โปรแกรมควบคุมไอพีไฟร์วอลล์ในเอ็กซ์วินโดว์บนระบบปฏิบัติการฟรีบีเอสดี

The Development of X-windows Based IP Firewall Configuration Software on FreeBSD

โดย

นางสาวสริตา ปรัชญาทิพย์

รหัส 41067003

อาจารย์ที่ปรึกษา

อาจารย์อัครินทร์ คุณกิตติ

รายงานนี้เป็นส่วนหนึ่งของวิชาโครงการพัฒนาระบบงาน

หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ

ภาคเรียนที่ 2 ปีการศึกษา 2542

คณะเทคโนโลยีสารสนเทศ

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ชื่อหัวข้อ	โปรแกรมควบคุมไอพีไฟร์วอลล์ในเอ็กซ์วินโดว์บนระบบปฏิบัติการฟรีบีเอสดี
นักศึกษา	นางสาวสริตา ปรัชญาทิพย์
อาจารย์ที่ปรึกษา	อาจารย์อัครินทร์ คุณกิตติ
ระดับการศึกษา	วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
แขนงวิชา	วิทยาการสารสนเทศ
ปีการศึกษา	2542

บทคัดย่อ

ไอพีไฟร์วอลล์บนฟรีบีเอสดีนำหลักการทำงานเป็นไฟร์วอลล์แบบกรองแพ็คเก็ตมาใช้ โดยอาศัยกฎหรือนโยบายในการควบคุมและป้องกันการเข้าออกของแพ็คเก็ตต่าง ๆ ไอพีไฟร์วอลล์มีการกระทำอยู่หลายแบบได้แก่ การอนุญาตและการปฏิเสธแพ็คเก็ต การกรองแพ็คเก็ตจะพิจารณาข้อมูลในส่วนหัวของไอพี/ทีซีพี/ยูดีพี เช่นแอดเดรสต้นทาง แอดเดรสปลายทาง เป็นต้น ในโครงงานได้มีการพัฒนาโปรแกรมเพื่อควบคุมฟังก์ชันการทำงานไอพีไฟร์วอลล์ โดยจะใช้ไอพีไฟร์วอลล์ที่มากับฟรีบีเอสบีเป็นตัวติดต่อกับส่วนกรองในเคอร์เนล เนื่องจากไอพีไฟร์วอลล์ในฟรีบีเอสดีมีรายละเอียดในการสร้างกฎจำนวน และลักษณะการติดต่อระหว่างผู้ใช้กับไอพีไฟร์วอลล์เป็นแบบเท็กซ์โหมด ทำให้ไม่สะดวกในการใช้งาน โปรแกรมที่พัฒนาขึ้นดังกล่าวจึงมีลักษณะการทำงานแบบกราฟฟิกทั้งหมดแทนการใช้งานที่เป็นแบบเดิม ซึ่งจะอยู่บนระบบเอ็กซ์วินโดว์ที่เรียกว่า "เอ็กซ์ฟรี 86" ภาษาและเครื่องมือที่ใช้ในการพัฒนาคือ ทีซีแอล/ทีเค ผลที่ได้คือโปรแกรมไอพีไฟร์วอลล์ที่พัฒนาขึ้นมาสามารถทำการเพิ่มกฎ ลบกฎ แสดงรายการของกฎ ลบค่าตัวนับแพ็คเก็ต ตั้งเวลาการกรอง วิเคราะห์กฎแบบง่าย ตรวจดูจำนวนแพ็คเก็ต และจัดการนโยบายให้กระจายเป็นกฎต่าง ๆ ได้ จากการพัฒนาโปรแกรมทำให้เข้าใจถึงความสามารถของฟังก์ชันไอพีไฟร์วอลล์และนำฟังก์ชันนี้มาใช้ประโยชน์ได้

Title	The Development of X-windows Based IP Firewall Configuration Software on FreeBSD
Student	Ms.Sarita Pratchayathip
Advisor	Mr.Akharin Khunkitti
Level of Study	Master of Science in Information Technology
Major	Information Science
Academic Year	1999

ABSTRACT

IP firewall or IPFW, the software supplied with FreeBSD, is a packet filtering system which resides in the kernel. Together, it allows administrator to define and query rules, which are used by the kernel in its filtering decisions. The main part of the IPFW system lives in the kernel and its command syntaxes are quite complicated, such as many descriptions for addition, and its configuration has been done in text mode. The developed software has graphical interface, running on X window system, XFree86. It is implemented by Tcl/Tk and provides rule addition/deletion, listing, flushing, clearing, scheduling, basic rule analysis, monitoring, and simple policy management.

กิตติกรรมประกาศ

ในการพัฒนาโปรแกรมควบคุมไอพีไฟร์วอลล์นี้ ต้องอาศัยแหล่งความรู้ต่าง ๆ คำแนะนำและปรึกษาทั้งในภาคทฤษฎีและภาคปฏิบัติ อุปกรณ์ทางด้านฮาร์ดแวร์และซอฟต์แวร์ที่จำเป็นต่างทั้งหลาย ตลอดจนกำลังใจและแรงที่ได้จากบุคคลต่าง ๆ ที่สมควรได้รับความขอบคุณเป็นพิเศษดังนี้

1. คุณพ่อ คุณแม่ ผู้ให้กำเนิด เลี้ยงดู เอาใจใส่ และดูแล อบรมให้ประพฤติในสิ่งที่ดีและถูกต้อง ตลอดจนส่งเสริมทางด้านการศึกษาอย่างดีที่สุด
2. มูลนิธิเพื่อการศึกษาคอมพิวเตอร์และการสื่อสาร (C&C) ที่ได้มอบทุนให้ศึกษาจนสำเร็จได้
3. อาจารย์อัครินทร์ คุณกิตติ อาจารย์ที่ปรึกษาโครงงาน ผู้ให้คำปรึกษาในการจัดทำโครงงาน และจัดหาทรัพยากรต่าง ๆ ให้แก่ข้าพเจ้า
4. พี่เกลียว พี่กิตติ รุ่นพี่ CS รุ่นพี่ IS3 และเพื่อน IS5 ทุกคนที่คอยให้กำลังใจในการทำงานตลอดเวลา

ทั้งหมดนี้ถูกรวบรวมได้จากหลายฝ่าย เพื่อให้การศึกษาและการพัฒนาโปรแกรมเป็นไปโดยสำเร็จ

นางสาวสริตา ปรัชญาทิพย์
ผู้จัดทำ

สารบัญ

หน้า

บทคัดย่อภาษาไทย I
บทคัดย่อภาษาอังกฤษ II
กิตติกรรมประกาศ III
สารบัญ IV
สารบัญตาราง VII
สารบัญภาพ VIII
บทที่
1. บทนำ 1
1.1 ความเป็นมาและความสำคัญของปัญหา 1
1.2 วัตถุประสงค์ในการพัฒนาระบบงาน 2
1.3 เป้าหมายของการพัฒนาระบบงาน 2
1.4 ประโยชน์ที่คาดว่าจะได้รับ 2
1.5 ขอบเขตของการพัฒนาระบบงาน 2
1.6 ทฤษฎีที่ใช้ในการพัฒนาระบบงาน 3
1.7 ขั้นตอนในการพัฒนาระบบงาน 3
1.8 รายละเอียดของแต่ละบท 4
2. ไอพีไฟร์วอลล์ 5
2.1 โปรโตคอลทีซีพี/ไอพี (TCP/IP protocol) 5
2.1.1 โครงสร้างของโปรโตคอล TCP/IP 5
2.1.2 ไอพี 7
2.1.3 ทีซีพี 8
2.1.4 ยูดีพี 9
2.2 ไฟร์วอลล์ 10
2.2.1 ประเภทของไฟร์วอลล์ 10
2.3 ระบบปฏิบัติการฟรีบีเอสดี 12
2.3.1 X-Window System 13

สารบัญ (ต่อ)

หน้า

2.3.2 เครื่องมือในการรักษาความปลอดภัยในฟรีบีเอสดี 13
2.4 ไอพีไฟร์วอลล์ 14
3. การพัฒนาระบบงาน 17
3.1 เครื่องมือในการใช้ในการพัฒนาระบบงาน 17
3.2 การเลือกโครงร่างของไอพีไฟร์วอลล์ 17
3.3 การสร้างโครงร่างของไอพีไฟร์วอลล์ 18
3.3.1 รูปแบบคำสั่งของ Addition/Deletion 18
3.3.2 รูปแบบคำสั่งของ Listing 20
3.3.3 รูปแบบคำสั่งของ Flushing 20
3.3.4 รูปแบบคำสั่งของ Clearing 20
3.4 ตัวอย่างการใช้คำสั่งของไอพีไฟร์วอลล์ในฟรีบีเอสดี 20
3.5 การทำงานของไอพีไฟร์วอลล์ในโครงงาน 21
4. การออกแบบระบบงาน 24
4.1 การออกแบบฟังก์ชันการทำงานต่าง ๆ 24
4.1.1 ฟังก์ชันการทำงานทั่วไป 24
4.1.2 ฟังก์ชันการทำงานเพิ่มเติม 30
4.2 การออกแบบฐานข้อมูลของกฎ 38
4.3 การออกแบบเมนูที่ใช้งานในระบบงาน 39
5. การสรุปผลการทำงานของระบบงาน 42
5.1 การทดสอบระบบงาน 42
5.2 ผลสรุปที่ได้จากการทดสอบระบบ 45
5.3 สรุปผลการพัฒนาโปรแกรม 48
5.4 ข้อเสนอแนะ 48
บรรณานุกรม 50
ภาคผนวก ก 51
ภาคผนวก ข 51

สารบัญ (ต่อ)

หน้า

ภาคผนวก ค 51
ภาคผนวก ง 51
ภาคผนวก จ 52
ประวัติผู้เขียน 57

สารบัญตาราง

หน้า

ตารางที่

2.1 ระดับความปลอดภัยของระบบ 13
5.1 ตัวอย่างกฎสำหรับการสร้างกฎในกรณีที่ 1 43
5.2 ตัวอย่างกฎสำหรับการสร้างกฎในกรณีที่ 2 44

สารบัญภาพ

หน้า

ภาพที่

2.1 โครงสร้างโปรโตคอลทีซีพี/ไอพี 6
2.2 หมายเลขเครื่องอินเตอร์เน็ตทั้ง 5 ประเภท 7
2.3 รูปแบบของไอพีดาต้าแกรม 8
2.4 รูปแบบของเซ็กเม้นต์ 9
2.5 รูปแบบของฟิลด์ในยูดีพีดาต้าแกรม 9
2.6 การใช้สกรีนนิ่งเราท์เตอร์เพื่อทำการกรองแพ็คเก็ต 10
2.7 โฟล์วชาร์ทการทำงานของการกรองแพ็คเก็ต 11
2.8 การใช้พร็อกซี่บริการกับโฮสต์ที่เป็นดูอัลโฮม 12
3.1 การกรองแพ็คเก็ตในระบบของโครงงาน 21
3.2 ภาพโดยรวมของโปรแกรม 22
3.3 โครงสร้างภายในโปรแกรม (1) 23
3.4 โครงสร้างภายในโปรแกรม (2) 23
4.1 การทำงานของการเพิ่มกฎ 25
4.2 รูปแบบการสร้างกฎโดยใช้โปรโตคอลไอพี 26
4.3 รูปแบบการสร้างกฎโดยใช้โปรโตคอลทีซีพี 26
4.4 รูปแบบการสร้างกฎโดยใช้โปรโตคอลยูดีพี 27
4.5 รูปแบบการสร้างกฎโดยใช้โปรโตคอลไอซีเอ็มพี 27
4.6 รูปแบบการสร้างกฎโดยใช้โปรโตคอลทั้งหมด 27
4.7 การทำงานของการลบกฎ 28
4.8 การทำงานของการลบกฎทั้งหมด 29
4.9 การทำงานของการแสดงรายการของกฎ 29
4.10 การทำงานของการลบค่าตัวนับแพ็คเก็ต 30
4.11 การทำงานของการตั้งเวลาการกรอง 31
4.12 การทำงานของการตรวจสอบจำนวนแพ็คเก็ต 32
4.13 ตัวอย่างการกระจายนโยบายให้เป็นกฎต่าง ๆ 33

สารบัญภาพ (ต่อ)

หน้า

4.14 การทำงานของการสร้างนโยบาย 34
4.15 การทำงานของการแก้ไขนโยบาย 35
4.16 การทำงานของการเพิ่มกลุ่ม 36
4.17 การทำงานของการแก้ไขกลุ่ม 37
4.18 ลักษณะของการเก็บข้อมูลในไฟล์กฎ 38
4.19 ลักษณะของการเก็บข้อมูลในไฟล์นโยบาย 38
4.20 ลักษณะของการเก็บข้อมูลในไฟล์กลุ่ม 39
4.21 หน้าต่างหลักของโปรแกรม 39
4.22 หน้าต่างของการเพิ่มกฎ 39
4.23 หน้าต่างของการลบกฎ 40
4.24 หน้าต่างของผลลัพธ์ที่ได้จากการแสดงรายการของกฎ 40
4.25 หน้าต่างของการตั้งเวลาการกรอง 40
4.26 หน้าต่างของการจัดการนโยบายของกฎ 40
4.27 หน้าต่างของการสร้างนโยบาย 41
4.28 หน้าต่างของการสร้างกลุ่ม 41
5.1 การบันทึกเวลาการกรอง 43
5.2 การลบกฎออกไปตามหมายเลขที่กำหนด 43
5.3 การแสดงรายการของกฎหลังจากลบรายการกฎที่ 3 ออกไป 44
5.4 การตอบรับการบันทึกเวลาการกรอง 45
5.5 การแสดงรายการของกฎของโปรแกรม 46
5.6 การแสดงรายการของกฎผ่านคอนโซล 46
5.7 แผนภูมิวงกลมแสดงจำนวนแพ็คเก็ตที่ได้รับ 46
5.8 การซ้ำกันของกฎ 47
5.9 การแสดงรายการของกฎที่ไม่ได้ถูกลบออกไป 47
5.10 การแสดงรายการของกฎที่ถูกลบออกไปหมด 47
5.11 นโยบายที่กระจายออกมาเป็นกฎต่าง ๆ 48

สารบัญภาพ (ต่อ)

หน้า

จ.1 การบันทึกไฟล์กฎ 53
จ.2 หน้าต่างที่ปรากฏเมื่อทำคำสั่ง Update สำเร็จ 53
จ.3 การแสดงรายการของกฎเมื่อทำคำสั่ง Update 53
จ.4 การลบค่าตัวนับแพ็คเก็ต 54
จ.5 การแสดงค่าเริ่มต้นของกฎเมื่อรายการของกฎทั้งหมดถูกลบออกไป 54
จ.6 ตัวอย่างการบันทึกเวลาการกรอง 55

บทที่ 1

บทนำ

การเติบโตอย่างต่อเนื่องของโลกอินเตอร์เน็ต มีส่วนผลักดันให้เครือข่ายต่าง ๆ มีความตื่นตัวทางด้านความปลอดภัยมากขึ้น เนื่องจากทรัพยากรของแต่ละเครือข่ายมีความสำคัญมาก จึงทำให้การรักษาความปลอดภัยต่าง ๆ ถูกนำมาใช้มากขึ้น ในโครงงานจึงได้มีการพัฒนาโปรแกรมเพื่อควบคุมฟังก์ชันการทำงานของไอพีไฟร์วอลล์ ซึ่งเป็นระบบรักษาความปลอดภัยอย่างหนึ่งที่ระบบปฏิบัติการฟรีบีเอสดีได้ให้บริการไว้แก่ผู้ใช้ (เวอร์ชันของฟรีบีเอสดีที่ใช้ในโครงงานคือ เวอร์ชัน 3.2) สำหรับป้องกันการรุกรานทรัพยากรในเครือข่ายของตน ดังนั้นในบทนี้จะกล่าวถึงความเป็นมาและความสำคัญของปัญหา วัตถุประสงค์ของการพัฒนาระบบงาน เป้าหมายของการพัฒนาระบบงาน ประโยชน์ที่คาดว่าจะได้รับ ขอบเขตของการพัฒนาระบบงาน ขั้นตอนการทำงาน ทฤษฎีที่นำมาใช้ในการพัฒนาระบบงาน และรายละเอียดในบทต่าง ๆ

1.1 ความเป็นมาและความสำคัญของปัญหา

ในโลกของการสื่อสารผ่านเครือข่ายอินเตอร์เน็ต ทุกเครือข่ายย่อมต้องการความปลอดภัยจากการเข้าถึงของเครือข่ายอื่น ๆ สิ่งที่แน่นอนคือ เครือข่ายภายในจำเป็นต้องมีระบบรักษาความปลอดภัยของตัวเครือข่าย เพื่อป้องการรุกรานจากผู้ที่แฝงตัวเข้ามาเพื่อต้องการประโยชน์ต่าง ๆ จากเครือข่ายภายใน ระบบรักษาความปลอดภัยนั้นคือไฟร์วอลล์ (Firewall)

ไฟร์วอลล์แบ่งเป็น 3-4 ประเภทขึ้นอยู่กับระดับความปลอดภัยที่ผู้ใช้ต้องการ ไฟร์วอลล์ที่นิยมใช้กันมากมีอยู่ 2 ประเภทคือ ไฟร์วอลล์แบบกรองแพ็คเก็ต (Packet filtering Firewall) และการบริการทำงานแทน (Proxy Services) ไฟร์วอลล์ 2 ประเภทนี้มีการนำเสนออยู่ในโครงงานนี้ด้วย แต่ว่าจะเน้นไปที่ไฟร์วอลล์แบบกรองแพ็คเก็ตมากกว่า

ปัจจุบันนี้หลักการไฟร์วอลล์ได้ถูกนำไปประยุกต์ใช้บนระบบปฏิบัติการยูนิกต์ (Unix)ได้แก่ ลีนุกต์ (Linux) และฟรีบีเอสดี (FreeBSD) เป็นต้น ในระบบปฏิบัติการฟรีบีเอสดีมีฟังก์ชันตัวหนึ่งที่ทำหน้าที่เป็นไฟร์วอลล์เรียกว่า “ไอพีไฟร์วอลล์” (IP Firewall หรือ IPFW) ซึ่งไอพีไฟร์วอลล์นี้ได้นำเอาหลักการของไฟร์วอลล์แบบกรองแพ็คเก็ตมาใช้ในการทำงาน โดยจะมีรายการของกฎ (Rule List) เป็นตัวควบคุมการเข้าและออกของแพ็คเก็ตที่ผ่านเครือข่ายภายในกับเครือข่ายภายนอก โดยจะ

ระบุการยอมรับหรือการปฏิเสธแพ็คเก็ตนั้น ๆ และแต่ละแพ็ตเก็ตจะถูกกรองโดยอาศัยคำสำคัญ (Keyword) ซึ่งเป็นฟิลด์ (Field) ที่อยู่ในแพ็คเก็ตเช่น แอดเดรสต้นทาง (Source Address) แอดเดรสปลายทาง (Destination Address) พอร์ตต้นทาง (Source Port) และพอร์ตปลายทาง (Destination Port) เป็นต้น ผู้ใช้สามารถเพิ่ม ลบ และแก้ไขกฎ โดยทำคำสั่งตามรูปแบบที่กำหนดไว้ ดังนั้นผู้ใช้จะต้องรู้รูปแบบของคำสั่งต่าง ๆ จึงจะสามารถเข้าไปกระทำกับกฎได้ จะเห็นได้ว่าลักษณะการทำงานดังกล่าวเป็นไปค่อนข้างยุ่งยาก เนื่องจากลักษณะการทำงานดังกล่าวเป็นแบบเท็กซ์โหมด (Text Mode) จึงได้มีแนวคิดในการพัฒนาโปรแกรมควบคุมฟังก์ชันการทำงานของไอพีไฟร์วอลล์ให้มีความสะดวกขึ้นในการใช้งานของผู้ใช้โดยปรับเปลี่ยนการทำงานจากเท็กซ์โหมดเป็นกราฟิคโหมด (Graphice Mode) รวมทั้งมีเครื่องมืออื่น ๆ ที่ประกอบในการทำงานของไอพีไฟร์วอลล์มีประสิทธิภาพมากยิ่งขึ้นด้วยเช่น การตั้งเวลาการกรองแพ็คเก็ตโดยมีการระบุช่วงเวลาที่ต้องการกรองลงไป (Scheduling) การวิเคราะห์กฎขั้นพื้นฐาน เพื่อไม่ให้กฎมีการซ้ำกัน (Basic Rule Analysis) การตรวจสอบจำนวนแพ็คเก็ตที่เข้ามา (Monitoring) และการจัดการนโยบาย โดยจะมีการสร้างนโยบายแล้วกระจายออกเป็นกฎต่าง ๆ (Policy Management)

1.2 วัตถุประสงค์ในการพัฒนาระบบงาน

- เพื่อศึกษาฟังก์ชันการทำงานของไอพีไฟร์วอลล์
- เพื่อวิเคราะห์และออกแบบ รวมถึงการพัฒนาโปรแกรมที่ควบคุมไอพีไฟร์วอลล์ในเอ็กซ์วินโดว์ (X-windows) บนฟรีบีเอสดี
- เพื่อลดความยุ่งยากในการทำคำสั่งไอพีไฟร์วอลล์

1.3 เป้าหมายของการพัฒนาระบบงาน

- ไอพีไฟร์วอลล์โปรแกรมที่สร้างขึ้นมาจะทำงานภายใต้ระบบปฏิบัติการฟรีบีเอสดี
- ไอพีไฟร์วอลล์โปรแกรมจะต้องสามารถกรองแพ็คเก็ตได้ตามเงื่อนไขที่กำหนด
- ผู้ใช้สามารถตั้งเวลาการกรองแพ็คเก็ตและตรวจดูแพ็คเก็ตที่เข้ามาได้
- ผู้ใช้จะได้รับการใช้งานในฟังก์ชันของไอพีไฟร์วอลล์ที่ง่าย โดยมีการติดต่อกับผู้ใช้แบบกราฟฟิก (Graphic User Interface : GUI)
- ไอพีไฟร์วอลล์โปรแกรมสามารถที่จะบันทึกและแสดงเหตุการณ์ที่เกี่ยวข้องกับการกรองแพ็คเก็ตไว้ในไฟล์ (File)

1.4 ประโยชน์ที่คาดว่าจะได้รับ

ผู้ใช้ได้รับความสะดวกมากขึ้นในการใช้งาน เนื่องจากมาการปรับเปลี่ยนการทำงานจากเท็กซ์โหมดเป็นกราฟฟิกโหมด รวมไปถึงมีฟังก์ชันการทำงานที่เพิ่มเติมเพื่อให้การทำงานของฟังก์ชันไอพีไฟร์วอลล์ถูกนำมาใช้ให้เป็นประโยชน์มากขึ้น

1.5 ขอบเขตของการพัฒนาระบบงาน

ไอพีไฟร์วอลล์โปรแกรมได้แบ่งการทำงานออกเป็น 2 ฟังก์ชันหลักใหญ่คือ ฟังก์ชันการทำงานทั่วไปกับฟังก์ชันการทำงานที่เพิ่มเติม

1) ฟังก์ชันการทำงานทั่วไปประกอบด้วยการทำงานย่อย ๆ ดังนี้
   - การเพิ่มกฎใหม่เข้าไป
   - การลบกฎที่ไม่ต้องการออก
   - การลบกฎทั้งหมดออกไป
   - การแสดงกฎที่มีทั้งหมด
   - การลบค่าตัวนับแพ็คเก็ต
2) ฟังก์ชันการทำงานที่เพิ่มเติมประกอบด้วย
   - การตั้งเวลาการกรองแพ็คเก็ตในช่วงเวลาที่สามารถกำหนดเองได้
   - การมอนิเตอร์ (Monitor) จำนวนแพ็คเก็ตที่เข้ามา
   - การวิเคราะห์กฎขั้นพื้นฐาน เพื่อไม่ให้กฎมีการซ้ำกัน
   - การจัดกลุ่มที่เป็นนโยบายแล้วกระจายออกเป็นกฎต่าง ๆ

