การพัฒนาระบบบริหารจัดการรักษาความปลอดภัย ของระบบเครือข่ายสารสนเทศภาครัฐ

The Development of Security Management Systems for Public Network System.

สำราญ วานนท์*

บทคัดย่อ

การวิจัยครั้งนี้มีวัตถุประสงค์ ดังนี้ 1) เพื่อหาแนวทางในการบริหารจัดการการป้องกันภัยคุกคามระบบเครือข่ายสารสนเทศภาครัฐ 2) เพื่อพัฒนาระบบบริหารจัดการรักษาความปลอดภัยของระบบเครือข่ายสารสนเทศภาครัฐ ประชากรและกลุ่มตัวอย่างเป็นบุคลากรและนักศึกษามหาวิทยาลัยราชภัฏชัยภูมิที่มาใช้บริการอินเทอร์เน็ตบริเวณลานพวงชมพู อาคารศูนย์ภาษาและเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏชัยภูมิ จำนวน 30 คน เครื่องมือที่ใช้ในการวิจัยไฟร์วอลล์โอเพ่นซอร์สพีเอฟเซนต์และแบบสอบถามเพื่อวัดความพึงพอใจ สถิติที่ใช้ในงานวิจัยได้แก่ จำนวน ร้อยละ ค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐาน ผลการวิจัยมีดังนี้ ส่วนใหญ่ผู้ใช้เครือข่ายสารสนเทศเป็นนักศึกษาเพศหญิง ช่วงอายุ 20-30 ปี มีวัตถุประสงค์เพื่อเช็ค Mail /Chat ความถี่ที่ใช้งานจะอยู่ที่ 5 วันต่อสัปดาห์ ความเร็วที่ใช้เครือข่ายอยู่ในระดับเร็ว มีความพึงพอใจในภาพรวมต่อการพัฒนาระบบบริหารจัดการรักษาความปลอดภัยของระบบเครือข่ายสารสนเทศภาครัฐ อยู่ในระดับมาก ($\overline{X}$ = 4.27, S.D. = 0.68)

คำสำคัญ: ความปลอดภัยของระบบเครือข่าย, ไฟร์วอลล์

ABSTRACT

The purposes of the research were 1) to find out to management of prevention threats for public network systems 2) to develop the security management for public network systems. The sample group of this study was personnel and students of Chaiyaphum Rajabhat University using the internet service at Puangkompoo area of Computer and Language Center building of 30 samples. By using the following tools to develop open source pfSense firewall and satisfaction questionnaire. The statistics that was

* อาจารย์ประจำคณะบริหารธุรกิจ มหาวิทยาลัยราชภัฏชัยภูมิ

used are percentages, mean and standard deviation. The results of the study were as follows. Most of the information network users were female students. The age between 20-30 years. The purpose was to check mails / chats. The most frequency of uses was 5 days per week. The speed of information network was at the fast level. Overall satisfaction with the development of security management systems for public network system was at the high level ($\overline{X}$ = 4.27, S.D. = 0.68).

Keyword: Network security systems, Firewall

บทนำ

ในช่วงหลายปีที่ผ่านไปนั้น ได้มีวิวัฒนาการหรือเหตุการณ์ต่างๆ มากมายเกี่ยวกับภัยคุกคามทางระบบคอมพิวเตอร์ ที่ทำให้ผู้ที่มีหน้าที่ดูแลระบบเกิดความตระหนักในระบบเครือข่ายสารสนเทศมากยิ่งขึ้น นั่นคือ เหตุการณ์โจมตี ระบบเครือข่ายของธนาคารในประเทศเกาหลีใต้ และสถานีโทรทัศน์อีก 3 แห่ง ส่งผลให้ระบบเครือข่ายสารสนเทศไม่สามารถออนไลน์ได้ สร้างความเสียหายให้กับธุรกิจเป็นอย่างมาก จากการกระทำของผู้ไม่ประสงค์ดี ซึ่งทำให้เกิดการตื่นตัวครั้งใหญ่ ในความมั่นคงของสถาบันการเงินและองค์กรต่าง ๆ เป็นอย่างมาก เนื่องจากยักษ์ใหญ่ด้านเทคโนโลยีสารสนเทศ อย่างประเทศเกาหลีใต้ ที่มีมาตรฐานการรักษาความปลอดภัยระบบสารสนเทศ (IT Security) ในระดับแนวหน้าของโลก ยังสามารถโดนเจาะเข้าระบบที่สำคัญอย่างธนาคาร และสถานีโทรทัศน์ได้ การพัฒนาป้องกันระบบเครือข่าย การเฝ้าระวัง และการให้ความรู้ในการใช้งานเครือข่ายจึงเป็นส่วนที่สำคัญยิ่งสำหรับองค์กร ในปัจจุบัน แนวโน้มของภัยคุกคามทางสารสนเทศ ในปี พ.ศ.2558 คงหนีไม่พ้นการโจมตีรูปแบบ Advanced Persistent Threat (APT) การโจมตีแบบ Denial Of Service Attacks (DOS) ที่ผู้ใช้ องค์กรต้องเตรียมการรับมือ รวมถึง Bring your own device (BYOD) ที่มีส่วนเข้ามาในองค์กรในปัจจุบันเป็นอย่างมาก

ปัจจุบันคนไอทียุคนี้ต้องรู้จัก “Cloud Computing” โดยเฉพาะ Personal Cloud ที่เป็นการใช้ Storage as a Service (SaaS) ซึ่งเป็นวิธีการหนึ่งที่ผู้ใช้งานสามารถเรียกใช้งานซอฟแวร์ (Software) ผ่านเครือข่ายอินเทอร์เน็ต (Internet)โดยไม่ต้องทำการติดตั้งซอฟแวร์ (Install)และดูแลรักษา (Maintenance) อย่างเช่น การต้องมาคอย สำรองข้อมูล (Backup) ข้อมูลป้องกันข้อมูลสูญหาย เป็นต้น จะเห็นว่าแนวคิดบริการ SaaS สร้างขึ้นมาเพื่อความสะดวก ซึ่งจะทำให้ผู้ใช้เพียงแค่เชื่อมต่อเครือข่ายก็สามารถใช้งานได้โดยไม่ต้อง สนใจความซับซ้อนภายในของซอฟแวร์ และยังไม่ต้องสนใจการดูแลรักษาฮาร์ดแวร์อีกด้วย ยกตัวอย่าง SaaS ที่รู้จักกัน อาทิเช่น Dropbox, iCloud หรือ Google Drive ซึ่งจริง ๆ แล้ว บริการประเภทนี้ได้ถือกำเนิดขึ้นเมื่อประมาณ 7 ปีที่แล้ว ซึ่งในปัจจุบันก็ได้กลายเป็นส่วนหนึ่งของผู้คนไอทียุคนี้ไปเสียแล้ว

