	PENTIUM 4 2.4 GHz DDR RAM 512 MB BUS 400Mhz IDE 40GB
ซอร์ฟแวร์ที่นำมาทำ Tunneling	LINUX Red Had 8 with IPTable for Qos

บทที่ 4
การวิเคราะห์ความเป็นไปได้ทางเศรษฐศาสตร์ของโครงการ

การศึกษาความเป็นไปได้ในการดำเนินโครงการ เพื่อช่วยในการตัดสินใจถึงความเป็นไปได้ของโครงการว่าจะสำเร็จไปได้ตามที่ต้องการหรือไม่ โดยจะทำการศึกษาใน 3 ลักษณะคือ การวิเคราะห์ความเป็นไปได้ในเชิงเทคนิค การวิเคราะห์ความเป็นไปได้ทางการเงิน และวิเคราะห์ความเป็นไปได้ในเชิงการปฏิบัติการ โดยในบทที่ 4 นี้จะเน้นไปที่การวิเคราะห์หาความเป็นไปได้ทางการเงินหรือเศรษฐศาสตร์เป็นหลัก

โดยในการวิเคราะห์นี้จะทำการนำเอาบทสรุปรูปแบบการใช้งานของเครือข่าย VPN จากบทที่ 3 มาเป็นฐานในการวิเคราะห์ โดยจะแยกการวิเคราะห์ออกเป็น 2 แนวทางคือ

ทางเลือกที่ 1 ฮาร์ดแวร์ VPN การนำเอาอุปกรณ์ฮาร์ดแวร์ที่มีความสามารถในการทำ VPN TUNNELING เข้ามาติดตั้ง

ทางเลือกที่ 2 ซอร์ฟแวร์ VPN การนำเอาซอร์ฟแวร์มาติดตั้งบนเครื่องคอมพิวเตอร์และทำหน้าที่ในการให้บริการเครือข่าย VPN TUNNELING

4.1 การวิเคราะห์ความเป็นไปได้ทางการเงิน (Economical Feasibility)

ในการศึกษาความเป็นไปได้ในด้านการเงินจะทำการศึกษาถึงปัจจัยด้านการลงทุนในระยะเริ่มแรกและการเลือกใช้เครือข่าย VPN ในแบบต่าง ๆ ตลอดจนพิจารณาถึงค่าใช้จ่ายในการดำเนินงานและการบำรุงรักษาระบบตลอดอายุการใช้งาน และนำผลการศึกษามาสรุปเพื่อใช้ในการตัดสินใจให้ได้ว่าจะใช้การติดตั้งเครือข่าย VPN แบบใดที่มีความเสี่ยงต่อการลงทุนต่ำ , ค่าใช้จ่ายต่ำและมีระยะเวลาในการคุ้มทุนเร็วที่สุด โดยทำการศึกษาการวางระบบเครือข่ายที่ใช้ VPN Server ที่เป็นฮาร์ดแวร์ และ ซอร์ฟแวร์ แยกออกจากกัน

4.1.1 การประมาณการลงทุนเริ่มแรกของทางเลือกที่ 1 (ฮาร์ดแวร์ VPN)

การประมาณค่าการลงทุนเริ่มแรกของโครงการเป็นการหาค่าใช้จ่ายที่ต้องใช้ในการเริ่มต้นโครงการทั้งที่เป็นค่าใช้จ่ายในด้านอุปกรณ์ รวมไปถึงค่าใช้จ่ายต่าง ๆ ที่คาดว่าจะเกิดขึ้นในระยะเริ่มแรก

ราคาอุปกรณ์ที่ต้องใช้ในการติดตั้งเครือข่าย VPN นั้นขึ้นอยู่กับความต้องการของผู้ใช้งานและความสามารถพิเศษในด้านต่าง ๆ ที่จะเข้ามามีผลกระทบต่อราคาของอุปกรณ์แต่ละตัว โดยความต้องการของเครือข่ายต้องสามารถทำการให้บริการการเชื่อมต่อเข้าหาเครือข่ายภายในได้ทั้งในแบบที่เป็น SITE TO SITE และในแบบที่เป็น REMOTE USERS สามารถทำการเข้ารหัสข้อมูลก่อนส่งผ่านเครือข่ายอินเทอร์เน็ต เพื่อเป็นการรักษาความปลอดภัยของข้อมูล มีประสิทธิภาพในการทำงานสูง สามารถรองรับการทำงานแบบ SITE TO SITE ได้ไม่น้อยกว่า 4 การเชื่อมต่อเพื่อรองรับการขยายการใช้งานในอนาคต และรองรับการทำงานแบบ REMOTE USERS ไม่น้อยกว่า 20 การเชื่อมต่อในขณะเวลาเดียวกัน

ตารางที่ 4.1 แสดงราคาอุปกรณ์เครือข่าย ฮาร์ดแวร์ VPN

อุปกรณ์	จำนวน	ราคาต่อหน่วย/บาท	ราคาทั้งหมด	รายละเอียด
Symantec Gateway Security Model 5420	1	120,000	120,000	ใช้ในการติดตั้งที่สำนักงานฝั่งสมุทรปราการ
Symantec FireWall/ VPN Model 200	4	20,000	80,000	ใช้ในการติดตั้งที่สำนักงานฝั่งที่สำนักงานต่างประเทศ
VPN Client (Notebook)	10	12,000**	120,000	เพื่อให้ผู้บริหารระดับกลางและพนักงานที่ต้องทำงานนอกสถานที่เพื่อใช้งาน
VPN Client (Smart Phone)	3	20,000	60,000	เพื่อให้ผู้บริหารระดับสูงสามารถเรียกดูข้อมูลผู้บริหารจากที่ใดก็ได้ผ่านโทรศัพท์มือถือ
ค่าอุปกรณ์ Broadband อินเทอร์เน็ต	1	5,000	5,000	
ระบบสำรองไฟฟ้า	2	25,000	50,000	
รวมราคาอุปกรณ์			435,000	

** ราคา 12,000 บาทเป็นราคาที่ผลต่างหลังจากเปลี่ยนสเปคของอุปกรณ์จากคอมพิวเตอร์ส่วนบุคคลเป็นคอมพิวเตอร์โน้ตบุค

ตารางที่ 4.2 แสดงราคาค่าใช้จ่ายในการติดตั้งระบบ (ฮาร์ดแวร์ VPN)

รายการ	จำนวน	ราคาต่อหน่วย/บาท	ราคาทั้งหมด	รายละเอียด
ค่าติดตั้ง BroadBand อินเทอร์เน็ต	1	5,000	5,000	ยังไม่รวมค่าใช้จ่ายรายเดือน
ค่าใช้จ่ายในการติดตั้งอุปกรณ์จากผู้ขาย	1	10,000	10,000	ในฝั่งสมุทรปราการ
ค่าใช้จ่ายในการติดตั้งอุปกรณ์ในฝั่งประเทศสิงคโปร์	5	10,000	50,000	
ค่าใช้จ่ายในการปรับเปลี่ยนระบบเครือข่ายภายใน	1	12,000	12,000	เพื่อให้เหมาะสมกับการใช้งานเครือข่าย VPN
รวมค่าใช้จ่ายในการติดตั้งระบบทั้งหมด			77,000	

4.1.2 การประมาณรายการค่าใช้จ่ายในการดำเนินการและบำรุงรักษาเครือข่าย (Operation and Maintenance Expense) (ฮาร์ดแวร์ VPN)

การประมาณค่าใช้จ่ายในการดำเนินงานและการบำรุงรักษาเครือข่ายนั้นเป็นการคำนวณหาค่าจ่ายที่เกิดขึ้นระหว่างดำเนินงานรวมถึงการคำนวณหาราคาค่าเสื่อมของอุปกรณ์แต่ละชิ้นของโครงการเพื่อให้เกิดเป็นค่าใช้จ่ายตามความเป็นจริงมากที่สุด

การคำนวณหาค่าเสื่อมอุปกรณ์จะทำการคำนวณค่าเสื่อมแบบเส้นตรง (Straight – Line Depreciation) เนื่องจากรายได้ที่ได้จากโครงการเป็นรายได้ที่ค่อนข้างคงที่ในตลอดระยะเวลาอายุของอุปกรณ์ และเป็นแนวคิดมาตรฐานของบริษัทฯ โดย

กำหนดให้ P คือราคาของอุปกรณ์

L คือมูลค่าซาก คิดเป็น 20% ของราคาอุปกรณ์

n คือออายุการใช้งานอุปกรณ์

ค่าเสื่อมราคาต่อปี $= (P - L) / n$

ตารางที่ 4.3 แสดงค่าเสื่อมอุปกรณ์เครือข่าย VPN (ฮาร์ดแวร์ VPN)

อุปกรณ์	ราคาทั้งหมด (P)	มูลค่าซาก (L)	อายุการใช้งาน (n)	ค่าเสื่อมราคาต่อปี
VPN Gateway	200,000	40,000	5	32,000
VPN Client (Notebook)	120,000	24,000	5	19,200
VPN Client (Smart Phone)	60,000	12,000	5	9,600
ค่าอุปกรณ์ Broadband อินเทอร์เน็ต	5,000	1,000	5	800
ระบบสำรองไฟฟ้า	50,000	10,000	5	8,000
รวมราคาอุปกรณ์	435,000	87,000		69,600

ตารางที่ 4.4 แสดงราคาอุปกรณ์เมื่อสิ้นปีที่ X (ฮาร์ดแวร์ VPN)

ปีที่ X	มูลค่าอุปกรณ์เมื่อวันสิ้นปี X (บาท)	ค่าเสื่อมราคาเมื่อปีที่ X (บาท)
0	435,000	
1	435,000 – 69,600 = 365,400	69,600
2	365,400 – 69,600 = 295,800	69,600 + 69,600 = 139,200
3	295,800 – 69,600 = 226,200	139,200 + 69,600 = 208,800
4	226,200 – 69,600 = 156,600	208,800 + 69,600 = 278,400
5	156,600 – 69,600 = 87,000	278,400 + 69,600 = 348,000
		รวมค่าเสื่อม = 348,000

บริการค่าอินเทอร์เน็ตนั้นเป็นบริการที่บวกบริการเสริม 20 VIP Account with International roaming การคำนวณหาค่าบริการอินเทอร์เน็ตในความเป็นจริงแล้วราคาในการใช้บริการจะมีการลดลงเป็นสัดส่วนในแต่ละปีจึงทำให้เราต้องคิดราคาจากการคำนวณลดราคาในแต่ละปี ปีละ 10 % ของราคาตั้งต้น

