ระบบบริหารจัดการผู้ใช้งานเครือข่ายตาม พรบ.ว่าด้วยการการกระทำผิดทางคอมพิวเตอร์

MANAGE USERS ON THE NETWORK FOLLOWED BY COMPUTER ACT SYSTEM

ภาคภูมิ เถิศสวัสดิ์วิชา
องอาจ อรรถโสภณศักดิ์

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต
ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ปีการศึกษา 2558

ระบบบริหารจัดการผู้ใช้งานเครือข่ายตาม พรบ.ว่าด้วยการการกระทำผิดทางคอมพิวเตอร์

MANAGE USERS ON THE NETWORK FOLLOWED BY COMPUTER ACT SYSTEM

ภาคภูมิ เลิศสวัสดิ์วิชา

องอาจ อรรถโสภณศักดิ์

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต

ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2558

ปริญญานิพนธ์ปีการศึกษา 2558

ภาควิชาวิศวกรรมคอมพิวเตอร์

คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

เรื่อง ระบบบริหารจัดการผู้ใช้งานเครือข่ายตาม พรบ.ว่าด้วยการการกระทำผิดทางคอมพิวเตอร์

MANAGE USERS ON THE NETWORK FOLLOWED BY COMPUTER ACT SYSTEM

ผู้จัดทำ

1. นายภาคภูมิเลิศสวัสดิ์วิชา รหัสนักศึกษา 55010932
2. นายองอาจ อรรถโสภณศักดิ์ รหัสนักศึกษา 55011386

_____อาจารย์ที่ปรึกษา

(รศ. ดร.สมศักดิ์ มิตะถา)

บริหารจัดการผู้ใช้งานเครือข่ายตาม พรบ.ว่าด้วยการการกระทำผิดทางคอมพิวเตอร์

นายภาคภูมิ เลิศสวัสดิ์วิชา 55010932
นายองอาจ อรรถโสภณศักดิ์ 55011386
รศ. ดร.สมศักดิ์ มิตะถา อาจารย์ที่ปรึกษา
ปีการศึกษา 2558

บทคัดย่อ

เนื่องจากในปีพุทธศักราช 2550 ประเทศไทยได้มีการประกาศใช้ กฎหมาย พรบ. คอมพิวเตอร์ เพื่อใช้เอาความผิดกับผู้กระทำความผิดทางคอมพิวเตอร์ ผู้ให้บริการเครือข่ายคอมพิวเตอร์จึงต้องมีการเก็บ log ข้อมูลการใช้งานเครือข่ายอินเตอร์เน็ตไว้เพื่อเอาความผิดกับผู้ที่ใช้อินเตอร์เน็ตในการกระทำความผิดทางคอมพิวเตอร์ ประกอบกับการขยายตัวของเครือข่ายอินเตอร์เน็ตที่มีขนาดใหญ่มากขึ้นเรื่อยๆ มีจำนวน Access point ในเครือข่ายจำนวนมาก ทำให้การตรวจสอบการทำงานของ Access point แต่ละตัว ทำได้ยาก จึงได้มีการจัดทำระบบบริหารจัดการผู้ใช้งานเครือข่ายตาม พรบ.ว่าด้วยการกระทำผิดทางคอมพิวเตอร์ ขึ้นนี้ขึ้นเพื่อทำหน้า บริหารจัดการผู้ใช้งานในระบบ โดยเก็บ log การใช้งานของผู้ใช้งาน และทำหน้าที่ตรวจสอบสถานะ Access point ในระบบ นอกจากนี้ยังสามารถสั่ง Reboot access point ตัวที่มีปัญหาได้ เพื่อเป็นการแก้ไขปัญหาเบื้องต้นจากการไม่ตอบสนองของ Access point

ระบบบริหารจัดการผู้ใช้งานเครือข่ายตาม พรบ.ว่าด้วยการกระทำผิดทางคอมพิวเตอร์ ใช้ Ubuntu Server เป็น OS พื้นฐานให้กับ Server และใช้ Pfsense เป็น Firewall ทำการสร้าง log การใช้งานขึ้นมา โดยทำงานร่วมกับ Free Radius ซึ่งเป็น Radius Server ที่ให้ผู้ใช้งานเข้ามา Authentication เพื่อใช้งานระบบ และ Syslog-ng เป็นตัวจัดการ log แล้วจึงส่งต่อ log เข้าไปเก็บบน Database ซึ่งใช้ MySQL เป็น Database ซึ่งระบบทั้งหมดนี้ ทำงานโดยใช้ Web Server ทำงานเป็นหลัก ทำให้ผู้ดูแลระบบสามารถดูแลระบบได้จากหน้าเว็บไซต์ ไม่ต้องลงโปรแกรมใดๆเพิ่มเติม สำหรับการตรวจสอบ Access point นั้น ใช้การ ping เข้าไปตรวจสอบ ส่วนการสั่ง Reboot และการตรวจสอบการใช้ทรัพยากรของ Firewall ใช้การ SSH เข้าไปที่อุปกรณ์เพื่อสั่งงาน

ระบบบริหารจัดการผู้ใช้งานเครือข่ายตาม พรบ.ว่าด้วยการกระทำผิดทางคอมพิวเตอร์ จึงเป็นระบบที่มีฟังก์ชั่นหลักๆสองส่วนคือทำหน้าที่เก็บ log การใช้งานให้เป็นไปตาม พรบ. คอมพิวเตอร์ และช่วยเหลือผู้ดูแลระบบในการตรวจสอบสถานะของเครือข่าย เช่น สถานะของ Access point และการใช้ทรัพยากรของ Firewall หากสถานะของ Access point ไม่มีการตอบสนองก็ยังสามารถสั่ง Reboot ได้ ซึ่งจะทำให้ผู้ดูแลระบบ สามารถบริหารจัดการระบบได้ง่ายยิ่งขึ้น

Manage Users on the Network followed by Computer Act System

Mr.Parkpoom Lertsawatwicha 55010932
Mr.Ongard Attasophonsak 55011386
Assoc.Prof.Dr.Somsak Mitatha Advisor
Academic Year 2015

ABSTRACT

In 2007, the Thai government declared the Computer Act for punishment of people who break the law through computer. Thus, internet service providers have to keep logs about internet usage of users. The log will be used as evidence when the offense occurs. And nowadays networks are bigger than past, more number of access points. It is difficult to check all of it. Therefore, we implement Manage Users on the Network followed by Computer Act System for keeping log and monitoring access point. In addition, the system can reboot the access point which has problem to primary solve the problem when access point not response.

Manage Users on the Network followed by Computer Act System uses Ubuntu server as OS on server, use Pfsense as firewall generate log of usage, use Free Radius as radius server to let users authentication, use Syslog-ng to manage log file and send to Database, MySQL, after. Main functions of the system use web server implement. It make administrator can monitoring and use the system via web browser without install any program. The system monitors access points by ping to check access point. The system uses SSH to command reboot access points and monitor resource of firewall.

Consequently, Manage Users on the Network followed by Computer Act System is the system that keeping log and monitoring access point with reboot function. It make administrators easy to use the system.

กิตติกรรมประกาศ

โครงงานนี้สำเร็จลุล่วงไปได้ด้วยความกรุณาจาก อาจารย์สมศักดิ์ มิตะถา อาจารย์ที่ปรึกษาโครงงาน ที่ให้คำปรึกษา และอำนวยความสะดวกสถานที่ทำโครงงาน ที่ห้อง HCRL และติดต่อกับอาจารย์ที่สำนักคอม เพื่อให้คำปรึกษาเพิ่มเติมในโครงงานชิ้นนี้

ขอขอบพระคุณอาจารย์นรฤทธิ์ สุนทรศารทูล อาจารย์ฝ่ายสำนักบริการคอมพิวเตอร์ ที่ให้คำปรึกษาในโครงงาน และพี่กฤษฎิ์ธนิก ศรีธนสาร หัวหน้าทีมงานบริการเครือข่ายการสื่อสาร สำนักบริการคอมพิวเตอร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง ที่ให้คำปรึกษาและแนะนำเครื่องมือ อุปกรณ์ ที่ใช้ในการทำโครงงานชิ้นนี้

ขอบคุณพี่ศราวุธ ขุนประเสริฐ พี่ห้อง HCRL ที่ให้คำปรึกษาในการวางแผนทำงาน ให้ข้อมูลการทำงาน แนะนำวิธีการทำงาน จัดหาอุปกรณ์ในการทำโครงงาน และการจัดทำรูปเล่มโครงงาน ให้โครงงานชินนี้สำเร็จลุล่วงไปได้

ภาคภูมิ เลิศสวัสดิ์วิชา

องอาจ อรรถโสภณศักดิ์

สารบัญ

หน้า

สารบัญ(ต่อ)

หน้า

สารบัญตาราง

ตาราง **หน้า**

สารบัญรูป

สารบัญรูป(ต่อ)

รูป **หน้า**

บทที่ 1
บทนำ

1.1 ความเป็นมา

เนื่องจากในปีพุทธศักราช 2550 ประเทศไทยได้มีการประกาศใช้ กฎหมาย พรบ. คอมพิวเตอร์ เพื่อใช้เอาความผิดกับผู้กระทำความผิดทางคอมพิวเตอร์ โดยในตัวกฎหมาย มีส่วนที่ได้ระบุให้ผู้ให้บริการการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ (Access Service Provider) หรือคือผู้ให้บริการอินเตอร์เน็ตกับบุคคลทั่วไป ต้องทำการเก็บข้อมูลการใช้งาน(log) ของผู้ที่เข้ามาใช้งานไว้ เป็นเวลา 90 วัน เพื่อใช้เป็นหลักฐานเมื่อมีการกระทำความผิดเกิดขึ้น หากไม่มีการเก็บข้อมูลการใช้งาน(log) ไว้ผู้ให้บริการอินเตอร์เน็ตจะมีความผิด ตามมาตราที่ 26 ได้ประกาศไว้ว่า

"ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็นพนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินหนึ่งปีเป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้ ผู้ให้บริการจะต้องเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการ นับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าเก้าสิบวันนับตั้งแต่การใช้บริการสิ้นสุดลง ความในวรรคหนึ่งจะใช้กับผู้ให้บริการประเภทใด อย่างไร และเมื่อใด ให้เป็นไปตามที่รัฐมนตรีประกาศในราชกิจจานุเบกษา ผู้ให้บริการผู้ใดไม่ปฏิบัติตามมาตรานี้ ต้องระวางโทษปรับไม่เกินห้าแสนบาท"

นอกจากนี้ ขนาดของเครือข่ายอินเตอร์เน็ต ยังมีขนาดใหญ่มากขึ้นเรื่อยๆ มีอุปกรณ์ไร้สายเกิดขึ้นมากมาย เช่น โน้ตบุค, สมาร์ทโฟน, แท็บเบล็ต ฯลฯ ทำให้การดูแล และบริหารจัดการ ทำได้ไม่ทั่วถึง และในบางครั้ง จุดกระจายสัญญาณนั้น มีระยะห่างกันมาก ทำให้เกิดความไม่สะดวก ถ้าต้องไปตรวจสอบและจัดการแก้ไขอุปกรณ์ด้วยตัวเอง

ดังนั้นหากมีระบบบริหารจัดการผู้ใช้งานเครือข่ายตาม พรบ.ว่าด้วยการกระทำผิดทางคอมพิวเตอร์ ก็จะช่วยให้ผู้ให้บริการอินเตอร์เน็ต สามารถเก็บข้อมูลการใช้งานเครือข่ายได้ถูกต้องตาม พรบ. คอมพิวเตอร์ และยังทำให้ ผู้ดูแลระบบ สามารถตรวจสอบ และจัดการกับจุดกระจายสัญญาณอินเตอร์เน็ตที่มีปัญหาได้ง่ายยิ่งขึ้น

1.2 ความมุ่งหมายและวัตถุประสงค์

1) ทำระบบบริหารจัดการผู้ใช้งานเครือข่าย
2) มีหน้าเว็บสำหรับ admin เข้ามาจัดการดูแลระบบได้
3) สามารถสั่ง Reset Access Point ได้ โดยผ่านหน้าเว็บไซต์
4) มีการแสดงสถานะการรับส่งข้อมูลของ Access Point บนหน้าเว็บไซต์
5) จัดการเก็บ log ข้อมูลของผู้ใช้งานตาม กฎหมาย พรบ. คอมพิวเตอร์ ปี 2550

1.3 ประโยชน์ที่คาดว่าจะได้รับ

1) ได้ความรู้เรื่องกฎหมายพรบ. คอมพิวเตอร์ปี 2550
2) ได้ความรู้เรื่องการสร้าง Rule ของ Firewall
3) ได้ความรู้เรื่องการใช้งาน Pfsense
4) ได้ความรู้เรื่องการเขียนเว็บไซต์
5) ได้ความรู้เรื่องการใช้งาน Ubuntu Server
6) ได้ความรู้เรื่องการใช้ Shell Script
7) ระบบสามารถนำไปใช้งานได้จริง

1.4 ขอบเขตของโครงงาน

1) ศึกษา พรบ. คอมพิวเตอร์ปี 2550
2) ศึกษาวิธีการใช้งานและหลักการทำงานของ Pfsense Firewall
3) ศึกษาภาษา UNIX ขั้นพื้นฐาน เพื่อนำมาใช้งานกับ Firewall, Server, Access Piont
4) ศึกษาภาษา php และ HTML เพื่อนำมาสร้างหน้าเว็บไซต์การใช้งาน
5) ศึกษาการใช้งาน Shell Script
6) ศึกษาการตั้งค่าต่างๆของ Access Point
7) ทำระบบจัดเก็บข้อมูลผู้ใช้งานและข้อมูลการใช้งานของเครือข่ายของผู้ใช้ตาม พรบ. คอมพิวเตอร์ ปี พ.ศ. 2550
8) ทดสอบระบบทั้งหมดใน Vitual Box
9) ทดสอบระบบสามารถใช้งานได้กับผู้ใช้งาน

บทที่ 2
ทฤษฎีและงานที่เกี่ยวข้อง

2.1 ทฤษฎีที่เกี่ยวข้อง

2.1.1 กฎหมาย พรบ. คอมพิวเตอร์ ปี 2550

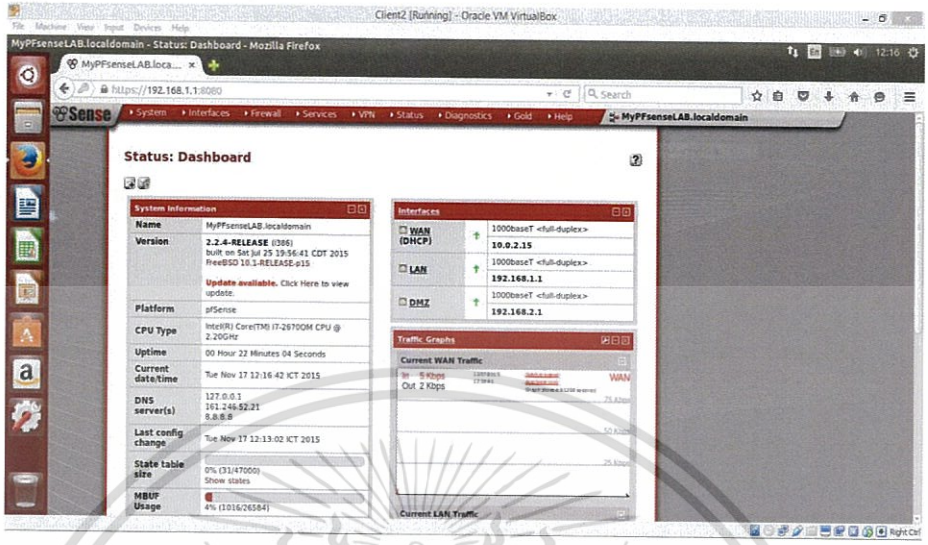
จากการประกาศใช้ พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ในมาตราที่ 26 ได้ประกาศไว้ว่า "ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็นพนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินหนึ่งปีเป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้ ผู้ให้บริการจะต้องเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการ นับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าเก้าสิบวันนับตั้งแต่การใช้บริการสิ้นสุดลง ความในวรรคหนึ่งจะใช้กับผู้ให้บริการประเภทใด อย่างไร และเมื่อใด ให้เป็นไปตามที่รัฐมนตรีประกาศในราชกิจจานุเบกษา ผู้ให้บริการผู้ใดไม่ปฏิบัติตามมาตรานี้ ต้องระวางโทษปรับไม่เกินห้าแสนบาท"

2.1.1.1 หลักเกณฑ์การเก็บรักษาข้อมูลตามกฎหมาย พรบ. คอมพิวเตอร์ ปี 2550

ตามหลักการผู้ให้บริการแต่ละประเภท สถานศึกษาหรือผู้ให้บริการอินเตอร์เน็ตถือเป็นผู้ให้บริการประเภท ข คือ ผู้ให้บริการการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ (Access Service Provider) โดยสิ่งที่ต้องจัดเก็บมีดังนี้

1) ข้อมูลอินเทอร์เน็ตที่เกิดจากการเข้าถึงระบบเครือข่าย
2) ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการจดหมายอิเล็กทรอนิกส์ (e-mail servers)
3) ข้อมูลอินเทอร์เน็ตจากการ โอนแฟ้มข้อมูลบนเครื่องให้บริการ โอนแฟ้มข้อมูล
4) ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการเว็บ
5) ชนิดของข้อมูลบนเครือข่ายคอมพิวเตอร์ขนาดใหญ่ (Usenet)
6) ข้อมูลที่เกิดจากการ โต้ตอบกันบนเครือข่ายอินเทอร์เน็ต เช่น Internet Relay Chat (IRC) หรือ Instance Messaging (IM) เป็นต้น

