# ระบบใช้งานส่วนต่อประสานแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์สำหรับผู้ใช้ผ่านเว็บ

# WEB-BASE USER INTERFACE FOR PACKET FILTER FIREWALL OF FREEBSD

คงกะพัน อรรถชัยพานิช

KONGGAPAN ATTACHAIPARNICH

อาจารย์ที่ปรึกษา

ผศ.อัครินทร์ คุณกิตติ



รายงานนี้เป็นส่วนหนึ่งของวิชาโครงการพัฒนาระบบงาน

หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ

คณะเทคโนโลยีสารสนเทศ

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ภาคเรียนที่ 1 ปีการศึกษา 2550

# WEB-BASE USER INTERFACE FOR

# PACKET FILTER FIREWALL OF FREEBSD

KONGGAPAN ATTACHAIPARNICH

A SYSTEM DEVELOPMENT PROJECT

OF THE REQUIREMENT FOR THE DEGREE OF

MASTER OF SCIENCE PROGRAM IN INFORMATION TECHNOLOGY

FACULTY OF INFORMATION TECNOLOGY

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

1/ 2007

# ใบรับรองโครงการพัฒนาระบบงาน

# (SYSTEM DEVELOPMENT PROJECT)

เรื่อง

## ระบบใช้งานส่วนต่อประสานแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์สำหรับผู้ใช้ผ่านเว็บ

## WEB-BASED USER INTERFACE FOR PACKET FILTER FIREWALL OF FREEBSD


นายคงกะพัน อรรถชัยพานิช

รหัสประจำตัว 47066102


ขอรับรองว่ารายงานฉบับนี้ ข้าพเจ้าไม่ได้คัดลอกมาจากที่ใด

รายงานฉบับนี้ได้รับการตรวจสอบและอนุมัติให้เป็นส่วนหนึ่งของ

การศึกษาวิชาโครงการพัฒนาระบบงาน หลักสูตรวิทยาศาสตรมหาบัณฑิต (เทคโนโลยีสารสนเทศ)

ภาคเรียนที่ 1 ปีการศึกษา 2550

.....อาจารย์ที่ปรึกษา

(ผศ. อัครินทร์ คุณกิตติ)

.....กรรมการสอบ

(ผศ.ดร. จันทร์บูรณ์ สถิตวิริยวงศ์)

.....กรรมการสอบ

(รศ.ดร. นพพร โชติกกำธร)

| | |
|---|---|
| **หัวข้อ** | ระบบใช้งานส่วนต่อประสานแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์สำหรับผู้ใช้ผ่านเว็บ |
| **นักศึกษา** | นายคงกะพัน อรรถชัยพานิช |
| **รหัสนักศึกษา** | 47066102 |
| **ปริญญา** | วิทยาศาสตรมหาบัณฑิต |
| **สาขาวิชา** | เทคโนโลยีสารสนเทศ |
| **แขนงวิชา** | วิทยาการสารสนเทศ |
| **ปีการศึกษา** | 2550 |
| **อาจารย์ที่ปรึกษา** | ผศ.อัครินทร์ คุณกิตติ |

## บทคัดย่อ

เนื่องจากการจัดการกับการกรองแพ็กเก็ต (Packet Filter) ของแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ในระบบปฏิบัติการ FreeBSD มีการใช้งานที่ยุ่งยากและซับซ้อน จึงได้มีแนวคิดการพัฒนาระบบจัดการที่ง่ายและสะดวกมากขึ้น โดยโครงการมีวัตถุประสงค์ เพื่อพัฒนาระบบการจัดการกฎของการกรองแพ็กเก็ตผ่านส่วนของการติดต่อผู้ใช้งานแบบเว็บ และศึกษาถึงการใช้งานการกรองแพ็กเก็ตของแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ โดยในการพัฒนาโครงการนี้ ได้เลือกใช้โปรแกรมภาษา JSP ในส่วนของการพัฒนาส่วนติดต่อกับผู้ใช้งานผ่านเว็บ และใช้ Apache Tomcat เป็นเว็บเซิร์ฟเวอร์ ในการวิเคราะห์แบบจำลองเชิงแนวคิดของระบบได้อาศัย Unified Modeling Language (UML) มาใช้ โดยแบ่งออกเป็น 3 มุมมองดังนี้คือ Use Case Model นำมาใช้ในการอธิบายระบบงานทั้งหมด และ Class Diagram นำมาใช้ในการวิเคราะห์โครงสร้างข้อมูลของระบบ สำหรับ Sequence Diagram นำมาใช้ในการวิเคราะห์กลไกของระบบในเชิงลักษณะพฤติกรรมของระบบ

ในการพัฒนาระบบได้สร้างส่วนของการติดต่อผู้ใช้งานแบบเว็บให้สามารถกรอกข้อมูลที่จำเป็นต่อเครื่องที่ทำหน้าที่ในการกรองแพ็กเก็ต สร้างหน้าเว็บจัดการกฎในการกรองแพ็กเก็ต รวมถึงสามารถสำรองข้อมูลกฎและนำข้อมูลที่สำรองกลับมาใช้งาน แสดงข้อมูลล็อกและข้อมูลกฎ รวมทั้งลดข้อผิดพลาดจากการสร้างกฎด้วยการใช้ตัวเลือกของข้อมูล ตรวจสอบข้อมูลที่ผู้ใช้ได้ทำการกรอก และมีตัวช่วยสร้างเพื่อให้ง่ายต่อการใช้งาน ระบบที่พัฒนาได้นำไปใช้เป็นเครื่องมือช่วยในการสร้างกฎแก่เครื่องที่ทำหน้าที่กรองแพ็กเก็ตในเครือข่าย ซึ่งสามารถช่วยสร้างความสะดวกในการใช้งานและเพิ่มช่องทางการใช้งานที่มีประสิทธภาพให้กับแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์

| | |
|---|---|
| **Title** | Web-Based User Interface for Packet Filter Firewall of FreeBSD |
| **Student** | Mr. Konggapan Attachaiparnich |
| **Student ID** | 47066102 |
| **Degree** | Master of Science |
| **Programme** | Information Science |
| **Academic Year** | 2007 |
| **Advisor** | Asst.Prof.Akharin Khunkitti |


# ABSTRACT

Because of the Packet Filter management of Packet Filter Firewall in FreeBSD has difficult and complicated operation so it has an developing management idea to make it easier operate. The project's objective is to develop the operation system order to build the rule of the Packet Filter through web-based user interface and educate the operation of Packet Filter Firewall Filter. this project use JSP language programming for developing the part of web-based User Interface and use Apache Tomcat to be a web server. Unified Modeling language (UML) analyze the model Theory system, that separate in 3 visions. Use Case Model use for explanation structure all of the task system, Class Diagram use for analysis information system and Sequence Diagram use for analysis the system dynamic in the part of system behavior.

The system development create web-based user interface that able to fill useful information for the Packet Filter , create the web page that able to add or delete rule of the Filter and able to backup and restore information ,display log information and filter rule status and decrease the failure from building the rule by using the information choice, then examine information which is filled by users and it also has a tool for make an easy operation. The developed system is the tool for build the rule for packet Filter in the network which is make the comfortable operation and increase the effective operation channel for Packet Filter Firewall.

# กิตติกรรมประกาศ

ขอขอบพระคุณ คุณพ่อ ที่ช่วยกระตุ้นให้ผมทำงานและทุกสิ่งทุกอย่างที่ทำให้ผมมีชีวิตมาได้ถึงทุกวันนี้ และเป็นผู้สนับสนุนการศึกษาให้ผม

ขอขอบพระคุณ คุณแม่ ที่คอยให้กำลังใจให้ผมในการศึกษา และเป็นที่ปรึกษาเวลาผมพบกับปัญหาต่างๆ ทำให้มีกำลังใจในการทำงานต่อไป

ขอขอบคุณ เจ้ฝน ส้ม และน้องต๋วย พี่และน้องที่ต้องทำงานและช่วยเหลือสนับสนุนการศึกษาให้กับผมมาโดยตลอด แม้จะชอบชวนกลับบ้านบ่อยๆ ทำให้เวลาในการทำงานน้อยลง แต่ก็เป็นเวลาที่ผมมีความสุขมาก

ขอขอบคุณ อาจารย์ ผศ.อัครินทร์ คุณกิตติ ที่ให้คำปรึกษาในการเรียนและตรวจสอบรายงานต่างๆ เป็นอย่างดี และขอบคุณอาจารย์กรรมการสอบทุกท่านที่ช่วยตรวจสอบดูแลรายงานเล่มนี้ได้สมบูรณ์มากที่สุด

ขอขอบคุณใหญ่ บี กิ๊บ พี่นาน พี่แหม่ม แอ้ น้องเห็ด และเพื่อนๆ พี่ๆ ทุกคน ที่อธิบายการการเขียนโปรแกรม การทำเอกสาร การใช้งานโปรแกรมต่างๆ รวมถึงการมาทำให้สนุกสนานเวลาที่เครียดๆ

คงกะพัน อรรถชัยพานิช

# สารบัญ

หน้า

# สารบัญ (ต่อ)

# สารบัญรูป

# สารบัญรูป (ต่อ)

# สารบัญรูป (ต่อ)

# สารบัญรูป (ต่อ)

รูปที่ หน้า

# บทที่ 1
# บทนำ

## 1.1 ความเป็นมา

ในปัจจุบันระบบเครือข่ายคอมพิวเตอร์มีบทบาทสำคัญต่อการดำเนินการต่างๆขององค์กร ทั้งทางด้านการติดต่อสื่อสาร การทำธุรกิจ หรือทางด้านความบันเทิง ทำให้มีการเชื่อมต่อเครือข่ายของคอมพิวเตอร์เพิ่มขึ้นทั้งภายในองค์กรและภายนอกองค์กร จึงทำให้เกิดปัญหาด้านความปลอดภัยเพิ่มมากขึ้น จากปัญหาดังกล่าวทำให้มีการนำไฟร์วอลล์มาช่วยในการจัดการด้านความปลอดภัยอย่างแพร่หลายในระบบเครือข่าย โดยในปัจจุบันมีไฟร์วอลล์ที่สามารถเลือกใช้งานหลากหลาย โดยสามารถแบ่งได้เป็นไฟร์วอลล์ที่เป็นฮาร์ดแวร์ที่ถูกออกแบบมาโดยเฉพาะและเป็นลักษณะของซอฟท์แวร์ ซึ่งทั้งสองแบบมีข้อดีและข้อเสียที่แตกต่างกัน นอกจากนี้ยังสามารถแบ่งเป็นไฟร์วอลล์ที่มีลิขสิทธิ์ และ ไฟร์วอลล์ที่เป็นของฟรีได้อีก โดยในแบบที่มีลิขสิทธิ์นี้ ทางบริษัทผู้ผลิตไฟร์วอลล์เหล่านี้มีการออกแบบระบบติดต่อกับผู้ใช้ และระบบตัวช่วยเหลือในการปรับแต่งกฎต่างๆ ให้ผู้ใช้สามารถใช้งานอย่างสะดวกและมีประสิทธิภาพ แต่ไฟร์วอลล์ที่เป็นของฟรีนั้น โดยส่วนมากแล้วจะมีระบบในการติดต่อกับผู้ใช้และคำสั่งที่ใช้ในการปรับแต่งกฎของไฟร์วอลล์ที่ยุ่งยาก ทำให้เกิดความยุ่งยากในการสร้างกฎสำหรับควบคุมการทำงานต่างๆ และนอกจากนี้ผู้ใช้งานจะต้องมีความรู้ความชำนาญในเรื่องระบบเครือข่ายจึงเป็นส่วนหนึ่งที่สร้างความลำบากให้กับผู้ใช้งานที่ไม่มีความชำนาญ

โดยไฟร์วอลล์ที่สามารถนำมาติดตั้งและใช้งานได้ฟรีในปัจจุบันมีอยู่หลายตัว ซึ่งแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ (Packet Filter Firewall : PF) ก็เป็นซอฟท์แวร์อีกตัวหนึ่งที่ไม่ต้องเสียค่าใช้จ่าย แต่เนื่องจากตัวซอฟท์แวร์ไม่มีส่วนติดต่อผู้ใช้ในลักษณะของกราฟฟิกยูสเซอร์อินเตอร์เฟสมากับตัวซอฟท์แวร์ ทำให้การใช้งานจะต้องใช้การพิมพ์คำสั่งในการควบคุมและแสดงผลเป็นตัวอักษรเท่านั้น จึงทำให้เกิดแนวคิดในการพัฒนาระบบกราฟฟิกยูสเซอร์อินเตอร์เฟสสำหรับแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ เพื่อช่วยในการควบคุมการทำงานและการสร้างกฎของไฟร์วอลล์ให้มีความสะดวกและง่ายต่อการทำความเข้าใจ โดยผู้ใช้งานสามารถเลือกและกำหนดกฎที่จะใช้ในไฟร์วอลล์ได้โดยผ่านทางส่วนติดต่อกับผู้ใช้งานแบบหน้าจอของเว็บทำให้ง่ายต่อการใช้งานมากยิ่งขึ้น

## 1.2 เป้าหมายในการพัฒนาระบบ

การติดตั้งกฎของแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ ที่มีอยู่เดิมเป็นการทำงานโดยการใช้การป้อนคำสั่ง จึงทำให้ไม่มีความสะดวกต่อการใช้งาน ดังนั้นระบบที่จะมีการพัฒนาขึ้นมาใหม่จะเป็นระบบที่มีการรองรับการใช้งานในส่วนของการสร้างกฎที่ใช้ในการกรองข้อมูล(Filter Rule) เพื่อใช้ในการกำหนดการทำงานในการเลือกที่จะส่งต่อแพ็กเก็ต (Pass) หรือทิ้งแพ็กเก็ต (Block) ที่ผ่านเข้ามา และการกำหนดคุณสมบัติการทำงานที่เกี่ยวข้องกับการทำงานในการกรองแพ็กเก็ตของแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ โดยที่ผู้ใช้สามารถเรียกใช้ระบบการติดตั้งกฎผ่านเว็บและทำการติดตั้งคำสั่งโดยการป้อนเพียงข้อมูลที่จำเป็นต่อระบบโดยในการทำงานผู้ใช้ไม่จำเป็นต้องจดจำคำสั่งในการเรียกใช้หรือการติดตั้งกฎของไฟร์วอลล์ และสามารถเรียกดูกฎทั้งหมดที่ได้ทำการติดตั้งไว้แล้วได้ นอกจากนั้นยังมีเครื่องมือสำหรับช่วยให้ผู้ใช้สามารถสร้างกฎผ่านทางหน้าเว็บ Wizard setup โดยสามารถเลือกคุณสมบัติต่างๆจากหน้าเว็บ จากนั้นระบบจะสร้างกฎตามข้อมูลที่ผู้ใช้กำหนดให้ทันทีรวมทั้งระบบยังสามารถทำการสำรองข้อมูลกฎก่อนที่จะมีการเปลี่ยนแปลงแก้ไขและสามารถเรียกกฎที่ได้มีการติดตั้งไว้ใช้งานอยู่เดิมก่อนมีการแก้ไขกลับขึ้นมาใช้งานใหม่ได้

## 1.3 ขอบเขตในการพัฒนาระบบ

พัฒนาโปรแกรมระบบการกำหนดกฎไฟร์วอลล์ โดยมีความสามารถในการควบคุมการทำงานในส่วนของการทำแพ็กเก็ตฟิลเตอร์ โดยความสามารถในการทำงานมีรายละเอียดดังนี้

- สามารถเข้าใช้งานระบบผ่านทางหน้าเว็บ(Web-Base Interface)
- สามารถป้อนข้อมูลที่จำเป็นสำหรับการสร้างกฎของไฟร์วอลล์ ตามรูปแบบของกฎที่มีอยู่ โดยสามารถระบุได้ถึง IP Source, Port Source, IP Destination, Port Destination, Protocol, Direction, Interface เพื่อใช้ในการสร้างกฎให้ตรงตามความต้องการของผู้ใช้
- สามารถเพิ่ม แก้ไข หรือลบกฎที่ทำการสร้างขึ้นได้
- สามารถจัดวางลำดับของกฎใหม่ได้ เพื่อความสะดวกในการแก้ไขกฎ
- สามารถแสดงกฎที่สร้างขึ้นใหม่และกฎที่มีอยู่เดิมได้ ในลักษณะของตารางข้อมูลที่มีการแสดงรายละเอียดของกฎที่จำเป็นให้แก่ผู้ใช้
- สามารถทำงานในแบบ Wizard Setup โดยผู้ใช้กำหนดคุณสมบัติต่างๆ ของไฟร์วอลล์ จากนั้นระบบทำการสร้างกฎจากข้อมูลที่ได้รับ
- สามารถรองรับการสร้างและแก้ไขกฎในแบบ Advance Configuration โดยผู้ใช้สามารถพิมพ์รูปประโยค(Syntax) ทั้งหมด

- สามารถสำรองข้อมูลกฎที่ทำการสร้างจากตัวโปรแกรมและเรียกกฎที่ทำการสำรองไว้มาใช้งานได้
- สามารถแสดงผลการทำงานและค่าสถิติต่างๆของกฎที่ทำงานอยู่ได้
- สามารถแสดงข้อมูลของไฟล์ Log ของแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ได้
- สามารถควบคุมการทำงานใช้งานแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ได้

## 1.4 องค์ประกอบของระบบงาน

ระบบงานประกอบด้วยองค์ประกอบต่างๆ ดังต่อไปนี้

**1.4.1 เครื่องคอมพิวเตอร์เซิร์ฟเวอร์** ติดตั้งระบบปฏิบัติการ FreeBSD และแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ เพื่อทำหน้าที่ตรวจสอบข้อมูลที่ผ่านเข้าออก ซึ่งได้รับการเตรียมความพร้อมดังนี้

- ติดตั้งระบบปฏิบัติการ FreeBSD version 5 เพื่อรองรับการตรวจสอบข้อมูลที่ผ่านเข้าออก
- ติดตั้งซอฟต์แวร์ไฟร์วอลล์ โดยเลือกใช้ แพ็กเก็ตฟิลเตอร์ไฟร์วอลล์
- ติดตั้งส่วนให้บริการเว็บเซิร์ฟเวอร์สำหรับเป็นส่วนติดต่อกับผู้ใช้เพื่อใช้ในการควบคุมระบบ โดยเลือกใช้ Apache Tomcat เวอร์ชัน 5.5
- ติดตั้งซอฟต์แวร์ภาษา โดยเลือกใช้ภาษา JSP
- ติดตั้งโปรแกรมระบบการกำหนดกฎไฟร์วอลล์

**1.4.2 เครื่องคอมพิวเตอร์ไคลเอ็นท์** ที่ใช้ควบคุมระบบการกำหนดกฎไฟร์วอลล์โดยผ่านทางเว็บ ซึ่งได้รับการเตรียมความพร้อมดังนี้

- ติดตั้งระบบปฏิบัติการ Windows XP Professional
- ติดตั้งโปรแกรมเว็บบราวเซอร์ สำหรับติดต่อกับเว็บเซิร์ฟเวอร์ เพื่อควบคุมโปรแกรมการกำหนดกฎไฟร์วอลล์

## 1.5 ขั้นตอนในการพัฒนาระบบ

ประกอบไปด้วยขั้นตอนต่างๆ ดังนี้

**1.5.1 ศึกษาความเป็นไปได้ในการพัฒนาระบบการกำหนดกฎแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์** เพื่อกำหนดขอบเขตของปัญหาและวางแผนวิธีการพัฒนาโปรแกรม รวมถึงกำหนดเป้าหมายในการพัฒนาโครงการ โดยศึกษา ดังนี้

- ศึกษาวิธีการติดตั้งและการใช้งานซอฟต์แวร์ต่างๆ ที่ใช้สำหรับการสร้างระบบไฟร์วอลล์และระบบเว็บเซิร์ฟเวอร์ เพื่อรองรับการติดต่อจากภายนอก ได้แก่ FreeBSD, แพ็กเก็ตฟิลเตอร์ไฟร์วอลล์, Apache Tomcat Web Server, JSP
- ศึกษาเทคโนโลยีการรักษาความปลอดภัยเครือข่ายโดยใช้ไฟร์วอลล์
- ศึกษาวิธีการสร้างกฎสำหรับไฟร์วอลล์ให้มีประสิทธิภาพ
- ศึกษาเทคโนโลยีแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์บนระบบปฏิบัติการ FreeBSD
- ศึกษาจากเอกสารคู่มือ OMG Unified Modeling Language Specification V1.4
- ศึกษาการใช้งานโปรแกรมภาษา Java และ JSP เพื่อพัฒนาโปรแกรมประยุกต์ ในส่วนของการติดต่อกับผู้ใช้งาน

### 1.5.2 การวิเคราะห์และออกแบบ

ทำการวิเคราะห์และออกแบบรวมถึงกำหนดความต้องการของโครงการพัฒนาระบบ โดยได้ทำการออกแบบให้ระบบสามารถเพิ่มหรือลบกฎที่ทำการสร้างและป้อนข้อมูลที่จำเป็นสำหรับการสร้างกฎของไฟร์วอลล์ ซึ่งระบุได้ถึง IP Source, Port Source, IP Destination, Port Destination, Protocol, Direction, Interface รวมถึงสามารถสำรองข้อมูลกฎและเรียกกฎที่มีการใช้งานอยู่เดิมก่อนที่จะทำการแก้ไขเปลี่ยนแปลงขึ้นมาทำงานได้ และแสดงผลการตรวจสอบการทำงานของไฟร์วอลล์

### 1.5.3 การพัฒนาและทดสอบ

- ทำการติดตั้งและทดสอบการทำงานของแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์
- ทำการพัฒนาโปรแกรมและทดสอบการทำงานของโปรแกรมในฟังก์ชันต่างๆ

### 1.5.4 การทดลองใช้งานและปรับปรุงแก้ไข

นำโปรแกรมมาทดลองใช้งานและปรับปรุงแก้ไขเพื่อให้สามารถใช้งานได้ถูกต้องและปรับปรุงให้การทำงานในส่วนที่ยุ่งยากมีความสะดวกมากยิ่งขึ้น

## 1.6 ประโยชน์ที่คาดว่าจะได้รับ

1. ได้พัฒนาความรู้ความเข้าใจเรื่องการทำงานพื้นฐานของไฟร์วอลล์
2. ได้พัฒนาความรู้ความเข้าใจเรื่องการทำงานของโปรแกรมแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์
3. ได้พัฒนาความรู้ความสามารถในการวิเคราะห์ ออกแบบและพัฒนาระบบงานและสามารถนำไปใช้ประโยชน์ต่อการทำงานในอนาคตได้
4. ได้โปรแกรมประยุกต์ที่ผู้ดูแลระบบหรือผู้ใช้งานทั่วไป สามารถนำไปใช้งานและทำการแก้ ไขการทำงานกฎต่างๆของระบบไอพีไฟร์วอลล์ได้โดยสะดวก รวดเร็ว ในลักษณะการทำงานแบบเว็บ

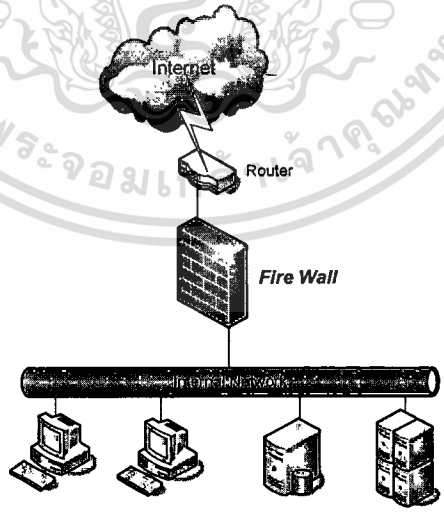
5. เป็นอีกทางเลือกหนึ่งในการเลือกใช้เป็นเครื่องมือที่ช่วยให้การทำงานกับไฟร์วอลล์มีความสะดวกมากขึ้น และมีส่วนติดต่อกับผู้ใช้ที่น่าสนใจกว่าระบบเดิม

# บทที่ 2
# แพ็กเก็ตฟิลเตอร์ไฟร์วอลล์บนระบบปฏิบัติการณ์ FreeBSD

ในปัจจุบันการทำงานได้มีการใช้เทคโนโลยีระบบเครือข่ายอินเทอร์เน็ตเข้ามาช่วยในการติดต่อสื่อสารแลกเปลี่ยนข้อมูลระหว่างภายในและภายนอกองค์กร ซึ่งข้อมูลที่ส่งผ่านในเครือข่ายนั้นมีทั้งข้อมูลที่เป็นความลับและมีความสำคัญต่อองค์กร และข้อมูลที่ไม่สำคัญ ซึ่งข้อมูลที่มีความสำคัญเหล่านี้เป็นข้อมูลที่จำเป็นต้องดูแลและป้องกันไม่ให้ข้อมูลดังกล่าวถูกนำไปใช้โดยผู้ไม่ประสงค์ดีหรือผู้ไม่มีสิทธิในการเข้าถึงข้อมูลเหล่านั้น ดังนั้นสิ่งหนึ่งที่ทำให้ผู้ดูแลระบบเครือข่ายส่วนใหญ่ควรให้ความสำคัญจึงเป็นไปในเรื่องของการรักษาความปลอดภัยให้กับระบบเครือข่ายโดยระบบที่ถูกนำมาใช้งานอย่างแพร่หลายคือไฟร์วอลล์

## 2.1 ไฟร์วอลล์

ไฟร์วอลล์เป็นระบบหนึ่งหรือกลุ่มของระบบที่บังคับใช้นโยบายการควบคุมการเข้าถึงระหว่างเครือข่ายที่เชื่อมต่อกัน โดยแต่ละระบบมีวิธีการในการทำงานที่แตกต่างกันไป แต่โดยหลักการแล้วสามารถแยกกลไกการทำงานของไฟร์วอลล์ได้เป็นสองส่วน ส่วนแรกคือการป้องกันข้อมูลที่ถูกส่งเข้ามา และส่วนที่สองคือการส่งผ่านข้อมูลออกไป โดยตัวอย่างการใช้งานไฟร์วอลล์สามารถแสดงได้ดังรูปที่ 2.1




**รูปที่ 2.1** ไฟร์วอลล์กั้นระหว่างอินเทอร์เน็ตกับเครือข่ายภายใน

**ขีดความสามารถของไฟร์วอลล์**

ขีดความสามารถโดยทั่วไปนั้นมีดังนี้

- บังคับใช้นโยบายด้านความปลอดภัย โดยการกำหนดกฎให้กับไฟร์วอลล์ว่าจะอนุญาตหรือไม่ให้ใช้บริการชนิดใด
- เป็นจุดรวมสำหรับรักษาความปลอดภัย ทำให้การพิจารณาดูแลและการตัดสินใจด้านความปลอดภัยของระบบเป็นไปได้ง่ายขึ้น เนื่องจากการติดต่อทุกชนิดกับเครือข่ายภายนอกจะต้องผ่านไฟร์วอลล์ การดูแลที่จุดนี้เป็นการดูแลความปลอดภัยในระดับของเครือข่าย (Network-based Security)
- บันทึกข้อมูลการทำงาน หรือกิจกรรมต่างๆ ที่ผ่านเข้าออกเครือข่าย
- ป้องกันเครือข่ายบางส่วนจากการเข้าถึงของเครือข่ายภายนอก เช่น ถ้าหากมีบริการบางส่วนที่ต้องการให้เครือข่ายภายนอกเข้ามาใช้บริการ (เช่น ถ้ามีเว็บเซิร์ฟเวอร์) แต่ส่วนที่เหลือไม่ต้องการให้เครือข่ายภายนอกเข้ามากรณี เช่นนี้จะสามารถใช้ไฟร์วอลล์ช่วยได้
- ปิดกั้นการส่งผ่านข้อมูลจากภายนอกเครือข่ายเข้ามาในเครือข่าย แต่ยอมให้เครื่องที่อยู่ภายในเครือข่ายสามารถติดต่อออกไปภายนอกได้
- ไฟร์วอลล์บางชนิดสามารถตรวจสอบไวรัสได้โดยทำการตรวจสอบไฟล์ที่ส่งผ่านเข้ามาโดยใช้โปรโตคอล HTTP, FTP และ SMTP

**ข้อจำกัดของไฟร์วอลล์**

ถึงแม้ว่าไฟร์วอลล์จะสามารถช่วยเพิ่มความปลอดภัยให้กับเครือข่ายได้เป็นอย่างมากโดยการตรวจดูข้อมูลที่ผ่านเข้าออก แต่ก็มีข้อจำกัดบางประการที่ไฟร์วอลล์ไม่สามารถป้องกันได้ ได้แก่

- อันตรายที่เกิดจากเครือข่ายภายใน ไม่สามารถป้องกันได้เนื่องจากอยู่ภายในเครือข่ายเองไม่ได้ผ่านไฟร์วอลล์เข้ามา
- อันตรายจากภายนอกที่ไม่ได้ผ่านเข้ามาทางไฟร์วอลล์ เช่นการ Dial-up เข้ามายังเครือข่ายภายในโดยตรงโดยไม่ได้ผ่านไฟร์วอลล์
- อันตรายจากวิธีใหม่ๆ ที่เกิดขึ้น ซึ่งทุกวันนี้มีการพบช่องโหว่ใหม่ๆ เกิดขึ้นทุกวัน จึงไม่สามารถไว้ใจไฟร์วอลล์โดยการติดตั้งเพียงครั้งเดียวแล้วคาดหวังให้ปลอดภัยตลอดไป ดังนั้นจึงต้องมีการดูแลรักษาอย่างต่อเนื่องสม่ำเสมอ
- ไม่สามารถป้องกันไวรัสได้อย่างมีประสิทธิภาพเนื่องจากจำนวนของไวรัสที่มีอยู่มากมายและมีการเกิดขึ้นของไวรัสใหม่ๆตลอดเวลา จึงเป็นเรื่องที่ยากมากที่ไฟร์วอลล์จะสามารถตรวจสอบรูปแบบของไวรัสได้ทั้งหมด

ถึงแม้ว่าไฟร์วอลล์จะเป็นเครื่องมือที่สามารถช่วยในการป้องกันการโจมตีจากภายนอกเครือข่ายได้อย่างมีประสิทธิภาพ แต่การที่จะใช้ไฟร์วอลล์ให้ได้ประโยชน์สูงสุดนั้นจะต้องขึ้นอยู่กับนโยบายโดยรวมขององค์กร ดังนั้นไฟร์วอลล์จึงเป็นเพียงองค์ประกอบหนึ่งที่จะช่วยทำให้เกิดความปลอดภัย

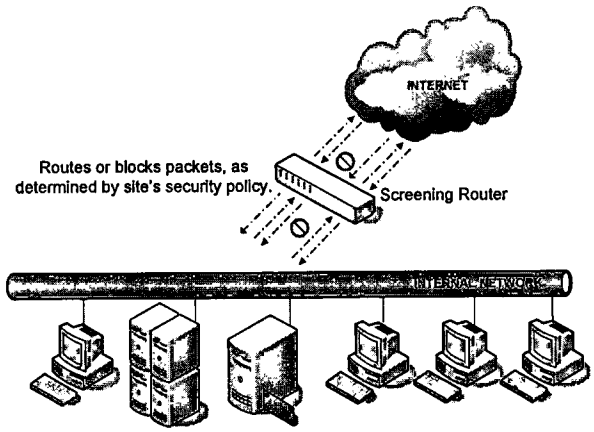
## 2.2 ชนิดของไฟร์วอลล์

เนื่องจากไฟร์วอลล์เป็นเครื่องมือควบคุมทราฟฟิคในเครือข่าย ทำให้มีเครื่องมือที่สามารถทำหน้าที่ดังกล่าวได้อยู่หลายลักษณะ และต่างก็เรียกว่าไฟร์วอลล์เหมือนกัน ซึ่งที่จริงแล้วลักษณะการทำงานและขีดความสามารถในการทำงาน รวมทั้งข้อจำกัดนั้นแตกต่างกันมาก การนำไปใช้และความเหมาะสมก็แตกต่างกันออกไป โดยสามารถแบ่งไฟร์วอลล์ตามลักษณะการทำงานเป็นเกณฑ์ จะสามารถแบ่งได้ดังนี้

### 2.2.1 Packet Filter Firewall

เป็นไฟร์วอลล์พื้นฐานที่มีความสามารถในการควบคุมทราฟฟิคโดยอาศัยการตรวจสอบข้อมูลที่ปรากฏอยู่ในแพ็กเก็ต ไฟร์วอลล์ประเภทนี้อาจเป็นความสามารถที่อยู่ในเราเตอร์ โดยการทำงานจะอาศัยโครงสร้างพื้นฐานที่เราเตอร์มีอยู่ให้ทำหน้าที่มากกว่าการเลือกเส้นทางให้แพ็กเก็ตเพียงอย่างเดียว แต่จะทำการตรวจสอบเปรียบเทียบกับเงื่อนไขที่กำหนดไว้ก่อนจึงจะทำการส่งแพ็กเก็ตออกไป

ไฟร์วอลล์ชนิดนี้โดยทั่วไปจะเรียกว่า Screening Router เพราะเป็นการนำเราเตอร์ทั่วไปที่สามารถกำหนดแอคเซสรูลได้มาดัดแปลงใช้ในการควบคุมทราฟฟิค ซึ่งการกำหนดแอคเซสรูลของทราฟฟิคทำได้โดยพิจารณาจากข้อมูลแต่ละแพ็กเก็ต แต่เนื่องจากเราเตอร์เป็นอุปกรณ์ที่ทำงานในอินเตอร์เน็ตเลเยอร์ ทำหน้าที่เลือกเส้นทางให้กับแพ็กเก็ตโดยพิจารณาจาก IP Address และจะทำการเลือกเส้นทางและส่งทีละแพ็กเก็ต ดังนั้นจึงทำให้สามารถควบคุมทราฟฟิคได้ดีในระดับ IP คือดูจาก IP Address ต้นทางและปลายทางเท่านั้น สำหรับข้อมูลของโปรโตคอลในเลเยอร์ที่สูงขึ้นไป เช่น TCP, UTP และ ICMP เนื่องจากเราเตอร์มีขีดจำกัดในการรับรู้ข้อมูลในเลเยอร์สูงขึ้นไปคือ ทรานสปอร์ตเลเยอร์ จึงทำให้การควบคุมทราฟฟิคโดยระบุเงื่อนไขของโปรโตคอลในทราน สปอร์ตเลเยอร์ทำได้อย่างจำกัด คือสามารถควบคุมทราฟฟิคได้เฉพาะเมื่อข้อมูลในทรานสปอร์ตเลเยอร์นั้นสามารถบันจุได้ในแพ็กเก็ตเดียว หากมีการแฟรกเมนต์และต้องเชื่อมโยงหลายแพ็กเก็ตเข้าด้วยกัน เราเตอร์จะไม่มารถรับรู้การถึงการเชื่อมโยงเหล่านั้นได้ โดยตัวอย่างการทำงานของ Packet Filter Firewall สามารถแสดงได้ดังรูปที่ 2.2




**รูปที่ 2.2** ใช้ Screening Router ทำหน้าที่ Packet Filtering

**ข้อดีของ Packet Filter Firewall**

1. ราคาถูกเพราะเป็นคุณสมบัติที่มักมีอยู่ในเราเตอร์ โดยอาศัยการกำหนดแอคเซสรูลที่เหมาะสมเท่านั้นซึ่งสามารถช่วยในการสร้างความปลอดภัยได้ในระดับหนึ่ง

2. หากขนาดของเครือข่ายไม่ใหญ่มาก และมีการใช้งานอินเตอร์เน็ตอย่างจำกัด ก็สามารถใช้งานแทนไฟร์วอลล์ได้

3. การใช้ Packet Filter Firewall ควบคู่ไปกับการใช้ไฟร์วอลล์อื่น จะเป็นการแบ่งเบาภาระของไฟร์วอลล์ได้มาก

4. การป้องกันบางประเภทไม่สามารถป้องกันได้โดยใช้ไฟร์วอลล์ แต่จะต้องทำโดยการกำหนดที่เราเตอร์เท่านั้น

**ข้อเสียของ Packet Filter Firewall**

1. การกำหนดแอคเซสรูลทำได้ยาก ไม่มีระบบยูสเซอร์อินเตอร์เฟสเพื่อช่วยในการทำงาน ส่วนใหญ่จะใช้วิธีการเทลเน็ตเข้าไปยังเร้าเตอร์ แล้วป้อนคำสั่งในลักษณะของ Command Line เข้าไปโดยตรงที่เราเตอร์ ทำให้มีโอกาสเกิดความผิดพลาดในการป้อนข้อมูลผิดรูปแบบ

2. คำสั่งในการทำงานยังผูกติดกับผู้ผลิตเราเตอร์ ไม่มีมาตรฐานของคำสั่ง หากเปลี่ยนยี่ห้อของเราเตอร์ก็ต้องศึกษาคำสั่งใหม่

3. ไม่สามารถกำหนดกฎที่มีความซับซ้อนได้ เนื่องจากขีดจำกัดของเราเตอร์ที่ทำงานโดยพิจารณาทีละแพ็กเก็ตเท่านั้น

4. มีความสามารถจำกัด เช่นไม่สามารถบันทึก Log ของแพ็กเก็ตที่มีความผิดปกติไว้ตรวจสอบภายหลังได้

5. เราเตอร์มีกำลังในการประมวลผลที่จำกัด ถ้าหากเครือข่ายมีขนาดใหญ่และมีการสื่อสารข้อมูลที่หนาแน่น เราเตอร์จะต้องทำงานหนักอยู่แล้ว เมื่อต้องทำการประมวลผลแอคเซส

รูลด้วยก็อาจจะทำให้ประสิทธิภาพในการเลือกเส้นทางให้แพ็กเก็ตที่ต่ำลง และจะทำให้เกิดปัญหาคอขวดที่เราเตอร์ได้

**2.2.2 Circuit-Level Firewall**

การสื่อสารข้อมูลโดยทั่วไปจะเป็นการสื่อสารแบบต่อเนื่อง โต้ตอบไปมาระหว่างผู้รับและผู้ส่ง โปรโตคอลที่อยู่ในเลเยอร์ที่สูงกว่าอินเตอร์เน็ตเลเยอร์ เช่น ระดับทรานสปอร์ตเลเยอร์ คือTCP, UTP หรือระดับแอพพลิเคชั่นเลเยอร์ คือ FTP, HTTP, SMTP ล้วนแล้วแต่ต้องมีสถานะในการสื่อสาร (State) สถานะนี้จะทำให้ทั้งสองฝั่งสามารถสื่อสารกันได้อย่างต่อเนื่องคือรู้ว่าตอนนี้กำลังอยู่นะจุดใดและต้องรับหรือส่งข้อมูลใดเป็นลำดับต่อไป

Circuit-Level Firewall เป็นไฟร์วอลล์ทำงานโดยที่สามารถเข้าใจสถานะการสื่อสารทั้งกระบวนการ เพราะว่าการสื่อสารข้อมูลจะสมบูรณ์ได้นั้นจะต้องมีการส่งและการรับอย่างสอดคล้องกัน หมายความว่าไฟร์วอลล์จะสามารถควบคุมการสื่อสารได้จริงต้องสามารถเข้าใจกระบวนการสื่อสารตั้งแต่เริ่มต้นจนจบการสื่อสาร โดยทั่วไปเราจะเรียกไฟร์วอลล์แบบนี้ว่า Stateful Inspection Firewall เป็นไฟร์วอลล์ที่ใช้หลักการของแพ็กเก็ตฟิลเตอร์ริ่งและการกำหนดแอคเซสรูลเช่นเดียวกับ Packet Filter Firewall แต่จะมีความสามารถในการวิเคราะห์และรับรู้ความต่อเนื่องของแพ็กเก็ตในโปรโตคอลระดับสูงขึ้นไปได้มากกว่า

Circuit-Level Firewall เป็นเครื่องมือที่ถูกออกแบบมาเพื่อทำหน้าที่ในการควบคุมทราฟฟิคโดยเฉพาะ ไม่ได้เป็นการดัดแปลงการทำงานจากเราเตอร์ ทำให้มีความสามารถในการควบคุมทราฟฟิคการกำหนดแอคเซสรูล การบริหาร รวมไปถึงความยืดหยุ่นของการควบคุมทราฟฟิค และประสิทธิภาพในการทำงานที่สูงกว่า Packet Filter Firewall โดยทั่วไปถ้าหากกล่าวถึงไฟร์วอลล์จะหมายถึง Circuit-Level Firewall

ความแตกต่างที่สำคัญของ Packet Filter Firewall กับ Circuit-Level Firewall ในแง่ของการตรวจสอบทราฟฟิคคือ Circuit-Level Firewall มีความสามารถในการวิเคราะห์ทราฟฟิคที่ผ่านไปมาในโปรโตคอลที่เลเยอร์สูงขึ้นไปได้อย่างสมบูรณ์ต่างจาก Packet Filter Firewall ที่สามารถวิเคราะห์ได้เฉพาะข้อมูลในหนึ่งแพ็กเก็ตเท่านั้น เพราะบางครั้งทราฟฟิคที่ถูกส่งผ่านไปมานั้นมีการเชื่อมโยงกันหลายแพ็กเก็ต โดยเฉพาะ TCP ซึ่งมีลำดับการติดต่อสื่อสารที่สัมพันธ์กันในแต่ละแพ็กเก็ต การพิจารณาแพ็กเก็ตใดแพ็กเก็ตหนึ่งโดนไม่พิจารณาถึงความสัมพันธ์ที่มีกับแพ็กเก็ตอื่น จึงไม่สามารถควบคุมทราฟฟิคของ TCP ได้ ซึ่ง Circuit-Level Firewall มีความสามารถในการประกอบรวมแฟรกเมนต์เข้าด้วยกันให้เป็นดาต้าแกรมที่สมบูรณ์ หลังจากนั้นจึงนำดาต้าแกรมนั้นมาทำการตรวจสอบเปรียบเทียบกับแอคเซสรูล

นอกจากการเชื่อมโยงกันของแพ็กเก็ตในโปรโตคอล TCP ในทรานสปอร์ตเลเยอร์แล้ว ในบางแอพพลิเคชั่นเลเยอร์ก็มีแอพพลิเคชั่นบางชนิดที่ต้องอาศัยการพิจารณาทราฟฟิคอย่างต่อเนื่องเพื่อนำมากำหนดเป็นแอคเซสรูล เช่น การทำงานของ FTP ซึ่งในระหว่างการทำงานของ

แอพพลิเคชั่นนั้น โฮสที่เป็นไคลเอนต์จะสามารถกำหนดพอร์ตชั่วคราวขึ้นมาทำหน้าที่รับส่งไฟล์ได้ โดยพอร์ตเหล่านี้จะปิดลงเมื่อการรับส่งข้อมูลเสร็จ การเปิดพอร์ตชั่วคราวของ FTP ไคลเอนต์นั้น เป็นการเปิดบริการใหม่ขึ้นมาได้ ดังนั้น Circuit-Level Firewall จึงมีการทำงานที่ต้องใกล้ชิดกับแอพพลิเคชั่นอย่างมาก จะต้องสามารถเข้าใจลักษณะการติดต่อสื่อสารของแต่ละแอพพลิเคชั่นเป็นอย่างดี ซึ่งหากเป็นแอพพลิเคชั่นที่ใช้งานอย่างแพร่หลาย โดยส่วนใหญ่ผู้พัฒนาจะกำหนดวิธีการควบคุมทราฟฟิคมาให้ แต่ก็สามารถที่จะปรับแต่งให้ไฟร์วอลล์สามารถทำงานกับแอพพลิเคชั่นที่เป็นโปรโตคอลไม่ได้เป็นมาตราฐานได้

**ข้อดีของ Circuit-Level Firewall**

1. ใช้งานง่ายเพราะถูกออกแบบมาให้ทำหน้าที่เป็นไฟร์วอลล์โดยเฉพาะ ตรวจสอบแก้ไขแอคเซสรูลได้ง่าย ทำให้ไม่ต้องกังวลถึงคำสั่ง และรูปแบบการเข้าถึงคำสั่ง ถึงแม้จะต่างผู้ผลิตกันแต่ก็สามารถเรียนรู้การใช้งานได้อย่างรวดเร็ว

2. ประสิทธิภาพในการทำงานสูง เนื่องจากถูกออกแบบมาให้ทำหน้าที่ไฟร์วอลล์โดยเฉพาะ สามารถรองรับแอคเซสรูลที่ซับซ้อนได้ โดยไม่ทำให้ความสามารถในการทำงานต่ำลง

3. มีคุณสมบัติเพิ่มเติมให้ใช้นอกจากการควบคุมทราฟฟิค เช่น สามารถนำไปใช้ร่วมกับระบบตรวจจับการบุกรุก เพื่อปรับเปลี่ยนการทำงานเพื่อการป้องกันการโจมตีได้ในเวลาที่รวดเร็ว สามารถบันทึกข้อมูลเพื่อนำกลับมาวิเคราะห์ภายหลังได้ เป็นต้น

4. การกำหนดแอคเซสรูลทำได้ง่าย เพราะไฟร์วอลล์มีความเข้าใจในการทำงานของโปรโตคอลระดับสูง ดังนั้นผู้ใช้ไม่จำเป็นต้องมีความเชียวชาญในเรื่อเครือข่ายมากนัก ก็สามารถทำงานกับไฟร์วอลล์ได้ โดยจะกำหนดกฎบนพื้นฐานของแอพลิเคชั่นที่ผู้ใช้รู้จัก มากกว่าการกำหนดกฎโดยใช้ข้อมูลของแพ็กเก็ตโดยตรง

5. สามารถเพิ่มเติมบริการอื่นๆได้ เช่น Virtual Private Network, Tunneling

6. สามารถเพิ่มเติมความปลอดภัยโดยระบบการตรวจสอบผู้ใช้ (Authentication)

**ข้อเสียของ Circuit-Level Firewall**

1. มีราคาแพง

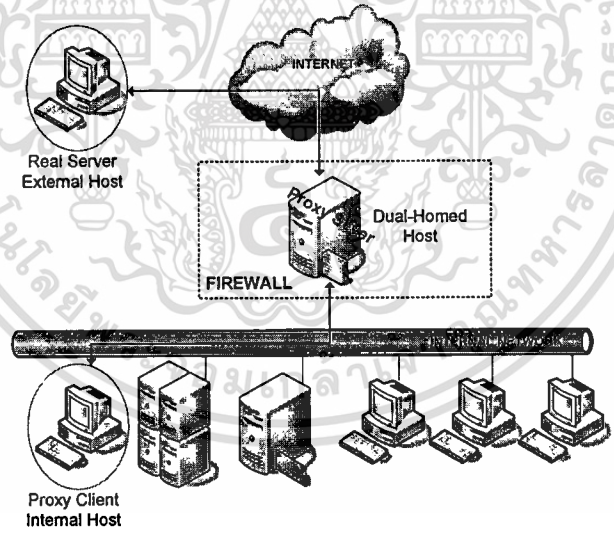
2. ในกรณีที่เป็นไฟร์วอลล์แบบซอฟต์แวร์ที่ทำงานอยู่บนระบบปฏิบัติการทั่วไป ก็มีความเสียงที่จะถูกเจาะได้ง่ายกว่าการเจาะเราเตอร์ เพราะช่องโหว่ในระบบปฏิบัติการมีมาก

3. ในกรณีไฟร์วอลล์เป็นประเภทที่ออกแบบทั้งซอฟต์แวร์และฮาร์ดแวร์เป็นเครื่องเดียวกัน (Network Appliance) เพื่อทำหน้าที่เป็นไฟร์วอลล์โดยเฉพาะ ผู้ใช้จำเป็นที่จะต้องพึ่งพาผู้ผลิตเป็นอย่างมาก หากเกิดปัญหาจะไม่สามารถแก้ไขโดยใช้อะไหล่ทดแทนจากที่อื่นได้

**2.2.3 Application Firewall หรือ Proxy**

พร็อกซี่เป็นเครื่องมือในการควบคุมทราฟฟิคชนิดหนึ่งซึ่งทำงานในระดับของแอพลิเคชั่นในลักษณะเป็นตัวกลางในการสื่อสารระหว่างไคลเอนต์กับเซิร์ฟเวอร์ โดยทำหน้าที่ป้องกันไม่ให้มีการสื่อสารกันโดยตรงระหว่างไคลเอนต์กับเซิร์ฟเวอร์ แต่ยังคงให้ไคลเอนต์สามารถใช้งานแอพพลิเคชั่นบนเซิร์ฟเวอร์ได้ตามปกติ และผู้ใช้ซึ่งใช้งานแอพลิเคชั่นจะไม่ได้รับผลกระทบแต่อย่างใด

โดยรูปแบบการทำงานของพร็อกซี่คือ เมื่อไคลเอนต์ต้องการใช้บริการภายนอก ไคลเอนต์จะทำการติดต่อไปยังพร็อกซี่ก่อน ไคลเอนต์จะเจรจา (Negotiate) กับพร็อกซี่เพื่อให้พร็อกซี่ติดต่อไปยังเครื่องปลายทางให้ เมื่อพร็อกซี่ติดต่อไปยังเครื่องปลายทางให้แล้วจะมีการเชื่อมต่อ (connection) 2 การเชื่อมต่อ คือ ไคลเอนต์กับพร็อกซี่และพร็อกซี่กับเครื่องปลายทาง โดยที่พร็อกซี่จะทำหน้าที่รับข้อมูลและส่งต่อข้อมูลให้ใน 2 ทิศทาง ทั้งนี้พร็อกซี่จะทำหน้าที่ในการตัดสินใจว่าจะให้มีการเชื่อมต่อกันหรือไม่ จะส่งต่อแพ็กเก็ตให้หรือไม่ โดยตัวอย่างการทำงานของ Application Firewall สามารถแสดได้ดังรูปที่ 2.3




**รูปที่ 2.3** ใช้ Dual-homed Host* เป็น Proxy Server

**ข้อดีของ Proxy**

1. สามารถควบคุมการติดต่อสื่อสารระหว่างอินเตอร์เน็ตกับเน็ตเวิร์กภายในให้อยู่ในระดับแอพพลิเคชั่นเท่านั้น ทำให้ตัดขาดการติดต่อโดยตรงในระดับเน็ตเวิร์กเลเยอร์ ทำให้ลดความเสียงต่อการถูกคุกคามจากการใช้เทคนิคระดับเน็ตเวิร์กเลเยอร์ที่จะเข้ามายังเน็ตเวิร์กภายใน

2. สามารถเพิ่มเติมหน้าที่การทำงานอื่นๆเขาไปยังพร็อกซี่ได้ เช่น เว็บพร็อกซี่นอกจากจะเป็นตัวกลางในการติดต่อสื่อสาร ยังสามารถควบคุมไม่ให้เว็บบราวเซอร์ติดต่อกับเว็บไซท์ที่ไม่เหมาะสมได้อีกด้วย