ตารางที่ 4.5 แสดงค่าบริการอินเทอร์เน็ต (ฮาร์ดแวร์ VPN)

ปีที่ X	ราคาค่าบริการปี X (บาท)
1	144,000
2	144,000 - (144,000 X 0.1) = 129,600
3	129,600 – (129,600 X 0.1) = 116,640
4	116,640 – (116,640 X 0.1) = 104,976
5	104,976 – (104,976 X 0.1) = 94,478
รวม	589,694 บาท

ตารางที่ 4.6 แสดงราคาค่าใช้จ่ายตลอด 5 ปี (ฮาร์ดแวร์ VPN)

รายการ	ระยะเวลา	ค่าใช้จ่ายต่อปี	ราคารวม	รายละเอียด
ค่าบริการอินเทอร์เน็ต 256/256 Kbps	5		589,694	Broadband Satellite อินเทอร์เน็ต (ข้อมูลจาก CS Internet)
ค่าใช้จ่ายในการบำรุงรักษา บริหารจัดการ อุปกรณ์	5	43,500	217,500	คิดจาก 10% ของราคาอุปกรณ์
ค่าเสื่อมราคาอุปกรณ์	5	69,600	348,000	
รวมค่าใช้จ่ายรวม			1,155,194	

ตารางที่ 4.7 แสดงค่าใช้จ่ายในแต่ละปี (บาท) (ฮาร์ดแวร์ VPN)

ปีที่ X	ค่าบริการอินเทอร์เน็ต	ค่าเสื่อม	ค่าบำรุงรักษา	รวม
1	144,000	69,600	43,500	257,100
2	129,600	69,600	43,500	242,700
3	116,640	69,600	43,500	229,740
4	104,976	69,600	43,500	218,076
5	94,478	69,600	43,500	207,578
รวม	589,694	348,000	217,500	1,155,194

ตารางที่ 4.8 แสดงค่าใช้จ่ายและค่าเริ่มต้นโครงการตลอดเวลา 5 ปี (บาท) (ฮาร์ดแวร์)

รายการ	โครงการ
ลงทุนเริ่มแรก	435,000 + 77,000 = 512,000
ค่าใช้จ่าย	1,155,194
อายุ (ปี)	5
รวม	1,667,194

4.1.3 การประมาณการลงทุนเริ่มแรกของโครงการ (ซอร์ฟแวร์ VPN)

การประมาณการลงทุนในการลงทุนด้าน ซอร์ฟแวร์ VPN Server เพื่อทำหน้าที่ในการให้บริการเครือข่าย VPN ทั้งในแบบ SITE TO SITE และในแบบ REMOTE USERS

ราคาซอร์ฟแวร์ที่ต้องใช้ในการติดตั้งเครือข่าย VPN นั้นขึ้นอยู่กับความต้องการของผู้ใช้งานและความสามารถพิเศษในด้านต่าง ๆ ที่จะเข้ามามีผลกระทบต่อราคาของซอร์ฟแวร์แต่ละตัว แต่ในเทคโนโลยีปัจจุบันนั้นมีซอร์ฟแวร์ที่เป็น OPEN SOURCE ที่สามารถนำมาสร้างเครือข่าย VPN ได้แทนการใช้อุปกรณ์ที่เป็นที่ทำหน้าที่ให้บริการได้อย่างดีและไม่เสียค่าใช้จ่าย

ตารางที่ 4.9 แสดงราคาซอร์ฟแวร์และอุปกรณ์ที่ใช้เครือข่าย VPN (ซอร์ฟแวร์ VPN)

อุปกรณ์	จำนวน	ราคาต่อหน่วย/บาท	ราคาทั้งหมด	รายละเอียด
VPN Server Software	2	0	0	ใช้ในการติดตั้งที่สำนักงานฝั่งสมุทรปราการและที่สำนักงานประเทศสิงคโปร์
PC Server (LINUX)	5	25,000	125,000	
VPN Client (Notebook)	10	12,000	120,000	เพื่อให้ผู้บริหารระดับกลางและพนักงานที่ต้องทำงานนอกสถานที่เพื่อใช้งาน
VPN Client (Smart Phone)	3	20,000	60,000	เพื่อให้ผู้บริหารระดับสูงสามารถเรียกดูข้อมูลผู้บริหารจากที่ใดก็ได้ผ่านโทรศัพท์มือถือ

ตารางที่ 4.9 แสดงราคาซอร์ฟแวร์และอุปกรณ์ที่ใช้เครือข่าย VPN (ซอร์ฟแวร์ VPN) (ต่อ)

อุปกรณ์	จำนวน	ราคาต่อ หน่วย/บาท	ราคา ทั้งหมด	รายละเอียด
ค่าอุปกรณ์ Broadband อินเทอร์เน็ต MODEM	1	5,000	5,000	
ระบบสำรองไฟฟ้า	2	25,000	50,000	
รวมราคาอุปกรณ์			360,000	

สำหรับในส่วนของค่าใช้จ่ายในการเริ่มต้นระบบนั้นไม่มีความแตกต่างจากการเริ่มต้นระบบแบบฮาร์ดแวร์โดยมีเพิ่มเติมในส่วนของการฝึกอบรมผู้ดูแลรักษาระบบที่เพิ่มเข้ามาเป็นเงิน 12,000 บาท ทำให้ค่าใช้จ่ายในด้านการเริ่มต้นติดตั้งระบบเป็น 77,000 (ตาราง 4.2) + 12,000 = 89,000 บาท

รวมค่าใช้จ่ายเริ่มต้นทั้งหมดในการติดตั้งระบบเครือข่าย VPN (ซอร์ฟแวร์) 360,000 + 89,000 = 449,000 บาท

4.1.4 การประมาณรายการค่าใช้จ่ายในการดำเนินการและบำรุงรักษาเครือข่าย (Operation and Maintenance Expense) (ซอร์ฟแวร์ VPN)

การประมาณค่าใช้จ่ายในการดำเนินงานและการบำรุงรักษาเครือข่าย VPN (ซอร์ฟแวร์) นั้นเป็นการคำนวณหาค่าจ่ายที่เกิดขึ้นระหว่างดำเนินงานรวมถึงการคำนวณหาราคาค่าเสื่อมของอุปกรณ์แต่ละชิ้นของโครงการเพื่อให้เกิดเป็นค่าใช้จ่ายตามความเป็นจริงมากที่สุด

การคำนวณหาค่าเสื่อมอุปกรณ์และซอร์ฟแวร์จะทำการคำนวณค่าเสื่อมแบบเส้นตรง (Straight – Line Depreciation) เหมือนกับการคำนวณใน VPN ฮาร์ดแวร์ โดย

ตารางที่ 4.10 แสดงค่าเสื่อมอุปกรณ์เครือข่าย VPN (ซอร์ฟแวร์ VPN)

อุปกรณ์	ราคาทั้งหมด (P)	มูลค่าซาก (L)	อายุการใช้งาน (n)	ค่าเสื่อมราคาต่อปี
PC Server	125,000	25,000	5	20,000
VPN Client (Notebook)	120,000	24,000	5	19,200
VPN Client (Smart Phone)	60,000	12,000	5	9,600
ค่าอุปกรณ์ Broadband อินเทอร์เน็ต MODEM	5,000	1,000	5	800
ระบบสำรองไฟฟ้า	50,000	10,000	5	8,000
รวมราคาอุปกรณ์	360,000	72,000		57,600

ตารางที่ 4.11 แสดงราคาอุปกรณ์เมื่อสิ้นปีที่ X (ซอร์ฟแวร์ VPN)

ปีที่ X	มูลค่าอุปกรณ์เมื่อวันสิ้นปี X (บาท)	ค่าเสื่อมราคาเมื่อปีที่ X (บาท)
0	360,000	
1	284,000 – 57,600 = 239,400	57,600
2	239,400 – 57,600 = 193,800	57,600+ 57,600 = 115,200
3	193,800 – 57,600 = 148,200	115,200 + 57,600 = 172,800
4	148,200 – 57,600 = 102,600	172,800 + 57,600 = 230,400
5	102,600 – 57,600 = 57,000	230,400 + 57,600 = 288,000
		รวมค่าเสื่อม = 288,000

การคำนวณหาค่าบริการอินเทอร์เน็ตนั้นสามารถใช้ได้ในตารางที่ 4.5 โดยคิดเป็นค่าใช้จ่าย 589,694 บาท

ในการหาราคาค่าใช้จ่ายในระบบเครือข่าย VPN แบบ ซอร์ฟแวร์นั้นมีส่วนเพิ่มในการ Admin ระบบ PC Server ที่มาทำหน้าที่เป็น VPN Server เป็นเงิน 36,000 บาทต่อปี

ตารางที่ 4.12 แสดงราคาค่าใช้จ่ายตลอด 5 ปี (ซอร์ฟแวร์ VPN)

รายการ	ระยะเวลา	ค่าใช้จ่ายต่อปี	ราคารวม	รายละเอียด
ค่าบริการอินเทอร์เน็ต 256/256 Kbps	5		589,694	Broadband Satellite อินเทอร์เน็ต (ข้อมูลจาก CS Internet)
ค่าใช้จ่ายในการบำรุงรักษา บริหารจัดการ อุปกรณ์	5	36,000	180,000	คิดจาก 10% ของราคาอุปกรณ์
ค่าใช้จ่ายส่วนเพิ่มในการ Admin PC Server	5	36,000	180,000	PC Server Open Source
ค่าเสื่อมราคาอุปกรณ์	5	57,600	288,000	
รวมค่าใช้จ่ายรวม			1,237,694	

ตารางที่ 4.13 แสดงค่าใช้จ่ายในแต่ละปี (บาท)

ปีที่ X	ค่าบริการอินเทอร์เน็ต	ค่า Admin PC Server	ค่าเสื่อม	ค่าบำรุงรักษา	รวม
1	144,000	36,000	57,600	36,000	273,600
2	129,600	36,000	57,600	36,000	259,200
3	116,640	36,000	57,600	36,000	246,240
4	104,976	36,000	57,600	36,000	234,576
5	94,478	36,000	57,600	36,000	224,078
รวม	589,694	180,000	288,000	180,000	1,237,694

ตารางที่ 4.14 แสดงค่าใช้จ่ายและค่าเริ่มต้นโครงการตลอดเวลา 5 ปี (บาท)

รายการ	โครงการ
ลงทุนเริ่มแรก	360,000 + 89,000 = 449,000
ค่าใช้จ่าย	1,237,694
อายุ (ปี)	5
รวม	1,686,694

