ระบบพิสูจน์ตัวตนผ่านเครือข่ายเสมือนโดยใช้ Token

AUTHENTICATION SYSTEM THROUGH A VIRTUAL PRIVATE NETWORK USING TOKEN

โดย

วิวรรธน์ โกพลรัตน์

WIWAT KOPHONRAT

อาจารย์ที่ปรึกษา

ดร.ปานวิทย์ ธุวะนุติ

รายงานนี้เป็นส่วนหนึ่งของวิชาการศึกษาอิสระ 2

หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ

คณะเทคโนโลยีสารสนเทศ

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ภาคเรียนที่ 1 ปีการศึกษา 2556

AUTHENTICATION SYSTEM THROUGH A VIRTUAL PRIVATE NETWORK USING TOKEN

WIWAT KOPHONRAT

A REPORT SUBMITTED IN PARTIAL FULFILLMENT OF THE

REQUIREMENT OF THE COURSE

INDEPENDENT STUDY 2

MASTER OF SCIENCE PROGRAM IN INFORMATION TECHNOLOGY

FACULTY OF INFORMATION TECHNOGY

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

1/2013

ใบรับรองการศึกษาอิสระ 2 (INDEPENDENT STUDY 2)

เรื่อง

ระบบพิสูจน์ตัวตนผ่านเครือข่ายเสมือนโดยใช้ Token

AUTHENTICATION SYSTEM THROUGH A VIRTUAL PRIVATE NETWORK USING TOKEN

นายวิวรรธน์ โกพลรัตน์

รหัสประจำตัว 53660536

ขอรับรองว่ารายงานฉบับนี้ ข้าพเจ้าไม่ได้ไปคัดลอกจากที่ใด
รายงานฉบับนี้ได้รับการตรวจสอบแล้วอนุมัติให้เป็นส่วนหนึ่งของ
การศึกษาวิชาการศึกษาอิสระ 2 หลักสูตรวิทยาศาสตรมหาบัณฑิต (เทคโนโลยีสารสนเทศ)
ภาคเรียนที่ 1 ปีการศึกษา 2556

.....อาจารย์ที่ปรึกษา
(ดร.ปานวิทย์ ธุวะนุติ)

.....กรรมการสอบ
(ผศ.ดร.กันต์พงษ์ วรรัตน์ปัญญา)

.....กรรมการสอบ
(ดร.กิติ์สุชาต พสุภา)

.....กรรมการสอบ
(ดร.สุภกิจ นุตยะสกุล)

หัวข้อ	ระบบพิสูจน์ตัวตนผ่านเครือข่ายเสมือนโดยใช้ Token
นักศึกษา	นายวิวรรธน์ โกพลรัตน์
รหัสนักศึกษา	53660536
ปริญญา	วิทยาศาสตรมหาบัณฑิต
สาขาวิชา	เทคโนโลยีสารสนเทศ
แขนงวิชา	เทคโนโลยีระบบสารสนเทศ
ปีการศึกษา	2556
อาจารย์ที่ปรึกษา	ดร.ปานวิทย์ ธุวะนุติ

บทคัดย่อ

ในปัจจุบันการใช้งานอินเทอร์เน็ตเป็นไปอย่างกว้างขวางการจะเข้าถึงข้อมูลนั้นได้สะดวกและง่าย แต่สำหรับในบางระบบที่มีการให้บริการแบบเว็บอินทราเน็ตรวมถึงองค์กรที่มีการจำกัดการเข้าถึงข้อมูล ระบบพิสูจน์ตัวตนจึงเป็นระบบที่สำคัญขององค์กร การเข้าถึงข้อมูลสารสนเทศต่างๆโดยเฉพาะข้อมูลสำคัญจำเป็นต้องมีการยืนยันตัวตนของผู้ใช้งาน จึงได้คิดพัฒนาระบบพิสูจน์ตัวตนเพื่อยืนยันตัวตนก่อนการใช้งานระบบและเพิ่มส่วนของการเชื่อมต่อผ่านเครือข่ายเสมือนก่อนการใช้งานด้วย

โครงการนี้เป็นการพัฒนาระบบพิสูจน์ตัวตนผ่านเครือข่ายเสมือน โดยใช้อุปกรณ์อิเล็กทรอนิกส์ที่ใช้เก็บคู่คีย์ เป็นลักษณะการพิสูจน์ตัวตนแบบ 2 ตัวประกอบ ในการเข้าใช้งานระบบผ่านเครือข่ายอินเทอร์เน็ต สำหรับองค์กรที่ต้องการความปลอดภัยในการเข้าใช้งานระบบผ่านเครือข่ายสาธารณะ โดยได้นำชื่อผู้ใช้ รหัสผ่านมาเป็นตัวประกอบที่ 1 และอุปกรณ์อิเล็กทรอนิกส์ที่ใช้เก็บคู่คีย์เป็นตัวประกอบที่ 2 ในการการยืนยันตัวตนเชื่อมต่อผ่านทางเครือข่ายเสมือนก่อนการเข้าใช้งานสารสนเทศภายในระบบเว็บอินทราเน็ต

ระบบถูกพัฒนาขึ้นในรูปแบบของแอนดรอยด์แอพพลิเคชันทำหน้าที่เป็นซอฟต์แวร์ที่ติดตั้งในอุปกรณ์อิเล็กทรอนิกส์ที่ใช้เก็บคู่คีย์ เว็บเซอร์วิส และนำซอฟต์แวร์โอเพนซอร์สมาช่วยในการสร้างเครือข่ายเสมือนเพื่อช่วยในการทำงานให้ระบบสมบูรณ์และมีประสิทธิภาพยิ่งขึ้น

Title	Authentication System Through a Virtual Private Network Using Token
Student	Mr. Wiwat Kophonrat
Student ID.	53660536
Degree	Master of Science
Program	Information Technology
Major	Information System Technology
Academic Year	2013
Advisor	Dr. Panwit Tuwanut

ABSTRACT

At present, the Internet is widely available and easy to access. However, some systems with intranet service including organization that has limited access to information. Therefore, the authentication system is important for organization. Information accessibility, especially for those important information must require the authentication of users. We have developed authentication system through a virtual private network using token.

This project proposes to develop the authentication system through a virtual network using token that characterize by two factors. First factor is the username and password. Second factor is the token. Both of factors are use for authentication via virtual network before access to intranet website.

The system are performed by developing an android application and installed to the token device and web services. And use software open source to create a virtual network to make more completely and effectively in the system.

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

ตารางที่ หน้า

สารบัญรูปภาพ

รูปที่ หน้า

สารบัญรูปภาพ(ต่อ)

รูปที่ หน้า

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ปัจจุบันเทคโนโลยีเครือข่ายอินเทอร์เน็ต เป็นที่แพร่หลายอย่างกว้างขวาง มีการใช้งานอยู่ทั่วไปซึ่งเป็นเรื่องปกติทั้งตามหน่วยงานรัฐ เอกชน องค์กรต่างๆ รวมถึงตามหอพัก หรือร้านค้าที่มีบริการอินเทอร์เน็ตทั้งนี้เพราะเหตุผลของเทคโนโลยีทางด้านเครือข่ายที่มีความเจริญเติบโตขึ้นอย่างรวดเร็วและมีการจัดตั้งจุดเชื่อมต่อเครือข่ายมากขึ้นราคาในการติดตั้งถูกลงมาก รวมถึงอุปกรณ์ที่หาซื้อได้ง่ายสามารถเรียนรู้วิธีการเพื่อจัดตั้งจุดเชื่อมต่อเครือข่ายทั้งแบบไร้สายหรือโครงข่ายสายสัญญาณได้ไม่ยากเย็น ทำให้เครือข่ายอินเทอร์เน็ตมีการใช้งานในชีวิตปัจจุบันอย่างมากมาย และเนื่องจากว่าการที่บุคคลใดจะเข้าสู่ระบบนั้นบางครั้งอาจอยู่ต่างสถานที่กันเมื่อมีการส่งข้อมูลสำคัญภายในเครือข่ายอินเทอร์เน็ตอาจถูกดักจับโดยผู้ไม่ประสงค์ดีได้โดยง่าย ดังนั้นจึงมีแนวคิดที่จะสร้างเครือข่ายเสมือนเพื่อทำให้การเข้าใช้งานเครือข่ายอินเทอร์เน็ตเป็นไปอย่างปลอดภัยระหว่างผู้ใช้งานที่อยู่ต่างที่กัน จึงได้มีการเชื่อมต่อกันระหว่างเครือข่ายในอินเทอร์เน็ตสาธารณะให้เสมือนอยู่บนเครือข่ายเดียวกันก่อนการใช้งานจริงและเพิ่มประสิทธิภาพของความปลอดภัยในการใช้งานเครือข่ายระบบงานภายใน โดยการพิสูจน์ตัวตน เนื่องจากว่าการที่บุคคลใดจะเข้าสู่ระบบได้จำเป็นต้องได้รับอนุญาตหรือได้รับการยืนยันว่าเป็นบุคคลคนนั้นจริง จึงจะเข้าสู่ข้อมูลหรือระบบส่วนตัวนั้นได้ ดังนั้นความปลอดภัยของข้อมูลจึงขึ้นอยู่กับการยืนยันตัวตนที่แท้จริง และเดิมทีระบบพิสูจน์ตัวตนของผู้ใช้งาน สอบถามชื่อผู้ใช้ (Username) และ รหัสผ่าน (Password) ซึ่งอาจถูกขโมยจากผู้ไม่หวังดี และถูกไปใช้งานในทางไม่ดี แต่สำหรับระบบที่ต้องการความปลอดภัยมากๆ คงจะต้องการความปลอดภัยที่มากไปกว่าการสอบถามแค่ชื่อผู้ใช้และ รหัสผ่าน และเพื่อทำให้การเข้าใช้งานเป็นไปอย่างปลอดภัย จึงได้ใช้การยืนยันตัวตนแบบการพิสูจน์ตัวตนแบบ 2 ตัวประกอบ (Two Factor Authentication)