3. สามารถทำการแคชข้อมูลไว้ที่ตัวพร็อกซี่ สำหรับข้อมูลที่มีการเรียกซ้ำบ่อยๆก็ไม่จำเป็นที่จะต้องไปอ่านข้อมูลจากเซิร์ฟเวอร์ทุกครั้ง แต่ใช้ได้กับข้อมูลที่เป็นสแตติกเท่านั้น

4. ทำให้ผู้ใช้มีการใช้แบนวิดร่วมกันอย่างมีประสิทธิภาพ

5. สามารถเพิ่มเติมส่วนการติดต่อผู้ใช้เข้าเป็นหน้าที่หนึ่งของพร็อกซี่ โดยอนุญาตให้สามารถเข้าใช้งานพร็อกซี่นั้นจะขึ้นอยู่กับสิทธิที่ผู้ใช้มีอยู่ ทำให้สามารถควบคุมการเข้าใช้งานได้ดีกว่าการพิจารณาจาก IP Address เพียงอย่างเดียว

6. สามารถกรองเนื้อหาของข้อมูลได้ (Content Filtering) ทำให้สามารถนำมาเป็นเงื่อนไขอนุญาตให้ข้อมูลเหล่านั้นผ่านได้ เช่น เว็บพร็อกซี่สามารถตรวจสอบเนื้อหาของเว็บไซท์ หากมีข้อความไม่เหมาะสมพร็อกซี่ก็สามารถยกเลิกการเชื่อมต่อนั้นได้ หรือการตรวจสอบเนื้อหาในอีเมล์ หรืออาจครอบคลุมถึงการตรวจหาไวรัสในอีเมล์ได้อีกด้วย

**ข้อเสียของ Proxy**

1. การทำงานขึ้นอยู่กับแอพพลิเคชั่น ถ้าแอพพลิเคชั่นไม่รองรับการสื่อสารผ่านพร็อกซี่ก็ไม่สามารถใช้งานได้

2. เสียงต่อการถูกละเมิดความเป็นส่วนตัว เพราะข้อมูลต่างๆต้องถูกส่งผ่านพร็อกซี่ก่อนและพร็อกซี่มีความสามารถในการเก็บข้อมูลไว้ตรวจสอบ ซึ่งถ้านำข้อมูลเหล่านั้นไปวิเคราะห์ก็จะทำให้ทราบถึงข้อมูลต่างๆของผู้ใช้ได้

3. เนื่องจากลักษณะของแต่ละแอพพลิเคชั่นแตกต่างกัน ดังนั้นพร็อกซี่ของแต่ละแอพพลิเคชั่นจึงทำงานได้เพราะกับแอพพลิเคชั่นนั้นๆ ไม่สามารถทำงานรวมกันได้ในตัวเดียว หากมีการใช้งานแอพพลิเคชั่นหลายแอพพลิเคชั่นก็จะต้องมีพร็อกซี่จำนวนมากเพื่อให้บริการแอพพลิเคชั่นแต่ละตัว

4. ความสามารถในการประมวลผลของเครื่องที่ทำหน้าที่เป็นพร็อกซี่จะเป็นคอขวดได้ เพราะการสื่อสารของไคลเอนร์และเซิร์ฟเวอร์จะถูกรวมไว้ที่พร็อกซี่ ทำให้เกิดปัญหาคอขวดได้ถ้ามีไคลเอนร์หลายๆเครื่อง

## 2.3 การใช้งานแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ (Packet Filter Firewall: PF)

แพ็กเก็ตฟิลเตอร์ไฟร์วอลล์เป็นซอฟต์แวร์ที่ถูกพัฒนามาเพื่อกรองทราฟฟิคของโปรโตคอล TCP/IP รวมถึงการทำงานอื่นๆ เช่น Network Address Translation (NAT), Bandwidth control, packet prioritization โดยแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์เริ่มต้นจากการพัฒนาให้

ทำงานบนระบบปฏิบัติการณ์ OpenBSD ถูกปรับปรุงให้สามารถนำมาใช้บนระบบปฏิบัติการ FreeBSD ในปี 2003 โดยสามารถทำการติดตั้งผ่านพอร์ต และถูกบรรจุเข้าเป็นส่วนหนึ่งของระบบปฏิบัติการ FreeBSD ในเมือปี 2004 ตั้งแต่เวอร์ชั่น 5.3 เป็นต้นไป ซึ่งแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์เป็นไฟร์วอลล์แบบซอฟท์แวร์ตัวหนึ่งที่เหมาะกับการนำไปใช้งานเนื่องจากเป็นไฟร์วอลล์ที่มีความสมบูรณ์และมีฟังชั่นการทำงานของไฟร์วอลล์ที่ครบถ้วน อีกทั้งไม่ต้องเสียค่าใช้จ่ายในการจัดซื้ออีกด้วย

### 2.3.1 การเริ่มต้นการทำงานของแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์

การเรียกใช้งานแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์บนระบบปฏิบัติการ FreeBSD สามารถทำได้โดยการแก้ไขไฟล์ rc.conf ที่เก็บอยู่ที่ /etc/rc.conf โดยต้องเพิ่มคำสั่งเข้าไปในไฟล์ เพื่อให้ระบบปฏิบัติการ FreeBSD เริ่มต้นการทำงานของแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์เมื่อทำการเปิดระบบขึ้นมาใหม่ โดยเพิ่มคำสั่งดังนี้

**pf_enable="YES"**

โดยหลังจากที่เริ่มต้นการทำงานของแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์จากการเพิ่มคำสั่งด้านบน เราสามารถความคุมการใช้งานแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์โดยการป้อนคำสั่งดังนี้

**#pfctl –e**

เป็นคำสั่งที่ใช้ในการสั่งให้แพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ทำงาน (Enable)

**#pfctl –d**

เป็นคำสั่งที่ใช้ในการสั่งให้แพ็กเก็ตฟิลเตอร์ไฟร์วอลล์หยุดทำงาน (Disable)

### 2.3.2 การกำหนดกฎและคำสั่งต่างๆแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์

แพ็กเก็ตฟิลเตอร์ไฟร์วอลล์จะอ่านกฎและคำสั่งต่างๆจากไฟล์ตัวอักษร(Text) ที่ภายในไฟล์มีการกำหนดกกและคำสั่งต่างๆเอาไว้ โดยค่าเริ่มต้นที่โปรแกรมกำหนดไว้จะเป็นการอ่านไฟล์ pf.conf ซึ่งเก็บอยู่ที่ /etc/pf.conf ซึ่งสามารถเข้าไปแก้ไขคำสั่งและกฎต่างได้ และผู้ใช้สามารถกำหนดให้แพ็กเก็ตฟิลเตอร์ไฟร์วอลล์สามารถอ่านไฟล์คำสั่งและกฎอื่นๆได้ โดยการทำการอ่านหลังจากขั้นตอนการเริ่มต้นการทำงานจบไปแล้ว

ข้อมูลภายในไฟล์ที่เก็บกฎและคำสั่งต่างๆ สามารถแบ่งได้ 7 ส่วนคือ

Macros: เป็นตัวแปร (variable) ที่กำหนดโดยผู้ใช้ ซึ่งสามารถใช้เป็นตัวแปรในการเก็บค่าต่างๆเช่น IP Address, Interface name และข้อมูลอื่นๆ

Table: เป็นโครงสร้างข้อมูลที่ใช้ในการเก็บกลุ่มของ IP Address

Option: Option ต่างๆที่ใช้ในการควบคุมการทำงานของแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์

Scrub: สำหรับทำ Normalize และ Defragment แพ็กเก็ต

Queueing: สำหรับทำ Bandwidth Control และ Packet Prioritization

Translation: สำหรับควบคุม Network Address Translation และ Packet Redirection

Filter Rule: เป็นกฎสำหรับกรองแพ็กเก็ตที่จะส่งต่อออกไปที่ Interface ต่างๆ

นอกจากนั้นบรรทัดว่างต่างๆจะไม่ถูกนำไปประมวลผล และรวมถึงบรรทัดที่ขึ้นต้นด้วยเครื่องหมาย # ก็จะไม่ถูกนำไปประมวลผล เพราะจะเป็นส่วนของ comment

**2.3.3 การควบคุมการทำงานของแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์**

หลังจากที่แพ็กเก็ตฟิลเตอร์ไฟร์วอลล์เริ่มต้นทำงาน การควบคุมการทำงานต่างๆของไฟร์วอลล์สามารถทำได้โดยใช้โปรแกรม pfctl(8) ซึ่งจะทำหน้าที่ติดต่อกับแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ ซึ่งการใช้งานโปรแกรม pfctl จะใช้การเขียนคำสั่ง ตัวอย่างของการใช้คำสั่ง pfctl ในการควบคุมแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์เช่น

**# pfctl –f /etc/pf.conf**

**# pfctl –Rf /etc/pf.conf**

จากตัวอย่างจะเป็นคำสั่งให้แพ็กเก็ตฟิลเตอร์ไฟร์วอลล์อ่านกฎและคำสั่งต่างๆ จากไฟล์ที่กำหนด โดยในคำสั่งแรกจะเป็นการอ่านกฎและคำสั่งทั้งหมดจากไฟล์ pf.conf แต่ในคำสั่งที่สองจะแตกต่างจากคำสั่งแรกคือแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์จะอ่านข้อมูลที่เป็น Filter Rule เท่านั้นจะไม่อ่านข้อมูลอื่นๆ

**# pfctl –sn**

**# pfctl –sr**

**# pfctl –sa**

จากตัวอย่างเป็นคำสั่งให้แพ็กเก็ตฟิลเตอร์ไฟร์วอลล์แสดงข้อมูลต่างๆออกมา โดยคำสั่งแรกจะเป็นการให้แพ็กเก็ตฟิลเตอร์ไฟร์วอลล์แสดงข้อมูลของกฎที่เป็นกฎของ NAT เท่านั้น ส่วนคำสั่งที่สองจะเป็นการให้แพ็กเก็ตฟิลเตอร์ไฟร์วอลล์แสดงข้อมูลของกฎที่เป็น Filer Rule เท่านั้น ส่วนคำสั่งสุดท้ายจะเป็นการให้แพ็กเก็ตฟิลเตอร์ไฟร์วอลล์แสดงข้อมูลทุกอย่าง (All) ที่สามารถแสดงได้

### 2.3.4 รูปแบบในการสร้างกฎและคำสั่งของแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์

**List**

List สามารถใช้ในการระบุถึงกลุ่มของข้อมูลที่ต้องการอ้างถึง ซึ่งเป็นข้อมูลชนิดเดียวกัน เช่น IP Address, Port number หรือ Protocol ต่างๆ ซึ่งแทนที่จะต้องเขียนกฎหนึ่งข้อต่อการระบุถึงข้อมูล IP Address หนึ่งค่าที่ต้องการจะ Block แต่สามารถใช้กฎเพียงข้อเดียวในการระบุถึง IP Address ทั้งหมดที่ต้องการ Block โดยในการสร้าง List ของกลุ่มข้อมูลจะอยู่ภายในเครื่องหมาย {}

เมื่อโปรแกรม pfctl(8) ทำการอ่านข้อมูลและประมวลผลมาพบกับ List ก็จะสร้างกฎให้กับแต่ละข้อมูลที่อยู่ภายใน List เช่น

**block out on fxp0 from {192.168.0.1, 10.5.32.1} to any**

จากกฎดังกล่าวเมื่อ pfctl อ่านข้อมูลมาพบจะทำให้เกิดการสร้างกฎขึ้นใหม่สองกฎคือ

**block out on fxp0 from 192.168.0.1 to any**

**block out on fxp0 from10.5.32.1 to any**

การใช้งาน List สามารถนำไปใช้ได้กับกฎอื่นๆ ไม่ได้จำกัดแค่เพียง Filter Rule เท่านั้น

**Macros**

Macros เป็นการสร้างตัวแปร (Variable) เพื่อใช้ในการเก็บข้อมูล เช่น IP Address, Port number และ Interface name เป็นต้น โดย Macros สามารถช่วยลดความซับซ้อนของกลุ่มกฎที่มีอยู่ และทำให้การดูแลรักษากลุ่มของกฎทำได้ง่ายขึ้น

ชื่อของ Macros จะต้องขึ้นต้นด้วยตัวอักษรและหลังจากนั้นอาจประกอบไปด้วยตัวอักษรหรือตัวเลขก็ได้ โดยชื่อที่ตั้งต้องไม่ซ้ำกับคำที่สงวนไว้ภายในโปรแกรม เช่น pass, out หรือ queue

```
ext_if = "fxp0"
block in on $ext_if from any to any
```

จากตัวอย่างคำสั่งบรรทัดแรกเป็นการสร้าง Macros ชื่อว่า ext_if ซึ่งเก็บค่า Interface name และในบรรทัดที่สองจะเป็นตัวอย่างการเรียกใช้ Macros ที่สร้างขึ้น โดยการอ้างถึง Macros จะต้องมีเครื่องหมาย $ นำหน้าเสมอ

**Table**

Table ใช้สำหรับบรรจุกลุ่มของ IP Address ซึ่งการทำงานจะมีความเร็วมากกว่าและใช้หน่วยความจำกับการประมวลผลที่น้อยกว่าการใช้ List โดย Table ถูกออกแบบมาให้เหมาะสมกับกลุ่มข้อมูล IP Address ที่มีขนาดใหญ่ ซึ่งการใช้เวลาในการเข้าถึงข้อมูลใน Table ที่มี IP

Address บรรจุอยู่ 50000 Address จะมีเวลาแตกต่างกันเล็กน้อยกับการเข้าถึง Table ที่มีข้อมูล IP Address เก็บอยู่ 50 Address

Table สามารถสร้างได้สองช่องทางคือสร้างไว้ในไฟล์ pf.conf โดยการเขียนคำสั่งลงในไฟล์ ซึ่งใช้คำสั่ง table ในการสร้างตัวอย่างของการเขียนคำสั่ง เช่น

table <goodguy > {192.168.1.0/24}

table <goodguy > {192.168.1.0/24, !192.168.1.1}

table <goodguy> file "/etc/goodguy"

จากตัวอย่างคำสั่งแรกเป็นการสร้าง Table ชื่อว่า goodguy โดยเก็บกลุ่มของ IP Address 192.168.1.0/24 ส่วนในคำสั่งที่สองคล้ายกับคำสั่งแรกแต่จะแตกต่างที่มีการระบุถึง IP Address ที่ต้องการตัดออกจากกลุ่มนั้นคือ IP Address 192.168.1.1 และในส่วนของคำสั่งสุดท้ายจะเป็นการอ่านกลุ่มของ IP Address จากไฟล์เข้ามาแทน โดยจากตัวอย่างจะอ่านข้อมูลจากไฟล์ goodguy ซึ่งอยู่ใน /etc/goodguy

อีกวิธีการหนึ่งในการสร้าง Table คือการสร้างผ่านทางโปรแกรม pfctl(8) โดยมีรูปแบบการสร้าง Table ดังตัวอย่าง

# pfctl –t goodguy –T add 192.168.1.0/24

# pfctl –t goodguy –T show

# pfctl –t goodguy –T delete 192.168.1.0/24

จากตัวอย่างเป็นการสร้าง Table ชื่อว่า goodguy โดยเก็บค่ากลุ่ม IP Address คือ 192.168.1.0/24 ส่วนในคำสั่งที่สองจะเป็นการเรียกดูข้อมูลของกลุ่ม IP Address ที่ถูกเก็บไว้ใน Table ชื่อ goodguy และในคำสั่งสุดท้ายจะเป็นการลบ IP Address 192.168.1.0/24 ที่เก็บใน Table ชื่อ goodguy

**Packet Filter Rule**

Packet Filter เลือกที่จะส่ง (pass) ผ่านแพ็กเก็ตหรือปิดกั้น (block) ไม่ให้แพ็กเก็ตนั้นผ่านไป โดยตรวจดูแพ็กเก็ตบนพื้นฐานของข้อมูลในเลเยอร์ 3(IPv4 และ IPv6) และเลเยอร์ 4 (TCP, UTP, ICMP และ ICMPv6) ซึ่งส่วนใหญ่จะเป็นการพิจารณาจาก IP Address ต้นทางและ IP Address ปลายทาง Port ต้นทางและ Port ปลายทาง หรือโปรโตคอล เป็นหลัก

Filter Rule จะระบุถึงลักษณะของแพ็กเก็ตจะต้องตรงกับเกณฑ์ที่ตั้งไว้และการกระทำที่จะเกิดขึ้นเมื่อพบแพ็กเก็ตที่ตรงกับเกณฑ์ที่ตั้งไว้ คือการ block หรือ pass โดย Filter Rule จะประเมินแพ็กเก็ตกับกฎตามลำดับของกฎที่เขียนไว้จากกฎข้อแรกไปยังกฎข้อสุดท้าย ซึ่งกฎที่ตรง

กับแพ็กเก็ตตัวล่าสุดจะเป็นกฎที่ถูกนำไปตัดสินใจในการที่จะ block หรือ pass แพ็กเก็ต นั้นก็คือ ถ้าเรากำหนดกฎให้ทำการส่งข้อมูลทุกแพ็กเก็ตที่เข้ามา (pass all) ไว้เป็น Filter Rule ข้อแรกจะหมายความว่าถ้าแพ็กเก็ตที่เข้ามายังไฟร์วอลล์ไม่ตรงกับเกณฑ์อื่นๆที่ตั้งไว้เลย ไฟร์วอลล์ก็จะทำการส่งแพ็กเก็ตนั้นต่อไป

**Rule Syntax**

โดยทั่วไปแล้วรูปแบบของ Filter Rule จะประกอบไปด้วยรายละเอียดดังต่อไปนี้

```
action [direction] [log] [quick] [on interface] [af] [proto protocol] \
   [from src_addr [port src_port]] [to dst_addr [port dst_port]] \
   [flags tcp_flags] [state]
```

**action**

เป็นการกำหนดการทำงานที่จะเกิดขึ้นเมื่อพบแพ็กเก็ตที่ตรงกับเกณฑ์ของ Filter Rule ตั้งไว้นั้นคือการ block หรือ pass โดยในส่วนของการ pass ก็จะทำการส่งแพ็กเก็ตออกไปตามปกติ แต่ในส่วนของ block จะมีการตอบสนองที่ขึ้นอยู่กับ block-policy option ซึ่งโดยปกติจะมีค่าเป็น block drop หรือ block return

**direction**

เป็นทิศทางของแพ็กเก็ตบน Interface ซึ่งประกอบไปด้วย in หรือ out

**log**

เป็นการกำหนดให้เก็บ Log ของแพ็กเก็ต

**quick**

ถ้าแพ็กเก็ตใดตรงกับ Filter Rule ที่กำหนด quick ไว้ จะถือว่ากฎข้อนั้นเป็น Filter Rule สุดท้ายที่ตรงทับเล็กเก็ต และจะทำงานตามการทำงานที่กำหนดไว้ใน Filter Rule นั้น

**on interface**

ชื่อหรือกลุ่มของ Network Interface ที่แพ็กเก็ตส่งผ่าน

**af**

กำหนดถึง IP Address version ที่แพ็กเก็ตใช้งานอยู่ โดยมีค่าเป็น inet เมื่อแพ็กเก็ตใช้ IP Address version 4 และเป็น inet6 เมื่อแพ็กเก็ตใช้ IP Address version 6 แต่ตามปกติแล้วแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ สามารถที่จะตัดสินใจได้เองจากข้อมูล IP Address ว่าเป็น IP Address version ไหน ทำให้ค่าในส่วนนี้อาจไม่จำเป็นต้องกำหนด

**protocol**

เป็นการระบุถึงโปรโตคอลที่ใช้ในเลเยอร์ 4 เช่น TCP, UTP เป็นต้น หรืออาจระบุโดยใช้ Protocol number ซึ่งมีค่าอยู่ระหว่าง 0-255 ลงไปก็ได้ และสามารถใช้ List ในการเก็บข้อมูลของกลุ่มโปรโตคอลได้อีกด้วย

**src_addr, det_addr**

เป็นการระบุถึง IP address ของต้นทางและ IP Address ของปลายทางที่อยู่ในแพ็กเก็ต โดยสามารถกำหนดได้หลายรูปแบบ เช่น

- กำหนดโดยการใส่ IP Address ลงไปโดยตรง
- กำหนดเป็น CIDR Network Block
- กำหนดโดยใช้ชื่อของ Network Interface
- ใช้การสร้าง Table หรือ List เข้ามาช่วยในการเก็บข้อมูล
- การระบุค่าเป็น any จะหมายถึงทุกๆ IP Address
- การระบุค่าเป็น all จะเป็นการเขียนแทนคำสั่ง any to any

**src_port, det_port**

เป็นการระบุถึง Port ต้นทางและ Port ปลายทางของโปรโตคอลที่ใช้ในการสื่อสารในเลเยอร์ 4 โดยสามารถระบุได้หลายรูปแบบ เช่น

- กำหนดเป็นตัวเลขของ Port number ซึ่งมีค่าระหว่าง 1 - 65535
- กำหนดโดยใช้ชื่อของบริการ
- ใช้การสร้าง List เพื่อเก็บกลุ่มของ Port number
- สามารถใช้เครื่องหมายเพื่อกำหนดช่วงของ Port number เช่น

  != ไม่เท่ากับ

  < น้อยกว่า

  <= น้อยกว่าหรือเท่ากับ

**tcp_flags**

ระบุถึง flags ที่จะต้องถูก set ใน TCP header เมื่อทำการระบุโปรโตคอลเป็น TCP

**state**

กำหนดให้ระบบติดตาม state ของแพ็กเก็ตที่ตรงกับ Filter Rule ที่กำหนด โดยมีการทำงาน 3 แบบ คือ

- keep state
- modulate state
- synproxy state

**2.3.4 ตัวอย่างการกำหนดกฎให้กับแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์**

ตัวอย่างการกำหนดค่าให้กับ Marco เพื่อลดความซ้ำซ้อนในการนำไปใช้งาน โดยสามารถกำหนดให้กับค่าของ Interface name หรือค่าของ IP Address ดังตัวอย่าง

```
ext_if = "fxp0"
int_if = "dc0"
lan_net = "192.168.0.0/24"
```

ตัวอย่างการสร้าง Table ชื่อ firewall เพื่อใช้ในการเก็บค่า IP Address หรือ Network number ที่ต้องใช้ในการระบุในการสร้างกฎ

```
table <firewall> const { self }
```

ตัวอย่างการกำหนดให้แพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ไม่ต้องตรวจจับข้อมูลที่ Loopback Interface (lo0)

```
set skip on lo0
```

ตัวอย่างการกำหนดค่า default deny policy ให้กับแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์

```
block all
```

ตัวอย่างการกำหนดค่าการป้องกัน spoofing ที่ Interface

```
antispoof quick for $int_if inet
```

ตัวอย่างการตั้งกฎโดยมีเงื่อนไขยอมให้การเชื่อมต่อที่ใช้พอร์ต ssh จากเครือข่ายภายในโดยต้องมีหมายเลข IP Address 192.168.0.15 เท่านั้นที่สามารถผ่านไปได้ แต่ถ้าไม่ตรงตามเงื่อนไขจะทำการ block และส่ง TCP RST แพ็กเก็ตกลับไปยังต้นทาง

```
block return in quick on $int_if proto tcp from ! 192.168.0.15 to $int_if port ssh /
flags S/SA
```

การกำหนดกฎให้ข้อมูลที่ส่งมาจากเครือข่ายภายนอกเข้ามาจากยัง Interface ของเครือข่ายภายในสามารถผ่านเข้ามาได้ และให้ข้อมูลที่ส่งจากเครือข่ายภายในไปยัง Interface ของเครือข่ายภายในสามารถส่งออกไปได้

**pass in on $int_if from $lan_net to any**

**pass out on $int_if from any to $lan_net**

กำหนดให้ Interface ที่เชื่อมต่อเครือข่ายภายนอกยอมให้ส่งข้อมูลออกไปได้ และทำการเก็บสถานะการเชื่อมต่อ (state) ของโปรโตคอล TCP ,UDP และ ICMP

**pass out on $ext_if proto tcp all modulate state flags S/SA**

**pass out on $ext_if proto { udp, icmp } all keep state**

เนื่องจากไฟร์วอลล์มีหน้าที่หลักในการกรอง (filter) ข้อมูลเฉพาะส่วนที่ได้รับอนุญาตเท่านั้น ดังนั้นการเขียนกฎสำหรับไฟร์วอลล์จึงเป็นเรื่องที่สำคัญอย่างยิ่ง การสร้างกฎของไฟร์วอลล์ที่ผิดพลาดจะทำให้ไฟร์วอลล์ ทั้งหลายไม่สามารถช่วยป้องกันเครือข่ายให้รอดพ้นจากการถูกบุกรุกหรือโจมตีได้อย่างแน่นอน

โดยหลักการในการสร้างกฎสำหรับไฟร์วอลล์ที่ดีคือ ความง่าย (Simplicity) ซึ่งความง่ายในที่นี้หมายถึงการสร้างกฎที่สั้นๆ อ่านง่าย ได้ใจความ ไฟร์วอลล์ที่ดีไม่ควรมีกฎมากกว่า 30 กฎ เพราะถ้ามากกว่านี้จะทำให้เกิดความสับสนได้ง่าย และอาจจะทำให้เกิดความผิดพลาดขึ้นได้ โดยง่ายนอกจาก นี้ยังมีข้อดีในส่วนที่ทำให้เครื่องทำงานน้อยลงอีกด้วย ซึ่งการสร้างกฎของไฟร์วอลล์ถือได้ว่าเป็นการนำนโยบายด้านความปลอดภัย ขององค์กรมาบังคับใช้งานในทางเทคนิค โดยใช้ไฟร์วอลล์เป็นเครื่องมือให้เกิดผลตามที่ต้องการ นอกจากนี้ยังมี กฎบางส่วนที่ถือได้ว่าผู้ดูแลระบบควรเพิ่มเข้าไปในกฎของไฟร์วอลล์เช่น การป้องกัน ip spoofing, การป้องกันการโจมตีแบบ land attack เป็นต้น

# บทที่ 3
# วิเคราะห์และออกแบบระบบ

## 3.1 ความต้องการของระบบ

จากการศึกษาแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์แล้ว จึงนำมาวิเคราะห์ความต้องการออกเป็นข้อๆ เพื่อนำไปออกแบบแผนภาพต่างๆ ด้วย UML ด้วยรูปแบบที่เป็นเชิงวัตถุทำให้การออกแบบต่างๆ สามารถนำกลับมาใช้งานใหม่ได้ หรือปรับเปลี่ยนการทำงานของระบบในส่วนต่างๆ โดยไม่มีผลกระทบกับส่วนการออกแบบอื่นๆ ทำให้สะดวกในการพัฒนาระบบและปรับเปลี่ยนระบบในอนาคต ซึ่งรายการความต้องการของระบบใหม่สามารถสรุปได้หลักๆ ดังต่อไปนี้

**Functional Requirement**

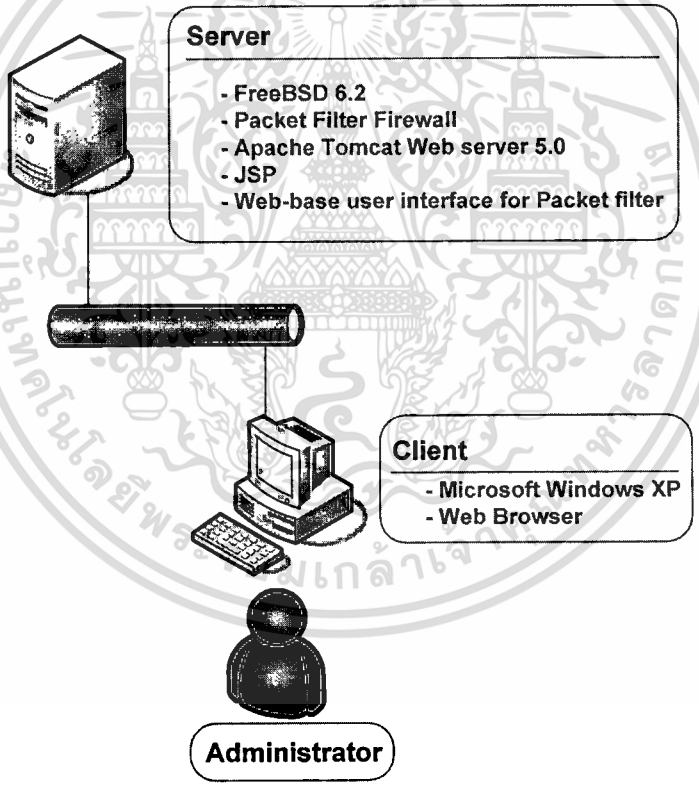
1. สามารถรองรับการทำงานผ่านทางหน้าเว็บ(Web-Base Interface)
2. สามารถป้อนข้อมูลที่จำเป็นสำหรับการสร้างกฎของไฟร์วอลล์ ซึ่งระบุได้ถึง IP Source, Port Source, IP Destination, Port Destination, Protocol, Direction, Interface, TCP flags และ State ผ่านทางหน้าจอเว็บที่สร้างขึ้น
3. สามารถเพิ่ม แก้ไข หรือลบกฎที่ทำการสร้างขึ้นได้ โดยการเปลี่ยนแปลงกฎจะมีผลต่อการทำงานของแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์
4. สามารถจัดเรียงลำดับของกฎใหม่ได้
5. สามารถกำหนดสถานะในการทำงานของกฎ คือ ใช้งานกฎ(Enable)หรือยกเลิกการใช้งาน(Disable) และสามารถปรับเปลี่ยนตำแหน่ง(Move)ของกฎเพื่อให้ได้ลำดับการทำงานตามที่ต้องการ
6. สามารถแสดงรายการของกฎที่สร้างขึ้นใหม่และกฎที่มีอยู่เดิมได้
7. สามารถรองรับทำงานแบบ Wizard เพื่อช่วยกำหนดกฎและลักษณะการทำงานเบื้องต้นของไฟร์วอลล์ได้
8. สามารถบันทึกข้อมูลกฎที่สร้างขึ้นลงในไฟล์และเรียกกฎที่สร้างขึ้นมาทำงานได้
9. สามารถคัดลอกกฎที่ใช้งานอยู่ออกมาในรูปแบบไฟล์ได้ เพื่อทำการสำรองกฎต่างๆ ไว้
10. สามารถอ่านข้อมูลจากไฟล์ที่ถูกสำรองไว้จากระบบเข้าสู่ระบบได้

## 3.2 ระบบใช้งานแพ็กเก็ตฟิลเตอร์ในปัจจุบัน

แพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ที่เป็นไฟร์วอลล์ที่อยู่ในระบบปฏิบัติการ FreeBSD ซึ่งมีการใช้งานไฟร์วอลล์ในลักษณะการกำหนดคำสั่งแบบ command line จึงทำให้เกิดความยุ่งยากในการสร้างกฎสำหรับควบคุมการทำงานต่างๆ และนอกจากนั่นในการทำงานกับแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ผู้ใช้งานจะต้องมีความรู้และเข้าใจในรูปแบบของกฎ (Filter Rule) ทำให้สร้างความลำบากให้กับผู้ใช้งานที่ไม่มีความชำนาญและไม่เคยทำงานกับแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์มาก่อน อีกทั้งผู้ใช้งานบางส่วนอาจไม่คุ้นเคยกับการใช้งานบนระบบปฏิบัติการ FreeBSD ก็จะทำให้การใช้งานยิ่งมีความยากลำบากมากขึ้น

**ภาพรวมของระบบงาน (System Architecture)**

ระบบงานประกอบด้วยองค์ประกอบต่างๆ ดังต่อไปนี้




**รูปที่ 3.1** แสดงภาพรวมของระบบงาน (System Architecture)

**เครื่องคอมพิวเตอร์เซิร์ฟเวอร์**

ติดตั้งระบบปฏิบัติการ FreeBSD และโปรแกรมแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ เพื่อทำหน้าที่ตรวจสอบข้อมูลที่ผ่านเข้าออก ซึ่งได้รับการเตรียมความพร้อมดังนี้

- ติดตั้งระบบปฏิบัติการ FreeBSD version 6.2 เพื่อรองรับการตรวจสอบข้อมูลที่ผ่านเข้าออก
- ติดตั้งซอฟต์แวร์ไฟร์วอลล์ โดยเลือกใช้ โปรแกรมแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์
- ติดตั้งส่วนให้บริการเว็บเซิร์ฟเวอร์สำหรับเป็นส่วนติดต่อกับผู้ใช้เพื่อใช้ในการควบคุมระบบ โดยเลือกใช้ Apache Tomcat เวอร์ชัน 5.0
- ติดตั้งซอฟต์แวร์ภาษา โดยเลือกใช้ JSP
- ติดตั้งระบบการใช้งานแพ็กเก็ตฟิลเตอร์สำหรับผู้ใช้แบบเว็บ

**เครื่องคอมพิวเตอร์ไคลเอ็นท์**

ที่ใช้ควบคุมระบบการกำหนดกฎไฟร์วอลล์โดยผ่านทางเว็บ ซึ่งได้รับการเตรียมความพร้อมดังนี้

- ติดตั้งระบบปฏิบัติการ Microsoft Windows XP
- ติดตั้งโปรแกรมเว็บบราวเซอร์ เช่น Internet Explorer, Fire Fox สำหรับติดต่อกับเว็บเซิร์ฟเวอร์ เพื่อควบคุมโปรแกรมการกำหนดกฎไฟร์วอลล์

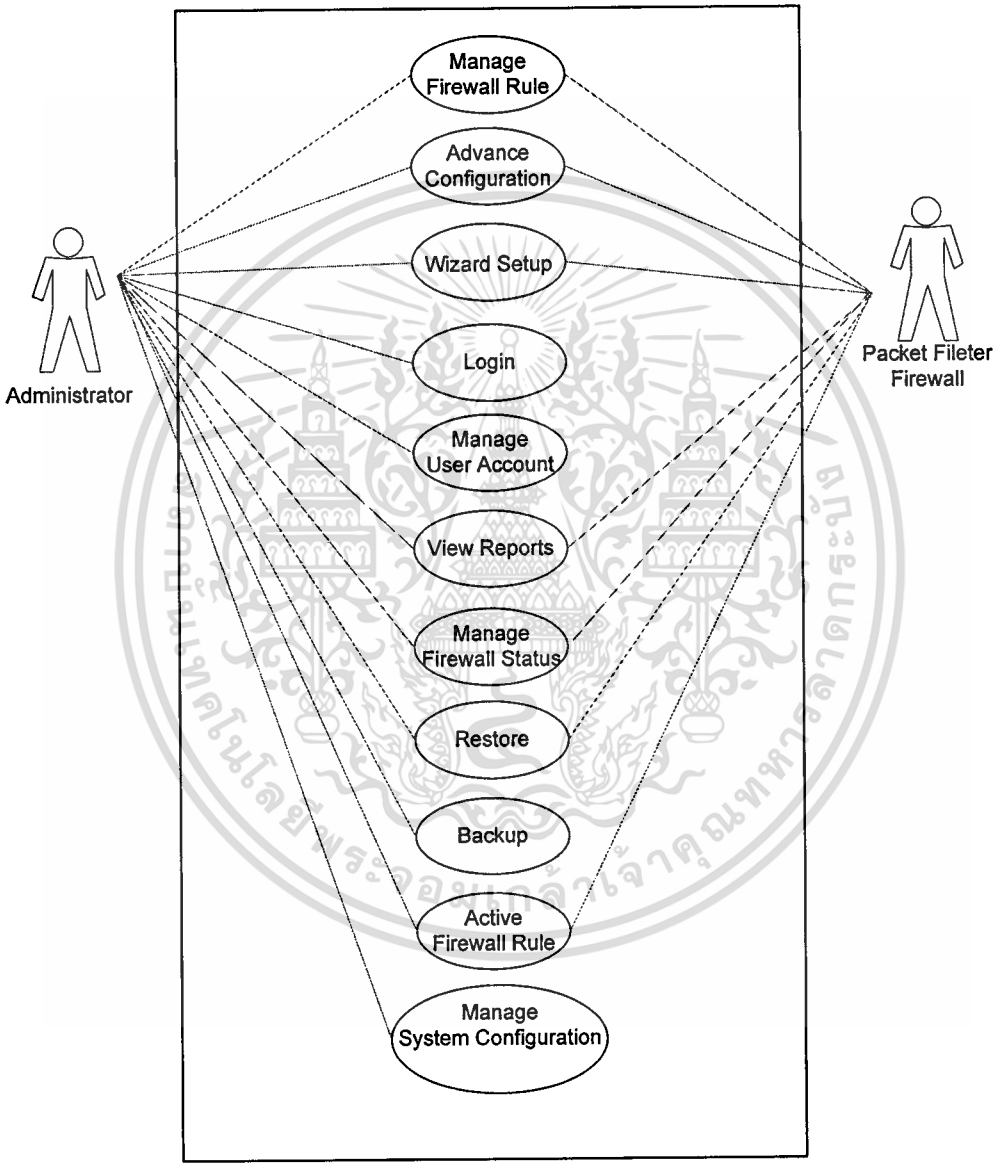
**ผู้ดูแลระบบ**

ทำหน้าที่ในการจัดการและดูแลการทำงานของแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ โดยทำงานผ่านทางระบบการใช้งานแพ็กเก็ตฟิลเตอร์สำหรับผู้ใช้แบบเว็บ ซึ่งจะเรียกใช้งานผ่านทางโปรแกรม Browser ของเครื่องคอมพิวเตอร์ไคลเอ็นท์

## 3.3 แบบจำลองเชิงแนวคิดของระบบ (Conceptual Models)

การวิเคราะห์ระบบการกำหนดกฎแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ วิเคราะห์โดยอาศัย OMG-Unified Modeling Language (UML) ซึ่งมีแบบจำลองเชิงแนวคิดของระบบ

### 3.3.1 การออกแบบแผนภาพยูสเคส (Use Case Model ) ใช้ในการอธิบายระบบงานทั้งหมด




**รูปที่ 3.2** แสดง Use Case Diagram ระบบใช้งานแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์สำหรับผู้ใช้แบบเว็บ

**USE CASE DESCRIPTION**

จากการออกแบบแผนภาพยูสเคสสามารถนำมาอธิบายขั้นตอนการปฏิบัติงานหรือขั้นตอนการติดต่อกับระบบในแต่ละงานได้โดยใช้แผนภาพลำดับ ซึ่งในแผนภาพลำดับนี้สามารถอธิบายการทำงานเป็นขั้นตอนเพิ่มเติมด้วยการใช้คำอธิบายยูสเคส (Use Case Description) ได้ดังต่อไปนี้

**Use Case:** Manage Firewall Rule

**Brief Description:** การจัดการกับกฎต่างๆที่จะใช้ในการทำงานของแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์

**Actor:** Administrator

**Precondition:** ผู้ใช้งานจะต้องทำการ Login เข้าสู่ระบบและได้รับสิทธิ์การใช้งานเป็น Admin

**Basic Flows:**

1. Administrator เปิดหน้าเว็บและเข้าสู่หน้าจอส่วนของการจัดการกฎต่างๆ เพื่อทำการจัดการกับกฎภายในแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ ซึ่งสามารถแยกกฎออกเป็น Runtime Options, Table, Antispoof rule และ Filter Rule โดยผู้ใช้งานสามารถเพิ่ม ลบ และแก้ไขกฎต่างๆได้
2. ตรวจสอบกฎมีความว่าถูกต้อง
3. ทำการเพิ่มกฎและบันทึกกฎที่เพิ่มเข้าสู่ระบบ
4. ระบบแจ้งผลการจัดการ

**Alternative Flow:**

2a. หากกฎไม่ถูกต้อง ระบบจะแสดงข้อความผิดพลาดขึ้นและไม่ทำการบันทึกผล

**Postcondition:**

1. กฎจะถูกบันทึกไว้ในระบบเพื่อรอการ Activate การทำงานจึงจะเกิดการทำงานตามกฎที่ได้สร้าง

**Use Case:** Advance Configuration

**Brief Description:** การแก้ไขไฟล์ที่ก็ข้อมูลกฎของแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ โดยการพิมพ์รูปประโยคของกฎเอง

**Actor:** Administrator

**Precondition:** ผู้ใช้งานจะต้องทำการ Login เข้าสู่ระบบและได้รับสิทธิ์การใช้งานเป็น Admin

**Basic Flows:**

1. Administrator เปิดหน้าเว็บและเข้าสู่หน้าจอส่วนของการจัดการกฎในระดับสูง
2. Administrator ทำการแก้ไขข้อมูลในไฟล์ โดยการพิมพ์รูปประโยคของกฎด้วยตัวเอง
3. ระบบทำการตรวจสอบกฎภายในไฟล์ที่ได้รับการแก้ไข

4. ทำบันทึกการแก้ไขเข้าสู่ระบบ
5. ระบบแจ้งผลการแก้ไขกฎ

**Alternative Flow:**

3a. ระบบทำการตรวจสอบแล้วถ้าพบความผิดของกฎจะรายงานผลออกทางหน้าจอ

**Postcondition:**

1. กฎที่แก้ไขจะถูกบันทึกไว้ในระบบเพื่อรอการ Activate การทำงานจึงจะเกิดการทำงาน

**Use Case:** Wizard Setup

**Brief Description:** การสร้างกฎจากการกำหนดค่าของผู้ใช้ให้กับแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์

**Actor:** Administrator

**Precondition:** ผู้ใช้งานจะต้องทำการ Login เข้าสู่ระบบและได้รับสิทธิ์การใช้งานเป็น Admin

**Basic Flows:**

1. Administrator เปิดหน้าเว็บและเข้าสู่หน้าจอเริ่มต้นการสร้างกฎและกำหนดการทำงานแบบ Wizard
2. เลือกคุณลักษณะการทำงานของแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ โดยระบบจะมีคุณสมบัติต่างๆให้ผู้ใช้เลือกตามความต้องการ
3. ทำการสร้างกฎจากข้อมูลคุณสมบัติที่ผู้ใช้เลือก
4. ทำการบันทึกกฎที่ได้
5. ระบบแจ้งผลของกฎที่ถูกสร้างขึ้น

**Alternative Flow: -**

**Postcondition:**

1. กฎที่สร้างจะถูกบันทึกไว้ในระบบเพื่อรอการ Activate การทำงานจึงจะเกิดการทำงาน

**Use Case:** Login

**Brief Description:** ทำการตรวจสอบ Username ว่ามีอยู่ในระบบหรือไม่ และ Password ถูกต้องหรือไม่

**Actor:** Administrator

**Precondition:** ผู้ใช้งานจะต้องได้รับการเพิ่มชื่อให้เป็นผู้ใช้งานระบบและได้รับสิทธิ์การใช้เป็น Admin

**Basic Flows:**

1. Administrator เปิดหน้าเว็บขึ้นเพื่อทำการ Login เพื่อเข้าใช้งานระบบ
2. ทำการป้อน Username และ Password ของผู้จะเข้าใช้ระบบ

3. ระบบทำการตรวจสอบความถูกต้องของข้อมูล
4. ข้อมูลถูกต้องทำการเข้าใช้งานส่วนต่างๆของระบบได้

**Alternative Flow:**

3a. ระบบทำการตรวจสอบแล้วหากไม่พบข้อมูลจะทำการแสดงข้อความผิดพลาดขึ้นและกลับเข้าสู่การ Login ใหม่อีกครั้ง

**Postcondition: -**

**Use Case:** Manage User Account

**Brief Description:** ทำการแก้ไข Username และ Password รวมถึงรายละเอียดเกี่ยวกับผู้ใช้

**Actor:** Administrator

**Precondition:** ผู้ใช้งานจะต้องทำการ Login เข้าสู่ระบบและได้รับสิทธิ์การใช้งานเป็น Admin

**Basic Flows:**

1. Administrator เปิดหน้าเว็บขึ้นเพื่อทำการจัดการแก้ไขกับข้อมูลรายละเอียดเกี่ยวกับ Username และ Password
2. Person ทำการบันทึกข้อมูลเข้าสู่ระบบ

**Alternative Flow: -**

**Postcondition: -**

**Use Case:** Manage Firewall Status

**Brief Description:** จะทำการกำหนดสถานะของแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์

**Actor:** Administrator

**Precondition:** ผู้ใช้งานจะต้องทำการ Login เข้าสู่ระบบและได้รับสิทธิ์การใช้งานเป็น Admin

**Basic Flows:**

1. Administrator เปิดหน้าเว็บและเข้าสู่หน้าจอส่วนของการจัดการกับสถานะของแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์
2. เลือกสถานะที่ต้องการกำหนด
3. ทำการ Active สถานะที่เลือก
4. ทำการกำหนดสถานะให้กับระบบ
5. ระบบแจ้งผลการกำหนดสถานะ

**Alternative Flow:**

4a. หากกฎที่ทำการสร้างไม่ถูกต้อง ระบบจะแสดงข้อความผิดพลาดขึ้นและไม่ทำการบันทึกผล

**Postcondition:**

1. กฎที่ทำการแก้จะถูกบันทึกไว้ในระบบเพื่อรอการ Activate การทำงานจึงจะเกิดการทำงาน

**Use Case:** View Reports

**Brief Description:** จะทำการเรียกดูรายงานของระบบ

**Actor:** Administrator

**Precondition:** ผู้ใช้งานจะต้องทำการ Login เข้าสู่ระบบและได้รับสิทธิ์การใช้งานเป็น Admin

**Basic Flows:**

1. Administrator เปิดหน้าเว็บขึ้นเพื่อเลือกดูรายงาน
2. เลือกรายงานที่ต้องการ
3. ระบบสร้างรายงานและแสดงผลให้กับผู้ใช้

**Alternative Flow:** -

**Postcondition:** -

**Use Case:** Backup

**Brief Description:** จะทำการบันทึกกฎของแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์

**Actor:** Administrator

**Precondition:** ผู้ใช้งานจะต้องทำการ Login เข้าสู่ระบบและได้รับสิทธิ์การใช้งานเป็น Admin

**Basic Flows:**

1. Administrator เปิดหน้าเว็บขึ้นเพื่อทำการเลือกการทำงานในส่วนของ Backup
2. ตั้งชื่อและรายละเอียดของไฟล์
3. ระบบแสดงหน้าจอยืนยันเก็บข้อมูล
4. ระบบทำการบันทึกข้อมูลลงไฟล์

**Alternative Flow:**

4a. หากระบบไม่สามารถบันทึกข้อมูลลงได้จะแสดงข้อความผิดพลาดขึ้น

**Postcondition:** -

**Use Case:** Restore

**Brief Description:** จะทำการอ่านไฟล์กฎของแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ที่ได้บันทึกไว้ มาใช้งาน

**Actor:** Administrator

**Precondition:** ผู้ใช้งานจะต้องทำการ Login เข้าสู่ระบบและได้รับสิทธิ์การใช้งานเป็น Admin

**Basic Flows:**

1. Administrator เปิดหน้าเว็บขึ้นเพื่อทำการเลือกการทำงานในส่วน Restore

2. เลือกไฟล์ที่ได้ทำการบันทึกไว้
3. ระบบทำการอ่านไฟล์และนำข้อมูลเข้าสู่แพ็กเก็ตฟิลเตอร์ไฟร์วอลล์
4. ระบบทำการบันทึกกฎใหม่ลงแทนที่ข้อมูลในไฟล์ที่ใช้ในการเก็บข้อมูลกฎ
5. ระบบแสดงผลรายงานการทำงาน

**Alternative Flow:**

3a. หากระบบไม่สามารถอ่านกฎเข้าสู่แพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ได้จะรายงานข้อผิดพลาดที่เกิดขึ้น

4a. หากระบบไม่สามารถบันทึกข้อมูลลงได้จะแสดงข้อความผิดพลาดขึ้น

**Postcondition:** -

**Use Case:** Active Filter Rule

**Brief Description:** จะเป็นการส่งค่าของกฎต่างๆที่ได้แก้ไขเข้าสู่แพ็กเก็ตฟิลเตอร์ไฟร์วอลล์และไฟล์ที่เก็บข้อมูลของกฎ เพื่อเริ่มต้นการทำงาน

**Actor:** Administrator

**Precondition:** ผู้ใช้งานจะต้องทำการ Login เข้าสู่ระบบและได้รับสิทธิ์การใช้งานเป็น Admin

**Basic Flows:**

1. Administrator เปิดหน้าเว็บขึ้นเพื่อทำการ Active กฎ
2. ระบบทำการเปลี่ยนแปลงกฎที่กำลังทำงานอยู่ในแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์
3. ระบบทำการบันทึกกฎลงไปแทนที่กฎที่อยู่ไฟล์เก็บข้อมูลของแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์
4. ระบบแจ้งผลการการดำเนินการ

**Alternative Flow:** -

2a. หากระบบไม่สามารถเปลี่ยนแปลงกฎในแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ได้จะแสดงข้อความผิดพลาดขึ้น

3a. หากระบบไม่สามารถบันทึกข้อมูลลงได้จะแสดงข้อความผิดพลาดขึ้น

**Postcondition:** -

**Use Case:** Manage System Configuration

**Brief Description:** กำหนดค่าต่างๆให้กับระบบ เช่น Host name, Domain, Gateway, DNS Server

**Actor:** Administrator

**Precondition:** ผู้ใช้งานจะต้องทำการ Login เข้าสู่ระบบและได้รับสิทธิ์การใช้งานเป็น Admin

**Basic Flows:**

1. Administrator เปิดหน้าเว็บขึ้นเพื่อจัดการกับค่าของระบบ

2. ระบบทำการเปลี่ยนแปลงค่าต่างๆของระบบ
3. ระบบทำการบันทึกค่าการเปลี่ยนแปลงลงในไฟล์ของระบบ
4. ระบบแจ้งผลการการดำเนินการ