4.1.5 การประมาณการผลตอบแทนที่จะได้รับจากระบบ

ผลตอบแทนที่ได้จากการวางระบบเครือข่าย VPN นั้นสามารถแยกออกเป็นสองลักษณะคือผลตอบแทนที่สามารถคิดเป็นตัวเงิน และ ผลตอบแทนที่ไม่สามารถคิดเป็นตัวเงินได้

- **ผลตอบแทนที่สามารถคิดเป็นตัวเงินได้ (Tangible Benefit)** เป็นผลตอบแทนที่สามารถคำนวณออกมาเป็นตัวเงินได้และสามารถนำมาคำนวณกลับหาค่าผลตอบแทนการลงทุนได้

  - ลดค่าใช้จ่ายค่า Oversea Traveling สำหรับผู้ให้คำปรึกษาจากประเทศสิงคโปร์ได้ 60% ต่อปี คิดเป็นเงิน 5,000S$ เป็น 2,000S$ คำนวณเป็นเงินบาท 5,000 – 2,000 = 3,000 (24) = 72,000 บาทต่อปี
  - ลดค่าใช้จ่ายในการบำรุงรักษาระบบยามฉุกเฉิน โดยฝ่ายผู้ดูแลระบบสามารถทำงานได้จากทุก ๆ ที่ที่เครือข่ายอินเทอร์เน็ตเข้าถึงโดยประมาณการการเข้าทำงานในนอกเวลางานในทุกกรณีเป็น 4 ครั้งต่อเดือน คิดเป็น

    O อัตราค่าล่วงเวลา = 1.5 เท่า

    SD อัตราเงินเดือนของผู้ดูและระบบต่อวัน = 500 บาท

    T ค่าพาหนะในการทำงานต่อวัน = 300 บาท

    d จำนวนวันในแต่ละปี = 48 วัน

    ((O X SD) + T) X 48 = 50,400 บาทต่อปี
  - ค่าบริการระบบที่ได้จากสำนักงานสาขาต่างประเทศ
    - คำนวณราคาค่าบริการได้จาก ค่าใช้จ่ายตลอดโครงการ 5 ปี 1,237,694 โดยแบ่งค่าใช้จ่ายออกเป็น 3 สำนักงานเนื่องจากไม่สามารถคิดค่าใช้จ่ายกับทาง ประเทศสิงคโปร์ได้ จึงต้องแบ่งค่าใช้จ่ายเป็น 6,876 บาท ต่อสำนักงาน โดยคิดกับเป็นสกุลเงินสิงคโปร์ 6,876/24 = 286S$ และได้คิดมูลการให้บริการเพิ่มอีกประมาณ 5 % จึงคิดเป็นค่าบริการ 300S$ ต่อสำนักงาน
    - ประเทศจีน 300S$ ต่อเดือน = 300 X 24 X 12 = 86,400 บาทต่อปี
    - ประเทศอินโดนีเซีย 300S$ ต่อเดือน = 300 X 24 X 12 = 86,400 บาทต่อปี
    - ประเทศมาเลเซีย 300S$ ต่อเดือน = 300 X 24 X 12 = 86,400 บาทต่อปี
    - รวมทั้งหมดเป็นเงิน 86,400 X 3 = 259,200 บาทต่อปี

หมายเหตุ : S$ = 24 บาท

ตารางที่ 4.15 แสดงผลตอบแทนที่ได้ใน 1 ปี (บาท)

รายการ	จำนวน
ลดค่าใช้จ่ายในการบริหาร	72,000
ลดค่าใช้จ่ายในกรณีฉุกเฉิน	50,400
ค่าบริการระบบ	259,200
รวม	381,600

4.1.6 การประมาณการจุดคุ้มทุนโครงการ

ต่อไปนี้เป็นคำอธิบายตารางการคำนวณระยะเวลาคุ้มทุนสำหรับโครงการสำหรับเครือข่ายทางเลือกทั้ง 2 ประเภท โดยรายได้นี้ได้จากการประมาณการรายได้ในขอ 4.1.5 โดยทำการคิดดอกเบี้ยในอัตรา 1% ต่อเดือน

ตารางที่ 4.16 แสดงค่ารายได้คิดตามสัดส่วนกับต้นทุนและค่าใช้จ่าย (บาท)

แบบ	ต้นทุนคงที่	ค่าดำเนินการและบำรุงรักษา	อัตราดอกเบี้ย %	รายได้	ระยะเวลาคุ้มทุน
ฮาร์ดแวร์ VPN	512,000	187,500	12	381,600	3 ปี 9 เดือน
ซอร์ฟแวร์ VPN	449,000	216,000	12	381,600	4 ปี

ตารางที่ 4.17 แสดงการคำนวณจุดคุ้มทุนโครงการ ฮาร์ดแวร์ VPN (บาท)

ปี	ต้นทุนคงที่	ยอดยกมา	อัตราดอกเบี้ย %	ดอกเบี้ยจ่าย	O&M	หนี้สิน	รายได้	หนี้สินสุทธิ
1	512,000	512,000	12	61,440	187,500	760,940	381,600	379,340
2		379,340	12	45,521	173,100	597,961	381,600	216,361
3		216,361	12	25,963	160,140	402,464	381,600	20,864
4		20,864	12	2,504	148,476	171,844	381,600	-209,756
5		-209,756	12	0	137,978	-71,778	381,600	-453,378

การคำนวณจุดคุ้มทุนของโครงการ VPN ฮาร์ดแวร์ นั้นใช้การคำนวณเป็นรายปี โดยตั้งต้นที่ต้นทุนคงที่ 512,000 ซึ่งเป็นค่าซื้ออุปกรณ์ที่ทำการลงทุนในครั้งแรก โดยกำหนดอัตรา

ดอกเบี้ย 12 % ต่อปี ค่าบำรุงรักษาและค่าดำเนินงานในแต่ละปีคิดโดยนำเอา ค่าบริการอินเทอร์เน็ต (แปรผันไปตามปี) + ค่าบำรุงรักษาอุปกรณ์ 43,500 บาทต่อปี

จากตาราง 4.17 ทำให้ทราบได้ว่าหลังการดำเนินการโครงการไป 3 ปีจะมีหนี้สินเหลือเพียง 20,864 บาท และจบการดำเนินการในรอบปีที่ 4 จะมีกำไรหลังจากหักค่าใช้จ่ายการดำเนินการแล้ว 209,756 บาท และเมื่อหมดอายุอุปกรณ์ทำให้มีกำไรสุทธิจากการดำเนินงานทั้งหมด 5 ปี ที่ 453,378 บาท

จุดคุ้มทุนโครงการอยู่ที่ 3.81 ปี หรือเท่ากับ 3 ปี 9 เดือน โดยคำนวณได้จาก

FC ต้นทุนคงที่

I ดอกเบี้ยจ่ายทั้งหมดตลอดอายุโครงการ

OM ค่าใช้จ่ายดำเนินงานตลอดอายุโครงการ

IC รายได้จากการดำเนินโครงการตลอดอายุโครงการ

Y อายุโครงการ

$$\text{จุดคุ้มทน} = \left(FC + I + OM/IC\right) * Y$$

$$= \left(512{,}000 + 135{,}428 + 807{,}194/1{,}908{,}000\right) * 5$$

$$= 3.81 \text{ ปี}$$

ตารางที่ 4.18 แสดงการคำนวณจุดคุ้มทุนโครงการ ซอร์ฟแวร์ VPN (บาท)

ปี	ต้นทุนคงที่	ยอดยกมา	อัตราดอกเบี้ย %	ดอกเบี้ยจ่าย	O&M	หนี้สิน	รายได้	หนี้สินสุทธิ
1	449,000	449,000	12	53,880	216,000	718,880	381,600	337,280
2		337,280	12	40,474	201,600	579,354	381,600	197,754
3		197,754	12	23,730	188,640	410,124	381,600	28,524
4		28,524	12	3,423	176,976	208,923	381,600	-172,677
5		-172,677	12	0	166,478	-6,199	381,600	-387,799

การคำนวณจุดคุ้มทุนของโครงการ VPN ซอร์ฟแวร์ นั้นใช้การคำนวณเป็นรายปี โดยตั้งต้นที่ต้นทุนคงที่ 449,000 ซึ่งเป็นค่าซื้ออุปกรณ์ที่ทำการลงทุนในครั้งแรก โดยกำหนดอัตรา

ดอกเบี้ย 12 % ต่อปี ค่าบำรุงรักษาและค่าดำเนินงานในแต่ละปีคิดโดยนำเอา ค่าบริการอินเทอร์เน็ต (แปรผันไปตามปี) + ค่าบำรุงรักษาอุปกรณ์ ค่าผู้ดูแลระบบ 72,000 บาทต่อปี

จากตาราง 4.18 ทำให้ทราบได้ว่าหลังการดำเนินการโครงการไป 3 ปีจะมีหนี้สินเหลือเพียง 28,524 บาท และจบการดำเนินการในรอบปีที่ 4 จะมีกำไรหลังจากหักค่าใช้จ่ายการดำเนินการแล้ว 172,667 บาท และเมื่อหมดอายุอุปกรณ์ทำให้มีกำไรสุทธิจากการดำเนินงานทั้งหมด 5 ปี ที่ 387,779 บาท

จุดคุ้มทุนโครงการอยู่ที่ 3.98 ปี หรือประมาณ 4 ปี โดยคำนวณได้จาก

FC ต้นทุนคงที่

I ดอกเบี้ยจ่ายทั้งหมดตลอดอายุโครงการ

OM ค่าใช้จ่ายดำเนินงานตลอดอายุโครงการ

IC รายได้จากการดำเนินโครงการตลอดอายุโครงการ

Y อายุโครงการ

$$\text{จุดคุ้มทน} = \left(FC + I + OM/IC\right) * Y$$

$$= \left(449{,}000 + 121{,}507 + 949{,}694/1{,}908{,}000\right) * 5$$

$$= 3.98 \text{ ปี}$$

4.1.7 การคำนวณเปรียบเทียบค่าใช้จ่ายโครงการที่มีอายุเท่ากันด้วยวิธีมูลค่าปัจจุบัน (Present Worth-Comparison of Equal-Lived Alternatives)

การนำเอาการเปรียบเทียบโครงการแบบนำมูลค่าปัจจุบันมาใช้โดยการเปลี่ยนแปลงค่าของเงินในช่วงเวลาต่าง ๆ มาที่ปีปัจจุบันแล้วทำการเปรียบเทียบกันว่าโครงการใดใช้ค่าใช้จ่ายต่ำสุดหรือได้กำไรสูงสุดจึงเลือกโครงการนั้น

