บทที่ 6

สรุปผลการวิจัย

6.1 สรุปผลการวิจัย

"ไฟร์วอลล์" เป็นอุปกรณ์ที่มีบทบาทในการป้องกันภัยจากเครือข่ายภายนอก ก็คือ สำหรับองค์กรภายในเครือข่ายหนึ่ง อาจประกอบไปด้วยไฟร์วอลล์จำนวนมากซึ่งทำให้เกิดความยุ่งยากในการบริหารจัดการ หรือการจัดสรรกฎจำนวนมากลงในไฟร์วอลล์แต่ละตัว เพื่อให้สอดคล้องกับนโยบายความมั่นคงของไฟร์วอลล์ หรือการเปลี่ยนแปลงนโยบายในอนาคต ในวิทยานิพนธ์นี้จึงนำเสนอวิธีการ และขั้นตอนวิธี ที่เรียกว่า "Intra-Firewall Anomaly Discovery and Correction Algorithm" และ "Inter- Firewall Anomaly Discovery and Correction Algorithm" เพื่อค้นหาและแก้ไขความผิดปกติของกฎหากพบว่าเกิดความผิดปกติกรณีใดกรณีหนึ่งขึ้น สามารถนำไปประยุกต์ใช้ในการจัดสรรกฎตามนโยบายความมั่นคงได้โดยอัตโนมัติ และสามารถทวนสอบความถูกต้องของการจัดสรรกฎเหล่านั้นด้วย โดยอำนวยความสะดวกแก่ผู้ดูแลไฟร์วอลล์ในการปรับเปลี่ยนนโยบายตามความต้องการที่เปลี่ยนแปลงไปได้ตลอดเวลา เนื่องจากทุกครั้งที่มีการปรับเปลี่ยนนโยบาย กลุ่มของกฎต่างๆ ที่อยู่ในไฟร์วอลล์ก็จะถูกปรับเปลี่ยนใหม่ด้วยเสมอ

นอกจากนั้น วิทยานิพนธ์นี้ได้พิสูจน์ขั้นตอนวิธีเพื่อแสดงให้เห็นว่าด้วยวิธีการที่นำเสนอไม่ทำให้นโยบายความมั่นคงเปลี่ยนแปลง จำนวนของกฎในไฟร์วอลล์ลดลง และจำนวนครั้งของกลุ่มข้อมูลที่ลดลง เมื่อกลุ่มข้อมูลเดินทางผ่านไฟร์วอลล์ที่มีกลุ่มของกฎแบบใหม่ และเพื่อเป็นการทวนสอบจึงได้ทำการทดลองขึ้นเพื่อแสดงถึงการนำไปใช้ประโยชน์และประสิทธิภาพของงานวิจัยนี้ด้วยกลุ่มตัวอย่างจำนวน 75 กลุ่มข้อมูล สำหรับไฟร์วอลล์เดี่ยว และ 360 กลุ่มข้อมูลสำหรับไฟร์วอลล์แบบกระจาย เพื่อวิเคราะห์กระบวนการกรองกลุ่มข้อมูลของไฟร์วอลล์ในเครือข่ายซึ่งผลการทดลองมีความสอดคล้องกับทฤษฎีบท

การวิเคราะห์และการปรับเปลี่ยนความผิดปกติของกฎ สามารถนำไปปรับใช้ได้กับไฟร์วอลล์แบบ Proxy หรือ Application Gateway และแบบ Stateful Firewall ถ้ามีการเพิ่มความสามารถของขั้นตอนวิธีในส่วนที่ตรงกับการทำงานของไฟร์วอลล์ทั้งสองแบบ