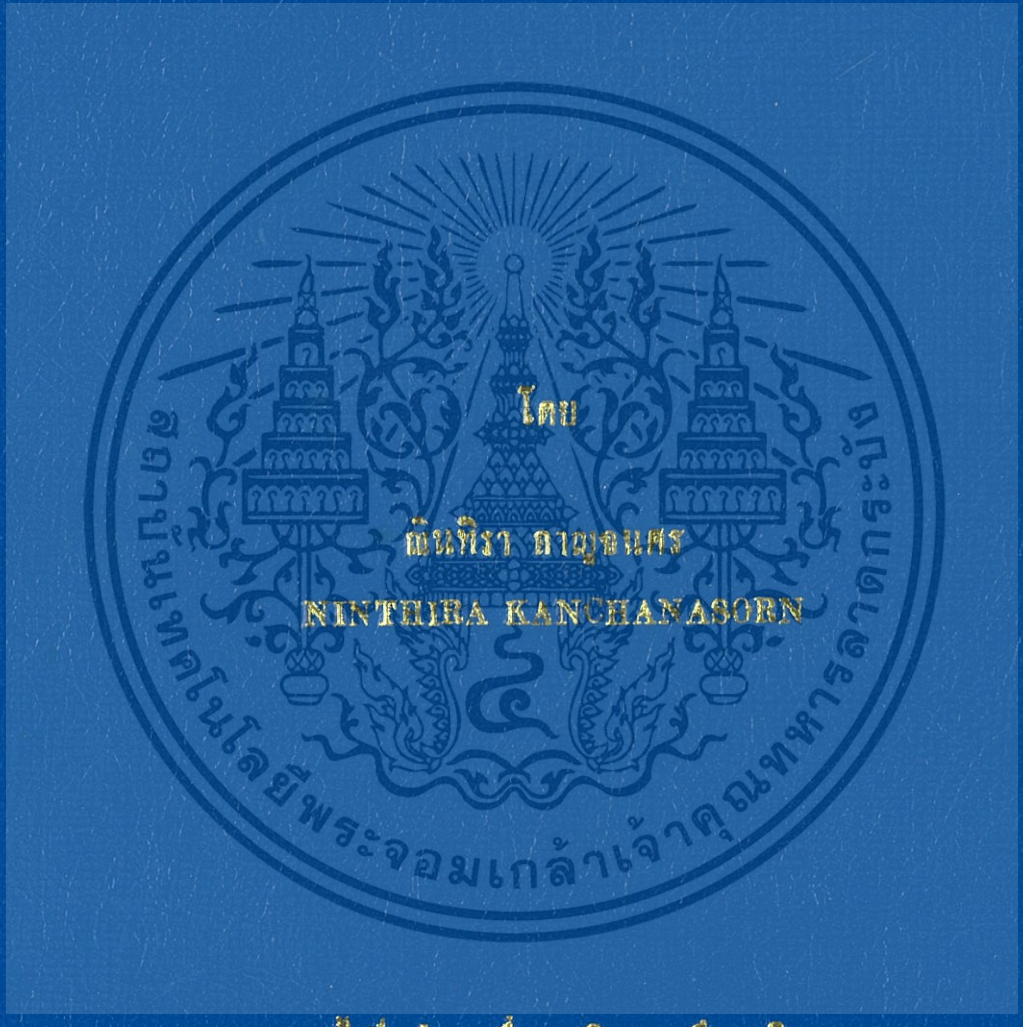
ระบบออกแบบและอิมพลีเมนท์นโยบายรักษาความปลอดภัย สำหรับอุปกรณ์ไฟร์วอลล์

SECURITY POLICY DESIGN AND IMPLEMENTATION SYSTEM FOR NETWORK FIREWALL



โดย

นินทิรา กาญจนศร

NINTHIRA KANCHANASORN

รายงานนี้เป็นส่วนหนึ่งของวิชาการศึกษาอิสระ 2

หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชานวัตกรรมโทรคมนาคม

คณะเทคโนโลยีสารสนเทศ

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ภาคเรียนที่ 2 ปีการศึกษา 2553

ระบบออกแบบและอิมพลีเมนท์นโยบายรักษาความปลอดภัย สำหรับอุปกรณ์ไฟร์วอลล์

SECURITY POLICY DESIGN AND IMPLEMENTATION SYSTEM FOR NETWORK FIREWALL

โดย

ณินทิรา กาญจนศร

NINTHIRA KANCHANASORN

อาจารย์ที่ปรึกษา

ผศ.ดร. สุเมธ ประภาวัต

รายงานนี้เป็นส่วนหนึ่งของวิชาการศึกษาอิสระ 2

หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ

คณะเทคโนโลยีสารสนเทศ

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ภาคเรียนที่ 2 ปีการศึกษา 2558

SECURITY POLICY DESIGN AND IMPLEMENTATION SYSTEM FOR NETWORK FIREWALL

NINTHIRA KANCHANASORN

A REPORT SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS OF THE COURSE

INDEPENDENT STUDY 2

MASTER OF SCIENCE PROGRAM IN INFORMATION TECHNOLOGY

FACULTY OF INFORMATION TECHNOLOGY

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

2/2015

ใบรับรองการศึกษาอิสระ 2 (Independent Study 2)

เรื่อง

ระบบออกแบบและอิมพลีเมนท์นโยบายรักษาความปลอดภัย สำหรับอุปกรณ์ไฟร์วอลล์

Security Policy Design and Implementation System for Network Firewall

นางสาวณินทิรา กาญจนศร

รหัสประจำตัว 54660510

ขอรับรองว่ารายงานฉบับนี้ข้าพเจ้าไม่ได้คัดลอกมาจากที่ใด

รายงานฉบับนี้ได้รับการตรวจสอบและอนุมัติให้เป็นส่วนหนึ่งของ

การศึกษาวิชาการศึกษาอิสระ 2 หลักสูตรวิทยาศาสตรมหาบัณฑิต (เทคโนโลยีสารสนเทศ)

ภาคเรียนที่ 2 ปีการศึกษา 2558

.....อาจารย์ที่ปรึกษา

(ผศ.ดร.สุเมธ ประภาวัต)

.....กรรมการสอบ

(รศ.ดร.จันทร์บูรณ์ สถิตวิริยวงศ์)

.....กรรมการสอบ

(ผศ.ดร.กันต์พงษ์ วรรัตน์ปัญญา)

หัวข้อ	ระบบออกแบบและอิมพลีเมนท์นโยบายรักษาความปลอดภัยสำหรับอุปกรณ์ไฟร์วอลล์
นักศึกษา	นางสาวณินทิรา กาญจนศร
รหัสนักศึกษา	54660510
ปริญญา	วิทยาศาสตรมหาบัณฑิต
สาขาวิชา	เทคโนโลยีสารสนเทศ
แขนงวิชา	เทคโนโลยีระบบสารสนเทศ
ปีการศึกษา	2558
อาจารย์ที่ปรึกษา	ผศ.ดร. สุเมธ ประภาวัต

บทคัดย่อ

ในปัจจุบันอุปกรณ์ไฟร์วอลล์ถูกใช้งานอย่างแพร่หลายในหลายๆองค์กร แต่โดยส่วนใหญ่ผู้ดูแลระบบในองค์กรขนาดกลางและขนาดเล็กยังคงขาดประสบการณ์และความรู้ความเข้าใจในการออกแบบนโยบายด้านความปลอดภัยสำหรับอุปกรณ์ไฟร์วอลล์หรือกฎในการควบคุมการผ่านเข้าออกของข้อมูลบนตัวอุปกรณ์ไฟร์วอลล์ที่มี ส่งผลให้ระบบเครือข่ายเกิดความหละหลวมจนกลายเป็นช่องโหว่ให้ผู้ไม่ประสงค์ดีสามารถเข้าถึงเครือข่ายภายในองค์กรได้ง่ายขึ้น โครงการนี้มีวัตถุประสงค์เพื่อศึกษาวิธีการกำหนดนโยบายด้านความปลอดภัยสำหรับอุปกรณ์ไฟร์วอลล์หรือกฎในการควบคุมการผ่านเข้าออกของข้อมูลบนตัวอุปกรณ์ไฟร์วอลล์จากผู้ที่มีความรู้ความเชี่ยวชาญเฉพาะทางมาใช้ในการออกแบบและพัฒนาระบบออกแบบและอิมพลีเมนท์นโยบายรักษาความปลอดภัยสำหรับอุปกรณ์ไฟร์วอลล์ โดยนโยบายที่ได้นอกจากจะมีความสอดคล้องกันกับสภาพแวดล้อมของแต่ละองค์กรแล้ว ยังช่วยปิดช่องโหว่ทางระบบเครือข่ายแล้วได้มากขึ้นอีกด้วย ซึ่งผู้ดูแลระบบสามารถนำนโยบายสำเร็จรูปที่ได้จากระบบระบบออกแบบและอิมพลีเมนท์นโยบายรักษาความปลอดภัยสำหรับอุปกรณ์ไฟร์วอลล์มาตั้งค่าการใช้งานลงในอุปกรณ์ไฟร์วอลล์ที่มีอยู่ได้ แต่หากเป็นอุปกรณ์ไฟร์วอลล์ตัวอื่นๆ นอกเหนือจากที่ระบบมี ผู้ดูแลระบบสามารถนำนโยบายตัวต้นแบบมาเป็นค่าพื้นฐานในการปรับเปลี่ยนและปรับปรุงการตั้งค่าของอุปกรณ์ไฟรร์วอลล์ที่มีอยู่ให้มีความครอบคลุมและความปลอดภัยจนสามารถลดช่องโหว่ต่างๆทางด้านระบบเครือข่ายได้

Title	Security Policy Design and Implementation System for Network Firewall
Student	Miss Ninthira Kanchanasorn
Student ID	54660510
Degree	Master of Science
Program	Information Technology
Major	Information System Technology
Academic Year	2015
Advisor	Asst Prof Dr. Sumet Prapawat

ABSTRACT

Nowadays the firewall device has become an essential part of security system for various organizations. However, most of IT administrators, especially SME or small organization, does not have much experiences and knowledge to design a good security policy on the firewall device to gain an adequate access control. And this may directly affects to business risk and asset from the result of threats exploiting a vulnerability as the network security system has high potential to be under attacked by hackers causing business lost. The objective of this project is to research for a solution to reduce network security leaks, based on advices and experiences from network security specialist, and determine precise firewall security policy and rules which can reduce potential business risk. This project does not only reduce the potential risk of network security system but it also supports the administrator to customize the policy to align with the corporate environment. The rule sets for available firewall devices list will be generated, which are ready to be deployed to the selected devices. Even though some appliance devices may not be included in the list, the new device for example, the system administrator can still customize and standardize the setting from the original policy and apply the policy to those devices as well.

กิตติกรรมประกาศ

โครงงานนี้สำเร็จได้อย่างดีด้วยคำแนะนะ และคำปรึกษาจาก ผศ.ดร.สุเมธ ประภาวัต ซึ่งเป็นอาจารย์ผู้ให้คำปรึกษาในโครงงานนี้ ข้าพเจ้ารู้สึกซาบซึ้งในความอนุเคราะห์จากท่านอาจารย์และขอขอบพระคุณเป็นอย่างสูง

ขอขอบพระคุณคณาจารย์ภาควิชาวิทยาการสารสนเทศ คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบังทุกท่าน ที่ได้ประสิทธิ์ประสาทวิชาให้กับข้าพเจ้า

ขอขอบคุณเพื่อนๆ พี่ๆ น้องๆ ในภาควิชาวิทยาการสารสนเทศ คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบังทุกคน ที่ให้คำแนะนำและความช่วยเหลือเสมอมา

สุดท้ายนี้ ข้าพเจ้าขอกราบขอบพระคุณบิดา มารดา และครอบครัวของข้าพเจ้าที่คอยให้การสนับสนุนในทุกๆเรื่อง ทำให้ข้าพเจ้าสามารถทำโครงงานฉบับนี้ให้สำเร็จลุล่วงด้วยดี

คุณค่าและประโยชน์อันพึงได้จากโครงงานฉบับนี้ ข้าพเจ้าขอมอบแด่ผู้มีพระคุณทุกท่าน

ณินทิรา กาญจนศร

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

ตารางที่ หน้า

สารบัญตาราง (ต่อ)

ตารางที่ หน้า

สารบัญรูปภาพ

รูปที่ หน้า

สารบัญรูปภาพ (ต่อ)

รูปที่ หน้า

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

หากกล่าวถึงเอกสารนโยบายหรือมาตรฐานด้านความปลอยภัยสำหรับองค์กร การเพิ่มความปลอดภัยทางด้านระบบเครือข่ายถือเป็นส่วนหนึ่งของนโยบายดังกล่าว เพื่อใช้สำหรับควบคุมให้การจราจรที่เกิดขึ้นในระบบเครือข่ายให้มีความปลอดภัยมากพอที่จะช่วยปิดช่องโหว่ให้กับองค์กร และอุปกรณ์ไฟร์วอลล์จึงถูกเลือกเป็นหนึ่งในปัจจัยสำหรับสนองต่อนโยบายด้านความปลอดภัยดังกล่าว เพราะอุปกรณ์ไฟรร์วอลล์มีหน้าที่ในการคัดกรองและความคุมการผ่านของข้อมูลในระบบเครือข่าย ช่วยให้การดำเนินงานเป็นไปอย่างราบรื่น ช่วยลดช่องโหว่ทางด้านระบบเครือข่ายจากผู้ไม่ประสงค์ดี และยังช่วยจัดการให้การใช้ปริมาณแบนด์วิธเป็นไปอย่างคุ้มค่า ซึ่งสามารถสนับสนุนนโยบายด้านความปลอดภัยสำหรับองค์กรได้เป็นอย่างดี

การทำให้อุปกรณ์ไฟร์วอลล์สามารถตอบสนองได้ตรงตามความต้องการขององค์กร ผู้ดูแลระบบจำเป็นต้องสร้างกฎให้ไฟรร์วอลล์เข้าใจถึงวิธีการในการคัดกรองข้อมูล ซึ่งกลุ่มของกฎดังกล่าวสามารถรวมเรียกว่านโยบายสำหรับไฟรร์วอลล์ (Firewall Policy) หรือกฎสำหรับควบคุมการผ่านเข้าออก (Access Control Rule) สำหรับไฟร์วอลล์ ซึ่งในการสร้างนโยบายดังกล่าวจำเป็นต้องอาศัยคนที่มีความรู้ทางด้านระบบเครือข่ายและข้อมูลการจราจรของแต่ละแอปพลิเคชั่นในการกำหนดให้เข้ากับสภาพแวดล้อมและแต่ละองค์กร ซึ่งบางครั้งผู้ดูแลระบบสำหรับองค์กรขนาดเล็กและขนาดกลางบางแห่งที่มีความต้องการเพิ่มความปลอดภัยให้กับองค์กรนั้นยังขาดประสบการณ์และความรู้ในส่วนดังกล่าวอยู่ ส่งผลให้นโยบายที่ได้มีความหละหลวมจนกลายเป็นช่องโหว่ทางด้านระบบเครือข่ายในลำดับต่อมา

ดังนั้นผู้จัดทำจึงมีแนวคิดที่จะทำระบบสำหรับสนับสนุนและช่วยเหลือผู้ดูแลระบบในการสร้างนโยบายสำหรบไฟรร์วอลล์ หรือกฎสำหรับควบคุมการผ่านเข้าออก (Access Control Rule) สำหรับไฟร์วอลล์ให้กับองค์กรขนาดกลางและขนาดเล็กเพื่อช่วยลดช่องโหว่ทางด้านระบบเครือข่าย โดยจะอาศัยการออกแบบและการวางเงื่อนไขของกฎที่มีการอ้างอิงมาจากผู้ที่มีความรู้ความเชี่ยวชาญและประสบการณ์ในการออกแบบกฎสำหรับควบคุมการผ่านเข้าออก (Access

Control Rule) เพื่อให้ได้กฎข้อบังคับบนตัวอุปกรณ์ไฟร์วอลล์ที่เหมาะสมกับสภาพแวดล้อมของแต่ละองค์กรได้

1.2 ความมุ่งมั่นและวัตถุประสงค์ของการศึกษา

วัตถุประสงค์ของการดำเนินโครงการพัฒนาระบบออกแบบและอิมพลีเมนท์นโยบายรักษาความปลอดภัยสำหรับอุปกรณ์ไฟร์วอลล์ มีดังนี้

1. เพื่อศึกษาหลักการในการสร้างกฎการควบคุมการผ่านเข้าออกของข้อมูลบนระบบเครือข่าย (Network Access Control) จากผู้ที่มีความรู้ความเชี่ยวชาญเฉพาะทาง เพื่อนำไปสู่การกำหนดนโยบายด้านความปลอดภัย (Security Policy) หรือกฎควบคุมการผ่านเข้าออกของข้อมูล (Access Control Rule) สำหรับไฟร์วอลล์
2. เพื่อพัฒนาระบบช่วยกำหนด นโยบายด้านความปลอดภัยหรือกฎการควบคุมการผ่านเข้าออกของข้อมูลสำหรับไฟร์วอลล์จากการวิเคราะห์ความต้องการของผู้ใช้ (User Requirements) และความเหมาะสมกับเครือข่ายรวมถึงสภาพแวดล้อมในองค์กร
3. เพื่อพัฒนาระบบสร้างกฎควบคุมการผ่านเข้าออกของข้อมูลสำหรับไฟร์วอลล์ที่เหมาะสมสำหรับอุปกรณ์ไฟร์วอลล์แต่ละตัวโดยสอดคล้องกับนโยบายด้านความปลอดภัยหรือกฎควบคุมการผ่านเข้าออกของข้อมูลสำหรับไฟร์วอลล์ที่กำหนดขึ้น โดยเป็นไปตามความต้องการของผู้ใช้และความเหมาะสมกับสภาพแวดล้อมอย่างรัดกุมแม่นยำ

1.3 ขอบเขตของการศึกษา

ระบบออกแบบและอิมพลีเมนท์นโยบายรักษาความปลอดภัยสำหรับอุปกรณ์ไฟร์วอลล์เป็นระบบที่สร้างขึ้นเพื่อตอบสนองความต้องการของผู้ดูแลระบบเครือข่ายสำหรับองค์กรขนาดเล็กและขนาดกลางเป็นหลัก โดยขอบเขตของการศึกษาได้จากการนำความรู้จากผู้ที่มีความรู้ความเชี่ยวชาญเฉพาะทางมาประยุกต์ใช้ในการกำหนดนโยบายด้านความปลอดภัย ดังนี้

1. สามารถกำหนดไอพีแอดเดรส (IP Address) ให้สอดคล้องกับการจัดวางเครื่องแม่ข่าย (Server) และเครื่องลูกข่าย (Client) ที่ถูกจัดแบ่งไว้ตามโซนความปลอดภัยได้อย่างเหมาะสม

2. สามารถออกแบบนโยบายด้านความสำหรับปลอดภัย (Security Policy) หรือกฎควบคุมการผ่านเข้าออก (Access Control Rule) สำหรับไฟร์วอลล์ ให้เป็นไปตามความต้องการของผู้ใช้ (User Requirements) และตามความเหมาะสมกับสภาพแวดล้อมของเครือข่ายในองค์กร
3. สามารถสร้างนโยบายด้านความปลอดภัย (Security Policy) หรือกฎควบคุมการผ่านเข้าออก (Access Control Rule) สำหรับไฟร์วอลล์ที่เหมาะสมกับอุปกรณ์ไฟร์วอลล์แต่ละตัวให้สอดคล้องกับนโยบายด้านความปลอดภัยหรือกฎควบคุมการผ่านเข้าออก (Access Control Rule)ที่กำหนดขึ้น

1.4 ประโยชน์ที่คาดว่าจะได้รับ

ประโยชน์ที่คาดว่าผู้ดูแลระบบเครือข่ายและผู้พัฒนาระบบจะได้รับจากการพัฒนาระบบออกแบบและอิมพลีเมนท์นโยบายรักษาความปลอดภัยสำหรับอุปกรณ์ไฟร์วอลล์ มีดังนี้

1. ผู้พัฒนาได้รับความรู้ในส่วนของโปรแกรมที่ใช้ในการพัฒนาและการวางนโยบายด้านความปลอดภัย (Security Policy) หรือกฎควบคุมการผ่านเข้าออก (Access Control Rule) สำหรับไฟร์วอลล์ได้อย่างเหมาะสมตามหลักการและความรู้ที่ได้รับจากผู้ที่มีความรู้ความเชี่ยวชาญเฉพาะทาง
2. ผู้พัฒนาได้รู้จักการคิดวิเคราะห์ เพื่อใช้ในการแก้ปัญหาระหว่างการพัฒนาระบบออกแบบและอิมพลีเมนท์นโยบายรักษาความปลอดภัยสำหรับอุปกรณ์ไฟร์วอลล์
3. ผู้ใช้งานสามารถนำระบบมาช่วยวางแนวทางในการสร้างนโยบายความปลอดภัย (Security Policy) หรือกฎควบคุมการผ่านเข้าออก (Access Control Rule) สำหรับไฟร์วอลล์ให้กับองค์กร
4. ผู้ใช้งานสามารถนำระบบมาช่วยในการตรวจสอบความรัดกุมของนโยบายด้านความความปลอดภัย (Security Policy) หรือกฎควบคุมการผ่านเข้าออก (Access Control Rule) สำหรับไฟร์วอลล์ที่มีอยู่เดิม
5. ระบบสามารถช่วยผู้ใช้งานในการวางแผนงานทางด้านความปลอดภัยบนระบบเครือข่ายได้ด้วยตนเอง

1.5 ขั้นตอนของการศึกษา

ขั้นตอนในการดำเนินโครงการประกอบด้วยขั้นตอนการทำงานต่างๆ ดังนี้

1. ศึกษาข้อมูลทางด้านรูปแบบในการจัดสร้างนโยบายด้านความปลอดภัย(Security Policy) หรือกฎควบคุมการผ่านเข้าออก (Access Control Rule) สำหรับไฟร์วอลล์บนระบบเครือข่าย

- ศึกษารายละเอียดและรูปแบบของการกำหนดนโยบายด้านความปลอดภัย (Security Policy) หรือกฎควบคุมการผ่านเข้าออก (Access Control Rule) สำหรับไฟร์วอลล์จากผู้ที่มีความรู้เฉพาะทาง เพื่อใช้เป็นส่วนหนึ่งในการสร้างกฎควบคุมการผ่านเข้าออกที่มีความถูกต้องและสัมพันธ์กันกับสภาพแวดล้อมขององค์กร
- ศึกษาการทำงานและรูปแบบการสื่อสารของแอพพลิเคชันหลักๆแต่ละชนิด เพื่อช่วยให้เกิดความถูกต้องและแม่นยำในการกำหนดนโยบายความปลอดภัยนโยบายด้านความปลอดภัย (Security Policy) หรือกฎควบคุมการผ่านเข้าออก (Access Control Rule)

2. พัฒนาระบบที่ช่วยกำหนดนโยบายด้านความปลอดภัยที่มีความเหมาะสมกับสภาพแวดล้อมของแต่ละองค์กร

- พัฒนาระบบสำหรับจัดเก็บข้อมูลของสภาพแวดล้อมของแต่ละองค์กรและข้อมูลความต้องการของผู้ดูแลระบบ
- พัฒนาระบบสำหรับคิดวิเคราะห์ข้อมูลที่ได้ของแต่ละองค์กรร่วมกับทฤษฎีการจัดวางระบบรักษาความปลอดภัยที่มีเพื่อให้ได้มาซึ่งนโยบายด้านความปลอดภัย (Security Policy) หรือกฎควบคุมการผ่านเข้าออก (Access Control Rule) สำหรับไฟร์วอลล์ที่มีความเหมาะสมกันกับองค์กร

3. พัฒนาระบบเพื่อสร้างกฎควบคุมการผ่านเข้าออกที่เหมาะสมกับอุปกรณ์ไฟร์วอลล์ตามความต้องการของแต่ละองค์กร

- ศึกษารูปแบบการวางกฎควบคุมการผ่านเข้าออก (Access Control Rule) ของอุปกรณ์ไฟร์วอลล์แต่ละชนิด และพัฒนาระบบโดยนำกฎควบคุมการผ่านเข้าออก (Access Control Rule)ที่ได้มาแปลงให้เหมาะกับอุปกรณ์ไฟร์วอลล์ขององค์กร

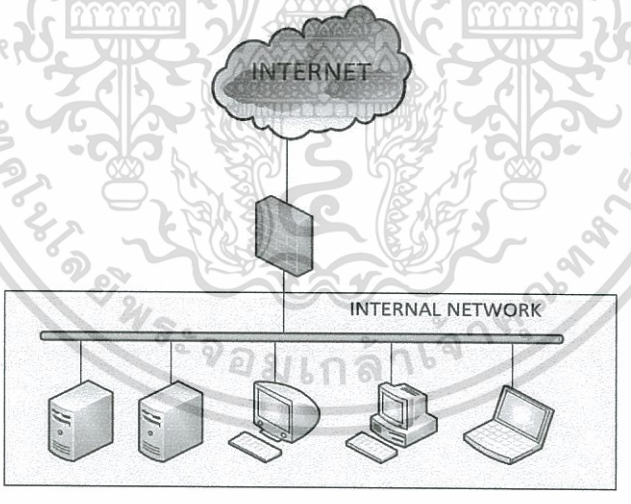
บทที่ 2
ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

ในบทความนี้จะกล่าวถึงทฤษฎีและหลักการต่างๆ ที่ใช้ในการพัฒนาระบบ ซึ่งเนื้อหาเกี่ยวข้องกับความหมายและหลักการทำงานของสเตทฟูลไฟร์วอลล์ (Stateful Firewall) บนโอเอสไอเลเยอร์ (OSI Layer) โดยจะเน้นในส่วนของเน็ตเวิร์คเลเยอร์และทรานสปอร์ตเทชันเลเยอร์เป็นหลัก การจัดแบ่งโซนเพื่อเพิ่มความปลอดภัยในระบบเครือข่าย ชนิดของเซิร์ฟเวอร์ที่ให้บริการตามมาตรฐานทั่วไปและการสร้างนโยบายด้านความปลอดภัยบนอุปกรณ์ไฟร์วอลล์

2.1 ความหมาย หน้าที่ วิวัฒนาการและคุณสมบัติของไฟร์วอลล์

ในหัวข้อนี้จะกล่าวถึงหน้าที่การทำงานของอุปกรณ์ไฟร์วอลล์ โดยจะเน้นในวิวัฒนาการในส่วนที่เป็นสเตทฟูลไฟร์วอลล์เป็นหลัก

2.1.1 ความหมายและหน้าที่ของไฟร์วอลล์



รูปที่ 2.1 แสดงหน้าที่ของอุปกรณ์ไฟร์วอลล์

ไฟร์วอลล์เป็นอุปกรณ์บนระบบเครือข่ายคอมพิวเตอร์ที่มีหน้าที่ในการควบคุมการผ่านเข้าและออกของข้อมูลซึ่งมีความสามารถในการสร้างเงื่อนไขเพื่อตรวจสอบข้อมูลที่มีการรับส่งผ่านระบบเครือข่ายคอมพิวเตอร์ว่าสามารถหรือไม่สามารถผ่านเข้าและออกเครือข่ายแต่ละเครือข่ายได้ โดยระบบเครือข่ายคอมพิวเตอร์ที่ไฟร์วอลล์สามารถควบคุมได้นั้นมีได้มากกว่าสองเครือข่ายขึ้นไป

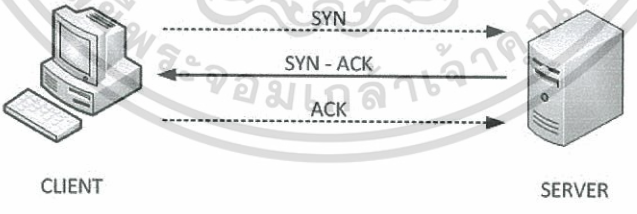
เช่นเครือข่ายภายในองค์กรด้วยกันเอง ระหว่างแผนก หรือเครือข่ายภายในองค์กร (Internal Network) กับเครือข่ายอินเทอร์เน็ต (Internet Network) ภายนอกองค์กร

ดังนั้นไฟร์วอลล์จึงเป็นเครื่องมือที่ใช้สำหรับปกป้องและป้องกันข้อมูลที่มีการรับส่งกันภายในระบบเครือข่าย ซึ่งสามารถป้องกันไม่ให้บุคคลที่ไม่ได้รับอนุญาตทั้งภายในและภายนอกองค์กรสามารถเข้าถึงข้อมูลที่สำคัญได้ ซึ่งหน้าที่ของไฟร์วอลล์จะช่วยกำหนดกฎเกณฑ์ในการควบคุมการเข้า-ออกหรือการรับ-ส่งข้อมูลในระบบเครือข่ายให้เหลือเฉพาะช่องทางที่จำเป็นต่อการรับและส่งข้อมูลเท่านั้น

2.1.2 วิวัฒนาการของไฟร์วอลล์

ไฟร์วอลล์ในยุคแรก (First Generation Firewall) หรือแพคเก็ตฟิลเทอริงไฟร์วอลล์ (Packet Filtering Firewall) มีเอกสารเกิดขึ้นครั้งแรกเมื่อปี ค.ศ. 1998 โดย Digital Equipment Corporation (DEC) เป็นผู้พัฒนาขึ้นมา โดยทำงานกับแพคเก็ตข้อมูลตั้งแต่เลเยอร์ 2 ถึงเลเยอร์ 4 ของ OSI model ซึ่งจะพิจารณาเงื่อนไขในการผ่านเข้าออกของข้อมูลจากไอพี ต้นทางและปลายทาง, พอร์ต TCP/UDP ต้นทางและพอร์ต TCP/UDP ปลายทางเป็นหลัก ถ้ามีแพคเก็ตผ่านและตรงตามเงื่อนไขที่กำหนดไฟร์วอลล์ถึงจะอนุญาตให้แพคเก็ตนั้นผ่านไปได้

ไฟร์วอลล์ในยุคที่สอง (Second Generation Firewall) ถูกพัฒนาขึ้นในปี ค.ศ. 1989-1990 จากนักพัฒนาทั้ง 3 คนของสถาบัน AT&T Bell Laboratories โดยในครั้งแรกเรียกไฟร์วอลล์ในยุคนี้ว่าเป็น เซอร์กิต เลเวล ไฟร์วอลล์ (Circuit Level Firewalls) หรือที่รู้จักกันดีในชื่อสเตทฟูล ไฟร์วอลล์ (Stateful firewall)



รูปที่ 2.2 แสดงลักษณะการทำงานของสเตทฟูลไฟร์วอลล์

การทำงานของสเตทฟูลไฟร์วอลล์ถูกพัฒนามาจากไฟร์วอลล์ในยุคแรก ซึ่งยังคงทำงานกับแพคเก็ตข้อมูลจนถึงเลเยอร์ 4 ของโอเอสไอโมเดล แต่ต่างกันตรงที่สเตทฟูลไฟร์วอลล์สามารถแยกแยะประเภทของการเชื่อมต่อได้ว่าเป็นการเชื่อมต่อใหม่หรือเป็นส่วนหนึ่งของการเชื่อมต่อเดิมและไม่ใช่ส่วนหนึ่งของการเชื่อมต่อเลยได้เช่นกัน ถึงแม้ว่าแพคเก็ตที่ผ่านมายังอุปกรณ์จะตรงตาม

เงื่อนไขที่อยู่ไอพีแอดเดรสกับพอร์ตแล้ว แต่ก็ไม่ใช่ว่าจะผ่านไปได้เสมอไป เพราะถ้าลักษณะของการเชื่อมต่อผิดแปลกไปจากเงื่อนไขตามข้อตกลงตามมาตรฐานกลางของ TCP/UDP ของไคลแอนท์และเซิร์ฟเวอร์กำหนดไว้ดังรูปที่ 2.2 ถ้าแพคเก็ตนั้นๆไม่ตรงตามเงื่อนไขแล้วแพคเก็ตนั้นๆก็จะไม่สามารถผ่านไปได้เช่นกัน

ไฟร์วอลล์ในยุคที่สาม (Third Generation Firewall) เริ่มขายในปี ค.ศ. 1991 โดยบริษัท DEC และต่อมาในปี ค.ศ. 1993 DARPA ได้พัฒนาไฟร์วอลล์ทูลคิท (Firewall Toolkit) ขึ้นเป็นซอฟต์แวร์ให้ใช้ฟรีไม่ใช่สำหรับในเชิงพาณิชย์

สำหรับไฟร์วอลล์ในยุคที่สามหรือดูอัลโฮมเกทเวย์ (Dual-home Gateway) หรือแอพพลิเคชัน พรอกซี ไฟร์วอลล์ (Application Proxy Firewall) มีหลายประเภทด้วยกันในการเลือกใช้งาน แต่การทำงานหลักๆคือการกรองแพคเก็ตจนถึงเลเยอร์ 7 ซึ่งเป็นเลเยอร์สูงสุดของ OSI model โดยหัวใจหลักของแอพ-พลิเคชัน พรอกซี ไฟร์วอลล์นี้คือการเข้าใจพฤติกรรมและโปรโตคอลของแอพพลิเคชันต่างๆ เช่น FTP DNS เว็บ เบราว์ซิง (Web Browsing) และโปรโตคอลในรูปแบบอื่นๆที่ไม่มีมาตรฐานของพอร์ตที่กำหนดไว้ตายตัว เพื่อช่วยในการป้องกันอันตรายที่อาจเกิดขึ้นทางด้านระบบเครือข่ายได้