2.1.2 Firewall Pfsense



รูป 2.1 Pfsense webpage

pfSense เป็นโปรเจ็คที่พัฒนาโดย Chris Buechler และ Scott Ullrich ถูกพัฒนาขึ้นจาก Linux ระบบ FreeBSD เมื่อปี 2004 มีจุดประสงค์เพื่อใช้งานเป็น ไฟร์วอล์ และเราเตอร์ และต้องสามารถจัดการตัวอุปกรณ์ ได้ผ่านหน้า Browser (IE, Firefox, Chrome ฯลฯ) ได้ โดยทำงานเป็น Stateful firewall สำหรับการติดตั้ง firewall pfSense ก็สามารถทำได้ง่าย

Stateful firewall เป็น firewall ที่มีหลักการการทำงานคือจะมีการจำ State ของแต่ละ Session ที่เกิดขึ้น ว่า Source เป็นอะไร ติดต่อกับ Destination อะไร โดยจะเก็บไว้ใน State Table ถ้ามี Source หรือ Destination อื่นเข้ามาสวมรอย ก็จะไม่สามารถทำได้ ซึ่งทำให้เพิ่มขีดความสามารถในการป้องกันที่ดีขึ้น และรองรับกับการใช้งาน Service ที่หลากหลายต่าง ๆ ได้ ทั้ง TCP และ UDP

การนำ Firewall Pfsense มาใช้ นำมาใช้เป็น Firewall หลักของระบบที่จะคอยทำหน้าที่จัดการเส้นทางให้ Packet ว่าจะต้องไปที่ไหนก่อน เช่น ผู้ใช้งานทำการ Login ระบบ Pfsense ก็จะให้ผู้ใช้งานไปที่ server Free Radius เพื่อตรวจสอบว่ามี Username Password ดังกล่าวหรือไม่ เพื่อทำการให้สิทธิ์การใช้งานต่อไป และเมื่อผู้ใช้ login แล้ว Pfsense ก็จะส่ง log การใช้งานต่างๆไปให้ syslog-ng เก็บข้อมูล log

Feature เด่น ของ pfSense

1) เป็น Stateful Firewall
2) ควบคุมการผ่านเข้าออกของทราฟฟิกด้วย source และ destination IP address, Protocol, Port
3) จำกัด Connection ต่อ 1 Rule ได้

4) มีระบบ OS/Networking fingerprinting ควบคุมการเข้าใช้งานระบบด้วย OS ตัวอย่างเช่น เราจะจำกัดเพียงแค่ ระบบปฏิบัติการ Windows เท่านั้นให้เข้าถึงเครือข่ายภายใน ส่วน Linux ให้ Block ได้
5) สามารถ Log Traffic บนแต่ละ rule ได้ เพื่อใช้ในการเก็บ Log ตาม พรบ. คอมพิวเตอร์
6) สามารถทำ Policy Routing ได้
7) ใช้ Aliases ในการจัดกลุ่ม Port, IP Address, Network ทำให้ง่ายต่อการจัดการกับ rule ของไฟร์วอล์
8) เลือกเป็นโหมด Transparent ได้ (โหมดนี้จะไม่ต้องไปแก้ไขระบบเดิมเลย เพียงแค่นำไปวางขวาง)
9) การทำ NAT (1:1, Outbound NAT, NAT Reflection)
10) รองรับการทำ HA (High Availability)
11) Multi WAN ใช้หลายๆขา internet ในการออกเข้าสู่ภายนอกได้
12) Server Loadbalancing
13) รองรับการทำ VPN (IPsec, OpenVPN, PPTP)
14) สนับสนุนการทำ Report และ Monitoring, Dynamic DNS, DHCP Server และ PPPoE Server

Hardware สำหรับ การติดตั้ง pfSense

1) เครื่องคอมพิวเตอร์ CPU ควรจะเป็น Core 2 Duo ขึ้นไป
2) Ram ขั้นต่ำควรจะอยู่ที่ 1 GB ขึ้นไป
3) การ์ดแลน 2 การ์ด (ขั้นต่ำ)
4) ฮาร์ดดิสก์ ขั้นต่ำ 1 GB

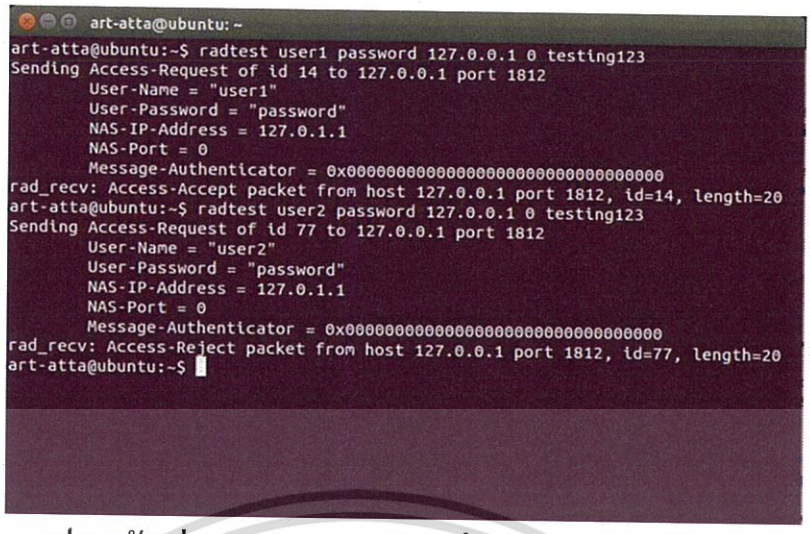
2.1.3 Free Radius

รูป 2.2 logo free radius

จะติดตั้งอยู่บน Ubuntu Server และองค์ประกอบพื้นฐานของ RADIUS server มีอยู่ 3 อย่างได้แก่

1) Access Clients คือ เครื่องคอมพิวเตอร์หรืออุปกรณ์ที่ผู้ใช้งานสั่งให้ติดต่อระบบเพื่อขอการใช้งาน
2) Network Access Servers (NAS) คือ อุปกรณ์ที่ทำหน้าที่เชื่อมต่อและจัดการการติดต่อระหว่าง Access Clients และ RADIUS server ซึ่ง NAS จะทำหน้าที่เป็น Client เชื่อมต่อกับ RADIUS server ส่งผ่านและจัดการข้อมูลที่ใช้ในการตรวจสอบสิทธิ์ กำหนดสิทธิ์ ของ Access Clients เมื่อ Access Clients ร้องขอการต่อเชื่อมซึ่งจะต้องต่อเชื่อมมายัง NAS ผ่านโพรโตคอลที่ใช้ในการต่อเชื่อมต่าง ๆ เช่น PPP (Pointto-Point Protocol), SLIP (Serial Line Internet Protocol), Extensible Protocol อื่น ๆ เป็นต้น ซึ่งจำเป็นต้องมีการส่งผ่าน Username และ Password จาก Access Clients มายัง NAS หลังจากนั้น NAS จะส่งข้อมูลที่จำเป็นต่าง ๆ เช่น Username, Password, NAS IP Address, NAS Port Number และข้อมูลอื่น ๆ ไปที่ RADIUS server เพื่อขอตรวจสอบสิทธิ์ (Request Authentication) ยกตัวอย่าง NAS ในที่นี้ได้แก่ Wireless Access Point
3) RADIUS server ทำการตรวจสอบสิทธิ์ โดยใช้ข้อมูลที่ NAS ส่งมา (Access-Request) กับข้อมูลที่จัดเก็บ ไว้ใน RADIUS server เอง หรือจากฐานข้อมูลภายนอกอื่น ๆ เช่น MS SQL Server, Oracle 54 Database, LDAP Database หรือ RADIUS server อื่น (ซึ่งเรียกการส่งผ่านการตรวจสอบสิทธิ์ แบบนี้ว่า Proxy)

โดยจะใช้ Free Radius Server จะทำหน้าที่เก็บข้อมูลผู้ใช้งาน คือ ชื่อผู้ใช้, Username, Password, เลขบัตรประจำตัวประชาชนของผู้ใช้งาน เมื่อผู้ใช้จะเข้ามาใช้งาน ก็จะต้องทำการ log in และตรวจสอบ Username, Password กับ Free Radius ก่อน เมื่อตรวจแล้วผ่าน ก็จะได้รับสิทธิ์การเข้าใช้งานระบบต่อไป



รูป 2.3 ตัวอย่างการ Authentication ผ่าน Free Radius ด้วย CLI

การ Authentication ผ่าน Free Radius จะใช้คำสั่งดังนี้ “radtest username password destination key” โดยให้ pfsense ร้องขอการ log in มาที่ Free Radius เอง

1) ถ้าทำการ Authentication ผ่าน Free Radius ได้ถูกต้อง Free Radius จะตอบกลับมาว่า “Access-Accept packet from host port, id length”
2) ถ้าทำการ Authentication ผ่าน Free Radius ไม่ถูกต้อง Free Radius จะตอบกลับมาว่า “Access-Reject packet from host port, id length”

2.1.4 Syslog-ng

ติดตั้งอยู่บน Ubuntu Server โดยเป็นระบบจัดเก็บบันทึกกิจกรรมส่วนกลาง(Centralized Log Server) เป็นโปรแกรมช่วยจัดการกับล็อกของเครื่องเซิร์ฟเวอร์ที่ให้บริการ เราเตอร์และสวิตซ์

Syslog-ng Server จะทำหน้าที่เก็บ Log ข้อมูลการใช้งานของผู้ใช้งานที่ใช้งานอุปกรณ์ในระบบ เช่น ประวัติการเข้าเว็บไซต์ เป็นต้น โดยจะเริ่มต้นเก็บ log หลังจากที่ผู้ใช้ได้ทำการ log in ผ่านเข้ามาจาก Free Radius แล้ว การใช้งานต่างๆของผู้ใช้ ก็จะถูกส่งเข้ามาเก็บที่ syslog-ng เพื่อใช้เป็นหลักฐานอ้างอิงเมื่อมีการขอตรวจสอบ

โครงสร้าง Log ของ Syslog-ng

<priority> VERSION ISOTIMESTAMP HOSTNAME APPLICATION PID MESSAGEID STRUCTURED-DATA MSG

1) priority จะเป็นเลขที่บอกสถานะของ Log นั้น โดยเลขหลักสุดท้ายจะบอก severity ซึ่งนำมาใช้เป็นตัวตรวจสอบสถานะของ Access Point
2) VERSION หมายเลขเวอร์ชั่น
3) ISOTIMESTAMP เวลาที่สร้าง log ใช้มาตรฐาน ISO 8601

4) HOSTNAME ชื่ออุปกรณ์ที่ส่ง log มา

5) APPLICATION อุปกรณ์หรือ Application ที่เป็นผู้สร้าง log

6) PID เป็น Process ID

7) STRUCTURED-DATA ข้อมูลของ log

8) MSG

ตัวอย่างข้อความ Log ของ Syslog-ng

"<34>1 2003-10-11T22:14:15.003Z mymachine.example.com su - ID47 - BOM'su root' failed for lonvick on /dev/pts/8"

2.1.5 Web Server

ติดตั้ง Apache บน Ubuntu Server โดยเป็นส่วนประมวลผลและเป็น Server สำหรับทำเว็บไซต์ของระบบ โดยจะมี 2 ส่วนคือ

1) ส่วนที่ทำงานเป็น Web Server ให้บริการหน้าเว็บ

2) ส่วนที่ทำงานเบื้องหลังของระบบเพื่อให้ระบบทำงานเองอย่างต่อเนื่อง

โดย Apache เป็น Open source ซึ่ง Apache จะเป็นโปรแกรมที่ทำให้คอมพิวเตอร์ที่ได้ติดตั้ง Apache สามารถให้บริการ Web Site ที่สามารถเรียกจากเครื่องอื่น ๆ ที่เป็น Client ได้

Apache ยังมีความสามารถอื่นอีกเช่น การเพิ่มความปลอดภัยในการสื่อสารผ่าน โพรโทคอล https หรือ สร้างโฮสท์เสมือนเช่น www.sample.com ภายในเครื่องเดียวกันได้ เป็นต้น

Apache จะรองรับระบบปฏิบัติการได้หลากหลาย เช่น Linux, Windows หรือ Mac OS

2.1.6 PHP & HTML

ใช้ภาษา PHP และ HTML ในการเขียนหน้าเว็บไซต์ของผู้ใช้เพื่อใช้ในการ log in ส่วน Admin ของระบบใช้งานในการจัดการกับระบบ และตรวจสอบการทำงานของ Access point

PHP เป็นภาษาคอมพิวเตอร์ที่มีการทำงานบนฝั่ง Server มีลิขสิทธิ์อยู่ในลักษณะโอเพนซอร์ส ภาษา PHP ใช้สำหรับจัดทำเว็บไซต์ และแสดงผลออกมาในรูปแบบ HTML โดยมีรากฐานโครงสร้างคำสั่งมาจากภาษา ภาษาซี ภาษาจาวา และ ภาษาเพิร์ล

HTML เป็นภาษามาร์กอัปหลักในปัจจุบันที่ใช้ในการสร้างเว็บไซต์ หรือข้อมูลอื่นที่เรียกดูผ่านทางเว็บเบราว์เซอร์ ซึ่งตัวโค้ดจะแสดงโครงสร้างของข้อมูล ในการแสดง หัวข้อ ลิงก์ ย่อหน้า รายการ รวมถึงการสร้างแบบฟอร์ม เชื่อมโยงภาพหรือวิดีโอด้วย โครงสร้างของโค้ดเอชทีเอ็มแอลจะอยู่ในลักษณะภายในวงเล็บสามเหลี่ยม

HTML เริ่มพัฒนาโดย ทิม เบอร์เนอร์ส ลี (Tim Berners Lee) สำหรับภาษา SGML นปัจจุบัน HTML เป็นมาตรฐานหนึ่งของISO ซึ่งจัดการโดย World Wide Web Consortium (W3C)

2.1.7 MySQL

MySQL เป็นโปรแกรมที่เอาไว้จัดการกับฐานข้อมูลที่สามารถจัดเก็บ ลบ ค้นหา เรียงข้อมูล และดึงข้อมูลได้ ผ่านภาษา SQL

MySQL เป็น Open source ที่สามารถรองรับได้หลายระบบปฏิบัติการ เช่น Windows, Linux, Mac OS เป็นต้น

2.1.8 Virtual Box

เป็นฟรีแวร์สำหรับจำลองระบบคอมพิวเตอร์ขึ้นมาบนเครื่อง Host หรือ Virtual Machine ทำให้สามารถสร้างเครื่องคอมพิวเตอร์จำลองขึ้นมาได้หลายเครื่อง บนเครื่องคอมพิวเตอร์จริงๆ เครื่องเดียว

2.1.9 Access Point

เลือกใช้ Access Point ที่รองรับ Service SSH ได้ ซึ่งจะทำให้สามารถสั่ง Reset Access Point จาก ศูนย์กลาง และเก็บข้อมูลต่างๆได้

SSH หรือ Secure Shell คือ Protocol ชนิดหนึ่ง ที่ออกแบบมาเพื่อให้เข้าไปยัง อุปกรณ์เครื่องอื่นๆ และทำงานต่างๆ บนเครื่องนั้น โดย SSH ได้รับการออกแบบให้มาแทนการใช้ Telnet, Rlogin, RSH เพราะ SSH จะมีความปลอดภัยมากกว่า โดยเวลาส่งข้อมูลระหว่างเครื่อง SSH จะทำการเข้ารหัส (Encryption) ข้อมูลเพื่อให้ข้อมูลมีความปลอดภัย

2.1.10 PHPExcel

PHPExcel เป็น Library หนึ่งของ php ที่จะนำมาใช้ทำเป็น Report ในรูปแบบของไฟล์ Excel ที่จะง่ายในการใช้งานดูข้อมูลต่างๆ และยังสามารถเพิ่มความปลอดภัยในการให้ใส่รหัสผ่านเวลาแก้ไขข้อมูลได้ เพื่อในกรณีที่ผู้ใช้งานจะไม่สามารถแก้ไข Report ที่ทำออกมาได้

2.1.11 Shell Script

Shell Script เป็นโปรแกรมคอมพิวเตอร์ที่นำไปประมวลผลบนระบบปฏิบัติการ UNIX โดย Shell Script จะรวบรวมกลุ่มคำสั่ง Command Line ของ Unix เอาไว้ซึ่งจะทำให้มีความสามารถในการใช้งานสูง เมื่อเรียกใช้งาน Shell Script ก็จะได้ผลลัพธ์ตามคำสั่งที่ได้เขียนไว้ใน Shell Script

2.1.12 UNIX Command

1) ssh ใช้เพื่อสั่ง remote เข้าไปยังเครื่องเป้าหมาย
2) crontab เป็นการตั้งเวลา เพื่อสั่งคำสั่งบน CLI ในระบบปฏิบัติการ ubuntu
3) grep เป็นการสั่งให้หน้าจอแสดงผลเฉพาะ บรรทัดที่ต้องการ โดยใช้คำสำคัญ
4) awk ใช้คำสั่งนี้เพื่อให้แสดงผลเฉพาะ คอลลัมของคำที่ต้องการ
5) top –n เพื่อเรียกดูการใช้ memory
6) ps aux เพื่อเรียกดูการใช้ cpu
7) df -hเพื่อเรียกดูการใช้ HDD

2.1.13 DD-Wrt

เป็นเฟิร์มแวร์ของ อุปกรณ์พวกเร้าเตอร์ โดยมีหลักการว่า Unleash your Router ซึ่งทำให้เร้าเตอร์สามารถใช้ความสามารถต่างๆได้มากขึ้น โดยสามารถลงบนอุปกรณ์เร้าเตอร์ได้หลายยี่ห้อด้วยกัน

ในที่นี้เลือกลงให้อุปกรณ์เร้าเตอร์ และตั้งค่าให้ทำงานเป็น Access Point และ เปิดให้สามารถสั่งงานผ่าน SSH ได้

2.2 ศึกษางานที่ใกล้เคียง

2.2.1 Bangkok Wifi

Bangkok Wifi คือ อินเตอร์เน็ตไร้สายความเร็วสูงที่ให้บริการฟรี ที่เกิดจากความร่วมมือระหว่างกรุงเทพมหานครและ Wifi by TruemoveH โดยสามารถเชื่อมต่ออินเตอร์เน็ตไร้สายความเร็วสูง Wifi by TruemoveH ที่จุดฮอตสปอตมากกว่า 20,000 จุดทั่วกรุงเทพมหานคร ซึ่งจะมี 2 แพ็คเกจให้เลือกคือ