1.2 วัตถุประสงค์

1.2.1 เพื่อศึกษาและพัฒนาระบบการยืนยันตัวตนแบบ Two Factor Authentication มาใช้แทนการยืนยันตัวตนแบบชื่อผู้ใช้และรหัสผ่าน

1.2.2 เพื่อเพิ่มความปลอดภัยสำหรับระบบในการยืนยันตัวตนก่อนการเข้าใช้งานระบบ เพราะเพียงแค่ชื่อผู้ใช้และรหัสผ่านสามารถถูกขโมยได้จากการใช้งานอินเทอร์เน็ตแต่ถ้าเรานำอุปกรณ์อิเล็กทรอนิกส์ที่ใช้เก็บคู่คีย์ (Token) มาช่วยในการยืนยันตัวตนอีกขั้นตอน ถึงแม้จะถูกขโมยชื่อผู้ใช้ หรือรหัสผ่านไป ก็จะไม่สามารถเข้าใช้งานระบบได้

1.2.3 เพื่อศึกษาการสร้างเครือข่ายเสมือนก่อนการเข้าใช้งานอินเทอร์เน็ตสาธารณะระหว่างการใช้งานที่อยู่ต่างสถานที่กันเพื่อเพิ่มระบบความปลอดภัยในการใช้งาน

1.3 ขอบเขตของงานวิจัย

การศึกษาวิจัยและพัฒนาระบบเรื่องการยืนยันตัวตนแบบ Two Factor Authentication ในการเข้าใช้งานระบบเครือข่ายอินเทอร์เน็ต สำหรับบุคคลผู้ที่ต้องการความปลอดภัยในการเข้าใช้งานเครือข่าย ครอบคลุมตามกรอบแนวคิดและกระบวนพัฒนา โดยได้นำ Token มาเป็นตัวประกอบที่ 1 และนำชื่อผู้ใช้ รหัสผ่านมาเป็นตัวประกอบที่ 2 ในการการยืนยันตัวตน ผ่านทางเครือข่ายเสมือนบุคคลโดยใช้โปรโตคอล HTTPS

1.4 ประโยชน์ที่คาดว่าจะได้รับ

1.4.1 เพิ่มความปลอดภัยในการเข้าใช้งานเครือข่ายอินเทอร์เน็ตผ่านทางเครือข่ายเสมือน

1.4.2 มั่นใจได้ว่าผู้ใช้งานเครือข่ายมีสิทธิ์เข้าใช้งาน

1.4.3 ได้ความรู้เกี่ยวกับการพิสูจน์ตัวตนแบบ Two Factor Authentication

1.4.4 ได้รับความรู้การสร้างและนำ Token มาใช้งาน

1.4.5 ได้รับความรู้เรื่องการสร้างระบบเครือข่ายเสมือน

1.5 นิยามศัพท์เฉพาะ

1.5.1 Authentication คือ การพิสูจน์ตัวตนว่าผู้ใช้ระบบคือใคร ซึ่งจะใช้กับระบบคอมพิวเตอร์ที่ต้องการความปลอดภัย บุคคลที่มีสิทธิเท่านั้นจึงจะสามารถใช้งานได้ วิธีการพิสูจน์ตัวตนที่มีการใช้งานแพร่หลายอยู่ด้วยกัน 3 วิธีคือ

1) สิ่งที่คุณรู้ (Something you know) เช่น รหัสผ่านหรือ PIN เป็นต้น

2) สิ่งที่คุณมี (Something you have) เช่น โทรศัพท์มือถือ หรือ Security Token เป็นต้น

3) สิ่งที่คุณเป็น (Something you are) เช่น ลายนิ้วมือ หรือ การสแกนม่านตา หรือ Biometric อื่นๆ เป็นต้น

1.5.2 Two Factor Authentication คือ การยืนยันตัวตนแบบ 2 ตัวประกอบโดยจะสอบถามถึง สิ่งที่คุณรู้ หรือ สิ่งที่คุณมี หรือ สิ่งที่คุณเป็น โดยเลือกการยืนยันตัวตน 2 ใน 3 ตัวประกอบ

1.5.3 Token คือ อุปกรณ์อิเล็กทรอนิกส์ที่ใช้เก็บคู่คีย์

1.5.4 PIN คือ ชุดตัวเลขหรือตัวอักษรที่กำหนดขึ้นเป็นรหัสลับเฉพาะส่วนบุคคล

1.5.5 VPN หรือ Virtual Private Network หมายถึง เครือข่ายเสมือนส่วนตัว ที่ทำงานโดยใช้โครงสร้างของเครือข่ายสาธารณะ หรืออาจจะวิ่งบนเครือข่ายอินเทอร์เน็ตก็ได้แต่ยังสามารถคงความเป็นเครือข่ายเฉพาะขององค์กรได้

1.5.6 HTTPS ย่อมาจาก Hypertext Transfer Protocol over Secure Socket Layer หรือ HTTP over SSL คือ โพรโตคอลที่มีการเชื่อมต่อแบบ Secure HTTP ซึ่งโพรโตคอล HTTPS สร้างเพื่อความปลอดภัยในการสื่อสารผ่านอินเตอร์เน็ตข้อมูลที่ทำการส่งได้ถูกเข้ารหัสเอาไว้ โดยใช้ Asymmetric Algorithm ซึ่งถ้าถูกดักจับได้ก็ไม่สามารถที่จะอ่านข้อมูลนั้นได้รู้เรื่อง

1.5.7 Router คือ อุปกรณ์ที่ใช้ในการเชื่อมต่อคอมพิวเตอร์ระหว่างเครือข่าย

1.5.8 Black Box คือ แผงวงจรหรืออุปกรณ์ที่ทำให้คอมพิวเตอร์ทำงานอย่างใดอย่างหนึ่งโดยเฉพาะ

บทที่ 2
ทฤษฎีและเทคโนโลยีที่เกี่ยวข้องกับการพัฒนาระบบ

2.1 การพิสูจน์ตัวตน

การพิสูจน์ตัวตน ผู้ใช้งานระบบจำเป็นต้องระบุตัวตนของตัวเองเพื่อให้ได้รับสิทธิ์และสามารถเข้าถึงระบบได้ เป็นกระบวนการตรวจสอบความถูกต้องของหลักฐานข้อมูล เพื่อแสดงว่าข้อมูลของบุคคลนั้นมีความถูกต้องและเป็นบุคคลนั้นจริงหรือไม่ โดยในทางปฏิบัติแล้วขั้นตอนการพิสูจน์ตัวตนนั้นแบ่งเป็น 2 ขั้นตอน

1) การระบุตัวตน คือ ขั้นตอนที่ผู้ใช้งานระบบแสดงหลักฐานเพื่อตรวจสอบคุณลักษณะของบุคคลนั้นซึ่งเป็นการพิสูจน์ว่าตนเองคือใครเช่น ชื่อผู้ใช้

2) การพิสูจน์ตัวตน คือ ขั้นตอนการพิสูจน์ว่าผู้ใช้งานที่เข้าใช้งานระบบคือผู้ใช้งานคนนั้นๆ ในระบบจริงหรือไม่ เป็นขั้นตอนในการตรวจสอบหลักฐานเพื่อแสดงว่าเป็นบุคคลนั้นจริง เช่น รหัสผ่าน หรือ PIN เป็นต้น

2.1.1 กลไกของการพิสูจน์ตัวตน เป็นกลไกของการตรวจสอบเพื่อสามารถบ่งชี้ได้ว่าเป็นบุคคลที่ถูกกล่าวอ้างนั้นจริงหรือไม่โดยแบ่งออกได้เป็น 3 คุณลักษณะได้แก่

1) Possession Factor คือ สิ่งที่คุณมี เช่น กุญแจ (Key) เครดิตการ์ด บัตรกดเงินอัตโนมัติ อุปกรณ์ที่ใช้ในการตรวจสอบหรือพิสูจน์ตัวตนของผู้ใช้งานในการเข้าใช้ระบบ หรือ หนังสือเดินทาง เป็นต้น

2) Knowledge Factor คือ สิ่งที่คุณรู้ เช่น รหัสผ่าน PIN หรือรหัสสำหรับล็อคอุปกรณ์ เป็นต้น

3) Biometric Factor คือ สิ่งที่คุณเป็น เช่น ลายนิ้วมือ ตรวจสอบเสียง ตรวจสอบม่านตา ตรวจสอบเยื่อชั้นในลูกตา หรือ สารพันธุกรรม เป็นต้น

ในกระบวนการพิสูจน์ตัวตนนั้นจะนำ 3 ลักษณะคือ สิ่งที่คุณรู้ สิ่งที่คุณมี สิ่งที่คุณเป็น มาใช้ในการยืนยันหลักฐานตามที่ผู้ออกแบบระบบได้จัดสร้างขึ้น แต่วิธีการพิสูจน์ตัวตนที่นำมาใช้เพียงลักษณะเดียว นั้นจะมีข้อจำกัดในการใช้ เช่น ถ้าใช้เพียงสิ่งที่คุณมีในบางครั้งอาจจะสูญหายหรือถูกขโมยได้ หรือถ้าใช้เฉพาะสิ่งที่คุณรู้อาจจะถูกดักฟัง ดักจับข้อมูล หรือขโมยจากเครื่องคอมพิวเตอร์ได้ หรือถ้าใช้เฉพาะสิ่งที่คุณเป็นอาจจะเป็นวิธีที่มีความปลอดภัยสูงแต่ก็ต้องใช้เงินลงทุนสูงตามไปด้วยเนื่องจากเป็นเทคโนโลยีที่ราคาแพงดังนั้นจึงได้มีการนำแต่ละคุณลักษณะมากกว่าหนึ่งคุณลักษณะมาใช้ร่วมกัน เช่น ใช้สิ่งที่คุณมีกับสิ่งที่คุณรู้มาใช้ร่วมกัน ตัวอย่างเช่น การใช้ลายมือชื่อร่วมกับการใช้บัตรเครดิตหรือการใช้รหัสผ่านร่วมกับการใช้บัตรกดเงินอัตโนมัติหรือการใช้รหัสผ่านร่วมกับอุปกรณ์ที่ใช้ในการตรวจสอบหรือพิสูจน์ตัวตนของผู้ใช้งานในการเข้าใช้ระบบ

