

ระบบไฟร์วอลล์แบบฝังตัว

EMBEDDED FIREWALL SYSTEM



เลขหมู่.....
เลขทะเบียน.....04789
วัน,เดือน,ปี ๒๕๕๑

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรบัณฑิต
สาขาวิชาเทคโนโลยีสารสนเทศ
คณะเทคโนโลยีสารสนเทศ
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับ.....
ภาคเรียนที่ 2 ปีการศึกษา 2550
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ib.....
i.....

EMBEDDED FIREWALL SYSTEM



**A PROJECT SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENT FOR THE DEGREE OF
BACHELOR OF SCIENCE PROGRAM IN INFORMATION TECHNOLOGY
FACULTY OF INFORMATION TECHNOLOGY
KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG**

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



COPYRIGHT 2008

FACULTY OF INFORMATION TECHNOLOGY

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

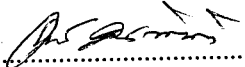
ใบรับรองปริญญาโท ประจำปีการศึกษา 2550
คณะเทคโนโลยีสารสนเทศ
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

เรื่อง ระบบไฟร์วอลล์แบบฝังตัว

EMBEDDED FIREWALL SYSTEM

ผู้จัดทำ

1. นางสาวสุพร รอดจากภัย รหัสประจำตัว 47070076
2. นายฉันทวัฒน์ โพธิ์ชัยทอง รหัสประจำตัว 47070111
3. นายปวิณวัชร วัฒนโมษิต รหัสประจำตัว 47070120


..... อาจารย์ที่ปรึกษา
(ผศ. อัครินทร์ คุณกิตติ)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

หัวข้อ	ระบบไฟร์วอลล์แบบฝังตัว : เดมอนการ์ด
นักศึกษา	นางสาวสุพร รอดจากภัย รหัสนักศึกษา 47070076 นายฉันทวัฒน์ โพธิ์ชัยทอง รหัสนักศึกษา 47070111 นายปวิณวัชร วัฒน โฆมิต รหัสนักศึกษา 47070120
ปริญญา	วิทยาศาสตรบัณฑิต
สาขาวิชา	เทคโนโลยีสารสนเทศ
ปีการศึกษา	2550
อาจารย์ที่ปรึกษา	ผศ.อัครินทร์ คุณกิตติ

บทคัดย่อ

เนื่องจากไฟร์วอลล์ในอุปกรณ์เน็ตเวิร์กที่มีใช้อยู่ในปัจจุบันนั้นมีราคาค่อนข้างที่จะสูง ซึ่งถ้าผู้ใช้นั้นต้องการจะนำอุปกรณ์ไฟร์วอลล์ไปใช้ในหน่วยงานขนาดเล็กหรือบ้านพักอาศัย ก็ทำให้ไม่สามารถที่จะมีกำลังซื้อไปใช้ได้ อันเนื่องมาจากราคาที่สูงของอุปกรณ์เหล่านี้นั่นเอง โครงการนี้จึงคิดที่จะพัฒนาอุปกรณ์ทางด้านเน็ตเวิร์กที่มีคุณภาพใกล้เคียงกัน แต่มีราคาต้นทุนที่ถูกกว่า เพื่อใช้สำหรับใช้งานในบ้านหรือสำนักงานขนาดเล็กได้ อีกทั้งระบบนั้นจะมีความเสถียรอันเนื่องมาจากมีการใช้หลักการของการทำระบบฝังตัวขึ้นมา ทำให้ไม่มีโปรเซสอื่นมารบกวนการทำงานและทำให้อุปกรณ์รันได้ต่อเนื่องตลอดเวลาและปิดเครื่องได้โดยไม่ต้องชัตดาวน์ อีกทั้งยังมีส่วนของคอมมานไลน์อินเตอร์เฟซ ที่จะช่วยให้การกำหนดค่าต่างๆของระบบนั้นง่ายและสะดวกรวดเร็วยิ่งขึ้น รวมไปถึงการพัฒนาในส่วนของเว็บอินเตอร์เฟซซึ่งจะสามารถทำการแก้ไขค่าได้ผ่านเว็บอินเตอร์เฟซในส่วนของการพัฒนาระบบมุ่งเน้นการใช้ระบบยูนิกซ์ ในที่นี้คือระบบปฏิบัติการฟรีบีเอสดี รุ่น 6.2 ซึ่งมีความเสถียรภาพสูง โดยทำการออกแบบส่วนติดต่อผู้ใช้เพิ่มเติมสองส่วนคือ ส่วนติดต่อคอมมานด์ไลน์พัฒนาโดยใช้ ซีเชลล์และบอร์นเชลล์ ส่วนติดต่อผ่านเว็บพัฒนาโดยใช้ภาษาพีเอชพี และไลททีพีดีเว็บเซิร์ฟเวอร์ ผลที่ได้คือระบบไฟร์วอลล์ที่มีขนาดเล็ก ประสิทธิภาพดี สามารถใช้งานได้จริง และเข้าใจวิธีการใช้งานได้ง่าย

Thesis Title	Embedded Firewall System : Daemon Guard	
Student	Ms. Suporn Rodjakpai	Student ID. 47070076
	Mr. Chantawat Pochaitong	Student ID. 47070111
	Mr. Paweenwach Wattanakosit	Student ID. 47070120
Degree	Bachelor of Science	
Programme	Information Technology	
Academic Year	2007	
Advisor	Asst.Prof. Akharin Khunkitti	

ABSTRACT

In the present , Network firewall tool has high cost, that users need to use taking firewall in the home or small institute , We can't buy it due to cost. Then this project will develop network tool that it has nearby quality. But It has lower cost for using in home or small institute. Embedded Firewall System will have stably due to use Embedded theory, so other process can't disturb, the tool can run all the time and can power-off without shutdown. By developing command line interface to use easily and quick command than the old one and developing web interface, it make us can order pass by web interface. The embedded firewall has three parts of development, the implement system is Unix name FreeBSD 6.2 that is stability, new command line interface develop by C shell and Bourne shell, new web interface develop by PHP and Lighttpd web server. Summarize all development is a small firewall system which efficiency, be usable and be easy understand.

กิตติกรรมประกาศ

โครงการพัฒนาระบบงานนี้เกิดขึ้น และสำเร็จลุล่วงไปได้ด้วยดี คณะผู้จัดทำโครงการ ขอขอบพระคุณ ผู้ช่วยศาสตราจารย์ อัครินทร์ คุณกิตติ ซึ่งเป็นอาจารย์ที่ปรึกษาโครงการที่ได้กรุณาเสียสละเวลาอันมีค่าในการให้คำแนะนำ แนวคิดในการจัดทำโครงการ และให้คำปรึกษาด้านวิชาการที่เป็นประโยชน์ในการทำโครงการและให้ความช่วยเหลือด้านอื่นๆ ทั้งสถานที่ทำโครงการ ด้านเครื่องมือและอุปกรณ์ในการจัดทำโครงการ ด้านการแก้ไขเอกสาร เรียบเรียงเอกสารรวมทั้งได้รับการดูแลเอาใจใส่ ให้ความเมตตา และให้กำลังใจแก่ผู้จัดทำด้วยดีเสมอมา คณะผู้จัดทำมีความซาบซึ้งในความกรุณาเป็นอย่างยิ่ง จึงขอกราบขอบพระคุณเป็นอย่างสูงไว้ ณ โอกาสนี้

ขอกราบขอบพระคุณ คุณพ่อ คุณแม่ ที่ให้กำเนิด ให้การศึกษา ให้กำลังใจและเป็นแรงผลักดันให้คณะผู้จัดทำมีกำลังใจที่จะมุ่งมั่นในการศึกษาครั้งนี้จนเป็นผลสำเร็จลุล่วงด้วยดี

สุดท้ายขอขอบคุณ คุณชำนาญ ฉลาดแพทย์ และคุณชาตรี ชะโลธร ที่ได้ให้คำแนะนำ เสนอแนะในการเขียน โปรแกรม การจัดทำเอกสาร การทำอุปกรณ์ไฟร์วอลล์ให้ประสบผลสำเร็จ

ฉันทวัฒน์ โพธิ์ชัยทอง
ปวีณวัชร วัฒนโฆษิต
สุพร รอดจากภัย

สารบัญ

บทคัดย่อ	หน้า
บทคัดย่อภาษาอังกฤษ	I
กิตติกรรมประกาศ	II
สารบัญ	III
สารบัญตาราง	IV
สารบัญรูป	VII
สารบัญรูป	VIII
บทที่ 1 บทนำ	VIII
1.1 ความเป็นมาและความสำคัญของปัญหา	1
1.2 ความมุ่งหมายและวัตถุประสงค์ของการศึกษา	1
1.3 สมมติฐานของการศึกษา	1
1.4 ทฤษฎีหรือแนวคิดที่ใช้ในการวิจัย	2
1.5 ขอบเขตของการวิจัย	2
1.6 ขั้นตอนของการศึกษา	2
1.6 ขั้นตอนของการศึกษา	3
บทที่ 2 ทฤษฎีและหลักการที่ใช้ในการพัฒนาระบบไฟร์วอลล์แบบฝังตัว	4
2.1 หลักการทำงานไฟร์วอลล์แบบแพ็คเกจไฟวอร์ริ่งไฟร์วอลล์	4
2.1.1 หลักการในการสร้างกฎของไฟร์วอลล์	4
2.1.2 ลำดับของกฎของไฟร์วอลล์	5
2.1.3 การกรอง TCP/IP	5
2.1.4 คำแนะนำอื่นๆ สำหรับการสร้าง กฎ ของไฟร์วอลล์	5
2.1.5 การเก็บข้อมูลล็อกและตรวจสอบจุดบกพร่อง	10
2.1.6 การกำหนดรูปแบบ Syntax ของกฎที่ใช้ในการปิดกั้น packet	11
2.2 ระบบแบบฝังตัว	12
2.3 เซลล์	12
2.3.1 หลักการทำงานของเซลล์	13
2.3.2 ประเภทของเซลล์	13
2.4 Tool ที่ใช้	13
2.4 Tool ที่ใช้	14

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญ (ต่อ)

	หน้า
2.4.1 ไลท์ทีพีดี	14
2.4.2 อีดิทพลัส	14
2.4.3 พีเอสพี	14
2.5 การเซตค่าต่างๆของกฎการทำงานในไฟร์วอลล์.....	16
2.5.1 การเซตค่าอินเทอร์เน็ตเฟส โดยแบ่งออกเป็น	16
2.5.2 การเซตค่าโปรโตคอลที่ใช้ในการติดต่อสื่อสาร	16
2.5.3 การกำหนดค่าแอดเดรสต้นทางและปลายทาง	26
2.5.4 การเซตค่าพอร์ต	28
บทที่ 3 วิเคราะห์และออกแบบระบบ	30
3.1 ขั้นตอนการวิเคราะห์และออกแบบระบบปฏิบัติการ	30
3.2 ขั้นตอนการออกแบบคอมมานไลน์	32
3.2.1 แผนภาพอธิบายลำดับการทำงานของสคริปต์ไฟล์	35
3.3 ขั้นตอนการออกแบบเว็บอินเทอร์เน็ตเฟส	65
3.3.1 การออกแบบฟังก์ชันการทำงาน	66
3.3.2 ฟังก์ชันเกี่ยวกับอินเทอร์เน็ตเฟส	68
บทที่ 4 การพัฒนาโปรแกรมในส่วนต่างๆของระบบ.....	87
4.1 การแสดงผลการทำงานของคอมมานไลน์อินเทอร์เน็ตเฟส	87
4.1.1 แสดงหน้า main.csh.....	87
4.1.2 แสดงหน้า firewall_rule.csh.....	87
4.1.3 แสดงหน้า create.csh.....	88
4.1.4 แสดงหน้า enable.csh	88
4.1.5 แสดงการตั้งค่าไอพี(IP) ให้กับอินเทอร์เน็ตเฟส (interface) ต่างๆ	89
4.1.6 แสดงค่าของไอพี(IP) ที่ทำการตั้งค่าไว้.....	89
4.1.7 แสดงหน้าการรีบูท (reboot) ระบบ.....	90
4.1.8 แสดงหน้าการจัดการเว็บอินเทอร์เน็ตเฟส	90
4.1.9 แสดงหน้า startup.csh.....	91
4.2 การแสดงผลการทำงานของเว็บอินเทอร์เน็ตเฟส.....	91

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญ (ต่อ)

	หน้า
บทที่ 5 สรุปผลการวิจัย และข้อเสนอแนะ	96
5.1 สรุปผลการวิจัย.....	96
5.1.1 ข้อจำกัดของระบบ.....	96
5.2 ปัญหาที่ได้อพบในการทำงาน	96
5.3 สรุปแนวทางในการพัฒนาในอนาคต.....	99
บรรณานุกรม	100
ภาคผนวก ก	101
ภาคผนวก ข	132
ภาคผนวก ค	133
ภาคผนวก ง.....	141



สารบัญตาราง

ตารางที่	หน้า
2.1 แสดง TCP/UDP service ที่ควรปิดกั้นที่ไฟร์วอลล์.....	6
2.2 แสดง TCP/UDP service ที่ควรปิดกั้นไม่ให้เข้ามาจากภายนอก	8
2.3 แสดง TCP/UDP service ที่อาจเปิดให้บริการใน DMZ.....	8
2.4 แสดง ICMP message ที่ควรอนุญาตให้ออกไปจากเครือข่ายภายในได้.....	9
2.5 แสดง ICMP message ที่ควรอนุญาตให้เข้ามายังเครือข่ายภายในได้.....	9
2.6 แสดงชนิดของแพ็กจ์.....	23
2.7 แสดงหมายเลขแอดเดรส	27
2.8 แสดงเน็ตเวิร์คแอดเดรสและเน็ตมาร์กของแต่ละเครือข่าย.....	27
3.1 แสดงคำอธิบายการเข้าใช้ระบบ.....	48
3.2 แสดงคำอธิบายการสร้างกฎใหม่.....	49
3.3 แสดงคำอธิบายการแก้ไขกฎในระบบ.....	50
3.4 แสดงคำอธิบายการลบกฎในระบบ.....	51
3.5 แสดงคำอธิบายการแสดงกฎที่มีในระบบ.....	52
3.6 แสดงคำอธิบายการให้กฎทำงาน.....	53
3.7 แสดงคำอธิบายการเข้าใช้ระบบ.....	70
3.8 แสดงคำอธิบายการสร้างกฎใหม่.....	71
3.9 แสดงคำอธิบายการแก้ไขกฎในระบบ.....	72
3.10 แสดงคำอธิบายการลบกฎในระบบ.....	73
3.11 แสดงคำอธิบายการแสดงกฎที่มีในระบบ.....	74
3.12 แสดงคำอธิบายการแสดงสถานะของกฎ.....	75
3.13 แสดงคำอธิบายการเริ่มระบบใหม่.....	76
3.14 แสดงคำอธิบายการแสดงผลหมายเลขไอพี.....	77

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญรูป

รูปที่	หน้า
2.1 แสดงความสัมพันธ์กันระหว่างเซลล์ เคอร์เนล และชุดคำสั่งของผู้ใช้	13
2.2 ขั้นตอนการเอนแคปซูเรชั่น และดีเม้าท์ไบท์เลขซึ่ง	17
2.3 โครงสร้าง ทีซีพี/ไบท	18
2.4 ส่วนหัวของไบท์	19
2.5 ส่วนหัวของไอซีเอ็มพี	21
2.6 ส่วนหัวของ ยูดีพี	22
2.7 ส่วนหัวของทีซีพี	23
2.8 แสดงลำดับขั้นตอนการส่งทีซีพีเซกเมนต์และการเชื่อมต่อระหว่างซ็อกเก็ตคู่เดียวกัน	24
2.9 แสดงเหตุการณ์ที่แพ็กเก็ตทีพีดียู	26
3.2 แสดงแผนภาพสถาปัตยกรรมของระบบ	32
3.4 แผนภาพแสดงลำดับการทำงานของสคริปต์ main.csh	35
3.5 แผนภาพแสดงลำดับการทำงานของสคริปต์ web_config.csh	36
3.6 แผนภาพแสดงลำดับการทำงานของสคริปต์ web_enable.csh	36
3.7 แผนภาพแสดงลำดับการทำงานของสคริปต์ web_disable.csh	37
3.8 แผนภาพแสดงลำดับการทำงานของสคริปต์ reboot.csh	37
3.9 แผนภาพแสดงลำดับการทำงานของสคริปต์ system_config.csh	38
3.10 แผนภาพแสดงลำดับการทำงานของสคริปต์ show_ip.csh	38
3.11 แผนภาพแสดงลำดับการทำงานของสคริปต์ ip_config.csh	39
3.12 แผนภาพแสดงลำดับการทำงานของสคริปต์ firewall_rule.csh	40
3.13 แผนภาพแสดงลำดับการทำงานของสคริปต์ create.csh	41
3.14 แผนภาพแสดงลำดับการทำงานของสคริปต์ create_wizard.csh	43
3.15 แผนภาพแสดงลำดับการทำงานของสคริปต์ edit.csh	43
3.16 แผนภาพแสดงลำดับการทำงานของสคริปต์ enable_rule.csh	44
3.17 แผนภาพแสดงลำดับการทำงานของสคริปต์ show_rule.csh	44
3.18 แผนภาพแสดงลำดับการทำงานของสคริปต์ disable_rule.csh	45
3.19 แผนภาพแสดงลำดับการทำงานของสคริปต์ enable_pf.csh	45
3.20 แผนภาพแสดงลำดับการทำงานของสคริปต์ disable_pf.csh	46
3.21 แผนภาพแสดงคุณสมบัติการทำงานของระบบกับผู้ใช้	47

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญรูป (ต่อ)

รูปที่	หน้า
3.22 แผนภาพแสดงคลาสที่มีในระบบ	54
3.23 แผนภาพแสดงลำดับการทำงานของการทำงานของการเข้าใช้งานระบบ	55
3.24 แผนภาพแสดงลำดับการทำงานของการทำงานของการสร้างกฎใหม่	55
3.25 แผนภาพแสดงลำดับการทำงานของการทำงานของการแก้ไขกฎที่มีในระบบ	56
3.26 แผนภาพแสดงลำดับการทำงานของการทำงานของการลบกฎในระบบ.....	57
3.27 แผนภาพแสดงลำดับการทำงานของคำสั่งยกเลิกการทำงานของกฎ	57
3.28 แผนภาพแสดงลำดับการทำงานของคำสั่งให้กฎทำงานทันที.....	58
3.29 แผนภาพแสดงลำดับการทำงานของการทำงานของการแสดงกฎที่มีอยู่ในระบบ.....	58
3.30 แผนภาพแสดงActivity Diagram ของ Login.....	59
3.31 แผนภาพแสดงActivity Diagram ของ Create New Rule.....	60
3.32 แผนภาพแสดงActivity Diagram ของ Edit Existing Rule.....	61
3.33 แผนภาพแสดงActivity Diagram ของ Delete Rule	62
3.34 แผนภาพแสดงActivity Diagram ของ Disable Rule.....	63
3.35 แผนภาพแสดงActivity Diagram ของ Enable Rule.....	63
3.36 แผนภาพแสดงActivity Diagram ของ Show Rule.....	64
3.37 แผนภาพแสดงลำดับการทำงานของการทำงานของการสร้างกฎใหม่	66
3.38 แผนภาพแสดงลำดับการแสดงผลกฎ การใช้งานกฎ และการลบกฎ	67
3.39 แสดงหน้าการแสดงผลไอพี.....	68
3.40 แผนภาพแสดงคุณสมบัติการทำงานจากระบบกับผู้ใช้	69
3.41 แผนภาพแสดงลำดับการทำงานของการทำงานของการเข้าใช้งานระบบ	78
3.42 แผนภาพแสดงลำดับการทำงานของการทำงานของการสร้างกฎใหม่	78
3.43 แผนภาพแสดงลำดับการทำงานของการทำงานของการแก้ไขกฎที่มีในระบบ	79
3.44 แผนภาพแสดงลำดับการทำงานของการทำงานของการลบกฎที่มีในระบบ	80
3.45 แผนภาพแสดงลำดับการทำงานของการทำงานของการแสดงกฎที่มีในระบบ	80
3.46 แผนภาพแสดงลำดับการทำงานของการทำงานของการแสดงกฎที่ทำงานอยู่.....	81
3.47 แผนภาพแสดงลำดับการทำงานของการทำงานของการเริ่มต้นระบบใหม่	81
3.48 แผนภาพแสดงลำดับการทำงานของการทำงานของการแก้ไขหมายเลขไอพี	82

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
 ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญรูป (ต่อ)

รูปที่	หน้า
3.49 แผนภาพแสดงActivity Diagram ของ Create New Rule.....	82
3.50 แผนภาพแสดงActivity Diagram ของ Login.....	83
3.51 แผนภาพแสดงActivity Diagram ของ Edit Existing Rule.....	84
3.52 แผนภาพแสดงActivity Diagram ของ Delete Rule	85
3.53 แผนภาพแสดงActivity Diagram ของ Show Rule.....	85
3.54 แผนภาพแสดงActivity Diagram ของ Reboot System	86
3.55 แผนภาพแสดงActivity Diagram ของ Show IP.....	86
4.1 แสดงหน้าแรกของคอมมานไลน์	87
4.2 แสดงหน้าของไฟร์วอลล์โมดูล.....	87
4.3 แสดงหน้าของสร้างกฎแบบคีย์ค่าด้วยตนเอง (manual).....	88
4.4 แสดงหน้าการใช้งานกฎ (enable rule).....	88
4.5 แสดงหน้าการตั้งค่าไอพี(IP).....	89
4.6 แสดงหน้าการแสดงค่าไอพี(IP).....	89
4.7 แสดงหน้าการรีบูท.....	90
4.8 แสดงหน้าการจัดการเว็บอินเตอร์เฟส.....	90
4.9 แสดงหน้า startup.csh.....	91
4.10 แสดงหน้าการเปลี่ยนแปลงชื่อผู้ใช้งาน.....	91
4.11 แสดงหน้าการสร้างกฎใหม่.....	92
4.12 แสดงตัวอย่างกฎที่มีอยู่ในเทมปไฟล์.....	92
4.13 แสดงตัวอย่างกฎที่มีอยู่ในบูทไฟล์.....	93
4.12 แสดงหน้าการรีบูทระบบ	93
4.13 แสดงหน้าการแสดงกฎ.....	94
4.14 แสดงหน้าการแสดงไอพี.....	94
4.15 แสดงหน้าการแสดงสถานะของกฎ	95

บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ในปัจจุบันอินเทอร์เน็ตมีบทบาทสำคัญต่อการดำเนินกิจกรรมต่างๆ เป็นอย่างมาก ไม่ว่าจะเป็นด้านการติดต่อสื่อสาร ธุรกิจ การศึกษา หรือว่าเพื่อความบันเทิง องค์กรต่างๆ ทั้งภาครัฐและเอกชน ต่างก็นำเอาเน็ตเวิร์กของตนเชื่อมต่อเข้ากับอินเทอร์เน็ตเพื่อที่จะได้รับประโยชน์เหล่านี้ แต่เราต้องไม่ลืมว่าการนำเอาเน็ตเวิร์กไปเชื่อมต่อกับอินเทอร์เน็ตนั้น ทำให้ใครก็ได้บนอินเทอร์เน็ตสามารถเข้ามายังเน็ตเวิร์กนั้นๆ ได้ ปัญหาที่ตามมาก็คือความปลอดภัยของระบบเน็ตเวิร์ก เช่น ทำให้เกิดความเสี่ยงต่อการถูกเจาะระบบ และ ขโมยข้อมูล เป็นต้น

จากปัญหาดังกล่าวทำให้เราต้องมีวิธีการในการรักษาความปลอดภัย สิ่งที่สามารถช่วยลดความเสี่ยงนี้ได้ก็คือ ไฟร์วอลล์ โดยไฟร์วอลล์นั้นจะทำหน้าที่ป้องกันอันตรายต่างๆ จากภายนอกที่จะเข้ามายังเน็ตเวิร์กของเราได้และเนื่องจากไฟร์วอลล์ในอุปกรณ์เน็ตเวิร์กที่มีอยู่ในปัจจุบันนั้นมีราคาค่อนข้างที่จะสูง ซึ่งถ้าผู้ใช้นั้นต้องการจะนำอุปกรณ์ไฟร์วอลล์ไปใช้ในหน่วยงานขนาดเล็กหรือบ้านพักอาศัย ก็จะทำให้ไม่สามารถที่จะมีกำลังซื้อไปใช้ได้อันเนื่องมาจากราคาที่สูงของอุปกรณ์เหล่านั้นนั่นเอง โครงการนี้จึงคิดที่จะพัฒนาอุปกรณ์ทางด้านเน็ตเวิร์กที่มีคุณภาพใกล้เคียงกันแต่มีราคาต้นทุนที่ถูกกว่ามาก เพื่อใช้สำหรับใช้งานในบ้านหรือสำนักงานขนาดเล็กได้ อีกทั้งระบบนั้นจะมีความเสถียรอันเนื่องมาจาก มีการใช้หลักการของการทำระบบฝังตัวขึ้นมา ทำให้ไม่มีโปรเซสอื่นมารบกวนการทำงานและทำให้อุปกรณ์รันได้ต่อเนื่องตลอดเวลา

1.2 ความมุ่งหมายและวัตถุประสงค์ของการศึกษา

การพัฒนาและศึกษาระบบในครั้งนี้เพื่อ

1. ทำให้เครือข่ายของเรามีความปลอดภัยด้วยตัวไฟร์วอลล์ที่พัฒนาขึ้น
2. สามารถนำฟรีบีเอสตีไปใช้กับอุปกรณ์ที่มีหน่วยความจำขนาดเล็กได้
3. ทำให้ระบบไฟร์วอลล์ของเรานั้นมีความเสถียร สามารถทำงานได้ตลอด ปิดเครื่องได้โดยไม่ต้องซัทดาว์น
4. เพื่อสร้างไฟร์วอลล์ที่มีขนาดเล็กในหน่วยความจำประเภทคอมแพ็คแฟลชการ์ด
5. พัฒนาระบบคอมมานด์ไลน์ให้ใช้งานได้ง่ายและรวดเร็ว อีกทั้งยังไม่ต้องมีการจดจำชุดคำสั่งที่ยุ่งยาก เพื่อรองรับผู้ใช้งานที่หลากหลาย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

6. พัฒนาระบบเว็บ เพื่อที่รองรับการใช้งานของผู้ใช้ โดยการใช้เว็บเบราว์เซอร์ ซึ่งทำให้ผู้ใช้งานสามารถที่จะใช้งานระบบได้อย่างสะดวกและมีหน้าเว็บเพจที่สวยงาม ง่ายต่อการใช้งาน

1.3 สมมติฐานของการศึกษา

การศึกษาและการพัฒนาระบบในครั้งนี้ คาดว่าจะประสบความสำเร็จในการพัฒนาและสามารถนำระบบไปใช้งานได้จริง เนื่องจากมีแหล่งข้อมูลที่ให้ค้นคว้าเพิ่มเติมในการทำงานได้ด้วยอย่างเช่น

- <http://ultradesic.org>
- <http://www.mikrotik.com/>
- <http://www.freebsd.org/>
- <http://www.pfsense.org/>

1.4 ทฤษฎีหรือแนวคิดที่ใช้ในการวิจัย

ใช้หลักการการทำงานของระบบไฟร์วอลล์แบบแพ็กเก็ตไฟวเทอร์ริง ซึ่งจะทำการหาเส้นทางและส่งต่อแพ็กเก็ตอย่างมีเงื่อนไข โดยจะพิจารณาจากข้อมูลส่วนที่อยู่ในเฮดเดอร์ของแพ็กเก็ตที่ผ่านเข้ามาเทียบกับกฎที่กำหนดไว้และตัดสินใจว่าจะทิ้งแพ็กเก็ตนั้นไปหรือว่าจะยอมให้แพ็กเก็ตนั้นผ่านไปได้ แต่เนื่องจากระบบปฏิบัติการฟรีบีเอสดีในรูปแบบปกตินั้นมีขนาดใหญ่ โครงการนี้จึงพัฒนาระบบปฏิบัติการให้เป็นระบบแบบฝังตัว ซึ่งทำให้มีขนาดเล็ก ทำงานได้รวดเร็ว และสามารถนำไปใช้กับอุปกรณ์ที่มีหน่วยความจำที่จำกัด โดยได้มีส่วนของคอมมานด์ไลน์อินเตอร์เฟซที่จะทำการกำหนดค่า แก้ไขการกำหนดค่าต่างๆ อาทิเช่น ไอพีแอดเดรส การบล็อกไอพีแอดเดรสที่เราไม่ต้องการให้เข้ามายังเครือข่ายของเรา รวมไปถึงการพัฒนาในส่วนของเว็บอินเตอร์เฟซซึ่งจะสามารถทำการได้ผ่านเว็บอินเตอร์เฟซ ซึ่งมีข้อดีคือ ง่ายต่อการใช้งาน และผู้ใช้ไม่จำเป็นต้องทราบถึงคำสั่งโดยตรง เพราะมีโปรแกรมเว็บเบราว์เซอร์ ที่ใช้ในการแสดงผลและเป็นยูสเซอร์อินเตอร์เฟซนั่นเอง

1.5 ขอบเขตของการวิจัย

ระบบที่ได้ทำการพัฒนาขึ้นมา จะมีขอบเขตการทำงานแบ่งออกได้เป็น 3 ส่วนดังต่อไปนี้

1. การพัฒนาส่วนของระบบปฏิบัติการฟรีบีเอสดี

โครงการระบบไฟร์วอลล์แบบฝังตัว จะมีระบบปฏิบัติการฟรีบีเอสดี ปฏิบัติงานเป็นพื้นฐาน ซึ่งระบบปฏิบัติการฟรีบีเอสดีในรูปแบบปกตินั้นมีขนาดใหญ่และมีส่วนปฏิบัติงานเกินกว่าเอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับใช้เพื่อการศึกษานี้เท่านั้น ไม่อนุญาตให้มีการนำไปใช้ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ความจำเป็น โครงการนี้จึงพัฒนาระบบปฏิบัติการให้เป็นระบบแบบฝังตัว ซึ่งทำให้มีขนาดเล็ก ทำงานได้รวดเร็ว และสามารถนำไปใช้กับอุปกรณ์ที่มีหน่วยความจำที่จำกัด

2. การพัฒนาในส่วนของคอมมานไลน์อินเตอร์เฟส

มีการกำหนดค่าในส่วนต่างๆของไฟร์วอลล์ผ่านทางคอมมานไลน์อินเตอร์เฟส โดยในส่วนนี้สามารถที่จะทำการกำหนดกฎ แก้ไขค่าของกฎหรือลบกฎที่ใช้ในไฟร์วอลล์ได้ อีกทั้งชุดคำสั่งที่ใช้ในส่วนนี้ยังง่ายต่อการใช้งาน เนื่องจากชุดคำสั่งนั้นได้มีการออกแบบให้เป็นแบบเมนูสื่อความหมายได้ชัดเจน ทำให้ผู้ใช้ไม่จำเป็นต้องจดจำชุดคำสั่งที่ยุ่งยากก็สามารถใช้งานได้อย่างรวดเร็วและครอบคลุมการทำงานของระบบได้

3. การพัฒนาในส่วนของเว็บอินเตอร์เฟส

เป็นโปรแกรมสำหรับไฟล์วอลล์บนพีวีเอสดีซึ่งจะสามารถทำการได้ผ่านเว็บอินเตอร์เฟส ซึ่งมีข้อดีคือ ง่ายต่อการใช้งาน และไม่จำเป็นต้องรู้คำสั่งโดยตรง เพราะมีโปรแกรมเว็บเบราว์เซอร์ที่ใช้ในการแสดงผลอยู่มากมาย เช่น โมซิลลา ไฟล์ฟ็อก อินเทอร์เน็ต เอ็กซ์พลอเรอร์

ส่วนไฟล์เก็บข้อมูล เป็นไอพีที่เก็บข้อมูลสำหรับการแสดงสถานะของไอพีในปัจจุบันว่ามีทั้งหมดกี่ไอพี ที่ถูกล็อก รวมถึงแสดงสถานะเครื่องว่าปัจจุบันมีสถานะอะไรบ้าง

1.6 ขั้นตอนของการศึกษา

ขั้นตอนในการพัฒนาระบบงานจะประกอบด้วยขั้นตอนดังต่อไปนี้

1. ศึกษารายละเอียดของการทำงานของไฟร์วอลล์
2. ศึกษารายละเอียดของระบบปฏิบัติการแบบฝังตัว
3. ศึกษารายละเอียดระบบปฏิบัติการของพีวีเอสดี
4. ศึกษารายละเอียดการทำงานของเซิร์ฟเวอร์
5. ศึกษาการออกแบบระบบแบบฝังตัว
6. ศึกษารายละเอียดในการสร้างชุดคำสั่งแบบคอมมานไลน์
7. ศึกษารายละเอียดของพีเอสพี
8. ศึกษารายละเอียดการออกแบบหน้าเว็บอินเตอร์เฟส
9. ศึกษารายละเอียดการเก็บข้อมูลจากเว็บอินเตอร์เฟส

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 2

ทฤษฎีและหลักการที่ใช้ในการพัฒนาระบบไฟร์วอลล์แบบฝังตัว

2.1 หลักการทำงานไฟร์วอลล์แบบแพ็กเก็ตฟิวเตอร์ริงไฟร์วอลล์

ไฟร์วอลล์ชนิดแพ็กเก็ตฟิวเตอร์ริง: ไฟร์วอลล์ประเภทนี้จะทำหน้าที่กรองแพ็กเก็ต โดยการจะตัดสินใจให้แพ็กเก็ตแต่ละแพ็กเก็ตผ่านไปได้อหรือไม่นั้นจะดูจากข้อมูลในส่วนหัวของแพ็กเก็ต เช่น ที่อยู่ผู้ส่งและผู้รับ โปรโตคอล และพอร์ต

ไฟร์วอลล์ประเภทนี้จะมีประสิทธิภาพสูงกว่าไฟร์วอลล์ประเภทอื่นแต่จะมีความซับซ้อนในการจัดการและตั้งค่าสูงกว่า เนื่องจากมันปฏิบัติงานในเน็ตเวิร์กเลเยอร์ที่ต่ำดังนั้นในการตั้งค่าไฟร์วอลล์ประเภทนี้ จึงจะต้องอาศัยความรู้ที่ดีเกี่ยวกับ โปรโตคอลต่างๆที่ใช้ในเครือข่าย

นอกจากนี้ การตั้งกฎในการกรองแพ็กเก็ตนั้นมีความซับซ้อนสูงและไม่มีเครื่องช่วยในการตรวจสอบว่ากฎที่ตั้งขึ้นมานั้นถูกต้องมากน้อยเพียงใด (ต้องตรวจสอบโดยละเอียดด้วยตัวเอง) และเมื่อได้มีการตั้งกฎขึ้นมาแล้ว ในบางครั้งก็จะต้องมีการสร้างข้อยกเว้นต่างๆขึ้นมาสำหรับความต้องการพิเศษของเครื่องต่างๆข้อยกเว้นเหล่านี้สามารถทำให้กฎมีความซับซ้อนสูงขึ้นมาและอาจทำให้เกิดช่องว่างขึ้นบนไฟร์วอลล์ได้

โดยที่ไฟร์วอลล์จะมีขั้นตอนในการทำงานที่เหมือนกันคือ ตรวจสอบข้อมูลเฮดเดอร์ของไอพี แพ็กเก็ต โดยสิ่งที่ถูกตรวจสอบคือ

- หมายเลขที่อยู่ของผู้ส่ง
- หมายเลขปลายทางของผู้ส่ง
- โปรโตคอล
- ออฟชั่น

โพลิซีของไฟร์วอลล์จะตรวจสอบความถูกต้องของแอดเดรส (ทั้งซอร์ซแอดเดรสและเดสทิเนชันแอดเดรส) ด้วย ขกเว้นกรณีที่ระบุเป็น “all” และข้อมูลในส่วนหัวของโปรโตคอลนั้นก็จะเป็นตัวบอกว่า ส่วนของข้อมูลนั้นบรรจุข้อมูลชนิดใดอยู่ เช่น ทีซีพี, ยูดีพี, ไอซีเอ็มพี กระบวนการในการตรวจสอบรูปแบบของเฮดเดอร์นั้นจะอยู่ที่เลย์เออร์ชั้นบนถัดไปและข้อมูลในส่วนออฟชั่นนั้นโดยปกติมักจะไม่มีค่าอะไร แต่อาจจะมีแพ็กเก็ตที่แสดงถึงซอร์ทเร้าติ้ง (source routing) ได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ที่ซีพี เซคเตอร์บรรจุข้อมูล 3 ส่วนที่สำคัญในเซคเตอร์ไว้คือ ซอร์ตพอร์ต, เดสทินเนชันพอร์ต , แฟ็ก ยูคพีเซคเตอร์บรรจุข้อมูลซอร์ทพอร์ตและเดสทินเนชันพอร์ตและบรรจุชนิดของไอซีเอมพี (ไอซีเอมพี แมจเสจ ไทป์) เช่น “echo request” , “destination unreachable”

2.1.1 หลักการในการสร้างกฎของไฟร์วอลล์

หลักการง่ายๆ(ที่ไม่ง่าย)ในการสร้างกฎของไฟร์วอลล์ที่ดีคือความง่าย (simplicity) ซึ่งความง่ายในที่นี้หมายถึงการสร้างกฎที่สั้นๆ อ่านง่ายได้ใจความ ไฟร์วอลล์ที่ดีไม่ควรมียกกฎมากกว่า 30 กฎ เพราะถ้ามากกว่านี้จะทำให้เกิดความสับสนได้ง่ายและอาจจะทำให้เกิดความผิดพลาดโดยไม่รู้ตัวขึ้น นอกจากนี้ยังมีข้อดีในส่วนที่ทำให้เครื่องทำงานน้อยลงอีกด้วย

การสร้างกฎของไฟร์วอลล์ถือได้ว่าเป็นการนำนโยบายทางด้านความปลอดภัย (security policy) ขององค์กรมาบังคับใช้งาน ในทางเทคนิค โดยใช้ไฟร์วอลล์เป็นเครื่องมือให้เกิดผลตามที่ต้องการ นอกจากนี้ยังมีกฎบางส่วนที่ถือได้ว่า ผู้ดูแลระบบควรเพิ่มเข้าไปในกฎของไฟร์วอลล์ เช่น การป้องกันไอพีปลอม(ip spoofing), ป้องกันการโจมตีแบบแลนด แอคแทค(land attack) ซึ่งรายละเอียดจะได้กล่าวถึงอีกครั้งในส่วนของที่ซีพี/ไอพี ฟิวเตอร์ (TCP/IP Filter)

2.1.2 ลำดับของกฎของไฟร์วอลล์

การเรียงลำดับของกฎก็มีความสำคัญเช่นเดียวกันเพราะไฟร์วอลล์โดยส่วนใหญ่ทำงานแบบลำดับ คือ ตรวจสอบแพ็กเก็ตเกี่ยวกับกฎตามลำดับกฎที่สร้างไว้

คำแนะนำในการวางลำดับของกฎ คือ ให้วาง กฎ ที่เป็นกฎทั่วไปไว้ด้านล่าง และให้นำกฎที่มีความเฉพาะเจาะจงมาไว้ด้านบน เพื่อป้องกันไม่ให้แพ็กเก็ตตรงกับกฎที่เป็นกฎทั่วไปก่อน ยกตัวอย่างเช่น ให้นำกฎที่ทำหน้าที่บล็อกไอพีแอดเดรสไปไว้ด้านบนเพื่อให้มั่นใจว่า ถ้ามีแพ็กเก็ตที่มีไอพีแอดเดรสตรงตามที่ระบุไว้ แพ็กเก็ตนั้นจะถูกทิ้งไปก่อนที่จะตรงกับกฎอื่น

2.1.3 การกรอง TCP/IP

ผู้ดูแลไฟร์วอลล์สามารถกำหนด default policy ได้ 2 รูปแบบคือ

- default ACCEPT : ผู้ดูแลไฟร์วอลล์จะต้องสร้างกฎเพื่อกำหนดว่าจะปิดบริการ(service) และโฮสต์ใดบ้าง โดยบริการ(service) และ โฮสต์อื่นๆ ที่ไม่ถูกกำหนดไว้ จะมีค่าเป็นเปิด
- default DROP : ผู้ดูแลไฟร์วอลล์จะต้องสร้างกฎเพื่อกำหนดว่าจะเปิดบริการ(service) และ โฮสต์ใดบ้าง โดยบริการ(service) และ โฮสต์อื่นๆ ที่ไม่ถูกกำหนดไว้ จะมีค่าเป็นปิด

อย่างไรก็ตาม ไม่ว่าจะกำหนด default policy ในรูปแบบใด ผู้ดูแลไฟร์วอลล์ก็ควรทราบ TCP/IP service ที่เป็นจุดอ่อนต่างๆ ในระบบ ดังนี้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 2.1 แสดง TCP/UDP service ที่ควรปิดกั้นที่ไฟร์วอลล์ โดยไม่ให้ใช้ทั้งจากภายในและ
ภายนอกเครือข่าย

Port(s) (Transport)	Server	Port(s) (Transport)	Server
1 (TCP & UDP)	Tcpmux	1981 (TCP)	Shockrave
7 (TCP & UDP)	Echo	1999 (TCP)	BackDoor
9 (TCP & UDP)	Discard	2001 (TCP)	Trojan Cow
11 (TCP & UDP)	Systat	2023 (TCP)	Ripper
13 (TCP & UDP)	Daytime	2049 (TCP & UDP)	Nfs
15 (TCP & UDP)	Netstat	2115 (TCP)	Bugs
17 (TCP & UDP)	Qotd	2140 (TCP)	Deep Throat
19 (TCP & UDP)	Chargen	2222 (TCP)	Subseven21
37 (TCP & UDP)	Time	2301 (TCP & UDP)	Compaqdiag
43 (TCP & UDP)	Whois	2565 (TCP)	Striker
67 (TCP & UDP)	Bootps	2583 (TCP)	WinCrash
68 (TCP & UDP)	Bootpc	2701 (TCP & UDP)	sms-rcinfo
69 (UDP)	Tftp	2702 (TCP & UDP)	sms-remctrl
93 (TCP)	Supdup	2703 (TCP & UDP)	sms-chat
111 (TCP & UDP)	Sunrpc	2704 (TCP & UDP)	sms-xfer
135 (TCP & UDP)	loc-srv	2801 (TCP)	Phineas P.
137 (TCP & UDP)	netbios-ns	4045 (TCP)	Lockd
138 (TCP & UDP)	netbios-dgm	5800 - 5899 (TCP)	winvnc web server
139 (TCP & UDP)	netbios-ssn	5900 - 5999 (TCP)	Winvnc
177 (TCP & UDP)	Xdmcp	6000 - 6063 (TCP)	X11 Window System
445 (TCP & UDP)	microsoft-ds	6665- 6669 (TCP)	Irc

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษเท่านั้น ไม่อนุญาตให้ทำไปใช้ประโยชน์ด้านการค้า

ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 2.1 (ต่อ) แสดง TCP/UDP service ที่ควรปิดกั้นที่ไฟร์วอลล์ โดยไม่ให้ใช้ทั้งจากภายในและภายนอกเครือข่าย

Port(s) (Transport)	Server	Port(s) (Transport)	Server
512 (TCP)	Rexec	6711 - 6712 (TCP)	Subseven
513 (TCP)	rlogin	6776 (TCP)	Subseven
513 (UDP)	Who	7000 (TCP)	Subseven21
514 (TCP)	rsh, rcp, rdist, rdump, rrestore	12345 - 12346 (TCP)	NetBus
515 (TCP)	Lpr	16660 (TCP)	Stacheldraht
517 (UCP)	Talk	27444 (UCP)	Trinoo
518 (UCP)	Ntalk	27666 (TCP)	Trinoo
540 (TCP)	Uucp	31335 (UCP)	Trinoo
1024 (TCP)	NetSpy	31337 -31338 (TCP & UDP)	Back Orifice
1045 (TCP)	Rasmin	32700 - 32900 (TCP & UDP)	RPC services
1090 (TCP)	Xtreme	32720 (TCP)	Trinity V3
1170 (TCP)	Psyber S.S	39168 (TCP)	Trinity V3
1234 (TCP)	Ultors Trojan	65000 (TCP)	Stacheldraht
1243 (TCP)	Backdoor-G		
1245 (TCP)	VooDoo Doll		
1349 (UCP)	Back Orifice DLL		
1492 (TCP)	FTP99CMP		
1600 (TCP)	Shivka-Burka		
1761 - 1764 (TCP & UDP)	sms-helpdesk		
1807 (TCP)	SpySender		

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 2.2 แสดง TCP/UDP service ที่ควรปิดกั้นไม่ให้เข้ามาจากภายนอก

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

ตารางที่ 2.3 แสดง TCP/UDP service ที่อาจเปิดให้บริการใน DMZ (ในทางปฏิบัติให้เปิดเฉพาะ service ที่มีการให้บริการจริงเท่านั้น)

Port(s) (Transport)	Server
20 (TCP)	Ftpdata
21 (TCP)	ftp
22 (TCP)	Ssh
23 (TCP)	telnet
25 (TCP)	Sntp
53 (TCP & UDP)	Domain
80 (TCP)	http
110 (TCP)	pop3
119 (TCP)	nntp
123 (TCP)	Ntp
143 (TCP)	Imap
179 (TCP)	Bgp
389 (TCP & UDP)	Ldap
443 (TCP)	Ssl

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 2.3 (ต่อ) แสดง TCP/UDP service ที่อาจเปิดให้บริการใน DMZ (ในทางปฏิบัติให้เปิดเฉพาะservice ที่มีการให้บริการจริงเท่านั้น)

Port(s) (Transport)	Server
1080 (TCP)	Socks
3128 (TCP)	Squid
8000 (TCP)	http (alternate)
8080 (TCP)	http-alt
8888 (TCP)	http (alternate)

ตารางที่ 2.4 แสดง ICMP message ที่ควรอนุญาตให้ออกไปจากเครือข่ายภายในได้

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

ตารางที่ 2.5 แสดง ICMP message ที่ควรอนุญาตให้เข้ามายังเครือข่ายภายในได้

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

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.1.4 คำแนะนำอื่นๆ สำหรับการสร้าง กฎ ของไฟร์วอลล์

• ควรมีการบันทึกข้อมูลลงล็อกสำหรับกฎที่ใช้บล็อกการเข้าถึง ซึ่งข้อมูลนี้จะเป็นประโยชน์ในการตรวจสอบการบุกรุก รายละเอียดของล็อกจะพบใน Logging and Debugging

• ป้องกันการปลอมไอพี (IP spoof) สำหรับข้อมูลขาเข้ามาจากอินเทอร์เน็ต โดยป้องกันไม่ให้ packet ที่มีไอพีดังต่อไปนี้เข้ามายังเครือข่ายภายใน

- 127.0.0.0 - 127.255.255.255 : local host address
- 10.0.0.0 - 10.255.255.255 : reserved address
- 172.16.0.0 - 172.31.255.255 : reserved address
- 192.168.0.0 - 192.168.255.255 : reserved address
- 224.0.0.0 - 239.255.255.255 : multicast address

• ป้องกันเครื่องไฟร์วอลล์จากการโจมตีแบบแลนดแอคแทค(Land attack) ซึ่งการโจมตีแบบนี้จะใช้วิธีส่งแพ็คเกจที่มี source ip address ตรงกันกับ destination ip address รวมทั้งค่า source port และ destination port ที่ตรงกัน ซึ่งก่อให้เกิดการโจมตีแบบ Denial of Service ได้ ซึ่งป้องกันได้โดย block ไม่ให้ข้อมูลขาเข้าที่มี source ip address ตรงกันกับไอพีของเครือข่ายภายในเข้ามาในระบบ

• ป้องกันการโจมตีแบบ SYN flood ที่เครื่องไฟร์วอลล์ ซึ่งผู้บุกรุกจะส่ง SYN packet จำนวนมากมายังเครื่องปลายทาง ทำให้คิวของการรับคอนเนกชัน(connection) ในบริการ(service) ดังกล่าว ทำให้ไม่สามารถให้บริการแก่เครื่องอื่นๆ ได้