ตารางที่ 4.19 แสดงค่าใช้จ่ายเปรียบเทียบสองโครงการ

รายการ	VPN ฮาร์ดแวร์ (A)	VPN ซอร์ฟแวร์ (B)
ค่าลงทุนเริ่มต้น	512,000	449,000
ค่าใช้จ่ายดำเนินงานปีที่ 1	187,500	216,000
ค่าใช้จ่ายดำเนินงานปีที่ 2	173,100	201,600
ค่าใช้จ่ายดำเนินงานปีที่ 3	160,140	188,640
ค่าใช้จ่ายดำเนินงานปีที่ 4	148,476	176,976
ค่าใช้จ่ายดำเนินงานปีที่ 5	137,978	166,478
มูลค่าซาก	87,000	72,000
อายุโครงการ	5	5

ทำการแปลงมูลค่าของเงินที่ช่วงเวลาต่าง ๆ ไปที่ช่วงเวลา 0 แล้วหักลบกันเป็นรายจ่ายเทียบเท่าเงินลงทุน ณ ปีปัจจุบันในการคำนวณนี้จำเป็นต้องใช้การคำนวณที่มีค่าใช้จ่ายแต่ละปีคงที่จึงจำเป็นต้องทำการหาค่าเฉลี่ยของค่าใช้จ่ายการดำเนินงานของทุกปี เป็น

A(Average) = (187,500 + 173,100 + 160,140 + 148,476 + 137,978) = 161,439 บาท

B(Average) = (216,000 + 201,600 + 188,640 + 176,976 + 166,478) = 189,393 บาท

FC	ต้นทุนคงที่
AVG(OM)	ค่าใช้จ่ายดำเนินงานเฉลี่ย
O	มูลค่าซาก
Y	อายุโครงการ
I	อัตราดอกเบี้ย

มูลค่าปัจจุบันของโครงการ VPN ฮาร์ดแวร์ A (PW_A)

PW_A = [-FC - AVG(OM)(P/A,I,Y) + O(P/F,I,Y)]

= [-512,000 – 161,439(3.605) + 87,000(0.5674)]

= - 1,044,623.8 บาท

มูลค่าปัจจุบันของโครงการ VPN ซอร์ฟแวร์ B (PW_B)

PW_B = [-FC - AVG(OM)(P/A,I,Y) + O(P/F,I,Y)]

= [-449,000 – 189,393(3.605) + 72,000(0.5674)]

= - 1,090,908.9 บาท

การลงทุนในการวางระบบ VPN ฮาร์ดแวร์ นั้นมีการเสียค่าใช้จ่ายที่ถูกกว่าเมื่อเปรียบเทียบกับการวางระบบแบบ ซอร์ฟแวร์

หมายเหตุ : P/A ดูจากตารางเปรียบเทียบในภาคผนวก ข

P/F ดูจากตารางเปรียบเทียบในภาคผนวก ข

4.1.8 การคำนวณหาผลตอบแทนจากสินทรัพย์ (Return on Investment)

หาได้โดยนำกำไรสุทธิหลังจากหักภาษี หารด้วยสินทรัพย์ทั้งหมด ผลตอบแทนจากสินทรัพย์นี้บางที่ก็นิยมเรียกว่า ผลตอบแทนจากการลงทุน (Return on investment – ROI)

- การคำนวณหาผลตอบแทนจากสินทรัพย์ในโครงการ ฮาร์ดแวร์ VPN

รายรับของโครงการหลังจากหักค่าใช้จ่าย (VPN ฮาร์ดแวร์)		
รายรับจากการดำเนินงาน		381,000
รายจ่ายการดำเนินงาน		
ค่าบริการอินเทอร์เน็ต	144,000	
ค่าบำรุงรักษาระบบ	43,500	
ค่าเสื่อราคาทรัพย์สิน	69,600	257,100
กำไรจากการดำเนินการ		123,900
ดอกเบี้ย		61,440
กำไรสุทธิหลังหักดอกเบี้ย		62,460

$$ROI = \frac{\text{Net income}}{\text{Total asset}}$$

$$= \frac{62{,}460 \times 100}{512{,}000}$$

$$= 12.19\ \%$$

- การคำนวณหาผลตอบแทนจากสินทรัพย์ในโครงการ ซอร์ฟแวร์ VPN

รายรับของโครงการหลังจากหักค่าใช้จ่าย (VPN ซอร์ฟแวร์)		
รายรับจากการดำเนินงาน		381,000
รายจ่ายการดำเนินงาน		
ค่าบริการอินเทอร์เน็ต	144,000	
ค่าบำรุงรักษาระบบ	36,000	
ค่าบริการ PC Server	36,000	
ค่าเสื่อราคาทรัพย์สิน	57,600	273,600
กำไรจากการดำเนินการ		107,400
ดอกเบี้ย		53,880
กำไรสุทธิหลังหักดอกเบี้ย		53,520

$$ROI = \frac{\text{Net income}}{\text{Total asset}}$$

$$= \frac{53{,}520 \times 100}{449{,}000}$$

$$= 11.92\ \%$$

4.1.9 การคำนวณหาอัตราส่วนผสประโยชน์การลงทุน(Benefit cost Ratio : B/C)

ผลประโยชน์ที่ได้จากการลงทุน (Benefit cost Ratio : B/C) ถ้าอัตราส่วนที่ได้มากกว่า 1 แสดงว่าควรตัดสินใจเลือกโครงการนั้น ๆ ซึ่งเป็นเกณฑ์ต่ำสุดที่ยอบรับได้ ซึ่งถ้าอัตราส่วนออกมาน้อยกว่า 1 ก็แสดงว่าโครงการนั้นไม่น่าลงทุน ในการวิเคราะห์อัตราส่วนของผลประโยชน์ต่อเงินลงทุนนั้นจริง ๆ แล้วมูลค่าของเงินจะอยู่ที่ช่วงเวลาในการลงทุนที่แตกต่างกัน จึงจำเป็นต้องทำการแปลงค่าของเงินลงทุนที่อยู่ตามช่วงเวลาต่าง ๆ มาอยู่ที่จุดเดียวกัน ซึ่งในที่นี้ได้ทำการแปลงเป็นมูลค่าปัจจุบันด้วยสมการด้านล่าง

สูตรปรับช่วงเวลาให้เป็นปัจจุบัน

$$PV = \frac{T}{(1+d)^{m}}$$

เมื่อ PV = Present value

T = มูลค่าของสิ่งใดๆ ในช่วงเวลาใดเวลาหนึ่ง

d = ดอกเบี้ย

สูตรการคำนวณหาอัตราส่วนผลประโยชน์การลงทุน

$$\frac{B}{C}\text{ratio} = \frac{PV\ of\ benefit}{PV\ of\ cost}$$

ตารางที่ 4.20 ค่าใช้จ่ายและผลตอบแทนในค่าปัจจุบัน ฮาร์ดแวร์ VPN

ปีที่	ค่าลงทุน	ค่าใช้จ่ายในการดำเนินการ	ผลตอบแทน	PV ค่าใช้จ่าย	PV ผลตอบแทน	ผลตอบแทนสุทธิ (NPV)
อัตราดอกเบี้ย			12%	-	-	-
1	512,000	-	-	457,142.86	-	-
1	-	187,500	381,000	167,410.71	340,178.57	172,767.86
2	-	173,100	381,000	154,553.57	303,730.87	149,177.30
3	-	160,140	381,000	142,982.14	271,188.28	128,206.14
4	-	148,476	381,000	132,567.86	242,132.39	109,564.53
5	-	137,978	381,000	123,194.64	216,189.63	92,994.99
	รวม	807,194	1,905,000	1,177,851.78	1,373,419.74	652,710.82

พิจารณาจากตารางข้างต้น ต้นทุน จะมี 2 ส่วน ค่าลงทุน กับ ค่าใช้จ่ายในการดำเนินการ มีผลตอบแทน ค่าลงทุนลงทุนในปีที่ 1 512,000 บาท เป็นค่าอุปกรณ์และค่าติดตั้งระบบ และมีผล ตอบแทนเกิดขึ้น ตั้งแต่ปีแรกและในปีต่อ ๆ ไป ก็จะมีทั้งค่าใช้จ่ายในการดำ เนินการและผลตอบแทนต่อเนื่องกันทุกปี การคำนวณเพื่อหาค่าใช่จ่ายและผลตอบแทนจริงนั้นต้องทำการแปลงค่าของเงินและเวลาทั้งหมดให้เป็นเวลาเดียวกันจึงทำให้ต้องใช้สูตรการปรับช่วงเวลาให้เป็นปัจจุบันเข้ามาช่วย

ตัวอย่าง การคำนวณค่าปัจจุบันของค่าลงทุนเริ่มต้นของ VPN ฮาร์ดแวร์

$$PV = \frac{T}{(1+d)^m}$$

$$= \frac{512,000}{(1+0.12)}$$

ค่าลงทุนเริ่มต้น = 457,142.86 บาท

$$\frac{B}{C}\text{ratio} = \frac{\text{PV of benefit}}{\text{PV of cost}}$$

$$= \frac{1,373,419}{1,177,851}$$

$$= 1.16$$

จากสมการข้าต้นได้ อัตราส่วนผลประโยชน์การลงทุนเท่ากับ 1.16 ซึ่งเป็นผลดีกับการลงทุนในโครงการ VPN ฮาร์ดแวร์

ตารางที่ 4.21 ค่าใช้จ่ายและผลตอบแทนในค่าปัจจุบัน ซอร์ฟแวร์ VPN

ปีที่	ค่าลงทุน	ค่าใช้จ่ายในการดำเนินการ	ผลตอบแทน	PV ค่าใช้จ่าย	PV ผลตอบแทน	ผลตอบแทนสุทธิ (NPV)
อัตราดอกเบี้ย			12%	-	-	-
1	449,000	-	-	400,892.86	-	-
1	-	216,000	381,000	192,857.14	340,178.57	147,321.43
2	-	201,600	381,000	180,000.00	303,730.87	123,730.87
3	-	188,640	381,000	168,428.57	271,188.28	102,759.71
4	-	176,976	381,000	158,014.29	242,132.39	84,118.10
5	-	166,478	381,000	148,641.07	216,189.63	67,548.56
	รวม	807,194	1,905,000	1,248,833.93	1,373,419.74	525,478.67

