การพัฒนา Virtual Private Network ของศูนย์เทคโนโลยีโลหะและวัสดุแห่งชาติ

วรรณวิมล ปัญญาจงถาวร* และ พยุง มีสัจ**

บทนำ

การพัฒนา Virtual Private Network ของศูนย์เทคโนโลยีโลหะและวัสดุแห่งชาติ จัดทำขึ้นเพื่อเพิ่มช่องทางการสื่อสารที่เชื่อมต่อจากภายนอกผ่านเครือข่ายสาธารณะ หรือเทคโนโลยีระบบเครือข่ายรูปแบบใหม่ ให้สามารถใช้บริการข่าวสารและระบบภายในได้อย่างปลอดภัย ระบบที่พัฒนาขึ้นทำการติดตั้งเครื่องแม่ข่ายวีพีเอ็น ที่ใช้โปรแกรม OpenVPN เวอร์ชัน 2.0 บนระบบปฏิบัติการ Windows เวอร์ชัน 2000 ในโซนเครื่องแม่ข่าย สำหรับการติดต่อสื่อสารกับเครือข่ายภายนอก (DMZ Zone) ในเครือข่ายของศูนย์เทคโนโลยีโลหะและวัสดุแห่งชาติ กำหนดและพิสูจน์สิทธิในการเข้าถึงเครื่องแม่ข่ายภายใน โดยใช้ใบรับรองดิจิตอล (Digital Certificate) กำหนดเงื่อนไขรองรับการทำงานและตรวจสอบความปลอดภัยตามระดับมาตรฐานของโปรแกรม ใช้วิธีการทดสอบและประเมินผลความพึงพอใจในการใช้งาน เป็นเครื่องมือวัดคุณภาพของระบบที่พัฒนาขึ้น จากกลุ่มตัวอย่าง 2 กลุ่ม ที่ใช้งานผ่านเครือข่ายสาธารณะ 5 สถานที่ ประเมินผลความพึงพอใจจากการติดตั้ง การเชื่อมต่อและการใช้งานด้วยแบบสอบถามความพึงพอใจ 4 ด้าน (Requirement Test, Usability Test, Performance Test และ Security Test)

คำสำคัญ: วีพีเอ็น เครือข่ายส่วนบุคคล เครือข่ายสาธารณะ

1. บทนำ

ศูนย์เทคโนโลยีโลหะและวัสดุแห่งชาติ เป็นหน่วยงานที่ทำการศึกษาวิจัยทางด้านโลหะและวัสดุ โดยช่วงแรกของการนำเทคโนโลยีคอมพิวเตอร์เข้ามาใช้งานในหน่วยงานจะเป็นการใช้งานลักษณะเป็นอุปกรณ์ประกอบและทดแทน เพื่อเพิ่มประสิทธิภาพให้กับการทำงาน เช่น การพิมพ์เอกสาร ต่อมาได้มีการนำเทคโนโลยีคอมพิวเตอร์และเครือข่ายมาใช้เพิ่มเติม ทั้งที่เป็นระบบบริการ และระบบสำนักงานอื่น ๆ ส่งผลให้การทำงานมีความสะดวก รวดเร็ว สามารถตรวจสอบได้ ลดความเสียหายของข้อมูลและอำนวยความสะดวกในการจัดเก็บข้อมูล อย่างเป็นระบบมากขึ้น

กลางปีพ.ศ.2546 หน่วยงานได้ย้ายสถานที่ตั้ง โดยยังมีสำนักงานชั่วคราวไว้ที่อาคารเดิม จึงมีการนำเทคโนโลยี Remote Access มาประยุกต์ใช้ จุดประสงค์เริ่มต้นในการนำมาใช้งาน เพื่ออำนวยความสะดวกในการทำงานจากต่างสถานที่ของผู้ดูแลระบบ ต่อมามีการพัฒนาระบบป้องกันความปลอดภัย จนสามารถให้บริการระบบงานภายในผ่านทางระบบ Remote Access กับพนักงานได้ ปลายปีพ.ศ. 2547 หน่วยงานมีอัตราเจริญเติบโตขึ้นอย่างรวดเร็ว มีความร่วมมือทำการวิจัยกับหน่วยงานภายนอก (หน่วยงานเครือข่าย) ทำให้เกิดการปรับเปลี่ยนระบบลงเวลาการทำงาน ให้มีความยืดหยุ่น สอดคล้องกับลักษณะการทำงานและการใช้สอยพื้นที่ ในขณะเดียวกันเทคโนโลยี Broadband และ ADSL ได้รับความนิยมในการใช้งานอย่างรวดเร็ว จากการแข่งขันด้านบริการที่มีผู้ให้บริการจำนวนมาก ความเร็วในการใช้งานสูง ค่าใช้จ่ายและอุปกรณ์ประกอบมีราคาต่ำลง แต่หน่วยงานยังไม่มีความพร้อมในการรองรับการเชื่อมต่อ ทำให้ไม่สามารถใช้งานระบบงานภายในที่มีอยู่ เหมือนดังเช่นการเข้าถึงเครือข่ายด้วย Remote Access ที่สามารถให้บริการได้