อย่างไรก็ตาม แม้เทคโนโลยี Cloud นั้น จะให้อรรถประโยชน์แก่ผู้ใช้งานและองค์กรอยู่มาก แต่ในรายงานและผลสำรวจที่มาจากบริษัทวิจัยชั้นนำระดับโลกต่างๆ พบว่าประเด็นที่ CIO ในหลายบริษัท ต่างกังวลเกี่ยวกับการปรับเปลี่ยนระบบไอทีแบบฟิสิคัลไปสู่โลกเสมือนและคลาวด์ คือเรื่องของ“ความปลอดภัย” ที่ยังเป็นคำถามคาใจแก่ผู้บริหารและผู้ดูแลระบบไอทีอยู่โดยตลอด หากวิเคราะห์กันลงลึกไปอีกระดับแล้วจะพบว่า ความกังวลใจขององค์กรต่างๆ เหล่านั้นเกิดจากวิธีการแก้ไขปัญหาในการป้องกันภัยคุกคามยุคเก่าขององค์กร ที่ไม่สามารถจะปรับตัวเพื่อป้องกันภัยคุกคามให้กับสภาพแวดล้อมระบบไอทีที่เปลี่ยนไปสู่โลกของ Visualization และ Cloud ได้นั่นเอง ที่เป็นเช่นนั้นเพราะมีปัจจัยหลายๆอย่างเช่น เทคโนโลยีความปลอดภัยที่ยังล้าหลัง วิธีการแก้ไขปัญหาที่ไม่เข้าใจในสภาวะการเปลี่ยนผ่านระบบขององค์กร โครงสร้างของซอฟต์แวร์ไม่เอื้ออำนวย เป็นต้น ประเด็นทั้งหมดทำให้วิธีการแก้ไขปัญหาความปลอดภัยแบบเดิมไม่สามารถที่จะทำงานสอดคล้องไปกับโลกของ Visualization และCloud ได้ส่งผลให้เกิด“ช่องโหว่”ของระบบเครือข่ายสารสนเทศอย่างหลีกเลี่ยงไม่ได้

ในบริบทด้านการป้องกันและปราบปรามภัยคุกคามที่อาจจะเกิดขึ้นในแวดวงระบบเครือข่ายสารสนเทศสำหรับประเทศไทย รัฐบาลได้มีการพัฒนากฎหมายที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศและการสื่อสารขึ้นโดยมีวัตถุประสงค์เพื่อให้ประเทศมีโครงสร้างพื้นฐานทางกฎหมายรองรับสังคมสารสนเทศ ซึ่งถือเป็นปัจจัยสำคัญของการดำรงอยู่ของสังคมในศตวรรษที่ 21 ใน พ.ศ.2540 คณะรัฐมนตรีได้เห็นชอบให้มีการพัฒนากฎหมายเทคโนโลยีสารสนเทศขึ้น 6 ฉบับ โดย 3 ฉบับแรก เป็นกฎหมายที่ส่งเสริมการประยุกต์ใช้เทคโนโลยีสารสนเทศและการสื่อสารในเชิง สร้างสรรค์ อันเอื้อต่อการทำธุรกรรมทางอิเล็กทรอนิกส์หรือพาณิชย์อิเล็กทรอนิกส์ หรือการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ ส่วนกฎหมายในลำดับที่ 4 และลำดับ 5 เป็นกฎหมายที่จะใช้เป็นมาตรการในการคุ้มครองหรือปกป้องสังคมจากการประยุกต์ ใช้เทคโนโลยีสารสนเทศและการสื่อสารในเชิงไม่สร้างสรรค์ และฉบับสุดท้ายเป็นกฎหมายฉบับที่จะสร้างกลไกเพื่อลดความเหลื่อมล้ำของสังคมสารสนเทศ โดย กฎหมายว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ได้จัดทำขึ้นเพื่อกำหนดฐานความผิดและบทลงโทษสำหรับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์และกำหนดอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ ซึ่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ได้จัดทำขึ้นเพื่อคุ้มครองสิทธิขั้นพื้นฐานในความเป็นส่วนตัว โดยมุ่งคุ้มครองข้อมูลส่วนบุคคล ที่อาจมีการละเมิดและสามารถนำไปใช้ในทางมิชอบได้โดยง่าย (ในการทำธุรกรรมทางออนไลน์หรือการใช้อินเทอร์เน็ต) ส่วนสาระสำคัญที่เกี่ยวข้องกับองค์กรที่ให้บริการด้านเทคโนโลยีเครือข่ายคอมพิวเตอร์มี ดังนี้

มาตรา 3 ในพระราชบัญญัติฯ

“ระบบคอมพิวเตอร์” หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์ หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

จากพระราชบัญญัติฯ ดังกล่าวจะเห็นได้ว่าองค์กรที่เป็นผู้ให้บริการตามนิยามในกฎหมายฉบับนี้จำเป็นต้องมีการจัดเตรียมระบบการพิสูจน์ตัวตนก่อนเข้าใช้งานเครือข่ายอินเทอร์เน็ต การจัดเก็บข้อมูลผู้ใช้งานอินเทอร์เน็ต การป้องกันการถูกโจมตีจากผู้ไม่ประสงค์ดีทั้งจากภายในและภายนอกองค์กร