ตัวอย่างการคำนวณค่าปัจจุบันของค่าลงทุนเริ่มต้นของ VPN ซอร์ฟแวร์

$$PV = \frac{T}{(1+d)^{m}}$$

$$= \frac{449,000}{(1+0.12)}$$

ค่าลงทุนเริ่มต้น = 400,892.86 บาท

$$\frac{B}{C}\text{ratio} = \frac{\text{PV of benefit}}{\text{PV of cost}}$$

$$= \frac{1,373,419}{1,248,833}$$

$$= 1.10$$

จากสมการข้าต้นได้ อัตราส่วนผลประโยชน์การลงทุนเท่ากับ 1.10 ซึ่งเป็นผลดีกับการลงทุนในโครงการ VPN ซอร์ฟแวร์

4.1.10 การคำนวณหาอัตราผลตอบแทนภายใน(Internal Rate Return : IRR)

IRR คืออัตราผลตอบแทนภายใน ทำการหาเพื่อให้ทราบว่ามีความคุ้มกับดอกเบี้ยหรือไม่ ถ้าสูงกว่ากว่าดอกเบี้ยโครงการสามารถกู้มาลงทุนได้ โดยปกติเราต้องทราบว่าโครงการที่เราจะเลือกจะได้ผลตอบแทนเท่าใดเมื่อเปรียบเทียบกับอัตราดอกเบี้ยเงินฝากหรือเงินกู้ ซึ่งตามหลักแล้วอัตราผลตอบแทนต้องสูงกว่าเงินฝากในกรณีที่เราใช้เงินส่วนตัว และต้องสูงกว่าเงินกู้สำหรับในกรณีที่ต้องใช้เงินกู้จากธนาคาร

สมการการคำนวณหา IRR

$$\text{IRR} = \text{อัตราส่วนลดตัวต่ำ} + \left(\text{ผลต่างระหว่างอัตราส่วนลดทั้งสอง} \times \frac{\text{NPV ที่ใช้อัตราส่วนลดตัวต่ำ}}{\text{ผลต่างของNPV ที่ใช้อัตราส่วนลดทั้งสอง}} \right)$$

กำหนดอัตราส่วนลด ตัวต่ำ = 10% ตัวสูง =15%

ตารางที่ 4.22 แสดงกระแสเงินสดของโครงการ ฮาร์ดแวร์ VPN

ปีที่	ค่าลงทุน	ค่าใช้จ่ายในการดำเนินการ	ผลตอบแทน	กระแสเงินสด	NPV of cash flow	
					Discount 10%	Discount 15%
1	512,000	-	-	-512,000	-465,454.55	-445,217.39
1	-	187,500	381,000	193,500	175,909.09	168,260.87
2	-	173,100	381,000	207,900	171,818.18	157,202.27
3	-	160,140	381,000	220,860	165,935.39	145,219.04
4	-	148,476	381,000	232,524	158,817.02	132,946.35
5	-	137,978	381,000	243,022	150,897.54	120,824.88
รวม	512,000	807,194	1,905,000		357,922.68	279,236.02

IRR ของโครงการ VPN ฮาร์ดแวร์

$$\text{IRR} = \text{อัตราส่วนลดตัวต่ำ} + \left(\text{ผลต่างระหว่างอัตราส่วนลดทั้งสอง} \times \frac{\text{NPV ที่ใช้อัตราส่วนลดตัวต่ำ}}{\text{ผลต่างของ NPV ที่ใช้อัตราส่วนลดทั้งสอง}} \right)$$

$$\text{IRR} = 10 + \left\{ (15-10) \times \frac{357,922.68}{357,922.68 - 279,236.02} \right\}$$

$$\text{IRR} = 10 + \{(15-10) \times 4.548\}$$

$$\text{IRR} = 32.74$$

ตารางที่ 4.23 แสดงกระแสเงินสดของโครงการ ซอร์ฟแวร์ VPN

ปีที่	ค่าลงทุน	ค่าใช้จ่ายในการดำเนินการ	ผลตอบแทน	กระแสเงินสด	NPV of cash flow	
					Discount 10%	Discount 15%
1	449,000	-	-	-449,000	-408,181.82	-390,434.78
1	-	216,000	381,000	165,000	150,000.00	143,478.26
2	-	201,600	381,000	179,400	148,264.46	135,652.17
3	-	188,640	381,000	192,360	144,522.92	126,479.82
4	-	176,976	381,000	204,024	139,351.14	116,651.38
5	-	166,478	381,000	214,522	133,201.28	106,655.35
รวม	449,000	949,694	1,905,000		307,157.98	238,482.21

IRR ของโครงการ VPN ซอร์ฟแวร์

$$\text{IRR} = \text{อัตราส่วนลดตัวต่ำ} + \left(\text{ผลต่างระหว่างอัตราส่วนลดทั้งสอง} \times \frac{\text{NPV ที่ใช้อัตราส่วนลดตัวต่ำ}}{\text{ผลต่างของ NPV ที่ใช้อัตราส่วนลดทั้งสอง}} \right)$$

$$\text{IRR} = 10 + \left\{ (15-10) \times \frac{307,157.98}{307,157.98 - 238,482.21} \right\}$$

$$= 10 + \{5 \text{ X } 4.472\}$$

$$= 32.36$$

4.1.11 การวิเคราะห์ผลจากการคำนวณค่าการเปรียบเทียบการลงทุนทั้ง 2 แบบ

จากที่ได้ทำการคำนวณหาค่าเปรียบเทียบเพื่อนำมาใช้วิเคราะห์โครงการทั้งสองทำให้ได้ค่าเปรียบเทียบในหลาย ๆ ด้านเพื่อนำมาวิเคราะห์หาความเป็นไปได้ในเชิงเศรษฐศาสตร์ของทั้งสองโครงการ และนำมาวิเคราะห์หาโครงการที่คุ้มค่าที่สุดในการดำเนินงานเพื่อให้ได้ผลตอบแทนสูงสุดและมีผลกระทบน้อยที่สุดต่อการลงทุน

ตารางที่ 4.24 แสดงการเปรียบเทียบโครงการทั้ง 2 แบบเพื่อวิเคราะห์ในการตัดสินใจ

	รายการ	ฮาร์ดแวร์ VPN	ซอร์ฟแวร์ VPN	ที่มา
1	ค่าลงทุนเริ่มแรก	512,000	449,000	
2	ค่าใช้จ่ายตลอดโครงการระยะเวลาโครงการ (ค่าเงินปัจจุบัน)	1,044,623.8 บาท	1,090,908.9 บาท	4.1.7
3	ระยะเวลาคืนทุน	3.81 ปี	3.98 ปี	4.1.6
4	อัตราผลตอบแทนการลงทุน (B/C Ratio)	1.16 เท่า	1.10 เท่า	4.1.9
5	อัตราส่วนผลตอบแทนต่อสินทรัพย์ (ROI)	12.19%	11.92%	4.1.8
6	อัตราส่วนผลตอบแทนภายใน (IRR)	32.74%	32.36%	4.1.10
7	ผลตอบแทนสุทธิ (NPV)	652,710.82 บาท	525,478.67 บาท	4.1.9

จากตาราง 4.22 เมื่อพิจารณาถึงต้นทุนเริ่มแรก และค่าใช้จ่ายในการดำเนินงานในแต่ละรอบปีซึ่งได้ทำการปรับค่าให้เป็นค่าเงินในรอบเวลาเดียวกันทำให้เราทราบว่าการวางระบบ VPN ที่ใช้ ฮาร์ดแวร์ในการทำเป็น VPN Gateway Server นั้นมีค่าใช้จ่ายในการเริ่มต้นสูงกว่าในแบบที่เป็นซอร์ฟแวร์ ค่ามีค่าใช้จ่ายในการดำเนินงานที่ต่ำกว่า เมื่อเปรียบเทียบปัจจัยทั้งสองแล้วค่อนข้างมีความใกล้เคียงกันจึงจำเป็นต้อนำเอาค่าการเปรียบเทียบอื่น ๆ มาคำนึงถึงด้วยในที่นี้มีการคำนวณออกมา อีก 4 แบบคือ การวิเคราะห์หาระยะเวลาคืนทุน อัตราผลตอบแทนการลงทุน (B/C Ratio) อัตราส่วนผลตอบแทนจากสินทรัพย์ (ROI) และอัตราส่วนผลตอบแทนภายใน (IRR) ซึ่งในค่าแต่ละค่านั้นมีความหมายแตกต่างกันในการวิเคราะห์แต่สามารถนำมาสรุปเพื่อเปรียบเทียบโครงการทั้งสองได้ดังนี้

การคำนวณหาระยะเวลาคืนทุน(PAYBACK Period) จากตาราง 4.16 ได้ทำการคำนวณออกมาว่าการวางระบบแบบ ฮาร์ดแวร์นั้นมีระยะเวลาการคืนทุน 3 ปี 9 เดือน ซึ่งเร็วกว่าในแบบที่เป็นซอร์ฟแวร์ที่มีระยะเวลาการคืนทุนที่ช้ากว่าประมาณ 3 เดือน หรือ 4 ปี ทำให้หากเราลงทุนที่โครงการ ฮาร์ดแวร์จะมีระยะเวลาในการทำกำไรตลอดอายุการทำงานของระบบได้มากกว่าในแบบที่เป็น ซอร์ฟแวร์

การคำนวณหาอัตราผลตอบแทนในการลงทุน(B/C Ratio) นั้นทั้งสองโครงการนั้นมีอัตราผลตอบแทนต่อการลงทุนมากกว่า 1 แสดงว่าการลงทุนของโครงการทั้งสองนั้นมีผลตอบแทนที่ดีกว่าการนำเงินลงทุนไปฝากธนาคารโดยทั้งสองโครงการมีอัตราส่วนเท่ากับ 1.44 และ 1.36 เท่าตามลำดับแต่ผลตอบแทนที่ได้จากโครงการ VPN ฮาร์ดแวร์นั้นมากกว่า VPN ซอร์ฟแวร์อยู่ประมาณ 1.16/1.10 = 1.054 เท่า หรือประมาณ 5.4 % ซึ่งเมื่อผลตอบแทนมากกว่าซึ่ง

ถึงแม้ต้องลงทุนมากกว่าแต่ก็ได้ผลตอบแทนในอัตราส่วนที่มากกว่าจึงน่าจะลงทุนในการวางระบบด้วย VPN ฮาร์ดแวร์