• เครื่องไฟร์วอลล์และเครื่องอื่นๆ ภายในเครือข่ายควรได้รับป้องกันจาก ICMP message บางชนิด เช่น ป้องกันการรับ ICMP Echo request ซึ่งสามารถส่งมาเพื่อรวบรวมข้อมูลสำหรับการโจมตีครั้งต่อไป หรือการส่ง ICMP Echo request packet ที่มีขนาดใหญ่ (Ping flood) ซึ่งถือว่าเป็นรูปแบบหนึ่งในการโจมตี นอกจากนี้ redirect packet ที่ส่งมาจากภายนอกยังสามารถเปลี่ยน routing table ใน host ได้อีกด้วย ซึ่งเป็นเรื่องอันตรายอย่างยิ่งสำหรับข้อมูลขาออกนั้น ควรอนุญาตให้ข้อมูล ICMP ดังต่อไปนี้เท่านั้นที่สามารถออกไปได้

- Echo request
- Parameter Problem
- Source Quench

สำหรับข้อมูลขาเข้านั้น ควรอนุญาตให้ข้อมูล ICMP ดังต่อไปนี้เท่านั้นที่สามารถเข้ามาภายในได้

- Echo Reply
- Destination Unreachable
- Source Quench
- Time Exceeded

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- Parameter Problem

● ป้องกันไฟร์วอลล์และเครื่องอื่นๆ ภายในเครือข่ายจาก traceroute เพราะ traceroute เป็นโปรแกรมที่ช่วยให้ทราบถึงไอพีแอดเดรสของ router ที่รับส่งต่อ packet ไปทีละ hop จนกระทั่งถึงปลายทางที่ต้องการ โดยใช้คุณสมบัติของ IP Time To Live (TTL) ในการทำงาน โดยมันจะกำหนดค่า TTL counter ที่ทำให้ router ที่ packet ผ่าน ไปนั้นต้องสร้าง ICMP message กลับมาเสมอ สำหรับคำสั่ง tracert ใน Windows นั้น จะใช้ ping (ICMP Echo) เป็นตัวส่ง packet ออกไป ในขณะที่ traceroute ใน Unix นั้น จะใช้ UDP datagram เป็นตัวส่งข้อมูลออกไป datagram ที่ถูกส่งออกไปนั้นจะถูกส่งไปยัง port 33434 โดยดีพอลต์ และ ค่าหมายเลข port นี้จะถูกเพิ่มขึ้นเมื่อได้รับ packet ที่ตอบกลับมาย่างถูกต้อง โดยปกติแล้ว traceroute มักจะส่ง datagram ออกไปจำนวน 3 datagram เพื่อป้องกันการสูญหายระหว่างทาง

ถึงแม้ว่าจะมีการป้องกันการใช้งาน traceroute จากทั้ง Unix และ Windows แล้วก็ตาม ผู้บุกรุกก็ยังสามารถใช้วิธีอื่นในการ trace เข้ามายังเครือข่ายภายใน เช่น การใช้โปรแกรม Firewalk ดังนั้นหากต้องการหยุดยั้งการใช้ traceroute รวมทั้ง Firewalk แล้ว จะต้องใช้วิธี drop TTL Exceeded in Transit packet ที่ขาออกไปสู่อินเทอร์เน็ต

- จำกัดการเข้าถึงเครื่องไฟร์วอลล์ โดยให้ใช้งานใน service ที่จำเป็นเท่านั้น(สำหรับผู้ดูแลระบบเท่านั้น) และให้บันทึกข้อมูลล็อกสำหรับทั้ง connection ที่สำเร็จและไม่สำเร็จ
- ถ้าหากมี SNMP server รั้นอยู่บนเครื่องไฟร์วอลล์ จะต้องจำกัดการใช้งานให้เฉพาะผู้ดูแลระบบเท่านั้น และให้บันทึกข้อมูลล็อกสำหรับทั้ง connection ที่สำเร็จและไม่สำเร็จ

2.1.5 การเก็บข้อมูลล็อกและตรวจสอบจุดบกพร่อง

การเก็บข้อมูลล็อกของเครื่องไฟร์วอลล์เป็นเรื่องที่จำเป็นอย่างยิ่ง โดยเฉพาะในกรณีที่เครื่องโดน compromise ไปแล้ว จะถือว่าเป็นหลักฐานที่แสดงให้เห็นถึงรูปแบบการโจมตีได้ มีคำแนะนำสำหรับการบันทึกข้อมูลล็อกดังนี้

- ให้ส่งข้อมูลล็อกที่มีความสำคัญไปยัง console ของเครื่องไฟร์วอลล์
- ส่งข้อมูลล็อกไปยังเครื่องที่ทำหน้าที่เก็บล็อกโดยเฉพาะ ซึ่งเครื่องนี้ได้รับการควบคุมการเข้าถึงอย่างเคร่งครัด และไม่ได้เปิดให้บริการอื่นโดยกเว้น syslog
- ตั้งเวลาเครื่องไฟร์วอลล์และเครื่องอื่นๆ ในเครือข่ายให้ใช้เวลาที่ตรงกันทั้งหมด โดยใช้ NTP (network time protocol) เพื่อรับข้อมูลเวลาจาก clock server เดียวกัน
- ป้องกันการโจมตีแบบ log flooding ซึ่งจะทำให้ฮาร์ดดิสก์เต็มอย่างรวดเร็ว
- ไม่ควรส่งข้อมูลล็อกออกไปยังเครื่องพิมพ์โดยตรง เพราะอาจจะเสี่ยงต่อการสูญเสียข้อมูลในกรณีที่เครื่องพิมพ์มีปัญหา

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.1.6 การกำหนดรูปแบบ Syntax ของกฎที่ใช้ในการปิดกั้น packet

action [direction] [on interface] [proto protocol] [from source_address]
[port source_address] [to destination_address] [port destination_address]

action

- pass ยอมให้มีการผ่านเข้ามาได้
- block ไม่ยอมให้มีการผ่านเข้ามา

direction

- in ขาเข้า
- out ขาออก

on ตามด้วย interface

proto ตามด้วย protocol (tcp,udp)

from ตามด้วย source IP address/netmask

port ตามด้วยหมายเลข port ของ source address

to ตามด้วย destination IP address/netmask

port ตามด้วยหมายเลข port ของ destination address

2.2 ระบบแบบฝังตัว

เป็นระบบอิเล็กทรอนิกส์ที่ใช้สำหรับงานควบคุมรวมถึงการแสดงผลการทำงานต่าง ๆ โดยที่ระบบเหล่านี้ถูกใช้เป็นส่วนหนึ่งของระบบและอุปกรณ์ควบคุม เครื่องมือ เครื่องจักรต่าง ๆ มักจะเป็นส่วนหนึ่งของระบบใหญ่ ระบบแบบฝังตัวแม้ไม่ใช่เครื่องคอมพิวเตอร์ แต่ก็มีระบบคอมพิวเตอร์อยู่ภายใน อาจจะเป็นเพียงไมโครโพรเซสเซอร์ หรือชิปประมวลผลหรือโพรเซสเซอร์ที่ประกอบด้วยชิปที่มีวงจรซับซ้อน โดยจะมีหลักการทำงาน คือ มีสัญญาณข้อมูลเข้า (Input) จากอุปกรณ์ เซนเซอร์ (Sensor) เข้าสู่ระบบ และมีสัญญาณผลลัพธ์ (Output) ของระบบไปควบคุมบังคับ สวิตซ์เครื่องควบคุมต่างๆ

นอกจากนี้แบบและรุ่นของระบบแบบฝังตัว (Embedded System) ก็มีมากมายมีทั้งระบบที่เป็นแบบง่าย ๆ การทำงานไม่ซับซ้อน ตลอดจนแบบระบบที่ซับซ้อน ซึ่งขึ้นอยู่กับประเภทและจำนวนไมโครโพรเซสเซอร์ รวมถึงงานโปรแกรมควบคุมในระบบ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.3 เซลล์

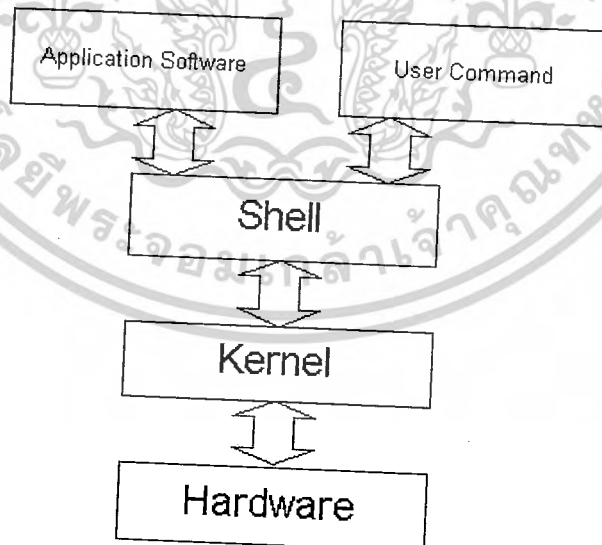
2.3.1 หลักการทำงานของเซลล์

เป็น โปรแกรมแปลคำสั่งที่พิมพ์จากคีย์บอร์ดแล้วตีความคำสั่งที่พิมพ์เพื่อทำงานต่อไป ที่เรียกว่าเซลล์เพราะเซลล์เป็นเหมือนเปลือกหุ้มเคอร์เนลไว้ เป็นตัวกลางระหว่างผู้ใช้กับเคอร์เนล. การสั่งงานเช่นการเรียกใช้โปรแกรมจากผู้ใช้ทุกอย่างต้องผ่านทางเซลล์ทั้งสิ้น จะพูดได้ว่าเซลล์ มีหน้าที่ไว้รองรับการทำงานของเราที่ไม่ผิดนัก เราจะไม่สามารถไปทำอะไรกับระบบปฏิบัติการได้โดยตรง ส่วนของระบบที่ทำหน้าที่ติดต่อกับฮาร์ดแวร์เพื่อทำงานเราจะเรียกว่า เคอร์เนล

ข้อดีของเซลล์ ก็คือเพื่อป้องกันไม่ให้ผู้ใช้เข้าถึงฮาร์ดแวร์ได้โดยตรง ทำให้ยูนิคซ์มีความเสถียรมาก และป้องกันการติดไวรัส เพราะเซลล์จะต้องติดต่อขออนุญาตจากเคอร์เนล ในการเข้าถึงฮาร์ดแวร์หรือทรัพยากรร่วมกัน

2.3.2 ประเภทของเซลล์

บอร์นเซลล์ (รู้จักกันในชื่อ sh) เป็นเซลล์ที่ถูกสร้างขึ้นมาเป็นชนิดแรก ซีเซลล์ (รู้จักกันในชื่อ csh) ซึ่งมีไวยากรณ์การใช้งานคล้ายเหมือนภาษาซี (C language) ซึ่งเซลล์ประเภทนี้นิยมใช้กับบีเอสดีในภายหลังก็มีเซลล์อื่นๆอีกมากมายเช่น คอร์นเซลล์ มีไวยากรณ์เหมือนกับบอร์นเซลล์ แต่มีความสามารถที่ซีเซลล์ทำได้



รูปที่ 2.1 แสดงความสัมพันธ์กันระหว่างเซลล์ เคอร์เนล และชุดคำสั่งของผู้ใช้

ซึ่งเซลล์ที่เลือกใช้เป็น c-shell เนื่องมาจากเหตุผลที่ว่า ระบบที่ทำการพัฒนานั้นใช้ฟรีบีเอสดีและจากการศึกษาก็ทำให้ทราบว่า c-shell เหมาะที่จะใช้งานกับระบบไฟร์วอลล์แบบฝังตัว เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.4 Tool ที่ใช้

2.4.1 ไลท์ทีพีดี

ใช้ ไลท์ทีพีดี เป็นเว็บเซิร์ฟเวอร์ ที่ใช้ในการทำส่วนแสดงผลให้กับผู้ใช้ในการติดต่อกับระบบ ออกเป็นลักษณะของภาษาเซชทีพีดีส่วนภาษาในการใช้งานทำเว็บโปรแกรมมิ่ง (เพอซอนนัล โฮมเพจ

2.4.1.1 ลักษณะการทำงานของไลท์ทีพีดี

ไลท์ทีพีดี เป็นตัวเว็บแปลไฟล์ภาษาพีเอชที โดยมิตัวแปรภาษาพีเอชทีหรือซีจีไอ (คอมมอน เกตเวย์อินเตอร์เฟส) เพื่อใช้ในการแปลงไฟล์ภาษาพีเอชที ออกมาเป็นภาษาเซชทีเอ็มแอล เพื่อแสดงข้อมูลสำหรับผู้ใช้ในการแก้ไขค่าเบื้องต้นสำหรับไฟร์วอลล์ที่สร้างขึ้นผ่านเว็บ เพื่อง่ายต่อการใช้งาน นอกจากนี้ ไลท์ทีพีดี ยังสามารถทำงานบนระบบพีริบีเอสดี ได้ด้วย อีกทั้ง ไลท์ทีพีดี เป็นลักษณะภาษาซีจีไอ ดังนั้น จึงมีขนาดเล็กมาก เพียง 1.2 เมกกะไบต์ จึงสามารถทำงานบนอุปกรณ์ที่มีความจุน้อย

2.4.1.2 วิธีการติดตั้ง

สามารถหาความรู้ไหลคโปรแกรม ไลท์ทีพีดี ได้จาก <http://trac.lighttpd.net/trac> คำสั่งในการติดตั้งสำหรับลินุกซ์

```
# cd /usr/ports/www/lighttpd
# make install distclean
# cd /usr/ports/lang/php5/
# make install clean
```

2.4.2 อีดีทพลัส

อีดีทพลัส เป็น โปรแกรมเท็กซ์ อิดิเตอร์ สำหรับใช้ในการเขียนโครงสร้างภาษาพีเอชที เพื่อตอบสนองต่อเหตุการณ์ของผู้ใช้

2.4.2.1 วิธีการติดตั้ง

สามารถ อินสตอร์ ได้จากตัว อินสตอเรียร์ ของอีดีทพลัส

2.4.3 พีเอชพี

เป็นภาษา สคริป สำหรับเว็บ โปรแกรมมิ่งที่ใช้ในการเขียนคำสั่งโปรแกรมเว็บให้ตอบสนองต่อทางเลือกของผู้ใช้ สามารถใช้ในการเขียนไฟล์ และทำการประมวลผลผ่านโปรแกรมเว็บเซิร์ฟเวอร์และคืนค่ากลับมาเป็นภาษาเซชทีพีดี ให้กับผู้ใช้ ซึ่งภาษาพีเอชพี จัดเป็นภาษาที่อยู่ในลักษณะเซิร์ฟเวอร์ไซด์สคริป

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.4.3.1 การทำงานพีเอสพี

ตั้งแต่เวอร์ชันแรกถึงเวอร์ชัน ปัจจุบัน ตั้งแต่เวอร์ชัน1-3 ใช้การแปลตามลำดับที่ละประโยค คือ แปลไปทำงานไปตามลำดับคำสั่งเหมือนกับภาษาเซชทีเอ็มแอล แต่ตั้งแต่เวอร์ชัน4 เป็นต้นมา ได้มีการเปลี่ยนกระบวนการทำงาน โดยจะทำการแปลเก็บไว้ในหน่วยความจำแล้วจึงทำงาน

2.4.3.2 รูปแบบภาษา

จัดเป็นภาษาสคริปต์ภาษาหนึ่งที่ดำเนินการฝั่งเซิร์ฟเวอร์ คือ เมื่อ โค้ดถูกเรียกใช้งาน โดยบราวเซอร์โปรแกรมพีเอสพี ที่อยู่บนเครื่องที่เป็นเว็บเซิร์ฟเวอร์จะทำการประมวลผลแล้วสร้างผลลัพธ์ที่อยู่ในรูปของภาษาเซชทีเอ็มแอล ขึ้นแล้วส่งให้กับเครื่องไคลเอ็นต์เพื่อให้บราวเซอร์แสดงผล ลักษณะการเขียนสคริปต์ จะเขียนแทรกไว้ภายในไฟล์เซชทีเอ็มแอล โดยเปิดด้วยแท็ก “<?php” และปิดด้วย “?”

- การประกาศตัวแปร ชนิดของข้อมูล ข้อมูลชนิด สตริงและอาร์เรย์
- การใช้งาน โอเปอเรเตอร์ เกี่ยวกับตัวเลข มีดังนี้ +, -, *, /, % โอเปอเรเตอร์ การกำหนดค่า ได้แก่ =, +=, -=, *= โอเปอเรเตอร์ การเปรียบเทียบที่ใช้เปรียบเทียบระหว่าง 2 ค่า ได้แก่ == เป็นต้น
- ประโยคควบคุม การใช้งาน if else เป็นคำสั่งที่ใช้เปรียบเทียบเพื่อดำเนินการอย่างใดอย่างหนึ่งหรือ 2 ทางเลือก , การใช้งาน for , foreach ใช้กับการดึงข้อมูลและคีย์ในตัวแปรอาร์เรย์ออกมาทำงานเป็นวงรอบโดยไม่ต้องใช้ลูป while
- การใช้งานอาร์เรย์ ประกาศตัวแปร , การนับจำนวนอีเรมีนอาร์เรย์โดยใช้ฟังก์ชัน count() , การทำลายตัวแปรอาร์เรย์ โดยใช้ unset()
- การจัดการไฟล์ และไดเรคทอรี
- การเปิดไฟล์โดยใช้คำสั่ง open รูปแบบ

```
int fopen(string filename,string mode[, int use_include_path])
```

-การอ่านไฟล์ ฟังก์ชัน fgets()

รูปแบบ

```
String fgets(int fp[, int length])
```

ฟังก์ชัน fgetcsv()

รูปแบบ

```
Array fgetcsv(resource handle[, int length[,string delimiter[, string enclosure]]])
```

- การเขียนลง- ไฟล์ ใช้คำสั่ง- fputs()

