บทที่ 5

การทดลอง

ในบทนี้เป็นการทดลองเพื่อค้นหาความผิดปกติและแก้ไขความผิดปกติด้วยวิธีการ และกระบวนการต่างๆ ที่ได้นำเสนอไว้ในวิทยานิพนธ์นี้เพื่อประเมินประสิทธิภาพและการนำไปใช้เพื่อให้เกิดประโยชน์สำหรับการบริหารจัดการไฟร์วอลล์ทั้งแบบไฟร์วอลล์เดี่ยวและไฟร์วอลล์แบบกระจายที่อยู่ในเครือข่าย

5.1 กลุ่มตัวอย่าง

ในการทดลอง ตัวอย่างของกลุ่มข้อมูล (Packet) ตามภาคผนวก ก ถูกสร้างขึ้นให้สอดคล้องกับกฎในไฟร์วอลล์ตามภาพที่ 4.1 และภาพที่ 4.2 ตามลำดับ โดยแบ่งออกเป็น 2 กลุ่ม ได้แก่

กลุ่มที่ 1 เป็นตัวอย่างกลุ่มข้อมูลที่จะใช้ทดลองกับไฟร์วอลล์เดี่ยว (Single firewall) จำนวน 75 กลุ่มข้อมูล

กลุ่มที่ 2 เป็นตัวอย่างกลุ่มข้อมูลที่จะใช้ทดลองกับไฟร์วอลล์แบบกระจาย (Distributed firewall) จำนวน 360 กลุ่มข้อมูล

ตัวอย่างกลุ่มข้อมูลที่สร้างขึ้นพิจารณาจากชุดกฎของนโยบายของไฟร์วอลล์นั้นว่ากฎเหล่านั้นสามารถกรองกลุ่มข้อมูลที่มาจากไอพีต้นทางและไปยังไอพีปลายทางใด และด้วยช่องทางใด โดยมีเส้นทางเครือข่าย (Network path) ที่เป็นไปได้ที่กลุ่มข้อมูลเดินทางผ่านอะไรบ้าง การจัดเส้นทางอธิบายไว้ในหัวข้อ 4.2.2 ซึ่งจะได้ว่า ถ้าเป็นไฟร์วอลล์เดี่ยวตามภาพที่ 3.1 จะมีเส้นทางเดียวระหว่างคู่ของไอพีต้นทางและไอพีปลายทาง จากนั้นเราจะสุ่มเลือกกลุ่มข้อมูลจำนวน 15 กลุ่มข้อมูล โดยใช้ 5 ช่องทาง ดังนั้นจะได้ตัวอย่างกลุ่มข้อมูลสำหรับไฟร์วอลล์เดี่ยวทั้งหมดจำนวน 75 กลุ่มข้อมูล ในขณะที่ถ้าเป็นไฟร์วอลล์แบบกระจายมีทั้งหมด 2 เส้นทาง แต่ละเส้นทางมี 4 คู่ของไอพีต้นทางและไอพีปลายทาง ทั้งหมดจึงมี 8 คู่ของไอพีต้นทางและไอพีปลายทาง จากนั้นสุ่มเลือกกลุ่มข้อมูลจากแต่ละคู่ของไอพีต้นทางและไอพีปลายทาง คู่ละ 9 กลุ่มข้อมูล โดยใช้ 5 ช่องทาง รวมกันเป็น 45 กลุ่มข้อมูลต่อคู่ ดังนั้นตัวอย่างของกลุ่มข้อมูลสำหรับไฟร์วอลล์แบบกระจายทั้งหมดจำนวน 360 กลุ่มข้อมูล

โปรแกรมที่ใช้ในการทดลองเขียนด้วยภาษาจาวา และทำงานบนเครื่องคอมพิวเตอร์ส่วนบุคคลซึ่งใช้ Pentium 4 CPU 3.0 GHz 3.01 GHz, 512 MB of RAM ขนาดฮาร์ดดิสก์ 80 GB ทำงานด้วยระบบปฏิบัติการ Microsoft Windows XP Professional, Version 2002 Service Pack 2