1.6 ทฤษฎีที่ใช้ในการพัฒนาระบบงาน

- หลักการของโปรโตคอลทีซีพี/ไอพี (TCP/IP) โดยจะเน้นไปที่โปรโตคอลไอพี (IP) ทีซีพี (TCP) และยูดีพี (UDP)
- การทำงานของไฟร์วอลล์โดยทั่วไป และลักษณะการทำงานของไฟร์วอลล์แบบกรองแพ็คเก็ตรวมถึงพร็อกซี่บริการ
- ลักษณะของฟรีบีเอสดี ซึ่งเป็นระบบปฏิบัติการยูนิกซ์แบบหนึ่งบนเครื่องพีซี
- การทำงานของไอพีไฟร์วอลล์ โดยที่ไอพีไฟร์วอลล์เป็นฟังก์ชันหนึ่งที่ระบบปฏิบัติการฟรีบีเอสดีได้จัดหาไว้สำหรับการรักษาความปลอดภัย

1.7 ขั้นตอนในการพัฒนาระบบงาน

- ศึกษาการทำงานของไอพีไฟร์วอลล์
- มองถึงปัญหาที่เกิดขึ้นในการใช้งานของฟังก์ชันไอพีไฟร์วอลล์
- ศึกษาการทำงานของไฟร์วอลล์แบบกรองแพ็คเก็ตและระบบปฏิบัติการฟรีบีเอสดี
- หาแนวทางในการแก้ไขปัญหาที่เกิดขึ้น
- ทำการออกแบบโปรแกรมควบคุมไอพีไฟร์วอลล์
- ศึกษาเครื่องมือที่จะนำมาใช้ในการพัฒนาระบบงาน
- พัฒนาโปรแกรมควบคุมไอพีไฟร์วอลล์ พร้อมทั้งสร้างเอกสารประกอบการพัฒนาโปรแกรม
- ทดสอบการใช้งานของโปรแกรมที่พัฒนาแล้ว
- สรุปผลการทดสอบจากการใช้งานที่เกิดขึ้น

1.8 รายละเอียดของแต่ละบท

<u>บทที่ 2</u> เป็นบทที่รวบรวมทฤษฎีต่าง ๆ ซึ่งเกี่ยวข้องกับไอพีไฟร์วอลล์ โดยจะกล่าวถึงโปรโตคอลทีซีพี/ไอพี ไฟร์วอลล์แบบกรองแพ็คเก็ต ระบบปฏิบัติการฟรีบีเอสดี และไอพีไฟร์วอลล์

<u>บทที่ 3</u> สำหรับบทนี้จะกล่าวถึงลักษณะการทำงาน หลักการ รูปแบบคำสั่งที่ใช้ และตัวอย่างการสร้างไอพีไฟร์วอลล์

<u>บทที่ 4</u> การออกแบบโปรแกรม จะแสดงความสัมพันธ์ขององค์ประกอบต่าง ๆ ภายในโปรแกรม ได้แก่ ฟังก์ชันการทำงานต่าง ๆ การออกแบบฐานข้อมูลของกฎ และการออกแบบหน้าจอ

<u>บทที่ 5</u> กล่าวถึงการสรุปผลการพัฒนาโปรแกรม โดยจะกำหนดสถานการณ์ 3 สถานการณ์ แสดงผลที่ได้จากการทดลอง และข้อเสนอแนะ

บทที่ 2

ไอพีไฟร์วอลล์

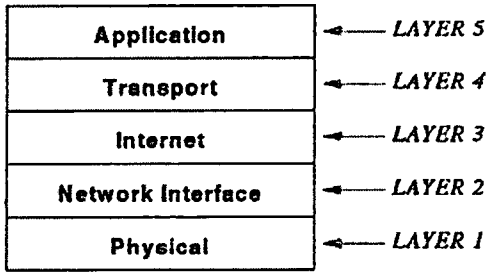
การสร้างระบบงานอย่างหนึ่งให้สำเร็จได้ จำเป็นต้องอาศัยหลักการต่าง ๆ มาประกอบ ซึ่งหลักการต่าง ๆ อาจจะมาจากหลักการที่มีอยู่หรือจากหลักการที่คิดขึ้นมาใหม่ ในโครงงานได้นำหลักการต่าง ๆ มาประกอบเพื่อทำให้เกิดความเข้าใจในการทำงานของไอพีไฟร์วอลล์ ซึ่งหลักการที่เกี่ยวข้องได้แก่ การทำงานของโปรโตคอลทีซีพี/ไอพี โดยเฉพาะชั้นอินเตอร์เน็ตและชั้นทรานสปอร์ต เนื่องทั้งสองชั้นนี้เกี่ยวข้องกับโปรโตคอลไอพี ทีซีพี และยูดีพี และนอกจากโปรโตคอลพวกนี้ก็ยังมีอีกหลายโปรโตคอลที่ให้บริการอยู่ ในส่วนของไฟร์วอลล์จะเน้นไฟร์วอลล์ในระดับพื้นฐาน นั่นคือไฟร์วอลล์แบบกรองแพ็คเก็ต ซึ่งเป็นไฟร์วอลล์ที่อาศัยกฎหรือนโยบายเป็นตัวควบคุมการทำงาน และในระบบปฏิบัติการฟรีบีเอสดีได้มีการจัดหาฟังก์ชันที่ให้บริการทางด้านการรักษาความปลอดภัยเรียกว่า “ไอพีไฟร์วอลล์” ดังนั้นไอพีไฟร์วอลล์จึงเกี่ยวข้องกับหลักการต่าง ๆ ที่ได้กล่าวมาในเบื้องต้น

2.1 โปรโตคอลทีซีพี/ไอพี (TCP/IP protocol)

แรกเริ่มโปรโตคอลทีซีพี/ไอพีคือระเบียบวิธีหรือโปรโตคอลในการสื่อสารกันระหว่างเครื่องคอมพิวเตอร์ที่เชื่อมต่อกันในระบบยูนิกซ์ (Unix) สำหรับปัจจุบันนี้โปรโตคอลทีซีพี/ไอพีมีใช้งานในเครื่องคอมพิวเตอร์แทบทุกแบบ ทำให้เครื่องคอมพิวเตอร์แบบใดก็ตามที่ทำงานกับซอฟต์แวร์โปรโตคอลทีซีพี/ไอพีก็สามารถเชื่อมเข้าในเครือข่ายโปรโตคอลทีซีพี/ไอพีได้ และแต่ละเครือข่ายก็สามารถเชื่อมโยงกันทำให้กลายเป็นเครือข่ายอินเตอร์เน็ตในที่สุด

2.1.1 โครงสร้างของโปรโตคอลทีซีพี/ไอพี

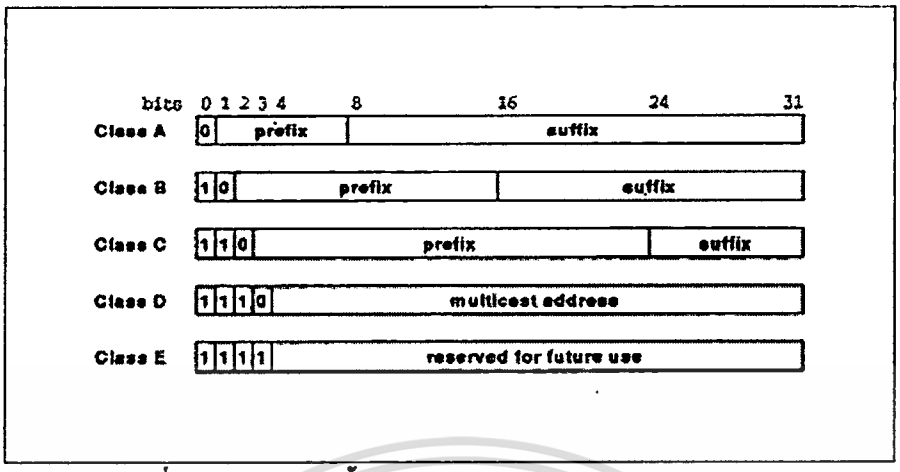
โปรโตคอลโปรโตคอลทีซีพี/ไอพีเป็นชุดโปรโตคอลที่ประกอบด้วยไอพี (IP: Internet Protocol), ทีซีพี (TCP: Transmission Control Protocol), ยูดีพี (UDP: User Datagram Protocol) ฯลฯ โครงสร้างของโปรโตคอลทีซีพี/ไอพีแสดงอยู่ในภาพที่ 2.1 มีจำนวน 5 ชั้น สอดคล้องกับชั้นต่าง ๆ ของแบบจำลองอ้างอิงสำหรับการเชื่อมต่อระหว่างระบบเปิด (OSI Reference Model) ดังนี้ (Comer:1997)



ภาพที่ 2.1 โครงสร้างโปรโตคอลทีซีพี/ไอพี

- **Layer 1: Physical** ในชั้นที่ 1 จะเกี่ยวกับอุปกรณ์เครือข่ายพื้นฐานอย่างเดียว ซึ่งจะสอดคล้องกับชั้นที่ 1 ของโมเดลการลำดับชั้นที่เป็นมาตรฐาน
- **Layer 2: Network Interface** โปรโตคอลของชั้นที่ 2 จะเกี่ยวกับการจัดข้อมูลลงในเฟรม (Frame) และการส่งเฟรมต่าง ๆ ข้ามเครือข่าย ซึ่งการทำงานจะคล้ายกับโปรโตคอลในชั้นที่ 2 ของโมเดลการลำดับชั้นที่เป็นมาตรฐาน
- **Layer 3: Internet** โปรโตคอลต่าง ๆ ในชั้นที่ 3 จะกำหนดรูปแบบของแพ็คเก็ตที่จะส่งข้ามเครือข่ายอินเตอร์เน็ต การทำงานจะคล้ายกับกลไกที่ใช้ในการส่งแพ็คเก็ตจากคอมพิวเตอร์เครื่องหนึ่งไปเครื่องปลายทางผ่านเราท์เตอร์ (Router)
- **Layer 4: Transport** การทำงานของโปรโตคอลต่าง ๆ ในชั้นที่ 4 จะคล้ายกับการทำงานของชั้นที่ 4 ของโมเดลการลำดับชั้นที่เป็นมาตรฐาน คือได้มีการกำหนดถึงการรับรองความไว้ใจในการส่งผ่านข้อมูล
- **Layer 5: Application** ในชั้นที่ 5 จะสอดคล้องกับชั้นที่ 6 และชั้นที่ 7 ของโมเดลการลำดับชั้นที่เป็นมาตรฐานโดยโปรโตคอลแต่ละตัวจะระบุถึงแอปพลิเคชั่นต่าง ๆ (Applications) ที่จะใช้ในอินเตอร์เน็ต

โปรโตคอลที่อยู่ในชั้นอินเตอร์เน็ตจะประกอบด้วยโปรโตคอลหลายตัวเช่น ไอพี ไอซีเอ็มพี (ICMP: Internet Control Message Protocol) โปรโตคอลเกตเวย์ (Gateway Protocol) ฯลฯ แต่ในเนื้อหาจะกล่าวถึงไอพีเพียงอย่างเดียวเท่านั้น



ภาพที่ 2.2 หมายเลขเครื่องอินเตอร์เน็ตทั้ง 5 ประเภท

2.1.2 ไอพี

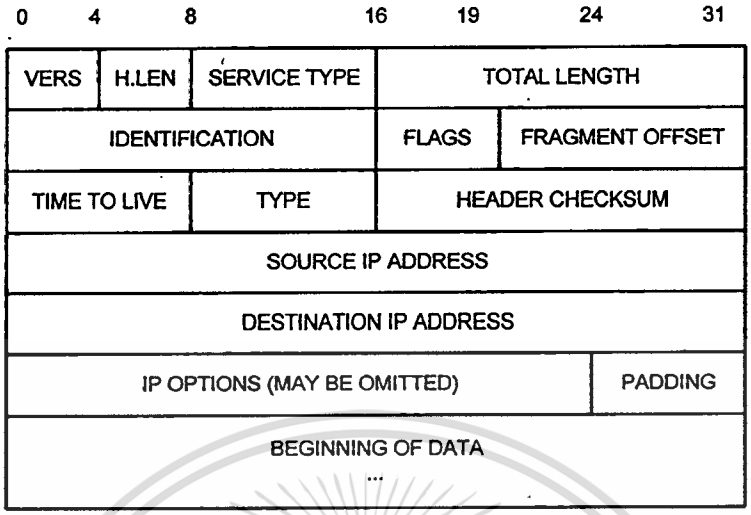
ไอพีเป็นโปรโตคอลระหว่างเครือข่าย (Internetworking Protocol) ที่ถูกพัฒนาโดยกระทรวงกลาโหมของสหรัฐอเมริกา ระบบต่าง ๆ ได้ถูกพัฒนาให้เป็นส่วนหนึ่งของโครงการดาร์ปาอินเตอร์-เน็ตเวิร์คโปรโตคอล (DARPA internetwork protocol) ซึ่งเป็นระบบที่มีการใช้อย่างทั่วโลก

- **การทำงานของส่วนไอพี**

เนื่องจากไอพีคือขั้นตอนของการส่งข้อมูลระหว่างเครื่องในเครือข่าย จะมีหมายเลขเครื่องในระบบอินเตอร์เน็ต (Internet Address) ซึ่งเป็นตัวกำหนดว่าจะส่งข้อมูลไปที่ส่วนใดในเครือข่าย ลักษณะของหมายเลขเครื่องในระบบอินเตอร์เน็ตแต่ละหมายเลขมีขนาด 32 บิต และได้มีการแบ่งหมายเลขออกเป็น 2 ส่วนคือส่วนที่เป็นหมายเลขเครือข่าย (Prefix) และส่วนของหมายเลขประจำเครื่อง (Suffix)

ส่วนของหมายเลขเครือข่ายจะถูกกำหนดโดยหน่วยงาน interNIC เพื่อไม่ให้มีการซ้ำซ้อนกัน ส่วนหมายเลขประจำเครื่องเป็นเลขที่กำหนดโดยผู้บริหารเครือข่ายให้กับเครื่องคอมพิวเตอร์ที่อยู่ภายในเครือข่าย

แต่ละหมายเลขที่ปรากฏก็จะเป็นอย่างใดอย่างหนึ่งใน 5 ประเภท ซึ่งแต่ละประเภทก็จะต่างกันที่ขนาดของหมายเลขเครื่องและหมายเลขประจำเครื่องนั่นเอง ในภาพที่ 2.2 จะแสดงหมายเลขเครื่องในระบบอินเตอร์เน็ตทั้ง 5 ประเภท และไอพีได้กำหนดไอพีดาต้าแกรม ซึ่งหน่วยพื้นฐานสำหรับการส่งผ่านข้ามไปมาในโปรโตคอลทีซีพี/ไอพี ดังแสดงในภาพที่ 2.3 (Comer:1997)



ภาพที่ 2.3 รูปแบบของไอพีดาต้าแกรม

โปรโตคอลในชั้นทรานสปอร์ตมีอยู่หลายโปรโตคอล โปรโตคอลที่เราสนใจคือ ทีซีพีและยูดีพี โดยที่ทีซีพีเป็นการติดต่อสื่อสารแบบมีการเชื่อมต่อ (Connection-oriented) และยูดีพีเป็นการติดต่อสื่อสารแบบไม่มีการเชื่อมต่อ (Connectionless)

2.1.3 ทีซีพี

โปรโตคอลทีซีพีจะกำหนดช่วงเวลาสำหรับการติดต่อเพื่อยืนยันการส่ง-รับข้อมูลระหว่างคอมพิวเตอร์ทั้ง 2 เครื่อง ทำให้โปรโตคอลทีซีพีเป็นโปรโตคอลที่มีความน่าเชื่อถือ (Reliable) เพราะให้ความแน่นอนว่าแพ็คเก็ตข้อมูลที่ถูกส่งออกไปจากต้นทางจะไปถึงยังปลายทางอย่างเป็นลำดับ และไม่มีความผิดพลาด หรือความสูญหายของข้อมูล ดังนั้นโปรโตคอลทีซีพีเป็นโปรโตคอลสำหรับควบคุมการสื่อสาร กำหนดตำแหน่งต้นทางและปลายทาง และอื่น ๆ กับข้อมูล

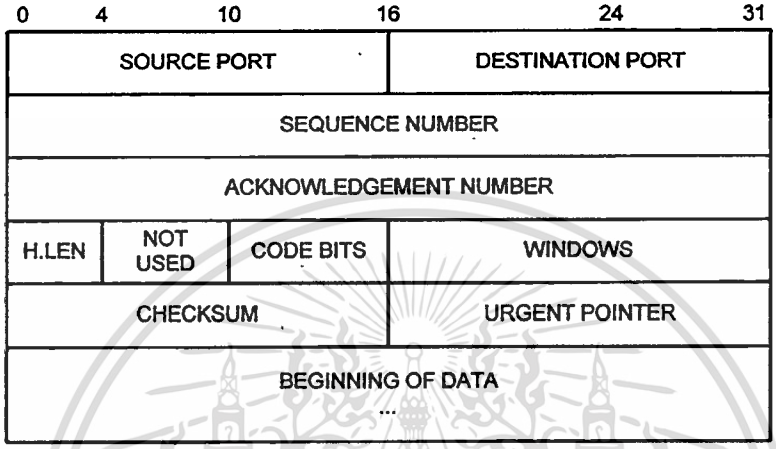
- **การทำงานของทีซีพี**

ขั้นตอนของทีซีพีจะเป็นส่วนการทำงานภายในคอมพิวเตอร์แต่ละเครื่อง มีหน้าที่ทำให้แน่ใจว่าไม่มีความผิดพลาดของข้อมูลที่ได้รับ ลำดับของข้อมูลถูกต้อง ครบถ้วนและไม่ซ้ำ

แอปพลิเคชั่นที่ต้องการส่งข้อมูล จะส่งข้อมูลมาให้ทีซีพีเพื่อตัดแบ่งข้อมูลออกเป็นส่วน ๆ เรียกว่า "เซ็กเม้นต์" (Segment) เพื่อไม่ให้ข้อมูลมีขนาดยาวเกินไป จากนั้นก็จะส่งข้อมูลแต่ละส่วนให้กับไอพีเพื่อสร้างชุดข้อมูลที่จะส่งให้กับเครือข่าย

ทีซีพีจะต้องทำกระบวนการรับ-ส่งข้อมูลพร้อมกัน ในขั้นตอนของการรับข้อมูลของทีซีพีจะต้องมีการส่งการตอบรับ (Acknowledge) แจ้งให้ผู้ส่งข้อมูลทราบว่าได้รับข้อมูลที่ถูกต้องมากี่ส่วนแล้ว ถ้าเครื่องที่ส่งข้อมูลยังไม่ได้รับการตอบรับภายในเวลาที่กำหนดทีซีพีก็จะส่งข้อมูลซ้ำออกไปอีก ทำให้มีบางครั้งข้อมูลชุดเดียวกันถูกส่งมามากกว่า 1 ครั้ง

เนื่องจากมีการแบ่งข้อมูลออกเป็นส่วน ๆ ข้อมูลแต่ละส่วนอาจจะใช้เวลาเดินทางไม่เท่ากัน ข้อมูลที่มาถึงจึงไม่เรียงลำดับกัน ทีซีพีจะทำการจัดลำดับข้อมูลให้ถูกต้อง ตัดข้อมูลที่ซ้ำซ้อน รวบรวมข้อมูลจนได้ครบทุกส่วนแล้วจึงส่งให้แอปพลิเคชั่นที่จะใช้ข้อมูลนั้นอีกทีหนึ่ง (Comer:1995)

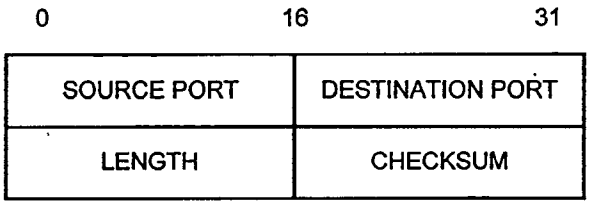


ภาพที่ 2.4 รูปแบบของเซ็กเม้นต์

2.1.4 ยูดีพี

โปรโตคอลยูดีพีคือโปรโตคอลที่ทำหน้าที่ควบคุมการส่ง-รับข้อมูลโดยไม่มีการรอดอยการยืนยันการตอบรับข้อมูลจากปลายทาง ทำให้การบริการแบบนี้ให้ความน่าเชื่อถือน้อยกว่า แต่ก็ทำให้การสื่อสารข้อมูลรวดเร็วยิ่งขึ้นถ้าไม่มีความผิดพลาดเกิดขึ้นในการส่ง-รับข้อมูล (Comer:1995)

ในลำดับชั้นตามภาพที่ 2.1 ยูดีพีจะอยู่เหนือไอพีเนื่องจากยูดีพีเป็นการสื่อสารแบบไม่มีการเชื่อมต่อ และยูดีพีจะเพิ่มความสามารถในการหาที่อยู่ของพอร์ต (Port) ให้กับไอพีโดยจะพิจารณาที่ส่วนหัวของยูดีพีดังแสดงในภาพที่ 2.5



ภาพที่ 2.5 รูปแบบของฟิลด์ในยูดีพีดาต้าแกรม

2.2 ไฟร์วอลล์

ไฟร์วอลล์เป็นกระบวนการกรองการจราจรทั้งหมดระหว่างเครือข่ายภายในที่ต้องการป้องกันกับเครือข่ายภายนอกที่ให้ความน่าเชื่อใจได้น้อย

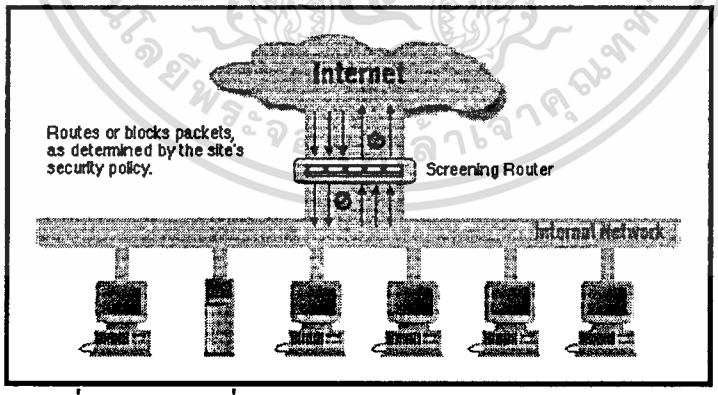
วัตถุประสงค์ของไฟร์วอลล์คือ เพื่อป้องกันอันตรายจากภายนอกที่จะเข้ามายังสิ่งแวดล้อมที่ถูกป้องกันไว้ โดยไฟร์วอลล์นี้จะอิมพลิเม็นต์นโยบายความปลอดภัยเพื่อใช้ในการป้องกันการเข้าถึงทั้งจากภายนอกเข้าภายในและจากภายในออกไปยังภายนอก หรืออาจอนุญาตให้เข้าถึงได้เฉพาะที่เฉพาะบุคคล และเฉพาะกิจกรรมเท่านั้น

2.2.1 ประเภทของไฟร์วอลล์

ในปัจจุบันนี้มีไฟร์วอลล์ 2 ประเภทที่นิยมใช้กันมากบนอินเตอร์เน็ตคือ การกรองแพ็คเก็ต (Packet Filtering) และการบริการทำงานแทน (Proxy Services)

ก. การกรองแพ็คเก็ต

การกรองแพ็คเก็ตเป็นวิธีการเลือกแพ็คเก็ตจากเครือข่ายภายนอกที่จะเข้ามาสู่เครือข่ายภายใน โดยแต่ละแพ็คเก็ตอาจได้รับอนุญาตให้เข้ามาได้หรืออาจถูกบล็อค ขึ้นอยู่กับนโยบายความปลอดภัยที่มีการสร้างไว้ และการกรองแพ็คเก็ตที่อยู่บนเราท์เตอร์จะเรียกว่า "แพ็คเก็ตฟิลเตอร์ริ่งเราท์เตอร์" (Packet Filtering Router) หรืออาจจะเรียกว่า "สกรีนนิ่งเราท์เตอร์" (Screening Router) ซึ่งแสดงได้ดังภาพที่ 2.6



