การพัฒนาระบบจัดการเครื่องลูกข่ายภายในเครือข่ายสัญญาณไร้สาย
DEVELOPMENT OF CLIENT MANAGEMENT IN THE WIRELRSS NETWORK

วรพล ระดมกิจ[1], ณัฐชามญฑ์ ศรีจำเริญรัตนา[2], กายรัฐ เจริญราษฎร์[1*]
Worapon Radomkit[1], Natchamol Srichumroenrattana[2], Kairat Jaroenrat[1*]

[1]ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ กำแพงแสน มหาวิทยาลัยเกษตรศาสตร์
[1]Department of Computer Engineering, Faculty of Engineering at KamphaengSaen, Kasetsart University
[2]โปรแกรมวิชาคอมพิวเตอร์ธุรกิจ คณะวิทยาการจัดการ มหาวิทยาลัยราชภัฏนครปฐม
[2] Business Computer Program, Faculty of Management Science, NakhonPathom Rajabhat University
[*]Corresponding author, E-mail: kairat.j@ku.ac.th

บทคัดย่อ

ในปัจจุบันการให้บริการอินเตอร์เน็ตไร้สายมีการให้บริการอย่างแพร่หลาย เนื่องจากการใช้งานที่สามารถเชื่อมต่อแบบไร้สายได้โดยง่ายและสะดวกสบายในทุกสถานที่ การเข้าถึงเว็บไซต์ต่างๆ จึงสามารถเข้าถึงได้อย่างไม่มีขีดจำกัด เมื่อเชื่อมต่อได้แล้วทุกคนจะสามารถเข้าเว็บไซต์ใดๆ ก็ได้ตามที่ต้องการ ผู้วิจัยจึงมีแนวคิดที่จะจำกัดการใช้งานเว็บไซต์ของผู้ใช้ โดยจำกัดขอบเขตการใช้งานเว็บไซต์ตามที่ผู้ดูแลกำหนดว่าเว็บไซต์ใดที่ไม่ต้องการให้เข้าถึง ด้วยการใช้หลักการดักจับข้อมูลแพคเกตภายในระบบเครือข่าย แล้วนำข้อมูลดังกล่าวมาใช้ในการจัดการระบบ หลังจากนั้นจึงทำการทดสอบประสิทธิภาพการทำงานของระบบในการจัดการเครื่องลูกข่าย ซึ่งพบว่ามีการทำงานได้อย่างรวดเร็วในการจำกัดการทำงานของเครื่องลูกข่ายไม่ให้ใช้งานเว็บไซต์ที่ถูกกำหนดว่าห้ามเข้าใช้งาน เมื่อมีเครื่องลูกข่ายเข้าใช้งานเว็บไซต์ดังกล่าว เครื่องลูกข่ายนั้นจะถูกปิดกั้นสัญญาณอินเตอร์เน็ตในระยะเวลาที่กำหนด โดยจะสามารถใช้งานได้หลังจากหมดสิ้นเวลาที่กำหนด และถูกบันทึกไว้ในรายงานของระบบ

คำสำคัญ: เอสเอ็นเอ็มพี เอสเอ็นเอ็มพีวอล์ค การตรวจสอบการทำงานของเซิร์ฟเวอร์

ABSTRACT

Presently, the wireless internet access is widely available. Due to the current Internet can connect to the Internet wirelessly with ease and comfortable in any place, access to various sites can be accessed without limitation. Anyone can access any site which they want. We had an idea to limit the user's access by limiting the scope of the site which administrator's policy. Our research's concept is to capture the packets in the network management system. After that, we do the performance test of the system and see that the system can quickly block the client from surfing the site which was blocked. When clients access to the blocked site, they also blocked to access the whole Internet. But they can surf the Internet again after the punishment period and their violation will report to the administrator.