จากการวิเคราะห์บทความข้างต้นเพื่อนำมาพิจารณาใช้ในโครงงานนี้ ทางผู้จัดทำได้นำข้อมูลในส่วนการทำงานของอุปกรณ์ไฟร์วอลล์ในยุคที่สองมาใช้เป็นหลัก เพราะการทำงานของอุปกรณ์ไฟร์วอลล์ในยุคนี้มีความสามารถพื้นฐานที่อุปกรณ์ไฟร์วอลล์ในทุกๆผลิตภัณฑ์สามาถทำได้

2.1.3 คุณสมบัติของ Firewall

1. ป้องกัน (Protect)

ไฟร์วอลล์เป็นเครื่องมือที่ทำงานในเชิงการป้องกัน โดยแพคเก็ตที่จะสามารถผ่านเข้าและออกได้นั้น จะต้องเป็นแพคเก็ตที่ถูกพิจารณามาแล้วว่ามีความเสี่ยงน้อยที่สุด หากแพคเก็ตใดที่มีความเสี่งสูงจะถูกตัดสินไม่ให้ผ่านเข้าและออกไปได้ ซึ่งสิ่งที่ช่วยตัดสินนั้นจะอยู่ที่ผู้ดูแลระบบเป็นคนตั้งกฎและนโยบายพื้นฐาน(Rule)เพื่อบังคับใช้ในการสื่อสาร

2. การตัดสินใจโดยการใช้กฎ (Rule Base)

ไฟร์วอลล์ จะทำการควบคุมการเข้าถึง (Access) โดยอาศัยการเปรียบเทียบแพคเก็ตที่ผ่านเข้าและออกควบคู่กับกฎพื้นฐานที่ผู้ดูแลระบบกำหนดไว้ หากพบว่าไม่มีกฎห้ามไว้หรือมีกฎ

อนุญาตก็จะอนุญาตขอมูลนั้นให้ผ่านไปได้ แต่ถ้ามีกฎข้อใดข้อหนึ่งห้าม แพคเก็ตนั้นๆก็จะไม่สามารถผ่านไปได้

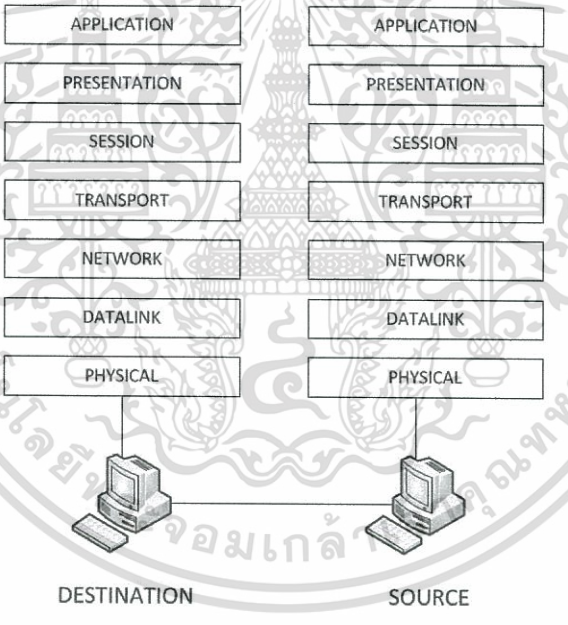
ซึ่งมีรูปแบบในการทำงานขั้นพื้นฐาน ดังนี้

If A = 1 (เงื่อนไข) Then …ข้อสรุป…

Else …กฎข้อต่อไป…

3. ควบคุมการเข้าถึง (Access Control)

ไฟร์วอลล์เป็นเครื่องมือที่ช่วยในการควบคุมการเข้าถึง (Access) ของโฮส (Host) ต่างๆให้เป็นไปตามกฎพื้นฐานที่ผู้ดูแลระบบได้กำหนดไว้ โดยหลักการควบคุมจะใช้โอเอสไอโมเดลเลเยอร์ในการอ้างอิงแพคเก็ตต่างๆ ดังรูปที่ 2.3 ที่แสดงแบบจำลองโอเอสไอ ที่มีการแบ่งการทำงานของระบบเครือข่ายออกเป็น 7 ชั้นดังรูป



รูปที่ 2.3 แสดงแบบจำลองโอเอสไอ 7 เลเยอร์

แต่ละชั้นของการติดต่อสื่อสารจะเรียกว่าเลเยอร์ (Layer) ซึ่งประกอบด้วยเลเยอร์ย่อยๆ ทั้งหมด 7 เลเยอร์ที่ทำหน้าที่รับส่งข้อมูลกับชั้นที่อยู่ติดกับตัวเองในเอง โดยจะไม่มีการติดต่อกระโดดข้ามไปยังชั้นอื่นๆ เช่น เลเยอร์ที่ 6 จะติดต่อกับเลเยอร์ที่ 5 และเลเยอร์ที่ 7 เท่านั้น

การส่งข้อมูลจะทำไล่จากเลเยอร์ที่อยู่บนสุด คือ เลเยอร์ 7 ลงมาจนถึงเลเยอร์ 1 ซึ่งเป็นชั้นที่มีการเชื่อมต่อทางด้านกายภาพ จากนั้นข้อมูลจะถูกส่งไปยังเครื่องผู้รับปลายทางโดยเริ่มจากชั้น

ล่างสุด คือ เลเยอร์ 1 และข้อมูลก็จะถูกถอดรหัสเพื่อส่งขึ้นเรื่อยๆจนถึงเลเยอร์ 7 และส่งให้แอพพลิเคชันนำไปใช้ในการประมวลผลในลำดับต่อไป

โดยในบทความจะเน้นกล่าวถึงเลเยอร์เยอร์ที่ 3 และเลเยอร์ที่ 4 เป็นหลัก เพราะการกำหนดกฎนโยบายด้านความปลอดภัยสำหรับโครงงานจะเน้นการทำงานแบบสเตทฟูลไฟร์วอลล์ จึงเป็นการทำงานในชั้นที่ 4 คือทรานสปอร์ทเทชันและชั้นที่ 3 เน็ตเวิร์คเท่านั้น

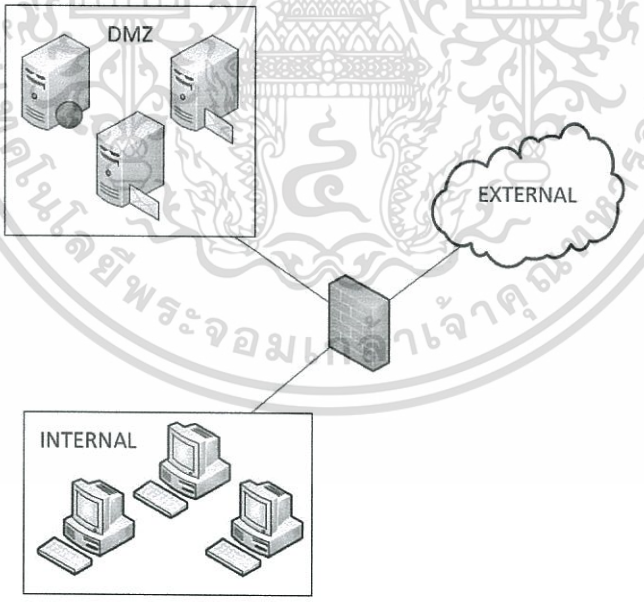
หน้าที่การทำงานของแต่ละเลเยอร์ เป็นดังนี้

1. ฟิสิคัลเลเยอร์ (Physical Layer) อธิบายคุณสมบัติทางกายภาพ เช่น คุณสมบัติทางไฟฟ้า ทางแสงและกลไกต่างๆ ของวัสดุที่ใช้เป็นสื่อกลางในการติดต่อสื่อสาร
2. ดาต้าลิงก์เลเยอร์ (Datalink Layer) อธิบายถึงการส่งข้อมูลเป็นแบบฮอบต่อฮอบ (hop by hop) โดยแบ่งออกเป็นชั้นย่อยๆ 2 ชั้นด้วยกัน คือ Logical Link Control (LLC) และ Media Access Control (MAC)
3. เน็ตเวิร์คเลเยอร์(Network Layer) อธิบายและให้ความสนใจกับแอดเดรสทางตรรกะการทำงาน ซึ่งในชั้นนี้จะใช้ในการคัดเลือกเส้นทางในการนำพาข้อมูลระหว่างเครื่องสองเครื่องที่อยู่ภายในเครือข่ายชั้นเน็ตเวิร์ค โดยให้บริการเชื่อมต่อในในชั้นนี้มีแบบ Connection Oriented เช่น X.25 และบริการแบบ Connectionless เช่น Internet Protocol ซึ่งถูกใช้งานโดยชั้นที่อยู่ถัดขึ้นไปคือทรานสปอร์ทเลเยอร์ (Transport Layer) ซึ่งขั้นตอนในการเลือกส้นทางนำพาข้อมูลไปยังปลายทางที่เรียกว่า เร้าติง (Routing) และใช้โปรโตคอล Internet Protocol (IP)
4. ทรานสปอร์ตเลเยอร์ (Transport Layer) อธิบายถึงโปรโตคอลที่ให้บริการซึ่งมีความใกล้เคียงกันกับที่ชั้นเน็ตเวิร์คมี โดยมีการบริการด้านคุณภาพที่ทำให้เกิดความน่าเชื่อถือ แต่ในบางโปรโตคอลที่ไม่มีการดูแลเรื่องคุณภาพดังกล่าวจะอาศัยการทำงานในชั้นนี้เพื่อเข้ามาช่วยดูแลเรื่องคุณภาพแทน เหตุผลที่สนับสนุนการใช้งานชั้นนี้เพื่อเพิ่มความมั่นใจในคุณภาพให้กับผู้ใช้บริการ ได้แก่ Transmission Control Protocol (TCP) ซึ่งเป็นโปรโตคอลที่มีการใช้งานกันมากที่สุดและเป็นการเชื่อมต่อแบบเชื่อถือได้ (Connection Oriented) และ User Datagram Protocol (UDP) ซึ่งเป็นโปรโตคอลในชั้นทรานสปอร์ตที่มักใช้กับข้อมูลที่มีลักษณะเป็นสตรีมมีเดียร์(Stream Media) และเป็นการเชื่อมต่อแบบไม่น่าเชื่อถือ (Connectionless)

5. เซสชั่นเลเยอร์ (Session Layer) อธิบายถึงการเชื่อมต่อกันในเชิงตรรกะ (Logic) ระหว่างปลายทางทั้งสองด้าน (เครื่อง 2 เครื่อง
6. พรีเซนเทชั่นเลเยอร์ (Presentation Layer) อธิบายถึงการให้บริการในการทำการตกลงกันระหว่างสองโปรโตคอลถึงไวยากรณ์ (Syntax) ที่จะใช้ในการรับและส่งข้อมูล การทำงานในชั้นนี้จึงมีบริการในการแปลข้อมูลตามที่ได้รับการร้องขอด้วย
7. แอพพลิเคชั่นเลเยอร์ (Application Layer) อธิบายถึงการที่ชั้นนี้เป็นชั้นที่ขอใช้บริการของชั้นพรีเซนเทชั่นเพื่อประยุกต์ใช้งานในด้านต่างๆ เช่น การทำ E-mail Exchange (การรับและส่งอีเมล์), การโอนย้ายไฟล์ หรือการประยุกต์ใช้งานทางด้านเครือข่ายอื่นๆ

2.2 การจัดแบ่งโซนเพื่อความปลอดภัยในระบบเครือข่าย

การจัดแบ่งโซนของไฟร์วอลล์โดยทั่วไปจะประกอบด้วย 3 โซนหลัก ซึ่งโซนในที่นี้จะขึ้นกับอินเตอร์เฟสของอุปกรณ์ไฟร์วอลล์เพียงอินเตอร์เฟสเดียวหรือเป็นกลุ่มของอินเตอร์เฟสก็ได้เช่นกัน โดยแต่ละโซนจะมีถูดจัดแบ่งดังรูปที่ 2.4 และมีความหมายดังต่อไปนี้



รูปที่ 2.4 แสดงตัวอย่างการจัดแบ่งโซนเพื่อความปลอดภัย

2.2.1 เครือข่ายภายใน (Internal)

เครือข่ายภายใน (Internal) หรือ แลน (LAN) หรือ Trusted Network เป็นส่วนที่คอมพิวเตอร์ภายในองค์กรณ์มีการเชื่อมต่อกันอยู่ผ่านอุปกรณ์ต่างๆภายในระบบเน็ตเวิร์ค และมีเส้นทางที่สามารถสื่อสารไปยังโซนแลนของไฟร์วอลล์ก่อนจะไปยังโซนอื่นๆ โดยทั่วไปโซนนี้จะไม่อนุญาตให้เข้าถึงได้จากโซนภายนอกแต่สามารถออกไปยังอินเตอร์เน็ตได้ ซึ่งโซนนี้จะประกอบไปด้วยคอมพิวเตอร์ของบุคลากร เครื่องพิมพ์หรือปริ้นท์เซิร์ฟเวอร์ และเครื่องแม่ข่าย (Server) บางชนิด

ไอพีแอดเดรส (IP Address) ที่ใช้ในโซนนี้มักเป็นไอพีในกลุ่มไอพีส่วนบุคคล (Private IP) โดยอ้างอิงตาม RFC 1918

ได้แก่ 10.0.0.0 - 10.255.255.255 (10/8 prefix)

172.16.0.0 - 172.31.255.255 (172.16/12 prefix)

192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

ไอพีส่วนบุคคลถูกนำมาใช้เพื่อรองรับไคลแอนท์ปริมาณมากๆ เพราะเราไม่สามารถให้ไอพีสาธารณะ(Public IP) กับเครื่องไคลแอนท์ทุกเครื่องได้ แต่ข้อจำกัดของไอพีส่วนบุคคลคือ ไม่สามารถสื่อสารกับไอพีสาธารณะ (Public IP) หรืออินเตอร์เตอร์เน็ตได้ ดังนั้นการจะทำการสื่อสารกับไอพีภายนอกได้ต้องผ่านการแปลงไอพีส่วนบุคคลให้เป็นไอพีสาธารณะเสียก่อน หรือในทางเทคนิคจะเรียกกระบวนการนี้ว่า การทำ NAT (Network Address Transtation)

2.2.2 เครือข่ายภายนอก (External)

เครือข่ายภายนอก(External) หรือ แวน(WAN) หรือ Untrusted Network เป็นโซนที่มีการเชื่อมต่อโดยตรงกับเน็ตเวิร์คภายนอกหรืออินเตอร์เน็ต โดยส่วนมากโซนนี้ของอุปกรณ์ไฟร์วอลล์จะเชื่อมต่ออยู่กับเร้าต์เตอร์ (Router) หรือ ADSL และเชื่อมต่อไปยังผู้ให้บริการอินเตอร์เน็ต (Internet Service Provider) ไอพีในโซนนี้จะเป็นกลุ่มของไอพีสาธารณะ ซึ่งผู้ให้บริการอินเตอร์เน็ตจะเป็นผู้กำหนดให้ ดังนั้นไอพีกลุ่มนี้จึงสามารถสื่อสารกับกลุ่มไอพีสาธารณะได้ทั่วโลก

โดยทั่วไปการใช้งานไอพีสาธารณะของโซนนี้จะมีทั้งแบบที่เป็นระบุมาแบบตายตัว (Fix)และเป็นแบบปรับเปลี่ยนไปเรื่อยๆ (Dynamic) โดยขึ้นอยู่กับผู้ใช้และผู้ให้บริการอินเตอร์เน็ต และด้วยเหตุผลการใช้ไอพีสาธารณะในโซนนี้จึงกลายไปเป็นช่องทางให้ผู้บุกรุกหรือแฮกเกอร์สามารถเข้าถึงเครือข่ายของภายในได้โดยง่ายหากปราศจากการป้องกัน

2.2.3 โซนปลอดทหาร หรือ DMZ (Demilitarized zone)

โซนปลอดทหารหรือ DMZ (Demilitarized zone) หรือ Semi-Trusted Network เป็นโซนที่สามารถเข้าถึงได้ทั้งจากภายในและภายนอก อุปกรณ์ที่อยู่ในโซนนี้ได้แก่เครื่องเซิร์ฟเวอร์ที่เปิดให้บริการแบบสาธารณะ เช่น เว็บเซิร์ฟเวอร์ (Web Server), เมล์เซิร์ฟเวอร์ (Mail Server), DNS เซิร์ฟเวอร์ เป็นต้น ไอพีที่ใช้ในโซนนี้เป็นได้ทั้งไอพีสาธารณและไอพีส่วนบุคคล ซึ่งขึ้นอยู่กับการออกแบบของผู้ดูแลระบบ

เนื่องด้วยโซนนี้มีการป้องกันน้อยที่สุด จึงจำเป็นต้องมีมาตรการณ์ในการควบคุมการผ่านเข้าออกอย่างเคร่งครัดเพื่อไม่ให้การเข้าถึงจากภายนอกทะลุต่อไปยังโซนอื่นๆที่อยู่ภายในได้

ดังนั้นในบางองค์กรจึงสามารถมีโซนมากกว่า 3 โซน ซึ่งจะขึ้นอยู่กับการออกแบบของผู้ดูแลระบบของของแต่ละองค์กร เช่น มีการเพิ่มโซนแขกหรือผู้มาเยือน (Guest or Visitor) เข้ามาไว้ให้สำหรับการให้บริการไวไฟ (Wi-Fi) เพื่อเข้าสู่อินเตอร์เน็ตเพียงอย่างเดียว ไม่สามารถเข้าถึงโซน LAN หรือเครื่องแม่ข่าย (Server) ขององค์กรได้

จากบทความข้างต้นทางผู้จัดทำได้นำมาวิเคราะห์ในโครงงานเพื่อใช้ในการคัดแยกเซิร์ฟเวอร์ต่างๆที่อยู่ภายในองค์กรให้อยู่ในโซนที่ถูกต้องเหมาะสม เพื่อเพิ่มความปลอดภัยในการเชื่อมต่อ เพื่อช่วยในการจัดสรรไอพีแอดเดรสให้อุปกรณ์ต่างๆและเพื่อกำหนดนโยบายด้านความปลอดภัยบนตัวอุปกรณ์ไฟร์วอลล์ได้อย่างถูกต้อง

2.3 ชนิด หน้าที่และตำแหน่งที่ควรจัดวางของเซิร์ฟเวอร์

จากการวิเคราะห์บทความต่างๆ ถึงชนิดและหน้าที่ของเซิร์ฟเวอร์ที่มีการใช้งานกันอย่างแพร่หลายในปัจุบัน และการค้นคว้าข้อมูลจากสื่อต่างๆ รวมถึงจากการสอบถามจากผู้เชี่ยวชาญฉพาะทางสามารถสรุปออกมาเป็นข้อมูลต่างๆได้ ตามตารางที่ 2.1

ตารางที่ 2.1 แสดงชนิด หน้าที่และตำแหน่งที่ควรจัดวางบนระบบเครือข่ายเพื่อความปลอดภัยของเซิร์ฟเวอร์แต่ละชนิด

Server	Service	Protocol/Port	Zone (Internal, DMZ)
Web Server	Web Service (Internal)	TCP: 80, 443	Internal
	Web Service (External)	TCP: 80, 443	DMZ

ตารางที่ 2.1 (ต่อ)

Server	Service	Protocol/Port	Zone (Internal, DMZ)
NTP Server	NTP Service	TCP: 123 UDP: 123	Internal
Window Server	DNS Service	TCP: 53	Internal
	Mail Server Exchange (SMTP)	TCP: 25	DMZ, Internal
	Mail Server Exchange (POP3)	TCP: 110	DMZ, Internal
	Active Directory Service	TCP: 88, 389, 3268-3269 UDP: 389, 88	Internal
	DHCP Service	UDP: 67, 68, 2535	Internal
IBM Server	Mail Server Lotus Note(Client)	TCP: 1352 UDP: 1352	DMZ
	Traveler Service non secure	TCP: 80, 8642	DMZ
	Traveler Service secure	TCP: 443, 8642	DMZ
	Sametime Chat Service	TCP: 1516, 1533	Internal
File Server	File Service	TCP: 21, 22	Internal
	File Shares Service	TCP: 139, 445 UDP: 137-138, 445	Internal
Database Server	MS SQL Monitor	TCP: 1434 UDP: 1434	Internal
	MS SQL Server	TCP: 1433 UDP: 1433	Internal
RADIUS Server	RADIUS Accounting Service	UDP: 1646	Internal
	RADIUS Acct RFC	UDP: 1813	Internal
	RADIUS RFC	UDP: 1812	Internal

ตารางที่ 2.1 (ต่อ)

Server	Service	Protocol/Port	Zone (Internal, DMZ)
SNMP Server	SNMP	UDP: 161	Internal
	SNMP-Trap	UDP: 162	Internal
VPN Gateway	VPN SSL Service	TCP: 443	DMZ
	VPN PPTP Service	TCP: 1723 GRE	DMZ
	VPN IP Sec Service	UDP: 500, 4500 ESP, AH	DMZ
Print Server	Print Service	TCP: 139, 445 UDP: 137-138, 445	Internal

2.4 การสร้างนโยบายด้านความปลอดภัย (Security Policy) บนอุปกรณ์ไฟร์วอลล์

ไฟร์วอลล์มีหน้าที่หลักในการกรองข้อมูลแพคเก็ตให้เหลือเพียงเฉพาะส่วนที่ได้รับอนุญาตให้สามารถผ่านตัวมันไปได้ ดังนั้นการเขียนนโยบายด้านความปลอดภัย (Security Policy) หรือกฎควบคุมการผ่านเข้าออก (Access Control Rule) สำหรับไฟร์วอลล์จึงเป็นเรื่องที่สำคัญ เพราะถ้ามีการเขียนหรือออกแบบในส่วนนี้ผิดพลาดหรือหละหลวมจะส่งผลให้องค์กรถูกผู้ไม่ประสงค์ดีจากทั้งภายในและภายนอกองค์กรบุกรุกโจมตีจนทำให้องค์กรเกิดความเสียหายได้

2.4.1 การเริ่มต้นก่อนการสร้างนโยบายบนอุปกรณ์ไฟร์วอล์

การเริ่มต้นในการสร้างนโยบายด้านความปลอดภัย (Security Policy) หรือกฎควบคุมการผ่านเข้าออก (Access Control Rule) ควรเริ่มจากการปิดการให้บริการทั้งหมดก่อน เพราะหากเริ่มจากการเปิดช่องทางการให้บริการ (Service) ทั้งหมดในตอนแรกอาจทำให้เกิดการสร้างกฎที่หละหลวมจนมากเกินความจำเป็น ส่งผลให้เกิดความเสี่ยงต่อการถูกบุกรุกได้โดยง่าย ดังนั้นการเปิดช่องทางการให้บริการยิ่งน้อยจะยิ่งสามารถลดช่องโหว่และลดโอกาสในการถูกโจมตีได้มากขึ้น

รวมถึงยังสามารถลดการใช้งานซีพียู (CPU) และหน่วยความจำของอุปกรณ์ไฟร์วอลล์ได้ด้วยเช่นกัน

2.4.2 การสร้างกฎในการควบคุมการผ่านเข้าออกของข้อมูล (Access Control Rule)

หลักการสร้างนโยบายบนไฟร์วอลล์และกฎที่ดีคือ ความง่าย (Simplicity) ซึ่งในที่นี้หมายถึงการสร้างกฎที่สั้น อ่านง่าย และได้ใจความสำคัญจากชื่อของกฎนั้นๆ การสร้างกฎในการควบคุมการผ่านเข้าออกของข้อมูลที่ดีไม่ควรมีกฎมากกว่า 30 ข้อเพราะข้อเสียของการมีกฎหลายข้อจะทำให้เกิดความสับสนและอาจจะทำให้เกิดความผิดพลาดของผู้สร้างเอง แต่ทั้งนี้ทั้งนั้นปริมาณกฎก็มักจะขึ้นอยู่กับความสามารถของตัวอุปกรณ์เองด้วยเช่นกัน ถ้าตัวอุปกรณ์ไม่รองรับการจับกลุ่มของกฎก็อาจจำเป็นต้องสร้างกฎที่มากกว่า 30 ข้อขึ้นไป

การสร้างกฎของไฟร์วอลล์ในแต่ละครั้งจะถือได้ว่าเป็นการนำนโยบายด้านความปลอดภัย (Security Policy) ขององค์กรมาบังคับใช้งานในทางเทคนิคโดยใช้ไฟร์วอลล์เป็นเครื่องมือทำให้เกิดผลตามที่ต้องการ นอกจากนี้ยังมีกฎบางข้อที่ผู้ดูแลระบบควรเพิ่มเข้าไปเพิ่มเติมเพื่อประสิทธิภาพด้านความปลอดภัยที่ดีขึ้นด้วยตนเอง เช่น การป้องกัน IP Spoofing และ Land Attack ซึ่งจะกล่าวไว้ในภาคผนวกเพิ่มเติม

2.4.3 การจัดเรียงลำดับของกฎบนอุปกรณ์ไฟร์วอลล์

การเรียงลำดับของกฎถือว่ามีความสำคัญเป็นอันดับต้นๆเพราะไฟร์วอลล์โดยส่วนใหญ่ทำงานแบบ ซีเควน (Sequence) คือตรวจสอบแพคเก็ตกับกฎตามลำดับที่ถูกสร้างไว้เมื่อข้อมูลตรงกับกฎข้อที่อยู่บนๆ ก็จะทำตามกฎข้อนั้นๆ โดยไม่พิจารณาข้อที่อยู่ในลำดับถัดไปแต่อย่างใด ดังนั้นหลักการคือให้วางกฎที่เป็นกฎทั่วๆไปไว้ด้านล่างและให้นำกฎที่มีความเฉพาะเจาะจงมาไว้ด้านบน

ตัวอย่างที่ 1 ให้นำกฎที่ทำหน้าที่บล็อกไอพีแอดเดรสไปไว้ด้านบนเพื่อให้มั่นใจว่าถ้ามีแพคเก็ตที่มีไอพีแอดเดรสตรงตามที่ระบุไว้แพคเก็ตนั้นๆจะถูกตัดทิ้ง (Drop)ไปก่อนที่จะไปตรงกับกฎข้ออื่นๆ

ตัวอย่างที่ 2 การวางกฎที่มีการตัดทุกแพคเก็ตทิ้ง (Drop)ไว้ด้านล่างสุดและกฎที่เหลือจะเป็นแค่กฎที่อนุญาต (Allow) เฉพาะบางช่องทางการใช้งานโดยจะวางอยู่ด้านบน

ในกรณีนี้ถ้ามีการเรียงผิดพลาดโดยนำกฎที่ตัดทิ้งทุกแพคเก็ตไว้บนสุดจะกลายเป็นว่าไม่มีเครื่องใดๆ ภายในระบบเครือข่ายสามารถรับส่งข้อมูลต่างๆผ่านไฟร์วอลล์ได้เลย

จากบทความข้างต้นทางผู้จัดทำได้นำมาปรับใช้งานในส่วนของระบบการเรียงลำดับและรูปแบบการสร้างกฎภายโครงงาน โดยการสร้างจะเริ่มจากการวางกฎที่ตัดทุกแพคเก็ตไว้ด้านล่างสุด (อันดับสุดท้าย) และเปิดช่องทางการให้บริการเฉพาะส่วนงานที่สำคัญไว้ส่วนที่อยู่เหนือขึ้นไป

2.4.4 การกรองข้อมูลตาม TCP/IP

การกรอง TCP/IP สามารถกำหนดได้ 2 รูปแบบคือ

1. Default ACCEPT: ผู้ดูแลระบบจะต้องสร้างกฎเพื่อกำหนดว่าจะปิด (Drop) การให้บริการ(Service)และโฮสต์ใดได้บ้าง โดยการให้บริการและโฮสต์อื่นๆ นอกเหนือจากที่กำหนดไว้จะมีค่าเป็นเปิดคืออนุญาต (Allow)
2. Default DROP: ผู้ดูแลระบบจะต้องสร้างกฎเพื่อกำหนดว่าจะเปิด (Allow) การให้บริการ(Service)และโฮสต์ใดได้บ้าง โดยการให้บริการและโฮสต์อื่นๆ นอกเหนือจากที่กำหนดไว้จะมีค่าเป็นปิดคือไม่อนุญาต (Drop)

ตารางที่ 2.2 แสดง TCP/UDP Service ที่ควรปิดกั้นที่ไฟร์วอลล์ไม่ให้ใช้ทั้งจากภายในและภายนอกเครือข่าย

Port(s) (Transport)	Server	Port(s) (Transport)	Server
1 (TCP & UDP)	tcpmux	1981 (TCP)	Shockrave
7 (TCP & UDP)	echo	1999 (TCP)	BackDoor
9 (TCP & UDP)	discard	2001 (TCP)	Trojan Cow
11 (TCP & UDP)	systat	2023 (TCP)	Ripper
13 (TCP & UDP)	daytime	2049 (TCP & UDP)	Nfs
15 (TCP & UDP)	netstat	2115 (TCP)	Bugs
17 (TCP & UDP)	qotd	2140 (TCP)	Deep Throat
19 (TCP & UDP)	chargen	2222 (TCP)	Subseven21
37 (TCP & UDP)	time	2301 (TCP & UDP)	Compaqdiag
43 (TCP & UDP)	whois	2565 (TCP)	Striker
67 (TCP & UDP)	bootps	2583 (TCP)	WinCrash
68 (TCP & UDP)	bootpc	2701 (TCP & UDP)	sms-rcinfo

ตารางที่ 2.2 (ต่อ)

Port(s) (Transport)	Server
69 (UDP)	tftp
93 (TCP)	supdup
111 (TCP & UDP)	sunrpc
135 (TCP & UDP)	loc-srv
137 (TCP & UDP)	netbios-ns
138 (TCP & UDP)	netbios-dgm
139 (TCP & UDP)	netbios-ssn
177 (TCP & UDP)	xdmcp
445 (TCP & UDP)	microsoft-ds
512 (TCP)	rexec
513 (TCP)	rlogin
513 (UDP)	who
514 (TCP)	rsh, rcp, rdist, rdump, rrestore
515 (TCP)	lpr
517 (UCP)	talk
518 (UCP)	ntalk

Port(s) (Transport)	Server
2702 (TCP & UDP)	sms-remctrl
2703 (TCP & UDP)	sms-chat
2704 (TCP & UDP)	sms-xfer
2801 (TCP)	Phineas P.
1600 (TCP)	Shivka-Burka
1761 - 1764 (TCP & UDP)	sms-helpdesk
1807 (TCP)	SpySender
4045 (TCP)	Lockd
5800 - 5899 (TCP)	winvnc web server
5900 - 5999 (TCP)	Winvnc
6000 - 6063 (TCP)	X11 Window System
6665 - 6669 (TCP)	Irc
6711 - 6712 (TCP)	Subseven
6776 (TCP)	Subseven
7000 (TCP)	Subseven21
12345 - 12346 (TCP)	NetBus

ตารางที่ 2.3 แสดง TCP/UDP Service ที่ควรปิดกั้นไม่ให้เข้ามาจากภายนอก

Port(s) (Transport)	Server
79 (TCP)	finger
161 (TCP & UDP)	snmp
162 (TCP & UDP)	snmp trap
514 (UDP)	syslog
550 (TCP & UDP)	new who

ตารางที่ 2.4 แสดง TCP/UDP service ที่อาจเปิดให้บริการใน DMZ โดยในทางปฏิบัติให้เปิดเฉพาะการให้บริการ(service) ที่มีการให้บริการจริงเท่านั้น

Port(s) (Transport)	Server
20 (TCP)	ftpdata
21 (TCP)	ftp
22 (TCP)	ssh
23 (TCP)	telnet
25 (TCP)	smtp
53 (TCP & UDP)	domain
80 (TCP)	http
110 (TCP)	pop3
119 (TCP)	nntp
123 (TCP)	ntp
143 (TCP)	imap
179 (TCP)	bgp
389 (TCP & UDP)	ldap
443 (TCP)	ssl
1080 (TCP)	socks
3128 (TCP)	squid
8000 (TCP)	http (alternate)
8080 (TCP)	http-alt
8888 (TCP)	http (alternate)

ตารางที่ 2.5 แสดง ICMP message ที่ควรอนุญาตให้ออกไปจากเครือข่ายภายในได้

Message Type	
Number	**Name**
4	source quench
8	echo request (ping)
12	parameter problem

ตารางที่ 2.6 แสดง ICMP message ที่ควรอนุญาตให้เข้ามายังเครือข่ายภายในได้

Message Type	
Number	**Name**
0	echo reply
3	destination unreachable
4	source quench
11	time exceeded
12	parameter problem

จากการวิเคราะห์ข้อมูลการกลั่นกรองข้อมูลทำให้ทราบว่าการควบคุมการผ่านเข้าและออกในส่วนที่เป็น TCP/UDP ไม่เพียงพอ จำเป็นต้องมีการอนุญาต ICMP เพิ่มเติมเพื่อช่วยให้ผู้ดูแลระบบสามารถวิเคราะห์หาปัญหาที่เกิดจากการเชื่อมต่อภายในระบบเครือข่ายได้ ซึ่งข้อมูลดังกล่าวจะถูกนำมาใช้ในการสร้างกฎและนโยบายแบบอัตโนมัติเพิ่มเติมมานอกเหนือจากการอนุญาตแค่การให้บริการตามเซิร์ฟเวอร์

2.5 ลักษณะของระบบสารสนเทศภายในองค์กร

จากการรวบรวมข้อมูลทางด้านระบบสารสนเทศสำหรับองค์กรในประเทศไทย ที่มีขนาดเล็กซึ่งมีจำนวนพนักงานไม่เกิน 50 คนและองค์กรขนาดกลางที่มีจำนวนพนักงานมากกว่า 50 คนแต่ไม่เกิน 200 คน พบว่ามีการออกแบบระบบหรือการแบ่งโซนทางด้านเครือข่ายที่คล้ายคลึงกัน โดยจะอธิบายแยกเป็นองค์กรขนาดเล็กและขนาดกลางดังนี้

