บทที่ 4
การทดสอบระบบ

บทนี้กล่าวถึงผลในการดำเนินงานทั้งหมด โดยวิเคราะห์ปัญหา การออกแบบแนวทางการแก้ไข้ปัญหา ดำเนินการพัฒนาระบบต้นแบบ ทำการทดสอบระบบต้นแบบ และการวิเคราะห์ข้อมูล

4.1 ข้อมูลที่ใช้ในการทดสอบ

ข้อมูลที่ใช้ในการทดสอบจะเป็นข้อมูล ที่จัดเตรียมไว้ใช้ในการออกแบบกฎไฟร์วอลล์ เพื่อใช้ในการทดสอบการจำแนกข้อมูลของกฎนั้นๆ ในการอ่านกฎ

```
-A OUTPUT -p udp -o eth0 --dport 53 -j ACCEPT
-A INPUT -p udp -i eth0 --sport 53 -j ACCEPT
-A INPUT -i eth0 -p tcp --dport 25 -m state --state NEW,ESTABLISHED -j ACCEPT
-A OUTPUT -o eth0 -p tcp --sport 25 -m state --state ESTABLISHED -j ACCEPT
-A INPUT -i eth0 -p tcp --dport 143 -m state --state NEW,ESTABLISHED -j ACCEPT
-A OUTPUT -o eth0 -p tcp --sport 143 -m state --state ESTABLISHED -j ACCEPT
-A INPUT -i eth0 -p tcp --dport 110 -m state --state NEW,ESTABLISHED -j ACCEPT
-A OUTPUT -o eth0 -p tcp --sport 110 -m state --state ESTABLISHED -j ACCEPT
-A INPUT  -p tcp -m multiport --dports 22,80,443 -j ACCEPT
-A OUTPUT -p tcp -m multiport --sports 22,80,443 -j ACCEPT
-A OUTPUT -p tcp -d 192.168.100.0/24 --dport 22 -j ACCEPT
-A INPUT -p tcp -s 15.15.15.0/24 --dport 3306 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
-A OUTPUT -p tcp -d 157.240.0.0/16 -j DROP
-A INPUT -s 192.168.1.0/24 --dport 22 -j ACCEPT
-A INPUT -i enp0s3 -p tcp --dport 80 -m state --state NEW,ESTABLISHED -j ACCEPT
-A OUTPUT -o enp0s3 -p tcp --sport 80 -m state --state ESTABLISHED -j ACCEPT
-A INPUT -i enp0s3 -p tcp --dport 443 -m state --state NEW,ESTABLISHED -j ACCEPT
-A OUTPUT -o enp0s3 -p tcp --sport 443 -m state --state ESTABLISHED -j ACCEPT
```

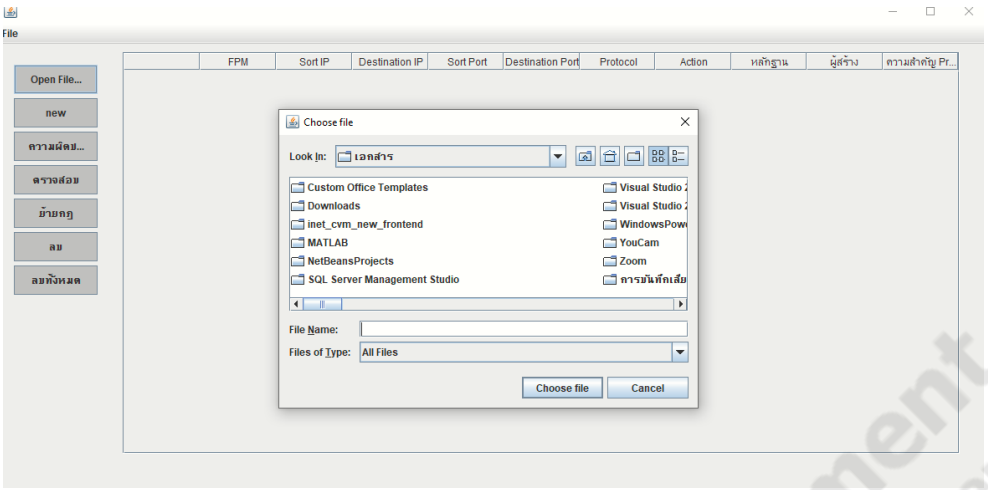
ภาพประกอบที่ 4.1 ตัวอย่างกฎไฟว์วอลล์ในการทดสอบ