5.2 การทดลองที่ 1

5.2.1 วิธีการทดลอง

เป็นการศึกษาในสภาวะ 2 แบบ คือ ไฟร์วอลล์เดี่ยว และ ไฟร์วอลล์แบบกระจาย ว่าเมื่อกฎต่างๆ ในไฟร์วอลล์ถูกแก้ไขโดยอัตโนมัติโดยการผ่าน Intra-Firewall Anomaly Discovery and Correction Algorithm และ Inter-Firewall Anomaly Discovery and Correction Algorithm แล้ว ไฟร์วอลล์ทั้งสองแบบมีนโยบายความมั่นคงเดิม ขณะที่จำนวนของกฎในไฟร์วอลล์ลดลง ดังต่อไปนี้

1. นำกลุ่มของกฎเดิมที่อยู่ในไฟร์วอลล์เดี่ยวมาผ่าน Intra-Firewall Anomaly Discovery and Correction Algorithm และกลุ่มของกฎเดิมที่อยู่ในไฟร์วอลล์แบบกระจายมาผ่าน Inter-Firewall Anomaly Discovery and Correction Algorithm

2. ผลที่ได้จาก 1) จะได้กลุ่มของกฎแบบใหม่ในไฟร์วอลล์เดี่ยวจำนวน 6 กฎซึ่งลดลงจาก เดิม 3 กฎ (จำนวนกฎเดิมเท่ากับ 9) และในไฟร์วอลล์แบบกระจายจำนวน 24 กฎซึ่งลดลงจากเดิม 11 กฎ (จำนวนกฎเดิมเท่ากับ 35)

3. นำตัวอย่างที่เตรียมไว้แล้วทั้ง 2 กลุ่ม มาทดลองกับชุดของกฎแบบเดิม และชุดของกฎแบบใหม่ จากนั้นให้บันทึกจำนวนของกลุ่มข้อมูลที่ถูกยอมรับ (Allow) หรือ ถูกปฏิเสธ (Deny) ของชุดของกฎทั้งสอง

5.2.2 ผลการทดลอง

ผลปรากฏว่าไฟร์วอลล์เดี่ยวเมื่อใช้กลุ่มของกฎแบบเดิมและกลุ่มของกฎแบบใหม่กรองกลุ่มข้อมูลที่ผ่านไฟร์วอลล์นี้ ทั้ง 2 กลุ่มได้ผลเหมือนกัน คือกลุ่มข้อมูลถูกยอมรับจำนวน 20 กลุ่มข้อมูล (27%) และ ถูกปฏิเสธจำนวน 55 กลุ่มข้อมูล (73%) ดังตารางที่ 5.1

ตารางที่ 5.1 ผลการทดลองของกลุ่มข้อมูลที่ผ่านไฟร์วอลล์เดี่ยว

Action	Original Rules	Modified Rules	(%)
Allow	20	20	27
Deny	55	55	73
Total	**75**	**75**	**100**

ส่วนไฟร์วอลล์แบบกระจายกฎทั้ง 2 กลุ่มได้ผลเท่ากัน คือกลุ่มข้อมูลถูกยอมรับจำนวน 51 กลุ่มข้อมูล (14%) และ ถูกปฏิเสธจำนวน 309 กลุ่มข้อมูล (86%) ดังตารางที่ 5.2

ตารางที่ 5.2 ผลการทดลองของกลุ่มข้อมูลที่ผ่านไฟร์วอลล์แบบกระจาย

Action	Original Rules	Modified Rules	(%)
Allow	51	51	14
Deny	309	309	86
Total	**360**	**360**	**100**

สรุปได้ว่าทั้งไฟร์วอลล์เดี่ยวและไฟร์วอลล์แบบกระจายเมื่อชุดของกฎในไฟร์วอลล์ทั้ง 2 แบบถูกปรับเปลี่ยนอย่างอัตโนมัติโดยใช้ Intra-Firewall Anomaly Discovery and Correction Algorithm และ Inter-Firewall Anomaly Discovery and Correction Algorithm ตามลำดับแล้ว ไฟร์วอลล์ทั้ง 2 แบบยังคงมีนโยบายความมั่นคงเหมือนเดิม และเนื่องจากในแต่ละไฟร์วอลล์จำนวนของกฎลดลงดังหัวข้อ 5.2.1 ดังนั้นการทดลองที่ 1 นี้สอดคล้องกับการพิสูจน์ในทฤษฎีบท 1 ตามหัวข้อ 4.1.3