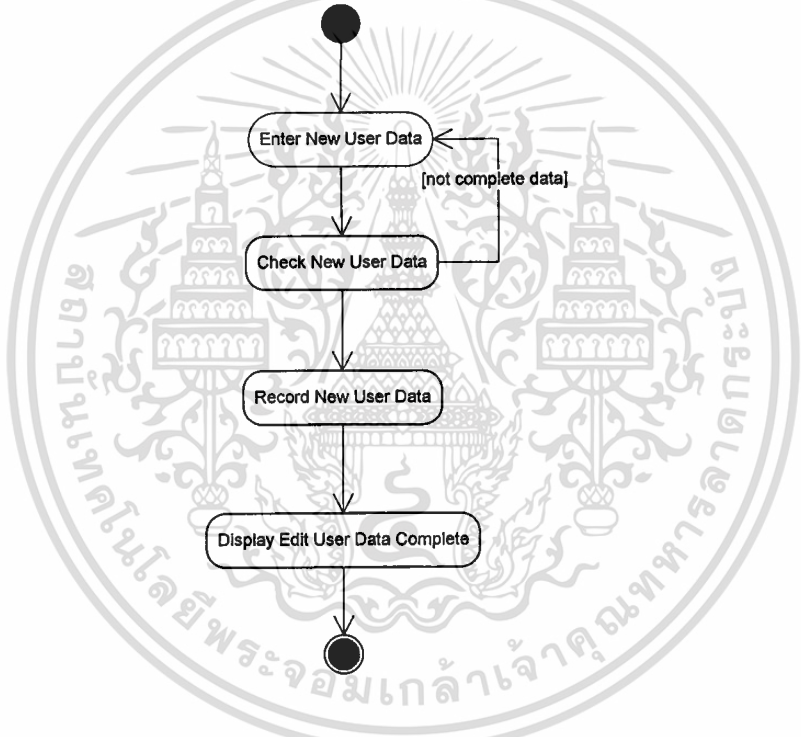
**Alternative Flow: -**

2a. หากระบบไม่สามารถเปลี่ยนแปลงค่าได้จะแสดงข้อความผิดพลาดขึ้น

3a. หากระบบไม่สามารถบันทึกข้อมูลลงได้จะแสดงข้อความผิดพลาดขึ้น

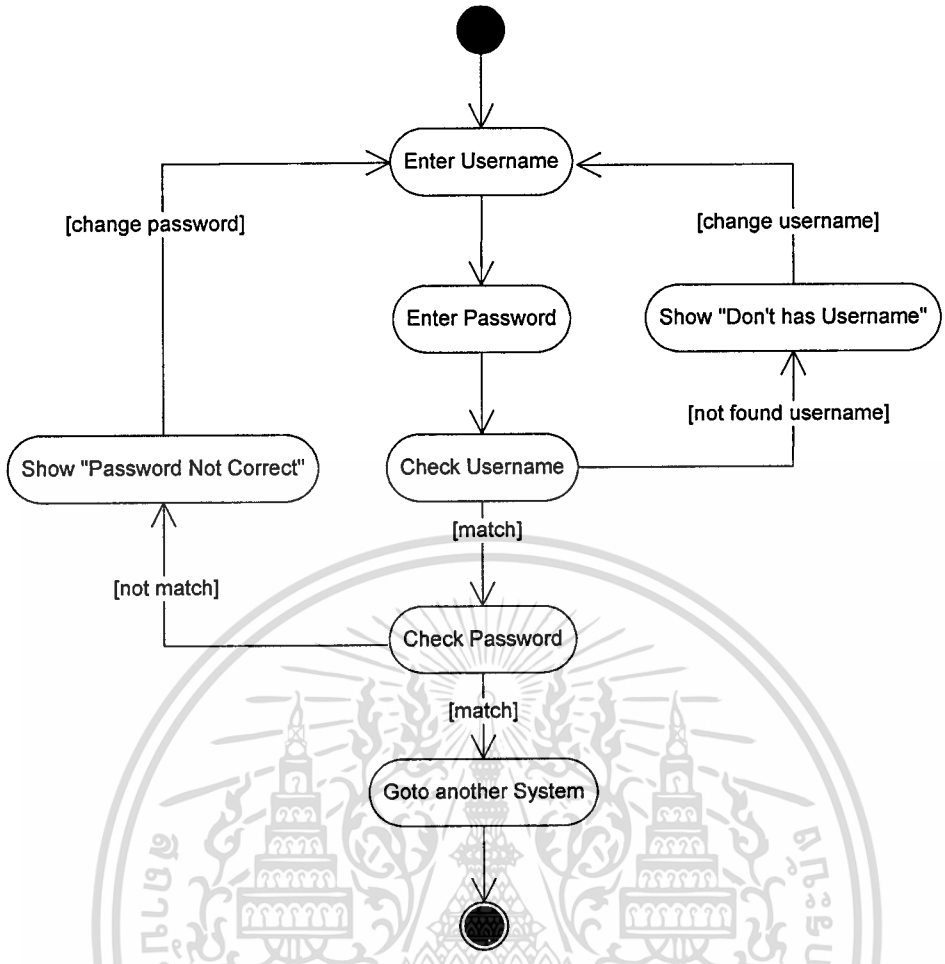
**Postcondition: -**

**Activity Diagram**



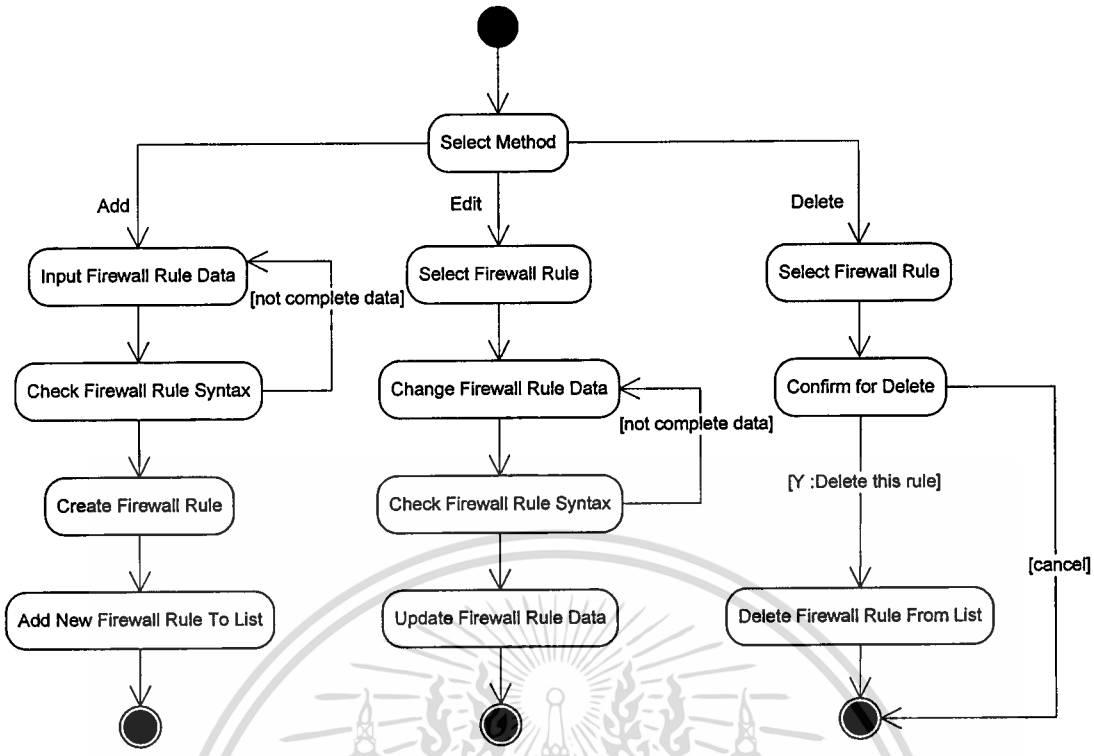

**รูปที่ 3.3** แสดง Activity Diagram ของ Manage User Account

Manage User Account เป็นการทำงานในการจัดการข้อมูลต่างๆของผู้ใช่ เช่น การแก้ไขชื่อและรหัสผ่านผู้ใช้ การลบ เพิ่ม ผู้ใช้ โดยการทำงานในส่วนของ Manage User Account เริ่มจากการรับข้อมูลของผู้ใช้เข้าสู่ระบบ และทำการตรวจสอบข้อมูลที่นำเข้ามาว่ามีความถูกต้องตรงตามรูปแบบที่กำหนด รวมถึงความครบถ้วนของข้อมูลที่รับเข้ามา ซึ่งเมื่อข้อมูลสามารถผ่านการตรวจสอบก็จะถูกกบันทึกเข้าสู่ระบบ และแสดงผลการเปลี่ยนแปลงข้อมูล




**รูปที่ 3.4** แสดง Activity Diagram ของ Login

Login เป็นการทำงานในส่วนของการตรวจสอบผู้เข้าใช้ระบบว่ามีสิทธิ์เข้าใช้ระบบหรือไม่ โดยการทำงานจะเริ่มจากการนำเข้าชื่อและรหัสผ่านของผู้ใช้ และทำการตรวจสอบข้อมูลผู้ใช้และรหัสผ่านทีละส่วน และจะมีการรายงานความผิดพลาดในแต่ละส่วนออกไปให้กับผู้ใช้เพื่อให้สามารถทราบถึงข้อผิดพลาดที่เกิดขึ้น ซึ่งถ้าไม่มีความผิดพลาดเกิดขึ้นก็จะอนุญาตให้ผู้ใช้เข้าสู่ระบบในส่วนต่อไป



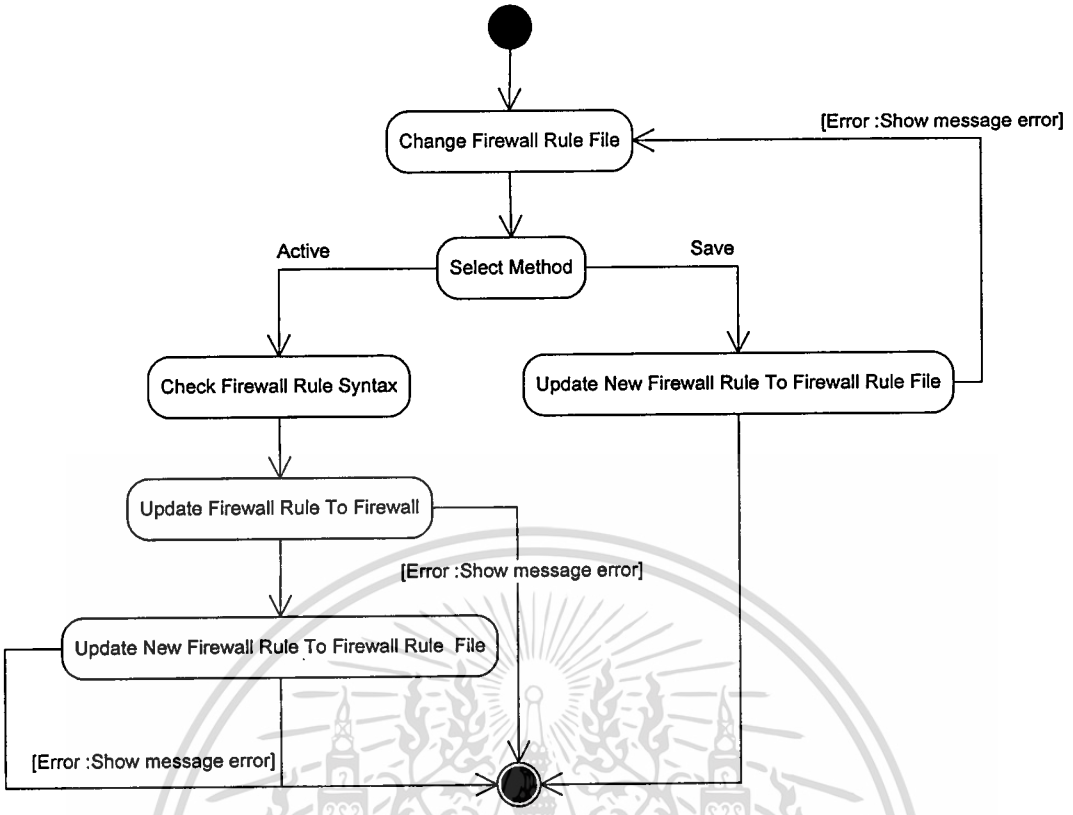

**รูปที่ 3.5** แสดง Activity Diagram ของ Manage Firewall Rule

Manage Firewall Rule เห็นการทำงานในการจัดการกับกฎต่างๆที่ออยู่ภายในระบบ ซึ่งกฎที่ทำการแก้ไขนี้จะยังไม่มีผลต่อการทำงานของแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ทันที จนกว่าจะมีการ Active ให้กฎนั้นเริ่มต้นการใช้งาน โดยการจัดการกับกฎสามารถแบ่งได้ 3 แบบคือ

การเพิ่มกฎ เริ่มต้นการทำงานโดยการรับข้อมูลของกฎเข้าสู่ระบบ และทำการตรวจสอบรูปประโยคของกฎ (Rule Syntax) ซึ่งถ้ามีรูปประโยคที่ผิดกับที่กำหนดไว้ก็จะกำหนดให้ผู้ใช้กำหนดค่าของกฎเข้ามาใหม่ โดยเมื่อผ่านการตรวจสอบก็จะสร้างกฎและเพิ่มกฎเข้าสู่ Firewall Rule List

การแก้ไขกฎ ผู้ใช้ทำการเลือกกฎที่ต้องการแก้ไข และทำการเปลี่ยนแปลงข้อมูลของกฎที่ได้เลือกไว้ จากนั้นระบบจะทำการตรวจสอบรูปประโยคของกฎ ก่อนที่จะทำการปรับเปลี่ยนข้อมูลของกฎที่เก็บไว้ใน Firewall Rule List

การลบกฎ ผู้ใช้เลือกกฎที่ต้องการลบออกจาก Firewall Rule List จากนั้นจะมีการยืนยันการลบกฎนั้นออกจากระบบ เมื่อตอบตกลงระบบจะทำการลบกฎออกจาก Firewall Rule List

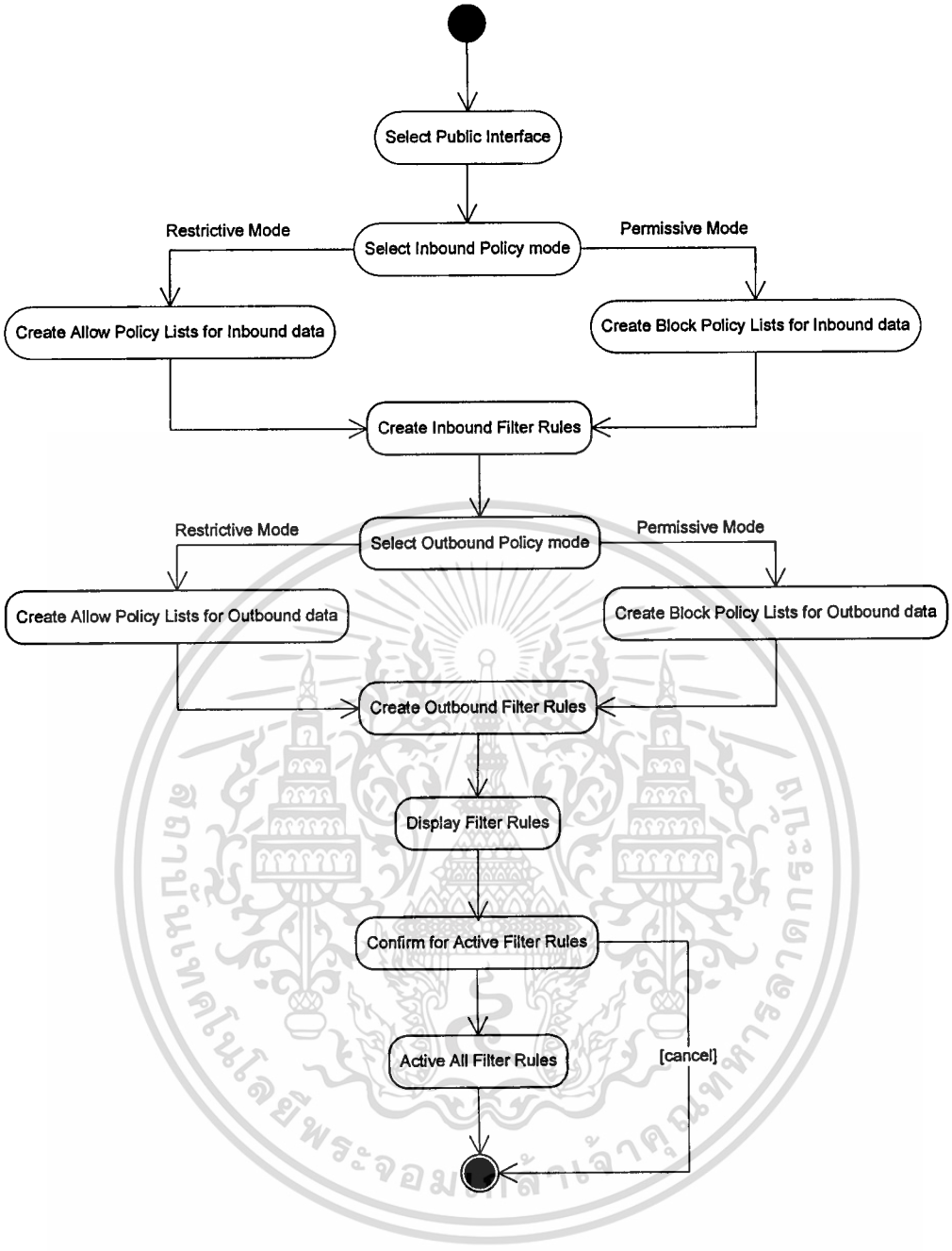



**รูปที่ 3.6** แสดง Activity Diagram ของ Advance Configuration

Advance Configuration เป็นการทำงานในส่วนของการจัดการกับกฎของแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์อีกทางหนึ่ง โดยผู้ใช้สามารถแก้ไขกับกฎภายในไฟล์ที่เก็บกฎต่างๆของไฟร์วอลล์ (Firewall Rule File) ได้โดยตรง การทำงานจะเริ่มจากผู้ใช้ทำการแก้ไขข้อมูลของไฟล์ และเลือกการจัดการกับข้อมูลที่แก้ไข โดยแบ่งเป็น

การเริ่มต้นการใช้งานกฎที่ได้แก้ไข (Active) โดยมีการตรวจสอบรูปประโยคของกฎและทำการนำกฎเข้าสู่แพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ จากนั้นจะทำการเขียนข้อมูลกฎใหม่ลงไปทับข้อมูลของกฎเดิมใน Firewall Rule File

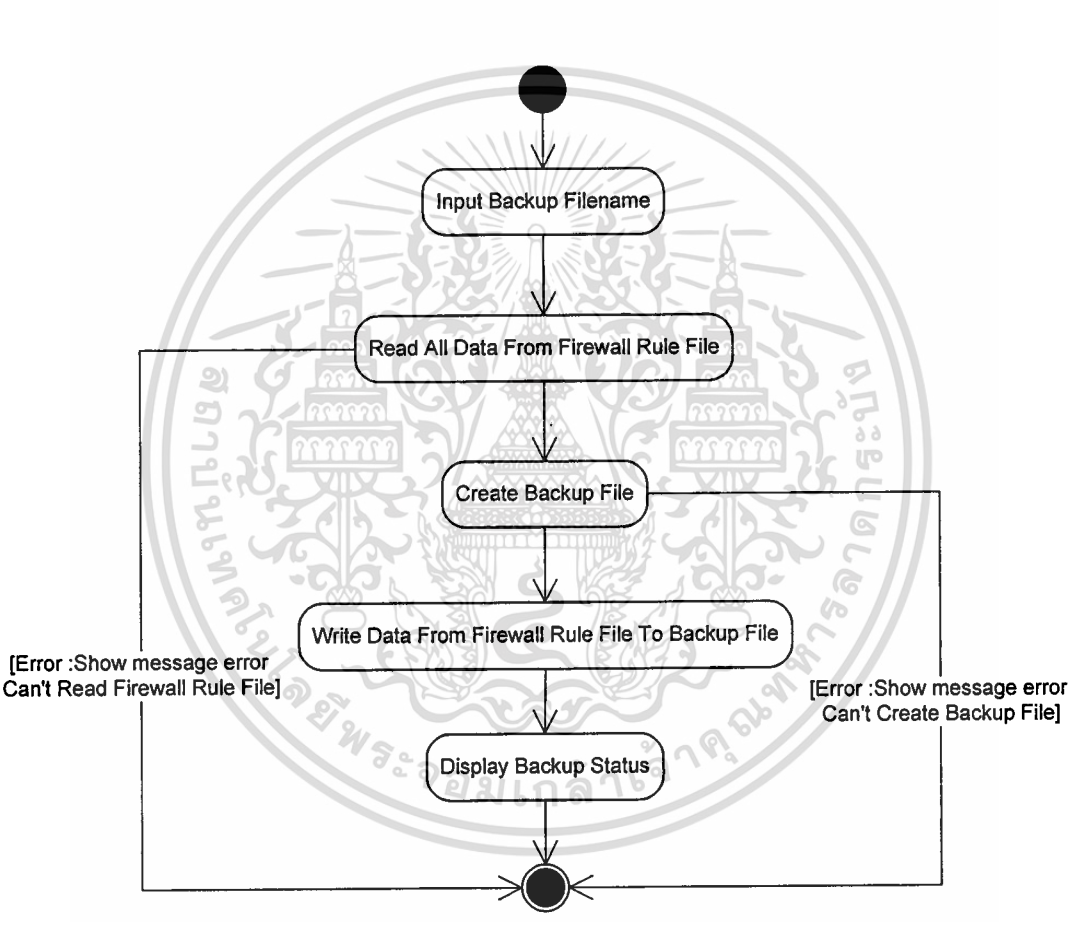
การเก็บข้อมูลกฎที่แก้ไข(Save) การเก็บข้อมูลจะไม่ทำการนำกฎเข้าสู่แพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ แต่จะเก็บข้อมูลลงใน Firewall Rule File อย่างเดียว




**รูปที่ 3.7** แสดง Activity Diagram ของ Wizard Setup

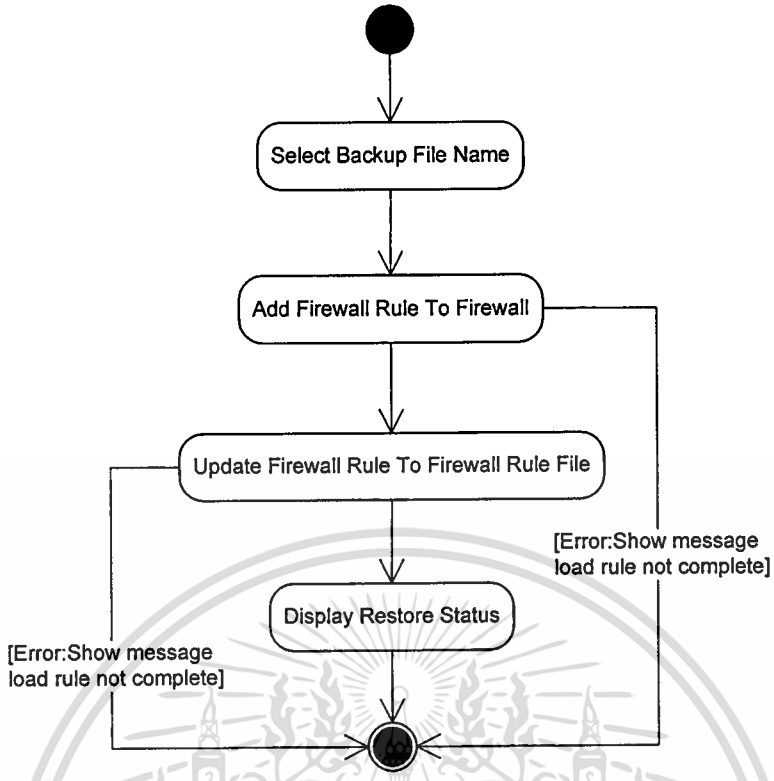
Wizard Setup เป็นเครื่องมือสำหรับช่วยในการสร้างกฎให้กับแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ โดยเริ่มต้นจากการเลือก Interface ของไฟร์วอลล์ที่เชื่อมต่อกับเครือข่ายภายนอก จากนั้นจะเข้าสู่การกำหนดกฎสำหรับกรองข้อมูลขาเข้า (Inbound) ของไฟร์วอลล์ ซึ่งผู้ใช้ต้องเลือกโหมดในการทำงานที่มีให้เลือก 2 โหมด คือ Permissive mode โดยจะส่งผ่านทุกแพ็กเก็ตทางด้านขาเข้าของไฟร์วอลล์ และ Restrictive mode โดยจะบล็อกทุกแพ็กเก็ตทางด้านขาเข้าของไฟร์วอลล์ จากนั้นต้องทำการสร้างรายละเอียดในการกรองข้อมูลทางด้านขาเข้า ถ้ามีการเลือกโหมดเป็น Permissive mode ผู้ใช้ต้องกำหนดรายละเอียดในการบล็อก (block) ข้อมูลทางขาเข้าที่ไม่ต้องการให้ส่งผ่าน

แต่ถ้าผู้ใช้เลือกโหมดการทำงานแบบ Restrictive mode ผู้ใช้ต้องกำหนดรายละเอียดในการส่งผ่าน (pass) ข้อมูลขาเข้าที่อนุญาตให้ส่งต่อไปได้ จากนั้นระบบจะสร้างกฎทางด้าน Inbound ที่ได้จากข้อมูลที่ได้รับ และเข้าสู่การกำหนดการกรองข้อมูลทางด้านขาออก (Outbound) โดยจะมีรูปแบบการกำหนดเหมือนกับในส่วนของการกรองข้อมูลขาเข้า คือทำการเลือกโหมดในการทำงานและกำหนดรายละเอียดในการกรองข้อมูลเพื่อส่งผ่านหรือบล๊อกข้อมูล ระบบสร้างกฎทางด้านขาออกจากข้อมูลที่ได้รับ ในส่วนสุดท้ายระบบแสดงข้อมูลของกฎทั้งหมดให้กับผู้ใช้ได้ทราบและรอการยืนยันการใช้งานกฎจากผู้ใช้เพื่อเริ่มต้นการทำงานของกฎที่สร้างขึ้น



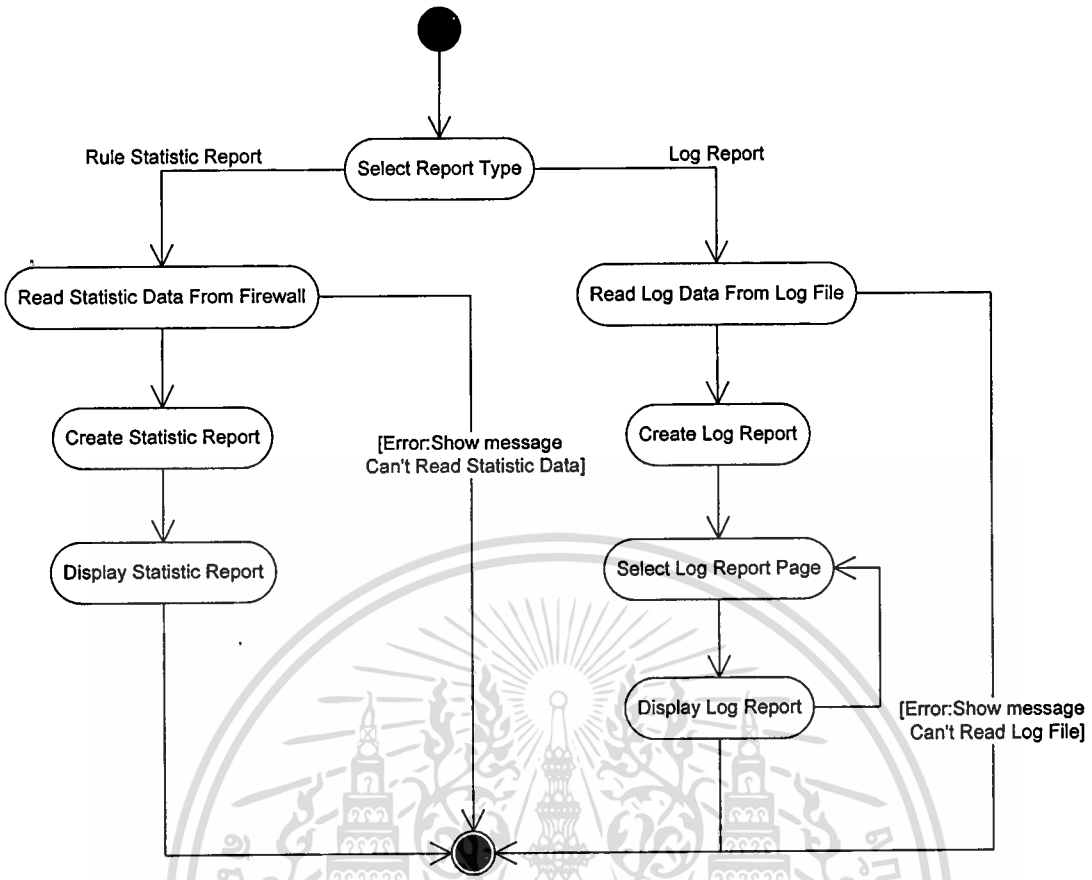

**รูปที่ 3.8** แสดง Activity Diagram ของ Backup

Backup เป็นการสำรองข้อมูลของกฎที่ใช้งานในปัจจุบัน ที่เก็บอยู่ใน Firewall Rule File ไปเก็บไว้ในไฟล์ใหม่ โดยการทำงานเริ่มจากการกำหนดชื่อของไฟล์ที่จะใช้ในการเก็บข้อมูล จากนั้นระบบจะทำการอ่านข้อมูลใน Firewall Rule File จากนั้นทำการสร้างไฟล์ที่จะใช้ในการสำรองข้อมูลตามชื่อไฟล์ที่กำหนด และทำการเขียนข้อมูลที่อ่านขึ้นมาจาก Firewall Rule File สู่ไฟล์ที่ใช้ในการสำรองข้อมูล และแสดงรายงานผลการทำงาน




**รูปที่ 3.9** แสดง Activity Diagram ของ Restore

Restore เป็นการทำงานในส่วนของการอ่านข้อมูลที่ได้ทำการสำรองไว้เข้าสู่ระบบ โดยการทำงานเริ่มจากการส่งชื่อของไฟล์ที่เก็บข้อมูลที่ได้สำรองไว้ จากนั้นระบบทำการอ่านไฟล์และนำกฎที่อ่านได้เข้าสู่โปรแกรมแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ จากนั้นจะทำการเขียนกฎลง Firewall Rule File และแสดงผลการทำงาน

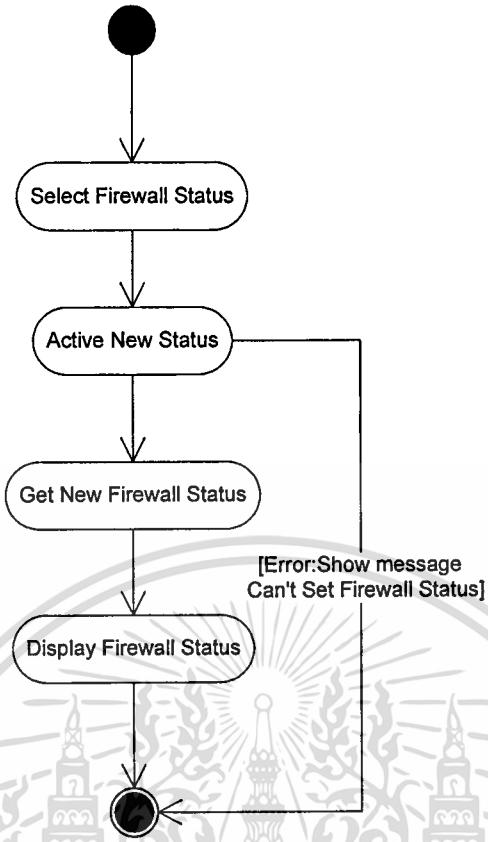



**รูปที่ 3.10** แสดง Activity Diagram ของ View Report

View Report เป็นการเรียกดูข้อมูลรายงานจากระบบ โดยการทำงานจะต้องเลือกรายงานที่ต้องการเรียกดู ซึ่งรายงานที่สามารถเรียกดูได้แบ่งได้ 2 แบบคือ

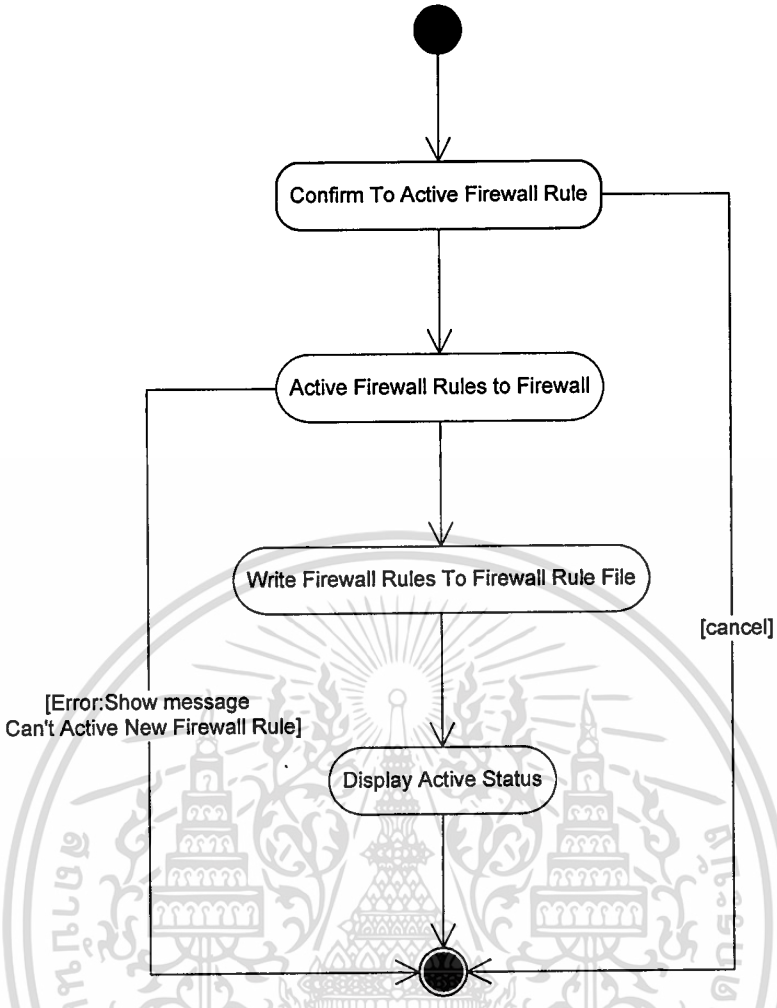
Rule Statistic Report เป็นรายงานที่แสดงรายละเอียดทางด้านสถิติต่างๆของกฎ โดยการสร้างรายงานจะเริ่มจากการอ่านค่าทางสถิติของกฎจากโปรแกรมแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์นำมาสร้างรายงานจากข้อมูลที่ได้รับ และแสดงรายงานให้กับผู้ใช้ แต่ในกรณีที่ไม่สามารถอ่านค่าจากโปรแกรมไฟร์วอลล์ได้กฎจะแจ้งข้อผิดพลาดให้กับผู้ใช้

Log Report เป็นรายงานเพื่อแสดงข้อมูลที่เก็บอยู่ใน Log File ของโปรแกรมแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ โดยทำการอ่านค่าภายใน Log File เข้าสู่ระบบ และทำการสร้างรายงานจากข้อมูลที่ได้รับ เนื่องจากข้อมูลที่ได้จากการเก็บ Log ของโปรแกรมแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์อาจมีปริมาณมากระบบจะทำการแบ่งกรแสดงออกเป็นหลายๆหน้าจอ เพื่อให้ผู้ใช้เลือกหน้าที่ต้องการดูข้อมูลได้



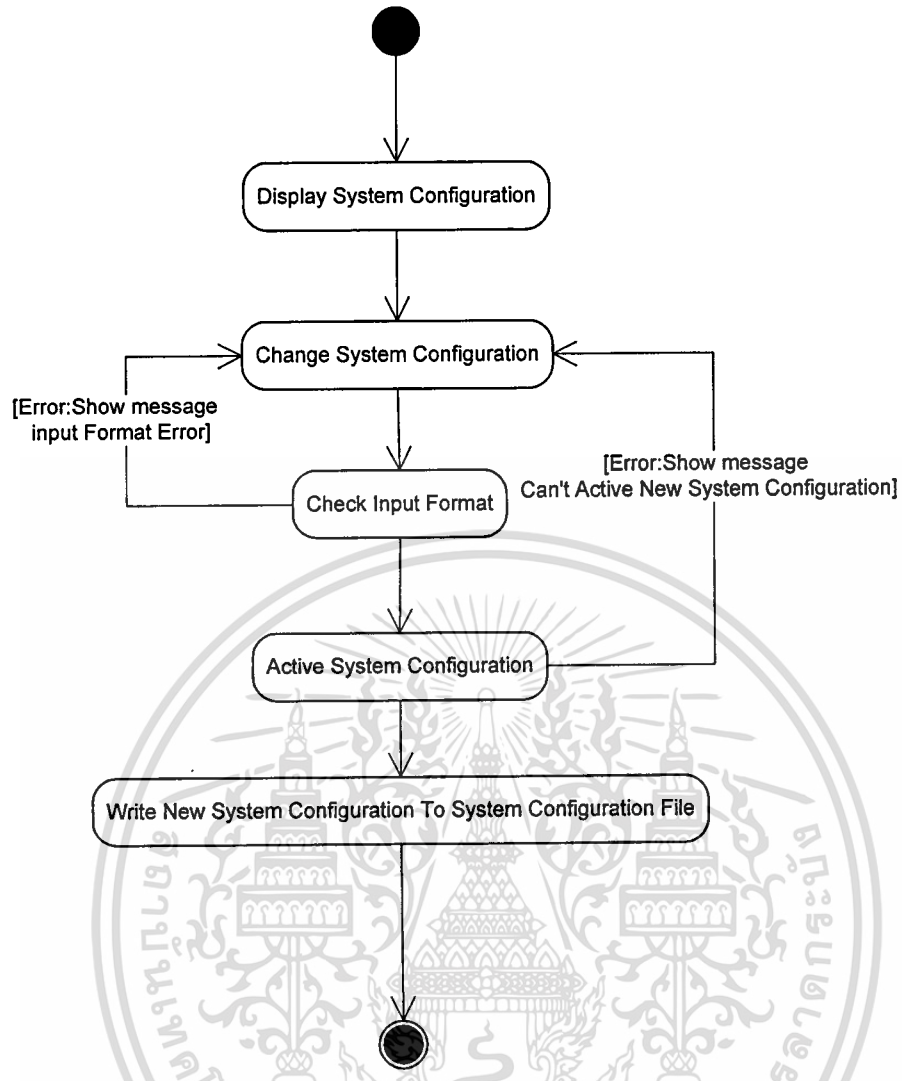

**รูปที่ 3.11** แสดง Activity Diagram ของ Manage Firewall Status

Manage Firewall Status เป็นการจัดการกับสถานะของไฟร์วอลล์ โดยเริ่มจากผู้ใช้เลือกสถานะที่ต้องการกำหนดให้กับแพ็กเก็ตฟิลเตอร์ จากนั้นระบบจะทำการเปลี่ยนสถานะของแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ตามที่ได้รับจากผู้ใช้ และทำการอ่านสถานะในปัจจุบันของแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ขึ้นมาใหม่ และแสดงสถานะในปัจจุบันของแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์




**รูปที่ 3.12** แสดง Activity Diagram ของ Active Firewall Rule

Active Firewall Rule เป็นการเริ่มต้นการใช้งานกฎของแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ที่มีการแก้ไขหรือเปลี่ยนแปลงจากกฎเดิมที่ใช้อยู่ โดยการทำงานระบบจะยืนยันการเริ่มต้นการใช้งานกฎใหม่ จากนั้นระบบจะนำกฎใหม่เข้าสู่โปรแกรมแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ และมีการตรวจสอบข้อผิดพลาดจากการนำกฎเข้า จากนั้นระบบจะทำการเขียนกฎใหม่เข้าสู่ Firewall Rule File และแสดงสถานะเริ่มต้นใช้งานกฎ

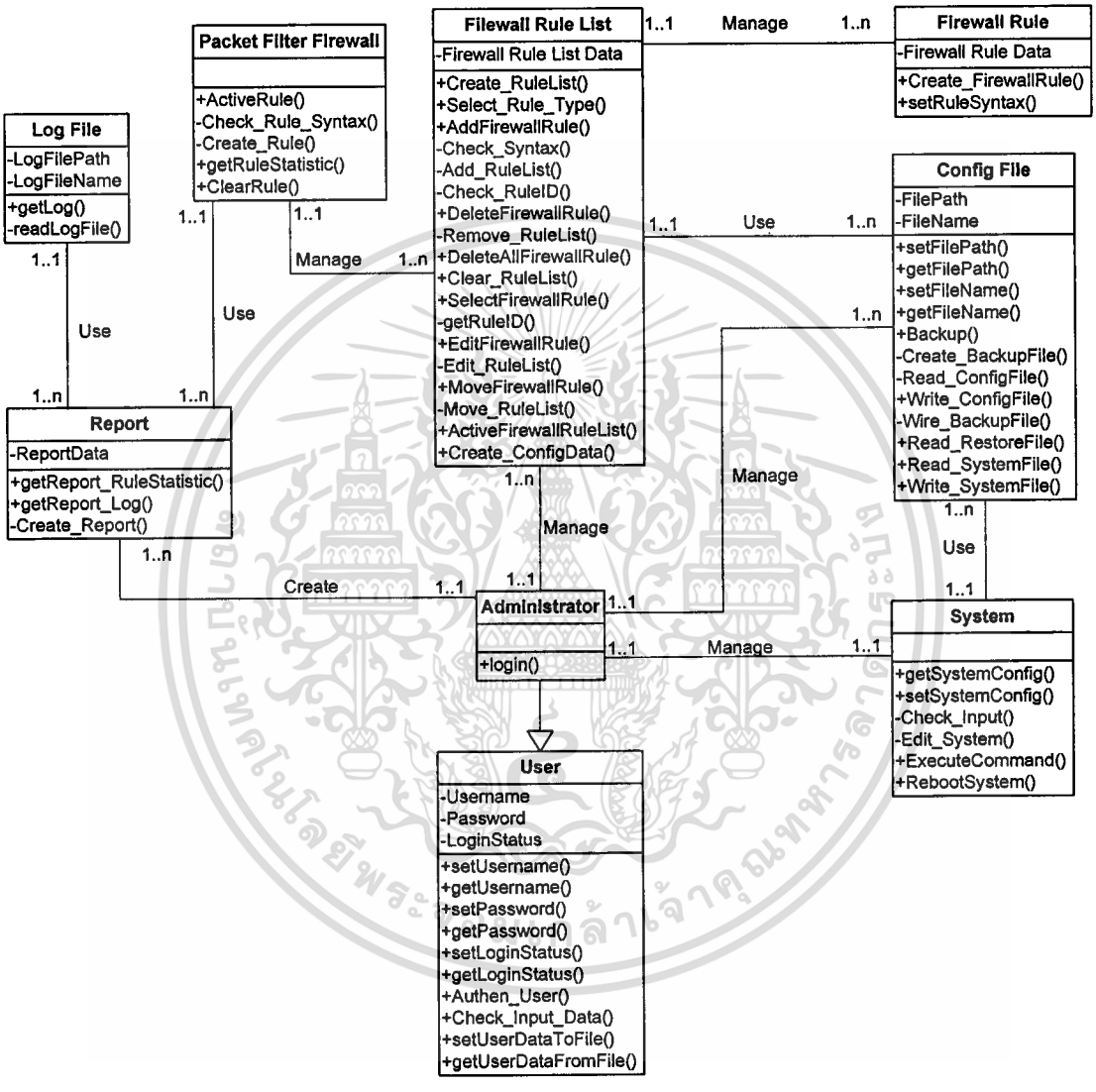



**รูปที่ 3.13** แสดง Activity Diagram ของ Manage System Configuration

Manage System Configuration เป็นการเรียกดูข้อมูลของระบบ และการปรับเปลี่ยนข้อมูลต่างๆของระบบ โดยการทำงานเริ่มต้นจากการเรียกดูข้อมูลของระบบจากผู้ใช้ และทำการเปลี่ยนแปลงข้อมูลต่างๆของระบบ จากนั้นจะมีการตรวจสอบข้อมูลการเปลี่ยนแปลงที่รับเข้ามาว่าถูกต้องตรงตามรูปแบบที่กำหนด ถ้าไม่เกิดข้อผิดพลาดก็จะทำการกำหนดข้อมูลใหม่ให้กับระบบ และเขียนข้อมูลใหม่ลงใน System Configuration File

### 3.3.2 Structural Models

เป็นการมองโครงสร้างข้อมูลของระบบ ซึ่งในที่นี้ใช้ Class Diagram เพื่อแสดงโครงสร้างข้อมูลของระบบการกำหนดกฎแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์




**รูปที่ 3.14** แสดง Class Diagram ของระบบ

**Class diagram ของระบบนี้ประกอบด้วย 7 คลาสดังนี้**

- **User** เป็นคลาสที่เก็บข้อมูลของผู้ใช้
- **Administrator** เมื่อมีการเพิ่มข้อมูลผู้ใช้เข้าสู่ระบบแล้ว ผู้ใช้คนดังกล่าวจะมีสิทธ์เป็นผู้ดูแลระบบซึ่งสามารถใช้งานระบบได้

**-Firewall Rule** เป็นคลาสที่เก็บข้อมูลของกฎข้อหนึ่งของไฟร์วอลล์

**-Firewall Rule List** เป็นคลาสที่เก็บข้อมูลกลุ่มของกฎทั้งหมด

**-Packet Filter Firewall** เป็นคลาสที่ใช่สำหรับจัดการกับแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์

**-Report** เป็นคลาสที่ใช้สำหรับสร้างรายงาน

**-Log File** เป็นคลาสที่ใช้สำหรับจัดการกับไฟล์ Log ของแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์

**-System** เป็นคลาสที่เก็บข้อมูลของระบบและใช้สำหรับจัดการกับระบบ

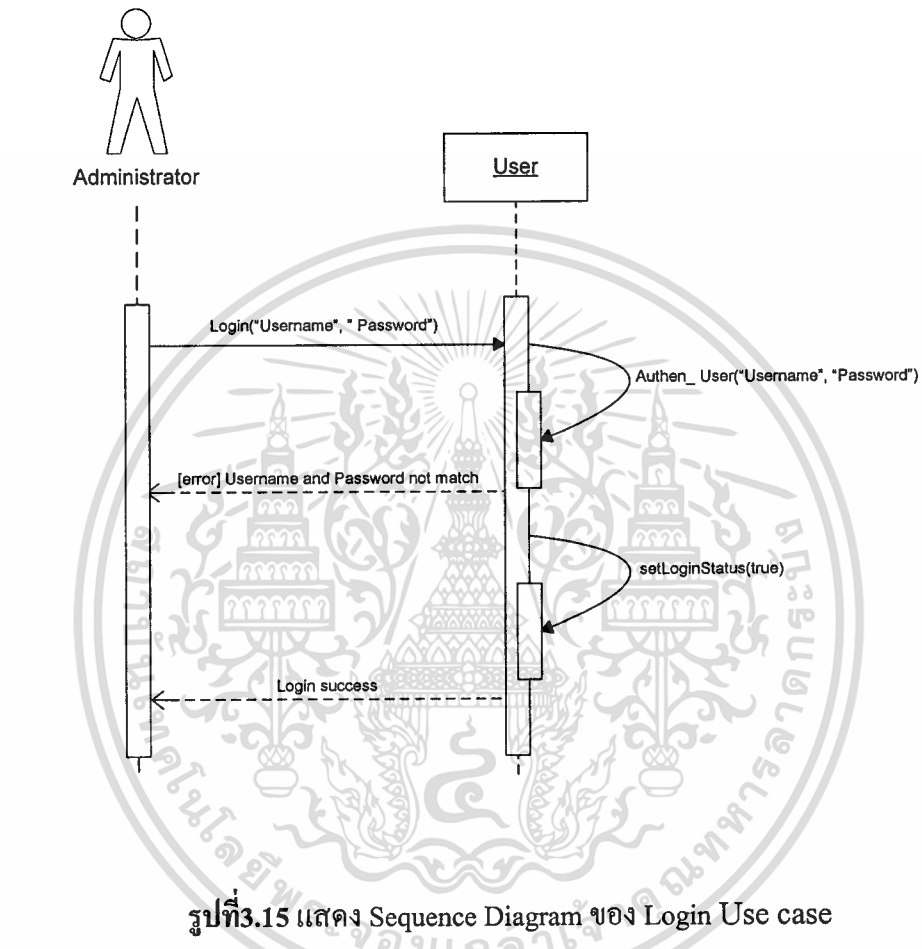
**-Config File** เป็นคลาสที่ใช้ในการจัดการกับ Configuration File ของแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์

**ภาพรวมของระบบคือ**

- Administrator มีความสัมพันธ์กับ Firewall Rule List คือ Administrator หนึ่งคนสามารถจัดการกับ Firewall Rule List ได้หลายตัว โดยแยกตามชนิดของกฎ
- Administrator มีความสัมพันธ์กับ Report คือ Administrator หนึ่งคนสามารถเรียกดู Report ได้หลาย Report
- Administrator มีความสัมพันธ์กับ Config File คือ Administrator หนึ่งคนสามารถจัดการกับ Config File ได้มากกว่าหนึ่งไฟล์ ตามการทำงานที่เกิดขึ้น
- Report มีความสัมพันธ์กับ Log File และ Packet Filter Firewall คือ Report หนึ่งตัวจะเรียกใช้ข้อมูลจาก Log File ได้เพียงหนึ่งตัว และ Report หนึ่งตัวจะเรียกใช้ข้อมูลจาก Packet Filter Firewall ได้เพียงตัวเดียวเหมือนกัน
- Firewall Rule List มีความสัมพันธ์กับ Packet Filter Firewall คือ Firewall Rule List หนึ่งตัวที่ถูกสร้างขึ้นจะถูกใช้ในการเก็บข้อมูลและจัดการกับ Packet Filter Firewall เพียงตัวเดียว
- Firewall Rule List มีความสัมพันธ์กับ Firewall Rule คือ Firewall Rule List หนึ่งตัวสามารถเก็บข้อมูลและจัดการกับ Firewall Rule ได้มากกว่าหนึ่งตัว

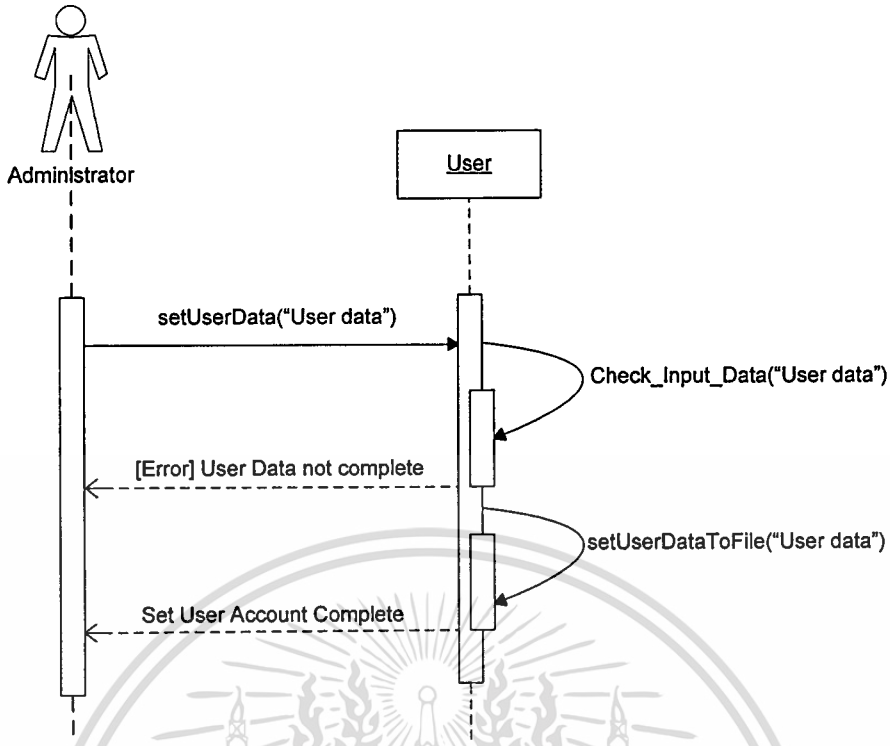
### 3.3.3 Behavioral Models

เป็นการมองกระบวนการของระบบหรือกลไกของระบบ โดยมองในลักษณะพฤติกรรมของระบบว่าระบบทำงานอย่างไร ซึ่งในที่นี้ใช้ Sequence Diagram เพื่ออธิบายกลไกของระบบในลักษณะพฤติกรรมของระบบ