1) ความเร็ว 256 Kbps / 128 Kbps ไม่จำกัดชั่วโมงการใช้งาน
2) ความเร็ว 2 Mbps / 512 Kbps ระยะเวลาใช้งาน 5 ชั่วโมงต่อเดือน

การใช้งาน Bangkok Wifi มีวิธีดังนี้

1) เมื่อเชื่อมต่อสัญญาณแล้วจะปรากฏหน้าให้ล็อคอิน
2) ถ้าผู้ใช้งานมีรหัสผ่านอยู่แล้วก็สามารถล็อคอินเข้าใช้งานได้เลย

แต่ถ้าผู้ใช้งานยังไม่มีรหัสผ่านให้ทำการเลือกปุ่ม สมัคร ซึ่งในการสมัครจะต้อง ไปรับ PIN Number และ Serial Number มาจากผู้ให้บริการ แล้วนำ Number ที่ได้ มาสมัคร Account โดยจะต้องกรอกข้อมูลผู้ใช้ตามกฎหมายพรบ. คอมพิวเตอร์ ปี 2550 ดังนี้

1) ชื่อ และ นามสกุล
2) หมายเลขประจำตัวประชาชน
3) E-mail
4) ชื่อผู้ใช้ และ รหัสผ่าน

ข้อดี

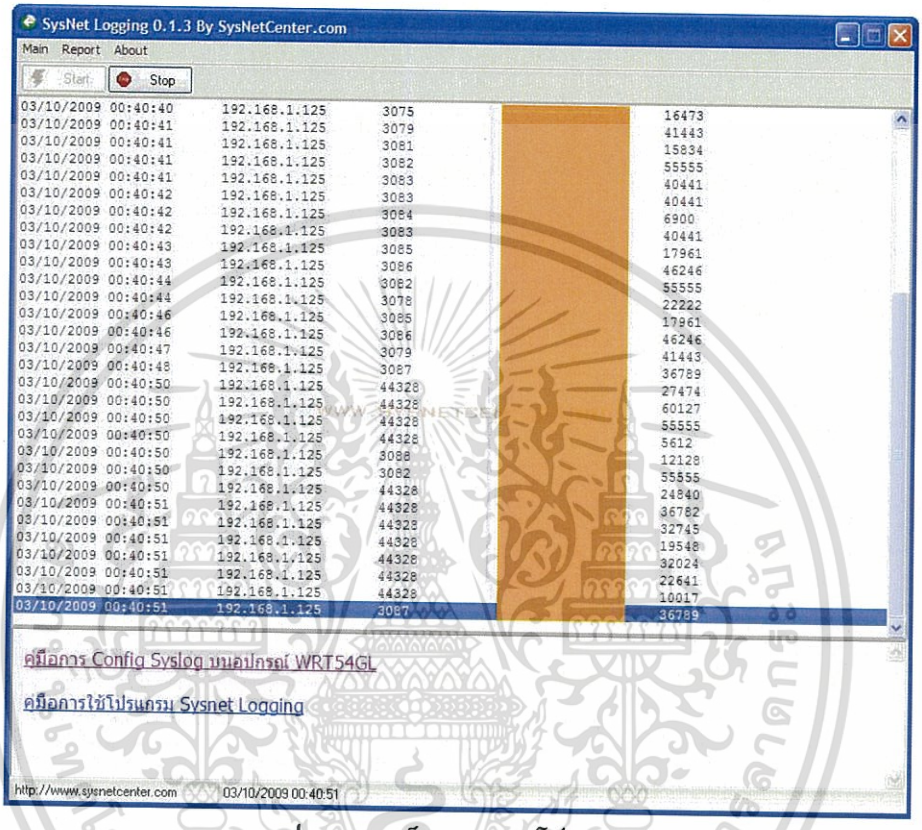
1) ครอบคลุมพื้นที่ส่วนใหญ่ในกรุงเทพฯ
2) ใช้งานสะดวก

ข้อเสีย

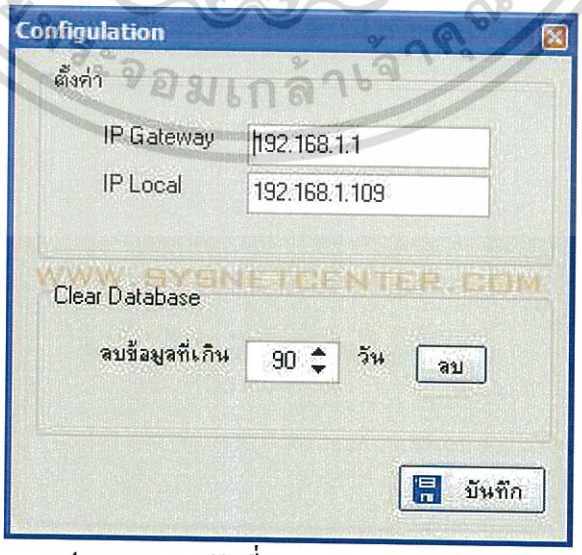
1) จำกัดความเร็วการใช้งาน

2.2.2 Sysnet Logging

เป็นโปรแกรมที่จะทำการเก็บ log ของ IP ต่างๆที่เข้า Internet อาจจะติดตั้งไว้เพื่อตรวจสอบการใช้งาน Internet ภายในองค์กรขนาดเล็ก มีการ Fix IP ไว้ที่เครื่องคอมพิวเตอร์แต่ละเครื่อง เพื่อง่ายต่อการตรวจสอบ



รูป 2.4 การเก็บ log ของโปรแกรม



รูป 2.5 การลบวันที่ตาม พรบ. คอมพิวเตอร์

ข้อดี

1) ใช้งานง่าย

2) โปรแกรมมีขนาดเล็ก

3) เป็นไปตามกฎหมายพรบ.คอมพิวเตอร์ปี 2550

ข้อเสีย

1) ใช้ได้กับองค์กรหรือเครือข่ายที่มีการกำหนด ip แบบ fix เท่านั้น

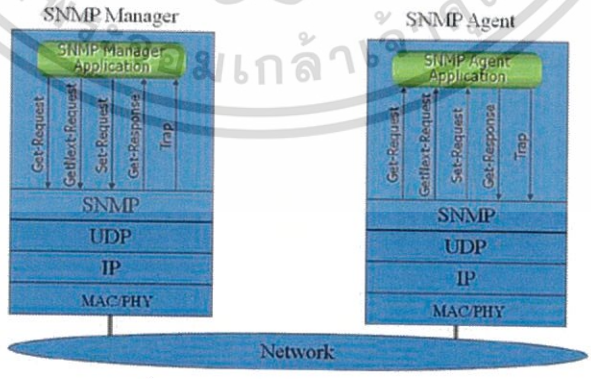
2.2.3 SNMP (Simple Network Management Protocol)

เป็นโปรโตคอลที่ทำงานบนแอพพลิเคชั่นเลเยอร์ของ TCP/IP รับส่งข้อมูลแบบ UDP โดยมีจุดประสงค์หลักเพื่อให้ผู้ดูแลระบบเครือข่ายสามารถเข้ามาจัดการอุปกรณ์เครือข่ายได้จากระยะไกลโดยง่าย

การทำงานของ SNMP ประกอบด้วย 2 ประเภทคือ ตัวเมเนเจอร์และเอเจนต์

ตัวเมเนเจอร์ โดยทั่วไป คือเซิร์ฟเวอร์ที่รันซอฟต์แวร์ หรือโปรแกรมประยุกต์สำหรับการบริหารจัดการระบบเครือข่าย บ่อยครั้งที่เมเนเจอร์ ถูกเรียกว่า NMS (Network Management Stations) เมเนเจอร์มีหน้าที่ร้องขอ (Request บางครั้งเรียกว่า Query) หรือโพลลิ่ง (Polling) หรือรับข้อมูลประเภทแทรป (Trap) ที่ถูกส่งจากตัวเอเยนต์โดยไม่ได้ร้องขอ

เอเยนต์ โดยทั่วไปคือโปรแกรม หรือเฟิร์มแวร์ (Firmware) ที่ติดตั้ง และทำงานบนตัวอุปกรณ์เครือข่ายที่ผู้ดูแลระบบเครือข่ายต้องการจัดการ ซึ่งอาจจะเป็นโปรแกรมเฉพาะ และทำงานเบื้องหลังเป็นแบ็กกราวด์โปรเซส (Background Process) หรือเดมอน (Daemon) เช่น ในไมโครซอฟต์วินโดว์ หรือยูนิกซ์ หรือเป็นส่วนหนึ่งในระบบปฏิบัติการ เช่น ในเราเตอร์ของ CISCO ซึ่งเป็นเฟิร์มแวร์ระดับต่ำ



รูป 2.6 การส่งข้อมูลบน SNMP

ข้อดี

1) สามารถจัดการความผิดปกติบนเครือข่ายได้
2) สามารถตั้งค่าอุปกรณ์ได้บางชนิด

ข้อเสีย

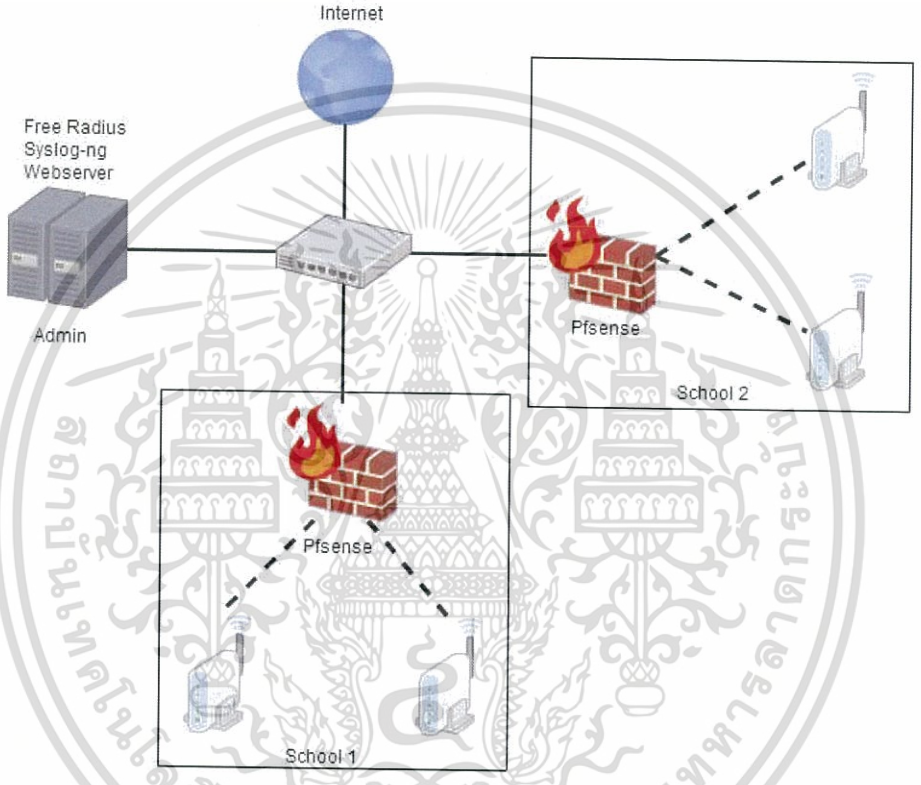
2) ใช้ traffic เพิ่มขึ้นจากการส่งข้อมูลให้เมเนเจอร์
3) ต้องมีการติดตั้งเมเนเจอร์และเอเจนต์

บทที่ 3

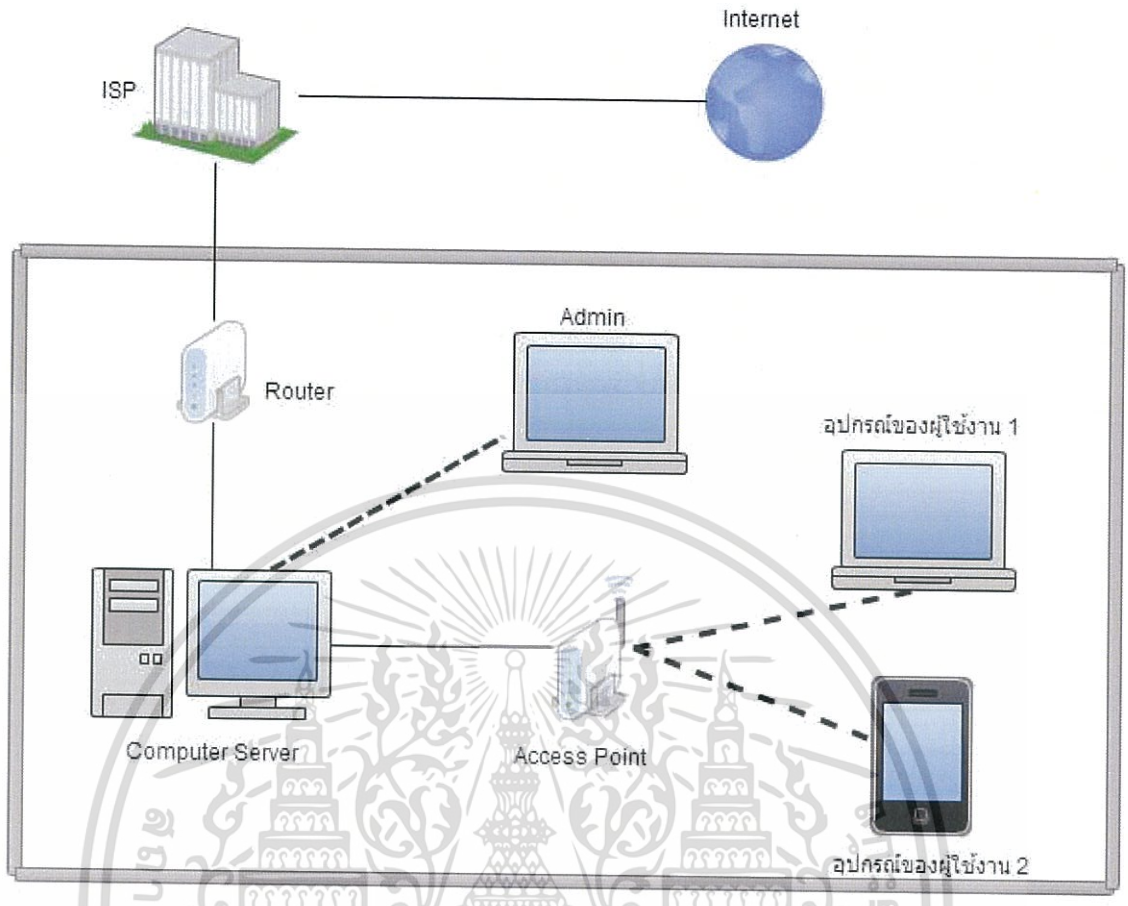
การออกแบบและพัฒนา

3.1 ภาพรวมของระบบ

3.1.1 ภาพรวมของระบบเมื่อนำไปใช้งานจริง



รูป 3.1 การวางตำแหน่งอุปกรณ์



รูป 3.2 การติดตั้งระบบในการใช้งานจริง

3.1.1.1 Computer Server 1 เครื่อง

Computer Server จะเป็นศูนย์กลางในการบริหารจัดการระบบทั้งหมด ซึ่งจะติดตั้ง Virtual Box โดยจะจำลองเครื่องคอมพิวเตอร์ขึ้นมา 2 เครื่อง แต่ละเครื่องจะติดตั้งซอฟแวร์ดังนี้

1) เครื่องที่ 1
   A) ติดตั้ง Pfsense
2) เครื่องที่ 2
   A) ติดตั้ง ubuntu server
      a) ติดตั้ง Free Radius
      b) ติดตั้ง Syslog-ng
      c) ติดตั้ง Web Server (Apache)

3.1.1.2 Access Point

เป็นอุปกรณ์สำหรับให้ผู้ใช้งานเชื่อมต่อกับระบบ ผ่าน Access Point

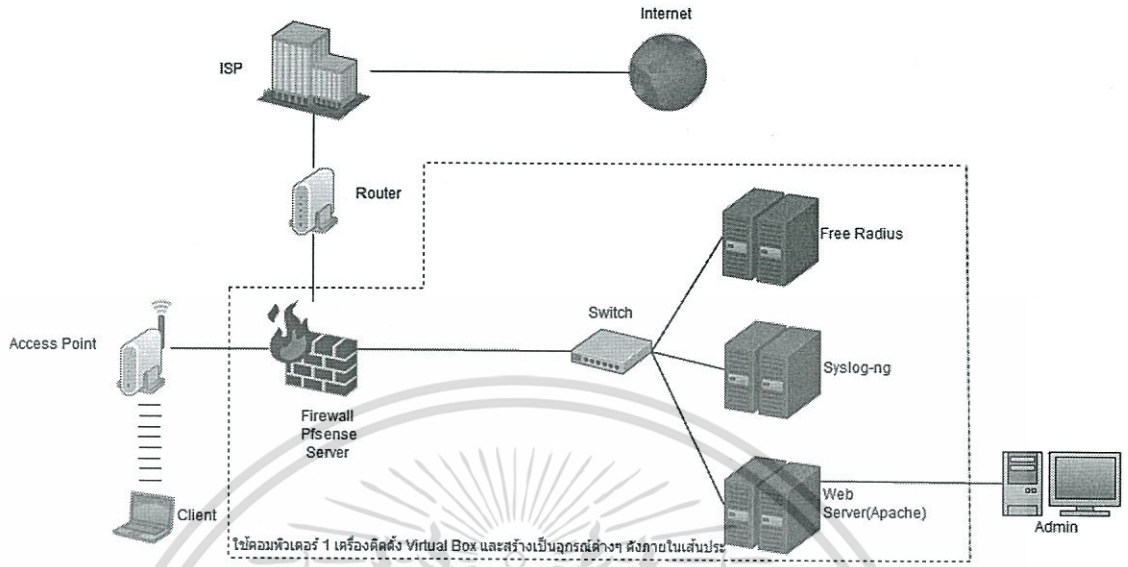
3.1.1.3 อุปกรณ์ของผู้ใช้งาน

เป็นอุปกรณ์ที่ผู้ใช้งาน ทำการเชื่อมต่อกับระบบผ่านเครือข่ายไร้สาย เช่น Notebook, Smart Phone เป็นต้น