5.3 การทดลองที่ 2

5.3.1 วิธีการทดลอง

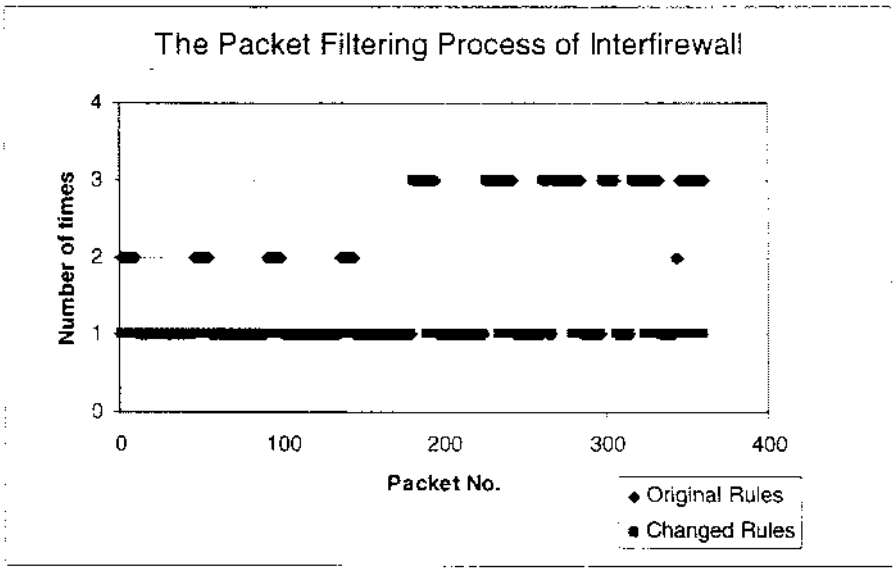
เพื่อเปรียบเทียบจำนวนครั้งของกลุ่มข้อมูลที่เดินทางผ่านไฟร์วอลล์ที่มีกลุ่มของกฎแบบเดิม กับ จำนวนครั้งของกลุ่มข้อมูลที่เดินทางผ่านไฟร์วอลล์ที่มีกลุ่มของกฎแบบใหม่ ซึ่งเป็นการทดลองสำหรับไฟร์วอลล์แบบกระจาย ดังนั้นตัวอย่างที่ใช้ในการทดลองที่ 2 นี้จึงใช้ตัวอย่างกลุ่มที่ 2 (จำนวน 360 กลุ่มข้อมูล) ดังนี้

1. นำกลุ่มข้อมูลทั้งหมด 360 กลุ่มข้อมูลทดสอบกับกลุ่มของกฎแบบเดิมและกลุ่มของกฎแบบใหม่ของไฟร์วอลล์

2. บันทึกจำนวนครั้งของกลุ่มข้อมูลที่ผ่านกลุ่มของกฎแบบเดิมและกลุ่มของกฎแบบใหม่

5.3.2 ผลการทดลอง

ผลจากการทดลองพบว่าจำนวนครั้งของกลุ่มข้อมูลที่ผ่านการกรองด้วยกลุ่มของกฎแบบใหม่ น้อยกว่าหรือเท่ากับ จำนวนครั้งของกลุ่มข้อมูลที่ผ่านการกรองด้วยกลุ่มของกฎแบบเดิม ดังภาพที่ 5.1



ภาพที่ 5.1 กราฟเปรียบเทียบจำนวนครั้งของกลุ่มข้อมูลที่เดินทางผ่านไฟร์วอลล์แบบกระจายที่มีกลุ่มของกฎแบบเดิม และกลุ่มของกฎแบบใหม่

สรุปได้ว่าการทดลองที่ 2 สำหรับในเครือข่ายที่มีไฟร์วอลล์มากกว่า 1 ไฟร์วอลล์บนเส้นทางเครือข่าย (Network path) เดียวกัน เราพบว่า จำนวนครั้งของกลุ่มข้อมูลที่เดินทางผ่านไฟร์วอลล์ที่มีชุดของกฎแบบใหม่ น้อยกว่าหรือเท่ากับ จำนวนครั้งของกลุ่มข้อมูลที่เดินทางผ่านไฟร์วอลล์ที่มีชุดของกฎแบบเดิม ซึ่งสอดคล้องกับที่การพิสูจน์ใน ทฤษฎีบท 2 ตามหัวข้อ 4.2.3