เป็นต้น ซึ่งการนำคุณลักษณะของการพิสูจน์ตัวตนมาใช้ร่วมกันมากกว่าหนึ่งคุณลักษณะจะช่วยเพิ่มประสิทธิภาพในการรักษาความปลอดภัยของข้อมูลเพิ่มมากยิ่งขึ้น

2.1.2 ประเภทของการพิสูจน์ตัวตน โดยมีส่วนประกอบพื้นฐาน 3 ส่วน ได้แก่

1) การพิสูจน์ตัวตน คือการตรวจสอบหลักฐานเพื่อแสดงว่าเป็นบุคคลนั้นจริง

2) การกำหนดสิทธิ์ คือการกำหนดข้อจำกัดของบุคคลที่เข้ามาใช้งานระบบว่าบุคคลนั้นมีสิทธิ์สามารถทำอะไรภายในระบบนั้นได้บ้าง

3) การบันทึกการใช้งาน คือการบันทึกรายละเอียดของการเข้าใช้งานระบบ

การพิสูจน์ตัวตนที่ใช้อยู่ในปัจจุบันมีหลากหลายลักษณะต่างๆ ดังตารางที่ 2.1

ตารางที่ 2.1 เปรียบเทียบระบบการพิสูจน์ตัวตนต่างๆ (สิริพร จิตต์เจริญธรรม. 2547)

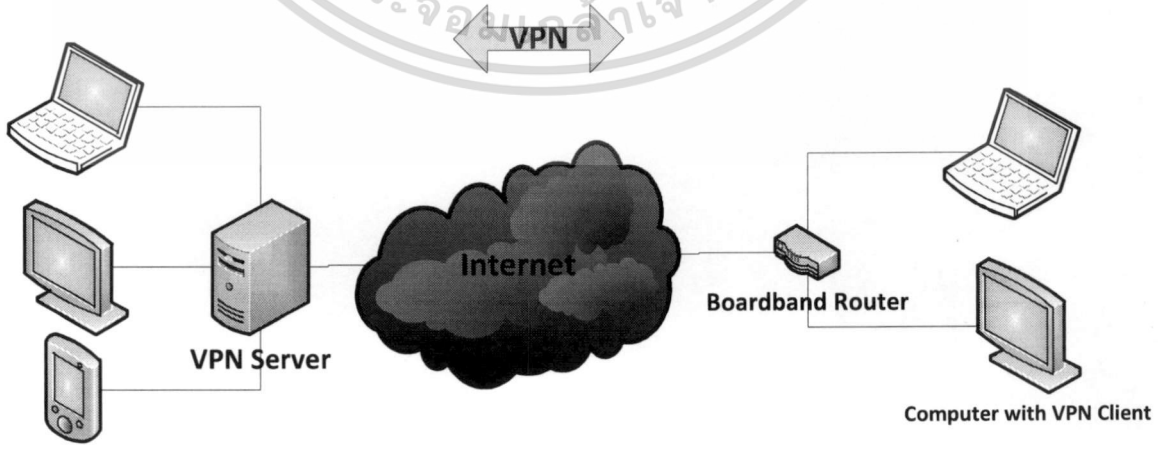
รูปแบบการพิสูจน์ตัวตน	ข้อดี	ข้อเสีย
ไม่มีระบบการพิสูจน์ตัวตน	ค่าใช้จ่ายถูกและง่ายสะดวกต่อการใช้งาน	ความปลอดภัยต่ำ
ระบบการพิสูจน์ตัวตนโดยใช้ชื่อผู้ใช้และรหัสผ่าน	เป็นระบบที่นิยมใช้โดยทั่วไป	มีความปลอดภัยแต่อาจถูกดักข้อมูลหรือขโมยชื่อผู้ใช้และรหัสผ่านได้
ระบบการพิสูจน์ตัวตนโดยใช้ PIN	เป็นระบบที่นิยมใช้โดยทั่วไปเนื่องจากง่ายต่อการใช้และมีความปลอดภัย เช่นการใช้บัตรต่างๆ	แต่ละระบบมีความเป็นเอกลักษณ์ของตัวเองซึ่งใช้ไม่ได้เมื่อต่างระบบกัน ราคาแพงและใช้ฮาร์ดแวร์เฉพาะ
ระบบการพิสูจน์ตัวตนโดยใช้ Token	มีความปลอดภัยสูง ไม่ต้องมีเครื่องอ่านการ์ดแบบ PIN	การใช้งานยุ่งยากกว่าแบบจำรหัสผ่านและอาจถูกขโมยได้ แต่ใช้งานไม่ได้เนื่องจากไม่มีชื่อผู้ใช้และรหัสผ่าน
ระบบการพิสูจน์ตัวตนโดยใช้ลักษณะเฉพาะทางชีวภาพของแต่ละบุคคล	มีความปลอดภัยสูงมากเนื่องจากแต่ละบุคคลไม่เหมือนกัน	มีความซับซ้อนและค่าใช้จ่ายสูง

ตารางที่ 2.1 (ต่อ)

ระบบการพิสูจน์ตัวตนแบบ ใช้รหัสผ่านครั้งเดียว	มีความปลอดภัยสูง ถูกขโมยยาก	ผู้ใช้ต้องจำรหัสผ่านและใช้งานทันทีถ้าจำรหัสไม่ได้หรือสูญหายก็ไม่สามารถใช้งานได้
การพิสูจน์ตัวตนโดยการเข้ารหัสแบบคู่รหัสกุญแจ	มีความปลอดภัยสูง สามารถใช้แบบระบุผู้ใช้งานได้โดยประยุกต์ใช้เป็นระบบลายมือชื่ออิเล็กทรอนิกส์ได้	ต้องสร้างระบบสนับสนุนเฉพาะและอาจใช้เวลาในการเข้าและถอดรหัสนาน
การพิสูจน์ตัวตนโดยวิธีคำถามคำตอบ	มีความปลอดภัยค่อนข้างสูงเนื่องจากคำถามและคำตอบจะรู้เพียงผู้ใช้และตัวระบบของเครื่องผู้ให้บริการเท่านั้น	ความปลอดภัยของระบบขึ้นอยู่กับการออกแบบและสร้างระบบที่ซับซ้อน

2.2 Virtual Private Network (VPN)

หมายถึงการสร้างเครือข่ายเสมือนส่วนตัวที่สามารถทำงานได้ผ่านการใช้โครงสร้างของเครือข่ายสาธารณะ เช่น การใช้งานผ่านเครือข่ายอินเทอร์เน็ตแต่ยังสามารถคงความเป็นเครือข่ายเฉพาะ ขององค์กรได้ด้วยการเข้ารหัสแพ็คเก็จ ก่อนการส่งข้อมูลเพื่อให้ข้อมูลมีความปลอดภัยมากขึ้น VPN เป็นเทคโนโลยีการเชื่อมต่อเครือข่ายภายนอกอาคารซึ่งในปัจจุบันมีการนำไปใช้ในหน่วยงานต่างๆที่มีหลายสาขาหรือมีสำนักงานกระจัดกระจายอยู่ในหลายภูมิภาค ในระบบ VPN เป็นการเชื่อมต่อระหว่างสำนักงานผ่านเครือข่ายอินเทอร์เน็ตแทนการต่อเชื่อมด้วยสายวงจรเช่าหรือเฟรมรีเลย์ โดยตรงซึ่งเป็นการประหยัดค่าใช้จ่ายมากขึ้น



รูปที่ 2.1 แสดงการเชื่อมต่อเครือข่ายเสมือน

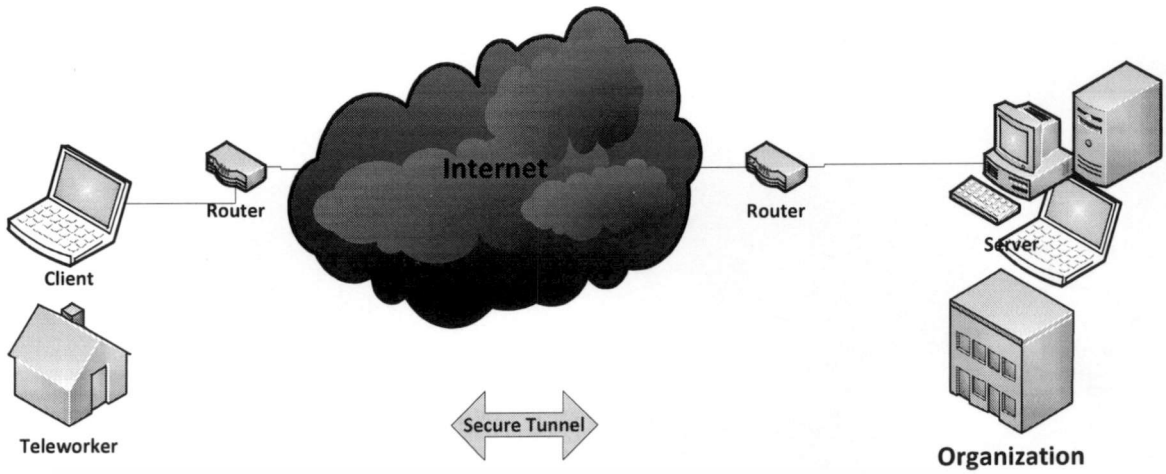
Private Network คือเครือข่ายภายในของแต่ละองค์กรซึ่งเป็นเครือข่ายส่วนตัว ส่วน Public Network คือเครือข่ายสาธารณะที่มีการใช้งานภายนอก เช่น เครือข่ายอินเทอร์เน็ต เมื่อทางองค์กรมีความประสงค์ต้องการเชื่อมเครือข่ายของแต่ละสาขา สำนักงาน ที่อยู่ต่างสถานที่เข้าด้วยกันซึ่งในสมัยก่อนจะทำการเชื่อมต่อเครือข่ายโดยตรงนั้นด้วยสายวงจรเช่าหรือเฟรมรีเลย์ ซึ่งมีค่าใช้จ่ายสูงแต่หลังจากในปัจจุบันการเติบโตของอินเทอร์เน็ตและการพัฒนาเทคโนโลยีที่เกี่ยวข้องมากขึ้น มีการปรับปรุงในเรื่องความเร็วของการเชื่อมต่อทำให้เกิดแนวคิดในการสร้างการเชื่อมต่อเครือข่ายเสมือนผ่านทางเครือข่ายอินเทอร์เน็ตแทนที่สายวงจรเช่า หรือเฟรมรีเลย์ ซึ่งมีราคาแพงด้วยเครือข่ายอินเทอร์เน็ตที่มีราคาถูกกว่า ทำให้เกิดเครือข่ายเสมือนผ่านเครือข่ายอินเทอร์เน็ตขึ้นมา