Keywords: SNMP, snmpwalk, Server Monitoring

บทนำ

เทคโนโลยีการสื่อสารในปัจจุบันก้าวหน้าและพัฒนาไปอย่างมาก จึงเกิดเทคโนโลยีใหม่ๆ เกิดขึ้นเพื่ออำนวยความสะดวกในการติดต่อสื่อสาร เช่น WiFi, WiMax, 3G และ 4G เป็นต้น (วิกิพีเดีย, 2555ข) ทำให้ผู้คนที่อยู่ห่างกันข้ามโลกสามารถติดต่อสื่อสารกันได้อย่างง่ายดายเสมือนว่าอยู่ใกล้กัน การสื่อสารกันโดยใช้การเครือข่ายสัญญาณไร้สายเพิ่มจำนวนมากขึ้น อาจกล่าวได้ว่า ในปัจจุบันนี้ ไม่ว่าสถานที่ใดก็ตามจะมีการสื่อสารกันโดยใช้สัญญาณไร้สาย และการเข้าถึงการบริการอินเตอร์เน็ตได้อย่างอิสระ (โรงเรียนเม็งรายมหาราชวิทยาคม, 2556) แต่ขาดการคัดกรองหรือป้องกันการใช้เว็บไซต์ที่ไม่พึงประสงค์ซึ่งอาจส่งผลเสียต่อการใช้ชีวิตประจำวันหรือไม่เกิดประโยชน์ โดยเฉพาะในหมู่เด็กและเยาวชนที่ยังขาดวิจารณญาณในการรับรู้ข้อมูลข่าวสารต่างๆ

จากการศึกษาโครงงานต่างๆ ที่เกี่ยวข้องกับระบบไฟร์วอลล์ (บุญฤทธิ์, 2555) (วิกิพีเดีย, 2555ก) และระบบเครือข่ายสัญญาณไร้สาย ซึ่งนายวัฒนพงศ์ ประสิทธิเม ได้ศึกษาเรื่องการนำระบบไฟล์วอลล์ สำหรับเครือข่ายขนาดเล็ก (Firewall Systems For Small Network) (วัฒนพงศ์, 2555) มาเป็นตัวช่วยปิดกั้นเว็บไซต์ และพอร์ตต่างๆ ในเครือข่ายทั้งขาเข้าและขาออก โดยสามารถคอนฟิกได้ภายในหน้าอินเตอร์เฟสที่สร้างขึ้นจากภาษา PHP (Personal Home Page Tools) (วิกิพีเดีย, 2555ง) ไม่จำเป็นต้องเข้าไปคอนฟิกในระบบโดยใช้ผู้เชี่ยวชาญ ส่วนระบบจัดการการให้บริการอินเตอร์เน็ตไร้สายแบบจำกัดพื้นที่ (Area-Limit Wifi-Internet Service Management System) นอกจากนั้น พฤษพล ตั้งสัจจะธรรม และกายรัฐ เจริญราษฎร์ ได้ศึกษาการจัดการการให้บริการเครือข่ายสัญญาณไร้สายในพื้นที่ที่กำหนด (พฤษพล, 2555) โดยใช้โปรโตคอล SNMP (มหาวิทยาลัยสงขลานครินทร์, 2555) (วิกิพีเดีย, 2555ค) เป็นตัวช่วยในการจัดการภายในตัวส่งสัญญาณวายฟาย มีการใช้เครื่องเซิร์ฟเวอร์เป็นตัวกลางในการจัดการเครื่องลูกข่ายในเครือข่ายสัญญาณไร้สาย ในการช่วยหาพิกัดในขอบเขตของพื้นที่ให้บริการ ถ้าเครื่องลูกข่ายในระบบมีการเคลื่อนที่ออกจากพื้นที่ให้บริการ จะทำการบล็อกไอพีของเครื่องลูกข่าย และไม่สามารถใช้บริการอินเตอร์เน็ตไร้สายได้

จากปัญหาการเข้าถึงเว็บไซต์ต่างๆได้ง่ายโดยขาดการคัดกรองนั้น ผู้จัดทำจึงเกิดแนวคิดที่จะสร้างระบบคัดกรองการใช้เว็บไซต์ของเครื่องลูกข่าย ในระบบเครือข่ายอินเตอร์เน็ตไร้สาย โดยจะทำการตรวจสอบการใช้งานเว็บไซต์ของเครื่องลูกข่ายที่ทำการใช้งานผ่านอินเตอร์เน็ตไร้สาย โดยจะทำการกรองการใช้งานเว็บไซต์ผ่านระบบ

ไฟล์วอลล์ที่ติดตั้งอยู่ในเครื่องเซิฟเวอร์ (วิกิพีเดีย, 2555จ) เมื่อเครื่องลูกข่ายเข้าเว็บไซต์ที่ผู้ดูแลระบบไม่ต้องการ ทางระบบจะทำการตัดการเชื่อมต่อของเครื่องลูกข่ายช่วงเวลาหนึ่ง โดยมีโปรโตคอล SMNP (Simple Network Management Protocol) (มหาวิทยาลัยสงขลานครินทร์, 2555) (กรมพัฒนาฝีมือแรงงาน, 2556) เป็นตัวช่วยจัดการไปยังตัวส่งสัญญาณไร้สายว่าให้ตัดการเชื่อมต่อของเครื่องลูกข่ายนี้ และศึกษาการเดินทางของข้อมูลในเครือข่ายและนำข้อมูลไปวิเคราะห์ เพื่อให้เกิดประสิทธิภาพในการใช้งานและเพื่อการศึกษาต่อไป