2.5.1 องค์กรขนาดเล็ก

ลักษณะการจัดแบ่งองค์กรสำหรับธุรกิจขนาดเล็กซึ่งมีจำนวนพนักงานไม่เกิน 50 คน มักมีการแบ่งแยกโซนทางด้านความปลอดภัยอยู่ในระดับ 2-3 โซน โดยนับรวมโซนที่เป็นเครือข่ายภายนอก(External) หรือ WAN เป็น 1 โซน และเซิร์ฟเวอร์ที่ทำหน้าที่ให้บริการส่วนใหญ่คือ เว็บเซิร์ฟเวอร์, อีเมล์เซิร์ฟเวอร์, ปริ๊นซ์เซิร์ฟเวอร์และเซิร์ฟเวอร์ที่จัดการเกี่ยวกับชื่อยูสเซอร์ (Active Directory Server) เป็นหลัก

2.5.2 องค์กรขนาดกลาง

ลักษณะการจัดแบ่งองค์กรสำหรับธุรกิจขนาดกลางซึ่งมีจำนวนพนักงานไม่ต่ำกว่า 50 และไม่เกิน 200 คน มักมีการแบ่งแยกโซนทางด้านความปลอดภัยอยู่ในระดับ 3-4 โซนโดยนับรวมโซนที่เป็นเครือข่ายภายนอก (External) เป็น 1 โซน และเซิร์ฟเวอร์ที่ทำหน้าที่ให้บริการส่วนใหญ่คือ เว็บเซิร์ฟเวอร์, อีเมล์เซิร์ฟเวอร์, ปริ๊นซ์เซิร์ฟเวอร์, ไฟล์เซิร์ฟเวอร์, เซิร์ฟเวอร์ที่จัดการเกี่ยวกับรายชื่อผู้ใช้งาน (Active Directory Server), เซิร์ฟเวอร์ที่ดูแลความปลอดภัยที่มาจากไวรัส (Anti-Virus Server), เว็บพร็อกซี่ (Web Proxy), อีเมล์เกตเวย์ (E-mail Gateway) และเซิร์ฟเวอร์ที่ทำงานเฉพาะทาง เช่น ERP และ POS สำหรับบางกลุ่มธุรกิจ และโซนที่ถูกแบ่งมักจะอยู่ในช่วง 2-4 โซน

โดยข้อมูลดังกล่าวข้างต้นได้จากการรวบรวมข้อมูลของบริษัทขนาดกลางและขนาดเล็กจากกลุ่มธุรกิจต่างๆกัน 17 แห่ง ดังตารางที่ 2.7 เพื่อนำมาใช้ในการวิเคราะห์ในส่วนการจัดสรรโซนทางด้านความปลอดภัย

ตารางที่ 2.7 แสดงข้อมูลเซิร์ฟเวอร์ขององค์กรขนาดเล็กและขนาดกลาง

ประเภทธุรกิจ	ประเภทของเซิร์ฟเวอร์	โซน *	หมายเหตุ
ธุรกิจหลักทรัพย์จัดการกองทุนรวม	Web Server for External Email Exchange Server	3	
ธุรกิจโรงสีข้าว	Web Server for External Email Exchange Server	2	
รับก่อสร้างตึกและบ้าน	Web Server for External Email Exchange Server ERP Server File Server	4	Guest
ค้าขายอุปกรณ์เกี่ยวกับอุปกรณ์ถ่ายภาพ	Web Server for External Email Exchange Server ERP Server POS Server AntiVirus Server	2	

ตารางที่ 2.7 (ต่อ)

ประเภทธุรกิจ	ประเภทของเซิร์ฟเวอร์	โซน *	หมายเหตุ
ผลิตยารักษาโรค	Web Server for External Email Lotus Note/Domino Server Email Gateway Server Proxy Server File Server AntiVirus Server ERP Server	4	
ผลิตเครื่องหนัง	Web Server for External Email Exchange Server	2	
อุตสาหกรรมอาหาร	Web Server for External Email Exchange Server Active Directory Server	3	
ผลิตผลไม้กระป๋อง	Web Server for External Email Lotus Note/Domino Server Email Gateway Server AntiVirus Server SSL/VPN Gateway Server IDS Server Email Lotus Traveller ERP Server Citrix Server	4	
ผลิตวัสดุขวดและฉลากพลาสติก	Email Lotus Note/Domino Application Server Active Directory Server DNS Server FTP Server	3	

ตารางที่ 2.7 (ต่อ)

ประเภทธุรกิจ	ประเภทของเซิร์ฟเวอร์	โซน *	หมายเหตุ
จัดทำสื่อโฆษณา	Web Server for External Email Exchange Server Active Directory Server Application Server	2	
แปลเอกสาร	Web Server for External Secure Web Server for External Web Server for Internal Email Exchange Server FTP Server Active Directory Server AntiVirus Server	4	
ผลิตชิ้นส่วนคอมพิวเตอร์ 1	Web Server for External Secure Web Server for External Email Exchange Server Active Directory Server AntiVirus Server	3	
ธุรกิจโรงแรม 1	Web Server for External Email Exchange Server	3	Wifi zone
ผลิตอุปกรณ์กีฬาฮ๊อกกี้	Web Server for External Secure Web Server for External Email Exchange Server Web OWA FTP Server AntiVirus Server	3	

ตารางที่ 2.7 (ต่อ)

ประเภทธุรกิจ	ประเภทของเซิร์ฟเวอร์	โซน *	หมายเหตุ
ผลิตชิ้นส่วนคอมพิวเตอร์ 2	Web Server for External Email Exchange Server Active Directory Server Application Server FTP Server CCTV Gateway Server	3	
ธุรกิจโรงแรม 2	Web Server for External Secure Web for External Email Exchange Server Remote Desktop Gateway Active Directory Server DNS Server	2	VLAN

* โซนภายนอก (External) นับเป็น 1 โซน โดยไม่รวมโซนที่เป็นกลุ่มของไคล์แอนท์

และรูปแบบการสื่อสารของแอปพลิเคชั่นและเซิร์ฟเวอร์แต่ละชนิดที่ทางผู้จัดทำได้จากการรวบรวมข้อมูลขององค์กรขนาดกลางและขนาดเล็ก สามารถสรุปได้ตามตารางที่ 2.8 – 2.15 ดังนี้

ตารางที่ 2.8 แสดงรูปแบบการสื่อสารของ Web Server Service

ลักษณะการเชื่อมต่อ	วัตถุประสงค์	พอร์ต	หมายเหตุ
Web Server Service			
เชื่อมต่อกับ Anti Virus Server Service	เพื่ออัพเดตแพทเทินของ Anti Virus	แตกต่างไปตาม Anti Virus Server Service แต่ละผลิตภัณฑ์ *	จะเกิดขึ้นเมื่อมี Anti Virus Server Service อยู่ในองค์กร
เชื่อมต่อกับ external ในการใช้งานอินเตอร์เน็ต (web service)	เพื่อใช้งานอินเตอร์เน็ต	HTTP (TCP 80), HTTPS (TCP 443) และ DNS (TCP,UDP 53)	จะเกิดขึ้นเมื่อเครื่องเซิร์ฟเวอร์ดังกล่าวต้องการใช้งานอินเตอร์เน็ต

ตารางที่ 2.8 (ต่อ)

ลักษณะการเชื่อมต่อ	วัตถุประสงค์	พอร์ต	หมายเหตุ
Web Server Service			
เชื่อมต่อกับ Active Directory Server Service	เพื่อเชื่อมต่อกับ Active Directory Server Service	LDAP (TCP/UDP 389), LDAP GC (TCP/UDP 3268), SMB (TCP/UDP 445), RPC (TCP135), Window Time (UDP 123) NetBIOS Datagram Service (UDP 138), NetBIOS Name Resolution (UDP 137), NetBIOS Session Service (TCP 139)	จะเกิดขึ้นเมื่อเครื่องเซิร์ฟเวอร์เป็นสมาชิกของโดเมน
รับการเชื่อมต่อจากภายนอก	เพื่อให้บริการเว็บเซอร์วิส	TCP 80 และ TCP 443	จะเกิดขึ้นเมื่อเครื่องเซิร์ฟเวอร์ดังกล่าวต้องให้บริการคนภายนอกองค์กร
รับการเชื่อมต่อจากภายใน (ไคลแอนและเซิร์ฟเวอร์)	เพื่อให้บริการเว็บเซอร์วิส	TCP 80 และ TCP 443	

ตารางที่ 2.9 แสดงรูปแบบการสื่อสารของ Exchange Email Server Service

ลักษณะการเชื่อมต่อ	วัตถุประสงค์	พอร์ต	หมายเหตุ
Exchange Email Server Service			
เชื่อมต่อกับ anti virus server service	เพื่ออัพเดตแพทเทินของ anti-virus	แตกต่างไปตามแต่ละผลิตภัณฑ์ *	จะเกิดขึ้นเมื่อมี anti-virus server อยู่ในองค์กร
เชื่อมต่อกับ external ในการใช้งานอีเมล	เพื่อใช้ในการส่งอีเมลกับภายนอก	TCP 25 (SMTP), TCP 465 (SMTPs)	

ตารางที่ 2.9 (ต่อ)

ลักษณะการเชื่อมต่อ	วัตถุประสงค์	พอร์ต	หมายเหตุ
Exchange Email Server Service			
เชื่อมต่อกับ external ในการใช้งานอินเตอร์เน็ต (web service)	เพื่อช้งานอินเตอร์เน็ต	HTTP (TCP 80), HTTPS (TCP 443) และ DNS (TCP,UDP 53)	จะเกิดขึ้นเมื่อเครื่องเซิร์ฟเวอร์ดังกล่าวต้องการใช้งานอินเตอร์เน็ต
รับการเชื่อมต่อจากไคล์แอนท์	เพื่อใช้ในการรับส่งอีเมล	POP3 (TCP 110), POP3s (TCP 995), IMAP (TCP 143), IMAPs (TCP 993)	
รับการเชื่อมต่อกับ external ในการใช้งานอีเมล	เพื่อใช้ในการรับอีเมลกับภายนอก	TCP 25 (SMTP), TCP 465 (SMTPs)	
เชื่อมต่อกับ Active Directory Server Service	เพื่อเชื่อมต่อกับ Active Directory Server Service	LDAP (TCP/UDP 389), LDAP GC (TCP/UDP 3268), SMB (TCP/UDP 445), RPC (TCP135), Window Time (UDP 123) NetBIOS Datagram Service (UDP 138), NetBIOS Name Resolution (UDP 137), NetBIOS Session Service (TCP 139)	จะเกิดขึ้นเมื่อเครื่องเซิร์ฟเวอร์เป็นสมาชิกของโดเมน

ตารางที่ 2.10 แสดงรูปแบบการสื่อสารของ Active Directory Server Service

ลักษณะการเชื่อมต่อ	วัตถุประสงค์	พอร์ต	หมายเหตุ
Active Directory Server Service			
เชื่อมต่อกับ anti virus server service	เพื่ออัพเดตแพทเทินของ anti-virus	แตกต่างไปตามแต่ละผลิตภัณฑ์ *	จะเกิดขึ้นเมื่อมี anti-virus server อยู่ในองค์กร
เชื่อมต่อกับ external ในการใช้งานอินเตอร์เน็ต (web service)	เพื่อช้างานอินเตอร์เน็ต	HTTP (TCP 80), HTTPS (TCP 443) และ DNS (TCP,UDP 53)	จะเกิดขึ้นเมื่อเครื่องเซิร์ฟเวอร์ดังกล่าวต้องการใช้งานอินเตอร์เน็ต
รับการเชื่อมต่อจากไคล์แอนท์	เพื่อใช้ในการของ Active Directory	LDAP (TCP/UDP 389), LDAP GC (TCP/UDP 3268), SMB (TCP/UDP 445), RPC (TCP135), Window Time (UDP 123) NetBIOS Datagram Service (UDP 138), NetBIOS Name Resolution (UDP 137), NetBIOS Session Service (TCP 139)	

ตารางที่ 2.11 แสดงรูปแบบการสื่อสารของ DHCP Server Service

ลักษณะการเชื่อมต่อ	วัตถุประสงค์	พอร์ต	หมายเหตุ
DHCP Server Service			
เชื่อมต่อกับ anti virus server service	เพื่ออัพเดตแพทเทินของ anti-virus	แตกต่างไปตามแต่ละผลิตภัณฑ์ *	จะเกิดขึ้นเมื่อมี anti-virus server อยู่ในองค์กร
รับการเชื่อมต่อจากไคล์แอนท์	เพื่อรับไอพีแอดเดรส	DHCP (UDP 67, UDP 2535)	

ตารางที่ 2.11 (ต่อ)

ลักษณะการเชื่อมต่อ	วัตถุประสงค์	พอร์ต	หมายเหตุ
DHCP Server Service			
เชื่อมต่อกับ external ในการใช้งานอินเตอร์เน็ต (web service)	เพื่อช้งานอินเตอร์เน็ต	HTTP (TCP 80), HTTPS (TCP 443) และ DNS (TCP,UDP 53)	จะเกิดขึ้นเมื่อเครื่องเซิร์ฟเวอร์ดังกล่าวต้องการใช้งานอินเตอร์เน็ต

ตารางที่ 2.12 แสดงรูปแบบการสื่อสารของ DNS Server Service

ลักษณะการเชื่อมต่อ	วัตถุประสงค์	พอร์ต	หมายเหตุ
DNS Server Service			
เชื่อมต่อกับ anti virus server service	เพื่ออัพเดตแพทเทินของ anti-virus	แตกต่างไปตามแต่ละผลิตภัณฑ์ *	จะเกิดขึ้นเมื่อมี anti-virus server อยู่ในองค์กร
เชื่อมต่อกับ external ในการใช้งานอินเตอร์เน็ต (web service)	เพื่อช้งานอินเตอร์เน็ต	HTTP (TCP 80), HTTPS (TCP 443) และ DNS (TCP,UDP 53)	จะเกิดขึ้นเมื่อเครื่องเซิร์ฟเวอร์ดังกล่าวต้องการใช้งานอินเตอร์เน็ต
รับการเชื่อมต่อจากไคล์แอนท์	เพื่อรับการขอใช้บริการ DNS	TCP 53, UDP 53	

ตารางที่ 2.13 แสดงรูปแบบการสื่อสารของ File Shared Server Service

ลักษณะการเชื่อมต่อ	วัตถุประสงค์	พอร์ต	หมายเหตุ
File Shared Server Service			
เชื่อมต่อกับ anti virus server service	เพื่ออัพเดตแพทเทินของ anti-virus	แตกต่างไปตามแต่ละผลิตภัณฑ์ [1]	จะเกิดขึ้นเมื่อมี anti-virus server อยู่ในองค์กร

ตารางที่ 2.13 (ต่อ)

ลักษณะการเชื่อมต่อ	วัตถุประสงค์	พอร์ต	หมายเหตุ
File Shared Server Service			
เชื่อมต่อกับ external ในการใช้งานอินเตอร์เน็ต (web service)	เพื่อช้งานอินเตอร์เน็ต	HTTP (TCP 80), HTTPS (TCP 443) และ DNS (TCP,UDP 53)	จะเกิดขึ้นเมื่อเครื่องเซิร์ฟเวอร์ดังกล่าวต้องการใช้งานอินเตอร์เน็ต
รับการเชื่อมต่อจากไคล์แอนท์	เพื่อรับการขอใช้บริการ ไฟล์แชร์	TCP 20, TCP 21	

ตารางที่ 2.14 แสดงรูปแบบการสื่อสารของ Lotus Email Server Service

ลักษณะการเชื่อมต่อ	วัตถุประสงค์	พอร์ต	หมายเหตุ
Lotus Email Server Service			
เชื่อมต่อกับ Anti-Virus Server Service	เพื่ออัพเดตแพทเทินของ Anti-Virus	แตกต่างไปตามแต่ละผลิตภัณฑ์ *	จะเกิดขึ้นเมื่อมี Anti-Virus Server อยู่ในองค์กร
เชื่อมต่อกับ External ในการใช้งานอีเมล	เพื่อใช้ในการส่งอีเมลกับภายนอก	TCP 25 (SMTP), TCP 465 (SMTPs)	
เชื่อมต่อกับ External ในการใช้งานอินเตอร์เน็ต (Web Service)	เพื่อใช้งานอินเตอร์เน็ต	HTTP (TCP 80), HTTPS (TCP 443) และ DNS (TCP,UDP 53)	จะเกิดขึ้นเมื่อเครื่องเซิร์ฟเวอร์ดังกล่าวต้องการใช้งานอินเตอร์เน็ต
รับการเชื่อมต่อจากไคล์แอนท์	เพื่อใช้ในการรับส่งอีเมล	TCP 1352	
รับการเชื่อมต่อกับ External ในการใช้งานอีเมล	เพื่อใช้ในการรับอีเมลกับภายนอก	TCP 25 (SMTP), TCP 465 (SMTPs)	

ตารางที่ 2.14 (ต่อ)

ลักษณะการเชื่อมต่อ	วัตถุประสงค์	พอร์ต	หมายเหตุ
Lotus Email Server Service			
เชื่อมต่อกับ Active Directory Server Service	เพื่อเชื่อมต่อกับ Active Directory Server Service	LDAP (TCP/UDP 389), LDAP GC (TCP/UDP 3268), SMB (TCP/UDP 445), RPC (TCP135), Window Time (UDP 123) NetBIOS Datagram Service (UDP 138), NetBIOS Name Resolution (UDP 137), NetBIOS Session Service (TCP 139)	จะเกิดขึ้นเมื่อเครื่องเซิร์ฟเวอร์เป็นสมาชิกของโดเมน

ตารางที่ 2.15 ตารางแสดงรูปแบบการสื่อสารของ Application Server Service อื่นๆ

ลักษณะการเชื่อมต่อ	วัตถุประสงค์	พอร์ต	หมายเหตุ
Application Server Service อื่นๆ			
เชื่อมต่อกับ Anti Virus Server Service	เพื่ออัพเดตแพทเทินของ Anti-Virus	แตกต่างไปตามแต่ละผลิตภัณฑ์ *	จะเกิดขึ้นเมื่อมี Anti-Virus Server อยู่ในองค์กร
เชื่อมต่อกับ External ในการใช้งานอินเตอร์เน็ต (Web Service)	เพื่อใช้งานอินเตอร์เน็ต	HTTP (TCP 80), HTTPS (TCP 443) และ DNS (TCP,UDP 53)	จะเกิดขึ้นเมื่อเครื่องเซิร์ฟเวอร์ดังกล่าวต้องการใช้งานอินเตอร์เน็ต
รับการเชื่อมต่อจากไคล์แอนท์	เพื่อใช้ให้บริการ	ตามพอร์ตที่มีการระบุด้วยตนเอง	

ตารางที่ 2.15 (ต่อ)

ลักษณะการเชื่อมต่อ	วัตถุประสงค์	พอร์ต	หมายเหตุ
Application Server Service อื่นๆ			
เชื่อมต่อกับ Active Directory Server Service	เพื่อเชื่อมต่อกับ Active Directory Server Service	LDAP (TCP/UDP 389), LDAP GC (TCP/UDP 3268), SMB (TCP/UDP 445), RPC (TCP135), Window Time (UDP 123) NetBIOS Datagram Service (UDP 138), NetBIOS Name Resolution (UDP 137), NetBIOS Session Service (TCP 139)	จะเกิดขึ้นเมื่อเครื่องเซิร์ฟเวอร์เป็นสมาชิกของโดเมน

Note: * การให้บริการของ Anti-Virus แต่ละผลิตภัณฑ์มีความแตกต่างกันดังนี้

Kaspersky Anti-Virus Server

- Update Anti-Virus Pattern: TCP 13000 -13001, TCP 14000 – 14001

Trend Micro Anti-Virus Server

- Update Anti-Virus Pattern: Update Anti-Virus Pattern: จะต้องระบุเพิ่มเติมลงไป

Symantec Anti-Virus Server

- Update Anti-Virus Pattern: TCP 2967

Mcafee Anti-Virus Server

- Update Anti-Virus Pattern: TCP 80, TCP 443

Nod 32 Anti-Virus Server

- Update Anti-Virus Pattern: TCP 80, TCP 443, TCP 2222

2.6 การจัดสร้างฎกและนโยบายบนอุปกรณ์ทางด้านระบบเครือข่าย

2.6.1 บนอุปกรณ์ซิสโก้ ASA (Cisco ASA)

รูปแบบคำสั่งในการสั่งงานของ Cisco ASA

```
access-list <access_list_name> extended <deny | permit> <protocol> <source_address>
<mask> <dest  address> <mask> <operator port>
```

access_list_name คือชื่อของ Access List

deny | permit คือคำสั่งที่ต้องการสั่งอนุญาตหรือปิดกั้นการสื่อสานชนิดนั้นๆ

protocol คือการระบุชนิดของโปรโตคอล ได้แก่ TCP, UDP หรือ ICMP

source_address, mask คือการกำหนดแอดเดรสต้นทาง หากเป็นเครื่องเดียวให้ระบุ host 192.168.1.1 แต่หากเป็นวงแอดเดรสให้ระบุ 192.168.0.0 255.255.255.0

dest_address, mask คือการกำหนดแอดเดรสต้นทาง ซึ่งระบุได้ดังนี้

- หากเป็นเครื่องเดียวให้ระบุ host 192.168.1.1
- หากเป็นวงแอดเดรสให้ระบุ 192.168.0.0 255.255.255.0

operator port คือการระบุพอร์ต ซึ่งระบุได้ดังนี้

- หากพอร์ตเป็นช่วงให้ระบุ Range 1111 1115 ซึ่งหมายถึง 1111-1115
- หากเป็นพอร์ตเดี่ยวให้ระบุ eq 110

ตัวอย่างที่ 1

```
#access-list client1-acl extended permit tcp 192.168.0.0
255.255.255.0 host 192.168.1.77 eq 80
#access-group client1-acl in interface client1
```

อธิบาย

1. กำหนดให้ Access Control List ชื่อ client1-acl อนุญาตให้เครื่องทุกเครื่องที่อยู่ในวง 1922.168.0.0/24 ไปยังเครื่อง 192.168.1.77 ผ่านทางพอร์ต TCP 80 (Web Server) ได้
2. กำหนดให้ Access Control List ชื่อ client1-acl ถูกประกาศไว้ที่อินเตอร์เฟสที่ชื่อ client1

2.6.2 บนไฟร์วอลล์ลีนุกซ์ IPTables

รูปแบบคำสั่งในการสั่งงานของ IP Table

```
iptable <Table> <Command> <Match> <Target/Jump>
```

Table คือตารางที่ต้องการให้ iptables ทำงานด้วยในกรณีที่ไม่ได้ระบบนั้นจะถือว่าทำงานอยู่กับ Filter Table

Command คือคำสั่งที่ต้องการสั่งให้ iptables ทำอะไร

Match คือการตรวจสอบข้อมูลที่ผ่านเข้ามาใน iptables ว่าตรงตามที่ระบุหรือไม่เพื่อจะได้กระทำกับข้อมูลนั้นต่อไป

Target/Jump คือการกำหนดการกระทำกับข้อมูลเมื่อข้อมูลนั้นตรงตามกฎที่ตั้งไว้ว่าจะอนุญาตให้ผ่านหรือไม่ผ่าน

1. Table

ใน iptables ประกอบด้วยกัน 3 ตาราง (table) หลักคือ Filter Table, NAT Table และ Mangle Table ซึ่งต้องเรียกใช้โดยออปชัน –t และตามด้วยชื่อ Table หารไม่ระบุออปชัน –t ก็จะถือว่าทำงานกับ Filter Table รายละเอียดของแต่ละ Table มีดังนี้

- **Filter Table :** ทำหน้าที่ในการกลั่นกรองข้อมูลที่เข้ามาหรือออกจากโดยที่มี chain หลักอยู่ 3 chain คือ FORWARD จะกลั่นกรองข้อมูลที่ผ่านเข้ามาหาไฟร์วอลล์เพื่อที่ผ่านไปยังปลายทางอื่น, INPUT จะกรองข้อมูลที่เข้ามาหาไฟร์วอลล์อละ OUTPUT จะกรองข้อมูลที่ออกจากไฟร์วอลล์
- **NAT Table:** ทำหน้าที่ในการเปลี่ยนำอพีต้นทาง หรือไอพีปลายทางของข้อมูลซึ่งจะมีอยู่ 2 chain หลักด้วยกันคือ PREROUTING Chain และ POSTROUTING Chain
- **Mangle Table:** ทำหน้าที่ในการแก้ไขค่าต่างๆของ TCP header เพื่อจัดการในส่วนของ QoS โดยจะมี chain ที่เกี่ยวข้องอยู่ดังนี้ PREROUTING, POSTROUTING, OUTPUT, INPUT และ FORWARD

2. Command

ใน iptabel มี command อยู่หลายชนิดด้วยกันดังนี้

- **-A *chain rule:*** เป็นการเพิ่มกฎเพื่อต่อท้าย chain

- **-D *chain rule*** หรือ **–D *chain rulenum:*** เป็นการลบกฎออกจาก chain ซึ่งทำได้ 2 วิธี โดยแบบแรกทำการลบโดยพิมพ์กฎที่ต้องการลบ แบบที่สองคือการลบโดยระบุเลขบรรทัดของกฎ
- **-R *chain [rulenum] rule*:** เป็นการเพิ่มกฎดดยการแทรกเข้าไปใน chain ตามบรรทัดที่ระบุ ถ้าระบุเป็น 1 จะเป็นการแทรกเข้าต้น chain
- **-L *[chain]*:** เป็นการแสดงกฎทั้งหมดที่มีอยู่ใน chain ที่ระบุ ถ้าไม่ระบุ chain จะเป็นการแสดงทุกกฎในทุกๆ chain
- **-F *[chain]*:** เป็นการลบกฎทั้งหมดที่มีอยู่ทั้งหมดใน chain ที่ระบุ ถ้าไม่ระบุเป็นการลบทุกกฎใน chain ดังนั้นการสั่งออปชันนี้ควรระวัง
- **-Z *[chain]*:** เป็นการปรับค่าตัวนับจำนวนข้อมูลของ chain ให้เป็นศูนย์
- **-N *[chain]*:** เป็นการเปิดให้ผู้ใช้สามารถสร้าง chain ใหม่ได้ แต่ชื่อห้ามซ้ำกับ chain เดิมที่มีอยู่
- **-X *[chain]*:** เป็นการลบ chain ที่ผู้ใช้สร้างขึ้น แต่ไม่สามารถลบ chain ที่ระบบสร้างไว้ได้

3. Match

ใช้เพื่อตรวจสอบข้อมูลว่าตรงตามที่ระบุไว้โดยมีออปชันดังนี้

- **-P *[!] protocol*:** เป็นการระบุโปรโตคอล โดยสามารถระบุได้ดังนี้คือ TCP, UDP, ICMP ถ้าใช้ ! เป็นการบอกว่าทุกโปรโตคอลยกเว้นที่ระบุไว้
- **-s *[!] address[/mask]*:** เป็นการระบุหมายเลขต้นทางที่เข้ามาของข้อมูล สามารถกำหนดเป็นชื่อ, ไอพี, ช่วงของไอพี หรือช่วงเน็ตเวิร์คโดยใช้ /mask ระบุ
- **-i *[!] name*:** เป็นการะบุอินเตอร์เฟสขาเข้าของข้อมูล
- **-o *[!] name*:** เป็นการระบุอินเตอร์เฟสขาออกของข้อมูล

4. Target/Jump

เป็นการกระทำกับข้อมูลที่ตรงตามกฎที่ตั้งไว้ว่าจะต้องทำอย่างไรกับข้อมูลนั้นๆ ซึ่งออปชันเหล่านี้จะทำงานตามหลังออปชัน –j

- **ACCEPT:** เป็นการยอมรับข้อมูลนั้นๆ ถือเป็นการจบกระบวนการของ iptables และทำการส่งข้อมูลนั้นๆให้ระบบปฏิบัติการหรือโปรแกรมอื่นๆทำงานต่อ
- **DROP:** เป็นการตัดข้อมูลนั้นๆทิ้ง และเป็นการจบกระบวนการของ iptables
- **REJECT:** เป็นการตัดข้อมูลนั้นๆทิ้งซึ่งเหมือนกับการ DROP แต่แตกต่างกันตรงที่จะมีการส่งข้อความกลับไปบอกผู้ส่งว่าข้อมูลดังกล่าวถูกตัดทิ้ง
- **LOG:** เป็นการบอกให้ส่งข้อมูลของแพคเก็ตไปยัง syslog และ iptables จะนำแพคเก็ตมาตรวจสอบกับกฎข้ออื่นๆต่อไป

ตัวอย่างที่ 1

```
# Iptables –A INPUT –p icmp –s 192.168.1.0/24 –j ACCEPT
# Iptables –A INPUT –p icmp –j DROP
```

อธิบาย

1. Iptable –A INPUT เป็นการเพิ่มกฎเข้าใน table filter /INPUT chain โดยเพิ่มเข้าต่อท้ายกฎเดิมที่มีอยู่, -p ICMP บอกว่าเป็นโปรโตคอล ICMP หรือการ ping, -s 192.168.1.0/24 ระบุต้นทางว่ามาจากเน็ตเวิร์ควง 192.168.1.0/24, -j ACCEPT บอกว่าอนุญาตให้ผ่านออกไป สรุปคืออนุญาตให้เครื่องที่อยู่ใน 192.168.1.0/24 สามารถ ping ได้
2. Iptable –A INPUT เป็นการเพิ่มกฎเข้าใน table filter /INPUT chain โดยเพิ่มเข้าต่อท้ายกฎเดิมที่มีอยู่, -p ICMP บอกว่าเป็นโปรโตคอล ICMP, -j DROP บอกว่าไม่อนุญาตให้ผ่านออกไป สรุปคือไม่อนุญาตให้มีการ ping เข้ามาที่ไฟร์วอลล์ในทุกๆกรณี

ตัวอย่างที่ 2

```
# Iptables -A FORWARD -p udp --dport 53 -j ACCEPT
```

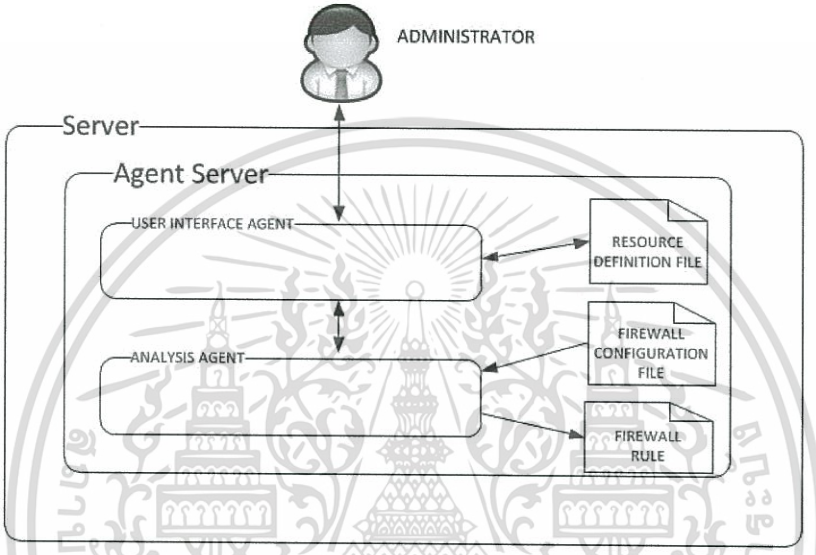
อธิบาย

1. Iptable –a FORWARD เป็นการเพิ่มกฎเข้าไปใน table filter/FORWARD chain โดยเพิ่มเข้าต่อท้ายกฎเดิมที่มีอยู่, -p udp บอกว่าปืนโปรโตคอล UDP, --dport 53 บอกพอร์ทปลายทางเป็นยนพะ 53 ซึ่งก็คือ DNS, -j ACCEPT บอกว่าอนุญาตให้ผ่านออกไป สรุปคืออนุญาตให้ทุกเครื่องใช้งาน DNS ได้

บทที่ 3
การวิเคราะห์และออกแบบระบบ

3.1 สถาปัตยกรรมของระบบออกแบบนโยบายรักษาความปลอดภัยสำหรับอุปกรณ์ไฟร์วอลล์

สถาปัตยกรรมสำหรับระบบออกแบบนโยบายที่ได้ออกแบบไว้แสดงได้ดังรูปที่ 3.1



รูปที่ 3.1 แสดงสถาปัตยกรรมระบบออกแบบนโยบายรักษาความปลอดภัยสำหรับอุปกรณ์ไฟร์วอลล์

ส่วนเซิร์ฟเวอร์ (Server) เป็นส่วนการทำงานที่ทำงานอยู่บนเครื่องที่ติดตั้งซอฟท์แวร์อันประกอบด้วย

1. เอเจนท์ส่วนต่อประสานกับผู้ใช้ (User Interface Agent) ทำหน้าที่เป็นตัวกลางในการติดต่อสื่อสารกับผู้ใช้ระบบกับระบบ มีหน้าที่แสดงข้อมูล, รับข้อมูลตามที่ระบบต้องการและแสดงผลลัพท์ที่ได้จากการวิเคราะห์เพื่อให้ผู้ใช้งานตรวจสอบความถูกต้องของข้อมูล
2. เอเจนท์วิเคราะห์ (Analysis Agent) ทำหน้าที่วิเคราะห์ข้อมูลที่ได้รับมาจากเอเจนท์ส่วนต่อประสานกับผู้ใช้เพื่อให้ได้มาซึ่งข้อมูลสำคัญที่นำมาใช้ประกอบการ