ปัจจุบัน หน่วยงานมีความพร้อมเพิ่มขึ้น ทั้งในด้านของเทคโนโลยีเครือข่าย ที่สามารถรองรับการใช้งาน ระบบงานภายในที่มีเพิ่มมากขึ้น ความพร้อมของผู้ใช้งาน ที่ตระหนักถึงความปลอดภัยในการใช้งานระบบและข้อมูลผ่านเครือข่ายสาธารณะ มีข้อมูลจากการใช้งานบริการของงานระบบคอมพิวเตอร์ว่าบุคลากรที่ใช้งานผ่าน Broadband จากหน่วยงานเครือข่าย หรือใช้ ADSL มีอัตราเพิ่มขึ้นอย่างรวดเร็ว ในขณะเดียวกันก็พบว่า เทคโนโลยี Virtual Private Networks หรือ VPN ที่ใช้ประโยชน์จากการส่งข้อมูลผ่านเครือข่ายอินเทอร์เน็ตสาธารณะ มีความน่าสนใจในการศึกษาเพิ่มเติม เพื่อการนำมาปรับใช้อย่างเหมาะสมกับหน่วยงาน ซึ่งจะทำให้ระบบการเข้าถึงเครือข่ายภายในของศูนย์เทคโนโลยีโลหะและวัสดุแห่งชาติจากเครือข่ายสาธารณะ ได้รับการปกป้องจากความเสี่ยงที่มีเพิ่มขึ้นอย่างมากและรวดเร็ว [1] มีความสอดคล้องในการทำงานตามนิยามความมั่นคงปลอดภัย [2] และสามารถสนับสนุนการให้บริการ ที่เคยให้ได้แต่เฉพาะการใช้งานภายในหรือผ่าน Remote Access ซึ่งพบข้อจำกัดด้านความเร็วในการให้บริการ เป็นการเพิ่มประสิทธิภาพและเพิ่มความคล่องตัว

* *ภาควิชาเทคโนโลยีสารสนเทศ คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ*

** *ภาควิชาครุศาสตร์ไฟฟ้า คณะครุศาสตร์อุตสาหกรรม มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ*

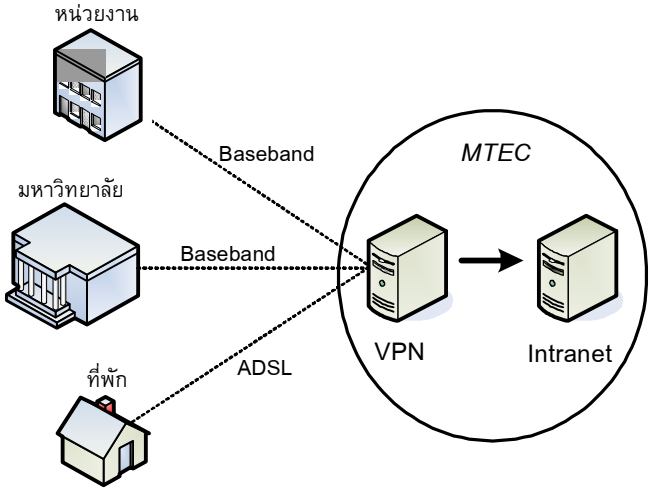
สำหรับผู้ทำงาน เป็นการสนับสนุนให้หน่วยงาน สามารถผลิตผลงานที่เป็นประโยชน์ให้แก่ประเทศได้อีกทางหนึ่ง

