โปสเตอร์โครงงาน

Computer Science Department
Faculty of Informatics, Mahasarakham University

ระบบแนะนำเพื่อแก้ไขความผิดปกติของกฎไฟร์วอลล์
RECOMMENDATION SYSTEM TO RESOLVE THE FIREWALL RULE ANOMALIES

บทนำ

ไฟร์วอลล์เป็นเครื่องมือหรือระบบของระบบคอมพิวเตอร์ที่ทำหน้าที่ป้องกันเครือข่ายจากผู้ที่ไม่ได้รับ
อนุญาต ไม่ให้สามารถมาใช้หรือมองเห็นข้อมูลหรือเครือข่ายคอมพิวเตอร์ได้ ถือว่าเป็นระบบที่ทำหน้าที่รักษา
ความปลอดภัยสำหรับเครือข่ายคอมพิวเตอร์ที่มีความสำคัญยิ่ง เพราะไฟร์วอลล์สามารถตรวจสอบและป้องกัน
การบุกรุกหรือการโจมตีที่เป็นอันตรายต่อระบบเครือข่าย โดยขั้นตอนในการทำงานของระบบไฟร์วอลล์จะทำ
หน้าที่ตรวจสอบการบุกรุกหรือการโจมตีโดยการค้นหาความผิดปกติ โดยการเปรียบเทียบกฎที่ถูกกำหนดไว้
เมื่อตรวจสอบพบความผิดปกติของข้อมูล ไฟร์วอลล์ก็จะทำการปิดกั้นไม่ให้ข้อมูลเหล่านั้นผ่านไปได้ ในทาง
กลับกัน ถ้าข้อมูลที่ถูกตรวจสอบไม่มีสิ่งผิดปกติใด ๆ ไฟร์วอลล์ก็จะอนุญาตให้ข้อมูลเหล่านั้นผ่านไปทำงานที่
ต้องการได้
ป

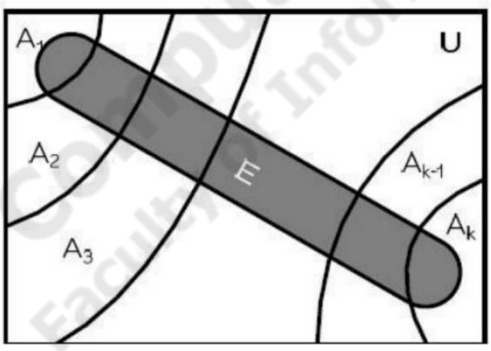
วัตถุประสงค์

ออกแบบและพัฒนาระบบเพื่อช่วยแนะนำการบริหารจัดการกฎที่แม่นยำขึ้น

ประโยชน์ที่คาดว่าจะได้รับ

1. เพื่อเพิ่มประสิทธิภาพการทำงานของกฎไฟร์วอลล์
2. ช่วยให้ผู้ดูแลระบบตัดสินเลือกกฎ อย่างมีเหตุผล
3. เพื่อช่วยแนะนำความผิดปกติของกฎไฟร์วอลล์

ทฤษฎีของเบย์(BAYES' THEOREM)



กฎไฟร์วอลล์

Rule-List A (Rule-3 shadowed by Rule-2)

order	Source IP	Dest. IP	Dest. Port	Action
1	10.0.0.1	20.0.0.1	80	ACCEPT
2	10.0.0.4 /30	20.0.0.5	23	ACCEPT
3	10.0.0.5	20.0.0.5	23	ACCEPT
4	any	any	any	DENY

Rule-List B (Rule-3 shadowed by Rule-1 and Rule-2)

order	Source IP	Dest. IP	Dest. Port	Action
1	10.0.0.1, 10.0.0.3	20.0.0.5	23	ACCEPT
2	10.0.0.5, 10.0.0.6	20.0.0.5	23	DENY
3	10.0.0.1, 10.0.0.6	20.0.0.5	23	ACCEPT
4	any	any	any	DENY

Rule-List C (Rule-3 shadowed by Rule-1 and Rule-2)

order	Source IP	Dest. IP	Dest. Port	Action
1	10.0.0.5	20.0.0.5	21, 25	ACCEPT
2	10.0.0.5	20.0.0.5	23 ,80	DENY
3	10.0.0.5	20.0.0.5	23, 25	ACCEPT
4	any	any	any	DENY

Rule-List D (Rule-3 shadowed by Rule-1 and Rule-2)

order	Source IP	Dest. IP	Dest. Port	Action
1	10.0.0.5	20.0.0.5	21-22	DENY
2	10.0.0.5	20.0.0.5	23-24	ACCEPT
3	10.0.0.5	20.0.0.5	22-23	ACCEPT
4	any	any	any	DENY

สรุป

การแก้ไขความผิดปกติของกฎที่ซ้ำซ้อนขึ้นอยู่กับผู้ดูแลระบบ ระบบนี้จัดทำขึ้นเพื่อเป็นการแนะนำการตัดสินใจในการแก้ไขกฎที่มากมาย โดยการให้คุณสมบัติ 4 อย่างมาช่วยในการหาความน่าจะเป็นที่ช่วยตัดสินใจ จัดการกับกฎที่ซ้ำซ้อนเหล่านี้

คุณสมบัติ 4 อย่าง

ความถี่ตกกระทบ
หลักฐานในการสร้างกฎ
ผู้ที่ทำการสร้างกฎ
Protocol

Computer Science Department
Faculty of Informatics, Mahasarakham University