สารบัญ

หน้า

บทคัดย่อ ..... ก
กิตติกรรมประกาศ ..... ข
สารบัญ ..... ค
สารบัญภาพประกอบ ..... จ
สารบัญตาราง ..... ซ
บทที่ 1 บทนำ 1
1.1 หลักการและเหตุผล 1
1.2 วัตถุประสงค์ของโครงงาน 1
1.3 ขอบเขตของโครงงาน 2
1.4 ภาพรวมของระบบ 3
1.5 ประโยชน์ที่คาดว่าจะได้รับ 4
1.6 อุปกรณ์และเครื่องมือที่ใช้ในการดำเนินงาน 5
1.7 แผนการดำเนินงาน 5
1.8 ตัวอย่างโปรแกรม 6
บทที่ 2 ทฤษฎีและงานวิจัยที่เกี่ยวข้อง 8
2.1 ทฤษฎีที่เกี่ยวข้อง 8
2.1.1 ไฟร์วอลล์ (Firewall) 8
2.1.2 ทฤษฎีของเบย์ (Bayes' theorem) 29
2.2 งานวิจัยที่เกี่ยวข้อง 34
บทที่ 3 วิธีดำเนินการวิจัย 35
3.1 นิยามกฎและความผิดปกติของกฎ 35
3.1.1 การปรับคุณสมบัติ Min-Max 38
3.1.2 ทฤษฎีของเบย์ 39
3.1.3 Moving Average (MA) 39
3.1.4 การแปลงที่อยู่ IP ให้เป็นจำนวนเต็มไม่ติดลบ 40
3.2 จุดเด่นของโครงงาน 40

สารบัญ (ต่อ)

หน้า

3.3 การออกแบบระบบ 41
3.3.1 การเตรียมไฟร์วอลล์ตามกฎ (ขั้นตอนที่ 1) 41
3.3.2 การวิเคราะห์และตรวจจับความผิดปกติ (ขั้นตอนที่ 2) 48
3.3.3 การคำนวณความน่าจะเป็นของแต่ละเส้นทางของ PST (ขั้นตอนที่ 3) 52
3.3.4 การเพิ่มประสิทธิภาพความผิดปกติของกฎ (ขั้นตอนสุดท้าย) 56
3.4 การใช้งาน PST และการประเมินผลการปฏิบัติงาน 59
3.5 สรุป 59
บทที่ 4 การทดสอบระบบ 61
4.1 ข้อมูลที่ใช้ในการทดสอบ 61
4.2 ทดสอบระบบ 61
4.2.1 ทดสอบการแยก iPTabel 61
4.2.2 ทดสอบหาความผิดปกติของกฎไฟร์วอลล์ 64
4.2.3 ทดสอบการคำนวณความน่าจะเป็น 65
4.2.4 ทดสอบการแก้ไขความผิดปกติของกฎ 66
บทที่ 5 สรุปผลและข้อเสนอแนะ 69
5.1 สรุปผลและอภิปรายผล 69
5.2 ปัญหาและอุปสรรค์ในการดำเนินงาน 69
5.3 ข้อเสนอแนะ 70
เอกสารอ้างอิง 71
ภาคแผนวก 73
ภาคแผนวก ก คู่มือการติดตั้ง 74
ภาคแผนวก ข คู่มือการใช้งาน 81
บทความวิจัย 86
โปสเตอร์โครงงาน 92
ประวัติย่อผู้จัดทำโครงงาน 94

สารบัญภาพประกอบ

หน้า

ภาพประกอบที่ 1.1 ภาพรวมระบบ 3
ภาพประกอบที่ 1.2 ตัวอย่างภาพหน้าหลัก 6
ภาพประกอบที่ 1.3 ตัวอย่างหน้าเพิ่มกฎ 7
ภาพประกอบที่ 1.4 ตัวอย่างหน้าแสดงเปอร์เซ็นต์การเกิดผลกระทบ 7
ภาพประกอบที่ 2.1 แสดงเส้นทางการเดินของ PACKET เมื่อเข้ามาในระบบ (FILTER TABLE) 10
ภาพประกอบที่ 2.2 ตัวอย่างของ LINUX FIREWALL LOG 12
ภาพประกอบที่ 2.3 การรวมกฎ 14
ภาพประกอบที่ 2.4 การยุบรวมกฎในรูปแบบของรีเลชัน 14
ภาพประกอบที่ 2.5 การยุบรวมโดยการย้าย RULE เข้ามาให้ชิดกันเสียก่อน 15
ภาพประกอบที่ 2.6 การยุบรวมโดยการแทรก CONSECUTIVE REDUNDANT RULE 15
ภาพประกอบที่ 2.7 ตัวอย่างของ RULE-LIST ที่มี SHADOWING ANOMALY 17
ภาพประกอบที่ 2.8 ตัวอย่างของ RULE-LIST ที่มี CORRELATION ANOMALY 18
ภาพประกอบที่ 2.9 ตัวอย่างของ RULE-LIST ที่มี GENERALIZATION ANOMALY 19
ภาพประกอบที่ 2.10 ตัวอย่างของ RULE-LIST ที่มี REDUNDANCY ANOMALY 20
ภาพประกอบที่ 2.11 แสดงโปรแกรมวิเคราะห์ LOG FILE 27
ภาพประกอบที่ 2.12 แสดงการแบ่งคลาสบนเครือข่ายอินเทอร์เน็ต 28
ภาพประกอบที่ 2.13 การใช้ VLSM ในการจัดสรรหมายเลข 4 IP Address ให้กับ WAN LinK 29
ภาพประกอบที่ 2.14 เหตุการณ์ E บนเหตุการณ์ K เหตุการณ์ที่เกิดพร้อมกันไม่ได้ 30
ภาพประกอบที่ 2.15 USING AN IP ADDRESS & PORT NAME 34
ภาพประกอบที่ 3.1 ความผิดปกติของกฎไฟร์วอลล์ 38
ภาพประกอบที่ 3.2 ภาพรวมของการออกแบบระบบ 41
ภาพประกอบที่ 3.3 การปรับทราฟฟิกแพ็กเก็ตให้ราบรื่นยิ่งขึ้นด้วย EMA 45
ภาพประกอบที่ 3.4 การสร้างกฎ $R_1(\mathrm{A}), R_2(\mathrm{B})$ และ $R_3(\mathrm{C})$ ลงใน PST 48
ภาพประกอบที่ 3.5 โครงสร้าง PST สมบูรณ์หลังจากรวบรวมกฎทั้งหมด 50
ภาพประกอบที่ 3.6 ความน่าจะเป็นแบบมีเงื่อนไขของ R ที่รู้ค่า E แสดงในเวนน์ไดอะแกรม 52
ภาพประกอบที่ 3.7 ความน่าจะเป็นที่มีเงื่อนไขของ R_i ที่ได้รับ e_k 53