มีรูปแบบคือ

```
Int fputs (int fp,string str[, intlength])
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- รับข้อมูลจากผู้ใช้งานด้วยฟอร์ม
- สร้างฟอร์มด้วยเซชทีเอ็มแอล

การสร้างฟอร์มในเว็บเพจทั่วไปจะใช้คำสั่งเซชทีเอ็มแอล ตั้งแต่การสร้างฟอร์มมีช่องรับข้อความ หรือ textbox , ปุ่มกด(button) เว็บเพจที่ต้องการรับค่าจากผู้ใช้งานเพื่อนำไปประมวลผลหรือบันทึกลงในฐานข้อมูล จำเป็นต้องมีคอนโทรลต่างๆ ได้แก่ ช่องรับข้อความปุ่ม, กล่องรายการ (checkbox) เพื่อเป็นส่วนที่ใช้รับข้อมูลจากผู้ใช้งานและเมื่อผู้ใช้งานกรอกข้อมูลครบแล้ว การส่งข้อมูลเหล่านี้ไปยังเพจที่ทำหน้าที่ประมวลผล จำเป็นต้องอาศัยแท็ก<form> ประกอบไปด้วยแอตทริบิวต์ที่สำคัญดังนี้

- action ใช้ระบุปลายทางที่จะส่งข้อมูลจากฟอร์มไปให้เมื่อฟอร์มถูกsubmit
- method วิธีการส่งข้อมูลคือ get และ post เมื่อใช้ get ข้อมูลในฟอร์มจะถูกส่งโดยพ่วงท้ายไปกับยูอาร์แอล ถ้าใช้post ข้อมูลในฟอร์มจะถูกไปยังเซิร์ฟเวอร์ โดยไม่แสดงใน address bar
- ชนิดของข้อมูลในฟอร์ม ช่องรับข้อความ คือ ช่องที่ให้ผู้ใช้กรอกข้อมูล เพื่อส่งไปประมวลผล คือ แท็ก <input type="text"> ที่เป็นช่องข้อความบรรทัดเดียว ใช้สำหรับกรอกเพื่อบันทึกข้อมูล ส่วน <input type="password"> เป็นช่องที่อยู่ในรูปแบบของเท็กซ์บ็อกซ์ ที่เป็นลักษณะของรหัสผ่าน ส่วน <input type="radio"> เป็นอินพุต แบบเดียวที่ไม่ได้ใช้ในรูปแบบของข้อความ แต่อยู่ในรูปแบบของตัวเลือก

2.5 การเซตค่าต่างๆของกฎการทำงานในไฟร์วอลล์

2.5.1 การเซตค่าอินเทอร์เน็ตเฟส โดยแบ่งออกเป็น

1. อินเทอร์เน็ตแบบแลนค์ มาจากเครือข่ายภายใน คือเครือข่ายคอมพิวเตอร์ระยะใกล้ เช่น ในโรงเรียน หรือสำนักงาน ที่ใดที่หนึ่ง การที่คอมพิวเตอร์แต่ละเครื่อง
2. อินเทอร์เน็ตแบบแวนด์ (Wide Area Natwork) คือการเชื่อมต่อระบบแลนค์ ตั้งแต่ 2 ระบบขึ้นไปเข้าด้วยกัน อาจอยู่บริเวณเดียวกันหรืออยู่ไกลกันมากก็ได้

2.5.2 การเซตค่าโปรโตคอลที่ใช้ในการติดต่อสื่อสาร

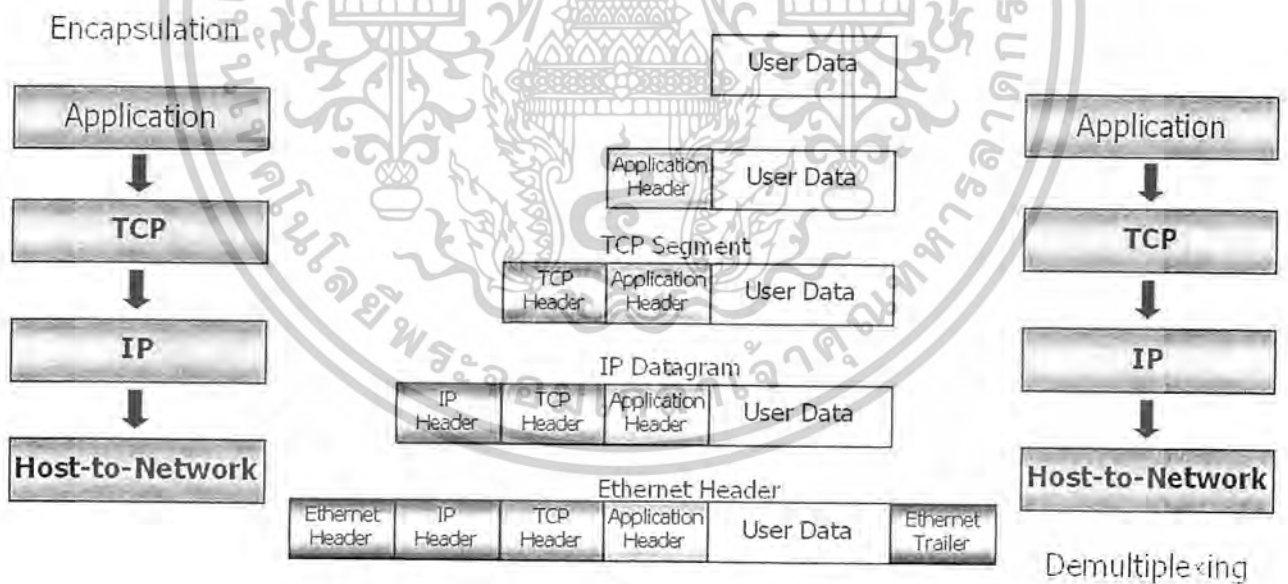
ทีซีพี/ไพบี (Transmitsion Control Protocol/Internet Protocol) เป็นชุดของโปรโตคอลที่ถูกใช้ในการสื่อสารผ่านเครือข่ายอินเทอร์เน็ต โดยมีวัตถุประสงค์เพื่อให้สามารถใช้สื่อสารจากต้นทางข้ามเครือข่ายไปยังปลายทางได้ และสามารถหาเส้นทางที่จะส่งข้อมูลไปได้เองโดยอัตโนมัติ ถึงแม้ว่าในระหว่างทางอาจจะผ่านเครือข่ายที่มีปัญหา โปรโตคอลก็ยังคงหาเส้นทางอื่นในการส่งผ่านข้อมูลไปให้ถึงปลายทางได้ ชุดโปรโตคอลนี้ได้รับการพัฒนามาตั้งแต่ปี 1960 ซึ่งถูกใช้เป็นครั้งแรกในเครือข่าย อาร์พาร์เน็ต ซึ่งต่อมาได้ขยายการเชื่อมต่อไปทั่วโลกเป็นเครือข่ายอินเทอร์เน็ต ทำให้ ทีซีพี/ไพบี เป็นที่ยอมรับอย่างกว้างขวางจนถึงปัจจุบัน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาค้นคว้าเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ที่ซีพี/ไบท์ มีจุดประสงค์ของการสื่อสารตามมาตรฐาน สามประการคือ

1. เพื่อใช้ติดต่อสื่อสารระหว่างระบบที่มีความแตกต่างกัน
2. ความสามารถในการแก้ไขปัญหาที่เกิดขึ้นในระบบเครือข่าย เช่น ในกรณีที่ผู้ส่งและผู้รับยังคงมีการติดต่อกันอยู่ แต่โหนดกลางที่ใช้เป็นผู้ช่วยรับ-ส่งเกิดเสียหายใช้การไม่ได้หรือสายสื่อสารบางช่วงถูกตัดขาด กฎการสื่อสารนี้จะต้องสามารถจัดหาทางเลือกอื่นเพื่อให้การสื่อสารดำเนินต่อไปได้โดยอัตโนมัติ
3. มีความคล่องตัวต่อการสื่อสารข้อมูลได้หลายชนิดทั้งแบบที่ไม่มีความเร่งด่วน เช่น การจัดส่งแฟ้มข้อมูล และแบบที่ต้องการรับประกันความเร่งด่วนของข้อมูล เช่น การสื่อสารแบบเวลาจริง(real time) และทั้งการสื่อสารแบบเสียง (Voice) และข้อมูล (data)

การส่งข้อมูลผ่านในแต่ละเลเยอร์ แต่ละเลเยอร์จะทำการประกอบข้อมูลที่รับมา กับข้อมูลส่วนควบคุมซึ่งถูกนำมาไว้ในส่วนหัวของข้อมูลเรียกว่าส่วนหัวภายใน ส่วนหัวจะบรรจุข้อมูลที่สำคัญของโปรโตคอลที่ทำการเอนแคปซูเลท เมื่อผู้รับได้รับข้อมูลก็จะเกิดกระบวนการทำงานย้อนกลับคือ โปรโตคอลเดียวกัน ทางฝั่งผู้รับก็จะได้รับข้อมูลส่วนที่เป็น ส่วนหัวก่อนและนำไปประมวลและทราบว่าข้อมูลที่ตามมามีลักษณะอย่างไร ซึ่งกระบวนการย้อนกลับนี้เรียกว่า ดีเม้าท์ไบท์เล็กซิ่ง



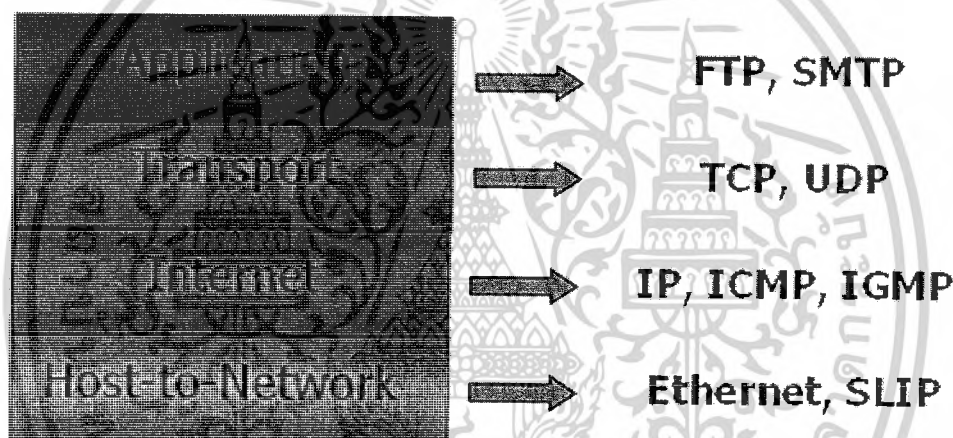
รูปที่ 2.2 ขั้นตอนการเอนแคปซูเรชั่น และดีเม้าท์ไบท์เล็กซิ่ง

ข้อมูลที่ผ่านการ เอนแคปซูเลท ในแต่ละเลเยอร์มีชื่อเรียกแตกต่างกัน ดังนี้

- ข้อมูลที่มาจากผู้ใช้หรือก็คือข้อมูลที่ผู้ใช้เป็นผู้ป้อนให้กับแอปพลิเคชัน เรียกว่า ข้อมูลผู้ใช้ (user data)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- เมื่อแอปพลิเคชันได้รับข้อมูลจากผู้ใช้ก็จะนำมาประกอบกับส่วนหัวของแอปพลิเคชัน เรียกว่า ข้อมูลแบบแอปพลิเคชันและส่งต่อไปยัง โพรโทคอลที่ซีพี
 - เมื่อ โพรโทคอลที่ซีพีได้รับข้อมูลแบบแอปพลิเคชันก็จะนำมารวมกับส่วนหัวของ โพรโทคอลที่ซีพี เรียกว่า ที่ซีพีเซกเมนต์และส่งต่อไปยังไอพีโพรโทคอล
 - เมื่อไอพีโพรโทคอลได้รับ ที่ซีพีเซกเมนต์ก็จะนำมารวมกับของไอพีโพรโทคอล เรียกว่า ไบท์ ดาต้าแกรม และส่งต่อไปยังชั้น โฮส-เครือข่าย
 - ในระดับชั้น โฮสต์-เครือข่าย จะนำ ไบท์ ดาต้าแกรม มาเพิ่มส่วนเอเธอร์เน็ตเฮดเดอร์ และ แฟมิลี่ เรียกว่าอินเทอร์เน็ตเฟรม ก่อนจะแปลงข้อมูลเป็นสัญญาณไฟฟ้าส่งผ่านสายสัญญาณที่ เชื่อมโยงอยู่ต่อไป
- ในแต่ละเลเยอร์ของ โครงสร้าง ทีซีพี/ไบท์ สามารถอธิบายได้ดังนี้



รูปที่ 2.3 โครงสร้าง ทีซีพี/ไบท์

- ชั้นโฮสต์-เครือข่าย (Host-to-Network Layer)

โพรโทคอลสำหรับการควบคุมการสื่อสารในชั้นนี้เป็นสิ่งที่ไม่มีการกำหนดรายละเอียดอย่างเป็นทางการ หน้าที่หลักคือการรับข้อมูลจากชั้นสื่อสาร ไอพีมาแล้วส่งไปยังโหนดที่ระบุไว้ในเส้นทางเดินข้อมูลทางด้านผู้รับก็จะทำงานในทางกลับกัน คือรับข้อมูลจากสายสื่อสารแล้วนำส่งให้กับโปรแกรมในชั้นสื่อสาร

- ชั้นสื่อสารอินเทอร์เน็ต (The Internet Layer)

ใช้ประเภทของระบบการสื่อสารที่เรียกว่า ระบบเครือข่ายแบบสลับช่องสื่อสารระดับแพ็กเก็ต (packet-switching network) ซึ่งเป็นการติดต่อแบบไม่ต่อเนื่อง (Connectionless) หลักการทำงานคือการปล่อยให้ข้อมูลขนาดเล็กที่เรียกว่า แพ็กเก็ต (Packet) สามารถไหลจากโหนดผู้ส่งไป ตามโหนดต่างๆ ในระบบจนถึงจุดหมายปลายทางได้โดยอิสระ หากว่ามีการส่งแพ็กเก็ตออกมาเป็น

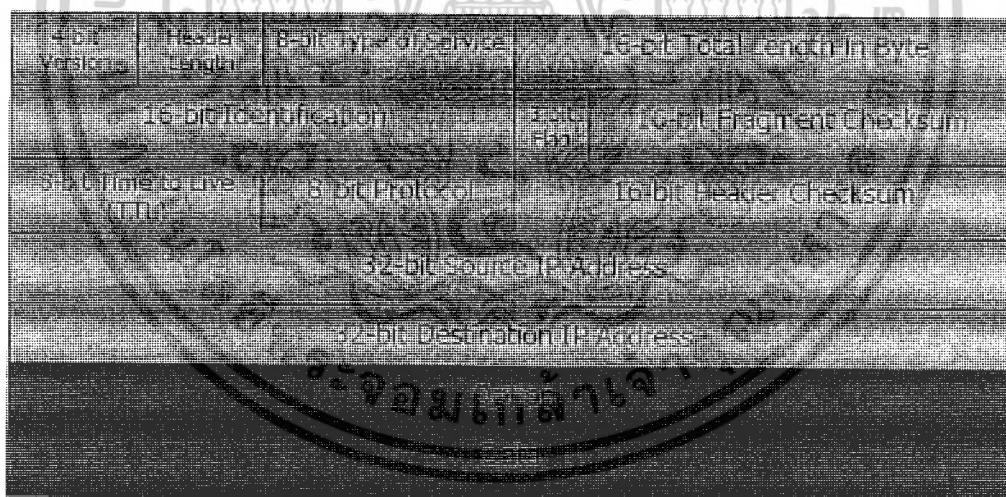
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ชุดโดยมีจุดหมายปลายทางเดียวกันในระหว่างการเดินทางในเครือข่าย เพื่อก่อกำเนิดแต่ละตัวในชุดนี้ก็จะ เป็นอิสระแก่กันและกัน ดังนั้น เพื่อก่อกำเนิดที่ส่ง ไปถึงปลายทางอาจจะไม่เป็นไปตามลำดับก็ได้

2.5.2.1 ไลท์(Internet Protocol)

ไลท์ เป็นโปรโตคอลในระดับชั้นเน็ตเวิร์ก ทำหน้าที่จัดการเกี่ยวกับแอดเดรสและ ข้อมูล และควบคุมการส่งข้อมูลบางอย่างที่ใช้ในการหาเส้นทางของเพื่อก่อกำเนิด ซึ่งกลไกในการหา เส้นทางของไลท์ จะมีความสามารถในการหาเส้นทางที่ดีที่สุด และสามารถเปลี่ยนแปลงเส้นทางได้ ในระหว่างการส่งข้อมูล และมีระบบการแยกและประกอบค้ำแกรม (datagram) เพื่อรองรับการ ส่งข้อมูลระดับค้ำแกรมที่มีขนาด เอมทิยู(Maximum Transmission Unit) ที่แตกต่างกัน ทำให้ สามารถนำ ไลท์ ไปใช้บนโปรโตคอลอื่นได้หลากหลาย เช่น อีเทอร์เน็ต ทอร์กเคน ริง หรือ แอปเปิลทอร์ก

การเชื่อมต่อของไลท์เพื่อทำการส่งข้อมูลจะเป็นแบบที่ไม่สร้างเส้นทางการ เชื่อมต่อหรือเกิดเส้นทางการเชื่อมต่อในทุกๆครั้งของการส่งข้อมูล 1 ค้ำแกรม โดยจะไม่ทราบถึง ข้อมูลค้ำแกรมที่ส่งก่อนหน้าหรือส่งตามมา แต่การส่งข้อมูลใน 1 ค้ำแกรม อาจเกิดการส่ง ได้หลายครั้งในกรณีที่มีการแบ่งข้อมูลออกเป็นส่วนย่อยๆ (fragmentation) และถูกนำไปรวมเป็น ค้ำแกรมเดิมเมื่อถึงปลายทาง



รูปที่ 2.4 ส่วนหัวของไลท์

เฮดเดอร์ของ ไลท์ โดยปกติจะมีขนาด 20 ไลท์ ยกเว้นในกรณีที่มีการเพิ่ม ออฟชั่นบางอย่าง ฟิลด์ของเฮดเดอร์ ไลท์ จะมีความหมายดังนี้

- เวอร์ชัน: หมายเลขเวอร์ชันของโปรโตคอล ที่ใช้งานในปัจจุบันคือ เวอร์ชัน 4 (ไลท์v4) และเวอร์ชัน 6 (ไลท์v6)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

b. ความยาวของเฮดเดอร์: ความยาวของเฮดเดอร์ โดยทั่วไปถ้าไม่มีส่วนออฟชั่น จะมีค่าเป็น 5 (5*32 bit)

c. ชนิดของการให้บริการ(Type of Service:)ใช้เป็นข้อมูลสำหรับเราเตอร์ในการตัดสินใจเลือกการค้นหาข้อมูลในแต่ละดาต้าแกรม แต่ในปัจจุบันไม่ได้มีการนำไปใช้งานแล้ว

d. ความยาว(Length): ความยาวทั้งหมดเป็นจำนวนไบต์ของดาต้าแกรม ซึ่งด้วยขนาด 16 บิตของฟิลด์ จะหมายถึงความยาวสูงสุดของดาต้าแกรม คือ 65535 ไบต์ (64k) แต่ในการส่งข้อมูลจริง ข้อมูลจะถูกแยกเป็นส่วนๆตามขนาดของเอมทียูที่กำหนดในลิงค์เลเยอร์ และนำมารวมกันอีกครั้งเมื่อส่งถึงปลายทาง แอปพลิเคชันส่วนใหญ่จะมีขนาดของดาต้าแกรมไม่เกิน 512 ไบต์

e. ไอเดนติไฟเคชัน: เป็นหมายเลขของดาต้าแกรมในกรณีที่มีการแยกดาต้าแกรมเมื่อข้อมูลส่งถึงปลายทางจะนำข้อมูลที่มี identification เดียวกันมารวมกัน

f. แฟ็กจ: ใช้ในกรณีที่มีการแยกดาต้าแกรม

g. แฟ็กเม้นออฟเซต:ใช้ในการกำหนดตำแหน่งข้อมูลในดาต้าแกรมที่มีการแยกส่วน เพื่อให้สามารถนำกลับมาเรียงต่อกันได้อย่างถูกต้อง

h. ทามทูลิฟ:กำหนดจำนวนครั้งที่มากที่สุดที่ดาต้าแกรมจะถูกส่งระหว่างฮอป(การส่งผ่านข้อมูลระหว่างเน็ตเวิร์ค) เพื่อป้องกันไม่ให้เกิดการส่งข้อมูลโดยไม่สิ้นสุด โดยเมื่อข้อมูลถูกส่งไป 1 ฮอป จะทำการลดค่าทามทูลิฟลง 1 เมื่อค่าของทามทูลิฟเป็น 0 และข้อมูลยังไม่ถึงปลายทาง ข้อมูลนั้นจะถูกยกเลิกและเราเตอร์สุดท้ายจะส่งข้อมูล ไอซีเอ็มพีแจ้งกลับมายังต้นทางว่าเกิดหมดเวลา (time out) ในระหว่างการส่งข้อมูล

i. โปรโตคอล: ระบุโปรโตคอลที่ส่งในดาต้าแกรม เช่น ทีซีพี, ยูดีพี หรือ ไอซีเอ็มพี

j. ส่วนหัว เช็กซัม: ใช้ในการตรวจสอบความถูกต้องของข้อมูลในเฮดเดอร์

k. ไบท์ แอดเดรสของต้นทาง: หมายเลข ไบท์ ของผู้ส่งข้อมูล

l. ไบท์ แอดเดรสปลายทาง: หมายเลข ไบท์ ของผู้รับข้อมูล

m. ข้อมูล: ข้อมูลจากโปรโตคอลระดับบน

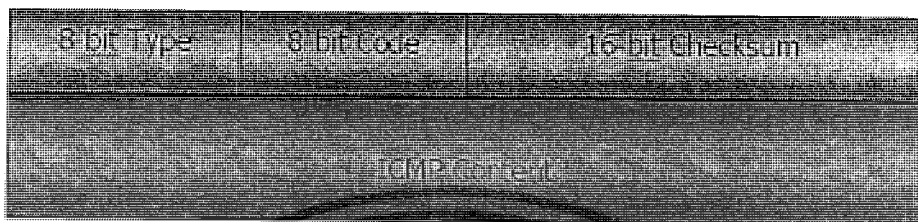
2.5.2.2 ไอซีเอ็มพี(InternetควบคุมMessage Protocol)

ไอซีเอ็มพี เป็นโปรโตคอลที่ใช้ในการตรวจสอบและรายงานสถานภาพของดาต้าแกรม (Datagram) ในกรณีที่เกิดปัญหาเกี่ยวกับดาต้าแกรม เช่น เราเตอร์ไม่สามารถส่งดาต้าแกรมไปถึงปลายทางได้ ไอซีเอ็มพี จะถูกส่งออกไปยังโฮสต์ต้นทางเพื่อรายงานข้อผิดพลาด ที่เกิดขึ้น อย่างไรก็ตาม ใม่มีอะไรรับประกันได้ว่า ไอซีเอ็มพีเมจแอสจ ที่ส่งไปจะถึงผู้รับจริงหรือไม่ หากมีการส่งดาต้าแกรมออกไปแล้วไม่มี ไอซีเอ็มพีเมจแอสจ ฟ้อง ข้อความผิดพลาดกลับมา ก็แปลความหมายได้สองกรณีคือ ข้อมูลถูกส่งไปถึงปลายทางอย่างเรียบร้อย หรืออาจจะมีปัญหา ในการสื่อสารทั้งการส่งดาต้าแกรม และ ไอซีเอ็มพี เมจแอสจ ที่ส่งกลับมาก็มีปัญหาระหว่างทางก็ได้ ไอซีเอ็มพี จึงเป็น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

โปรโตคอลที่ไม่มีที่น่าเชื่อถือ (unreliable) ซึ่งจะเป็นหน้าที่ของ โปรโตคอลในระดับสูงกว่าชั้นเน็ตเวิร์กในการจัดการให้การสื่อสารนั้นๆ มีที่น่าเชื่อถือ

ในส่วนของ ไอซีเอ็มพี เมจแสจ จะประกอบด้วยชนิด (type) ขนาด 8 บิต เช็คซั่มขนาด 16 บิต และส่วนของ เนื้อหา ซึ่งจะมีขนาดแตกต่างกันไปตามชนิด (type)และ โทคิต



รูปที่ 2.5 ส่วนหัวของไอซีเอ็มพี

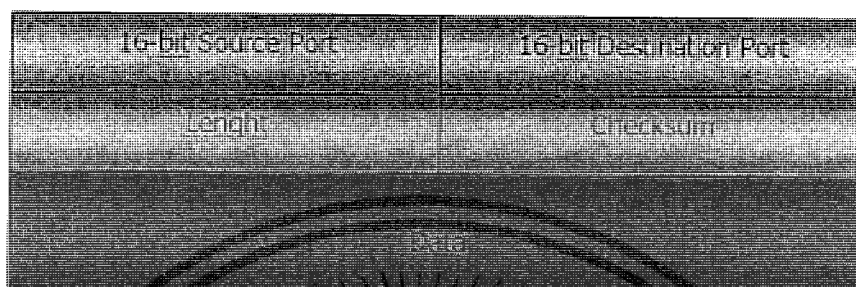
3. ชั้นสื่อสารนำส่งข้อมูล (Transport Layer)

แบ่งเป็น โปรโตคอล 2 ชนิดตามลักษณะ ลักษณะแรกเรียกว่าการส่งผ่าน(Transmission) ควบคุม โปรโตคอล(ทีซีพี)เป็นแบบที่มีการกำหนดช่วงการสื่อสารตลอดระยะเวลาการสื่อสาร (connection-oriented) ซึ่งจะยอมให้มีการส่งข้อมูลเป็นแบบ การไหลของไบนารี (byte stream) ที่ไว้ใจได้โดยไม่มีข้อผิดพลาด ข้อมูลที่มีปริมาณมากจะถูกแบ่งออกเป็นส่วนเล็กๆ เรียกว่า เมจแสจ ซึ่งจะ ถูกส่งไปยังผู้รับผ่านทางชั้นสื่อสารของอินเทอร์เน็ต ทางฝ่ายผู้รับจะนำเมจแสจมาเรียงต่อกัน ตามลำดับเป็นข้อมูลตัวเดิม ทีซีพียังสามารถในการควบคุมการไหลของข้อมูลเพื่อป้องกันไม่ให้ผู้ส่งส่งข้อมูลเร็วเกินกว่าที่ผู้รับจะทำงานได้ทันอีกด้วย โปรโตคอลการนำส่งข้อมูลแบบที่สอง เรียกว่า ยูดีพี (ผู้ใช้ Datagram Protocol) เป็นการติดต่อแบบไม่ต่อเนื่อง (connectionless) มีการ ตรวจสอบความถูกต้องของข้อมูลแต่จะไม่มี การแจ้งกลับไปยังผู้ส่ง จึงถือได้ว่าไม่มีการตรวจสอบ ความถูกต้องของข้อมูล อย่างไรก็ตามวิธีการนี้มีข้อดีในด้านความรวดเร็วในการส่งข้อมูล จึงนิยมใช้ ในระบบผู้ให้และผู้ให้บริการ ซึ่งมีการสื่อสารแบบถาม/ตอบ(request/reply) นอกจากนั้นยังใช้ในการ ส่งข้อมูลประเภทภาพเคลื่อนไหวหรือการส่งเสียง (voice) ทางอินเทอร์เน็ต

a. ยูดีพี : (User Datagram Protocol)

เป็น โปรโตคอลที่อยู่ในชั้นทรานสปอร์ตเมื่อเทียบกับโมเดลโอเอสไอ โดยการส่งข้อมูลของ ยูดีพีนั้นจะเป็นการส่งครั้งละ 1 ชุดข้อมูล เรียกว่า ยูดีพีดาต้าแกรม ซึ่งจะไม่มีความสัมพันธ์กัน ระหว่างดาต้าแกรมและจะไม่มีการตรวจสอบความสำเร็จในการรับส่งข้อมูล กลไกการ ตรวจสอบโดยเช็คซั่มของยูดีพีนั้นเพื่อเป็นการป้องกันข้อมูลที่อาจจะถูกแก้ไข หรือมีความผิดพลาด ระหว่างการส่ง และหากเกิดเหตุการณ์ดังกล่าว ปลายทางจะรับรู้ว่ามีข้อผิดพลาดเกิดขึ้น แต่มันจะ เป็นการตรวจสอบเพียงฝ่ายเดียวเท่านั้น โดยในข้อกำหนดของยูดีพี หากพบว่าเช็คซั่มเกิดผิดพลาดก็ ให้ผู้รับปลายทางทำการทิ้งข้อมูลนั้น แต่จะไม่มี การแจ้งกลับไปยังผู้ส่งแต่อย่างใด การรับส่งข้อมูล เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่นับญาติให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

แต่ถ้าเกิดข้อผิดพลาดในระดับไบนารี เช่น ส่งไม่ถึง, หมดเวลา ผู้ส่งจะได้รับข้อความผิดพลาด (Error Message) จากระดับไบนารีเป็นไอซีเอ็มพีข้อความผิดพลาด (Error Message) แต่เมื่อข้อมูลส่งถึงปลายทางถูกต้อง แต่เกิดข้อผิดพลาดในส่วนของผู้ตีพีเองจะ ไม่มีการยืนยันหรือแจ้งให้ผู้ส่งทราบแต่อย่างใด



รูปที่ 2.6 ส่วนหัวของ ยูดีพี

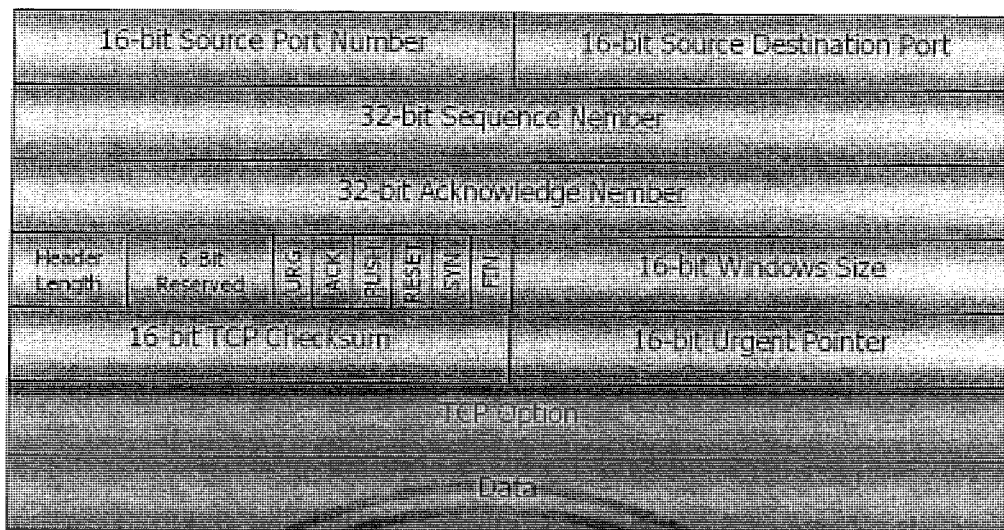
มีรายละเอียด ดังนี้

- หมายเลขพอร์ตต้นทาง: หมายเลขพอร์ตต้นทางที่ส่งค่าตัวแกรมนี้
- หมายเลขพอร์ตปลายทาง: หมายเลขพอร์ตปลายทางที่จะเป็นผู้รับค่าตัวแกรม
- ความยาวของค่าตัวแกรม (UDP Length): ความยาวของค่าตัวแกรม ทั้งส่วน ส่วนหัว และ ส่วนข้อมูล นั้นหมายความว่า ค่าที่น้อยที่สุดในฟิลด์นี้คือ 8 ซึ่งเป็นขนาดของ ส่วนหัว
- เช็คซัม(checksum): เป็นตัวตรวจสอบความถูกต้องของ ยูดีพีค่าตัวแกรม และจะนำข้อมูล บางส่วนใน ไบนารี ส่วนหัว มาคำนวณด้วย

2.5.2.3 ทีซีพี : (Transmission Control Protocol)

อยู่ใน ชั้นทรานสปอร์ต เช่นเดียวกับ ยูดีพี ทำหน้าที่จัดการและควบคุมการรับส่ง ข้อมูล ซึ่งมีความสามารถและรายละเอียดมากกว่า ยูดีพี โดยค่าตัวแกรมของ ทีซีพี จะมีความสัมพันธ์ ต่อเนื่องกัน และมีกลไกควบคุมการรับส่งข้อมูลให้มีความถูกต้อง (reliable) และมีการสื่อสารอย่างเป็นกระบวนการ (connection-oriented)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 2.7 ส่วนหัวของทีซีพี

มีรายละเอียด ดังนี้

- หมายเลขพอร์ตต้นทาง: หมายเลขพอร์ตต้นทางที่ส่งค่าตัวแกรมนี้
- หมายเลขพอร์ตปลายทาง : หมายเลขพอร์ตปลายทางที่จะเป็นผู้รับค่าตัวแกรม
- หมายเลขลำดับ: ฟิลด์ที่ระบุหมายเลขลำดับอ้างอิงในการสื่อสารข้อมูลแต่ละครั้ง เพื่อใช้ในการแยกแยะว่าเป็นข้อมูลของชุดใด และนำมาจัดลำดับได้ถูกต้อง
- หมายเลขของการตอบรับ : ทำหน้าที่เช่นเดียวกับ Sequence Number แต่จะใช้ในการตอบรับ
- ความยาวของเฮดเดอร์: โดยปกติความยาวของเฮดเดอร์ ทีซีพี จะมีความยาว 20 ไบต์ แต่อาจจะมากกว่านั้น ถ้ามีข้อมูลในฟิลด์ออฟชั่น แต่ต้องไม่เกิน 60 ไบต์
- แฟล็ก: เป็นข้อมูลระดับบิตที่อยู่ในเฮดเดอร์ ทีซีพี โดยใช้เป็นตัวบอกคุณสมบัติของแฟล็กเกิดทีซีพี ขณะนั้นๆ และใช้เป็นตัวควบคุมจังหวะการรับส่งข้อมูลด้วย ซึ่งแฟล็กมีอยู่ทั้งหมด 6 บิต แบ่งได้ดังนี้

ตารางที่ 2.6 แสดงชนิดของแฟล็ก

Type	Description
URG	ใช้บอกความหมายเป็นข้อมูลด่วน และมีข้อมูลพิเศษมาด้วย (อยู่ใน Urgent pointer)
ACK	แสดงว่าข้อมูลในฟิลด์ Acknowledge Number นำมาใช้งานได้
DSH	เป็นการแจ้งให้ผู้รับข้อมูลทราบว่าควรส่งข้อมูล Segment นี้ไปยัง Application ที่กำลังรออยู่โดยเร็ว
RST	ยกเลิกการติดต่อ (reset) เนื่องจากในกรณีที่เกิดการสับสนขึ้นด้วยเหตุผลต่างๆ

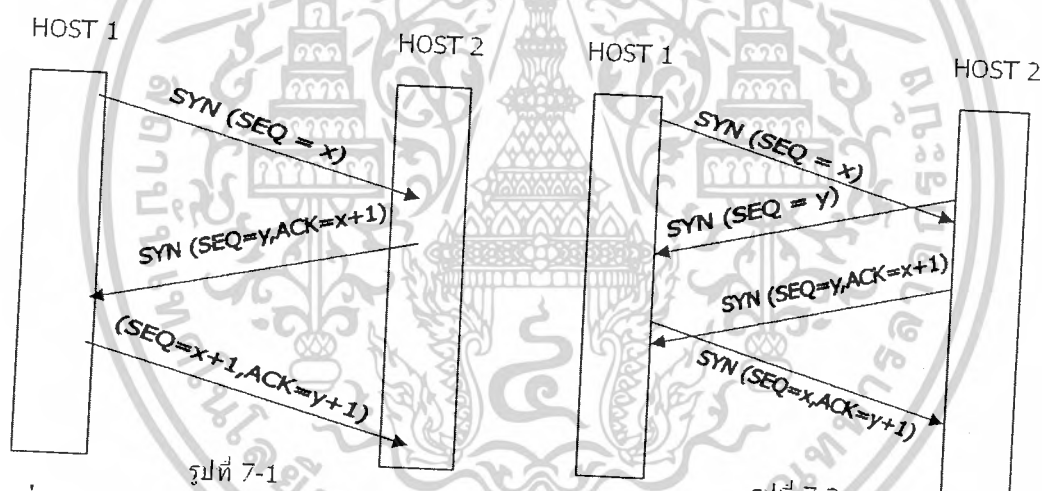
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 2.6 (ต่อ) แสดงชนิดของแพ็กจ

SYN	ใช้ในการเริ่มต้นขอติดต่อกับปลายทาง
FIN	ใช้ส่งเพื่อแจ้งให้ปลายทางทราบว่ายุติการติดต่อ

แพ็กจในเฮดเดอร์ของทีซีพีมีความสำคัญในการกำหนดการทำงานของทีซีพีเสกเมนต์ เนื่องจากข้อมูลในเฮดเดอร์ของทีซีพี จะมีข้อมูลครบถ้วนทั้งการรับและการส่งข้อมูล ซึ่งในการทำงานแต่ละอย่างจะมีการใช้งานฟิลด์ไม่เหมือนกันแพ็กจจะเป็นตัวกำหนดว่าให้ใช้งานฟิลด์ไหน เช่น ฟิลด์หมายเลขของการตอบรับ (Acknowledgment number) จะไม่ถูกใช้ในขั้นตอนการเริ่มต้นการเชื่อมต่อ แต่จะมีข้อมูลในฟิลด์ซึ่งเป็นข้อมูลที่ไม่มีความหมายใดๆ ซึ่งถ้าไม่มีแพ็กจเป็นตัวกำหนดก็อาจจะมีการนำข้อมูลมาใช้ และก่อให้เกิดความผิดพลาดได้

การสื่อสารของ ทีซีพี



รูปที่ 2.8 แสดงลำดับขั้นตอนการส่งทีซีพีเซกเมนต์และการเชื่อมต่อระหว่างซ็อกเก็ตคู่เดียวกัน

เมื่อเซกเมนต์คอนเนก (SYN = "1" และ ACK = "0") เดินทางมาถึงเอนดตี้ ทีซีพี ที่โฮสต์ปลายทางจะค้นหาโปรเซสตามหมายเลขพอร์ตที่กำหนดในเขตข้อมูลพอร์ตปลายทาง ซึ่งถ้าหากไม่พบก็จะตอบปฏิเสธด้วยเซกเมนต์ที่มีอาร์เอสที="1"กลับไปยังผู้ส่งเซกเมนต์คอนเนกของผู้ส่งจะถูกส่งต่อไปยังโปรเซส ตามพอร์ตที่ระบุซึ่งอาจจะตอบรับหรือตอบปฏิเสธก็ได้ ถ้าโปรเซสนั้นต้องการสื่อสารด้วยก็จะส่งเซกเมนต์ตอบรับกลับไป รูปที่ 2.8 แสดงลำดับขั้นตอนการส่ง ทีซีพีเซกเมนต์ในการสร้างการเชื่อมต่อในสภาวะปกติระหว่างผู้ส่งและผู้รับ

ในกรณีที่โฮสต์สองแห่งพยายามสร้างการเชื่อมต่อระหว่างซ็อกเก็ตคู่เดียวกันจะเกิดเป็นลำดับขั้นตอนแสดงในรูปที่ 2.9 ผลสุดท้ายจะมีการเชื่อมต่อเกิดขึ้นเพียงหนึ่งช่องทางเท่านั้นเนื่องจากการเชื่อมต่อในแต่ละช่องทางจะถูกกำหนดขึ้นโดยใช้หมายเลขซ็อกเก็ตผู้ส่งและผู้รับ ถ้าการเชื่อมต่อไม่สำเร็จใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ลำดับแรกสำเร็จก็จะถูกบันทึกไว้ในตารางการสื่อสาร เช่น (x, y) ถ้าการเชื่อมต่อลำดับที่สองสำเร็จในเวลาต่อมา ข้อมูลนี้ก็จะถูกบันทึกไว้ที่เดียวกันคือ (x, y)

ขั้นตอนในการสร้างการเชื่อมต่อและการยกเลิกสามารถเขียนอธิบายด้วยไฟในทศตวรรษที่ 11 สถานะ ดังแสดงในตารางข้างล่าง ในแต่ละสถานะจะมีเหตุการณ์บางอย่างที่เป็นไปได้ซึ่งจะได้รับการตอบสนองด้วยการกระทำที่เหมาะสม ในทางตรงกันข้าม เหตุการณ์ที่เป็นไปไม่ได้จะกลายเป็นข้อผิดพลาดที่จะต้องรายงานให้ทราบ

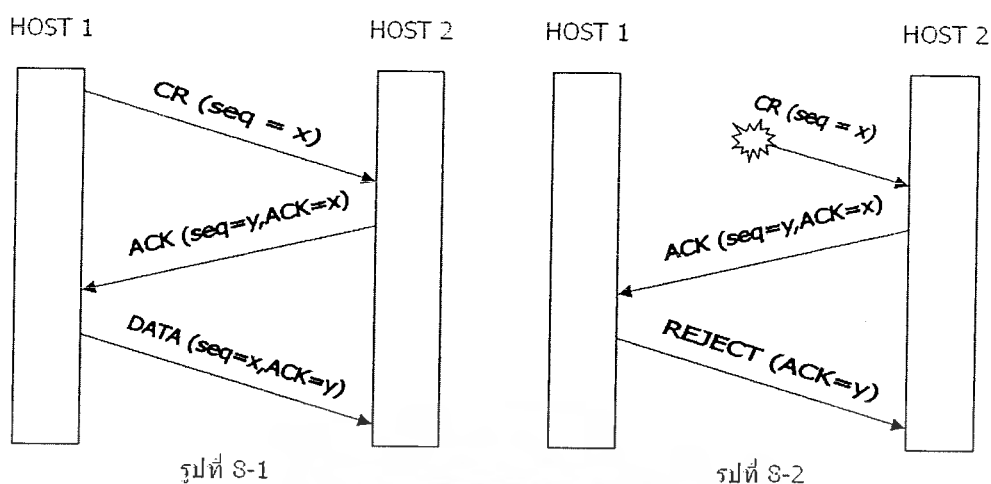
การเชื่อมต่อเริ่มต้นจากสถานะ ปิดเมื่อเรียกใช้บริการการรอรับฟัง(Listen) หรือ เชื่อมต่อ ก็จะมีการเปลี่ยนสถานะไปจากเดิม และถ้าอีกฝ่ายต้องการเชื่อมต่อด้วย การเชื่อมต่อก็จะเกิดขึ้นและย้ายไปอยู่ในสถานะสร้างการเชื่อมต่อ (ESTABLISHED) คือการเชื่อมต่อสมบูรณ์ และเมื่อยกเลิกการติดต่อก็จะกลับไปสู่สถานะปิดอย่างเดิม

การเริ่มต้นการสื่อสารของ ทีซีพี โดยใช้การบันทึกเวลาแบบทีเวย์แฮนเช็ค

ทีเวย์แฮนเช็คเป็นวิธีการส่งแพ็กเก็ตที่สามารถช่วยแก้ปัญหาในเรื่องแพ็กเก็ตซ้ำซ้อนได้ดี แต่วิธีนี้จำเป็นจะต้องสร้างช่องสื่อสารให้ได้ก่อนที่จะเริ่มรับ-ส่งข้อมูล อย่่างไรก็ตาม แพ็กเก็ตความคุมที่ใช้ในการต่อรองค่าตัวแปรสำหรับการสื่อสารต่างๆ อาจเกิดการตกค้างอยู่ในระบบได้ ทำให้การกำหนดค่าหมายเลขลำดับมีปัญหาไปด้วย เช่นการสร้างช่องสื่อสารระหว่าง โฮสต์1 และ โฮสต์2 เริ่มจากโฮสต์1 ขอเริ่มการเชื่อมต่อด้วยการส่งแพ็กเก็ตเชื่อมต่อ (Connection Request) ไปยังโฮสต์2 ซึ่งจะมีค่าตัวแปรต่างๆสำหรับการสื่อสารรวมทั้งหมายเลขลำดับและหมายเลขช่องสื่อสารไปด้วย ผู้รับคือ โฮสต์2 ก็จะส่ง ACK (Acknowledge) กลับมายังโฮสต์1 แต่ถ้าแพ็กเก็ตจากผู้ส่งเกิดสูญหายระหว่างทางและสำเนาแพ็กเก็ตที่ยังตกค้างอยู่ระบบเกิดเดินทางไปถึงผู้รับในภายหลังก็จะทำให้การสร้างช่องสื่อสารใช้การไม่ได้เนื่องจากมีค่าตัวแปรต่างๆไม่ตรงกัน

การใช้ ทีเวย์แฮนเช็คเป็นการไม่บังคับให้ผู้ส่งและผู้รับข้อมูลจะต้องกำหนดค่าเริ่มต้นของหมายเลขลำดับเป็นเลขเดียวกัน ทำให้สามารถนำวิธีนี้มาใช้ร่วมกับวิธีการจัดจังหวะการทำงานให้พร้อมกัน (Synchronization) แบบต่างๆ ได้แทนที่จะเป็นการใช้วิธีการบันทึกเวลา ดังรูปที่ 7-1 แสดงขั้นตอนการเริ่มต้นการทำงานจากโฮสต์ 1 ไปยังโฮสต์ 2 สมมุติให้โฮสต์ 1 เลือกหมายเลขลำดับเป็นเอ็ก และส่งแพ็กเก็ตการร้องขอการเชื่อมต่อ (CONNECTION REQUEST) ไปยังโฮสต์ 2 โฮสต์ 2 ตอบรับด้วยแพ็กเก็ตยอมรับการเชื่อมต่อ (CONNECTION ACCEPTED) ซึ่งจะยอมรับหมายเลขลำดับเอ็ก พร้อมกับประกาศหมายเลขลำดับอาร์ ที่เป็นของตนเอง จากนั้นโฮสต์ 1 ก็จะตอบรับค่าตัวเอ็กของโฮสต์ 2 ผ่านทางเขตข้อมูลสำหรับการควบคุมในแพ็กเก็ตข้อมูลแรกที่ส่งมา

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 8-1

รูปที่ 8-2

รูปที่ 2.9 แสดงเหตุการณ์ที่แพ็กเก็ตที่ผิดพลาด

สมมติว่าได้เกิดปัญหาการสูญหายของแพ็กเก็ตในขณะที่สำเนาแพ็กเก็ตที่ค้างในระบบเดินทางไปถึงผู้รับแทน รูปที่ 2.10 แสดงเหตุการณ์ที่แพ็กเก็ตที่ผิดพลาด (ตัวแรกในรูป) เป็นสำเนาแพ็กเก็ตเก่าที่เพิ่งจะเดินทางไปถึงโฮสต์ 2 โดยที่โฮสต์ 1 ไม่ทราบ โฮสต์ 2 ก็จะทำงานตามปกติคือจะตอบรับด้วยการส่งแพ็กเก็ต CONNECTION ACCEPTED TPDU กลับมา ที่โฮสต์ 1 ซึ่งโฮสต์ 1 จะสามารถตรวจสอบได้ว่า หมายเลขลำดับโฮสต์ 2 ตอบกลับมานั้นเป็นหมายเลขลำดับที่ได้เลิกใช้ไปแล้ว จึงมีการส่งแพ็กเก็ตการปฏิเสธ (REJECT) กลับมายังโฮสต์ 2 เพื่อบอกยกเลิกการทำงาน จะเห็นว่าวิธีการนี้อาศัยการสื่อสารผ่านแพ็กเก็ต 3 ตัว ซึ่งเป็นที่มาของคำว่า “การจับมือร่วมสามขั้นตอน” ผลสุดท้าย ทั้งโฮสต์ 1 และโฮสต์ 2 ก็จะไม่มีการสร้างช่องสื่อสารขึ้นมาจากข้อมูลในสำเนาแพ็กเก็ตเก่าแต่อย่างใด

4. ชั้นสื่อสารการประยุกต์ (Application Layer)

มีโพรโตคอลสำหรับสร้างจอเทอร์มินัลเสมือน เรียกว่า เทลเน็ต โพรโตคอลสำหรับการจัดการเพิ่มข้อมูล เรียกว่า FTP และโพรโตคอลสำหรับการให้บริการจดหมายอิเล็กทรอนิกส์ เรียกว่า เอสเอ็มทีพี โดยโพรโตคอลสำหรับสร้างจอเทอร์มินัลเสมือนช่วยให้ผู้ใช้สามารถติดต่อกับเครื่องโฮสต์ที่อยู่ไกลออกไปโดยผ่านอินเทอร์เน็ต และสามารถทำงานได้เสมือนกับว่ากำลังนั่งทำงานอยู่ที่เครื่องโฮสต์นั้น โพรโตคอลสำหรับการจัดการเพิ่มข้อมูลช่วยในการคัดลอกเพิ่มข้อมูลมาจากเครื่องอื่นที่อยู่ในระบบเครือข่ายหรือส่งสำเนาเพิ่มข้อมูลไปยังเครื่องใดๆก็ได้ โพรโตคอลสำหรับให้บริการจดหมายอิเล็กทรอนิกส์ช่วยในการจัดส่งข้อความไปยังผู้ใช้ในระบบ หรือรับข้อความที่มีผู้ส่งเข้ามา

2.5.3 การกำหนดค่าแอดเดรสต้นทางและปลายทาง

ประกอบด้วยตัวเลขฐานสอง 4 ไบท์ (32 bits) เวลาใช้เพื่อให้ง่ายต่อการเข้าใจ จะเขียนอยู่ในรูป เลขฐานสิบ ขึ้นด้วยจุด "." เมื่อแปลงเป็นเลขฐานสิบแล้ว แต่ละชุดจะมีตัวเลขระหว่าง 0-255 เช่น

192.168.1.1 เป็นต้น เรียกว่า ไอพีแอดเดรส โดยไอพีแอดเดรสที่เรียงต่อกันไป ซึ่งจะมี

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น เมื่อผู้ใดเห็นไปใช้โดยไม่ได้รับอนุญาต
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ความหมายดังนี้ แอดเดรสทั้งหมดที่อยู่ภายในเครือข่ายเดียวกันและมีตัวเลขเหมือนกัน เรียกว่า ส่วนของเครือข่าย(Network portion) ตัวเลขที่เหลือจะเรียกว่าส่วนของเจ้าของ (host portion) ตัวเลขที่ใช้ร่วมกัน สำหรับทุกแอดเดรสภายในเครือข่ายเรียกว่าเน็ตมาร์กและเน็ตมาร์กนี้ก็ใช้เป็น ตัวกำหนดว่าแอดเดรส ใดอยู่ภายในเครือข่าย หรือแอดเดรสใดไม่อยู่

ตารางที่ 2.7 แสดงหมายเลขแอดเดรส

ส่วนของเครือข่าย (Network Portion)	192.168.1.	ภายใน เครือข่าย นี้ ทุก แอดเดรส จะขึ้นต้นด้วยเลขนี้ เหมือนกันหมด
ส่วนของเจ้าของ (Host Portion)	.10	แต่ละ โฮสต์ ก็จะมีเลข ส่วนของเจ้าของ(Host Portion)เป็นของตัวเองไม่ซ้ำกัน
ที่อยู่ของ โฮสต์ (Host Address)	192.168.1.10	ส่วนของเครือข่าย(Network Portion)+ส่วนของเจ้าของ(Host Portion)
เน็ตเวิร์ก มาร์ก (netmask)	255.255.255.0	ทุก แอดเดรส ภายใน เครือข่าย เดียวกัน ต้องใช้ค่าเดียวกัน และ หมายเลขนี้ ก็จะแสดงให้เห็นว่า ภายใน เครือข่าย นี้มี ไบท์ รวมกัน ทั้งหมดกี่หมายเลข ในที่นี้จะมี 256 ไบท์
เน็ตเวิร์ก แอดเดรส	192.168.1.0	
บรอดคาสต์ แอดเดรส	192.168.1.255	

เครือข่ายคลาส

การแบ่ง ไอพีแอดเดรส ออกเป็นหลายระดับความจริงก็แบ่งตามความใหญ่ของเครือข่ายนั่นเอง

ตารางที่ 2.8 แสดงเน็ตเวิร์กแอดเดรสและเน็ตมาร์กของแต่ละเครือข่าย

เครือข่ายคลาส	เน็ตมาร์ก	เน็ตเวิร์ก แอดเดรส
เอ	255.0.0.0	0.0.0.0 - 127.255.255.255
บี	255.255.0.0	128.0.0.0 - 191.255.255.255
ซี	255.255.255.0	192.0.0.0 - 223.255.255.255
มัลติคลาส	240.0.0.0	224.0.0.0 - 239.255.255.255

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

คลาสเอเครือข่าย

ระบบเครือข่ายคลาส เอ มีแอดเดรสเริ่มต้นตั้งแต่ 0 จนถึง 127 เป็นส่วนของเครือข่าย(Network Portion) ตัวเลขที่เหลืออีกสามส่วนเป็นส่วนของเจ้าของ(host portion)ระบบเครือข่ายที่ใหญ่มากสามารถมีอุปกรณ์ (เราเตอร์, ส่วนของเจ้าของ(host)) ต่างๆ ไม่ซ้ำกันได้ถึง 16 ล้านตัว ระบบเครือข่ายคลาสเอได้ถูกกำหนดให้กับบริษัทต่างจนหมดไปนานแล้ว

คลาสบีเครือข่าย

มีแอดเดรสเริ่มตั้งแต่ 128 จนถึง 192 มีระบบเครือข่ายคลาส B อยู่ 16,000 เครือข่าย ในแต่ละเครือข่าย จะมีแอดเดรสที่ไม่ซ้ำกันอยู่ 64,000 แอดเดรส และก็ถูกกำหนดให้กับองค์กร หรือบริษัทใหญ่ๆ หมดแล้วเช่นกัน เหตุที่เครือข่ายนี้ไม่ใหญ่เท่า เครือข่ายคลาส A เนื่องจากถูกกำหนดโดย เน็ตมาร์ก

คลาสซีเครือข่าย

มีแอดเดรสเริ่มตั้งแต่ 192 จนถึง 223 ซึ่งมีอยู่ประมาณ 2 ล้านเครือข่าย แต่ละเครือข่ายมีอุปกรณ์ได้สูงสุด 254 ตัว

มัลติคลาส

หรืออาจเรียกได้ว่าเป็น เครือข่ายคลาส ดี มีแอดเดรสเริ่มต้นตั้งแต่ 224 จนถึง 239 สำหรับใช้งานในลักษณะเหมือนกับวิทยุหรือโทรทัศน์คือส่งออกไปอย่างเดียว ใครจะรับก็ไปดักรับเอา ส่วนแอดเดรส 240 ถึง 247 เป็นของระบบเครือข่ายคลาส อี ซึ่งในส่วนนี้เก็บไว้ใช้ในอนาคต

สับเน็ต

เป็นส่วนหนึ่งของระบบเครือข่าย ซึ่งเหมือนกับแยกตัวออกมาต่างหาก แต่จะมีจุดเชื่อมต่อเพียงจุดเดียวโดยผ่าน เราเตอร์ สิ่งที่จะช่วยให้เราแยกตัวออกมาจากเครือข่าย คือ สับเน็ต มาร์กแต่คอมพิวเตอร์ในสับเน็ตมาร์กเดียวกันสามารถติดต่อกันได้โดยตรง ตัวอย่างมาร์สของเครือข่ายคลาสซี คือ 255.255.255.0 ขอยกตัวอย่างให้ดูเช่น ไอพีแอดเดรส ของคอมพิวเตอร์เครื่องหนึ่งเป็น 192.168.1.20 คอมพิวเตอร์เครื่องนี้ก็จะสามารถติดต่อกับคอมพิวเตอร์ที่มีไอพีตั้งแต่ 192.168.1.0 - 192.168.1.255 จะไม่สามารถติดต่อกับเครื่องคอมพิวเตอร์ 192.168.2.1 ได้เลยเพราะอยู่คนละสับเน็ต

2.5.4 การเซตค่าพอร์ต

ทีซีพี/ไบท์ พอร์ตนัมเบอร์ หมายเลขพอร์ตจะเป็น ตัวเลขที่ไม่กำหนดค่า(Unsigned Numbers) แบบ 16 บิต จะมีพอร์ตได้ทั้งหมด 65536 (0-65535)

- พอร์ตที่รู้จัก (0 - 1023)
- พอร์ตที่จดทะเบียนไว้แล้ว (1024 - 49151)
- พอร์ตที่เปลี่ยนแปลงค่าได้ (49152 - 65535)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

พอร์ตที่รู้จัก (0-1023) จะเป็นพอร์ตสำหรับ แอปพลิเคชันต่างๆ เช่น

- ที่ซีพี 20 and 21 (File Transfer Protocol, FTP)
- ที่ซีพี 22 (Secure Shell, SSH)
- ที่ซีพี 23 (Telnet)
- ที่ซีพี 25 (Simple Mail Transfer Protocol, SMTP)
- ที่ซีพี and ยูดีพี 53 (Domain Name System, ดีเอ็นเอส)
- ยูดีพี 69 (Trivial File Transfer Protocol, tftp)
- ที่ซีพี 79 (finger)
- ที่ซีพี 80 (Hypertext Transfer Protocol, HTTP)
- ที่ซีพี 110 (Post Office Protocol v3, POP3)
- ที่ซีพี 119 (Network News Protocol, NNTP)
- ยูดีพี 161 and 162 (Simple Network Management Protocol, SNMP)
- ยูดีพี 443 (Secure Sockets Layer over HTTP, https)

พอร์ตที่ไม่รับมาตรฐานหมายถึงพอร์ตที่มีหมายเลขมากกว่า 1023 ดังตัวอย่าง

- วินส์ 1512/ที่ซีพี # Microsoft Windows Internet Name Service
- เรเดียส 1812/ยูดีพี # RADIUS authentication protocol
- ยาฮู 5010 # Yahoo! Messenger
- x11 6000-6063/ที่ซีพี # X Window System

บทที่ 3

วิเคราะห์และออกแบบระบบ

3.1 ขั้นตอนการวิเคราะห์และออกแบบระบบปฏิบัติการ

ในส่วนของระบบไฟร์วอลล์มีการออกแบบเป็นระบบแบบฝังตัว โดยคำนึงถึงความเสถียรและการเพิ่มประสิทธิภาพในการตอบสนองของระบบการออกแบบเริ่มต้น โดยการเลือกระบบปฏิบัติการที่จะนำมาใช้ซึ่งในโครงการนี้ได้เลือกใช้ระบบปฏิบัติการฟรีบีเอสดีเวอร์ชัน 4 ขึ้นไป ซึ่งฟรีบีเอสดีเป็นระบบปฏิบัติการที่มีความมั่นคงปลอดภัยและใช้กันแพร่หลายในการทำเว็บเซิร์ฟเวอร์

หลังจากเลือกระบบปฏิบัติการแล้วก็ทำการเลือกอุปกรณ์ที่จะนำมาบันทึกในระบบไฟร์วอลล์เนื่องจากโครงการนี้มีขึ้นเพื่อวัตถุประสงค์จะทำอุปกรณ์ด้านความปลอดภัยในสำนักงานที่มีราคาถูก การเลือกอุปกรณ์จึงอยู่บนพื้นฐานของประสิทธิภาพและราคาเป็นหลัก ในโครงการนี้เลือกจะใช้คอมแพคแฟลชการ์ดซึ่งมีราคาไม่แพงมาก และมีความจำที่พอดี ประมาณ 512 เมกะไบต์หรือมากกว่า เพื่อให้สามารถติดตั้งระบบปฏิบัติการและส่วนอินเตอร์เฟสที่เกี่ยวข้องทั้งหมดได้

การออกแบบระบบปฏิบัติการนี้จะเน้นให้มีขนาดเล็กที่สุดเพื่อให้มีความเสถียรและสามารถเพิ่มเติมคอมโพเนนต์ได้อย่างอิสระ ในโครงการนี้จะนำระบบปฏิบัติการฟรีบีเอสดีมาปรับปรุงโดยวิธีการดังต่อไปนี้

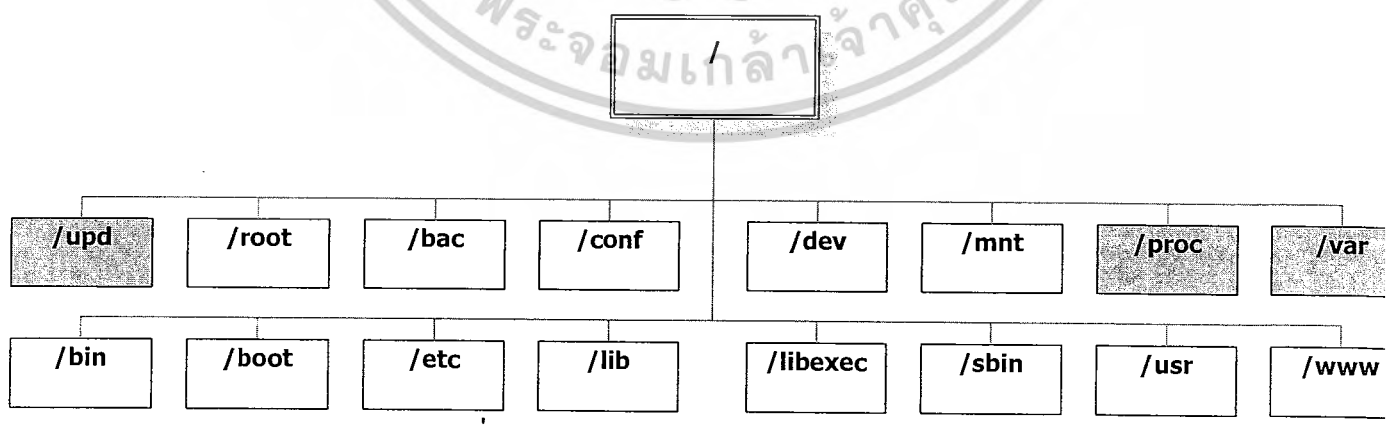
1. ทำการติดตั้งระบบปฏิบัติการฟรีบีเอสดีทั้งหมดลงในคอมพิวเตอร์
2. เลือกระบบการติดตั้งให้เป็นแบบเล็กที่สุด
3. เลือกการติดตั้งซอร์สโค้ด โดยมีโค้ดของระบบและไลบรารีที่เกี่ยวข้อง
4. ทำการติดตั้งระบบฟรีบีเอสดีให้อยู่ในโฟลเดอร์ /usr/jail
5. ทำการเปลี่ยนไฟล์ระบบใน โฟลเดอร์ให้กลายเป็นแบบอ่านเท่านั้น
6. ทำการติดตั้งเซลล์ต่างๆเพื่อให้ระบบมีความเสถียรเช่นเดียวกับระบบปฏิบัติการตัวเต็ม
7. ทำการติดตั้งเว็บเซิร์ฟเวอร์เพื่อให้สามารถสร้างหน้าเว็บเป็นอินเตอร์เฟสได้

ในส่วนการออกแบบระบบนั้น เมื่อคำนึงถึงความเสถียรและขนาดเล็ก จึงมีไคเรคทอรีที่สร้างขึ้นมาดังต่อไปนี้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

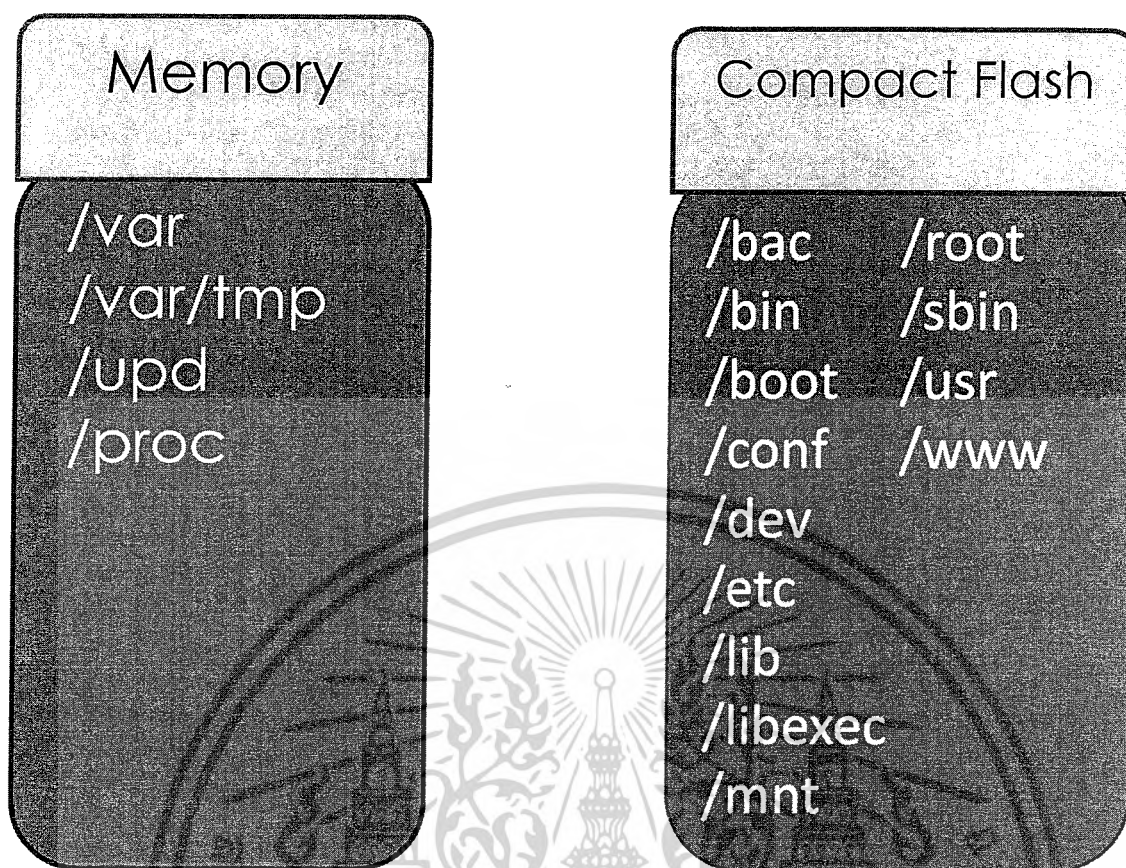
คำอธิบายของแต่ละไดเรกทอรีเป็น ดังนี้

- / เป็นไดเรกทอรีรากของฟรีบีเอสดี ไดเรกทอรีย่อยและไฟล์ต่างๆจะอยู่ภายใต้ไดเรกทอรีนี้
- /upd ใช้สำหรับทำการอัปเดต ระบบทั้งเคอร์เนลคอนฟิกและยูทิลิตี้ต่างๆ
- /root ใช้สำหรับเริ่มต้นระบบในการทำงานของผู้ใช้ root
- /bac ใช้สำหรับ backup ทั้ง config หรือ ไฟล์งานขนาดเล็ก
- /conf ใช้เก็บ config ของระบบ ซึ่งเป็นส่วนเพิ่มเติมจาก /etc
- /dev ใช้เก็บอุปกรณ์ในระบบที่สามารถทำการ mount ขึ้นมาใช้งานได้
- /mnt เป็นพื้นที่สำหรับ mount อุปกรณ์และไฟล์งานบางชนิด
- /proc ใช้สำหรับเป็นแหล่งรวม process thread ,บอกร state ของเคอร์เนลที่ทำงานอยู่
- /var เป็นไดเรกทอรีที่เก็บข้อมูลที่เปลี่ยนแปลงตลอดเวลาจากการเซตอัพต่างๆ
- /bin เก็บคำสั่งทั่วไปและไฟล์ที่เป็นไบนารี
- /boot เก็บเคอร์เนลของระบบและไฟล์ที่ใช้บูตระบบ
- /etc เก็บไฟล์ข้อมูลประเภท configuration และไดเรกทอรีย่อยหลักๆในการเซตอัพระบบ การดูแลระบบของ root
- /lib เก็บไลบรารีต่างๆที่ใช้ของระบบ
- /libexec เก็บไลบรารีต่างๆที่ใช้ของระบบ
- /sbin ใช้เก็บคำสั่งในการดูแลระบบจำพวก system binary file เป็น ไฟล์ที่ใช้ในการ Startup และ Shutdown ระบบ ต่างจากใน /bin
- /usr เป็นไดเรกทอรีที่เก็บ ไดเรกทอรีย่อยในการเซตอัพระบบหลายตัวด้วยกัน เช่น /usr/bin /usr/include /usr/lib /usr/local /usr/sbin
- /www ใช้สำหรับเก็บส่วนของหน้าเว็บ



รูปที่ 3.1 แสดงแผนภาพสถาปัตยกรรมของระบบ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 3.2 แสดงแผนภาพสถาปัตยกรรมของระบบ

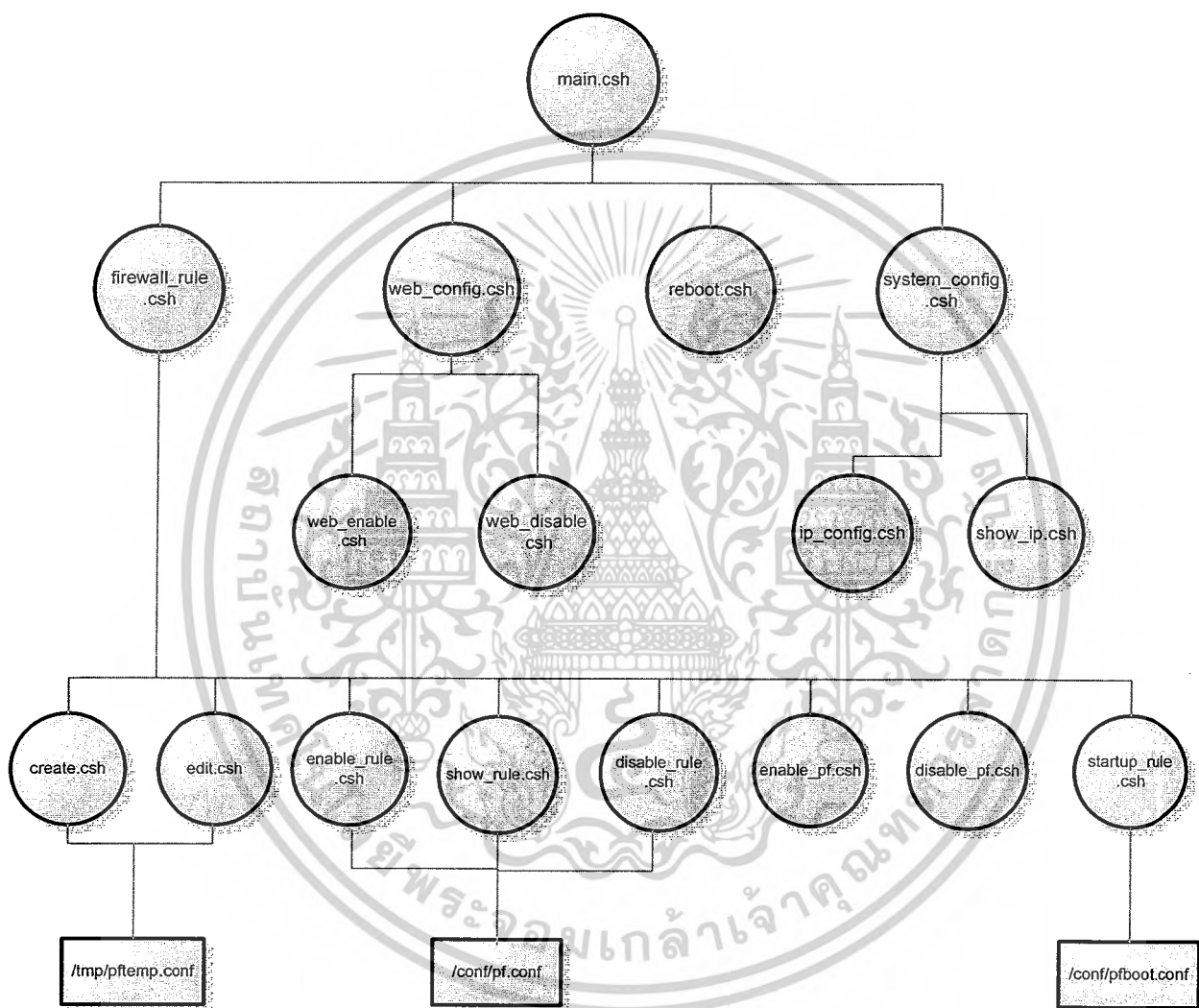
3.2 ขั้นตอนการออกแบบคอมพิวเตอร์ออนไลน์

เนื่องจากในระบบคอมพิวเตอร์ออนไลน์ของการทำการแก้ไขค่าที่เกี่ยวข้องกับไฟร์วอลล์ที่ใช้อยู่เดิมนั้นยังใช้งานอย่างยุ่งยากอยู่ ผู้ใช้ต้องมีความรู้และความเข้าใจเกี่ยวกับรูปแบบของไวยากรณ์จึงจะสามารถทำการแก้ไขกฎต่างๆให้สามารถทำงานได้ดี อีกทั้งชุดคำสั่งที่เรียกใช้งานแอปพลิเคชันที่เกี่ยวข้องกับการตั้งค่าไฟร์วอลล์นั้นเป็นคำสั่งที่ผู้ใช้ต้องมีการจดจำชุดคำสั่งและในการเรียกใช้แต่ละครั้งต้องมีการพิมพ์คำสั่งที่ยืดยาว ทางผู้พัฒนาระบบจึงคิดที่จะทำการใช้งานระบบไฟร์วอลล์ผ่านคอมพิวเตอร์ให้ง่ายต่อการใช้งานและรวดเร็วยิ่งขึ้น อีกทั้งยังไม่ต้องมีการจดจำชุดคำสั่งที่ยุ่งยาก โดยให้การทำงานผ่านคอมพิวเตอร์นั้นเป็นแบบเมนู ผู้ใช้เพียงแค่เลือกหมายเลขตามที่ระบุไว้ก็สามารถทำงานได้อย่างรวดเร็ว ผู้ที่ไม่เคยใช้งานระบบมาก่อนก็สามารถที่จะใช้งานระบบโดยใช้คอมพิวเตอร์อินเทอร์เน็ตได้โดยไม่ยุ่งยาก โดยหลักการออกแบบมีทั้งหมด 5 ขั้นตอนดังนี้

1. เลือกเครื่องมือที่ใช้ในการเขียนชุดคำสั่ง ซึ่งจะมีการนำหลักของการเขียนเซลล์สคริปต์มาใช้งาน โดยเซลล์ที่เลือกมาใช้นั้นเป็น ซีเซลล์ ซึ่งนิยมใช้กับระบบปฏิบัติการพีวีเอสดี
2. ศึกษาวิธีการเขียนสคริปต์ไฟล์เพื่อที่จะได้เข้าใจและรู้ถึงวิธีที่จะออกแบบชุดคำสั่งให้ง่ายต่อการใช้งานของผู้ใช้มากที่สุด

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3. ขั้นตอนในส่วนของการวิเคราะห์และออกแบบ จะทำการวิเคราะห์ว่าควรจะมีสคริปต์ไฟล์ใดที่ใช้ทำงานในระบบบ้าง ซึ่งต้องคำนึงถึงการใช้งานที่ครอบคลุมและเพียงพอต่อการใช้งานในระบบ ต่อมาก็เป็นการออกแบบให้สคริปต์ไฟล์ต่างๆที่ใช้ทำงานในระบบทำงานอย่างไร ซึ่งจากการออกแบบนั้นจะกำหนดให้เริ่มต้นจากสคริปต์ที่ชื่อ main.csh แล้วมีการเรียกใช้งานเป็นลำดับขั้นต่อไปตามความต้องการของผู้ใช้งานระบบ



รูปที่ 3.3 แสดงแผนภาพการทำงานของสคริปต์ไฟล์ของระบบเป็นลำดับขั้น

4. จากรูปที่ 3.3 จะมีการออกแบบโมดูลที่ใช้ในระบบเป็น 4 โมดูลใหญ่ๆ คือ

4.1 ไฟร์วอลล์โมดูล เป็นส่วนที่ใช้กำหนด ตั้งค่ากฎที่ใช้จัดการในส่วนของ การปิดกั้นแพคเกจต่างๆที่ผ่านเข้ามาในระบบ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4.2 เว็บอินเตอร์เฟซคอนฟิกูเรชัน เป็นส่วนที่ใช้จัดการกับเว็บอินเตอร์เฟซ โดยจะมีในส่วนของการทำงานเว็บอินเตอร์เฟซ เพื่อช่วยในเรื่องของความปลอดภัยภายในระบบ

4.3 การรีบูทระบบ จะจัดการรีบูทระบบเมื่อต้องการโหลดค่าต่างๆที่เป็นดีฟอลท์ของระบบขึ้นมาใช้งาน

4.4 การจัดการส่วนต่างๆของระบบ เป็นส่วนที่ใช้ในการตั้งค่าต่างๆที่เกี่ยวข้องในระบบ ไม่ว่าจะเป็นการแสดงผลและเปลี่ยนแปลงค่าของอินเตอร์เฟซที่ใช้

5. ออกแบบตำแหน่งของไฟล์ที่ใช้ในการจัดเก็บกฎทั้งหมดของระบบ ดังนี้

5.1 เทมพ์ไฟล์ (Temp file) จะทำการแก้ไขเปลี่ยนแปลงค่าที่ไฟล์ตัวนี้ก่อนที่จะนำไปใช้จริง (ตำแหน่งไฟล์ /tmp/pftemp.conf) ซึ่งที่เก็บไว้ในไดเรกทอรี /tmp นั้นเนื่องจากเป็นไดเรกทอรีที่เป็นเมมโมรีดิสก์ (memory disk) คือ เป็นค่าที่เก็บอยู่ในเมมโมรีค่าที่เราเปลี่ยนแปลงแก้ไขนั้นก็ยังคงอยู่จนกระทั่งปิดเครื่องหรือไฟดับนั่นเอง จึงสามารถแก้ไขค่าได้ตลอดเวลาโดยไม่ต้องผ่านการเพอร์มิสชัน (permission)

5.2 ไฟล์ pf.conf เป็นไฟล์ที่ใช้เก็บกฎที่จะนำไปใช้งานจริงๆ ซึ่งเราไม่สามารถเปลี่ยนแปลงแก้ไขได้จากไฟล์นี้โดยตรง ต้องทำการแก้ไขที่เทมพ์ไฟล์ (Temp file) ก่อนแล้วจึงค่อยเพิ่มเข้าไปในไฟล์นี้ได้ (ตำแหน่ง /conf/pf.conf) โดยก่อนที่จะทำการนำค่าจาก เทมพ์ไฟล์ (Temp file) มาแทนที่ไฟล์ pf.conf ต้องมีการเปลี่ยนเพอร์มิสชัน(permission) ของไดเรกทอรี /conf เสียก่อน จากอ่านเท่านั้น (Read-only) ไปเป็นอ่านและเขียน (Read-Write) ด้วยคำสั่ง

