บทที่ 5

บทวิจารณ์และสรุป

5.1 บทสรุป

เนื่องด้วยการรักษาความปลอดภัยในระบบเครือข่ายคอมพิวเตอร์ในปัจจุบันนั้น องค์กรทุกๆ องค์กรนั้นจะใช้ตัวไฟร์วอลล์ในการรักษาระบบความปลอดภัย ซึ่งเรียกได้ว่าระบบเครือข่ายนั้นจะขาดไฟร์วอลล์เสียไม่ได้ โดยเฉพาะไอพีเทเบิ้ลส์เป็นไฟร์วอลล์พื้นฐานที่มีอยู่ในระบบปฏิบัติการลินุกซ์ ซึ่งมีการใช้งานกันอย่างแพร่หลาย ด้วยเหตุผลนี้สิ่งสำคัญคือไฟร์วอลล์ควรจะทำงานได้อย่างมีประสิทธิภาพมากที่สุด

ไฟร์วอลล์เป็นโปรแกรมหนึ่งที่มีความสำคัญกับระบบคอมพิวเตอร์ การทำงานของไฟร์วอลล์จะทำงานโดยใช้กฎเพื่ออนุญาตหรือไม่อนุญาตการติดต่อจากเครื่องอื่นๆ โดยจะทำงานตามกฎจากบนลงล่าง ซึ่งกลุ่มผู้วิจัยได้มีการเล็งเห็นแล้วว่าหากมีกฎจำนวนมาก จะทำให้การทำงานต่างๆ ของไฟร์วอลล์นั้นทำงานช้าลง โดยโครงงานนี้จะศึกษาวิธีการต่างๆ ที่จะปรับปรุงการทำงานของไฟร์วอลล์ให้มีการทำงานที่เร็วขึ้น ซึ่งจะเน้นส่วนที่เป็นลำดับต่างๆ ของกฎในแต่ละตารางและด้านความซ้ำซ้อนต่างๆ ของกฎ ที่จะพิจารณาถึงความสัมพันธ์ของกฎที่ซ้ำซ้อนกันว่าสามารถลบออกไปได้หรือไม่ โดยไม่ให้มีผลกระทบต่อความหมายโดยรวมของกฎทั้งหมด

5.2 วิจารณ์สิ่งที่ได้จากโครงงาน

ไอพีเทเบิ้ลส์เป็นสเตรทฟูลไฟร์วอลล์ซึ่งในการตรวจสอบรายละเอียดของแพ็คเก็ตกับกฎของไฟร์วอลล์นั้น จะทำการตรวจสอบกับกฎด้านบนลงมาเรื่อยๆ จนถึงด้านล่างจนกว่าจะเจอกฎที่มีรายละเอียดตรงกับแพ็คเก็ตนั้นๆ เมื่อตรงกับกฎใดนั้นจะไปทำตามทาร์เก็ตฟังก์ชันของกฎนั้น ในการปรับปรุงความเร็วในการทำงานของไฟร์วอลล์นั้น ใช้หลักการตรวจสอบรายละเอียดแพ็คเก็ตของสเตรทฟูลไฟร์วอลล์มาใช้ในการปรับปรุง นั่นคือเมื่อแพ็คเก็ตตรงกับกฎนั้น ก็จะไปทำตามทาร์เก็ตฟังก์ชันของกฎนั้นๆ และจะไม่ทำการตรวจสอบกับกฎใดๆ ด้านล่างต่อไปอีกเลย ทำให้สามารถทำการลบกฎที่มีรายละเอียดและทาร์เก็ตฟังก์ชันของกฎซ้ำซ้อนกัน เนื่องจากกฎดังกล่าวจะไม่มีการนำไปใช้อย่าง

แน่นอนและเนื่องมาจากลักษณะการตรวจสอบกฎนั้นเป็นไปแบบจากบนลงล่างดังนั้นลำดับของกฎจึงมีความสำคัญ ถ้ากฎที่มีรายละเอียดตรงกับแพ็คเก็ตของข้อมูลที่มีปริมาณมากๆ อยู่ด้านล่างๆ ในการตรวจสอบกฎจะต้องผ่านกฎที่ไม่ได้เกี่ยวข้องจำนวนหนึ่งจนกว่าจะถึงกฎนั้นๆ การจัดลำดับของกฎโดยให้กฎที่มีการใช้งานบ่อยๆ มาอยู่ด้านบน จะลดเวลาในการตรวจสอบแพ็คเก็ตกับกฎลงได้มาก ยิ่งแพ็คเก็ตของข้อมูลยิ่งมีปริมาณมากเท่าไหร่จะยิ่งลดเวลาในการทำงานได้มากขึ้นไปอีก แต่ในการเคลื่อนย้ายกฎนั้นจะต้องไม่ทำให้ความหมายโดยรวมของกฎทั้งหมดนั้นยังไม่เปลี่ยนแปลง

5.3 ปัญหาอุปสรรคในการทำโครงงาน

1. ระบบปฏิบัติการลินุกซ์ เป็นระบบปฏิบัติการที่ไม่เป็นที่คุ้นเคยมากนัก ทำให้ต้องมีการใช้ระยะเวลาสักพักหนึ่งเพื่อเรียนรู้การติดตั้งและใช้งานเบื้องต้นรวมถึงคำสั่งต่างๆ ที่ใช้บ่อยๆ
1. ไฟร์วอลล์ไอพีเทเบิ้ลไม่มีส่วนที่อำนวยความสะดวกในการติดต่อกับโปรแกรม (API) ในการจัดการกับกฎ ทำให้เกิดปัญหาในการที่จะเขียนโปรแกรมให้เพิ่มลบหรือจัดลำดับของกฎตามที่ต้องการ
2. ในส่วนการตรวจจับเครือข่าย ไม่สะดวกที่จะแยกแพ็คเก็ตของข้อมูลตามวันและเวลาที่ต้องการ ในส่วนการเก็บรายละเอียดของล็อคไฟล์

5.4 แนวทางการพัฒนาต่อ

1. พัฒนาในส่วนของโปรแกรมให้มีส่วนติดต่อกับผู้ใช้และแสดงกฎของไฟร์วอลล์ที่มีอยู่ในขณะนั้นและมีการรวบรวมรายงานการเปลี่ยนแปลงพร้อมเหตุผลที่ทำการเปลี่ยนแปลงกฎนั้นๆ แก่ผู้ใช้งาน
2. พัฒนาการปรับปรุงความเร็วในการทำงานของไฟร์วอลล์มากกว่า 1 ตัว ให้มีการสื่อสารกันระหว่างไฟร์วอลล์ทั้ง 2 ตัว