ทฤษฎีที่เกี่ยวข้องและถูกนำมาเป็นข้อมูลประกอบการดำเนินการได้แก่ ความปลอดภัยในการสื่อสารคอมพิวเตอร์ เทคโนโลยีวีพีเอ็น (Virtual Private Network: VPN) และ Socket Secure Layer (SSL) อีกทั้งยังได้ศึกษางานวิจัยเพื่อนำมาใช้ในการออกแบบระบบและกำหนดเทคโนโลยีที่จะนำมาใช้ โดยได้รายละเอียดจากงานวิจัยของ Khanvilkar และ Khokhar [3] ที่ทำการประเมินประสิทธิภาพของ Virtual Private Network โดยใช้ Open-Source Linux-based VPN Solutions (OSLVs) เปรียบเทียบกับประสิทธิภาพของเครือข่ายที่คาดหวังไว้ ซึ่งผลการศึกษาพบว่า UDP-based Data Channels มีประสิทธิภาพในการทำงานมากกว่า TCP-based Data Channels งานวิจัยของ Clercq และ Paridaens [4] ได้ทำการวิเคราะห์พื้นฐานของการให้บริการ Virtual Private Network จากเครือข่ายหลักของผู้ให้บริการอินเทอร์เน็ต กับมาตรการความปลอดภัยที่เหมาะสมซึ่งเครือข่ายวีพีเอ็นสามารถทำได้ ซึ่งพบว่า สิ่งที่ต้องคำนึงถึงในด้านความปลอดภัยคือ การเลือกใช้การเข้ารหัส การดูแลและจำกัดจำนวนของข้อมูลที่รับ-ส่ง และจากงานวิจัยของ Venkateswaran [5] ที่ทำการศึกษารูปแบบของ Virtual Private Network ที่สามารถใช้เชื่อมโยงเครือข่ายส่วนบุคคล พบว่า บริการวีพีเอ็น ทำให้การเข้าถึงเครือข่ายมีค่าใช้จ่ายต่ำลง สามารถรองรับการใช้งานแบบเคลื่อนที่ได้ มีความน่าเชื่อถือในการตรวจสอบสิทธิและโดยสามารถใช้อุปกรณ์และช่องทางการสื่อสารที่หลากหลาย

จากการศึกษาเบื้องต้นพบว่า เทคโนโลยี Virtual Private Network ได้รับความนิยมในการนำมาใช้งานร่วมกับระบบเครือข่ายอย่างแพร่หลาย โดยเฉพาะการใช้งานผ่านเครือข่ายสาธารณะเข้าสู่เครือข่ายส่วนบุคคล โดยมีปัจจัยหลายประการให้ต้องพิจารณาความเหมาะสม ประกอบการนำมาใช้งาน อันได้แก่ ความต้องการการใช้งาน รูปแบบหรือโครงสร้างของระบบเครือข่ายและอุปกรณ์ที่มีอยู่ ระดับความปลอดภัยที่ต้องคำนึงถึง คุณสมบัติของโปรแกรม (Software) ที่จะนำมาใช้งาน และค่าใช้จ่ายที่ใช้ในการลงทุน

2. วิธีการดำเนินงาน

แนวคิดในการวิจัยระบบ Virtual Private Network ต้องการระบบที่สามารถรองรับการเชื่อมต่อจากระบบเครือข่ายสาธารณะภายนอกมายังระบบเครือข่ายภายใน เพื่อทำการใช้ระบบหรือข้อมูลข่าวสารที่มีการใช้งานเฉพาะของหน่วยงาน โดยสามารถทำการพิสูจน์ตัวตน (Authentication) ให้ได้สิทธิในการเข้าถึงและใช้งานข้อมูลของเครื่องแม่ข่ายที่กำหนดอย่างเหมาะสมและปลอดภัยได้ถูกนำเสนอ ดังภาพที่ 1



ภาพที่ 1 แนวคิดในการเชื่อมต่อระบบ

2.1 การศึกษาและรวบรวมข้อมูล

งานวิจัยนี้ได้กำหนดข้อมูลที่นำมาใช้ในการศึกษาออกเป็น 4 กลุ่ม ได้แก่ 1) ข้อมูลความต้องการการใช้งาน (ตารางที่ 1 และ 2) จากงานระบบคอมพิวเตอร์ศูนย์เทคโนโลยีโลหะและวัสดุแห่งชาติ 2) ระเบียบสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติว่าด้วย การใช้ระบบเครือข่ายคอมพิวเตอร์และความมั่นคงสารสนเทศ พ.ศ. 2549 และแนวทางความปลอดภัยในการใช้งานคอมพิวเตอร์ ของศูนย์เทคโนโลยีโลหะและวัสดุแห่งชาติ 3) ข้อมูลรูปแบบเครือข่ายและข้อกำหนดด้านความปลอดภัยในเครือข่ายวีพีเอ็น ของศูนย์พันธุวิศวกรรมและเทคโนโลยีชีวภาพแห่งชาติและ 4) เทคโนโลยีที่เกี่ยวข้องกับเครื่องมือ ที่ใช้ในการพัฒนา โดยเฉพาะที่เกี่ยวข้องกับโปรแกรมประเภท Open-Source ซึ่งหน่วยงานให้การสนับสนุนการนำมาใช้ทดแทนโปรแกรมลิขสิทธิ์ แล้วทำการรวบรวมข้อมูลจากแหล่งข้อมูลทั้งหมด