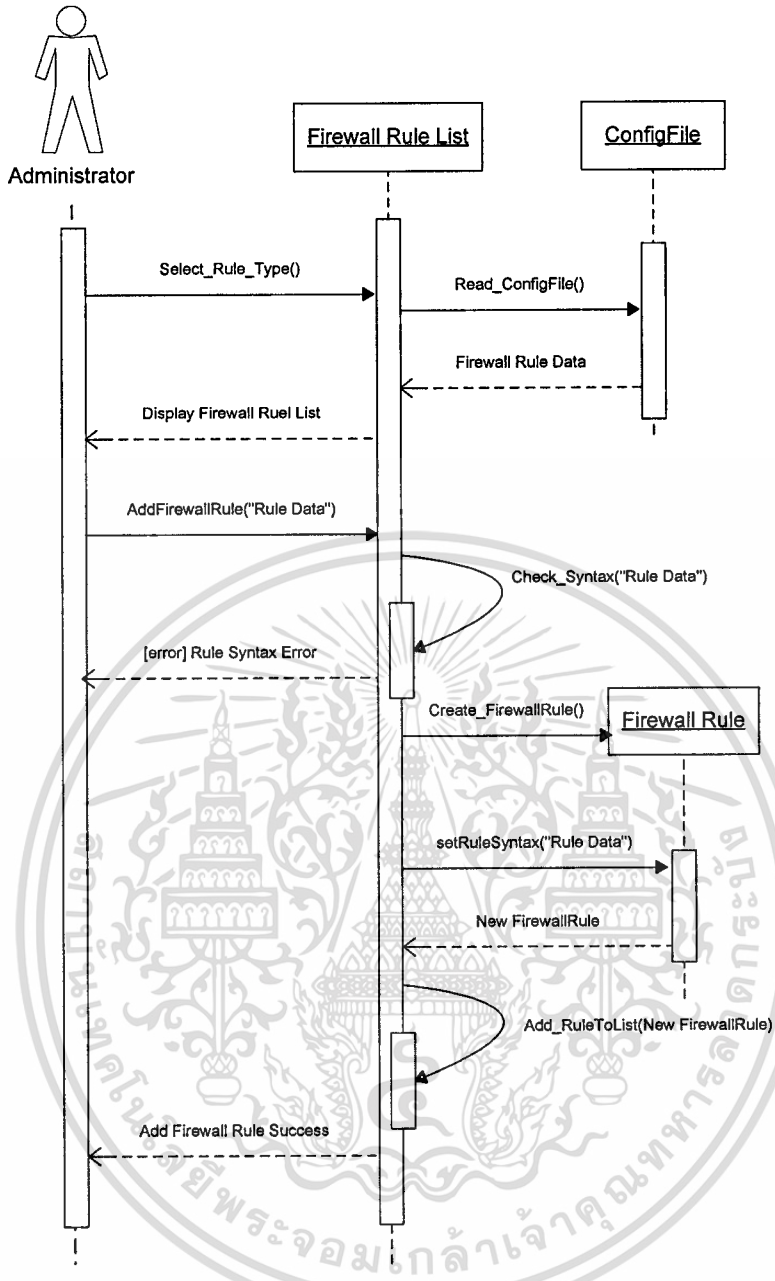

**รูปที่3.15** แสดง Sequence Diagram ของ Login Use case

จากรูปที่ 3.15 จะเป็นการแสดงถึงการทำงานของ Login Use case โดยเมื่อผู้ใช้งานระบบเข้ามาทำการใช้งานโดยการป้อนข้อมูลในส่วนของ username และ password โมดูลในส่วนของ User ก็จะทำการตรวจเช็คข้อมูลและถ้าหากข้อมูลถูกต้องก็จะอนุญาตให้ผู้ใช้งานสามารถใช้งานระบบในส่วนต่างๆได้แต่ถ้าไม่ถูกต้องก็จะทำการแจ้งข้อความผิดพลาดขึ้น



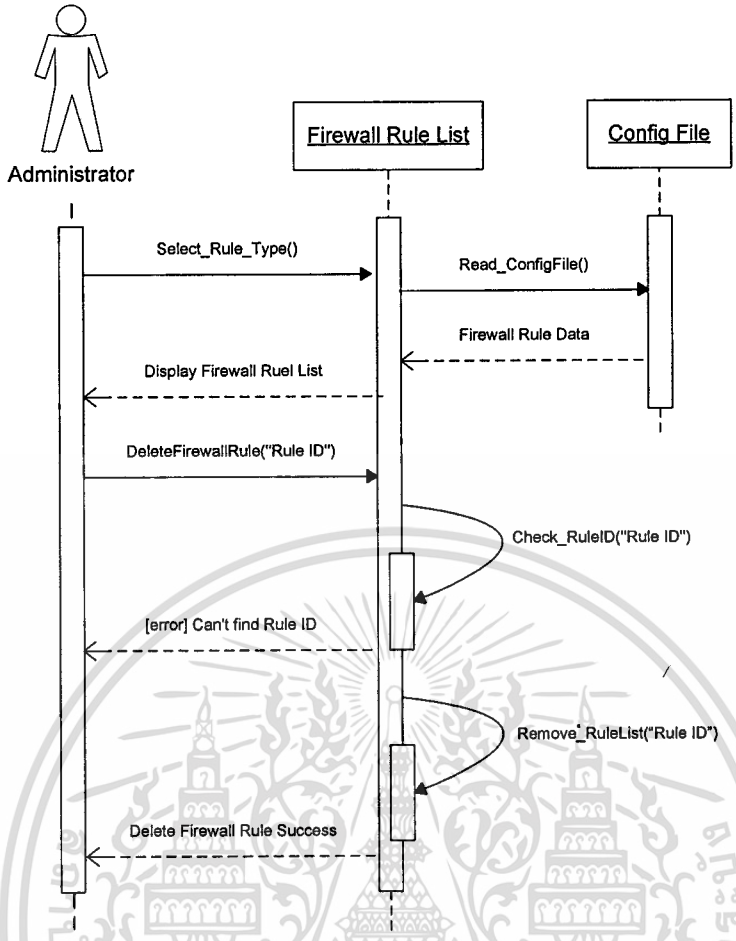

**รูปที่3.16** แสดง Sequence Diagram ของ Manage User Account Use case

จากรูปที่ 3.16 จะเป็นการแสดงถึงการทำงานของ Manage User Account Use case โดยเมื่อผู้ใช้งานระบบเข้ามาทำการใช้งานโดยการป้อนข้อมูลของผู้ใช้ โมดูลใน User จะตรวจสอบข้อมูลที่ผู้ใช้ป้อนเข้ามา ถ้ามีข้อผิดพลาดของข้อมูลจะแจ้งความผิดพลาดที่เกิดขึ้น หากไม่มีจะตรวจสอบ ถ้าข้อมูลถูกต้องก็จะทำการเปลี่ยนแปลงข้อมูลของผู้ใช้ตามที่ได้รับ



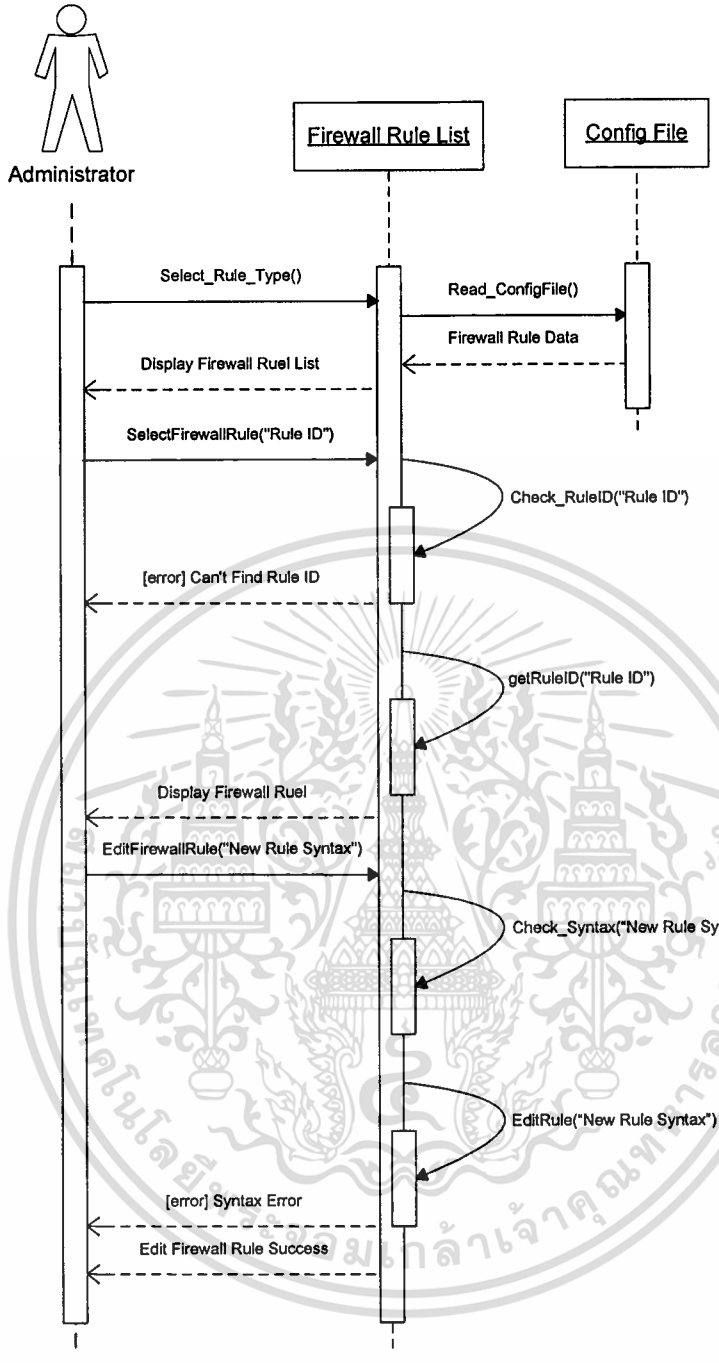

**รูปที่3.17** แสดง Sequence Diagram ของ Manage Firewall Rule Use case ส่วนการเพิ่มกฎ

จากรูปที่ 3.17 จะเป็นการแสดงถึงการทำงานของ Manage Firewall Rule Use case ในส่วนของการเพิ่มกฎ (Add) โดยเมื่อผู้ใช้งานล็อกอินเข้าสู่ระบบ Firewall Rule List จะถูกสร้างขึ้นโดยอ่านข้อมูลกฎมาจาก Configuration File และแสดงรายการกฎให้กับผู้ใช้ จากนั้นผู้ใช้จะทำการเพิ่มกฎโดยการป้อนข้อมูลของกฎที่ต้องการสร้างเข้าสู่ระบบ ระบบจะทำการตรวจจอบข้อมูลว่าความถูกต้องและครบถ้วน จากนั้นจะทำการสร้างกฎ (Firewall Rule) และกำหนดค่าให้กับกฎและเพิ่มกฎนั้นเข้าสู่ Firewall Rule List




**รูปที่3.18** แสดง Sequence Diagram ของ Manage Firewall Rule Use case ส่วนการลบกฎ

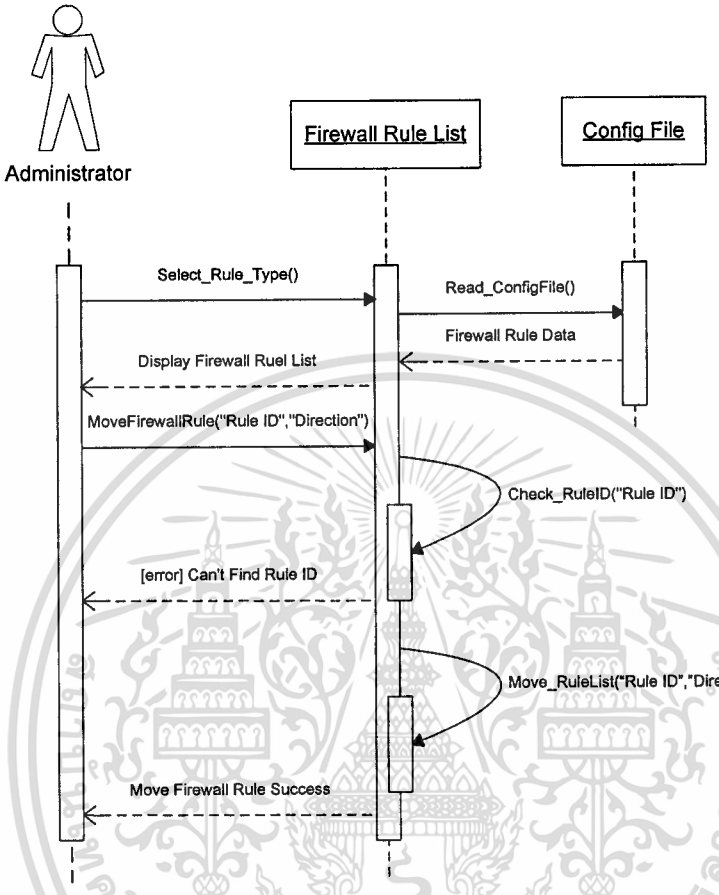
จากรูปที่ 3.18 จะเป็นการแสดงถึงการทำงาน Manage Firewall Rule Use case ส่วนการลบกฎ (Delete) โดยเมื่อผู้ใช้งานล็อกอินเข้าสู่ระบบ Firewall Rule List จะถูกสร้างขึ้นโดยอ่านข้อมูลกฎมาจาก Configuration File และแสดงรายการกฎให้กับผู้ใช้ จากนั้นเมื่อผู้ใช้ทำการลบกฎโดยการเลือกกฎที่ต้องการลบจะทำการส่งหมายเลขของกฎ(Rule ID)เข้าสู่ระบบ ระบบจะทำการตรวจสอบหมายเลขของกฎว่ามีอยู่จริงใน Firewall Rule List ซึ่งถ้าไม่พบก็จะแจ้งข้อผิดพลาดออกไป ถ้าไม่มีข้อผิดพลาดจะทำการลบข้อมูลของกฎออกจาก Firewall Rule List




**รูปที่3.19** แสดง Sequence Diagram ของ Manage Firewall Rule Use case ส่วนการแก้ไขกฎ

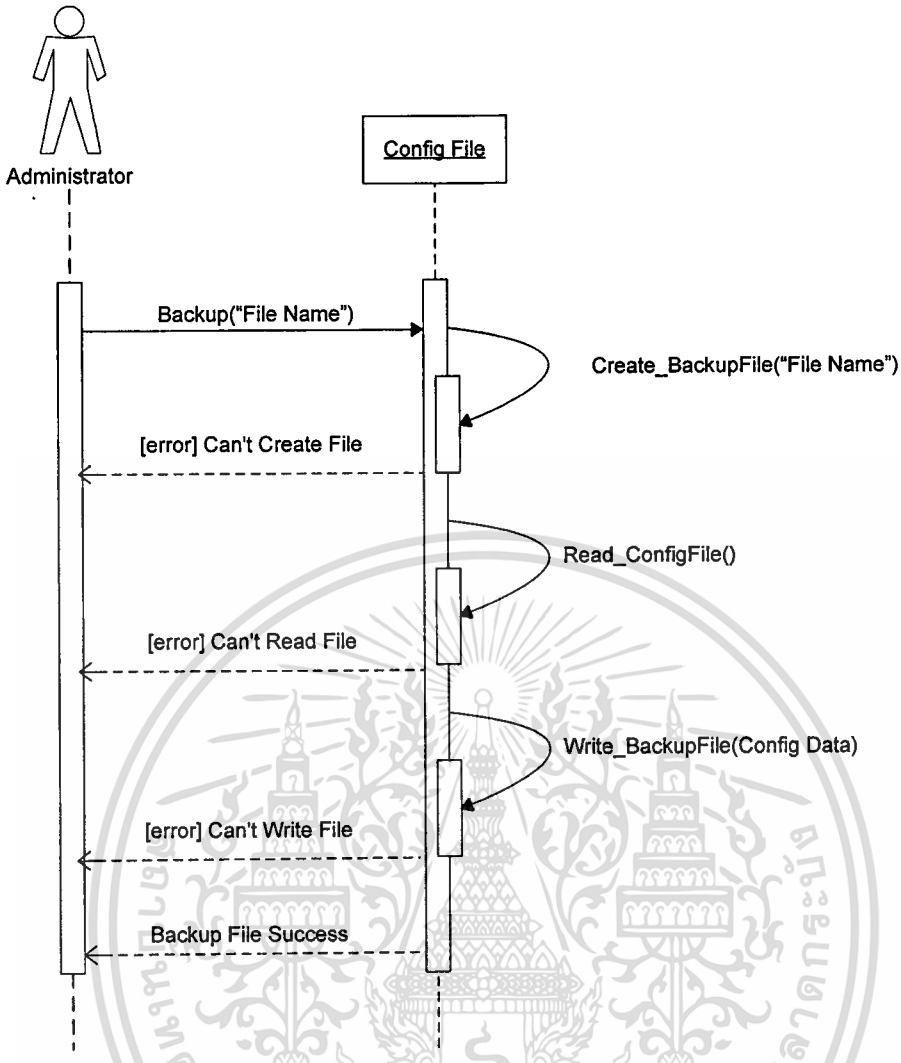
จากรูปที่ 3.19 จะเป็นการแสดงถึงการทำงานของ Manage Firewall Rule Use case ส่วนการแก้ไขกฎ (Edit) โดยเมื่อผู้ใช้งานล็อกอินเข้าสู่ระบบ Firewall Rule List จะถูกสร้างขึ้นโดยอ่านข้อมูลกฎมาจาก Configuration File และแสดงรายการกฎให้กับผู้ใช้ จากนั้นเมื่อผู้ใช้ทำการแก้ไขกฎโดยการเลือกกฎที่ต้องการแก้ไขจะทำการส่งหมายเลขของกฎ (Rule ID) เข้าสู่ระบบ และระบบจะทำการอแสดงรายละเอียดของกฎให้กับผู้ใช้ ผู้ใช้ทำการการแก้ไขกฎที่ต้องการและทำการส่ง

ข้อมูลเข้าสู่ระบบ ระบบจะทำการตรวจสอบข้อมูลของกฎที่จะแก้ไขว่าครบถ้วนและถูกต้องหรือไม่ แล้วจึงแก้ไขกฎภายใน Firewall Rule List



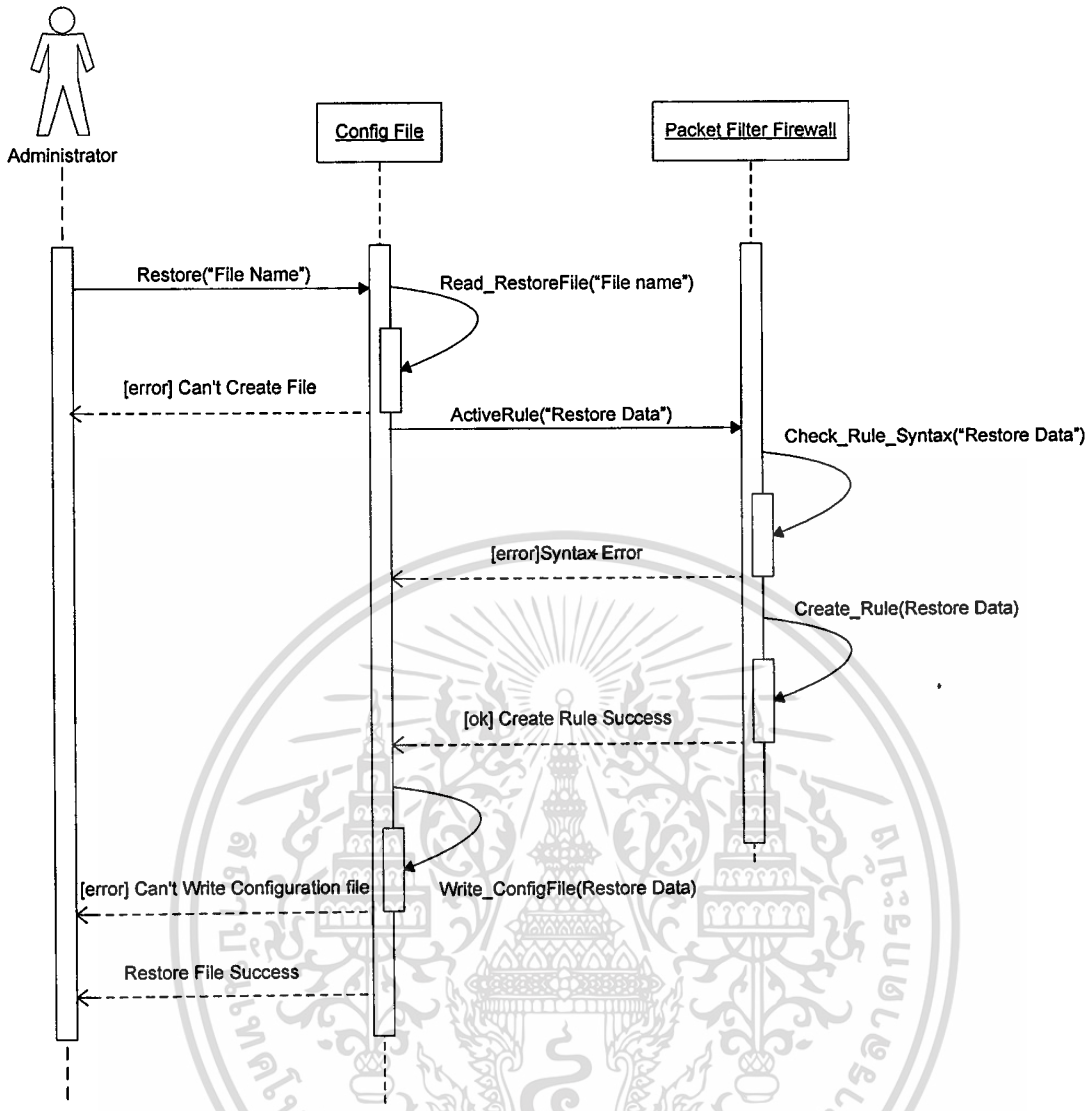

**รูปที่3.20** แสดง Sequence Diagram ของ Manage Firewall Rule Use case ส่วนการจัดเรียง

จากรูปที่ 3.20 จะเป็นการแสดงถึงการทำงานของ Manage Firewall Rule Use case ส่วนส่วนการจัดเรียง (Move)โดยเมื่อผู้ใช้งานล็อกอินเข้าสู่ระบบ Firewall Rule List จะถูกสร้างขึ้นโดยอ่านข้อมูลกฎมาจาก Configuration File และแสดงรายการกฎให้กับผู้ใช้ จากนั้นเมื่อผู้ใช้ทำการเลือกจัดเรียงกฎโดยการเลือกกฎที่ต้องการจัดเรียง จะทำการส่งหมายเลขของกฎ (Rule ID) และทิศทางในการจัดเรียงเข้าสู่ระบบ จะทำการตรวจสอบหมายเลขของกฎว่ามีอยู่จริงใน Firewall Rule List ซึ่งถ้าไม่พบก็จะแจ้งข้อผิดพลาดออกไป ถ้าไม่มีข้อผิดพลาดจะจัดเรียงลำดับกฎตามที่กำหนด



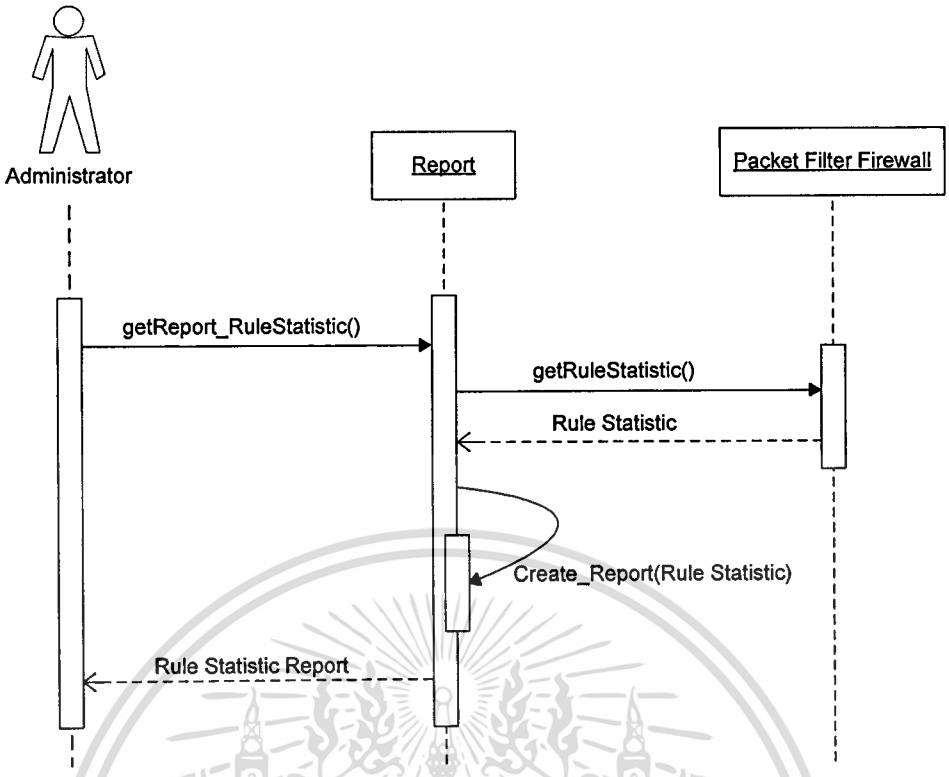

**รูปที่3.21** แสดง Sequence Diagram ของ Backup Use case

จากรูปที่ 3.21 จะเป็นการแสดงถึงการทำงานของ Backup Use case โดยเมื่อผู้ใช้งานล็อกอินเข้าสู่ระบบ และทำสำรองข้อมูล โดยการเรียกใช้โมดูลของระบบและส่งชื่อของไฟล์ที่ใช้เก็บข้อมูล ระบบจะสร้างไฟล์สำหรับสำรองข้อมูล จากนั้นระบบจะอ่านข้อมูลกฎต่างๆจาก Configuration File และทำการบันทึกข้อมูลที่อ่านไปไว้ที่ไฟล์ที่ใช้สำรองข้อมูล



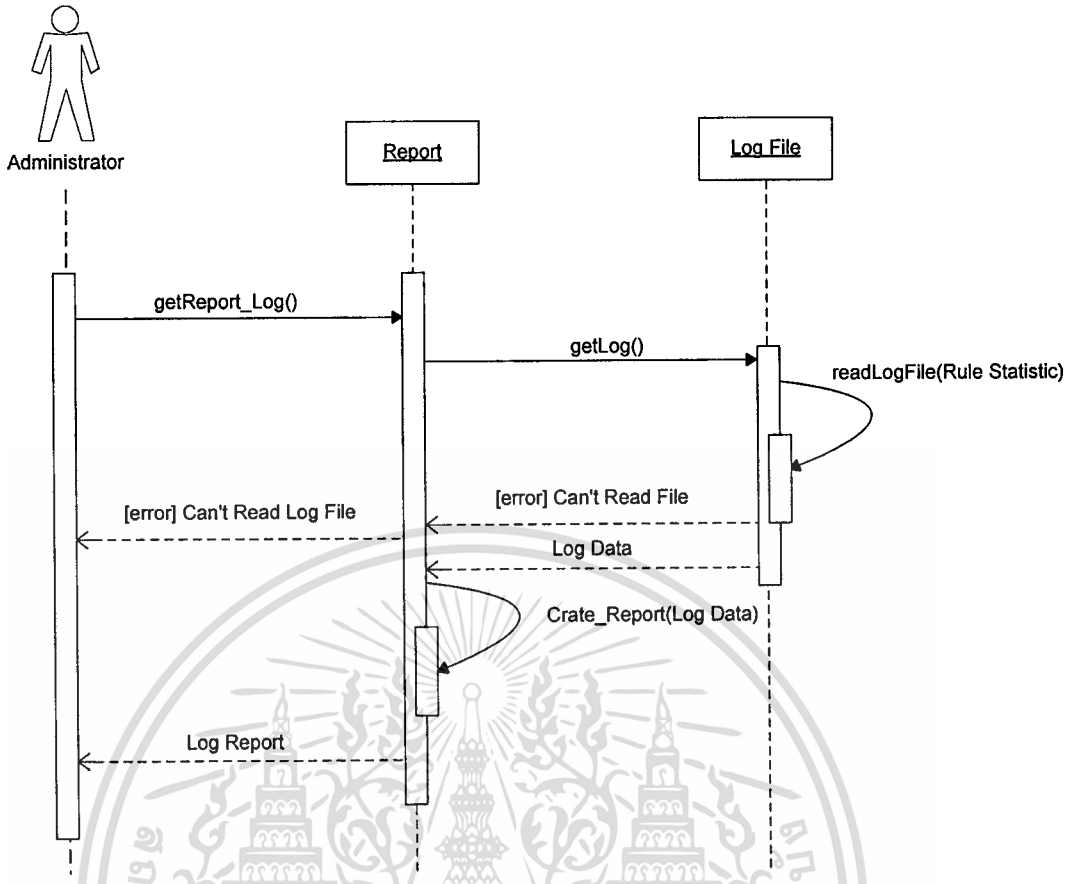

**รูปที่3.22** แสดง Sequence Diagram ของ Restore Use case

จากรูปที่ 3.22 จะเป็นการแสดงถึงการทำงานของ Restore Use case โดยเมื่อผู้ใช้งานล็อกอินเข้าสู่ระบบ ผู้ใช้เรียกใช้งานโมดูลของระบบและส่งชื่อไฟล์ที่เป็นไฟล์ที่ได้สำรองเอาไว้ จากนั้นระบบจะทำการอ่านข้อมูลจากไฟล์ต้นฉบับที่กำหนดมา และทำการส่งข้อมูลของกฎทั้งหมดให้กับแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์เพื่อเริ่มใช้งานกฎ โดยมีการทำการตรวจสอบข้อมูลและสร้างกฎให้อยู่ในรูปแบบที่พร้อมใช้งาน จากนั้นเขียนข้อมูลของกฎลงใน Configuration File



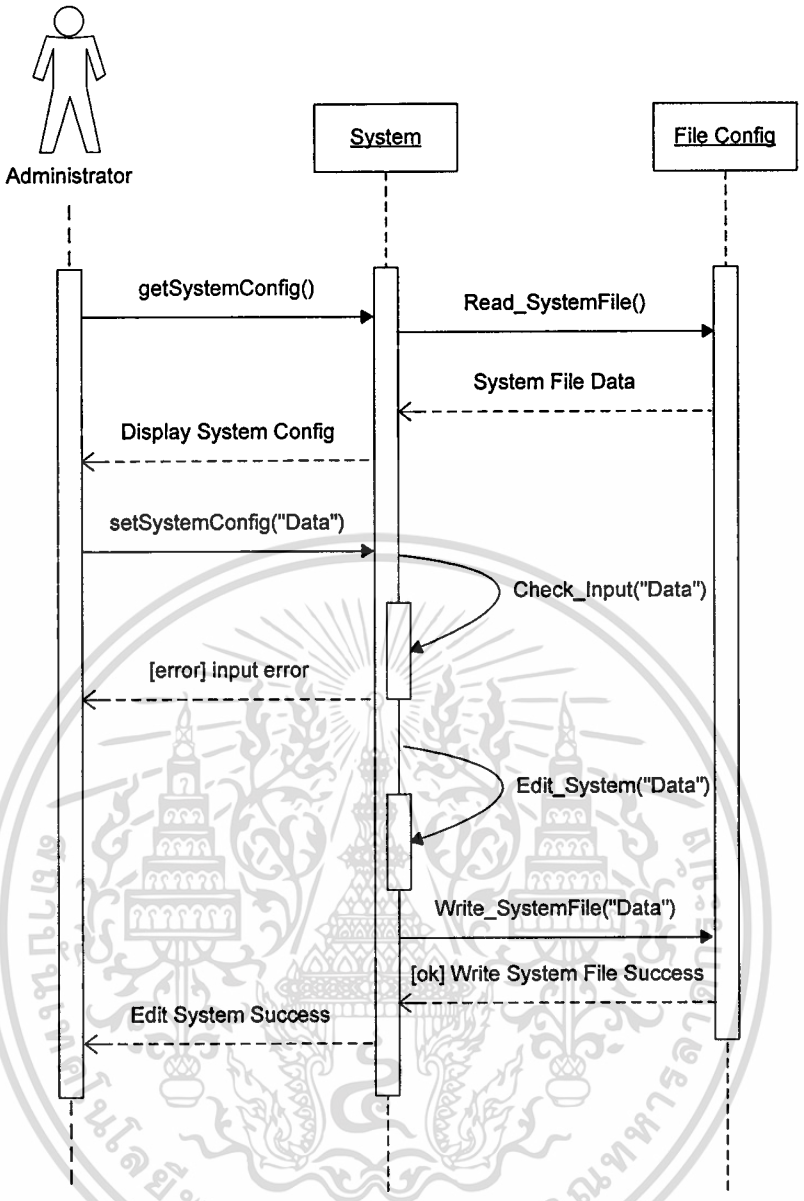

**รูปที่3.23** แสดง Sequence Diagram ของ Report Use case ส่วนของ Rule Statistic Report

จากรูปที่ 3.23 จะเป็นการแสดงถึงการทำงานของ Report Use case ส่วนของ Rule Statistic Report โดยเมื่อผู้ใช้งานล็อกอินเข้าสู่ระบบ ผู้ใช้เรียกใช้งาน Rule Statistic Report โดยเรียกใช้โมดูลของระบบจากนั้นระบบจะอ่านข้อมูลทางสถิติของกฎจากแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ และนำข้อมูลที่ได้รับมาสร้างเป็นเอกสารและแสดงผลให้กับผู้ใช้



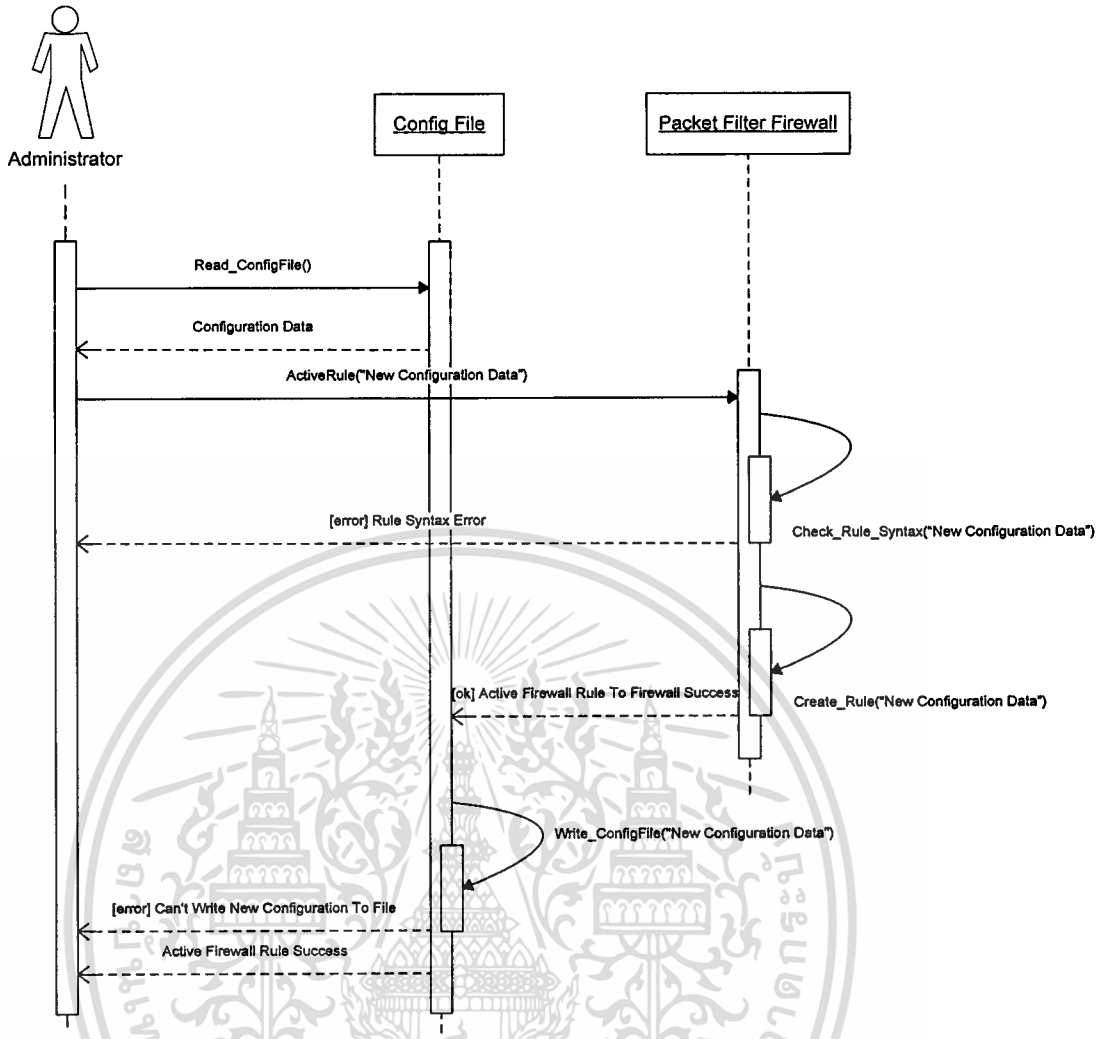

**รูปที่3.24** แสดง Sequence Diagram ของ Report Use case ส่วนของ Log Report

จากรูปที่ 3.24 จะเป็นการแสดงถึงการทำงานของ Report Use case ส่วนของ Log Report โดยเมื่อผู้ใช้งานล็อกอินเข้าสู่ระบบ ผู้ใช้เรียกใช้งาน Log Report โดยเรียกใช้โมดูลของระบบ จากนั้นระบบจะอ่านข้อมูลจาก Log File ของแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ และนำข้อมูลที่ได้รับมาสร้างเป็นเอกสารและแสดงผลให้กับผู้ใช้



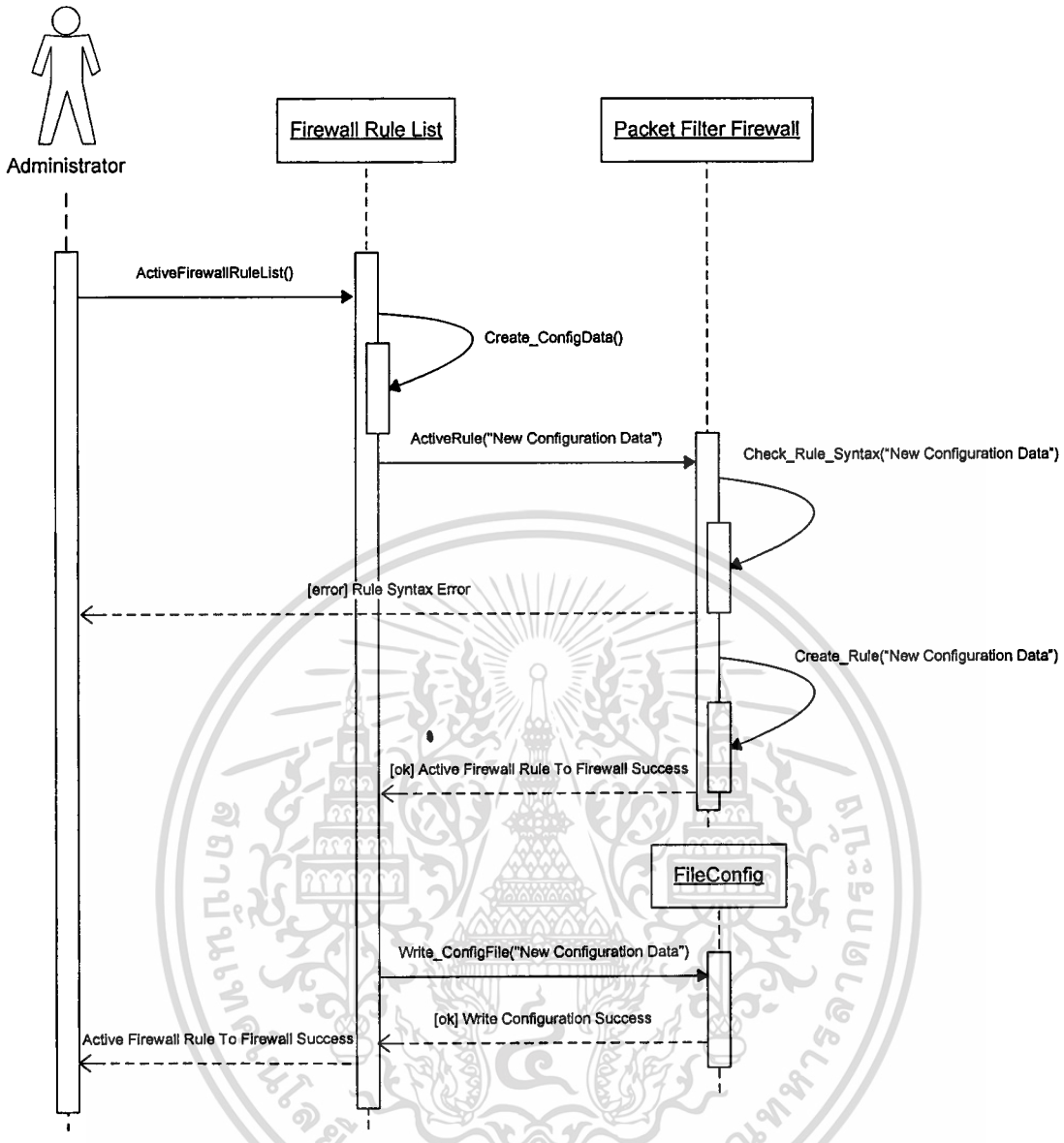

**รูปที่3.25** แสดง Sequence Diagram ของ Manage System Configuration Use case

จากรูปที่ 3.25 จะเป็นการแสดงถึงการทำงานของ Manage System Configuration Use case โดยเมื่อผู้ใช้งานล็อกอินเข้าสู่ระบบ ผู้ใช้เรียกใช้ดูข้อมูลของระบบ (System Configuration) โดยระบบทำการอ่านข้อมูลของระบบจาก System Configuration File และแสดงผลให้กับผู้ใช้ ผู้ใช้ทำการแก้ไขข้อมูลของระบบและส่งข้อมูลกลับเข้าสู่ระบบ ระบบจะทำการตรวจสอบข้อมูลที่ได้รับ ถ้ามีข้อผิดพลาดจะรายงานผลให้ผู้ใช้ทราบ ถ้าไม่มีข้อผิดพลาดจะทำการแก้ไขข้อมูลของระบบ และเขียนข้อมูลเหล่านั้นลง System Configuration File



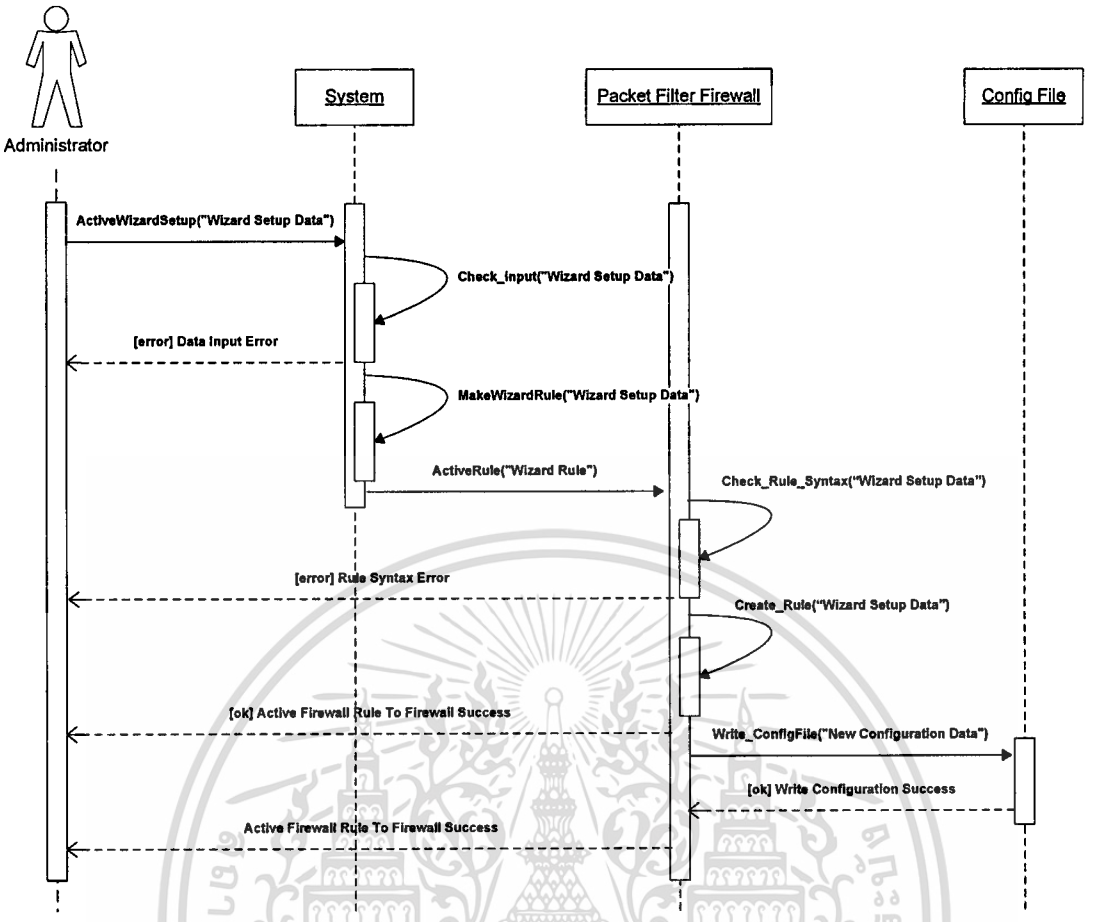

**รูปที่3.26** แสดง Sequence Diagram ของ Advance Configuration Use case

จากรูปที่ 3.26 จะเป็นการแสดงถึงการทำงานของ Advance Configuration Use case โดย เมื่อผู้ใช้งานล็อกอินเข้าสู่ระบบ ผู้ใช้เรียกใช้ดูข้อมูลของ Firewall Rule File ระบบทำการอ่านข้อมูลของระบบจาก Firewall Rule File และแสดงผลให้กับผู้ใช้ ผู้ใช้ทำการแก้ไขข้อมูลกฎ และส่งข้อมูลกลับเข้าสู่ระบบ ระบบจะทำการตรวจสอบข้อมูลกฎที่ได้รับ ถ้ามีข้อผิดพลาดจะรายงานผลให้ผู้ใช้ทราบ ถ้าไม่มีข้อผิดพลาดจะสร้างกฎล่านั้นในแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์เพื่อเริ่มต้นทำงาน และเขียนข้อมูลของกฎที่ผู้ใช้แก้ไขลงสู่ Firewall Rule File



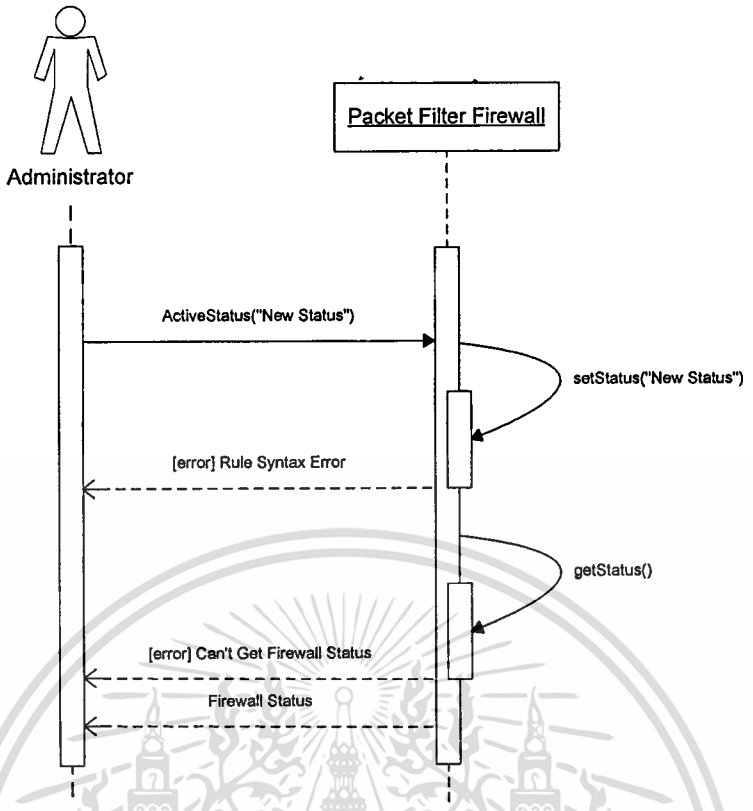

**รูปที่3.27** แสดง Sequence Diagram ของ Active Firewall Rule Use case

จากรูปที่ 3.27 จะเป็นการแสดงถึงการทำงานของ Active Firewall Rule Use case โดยเมื่อผู้ใช้งานล็อกอินเข้าสู่ระบบ ผู้ใช้เริ่มต้นการทำงานของกฎ (Active) ผ่านโมดูลของระบบ จากนั้นระบบทำการสร้างข้อมูล (New Configuration Data) สำหรับการกำหนดกฎต่างๆให้กับแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ และส่งข้อมูลที่สร้างขึ้นให้กับให้กับแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ เพื่อเริ่มต้นใช้งานกฎ โดยจะมีการตรวจสอบรูปประโยคของกฎที่ส่งเข้ามา และรายงานข้อผิดพลาดไปหาผู้ใช้ แต่ถ้าไม่มีความผิดพลาดก็จะสร้างกฎจากข้อมูลเหล่านั้นเข้าสู่แพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ จากนั้นทำการบันทึกข้อมูลของกฎใหม่เข้าสู่ Firewall Rule File