ความสามารถในการให้ผลตอบแทนที่คำนวณออกมาเป็นกำไรสุทธิ (ROI) เมื่อเทียบกับปริมาณ สินทรัพย์อยู่ที่ประมาณ 12.19% และ 11.92% ตามลำดับแสดงว่าโครงการทั้งสองโครงการนั้นมีความสามารถในการทำกำไรที่ดีทั้งสองโครงการโดยที่ แต่โครงการแรกนั้นให้ผลตอบแทนที่ดีกว่าจึงมีความเหมาะสมมากกว่าในการลงทุน

จากการคำนวณผลตอบแทนสุทธิหลังจากคำนวณด้วยค่าเงินปัจจุบัน(NPV) แล้วจะเห็นได้ว่าโครงการ VPN ฮาร์ดแวร์นั้นให้ผลตอบแทนที่มากกว่าโครงการ VPN ซอร์ฟแวร์ เมื่อครบอายุโครงการแล้วถึง 652,710.82 - 525,478.67 = 127,232.15 บาท ซึ่งทำให้เห็นได้ว่าโครงการแรกนั้นให้ผลตอบแทนที่ดีกว่าจึงมีความน่าลงทุนมากกว่า

4.2 ผลตอบแทนที่ไม่สามารถนำมาคำนวณเป็นเงินได้ (Intangible Benefit)

นอกจากผลตอบแทนที่ได้จากการคำนวณในข้อ 4.1.2 ถึง 4.1.11 แล้ว หลังจากการวางระบบ ยังได้ผลตอบแทนจากระบบที่ไม่สามารถนำมาคำนวณเป็นเงินได้อีก เช่น

- การเพิ่มช่องทางการส่งถ่ายข้อมูลที่เป็นความลับให้กับสำนักงานแต่ละสำนักงาน
- เพิ่มความสามารถในกาดูแลรักษาระบบปัจจุบันผ่านเครือข่ายอินเทอร์เน็ตได้อย่างปลอดภัย
- เพิ่มช่องทางการสื่อสารระหว่างเครือข่ายปัจจุบันกับผู้บริหารได้ผ่านทางอุปกรณ์ไร้สาย เช่น โทรศัพท์มือถือ
- เพิ่มช่องทางในการรับส่งข้อมูลให้พนักงานที่ปฏิบัติงานนอกสถานที่
- เป็นแผนต่อเนื่องในการรวมระบบทั้งหมดให้เป็นไปในแนวทางเดียวกันและตรวจสอบได้ผ่านเครือข่ายออนไลน์

บทที่ 5
บทสรุป

จากการศึกษาความเป็นไปได้ในการนำเอาเครือข่าย VPN (VIRTUAL PRIVATE NETWORK) เข้ามาใช้ใน บริษัทฯ ได้แสดงให้เห็นถึงการศึกษารูปแบบต่าง ๆ ของเครือข่าย VPN และแบบใดเหมาะสมสำหรับบริษัทฯมากที่สุด โดยได้อาศัยการวิเคราะห์ความเป็นไปได้จากปัจจัยหลาย ด้าน เช่น การคำนวณค่าลงทุนเริ่มแรก , ค่าใช้จ่ายในการดำเนินงาน , จุดคุ้มทุนของแต่ละโครงการ ,อัตราผลตอบแทนต่อทรัพย์สิน, อัตราผลตอบแทนต่อการลงทุน, ตลอดจนผลตอบแทนตลอดโครงการ โดยได้แสดงให้เห็นตลอดอายุโครงการที่กำหนดไว้ตามอายุของอุปกรณ์ที่ลงทุนแล้วได้นำมาวิเคราะห์หาปัจจัยสนับสนุนการตัดสินใจเลือกโครงการที่ถูกต้อง

5.1 การเลือกรูปแบบเครือข่าย VPN

ในการศึกษาพบว่าเครือข่าย VPN แต่ละรูปแบบนั้นมีความเหมาะสมกับการใช้งานที่แตกต่างกันแต่ในบริษัทฯนั้นมีความเหมาะสมในการใช้งาน VPN เป็น 2 แบบ คือการใช้งานเครือข่ายในแบบที่มีการทำอุโมงค์ที่สองฝั่งที่เป็นเครื่องแม่ข่ายหรือที่เป็นอุปกรณ์ GATEWAY หรือที่เรียกว่าแบบ GATEWAY TO GATEWAY เพื่อให้บริการข้อมูลข่าวสารสนเทศแก่ผู้บริหารที่จำเป็นต้องเดินทางไปในสาขาต่าง ๆ ที่อยู่ต่างประเทศ และในรูปแบบที่มีการทำอุโมงค์ที่ฝั่งของอุปกรณ์กับอุปกรณ์หรือเครื่องที่เป็นผู้ใช้สุดท้าย หรือที่เรียกว่าแบบ GATEWAY TO CLIENT เพื่อให้บริการด้านสารสนเทศแก้บุคลากรที่ต้องเดินทางไปทำงานนอกสถานที่

โดยหลังจากที่ได้ทำการเลือกรูปแบบของเครือข่าย VPN ที่จะทำการติดตั้งแล้วก็ได้ทำการศึกษาเกี่ยวกับวิธีการในการติดตั้งเครือข่าย VPN ซึ่งสามารถทำได้ใน 2 วิธีคือการใช้งานอุปกรณ์ที่มีความสามารถในการทำอุโมงค์ VPN (TUNNELING) หรือการติดตั้งเครื่องแม่ข่ายแล้วทำการติดตั้งซอร์ฟแวร์ที่มีความสามารถในการทำอุโมงค์ VPN (TUNNELING) ทำให้ได้ 2 แนวทางเลือกในการนำมาเพื่อวิเคราะห์หาแนวทางการวางระบบ VPN ที่มีผลให้สามารถใช้งานได้จริงและคุ้มค่าต่อการลงทุนที่สุด

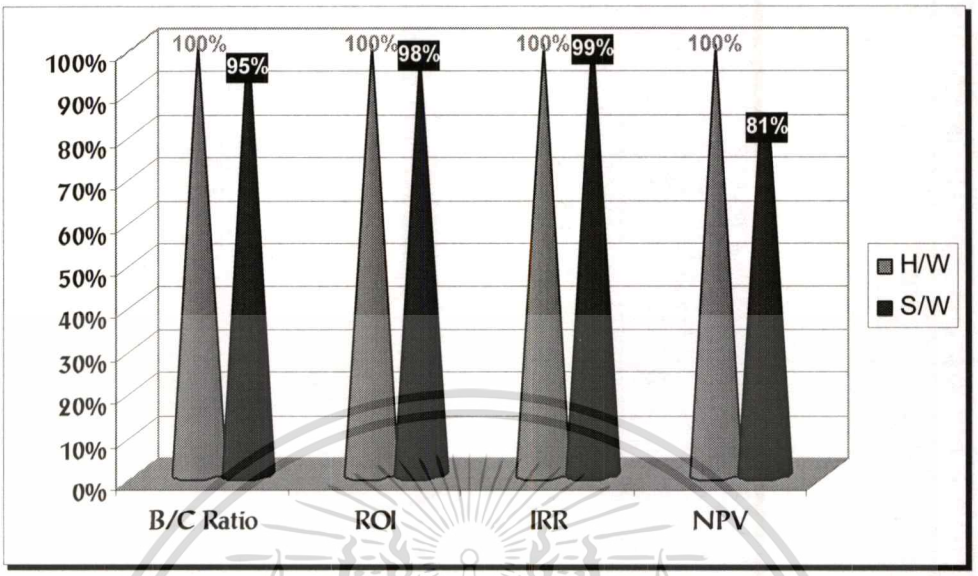
5.2 ปัจจัยที่นำมาวิเคราะห์

ปัจจัยที่นำมาวิเคราะห์ทางเลือกในการวางระบบเครือข่าย VPN นั้นได้ใช้ปัจจัยทั้งหมด 7 ปัจจัยตามตารางที่ 4.22 อันได้แก่ ค่าลงทุนเริ่มต้น(CONSTRUCTION COST), ค่าดำเนินการและบำรุงรักษา (OPERATION AND MAINTENANCE), ผลตอบแทน NPV(NET PROFIT PRESENT VALUE),อัตราผลตอบแทนต่อทรัพย์สิน (ROI), อัตราผลตอบแทนการลงทุน (B/C RATIO), ระยะเวลาคืนทุน (PAYBACK PERIOD), อัตราผลตอบแทนภายใน (IRR) จากการศึกษาวิเคราะห์โครงการจากปัจจัยทั้ง 7 แล้วจะได้ผลไปในแนวทางเดียวกันคือโครงการการวางระบบ VPN แบบที่ใช้ ฮาร์ดแวร์เป็นตัวทำอุโมงค์ VPN นั้นให้ผลประโยชน์ที่มากกว่า และเสี่ยงต่อการเปลี่ยนแปลงของเงินลงทุน และดอกเบี้ยน้อยกว่าในแบบที่ใช้ ซอร์ฟแวร์ทำอุโมงค์ VPN

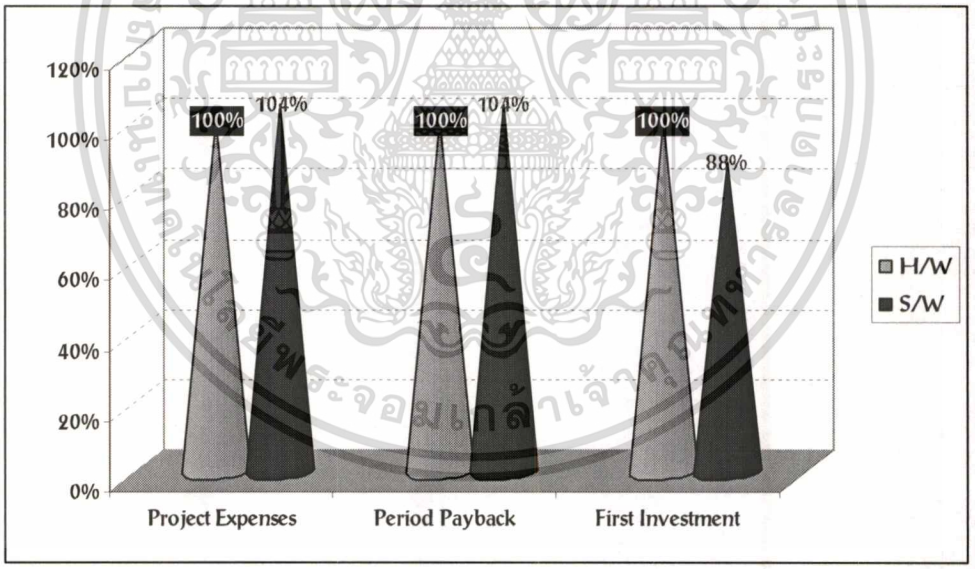
5.3 ผลการวิเคราะห์

ตารางที่ 5.1 เปรียบเทียบโครงการทั้ง 2 โดยใช้ ฮาร์ดแวร์ VPN เป็นตัวตั้ง

	รายการ	ฮาร์ดแวร์ VPN	ซอร์ฟแวร์ VPN	เปรียบเทียบทั้งสองโครงการ
1	ค่าลงทุนเริ่มแรก	512,000	449,000	-12 %
2	ค่าใช้จ่ายตลอดโครงการระยะเวลาโครงการ(ค่าเงินปัจจุบัน)	1,044,623.8	1,090,908.9	4 %
3	ระยะเวลาคืนทุน	3.81 ปี	3.98 ปี	4 %
4	อัตราผลตอบแทนการลงทุน (B/C Ratio)	1.16 เท่า	1.10 เท่า	5%
5	อัตราส่วนผลตอบแทนต่อสินทรัพย์ (ROI)	12.19%	11.92%	2%
6	อัตราส่วนผลตอบแทนภายใน (IRR)	32.74%	32.36%	0.38%
7	ผลตอบแทนสุทธิ (NPV)	652,710.82	525,478.67	19 %