ตารางที่ 1 ลักษณะการใช้งานจากภายนอก

ปี	Remote Access	ADSL	Broadband
2547	70	1	5
2548	107	9	17
2549 (May)	131	14	27

ตารางที่ 2 ระบบหรือข้อมูลที่ต้องการเข้าถึงจากภายนอก

ประเภท / ปี	Access Data	Used Application	Check News
2547	3	3	10
2548	5	9	17
2549 (May)	11	14	33

2.2 การวิเคราะห์ข้อมูลและออกแบบระบบ

งานวิจัยนี้ได้ทำการจัดการกับข้อมูลที่ได้ศึกษาและรวบรวมมา โดยนำมาสรุปเป็นประเด็นสำคัญที่ต้องดำเนินการ อาทิ ข้อมูลการใช้งานเครือข่าย มีผู้ใช้งานจากภายนอกจำนวน 131 คนคิดเป็น 10% ของบุคลากรทั้งหน่วยงานทำให้ประสิทธิภาพในการรองรับการใช้งานผ่านระบบ Remote Access ไม่เพียงพอ และไม่สามารถตอบสนองด้านความเร็วในการใช้งาน การพัฒนาระบบใหม่ที่เพื่อสนับสนุนการใช้งานโปรแกรม Open-Source และสามารถป้องกันความปลอดภัยจากการดักจับข้อมูลใช้งานระหว่างการใช้งานได้ โดยการทำงานของระบบ Virtual Private Network ที่สามารถรองรับการให้บริการผ่านเครือข่ายสาธารณะ รองรับการทำงานของอุปกรณ์เชื่อมต่อที่มีความเร็วสูงกว่าอุปกรณ์ Modem ทั่วไป เช่น ADSL และสามารถเลือกรูปแบบในการควบคุมความปลอดภัยของการใช้งาน ซึ่งเหมาะที่จะนำมาปรับใช้ได้อย่างสอดคล้องกับระเบียบและแนวทางของศูนย์เทคโนโลยีโลหะและวัสดุแห่งชาติ

2.3 การพัฒนาระบบ

การพัฒนาระบบ Virtual Private Network ของศูนย์เทคโนโลยีโลหะและวัสดุแห่งชาติ ได้ทำการจำลองเครื่องคอมพิวเตอร์ส่วนบุคคลที่มีประสิทธิภาพสูงให้เป็นเครื่องแม่ข่ายภายในระบบเครือข่ายของศูนย์เทคโนโลยีโลหะและวัสดุแห่งชาติ ทำการติดตั้งโปรแกรม OpenVPN เวอร์ชัน 2.0 ทำหน้าที่ให้บริการระบบวีพีเอ็น ควบคุมและเก็บข้อมูลการเข้าใช้งานตามสิทธิที่กำหนดขึ้น ตั้งอยู่หลังอุปกรณ์ Firewall ที่เป็นตัวเชื่อมต่อกับเครือข่ายสาธารณะของหน่วยงาน โครงร่างของโปรแกรม (Configuration) กำหนดให้ใช้ค่าตั้งต้น (Default) เพื่อทดสอบการรองรับการทำงานและตรวจสอบความปลอดภัย โดยใช้วิธีการพิสูจน์สิทธิด้วยใบรับรอง (Certificate) ของระบบปฏิบัติการ Windows ซึ่งไม่เคยมีการใช้งานมาก่อนในหน่วยงาน พารามิเตอร์ในการเข้ารหัสแบบ Diffie Hellman ขนาด 1024 Bits วิธีการเข้ารหัสข้อมูลแบบ Blowfish ทำงานด้วยโพรโทคอล UDP และช่องทางที่ใช้งานเป็นแบบ Ethernet Tunnel ที่ไม่ให้สิทธิในการกระจายข่าวสาร (Broadcast) ผ่านเครือข่ายโปรแกรมประเภท Open-Source

การกำหนดสิทธิการเข้าถึงเครือข่ายบนเครื่องแม่ข่ายวีพีเอ็นให้กับกลุ่มตัวอย่าง ได้กำหนดให้สามารถทำการติดต่อเข้าถึงข้อมูล หรือระบบบนเครื่องแม่ข่าย Intranet Web Server เท่านั้น โดยจะสามารถเรียกใช้งาน Intranet Web และ Application บน Intranet Web Server ผ่านโปรแกรม Web Browser

