ห้องสมุดคณะเทคโนโลยีสารสนเทศ สจล.

การพัฒนายูสเซอร์อินเตอร์เฟสของไอพีไฟร์วอลล์บนฟรีบีเอสดี

THE DEVELOPMENT OF IPFIREWALL'S USER INTERFACE ON FREEBSD

โดย

ภาสพงศ์ ทักษิณา

PASSAPONG TAKSINA

H003480

อาจารย์ที่ปรึกษา

ผศ. อัครินทร์ คุณกิตติ

วัน เดือน ปี 4 ธ.ค. 2550
เลขทะเบียน H003480
เลขเรียกหนังสือ วพ. ภ 494ก 2549
"ห้องสมุดคณะเทคโนโลยีสารสนเทศ สจล."

6118420729
1117768-2

รายงานนี้เป็นส่วนหนึ่งของวิชาโครงการพัฒนาระบบงาน
หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
คณะเทคโนโลยีสารสนเทศ
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ภาคเรียนที่ 2 ปีการศึกษา 2549

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

THE DEVELOPMENT OF IPFIREWALL'S USER INTERFACE ON FREEBSD

PASSAPONG TAKSINA

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

2/ 2006

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

COPYRIGHT 2007

FACULTY OF INFORMATION TECHNOLOGY

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

หัวข้อ	การพัฒนายูสเซอร์อินเตอร์เฟสของไอพีไฟร์วอลล์บนฟรีบีเอสดี
นักศึกษา	นายภาสพงศ์ ทักษิณา
รหัสนักศึกษา	47066409
ปริญญา	วิทยาศาสตรมหาบัณฑิต
สาขาวิชา	เทคโนโลยีสารสนเทศ
แขนงวิชา	วิทยาการสารสนเทศ
ปีการศึกษา	2549
อาจารย์ที่ปรึกษา	ผศ. อัครินทร์ คุณกิตติ

บทคัดย่อ

ในการใช้งานเครือข่ายปัจจุบัน โปรแกรมไฟร์วอลล์นับเป็นเครื่องมือที่สำคัญที่สุดชิ้นหนึ่งที่ใช้ในการรักษาความปลอดภัยของเครือข่าย ในระบบปฏิบัติการฟรีบีเอสดีที่เป็นที่นิยมใช้ในการเป็นเครื่องแม่ข่ายนั้น ก็มีโปรแกรมไอพีไฟร์วอลล์ให้ใช้งานอยู่ด้วย ซึ่งการใช้งานโดยปกติแล้วมีความยุ่งยากและไม่สะดวกสบายในการจัดการ จึงได้มีการพัฒนาโปรแกรมเพื่อช่วยในการจัดการให้มีรูปแบบเป็น กราฟิกโดยการใช้งานผ่านโปรแกรมเว็บบราวเซอร์ ซึ่งเป็นที่ นิยมในปัจจุบัน แต่ในการใช้งานจริงกลับยังไม่มีความสะดวกสบายเท่าที่ควร ในโครงงานนี้จึงได้มีการพัฒนาเพิ่มเติมให้มีรูปแบบการใช้งานที่ง่ายโดยมีฟังก์ชั่น ในการทำงานคือ การเพิ่ม, ลบ และแสดงกฎรวมทั้งการลบค่าตัวนับแพ็คเก็ต และเพิ่มความสามารถในการจัดการส่วนต่างๆที่เกี่ยวข้อง เช่น การจัดการในเรื่องการวิเคราะห์กฎ โดยนำเอาทฤษฎีและผลการทดลองของ Ehab S. Al-Shaer ซึ่งได้ใช้ทฤษฎีของเซตในการนิยามความสัมพันธ์ของกฎเป็นแนวทางในการพัฒนา และมีฟังก์ชั่นในการปรับแต่งกฎเบื้องต้น รวมทั้งการตั้งค่าต่างๆ เช่น ดีเอชซีพี และแนท โดยมีการออกแบบระบบงานด้วยยูเอ็มแอลซึ่งเป็นเครื่องมือมาตรฐานในการออกแบบระบบงานต่างๆ ให้มีความสะดวกรวดเร็ว โดยนำเอาไดอะแกรมต่างๆ มาใช้ในการอธิบายระบบงานดังนี้ คือ ยูสเคสไดอะแกรมใช้อธิบายความต้องการฟังก์ชั่นของระบบ, แอคทิวิตีไดอะแกรมใช้อธิบายกิจกรรมที่เกิดขึ้นในการทำงาน, คลาสไดอะแกรมในการอธิบายโครงสร้างพื้นฐานของระบบ และซีเควันซ์ไดอะแกรมใช้อธิบายลำดับการทำงานของออบเจ็คต์ ซึ่งในการพัฒนาโครงงานนี้ มีผลการพัฒนาที่สามารถใช้งานฟังก์ชั่นต่างๆ และทำงานได้อย่างถูกต้อง เพื่อเป็นแนวทางในการนำไปพัฒนาต่อให้มีประสิทธิภาพยิ่งขึ้น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Title	The Development of IPFIREWALL's User Interface on FreeBSD
Student	Mr. Passapong Taksina
Student ID.	47066409
Degree	Master of Science
Programme	Information Science
Academic Year	2006
Advisor	Assist. Prof. Akharin Khunkitti

ABSTRACT

To day, in the using of network system. Firewall is the most important security program. FreeBSD, a famous network server operating system, also has IPFIREWALL for security using the properly use is not comfortable to manage program. The development of IPFIREWALL's web-based user interface has developed. But in real using program are not enough convenient using. This project have develop new form for easily using with insert, delete and show rules function including zero the counters and improve managing capacity, ie. Analyzing rules that bring an experiment of Ehab S. Al-Shaer, that use theory of set to prove association between rules. And have more configuration to customize rules including config DHCP and NAT. By analysis and design with UML, standard tool for design system, that can work quickly. Using diagram for describe system. Use-case diagram for describe functional requirement of system, activity diagram for describe activity in each scenario, class diagram for describe infrastructure of system, and sequence diagram for describe order of work between object. In this project has a result of using that work every function. For guideline to develop make more performance.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

กิตติกรรมประกาศ

โครงงานฉบับนี้สำเร็จได้อย่างดี ด้วยคำแนะนำ และคำปรึกษาจาก ผศ. อัครินทร์ คุณกิตติ ซึ่งเป็นอาจารย์ผู้ควบคุมโครงงาน ข้าพเจ้ารู้สึกซาบซึ้งในความอนุเคราะห์จากท่านอาจารย์ และขอขอบพระคุณเป็นอย่างสูง

ขอกราบพระคุณคณาจารย์ภาควิชาเทคโนโลยีสารสนเทศ คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง ทุก ๆ ท่านที่ได้ประสิทธิ์ประสาทวิชาให้กับข้าพเจ้า

ขอขอบคุณเพื่อนๆ พี่ๆ น้องๆ ในภาควิชาเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยี พระจอมเกล้าเจ้าคุณทหารลาดกระบัง ทุกคนที่ให้คำแนะนำต่างๆ และคอยให้กำลังใจเสมอมา

ขอขอบคุณบัณฑิตศึกษาและบัณฑิตวิทยาลัย คณะเทคโนโลยีสารสนเทศที่ให้ความช่วยเหลือ ในเรื่องต่างๆ

สุดท้ายนี้ข้าพเจ้าขอกราบขอบพระคุณ บิดา มารดา และครอบครัวของข้าพเจ้าที่เป็นกำลังใจและให้การสนับสนุนในทุกเรื่องๆ ทำให้ข้าพเจ้าสามารถทำโครงงานฉบับนี้สำเร็จลุล่วงด้วยดี

คุณค่าและประโยชน์อันพึงมาจากโครงงานฉบับนี้ ข้าพเจ้าขอมอบแด่ผู้มีพระคุณทุกท่าน

ภาสพงศ์ ทักษิณา

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญ

หน้า

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญ (ต่อ)

หน้า

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญ (ต่อ)

หน้า

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญตาราง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญรูป

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญรูป (ต่อ)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญรูป (ต่อ)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ในการทำงานของระบบงานต่างๆ ในปัจจุบันจำเป็นจะต้องมีการติดต่อสื่อสารกันทั้งภายในเครือข่ายเดียวกันเองและระหว่างเครือข่ายภายนอก ซึ่งอาจเป็นไปได้ว่าจะมีผู้ไม่ประสงค์ดีจากเครือข่ายภายนอกอาจใช้ประโยชน์จากข้อมูลต่างๆ ที่อาจถูกเผยแพร่ออกไปภายนอกทำการบุกรุกเข้ามายังเครือข่ายภายในองค์กรทำให้เกิดความเสียหายได้ ดังนั้นการป้องกันและรักษาความปลอดภัยของเครือข่ายจึงต้องมีเครื่องมือ ต่างๆ เพิ่มเข้ามาเพื่อควบคุมและจัดการการส่งผ่านเข้าออกและกำหนดสิทธิของข้อมูลจากเครือข่ายภายนอก ซึ่งก็คือไฟร์วอลล์ นั่นเอง ซึ่งไฟร์วอลล์มีอยู่หลายประเภท เพื่อให้เหมาะกับลักษณะการทำงานของเครือข่ายนั้นๆ คือ ไฟร์วอลล์แบบการกรองแพ็คเก็ตซึ่งอนุญาตหรือ ปฏิเสธแพ็คเก็ตต่างๆ ที่จะเข้ามาในระบบโดยการตั้งกฎ ส่วนไฟร์วอลล์ประเภทพร็อกซี่บริการ ซึ่งมักจะเป็นโปรแกรมเฉพาะที่ทำงานอยู่บนโฮสต์โดยตั้งอยู่ระหว่างผู้ใช้ภายในกับอินเทอร์เน็ตภายนอกและทำหน้าที่ในการติดต่อขอใช้บริการต่างๆ จากภายนอกแทนผู้ใช้บริการ ไฟร์วอลล์ที่นิยมใช้กันส่วนใหญ่ก็คือ ไฟร์วอลล์ประเภทการกรองแพ็คเก็ต หรือ แพ็คเก็ตฟิลเตอริ่ง ซึ่งในการใช้งานของไฟร์วอลล์ประเภทนี้จะนำไปติดตั้งอยู่บนอุปกรณ์เครือข่ายต่างๆ เช่น เร้าเตอร์ หรืออยู่บนตัวเครื่องเซิร์ฟเวอร์ของเครือข่าย ซึ่งจะต้องทำการคอนฟิกหรือปรับแต่งค่าต่างๆ ที่จำเป็นต้องใช้ในเครือข่ายโดยผู้ดูแลระบบ ซึ่งสามารถที่จะเข้าไปจัดการในส่วนของกฎที่ใช้อยู่ เช่น การนิยามกฎต่างๆ ในการจัดการการทำงานต่างๆเหล่านี้อาจจะใช้งานได้ไม่สะดวก ซึ่งผู้ใช้จะต้องจดจำคำสั่ง และตัวเลือกต่างๆ ในการตั้งค่าเพื่อที่จะใช้งานไฟร์วอลล์ จึงเป็นที่มาของโครงงานที่จะพัฒนาในส่วนติดต่อกับผู้ใช้ขึ้น เพื่อให้มีความสะดวกและใช้งานได้ง่ายขึ้น โดยเลือกโปรแกรมไอพีไฟร์วอลล์ที่ใช้งานบนระบบปฏิบัติการฟรีบีเอสดี ซึ่งเป็นระบบปฏิบัติการที่สามารถใช้งานได้ฟรีและเป็นโอเพ่นซอร์ส ที่ผู้ใช้สามารถนำตัวระบบไปปรับแต่งได้เองเพื่อให้สามารถใช้งานได้อย่างเหมาะสมกับลักษณะของงานได้

1.2 ความมุ่งหมายและวัตถุประสงค์ของการศึกษา

โครงงานฉบับนี้มุ่งหวังเพื่อศึกษาการทำงานของโปรแกรมไอพีไฟร์วอลล์ ซึ่งเป็นบริการส่วนหนึ่งในระบบปฏิบัติการฟรีบีเอสดี โดยเป็นระบบปฏิบัติการที่เป็นโอเพ่นซอร์สและสามารถหามาใช้งานได้ง่ายและไม่ต้องเสียค่าใช้จ่ายใดๆ อีกทั้งผู้ใช้ยังสามารถนำมาปรับแต่งการทำงานต่างๆ ได้ด้วยตัวเองเพื่อให้เหมาะสมกับลักษณะงานที่ใช้ได้ ซึ่งระบบปฏิบัติการฟรีบีเอสดีนี้ได้รับความนิยมในการใช้งานมากและนำไปใช้ในระบบเครือข่ายมากขึ้น ดังนั้นในโครงงานนี้จึงเสนอ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งไม่อนุญาตให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารนี้ทุกครั้งที่มีการนำไปใช้

การพัฒนายูสเซอร์อินเตอร์เฟสในการใช้งานโปรแกรมไอพีไฟร์วอลล์ ซึ่งเป็นบริการในการรักษาความปลอดภัยในการใช้งานแบบเครือข่าย ที่โดยปกติแล้วในการปรับแต่งใช้งานโปรแกรมยังไม่มีความสะดวกสบายนัก ให้สามารถใช้งานได้ง่ายมากขึ้นกว่าเดิม และเป็นแนวทางในการพัฒนาให้กับผู้ที่สนใจนำไปพัฒนาต่ออีกด้วย

1.3 สมมติฐานของการศึกษา

ระบบปฏิบัติการฟรีบีเอสดีเป็นระบบปฏิบัติการยูนิกส์ที่พัฒนาต่อมาจาก AT&T's UNIX ของมหาวิทยาลัย Berkley ซึ่งระบบปฏิบัติการฟรีบีเอสดีได้รับการพัฒนาจากกลุ่มคนที่ทำงานวิจัยของคณะวิทยาศาสตร์คอมพิวเตอร์ของมหาวิทยาลัย Berkley ที่แคลิฟอร์เนีย ให้เป็นระบบปฏิบัติการที่สามารถทำงานได้บนหลายแพลตฟอร์มและมีความสามารถหลากหลายขึ้น ซึ่งระบบปฏิบัติการฟรีบีเอสดีมีบริการของไฟร์วอลล์ให้ใช้งานและถูกนำไปรวมอยู่ในเคอร์เนลทำให้สามารถดูแลและควบคุมพฤติกรรมโดยรวมและเปลี่ยนแปลงนโยบายทางด้านความปลอดภัยของการติดต่อสื่อสารได้ ซึ่งไฟร์วอลล์บนระบบปฏิบัติการฟรีบีเอสดีที่กล่าวถึงนี้คือ ไอพีไฟร์วอลล์ เป็นไฟร์วอลล์ประเภทการกรองแพ็คเก็ต โดยการใช้งานจะต้องมีการคอมไพล์เคอร์เนล ซึ่งต้องทำการแก้ไขคอนฟิกไฟล์ของเคอร์เนลโดยการเพิ่มตัวเลือก เพื่อให้สามารถใช้งานไอพีไฟร์วอลล์ได้ การจัดการและดูแลการทำงานของไอพีไฟร์วอลล์ ปัจจุบันจะต้องมีการตั้งค่าโดยให้ผู้ใช้ โดยมีส่วนติดต่อกับผู้ใช้ ในรูปแบบที่ต้องพิมพ์คำสั่งในการจัดการผ่าน คอมมานด์ไลน์ ซึ่งใช้งานได้ยากและไม่สะดวกนัก อาจทำให้เกิดความผิดพลาดในการตั้งค่าต่างๆ ในไฟร์วอลล์ได้ จึงเป็นแนวคิดที่จะพัฒนารูปแบบในการจัดการและใช้งานไอพีไฟร์วอลล์ให้มีความเรียบร้อยและใช้งานได้ง่ายมากขึ้น

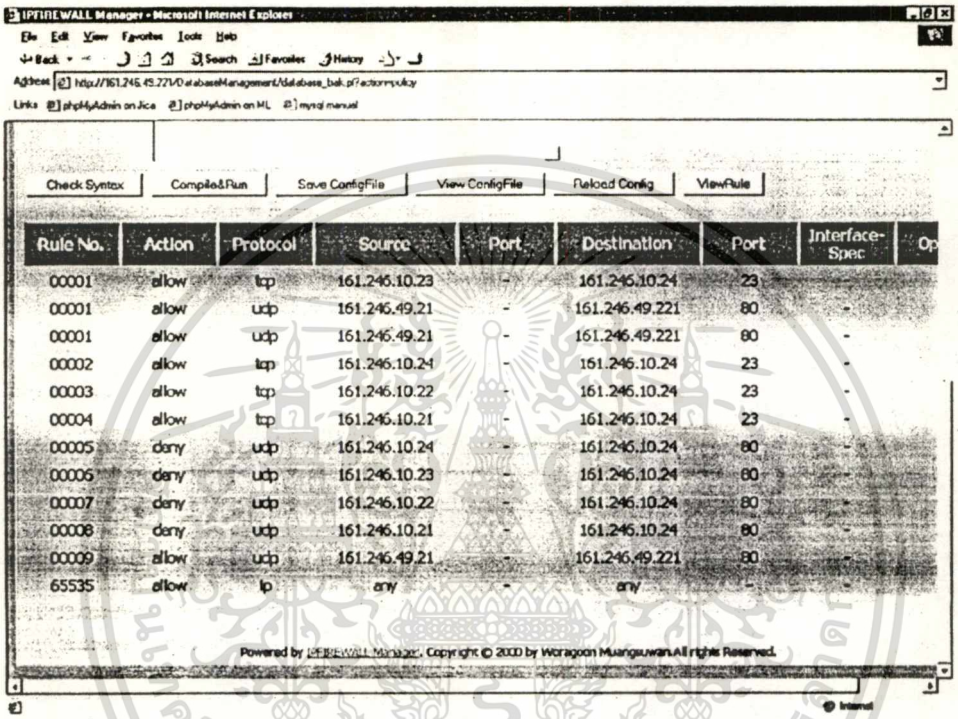
ในการกำหนดรูปแบบของนโยบายหรือกฎขึ้นมาใหม่นั้นจุดประสงค์คือ เพื่อให้เป็นรูปแบบที่ผู้ใช้สามารถที่จะใช้และเข้าใจได้ง่าย และสะดวกในการทำงานมากกว่ารูปแบบเดิม อีกทั้งยังมีการกำหนดรายละเอียดในรูปแบบของนโยบายหรือกฎให้มีความสามารถ ในการจัดการเมื่อมีความขัดแย้งของกฎเกิดขึ้น เพื่อเพิ่มประสิทธิภาพของการทำงาน เช่น มีการระบุรายละเอียดต่างๆ เพื่อให้สอดคล้องกับการกำหนดลำดับความสำคัญของกฎหรือนโยบายขึ้น

เมื่อผู้ใช้กำหนดนโยบายหรือกฎที่โปรแกรมต้องการแล้วจึงดำเนินการแปลงรูปแบบของกฎให้อยู่ในรูปแบบเดิมที่โปรแกรมไอพีไฟร์วอลล์สามารถเข้าใจได้ แล้วจึงดำเนินการตามที่ได้กำหนดไว้ในกฎที่เขียนขึ้น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

1.4 ระบบงานเดิม

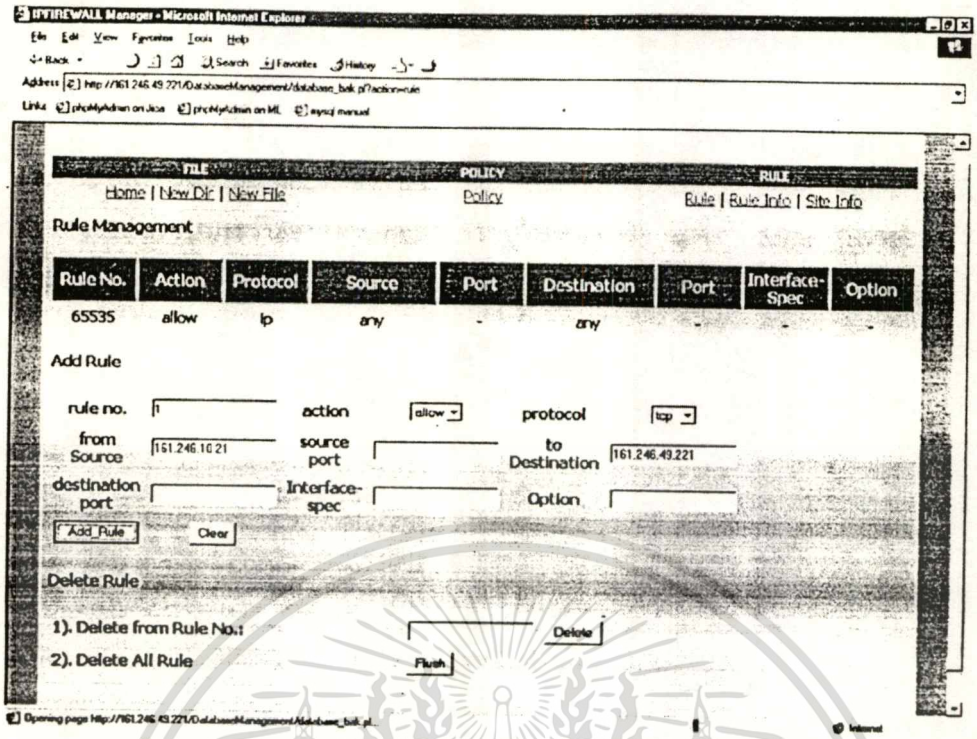
การพัฒนาโปรแกรมจัดการไอพีไฟร์วอลล์ได้มีการพัฒนาเป็นรูปแบบการใช้งานเป็น กราฟิค มาแล้ว ซึ่งในระบบงานเดิมนั้นได้มีผู้พัฒนาคือในโครงงานของคุณ วรกุล เมืองสุวรรณที่ได้มีการพัฒนาโปรแกรมจัดการผ่านทางโปรแกรมเว็บบราวเซอร์ซึ่งมีข้อดีที่สามารถใช้งานได้ง่ายและทำงานได้ในหลากหลายแพล็ตฟอร์ม ซึ่งมีลักษณะอินเตอร์เฟสดังนี้



รูปที่ 1.1 อินเตอร์เฟสในการแสดงผลกฎในระบบงานของวรกุล เมืองสุวรรณ

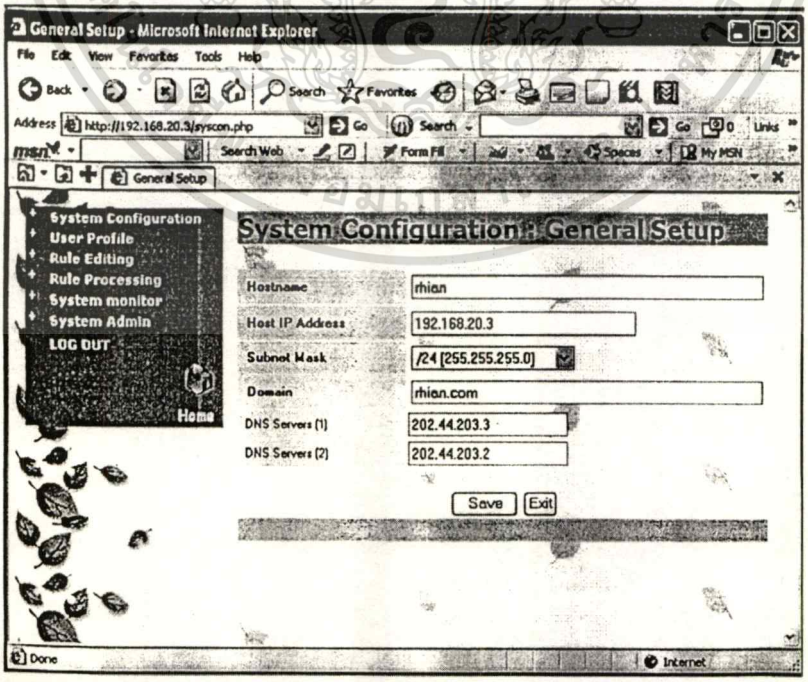
ในส่วนของการแสดงผลรายการกฎนี้ได้แบ่งการแสดงผลออกเป็นรูปแบบตาราง ซึ่งมีการแสดงฟิลด์ต่างๆ ของกฎที่ใช้อยู่อย่างชัดเจนและเข้าใจได้ง่าย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 1.2 ลักษณะอินเตอร์เฟสในการจัดการกฎของวรกุล เมืองสุวรรณ

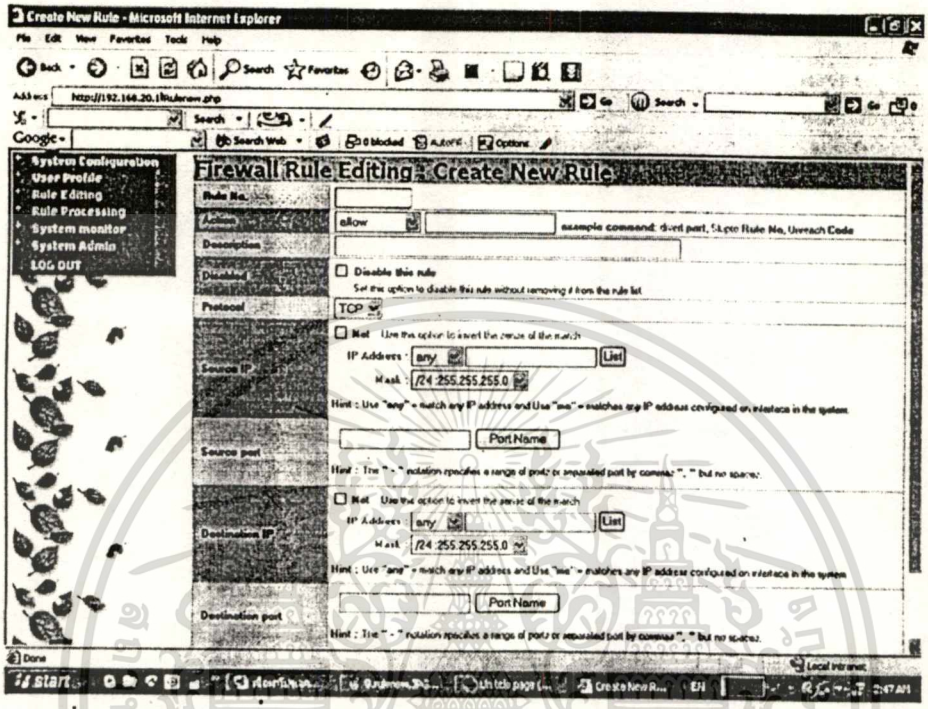
ซึ่งจากลักษณะอินเตอร์เฟสดังรูป จะเป็นการจัดการการทำงานต่างๆ อยู่ภายในหน้าจอเดียว ซึ่งผู้ใช้จะต้องมีการกำหนดค่าเอง ไม่ต่างจากการใช้งานโปรแกรมดั้งเดิมมากนัก และการแสดงผลอาจทำให้ผู้ใช้สับสนหรือเข้าใจการใช้งานได้ยาก ซึ่งต่อมาได้มีการพัฒนา ขึ้นจากโครงงานของคุณ ธัญลักษณ์ ผังชัยมงคลซึ่งมีลักษณะอินเตอร์เฟสที่มีความสวยงามมากขึ้น



รูปที่ 1.3 ลักษณะอินเตอร์เฟสในส่วนการจัดการค่าต่างๆ ของธัญลักษณ์ ผังชัยมงคล

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ในการพัฒนาโครงงานของคุณ ธัญลักษณ์ ได้มีการแบ่งส่วนการทำงานต่างๆ ออกเป็นเมนูต่างๆ ให้สามารถใช้งานได้ง่ายขึ้นและมีการเพิ่มเติมการทำงานในส่วนการจัดการกับข้อมูลระบบที่เกี่ยวข้องอีกด้วย



รูปที่ 1.4 ลักษณะอินเตอร์เฟสในส่วนการสร้างกฎของ ธัญลักษณ์ ผังชัยมงคล

ในการพัฒนาของระบบงานเดิมนั้นยังมีส่วนของการจัดการเกี่ยวกับกฎที่ไม่มากนักซึ่งการเพิ่มเติมฟังก์ชันการทำงานอื่นๆ ที่เกี่ยวข้องนั้น เช่น การวิเคราะห์กฎหรือส่วนของกฎปรับแต่งกฎเบื้องต้น จะช่วยเพิ่มความสะดวกให้กับผู้ใช้มากขึ้น

1.5 ทฤษฎีหรือแนวคิดที่ใช้ในการพัฒนา

ทฤษฎีที่ใช้ได้แก่โครงสร้างและการทำงานของโปรแกรมไอพีไฟร์วอลล์ ระบบปฏิบัติการฟรีบีเอสดี การวิเคราะห์และออกแบบโดยใช้ UML และการพัฒนาโปรแกรมโดยใช้ PHP ให้สามารถใช้งานโปรแกรมผ่านทางเว็บบราวเซอร์ และทฤษฎีในการตรวจหา ความผิดปกติที่เกิดขึ้นระหว่างกฎที่มีความสัมพันธ์กัน โดยยึดตามเอกสารของ Ehab S. Al-Shaer ซึ่งมีการใช้ทฤษฎีของเซตในการนิยามความสัมพันธ์ของกฎต่างๆ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

1.6 ขอบเขตการพัฒนา

-สามารถทำให้โปรแกรมไอพีไฟร์วอลล์ทำงานผ่านหน้าโปรแกรมเว็บบราวเซอร์ที่เขียนขึ้นด้วย PHPได้

-โปรแกรมสามารถทำงานได้โดยไม่ทำให้เสียประสิทธิภาพและความถูกต้องของโปรแกรมไอพีไฟร์วอลล์ดั้งเดิม ซึ่งมีฟังก์ชันในการทำงานต่างๆ ในระบบงานเดิมดังนี้

ฟังก์ชันการทำงานพื้นฐาน

- สามารถเพิ่มกฎได้
- สามารถลบกฎ ที่มีอยู่ออกได้
- สามารถแสดงรายการกฎที่ใช้ในปัจจุบันได้
- สามารถปรับค่าตัวนับแพ็คเก็ตได้

ฟังก์ชันการทำงานเพิ่มเติมที่ได้มีการพัฒนาเพิ่มจากระบบงานเก่า

- สามารถตรวจสอบการทำงานของจำนวนแพ็คเก็ตที่ผ่านเข้ามาจาก log file ได้
- สามารถวิเคราะห์กฎขั้นพื้นฐานและจัดการกับความผิดปกติได้
- สามารถตั้งค่า NAT ได้
- สามารถตั้งค่า DHCP ได้

1.7 ขั้นตอนของการศึกษา

โครงงานฉบับนี้ได้แบ่งเนื้อหาออกเป็น 5 บทด้วยกันคือ

บทที่ 1 กล่าวถึงความเป็นมาของงานวิจัย ความมุ่งหมายและวัตถุประสงค์ สมมติฐาน ทฤษฎีที่ใช้ ขอบเขตของการพัฒนาโครงงาน และขั้นตอนการศึกษาโครงงาน

บทที่ 2 กล่าวถึงทฤษฎีพื้นฐานที่ใช้ในการพัฒนาโครงงาน

บทที่ 3 กล่าวถึงการออกแบบตัวโครงงานของยูสเซอร์อินเตอร์เฟสของไอพีไฟร์วอลล์

บทที่ 4 กล่าวถึงการทำงานของตัวโปรแกรมและผลลัพธ์ที่ได้จากการใช้งาน

บทที่ 5 เป็นบทสรุปผลการพัฒนาและข้อเสนอแนะ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 2
การพัฒนาโปรแกรมจัดการไอพีไฟร์วอลล์

ในหัวข้อนี้จะกล่าวถึงทฤษฎีพื้นฐานต่างๆ ที่เกี่ยวข้องในการพัฒนาโปรแกรม ซึ่งเนื้อหาในบทนี้จะกล่าวถึงความหมายของชื่อ และลักษณะของระบบปฏิบัติการรวมถึง ประเภทของไฟร์วอลล์ที่ใช้งานอยู่ในปัจจุบัน รวมถึงภาษา, เครื่องมือ และอัลกอริทึมต่างๆ ที่ใช้ในการพัฒนาโครงงานอีกด้วย ซึ่งเนื้อหาทั้งหมดนี้จำเป็นสำหรับการศึกษา และพัฒนาโครงงานนี้

2.1 ระบบปฏิบัติการฟรีบีเอสดี

ระบบปฏิบัติการฟรีบีเอสดี (FreeBSD : Free Berkeley Software Distribution) เป็นระบบปฏิบัติการขั้นสูงที่สามารถทำงานได้บนสถาปัตยกรรมหลายๆ แบบ เช่น x86 (รวมทั้ง Pentium® and Athlon™), amd64 (รวมทั้ง Opteron™, Athlon 64, และ EM64T), UltraSPARC®, IA-64, PC-98 และ สถาปัตยกรรมแบบ ARM โดยมีต้นกำเนิดมาจาก BSD Unix ของมหาวิทยาลัย California, Berkeley ซึ่งมีการดูแลและพัฒนาโดยทีมงานขนาดใหญ่ ระบบปฏิบัติการฟรีบีเอสดี มีคุณสมบัติที่โดดเด่นหลายๆ ด้าน ทั้งความสามารถในการจัดการกับเครือข่ายชั้นสูง, มีประสิทธิภาพ, ความปลอดภัยของระบบ และสามารถเข้ากันได้กับเครื่องคอมพิวเตอร์หลายๆ สถาปัตยกรรม เราสามารถใช้ระบบปฏิบัติการฟรีบีเอสดีในการสร้างเซิร์ฟเวอร์แบบอินเทอร์เน็ตและอินทราเน็ตพร้อมทั้งยังสามารถรองรับการทำงานกับเครือข่ายที่มีการโหลดข้อมูลมากๆ และสามารถใช้หน่วยความจำได้อย่างมีประสิทธิภาพถึงแม้จะมีการใช้งานของผู้ใช้เข้ามาในระบบในปริมาณมากๆ ก็ตาม ซึ่งเราสามารถดาวน์โหลดระบบปฏิบัติการนี้มาใช้งานได้โดยไม่เสียค่าใช้จ่ายใดๆ

เป้าหมายของโครงการฟรีบีเอสดีนี้คือ การจัดหาซอฟต์แวร์ที่สามารถใช้งานได้หลายวัตถุประสงค์โดยไม่มีการผูกมัดใดๆ

ซอร์สโค้ดทั้งหมดของระบบปฏิบัติการฟรีบีเอสดี อยู่ภายใต้ BSD License ซึ่งสามารถนำไปพัฒนาเพิ่มความซับซ้อนเพื่อนำไปใช้ในการค้าได้ ถึงแม้ว่าจะอยู่ภายใต้ลิขสิทธิ์ของ BSD ก็ตาม

ฟรีบีเอสดีมีการพัฒนาโปรแกรมประยุกต์คุณภาพสูงขึ้นใช้งานอย่างมากมายโดยศูนย์วิจัยและมหาวิทยาลัยต่างๆ ทั่วโลกซึ่งส่วนใหญ่จะไม่ต้องเสียค่าใช้จ่ายในการใช้งาน และยังมีการพัฒนาปรากฏเป็นจำนวนมากขึ้นทุกๆ วัน

เพราะว่าซอร์สโค้ดของฟรีบีเอสดีมีอยู่ทั่วไป ระบบจึงสามารถนำมาปรับแต่งให้ใช้งานโดยเฉพาะโปรแกรมหรือโครงการใดๆ ซึ่งโดยปกติแล้วไม่สามารถทำได้จากระบบปฏิบัติการที่มี

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น ไม่อนุญาตให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ขายอยู่ส่วนใหญ่ ตัวอย่างในการใช้งานของโปรแกรมที่ผู้ใช้นิยมในระบบฟรีบีเอสดีในปัจจุบันคือบริการทางด้านเครือข่ายอินเทอร์เน็ต เช่น FTP servers, World Wide Web servers (standard หรือ secure [SSL]), Firewalls และ NAT ("IP masquerading") gateways, Electronic Mail servers, USENET News หรือ Bulletin Board Systems

ระบบปฏิบัติการฟรีบีเอสดีได้มีการพัฒนาจนออกตัวล่าสุดคือ ฟรีบีเอสดีเวอร์ชัน 6.1 โดยพัฒนามาจากแขนงของเวอร์ชัน 6.X โดยมีการเพิ่มประสิทธิภาพและแก้ไขบั๊กหลายๆ ตัว และเพิ่มการทำงานใหม่ๆ รวมทั้ง รองรับการใช้คีย์บอร์ดทั้งชนิด USB และ PS/2 ได้โดยไม่ต้องทำการเริ่มระบบใหม่อีกครั้ง, แก้ไขความเสถียรของระบบไฟล์หลายแห่ง ให้สามารถรองรับการทำงานในปริมาณมากๆ ได้, ปรับแต่งการใช้งานอุปกรณ์ Bluetooth โดยอัตโนมัติ แบบเดียวกันกับการสนับสนุนการใช้งานอุปกรณ์ WiFi อัตโนมัติ, เพิ่มไดรฟ์เวอร์ควบคุม Ethernet และ SATA Raid ใหม่ และอัพเดท BIND และ Sendmail ใหม่

