การวิเคราะห์หาความขัดแย้งของกฎไฟร์วอลล์ กรณีศึกษามหาวิทยาลัยกาฬสินธุ์

นนทนันท์ จันทดวง[1], สุรยุทธ กีสาวัน[1], พรสวรรค์ ศิริกุล[1] และ อภิชัย สารทอง[2]

[1]สาขาเทคโนโลยีสารสนเทศ คณะเทคโนโลยีสังคม มหาวิทยาลัยกาฬสินธุ์ กาฬสินธุ์
[2]คณะเทคโนโลยีสังคม มหาวิทยาลัยกาฬสินธุ์ กาฬสินธุ์
Emails: nontanan99.as@gmail.com, arm_surayut141@hotmail.com, phonsawankarn1993@gmail.com, iapichais.th@gmail.com

บทคัดย่อ

การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อศึกษากฎการทำงานของไฟร์วอลล์ภายในมหาวิทยาลัยกาฬสินธุ์ที่ประกอบไปด้วยกฎที่หลากหลายและมีการทำงานที่ซับซ้อน จึงทำให้การทำงานอาจมีความล่าช้า ผู้จัดทำจึงได้หาแนวทางในการจัดการที่จะทำให้ไฟร์วอลล์มีการทำงานที่รวดเร็วมากยิ่งขึ้นโดยระบบความปลอดภัยไม่เปลี่ยนแปลงแต่เน้นเพิ่มประสิทธิภาพความรวดเร็วในการประมวลผล โดยใช้การวิเคราะห์หาข้อขัดแย้งใช้การปรับเปลี่ยนลำดับกฎใหม่โดยใช้กฎ Shadowing Anomaly, Correlation Anomaly, Generalization Anomaly และ Redundancy Anomaly เพื่อหาแนวทางและข้อเสนอแนะ ให้ทางหน่วยงานที่รับผิดชอบดังกล่าว นำไปประเมินใช้งานต่อไป

คำสำคัญ-- ไฟร์วอลล์, กฎไฟร์วอลล์, กฎที่ขัดแย้ง

ABSTRACT

The object of research to study the process of the internal firewall rules Case Study: Kalasin University. Therefore, it may be delayed of anomalies rule. to adjustment performance firewall rule. Without changing the security system, but the emphasis is on efficiency for fast processing. Using conflict analysis. Use the modify rules using shadowing Anomaly, Correlation Anomaly, Generalization Anomaly Redundancy Anomaly. Usual redundant characteristics common to fair practices and suggestions to the Network team responsible for such.

Keywords-- Firewall, Firewall rules, Rule anomalies

1. บทนำ

เมื่อกล่าวถึงมาตรการการรักษาความปลอดภัยบนเครือข่ายไฟล์วอลล์ เป็นระบบที่นักออกแบบระบบเครือข่ายให้ความสำคัญเป็นลำดับต้นๆ เนื่องจากไฟร์วอลล์มีคุณสมบัติที่สามารถป้องกันการเข้าถึงบริการบนระบบเครือข่ายได้เป็นอย่างดีโดยปกตินิยมติดตั้งไฟร์วอลล์ระหว่างทางเข้าออกขององค์กรกับเครือข่ายสาธารณะ สำหรับการตรวจสอบข้อมูลไฟร์วอลล์ จะทำการเปรียบเทียบข้อมูลที่ไหลผ่านตัวเองกับกฎที่ได้ถูกกำหนดไว้ หรือเรียกว่า Policy (โดยปกติจะเป็นหน้าที่ของผู้ดูแลระบบเครือข่าย) ข้อมูลทั้งหมดที่ผ่านเข้าและออกจากองค์กรจะต้องผ่านไฟร์วอลล์เสมอ ส่งผลให้ประสิทธิภาพโดยรวมของไฟร์วอลล์ จะขึ้นอยู่กับการบริหารจัดการกฎที่ดี เมื่อผู้ดูแลระบบขาดความรู้ ความเข้าใจในพฤติกรรมการทำงานขององค์กร จะส่งผลให้มีโอกาสสร้างกฎที่ผิดปกติได้หลายลักษณะ เช่น การสร้างกฎขัดแย้งกันเอง กฎมากเกินความจำเป็นและไม่ถูกใช้งาน สร้างกฎที่ซับซ้อนและเข้าใจได้ยาก หรือการจัดลำดับของกฎที่ไม่เหมาะสม จึงได้หาแนวทางในการจัดการที่จะทำให้ไฟร์วอลล์มีการทำงานที่รวดเร็วมากยิ่งขึ้น โดยระบบความปลอดภัยไม่เปลี่ยนแปลงแต่เน้นเพิ่มประสิทธิภาพความรวดเร็วในการประมวลผล โดยใช้การวิเคราะห์หาข้อขัดแย้งใช้การปรับเปลี่ยนลำดับกฎใหม่