ดังนั้น จากที่ได้กล่าวมาแล้วข้างต้นทำให้เห็นได้อย่างชัดเจนว่า สิ่งที่เป็นการเชื่อมโยงเครือข่ายสังคมออนไลน์ การเชื่อมต่ออยู่ใกล้เข้ามามากขึ้นทุกที ข้อมูลองค์กร ข้อมูลส่วนตัว อาจไม่เป็นข้อมูลที่ส่วนตัวอีกต่อไป การใช้ช่องโหว่เพื่อเจาะเข้าหาข้อมูลส่วนบุคคล อาจนำไปสู่การเข้าถึงของข้อมูลขององค์กรได้ หากไม่มีนโยบายในการบริหารจัดการหรือแนวทางการป้องกันภัยคุกคามที่นำไปสู่การปฏิบัติอย่างเป็นรูปธรรม ดังนั้นแล้วการจัดเตรียมระบบความปลอดภัยทางเครือข่ายสารสนเทศขององค์กรและการให้ความรู้ความเข้าใจกับผู้ใช้ ให้ตระหนักถึงข้อควรคำนึงในการเข้าถึงข้อมูล และการใช้งานระบบเครือข่ายสารสนเทศ จึงเป็นสิ่งเร่งด่วนและจำเป็นอย่างมากขององค์กร คณะผู้วิจัยจึงมีความสนใจที่จะทำการศึกษาและพัฒนาระบบป้องกันรักษาความปลอดภัยทางระบบเครือข่ายสารสนเทศขององค์กรภาครัฐ เพื่อให้สอดคล้องเป็นไปตามที่กฎหมายกำหนด เกิดประโยชน์ต่อองค์กร ลดค่าใช้จ่ายจากงบประมาณด้านการจัดซื้อระบบรักษาความปลอดภัยเครือข่ายฯ และเป็นแนวทางในการศึกษาทางด้านการรักษาความปลอดภัยในเครือข่ายระบบสารสนเทศต่อไป

วัตถุประสงค์การวิจัย

1. เพื่อหาแนวทางในการบริหารจัดการการป้องกันภัยคุกคามระบบเครือข่ายสารสนเทศภาครัฐ
2. เพื่อพัฒนาระบบบริหารจัดการรักษาความปลอดภัยของระบบเครือข่ายสารสนเทศภาครัฐ

เอกสารและงานวิจัยที่เกี่ยวข้อง

ศราวุฒิ จันทะคัด (2554 :บทคัดย่อ) วิจัยเรื่อง การจัดการความปลอดภัยภายในเครือข่ายคอมพิวเตอร์ กรณีศึกษา : บริษัทแซนด์แอนด์ซอยล์อุตสาหกรรม จำกัด ผลการวิจัย ได้นำ pfSense เข้ามาจัดการความปลอดให้กับบริษัท แซนด์แอนด์ซอยล์ สอดคล้องกับนโยบายของบริษัทที่จะจัดทำขึ้น ระบบคอมพิวเตอร์ภายในบริษัท แซนด์แอนด์ซอยล์จากเดิมมีระบบ Firewall เพียงสำนักงานใหญ่เท่านั้น แต่สาขาย่อยสองแห่งนั้นยังไม่มี Firewall ในการจัดการข้อมูลภายในเครือข่ายคอมพิวเตอร์

อนันต์ บัณฑุเดช (มปป.) วิจัยเรื่อง การประเมินประสิทธิภาพการป้องกันภัยคุกคามด้วยฮาร์ดแวร์ซอฟต์แวร์ และโอเพ่นซอร์สไฟวอลล์ ผลการวิจัย การประเมินประสิทธิภาพการป้องกันภัยคุกคามด้วยฮาร์ดแวร์ ซอฟต์แวร์และโอเพ่นซอร์สไฟวอลล์ คือการศึกษาถึงความสามารถในการทำงานของตัวอุปกรณ์ที่นำมาใช้งานและมีความสามารถเป็นที่ยอมรับอยู่ในองค์กร ในการจัดการปัญหาต่างๆจากภัยคุกคามในรูปแบบต่างๆ จากผู้ประสงค์ร้ายที่ใช้ช่องทางจากเครือข่ายและช่องโหว่ของระบบของหน่วยงานหรือองค์กรที่

ขาดการป้องกันอย่างดี เพื่อบุกรุกเข้ามาล้วงข้อมูลที่เป็นความลับซึ่งมีความสำคัญ และเพื่อแก้ปัญหาผลกระทบในด้านความมั่นคงปลอดภัย อุปกรณ์ฮาร์ดแวร์ซอฟต์แวร์และโอเพ่นซอร์สไฟวอลล์ จึงอาจเป็นอุปกรณ์เริ่มต้น ตัวหนึ่งในการเสนอแนวคิดยุคที่ต้องการให้ข้อมูลข่าวสารมีความปลอดภัย เพื่อเป็นการจัดการ

ศุภพร รัฐอาจและคณะ (มปป) วิจัยเรื่อง การปรับแต่งไฟร์วอลล์โอเพ่นซอร์สให้มีประสิทธิภาพสูงสุด ไฟล์วอลล์ ผลการวิจัยเป็นระบบที่มีความปลอดภัยเป็นอย่างยิ่งที่ใช้สำหรับควบคุมการไหลของข้อมูลบนเครือข่ายคอมพิวเตอร์ นับว่าเป็นสิ่งที่สำคัญมากต่อการรักษาความปลอดภัยภายในองค์กร อย่างไรก็ตามไฟล์วอลล์ในเชิงพาณิชย์โดยทั่วไปแล้วจะมีราคาแพง (ประมาณ 100,000 ถึง 1,000,000 บาท) จะเห็นว่าไฟล์วอลล์แบบโอเพ่นซอร์สโดยทั่วไปแล้วจะมีประสิทธิภาพการทำงานที่ต่ำ อีกทั้งยังมีการออกแบบส่วนติดต่อผู้ใช้งานที่ยากต่อการใช้งาน งานวิจัยฉบับนี้จึงมุ้งเน้น ไปทางด้านการพัฒนาไฟล์วอลล์แบบโอเพ่นซอร์สให้มี ประสิทธิภาพการใช้งานสูงและมีส่วนติดต่อผู้ใช้งานที่ดี ไฟลล์วอลล์ในรูปแบบใหม่นี้เรียกว่า HIFAF ซึ่งได้พัฒนาในเรื่องของการใช้ ipset, iptables, l7filter, java และ sqlite HIFAF มีจุดมุ่งหมายเพื่อพัฒนาให้มีประสิทธิภาพในการตรวจจับแพ็กเกจ (ประสิทธิภาพการใช้งานสูง) มีความยดยุ่นต่อการบริหารจัดการและง่ายต่อการใช้งาน (เป็นมิตรกับผู้ใช้งาน) ทั้งนี้ กฎของวอลล์ก็สามารถที่จะติดตามและตรวจสอบในส่วนของผู้ที่เคยลงชื่อเข้าใช้งานระบบอีกด้วย