4.2 ทดสอบระบบ

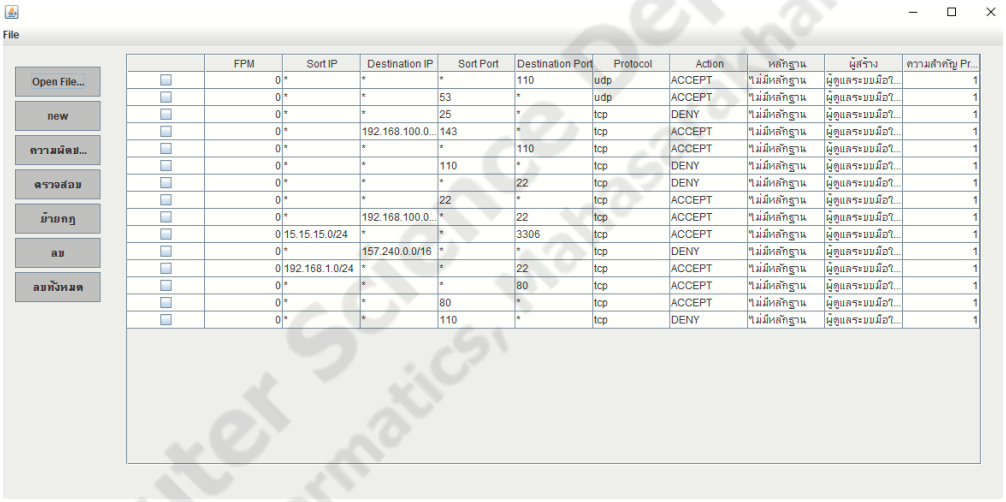
4.2.1 ทดสอบการแยก iPTabel

1. การอ่านข้อมูลจากไฟล์ txt

จะทำการทดสอบการอ่านไฟล์ข้อมูลจากไฟล์ txt ว่าโปรแกรมสสามารถจำแนกกฎไฟร์วอลล์แต่ละกฎได้หรือไม่ และทดสอบว่าสามารถแยก sort_ip destination_ip sort_port destination protocol และ action ของกฎนั้นๆ ได้อย่างถูกต้อง



ภาพประกอบที่ 4.2 การอ่านไฟล์ข้อมูลจากไฟล์ txt



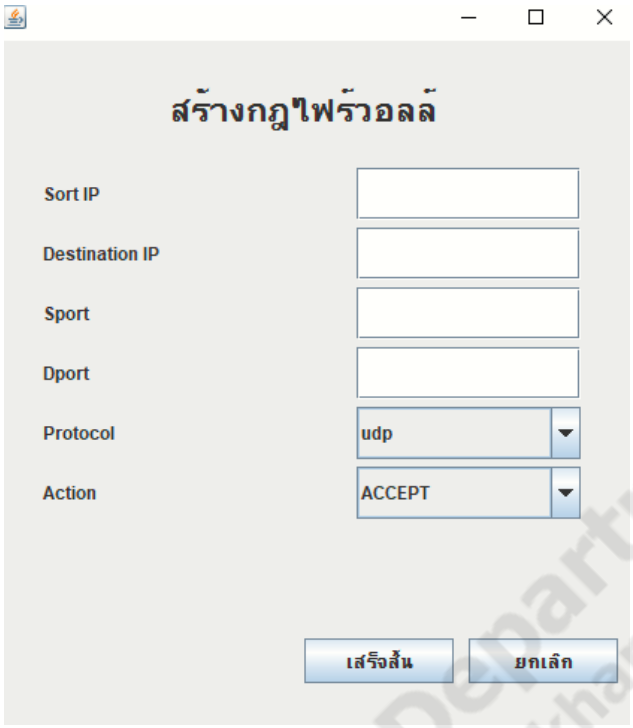
ภาพประกอบที่ 4.3 ไฟร์วอลล์ที่ทำการแยกข้อมูล