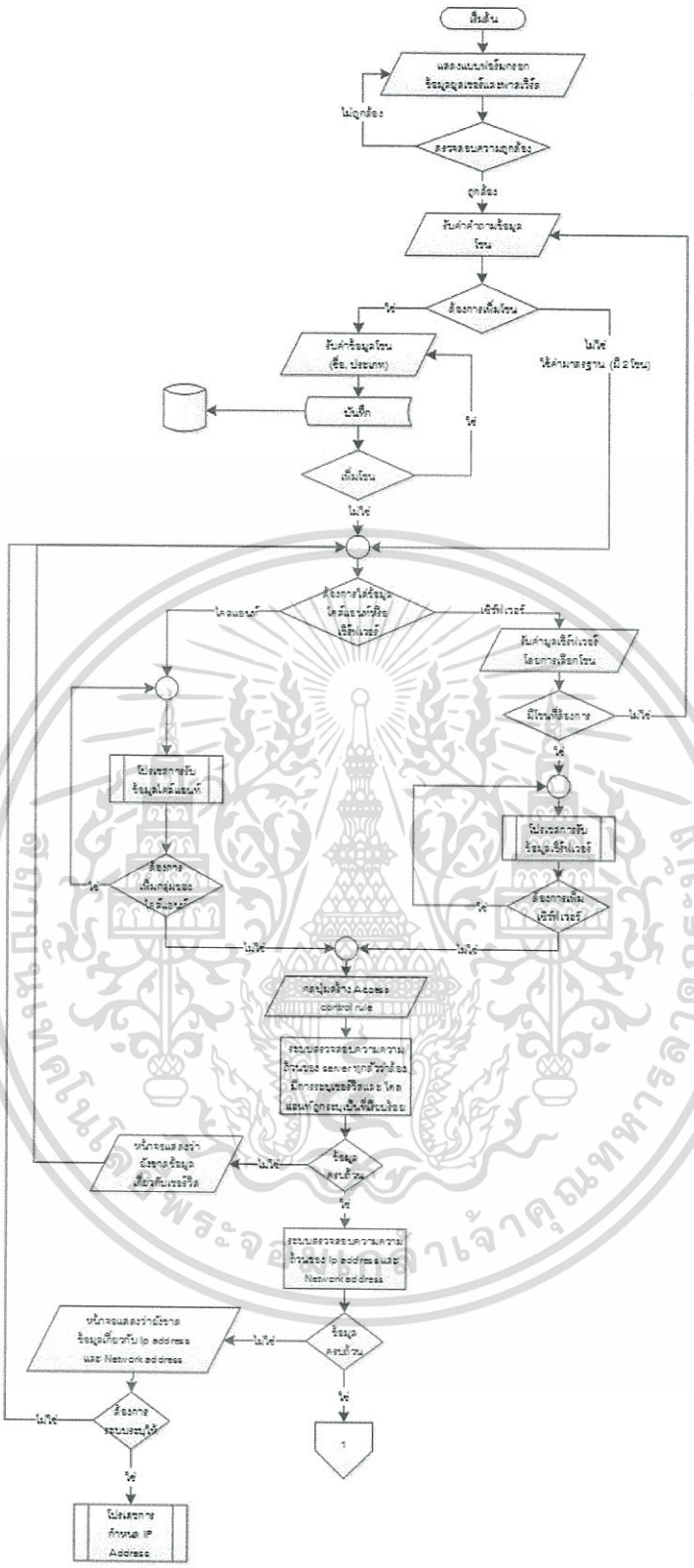
วิเคราะห์หานโยบายด้านความปลอดภัย (Security Policy) หรือกฎควบคุมการผ่านเข้าออก (Access Control Rule) ของแต่ละองค์กร

3. แฟ้มนิยามทรัพยากร (Resource Definition Files) ทำหน้าที่จัดเก็บข้อมูลความสัมพันธ์ระหว่างเซิร์ฟเวอร์และเซอร์วิสของเซิร์ฟเวอร์เพื่อให้ผู้ใช้สามารถใส่ข้อมูลได้ตรงตามความต้องการของระบบ
4. แฟ้มข้อมูลไฟร์วอล์ (Firewall Configuration Files) ทำหน้าที่จัดเก็บข้อมูลรูปแบบโค้ดของไฟร์วอลล์แต่ละผลิตภัณฑ์เพื่อใช้ในการแปลงข้อมูลใช้ตรงตามนโยบายด้านความปลอดภัย (Security Policy) หรือกฎควบคุมการผ่านเข้าออก (Access Control Rule) ของผลิตภัณฑ์นั้นๆ
5. แฟ้มข้อมูลกฎของไฟร์วอลล์ (Firewall Rule) ทำหน้าที่จัดเก็บข้อมูลเอาท์พุตที่ได้จากการสร้างกฎของไฟร์วอลล์ตามโปรไฟล์แต่ละตัวเพื่อนำไปใช้กับอุปกรณ์ไฟร์วอลล์ในลำดับต่อไป

3.2 แผนผังขั้นตอนการทำงานของระบบ

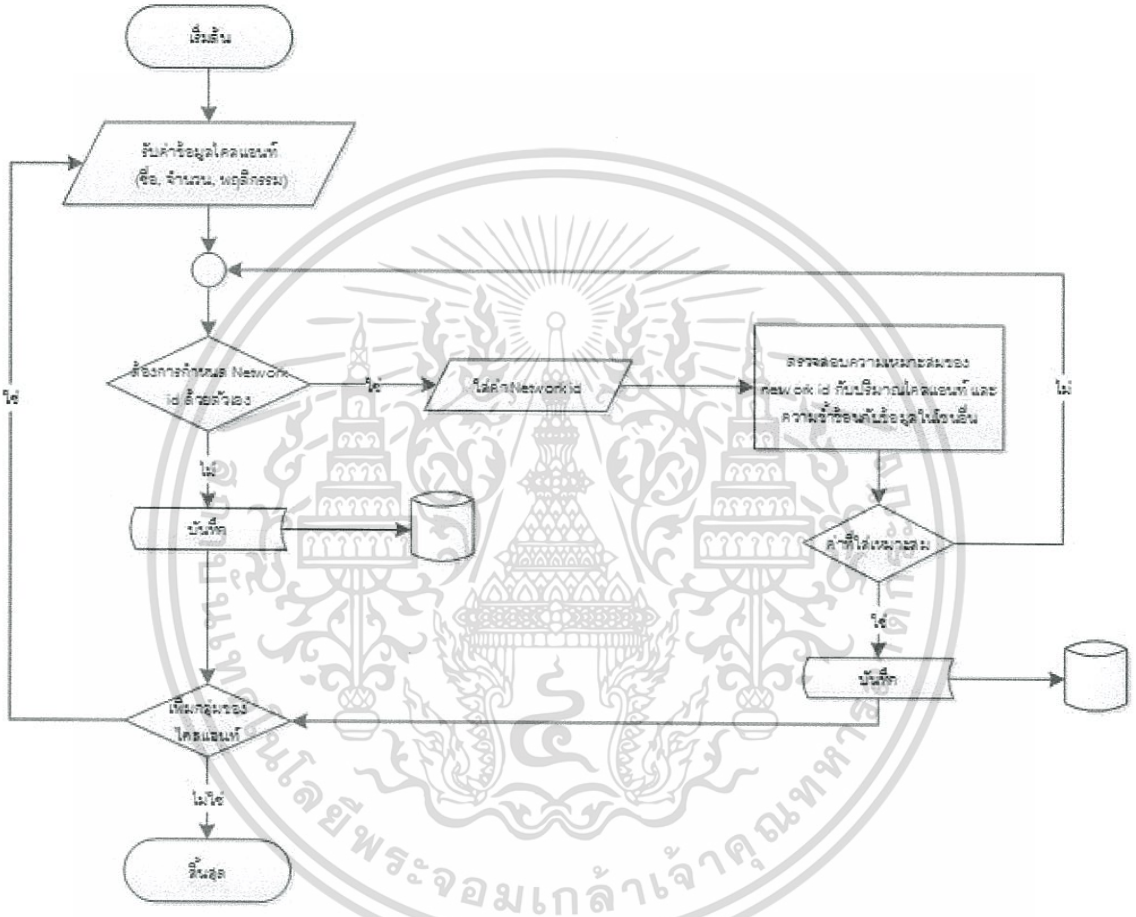
การทำงานขั้นตอนแรกจะเริ่มจากผู้ดูแลระบบเปิดระบบออกแบบและอิมพลีเมนท์นโยบายรักษาความปลอดภัยสำหรับอุปกรณ์ไฟร์วอลล์ ระบบจะแสดงหน้าจอหลักของระบบเพื่อล็อคอิน ซึ่งส่วนนี้ระบบจะรับข้อมูลโซนทางด้านความปลอดภัยที่มีอยู่ในปัจจุบัน โดยผู้ดูแลระบบสามารถใส่จำนวนโซนและชนิดที่มีอยู่ทั้งหมดเข้าระบบได้ทันที แต่ถ้ายังไม่มีการจัดสรรโซนด้านความปลอดภัย ระบบจะมองว่าปัจจุบันมีการแบ่งโซนเพียง 2 โซนคือภายนอก (External หรือ WAN) และภายใน (Internal) ซึ่งระหว่างนั้นผู้ดูแลระบบสามารถใส่ข้อมูลของเซิร์ฟเวอร์ ลักษณะการให้บริการของเซิร์ฟเวอร์ เซอร์วิสที่ให้บริการ ข้อมูลไคลแอนท์ และไอพีแอดเดรสไปพร้อมๆกันได้ โดยโซนสำหรับไคลแอนท์จะถูกแยกออกจากโซนที่มีการวางเซิร์ฟเวอร์อย่างชัดเจน

การใส่ข้อมูลไอพีแอดเดรส ผู้ดูแลระบบสามารถกำหนดได้เอง หรือถ้ายังไม่แน่ใจในการกำหนดข้อมูลดังกล่าวสามารถให้ระบบสร้างให้ในภายหลังได้เช่นกัน ดังรายละเอียดที่แสดงในรูปที่ 3.2



รูปที่ 3.2 แสดงแผนผังการทำงานขั้นตอนโดยรวมของการรับข้อมูลเซิร์ฟเวอร์ ไคลแอนท์และไอพีแอดเดรส

สำหรับโปรเสซการรับข้อมูลของไคลแอนท์นั้น ผู้ดูแลระบบต้องตั้งชื่อโซนหรือกลุ่มของไคลแอนท์ ระบุจำนวนของเครื่องไคลแอนท์ที่มีอยู่ในโซนดังกล่าว กำหนดฤติกรรมว่าไคลแอนท์ที่อยู่ในโซนนั้นๆสามารถใช้งานอินเตอร์เน็ตได้หรือไม่ และกำหนดค่าเน็ตเวิร์คแอดเดรสให้กับไคลแอนท์ในโซนนั้นๆ แต่การกำหนดค่าเน็ตเวิร์คแอดเดรสนั้นทางผู้ดูแลระบบสามารถเลือกที่จะไม่กำหนดแล้วให้ระบบเป็นตัวกำหนดให้ในภายหลังได้ ดังรายละเอียดที่แสดงในรูปที่ 3.3



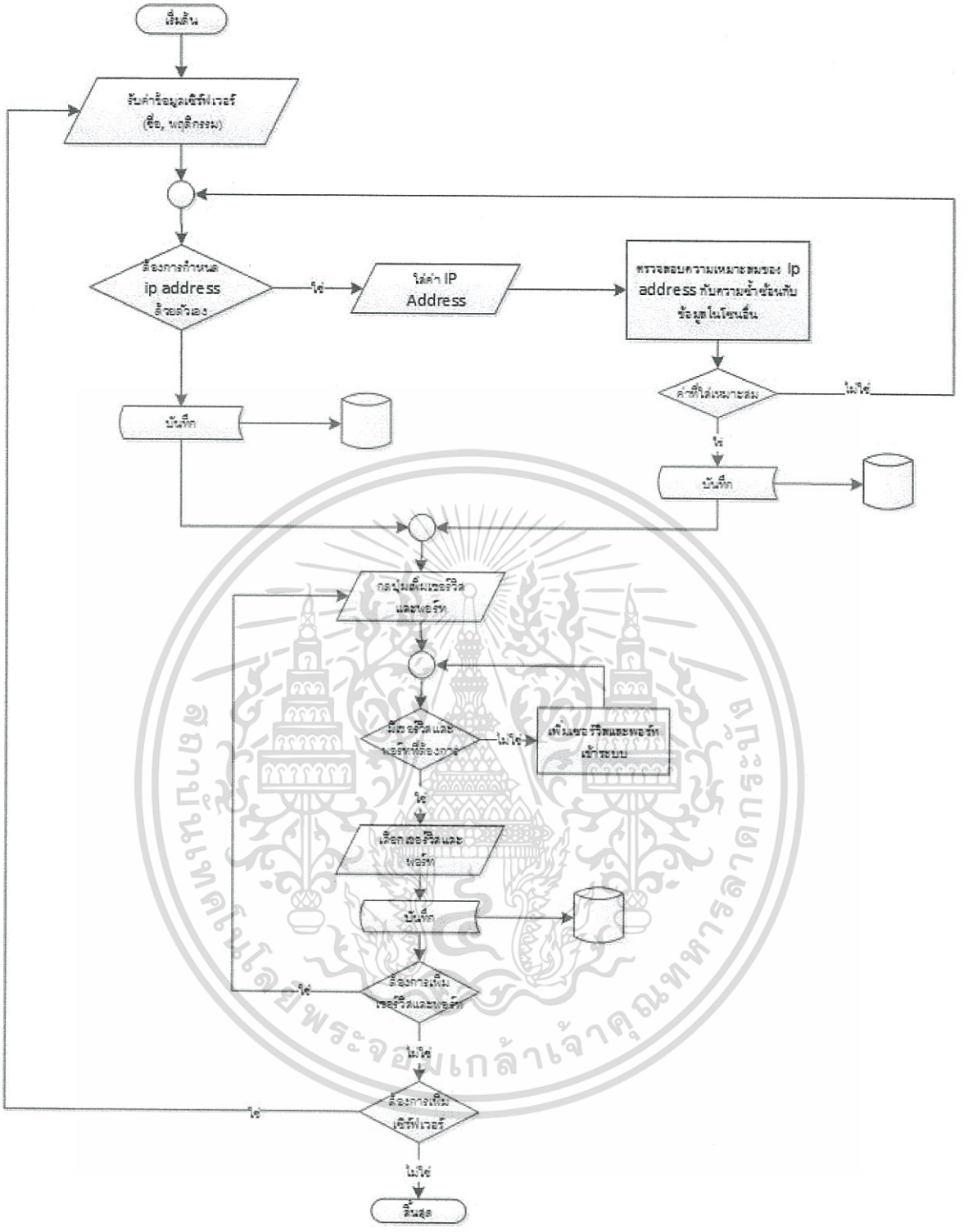
รูปที่ 3.3 แสดงแผนผังการทำงานขั้นตอนการรับข้อมูลไคลแอนท์

สำหรับโปรเสซการรับข้อมูลของเซิร์ฟเวอร์นั้น ผู้ดูแลระบบต้องตั้งชื่อเซิร์ฟเวอร์ กำหนดฤติกรรมว่าเซิร์ฟเวอร์เครื่องนั้นๆสามารถใช้งานอินเตอร์เน็ตได้หรือไม่ ระบุหน้าที่การให้บริการของเซิร์ฟเวอร์เครื่องนั้นๆ โดยการเลือกจากค่ามาตรฐานที่ระบบมีตั้งต้นให้อยู่แล้ว แต่หากตัวเลือกที่ระบบมีให้ไม่ตรงตามลักษณะการทำงานตามที่องค์กรมี ทางผู้ดูแลระบบสามารถกำหนดรายละเอียดในส่วนดังกล่าวเพิ่มเติมลงไปได้เช่นกัน

ในกำหนดหน้าที่การให้บริการของเซิร์ฟเวอร์ ทางผู้ดูแลระบบสามารถเลือกหน้าที่ได้มากกว่าหนึ่ง ซึ่งขึ้นอยู่กับสภาพแวดล้อมขององค์กรที่มี

หลังจากระบุข้อมูลข้างต้นเป็นที่เรียบร้อย ผู้ดูแลระบบสามารถกำหนดค่าไอพีแอดเดรสลงไปในส่วนนี้ได้เลยเช่นกัน ซึ่งในการกำหนดค่าไอพีแดอเดรสนั้น ระบบจะมีการตรวจสอบอยู่เสมอว่าค่าที่กำหนดลงไปนั้นมีไอพีซ้ำกับเซิร์ฟเวอร์ตัวอื่น หรือมีค่าเน็ตเวิร์คที่ซ้ำกับโซนอื่นๆที่มีอยู่แล้วหรือไม่

โดยในการกำหนดค่าไอพีแอดเดรสนั้นสามารถเลือกที่จะไม่กำหนดแล้วให้ระบบเป็นตัวกำหนดให้ในภายหลังได้ ดังรายละเอียดที่แสดงในรูปที่ 3.4

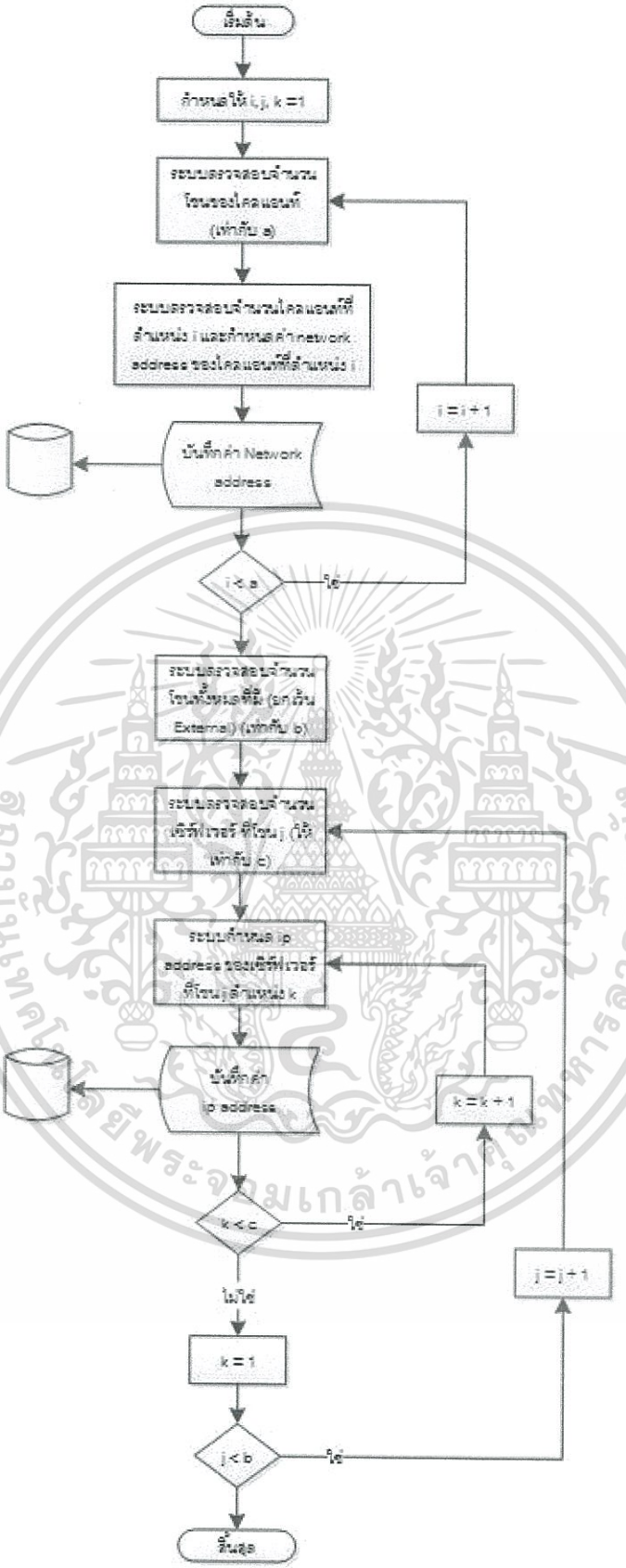


รูปที่ 3.4 แสดงแผนผังการทำงานขั้นตอนการรับข้อมูลเซิร์ฟเวอร์

สำหรับโปรเสซการกำหนดำไอพีแอดเดรส จะแบ่งออกเป็น 2 กรณี

1. ยังไม่มีการระบุไอพีแอดเดรสหรือเน็ตเวิร์คแอดเดรสไว้แต่อย่างใด
2. มีการระบุไอพีแอดเดรสหรือเน็ตเวิร์คแอดเดรสไว้ในบางส่วน

ในกรณีที่ยังไม่มีการระบุไอพีแอดเดรสหรือเน็ตเวิร์คแอดเดรสไว้แต่อย่างใด ระบบจะเริ่มจากข้อมูลในส่วนของไคลแอนท์ โดยพิจารณาจากจำนวนของไคลแอนท์ที่มีในแต่ละโซนและสร้างเน็ตเวิร์คแอดเดรสที่สัมพันธ์กับจำนวนนั้นๆ ออกมา และหลังจากนั้นระบบจะกำหนดค่าไอพีแอดเดรสให้กับเครื่องเซิร์ฟเวอร์ทีละโซน ดังรายละเอียดที่แสดงในรูปที่ 3.5

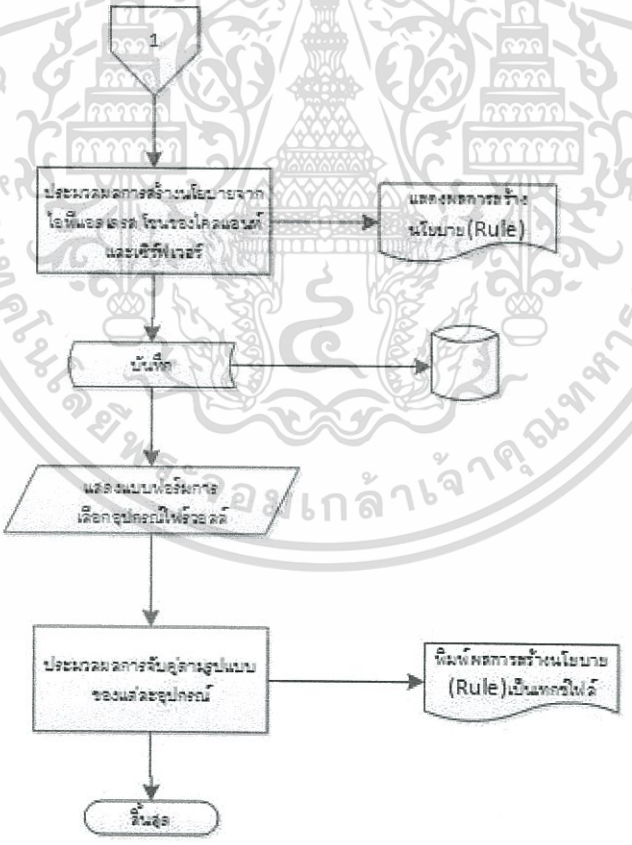


รูปที่ 3.5 แสดงแผนผังการทำงานขั้นตอนการกำหนดไอพีแอดเดรส

ในกรณีที่มีการระบุไอพีแอดเดรสหรือเน็ตเวิร์คแอดเดรสไว้ในบางส่วน ระบบจะเริ่มจากข้อมูลในส่วนของไคลแอนท์เช่นกัน ซึ่งระบบจะพิจารณาจากจำนวนของไคลแอนท์ที่มีในแต่ละโซนและสร้างเน็ตเวิร์คแอดเดรสที่สัมพันธ์กับจำนวนนั้นๆ โดยไม่ให้ซ้ำกับเน็ตเวิร์คแอดเดรสที่มีอยู่เดิม และหลังจากนั้นระบบจะกำหนดค่าไอพีแอดเดรสให้กับเครื่องเซิร์ฟเวอร์ทีละโซน โดยไอพีที่ได้จะเป็นไอพีที่อยู่วงเดียวกับเซิร์ฟเวอร์ที่มีอยู่เดิมแต่ไม่ซ้ำค่ากัน

หลังจากข้อมูลข้างต้นถูกกำหนดครบถ้วนและได้รับการยืนยันเป็นที่เรียบร้อย ระบบจะทำการวิเคราะห์เพื่อสร้างกฎควบคุมการผ่านเข้าและออกของข้อมูลทางด้านระบบเครือข่ายออกมาตามหลักการและจัดลำดับเพื่อให้ผู้ดูแลระบบนำข้อมูลไปใช้ในการพัฒนาความปลอดภัยให้กับระบบเครือข่ายขององค์กรตนเอง

จากนั้นระบบจะแสดงรายชื่อผลิตภัณฑ์ไฟร์วอลล์ให้ผู้ดูแลระบบเลือกและสร้างออกมาเป็นไฟล์ให้ผู้ดูแลระบบทำการบันทึกเพื่อนำไปใช้ประโยชน์ในลำดับถัดไป ดังรายละเอียดที่แสดงในรูปที่ 3.6



รูปที่ 3.6 แสดงแผนผังการทำงานขั้นตอนการกำหนดไอพีแอดเดรส

3.3 ยูสเคสไดอะแกรม

ยูสเคสไดอะแกรมเป็นแผนภาพที่แสดงให้เห็นถึงความสัมพันธ์และปฏิสัมพันธ์ระหว่างระบบกับสิ่งแวดล้อมภายนอกระบบ ทำให้ทราบถึงความสามารถหรือฟังก์ชันการทำงานของระบบและผู้ที่เกี่ยวข้องกับระบบที่พัฒนา โยยูสเคสไดอะแกรมของระบบออกแบบและอิมพลีเมนท์นโยบายรักษาความปลอดภัยสำหรับอุปกรณ์ไฟร์วอลล์ประกอบด้วย 7 ยูสเคส คือ ระบบจัดการผู้ใช้งาน (User) ระบบรับข้อมูลโซนด้านความปลอดภัยและข้อมูลเซิร์ฟเวอร์/ไคลแอนท์ ระบบจัดแบ่งโซนเพื่อความปลอดภัย ระบบจัดสรรไอพีแอดเดรส (IP Address) ระบบสร้างกฎและนโยบายเพื่อความปลอดภัย ระบบเรียงลำดับกฎและนโยบายด้านความปลอดภัยและระบบสร้างกฎและนโยบายด้านความปลอดภัยสำหรับอุปกรณ์ไฟร์วอลล์แบบระบุชื่อผลิตภัณฑ์ ดังรูปที่ 3.7

รูปที่ 3.7 แสดงยูสเคสไดอะแกรมของระบบออกแบบและอิมพลีเมนท์นโยบายรักษาความปลอดภัยสำหรับอุปกรณ์ไฟร์วอลล์

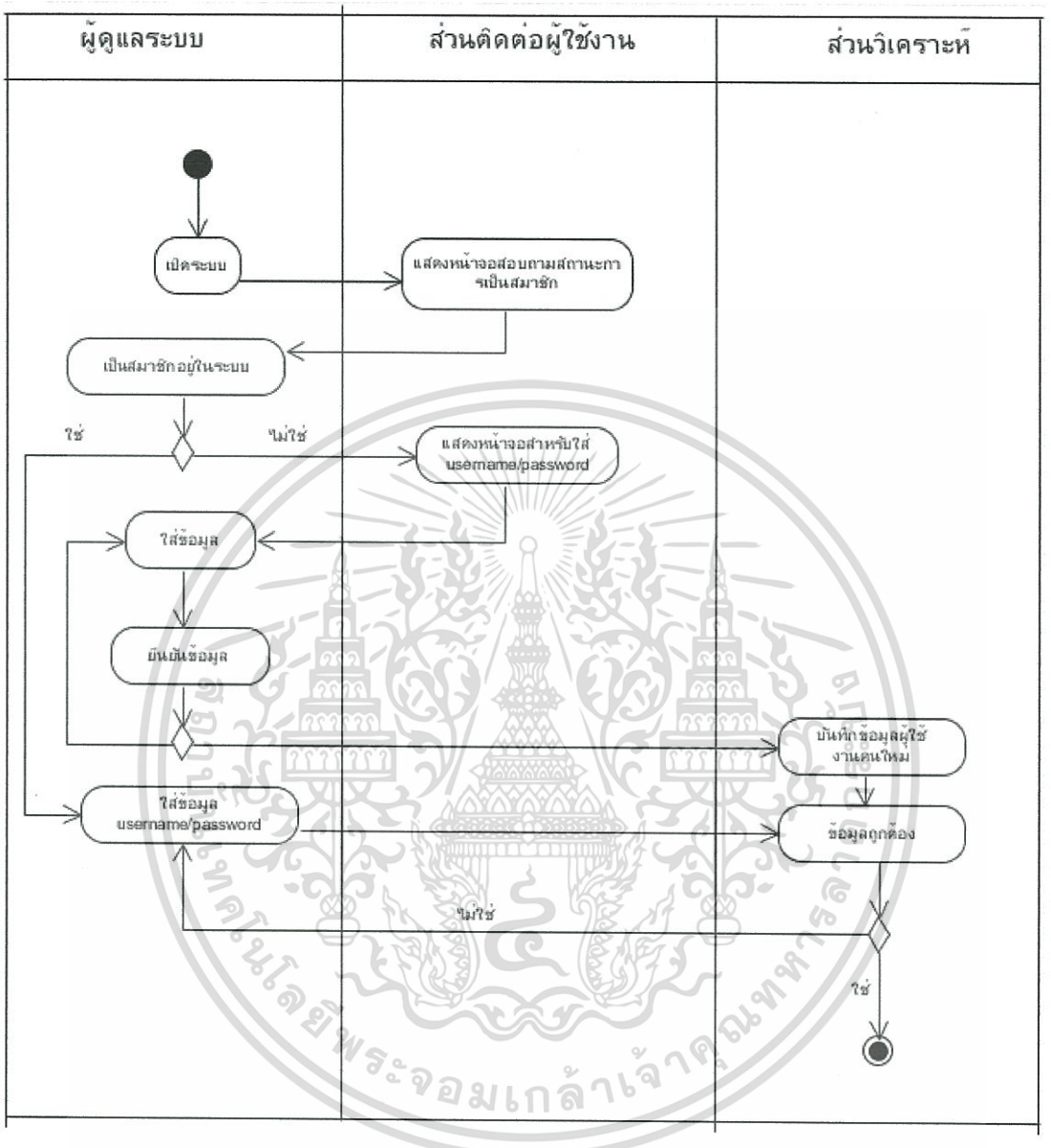
ตารางที่ 3.1 คำอธิบายยูสเคสจัดการผู้ใช้งาน (User)

รหัสยูสเคส	UC01
ยูสเคส	จัดการผู้ใช้งาน (User)
วัตถุประสงค์	เพื่อตรวจสอบความถูกต้องของยูสเซอร์
เงื่อนไขเมื่อเริ่มต้น	ผู้ดูแลระบบเปิดระบบ
เมื่อทำงานเสร็จ	สามารถสร้างโปรไฟล์เพื่อสร้างนโยบายทางด้านความปลอดภัยในลำดับถัดไป

ตารางที่ 3.1 (ต่อ)

เมื่อทำงานไม่เสร็จ	ไม่สามารถเข้าสู่ระบบได้	
แอกเตอร์ที่เกี่ยวข้อง	ผู้ดูแลระบบและผู้ดูแลความปลอดภัยของระบบ	
สิ่งกระตุ้นการทำงาน	ผู้ดูแลระบบและผู้ดูแลความปลอดภัยของระบบเข้าสู่หน้าหลักของระบบและต้องการทราบนโยบายด้านความปลอดภัยสำหรับองค์กรตนเอง	
อินพุต	ยูสเซอร์เนมและพาสเวิร์ด	
เอาต์พุต	หน้าจอรับค่าเพื่อสร้างโปรไฟล์	
สถานการณ์	-	
รายละเอียด	**แอกเตอร์**	**ระบบ**
	1. ผู้ดูแลระบบเปิดระบบ	1.1 ระบบแสดงหน้าจอสอบถามสถานะของการเป็นสมาชิก
	2. กดปุ่ม	
	2a. กดปุ่มไม่ใช่เมื่อไม่ได้เป็นสมาชิก - ใส่ข้อมูลเพื่อทำการลงทะเบียน - ยันยันข้อมูล	2a.1 ระบบแสดงหน้าจอสำหรับใส่ยูสเซอร์เนมและพาสเวิร์ด 2a.2 ระบบบันทึกข้อมูลผู้ใช้งาน
	2b. กดปุ่มใช่เมื่อไม่ได้เป็นสมาชิก - ใส่ข้อมูลเพื่อยืนยันตัวตน	2b.1 ระบบแสดงหน้าจอสำหรับใส่ยูสเซอร์เนมและพาสเวิร์ด 2b.2 ระบบตรวจสอบความถูกต้องของข้อมูล - ข้อมูลถูกต้องจะเข้าสู่หน้าหลักของระบบ ข้อมูลไม่ถูกต้อง กลับไปขั้นตอน 2b

แอกทิวิตีไดอะแกรมการทำงานสำหรับยูสเคสจัดการผู้ใช้งาน (User) สามารถแสดงได้ดังรูปที่ 3.8



รูปที่ 3.8 แอกทิวิตีไดอะแกรมการทำงานสำหรับจัดการผู้ใช้งาน (User)

ตารางที่ 3.2 คำอธิบายยูสเคสรับข้อมูลในส่วนติดต่อผู้ใช้งาน

รหัสยูสเคส	UC02
ยูสเคส	รับข้อมูลโซนด้านความปลอดภัยและข้อมูลเซิร์ฟเวอร์ในส่วนติดต่อผู้ใช้งาน
วัตถุประสงค์	เพื่อให้ผู้ดูแลระบบสามารถใส่ข้อมูลของอุปกรณ์เครือข่ายที่มีแตกต่างกันในแต่ละองค์กร
เงื่อนไขเมื่อเริ่มต้น	ผู้ดูแลล็อคอินเข้าระบบ