วัตถุประสงค์ของการวิจัย

เพื่อทดสอบความสามารถของโปรโตคอล SNMP ในการตรวจสอบการทำงานของเครื่อง Access Point ในระบบเครือข่าย โดยพัฒนาเป็นระบบจัดการเครื่องลูกข่ายภายในเครือข่ายสัญญาณไร้สาย ด้วยการใช้ Shell script และคำสั่ง IPtables

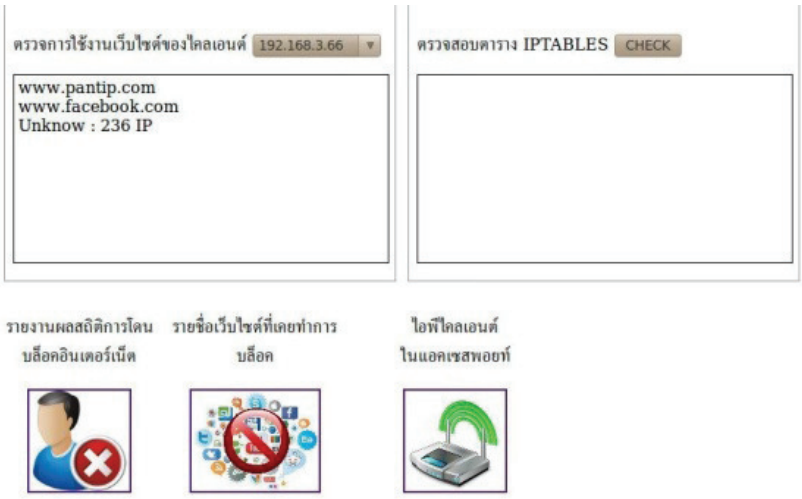
วิธีดำเนินการวิจัย

1. ทำการสร้างระบบควบคุมโดยใช้ภาษา PHP

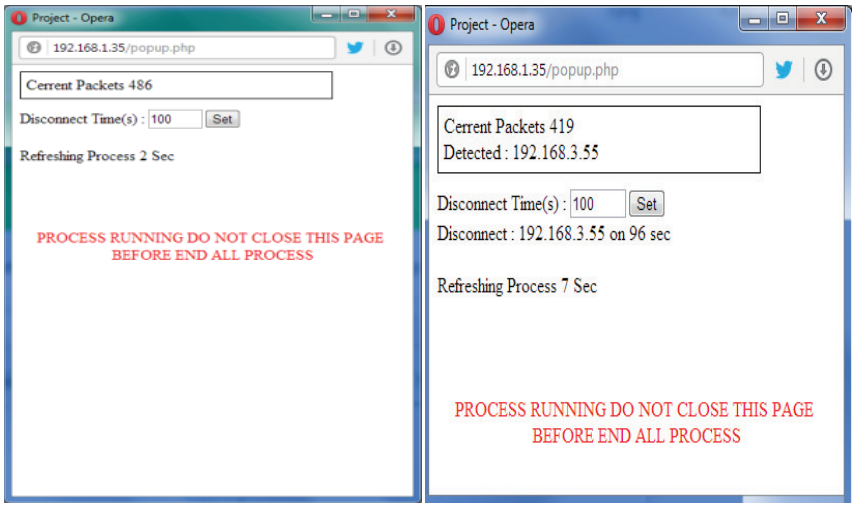
ทำระบบโดยการสร้างหน้าเว็บเพจเพื่อติดต่อกับเซิร์ฟเวอร์ฐานข้อมูล มีการทำงานส่วนใหญ่อยู่บนหน้าเว็บเพจ อันประกอบไปด้วยการตรวจสอบสิทธิ์การใช้งาน การจำกัดเว็บไซต์ ควบคุมเครื่องลูกข่ายและการแสดงผลของระบบ ดังแสดงในรูปที่ 1 ถึง 4