จากการทดสอบการอ่านไฟล์ข้อมูลในรูปแบบไฟล์ txt ข้อมูลที่นำมาใช้ต้องอยู่ในรูปแบบกฎ ดังภาพประกอบที่ 4.1 เท่านั้น โปรแกรมจึงจะสามารถ แยกประแภทของกฎไฟร์วอลล์ได้

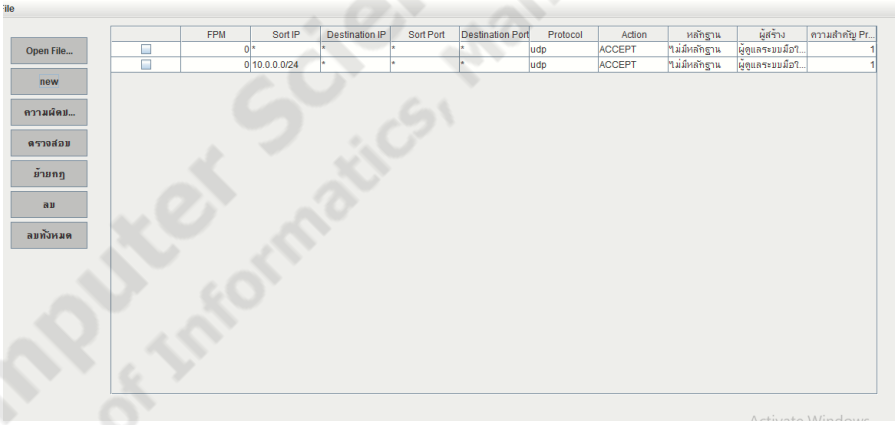
2. การสร้างกฎไฟร์วอลล์ขึ้นใหม่

สร้างกฎไฟร์วอลล์ขึ้นใหม่ โดยกฎไฟร์วอลล์ที่สร้างมีเงื่อนไขและข้อมูลที่ใช้ในการสร้างกฎ ดังภาพประกอบที่ 4.4 ทดสอบว่าหากไม่ทำการกรอกข้อมูลอะไรเลยของกฎไฟร์วอลล์ โปรแกรมจะยังสามารถสร้างกฎไฟร์วอลล์ให้ตรงตามเงื่อนไขหรือไม่

Computer Science Department
Faculty of Informatics, Mahasarakham University



ภาพประกอบที่ 4.4 ข้อมูลการสร้างกฎไฟร์วอลล์ขึ้นใหม่



ภาพประกอบที่ 4.5 กฎไฟร์วอลล์ที่สร้างขึ้นใหม่

จากการทอดสอบการสร้างกฎไฟร์วอลล์ขึ้นใหม่ของโปรแกรม พบว่ากฎที่ถูกสร้างขึ้นมาใหม่ถูกต้องตามเงื่อนไขของกฎไฟร์วอลล์ แต่ในการสร้างกฎไฟร์วอลล์ขึ้นมาใหม่พบว่าโปรแกรมไม่สามารถตรวจสอบความผิดพลาด หากผู้ใช้กรอกข้อมูลผิด โปรแกรมจะทำการ Retext ข้อมูลออกมาในรูปแบบที่ ผู้ใช้ทำการกรอก