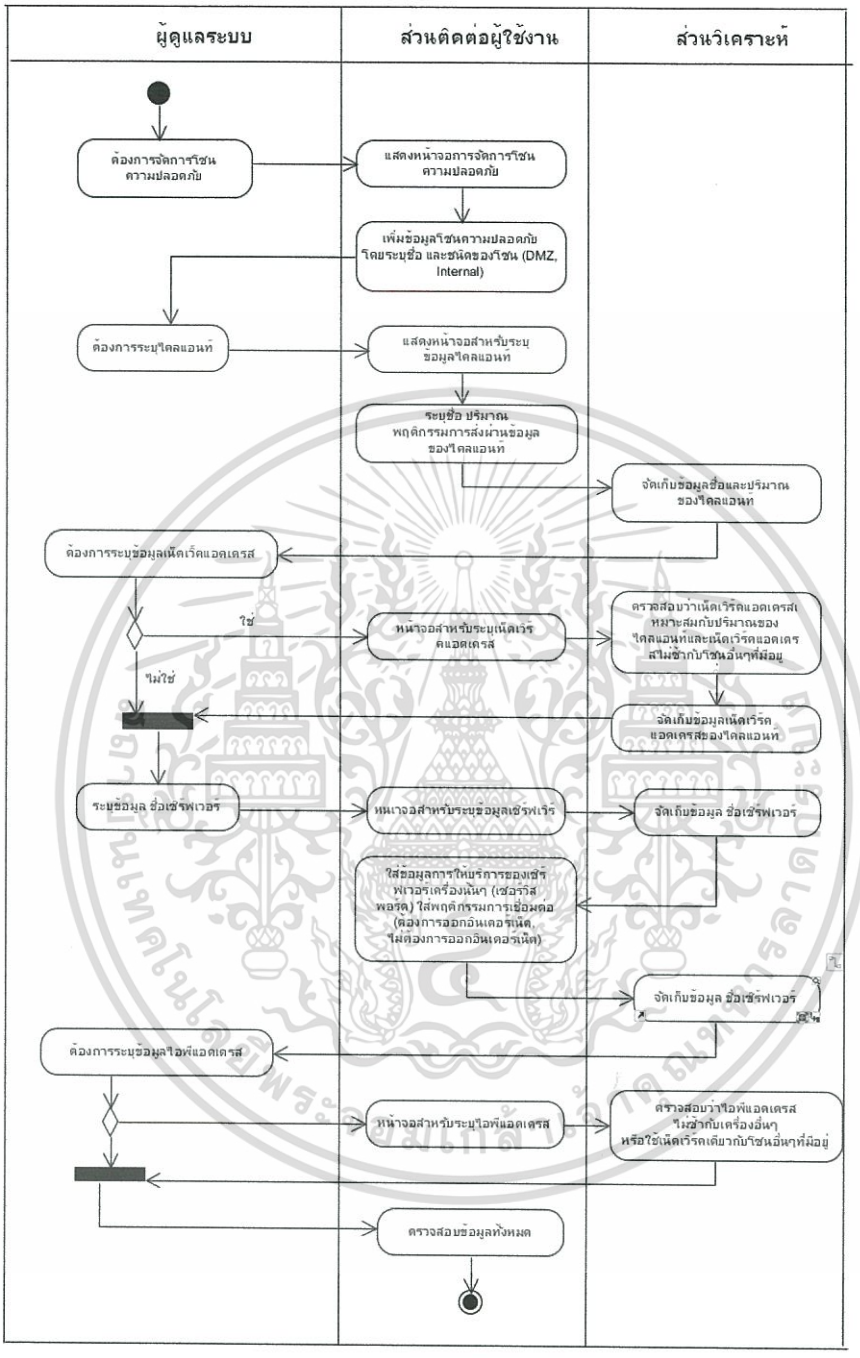
ตารางที่ 3.2 (ต่อ)

เมื่อทำงานเสร็จ	แสดงข้อมูลปริมาณโซนทางด้านความปลอดภัยและข้อมูลเซิร์ฟเวอร์ทั้งหมดได้อย่างถูกต้อง	
เมื่อทำงานไม่เสร็จ	ไม่สามารถจัดแบ่งโซนตามสภาพแวดล้อมของแต่ละองค์กรได้	
แอกเตอร์ที่เกี่ยวข้อง	ผู้ดูแลระบบและผู้ดูแลความปลอดภัยของระบบ	
สิ่งกระตุ้นการทำงาน	ผู้ดูแลระบบล็อคอินถูกต้อง	
อินพุต	1. ข้อมูลโซนทางด้านความปลอดภัยในปัจจุบันที่มีอยู่ 2. ข้อมูลไคลแอนท์ ได้แก่ ปริมาณและพฤติกรรมการเชื่อมต่อ 3. ข้อมูลเซิร์ฟเวอร์ได้แก่ ชนิดการให้บริการ, พอร์ต และพฤติกรรมการเชื่อมต่อ	
เอาต์พุต	ข้อมูลสภาพแวดล้อมบนระบบเครือข่ายที่มีอยู่ทั้งหมดของแต่ละองค์กร	
สถานการณ์	แก้ไขข้อมูลให้ถูกต้อง	
รายละเอียด	**แอกเตอร์**	**ระบบ**
	1. ผู้ดูแลระบบผ่านการล็อคอินเข้าสู่ระบบ และเลือกที่จะจัดการข้อมูลโซนความปลอดภัยที่มีอยู่	1.1 แสดงหน้าจอการจัดการโซนความปลอดภัย
	2. ผู้ดูแลระบบเริ่มกรอกข้อมูลโซน	
	2a. ไม่มีการกรอกข้อมูลเพิ่มเติม ซึ่งหมายความว่ามีโซนอยู่แค่2 โซน คืออินเทอร์เน็ตและโซนภายใน (ไม่รวมโซนไคลแอนท์)	2a.1 ข้ามไปที่ข้อ 3
	2b. มีการกรอกข้อมูลเพิ่มเติม - ใส่ชื่อของโซน - ระบุชนิดของโซน (DMZ, Internal)	2b.1 ระบบจัดเก็บข้อมูลโซน
	3. ใส่ข้อมูลไคลแอนท์	
	3a. ใส่ชื่อกลุ่มของไคลแอนท์	3a.1 ระบบจัดเก็บชื่อของไคลแอนท์
	3b. ใส่ปริมาณไคลแอนท์ในกลุ่มนั้น	3b.1 ระบบจัดเก็บปริมาณของไคลแอนท์
	3c. ใส่พฤติกรรมการเชื่อมต่อ (ต้องการออกอินเตอร์เน็ต, ไม่ต้องการออกอินเตอร์เน็ต)	3c.1 ระบบจัดเก็บพฤติกรรมการเชื่อมต่อ
	3d. ใส่ค่าเน็ตเวิร์คแอดเดรส	3d.1 ระบบตรวจสอบว่าเน็ตเวิร์คแอดเดรสเหมาะสมกับปริมาณของไคลแอนท์

ตารางที่ 3.2 (ต่อ)

รายละเอียด	แอกเตอร์	ระบบ
		3d.2 ระบบตรวจสอบว่าเน็ตเวิร์คแอดเดรสไม่ซ้ำกับโซนอื่นๆที่มีอยู่ 3d.3 ระบบจัดเก็บข้อมูลเน็ตเวิร์คแอดเดรส
	4. ใส่ข้อมูลเซิร์ฟเวอร์	
	4a. ใส่ชื่อเซิร์ฟเวอร์	4a.1 ระบบจัดเก็บชื่อของเซิร์ฟเวอร์
	4b. ใส่ข้อมูลการให้บริการของเซิร์ฟเวอร์เครื่องนั้นๆ (เซอร์วิสพอร์ต)	4b.1 ระบบแสดงรูปแบบการให้บริการเป็นตัวเลือก 4b.1 ระบบจัดเก็บรูปแบบการให้บริการเป็นตัวเลือก
	4c. ใส่พฤติกรรมการเชื่อมต่อ (ต้องการออกอินเตอร์เน็ต, ไม่ต้องการออกอินเตอร์เน็ต)	4c.1 ระบบจัดเก็บพฤติกรรมการเชื่อมต่อ
	4d. ใส่ค่าไอพีแอดเดรส (ถ้ามี)	4d.1 ระบบตรวจสอบว่าไอพีแอดเดรสไม่ซ้ำกับโซนอื่นๆที่มีอยู่ 4d.2 ระบบจัดเก็บข้อมูลไอพีแอดเดรส
	5. ผู้ดูแลระบบตรวจสอบข้อมูล	
	5a. ข้อมูลไม่ถูกต้องถูกต้อง	5a.1 กลับไปที่ข้อ 2 ข้อ 3 และ ข้อ 4 เพื่อให้ผู้ดูแลระบบใส่ข้อมูลใหม่อีกครั้ง
	5b. ข้อมูลถูกต้อง จะกดปุ่มเพื่อสร้าง access control rule	5b.1 ไปยังการทำงานส่วนถัดไป

แอกทิวิตีไดอะแกรมการทำงานสำหรับยูสเคสรับข้อมูลโซนด้านความปลอดภัยและข้อมูลเซิร์ฟเวอร์ในส่วนติดต่อผู้ใช้งาน สามารถแสดงได้ดังรูปที่ 3.9



รูปที่ 3.9 แอกทิวิตีไดอะแกรมการทำงานสำหรับรับข้อมูลโซนด้านความปลอดภัย ข้อมูลไคลแอนท์และข้อมูลเซิร์ฟเวอร์ในส่วนติดต่อผู้ใช้งาน

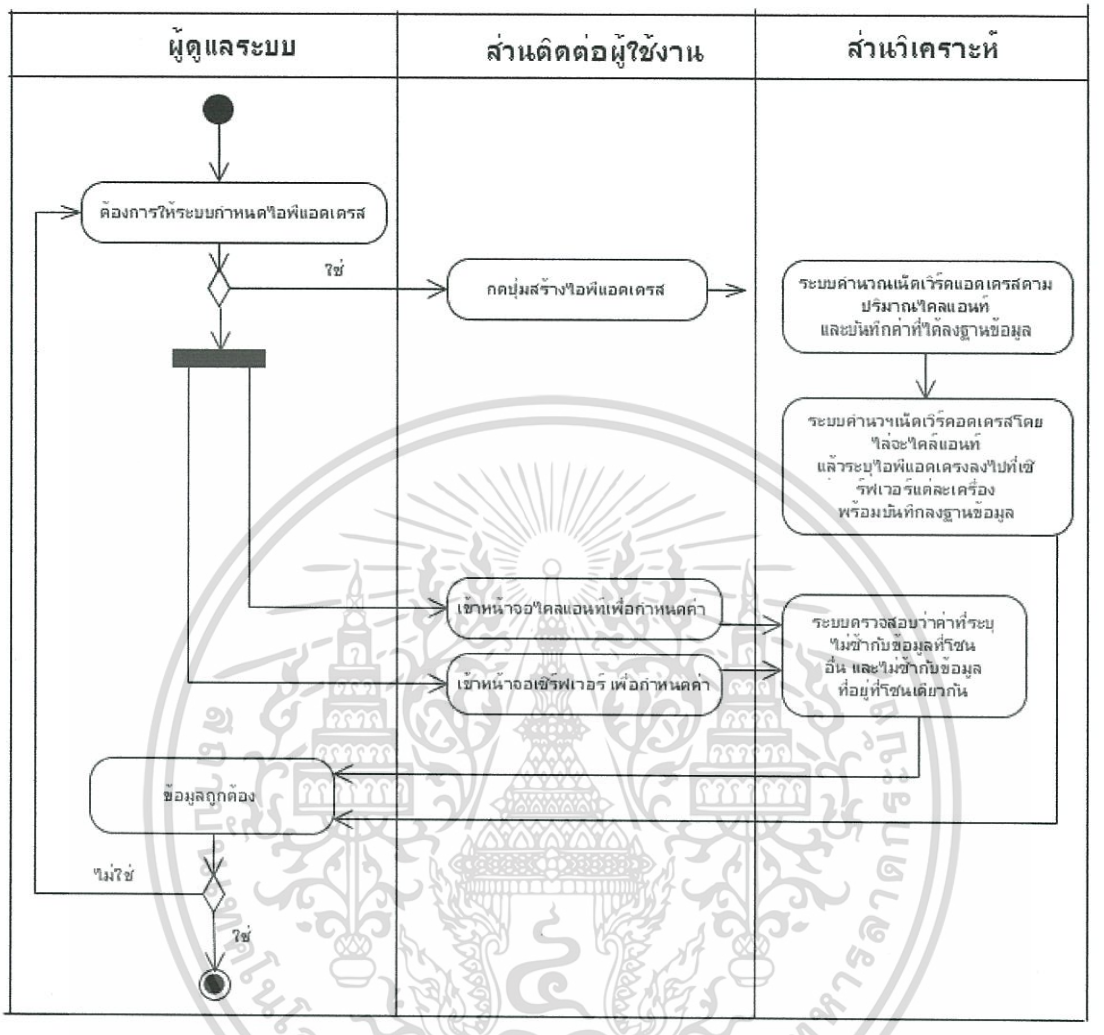
ตารางที่ 3.3 คำอธิบายยูสเคสจัดสรรไอพี แอดเดรส (IP Address)

รหัสยูสเคส	UC03	
ยูสเคส	จัดสรรไอพี แอดเดรส (IP Address)	
วัตถุประสงค์	เพื่อจัดวางไอพีแอดเดรสให้กับอุปกรณ์ทั้งหมดภายในระบบเครือข่าย	
เงื่อนไขเมื่อเริ่มต้น	เมื่อมีข้อมูลเซิร์ฟเวอร์และไคลแอนท์ที่ถูกจัดวางตามโซนทางด้านความปลอดภัย	
เมื่อทำงานเสร็จ	อุปกรณ์ที่อยู่ในระบบทุกเครื่องจะมีไอพีแอดเดรสถูกต้องตามโซนทางด้านความปลอดภัยที่ถูกจัดแบ่งไว้ในตอนแรก	
เมื่อทำงานไม่เสร็จ	ไม่สามารถวางนโยบาย (Rule) ได้	
แอกเตอร์ที่เกี่ยวข้อง	ผู้ดูแลระบบและผู้ดูแลความปลอดภัยของระบบ	
สิ่งกระตุ้นการทำงาน	การกดปุ่มสร้างไอพีแอดเดรส	
อินพุต	1. โซนทางด้านความปลอดภัยที่มีทั้งหมด 2. ปริมาณเครื่องไคลแอนท์ 3. ปริมาณเครื่องเซิร์ฟเวอร์ในแต่ละโซน	
เอาต์พุต	ไอพีแอดเดรสสำหรับอุปกรณ์ในระบบเครือข่ายทั้งหมด	
สถานการณ์	ต้องการให้ระบบสร้างให้เองแบบอัตโนมัติทั้งหมด	
รายละเอียด	**แอกเตอร์**	**ระบบ**
	1. ผู้ดูแลระบบกดปุ่มสร้างไอพีแอดเดรส	1.1 ระบบนำโซนของไคลแอนท์ทั้งหมดมาตรวจสอบโดยการดูปริมาณเครื่องที่มีมาจัดสรรเน็ตเวิร์คแอดเดรสให้สอดคล้องกัน 1.2 ระบบนำโซนของเซิร์ฟเวอร์ที่มีมาแจกจ่ายเน็ตเวิร์คแอดเดรส โดยให้ตัวเลขเรียงต่อจากโซนที่ไคล์แอนท์มี - เริ่มจากไอพีแอดเดรสแรก (หากถูกใช้ในอุปกรณ์อื่นจสามารถแก้ไขได้ในภายหลัง) - ไอพีแอดเดรสสุดท้ายเป็น บรอดแคสแอดเดรส จะไม่ถูกแจกจ่ายให้กับเครื่องใดๆ 1.3 ระบบแจ้งว่าไอพีแอดเดรสถูกกำหนดเรียบร้อย

ตารางที่ 3.3 (ต่อ)

รายละเอียด	แอกเตอร์	ระบบ
	2. ผู้ดูแลระบบตรวจสอบข้อมูลที่ได้ 2a. ผู้ดูแลระบบต้องการแก้ไขข้อมูลด้วยตนเอง	2a.1 ระบบจะทำการตรวจสอบเน็ตเวิร์คแอดเดรสไอพีที่ถูกแก้ไข 2a.2 หากข้อมูลที่ถูกแก้ไขถูกต้อง ระบบจะทำการบันทึกลงฐานข้อมูล
สถานการณ์	ต้องการให้ใส่ข้อมูลไอพีแอดเดรสด้วยตนเองทั้งหมดหรือบางส่วน	
รายละเอียด	**แอกเตอร์**	**ระบบ**
	1. ผู้ดูแลระบบทำการข้อมูล 1a. เพิ่มเน็ตเวิร์คแอดเดรสลงไปที่ไคล์แอนท์โซน 1b. เพิ่มไอพีแอดเดรสลงไปในเซิร์ฟเวอร์แต่ละโซน 2. ผู้ดูแลระบบกดปุ่มเพื่อสร้าง access control rule	 1a.1 ระบบตรวจสอบค่าต้องไม่ซ้ำกับเน็ตเวิร์คแอดเดรสที่มีอยู่เดิม 1a.2 ระบบตรวจสอบค่าต้องไม่ซ้ำกับค่าเน็ตเวิร์คแอดเดรสในโซนอื่นๆ 1a.3 ระบบบันทึกค่าเน็ตเวิร์คแอดเดรสลงฐานข้อมูล 1b.1 ระบบตรวจสอบค่าต้องไม่ซ้ำกับไอพีแอดเดรสที่มีอยู่เดิม 1b.2 ระบบตรวจสอบค่าต้องไม่ซ้ำกับค่าเน็ตเวิร์คแอดเดรสในโซนอื่นๆ 1b.3 ระบบบันทึกค่าไอพีแอดเดรสลงฐานข้อมูล 2.1 หากข้อมูลเน็ตเวิร์คแอดเดรสหรือไอพีแอดเดรสไม่ครบ ระบบจะแจ้งเตือน 2.2 หากข้อมูลเน็ตเวิร์คแอดเดรสหรือไอพีแอดเดรสครบถ้วน ระบบจะแสเง access control rule ออกมา

แอกทิวิตีไดอะแกรมการทำงานสำหรับยูสเคสจัดสรรไอพี แอดเดรส (IP Address) สามารถแสดงได้ดังรูปที่ 3.10



รูปที่ 3.10 แอกทิวิตีไดอะแกรมการทำงานสำหรับการจัดสรรไอพี แอดเดรส (IP Address)

ตารางที่ 3.4 คำอธิบายยูสเคสสร้างกฎและนโยบายเพื่อความปลอดภัย

รหัสยูสเคส	UC04
ยูสเคส	สร้างกฎและนโยบายเพื่อความปลอดภัย
วัตถุประสงค์	เพื่อจัดสรรกฎและนโยบายด้านความปลอดภัยให้เหมาะสมตามแต่ละสภาพแวดล้อมของแต่ละองค์กร
เงื่อนไขเมื่อเริ่มต้น	ข้อมูลทางด้านโซนด้านความแลอดภัยและข้อมูลทางด้านไอพีแอดเดรสทั้งหมด
เมื่อทำงานเสร็จ	ได้กฎและนโยบายด้านความปลอดภัยที่มีความเหมาะสมตามแต่ละสภาพแวดล้อมของแต่ละองค์กร
เมื่อทำงานไม่เสร็จ	ไม่สามารถแปลงกฎให้เป็นไปตามอุปกรณ์ไฟร์วอลล์แล่ละชนิดได้

ตารางที่ 3.4 (ต่อ)

แอกเตอร์ที่เกี่ยวข้อง	ผู้ดูแลระบบและผู้ดูแลความปลอดภัยของระบบ	
สิ่งกระตุ้นการทำงาน	ผู้ดูแลระบบกฎปุ่มสร้างกฎควบคุมการผ่านเข้าออกของข้อมูล (Generate Rule)	
อินพุต	1. โซนทางด้านความปลอดภัย 2. ไอพีแอดเดรสของเซิร์ฟเวอร์ 3. พอร์ตและเซอร์วิสของเซิร์ฟเวอร์แต่ละตัว 4. เน็ตเวริ์กแอดเดรสของเครื่องไคลแอนท์	
เอาต์พุต	กฎและนโยบายด้านความปลอดภัยให้เหมาะสมตามแต่ละสภาพแวดล้อมของแต่ละองค์กร	
สถานการณ์	-	
รายละเอียด	**แอกเตอร์**	**ระบบ**
	1. ผู้ดูแลระบบกฎปุ่มสร้างกฎควบคุมการผ่านเข้าออกของข้อมูล (Generate Rule)	1.1 ระบบสร้างกฎที่อนุญาตการเข้าและออกของแต่ละเครื่องเซิร์ฟเวอร์ตามเซอร์วิสที่ให้บริการ 1.2 ระบบสร้างกฎที่อนุญาตการเข้าและออกของแต่ละเครื่องเซิร์ฟเวอร์พฤติกรรมการทำงาน (ต้องการออกอินเตอร์เน็ต, ไม่ต้องการออกอินเตอร์เน็ต) 1.3 ระบบสร้างกฎสำหรับกลุ่มของไคลแอนท์ โดยอ้างอิงตามพฤติกรรมการทำงาน (ต้องการออกอินเตอร์เน็ต, ไม่ต้องการออกอินเตอร์เน็ต) 1.4 ระบบสร้างกฎสำหรับกลุ่มของไคลแอนท์ โดยอ้างอิงตามเซิร์ฟเวอร์และเซอร์วิสที่ให้บริการ 1.5 ระบบสร้างนโยบายที่บล็อกทุกส่วนจัดเก็บข้อมูลที่ได้เป็นบรรทัด

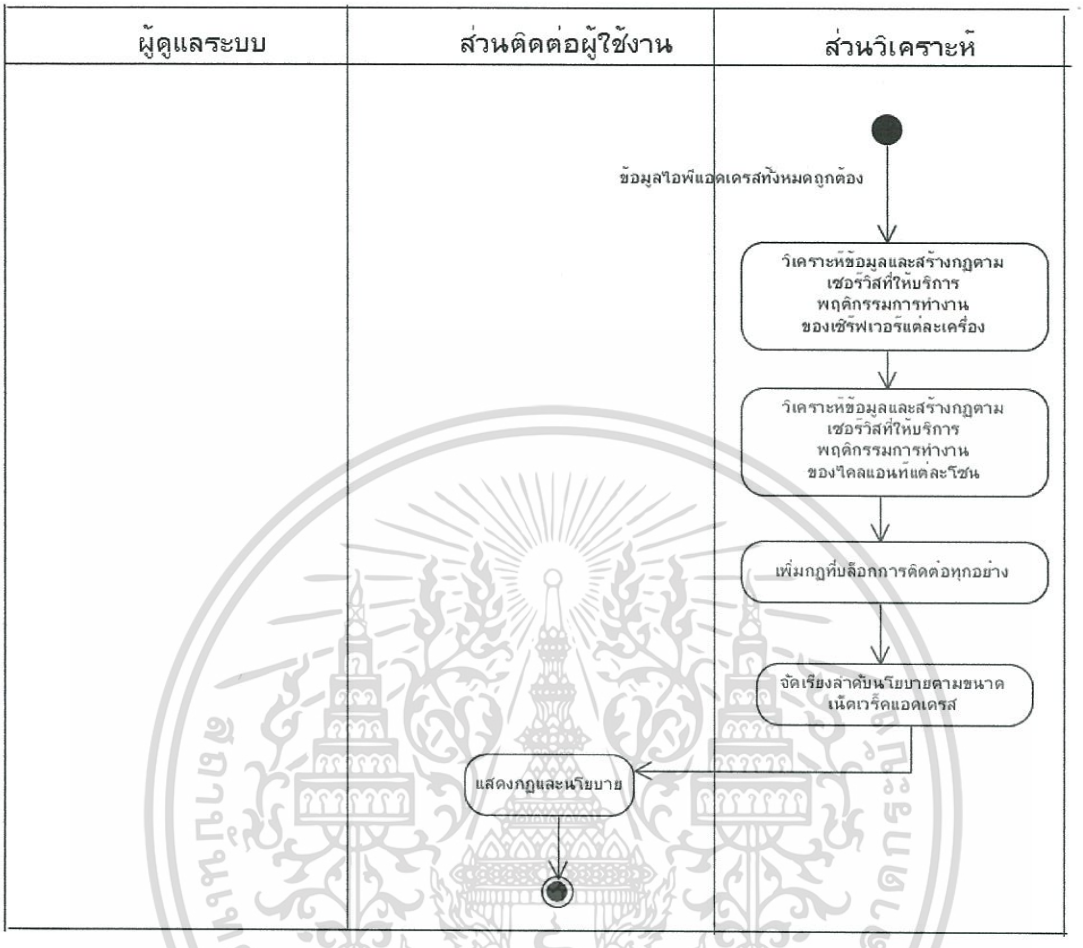
ตารางที่ 3.5 คำอธิบายยูสเคสเรียงลำดับกฎและนโยบายด้านความปลอดภัย

รหัสยูสเคส	UC05
ยูสเคส	เรียงลำดับกฎและนโยบายด้านความปลอดภัย
วัตถุประสงค์	เพื่อให้กฎและนโยบายด้านความปลอดภัยเรียงถูกต้องและสามารถทำงานได้อย่างถูกต้องตามหลักการทำงานของอุปกรณ์ไฟร์วอลล์
เงื่อนไขเมื่อเริ่มต้น	มีกฎและนโยบายด้านความปลอดภัยที่ถูกสร้างออกมา
เมื่อทำงานเสร็จ	ได้กฎและนโยบายด้านความปลอดภัยที่เรียงลำดับได้ถูกต้อง

ตารางที่ 3.5 (ต่อ)

เมื่อทำงานไม่เสร็จ	ไม่สามารถสร้างกฎสำหรับไฟร์วอลล์แต่ละชนิดได้	
แอกเตอร์ที่เกี่ยวข้อง	-	
สิ่งกระตุ้นการทำงาน	เมื่อระบบสร้างกฎและนโยบายด้านความปลอดภัย	
อินพุต	กฎและนโยบายด้านความปลอดภัยที่ยังไม่ถูกจัดเรียง	
เอาต์พุต	กฎและนโยบายด้านความปลอดภัยที่ถูกจัดเรียงเรียบร้อย	
สถานการณ์	ผู้ดูแลระบบและผู้ดูแลความปลอดภัยของระบบ	
รายละเอียด	**แอกเตอร์**	**ระบบ**
	6. ผู้ดูแลระบบตรวจสอบผลที่ได้	1. ระบบเปิดไฟล์ที่มีกฎและนโยบายเขียนอยู่ 2. ระบบตรวจสอบไอพีแอดเดรสและกลุ่มของไอพีแอดเดส 3. เรียงนโยบายจากข้อที่มีกลุ่มของไอพีแอดเดรสน้อยที่สุดไว้ด้านบน และกลุ่มที่ใหญ่ไว้ในอันดับถัดมา 4. นำกฎและนโยบายที่บล็อกทุกอย่างไว้ด้านล่างสุด 5. แสดงผลที่ได้ออกทางหน้าจอ

แอกทิวิตีไดอะแกรมการทำงานสำหรับยูสเคสเรียงลำดับกฎและนโยบายด้านความปลอดภัยและการจัดเรียงนโยบาย สามารถแสดงได้ดังรูปที่ 3.11



รูปที่ 3.11 แอกทิวิตีไดอะแกรมการทำงานสำหรับการสร้างกฎและนโยบายและการจัดเรียงนโยบายเพื่อความปลอดภัย

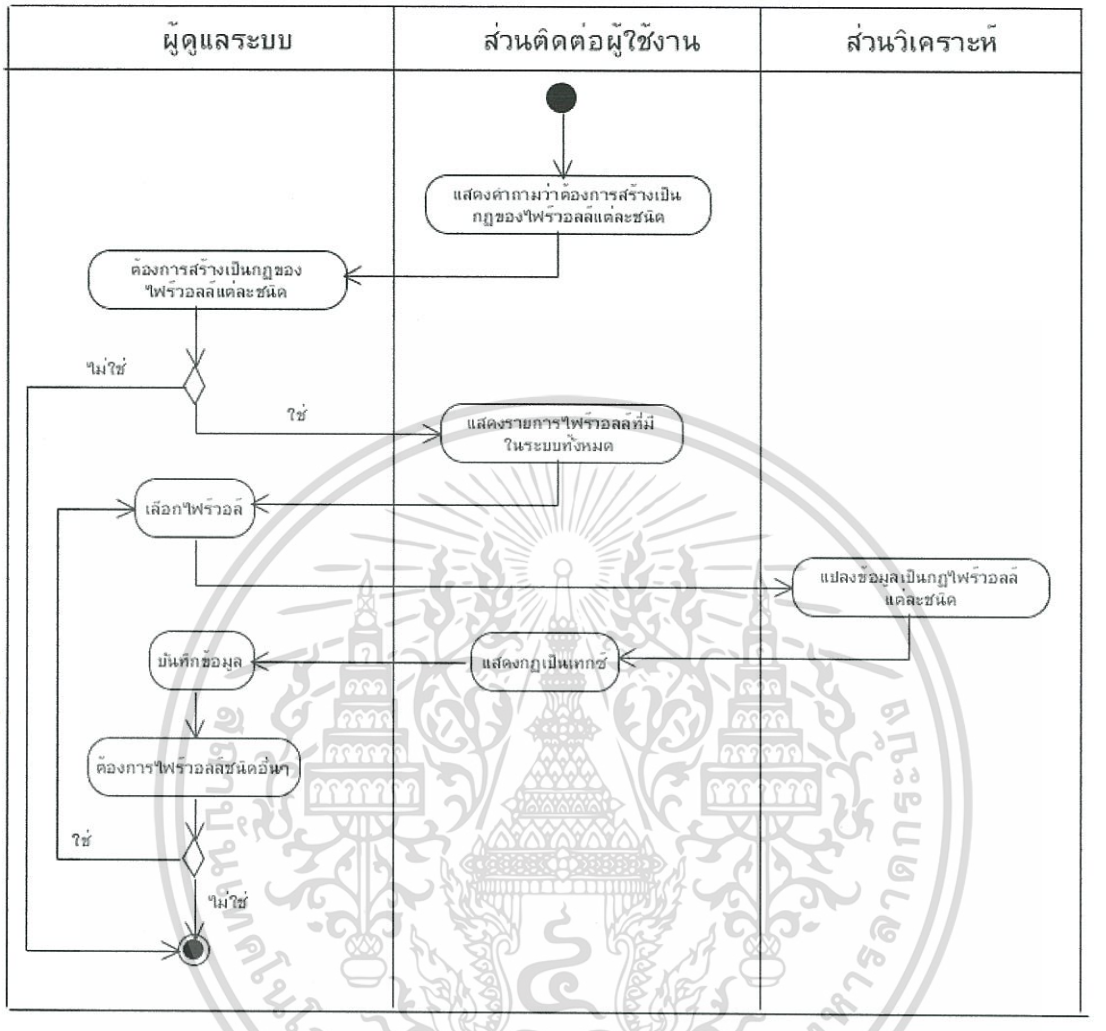
ตารางที่ 3.6 คำอธิบายยูสเคสสร้างกฎและนโยบายด้านความปลอดภัยสำหรับอุปกรณ์ไฟร์วอลล์แบบระบุชื่อผลิตภัณฑ์

รหัสยูสเคส	UC06
ยูสเคส	สร้างกฎและนโยบายด้านความปลอดภัยสำหรับอุปกรณ์ไฟร์วอลล์แบบระบุชื่อผลิตภัณฑ์
วัตถุประสงค์	เพื่อนำกฎที่ได้ไปปรับใช้กับอุปกรณ์ไฟร์วอลล์ที่มีอยู่ในองค์กร
เงื่อนไขเมื่อเริ่มต้น	มีกฎและนโยบายด้านความปลอดภัยของสภาพแวดล้อมของแต่ละองค์กร
เมื่อทำงานเสร็จ	ได้กฎที่ตรงตามชนิดของอุปกรณ์ไฟร์วอลล์ที่มีแบบเทกซ์ไฟล์

ตารางที่ 3.6 (ต่อ)

เมื่อทำงานไม่เสร็จ	-	
แอกเตอร์ที่เกี่ยวข้อง	ผู้ดูแลความปลอดภัยของระบบ	
สิ่งกระตุ้นการทำงาน	ผู้ดูแลระบบเลือกชนิดของอุปกรณ์ไฟร์วอลล์และสั่งให้ระบบสร้าง	
อินพุต	นโยบายด้านความปลอดภัยที่ถูกเรียงลำดับไว้เรียบร้อยแล้ว	
เอาต์พุต	เอกสารเทกซ์ที่เป็นค่าติดตั้งผ่านคำสั่งแบบเทกซ์ (Command Line)	
สถานการณ์	สร้างกฎและนโยบายตามความต้องการของผู้ดูแลความปลอดภัยของระบบ	
รายละเอียด	**แอกเตอร์**	**ระบบ**
	1. เลือกชนิดของอุปกรณ์ไฟร์วอลลที่มีอยู่ 2. กดปุ่มสร้างกฎ 3. กดปุ่มบันทึก	 2.1 ระบบค้นหารูปแบบการวางกฎและนโยบายของอุปกรณ์ไฟร์วอลล์ตามชนิดที่เลือก 2.2 ระบบจัดการจับคู่กฎที่มีตามรูปแบบของไฟร์วอลล์ชนิดนั้นๆ 2.3 ระบบแสดงผลเป็นข้อมูลเทกซ์ 3.1 ระบบป๊อบอัพเป็นหน้าต่างให้บันทึก
สถานการณ์	เลือกอุปกรณ์ไฟร์วอลล์ชนิดอื่นเพิ่มเติม	
รายละเอียด	**แอกเตอร์**	**ระบบ**
	1. กดปุ่มต้องการสร้างกฎสำหรับไฟร์วอลชนิดอื่นๆ 2. เลือกชนิดของอุปกรณ์ไฟร์วอลลชนิดอื่นๆ 3. กดปุ่มสร้างกฎ 4. กดปุ่มบันทึก	1.1 แสดงหน้าจอให้เลือกไฟร์วลล์ชนิดอื่นๆ 2.1 ระบบค้นหารูปแบบการวางกฎและนโยบายของอุปกรณ์ไฟร์วอลล์ตามชนิดที่เลือก 3.1 ระบบจัดการจับคู่กฎที่มีตามรูปแบบของไฟร์วอลล์ชนิดนั้นๆ 3.2 ระบบแสดงผลเป็นข้อมูลเทกซ์ 3.3 ระบบป๊อบอัพเป็นหน้าต่างให้บันทึก