2.2.1 หลักการทำงาน

เนื่องจากเครือข่ายอินเทอร์เน็ตซึ่งเป็นเครือข่ายที่ใช้ในการสื่อสารอย่างกว้างขวางมีค่าใช้จ่ายต่ำกว่าและมีพื้นที่ครอบคลุมทั่วโลกมากกว่าการใช้สายวงจรเช่า หรือเฟรมรีเลย์ หรือ ATM (Asynchronous Transfer Mode) จึงมีการพัฒนา VPN แทนเครือข่ายส่วนตัวที่มีอยู่หลากหลายสถานที่ผ่านทางเครือข่ายอินเทอร์เน็ต ในขั้นตอนการทำงานของ VPN จะต้องมีการพิสูจน์ตัวตนเพื่อยืนยันความถูกต้องของข้อมูลผู้ใช้งาน การเข้ารหัสข้อมูลเป็นการเข้ารหัสข้อมูลก่อนการส่งเพื่อรักษาความปลอดภัยและป้องกันการถูกดักข้อมูลจากบุคคลนอกองค์กร การสร้างอุโมงค์เพื่อเป็นช่องทางในการส่งข้อมูลระหว่างผู้ใช้งานภายนอกกับองค์กรหรือระหว่างองค์กรกับองค์กรที่มีการเชื่อมเครือข่ายกันจึงเป็นการรักษาความปลอดภัยอย่างหนึ่งเนื่องจากเป็นการเชื่อมต่อเส้นทางบนเครือข่าย และระบบไฟร์วอลล์เป็นระบบรักษาความปลอดภัยมีหน้าที่ในการอนุญาตและไม่อนุญาตสำหรับจัดการผู้ใช้งานที่ต้องการเข้ามาใช้งานในระบบเครือข่าย

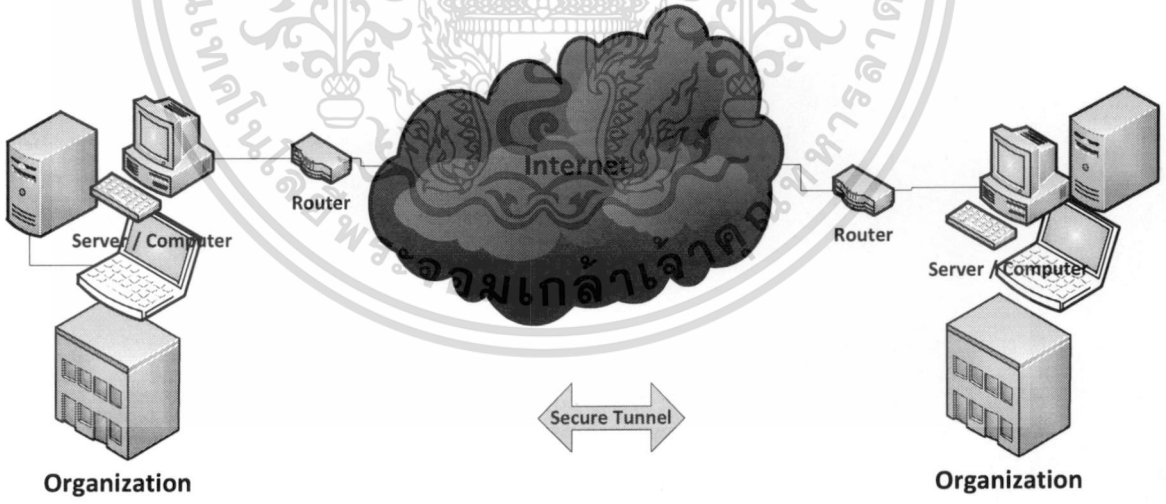
2.2.2 รูปแบบของ VPN

1) การเข้าถึงระยะไกล (Remote access) เป็นการติดต่อภายในเครือข่ายเดียวกันเช่น พนักงานขององค์กรสามารถติดต่อกับอีกเครือข่ายขององค์กรที่อยู่ไกลออกไปได้ ซึ่งองค์กรจะทำการสร้างระบบใหญ่ไว้รอรับการเชื่อมต่อจากเครื่องลูกข่าย และจะทำการติดต่อโดยใช้ซอฟต์แวร์ซึ่งติดตั้งในคอมพิวเตอร์ลูกข่าย (VPN Client) เพื่อทำการเชื่อมต่อเข้าไปในเครือข่ายภายในขององค์กร เหมาะสมสำหรับองค์กรขนาดใหญ่ที่มีพนักงานหลายร้อยคน เพราะมีการรักษาความปลอดภัยที่ดีในการทำงานนั้นที่สำนักงานจะต้องมีการเชื่อมต่ออินเทอร์เน็ตตลอดเวลาและลงซอฟต์แวร์ VPN ไว้สำหรับติดตั้งในคอมพิวเตอร์แม่ข่ายเพื่อรอรับการติดต่อ สำหรับเครื่องลูกข่ายก็จะลงซอฟต์แวร์ไว้สำหรับติดตั้งในคอมพิวเตอร์ลูกข่ายเพื่อสร้างการเชื่อมต่อกับเครื่องแม่ข่ายเพื่อเข้าใช้งาน



รูปที่ 2.2 แสดงเครือข่ายเสมือนแบบ Remote access VPN

2) การเชื่อมต่อระหว่างเครือข่าย (Site to site) เป็นการติดต่อกันระหว่างเครือข่ายหลายเครือข่ายเชื่อมโยงเข้าด้วยกันเช่น องค์กรสำนักงานใหญ่ที่กรุงเทพมหานคร ต้องการติดต่อกับสำนักงานสาขาที่หาดใหญ่ เป็นต้น โดยจะทำการเชื่อมต่อเครือข่ายผ่านทางเครือข่ายสาธารณะ การเชื่อมต่อเครือข่ายแบบระหว่างเครือข่ายแบ่งออกเป็น 2 รูปแบบ คือ อินทราเน็ตเป็นการติดต่อกันระหว่างเครือข่ายภายในเครือข่ายเดียวกันที่ตั้งอยู่ต่างสถานที่อยู่ห่างไกลกันมาก เช่น การติดต่อกันระหว่างสำนักงานที่กรุงเทพมหานครกับสำนักงาน เอกซ์ทราเน็ตเป็นการติดต่อระหว่างเครือข่ายของเรากับเครือข่ายอื่นๆเป็นการเชื่อมต่อระหว่างองค์กรเรากับองค์กร



รูปที่ 2.3 แสดงเครือข่ายเสมือนแบบ Site to site VPN

2.2.3 การสร้างอุโมงค์ (Tunneling)

เป็นเทคนิคที่พัฒนาขึ้นโดยมีลักษณะคล้ายการสร้างอุโมงค์การเชื่อมต่อให้ใช้งานผ่านทางเครือข่ายเพื่อเพิ่มความปลอดภัย เรียกว่า Tunnel เป็นการที่คอมพิวเตอร์ต้นทางติดตั้งซอฟต์แวร์

VPN ซึ่งไว้สำหรับติดตั้งในคอมพิวเตอร์ลูกข่าย จะติดต่อกับคอมพิวเตอร์ปลายทางผ่านคอมพิวเตอร์ที่ทำหน้าที่เป็นเครื่องบริการ VPN ตามหลักการเชื่อมต่อของเครือข่ายอินเทอร์เน็ตนั้นจะไม่มีการกำหนดเส้นทางการเชื่อมต่อตายตัวโดย VPN นั้นจะอาศัยการสร้างอุโมงค์เพื่อใช้ในการสร้างเครือข่ายส่วนตัวสำหรับส่งข้อมูลที่เป็นแพ็คเก็จหนึ่งไปยังอีกแพ็คเก็จหนึ่งผ่านระบบเครือข่ายอินเทอร์เน็ต โดยใช้โพรโตคอลที่เรียกว่า Tunnel Interface รูปแบบของการสร้างอุโมงค์มีอยู่ 2 แบบ คือ Voluntary Tunneling เป็นลักษณะของเครื่องคอมพิวเตอร์ภายนอกที่ติดตั้งซอฟต์แวร์ไว้สำหรับติดตั้งในคอมพิวเตอร์ลูกข่ายทำหน้าที่ในการติดต่อเข้าไปยังผู้ให้บริการอินเทอร์เน็ตหลังจากนั้นจึงสร้างอุโมงค์เชื่อมต่อไปยังเครื่องบริการ VPN และCompulsory Tunneling เป็นหน้าที่ของผู้ให้บริการอินเทอร์เน็ตที่ต้องสร้างการเชื่อมต่อ ผู้ใช้เพียงแต่เชื่อมต่อเข้ามาเท่านั้น หลังจากตรวจสอบสิทธิจึงจะทำการเชื่อมต่อเครื่องของผู้ใช้เข้ากับเครือข่าย VPN ของผู้ใช้