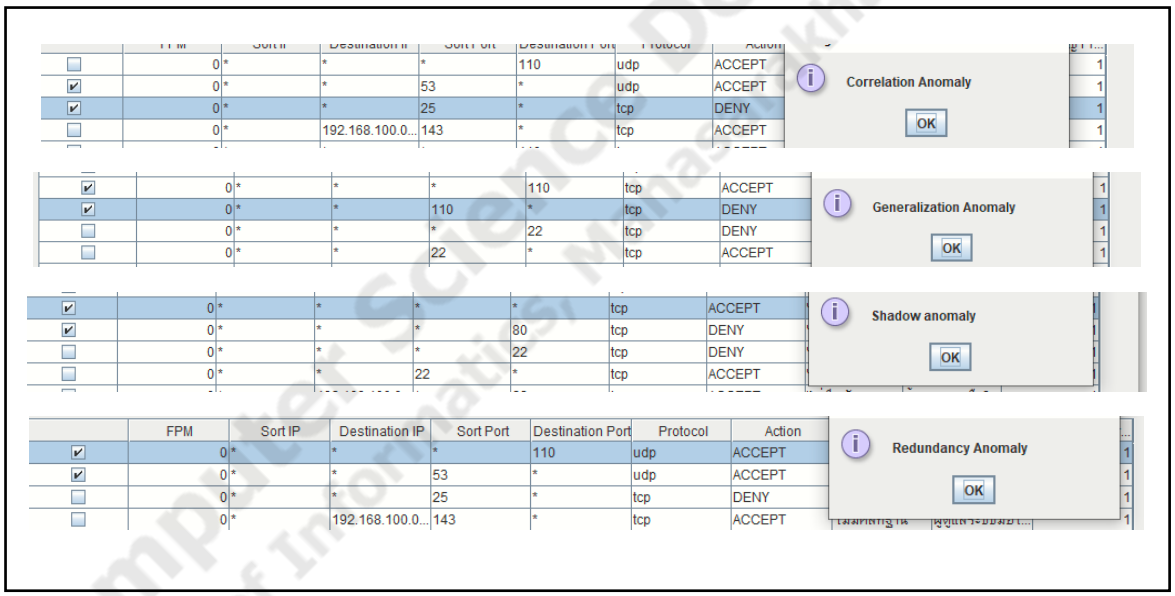
Computer Science Department
Faculty of Informatics, Mahasarakham University

4.2.2 ทดสอบหาความผิดปกติของกฎไฟร์วอลล์

ความผิดปกติของกฎไฟร์วอลล์จะแบ่งออกได้ 5 รูปแบบ

- Shodow
- Correlation
- Generalization
- Redundoncy
- Lrrelevance

โปรแกรมจะทำการตรวจสอบความผิดปกติของกฎไฟร์วอลล์ โดยการเช็คความผิดปกติของกฎที่ 1 และกฎที่ 2 ว่ากฎนั้นมีความขัดแย้งในรูปแบบใด



ภาพประกอบที่ 4.6 การเกิดความขัดแย้งการกฎไฟร์วอลล์

จากการทดสอบจะเห็นได้ว่าการทดสอบความผิดปกติของกฎไฟร์วอลล์ ไม่สามารถตรวจสอบความผิดปกติขของกฎในการตรวจสอบครั้งเดียว โปรแกรมนี้สามารถวัดความผิดปกติได้เพียงการจับคู่ของกฎระหว่างกฎเท่านั้น ดังภาพประกอบที่ 4.6

Computer Science Department
Faculty of Informatics, Mahasarakham University

4.2.3 ทดสอบการคำนวณความน่าจะเป็น

การคำนวณหาความน่าจะเป็น จะใช้ทฤษฎีของเบย์ (Bayes' theorem) เข้ามาช่วยในการตรวจสอบ โดยจะทำการนคุณสมบัติพิเศษ 4 แบบ เข้ามาใช้ในการออกแบบ และคำนวณ