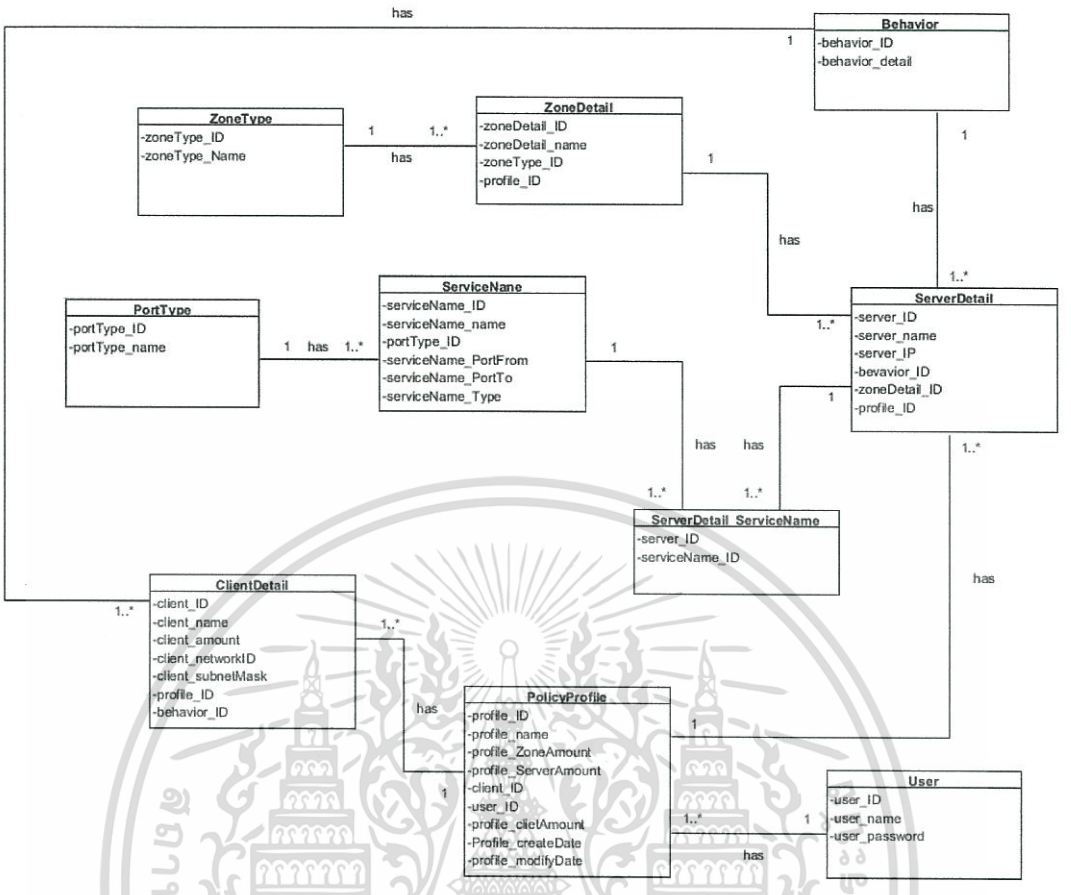
แอกทิวิตีไดอะแกรมการทำงานสำหรับยูสเคสสร้างกฎและนโยบายด้านความปลอดภัยสำหรับอุปกรณ์ไฟร์วอลล์แบบระบุชื่อผลิตภัณฑ์สามารถแสดงได้ดังรูปที่ 3.12



รูปที่ 3.12 แอกทิวิตีไดอะแกรมการทำงานสำหรับการสร้างกฎและนโยบายด้านความปลอดภัยสำหรับอุปกรณ์ไฟร์วอลล์แบบระบุชื่อผลิตภัณฑ์

3.4 คลาสไดอะแกรม

คลาสไดอะแกรมเป็นแผนภาพที่ใช้แสดงความสัมพันธ์ระหว่างคลาสของวัตถุต่างๆที่มีในระบบ รวมถึงคุณสมบัติ และการกระทำที่วัตถุในคลาสต่างๆสามารถกระทำได้ โดยระบบที่ได้ออกแบบประกอบด้วยคลาสต่างๆดังรูปที่ 3.13



รูปที่ 3.13 คลาสไดอะแกรม

3.4.1 ความหมายของคลาส

คลาสแต่ละตัวมีหน้าที่ในการจัดเก็บข้อมูลเพื่อให้ในการทำงานที่แตกต่างกันออกไป ดังนี้

Server Detail คือคลาสหลักที่ทำหน้าที่จัดเก็บข้อมูลการทำงานของเซิร์ฟเวอร์ที่มีความแตกต่างกันไปในแต่ละองค์กร เพื่อที่จะนำข้อมูลดังกล่าวมาแปลงเป็นกฎและนโยบาย ดังนั้นข้อมูลภายในจึงประกอบด้วยชื่อ, ข้อมูล IP Address, โซนที่อยู่ พฤติกรรมการทำงานและพอร์ทที่ให้บริการทั้งหมด

Behavior คือคลาสที่จัดเก็บพฤติกรรมการเชื่อมต่อของฟิลิคัลเซิร์ฟเวอร์และไคลแอนท์ว่ามีความจำเป็นต้องออกอินเตอร์เน็ตหรือไม่ สำหรับนำมาวิเคราะห์เพื่อจัดสรรกฎการควบคุมการผ่านเข้าออก

User คือคลาสที่จัดเก็บข้อมูลยูสเซอร์ที่เข้ามาใช้งานระบบเพื่อยันยันข้อมูล

PolicyProfile คือคลาสที่จัดเก็บข้อมูลของโปรไฟล์นั้นๆ ซึ่งได้แก่ ชื่อ, ข้อมูลโซนทั้งหมดที่มี, ข้อมูลปริมาณเซิร์ฟเวอร์ ข้อมูลปริมาณไคลแอนท์ที่มีอยู่ทั้งหมด วันที่สร้างและวันที่แก้ไข

ServiceName คือคลาสที่จัดเก็บข้อมูลการให้บริการต่างๆ เช่น ให้บริการ DNS, ให้บริการอีเมล์ของ Microsoft Exchange และบ่งบอกเลขพอร์ตของการให้บริการของแต่ละเซอร์วิส โดยจะมีข้อมูลพอร์ตต้นทางและปลายทางจัดเก็บอยู่

ServerDetail_ServiceName คือคลาสที่ทำหน้าที่เชื่อมต่อข้อมูลระหว่าง ServiceName และ Server Detail เพื่อจะได้ทราบว่าเครื่องเซิร์ฟเวอร์แต่ละเครื่องนั้นให้บริการอะไร

ClientDetail คือคลาสที่จัดเก็บข้อมูลไคลแอนท์ ซึ่งได้แก่ ชื่อ, ปริมาณ, เน็ตเวิร์คแอดเดรส และพฤติกรรมการเชื่อมต่อว่าไคลแอนท์ในกลุ่มนั้นมีความจำเป็นต้องออกอินเตอร์เน็ตหรือไม่

ZoneDetail คือคลาสที่จัดเก็บข้อมูลโซนต่างๆที่ได้จากการที่ผู้ใช้งานระบบใส่เพิ่มเข้ามาตามขนาดของโซนที่มีอยู่ในปัจจุบัน

ZoneType คือคลาสที่จัดเก็บข้อมูลโซนพื้นฐานทางระบบเครือข่าย ซึ่งแบ่งออกเป็น 3 โซนหลักๆคือ โซนภายนอก (External), โซนภายใน (Internal) และโซนปลอดทหาร (DMZ) ซึ่งจะถูกเรียกใช้ตอนใส่ข้อมูล ZoneDetail

PortType คือคลาสที่จัดเก็บข้อมูลชนิดของพอร์ตที่ใช้ในการให้บริการแต่ละประเภท โดยจะเก็บเป็นข้อมูล ดังนี้ TCP, UDP, ICMP เป็นต้น

3.4.2 ความสัมพันธ์ระหว่างคลาส

คลาส PolicyProfile

- มีความสัมพันธ์กับคลาส User โดยคลาส User มีหน้าที่เก็บข้อมูลของผู้ล็อกอินเข้าระบบ และคลาส PolicyProfile จะช่วยบ่งบอกว่าโปรไฟล์ที่ถูกสร้างขึ้นมาเป็นของยูสเซอร์ใด โดยยูสเซอร์หนึ่งคนสามารถมีโปรไฟล์ได้มากกว่าหนึ่งโปรไฟล์
- มีความสัมพันธ์กับ ClientDetail โดยคลาส ClientDetail มีหน้าที่จัดเก็บข้อมูลไคลแอนท์ของข้อมูลโปรไฟล์นั้นๆ โดยโปรไฟล์สามารถมีข้อมูลไคลแอนท์ได้มากกว่าหนึ่งชุด

- มีความสัมพันธ์กับ ServerDetail โดยคลาส ServerDetail มีหน้าที่จัดเก็บข้อมูลรายละเอียดของเซิร์ฟเวอร์แต่ละตัว และจะได้ทราบว่าโปรไฟล์ดังกล่าวมีเซิร์ฟเวอร์อะไรบ้าง และเซิร์ฟเวอร์นั้นๆมีการให้บริการส่วนใด โดยโปรไฟล์ต้องมีข้อมูลเซิร์ฟเวอร์อย่างน้อยหนึ่งตัวหรือมากกว่าและรายละเอียดเซิร์ฟเวอร์นั้นๆจะเป็นของโปรไฟล์เพียงโปรไฟล์เดียว

คลาส ServerDetail

- มีความสัมพันธ์กับคลาส Behavior โดยคลาส Behavior มีหน้าที่จัดเก็บข้อมูลพฤติกรรมการส่งรับส่งข้อมูลของการให้บริการภายในเซิร์ฟเวอร์นั้นๆ ว่าจำเป็นต้องติดต่อกับเครือข่ายภายนอกหรือไม่ โดยข้อมูลคลาส ServerDetail หนึ่งตัวจะมีพฤติกรรมการรับส่งข้อมูลได้เพียงหนึ่งพฤติกรรมเท่านั้น
- มีความสัมพันธ์กับคลาส ServerDetail_ServiceName และ ServiceName โดยคลาส ServiceName มีหน้าที่จัดเก็บประเภทของการให้บริการต่างๆไว้ โดยเซิร์ฟเวอร์หนึ่งตัวสามารถให้บริการได้หลากหลายและบริการแต่ละบริการก็ถูกให้โดยเซิร์ฟเวอร์หลายๆตัวได้ด้วยเช่นกัน
- มีความสัมพันธ์กับคลาส ZoneDetail โดยคลาส ZoneDetail มีหน้าที่จัดเก็บค่าโซนความปลอดภัยทั้งหมด ดังนั้นความสัมพันธ์นี้จะบอกได้ว่าเครื่องเซิร์ฟเวอร์ดังกล่าววางอยู่ที่โซนเน็ตเวิร์คโซนใด โดยข้อมูลคลาส ServerDetail หนึ่งตัวจะอยู่ในโซนได้เพียงแค่โซนเดียว
- มีความสัมพันธ์กับคลาส PolicyProfile โดยรายละเอียดระบุไว้ในส่วนของรายละเอียด PolicyProfile ด้านบน

คลาส ZoneDetail

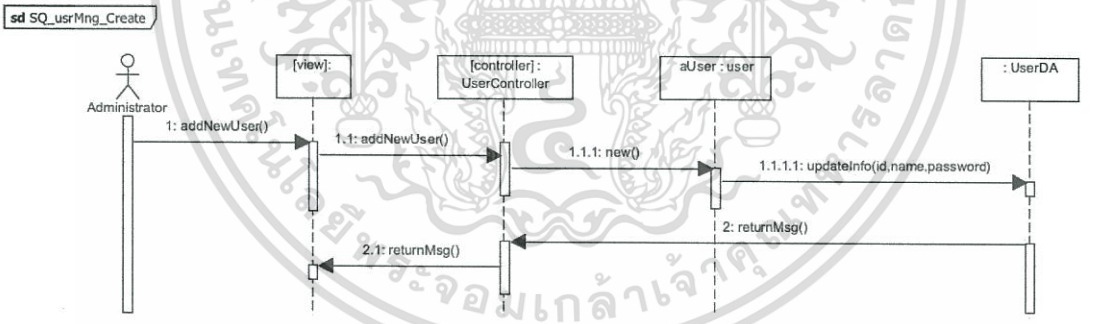
- มีความสัมพันธ์กับคลาส ZoneType โดยคลาส ZoneType มีหน้าที่จัดเก็บประเภทของโซนที่มีอยู่ทั่วไปภายในระบบเครือข่าย โดย ZoneDetailหนึ่งโซนที่ถูกสร้างขึ้นจะมีเป็นเป็นของโซนได้เพียงแค่หนึ่ง แต่ประเภทของโซนแต่ละตัวสามารถอยู่บน ZoneDetail ได้มากกว่าหนึ่ง
- มีความสัมพันธ์กับคลาส ServerDetail โดยรายละเอียดระบุไว้ในส่วนของรายละเอียด ServerDetail ด้านบน

คลาส ServiceName

- มีความสัมพันธ์กับคลาส PortType โดยคลาส PortType มีหน้าที่จัดเก็บชนิดของพอร์ตหลักๆเพื่อให้คลาส ServiceName เรียกใช้ โดยชนิดของการให้บริการ (ภายในคลาส ServiceName) มีพอร์ตที่เปิดให้บริการได้หนึ่งชนิดของพอร์ต และพอร์ตชนิดหนึ่งๆสามารถถูกเรียกใช้ได้มากกว่าหนึ่งการให้บริการ
- มีความสัมพันธ์กับคลาส ServerDetail_ServiceName และ ServerDetail โดยรายละเอียดระบุไว้ในส่วนของ รายละเอียด PolicyProfile ด้านบน

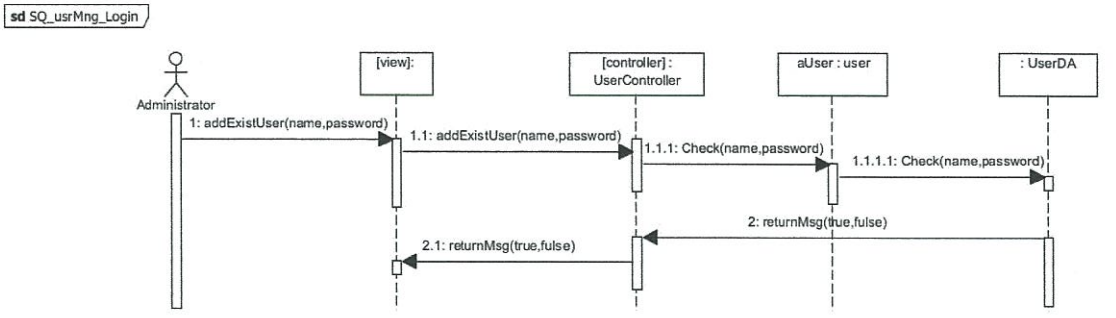
3.5 ซีเควนซ์ไดอะแกรม

ซีเควนซ์ไดอะแกรมหรือแผนภาพลำดับเหตุการณ์ เป็นแผนภาพแสดงลำดับเวลาของการทำงานที่เกิดขึ้นระหว่างวัตถุหนึ่งกับอีกวัตถุหนึ่ง โดยลำดับเหตุการณ์การทำงานที่สำคัญของระบบออกแบบและอิมพลีเมนท์นโยบายรักษาความปลอดภัยสำหรับอุปกรณ์ไฟร์วอลล์ประกอบด้วย การสร้างยูสเซอร์ผู้ใช้งาน การล็อคอินเข้าระบบ การสร้างโปรไฟล์เพื่อสร้างนโยบายด้านความปลอดภัยสำหรับอุปกรณ์ไฟร์วอลล์ การใส่รายละเอียดข้อมูลไคลแอนท์ การใส่ข้อมูลรายละเอียดของเซิร์ฟเวอร์ การใส่ข้อมูลโซนและลักษณะการเชื่อมต่อของเซิร์ฟเวอร์ของเซิร์ฟเวอร์แต่ละตัว และการเพิ่มเซอร์วิสใหม่ๆ ตามลำดับ



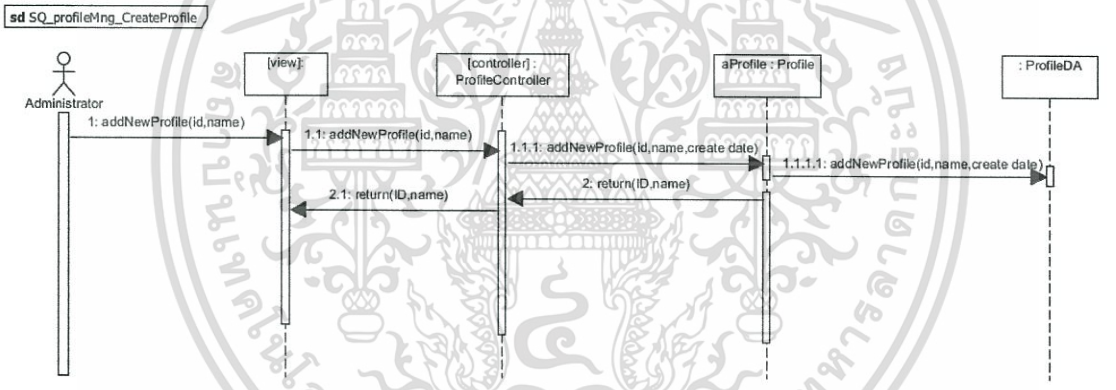
รูปที่ 3.14 ซีเควนซ์ไดอะแกรมแสดงลำดับการทำงานในการสร้างยูสเซอร์ผู้ใช้งาน

จากรูปที่ 3.14 แสดงลำดับการทำงานในการสร้างยูสเซอร์ผู้ใช้งาน โดยเริ่มจากผู้ดูแลระบบต้องการสร้างยูสเซอร์ใหม่โดยติดต่อส่งค่าชื่อ ยูสเซอร์เนมและพาสเวิร์ดไปยังหน้าจออินเตอร์เฟส จากนั้นหน้าจออินเตอร์เฟสจะส่งค่าต่อไปยังคอนโทรเลอร์เพื่อให้คอนโทรเลอร์อัพเดทข้อมูลดังกล่าวลง Data Access (DA) ในส่วนของข้อมูลยูสเซอร์ใหม่ หลังจากนั้นระบบจะทำการแจ้งเตือนเพื่อบอกผู้ดูแลระบบว่าข้อมูลมีการอัพเดทเรียบร้อย



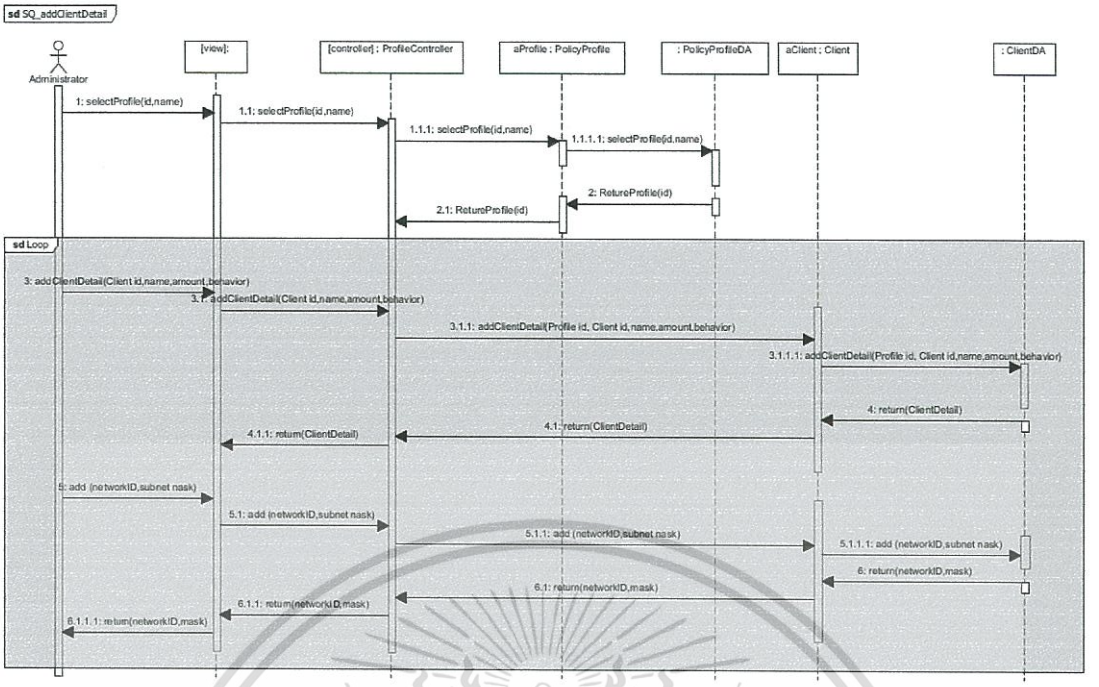
รูปที่ 3.15 ซีเควนซ์ไดอะแกรมแสดงลำดับการทำงานในการล็อคอินเข้าระบบ

จากรูปที่ 3.15 แสดงลำดับการทำงานในการล็อคอินเข้าระบบโดยเริ่มจากผู้ดูแลระบบใส่ข้อมูลยูสเซอร์เนมและพาสเวิร์ดของตนเข้าไปในส่วนติดต่อผู้ใช้งาน จากนั้นข้อมูลจะถูกส่งต่อไปยังคอนโทรเลอร์เพื่อตรวจสอบข้อมูลที่ฐานข้อมูลว่าถูกต้องหรือไม่ เมื่อได้คำตอบจะส่งผลที่ได้ให้ผู้ดูแลระบบทราบ



รูปที่ 3.16 ซีเควนซ์ไดอะแกรมแสดงลำดับการทำงานในการสร้างโปรไฟล์ของระบบเครือข่าย

จากรูปที่ 3.16 แสดงลำดับการทำงานในการสร้างโปรไฟล์ของระบบเครือข่าย โดยเริ่มจากผู้ดูแลระบบส่งคำร้องขอในการสร้างโปรไฟล์ใหม่ไปยังส่วนติดต่อผู้ใช้งานโดยการส่งชื่อโปรไฟล์ไป ส่วนควบคุมจะส่งคำร้องขอต่อไปยังฐานข้อมูลโปรไฟล์เพื่อสร้างไอดีของโปรไฟล์ใหม่และนำชื่อที่ผู้ดูแลระบบให้มาใส่ลงไปพร้อมกับวันที่มีการสร้างขึ้นมาบันทึกลงไปฐานข้อมูล



รูปที่ 3.17 ซีเควนซ์ไดอะแกรมแสดงลำดับการทำงานในการใส่ข้อมูลรายละเอียดของไคลแอนท์

จากรูปที่ 3.17 แสดงลำดับการทำงานในการใส่ข้อมูลรายละเอียดของไคลแอนท์โดยเริ่มจากผู้ดูแลระบบเลือกไปยังโปรไฟล์ที่ต้องการสร้างไคลแอนท์และกดปุ่มสร้างไคลแอนท์ หลังจากนั้นผู้ดูแลระบบกำหนดชื่อ ปริมาณไคลแอนท์และพฤติกรรมของไคลแอนท์ในกลุ่มนั้นๆว่าต้องการออกอินเตอร์เน็ตหรือไม่ หากในโปรไฟล์ดังกล่าวมีไคลแอนท์มากกว่าหนึ่งกลุ่มก็สามารถเพิ่มเข้าไปได้โดยไม่จำเป็นต้องกำหนดเน็ตเวิร์คแอดเดรส

ในกรณีที่ผู้ดูแลระบบต้องการเพิ่มเน็ตเวิร์คแอดเดรสด้วยตนเอง ทุกครั้งที่มีการกำหนดข้อมูลระบบจะทำการตรวจสอบกับปริมาณที่มีอยู่ว่าเหมาะสมหรือไม่ และข้อมูลจะถูกบันทึกลงฐานข้อมูลทันทีที่ข้อมูลถูกต้องเหมาะสม

ในกรณีที่ผู้ดูแลระบบยังไม่ต้องการกำหนดค่าเน็ตเวิร์คแอดเดรส สามารถเว้นว่างข้อมูลในส่วนมูลในส่วนนั้นแล้วมากำหนดในภายหลัง หรือให้ระบบกำหนดให้ก็ได้เช่นกัน

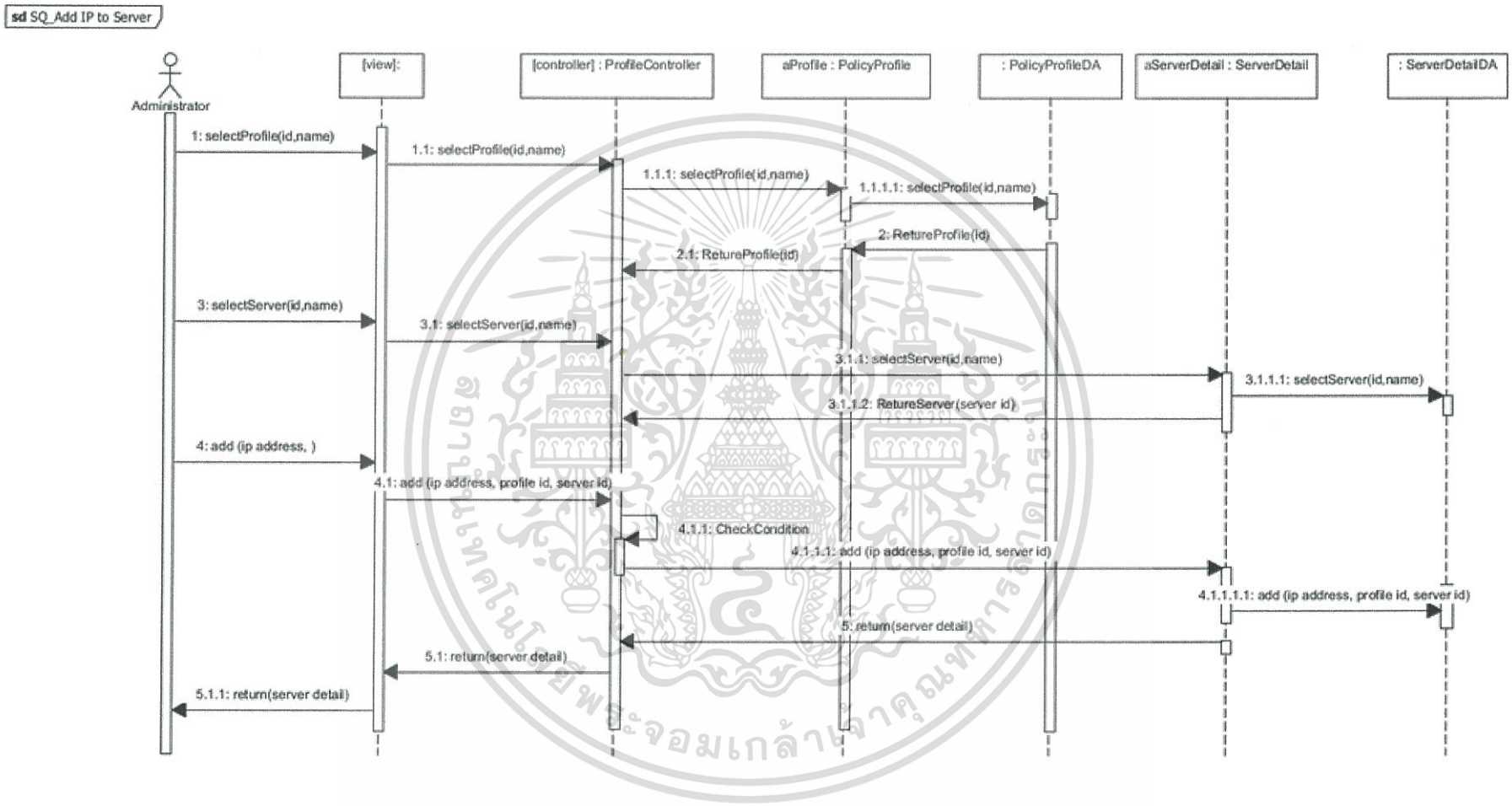
รูปที่ 3.18 ซีเควนซ์ไดอะแกรมแสดงลำดับการทำงานในการใส่ข้อมูลรายละเอียดของเซิร์ฟเวอร์

ภาพที่ 3.18 แสดงลำดับการทำงานในการใส่ข้อมูลรายละเอียดของเซิร์ฟเวอร์

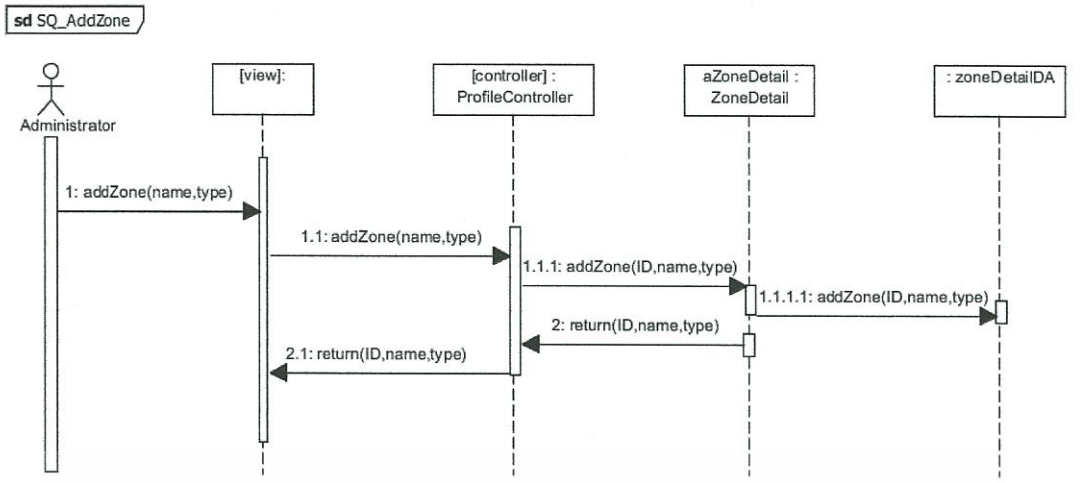
เซิร์ฟเวอร์โดยการกำหนดชื่อและพฤติกรรมลงไป และระบบจะทำการบันทึกข้อมูลไอดีและข้อมูลเพิ่มเข้ามาใหม่ลงฐานข้อมูลรายละเอียดของเซิร์ฟเวอร์ (ServerDetail)

จากนั้นผู้ดูแลระบบจะทำการใส่ข้อมูลเซอร์วิสการให้บริการของเซิร์ฟเวอร์โดยเลือกจากชื่อและคอนโทรเลอร์จะดึงข้อมูลพอร์ตของการให้บริการออกมาแบบอัตโนมัติ หากใสเครื่องเซิร์ฟเวอร์เดียวกันมีการให้บริการมากกว่าหนึ่ง ทางผู้ดูแลระบบจะสามารถใส่ข้อมูลเซอร์วิสเพิ่มเติมลงไปได้ ซึ่งข้อมูลของเซิร์ฟเวอร์และเซอร์วิสจะถูกบันทึกลงในฐานข้อมูลที่ชื่อ ServerDetail_ServiceName

จากรูปที่ 3.19 แสดงลำดับการทำงานในการกำหนดไอพีแอดเดรส โดยแรกเริ่มผู้ดูแลระบบทำการเลือกโปรไฟล์ และเครื่องเซิร์ฟเวอร์ที่ต้องการกำหนดไอพี พอกำหนดไอพีแอดเดรสเรียบร้อยระบบจะทำการตรวจสอบเงื่อนไขดูว่าไอพีแอดเดรสนั้นๆ ไม่ได้อยู่ในวงเน็ตเวิร์คที่ซ้ำกับโซนอื่นๆ หรือมีไอพีแอดเดรสที่ซ้ำกับเครื่องอื่นๆ หากเงื่อนไขที่ถูกตรวจสอบสมบูรณ์ ระบบจะทำการบันทึกค่าลงในฐานข้อมูลรายละเอียดของเซิร์ฟเวอร์ (Server Detail)