รูปที่ 5.1 แผนภูมิแสดงการเปรียบเทียบทั้ง 2 โครงการ โดยให้โครงการ ฮาร์ดแวร์ VPN เป็น 100%



รูปที่ 5.2 แผนภูมิแสดงการเปรียบเทียบทั้ง 2 โครงการ โดยให้โครงการ ซอร์ฟแวร์ VPN เป็น 100%

สรุปผลจากการวิเคราะห์ในบทที่ 4 ที่ได้จากปัจจัยทั้ง 7 แล้วมีบทสรุปที่การวางเครือข่าย VPN แบบใช้ฮาร์ดแวร์ในการอุโมงค์ VPN เป็นแนวทางที่ดีที่สุดในการวางระบบ จะมีก็แต่การลงทุนเริ่มแรกเท่านั้นที่ต้องลงทุนมากกว่า และมีระยะเวลาคุ้มทุนอยู่ที่ประมาณ 3 ปี 9 เดือน และให้ผลตอบแทนที่สูงกว่าโครงการอื่น 127,232.15 หรือ บาทตลอดระยะเวลาโครงการ 5 ปี และมีความเสี่ยงต่อการเปลี่ยนแปลงของดอกเบี้ยได้ดีมากเนื่องจากสามารถรองรับการขึ้นของดอกเบี้ย

ได้ถึงประมาณ 32.74% ซึ่งยังคงทำให้สามารถวางระบบได้ด้วยการกู้เงินมาลงทุนเพราะค่าของการเปลี่ยนแปลงดอกเบี้ยที่สามารถยอมรับได้เป็น 32.74% ซึ่งเงินกู้โดยปกติไม่เกิน 18%

ซึ่งในผลสรุปที่ออกมาจากปัจจัยทั้ง 7 นั้น จาก 2 โครงนั้นได้ผลลัพธ์ที่ค่อนข้างใกล้เคียงกันและมีผลตอบแทนการลงทุนที่เป็นบวกทั้งสองโครงการ แต่ที่เลือกโครงการ VPN แบบฮาร์ดแวร์เนื่องจากเป็นระบบที่มีค่าใช้จ่ายในการดำเนินงานต่ำให้ผลตอบแทนโครงการสูงกว่าในโครงการแบบซอร์ฟแวร์ประมาณ 19 % โดยทั้งยังไม่ต้องไปยุ่งยากในการหาผู้ดูแลระบบที่เป็น VPN ซอร์ฟแวร์และการที่ใช้งาน VPN ฮาร์ดแวร์นั้นยังมีประสิทธิภาพในการทำงานที่ดีกว่าทำให้ข้อมูลสารสนเทศที่ส่งผ่านเครือข่าย VPN มีประสิทธิภาพที่ดีกว่า

5.4 ผลตอบแทนที่ได้รับจากเครือข่ายใหม่

5.4.1 ได้ช่องทางการสื่อสารข้อมูลให้กับผู้บริหารและพนักงานที่ต้องทำงานนอกสถานที่ให้สามารถรับรู้ข่าวสารและสารสนเทศภายในได้จากทุก ๆ สถานที่ที่สามารถเชื่อมต่อเข้าเครือข่ายอินเทอร์เน็ตได้

5.4.2 เพิ่มประสิทธิภาพในการดูแลรักษาระบบสารสนเทศภายในโดยสามารถเข้ามาตรวจสอบและแก้ไขข้อผิดพลาดของระบบภายในจากภายนอกได้อย่างปลอดภัย

5.4.3 เพิ่มช่องทางการค้นหาข้อมูลจากระบบภายในของสำนักงานแต่ละสาขาได้นอกจากทางอิเลคทรอนิกส์เมล์

5.4.4 ลดค่าใช้จ่ายในการเช่าสายสัญญาณ LEASED LINE ซึ่งมีค่าใช้จ่ายที่สูงมากเมื่อเปรียบเทียบกับการใช้งานผ่านเครือข่ายอินเทอร์เน็ตถึงแม้ว่าประสิทธิภาพจะไม่สามารถนำมาเทียบกับการเช่าสัญญาณ LEASED LINE (ในกรณีเปรียบเทียบกับ INTERNATIONAL LEASED LINE)

5.4.5 เพิ่มความปลอดภัยของข้อมูลที่ทำการสื่อสารระหว่างสำนักงานต่าง ๆ เนื่องจากก่อนการวางเครือข่าย VPN นั้นเครือข่ายระหว่างประเทศนั้นส่งข้อมูลส่วนใหญ่ผ่านอินเทอร์เน็ตโดยการรับส่ง จดหมายอิเลคทรอนิกส์ ซึ่งการรับส่ง จดหมายอิเลคทรอนิกส์ ผ่านเครือข่ายอินเทอร์เน็ตโดยตรงนั้นสามารถที่จะดักจับข้อมูลแล้วนำมาตีความได้เพราะข้อมูลที่ผ่านเครือข่ายอินเทอร์เน็ตเป็นข้อความที่มิได้มีการเข้ารหัสแต่อย่างใด

5.4.6 ได้ผลตอบแทนจากการอนุญาตให้เข้าใช้ระบบจากสำนักงานสาขาต่าง ประเทศ คือ มาเลเซีย อินโดนีเซีย และ จีน

ภาคผนวก ก.

ความหมายของ TCP/IP (Transmission Control Protocol / Internet Protocol)

เครื่องคอมพิวเตอร์บนเครือข่ายอินเทอร์เน็ต สื่อสารระหว่างกันโดยใช้ Transmission Control Protocol (TCP) และ Internet Protocol (IP) รวมเรียกว่า TCP/IP ข้อมูลที่ส่งจะถูกตัดออกเป็นส่วนๆ เรียก packet แล้วจ่าหน้าไปยังผู้รับด้วยการกำหนด IP Address เช่น สมมติเราส่ง e-mail ไปหาใครสักคน e-mail ของเราจะถูกตัดออกเป็น packet ขนาดเล็กๆ หลายๆ อัน ซึ่งแต่ละอันจะจ่าหน้าถึงผู้รับเดียวกัน packets พวกนี้ก็จะวิ่งไปรวมกับ packets ของคนอื่นๆ ด้วย ทำให้ในสายของข้อมูล packets ของเราอาจจะไม่ได้เรียงติดกัน packets พวกนี้จะวิ่งผ่าน ชุมทาง (gateway) ต่างๆ โดยตัว gateway (อาจเรียก router) จะอ่านที่อยู่ที่จ่าหน้า แล้วจะบอกทิศทางที่ไปของแต่ละ packet ว่าจะวิ่งไปในทิศทางไหน packet ก็จะวิ่งไปตามทิศทางนั้น เมื่อไปถึง gateway ใหม่ก็จะถูกกำหนดเส้นทางให้วิ่งไปยัง gateway ใหม่ที่อยู่ถัดไป จนกว่าจะถึงเครื่องปลายทาง เช่น เราติดต่อกับเครื่องในอเมริกา อาจจะต้องผ่าน gateway ถึง 10 แห่ง เมื่อ packet วิ่งมาถึงปลายทางแล้ว เครื่องปลายทางก็จะเอา packets เหล่านั้นมาเก็บสะสมจนกว่าจะครบ จึงจะต่อกลับคืนให้เป็น e-mail

ความรู้ทั่วไปเกี่ยวกับ Port ในเครือข่าย TCP/IP & UDP/IP

สำหรับพวก Application ในชั้น layer สูงๆ ที่ใช้ TCP (Transmission Control Protocol) หรือ UDP (User Datagram Protocol) จะมีหมายเลข Port หมายเลขของ Port จะเป็นเลข 16 bit เริ่มตั้งแต่ 0 ถึง 65535 หมายเลข Port ใช้สำหรับตัดสินว่า service ใดที่ต้องการเรียกใช้ ในทางทฤษฎี หมายเลข Port แต่ละหมายเลขถูกเลือกสำหรับ service ใดๆ ขึ้นอยู่กับ OS (operating system) ที่ใช้ ไม่จำเป็นต้องเหมือนกัน แต่ได้มีกำหนดขึ้นให้ใช้ค่อนข้างเป็นมาตรฐานเพื่อให้มีการติดต่อการส่งข้อมูลที่ดีขึ้น ทาง Internet Assigned Numbers Authority (IANA) เป็นหน่วยงานกลางในการประสานการเลือกใช้ Port ว่า Port หมายเลขใดควรเหมาะสำหรับ Service ใด และได้กำหนดใน Request For Comments (RFC') 1700 ตัวอย่างเช่น เลือกใช้ TCP Port หมายเลข 23 กับ Service Telnet และเลือกใช้ UDP Port หมายเลข 69 สำหรับ Service Trivial File transfer Protocol (TFTP) ตัวอย่างต่อไปนี้เป็นบางส่วนของ File/etc/services แสดงให้เห็นว่า หมายเลข Port แต่ละหมายเลขได้ถูกจับคู่กับ Transport Protocol หนึ่งหรือสอง Protocol ซึ่งหมายความว่า UDP หรือ TCP อาจจะใช้ หมายเลข Port เดียวกันก็ได้ เนื่องจากเป็น Protocol ที่ต่างกัน หมายเลข Port ถูกจัดแบ่งเป็น 2