ตารางที่ 4.1 คุณสมบัติพิเศษ

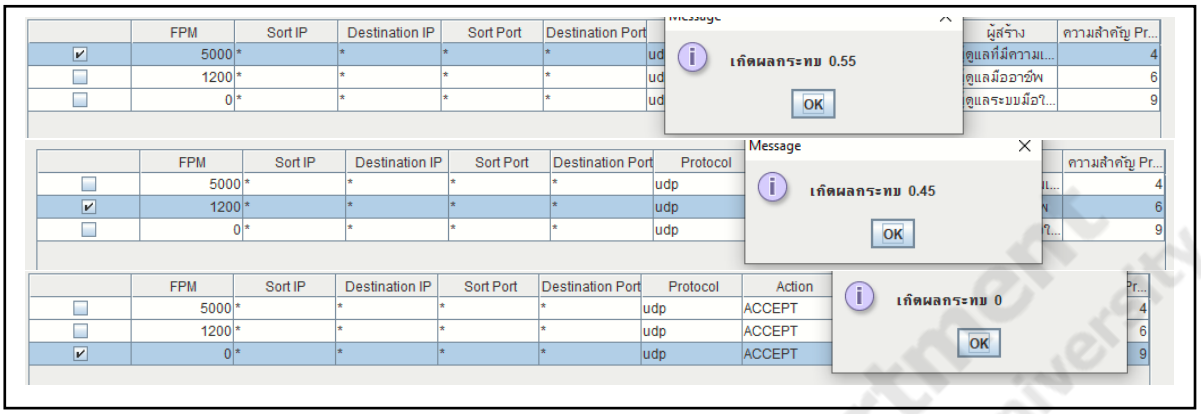
คุณสมบัติพิเศษ			
ความถี่ในการตกกระทบของกฎไฟร์วอลล์	**หลักฐานการสร้าง**	**ผู้สร้างกฎ**	**ความสำคัญของ Protocol**
ขึ้นอยู่กับกฎไฟร์วอลล์ที่เข้ามา	ไม่มีหลักฐาน (0)	ผู้ดูแลระบบมือใหม่ (0)	1-9
	ผู้ดูแลระบบ (1)	ผู้ดูแลระบบปกติ (1)	
	หัวหน้าแผนก (2)	ผู้ดูแลระบบมืออาชีพ (2)	
	เจ้าขององกร (3)	ผู้ดูแลระบบที่เชียวชาญมาก (3)	

ตารางที่ 4.2 แปลงคุณสมบัติ max-min

กฎที่	**ความถี่การตกกระทบ**	**หลักฐานการสร้าง**	**ผู้สร้างกฎ**	**ความสำคัญ Protocol**
R_1	5000	1	1	4
	1	0.33	0.33	0.625
R_2	1200	3	2	6
	0.24	1	0.67	0.25
R_3	0	0	0	9
	0	0	0	1
R_4	0	2	3	1
	0	0.67	1	9

Computer Science Department Faculty of Informatics, Mahasarakham University

หลักจากนำคุณสมบัติทั้ง 4 เข้าแปลงคุณสมบัติ max-min แล้วนั้น จะนำมาทดสอบกับระบบผลที่ได้ดังภาพประกอบที่ 4.6 คุณสมบัติที่กำหนดต่างกันผลลัพธ์ที่ได้ในการคำนวณก็มีค่าต่างกัน



ภาพประกอบที่ 4.7 การตรวจสอบความน่าจะเป็น

4.2.4 ทดสอบการแก้ไขความผิดปกติของกฎ

ระบบแนะนำเพื่อการแก้ไขความผิดปกติของกฎไฟร์วอลล์ การแก้ไขกฎไฟร์วอลล์ก่อให้เกิดผลกระทบระหว่างกฎด้วยกันอย่างมาก ซึ่งในระบบนี้สามารถดำเนินการแก้ไขกฎ โดยที่ผู้ใช้สามารถทำการแก้ไขกฎที่ขัดแย้งกันได้ ดังตารางที่ 3.4