การสร้างอุโมงค์ใน VPN ต้องอาศัยโพรโตคอล 3 แบบ คือ

1) Carrier Protocol เป็นโพรโตคอลสำหรับนำข้อมูลส่งไปยังระบบเครือข่าย

2) Encapsulating Protocol เป็นโพรโตคอลสำหรับการจัดการจัดกลุ่มของข้อมูลก่อนและหลังส่งจากต้นทางไปยังปลายทางในระบบเครือข่าย เช่น

- IPSec เป็นโพรโตคอลสำหรับการสื่อสารผ่านทางเครือข่ายอินเทอร์เน็ตที่เพิ่มความปลอดภัยซึ่งได้รับการพัฒนาและสนับสนุนโดย IETF (Internet Engineering Task Force)

- Open VPN พัฒนาจาก SSL หรือ HTTPS ซึ่ง มีความปลอดภัยสูงมาก มีการแก้ไขปรับปรุงจาก VPN แบบ PPTP หรือ IPSec เช่นการกำหนดพอร์ตการเชื่อมต่อและสามารถเปลี่ยนแปลงได้โดยง่าย หรือ สามารถใช้งานหลายๆพอร์ตได้พร้อมๆ กัน ทำให้ Open VPN มีทั้งความปลอดภัย ความสะดวกในการติดตั้ง ปรับปรุง

- SSL VPN เป็นการสร้าง VPN ในระดับเลเยอร์แอพพลิเคชัน (Application Layer) ผ่านพอร์ต 443 ซึ่งสามารถเชื่อมต่อได้ผ่านเว็บเบราว์เซอร์รองรับการใช้งานโพรโตคอล HTTPS เมื่อเทียบกับ IPSec VPN แล้ว SSL VPN จะเพิ่มความสะดวกสบายให้กับผู้ใช้งาน เนื่องจากผู้ใช้งานใช้งานผ่านเว็บเบราว์เซอร์ทำให้ลดปัญหาจากการติดตั้ง

3) Passenger Protocol เป็นโพรโตคอลสำหรับรับข้อมูลเมื่อข้อมูลถูกส่งไปถึงยังผู้รับ

ตารางที่ 2.2 เปรียบเทียบการทำงานของระบบ VPN ต่างๆ (กรมตรวจบัญชีสหกรณ์. 2556)

รูปแบบ VPN	ข้อดี	ข้อเสีย
ฮาร์ดแวร์ VPN	ประสิทธิภาพสูง ใช้งานง่าย	ความยืดหยุ่นต่ำ ราคาสูง
ซอฟต์แวร์ VPN	ติดตั้งเพิ่มเติมได้ง่ายและสามารถทำงานร่วมกับระบบปฏิบัติการที่หลากหลาย	ประสิทธิภาพในการเข้ารหัสและสร้างอุโมงค์ต่ำ
ไฟร์วอลล์ VPN	ติดตั้งเพิ่มเติมได้ง่ายและสามารถทำงานร่วมกับระบบปฏิบัติการที่หลากหลาย	ประสิทธิภาพในการเข้ารหัสและสร้างอุโมงค์ต่ำ

ตารางที่ 2.2 (ต่อ)

Router VPN	เพิ่มเติมความสามารถและเทคโนโลยี VPN เข้าในตัวอุปกรณ์ได้เลย	ข้อจำกัดในตัวอุปกรณ์ Router แต่ละชนิด
Black Box VPN	ทำงานได้รวดเร็ว	จำเป็นต้องมีคอมพิวเตอร์สำหรับบริหารจัดการเพิ่ม

2.3 Pfsense

เป็นระบบปฏิบัติการที่สามารถใช้งานได้ฟรีแบบโอเพนซอร์สมีการรวมเอาคุณสมบัติของไฟร์วอลล์ที่หลากหลายไว้ด้วยกันโดยเราได้มีการนำฟังก์ชันการทำงานของระบบที่เกี่ยวข้องกับโครงงานมาใช้ ได้แก่

Open VPN ซึ่งเป็นฟังก์ชันที่ใช้ในการสร้างเครือข่ายเสมือนมีความยืดหยุ่นในการติดตั้งและมีการใช้งานแบบ SSL VPN สามารถรองรับการสนับสนุนบนระบบปฏิบัติการของเครื่องลูกข่ายที่หลากหลาย

Captive Portal เป็นการสร้างการพิสูจน์ตัวตนก่อนใช้งานอินเทอร์เน็ตซึ่งเหมาะสมและสามารถนำไปใช้ได้กับเครือข่ายขององค์กรเพื่อระดับความปลอดภัยบนเครือ มีการติดตั้งฟังก์ชัน Free Radius เพื่อใช้จัดการฐานข้อมูลผู้ใช้งาน และSquid เพื่อใช้เป็นเครื่องบริการแทนด้วย

2.4 แอนดรอยด์

เป็นระบบปฏิบัติการที่มีพื้นฐานอยู่บนระบบปฏิบัติการลินุกซ์ ออกแบบมาให้เหมาะสมกับการใช้งานบนโทรศัพท์เคลื่อนที่ มีการใช้งานกับอุปกรณ์ระบบสัมผัสซึ่งการสัมผัสที่สอดคล้องกับการกระทำจริงมีการออกแบบมาอย่างดีตอบสนองต่างๆ กับผู้ใช้ ได้หลากหลายการใช้งานแอนดรอยด์นั้นมีแอพพลิเคชันที่สามารถใช้งานมากขึ้นเรื่อยๆ เป็นที่นิยมใช้ทั่วโลกสามารถติดตั้งผ่านไฟล์ APK แอพพลิเคชันจะเขียนโดยใช้ภาษาจาวา และใช้แอนดรอยด์ซอฟต์แวร์ดีเวล็อปเมนต์คิตในการพัฒนาแอพพลิเคชัน ในอุปกรณ์แอนดรอยด์นั้นจะมีการใช้งานแบตเตอรีที่ใช้พลังงานน้อยสามารถใช้ได้นานและมีระบบช่วยจัดการเมื่อพลังงานใกล้จะหมด

2.5 อาร์เอสเอ (RSA) Token

เป็นระบบการพิสูจน์ตัวตน 2 ปัจจัยหรือ 2 ตัวประกอบโดยจะขึ้นอยู่กับสิ่งที่คุณมีและสิ่งที่คุณรู้เป็นการเพิ่มระดับมากน่าเชื่อถือของการตรวจสอบผู้ใช้งานระบบที่มากกว่าแค่รหัสผ่านที่ง่ายต่อการคาดเดา

เป็นการรักษาความปลอดภัยโดยมุ่งเน้นข้อมูลโดยระบบรักษาความปลอดภัยของอาร์เอสเอร่วมมือกับบริษัทอีเอ็มซีในการพัฒนาความสามารถในเรื่องการพิสูจน์ตัวตนเพื่อคุ้มครองโครงสร้าง

พื้นฐานระบบสารสนเทศของลูกค้ามีการออกแบบและปรับใช้การเข้ารหัสสตอเรจโดยมีโซลูชั่นการเข้ารหัสข้อมูลแบบครบวงจรเพื่อคุ้มครองข้อมูลในสภาพแวดล้อมเครือข่ายอินเทอร์เน็ตอย่างเหมาะสมด้วยอุปกรณ์การเข้ารหัสชั้นนำ นอกจากนี้ อาร์เอสเอ ยังได้ร่วมมือกับ CipherOptics อีเอ็มซี คอร์ปอเรชั่น Decru และ NeoScale Systems เพื่อพัฒนาการเข้ารหัส สร้างมาตรฐานร่วมสำหรับการแลกเปลี่ยนและการจัดการคีย์ ปรับปรุงขีดความสามารถในการแข่งขันและใช้ประโยชน์อย่างคุ้มค่าจากข้อมูลที่มีอยู่

ลักษณะของระบบคือ เป็นระบบที่ใช้อาร์เอสเอ SecurID Token ของผู้รับบริการจะเป็นฮาร์ดแวร์ที่สร้างชุดรหัสเป็นตัวเลขทุกๆ 60 วินาที มีการเปลี่ยนรหัสตลอดเวลาซึ่งต้องซิงโครนัสกับเครื่องผู้ให้บริการอาร์เอสเอ ในการตรวจสอบตัวตนของผู้ใช้โดยองค์กรที่จะใช้งานต้องมีการเตรียมอุปกรณ์คอมพิวเตอร์สำหรับเป็นผู้ให้บริการอาร์เอสเอ อาร์เอสเอ SecurID Token และเครื่องผู้ให้บริการสำหรับตรวจสอบผู้ใช้งานระยะไกล (Radius Server) เพื่อใช้ในระบบ Two Factor Authentication ตัวระบบสามารถป้องกันการดักจับข้อมูลจากโปรแกรมจำพวกดักจับแพ็คเก็จเนื่องจากรหัสผ่านมีการเปลี่ยนแปลงไปเรื่อยๆ และไม่ต้องมีผู้ให้บริการออกใบรับรองหรือโครงสร้างพื้นฐานกุญแจสาธารณะมาเกี่ยวข้องก็ทำงานได้ ส่วนข้อเสียของระบบจะต้องลงทุนกับคอมพิวเตอร์สำหรับเป็นผู้ให้บริการอาร์เอสเอ อาร์เอสเอ SecurID Token ซึ่งมีค่าใช้จ่ายสูงอาจไม่คุ้มค่าในการใช้ระยะยาว