รูปที่ 2.1 หน้าเว็บไซต์ของฟรีบีเอสดี

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.2 Apache Web Server

Apache Web Server เป็นโปรแกรมที่ทำหน้าที่เป็นเว็บเซิร์ฟเวอร์ ที่มีประสิทธิภาพสูงและได้รับความนิยมสูงมากในปัจจุบัน สามารถรองรับการทำงานได้หลากหลายแพลตฟอร์ม ไม่ว่าจะเป็น MS-Windows, Linux, Unix รวมทั้ง FreeBSD เองก็สามารถทำงานได้ และตัวโปรแกรมของ Apache Web Server ก็สามารถสนับสนุนการรักษาความปลอดภัยโดยเราสามารถเพิ่มส่วนของการทำงานเป็น SSL (Secure Socket Layer) เพื่อทำให้การรับส่งข้อมูลระว่างเว็บไคลเอ็นท์ และเว็บเซิร์ฟเวอร์ถูกเข้ารหัสข้อมูล ทำให้ผู้ที่แอบขโมยข้อมูลระหว่างทาง ไม่สามารถขโมยข้อมูลได้ หรือ ขโมยได้ลำบากมากขึ้นด้วย

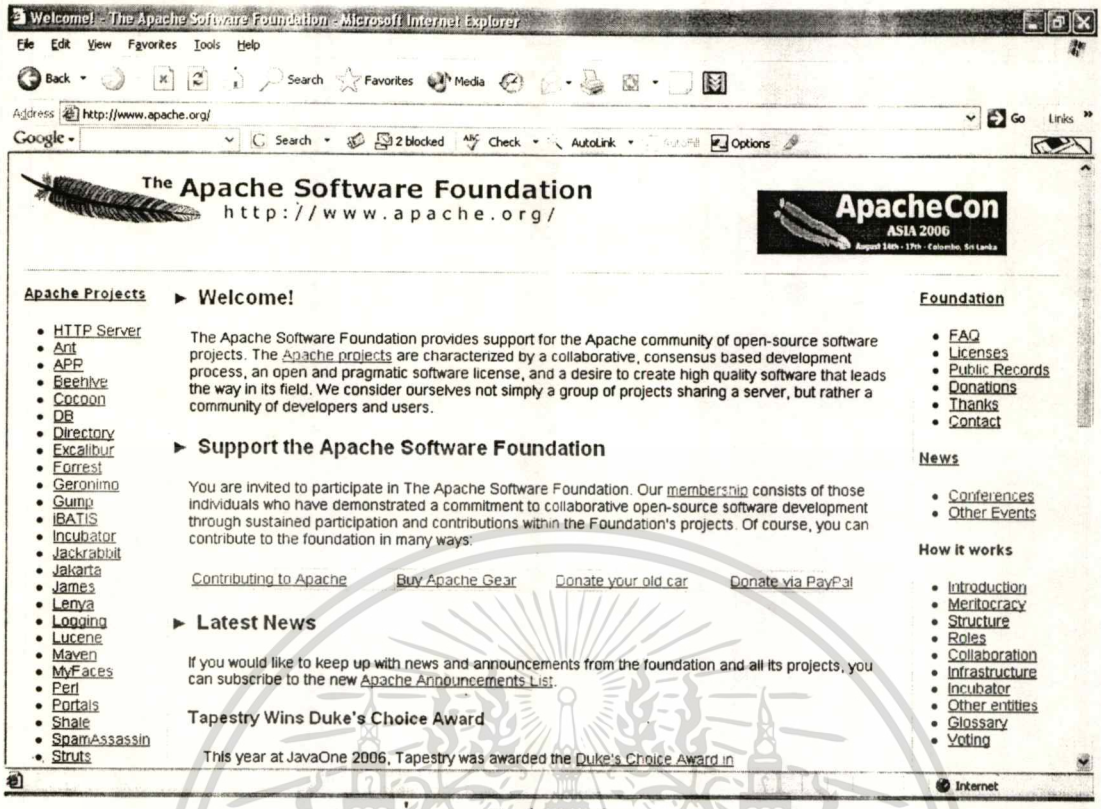
Apache Software Foundation (ASF) เป็นองค์กรที่ไม่แสวงหาผลกำไรที่จัดตั้งขึ้นในสหรัฐอเมริกา ซึ่งมีสร้างมาเพื่อจุดประสงค์หลักคือ ร่วมมือกันพัฒนาซอฟต์แวร์เปิด โดยจัดหาฮาร์ดแวร์, การติดต่อสื่อสาร และโครงสร้างพื้นฐานทางธุรกิจ สร้างความชอบธรรมในการที่บุคคลและบริษัทสามารถบริจาคทรัพยากรให้ใช้เพื่อประโยชน์ส่วนรวม และป้องกันเครื่องหมาย 'Apache' ให้กับผลิตภัณฑ์ซอฟต์แวร์ไม่ให้องค์กรอื่นๆ นำไปใช้ในทางที่ผิด

ในปี ค.ศ. 1999 กลุ่มคนกลุ่มหนึ่งซึ่งเรียกตัวพวกเขาว่า 'Apache Group' ได้เป็นอาสาสมัครในการสนับสนุนและดูแลเว็บเซิร์ฟเวอร์ HTTPD ที่เขียนขึ้นโดย NCSA ซึ่งเปิดให้ใช้งานฟรี โดยพยายามให้มีคุณภาพระดับเดียวกันกับซอฟต์แวร์ในทางการค้า พร้อมกับมีซอร์สโค้ดและลิขสิทธิ์ ซึ่งอนุญาตให้มีการแก้ไขดัดแปลงและเผยแพร่ได้ ผู้ใช้บางกลุ่มจึงได้เริ่มแลกเปลี่ยนร่วมมือดูแลแก้ไข (หรือเรียกว่า 'patch') และให้ข้อมูลในการป้องกันไม่ให้เกิดปัญหาและเพิ่มประสิทธิภาพของซอฟต์แวร์ให้ดียิ่งขึ้น

ชื่อ 'Apache' ได้ถูกนำมาใช้จากชื่อของชนเผ่าพื้นเมืองอินเดียนอเมริกันที่ชื่อว่าชนเผ่า Apache ซึ่งมีทักษะในการวางกลยุทธ์ในการสู้รบและมีความอดทนไม่เหน็ดไม่เหนื่อย ดังนั้นจึงนำมาใช้สร้างเว็บเซิร์ฟเวอร์ให้มีความหมายดังกล่าวนั่นเอง

Apache ได้มีการพัฒนามาแล้วจนถึงเวอร์ชัน 2.2.2 ซึ่งได้เพิ่มเติมความสามารถหลายอย่าง รวมทั้ง Smart Filtering, เพิ่มการ Caching, Proxy Load Balancing, สนับสนุน Graceful Shutdown, สนับสนุนไฟล์ขนาดใหญ่, Event MPM และจัดองค์ประกอบในการ Authentication/Authorization ใหม่

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 2.2 หน้าเว็บไซต์ของ Apache

2.3 ไฟร์วอลล์ (Firewall)

ไฟร์วอลล์ คือ อุปกรณ์ต่างๆ ซึ่งใช้ป้องกันข้อมูลสารสนเทศที่มีรูปแบบเฉพาะที่ได้กำหนดไว้ จากเครือข่ายภายนอกซึ่งไม่น่าเชื่อถือ มายังเครือข่ายภายในของเรา ไฟร์วอลล์เป็นส่วนหนึ่งของเครือข่ายซึ่งคอยควบคุมการผ่านของแพ็คเก็ตต่างๆ ข้ามขอบเขตความปลอดภัยในเครือข่าย โดยมีพื้นฐานจากกลุ่มของกฎหรือนโยบายเพื่อความปลอดภัย(policy)ที่ได้ระบุไว้ กลุ่มของกฎของไฟร์วอลล์เป็นลิสต์ลำดับของการกรองกฎต่างๆ ซึ่งกำหนดการกระทำที่จะทำการกับแพ็คเก็ตต่างๆ ที่แม็ทช์กัน

2.3.1 ลักษณะของไฟร์วอลล์

ไฟร์วอลล์มีอยู่หลายลักษณะดังนี้

- Packet filtering firewalls (เร้าเตอร์)โดยจะมองทุกๆ เฮดเดอร์ของแพ็คเก็ตและเลือกกรองแพ็คเก็ตโดยดูจาก ที่อยู่, ลักษณะของแพ็คเก็ต, พอร์ตที่ต้องการและ ส่วนประกอบอื่นๆ โดยส่วนมากจะถูกสร้างโดยมีพื้นฐานจาก IP ต้นทางและที่อยู่ปลายทาง, ทิศทาง(เข้าหรือออกจากเครือข่าย), TCP หรือ UDP ต้นทางและ พอร์ตปลายทางร้องขอ

- Application-level firewall หรือ proxy server ส่วนใหญ่จะถูกใช้งานแยกจากตัวกรองของเร้าเตอร์ มักจะมีการปรับแต่งที่ตัวพร็อกซี่เซิร์ฟเวอร์ให้ติดต่อกับโลกภายนอกมากกว่าตัวเซิร์ฟเวอร์โดยตรง และยังสามารถนำตัวกรองของเร้าเตอร์มาใช้งานร่วมกันได้ โดยติดตั้งเอาไว้หลังพร็อกซี่เซิร์ฟเวอร์ ซึ่งข้อด้อยของไฟร์วอลล์ประเภทนี้คือไฟร์วอลล์จะถูกออกแบบมาสำหรับ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น ไม่อนุญาตให้นำไปใช้

โปรโตคอลบางตัวโดยเฉพาะและไม่สามารถปรับแต่งได้ง่ายๆ ในการป้องกันการโจมตีบนโปรโตคอลที่ไม่ได้ถูกออกแบบไว้

- Stateful inspection firewalls โดยจะมีการติดตามสถานะของการเชื่อมต่อระหว่างระบบภายในและภายนอกโดยใช้ตารางสถานะ (state table) ซึ่งจะเก็บบันทึกสถานะของการติดต่อของแต่ละแพ็คเก็ตเอาไว้ ถ้าไฟร์วอลล์ได้รับแพ็คเก็ตซึ่งไม่แม็ทช์กันกับในตารางสถานะ ก็จะส่งไปยังกลุ่มของกฎที่ได้ตั้งเอาไว้เพื่อกำหนดว่าจะยอมให้แพ็คเก็ตนั้นผ่านไปหรือไม่ ข้อด้อยของไฟร์วอลล์ประเภทนี้คือกระบวนการที่เพิ่มขึ้นมาเพื่อใช้ในการตรวจสอบแพ็คเก็ตบนตารางสถานะอาจทำให้ระบบถูกโจมตีการให้บริการได้ (DoS Attack)

- Dynamic filtering firewalls ไฟร์วอลล์แบบแรกและแบบที่ 3 จะมีลักษณะเป็นแบบ Static filtering firewalls คือจะอนุญาตให้กลุ่มของแพ็คเก็ตทั้งหมดชนิดหนึ่ง เข้าสู่ระบบตามการร้องขอ แต่ Dynamic filtering firewalls จะอนุญาตเพียงแค่แพ็คเก็ตเฉพาะกับต้นทาง, ปลายทางเฉพาะและที่อยู่พอร์ตเท่านั้นที่จะผ่านไฟร์วอลล์มาได้ ซึ่งจะต้องทำความเข้าใจการทำงานของโปรโตคอลและ การเปิดและการปิด "ประตู" ของไฟร์วอลล์โดยดูจากข้อมูลที่บรรจุอยู่ในเฮดเดอร์ของแพ็คเก็ต ซึ่งการกระทำของ Dynamic filtering firewalls นี้จะมีรูปแบบกึ่งกลางระหว่าง Static filtering firewalls กับ application proxies

- Kernel proxy จะมีรูปแบบพิเศษซึ่งจะทำงานอยู่ภายในเคอร์เนลของ Windows NT โดยจะคำนวณแพ็คเก็ตเป็นหลายๆชั้นโดยตรวจสอบความปลอดภัยในตัวข้อมูลของเคอร์เนล

2.3.2 องค์ประกอบของไฟร์วอลล์

ไฟร์วอลล์มีองค์ประกอบหลักๆ คือ

- นโยบายของเครือข่าย (network policy) แบ่งออกเป็น 2 ระดับซึ่งมีผลต่อการออกแบบติดตั้งและใช้งานไฟร์วอลล์ นโยบายระดับสูงจะกำหนดว่าจะอนุญาตใช้บริการหรือปฏิเสธการใช้บริการจากเครือข่ายใดบ้าง และใช้บริการเหล่านี้อย่างไร และเงื่อนไขใดเป็นข้อยกเว้น ส่วนนโยบายระดับต่ำจะอธิบายว่าไฟร์วอลล์ในตอนนี้จำกัดการเข้าถึงของบริการซึ่งถูกกำหนดไว้ในนโยบายระดับสูงกว่าอย่างไร

- กลไกในการตรวจสอบตัวจริง ไฟร์วอลล์สามารถควบคุมได้จากการเข้าถึงระยะไกลจะต้องมีซอฟต์แวร์หรือฮาร์ดแวร์ในการตรวจสอบตัวจริงของผู้ใช้

- การกรองแพ็คเก็ต ส่วนใหญ่จะกรองแพ็คเก็ตโดยดูจากฟิลด์ต่างๆเหล่านี้คือ IP ต้นทาง, IP ปลายทาง, พอร์ต TCP /UDP ต้นทาง และ พอร์ต TCP/UDP ปลายทาง

- Application gateways หรือ proxy ใช้ในการรับคำร้องจากภายนอก ซึ่งอาจใช้งานร่วมกันกับการกรองแพ็คเก็ตของเร้าเตอร์เพื่อกรองการติดต่อของบริการประเภท TELNET และ FTP

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.3.3 การทำงานของไฟร์วอลล์

การทำงานของไฟร์วอลล์นั้นไฟร์วอลล์จะทำตามกลุ่มของกฎที่เราได้ตั้งไว้หรือที่เรียกว่า โพลิซี (policy) หรือ รูลลิสต์ (rule list) หรือแอคเซสคอนโทรลลิสต์ (ACL: access control list) กฎจะถูกเรียบเรียงฟิลด์ในการกรอง (หรือที่เรียกว่า network fields) เช่น ชนิดของโปรโตคอล, IP แอดเดรสต้นทาง, IP แอดเดรสปลายทาง, พอร์ตต้นทาง และ พอร์ตปลายทาง และฟิลด์ที่ใช้กรอง แต่ละ network field สามารถเป็นค่าต่างๆ เพียงค่าเดียวหรือเป็นช่วงของค่าต่างๆ ได้ การกรองจะมีการดำเนินการคือ ยอมรับ (accept)ให้แพ็คเก็ตที่ผ่านเข้ามาจากเครือข่ายภายนอก หรือ ปฏิเสธ (deny) ซึ่งจะทำให้แพ็คเก็ตนั้นถูกทิ้งไป แพ็คเก็ตที่ถูกยอมรับหรือถูกปฏิเสธโดยกฎที่ถูกกำหนดไว้ถ้าเฮดเดอร์ของแพ็คเก็ต มีข้อมูลแม็ทช์กับ network field ทั้งหมดของกฎนี้ มิฉะนั้นกฎในลำดับถัดไปก็จะถูกใช้ทดสอบการแม็ทช์กับแพ็คเก็ตนั้นอีกครั้ง ซึ่งกระบวนการเดียวกันนี้จะทำซ้ำไปเรื่อยๆ จนกระทั่งจะเจอกฎที่แม็ทช์กัน ซึ่งถ้าไม่ตรงกันกับกฎใดเลยจะต้องกำหนดการดำเนินการไว้ใน กลุ่มของกฎ ซึ่งมักจะตั้งค่าเริ่มต้นไว้เป็น “deny”

รูปแบบของกฎในการกรอง มักจะใช้เป็นทุกๆฟิลด์เฮดเดอร์ของ IP, UDP หรือ TCP ในส่วนการกรองของกฎ อย่างไรก็ตาม ประสบการณ์ตามความเป็นจริง แสดงให้เห็นว่าโดยส่วนใหญ่แล้วฟิลด์ที่ถูกใช้ในการแม็ทช์กันคือ ชนิดของโปรโตคอล, IP ต้นทาง, พอร์ตต้นทาง, IP ปลายทาง และพอร์ตปลายทาง ในบางฟิลด์ เช่น TTL และ TCP flag ต่างๆ เป็นเฉพาะโอกาสที่ถูกใช้เพื่อจุดประสงค์ที่ใช้ในการกรอง ตามรูปแบบปกติกฎที่ใช้ในการกรองของกลุ่มของกฎของไฟร์วอลล์เป็นดังนี้ :

<order> <protocol> <src_ip> <src_port> <dst_ip> <dst_port> <action>

โดยในส่วนที่อยู่ในกรอบคือ network field ที่ใช้ในการแม็ทช์ หรือที่เรียกว่า 5-tuple filter การกำหนดลำดับของกฎต้องดูตำแหน่งที่สัมพันธ์กับกฎอื่นๆที่ใช้กรองด้วย โปรโตคอลที่กำหนดเป็น transport protocol ของแพ็คเก็ตและมีค่าเป็นดังนี้คือ IP, ICMP, IGMP, TCP หรือ UDP ที่ src_ip และ dst_ip จะระบุ IP แอดเดรส ของต้นทางและปลายทางของแพคเก็ต IP แอดเดรสเป็นได้ทั้ง host address (เช่น 140.192.37.120) หรือ network address (เช่น 140.192.37.*) ฟิลด์ src_port และ dst_port จะกำหนดพอร์ตแอดเดรสของต้นทางและปลายทางของแพคเก็ต สามารถตั้งค่าเป็นพอร์ตเดี่ยวๆ หรือตั้งค่าเป็นทุกพอร์ต (any) ได้ เช่นตัวอย่าง กลุ่มของกฎต้องการ บล๊อกทุก TCP traffic ที่เข้ามาจากเครือข่าย 140.192.27.* ยกเว้น HTTP จะเป็นดังนี้ :

1: tcp, 140.192.37.*, any, *.*.*.*, 80, accept

2: tcp, 140.192.37.*, any, *.*.*.*, any; deny

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 2.1 กลุ่มของกฎของไฟร์วอลล์

order	protocol	src_ip	src_port	dst_ip	dst_port	action
1:	tcp,	140.192.37.20,	any,	*.*.*.*,	80,	deny
2:	tcp,	140.192.37.*,	any,	*.*.*.*,	80,	accept
3:	tcp,	*.*.*.*,	any,	140.192.37.40,	80,	accept
4:	tcp,	140.192.37.*,	any,	140.192.37.40,	80,	deny
5:	tcp,	140.192.37.30,	any,	*.*.*.*,	21,	deny
6:	tcp,	140.192.37.*,	any,	*.*.*.*,	21,	accept
7:	tcp,	140.192.37.*,	any,	140.192.37.40,	21,	accept
8:	tcp,	*.*.*.*,	any,	140.192.37.40,	21,	accept
9:	tcp,	*.*.*.*,	any,	*.*.*.*,	any,	deny
10:	udp,	140.192.37.*,	any,	*.*.*.*,	53,	accept
11:	udp,	*.*.*.*,	any,	140.192.37.*,	53,	accept
12:	udp,	*.*.*.*,	any,	*.*.*.*,	any,	deny

จากตัวอย่างด้านบนจะเห็นว่ากฎที่อยู่ในลำดับสุดท้าย จะเป็นการตั้งค่าให้แม็ทช์กันกับทุกแพ็คเก็ต เพื่อเป็นการบล็อกทุกแพ็คเก็ตที่ผ่านเข้ามาในไฟร์วอลล์เพื่อไม่ให้มีแพ็คเก็ตใดสามารถเล็ดลอดผ่านเข้าไปใน เครื่อข่ายภายในได้

2.3.4 ไอพีไฟร์วอลล์ (IPFirewall)

ไฟร์วอลล์เป็นอุปกรณ์ป้องกันเครือข่ายจากเครือข่ายภายนอกที่ไม่มีสิทธิที่จะเข้ามาในเครือข่ายและเครือข่ายที่ไม่มีการจัดการเรื่องความปลอดภัย เช่น ในอินเทอร์เน็ต ไฟร์วอลล์มีความสามารถในการให้บริการต่างๆ คือ

1. ป้องกันเครือข่ายจากโปรโตคอลและบริการที่ไม่ปลอดภัย

2. เก็บข้อมูลเกี่ยวกับผู้ใช้, ระบบ, ที่อยู่เครือข่าย และการทำงานของโปรแกรมต่างๆ บนเครือข่ายจากภายนอก

3. ให้บริการการตรวจสอบข้อมูลและที่มาผ่านล็อกไฟล์ ซึ่งไฟร์วอลล์ที่ดีอาจให้ผู้ดูแลสามารถปรับแต่งการเตือนภัยเมื่อตรวจพบแพ็คเก็ตที่ไม่ปลอดภัยได้

4. ให้บริการ จัดการความปลอดภัยของเครือข่ายจากภายนอก โดยทำหน้าที่เหมือนกับประตูเข้าออกสู่อินเทอร์เน็ต

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ไฟร์วอลล์ไม่สามารถป้องกันสิ่งเหล่านี้ได้

ไวรัส (ไฟร์วอลล์บางชนิดสามารถป้องกันไวรัสได้)

ม้าโทรจัน

การโจมตีทางวิศวกรรม

การโจมตีทางกายภาพของเครือข่าย

การไร้ความสามารถของผู้ดูแลระบบ

การโจมตีจากภายใน

2.3.5 การทำงานของไอพีไฟร์วอลล์บนฟรีบีเอสดี

โปรแกรมไอพีไฟร์วอลล์เป็นไฟร์วอลล์ประเภทกรองแพ็คเก็ต ซึ่งเป็นชุดของโปรแกรมหนึ่งที่มีมาพร้อมกับระบบปฏิบัติการ ฟรีบีเอสดี

การทำงานของไอพีไฟร์วอลล์ จะมีลักษณะ ทำตามลำดับของกฎที่ได้ตั้งเอาไว้ที่เรียกว่าโพลิซีหรือรูลลิสต์ โดยจะนำเอาค่าของเฮดเดอร์ในแพ็คเก็ตที่ผ่านเข้ามาในเครือข่ายมาพิจารณาเทียบกับ ค่าที่อยู่ในกฎ ซึ่งค่าที่ใช้เทียบมักจะอยู่ในฟิลด์ต่างๆ ที่สำคัญๆ เช่น ไอพีแอดเดรส, พอร์ตของทั้งต้นทางและปลายทาง, โปรโตคอลที่ใช้ และหมายเลข ICMP ถ้านำฟิลด์ต่างๆ เหล่านี้มาเทียบแล้วตรงกับกฎข้อใด ก็จะมีการตอบสนองว่าจะยอมให้แพ็คเก็ตนั้นๆ ผ่านเข้าไปในเครือข่ายหรือทำการทิ้งแพ็คเก็ตนั้นไป

ในการตั้งค่าคอนฟิกของไอพีไฟร์วอลล์ คือการสร้างรายการของกฎขึ้นโดยจะเริ่มตั้งแต่กฎ หมายเลข 1 ถึง หมายเลข 65535 และทำหน้าที่รับแพ็คเก็ตให้ผ่านเข้ามาโดยแพ็คเก็ตที่นำมาเทียบแล้วไม่ตรงกับกฎแบบเรียงตามลำดับ ก็จะถูกเลื่อน มาเทียบกับกฎลำดับถัดไป จนกระทั่งสามารถจับคู่กับกฎข้อใดข้อหนึ่งได้ แพ็คเก็ตนั้นก็จะถูกตอบสนองตามกฎที่ได้ตั้งไว้ ขึ้นอยู่กับการตั้งค่าของระบบ ว่าแพ็คเก็ตนั้นจะสามารถนำกลับมาใส่ลงในไฟร์วอลล์เพื่อเทียบกับกฎที่อยู่หลังจากกฎลำดับที่จับคู่กันได้แล้วเพื่อทำการเปรียบเทียบต่อไปจนครบกฎทุกข้อหรือไม่ โดยการตั้งค่าเริ่มต้นของกฎลำดับสุดท้าย (กฎหมายเลข 65535) จะไม่สามารถแก้ไขหรือลบทิ้งได้ และจะตรงกับทุกๆ แพ็คเก็ตที่มาถึง ซึ่งจะมีการกระทำคือ ให้ทิ้งแพ็คเก็ตนั้นๆ แต่สามารถแก้ไขการกระทำได้ว่าจะยอมรับหรือทิ้งแพ็คเก็ตนั้น ขึ้นอยู่กับการตั้งค่าของเคอร์เนล กฎทั้งหมดจะมีความสัมพันธ์กับตัวนับ 2 ตัว คือ ตัวนับแพ็คเก็ตและตัวนับไบต์ โดยที่ตัวนับเหล่านี้จะถูกเปลี่ยนแปลงเมื่อมีแพ็คเก็ตที่เข้ามาสามารถจับคู่กับกฎ การกำหนดกฎต่างๆ ของไอพีไฟร์วอลล์มีพื้นฐานดังต่อไปนี้

-การเพิ่มกฎ (addition)

-การลบกฎที่มีอยู่ (deletion)

-การลบกฎทั้งหมด (flush)

-แสดงรายละเอียดของกฎทั้งหมด (show/list)

-ปรับค่าตัวนับต่างๆ (zero/resetlog)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ถ้ามีกฎข้อใดมีการตั้งค่าให้เป็น keep-state หรือ limit ไอพีไฟร์วอลล์จะมีการทำงานเป็นแบบ stateful โดยกฎนั้นจะมีช่วงเวลาจำกัดและจะถูกตรวจสอบสถานะ มักจะใช้งานกับการจราจรที่มีการขึ้นทะเบียนไว้ ทุกๆ กฎ จะมีตัวนับ ทั้งตัวนับแพ็คเก็ต, ตัวนับไบต์, ตัวนับล็อก ซึ่งสามารถแสดงหรือลบค่าทิ้งได้จากคำสั่งในไอพีไฟร์วอลล์

กฎสามารถเพิ่ม, ลบ ได้ทั้งทีละกฎหรือเป็นกลุ่ม โดยใช้คำสั่ง add, delete หรือ flush และสามารถแสดงได้โดยใช้คำสั่ง show และ list และสามารถตั้งค่าตัวนับให้เป็นศูนย์ได้โดยใช้คำสั่ง zero และ resetlog และยังมีการเพิ่มตัวเลือกต่อท้ายในคำสั่ง เพื่อให้มีการทำงานเฉพาะเจาะจงมากขึ้น เพื่อให้ตั้งค่าคอนฟิกได้ง่ายขึ้นสามารถเขียนกฎต่างๆ ลงในไฟล์ได้

คำสั่งในไอพีไฟร์วอลล์ ที่ใช้ในการจัดการกลุ่มของกฎ ได้แก่

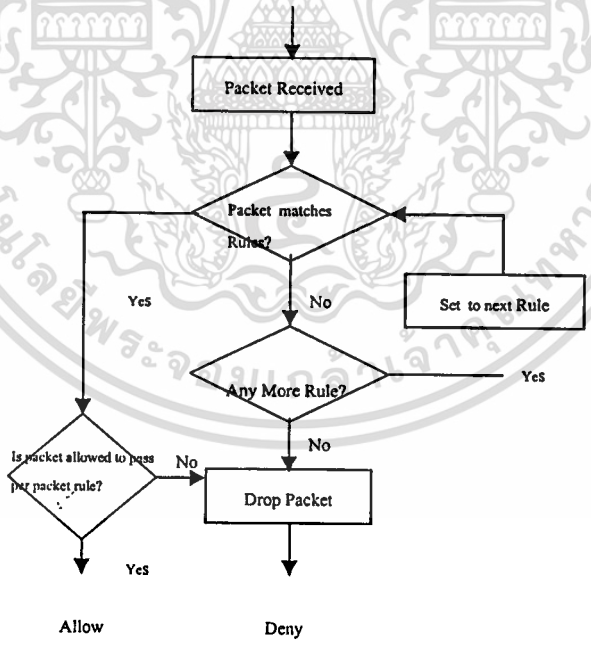
IP_FW_ADD แทรกกฎลงในกลุ่มของกฎ

IP_FW_DEL ลบกฎทั้งหมดที่ตรงกับหมายเลขที่ใส่

IP_FW_GET ย้อนกลับไปยังกฎแรกที่ตรงกับหมายเลขนั้น

IP_FW_ZERO ลบสถิติที่สัมพันธ์กับกฎทั้งหมดที่ตรงกับหมายเลขของกฎนั้น ถ้าใส่เลขเป็นศูนย์ จะลบสถิติทั้งหมด

IP_FW_FLUSH ลบกฎทั้งหมด ยกเว้นกฎข้อที่ 65535



รูปที่ 2.3 โฟลวของการกรองแพ็คเก็ตในระบบ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

โดยมีขั้นตอนคือ เริ่มจากการรับแพ็คเก็ตแล้วจึงตรวจสอบว่าแพ็คเก็ตนั้นตรงกับกฎหรือไม่ถ้าตรงกับกฎนั้นก็จะทำการตอบสนองตามกฎที่ตั้งไว้ว่าจะยอมรับหรือปฏิเสธแพ็คเก็ตตัวนั้นแล้วจึงจบการทำงาน แต่ถ้าแพ็คเก็ตไม่ตรงกับกฎนั้นก็จะตรวจสอบดูว่ามีกฎข้อถัดไปหรือไม่ถ้ามีก็จะวนซ้ำทำการตรวจสอบแพ็คเก็ตนี้ไปเรื่อยๆ ถ้าไม่มีกฎข้อใดเลยที่ตรงกับแพ็คเก็ตนี้ ก็จะทำการปฏิเสธแพ็คเก็ตไป

2.4 ภาษา PHP

PHP ย่อมาจากคำว่า "Personal Home Page Tool" เป็นการเขียนคำสั่งหรือโค้ดโปรแกรมที่เก็บและทำงานบนฝั่งเซิร์ฟเวอร์ (Server-Side Script) ซึ่งรูปแบบในการเขียนคำสั่งการทำงานนั้นจะมีลักษณะคล้ายกับภาษา Perl หรือภาษา C และสามารถที่จะใช้ร่วมกับภาษา HTML ได้อย่างมีประสิทธิภาพทำให้รูปแบบเว็บเพจของเรามีลูกเล่นมากขึ้น

เดิมทีนั้น PHP ได้ถูกคิดค้นขึ้นในปี ค.ศ. 1994 โดยนาย Rasmus Lerdorf ซึ่งถูกนำมาใช้ในการเก็บข้อมูลสถิติผู้เข้าชมเว็บของเขาเองเท่านั้น ต่อมา PHP เวอร์ชันแรกนั้นได้ถูกพัฒนาและเผยแพร่ให้กับผู้อื่นที่ต้องการศึกษามากขึ้น ซึ่งยังไม่มีความสามารถอะไรโดดเด่นมากมายจนกระทั่ง Rasmus ได้คิดค้นและพัฒนาให้ PHP มีความสามารถในการจัดการเกี่ยวกับฟอร์มข้อมูลที่ถูกสร้างมาจากภาษา HTML และสนับสนุนการติดต่อกับโปรแกรมจัดการระบบฐานข้อมูลได้ จึงทำให้ PHP เริ่มถูกใช้มาขึ้นอย่างรวดเร็วและเริ่มมีผู้สนับสนุนการใช้งาน PHP มากขึ้น

PHP สามารถทำงานเกี่ยวกับ Dynamic Web ได้ทุกรูปแบบไม่ว่าจะเป็นด้านการดูแลจัดการระบบฐานข้อมูล ระบบรักษาความปลอดภัยของเว็บเพจ การรับ-ส่ง Cookies เป็นต้น และยังสามารถที่จะติดต่อกับบริการต่างๆ ผ่านทางโปรโตคอล เช่น IMAP, SNMP, NNTP, POP3 HTTP และยังสามารถติดต่อกับ Socket ได้อีกด้วย

PHP ถูกเลือกใช้งานด้วยเหตุผลหลายประการคือ

- มีความรวดเร็วในการพัฒนาโปรแกรม เพราะ PHP เป็น สคริปต์แบบ Embeded คือสามารถแทรกร่วมกับภาษา HTML ได้อย่างอิสระและยังสามารถพัฒนาให้โค้ดอยู่ในรูป Class เพื่อให้นำมาใช้งานได้หลายครั้ง ทำให้สะดวกและรวดเร็วในการพัฒนาโปรแกรมต่างๆ

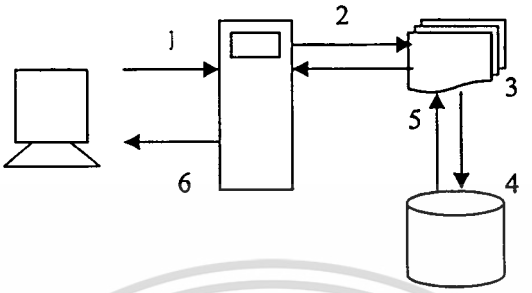
- PHP เป็นโอเพ่นซอร์ส หรือเป็นโค้ดแบบเปิดเผย เนื่องจาก PHP มีกลุ่มของผู้ใช้งานอยู่เป็นจำนวนมากทั่วโลกและมีเว็บไซต์อยู่เป็นจำนวนมากที่เป็นแหล่งรวบรวมซอร์สโค้ดโปรแกรมหรือบทความต่างๆ ให้ผู้ใช้มือใหม่สามารถหาและนำมาศึกษาได้ง่ายและไม่เสียค่าใช้จ่ายใดๆ

- PHP มีการบริหารหน่วยความจำในการใช้งานโดยไม่จำเป็นต้องเรียกใช้หน่วยความจำตลอดเวลาทำให้เซิร์ฟเวอร์ไม่ต้องมีทรัพยากรให้มากนัก

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- PHP สามารถนำมาใช้งานได้กับระบบปฏิบัติการหลายๆ ระบบรวมทั้ง Unix, Linux หรือ Windows เป็นต้น

เว็บ PHP จะมีการทำงานเป็นขั้นตอนต่างๆ ดังนี้



รูปที่ 2.4 การทำงานของเว็บ PHP

1. ฝั่งไคลเอ็นท์ ทำการร้องขอหรือเรียกใช้งานไฟล์ PHP ที่เก็บในเครื่องเซิร์ฟเวอร์
2. ฝั่งเซิร์ฟเวอร์จะทำการค้นหาไฟล์ PHP ตัวที่ถูกร้องขอแล้วทำการประมวลผลไฟล์ PHP ตามที่ไคลเอ็นท์ทำการร้องขอมา
3. ทำการประมวลผลไฟล์ PHP
4. เป็นการติดต่อกับข้อมูล (อาจเป็นแฟ้มข้อมูลหรือฐานข้อมูลก็ได้) และนำข้อมูลมาใช้ร่วมกับการประมวลผล
5. ส่งผลลัพธ์จากการประมวลผลไปให้เครื่องไคลเอ็นท์

2.5 การใช้งาน IPFW

IPFW จะมีกลุ่มของกฎตัวอย่างมาให้ (ในแฟ้ม /etc/rc.firewall) FreeBSD ในการติดตั้งมาตรฐานซึ่งจะเป็นกฎพื้นฐานง่ายๆ และไม่เหมาะจะนำมาใช้โดยตรงโดยไม่ได้มีการปรับแต่ง

2.5.1 เปิดการใช้งาน IPFW

IPFW จะมีการติดตั้งมาพร้อมกันกับระบบปฏิบัติการ FreeBSD โดยระบบจะโหลดการใช้งานอัตโนมัติเมื่อมีการตั้งค่าในไฟล์ rc.conf ส่วนที่ firewall_enable="YES" ซึ่งจะไม่ต้องทำการคอมไพล์ IPFW ลงในเคอร์เนลใหม่จนกว่าจะมีการใช้ NAT function

หลังจากตั้งค่า firewall_enable="YES" ใน rc.conf แล้วจะปรากฏข้อความขึ้นหลังจากการบูทดังนี้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ipfw2 initialized, divert disabled, rule-based forwarding disabled, default to deny, logging disabled