2. วัตถุประสงค์ของโครงการ

1.เพื่อตรวจสอบประสิทธิภาพการทำงานของไฟร์วอลล์ ว่ามีการทำงานในรูปแบบไหน และมีความเร็วในการทำงานเท่าใด
2.เพื่อวิเคราะห์และนำเสนอแนวทางการปรับแก้ไขกฎ ที่จะทำให้ไฟร์วอลล์ ทำงานได้มีประสิทธิภาพมากขึ้น โดยมีความปลอดภัยในระบบเครือข่ายไม่ลดลง

3. ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

ความขัดแย้งของกฎไฟร์วอลล์ (Firewall rule anomalies) จากงานวิจัยของ Al-Shaer et al [5] มีด้วยกันหลายรูปแบบแต่มีจำนวน 4 รูปแบบที่พบปัญหามากที่สุด ดังนี้

1.Shadowing Anomaly คือ การที่กฎใดๆ ถูกบังโดยกฎอื่นอยู่ลำดับก่อนหน้า เมื่อทุกฟิลด์ของ Rule2 เป็นสมาชิกของ Rule1 ทั้งสองกฎมีผลการกระทำที่แตกต่างกัน

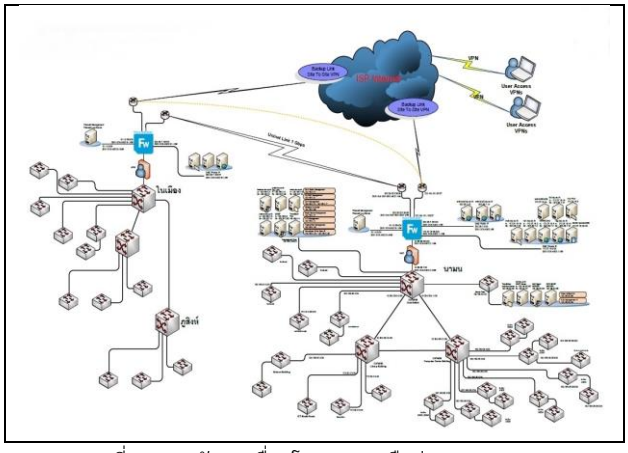
2.Correlation Anomaly คือ การที่กฎใดๆ มีการเกี่ยวพันกับกฎอื่น เมื่อบางฟิลด์ของ Rule1 เป็นสมาชิกของ Rule2 และมีบางฟิลด์ของ Rule2 เป็นสมาชิกของ Rule1 ทั้งสองกฎมีผลการกระทำที่แตกต่างกัน

3.Generalization Anomaly คือ การที่กฎใดๆ คลุมกฎอื่น เมื่อทุกฟิลด์ของ Rule1 เป็นสมาชิกของแต่ละฟิลด์บน Rule2 ทั้งสองกฎมีผลการกระทำที่แตกต่างกัน

4.Redundancy Anomaly คือ การที่กฎใดๆ ซ้ำซ้อนกับกฎอื่น เมื่อทุกฟิลด์ของ Rule1 เป็นสมาชิกของ Rule2 ทั้งสองมีผลการกระทำที่เหมือนกัน