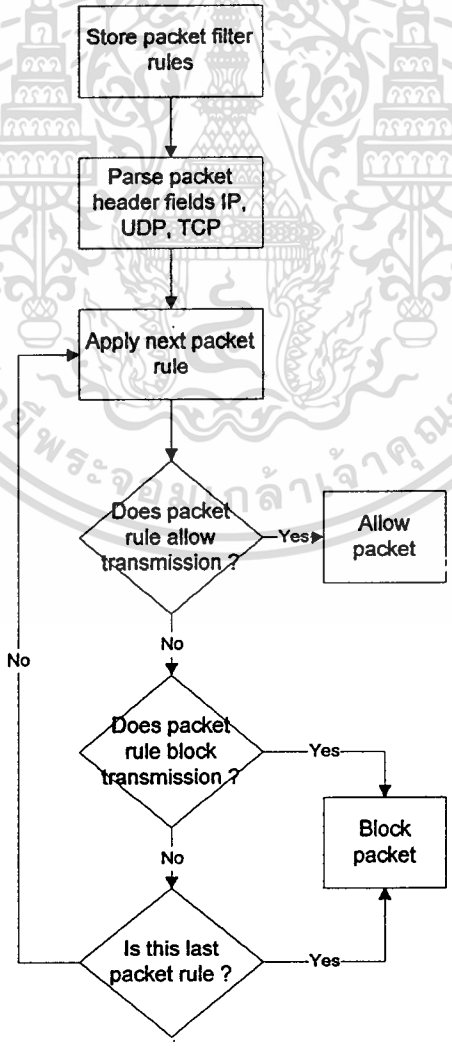
ภาพที่ 2.6 การใช้สกรีนนิ่งเราท์เตอร์เพื่อทำการกรองแพ็คเก็ต

- **ขั้นตอนการทำงานของการกรองแพ็คเก็ตในอุปกรณ์เราท์เตอร์ มีดังนี้**

1) เงื่อนไขของการกรองแพ็คเก็ตสำหรับพอร์ตของอุปกรณ์เราท์เตอร์จะต้องถูกเก็บไว้ ซึ่งเงื่อนไขของการกรองแพ็คเก็ตจะเรียกว่า "กฎของการกรองแพ็คเก็ต" (Packet filter rules)

2) เมื่อแพ็คเก็ตเข้ามายังพอร์ต ส่วนหัวของแพ็คเก็ตจะถูกกระจายออก ซึ่งอุปกรณ์เราท์เตอร์ส่วนใหญ่ที่กรองแพ็คเก็ตจะพิจารณาฟิล์ดเฉพาะในส่วนหัวของไอพี ทีซีพี และยูดีพีเท่านั้น
3) กฎของการกรองแพ็คเก็ตที่ถูกเก็บไว้ จะมีการระบุถึงลำดับ ทำให้แต่ละกฎตรวจสอบแต่ละแพ็คเก็ตอย่างเป็นลำดับด้วย
4) ถ้ากฎเป็นการบล็อกการส่งผ่านหรือการบล็อกการรับแพ็คเก็ตเข้ามา แสดงว่าแพ็คเก็ตนั้นไม่ได้รับอนุญาต
5) ถ้ากฎเป็นการอนุญาตให้ส่งผ่านหรือการอนุญาตให้รับแพ็คเก็ตเข้ามา แสดงว่าแพ็คเก็ตนั้นได้รับอนุญาตให้กระทำต่อไปได้
6) ถ้าแพ็คเก็ตไม่เข้าคู่กับกฎใด ๆ เลย แพ็คเก็ตนั้นจะถูกบล็อก

จากขั้นตอนการทำงานของการกรองแพ็คเก็ต สามารถแสดงได้ด้วยโฟล์วชาร์ทดังภาพที่ 2.7

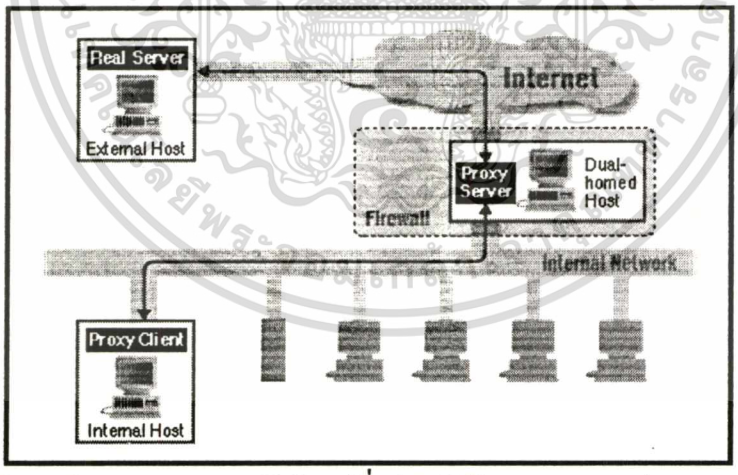


ภาพที่ 2.7 โฟล์วชาร์ทการทำงานของการกรองแพ็คเก็ต

ข. การบริการทำงานแทน

การบริการทำงานแทนเป็นแอปพลิเคชั่นที่ทำขึ้นมาเฉพาะหรือเป็นโปรแกรมของเซิร์ฟเวอร์ (Server Program) ที่ทำงานอยู่บนโฮสต์ที่เป็นไฟร์วอลล์ (Firewall Host) เรียกว่า "พร็อกซี่บริการ" โดยที่พร็อกซี่บริการจะตั้งอยู่ระหว่างผู้ใช้ที่อยู่ในเครือข่ายภายในและการบริการอินเตอร์เน็ตที่อยู่ภายนอก และแทนที่ผู้ใช้กับการบริการดังกล่าวจะติดต่อกันโดยตรง ก็จะติดต่อกับพร็อกซี่แทน ดังนั้นพร็อกซี่จะทำหน้าที่ดูแลการติดต่อสื่อสารทั้งหมดระหว่างผู้ใช้กับการบริการอินเตอร์เน็ตเช่น ไฟล์ทรานส์เฟอร์ (FTP) หรือ เทลเน็ต (Telnet)

จากภาพที่ 2.8 แสดงการทำงานของพร็อกซี่บริการบนเครื่องโฮสต์ที่เป็นไฟร์วอลล์ ซึ่งจะเรียกเครื่องดังกล่าวว่าเป็น "ดูอัลโฮมโฮสต์" (Dual-homed Host) โดยที่พร็อกซี่เซิร์ฟเวอร์จะเป็นตัวแทนของเครื่องเซิร์ฟเวอร์จริง สามารถที่จะติดต่อกับผู้ใช้ผ่านตัวแทนโฮสต์ที่เป็นเครื่องไคล์เอนต์ซึ่งเรียกว่า "พร็อกซี่ไคลเอนต์" โดยพร็อกซี่ทั้งสองนี้ต่างก็เป็นตัวแทนของทั้งเครื่องไคล์เอนต์และเครื่องเซิร์ฟเวอร์ สามารถที่จะติดต่อกันได้ แต่ว่าการที่จะติดต่อออกไปยังเครือข่ายภายนอก พร็อกซี่เซิร์ฟเวอร์จะทำหน้าที่แทนพร็อกซี่ไคลเอนต์อีกทีหนึ่ง ดังนั้นพร็อกซี่เซิร์ฟเวอร์สามารถที่จะตัดสินใจในการอนุญาตหรือปฏิเสธการร้องขอที่มาจากเครือข่ายภายนอกได้



ภาพที่ 2.8 การใช้การบริการทำงานแทนกับโฮสต์ที่เป็นดูอัลโฮม

2.3 ระบบปฏิบัติการฟรีบีเอสดี

ฟรีบีเอสดีเป็นระบบปฏิบัติการยูนิกต์ที่สามารถทำงานบนเครื่องพีซีตั้งแต่ตระกูล 386 ขึ้นไป และระบบปฏิบัติการนี้ถูกพัฒนาจากกลุ่มคนที่ทำงานวิจัยของคณะวิทยาศาสตร์คอมพิวเตอร์ของมหาวิทยาลัยเบอร์กเลย์ที่แคลิฟอร์เนีย (University of California, Berkeley: UCB)

ฟรีบีเอสดีได้มีการพัฒนามาตั้งแต่เวอร์ชัน 1.0 (ธันวาคม 2536) ปัจจุบันนี้เวอร์ชันล่าสุดของฟรีบีเอสดีคือ เวอร์ชัน 4.0 (มีนาคม 2543) แต่ในโครงงานจะใช้เวอร์ชัน 3.2

ความสามารถของฟรีบีเอสดีที่ผู้ใช้จะได้รับคือ การเพิ่มการเข้าถึงเคอร์เนลของมันเอง การอนุญาตให้ผู้ใช้เปลี่ยนแปลงพฤติกรรมแรก ๆ ได้ และอนุญาตให้ดูแลการติดต่อสื่อสารเองได้ และสิ่งที่สำคัญมากคือ มีการพัฒนาไฟร์วอลล์อยู่ในฟรีบีเอสดี (Lehey:1996)

บนระบบปฏิบัติการฟรีบีเอสดีจะมีการใช้งานในลักษณะของเท็กซ์โหมด แต่ผู้ใช้ก็สามารถจะติดตั้งลักษณะการทำงานแบบกราฟฟิกเข้าไปได้ โดยใช้ระบบเอ็กซ์วินโดว์ที่เรียกว่า "เอ็กซ์ฟรี86" (XFree86) ที่สามารถติดต่อกับผู้ใช้เป็นแบบกราฟฟิก (Graphic User Interface: GUI) ทำให้ผู้ใช้สามารถใช้งานได้สะดวกขึ้น

2.3.1 X-Window System

ระบบเอ็กซ์วินโดว์หรือที่เรียกสั้น ๆ ว่า เอ็กซ์ (X) เป็นระบบวินโดว์แบบกราฟฟิคบนเครือข่าย ที่ถูกพัฒนาโดย MIT ในปี ค.ศ. 1984 และได้พัฒนาจนกลายเป็นมาตราฐานทางอุตสาหกรรม เวอร์ชันของเอ็กซ์ได้ถูกพัฒนามาเรื่อย ๆ ล่าสุดคือ เวอร์ชัน 11 (X11) และในปี ค.ศ. 1987 ก็มีรีลีส (Release) แรกออกมา ปัจจุบันนี้รีลีสล่าสุดคือ X11R6 ("XFree86™:Home Page":2000)

2.3.2 เครื่องมือในการรักษาความปลอดภัยในฟรีบีเอสดี (Security Tools in FreeBSD)

ฟรีบีเอสดีจะให้คุณลักษณะที่ไม่มีอยู่ในระบบปฏิบัติการยูนิกต์แบบอื่น ๆ และบางคุณลักษณะทั่ว ๆ ไปจะมีอยู่ในตระกูลบีเอสดีต่าง ๆ และลีนุกซ์ (Linux) ซึ่งคุณลักษณะดังกล่าวมีดังนี้

- **System Security Levels** ระดับความปลอดภัยของระบบที่เพิ่มขึ้นจะป้องกันการกระทำต่าง ๆ ของระบบที่ไม่มีการจำกัดสิทธิพิเศษของผู้ใช้ ทำให้สามารถป้องกันระบบที่อันตรายได้ เช่นการเข้ามาของ Trojan horses และการเข้าทางประตูหลังเพื่อเข้ามายัง Binary system และทำการแก้ไขไฟล์โครงร่าง (Configuration file) ระดับความปลอดภัยของระบบแสดงอยู่ในตารางที่ 2.1

ตารางที่ 2.1 ระดับความปลอดภัยของระบบฟรีบีเอสดี

Level	Mode
-1	Permanently Unsecure
0	Unsecure
1	Secure
2	High Secure
3	Extended Secure

- **ไอพีไฟร์วอลล์** ส่วนของเคอร์เนลที่มีชื่อว่า "ไอพีไฟร์วอลล์" ของฟรีบีเอสดีได้มีการนำกฎการกรองมาใช้กับไอพีแพ็คเก็ต (IP Packet) การทำงานคือจะครอปไอพีแพ็คเก็ตที่ไม่ได้รับอนุญาตออกไป และจะอนุญาตให้แพ็คเก็ตที่ได้รับการอนุญาตเข้ามาเท่านั้น รวมถึงการใช้กฎการกรองกับตัวระบบ เพื่อให้ใช้กฎในการตัดสินใจถึงการยอมรับหรือไม่ยอมรับไอพีแพ็คเก็ตนั้นและรายละเอียดอื่น ๆ จะกล่าวในส่วนถัดไป
- **One-Time Passwords** เป็นป้องกันการนำรหัสผ่านกลับมาใช้อีก ซึ่งวิธีการนี้จะทำให้การใช้รหัสผ่านใช้ได้เพียงเดียวเท่านั้น เมื่อต้องการล็อกอิน (Log in) เข้ามาใหม่ก็ต้องใช้รหัสผ่านอันใหม่ ตัวอย่างเช่นการล็อกอินเข้ามาเพื่อ Telnet หรือ FTP ข้ามเครือข่ายอินเตอร์เน็ตของผู้ใช้อาจจะมีการแนะนำให้ใช้ระบบรหัสผ่านครั้งเดียว (One-Time Passwords) สำหรับการล็อคอินจากรีโมท์ไซต์ (Remote Site) เพื่อป้องกันการขโมยรหัสผ่าน โดยจะหลีกเลี่ยงการนำรหัสผ่านกลับมาใช้อีกครั้ง ในระบบปฏิบัติการฟรีบีเอสดีใช้ซอฟต์แวร์ที่เรียกว่า "S\Key" ในการทำรหัสผ่านครั้งเดียว ซึ่งผู้ใช้สามารถติดตั้งระบบรหัสผ่านครั้งเดียวโดยใช้คำสั่ง **Keyinit**
- **Disallowing Logins** ถ้ารหัสผ่านถูกเปิดเผยแก่ขโมย จะทำให้ขโมยสามารถเข้าถึงบัญชีผู้ใช้ซึ่งจะเป็นอันตรายได้ ตัวอย่างโปรโตคอลที่ใช้เช่น Telnet และ FTP เป็นการนำภัยไปสู่ระบบและเครือข่ายใกล้เคียงได้

  ผู้ดูแลระบบสามารถจำกัดการเข้าใช้เทลเน็ตและไฟล์ทรานส์เฟอร์สำหรับผู้ใช้บางส่วนและไซต์ (Site) บางส่วนได้ โดยการแก้ไขที่ไฟล์ /etc/login.access ให้เหมาะสม ซึ่งตัวเลือกนี้สามารถลดความเป็นประโยชน์ของรหัสผ่านที่เป็นภัยได้ โดยการจำกัดการเข้าใช้ของไซต์ที่น่าสงสัยได้ ("FreeBSD Handbook":2000)

2.3 ไอพีไฟร์วอลล์ (Lehey:1996)

เนื่องจากโครงงานที่จะทำขึ้นมีความเกี่ยวข้องการรักษาความปลอดภัยในระบบปฏิบัติการฟรีบีเอสดีที่เรียกว่า "ไอพีไฟร์วอลล์" ดังนั้นในเนื้อหาส่วนหลังนี้จะกล่าวถึงรายละเอียดของไอพีไฟร์วอลล์ได้แก่ ความหมายและความสามารถในการทำงาน และเนื้อหาส่วนอื่นจะอธิบายเพิ่มเติมในบทที่ 3

ไอพีไฟร์วอลล์เป็นไฟร์วอลล์แบบกรองแพ็คเก็ต ที่จะจัดหาการควบคุมการเข้าถึงที่ระดับไอพีและระดับทรานสปอร์ตในโปรโตคอลทีซีพี/ไอพีดังภาพที่ 2.1 และอาจจะมีการอนุญาต (Allow)[1]

---

[1] Allow เป็นการกระทำที่อนุญาตให้แพ็คเก็ตที่เข้าคู่กับกฎผ่านเข้ามาได้ (Allow packets that match rule) และคำที่มีความหมายเหมือนกับ "Allow" คือ "Pass" "Permit" และ "Accept"

หรือการปฏิเสธ (Deny)[2] แพ็คเก็ตก็ได้ ขึ้นอยู่กับแอดเดรสต้นทาง แอดเดรสปลายทาง ชนิดของแอปพลิเคชั่นเป็นหลัก และอื่น ๆ โดยที่ไฟร์วอลล์แบบกรองแพ็คเก็ตนี้ได้จัดหาความปลอดภัยในระดับง่าย ๆ และมีประสิทธิภาพในการทำงานมาก

ไอพีไฟร์วอลล์ประกอบด้วยการกรองแพ็คเก็ตโดยไอพีไฟร์วอลล์จะอาศัยอยู่ในเคอร์เนล และมียูทิลิตี้ในการการควบคุมผู้ใช้ รวมถึงจะอนุญาตให้ผู้ใช้นิยามและสอบถามถึงกฎที่ใช้อยู่ในปัจจุบัน และมีอยู่ 2 ส่วนที่สัมพันธ์กับไอพีไฟร์วอลล์ คือส่วนของไฟร์วอลล์ และส่วนของการทำบัญชีของกฎ ในส่วนแรกจะอนุญาตให้ทำในส่วนของการกรองแพ็คเก็ต และส่วนที่สองจะอนุญาตให้จัดการเกี่ยวกับกฎความปลอดภัยของระบบ

- **ความสามารถของไอพีไฟร์วอลล์ (Enabling IPFW on FreeBSD)**

ไอพีไฟร์วอลล์เป็นบริการอย่างหนึ่งที่ซ่อนอยู่ในฟรีบีเอสดีและถูกนำมารวมอยู่ในเคอร์เนลทำให้สามารถดูแลและควบคุมการเปลี่ยนแปลงพฤติกรรมโดยรวมและการเปลี่ยนแปลงนโยบายทางด้านความปลอดภัยของการติดต่อสื่อสารที่ระดับไอพีได้ตลอดเวลา และสิ่งที่ได้จากการออกแบบไอพีไฟร์วอลล์คือ สามารถใช้ไอพีไฟร์วอลล์บนเครื่องที่ไม่ใช่เราท์เตอร์ได้

ถึงแม้ว่าไอพีไฟร์วอลล์เป็นเวอร์ชันที่ง่ายมากและเป็นพื้นฐานของไฟร์วอลล์แบบกรองแพ็คเก็ต มันก็สามารถใช้แก้ไขกลุ่มของกฎก่อนที่จะจำกัดการเข้ามาได้ และสามารถเพิ่มกฎเข้าไปได้ แต่ว่ามันไม่สามารถแสดงรายละเอียดของเหตุการณ์ของการล็อคและไม่สามารถวิเคราะห์การติดต่อสื่อสารที่เลยช่วงเวลานั้นมาแล้วได้ เนื่องจากการควบคุมที่นอกเหนือจากไอพีไฟร์วอลล์จะอนุญาตให้เพียงผู้ใช้พิเศษเท่านั้นที่ทำได้

เป็นที่ทราบว่าส่วนหลัก ๆ ของไอพีไฟร์วอลล์จะอยู่ในเคอร์เนล ดังนั้นถ้าผู้ใช้ต้องการเพิ่มตัวเลือก (Option) ในไฟล์โครงร่างของเคอร์เนลของผู้ใช้ หลังจากนั้นจะต้องทำการคอมไพล์เคอร์เนลอีกครั้ง

ตัวอย่างเมื่อมีการขยายกลุ่มของกฎออกไป ทำให้การจำกัดแพ็คเก็ตถูกระบุมากขึ้น และทำให้การบันทึกแพ็คเก็ตบางส่วนถูกปิดลง เนื่องจากมีการเปลี่ยนแปลงกฎ และถ้าต้องการบันทึกต่อไป จะต้องตั้งค่าตัวนับแพ็คเก็ตที่เกี่ยวข้องด้วยอีกครั้ง โดยใช้คำสั่งของไอพีไฟร์วอลลที่เรียกว่า "ipfw clear [rule no.]"

แต่ละแพ็คเก็ตที่ถูกส่งออกไปและที่รับเข้ามาจะต้องมาจากการผ่านกฎของไอพีไฟร์วอลล์ แต่ละแพ็คเก็ตสามารถที่จะกรองได้ จะต้องสอดคล้องกับข้อมูลดังต่อไปนี้

- Receive Interface เป็นอินเตอร์เฟสที่จะรับแพ็คเก็ตเข้ามา

---

[2] Deny เป็นการกระทำที่ลบแพ็คเก็ตที่เข้าคู่กับกฎออกไป (Discard packets that match this rule) และคำที่มีความหมายเหมือนกับ "Deny" คือ "Drop"

- Transmit Interface เป็นอินเตอร์เฟสที่จะส่งแพ็คเก็ตออกไป
- Incoming เป็นแพ็คเก็ตที่เพิ่งได้รับมา
- Outgoing เป็นแพ็คเก็ตที่จะต้องถูกส่งออกไป
- Source IP Address เป็นไอพีแอดเดรสของผู้ส่ง
- Destination IP Address เป็นไอพีแอดเดรสของผู้รับ
- Protocol เป็นไอพีโปรโตคอลที่ประกอบด้วยไอพี (IP) ยูดีพี (UDP) ทีซีพี (TCP) และไอซี-เอ็มพี (ICMP)
- Source port เป็นพอร์ตของยูดีพีหรือทีซีพีของผู้ส่ง
- Destination Port แพ็คเก็ตนี้เป็นพอร์ตของยูดีพีหรือทีซีพีของผู้รับ
- Connection Setup Flag แพ็คเก็ตนี้เป็นการร้องขอให้มีการจัดตั้ง TCP Connection
- Connection Established Flag แพ็คเก็ตนี้เป็นส่วนของการสร้าง TCP Connection
- All TCP Flags แพ็คเก็ตนี้เป็น TCP Flag ต่าง ๆ เช่นการปิดการติดต่อ(fin) การเปิดการติดต่อ (syn) การตั้งการติดต่อใหม่(rst) ฯลฯ
- Fragment Flag แพ็คเก็ตนี้เป็น Fragment ของไอพีแพ็คเก็ต
- IP Option แพ็คเก็ตนี้เป็น Option ต่าง ๆ ของไอพีเช่น Strict source route (ssrr) หรือ Loose source route (lsrr) เป็นต้น
- ICMP Types แพ็คเก็ตนี้เป็นชนิดต่าง ๆ ของไอซีเอ็มพีเช่น Echo reply(0) หรือ Destination unreachable(3) เป็นต้น

การกรองแพ็คเก็ตเป็นส่วนหนึ่งของไฟร์วอลล์ โดยหลักการนี้ถูกนำมาใช้ในไอพีไฟร์วอลล์ มีความสามารถคือ มีการระบุกฎหรือนโยบายของเครือข่าย โดยที่ในกฎจะมีการระบุถึงฟิลด์ที่สามารถกรองได้ (กรองแล้วมีประโยชน์) ประกอบด้วยแอดเดรสต้นทางและปลายทางของไอพี ชนิดของโปรโตคอล และพอร์ตต้นทางและปลายทางของทีซีพีและยูดีพี และอื่น ๆ

บทที่ 3

การพัฒนาระบบงาน

ในเนื้อหาส่วนหลังของบทที่ 2 ได้มีการอธิบายถึงไอพีไฟร์วอลล์มาบ้างแล้ว สำหรับในบทนี้จะกล่าวถึงเครื่องมือที่ใช้ในการพัฒนาระบบงาน การใช้คำสั่งของไอพีไฟร์วอลล์ การนำหลักการกรองแพ็คเก็ตมาใช้ในระบบงาน และโครงสร้างภายในโปรแกรม

3.1 เครื่องมือที่ใช้ในการพัฒนาระบบงาน

- Microsoft Word ใช้ในการผลิตเอกสารประกอบโครงงาน
- Visio และ Photoshop ใช้ในการวาดภาพประกอบเช่น โฟลว์ชาร์ท (Flow Chart) รูปภาพ และไดอะแกรม (Diagram)
- TCL/TK การพัฒนาโปรแกรมควบคุมไอพีไฟร์วอลล์ เพื่อให้ผู้ใช้ใช้งานฟังกชันของไอพีไฟร์วอลล์บนฟรีบีเอสดีได้สะดวกขึ้น ได้ถูกพัฒนาขึ้นมาจากภาษาทีซีแอลและการใช้ทูลคิด (Toolkit) ของทีซีแอล (Flynt:1999, Ousterhout:1994)