วงศกร เสนาะดนตรี (2554:บทคัดย่อ) วิจัยเรื่อง การเปรียบเทียบประสิทธิภาพลินุกซ์ไฟร์วอลล์สำหรับเครือข่ายขนาดเล็ก ผลการวิจัยการดูแลระบบเครือข่าย สิ่งหนึ่งที่สำคัญ คือ การดูแลความปลอดภัยในระบบเครือข่ายคอมพิวเตอร์ แต่ด้วยงบประมาณที่จำกัด ลินุกซ์ไฟร์วอลล์เป็นอีกหนึ่งทางเลือกในการดูแลระบบความปลอดภัยในระบบเครือข่ายขนาดเล็ก แต่เนื่องด้วยลินุกซ์ไฟร์วอลล์เป็นจำนวนมาก แต่เราไม่สามารถทราบถึงประสิทธิภาพของลินุกซ์ไฟร์วอลล์แต่ละตัวนั้นมีประสิทธิภาพในการทำงานเป็น อย่างไรจึงทำให้เกิดเป็นปัญหาพิเศษในหัวข้อ การเปรียบเทียบประสิทธิภาพลินุกซ์ไฟร์วอลล์สำหรับเครือข่ายขนาดเล็กโดยเลือกลินุกซ์ไฟร์วอลล์ที่ได้รับความนิยมในการใช้งาน 3 ระบบปฏิบัติการ คือ ไอพีคอร์ป เอ็นเดรียนไฟร์วอลล์คอมมิวทิตี้ และพีเอฟเซนต์ มาทำการ ตรวจสอบตามหลักการตรวจสอบระบบสารสนเทศของสถาบัน SANS ทั้งในส่วนการตรวจสอบการดูแลเครือข่ายและการตรวจสอบการทนทานต่อการโจมตีเมื่อการทดสอบเสร็จสิ้นสามารถสรุปได้ว่า ในหัวข้อการดูแลเครือข่ายนั้นทั้ง 3 ระบบปฏิบัติการผ่านการทดสอบตามเกณฑ์มาตรฐานโดยมีไอพีคอร์ปทำงานมีประสิทธิภาพดีที่สุด แต่ในส่วนของหัวข้อการทนทานต่อการโจมตี ทั้ง 3 ระบบปฏิบัติการ ไม่ผ่านการทดสอบเนื่องจากส่วนใหญ่ถึงจะสามารถป้องกันการโจมตีได้แต่ไม่มีรายงานการโจมตี จึงถือว่าไม่ปลอดภัยต่อเครือข่าย มีเพียงพีเอฟเซนต์ที่สามารถผ่านหัวข้อการทดสอบได้มากที่สุด จากงานวิจัยจึงสรุปได้ว่าลินุกซ์ไฟร์วอลล์นั้นมีความสามารถเพียงพอในการดูแลระบบเครือข่ายแต่ยังไม่มีความสามารถเพียงพอต่อการทนทานต่อการโจมตี หากต้องการใช้งานไฟร์วอลล์เพื่อป้องกันการโจมตีควรใช้ฮาร์ดแวร์ไฟร์วอลล์

วิธีดำเนินการวิจัย

ในการวิจัยครั้งนี้เป็นการวิจัยเชิงทดลอง เพื่อการพัฒนาระบบบริหารจัดการรักษาความปลอดภัยของระบบเครือข่ายสารสนเทศภาครัฐและศึกษาความพึงพอใจของผู้ใช้งานระบบ ซึ่งผู้วิจัยได้ดำเนินการศึกษารายละเอียดเกี่ยวกับวิธีดำเนินการวิจัยและได้นำเสนอเป็นหัวข้อตามลำดับ ดังนี้

1. ประชากรและกลุ่มตัวอย่าง

1.1. ประชากร

ประชากรที่ใช้ในการศึกษาครั้งนี้ คือ บุคลากรและนักศึกษาที่มาใช้บริการอินเทอร์เน็ตบริเวณลานพวงชมพู อาคารศูนย์ภาษาและเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏชัยภูมิ

1.2 กลุ่มตัวอย่าง

กลุ่มตัวอย่างที่ใช้ในการศึกษาวิจัยในครั้งนี้ คือ บุคลากรและนักศึกษาที่มาใช้บริการอินเทอร์เน็ตบริเวณลานพวงชมพู อาคารศูนย์ภาษาและเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏชัยภูมิ จำนวน 30 คน โดยใช้วิธีเลือกแบบเจาะจง (Purposive Sampling)

2. เครื่องมือในการวิจัย

2.1 ไฟร์วอลล์โอเพ่นซอร์สพีเอฟเซนต์

2.2 แบบสอบถามเพื่อวัดความพึงพอใจของบุคลากรและนักศึกษาที่มาใช้บริการอินเทอร์เน็ตบริเวณลานพวงชมพู อาคารศูนย์ภาษาและเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏชัยภูมิ

3. การสร้างและหาคุณภาพเครื่องมือการวิจัย

3.1 ศึกษาและรวบรวมข้อมูลสำหรับการใช้งานไฟร์วอลล์โอเพ่นซอร์สพีเอฟเซนต์ ซึ่งมีขั้นตอนดังนี้