ถ้าต้องการให้มีการสร้าง Log สามารถกำหนดใช้และจำกัดได้ใน /etc/sysctl.conf โดยเพิ่มข้อความดังนี้ลงในแฟ้ม rc.conf และจะสามารถสร้าง Log ได้หลังจากการรีบูทแล้ว

net.inet.ip.fw.verbose=1

net.inet.ip.fw.verbose_limit=5

2.5.2 Kernel Options ตัวเลือกของเคอร์เนล

เมื่อต้องการเปิดการใช้งาน IPFWให้เพิ่มตัวเลือกคือ

options IPFIREWALL เปิดการใช้งาน IPFW เป็นส่วนหนึ่งของเคอร์เนล

options IPFIREWALL_VERBOSE เปิดการใช้งาน Log

options IPFIREWALL_VERBOSE_LIMIT=5 จำกัดจำนวนในการสร้าง Log เป็น 5

options IPFIREWALL_DEFAULT_TO_ACCEPT เปิดให้ตั้งค่าเริ่มต้นให้ยอมรับแพ็คเก็ตทั้งหมด ถ้าไม่ได้ตั้งค่านี้ไว้ ระบบจะตั้งค่าให้ทำการปฏิเสธแพ็คเก็ตทั้งหมด

options IPDIVERT เปิดเมื่อต้องการใช้ NAT

หลังจากทำการตั้งค่าตัวเลือกนี้แล้วจะต้องทำการคอมไพล์เคอร์เนลใหม่อีกครั้งจึงจะใช้งานได้

2.5.3 /etc/rc.conf Options ตัวเลือกใน /etc/rc.conf

ถ้าไม่ได้คอมไพล์ IPFW ไว้ในตัวเคอร์เนลให้ตั้งค่าใน /etc/rc.conf

firewall_enable="YES"

โดยเลือกชนิดของไฟร์วอลล์ที่ต้องการเปิดใช้ใน /etc/rc.firewall แล้วเติมข้อความดังนี้

firewall_type="open"

หรือโหลดกฎที่สร้างขึ้นจากแฟ้มข้อมูลดังนี้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

firewall_script="/etc/ipfw.rules"

เปิดการใช้ Log

firewall_logging="YES"

2.5.4 The IPFW Command คำสั่งในการใช้ IPFW

ipfw list แสดงรายการกฎทั้งหมด

ipfw -t list แสดงข้อมูลรายการกฎทั้งหมดที่มีการตรงกันกับแพ็คเก็ตจนถึงช่วงเวลาที่มีการ time stamp

ipfw -a list แสดงจำนวนครั้งที่กฎมีการตรงกันกับแพ็คเก็ต

ipfw -d list แสดงรายการกฎที่เป็น dynamic เพิ่มลงในกฎที่เป็น static

ipfw -d -e list แสดงรายการกฎแบบ dynamicที่ไม่ได้ใช้แล้ว

ipfw zero ตั้งค่าตัวนับเป็น 0

ipfw zero NUM ตั้งค่าตัวนับเป็น 0 ในกฎข้อที่ NUM

2.5.5 Rule Syntax

รูปแบบของกฎจะประกอบด้วยคีย์เวิร์ดดังนี้

CMD RULE_NUMBER ACTION LOGGING SELECTION STATEFUL

CMD

ใช้ระบุว่าต้องการจะให้ทำอะไรกับกฎนั้นเช่น ต้องการ add หรือ del

RULE_NUMBER

หมายเลขของแต่ละกฎ สามารถเลือกได้ตั้งแต่ 0 - 65535

ACTION

การกระทำของกฎ มีดังนี้คือ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

allow | accept | pass | permit

ยอมรับแพ็คเก็ต ซึ่งทั้งหมดนี้เมื่อมีการกระทำเสร็จสิ้นแล้วจะทำให้ออกไปจากส่วนของกระบวนการกรองกฎของไฟร์วอลล์

check-state

ตรวจดูแพ็คเก็ตทั้งหมดในตารางกฎ ว่าตรงกับกฎใด

deny | drop

ทั้ง 2 หมายถึงทำการทิ้งแพ็คเก็ตนั้น

Logging

log หรือ logamount เมื่อแพ็คเก็ตมีการจับคู่กับกฎแล้ว จะมีการบันทึกข้อความนั้นโดยเก็บไว้ใน syslogd โดยจำนวนของการ logamount จะกำหนดเอาไว้ใน sysctl โดยตัวแปร net.inet.ip.fw.verbose_limit

Selection

ใช้อธิบายคุณสมบัติของแพ็คเก็ตดังนี้

udp | tcp | icmp ชนิดของโปรโตคอล

from src to dst IP ต้นทางและปลายทาง

port number หมายเลขพอร์ต

in | out แพ็คเก็ตเข้าหรือออก

via IF อินเตอร์เฟสที่แพ็คเก็ตใช้ผ่าน

setup เริ่ม session เมื่อแพ็คเก็ตเป็น TCP

keep-state เก็บค่าในการจับคู่ระหว่างแพ็คเก็ตกับกฎ

limit {src-addr | src-port | dst-addr | dst-port}

จำกัดการเชื่อมต่อโดยจำไม่สามารถใช้ได้กับกฎที่มีการตั้งค่า keep-state ไว้แล้ว

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.6 การออกแบบโดยใช้ UML

UML (Unified Modeling Language) คือภาษามาตรฐานในการสร้างแบบจำลองที่ถูกออกแบบมาให้มีความยืดหยุ่นและสามารถปรับแต่งได้มาก เพื่อให้ผู้พัฒนาและผู้ใช้งานสามารถเข้าใจในกระบวนการของโครงงานที่ทำการออกแบบได้ตรงกัน โดย UML สามารถนำมาใช้ได้กับ กระบวนการทางธุรกิจ, ลำดับของการทำงาน, โปรแกรมประยุกต์, ฐานข้อมูลและอื่นๆ ซึ่งไม่จำเป็นต้องใช้กับแบบจำลองที่เป็น Object-Oriented (OO) เท่านั้น

UML ประกอบด้วยไดอะแกรมต่างๆ หลายๆไดอะแกรมเพื่อในขั้นตอนวิเคราะห์และออกแบบ โดยจะแบ่งออกหลักๆ เป็น Structure Diagram ที่ใช้อธิบายโครงสร้างของระบบและ Behavior Diagram ที่ใช้อธิบายพฤติกรรมของระบบ

Structure Diagram ได้แก่

- Class Diagrams
- Component Diagrams
- Object Diagrams
- Deployment Diagrams
- Composite Structure Diagrams
- Package Diagrams

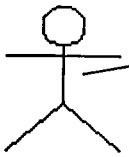
Behavior Diagrams ได้แก่

- Use Case Diagrams
- Activity Diagrams
- Statechart Diagrams
- Collaboration Diagrams
- Sequence Diagrams
- Timing Diagrams
- Interaction Diagrams

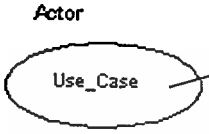
ซึ่งในโครงงานนี้นำไดอะแกรมมาใช้คือ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Use Case Diagrams เป็นไดอะแกรมที่ใช้บอกว่าในระบบมี requirement ที่เป็น functional requirement อะไรบ้างในรูปแบบของ use cases รวมทั้งสิ่งแวดล้อมอื่นๆ ของระบบ (actor)โดยจะไม่ได้อธิบายว่าในแต่ละขั้นตอนนั้นต้องทำอย่างไร Use Case Diagrams จะมีการใช้สัญลักษณ์ต่างๆ ดังนี้คือ



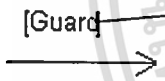
actor ใช้แทนสิ่งใดๆ ที่เข้ามามีการติดต่อกับระบบโดยอาจจะเป็นคนหรือระบบอื่นๆก็ได้



use case ใช้แทน ไดอะล็อกระหว่าง actor กับระบบโดยจะถูกเริ่มและเรียกใช้โดย actor ซึ่งจะคืนค่าผลลัพธ์กลับมาเพื่อเป้าหมายอย่างใดอย่างหนึ่ง ในหนึ่ง use case อาจมีเหตุการณ์เกิดขึ้นได้หลายเหตุการณ์ก็ได้

Activity Diagrams เป็นไดอะแกรมที่ใช้อธิบายการทำงานของระบบว่ามีกิจกรรมอย่างไร โดยมากจะใช้เพื่อขยายความ use case ที่บอกเพียงแค่ไดอะล็อกเท่านั้น ซึ่งอาจจะนำอัลกอริทึมมาเขียนก็ได้ถ้าต้องการความละเอียดมากขึ้น Activity Diagrams มีการใช้สัญลักษณ์ต่างๆ ดังนี้คือ

Activity box ใช้แทนงานหรือวิธีการที่จำเป็นต้องทำโดยคนหรือคอมพิวเตอร์โดยมีเส้นเชื่อมเป็นตัวกระตุ้นการทำงาน



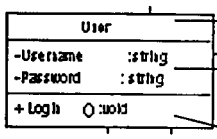
Guard เป็นตัวกำหนดเงื่อนไขว่าจะทำการใช้เส้นทางใดในการกระตุ้นการทำงานต่อไป

Decision activity ใช้แทนเงื่อนไขที่เกิดการวนซ้ำขึ้น

Synchronization bars ใช้แทนการเริ่มและการรวมการทำงานแบบขนานที่เกิดขึ้นในกิจกรรมนั้น

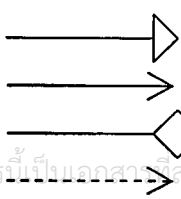
Class Diagrams เป็นไดอะแกรมที่ใช้แสดงกลุ่มของ class, interface และ collaboration และ relationship ที่เกิดขึ้นในระบบ ซึ่งจะประกอบด้วยคอมโพเน็นท์ หลักๆ คือ

Class เป็นตัวอธิบายรายละเอียดสำหรับกลุ่มของออบเจ็กต์ที่มีโครงสร้างและพฤติกรรมและความสัมพันธ์เหมือนๆ กันโดยประกอบด้วยส่วนต่างๆ คือ



- Class name ชื่อของ class โดยจะต้องไม่ซ้ำกัน
- Attribute ค่าใดๆ ที่ class นั้นอ้างถึง
- Operation พฤติกรรมของออบเจ็กต์

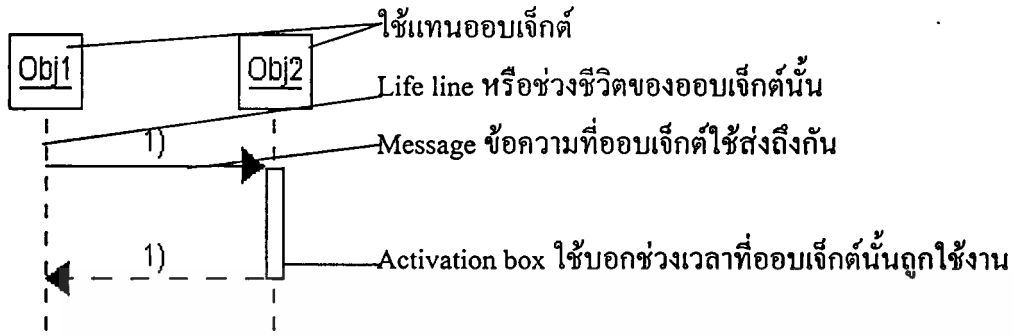
Relationships ลักษณะความสัมพันธ์ระหว่าง class ซึ่งแบ่งออกเป็น



- Generalization ความสัมพันธ์แบบ “is-a-kind-of”
- Association ความสัมพันธ์ว่ามีการติดต่อด้วย
- Aggregation ความสัมพันธ์แบบเป็นส่วนใดส่วนหนึ่ง
- Dependency ความสัมพันธ์แบบมีผลต่อกัน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Sequence Diagrams เป็นไดอะแกรมรูปแบบ Interaction แบบหนึ่งซึ่งใช้แสดงว่าออบเจ็กต์มีการติดต่อ (Interact) กับออบเจ็กต์อื่นๆ อย่างไรโดยจะเน้นที่ลำดับในการส่งข้อความระหว่างกัน Sequence Diagrams มีสัญลักษณ์ดังนี้คือ



2.7 การสร้างแบบจำลองกลุ่มของกฎของไฟร์วอลล์ของ Ehab S. Al-Shaer

สิ่งจำเป็นพื้นฐานในการจัดการกลุ่มของกฎของไฟร์วอลล์ อย่างแรกคือการจำลองความสัมพันธ์และการแสดงตัวอย่างของกฎของไฟร์วอลล์ในกลุ่มของกฎ เมื่อแบบจำลองนี้สมบูรณ์ และมีประสิทธิภาพ ความสัมพันธ์ของกฎในแบบจำลองนี้จะจำเป็นในการวิเคราะห์ กลุ่มของกฎของไฟร์วอลล์ และออกแบบเทคนิคที่ใช้ในการจัดการ เช่น การตรวจหาความผิดปกติ และการปรับแต่งกฎ การสร้างแบบจำลองในการแสดงตัวอย่างกฎหรือกลุ่มของกฎเป็นสิ่งสำคัญสำหรับการนำไปใช้ในเทคนิคการจัดการและทำให้เห็นโครงสร้างของกลุ่มของกฎของไฟร์วอลล์

การจัดรูปแบบความสัมพันธ์ของกฎของไฟร์วอลล์เพื่อให้สามารถสร้างแบบจำลองที่ใช้ประโยชน์สำหรับกฎที่ใช้ในการกรองได้ เราจำเป็นต้องกำหนดความสัมพันธ์ ซึ่งอาจสัมพันธ์กับ 2 แพ็คเก็ตหรือมากกว่านั้น เราจะกำหนดความสัมพันธ์ที่เป็นไปได้ซึ่งอาจมีอยู่ระหว่างกฎที่ใช้ในการกรอง และพิสูจน์ได้ว่าไม่มีความสัมพันธ์อื่นๆ อยู่อีก โดยกำหนดความสัมพันธ์จากการเปรียบเทียบ network field ของกฎที่ใช้ในการกรองได้ดังนี้

นิยาม 1 : กฎ Rx และ Ry จะเท่าเทียมกันอย่างชัดเจน ถ้า ทุกๆ ฟิลด์ใน Rx เท่ากันกับทุกๆ ฟิลด์ที่ใช้กรองใน Ry :

Rx จะเท่าเทียมกันกับ Ry ถ้า

$\forall i : Rx[i] = Ry[i]$ เมื่อ $i \in$ {protocol, src_ip, src_port, dst_ip,dst_port}

ตัวอย่าง กฎที่ 1 และ กฎที่ 2 ด้านล่างนี้ เท่าเทียมกันทุกๆ ฟิลด์ที่ใช้ในการแม็ทช์ของทั้ง 2 กฎเท่ากัน

1 : tcp, 140.192.37.10, any, 163.122.51.*, 21, accept

2 : tcp, 140.192.37.10, any, 163.122.51.*, 21, deny

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

นิยาม 2 : กฎ Rx และ Ry จะแม็ทช์กันแบบครอบคลุมกัน ถ้ากฎนั้น ไม่ได้เท่าเทียมกัน และ ถ้าทุกฟิลด์ใน Rx เป็นสับเซตหรือเท่ากันกับฟิลด์ที่ใช้แม็ทช์กันใน Ry :

Rx แม็ทช์กันแบบครอบคลุมกันกับ Ry ถ้า

$\forall i : Rx[i] \subseteq Ry[i]$ และ $\exists j$ ซึ่ง Rx[j] != Ry[j]

เมื่อ $i, j \in$ {protocol, src_ip, src_port, dst_ip, dst_port}

ในความสัมพันธ์นี้ Rx ถูกเรียกว่า แม็ทช์กันแบบสับเซต ขณะที่ Ry ถูกเรียกว่าเป็น ซูเปอร์เซต ตัวอย่างเช่น กฎที่1 และกฎที่ 2 ด้านล่างเป็นการแม็ทช์กันแบบครอบคลุม เมื่อ กฎนั้นไม่ได้เท่าเทียมกันทุกประการ และทุกฟิลด์ในกฎที่ 1 เป็นสับเซตหรือเท่ากับฟิลด์ที่ใช้ในการแม็ทช์กันในกฎที่ 2 กฎ ข้อที่ 1 เป็น การแม็ทช์กันแบบสับเซต ขณะที่กฎที่ 2 เป็นการแม็ทช์กันแบบซูเปอร์เซต

1 : tcp, 140.192.37.10, any, 163.122.51.*, 80, accept

2 : tcp, 140.192.37.*, any, 163.122.51.*, any, deny

นิยาม 3 : กฎ Rx และ Ry จะเป็นอิสระต่อกัน ถ้า ทุกฟิลด์ใน Rx ไม่ได้เป็นสับเซตและซูเปอร์เซตและไม่เท่ากันกับฟิลด์ที่ใช้ในการแม็ทช์กันใน Ry :

Rx และ Ry จะเป็นอิสระต่อกัน ถ้า

$\forall i : Rx[i] \bowtie Ry[i]$ เมื่อ $\bowtie \in \{ \subset , \supset , = \}$, i {protocol, src_ip, src_port, dst_ip, dst_port}

ตัวอย่าง กฎที่ 1 และ กฎที่ 2 ด้านล่างจะเป็นอิสระต่อกัน เมื่อฟิลด์ที่ใช้ในการแม็ทช์กันทั้งหมดของทั้ง 2 กฎแตกต่าง

1 : tcp, 140.192.37.10, 2000, 163.122.51.50, 80, accept

2 : udp, 140.192.37.20, 3000, 163.122.51.60, 21, accept

นิยาม 4 : กฎ Rx และ Ry จะเป็นอิสระต่อกันบางส่วน (หรือแม็ทช์กันบางส่วน) ถ้า มีอย่างน้อย 1 ฟิลด์ใน Rx ซึ่งไม่ได้เป็นสับเซตและไม่ได้เป็นซูเปอร์เซตและไม่เท่ากันกับฟิลด์ที่ใช้แม็ทช์กันใน Ry :

Rx จะเป็นอิสระต่อกันบางส่วน (แม็ทช์กันบางส่วน) ถ้า

$\exists$ i , j ซึ่ง $Rx[i] \bowtie Ry[i]$ และ $Rx[j] \not\bowtie Ry[j]$

เมื่อ $\bowtie \in \{ \subset , \supset , = \}$ และ $i, j \in$ {protocol, src_ip, src_port, dst_ip, dst_port}

ตัวอย่าง กฎที่ 1 และกฎที่ 2 ด้านล่างนี้ จะเป็นอิสระต่อกันบางส่วน (หรือแม็ทช์กันบางส่วน) เมื่อทุกฟิลด์ในกฎที่ 1 สัมพันธ์กันกับฟิลด์ที่ใช้ในการแม็ทช์กันในกฎที่ 2 ยกเว้นฟิลด์ พอร์ตปลายทาง

1 : tcp, 140.192.37.10, any, *.*.*.*, 80, accept

2 : tcp, 140.192.37.*, any, *.*.*.*, 21, deny

นิยาม 5 : กฎ Rx และ Ry จะ เทียบเคียงกัน ถ้าบางฟิลด์ใน Rx เป็นสับเซตหรือเท่ากับฟิลด์ที่ใช้ในการแม็ทช์กันใน Ry และ ส่วนที่เหลือของฟิลด์ใน Rx เป็นซูเปอร์เซตของฟิลด์ที่ใช้ในการแม็ทช์กันของ Ry :

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Rx และ Ry จะเทียบเคียงกัน ถ้า

$\forall$ i : Rx[i] $\bowtie$ Ry[i] และ

$\exists$ i,j ซึ่ง Rx[i] $\subset$ Ry[i] และ Rx[j] $\supset$ Ry[j]

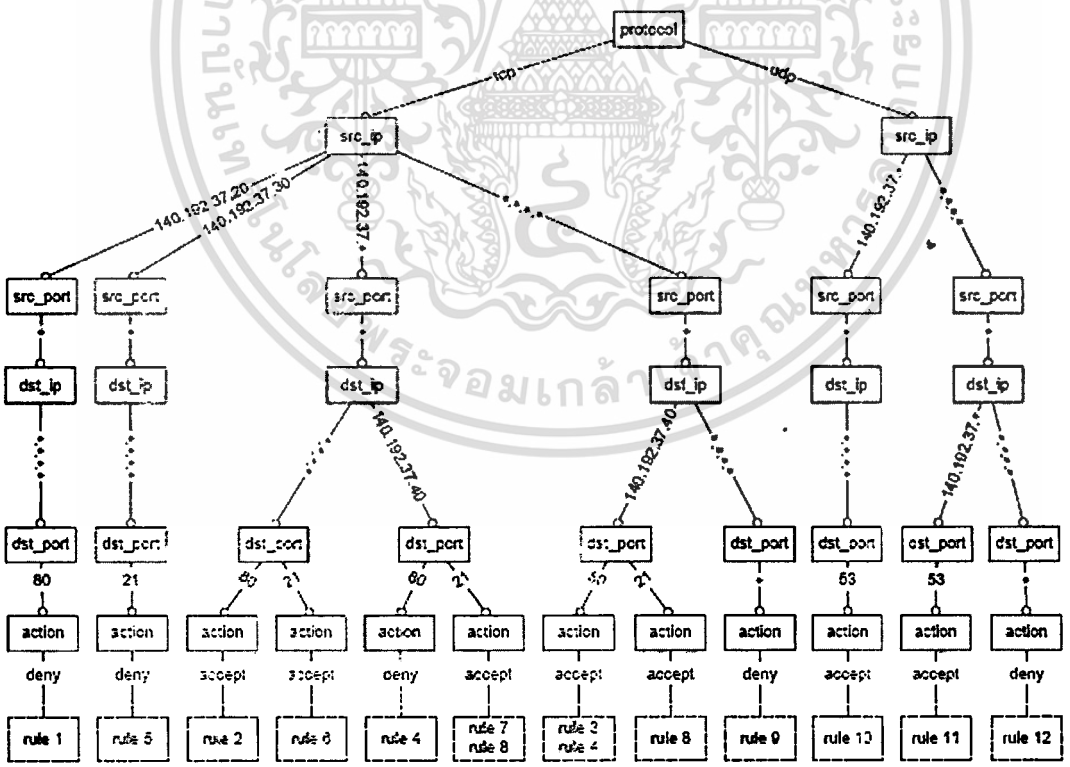
เมื่อ $\bowtie \in \{\subset, \supset, =\}$ และ i,j $\in$ {protocol, src_ip, src_port, dst_ip, dst_port}

ตัวอย่าง กฎที่ 1 และกฎที่ 2 ด้านล่าง จะเทียบเคียงกัน เมื่อ กฎนั้นมี โปรโตคอล, พอร์ตต้นทางและปลายทาง และแอดเดรสต้นทาง ของกฎที่ 1 เป็นสับเซตของฟิลด์ที่ใช้ในการแม็ทช์ในกฎที่ 2 และแอดเดรสปลายทางของกฎที่ 1 เป็น ซูเปอร์เซตของกฎที่ 2

1 : tcp, 140.192.37.10, any, *.*.*.*, 80, accept

2 : tcp, *.*.*.*, any, 140.192.37.*, 80, deny

การแสดงกฎของไฟร์วอลล์ในที่นี้จะใช้แทนด้วยโครงสร้างแบบ single rooted tree โดยเรียกว่า โพลิซีทรี เป็นแบบจำลองที่ใช้แสดงเน็ตเวิร์คฟิลด์ต่างๆ ที่ใช้ในการกรองกฎและยังช่วยให้สามารถตรวจพบความผิดปกติที่เกิดขึ้นระหว่างกฎได้ง่ายขึ้น แต่ละโหนดในโพลิซีทรีจะใช้แสดงฟิลด์ต่างๆ ของกฎที่ใช้กรอง และแต่ละสาขาของโหนดจะแสดงค่าที่เป็นไปได้ของฟิลด์นั้นๆ ที่รูทโหนดจะใช้แสดงฟิลด์โปรโตคอลและที่ลีฟโหนดจะแสดงฟิลด์แอ็คชั่น



รูปที่ 2.5 โพลิซีทรีของไฟร์วอลล์จากตาราง 2.1

โดยจะนำแต่ละกฎมา insert ลงในโพลิซีทรี จากรูทโหนดและตรวจสอบว่าในสาขาของโหนดฟิลด์นั้นมีข้อมูลค่าใดตรงกันกับกฎนั้น ถ้ามีค่าที่ตรงกันกฎก็จะถูก insert ลงในสาขานั้น แต่

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ถ้าไม่มีค่าใดตรงกัน ก็จะทำการ สร้างสาขาใหม่ลงในฟิลด์นั้น โดยจะรวมถึงสาขาที่เป็น สับเซต หรือซูเปอร์เซตกันด้วย เพื่อรักษาความสัมพันธ์กันระหว่างกฎ

2.7.1 การตรวจหา anomaly ที่เกิดขึ้นจากกฎของไฟร์วอลล์

ลำดับในการกรองของกฎเป็นสิ่งที่มีความสำคัญมากในการกำหนดกฎของไฟร์วอลล์ เพราะกระบวนการในการกรองกฎ จะดำเนินการไปตามลำดับของกฎจนกระทั่งสามารถจับคู่กับแพ็คเก็ตนั้นๆ ได้ ซึ่งถ้าแต่ละกฎนั้นไม่มีความเกี่ยวข้องหรือเป็นอิสระต่อกัน ลำดับของกฎก็อาจจะไม่มีความสำคัญ อย่างไรก็ตามปกติแล้วกฎส่วนใหญ่มักจะมีความสัมพันธ์เกี่ยวเนื่องกัน ในบางกรณี เช่นถ้ากฎที่สัมพันธ์กันถูกวางไว้ผิดลำดับ บางกฎอาจจะถูกกันออกโดยกฎอื่นที่ให้ผลลัพธ์ต่างกัน และยังอาจเป็นไปได้ว่าจะมีเนื้อหาของกฎขัดแย้งหรือซ้ำซ้อนกันได้ ดังนั้นจึงมีการกำหนด anomaly ของไฟร์วอลล์เพื่อให้ทราบชนิดและความแตกต่างของความผิดปกติของกฎในไฟร์วอลล์ โดยแบ่งออกเป็น

(1) Shadow anomaly : คือ กฎที่ถูกบังโดยกฎใดกฎหนึ่งที่อยู่ก่อนหน้า ซึ่งกฎที่ถูกบังนั้นจะไม่ได้ถูกนำมาใช้งาน ซึ่งก็คือ ถ้ากฎที่ถูกบังนั้นถูกลบออกไปก็ไม่มีผลอะไรกับ กลุ่มของกฎ กฎ Rx จะถูกบังโดยกฎ Ry ถ้า Rx มีลำดับอยู่หลัง Ry และ Rx เป็นสับเซตของ Ry และ Rx มีการกระทำต่างจาก Ry

(2) Correlation Anomaly : 2 กฎที่สัมพันธ์กัน ถ้ากฎแรกในลำดับแม็ทช์กับบางแพ็คเก็ตซึ่งตรงกันกับกฎข้อที่ 2 และกฎข้อที่ 2 แม็ทช์กันกับบางแพ็คเก็ตซึ่งตรงกันกับกฎข้อแรก
กฎ Rx และกฎ Ry จะมี correlation anomaly ถ้า Rx และ Ry สัมพันธ์กันและการกระทำของ Rx และ Ry แตกต่างกัน

(3) Redundancy anomaly : กฎที่มีความซ้ำซ้อนกันที่ดำเนินการให้ผลแบบเดียวกันบนแพ็คเก็ตเดียวกันโดยกฎคนละตัวกัน ซึ่งถ้ากฎที่ซ้ำซ้อนกันถูกลบออกไป ก็ไม่เกิดผลอะไรกับกลุ่มของกฎ
กฎ Rx จะซ้ำซ้อนกันกับ กฎ Ry ถ้า Rx เป็นสับเซตของ Ry และ การกระทำของ Rx และ Ry เหมือนกัน ความซ้ำซ้อนเป็นข้อผิดพลาดที่ต้องนำมาพิจารณา กฎที่ซ้ำซ้อนอาจไม่ได้ช่วยอะไรในการกรองแพ็คเก็ต และมันก็ไปเพิ่มขนาดให้กับ ตารางกฎที่มี ซึ่งอาจทำให้ต้องใช้เวลาและทรัพยากรในการค้นหาเพิ่มขึ้นได้

(4) Generalization anomaly : กฎใดๆ จะเป็น generalization (ครอบคลุม) ของกฎอื่นๆ ได้ ถ้ากฎแรก แม็ทช์กันกับแพ็คเก็ตทั้งหมดซึ่งกฎข้อที่ 2 สามารถแม็ทช์กันได้เช่นกัน แต่กฎข้อที่ 2 ไม่สามารถแม็ทช์กันได้กับแพ็คเก็ตทั้งหมดที่แม็ทช์กันกับกฎข้อแรก
กฎ Rx จะเป็น generalization ของกฎ Ry ถ้า Rx อยู่ในลำดับหลังจาก Ry และ Rx เป็นซูเปอร์เซตของ Ry และ การกระทำของ Rx และ Ry แตกต่างกัน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.7.2 อัลกอริทึมในการตรวจหา anomaly

อัลกอริทึมที่ใช้ในการตรวจหา anomaly นี้จะมีลักษณะการทำงานแบบเดียวกับอัลกอริทึมที่ใช้ในการสร้าง โพลิซีทรี โดยจะเริ่มจากนำแต่ละกฎมา insert ลงในโพลิซีทรี เริ่มจากฟิลด์โปรโตคอล และถัดไปเรื่อยๆ จะถึงฟิลด์แอ็คชั่น ซึ่ง ถ้ายังไม่ใช่ฟิลด์แอ็คชั่นของกฎนั้นอัลกอริทึมจะทำการตรวจสอบอินพุทในฟิลด์นั้น ว่ามีค่าตรงกันหรือมีความสัมพันธ์กันตามนิยามของกฎกับค่าใดในแต่ละสาขาที่ถูกสร้างขึ้นแล้ว ในอินพุทโหนดนั้นบ้าง ถ้ามีค่าที่ตรงกันอัลกอริทึมจะทำการเรียกตัวเองวนซ้ำด้วยกฎเดิมในฟิลด์ถัดไป และทำการตรวจหา ค่าที่ตรงกันในอินพุทโหนดนั้นๆ ซึ่งถ้าค่าในฟิลด์นั้นไม่ตรงกันกับสาขาใดเลยก็จะทำการสร้างสาขาขึ้นใหม่ด้วยค่าในฟิลด์นั้นและทำการวนซ้ำจนครบถึงฟิลด์แอ็คชั่น แล้วจึงทำการกำหนดสถานะและรายงานว่าตรวจพบ anomaly หรือไม่ และเป็น anomaly ชนิดใด ตาม routine ที่ได้แสดงไว้ด้านล่าง ดังนี้

```
function DiscoverAnomaly(rule, field, node, anomaly_state)
  if field ≠ ACTION then
    value_found = FALSE
    for each branch in node.branch_list do
      if branch.value = rule.field.value then
        value_found = TRUE
        if anomaly_state = NOANOMALY then
          anomaly_state = REDUNDANT
        DiscoverAnomaly(rule, field.next, branch.node, anomaly_state)
      else
        if rule.field.value ⊂ branch.value then
          if anomaly_state = GENERALIZATION then
            DiscoverAnomaly(rule, field.next, branch.node, CORRELATION)
          else
            DiscoverAnomaly(rule, field.next, branch.node, SHADOWING)
        else if rule.field.value ⊃ branch.value then
          if anomaly_state = SHADOWING then
            DiscoverAnomaly(rule, field.next, branch.node CORRELATION)
          else
            DiscoverAnomaly(rule, field.next, branch.node GENERALIZATION),
        end if
      end if
    end for
    if value_found = FALSE then
      new_branch = new TreeBranch(rule, rule.field, rule.field.value);
      node.branch_list.add(new_branch);
      DiscoverAnomaly(rule, field.next, new_branch.node, NOANOMALY);
    end if
  else /* action field reached */
    call DecideAnomaly(rule, field, node, anomaly_state)
  end if
end function
```