```
/umount /conf/
```

```
/mount -w /dev/ad0e /conf/
```

และเมื่อเราทำการเขียนไฟล์เรียบร้อยแล้ว ก็ต้องทำการเปลี่ยนเพอร์มิสชัน(permission) กลับไปเป็นอ่านเท่านั้น (Read-only) เหมือนเดิม ด้วยคำสั่ง

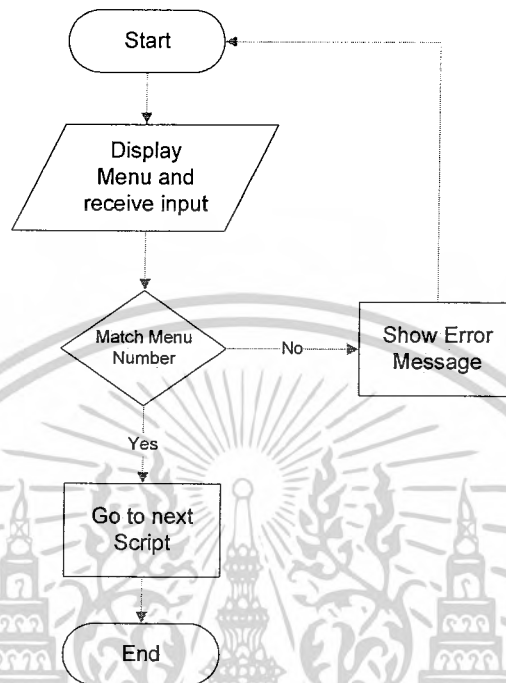
```
/umount /conf/
```