3.1.1.4 Admin

คืออุปกรณ์ที่ Admin ทำการเชื่อมต่อกับระบบ เพื่อที่จะบริหารจัดการ หรือ Monitor ระบบ

3.1.2 ภาพรวมของระบบในการจำลองการทำงาน



รูป 3.3 การออกแบบระบบแบบ Logical

3.1.2.1 Free Radius

1) เป็น Server สำหรับการ Authen ของผู้ใช้งานในระบบ
2) เป็น Server สำหรับเก็บข้อมูลผู้ใช้งาน ในระบบ

3.1.2.2 Syslog-ng

1) เป็น Server สำหรับการเก็บ Log การใช้งานของผู้ใช้งาน
2) นำ Log จาก Syslog-ng ไปวิเคราะห์ เพื่อทำเป็นระบบMonitoring สำหรับ Admin

3.1.2.3 Web Server

1) นำ Log จาก Syslog-ng มาประมวลผลเพื่อตรวจสอบการทำงานของ Access Point
2) เป็น Server สำหรับทำเว็บไซต์ของระบบ โดยจะมี 2 ส่วนคือ
   A) สำหรับผู้ใช้งานทั่วไปทำการ Authen ระบบ เพื่อเข้าใช้งาน
   B) สำหรับ Admin เพื่อที่จะบริหารจัดการและ Monitoring ระบบ

3.1.2.4 Firewall Pfsense Server

1) เป็นตัวกลางในการควบคุมการเข้าใช้งานของผู้ใช้ในระบบ
2) เป็นตัวกลางในการส่งผ่านข้อมูลการใช้งาน (Packet)
3) เป็นตัวกลางในการเชื่อมต่อระหว่างอุปกรณ์ต่างๆ

3.2 ความต้องการของระบบ

3.2.1 อุปกรณ์ที่ใช้

3.2.1.1 Hardware

1) Access point
2) คอมพิวเตอร์อย่างน้อย 1 เครื่อง
3) Router (กรณีที่ใช้บริการ ADSL)

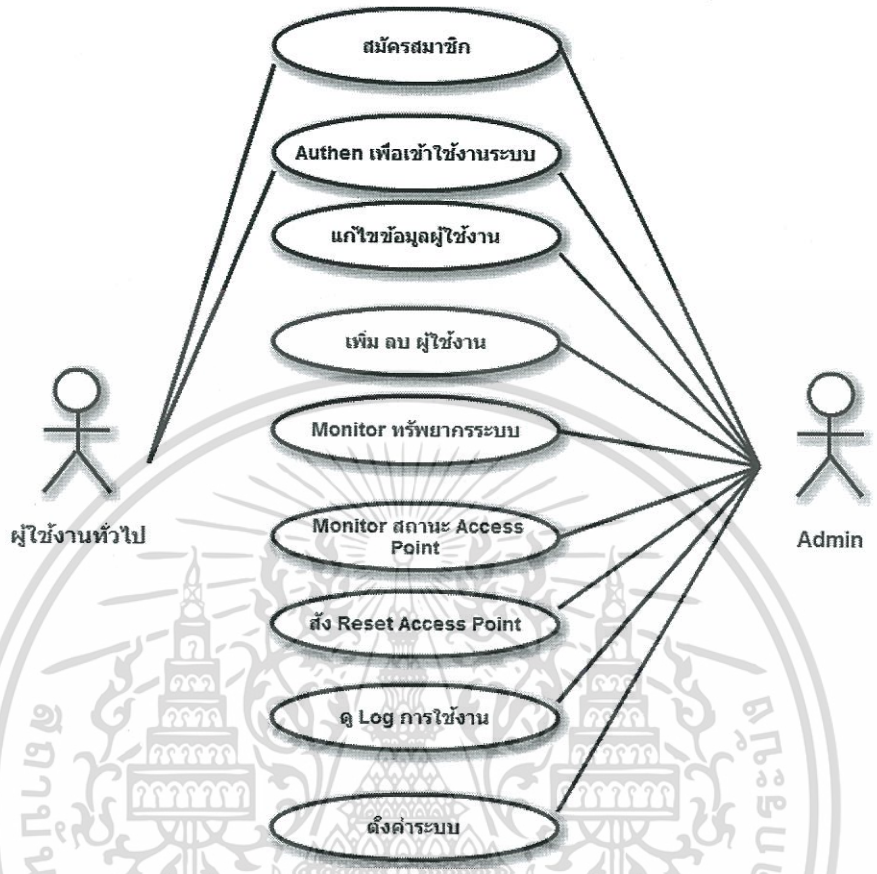
3.2.1.2 Software

1) ซอฟต์แวร์ Virtual Box
2) ซอฟต์แวร์ Free Radius
3) ซอฟต์แวร์ Syslog - ng
4) ซอฟต์แวร์ Apache
5) ซอฟต์แวร์ Pfsense

3.2.1.3 ระบบปฏิบัติการ

1) Ubuntu Server

3.3 Usecase Diagram



รูป 3.4 Usecase diagram

3.3.1 สิ่งที่ผู้ใช้งานทั่วไปทำได้

1) สมัครสมาชิก
2) Authen เพื่อเข้าใช้งานระบบ
3) สมัครใช้งาน แบบ Guest

3.3.2 สิ่งที่ Admin ทำได้

1) สมัครสมาชิก
2) Authen เพื่อเข้าใช้งานระบบ
3) แก้ไขข้อมูลผู้ใช้งาน(แก้อะไร)
4) เพิ่ม ลบ ผู้ใช้งาน
5) Monitor ทรัพยากรระบบ
6) Monitor สถานะ Access Point
7) สั่ง Reset Access Point

8) ดู Log การใช้งาน

9) ตั้งค่าต่างๆของระบบ

3.4 คุณสมบัติของระบบ

3.4.1 คุณสมบัติ

1) เว็บไซต์

A) สำหรับ User

a) สมัครสมาชิกชั่วคราว

b) Authentication

I) Username

II) Password

B) สำหรับ Admin

a) ระบบ Monitoring

I) Monitoring ระบบ

i) ดูทรัพยากรระบบ

1st) ดู CPU

2nd) ดู RAM

3rd) ดู HDD

ii) ดู Access Point

1st) ดูที่ตั้ง Access Point (ดูจาก Database)

2nd) ดูสถานะ Access Point (สถานะการรับส่งข้อมูล)

b) ระบบ Management

I) Manage ผู้ใช้งาน

i) บริหารผู้ใช้งาน

1st) เพิ่มผู้ใช้งาน

2nd) ลบผู้ใช้งาน

3rd) แก้ไขข้อมูลผู้ใช้งาน

II) Manage ระบบ

i) มองเห็นการทำงานของ Access Point

ii) สั่ง Reset Access Point

III) ดู Log การใช้งาน

i) ระบบออก Report

ii) ออก Report เกี่ยวกับ Log การใช้งาน

2) ระบบเก็บ Log การใช้งาน

A) เก็บ Log การใช้งานของผู้ใช้ตามพรบ. ว่าด้วยการกระทำผิดทางคอมพิวเตอร์

a) เก็บเป็นระยะเวลา 90 วัน

I) ชื่อ User

II) เวลาที่ใช้ (Time)

III) IP ปลายทาง

IV) Port ปลายทาง

V) Port ต้นทาง

3) ระบบเก็บข้อมูลผู้ใช้งาน

A) เก็บข้อมูลผู้ใช้งานตามพรบ. ว่าด้วยการกระทำผิดทางคอมพิวเตอร์

a) ชื่อ นามสกุล

b) รหัสบัตรประชาชน

c) Username

d) Password

3.4.2 การใช้งานระบบ

3.4.2.1 มุมมองผู้ใช้งาน

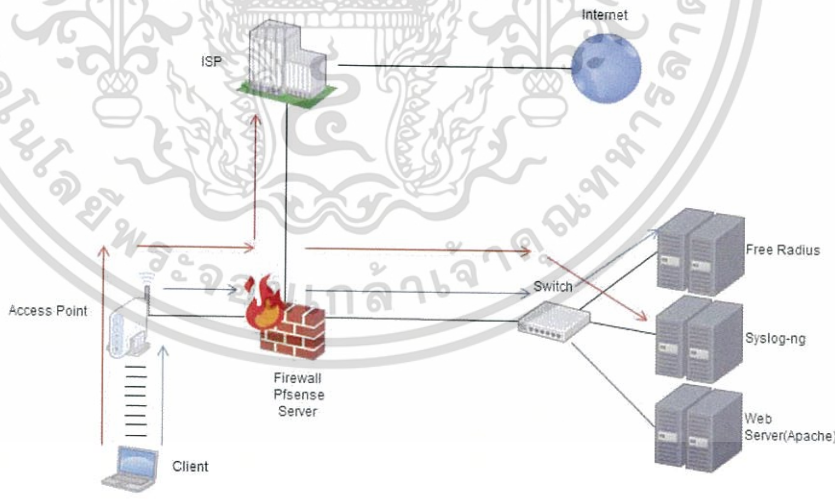
การเข้าใช้งานของผู้ใช้งาน (สำหรับผู้ใช้งานใหม่ที่ไม่เคยลงทะเบียนมาก่อนและต้องการเป็นสมาชิกถาวร)

1) ผู้ใช้งานต้องทำการลงทะเบียนกับผู้ดูแลระบบโดยใช้บัตรประชาชน
2) ผู้ดูแลระบบจะทำการลงทะเบียนผู้ใช้งาน และให้ username กับ password แก่ผู้ใช้งาน
3) ผู้ใช้งานสามารถนำ username กับ password ไปใช้ทำการ log in เข้าใช้งานได้ทันที

การเข้าใช้งานของผู้ใช้งาน (สำหรับผู้ใช้งานใหม่ที่ไม่เคยลงทะเบียนมาก่อนและต้องการเป็นสมาชิกชั่วคราว)

1) ผู้ใช้งานทำการลงทะเบียนผ่านหน้าเว็บไซต์
2) ผู้ใช้งานสามารถนำ username กับ password ไปใช้ทำการ log inเข้าใช้งานได้ทันที โดยผู้ใช้งานจะมีสถานะเป็น “Guest” และจะมีอายุการใช้งานถึง เที่ยงคืน (00.00 นาฬิกา) ของวันนั้นๆ

3.4.2.2 มุมมองของระบบ



รูป 3.5 มุมมองการทำงานของระบบ

การเข้าใช้งานของผู้ใช้งาน(จากภาพจะเป็นเส้นสีน้ำเงิน)

1) ผู้ใช้งานทำการเชื่อมต่อ Access point
2) Pfsense server ทำการร้องขอสิทธิ์การใช้งาน กับ Free Radius (Authentication) โดยจะแสดงหน้า log in ออกมา

3) ผู้ใช้ทำการ Login เข้าใช้งาน

4) Free Radius ให้สิทธิ์การใช้งานแก่ผู้ใช้งาน

การใช้งานของผู้ใช้งานหลังได้รับสิทธิ์การใช้งาน(จากภาพจะเป็นเส้นสีแดง)

1) ผู้ใช้งานทำการใช้งานตามปกติ

2) Pfsense server ทำการ Forward ข้อมูล พร้อมๆกับส่งข้อมูลการใช้งานไปให้ syslog-ng เก็บ log ไว้

3.4.2.3 มุมมองของผู้ดูแลระบบ

ผู้ดูแลระบบจะจัดการสิ่งต่างๆจากหน้าเว็บของระบบที่อยู่บน Web Server โดยจะสามารถ

1) จัดการกับผู้ใช้งาน
   A) ตัดผู้ใช้ออกจากระบบ
   B) เพิ่มผู้ใช้งานใหม่
   C) ลบผู้ใช้งาน
   D) แก้ไขข้อมูลผู้ใช้งาน
2) จัดการ Access Point
   A) มองเห็นการทำงานของ Access Point
   B) สามารถ Reset Access Point ได้

3.5 การทำงานของระบบ

3.5.1 การออกแบบ Database

ใช้ MySQL เป็น Database โดยมี 2 Database คือ

1) Database เก็บรายชื่อผู้ใช้งาน

2) Database เก็บ log การใช้งาน

โดยโครงสร้างของ Database เก็บรายชื่อผู้ใช้งาน ประกอบไปด้วย Username, Password, ชื่อผู้ใช้, นามสกุล, รหัสบัตรประชาชน, email

ตาราง 3.1 ตัวอย่าง Database เก็บชื่อผู้ใช้งาน

Username	Attribute	op	Value	Name	Surname	IDCard	email	Class
143569	User-Password	==	JhJ9	มานะ	มานี	1100701772791	manee@gmail.com	Admin

ส่วนโครงสร้าง Database เก็บ log การใช้งาน ใช้ตามโครงสร้างของ syslog-ng คือ <priority> VERSION ISOTIMESTAMP HOSTNAME APPLICATION PID MESSAGEID STRUCTURED-DATA MSG

ตาราง 3.2 ตัวอย่าง Database เก็บ log การใช้งาน

Host	Facility	Prioty	Level	Tag	Datetime	Program	Msg	Seq
192.168.2.1	local4	info	info	86	2016-02-18 16:33:41	filterlog	90,16777216,,100000101,em1,match,pass ,in,4,0x0,,64,21942,0,DF,6,tcp,60, **sort_ip,des_ip,**47478,443,0,S,4026572576,,29200,,mss;sackOK;TS;nop;wscale	209

3.5.2 การ Monitoring Access Point

การ Monitoring Access Point ใช้วิธีการ ให้หน้าเว็บไซต์ ทำการ Ping ไปยัง Access Point ตามรายชื่อที่มีใน Database เพื่อดูสถานะการรับส่งข้อมูล(Packet Loss) ของ Access Point แล้วนำไปแสดงบนหน้าเว็บไซต์ หาก Access point ไม่มีการตอบสนอง ก็จะเก็บลงใน Database เพื่อเป็นประวัติการทำงานผิดปกติด้วย

ในกรณีที่ผู้ดูแลระบบเปิดหน้าเว็บไซต์ไว้ เมื่อระบบได้รับว่ามีสถานะการรับส่งข้อมูลของ Access Point ตัวใดตัวหนึ่งมีค่าที่น้อยกว่าค่าที่ได้ประเมินไว้ ระบบจะแสดงการแจ้งเตือนว่า Access Point มีปัญหาและให้เลือกว่าจะทำการ Reboot Access Point หรือไม่ ถ้า Reboot สำเร็จ ก็จะเก็บลงในประวัติว่า สามารถ Reboot ได้ เมื่อเกิดปัญหาขึ้นมา

ในกรณีที่ผู้ดูแลระบบไม่ได้เปิดหน้าเว็บไซต์ไว้หรือไม่ได้อยู่ดูแลระบบ ระบบจะทำการตรวจสอบสถานะการรับส่งของ Access Point ทุกๆ 15 นาที ด้วย crontab ที่สั่งรัน shell script ไว้ เมื่อระบบได้รับว่ามีสถานะการรับส่งข้อมูลของ Access Point ตัวใดตัวหนึ่งมีค่าที่น้อยกว่าค่าที่ได้กำหนดไว้ ระบบจะทำการ Reset Access Point ตัวนั้นโดยอัตโนมัติ และเก็บไว้ในประวัติการแก้ปัญหาด้วยเช่นกัน ว่าผลการแก้ไขปัญหา เป็นอย่างไรบ้าง

เหตุผลที่ไม่ใช้ SNMP เนื่องจาก SNMP จำเป็นต้องมีการติดตั้งเมเนเจอร์ และเอเจนต์ที่อุปกรณ์ และมีความซับซ้อนในการตั้งค่า บนยี่ห้อ และรุ่นของอุปกรณ์ที่ต่างกันอยู่ นอกจากนี้ ยังมีการใช้ traffic ที่เพิ่มขึ้นมากพอสมควร ซึ่งมากกว่าการทดสอบด้วยการ ping ยิ่งถ้าเครือข่ายมีขนาดใหญ่มากเท่าไหร่ SNMP traffic ก็ยิ่งใช้งานมากเพิ่มขึ้นเท่านั้น

3.5.3 การ Reset Access Point

ใช้การสั่งงานด้วย SSH(Secure Shell) เข้าไปสั่ง Access Point แล้วใช้คำสั่ง Reboot โดยผู้ดูแลระบบจะสามารถสั่งการรีเซ็ต Access Point ได้ผ่านหน้าเว็บไซต์ โดยไม่ต้องเข้าไปในหน้า config ของ Access Point แต่ละตัว

3.5.4 การ Monitor ทรัพยากร Firewall

ใช้การสั่งงานด้วย SSH(Secure Shell) เข้าไปควบคุม Firewall ให้แสดงค่าทรัพยากรต่างๆของ Firewall กลับมา และนำกลับมาเขียนลงไปในไฟล์ที่อยู่บนเครื่อง server และนำไปแสดงบนหน้าเว็บไซต์จากจากนำค่าในไฟล์มาแสดง หาก Firewall ไม่มีการตอบสนอง ก็จะมีการเก็บไว้ในประวัติว่า Firewall ไม่มีการตอบสนอง เมื่อเวลา และวันที่เท่าไหร่