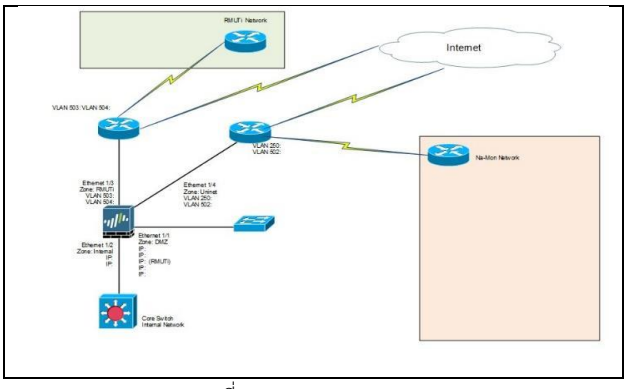
4. ปัญหาของระบบเดิม

จากการศึกษาระบบการทำงานของไฟร์วอลล์ในมหาวิทยาลัยกาฬสินธุ์ พบว่ามีการทำงานที่ช้าผิดปกติ เนื่องจากมีกฎที่ซ้ำซ้อนและมีกฎที่ถูกสร้างขึ้นมา แต่ไม่ได้นำมาใช้งาน นั่นเป็นสาเหตุหลักๆที่ทำให้ ไฟร์วอลล์ในมหาวิทยาลัยทำงานช้า ดังนั้นวิธีการแก้ไขจะมุ่งเน้นไปที่การปรับเปลี่ยนกฎที่ถูกสร้างขึ้นมา โดยทำการสลับกฎการทำงานของไฟร์วอลล์ และทดสอบว่ามีความเร็วในการทำงานเพิ่มขึ้นมากน้อยเพียงใด



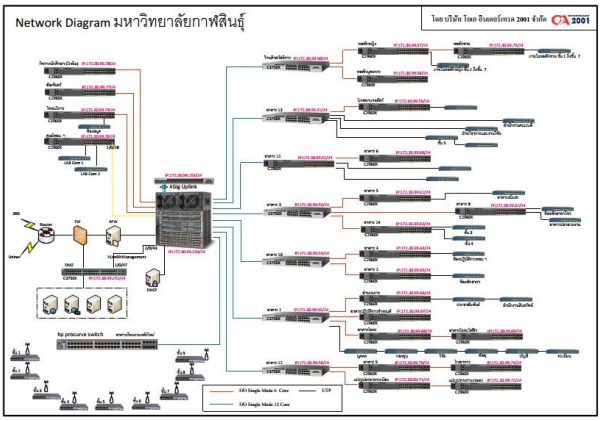
รูปที่ 1. แผนผังการเชื่อมโยงระบบเครือข่ายสารสนเทศ มหาวิทยาลัยกาฬสินธุ์
ที่มา www.ksu.ac.th

จากรูปที่ 1 เป็นแผนผังการเชื่อมโยงระบบเครือข่ายสารสนเทศ ซึ่งจะเห็นว่ามหาวิทยาลัยกาฬสินธุ์ จะมีสองวิทยาเขต ประกอบไปด้วย วิทยาเขตในเมือง และวิทยาเขตนามน มีระบบเครือข่ายที่เชื่อมถึงกัน



รูปที่ 2. Network Diagram
ที่มา www.ksu.ac.th

จากรูปที่ 2 เป็นภาพ Network Diagram ซึ่งบอกถึงการทำงานของระบบเน็ตเวิร์ก ว่ามีการส่งสัญญาณผ่าน Router ตัวไหน โดยมีการกำหนดช่องทางการส่งที่ชัดเจน



รูปที่ 3. Network Diagram KSU
ที่มา www.ksu.ac.th

จากรูปที่ 3 เป็น Diagram Network KSU ภายในมหาวิทยาลัยกาฬสินธุ์ จะเห็นได้ว่า มี switch หลายตัว ซึ่งถูกติดตั้งไว้ทุกอาคารโดยมีจุดศูนย์กลางการประมวลผลที่เครื่อง Server เมื่อมีการส่งออก หรือนำเข้าข้อมูล จะมีไฟร์วอลล์เป็นตัวตรวจสอบและดักจับข้อมูล เพื่อพิจารณาว่าปลอดภัยต่อระบบหรือไม่

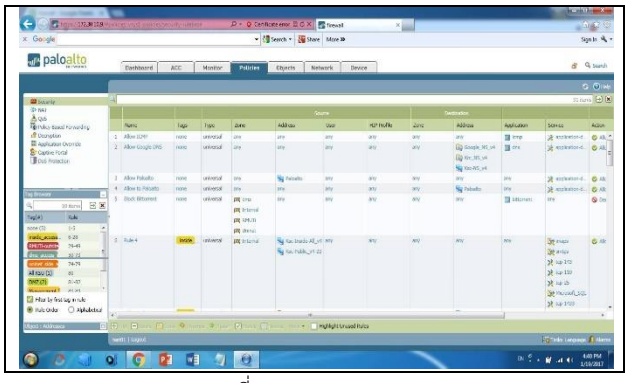
กระบวนการ Routing เป็นกระบวนการที่ใช้ในการเรียนรู้เส้นทางของเราท์เตอร์ เพื่อให้ส่งข้อมูลไปยังปลายทางได้อย่างถูกต้อง ซึ่งสามารถทำได้สองวิธีคือ static routing และ dynamic routing