```
/mount -r /dev/ad0e /conf/
```

5.3 ไฟล์ pfboot.conf เป็นไฟล์ที่ใช้เก็บกฎที่เปรียบเสมือนเป็นดีฟอลท์ของระบบ ซึ่งเราสามารถที่จะเปลี่ยนแปลงค่าในส่วนนี้ได้ผ่านสคริปต์ startup.csh ซึ่งกฎในส่วนนี้จะถูกนำมาใช้งานก็ต่อเมื่อผู้ใช้ระบบสั่งให้มีการนำไฟล์นี้ไปแทนที่ไฟล์ pf.conf ซึ่งการจะนำไฟล์ไปแทนที่ได้นั้นก็ต้องมีขั้นตอนการเปลี่ยนเพอร์มิสชัน (permission) ก่อน เหมือนกับข้อ 5.2 นั่นเอง

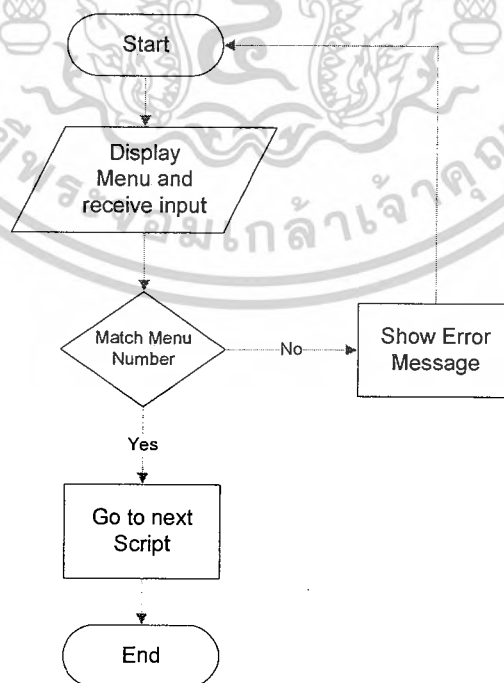
3.2.1 แผนภาพอธิบายลำดับการทำงานของสคริปต์ไฟล์

3.2.1.1 แผนภาพอธิบายลำดับการทำงานของสคริปต์ main.csh



รูปที่ 3.4 แผนภาพแสดงลำดับการทำงานของสคริปต์ main.csh

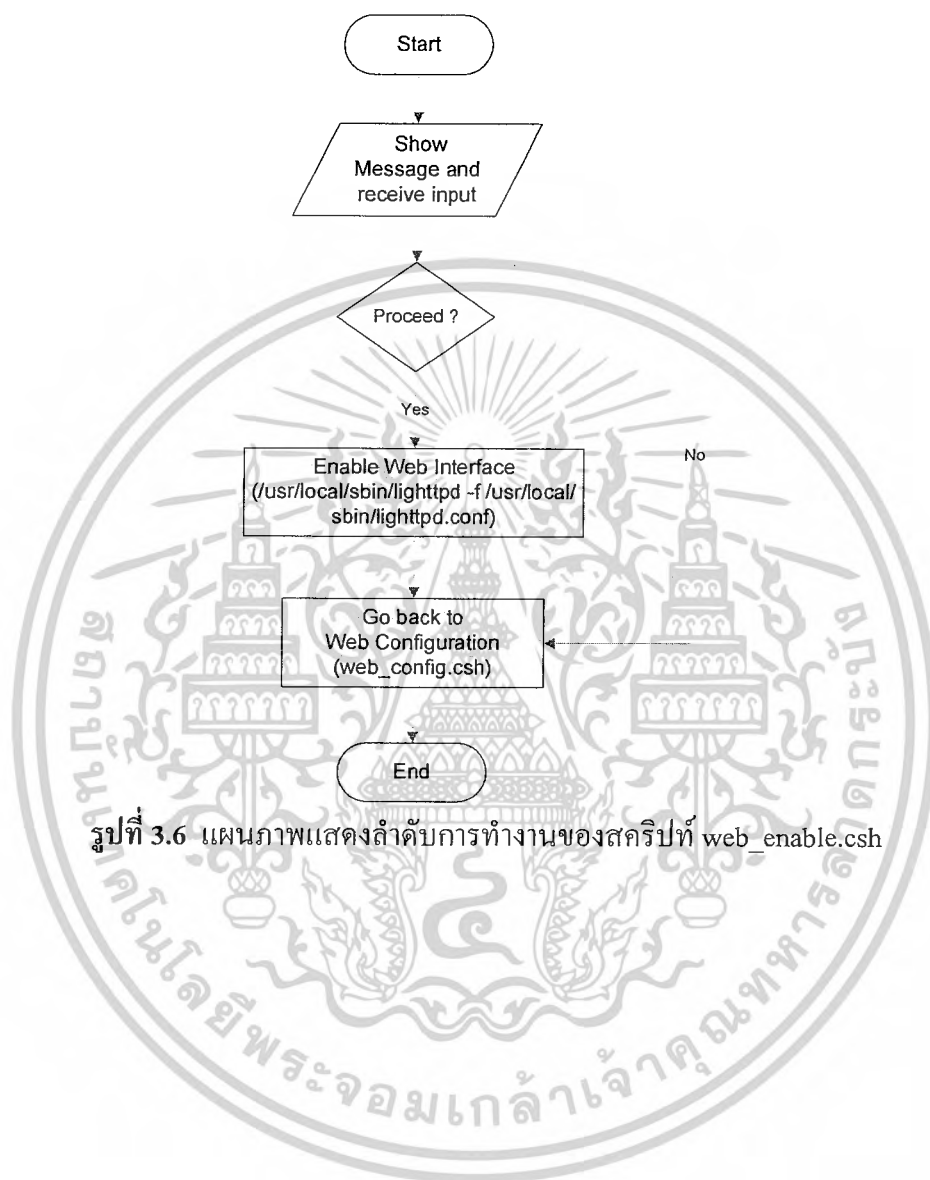
3.2.1.2 แผนภาพอธิบายลำดับการทำงานของสคริปต์ web_config.csh



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

รูปที่ 3.5 แผนภาพแสดงลำดับการทำงานของสคริปต์ web_config.csh

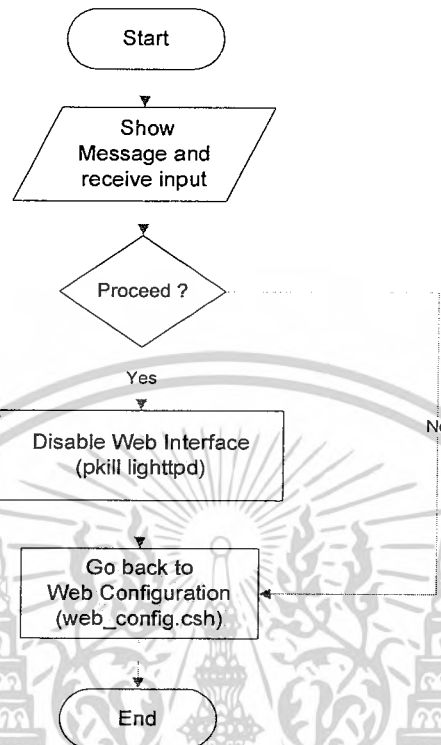
3.2.1.3 แผนภาพอธิบายลำดับการทำงานของสคริปต์ web_enable.csh



รูปที่ 3.6 แผนภาพแสดงลำดับการทำงานของสคริปต์ web_enable.csh

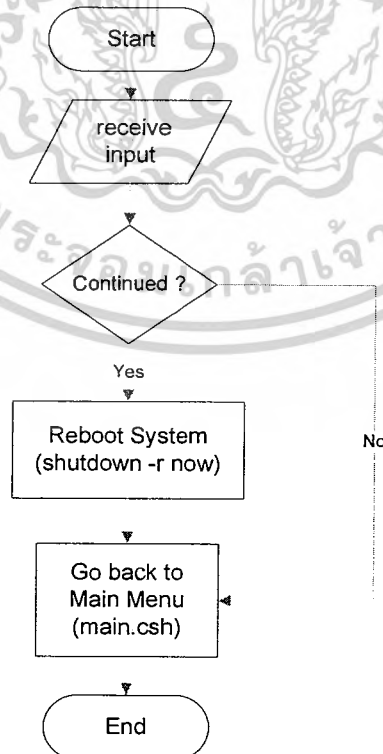
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.2.1.4 แผนภาพอธิบายลำดับการทำงานของสคริปต์ web_disable.csh



รูปที่ 3.7 แผนภาพแสดงลำดับการทำงานของสคริปต์ web_disable.csh

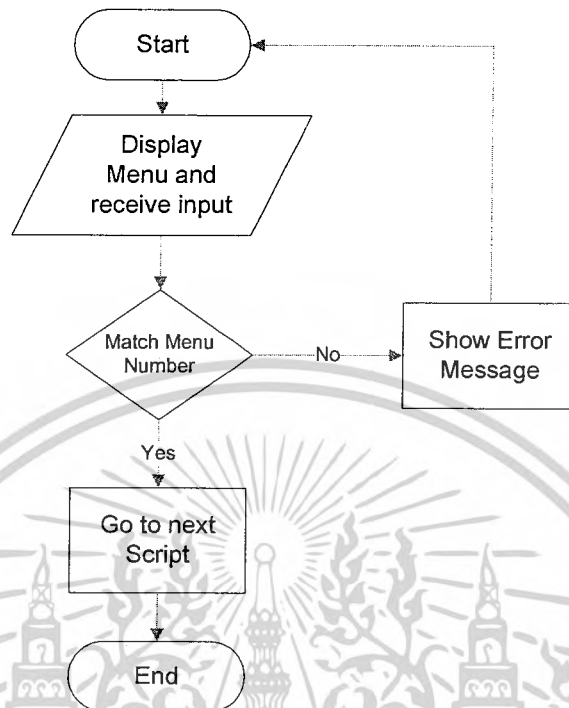
3.2.1.5 แผนภาพอธิบายลำดับการทำงานของสคริปต์ reboot.csh



รูปที่ 3.8 แผนภาพแสดงลำดับการทำงานของสคริปต์ reboot.csh

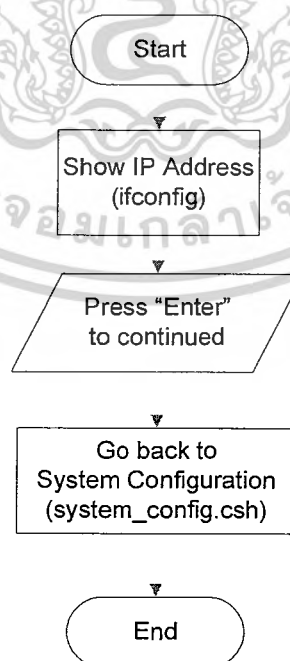
เอกสารนี้เป็นเอกสารที่สงวนลิขสิทธิ์ไว้เพื่อใช้ในหน่วยงานที่รับผิดชอบดูแลระบบคอมพิวเตอร์ของศูนย์วิจัยและพัฒนาระบบสารสนเทศของมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง ไม่ว่าจะกรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.2.1.6 แผนภาพอธิบายลำดับการทำงานของสคริปต์ system_config.csh



รูปที่ 3.9 แผนภาพแสดงลำดับการทำงานของสคริปต์ system_config.csh

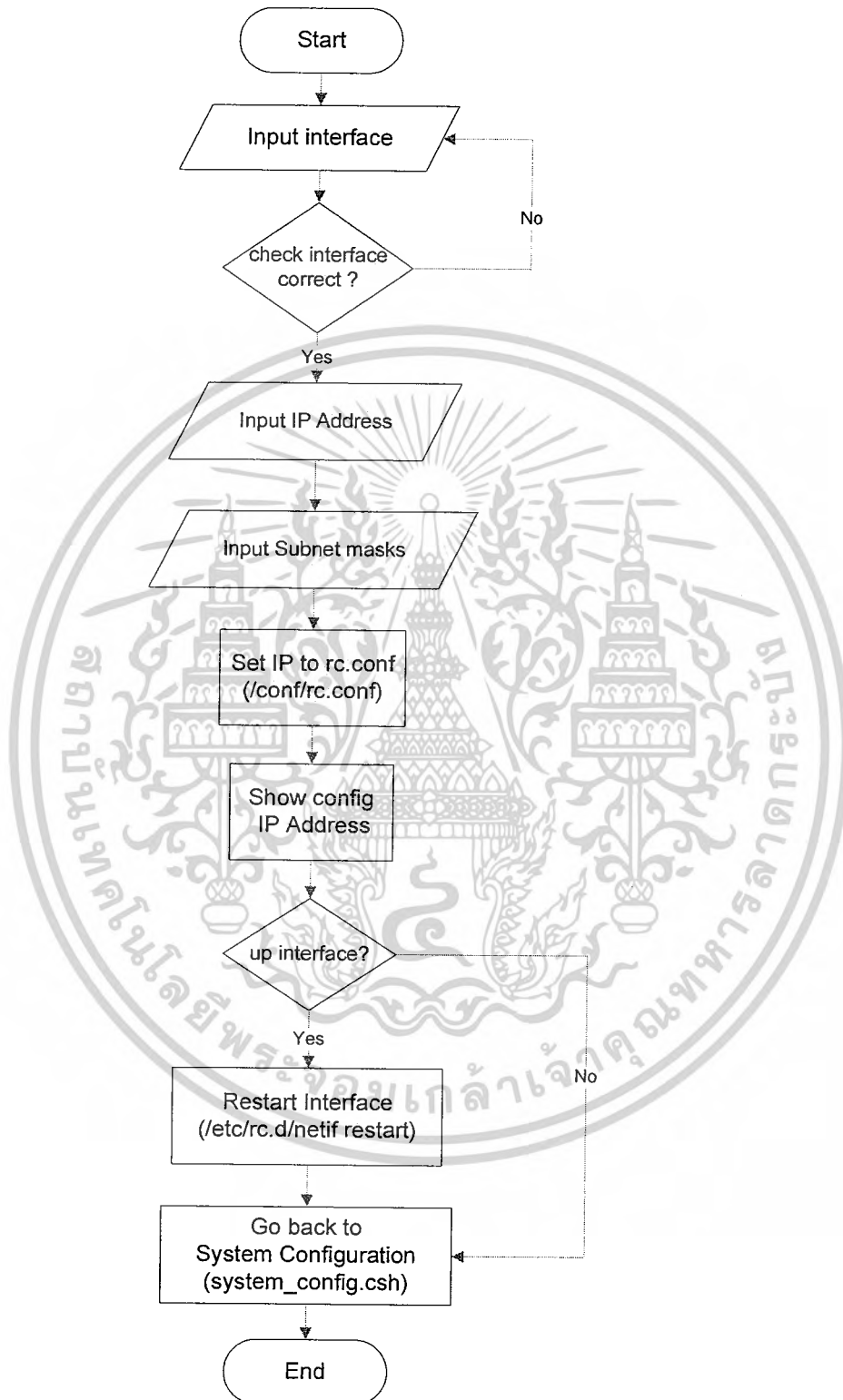
3.2.1.7 แผนภาพอธิบายลำดับการทำงานของสคริปต์ show_ip.csh



รูปที่ 3.10 แผนภาพแสดงลำดับการทำงานของสคริปต์ show_ip.csh

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

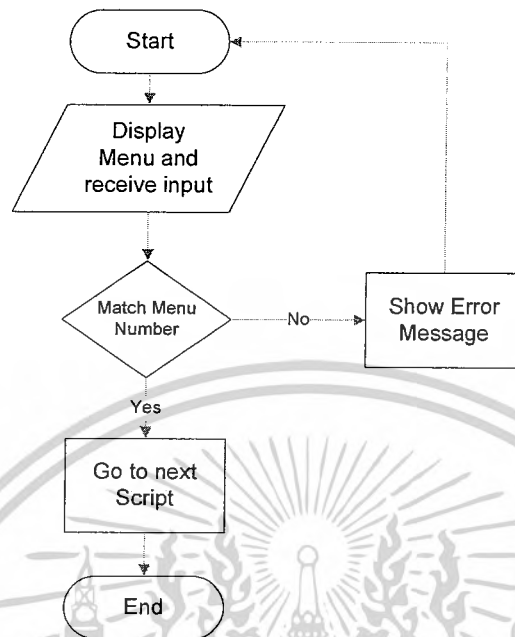
3.2.1.8 แผนภาพอธิบายลำดับการทำงานของสคริปต์ ip_config.csh



รูปที่ 3.11 แผนภาพแสดงลำดับการทำงานของสคริปต์ ip_config.csh

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

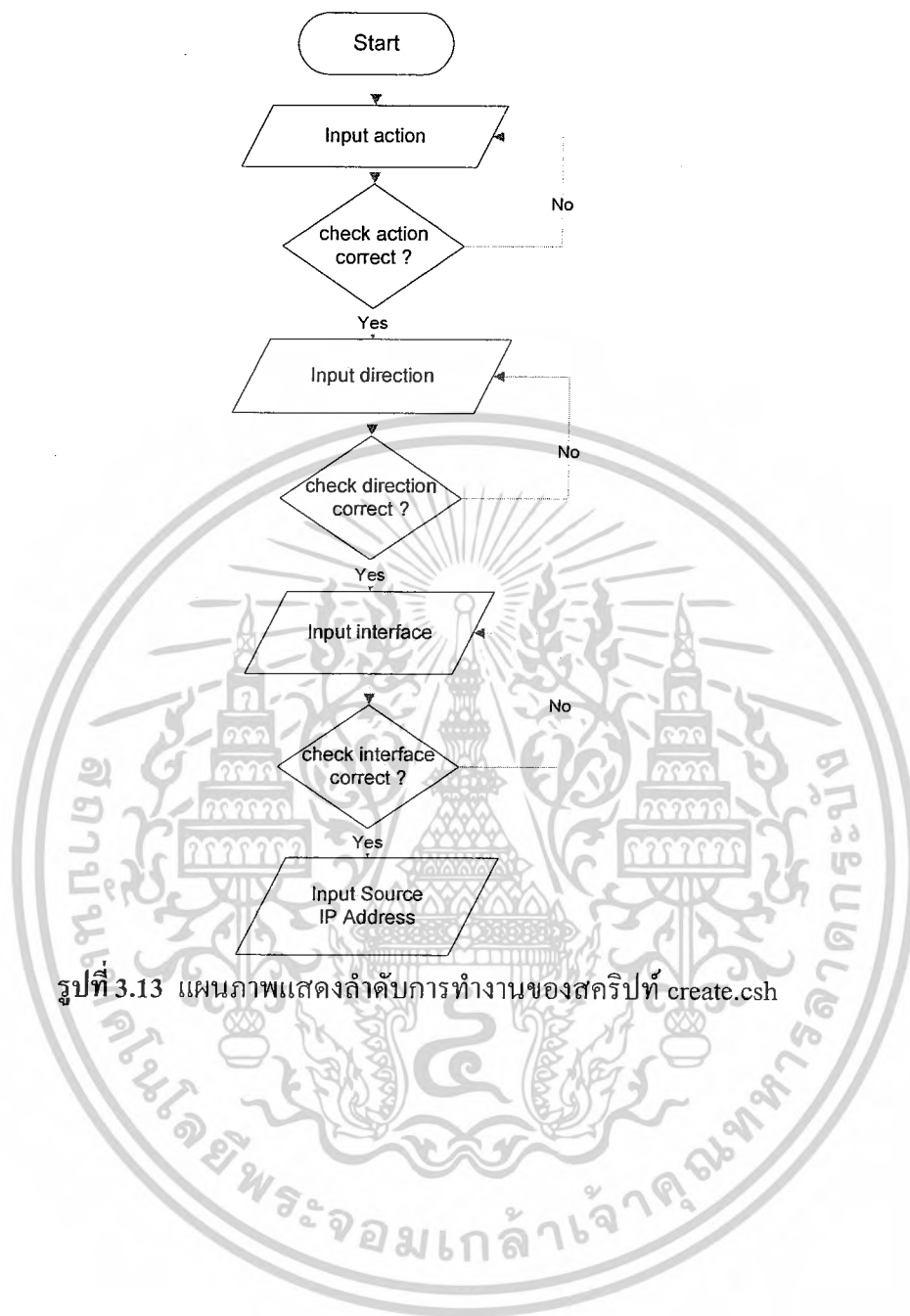
3.2.1.9 แผนภาพอธิบายลำดับการทำงานของสคริปต์ firewall_rule.csh



รูปที่ 3.12 แผนภาพแสดงลำดับการทำงานของสคริปต์ firewall_rule.csh

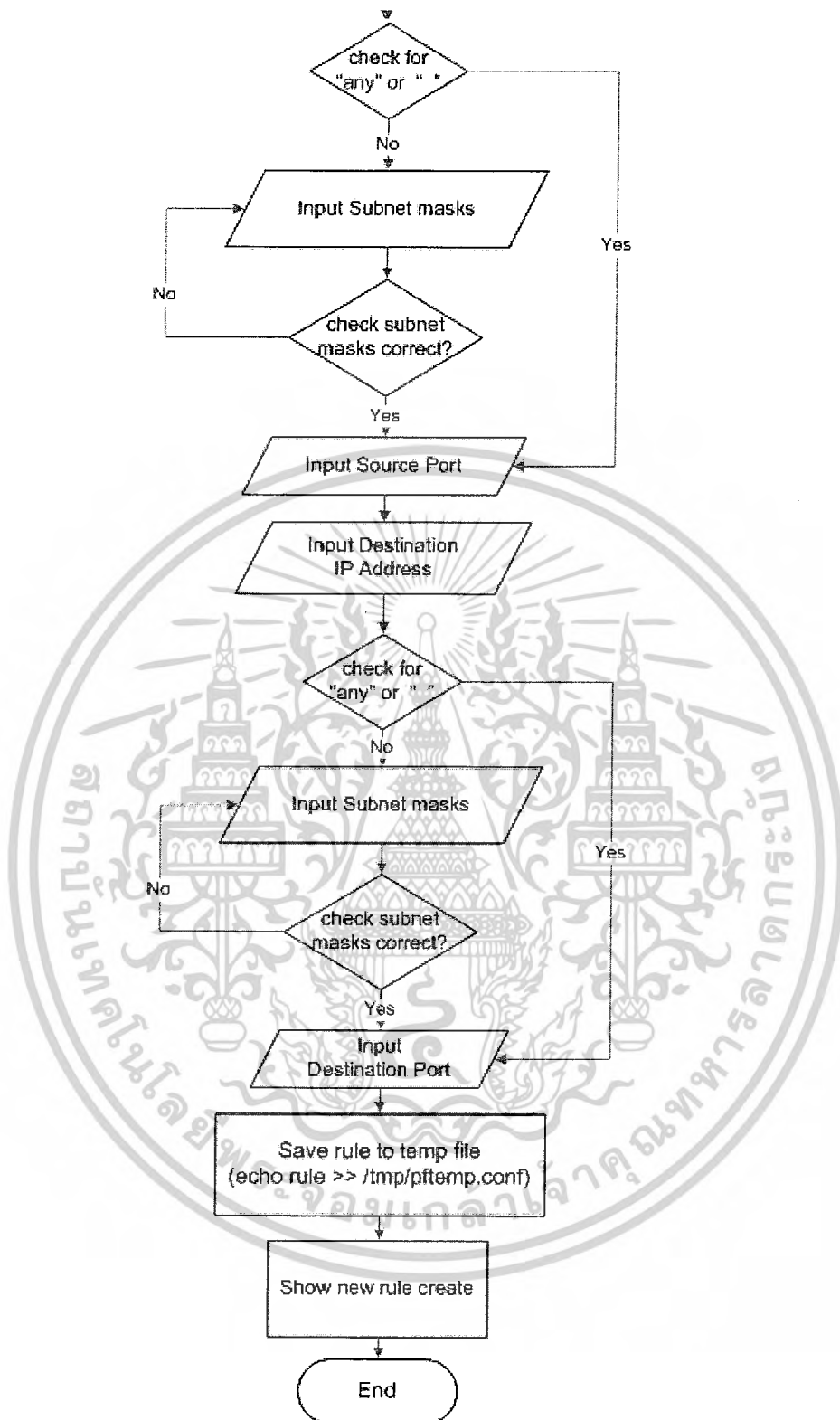
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.2.1.10 แผนภาพอธิบายลำดับการทำงานของสคริปต์ create.csh



รูปที่ 3.13 แผนภาพแสดงลำดับการทำงานของสคริปต์ create.csh

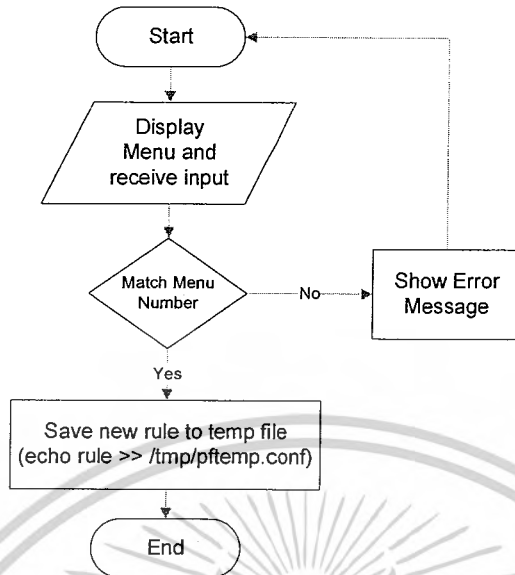
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 3.13 (ต่อ) แผนภาพแสดงลำดับการทำงานของสคริปต์ create.csh

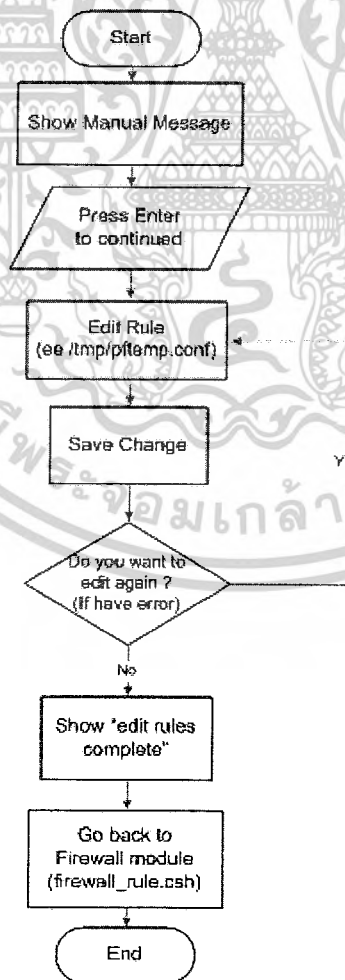
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.2.1.11 แผนภาพอธิบายลำดับการทำงานของสคริปต์ create_wizard.csh



รูปที่ 3.14 แผนภาพแสดงลำดับการทำงานของสคริปต์ create_wizard.csh

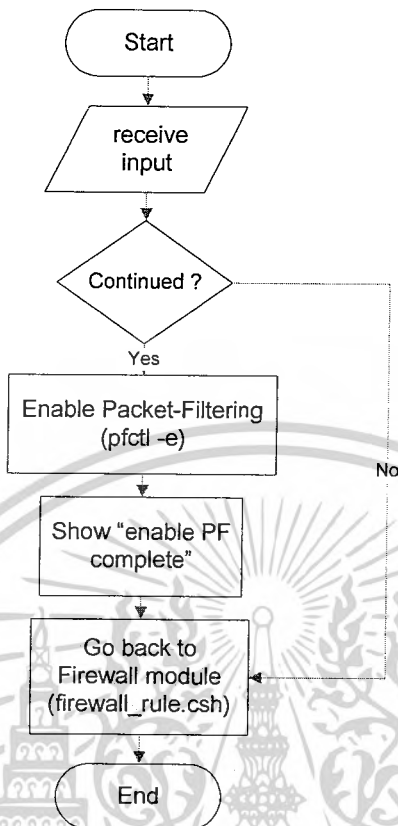
3.2.1.12 แผนภาพอธิบายลำดับการทำงานของสคริปต์ edit.csh



รูปที่ 3.15 แผนภาพแสดงลำดับการทำงานของสคริปต์ edit.csh

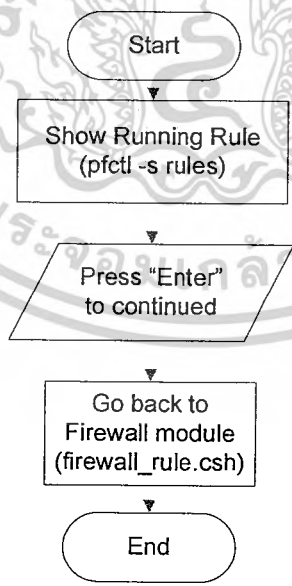
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานในหอการศึกษานี้เท่านั้น เมื่อผู้ดูแลเห็นว่าไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.2.1.13 แผนภาพอธิบายลำดับการทำงานของสคริปต์ enable_rule.csh



รูปที่ 3.16 แผนภาพแสดงลำดับการทำงานของสคริปต์ enable_rule.csh

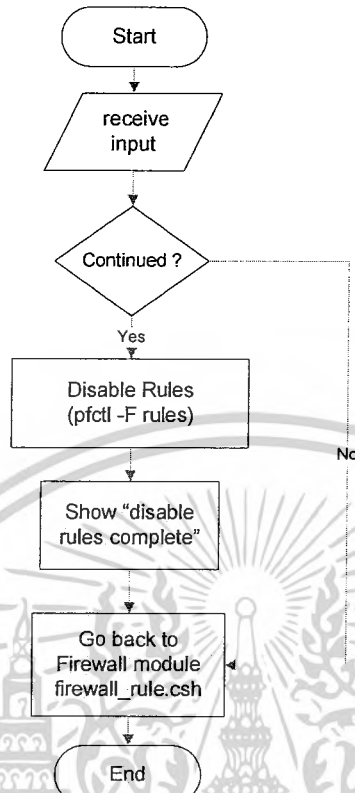
3.2.1.14 แผนภาพอธิบายลำดับการทำงานของสคริปต์ show_rule.csh



รูปที่ 3.17 แผนภาพแสดงลำดับการทำงานของสคริปต์ show_rule.csh

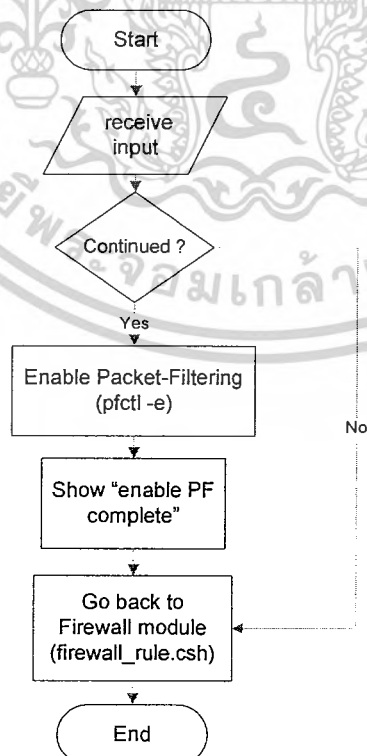
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.2.1.15 แผนภาพอธิบายลำดับการทำงานของสคริปต์ disable_rule.csh



รูปที่ 3.18 แผนภาพแสดงลำดับการทำงานของสคริปต์ disable_rule.csh

3.2.1.16 แผนภาพอธิบายลำดับการทำงานของสคริปต์ enable_pf.csh



รูปที่ 3.19 แผนภาพแสดงลำดับการทำงานของสคริปต์ enable_pf.csh

เอกสารนี้เป็นเอกสารที่สงวนลิขสิทธิ์ไว้สำหรับการศึกษาค้นคว้าเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.2.1.17 แผนภาพอธิบายลำดับการทำงานของสคริปต์ disable_pf.csh



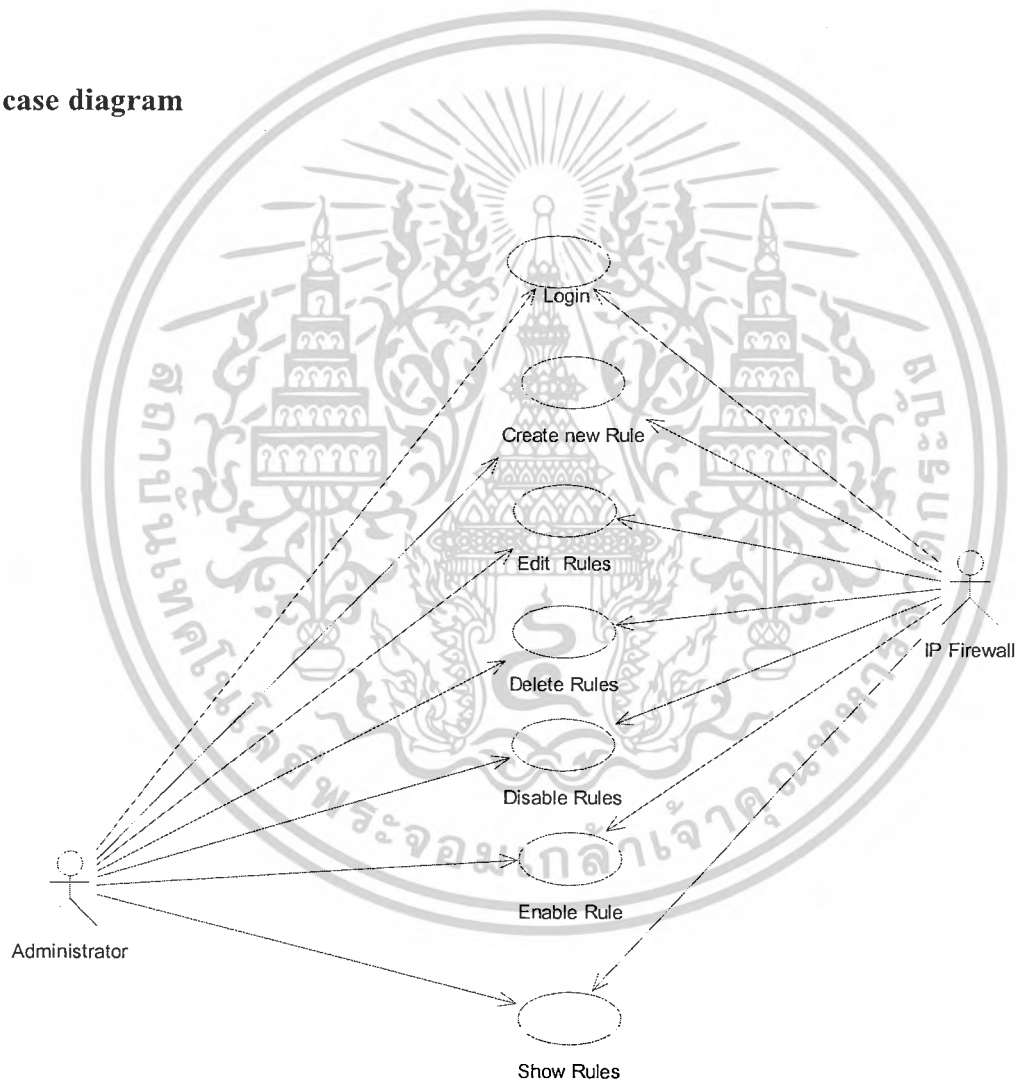
รูปที่ 3.20 แผนภาพแสดงลำดับการทำงานของสคริปต์ disable_pf.csh

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ฟังก์ชันการใช้งาน

- 1.สามารถทำการล็อกอินเข้าสู่ระบบได้(Log in)
- 2.ทำการสร้างกฎขึ้นใหม่ได้(Create New Rule)
- 3.ทำการแก้ไขกฎได้(Edit Existing Rules)
- 4.สามารถทำการลบกฎที่มีได้>Delete Rules)
- 5.ทำการแสดงกฎที่สร้างขึ้นได้>Show Rule)
- 6.ทำการเลือกให้ไฟร์วอลล์ทำตามกฎที่สร้างขึ้น(Enable Rule)
- 7.ทำการเลือกไม่ให้กฎมีผลต่อการทำงานของไฟร์วอลล์(Disable Rule)

Use case diagram



รูปที่ 3.21 แผนภาพแสดงคุณสมบัติการทำงานของระบบกับผู้ใช้
ผ่านทางคอมพิวเตอร์ไบนารี

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Use case Description

ตารางที่ 3.1 แสดงคำอธิบายการเข้าใช้ระบบ

ผู้ช่อยุสเคส : Login	ไอดี : 1
ไฟเมรีเอ็คเตอร์ : Administrator	
สะเต็กโฮลเดอร์ :	
คำอธิบายโดยย่อ : จะทำการตรวจสอบ Username และ Password ว่ามีอยู่ในระบบหรือไม่	
เรียกใช้เมื่อ :	
ความสัมพันธ์กับยูสเคสอื่น : Association : - Include : - Extend : - Generalization : -	
ลำดับการทำงานปกติ : <ol style="list-style-type: none"> 1. Administrator ทำการ Login เพื่อเข้าใช้งานระบบ 2. ทำการป้อน Username และ Password ของผู้จะเข้าใช้ระบบ 3. ระบบทำการตรวจสอบความถูกต้องของข้อมูล 4. ข้อมูลถูกต้องทำการเข้าใช้งานส่วนต่างๆของระบบได้ 	
เงื่อนไขจากการทำงานปกติ : 3a. ระบบทำการตรวจสอบแล้วหากไม่พบข้อมูลจะทำการแสดงข้อความผิดพลาดขึ้นและกลับเข้าสู่การ Login ใหม่อีกครั้ง	

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 3.2 แสดงคำอธิบายการสร้างกฎใหม่

ชื่อยุสเคส : Create New Rule	ไอดี : 2
ไฟเพรีเอ็คเตอร์ : Administrator	
สะเต็คโฮลเดอร์ :	
คำอธิบายโดยย่อ : จะทำการสร้างกฎต่างๆที่จะใช้ในการทำงานของไฟร์วอลล์	
เรียกใช้เมื่อ :	
ความสัมพันธ์กับยูสเคสอื่น : Association : - Include : - Extend : - Generalization : -	
ลำดับการทำงานปกติ : <ol style="list-style-type: none"> 1. Administrator ต้องการทำการสร้างกฎใหม่ โดยป้อนข้อมูลที่จำเป็น เช่น ไอพีต้นทาง , พอร์ตต้นทาง , ไอพีปลายทาง , พอร์ตปลายทาง , โพรโตคอล , อินเตอร์เฟซ 2. ตรวจสอบกฎที่จะทำการเพิ่มว่าถูกต้องตามหลักการสร้างกฎหรือไม่ 3. ทำการเพิ่มกฎและบันทึกกฎที่เพิ่มเข้าสู่ระบบ 4. ระบบแจ้งผลการเพิ่มกฎ 	
เงื่อนไขจากการทำงานปกติ : 2a. หากกฎที่ทำการสร้างไม่ถูกต้อง ระบบจะแสดงข้อความผิดพลาดขึ้นและไม่ทำการบันทึกผล	

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 3.3 แสดงคำอธิบายการแก้ไขกฎในระบบ

ชื่อยุสเคลส : Edit Rule	ไอดี : 3
ไฟเพรีเอ็คเตอร์ : Administrator	
สะเต็คโฮลเดอร์ :	
คำอธิบายโดยย่อ : ทำการแก้ไขกฎต่างๆที่ได้มีการสร้างไว้ทั้งที่สร้างใหม่และมีอยู่เดิม	
เรียกใช้เมื่อ :	
ความสัมพันธ์กับยูสเคลสอื่น : Association : - Include : - Extend : - Generalization : -	
ลำดับการทำงานปกติ : 1. Administrator เรียกดูกฎที่สร้างขึ้น 2. ตรวจสอบว่ามีกฎอยู่หรือไม่ 3. ทำการอ่านกฎที่มีอยู่ออกมา 4. Administrator จะทำการส่งข้อมูลที่ต้องการปรับปรุง 5. ตรวจสอบกฎที่ทำการแก้ไขว่าถูกต้องตามหลักการสร้างกฎ 6. ทำการปรับปรุงและแก้ไขกฎไฟร์วอลล์ 7. ทำการบันทึกกฎที่ได้รับการแก้ไขเข้าสู่ระบบ 8. ระบบแจ้งผลการบันทึกกฎที่ได้รับการแก้ไขใหม่	
เงื่อนไขจากการทำงานปกติ : 1a. หากไม่พบกฎที่สร้างขึ้นระบบจะแสดงข้อผิดพลาดขึ้น 4a. หากกฎที่ทำการแก้ไขไม่ถูกต้อง ระบบจะแสดงข้อความผิดพลาดขึ้นและไม่ทำการบันทึกผล	

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
 ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 3.4 แสดงคำอธิบายการลบกฎในระบบ

ชื่อยุสเคส : Delete Rule	ไอดี : 4
ไฟเพรีเอ็คเตอร์ : Administrator	
สะเท็คโฮลเดอร์ :	
คำอธิบายโดยย่อ : จะทำการลบกฎต่างๆที่ได้มีการสร้างไว้ที่มีอยู่เดิม	
เรียกใช้เมื่อ :	
ความสัมพันธ์กับยูสเคสอื่น :	
<p>Association : -</p> <p>Include : -</p> <p>Extend : -</p> <p>Generalization : -</p>	
ลำดับการทำงานปกติ :	
<ol style="list-style-type: none"> 1. Administrator ทำการเรียกดูกฎที่สร้าง 2. ตรวจสอบว่ามีกฎอยู่หรือไม่ 3. ทำการอ่านกฎที่มีอยู่ออกมา 4. ตรวจสอบกฎที่จะทำการลบว่าสามารถทำการลบได้หรือไม่ 5. ทำการลบกฎและบันทึกผล 6. ระบบแจ้งผลการลบ 	
เงื่อนไขจากการทำงานปกติ :	
<ol style="list-style-type: none"> 1a. หากไม่พบกฎที่สร้างขึ้นระบบจะแสดงข้อผิดพลาดขึ้น 4a. หากกฎที่ทำการลบไม่ถูกต้องระบบจะไม่แสดงข้อความผิดพลาดขึ้น 	

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 3.5 แสดงคำอธิบายการแสดงกฎที่มีในระบบ

ชื่อยุสเคส : Show Rule	ไอดี : 5
ไพรมารีเอ็กเตอร์ : Administrator	
สะเท็กโสดเตอร์ :	
คำอธิบายโดยย่อ : จะทำการเรียกกฎมาแสดงผล	
เรียกใช้เมื่อ :	
ความสัมพันธ์กับยูสเคสอื่น :	
Association : -	
Include : -	
Extend : -	
Generalization : -	
ลำดับการทำงานปกติ :	
<ol style="list-style-type: none"> 1. Administrator ทำการเรียกดูกฎที่สร้าง 2. ตรวจสอบว่ามีกฎอยู่หรือไม่ 3. ทำการอ่านกฎที่มีอยู่ออกมา 	
เงื่อนไขจากการทำงานปกติ :	
1a. เมื่อยังไม่มียกกฎจะแสดงผลว่าไม่พบกฎ	

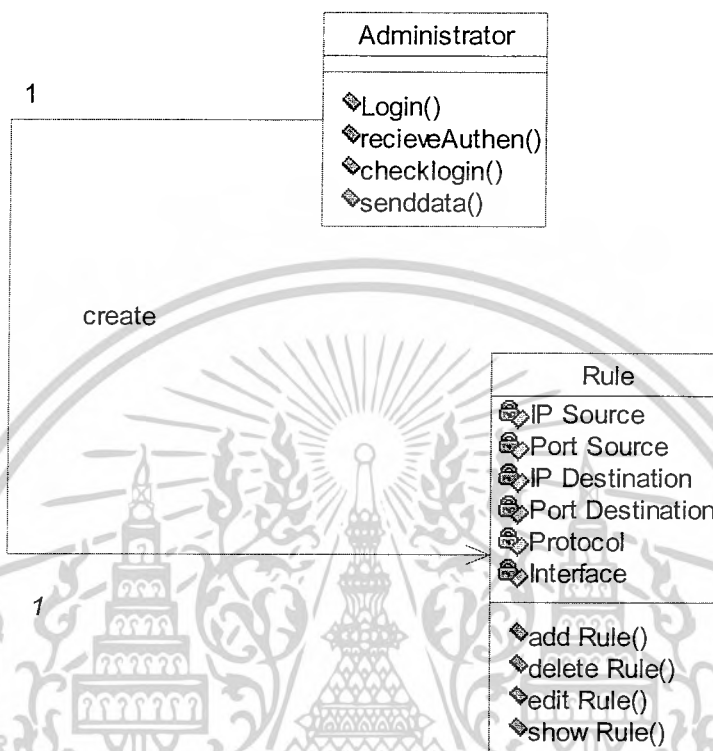
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 3.6 แสดงคำอธิบายการให้กฎทำงาน

ชื่อยูสเคส : Enable Rule	ไอดี : 6
ไฟแอมรีเอคเตอร์ : Administrator	
สะเท็กโฮลเดอร์ :	
คำอธิบายโดยย่อ : ทำการเลือกทำให้กฎทำงาน	
เรียกใช้เมื่อ : ต้องการให้กฎมีผลกับการทำงานของไฟร์วอลล์	
ความสัมพันธ์กับยูสเคสอื่น : Association : - Include : - Extend : - Generalization : -	
ลำดับการทำงานปกติ : 1.Administrator เข้ามาเซตค่าที่กฎเพื่อให้กฎมีผลกับการทำงานของไฟร์วอลล์ 2...ทำการเซตกฎและบันทึกผล	
เงื่อนไขจากการทำงานปกติ :	

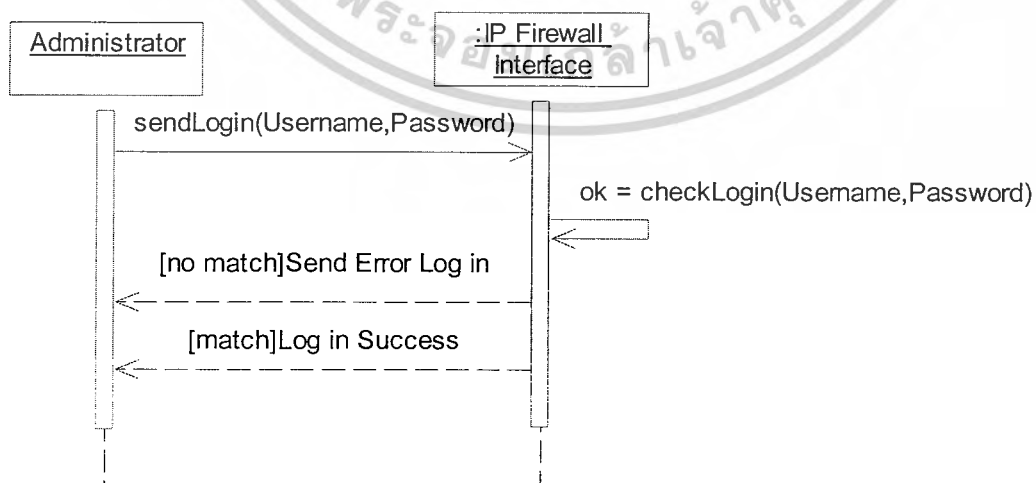
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Class Diagram



รูปที่ 3.22 แผนภาพแสดงคลาสที่มีในระบบ

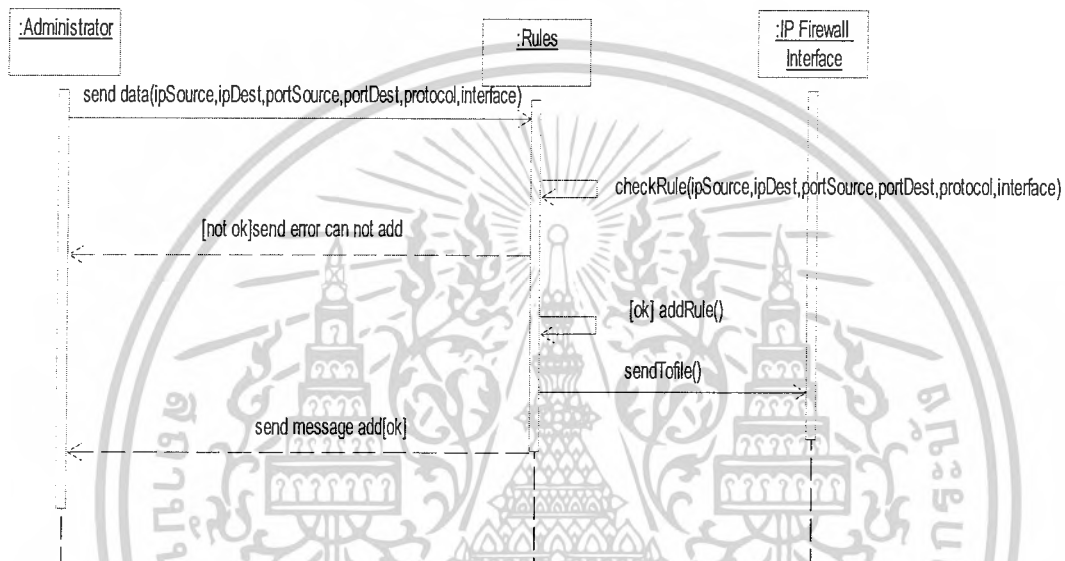
Sequence Diagram



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

รูปที่ 3.23 แผนภาพแสดงลำดับการทำงานของการทำงานของการเข้าใช้งานระบบ

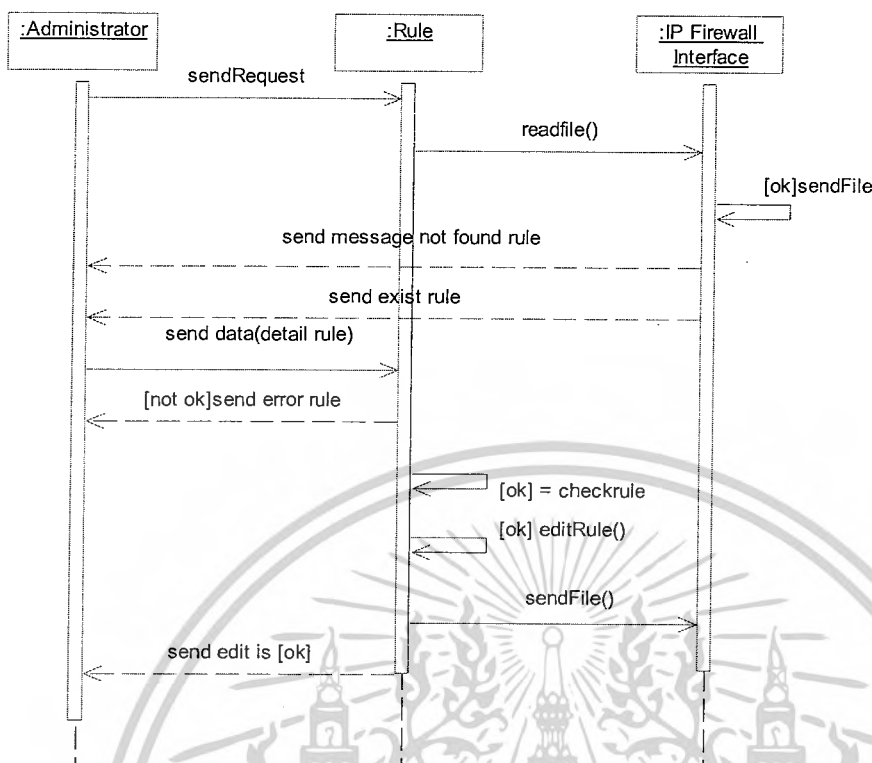
Sequence Diagram ของ Login เป็นการแสดงถึงการทำงานของ Login Firewall Use case โดยเมื่อผู้ดูแลระบบเข้ามาทำงานโดยการป้อนข้อมูลในส่วนของ username,password โมดูลในส่วนของผู้ดูแลระบบก็จะทำการตรวจสอบข้อมูลและถ้าหากข้อมูลถูกต้องก็จะอนุญาตให้ผู้ดูแลระบบสามารถใช้งานระบบต่างๆ ได้ถ้าไม่ถูกต้องก็จะทำการแจ้งข้อความผิดพลาดขึ้น



รูปที่ 3.24 แผนภาพแสดงลำดับการทำงานของการทำงานของการสร้างกฎใหม่

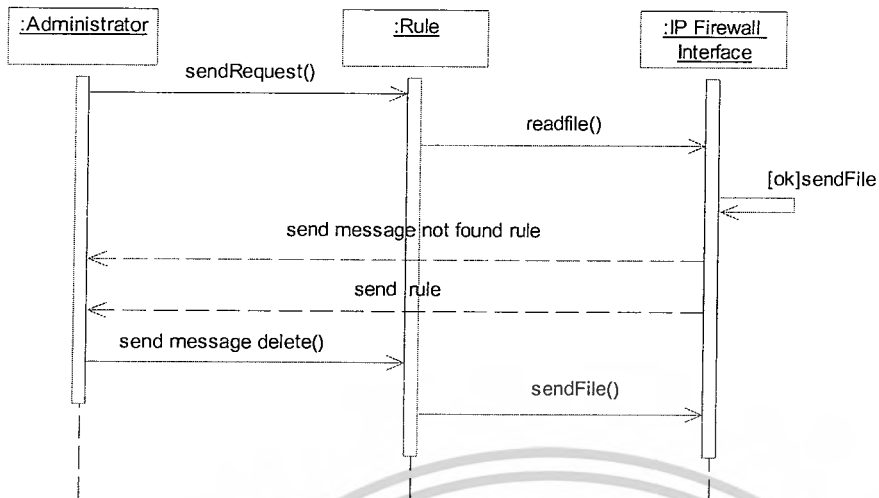
Sequence Diagram ของ Create New Rule หลังจากผู้ดูแลระบบได้ทำการล็อกอินเข้าสู่ระบบเรียบร้อยแล้วจะทำการสร้างกฎของไฟร์วอลล์โดยป้อนข้อมูลในส่วนของ ip source,ip destination,port source,port destination,protocol,interface เข้าสู่ระบบแล้ว ระบบจะทำการตรวจสอบข้อมูลที่ส่งเข้ามาสู่ระบบว่าถูกต้องหรือไม่และแจ้งผลการสร้างกฎให้กับผู้ดูแลระบบ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



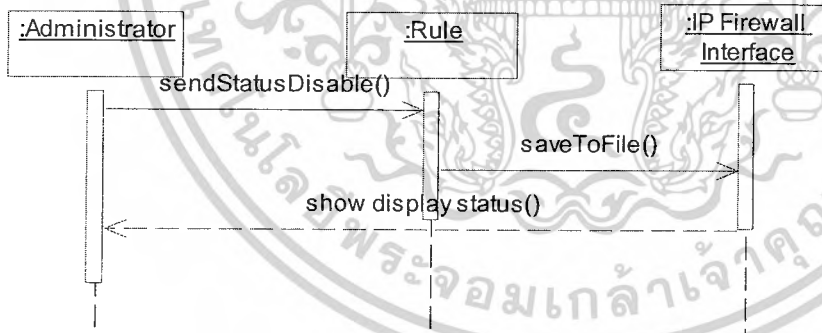
รูปที่ 3.25 แผนภาพแสดงลำดับการทำงานของการทำงานของการแก้ไขกฎที่มีในระบบ

Sequence Diagram ของ Edit Existing Rules Use case แสดงการทำงานในส่วนของการแก้ไขกฎที่ได้มีการสร้างไว้แล้วโดยผู้ใช้จะทำการร้องขอและระบบจะทำการตรวจสอบว่ามีกฎอยู่ในไฟล์ข้อมูลหรือไม่ ถ้าพบระบบก็จะทำการดึงกฎจากไฟล์และทำการแสดงผลของกฎ จากนั้นผู้ดูแลระบบทำการแก้ไขโดยผู้ใช้ทำการป้อนข้อมูลเพิ่มหรือแก้ไขข้อมูลจากนั้นนำส่งเข้าสู่ระบบเพื่อตรวจเช็คความถูกต้องและระบบจะแจ้งผลการตรวจสอบ



รูปที่ 3.26 แผนภาพแสดงลำดับการทำงานของลบกฎในระบบ

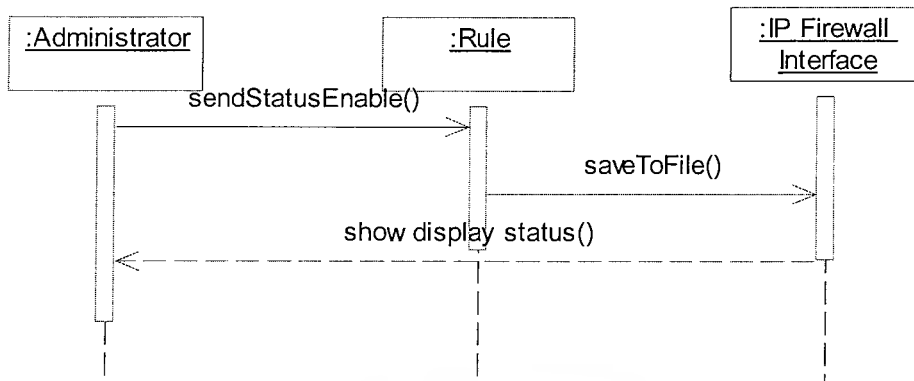
Sequence Diagram ของ Delete Rules แสดงการทำงานในส่วนของการลบกฎที่ได้มีการสร้างไว้แล้ว โดยผู้ใช้จะส่งคำร้องขอและระบบจะทำการตรวจสอบในไฟล์ข้อมูลว่ามีกฎอยู่หรือไม่ ถ้าพบก็จะทำให้ทำการลบกฎได้ จากนั้นระบบจะแจ้งผลการทำงาน



รูปที่ 3.27 แผนภาพแสดงลำดับการทำงานของคำสั่งยกเลิกการทำงานของกฎ

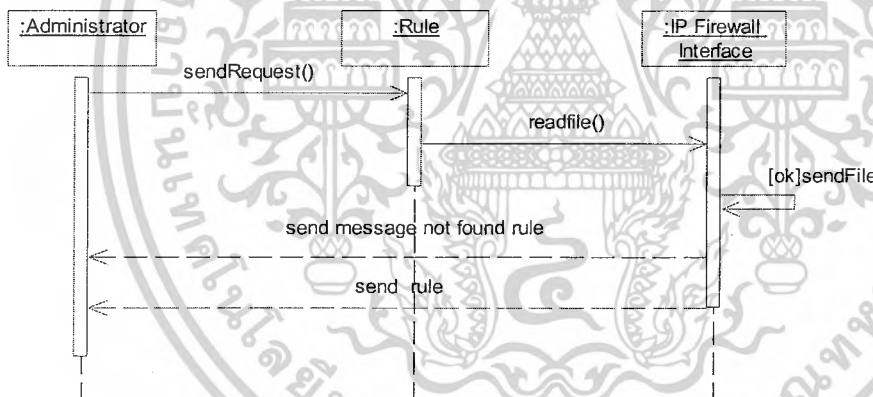
Sequence Diagram ของ Disable Rule ในขณะที่ทำการสร้างกฎใหม่หรือทำการเปลี่ยนแปลงแก้ไขเมื่อต้องการให้กฎนั้นไม่มีผลต่อการทำงานของไฟร์วอลล์ จากนั้นระบบจะบันทึกผล

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 3.28 แผนภาพแสดงลำดับการทำงานของคำสั่งให้กฎทำงานทันที

Sequence Diagram ของ Enable Rule ในขณะที่ทำการสร้างกฎใหม่หรือทำการเปลี่ยนแปลงแก้ไขแล้วต้องการให้กฎนั้นมีผลต่อการทำงานของไฟร์วอลล์ จากนั้นระบบจะบันทึกผล

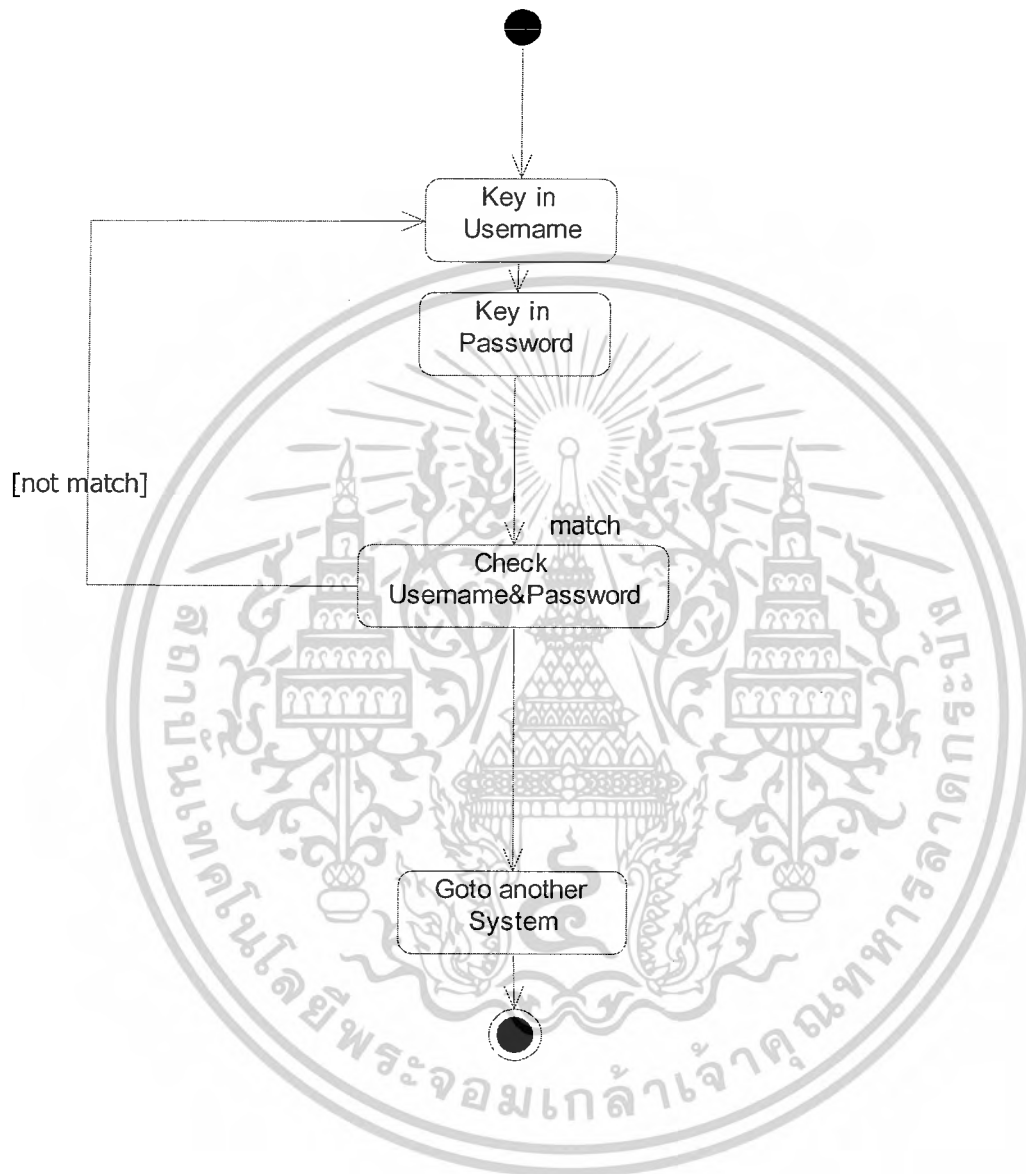


รูปที่ 3.29 แผนภาพแสดงลำดับการทำงานของการแสดงกฎที่มีอยู่ในระบบ

Sequence Diagram ของ Show Rule Use case แสดงการทำงานในส่วนของการแก้ไขกฎที่ได้มีการสร้างไว้แล้วโดยผู้ใช้จะทำการร้องขอและระบบจะทำการตรวจสอบว่ามีกฎอยู่ในไฟล์ข้อมูลหรือไม่ ถ้าพบระบบก็จะทำการดึงกฎจากไฟล์และทำการแสดงผลของกฎ

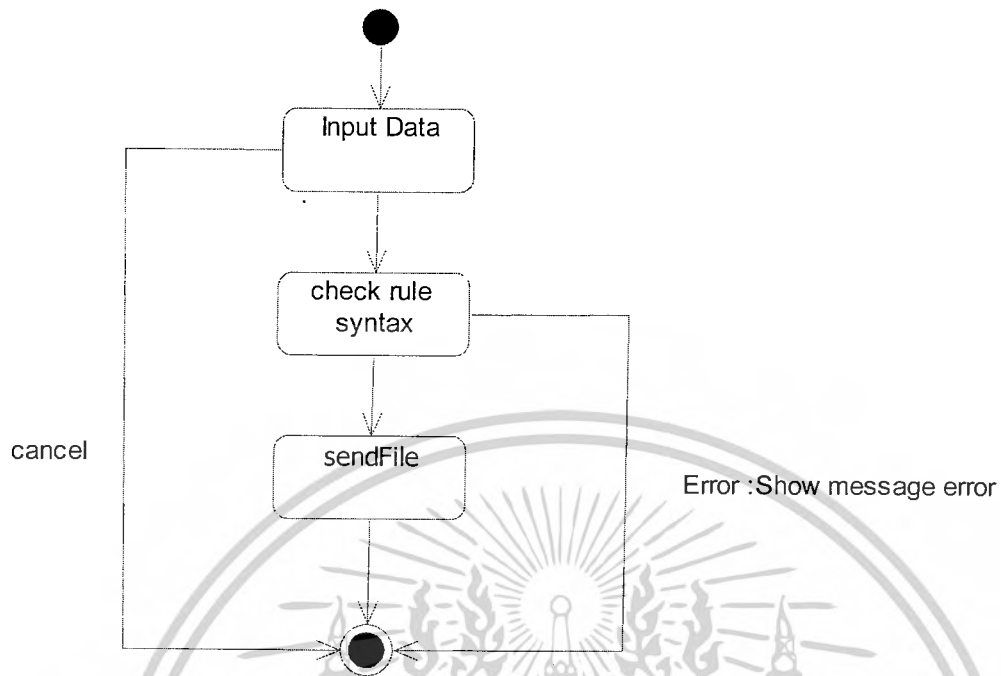
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Activity Diagram



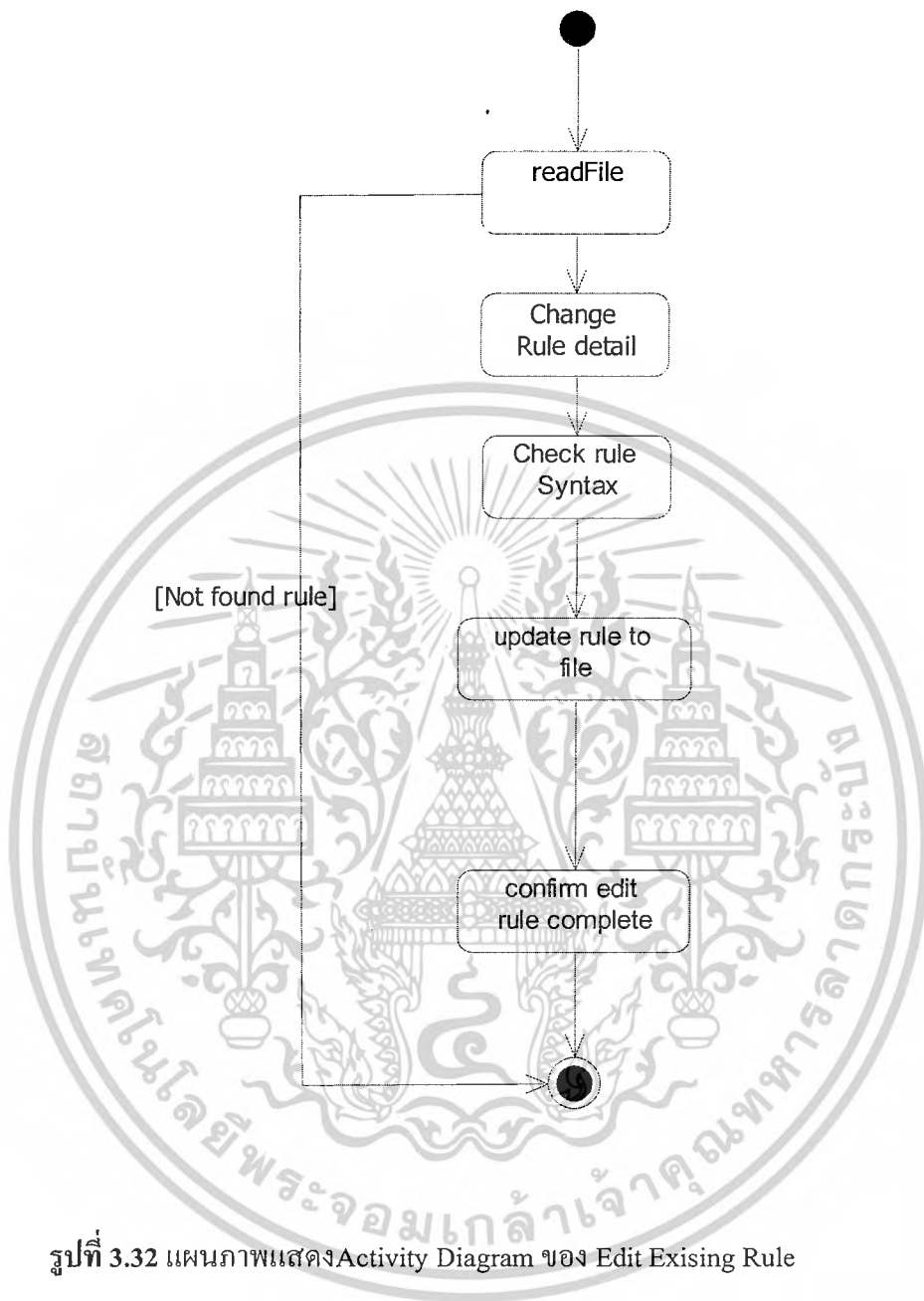
รูปที่ 3.30 แผนภาพแสดงActivity Diagram ของ Login

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



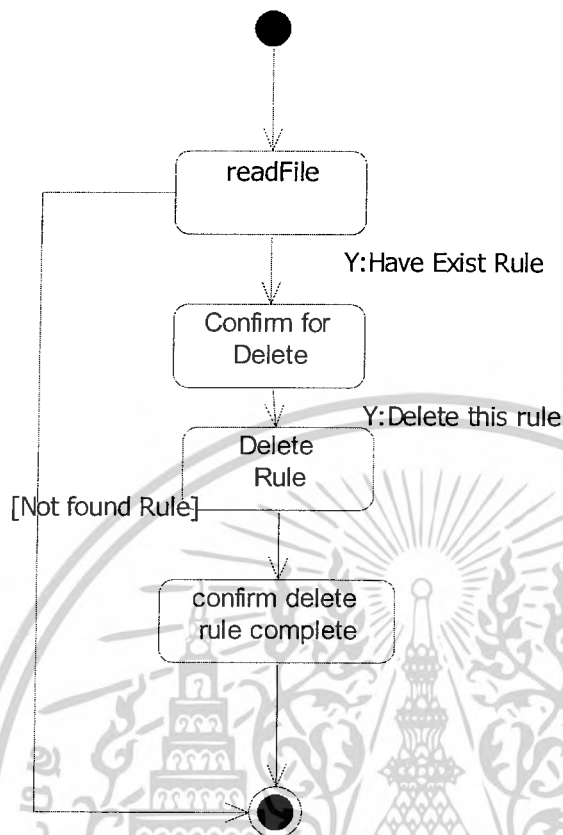
รูปที่ 3.31 แผนภาพแสดงActivity Diagram ของ Create New Rule

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



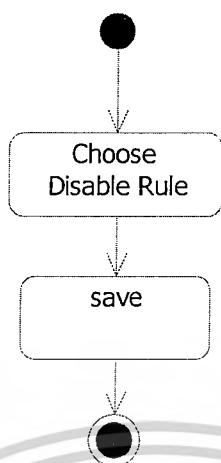
รูปที่ 3.32 แผนภาพแสดงActivity Diagram ของ Edit Existing Rule

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 3.33 แผนภาพแสดงActivity Diagram ของ Delete Rule

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

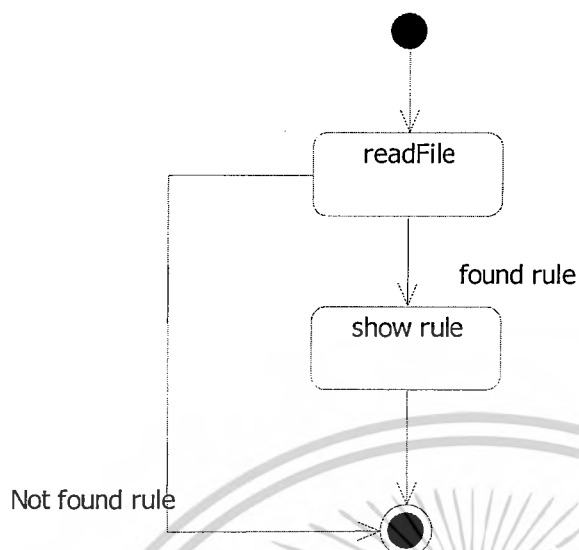


รูปที่ 3.34 แผนภาพแสดงActivity Diagram ของ Disable Rule



รูปที่ 3.35 แผนภาพแสดงActivity Diagram ของ Enable Rule

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 3.36 แผนภาพแสดง Activity Diagram ของ Show Rule

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.3 ขั้นตอนการออกแบบเว็บอินเตอร์เฟส

1. ทำการออกแบบหน้าเว็บ โดยส่วนแรกจะเป็นการล็อกอินเข้าสู่ระบบ
 2. ทำการออกแบบให้ผู้ดูแลระบบ สามารถสร้างกฎ แก้ไข เรียกกฎขึ้นมาดูได้
 3. ทำการออกแบบให้ผู้ดูแลระบบ ทำการแก้ไขไอพีของอินเตอร์เฟสได้
- การออกแบบ เริ่มออกแบบโดยแบ่งออกเป็นเมนูต่างๆ อยู่ด้านซ้ายมือ ประกอบไปด้วย
- การสร้างกฎขึ้นมาใหม่ ออกแบบให้เป็น form ให้ผู้ใช้กรอกค่าต่างๆ ที่ต้องการเซตค่า มีปุ่ม save เพื่อบันทึกลงสู่ไฟล์
 - การแก้ไขกฎ ออกแบบให้เป็น list box ให้ดูแลทำการเลือกว่าจะแก้ไขกฎจาก Temp File , Boot File มีปุ่ม reset ไว้แก้ไขกฎไปเป็นอันก่อนหน้า (เหมือนปุ่ม undo)
 - การลบกฎ การแสดงกฎที่มีอยู่ทั้งหมดระบบ การสั่งงานให้กฎนั้นๆทำงานได้รวมอยู่ในส่วนเดียว โดยได้ออกแบบระบบให้มี ไฟล์อยู่ 2 ประเภท ได้แก่ Temp File คือ ไฟล์ที่เก็บกฎทั้งหมดที่มีในระบบ และ Boot File เป็นไฟล์ที่ใช้ตอนรีบูตระบบขึ้นมา และได้ออกแบบให้ผู้ใช้งานทำการแก้ไขกฎต่างๆ ใน Temp File ก่อนจากนั้นจึงบันทึกลงสู่ Temp File เพื่อป้องกันข้อผิดพลาด การแสดงได้ออกเป็นตาราง แบ่งๆเป็นช่องๆ โดยใช้การใช้การตัดคำ เพื่อให้สะดวกในการใช้งาน
 - การแสดงกฎที่รันอยู่ในขณะนั้น โดยออกแบบให้แสดงผลแบบธรรมดา เนื่องจากไม่ต้องการเอาไปใช้สำหรับการแสดงผลเพียงอย่างเดียว
 - การแสดง ไอพีแอดเดรสของอินเตอร์เฟสต่างๆ ที่มีในระบบ โดยได้ออกแบบเป็นตาราง มี link edit ให้เลือกเฉพาะแต่ละอินเตอร์เฟสมาแก้ไขได้ จากนั้นมีปุ่ม เพื่อเป็นการสั่งให้ ไอพีนั้นๆมีผลต่ออินเตอร์เฟสนั้นๆ
 - การรีบูตระบบขึ้นมาใหม่ ได้ออกแบบให้เป็นปุ่ม เพื่อให้ผู้ดูแลระบบสามารถรีบูตระบบผ่านทางหน้าเว็บได้

3.3.1 การออกแบบฟังก์ชันการทำงาน ฟังก์ชันที่เกี่ยวข้อง ได้แก่

3.3.1.1 ฟังก์ชันเกี่ยวกับกฎที่สร้างขึ้นในระบบ

การสร้างกฎขึ้นมาใหม่

ขั้นตอนการทำงาน

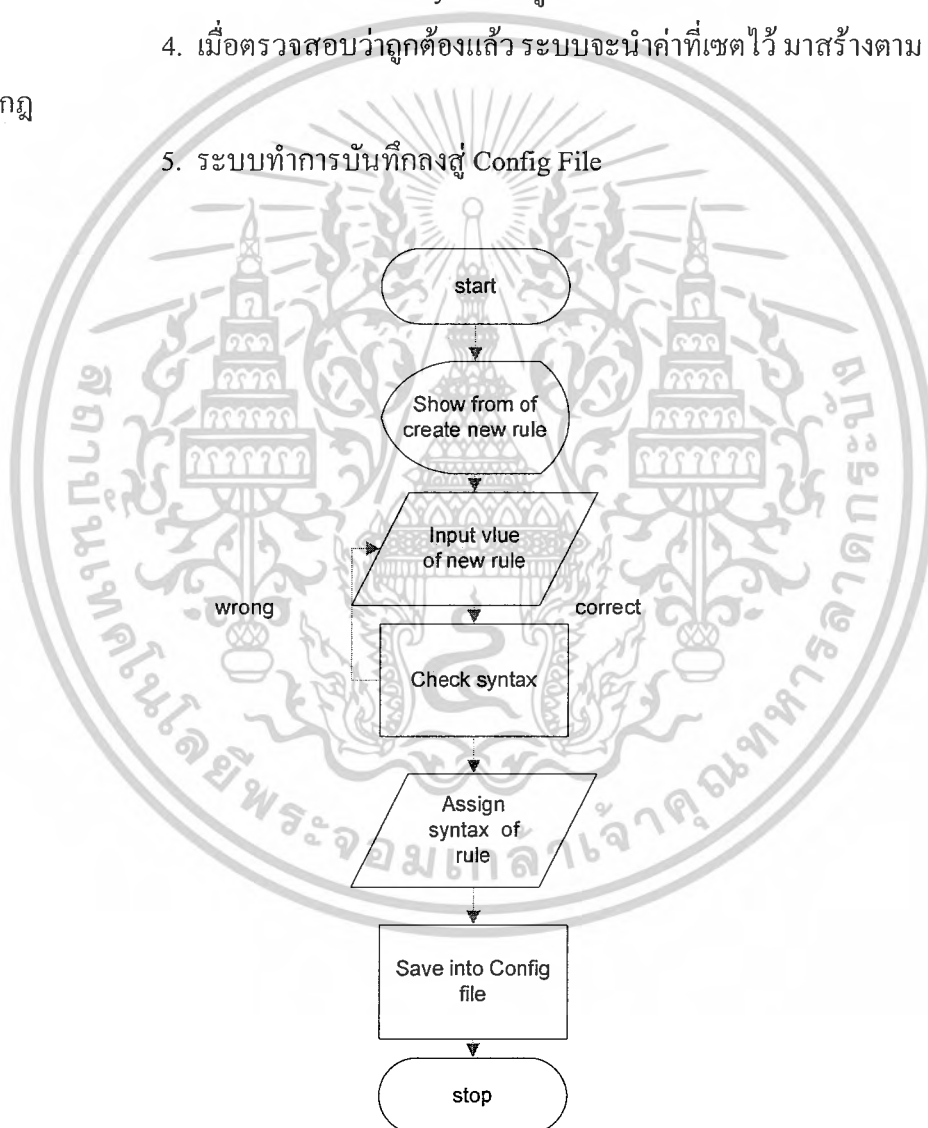
1. ระบบจะแสดงฟอร์มให้ผู้ดูแลระบบทำการเซตค่าสร้างกฎขึ้นมาใหม่
2. ผู้ดูแลระบบทำการเซตค่าต่างๆ ของกฎที่ต้องการสร้าง ได้แก่ ค่าไอพี

แอดเดรส ค่าพอร์ต เป็นต้น

3. ระบบจะทำการเช็ค syntax ว่าถูกต้องหรือไม่
4. เมื่อตรวจสอบว่าถูกต้องแล้ว ระบบจะนำค่าที่เซตไว้ มาสร้างตาม

syntax ของกฎ

5. ระบบทำการบันทึกลงสู่ Config File



รูปที่ 3.37 แผนภาพแสดงลำดับการทำงานของการสร้างกฎใหม่

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

การแสดงกฎ แบ่งออกเป็น 3 ส่วน ได้แก่

1. ส่วนการแสดงกฎ

ขั้นตอนการทำงาน

1.1 ระบบอ่านค่ากฎจาก Config File มาแสดง

1.2 ระบบทำการแสดงกฎในตารางที่กำหนดไว้

2. ส่วนการนำกฎไปใช้งาน

ขั้นตอนการทำงาน

2.1 ระบบทำการ copy กฎ จาก Temp File ไปยัง Boot File

2.2 ระบบจะโหลดกฎจาก Boot File ลงสู่หน่วยความจำ

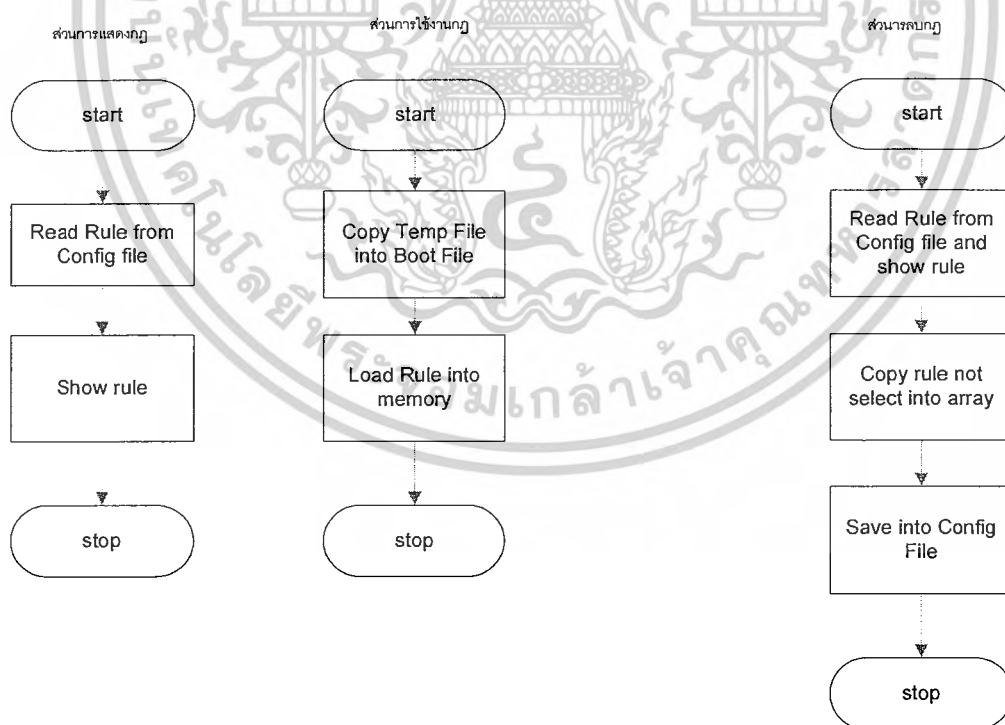
3. ส่วนการลบกฎ

ขั้นตอนการทำงาน

3.1 อ่านกฎจาก Config File มาเก็บไว้ในอาร์เรย์

3.2 ทำการ copy กฎที่ไม่ต้องการลบไปไว้ในอาร์เรย์ตัวใหม่

3.3 ทำการเขียนค่าในอาร์เรย์ตัวใหม่ทับในไฟล์เดิม



รูปที่ 3.38 แผนภาพแสดงลำดับการแสดงกฎ การใช้งานกฎ และการลบกฎ

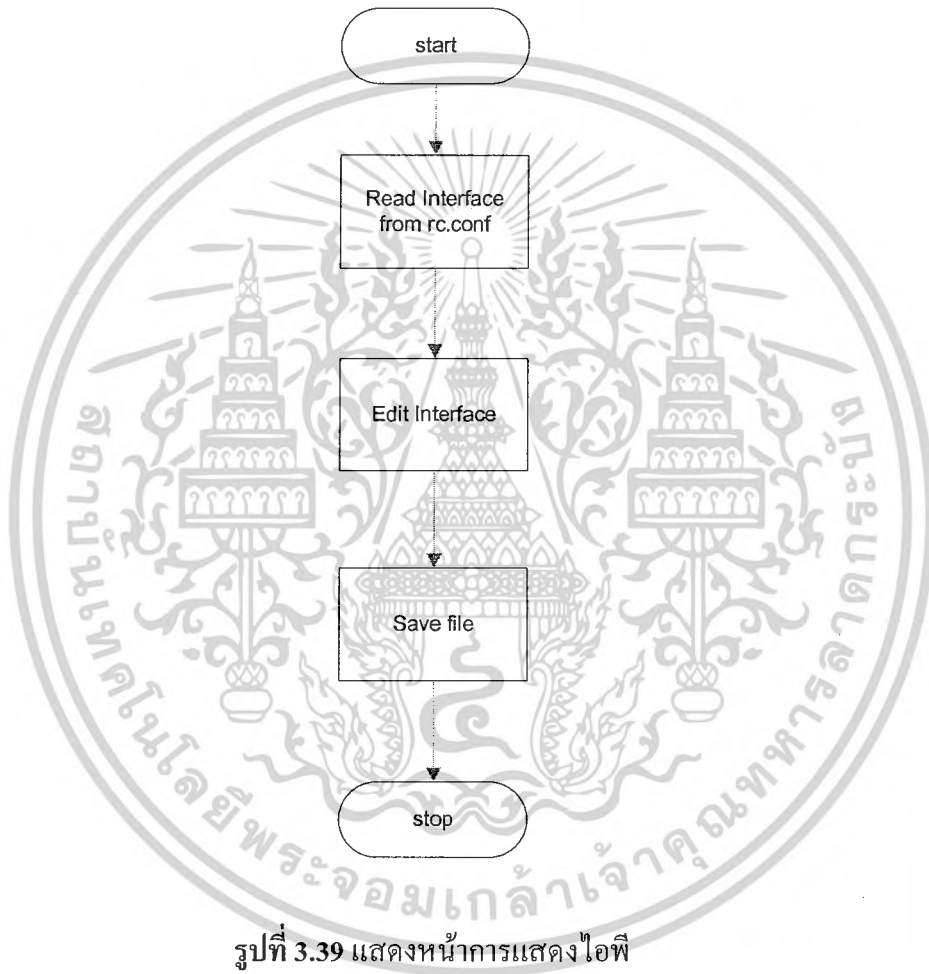
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.3.2 ฟังก์ชันเกี่ยวกับอินเตอร์เฟซ

การแก้ไขอินเตอร์เฟซ

ขั้นตอนการทำงาน

1. ระบบทำการอ่านค่าอินเตอร์เฟซจากไฟล์ rc.conf มาแสดงผล
2. ผู้ดูแลระบบทำการเลือกอินเตอร์เฟซที่จะทำการแก้ไข
3. ระบบทำการบันทึกลงสู่ rc.conf ไฟล์

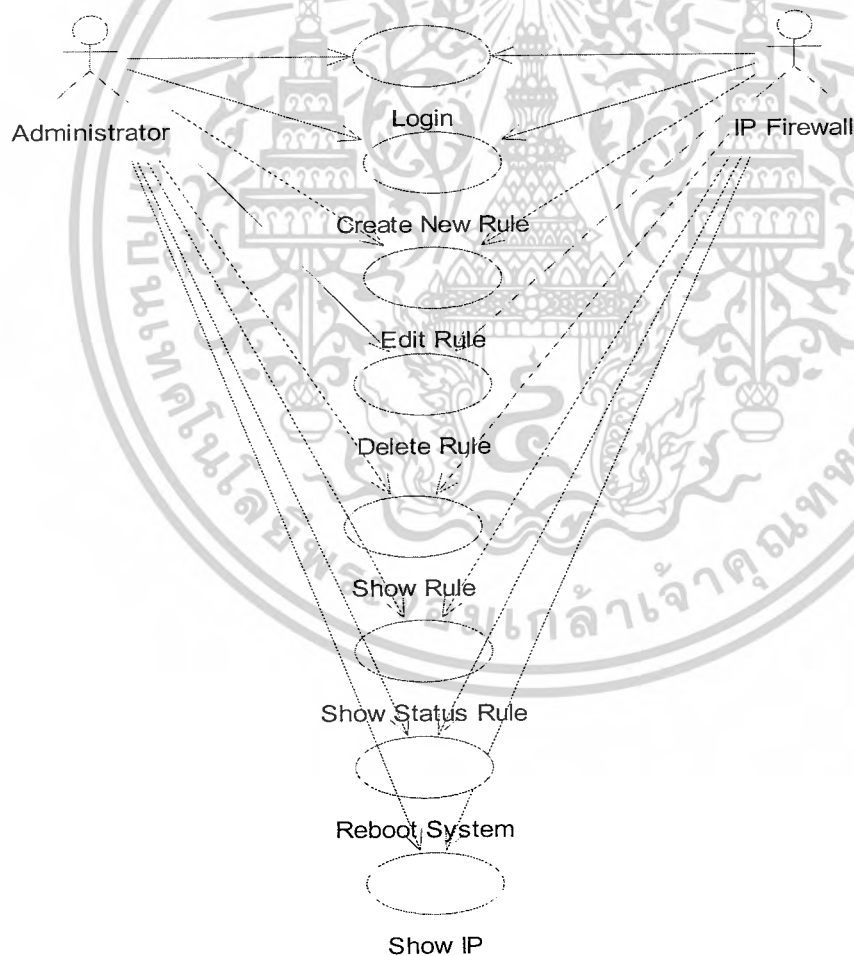


เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ฟังก์ชันการใช้งาน

1. สามารถทำการล็อกอินเข้าสู่ระบบได้(Log in)
2. ทำการสร้างกฎขึ้นมาใหม่ได้(Create New Rule)
3. ทำการแก้ไขกฎ(Edit Existing Rules)
4. สามารถทำการลบกฎที่มีได้>Delete Rules)
5. ทำการแสดงกฎที่สร้างขึ้นได้>Show Rule)
6. ทำการแสดงกฎที่ทำงานอยู่ ณ ขณะนั้น>Show status rule)
7. ทำการเริ่มต้นการทำงานระบบใหม่(reboot system)
8. ทำการแก้ไขไอพีแอดเดรสของอินเทอร์เน็ต(show ip)

Use case Diagram



รูปที่ 3.40 แผนภาพแสดงคุณสมบัติการทำงานของระบบกับผู้ใช้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับใช้ทางการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Use case Description

ตารางที่ 3.7 แสดงคำอธิบายการเข้าใช้ระบบ

ชื่อยูสเคส : Login	ไอดี : 1
ไฟเมอร์เอดเดอร์ : Administrator	
สเตอร์กโฮลเดอร์ :	
คำอธิบายโดยย่อ : จะทำการตรวจสอบ Username และ Password ว่ามีอยู่ในระบบหรือไม่	
เรียกใช้เมื่อ :	
ลำดับการทำงานปกติ : <ol style="list-style-type: none"> 5. Administrator ทำการ Login เพื่อเข้าใช้งานระบบ 6. ทำการป้อน Username และ Password ของผู้จะเข้าใช้ระบบ 7. ระบบทำการตรวจสอบความถูกต้องของข้อมูล 8. ข้อมูลถูกต้องทำการเข้าใช้งานส่วนต่างๆของระบบได้ 	
เงื่อนไขจากการทำงานปกติ : <ol style="list-style-type: none"> 3a. ระบบทำการตรวจสอบแล้วหากไม่พบข้อมูลจะทำการแสดงข้อความผิดพลาดขึ้นและกลับเข้าสู่การ Login ใหม่อีกครั้ง 	

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 3.8 แสดงคำอธิบายการสร้างกฎใหม่

ชื่อยุสเคส : Create New Rule	ไอดี : 2
ไฟเมรีเอ็กเตอร์ : Administrator	
สะเท็กโฮลเตอร์ :	
คำอธิบายโดยย่อ : จะทำการสร้างกฎต่างๆที่จะใช้ในการทำงานของไฟร์วอลล์	
เรียกใช้เมื่อ :	
ความสัมพันธ์กับยูสเคสอื่น : Association : - Include : Extend : Generalization :	
ลำดับการทำงานปกติ : 5. Administrator ต้องการทำการสร้างกฎใหม่ โดยป้อนข้อมูลที่จำเป็น เช่น ไอพีต้นทาง , พอร์ตต้นทาง , ไอพีปลายทาง , พอร์ตปลายทาง , โพรโตคอล , อินเตอร์เฟซ 6. ตรวจสอบกฎที่จะทำการเพิ่มว่าถูกต้องตามหลักการสร้างกฎหรือไม่ 7. ทำการเพิ่มกฎและบันทึกกฎที่เพิ่มเข้าสู่ระบบ 8. ระบบแจ้งผลการเพิ่มกฎ	
เงื่อนไขจากการทำงานปกติ : 2a. หากกฎที่ทำการสร้างไม่ถูกต้อง ระบบจะแสดงข้อความผิดพลาดขึ้นและไม่ทำการบันทึก ผล	

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 3.9 แสดงคำอธิบายการแก้ไขกฎในระบบ

ชื่อยูสเคส : Edit Rule	ไอดี : 3
ไฟเมรีเอ็คเตอร์ : Administrator	
สเตอร์กโฮลเตอร์ :	
คำอธิบายโดยย่อ : ทำการแก้ไขกฎต่างๆที่ได้มีการสร้างไว้ทั้งที่สร้างใหม่และมีอยู่เดิม	
เรียกใช้เมื่อ :	
ความสัมพันธ์กับยูสเคสอื่น : Association : - Include : - Extend : - Generalization : -	
ลำดับการทำงานปกติ : 9. Administrator เรียกดูกฎที่สร้างขึ้น 10. ตรวจสอบว่ามีกฎอยู่หรือไม่ 11. ทำการอ่านกฎที่มีอยู่ออกมา 12. Administrator จะทำการส่งข้อมูลที่ต้องการปรับปรุง 13. ตรวจสอบกฎที่ทำการแก้ไขว่าถูกต้องตามหลักการสร้างกฎ 14. ทำการปรับปรุงและแก้ไขกฎไฟร์วอลล์ 15. ทำการบันทึกกฎที่ได้รับการแก้ไขเข้าสู่ระบบ 16. ระบบแจ้งผลการบันทึกกฎที่ได้รับการแก้ไขใหม่	
เงื่อนไขจากการทำงานปกติ : 1a. หากไม่พบกฎที่สร้างขึ้นระบบจะแสดงข้อผิดพลาดขึ้น 4a. หากกฎที่ทำการแก้ไขไม่ถูกต้อง ระบบจะแสดงข้อความผิดพลาดขึ้นและไม่ทำการบันทึกผล	

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
 ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 3.10 แสดงคำอธิบายการลบกฎในระบบ

ชื่อยูสเคส : Delete Rule	ไอดี : 4
ไฟเวรีเอ็คเตอร์ : Administrator	
สะเต็กโฮลเดอร์ :	
คำอธิบายโดยย่อ : จะทำการลบกฎต่างๆที่ได้มีการสร้างไว้ที่มีอยู่เดิม	
เรียกใช้เมื่อ :	
ความสัมพันธ์กับยูสเคสอื่น : Association : - Include : - Extend : - Generalization : -	
ลำดับการทำงานปกติ : 7. Administrator ทำการเรียกดูกฎที่สร้าง 8. ตรวจสอบว่ามีกฎอยู่หรือไม่ 9. ทำการอ่านกฎที่มีอยู่ออกมา 10. ตรวจสอบกฎที่จะทำการลบว่าสามารถทำการลบได้หรือไม่ 11. ทำการลบกฎและบันทึกผล 12. ระบบแจ้งผลการลบ	
เงื่อนไขจากการทำงานปกติ : 1a. หากไม่พบกฎที่สร้างขึ้นระบบจะแสดงข้อผิดพลาดขึ้น 4a. หากกฎที่ทำการลบไม่ถูกต้องระบบจะไม่แสดงข้อความผิดพลาดขึ้น	

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 3.11 แสดงคำอธิบายการแสดงกฎที่มีในระบบ

ชื่อยุสเคส : Show Rule	ไอดี : 5
ไฟเมรีเอ็คเตอร์ : Administrator	
สะเต็กโฮลเดอร์ :	
คำอธิบายโดยย่อ : จะทำการเรียกกฎมาแสดงผล	
เรียกใช้เมื่อ :	
ความสัมพันธ์กับยูสเคสอื่น :	
Association : -	
Include : -	
Extend : -	
Generalization : -	
ลำดับการทำงานปกติ :	
<ol style="list-style-type: none"> 1.Administrator ทำการเรียกดูกฎที่สร้าง 2.ตรวจสอบว่ามีกฎอยู่หรือไม่ 3.ทำการอ่านกฎที่มีอยู่ออกมา 	
เงื่อนไขจากการทำงานปกติ :	
1a.เมื่อยังไม่มีการแสดงผลว่าไม่พบกฎ	

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 3.12 แสดงคำอธิบายการแสดงสถานะของกฎ

ชื่อยุสเคส : Show Status Rule	ไอดี : 6
ไฟเมรีเอ็คเตอร์ : Administrator	
สะเต็กโฮลเตอร์ :	
คำอธิบายโดยย่อ : ทำการแสดงผลที่ทำงานอยู่ ณ ปัจจุบัน	
เรียกใช้เมื่อ :	
ความสัมพันธ์กับยูสเคสอื่น :	
Association : -	
Include : -	
Extend : -	
Generalization : -	
ลำดับการทำงานปกติ :	
<ol style="list-style-type: none"> 1. Administrator ทำการเรียกดูกฎ 2. ระบบทำการแสดงผลกฎที่ทำงานอยู่ ณ ปัจจุบัน 	
เงื่อนไขจากการทำงานปกติ :	

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 3.13 แสดงคำอธิบายการเริ่มระบบใหม่

ข้อยุสเคส : Reboot System	ไอดี : 7
ไฟแอมริเอ็คเตอร์ : Administrator	
สะเท็กโฮลเดอร์ :	
คำอธิบายโดยย่อ : ทำการเริ่มต้นการทำงานระบบใหม่	
เรียกใช้เมื่อ :	
ความสัมพันธ์กับยูสเคสอื่น :	
Association :	
Include :	
Extend :	
Generalization :	
ลำดับการทำงานปกติ :	
1) Administrator ทำการร้องขอเพื่อขอเริ่มการทำงานระบบใหม่	
2) ระบบเริ่มทำงานใหม่	
เงื่อนไขจากการทำงานปกติ :	

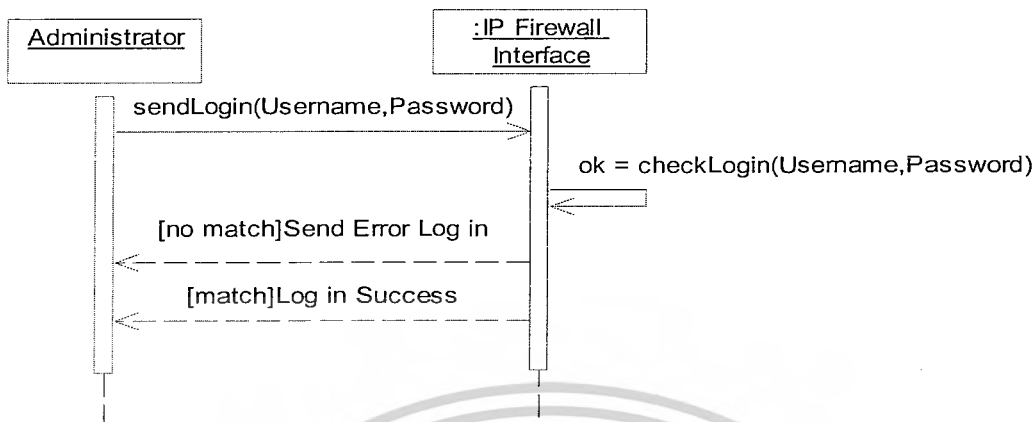
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 3.14 แสดงคำอธิบายการแสดงผลหมายเลขไอพี

ข้อยูสเคส : Show IP	ไอพี : 8
ไฟเมรีเอ็คเตอร์ : Administrator	
สะเด็กโฮสเคอร์ :	
คำอธิบายโดยย่อ :	
เรียกใช้เมื่อ :	
ความสัมพันธ์กับยูสเคสอื่น : Association : - Include : - Extend : - Generalization : -	
ลำดับการทำงานปกติ : 1) Administrator ทำการร้องขอแก้ไข ไอพีแอดเดรสของอินเทอร์เน็ตเฟส 2) ระบบทำการแสดงไอพีแอดเดรสของอินเทอร์เน็ตเฟสนั้น 3) Administrator ทำการแก้ไข ไอพีแอดเดรสของอินเทอร์เน็ตเฟส 4) ระบบทำการตรวจสอบความถูกต้อง 5) ระบบทำการบันทึกผล 6) ระบบทำการแสดงผลให้ผู้ใช้งานทราบ	
เงื่อนไขจากการทำงานปกติ : 4a) ถ้าผู้ใช้กรอกไอพีแอดเดรสไม่ถูกต้อง ระบบจะแจ้งเตือน ให้ผู้ใช้ทำการกรอกค่าใหม่	

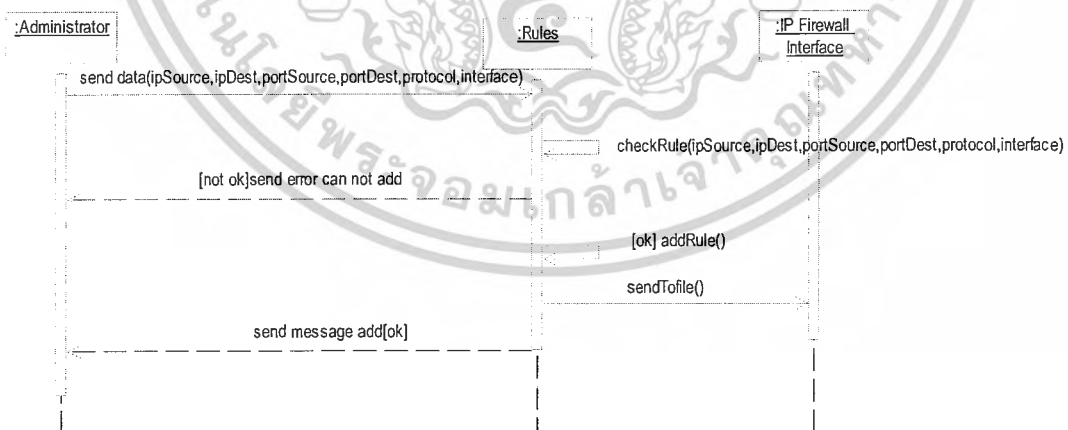
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Sequence Diagram



รูปที่ 3.41 แผนภาพแสดงลำดับการทำงานของการทำงานของการเข้าใช้งานระบบ

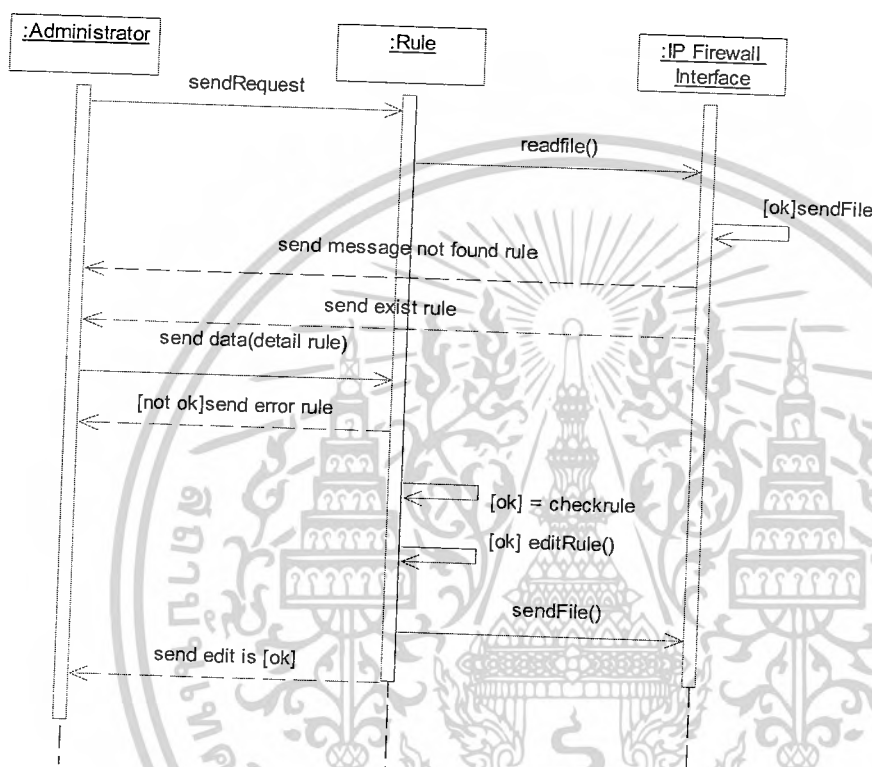
Sequence Diagram ของ Login เป็นการแสดงถึงการทำงานของ Login Firewall Use case โดยเมื่อผู้ดูแลระบบเข้ามาทำงานโดยการป้อนข้อมูลในส่วนของ username,password โมดูลในส่วนของผู้ดูแลระบบก็จะทำการตรวจสอบเช็คข้อมูลและถ้าหากข้อมูลถูกต้องก็จะอนุญาตให้ผู้ดูแลระบบสามารถใช้งานระบบต่างๆ ได้ถ้าไม่ถูกต้องก็จะทำการแจ้งข้อความผิดพลาดขึ้น



รูปที่ 3.42 แผนภาพแสดงลำดับการทำงานของการทำงานของการสร้างกฎใหม่

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

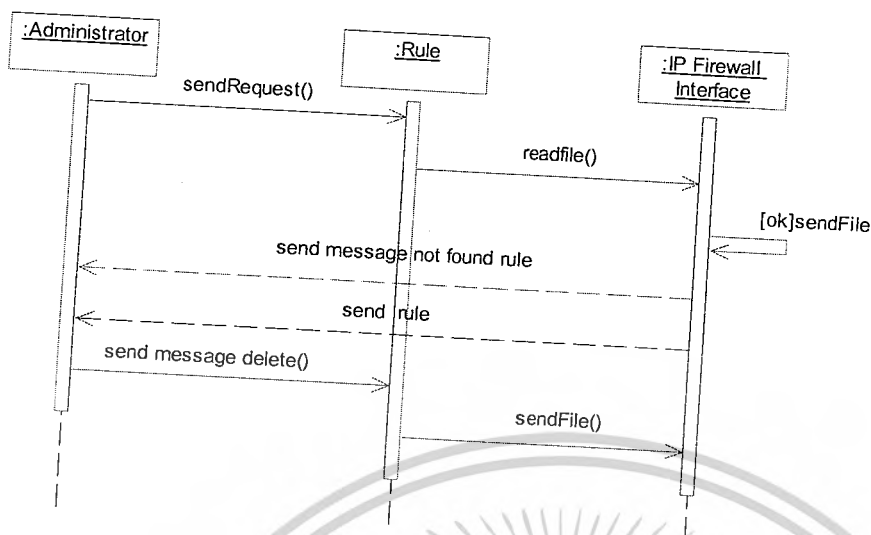
Sequence Diagram ของ Create New Rule หลังจากผู้ดูแลระบบได้ทำการล็อกอินเข้าสู่ระบบเรียบร้อยแล้วจะทำการสร้างกฎของไฟร์วอลล์โดยป้อนข้อมูลในส่วนของ ip source, ip destination, port source, port destination, protocol, interface เข้าสู่ระบบแล้ว ระบบจะทำการตรวจเช็คข้อมูลที่ส่งเข้ามาสู่ระบบว่าถูกต้องหรือไม่และแจ้งผลการสร้างกฎให้กับผู้ดูแลระบบ



รูปที่ 3.43 แผนภาพแสดงลำดับการทำงานของการทำงานของการแก้ไขกฎที่มีในระบบ

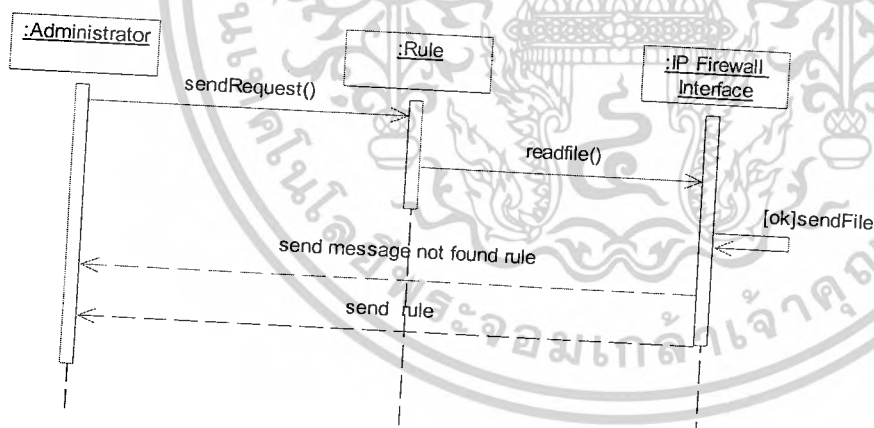
Sequence Diagram ของ Edit Existing Rules Use case แสดงการทำงานในส่วนของการแก้ไขกฎที่ได้มีการสร้างไว้แล้วโดยผู้ใช้งานจะทำการร้องขอและระบบจะทำการตรวจสอบว่ามีกฎอยู่ในไฟล์ข้อมูลหรือไม่ ถ้าพบระบบก็จะทำการดึงกฎจากไฟล์และทำการแสดงผลของกฎ จากนั้นผู้ดูแลระบบทำการแก้ไขโดยผู้ใช้งานทำการป้อนข้อมูลเพิ่มหรือแก้ไขข้อมูลจากนั้นนำส่งเข้าสู่ระบบเพื่อตรวจเช็คความถูกต้องและระบบจะแจ้งผลการตรวจสอบ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 3.44 แผนภาพแสดงลำดับการทำงานของลบกฎที่มีในระบบ

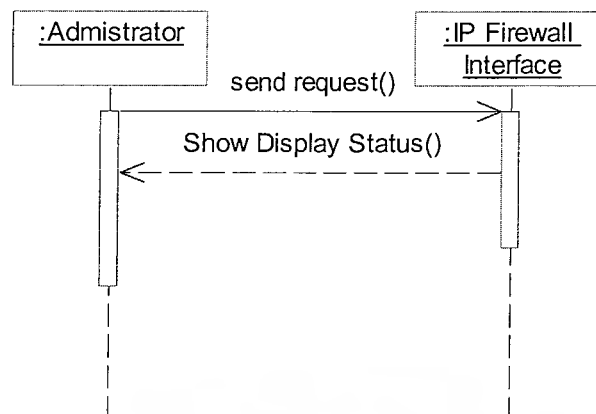
Sequence Diagram ของ Delete Rules แสดงการทำงานในส่วนของการลบกฎที่ได้มีการสร้างไว้แล้วโดยผู้ใช้งานจะส่งคำร้องขอและระบบจะทำการตรวจสอบในไฟล์ข้อมูลว่ามีกฎอยู่หรือไม่ ถ้าพบก็จะทำให้ทำการลบกฎได้ จากนั้นระบบจะแจ้งผลการทำงาน



รูปที่ 3.45 แผนภาพแสดงลำดับการทำงานของแสดงกฎที่มีในระบบ

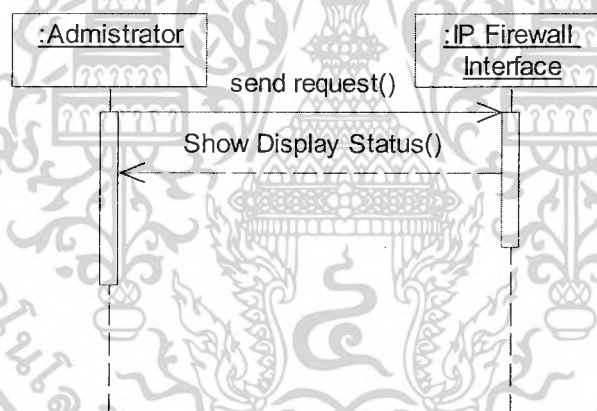
Sequence Diagram ของ Show Rule Use case แสดงการทำงานในส่วนของการแก้ไขกฎที่ได้มีการสร้างไว้แล้วโดยผู้ใช้งานจะทำการร้องขอและระบบจะทำการตรวจสอบว่ามีกฎอยู่ในไฟล์ข้อมูลหรือไม่ ถ้าพบระบบก็จะทำการดึงกฎจากไฟล์และทำการแสดงผลของกฎ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 3.46 แผนภาพแสดงลำดับการทำงานของการทำงานของการแสดงกฎที่ทำงานอยู่

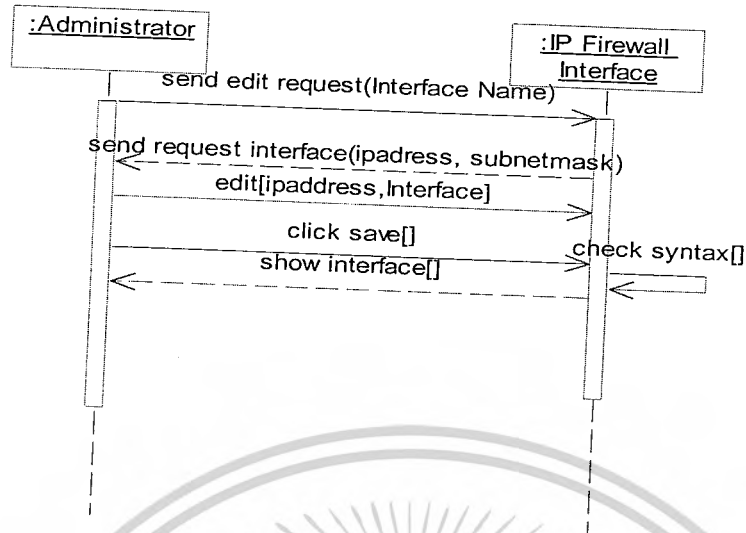
Sequence Diagram ของ Show Status Rule แสดงการทำงานของกฎที่ทำงานอยู่ ณ ขณะนั้น ระบบ จะทำการอ่านค่ากฎที่มีอยู่ในหน่วยความจำมาแสดงผล



รูปที่ 3.47 แผนภาพแสดงลำดับการทำงานของการทำงานการเริ่มต้นระบบใหม่

Sequence Diagram ของ Reboot System ผู้ใช้ทำการร้องขอให้มีการเริ่มต้นทำงานระบบใหม่ ระบบจะทำงานตามที่ผู้ใช้ร้องขอ

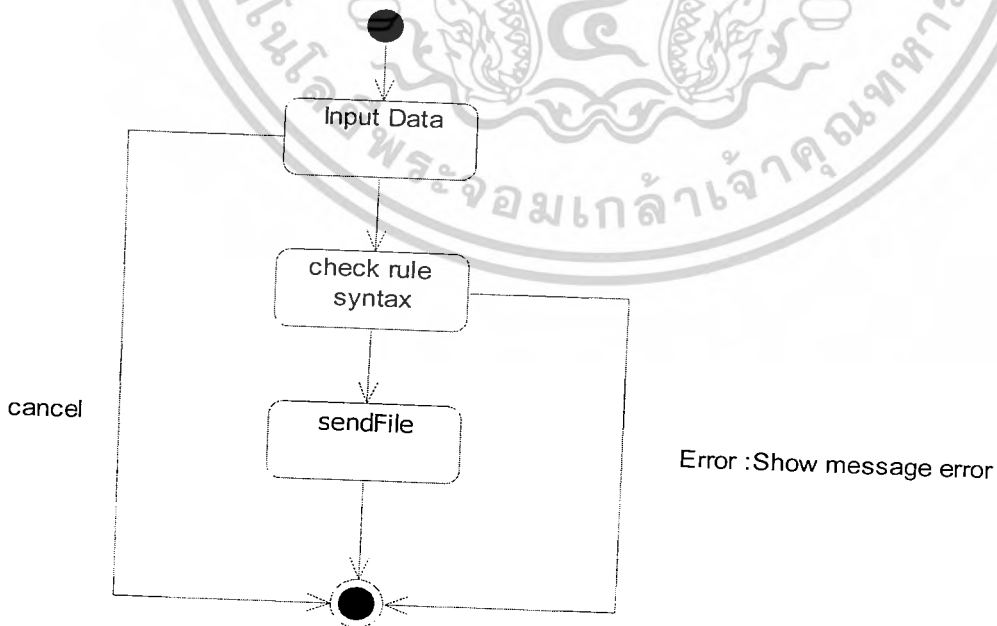
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



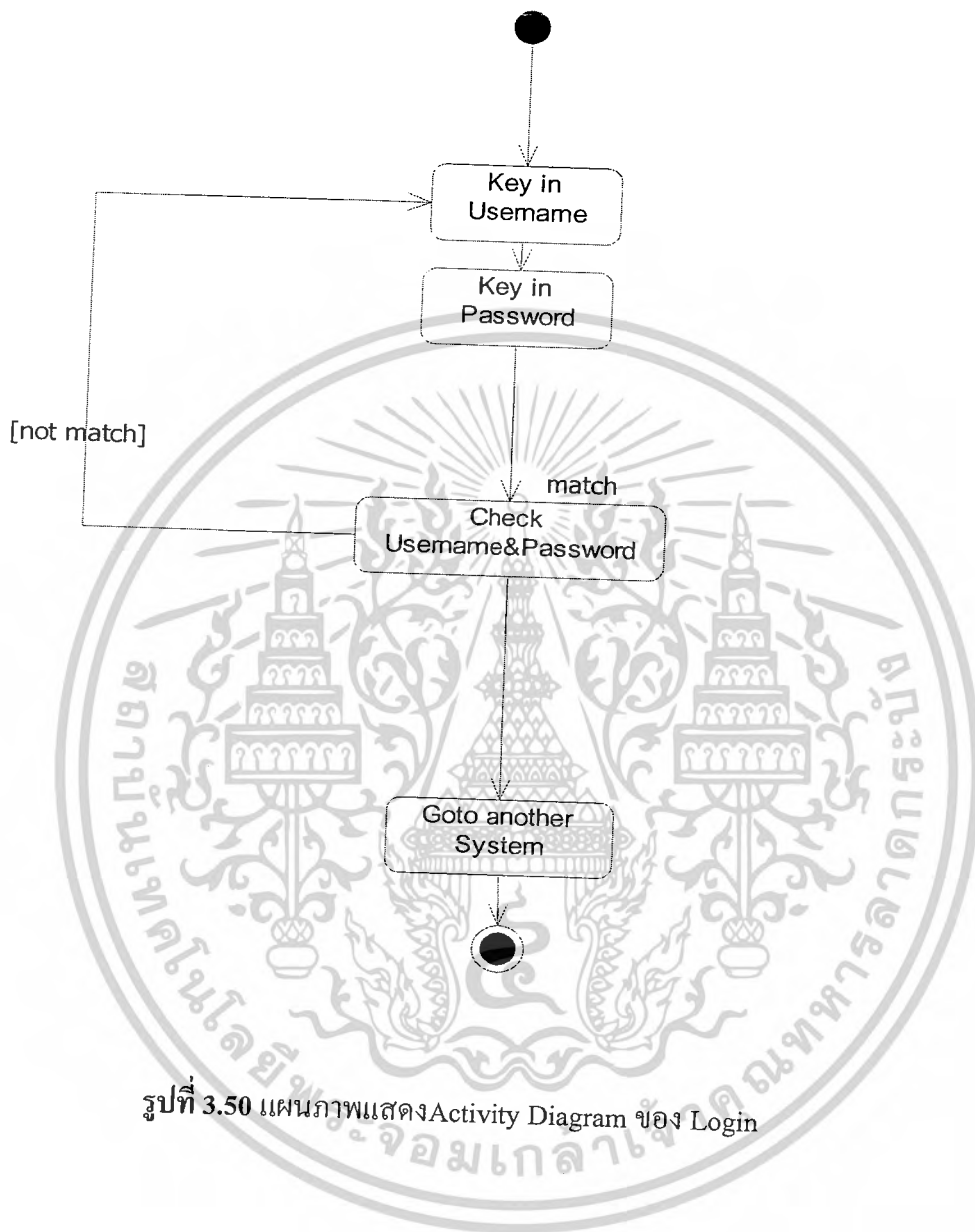
รูปที่ 3.48 แผนภาพแสดงลำดับการทำงานของการทำงานของการแก้ไขหมายเลขไอพี

Sequence Diagram ของ Show IP แสดงการทำงานในส่วนของการแก้ไขไอพีแอดเดรสของอินเทอร์เฟซต่างๆ รวมถึง default gateway โดยเมื่อผู้ใช้ทำการแก้ไขไอพีแอดเดรสของอินเทอร์เฟซนั้นๆ เรียบร้อยแล้ว ระบบทำการบันทึกลงสู่ไฟล์ และทำการแสดงผลให้ผู้ใช้ทราบ

Activity Diagram

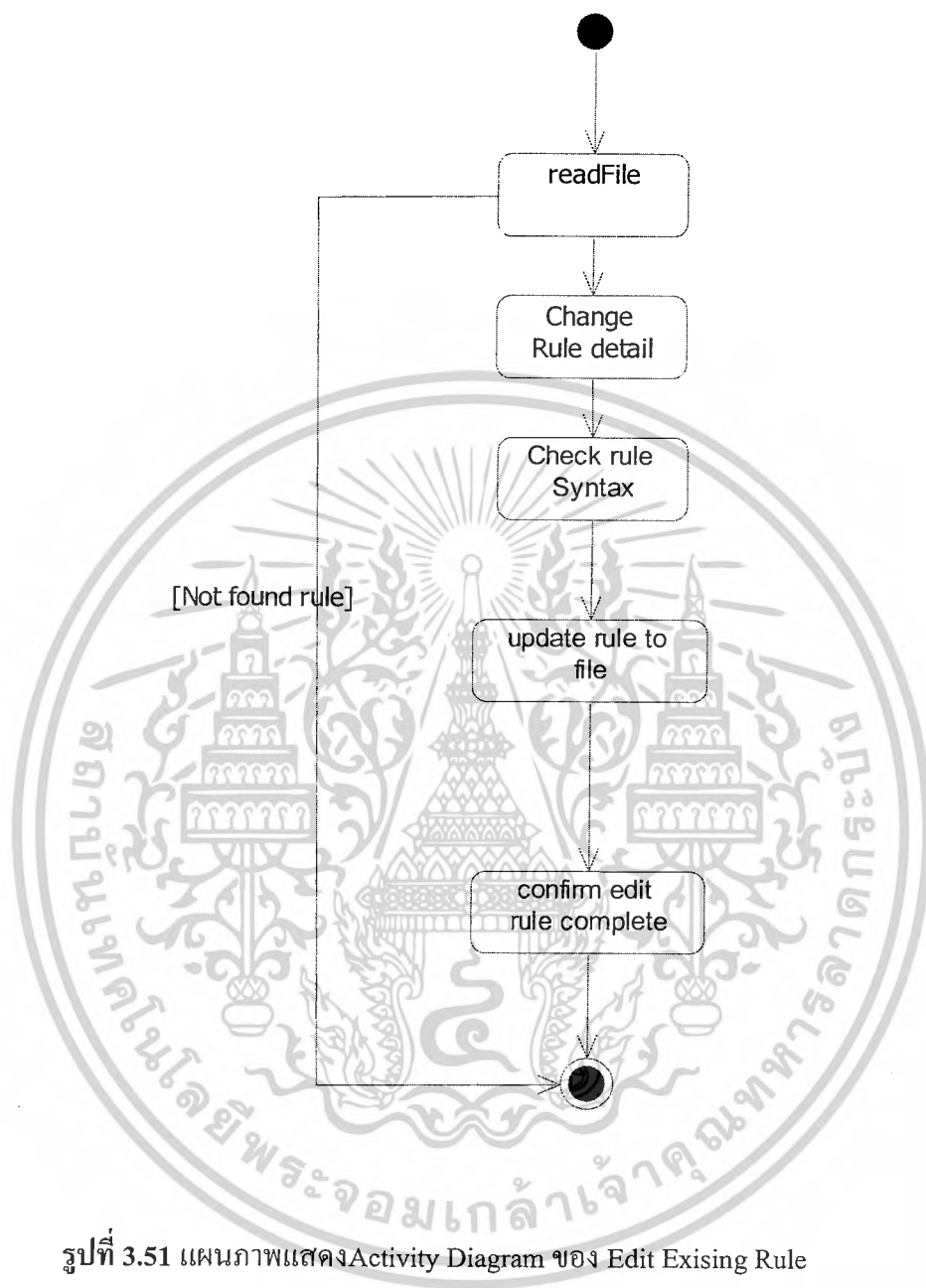


รูปที่ 3.49 แผนภาพแสดงActivity Diagram ของ Create New Rule เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น เมื่อนำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



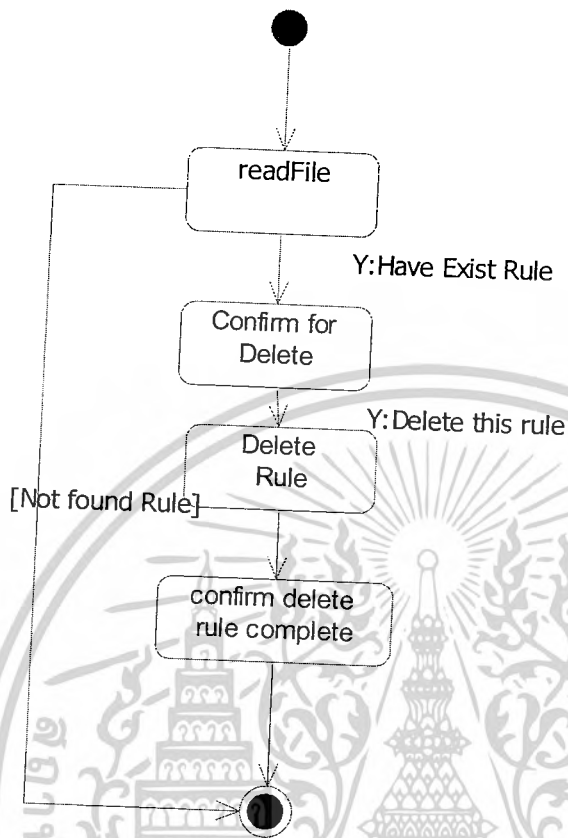
รูปที่ 3.50 แผนภาพแสดง Activity Diagram ของ Login

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

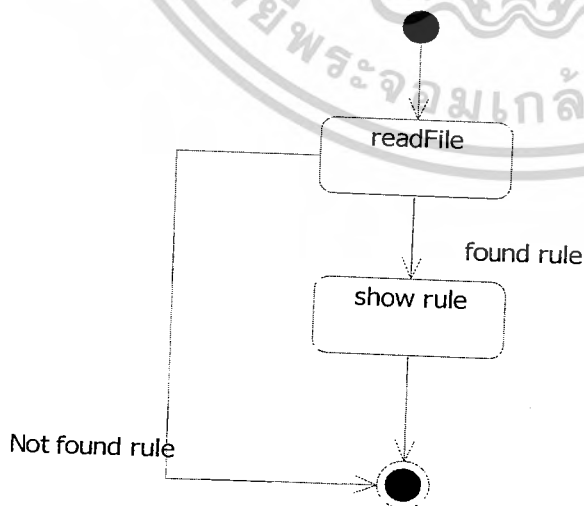


รูปที่ 3.51 แผนภาพแสดงActivity Diagram ของ Edit Existing Rule

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

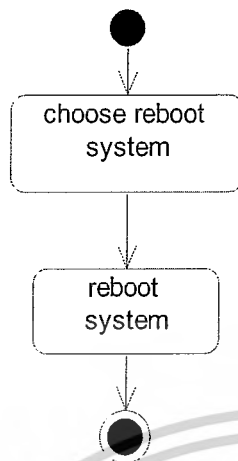


รูปที่ 3.52 แผนภาพแสดง Activity Diagram ของ Delete Rule

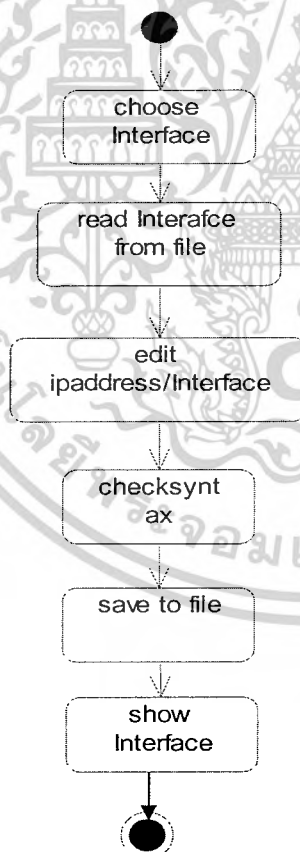


รูปที่ 3.53 แผนภาพแสดง Activity Diagram ของ Show Rule

เอกสารนี้เป็นเอกสารที่สงวนลิขสิทธิ์ไว้ ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 3.54 แผนภาพแสดงActivity Diagram ของ Reboot System



รูปที่ 3.55 แผนภาพแสดงActivity Diagram ของ Show IP

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 4

การพัฒนาโปรแกรมในส่วนต่างๆของระบบ

4.1 การแสดงผลการทำงานของคอมมานด์ไลน์อินเตอร์เฟส

4.1.1 แสดงหน้า main.csh