รูปที่ 1: ระบบตรวจสอบสิทธิการใช้งานของผู้ดูแลระบบ

รูปที่ 2: หน้าเว็บเพจควบคุมจำกัดเว็บไซต์



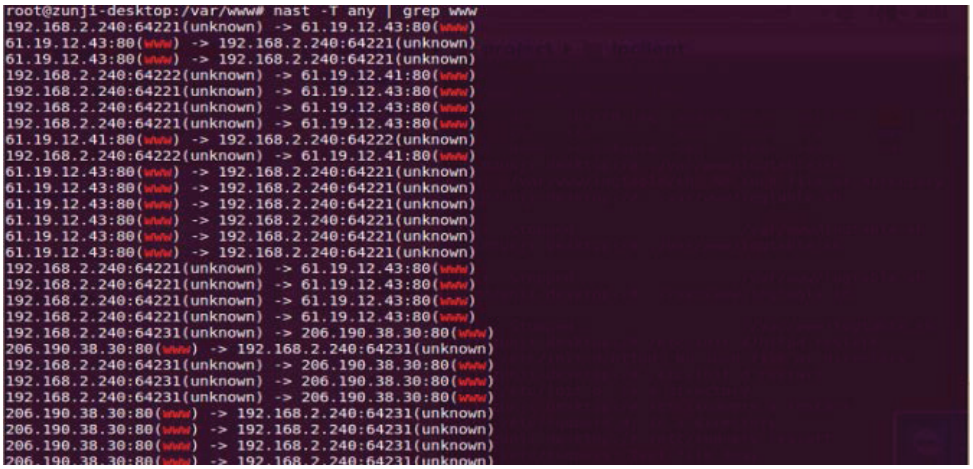
รูปที่ 3: หน้าเว็บเพจควบคุมการทำงานของเครื่องลูกข่าย



รูปที่ 4: หน้าเว็บเพจแสดงการทำงานของระบบ

2. จัดการเก็บข้อมูลการใช้งานของเครื่องลูกข่ายภายในเครือข่ายโดยการสั่งงานที่เครื่องเซิร์ฟเวอร์

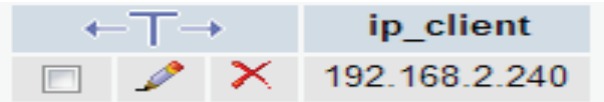
เขียนคำสั่งเพื่อทำการเก็บ Log ของแพคเก็ตภายในเครือข่ายโดยใช้ Network Command (nast–T any | grep) ดังแสดงในรูปที่ 5 เพื่อเก็บลงระบบฐานข้อมูล



รูปที่ 5: Log ข้อมูลแพคเก็ตภายในเครือข่าย

3. เก็บข้อมูลการเชื่อมต่อเครื่องลูกข่ายภาย

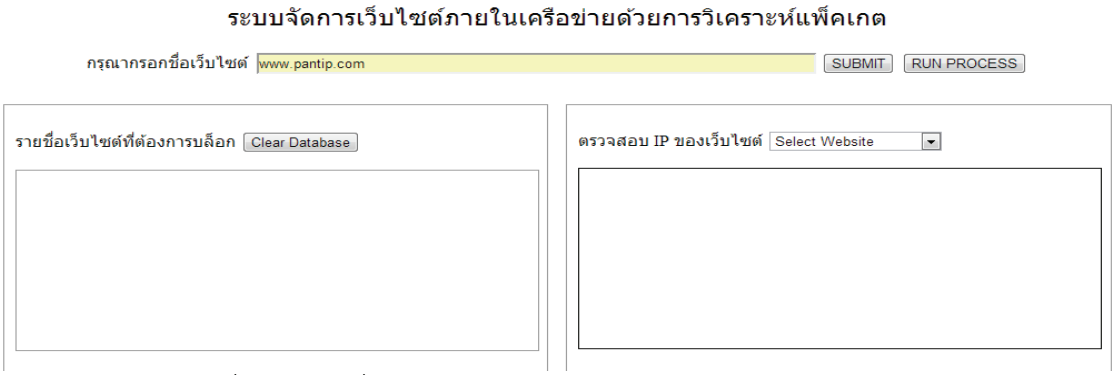
เขียนคำสั่งเพื่อตรวจสอบการเชื่อมต่อของเครื่องลูกข่ายกับ Access Point โดยการใช้ Network Command >snmpwalk -v1 -c public 192.168.2.1 เพื่อที่จะนำไปใช้ในการตรวจสอบโดยดูจากหมายเลขไอพีของเครื่องลูกข่ายว่ามีการใช้งานเว็บไซต์ใดบ้าง ดังตัวอย่างในรูปที่ 6