3.2 การเลือกโครงร่างของไอพีไฟร์วอลล์

ส่วนหลักของระบบไอพีไฟร์วอลล์อยู่ในเคอร์เนล ถ้าต้องการเพิ่มตัวเลือก 1 ตัวหรือมากกว่านั้นในไฟล์โครงร่างภายในเคอร์เนล จำเป็นต้องคอมไพล์เคอร์เนลอีกครั้ง เพื่อให้การทำงานต่าง ๆ ถูกต้อง

ในปัจจุบันมี 3 ตัวเลือกที่ใช้ในไอพีไฟร์วอลล์สำหรับการจัดโครงร่างเคอร์เนล

1) options IPFIREWALL เป็นการคอมไพล์ตัวเคอร์เนลให้สร้างโค้ดสำหรับกรองแพ็คเก็ต
2) options IPFIREWALL_VERBOSE เป็นโค้ดที่อนุญาตให้มีการบันทึก (Log) แพ็คเก็ตผ่านคำสั่ง syslogd(8) ถ้าไม่มีการใช้ตัวเลือกนี้ แล้วมีการระบุแพ็คเก็ตที่ควรจะถูกบันทึกในกฎการกรอง จะไม่มีอะไรเปลี่ยนแปลง
3) options IPFIREWALL_VERBOSE_LIMIT=10 เป็นการจำกัดจำนวนแพ็คเก็ตที่ถูกล็อกผ่านคำสั่ง syslogd(8) ต่อหนึ่งกฎ และอาจต้องใช้ตัวเลือกนี้ในสภาพแวดล้อมที่มีผู้รุกราน

3.3 การสร้างโครงร่างของไอพีไฟร์วอลล์ (The Configuration IP Firewall)

ไอพีไฟร์วอลล์โค้ดจะทำงานโดยที่แต่ละแพ็คเก็ตจะต้องผ่านรายการของกฎจนกระทั่งพบกฎที่เข้าคู่ โดยที่กฎจะมีการเรียงลำดับด้วยเลขของบรรทัด (Line-number) คือตั้งแต่เลข 1 จนถึง 65534 และกฎทั้งหมดจะมีความสัมพันธ์กับตัวนับ 2 ตัวคือ ตัวนับแพ็คเก็ต (Packet counter) กับตัวนับไบต์ (Byte counter) โดยที่ตัวนับทั้ง 2 ตัวนี้จะถูกเปลี่ยนแปลงเมื่อแพ็คเก็ตนั้นเข้าคู่กับกฎ และเนื่องจากว่าไอพีไฟร์วอลล์เป็นไฟร์วอลล์แบบกรองแพ็คเก็ตที่ได้มีการสร้างกฎต่าง ๆ เอาไว้ในการจับคู่กับแพ็คเก็ตที่เข้ามายังเครือข่าย เพื่อตัดสินใจว่าแพ็คเก็ตใดสามารถให้ผ่านเข้ามาได้หรือผ่านเข้ามาไม่ได้ ดังนั้นการสร้างกฎจึงมีความสำคัญอย่างยิ่ง สิ่งที่จะต้องพิจารณาต่อไปจะเกี่ยวข้องกับการสร้างกฎซึ่งมี 4 อย่างคือ

- Addition/Deletion การเพิ่ม/ลบออกจะใช้ในการสร้างกฎเพื่อควบคุมแพ็คเก็ตที่เข้ามาว่าจะยอมรับหรือไม่ยอมรับแพ็คเก็ตนั้นไว้
- Listing การทำบัญชีของกฎจะใช้ในการพิจารณาถึงสารบาญของกลุ่มของกฎ (หรือที่เรียกว่า Chain) และตัวนับแพ็คเก็ต (Packet Counter)
- Flushing การเคลื่อนย้ายกฎที่เข้ามาทั้งหมดออกจากกลุ่ม
- Clearing การลบค่าที่ตัวนับแพ็คเก็ตให้เป็นศูนย์

หมายเหตุ: *การทำงานทั้ง 4 อย่างที่กล่าวมาจะอยู่ในโปรแกรมไอพีไฟร์วอลล์ที่มากับฟรีบีเอสดี*

3.3.1 รูปแบบคำสั่งของ Addition/Deletion

```
ipfw [-N] command [index] action [log] protocol address [options]
```

โดยที่...

- -N ใช้แยกส่วนของแอดเดรสและชื่อบริการต่าง ๆ ใน Output
- command เป็นคำสั่งซึ่งอยู่ในรูปแบบที่สั้นและไม่ซ้ำ ได้แก่
  - add เป็นการเพิ่มกฎในกลุ่มของกฎ
  - delete เป็นการลบกฎในกลุ่มของกฎ
- index เป็นการระบุตำแหน่งของกฎในกลุ่มของกฎ
- action ประกอบด้วย
  - allow เป็นการอนุญาตให้แพ็คเก็ตผ่านไปโดยปกติ
  - deny เป็นการดร็อปแพ็คเก็ต ดังนั้นแพ็คเก็ตจะไม่สามารถส่งไปยังต้นทางได้
  - reject เป็นการลบแพ็คเก็ตที่เข้าคู่กับกฎและจะส่งข้อความไปที่โฮสต์ไอซีเอ็มพีที่ไม่สามารถขยายต่อไปได้ (Unreachable)

- unreach code เป็นการลบแพ็คเก็ตที่เข้าคู่กับกฎและจะส่งข้อความไปที่โฮสต์ไอซีเอ็มพีที่ไม่สามารถขยายต่อไปได้ด้วยโค้ดซึ่งมีค่าตั้งแต่ 0-255
- reset จะใช้กับแพ็คเก็ตที่เป็นทีซีพีเท่านั้น โดยจะลบแพ็คเก็ตที่เข้าคู่กับกฎและจะส่งข้อความที่เป็นทีซีพีรีเซ็ท (TCP reset Message)
- count เป็นการปรับค่าตัวนับแพ็คเก็ต
- divert port จะทำการเบี่ยง (Divert) แพ็คเก็ตที่เข้าคู่กับกฎไปยังพอร์ตที่ระบุ
- tee port จะส่งการคัดลอกแพ็คเก็ตที่เข้าคู่กับกฎไปยังพอร์ตที่ระบุ

- log ทำให้เกิดการเข้าคู่กฎเพื่อไปแสดงผลที่คอนโซลระบบ (System console) ถ้าเคอร์เนลถูกคอมไพล์ด้วย options IPFIREWALL_VERBOSE
- protocol โปรโตคอลสามารถระบุได้ดังนี้
  - all เป็นการจับคู่กับทุกไอพีแพ็คเก็ต
  - icmp เป็นการจับคู่กับไอซีเอ็มพีแพ็คเก็ต
  - tcp เป็นการจับคู่กับทีซีพีแพ็คเก็ต
  - udp เป็นการจับคู่กับยูดีพีแพ็คเก็ต
- address แอดเดรสจะมีการระบุดังนี้

from address/mark[port] to address/mark[port] [via interface]

  - สามารถระบุพอร์ตที่เชื่อมกับโปรโตคอลที่สนับสนุนพอร์ตเช่น ทีซีพี ยูดีพี
  - "via" เป็นสิ่งที่เลือกได้และอาจจะมีการระบุไอพีแอดเดรสหรือชื่อโดเมนของอินเตอร์เฟสของไอพีอินเตอร์เฟสภายในหรือชื่ออินเตอร์เฟส เช่น ed0 เพื่อจับคู่เฉพาะแพ็คเก็ตที่ผ่านเข้ามาในอินเตอร์เฟสนี้
  - รูปแบบที่ใช้ในการระบุ address/mark มีดังนี้
    1) address ไอพีแอดเดรส
    2) address/mark-bits ไอพีแอดเดรสที่มีสับเน็ตมาร์ก (Sub-netmask) แบบย่อ
    3) address:mark-pattern ไอพีแอดเดรสที่มีสับเน็ตมาร์ก (Sub-netmask) แบบยาว
  - ตัวเลขของพอร์ตที่จะถูกบล็อกสามารถระบุได้ดังนี้
    1) port[,port[,port[…]]] เป็นการระบุถึงพอร์ตเพียงพอร์ตเดียวหรือระบุเป็นรายการของพอร์ต
    2) port-port เป็นการระบุช่วงของพอร์ต
- options ตัวเลือกที่สามารถใส่เข้าไปได้มีดังนี้
  - frag จะจับคู่ถ้าแพ็คเก็ตไม่ได้อยู่ใน fragment แรกของดาต้าแกรม

- in จะจับคู่ถ้าแพ็คเก็ตนั้นเป็นแพ็คเก็ตที่เข้ามา
- out จะจับคู่ถ้าแพ็คเก็ตนั้นเป็นแพ็คเก็ตที่ออกไป
- ipoptions spec จะจับคู่ถ้าส่วนหัวของไอพีมี comma separated list ของตัวเลือกที่ถูกระบุใน spec เช่น ssrr (strict source route)
- established จะจับคู่ถ้าแพ็คเก็ตนั้นเป็นส่วนของการจัดสร้างการเชื่อมต่อของทีซีพี
- setup จะจับคู่ถ้าแพ็คเก็ตนั้นเป็นแพ็คเก็ตที่พยายามจะจัดสร้างการเชื่อมต่อของทีซีพี
- tcpflags flags จะจับคู่ถ้าส่วนหัวของทีซีพีมี comma separated list ของ flags เช่น fin syn rst psh ack และ urg
- icmptypes types จะจับคู่ถ้าชนิดของไอซีเอ็มพีปรากฏอยู่ในรายการของ types

3.3.2 รูปแบบคำสั่งของ Listing

```
ipfw [-a][-t][-N] l
```

ในการทำรายการของกฎประกอบด้วย 3 ส่วนที่ใช้ในคำสั่งนี้คือ

-a ขณะที่ทำการแสดงรายการของกฎจะแสดงค่าของตัวนับ

-t แสดงการจับคู่กฎกับแพ็คเก็ตในครั้งสุดท้ายในแต่ละกฎ

-N การพยายามแยกส่วนของแอดเดรสและชื่อบริการต่าง ๆ

3.3.3 รูปแบบคำสั่งของ Flushing

```
ipfw flush
```

สิ่งต้องระวังเมื่อมีการใช้คำสั่งนี้คือ ค่าเริ่มต้นของนโยบายจะเป็นการปฏิเสธการบริการทุกอย่างในเครือข่ายจนกวาจะมีการเพิ่มกฎเข้าไป

3.3.4 รูปแบบคำสั่งของ Clearing

```
ipfw zero [index]
```

เมื่อการใช้คำสั่งนี้ไม่มีส่วนของ index จะทำให้ตัวนับแพ็คเก็ตทั้งหมดถูกลบค่าออกไปด้วย แต่ถ้ามีการระบุค่าใน index การลบค่าตัวนับแพ็คเก็ตจะกระทำเฉพาะกฎนั้น ๆ

3.4 ตัวอย่างการใช้คำสั่งของไอพีไฟร์วอลล์ในฟรีบีเอสดี

- การปฏิเสธแพ็คเก็ตทั้งหมดจากโฮสต์ที่ชื่อว่า evil.crackers.org เพื่อเทลเน็ตมาที่พอร์ตของโฮสต์ nice.people.org

```
# ipfw add deny tcp from evil.crackers.org to nice.people.org 23
```

- การปฏิเสธและล็อกทุกการจราจรของทีซีพีจากเครือข่าย crackers.org (Class C) เพื่อที่จะเข้ามายังเครื่อง nice.people.org ในทุกพอร์ต

  # ipfw add deny log tcp from evil.crackers.org/24 to nice.people.org

- การดูเรคคอร์ดของรายการของกฎ

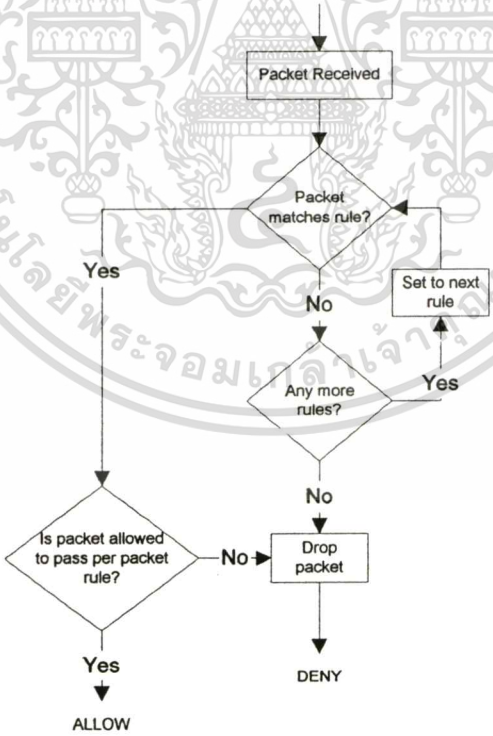
  # ipfw –a list หรือ # ipfw –a l

- การดูกฎที่เข้าคู่กับแพ็คเก็ตได้ในครั้งสุดท้าย

  # ipfw –at l

3.5 การทำงานของไอพีไฟร์วอลล์ในโครงงาน

การทำงานไอพีไฟร์วอลล์อยู่บนพื้นฐานของไฟร์วอลล์แบบกรองแพ็คเก็ต และการทำงานของโมดูลการกรองแพ็คเก็ตสามารถแสดงได้ดังภาพที่ 3.1 สำหรับภาพรวมการทำงานของโปรแกรมว่าจะนำไปใช้ ณ จุดใดสามารถแสดงได้ดังภาพที่ 3.2

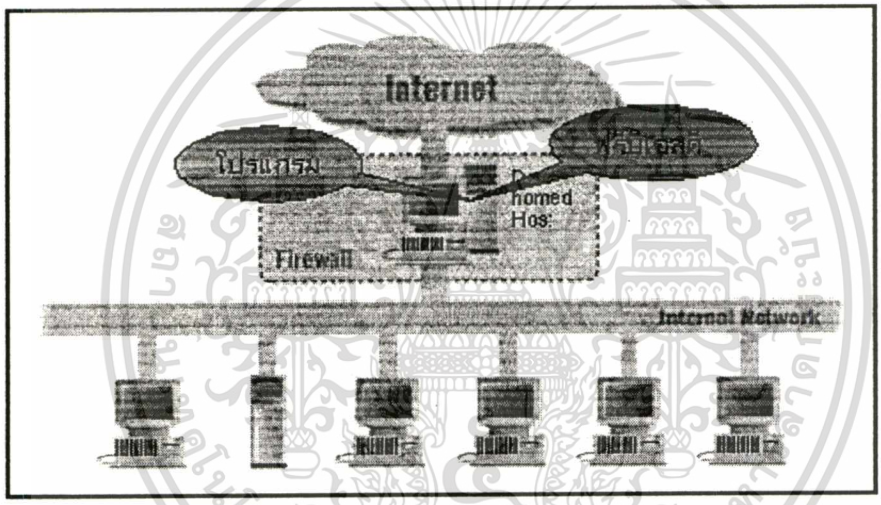


ภาพที่ 3.1 การกรองแพ็คเก็ตในระบบของโครงงาน

จากภาพที่ 3.2 จะเห็นว่าโปรแกรมที่ควบคุมไอพีไฟร์วอลล์จะอยู่ในฟรีบีเอสดีซึ่งทำงานอยู่ในสภาพแวดล้อมที่เป็นเอ็กซ์วินโดว์ และภายในโปรแกรมจะประกอบด้วยฟังก์ชัน 2 ฟังก์ชันหลัก

โดยที่ฟังก์ชันการทำงานต่าง ๆ นี้ผู้ใช้จะทำผ่านการติดต่อที่เป็นแบบกราฟฟิก กฎต่าง ๆ นี้จะถูกเก็บอยู่ในฐานข้อมูลของกฎ ทำให้ทุกครั้งที่ทำการปรับรายการของกฎให้เป็นปัจจุบัน ก็จะไปทำการปรับปรุงฐานข้อมูลอันนี้ด้วย เพื่อรักษาความสม่ำเสมอระหว่างการติดต่อทางหน้าจอกับฐานข้อมูลที่เก็บกฎให้คงที่ (Consistency) สำหรับการปรับรายการของกฎให้เป็นปัจจุบันก็จะมีการปรับทุกครั้งที่มีการเปลี่ยนแปลงกฎ ได้แก่ การเพิ่มและการลบกฎ เป็นต้น

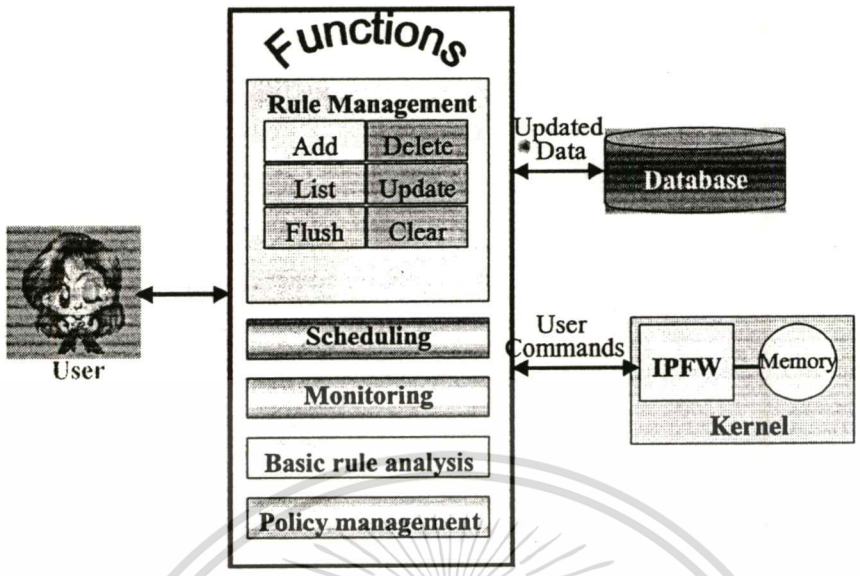
ดังนั้นเมื่อมีแพ็คเก็ตเข้ามาในโมดูลของการกรองแพ็คเก็ต แพ็คเก็ตเหล่านั้นก็จะถูกตรวจสอบด้วยกฎที่มีทั้งหมด และถ้าแพ็คเก็ตเหล่านั้นเข้าคู่กับกฎ โดยกฎจะแบ่งออกเป็นการอนุญาตกับการปฏิเสธ



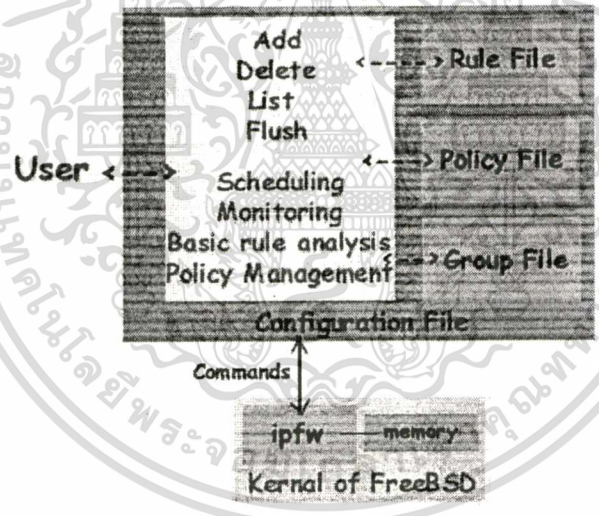
ภาพที่ 3.2 ภาพโดยรวมของโปรแกรม

ถ้าแพ็คเก็ตนั้นเข้าคู่กับกฎการปฏิเสธแพ็คเก็ตนั้นก็จะถูกลบออกไป ถ้าแพ็คเก็ตนั้นเข้าคู่กับกฎการอนุญาตแพ็คเก็ตนั้นก็จะผ่านเข้ามาได้ การทำงานจะเป็นไปตามโฟลว์ชาร์ทในภาพที่ 3.1

ฟังก์ชันที่อาจมีเพิ่มเติมอย่างเช่น การตั้งเวลาการกรองแพ็คเก็ตในช่วงที่สามารถกำหนดเองได้ โดยจัดทำเป็นตารางการทำงานของการกรองว่าจะให้ทำการกรอง ณ ช่วงเวลาใด หรืออาจจะเป็นฟังก์ชันที่เกี่ยวกับการวิเคราะห์สถิติของแพ็คเก็ตที่เข้ามาว่าแพ็คเก็ตชนิดไหนที่มีเข้ามามากที่สุดและเข้ามาในช่วงไหนเป็นต้น และโครงสร้างการทำงานของโปรแกรมที่จะสร้างขึ้นจะแสดงได้อยู่ในภาพที่ 3.3



ภาพที่ 3.3 โครงสร้างภายในโปรแกรม (1)



ภาพที่ 3.4 โครงสร้างภายในโปรแกรม (2)

จากภาพที่ 3.3 จะเห็นได้ว่าผู้ใช้สามารถใช้งานโปรแกรมเป็นกราฟฟิกเปรียบเสมือนกับเป็นส่วนหน้า (Front-end) ส่วนการประมวลผลของโปรแกรมจะทำงานอยู่ด้านหลัง (Back-end) โดยจะมีการส่งคำสั่งไปกระทำแทน เมื่อไอพีไฟร์วอลล์ถูกสั่งให้กระทำคำสั่งต่าง ๆ เช่น การเพิ่มกฎ กฎที่เพิ่มเข้าจะถูกบันทึกไปที่ไฟล์ที่มันเก็บกฎนั้นอยู่ และกฎนี้จะถูกบันทึกอยู่ในฐานข้อมูลของกฎด้วยเช่นกัน และในส่วนของการออกแบบฐานข้อมูลของกฎจะกล่าวในบทต่อไป

บทที่ 4

การออกแบบระบบงาน

สำหรับรายละเอียดในการออกแบบระบบงานได้มีการออกแบบฟังก์ชันการทำงาน ทั้งแบบฟังก์ชันการทำงานทั่วไปและการทำงานที่เพิ่มเติม ตัวอย่างการสร้างกฎต่าง ๆ การออกแบบฐานข้อมูลที่จะเก็บกฎ นโยบาย และกลุ่ม รวมทั้งการออกแบบอินเตอร์เฟสที่ใช้ในการติดต่อกับผู้ใช้ซึ่งก็คือหน้าต่างหลักที่ใช้งานได้แก่ หน้าจอของเมนูและของแต่ละฟังก์ชัน

4.1 การออกแบบฟังก์ชันการทำงานต่าง ๆ

การออกแบบฟังก์ชันแบ่งได้เป็น 2 ส่วนคือส่วนของการทำงานทั่วไปตามที่ไอพีไฟร์วอลล์ได้จัดหาไว้ให้ และส่วนการทำงานที่เพิ่มเติมเพื่อเสริมการทำงานทั่วไป