```
*** Welcome to Embedded Firewall System ***
```

```
*****  
** Embedded Firewall System setup **  
*****
```

- 1) Firewall Rules Module
- 2) Configuration Web Interface
- 3) Reboot System
- 4) System Configuration
- 5) Manual for user

```
Enter Your Option : █
```

รูปที่ 4.1 แสดงหน้าแรกของคอมมานด์ไลน์

4.1.2 แสดงหน้า firewall_rule.csh

```
** Firewall Rules Setup **  
*****
```

- 0) Go to Main Menu
- 1) Create Firewall Rules
- 2) Edit/Delete Firewall Rules
- 3) Enable Rules
- 4) Show Running Rules
- 5) Disable Rules
- 6) Enable Packet-Filtering
- 7) Disble Packet-Filtering
- 8) Setup Start-up Rules
- 9) PF Rule Syntax Manual

```
Enter Your Option : █
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับรูปที่ 4.2 แสดงหน้าของไฟร์วอลล์โมดูลอนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4.1.3 แสดงหน้า create.csh (สร้างกฎแบบ Manual)

```

*** Insert your rules manually below ***

Action [pass:block] : pass

Direction [in:out] : in

Interface [vr0:vr1:vr2:vr3] : vr0

Protocol [tcp:udp] :

If you want to choose all IP Address type "any"
or type IP Address that you want
Source IP Address : any

Port are entered as number
e.g. HTTP port 80 , FTP port 21
Source Port : 21

If you want to choose any IP Address type "any"
or type number of IP Address that you want
Destination IP Address : any

Port are entered as number
e.g. HTTP port 80 , FTP port 21
Destination Port :

```

รูปที่ 4.3 แสดงหน้าของสร้างกฎแบบคีย์ค่าด้วยตนเอง (manual)

4.1.4 แสดงหน้า enable.csh ซึ่งจะแสดงกฎที่เราทำการกำหนดไว้ในเทมพ์ไฟล์ (Temp File) ก่อนแล้วจึงจะให้เลือกตัดสินใจว่าจะนำกฎเหล่านี้มาทำงานหรือไม่

- 4) Show Running Rules
- 5) Disable Rules
- 6) Enable Packet-Filtering
- 7) Disble Packet-Filtering
- 8) Setup Start-up Rules
- 9) PF Rule Syntax Manual

Enter Your Option : 3

```

block out proto tcp from any port 80 to any port 80
pass in all
block out proto tcp to any port 80
pass in on vr0 from any port 80
pass in on vr0 from any port 21 to any

```

Do you want to proceed [y:n]? █

รูปที่ 4.4 แสดงหน้าการใช้งานกฎ (enable rule) ก่อนอนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับใช้ภายในเท่านั้น ไม่ควรเผยแพร่ให้ผู้อื่นได้รับรู้
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4.1.5 แสดงการตั้งค่าไอพี(IP) ให้กับอินเทอร์เฟซ (interface) ต่างๆ

```

*** Assign new IP Address below ***
Enter Interface [vr0:vr1:vr2:vr3] : vr1
Enter new IP Address : 192.168.100.11
Subnet masks are entered as binary count
e.g. Subnet masks 24,Your input is 255.255.255.0
Subnet masks : 24
Your new IP Address is Interface vr1 IP address 192.168.100.11/24
Set IP Interface Complete
Would you like to bring the vr1 interface up right now? [y/n]? █

```

รูปที่ 4.5 แสดงหน้าการตั้งค่าไอพี(IP)

4.1.6 แสดงค่าของไอพี(IP) ที่ทำการตั้งค่าไว้

```

*****
0) Go to Main Menu
1) Show IP Interface
2) Assign new IP Interface
3) Upgrade Firmware

Enter Your Option : 1

In0: flags=108843<UP, BROADCAST, RUNNING, SIMPLEX, MULTICAST, NEEDSGIANT> mtu 1500
    inet 192.168.100.10 netmask 0xfffff00 broadcast 192.168.100.255
    ether 00:0c:29:c3:57:75
plip0: flags=108810<POINTOPOINT, SIMPLEX, MULTICAST, NEEDSGIANT> mtu 1500
lo0: flags=8049<UP, LOOPBACK, RUNNING, MULTICAST> mtu 16384
    inet6 fe80::1%lo0 prefixlen 64 scopeid 0x3
    inet6 ::1 prefixlen 128
    inet 127.0.0.1 netmask 0xff000000
pflog0: flags=100<PROMISC> mtu 33208

Press Enter to continued... █

```

รูปที่ 4.6 แสดงหน้าการแสดงผลค่าไอพี(IP)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4.1.7 แสดงหน้าการรีบูท (reboot) ระบบ

```
*** Welcome to Embedded Firewall System ***
```

```
*****  
** Embedded Firewall System setup **  
*****
```

- 1) Firewall Rules Module
- 2) Configuration Web Interface
- 3) Reboot System
- 4) System Configuration
- 5) Manual for user

```
Enter Your Option : 3
```

```
Are you sure to reboot [y:n]? y
```

รูปที่ 4.7 แสดงหน้าการรีบูท

4.1.8 แสดงหน้าการจัดการเว็บอินเตอร์เฟซ

```
*****  
** Web Interface Configuration **  
*****
```

- 0) Go to Main Menu
- 1) Enable Web Interface
- 2) Disable Web Interface

```
Enter Your Option : 
```

รูปที่ 4.8 แสดงหน้าการจัดการเว็บอินเตอร์เฟซ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4.1.9 แสดงหน้า startup.csh

Start-up Rules will running when you reboot system

- 0) Go back to prevoius menu
- 1) Setup Start-up Rules from temp file
- 2) Setup Start-up Rules Manually
- 3) Edit/Delete Start-up Rules
- 4) Enable Start-up Rules

Enter Your Option : █

รูปที่ 4.9 แสดงหน้า startup.csh

4.2 การแสดงผลการทำงานของเว็บอินเตอร์เฟซ

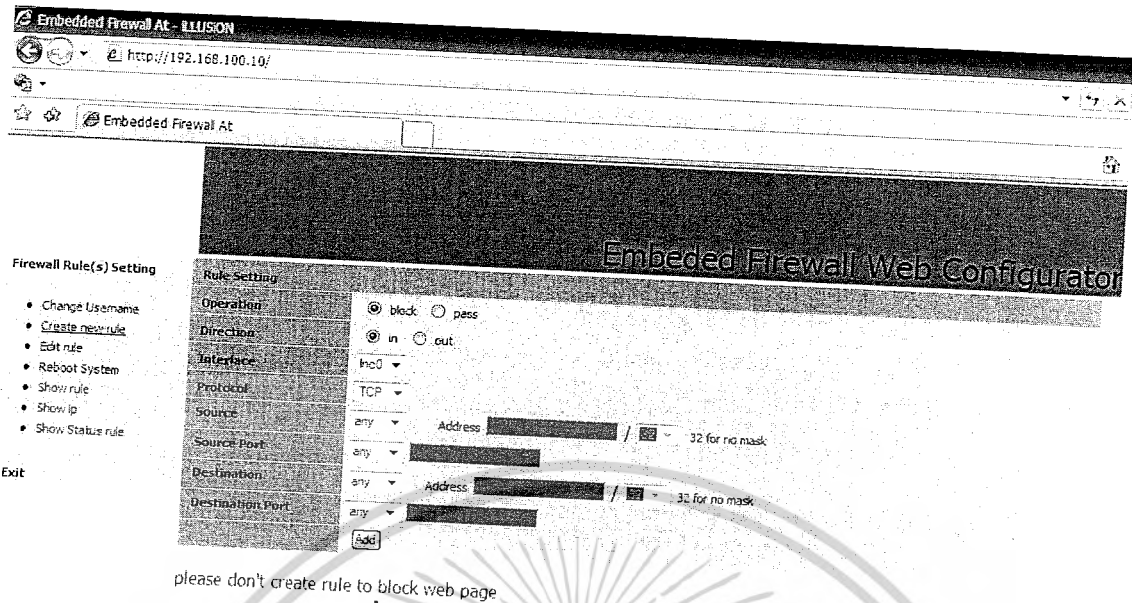
- ระบบอนุญาตให้ผู้ดูแลระบบทำการเปลี่ยนแปลงชื่อผู้ใช้และรหัสผ่าน โดยเมื่อผู้ดูแลระบบต้องการเปลี่ยนแปลงชื่อผู้ใช้และรหัสผ่านทำได้โดยการคลิกที่แถบการเปลี่ยนแปลงชื่อผู้ใช้งาน ดังรูป



รูปที่ 4.10 แสดงหน้าการเปลี่ยนแปลงชื่อผู้ใช้งาน

- ระบบอนุญาตให้ผู้ดูแลระบบสร้างกฎขึ้นมาใหม่ โดยทำการกรอกรายละเอียดของกฎที่ต้องการตามช่องที่กำหนดไว้ให้ โดยคลิกไปที่แถบการสร้าง ดังรูป

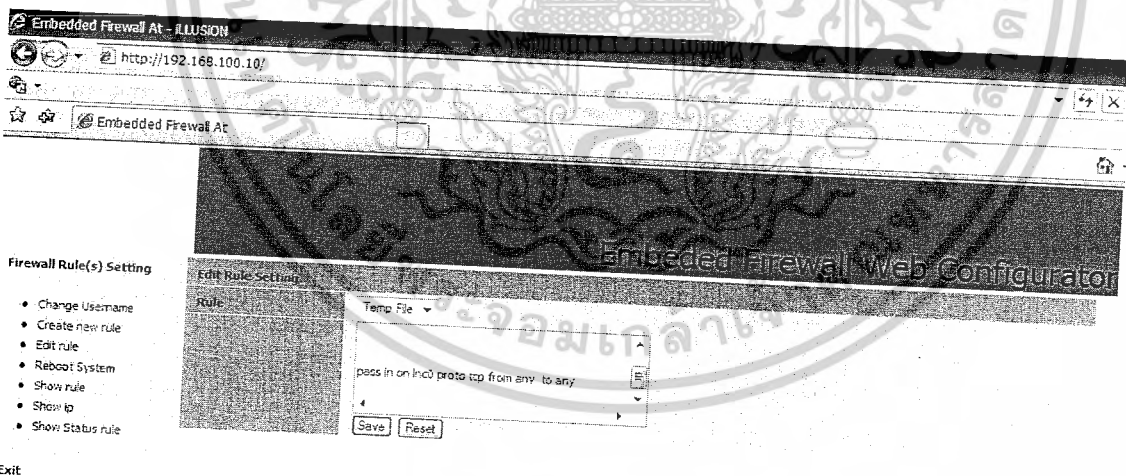
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.11 แสดงหน้าการสร้างกฎใหม่

- ระบบอนุญาตให้ผู้ดูแลระบบทำการแก้ไขกฎได้เอง ทั้งกฎที่อยู่ในบทไฟล์ และเทมปไฟล์ โดยคลิกที่แถบแก้ไขกฎ (Edit Rule) ดังรูป

ตัวอย่างกฎที่สร้างอยู่ในเทมปไฟล์



รูปที่ 4.12 แสดงตัวอย่างกฎที่มีอยู่ในเทมปไฟล์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตัวอย่างกฎที่สร้างอยู่ในบทไฟล์



รูปที่ 4.13 แสดงตัวอย่างกฎที่มีอยู่ในบทไฟล์

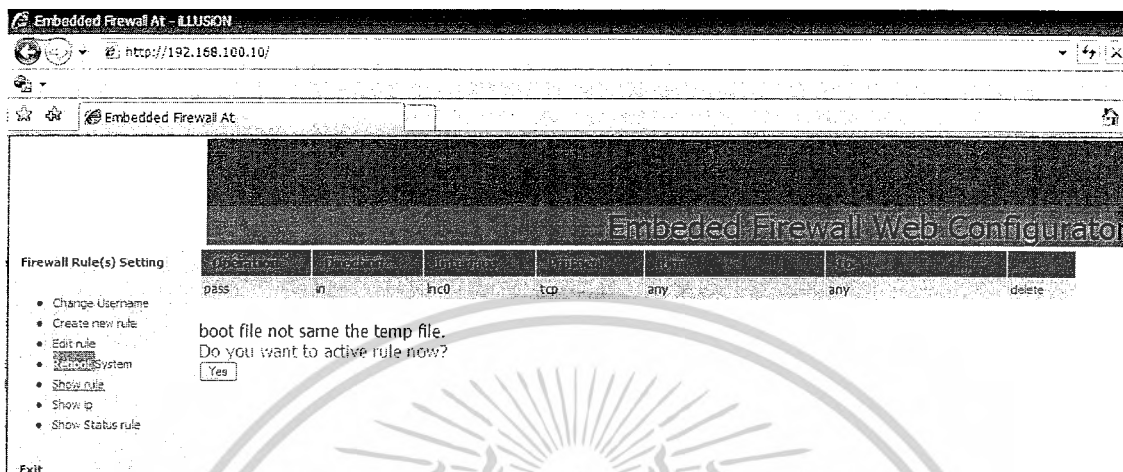
- ระบบทำการอนุญาตให้ผู้ดูแลระบบทำการรีบูตระบบขึ้นมาใหม่ได้ โดยการคลิกที่แถบรีบูตระบบ ดังรูป