Static routing เป็นวิธีที่ผู้ใช้หรือผู้ดูแลระบบต้องกำหนดค่าด้วยตนเอง โดยให้ข้อมูลที่เราท์เตอร์ต้องการเพื่อหาเส้นทาง ส่วนวิธี dynamic routing จะใช้ protocol ต่างๆในการเรียนรู้เส้นทางเกี่ยวกับ Subnet Address ต่างๆ จาก Router เพื่อนบ้าน ส่วนใหญ่ static routing ใช้การแก้ไขปัญหาเล็กๆหรือหลุมในเครือข่ายและใช้ในการเลือกเส้นทางสำรองเมื่อเส้นทางหลักล้มเหลว (floating static route) นอกจากนี้ยังสามารถใช้เพื่อกำหนดค่า default route ได้อีกด้วย ค่าหนึ่งที่สำคัญสำหรับการทำ static routing คือ Administrative Distance เป็นค่าที่กำหนดให้กับทุกๆประเภทของข้อมูลการหาเส้นทางที่เราท์เตอร์อาจจะได้รับ เพื่อใช้ในการเลือกหาเส้นทางที่ดีที่สุด ในกรณีที่มีเส้นทางมากกว่าหนึ่งเส้นทางที่ไปยังเครือข่ายปลายทางเดียวกัน

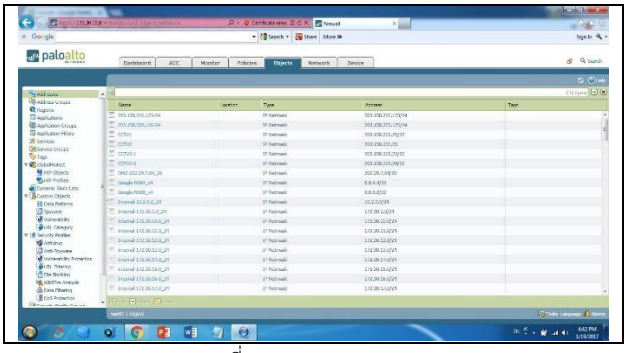
Distance Vector Protocols เป็นโปรโตคอลเส้นทางประเภทหนึ่งที่อยู่ใน dynamic routing การลู่เข้าอย่างช้าๆของ distance vector routing protocols สามารถก่อให้เกิดผลในตารางเส้นทางไม่แน่นอนและเกิดลูปของการหาเส้นทาง (routing loops) โปรโตคอลที่ในประเภทนี้คือ The Routing Information Protocol (RIP) และ Interior Gateway Routing Protocol (IGRP) ซึ่งกระบวนการ RIP ประกอบด้วย RIPv1 และ RIPv2 ส่วน IGRP เป็นโปรโตคอลซึ่งเป็นโปรโตคอลกรรมสิทธิ์ของ Cisco แต่ในปัจจุบันได้เลิกใช้ไปแล้ว

5. วิธีดำเนินการวิจัย

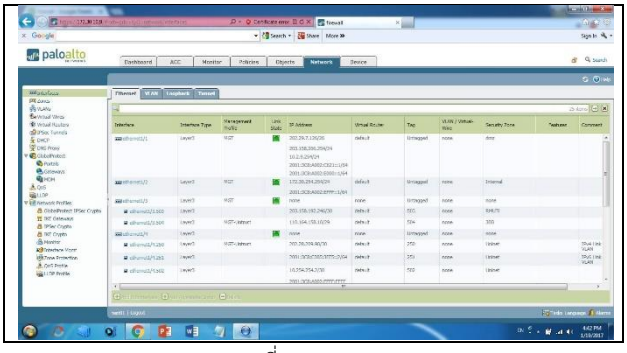
1. ศึกษากฎและการทำงานไฟร์วอลล์ของมหาวิทยาลัยกาฬสินธุ์
กฎการทำงานของไฟร์วอลล์มหาวิทยาลัยกาฬสินธุ์มีหลายหลาย ผู้วิจัยได้ศึกษาข้อมูลจากระบบภายในโดยตรง โดยหลักๆจะดูในส่วนของ Policy, Object และ Network



รูปที่ 4. Policy firewall



รูปที่ 5. Object Network



รูปที่ 6. Network

2. รวมรวมข้อมูล
รวบรวมข้อมูลที่ได้ มาขยายส่วนข้อมูล เพื่อให้ง่ายต่อการวิเคราะห์กฎการทำงานของไฟร์วอลล์