3.5.5 การเก็บ log

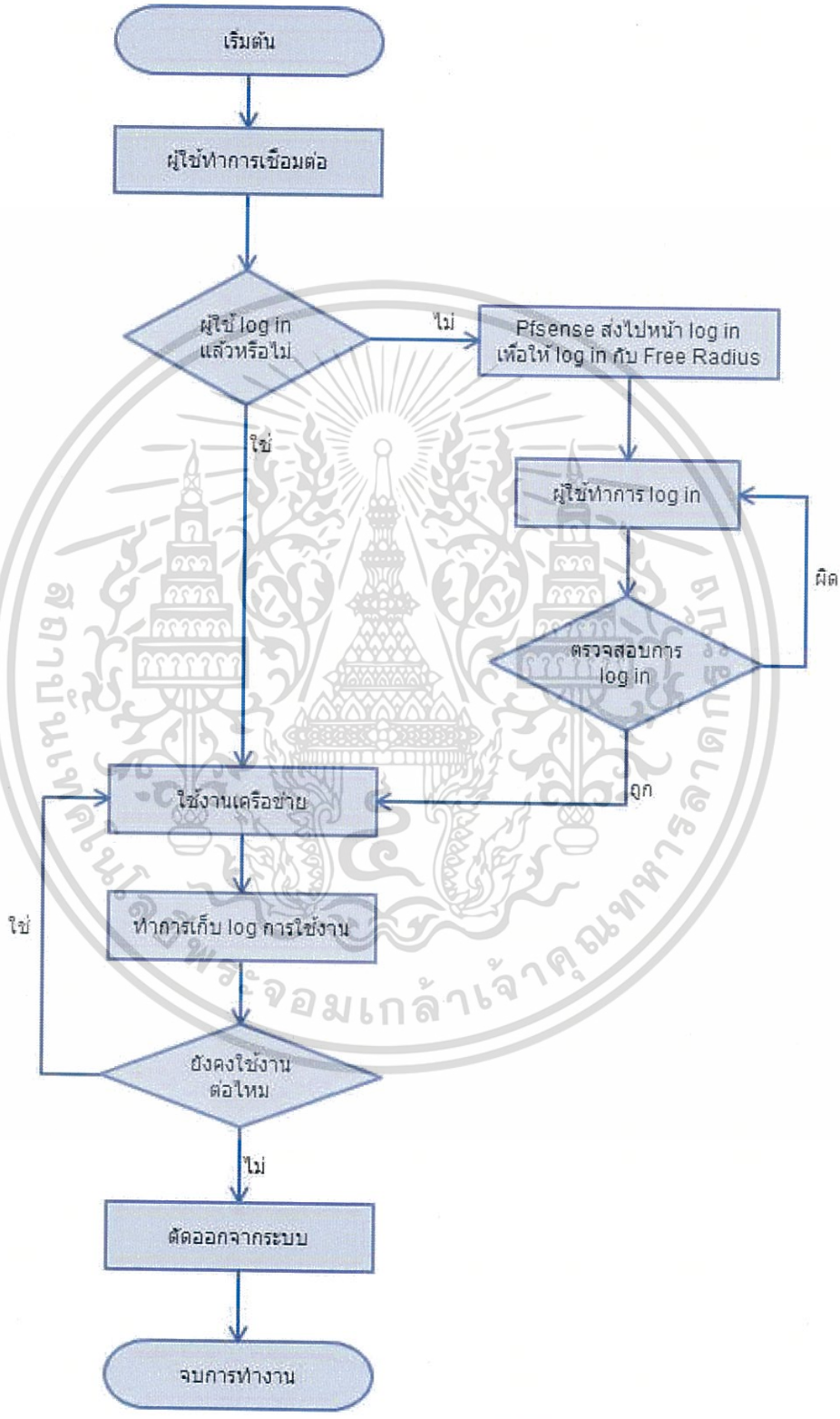
ใช้ syslog-ng ในการเก็บ log โดยจะได้รับ log การใช้งานจาก pfsense แล้วทำการเก็บลงใน syslog-ng แล้วส่งต่อให้ฐานข้อมูลอีกที เพื่อให้ admin ของระบบ สามารถทำการตรวจสอบ log และนำ log ออกมาในรูปแบบของ excel ได้

3.5.6 การนำออก log การใช้งาน

เมื่อเจ้าหน้าที่ต้องการนำ log การใช้งานไปตรวจสอบ เจ้าหน้าที่จะทำการนำออก log การใช้งานด้วยตัวเองในรูปแบบของฮาร์ดดิสก์หรือไฟล์ log เมื่อเจ้าหน้าที่นำ log ออกมาเป็นที่เรียบร้อยเจ้าหน้าที่จะให้ผู้ดูแลระบบลงนามกำกับเพื่อเป็นหลักฐาน โดยผู้ดูแลระบบจะไม่สามารถยุ่งเกี่ยวหรือแก้ไขข้อมูล log การใช้งานของระบบได้เลย

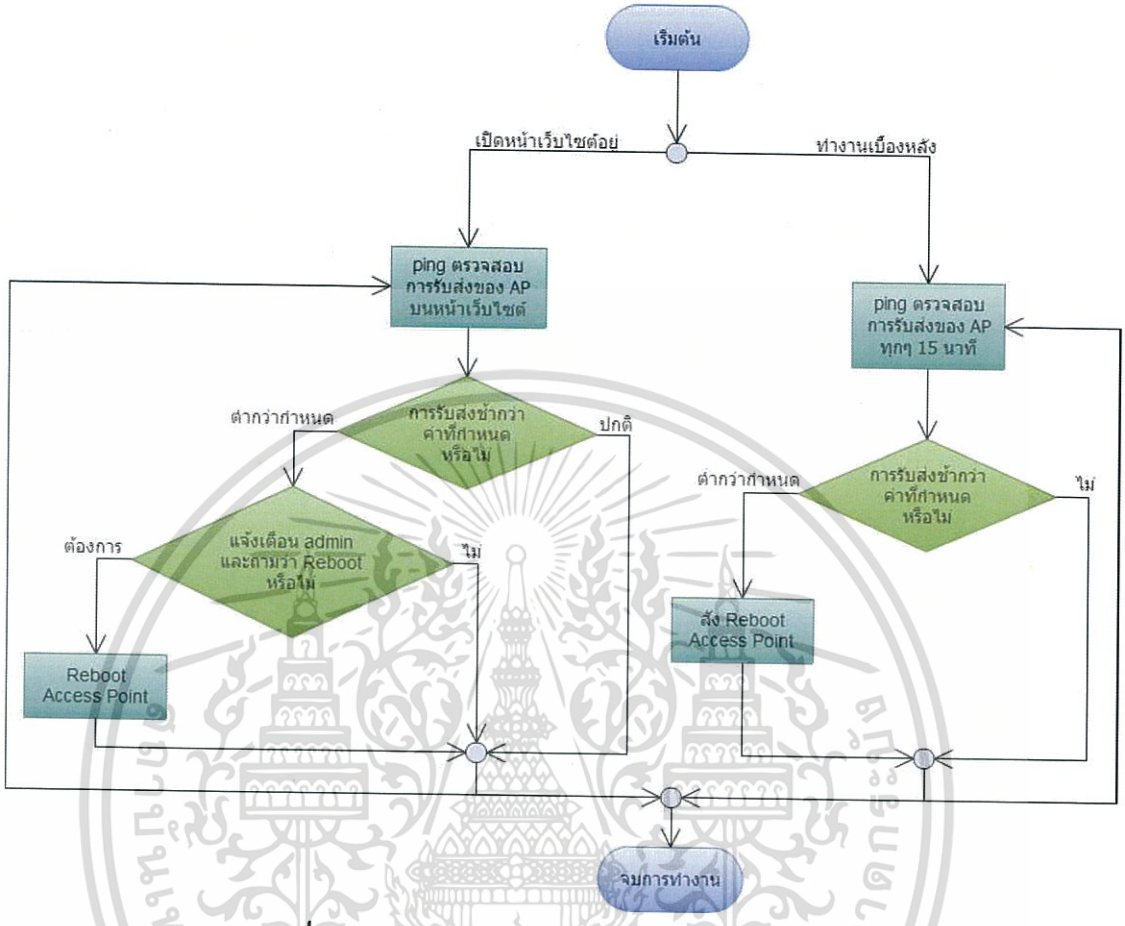
3.6 Flowchart

3.6.1 การเข้าใช้งาน



รูป 3.6 Flowchart การเข้าใช้งาน

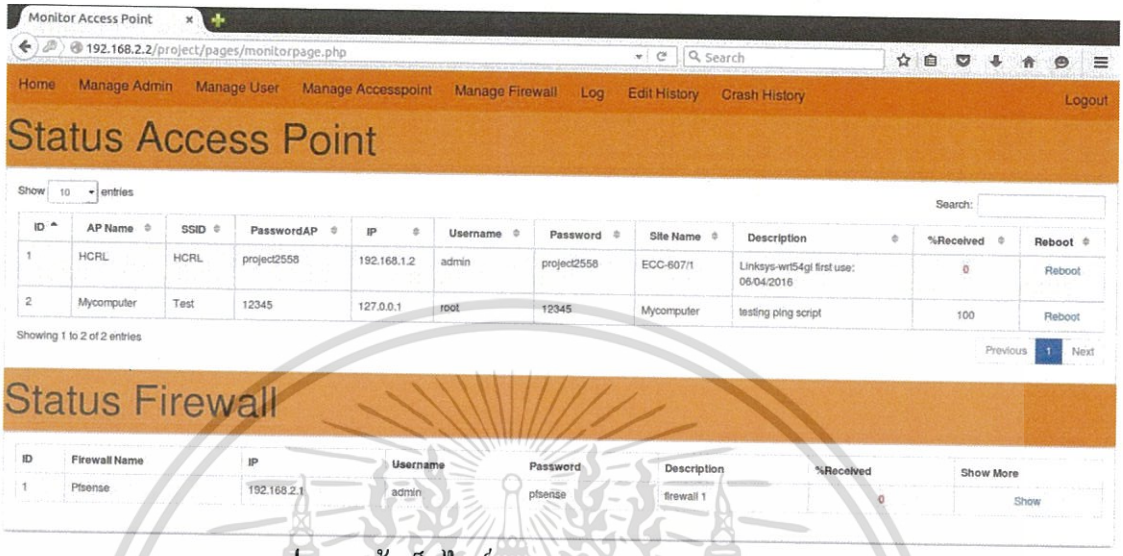
3.6.2 การ Monitoring Access Point



รูป 3.7 Flowchart การ Monitoring Access Point

3.7 การออกแบบหน้าเว็บไซต์

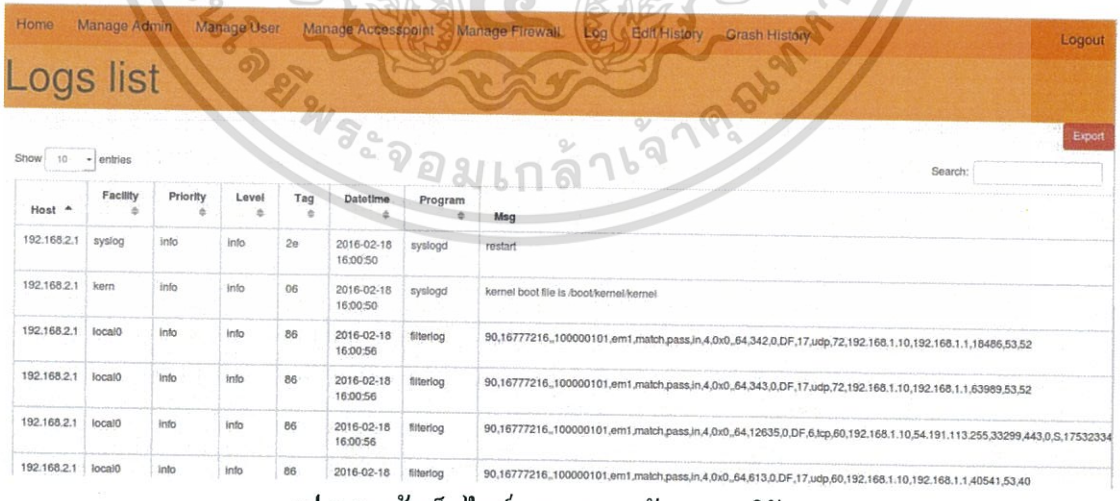
3.7.1 หน้าเว็บไซต์ Monitor สถานะของระบบ



รูป 3.8 หน้าเว็บไซต์การ Monitor สถานะของระบบ

ออกแบบหน้าเว็บไซต์การ Monitor สถานะของระบบ โดยให้สามารถดูสถานะของ Access Point และ Firewall ในระบบผ่านหน้าเว็บไซต์หน้าเดียวและสามารถสั่ง Reboot Access Point ผ่านหน้าเว็บไซต์นี้ได้เลย

3.7.2 หน้าเว็บไซต์แสดง Log ข้อมูลการใช้งาน



รูป 3.9 หน้าเว็บไซต์แสดง Log ข้อมูลการใช้งาน

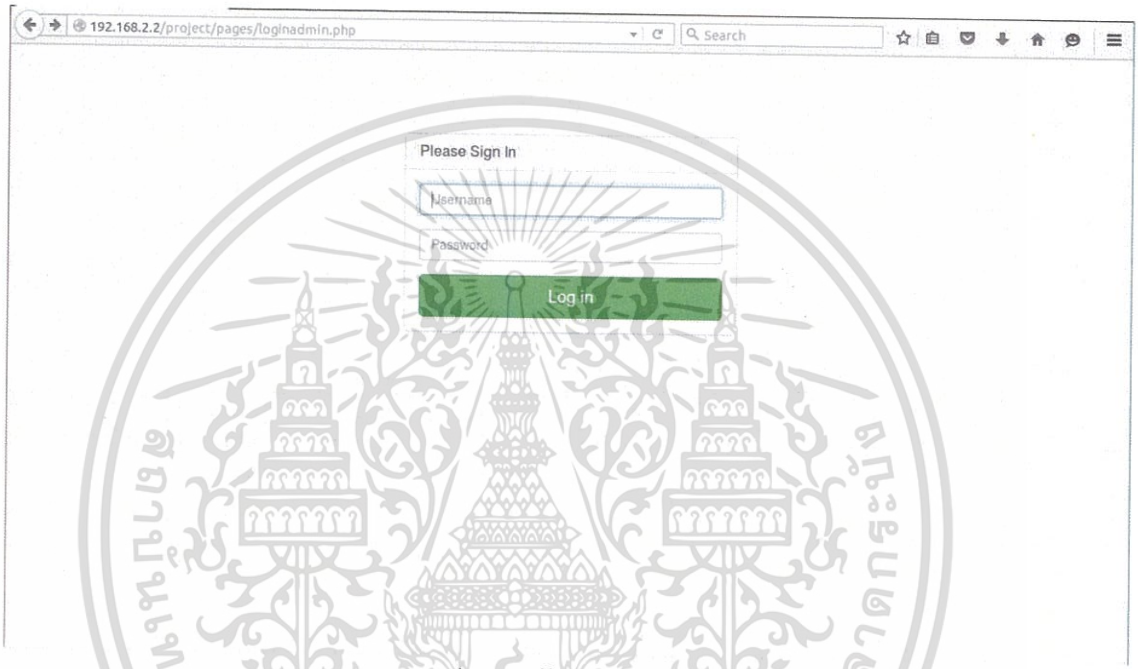
ออกแบบหน้าเว็บไซต์ให้แสดง Log การใช้งานของผู้ใช้งานผ่านหน้าเว็บไซต์ เพื่อในกรณี Admin จะตามตัวผู้ใช้งานผ่านการดู Log การใช้งาน