**รูปที่3.28** แสดง Sequence Diagram ของ Wizard Setup Use case

จากรูปที่ 3.28 จะเป็นการแสดงถึงการทำงานของ Wizard Setup Use case โดยเมื่อผู้ใช้งานล็อกอินเข้าสู่ระบบ ผู้ใช้เริ่มต้นการทำงานของ Wizard setup โดยทำการกำหนดค่าสำหรับนำไปสร้างกฎ (Wizard Setup Data) จากนั้นผู้ใช้จะส่งข้อมูลเข้าระบบ ระบบทำการตรวจสอบข้อมูลที่ได้รับและรายงานข้อผิดพลาด ถ้าไม่มีข้อผิดพลาดระบบจะทำการสร้างกฎจากข้อมูลที่ได้จาก Wizard Setup (Wizard Rule) และส่งข้อมูลที่กฎเหล่านั้นเข้าสู่เข้าสู่แพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ เพื่อเริ่มต้นการทำงานของกฎ และจากนั้นจะทำการเขียนข้อมูลของกฎที่สร้างขึ้นลงที่ Firewall Rule File




**รูปที่3.29** แสดง Sequence Diagram ของ Manage Firewall Status Use case

จากรูปที่ 3.29 จะเป็นการแสดงถึงการทำงานของ Manage Firewall Status Use case โดยเมื่อผู้ใช้งานล็อกอินเข้าสู่ระบบ ผู้ใช้เริ่มต้นการทำงานโดยทำการกำหนดค่าสถานะ (Status) ของแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ และส่งค่าสถานะให้กับระบบ จากนั้นระบบจะทำการกำหนดค่าสถานะให้กับแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ และระบบทำการอ่านค่าสถานะในปัจจุบันขึ้นมาเพื่อส่งสถานะปัจจุบันให้กับผู้ใช้

## 3.4 การออกแบบโครงสร้างไฟล์ของระบบ

เนื่องจากระบบใช้การเก็บข้อมูลในรูปแบบไฟล์ โดยในการเก็บข้อมูลกฎของแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์จะใช้การเก็บข้อมูลลงในไฟล์คอนฟิก (pf.conf) ซึ่งมีรูปแบบการจัดเก็บตามรูปแบบของการเขียนกฎ และข้อมูลของระบบจะถูกจัดเก็บลงในไฟล์คอนฟิกของระบบปฏิบัติการ FreeBSD (rc.conf) ในรูปแบบเดียวกับการกำหนดค่าให้กับระบบปฏิบัติการ นอกจากนั้นระบบจะทำการจัดเก็บข้อมูลที่เกิดจากการทำงานของโปรแกรมในไฟล์ที่โปรแกรมสร้างขึ้นใหม่ (pfwi.conf)

**ไฟล์คอนฟิกของแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ (/etc/pf.conf)**

ใช้เก็บข้อมูลกฎของแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ ซึ่งจัดเก็บอยู่ที่ /etc/pf.conf โดยจะประกอบไปด้วยข้อมูลของกฎที่ประกอบด้วย Runtime Option, Table, Antispoof Rule และFilter Rule ซึ่งกฎแต่ละประเภทมีรายละเอียดในการจัดเก็บดังนี้

**Runtime Option**

เก็บข้อมูลที่ใช้ในการกำหนดค่า Option ต่างๆ ให้กับโปรแกรมแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์โดยมีรูปแบบการจัดเก็บข้อมูลของ Runtime Option จะประกอบไปด้วย

set **option name value**

โดยสามารถอธิบายข้อมูลแต่ละส่วนได้ดังนี้

set

เป็นคำสั่งที่ใช้ในการกำหนดค่าให้กับ Runtime Option

**option name**

เป็นชื่อของ Runtime Option ที่ต้องการกำหนดค่า

**value**

เป็นค่าที่ต้องการกำหนดให้กับ Runtime Option ที่กำหนดใน [option name]

**Table**

ใช้ในการเก็บค่าของกลุ่ม IP Address ต่างๆ เพื่อใช้ในการจัดการกับกลุ่ม IP Address โดยมีรูปแบบการจัดเก็บข้อมูลของ Runtime Option จะประกอบไปด้วย

table **<table name> {value}**

โดยสามารถอธิบายข้อมูลในแต่ละส่วนได้ดังนี้

table

เป็นคำสั่งที่ใช้ในการสร้าง table

**table name**

กำหนดชื่อให้กับ table โดยชื่อต้องอยู่ภายในเครื่องหมาย < และ>

**value**

กำหนดค่าของข้อมูลของกลุ่ม IP Addressที่จัดเก็บภายใน table โดยจะเขียนอยู่ภายในเครื่องหมายปีกกา

**Antispoof Rule**

เป็นคำสั่งที่ใช้สำหรับการกำหนดการป้องกันการปลอมแปลง IP Address เข้ามาที่ Interface โดยมีรูปแบบการจัดเก็บข้อมูลของ Antispoof Rule ดังนี้

antispoof on **{interface name}** **[log]** **[quick]**

โดยสามารถอธิบายข้อมูลในแต่ละส่วนได้ดังนี้

antispoof on

เป็นคำสั่งหลักที่ใช้ในการสร้างกฎการป้องกันการปลอมแปลง IP Address

**interface name**

เป็นกลุ่มของ Interface ที่ต้องการป้องกันการปลอมแปลง IP Address โดยถ้ามีมากกว่าหนึ่ง Interface จะต้องเขียนอยู่ภายใต้เครื่องหมายปีกกา

**log**

เป็นคำสั่งที่ใช้สำหรับกำหนดให้ทำการเก็บ log ของแพ็กเก็ตที่มีการปลอมแปลง IP Address เข้ามา และถูกตรวจสอบพบโดยกฎ

**quick**

เป็นคำสั่งที่ใช้สำหรับการกำหนดให้กฎทำงานในทันทีเมื่อตรวจพบการปลอมแปลงข้อมูล

**Filter Rule**

เป็นคำสั่งที่ใช้สำหรับการกำหนดกฎในการกรองข้อมูลที่ถูกส่งผ่านมายังไฟร์วอลล์ โดยมีรูปแบบของการจัดเก็บข้อมูลของ Filter Rule ดังนี้

*action* **[*direction*]** **[log]** **[quick]** **[on *interface*]** **[*af*]** **[proto *protocol*]** \
**[from *src_addr* [port *src_port*]]** **[to *dst_addr* [port *dst_port*]]** \
**[flags *tcp_flags*]** **[*state*]**

โดยสามารถอธิบายข้อมูลในแต่ละส่วนได้ดังนี้

**action**

เป็นการกำหนดการทำงานที่จะเกิดขึ้นเมื่อพบแพ็กเก็ตที่ตรงกับเกณฑ์ของ Filter Rule ตั้งไว้นั้นคือการ block หรือ pass โดยในส่วนของการ pass ก็จะทำการส่งแพ็กเก็ตออกไปตามปกติ แต่ในส่วนของ block จะมีการตอบสนองที่ขึ้นอยู่กับ block-policy option ซึ่งโดยปกติจะมีค่าเป็น block drop หรือ block return

**direction**

เป็นทิศทางของแพ็กเก็ตบน Interface ซึ่งประกอบไปด้วย in หรือ out

**log**

เป็นการกำหนดให้เก็บ Log ของแพ็กเก็ต

**quick**

ถ้าแพ็กเก็ตใดตรงกับ Filter Rule ที่กำหนด quick ไว้ จะถือว่ากฎข้อนั้นเป็น Filter Rule สุดท้ายที่ตรงทับเล็กเก็ต และจะทำงานตามการทำงานที่กำหนดไว้ใน Filter Rule นั้น

**on interface**

ชื่อหรือกลุ่มของ Network Interface ที่แพ็กเก็ตส่งผ่าน

**af**

กำหนดถึง IP Address version ที่แพ็กเก็ตใช้งานอยู่ โดยมีค่าเป็น inet เมื่อแพ็กเก็ตใช้ IP Address version 4 และเป็น inet6 เมื่อแพ็กเก็ตใช้ IP Address version 6 แต่ตามปกติแล้วแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ สามารถที่จะตัดสินใจได้เองจากข้อมูล IP Address ว่าเป็น IP Address version ไหน ทำให้ค่าในส่วนนี้อาจไม่จำเป็นต้องกำหนด

**protocol**

เป็นการระบุถึงโปรโตคอลที่ใช้ในเลเยอร์ 4 เช่น TCP, UTP เป็นต้น หรืออาจระบุโดยใช้ Protocol number ซึ่งมีค่าอยู่ระหว่าง 0-255 ลงไปก็ได้ และสามารถใช้ List ในการเก็บข้อมูลของกลุ่มโปรโตคอลได้อีกด้วย

**src_addr, det_addr**

เป็นการระบุถึง IP address ของต้นทางและ IP Address ของปลายทางที่อยู่ในแพ็กเก็ต โดยสามารถกำหนดได้หลายรูปแบบ เช่น

- กำหนดโดยการใส่ IP Address ลงไปโดยตรง
- กำหนดเป็น CIDR Network Block
- กำหนดโดยใช้ชื่อของ Network Interface
- ใช้การสร้าง Table หรือ List เข้ามาช่วยในการเก็บข้อมูล
- การระบุค่าเป็น any จะหมายถึงทุกๆ IP Address
- การระบุค่าเป็น all จะเป็นการเขียนแทนคำสั่ง any to any

**src_port, det_port**

เป็นการระบุถึง Port ต้นทางและ Port ปลายทางของโปรโตคอลที่ใช้ในการสื่อสารในเลเยอร์ 4 โดยสามารถระบุได้หลายรูปแบบ เช่น

- กำหนดเป็นตัวเลขของ Port number ซึ่งมีค่าระหว่าง 1 - 65535
- กำหนดโดยใช้ชื่อของบริการ

- ใช้การสร้าง List เพื่อเก็บกลุ่มของ Port number
- สามารถใช้เครื่องหมายเพื่อกำหนดช่วงของ Port number เช่น

  != ไม่เท่ากับ

  < น้อยกว่า

  <= น้อยกว่าหรือเท่ากับ

**tcp_flags**

ระบุถึง flags ที่จะต้องถูก set ใน TCP header เมื่อทำการระบุโปรโตคอลเป็น TCP

**state**

กำหนดให้ระบบติดตาม state ของแพ็กเก็ตที่ตรงกับ Filter Rule ที่กำหนด โดยมีการทำงาน 3 แบบ คือ

- keep state
- modulate state
- synproxy state

**ไฟล์คอนฟิกเก็บข้อมูลสำรองของแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ (pf.conf.backup)**

ถูกสร้างขึ้นเมื่อมีการสำรองข้อมูลเกิดขึ้น ซึ่งจะเก็บอยู่ที่ /usr/local/project/backup/ โดยรูปแบบการเก็บข้อมูลจะเหมือนกับไฟล์คอนฟิกแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ที่ได้อธิบายมาแล้ว

**ไฟล์เก็บข้อมูลของระบบ (/etc/rc.conf)**

ไฟล์ข้อมูลของระบบจะใช้ข้อมูลจากไฟล์ของระบบปฏิบัติการ FreeBSD ในการจัดการข้อมูลข้อมูล ดังนั้นในการอธิบายโครงสร้างข้อมูลจึงใช้การอธิบายรูปแบบของคำสั่งที่เขียนในไฟล์คอนฟิก เพื่อให้ทราบว่าข้อมูลต่างๆที่ระบบใช้งานถูกจัดเก็บอยู่ในรูปแบบใด โดยสามารถอธิบายได้ดังนี้

**Host name และ Domain name**

เป็นข้อมูลชื่อเครื่องและโดเมนที่เครื่องอยู่ โดยมีรูปแบบการจัดเก็บในไฟล์ดังนี้

hostname="***Hoset_name.Domain_name***"

สามารถอธิบายข้อมูลในแต่ละส่วนได้ดังนี้

hostname=""

เป็นคำสั่งในการกำหนดชื่อเครื่อง

***Hoset_name***

เป็นส่วนที่เก็บข้อมูลชื่อเครื่อง

***Domain_name***

เป็นส่วนที่เก็บข้อมูลของโดเมน

**Default Router**

เป็นข้อมูล Gateway ของระบบ โดยมีรูปแบบในการจัดเก็บในไฟล์ดังนี้

defaultrouter="***Gateway_IP_Address***"

สามารถอธิบายข้อมูลในแต่ละส่วนได้ดังนี้

defaultrouter=""

เป็นคำสั่งในการกำหนดค่า Gateway

***Gateway_IP_Address***

เป็นส่วนที่เก็บค่า IP Address ของ Gateway

**Interface**

เป็นส่วนที่ใช้ในการเก็บข้อมูลของ Interface ของระบบ โดยมีรูปแบบในการจัดเก็บข้อมูลดังนี้

ifconfig_***Interface_Name*** ="***Address_Family IP_Address*** netmask ***Subnet_Mask***"

สามารถอธิบายข้อมูลในแต่ละส่วนได้ดังนี้

ifconfig_***Interface_Name*** =""

เป็นคำสั่งที่ใช้ในการกำหนดค่าให้กับ Interface

***Interface_Name***

เป็นชื่อของ Interface

***Address_Family***

เป็นส่วนที่เก็บค่า Address Family คือ inet หรือ inet6

***IP_Address***

เป็นส่วนที่เก็บค่า IP Address ของ Interface

***Subnet_Mask***

เป็นส่วนที่ใช้ในการเก็บค่า Subnet Mask ของ Interface

**ไฟล์เก็บข้อมูลของโปรแกรม (/usr/local/project/config/pfwi.conf)**

ใช้ในการเก็บข้อมูลของระบบโดยสามารถแยกออกเป็นสองส่วนคือเก็บข้อมูลของผู้ใช้และส่วนของการเก็บข้อมูลในการควบคุมการเข้าใช้ระบบ โดยสามารถอธิบายโครงสร้างในการเก็บข้อมูลได้ดังนี้

ในส่วนแรกคือการจัดเก็บข้อมูลของผู้ใช้ซึ่งประกอบด้วย

user_name="**user name**"

password="**password**"

สามารถอธิบายการจัดเก็บข้อมูลแต่ละส่วนได้ดังนี้

user_name=""

เป็นชื่อเพื่อใช้สำหรับอธิบายข้อมูลที่ถูกจัดเก็บ โดยในส่วนนี้เป็นชื่อของผู้ใช้งานระบบ

**user name**

เป็นข้อมูลชื่อของผู้ใช้ที่สามารถเข้าใช้งานระบบได้ โดยจัดเก็บเป็นลักษณะตัวอักษร

password=""

เป็นชื่อเพื่อใช้สำหรับอธิบายข้อมูลที่ถูกจัดเก็บ โดยในส่วนนี้เป็นรหัสผ่านของผู้ใช้

**password**

เป็นข้อมูลรหัสผ่านของผู้ใช้ที่สามารถเข้าใช้งานระบบได้ โดยจัดเก็บเป็นลักษณะตัวอักษร

ในส่วนที่สองคือการจัดเก็บข้อมูลที่ใช้สำหรับควบคุมการเข้าใช้งานระบบ โดยประกอบไปด้วยการจัดเก็บข้อมูลดังนี้

remote_ip="**ip address**"

remote_on_interface="**interfacename**"

สามารถอธิบายการจัดเก็บข้อมูลแต่ละส่วนได้ดังนี้

remote_ip=""

เป็นชื่อเพื่อใช้สำหรับอธิบายข้อมูลที่ถูกจัดเก็บ โดยในส่วนนี้เป็น IP Address ของเครื่องต้นทางที่อนุญาตให้เข้าใช้ระบบได้

**ip address**

เป็นข้อมูลของ IP Address ต้นทางที่อนุญาตให้เชื่อมต่อเข้ามาใช้ระบบ โดยจัดเก็บเป็นกลุ่มตัวอักษรของ IP Address

remote_on_interface=""

เป็นชื่อเพื่อใช้สำหรับอธิบายข้อมูลที่ถูกจัดเก็บ โดยในส่วนนี้เป็น Interface ของไฟร์วอลล์ที่อนุญาตให้ทำการเชื่อมต่อเข้ามาใช้งานระบบ

**interfacename**

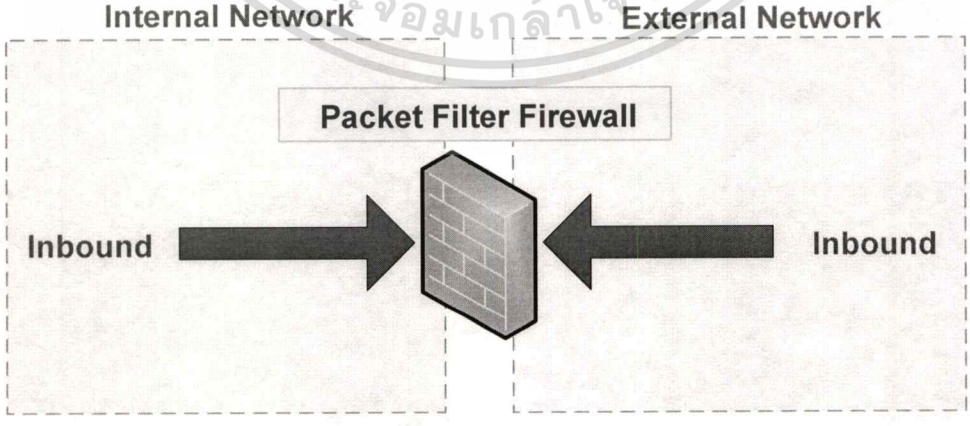
เป็นข้อมูลของ Interface ของไฟร์วอลล์ที่อนุญาตให้เชื่อมต่อเข้ามาใช้ระบบ โดยจัดเก็บเป็นกลุ่มตัวอักษรของ Interface บนไฟร์วอลล์

## 3.5 การออกแบบตัวช่วยสร้างกฎ (Wizard setup)

การออกแบบการทำงานในส่วนของตัวช่วยสร้างกฎ ผู้พัฒนาได้ใช้หลักการในการกรองข้อมูลของไฟร์วอลล์ที่แบ่งเป็นสองส่วนคือการกรองข้อมูลทางด้านเข้ามาสู่ไฟร์วอลล์ (Inbound) ซึ่งหมายถึงข้อมูลที่ถูกส่งมาจากเครือข่ายภายนอกมาที่ไฟร์วอลล์ หรือข้อมูลที่ส่งมาจากเครือข่ายภายในมายังไฟร์วอลล์ และการกรองข้อมูลออกจากไฟร์วอลล์ (Outbound) ซึ่งหมายถึงการกรองข้อมูลที่มาจากเครือข่ายภายในที่จะส่งต่อออกไปยังเครือข่ายภายนอก โดยผู้พัฒนานำหลักการทำงานทั้งสองส่วนนี้มาเป็นหลักการในการสร้างตัวช่วยสร้างกฎ สามารถอธิบายการออกแบบของทั้งสองส่วนได้ดังนี้

**การกรองข้อมูลทางด้านเข้าสู่ไฟร์วอลล์**

การออกแบบการกรองข้อมูลทางด้านเข้าสู่ไฟร์วอลล์ จะทำการพิจารณาข้อมูลทั้งที่ส่งมาจากเครือข่ายภายในและส่งมาจากเครือข่ายภายนอกเข้ามาที่ไฟร์วอลล์ โดยสามารถแสดงลักษณะการทำงานได้ดังรูปที่ 3.30




รูปที่ 3.30 แสดงการกรองข้อมูลทางด้านเข้าสู่ไฟร์วอลล์ (Inbound)

remote_on_interface=""

เป็นชื่อเพื่อใช้สำหรับอธิบายข้อมูลที่ถูกจัดเก็บ โดยในส่วนนี้เป็น Interface ของไฟร์วอลล์ที่อนุญาตให้ทำการเชื่อมต่อเข้ามาใช้งานระบบ

**interfacename**

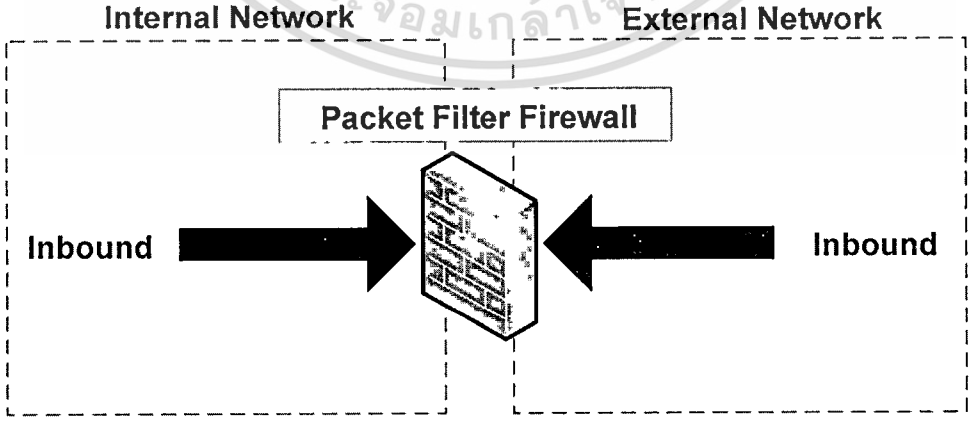
เป็นข้อมูลของ Interface ของไฟร์วอลล์ที่อนุญาตให้เชื่อมต่อเข้ามาใช้ระบบ โดยจัดเก็บเป็นกลุ่มตัวอักษรของ Interface บนไฟร์วอลล์

## 3.5 การออกแบบตัวช่วยสร้างกฎ (Wizard setup)

การออกแบบการทำงานในส่วนของตัวช่วยสร้างกฎ ผู้พัฒนาได้ใช้หลักการในการกรองข้อมูลของไฟร์วอลล์ที่แบ่งเป็นสองส่วนคือการกรองข้อมูลทางด้านเข้ามาสู่ไฟร์วอลล์ (Inbound) ซึ่งหมายถึงข้อมูลที่ถูกส่งมาจากเครือข่ายภายนอกมาที่ไฟร์วอลล์ หรือข้อมูลที่ส่งมาจากเครือข่ายภายในมายังไฟร์วอลล์ และการกรองข้อมูลออกจากไฟร์วอลล์ (Outbound) ซึ่งหมายถึงการกรองข้อมูลที่มาจากเครือข่ายภายในที่จะส่งต่อออกไปยังเครือข่ายภายนอก โดยผู้พัฒนานำหลักการทำงานทั้งสองส่วนนี้มาเป็นหลักการในการสร้างตัวช่วยสร้างกฎ สามารถอธิบายการออกแบบของทั้งสองส่วนได้ดังนี้

**การกรองข้อมูลทางด้านเข้าสู่ไฟร์วอลล์**

การออกแบบการกรองข้อมูลทางด้านเข้าสู่ไฟร์วอลล์ จะทำการพิจารณาข้อมูลทั้งที่ส่งมาจากเครือข่ายภายในและส่งมาจากเครือข่ายภายนอกเข้ามาที่ไฟร์วอลล์ โดยสามารถแสดงลักษณะการทำงานได้ดังรูปที่ 3.30




รูปที่ 3.30 แสดงการกรองข้อมูลทางด้านเข้าสู่ไฟร์วอลล์ (Inbound)

การออกแบบตัวสร้างกฎในส่วนของการกรองข้อมูลทางด้านเข้าสู่ไฟร์วอลล์ ได้มีการออกแบบให้ผู้ใช้สามารถเลือกที่จะทำการกรองข้อมูลผ่านทางหน้าจอเว็บ โดยแบ่งรูปแบบในการกรองข้อมูลออกเป็นสามรูปแบบคือ

- กรองข้อมูลด้านเข้าสู่ไฟร์วอลล์จาก IP Address เครื่องต้นทาง

เป็นการรองรับให้ผู้ใช้ทำการกำหนด IP Address เครื่องต้นทางที่จะอนุญาตให้ทำการส่งผ่าน หรือบล็อกข้อมูลของเครื่องเหล่านั้นที่ถูกส่งผ่านมาทางด้านเข้าสู่ไฟร์วอลล์

- กรองข้อมูลด้านเข้าสู่ไฟร์วอลล์จาก IP Address เครื่องปลายทาง

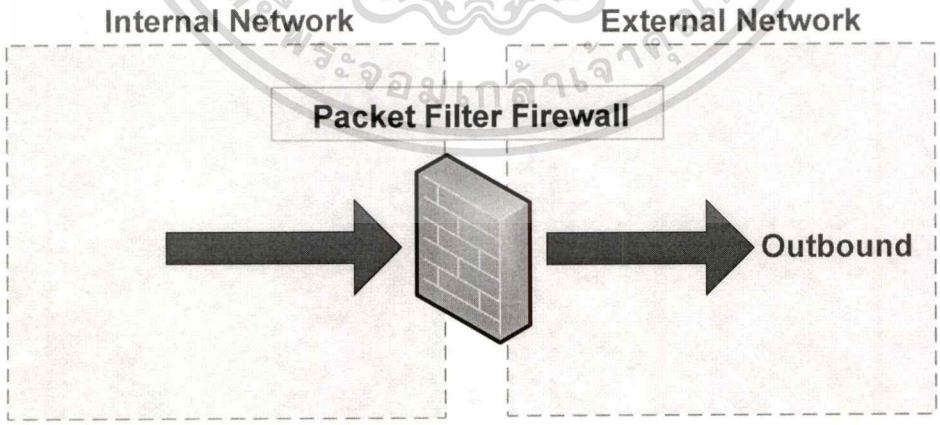
เป็นการรองรับให้ผู้ใช้ทำการกำหนด IP Address เครื่องปลายทางที่จะอนุญาตให้ทำการส่งผ่าน หรือบล็อกข้อมูลของเครื่องเหล่านั้นที่ถูกส่งผ่านมาทางด้านเข้าสู่ไฟร์วอลล์

- กรองข้อมูลด้านเข้าสู่ไฟร์วอลล์จากบริการและ IP Address เครื่องต้นทาง

เป็นการรองรับให้ผู้ใช้ทำการกำหนดบริการที่เครื่องปลายทางสามารถที่จะใช้งานได้ หรือบล็อกข้อมูลของบริการเครื่องเหล่านั้นที่ถูกส่งผ่านมาทางด้านเข้าสู่ไฟร์วอลล์ โดยบริการต่างๆผู้ใช้สามารถเลือกได้จากรายการของระบบ หรือในกรณีที่ไม่มีบริการที่ต้องการอยู่ในรายการก็สามารถกำหนดโดยระบุเป็นหมายเลขของพอร์ตของบริการตามความต้องการของผู้ใช้

**การกรองข้อมูลทางด้านออกจากไฟร์วอลล์**

การออกแบบการกรองข้อมูลทางด้านออกจากไฟร์วอลล์ จะทำการพิจารณาข้อมูลที่ส่งมาจากเครือข่ายภายในที่จะทำการส่งผ่านออกไปสู่เครือข่ายภายนอก โดยสามารถแสดงลักษณะการทำงานได้ดังรูปที่ 3.31




รูปที่ 3.31 แสดงการกรองข้อมูลทางด้านออกจากไฟร์วอลล์ (Outbound)

การออกแบบตัวสร้างกฎในส่วนของการกรองข้อมูลทางด้านเข้าสู่ไฟร์วอลล์ ได้มีการออกแบบให้ผู้ใช้สามารถเลือกที่จะทำการกรองข้อมูลผ่านทางหน้าจอเว็บ โดยแบ่งรูปแบบในการกรองข้อมูลออกเป็นสามรูปแบบคือ

- กรองข้อมูลด้านเข้าสู่ไฟร์วอลล์จาก IP Address เครื่องต้นทาง

เป็นการรองรับให้ผู้ใช้ทำการกำหนด IP Address เครื่องต้นทางที่จะอนุญาตให้ทำการส่งผ่าน หรือบล็อกข้อมูลของเครื่องเหล่านั้นที่ถูกส่งผ่านมาทางด้านเข้าสู่ไฟร์วอลล์

- กรองข้อมูลด้านเข้าสู่ไฟร์วอลล์จาก IP Address เครื่องปลายทาง

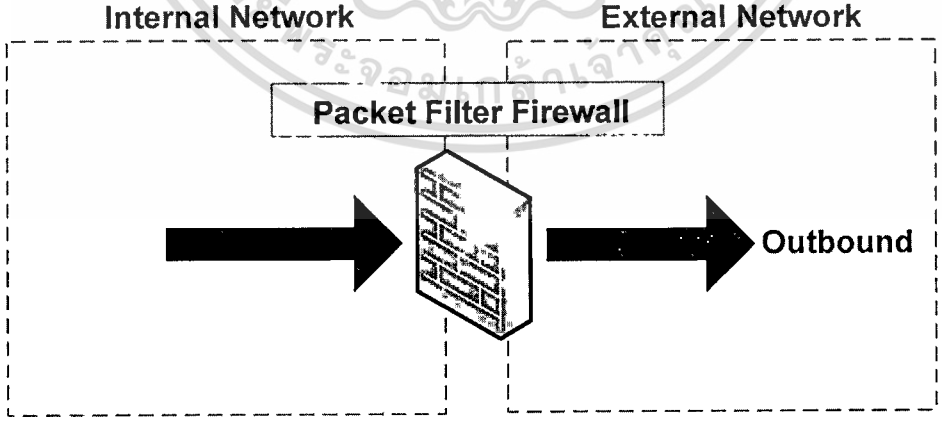
เป็นการรองรับให้ผู้ใช้ทำการกำหนด IP Address เครื่องปลายทางที่จะอนุญาตให้ทำการส่งผ่าน หรือบล็อกข้อมูลของเครื่องเหล่านั้นที่ถูกส่งผ่านมาทางด้านเข้าสู่ไฟร์วอลล์

- กรองข้อมูลด้านเข้าสู่ไฟร์วอลล์จากบริการและ IP Address เครื่องต้นทาง

เป็นการรองรับให้ผู้ใช้ทำการกำหนดบริการที่เครื่องปลายทางสามารถที่จะใช้งานได้ หรือบล็อกข้อมูลของบริการเครื่องเหล่านั้นที่ถูกส่งผ่านมาทางด้านเข้าสู่ไฟร์วอลล์ โดยบริการต่างๆผู้ใช้สามารถเลือกได้จากรายการของระบบ หรือในกรณีที่ไม่มีบริการที่ต้องการอยู่ในรายการก็สามารถกำหนดโดยระบุเป็นหมายเลขของพอร์ตของบริการตามความต้องการของผู้ใช้

**การกรองข้อมูลทางด้านออกจากไฟร์วอลล์**

การออกแบบการกรองข้อมูลทางด้านออกจากไฟร์วอลล์ จะทำการพิจารณาข้อมูลที่ส่งมาจากเครือข่ายภายในที่จะทำการส่งผ่านออกไปสู่เครือข่ายภายนอก โดยสามารถแสดงลักษณะการทำงานได้ดังรูปที่ 3.31




รูปที่ 3.31 แสดงการกรองข้อมูลทางด้านออกจากไฟร์วอลล์ (Outbound)

การออกแบบตัวสร้างกฎในส่วนของการกรองข้อมูลทางด้านออกจากไฟร์วอลล์ ได้มีการออกแบบให้ผู้ใช้สามารถเลือกที่จะทำการกรองข้อมูลผ่านทางหน้าจอเว็บ โดยแบ่งรูปแบบในการกรองข้อมูลออกเป็นสามรูปแบบคือ

- กรองข้อมูลด้านออกจากไฟร์วอลล์จาก IP Address เครื่องต้นทาง

เป็นการรองรับให้ผู้ใช้ทำการกำหนด IP Address เครื่องต้นทางที่จะอนุญาตให้ทำการส่งผ่าน หรือบล็อกข้อมูลของเครื่องเหล่านั้นที่ถูกส่งผ่านมาทางด้านออกจากไฟร์วอลล์

- กรองข้อมูลด้านออกจากไฟร์วอลล์จาก IP Address เครื่องปลายทาง

เป็นการรองรับให้ผู้ใช้ทำการกำหนด IP Address เครื่องปลายทางที่จะอนุญาตให้ทำการส่งผ่าน หรือบล็อกข้อมูลของเครื่องเหล่านั้นที่ถูกส่งผ่านมาทางด้านออกจากไฟร์วอลล์

- กรองข้อมูลด้านออกจากไฟร์วอลล์จากบริการและ IP Address เครื่องต้นทาง

เป็นการรองรับให้ผู้ใช้ทำการกำหนดบริการที่เครื่องปลายทางสามารถที่จะใช้งานได้ หรือบล็อกข้อมูลของบริการเครื่องเหล่านั้นที่ถูกส่งผ่านมาทางด้านออกจากไฟร์วอลล์ โดยบริการต่างๆผู้ใช้สามารถเลือกได้จากรายการของระบบ หรือในกรณีที่ไม่มีบริการที่ต้องการอยู่ในรายการก็สามารถกำหนดโดยระบุเป็นหมายเลขของพอร์ตของบริการตามความต้องการของผู้ใช้

หลังจากผู้ใช้ทำการกำหนดการกรองข้อมูลทางด้านเข้าสู่ไฟร์วอลล์และทางด้านออกจากไฟร์วอลล์สู่เครือข่ายภายนอกแล้วระบบจะทำการสร้างกฎ และแสดงรายการกฎให้กับผู้ใช้ได้ตรวจสอบกฎที่ระบบได้สร้างขึ้น จากนั้นก็จะรอการยืนยันการใช้งานกฎที่สร้างขึ้นจากผู้ใช้เพื่อส่งข้อมูลกฎให้กับแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ ให้เริ่มต้นทำงานตามกฎและเขียนข้อมูลของกฎที่ได้สร้างขึ้นลงในไฟร์หลักที่ใช้เก็บกฎของแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ (/etc/pf.conf) ซึ่งจะจบการทำงานในส่วนของตัวช่วยในการสร้างกฎที่ได้ออกแบบ

การออกแบบตัวสร้างกฎในส่วนของการกรองข้อมูลทางด้านออกจากไฟร์วอลล์ ได้มีการออกแบบให้ผู้ใช้สามารถเลือกที่จะทำการกรองข้อมูลผ่านทางหน้าจอเว็บ โดยแบ่งรูปแบบในการกรองข้อมูลออกเป็นสามรูปแบบคือ

- กรองข้อมูลด้านออกจากไฟร์วอลล์จาก IP Address เครื่องต้นทาง

เป็นการรองรับให้ผู้ใช้ทำการกำหนด IP Address เครื่องต้นทางที่จะอนุญาตให้ทำการส่งผ่าน หรือบล็อกข้อมูลของเครื่องเหล่านั้นที่ถูกส่งผ่านมาทางด้านออกจากไฟร์วอลล์

- กรองข้อมูลด้านออกจากไฟร์วอลล์จาก IP Address เครื่องปลายทาง

เป็นการรองรับให้ผู้ใช้ทำการกำหนด IP Address เครื่องปลายทางที่จะอนุญาตให้ทำการส่งผ่าน หรือบล็อกข้อมูลของเครื่องเหล่านั้นที่ถูกส่งผ่านมาทางด้านออกจากไฟร์วอลล์

- กรองข้อมูลด้านออกจากไฟร์วอลล์จากบริการและ IP Address เครื่องต้นทาง

เป็นการรองรับให้ผู้ใช้ทำการกำหนดบริการที่เครื่องปลายทางสามารถที่จะใช้งานได้ หรือบล็อกข้อมูลของบริการเครื่องเหล่านั้นที่ถูกส่งผ่านมาทางด้านออกจากไฟร์วอลล์ โดยบริการต่างๆผู้ใช้สามารถเลือกได้จากรายการของระบบ หรือในกรณีที่ไม่มีบริการที่ต้องการอยู่ในรายการก็สามารถกำหนดโดยระบุเป็นหมายเลขของพอร์ตของบริการตามความต้องการของผู้ใช้

หลังจากผู้ใช้ทำการกำหนดการกรองข้อมูลทางด้านเข้าสู่ไฟร์วอลล์และทางด้านออกจากไฟร์วอลล์สู่เครือข่ายภายนอกแล้วระบบจะทำการสร้างกฎ และแสดงรายการกฎให้กับผู้ใช้ได้ตรวจสอบกฎที่ระบบได้สร้างขึ้น จากนั้นก็จะรอการยืนยันการใช้งานกฎที่สร้างขึ้นจากผู้ใช้เพื่อส่งข้อมูลกฎให้กับแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ ให้เริ่มต้นทำงานตามกฎและเขียนข้อมูลของกฎที่ได้สร้างขึ้นลงในไฟร์หลักที่ใช้เก็บกฎของแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ (/etc/pf.conf) ซึ่งจะจบการทำงานในส่วนของตัวช่วยในการสร้างกฎที่ได้ออกแบบ

# บทที่ 4
# การพัฒนาระบบ

ในการพัฒนาระบบใช้งานส่วนต่อประสานแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์สำหรับผู้ใช้ผ่านเว็บ ได้มีการกำหนดขั้นตอนในการพัฒนาดังนี้

## 4.1 การวางแผนปฏิบัติงาน

การพัฒนาระบบได้เลือกใช้งานซอฟต์แวร์ดังต่อไปนี้

1. **ระบบปฏิบัติการเลือกใช้ FreeBSD 6.2**

   เป็นระบบปฏิบัติการที่ได้รับความนิยมอย่างแพร่หลาย และไม่ต้องมีค่าใช้จ่าย โดยสามารถดาวน์โหลดซอฟต์แวร์ระบบปฏิบัติการ FreeBSD ได้จาก ftp.FreeBSD.org และระบบปฏิบัติการ FreeBSD ยังมีซอฟต์แวร์แอพพลิเคชั่นให้ใช้งานหลากหลาย ซึ่งทำให้ระบบปฏิบัติการ FreeBSD สามารถตอบสนองความต้องการของระบบต่างๆ เช่น ระบบเว็บเซิร์ฟเวอร์ ระบบเมล์เซิร์ฟเวอร์ ระบบไฟร์วอลล์ ฯลฯ

2. **ซอฟต์แวร์ไฟร์วอลล์เลือกใช้แพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ (Packet Filter Firewall)**

   แพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ เป็นระบบที่ถูกติดตั้งมากับระบบปฏิบัติการ FreeBSD โดยสามารถเริ่มต้นการทำงานได้ในภายหลัง โดยการควบคุมการทำงานของแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ สามารถทำผ่านทาง Command line โดยผู้ใช้สามารถกำหนดการทำงานผ่านทางพิมพ์คำสั่งต่างๆ

3. **ซอฟต์แวร์ภาษา เลือกใช้ JSP (Java Server Page)**

   JSP เป็นเทคโนโลยีที่ทำงานบนเซิร์ฟเวอร์ (Server Side Script) มีความสามารถในการจัดการกับเว็บแอปพลิเคชั่นแบบ Dynamic Content ทำให้ข้อมูลบนเว็บมีการเปลี่ยนแปลงโดยอัตโนมัติ โดย JSP มีความสามารถในการรองรับการพัฒนาระบบเว็บแอปพลิเคชั่นขนาดใหญ่ และมีอิสระกับ Platform ต่างๆ

4. **เว็บเซิร์ฟเวอร์ที่รองรับการทำงานของ JSP เลือกใช้ Apache Tomcat 5.0**

   Apache Tomcat เป็นซอฟแวร์สำหรับให้บริการเว็บเซิร์ฟเวอร์ (HTTP/Web Server) ผ่านทางโปรโตคอล HTTP โดยเป็นซอฟแวร์แบบ Open Source สามารถนำมาใช้งานได้โดยไม่มีค่าใช้จ่าย และรองรับการทำงานร่วมกับ JSP โดยสามารถดาวน์โหลดซอฟต์แวร์มาติดตั้งได้ที่ http://jakarta.apache.org/tomcat/

# บทที่ 4
# การพัฒนาระบบ

ในการพัฒนาระบบใช้งานส่วนต่อประสานแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์สำหรับผู้ใช้ผ่านเว็บ ได้มีการกำหนดขั้นตอนในการพัฒนาดังนี้

## 4.1 การวางแผนปฏิบัติงาน

การพัฒนาระบบได้เลือกใช้งานซอฟต์แวร์ดังต่อไปนี้

1. **ระบบปฏิบัติการเลือกใช้ FreeBSD 6.2**

   เป็นระบบปฏิบัติการที่ได้รับความนิยมอย่างแพร่หลาย และไม่ต้องมีค่าใช้จ่าย โดยสามารถดาวน์โหลดซอฟต์แวร์ระบบปฏิบัติการ FreeBSD ได้จาก ftp.FreeBSD.org และระบบปฏิบัติการ FreeBSD ยังมีซอฟต์แวร์แอพพลิเคชั่นให้ใช้งานหลากหลาย ซึ่งทำให้ระบบปฏิบัติการ FreeBSD สามารถตอบสนองความต้องการของระบบต่างๆ เช่น ระบบเว็บเซิร์ฟเวอร์ ระบบเมล์เซิร์ฟเวอร์ ระบบไฟร์วอลล์ ฯลฯ

2. **ซอฟต์แวร์ไฟร์วอลล์เลือกใช้แพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ (Packet Filter Firewall)**

   แพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ เป็นระบบที่ถูกติดตั้งมากับระบบปฏิบัติการ FreeBSD โดยสามารถเริ่มต้นการทำงานได้ในภายหลัง โดยการควบคุมการทำงานของแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ สามารถทำผ่านทาง Command line โดยผู้ใช้สามารถกำหนดการทำงานผ่านทางพิมพ์คำสั่งต่างๆ

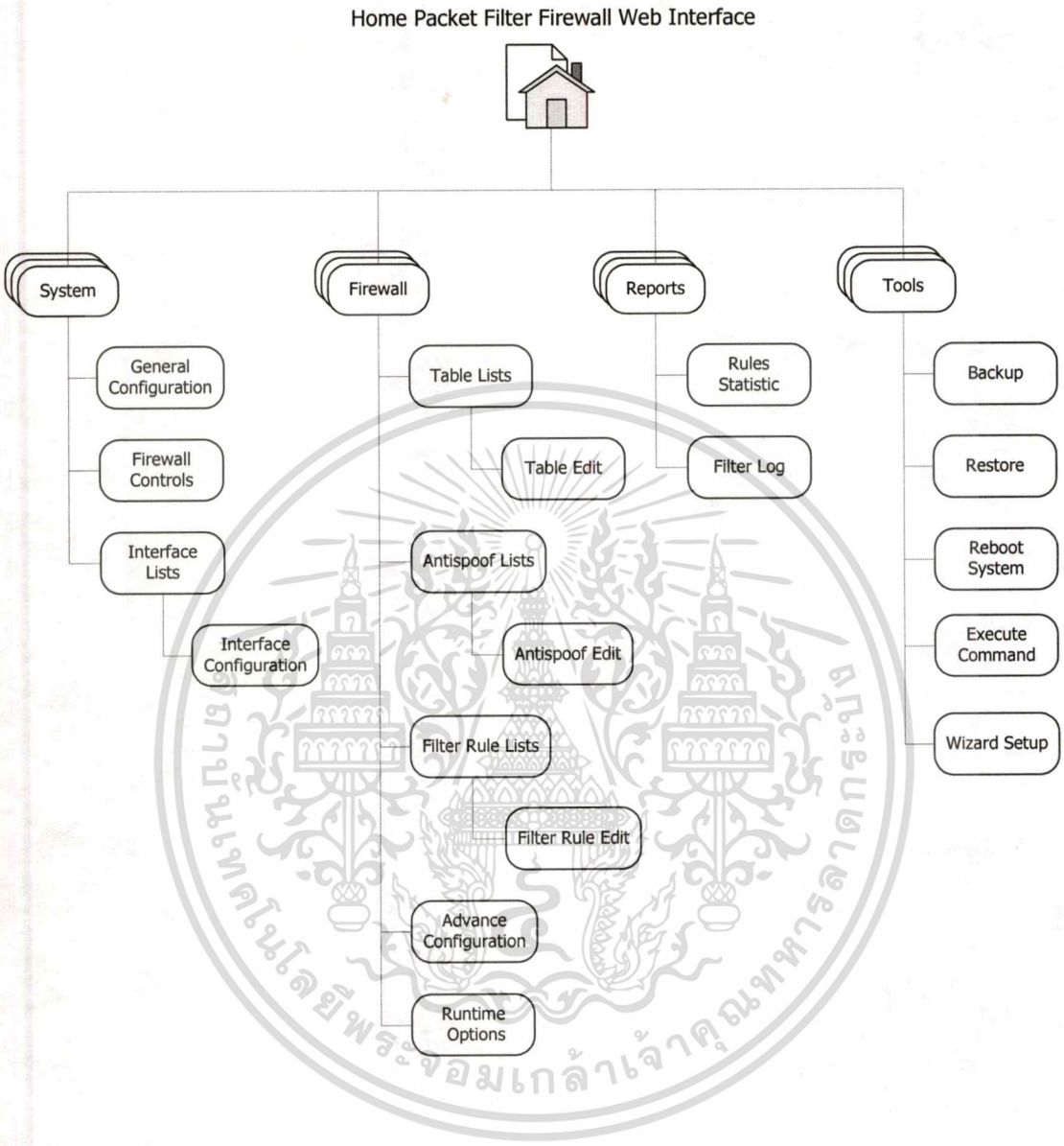
3. **ซอฟต์แวร์ภาษา เลือกใช้ JSP (Java Server Page)**

   JSP เป็นเทคโนโลยีที่ทำงานบนเซิร์ฟเวอร์ (Server Side Script) มีความสามารถในการจัดการกับเว็บแอปพลิเคชั่นแบบ Dynamic Content ทำให้ข้อมูลบนเว็บมีการเปลี่ยนแปลงโดยอัตโนมัติ โดย JSP มีความสามารถในการรองรับการพัฒนาระบบเว็บแอปพลิเคชั่นขนาดใหญ่ และมีอิสระกับ Platform ต่างๆ

4. **เว็บเซิร์ฟเวอร์ที่รองรับการทำงานของ JSP เลือกใช้ Apache Tomcat 5.0**

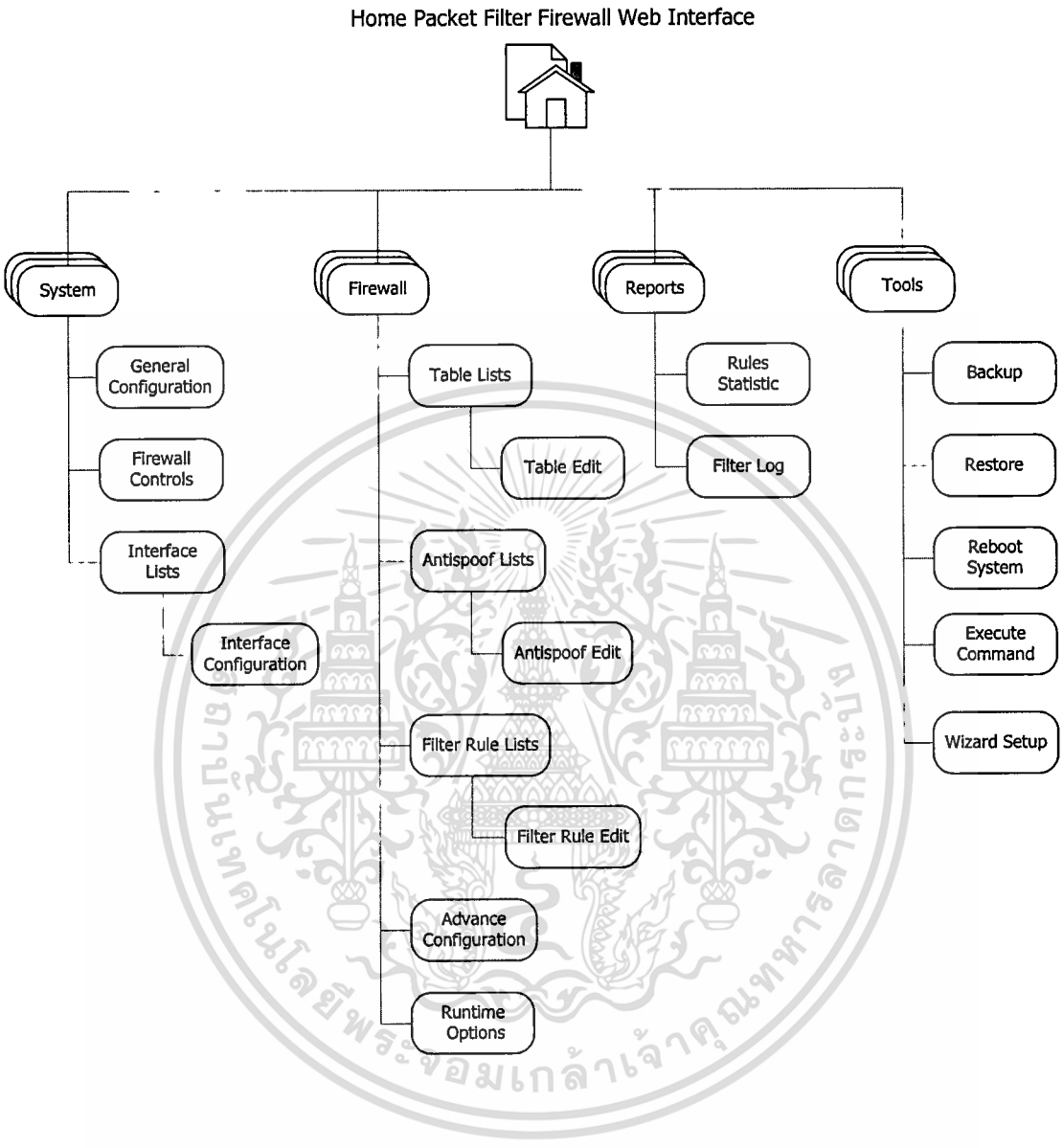
   Apache Tomcat เป็นซอฟแวร์สำหรับให้บริการเว็บเซิร์ฟเวอร์ (HTTP/Web Server) ผ่านทางโปรโตคอล HTTP โดยเป็นซอฟแวร์แบบ Open Source สามารถนำมาใช้งานได้โดยไม่มีค่าใช้จ่าย และรองรับการทำงานร่วมกับ JSP โดยสามารถดาวน์โหลดซอฟต์แวร์มาติดตั้งได้ที่ http://jakarta.apache.org/tomcat/