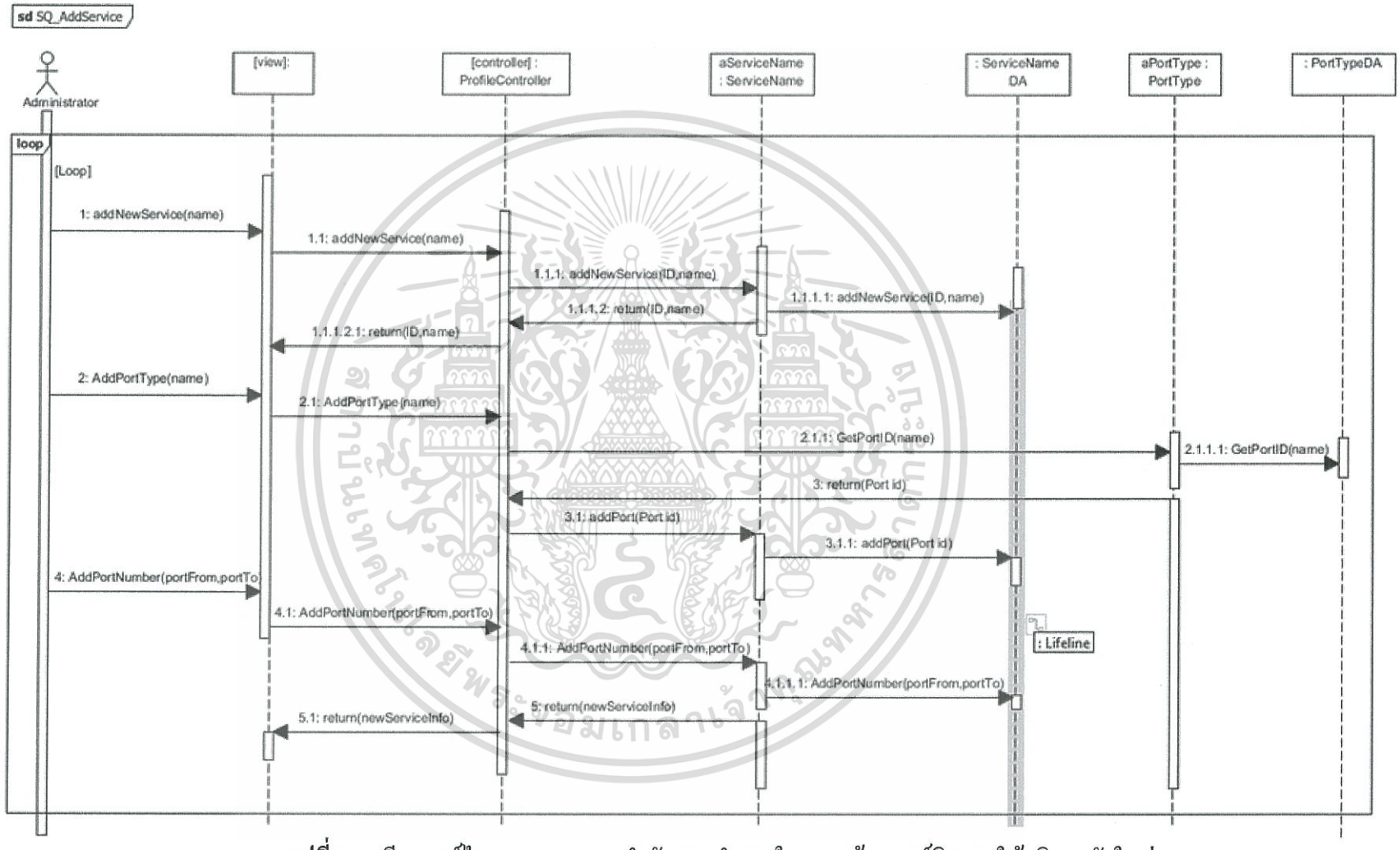


รูปที่ 3.19 ซีเควนซ์ไดอะแกรมแสดงลำดับการทำงานในการใส่ไอพีแอดเดรสให้เซิร์ฟเวอร์



รูปที่ 3.20 ซีเควนซ์ไดอะแกรมแสดงลำดับการทำงานในการใส่ข้อมูลโซนและลักษณะการเชื่อมต่อของเซิร์ฟเวอร์

จากรูปที่ 3.20 แสดงลำดับการทำงานในการใส่ข้อมูลโซน โดยแรกเริ่มระบบจะกำหนดให้มีโซนทั้งหมด 2 โซน คือ โซนภายนอก (External หรือ WAN) และโซนภายใน Internal หรือ Trusted) ที่ไว้สำหรับวางเซิร์ฟเวอร์ ซึ่งผู้ดูแลระบบสามารถเพิ่มโซนความปลอดภัยเข้าไปได้โดยการกำหนดชื่อและชนิดของโซนเพิ่มเข้าไปว่าเป็น โซนภายใน (Internal) หรือโซนปลอดทหาร (DMZ) หรือ โซนภายนอก (External) และระบบจะทำการจะบันทึกข้อมูลโซนที่ได้ลงในฐานข้อมูลรายละเอียดโซน (ZoneDetail)



รูปที่ 3.21 ซีเควนซ์ไดอะแกรมแสดงลำดับการทำงานในการสร้างเซอร์วิสการให้บริการตัวใหม่

จากรูปที่ 3.21 แสดงลำดับการทำงานในการสร้างเซอร์วิสการให้บริการตัวใหม่ โดยเริ่มจากผู้ดูแลระบบเลือกเพิ่มเซอร์วิส ตัวคอนโทรเลอร์จะทำงานในส่วนที่ให้ผู้ดูแลระบบใส่ข้อมูลเซอร์วิสตัวใหม่โดยการให้ผู้ดูแลระบบตั้งชื่อเซอร์วิส ใส่ชนิดของพอร์ตโดยคอนโทรเลอร์จะดึงข้อมูลมาจากฐานข้อมูลที่จัดเก็บชนิดของพอร์ตเอาไว้ (PortType)เพื่อแสดงให้ผู้ดูแลระบบเลือก และใส่ข้อมูลตัวเลขพพอร์ตที่ใช้ลงในส่วนติดต่อผู้ใช้งาน ในลำดับถัดไปคอนโทรเลอร์จะทำการบันทึกค่าทั้งหมดลงในฐานข้อมูลรายละเอียดของเซอร์วิส (ServiceName)

บทที่ 4
การพัฒนาระบบ

4.1 เครื่องมือและภาษาที่ใช้ในการพัฒนาระบบ

การออกแบบและพัฒนาระบบออกแบบและอิมพลีเมนท์นโยบายรักษาความปลอดภัยสำหรับอุปกรณ์ไฟร์วอลล์ในโครงการนี้ใช้เครื่องมือ ภาษา และโปรแกรมในการพัฒนาระบบดังนี้

4.1.1 ฮาร์ดแวร์

เครื่องคอมพิวเตอร์ที่ใช้ในการพัฒนาระบบ จำลองระบบ และทดสอบระบบมีคุณสมบัติดังนี้

- เครื่องคอมพิวเตอร์โน้ตบุ๊ค Dell รุ่น Vostro 5460
- หน่วยประมวลผล Intel Core i5 ความเร็ว 2.60 GHz
- หน่วยความจำขนาด 4 GB
- ฮาร์ดดิสก์ SSD ความจุ 256 GB
- หน่วยแสดงผล NVIDIA GeForce 630M GT ขนาดหน่วยความจำ 2 GB

4.1.2 ซอฟต์แวร์

ซอฟต์แวร์ที่ใช้ในการพัฒนาและทดสอบระบบ ประกอบด้วยซอฟต์แวร์ต่างๆ ดังนี้

- ระบบปฏิบัติการ Window 8.1 Pro 64 bit
- ระบบจัดการฐานข้อมูล MySQL Workbench Version 6.3
- Microsoft Visual Studio 2015

4.1.3 เครื่องมือ

เครื่องมือที่ใช้ในการพัฒนา และออกแบบระบบ มีดังนี้

- Visual Paradigm 13.0 เป็นซอฟต์แวร์ที่ช่วยในการจัดทำแบบจำลองระบบตามมาตรฐาน UML ในโครงนี้ได้นำมาใช้ในการจัดทำแบบจำลองในขั้นตอนการออกแบบระบบ ได้แก่ ยูสเคสไดอะแกรม แอกทิวิตีไดอะแกรม ซีเควนซ์ไดอะแกรม คลาสไดอะแกรมและอีอาร์ไดอะแกรม
- Microsoft Visio 2015 เป็นซอฟต์แวร์ที่ช่วยในการจัดทำแผนผังและไดอะแกรม ในโครงนี้ได้นำมาใช้ในการจัดทำแผนผังการทำงานของระบบ ได้แก่ แผนผังการทำงาน (Flow Chart)

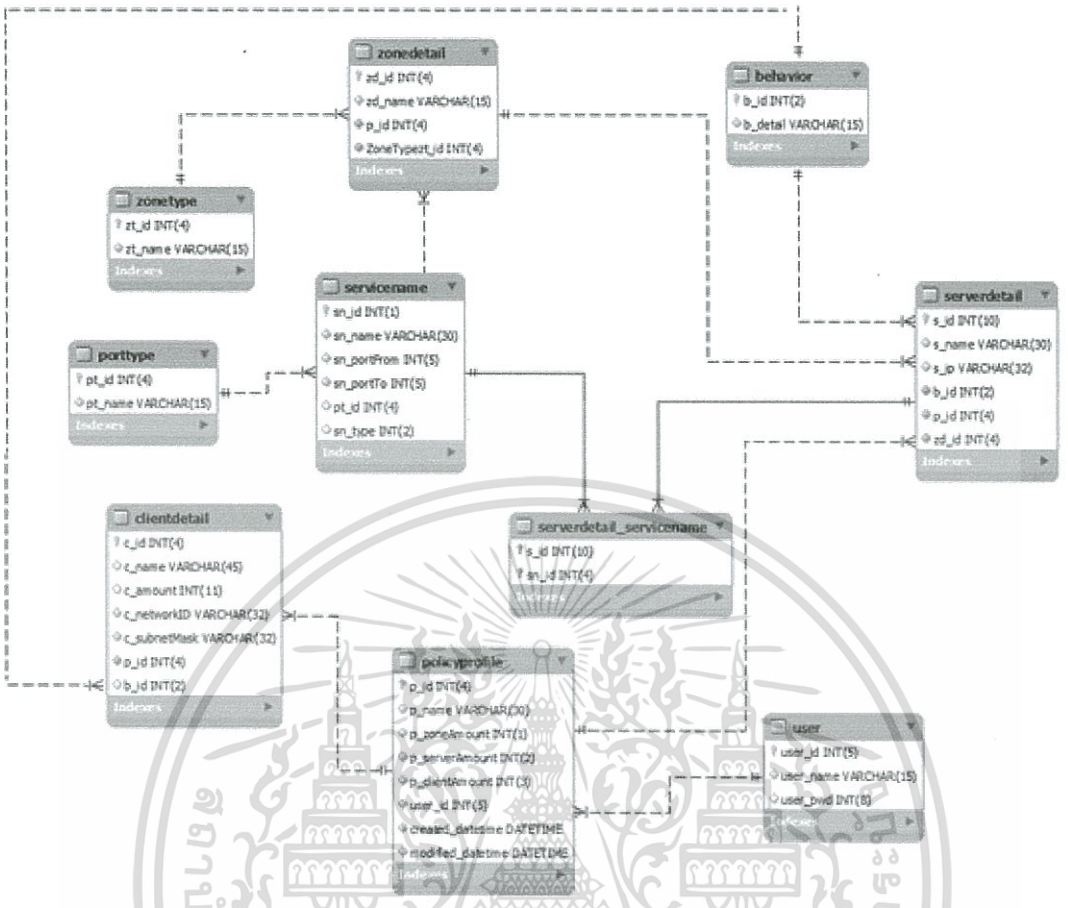
- MySQL Workbench version 6.3 เป็นซอฟต์แวร์ที่ช่วยจัดเก็บข้อมูลในระบบฐานข้อมูล MySQL ได้ง่ายขึ้น ซึ่งนำมาช่วยในขั้นตอนการจำลองฐานข้อมูลรายละเอียดเซิร์ฟเวอร์และไคลแอนท์ต่างๆภายในองค์กร
- Microsoft Visual Studio 2015 เป็นเครื่องมือที่ช่วยในการพัฒนาหน้าจอในส่วนการติดต่อประสานงานกับผู้ใช้งานระบบ (User Interface)

4.2 การพัฒนาการจำลองฐานข้อมูล

การจำลองฐานข้อมูลที่จะนำมาใช้ในระบบออกแบบและอิมพลีเมนท์นโยบายรักษาความปลอดภัยสำหรับอุปกรณ์ไฟร์วอลล์ ประกอบด้วยสองส่วนคือ แผนภาพความสัมพันธ์ระหว่างเอนทิตี้ (E-R Diagram) และพจนานุกรมข้อมูล (Data Dictionary) โดยมีรายละเอียดดังต่อไปนี้

4.2.1 แผนภาพความสัมพันธ์ระหว่างเอนทิตี (E-R Diagram)

อีอาร์ไดอะแกรมเป็นแผนภาพที่ใช้แสดงโครงสร้างและความสัมพันธ์ระหว่างเอนทิตีต่างๆภายในฐานข้อมูล รวมถึงแอตทริบิวทั้งหมดที่มีอยู่ภายในเอนทิตี โดยระบบที่ได้ทำการออกแบบประกิบด้วยเอนทิตีต่างๆดังรูปที่ 4.1



รูปที่ 4.1 แผนผังแสดงความสัมพันธ์ระหว่างเอนทิตีของระบบระบบออกแบบและอิมพลีเมนท์นโยบายรักษาความปลอดภัยสำหรับอุปกรณ์ไฟร์วอลล์

ตารางที่ 4.1 ตารางแสดงหน้าที่การทำงานของแต่ละเอนทิตี้

Name	Detail
User	จัดเก็บข้อมูลผู้ดูแลระบบ
PolicyProfile	จัดเก็บข้อมูลคุณลักษณะของโปรไฟล์
ClientDetail	จัดเก็บข้อมูลและปริมาณของไคลแอนท์
Behavior	จัดเก็บข้อมูลคุณลักษณะการเชื่อมต่อเพื่อเป็นตัวเลือกในการกำหนดคุณลักษณะของเซิร์ฟเวอร์แต่ละตัว
ServerDetail	จัดเก็บคุณลักษณะเซิร์ฟเวอร์แต่ละตัว
ZoneDetail	จัดเก็บข้อมูลโซนทางด้านความปลอดภัยต่างๆ
ServiceName	จัดเก็บข้อมูลการให้บริการแต่ละชนิด

ตารางที่ 4.1 (ต่อ)

Name	Detail
ZoneType	จัดเก็บข้อมูลชนิดของโซน เพื่อเป็นตัวเลือกในการกำหนดรายละเอียดของแต่ละโซน
ServerDetail_ServiceName	เป็นบริดจ์เอนทิตี้ระหว่าง ServerDetail และ ServiceName
PortType	จัดเก็บข้อมูลชนิดของพอร์ต เพื่อเป็นตัวเลือกในการกำหนดคุณลักษณะของพอร์ตของแต่ละเซอร์วิส

4.2.2 พจนานุกรมข้อมูล (Data Dictionary)

พจนานุกรมข้อมูลอธิบายคุณลักษณะของแอททริบิวภายในเอนทิตีต่างๆ ดังนี้

ตารางที่ 4.2 ตาราง User

ชื่อแอททริบิวต์	ชนิดข้อมูล	คีย์	ตารางอ้างอิง
user_id	integer(5)	PK	
user_name	char(15)		
user_pwd	integer(8)		

ตารางที่ 4.3 ตาราง PolicyProfile

ชื่อแอททริบิวต์	ชนิดข้อมูล	คีย์	ตารางอ้างอิง
p_id	integer(4)	PK	
p_name	char(30)		
p_zoneAmount	integer(1)		
p_serverAmount	integer(2)		
p_clientAmount	integer(3)		
user_id	integer(5)	FK	User
created_datetime	datetime		
Modified_datetime	datetime		

ตารางที่ 4.4 ตาราง ClientDetail

ชื่อแอททริบิวต์	ชนิดข้อมูล	คีย์	ตารางอ้างอิง
c_id	integer(4)	PK	
c_name	char(45)		
c_amount	integer(11)		
c_networkID	char(32)		
c_subnetMask	char(32)		
p_id	integer(4)	FK	PolicyProfile
b_id	integer(2)	FK	behavior

ตารางที่ 4.5 ตาราง Behavior

ชื่อแอททริบิวต์	ชนิดข้อมูล	คีย์	ตารางอ้างอิง
b_id	integer(2)	PK	
b_detail	char(15)		

ตารางที่ 4.6 ตาราง ServerDetail

ชื่อแอททริบิวต์	ชนิดข้อมูล	คีย์	ตารางอ้างอิง
s_id	integer(10)	PK	
s_name	char(30)		
s_ip	char(32)		
b_id	integer(2)	FK	Behavior
p_id	integer(4)	FK	PolicyProfile
zd_id	integer(4)	FK	ZoneDetail

ตารางที่ 4.7 ตาราง ZoneDetail

ชื่อแอททริบิวต์	ชนิดข้อมูล	คีย์	ตารางอ้างอิง
zd_id	integer(4)	PK	
zd_name	char(15)		
p_id	integer(4)	FK	PolicyProfile
ZoneTypezt_id	integer(4)	FK	ZoneType

ตารางที่ 4.8 ตาราง ServiceName

ชื่อแอททริบิวต์	ชนิดข้อมูล	คีย์	ตารางอ้างอิง
sn_id	integer(1)	PK	
sn_name	char(30)		
sn_portFrom	integer(5)		
sn_portTo	integer(5)		
sn_type	int(2)		
pt_id	integer(4)	FK	PortType

ตารางที่ 4.9 ตาราง ZoneType

ชื่อแอททริบิวต์	ชนิดข้อมูล	คีย์	ตารางอ้างอิง
zt_id	integer(4)	PK	
zt_name	char(15)		

ตารางที่ 4.10 ตาราง ServerDetail_serviceName

ชื่อแอททริบิวต์	ชนิดข้อมูล	คีย์	ตารางอ้างอิง
s_id	integer(10)	PK/FK	ServerDetail
sn_id	integer(4)	PK/FK	ServiceName

ตารางที่ 4.11 ตาราง PortType

ชื่อแอททริบิวต์	ชนิดข้อมูล	คีย์	ตารางอ้างอิง
pt_id	integer(4)	PK	
pt_name	char(15)		

4.3 การพัฒนาระบบออกแบบและอิมพลีเมนท์นโยบายรักษาความปลอดภัยสำหรับอุปกรณ์ไฟร์วอลล์

ในส่วนการพัฒนาระบบออกแบบและอิมพลีเมนท์นโยบายรักษาความปลอดภัยสำหรับอุปกรณ์ไฟร์วอลล์ จะกล่าวถึงรายละเอียดขั้นตอนการทำงานของเอเจนท์แต่ละตัวที่ทำงานอยู่ภายในระบบ ซึ่งประกอบไปด้วยเอเจนท์ 2 ตัวที่ทำงานร่วมกับบนเซิร์ฟเวอร์ตัวเดียวกัน ได้แก่ เอเจนท์ส่วนติดต่อประสานกับผู้ใช้ และเอเจนท์วิเคราะห์

4.3.1 เอเจนท์ติดต่อประสานกับผู้ใช้

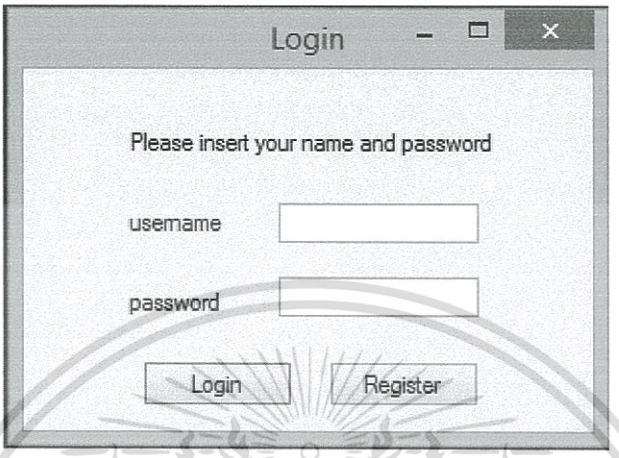
เอเจนท์ส่วนติดต่อประสานงานกับผู้ใช้เป็นส่วนเริ่มต้นการทำงานของระบบเพื่อจัดเก็บข้อมูลต่างๆ ก่อนนำมาวิเคราะห์ ซึ่งมีหน้าที่ติดต่อประสานกับผู้ใช้งานโดยตรง เพื่อรับข้อมูลยูสเซอร์ของผู้ใช้งานระบบ รับรายละเอียดในการจัดแบ่งโซนความปลอดภัย รับข้อมูลการให้บริการของเซิร์ฟเวอร์ รับข้อมูลของไคลแอนท์ รับรายละเอียดในการจัดสรรไอพีแอดเดรส รับรายละเอียดในการเลือกอุปกรณ์ไฟร์วอลล์ และแสดงผลที่ได้จากการการวิเคราะห์นโยบาย ซึ่งประกอบไปด้วย 9 หน้าจอหลักดังต่อไปนี้

1. หน้าการรับข้อมูลยูสเซอร์ของผู้ใช้งานระบบ
2. หน้าจอหลักของระบบ
3. หน้าจอรับรายละเอียดในการสร้างโปรไฟล์
4. หน้าจอรับรายละเอียดโซน
5. หน้าจอการรับรายละเอียดไคลแอนท์
6. หน้าจอรับข้อมูลรายละเอียดของเซิร์ฟเวอร์
7. หน้าจอแสดงวิธีการสร้างเซอร์วิสใหม่
8. หน้าจอการจัดสรรไอพีแอดเดรสและแสดงผล
9. หน้าจอแสดงผลที่ได้จากการการวิเคราะห์นโยบายด้านความปลอดภัย

ซึ่งรายละเอียดสำหรับหน้าจอต่างๆ แสดงได้ดังนี้

1. หน้าการรับข้อมูลยูสเซอร์ของผู้ใช้งานระบบ

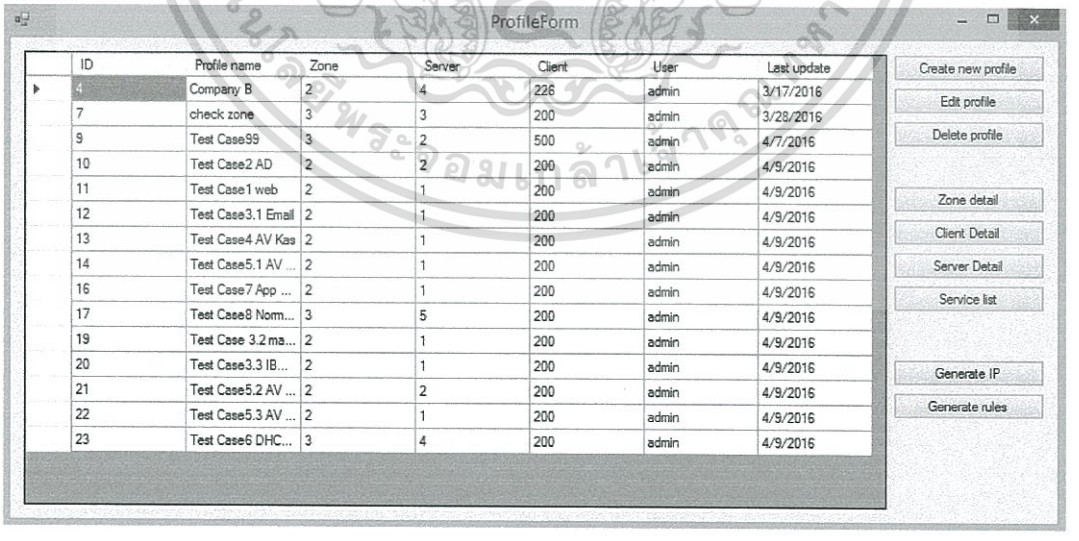
เป็นหน้าจอแรกที่จะพบหลังจากเปิดระบบขึ้นมา โดยรูปที่ 4.2 แสดงหน้าการรับข้อมูลยูสเซอร์ของผู้ใช้งานระบบซึ่งเป็นหน้าจอแรกที่ถูกแสดงขึ้นมา เพื่อให้ผู้ใช้งานระบบยืนยันตัวตนหรือทำการลงทะเบียนก่อนเข้าใช้งานระบบ ซึ่งผู้ใช้งานแต่ละคนสามารถสร้างโปรไฟล์ส่วนตัวได้



รูปที่ 4.2 แสดงหน้าการรับข้อมูลยูสเซอร์ของผู้ใช้งานระบบ

2. หน้าจอหลักของระบบ

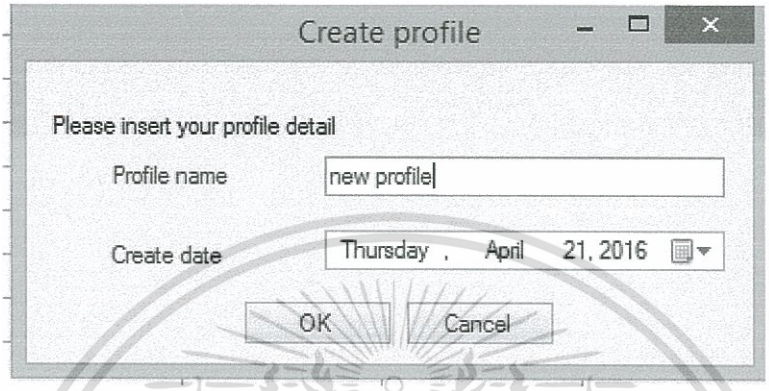
เกิดขึ้นหลังจากมีการล็อคอินเข้าระบบ โดย รูปที่ 4.3 แสดงหน้าจอหลักของระบบ ซึ่งจะประกอบไปด้วยโปรไฟล์ที่มีอยู่ทั้งหมด รวมถึงรายละเอียดวันที่ของแต่ละโปรไฟล์ที่มีการอัพเดตล่าสุด



รูปที่ 4.3 แสดง หน้าจอหลักในการแสดงโปรไฟล์และรับค่าในส่วนต่างๆ

3. หน้าจอรับรายละเอียดในการสร้างโปรไฟล์

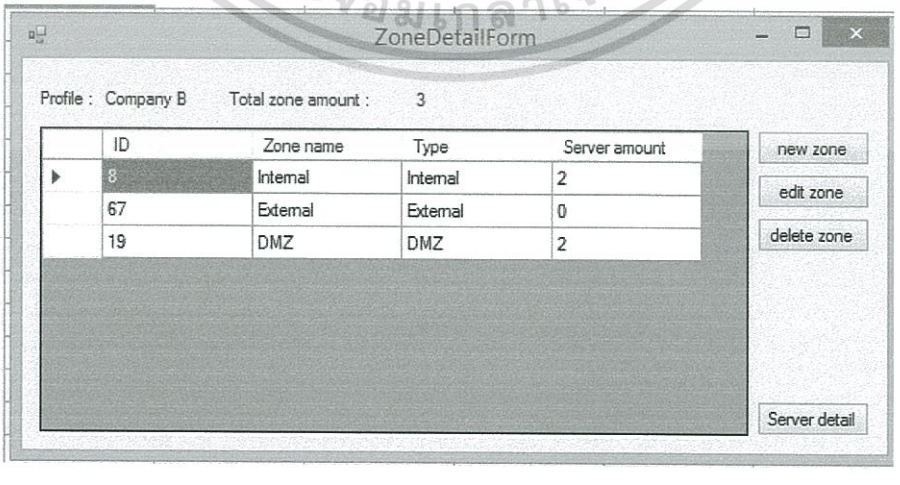
หลังจากกดปุ่ม Create new profile ที่หน้าจอหลักรายละเอียดจะแสดงดังรูปที่ 4.4 ซึ่งแสดงหน้าจอรับรายละเอียดในการสร้างโปรไฟล์ โดยผู้ใช้งานเริ่มต้นจากการตั้งชื่อโปรไฟล์ โดยวันที่ระบบจะสร้างขึ้นมาให้โดยการอ้างอิงจากวันที่ในปัจจุบัน



รูปที่ 4.4 แสดงหน้าจอรับรายละเอียดในการสร้างโปรไฟล์

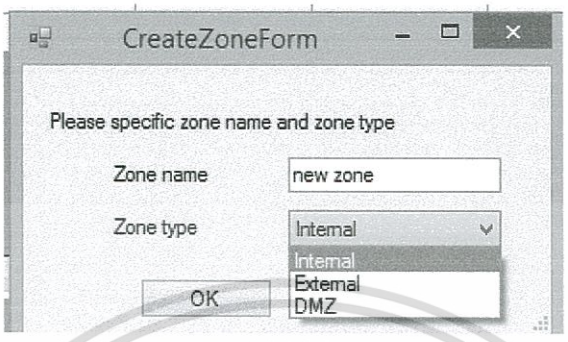
4. หน้าจอรับรายละเอียดโซน

หลังจากกดปุ่ม Zone detail ที่หน้าจอหลักรายละเอียดจะแสดงดังรูปที่ 4.5 ซึ่งแสดงหน้าจอโซนที่มีอยู่ทั้งหมด ซึ่งโดยพื้นฐานจะมีอยู่ 2 โซนคือ โซนภายใน (Internal) และโซนภายนอก (External) หากต้องการแก้ไขโซนให้คลิกไปยังโซนที่ต้องการแก้ไขและกดปุ่ม Edit zone และหากต้องการลบทิ้งให้คลิกไปยังโซนที่ต้อวการลบและกดปุ่ม Delete zone



รูปที่ 4.5 แสดงหน้าคำถามรายละเอียดในการจัดแบ่งโซน

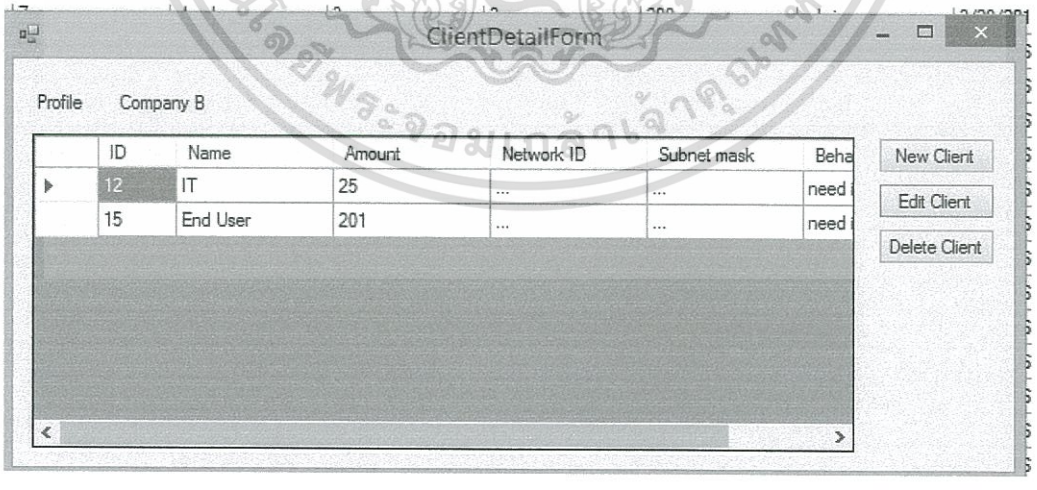
ในกรณีที่ต้องการสร้างโซนใหม่ ให้กดปุ่ม New zone แล้วหน้าจอจะแสดงรูปที่ 4.6 โดยในส่วนนี้ต้องกำหนดชื่อโซนและชนิดของโซนว่าเป็นโซนปลอดทหาร โซนภายใน หรือโซนภายนอก โดยโซนภายนอกคืออินเตอร์เน็ต



รูปที่ 4.6 แสดงหน้าจอการสร้างโซนใหม่

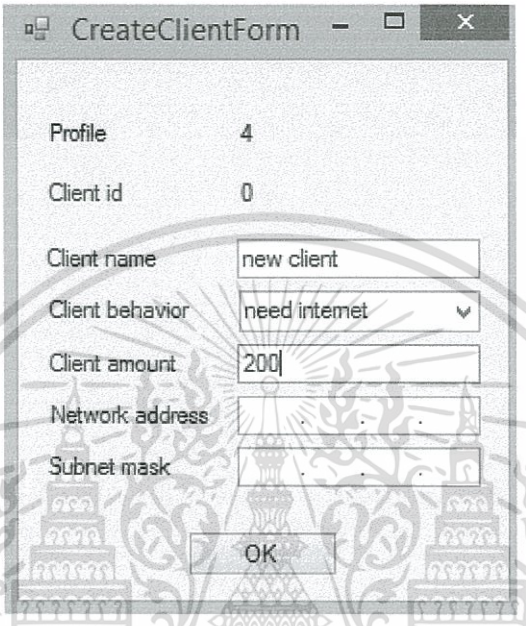
5. หน้าจอการรับรายละเอียดไคลแอนท์

หลังจากกดปุ่ม client detail ที่หน้าจอหลักรายละเอียดจะแสดงดังรูปที่ 4.7 ซึ่งแสดงหน้าจอรายละเอียดในส่วนของการรับข้อมูลไคลแอนท์ หากต้องการเพิ่มให้กดปุ่ม New client หากต้องการแก้ไขโซนให้คลิกไปยังไคลแอนท์ตัวที่ต้องการแก้ไขและกดปุ่ม Edit client และหากต้องการลบทิ้งให้คลิกไคลแอนท์กลุ่มที่ต้องการลบและกดปุ่ม Delete client