รูปที่ 2.6 อัลกอริทึมสำหรับสร้างโพลิซีทรีและค้นหา anomaly

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
function DecideAnomaly(rule, field, node, anomaly)
  if node has branch_list then
    branch = node.branch_list.first()
    if anomaly = CORRELATION then
      if rule.action = branch.value then
        report rule rule.id is in correlation with rule branch.rule.id
    else if anomaly = GENERALIZATION and rule.action = branch.value then
      report rule rule.id is a generalization of rule branch.rule.id
    else if anomaly = GENERALIZATION and rule.action = branch.value then
      branch.rule.setAnomaly(REDUNDANCY)
      report rule branch.rule.id is redundant to rule rule.id
    else if rule.action = branch.value then
      anomaly = REDUNDANCY
      report rule rule.id is redundant to rule branch.rule.id
    else if rule.action = branch.value then
      anomaly = SHADOWING
      report rule rule.id is shadowed by rule branch.rule.id
    end if
  end if
  rule.setAnomaly(anomaly)
end function
```

รูปที่ 2.7 อัลกอริทึมสำหรับตัดสิน anomaly

อัลกอริทึมที่ใช้ในการวิเคราะห์ของ Ehab S. Al-Shaer นี้สามารถตรวจพบ anomaly ได้ครบทั้ง 4 ชนิด แต่ยังมีข้อจำกัดในการนำแต่ละฟิลด์ที่มีความสัมพันธ์กัน มาใช้เปรียบเทียบกันทีละคู่ ซึ่งทำให้กระบวนการง่ายขึ้นแต่อาจจะไม่ครอบคลุมถึงฟิลด์ของกฎอื่นๆ ที่อาจมีความเกี่ยวข้องกันกับฟิลด์ที่นำมาตรวจสอบนั้นอีก จึงอาจทำให้ผลลัพธ์ที่ได้ยังไม่สมบูรณ์ครบ 100% นัก และการนำกฎมาแบ่งออกเป็นแต่ละฟิลด์นั้นอาจทำให้มีความยืดหยุ่นในการใช้งานน้อยลงเพราะจะทำให้การใช้งานกฎอื่นๆ ที่มีการตั้งค่าฟิลด์ต่างๆ ในกฎแตกต่างกันมาก แต่ในอัลกอริทึมนี้มีข้อดีคือการทำให้สามารถนำมาอิมพลีเม้นท์ได้ง่ายและสามารถตรวจหา anomaly ได้ครบทุกรูปแบบ ซึ่งเหมาะแก่การนำไปศึกษาและพัฒนาต่อไป

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 3

การออกแบบระบบงาน

ในบทนี้จะกล่าวถึงขั้นตอนการทำงานของระบบและการออกแบบการทำงานของยูสเซอร์อินเตอร์เฟสของไอพีไฟร์วอลล์บนระบบปฏิบัติการฟรีบีเอสดี โดยจะแสดงในรูปแบบที่ใช้ภาษา UML เป็นเครื่องมือช่วยในการสร้างแบบจำลองของระบบ

3.1 Software Requirement Specification ของระบบ

3.1.1. บทนำ Introduction

ในปัจจุบันการใช้งานเครือข่ายเป็นที่แพร่หลายกับองค์กรและหน่วยงานต่างๆ มากมาย แต่การที่จะต้องดูแลความปลอดภัยของเครือข่าย อาจต้องใช้บุคลากรที่มีความเชี่ยวชาญในการใช้งานในระบบปฏิบัติการ และการใช้งานโปรแกรมไฟร์วอลล์ต่างๆ ซึ่งมีความยุ่งยากและเสียเวลาในการควบคุมและจัดการ จึงมีความต้องการที่จะให้โปรแกรมใช้งานได้ง่ายและรวดเร็วมากขึ้น โดยมีวัตถุประสงค์ให้ผู้ดูแลและจัดการเครือข่ายทุกคนมีความสะดวกสบายในการใช้งานมากขึ้น

3.1.2.รายละเอียดโดยรวมOverallDescription

การใช้งานโปรแกรมไอพีไฟร์วอลล์ ในระบบ ปกติแล้วจะมีความยุ่งยากและผู้ใช้จะต้องมีประสบการณ์ในการใช้งานพอสมควร จึงมีการพัฒนาและออกแบบขึ้นให้สามารถใช้งานได้ง่ายและเร็วขึ้น โปรแกรมไอพีไฟร์วอลล์เป็นโปรแกรมที่ติดตั้งมาพร้อมกับระบบปฏิบัติการฟรีบีเอสดี ซึ่งเป็นระบบปฏิบัติการที่นิยมแพร่หลายในการควบคุมเซิร์ฟเวอร์ของเครือข่ายโดยรูปแบบของโปรแกรมที่ต้องการพัฒนาจะใช้งานผ่านโปรแกรมเว็บบราวเซอร์ เพื่อให้มีความคุ้นเคยกับผู้ใช้และสามารถใช้งานได้ในหลายๆ แพล็ตฟอร์ม โดยการทำงานส่วนต่างๆ จะนำมาอธิบายในการออกแบบไดอะแกรมอีกครั้ง ซึ่งโปรแกรมอาจมีข้อจำกัดในการพัฒนาคือ การควบคุมการทำงานโปรแกรมไอพีไฟร์วอลล์ได้ครบทุกฟังก์ชั่นมีความซับซ้อนมาก, ผู้พัฒนายังขาดความรู้และประสบการณ์ในการใช้งานโปรแกรม, เครื่องมือที่ใช้พัฒนายังไม่มีความสะดวกสบายทำให้พัฒนาได้ล่าช้า

3.1.3. ความต้องการส่วนติดต่อภายนอก External Interface Requirements

- User interfaces ส่วนติดต่อกับผู้ใช้เป็นแบบ GUI โดยทำงานผ่านโปรแกรมเว็บบราวเซอร์
- Hardware interfaces ส่วนติดต่อกับฮาร์ดแวร์โดยใช้ระบบปฏิบัติการฟรีบีเอสดี
- Software interfaces ส่วนติดต่อกับซอฟต์แวร์โดยใช้โปรแกรมไอพีไฟร์วอลล์เป็นส่วนของการทำงานของโปรแกรม

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.1.4. ความต้องการของระบบหรือส่วนที่เป็น functional requirement System Features

- สามารถจัดการเกี่ยวกับการใช้งานทั่วไปได้ ได้แก่

การเพิ่มกฎใหม่

การลบกฎ ที่มีอยู่ออก

การแสดงรายการกฎที่ใช้ในปัจจุบัน

การปรับค่าตัวนับแพ็คเก็ตต่างๆ

- สามารถจัดการเกี่ยวกับการใช้งานขั้นสูงได้

การตรวจสอบการทำงานของจำนวนแพ็คเก็ตที่ผ่านเข้ามา

การวิเคราะห์กฎขั้นพื้นฐาน

การตั้งค่า NAT

การตั้งค่า DHCP

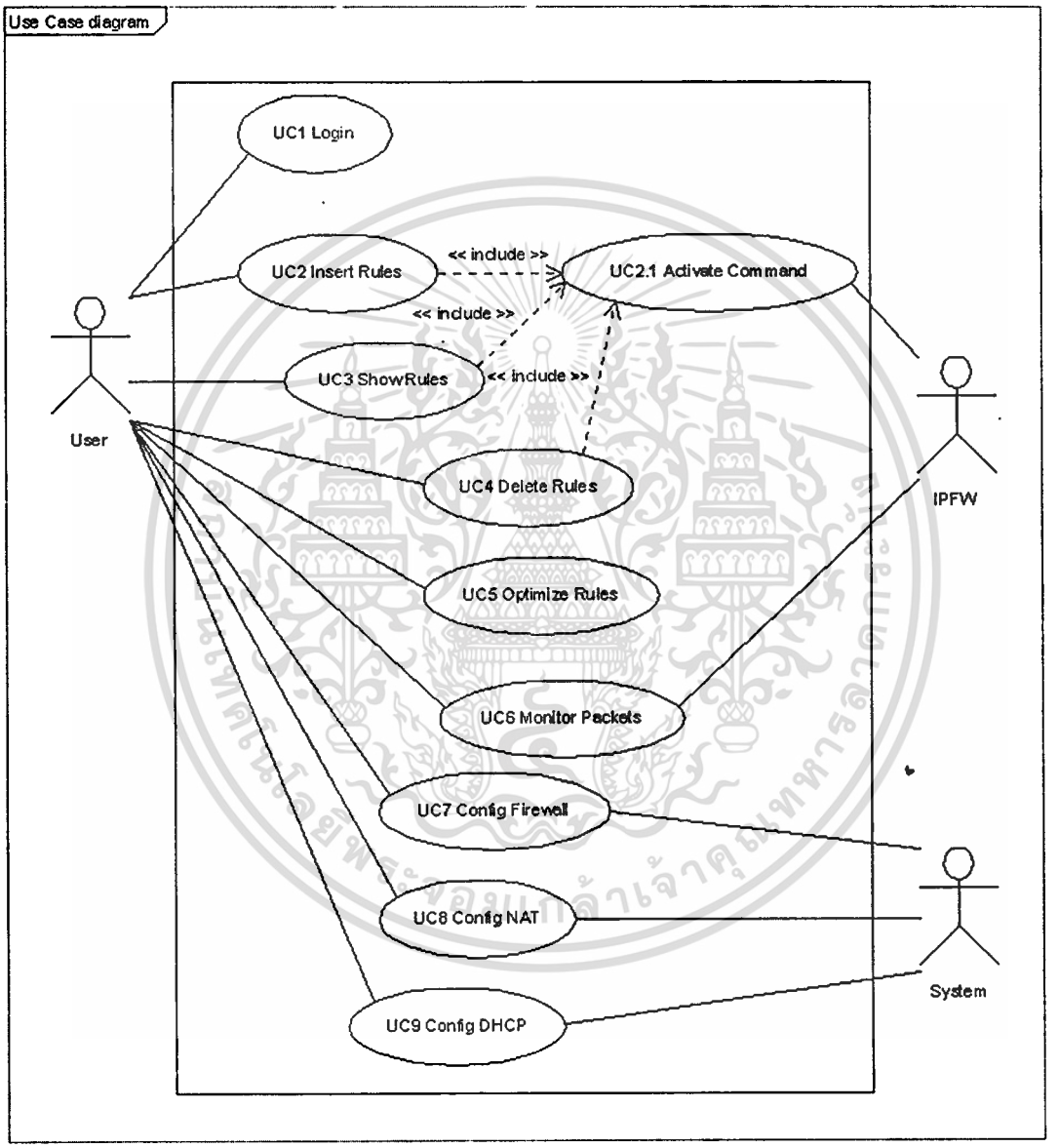
3.1.5. ความต้องการแบบ Nonfunctional อื่นๆ Other Nonfunctional Requirements

- Performance requirements ความต้องการทางด้านประสิทธิภาพ จะต้องใช้งานโปรแกรมได้อย่างถูกต้องและครบถ้วน โดยที่ยังไอพีไฟร์วอลล์ ยังสามารถทำงานได้เป็นปกติ
- Safety requirements การทำงานของส่วนต่างๆ จะต้องไม่สูญหาย หรือบกพร่อง
- Security requirements มีความปลอดภัยโดยผู้อื่นไม่สามารถแก้ไขการตั้งค่าโดยไม่ได้รับอนุญาตได้
- Software quality attributes สามารถดูแลจัดการและทดสอบการทำงานได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.2 ยูสเคสไดอะแกรมของระบบ

หัวข้อนี้จะแสดงในส่วนของแบบจำลอง เพื่อนำเสนอ กลุ่มของเหตุการณ์ที่เป็นไปได้ทั้งหมดที่เกิดขึ้นระหว่างผู้ใช้และระบบ ซึ่งแสดงเฉพาะในส่วนของ Functional Requirement ของระบบเท่านั้น อยู่ในรูปวงรีหรือเป็นยูสเคสดังนี้



รูปที่ 3.1 ยูสเคสไดอะแกรมของระบบ

ซึ่งในยูสเคสไดอะแกรมนี้มี Actor ที่เกี่ยวข้องอยู่ 3 Actor คือ User หมายถึงผู้ใช้งานระบบ, IPFW หมายถึงตัวโปรแกรมไอพีไฟร์วอลล์ และ System หมายถึงโปรแกรมของตัวระบบปฏิบัติการ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

คำอธิบายยูสเคส (Use-case Description) คือส่วนที่ใช้ในการอธิบายเหตุการณ์ที่เกิดขึ้นของแต่ละยูสเคสดังนี้

ตารางที่ 3.1 UC1 Login

Use-case ID :	UC1
Use-case Name :	Login
Brief Descriptions :	เป็น UC ที่อธิบายการตรวจสอบยืนยันตัวจริงของผู้ใช้งาน
Primary Actors :	User
Passive Actors :	-
Preconditions :	ผู้ใช้มี Username และ Password ในการเข้าใช้งาน
Basic Flows :	1. ผู้ใช้กรอก Username และ Password 2. ระบบตรวจสอบยืนยันผู้ใช้งานถูกต้อง 3. เริ่มการทำงานของโปรแกรม
Alternatives Flows:	2a. ระบบตรวจสอบยืนยันผู้ใช้งานไม่ถูกต้อง 2b. ระบบแสดงข้อความเตือน 2c. กลับไปทำข้อ 1. ใหม่อีกครั้ง
Postconditions :	ระบบสามารถทำการตรวจสอบผู้ใช้งานได้

ตารางที่ 3.2 UC2 Insert Rules

Use-case ID :	UC2
Use-case Name :	Insert Rules
Brief Descriptions :	เป็น UC ที่อธิบายการเพิ่มกฎของไอพีไฟร์วอลล์
Primary Actors :	User
Passive Actors :	-
Preconditions :	1. ระบบทำ UC1Login แล้ว
Basic Flows :	1. ผู้ใช้กรอกรายละเอียดกฎที่ต้องการเพิ่ม 2. ระบบตรวจสอบว่าผู้ใช้กรอกข้อมูลกฎนั้นครบถ้วน 3. ระบบตรวจสอบว่ากฎนั้นไม่ซ้ำกับกฎที่มีอยู่ 4. ระบบทำ UC2.1Activate Command
Alternatives Flows :	2a. ระบบตรวจสอบว่าข้อมูลที่กรอกไม่ครบถ้วน 2b. กลับไปข้อ 1. 3a. ระบบตรวจพบกฎที่ซ้ำกัน 3b. กลับไปข้อ 1.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 3.2 UC2 Insert Rules(ต่อ)

Postconditions :	ระบบสามารถทำการเพิ่มกฎได้

ตารางที่ 3.3 UC2.1 Activate Command

Use-case ID :	UC2.1
Use-case Name :	Activate Command
Brief Descriptions :	เป็น UC ที่อธิบายการสั่งให้ไอพีไฟร์วอลล์ทำงานตามคำสั่งที่ได้รับ
Primary Actors :	
Passive Actors :	IPFW
Preconditions :	-
Basic Flows :	1. ระบบทำการรับข้อมูลคำสั่ง 2. นำคำสั่งที่ได้ส่งให้ IPFW ทำงาน 3. แสดงผลลัพธ์ที่ได้อย่างถูกต้อง
Alternatives Flows:	3a. ผลลัพธ์ที่ได้ไม่ถูกต้อง 3b. แจ้งเตือนข้อผิดพลาดให้ผู้ใช้
Postconditions :	ระบบสามารถทำการแก้ไขกฎในโปรแกรมไอพีไฟร์วอลล์ได้อย่างถูกต้อง

ตารางที่ 3.4 UC3 Show Rules

Use-case ID :	UC3
Use-case Name :	Show Rules
Brief Descriptions :	ทำการแสดงกฎของไอพีไฟร์วอลล์ที่มีอยู่
Primary Actors :	User
Passive Actors :	-
Preconditions :	1. ระบบทำ UC1Login แล้ว
Basic Flows :	1. ผู้ใช้เลือกลักษณะการแสดงรายการกฎ 2. ระบบทำ UC2.1Activate Command
Alternatives Flows :	-
Postconditions :	ระบบสามารถแสดงผลได้อย่างถูกต้องและครบถ้วน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 3.5 UC4 Delete Rules

Use-case ID :	UC4
Use-case Name :	Delete Rules
Brief Descriptions :	เป็น UC ที่อธิบายการลบกฎของไอพีไฟร์วอลล์
Primary Actors :	User
Passive Actors :	
Preconditions :	1. ระบบทำ UC1Login แล้ว
Basic Flows :	1. ระบบแสดงกฎที่มีอยู่ 2. ผู้ใช้เลือกกฎที่ต้องการลบออก 3. ระบบทำ UC2.1Activate Command
Alternatives Flows :	-
Postconditions :	ระบบสามารถลบกฎที่เลือกได้อย่างถูกต้อง

ตารางที่ 3.6 UC5 Optimize Rules

Use-case ID :	UC5
Use-case Name :	Optimize Rules
Brief Descriptions :	เป็น UC ที่อธิบายการปรับแต่งกฎของไอพีไฟร์วอลล์
Primary Actors :	User
Passive Actors :	
Preconditions :	1. ระบบทำ UC1Login แล้ว
Basic Flows :	1. ระบบทำการตรวจสอบหา anomaly ที่เกิดขึ้น 2. ระบบแจ้งเตือน anomaly ที่จะทำการลบออก 3. ผู้ใช้ยืนยันการแก้ไขกฎ 4. ระบบเก็บหมายเลขกฎที่จะทำการลบออก 5. ระบบทำ UC4Delete Rules จนครบทุกกฎ
Alternatives :	3a. ผู้ใช้ไม่ตกลงในการลบกฎที่เกิด anomaly 3b. ระบบแจ้งเตือนผู้ใช้ให้รับทราบ
Postconditions :	ระบบสามารถทำการแก้ไขกฎของไอพีไฟร์วอลล์ได้อย่างเหมาะสม

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 3.7 UC6 Monitor Packets

Use-case ID :	UC6
Use-case Name :	Monitor Packets
Brief Descriptions :	เป็น UC ที่อธิบายเกี่ยวกับการผ่านเข้าออกและจับคู่กันระหว่างแพ็คเก็ตกับกฎของไอพีไฟร์วอลล์
Primary Actors :	User
Passive Actors :	IPFW
Preconditions :	2. ระบบทำ UC1Login แล้ว
Basic Flows :	1. ผู้ใช้เลือกการดูข้อมูลของแพ็คเก็ต 2. ระบบอ่านค่าจาก log file ที่เก็บข้อมูลการเข้าออกของแพ็คเก็ตไว้ 3. ระบบแสดงข้อมูลแพ็คเก็ตทั้งหมดที่มีการจับคู่กันกับกฎ
Alternatives Flows :	-
Postconditions :	ระบบสามารถแสดงข้อมูลการเข้าออกของแพ็คเก็ตจาก log file ได้อย่างถูกต้อง

ตารางที่ 3.8 UC7 Config Firewall

Use-case ID :	UC7
Use-case Name :	Config Firewall
Brief Descriptions :	เป็น UC ที่อธิบายเกี่ยวกับการตั้งค่า Firewall ในระบบปฏิบัติการฟรีบีเอสดี
Primary Actors :	User
Passive Actors :	FreeBSD Config file
Preconditions :	1. ระบบทำ UC1Login แล้ว
Basic Flows :	1. ระบบแสดง การตั้งค่าใช้งาน Firewall ในปัจจุบัน 2. ผู้ใช้ทำการแก้ไขตั้งค่าใหม่ 3. ระบบทำการบันทึกการแก้ไขของผู้ใช้ 4. ระบบทำการเปลี่ยนแปลงการตั้งค่าในระบบปฏิบัติการ
Alternatives :	-
Postconditions :	ระบบสามารถทำการแก้ไขการตั้งค่าใช้งาน Firewall ได้อย่างถูกต้อง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 3.9 UC8 Config NAT

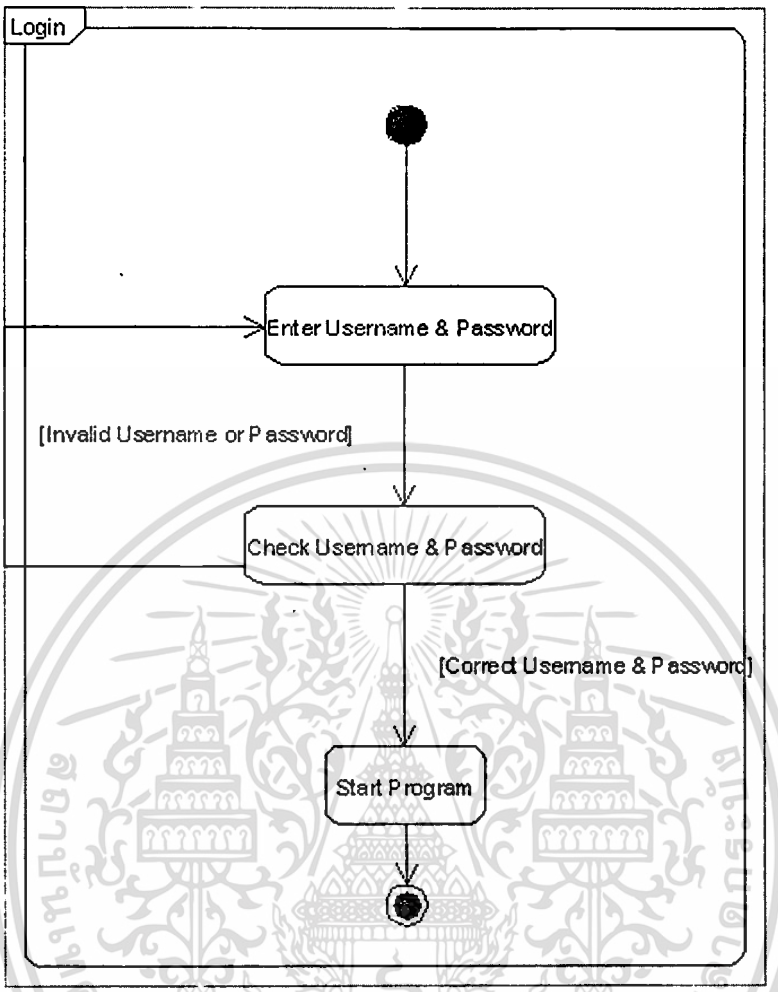
Use-case ID :	UC8
Use-case Name :	Config NAT
Brief Descriptions :	เป็น UC ที่อธิบายเกี่ยวกับการตั้งค่า NATในระบบปฏิบัติการฟรีบีเอสดี
Primary Actors :	User
Passive Actors :	FreeBSD Config file
Preconditions :	1. ระบบทำ UC1Login แล้ว
Basic Flows :	1. ระบบแสดง การตั้งค่าใช้งาน NATในปัจจุบัน 2. ผู้ใช้ทำการแก้ไขตั้งค่าใหม่ 3. ระบบทำการบันทึกการแก้ไขของผู้ใช้ 4. ระบบทำการเปลี่ยนแปลงการตั้งค่าในระบบปฏิบัติการ
Alternatives :	-
Postconditions :	ระบบสามารถทำการแก้ไขการตั้งค่าใช้งาน NAT ได้อย่างถูกต้อง

ตารางที่ 3.10 UC9 Config DHCP

Use-case ID :	UC9
Use-case Name :	Config DHCP
Brief Descriptions :	เป็น UCที่อธิบายเกี่ยวกับการตั้งค่าDHCPในระบบปฏิบัติการฟรีบีเอสดี
Primary Actors :	User
Passive Actors :	FreeBSD Config file