2.4 การทดสอบระบบ

ได้กำหนดรูปแบบการทดสอบระบบด้วยการประเมินผลคุณภาพของระบบที่ได้พัฒนาขึ้น เป็นการทดสอบความพึงพอใจในการใช้งาน กระบวนการประเมินผลแบ่งการทดสอบออกเป็น 2 ขั้นตอนได้แก่

2.4.1 ทดสอบระบบในขั้นแอลฟา (Alpha Stage)

เป็นการทดสอบหาข้อบกพร่องของการกำหนดโครงร่างและการติดตั้งโปรแกรมโดยผู้พัฒนา ใช้วิธีการบันทึกข้อมูลปัญหาที่พบและข้อควรสังเกต ในรูปแบบตารางอย่างง่าย หลังจากนั้นทำการแก้ไขปรับปรุงระบบให้สามารถรองรับการใช้งานตามที่มีการกำหนดไว้

2.4.2 ทดสอบระบบในขั้นเบต้า (Beta Stage)

เป็นการทดสอบคุณภาพของระบบ โดยกลุ่มตัวอย่าง 2 กลุ่ม โดยการทดสอบจะทำตั้งแต่การติดตั้งโปรแกรม การเชื่อมต่อเครือข่ายจากเครือข่ายสาธารณะภายนอกและการใช้งานข้อมูลหรือระบบภายใน ซึ่งจะมีการส่งโปรแกรมและคู่มือการติดตั้งให้กลุ่มตัวอย่างก่อนการดำเนินการ ในการทดสอบของกลุ่มผู้เชี่ยวชาญและผู้ดูแลระบบ จะมีการให้โปรแกรมสุ่มดักจับข้อมูลระหว่างการทดสอบ เพื่อใช้ประกอบการประเมินด้านความปลอดภัยให้กลุ่มตัวอย่าง หลังจากนั้นจึงจะทำการตอบแบบประเมินผลความพึงพอใจในการใช้งานระบบ กำหนดให้เวลาในการทดสอบภายใน 2 สัปดาห์

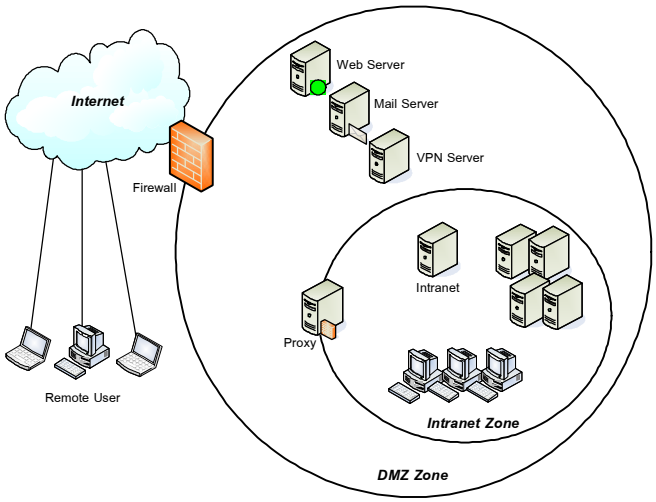
การทดสอบการใช้งาน กำหนดสถานที่ให้ดำเนินการจากเครือข่ายสาธารณะอย่างน้อย 3 สถานที่ ได้แก่ หน่วยงานเครือข่ายในมหาวิทยาลัย ศูนย์พันธุวิศวกรรมและเทคโนโลยีชีวภาพแห่งชาติและผ่านเครือข่าย ADSL (บ้านของกลุ่มตัวอย่าง) และมีการกำหนดเกณฑ์ในการให้คะแนนในเชิงคุณภาพ แบ่งได้เป็น 5 ระดับด้วยกัน ดังตารางที่ 3

ตารางที่ 3 เกณฑ์ในการให้คะแนนของแบบประเมินผล

คะแนน	ความหมาย
4.51 - 5.00	ระบบที่พัฒนาสามารถรองรับการใช้งานได้ดีมาก
3.51 - 4.50	ระบบที่พัฒนาสามารถรองรับการใช้งานได้ดี
2.51 - 3.50	ระบบที่พัฒนาสามารถรองรับการใช้งานได้ปานกลาง
1.51 - 2.50	ระบบที่พัฒนาสามารถรองรับการใช้งานได้น้อย
1.00 - 1.50	ระบบที่พัฒนาสามารถรองรับการใช้งานได้น้อยมาก