5.4 การทดลองที่ 3

5.4.1 วิธีการทดลอง

เป็นการทดลองสำหรับไฟร์วอลล์แบบกระจายใช้ตัวอย่างจำนวน 360 กลุ่มข้อมูล เพื่อเปรียบเทียบจำนวนของกลุ่มข้อมูลที่เดินทางผ่านไฟร์วอลล์ที่มีชุดของกฎแบบเดิมจำนวน 1 ครั้ง จำนวน 2 ครั้ง และจำนวน 3 ครั้ง กับ จำนวนของกลุ่มข้อมูลที่เดินทางผ่านไฟร์วอลล์ที่มีชุดของกฎแบบใหม่จำนวน 1 ครั้ง จำนวน 2 ครั้ง และจำนวน 3 ครั้ง ดังนี้

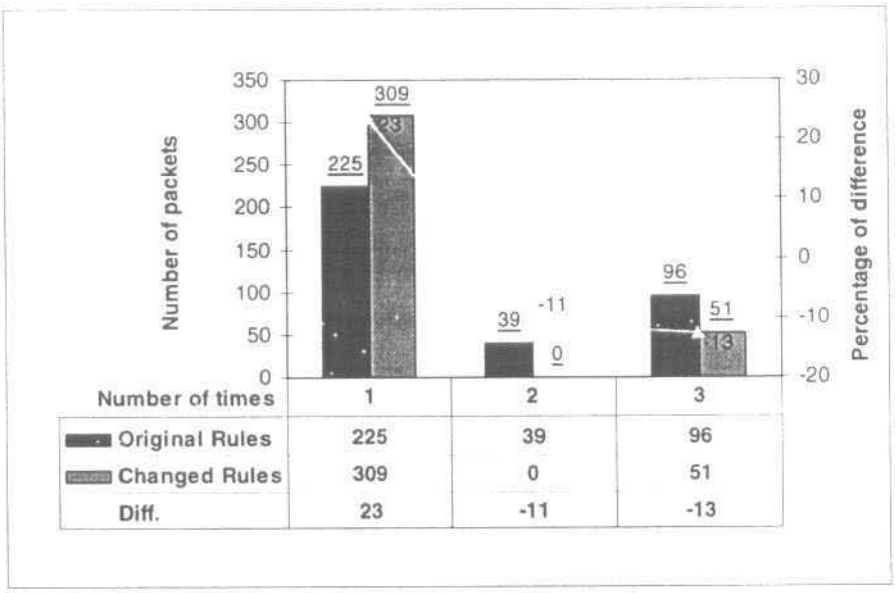
1. ใช้ตัวอย่างเดียวกับการทดลองที่ 2 จำนวน 360 กลุ่มข้อมูล โดยเราจะนำตัวอย่างที่เตรียมไว้ทดสอบกับการกรองกลุ่มข้อมูลด้วยชุดของกฎแบบเดิม และชุดของกฎแบบใหม่

2. บันทึกจำนวนของกลุ่มข้อมูลที่ถูกยอมรับและถูกปฏิเสธด้วยชุดของกฎแบบเดิมที่ผ่านไฟร์วอลล์ จำนวน 1 ครั้ง 2 ครั้ง และ3 ครั้ง (ไม่เกิน 3 ครั้ง เนื่องจากเป็นตัวอย่างของไฟร์วอลล์แบบกระจาย 3 ตัว) และชุดของกฎแบบใหม่ก็ทำเช่นเดียวกัน

5.4.2 ผลการทดลอง

ผลการทดลอง เราพบว่ากลุ่มข้อมูลที่ผ่านการกรองด้วยชุดของกฎแบบเดิม จากทั้งหมด 360 กลุ่มข้อมูล จะเดินทางผ่านไฟร์วอลล์ จำนวน 1 ครั้ง 225 กลุ่มข้อมูล จำนวน 2 ครั้ง 39 กลุ่มข้อมูล และจำนวน 3 ครั้ง 96 กลุ่มข้อมูล

ส่วนกลุ่มข้อมูลที่ผ่านการกรองด้วยชุดของกฎแบบใหม่ จากทั้งหมด 360 กลุ่มข้อมูล จะเดินทางผ่าน ไฟร์วอลล์ จำนวน 1 ครั้ง 309 กลุ่มข้อมูล ไม่พบจำนวน 2 ครั้ง และจำนวน 3 ครั้ง 51 กลุ่มข้อมูล ดังภาพที่ 5.2