4.1.1 ฟังก์ชันการทำงานทั่วไป

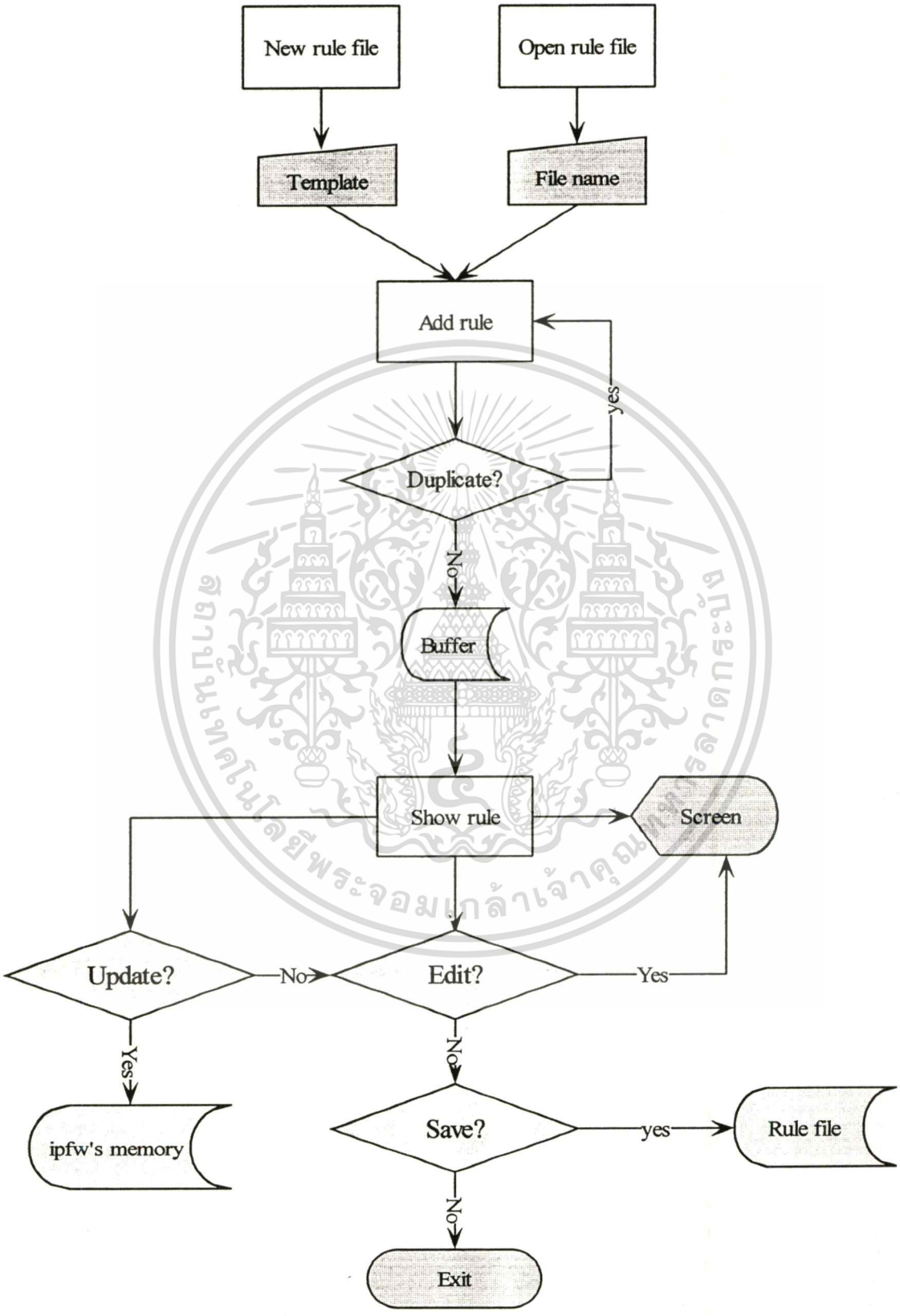
- Add การการเพิ่มกฎใหม่เข้าไปแบ่งเป็น 2 กรณี คือการสร้างไฟล์กฎใหม่ (New rule file) และการเรียกใช้ไฟล์กฎที่มีอยู่เดิมขึ้นมาแก้ไข (Open rule file)

กรณีที่ 1 – การสร้างไฟล์กฎใหม่มี 4 ขั้นตอน

1) ต้องมีการสร้างที่ว่างสำหรับไฟล์กฎที่กำลังจะถูกสร้างขึ้น
2) เลือกคำสั่ง “Add rule” จากเมนูในหมวดของการแก้ไข (Edit menu)
3) เมื่อเปิดหน้าต่างของการ Add rule แล้วทำการสร้างกฎ กฎที่ถูกสร้างจะปรากฏบนที่ว่างที่ได้เตรียมไว้
4) เมื่อทำการสร้างกฎจนเป็นที่ต้องการแล้ว ให้เลือกคำสั่งของการจัดเก็บไฟล์ (Save file)

กรณีที่ 2 – การเรียกใช้ไฟล์กฎที่มีอยู่เดิมขึ้นมาแก้ไขมี 4 ขั้นตอน

1) เมื่อเรียกใช้คำสั่ง Open rule file ให้ทำการเลือกชื่อไฟล์กฎที่ต้องการขึ้นมาเพื่อทำการแก้ไข
2) รายการของกฎในไฟล์กฎที่ถูกเรียกจะปรากฏบนที่ว่างที่ได้เตรียมไว้ เพื่อให้ผู้ใช้สามารถตรวจดูรายการของกฎดังกล่าวได้
3) ทำการเพิ่มรายการของกฎเข้าไป โดยใช้คำสั่ง Add rule
4) เมื่อทำการเพิ่มกฎจนเป็นที่ต้องการแล้ว ให้เลือกคำสั่งของการจัดเก็บไฟล์



ภาพที่ 4.1 การทำงานของการเพิ่มกฎ

รูปแบบและตัวอย่างของการ Add rule

1) การใช้โปรโตคอลไอพี (IP) เป็นคีย์สำหรับการกรอง

```
ipfw add [rule no.] allow ip from $SourceAddr to $DestAddr [options]
ipfw add [rule no.] deny ip from $SourceAddr to $DestAddr [options]
ipfw add [rule no.] divert [port] ip from $SourceAddr to $DestAddr [options]
```

ภาพที่ 4.2 รูปแบบการสร้างกฎโดยใช้โปรโตคอลไอพี

ตัวอย่าง

ipfw add 00001 allow ip from 192.168.0/24 to any via ed1 out

ipfw add 00002 deny ip from any to any

ipfw add 00003 divert natd ip from any to any via tun0

2) การใช้โปรโตคอลทีซีพี (TCP) เป็นคีย์สำหรับการกรอง

```
ipfw add [rule no.] allow tcp from $SourceAddr $SPort to $DestAddr $DPort [options]
ipfw add [rule no.] deny tcp from $SourceAddr $SPort to $DestAddr $DPort [options]
ipfw add [rule no.] reset tcp from $SourceAddr $SPort to $DestAddr $DPort [options]
ipfw add [rule no.] unreach [code] tcp from $SourceAddr $SPort to $DestAddr $DPort [options]
```

ภาพที่ 4.3 รูปแบบการสร้างกฎโดยใช้โปรโตคอลทีซีพี

ตัวอย่าง

ipfw add 10 allow tcp from any to any established[3]

ipfw add 11 deny tcp from any to any in via tun0 setup

ipfw add 12 reset[4] tcp from any to any 133 in via tun0

3) การใช้โปรโตคอลยูดีพี (UDP) เป็นคีย์สำหรับการกรอง

---

[3] การใช้คีย์ "setup" และ "establish" จะใช้เฉพาะโปรโตคอลทีซีพีเท่านั้น

[4] การใช้การกระทำแบบ "reset" จะใช้เฉพาะโปรโตคอลทีซีพีเท่านั้น

```
ipfw add [rule no.] allow udp from $SourceAddr $SPort to $DestAddr $DPort [options]
ipfw add [rule no.] deny udp from $SourceAddr $SPort to $DestAddr $DPort [options]
ipfw add [rule no.] reject udp  from $SourceAddr $SPort to $DestAddr $DPort [options]
ipfw add [rule no.] unreach [code] udp from $SourceAddr $SPort to $DestAddr $DPort [options]
```

ภาพที่ 4.4 รูปแบบการสร้างกฎโดยใช้โปรโตคอลยูดีพี

ตัวอย่าง

ipfw add 20 allow udp from x.x.x.x 53 to any 1024-65535 in recv tuno

ipfw add 21 reject udp from any to any 137 via tun0

ipfw add 22 unreach net udp from any to any 33400-33499 in recv tun0

4) การใช้โปรโตคอลไอซีเอ็มพี (ICMP) เป็นคีย์สำหรับการกรอง

```
ipfw add [rule no.] allow icmp from $SourceAddr to $DestAddr [options]
ipfw add [rule no.] unreach [code] icmp from $SourceAddre to $DestAddr [options]
```

ภาพที่ 4.5 รูปแบบการสร้างกฎโดยใช้โปรโตคอลไอซีเอ็มพี

ตัวอย่าง

ipfw add 30 allow icmp from any to any

ipfw add 31 unreach 13 icmp from any to any via ed1 in

5) การใช้โปรโตคอลทั้งหมด (all) เป็นคีย์สำหรับการกรอง

```
ipfw add [rule no.] allow all from $SourceAddr to $DestAddr [options]
ipfw add [rule no.] deny all from $SourceAddr to $DestAddr [options]
```

ภาพที่ 4.6 รูปแบบการสร้างกฎโดยใช้โปรโตคอลทั้งหมด

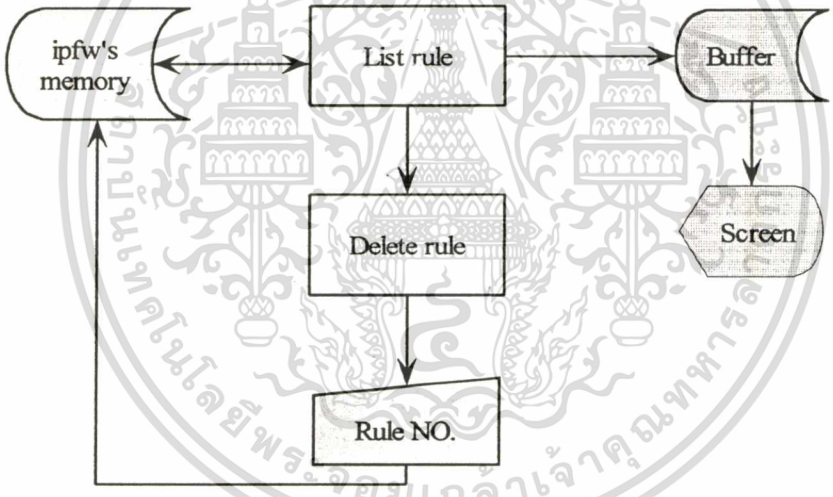
ตัวอย่าง

ipfw add 40 allow all from10.0.0.0:255.0.0.0 to any via ppp0

ipfw add 41 deny all from any to any

- Delete การลบกฎที่ใช้ ณ ปัจจุบันออกทีละกฎ โดยกำหนดหมายเลขกำกับลงไปด้วย การใช้คำสั่ง delete นี้จะไม่เกี่ยวข้องกับไฟล์กฎแต่อย่างใด เพราะจะกระทำเฉพาะกับกฎที่ถูกเรียกใช้อยู่เท่านั้น (ในหน่วยความจำของไอพีไฟร์วอลล์) ทำให้การเรียกใช้คำสั่งนี้สามารถกระทำได้โดยตรง ซึ่งจะมีขั้นตอนดังนี้

  1) ทำการตรวจสอบรายการของกฎก่อน โดยใช้คำสั่ง List Rule ในเมนูของการแก้ไข และคำสั่งที่ใช้ในการแสดงรายการของกฎคือ exec ipfw –a list
  2) เมื่อเรียกใช้คำสั่ง Delete จะปรากฏหน้าต่างของการลบกฎขึ้นมา ให้ทำการใส่หมายเลขของกฎที่ต้องการลบลงไป และคำสั่งที่ใช้ในการลบกฎคือ exec ipfw delete [rule no.]
  3) กดปุ่มตกลง เพื่อยืนยันการลบกฎ หลังจากนั้นกฎก็จะถูกลบออกไป

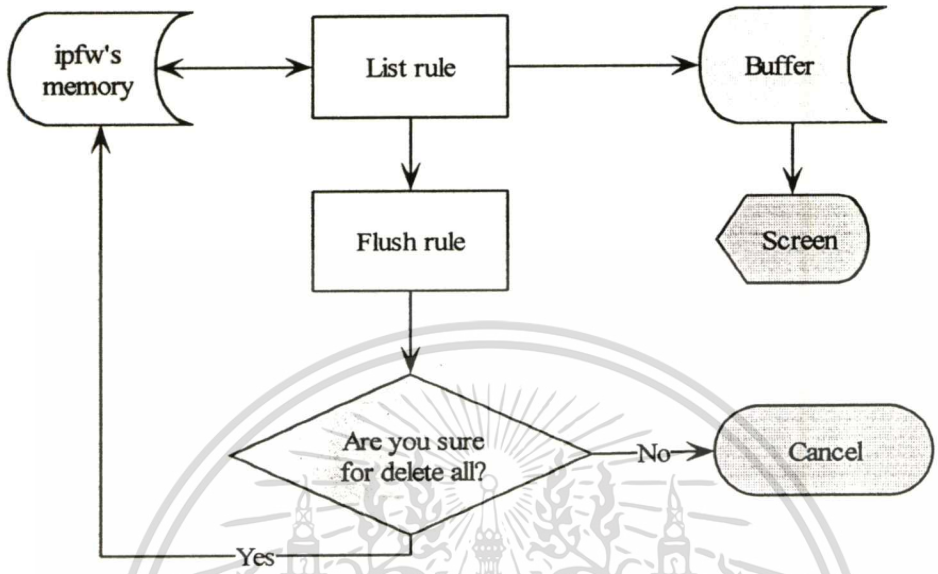


ภาพที่ 4.7 การทำงานของการลบกฎ

- Flush การลบกฎที่ใช้ ณ ปัจจุบันออกไปทั้งหมด การใช้คำสั่งนี้สามารถกระทำได้โดยตรงกับกฎที่ถูกเรียกใช้ เหมือนกับการเรียกใช้คำสั่ง delete มีขั้นตอนดังนี้

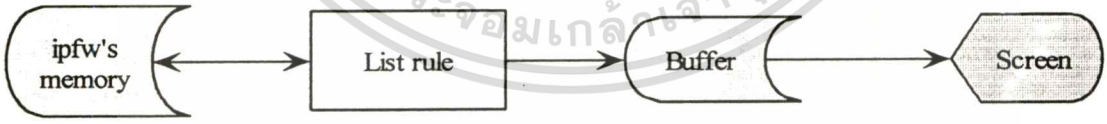
  1) ทำการตรวจสอบรายการของกฎก่อน โดยใช้คำสั่ง List Rule ในเมนูของการแก้ไข
  2) หลังจากนั้นจะทำคำสั่ง Flush
  3) เมื่อคำสั่ง Flush ถูกเรียกใช้จะมีหน้าต่างปรากฏขึ้นมาเพื่อถามความแน่ใจในการลบกฎทั้งหมด โดยที่...
     - ถ้าตอบ Yes กฎจะถูกลบออกไปทั้งหมด
     - ถ้าตอบ No ยกเลิกการลบกฎ

และคำสั่งที่ใช้ในการลบกฎทั้งหมดคือ exec ipfw flush



ภาพที่ 4.8 การทำงานของการลบกฎทั้งหมด

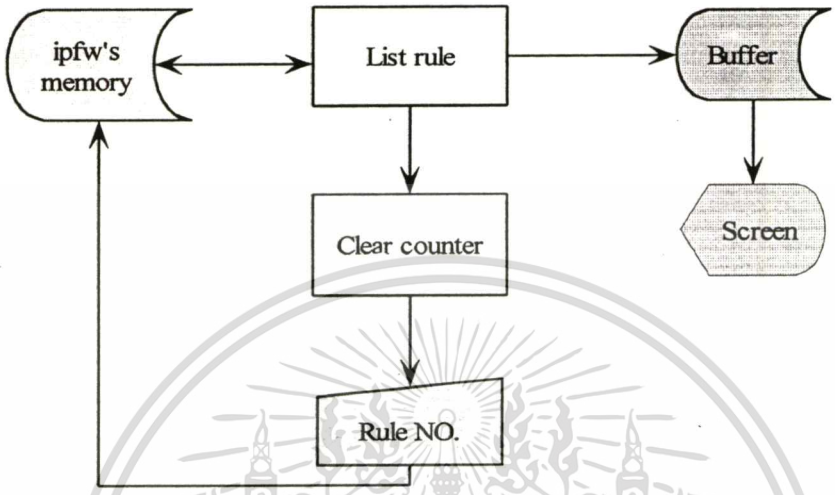
- List การแสดงกฎที่มีใช้ทั้งหมดในปัจจุบันมีขั้นตอนดังนี้
  1) เลือกคำสั่ง List Rule ในเมนูของการแก้ไข
  2) เมื่อคำสั่งนี้ถูกเรียกใช้ รายการของกฎจะปรากฏยังที่ว่างที่ได้เตรียมไว้ และคำสั่งที่ใช้ในการแสดงรายการของกฎคือ exec ipfw –a list



ภาพที่ 4.9 การทำงานของการแสดงรายการของกฎ

- Clear counter การลบค่าตัวนับแพ็คเก็ตให้เป็นศูนย์ มีขั้นตอนดังนี้
  1) ทำการตรวจสอบรายการของกฎก่อน โดยใช้คำสั่ง List Rule ในเมนูของการแก้ไข และคำสั่งที่ใช้ในการแสดงรายการของกฎคือ exec ipfw –a list โดยที่ –a จะมีการแสดงค่าของตัวนับแพ็คเก็ตด้วย
  2) เมื่อเรียกใช้คำสั่ง Clear counter จะปรากฏหน้าต่างของการลบค่าตัวนับแพ็คเก็ตขึ้นมา ให้ทำการใส่หมายเลขของกฎที่ต้องการลบค่าลงไป และคำสั่งที่ใช้ในการลบกฎคือ exec ipfw –q clear [rule no.]

3) กดปุ่มตกลง เพื่อยืนยันการลบกฎ หลังจากนั้นค่าของตัวนับแพ็คเก็ตนั้นก็จะถูกลบออกไป

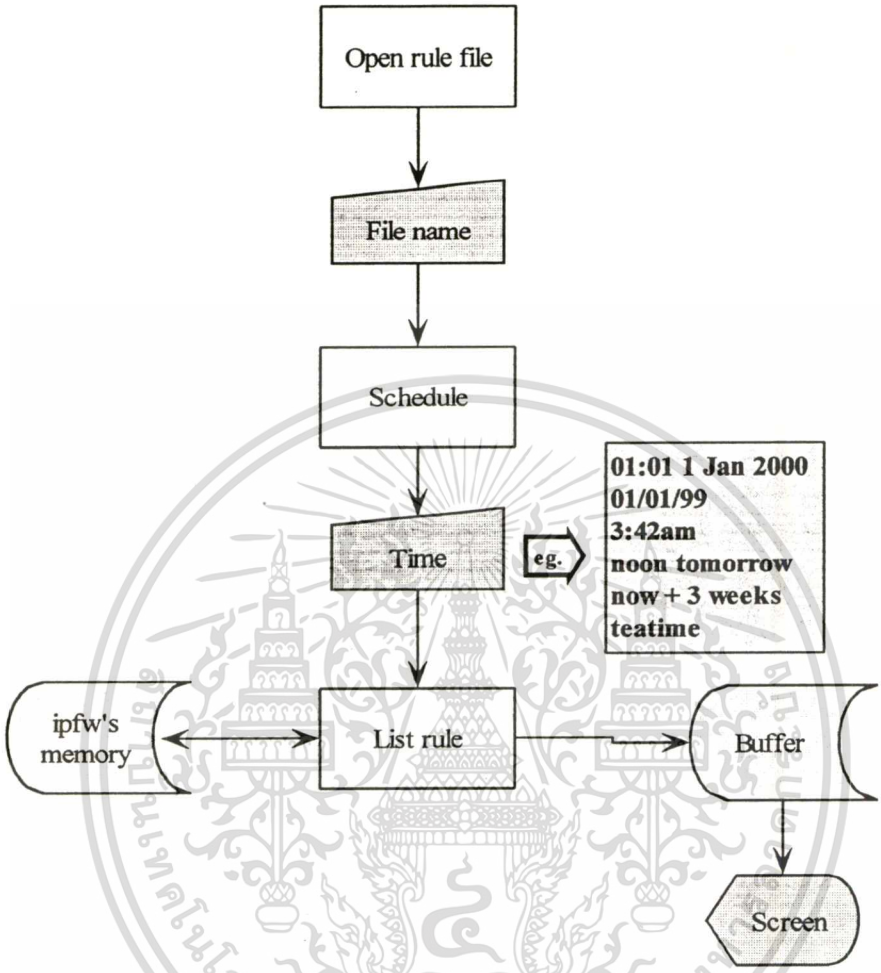


ภาพที่ 4.10 การทำงานของการลบค่าตัวนับแพ็คเก็ต

- Update rule การนำกฎที่แสดงอยู่บนหน้าจอ ใส่เข้าไปในหน่วยความจำของไอพีไฟร์วอลล์ เพื่อให้กฎนั้นทำงาน (ดูในรูปการเพิ่มกฎ) การกระทำนี้จะกระทำบ่อยครั้งแค่ไหน ขึ้นอยู่กับความต้องการของผู้ใช้ และคำสั่งที่ใช้คือ exec ipfw add [rule description] โดยที่ [rule description] คือรายละเอียดของกฎที่เราต้องการจะให้กฎนั้นทำงาน (มาจากหน้าจอ)

4.1.2 ฟังก์ชันการทำงานเพิ่มเติม

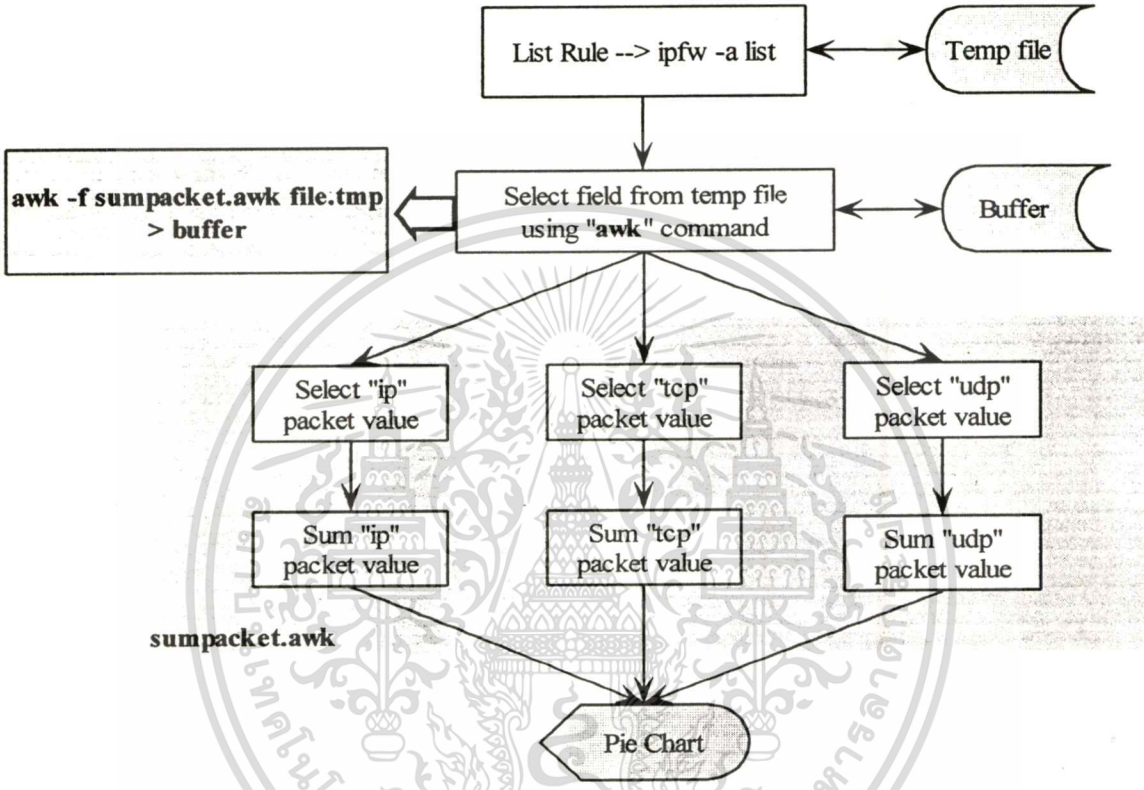
- Scheduling การตั้งเวลาการกรองแพ็คเก็ตในช่วงเวลาที่สามารถกำหนดเองได้ คำสั่งที่ใช้คือ "at" ซึ่งเป็นคำสั่งหนึ่งบนยูนิกต์ (ฟรีบีเอสดี) และการใช้คำสั่งจะทำดังนี้คือ exec at –f [file] [time] โดยที่ file คือไฟล์กฎที่เราต้องการจะให้กฎนั้นทำงาน และ time คือเวลาที่เรากำหนด ตัวอย่างของการบันทึกเวลาดูได้จากภาพที่ 4.11 และเมื่อถึงเวลาที่บันทึก กฎนั้นจึงจะเริ่มทำงาน มีขั้นตอนดังนี้
  1) ทำการเปิดไฟล์กฎที่ต้องการตั้งเวลาการกรอง แล้วเลือกคำสั่ง Scheduling
  2) บันทึกเวลาที่ต้องการให้กฎนี้ทำงาน เช่น...
     - ต้องการเวลา 4 โมงเย็น ---→ 16:00 หรือ 4:00pm
     - ต้องการเวลา 4 โมงเย็นพรุ่งนี้ ---→ 16:00 tomorrow