รูปที่ 4.14 แสดงหน้าการรีบูตระบบ

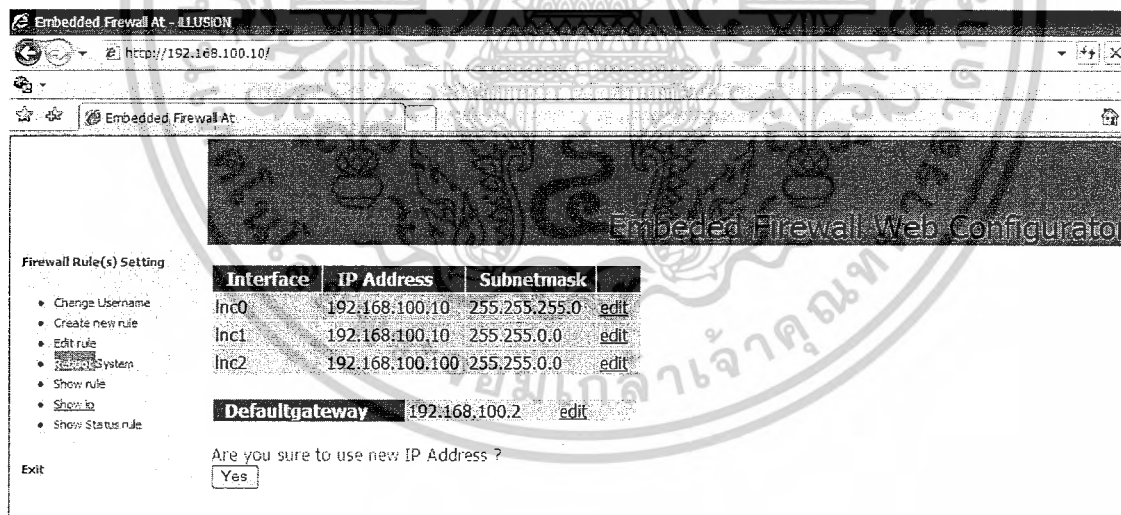
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- ระบบทำการแสดงกฎที่มีอยู่ทั้งหมด ลบกฎได้ และสามารถโหลดกฎที่ต้องการใช้งาน หน่วยความจำได้ โดยคลิกที่แถบ การแสดงกฎ ดังรูป



รูปที่ 4.15 แสดงหน้าการแสดงกฎ

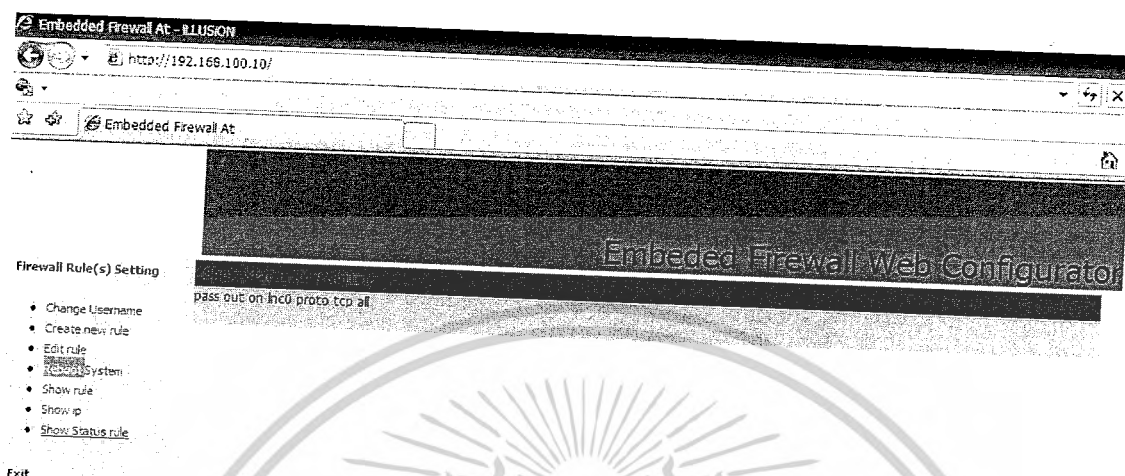
- ระบบอนุญาตให้ผู้ใช้ระบบทำการแก้ไขค่าไอพีแอดเดรสของอินเตอร์เฟซที่มีอยู่ในระบบได้ โดยคลิกที่แถบ การแสดงไอพี ดังรูป



รูปที่ 4.16 แสดงหน้าการแสดงไอพี

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- ระบบทำการแสดงกฎที่ทำงานอยู่ ณ ปัจจุบัน โดยคลิกที่แถบ การแสดงสถานะของกฎ ดังรูป



รูปที่ 4.17 แสดงหน้าการแสดงผลสถานะของกฎ



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 5

สรุปผลการวิจัย และข้อเสนอแนะ

5.1 สรุปผลการวิจัย

การพัฒนาระบบเกิดภายในห้องทดลองซึ่งเป็นสภาวะแวดล้อมที่ถูกติดตั้งมาแต่เดิม โปรแกรมที่ใช้คือระบบปฏิบัติการฟรีบีเอสดี (FreeBSD) ซีเชลล์สคริปต์ (C-shell Script) โปรแกรมเว็บเซิร์ฟเวอร์ไลท์ทีพีดี (lighttpd) และภาษาพีเอชพี (PHP) พัฒนาให้ทำงานได้จริงบนบอร์ดเดี่ยว (single board) ของ soekris รุ่น 5501

5.1.1 ข้อจำกัดของระบบ

1. อุปกรณ์ได้รับการติดตั้งตัวประมวลผลกลางมาจากโรงงานทำให้มีความสามารถในการทำงานที่จำกัด นอกจากนี้อุปกรณ์ประเภทคอมแพคแฟลชซึ่งใช้ทำหน้าที่แทน ฮาร์ดดิส ถึงแม้จะมีความทนทานสูง ขนาดเล็กและราคาถูก แต่มีการทำงานที่ช้ากว่ามากและมีความจุข้อมูลน้อย จึงทำให้ระบบที่เราสร้างขึ้นถูกจำกัดด้วยขนาดพื้นที่และความเร็วในการเข้าถึงข้อมูลของคอมแพคแฟลช

2. อุปกรณ์ไฟร์วอลล์ ที่พัฒนาครั้งนี้ไม่ได้เพิ่มเติมคุณสมบัติอื่นๆ เช่น การทำหน้าที่แจก IP Address (DHCP Server) , การทำหน้าที่เป็นเนต (NAT : Network Address Translation) ดังนั้นเมื่อนำไปใช้งานจริงในเครือข่ายจะต้องจัดหาเครื่องเวิร์ฟเวอร์ (Server) ที่ทำหน้าที่ดังกล่าวมาเพิ่มเพื่อเป็นการลดภาระงานของอุปกรณ์ไฟร์วอลล์

3. การพัฒนาครั้งนี้เลือกใช้โปรแกรมไลท์ทีพีดี (lighttpd) มาทำเว็บเซิร์ฟเวอร์ที่มีความสามารถใกล้เคียงกับ โปรแกรมเว็บเซิร์ฟเวอร์อื่นๆ แต่มีขนาดไม่ใหญ่เพื่อสะดวกในการทำเป็น MiniBSD นอกจากนี้ lighttpd ยังสามารถทำ Authentication ได้แต่การพัฒนาโครงการนี้การทำ Authentication ยังไม่ได้ทำการเข้ารหัสของ username และ password ซึ่งอาจโดนดักจับได้จึงควรมีการพัฒนาเพิ่มเติมในส่วนนี้

5.2 ปัญหาที่พบในการทำงาน

1. การปรับแต่งระบบจากระบบฟรีบีเอสดีธรรมดา จำเป็นต้องใช้ความรู้และความเข้าใจในสถาปัตยกรรมของระบบปฏิบัติการ ทำให้ใช้เวลาในการศึกษาเองนานมาก

2. ความไม่เสถียรของระบบปฏิบัติการมินิบีเอสดี (MiniBSD) เป็นเพราะระบบปฏิบัติการมินิบีเอสดีเป็นระบบปฏิบัติการที่เกิดจากการดัดแปลงระบบปฏิบัติการฟรีบีเอสดี (FreeBSD) ทำให้ความเสถียรของระบบขึ้นอยู่กับารปรับแต่งของผู้สร้างเอง ระบบนี้เดิมทีเขียนขึ้นบนฮาร์ดดิสก์ เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ขนาด 20 กิกะไบต์แล้วนำไปปรับแต่งเพื่อใช้กับคอมแพคแฟลชการ์ดและเกิดปัญหาขึ้นในระบบ ดังนี้

2.1 ความผิดพลาดเมื่อเริ่มต้นระบบ เกิดจากการเขียนสคริปต์ (Script) ซึ่งกำหนดค่าเริ่มต้นของระบบในส่วนต่างๆ ความผิดพลาดในข้อนี้จะเกิดขึ้นบางครั้งที่ระบบเริ่มการทำงาน (Booting) ซึ่งในตอนนี้ก็เกิดความผิดพลาดนี้เป็นบางครั้ง ในการเริ่มทำงานใหม่ (Reboot) สันนิษฐานว่าเกิดจากการที่อุปกรณ์ที่มีความแตกต่างกัน เช่น จากฮาร์ดดิสก์ (Hard disk) มายังคอมแพคแฟลชการ์ด (Compact flash card) ซึ่งมีความจุข้อมูลแตกต่างกัน ทำให้เมื่อเริ่มการทำงานของระบบเกิดการระบุขนาดของพื้นที่ผิดพลาด ขณะนี้กำลังทำการแก้ไข (23 กันยายน 2550)

2.2 ความผิดพลาดที่เกิดจากส่วนกำหนดค่าเริ่มต้น เกิดจากการเขียนเชลล์สคริปต์ (Shell script) ที่กำหนดค่าเริ่มต้นของระบบผิดพลาด ทำให้ค่าที่กำหนดมาแต่เดิมบางค่าไม่สามารถใช้ได้ เมื่อนำระบบมาใช้ในอุปกรณ์ชนิดใหม่

2.3 ความผิดพลาดที่เกิดจากการกำหนดเวลาของเครื่อง เกิดจากการที่ไม่ได้กำหนดสถานที่ในการเก็บค่าของซีมอสคล็อก (C_Mos_Clock) ซึ่งมีผลให้เมื่อทำการตัดแปลงระบบจากฟรีบีเอสดี (FreeBSD) มาเป็นมินิบีเอสดี (MiniBSD) แล้ว ระบบหาเวลาในเครื่องไม่พบแล้วไม่สามารถตั้งค่าเริ่มต้นที่เคยกำหนดไว้ออกมาได้

2.4 ความผิดพลาดที่เกิดจากการกำหนดอุปกรณ์ในระบบ เกิดจากการที่ไม่ได้กำหนดอุปกรณ์ที่จำเป็นในระบบทั้งหมด เมื่อระบบเริ่มต้นการทำงานทำให้ระบบหาอุปกรณ์ที่ต้องการนั้นไม่เจอและเป็นผลให้ระบบทำงานค้างไม่ทำการตอบสนอง (hang)

2.5 ความผิดพลาดในการกำหนดไฟล์สนับสนุนของระบบ เนื่องจากไฟล์นี้เป็นไฟล์ที่ช่วยตรวจสอบบัฟเฟอร์ (Buffer) หน่วยความจำที่มี (Free RAM) โมดูล (Module) ที่จำเป็น ค่าคงที่ (Parameter) ค่าองค์ประกอบ (Configuration file) ทำให้ระบบสามารถเริ่มการทำงานได้ เมื่อเกิดความผิดพลาดขึ้นระบบจะสามารถเริ่มการทำงานได้ช่วงเวลาหนึ่งแล้วจะหยุดทำการตอบสนอง

2.6 ความผิดพลาดที่เกิดจากการเมาท์ (Mount) อุปกรณ์ เนื่องจากการเมาท์อุปกรณ์ทำให้เราสามารถรู้ว่าในอุปกรณ์นั้นมีข้อมูลอะไรอยู่บ้าง เมื่อไฟล์นี้เกิดความผิดพลาดขึ้นระบบจะแจ้งข้อผิดพลาดโดยให้เรากำหนดที่อยู่เต็มของข้อมูล แต่ถึงจะกำหนดไปอย่างถูกต้องก็ยังไม่สามารถหาข้อมูลนั้นเจอได้

2.7 ความเข้าใจในการใช้เครื่องมือของระบบปฏิบัติการ โดยเป็นการเลือกฟังก์ชันต่างๆ ของระบบเดิม มาลงในระบบมินิบีเอสดีทำให้ไอบารีบางส่วนทำงานหรือไม่สามารถเรียกใช้ได้ ปัญหานี้เราสามารถแก้ไขได้โดยดูใน เว็บไซต์ www.freebsd.org ซึ่งจะมีผู้คนเข้าไปถามตอบปัญหาเป็นจำนวนมาก

2.8 การเมาท์ไฟล์ซิสเต็มของระบบ เมื่อมีการเขียนระบบขึ้นมาแล้วต้องการให้ทำงานได้ เราจำเป็นต้องล้างข้อมูลก่อน จากนั้นจึงเมาท์ไฟล์ขึ้นมาใหม่ แต่มีความแตกต่างระหว่างการสร้างเอกสารเป็นเอกสารที่สงวนไว้สำหรับภารกิจการศึกษาค้นคว้าเท่านั้น เมื่ออนุญาตให้ไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เมมโมรีคิสและไฟล์ซิสเต็มเดิม โดยไฟล์ซิสเต็มจะกำหนดค่าในลาเบลหลักเป็น 1 1 เพื่อจะมีการเช็คระบบหากมีการแก้ไข ส่วนลาเบลอื่นๆจะกำหนดค่าไว้เป็น 0 0 เพื่อให้ระบบทำงานได้รวดเร็ว แต่ในคอมแพคแฟลชจะไม่สามารถมองเห็นลาเบลเหล่านี้ได้ การแก้ไขปัญหาสามารถทำได้โดยกำหนดค่าของลาเบลที่ไม่ใช่ลาเบลหลักเป็น 2 2

2.9 การตั้งค่าระบบซึ่งเป็น read-only ให้สามารถเปลี่ยนแปลงค่าได้แต่ละไฟล์ตามที่กำหนด โดยปกติจะทำการเม้าท์ทั้งลาเบลขึ้นมาใหม่ แต่หากทำอย่างนั้นระบบไฟล์ซิสเต็มบางตัวจะได้รับผลกระทบจนไม่สามารถทำงานได้

2.10 เนื่องจากการทำงานของระบบไฟร์วอลล์มีสองอินเตอร์เฟซคือ คอมมานด์ไลน์และเว็บอินเตอร์เฟซ ซึ่งทั้งสองอย่างมีสภาพแวดล้อมการทำงานที่แตกต่างกันจึงเป็นปัญหาสำหรับส่วนเคอร์เนลที่ต้องทำการปรับสภาพแวดล้อมให้ทั้งสองอินเตอร์เฟซ ทำงานและมีการส่งข้อมูลเป็นข้อมูลเดียวกัน ยกตัวอย่างเช่น การปรับปรุงกฎของไฟร์วอลล์ซึ่งเว็บอินเตอร์เฟซจะทำให้ที่ละข้อจากหน้าสร้างกฎใหม่ (create new rule) และสามารถปรับปรุงได้หลายข้อในหน้าเปลี่ยนแปลงกฎ (edit rule) ซึ่งทั้งสองหน้าต้องมีการส่งข้อมูลไปยังที่เดียวกัน คือ ไฟล์ชั่วคราวของเว็บอินเตอร์เฟซ (Web temp file) ซึ่งอาจเป็นแคช (Cache) ของเว็บเบราว์เซอร์ หรือไฟล์ใดๆบนคอมพิวเตอร์เครื่องอื่น สามารถถ่ายโอนเข้ามายังอุปกรณ์ไฟร์วอลล์ได้โดยตรง แต่คอมมานด์ไลน์อินเตอร์เฟซไม่เป็นเช่นนั้น เพราะคอมมานด์ไลน์อินเตอร์เฟซสามารถใช้อีดิเตอร์ (editor) ในการแก้ไขไฟล์คอมพิลได้โดยตรง แต่เมื่อจะทำการบันทึกข้อมูลการเปลี่ยนแปลงที่เกิดขึ้น ต้องมีการสร้างเมมโมรีไฟล์หรือไฟล์ชั่วคราวของคอมมานด์ไลน์อินเตอร์เฟซ (Command line temp file) จากนั้นจึงทำการเม้าท์ไฟล์นั้นลงไปบนคอมแพคแฟลช ซึ่งการทำงานเหล่านี้เราต้องให้แน่ใจว่าจะเกิดข้อผิดพลาดน้อยที่สุด และทั้งสองอินเตอร์เฟซเมื่อมีการดึงค่าไปแก้ไขอีกครั้งจะต้องมองเห็นค่าที่อินเตอร์เฟซอื่นๆได้เพิ่มลงไปแล้ว

3. ปัญหาที่พบในส่วนคอมมานด์ไลน์

3.1 การกำหนดค่าบางค่าในคอมมานด์ไลน์อินเตอร์เฟซไม่สามารถนำมาแสดงบนเว็บอินเตอร์เฟซได้ ต้องทำการแปลงค่าที่ได้อีกครั้งหนึ่งก่อน เพื่อกำหนดให้เว็บอินเตอร์เฟซตีความและแสดงผลได้

3.2 ความผิดพลาดในการออกแบบระบบของเซลล์สคริปต์ไฟล์ ทำให้ระบบนั้นทำงานได้ไม่ดีนัก จึงต้องมีการออกแบบและเปลี่ยนแปลงใหม่อยู่หลายครั้งจนผลที่ได้เป็นที่น่าพอใจ

3.3 ความไม่เข้าใจในส่วนของการทำการสร้าง Wizard ให้กับระบบในการสร้างกฎใหม่ เป็นผลทำให้เกิดความไม่ยืดหยุ่นในการทำงานมากเท่าที่ควร

3.4 มีปัญหาในการเก็บค่าลงไฟล์ที่ค่านั้นทำการเช็คค่าได้ยาก เช่น ไอพีแอดเดรส ซึ่งจากที่ศึกษาการเขียนซี-เซลล์สคริปต์มาก็พบว่าไม่มีฟังก์ชันที่ช่วยเช็คได้ จึงต้องทำการกำหนดเงื่อนไขในการเช็คค่าด้วยตนเอง แต่พอทำจริงแล้วก็เกิดผิดพลาด อยู่หลายจุด จุดนี้จึงยังไม่ได้ทำการพัฒนาต่อ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับใช้เพื่อการศึกษาค้นคว้าเท่านั้น ไม่อนุญาตให้นำไปเผยแพร่โดยไม่ผ่านการอนุญาต
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.5 มีความสับสนของการเก็บไฟล์ในตอนเริ่มระบบขึ้นมาใหม่ ว่าในตอนนั้นเราจะดึงไฟล์ตัวไหนมารันเป็นกฎพื้นฐานให้กับระบบ ซึ่งปัญหาก็แก้ไขได้เรียบร้อยแล้ว

3.6 เนื่องจากไม่เคยเขียนโค้ดที่เป็นเชลล์สคริปต์มาก่อน จึงเกิดปัญหาเล็กๆน้อยๆในการทำงานอยู่เสมอถึงแม้ว่าจะค้นคว้าหาข้อมูลมาช่วยแล้วก็ตาม ในส่วนนี้ก็คืออยุ่มีการพัฒนาตนเองเรียนรู้เพิ่มเติมขึ้นไปเรื่อยๆ

3.7 ในบางส่วนที่มีการสร้างกฎใหม่ขึ้นมาขึ้น ถ้าผู้ใช้ไม่เข้าใจรูปแบบของกฎที่ดีก็อาจจะเป็นผลทำให้ใช้งานระบบได้อย่างไม่มีประสิทธิภาพมากนัก ในที่นี้จึงมีการแสดงข้อความแจ้งเตือนและบอกวิธีการที่ถูกต้องในการใช้งานอยู่หลายจุด

3.8 ในการเริ่มระบบขึ้นมา ไม่สามารถที่จะทำให้ระบบนั้นไปดึงสคริปต์ที่ชื่อ main.csh มารันได้เนื่องจากยังไม่ทราบว่าต้องนำสคริปต์นี้ไปไว้ที่ใดเรคทอรีใดและใช้คำสั่งใดในการเรียกใช้ขึ้นมาในตอนเริ่มระบบ

4. ความยุ่งยากในการออกแบบเว็บอินเตอร์เฟส

- 4.1 การออกแบบให้ง่าย ในการเรียกหน้าเว็บที่เชื่อมต่อระหว่างกัน
- 4.2 ผิดพลาดในการอ่านเขียนลงไฟล์
- 4.3 การคิดฟังก์ชันในการตัดคำ ซึ่งมีความยุ่งยาก
- 4.4 ความยุ่งยากในการดึงค่าอินเตอร์เฟสมาแสดง

5.3 สรุปแนวทางในการพัฒนาในอนาคต

นำไฟร์วอลล์ไปใช้ในระบบเน็ตเวิร์กภายนอกในสภาพแวดล้อมจริง เพื่อหาข้อผิดพลาดของระบบที่อาจเกิดขึ้นได้

เพิ่มประสิทธิภาพของระบบโดยเพิ่มซอฟต์แวร์ ดีเอ็นเอส ดีเฮกซ์พี เซิร์ฟเวอร์ หรือเพิ่มยูทิลิตี้อื่นๆให้ระบบทำงานได้ครอบคลุมยิ่งขึ้น

การเข้าสู่ระบบผ่านหน้าเว็บยูสเซอร์อินเตอร์เฟสนั้นยังไม่มีการเข้ารหัสของชื่อผู้ใช้และรหัสผ่าน การนำไปพัฒนาต่อไปควรได้ทำการแก้ไขปรับปรุงในส่วนนี้เพื่อความปลอดภัยจากการดักจับข้อมูลของผู้ไม่หวังดี

แก้ไขคอมมานด์ไลน์อินเตอร์เฟสให้ครอบคลุมความต้องการของผู้ใช้มากยิ่งขึ้นตามที่ต้องการพัฒนาเพิ่มเติม

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บรรณานุกรม

บัณฑิต จามรภูติ.2549. **คู่มือระบบยูนิกซ์ FreeBSD เล่ม 1.** กรุงเทพฯ: บริษัท ซีเอ็ดดูเคชั่น จำกัด
สมศักดิ์ โชตชัยชุตติกุล.2547. **อินไซต์ PHP 5.** กรุงเทพฯ: บริษัท โปรวิชั่น จำกัด



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ภาคผนวก ก

การทำระบบ MiniBSD

ระบบไฟร์วอลล์แบบฝังตัวเดมอนการ์ด(DaemonGuard)ที่ได้ทำในโครงการพัฒนาระบบในครั้งนี้จำเป็นต้องเตรียมให้โปรแกรมระบบปฏิบัติการฟรีบีเอสดี(FreeBSD) ระบบคอมมานด์ไลน์อินเตอร์เฟซ(Command line interface)และเว็บอินเตอร์เฟซ(Web interface) ทั้งหมดนั้นบันทึกสู่หน่วยความจำประเภทคอมแพคแฟลช(Compact Flash) เพื่อสามารถนำมาบูตระบบได้บนอุปกรณ์บอร์ดเดี่ยว(Single Board)ของโซคริสเน็ต5501(Soekris net5501) ซึ่งต้องทำตามแบบมินิบีเอสดี(MiniBSD) ตามขั้นตอนดังต่อไปนี้

ก่อนการทำตามขั้นตอนต่อไปนี้อาจต้องติดตั้งระบบปฏิบัติการฟรีบีเอสดี(FreeBSD)6.2 ตามปกติให้เรียบร้อยเสีย ก่อนจึงจะทำตามขั้นตอนต่อไปนี้ได้

1. ติดตั้ง ฟรีบีเอสดีเจลล์ (FreeBSD jail)

- ให้ผู้ใช้เข้าใช้ระบบเป็นผู้ใช้ที่ชื่อว่า รุท (root) เข้าสู่เครื่องที่ได้ทำการติดตั้งฟรีบีเอสดีไว้แล้ว(FreeBSD Host Machine) และ เรียกเมนูระบบขึ้นมา (Sysinstall) โดยการพิมพ์

```
#sysinstall
```

- จากเมนู ของระบบเลือก

- Custom

- Options

เมื่อพบหน้าจอใดๆที่ประกอบด้วยข้อความมากมายให้เลื่อนลูกศรมาที่ Install Root เพื่อเป็นการเปลี่ยนตำแหน่งผู้ใช้รุท(root) ที่ต้องการติดตั้งใหม่เป็น

```
/usr/jail
```

- หลังจากเลือกได้แล้วให้เคาะปุ่มเอ็นเทอร์(Enter) และคิว(Q) เพื่อออกจากหน้าจอนี้

- ข้ามตัวเลือก Over Partition และ Label และให้ไปเลือก Distributions

- ที่หน้าจอ Distributions ให้เลื่อนลูกศรมาที่ Minimal Options และเลือก Minimal distribution package โดยการเคาะแป้นว่าง(space bar) และเลือก custom option เลือก src ให้เลือกเพิ่มคือ

- lib

- sys

- ออกไปสู่เมนูหลักแล้วเลือก สื่อที่เป็นแหล่งของไฟล์คือ CD/DVD แล้วตกลง(Commit)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2. ปรับแต่ง ฟรีบีเอสดีเจลล์(FreeBSD jail)

เมื่อได้ทำการติดตั้งฟรีบีเอสดี(FreeBSD) อีกครั้งไว้ในเจลล์(jail) เป็นที่เรียบร้อยแล้วให้เริ่มทำการปรับแต่ง โดยการเข้าไปแก้ไข การปรับแต่งนี้ได้ใช้สคริปต์(script) ของultradesicสามารถดาวน์โหลด(download) ได้จากเว็บไซต์ <http://www.ultradesic.com> โดยสั่งดังนี้

```
cd /root
```

```
ee minichroot.sh
```

แล้วทำการเขียนสคริปต์(script) ดังต่อไปนี้

```
#!/bin/sh
```

```
#
```

```
# /root/minichroot.sh
```

```
#
```

```
touch /root_check ;
```

```
cp -f /etc/resolv.conf /usr/jail/etc/resolv.conf ;
```

```
if [ ! -f /usr/jail/boot/kernel/kernel ] ; then
```

```
    cp /boot/kernel/kernel /usr/jail/boot/kernel/kernel ;
```

```
fi ;
```

```
if [ ! -f /usr/jail/etc/localtime ] ; then
```

```
    cp /etc/localtime /usr/jail/etc/localtime ;
```

```
fi ;
```

```
if ( [ ! -f /usr/jail/etc/wall_cmos_clock ] && [ -f /etc/wall_cmos_clock ] ) ; then
```

```
    cp /etc/wall_cmos_clock /usr/jail/etc/wall_cmos_clock ;
```

```
fi ;
```

```
if [ ! -c /usr/jail/dev/null ] ; then
```

```
    mount -t devfs devfs /usr/jail/dev ;
```

```
if [ ! -c /usr/jail/dev/null ] ; then
```

```
    echo ;
```

```
    echo "Unable to mount dev file system!" ;
```

```
    echo ;
```

```
    echo "Exiting..." ;
```

```
    echo ;
```

```
    exit ;
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
fi ;
fi ;
chroot /usr/jail /bin/csh ;
rm /root_check ;
# End of /root/minichroot.sh
```

บันทึกไฟล์แล้วเปลี่ยนสิทธิ์ของไฟล์

```
chmod 700 minichroot.sh
```

ก่อนเริ่มการปรับแต่งให้เริ่มคัดลอก(copy) เอกสาร /etc/resolv.conf และ /etc/localtime จากเครื่องหลัก(host machine) ไปยัง /usr/jail/etc โดยการพิมพ์

```
cp /etc/resolv.conf /usr/jail/etc
```

```
cp /etc/localtime /usr/jail/etc
```

ถ้าเครื่องคอมพิวเตอร์ของเราเวลาอยู่ในแบบยูทีซี(UTC) เราสามารถที่จะยกเว้นการกระทำต่อไปได้ แต่ถ้าเครื่องคอมพิวเตอร์ของเราเวลาอยู่ในแบบเวลาพื้นที่(local time) ต้องแน่ใจว่าได้คัดลอก(copy)เอกสาร /etc/wall_cmos_clock โดยการพิมพ์

```
cp /etc/wall_cmos_clock /usr/jail/etc
```

ต่อไปคือเข้าไปแก้ไข /usr/jail/root/.cshrc ไฟล์และเพิ่มคำสั่งต่อไปนี้ในบรรทัดสุดท้าย

```
set prompt = "MiniBSD %~ %# "
```

ที่จะทำหน้าที่กำหนด(set) เครื่องหมายพร้อมต์(prompt) เมื่อเปลี่ยนผู้ใช้รุต(root) เข้าสู่ฟรีบีเอสดีเจลล์(FreeBSD jail) และเมื่อเสร็จเรียบร้อยแล้วให้เข้าสู่เจลล์(jail) โดยการใส่สคริปต์ (script)

```
/root/minichroot.sh
```

ถ้าคุณไม่ใช่ สคริปต์(script) พิมพ์คำสั่งต่อไปนี้ เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับใช้ในงานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
touch /root_check
mount -t devfs devfs /usr/jail/dev
chroot /usr/jail /bin/csh
```

3. Safety Checks

ต่อไปเป็นการเริ่มต้นทำระบบมินิบีเอสดี(miniBSD) แต่ก่อนจะเริ่มทำต้องแน่ใจก่อนว่าได้อยู่ใน ฟรียูเอสบีเอสดีเจลล์(FreeBSD jail) เสียก่อนและ dev ได้ mount เรียบร้อยแล้วใน ฟรียูเอสบีเอสดีเจลล์(FreeBSD jail) ให้คุณพิมพ์

```
ls /root_check
```

ถ้าคุณอยู่ใน ฟรียูเอสบีเอสดีเจลล์(FreeBSD jail) คุณจะต้องไม่เห็นไฟล์นี้ถ้าคุณเห็นไฟล์นี้แสดงว่ามีบางอย่างผิดพลาดให้หยุดแล้วเริ่มทำใหม่

เมื่อคุณอยู่ใน ฟรียูเอสบีเอสดีเจลล์(FreeBSD jail) เรียบร้อยแล้ว ให้ตรวจสอบเพื่อความแน่ใจว่า device nodes มีอยู่แล้ว โดยพิมพ์ดังนี้

```
ls /dev
```

ถ้าคุณไม่เห็นไฟล์แสดงว่ามีบางอย่างผิดพลาดให้หยุดแล้วเริ่มต้นใหม่

4. Building miniBSD 6.x

ส่วนต่อไปนี้เป็นสร้าง มินิบีเอสดี(miniBSD) ในการทำงานครั้งนี้ได้ทำกับ ฟรียูเอสบีเอสดี(FreeBSD) 6.2 ถ้าคุณรู้สึกว่าการทำงานบางอย่างไม่ค่อยเป็นตามที่คาดคุณสามารถออกจาก ฟรียูเอสบีเอสดีเจลล์(FreeBSD jail) ได้โดยการ unmount /usr/jail/dev และ ลบไคลเรคทอรี /usr/jail ได้

5. Create Directory Structure

สิ่งแรกที่คุณควรทำคือการสร้าง โครงสร้างของ ไคลเรคทอรี ของระบบ มินิบีเอสดี (miniBSD) คุณสามารถใช้คำสั่ง mkdir สร้างเองหรือใช้ สคริปต์(script) โดยทำดังนี้

```
cd /root
ee create-minibsd-dirs.sh
```

```
#!/bin/sh
```

```
#
```

```
#
```

```
MINIBSD_DIR=/usr/minibsd ;
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```

if [ -d $MINIBSD_DIR ] ; then
    echo ;
    echo "$MINIBSD_DIR already exists. Remove the directory" ;
    echo "before running this script." ;
    echo ;
    echo "Exiting..." ;
    echo ;
    exit ;
fi ;

```

```

mkdir $MINIBSD_DIR ;
cd $MINIBSD_DIR ;
mkdir bin ;
mkdir boot ;
mkdir boot/defaults ;
mkdir dev ;
mkdir etc ;
mkdir etc/defaults ;
mkdir etc/mtree ;
mkdir lib ;
mkdir libexec ;
mkdir mnt ;
mkdir -m 0555 proc ;
mkdir -m 0700 root ;
mkdir sbin ;
mkdir usr ;
mkdir usr/bin ;
mkdir usr/lib ;
mkdir usr/lib/aout ;
mkdir usr/libexec ;

```

```

mkdir usr/local ;

```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
mkdir usr/sbin ;
mkdir usr/share ;
mkdir usr/share/misc ;
mkdir var ;
mkdir var/tmp ;
ln -s /var/tmp tmp
```

บันทึกไฟล์และเปลี่ยนสิทธิ์ของไฟล์

```
chmod 0700 /root/create-minibsd-dirs.sh
```

```
/root/create-minibsd-dirs.sh
```

ถ้าคุณต้องการสร้างเองสามารถใช้โครงสร้างดังนี้

- usr/minibsd
 - bin
 - boot
 - defaults
 - dev
 - etc
 - defaults
 - mtree
 - lib
 - libexec
 - mnt
 - proc
 - root
 - sbin
 - usr
 - bin
 - lib
 - aout
 - libexec
 - local

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- sbin
- share
- misc
- var

คุณต้องแน่ใจว่าได้ ตั้งค่า permissions ของ ไดรคทอรี proc เป็น 555 และ permission ของ root ไดรคทอรีเป็น 700 แล้วสร้าง symlink จาก /var/tmp ไป /tmp

6. Rebuilding the boot loader

ไบออสของเครื่อง Soekris มี bug อยู่ที่ serial console emulation ถ้าคุณใช้ FreeBSD boot loader แบบมาตรฐานอาจจะมีตัวอักษรแปลกๆออกมา เช่น (- \ | / - ...) แก้ไขได้โดยแก้ที่ไฟล์ต่อไปนี้

Edit /sys/boot/i386/libi386/Makefile and comment out the line that reads:

```
CFLAGS+= -DTERM_EMU
```

บันทึกงไฟล์

พิมพ์คำสั่งต่อไปนี้

```
mkdir -p /usr/share/man/man{1,2,3,4,5,6,7,8}
```

ขณะนี้คุณต้อง compile และ install bootloader โดยพิมพ์

```
cd /sys/boot
```

```
make clean
```

```
make
```

```
make install
```

7. Building Dynamic Executables

ขั้นตอนต่อไปนี้อาจจะยกเว้นได้แต่ถ้าต้องการประหยัดเนื้อที่ของ มินิบีเอสดี(miniBSD) ให้ทำดังนี้ แก้ไขที่ไฟล์ /etc/make.conf โดยการเพิ่มบรรทัดนี้ลงไป

```
NO_SHARED=no
```

ตารางต่อไปนี้เป็นเนื้อที่ของแต่ละพาร์ทิชัน(partition)ที่คุณสามารถประหยัดได้ถ้าทุกๆ ไบต์มีคุณค่าสำหรับคุณ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Default Size	Size after compiling with NO_SHARED=no
/bin = 802K	/bin = 802K
/sbin = 1.2M	/sbin = 766K
/usr/bin = 3.3M	/usr/bin = 3.3M
/usr/sbin = 1.0M	/usr/sbin = 1.0M

ก่อนที่คุณจะ rebuild ไฟล์ binary คุณต้องรัน sysinstall จาก ฟรีบีเอสดีเจดัลล์(FreeBSD jail) ของคุณดังนี้

/usr/sbin/sysinstall

เลือกจากเมนู

- Configure
 - Distributions

คุณต้องเลือก src option แล้วเลือกต่อไปนี่

- contrib
- libexec
- release
- bin
- sbin
- ubin
- usbin

ออกมาจาก sysinstall เลือก Media source แล้ว commit รอดติดตั้งแล้ว ให้ทำการต่อไปนี่

เอง

```
cd /usr/src/lib/libsm
```

```
make clean
```

```
make
```

คอมไพล์และติดตั้ง bin

```
cd /usr/src/bin
```

```
make clean
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
make
make install
```

ต่อไปพิมพ์

```
cd /usr/src/contrib/ipfilter/tools
make clean
make
cd /usr/src/sbin/ipf
make clean
make
```

ต่อไป compile และติดตั้ง sbin ต้องแน่ใจว่า /usr/share/docatm ไดรเวอร์มีอยู่ไม่เช่นนั้น
จะเกิดข้อผิดพลาดแต่ถ้ายังไม่มีให้พิมพ์บรรทัดบนก่อนเพื่อสร้าง

```
mkdir -p /usr/share/doc/atm
cd /usr/src/sbin
make clean
make
make install
```

ต่อไป compile และติดตั้ง usr.bin ก่อนอื่น usr.bin ต้องการ libraries ก่อนต้องสร้างให้

ดังนี้

```
cd /usr/src/lib/bind
make clean
make

cd /usr/src/lib/libtelnet
make clean
make

cd /usr/src/lib/libsmutil
make clean
make
```

```
cd /usr/src/lib/libsmdb
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```

make clean

make
ติดตั้ง usr.bin

cd /usr/src/usr.bin

make clean

make

mkdir -p /usr/share/info

make install

```

7. Copy the binaries over

ขณะนี้คุณต้องดาวน์โหลด(download) mkmini.sh และ minibsd6.files ที่จะทำให้สามารถคัดลอก(copy) binary มาสู่มินิเบสดี(miniBSD) ได้

```

cd /root
ee minibsd6.files

# minibsd.files
# by Manuel Kasper <mk@neon1.net>
# List of files required for a very minimal FreeBSD system,
# intended to be parsed by mkmini.pl
#
# Modified by David Courtney <minibsd@ultradesic.com>
# - sbin/rcorder is required for FreeBSD 5.x
# - bin/kenv is required for FreeBSD 6.x
# - Removed ssh files out of the default minibsd6.files
# - Removed named files out of the default minibsd6.files
# - Removed ppp files out of the default minibsd6.files
# - Removed usr/sbin/ndc
# - Removed usr/sbin/ipsend
# - Added usr/bin/cut
# - Added sbin/mount_mfs
# - Added sbin/nextboot
# - Removed the usr/sbin/tset hard link to usr/bin/reset

```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
# Lines with colons (':') in them list files that should be hard-linked
# to each other, e.g.
# bin/link:bin/ln
# instructs mkmini.pl to copy over bin/link, then hard link ln to it.
```

```
# contents of /boot
```

```
boot/boot0
```

```
boot/boot1
```

```
boot/boot2
```

```
boot/defaults/loader.conf
```

```
boot/device.hints
```

```
boot/loader
```

```
boot/loader.4th
```

```
boot/loader.help
```

```
boot/loader.rc
```

```
boot/mbr
```

```
boot/support.4th
```

```
# contents of /libexec
```

```
libexec/ld-elf.so.1:usr/libexec/ld-elf.so.1
```

```
# contents of /bin
```

```
bin[:bin/test
```

```
bin/cat
```

```
bin/chflags
```

```
bin/chio
```

```
bin/chmod
```

```
bin/cp
```

```
bin/csh:bin/tcsh
```

```
bin/date
```

```
bin/dd
```

```
bin/df
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

`bin/domainname``bin/echo``bin/ed:bin/red``bin/expr``bin/hostname``bin/kenv``bin/kill``bin/link:bin/ln``bin/lis``bin/mkdir``bin/mv``bin/pax``bin/ps``bin/pwd``bin/realpath``bin/rm:bin/unlink``bin/rmdir``bin/sh``bin/sleep``bin/stty``bin/sync``# contents of /sbin``sbin/adjkerntz``sbin/comcontrol``sbin/dhclient``sbin/dhclient-script``sbin/disklabel``sbin/dmesg``sbin/fastboot:sbin/fasthalt:sbin/halt:sbin/reboot``sbin/fsck``sbin/fsck_ufs:sbin/fsck_ffs:sbin/fsck_4.2bsd`

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

sbin/ifconfig
 sbin/init
 sbin/ipfw
 sbin/kldconfig
 sbin/kldload
 sbin/kldstat
 sbin/kldunload
 sbin/ldconfig
 sbin/md5
 sbin/mdconfig
 sbin/mknod
 sbin/mdmfs
 sbin/mount
 sbin/mount_devfs:sbin/mount_fdscfs:sbin/mount_linprocfs:sbin/mount_procfs:sbin/mount_std
 sbin/mount_mfs
 sbin/mount_nullfs
 sbin/mount_umapfs
 sbin/mount_unionfs
 sbin/natd
 sbin/newfs
 sbin/nextboot
 sbin/nologin
 sbin/nos-tun
 sbin/rcorder
 sbin/ping
 sbin/route
 sbin/setkey
 sbin/shutdown
 sbin/slattach
 sbin/swapon
 sbin/sysctl
 sbin/umount

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
 ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```

# contents of /usr/sbin
usr/bin/at:usr/bin/atq:usr/bin/atrm:usr/bin/batch
usr/bin/awk
usr/bin/basename
usr/bin/bunzip2:usr/bin/bzcat:usr/bin/bzip2
usr/bin/chat
usr/bin/chfn:usr/bin/chpass:usr/bin/chsh
usr/bin/chgrp
usr/bin/cksum
usr/bin/clear
usr/bin/cmp
usr/bin/compress:usr/bin/uncompress
usr/bin/cpio
usr/bin/crontab
usr/bin/cu
usr/bin/cut
usr/bin/dig
usr/bin/dirname
usr/bin/du
usr/bin/ee
usr/bin/egrep:usr/bin/fgrep:usr/bin/grep
usr/bin/env
usr/bin/false
usr/bin/fetch
usr/bin/find
usr/bin/finger
usr/bin/fstat
usr/bin/fsync
usr/bin/ftp
usr/bin/gunzip:usr/bin/gzcat:usr/bin/gzip
usr/bin/gzexe

```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```

usr/bin/head
usr/bin/hexdump
usr/bin/id:usr/bin/whoami
usr/bin/ident
usr/bin/killall
usr/bin/last
usr/bin/less:usr/bin/more
usr/bin/limits
usr/bin/lock
usr/bin/lockf
usr/bin/logger
usr/bin/login
usr/bin/logname
usr/bin/mesg
usr/bin/minigzip
usr/bin/mkfifo
usr/bin/mktemp
usr/bin/msgs
usr/bin/netstat
usr/bin/nice
usr/bin/nohup
usr/bin/objformat
usr/bin/openssl
usr/bin/passwd
usr/bin/printf
usr/bin/renice
usr/bin/reset
usr/bin/script
usr/bin/sed
usr/bin/shar
usr/bin/sort
usr/bin/split

```



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```

usr/bin/su
usr/bin/tail
usr/bin/tar
usr/bin/tee
usr/bin/telnet
usr/bin/tftp
usr/bin/time
usr/bin/top
usr/bin/touch
usr/bin/tput
usr/bin/tr
usr/bin/true
usr/bin/tty
usr/bin/uname
usr/bin/uptime:usr/bin/w
usr/bin/users
usr/bin/uudecode
usr/bin/uuencode
usr/bin/vi
usr/bin/vmstat
usr/bin/wall
usr/bin/who
usr/bin/whois
usr/bin/write
usr/bin/yes

```

contents of usr/sbin

```

usr/sbin/arp
usr/sbin/boot0cfg
usr/sbin/chown
usr/sbin/chroot

```

usr/sbin/cron

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

usr/sbin/idprio:usr/sbin/rtprio

usr/sbin/inetd

usr/sbin/iostat

usr/sbin/kbdcontrol

usr/sbin/lastlogin

usr/sbin/memcontrol

usr/sbin/mtree

usr/sbin/newsyslog

usr/sbin/ngctl

usr/sbin/nghook

usr/sbin/ntpdate

usr/sbin/pciconf

usr/sbin/pw

usr/sbin/pwd_mkdb

usr/sbin/slstat

usr/sbin/syslogd

usr/sbin/tcpdchk

usr/sbin/tcpdmatch

usr/sbin/tcpdump

usr/sbin/traceroute

usr/sbin/vidcontrol

usr/sbin/vipw

usr/sbin/vnconfig

usr/sbin/watch

contents of /usr/libexec

usr/libexec/atrun

usr/libexec/ftpd

usr/libexec/getty

usr/libexec/telnetd

usr/libexec/tftpd

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
# contents of /usr/share
usr/share/misc/termcap
```

จากนั้นทำการบันทึกไฟล์

```
ee mkmini.sh
```

```
#!/bin/sh
```

```
#
```

```
if [ ! $1 ]; then
```

```
    echo ;
```

```
    echo "Syntax : mkmini.sh <input file>";
```

```
    echo "Example: mkmini.sh /root/minibsd6.files" ;
```

```
    echo ;
```

```
    exit ;
```

```
fi ;
```

```
MINIBSDFILES="$1" ;
```

```
MINIBSDDIR="/usr/minibsd" ;
```

```
sed -nE -e 's/^(^#|) *A1/p' < $MINIBSDFILES | tr ':' '\n' | tar -C / -cvf - -T - | tar -C
$MINIBSDDIR -x -f -
```

แล้วทำการบันทึกไฟล์

ถ้าคุณใช้ ฟรีบีเอสดี(FreeBSD) เวอร์ชันที่ต่ำกว่า 6.1 คุณอาจจะต้องแก้ไข minibsd6.files และเปลี่ยน location ของ /sbin/setkey ไปเป็น /usr/sbin/setkey

แนะนำให้บันทึกไฟล์ใน root ไดรคทอรีของ ฟรีบีเอสดีเจลล์(FreeBSD jail) ก่อน

```
cd /root
```

```
chmod 0700 /root/mkmini.sh
```

```
/root/mkmini.sh /root/minibsd6.files
```

ถ้าคุณติดตั้ง source package ใน ฟรีบีเอสดีเจลล์(FreeBSD jail) คุณสามารถ คัดลอก (copy) termcap และ services ไฟล์โดยการทำดังนี้

```
cp /usr/src/release/picobsd/mfs tree/etc/termcap /usr/minibsd/usr/share/misc
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการศึกษาเท่านั้น เมื่อนำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
cp /usr/src/release/picobsd/mfs_tree/etc/services /usr/minibsd/usr/share/misc
```

8. Configuration boot files

เมื่อคุณบูตระบบมินิบีเอสดี(miniBSD) อาจจะไม่สามารถหา /boot/beasties.4th เพราะเราไม่ได้ คัดลอก(copy) เอามาถ้าคุณต้องการ beasties menu แสดงตอน boot คุณต้อง คัดลอก(copy) มาตามนี้

```
cp /boot/beastie.4th /usr/minibsd/boot
```

```
cp /boot/screen.4th /usr/minibsd/boot
```

```
cp /boot/frames.4th /usr/minibsd/boot
```

แต่ถ้าคุณไม่สนใจหรือต้องการ beasties menu นั้นคุณสามารถ comment หรือลบได้ที่ /usr/minibsd/boot/loader.rc

ดังนี้ โดยการเพิ่มเครื่องหมาย \ ลงไปหน้าข้อความ

```
\ Load in the boot menu
```

```
\ include /boot/beastie.4th
```

```
\ Start the boot menu
```

```
\ beastie-start
```

ถ้าคุณต้องการให้ระบบไม่มีการ delay หรือ delay น้อยคุณต้องแก้ไขดังนี้ที่ไฟล์ /usr/minibsd/boot/loader.rc และพิมพ์ autoboot 0

9. Kernel Compile

ถ้าคุณวางแผนที่จะใช้ GENERIC kernel ให้พิมพ์ดังนี้

```
mkdir -p /usr/minibsd/boot/kernel
```

```
cp /boot/kernel/kernel /usr/minibsd/boot/kernel
```

```
cd /usr/minibsd/boot/kernel
```

```
gzip -9 kernel
```

แต่ถ้าคุณต้องการที่จะ compile kernel เองให้เริ่มทำตามนี้

```
cd /usr/src/sys/i386/conf
```

```
cp GENERIC MINIBSD
```

ถ้าคุณใช้ soekris รุ่น net4801/net4826 คุณต้องการที่จะใช้ kernel config ของ ultradesic ให้ทำการดาวน์โหลด(download) ตามนี้

```
cd /usr/src/sys/i386/conf
```

```
fetch http://www.ultradesic.com/pub/miniBSD_Files/MINIBSD
```