บทที่ 4

การทดลอง

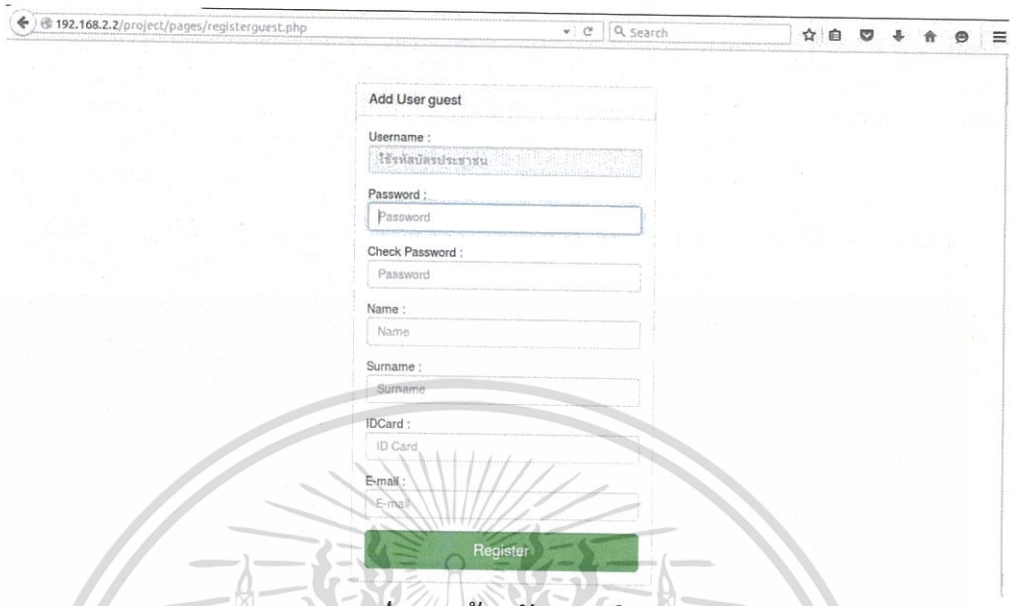
4.1 การสร้างหน้าเว็บไซต์

1) หน้าเว็บล็อกอิน เป็นหน้าเว็บสำหรับให้ Admin เข้าใช้งานระบบ



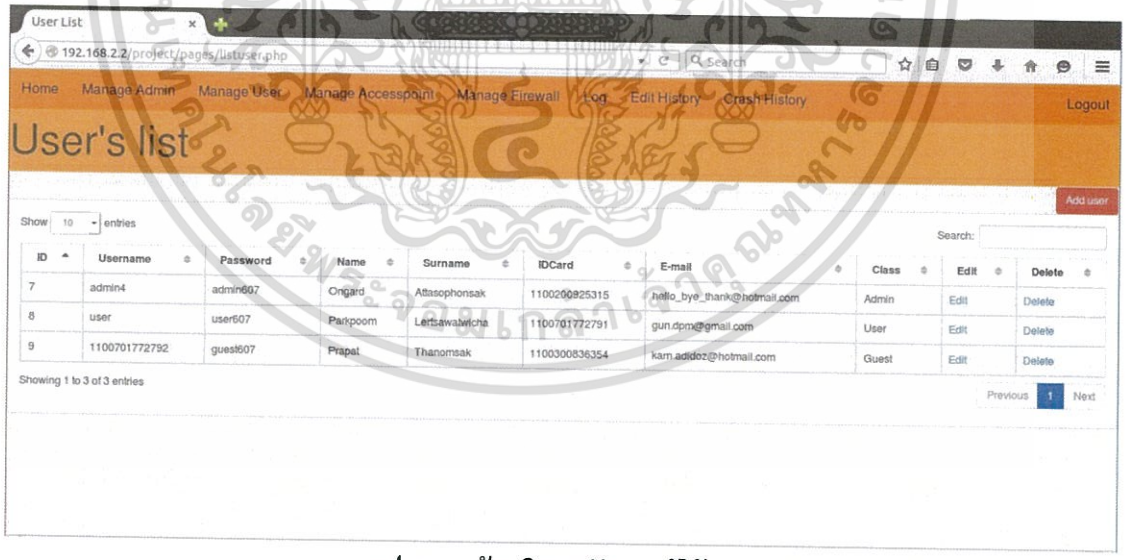
รูป 4.1 หน้าเว็บล็อกอิน

2) หน้าสมัครสมาชิก เป็นหน้าเว็บสำหรับให้ผู้ใช้งานสมัครเป็นสมาชิกชั่วคราว



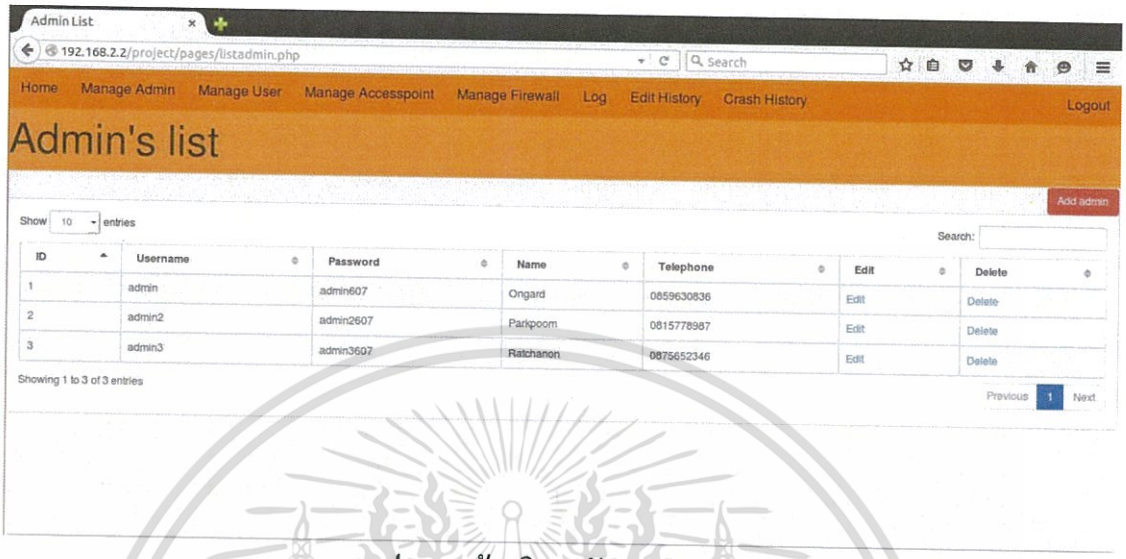
รูป 4.2 หน้าสมัครสมาชิก

3) หน้าบริหารจัดการข้อมูลผู้ใช้งาน เป็นหน้าเว็บสำหรับให้ Admin ดูข้อมูลผู้ใช้งาน และสามารถแก้ไข เพิ่ม หรือลบผู้ใช้งานได้



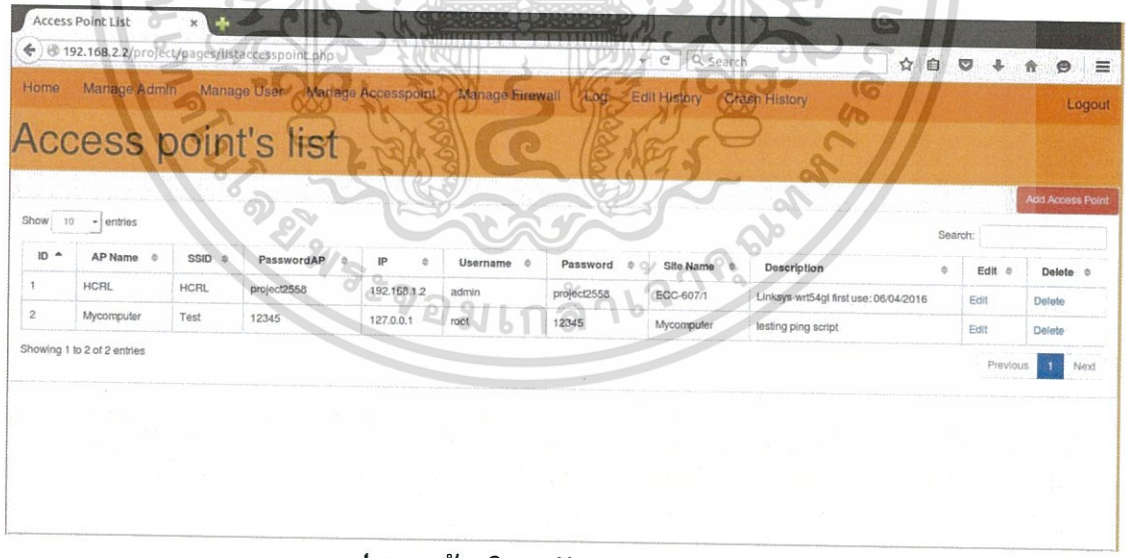
รูป 4.3 หน้าบริหารจัดการผู้ใช้งาน

4) หน้าบริหารจัดการ Admin เป็นหน้าเว็บสำหรับให้ Admin ดูข้อมูลของ Admin ที่มีในระบบ และสามารถแก้ไข เพิ่ม หรือลบ Admin ได้



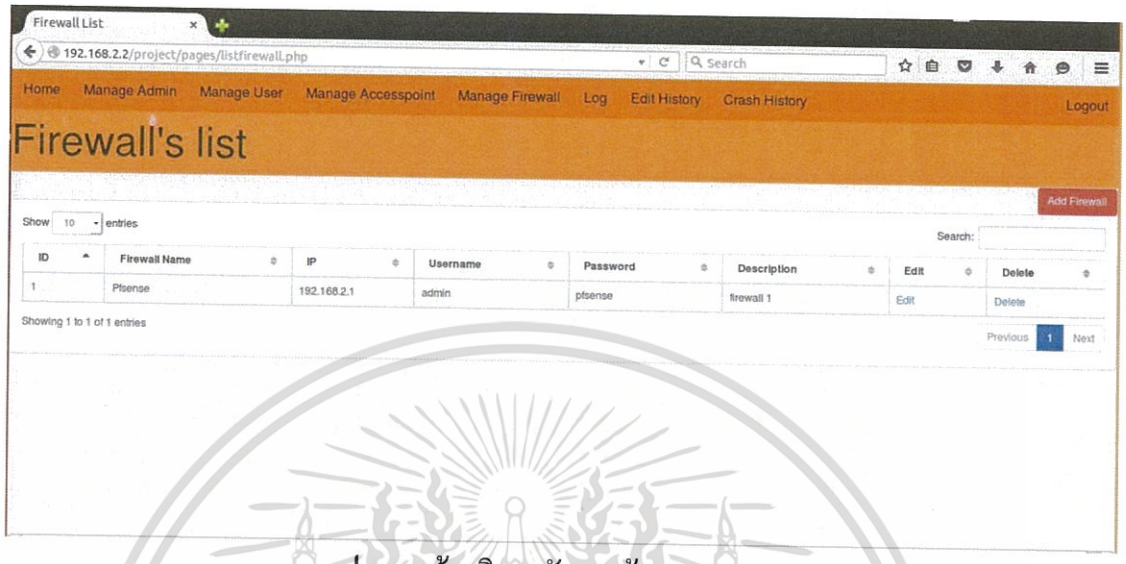
รูป 4.4 หน้าบริหารจัดการ Admin

5) หน้าบริหารจัดการ Access Point เป็นหน้าเว็บสำหรับให้ Admin ดูข้อมูลของ Access Point และสามารถแก้ไข เพิ่ม หรือลบข้อมูล Access Point ได้



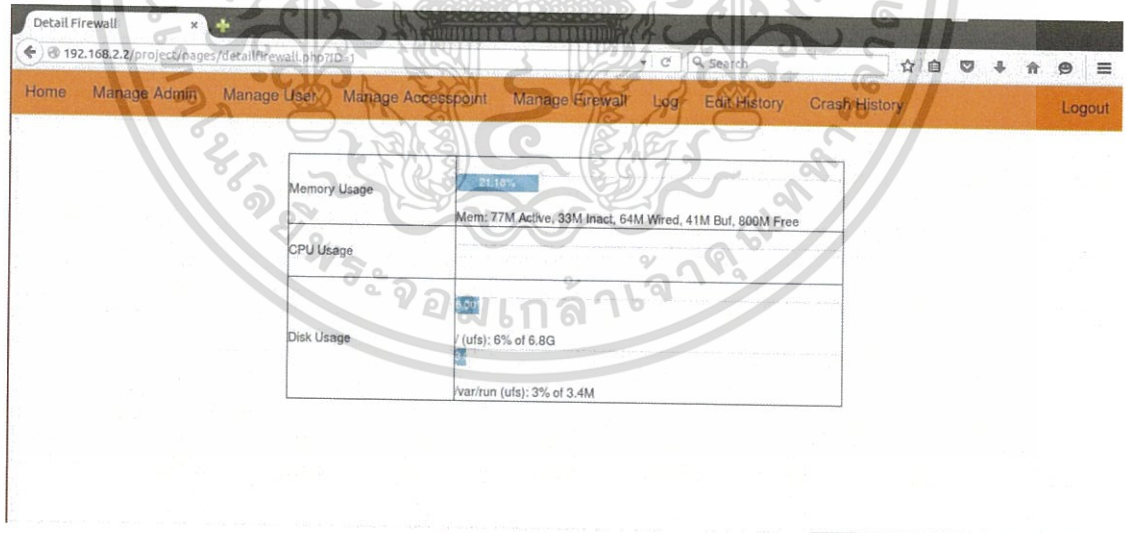
รูป 4.5 หน้าบริหารจัดการ Access Point

6) หน้าบริหารจัดการข้อมูล Firewall เป็นหน้าเว็บสำหรับให้ Admin ดูข้อมูลของ Firewall และสามารถแก้ไข เพิ่ม หรือลบข้อมูล Firewall ได้



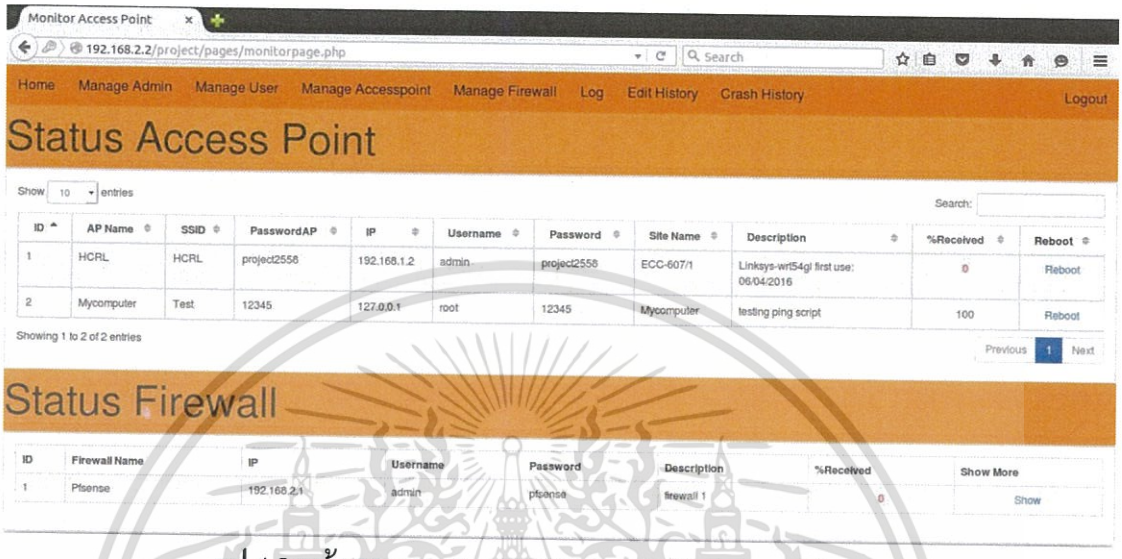
รูป 4.6 หน้าบริหารจัดการข้อมูล Firewall

7) หน้าแสดงทรัพยากรของ Firewall เป็นหน้าเว็บสำหรับให้ Admin ดูข้อมูลการใช้งานทรัพยากรของ Firewall



รูป 4.7 หน้าแสดงทรัพยากรของ Firewall

8) หน้า Monitoring สถานะ Access Point และ Firewall เป็นหน้าเว็บสำหรับให้ Admin ดูสถานะของ Access Point และ Firewall ในระบบ โดยจะทดสอบสถานะด้วยการ ping ไปทุกๆ 10 วินาที

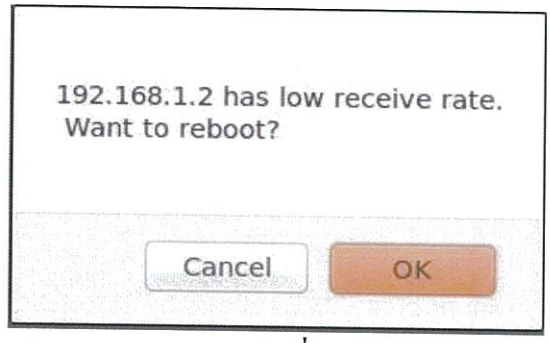


รูป 4.8 หน้า Monitoring สถานะ Access Point และ Firewall

9) หน้าแสดง Log การใช้งานของผู้ใช้งาน เพื่อให้ Admin สามารถดู Log การใช้งานของผู้ใช้งานได้

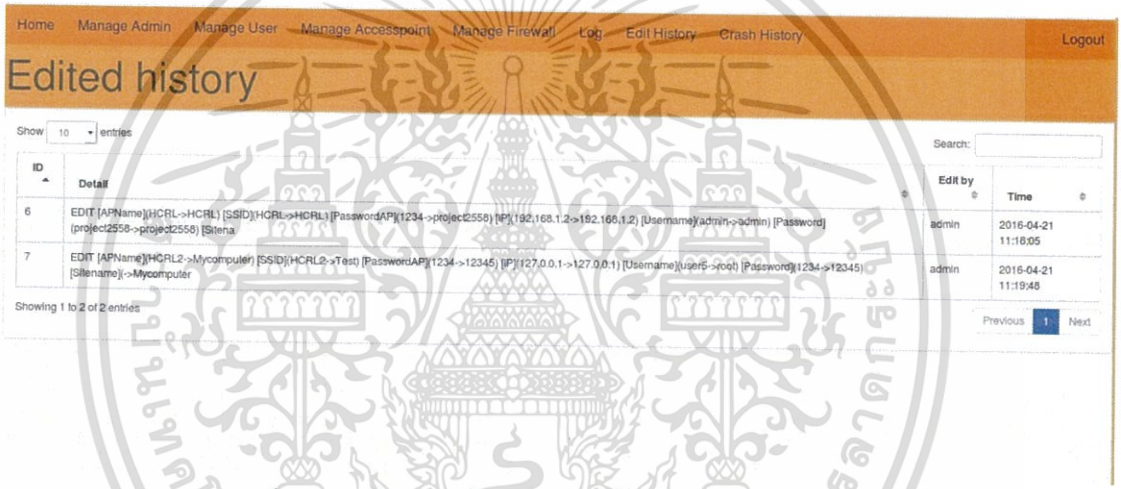
รูป 4.9 หน้าแสดง Log การใช้งานของผู้ใช้งาน

10) Pop up แสดงสถานะ Access Point เมื่อ Access Point มีสถานะต่ำกว่าที่กำหนด



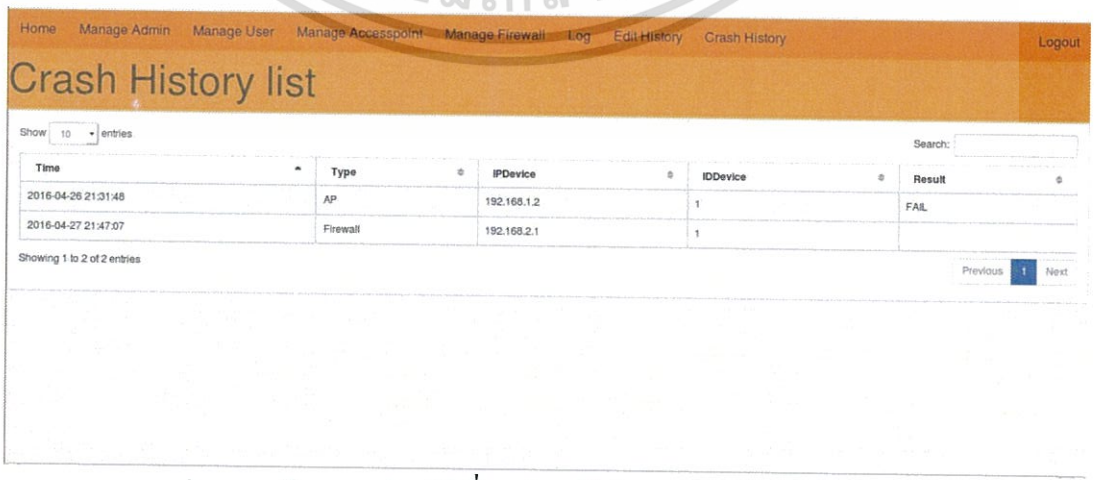
รูป 4.10 Pop up แสดงสถานะ Access Point เมื่อ Access Point มีสถานะต่ำกว่าที่กำหนด