Preconditions :	1. ระบบทำ UC1Login แล้ว
Basic Flows :	1. ระบบแสดง การตั้งค่าใช้งาน DHCP ในปัจจุบัน 2. ผู้ใช้ทำการแก้ไขตั้งค่าใหม่ 3. ระบบทำการบันทึกการแก้ไขของผู้ใช้ 4. ระบบทำการเปลี่ยนแปลงการตั้งค่าในระบบปฏิบัติการ
Alternatives :	-
Postconditions :	ระบบสามารถทำการแก้ไขการตั้งค่าใช้งาน DHCP ได้อย่างถูกต้อง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.3 แอ็คทิวิตี ไดอะแกรมของระบบ

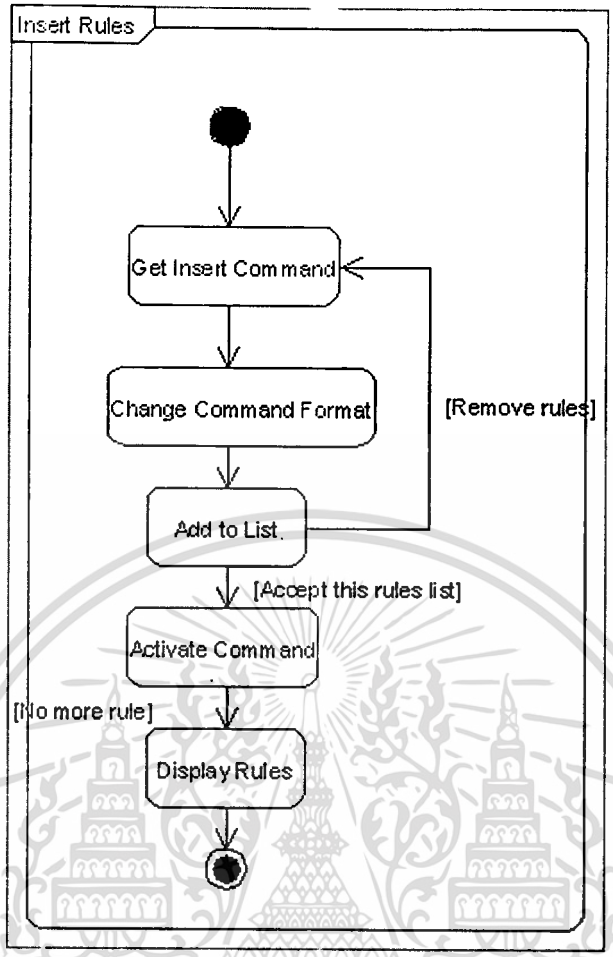


รูปที่ 3.2 แอ็คทิวิตีไดอะแกรมของการล็อกอิน

เป็นแอ็คทิวิตีไดอะแกรม สำหรับการอธิบายการล็อกอินเข้าสู่โปรแกรมโดยมีการทำงานดังนี้

1. ผู้ใช้ทำการกรอกข้อมูล Username และ Password ลงในหน้าจอล็อกอิน
2. ระบบทำการตรวจสอบข้อมูล Username และ Password ของผู้ใช้
   - ถ้าข้อมูล Username และ Password ถูกต้องตรงกับข้อมูลของผู้ใช้ที่สร้างไว้ ระบบจะยอมรับการเข้าใช้งานของผู้ใช้
   - ถ้าข้อมูล Username หรือ Password ไม่ถูกต้องระบบจุแสดงข้อความเตือน และกลับสู่หน้าจอล็อกอินอีกครั้ง
3. ระบบทำการเริ่มการทำงานของโปรแกรม

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

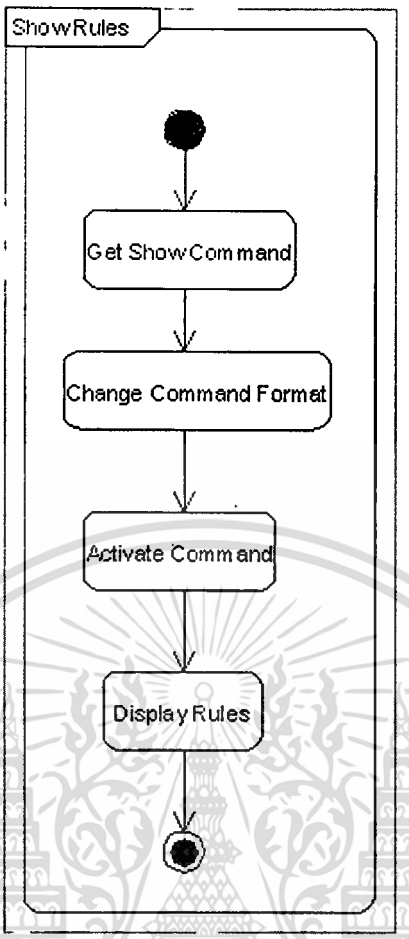


รูปที่ 3.3 แอ็คทิวิตีไดอะแกรมของการเพิ่มกฎ

เป็นแอ็คทิวิตีไดอะแกรม สำหรับการอธิบายการเพิ่มกฎลงในโปรแกรมไอพีไฟร์วอลล์โดยมีการทำงานดังนี้

1. **ระบบทำการรับค่าข้อมูลคำสั่งจากผู้ใช้**
2. **ระบบทำการเปลี่ยนรูปแบบคำสั่งให้ตรงกับที่โปรแกรมไอพีไฟร์วอลล์ใช้งานปกติ**
3. **โปรแกรมทำการเพิ่มกฎลงในรายการกฎเพื่อให้ผู้ใช้ตกลงใช้งาน**
4. **ระบบทำการเริ่มใช้งานไอพีไฟร์วอลล์ด้วยคำสั่งที่แปลงรูปแบบแล้ว**
5. **ระบบแสดงข้อมูลกฎที่ให้เพิ่มลงไปแล้วให้ผู้ใช้ทราบ**

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

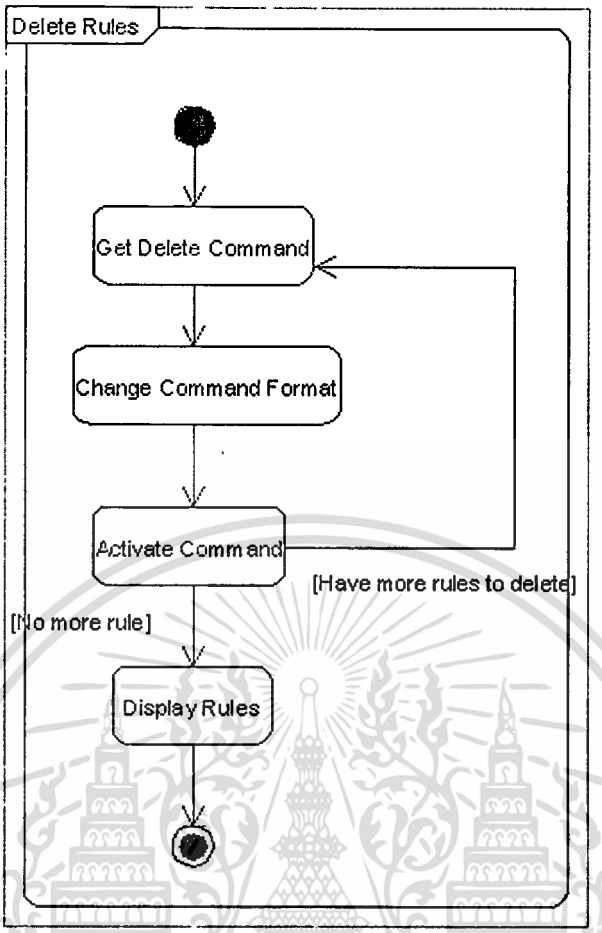


รูปที่ 3.4 แอ็คทิวิตีไดอะแกรมของการแสดงกฎ

เป็นแอ็คทิวิตีไดอะแกรม สำหรับการอธิบายการแสดงกฎ โดยมีการทำงานดังนี้

1. **ระบบรับค่าตัวเลือกคำสั่งรูปแบบกฎที่ผู้ใช้ต้องการดู**
2. **ระบบทำการเปลี่ยนรูปแบบคำสั่งให้ตรงกับที่โปรแกรมไอพีไฟร์วอลล์ใช้งานปกติ**
3. **ระบบทำการเริ่มใช้งานไอพีไฟร์วอลล์ด้วยคำสั่งที่แปลงรูปแบบแล้ว**
4. **ระบบแสดงข้อมูลกฎที่เลือกไว้ ให้ผู้ใช้ทราบ**

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 3.5 แอ็คทิวิตีไดอะแกรมของการลบกฎ

เป็นแอ็คทิวิตีไดอะแกรม สำหรับการอธิบายการลบกฎ โดยมีการทำงานดังนี้

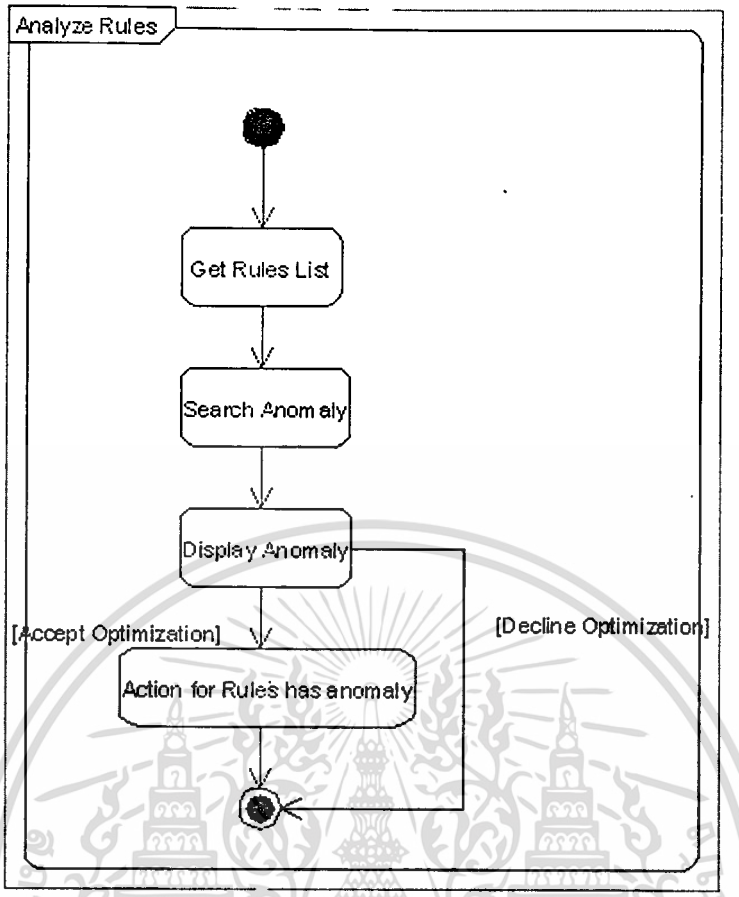
1. **ระบบรับคำสั่งกฎที่ผู้ใช้ต้องการลบออก**
2. **ระบบทำการเปลี่ยนรูปแบบคำสั่งให้ตรงกับที่โปรแกรมไอพีไฟร์วอลล์ใช้งานปกติ**
3. **ระบบทำการเริ่มใช้งานไอพีไฟร์วอลล์ด้วยคำสั่งที่แปลงรูปแบบแล้ว**

-ถ้ามีคำสั่งให้ลบกฎอื่นๆ อีกโปรแกรมจะทำการรับค่าคำสั่งและทำงาน 1-3 ใหม่

-ถ้าไม่มีกฎที่ต้องการลบจะทำการเสร็จสิ้นโปรแกรม

4. **ระบบแสดงข้อมูลกฎที่ทำการลบกฎที่ไม่ต้องการออกแล้ว ให้ผู้ใช้ทราบ**

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 3.6 แอ็คทิวิตีไดอะแกรมของการปรับแต่งกฎ

เป็นแอ็คทิวิตีไดอะแกรม สำหรับการอธิบายการปรับแต่งกฎ โดยมีการทำงานดังนี้

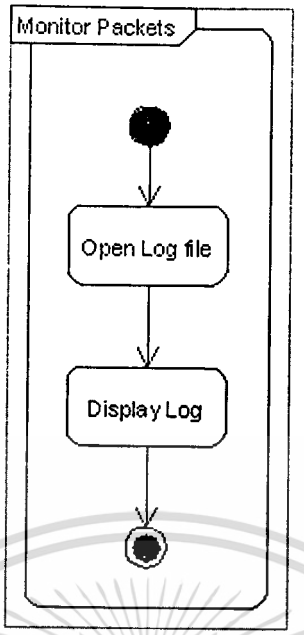
1. **ระบบรับข้อมูลกฎทั้ง หมดที่ใช้งานอยู่**
2. **ระบบทำการค้นหาและแสดงสถานะกฎที่ทำให้เกิด anomaly**
3. **ระบบแสดงข้อมูลกฎที่ทำการปรับแต่งแล้วให้ผู้ใช้ทราบ**

-ถ้าผู้ใช้ตกลงโปรแกรมจะทำการจัดการตอบสนองกับการจัดการกฎโดยผู้ใช้

-ถ้าผู้ใช้ไม่ตกลงจะจบการทำงาน

4. **ระบบทำการจัดการกฎที่เกิด anomaly ตามที่ผู้ใช้ต้องการ**

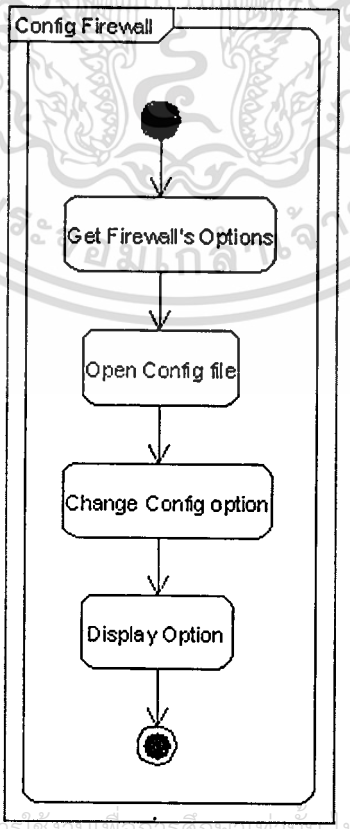
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 3.7 แอ็คทิวิตีไดอะแกรมของการตรวจสอบแพ็คเก็ต

เป็นแอ็คทิวิตีไดอะแกรม สำหรับการอธิบายการตรวจสอบแพ็คเก็ต โดยมีการทำงานดังนี้

1. ระบบข้อมูลภายในแฟ้ม log
2. ระบบทำการแสดงข้อมูลภายในแฟ้ม log นั้น

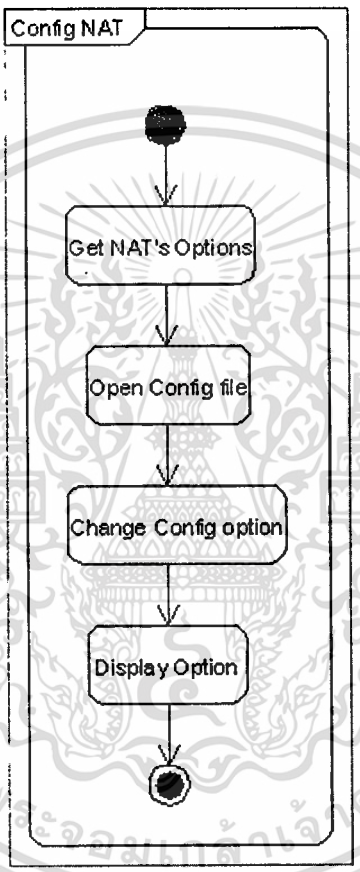


เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

รูปที่ 3.8 แอ็คทิวิตีไดอะแกรมของการปรับแต่ง Firewall

เป็นแอ็คทิวิตีไดอะแกรม สำหรับการอธิบายการแก้ไขตัวเลือกของไฟร์วอลล์ โดยมีการทำงาน ดังนี้

1. ระบบรับค่าตัวเลือกคำสั่งจากผู้ใช้
2. ระบบเปิดแฟ้มข้อมูลที่เก็บค่าคอนฟิกของไฟร์วอลล์
3. ระบบทำการแก้ไขข้อมูลลงในแฟ้มคอนฟิก
4. ระบบแสดงข้อมูลตัวเลือกที่ใช้งาน ให้ผู้ใช้ทราบ

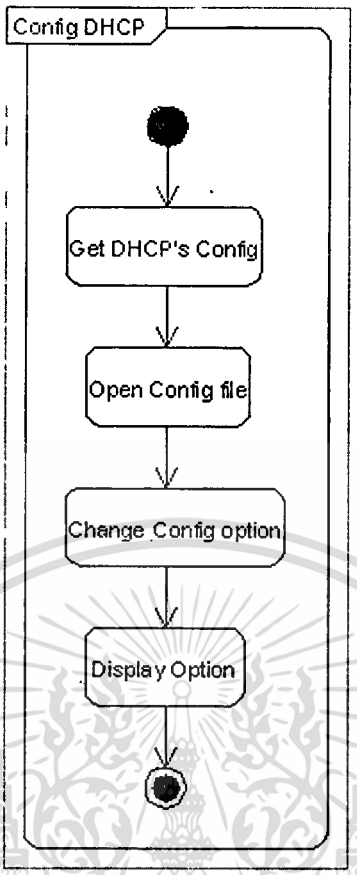


รูปที่ 3.9 แอ็คทิวิตีไดอะแกรมของการปรับแต่ง NAT

เป็นแอ็คทิวิตีไดอะแกรม สำหรับการอธิบายการแก้ไขตัวเลือกของ NAT ฟังก์ชั่น โดยมีการทำงาน ดังนี้

1. ระบบรับค่าตัวเลือกคำสั่งจากผู้ใช้
2. ระบบเปิดแฟ้มข้อมูลที่เก็บค่าคอนฟิกของ NAT ฟังก์ชั่น
3. ระบบทำการแก้ไขข้อมูลลงในแฟ้มคอนฟิก
4. ระบบแสดงข้อมูลตัวเลือกที่ใช้งาน ให้ผู้ใช้ทราบ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



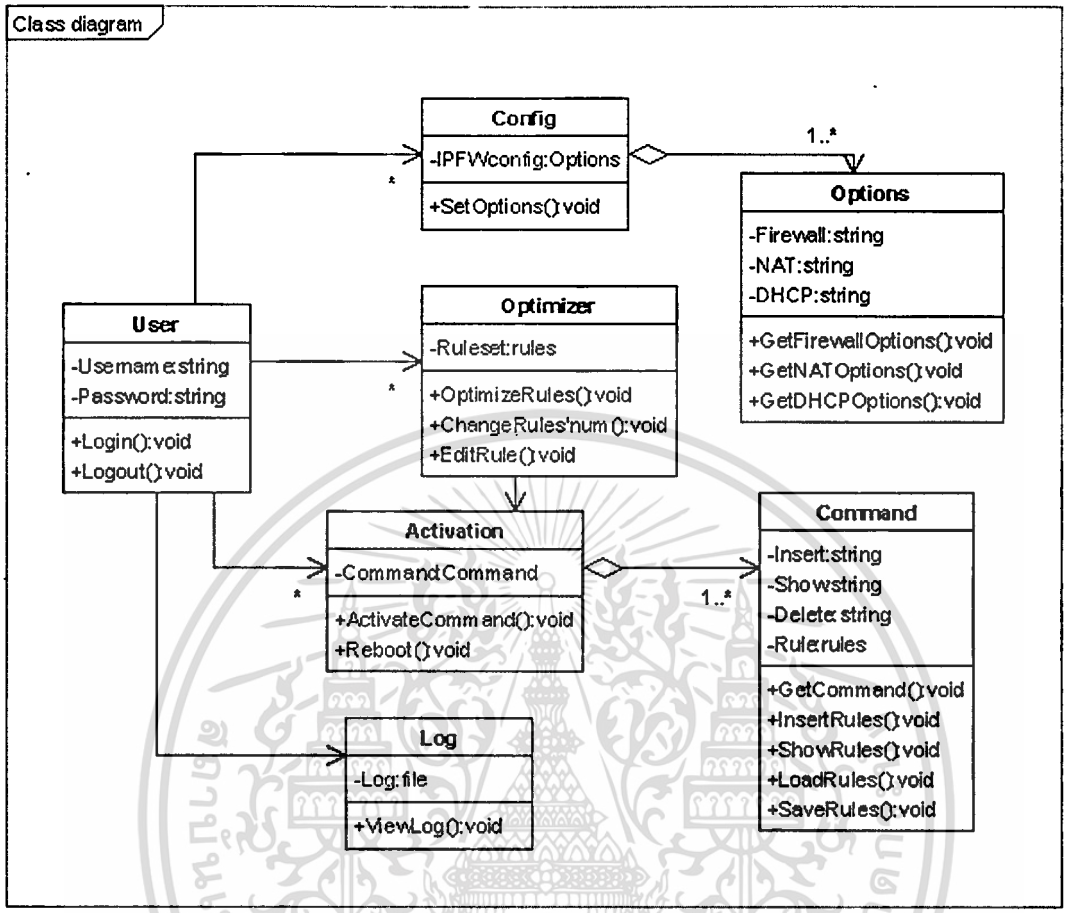
รูปที่ 3.10 แอ็คทิวิตีไดอะแกรมของการปรับแต่ง DHCP

เป็นแอ็คทิวิตีไดอะแกรม สำหรับการอธิบายการแก้ไขตัวเลือกของ DHCP โดยมีการทำงานดังนี้

1. ระบบรับค่าตัวเลือกคำสั่งจากผู้ใช้
2. ระบบเปิดแฟ้มข้อมูลที่เก็บค่าคอนฟิกของ DHCP
3. ระบบทำการแก้ไขข้อมูลลงในแฟ้มคอนฟิก
4. ระบบแสดงข้อมูลตัวเลือกที่ใช้งาน ให้ผู้ใช้ทราบ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.4 คลาสไดอะแกรมของระบบ



รูปที่ 3.11 คลาสไดอะแกรมของระบบ

เป็นไดอะแกรมที่ใช้อธิบายโครงสร้างพื้นฐานของระบบว่ามีการใช้งานแต่ละออบเจ็กต์ ที่มีความสัมพันธ์กัน

คลาส User มีความสัมพันธ์แบบ association กับคลาส Config, Optimizer และ Activation โดยมี connectivity เป็น (1,0...*) และมีความสัมพันธ์แบบ association กับคลาส Log โดยมี connectivity เป็น (1,1)

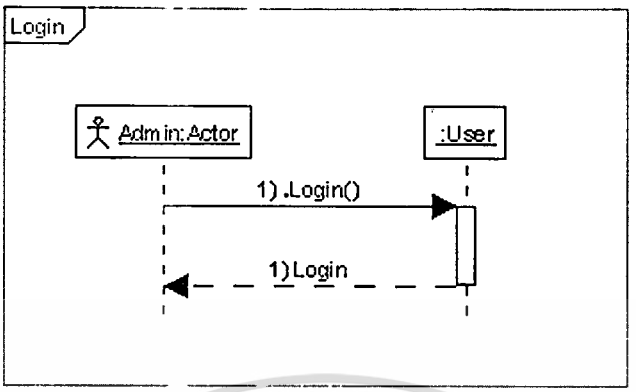
คลาส Optimizer มีความสัมพันธ์แบบ association กับคลาส Activation โดยมี connectivity เป็น (1,1)

คลาส Config มีความสัมพันธ์แบบ aggregation กับคลาส Options โดยมี connectivity เป็น (1,1...*)

คลาส Activation มีความสัมพันธ์แบบ aggregation กับคลาส Command โดยมี connectivity เป็น (1,1...*)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.5 ซีเควนซ์ไดอะแกรมของระบบ

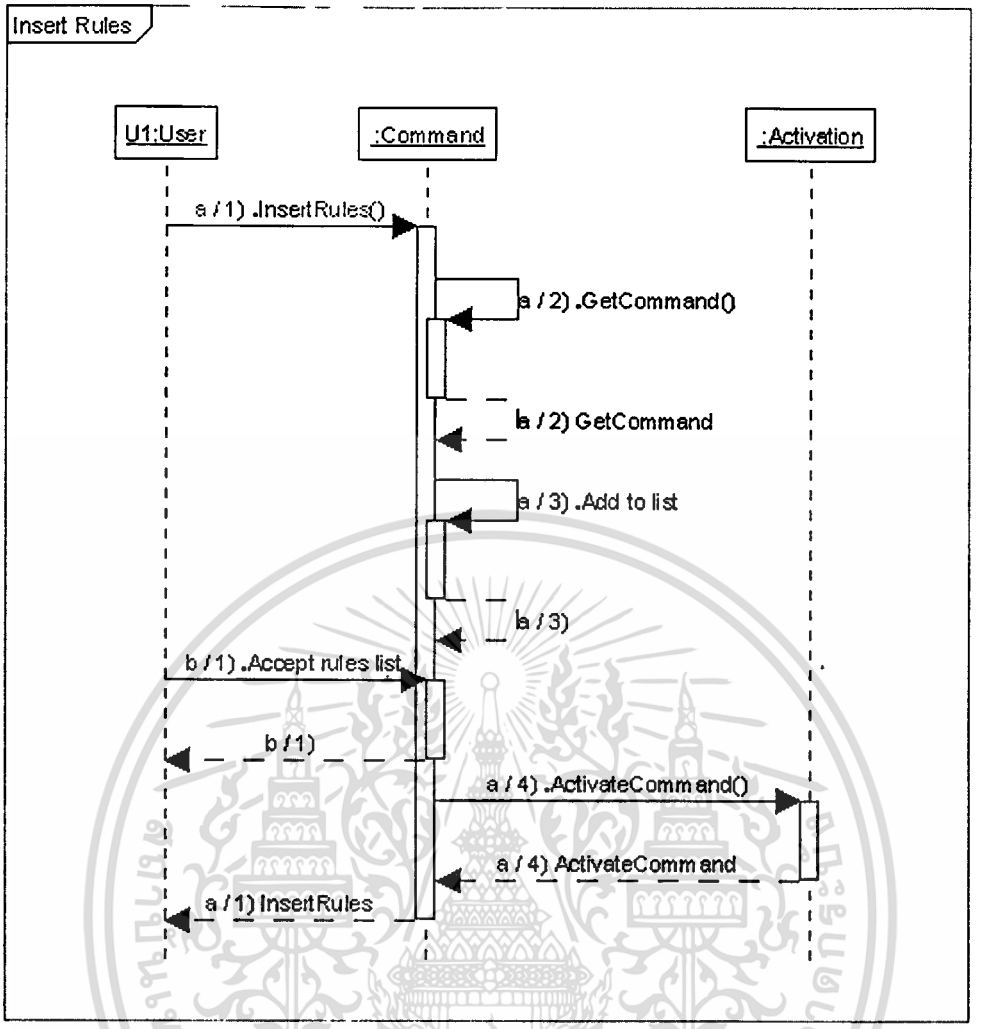


รูปที่ 3.12 ซีเควนซ์ไดอะแกรมของการล็อกอิน

โดยกิจกรรมจะเริ่มต้นและดำเนินไปตามลำดับดังนี้

1. ผู้ดูแลระบบทำการเรียกoperation login ของคลาส User
2. คลาส User ทำการส่ง message เพื่อแจ้งผลการล็อกอิน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

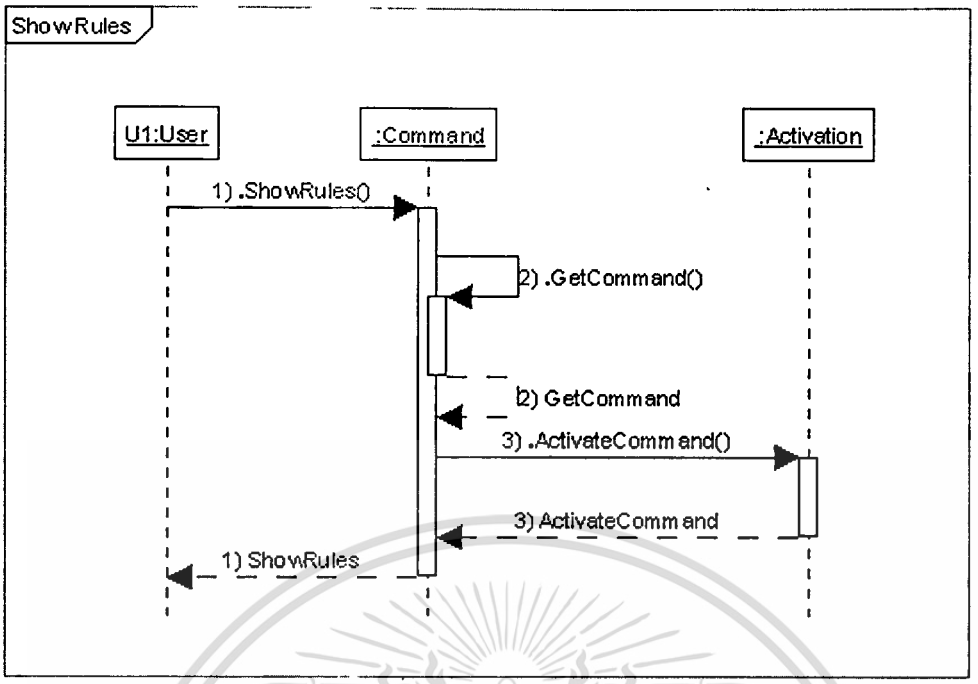


รูปที่ 3.13 ซีเควนซ์ไดอะแกรมของการเพิ่มกฎ

โดยกิจกรรมจะเริ่มต้นและดำเนินไปตามลำดับดังนี้

1. ผู้ใช้ U1 ทำการส่ง message เรียก operation InsertRules ของคลาส Command
2. คลาส Command ทำการเรียก operation GetCommand ของตัวเอง
3. คลาส Command ทำการเรียก operation ActivateCommand ของ คลาส Activation
4. คลาส Activation ทำการคืนค่าการใช้งานให้คลาส command และคลาส Command คืนค่าให้ผู้ใช้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

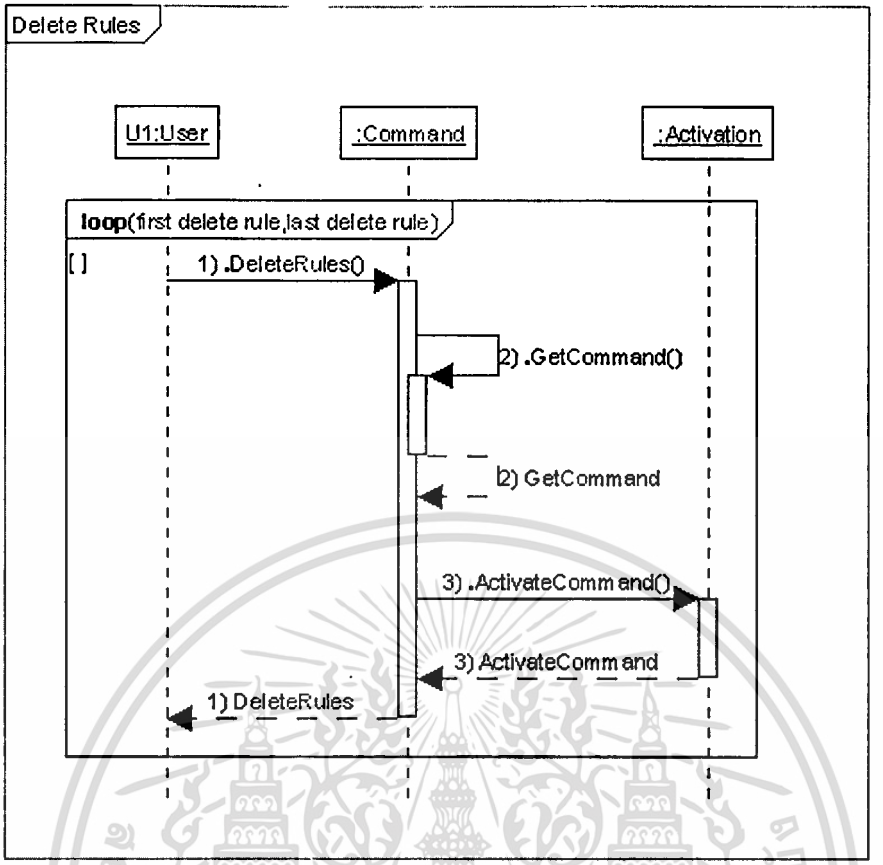


รูปที่ 3.14 ซีเควนซ์ไดอะแกรมของการแสดงกฎ

โดยกิจกรรมจะเริ่มต้นและดำเนินไปตามลำดับดังนี้

1. ผู้ใช้ U1 ทำการส่ง message เรียก operation ShowRules ของคลาส Command
2. คลาส Command ทำการเรียก operation GetCommand ของตัวเอง
3. คลาส Command ทำการเรียก operation ActivateCommand ของ คลาส Activation
4. คลาส Activation ทำการคืนค่าการใช้งานให้คลาส command และคลาส Command คืนค่าให้ผู้ใช้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

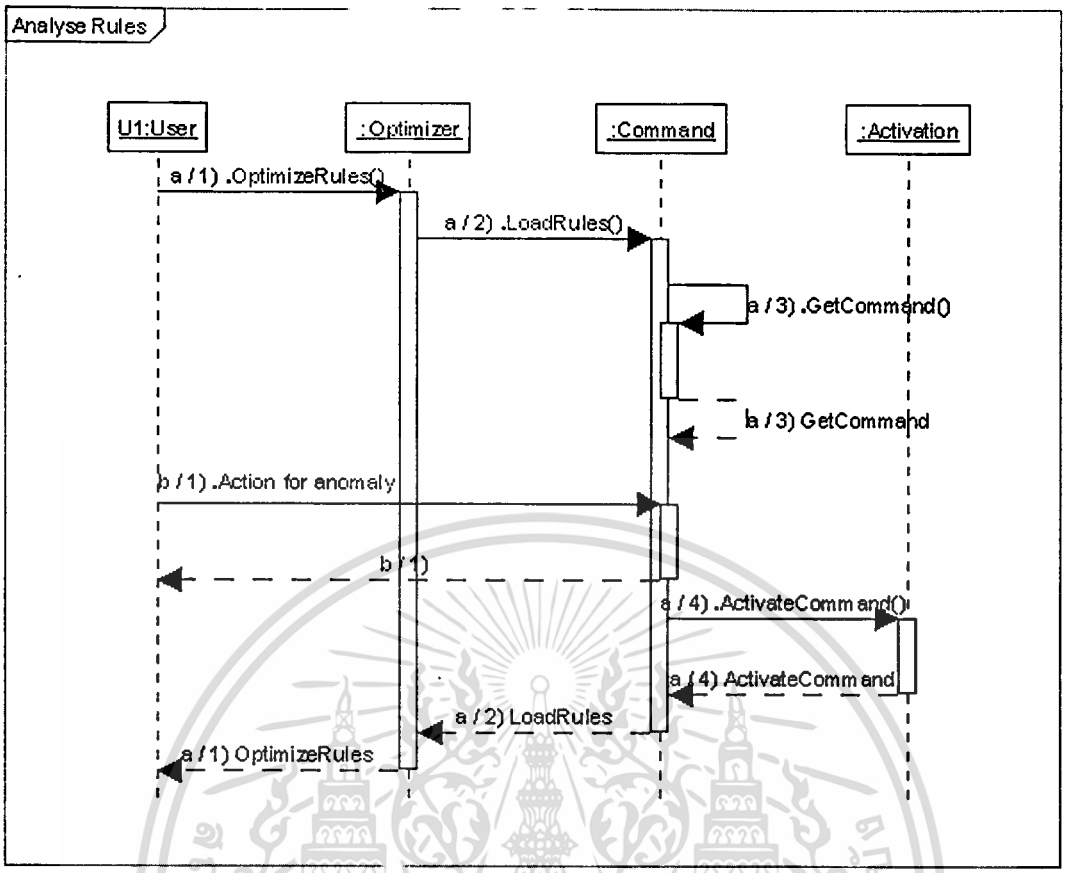


รูปที่ 3.15 ซีเควนซ์ไดอะแกรมของการลบกฎ

โดยกิจกรรมจะเริ่มต้นและดำเนินไปตามลำดับดังนี้

1. ผู้ใช้ U1 ทำการส่ง message เรียก operation DeleteRules ของคลาส Command
2. คลาส Command ทำการเรียก operation GetCommand ของตัวเอง
3. คลาส Command ทำการเรียก operation ActivateCommand ของ คลาส Activation
4. คลาส Activation ทำการคืนค่าการใช้งานให้คลาส command และคลาส Command คืนค่าให้ผู้ใช้
5. ทำการวนซ้ำจนกว่าข้อมูลจำนวนกฎที่ต้องการลบจะหมด

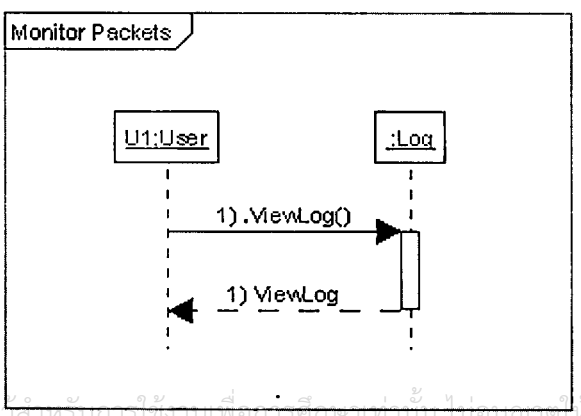
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 3.16 ซีเควนซ์ไดอะแกรมของการปรับแต่งกฎ

โดยกิจกรรมจะเริ่มต้นและดำเนินไปตามลำดับดังนี้

1. ผู้ใช้ U1 ทำการส่ง message เรียก operation OptimizeRules ของคลาส Optimizer
2. คลาส Optimizer ทำการเรียก operation DeleteRules ของคลาส Command
3. คลาส Command ทำการเรียก operation GetCommand ของตัวเอง
4. คลาส Command ทำการเรียก operation ActivateCommand ของ คลาส Activation
5. คลาส Activation ทำการคืนค่าการใช้งานให้คลาส command และคลาส Command คืนค่าให้ผู้ใช้

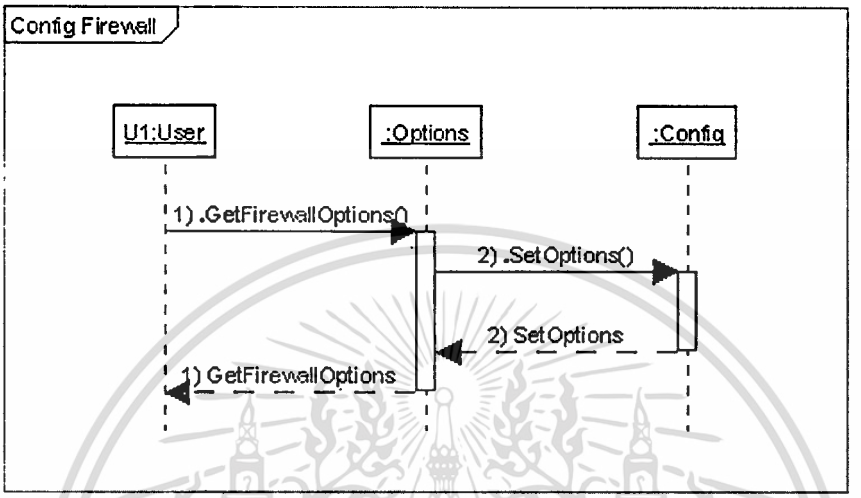


รูปที่ 3.17 ซีเควนซ์ไดอะแกรมของการตรวจสอบแพ็คเก็ต

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

โดยกิจกรรมจะเริ่มต้นและดำเนินไปตามลำดับดังนี้

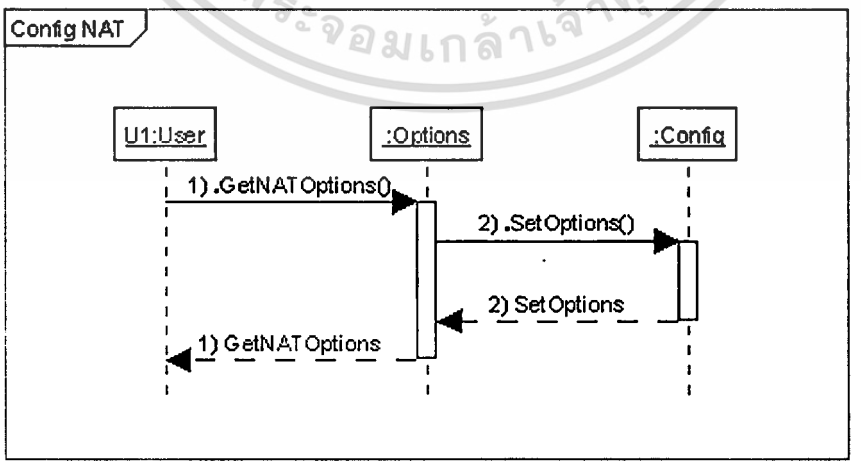
1. ผู้ใช้ U1 ทำการส่ง message เรียก operation ViewLog ของคลาส Log
2. คลาส Log ทำการส่ง message เพื่อแจ้งผลการตรวจสอบ



รูปที่ 3.18 ซีเควนซ์ไดอะแกรมของการปรับแต่งไฟร์วอลล์

โดยกิจกรรมจะเริ่มต้นและดำเนินไปตามลำดับดังนี้

1. ผู้ใช้ U1 ทำการส่ง message เรียก operation GetFirewallOption ของคลาส Options
2. คลาส Options ทำการเรียก operation SetOptions ของคลาส Config
3. คลาส Config ทำการคืนค่าตัวเลือกที่ผู้ใช้ U1 เลือก

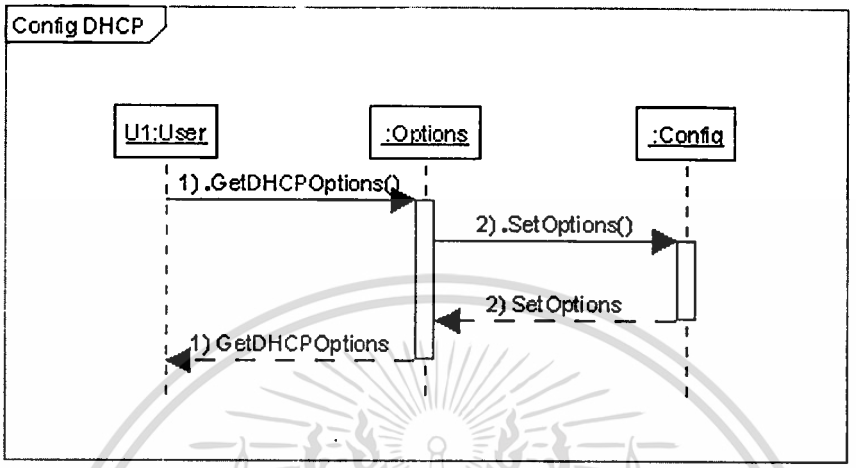


รูปที่ 3.19 ซีเควนซ์ไดอะแกรมของการปรับแต่ง NAT

โดยกิจกรรมจะเริ่มต้นและดำเนินไปตามลำดับดังนี้

เอกสารนี้มีลิขสิทธิ์ สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

1. ผู้ใช้ U1 ทำการส่ง message เรียก operation GetNATlOption ของคลาส Options
2. คลาส Options ทำการเรียก operation SetOptions ของคลาส Config
3. คลาส Config ทำการคืนค่าตัวเลือกที่ผู้ใช้ U1 เลือก



รูปที่ 3.20 ซีเควนซ์ไดอะแกรมของการปรับแต่ง DHCP

โดยกิจกรรมจะเริ่มต้นและดำเนินไปตามลำดับดังนี้

1. ผู้ใช้ U1 ทำการส่ง message เรียก operation GetDHCPlOption ของคลาส Options
2. คลาส Options ทำการเรียก operation SetOptions ของคลาส Config
3. คลาส Config ทำการคืนค่าตัวเลือกที่ผู้ใช้ U1 เลือก

ในการออกแบบระบบงานนี้โดยใช้ UML เป็นเครื่องมือในการพัฒนาช่วยให้ผู้ใช้งานสามารถเข้าใจ และ มองภาพรวมของระบบได้ง่ายขึ้น และยังทำให้ทราบรายละเอียดต่างๆ ในการทำงานของระบบส่วนใหญ่อีกด้วย โดยที่ ไดอะแกรมที่นำมาใช้งานในที่นี้จะใช้เพียง 4 ไดอะแกรม คือ ยูสเคสไดอะแกรม, แอคทิวิตีไดอะแกรม, คลาสไดอะแกรม และ ซีเควันซ์ไดอะแกรม ซึ่งนับว่าเพียงพอสำหรับระบบงานที่มีขนาดไม่ใหญ่นัก และยังแสดงข้อมูลต่างๆ ที่จำเป็นให้ผู้ใช้ได้ทราบพอสมควร ทำให้ระบบมีความชัดเจนขึ้นอีกด้วย

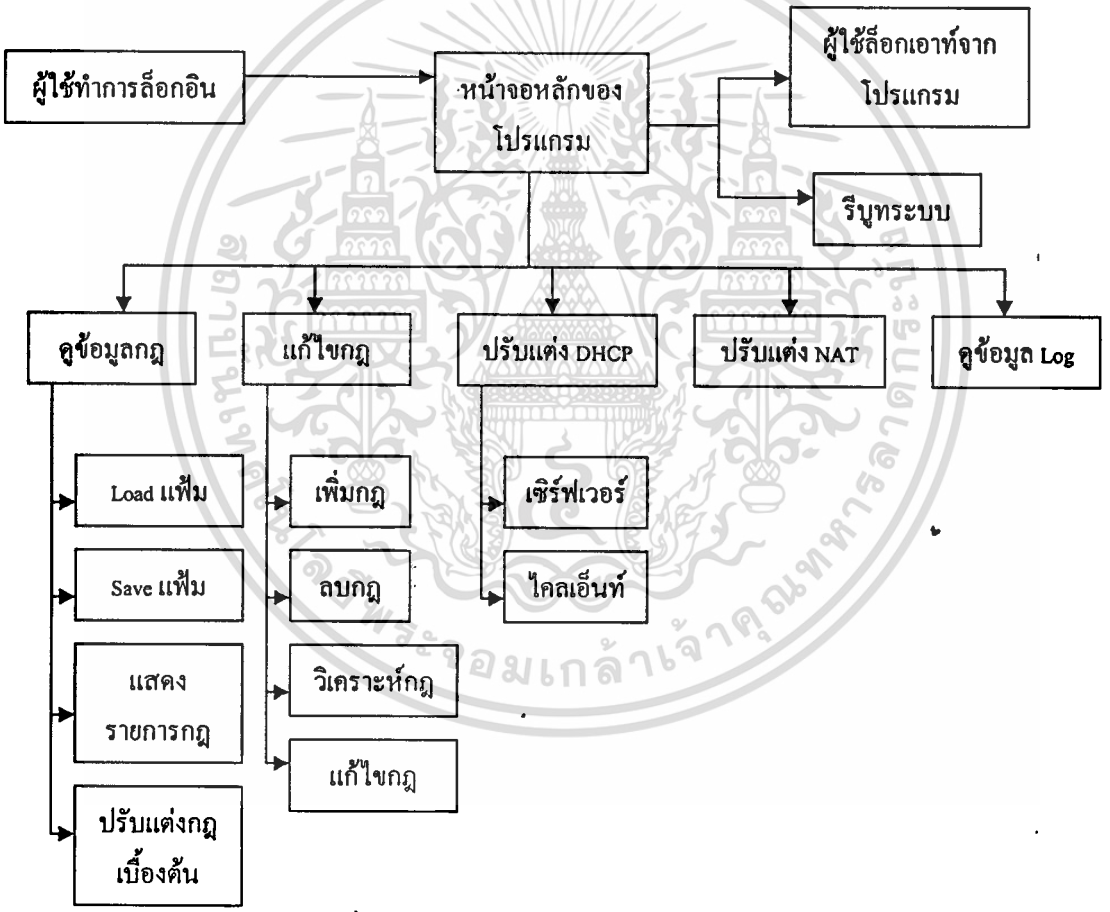
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 4
ผลการพัฒนาของโปรแกรม

ในบทนี้จะกล่าวถึงอินเตอร์เฟสที่ใช้ในการสร้างโปรแกรมที่ได้ออกแบบไว้ แสดงให้เห็นลักษณะการใช้งานของโปรแกรม และผลที่ได้จากการใช้งานโปรแกรม

4.1 หน้าจอที่ใช้งานหลัก

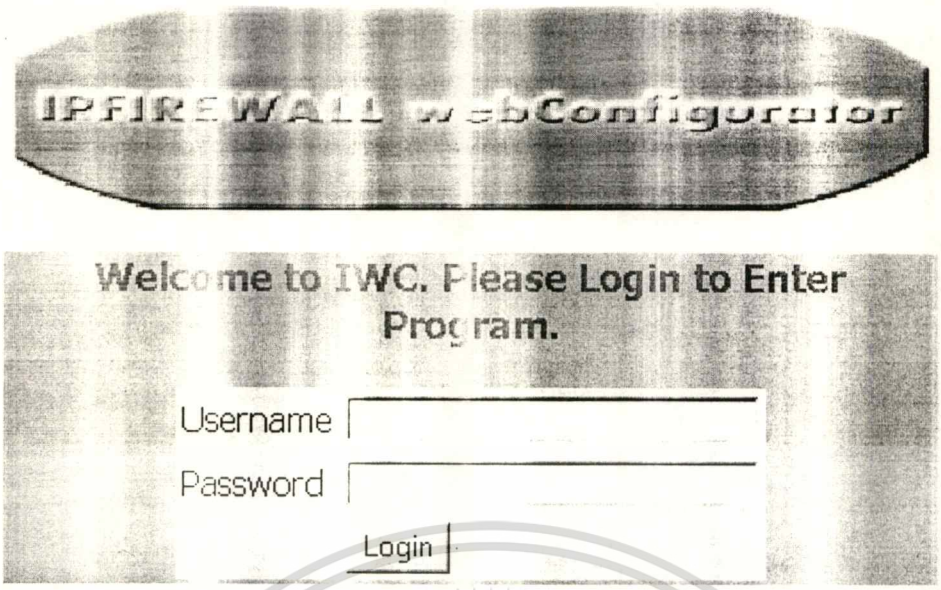
การพัฒนาโปรแกรมนี้จะมีลับดับและโฟลวของการทำงานเป็นดังนี้



รูปที่ 4.1 โฟลวในการทำงานของโปรแกรม

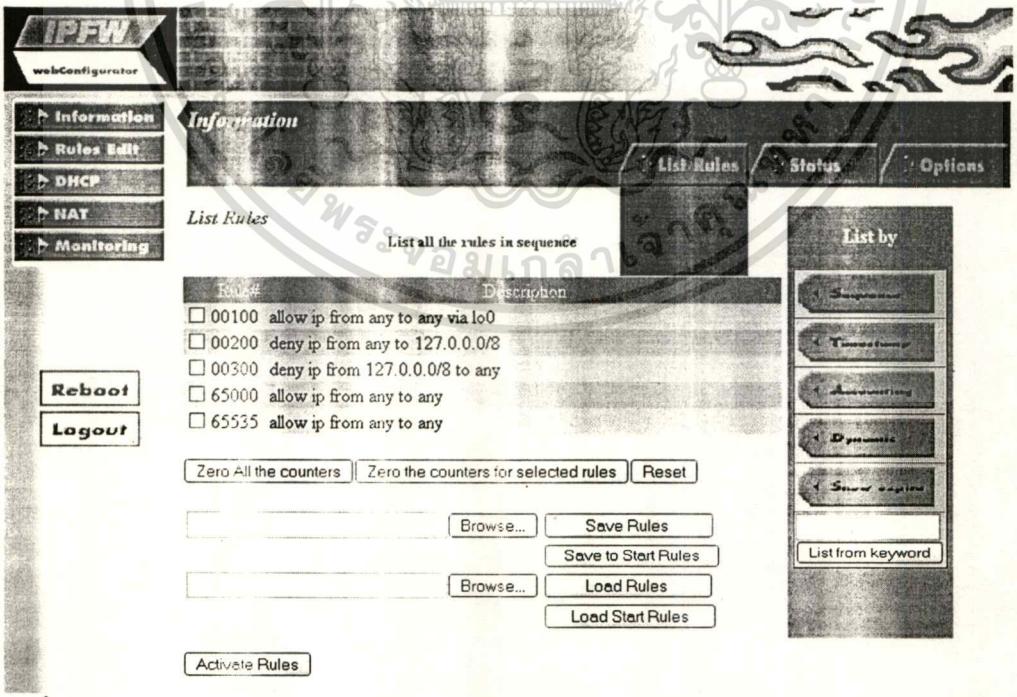
โปรแกรมจะมีการทำงานผ่านเว็บบราวเซอร์ จึงจำเป็นต้องมีการติดตั้งโปรแกรมเว็บบราวเซอร์เอาไว้แล้ว โดยอาจหาดาวน์โหลดได้จาก http://www.mozilla.org

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.2 หน้าจอโปรแกรมในส่วนการล็อกอินเข้าใช้งานโปรแกรม

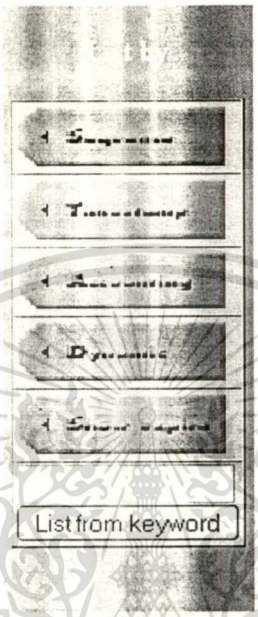
โดยผู้ใช้จะต้องทำการเข้าล็อกอินก่อนเข้าใช้งาน ซึ่งจะเก็บรายละเอียดผู้ใช้ไว้ในแฟ้มข้อมูลโดยจะทำการตั้งค่าสิทธิ์ในการใช้งานแฟ้มนี้ให้สามารถอ่านและแก้ไขแฟ้มนี้ได้ จากผู้ที่ล็อกอินเข้าสู่ระบบเป็นรูทเท่านั้น