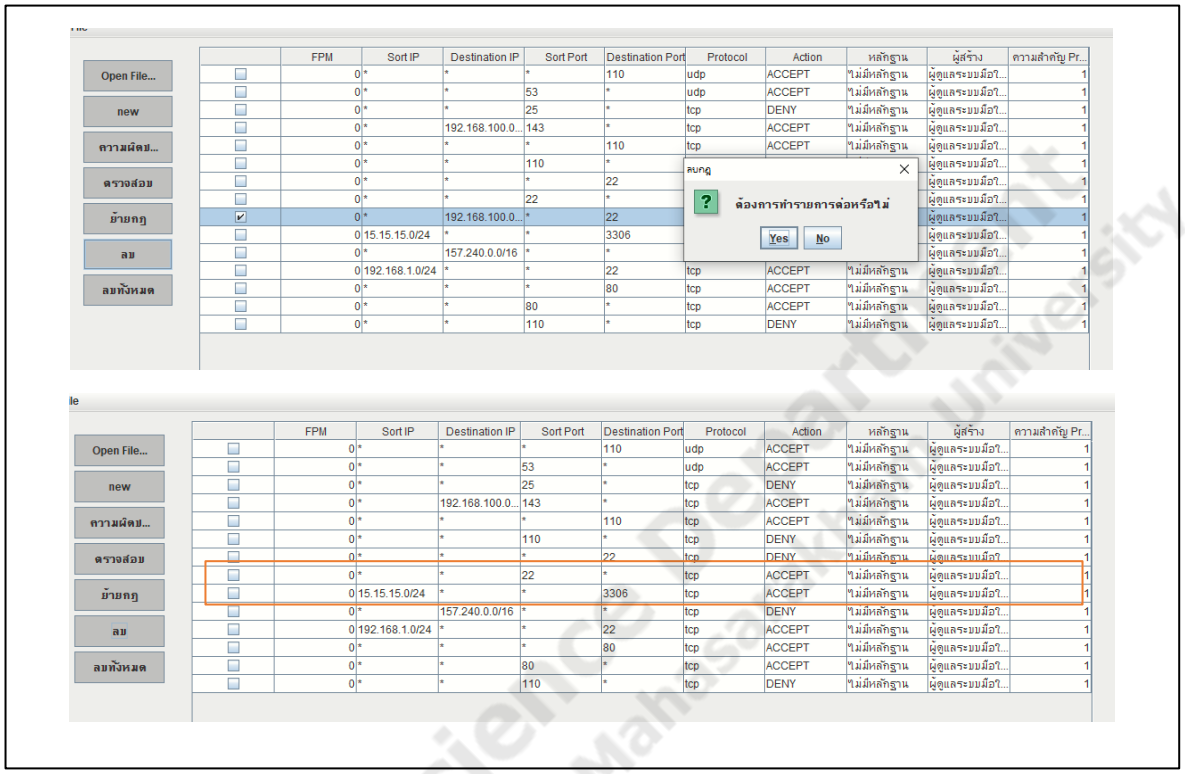
ตารางที่ 4.3 การแก้ไขกฎไฟร์วอลล์

การแก้ไขกฎฟร์วอลล์	**ความสามารถของระบบ**
การเพิ่มกฎ	ได้
การรวมกฎ	ไม่ได้
การลบกฎ	ได้
การย้ายกฎ	ได้

1. การลบกฎไฟร์วอลล์

การลบกฎไฟร์วอลล์ เป็นการนำกฎไฟร์วอลล์ที่มีอยู่แล้วออกไปจากระบบ ซึ่งผู้ดูแลระบบจะมีการนำเนินการหลังจากที่ทำการตรวจสอบความน่าจะเป็นในเงื่อไขนั้นๆ แล้ว โดยขั้นตอนการทำงานของระบบจะทำงานดังต่อไปนี้