ภาพที่ 4.11 การทำงานของการตั้งเวลาการกรอง

- Monitoring การตรวจสอบจำนวนแพ็คเก็ตที่ผ่านเข้ามา การจัดเก็บจำนวนแพ็คเก็ตจะใช้คำสั่ง exec ipfw –a list ซึ่ง -a จะมีการแสดงค่าของแพ็คเก็ตที่เข้าคู่กับกฎ ตามโปรโตคอลที่ระบุ แล้วนำค่าดังกล่าวไปเก็บไว้ในไฟล์อันหนึ่ง (อาจเรียกว่าเป็นล็อคไฟล์ก็ได้) ไฟล์ดังกล่าวประกอบด้วยฟิลด์ดังนี้คือ เลขที่กฎ จำนวนแพ็คเก็ต จำนวนไบต์ การกระทำของกฎ โปรโตคอล แอดเดรส/พอร์ตต้นทาง แอดเดรส/พอร์ตปลายทาง และตัวเลือกอื่น ๆ หลังจากนั้นก็จะทำการเลือกฟิลด์ที่ต้องการได้แก่ ฟิลด์จำนวนแพ็คเก็ต และฟิลด์โปรโตคอล โดยใช้คำสั่ง “awk” ในยูนิกต์ และจะมีการเรียกใช้คำสั่งดังนี้คือ exec awk –f sumpacket.awk file(log file) โดยที่ไฟล์ sumpacket.awk ทำหน้าที่ในการเลือกฟิลด์ที่เป็นไอพีแพ็คเก็ต ทีซีพีแพ็คเก็ต และยูดีพีแพ็คเก็ต แล้วทำการรวมค่าแพ็คเก็ตของแต่ละโปรโตคอล

ฟังก์ชันของไอพีไฟร์วอลล์จะเป็นทำการตรวจสอบจากการจราจรของเครือข่าย โปรโตคอลที่จะแสดงได้แก่ โปรโตคอลไอพี ทีซีพี และยูดีพี และการแสดงจำนวนแพ็คเก็ตเหล่านี้จะแสดงอยู่ในรูปของแผนภูมิวงกลม (PieChart)

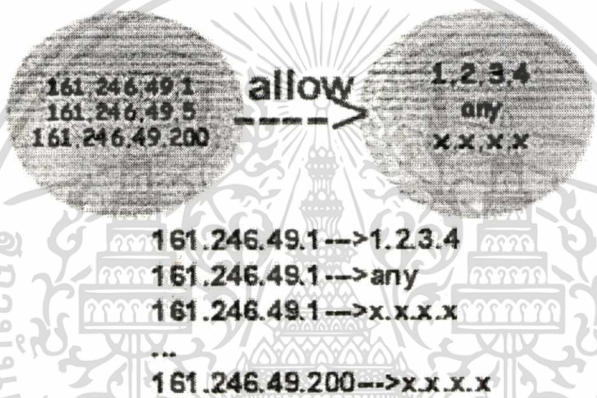


ภาพที่ 4.12 การทำงานของการตรวจสอบจำนวนแพ็คเก็ต

- Basic rule analysis การวิเคราะห์กฎขั้นพื้นฐาน เพื่อไม่ให้กฎมีการซ้ำกัน เนื่องจากโดยปกติการเพิ่มกฎเข้าไปมักจะเพิ่มเข้าไปเรื่อย ๆ ทำให้สิ้นเปลืองเนื้อที่สำหรับเก็บไฟล์กฎ การป้องกันการซ้ำกันของกฎจะกระทำในช่วงของการสร้างกฎและเพิ่มกฎ ถ้ากฎที่ถูกสร้างขึ้นมาใหม่เกิดซ้ำกับกฎที่มีอยู่เดิม กฎนั้นก็จะไม่เพิ่มเข้าไป (ดูในรูปการเพิ่มกฎ) คำสั่งที่ใช้คือ String compare *inputValue dataValue* โดยที่ inputValue เป็นรายการของกฎอันใหม่ ส่วน dataValue เป็นรายการของกฎที่มีอยู่เดิม และทั้ง inputValue และ dataValueจะมีเฉพาะรายละเอียดของกฎเท่านั้น ไม่ได้รวมเลขที่กฎไว้ด้วย

- Policy management เป็นโปรแกรมพิเศษของการจัดการในเรื่องนโยบาย มีลักษณะดังนี้คือ มีการจัดกลุ่มที่เป็นนโยบายแล้วกระจายออกเป็นกฎต่าง ๆ ฟังก์ชันการทำงานที่สำคัญมี 2 ส่วนคือ
  1) ส่วนของการสร้างและแก้ไขนโยบาย (Policy) ตัวอย่าง การอนุญาตให้กลุ่ม A ติดต่อกลุ่ม B ได้ (แต่ว่าในกลุ่ม A และ B จะต้องมีสมาชิกในกลุ่มด้วย)
  2) ส่วนของการสร้างและแก้ไขกลุ่ม (Group) เป็นการรวมสมาชิกเป็นกลุ่ม ๆ หนึ่ง เช่นกลุ่มของหมายเลขไอพี เป็นต้น

การแตกนโยบายออกเป็นกฎนั้นสามารถแสดงได้ดังภาพที่ 4.13



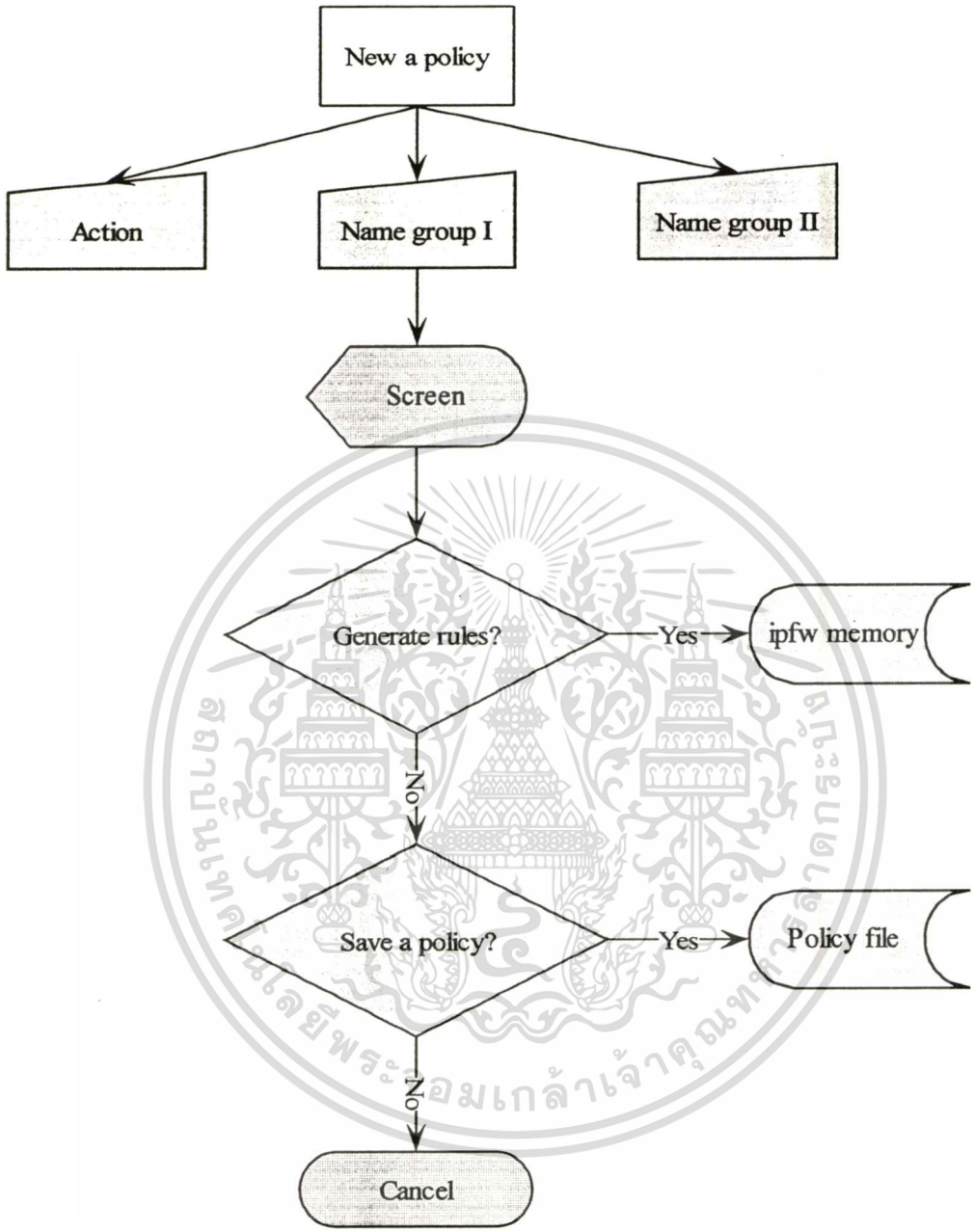
ภาพที่ 4.13 ตัวอย่างการกระจายนโยบายให้เป็นกฎต่าง ๆ

จากภาพที่ 4.13 จะเป็นลักษณะของการกระจายกฎจากนโยบาย โดยกลุ่มทางซ้ายเป็นกลุ่มต้นทาง และกลุ่มทางขวาเป็นกลุ่มปลายทาง การสร้างนโยบายนี้จะสอดคล้องกับการสร้างกฎคือ

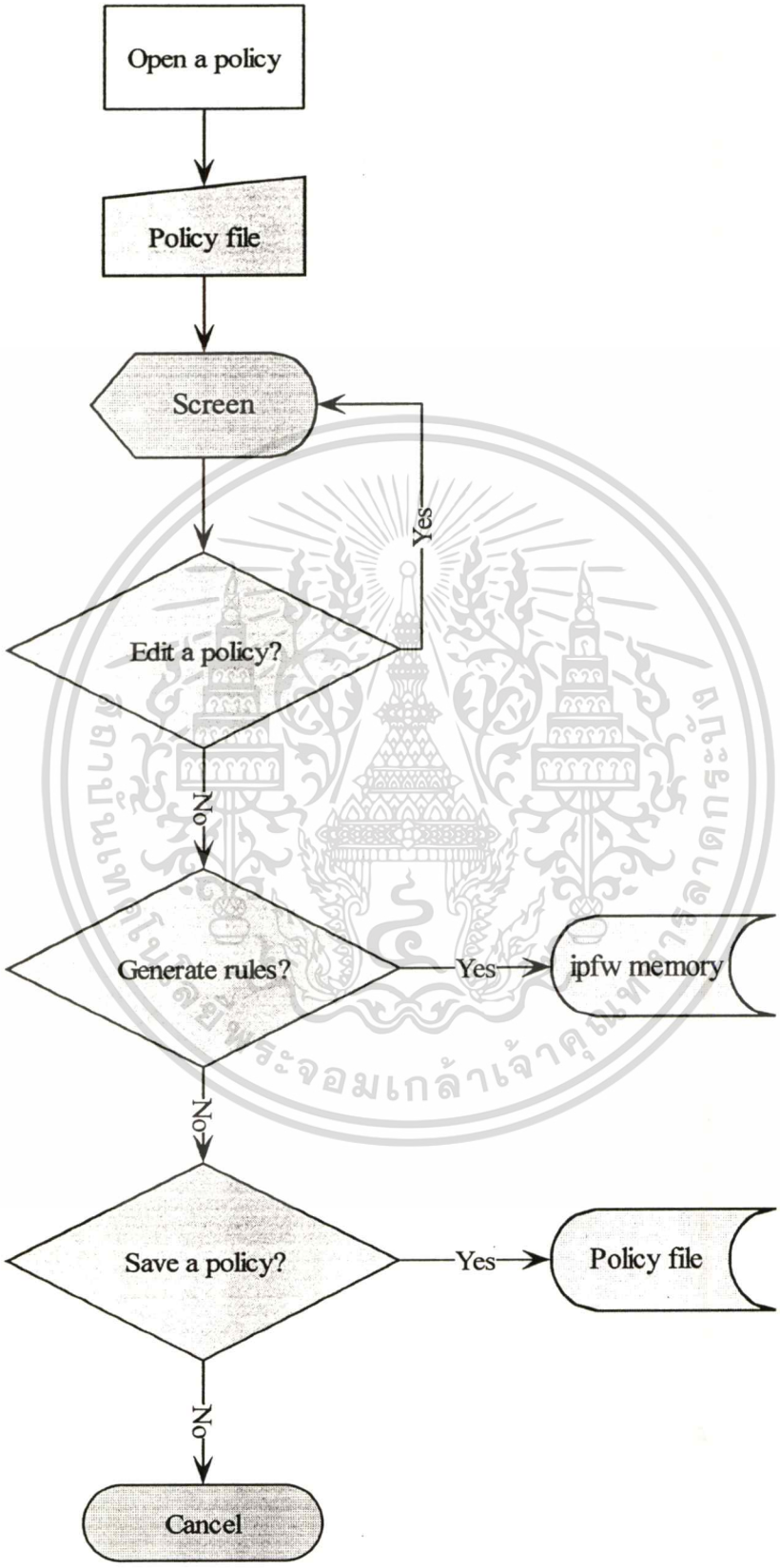
กลุ่มต้นทาง -→ แอดเดรสต้นทาง

กลุ่มปลายทาง -→ แอดเดรสปลายทาง

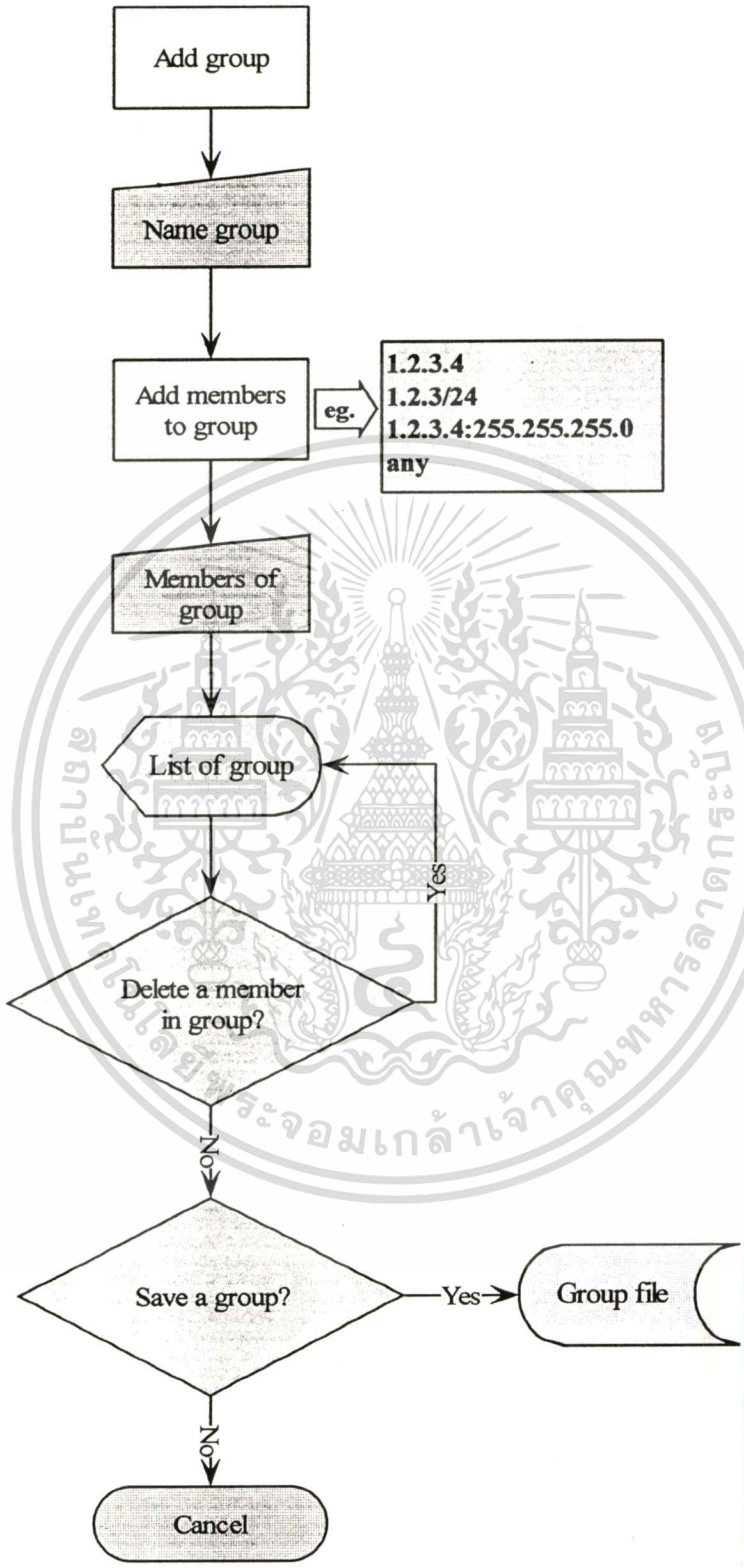
คำสั่งที่ใช้ในการกระจายกฎคือ exec ipfw add [rule descriptions]



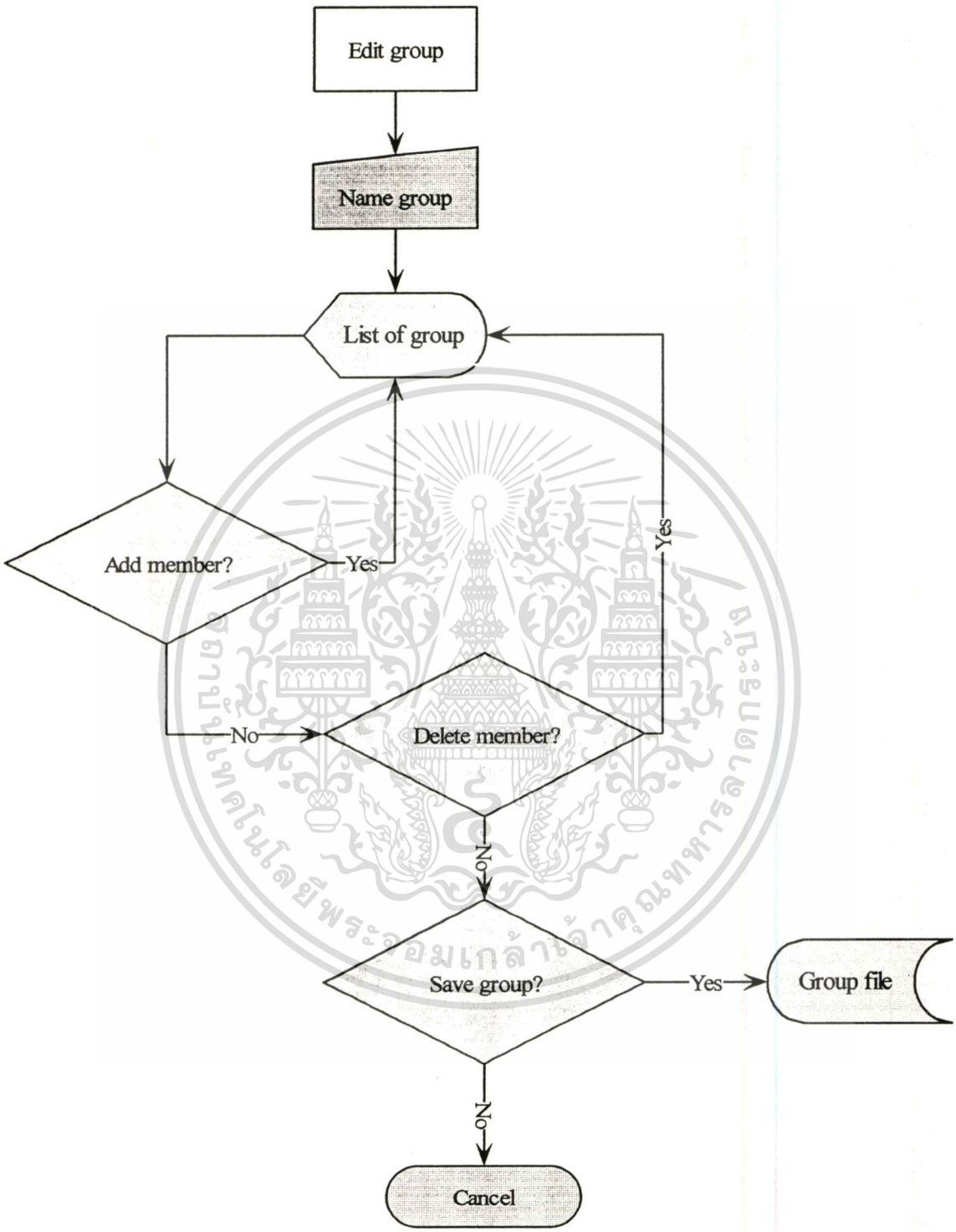
ภาพที่ 4.14 การทำงานของการสร้างนโยบาย



ภาพที่ 4.15 การทำงานของการแก้ไขนโยบาย



ภาพที่ 4.16 การทำงานของการเพิ่มกลุ่ม

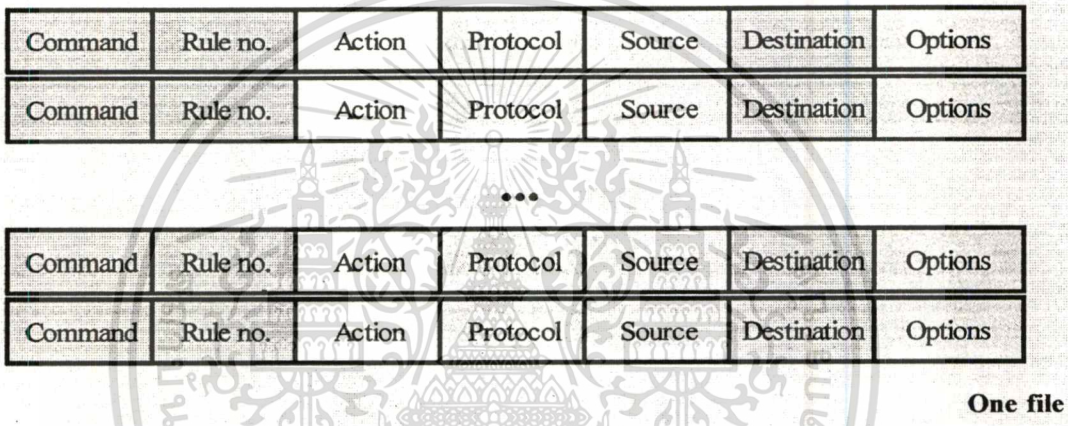


ภาพที่ 4.17 การทำงานของการแก้ไขกลุ่ม

4.2 การออกแบบฐานข้อมูลของกฎ

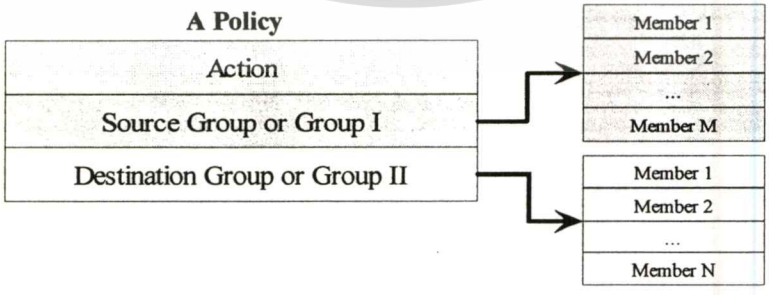
ฐานข้อมูลของกฎจะประกอบไปด้วยไฟล์ 3 หลักคือ ไฟล์กฎ (Rule file) ไฟล์นโยบาย (Policy file) และไฟล์กลุ่ม (Group file) ซึ่งมีลักษณะดังนี้