No	Name	Tags	Type	Source Zone	Enable	Destination Address	SOurce	แปลงจาก Destination	Prefix	Host
1	Allow ICMP	none	universal	any	1	202.97.7.126/255.255.242.0	any			
2	Allow Google DNS	none	universal	any	1	any	any			
3	Allow Paloalto	none	universal	any	1	Paloalto	any	172.30.10.9		
4	Allow to Paloalto	none	universal	any	1	any	any			
5	Block Bittorrent	none	universal	dmz		any	202.29.7.126/26			
				Internal	1		172.30.254.254/24			
				RMUTI	0		203.158.192.246/30			
				Uninet	0		202.28.209.98/30			
6	Rule 4	inside_access_in	universal	Internal		Ksc-Inside-All_v4	Internal-10.2.9.0_24		255.254.0.0	13
						Ksc-Public_v4-23		203.158.206.0/23	255.255.254.0	

รูปที่ 7. ขยายข้อมูลหน้า Policy

Address	Prefix	network วงไหนผ่านได้	HOST	Rule	Application	Acti
any					icmp	Allow
8.8.4.4 255.255.255.255	255.255.255.255	8.8.4.4			dns	Allow
Krc_NS_v4	255.255.255.255	203.158.206.1/32	1			
Ksc-NS_v4	255.255.255.255	203.158.206.1/32	1			
any					any	Allow
Paloalto		172.30.10.9			any	Allow
any					bittorrent	Deny
any					any	Allow

รูปที่ 8. ขยายข้อมูลหน้า Policy(ต่อ)

จากรูปที่ 7 และ 8 จะเห็นได้ว่าส่วนที่ขยายออกมานั้นจะประกอบไปด้วย Source, Destination, Prefix และ Host ซึ่งจะทำให้การวิเคราะห์กฎของไฟร์วอลล์ ดูได้ง่ายมากยิ่งขึ้น

Name	Location	Type	Address
Name		IP Netmask	203.158.206.123/24
Name		IP Netmask	203.158.206.126/24
CCTV1		IP Netmask	203.158.206.20/32
CCTV2		IP Netmask	203.158.206.25
CCTV2-1		IP Netmask	203.158.206.23/32
CCTV2-2		IP Netmask	203.158.206.24/32
DMZ-202.29.7.64_26		IP Netmask	202.29.7.64/26
Google-NS84_v4		IP Netmask	8.8.4.4/32
Google-NS88_v4		IP Netmask	8.8.8.8/32
Internal-10.2.9.0_24		IP Netmask	10.2.9.0/24
Internal-172.30.1.0_24		IP Netmask	172.30.1.0/24
Internal-172.30.10.0_24		IP Netmask	172.30.10.0/24
Internal-172.30.11.0_24		IP Netmask	172.30.11.0/24
Internal-172.30.12.0_24		IP Netmask	172.30.12.0/24
Internal-172.30.13.0_24		IP Netmask	172.30.13.0/24
Internal-172.30.14.0_24		IP Netmask	172.30.14.0/24
Internal-172.30.15.0_24		IP Netmask	172.30.15.0/24
Internal-172.30.16.0_24		IP Netmask	172.30.16.0/24
Internal-172.30.17.0_24		IP Netmask	172.30.17.0/24

รูปที่ 9. ส่วนขยาย Object

Interface	Template	Interfaces	Interface Type	Management Profile	Link State	IP Address
ethernet1/1		Slot 1	Layer3	MGT		202.29.7.126/26
						203.158.206.254/24
						10.2.9.254/24
						2001:3C8:A002:C621::1/64
						2001:3C8:A002:E000::1/64
ethernet1/2		Slot 1	Layer3	MGT		172.30.254.254/24
						2001:3C8:A002:EFFF::1/64
ethernet1/3		Slot 1	Layer3	MGT		none
ethernet1/3.503		Slot 1	Layer3			203.158.192.246/30
ethernet1/3.504		Slot 1	Layer3	MGT-Untrust		110.164.158.10/29
ethernet1/4		Slot 1	Layer3			none
ethernet1/4.250		Slot 1	Layer3	MGT-Untrust		202.28.209.98/30
ethernet1/4.251		Slot 1	Layer3			2001:3C8:C305:3FF5::2/64
ethernet1/4.502		Slot 1	Layer3			10.254.254.2/30
						2001:3C8:A002:FFFF:FFFF:FFFF:2:2/1
ethernet1/5		Slot 1				none
ethernet1/6		Slot 1				none
ethernet1/7		Slot 1				none
ethernet1/8		Slot 1				none
ethernet1/9		Slot 1				none