สารบัญภาพประกอบ (ต่อ)

หน้า

ภาพประกอบที่ 3.8 การใส่ความน่าจะเป็นของแต่ละ Ri ลงใน PSD 56
ภาพประกอบที่ 3.9 การแก้ไขเงาโดยการสลับการรวมและการลบกฎ 58
ภาพประกอบที่ 3.10 การนำตัวชี้ไปยังต้นไม้ k-ary โดยที่ m = 4, L = 2 59
ภาพประกอบที่ 4.1 ตัวอย่างกฎไฟว์วอลล์ในการทดสอบ 61
ภาพประกอบที่ 4.2 การอ่านไฟล์ข้อมูลจากไฟล์ TXT 62
ภาพประกอบที่ 4.3 ไฟร์วอลล์ที่ทำการแยกข้อมูล 62
ภาพประกอบที่ 4.4 ข้อมูลการสร้างกฎไฟร์วอลล์ขึ้นใหม่ 63
ภาพประกอบที่ 4.5 กฎไฟร์วอลล์ที่สร้างขึ้นใหม่ 63
ภาพประกอบที่ 4.6 การเกิดความขัดแย้งการกฎไฟร์วอลล์ 64
ภาพประกอบที่ 4.7 การตรวจสอบความน่าจะเป็น 66
ภาพประกอบที่ 4.8 การลบกฎไฟร์วอลล์ 67
ภาพประกอบที่ ก-1 ไฟล์ ECLIQSE สำหรับติดตั้ง 75
ภาพประกอบที่ ก-2 เลือกตัวเลือกการติดตั้งโปรแกรม 75
ภาพประกอบที่ ก-3 ขั้นตอนการติดตั้งไฟล์ 76
ภาพประกอบที่ ก-4 ไอคอนโปรแกรม ECLIPSE 76
ภาพประกอบที่ ก-5 แสดงข้อความ ERROR ของโปรแกรม ECLIPSE 77
ภาพประกอบที่ ก-6 แสดงไฟล์ไฟล์ JDK.EXE 77
ภาพประกอบที่ ก-7 แสดงการติดตั้ง JDK ขั้นตอนที่ 1 78
ภาพประกอบที่ ก-8 แสดงการติดตั้ง JDK ขั้นตอนที่ 2 78
ภาพประกอบที่ ก-9 แสดงการติดตั้ง JDK ขั้นตอนที่ 3 79
ภาพประกอบที่ ก-10 แสดงการติดตั้ง JDK ขั้นตอนที่ 4 79
ภาพประกอบที่ ก-11 แสดงการติดตั้ง JDK ขั้นตอนที่ 5 80
ภาพประกอบที่ ก-12 แสดงการติดตั้ง JDK เสร็จสิ้นสมบูรณ์ 80
ภาพประกอบที่ ข-1 ตัวอย่างปรแกรมหน้าหลัก 81
ภาพประกอบที่ ข-2 ตัวอย่างโปรแกรมหน้าหลัก 83
ภาพประกอบที่ ข-3 ตัวอย่างการแสดงกฎไฟร์วอลล์ที่เข้ามา 84

สารบัญภาพประกอบ (ต่อ)

หน้า

ภาพประกอบที่ ข-4 ตรวจสอบความผิดปกติของกฎ 84
ภาพประกอบที่ ข-5 แจ้งการเกิดผลกระทบ 85

สารบัญตาราง

หน้า

ตารางที่ 1.1 แผนการดำเนินงาน 5
ตารางที่ 2.1 แสดง TCP/IP SERVICE ที่ควรปิดกั้นที่ไฟร์วอลล์ 23
ตารางที่ 2.2 แสดง TCP/UDP SERVICE ที่ควรปิดกั้นไม่ให้เข้ามาจากภายนอก 24
ตารางที่ 2.3 แสดง TCP/UDP SERVICE ที่อาจเปิดให้บริการใน DMZ 25
ตารางที่ 3.1 ฟิลด์สมาชิกพื้นฐานของ Ci และ Ai 42
ตารางที่ 3.2 ข้อมูลพิเศษของ Ri 43
ตารางที่ 4.1 คุณสมบัติพิเศษ 65
ตารางที่ 4.2 แปลงคุณสมบัติ MAX-MIN 65
ตารางที่ 4.3 การแก้ไขกฎไฟร์วอลล์ 66