1) **ไฟล์กฎ** เป็นไฟล์สำหรับรายการของกฎประกอบด้วยฟิลด์ต่าง ๆ ได้แก่ คำสั่งของไอพีไฟร์วอลล์ หมายเลขของกฎ การกระทำของกฎ ชนิดของโปรโตคอล แอดเดรสต้นทาง พอร์ตต้นทางแอดเดรสปลายทาง พอร์ตปลายทาง และตัวเลือกอื่น ๆ



ภาพที่ 4.18 ลักษณะของการเก็บข้อมูลในไฟล์กฎ

2) **ไฟล์นโยบาย** เป็นไฟล์สำหรับการบันทึกนโยบายประกอบด้วยฟิลด์ต่าง ๆ ได้แก่ การกระทำของกฎ กลุ่มที่ถูกเลือกให้เป็นทาง และกลุ่มที่ถูกเลือกให้เป็นปลายทาง



A Policy = M*N Rules

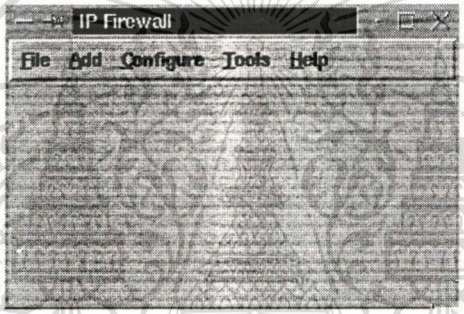
ภาพที่ 4.19 ลักษณะของการเก็บข้อมูลในไฟล์นโยบาย

3) **ไฟล์กลุ่ม** เป็นไฟล์สำหรับการบันทึกกลุ่มประกอบด้วยไอพีแอดเดรสต่าง ๆ ที่ต้องการจะจัดให้อยู่ในกลุ่มเดียวกัน

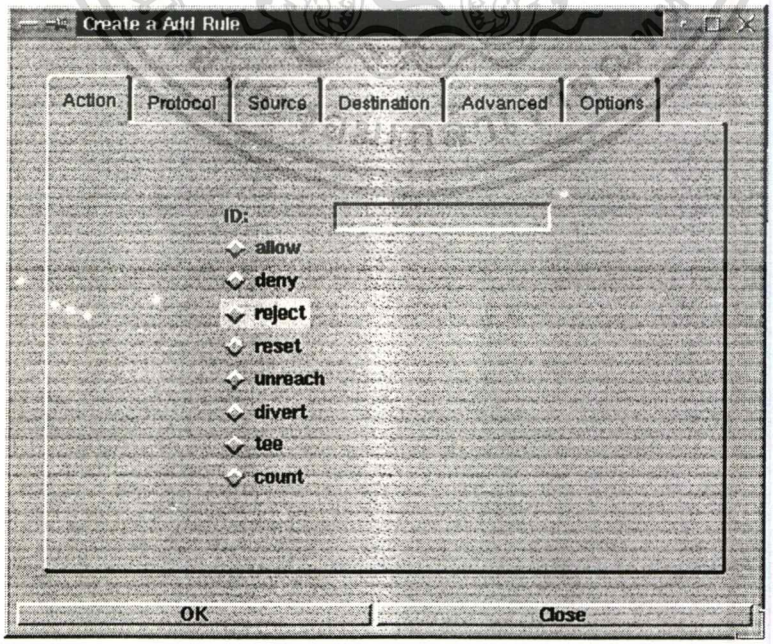
Member 1
Member 2
...
Member M

ภาพที่ 4.20 ลักษณะของการเก็บข้อมูลในไฟล์กลุ่ม

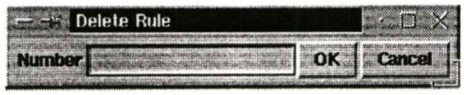
4.3 การออกแบบหน้าต่างหลักในระบบงาน



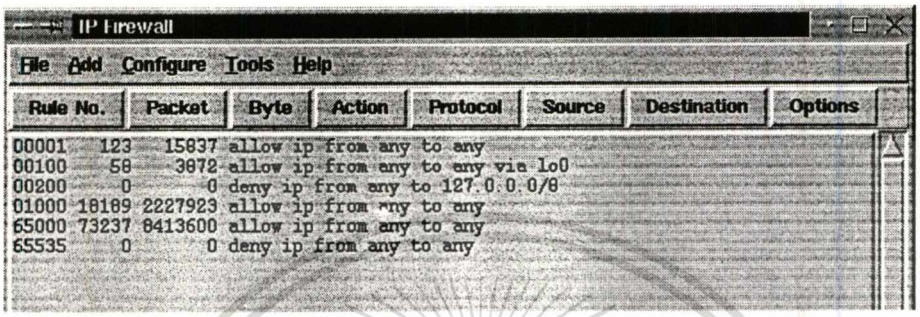
ภาพที่ 4.21 หน้าต่างหลักของโปรแกรม



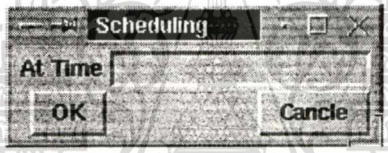
ภาพที่ 4.22 หน้าต่างของการเพิ่มกฎ



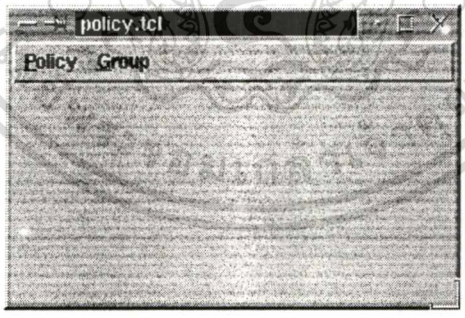
ภาพที่ 4.23 หน้าต่างของการลบกฎ



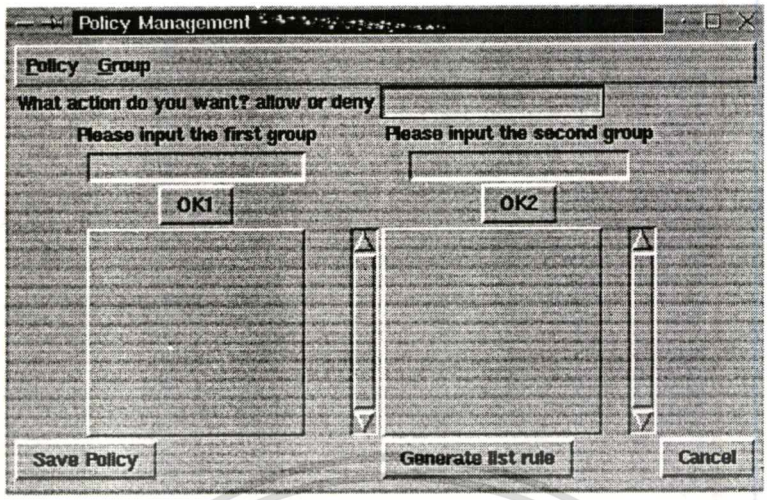
ภาพที่ 4.24 หน้าต่างของผลลัพธ์ที่ได้จากการแสดงรายการของกฎ



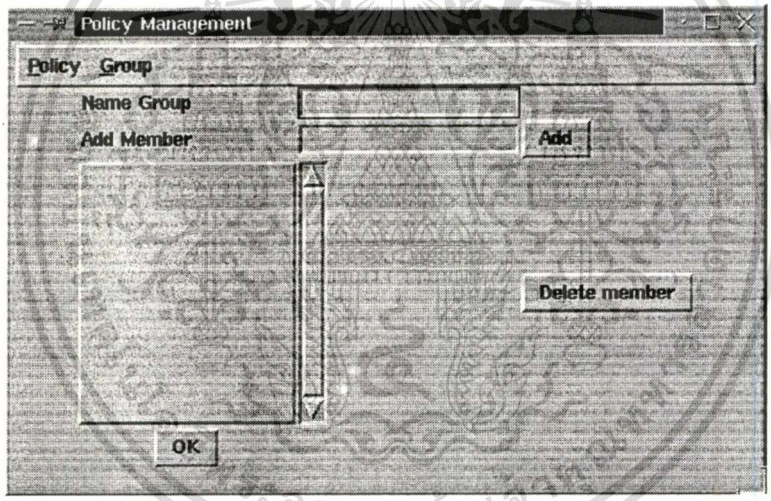
ภาพที่ 4.25 หน้าต่างของการตั้งเวลาการกรอง



ภาพที่ 4.26 หน้าต่างหลักของการจัดการนโยบายของกฎ



ภาพที่ 4.27 หน้าต่างการสร้างนโยบาย



ภาพที่ 4.28 หน้าต่างการสร้างกลุ่ม

บทที่ 5

การสรุปผลการทำงานของระบบงาน

ในบทนี้จะมีการสร้างสถานการณ์ออกเป็น 3 กรณีเพื่อให้ครอบคลุมการทำงานทั้งหมด โปรแกรมควบคุมไอพีไฟร์วอลล์จะถูกทดสอบการใช้งานตามสถานการณ์ดังกล่าว เมื่อได้ผลที่ได้จากการทดลอง ก็นำมาเปรียบเทียบกับการทำงานตามฟังก์ชันต่าง ๆ ที่กำหนดไว้กับที่เกิดขึ้นจริง แล้วสรุปผลออกมา

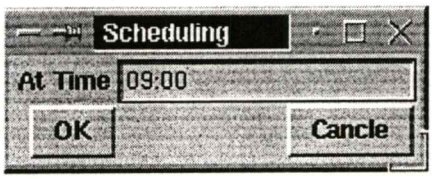
5.1 การทดสอบระบบงาน

การทดสอบระบบงานในกรณีแรกจะเริ่มจากการสร้างกฎขึ้นมาใหม่และทำการบันทึกลงในไฟล์กฎ หลังจากนั้นทำการทดสอบดูว่าไฟล์กฎดังกล่าวถูกนำมาใช้ได้จริง โดยการทดสอบจากฟังก์ชันของการตั้งเวลาการกรอง สำหรับการเรียกใช้ฟังก์ชันการตั้งเวลาการกรองนั้นเมื่อถึงเวลาที่กำหนดไว้กฎที่ถูกสร้างไว้จะถูกเรียกขึ้นมาใช้ และเครื่องจะมีการส่งการติดต่อกลับมายังรูท (Root) ของเครื่องเพื่อบอกว่ามันได้ทำงานตามคำสั่งเรียบร้อยแล้ว โดยผ่านระบบอิเล็กทรอนิกส์เมล์ (Electronic Mail System)

ขั้นตอนต่อไปคือ เมื่อกฎเหล่านั้นถูกเรียกขึ้นมาใช้งาน จะทำการแสดงรายการของกฎด้วยฟังก์ชันการแสดงรายการของกฎ (List Rule) แล้วเปรียบเทียบกับการทำคำสั่งโดยตรง (Command Line) หลังจากนั้นจะตรวจสอบดูว่ามีแพ็คเก็ตของโปรโตคอลใดผ่านเข้ามาบ้าง โดยใช้ฟังก์ชันของการมอนิเตอร์ (Monitoring) ซึ่งแพ็คเก็ตที่เข้าคู่กับกฎการอนุญาตจะถูกนับเอาไว้และแสดงออกมาอยู่ในรูปของแผนภูมิวงกลม

<u>ตัวอย่างของกรณีที่ 1</u>

1) เมื่อต้องการสร้างไฟล์กฎอันใหม่ขึ้นมา ให้เลือกคำสั่ง New ที่เมนูไฟล์
2) เลือกคำสั่ง Add Rule ที่เมนูแก้ไข แล้วทำการสร้างกฎตามคีย์ในตารางที่ 5.1
3) เลือกคำสั่ง Save ที่เมนูไฟล์ โดยตั้งชื่อไฟล์ว่า “test.ru”
4) เมื่อต้องการตั้งเวลาการกรองล่วงหน้า เลือกคำสั่ง Scheduling ที่เมนูแก้ไข
5) เมื่อมีหน้าต่างปรากฏขึ้นมาให้ใส่เวลา 09:00 (เวลาที่ใกล้เคียงในขณะนั้น) ลงไปในช่องว่างนั้น แล้วกดปุ่ม OK ดังภาพที่ 5.1



ภาพที่ 5.1 การบันทึกเวลาการกรอง

6) หลังเวลา 09:00 เลือกคำสั่ง List Rule ในเมนูแก้ไข เพื่อแสดงรายการของกฎ
7) เมื่อต้องการตรวจจำนวนแพ็คเก็ตที่เข้ามา ให้เลือกคำสั่ง Monitoring ที่เมนูแก้ไข

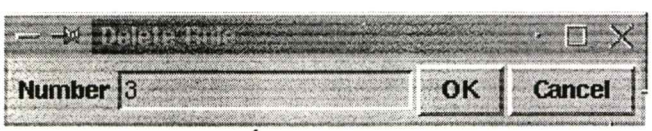
ตารางที่ 5.1 ตัวอย่างกฎสำหรับการสร้างกฎในกรณีที่ 1

Rule	1	2	3
ID	001	002	003
Action	allow	allow	Allow
Protocol	ip	tcp	Udp
Source Address	any	161.246.49.221	Any
Source Port	-	-	53,137,123
Destination Address	any	any	Any
Destination Port	-	-	114-65535
Extras	via lo0 in	via tun0 in	Via tun0 in

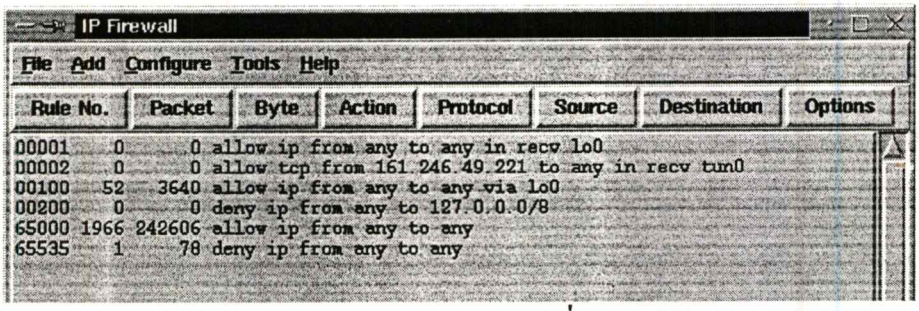
การทดสอบระบบงานในกรณีที่ 2 เป็นการนำเอาไฟล์กฎที่อยู่แล้วมาทำการปรับปรุง เช่นการลบกฎเดิมออกไป และเพิ่มกฎใหม่เข้าไปแทน ขณะทำการเพิ่มกฎอันใหม่เข้าไป ถ้าพบว่ามีการซ้ำกันของกฎ โปรแกรมจะเตือนถึงการซ้ำของกฎ เพื่อให้ผู้ใช้ทราบถึงการซ้ำกันของกฎนั้น ต่อจากนั้นให้ทำการลบกฎที่ไม่ต้องการออก โดยกำหนดหมายเลขของกฎลงไป การลบกฎจะลบได้ทีละหมายเลขเท่านั้น ถ้าต้องการลบกฎทั้งหมดจะต้องใช้ฟังก์ชันการลบกฎทั้งหมด (Flush or Delete all)

ตัวอย่างของกรณีที่ 2

1) เปิดไฟล์กฎที่ชื่อว่า "test.ru" ขึ้นมาเพื่อทำการเพิ่มกฎตามตัวอย่างในตารางที่ 5.2
2) หลังจากนั้นให้ทำการลบไฟล์กฎที่หมายเลข "003" ออกไป โดยใช้ฟังก์ชัน "Delete" ดังภาพที่ 5.2
3) จากภาพที่ 5.3 แสดงรายการของกฎ เพื่อดูว่ากฎหมายเลข 003 ถูกลบออกไปแล้ว
4) ถ้าต้องลบกฎทั้งหมด ให้ใช้คำสั่ง "Delete All" ในเมนูแก้ไข



ภาพที่ 5.2 การลบกฎออกไปตามหมายเลขที่กำหนด



ภาพที่ 5.3 การแสดงรายการของกฎหลังจากลบรายการกฎที่ 3 ออกไป

ตารางที่ 5.2 ตัวอย่างกฎสำหรับการสร้างกฎในกรณีที่ 2

Rule	**1**	**2**
ID	101	102
Action	Allow	Allow
Protocol	Ip	Udp
Source Address	Any	161.246.49.221
Source Port	-	-
Destination Address	Any	Any
Destination Port	-	53
Extras	via lo0 in	-

การทดสอบระบบงานในกรณีที่ 3 เป็นการใช้ฟังก์ชันการจัดการนโยบาย (Policy Management) ซึ่งเป็นโปรแกรมพิเศษโปรแกรมหนึ่ง สามารถสร้างนโยบายแบบง่าย ๆ ได้ และสามารถกระจายนโยบายให้เป็นกฎต่าง ๆ โดยจะต้องมีการจัดกลุ่ม 2 กลุ่มให้กับนโยบาย ดังนั้นเริ่มต้นจะต้องสร้างกลุ่มขึ้นมาก่อน ซึ่งจำนวนกลุ่มที่จะใช้ในนโยบาย 1 นโยบายมีจำนวน 2 กลุ่ม กลุ่มที่สร้างนี้จะเป็นกลุ่มที่ประกอบด้วยสมาชิกได้แก่ ไอพีแอดเดรส เป็นต้น เมื่อสร้างกลุ่มเป็นที่เรียบร้อยแล้วจึงค่อยสร้างนโยบายต่อไป เมื่อสร้างนโยบายเสร็จ ก็สามารถกระจายนโยบายอันนั้นออกมาเป็นกฎต่าง ๆ ได้ โดยจะใช้คำสั่งการกระจายกฎซึ่งอยู่บนหน้าต่างที่ปรากฏ (Generate List Rule)

<u>ตัวอย่างของกรณีที่ 3</u>

1) ทำการสร้างกลุ่มที่ต้องการก่อน เลือกที่เมนูกลุ่ม (Group Menu) หลังจากนั้นเลือกคำสั่ง “Add Group”
2) ตั้งชื่อของกลุ่มว่า mygroup1 แล้วพิมพ์ในช่องเพิ่มสมาชิกว่า 161.246.10.21 แล้วกดปุ่ม “Add” หลังจากนั้นพิมพ์ 161.246.49.1 และ 161.246.49.0 ตามลำดับ
3) ทำการเพิ่มกลุ่มที่มีชื่อว่า mygroup2 หลังจากนั้นทำการใส่สมาชิกลงไปดังนี้คือ any และ 161.246.49.221

4) ทำการสร้างนโยบายใหม่ ให้เลือกที่เมนูนโยบาย (Policy Menu) แล้วเลือกคำสั่ง “New Policy”
5) เลือกการกระทำแบบอนุญาต โดยพิมพ์คำว่า “allow”
6) เลือกชื่อกลุ่ม mygroup1 และ mygroup2 ใส่ลงในช่อง ตามลำดับ
7) เมื่อต้องการบันทึกไฟล์นโยบายให้กดปุ่ม “Save” และบันทึกไฟล์ที่ชื่อว่า “test.pol”
8) ถ้าต้องการกระจายนโยบายให้เป็นกฎต่าง ๆ ให้กดปุ่ม “Generate List Rule” หลังจากนั้นทำการตรวจสอบกฎโดยพิมพ์คำสั่งโดยตรงผ่านบรรทัดคำสั่ง (Command Line) ว่า “ipfw list” หรือ ใช้คำสั่ง “List Rule” ในโปรแกรม

5.2 ผลสรุปที่ได้จากการทดสอบระบบ

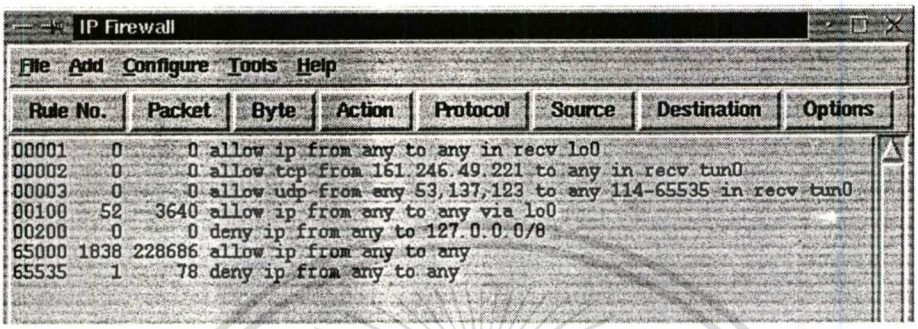
ผลสรุปที่ได้จากการทดสอบระบบแบ่งตามกรณีทั้ง 3 ดังนี้คือ กรณีที่ 1 เกี่ยวกับการใช้ฟังก์ชันการสร้างกฎ การตั้งเวลาการกรอง การแสดงรายการของกฎ และการมอนิเตอร์แพ็คเก็ต ส่วนกรณีที่ 2 เกี่ยวกับการใช้ฟังก์ชันการเพิ่มกฎ การวิเคราะห์กฎขั้นพื้นฐาน การลบกฎทีละกฎ และการลบกฎทั้งหมด และกรณีที่ 3 เกี่ยวกับการใช้ฟังก์ชันการจัดการนโยบาย

ผลการทดลองของกรณีที่ 1

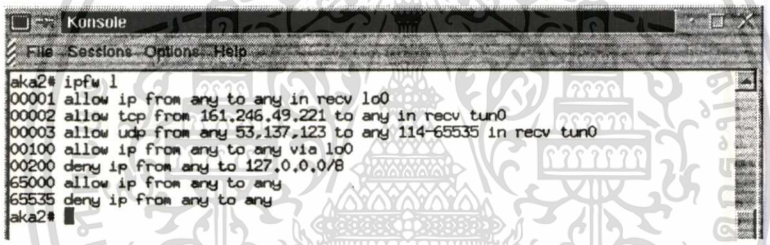
1) เมื่อทำคำสั่ง “Scheduling” ตัวระบบจะส่งอีเมล์มาให้รูท เพื่อบอกว่ามันได้ทำงานให้เรียบร้อยแล้วดังภาพที่ 5.4

ภาพที่ 5.4 การตอบรับการบันทึกเวลาการกรอง

2) เมื่อทำคำสั่ง “List Rule” จะแสดงรายการของกฎบนที่ว่างที่ได้เตรียมไว้ในโปรแกรม ดังภาพที่ 5.5 และเมื่อเปรียบเทียบกับการทำคำสั่งโดยตรงดังภาพที่ 5.6 จะเห็นว่าเหมือนกัน

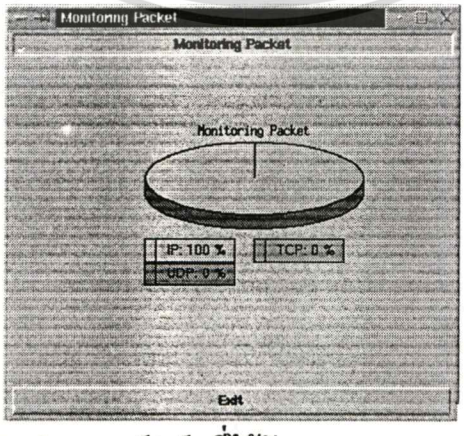


ภาพที่ 5.5 การแสดงรายการของกฎของโปรแกรม



ภาพที่ 5.6 การแสดงรายการของกฎผ่านคอนโซล

3) เมื่อทำคำสั่ง “Monitoring” จะทำการรวบรวมจำนวนแพ็คเก็ตของโปรโตคอลไอพี ทีซีพี และยูดีพี มาแสดงอยู่ในรูปของแผนภูมิวงกลมดังภาพที่ 5.7