รูปที่ 4.3 หน้าจอโปรแกรมในส่วนดูข้อมูลต่างๆ ของระบบโดยจะดูข้อมูลกฎของไฟร์วอลล์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

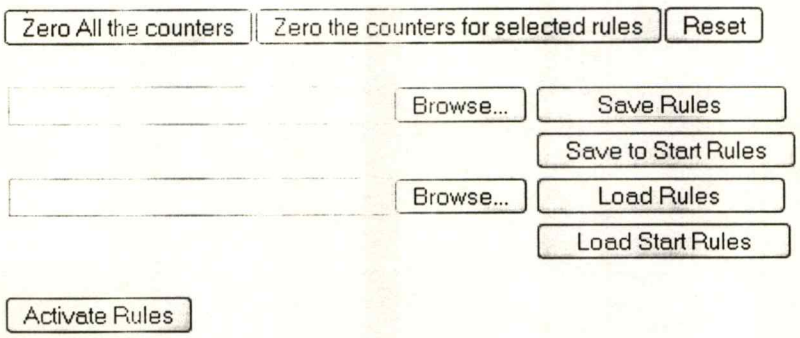
หน้าจอส่วนนี้จะใช้ในการดูข้อมูลกฎทั้งหมดที่ใช้อยู่ และเลือกรายการได้ว่าต้องการดูแบบใด โดยเลือกจากช่องทางขวา เช่น ดูรายการกฎทั้งหมดที่มีการตรงกันกับแพ็คเก็ตใน time stamp ล่าสุด, ดูข้อมูลจำนวนครั้งที่มีการตรงกับกฎที่ได้นับไว้, ดูรายการกฎที่เป็นแบบ dynamic หรือกฎที่เป็น dynamic ที่หมดอายุแล้ว เป็นต้น



รูปที่ 4.4 ลักษณะในการแสดงรายการกฎ

ส่วนการแสดงผลรายการกฎ สามารถเลือกการแสดงผลได้คือ

- Sequence แสดงกฎทั้งหมดตามลำดับหมายเลย
- Timestamp แสดงกฎทั้งหมดและเวลาที่มีการใช้กฎล่าสุด
- Accounting แสดงข้อมูลการใช้งานกฎ
- Dynamic แสดงกฎชนิด dynamic ที่เพิ่มลงในกฎที่ใช้
- Show expire แสดงกฎรวมทั้งกฎที่หมดอายุแล้ว
- List from keyword แสดงรายการกฎตาม keyword เช่น ดูกฎที่มีการ allow เป็นต้น

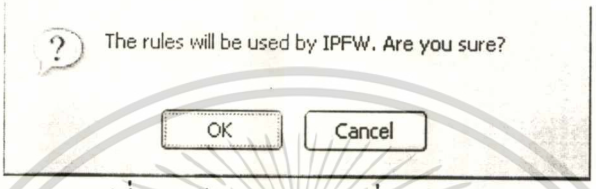


รูปที่ 4.5 ตัวเลือกที่สามารถทำได้ในการแสดงรายการกฎ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

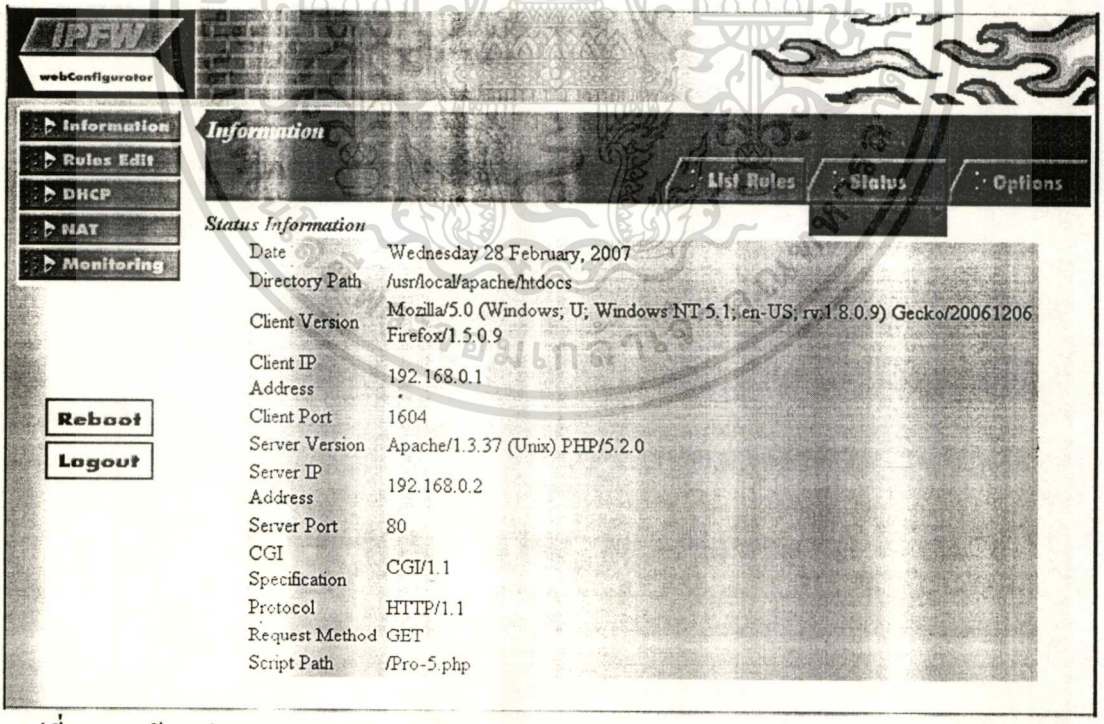
ในหน้าจอแสดงรายการกฎสามารถใช้ตัวเลือกต่างๆ ช่วยในการจัดการได้คือ

- Zero All the counters ใช้ลบตัวนับแพ็คเก็ตทั้งหมด
- Zero the counters for selected rules ใช้ลบตัวนับแพ็คเก็ตจากกฎที่เลือกไว้
- Save Rules ทำการบันทึกกฎที่แสดงอยู่ลงในแฟ้มข้อมูลที่เลือก
- Save to Start Rules ทำการตั้งค่ากฎที่แสดงอยู่ให้เป็นค่าเริ่มต้น
- Load Rules ทำการโหลดข้อมูลกฎจากแฟ้มที่เลือกไว้
- Load Start Rules ทำการโหลดข้อมูลกฎจากค่าเริ่มต้น



รูปที่ 4.6 ข้อความยืนยันเพื่อใช้งานกฎ

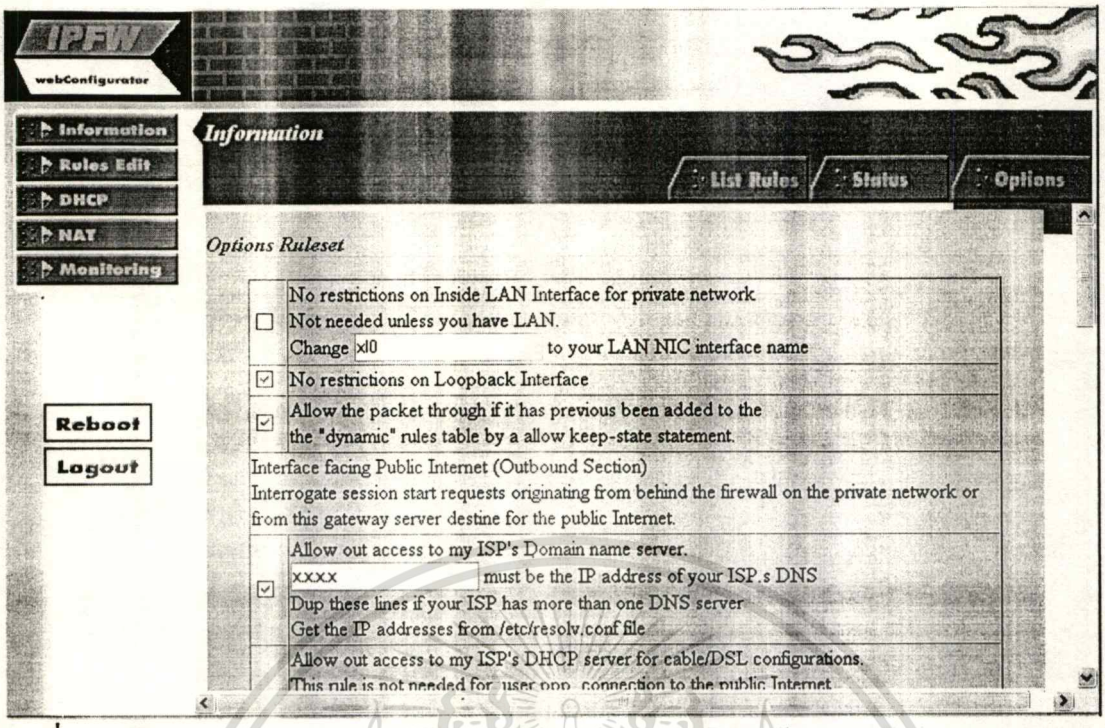
หลังจากที่โหลดค่ากฎที่ต้องการจากแฟ้มข้อมูลแล้วจะต้องทำการยืนยันเพื่อใช้งานกฎ โดยจะแสดงข้อความแจ้งให้ผู้ใช้ทราบ



รูปที่ 4.7 หน้าจอโปรแกรมในส่วนดูข้อมูลต่างๆ ของระบบโดยจะดูข้อมูลของสถานะของระบบ

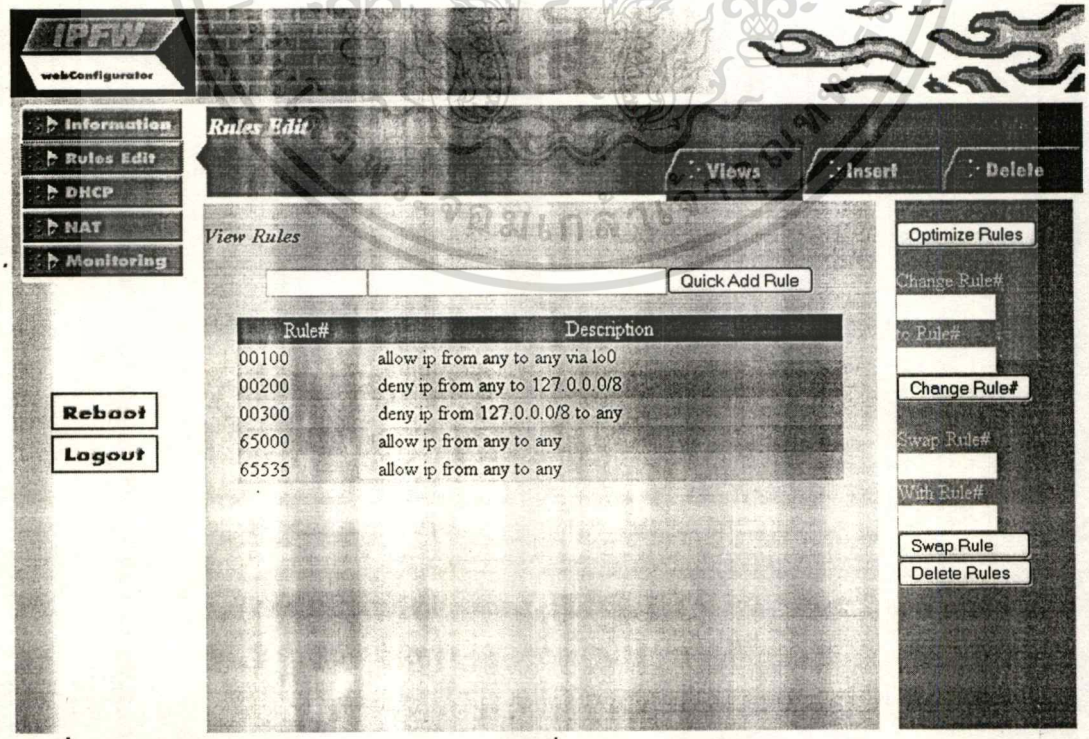
ในส่วนนี้จะมีการแสดงข้อมูลต่างๆ เช่น วันที่ที่มีการใช้งานล่าสุด, ที่อยู่ของแฟ้มข้อมูล, ที่อยู่ของไคลเอนต์ที่เชื่อมต่ออยู่ และพอร์ตที่ใช้, เวอร์ชั่นของเซิร์ฟเวอร์ และโปรโตคอลที่ใช้ เป็นต้น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



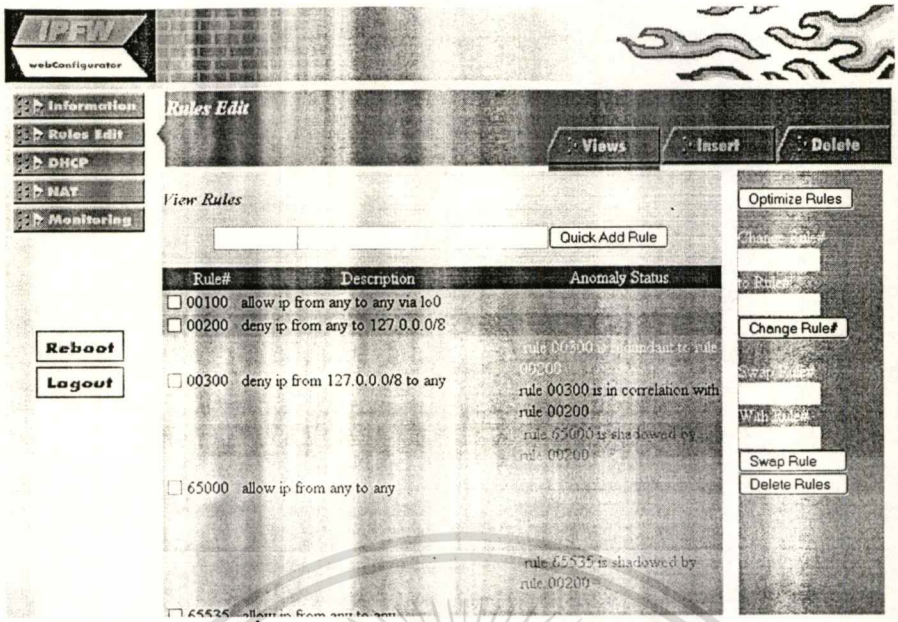
รูปที่ 4.8 หน้าจอโปรแกรมในส่วนดูข้อมูลต่างๆ ของระบบ โดยจะดูข้อมูลตัวเลือกต่างๆ ในระบบ

ในส่วนนี้จะแสดงข้อมูลตัวเลือกต่างๆ ที่ใช้ปรับแต่งค่าในไฟร์วอลล์ สำหรับผู้ใช้ที่ไม่ต้องการสร้างกฎขึ้นเอง โดยจะมีตัวเลือกให้ผู้ใช้เลือกว่าต้องการให้ไอพีไฟร์วอลล์ยอมรับหรือปฏิเสธแพ็คเก็ตใดบ้าง



รูปที่ 4.9 หน้าจอโปรแกรมในส่วนการจัดการเกี่ยวกับกฎ ในส่วนการแสดงกฎและปรับแต่งกฎ

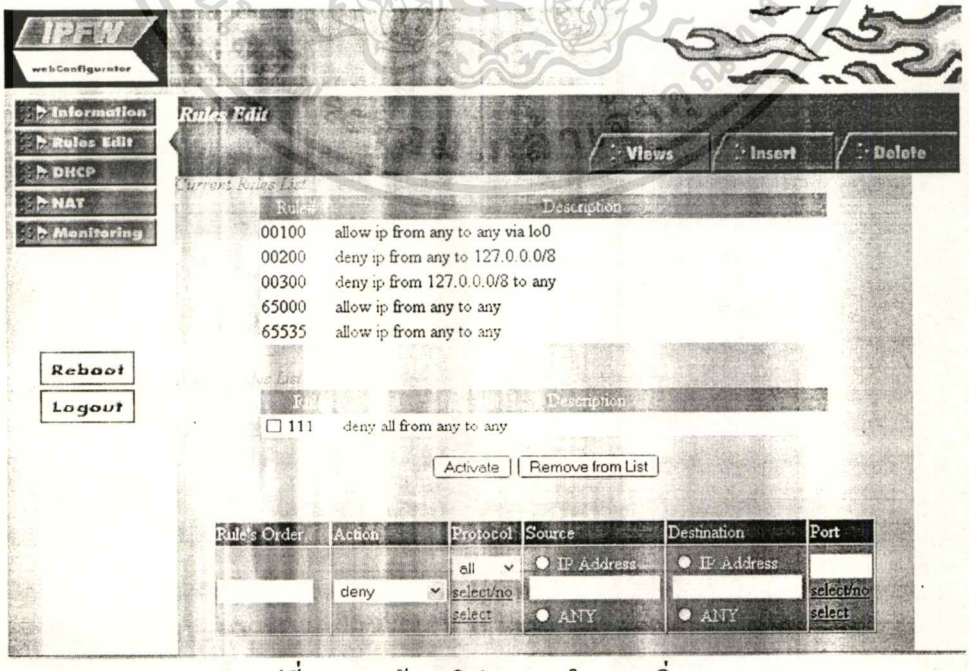
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.10 ฟังก์ชัน ในส่วนการปรับแต่งกฎ

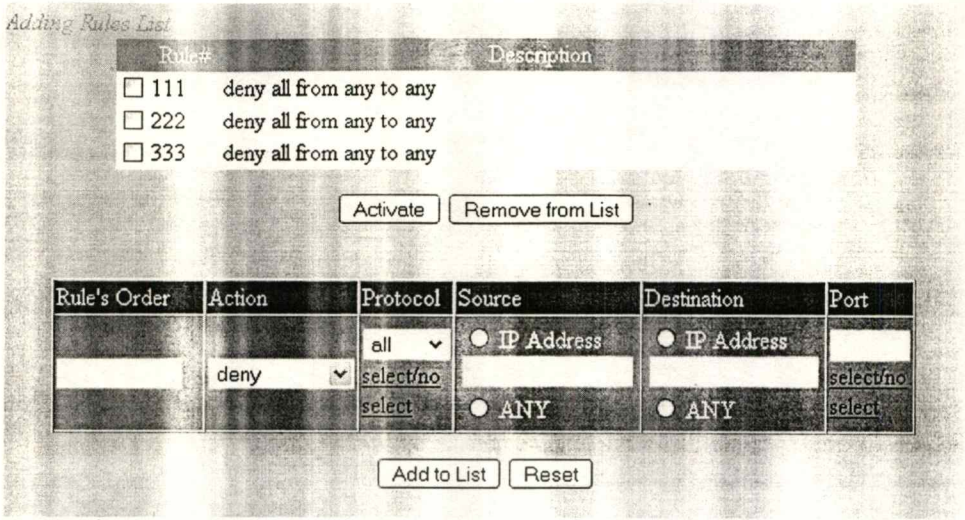
ฟังก์ชันที่สามารถใช้งานได้จากหน้าจอนี้ คือ ฟังก์ชันในการหา anomaly ที่เกิดขึ้น เมื่อตรวจพบ anomaly แล้ว ผู้ใช้สามารถแก้ไขกฎได้เบื้องต้น คือ สลับข้อ หรือแก้ไขหมายเลข กฎที่อาจถูกบังอยู่ ซึ่งจะสามารถสลับกฎได้ทีละ 1 คู่ หรือทำการแก้ไขข้อมูลกฎ และสามารถเลือกหมายเลขกฎถ้าต้องการลบกฎที่ซ้ำซ้อนได้

ในส่วนนี้จะแสดงข้อมูลกฎในไฟร์วอลล์ สามารถปรับแต่งกฎเพื่อหา anomaly ได้โดยเลือกปรับแต่งกฎ ซึ่งสามารถสลับหรือลบกฎที่ทำให้เกิด anomaly ได้



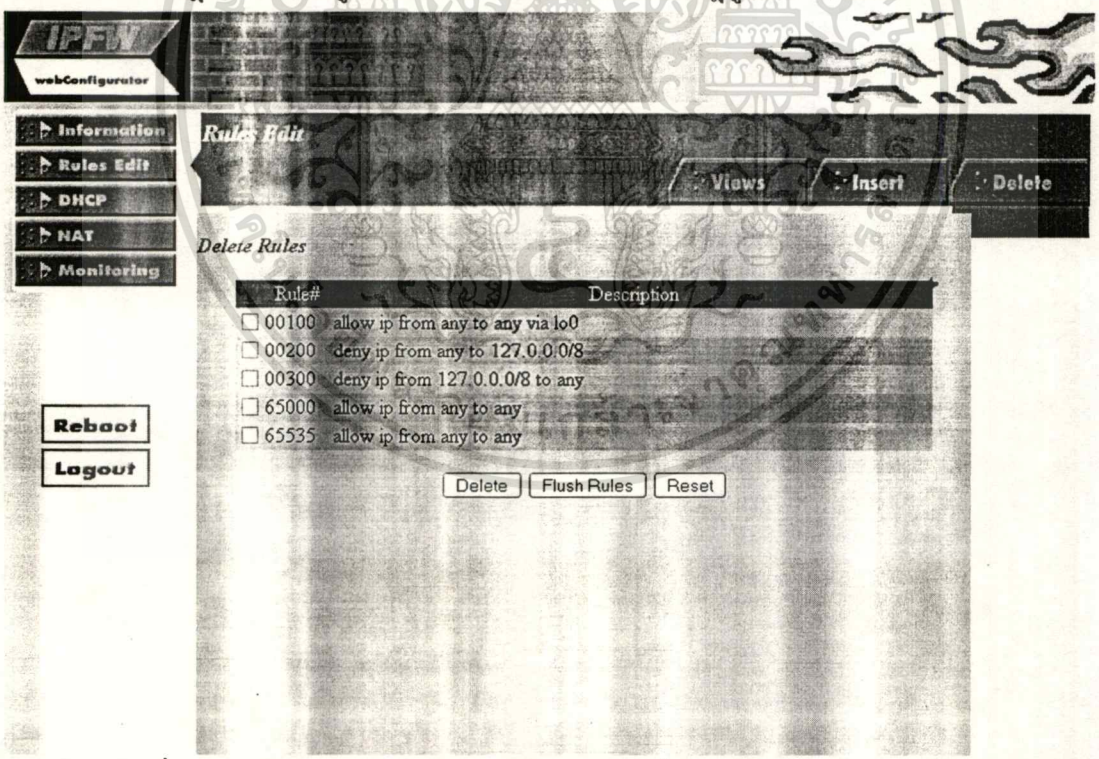
รูปที่ 4.11 หน้าจอโปรแกรมในการเพิ่มกฎ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.12 หน้าจอโปรแกรมในส่วนการจัดการเกี่ยวกับกฎ ในส่วนการเพิ่มกฎ

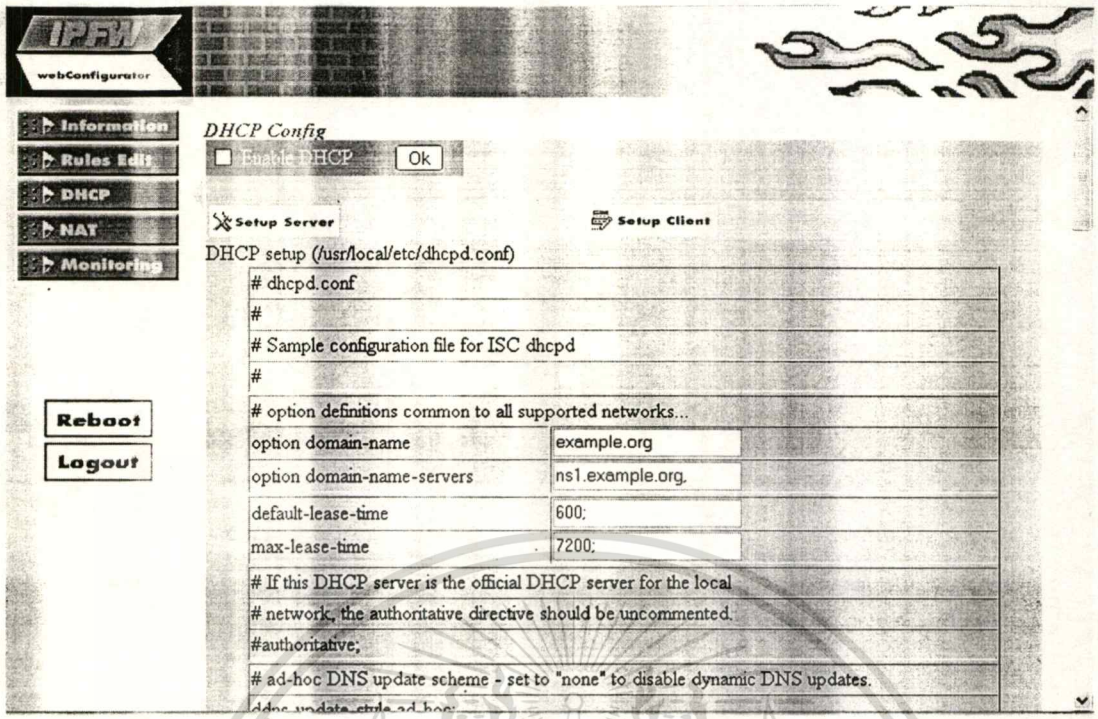
ในส่วนนี้จะเป็นการเพิ่มกฎลงในไฟร์วอลล์โดยจะต้องกรอกข้อมูลที่จำเป็นทั้งหมดลงในช่องเพื่อตกลง คือ ลักษณะการกระทำที่จะให้เกิดขึ้น, โปรโตคอล, ที่อยู่, พอร์ตทั้งต้นทางและปลายทาง ในการเพิ่มกฎเข้าใช้งาน เมื่อทำการสร้างกฎแล้ว กฎจะถูกเพิ่มลงใน list ด้านล่างซึ่งถ้าต้องการใช้งานกฎใน list นั้น ผู้ใช้ต้องทำการ Activate เพื่อให้กฎถูกใช้งานโดยโปรแกรม



รูปที่ 4.13 หน้าจอโปรแกรมในส่วนการจัดการเกี่ยวกับกฎ ในส่วนการลบกฎ

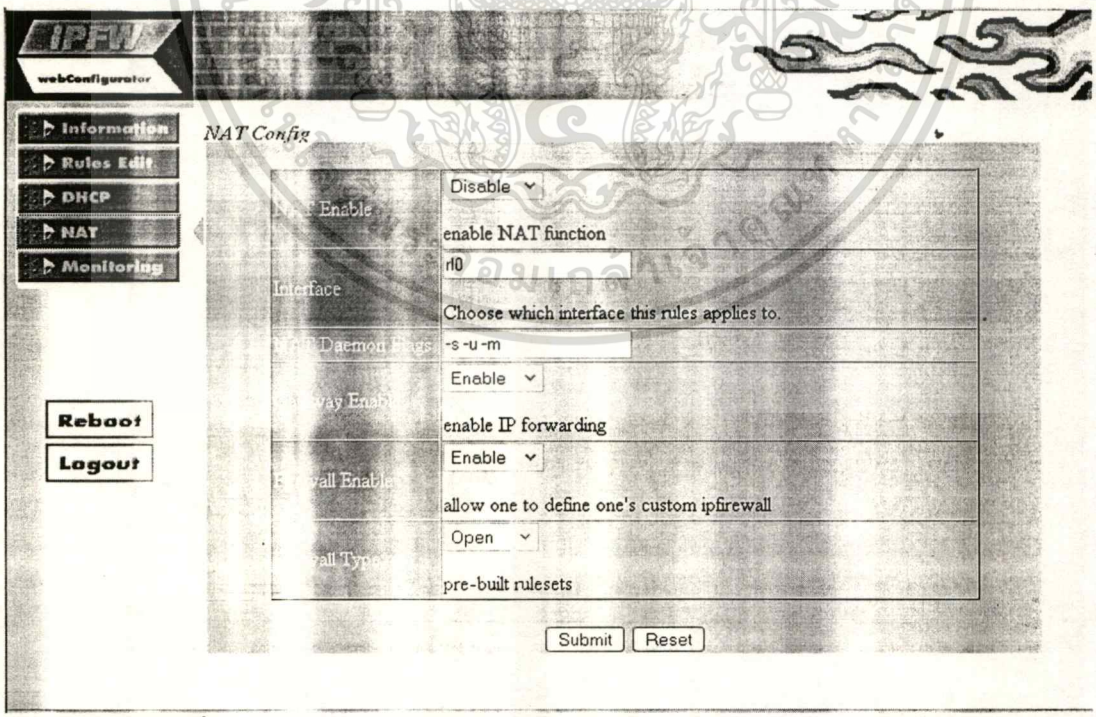
ในส่วนนี้จะแสดงข้อมูลกฎทั้งหมด ซึ่งสามารถลบกฎที่ไม่ต้องการ หรือทำการลบกฎทั้งหมดออกได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.14 หน้าจอโปรแกรมในส่วนการปรับแต่งค่า DHCP

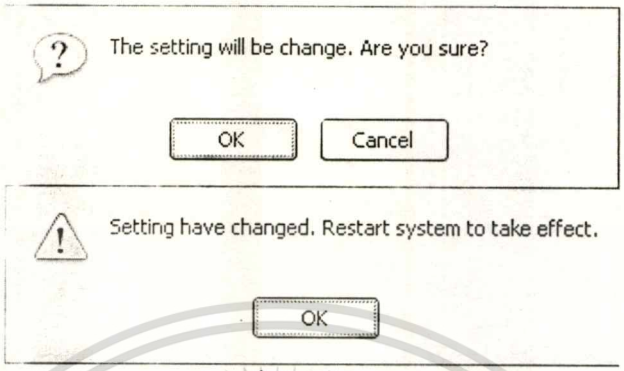
ในส่วนนี้จะเป็นการตั้งค่าต่างๆ ถ้าต้องการใช้ DHCP เช่น เปิด-ปิดการใช้งาน DHCP, สับเนต, สับเนตมาสค์ เป็นต้น ซึ่งหลังจากทำการแก้ไขค่าต่างๆ และตกลงแล้ว จะต้องทำการเริ่มระบบใหม่อีกครั้งเพื่อให้ค่าที่แก้ไขไปนั้นมีผลขึ้น



รูปที่ 4.15 หน้าจอโปรแกรมในส่วนการปรับแต่งค่าของ NAT ฟังก์ชั่น

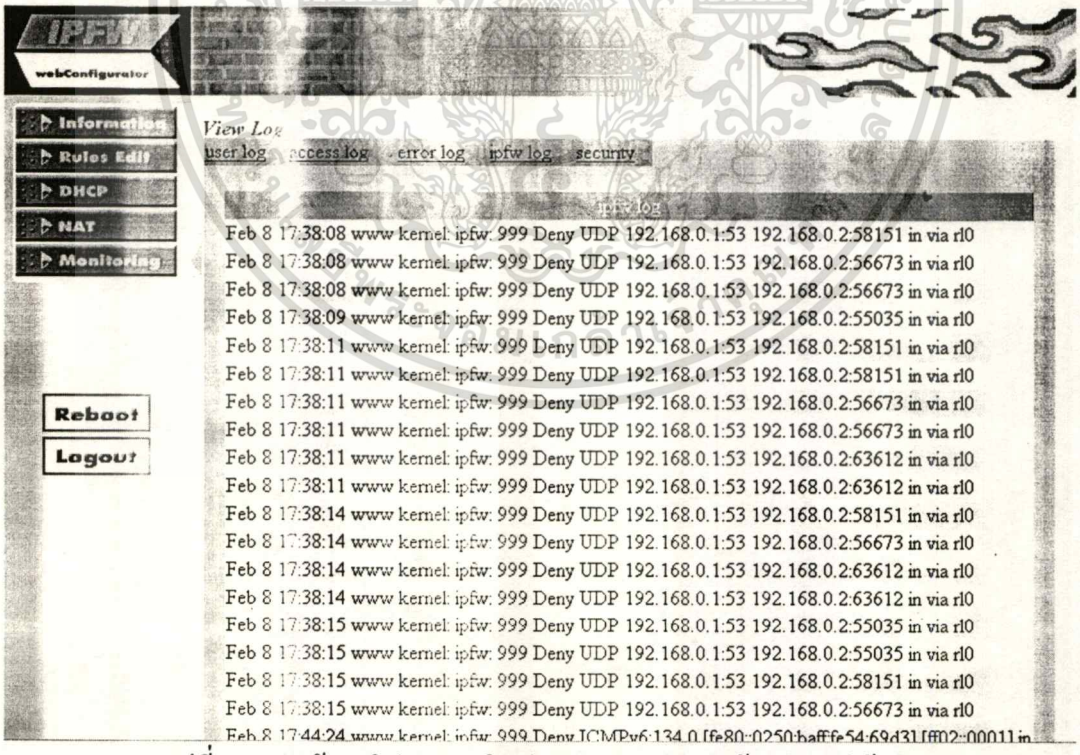
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ในส่วนนี้จะเป็นการตั้งค่าต่างๆ เมื่อมีการเปิดใช้งาน NAT และไฟร์วอลล์ เช่น อินเตอร์เฟส, ค่า daemon flags, การเปิดใช้เกทเวย์, การเปิดใช้ไฟร์วอลล์ และชนิดของไฟร์วอลล์ที่ต้องการเปิดได้แก่ Open, Client, Simple, Closed เป็นต้น



รูปที่ 4.16 หน้าต่างแสดงข้อความเตือนเมื่อมีการปรับแต่งค่าของ DHCP หรือ NAT

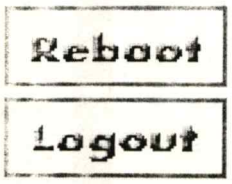
เมื่อมีการแก้ไขค่าต่างๆ ของ DHCP หรือ NAT ไปแล้วจะต้องทำการ Restart ระบบใหม่อีกครั้งเพื่อให้การใช้งานมีผล โดยสามารถเริ่มระบบใหม่ได้ด้วยคำสั่ง Reboot ที่อยู่บนหน้าจอด้านซ้ายล่าง



รูปที่ 4.17 หน้าจอโปรแกรมในส่วนการตรวจสอบข้อมูลการใช้งาน

ในส่วนนี้จะแสดงข้อมูล โดยเปิดจากแฟ้มข้อมูล log ถ้าได้มีการตั้งค่าของ log เอาไว้แล้ว

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



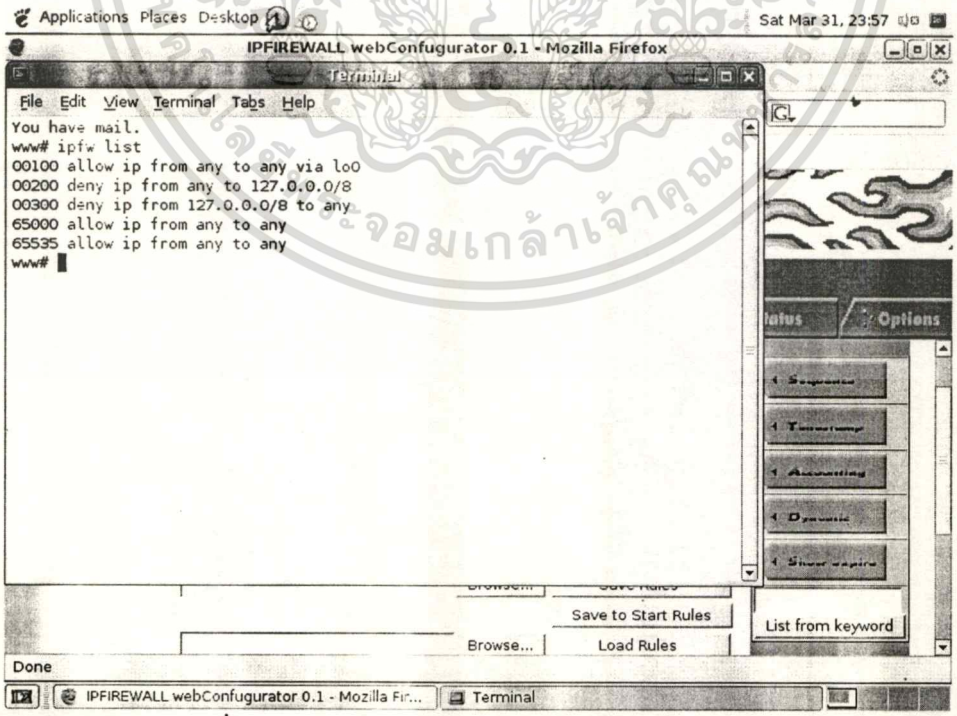
รูปที่ 4.18 คำสั่งในส่วนการ Reboot ระบบ และออกจากโปรแกรม

ผู้ใช้สามารถใช้คำสั่ง Reboot เมื่อต้องการให้ค่าที่ได้แก้ไขไว้ของระบบ เริ่มใช้งานใหม่ และใช้คำสั่ง Logout เมื่อผู้ใช้ต้องการออกจากโปรแกรม

4.2 ผลการใช้งานโปรแกรม

จากการใช้งานโปรแกรมที่ได้พัฒนาขึ้นนั้น ได้ผลลัพธ์ออกมาดังนี้

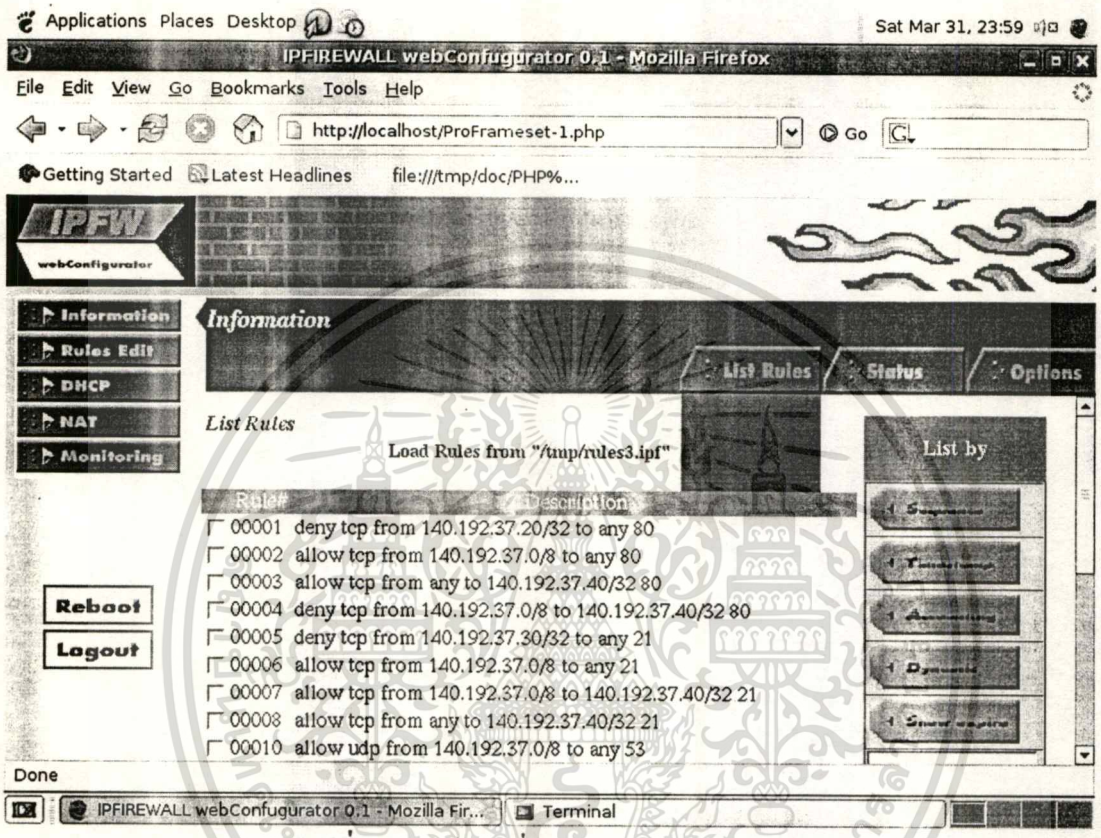
ในส่วนของการดูรายการกฎ สามารถแสดงรายการกฎของไอพีไฟร์วอลล์ได้อย่างถูกต้อง สามารถบันทึกกฎในรายการลงในแฟ้มข้อมูลได้ และสามารถโหลดข้อมูลกฎจากแฟ้มข้อมูลที่ได้มีการบันทึกไว้ได้ แต่ในการแสดงรายการกฎ ส่วนที่ได้มีการนับแพ็คเก็ตเอาไว้ยังดูเข้าใจไม่ละเอียดชัดเจนนัก และเมื่อทำการโหลดข้อมูลจากแฟ้มข้อมูลอื่นๆ ที่ไม่ใช่แฟ้มที่สร้างขึ้นจากโปรแกรมแล้ว อาจมีการแสดงผลผิดพลาดได้



รูปที่ 4.19 การแสดงกฎแบบปกติของโปรแกรมไอพีไฟร์วอลล์

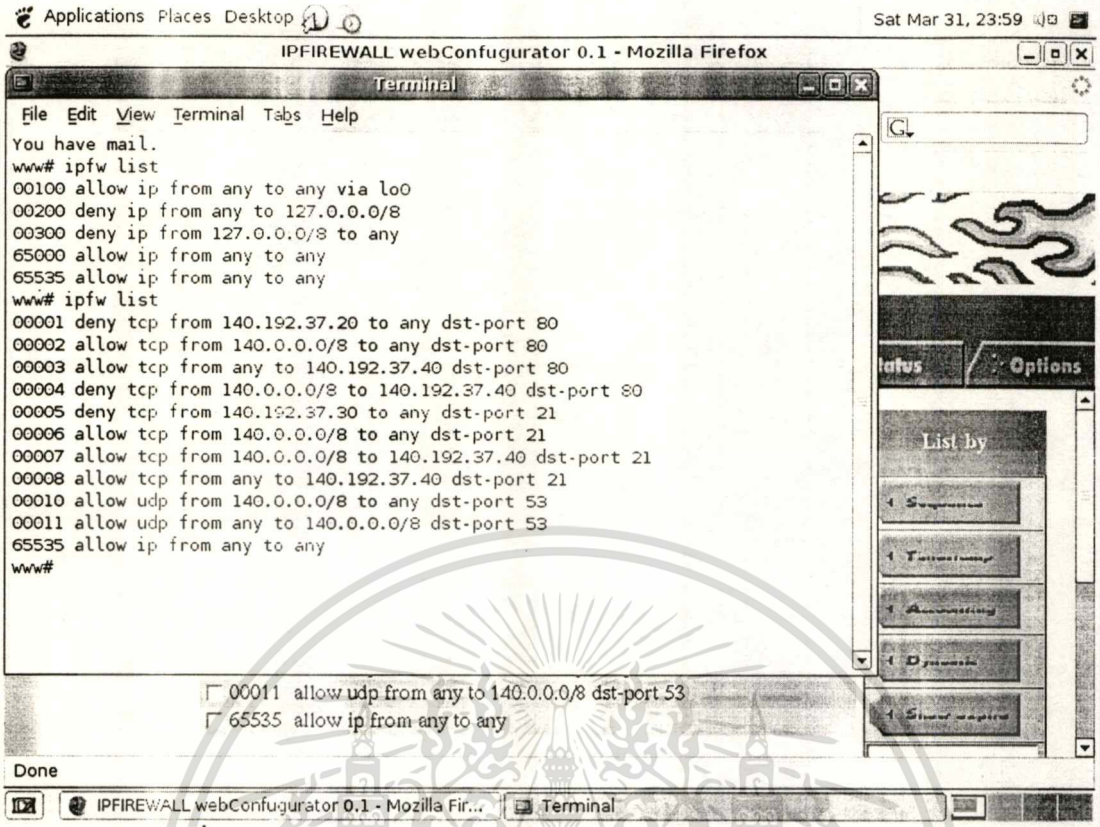
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ในส่วนการโหลดข้อมูลกฎจากแฟ้มข้อมูล ผู้ใช้จะต้องทำการโหลดแฟ้มกฎจากแฟ้มที่ได้สร้างขึ้นโดยมีรูปแบบเดียวกับแฟ้มที่สร้างขึ้นจากโปรแกรม เมื่อทำการโหลดแฟ้มแล้วโปรแกรมจะแสดงผลข้อมูลกฎในแฟ้ม ซึ่งผู้ใช้ต้องทำการ Actiovate เพื่อให้กฎที่แสดงอยู่มีผลใช้งานและจะทับลงไปบนกฎของเดิม โดยเลือกที่ปุ่ม Activate Rules ด้านล่างของหน้าจอ



รูปที่ 4.20 หน้าจอเมื่อทำการโหลดกฎจากแฟ้มข้อมูล

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.21 ผลการโหลดแฟ้มกฎเพื่อใช้งานในโปรแกรมไอพีไฟร์วอลล์

ในการโหลดข้อมูลกฎจากแฟ้มข้อมูลสามารถทำงานได้ถูกต้อง และกฎที่ทำการโหลดจะสามารถตรวจดูได้จากการใช้งานไอพีไฟร์วอลล์แบบปกติ

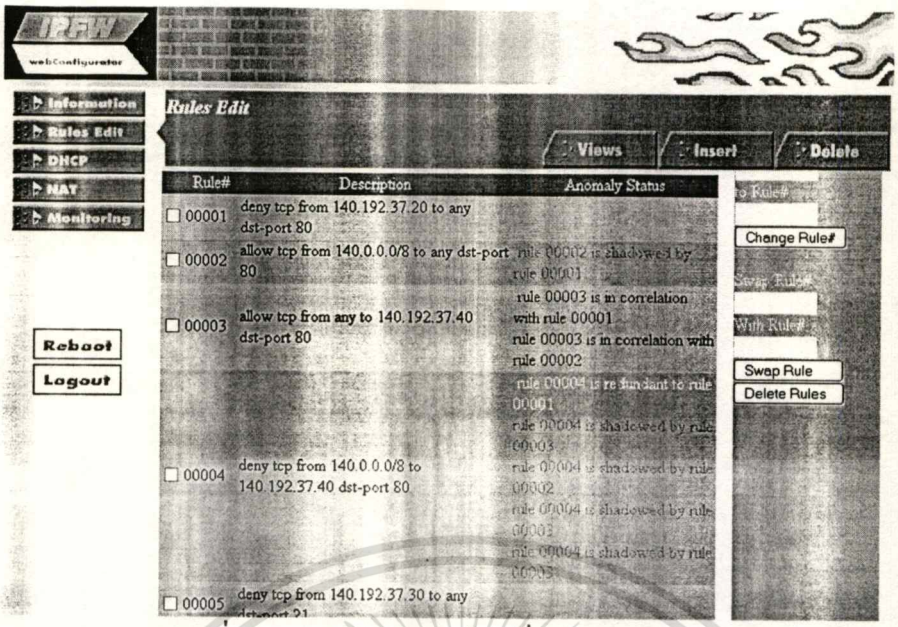
ในส่วนของการแสดงข้อมูลสถานะของระบบ สามารถแสดงข้อมูลได้ถูกต้องและชัดเจน

ในส่วนการใช้งาน ruleset ที่มีการตั้งค่าเบื้องต้นไว้แล้ว ผู้ใช้สามารถเลือกใช้งานกฎที่ต้องการได้ และแสดงรายละเอียดค่อนข้างชัดเจน

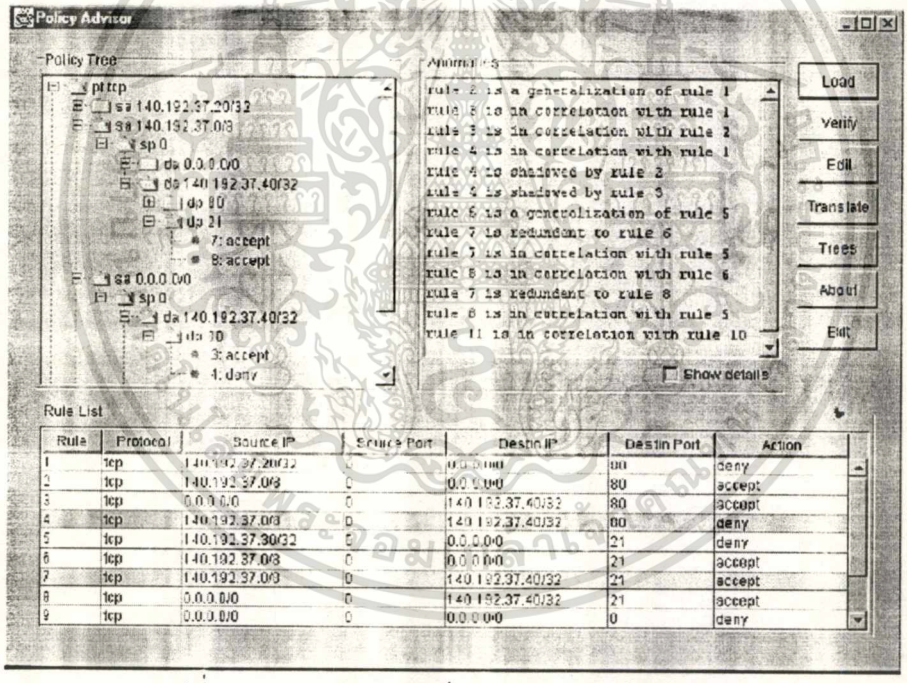
ในส่วนการปรับแต่งแก้ไขกฎ สามารถใช้งานฟังก์ชันเพื่อหา anomaly ได้ตรงตามอัลกอริทึมต้นฉบับของ Ehab S. Al-Shaer และทำการสลับข้อ แก้ไขข้อมูลและเลขลำดับกฎ หรือลบกฎได้อย่างถูกต้อง ซึ่งผู้ใช้ควรระวัง ถ้ามีการสลับหรือลบกฎข้อที่ทำให้มีผลกับโปรแกรม เช่น ทำการสลับกฎข้อที่อนุญาติให้แพ็คเก็ตของโปรแกรมผ่านได้ กับกฎข้อที่ทำการบล็อคแพ็คเก็ตของโปรแกรม ซึ่งจะทำให้ไม่สามารถใช้งานโปรแกรมต่อได้ เป็นต้น

จากการทดลองของงานต้นฉบับยังพบว่ามีความผิดพลาดเกิดขึ้นบ้าง เช่น ตัวอย่างในรูปที่ 4.23 ซึ่งกฎข้อที่ 1 กับกฎข้อที่ 2 ลักษณะความสัมพันธ์ควรจะทำให้เกิด Shadow anomaly ซึ่งในตัวอย่างเดิมนั้นกลับแสดงผลเป็น Generalization anomaly และในการพัฒนาโครงงานนี้มีการทำงานแสดงผลได้ถูกต้อง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



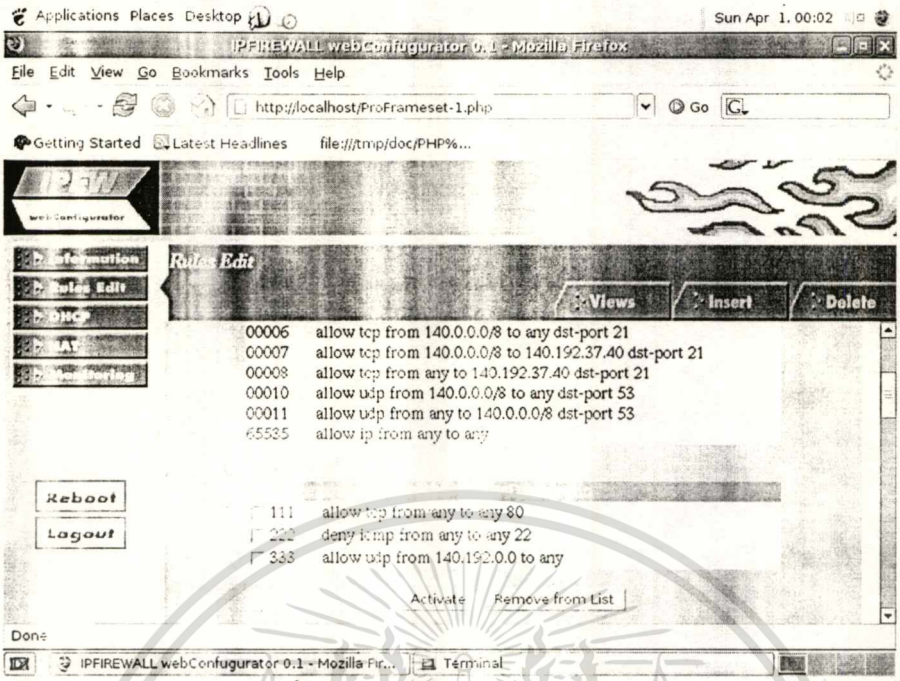
รูปที่ 4.22 ผลการวิเคราะห์กฎเพื่อค้นหา anomaly



รูปที่ 4.23 ผลการวิเคราะห์กฎของอัลกอริทึมต้นฉบับ

ในส่วนของการเพิ่มกฎ สามารถแสดงข้อมูลกฎและเพิ่มกฎได้อย่างถูกต้องซึ่งผู้ใช้ควรตรวจสอบกฎที่ต้องการเพิ่มให้มีความชัดเจนและถูกต้องก่อนทำการเพิ่มกฎ ในการเพิ่มกฎนี้จะระบุให้ใส่ข้อมูลที่จำเป็นการการตรวจสอบเน็ตเวิร์คฟิลด์ คือ หมายเลขลำดับของกฎ,โปรโตคอล, ไอพีแอดเดรสต้นทางและปลายทาง, พอร์ต และการกระทำที่ต้องการใช้กับแพ็คเก็ตนั้น ซึ่งถ้าผู้ใช้ต้องการเพิ่มกฎที่มีการบอกรายละเอียดมากขึ้นนั้น เช่น กฎที่มีการ divert แพ็ตเก็ตเมื่อมีการใช้ NAT หรือกฎที่มีการระบุอินเตอร์เฟสที่มีการใช้งาน ยังไม่สามารถทำได้ เนื่องจากเมื่อนำไปทำการหา anomaly จากฟังก์ชันในการปรับแต่งกฎแล้วจะทำให้ผลลัพธ์ที่ได้เกิดความผิดพลาดขึ้น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.24 การเพิ่มกฎของโปรแกรม

ในส่วนของการลบกฎ สามารถแสดงรายการกฎและทำการลบกฎที่ต้องการ หรือกฎทั้งหมดได้อย่างถูกต้อง และ ชัดเจน

ในส่วนการปรับแต่ค่าของ DHCP สามารถทำการเปิดใช้ DHCP ได้ และการปรับแต่งค่าคอนฟิกของ DHCP Server และ DHCP Client สามารถแก้ไขข้อมูลได้ถูกต้อง แต่ในการแสดงข้อมูลค่าต่างๆ ยังยุ่งยากและไม่ค่อยชัดเจนนัก

ในส่วนการปรับแต่งค่าของ NAT สามารถทำการแก้ไขค่าต่างๆ ในแฟ้มคอนฟิกได้ถูกต้องและเข้าใจง่าย

ในส่วนการดูข้อมูลแพ็คเก็ตและค่า Log ต่างๆ สามารถแสดงผลได้ถูกต้อง แต่ไม่มีฟังก์ชันในการทำงานเพิ่มเติม เช่นการเคลียร์ค่า Log เป็นต้น

สรุปการใช้งานโปรแกรมได้ผลลัพธ์ต่างๆ ค่อนข้างดี มีจุดบกพร่องที่ทำให้โปรแกรมใช้งานได้ไม่ค่อยสะดวกบ้าง แต่สามารถนำไปใช้งานได้ในเบื้องต้น ซึ่งจะนำไปพัฒนาต่อเพื่อเสริมการใช้งานส่วนอื่นๆ ให้มีความสะดวกมากขึ้นได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 5
สรุปผลการพัฒนา และข้อเสนอแนะ

ในระบบการรักษาความปลอดภัยของเครือข่าย ไฟร์วอลล์นับเป็นเทคโนโลยีที่สำคัญมากอย่างหนึ่ง และเช่นเดียวกับเทคโนโลยีอื่นๆ ที่ต้องใช้การจัดการที่เหมาะสมกับการบริการด้านความปลอดภัย เหตุผลหนึ่งที่ทำให้การจัดการทำได้ยาก คือความซับซ้อนในการใช้งานและช่องโหว่ต่างๆ ในเครือข่าย การพัฒนาโครงงานนี้จึงได้นำเสนอเครื่องมือเพื่อช่วยในการใช้งานโปรแกรม ไอพีไฟร์วอลล์ให้มีความเหมาะกับผู้ใช้และเพิ่มความสะดวกมากขึ้น โดยมีความสามารถในการจัดการคือ เพิ่ม, ลบกฎ, แสดงรายการกฎ และในส่วนของการวิเคราะห์กฎเพื่อตรวจหา anomaly ซึ่งช่วยให้ผู้ดูแลระบบสามารถใช้โปรแกรมนี้เพื่อจัดการกลุ่มของกฎในไอพีไฟร์วอลล์ทั่วๆ ไปได้โดยไม่ต้องให้ความสำคัญกับการวิเคราะห์กฎมากนัก และยังสามารถปรับแต่งค่าคอนฟิกต่างๆ ที่มีความเกี่ยวข้องในการใช้งานได้