รูปที่ 10. ส่วนขยาย Network

Virtual Router	Tag	VLAN / Virtual-Wire	Virtual System	Security Zone
default	Untagged	none	vsys1	dmz
default	Untagged	none	vsys1	Internal
none	Untagged	none	vsys1	none
default	503	none	vsys1	RMUTI
default	504	none	vsys1	3BB
none	Untagged	none	vsys1	none
default	250	none	vsys1	Uninet
default	251	none	vsys1	Uninet
default	502	none	vsys1	Uninet
none	Untagged	none	none	none
none	Untagged	none	none	none
none	Untagged	none	none	none
none	Untagged	none	none	none
none	Untagged	none	none	none

รูปที่ 11. ส่วนขยาย Network(ต่อ)

3. นำทฤษฎีเข้ามาวิเคราะห์กฎการทำงานของไฟร์วอลล์ เพื่อหากฎที่มีความซ้ำซ้อน โดยใช้ทฤษฎี Shadowing Anomaly, Correlation Anomaly, Generalization Anomaly และ Redundancy Anomaly

Rule	S	C	G	R	สาเหตุ	IP ที่ซ้ำ 1	IP ที่ซ้ำ 2	IP ที่ซ้ำ 3
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14				1	ประกาศซ้ำกับกฎที่ 13	172.30.0.0/15	203.158.206.0/23	
15				1	ประกาศซ้ำกับกฎที่ 14	172.30.0.0/15	203.158.206.0/23	
16				1	ประกาศซ้ำกับกฎที่ 15	172.30.0.0/15	203.158.206.0/23	
17				1	ประกาศซ้ำกับกฎที่ 16	172.30.0.0/15		

รูปที่ 12. การวิเคราะห์กฎตามทฤษฎี

จากการวิเคราะห์กฎการทำงานของไฟล์วอลล์ 91 กฎ พบว่ามีกฎที่ขัดแย้งกันตรงกับทฤษฎีกฎข้อที่ 4 คือ Redundancy Anomaly ดังนั้นจึงทำการลบกฎที่ซ้ำซ้อนออกไป ซึ่งได้ลบกฎที่ 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 30, 31, 33, 35, 36, 37, 38, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 65, 66, 67, 68 และ

72 รวมทั้งหมดเป็น 45 กฎ คิดเป็นร้อยละ 50.55 เปอร์เซ็นต์ ซึ่งมีความปลอดภัยเท่าเดิม

5.1 วิเคราะห์ความเร็วในการทำงานของไฟล์วอลล์ก่อนการปรับเปลี่ยนกฎ

Rule	กฎที่ตรวจสอบ	เวลาที่ใช้ CPU (วินาที)
R1	Any	1
R2	Any	3
R3	Firewall	1
R4	Any	1
R5	Any	4
R6	Ksc-Inside-All_v4 Ksc-Public_v4-23	2
R7	Internal Network	1
R8	Internal Network	1
R9	Any	1
R10	Internal Network	1

รูปที่ 13. ระยะเวลาในการประมวลผลของไฟล์วอลล์ก่อนการปรับเปลี่ยนกฎ

เนื่องจากต้องการวัดความเร็วในการทำงานของไฟล์วอลล์ จึงได้อนุมานให้กฎการทำงาน มีหน่วยเป็นมิลลิวินาที ซึ่งจำนวนแต่ละมิลลิวินาที จะพิจารณาจากกฎแต่ละข้อ ว่ามีลำดับการทำงานมากน้อยเพียงใด โดยให้การประมวลผลในแต่ละขั้น มีระยะเวลาต่อหนึ่งมิลลิวินาที เพื่อให้เห็นผลต่างที่ชัดเจนเมื่อทำการลดความซ้ำซ้อนของกฎ