รูปที่ 6: จัดเก็บไอพีของเครื่องลูกข่ายลงฐานข้อมูล

4. เก็บเว็บไซต์ที่จะทำการปิดกั้น ลงระบบฐานข้อมูล โดยการกรอกข้อมูลบนหน้าเว็บเพจควบคุม

จากรูปที่ 7 และ 8 เป็นตัวอย่างการกรอกข้อมูลเว็บไซต์ที่ต้องการบล็อกและทำการกดปุ่ม INSERT แล้วระบบจะทำการเก็บชื่อเว็บไซต์และหมายเลขไอพีของเว็บไซต์ลงฐานข้อมูล



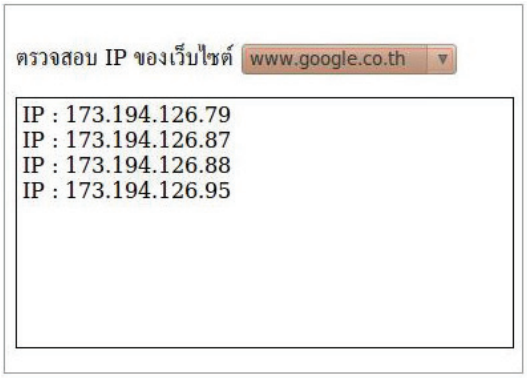
รูปที่ 7: หน้าเว็บเพจกรอกชื่อเว็บไซต์เพื่อทำการบล็อค

	www2	ipwww2
	www.dek-d.com	61.47.61.39
	www.facebook.com	31.13.79.33
	www.google.co.th	74.125.135.94
	www.kapook.com	202.183.165.60

รูปที่ 8: เก็บข้อมูลลงฐานข้อมูล

5. ส่วนตรวจสอบการไอพีแอดแดรสของเว็บไซต์ต่างๆ

ระบบนี้มีส่วนของฐานข้อมูลเว็บไซต์ เพื่อให้ผู้ใช้สามารถตรวจสอบไอพีแอดแดรสของเว็บไซต์ ดังตัวอย่างในรูปที่ 9



รูปที่ 9: ตรวจสอบไอพีแอดแดรสของเว็บไซต์

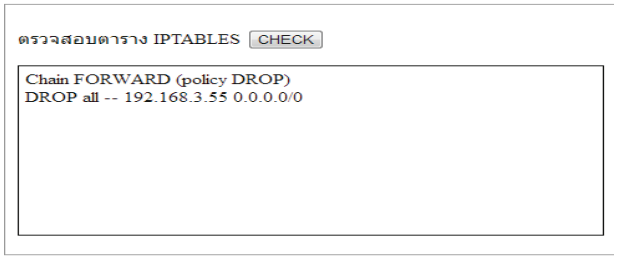
6. ส่วนตรวจสอบการใช้งานของเครื่องลูกข่าย

ผู้ดูแลระบบสามารถตรวจสอบว่าเครื่องลูกข่ายแต่ละเครื่องว่าใช้งานเว็บไซต์ใดบ้าง โดยระบบจะแสดงชื่อเว็บไซต์ ซึ่งอ้างอิงจากฐานข้อมูลเว็บไซต์ที่มีรายชื่อจากส่วนการเก็บข้อมูลในฐานข้อมูล ถ้าเกิดเครื่องลูกข่ายทำการเข้าเว็บไซต์ที่ทางฐานข้อมูลไม่มีชื่อเว็บไซต์จะแสดงผลชื่อเป็น Unknow ดังตัวอย่างในรูปที่ 10

รูปที่ 10: การตรวจสอบรายชื่อเว็บไซต์ที่เครื่องลูกข่ายใช้งาน

7. ส่วนตรวจสอบตาราง iptables

ตาราง iptales จะแสดงไอพีแอดแดรสของเครื่องลูกข่ายที่โดน Firewall ตัดการเชื่อมต่อข้อมูลชั่วคราว เมื่อมีการใช้งานเว็บไซต์ที่ไม่ต้องการ ดังตัวอย่างในรูปที่ 11



รูปที่ 11: จากตาราง iptables แสดงไอพีเครื่องลูกข่ายใดโดนบล็อคอยู่บ้าง

8. ระบบจัดการ Access Point หลายตัว

Access Point แต่ละตัวมีข้อจำกัดในการเชื่อมต่อของเครื่องลูกข่ายในจำนวนไม่มาก ระบบนี้จึงออกแบบมาให้สามารถเพิ่ม Access Point ได้หลายตัวทำให้รองรับการใช้งานของเครื่องลูกข่ายได้จำนวนมากขึ้น ดังแสดงในรูปที่ 12