1) ศึกษาการติดตั้งและใช้งานระบบไฟร์วอลล์

2) ศึกษาการกำหนดนโยบายความปลอดภัยเครือข่าย

3) ศึกษามาตรฐานในการตรวจสอบไฟร์วอลล์

4) ศึกษาการใช้เครื่องมือทดสอบและตรวจที่อยู่ในที่ใช้ในการทดสอบไฟร์วอลล์

3.2 ติดตั้งระบบไฟร์วอลล์โอเพ่นซอร์สพีเอฟเซนต์

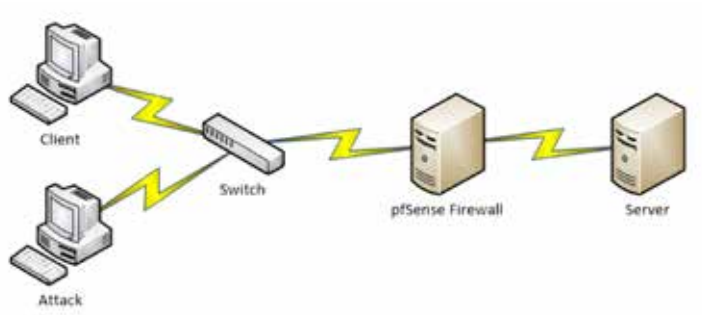
3.3 ทดสอบไฟร์วอลล์

โดยจำลองเครือข่ายคอมพิวเตอร์ออกเป็น 3 ส่วนดังต่อไปนี้

1) ส่วนที่เป็นเครื่องแม่ข่าย (Server) ให้บริการทรัพยากรต่าง เช่น Web Server (HTTP), Database Server หรือ File Server (FTP) เป็นต้น

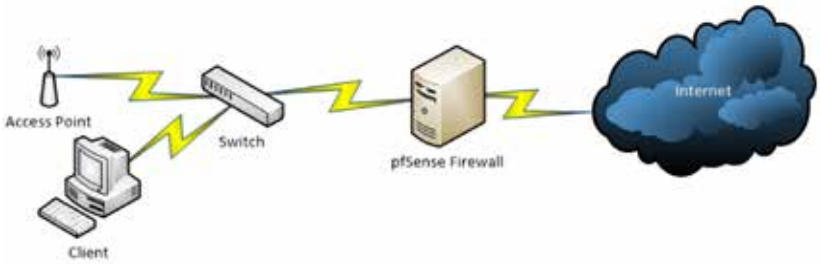
2) ส่วนที่เป็นเครื่องไฟร์วอลล์โอเพ่นซอร์สพีเอฟเซนต์สำหรับป้องกันเครือข่าย

3) ส่วนที่เป็นผู้ขอใช้บริการจะมีเครื่องลูก (Client) และเครื่องสำหรับทำหน้าที่โจมตี (Attack)



ภาพที่ 1 แสดงเครือข่ายคอมพิวเตอร์สำหรับทดสอบระบบไฟร์วอลล์

3.4 ทดสอบระบบไฟร์วอลล์สำหรับการใช้งานจริงบริเวณลานพวงชมพูโดยการเชื่อมต่อกับจุดให้บริการเครือข่ายแบบไร้สาย (Access Point) กับโลกอินเทอร์เน็ต



ภาพที่ 2 แสดงเครือข่ายคอมพิวเตอร์สำหรับทดสอบระบบไฟร์วอลล์สำหรับใช้งานอินเทอร์เน็ต

จากภาพที่ 2 จะประกอบด้วย 2 เครือข่ายดังนี้ 1) เครือข่ายที่อยู่หลังไฟร์วอลล์ซึ่งมี IP Address 192.168.100.10/24 เป็นเครือข่ายภายใน 2) เครือข่ายที่อยู่ภายนอกไฟร์วอลล์หรืออินเทอร์เน็ต

4. การเก็บรวบรวมข้อมูล

การดำเนินการทดลองให้กลุ่มตัวอย่างทดลองใช้งานอินเทอร์เน็ตผ่านระบบไฟร์วอลล์ที่จัดเตรียมไว้แล้วทำแบบวัดความพึงพอใจต่อระบบในช่วงเวลาที่ผู้วิจัยกำหนด

5. การวิเคราะห์ข้อมูล

การวิเคราะห์ข้อมูลของการวิจัยครั้งนี้มีขั้นตอนการวิเคราะห์ดังนี้

5.1 ข้อมูลทั่วไปของกลุ่มตัวอย่างประกอบด้วยข้อมูลสถานะของกลุ่มตัวอย่างและประสบการณ์ในการใช้งานอินเทอร์เน็ต วิเคราะห์ข้อมูลโดยการแจกแจงความถี่ และหาค่าร้อยละ

5.2 ข้อมูลความพึงพอใจต่อการใช้ระบบไฟร์วอลล์ วิเคราะห์ข้อมูลโดยการแจกแจงความถี่ หาค่าร้อยละ ค่าเฉลี่ย ($\overline{X}$) และส่วนเบี่ยงเบนมาตรฐาน (S.D.) โดยหาค่าคะแนนเฉลี่ยภาพรวม รายด้านและรายข้อซึ่งมีค่าคะแนนดังนี้คะแนนเฉลี่ย 4.51–5.00 หมายถึง ระดับมากที่สุดคะแนนเฉลี่ย 3.51 – 4.50 หมายถึง ระดับมากคะแนนเฉลี่ย 2.51 – 3.50 หมายถึง ระดับปานกลางคะแนนเฉลี่ย 1.51 – 2.50 หมายถึง ระดับน้อยคะแนนเฉลี่ย 1.00 – 1.50 หมายถึง ระดับน้อยที่สุด

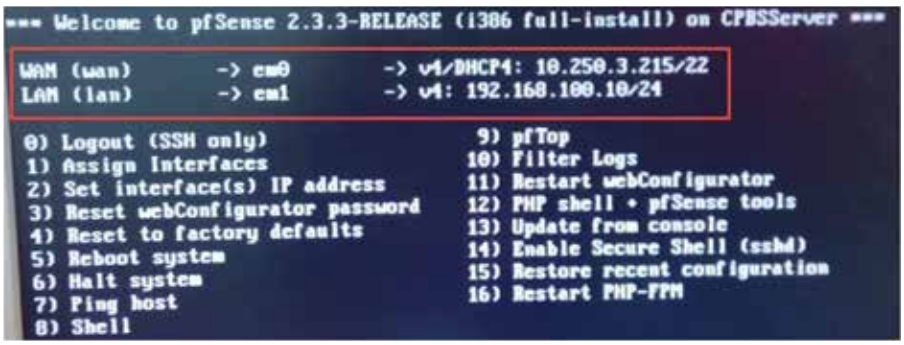
5.3 ข้อมูลที่ได้จากข้อเสนอแนะ ซึ่งมีลักษณะเป็นความคิดเห็น และข้อเสนอแนะนำเสนอในลักษณะข้อมูลเชิงคุณภาพ