Computer Science Department
Faculty of Informatics, Mahasarakham University



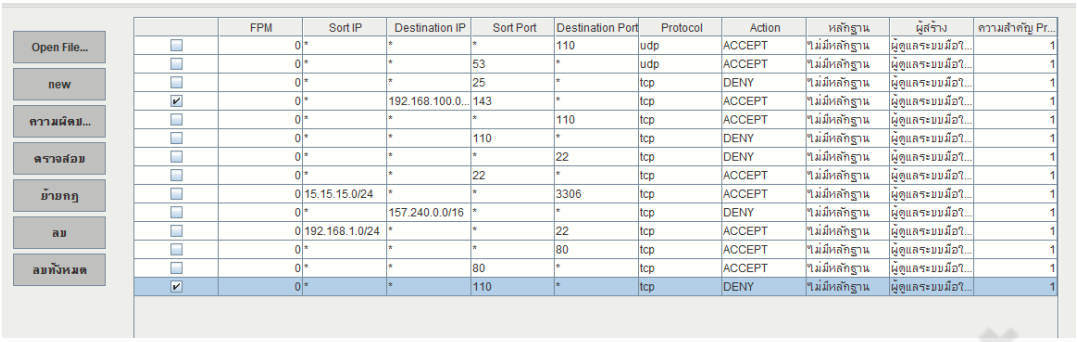
ภาพประกอบที่ 4.8 การลบกฎไฟร์วอลล์

การลบกฎไฟร์วอลล์จะสามารถดำเนินการทำงานโดยการเลือกกฎที่ต้องการ ลบ จากนั้นทำการคลิกที่ปุ่ม ลบ ระบบจะทำการลบกฎนั้นออกไปโดยทั้งที จากภาพประกอบที่ 4.8 จะเห็นได้ว่ากฎไฟร์วอลล์ที่อยู่ระหว่างเส้นสีแดงได้ถูกลบออกไปจากระบบเรียบร้อย

2. การย้ายกฎไฟร์วอลล์

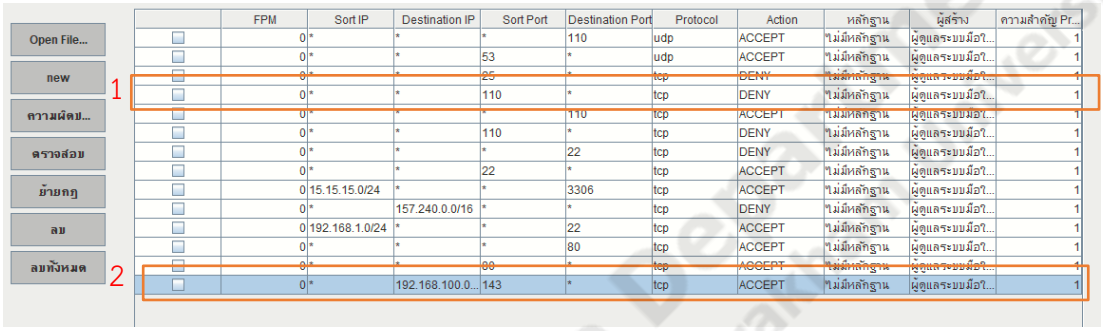
การย้ายกฎไฟร์วอลล์ จะต้องทำการเลือกกฎไฟร์วอลล์ 2 กฎ ดังภพประกอบที่ 4.9 จากนั้นให้ทำการคลิกที่ปุ่ม ย้ายกฎ ระบบจึงจะทำการย้ายกฎนั้นๆ ได้ โดยกฎที่ถูกเลือกจะทำการสรับกันระหว่างกฎนั้นๆ ตัวอย่างดังรูปประกอยที่ 4.10