รูปที่ 12: หน้าจัดการ Access Point

ผลการวิจัยและอภิปรายผล

1. การเก็บข้อมูลการใช้งานของเครื่องลูกข่ายลงฐานข้อมูล

เมื่อเริ่มต้นระบบ ระบบจะเก็บข้อมูลการใช้งานลงฐานข้อมูล โดยจะเก็บส่วนของหมายเลข source และ destination ลงฐานข้อมูล ดังแสดงในรูปที่ 13

←T→	source	destination
	192.168.2.135	184.50.85.123
	192.168.2.135	184.50.85.133
	192.168.2.135	184.50.85.147
	192.168.2.135	184.50.85.94

รูปที่ 13: ฐานข้อมูลไอพีต้นทางและไอพีปลายทาง

2. การแสดงผลแบบสถิติและข้อมูลของระบบ

ระบบจะทำการเก็บสถิติข้อมูลต่างๆ ในการใช้งานของเครื่องลูกข่ายเพื่อนำมารายงานผลได้ดังรูปที่ 14 และรูปที่ 15

รายงานผลแสดงสถิติของแต่ละไอพีไคลเอนต์

ไอพีแอดแดรส	จำนวนครั้ง(Denied)	วัน/เดือน/ปี
192.168.3.123	1	17-09-2014
192.168.3.55	7	17-09-2014 17-09-2014 17-09-2014

แสดงผลรายงานยอดการโดนบล็อกอินเตอร์เน็ตรายวัน

วัน/เดือน/ปี	จำนวนครั้ง(Denied)
17-09-2014	8

รูปที่ 14: สถิติของการโดนปิดกั้นการใช้งานของแต่ละเครื่องลูกข่าย

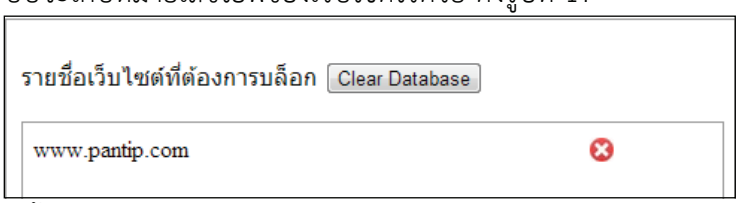
SEARCH

ชื่อเว็บไซต์	วัน/เดือน/ปี
google.com	2014-09-19
hon.in.th	2014-10-30
localhost	2014-09-27
www.123.com	2014-09-18
www.4shared.com	2014-10-30
www.adobe.com	2014-12-03
www.apple.com	2014-11-2 2014-11-2
www.aura.co.th	2014-08-19 2014-11-13

รูปที่ 15: รายชื่อเว็บไซต์ที่เคยทำการบล็อค และมี Filter ในการค้นหา

3. ผลทดลองตรวจสอบการใช้งานของเครื่องลูกข่าย

ตัวอย่างการทดลองในรูปที่ 16 แสดงเครื่องลูกข่ายเป้าหมายคือเครื่องหมายเลข “192.1682.240” ทดลองบล็อกเว็บไซต์ www.pantip.com เพื่อตรวจสอบระบบว่าสามารถปิดกั้นได้จริงหรือไม่ โดยเมื่อกรอกชื่อเว็บไซต์ดังกล่าวแล้ว ระบบจะเก็บหมายเลขไอพีของเว็บไซต์ไว้ด้วย ดังรูปที่ 17



รูปที่ 16: ตัวอย่างการปิดกั้นเว็บไซต์ www.pantip.com

	www2	ipwww2
	www.pantip.com	203.151.13.167
	www.pantip.com	203.151.13.169
	www.pantip.com	203.151.13.166
	www.pantip.com	203.151.13.168

รูปที่ 17: รายการหมายเลขไอพีของเว็บไซต์

จากรูปที่ 18 จะพบว่าระบบได้ทำการเก็บ source ซึ่งคือหมายเลขของเครื่องลูกข่าย และ destination ซึ่งคือหมายเลขของเว็บไซต์ www.pantip.com ลงฐานข้อมูล จากเป้าหมายที่ทดลอง “ip : 192.168.2.240” มีการใช้งานเว็บไซต์อื่นๆ รวมอยู่ด้วย เว็บไซต์เป้าหมาย คือ www.pantip.com โดยจากรูปที่ 17 มีการเก็บไอพีของเว็บไซต์ไว้ด้วยซึ่งตรงกัน

	source	destination
	117.18.237.139	192.168.2.240
	118.214.31.139	192.168.2.240
	192.168.2.240	117.18.237.139
	192.168.2.240	118.214.31.139
	192.168.2.240	202.79.210.121
	192.168.2.240	203.151.13.166
	192.168.2.240	203.151.13.167
	192.168.2.240	203.151.13.168
	192.168.2.240	203.151.13.169