บทที่ 3
การวิเคราะห์และการออกแบบระบบ

ในการพัฒนาระบบพิสูจน์ตัวตนผ่านเครือข่ายเสมือนโดยใช้ Token ประกอบด้วย 3 ส่วน คือส่วนที่ทำหน้าที่เป็นคอมพิวเตอร์แม่ข่ายไว้สำหรับเป็นผู้ให้บริการ (Server) ทำหน้าที่เป็นผู้ให้บริการสำหรับการพิสูจน์ตัวตนก่อนเชื่อมต่อผ่านเครือข่ายเสมือนคือ เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการระบบเครือข่ายเสมือน (VPN Server) ส่วนที่สองคือส่วนที่เป็นเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการระบบพิสูจน์ตัวตนด้วย Token (Token Server) สำหรับพิสูจน์ตัวตนก่อนการเข้าใช้งานระบบงานภายในโดยผ่านเว็บเบราว์เซอร์และเก็บบันทึกเหตุการณ์ (Log) ข้อมูลผู้ใช้งาน และส่วนสุดท้ายคือส่วนของผู้ใช้งานซึ่งจะเป็นคอมพิวเตอร์บุคคลทั่วไปที่เชื่อมต่ออินเทอร์เน็ตและสามารถติดต่อกับเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการได้ต้องทำการ VPN ก่อน หลังจากนั้นทำการพิสูจน์ตัวตนผ่านเว็บเบราว์เซอร์ในลักษณะ 2 ตัวประกอบ โดยใช้ชื่อผู้ใช้ รหัสผ่าน และ Token ซึ่งรายระเอียดการดำเนินงานจะอธิบายไว้ในบทนี้

3.1 การวิเคราะห์และเปรียบเทียบกับระบบอื่นๆ

ระบบพิสูจน์ตัวตนเป็นระบบการพิสูจน์ตัวตนโดยใช้ Token ลักษณะการทำงานของระบบเป็นโปรแกรมที่ทำการสร้างชุดรหัสตัวเลข 6 หลักโดยมีเวลาเข้ามาเกี่ยวข้องโดยหลักการคือ ทั้งเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการและแอพพลิเคชันบนแอนดรอยด์จะมีชุดโปรแกรมและอัลกอริทึมเดียวกันทำการรันโปรแกรมไปเรื่อยๆ โดยเปลี่ยนแปลงทุกๆ 60 วินาที ในการซิงโครนัสรหัสตัวเลขจะใช้เวลาอ้างอิงเหมือนกันในที่นี้ใช้การเชื่อมต่อกับเวลาทางอินเทอร์เน็ตตัวเดียวกันซึ่งจะคล้ายกับระบบ อาร์เอสเอ ในเรื่องของการเปลี่ยนแปลงตัวเลขแต่จะต่างที่เรื่องการซิงโครนัสระหว่างเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการกับตัวอุปกรณ์ Token และมีค่าใช้จ่ายในเรื่องของอุปกรณ์การวางระบบที่แพง

ระบบ VPN เป็นการสร้างระบบที่สามารถเชื่อมต่อเครือข่ายได้แม้ว่าเครือข่ายนั้นจะอยู่สถานที่ต่างกันสามารถเชื่อมโยงเครือข่ายและแลกเปลี่ยนข้อมูลออกภายนอกองค์กรได้อย่างปลอดภัย โดยระบบที่เลือกใช้คือ Open VPN ซึ่งเป็นโปรแกรมโอเพนซอร์สที่มีการใช้งานอย่างแพร่หลาย มีการใช้ SSL เพื่อเพิ่มความปลอดภัย

3.2 ส่วนประกอบของระบบ

1) ส่วนที่ทำหน้าที่เป็นเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ VPN โดยติดตั้งระบบปฏิบัติการและซอฟต์แวร์ต่างๆ ดังนี้

- คอมพิวเตอร์ติดตั้งซอฟต์แวร์ระบบปฏิบัติการ Pfsense
- ติดตั้งฟังก์ชันผู้ให้บริการ VPN ในที่นี้เราได้เลือกใช้ระบบ Open VPN

- ติดตั้งฟังก์ชันผู้ให้บริการระบบพิสูจน์ตัวตน ในที่นี้เราได้เลือกใช้คือ Captive Portal

- ติดตั้งฟังก์ชันบันทึกข้อมูลผู้ใช้งานและเครื่องบริการแทน (Proxy Server)

- ติดตั้งฟังก์ชันบริหารจัดการผู้ใช้งานระบบโดยเราได้เลือกใช้คือ Free Radius

- เชื่อมต่อเครือข่าย 3 ช่องทาง (Interface) ทั้งส่วนที่เป็นเครือข่ายภายในที่มีผู้ใช้งานจากภายในองค์กร ส่วนที่เป็นเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการไว้สำหรับบริการแอพพลิเคชั่นต่างๆ ตั้งอยู่ภายในกลุ่มของเครื่องคอมพิวเตอร์แม่ข่ายและส่วนที่เชื่อมต่อเครือข่ายอินเทอร์เน็ต

- ทำหน้าที่เป็นตัวกลางสำหรับคอมพิวเตอร์เครือข่ายภายใน ที่จะเชื่อมต่อออกสู่อินเทอร์เน็ต

- ทำหน้าที่เป็นตัวกลางสำหรับคอมพิวเตอร์เครือข่ายภายในที่จะเชื่อมต่อและใช้งานระบบคอมพิวเตอร์กลุ่มของเครื่องคอมพิวเตอร์แม่ข่ายภายในองค์กร

- ทำหน้าที่เป็นตัวกลางสำหรับคอมพิวเตอร์ภายนอกที่จะเชื่อมต่อเข้าใช้งานระบบคอมพิวเตอร์ที่ตั้งอยู่ภายในกลุ่มของเครื่องคอมพิวเตอร์แม่ข่ายภายในองค์กร

- มีความปลอดภัยในการใช้งานระบบ ทั้งการตรวจสอบสิทธิ การพิสูจน์ตัวตน ก่อนการใช้งานอินเทอร์เน็ตและจากเครือข่ายอินเทอร์เน็ตผ่านเครือข่ายเสมือนสู่ระบบงานภายในกลุ่มของเครื่องคอมพิวเตอร์แม่ข่ายภายในองค์กร

2) ส่วนที่ทำหน้าที่เป็นเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Token และเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการเว็บด้วย โดยติดตั้งระบบปฏิบัติการและซอฟต์แวร์ต่างๆ ดังนี้

- คอมพิวเตอร์ติดตั้งระบบปฏิบัติการไมโครซอฟท์ วินโดวส์เอกซ์พี (Microsoft Windows XP)

- ติดตั้งฟังก์ชันผู้ให้บริการเว็บ คือ Apache และ ใช้ PHP ช่วยในการพัฒนาเว็บไซต์

- ติดตั้งฟังก์ชันสำหรับเพิ่มความปลอดภัยให้เว็บไซต์คือ Apache Mod SSL

- ติดตั้งฟังก์ชันฐานข้อมูล คือ MySQL

- ติดตั้งฟังก์ชันการพิสูจน์ตัวตน

- ติดตั้งฟังก์ชันบริหารจัดการผู้ใช้งานระบบ

- ติดตั้งฟังก์ชันสำหรับสร้างชุดรหัสตัวเลขใน Token

- ติดตั้งฟังก์ชันอ่านข้อมูลผู้ใช้งานระบบ

- ตั้งค่าการทำงานเชื่อมต่อกับ Pfsense

- ทำหน้าที่พิสูจน์ตัวตนสำหรับผู้ใช้งานระบบคอมพิวเตอร์เครือข่ายภายในที่จะเชื่อมต่อกับระบบคอมพิวเตอร์ภายในกลุ่มของเครื่องคอมพิวเตอร์แม่ข่าย

- ทำหน้าที่พิสูจน์ตัวตนสำหรับคอมพิวเตอร์ภายนอกที่จะเชื่อมต่อเข้าใช้งานระบบคอมพิวเตอร์ภายในของกลุ่มเครื่องคอมพิวเตอร์แม่ข่าย

3) ผู้ดูแลระบบ (Admin)

สามารถจัดการระบบได้ 2 ส่วนคือส่วนที่เป็นระบบคอมพิวเตอร์ผู้ให้บริการ VPN และส่วนที่เป็นระบบการพิสูจน์ตัวตนผ่านเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการเว็บและเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Token

- สามารถสร้าง ลบ แก้ไข รายการผู้ใช้งานระบบผ่านเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ VPN และส่วนที่เป็นระบบการพิสูจน์ตัวตนผ่านเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการเว็บและเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Token ได้

- สามารถตรวจสอบและกำหนดสิทธิการใช้งานของผู้ใช้งานระบบผ่านเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ VPN และส่วนที่เป็นระบบการพิสูจน์ตัวตนผ่านเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการเว็บได้

- สามารถดูข้อมูลผู้ใช้งานในระบบการพิสูจน์ตัวตนผ่านเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการเว็บได้

4) ส่วนที่เป็นผู้ใช้งานระบบ (User) โดยแบ่งเป็น 2 ส่วนคือ

ผู้ใช้งานระบบภายในใช้งานภายในเครือข่าย

- สามารถเชื่อมต่อผ่านทางเว็บเบราว์เซอร์ด้วยโพรโตคอล HTTPS

- ลงบันทึกเข้าใช้งาน (Login) อินเทอร์เน็ตโดยใส่ข้อมูลชื่อผู้ใช้และรหัสผ่าน

- Login เข้าใช้งานอินทราเน็ตโดย ชื่อผู้ใช้ รหัสผ่าน และ Token

ผู้ใช้งานระบบจากภายนอกใช้งานผ่านเครือข่ายภายนอก

- Login เข้าใช้งานเครือข่ายภายใน ด้วยระบบ VPN โดยชื่อผู้ใช้ รหัสผ่าน ผ่านโปรแกรม VPN สำหรับติดตั้งในเครื่องลูกข่าย