ประเภท ตามที่ได้กำหนดใน RFC' 1700 (รายละเอียด Download และศึกษาได้ที่ ftp://ftp.isi.edn/in-notes/rfc'1700.txt) คือ well known Ports และ Registered Ports

- Well Known Ports คือจะเป็น Port ที่ระบบส่วนใหญ่ กำหนดให้ใช้โดย Privileged User (ผู้ใช้ที่มีสิทธิพิเศษ) โดย port เหล่านี้ ใช้สำหรับการติดต่อระหว่างเครื่องที่มีระบบเวลาที่ยาวนาน วัตถุประสงค์เพื่อให้ service แก่ผู้ใช้ (ที่ไม่รู้จักหรือคุ้นเคย) แปลกหน้า จึงจำเป็นต้องกำหนด Port ติดต่อสำหรับ Service นั้นๆ
- Registered Ports จะเป็น Port หมายเลข 1024 ขึ้นไป ซึ่ง IANA ไม่ได้กำหนดไว้

Hypertext Transfer Protocol (HTTP) และ Hypertext Markup Language (HTML)

HTTP คือโปรโตคอลที่ใช้สื่อสารระหว่าง client computer กับ server computer ทำให้ทั้งสองเครื่องรู้ว่าจะจัดการส่งข้อมูลไปอย่างไร ส่วน HTML คือสื่อภาษาที่ทำให้เอกสารหรือ contents ที่อยู่บนเครื่อง server computer เมื่อถูกส่งมาที่ client computer แล้วจะนำไปแสดงได้อย่างไร เราเรียกซอฟท์แวร์ที่ใช้แสดงนี้ว่า Browser โดย HTTP ใช้งาน Port 80

SMTP AND POP

Simple Mail Transfer Protocol (SMTP) และ POP (Post Office Protocol) นั้นเป็นโปรโตคอลที่ต้องทำงานควบคู่กันโดย SMTP นั้นทำหน้าที่ในการส่ง E-MAIL และ POP ทำหน้าที่ในการรับ E-MAIL โปรโตคอลทั้งสองตัวจะทำงานในชั้น Application Layer โดยใช้งาน TCP Port 25,110 ตามลำดับ

FTP (File Transfer Protocol)

มาตรฐานในอินเทอร์เนตสำหรับการถ่ายโอนแฟ้มข้อมูล โดยจะเป็นการบรรจุลง (download) แฟ้มข้อมูลจากคอมพิวเตอร์ เครื่องอื่นในอินเทอร์เนตมาไว้ในคอมพิวเตอร์ของเรา หรือจะเป็นการบรรจุขึ้น (upload) แฟ้มข้อมูลของเราส่งไปยังศูนย์ บริการตามกฎเกณฑ์การถ่ายโอนแฟ้มก็ได้เช่นกัน FTP (พิมพ์ด้วยอักษรตัวใหญ่) จะเป็นชุดกฎเกณฑ์เฉพาะที่ประกอบด้วย ftp (พิมพ์ด้วยอักษรตัวเล็ก) ซึ่งเป็นมาตรฐานในการติดต่อสื่อสารแบบไม่ประสานจังหวะ ดู file transfer protocol (ftp) ประกอบในการใช้กฎเกณฑ์การถ่ายโอนแฟ้มนี้ เราต้องเริ่มต้นด้วยการเป็นผู้รับบริการหรือเป็นสมาชิกเอฟทีพี โดยจะมีโปรแกรมใช้งานที่ช่วยให้เราสามารถติดต่อกับคอมพิวเตอร์เครื่องอื่นในอินเทอร์เนตและแลกเปลี่ยนหรือถ่ายโอนแฟ้มระหว่างกันได้ ในการเข้าถึงคอมพิวเตอร์เครื่องอื่นนั้น เราต้องมีชื่อลงบันทึกเข้า (login name) และรหัสผ่าน หลังจากนั้นเราจะสามารถเข้าถึงระบบสา

รบบแฟ้มของคอมพิวเตอร์และสามารถทำการบรรจุลงหรือบรรจุขึ้นแฟ้มต่างๆ ที่ต้องการได้ สิ่งยกเว้นอย่างหนึ่งได้แก่ เอฟทีพีที่ไม่ระบุชื่อ (anonymous FTP) ซึ่งจะทำให้ผู้ใช้อินเทอร์เนตที่เป็นสมาชิกของเอฟทีพีสามารถเข้าถึงแฟ้มที่เก็บ บันทึกได้ แต่ต้องพิมพ์คำว่า anonymous แทนชื่อลงบันทึกเข้า และต้องใส่เลขที่อยู่ของไปรษณีย์อิเล็กทรอนิกส์แทนรหัส ผ่าน โปรแกรมสำรวจข้อมูลในเวิลด์ไวด์เว็บหลายๆ โปรแกรมสามารถช่วยให้สมาชิกเอฟทีพีสามารถบรรจุลงแฟ้มจากเอฟ ทีพีที่ไม่ระบุชื่อได้

RDP (REMOTE DESKTOP PROTOCOL)

เป็นโปรโตคอลที่ใช้ในการติดต่อสื่อสารระหว่างเครื่อง MICROSOFT WINDOWS 2000 TERMINAL SERVER กับเครื่อง TERMINAL CLIENT โดยเรียกใช้การเชื่อมต่อผ่านโปรโตคอล TCP/IP เพื่อประโยชน์ใน 2 รูปแบบการใช้งานคือการทำเพื่อเข้าควบคุมระบบทางไกล รวมถึงการสร้าง APPLICATION SERVER เพื่อลดการจราจรในระบบเครือข่าย โดยทั่วไปมักนิยมใช้กับเครือข่ายที่เป็น WAN (WIDE AREA NETWORK) ที่มีความกว้างของช่องสัญญาณต่ำเพื่อให้สามารถใช้ช่องสัญญาณได้อย่างมีประโยชน์สูงสุดโดยปกติแล้ว RDP โปรโตคอลสามารถรองรับการเชื่อมต่อได้มากถึง 64,000 การเชื่อมต่อในขณะเวลาเดียวกัน แต่ประสิทธิภาพและสิทธิ์ในการเชื่อมต่อต้องถูกกำหนดผ่าน TERMINAL SERVER

ภาคผนวก ข.

Present Value Table

Year	1%	2%	3%	4%	5%	6%	7%	8%	9%	10%
1	0.990	0.980	0.971	0.962	0.952	0.943	0.935	0.926	0.917	0.909
2	0.980	0.961	0.943	0.925	0.907	0.890	0.873	0.857	0.842	0.826
3	0.971	0.942	0.915	0.889	0.864	0.840	0.816	0.794	0.772	0.751
4	0.961	0.924	0.888	0.855	0.823	0.792	0.763	0.735	0.708	0.683
5	0.951	0.906	0.863	0.822	0.784	0.747	0.713	0.681	0.650	0.621
6	0.942	0.888	0.837	0.790	0.746	0.705	0.666	0.630	0.596	0.564
7	0.933	0.871	0.813	0.760	0.711	0.665	0.623	0.583	0.547	0.513
8	0.923	0.853	0.789	0.731	0.677	0.627	0.582	0.540	0.502	0.467
9	0.914	0.837	0.766	0.703	0.645	0.592	0.544	0.500	0.460	0.424
10	0.905	0.820	0.744	0.676	0.614	0.558	0.508	0.463	0.422	0.386
	11%	12%	13%	14%	15%	16%	17%	18%	19%	20%
1	0.901	0.893	0.885	0.877	0.870	0.862	0.855	0.847	0.840	0.833
2	0.812	0.797	0.783	0.769	0.756	0.743	0.731	0.718	0.706	0.694
3	0.731	0.712	0.693	0.675	0.658	0.641	0.624	0.609	0.593	0.579
4	0.659	0.636	0.613	0.592	0.572	0.552	0.534	0.516	0.499	0.482
5	0.593	0.567	0.543	0.519	0.497	0.476	0.456	0.437	0.419	0.402
6	0.535	0.507	0.480	0.456	0.432	0.410	0.390	0.370	0.352	0.335
7	0.482	0.452	0.425	0.400	0.376	0.354	0.333	0.314	0.296	0.279
8	0.434	0.404	0.376	0.351	0.327	0.305	0.285	0.266	0.249	0.233
9	0.391	0.361	0.333	0.308	0.284	0.263	0.243	0.225	0.209	0.194
10	0.352	0.322	0.295	0.270	0.247	0.227	0.208	0.191	0.176	0.162

บรรณานุกรม

ธนิตศักดิ์ ทุมแสน. 2543. “THE FEASIBILITY STUDY OF OPTICAL PLANT TECHNOLOGY FOR LOCAL DISTRIBUTION NETWORKS” ,โครงการศึกษากรณีพิเศษวิทยาศาสตร์มหาบัณฑิต คณะเทคโนโลยีสารสนเทศ, สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ไพบูลย์ แย้มเผื่อน. 2545. เศรษฐศาสตร์วิศวกรรม (ENGINEERING ECONOMY). กรุงเทพ : ซีเอ็ดยูเคชั่น

3Com corporation. 2001. Virtual Private Network: Internet Base VPNs white paper. U.S.A.

Microsoft corporation.1999. Virtual Private Network in Windows 2000 Overview.U.S.A.

Pual Ferguson & Geoff Huston. April 1996. What is a VPN Revision 1. U.S.A.

ประวัติผู้เขียน

นายบงการ ช้างเสวก เกิดเมื่อวันที่ 23 มีนาคม พ.ศ. 2518 ที่จังหวัดกรุงเทพมหานคร สำเร็จการศึกษาศิลปศาสตร์บัณฑิต จากสถาบันราชภัฏเพชรบุรี วิทยาลงกรณ์ในพระบรมราชูปถัมป์ เมื่อปีการศึกษา 2541 เข้าศึกษาระดับปริญญาวิทยาศาสตรมหาบัณฑิต สาขาเทคโนโลยีสารสนเทศ แขนงวิชาการจัดการเทคโนโลยีสารสนเทศ สถาบันพระจอมเกล้า เจ้าคุณทหาร ลาดกระบัง ในปีการศึกษา 2544

ตำแหน่งและหน้าที่การทำงานปัจจุบัน เป็นผู้ช่วยผู้จัดการฝ่ายสารสนเทศ บริษัทอาร์มสตรอง รับเบอร์แอนด์เคมิคัล โปรดักส์ จำกัด