รูปที่ 18: Log การใช้งานของเครื่องลูกข่าย

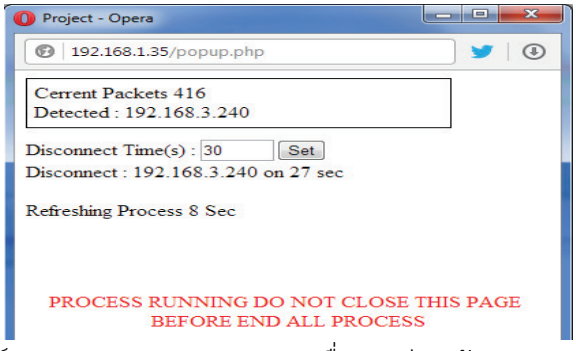
```
root@zunji-desktop:/var/www# iptables -nL
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy DROP)
target     prot opt source               destination
REJECT     all  --  0.0.0.0/0            0.0.0.0/0           STRING match "www.apple.com" ALGO name bm T
O 65535 reject-with icmp-port-unreachable
ACCEPT     all  --  0.0.0.0/0            127.0.0.1           STRING match "www.apple.com" ALGO name bm T
O 65535
ACCEPT     all  --  0.0.0.0/0            192.168.3.0/24
ACCEPT     all  --  192.168.3.0/24       0.0.0.0/0

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@zunji-desktop:/var/www#
```

รูปที่ 19: Iptables Rule

ระบบจะเพิ่มกฎการปิดกั้นการใช้งานตามที่ผู้ดูแลระบบได้ป้อนไว้ และหลังจากทำการ กดปุ่ม RUN PROCESS ระบบจะแสดงหน้า POPUP ดังแสดงในรูปที่ 20 และเมื่อมีการตรวจพบว่า เครื่องลูกข่ายหมายเลข 192.168.2.240 มีใช้งานเว็บไซต์ www.pantip.com ระบบจะทำการปิดกั้นการใช้งานของเครื่องหมายเลข 192.168.2.240 นี้ แต่จะสามารถกลับมาใช้งานอินเตอรเน็ตอีกครั้งได้ภายใน ระยะเวลาที่ได้ตั้งค่าเอาไว้ ข้างต้นตั้งค่าเวลาไว้ 30 วินาที



รูปที่ 20: การพบใช้งานเว็บไซต์ www.pantip.com ของเครื่องลูกข่ายเป้าหมาย

สรุป

จากการทดลองพบว่าระบบสามารถทำงานได้อย่างมีประสิทธิภาพในการจำกัดการใช้งานของเครื่องลูกข่ายในการการใช้งานเว็บไซต์ที่ผู้ควบคุมระบบไม่ต้องการให้เข้าถึง โดยทำการตรวจสอบชื่อเว็บไซต์ปลายจากการใช้งานของเครื่องลูกข่าย แล้วไปตรวจเทียบกับรายการเว็บไซต์ที่ไม่ต้องการให้เข้าถึง ซึ่งถ้าเกิดตรงกันจะทำการปิดกั้นการใช้งานของเครื่องลูกข่ายนั้นด้วยไฟร์วอลล์ตามระยะเวลาที่กำหนดเอาไว้ ซึ่งจะทำให้เครื่องลูกข่ายไม่สามารถใช้งานอินเตอร์เน็ตได้ชั่วคราว หลังจากหมดเวลาตามที่ตั้งค่าไว้เครื่องลูกข่ายจะสามารถกลับมาใช้งานอินเตอร์เน็ตได้อีกครั้ง หรือผู้ดูแลระบบสามารถสั่งงานยกเลิกการตัดสัญญาณอินเตอร์เน็ตได้จากหน้าระบบควบคุม ทั้งนี้ ผู้ดูแลระบบสามารถตั้งค่ารายการเว็บไซต์ที่ไม่ต้องการให้เข้าถึงได้หลายเว็บไซต์ และสามารถบล็อกเครื่องลูกข่ายได้หลายเครื่องลูกข่ายในเวลาเดียวกัน ระบบจะทำงานโดยอัตโนมัติหลังจากการเริ่มโปรแกรม และจะสิ้นสุดเมื่อปิดโปรแกรม แต่ระบบจะยังทำการเก็บ Log ของเครื่องลูกข่ายต่อไปถ้าเกิดยังมีการใช้งานในระบบเครือข่ายอยู่ระบบ