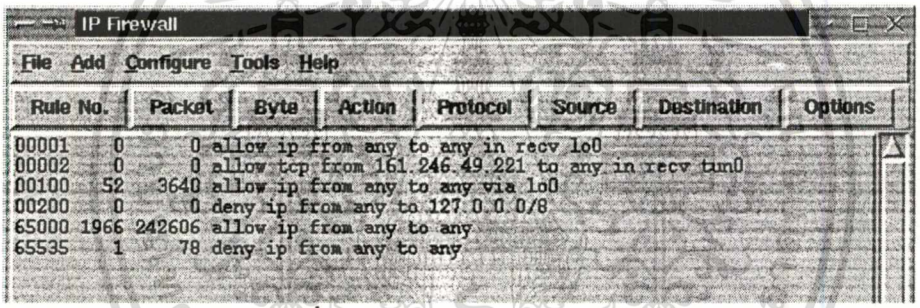
ภาพที่ 5.7 แผนภูมิวงกลมแสดงจำนวนแพ็คเก็ตที่ได้รับ

ผลการทดลองของกรณีที่ 2

1) เมื่อทำการเพิ่มกฎใหม่ โดยใช้ตัวอย่างแรกของกฎในตารางที่ 5.2 จะพบว่ามีการซ้ำกันเกิด จะปรากฏหน้าต่างดังภาพที่ 5.8 และกฎนั้นก็จะไม่ถูกเพิ่มเข้าไป

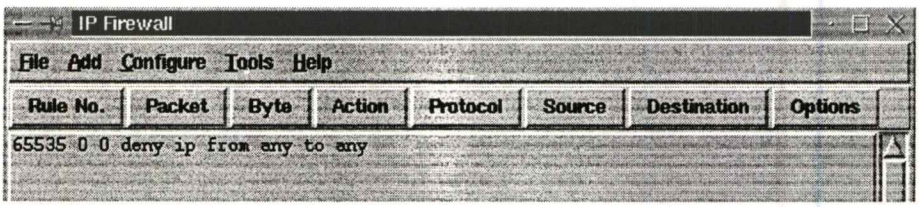
ภาพที่ 5.8 การซ้ำกันของกฎ

2) เมื่อทำการลบกฎโดยใช้คำสั่ง "Delete" หมายเลข 003 จะพบว่ากฎรายการนั้นหายไป สามารถแสดงรายการของกฎได้ดังภาพที่ 5.9



ภาพที่ 5.9 การแสดงรายการของกฎที่ไม่ได้ถูกลบ

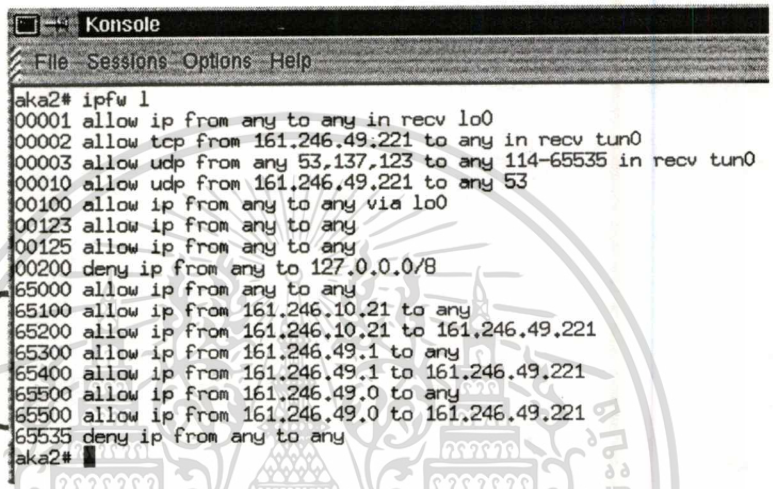
3) เมื่อทำการลบกฎทั้งหมดโดยใช้คำสั่ง "Delete all" จะพบว่ากฎทั้งหมดหายไป เหลือแต่ค่าเริ่มต้นเท่านั้น แสดงได้ดังภาพที่ 5.10



ภาพที่ 5.10 การแสดงรายการของกฎถูกลบไปหมด

ผลการทดลองของกรณีที่ 3

1) เมื่อทำคำสั่งการจัดการนโยบาย ทำให้สามารถสร้างนโยบายเบื้องต้นต่าง ๆ ได้ โดยในนโยบายจะต้องประกอบด้วยกลุ่ม 2 กลุ่ม เพราะว่ากลุ่ม 2 กลุ่มนี้จะต้องมีการกระทำต่อกันซึ่งอาจจะเป็นแบบยอมรับ หรือปฏิเสธก็ได้
2) เมื่อสร้างนโยบายได้แล้ว ก็สามารถกระจายออกมาเป็นกฎต่าง ๆ ได้ดังภาพที่ 5.11



ภาพที่ 5.11 นโยบายที่กระจายออกมาเป็นกฎต่าง ๆ

5.3 สรุปผลการพัฒนาโปรแกรม

จากการพัฒนาโปรแกรมทำให้เข้าใจถึงความสามารถของฟังก์ชันไอพีไฟร์วอลล์และการนำฟังก์ชันการทำงานนี้มาใช้ประโยชน์ รวมถึงได้มีการพัฒนาฟังก์ชันการทำงานเพิ่มเติมแก่ไอพีไฟร์วอลล์ด้วย

ผลที่ได้จากการทดลองทั้ง 3 กรณีดังกล่าว เป็นเครื่องพิสูจน์ได้ว่าการทำงานของโปรแกรมสามารถควบคุมการทำงานของไอพีไฟร์วอลล์ได้จริง เช่นการเพิ่มกฎ การแสดงรายการของกฎ การลบกฎ การลบค่าตัวนับแพ็คเก็ต การตั้งเวลาการกรอง ณ เวลาที่เรากำหนดให้ทำงาน การตรวจสอบจำนวนแพ็คเก็ต การวิเคราะห์กฎขั้นพื้นฐานเพื่อไม่ให้กฎที่เพิ่มเข้ามาซ้ำกับกฎที่มีอยู่ และการสร้างนโยบาย

5.4 ข้อเสนอแนะ

โปรแกรมควบคุมไอพีไฟร์วอลล์ที่ถูกพัฒนาขึ้นมานี้ยังสามารถพัฒนาต่อไปให้สมบูรณ์ได้ โดยการปรับเปลี่ยนฟังก์ชันการทำงานต่าง ๆ ดังนี้

- ด้านความสวยงาม เช่นการเพิ่มเติมทางด้านไอคอน (Icon) เพื่อให้ผู้ใช้มองภาพการทำงานได้ง่ายขึ้นกว่าเดิม
- ในฟังก์ชันของการมอนิเตอร์แพ็คเก็ตอาจจะมีการปรับให้เป็นลักษณะของการตรวจสอบแพ็คเก็ตในช่วงเวลาที่กำหนดและส่งค่าการมอนิเตอร์มาเป็นระยะ ๆ
- ลักษณะของแผนภูมิอาจจะปรับเปลี่ยนไปเป็นลักษณะอื่นได้ เช่นแผนภูมิแท่ง แผนภูมิเส้น เป็นต้น
- ในฟังก์ชันของการวิเคราะห์กฎอาจจะไม่ได้ทำแค่เพียงในระดับพื้นฐานเช่นปัจจุบัน คือการตรวจความซ้ำซ้อนของกฎ อาจจะเพิ่มเติมการทำงานให้สามารถทำในระดับสูงได้เช่น การวิเคราะห์ว่ากฎใดที่เป็นส่วนย่อยของกฎใดบ้าง เป็นต้น
- สำหรับการกำหนดเวลาการกรองอาจจะสร้างฟังก์ชันพิเศษให้กฎต่าง ๆ ถูกกระทำโดยอัตโนมัติในเวลาที่เรากำหนดไว้ เช่น การกำหนดวัน-เวลา เวลาเริ่มต้น เวลาสิ้นสุด และทุกช่วงเวลาใดบ้าง เป็นต้น

จากการทดลองใช้งานของโปรแกรมจะเห็นได้ว่า มันสามารถทำงานได้อย่างที่ต้องการ ตามฟังก์ชันการทำงานทั่วไป และฟังก์ชันที่เพิ่มเติมอย่างที่กล่าวไว้ในบทแรก ๆ อย่างไรก็ตามโปรแกรมนี้สามารถนำไปพัฒนาต่อได้เพื่อได้โปรแกรมที่สมบูรณ์มากขึ้นและเกิดประโยชน์มากที่สุด

บรรณานุกรม

Comer, Douglas E. 1995. **Internetworking with TCP/IP Vol. I.** London:Prentice-Hall.

Comer, Douglas E. 1997. **Computer Networks And Internets.** London:Prentice-Hall.

Flynt, Clif. 1999. **Tcl/Tk For Real Programmers.** USA:Acadaemic-Press.

"FreeBSD Handbook." 2000. [Online]. Available:http://www.freebsd.org/handbook/index.html

Lehey, Greg. 1996. **The Complete FreeBSD.** Third ed. Canada:Walnut-Creek.

Ousterhout, John K. 1994. **Tcl and the Tk Toolkit.** USA:Addison-Wesley.

"XFree86™:Home Page." 2000. [Online]. Available:http://www.XFree86.org/

ภาคผนวก

ก. แนะนำโปรแกรม

"IPFW" เป็นโปรแกรมควบคุมการทำงานของฟังก์ชันไอพีไฟร์วอลล์บนฟรีบีเอสดี ทำงานอยู่บนเอ็กซ์ฟรี86 และโปรแกรมนี้ถูกพัฒนาจากภาษาทีซีแอลและทูลคิดของทีซีแอล รวมถึงมีการนำ Tkpiechart มาใช้ด้วย

ข. การติดตั้ง

1) สร้างโฟล์เดอร์ /IPFW ไว้ในเส้นทาง /usr
2) คัดลอกไฟล์ต่าง ๆ ไปไว้ในโฟล์เดอร์ /IPFW
3) เรียกใช้โปรแกรมโดยใช้คำสั่ง
   - cd /usr/IPFW
   - wish8.0 main.tcl หรือพิมพ์ ./ipfw1.0

ค. ความต้องการของระบบ

1) FreeBSD Version 3.2 และ XFree86
2) ต้องมีการเซ็ทโหมดการทำงานของไฟร์วอลล์ในฟรีบีเอสดี สามารถดูได้จากคู่มือฟรีบีเอสดี
3) Tcl 8.0 และ Tk 8.0
4) Tkpiechart 5.3

ง. การใช้งานโปรแกรม

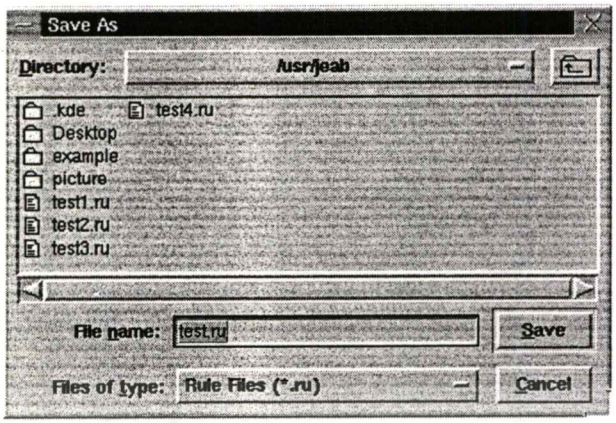
1) การทำงานเกี่ยวกับเมนู File ประกอบด้วยคำสั่งดังนี้
   - **New** การสร้างไฟล์กฎใหม่
   - **Open** การเปิดไฟล์กฎที่มีอยู่ขึ้นมา
   - **Save** การบันทึกไฟล์กฎ
   - **Close** การออกจากโปรแกรม
2) การทำงานเกี่ยวกับเมนู Add
   - **Add** การเพิ่มกฎในไฟล์กฎ

- **Update** การนำกฎที่ปรากฏอยู่บนหน้าจอไปไว้ในหน่วยความจำของไอพีไฟร์วอลล์ เพื่อให้กฎนี้ทำงาน

3) การทำงานเกี่ยวกับเมนู Configure
   - **List rule** การแสดงรายการของกฎ
   - **Delete rule** การลบกฎทีละหนึ่งรายการ
   - **Flush rule** การลบกฎทั้งหมด
   - **Clear counter** การลบค่าของตัวนับแพ็คเก็ต
4) การทำงานเกี่ยวกับเมนู Tools
   - **Scheduling** การตั้งเวลาการกรองแพ็คเก็ต
   - **Monitoring** การตรวจสอบจำนวนแพ็คเก็ตที่เข้ามา
   - **Policy Management** การจัดการนโยบาย แบ่งเป็นการสร้างนโยบายและการสร้างกลุ่มให้กับนโยบาย
   - **Direct Command** การทำคำสั่งของไอพีไฟร์วอลล์โดยตรง

จ. ตัวอย่างการใช้งานโปรแกรม

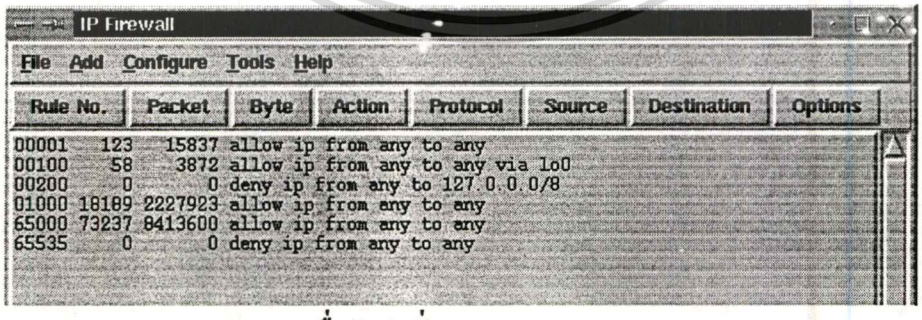
- ถ้าต้องการสร้างไฟล์กฎใหม่
  1. เลือกเมนู File แล้วเลือกคำสั่ง New
  2. เลือกเมนู Add แล้วเลือกคำสั่ง Add rule จะปรากฏหน้าต่างดังภาพที่ 4.22
  3. หลังจากนั้นผู้ใช้สามารถใส่รายละเอียดของกฎได้ตามที่ต้องการ และเมื่อใส่รายละเอียดของกฎเรียบร้อย ให้กดปุ่ม OK
  4. หลังจากการกดปุ่ม OK รายละเอียดของกฎดังกล่าวจะปรากฏยังหน้าจอหลัก และถ้าผู้ใช้ต้องการเพิ่มกฎก็สามารถกระทำต่อไปได้
  5. หลังจากการเพิ่มกฎเสร็จสิ้น ให้ผู้ใช้ทำการบันทึกไฟล์กฎดังกล่าว โดยการใช้คำสั่ง Save ที่อยู่ในเมนู File ดังภาพที่ จ.1



ภาพที่ จ.1 การบันทึกไฟล์กฎ

ภาพที่ จ.2 หน้าต่างที่ปรากฏเมื่อทำคำสั่ง Update สำเร็จ

- ถ้าต้องการนำกฎที่สร้างไปใช้โดยทันที สามารถกระทำหลังจากการบันทึกไฟล์กฎ หรือมีการเปิดไฟล์กฎอีกครั้ง
  1. เลือกเมนู Add แล้วเลือกคำสั่ง Update
  2. ผู้ใช้สามารถตรวจสอบการใช้คำสั่ง Update ได้โดยการใช้คำสั่ง List rule
  3. ผลที่ได้จากการใช้คำสั่ง List rule จะปรากฏดังภาพที่ จ.3

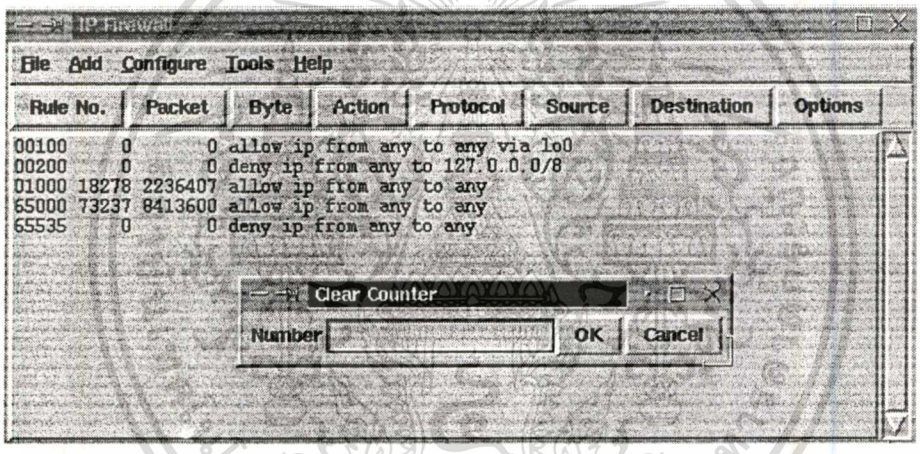


ภาพที่ จ.3 การแสดงรายการของกฎเมื่อทำคำสั่ง Update

- ถ้าต้องการลบกฎที่ทำงาน ณ ปัจจุบันออกไป
  1. เลือกเมนู Configure แล้วเลือกคำสั่ง Delete rule

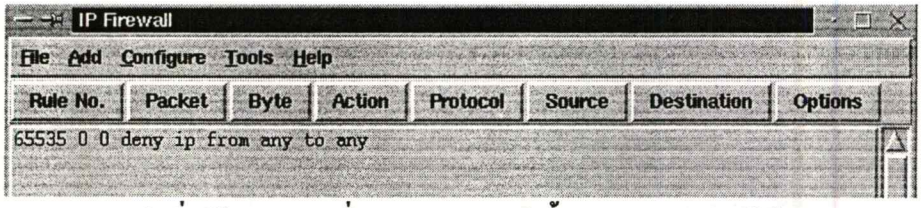
2. หลังจากเลือกคำสั่ง Delete rule จะปรากฏหน้าต่างดังภาพที่ 4.23 ผู้ใช้สามารถใส่เลขที่กฎที่ต้องการจะลบลงไป โดยเลขที่กฎสามารถดูได้จากคอลัมน์แรกในรายการของกฎที่ปรากฏอยู่

- ถ้าต้องการลบค่าตัวนับแพ็คเก็ตของกฎใดกฎหนึ่ง
  1. เลือกเมนู Configure แล้วเลือกคำสั่ง Clear counter
  2. หลังจากเลือกคำสั่ง Clear counter จะปรากฏหน้าต่างดังภาพที่ จ.4 ผู้ใช้สามารถใส่เลขที่กฎที่ต้องการลบค่าตัวนับแพ็คเก็ตลงไปได้ โดยที่เลขที่กฎสามารถดูได้จากคอลัมน์แรก ส่วนค่าของตัวนับแพ็คเก็ตให้ดูที่คอลัมน์ที่ 2 ในรายการของกฎที่ปรากฏอยู่



ภาพที่ จ.4 การลบค่าตัวนับแพ็คเก็ต

- ถ้าต้องการลบกฎทั้งหมด
  1. เลือกเมนู Configure แล้วเลือกคำสั่ง Flush rule
  2. หลังจากเลือกคำสั่ง Flush rule จะมีหน้าต่างปรากฏขึ้นมา ถ้าผู้ใช้เลือกปุ่ม OK หมายความว่า กฎที่ทำงานอยู่ทั้งหมดจะถูกลบออกไปแต่จะคงเหลือไว้แต่กฎที่เป็นค่าเริ่มต้นเท่านั้นดังภาพที่ จ.5



ภาพที่ จ.5 การแสดงค่าเริ่มต้นของกฎเมื่อรายการของกฎทั้งหมดถูกลบออกไป

- ถ้าต้องการตั้งค่าเวลาการกรอง
  1. ทำการเปิดไฟล์กฎขึ้นมาก่อน เลือกเมนู File แล้วเลือกคำสั่ง Open
  2. เลือกเมนู Tools แล้วเลือกคำสั่ง Scheduling ดังภาพที่ 4.25 ผู้ใช้สามารถบันทึกเวลาที่ต้องการจะให้กฎนี้ทำงาน ณ เวลาที่ต้องการได้ ตัวอย่างการบันทึกเวลาสามารถดูได้จากภาพที่ จ.6

```
01:01 1 Jan 2000
01/01/99
3:42am
noon tomorrow
now + 3 weeks
teatime
```

ภาพที่ จ.6 ตัวอย่างการบันทึกเวลาการกรอง

- ถ้าต้องการตรวจสอบดูจำนวนแพ็คเก็ต
  1. เลือกเมนู Tools แล้วเลือกคำสั่ง Monitoring
  2. การตรวจสอบดูจำนวนแพ็คเก็ตของโปรโตคอลไอพี ทีซีพีและยูดีพี สามารถดูได้จากภาพที่ 5.7

- ถ้าต้องการสร้างนโยบาย (แบบง่าย ๆ ในระดับโปรโตคอลไอพี) สามารถเข้าไปที่คำสั่ง Policy Management ในเมนู Tools คำสั่งนี้เหมือนเป็นโปรแกรมพิเศษหนึ่งที่สามารถจัดสร้างนโยบาย โดยนโยบายจะประกอบด้วยส่วนหลัก ๆ ดังนี้คือ การกระทำของกฎ กลุ่มต้นทาง และกลุ่มปลายทาง ดังนั้นการสร้างกลุ่ม 2 กลุ่มเพื่อให้มีความสอดคล้องกับการสร้างกฎในระดับของโปรโตคอลไอพีแบบง่ายอย่างที่กล่าวมา และนโยบายจำเป็นต้องมีการกระทำของกฎด้วย เพื่อจะได้ทราบว่ากลุ่มต้นทางและกลุ่มปลายทางมีการกระทำใดต่อกัน เช่น การอนุญาต และการปฏิเสธ เป็นต้น

  หน้าต่างของการสร้างนโยบายแสดงดังภาพที่ 4.27 และการสร้างกลุ่มจะแสดงดังภาพที่ 4.28 และก่อนการสร้างนโยบายจะต้องมีการสร้างกลุ่มก่อนทุกครั้ง ยกเว้นแต่ว่ากลุ่มนั้นได้มีการสร้างขึ้นมาไว้ก่อนแล้ว ในการสร้างกลุ่มสามารถที่จะทำการเพิ่มสมาชิกในกลุ่มและลบสมาชิกที่ไม่ต้องการออกได้ โดยใช้ปุ่ม Add และ Delete ที่อยู่ในหน้าจอดังภาพที่ 4.28 และหลังจากการรวบรวมสมาชิกของกลุ่มได้ จะต้องทำการบันทึกด้วย

เมื่อกลุ่มได้ถูกสร้างไว้เรียบร้อยแล้วอย่างน้อย 2 กลุ่ม ผู้ใช้สามารถที่จะสร้างนโยบายได้ โดยใช้กลุ่มดังกล่าว เมื่อผู้ใช้บันทึกชื่อกลุ่มที่ต้องการ ผู้ใช้สามารถตรวจดูสมาชิกของกลุ่มได้โดยกดปุ่ม OK ที่อยู่ใต้การบันทึกชื่อกลุ่ม (เหมือนกันทั้งกลุ่มต้นทางและกลุ่มปลายทาง) การบันทึกนโยบายสามารถกระทำได้โดยการกดปุ่ม Save Policy ในหน้าจอที่แสดงดังภาพที่ 4.27 การกระจายนโยบายเป็นกฎต่าง ๆ สามารถกระทำได้โดยการเลือกไปที่ปุ่ม Generate list rule จะทำให้กลุ่มของกฎที่มีการกระทำต่อกันกระจายเป็นกฎต่าง ๆ และผู้ใช้สามารถตรวจดูการกระจายกฎได้โดยการใช้คำสั่ง List rule

ประวัติผู้เขียน

ชื่อผู้เขียน	นางสาวสริตา ปรัชญาทิพย์
วันเดือนปีเกิด	21 เมษายน 2519
สถานที่เกิด	จ.จันทบุรี
วุฒิการศึกษาระดับปริญญาตรี	วท.บ. (วิทยาการคอมพิวเตอร์)
สถานที่สำเร็จการศึกษา	คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยหัวเฉียวเฉลิมพระเกียรติ
ปีที่สำเร็จการศึกษา	ปีการศึกษา 2540