## 4.2 แผนภาพการแตกฟังก์ชั่นการทำงานของระบบ




**รูปที่ 4.1** แผนผังการทำงานของโปรแกรม

## 4.2 แผนภาพการแตกฟังก์ชั่นการทำงานของระบบ




**รูปที่ 4.1** แผนผังการทำงานของโปรแกรม

## 4.3 การพัฒนาระบบ

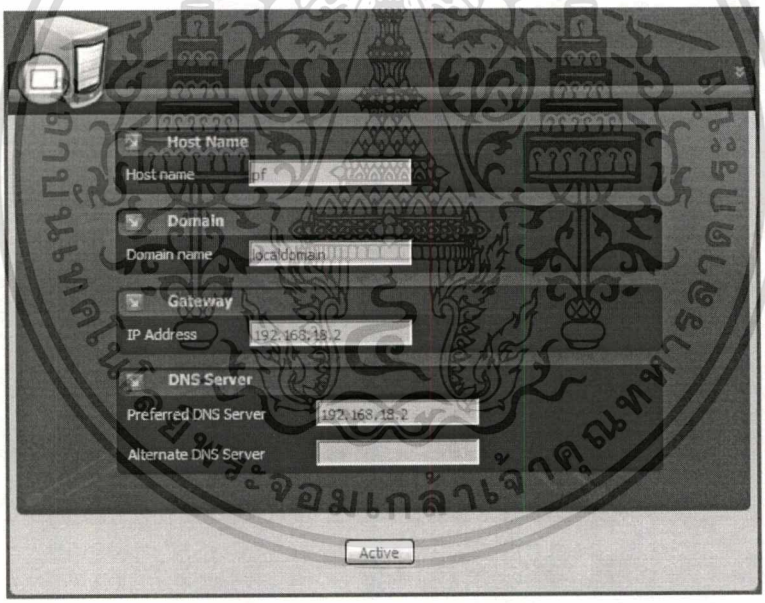
จากแผนภาพการแตกฟังก์ชั่นการทำงานของระบบ สามารถแบ่งการพัฒนาระบบออกเป็น 4 ส่วนโดยสามารถอธิบายการพัฒนาระบบแต่ระส่วนได้ดังต่อไปนี้

**1. กลุ่มหน้าเว็บ System**

ประกอบด้วยหน้าเว็บที่ใช้ในการกำหนดลักษณะและคุณสมบัติต่างๆของระบบปฏิบัติการ FreeBSD รวมทั้งการควบคุมแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ โดยประกอบด้วยหน้าเว็บดังต่อไปนี้

**1.1 General Configuration**

ใช้สำหรับการกำหนดค่าคุณสมบัติต่างๆ ที่เกี่ยวข้องกับตัวระบบปฏิบัติการเช่น Host name, Domain, Gateway และ DNS Server โดยสามารถแสดงรายละเอียดของหน้าเว็บ General Configuration ได้ดังรูปที่ 4.2




**รูปที่ 4.2** แสดงหน้าเว็บ General Configuration

**1.2 Firewall Controls**

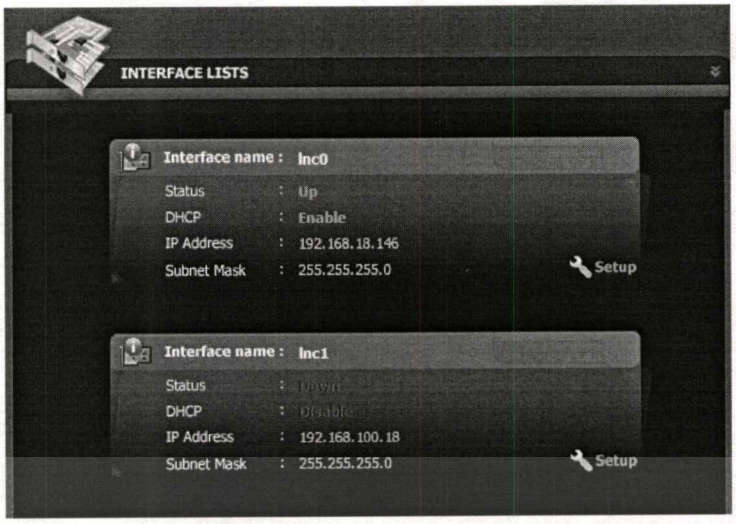
ใช้สำหรับควบคุมการทำงานของแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ และสามารถดูข้อมูลที่เป็นภาพรวมของไฟร์วอลล์ในปัจจุบันได้ ซึ่งภายในหน้าเว็บ Firewall Controlsประกอบด้วยสวนแสดงผลของสถานะ (Status) ของไฟร์วอลล์ และช่วงเวลาที่ไฟร์วอลล์ทำงาน (Live Time) และ

ส่วนที่ใช้ควบคุมสถานะของไฟร์วอลล์ นอกจากนั้นยังสามารถเรียกดูข้อมูลโดยสรุปของไฟร์วอลล์ โดยหน้าเว็บ Firewall Controls สามารถแสดงได้ดังรูปที่ 4.3


**รูปที่ 4.3** แสดงหน้าเว็บ Firewall Controls

**1.3 Interface Lists**

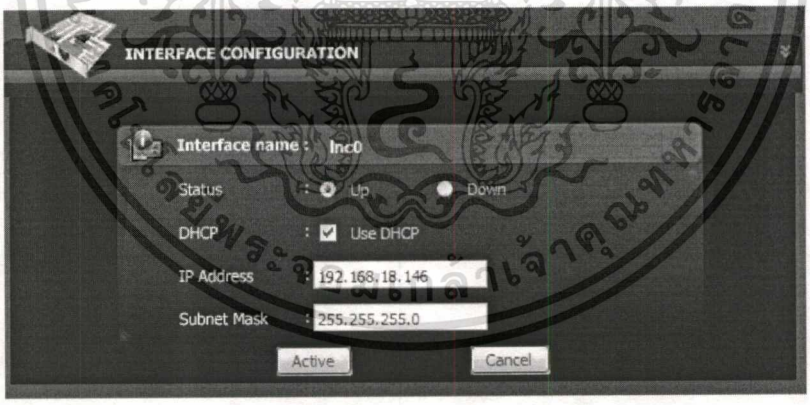
หน้าเว็บแสดง Network Interface ของระบบ โดยประกอบไปด้วยรายละเอียดต่างๆของ Network Interface เช่น สถานะของ Network Interface หรือการใช้งาน DHCP รวมถึงค่า IP Address และ Subnet Mask โดยหน้าเว็บ Interface Lists มีรายละเอียดดังแสดงในรูปที่ 4.4




**รูปที่ 4.4** แสดงหน้าเว็บ Interface Lists

**1.4 Interface Configuration**

หน้าเว็บสำหรับกำหนดค่าและคุณสมบัติต่างๆ ให้กับ Network Interface โดยสามารถกำหนดค่าของ สถานะ (Status), การใช้งาน DHCP, IP Address และSubnet Mask ซึ่งสามารถแสดงรายละเอียดของหน้าเว็บได้ดังรูปที่ 4.5



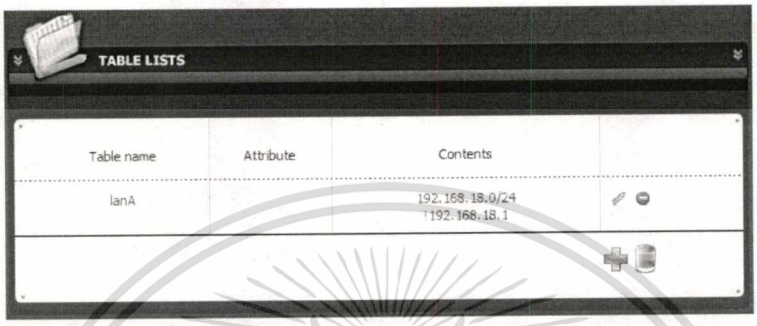

**รูปที่ 4.5** แสดงหน้าเว็บ Interface Configuration

**2. กลุ่มหน้าเว็บ Firewall**

ประกอบด้วยหน้าเว็บที่ใช้ในการจัดการกับกฎ เช่น การสร้าง การแก้ไข การลบ หรือการเปลี่ยนแปลงลำดับของกฎ และกำหนดค่าการทำงานต่างๆของแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ โดยประกอบไปด้วยกลุ่มหน้าเว็บที่มีรายละเอียดและการทำงานดังต่อไปนี้

### 2.1 Table Lists

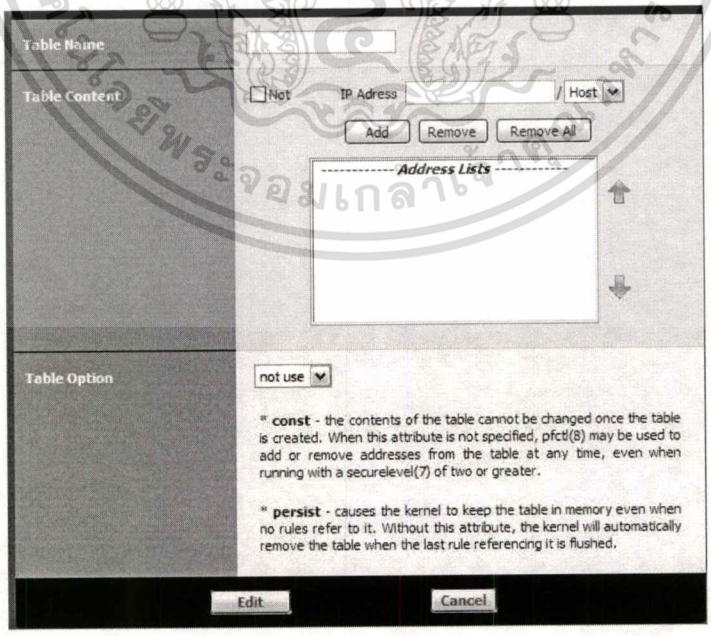
หน้าเว็บสำหรับแสดง Table ที่มีอยู่ในไฟร์วอลล์ โดยจะแสดงรายละเอียดในลักษณะของตาราง ซึ่งประกอบด้วย ชื่อของตาราง (Table name), Attribute และข้อมูลที่เก็บอยู่ในตาราง นอกจากนั้นยังมีเครื่องมือสำหรับจัดการกับตาราง เช่น การเพิ่มตาราง (Add), การแก้ไข (Edit) และการลบตาราง (Delete) โดยรายละเอียดของหน้าเว็บ Table Lists สามารถแสดงได้ดังรูปที่ 4.6




**รูปที่ 4.6** แสดงหน้าเว็บ Table Lists

### 2.2 Table Edit

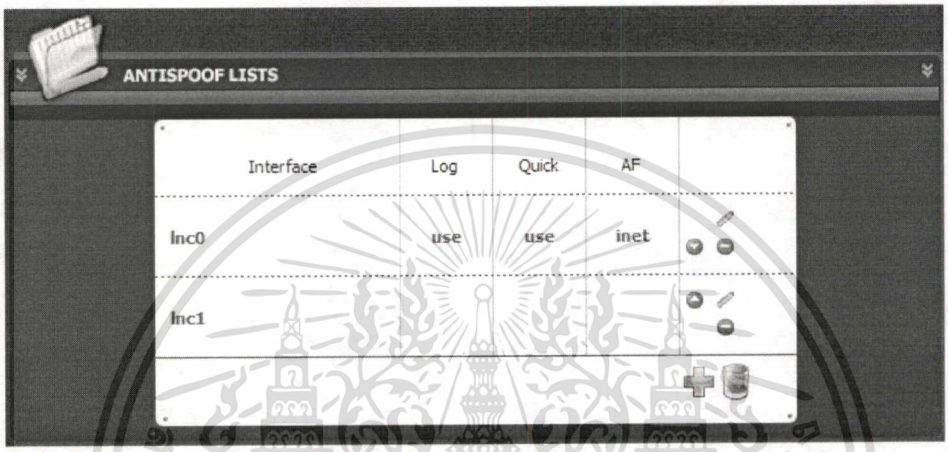
หน้าเว็บสำหรับแก้ไขและกำหนดค่าต่างๆให้กับ Table เช่น ชื่อของ Table และข้อมูลของ IP Address ที่อยู่ภายใน Table โดยสามารถแสดงรายละเอียดของหน้าเว็บ Table Editได้ดังรูปที่ 4.7




**รูปที่ 4.7** แสดงหน้าเว็บ Table Edit

**2.3 Antispoof Lists**

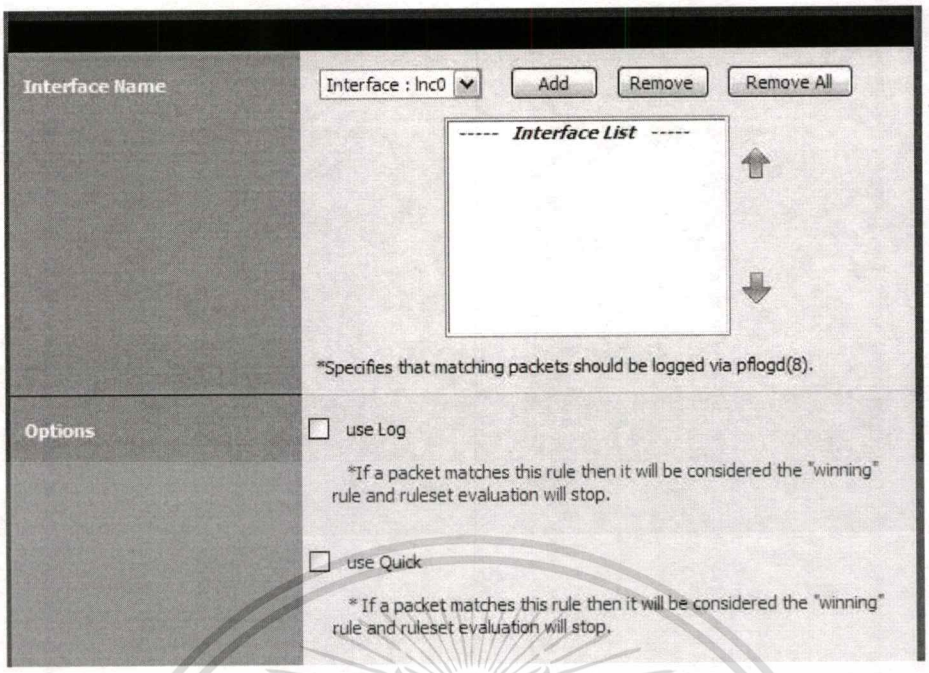
หน้าเว็บสำหรับแสดงกฎ Antispoof ที่มีอยู่ในไฟร์วอลล์ โดยจะแสดงรายละเอียดในลักษณะของตาราง ซึ่งประกอบด้วย ชื่อของ Interface, สถานะของคำสั่ง Log, สถานะของคำสั่ง Quick และค่าของ Address Family (AF) นอกจากนั้นยังมีเครื่องมือสำหรับจัดการกับกฎ เช่น การเพิ่มกฎ (Add), การแก้ไขกฎ (Edit) และการลบกฎ (Delete) โดยรายละเอียดของหน้าเว็บ Antispoof Lists สามารถแสดงได้ดังรูปที่ 4.8




**รูปที่ 4.8** แสดงหน้าเว็บ Antispoof Lists

**2.4 Antispoof Edit**

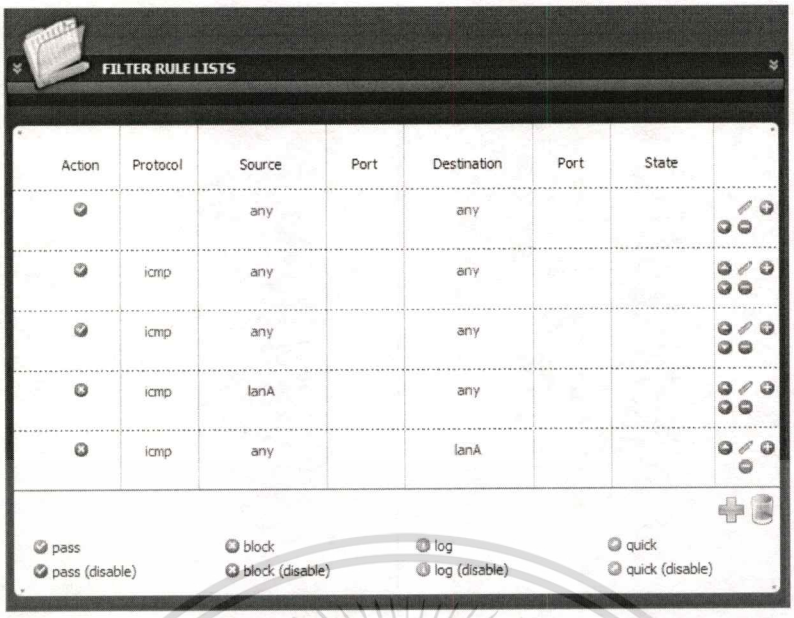
หน้าเว็บสำหรับกำหนดค่าต่างๆให้กับกฎ Antispoof เช่น การกำหนดกลุ่ม Network Interface ที่จะถูกใช้งานในกฎ และ Option ต่างๆของกฎ โดยหน้าเว็บ Antispoof Edit สามารถแสดงได้ดังรูปที่ 4.9




**รูปที่ 4.9** แสดงหน้าเว็บ Antispoof Edit

**2.5 Filter Rule Lists**

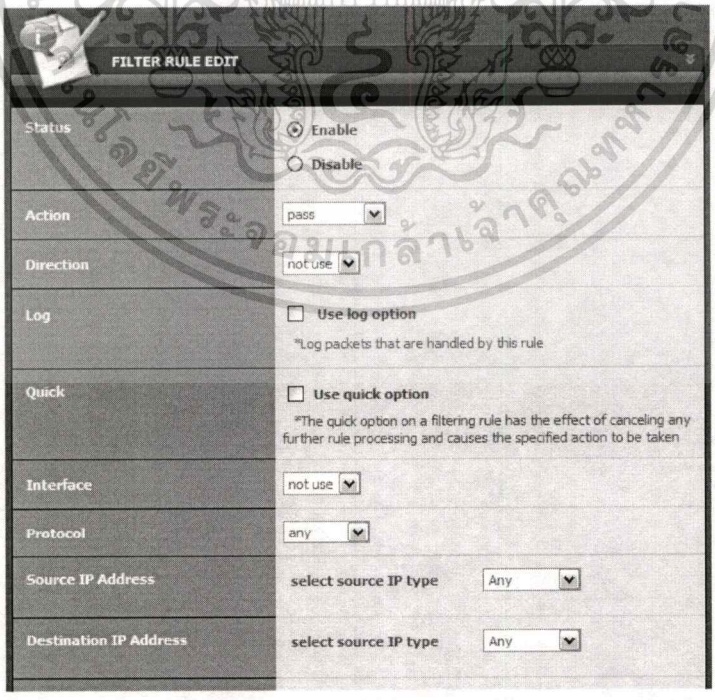
หน้าเว็บสำหรับแสดงกฎ Filter ที่มีอยู่ในไฟร์วอลล์ โดยจะแสดงรายละเอียดในลักษณะของตาราง ซึ่งแสดงค่าที่กำหนดภายในตาราง เช่น Action การทำงานของกฎ, Protocol ที่ทำการตรวจสอบ และข้อมูลของต้นทางและปลายทางที่ใช้ในการตรวจสอบแพ็กเก็ตกับกฎ นอกจากนั้นยังมีเครื่องมือสำหรับจัดการกับกฎ เช่น การเพิ่มกฎ (Add), การแก้ไขกฎ (Edit), การลบกฎ (Delete) และการปรับเปลี่ยนลำดับของกฎ (Move) โดยรายละเอียดของหน้าเว็บ Filter Rule Lists สามารถแสดงได้ดังรูปที่ 4.10




**รูปที่ 4.10** แสดงหน้าเว็บ Filter Rule Lists

**2.6 Filter Rule Edit**

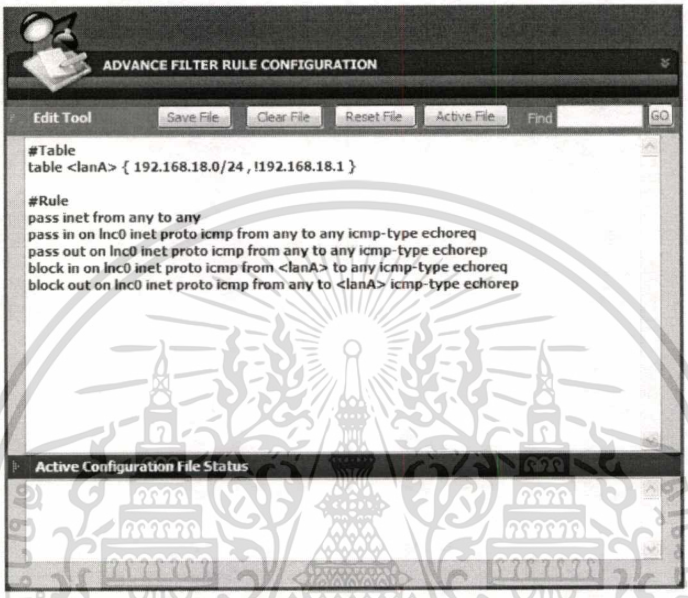
หน้าเว็บสำหรับแก้ไขและกำหนดค่าต่างๆให้กับ Filter Rule โดยสามารถแสดงรายละเอียดของหน้าเว็บ Table Edit ได้ดังรูปที่ 4.11




**รูปที่ 4.11** แสดงหน้าเว็บ Filter Rule Edit

### 2.7 Advance Configuration

ใช้สำหรับการแก้ไขกฎและค่าต่างๆภายในไฟล์ที่เก็บค่าของไฟร์วอลล์(/etc/pf.conf) โดยสามารถทำการแก้ไขข้อมูลภายในไฟล์โดยการพิมพ์ข้อมูลเข้าสู่ไฟล์ และสามารถทำการบันทึก (Save file) และเริ่มต้นการทำงานของไฟล์ที่ได้ทำการแก้ไข (Active) โดยสามารถแสดงรายละเอียดของเว็บ Advance Configuration ได้ดังรูปที่ 4.12




**รูปที่ 4.12** แสดงหน้าเว็บ Advance Configuration

### 2.8 Runtime Options

หน้าเว็บสำหรับแก้ไขและกำหนดค่าต่างๆให้กับ Runtime Options เช่น โดยสามารถแสดงรายละเอียดของหน้าเว็บ Runtime Options ได้ดังรูปที่ 4.13

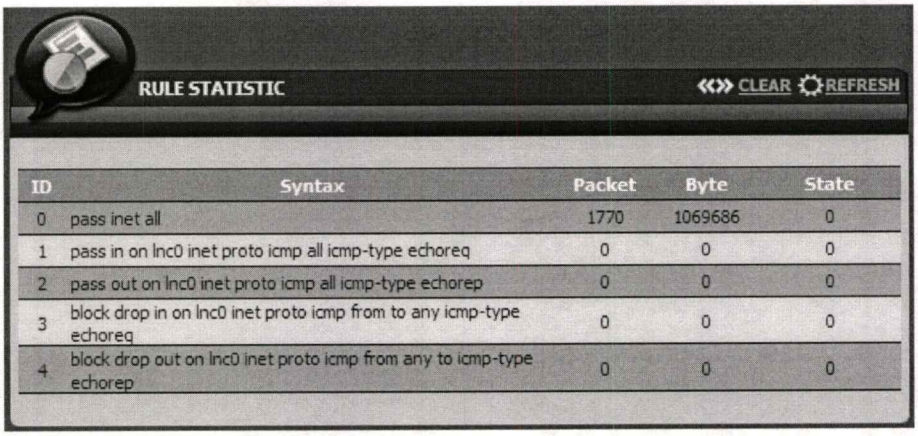

**รูปที่ 4.13** แสดงหน้าเว็บ Runtime Options

**3. กลุ่มหน้าเว็บ Reports**

ประกอบด้วยหน้าเว็บที่ใช้สำหรับเรียกดูรายงานของระบบ โดยมีรายงานให้เลือกสองแบบคือ Filter Rule Statistic Report และ Log Report โดยสามารถอธิบายรายละเอียดของรายงานแต่ละแบบได้ดังนี้

**3.1 Filter Rule Statistic Report**

แสดงรายงานทางด้านสถิติของกฎที่ทำงานอยู่ในไฟร์วอลล์ โดยมีการรายงานผลในลักษณะของตาราง และมีการบอกถึงรายละเอียดของ หมายเลขกฎ(Rule ID), รูปประโยคของกฎ (Rule Syntax), แพ็กเก็ตที่ตรงกับกฎ (Packet), ขนาดข้อมูลทั้งหมด (Byte) และจำนวนของ State ที่เกิดจากกฎ นอกจากนั้นยังสามารถลบค่าที่เก็บไว้ทั้งหมดออกเริ่มต้นใหม่ โดยใช้ปุ่ม Clear เพื่อลบค่าทั้งหมด โดยสามารถแสดงรายละเอียดของหน้าเว็บ Filter Rule Statistic Report ได้ดังรูปที่ 4.14



RULE STATISTIC

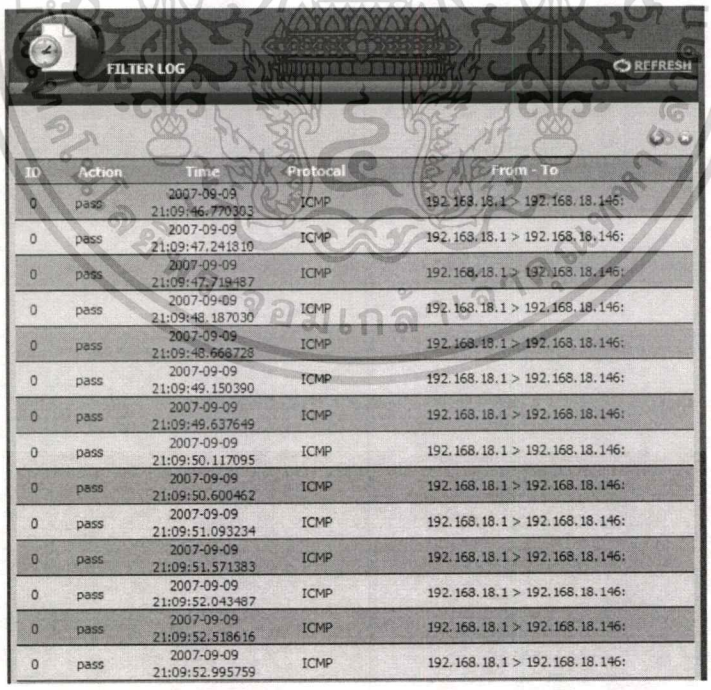
CLEAR REFRESH

| ID | Syntax | Packet | Byte | State |
|---|---|---|---|---|
| 0 | pass inet all | 1770 | 1069686 | 0 |
| 1 | pass in on lnc0 inet proto icmp all icmp-type echoreq | 0 | 0 | 0 |
| 2 | pass out on lnc0 inet proto icmp all icmp-type echorep | 0 | 0 | 0 |
| 3 | block drop in on lnc0 inet proto icmp from to any icmp-type echoreq | 0 | 0 | 0 |
| 4 | block drop out on lnc0 inet proto icmp from any to icmp-type echorep | 0 | 0 | 0 |

**รูปที่ 4.14** แสดงหน้าเว็บ Filter Rule Statistic Report

### 3.2 Log Report

แสดงรายงานข้อมูลที่เกิดจากการเก็บ Log ของกฎต่างๆ ที่เกิดขึ้น โดยมีการรายงานผลในลักษณะของตาราง และมีการบอกถึงรายละเอียดของ หมายเลขกฎ (Rule ID), Action, ช่วงเวลาที่ข้อมูลถูกเก็บ (Time), โปรโตคอล (Protocol) และต้นทางกับปลายทางของข้อมูล (From - To) สามารถแสดงรายละเอียดของหน้าเว็บ Log Report ได้ดังรูปที่ 4.15



FILTER LOG

REFRESH

| ID | Action | Time | Protocal | From - To |
|---|---|---|---|---|
| 0 | pass | 2007-09-09 21:09:46.770303 | ICMP | 192.168.18.1 > 192.168.18.146: |
| 0 | pass | 2007-09-09 21:09:47.241810 | ICMP | 192.168.18.1 > 192.168.18.146: |
| 0 | pass | 2007-09-09 21:09:47.718487 | ICMP | 192.168.18.1 > 192.168.18.146: |
| 0 | pass | 2007-09-09 21:09:48.187030 | ICMP | 192.168.18.1 > 192.168.18.146: |
| 0 | pass | 2007-09-09 21:09:48.666728 | ICMP | 192.168.18.1 > 192.168.18.146: |
| 0 | pass | 2007-09-09 21:09:49.150390 | ICMP | 192.168.18.1 > 192.168.18.146: |
| 0 | pass | 2007-09-09 21:09:49.637649 | ICMP | 192.168.18.1 > 192.168.18.146: |
| 0 | pass | 2007-09-09 21:09:50.117095 | ICMP | 192.168.18.1 > 192.168.18.146: |
| 0 | pass | 2007-09-09 21:09:50.600462 | ICMP | 192.168.18.1 > 192.168.18.146: |
| 0 | pass | 2007-09-09 21:09:51.093234 | ICMP | 192.168.18.1 > 192.168.18.146: |
| 0 | pass | 2007-09-09 21:09:51.571383 | ICMP | 192.168.18.1 > 192.168.18.146: |
| 0 | pass | 2007-09-09 21:09:52.043487 | ICMP | 192.168.18.1 > 192.168.18.146: |
| 0 | pass | 2007-09-09 21:09:52.518616 | ICMP | 192.168.18.1 > 192.168.18.146: |
| 0 | pass | 2007-09-09 21:09:52.995759 | ICMP | 192.168.18.1 > 192.168.18.146: |

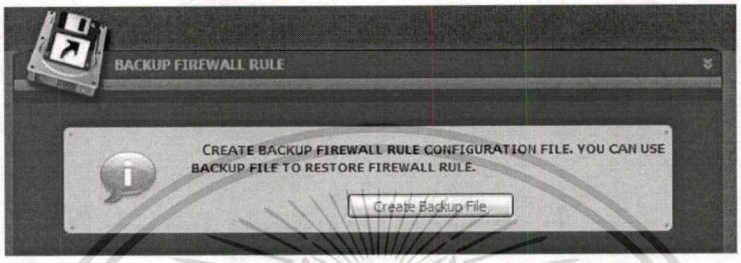
**รูปที่ 4.15** แสดงหน้าเว็บ Log Report

**4. กลุ่มหน้าเว็บ Tools**

ประกอบด้วยหน้าเว็บที่ใช้เป็นเครื่องมือในการจัดการและดูแลระบบ โดยประกอบด้วยหน้าเว็บต่างๆ ดังต่อไปนี้

**4.1 Backup**

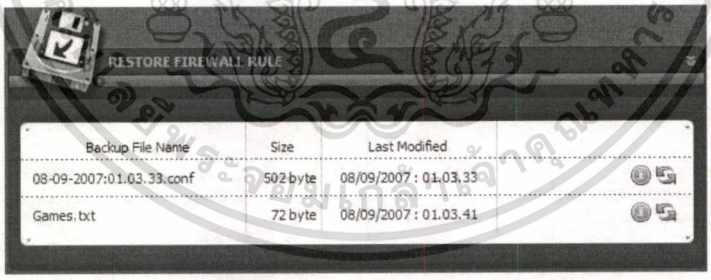
หน้าเว็บสำหรับทำการสำรองข้อมูลของไฟร์วอลล์ โดยสามารถแสดงรายละเอียดของหน้าเว็บ Backup ได้ดังรูป 4.16




**รูปที่ 4.16** แสดงหน้าเว็บ Backup

**4.2 Restore**

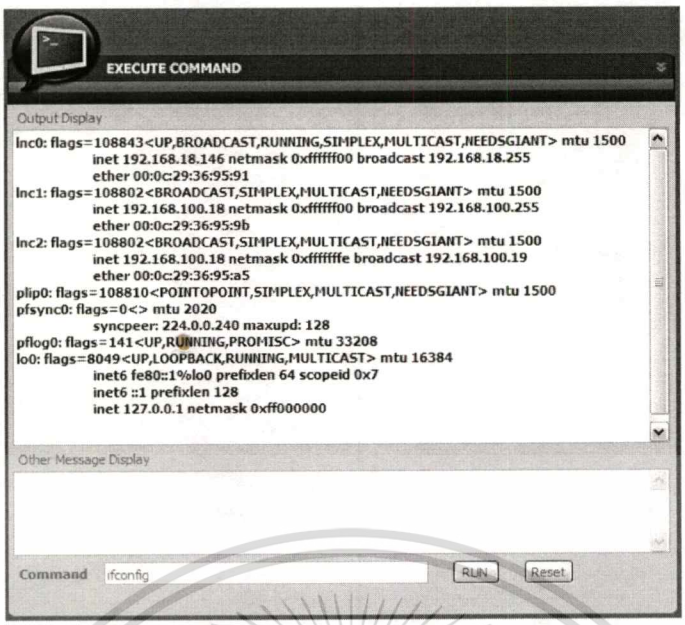
หน้าเว็บสำหรับนำค่าข้อมูลของไฟร์วอลล์ที่ได้ทำการสำรองไว้ มาใช้งาน โดยสามารถแสดงรายละเอียดของหน้าเว็บ Restore ได้ดังรูป 4.17




**รูปที่ 4.17** แสดงหน้าเว็บ Restore

**4.3 Execute Command**

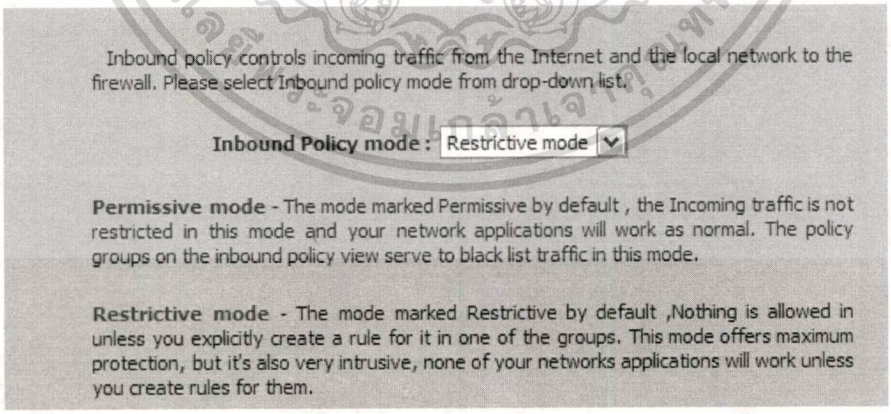
ใช้ในการสั่งคำสั่งต่างๆ ผ่านทางหน้าเว็บ สามารถแสดงผลลัพธ์ของคำสั่ง และความผิดพลาด(Error) ของคำสั่งที่เกิดขึ้น โดยรายละเอียดของหน้าเว็บ Execute Command สามารถแสดงได้ดังรูป 4.18




**รูปที่ 4.18** แสดงหน้าเว็บ Execute Command

### 4.5 Wizard Setup

เพื่อช่วยอำนวยความสะดวกในการติดตั้งกฎต่างๆ หน้าเว็บ Wizard Setup จะทำการสร้างกฎต่างๆให้โดยอัตโนมัติ ซึ่งผู้ใช้จะต้องกำหนดคุณลักษณะต่างๆ ของไฟร์วอลล์ที่ต้องการ จากนั้นกฎจะถูกสร้างขึ้นตามคุณสมบัติที่ได้กำหนดไว้ โดยสามารถแสดงตัวอย่างของหน้าเว็บ Wizard setup ได้ดังรูป 4.19




**รูปที่ 4.19** แสดงหน้าเว็บ Wizard Setup

## 4.4 การทดสอบระบบ

การทดสอบการทำงานของโปรแกรมจะทำการทดสอบโดยการใช้โปรแกรม Ping จากเครื่องคอมพิวเตอร์ที่เชื่อมต่ออยู่กับไฟร์วอลล์เข้ามาที่ไฟร์วอลล์ และในระหว่างการทำการทดสอบจะมีการปรับเปลี่ยนกฎ เพื่อทำการทดสอบการทำงานของโปรแกรม โดยในการทดลองจะมีการติดตามดูการเปลี่ยนแปลงของกฎภายในไฟร์วอลล์ ผ่านทางคำสั่ง pfctl –sr และติดตามดูการปรับเปลี่ยนข้อมูลในไฟล์ /etc/pf.conf อีกด้วย

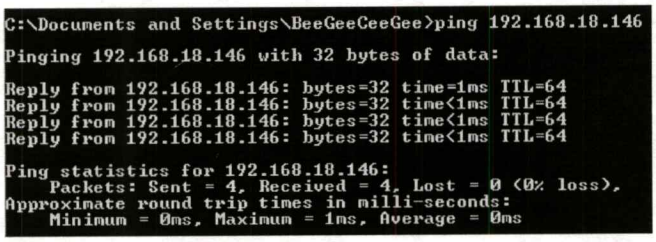
เริ่มต้นการทดสอบโดยการตรวจสอบกฎที่อยู่ภายในไฟร์วอลล์ และค่าต่างๆในปัจจุบัน โดยเมื่อเริ่มต้นทำงานไฟร์วอลล์จะไม่มีกฎอยู่ ซึ่งสามารถตรวจสอบด้วยคำสั่ง pfctl –sr ซึ่งได้ผลลัพธ์ดังรูปที่ 4.20


**รูปที่ 4.20** แสดงผลลัพธ์ของคำสั่ง pfctl –sr ก่อนสร้างกฎ

จากนั้นทำการตรวจสอบข้อมูลที่เก็บอยู่ภายในไฟล์ /etc/pf.conf โดยใช้คำสั่ง more /etc/pf.conf ซึ่งจะได้ผลลัพธ์ดังรูปที่ 4.21


**รูปที่ 4.21** แสดงผลลัพธ์ของคำสั่ง more /etc/pf.conf ก่อนสร้างกฎ

จากการทดสอบจะพบว่าไม่มีข้อมูลกฎอยู่ภายในไฟร์วอลล์และไฟล์ /etc/pf.conf จากนั้นทำการทดสอบโดยการ Ping จากเครื่องคอมพิวเตอร์ที่เชื่อมต่อกับไฟร์วอลล์ โดยจะได้ผลลัพธ์ดังรูปที่ 4.22



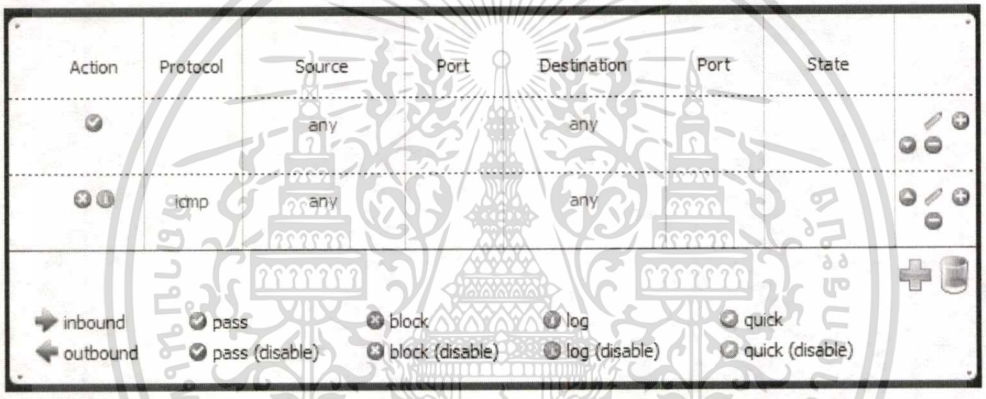

**รูปที่ 4.22** แสดงผลลัพธ์ของคำสั่ง ping จากเครื่องคอมพิวเตอร์ก่อนทำการสร้างกฎ

จะพบว่าเราสามารถ Ping จากเครื่องคอมพิวเตอร์ไปที่ไฟร์วอลล์ได้ เพราะว่ายังไม่มีการสร้างกฎภายในไฟร์วอลล์ ต่อจากนั้นเราจะทำการทดสอบโดยการเปิดหน้าเว็บ Filter Rule Lists ขึ้นมาและทำการเพิ่มกฎเข้าไป โดยกำหนดกฎดังนี้

**pass from any to any**

**block log proto icmp from any to any**

โดยกฎข้อแรกจะเป็นการกำหนดให้ไฟร์วอลล์ส่งผ่านแพ็กเก็ตข้อมูลทั้งหมด และกฎข้อที่สองจะเป็นการกำหนดให้ไฟร์วอลล์ไม่ส่งผ่านแพ็กเก็ตที่เป็นของ Protocol ICMP และจะทำการเก็บ Log ของแพ็กเก็ตเหล่านั้นด้วย จากนั้นทำการ Active กฎที่สร้างขึ้นเข้าสู่ไฟร์วอลล์ โดยจะได้ผลลัพธ์ดังรูปที่ 4.23




**รูปที่ 4.23** แสดงหน้าจอเว็บ Filter Rule Lists หลังจากสร้างกฎ

ทดลองใช้ pfctl –sr ในการดูรายละเอียดของกฎที่อยู่ภายในไฟร์วอลล์ จะพบว่ามีข้อมูลของกฎที่ได้สร้างเข้าไปใหม่อยู่ในไฟร์วอลล์ดังรูปที่ 4.24

```
pf# pfctl -sr
pass inet all
block drop log inet proto icmp all
pf#
```

**รูปที่ 4.24** แสดงผลลัพธ์ของคำสั่ง pfctl –sr หลังสร้างกฎ

ทดลองเปิดดูข้อมูลภายในไฟล์ /etc/pf.conf โดยการใช้คำสั่ง more /etc/pf.conf จะพบว่ามีข้อมูลของกฎที่ได้สร้างขึ้นมาใหม่ถูกเขียนลงในไฟล์แล้วดังรูปที่ 4.25

```
pf# more /etc/pf.conf
#Rule
pass inet from any to any
block log inet proto icmp from any to any
```

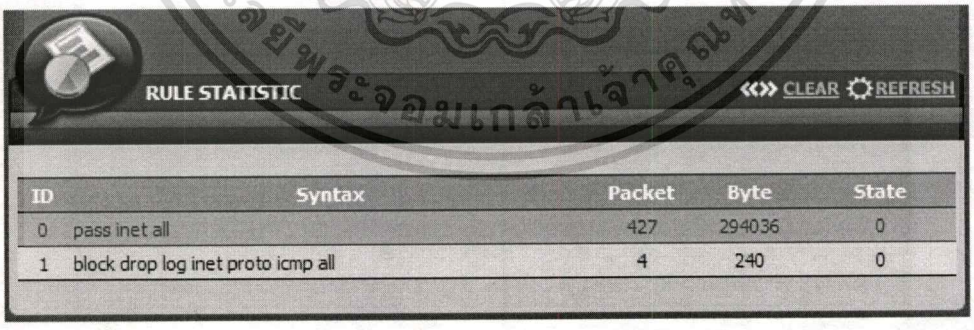
**รูปที่ 4.25** แสดงผลลัพธ์ของคำสั่ง more /etc/pf.conf หลังสร้างกฎ