Number of times	1	2	3
Original Rules	225	39	96
Changed Rules	309	0	51
Diff.	23	-11	-13

ภาพที่ 5.2 กราฟเปรียบเทียบจำนวนของกลุ่มข้อมูลที่เดินทางผ่านไฟร์วอลล์แบบกระจายที่ใช้ชุดของกฎแบบเดิม และชุดของของกฎแบบใหม่

ดังนั้นเราสามารถสรุปได้ว่ากลุ่มข้อมูลที่ผ่านการกรองด้วยกลุ่มของกฎแบบใหม่จะเดินทางผ่านไฟร์วอลล์ จำนวน 1 ครั้งเพิ่มขึ้น 23% จำนวน 2 ครั้งลดลง 11% และจำนวน 3 ครั้งลดลง 13% นั่นคือมีจำนวนกลุ่มข้อมูลที่ผ่านการกรองด้วยกลุ่มของกฎแบบใหม่ที่ผ่านไฟร์วอลล์จำนวน 1 ครั้ง มากกว่า และผ่านไฟร์วอลล์ จำนวน 2 ครั้ง และ 3 ครั้ง น้อยกว่า จำนวนกลุ่มข้อมูลที่ผ่านการกรองด้วยกลุ่มของกฎแบบเดิม นั่นคือกลุ่มข้อมูลที่ผ่านการกรองด้วยกลุ่มของกฎแบบใหม่จะเดินทางผ่านไฟร์วอลล์เป็นจำนวนน้อยครั้งกว่าหรือเท่ากับจำนวนครั้งที่เดินทางผ่านไฟร์วอลล์ของกลุ่มข้อมูลที่ผ่านการกรองด้วยกลุ่มของกฎแบบเดิม ซึ่งสอดคล้องกับที่การพิสูจน์ใน ทฤษฎีบท 2 ตามหัวข้อ 4.2.3 เช่นกัน

5.5 การทดลองที่ 4

5.5.1 วิธีการทดลอง

ศึกษาการเปรียบเทียบระหว่างการจัดสรรกฎด้วยขั้นตอนวิธีที่ 1 และ 2 และการจัดสรรกฎโดยขั้นตอนวิธีที่ 3 ว่าให้ผลลัพธ์เหมือนกัน ตามขั้นตอนต่อไปนี้

1. ให้ผู้ดูแลไฟร์วอลล์พิจารณานโยบายความมั่นคงที่ให้มาซึ่งประกอบด้วยกฎจำนวนหนึ่ง และจัดสรรกฎเหล่านั้นตามความชำนาญของผู้ดูแลไฟร์วอลล์ลงในไฟร์วอลล์ที่อยู่ในเครือข่าย โดยขณะที่ทำการเพิ่มกฎลงในไฟร์วอลล์จะต้องทำการค้นหาและแก้ไขความผิดปกติของกฎด้วยขั้นตอนวิธีที่ 1 และขั้นตอนวิธีที่ 2 ด้วย

2. นำกฎที่ถูกจัดสรรลงในไฟร์วอลล์ตามข้อ 1. มาสร้างเป็นนโยบายความมั่นคงชุดใหม่ และให้ใช้ขั้นตอนวิธีที่ 3 เพื่อจัดสรรกฎไปยังไฟร์วอลล์ต่างๆ

3. นำชุดของกฎที่ได้จาก 1. และ 2. มาเปรียบเทียบความแตกต่าง

5.5.2 ผลการทดลอง

ผลการทดลองปรากฏว่าชุดของกฎที่ได้จาก 1. และ 2. เหมือนกันทุกประการ แสดงว่าเราสามารถใช้ขั้นตอนวิธีที่ 1 และ 2 เพื่อแก้ไขความผิดปกติของกฎที่ผู้ดูแลไฟร์วอลล์เป็นผู้กำหนดให้ หรืออาจให้ผู้ดูแลไฟร์วอลล์กำหนดเป็นนโยบายความมั่นคงและใช้ขั้นตอนวิธีที่ 3 ในการจัดสรรกฎลงในไฟร์วอลล์แต่ละตัว