3. ผลการดำเนินงาน

ลักษณะของเครือข่ายที่พัฒนาตามที่แสดงในภาพที่ 2 ได้มีการเพิ่มเติมเครื่องแม่ข่ายวีพีเอ็น เพื่อการใช้งานผ่านเครือข่ายสาธารณะสามารถเข้าถึงเครือข่ายและข้อมูลภายใน (Intranet Zone) ได้ โดยอุปกรณ์ Firewall ของเครือข่ายเดิมจะทำการอนุญาตให้มีการเข้าถึงเครื่องแม่ข่ายวีพีเอ็น เพื่อทำการพิสูจน์สิทธิ์ หรือตรวจสอบการขอเข้าถึงข้อมูลเครือข่ายภายในหลังจากนั้นจึงจะสามารถทำการติดต่อโดยตรงระหว่างเครื่องลูกข่ายภายนอกกับเครื่องแม่ข่ายภายใน จนกระทั่งการเชื่อมต่อสิ้นสุดลง ทั้งนี้สิทธิการเข้าถึงข้อมูลภายใน ยังถูกกำหนดไว้เพียงเครื่องแม่ข่ายเครื่องเดียว (Intranet Web Server) ซึ่งมีข้อมูลข่าวสารและระบบที่จำเป็นต่อการทำงานจากภายนอกเท่านั้น เพื่อป้องกันการเข้าถึงข้อมูลภายในอื่นที่สำคัญและยังไม่มีความจำเป็นต้องใช้งานจากภายนอก



ภาพที่ 2 Network Diagram

ในส่วนของการติดตั้งโปรแกรม OpenVPN ที่ทำการติดตั้งเป็นโปรแกรมทำงานในลักษณะของ Router VPN ซึ่งทำให้ความสามารถในการรับส่งข้อมูล (Throughput) สูง มีคุณสมบัติในการจัดการการใช้งานในช่องทางที่มีอยู่ได้ดี โดยสามารถใช้งานผ่านช่องทางที่ติดต่อเข้ามา หรือใช้งานผ่านช่องทางของเครือข่ายหลักที่มีการติดต่อด้วยแทนช่องทางที่ติดต่อเข้ามาได้ สามารถใช้โปรแกรมตัวเดียวกันในการติดตั้งบนเครื่องแม่ข่ายและเครื่องลูกข่าย ทำให้การดูแลจัดการมีความยุ่งยากลดลงมากและสามารถติดตั้งได้ทั้งในระบบปฏิบัติการ Windows และ Linux ซึ่งมีการบริหารจัดการตามโครงสร้างมาตรฐานของ X.509 PKI (Public Key Infrastructure) ที่เป็นการทำงานร่วมกันในการใช้ใบรับรอง (Certificate) และกุญแจส่วนตัว (Private Key) และสนับสนุนการทำงานแบบการพิสูจน์สิทธิ์ 2 ทาง (Bidirectional Authentication) ในการตรวจสอบใบรับรอง ซึ่งหมายถึงมีการตรวจสอบทั้งจากเครื่องแม่ข่ายและการตรวจสอบจากเครื่องลูกข่าย เพื่อยืนยันตัวตนของทั้ง 2 ทาง ปัญหาที่พบจากการดำเนินการในขั้นตอนนี้คือ ปัญหาในการแก้ไขและกำหนดรายละเอียดในอุปกรณ์ Firewall ซึ่งมีความซับซ้อนและอ่อนไหวในการดำเนินการ ที่จะต้องไม่ให้ส่งผลกระทบกับระบบเครือข่ายที่ให้บริการอยู่

ส่วนการทดสอบระบบในขั้นแอลฟา (Alpha Stage) โดยผู้วิจัยเอง ผ่านเครื่องลูกข่ายที่ได้จัดเตรียมไว้ ทดสอบใช้งานทั้งแบบเครื่องเดียว แบบใช้งาน 2 เครื่องพร้อมกัน และทดสอบแบบใช้งาน 2 เครื่องพร้อมกันโดยใช้ใบรับรองเดียวกัน ได้ประเด็นที่ต้องคำนึงถึงดังนี้ 1) โปรแกรม OpenVPN ในเครื่องแม่ข่าย ถ้าเลือกใช้งานในระบบปฏิบัติการ Linux จะสามารถเพิ่มการพิสูจน์สิทธิ์ (Authenticate) ด้วยชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) กับผู้ใช้งานในระบบได้ 2) โปรแกรม OpenVPN ต้องการสิทธิในการจัดการแบบ Administrator ในเครื่องลูกข่าย 3) การจัดเก็บใบรับรองและกุญแจ สามารถย้ายสถานที่จากที่กำหนด ได้ทั้งในเครื่องแม่ข่ายและเครื่องลูกข่าย 4) โปรแกรม OpenVPN เวอร์ชัน 2.0.7 มีส่วนที่ผิดพลาด (Bug) ต้องติดตั้งใหม่ เมื่อใช้งานแล้ว 2 ถึง 3 ครั้ง และมีการแก้ไขในเวอร์ชัน 2.0.9 5) การเข้าใช้งานพร้อมกันและใช้ใบรับรองเดียวกัน ไม่สามารถทำงานได้พร้อมกัน และ 6) โปรแกรม OpenVPN สามารถกำหนดหมายเลขไอพี เครื่องแม่ข่ายที่จะเข้าถึงได้ทั้งเป็นเครื่องเดียวและกลุ่มของเครื่องแม่ข่าย