รูปที่ 4.7 แสดงหน้าจอการรับรายละเอียดไคลแอนท์

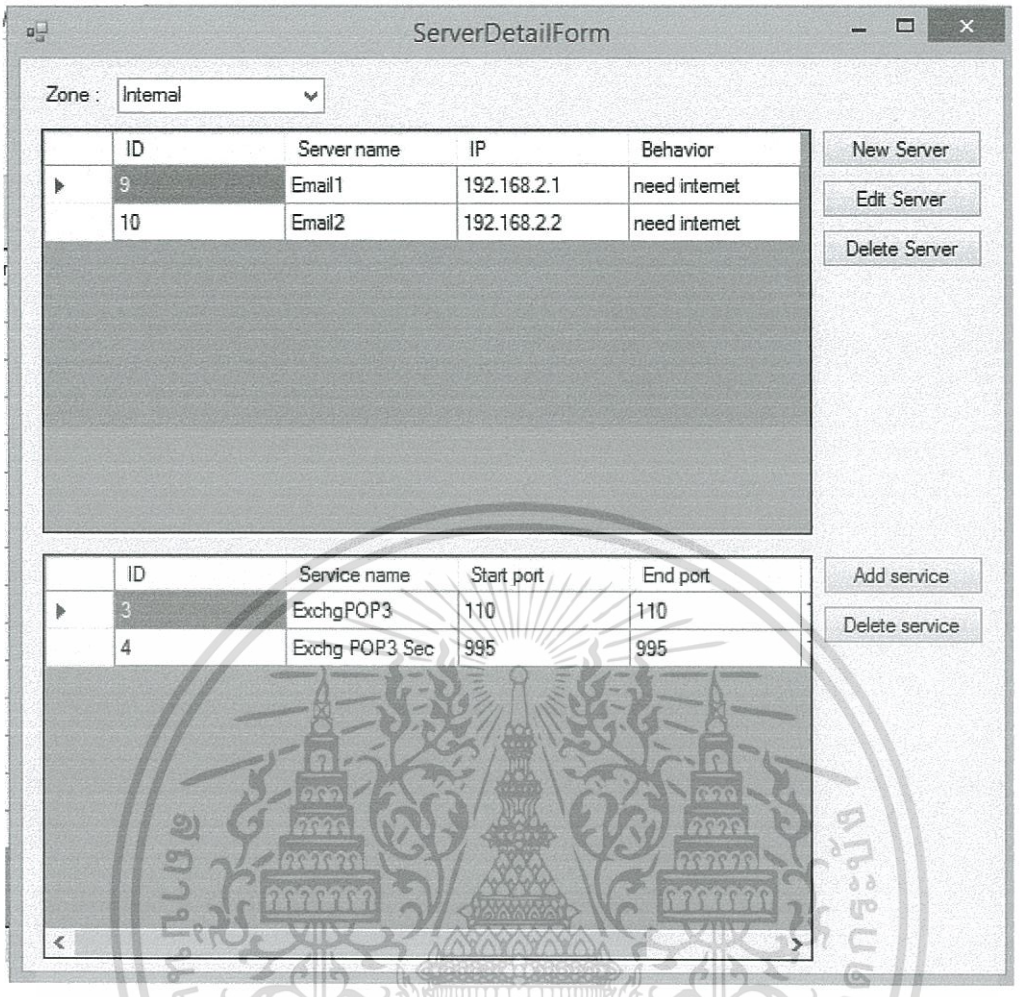
ในกรณีที่ต้องการสร้างไคลแอนท์กลุ่มใหม่ ให้กดปุ่มกดปุ่ม New client แล้วหน้าจอจะแสดงดัง รูปที่ 4.8 โดยในส่วนนี้ต้องกำหนดชื่อ พฤติกรรมว่าต้อการออกอินเตอร์เน็ตหรือไม่ และจำนวนของไคลแอนท์ในกลุ่มนั้นๆ ส่วนข้อมูลในส่วนของเน็ตเวิร์คไอดีสามารถเว้นและกำหนดในภายหลังได้



รูปที่ 4.8 แสดงหน้าจอการเพิ่มกลุ่มของไคลแอนท์

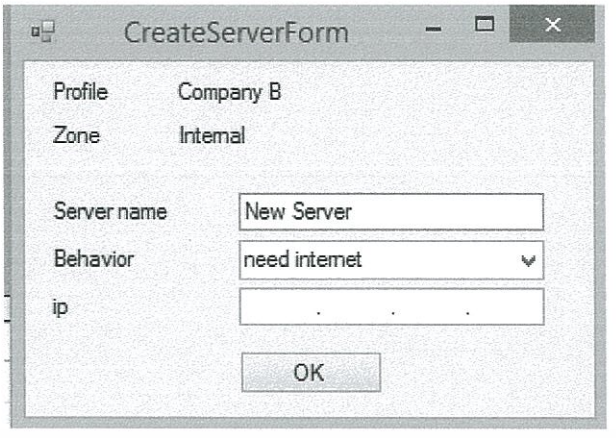
6. หน้าจอรับข้อมูลรายละเอียดของเซิร์ฟเวอร์

หลังจากกดปุ่ม Server detail ที่หน้าจอหลักรายละเอียดจะแสดงดังรูปที่ 4.9 ซึ่งแสดงหน้าจอหลักของการรับข้อมูลเซิร์ฟเวอร์ โดยผู้ใช้งานระบบต้องเลือกโซนที่ต้องการให้เครื่องเซิร์ฟเวอร์อยู่ และเพิ่มข้อมูลลงไป



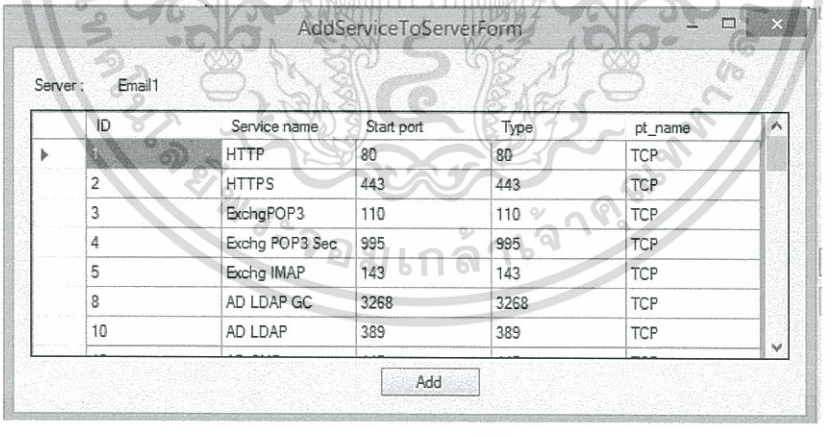
รูปที่ 4.9 แสดงหน้าจอหลักของการรับข้อมูลเซิร์ฟเวอร์

ในกรณีที่ต้องการรับข้อมูลพื้นฐานของเซิร์ฟเวอร์ ให้กดปุ่ม New Server แล้วหน้าจอจะแสดงดังรูปที่ 4.10 โดยผู้ดูแลระบบต้องตั้งชื่อให้เซิร์ฟเวอร์แต่ละตัว กำหนดพฤติกรรมของเซฟเวอร์นั้นๆว่ามีความจำเป็นต้องติดต่อกับอินเตอร์เน็ตภายนอกหรือไม่จำเป็น และกำหนดไอพีแอดเดรส ซึ่งไม่สามารถกำหนดข้อมูลไอพีแอดเดรสได้สามารถเว้นว่างข้อมูลในส่วนนี้ไปก่อนแล้วทำการเพิ่มหรือให้ระบบสร้างให้ในภายหลัง แต่หากผู้ดูแลระบบต้องการกำหนดด้วยตัวเอง ทุกครั้งที่มีการเพิ่มค่าลงในช่อง 'ip' ระบบจะมีการตรวจสอบว่าไอพีแอดเดรสนั้นอยู่ในวงเน็ตเวิร์คที่ซ้ำกับโซนอื่นๆ หรือซ้ำกับไอพีที่มีอยู่เดิมหรือไม่



รูปที่ 4.10 แสดงหน้าจอการรับข้อมูลพื้นฐานของเซริ์ฟวอร์

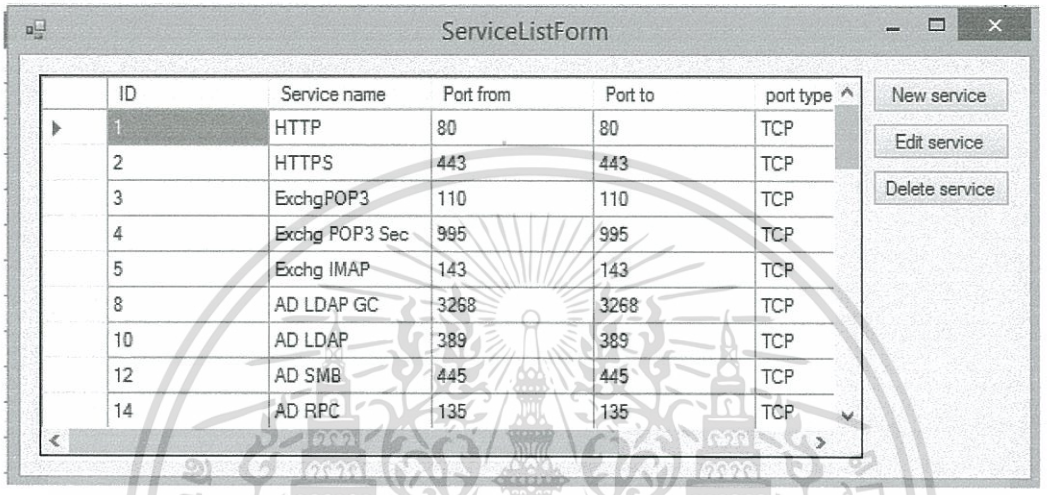
จากรูปที่ 4.11 แสดงหน้าจอการรับข้อมูลประเภทของเซิร์ฟเวอร์ เช่น อีเมลเซิร์ฟเวอร์ หรือเว็บเซิร์ฟเวอร์ เป็นต้น ซึ่งผู้ดูแลระบบสามารถกำหนดได้โดยการกดปุ่ม Add Service ที่หน้าจอหลักของการรับขอมูลเซิร์ฟเวอร์ ซึ่งสามารถเลือกจากเซอร์วิสพื้นฐานได้ทันที โดยจะกำหนดเพียงแค่หนึ่งอย่างหรือมากกว่าได้ ในกรณีที่ไม่มีเซอร์วิสให้เลือกผู้ใช้งานสามารถสร้างเซอร์วิสใหม่ๆขึ้นมาได้และมีการระบุพอร์ทลงไป ซึ่งจะแสดงเพิ่มเติมในส่วนถัดไป



รูปที่ 4.11 แสดงหน้าจอการรับข้อมูลประเภทของเซิร์ฟเวอร์

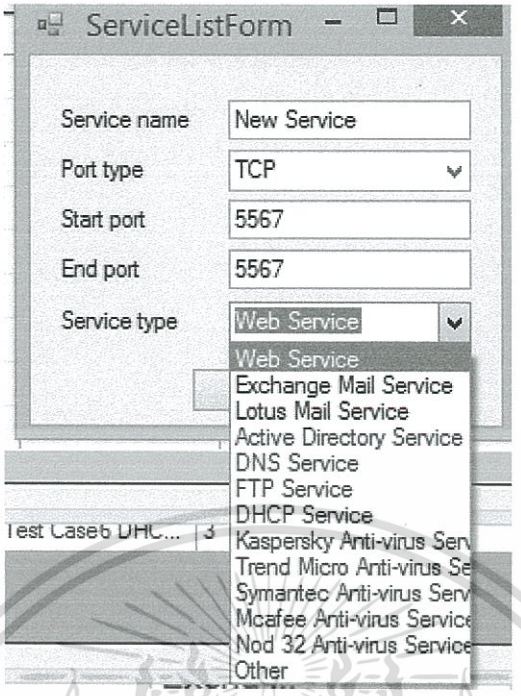
7. หน้าจอแสดงวิธีการสร้างเซอร์วิสใหม่

หลังจากกดปุ่ม Service list ที่หน้าจอหลักรายละเอียดจะแสดงดังรูปที่ 4.12 แสดงหน้าจอหลักในการสร้างเซอร์วิสใหม่ ซึ่งผู้ดูแลระบบสามารถเข้าสู่หน้าจอดังกล่าวได้จากการกดปุ่ม Service list ที่หน้าจอหลักของระบบ ซึ่งหน้าจอดังกล่าวจะแสดงข้อมูลเซอร์วิสพื้นฐานที่มีอยู่ทั้งหมด



รูปที่ 4.12 แสดงหน้าจอหลักในการสร้างเซอร์วิสใหม่

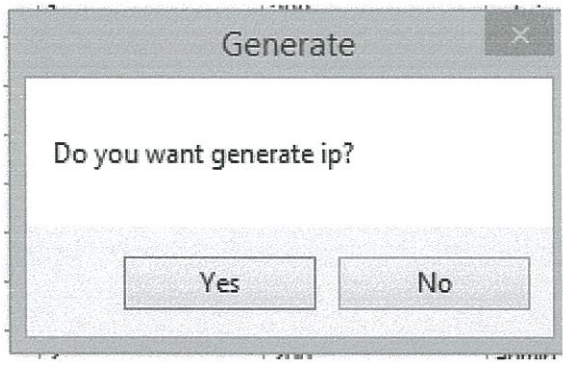
ในกรณีต้องการสร้างเซอร์วิสใหม่ ซึ่งในรูปที่ 4.13 แสดงหน้าจอในการสร้างเซอร์วิสใหม่ ซึ่งผู้ดูแลระบบสามารถเข้าสู่หน้าจอดังกล่าวได้จากการกดปุ่ม New Service ที่หน้าจอหลักในการสร้างเซอร์วิสใหม่ และผู้ดูแลระบบต้องตั้งชื่อให้เซอร์วิสแต่ละตัว เลือกชนิดของพอร์ต ใส่เลขพอร์ตและลักษณะการให้บริการ



รูปที่ 4.13 แสดงหน้าจอในการสร้างเซอร์วิสใหม่

8. หน้าจอการจัดสรรไอพีแอดเดรสและแสดงผล

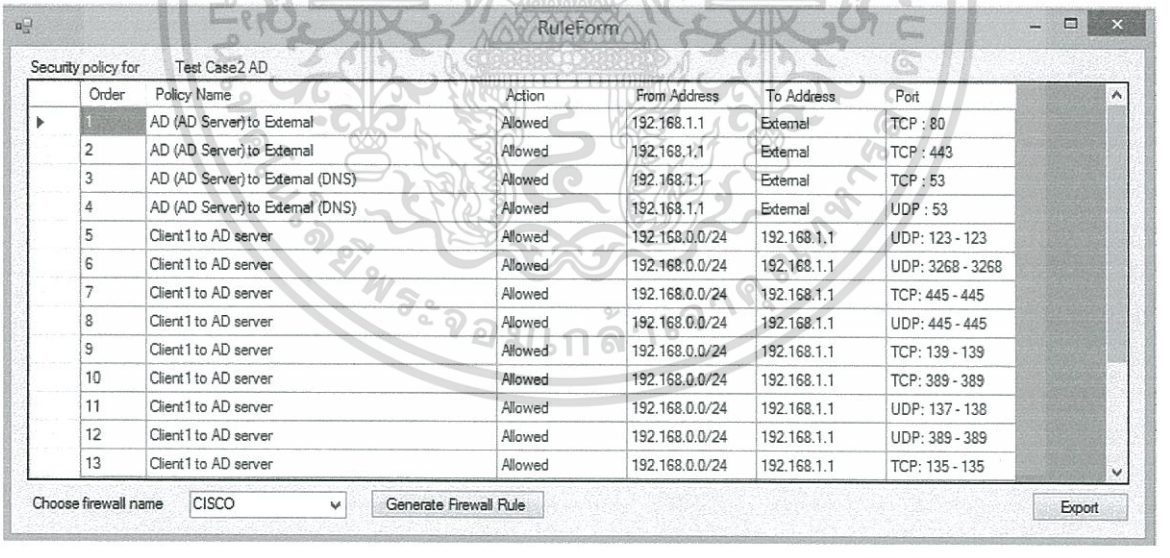
หลังจากกดปุ่ม Generate IP ที่หน้าจอหลักรายละเอียดจะแสดงดังรูปที่ 4.14 โดยหน้าจอจะแสดงคำถามในการจัดสรรไอพีแอดเดรสว่าต้องการให้ระบบจัดการให้หรือไม่ หากให้ระบบทำ ให้กด Yes และช่องข้อมูลไอพีแอดเดรสส่วนที่ยังว่างอยู่ ระบบจะเติมให้โดยอัตโนมัติ ทั้งค่าเน็ตเวิร์คแอดเดรสที่ไคลแอนท์และที่เซิร์ฟเวอร์ โดยผู้ดูแลระบบสามารถกดดูข้อมูลได้ที่หน้าจอหลักของการรับค่าไคล์แอนท์ (ที่ปุ่ม Client Detail) และหน้าจอหลักของการรับค่าเซิร์ฟเวอร์ (ที่ปุ่ม Server Detail)



รูปที่ 4.14 แสดงหน้าจอคำถามในการจัดสรรไอพีแอดเดรส

9. หน้าจอแสดงผลที่ได้จากการการวิเคราะห์นโยบายด้านความปลอดภัย

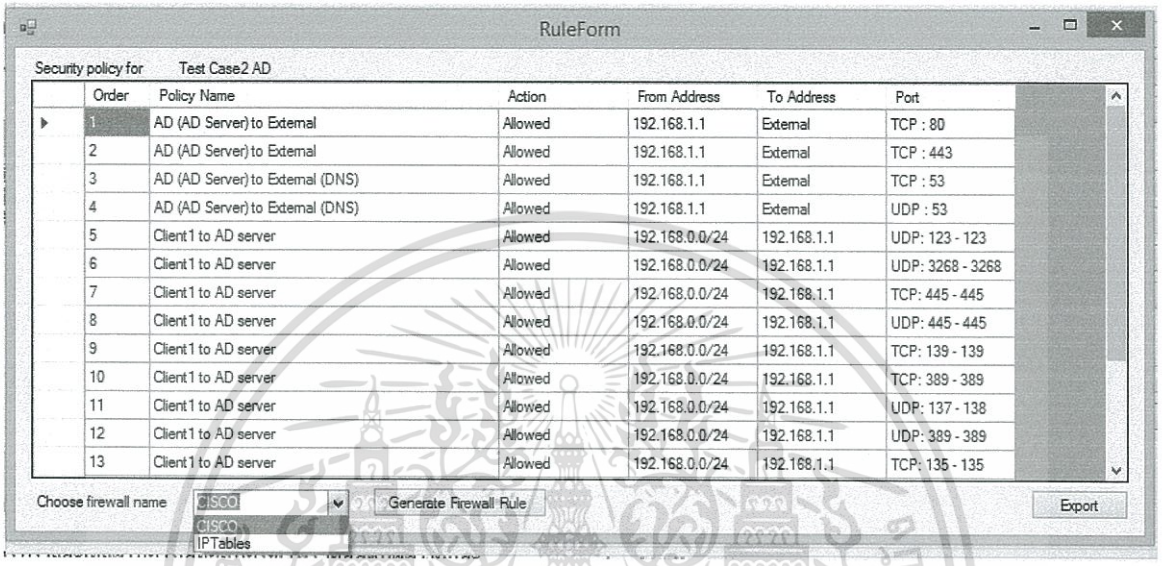
หลังจากใส่ข้อมูลพื้นฐานแล้วทั้งหมดระบบถึงจะสามารถวิเคราะห์นโยบายด้านความปลอดภัยได้ โดยในรูปที่ 4.15 แสดงหน้าจอแสดงผลที่ได้จากการการวิเคราะห์นโยบายด้านความปลอดภัย โดยแสดงผลเป็นข้อและเรียงตามลำดับเพื่อให้เกิดความถูกต้องในการนำข้อมูลที่ได้ไปใช้งาน



รูปที่ 4.15 แสดงหน้าจอแสดงผลที่ได้จากการการวิเคราะห์นโยบายด้านความปลอดภัย

10. หน้าการรับรายละเอียดในการเลือกอุปกรณ์ไฟร์วอลล์ชนิดต่างๆและแสดงผล

รูปที่ 4.16 แสดงหน้าจอรับรายละเอียดในการเลือกอุปกรณ์ไฟร์วอลล์ชนิดต่างๆและแสดงผลในการสร้างกฎให้ได้ตามนโยบายที่วางเอาไว้ โดยผลที่ได้จะตรงตามชนิดของอุปกรณ์ไฟร์วอลล์ที่เลือก ทำให้ผู้ใช้งานสามารถนำไปใช้งานกับอุปกรณ์ของตนเองได้



รูปที่ 4.16 แสดงหน้าจอรับรายละเอียดในการเลือกอุปกรณ์ไฟร์วอลล์ชนิดต่างๆและแสดงผล

บทที่ 5
บทสรุป

5.1 สรุปโครงการ

จากปัญหาการสร้างกฎสำหรับควบคุมการผ่านเข้าออก (Access Control Rule) สำหรับไฟร์วอลล์ในองค์กรขนาดเล็กและขนาดกลางที่ยังคงขาดคนที่มีความรู้ทางด้านความปลอดภัยบนระบบเครือข่าย ทำกฎที่ได้เกิดความหละหลวมจนกลายเป็นช่องโหว่ทางด้านระบบเครือข่าย โครงการนี้จึงทำการรวบรวมองค์ความรู้จากผู้ที่มีความรู้ความเชี่ยวชาญเฉพาะทางมาช่วยในการวางพื้นฐานการแบ่งโซนความปลอดภัย จัดการค่าไอพีแอดเดรสและเน็ตเวิร์คแอดเดรส และช่วยสร้างกฎสำหรับควบคุมการผ่านเข้าออก (Access Control Rule) ของข้อมูลบนอุปกรณ์ไฟร์วอลล์ ส่งผลให้ช่องโหว่ทางด้านระบบเครือข่ายลดลง ช่องทางการสื่อสารที่ไม่จำเป็นถูกตัดทิ้ง และปริมาณแบนด์วิธขององค์กรถูกใช้อย่างคุ้มค่า

5.2 ประโยชน์ที่ได้รับ

จากการรวบรวมองค์ความรู้จากผู้ที่มีความรู้ความเชี่ยวชาญเฉพาะทางมาช่วยในการวางพื้นฐานการแบ่งโซนความปลอดภัย จัดการค่าไอพีแอดเดรสและเน็ตเวิร์คแอดเดรส และช่วยสร้างกฎสำหรับควบคุมการผ่านเข้าออกของข้อมูล (Access Control Rule) บนอุปกรณ์ไฟร์วอลล์ ทำให้ระบบสามารถให้บริการได้ดังต่อไปนี้

1. สามารถรับรายละเอียดข้อมูลสภาพแวดล้อมทางด้านระบบเครือข่ายและการให้บริการได้
2. สามารถจัดสรรไอพีแอดเดรสสำหรับเซิร์ฟเวอร์ตามแต่ละโซนได้
3. สามารถจัดสรรเน็ตเวิร์คแอดเดรสของไคลแอนท์แต่ละกลุ่มได้
4. สามารถตรวจสอบค่าความซ้ำซ้อนของไอพีแอดเดรสและเน็ตเวิร์แอดเดรสได้
5. สามารถสร้างกฎสำหรับควบคุมการผ่านเข้าออกของข้อมูล (Access Control Rule) ที่สอดคล้องกับสภาพแวดล้อมของแต่ละองค์กรได้
6. สามารถสร้างกฎสำหรับควบคุมการผ่านเข้าออกของข้อมูล (Access Control Rule) สำหรับอุปกรณ์ไฟร์วอลล์แต่ละแบรนด์ได้

ประโยชน์ที่ผู้ใช้งาน องค์กรที่นำระบบไปใช้งาน และผู้พัฒนาระบบได้รับจากการพัฒนาระบบออกแบบและอิมพลีเมนท์นโยบายรักษาความปลอดภัยสำหรับอุปกรณ์ไฟร์วอลล์ มีดังนี้

1. ผู้พัฒนาระบบมีความรู้ความเข้าใจในหลักการทำงานของเซอร์วิสต่างๆ ในระบบสารสนเทศมากยิ่งขึ้น
2. ผู้พัฒนาระบบมีความรู้ความเข้าใจในการออกแบบกฎสำหรับควบคุมการผ่านเข้าออกของข้อมูล (Access Control Rule)
3. ผู้ใช้งานที่ยังขาดความรู้ความเข้าใจในการออกแบบกฎสำหรับควบคุมการผ่านเข้าออกของข้อมูล (Access Control Rule) สามารถทำงานได้ง่ายขึ้น
4. ช่วยลดช่องโหว่ทางด้านระบบเครือข่ายให้กับองค์กร
5. ช่วยปรับลดการสื่อสารที่ไม่จำเป็น และปริมาณแบนด์วิธขององค์กรถูกใช้อย่างคุ้มค่า

5.3 ข้อจำกัดของระบบ

ระบบออกแบบและอิมพลีเมนท์นโยบายรักษาความปลอดภัยสำหรับอุปกรณ์ไฟร์วอลล์ ยังมีข้อจำกัดอยู่ กล่าวคือ องค์กรใดที่มีการใช้งานวีแลน (VLAN) จะไม่รองรับการสร้างกฎของเน็ตเวิร์คที่มีการทำวีแลน (VLAN) อยู่ในอินเตอร์เฟสเดียวกัน และในการจัดกลุ่มของกฎเพื่อลดจำนวนข้อของกฎลงยังต้องอาศัยความรู้ความเข้าใจของผู้ที่ทำงานเฉพาะทางในการคิดและตัดสินใจ

5.4 ข้อเสนอแนะและแนวทางในการพัฒนาต่อ

ข้อเสนอแนะและแนวทางในการพัฒนาระบบออกแบบและอิมพลีเมนท์นโยบายรักษาความปลอดภัยสำหรับอุปกรณ์ไฟร์วอลล์ มีดังนี้

1. เพิ่มความสามารถในการจัดกลุ่มของกฎให้มีความกระชับมากยิ่งขึ้น
2. รองรับความต้องการของระบบเครือข่ายที่มีการทำวีแลน (VLAN)
3. เพิ่มความสามารถในการสร้างกฎโดยการจับข้อมูลการจราจรที่เกิดขึ้นจริงในระบบเครือข่าย ทำการวิเคราะห์ และสร้างกฎที่เหมาะสมแทนการรับความต้องการจากผู้ใช้
4. ปรับปรุงหน้าจอการแสดงผลกฎการควบคุมการผ่านเข้าออกของข้อมูล (Access Control Rule) ให้แสดงผลออกมาให้มีความหลากหลายมากยิ่งขึ้น

ภาคผนวก

1. ส่วนเพิ่มเติมสำหรับการสร้างกฎบนอุปกรณ์ไฟร์วอลล์เพื่อป้องกันการโจมตีแบบต่างๆ

การป้องกันการโจมตีต่างๆมีด้วยกันหลากหลายรูปแบบดังนี้

1.1 ป้องกันการปลอมไอพี (IP spoof)

สำหรับข้อมูลขาเข้ามาจากอินเทอร์เน็ตโดยป้องกันไม่ให้แพคเก็ตที่มีไอพีดังต่อไปนี้เข้ามาภายในเครือข่ายภายใน

127.0.0.0 - 127.255.255.255: Local Host Address

10.0.0.0 - 10.255.255.255: Reserved Address

172.16.0.0 - 172.31.255.255: Reserved Address

192.168.0.0 - 192.168.255.255: Reserved Address

224.0.0.0 - 239.255.255.255: Multicast Address

1.2 ป้องกันการโจมตีแบบ Land attack

การโจมตีแบบนี้จะใช้วิธีส่งแพคเก็ตที่มีข้อมูลต้นทาง (Source IP Address) ที่ตรงกันกับข้อมมูลปลายทาง (Destination IP Address) รวมทั้งค่าพอร์ตต้อนทาง (Source Port) และพอร์ตปลายทาง (Destination Port) ที่ตรงกัน จึงก่อให้เกิดการโจมตีแบบ Denial of Service (DOS)ได้ และการป้องกันคือการละทิ้ง (Drop) ไม่ให้ข้อมูลขาเข้าที่มีต้นทาง (Source IP address) ตรงกันกับไอพีของเครือข่ายภายในเข้ามาในระบบ

1.3 ป้องกันการโจมตีแบบ SYN Flood

การโจมตีที่ผู้บุกรุกจะส่ง SYN packet จำนวนมากมายังเครื่องปลายทางทำให้คิวของการรับการเชื่อมต่อ (Connection) ในการให้บริการอื่นๆเต็ม ทำให้ไม่สามารถให้บริการแก่เครื่องอื่นๆได้

1.4 การป้องกันจาก ICMP message บางชนิด

เครื่องไฟร์วอลล์และเครื่องอื่นๆภาย ในเครือข่ายควรได้รับป้องกันจาก ICMP message บางชนิด เช่น ป้องกันการรับ ICMP Echo Request ซึ่งสามารถส่งมาเพื่อรวบรวมข้อมูลสำหรับการโจมตีครั้งต่อไปหรือการส่ง ICMP Echo Request Packet ที่มีขนาดใหญ่ (Ping Flood) ซึ่งถือว่าเป็นรูปแบบ

หนึ่งในการโจมตี นอกจาก นี้ Redirect Packet ที่ส่งมาจากภายนอกยังสามารถเปลี่ยน Routing Table ในโฮสได้ซึ่งเป็นเรื่องที่อันตรายที่ควรป้องกัน

สำหรับข้อมูลขาออกนั้นควรอนุญาตให้ข้อมูล ICMP ดังต่อไปนี้เท่านั้นที่สามารถออกไปยังภายนอกได้

Echo request

Parameter Problem

Source Quench

สำหรับข้อมูลขาเข้านั้นควรอนุญาตให้ข้อมูล ICMP ดังต่อไปนี้เท่านั้นที่สามารถเข้ามาภายในได้

Echo Reply

Destination Unreachable

Source Quench

Time Exceeded

Parameter Problem

1.5 การป้องกันไฟรร์วอลล์จากการ Trace Route

ป้องกันไฟร์วอลล์และเครื่องอื่นๆภายในเครือข่ายจาก Trace Route เพราะ Trace Route เป็นโปรแกรมที่ช่วยให้ทราบถึงไอพีแอดเดรสของเร้าเตอร์ที่รับเพื่อส่งต่อแพคเก็ตไปทีละฮอบ (hop)จนกระทั่งถึงปลายทางที่ต้องการโดยใช้คุณสมบัติของ IP Time To Live (TTL)ในการทำงาน

โดยจะมีการกำหนด ค่า TTL counter ที่ทำให้เร้าเตอร์ที่แพคเก็ตผ่านต้องสร้าง ICMP Message ตอบกลับมาเสมอ สำหรับคำสั่ง “tracert” ในวินโดวส์จะใช้ Ping (ICMP Echo) เป็นตัวส่งแพคเก็ตออกไป ในขณะที่ Trace Route ในยูนิกซ์นั้นจะใช้ UDP Datagram เป็นตัวส่งข้อมูลออกไปดาต้าแกรม (Datagram)ที่ถูกส่งออกไปนั้นจะถูกส่งไปยังพอร์ต 33434 โดยดีฟอลต์และค่าหมายเลขพอร์ตนี้จะถูกเพิ่มขึ้นเมื่อได้รับแพคเก็ตที่ตอบกลับมาอย่างถูกต้อง

โดยปกติแล้ว Trace Route มักจะส่งดาต้าแกรมออกไปจำนวน 3 ดาต้าแกรมเพื่อป้องกันการสูญหายระหว่างทาง ถึงแม้ว่าจะมีการป้องกันการใช้งาน Trace Route จาก ทั้งยูนิกซ์และวินโดวส์แล้วก็ตามผู้บุกรุกก็ยังสามารถใช้วิธีอื่นในการ Trace เข้ามายังเครือข่ายภายในได้ เช่น การใช้โปรแกรม Firewalk หากต้องการหยุดยั้งการใช้ Trace Route รวมทั้ง Firewalk แล้วจะต้องใช้ วิธี Drop TTL Exceeded in Transit Packet ที่ขาออกไปสู่อินเทอร์เน็ต

บรรณานุกรม

คำอ้าย วิชุดา. 2010. **ความรู้เกี่ยวกับ OSI Model.** ค้นหาเมื่อ สิงหาคม 10, 2555, จาก http://mymint.tripod.com/report5.html

ภูวดล ด่านระหาญ. 2544. **Linux 2.4 Stateful Firewall: IPTABLES**. ค้นหาเมื่อ สิงหาคม 10, 2555, จาก http://www.thaicert.org/paper/firewall/iptables.php

Aziz, A. A. 2009. **Intrusion Detection & Response Leveraging Next Generation Firewall Technology**. Bethesda: SANS Institute.

Basic Firewall ที่ควรรู้. 2553. **Basic Firewall ที่ควรรู้.** ค้นหาเมื่อ สิงหาคม 10, 2555, จาก http://www.compspot.net/index.php?option=com_content&task=view&id=352&Itemid=49

Blueboard. 2553. **Firewall คืออะไร.** ค้นหาเมื่อ สิงหาคม 10, 2555, จาก http://blueboard-in-th.blogspot.com/2010/09/firewall.html

CISCO. 2010. **Configuring IP Access Lists (Document ID: 23602)**. Retrieved August 27, 2555, from http://www.cisco.com

Computer Science. 2553. **หน้าที่ OSI Model แต่ละ Layer.** ค้นหาเมื่อ สิงหาคม 10, 2555, จาก http://hub-analyst.blogspot.com/ 2010/05/ osi-model-layer.html

Edwards, W. et al. 2005. **CCSP Complete Study Guide**. San Francisco: SYBEX.

Firewall คืออะไร. 2555. **Firewall คืออะไร.** ค้นหาเมื่อ สิงหาคม 10, 2555, จาก http://www.it-guides.com/training-a-tutorial/network-system/109-what-is-firewall

Firewall (computing). 2012. **Firewall (computing)**. Retrieved January 14, 2012, from http://en.wikipedia.org/wiki/Firewall_%28computing%29

Smith. 2002. **Understand the evolution of firewalls.** Retrieved February 10, 2012, from http://www.techrepublic.com/article/understand-the-evolution-of-firewalls/1051837

Thaicert. 2008. **design.** Retrieved August 10, 2012, from http://thaicert.nectec.or.th/ paper/firewall/design.pdf

ประวัติผู้เขียน

นางสาวณินทิรา กาญจนศร เกิดวันที่ 9 สิงหาคม พ .ศ.2530 ที่จังหวัดชลบุรี สำเร็จการศึกษาปริญญาตรีวิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง เมื่อปี พ .ศ.2552 และศึกษาต่อในหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง เมื่อปี พ .ศ.2556