จากนั้นทำการทดสอบโดยการ Ping จากเครื่องคอมพิวเตอร์อีกครั้งจะได้ผลลัพธ์ คือ ไม่สามารถ Ping ไปยังไฟร์วอลล์ได้ดังรูปที่ 4.26

```
C:\Documents and Settings\BeeGeeCeeGee>ping 192.168.18.146

Pinging 192.168.18.146 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.18.146:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

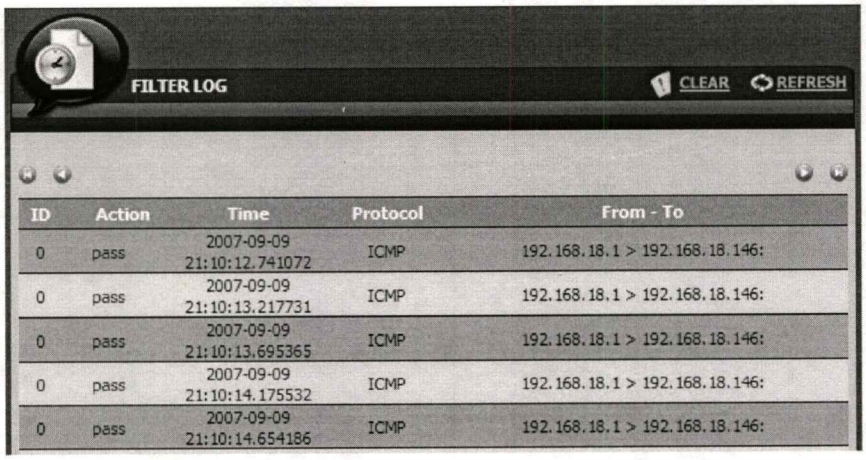
**รูปที่ 4.26** แสดงผลลัพธ์ของคำสั่ง ping จากเครื่องคอมพิวเตอร์หลังทำการสร้างกฎ

จากนั้นเปิดหน้าเว็บ Filter Rule Statistic Report เพื่อตรวจสอบค่าสถิติต่างๆของกฎ จะพบว่ากฎที่ใช้ในการป้องกันการส่งผ่าน ICMP ซึ่งอยู่ในบรรทัดที่สอง มีการตรวจพบแพ็กเก็ตที่ตรงกับกฎ 4 แพ็กเก็ต โดยตรงกับข้อมูลการใช้คำสั่ง ping สามารถแสดงรายละเอียดได้ดังรูปที่ 4.27




**รูปที่ 4.27** แสดงหน้าเว็บ Filter Rule Statistic Report

จากนั้นเปิดหน้าเว็บ Log Report เพื่อทำการตรวจสอบการเก็บข้อมูล log โดยจะได้ผลลัพธ์ดังรูปที่ 4.28




| ID | Action | Time | Protocol | From - To |
|---|---|---|---|---|
| 0 | pass | 2007-09-09 21:10:12.741072 | ICMP | 192.168.18.1 > 192.168.18.146: |
| 0 | pass | 2007-09-09 21:10:13.217731 | ICMP | 192.168.18.1 > 192.168.18.146: |
| 0 | pass | 2007-09-09 21:10:13.695365 | ICMP | 192.168.18.1 > 192.168.18.146: |
| 0 | pass | 2007-09-09 21:10:14.175532 | ICMP | 192.168.18.1 > 192.168.18.146: |
| 0 | pass | 2007-09-09 21:10:14.654186 | ICMP | 192.168.18.1 > 192.168.18.146: |

**รูปที่ 4.28** แสดงหน้าเว็บ Log Report

สรุปการทำงานของระบบการใช้งานส่วนต่อประสานแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์สำหรับผู้ใช้ผ่านเว็บสามารถทำการเปิดและปิด อนุญาตและไม่อนุญาตให้ Packet ต่างๆ ได้ตามกฎที่ได้สร้างขึ้นโดยผู้ใช้สามารถควบคุมการใช้งานโดยใช้คำสั่งต่างๆ ตามต้องการ อย่างไรก็ตามผู้ใช้งานควรจะต้องคำนึงถึงนโยบายด้านความปลอดภัยขององค์กรเป็นหลัก เพื่อให้ไฟร์วอลล์นั้นสามารถนำไปใช้งานได้อย่างมีประสิทธิภาพสูงสุด

# บทที่ 5
# บทสรุปและแนวทางพัฒนาในอนาคต

## 5.1 สิ่งที่ได้รับจากการพัฒนาระบบ

หลังจากผ่านกระบวนการทำการวิเคราะห์ ออกแบบ พัฒนาระบบ และทดสอบระบบที่พัฒนา สามารถสรุปผลลัพธ์ที่ผู้พัฒนาระบบได้รับจากการจัดทำระบบใช้งานส่วนต่อประสานแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์สำหรับผู้ใช้ผ่านเว็บออกเป็นหัวข้อดังนี้

- ได้รับระบบที่รองรับการทำงานผ่านทางหน้าเว็บ ที่สามารถช่วยเป็นเครื่องมือให้ผู้ดูแลระบบสามารถจัดการกับกฎในการกรองข้อมูลได้สะดวกมากขึ้น รวมถึงสามารถช่วยให้ผู้ใช้สามารถควบคุมและติดตามการทำงานของโปรแกรมแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ได้สะดวกมากขึ้น ผ่านทางเครื่องมือต่างๆที่ได้พัฒนาขึ้น
- ได้รับความรู้และความสามารถในการกระบวนการวิเคราะห์ ออกแบบ พัฒนา และทดสอบระบบ
- ได้รับความรู้และความเข้าใจในการใช้งานโปรแกรมแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ รวมถึงการสร้างกฎในการกรองข้อมูล

## 5.2 ข้อจำกัดของระบบ

เนื่องจากกฎของแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์มีรูปแบบประโยค (Syntax) ที่มีความยืดหยุ่นในการเขียนได้หลายแบบ แต่สามารถทำงานในผลลัพธ์ที่เหมือนกัน และกฎบางกฎอาจใช้คำสั่งที่มีความซับซ้อนสูง โดยโปรแกรมในส่วนของการตีความรูปประโยคยังไม่สามารถรองรับต่อวิธีการเขียนรูปประโยคทั้งหมด ซึ่งอาจเกิดปัญหาในส่วนของหน้าเว็บสำหรับแก้ไขกฎที่อาจไม่สามารถรองรับการแสดงกฎบางรูปแบบได้ แต่ทางผู้พัฒนาได้เพิ่มการทำงานในส่วนของ Advance Configuration File เพื่อช่วยให้ผู้ใช้แก้ไขไฟล์ระบบได้โดยตรง แต่การแก้ไขในแบบนี้จะไม่มีเครื่องมือช่วยในการสร้างกฎ ผู้ใช้จึงจำเป็นต้องมีความรู้และเข้าใจในการสร้างกฎ ซึ่งทำให้การใช้งานระบบกับกฎที่มีความซับซ้อนสูงไม่สะดวก

ในการติดต่อสื่อสารผ่านเครือข่ายอินเทอร์เน็ตอาจจะมีเครื่องคอมพิวเตอร์จำนวนมากที่ติดต่อเข้ามาสู่เครือข่ายเพื่อใช้งานในทางที่ดีและถูกต้อง แต่ก็ยังคงมีเครื่องคอมพิวเตอร์และผู้ใช้งานจำนวนไม่น้อยที่มุ่งประสงค์ร้ายต่อเครือข่ายและเครื่องคอมพิวเตอร์ที่ต่อเข้าสู่ระบบอินเทอร์เน็ตอยู่ด้วยเช่นกัน ดังนั้นจึงไม่เป็นการปลอดภัยถ้าหากว่าเราได้เชื่อมต่อเครื่องคอมพิวเตอร์ให้บริการเข้าสู่อินเทอร์เน็ตโดยไม่มีการป้องกันใดๆให้กับเครื่องคอมพิวเตอร์ภายใน

เครือข่ายเหล่านี้ ระบบไฟร์วอลล์จึงเป็นหนึ่งในทางเลือกที่นำมาใช้ในการเพิ่มความปลอดภัยให้กับทรัพย์สินและข้อมูลที่สำคัญภายในระบบเครือข่ายที่ต่อเชื่อมเข้าใช้งานอินเทอร์เน็ต

## 5.3 สรุปแนวทางในการพัฒนาในอนาคต

ระบบไฟร์วอลล์จึงเข้ามามีบทบาทอย่างมากในเรื่องการรักษาความปลอดภัยของเครือข่ายคอมพิวเตอร์โดยมีหน้าที่หลักในการกรอง (filter) ข้อมูลเฉพาะส่วนที่ได้รับอนุญาตเท่านั้น ดังนั้นการเขียนกฎหรือ rule สำหรับไฟร์วอลล์จึงเป็นเรื่องที่สำคัญอย่างยิ่ง การสร้าง rule ของไฟร์วอลล์ที่ผิดพลาดจะทำให้ไฟร์วอลล์ ที่ทั้งราคาแพงและใช้งานฟรี ทั้งหลายไม่สามารถช่วยป้องกันเครือข่ายให้รอดพ้นจากการถูกบุกรุกหรือโจมตีได้อย่างแน่นอน แต่สำหรับไฟร์วอลล์ที่จำหน่ายในเชิงพาณิชย์ส่วนใหญ่จะมีโปรแกรมสำหรับช่วยในการกำหนดกฎไฟร์วอลล์ซึ่งช่วยในการลดความผิดพลาดอันเนื่องมาจากการสร้างกฎไฟร์วอลล์อยู่แล้ว แต่สำหรับไฟร์วอลล์ที่เป็นชนิด Freeware ส่วนใหญ่มักจะยังไม่มีโปรแกรมสำหรับการคอนฟิกกฎของไฟร์วอลล์จึงทำให้อาจเกิดความผิดพลาดของการกำหนดกฎของไฟร์วอลล์ได้

ดังนั้นการพัฒนาระบบการกำหนดกฎหรือการสร้างกฎของไฟร์วอลล์จึงมีส่วนช่วยให้ไฟร์วอลล์ที่เป็น Freeware สามารถสร้าง rule ที่ถูกต้อง เพื่อเป็นการลดความผิดพลาดอันเนื่องจากการกำหนดกฎของไฟร์วอลล์ลงได้ แต่ทั้งนี้ผู้ดูแลไฟร์วอลล์จะต้องมั่นใจว่าเครื่องไฟร์วอลล์นั้นมีความปลอดภัยในระดับโฮสอยู่แล้ว (host based security) เพราะถึงแม้ว่า rule ที่สร้างขึ้นจะสามารถป้องกันเครื่องอื่นๆ ภายในเครือข่ายได้ แต่ถ้าเครื่องไฟร์วอลล์เองไม่สามารถทนต่อการบุกรุกได้ก็เป็นจุดที่อันตรายไม่ยิ่งหย่อนไปกว่าการสร้างกฎที่ผิดพลาดแต่อย่างใด ซึ่งแนวทางในการพัฒนาในอนาคตนั้นอาจจะมีการรวมความสามารถในการทำงานกับระบบอื่นที่มากขึ้น เช่น การเพิ่มระบบ NAT เข้ามาทำงานร่วมกับซอฟต์แวร์ไฟร์วอลล์ หรือการเพิ่มความสามารถในการทำงาน เช่น การเพิ่มการทำงานในส่วนของ Load Balance นอกจากนั้นอาจมีการพัฒนาให้ส่วนติดต่อผู้ใช้สามารถตอบสนองกับความต้องการของผู้ใช้ได้อย่างรวดเร็วและมีรูปแบบการทำงานที่กระชับมากขึ้น และอาจพัฒนาระบบเพื่อให้สามารถนำไปใช้กับซอฟต์แวร์ไฟร์วอลล์อื่นได้หลายชนิดมากขึ้น

# บรรณานุกรม

กิตติ ภักดีวัฒนะกุล. 2546. **การวิเคราะห์และออกแบบระบบ.** กรุงเทพฯ : เคทีพีคอมพ์แอนด์คอนซัลท์.

กิตติ ภักดีวัฒนะกุล และกิตติพงษ์ กลมกล่อม. 2544. **UML วิเคราะห์และออกแบบระบบเชิงวัตถุ.** กรุงเทพฯ : เคทีพีคอมพ์แอนด์คอนซัลท์.

กิตติพงษ์ สุวรรณราช. 2537. **การบริหารจัดการเครือข่ายอินเตอร์เน็ต ด้วยระบบปฏิบัติการ FreeBSD** กรุงเทพฯ : ออฟเซ็ท เพรส .

ทินกร วัฒนเกษมสกุล. 2548. **คัมภีร์ JSP.** กรุงเทพฯ : เคทีพี คอมพ์ แอนด์ คอนซัลท์.

บัณฑิต จามรภูมิ. 2549. **คู่มือระบบยูนิกซ์ FreeBSD เล่ม 1.** กรุงเทพฯ : บริษัท บัณฑิตเพลส จำกัด.

พันจันทร์ ธนวัฒนเสถียร. 2548. **ออกแบบและสร้างเว็บสวยด้วย Dreamweaver8.** กรุงเทพฯ : บริษัท ซัคเซส มีเดีย จำกัด.

วันชัย แซ่เตีย และ สิทธิชัย ประสานวงศ์. 2543. **สร้าง Dynamic Web Pages ด้วย JavaScript.**

สรวุฒิ กอสุวรรณศิริ. 2544. **เสริมแต่งโฮมเพจครั้งใหม่! ให้มีชีวิตชีวาด้วย JavaScript.** กรุงเทพฯ : บริษัท วิตตี้ กรุ๊ปจำกัด.

สาธิต ชัยวิวัฒน์กูล. 2545. **เก่ง JSP ให้ครบสูตร.** กรุงเทพฯ : บริษัท วิตตี้ กรุ๊ปจำกัด.

สันติ ศรีลาศักดิ์ และวินัย สุขอารีย์ชัย. 2547. **ทำไมใช้ง่ายอย่างนี้ MS Visio 2003.** กรุงเทพฯ : ออฟเซ็ท เพรส.

สุนทริน วงศ์สิริกุล. 2544. **พัฒนาโมเดลยุคใหม่ UML (Unified Modeling Language.)** กรุงเทพฯ : ออฟเซ็ท เพรส.

โอภาส เอี่ยมสิริวงศ์. 2547. **การวิเคราะห์และออกแบบระบบ.** กรุงเทพฯ : ซีเอ็ดยูเคชั่น. กรุงเทพฯ : ซอฟท์เพรซ.

Peter N. M. Hansteen. 2007. **Firewalling with OpenBSD's PF packet filter** . [Online]. Available : http://www.openbsd.org/faq/pf/

The FreeBSD Documentation Project. 2007. **FreeBSD Handbook.** . [Online]. Available : http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/

# ภาคผนวก

# ภาคผนวก ก.

# การติดตั้งระบบใช้งานส่วนต่อประสาน แพ็กเก็ตฟิลเตอร์ไฟร์วอลล์สำหรับผู้ใช้ผ่านเว็บ

**1. โปรแกรมที่ใช้ในการทำงานของระบบ**

โปรแกรมที่ใช้ในการทำงานของระบบจะประกอบไปด้วย โปรแกรมแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ และโปรแกรมที่ใช้ในการทำงานเป็นเซิร์ฟเวอร์ โดยโปรแกรมที่ใช้ในการพัฒนาระบบมีดังนี้

1.) **โปรแกรมแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์** เป็นโปรแกรมที่ทำให้เครื่องเริ่มต้นทำงานเป็นไฟร์วอลล์ โดยโปรแกรมแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ถูกติดตั้งมากับระบบปฏิบัติการ FreeBSD อยู่แล้ว โดยไม่จำเป็นต้องติดตั้งโปรแกรมเพิ่มแต่ต้องกำหนดให้โปรแกรมเริ่มต้นการทำงาน

2.) **โปรแกรมเว็บเซิร์ฟเวอร์ Apache Tomcat 5.0** เป็นโปรแกรมที่ทำให้เครื่องทำงานเป็นเว็บเซิร์ฟเวอร์ให้บริการกับเครื่องที่เข้ามาของใช้บริการในเครื่องได้ รวมถึงการจัดการกำหนดสิทธิ์การใช้งานและการกำหนดการทำงานของโปรแกรมได้ด้วย

3.) **โปรแกรม Browser** โปรแกรมที่ใช้ในการท่องอินเทอร์เน็ต โดยโปรแกรมนี้มีติดมากับระบบปฏิบัติการอยู่แล้วได้แก่ Internet Explorer แต่สามารถที่จะใช้โปรแกรมอื่นๆ ที่ใช้งานกับระบบปฏิบัติการวินโดวส์ได้ มาใช้งานแทนได้

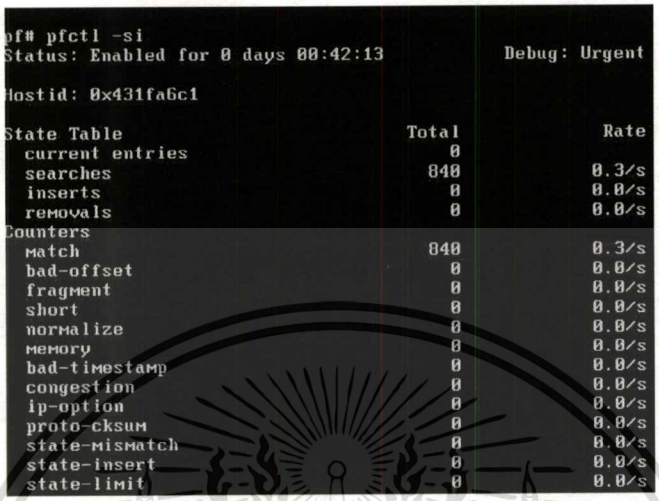
**2. ขั้นตอนการติดตั้งระบบ**

**2.1 การเริ่มใช้งานโปรแกรมแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์**

การเรียกใช้งานแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์บนระบบปฏิบัติการ FreeBSD สามารถทำได้โดยการแก้ไขไฟล์ rc.conf ที่เก็บอยู่ที่ /etc/rc.conf โดยต้องเพิ่มคำสั่งเข้าไปในไฟล์ เพื่อให้ระบบปฏิบัติการ FreeBSD เริ่มต้นการทำงานของแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์เมื่อทำการเปิดระบบขึ้นมาใหม่ โดยเพิ่มคำสั่งดังนี้

| | |
|---|---|
| **pf_enable="YES"** | เริ่มต้นการทำงานของแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ |
| **pf_rules="/etc/pf.conf"** | กำหนดไฟล์ที่ใช้ในการเก็บกฎของไฟร์วอลล์ |
| **pflog_enable="YES"** | เริ่มต้นการทำงานของ pflog เพื่อทำการเก็บ Log ข้อมูล |
| **pflog_logfile="/var/log/pflog"** | กำหนดไฟล์ที่ใช้ในการเก็บข้อมูลของ Log |

จากนั้นทำการบันทึกไฟล์และเริ่มต้นการทำงานของระบบปฏิบัติการใหม่ จากนั้นทดลองโดยการใช้คำสั่ง pfctl –si โดยคำสั่งจะแสดงข้อมูลของแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ ถ้าไม่สามารถใช้คำสั่งได้ ให้ทำการตรวจสอบความถูกต้องของค่าที่กำหนดใน /etc/rc.conf อีกครั้ง




รูปที่ ก.1 แสดงหน้าจอทดสอบการทำงานของแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์

**2.2 การติดตั้งเว็บเซิร์ฟเวอร์ Apache Tomcat 5.0**

การติดตั้งเว็บเซิร์ฟเวอร์ Apache Tomcat 5.0 จำเป็นที่จะต้องติดตั้งโปรแกรมภาษาจาวา (Java) เพื่อให้สามารถทำงานได้ โดยในการติดตั้งจะใช้การติดตั้งผ่านพอร์ตของระบบปฏิบัติการ FreeBSD มีขั้นตอนการติดตั้งและกำหนดค่าดังนี้

1. เข้าไปที่ /usr/ports/www/jarata-tomcat5 ด้วยคำสั่ง

   **cd /usr/ports/www/jarata-tomcat5**

2. จากนั้นใช้คำสั่ง make install เพื่อทำการติดตั้ง โดยจะใช้เวลาในการติดตั้งซักพักหนึ่ง
3. จากนั้นเข้าไปแก้ไขไฟล์ /usr/local/etc/rc.d/tomcat โดยทำการแก้ไขข้อมูลดังนี้

   **tomcat50_enable=”${tomcat55_enable:-”YES”}”**

   **tomcat50_user=”${tomcat55_user:-”root”}”**

4. จากนั้นเพื่อให้เว็บเซิร์ฟเวอร์ทำงานทุกครั้งที่เปิดเครื่อง โดยเข้าไปแก้ไขไฟล์ /etc/rc.conf โดยเพิ่มคำสั่งเข้าไปในไฟล์ดังนี้

   **tomcat50_enable=”YES”**

5. ทำการทดสอบการติดตั้งโปรแกรม โดยเปิดโปรแกรม Browser และพิมพ์ Url ไปที่

   **http://local_ip:8180**

จากนั้นทำการบันทึกไฟล์และเริ่มต้นการทำงานของระบบปฏิบัติการใหม่ จากนั้นทดลองโดยการใช้คำสั่ง pfctl –si โดยคำสั่งจะแสดงข้อมูลของแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ ถ้าไม่สามารถใช้คำสั่งได้ ให้ทำการตรวจสอบความถูกต้องของค่าที่กำหนดใน /etc/rc.conf อีกครั้ง


รูปที่ ก.1 แสดงหน้าจอทดสอบการทำงานของแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์

**2.2 การติดตั้งเว็บเซิร์ฟเวอร์ Apache Tomcat 5.0**

การติดตั้งเว็บเซิร์ฟเวอร์ Apache Tomcat 5.0 จำเป็นที่จะต้องติดตั้งโปรแกรมภาษาจาวา (Java) เพื่อให้สามารถทำงานได้ โดยในการติดตั้งจะใช้การติดตั้งผ่านพอร์ตของระบบปฏิบัติการ FreeBSD มีขั้นตอนการติดตั้งและกำหนดค่าดังนี้

1. เข้าไปที่ /usr/ports/www/jarata-tomcat5 ด้วยคำสั่ง

   **cd /usr/ports/www/jarata-tomcat5**

2. จากนั้นใช้คำสั่ง make install เพื่อทำการติดตั้ง โดยจะใช้เวลาในการติดตั้งซักพักหนึ่ง
3. จากนั้นเข้าไปแก้ไขไฟล์ /usr/local/etc/rc.d/tomcat โดยทำการแก้ไขข้อมูลดังนี้

   **tomcat50_enable=”${tomcat55_enable:-”YES”}”**

   **tomcat50_user=”${tomcat55_user:-”root”}”**

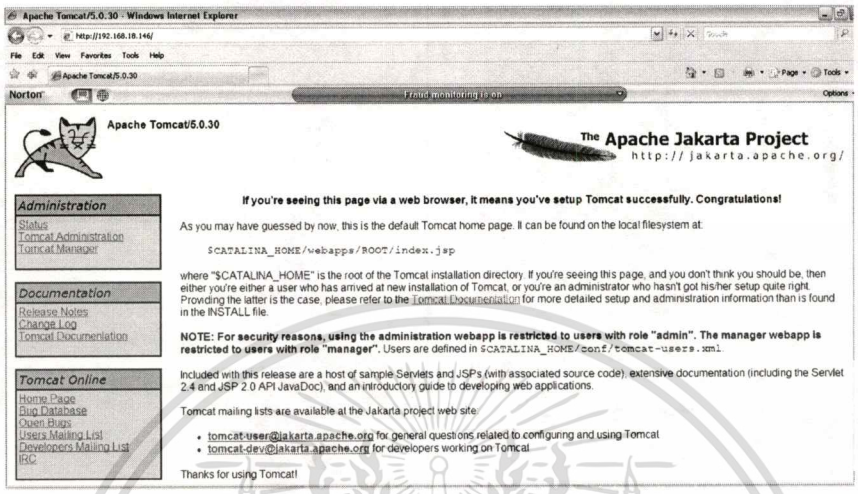
4. จากนั้นเพื่อให้เว็บเซิร์ฟเวอร์ทำงานทุกครั้งที่เปิดเครื่อง โดยเข้าไปแก้ไขไฟล์ /etc/rc.conf โดยเพิ่มคำสั่งเข้าไปในไฟล์ดังนี้

   **tomcat50_enable=”YES”**

5. ทำการทดสอบการติดตั้งโปรแกรม โดยเปิดโปรแกรม Browser และพิมพ์ Url ไปที่

   **http://local_ip:8180**

โดยค่าของ local_ip คือค่าของ IP Address ของเครื่องที่ทำการติดตั้งเว็บเซิร์ฟเวอร์ ซึ่งถ้าสามารถติดตั้งให้ทำงานได้ โปรแกรม Browser จะแสดงผลดังรูปที่ ก.2




**รูปที่ ก.2** แสดงหน้าจอทดสอบการทำงานของเว็บเซิร์ฟเวอร์

**2.3 การติดตั้งระบบใช้งานแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์สำหรับผู้ใช้แบบเว็บ**

1. การติดตั้งสามารถทำได้โดยการคัดลอกไฟล์ของโปรแกรมทั้งหมดไปวางไว้ใน

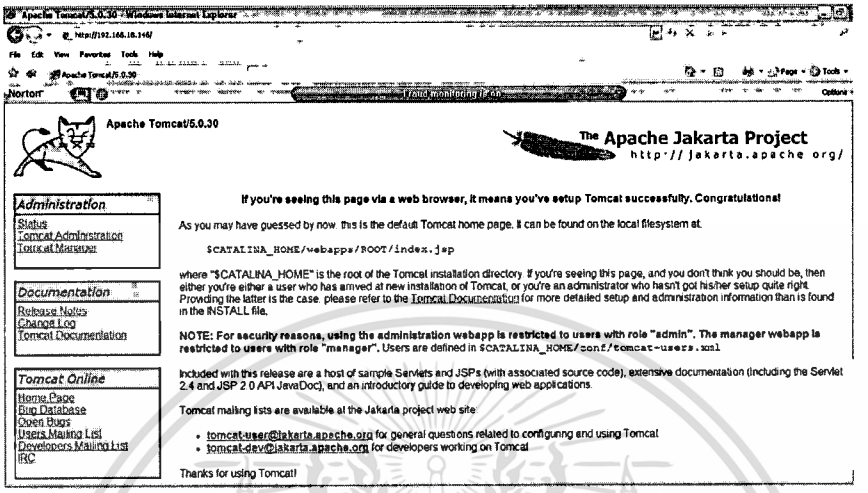
   **/usr/local/Jakarta-tomcat5.0/webapp/ROOT**

2. จากนั้นเปิดโปรแกรม Browser และพิมพ์ Url ไปที่

   **http://local_ip:8180/home.jsp**

   โดยค่าของ local_ip คือค่าของ IP Address ของเครื่องที่ทำการติดตั้งระบบ เพื่อเริ่มต้นใช้งานระบบ

โดยค่าของ local_ip คือค่าของ IP Address ของเครื่องที่ทำการติดตั้งเว็บเซิร์ฟเวอร์ ซึ่งถ้าสามารถติดตั้งให้ทำงานได้ โปรแกรม Browser จะแสดงผลดังรูปที่ ก.2




**รูปที่ ก.2** แสดงหน้าจอทดสอบการทำงานของเว็บเซิร์ฟเวอร์

**2.3 การติดตั้งระบบใช้งานแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์สำหรับผู้ใช้แบบเว็บ**

1. การติดตั้งสามารถทำได้โดยการคัดลอกไฟล์ของโปรแกรมทั้งหมดไปวางไว้ใน

   **/usr/local/Jakarta-tomcat5.0/webapp/ROOT**

2. จากนั้นเปิดโปรแกรม Browser และพิมพ์ Url ไปที่

   **http://local_ip:8180/home.jsp**

   โดยค่าของ local_ip คือค่าของ IP Address ของเครื่องที่ทำการติดตั้งระบบ เพื่อเริ่มต้นใช้งานระบบ

# ภาคผนวก ข.

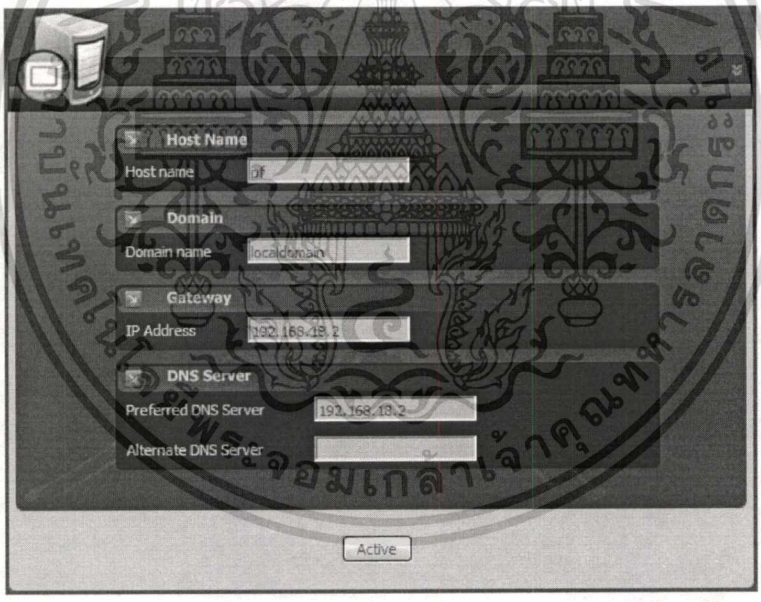
# คู่มือการใช้งานระบบใช้งานส่วนต่อประสานแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์สำหรับผู้ใช้ผ่านเว็บ

## 1. กลุ่มหน้าเว็บ System

ประกอบด้วยหน้าเว็บที่ใช้ในการกำหนดลักษณะและคุณสมบัติต่างๆของระบบปฏิบัติการ FreeBSD รวมทั้งการควบคุมแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ โดยประกอบด้วยหน้าเว็บดังต่อไปนี้

### 1.1 General Configuration

ใช้สำหรับการกำหนดค่าคุณสมบัติต่างๆ ที่เกี่ยวข้องกับตัวระบบปฏิบัติการโดยสามารถแสดงรายละเอียดของหน้าเว็บ General Configuration ได้ดังรูปที่ ข.1




**รูปที่ ข.1** แสดงหน้าเว็บ General Configuration

โดยส่วนประกอบต่างๆภายในหน้าเว็บ General Configuration สามารถอธิบายได้ดังนี้

**Host name**

ใช้สำหรับกำหนดชื่อของเครื่องที่ไฟร์วอลล์ทำงานอยู่ โดยมีจะรับค่าเป็นกลุ่มตัวอักษรชื่อของเครื่อง

# ภาคผนวก ข.

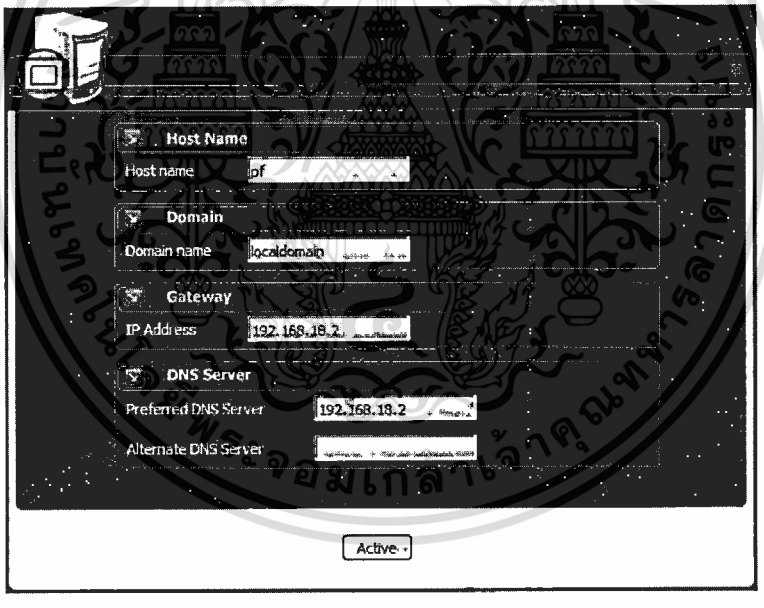
# คู่มือการใช้งานระบบใช้งานส่วนต่อประสานแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์สำหรับผู้ใช้ผ่านเว็บ

## 1. กลุ่มหน้าเว็บ System

ประกอบด้วยหน้าเว็บที่ใช้ในการกำหนดลักษณะและคุณสมบัติต่างๆของระบบปฏิบัติการ FreeBSD รวมทั้งการควบคุมแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ โดยประกอบด้วยหน้าเว็บดังต่อไปนี้

### 1.1 General Configuration

ใช้สำหรับการกำหนดค่าคุณสมบัติต่างๆ ที่เกี่ยวข้องกับตัวระบบปฏิบัติการโดยสามารถแสดงรายละเอียดของหน้าเว็บ General Configuration ได้ดังรูปที่ ข.1




**รูปที่ ข.1** แสดงหน้าเว็บ General Configuration

โดยส่วนประกอบต่างๆภายในหน้าเว็บ General Configuration สามารถอธิบายได้ดังนี้

**Host name**

ใช้สำหรับกำหนดชื่อของเครื่องที่ไฟร์วอลล์ทำงานอยู่ โดยมีจะรับค่าเป็นกลุ่มตัวอักษรชื่อของเครื่อง

**Domain name**

ใช้สำหรับกำหนดชื่อโดเมนของเครื่องที่ไฟร์วอลล์ทำงานอยู่ โดยมีจะรับค่าเป็นกลุ่มตัวอักษรชื่อของโดเมน

**Gateway**

ใช้สำหรับกำหนด Gateway ในการส่งผ่านข้อมูล โดยการกำหนดค่าจะระบุเป็นค่า IP Address

**DNS server**

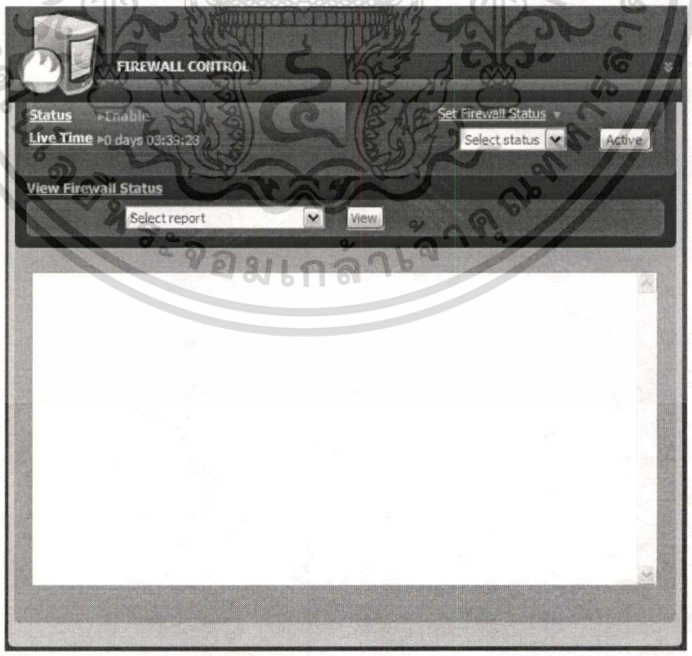
ใช้สำหรับกำหนด Domain Name Server ให้กับระบบ โดยสามารถกำหนดได้สองค่าคือ Preferred DNS Server และ Alternate DNS Server โดยการกำหนดค่าจะใช้ค่า IP Address ของ Domain Name Server

**ปุ่ม Active**

ใช้สำหรับเริ่มต้นการกำหนดค่าต่างๆให้กับระบบ

**1.2 Firewall Controls**

ใช้สำหรับควบคุมการทำงานของแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ และสามารถดูข้อมูลที่เป็นภาพรวมของไฟร์วอลล์ในปัจจุบันได้ หน้าเว็บ Firewall Controls สามารถแสดงได้ดังรูปที่ ข.2




**รูปที่ ข.2** แสดงหน้าเว็บ Firewall Controls

**Domain name**

ใช้สำหรับกำหนดชื่อโดเมนของเครื่องที่ไฟร์วอลล์ทำงานอยู่ โดยมีจะรับค่าเป็นกลุ่มตัวอักษรชื่อของโดเมน

**Gateway**

ใช้สำหรับกำหนด Gateway ในการส่งผ่านข้อมูล โดยการกำหนดค่าจะระบุเป็นค่า IP Address

**DNS server**

ใช้สำหรับกำหนด Domain Name Server ให้กับระบบ โดยสามารถกำหนดได้สองค่าคือ Preferred DNS Server และ Alternate DNS Server โดยการกำหนดค่าจะใช้ค่า IP Address ของ Domain Name Server

**ปุ่ม Active**

ใช้สำหรับเริ่มต้นการกำหนดค่าต่างๆให้กับระบบ

**1.2 Firewall Controls**

ใช้สำหรับควบคุมการทำงานของแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ และสามารถดูข้อมูลที่เป็นภาพรวมของไฟร์วอลล์ในปัจจุบันได้ หน้าเว็บ Firewall Controls สามารถแสดงได้ดังรูปที่ ข.2


**รูปที่ ข.2** แสดงหน้าเว็บ Firewall Controls

โดยส่วนประกอบต่างๆภายในหน้าเว็บ Firewall Controls สามารถอธิบายได้ดังนี้

**Status**

แสดงสถานะของแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ในปัจจุบัน โดยมีสองสถานะคือ ทำงาน (Enable) และ หยุดการทำงาน (Disable)

**Live Time**

แสดงเวลาทั้งหมดที่แพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ถูกใช้งานมาจนถึงขณะนั้น โดยค่าจะถูกลบทิ้งและเริ่มต้นนับใหม่เมื่อมีการกำหนด สถานะของแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ เช่น การหยุดการทำงาน

**Set Firewall Status**

ใช้สำหรับควบคุมสถานะการทำงานของแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ โดยสามารถเลือกสถานะของไฟล์วอลล์และทำการส่งค่าให้กับระบบเพื่อกำหนดสถานะให้กับไฟร์วอลล์

**View Firewall Report**

แสดงรายงานโดยสรุปของสถานะไฟร์วอลล์ในปัจจุบัน เพื่อช่วยอำนวยความสะดวกในการตรวจสอบการทำงานของไฟร์วอลล์ในเบื้องต้น

### 1.3 Interface Lists

หน้าเว็บที่แสดง Network Interface ของระบบ โดยจะประกอบไปด้วยรายละเอียดต่างๆ ของ Network Interface เช่น สถานะของ Network Interface หรือการใช้งาน DHCP รวมถึงค่า IP Address และ Subnet Mask โดยหน้าเว็บ Interface Lists มีรายละเอียดดังแสดงในรูปที่ ข.3


**รูปที่ ข.3** แสดงหน้าเว็บ Interface Lists

โดยส่วนประกอบต่างๆภายในหน้าเว็บ Interface Lists สามารถอธิบายได้ดังนี้

โดยส่วนประกอบต่างๆภายในหน้าเว็บ Firewall Controls สามารถอธิบายได้ดังนี้

**Status**

แสดงสถานะของแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ในปัจจุบัน โดยมีสองสถานะคือ ทำงาน (Enable) และ หยุดการทำงาน (Disable)

**Live Time**

แสดงเวลาทั้งหมดที่แพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ถูกใช้งานมาจนถึงขณะนั้น โดยค่าจะถูกลบทิ้งและเริ่มต้นนับใหม่เมื่อมีการกำหนด สถานะของแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ เช่น การหยุดการทำงาน

**Set Firewall Status**

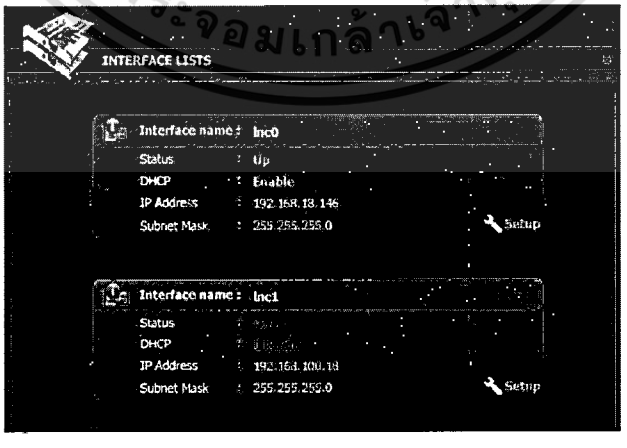
ใช้สำหรับควบคุมสถานะการทำงานของแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ โดยสามารถเลือกสถานะของไฟล์วอลล์และทำการส่งค่าให้กับระบบเพื่อกำหนดสถานะให้กับไฟร์วอลล์

**View Firewall Report**

แสดงรายงานโดยสรุปของสถานะไฟร์วอลล์ในปัจจุบัน เพื่อช่วยอำนวยความสะดวกในการตรวจสอบการทำงานของไฟร์วอลล์ในเบื้องต้น

**1.3 Interface Lists**

หน้าเว็บที่แสดง Network Interface ของระบบ โดยจะประกอบไปด้วยรายละเอียดต่างๆ ของ Network Interface เช่น สถานะของ Network Interface หรือการใช้งาน DHCP รวมถึงค่า IP Address และ Subnet Mask โดยหน้าเว็บ Interface Lists มีรายละเอียดดังแสดงในรูปที่ ข.3




**รูปที่ ข.3** แสดงหน้าเว็บ Interface Lists

โดยส่วนประกอบต่างๆภายในหน้าเว็บ Interface Lists สามารถอธิบายได้ดังนี้

**Interface name**

แสดงชื่อของ Network Interface

**Status**

แสดงสถานะปัจจุบันของ Network Interface โดยมีสองสถานะคือ UP เป็นสถานะที่ Network Interface ทำงานอยู่ โดยจะแสดงตัวอักษรสีเขียว และ DOWN เป็นสถานะที่ Network Interface ไม่ทำงาน โดยจะแสดงอักษรสีแดง

**DHCP**

แสดงสถานะของการใช้งาน DHCP ที่ Network Interface โดยแบ่งเป็นสองสถานะคือ Enable เป็นอักษรสีเขียว แสดงว่ามีการกำหนดให้ Network Interface ดังกล่าวใช้ DHCP และอีกสถานะคือ Disable เป็นอักษรสีแดง หมายความว่า Network Interface ไม่ได้กำหนด DHCP ให้ทำงาน

**IP Address**

แสดงค่า IP Address ของ Network Interface

**Subnet Mask**

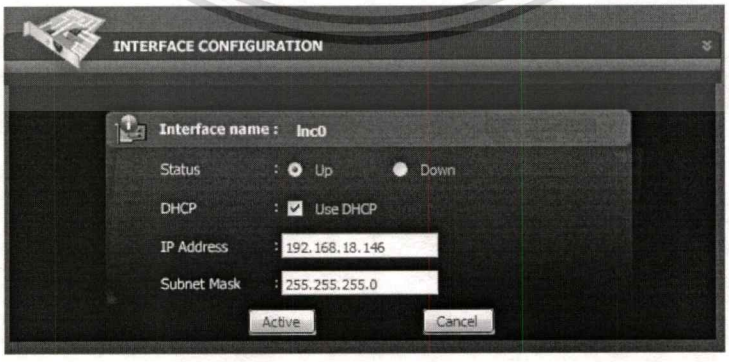
แสดงค่า Subnet Mask ของ IP Address

**ปุ่ม Setup**

ใช้สำหรับเข้าถึงหน้าเว็บ Interface Configuration

**1.4 Interface Configuration**

หน้าเว็บสำหรับกำหนดค่าและคุณสมบัติต่างๆ ให้กับ Network Interface โดยสามารถแสดงรายละเอียดของหน้าเว็บได้ดังรูปที่ ข.4




**รูปที่ ข.4** แสดงหน้าเว็บ Interface Configuration

**Interface name**

แสดงชื่อของ Network Interface

**Status**

แสดงสถานะปัจจุบันของ Network Interface โดยมีสองสถานะคือ UP เป็นสถานะที่ Network Interface ทำงานอยู่ โดยจะแสดงตัวอักษรสีเขียว และ DOWN เป็นสถานะที่ Network Interface ไม่ทำงาน โดยจะแสดงอักษรสีแดง