การทดสอบระบบในขั้นเบต้า (Beta Stage) จากที่กำหนดดำเนินการจากเครือข่ายสาธารณะ อย่างน้อย 3 สถานที่ ในการ

ดำเนินการจริงได้รับความร่วมมือจากกลุ่มตัวอย่าง 5 สถานที่ ได้แก่ หน่วยงานเครือข่ายในมหาวิทยาลัยเชียงใหม่ หน่วยงานเครือข่ายในมหาวิทยาลัยมหิดลศาลายา เครือข่าย ADSL (บ้านของกลุ่มตัวอย่าง) เครือข่ายของศูนย์พันธุวิศวกรรมและเทคโนโลยีชีวภาพแห่งชาติและเครือข่ายแลนไร้สาย (Wireless LANs) ของสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ รวมผลการทดสอบทั้งหมด 16 ท่าน

ผลความพึงพอใจทางคุณภาพจากกลุ่มผู้เชี่ยวชาญและผู้ดูแลระบบ ด้าน Usability Test หรือการทดสอบลักษณะการใช้งานของระบบ พบว่า ระบบมีความง่ายต่อการใช้งานคิดเป็น 4.33 ส่วนเบี่ยงเบนมาตรฐานเท่ากับ 0.56 ด้าน Performance Test หรือการทดสอบความถูกต้องและคุณภาพในการทำงานของระบบ พบว่า ระบบสามารถทำงานได้ตามหน้าที่คิดเป็น 4.42 ส่วนเบี่ยงเบนมาตรฐานเท่ากับ 0.58 และด้าน Security Test หรือการทดสอบการรักษาความปลอดภัยของระบบให้กับข้อมูลหรือระบบที่มีการใช้งานร่วม พบว่า ระบบมีความปลอดภัยคิดเป็น 4.00 ส่วนเบี่ยงเบนมาตรฐานเท่ากับ 0.84

ความพึงพอใจในการใช้งานของกลุ่มผู้ใช้งานทั่วไป ด้าน Requirement Test หรือการทดสอบความถูกต้องและคุณภาพของระบบ พบว่า ระบบสามารถตอบสนองความต้องการของผู้ใช้งานคิดเป็น 4.26 ส่วนเบี่ยงเบนมาตรฐานเท่ากับ 0.63 ด้าน Usability Test หรือการทดสอบลักษณะการใช้งานของระบบ พบว่า ระบบมีความง่ายต่อการใช้งานคิดเป็น 4.28 ส่วนเบี่ยงเบนมาตรฐานเท่ากับ 0.64 ด้าน Performance Test หรือมีการทดสอบความถูกต้องและคุณภาพในการทำงานของระบบ พบว่า ระบบสามารถทำงานได้ตามหน้าที่คิดเป็น 4.35 ส่วนเบี่ยงเบนมาตรฐานเท่ากับ 0.74

4. สรุป

การพัฒนา Virtual Private Network ของศูนย์เทคโนโลยีโลหะและวัสดุแห่งชาติ จัดทำขึ้นเพื่อเพิ่มช่องทางการสื่อสารที่เชื่อมต่อจากภายนอกผ่านเครือข่ายสาธารณะ หรือเทคโนโลยีระบบเครือข่ายรูปแบบใหม่ ให้สามารถใช้บริการข่าวสารและระบบภายในได้อย่างปลอดภัย ระบบที่พัฒนาขึ้น ทำการติดตั้งเครื่องแม่ข่ายวีพีเอ็น ที่ใช้โปรแกรม OpenVPN เวอร์ชัน 2.0 บนระบบปฏิบัติการ Windows เวอร์ชัน 2000 ในโซนเครื่องแม่ข่าย สำหรับการติดต่อสื่อสารกับเครือข่ายภายนอก (DMZ Zone) ในเครือข่ายของศูนย์เทคโนโลยีโลหะและวัสดุแห่งชาติ กำหนดและพิสูจน์สิทธิในการเข้าถึงเครื่องแม่ข่ายภายในโดยใช้ใบรับรองดิจิตอล (Digital Certificate) กำหนดเงื่อนไขรองรับการทำงานและตรวจสอบความปลอดภัย ตามระดับมาตรฐานของโปรแกรม