ผลการวิจัย

จากการศึกษาข้อมูล วิเคราะห์ ออกแบบ พัฒนาระบบบริหารจัดการรักษาความปลอดภัยของระบบเครือข่ายสารสนเทศและเพื่อศึกษาความพึงพอใจของผู้ใช้งานระบบมีผลการวิจัย ดังนี้

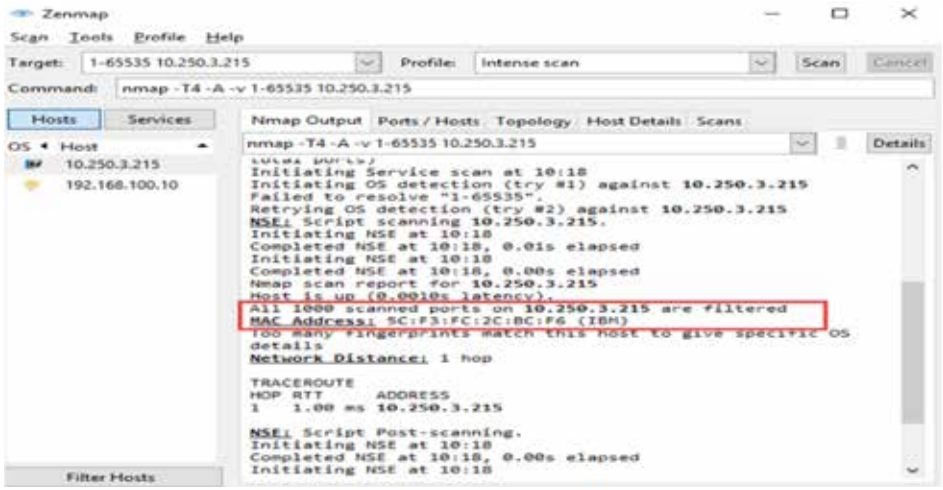
1. ผลการทดสอบไฟร์วอลล์

1.1 กำหนดค่าให้กับไฟร์วอลล์พีเอฟเซนต์ IP WAN คือ 10.250.3.215/22 ส่วน IP LAN คือ 192.168.100.10/24 ดังภาพที่ 3



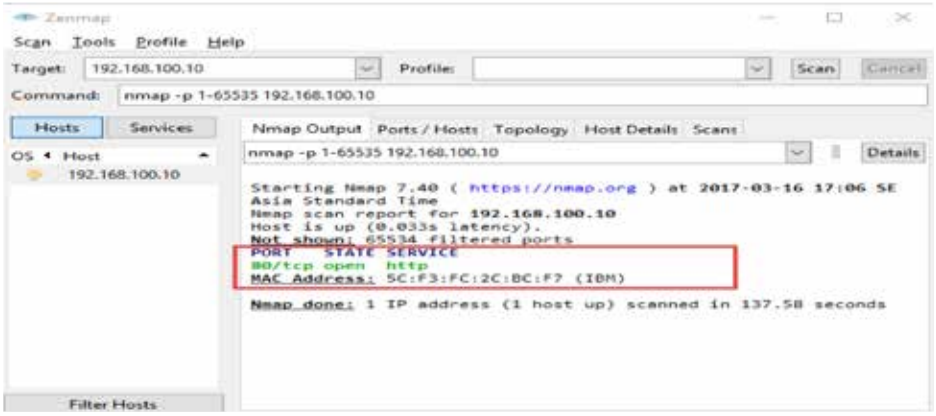
ภาพที่ 3 กำหนดค่าให้กับไฟร์วอลล์พีเอฟเซนต์

1.2 ทดสอบการเปิดพอร์ตจากภายนอกเครือข่ายว่าเปิดพอร์ตไว้หรือไม่จากผลการทดสอบพบว่าไม่มีพอร์ตใดเปิดอยู่ ดังภาพที่ 4



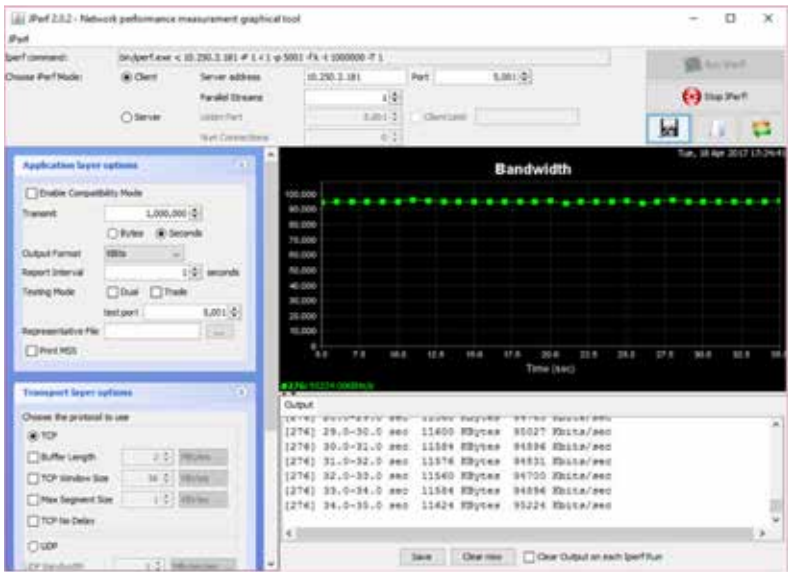
ภาพที่ 4 แสดงผลการเปิดพอร์ตของไฟร์วอลล์จากภายนอก