11) หน้าแสดงประวัติการแก้ไขข้อมูลต่างๆในระบบ



รูป 4.11 หน้าแสดงประวัติการแก้ไขข้อมูลต่างๆในระบบ

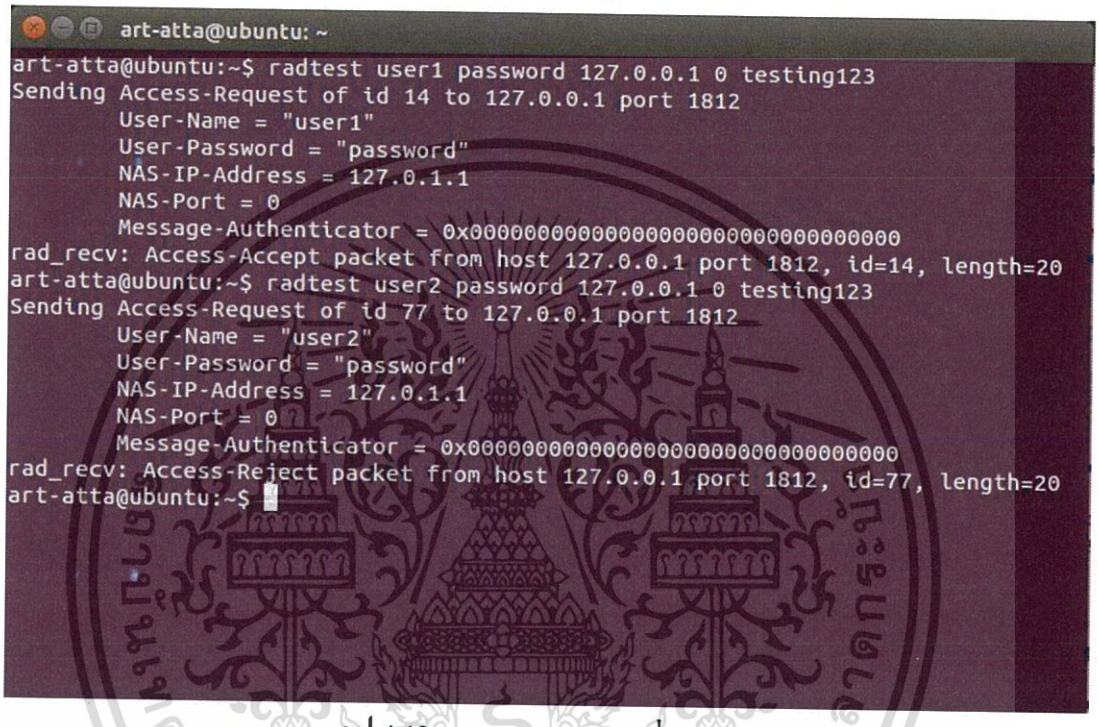
12) หน้าแสดงประวัติเมื่ออุปกรณ์ไม่ตอบสนอง และผลการแก้ไข



รูป 4.12 หน้าแสดงประวัติเมื่ออุปกรณ์ไม่ตอบสนอง และผลการแก้ไข

4.2 การทดลองใช้งาน Free Radius

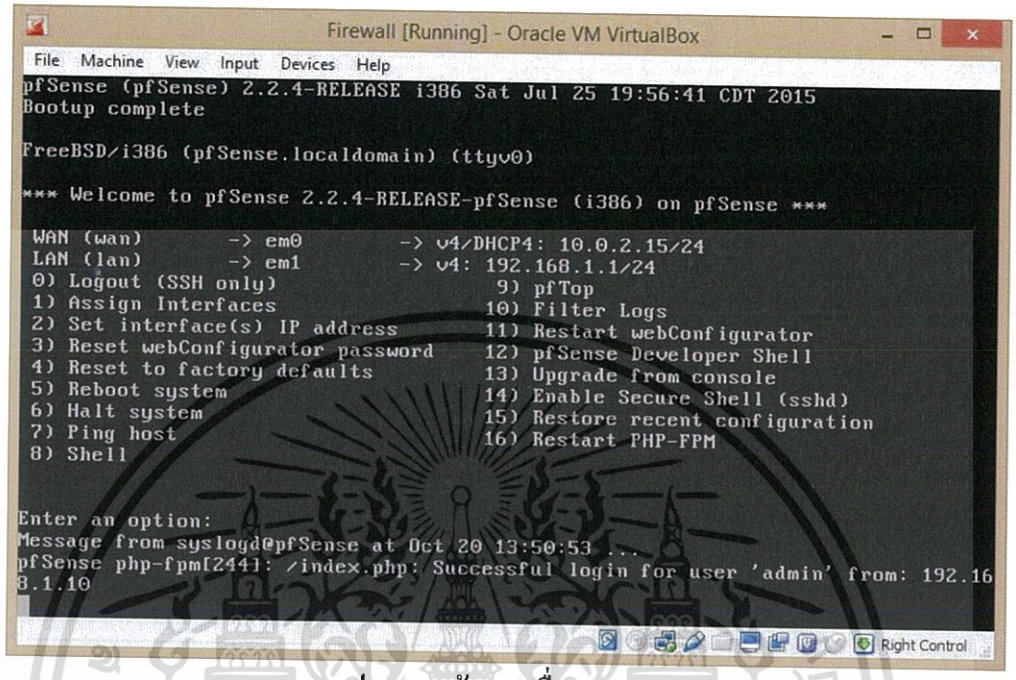
1) ได้ทำการติดตั้ง Free Radius ลงบน Ubuntu Server
2) แล้วจึงทดลองทำการ Authentication ผ่าน Free Radius ผ่านคำสั่ง radtest ได้ดังภาพ
   A) ทำการ Authentication แบบถูกต้อง Free Radius จะตอบกลับมาว่า “Access-Accept”
   B) ทำการ Authentication ให้ไม่ถูกต้อง Free Radius จะตอบกลับมาว่า “Access-Reject”



รูป 4.13 การทดลอง log in ผ่าน CLI

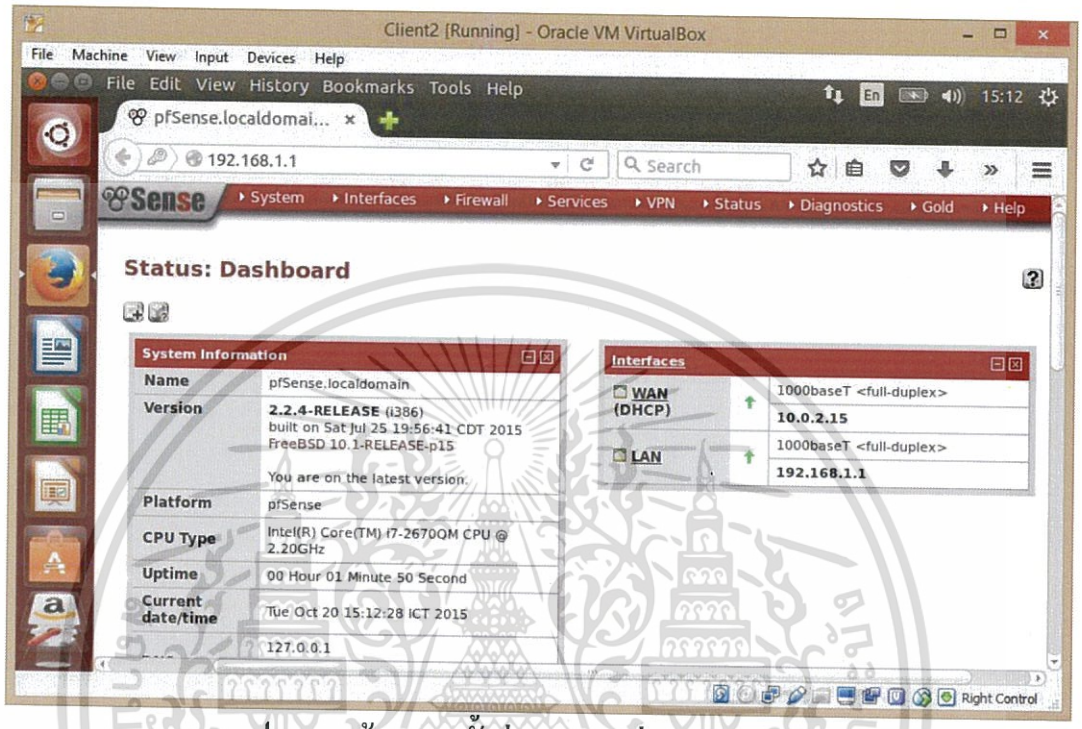
4.3 การทดลองใช้งาน Pfsense

1) ทดลองทำการติดตั้ง Pfsense แล้วเข้าใช้งานดูได้ดังภาพ



รูป 4.14 หน้าจอเครื่อง Pfsense

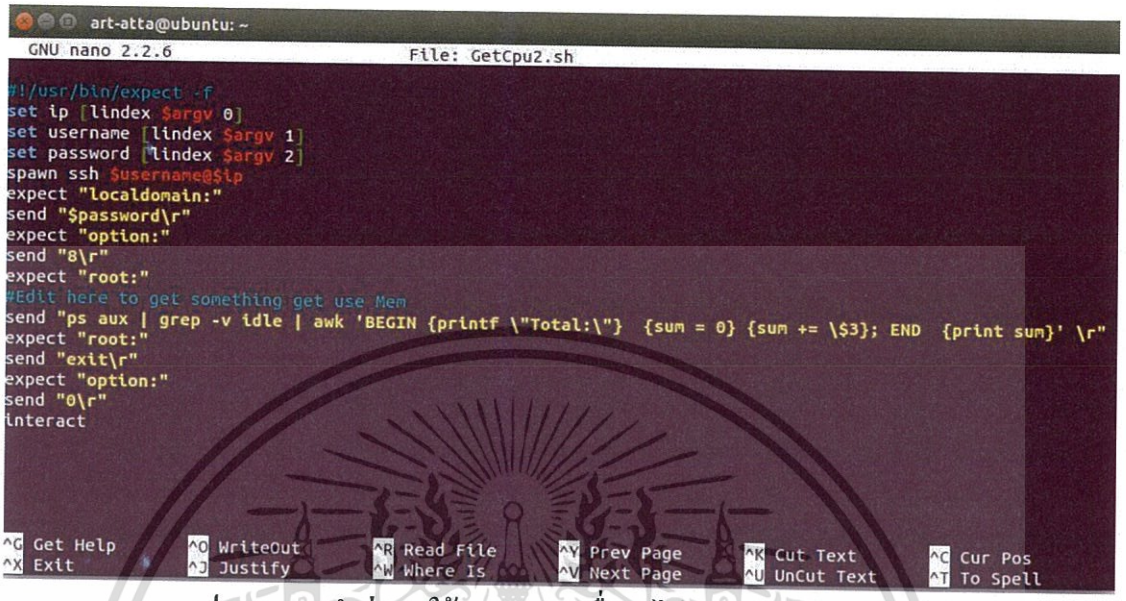
2) ทดลองทำการใช้ DHCP ในการแจก Address ให้คอมพิวเตอร์ที่เชื่อมต่อกับ Pfsense และทดลองนำเครื่องคอมพิวเตอร์ที่ได้รับ Address เข้าไปใช้งาน Pfsense ผ่าน Web Browser ซึ่งเป็นหน้า GUI ของ pfsense ที่ใช้งานง่าย



รูป 4.15 หน้าจอการตั้งค่า Pfsense ผ่าน web browser

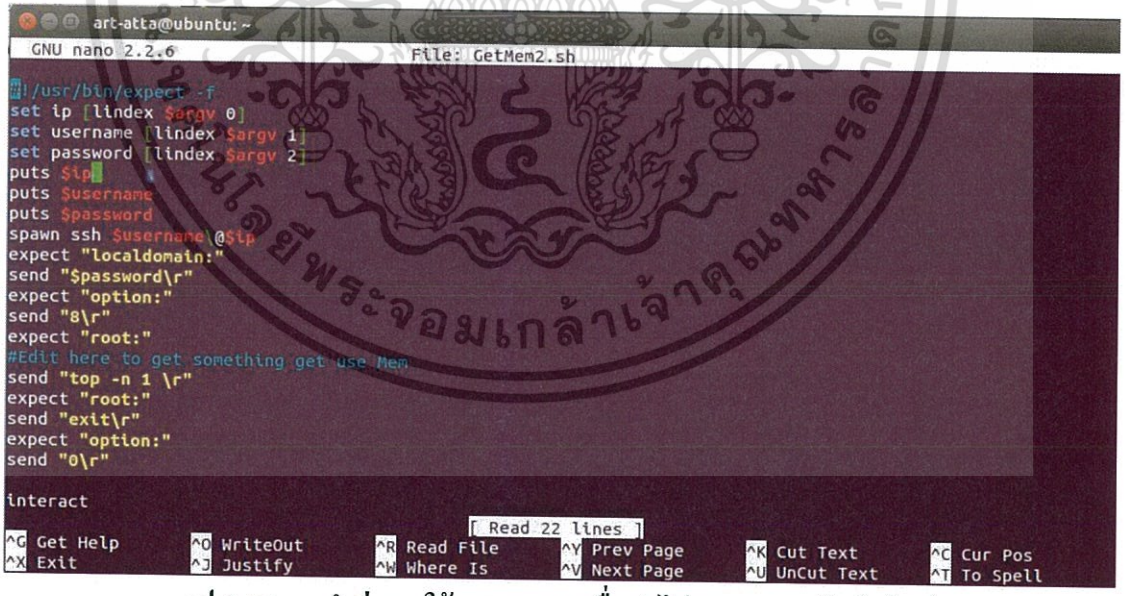
4.4 การใช้ Code Shell script ในการ Monitor ทรัพยากรของ Firewall

1) การนำค่าการใช้งาน CPU ของ Firewall เพื่อนำไปแสดงบนหน้าเว็บไซต์



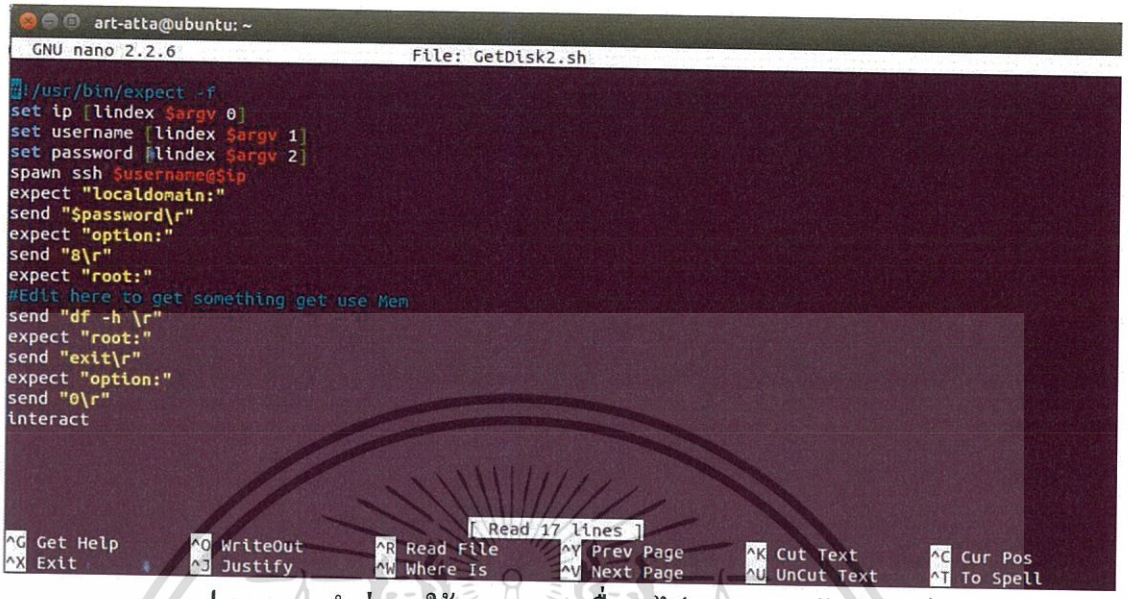
รูป 4.16 การนำค่าการใช้งาน CPU เพื่อนำไปแสดงบนหน้าเว็บไซต์

2) การนำค่าการใช้งาน RAM ของ Firewall เพื่อนำไปแสดงบนหน้าเว็บไซต์



รูป 4.17 การนำค่าการใช้งาน RAM เพื่อนำไปแสดงบนหน้าเว็บไซต์

3) การนำค่าการใช้งาน HDD เพื่อนำไปแสดงบนหน้าเว็บไซต์



รูป 4.18 การนำค่าการใช้งาน HDD เพื่อนำไปแสดงบนหน้าเว็บไซต์

4) การตั้งการทำงานอัตโนมัติโดย crontab

A) บรรทัดที่ 1 เป็นการเรียกใช้ Shell ที่ดึงค่า Ram ออกมาเป็น Output ไฟล์ชื่อ resultMEM(z).txt ซึ่ง (z) คือ ID ของ Firewall บนฐานข้อมูล โดยจะรันทุกๆ 3 นาที

B) บรรทัดที่ 2 เป็นการเรียกใช้ Shell ที่ดึงค่า CPU ออกมาเป็น Output ไฟล์ชื่อ resultCPU(z).txt ซึ่ง (z) คือ ID ของ Firewall บนฐานข้อมูล โดยจะรันทุกๆ 3 นาที

C) บรรทัดที่ 3 เป็นการเรียกใช้ Shell ที่ดึงค่า HDD ออกมาเป็น Output ไฟล์ชื่อ resultDISK(z).txt ซึ่ง (z) คือ ID ของ Firewall บนฐานข้อมูล โดยจะรันทุกๆ 3 นาที