ยกตัวอย่างจากการเข้าใช้งาน www.sanook.com ซึ่งมี IP Address 203.151.129.168 โดยกฎของไฟล์วอลล์ จะเริ่มทำงานเรียงตามลำดับ ตั้งแต่ Rule1 ถึง Rule91 ซึ่งเว็บไซต์ www.sanook.com เข้าใช้งานได้เมื่อถึง Rule88 ดังนั้นจึงใช้สูตรหาเวลาในการรอคอย Average Waiting Time(AVG) โดยมีสมการดังนี้

$$AVG = \frac{R_1+R_2+\ldots+R_N}{\mathrm{N}} \qquad (1)$$

เมื่อ AVG คือ ผลรวมของระยะเวลาที่รอคอย

$R_1 \ldots R_N$ คือ ระยะเวลาการรอคอยเพื่อประมวลผลของแต่ละกฎ

N คือ จำนวนกฎทั้งหมดที่ประมวลผล

เมื่อแทนค่าเข้าไปในสมการแล้วจะได้ผลลัพธ์ดังนี้

$$AVG = \frac{R_1 + R_2 + R_3 + \ldots + R_{88}}{91}$$

$$AVG = \frac{1+3+1+\ldots+1}{91}$$

$$AVG = \frac{157}{91}$$

$$AVG = \frac{1.7}{1000} = 0.0017\ ms$$

จะได้ผลสรุปว่า เมื่อมีการเข้าถึง www.sanook.com จากภายในเครือข่ายของมหาวิทยาลัยกาฬสินธุ์ ได้มีระยะเวลาในการประมวลผลกฎของไฟล์วอลล์ อยู่ที่ 0.0017 มิลลิวินาที

5.2 วิเคราะห์ความเร็วในการทำงานของไฟล์วอลล์หลังการปรับเปลี่ยนกฎ

Rule	กฎที่ตรวจสอบ	เวลาที่ใช้ CPU (วินาที)
R13	Ksc-Inside-All_v4 Ksc-Public_v4-23	2
R14	Ksc-Inside-All_v4 Ksc-Public_v4-23	0
R15	Ksc-Inside-All_v4 Ksc-Public_v4-23	0
R16	Ksc-Inside-All_v4 Ksc-Public_v4-23	0
R17	Ksc-Inside-All_v4	0
R18	Ksc-Inside-All_v4 Ksc-Public_v4-23	0

รูปที่ 14. ระยะเวลาในการประมวลผลของไฟล์วอลล์หลังการปรับเปลี่ยนกฎ

ข้อมูลในตารางได้ทำการปรับเปลี่ยนระยะเวลาในการประมวลผลให้เท่ากับ 0 สำหรับกฎที่ได้ทำการลบออกไปทั้ง 49 กฎ ซึ่งจะส่งผลให้ไฟล์วอลล์มีการทำงานที่รวดเร็วยิ่งขึ้น โดยจะทำการทดสอบระยะเวลาในการทำงานด้วยสมการ AVG เช่นเดิม โดยทดสอบจากการเข้าถึง www.sanook.com ที่มีการปรับกฎเหลือเพียง 42 กฎ

เมื่อแทนค่าเข้าไปในสมการแล้วจะได้ผลลัพธ์ดังนี้

$$AVG = \frac{R_1 + R_2 + R_3 + \ldots + R_{88}}{42}$$

$$AVG = \frac{1+3+1+\ldots+1}{42}$$

$$AVG = \frac{63}{42}$$

$$AVG = \frac{1.5}{1000} = 0.0015\ ms$$

จะได้ผลสรุปว่า เมื่อมีการเข้าถึง www.sanook.com จากภายในเครือข่ายของมหาวิทยาลัยกาฬสินธุ์ ได้มีระยะเวลาในการประมวลผลกฎของไฟล์วอลล์ที่ได้มีการปรับเปลี่ยนกฎแล้ว อยู่ที่ 0.0015 มิลลิวินาที ซึ่งมีระยะเวลาน้อยกว่าครั้งแรก 0.0017-0.0015 = 0.0002 มิลลิวินาที

6. สรุปผลการวิเคราะห์

ผลจากการวิเคราะห์กฎการทำงานของไฟร์วอลล์ มหาวิทยาลัยกาฬสินธุ์ จากเดิมมีการประกาศกฎการทำงานไฟร์วอลล์ 91 กฎการทำงาน พบว่ามีความซ้ำซ้อนของกฎเกิดขึ้น และมีกฎที่ถูกประกาศขึ้นมา แต่ไม่ได้ถูกเรียกใช้งาน ซึ่งที่ได้กล่าวมานี้ส่งผลโดยตรงที่จะทำให้การทำงานของไฟร์วอลล์นั้นช้ามากขึ้น