**DHCP**

แสดงสถานะของการใช้งาน DHCP ที่ Network Interface โดยแบ่งเป็นสองสถานะคือ Enable เป็นอักษรสีเขียว แสดงว่ามีการกำหนดให้ Network Interface ดังกล่าวใช้ DHCP และอีกสถานะคือ Disable เป็นอักษรสีแดง หมายความว่า Network Interface ไม่ได้กำหนด DHCP ให้ทำงาน

**IP Address**

แสดงค่า IP Address ของ Network Interface

**Subnet Mask**

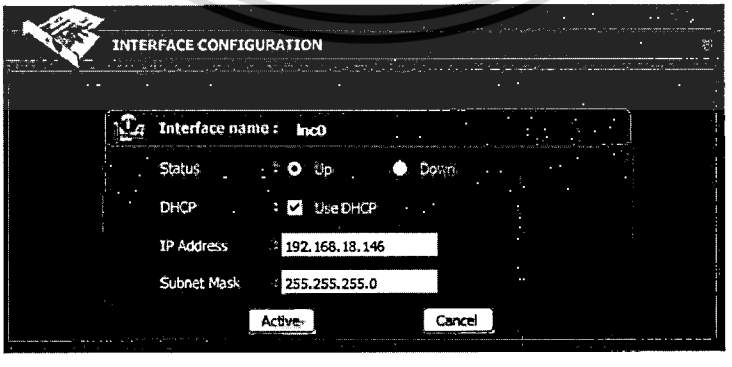
แสดงค่า Subnet Mask ของ IP Address

**ปุ่ม Setup**

ใช้สำหรับเข้าถึงหน้าเว็บ Interface Configuration

**1.4 Interface Configuration**

หน้าเว็บสำหรับกำหนดค่าและคุณสมบัติต่างๆ ให้กับ Network Interface โดยสามารถแสดงรายละเอียดของหน้าเว็บได้ดังรูปที่ ข.4




**รูปที่ ข.4** แสดงหน้าเว็บ Interface Configuration

โดยส่วนประกอบต่างๆภายในหน้าเว็บ Interface Configuration สามารถอธิบายได้ดังนี้

**Status**

ใช้กำหนดสถานะของ Network Interface โดยแบ่งเป็น UP คือกำหนดให้ Network Interface นั้นทำงาน และ Down คือกำหนดให้ Network Interface ไม่ทำงาน

**DHCP**

ใช้กำหนดให้ Network Interface ใช้ DHCP ในการกำหนด IP Address โดยการเลือกที่ Check box เพื่อกำหนดให้ใช้งาน DHCP

**IP Address**

กำหนดค่า IP Address ของ Network Interface ยกเว้นในกรณีที่ใช้ DHCP จะไม่ต้องกำหนดในส่วนนี้

**Subnet Mask**

แสดงค่า Subnet Mask ของ IP Address ยกเว้นในกรณีที่ใช้ DHCP จะไม่ต้องกำหนดในส่วนนี้

**ปุ่ม Active**

ใช้สำหรับนำเข้าข้อมูลต่างๆที่กำหนด เข้าสู่ระบบ เพื่อทำการปรับเปลี่ยน Network Interface ให้ทำงานตามที่ได้กำหนด

**ปุ่ม Cancel**

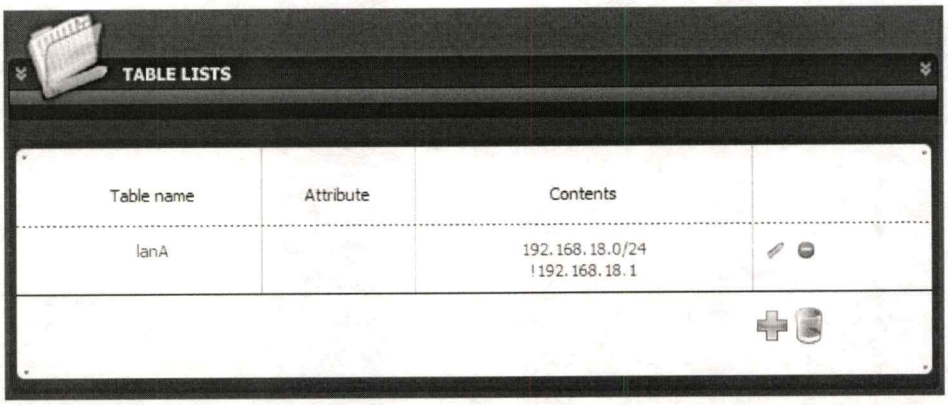
ใช้สำหรับเข้าถึงหน้า Interface Lists ในกรณีที่ไม่ต้องการปรับเปลี่ยนคุณสมบัติต่างๆของ Network Interface

## 2. กลุ่มหน้าเว็บ Firewall

ประกอบด้วยหน้าเว็บที่ใช้ในการจัดการกับกฎ เช่น การสร้าง การแก้ไข การลบ หรือการเปลี่ยนแปลงลำดับของกฎ และกำหนดค่าการทำงานต่างๆของแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์ โดยประกอบไปด้วยหน้าเว็บที่มีรายละเอียดและการทำงานดังต่อไปนี้

### 2.1 Table Lists

หน้าเว็บสำหรับแสดง Table ที่มีอยู่ในไฟร์วอลล์ โดยจะแสดงรายละเอียดในลักษณะของตาราง ซึ่งแสดงค่าที่กำหนดภายในตาราง โดยรายละเอียดของหน้าเว็บ Table Lists สามารถแสดงได้ดังรูปที่ ข.5




**รูปที่ ข.5** แสดงหน้าเว็บ Table Lists

โดยส่วนประกอบต่างๆภายในหน้าเว็บ Table Lists สามารถอธิบายได้ดังนี้

**Table name**

แสดงชื่อของ Table

**Attribute**

แสดงค่า Attribute ของ Table

**Contents**

แสดงค่าของข้อมูลที่เก็บอยู่ภายใน Table

**ปุ่ม Edit**

ใช้สำหรับเข้าถึงหน้าเว็บ Table Edit สำหรับปรับเปลี่ยน Table ที่ต้องการ

**ปุ่ม Delete**

ใช้สำหรับลบ Table ที่เลือก

**ปุ่ม Add**

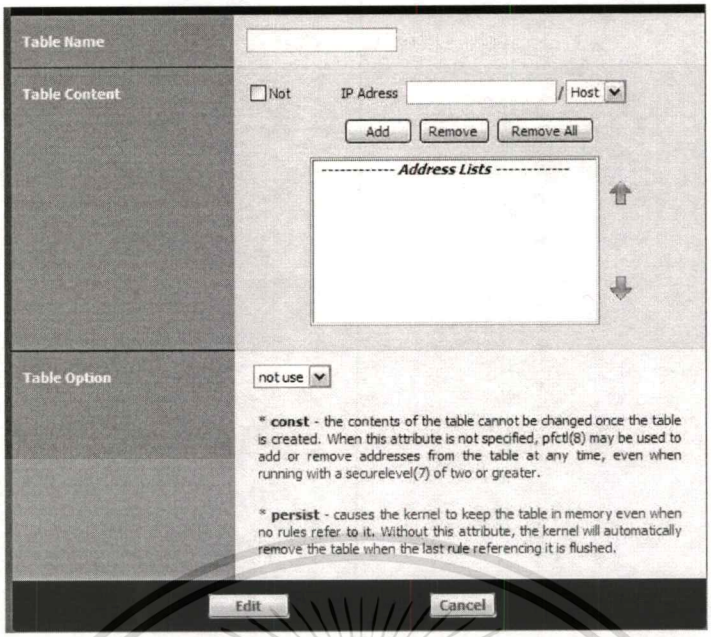
ใช้สำหรับเพิ่ม Table ใหม่ โดยจะมีการเข้าสู่หน้า Table Edit เพื่อทำการกำหนดค่าของ Table ที่ต้องการเพิ่ม

**ปุ่ม Delete All**

ใช้สำหรับลบ Table ทั้งหมดที่มีอยู่ใน Lists

**2.2 Table Edit**

หน้าเว็บสำหรับแก้ไขและกำหนดค่าต่างๆให้กับ Table เช่น ชื่อของ Table และข้อมูลของ IP Address ที่อยู่ภายใน Table สามารถแสดงรายละเอียดของหน้าเว็บ Table Edit ได้ดังรูปที่ ข.6




**รูปที่ ข.6** แสดงหน้าเว็บ Table Edit

โดยส่วนประกอบต่างๆภายในหน้าเว็บ Table Edit สามารถอธิบายได้ดังนี้

**Table name**

เป็นส่วนที่ใช้ในการกำหนดชื่อของ Table

**Table Content**

ใช้ในการกำหนดค่าของข้อมูลที่จัดเก็บอยู่ใน Table โดยในการเพิ่มข้อมูลจะใช้การกำหนดค่าภายในกล่อง IP Address และเลือกค่า Subnet Mask แล้วทำการเพิ่มข้อมูลเข้าสู่ Address Lists ผ่านทางปุ่ม Add และสามารถลบข้อมูลภายใน Address Lists ผ่านทางปุ่ม Remove โดยการเลือกข้อมูลใน Address Lists แล้วทำการลบ หรือลบทั้งหมดผ่านทางปุ่ม Remove All นอกจากนั้นยังสามารถจัดเรียงลำดับของ IP Address ภายใน Address Lists ผ่านทางปุ่มลูกศรด้านข้างของ Address Lists

**Table Option**

เป็นส่วนที่ใช้ในการกำหนด Attribute ให้กับ Table

**ปุ่ม Edit**

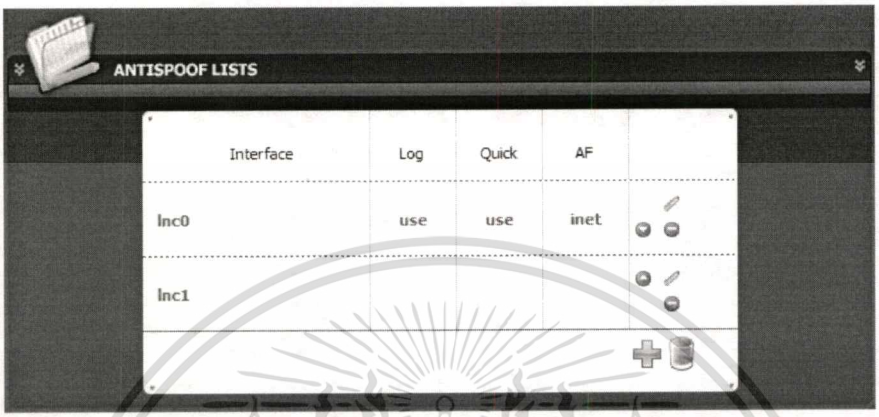
ใช้สำหรับนำเข้าข้อมูลของที่กำหนดเข้าสู่ระบบ เพื่อปรับปรุงข้อมูลให้ตรงตามค่าที่กำหนด

**ปุ่ม Cancel**

ใช้สำหรับเข้าถึงหน้า Table Lists ในกรณีที่ไม่ต้องการปรับเปลี่ยนคุณสมบัติต่างๆของ Table

**2.3 Antispoof Lists**

หน้าเว็บสำหรับแสดงกฎ Antispoof ที่มีอยู่ในไฟร์วอลล์ โดยจะแสดงรายละเอียดในลักษณะของตาราง ซึ่งแสดงค่าที่กำหนดภายในตาราง โดยรายละเอียดของหน้าเว็บ Antispoof Lists สามารถแสดงได้ดังรูปที่ ข.7




**รูปที่ ข.7** แสดงหน้าเว็บ Antispoof Lists

โดยส่วนประกอบต่างๆภายในหน้าเว็บ Antispoof Lists สามารถอธิบายได้ดังนี้

**Interface**

แสดงชื่อของ Network Interface ที่ถูกกำหนดภายในกฎ Antispoof โดยสามารถมีได้มากกว่าหนึ่ง Interface

**Log**

แสดงสถานะ Log ของกฎ Antispoof โดยถ้ามีการกำหนดจะมีการแสดงอักษร use แต่ถ้าไม่มีการกำหนดจะไม่แสดงค่าออกมา

**Quick**

แสดงคุณสมบัติ Quick ของกฎ Antispoof โดยถ้ามีการกำหนดจะมีการแสดงอักษร use แต่ถ้าไม่มีการกำหนดจะไม่แสดงค่าออกมา

**AF**

แสดงคุณสมบัติ AF (Address Family) ของกฎ Antispoof โดยถ้ามีการกำหนดจะมีที่เป็นไปได้สองค่าคือ inet และinet6 แต่ถ้าไม่มีการกำหนดจะไม่แสดงค่าออกมา

**ปุ่ม Edit**

ใช้สำหรับเข้าถึงหน้าเว็บ Antispoof Edit เพื่อแก้ไขกฎ Antispoof ที่เลือก

**ปุ่ม Delete**

ใช้สำหรับลบกฎ Antispoof ที่เลือก

**ปุ่ม Add**

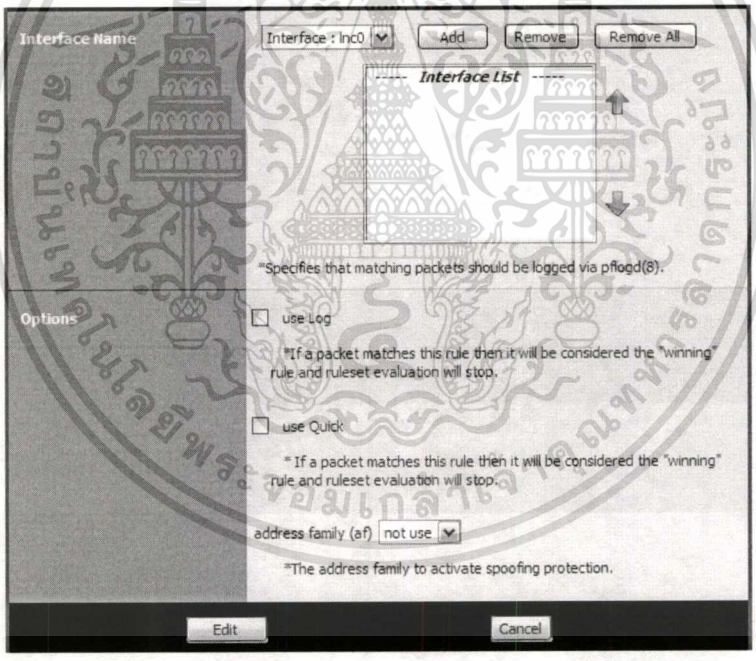
ใช้สำหรับเพิ่ม Antispoof ใหม่ โดยจะมีการเข้าสู่หน้า Antispoof Edit เพื่อทำการกำหนดค่าของกฎ Antispoof ที่สร้างขึ้น

**ปุ่ม Delete All**

ใช้สำหรับลบ Antispoof ทั้งหมดที่มีอยู่ใน Lists

**2.4 Antispoof Edit**

หน้าเว็บสำหรับกำหนดค่าต่างๆให้กับกฎ Antispoof เช่น การกำหนดกลุ่ม Network Interface ที่จะถูกใช้งานในกฎ และ Option ต่างๆของกฎ โดยหน้าเว็บ Antispoof Edit สามารถแสดงได้ดังรูปที่ ข.8




**รูปที่ ข.8** แสดงหน้าเว็บ Antispoof Edit

โดยส่วนประกอบต่างๆภายในหน้าเว็บ Antispoof Edit สามารถอธิบายได้ดังนี้

**Select Interface**

กำหนด Network Interface ที่จะใช้ภายในกฎ Antispoof โดยการเลือกจาก Network Interface name และสามารถเพิ่มเข้า Interface Lists ผ่านปุ่ม Add และสามารถลบ Network Interface ที่ไม่ต้องการใช้ได้จากการใช่ปุ่ม Remove และ Remove All

**Option**

เป็นส่วนที่ใช้ในการกำหนด Option ต่างๆให้กับกฎ Antispoof โดยจะประกอบด้วย

- Use Log กำหนดให้กฎ Antispoof ใช้คำสั่ง log เพื่อเก็บ log ของข้อมูลที่ถูกตรวจสอบโดยกฎ Antispoof
- Use Quick กำหนดให้กฎ Antispoof ใช้คำสั่ง quick
- Address Family (AF) กำหนดให้กฎ Antispoof ฝช่คำสั่งในการกำหนด address family โดยสามารถเลือกค่าได้สองค่าคือ inet และ inet6

**ปุ่ม Edit**

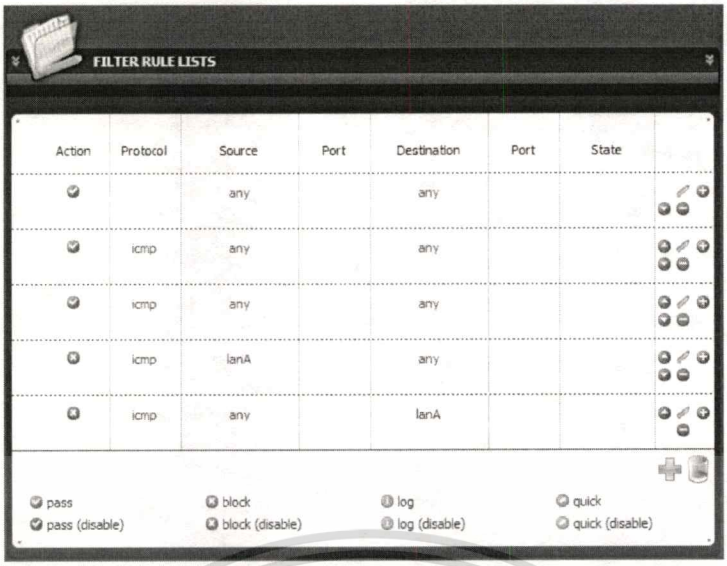
ใช้สำหรับนำเข้าข้อมูลของกฎ Antispoof ที่กำหนดเข้าสู่ระบบ เพื่อปรับปรุงข้อมูลให้ตรงตามค่าที่กำหนด

**ปุ่ม Cancel**

ใช้สำหรับเข้าถึงหน้า Antispoof Lists ในกรณีที่ไม่ต้องการปรับเปลี่ยนคุณสมบัติต่างๆของกฎ Antispoof

**2.5 Filter Rule Lists**

หน้าเว็บสำหรับแสดงกฎ Filter ที่มีอยู่ในไฟร์วอลล์ โดยจะแสดงรายละเอียดในลักษณะของตาราง ซึ่งแสดงค่าที่กำหนดภายในตาราง เช่น Action การทำงานของกฎ และข้อมูลที่ใช้ในการเปรียบเทียบแพ็กเก็ตกับกฎ โดยรายละเอียดของหน้าเว็บ Filter Rule Lists สามารถแสดงได้ดังรูปที่ ข.9




**รูปที่ ข.9** แสดงหน้าเว็บ Filter Rule Lists

โดยส่วนประกอบต่างๆภายในหน้าเว็บ Filter Rule Lists สามารถอธิบายได้ดังนี้

**Action**

แสดง Action ในการทำงานของกฎ เมื่อมีแพ็กเก็ตที่ตรงกับคุณสมบัติที่กำหนดไว้ภายในกฎ โดยแบ่งออกเป็นสองแบบคือ

**Pass** หมายถึง กฎมีการกำหนดค่าให้ส่งผ่านแพ็กเก็ตที่ตรงกับกฎ

**Block** หมายถึง กฎมีการกำหนดค่าให้ไม่ส่งผ่านแพ็กเก็ตที่ตรงกับกฎ

นอกจากนั้นจะมี Action การทำงานที่เป็น Option ของกฎอีกสองคำสั่ง ซึ่งจะมีการกำหนดหรือไม่มีการกำหนดก็ได้ คือ

**Log** หมายถึง กฎมีการกำหนดคำสั่ง log ซึ่งจะเก็บ log ของข้อมูลที่ตรงกับกฎ

**Quick** หมายถึง กฎมีการกำหนดคำสั่ง Quick อยู่ภายในกฎ

**Protocol**

แสดงค่า Protocol ที่ถูกกำหนดอยู่ในกฎ เพื่อใช้ในการตรวจสอบแพ็กเก็ต

**Source**

แสดงค่าที่ใช้ในการตรวจสอบต้นทางของแพ็กเก็ตที่ทำการตรวจสอบ

**Destination**

แสดงค่าที่ใช้ในการตรวจสอบปลายทางของแพ็กเก็ตที่ทำการตรวจสอบ

**Port**

แสดงค่าที่ใช้ในการตรวจสอบ Port ต้นทาง และ Port ปลายทาง ของแพ็กเก็ตที่ทำการตรวจสอบ

**State**

แสดงค่ารูปแบบของ State ที่ถูกกำหนดในกฎ

**ปุ่ม Move Up**

เปลี่ยนตำแหน่งกฎภายใน Filter Rule Lists โดยเลื่อนกฎที่เลือกขึ้นไปแทนที่กฎที่อยู่ด้านบนของกฎที่เลือก

**ปุ่ม Move Down**

เปลี่ยนตำแหน่งกฎภายใน Filter Rule Lists โดยเลื่อนกฎที่เลือกลงไปแทนที่กฎที่อยู่ด้านล่างของกฎที่เลือก

**ปุ่ม Edit**

แก้ไขกฎที่เลือก โดยแก้ไขผ่านทางหน้าเว็บ Filter Rule Edit

**ปุ่ม Delete**

ลบกฎที่เลือกออกจาก Filter Rule Lists

**ปุ่ม Insert**

เพิ่มกฎใหม่เข้าไปในตำแหน่งก่อนหน้าศฎที่เลือก และจะมีการกำหนดคุณสมบัติต่างๆของกฎผ่านทางหน้าเว็บ Filter Rule Edit

**ปุ่ม Add**

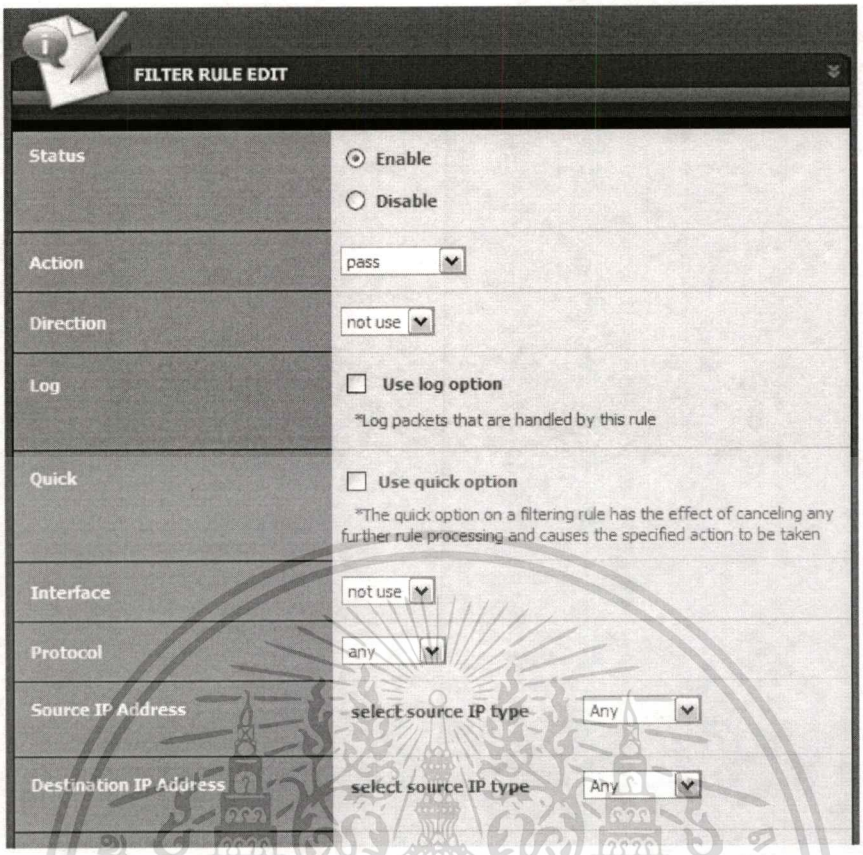
เพิ่มกฎใหม่เข้าไปในตำแหน่งสุดท้ายของ Filter Rule List และจะมีการกำหนดคุณสมบัติต่างๆของกฎผ่านทางหน้าเว็บ Filter Rule Edit

**ปุ่ม Delete All**

ลบกฎทั้งหมดออกจาก Filter Rule Lists

**2.7 Filter Rule Edit**

หน้าเว็บสำหรับแก้ไขและกำหนดค่าต่างๆให้กับ Filter Rule โดยสามารถแสดงรายละเอียดของหน้าเว็บ Table Editได้ดังรูปที่ ข.10




**รูปที่ ข.10** แสดงหน้าเว็บ Filter Rule Edit

โดยส่วนประกอบต่างๆภายในหน้าเว็บ Filter Rule Lists สามารถอธิบายได้ดังนี้

**Status**

กำหนดสถานะของกฎ เพื่อทำการใช้งาน (Enable) กฎ หรือยกเลิกการใช้งาน (Disable) กฎ โดยกฎจะไม่ถูกลบ แต่จะถูกยกเลิกการใช้งานชั่วคราว

**Action**

กำหนดการทำงานของกฎที่จะเกิดขึ้นเมื่อมีแพ็กเก็ตที่ตรงกับข้อกำหนดต่างๆที่ถูกกำหนดไว้ในกฎ โดยแบ่งออกเป็น Pass, Block, Block drop และBlock return

**Direction**

กำหนดทิศทางในการตรวจสอบของกฎ โดยแบ่งเป็น In และ Out

**Interface**

กำหนด Interface ที่ต้องการให้กฎทำการตรวจสอบ

**Protocol**

กำหนด Protocol ที่ต้องการให้กฎทำการตรวจสอบ

**Source IP Address**

กำหนด IP Address ของต้นทางที่ต้องการให้กฎทำการตรวจสอบ โดยสามารถกำหนดข้อมูลในส่วนนี้ได้ 2 วิธีคือ

1. ใช้ Table ที่บรรจุ IP Address ที่ต้องการตรวจสอบ
2. ใช้การกรอกข้อมูล IP Address เข้าไป

**Source Port**

กำหนด Port ของต้นทางที่ต้องการใช้ในการตรวจสอบ

**Destination IP Address**

กำหนด IP Address ของปลายทางที่ต้องการให้กฎทำการตรวจสอบ โดยสามารถกำหนดข้อมูลในส่วนนี้ได้ 2 วิธีคือ

1. เลือกใช้ Table ที่บรรจุ IP Address ที่ต้องการตรวจสอบ
2. ใช้การกรอกข้อมูล IP Address เข้าไป

**Destination Port**

กำหนด Port ของปลายทางที่ต้องการใช้ในการตรวจสอบ

**TCP Flags**

กำหนด TCP Flags ที่ต้องการให้กฎตรวจสอบ (Option นี้จะถูกใช้ก็ต่อเมื่อมีการเลือก Protocol มีค่าเป็น TCP)

**State**

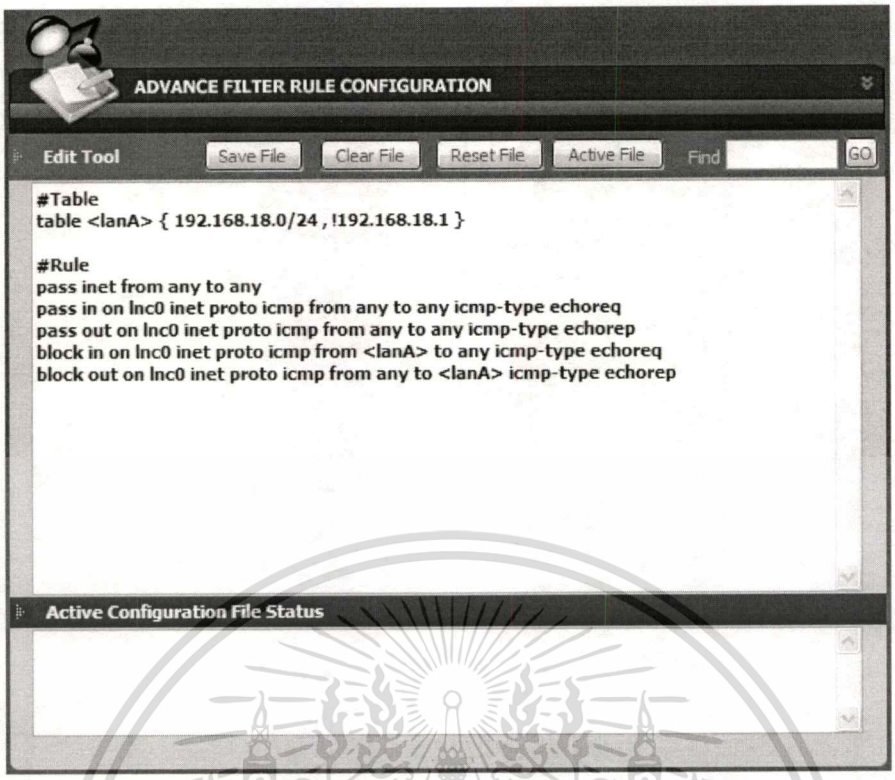
กำหนดชนิดของ State ที่จะใช้ในกฎ โดยแบ่งออกเป็น keep state, modulate state และ synproxy state

**Advance Options**

กำหนดการทำงานของกฎในระดับสูง โดยจะใช้งานได้ก็ต่อเมื่อมีการเลือกใช้ State ซึ่งจะเป็นส่วนที่ใช้ในการกำหนดค่าให้กับการทำงานของ State

**2.8 Advance Configuration**

ใช้สำหรับการแก้ไขกฎและค่าต่างๆภายในไฟล์ระบบของไฟร์วอลล์(/etc/pf.conf) โดยสามารถทำการแก้ไขข้อมูลภายในไฟล์โดยการพิมพ์ข้อมูลเข้าสู่ไฟล์ และสามารถทำการบันทึก (Save file) และเริ่มต้นการทำงานของไฟล์ที่ได้ทำการแก้ไข (Active) โดยสามารถแสดงรายละเอียดของเว็บ Advance Configuration ได้ดังรูปที่ ข.11




**รูปที่ ข.11** แสดงหน้าเว็บ Advance Configuration

โดยส่วนประกอบต่างๆภายในหน้าเว็บ Advance Configuration สามารถอธิบายได้ดังนี้

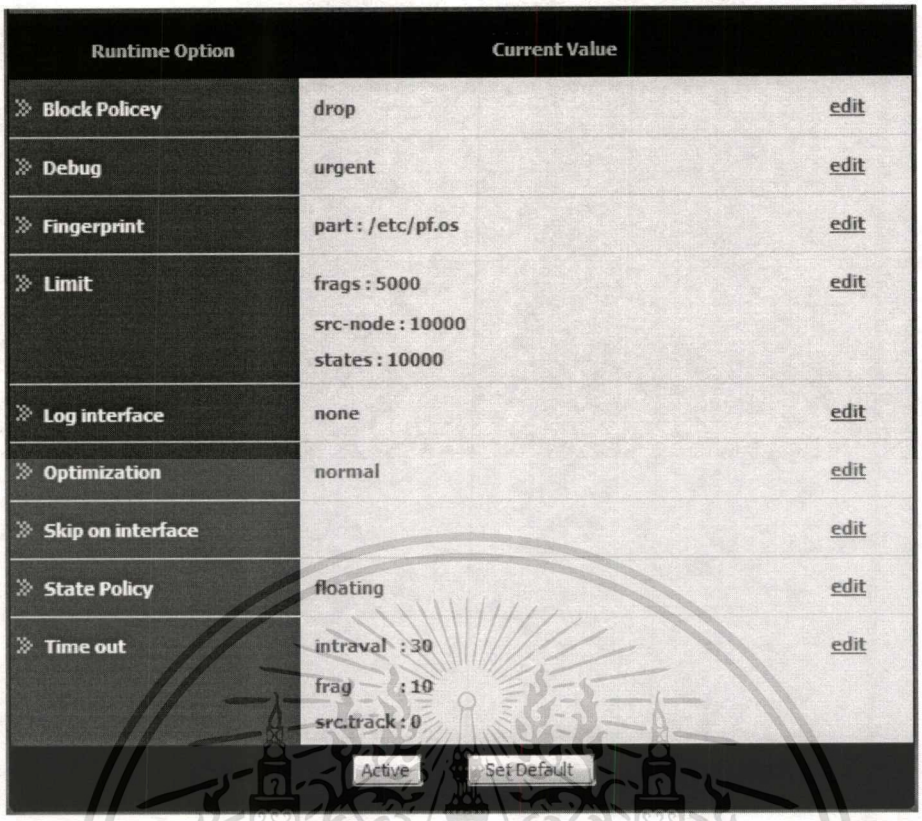
**Edit Tool** ประกอบด้วยเครื่องมือที่ใช้ในการควบคุมการทำงาน โดยประกอบไปด้วย

- Save File ใช้สำหรับบันทึกข้อมูลที่แก้ไขลงในไฟล์ระบบของไฟร์วอลล์
- Clear File ใช้สำหรับการลบข้อมูลทั้งหมดบนไฟล์
- Reset File ยกเลิกการแก้ไข
- Active File ส่งค่าในไฟล์ที่แก้ไขให้กับแพ็กเก็ตฟิลเตอร์ไฟร์วอลล์เพื่อเริ่มทำงาน

**Active Configuration File Status** ใช้สำหรับแสดงผลการ Active File และ Save File

### 2.9 Runtime Options

หน้าเว็บสำหรับแก้ไขและกำหนดค่าต่างๆให้กับ Runtime Options เช่น โดยสามารถแสดงรายละเอียดของหน้าเว็บ Runtime Options ได้ดังรูปที่ ข.12




**รูปที่ ข.12** แสดงหน้าเว็บ Runtime Options

โดยส่วนประกอบต่างๆภายในหน้าเว็บ Runtime Options สามารถอธิบายได้ดังนี้

**Runtime Option Name**

เป็นแถบที่ใช้ในการแสดงชื่อของ Runtime Option

**Current Value**

เป็นแถบที่ใช้ในการแสดงค่าปัจจุบันของ Runtime Option แต่ละชนิด

**Edit**

สำหรับแก้ไขค่าของ Runtime Option แต่ละชนิด

**ปุ่ม Active**

ใช้สำหรับเริ่มต้นใช้งานค่าของ Runtime Option ที่กำหนด

**ปุ่ม Set Default**

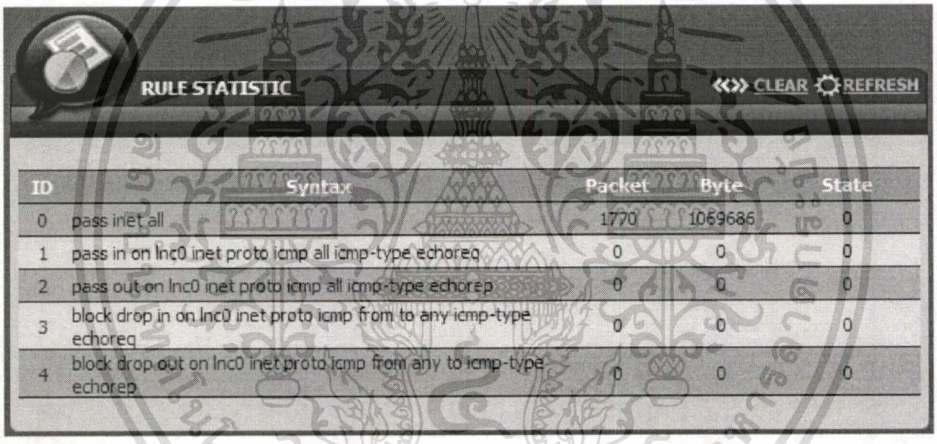
ใช้สำหรับกำหนดให้ค่าของ Runtime Option กลับไปสู่ค่าตั้งต้น

**3. กลุ่มหน้าเว็บ Reports**

ประกอบด้วยหน้าเว็บที่ใช้สำหรับเรียกดูรายงานของระบบ โดยมีรายงานให้เลือกสองแบบคือ Filter Rule Statistic Report และ Log Report โดยสามารถอธิบายรายละเอียดของรายงานแต่ละแบบได้ดังนี้

**3.1 Filter Rule Statistic Report**

แสดงรายงานทางด้านสถิติของกฎที่ทำงานอยู่ในไฟร์วอลล์ โดยมีการรายงานผลในลักษณะของตาราง และมีการบอกถึงรายละเอียดของ หมายเลขกฎ(Rule ID), รูปประโยคของกฎ (Rule Syntax), แพ็กเก็ตที่ตรงกับกฎ (Packet), ขนาดข้อมูลทั้งหมด (Byte) และจำนวนของ State ที่เกิดจากกฎ นอกจากนั้นยังสามารถลบค่าที่เก็บไว้ทั้งหมดออกเริ่มต้นใหม่ โดยใช้ปุ่ม Clear เพื่อลบค่าทั้งหมด โดยสามารถแสดงรายละเอียดของหน้าเว็บ Filter Rule Statistic Report ได้ดังรูปที่ ข.13




**รูปที่ ข.13** แสดงหน้าเว็บ Filter Rule Statistic Report

โดยส่วนประกอบต่างๆภายในหน้าเว็บ Filter Rule Statistic Report สามารถอธิบายได้ดังนี้

**ID**

แสดงหมายเลขประจำกฎ ที่ทำงานอยู่ในขณะนั้น

**Syntax**

แสดงรูปประโยคของกฎ

**Packet**

แสดงปริมาณแพ็กเก็ตที่ถูกกรองโดยกฎ

**Byte**

แสดงปริมาณของข้อมูลที่ถูกกรองโดยกฎ

**State**

แสดงจำนวนของ State ที่ถูกสร้างโดยกฎ

**ปุ่ม Clear**

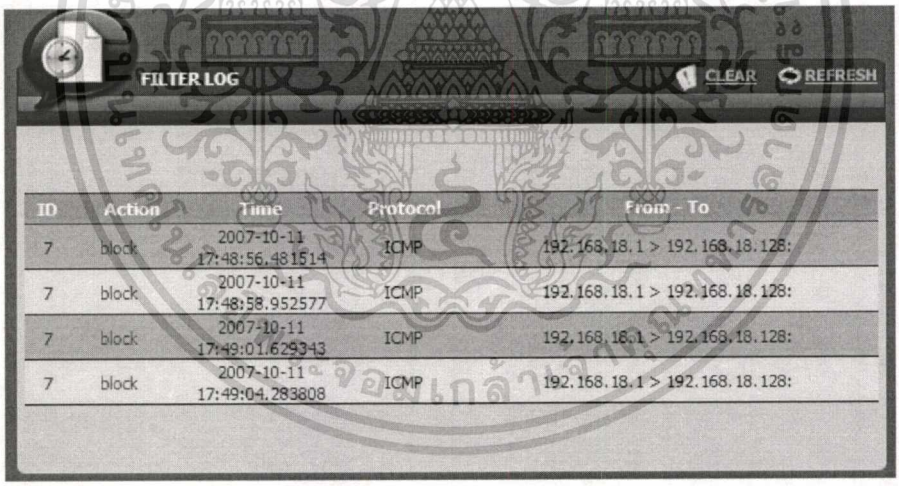
ลบค่าสถิติทั้งหมดของกฎ

**ปุ่ม Refresh**

โหลดข้อมูลล่าสุดจากไฟร์วอลล์ขึ้นมาแสดงผล

### 3.2 Log Report

แสดงรายงานข้อมูลที่เกิดจากการเก็บ Log ของกฎต่างๆ ที่เกิดขึ้น โดยมีการรายงานผลในลักษณะของตาราง และมีการบอกถึงรายละเอียดของ หมายเลขกฎ (Rule ID), Action, ช่วงเวลาที่ข้อมูลถูกเก็บ (Time), โปรโตคอล (Protocol) และต้นทางกับปลายทางของข้อมูล (From - To) โดยสามารถแสดงรายละเอียดของหน้าเว็บ Log Report ได้ดังรูปที่ ข.14




**รูปที่ ข.14** แสดงหน้าเว็บ Log Report

โดยส่วนประกอบต่างๆภายในหน้าเว็บ Log Report สามารถอธิบายได้ดังนี้

**ID**

แสดงหมายเลขประจำกฎ ที่ทำงานอยู่ในขณะนั้น

**Action**

แสดงการทำงาน(Action) ของกฎที่เกิดขึ้นกับข้อมูลที่ถูกเก็บลงในไฟล์ Log

**Time**

แสดงช่วงเวลาที่ข้อมูลถูกตรวจพบโดยกฎ

**Protocol**

แสดงโปรโตคอลของข้อมูลที่ถูกเก็บ

**From-To**

แสดงข้อมูล IP Address และ Port ของต้นทางและปลายทางที่อยู่ภายในข้อมูล

**ปุ่ม Refresh**

โหลดข้อมูลล่าสุดจากไฟล์ Log ขึ้นมาแสดงผล

**ปุ่ม Next, Back, First และ Last**

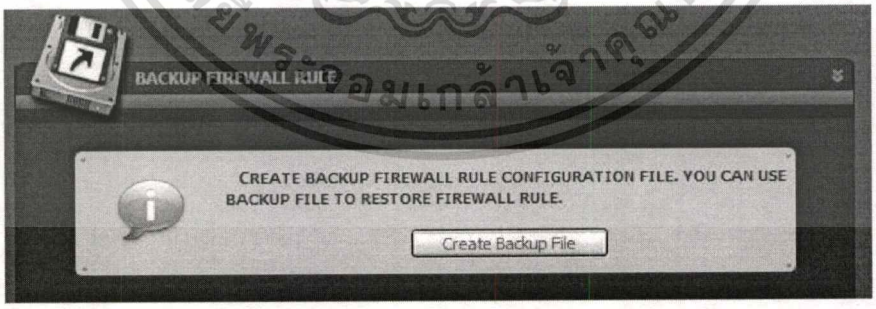
ใช้ในการเข้าถึงข้อมูล Log ในแต่ละหน้า

**4. กลุ่มหน้าเว็บ Tools**

ประกอบด้วยหน้าเว็บที่ใช้เป็นเครื่องมือในการจัดการและดูแลระบบ โดยประกอบด้วยหน้าเว็บต่างๆ ดังต่อไปนี้

**4.1 Backup**

หน้าเว็บสำหรับทำการสำรองข้อมูลของไฟร์วอลล์ โดยสามารถแสดงรายละเอียดของหน้าเว็บ Backup ได้ดังรูปที่ ข.15




**รูปที่ ข.15** แสดงหน้าเว็บ Backup

โดยส่วนประกอบต่างๆภายในหน้าเว็บ Backup สามารถอธิบายได้ดังนี้

**File Name**

แสดงชื่อไฟล์

**Size**

แสดงขนาดของไฟล์

**Last Date**

แสดงเวลาล่าสุดที่ไฟล์ถูกแก้ไข

**ปุ่ม Backup**

เริ่มต้นการสำรองข้อมูล

**4.2 Restore**

หน้าเว็บสำหรับนำค่าข้อมูลของไฟร์วอลล์ที่ได้ทำการสำรองไว้ มาใช้งาน โดยสามารถแสดงรายละเอียดของหน้าเว็บ Restore ได้ดังรูปที่ ข.16


**รูปที่ ข.16** แสดงหน้าเว็บ Restore

โดยส่วนประกอบต่างๆภายในหน้าเว็บ Restore สามารถอธิบายได้ดังนี้

**File Name**

แสดงชื่อไฟล์

**Size**

แสดงขนาดของไฟล์

**Last Date**

แสดงเวลาล่าสุดที่ไฟล์ถูกแก้ไข

**ปุ่ม View**

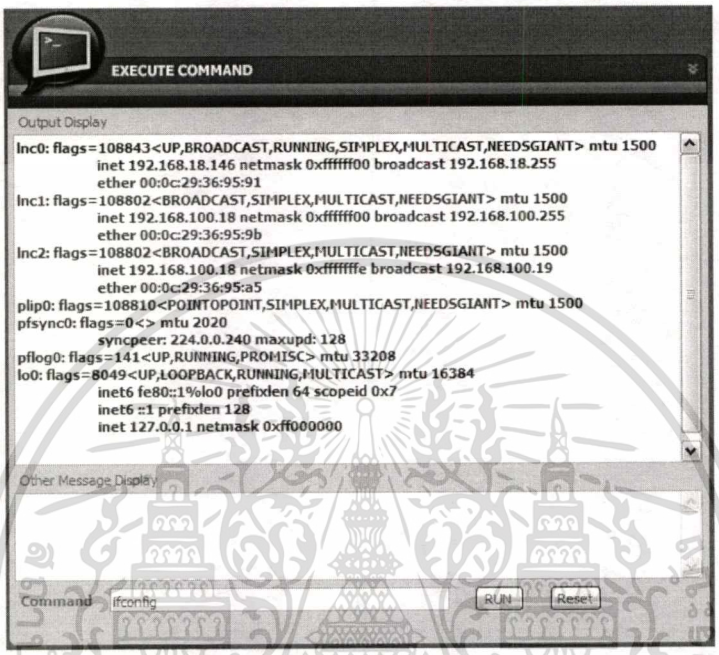
แสดงข้อมูลภายในไฟล์

**ปุ่ม Restore**

เริ่มต้นการโหลดข้อมูลจากไฟล์ที่เลือก

**4.4 Execute Command**

ใช้ในการสั่งคำสั่งต่างๆ ผ่านทางหน้าเว็บ สามารถแสดงผลลัพธ์ของคำสั่ง และความผิดพลาด(Error) ของคำสั่งที่เกิดขึ้น โดยรายละเอียดของหน้าเว็บ Execute Command สามารถแสดงได้ดังรูปที่ ข.17




**รูปที่ ข.17** แสดงหน้าเว็บ Execute Command

โดยส่วนประกอบต่างๆภายในหน้าเว็บ Execute Command สามารถอธิบายได้ดังนี้

**Output Display**

แสดงผลลัพธ์จากการดำเนินการของคำสั่ง

**Other Massage Display**

แสดงผลลัพธ์ของข้อผิดพลาดและข้อความอื่นๆ

**Command**

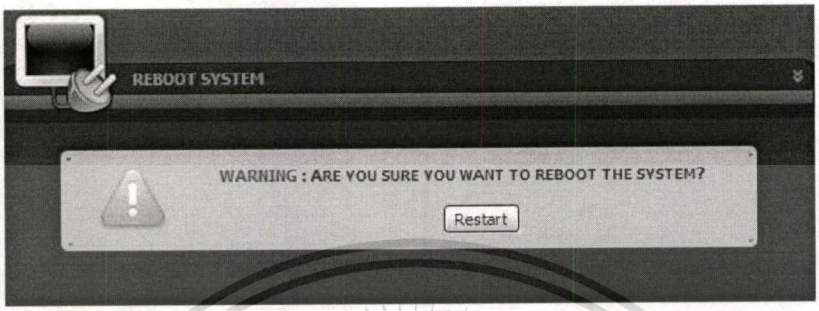
ใช้สำหรับรับค่าของคำสั่ง

**ปุ่ม Run**

เริ่มต้นการดำเนินการตามคำสั่งที่กำหนด

**4.3 Reboot System**

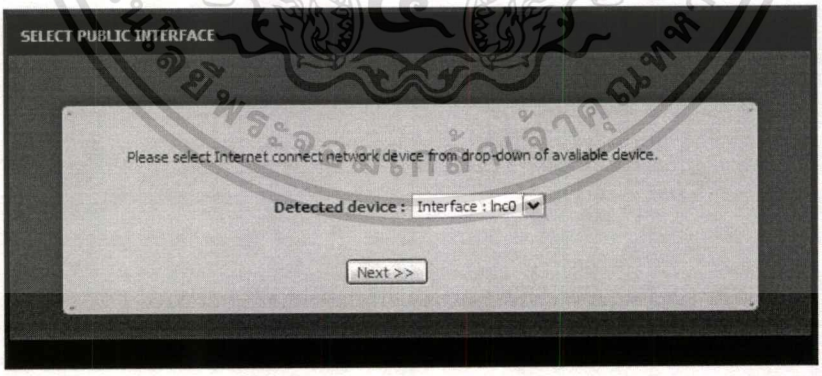
หน้าเว็บสำหรับสั่งให้ระบบทำการ Reboot เมื่อตอบตกลงแล้วจะต้องใช้เวลาในการ Reboot ช่วงหนึ่ง โดยจะไม่สามารถเรียกใช้งานหน้าเว็บได้ในขณะนั้นโดยสามารถแสดงตัวอย่างของหน้าเว็บ Reboot System ได้ดังรูปที่ ข.18




**รูปที่ ข.18** แสดงหน้าเว็บ Reboot System

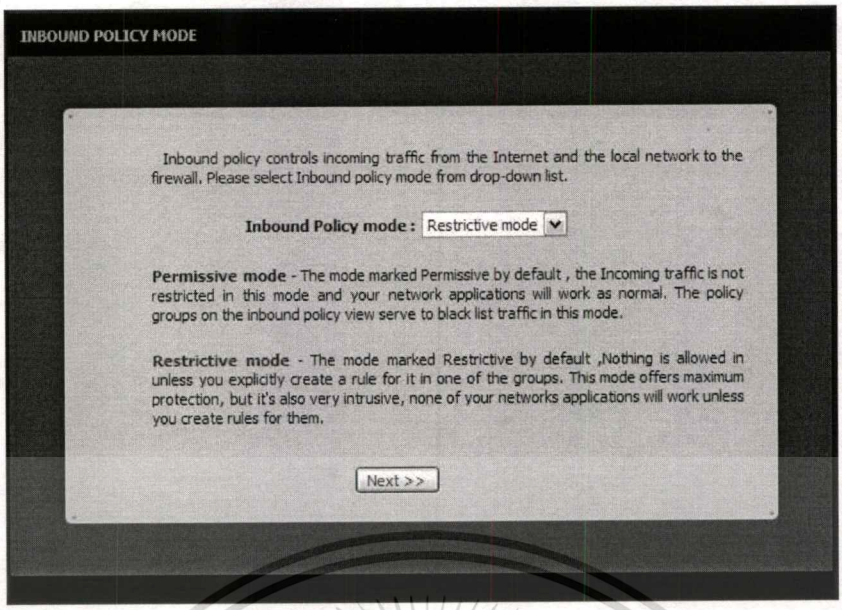
**4.5 Wizard Setup**

เพื่อช่วยอำนวยความสะดวกในการติดตั้งกฎต่างๆ หน้าเว็บ Wizard Setup จะทำการสร้างกฎต่างๆให้โดยอัตโนมัติ ซึ่งผู้ใช้จะต้องกำหนดคุณลักษณะต่างๆ ของไฟร์วอลล์ที่ต้องการ จากนั้นกฎจะถูกสร้างขึ้นตามคุณสมบัติที่ได้กำหนดไว้ โดยสามารถแสดงตัวอย่างของหน้าเว็บ Wizard setup ได้ดังรูปที่ ข.19




**รูปที่ ข.19** แสดงหน้าเว็บ Wizard setup กำหนด Public interface

จากรูปที่ ข.19 เป็นการทำงานในส่วนแรกของการกำหนดกฎแบบ Wizard setup โดยผู้ใช้ต้องทำการเลือก Interface ที่ติดต่อกับเครือข่ายภายนอกจากรายการที่ระบบตรวจพบ และจากนั้นเลือกปุ่ม Next เพื่อเข้าสูหน้าต่อไปคือการกำหนด Inbound policy mode ดังรูปที่ ข.20




**รูปที่ ข.20** แสดงหน้าเว็บ Wizard setup การกำหนด Inbound policy mode

จากรูปที่ ข.20 ผู้ใช้ต้องเลือกโหมดการทำงานทางด้าน Inbound ของไฟร์วอลล์ ซึ่งมีให้เลือก 2 โหมดคือ

**Permissive mode** คือ ส่งผ่านทุกแพ็กเก็ตทางด้านขาเข้าของไฟร์วอลล์

**Restrictive mode** คือ บล็อกทุกแพ็กเก็ตทางด้านขาเข้าของไฟร์วอลล์

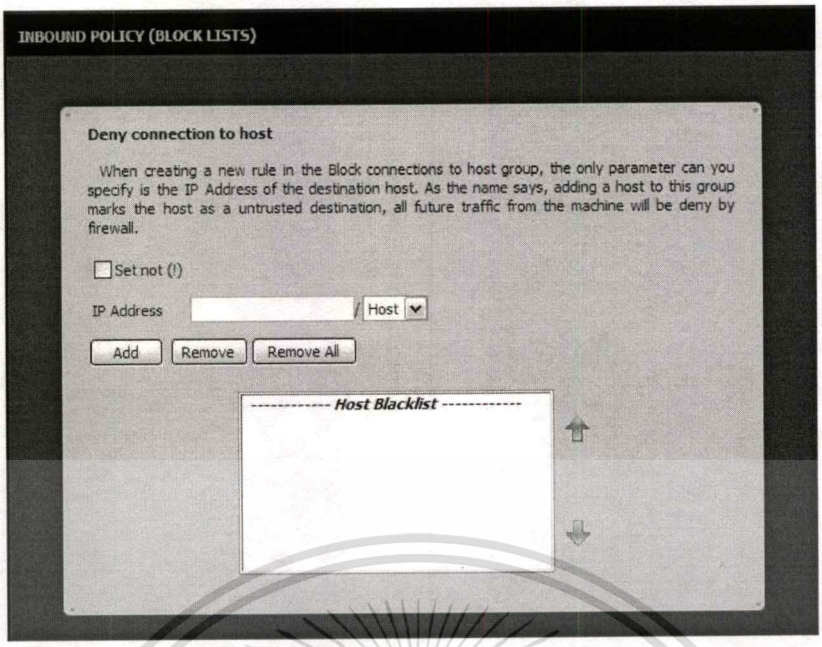
โดยเมื่อทำการเลือกโหมดใดโหมดหนึ่งจะทำให้มีผลต่อการทำงานในหน้าต่อไป ซึ่งถ้าเลือกเป็น Permissive mode จะทำให้การทำงานในส่วนต่อไปจะเป็นหน้าเว็บสำหรับกำหนดการทำงานในการบล็อกทางขาเข้าของไฟร์วอลล์ (Inbound block policy list) แต่ถ้าเลือก Restrictive mode จะเป็นหน้าเว็บสำหรับการกำหนดการทำงานในการส่งผ่านแพ็กเก็ตของไฟร์วอลล์ (Inbound allow policy list) โดยในหน้าเว็บสามารถกำหนดการทำงานได้สามส่วนคือ

กำหนดการตรวจสอบจากเครื่องปลายทางของแพ็กเก็ต (Deny /Allow connect to host)

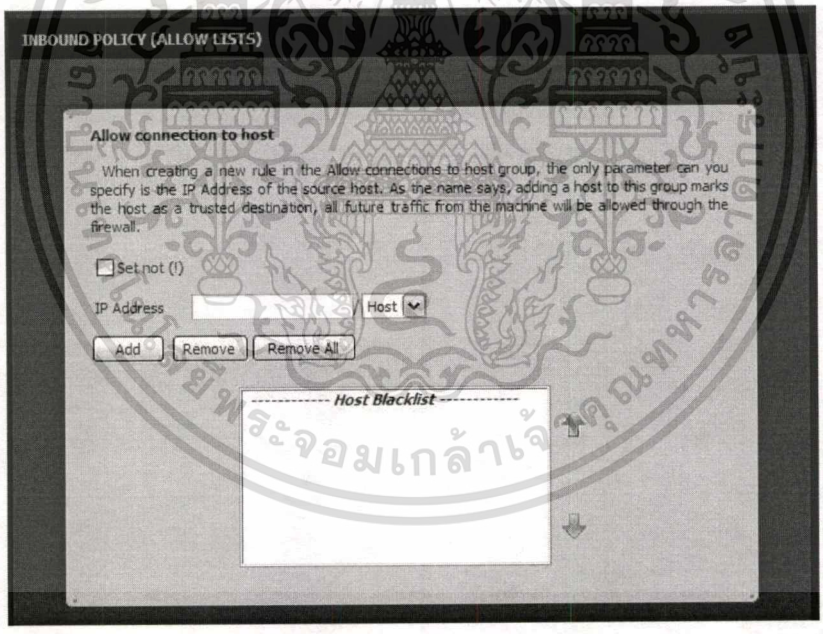
กำหนดการตรวจสอบจากเครื่องต้นทางของแพ็กเก็ต (Deny /Allow connect from host)

กำหนดการตรวจสอบจากพอร์ตและเครื่องต้นทางของแพ็กเก็ต (Deny /Allow service from host)

โดยทั้งสองหน้าเว็บแบบจะมีรูปแบบการกำหนดค่าที่เหมือนกัน ซึ่งสามารถแสดงได้ดังรูปที่ ข.21 และ ข.22

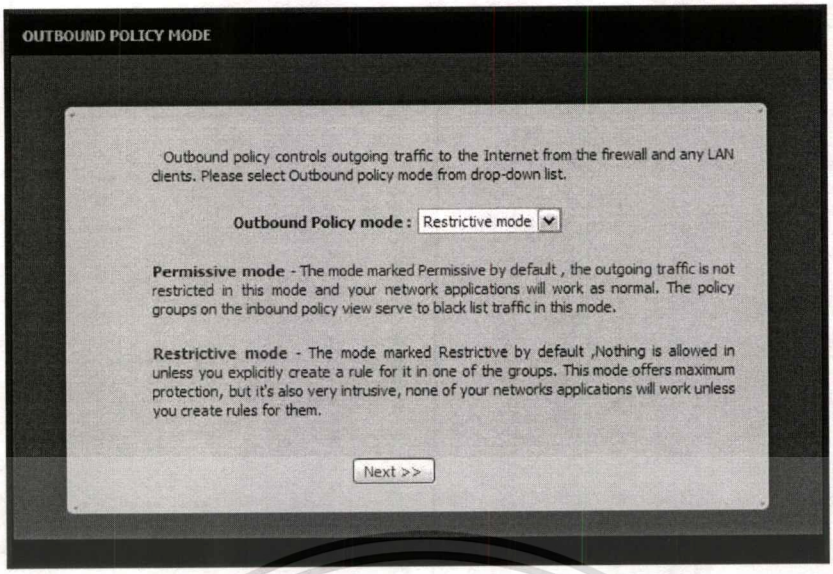



**รูปที่ ข.21** แสดงหน้าเว็บ Wizard setup การกำหนด Inbound block policy list




**รูปที่ ข.22** แสดงหน้าเว็บ Wizard setup การกำหนด Inbound allow policy list

หลังจากทำการกำหนดค่าในส่วนของ Inbound เรียบร้อยแล้ว ส่วนต่อไปจะเป็นส่วนของการกำหนดค่า Outbound ของไฟร์วอลล์ โดยส่วนแรกคือต้องเลือก Outbound policy mode โดยสามารถแสดงรายละเอียดได้ดังรูป ข.23




**รูปที่ ข.23** แสดงหน้าเว็บ Wizard setup การกำหนด Outbound policy mode

จากรูปที่ ข.23 ผู้ใช้ต้องเลือกโหมดการทำงานทางด้าน Outbound ของไฟร์วอลล์ ซึ่งมีให้เลือก 2 โหมดคือ

**Permissive mode** คือ ส่งผ่านทุกแพ็กเก็ตทางด้านขาออกของไฟร์วอลล์

**Restrictive mode** คือ บล็อกทุกแพ็กเก็ตทางด้านขาออกของไฟร์วอลล์

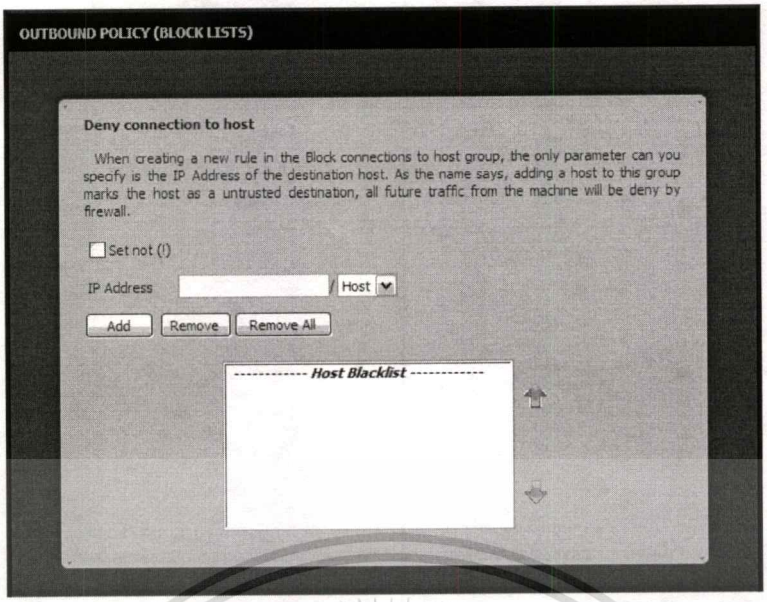
โดยเมื่อทำการเลือกโหมดใดโหมดหนึ่งจะทำให้มีผลต่อการทำงานในหน้าต่อไป ซึ่งถ้าเลือกเป็น Permissive mode จะทำให้การทำงานในส่วนต่อไปจะเป็นหน้าเว็บสำหรับกำหนดการทำงานในการบล็อกทางขาออกของไฟร์วอลล์ (Outbound block policy list) แต่ถ้าเลือก Restrictive mode จะเป็นหน้าเว็บสำหรับการกำหนดการทำงานในการส่งผ่านแพ็กเก็ตของไฟร์วอลล์ (Outbound allow policy list) โดยในหน้าเว็บสามารถกำหนดการทำงานได้สามส่วนคือ

กำหนดการตรวจสอบจากเครื่องปลายทางของแพ็กเก็ต (Deny /Allow connect to host)

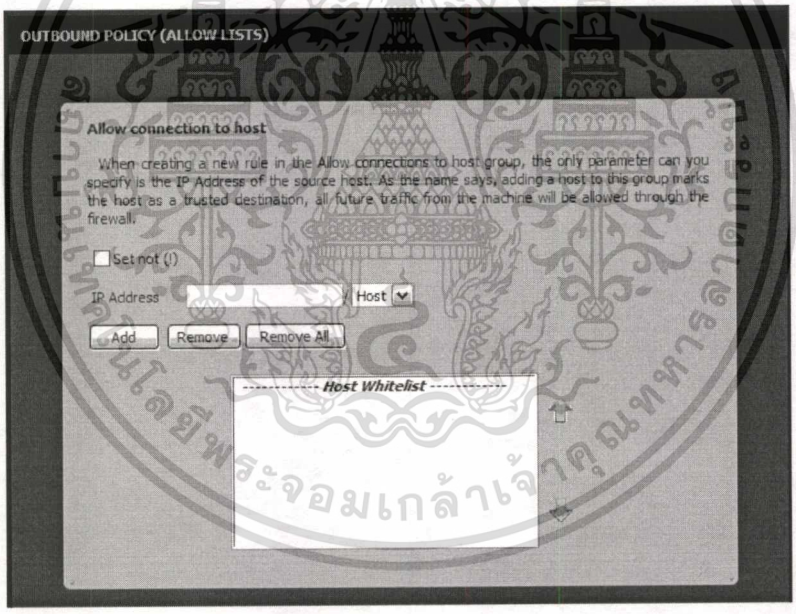
กำหนดการตรวจสอบจากเครื่องต้นทางของแพ็กเก็ต (Deny /Allow connect from host)

กำหนดการตรวจสอบจากพอร์ตและเครื่องต้นทางของแพ็กเก็ต (Deny /Allow service from host)

โดยทั้งสองหน้าเว็บแบบจะมีรูปแบบการกำหนดค่าที่เหมือนกัน ซึ่งสามารถแสดงได้ดังรูปที่ ข.24 และ ข.25

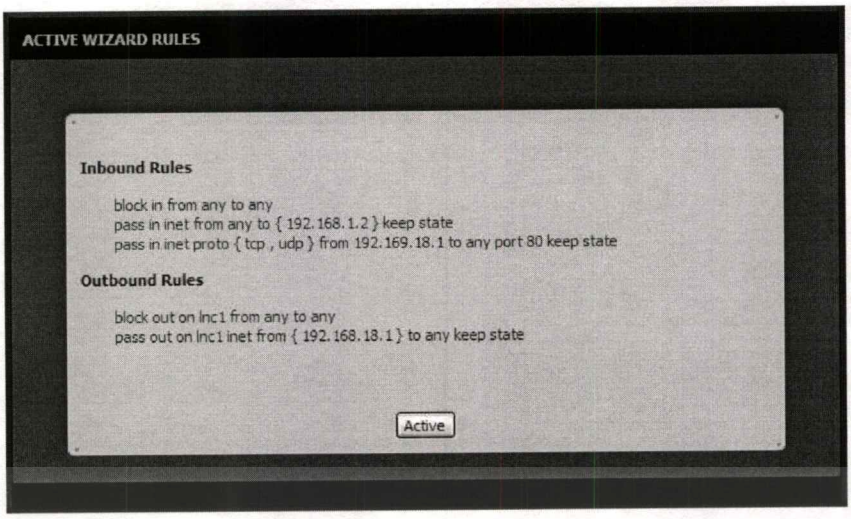



**รูปที่ ข.24** แสดงหน้าเว็บ Wizard setup การกำหนด Outbound block policy list




**รูปที่ ข.25** แสดงหน้าเว็บ Wizard setup การกำหนด Outbound allow policy list

หลังจากกำหนดข้อมูลทั้งในส่วนของ Inbound และ Outbound แล้วระบบจะสร้างกฎจากข้อมูลและแสดงข้อมูลของกฎและรอให้ผู้ใช้เลือกที่จะใช้งานกฎ ดังรูปที่ ข.24 โดยจะจบการทำงานในส่วนของ Wizard setup




**รูปที่ ข.26** แสดงหน้าเว็บ Wizard setup แสดงกฎที่ถูกสร้างขึ้นจากระบบ

# ประวัติผู้เขียน

| | |
|---|---|
| **ชื่อผู้เขียน** | **นายคงกะพัน อรรถชัยพานิช** |
| **วัน เดือน ปีเกิด** | 14 กันยายน 2522 |
| **สถานที่เกิด** | **จังหวัดกรุงเทพมหานคร** |
| **วุฒิระดับการศึกษา** | **อุตสาหกรรมศาสตรบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศเพื่ออุตสาหกรรม** |
| **สถาบันที่สำเร็จการศึกษา** | **สถาบันเทคโนโลยีพระจอมเกล้าพระนครเหนือ** |
| **ปีที่สำเร็จการศึกษา** | 2546 |