1.3 ทดสอบการเปิดพอร์ตจากภายในเครือข่ายเดียวกันว่าเปิดพอร์ตไว้หรือไม่จากผลการทดสอบพบว่าไม่มีพอร์ตใดเปิดอยู่ ยกเว้นพอร์ต 80 ยังเปิดเพื่อใช้งานบริหารจัดการไฟร์วอลล์ ดังภาพที่ 5



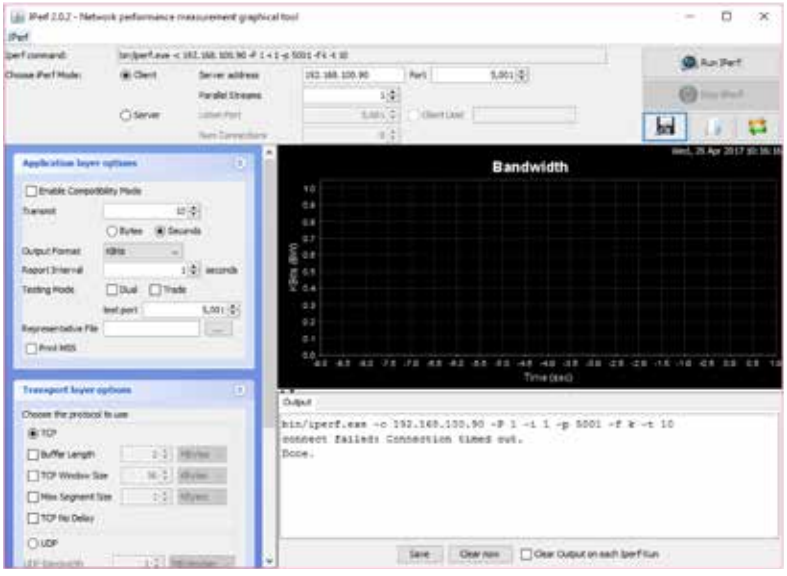
ภาพที่ 5 แสดงผลการเปิดพอร์ตของไฟร์วอลล์จากภายใน

.1.4 ทดสอบการส่งผ่านข้อมูลจากเครื่องที่อยู่หลังไฟร์วอลล์พีเอฟเซนต์ส่งข้อมูลไปยังเครื่องที่อยู่นอกเครือข่ายไฟร์วอลล์พีเอฟเซนต์ จากผลการทดสอบพบว่าไฟร์วอลล์ทำงานได้ถูกต้องตามกฎ ขนาดของ Bandwidth อยู่ในระดับที่สูง ดังภาพที่ 6



ภาพที่ 6 แสดงผลการทดสอบการส่งผ่านข้อมูลอยู่ภายในไฟร์วอลล์พีเอฟเซนต์ส่งข้อมูลไปยังเครื่องที่อยู่นอกเครือข่ายไฟร์วอลล์พีเอฟเซนต์

1.5 ทดสอบการส่งผ่านข้อมูลจากเครื่องที่อยู่ภายนอกไฟร์วอลล์พีเอฟเซนต์ส่งข้อมูลไปยังเครื่องที่อยู่ภายในเครือข่ายไฟร์วอลล์พีเอฟเซนต์ จากผลการทดสอบพบว่าไฟร์วอลล์ทำงานได้ถูกต้องตามกฎ ดังตัวอย่างไม่เปิดพอร์ต 5001 ดังภาพที่ 7



ภาพที่ 7 แสดงผลการทดสอบการส่งผ่านข้อมูลจากเครื่องที่อยู่นอกเครือข่ายไฟร์วอลล์พีเอฟเซนต์ไปยังเครื่องที่อยู่ภายในเครือข่ายไฟร์วอลล์พีเอฟเซนต์

2. ผลการศึกษาความพึงพอใจของบุคลากรและนักศึกษาที่มาใช้บริการอินเทอร์เน็ตบริเวณลานพวงชมพู อาคารศูนย์ภาษาและเทคโนโลยีสารสนเทศ

ผลการวิเคราะห์ข้อมูลเกี่ยวกับความพึงพอใจเกี่ยวกับการใช้ระบบเครือข่ายของผู้ตอบแบบสอบถามผู้ใช้บริการอินเทอร์เน็ตบริเวณลานพวงชมพู อาคารศูนย์ภาษาและเทคโนโลยีสารสนเทศ พบว่าผู้ตอบแบบสอบถามมีความพึงพอใจระบบเครือข่ายโดยรวมอยู่ในระดับมาก ($\overline{X}$ = 4.27) และเมื่อพิจารณาเป็นรายข้อพบว่าอยู่ในระดับมากทั้งหมดคือ การใช้งานระบบเครือข่ายอินเทอร์เน็ตในการใช้สืบค้นข้อมูล ($\overline{X}$ =4.47) ประสิทธิภาพของการใช้งานระบบเครือข่าย ($\overline{X}$ =4.40) ความพึงพอใจโดยภาพรวมในการใช้บริการเครือข่าย ($\overline{X}$ =4.27) การใช้งานระบบเครือข่ายอินเทอร์เน็ตในการใช้ Social Network ($\overline{X}$ =4.37) ความพึงพอใจโดยภาพรวมในการใช้บริการเครือข่ายอินเทอร์เน็ต ($\overline{X}$ =4.37) ไม่พบการปัญหาการโจมตี/ไวรัส/มัลแวร์ บนเครือข่าย ($\overline{X}$ =4.23) ความง่ายในการเชื่อมต่อเครือข่ายอินเทอร์เน็ต ($\overline{X}$ =4.20) การใช้งานระบบเครือข่ายอินเทอร์เน็ตในการ Download/Upload ข้อมูล ($\overline{X}$ =4.20) เสถียรภาพของระบบเครือข่ายในการรับ/ส่ง/สื่อสารข้อมูล ($\overline{X}$ =4.13) และความเร็วในการใช้งานเครือข่ายอินเทอร์เน็ต ($\overline{X}$ = 4.07) ตามลำดับรายละเอียดแสดงดังตารางที่ 1

ตารางที่ 1 ค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐานของผู้ตอบแบบสอบถามผู้ใช้บริการอินเทอร์เน็ตบริเวณลานพวงชมพู อาคารศูนย์ภาษาและเทคโนโลยีสารสนเทศที่มีความพึงพอใจเกี่ยวกับระบบเครือข่ายอินเทอร์เน็ต