โครงงานฉบับนี้ได้นำเสนอ การพัฒนายูสเซอร์อินเตอร์เฟสของไอพีไฟร์วอลล์บนระบบปฏิบัติการฟรีบีเอสดี ซึ่งการพัฒนาโปรแกรมอินเตอร์เฟสของไอพีไฟร์วอลล์ ให้เป็นรูปแบบกราฟิกมีส่วนช่วยให้ผู้ใช้งานสามารถใช้งานได้สะดวกและรวดเร็วมากขึ้น โดยพัฒนาให้ใช้งานผ่านโปรแกรมเว็บบราวเซอร์ ซึ่งจะทำให้ผู้ใช้มีความคุ้นเคยได้อย่างรวดเร็วและสามารถใช้งานผ่านแพล็ตฟอร์มที่หลากหลายมากขึ้น และได้เลือกใช้ UML เป็นเครื่องมือในการออกแบบเพื่อให้ผู้ที่อ่านรายละเอียดสามารถเข้าใจและสามารถอธิบายลักษณะการทำงานของโปรแกรมได้ ในการพัฒนาโปรแกรมได้ใช้ภาษา PHP เนื่องจากเป็นภาษาที่เขียนได้ง่ายและสามารถเขียนโปรแกรมได้ทั้งแบบเชิงโครงสร้างและเชิงวัตถุ ในการใช้งานไฟร์วอลล์ลำดับของกฎนั้นมีความสำคัญมากเนื่องจากลักษณะการทำงานของไฟร์วอลล์แบบกรองแพ็คเก็ตจะทำงาน โดยจับคู่กฎกับแพ็คเก็ตไปตามลำดับ จึงอาจทำให้เกิดความผิดปกติที่เรียกว่า anomaly ขึ้นระหว่างกฎที่มีความสัมพันธ์กันได้ ซึ่งในฟังก์ชั่นการทำงานของโปรแกรมส่วนของการปรับแต่งกฎเพื่อใช้ตรวจหา anomaly ได้เลือกใช้อัลกอริทึมของ Ehab S. Al-Shaer เนื่องจากสามารถเข้าใจและนำมาพัฒนาได้ง่าย โดยมองรูปแบบของกฎให้มีลักษณะโครงสร้างเป็นแบบ single root tree ที่เรียกว่าโพลิซีทรี ซึ่งอัลกอริทึมนี้สามารถตรวจหา anomaly ได้ครบทั้ง 4 ประเภท แต่ก็ยังไม่สามารถบอกได้ว่าตรวจพบ anomaly ได้ครบถ้วน เนื่องจากตัว routine จะเป็นการจับคู่ในแต่ละฟิลด์ของกฎทีละคู่ จึงอาจทำให้ไม่สามารถตรวจพบ anomaly ที่เกิดขึ้นจากกฎที่มีความสัมพันธ์กันหลายๆ กฎได้

ในการออกแบบโครงงานจะใช้ UML เป็นเครื่องมือในการพัฒนาซึ่งจะมีไดอะแกรมต่างๆ ให้เลือกใช้งานได้ ซึ่งในโครงงานนี้ได้เลือกเอาไดอะแกรมมาใช้ 4 ไดอะแกรมคือ ยูสเคสไดอะแกรมซึ่งเป็นไดอะแกรมที่ใช้บอกว่าในระบบมี requirement ที่เป็น functional requirement

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

อะไรบ้างและมีลำดับขั้นตอนในการทำงานคร่าวๆ อย่างไร, แอคทิวิตีไดอะแกรมซึ่งใช้อธิบายการทำงานของระบบว่ามีกิจกรรมอย่างไร โดยมากจะใช้เพื่อขยายความจากยูสเคส, คลาสไดอะแกรมเป็นไดอะแกรมที่ใช้แสดงกลุ่มของ class, interface และ collaborationและ relationship ที่เกิดขึ้นในระบบ และ ซีเควันซ์ไดอะแกรมซึ่งเป็นไดอะแกรมรูปแบบ Interaction แบบหนึ่งซึ่งใช้แสดงว่าออบเจ็กต์มีการติดต่อ (Interact) กับออบเจ็กต์อื่นๆ อย่างไร โดยไดอะแกรมทั้งหมดนี้สามารถใช้ในการอธิบายโครงงานได้อย่างชัดเจนและครบถ้วนพอสมควรซึ่งทำให้สามารถออกแบบลักษณะงานต่างๆ ได้อย่างรวดเร็วมากขึ้น

โปรแกรมที่ได้พัฒนาขึ้นนั้นจะมีฟังชันในการทำงานแบ่งออกเป็นส่วนๆ ได้แก่

1. ส่วนของการดูข้อมูลกฎและจัดการกับแฟ้มกฎ ซึ่งจะมีการทำงานหลัก 3 ฟังก์ชั่น คือ ฟังก์ชันในการโหลดและเซฟแฟ้มกฎ, การแสดงรายการกฎในรูปแบบต่างๆ และการปรับค่าตัวนับแพ็คเก็ต ฟังก์ชันในการดูข้อมูลสถานะของระบบ และฟังก์ชันในการปรับแต่งกฎเบื้องต้นให้กับผู้ใช้
2. ส่วนของการจัดการเกี่ยวกับกฎ ได้แก่ การเพิ่มกฎ การลบกฎ และในส่วนการวิเคราะห์กฎ ซึ่งสามารถทำการตอบสนองในกรณีที่เกิด anomaly ได้ คือ แก้ไขข้อมูลเลขลำดับและรายละเอียดของกฎ, สลับข้อกฎ หรือทำการลบกฎออก
3. ส่วนของการปรับแต่งค่าต่างๆ ของ DHCP ซึ่งจะมีการปรับแต่งในส่วนของเซิร์ฟเวอร์และไคลเอ็นท์
4. ส่วนของการปรับแต่งค่าเกี่ยวกับ NAT เช่นการเปิดปิดใช้ NAT และไฟร์วอลล์ การเลือกชนิดของไฟร์วอลล์ และการตั้งค่าอินเตอร์เฟสต่างๆ
5. ส่วนของการมอนิเตอร์ดูค่าต่างๆ จากแฟ้ม log เช่นการเข้าใช้งานระบบ หรือการใช้งานกฎของไอพีไฟร์วอลล์

และในการใช้งานโปรแกรมที่ได้ทำการพัฒนาขึ้นนั้นได้ผลลัพธ์ที่ค่อนข้างดี ส่วนของการแสดงผลทำออกมาได้ครบถ้วนและค่อนข้างชัดเจน และมีความสะดวกสบายในการใช้งานเบื้องต้นมากขึ้น ซึ่งยังคงมีข้อบกพร่องอยู่บ้าง และมีข้อจำกัดในการใช้งาน เช่น ผู้ใช้จะต้องทำการอนุญาตให้แพ็คเก็ตของโปรแกรมสามารถผ่านไฟร์วอลล์ได้ เนื่องจากโปรแกรมมีการทำงานผ่านโปรแกรมเว็บบราวเซอร์ จึงต้องให้ไฟร์วอลล์อนุญาตให้แพ็คเก็ตผ่านเข้ามาได้ และการตั้งกฎหรือลบที่มีผลต่อการทำงานของโปรแกรมอาจทำให้โปรแกรมไม่สามารถทำงานต่อได้ หรือแม้แต่การสลับข้อของกฎในไฟร์วอลล์ที่มีผลต่อโปรแกรม อาจทำให้โปรแกรมไม่สามารถทำงานต่อได้เช่นกัน อย่างไรก็ตาม โครงงานนี้ เป็นตัวอย่างให้ผู้ที่สนใจจะนำไปแก้ไขและพัฒนาต่อให้สามารถใช้งานได้สะดวกและหลากหลายประโยชน์มากกว่าเดิม

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ข้อเสนอแนะของการพัฒนาโปรแกรม ควรจะมีการจัดการเกี่ยวกับการตั้งค่าต่างๆในระบบ โดยเบื้องต้นให้กับผู้ใช้ทั่วๆ ไปซึ่งอาจมีความรู้ในการจัดการระบบไม่มากนัก และทำการบันทึกการตั้งค่าต่างๆ เพื่อโหลดใช้งานได้ทันที เพิ่มเติมส่วนของการมอนิเตอร์ เช่นการเคลียร์ค่า log หรือทำการเก็บข้อมูล log ในการจัดการกับกฎหรือโปรแกรมส่วนต่างๆ ในการใช้งานอัลกอริทึมอาจเลือกใช้อัลกอริทึมหลายๆ ตัวในการใช้งาน เช่น ในการวิเคราะห์กฎ เพื่อเพิ่มความยืดหยุ่นและประสิทธิภาพในการตรวจสอบ ซึ่งการพัฒนาควรมีการรองรับอินเตอร์เฟส เป็นภาษาไทย เพื่อให้ผู้ใช้ที่ไม่มีความรู้ด้านภาษาอังกฤษก็สามารถใช้งานโปรแกรมนี้ได้เช่นกัน

วิธีการที่นำเสนอในโครงงานฉบับนี้เป็นเทคนิคหนึ่งเท่านั้น ที่ช่วยในการปรับปรุงและพัฒนาการใช้งาน ไอพีไฟร์วอลล์ในรูปแบบของการใช้งานผ่านโปรแกรมเว็บบราวเซอร์แต่ก็ยังมีเทคนิควิธีการอื่นที่น่าสนใจ และสามารถที่ทำให้การใช้งานมีความสะดวกสบายและใช้งานได้หลากหลายมากขึ้น เช่นการนำอัลกอริทึมในการปรับแต่งกฎหลายๆ ตัวมาใช้เปรียบเทียบกันและการเพิ่มกฎโดยมีการตรวจหาความผิดปกติที่เกิดขึ้นเมื่อมีการใช้งานกฎดังกล่าว เป็นต้น ซึ่งเทคนิคเหล่านี้ยังสามารถนำไปพัฒนาต่อให้โปรแกรมมีความสมบูรณ์ และสามารถนำไปใช้งานจริงได้มีประสิทธิภาพมากขึ้น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บรรณานุกรม

กิตติพงษ์ สุวรรณราช. 2547. **การบริหารและจัดการเครือข่ายอินเทอร์เน็ตด้วยระบบปฏิบัติการ FreeBSD**. พิมพ์ครั้งที่2. นนทบุรี. ประเทศไทย: บริษัท ออฟเซ็ท เพรส จำกัด.

กิตติศักดิ์ เจริญโภคานนท์. 2548. **คู่มือเรียนเขียนเว็บอีคอมเมิร์ซด้วย PHP5.** พิมพ์ครั้งที่ 1. กรุงเทพฯ. ประเทศไทย. บริษัท ซักเซส มีเดีย จำกัด.

ธัญลักษณ์ ผังชัยมงคล. 2548. **การพัฒนายูสเซอร์อินเตอร์เฟสแบบเว็บสำหรับไอพีไฟร์วอลล์ของฟรีบีเอสดี**. วิทยาศาสตรมหาบัณฑิต. โครงการพัฒนาระบบงาน. สาขาเทคโนโลยีสารสนเทศ. คณะเทคโนโลยีสารสนเทศ, สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง.

ปณิธาน เขินอำนวย. 2546. **ระบบปรับแต่งกฎของไฟร์วอลล์โดยอัตโนมัติ**. วิทยาศาสตรมหาบัณฑิต. โครงการพัฒนาระบบงาน. สาขาเทคโนโลยีสารสนเทศ. คณะเทคโนโลยีสารสนเทศ, สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง.

วรกุล เมืองสุวรรณ. 2543. **การพัฒนาโปรแกรมจัดการไอพีไฟร์วอลล์บนระบบฟรีบีเอสดีผ่านทางเว็บ**. วิทยาศาสตรมหาบัณฑิต. โครงการพัฒนาระบบงาน. สาขาเทคโนโลยีสารสนเทศ. คณะเทคโนโลยีสารสนเทศ, สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง.

วิชิตฤกษ์ บริบูรณ์. 2547. **โปรแกรมควบคุมระบบไฟร์วอลล์บนลินุกซ์**. วิทยาศาสตรมหาบัณฑิต. โครงการพัฒนาระบบงาน. สาขาเทคโนโลยีสารสนเทศ. คณะเทคโนโลยีสารสนเทศ, สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง.

Ehab S. Al-Shaer and Hazem H. Hamed. 2002. **"Design and Implement of Firewall Policy Advisor Tool"**. Technical Report CTI-techrep0801. School of Computer Science Telecommunications and Information Systems. DePaul University.

The Apache HTTP Server Project. 2006. Available URL: http://httpd.apache.org/docs/

FreeBSD Documentation Project. 2006. Available URL: http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/introduction.html

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ภาคผนวก

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ภาคผนวก ก.
คู่มือการติดตั้งโปรแกรม

การติดตั้งระบบปฏิบัติการฟรีบีเอสดี

เมื่อเราได้ตรวจสอบความพร้อมของอุปกรณ์ และสถาปัตยกรรมของซีพียูแล้ว เราจะสามารถติดตั้งระบบปฏิบัติการฟรีบีเอสดีได้จากแผ่นติดตั้ง ซึ่งสามารถหาดาวน์โหลดได้จาก http://www.freebsd.org เมื่อเปิดเครื่องและให้ระบบทำการบูทจากแผ่นติดตั้งแล้ว โปรแกรมจะทำการรันโปรแกรมติดตั้ง พร้อมทั้งแสดงรายละเอียดของอุปกรณ์ต่างๆ ที่มีอยู่ในเครื่อง และแสดงรายการให้เราเลือกรูปแบบของการติดตั้ง ทั้งหมด 3 แบบคือ

เมนู Skip kernel configuration and continue with installation เมื่อต้องการข้ามขั้นตอนของการปรับแต่งค่าต่างๆ ของเคอร์เนล และเข้าสู่หน้าจอการติดตั้งต่อไป

เมนู Start kernel configuration in full-screen visual mode เมื่อต้องการปรับแต่งค่าต่างๆ เช่น Network Card ที่เราใช้ต้องการเปลี่ยนค่า IRQ และ IO port

เมนู Start kernel configuration in CLI mode เมื่อต้องการปรับแต่งค่าต่างๆ โดยจะเป็นการสั่งงานในรูปแบบของ Command line

ในที่นี้จะเลือกเมนู Skip kernel cond\figuration and continue with installation ซึ่งจะแสดงเมนูในการติดตั้งระบบโดยเลือกทำการติดตั้งระบบแบบมาตรฐานในเมนู Standard ซึ่งจะแสดงข้อความแจ้งให้เราทำการกำหนดโครงสร้าง Partition ที่เราใช้งานเมื่อเราทำการกำหนดขนาดของ Disk ที่เราจะใช้งานทั้งหมดแล้วให้เราเลือกรูปแบบการบูทแบบ Standard เพื่อให้ระบบทำการบูทเข้าสู่ฟรีบีเอสดีทันทีที่เปิดเครื่อง

จากนั้นโปรแกรมติดตั้งจะแสดงหน้าจอในการกำหนดการใช้งาน Disk โดยละเอียดอีกครั้งว่าต้องการใช้พื้นที่ใน mount point ส่วนไหนบ้าง เราสามารถกดปุ่ม A (Auto Default) เพื่อให้ระบบกำหนดและสร้าง mount point ให้อัตโนมัติ จากนั้นให้เราเลือกว่าจะทำการติดตั้งแพ็คเกจใดบ้าง

เมื่อเลือกแพ็คเกจต่างๆ เรียบร้อยแล้ว โปรแกรมจะแสดงหน้าจอให้เลือกว่าต้องการติดตั้งระบบจากสื่อชนิดใด เช่น CD/DVD, FTP, HTTP และ DOS Partition และให้เราตกลงทำการติดตั้ง

เมื่อโปรแกรมทำการติดตั้งแพ็คเกจต่างๆ เสร็จเรียบร้อยแล้ว จะแสดงข้อความให้เราทำการกำหนดค่าต่างๆ ให้กับเครือข่าย เช่น Network Card, ชื่อโฮสต์, ชื่อโดเมน, เกทเวย์ของเครือข่ายที่เรากำลังใช้งานอยู่, หมายเลขไอพีของ DNS Server ที่เครือข่ายเราใช้งานอยู่, ไอพีแอดเดรสที่เราจะกำหนดให้กับเครื่องของเรา

จากนั้นโปรแกรมจะให้เราทำการปรับแต่งค่า Console และค่าของ Time Zone แล้ว โปรแกรมจะให้เราเพิ่ม User Account และ Group ของระบบให้เราใส่รายละเอียดของ Group ที่เราต้องการใช้งาน แล้วจึงทำการสร้าง User Account ขึ้นเพื่อใช้งาน หลังจากที่เรากำหนด User Account แล้วโปรแกรมติดตั้งจะให้เรากำหนดรหัสผ่านของผู้ดูแลระบบ (root) เมื่อกำหนดรหัสผ่านแล้วให้เราออกจากโปรแกรมติดตั้งแล้ว ระบบจะทำการ Reboot เครื่องเป็นอันเสร็จสิ้นกระบวนการติดตั้งระบบปฏิบัติการฟรีบีเอสดี

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

การติดตั้งและใช้งานโปรแกรม IPFW

โปรแกรม IPFW โดยทั่วไปเป็นโปรแกรมไฟร์วอลล์ที่มีการติดตั้งมาพร้อมกับ ระบบปฏิบัติการฟรีบีเอสดี อยู่แล้ว ซึ่งเพื่อให้เรามั่นใจว่าเคอร์เนลที่เราใช้งานอยู่รองรับการทำงานของไฟร์วอลล์ สามารถตรวจสอบได้ในตอนที่เราทำการคอมไพล์เคอร์เนลมีการใช้ตัวเลือกไฟร์วอลล์หรือไม่ โดยทำการคัดลอกแฟ้มจาก /usr/src/sys/i386/conf/GENERIC และทำการสร้างแฟ้มแล้วใช้โปรแกรมอิดิเตอร์เพื่อแก้ไขข้อมูลดังนี้

Ident ***ชื่อแฟ้ม***(เช่น PSRU)

Options IPFIREWALL

Options IPFIREWALL_FORWARD

Options IPFIREWALL_DEFAULT_TO_ACCEPT

Options IPFIREWALL_VERBOSE

Options IPFIREWALL_VERBOSE_LIMIT=120

Options IPDIVERT

เมื่อแก้ไขแฟ้มเสร็จแล้วให้เราทำการคอมไพล์เคอร์เนลใหม่ให้กับระบบดังนี้

#config ***ชื่อแฟ้ม***

#cd ../compile/***ชื่อแฟ้ม***

#make depend;make;make install

เมื่อเราทำการคอมไพล์เคอร์เนลเสร็จเรียบร้อยแล้วให้เราทำการ reboot ระบบใหม่อีกครั้ง แล้วทำการตรวจสอบดูแฟ้ม /etc/rc.local ว่ามีคำสั่งด้านล่างนี้หรือไม่ หากยังไม่มีให้เราเพิ่มคำสั่งลงในแฟ้มนี้ แล้วทำการรีบูทระบบใหม่อีกครั้ง

Firewall_enable="YES"

Firewall_type="OPEN"

Firewall_quiet="YES"

เมื่อทำตามขั้นตอนต่างๆ เสร็จสิ้นแล้ว จะสามารถใช้งานโปรแกรม IPFW ได้ทันที

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

การติดตั้งโปรแกรม APACHE web server และ PHP

สำหรับผู้ที่ต้องการตัวติดตั้งโปรแกรมสามารถหาดาวน์โหลดได้ที่ http://www.php.net และ http://httpd.apache.org เมื่อทำการดาวน์โหลดตัวติดตั้ง Apache มาแล้วให้เริ่มทำการติดตั้งดังนี้

คลาย ZIP ไฟล์ httpd-2.X.XX.tar.gz ที่เราดาวน์โหลดมาโดยใช้คำสั่งจากโปรแกรม tar