เข้าไปแก้ไข ไฟล์มินิบีเอสดี(miniBSD) แล้วบันทึก

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

หลังจากนั้นทำตามนี้

```
/usr/sbin/config MINIBSD
cd ../compile/MINIBSD
make clean && make cleandepend && make depend && make
gzip -9 kernel
mkdir -p /usr/minibsd/boot/kernel
cp kernel.gz /usr/minibsd/boot/kernel
```

คำแนะนำ สำหรับผู้ที่ต้องการทำ kernel เองต้องระบุได้ว่าระบบของเราจะรองรับอุปกรณ์ใดบ้าง เพื่อจะได้จัดสรรไดรเวอร์ที่ใช้ในระบบได้ถูกต้อง

10. Copying the libraries

เรายังไม่ได้คัดลอก libraries มาสู่ /usr/lib ซึ่งไม่มีรายการอยู่ใน minibsd6.files เพราะรายการของ libraries ที่ต้องการต้องอาศัยการติดตั้ง ให้ดาวน์โหลด(download) ไฟล์ mklibs.sh ดังนี้

```
cd /root
ee mklibs.sh
#!/bin/sh
#
MINIBSDDIR="/usr/minibsd" ;
find -X $MINIBSDDIR !-name "*.ko" -and -type f -and -perm +111 | xargs ldd -f "%p\n" 2>
/dev/null | sort | uniq | sed 's/^/|'
```

ทำการบันทึกไฟล์

```
chmod 0700 /root/mklibs.sh
/root/mklibs.sh > /root/minibsd.libs
```

หลังดูที่ output ของ minibsd.libs แล้วถูกต้องให้รันสคริปต์ดังนี้

```
/root/mkmini.sh minibsd.libs
```

Library ที่ยังขาดอยู่คือ PAM ให้ คัดลอก(copy) ดังนี้

```
cp -p /usr/lib/pam* /usr/minibsd/usr/lib
```

```
cp -p /usr/lib/*opic* /usr/minibsd/usr/lib
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

11. Populating /etc

ถึงตอนนี้คุณต้องการที่จะปรับแต่ง มินิบีเอสดี(miniBSD) ของคุณเช่นการตั้งค่ารหัสผ่าน เพิ่ม user เป็นต้น คุณอาจจะ คัดลอก(copy) จาก /etc ของเดิมมาได้ภายใต้ ฟรีบีเอสดีเจลล์(FreeBSD jail) แต่เมื่อตอนติดตั้งครั้งแรกเรายังไม่ได้ตั้งรหัสผ่านที่ ฟรีบีเอสดีเจลล์(FreeBSD jail) ให้ตั้งรหัสผ่านและเพิ่ม user ก่อน เมื่อคุณได้ตั้งรหัสผ่าน เพิ่ม user เรียบร้อยแล้วและปรับแต่งที่ ฟรีบีเอสดีเจลล์(FreeBSD jail) แล้วจึงเริ่ม คัดลอก(copy) มายัง มินิบีเอสดี(miniBSD) แต่ถ้าคุณมีการเพิ่ม service คุณจะต้อง คัดลอก(copy) มาด้วยแล้ว ใช้ สคริปต์(script) นี้ในการคัดลอก(copy) ไดรคทอรี /etc

```

cd /root
ee copy-etc-6.sh

#!/bin/sh
#
DEST=/usr/minibsd/etc ;

cp /etc/auth.conf $DEST
cp /etc/crontab $DEST
cp /etc/defaults/devfs.rules $DEST/defaults
cp /etc/defaults/periodic.conf $DEST/defaults
cp /etc/defaults/rc.conf $DEST/defaults
#cp /etc/disktab $DEST
if [ ! -f /etc/fstab ] ; then
    touch /etc/fstab ;
fi ;
cp /etc/fstab $DEST
#cp /etc/ftpusers $DEST
cp /etc/gettytab $DEST
cp /etc/group $DEST
if [ ! -f /etc/host.conf ] ; then
    cd $DEST ;

```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```

ln -s /tmp/host.conf ;

else

    cp /etc/host.conf $DEST ;

fi ;

cp /etc/hosts $DEST
cp /etc/hosts.allow $DEST
#cp /etc/hosts.equiv $DEST
#cp /etc/hosts.lpd $DEST
cp /etc/inetd.conf $DEST
cp /etc/localtime $DEST
cp /etc/login.access $DEST
cp /etc/login.conf $DEST
cp /etc/master.passwd $DEST
cp /etc/mtree/BSD.include.dist $DEST/mtree
cp /etc/mtree/BSD.local.dist $DEST/mtree
cp /etc/mtree/BSD.root.dist $DEST/mtree
cp /etc/mtree/BSD.sendmail.dist $DEST/mtree
cp /etc/mtree/BSD.usr.dist $DEST/mtree
cp /etc/mtree/BSD.var.dist $DEST/mtree
cp /etc/mtree/BSD.x11-4.dist $DEST/mtree
cp /etc/mtree/BSD.x11.dist $DEST/mtree
#cp /etc/namedb/PROTO.localhost.rev $DEST/namedb
#cp /etc/namedb/make-localhost $DEST/namedb
#cp /etc/namedb/named.conf $DEST/namedb
#cp /etc/namedb/named.root $DEST/namedb
cp /etc/network.subr $DEST
cp /etc/networks $DEST
cp /etc/newsyslog.conf $DEST
if [ ! -f /etc/nsswitch.conf ] ; then
    cd $DEST ;
    ln -s /tmp/nsswitch.conf ;

```

else

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```

cp /etc/nsswitch.conf $DEST ;

fi ;

cp -R /etc/pam.d $DEST

cp /etc/passwd $DEST

cp /etc/profile $DEST

cp /etc/protocols $DEST

cp /etc/pwd.db $DEST

cp /etc/rc $DEST

if [ -f /etc/rc.conf ] ; then

    cp /etc/rc.conf $DEST ;

fi ;

cp -R /etc/rc.d $DEST

cp /etc/rc.firewall $DEST
#cp /etc/rc.i368 $DEST
#cp /etc/rc.local $DEST
#cp /etc/rc.network $DEST
#cp /etc/rc.serial $DEST
cp /etc/rc.shutdown $DEST
cp /etc/rc.subr $DEST
cp /etc/resolv.conf $DEST
#cp /etc/security $DEST
cp /etc/services $DEST
cp /etc/shells $DEST
#cp /etc/skeykeys $DEST
cp /etc/spwd.db $DEST

#cp /etc/ssh/primers $DEST/ssh
#cp /etc/ssh/ssh_config $DEST/ssh
#cp /etc/ssh/ssh_host_dsa_key $DEST/ssh
#cp /etc/ssh/ssh_host_dsa_key.pub $DEST/ssh
#cp /etc/ssh/ssh_host_key $DEST/ssh
#cp /etc/ssh/ssh_host_key.pub $DEST/ssh

#cp /etc/ssh/sshd_config $DEST/ssh

```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
#cp /etc/ssl/openssl.cnf $DEST/ssl
cp /etc/sysctl.conf $DEST
cp /etc/syslog.conf $DEST
if [ ! -f $DEST/termcap ] ; then
    ln -s /usr/share/misc/termcap $DEST/termcap ;
fi ;
cp /etc/ttytys $DEST
if [ -f /etc/wall_cmos_clock ] ; then
    cp /etc/wall_cmos_clock $DEST ;
fi ;
```

บันทึกไฟล์

```
chmod 0700 /root/copy-etc-6.sh
/root/copy-etc-6.sh
```

ซึ่ง สคริปต์(script) จะ คัดลอก(copy) ไดรคทอรี /etc ตามนี้

- /etc/auth.conf
- /etc/crontab
- /etc/defaults/devfs.rules
- /etc/defaults/periodic.conf
- /etc/defaults/rc.conf สามารถแก้ไข rc_conf_files ให้โหลดที่อื่นได้
- /etc/fstab ^{ตั้ง}การ mount
- /etc/ftusers
- /etc/gettytab
- /etc/group
- /etc/host.conf
- /etc/hosts ^{ตั้ง}ชื่อเครื่อง
- /etc/hosts.allow
- /etc/inetd.conf
- /etc/localtime
- /etc/login.access

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- /etc/login.conf
- /etc/master.passwd
- /etc/mtree/ (copy the directory plus its contents)
- /etc/network.subr
- /etc/networks
- /etc/newsyslog.conf
- /etc/nsswitch.conf
- /etc/pam.d/ (copy the directory plus its contents)
- /etc/passwd
- /etc/profile
- /etc/protocols
- /etc/pwd.db
- /etc/rc
- **/etc/rc.conf** ตั้งค่าตอนboot
- /etc/rc.d/ (copy the directory plus its contents)
- /etc/rc.firewall
- /etc/rc.shutdown
- /etc/rc.subr
- **/etc/resolv.conf** ตั้งค่า dns
- /etc/services
- /etc/shells
- /etc/spwd.db
- /etc/sysctl.conf
- /etc/syslog.conf ตั้งค่าว่า system log เก็บไว้ที่ไหน
- /etc/termcap -> /usr/share/misc/termcap
- **/etc/tty** ตั้งค่าterminal

ในกรณีที่ต้องการติดตั้ง pf firewall ต้องเพิ่มไดเรกทอรีต่อไปนี้เอง

- /etc/rc.d/pf
- /etc/rc.d/pflog
- /etc/rc.d/pfsync

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

-
- /etc/pf.conf
- /etc/pf.os
- /etc/devd.conf ตั้งค่าไว้ให้ devd โหลด

ไฟล์ /etc/fstab ยังไม่มีอยู่ใน ฟรีบีเอสดีเจลล์(FreeBSD jail) /etc ไดรเรททอรี คุณจะต้องสร้างใหม่ได้โดยไมยากเพราะคุณต้องพิมพ์แค่สองบรรทัดคือ (อย่างน้อยคุณตั้งเอาไว้สอง พาร์ทิชัน (partition)) โดยการสร้างไฟล์ /usr/minibsd/etc/fstab ด้วย text editor ที่คุณชอบแล้วพิมพ์สองบรรทัดนี้ลงไป

```
/dev/ad0a / ufs ro 1 1
proc /proc procfs rw 0 0
```

ตัวอย่างเพิ่ม

```
/dev/ad0a / ufs ro 1 1
proc /proc procfs rw 0 0
```

แนะนำให้เป็น rw ก่อน พอลงเครื่องจึงค่อยตั้งเป็น ro

```
/dev/ad0d /conf ufs rw 2 2
```

/conf สร้างเพิ่ม แนะนำให้ใส่บรรทัดนี้ที่หลัง

ไฟล์ host.conf ถูกสร้างขึ้นโดยอัตโนมัติเมื่อ ระบบ ฟรีบีเอสดี(FreeBSD) บูตขึ้นมาถ้าไม่มีอยู่และไม่มีอยู่ใน ฟรีบีเอสดีเจลล์(FreeBSD jail) จะต้องสร้างขึ้นหรือสร้าง symlink ถ้าต้องการทำ symlink ให้พิมพ์ดังนี้

```
cd /usr/minibsd/etc
```

```
ln -s /tmp/host.conf
```

ไฟล์ nsswitch.conf ถูกสร้างขึ้นโดยอัตโนมัติเมื่อบูตระบบแต่ถ้าไม่มีทำดังนี้

```
cd /usr/minibsd/etc
```

```
ln -s /tmp/nsswitch.conf
```

ฟรีบีเอสดีเจลล์(FreeBSD jail) ของเรายังมีค่าการปรับแต่งที่ไม่ถูกต้องให้เข้าไปแก้ไขดังนี้ เช่น

```
hostname="workbox.ultradesic.build"
```

```
ifconfig_sis0="192.168.1.4 netmask 255.255.255.0"
```

```
defaultrouter="192.168.1.1"
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```

sshd_enable="NO"
usbd_enable="NO"
sendmail_enable="NONE"
inetd_enable="NO"
portmap_enable="NO"
update_motd="NO"
varsize=8192
varmfs="YES"
tmpmfs="YES"
tmpsize=8192

```

หากต้องการติดตั้ง pf firewall ให้เพิ่มค่าดังต่อไปนี้

```

pf_enable="YES"
pf_rules="/etc/pf.conf" ตั้งค่าconfig file
pflog_enable="YES"
pflog_logfile="/var/log/pflog"
gateway_enable="YES"
sshd_enable="YES"

```

ในบรรทัดที่ varmfs และ tmpmfs ใน /usr/minibsd/etc/rc.conf เราสามารถใส่ไว้ในไฟล์ /usr/minibsd/etc/fstab ได้โดยไม่ต้องใส่ใน /usr/minibsd/etc/rc.conf ดังนี้

```

md /var mfs rw,-s8m 2 0
md /tmp mfs rw,-s8m 2 0

```

ซึ่งจะทำงานเหมือนกันแต่ผู้คนมักจะ กำหนด mount point ไว้ในไฟล์ fstab ถ้าบูตระบบแล้วพบข้อความ

```
/etc/rc: WARNING: Dump device does not exist. Savecore not run.
```

ข้อความนี้จะปรากฏเมื่อขาด swap พาร์ทิชัน(partition) เพื่อที่จะกำจัดข้อความนี้ให้แก้ไขไฟล์ /usr/minibsd/etc/rc.conf ตามนี้

```
dumpdev="NO"
```

บนระบบ embedded แนะนำให้แก้ไขไฟล์ /usr/minibsd/etc/ttyd และปิด virtual console

ทั้งหมดซึ่งไม่ได้ใช้และสิ้นเปลืองหน่วยความจำ อาจจะเป็นไปได้ที่ความต้องการนี้ เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น เมื่อนำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```

# If console is marked "insecure", then init will ask for the root password
# when going to single-user mode.

console none          unknown off secure

#

ttyv0 "/usr/libexec/getty Pc"   cons25 off secure   cons25 ให้ off หมด
# Virtual terminals
ttyv1 "/usr/libexec/getty Pc"   cons25 off secure
ttyv2 "/usr/libexec/getty Pc"   cons25 off secure
ttyv3 "/usr/libexec/getty Pc"   cons25 off secure
ttyv4 "/usr/libexec/getty Pc"   cons25 off secure
ttyv5 "/usr/libexec/getty Pc"   cons25 off secure
ttyv6 "/usr/libexec/getty Pc"   cons25 off secure
ttyv7 "/usr/libexec/getty Pc"   cons25 off secure
ttyv8 "/usr/X11R6/bin/xdm -nodaemon" xterm off secure
# Serial terminals
# The 'dialup' keyword identifies dialin lines to login, fingerd etc.
ttyd0 "/usr/libexec/getty std.9600" vt100 on secure  ttyd0 ให้ on และเป็น vt100

```

12. สร้าง Binary image

ขั้นตอนสุดท้ายคือการสร้างทั้งหมดไว้ใน binary ไฟล์เพียงไฟล์เดียวเพื่อนำไป write ลงสู่ cf card หรือ Harddisk ถ้าต้องการใช้ สคริปต์(script) ให้ ดาวน์โหลด(download) แล้วทำดังนี้

```

cd /root
fetch http://www.ultradesic.com/pub/miniBSD_Files/build-image.sh
chmod 0700 /root/build-image.sh
/root/build-image.sh

```

เมื่อสั่งรัน สคริปต์(script) แล้วควร ได้ผลลัพธ์ดังนี้

```
MiniBSD ~ # ./build-image.sh 0.1.0
```

```
Generating an empty binary image file...[ OK ]
```

```
Linking binary image to device file...[ OK ]
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Creating MBR on binary image.....[OK]
 Partitioning binary image.....[OK]
 Formatting the binary image.....[OK]
 Mounting temporary mount point.....[OK]
 Writing miniBSD to the binary image.....[OK]
 Unmounting temporary mount point.....[OK]
 Unlinking binary image.....[OK]
 Compressing the binary image.....[OK]
 Checking file integrity.....[OK]
 Generating MD5 SUM of binary image.....[OK]

Done!

คำแนะนำ ให้ปฏิบัติเองจะเป็นการยืดหยุ่นกว่า เพราะระบบแต่ละระบบมีข้อปลีกย่อยแตกต่างกัน สคริปต์(script) ที่ใช้จึงควรเขียนขึ้นเอง ต้องการทำตามขั้นตอนให้ทำตามนี้

Generating the flash image

เราใช้ vnconfig เพื่อกำหนด virtual disk และเราสามารถ ใช้ bsdlable เพื่อรู้ขนาดของ flash card ในหน่วย sectors (512 byte units) ให้พิมพ์คำสั่งนี้เพื่อทราบขนาด

```
bsdlable -Awn ad[n] auto | grep sectors/unit
```

ถ้า bsdlable รายงานข้อผิดพลาดให้พิมพ์

```
dd if=/dev/zero of=/dev/ad[n] bs=1k count=20
```

นี่เป็นการลบข้อมูลทุกพาร์ติชันที่รายงานบน CF card

ต่อไปเป็นการสร้าง disk image ของขนาดเท่ากับ CF Card ดังนี้

```
dd if=/dev/zero of=/usr/minibsd-disk.bin bs=512 count=[number of sectors on your flash card]
```

อนุญาตให้ disk image files เป็นเช่นเดียวกับ vn device ดังนี้

```
mdconfig -a -t vnode -u 0 -f /usr/minibsd-disk.bin
```

virtual disk ของเราต้องเป็น พาร์ติชัน(partition)s และสร้าง file system ดังนี้

```
bsdlable -Bw md0 auto
```

```
bsdlable -e md0
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

คุณต้องใช้ text editor ที่ชอบเพื่อหาบรรทัดที่เริ่มด้วย C: และ คัดลอก(copy) มันเพื่อเปลี่ยนเป็น a: และเปลี่ยนชนิดเป็น 4.2BSD นี่คือ root partition ที่ใช้ทั้ง slice ถ้าคุณต้องการ พาร์ติชัน(partition) ที่สองเพื่อเก็บ configuration ให้ลดขนาดของ a: slice โดยการกำหนดค่าของ พาร์ติชัน(partition) ที่สองที่คุณต้องการ หลังจากนั้นให้อีกบรรทัดที่เริ่มจาก e: และลบขนาดออกจาก a: บันทึก จำไว้ว่าเราไม่สามารถสร้าง swap partition ได้บน CF Card เพราะมันช้ามากๆ

ตัวอย่าง bsdlable -e md0

```
# /dev/md0:
```

8 partitions:

#	size	offset	fstype	[fsize	bsize	bps/cpg]
a:	409600	0	4.2BSD	0	0	0
c:	509952	0	unused	0	0	# "raw" part, don't edit
d:	100352	409600	4.2BSD	0	0	0

ตัวอย่าง เพิ่มเติม

```
# /dev/md0:
```

8 partitions:

#	size	offset	fstype	[fsize	bsize	bps/cpg]
a:	200m	0	4.2BSD	0	0	0
c:	509952	0	unused	0	0	# "raw" part, don't edit
d:	*	*	4.2BSD	0	0	0

หลังจากที่คุณบันทึกแล้วคุณควรสร้าง ASCII file ที่บรรจุข้อมูลตาราง คุณสามารถนำเข้า ASCII file ได้ในขนาดตามคำสั่งนี้

```
bsdlable md0 > /root/minibsd-disklabel
```

ในครั้งต่อไปคุณสามารถรัน bsdlable -e md0 คุณสามารถใช้คำสั่งนี้แทนได้

```
bsdlable -R md0 /root/minibsd-disklabel
```

ต่อไปสร้าง newfs และ mount พาร์ติชันของเราที่สร้างขึ้น newfs ยังไม่ได้มีใน /etc/fstab เพราะคุณไม่มี /etc/fstab ใน ฟรีบีเอสดีเจลล์(FreeBSD jail) คุณสามารถสร้างไฟล์ว่างๆก่อนที่จะรัน newfs พิมพ์ดังนี้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
touch /etc/fstab
newfs -b 8192 -f 1024 -U /dev/md0a
mount /dev/md0a /mnt
```

ตัวอย่างเพิ่ม ถ้ามีอีก พาร์ทิชัน(partition)

```
newfs -b 8192 -f 1024 -U /dev/md0
newfs -b 8192 -f 1024 -U /dev/md0a
newfs -b 8192 -f 1024 -U /dev/md0d
mount /dev/md0 /mnt
```

ถ้าคุณได้สร้าง พาร์ทิชัน(partition) ที่สองอย่าลืม newfs พาร์ทิชันนั้นด้วย
ต่อไปคือการคัดลอกไฟล์จาก มินิบีเอสดี(miniBSD) ไปยัง /mnt ดังนี้

```
(cd /usr/minibsd ; tar cPf - .) | (cd /mnt ; tar xf -);
```

หลังจากนั้น clean up ดังนี้

```
cd /
umount /mnt
mdconfig -d -u 0
```

13. Writing the binary image to the media

คำสั่งสำหรับการเขียนลง CF Card ดังนี้

```
dd if=/usr/minibsd-disk.bin of=/dev/ad[n] ibs=8k obs=8k
```

ต้องระวัง [n] ต้องกำหนดให้ถูกต้องตาม CF card หรือสื่อที่ใช้

ถ้าคุณได้ บีบอัด ไฟล์ไว้ให้พิมพ์ดังนี้

```
gzcat /usr/minibsd-disk.bin.gz | dd of=/dev/ad[n] ibs=8k obs=8k
```

หรือ

```
cat /usr/minibsd-disk.bin.gz | gunzip | dd of=/dev/ad[n] ibs=8k obs=8k
```

ถ้าคุณต้องการดูการทำงานให้พิมพ์ Ctrl - T

14. First Boot

หลังจากที่ได้ทำตามขั้นตอนนั้นแล้วให้ทดลอง boot ระบบด้วย CF Card ที่ได้ทำมา

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ภาคผนวก ข

คู่มือการติดตั้งเพื่อใช้งานคอมมานด์ไลน์อินเทอร์เน็ตเฟสและเว็บอินเทอร์เน็ตเฟส

1. การติดตั้ง CSH Script (Commandline interface)

ในตัวของฟรีบีเอสดีนั้นจะมี CSH อยู่ในระบบอยู่แล้วจึงไม่จำเป็นต้องติดตั้ง CSH เพิ่มเข้าสู่ระบบ

เราเพียงแต่ติดตั้งตัวสคริปท์ไฟล์ที่พัฒนาขึ้น โดยนำสคริปท์ไฟล์ทั้งหมดใส่เข้าไปในไดเรกทอรี

```
/bin/project
```

แล้วทำการให้ระบบนั้นเรียกไฟล์ไปใช้โดยเพิ่มคำสั่งเข้าไปในไฟล์ที่ชื่อ /etc/rc.local ด้วยคำสั่ง

```
#/bin/project/./main.csh
```

2. การติดตั้ง Lighttpd Web server

1) ดาวน์โหลด(download) โปรแกรม lighttpd-1.4.15.tar.gz จากเว็บไซต์ <http://www.lighttpd.net> จากนั้นทำการอันซิปไฟล์(unzip)

2) ติดตั้งด้วยคำสั่ง

```
#gzip -cd lighttpd-1.4.15.tar.gz | tar xvf -
```

```
#cd lighttpd-1.4.15
```

```
#!/configure
```

```
#make
```

```
#make install
```

3) ปรับแต่งไฟล์ configuration ของ lighttpd

3. การติดตั้ง PHP

1) ดาวน์โหลด(download) โปรแกรม php-4.4.7.tar.gz จากเว็บไซต์(web site) <http://www.php.net> จากนั้นทำการ unzip

2) ติดตั้งด้วยคำสั่ง

```
#gzip -cd php-4.4.7.tar.gz | tar xvf -
```

```
#cd php-4.4.7
```

```
#!/configure
```

```
#make
```

```
#make install
```

3) ปรับแต่งไฟล์ php.ini แล้วบันทึกไว้ที่ /usr/local/lib/php.ini

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ภาคผนวก ก

คู่มือการใช้งานคอมพิวเตอร์อินเทอร์เน็ต

*** Welcome to Embedded Firewall System ***

** Embedded Firewall System setup **

- 1) Firewall Rules Module
- 2) Configuration Web Interface
- 3) Reboot System
- 4) System Configuration
- 5) Manual for user

Enter Your Option : █

แสดงหน้าหลักของระบบ

หลังจากนั้นเมื่อเราต้องการจะใช้งานในส่วนใด ให้ทำการกดเมนูเลือก อย่างเช่นตัวอย่างนี้ เราจะทำการสร้างกฎใหม่ เราจึงทำการเลือกเมนูหมายเลข 1 นั่นคือ ในส่วนของไฟร์วอลล์โมดูล

** Firewall Rules Setup **

- 0) Go to Main Menu
- 1) Create Firewall Rules
- 2) Edit/Delete Firewall Rules
- 3) Enable Rules
- 4) Show Running Rules
- 5) Disable Rules
- 6) Enable Packet-Filtering
- 7) Disble Packet-Filtering
- 8) Setup Start-up Rules
- 9) PF Rule Syntax Manual

Enter Your Option : █

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

หลังจากนั้นก็เลือกการ Create Firewall Rules โปรแกรมจะแสดงผล ดังนี้

```
*** Create Rule Wizard ***
```

```
Easy create rule by choosing these option
```

```
*****
```

- 0) Back to Previous Menu
- 1) Create Rule by Wizard
- 2) Create Rule Manually

```
Enter Your Option : █
```

ต่อไปก็เป็นการแสดงตัวอย่างการสร้างกฎแบบเป็น Wizard ซึ่งผู้ใช้เพียงแค่เลือกตามเมนู ระบบก็จะทำการ Generate กฎออกมาให้แก่ผู้ใช้ ซึ่งง่ายและไม่ยุ่งยาก

```
Enter Your Option : 1
```

```
Assign your Inbound interface : vr0
```

```
Assign your Outbound interface : vr1
```

```
** You assign Inbound is vr0 and Outbound is vr1 **
```

```
Choose Interface that you want to Assign :
```

- 1) Inbound interface
- 2) Outbound interface

```
Enter Interface : 1
```

```
Then choose Default Rule that you want
```

- 1) Default Allow
- 2) Default Deny

```
Enter Your Option : █
```

```
Choose service that you want to specified Block
```

- 1) File Transfer
- 2) Secure Shell Login
- 3) Telnet
- 4) Simple Mail Transfer
- 5) Domain Name Server
- 6) World Wide Web HTTP
- 7) Post Office Protocol (POP3)
- 8) Network News Transfer Protocol (NTP)
- 9) Interim Mail Access Protocol (IMAP)
- 10) Specified IP Address
- 0) Finish , Exit Wizard

```
Enter Your Option : █
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เนื่องจากตัวอย่างนี้เราเลือกเป็นแบบ Default Allow เราจึงต้องมีการเลือกปิดกั้นบาง service ตามที่เราไม่ต้องการ

```

10) Specified IP Address
0) Finish , Exit Wizard
Enter Your Option : 1
Another Service : 3
Another Service : 4
Another Service : 5
Another Service : 10
Type IP Address that you want to specify Block
IP Address : 192.168.1.1
Subnet masks are entered as bit count
e.g. 255.255.255.0 = 24
Subnet masks : 24
Another Service : 10
Type IP Address that you want to specify Block
IP Address : 192.168.0.2

```

เห็นดังนี้ ผลที่ได้ก็คือกฎที่เราทำการสร้างนั้นจะไปอยู่ใน /tmp/temp.conf ซึ่งจะดึงค่ามาแสดงให้

- ```

4) Show Running Rules
5) Disable Rules
6) Enable Packet-Filtering
7) Disble Packet-Filtering
8) Setup Start-up Rules
9) PF Rule Syntax Manual

```

Enter Your Option : 3

```

pass out all
block out on vr0 proto tcp to any port 21
block out on vr0 proto tcp to any port 23
block out on vr0 proto tcp to any port 25
block out on vr0 proto tcp to any port 53
block out on vr0 from 192.168.1.1/24
block out on vr0 from 192.168.0.2/32

```

Do you want to proceed [y:n]? █

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ต่อไปก็ทดลองทำการนำกฎเหล่านี้ไปใช้จริงโดยคำสั่ง Enable Rules ซึ่งระบบจะทำการคัดลอกกฎที่อยู่ใน /tmp/pftemp.conf ไปแทนที่ /conf/pf.conf แล้วระบบก็จะทำการ Enable คำสั่งซึ่งผลที่ได้จะเป็นดังนี้ คือ รูปแสดงกฎที่รันใช้งานอยู่จริงในระบบ

- 5) Disable Rules
- 6) Enable Packet-Filtering
- 7) Disable Packet-Filtering
- 8) Setup Start-up Rules
- 9) PF Rule Syntax Manual

Enter Your Option : 4

```
pass out all
block drop out on vr0 proto tcp from any to any port = ftp
block drop out on vr0 proto tcp from any to any port = telnet
block drop out on vr0 proto tcp from any to any port = smtp
block drop out on vr0 proto tcp from any to any port = domain
block drop out on vr0 inet from 192.168.1.0/24 to any
block drop out on vr0 inet from 192.168.0.2 to any
```

Press any key to continued... █

ถ้าต้องการจะยกเลิกกฎที่ใช้อยู่ให้ทำการเลือก Disable Rules แล้วผลที่ได้เป็นดังนี้คือ กฎที่ใช้งานอยู่ก็จะถูกลบออกไปจาก memory

- 5) Disable Rules
- 6) Enable Packet-Filtering
- 7) Disable Packet-Filtering
- 8) Setup Start-up Rules
- 9) PF Rule Syntax Manual

Enter Your Option : 4

Press any key to continued... █

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

อีกทางหนึ่งเราสามารถเพิ่มกฎเข้าไปใหม่ได้ โดยการสร้างกฎเองแบบ Manual

\*\*\* Insert your rules manually below \*\*\*

Action [pass:block] :

Direction [in:out] :

Interface [vr0:vr1:vr2:vr3] :

Protocol [tcp:udp:icmp] :

If you want to choose all IP Address type "any"  
or type IP Address that you want

Source IP Address :

Port are entered as number  
e.g. HTTP port 80 , FTP port 21

Source Port :

If you want to choose any IP Address type "any"  
or type number of IP Address that you want

Destination IP Address :

Subnet masks are entered as bit count  
e.g. 255.255.255.0 = 24

Subnet masks :

ซึ่งกฎที่สร้างใหม่นั้นจะไปเพิ่มต่อจากกฎเดิมที่เคยสร้างไว้แล้ว ซึ่งแน่นอนว่ากฎที่สร้างใหม่นั้นจะอยู่ในไฟล์ /tmp/pftemp.conf

- 5) Disable Rules
- 6) Enable Packet-Filtering
- 7) Disble Packet-Filtering
- 8) Setup Start-up Rules
- 9) PF Rule Syntax Manual

Enter Your Option : 3

```
pass out all
block out on vr0 proto tcp to any port 21
block out on vr0 proto tcp to any port 23
block out on vr0 proto tcp to any port 25
block out on vr0 proto tcp to any port 53
block out on vr0 from 192.168.1.1/24
block out on vr0 from 192.168.0.2/32
pass in on vr1 proto tcp from any port 55 to 192.168.1.1/24
```

Do you want to proceed [y:n]? █

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ต่อไปจะเป็นในส่วนของการแก้ไข/ลบกฎที่เคยได้ทำการสร้างไว้แล้ว ซึ่งในหน้าแรกของ การแก้ไข/ลบกฎนั้น จะมีคำอธิบายการใช้งานก่อน เพื่อที่จะให้ผู้ใช้งานง่ายต่อการทำงาน

If you want to edit Rules,you can do easily  
It's just like simple editor

If you want to know syntax goto "Firewall Rules Setup"  
then "PF Rules Syntax Manual"  
you also can create new one rule here

When you finished your job ,do steps below

- 1) Press "ESC" button
- 2) Press "a" button to exit (or waiting for menu)
- 3) Press "a" button again to save change or  
Press "b" button to not save(or waiting for menu)

Press Enter to continued... █

```

^I (escape) menu ^y search prompt ^k delete line ^p prev li ^g prev page
^o ascii code ^x search ^l undelete line ^n next li ^v next page
^u end of file ^a begin of line ^w delete word ^b back 1 char
^t begin of file ^e end of line ^r restore word ^f forward 1 char
^c command ^d delete char ^j undelete char ^z next word

```

```

1 C: 1
pass out all
block out on vr0 proto tcp to any port 21
block out on vr0 proto tcp to any port 23
block out on vr0 proto tcp to any port 25
block out on vr0 proto tcp to any port 53
block out on vr0 from 192.168.1.1/24
block out on vr0 from 192.168.0.2/32
pass in on vr1 proto tcp from any port 55 to 192.168.1.1/24

```

ต่อไปจะเป็นการตั้งค่ากฎจาก Startup Rule ซึ่งในที่นี้ก็เป็นกฎเบื้องต้นพื้นฐานที่เราทำการเก็บค่ากฎนั้นเอาไว้ ถ้าเกิดเหตุการณ์ที่เราทำการเปลี่ยนแปลงค่าไปแล้วต้องการให้นำกฎพื้นฐานของระบบขึ้นมาใช้ ก็ให้เรียกใช้ไฟล์นี้มาแทนที่ไฟล์ที่รันอยู่ ซึ่งก็คือ ไฟล์ /conf/pfboot.conf ไปแทนที่ในส่วน of /conf/pf.conf โดยเรานั้นสามารถที่จะแก้ไขเปลี่ยนแปลงกฎในไฟล์นี้ได้ เช่นเดียวกับการแก้ไขใน /tmp/pftemp.conf

Start-up Rules will running when you reboot system

- 0) Go back to previous menu
- 1) Setup Start-up Rules from temp file
- 2) Setup Start-up Rules Manually
- 3) Edit/Delete Start-up Rules
- 4) Enable Start-up Rules

Enter Your Option : █

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เราจะทำการให้ระบบนำค่ากฎพื้นฐานมาใช้งาน โดยเลือกเมนูที่ 4 จะได้ผลดังนี้

```
Start-up Rules will running when you reboot system
```

- 0) Go back to previous menu
- 1) Setup Start-up Rules from temp file
- 2) Setup Start-up Rules Manually
- 3) Edit/Delete Start-up Rules
- 4) Enable Start-up Rules

```
Enter Your Option : 4
```

```
Are you sure to enable start-up rule [y:n]? y
```

แล้วมาดูกฎที่ทำการรันอยู่จะเป็นกฎพื้นฐานที่เราทำการตั้งค่าไว้

- 4) Show Running Rules
- 5) Disable Rules
- 6) Enable Packet-Filtering
- 7) Disable Packet-Filtering
- 8) Setup Start-up Rules
- 9) PF Rule Syntax Manual

```
Enter Your Option : 4
```

```
pass in all
pass in on vr0 proto tcp from any port = http to any
pass in on vr0 proto tcp all
pass in on vr0 all
```

```
Press any key to continued...
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ต่อไปเป็นการตั้งค่าการใช้งานต่างๆของระบบ ซึ่งการที่จะใช้งานเว็บอินเตอร์เฟสนั้นต้องมีการสั่งให้เว็บเซิร์ฟเวอร์ทำงานเสียก่อน ดังนี้

```

** Web Interface Configuration **

0) Go to Main Menu
1) Enable Web Interface
2) Disable Web Interface

Enter Your Option : 1

If you want to config Embedded Firewall System through Web Interface
You have to enable web interface first

Do you want to proceed [y;n] : y
```

อีกทั้งระบบสามารถปรับเปลี่ยนไอพีของแต่ละอินเตอร์เฟสที่มีในระบบได้ ซึ่งในการตั้งค่าส่วนนี้เป็นส่วนที่จำเป็นในการทำงานต่างๆของระบบไฟร์วอลล์

```
*** Assign new IP Address below ***

Enter Interface [vr0:vr1:vr2:vr3] : vr0

Enter new IP Address : 192.168.100.10

Subnet masks are entered as binary count
e.g. Subnet masks 24,Your input is 255.255.255.0
Subnet masks : 255.255.255.0

Your new IP Address is Interface vr0 IP address 192.168.100.10/255.255.255.0

Set IP Interface Complete

Would you like to bring the vr0 interface up right now? [y;n]? y
```

อีกทั้งเราสามารถที่จะทำการสั่งให้ระบบรีสตาร์ทขึ้นมาได้ผ่านทางคอมพิวเตอร์อินเตอร์เฟสเช่นกัน

```
*** Welcome to Embedded Firewall System ***

** Embedded Firewall System setup **

1) Firewall Rules Module
2) Configuration Web Interface
3) Reboot System
4) System Configuration
5) Manual for user
6) Exit to shell

Enter Your Option : 3

Are you sure to reboot [y;n]? y
```

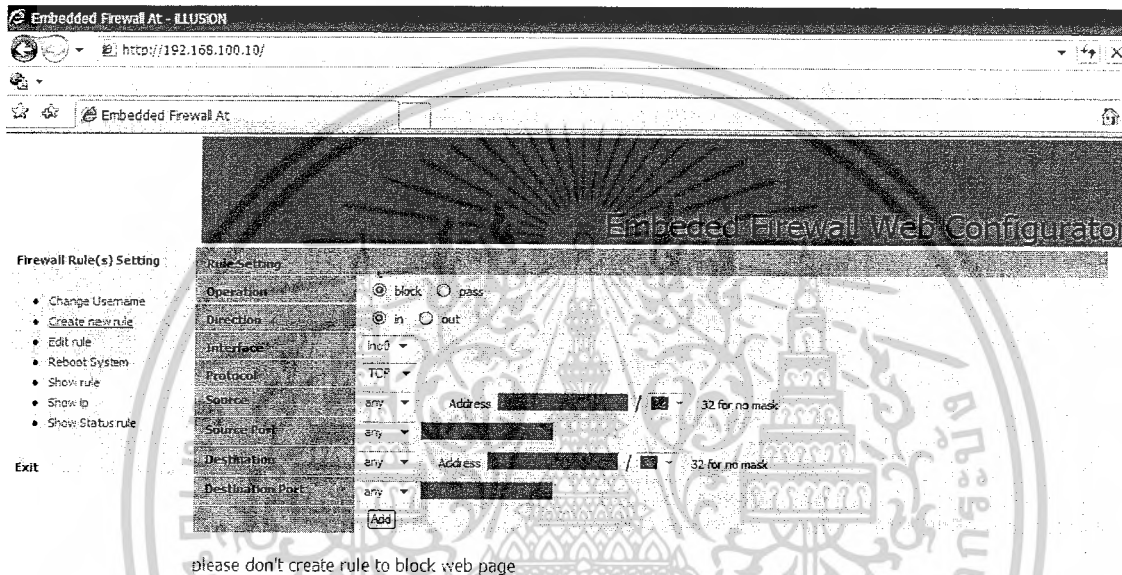
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## ภาคผนวก ง

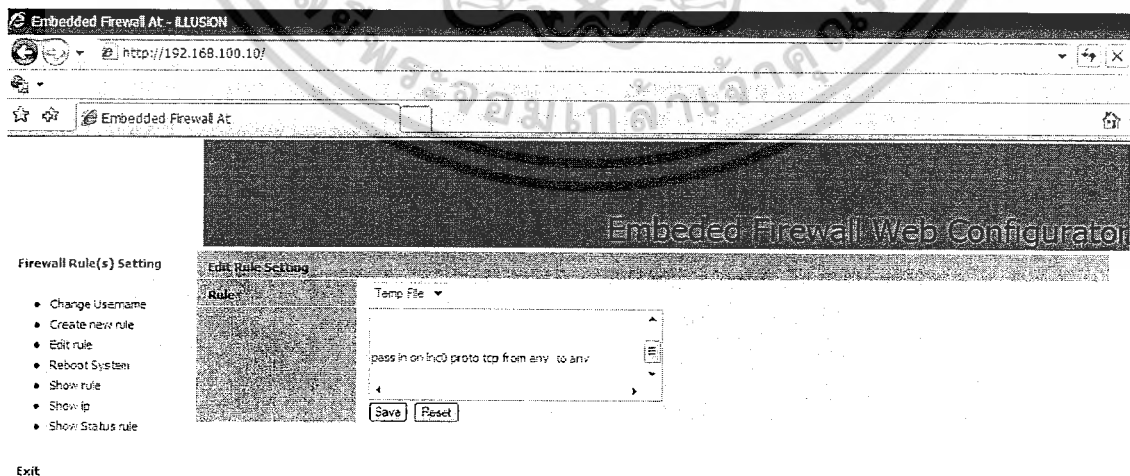
### คู่มือการใช้งานเว็บอินเตอร์เฟส

ส่วนแสดงผล

-ส่วนการสร้างกฎใหม่ ให้ผู้ดูแลระบบกรอกค่าต่างๆ ในการสร้างกฎขึ้นมาใช้ใหม่ มีปุ่ม add เพื่อทำการบันทึกกฎที่สร้างลงสู่ Config File

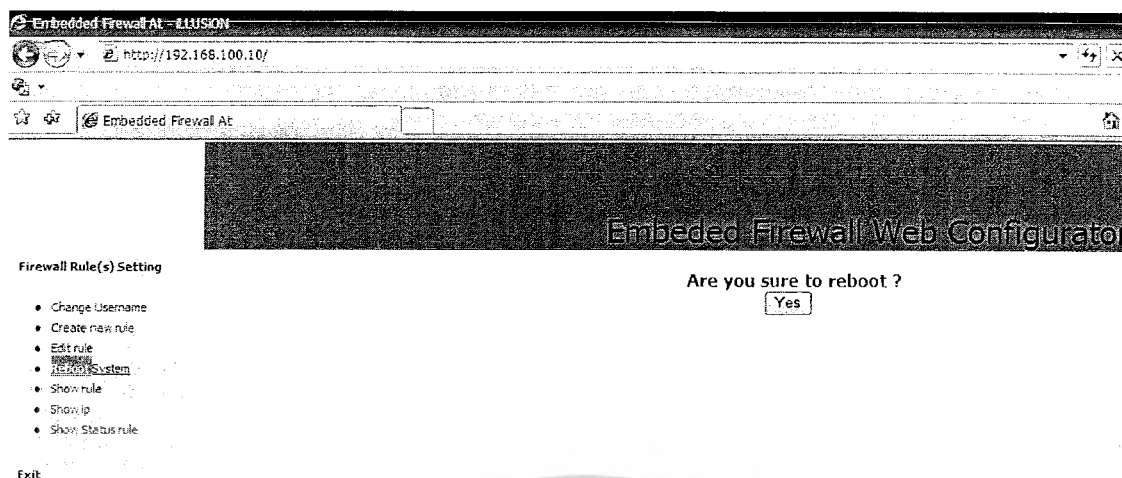


-ส่วนการแก้ไขกฎ ให้ผู้ดูแลระบบสร้างขึ้นใช้เอง เนื่องจากรู้ syntax ในการสร้างกฎและสามารถแก้ไขกฎทีละหลายข้อได้ มีปุ่ม save เพื่อบันทึกลงสู่ Config File และมี reset ทำหน้าที่เหมือน undo

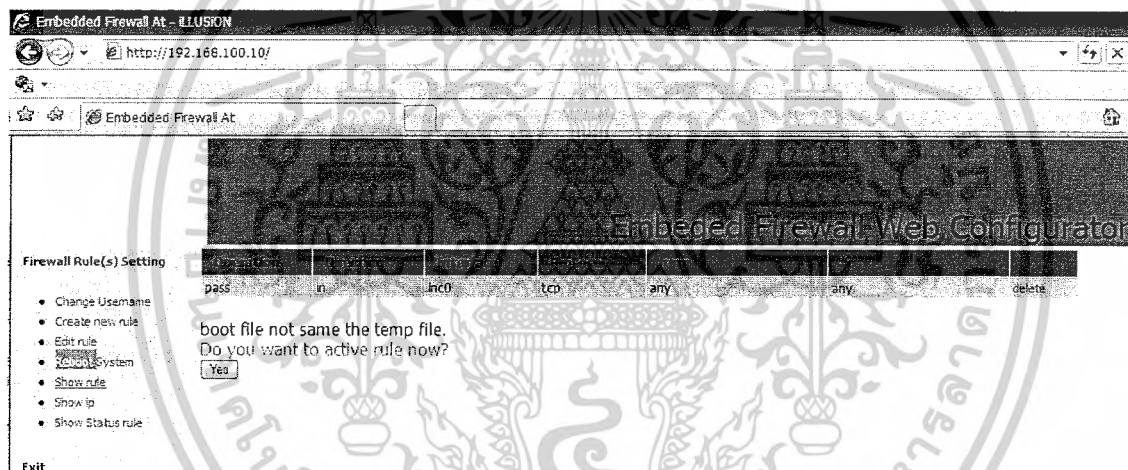


-ส่วนการรีบูตระบบ ให้ระบบเริ่มต้นการทำงานใหม่

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



-ส่วนการแสดงกฎ ใช้งานกฎ ลบกฎ ระบบทำการแสดงกฎ ผู้ใช้ระบบสามารถกด delete ได้ และกด yes เพื่อทำการบันทึกลงสู่ Boot File จากนั้นโหลดกฎลงสู่หน่วยความจำ



-ส่วนการแก้ไขไอพีแอดเดรสของอินเทอร์เน็ตเฟส ระบบทำการแสดงไอพีแอดเดรสของอินเทอร์เน็ตเฟสต่างๆ ผู้ดูแลระบบทำการ edit ได้ จากนั้นกดปุ่ม yes ไอพีแอดเดรสของอินเทอร์เน็ตเฟสนั้นจะถูกแก้ไขและระบบจะแสดงผลขึ้นมา

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Embedded Firewall At - ILLUSION

http://192.168.100.10/

Embedded Firewall At

### Embedded Firewall Web Configurator

Firewall Rule(s) Setting

- Change Username
- Create new rule
- Edit rule
- Firewall System
- Show rule
- Show log
- Show Status rule

| Interface | IP Address      | Subnetmask    |      |
|-----------|-----------------|---------------|------|
| Inc0      | 192.168.100.10  | 255.255.255.0 | edit |
| Inc1      | 192.168.100.10  | 255.255.0.0   | edit |
| Inc2      | 192.168.100.100 | 255.255.0.0   | edit |

**Defaultgateway** 192.168.100.2 edit

Are you sure to use new IP Address ?

Exit

-ส่วนการแสดงกฎที่ทำงานอยู่ ณ ปัจจุบัน ระบบทำการแสดงกฎทั้งหมดที่มีอยู่ในหน่วยความจำ ณ ขณะนั้น

Embedded Firewall At - ILLUSION

http://192.168.100.10/

Embedded Firewall At

### Embedded Firewall Web Configurator

Firewall Rule(s) Setting

- Change Username
- Create new rule
- Edit rule
- Firewall System
- Show rule
- Show log
- Show Status rule

pass out on Inc0 proto tcp all

Exit

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## ประวัติผู้เขียน

|                 |                                                                                 |
|-----------------|---------------------------------------------------------------------------------|
| ชื่อ-นามสกุล    | นางสาวสุพร รอดจากภัย                                                            |
| เดือน ปีเกิด    | มิถุนายน 2529                                                                   |
| จังหวัด         | กรุงเทพมหานคร                                                                   |
| ประวัติการศึกษา | วิทยาศาสตรบัณฑิต คณะเทคโนโลยีสารสนเทศ                                           |
| 2550            | สาขาวิชาเทคโนโลยีสารสนเทศ<br>สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหาร<br>ลาดกระบัง |
| ชื่อ-นามสกุล    | นายฉันทวัฒน์ โพธิ์ชัยทอง                                                        |
| เดือน ปีเกิด    | มีนาคม 2529                                                                     |
| จังหวัด         | ขอนแก่น                                                                         |
| ประวัติการศึกษา | วิทยาศาสตรบัณฑิต คณะเทคโนโลยีสารสนเทศ                                           |
| 2550            | สาขาวิชาเทคโนโลยีสารสนเทศ<br>สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหาร<br>ลาดกระบัง |
| ชื่อ-นามสกุล    | นายปวิณวัชร วัฒนโมยิต                                                           |
| เดือน ปีเกิด    | ธันวาคม 2528                                                                    |
| จังหวัด         | ชลบุรี                                                                          |
| ประวัติการศึกษา | วิทยาศาสตรบัณฑิต คณะเทคโนโลยีสารสนเทศ                                           |
| 2550            | สาขาวิชาเทคโนโลยีสารสนเทศ<br>สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหาร<br>ลาดกระบัง |

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้