ความพึงพอใจเกี่ยวกับการใช้ระบบเครือข่าย	$\overline{X}$	S.D.	แปลความ
1. ประสิทธิภาพของการใช้งานระบบเครือข่าย	4.40	0.67	มาก
2. เสถียรภาพของระบบเครือข่ายในการรับ/ส่ง/สื่อสารข้อมูล	4.13	0.62	มาก
3. ไม่พบการปัญหาการโจมตี/ไวรัส/มัลแวร์ บนเครือข่าย	4.23	0.72	มาก
4. ความพึงพอใจโดยภาพรวมในการใช้บริการเครือข่าย	4.27	0.64	มาก
5. ความง่ายในการเชื่อมต่อเครือข่ายอินเทอร์เน็ต	4.20	0.66	มาก
6. ความเร็วในการใช้งานเครือข่ายอินเทอร์เน็ต	4.07	0.78	มาก
7. ความพึงพอใจโดยภาพรวมในการใช้บริการเครือข่ายอินเทอร์เน็ต	4.37	0.71	มาก
8. การใช้งานระบบเครือข่ายอินเทอร์เน็ตในการ Download/Upload ข้อมูล	4.20	0.76	มาก
9. การใช้งานระบบเครือข่ายอินเทอร์เน็ตในการใช้ Social Network	4.37	0.66	มาก
10. การใช้งานระบบเครือข่ายอินเทอร์เน็ตในการใช้สืบค้นข้อมูล	4.47	0.57	มาก
รวม	**4.27**	**0.68**	**มาก**

อภิปรายผลการวิจัย

การศึกษาความพึงพอใจการพัฒนาระบบบริหารจัดการรักษาความปลอดภัยของระบบเครือข่ายสารสนเทศภาครัฐ ผู้ใช้ได้ตอบแบบสอบถามความพึงพอใจของกลุ่มตัวอย่าง จำนวน 30 คน พบว่าโดยภาพรวมอยู่ในระดับพึงพอใจมากสอดคล้องกับการศึกษาของ วงศกร เสนาะดนตรี. (2554:บทคัดย่อ). ได้การเปรียบเทียบประสิทธิภาพลินุกซ์ไฟร์วอลล์สำหรับเครือข่ายขนาดเล็กที่พบว่าผลการประเมินการใช้ระบบลินุกซ์ไฟร์วอลล์นั้นมีประสิทธิภาพพอกับการใช้งานทั่วไปสำหรับสำนักงานขนาดเล็ก ประสิทธิภาพในการใช้งานทั่วไปได้ดีและพีเอฟเซนต์จะมีความสามารถในการป้องกันได้ดี

จากการอภิปรายผลการวิจัย โดยรวมของระบบบริหารจัดการรักษาความปลอดภัยของระบบเครือข่ายสารสนเทศภาครัฐนั้น ตรงกับวัตถุประสงค์ตั้งไว้ คือ

1. เพื่อหาแนวทางในการบริหารจัดการการป้องกันภัยคุกคามระบบเครือข่ายสารสนเทศภาครัฐ
2. เพื่อพัฒนาระบบบริหารจัดการรักษาความปลอดภัยของระบบเครือข่ายสารสนเทศภาครัฐ

ข้อเสนอแนะ

จากการวิเคราะห์ ออกแบบระบบ และการพัฒนาระบบบริหารจัดการรักษาความปลอดภัยของระบบเครือข่ายสารสนเทศภาครัฐ ผู้วิจัยมีข้อเสนอแนะเกี่ยวกับการทำงานของระบบเพิ่มเติมในอนาคต ดังต่อไปนี้

1. ข้อเสนอแนะในการนำผลการวิจัยไปใช้

การนำระบบบริหารจัดการรักษาความปลอดภัยของระบบเครือข่ายสารสนเทศภาครัฐ ที่ใช้ซอฟต์แวร์ไฟร์วอลล์โอเพ่นซอร์สพีเอฟเซนต์นั้นควรจะใช้เครื่องคอมพิวเตอร์ที่มีทรัพยากรที่เพียงพอในการติดตั้งซอฟต์แวร์ไฟร์วอลล์เพื่อรองรับจำนวนผู้ใช้เครือข่าย

2. ข้อเสนอแนะในการทำวิจัยครั้งต่อไป

การทำวิจัยในครั้งต่อไปควรทำวิจัยเปรียบเทียบซอฟต์แวร์ไฟร์วอลล์โอเพ่นซอร์สพีเอฟเซนต์กับไฟร์วอลล์ที่เป็นเครื่องฮาร์ดแวร์ ทั้งประสิทธิภาพและงบประมาณที่ใช้ในการลงทุน

บรรณานุกรม

วงศกร เสนาะดนตรี. **การเปรียบเทียบประสิทธิภาพลินุกซ์ไฟร์วอลล์สำหรับเครือข่ายขนาดเล็ก.**ปริญญานิพนธ์ หลักสูตรปริญญามหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ. 2554.

ศราวุฒิ จันทะคัด. **การจัดการความปลอดภัยภายในเครือข่ายคอมพิวเตอร์ กรณีศึกษา :บริษัทแซนด์แอนด์ซอยล์อุตสาหกรรม จำกัด.**ปริญญานิพนธ์ หลักสูตรปริญญามหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีมหานคร. 2554.

ศุภพร รัฐอาจและคณะ. **การปรับแต่งไฟร์วอลล์โอเพ่นซอร์สให้มีประสิทธิภาพสูงสุด ไฟล์วอลล์.** ปริญญานิพนธ์ วิทยาการคอมพิวเตอร์ คณะวิทยาการสารสนเทศ มหาวิทยาลัยมหาสารคาม. (มปป).

อนันต์ บัณฑุเดช. **การประเมินประสิทธิภาพการป้องกันภัยคุกคามด้วยฮาร์ดแวร์ซอฟต์แวร์ และโอเพ่นซอร์สไฟ วอลล์.** ปริญญานิพนธ์ หลักสูตรปริญญามหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม.(มปป).