- Login เข้าใช้งานอินทราเน็ตโดย ชื่อผู้ใช้ รหัสผ่าน และToken ผ่านโพรโตคอล HTTPS ใน เว็บเบราว์เซอร์

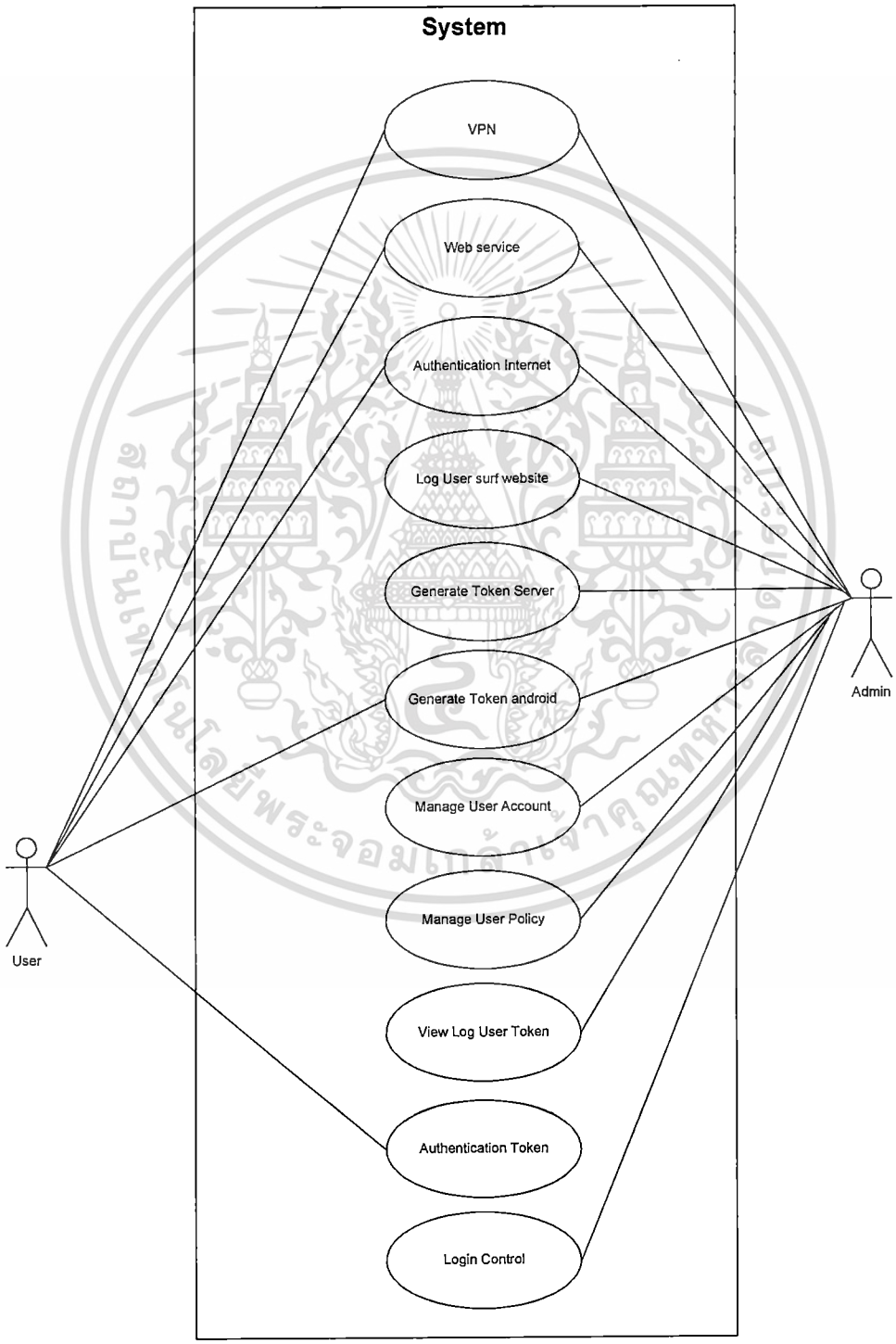
- มีความปลอดภัยในการใช้งานระบบเพราะมีทั้งการพิสูจน์ตัวตนและการเชื่อมต่อในลักษณะเครือข่ายเสมือน

ในการออกแบบระบบนั้นมีการนำยูเอ็มแอลมาใช้เป็นเครื่องมือในการออกแบบระบบ ได้แก่ ยูสเคสไดอะแกรม แอคทีวิตีไดอะแกรม ซีเควนซ์ไดอะแกรม และใช้ภาพแสดงความสัมพันธ์ระหว่างเอนทิตีในการออกแบบฐานข้อมูลซึ่งมีแบบจำลองที่นำเสนอ ดังนี้

3.3 การวิเคราะห์ระบบด้วยยูสเคส (Usecase Diagram)

1) ยูสเคสไดอะแกรม เพื่อใช้ในการแสดงขอบเขตการทำงานของระบบ ซึ่งเป็นเครื่องมือที่ใช้ในการแสดงขอบเขตการทำงานของระบบ และการมีปฏิสัมพันธ์ระหว่างแอกเตอร์และฟังก์ชันการทำงานของระบบ ซึ่งมีฟังก์ชันการทำงานต่างๆ 11 ฟังก์ชัน ได้แก่ ฟังก์ชัน VPN ฟังก์ชันบริการผ่านเว็บ (Web Service) ฟังก์ชันพิสูจน์ตัวตนก่อนการใช้งานอินเทอร์เน็ต (Authentication Internet)

ฟังก์ชันดูข้อมูลผู้ใช้งานเว็บไซต์ (Log User Surf Website) ฟังก์ชันพิสูจน์ตัวตนร่วมกับอุปกรณ์ Token (Authentication Token) ฟังก์ชันสำหรับสร้างรหัสตัวเลขที่คอมพิวเตอร์แม่ข่าย (Generate Token Server) ฟังก์ชันสร้างรหัสตัวเลขบนโทรศัพท์เคลื่อนที่ติดตั้งระบบปฏิบัติการแอนดรอยด์ (Generate Token Android) ฟังก์ชันจัดการบัญชีผู้ใช้งาน (Manage User Account) ฟังก์ชันกำหนดสิทธิผู้ใช้งาน (Manage User Policy) ฟังก์ชันดูข้อมูลผู้ใช้งาน Token (View Log User Token) และฟังก์ชันกำกับการบันทึกเข้าใช้งานระบบ (Login Control) ดังรูปที่ 3.1



รูปที่ 3.1 แสดงยูสเคสไดอะแกรม

2) รายละเอียดยูสเคส (Usecase Description)

จากยูสเคสไดอะแกรมของระบบซึ่งประกอบด้วย 11 ฟังก์ชันการทำงานสามารถอธิบายรายละเอียดการทำงานได้ ดังตารางที่ 3.1 - 3.11

ตารางที่ 3.1 ยูสเคสแสดงการทำงานของฟังก์ชัน VPN

ชื่อยูสเคส	VPN
วัตถุประสงค์	บริการตอบรับการเชื่อมต่อเครือข่ายเสมือน
Actor	ผู้ดูแลระบบและผู้ใช้งานระบบ
เงื่อนไขก่อนหน้า	1)เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการที่ทำการติดตั้งฟังก์ชัน VPN เปิดทำงานและพร้อมให้บริการการติดต่อจากเครื่องภายนอก
ลำดับเหตุการณ์ปกติ	1)ผู้ดูแลระบบทำการ Login เข้าใช้งานที่เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ VPN หลังจากนั้นทำการเปิดการใช้งานฟังก์ชัน VPN เพื่อรอให้บริการการเชื่อมต่อจากเครื่องคอมพิวเตอร์ภายนอก 2)ฟังก์ชัน VPN ทำหน้าที่รอรับการร้องขอการเชื่อมต่อเครือข่ายเสมือนจากผู้ใช้งานระบบภายนอกที่ใช้งานอยู่ตามเครือข่ายสาธารณะจากต่างสถานที่กันผ่านโปรแกรม VPN 3)เมื่อผู้ใช้งานระบบจากภายนอกที่ใช้งานเครือข่ายอินเทอร์เน็ตสาธารณะเชื่อมต่อเข้ามาเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ VPN จะทำการตรวจสอบสิทธิเพื่อยืนยันตัวตนก่อนการใช้งานและถ้าตรวจสอบแล้วมีสิทธิถูกต้องจะทำการสร้างอุโมงค์เพื่อเชื่อมต่อระหว่างเครือข่ายที่ผู้ใช้งานระบบใช้อยู่ผ่านเครือข่ายอินเทอร์เน็ตสาธารณะกับเครือข่ายภายในองค์กร 4)เมื่อผู้ใช้งานระบบจากภายนอกใช้งานเสร็จแล้วต้องการสิ้นสุดการทำงานจึงทำการยกเลิกการเชื่อมต่อเครือข่ายเสมือนระหว่างสองเครือข่าย
เหตุการณ์ที่เป็นทางเลือก	1)เมื่อตรวจสอบแล้วไม่มีบัญชีผู้ใช้งานระบบนั้นจากเครือข่ายภายนอกในฐานข้อมูลของเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ VPN หรือมีการใส่ข้อมูลที่ผิดให้ระบบทำการปฏิเสธการเชื่อมต่อ
เงื่อนไขภายหลัง	-