จะทำการเก็บสถิติการใช้งานในรูปแบบต่างๆเพื่อการรายงานผล

จากระบบที่ได้ทำการทดลองผู้จัดทำคิดว่าจะเป็นประโยชน์ต่อการควบคุมการทำงานของบุคลากรต่างๆ ให้ทำงานได้อย่างมีประสิทธิภาพ โดยถ้าหากนำมาใช้กับสถานศึกษา ครู อาจารย์จะสามารถควบคุมนักเรียนให้อยู่ในของเขตในการศึกษาหาความรู้ จากอินเตอร์เน็ตได้อย่างมีประสิทธิภาพไม่ได้ใช้เทคโนโลยีไปทางเสื่อมเสียให้เกิดโทษจากเทคโนโลยีที่ก้าวหน้าไปมากกว่านี้ อีกทั้งถ้ามีนิสิตนักศึกษาจะมาพัฒนาต่อในส่วนที่ขาดจะเกิดผลดีต่อทั้งตัวผู้พัฒนาและต่อผู้ใช้งานระบบอีกด้วย

เอกสารอ้างอิง

บุญฤทธิ์ คิดหงัน. 2555. *ไฟร์วอลล์คืออะไร*. สืบค้นเมื่อ 23 กรกฎาคม 2556, จาก เว็บไซต์: http://sci.feu.ac.th/boonrit/security/ch8%20

พฤษพล ตั้งสัจจะธรรม. (2555). *ระบบจัดการการให้บริการอินเตอร์เน็ตไร้สายแบบจำกัดพื้นที่, งานประชุมวิชาการระดับชาติ มหาวิทยาลัยราชภัฏนครปฐม ครั้งที่ 5*, 18-19 กรกฎาคม 2556 มหาวิทยาลัยราชภัฏนครปฐม.

มหาวิทยาลัยสงขลานครินทร์. (2555). *SNMP.* สืบค้นเมื่อ 23 กรกฎาคม 2556, จากเว็บไซต์: http://csn.cs.psu.ac.th/~suphipan/doc/snmp-doc.pdf

โรงเรียนเม็งรายมหาราชวิทยาคม. (2556). *ความหมายของอินเตอร์เน็ต*. สืบค้นเมื่อ 23 กรกฎาคม 2556, จากเว็บไซต์: http://vclass.mgt.psu.ac.th/~465-302/2007-1/Assignment-02/BPA_30_32/Internet%20Services%20Provider/01.htm

วัฒนพงศ์ ประสิทธิเม. (2555). *ไฟร์วอลล์สำหรับเครือข่ายขนาดเล็ก.* ปริญญานิพนธ์สาขาวิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ กำแพงแสน มหาวิทยาลัยเกษตรศาสตร์.

วิกิพีเดีย สารานุกรมเสรี. (2555ก). *ไฟร์วอล.* สืบค้นเมื่อ 23 กรกฎาคม 2556, จากเว็บไซต์: http://th.wikipedia.org/wiki/

วิกิพีเดีย สารานุกรมเสรี. (2556ข). *วายฟาย*. สืบค้นเมื่อ 23 กรกฎาคม 2556, จากเว็บไซต์: http://th.wikipedia.org/wiki/

วิกิพีเดีย สารานุกรมเสรี. (2556ค). *Simple Network Management Protocol*. สืบค้นเมื่อ 23 กรกฎาคม 2556, จากเว็บไซต์: http://en.wikipedia.org/wiki/Simple_Network_Management_Protocol,

วิกิพีเดีย สารานุกรมเสรี. (2556ง). *Personal Home Page Tools*. สืบค้นเมื่อ 23 กรกฎาคม 2556, จากเว็บไซต์: http://www.mindphp.com/คู่มือ/73-คืออะไร/2127-php-คืออะไร.html,

วิกิพีเดีย สารานุกรมเสรี. (2556จ). *เซิร์ฟเวอร์*. สืบค้นเมื่อ 23 กรกฎาคม 2556, จากเว็บไซต์: http://th.wikipedia.org/wiki/