Computer Science Department
Faculty of Informatics, Mahasarakham University



	FPM	Sort IP	Destination IP	Sort Port	Destination Port	Protocol	Action	หลักฐาน	ผู้สร้าง	ความสำคัญ Pr...
☐	0	*	*	*	110	udp	ACCEPT	ไม่มีหลักฐาน	ผู้ดูแลระบบมือใ...	1
☐	0	*	*	53	*	udp	ACCEPT	ไม่มีหลักฐาน	ผู้ดูแลระบบมือใ...	1
☐	0	*	*	25	*	tcp	DENY	ไม่มีหลักฐาน	ผู้ดูแลระบบมือใ...	1
☑	0	*	192.168.100.0...	143	*	tcp	ACCEPT	ไม่มีหลักฐาน	ผู้ดูแลระบบมือใ...	1
☐	0	*	*	*	110	tcp	ACCEPT	ไม่มีหลักฐาน	ผู้ดูแลระบบมือใ...	1
☐	0	*	*	110	*	tcp	DENY	ไม่มีหลักฐาน	ผู้ดูแลระบบมือใ...	1
☐	0	*	*	*	22	tcp	DENY	ไม่มีหลักฐาน	ผู้ดูแลระบบมือใ...	1
☐	0	*	*	22	*	tcp	ACCEPT	ไม่มีหลักฐาน	ผู้ดูแลระบบมือใ...	1
☐	0	15.15.15.0/24	*	*	3306	tcp	ACCEPT	ไม่มีหลักฐาน	ผู้ดูแลระบบมือใ...	1
☐	0	*	157.240.0.0/16	*	*	tcp	DENY	ไม่มีหลักฐาน	ผู้ดูแลระบบมือใ...	1
☐	0	192.168.1.0/24	*	*	22	tcp	ACCEPT	ไม่มีหลักฐาน	ผู้ดูแลระบบมือใ...	1
☐	0	*	*	*	80	tcp	ACCEPT	ไม่มีหลักฐาน	ผู้ดูแลระบบมือใ...	1
☐	0	*	*	80	*	tcp	ACCEPT	ไม่มีหลักฐาน	ผู้ดูแลระบบมือใ...	1
☑	0	*	*	110	*	tcp	DENY	ไม่มีหลักฐาน	ผู้ดูแลระบบมือใ...	1

ภาพประกอบที่ 4.9 การย้ายกฎไฟร์วอลล์



	FPM	Sort IP	Destination IP	Sort Port	Destination Port	Protocol	Action	หลักฐาน	ผู้สร้าง	ความสำคัญ Pr...
☐	0	*	*	*	110	udp	ACCEPT	ไม่มีหลักฐาน	ผู้ดูแลระบบมือใ...	1
☐	0	*	*	53	*	udp	ACCEPT	ไม่มีหลักฐาน	ผู้ดูแลระบบมือใ...	1
☐	0	*	*	25	*	tcp	DENY	ไม่มีหลักฐาน	ผู้ดูแลระบบมือใ...	1
☐	0	*	*	110	*	tcp	DENY	ไม่มีหลักฐาน	ผู้ดูแลระบบมือใ...	1
☐	0	*	*	*	110	tcp	ACCEPT	ไม่มีหลักฐาน	ผู้ดูแลระบบมือใ...	1
☐	0	*	*	110	*	tcp	DENY	ไม่มีหลักฐาน	ผู้ดูแลระบบมือใ...	1
☐	0	*	*	*	22	tcp	DENY	ไม่มีหลักฐาน	ผู้ดูแลระบบมือใ...	1
☐	0	*	*	22	*	tcp	ACCEPT	ไม่มีหลักฐาน	ผู้ดูแลระบบมือใ...	1
☐	0	15.15.15.0/24	*	*	3306	tcp	ACCEPT	ไม่มีหลักฐาน	ผู้ดูแลระบบมือใ...	1
☐	0	*	157.240.0.0/16	*	*	tcp	DENY	ไม่มีหลักฐาน	ผู้ดูแลระบบมือใ...	1
☐	0	192.168.1.0/24	*	*	22	tcp	ACCEPT	ไม่มีหลักฐาน	ผู้ดูแลระบบมือใ...	1
☐	0	*	*	*	80	tcp	ACCEPT	ไม่มีหลักฐาน	ผู้ดูแลระบบมือใ...	1
☐	0	*	*	80	*	tcp	ACCEPT	ไม่มีหลักฐาน	ผู้ดูแลระบบมือใ...	1
☐	0	*	192.168.100.0...	143	*	tcp	ACCEPT	ไม่มีหลักฐาน	ผู้ดูแลระบบมือใ...	1

ภาพประกอบที่ 4.10 กฎไฟร์วอลล์ที่ถูกย้าย

Computer Science Department
Faculty of Informatics, Mahasarakham University