ระบบวีพีเอ็นที่พัฒนาขึ้นผ่านการประเมินความพึงพอใจโดยผู้ใช้ ได้คะแนนเฉลี่ยของความพึงพอใจจากกลุ่มตัวอย่างทั้ง 2 กลุ่มในระดับดี (3.51-4.50) ในทุกด้านที่มีการประเมินผลและมีค่าการกระจายตัวของข้อมูล (ส่วนเบี่ยงเบนมาตรฐาน) อยู่ในเกณฑ์ที่รับได้ (น้อยกว่า 1) แสดงว่า ระบบ Virtual Private Network ที่พัฒนาขึ้น มีคุณภาพในการใช้งานในระดับดี สามารถอำนวยความสะดวกในการเข้าถึงข้อมูลและระบบภายใน สอดคล้องกับขอบเขตความปลอดภัยที่กำหนดขึ้น สามารถนำไปประยุกต์ใช้ในการเชื่อมต่อ จากเครือข่ายสาธารณะ เข้าสู่เครือข่ายภายในและเพิ่มช่องทางการทำงานให้แก่บุคลากรของศูนย์เทคโนโลยีโลหะและวัสดุแห่งชาติได้จริง

โปรแกรม OpenVPN เป็นโปรแกรมประเภท Open Source ที่ผู้ใช้งานทั่วไปร่วมกันพัฒนา การเพิ่มเติมคุณสมบัติการทำงานใหม่ ๆ ให้กับโปรแกรมจากผู้พัฒนาแต่ละท่านอาจส่งผลกระทบกับส่วนอื่นของโปรแกรม เกิดเป็นข้อผิดพลาดดังที่ได้พบตั้งแต่การทดสอบขั้นตอนแรก ในขณะเดียวกันลักษณะการเป็นโปรแกรมประเภท Open Source ก็มีผลดีในแง่ของการปรับปรุงข้อบกพร่องที่มีอยู่อย่างรวดเร็ว ซึ่งพบจากการที่มีโปรแกรมเวอร์ชันใหม่ออกมาแก้ไขข้อบกพร่องระหว่างการทดสอบโปรแกรมในขั้นตอนแรก ดังนั้น แนวทางที่น่าสนใจต่อไปคือ การทดลองดัดแปลงรูปแบบการดำเนินการข้อกำหนดและรายละเอียดของคุณสมบัติของโปรแกรมให้มีความรัดกุม หรือเงื่อนไขในการทำงานเพิ่มขึ้น เพื่อที่จะสามารถปกป้องการเข้าถึงเครือข่ายได้อย่างมีคุณภาพและเหมาะสมกับการใช้งานร่วมกับข้อมูลในรูปแบบอื่น หรือเทคโนโลยีใหม่ หรือทำการพัฒนาโปรแกรม OpenVPN เพิ่มเติม แก้ไขข้อพร่อง หรือพัฒนาประสิทธิภาพการรองรับการทำงานให้กับโปรแกรม เพื่อประโยชน์ในการใช้งานต่อไป

5. เอกสารอ้างอิง

[1] CERT and CERT Coordination Center. “CERT/CC Statistics 1988-2006.” Available online at: http://www.cert.org/stats/cert_stats.html.

[2] สิริพร จิตต์เจริญธรรม, เสาวภา ปานจันทร์ และเลอศักดิ์ ลิ้มวิวัฒน์กุล. “ความรู้เบื้องต้นเกี่ยวกับการ

พิสูจน์ตัวตน" *ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ.* 2547.

[3] Khanvilkar, Shashank and Khokhar, Ashfaq. "Virtual Private Networks: An Overview with Performance Evaluation." *IEEE Communications Magazine.* (October 2004) : 146-154.

[4] Clercq, Jeremy De. and Paridaens, Olivier. "Scalability Implications of Virtual Private Networks." *IEEE Communications Magazine.* (May 2002) : 151-157.

[5] Venkateswaran, R. "Virtual private networks." *Lucent Technol. Bell Lab., IEEE,* Volume: 20, Issue: 1. (March 2001) : 11-15.