```
#tar xzf httpd-2.X.XX.tar.gz
```

ให้ติดตั้ง Apache ที่ path /usr/local/apache2

```
#./configure –prefix=/usr/local/apache2 –enable-so
#make
#make install
```

เมื่อเสร็จสิ้นการติดตั้ง Apache เราสามารถ start / stop เว็บเซิร์ฟเวอร์ Apache ได้ด้วยคำสั่ง

```
#/usr/local/apache2/bin/apachectl start
#/usr/local/apache2/bin/apachectl stop
```

เมื่อทำการติดตั้งเว็บเซิร์ฟเวอร์ Apache แล้วสามารถติดตั้ง PHP ได้โดย เราจะต้องติดตั้งไลบรารีก่อน 2 ตัว ดังนี้

Libxml2 library จากเว็บไซต์ http://www.xmlsoft.org

Zlib library จากเว็บไซต์ http://www.gzip.org/zlib

ให้ทำการดาวน์โหลดและคลาย ZIP

```
#tar xzf zlib-1.X.X.tar.gz
#tar xzf libxml2-2.X.XX.tar.gz
```

ให้ติดตั้ง zlib ที่ /usr/local/lib

```
#cd zlib-1.X.X/
#./configure
#make
#make install
```

และติดตั้ง libxml2 ที่ /usr/local/lib เช่นเดียวกัน

```
#cd libxml2-2.X.XX
#./configure
#make
#make install
```

หลังจากนั้นให้ติดตั้ง PHP โดยคลาย ZIP ไฟล์ php-5.X.X.tar.bz2 ที่เราดาวน์โหลดมา

```
#tar xjf php-5.X.X.tar.bz2
```

ให้ติดตั้ง PHP ที่ /usr/lacal/php5

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่อนุญาตให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
#cd php-5.X.X
#./configure –prefix=/usr/local/php5 \
 --with-apxs2=/usr/local/apache2/bin/apxs \
 --with-libxml-dir=/usr/local/lib –with-zlib \
 --with-gd –enable-soap –enable-sockets \
 --with-jpeg-dir=/usr/ --enable-exif
#make
#make install
```

จากนั้นให้คัดลอกแฟ้ม php.ini-dist ไปที่ /usr/local/php5/lib/ และเปลี่ยนชื่อแฟ้มเป็น php.ini

```
#cp php.ini-dist /usr/local/php5/lib/php.ini
```

เมื่อติดตั้งเสร็จเรียบร้อยแล้วให้ทำการตั้งค่า PHP **ให้เว็บเซิร์ฟเวอร์** Apache **โดยเปิดแฟ้ม** /usr/local/apache2/conf/httpd.conf **แล้วแก้ไขหรือเพิ่มบรรทัดเหล่านี้**

```
LoadModule php5_module modules/lib/libphp5.so
DirectoryIndex.html index.htm index.php
AddType application/x-httpd-php .php .php3 .phtml
```

หลังจากแก้ไขเสร็จสิ้นแล้ว เราสามารถทดสอบระบบได้โดย
รีสตาร์ทเว็บเซิร์ฟเวอร์

```
#/usr/local/apache2/bin/apachectl stop
#/usr/local/apache2/bin/apachectl start
```

สร้างแฟ้ม php **ขึ้นโดยมีข้อมูลในแฟ้มดังนี้**

```
<?php phpinfo(); ?>
```

ตั้งชื่อว่า test.php **และเก็บที่** /usr/local/apache2/htdocs/

```
/usr/local/apache2/htdocs/test.php
```

ใช้โปรแกรมบราวเซอร์เปิดหน้าเว็บนี้ที่ url **ว่า** http://localhost/test.php **จะปรากฏหน้าเว็บแสดงข้อมูลของ** PHP **ที่ติดตั้งอยู่ในเครื่อง**

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

การติดตั้งโปรแกรมจัดการไอพีไฟร์วอลล์บนเว็บบราวเซอร์

เนื่องจากการใช้งานคำสั่งต่างๆ ในโปรแกรมไอพีไฟร์วอลล์นั้น เป็นคำสั่งที่มีผลต่อความปลอดภัยของระบบ จึงทำให้ผู้ใช้ทั่วไปไม่มีสิทธิ์ ในการใช้งานคำสั่งดังกล่าว ซึ่งการใช้งานโปรแกรมผ่านทางเว็บบราวเซอร์ถือเป็นการใช้งานผ่าน user ที่เป็น http และไม่สามารถใช้งานคำสั่งใรการจัดการไอพีไฟร์วอลล์ได้ จึงต้องมีการติดตั้งโปรแกรม Super User Do หรือ sudo เพื่อช่วยให้ผู้ใช้อื่นๆ สามารถใช้งานคำสั่งต่างๆ ได้เช่นเดียวกับผู้ดูแลระบบ

sudo (Super User do) เป็น Package ที่เราสามารถติดตั้งเพิ่มเติม เพื่อให้ user ทั่วไปมีสิทธิ์ในการใช้งานคำสั่งที่ root สามารถสั่งงานได้เช่น ipfw , adduser , rmuser และอื่น ๆ ครับ เพราะเนื่องจากโดยปรกติแล้ว user ทั่วไปจะไม่มีสิทธิ์ในการสั่งงานคำสั่งเหล่านี้

วิธีการติดตั้ง sudo

```
# cd /usr/ports/security/sudo
# make install
# reboot
```

(เพื่อให้ sudo ทำงานได้ในกรั๊งต่อๆ ไป)หรือหากไม่ต้องการ reboot ก็สามารถสั่ง rehash ได้เพื่อให้คำสั่งนั้น ๆ มีผลทันที

การปรับแต่ง sudo

sudo นั้นจะใช้ไฟล์ sudoers ในการปรับแต่งระบบครับว่าต้องการให้ใครสามารถใช้คำสั่งใดได้บ้าง ซึ่งไฟล์นี้จะถูกเก็บไว้ใน /usr/local/etc/ ในไฟล์นี้จะมีตัวอย่างของการใช้งาน ซึ่งเราสามารถอ่านและทำความเข้าใจได้ ยกตัวอย่างเช่น

```
www ALL=/sbin/ipfw
```

อธิบายได้ดังนี้

www คือ user ที่ชื่อ www

ALL คือ มาจาก ALL host

=/sbin/ipfw มีสิทธิ์ให้สามารถรันคำสั่ง ipfw ได้ (โดยปกติแล้ว user www จะไม่มีสิทธิ์ในการใช้งานคำสั่งนี้)

เมื่อทำการติดตั้งโปรแกรม sudo **แล้ว ให้แก้ไขแฟ้ม /usr/local/etc/sudoers โดยเพิ่มข้อความดังนี้**

```
Cmnd_Alias      CMD=/sbin/ipfw, /sbin/chmod, /bin/sh
www     ALL=NOPASSWORD:CMD
```

เมื่อแก้ไขแฟ้มแล้วให้คัดลอกแฟ้มโปรแกรมทั้งหมดไปที่ /usr/local/apache2/htdocs/ แล้วทำการรีบูทระบบอีกครั้ง ก็จะสามารถใช้งานโปรแกรมได้

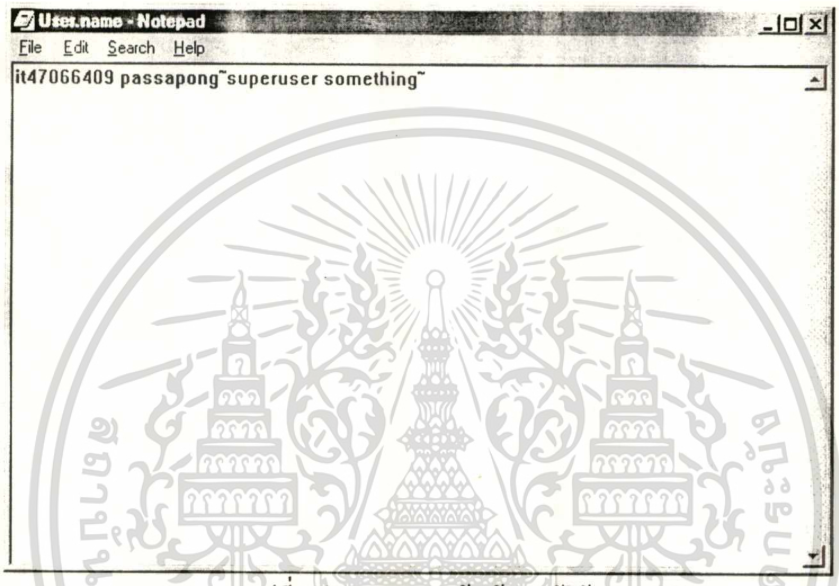
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ภาคผนวก ข.

คู่มือการใช้งานโปรแกรม

ในการใช้งานโปรแกรม

เริ่มการใช้งานโปรแกรมจากการล็อกอินโดยผู้ใช้ต้องเปิดโปรแกรมจากแฟ้ม FrmUserLogin.php แล้วทำการใส่ username และ password ซึ่งจะมีการเก็บข้อมูลไว้เป็นแฟ้มเอกสาร ที่จะมีการตั้งค่าสิทธิ์ของผู้ใช้เป็น 600 คือผู้ที่ไม่ได้เข้าสู่ระบบเป็นรูท จะไม่สามารถอ่านหรือเขียนแฟ้มนี้ได้



รูปที่ 1 ลักษณะของแฟ้มข้อมูลผู้ใช้

รูปที่ 2 หน้าจอในการล็อกอินเข้าใช้งานโปรแกรม

เมื่อผู้ใช้ทำการล็อกอินเข้าสู่ระบบแล้ว โปรแกรมจะแสดงหน้าจอในการใช้งานหลัก โดยแบ่งออกเป็นเมนูต่างๆ ดังนี้

1. เมนูในการแสดงข้อมูลต่างๆ ซึ่งจะแบ่งออกเป็นเมนูย่อยๆ 3 เมนู คือ
   - เมนูในการแสดงรายการกฎที่ใช้งานอยู่ ซึ่งจะสามารถทำการ โหลดหรือเซฟข้อมูลกฎลงเป็นแฟ้มข้อมูลได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

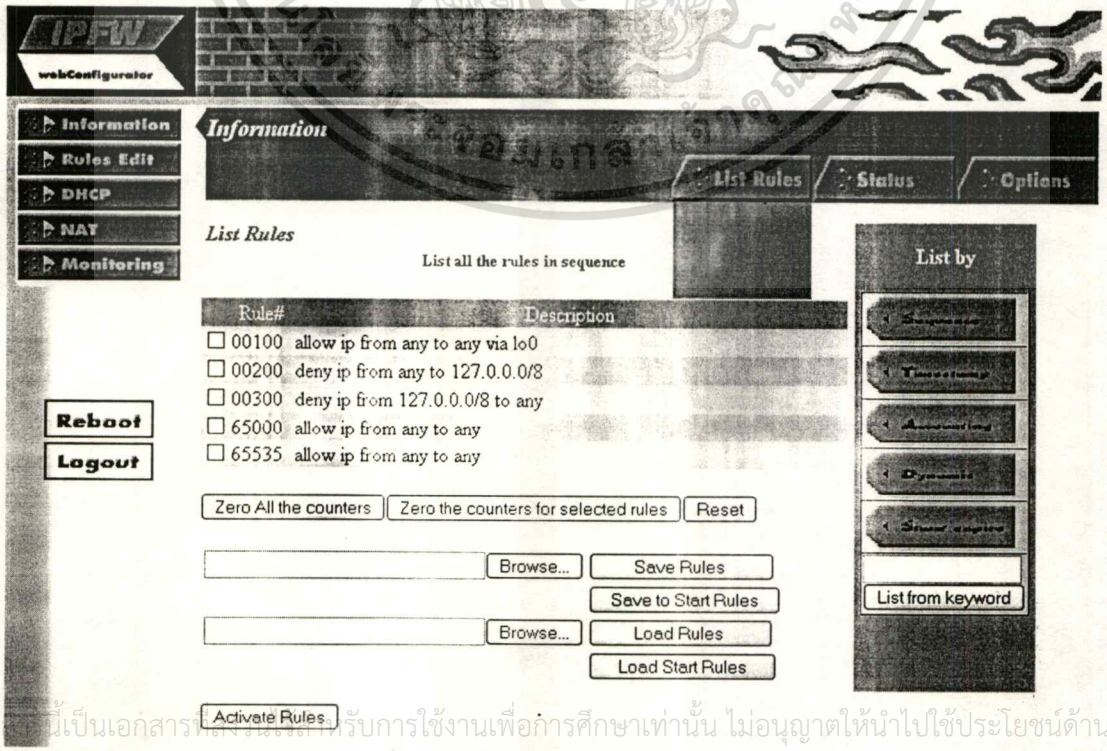
- เมนูในการแสดงข้อมูลต่างๆ เกี่ยวกับสถานะของระบบ
- เมนูในการปรับแต่งกฎเบื้องต้น

2. เมนูในการจัดการเกี่ยวกับกฎ ซึ่งจะมีเมนูย่อย 3 เมนู คือ
   - เมนูในการวิเคราะห์ข้อมูลกฎ ซึ่งสามารถทำการแก้ไขกฎที่เกิด anomaly ได้
   - เมนูในการเพิ่มกฎ หรือทำการสร้างกฎใหม่
   - เมนูในการลบกฎที่มีอยู่เดิมออก
3. เมนูในการจัดการเกี่ยวกับค่าต่างๆ ของ DHCP
4. เมนูในการจัดการเกี่ยวกับค่าต่างๆ ของ NAT
5. เมนูในการดูข้อมูล log ต่างๆ

เมื่อผู้ใช้ต้องการออกจากโปรแกรม หรือต้องการให้การปรับแต่งค่าต่างๆ บางอย่างมีผลใช้งานสามรถเลือกที่ด้านซ้ายล่างของหน้าจอโปรแกรมเพื่อทำการ รีบูท หรือออกจากโปรแกรมได้

รูปที่ 3 การรีบูทระบบและออกจากโปรแกรม

ในการใช้งานเมนูแรก คือส่วนของการแสดงข้อมูลต่างๆ ผู้ใช้สามารถเลือกลักษณะในการแสดงข้อมูลกฎได้จากปุ่มทางด้านขวาโดยจะมีการแสดงรายการกฎรูปแบบต่างๆ ดังนี้



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

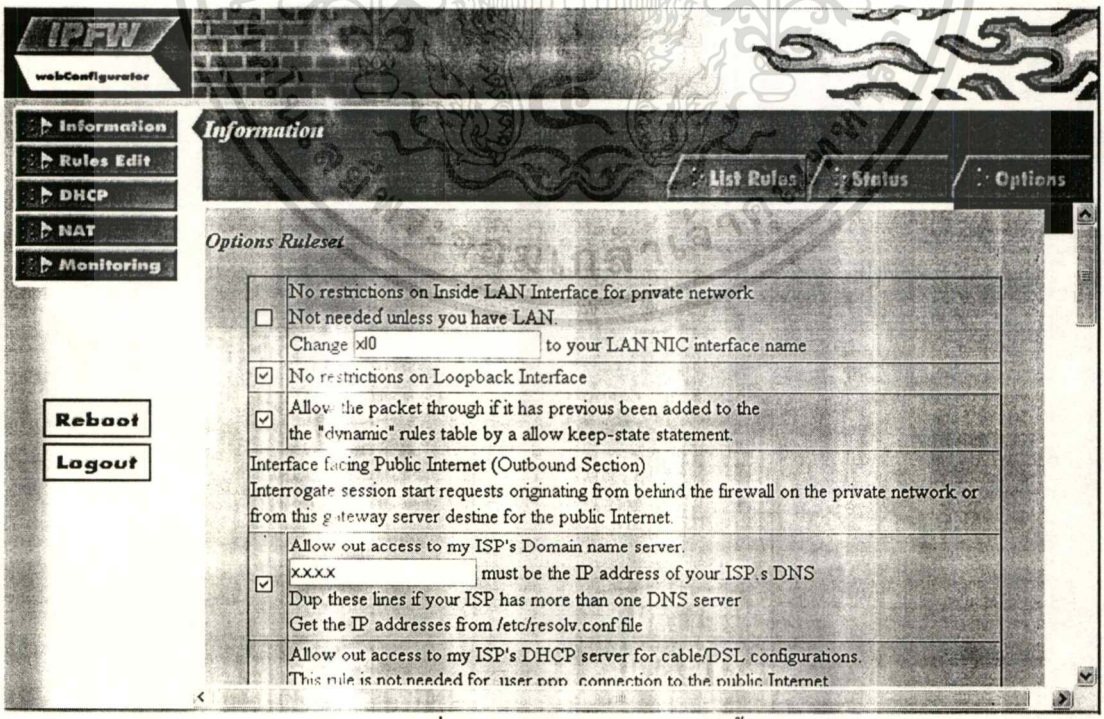
รูปที่ 4 การใช้งานและแสดงรูปกฎในรูปแบบต่างๆ

- Sequence แสดงกฎทั้งหมดตามลำดับหมายเลย
- Timestamp แสดงกฎทั้งหมดและเวลาที่มีการใช้กฎล่าสุด
- Accounting แสดงข้อมูลการใช้งานกฎ
- Dynamic แสดงกฎชนิด dynamic ที่เพิ่มลงในกฎที่ใช้
- Show expire แสดงกฎรวมทั้งกฎที่หมดอายุแล้ว
- List from keyword แสดงรายการกฎตาม keyword เช่น ดูกฎที่มีการ allow เป็นต้น

การลบค่าตัวนับแพ็คเก็ตของกฎที่ถูกใช้ไปทำได้โดย เลือกกฎจากช่องด้านหน้าหมายเลขลำดับกฎ แล้วกดที่ปุ่ม Zero the counters for selected rules หรือถ้าต้องการลบตัวนับแพ็คเก็ตทั้งหมดให้เลือกที่ปุ่ม Zero All the counters แทน

ในการจัดการเกี่ยวกับแฟ้มกฎ ผู้ใช้สามารถทำการบันทึกแฟ้ม และโหลดข้อมูลจากแฟ้มกฎได้ โดยเลือกที่ปุ่ม Browse เพื่อเลือกแฟ้มที่ต้องการและกดที่ปุ่ม Save Rules หรือ Load Rules ซึ่งกฎที่ถูกโหลดจากหน้าจอนี้จะถูกนำมาแสดงผลแต่จะยังไม่ถูกใช้งานจนกระทั่งผู้ใช้ เลือกที่ปุ่ม Activate Rules จากนั้นกฎที่โหลดมานั้นจะถูกนำไปใช้แทนที่กฎเดิม และถ้าต้องการโหลดกฎที่เป็นค่าเริ่มต้นในการบูทระบบ สามารถทำได้โดยเลือกที่ปุ่ม Load Start Rules โปรแกรมจะทำการโหลดให้กฎเริ่มต้นถูกใช้งานทันที และยังสามารถนำกฎที่สร้างขึ้นเองตั้งค่าให้เป็นกฎเริ่มต้นได้ โดยเลือกแฟ้มข้อมูลและทำการกดปุ่ม Save to Start Rules แล้วโปรแกรมจะทำการบันทึกให้กฎนั้นเป็นกฎเริ่มต้น

ในส่วนการปรับแต่งค่ากฎเบื้องต้น โปรแกรมจะแสดงรายการข้อมูลแพ็คที่ที่มีผลกับกฎให้ผู้ใช้ทราบดังนี้

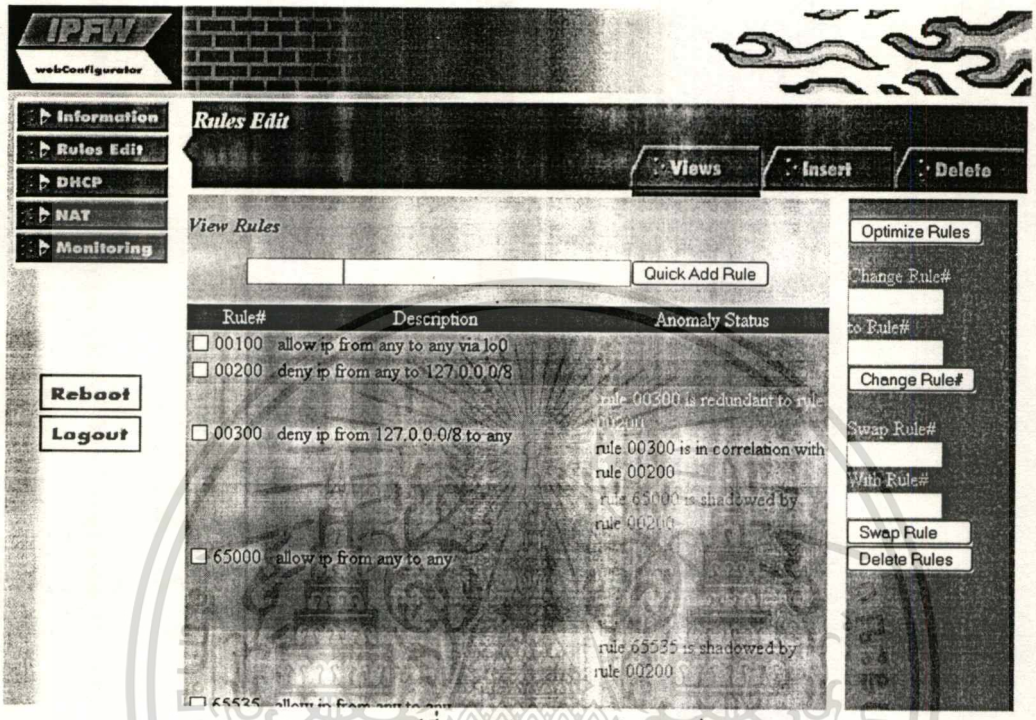


รูปที่ 5 การใช้งานปรับแต่งค่ากฎเบื้องต้น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

การปรับแต่งค่ากฎ ให้ผู้ใช้ทำการเลือกว่าต้องการให้กฎยอมรับหรือแพ็คเก็ตชนิดใดบ้าง โดยเลือกที่ช่องด้านหน้า แล้วให้กดปุ่ม Submit โปรแกรมจะทำการโหลดกฎที่ได้ตั้งค่าเอาไว้ลงในโปรแกรมไอพีไฟร์วอลล์

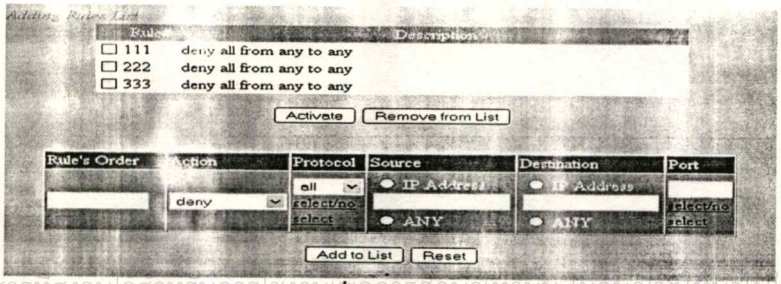
เมนูในการจัดการเกี่ยวกับกฎ จะแบ่งออกเป็น การจัดการและวิเคราะห์กฎซึ่งจะมีหน้าจอดังนี้



รูปที่ 6 การจัดการและวิเคราะห์กฎ

ผู้ใช้สามารถวิเคราะห์กฎเพื่อหา anomaly ได้โดยการเลือกที่ปุ่ม Analyse บนหน้าจอด้านขวา เมื่อโปรแกรมทำการวิเคราะห์แล้วจะแสดงสถานะของกฎ ว่ามี anomaly เกิดขึ้นหรือไม่ และเป็น anomaly ชนิดใดบ้าง ซึ่งผู้ใช้สามารถจัดการกับกฎที่เกิด anomaly ได้ คือ ทำการเปลี่ยนเลขลำดับกฎหรือสลับข้อกฎ ด้วยเมนูด้านขวา ซึ่งผู้ใช้จะต้องกรอกหมายเลขของกฎที่ต้องการแก้ไข แต่จะไม่สามารถเปลี่ยนเลขลำดับซ้ำกับกฎเดิมที่มีอยู่ได้ โดยวิธีนี้สามารถใช้แก้ไข Shadow anomaly และ Generalization anomaly ได้ หรือทำการแก้ไขกฎ ด้วยช่องแสดงผลด้านบนและกดที่ Quick Add Rule โดยกฎที่ถูกแก้ไขนี้จะถูกเขียนทับกฎเดิมที่มีอยู่ เพื่อแก้ Correlation anomaly หรือทำการลบกฎโดยเลือกกฎที่ต้องการลบที่ช่องด้านหน้าหมายเลขกฎ แล้วกดที่ปุ่ม Delete Rules เพื่อแก้ Redundancy anomaly เป็นต้น

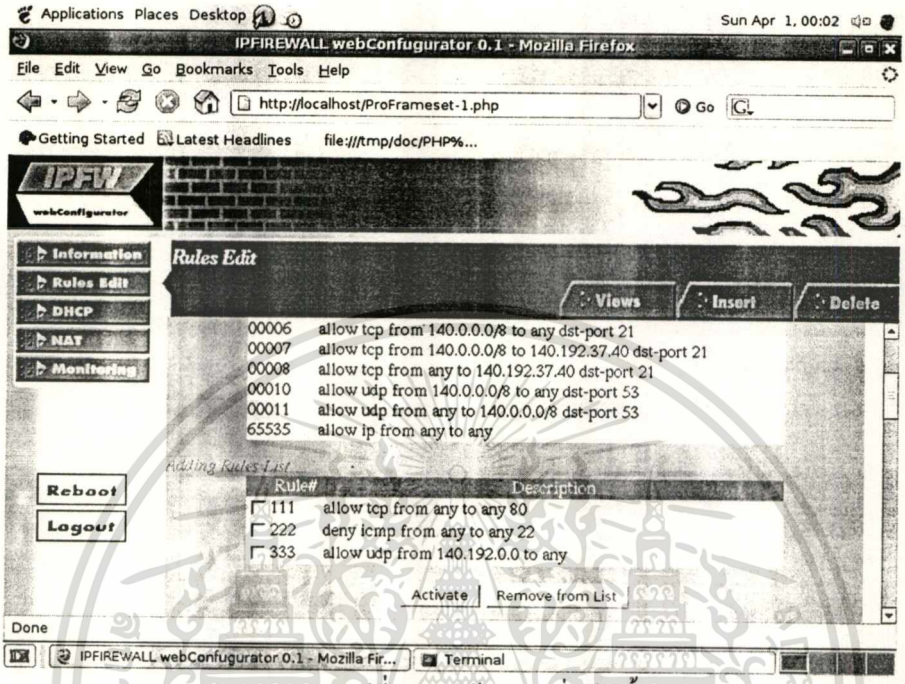
ในส่วนของการเพิ่มกฎ ผู้ใช้สามารถสร้างกฎได้จากตัวเลือกในเมนู



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

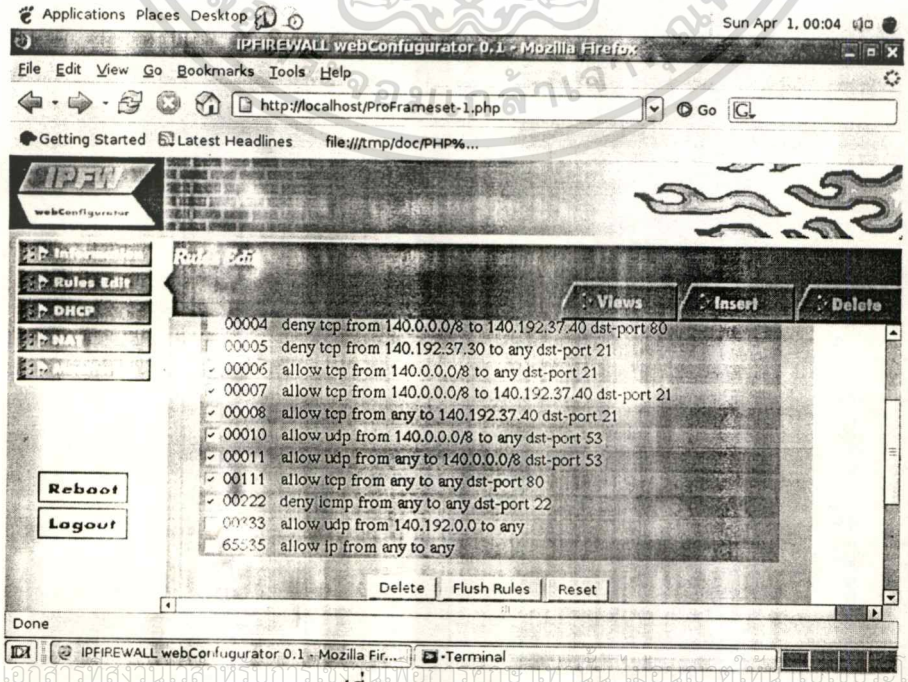
รูปที่ 7 การสร้างและเพิ่มกฎ

ผู้ใช้สามารถสร้างกฎขึ้นได้ เมื่อใส่ข้อมูลครบแล้วให้ทำการเพิ่มกฎ โดยเลือกที่ปุ่ม Add to List โดยกฎที่ถูกสร้างนั้นจะ ถูกนำมาเพิ่มไว้ใน List ด้านบนก่อน และสามารถลบออกจาก List ได้โดยเลือกกฎแล้วกดที่ปุ่ม Remove from List เมื่อผู้ใช้ต้องการใช้งานกฎที่อยู่ใน List ให้กดที่ปุ่ม Activate แล้วกฎที่อยู่ใน List จะมีผลใช้งานทันที



รูปที่ 8 การใช้งานกฎที่สร้างขึ้น

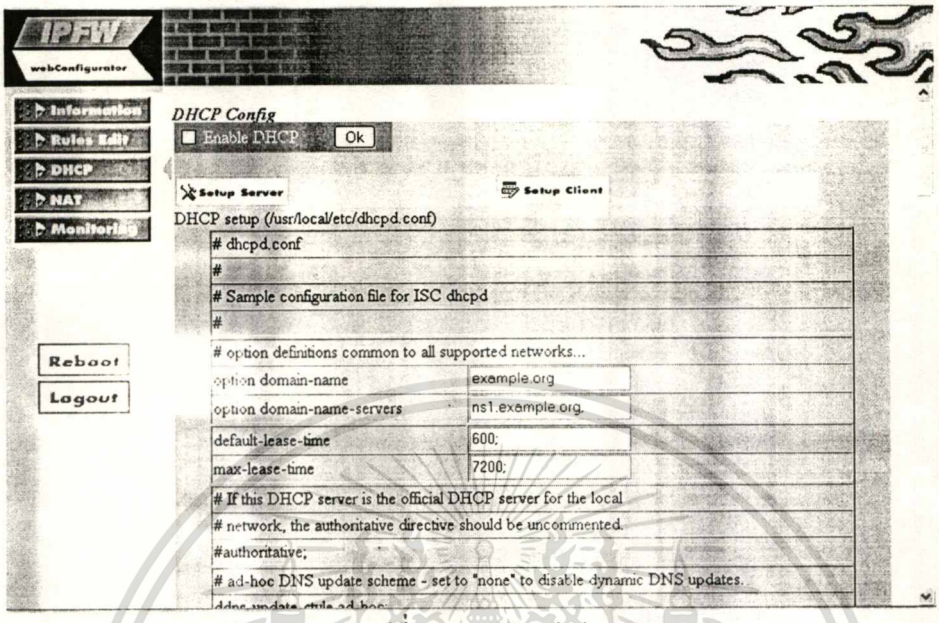
ในส่วนเมนูของการลบกฎ โปรแกรมจะแสดงข้อมูลของกฎที่ถูกใช้งานอยู่ทั้งหมด แล้วให้ผู้ใช้ทำการเลือกกฎที่ต้องการลบที่ช่องด้านหน้าหมายเลขกฎ และกดที่ปุ่ม Delete Rules เพื่อทำการลบกฎที่ถูกเลือกหรือถ้าต้องการลบกฎทั้งหมดให้เลือกที่ FlushRule โปรแกรมจะทำการลบกฎทั้งหมดออก



รูปที่ 9 การลบกฎออกจากโปรแกรม

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

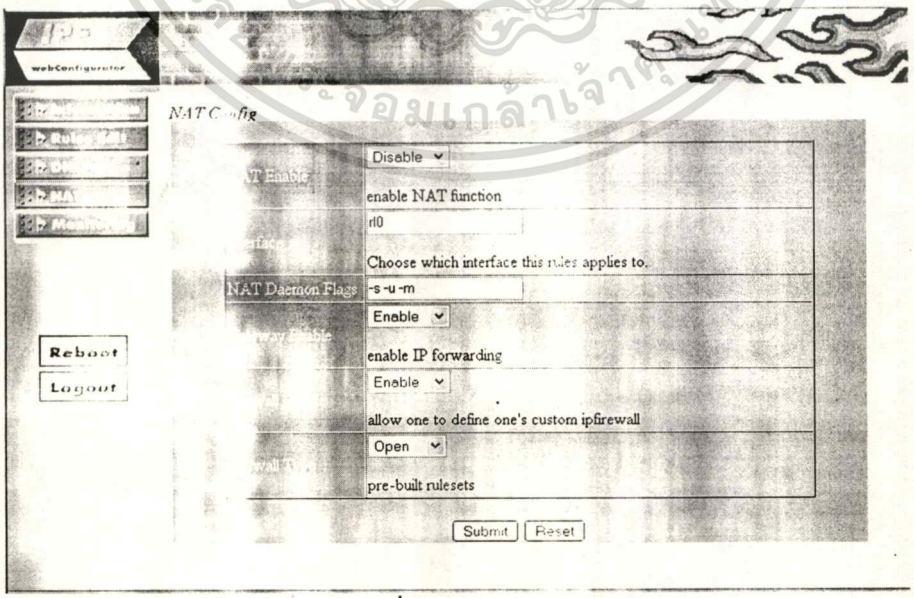
ในส่วนเมนูในการแก้ไขข้อมูลต่างๆ เกี่ยวกับ DHCP จะแบ่งออกเป็นการปรับแต่งค่าของ เซิร์ฟเวอร์ และไคลเอ็นท์โดยจะเป็นการแก้ไขแฟ้มข้อมูล /usr/local/etc/dhcpd.conf และ /usr/local/etc/dhclient.conf



รูปที่ 10 การปรับแต่งค่า DHCP

เมื่อผู้ใช้ทำการปรับแต่งค่าต่างๆ แล้ว ให้ผู้ใช้กดที่ปุ่ม Submit เพื่อทำการบันทึกการแก้ไข ซึ่งจะมีผลใช้งานหลังจากที่ผู้ใช้ทำการรีบูทระบบใหม่อีกครั้งหนึ่ง

เมนูในส่วนของการปรับแต่งค่า NAT จะแสดงข้อมูลการใช้งาน เช่นการปิด-เปิด NAT และไฟร์วอลล์ การเลือกชนิดของไฟร์วอลล์ และอินเตอร์เฟสที่ใช้ เมื่อทำการปรับแต่งค่าแล้วให้กด Submit เพื่อทำการบันทึกการแก้ไข ซึ่งจะมีผลใช้งานหลังจากที่ผู้ใช้ทำการรีบูทระบบใหม่ เช่นกัน



รูปที่ 11 การปรับแต่งค่า NAT

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ประวัติผู้เขียน

นายภาสพงศ์ ทักษิณา เกิดเมื่อวันที่ 18 กุมภาพันธ์ พ.ศ. 2525 ที่จังหวัดฉะเชิงเทรา สำเร็จการศึกษาปริญญาตรีวิทยาศาสตรบัณฑิต สาขาวิทยาการคอมพิวเตอร์ จากภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ มหาวิทยาลัยบูรพา ในปีการศึกษา 2547 และเข้าศึกษาต่อในระดับปริญญาโท หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาเทคโนโลยีสารสนเทศ ภาควิชาเทคโนโลยีสารสนเทศ คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้