D) บรรทัดที่ 4 เป็นการใช้งาน nodejs เพื่อเรียกใช้ JavaScript ชื่อ AutoReboot2 ซึ่งทำงานโดยการ ping ไปหา Access Point ทุกตัวในฐานข้อมูล เพื่อตรวจสอบสถานะ ถ้า Access Point ตัวใดมีสถานะที่ผิดปกติ ก็จะสั่ง Reboot โดยอัตโนมัติ

```
*/3 * * * * ./GetMem2.sh 192.168.2.1 admin pfsense | grep Mem: > /var/www/html/project/pages/resultMEM1.txt
*/3 * * * * ./GetCpu2.sh 192.168.2.1 admin pfsense | grep Total: | grep -v END > /var/www/html/project/pages/resultCPU1.txt
*/3 * * * * ./GetDisk2.sh 192.168.2.1 admin pfsense | grep /dev/  > /var/www/html/project/pages/resultDISK1.txt
*/15 * * * * node /var/www/html/project/pages/AutoReboot2.js
```

รูป 4.19 การตั้งการทำงานอัตโนมัติโดย crontab

4.5 Database ที่ใช้งาน

1) ตัวอย่างข้อมูลบนฐานข้อมูลที่เก็บข้อมูลของ Admin

Username	Password	Name	Telephone
admin	admin607	Ongard	0859630836
admin2	admin2607	Parkpoom	0815778987
admin3	admin3607	Ratchanon	0875652346

รูป 4.20 Database Admin

2) ตัวอย่างข้อมูลบนฐานข้อมูลที่เก็บข้อมูลของผู้ใช้งาน

username	attribute	op	value	Name	Surname	IDCard	Email	Class
admin4	password	==	admin607	Ongard	Attasophonsak	1100200925315	hello_bye_thank@hotmail.com	Admin
user	password	==	user607	Parkpoom	Lertsawatwicha	1100701772791	gun.dpm@gmail.com	User
1100701772792	password	==	guest607	Prapat	Thanomsak	1100300836354	karn.adidoz@hotmail.com	Guest

รูป 4.21 Database User

3) ตัวอย่างข้อมูลบนฐานข้อมูลที่เก็บข้อมูลของ Access Point

APName	SSID	PasswordAP	Username	IP	Password	SiteName	Description
HCRL	HCRL	project2558	admin	192.168.1.2	project2558	ECC-607/1	Linksys-wrt54gl first use: 06/04/2016
Mycomputer	Test	12345	root	127.0.0.1	12345	Mycomputer	testing ping script

รูป 4.22 Database Access Point

4) ตัวอย่างข้อมูลบนฐานข้อมูลที่เก็บข้อมูลของ Firewall

ID	FWName	IP	Username	Password	Description
1	Pfsense	192.168.2.1	admin	pfsense	firewall 1

รูป 4.23 Database Firewall

5) ตัวอย่างข้อมูลบนฐานข้อมูลที่เก็บข้อมูลการใช้งานของผู้ใช้งาน

host	facility	priority	level	tag	datetime	program	msg	seq
192.168.2.1	local0	info	info	86	2016-02-18 16:28:11	filterlog	90,16777216,,100000101,em1,match,pass,in,4,0x0,,64,14979,0,DF,17,udp,75,192.168.1.10,192.168.1.1,55446,53,55	1999
192.168.2.1	local0	info	info	86	2016-02-18 16:28:11	filterlog		2000
192.168.2.1	local0	info	info	86	2016-02-18 16:28:11	filterlog		2001
192.168.2.1	local0	info	info	86	2016-02-18 16:28:11	filterlog		2002
192.168.2.1	local0	info	info	86	2016-02-18 16:28:11	filterlog		2003
192.168.2.1	local0	info	info	86	2016-02-18 16:28:11	filterlog		2004
192.168.2.1	local0	info	info	86	2016-02-18 16:28:11	filterlog		2005
192.168.2.1	local0	info	info	86	2016-02-18 16:28:11	filterlog		2006
192.168.2.1	local0	info	info	86	2016-02-18 16:28:12	filterlog		2007
192.168.2.1	local0	info	info	86	2016-02-18 16:28:12	filterlog		2008
192.168.2.1	local0	info	info	86	2016-02-18 16:28:12	filterlog	90,16777216,,100000101,em1,match,pass,in,4,0x0,,64...	2009
192.168.2.1	local0	info	info	86	2016-02-18 16:28:12	filterlog	90,16777216,,100000101,em1,match,pass,in,4,0x0,,64...	2010
192.168.2.1	local0	info	info	86	2016-02-18 16:28:12	filterlog	90,16777216,,100000101,em1,match,pass,in,4,0x0,,64...	2011
192.168.2.1	local0	info	info	86	2016-02-18 16:28:12	filterlog	90,16777216,,100000101,em1,match,pass,in,4,0x0,,64...	2012

Null : ☐

90,16777216,,100000101,em1,match,pass,in,4,0x0,,64,14979,0,DF,17,udp,75,192.168.1.10,192.168.1.1,55446,53,55

Press escape to cancel editing

รูป 4.24 Database Log การใช้งาน

4.6 ตัวอย่างการติดตามผู้ใช้งานที่กระทำความผิด

ในกรณีที่ต้องการหาว่า user คนไหนที่มีการใช้งานไปยังปลายทางที่ผิดปกติ จาก log ในตาราง สมมติให้ต้องการที่จะรู้ว่า ใครเป็นผู้ใช้งาน ปลายทาง 203.150.94.17 ในวันที่ 25 เดือนเมษายน เวลาประมาน 2 ทุ่ม

Msg
87,16777216,,100000101,em1,match,pass,in,4,0x0,,63,52340,0,DF,6,tcp,64,192.168.1.49,203.150.94.17,53928,80,0,S,2889766183,,65535,,mss;nop;wscale;nop;nop;TS;sackOK;eol

ก)

Datetime
2016-04-25 20:13:37

ข)

รูป 4.25 log ข้อมูลการใช้งานของผู้ใช้ที่ใช้งานปลายทางที่ผิดปกติ

ก) column msg ใน log

ข) column Datetime ใน log

จากรูป 4.25 ก) ผู้ใช้ที่ใช้งานปลายทาง 203.150.94.17 คือผู้ใช้ที่ได้ IP เป็น 192.168.1.49

Msg
Zone: commonuser - USER LOGIN: user, , 192.168.1.49

ก)

Datetime
2016-04-25 20:13:36

ข)

รูป 4.26 log ข้อมูลการใช้งานของผู้ใช้ที่ได้รับ IP

ก) column msg ใน log

ข) column Datetime ใน log

จากรูป 4.26 ก) และ ข) คือผู้ใช้ที่ได้รับ IP เป็น 192.168.1.49 เมื่อเวลา 20:13 นาฬิกา ซึ่งผู้ใช้คนนี้ ใช้ชื่อ log in ว่า user

Username	Password	Name	Surname	IDCard	E-mail	Class
user	user607	Parkpoom	Lerisawatwicha	1100701772791	gun.dpm@gmail.com	User

รูป 4.27 ข้อมูลของผู้ใช้ชื่อ user

เมื่อได้ข้อมูลชื่อ log in ของผู้ใช้แล้ว ก็นำไปค้นหาใน Database ก็จะพบว่า ผู้ใช้ชื่อ Parkpoom มีการใช้งานไปยังปลายทาง 203.150.94.17 เมื่อเวลา 20:13 นาที

4.7 อุปกรณ์ทำการทดลอง

ในการทดลองครั้งนี้ ใช้

1) คอมพิวเตอร์ โน้ตบุค 1 เครื่อง ลง virtual box 2 ตัว
2) Access Point 1 ตัว
3) อุปกรณ์ทดลองเชื่อมต่อเข้าระบบ (โทรศัพท์มือถือ, โน้ตบุค)

จากการทดลองครั้งนี้มีการใช้งาน Access point แค่ 1 ตัว ยี่ห้อ Lingsys wrt54gl มาตรฐาน 802.11g มี port LAN 4 port และ port WAN 1 port รองรับ DHCP และในกรณีที่มีหลายตัว ให้ทำการเพิ่ม Access point ลงใน หน้าเว็บ Manage Access Point ต่อไป

บทที่ 5
สรุป

5.1 สรุป

ระบบบริหารจัดการผู้ใช้งานเครือข่ายตาม พรบ.ว่าด้วยการกระทำผิดทางคอมพิวเตอร์ เป็นระบบที่มีฟังก์ชั่นหลักๆอยู่สองส่วนคือ

ทำหน้าที่เก็บ log การใช้งานให้เป็นไปตาม พรบ.คอมพิวเตอร์ โดย log สร้างจาก Firewall และส่งไปให้ Syslog-ng จัดการเก็บ แล้วส่งต่อให้กับ Database อีกทีหนึ่ง เพื่อให้ผู้ดูแลระบบสามารถเรียกดูได้จากหน้าเว็บไซต์ หรือนำออกมาดูเองได้

ส่วนการตรวจสอบสถานะของ Access point ใช้วิธีการ ping เข้าไปที่ตัวอุปกรณ์แต่ละตัว นอกจากนี้ ยังมีการทำ crontab ไว้ใน Server ซึ่งจะสั่ง run คำสั่งในการดึงเอาข้อมูล CPU, RAM, HDD ออกมาจาก Firewall ทุกๆ 3 นาที และยังมีคำสั่งที่ใช้งานการ ping ไปหา Access point เพื่อตรวจสอบสถานะ อย่างต่อเนื่องทุกๆ 15 นาที หากสถานะของ Access point ไม่มีการตอบสนอง ก็จะไปสั่งงาน script ที่ไปทำการ Reboot Access point ต่อไป

โดยการทำงานของระบบนั้น อยู่ในรูปแบบของการทำเป็น Web application ซึ่งผู้ดูแลระบบสามารถตรวจสอบ และสั่งงาน Reboot Access point ได้บนหน้าเว็บไซต์เองเลย หลังจากนั้น ระบบจะเรียกใช้งาน script ในการ Reboot ต่อไป โดยได้รับรหัส และ ip จาก Database ของ Access point ที่เก็บไว้

5.2 ปัญหาและอุปสรรค

โครงงานชิ้นนี้ เป็นโครงงานที่พัฒนาขึ้นโดยใช้ซอร์ฟแวร์หลายตัวนำมาประกอบเข้าด้วยกัน ทำให้ จำเป็นต้องศึกษาซอร์ฟแวร์แต่ละตัวก่อนในเบื้องต้น เพื่อทำให้สามารถใช้งานซอร์ฟแวร์นั้นๆได้ ซึ่งทำให้ต้องเสียเวลา ไปกับการศึกษาและทดลองพอสมควร ในการจะทำให้ซอร์ฟแวร์นั้นๆทำงานตามที่ต้องการ

นอกจากนี้ยังต้องแก้ไขปัญหาที่เกิดจากการทำงานร่วมกันของซอร์ฟแวร์แต่ละตัวด้วย เพราะซอร์ฟแวร์แต่ละตัว มีการออกแบบและทำงานที่ต่างกัน การจะให้นำมาใช้งานร่วมกันได้ ต้องอาศัยการตั้งค่าให้เป็นมาตรฐาน และระบบเดียวกัน ซึ่งต้องใช้เวลาทดลองไปในทีละจุด

การทำงานกับ virtual box ต้องใช้เครื่องโฮสเป็นพื้นฐาน ซึ่งบางครั้งที่มีการทำงานหนัก ทรัพยากรของเครื่องโฮสมีไม่พอ ทำให้ประสบปัญหา เครื่องค้าง หรือเครื่องหยุดทำงาน หรืออาจต้องรอเป็นระยะเวลาหนึ่ง

ในโครงงานนี้ มีการใช้งานระบบปฏิบัติการ linux กับ unix ทั้งสองชนิด และต้องทำงานด้วยกัน ซึ่งบางคำสั่ง เมื่อใช้ด้วยกัน ให้ผลที่ต่างกัน ทำให้ต้องใช้เวลาในการทดลอง แก้ไขปัญหาที่เกิดขึ้นมา

5.3 เหตุผลที่เลือกใช้วิธีการนี้

1) เลือกใช้ Pfsense เป็น Firewall เพราะ Pfsense เป็น Firewall ที่เป็นฟรีแวร์ ใช้งานง่าย สามารถตั้งค่าได้ผ่านหน้าเว็บไซต์ได้ และมีความยืดหยุ่นสูง สามารถติดตั้ง Tool เพิ่มเติมได้ง่าย ทำให้รองรับการพัฒนาเพิ่มเติมและการเปลี่ยนแปลงได้ดี
2) เลือกใช้ Free Radius เป็น Radius Server เพราะ Free Radius เป็นฟรีแวร์ และมีความปลอดภัยสูงกว่า การใช้วิธีการตรวจสอบสิทธิ์(Authentication) บนฐานข้อมูล
3) เลือกใช้ Syslog-ng เป็นตัวช่วยในการจัดการ Log การใช้งานเพราะเป็นฟรีแวร์ ที่ใช้งานง่าย และมีความยืดหยุ่นในการตั้งค่าต่างๆ
4) เลือกใช้วิธีการเช็คสถานะโดยการ Ping เพราะ
5) Reboot Access Point ด้วยวิธีการใช้ Secure shell

5.4 แนวทางการพัฒนาต่อ

สำหรับการพัฒนาต่อนั้น สามารถที่จะใช้ Access Point ที่มี controller อยู่ภายในเข้ามาใช้แทนได้ และใช้วิธีการเขียนโปรแกรมลงบน controller แทนวิธีการ ping เพื่อเช็คสถานะของ Access Point โดยให้ Access Point ส่งค่าสถานะกลับมาแทน เมื่อมีปัญหา หรืออาจให้ส่งกลับมาทุกๆ ช่วงเวลาหนึ่ง เพื่อเป็นการยืนยันว่า ในเวลานั้น Access Point ยังคงมีการตอบสนองอยู่

พัฒนาเพิ่มความสามารถในการทำงาน ด้วยการแยก Server ที่ทำการ ping ไปวางไว้ในจุดเดียวกับที่มีการวาง Firewall ไว้ เป็นการแบ่งเบาเว็บเซิร์ฟเวอร์ที่ส่วนกลาง และลด traffic ที่เกิดขึ้นในเครือข่าย และให้เว็บเซิร์ฟเวอร์เป็นเพียงผู้ที่ดึงข้อมูล จากแต่ละจุดย่อยๆ ออกมาแสดงเท่านั้น

เพิ่มความสามารถของการดู log ด้วยการจัดการตาราง เพื่อให้ admin สามารถมองเห็นได้ว่า ผู้ใช้คนไหน ที่เป็นคนใช้งานเว็บไซต์อะไรโดยตรง โดยไม่ต้องเทียบกับ ip address เอง และเพิ่มการตรวจจับผู้ใช้ที่มีแนวโน้มจะกระทำความผิด เช่น มี user id คนหนึ่ง เข้าใช้เครือข่ายจากจุดหนึ่ง หลังจากนั้น 5 นาที ได้ย้ายไปเข้าอีกจุดหนึ่ง ซึ่งมีระยะห่างกันจนไม่น่าจะเป็นไปได้ ก็ให้ขึ้นเตือน หรือ ไฮไลต์ไว้ หรือ เมื่อมีผู้ใช้ ที่เข้าใช้งานแบบต่างๆ ซึ่งผิดปกติ เป็นต้น

เพิ่มความสามารถของหน้าเว็บไซต์ระบบ ด้วยการใช้ SSH ดึงข้อมูลผู้ใช้ ที่กำลังออนไลน์อยู่ในระบบ จาก Firewall Pfsense ความสามารถ ในการตัดผู้ใช้บางคนออกจากระบบ และเปิดให้ผู้ใช้งานทั่วไปสามารถแก้ไขข้อมูลส่วนตัวของตัวเองได้ เช่นการเปลี่ยนรหัสผ่านของตัวเอง

เพิ่มความปลอดภัยของการลงทะเบียนแบบ guest การตรวจสอบความถูกต้องของข้อมูลผู้ใช้งาน ทำให้การติดตามตัวผู้กระทำผิด ในกรณีที่มีการกระทำผิดนั้น สามารถทำได้ง่ายยิ่งขึ้น

การขยายขนาดของเครื่องข่ายนั้น ในกรณีที่เครือข่ายมีขนาดใหญ่มากขึ้น ควรเพิ่ม web server เข้าไปเชื่อมต่อ ในแต่ละจุดที่มี Firewall อยู่ เพื่อให้ใช้ web server นั้นช่วยในการตรวจสอบสถานะ Access point ในเครือข่ายย่อยของตัวเอง แต่ยังคงใช้ Database อยู่ที่จุดเดียว เพื่อความถูกต้องของข้อมูลที่มีการเก็บบน Database

บรรณานุกรม

นายกฤษฎพิฏิ์ธนพิก ศรีธนสาร.**“เอกสารประกอบการฝึกอบรมระบบความปลอดภัยบนเครือข่ายคอมพิวเตอร์ด้วยเครื่องจักรเสมือน”** : สำนักบริการคอมพิวเตอร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ภาควิชาวิศวกรรมคอมพิวเตอร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง. **“ระบบพิสูจน์ตัวตน”** : ภาควิชาวิศวกรรมคอมพิวเตอร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ภาควิชาวิศวกรรมคอมพิวเตอร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง. **“ระบบจัดเก็บบันทึกกิจกรรมส่วนกลาง”** : ภาควิชาวิศวกรรมคอมพิวเตอร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ไอ.ที.แอดแวนเทจ. ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร.[Online]. Available : http://www.itac.co.th/index.php?option=com_content&view=article&id=92

Nattapong Thitichawalitkul.ติดตั้ง pfSense กัน.[Online]. Available : http://thaiopensource.org/%E0%B8%95%E0%B8%B4%E0%B8%94%E0%B8%95%E0%B8%B1%E0%B9%89%E0%B8%87-pfsense/

วิกิพีเดีย สารานุกรมเสรี.อะแพชี เว็บเซิร์ฟเวอร์.[Online]. Available : https://th.wikipedia.org/wiki/อะแพชี_เว็บเซิร์ฟเวอร์