7. สรุปผลการดำเนินงาน

ผลสรุปจากการวิเคราะห์กฎการทำงานของไฟร์วอลล มหาวิทยาลัยกาฬสินธุ์ นำกฎไฟร์วอล์ของมหาวิทยาลัยกาฬสินธุ์มาวิเคราะห์ขั้นตอนในการทำงานทีละกฎ เพื่อที่จะตรวจสอบหาความล่าช้าที่เกิดขึ้นส่วนมากเกิดจากกฎการทำงานแบบ Redundancy Anomalyและ Correlation Anomaly จากนั้นจะใช้ทฤษฎีในการวิเคราะห์กฎ และทำการปรับกฎเพื่อให้มีการทำงานที่รวดเร็วยิ่งขึ้น

เมื่อผู้วิจัยได้ทำการสลับกฎการทำงานของไฟร์วอลล์ตามทฤษฎี Shadowing Anomaly, Correlation Anomaly, Generalization Anomaly และ Redundancy Anomaly แล้วผลปรากฏว่าไฟร์วอลล์มีการทำงานที่รวดเร็วมากยิ่งขึ้นกว่าแต่ก่อน โดยที่ไม่ได้มีการลบหรือแก้ไข กฎเดิมแต่อย่างใด

ผลจากการวิเคราะห์กฎการทำงานของไฟร์วอลล์ มหาวิทยาลัยกาฬสินธุ์ ผู้จัดทำจึงได้ทำการวิเคราะห์ตามทฤษฎีของ Al-Shaer et al โดยพบว่าตรงตามกฎข้อ Redundancy และได้จัดเรียงกฎใหม่ จากเดิมมีการประกาศกฎการทำงานไฟร์วอลล์ 91 กฎการทำงาน พบว่ามีความซ้ำซ้อนของกฎเกิดขึ้นและมีกฎที่ถูกประกาศขึ้นมา จึงได้ลดความซ้ำซ้อนของกฎ เหลือ 42 กฎ หรือลดไป 46.15% ส่งผลให้ไฟล์วอลล์มีการทำงานเร็วขึ้น 0.0002 มิลลิวินาที

เอกสารอ้างอิง

[1] K. Golnabi, R. Min, L. Khan and E. Al-Shaer. "**Analysis of Firewall Policy Rules Using Data Mining Techniques.**" **In Proceedings of IEEE/IFIP Network Operations and Management Symposium**, Vancouver,Canada, pp. 305-315, April 2006.

[2] อธิพงศ์ คำสีลา. "**การปรับปรุงการจัดการกฎไฟร์วอลล์ด้วยแนวคิดการตัดสินใจแบบโดเมนเดี่ยว**". เทคโนโลยีสารสนเทศ ปีที่ 10, ฉบับที่2 (กรกฎาคม - ธันวาคม 2557). หน้า 1-3.

[3] A. Liu. "**Formal Verification of Firewall Policies.**" *In Proceedings of IEEE International Conference on Communications,* Beijing, China, pp. 1494-1498, May 2008.

[4] A. Bouhoula and Z. Trabelsi. "**Handling Anomalies in Distributed Firewalls.**" *In Proceeding of IEEE Innovations in Information Technology,* Dubai, United Arab emirates, pp. 1-5, November 2006.

[5] E. Al-Shaer and H. Harmed. "**Modeling and Management of Firewall Policies.**" *IEEE Transactions on Network and Service Management,* Vol. 1, Issue 1, pp. 2-10, April 2004.

[6] H. Hamed, A. El-Atawy and E. Al-Shaer. "**On Dynamic Optimization of Packet Matching in High-Speed Firewalls.**" *IEEE Journal on Selected Areas in Communications,* Vol. 24, Issue. 10, pp. 1817-1830, October 2006.

[7] สุชาติ คุ้มมะณี และจุรภรณ์ ตั้งมั่นดี. "**การจัดการกฎของไฟร์วอลล์แบบกึ่งอัตโนมัติ**" วารสารเทคโนโลยีสารสนเทศพระจอมเกล้าพระนครเหนือ (Information Technology Journal) ปีที่ 5 ฉบับที่ 9 มกราคม-มิถุนายน 2552, หน้า 8-17.

[8]จุรีภรณ์ ตั้งมั่นดี ปริญญา ระดาบุตร และ สุชาติ คุ้มมะณี. "**ประยุกต์ VLSM กับการตรวจสอบกฎของ ไฟล์วอลล์**" in In Proceedings of the Joint conference on Computer Science and Software Engineering (JCSSE). Kanjanaburi, Thailand. May 2008.