ตารางที่ 3.2 ยูสเคสแสดงการทำงานของฟังก์ชัน Web Service

ชื่อยูสเคส	Web Service
วัตถุประสงค์	เป็นการเปิดบริการตอบรับการเชื่อมต่อจากผู้ใช้งานเมื่อต้องการเชื่อมต่อเข้าระบบงานภายในเพื่อทราบจุดหมายในการเชื่อมต่อ
Actor	ผู้ดูแลระบบและผู้ใช้งานระบบ
เงื่อนไขก่อนหน้า	1)เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการที่ทำการติดตั้งฟังก์ชันเว็บเปิดทำงานและพร้อมให้บริการการติดต่อจากเครื่องภายนอก
ลำดับเหตุการณ์ปกติ	1)ผู้ดูแลระบบทำการ Login เข้าใช้งานที่เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการเว็บหลังจากนั้นทำการเปิดการใช้งานฟังก์ชันเว็บเพื่อรอให้บริการการเชื่อมต่อจากเครื่องคอมพิวเตอร์ต่างๆที่มีการเชื่อมต่อเครือข่ายถึงกัน 2)ฟังก์ชันเว็บรอรับการร้องขอการเชื่อมต่อจากผู้ใช้งานทั้งส่วนของผู้ใช้งานภายในเครือข่ายหรือผู้ที่ใช้งานผ่านเครือข่ายอินเทอร์เน็ตสาธารณะโดยสามารถระบุตำแหน่งที่ถูกต้องของเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการเว็บได้เมื่อมีความต้องการเชื่อมต่อเพื่อใช้งาน 3)เมื่อผู้ใช้งานระบบทั้งจากเครือข่ายภายในและเครือข่ายภายนอกผ่านอินเทอร์เน็ตสาธารณะต้องการเชื่อมต่อเข้ามาใช้งานเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการเว็บทำการตรวจสอบสิทธิการใช้งานและถ้าถูกต้องจึงทำการสร้างการเชื่อมต่อระหว่างผู้ใช้งานระบบกับเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการเว็บ 4)เมื่อผู้ใช้งานระบบใช้งานเสร็จแล้วต้องการสิ้นสุดการทำงานจึงทำการยกเลิกการเชื่อมต่อเครือข่าย
เหตุการณ์ที่เป็นทางเลือก	1)เมื่อตรวจสอบแล้วไม่มีบัญชีผู้ใช้งานระบบนั้นจากเครือข่ายภายนอกในฐานข้อมูลของเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการเว็บหรือมีการใส่ข้อมูลที่ผิดให้ระบบทำการปฏิเสธการเชื่อมต่อ
เงื่อนไขภายหลัง	-

ตารางที่ 3.3 ยูสเคสแสดงการทำงานของฟังก์ชัน Authentication Internet

ชื่อยูสเคส	Authentication Internet
วัตถุประสงค์	สามารถบริการตอบรับการเชื่อมต่อเพื่อตรวจสอบสิทธิการใช้งานสำหรับการพิสูจน์ตัวตนของผู้ใช้งานระบบ
Actor	ผู้ดูแลระบบและผู้ใช้งานระบบ
เงื่อนไขก่อนหน้า	1)เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการที่ทำการติดตั้งฟังก์ชัน Proxy เปิดทำงานและพร้อมให้บริการการติดต่อจากเครื่องผู้ใช้งานภายในเครือข่าย
ลำดับเหตุการณ์ปกติ	1)ผู้ดูแลระบบทำการ Login เข้าใช้งานที่เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Proxy หลังจากนั้นทำการเปิดการใช้งานฟังก์ชัน Proxy เพื่อรอให้บริการการเชื่อมต่อจากเครื่องคอมพิวเตอร์เครือข่ายภายใน 2)ฟังก์ชัน Proxy รอรับการร้องขอการเชื่อมต่อจากผู้ใช้งานภายในเครือข่ายเมื่อต้องการเชื่อมต่อออกสู่เครือข่ายอินเทอร์เน็ต 3)เมื่อผู้ใช้งานระบบจากเครือข่ายภายในร้องขอการเชื่อมต่อเพื่อใช้งาน คอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Proxy ทำการตรวจสอบสิทธิการใช้งานและถ้าถูกต้องจึงทำการสร้างการเชื่อมต่อเพื่อให้ผู้ใช้งานติดต่อกับเครือข่ายอินเทอร์เน็ตได้ 4)เมื่อผู้ใช้งานระบบใช้งานเสร็จแล้วต้องการสิ้นสุดการทำงานจึงทำการยกเลิกการเชื่อมต่อ
เหตุการณ์ที่เป็นทางเลือก	1)เมื่อตรวจสอบแล้วไม่มีบัญชีผู้ใช้งานในฐานข้อมูลของเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Proxy หรือมีการใส่ข้อมูลที่ผิดให้ระบบทำการปฏิเสธการเชื่อมต่อ
เงื่อนไขภายหลัง	-

ตารางที่ 3.4 ยูสเคสแสดงการทำงานของฟังก์ชัน Log User Surf Website

ชื่อยูสเคส	Log User Surf Website
วัตถุประสงค์	สามารถให้บริการจัดเก็บบันทึกข้อมูลผู้ใช้งานระบบที่ใช้งานเว็บไซต์และสามารถตอบรับเมื่อมีการเรียกดึงข้อมูลมาแสดงเป็นรายงานได้
Actor	ผู้ดูแลระบบ
เงื่อนไขก่อนหน้า	1)เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการที่ทำการติดตั้งฟังก์ชัน Proxy เปิดทำงานและพร้อมให้บริการการติดต่อจากเครื่องภายในเครือข่าย 2)เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการที่ทำการติดตั้งฟังก์ชันสำหรับการพิสูจน์ตัวตนเปิดทำงานและพร้อมให้บริการ
ลำดับเหตุการณ์ปกติ	1)ผู้ดูแลระบบทำการ Login เข้าใช้งานที่เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Proxy หลังจากนั้นทำการเปิดการใช้งานฟังก์ชัน Proxy เพื่อรอให้บริการ 2)ผู้ดูแลระบบทำการ Login เข้าใช้งานที่เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการที่ไว้สำหรับระบบพิสูจน์ตัวตนหลังจากนั้นทำการเปิดการใช้งานฟังก์ชันสำหรับการพิสูจน์ตัวตนเพื่อรอให้บริการการเชื่อมต่อจากเครื่องคอมพิวเตอร์เครือข่ายภายใน 3)เมื่อผู้ใช้งานระบบจากเครือข่ายภายในร้องขอการเชื่อมต่อเพื่อใช้งาน เครื่องคอมพิวเตอร์ที่ติดตั้งฟังก์ชันให้บริการ Proxy ทำการตรวจสอบสิทธิการใช้งานก่อนอนุญาตผู้ใช้งานติดต่อกับเครือข่ายอินเทอร์เน็ตได้ 4)เมื่อผู้ใช้งานระบบจากเครือข่ายภายในร้องขอการเชื่อมต่อเพื่อใช้งานเครื่องคอมพิวเตอร์ที่ติดตั้งฟังก์ชันระบบพิสูจน์ตัวตน ระบบจะทำการตรวจสอบสิทธิการใช้งานและถ้าถูกต้องจึงทำการสร้างการเชื่อมต่อเพื่อให้ผู้ใช้งานติดต่อกับเครือข่ายอินเทอร์เน็ตได้ 5)ในระหว่างการใช้งานที่ผู้ใช้งานระบบเชื่อมต่อเข้ามาจะทำการบันทึกข้อมูลการใช้และเก็บข้อมูลการทำงานของผู้ใช้งานอินเทอร์เน็ตและส่งข้อมูลผู้ใช้งานไปยังเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ VPN เพื่อทำการบันทึกและสามารถเรียกดูข้อมูลได้ 6)เมื่อผู้ใช้งานระบบใช้งานเสร็จแล้วต้องการสิ้นสุดการทำงานระบบทำการยกเลิกการบันทึกข้อมูล
เหตุการณ์ที่เป็นทางเลือก	-
เงื่อนไขภายหลัง	-

ตารางที่ 3.5 ยูสเคสแสดงการทำงานของฟังก์ชัน Authentication Token

ชื่อยูสเคส	Authentication Token
วัตถุประสงค์	สามารถบริการตอบรับการเชื่อมต่อเพื่อตรวจสอบการพิสูจน์ตัวตนของผู้ใช้งานระบบ
Actor	ผู้ดูแลระบบและผู้ใช้งานระบบ
เงื่อนไขก่อนหน้า	1)เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการที่ทำการติดตั้งฟังก์ชัน Token เปิดทำงานและพร้อมให้บริการการติดต่อ 2)เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการที่ทำการติดตั้งฟังก์ชันเว็บเปิดทำงานและพร้อมให้บริการ
ลำดับเหตุการณ์ปกติ	1)ผู้ดูแลระบบทำการ Login เข้าใช้งานที่เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Token หลังจากนั้นทำการเปิดการใช้งานฟังก์ชันเพื่อรอให้บริการการเชื่อมต่อจากเครื่องคอมพิวเตอร์ที่เชื่อมต่อเครือข่ายถึงกันได้ 2)เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Token รอรับการร้องขอการเชื่อมต่อจากผู้ใช้งานที่ต้องการเชื่อมต่อระบบพิสูจน์ตัวตันก่อนใช้งานเว็บอินทราเน็ต 3)เมื่อผู้ใช้งานระบบร้องขอการเชื่อมต่อเพื่อใช้งาน เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Token ทำการตรวจสอบสิทธิการใช้งานและถ้าถูกต้องจึงอนุญาตให้ใช้งาน 4)เมื่อผู้ใช้งานระบบใช้งานเสร็จแล้วต้องการสิ้นสุดการทำงานจึงทำการยกเลิกการเชื่อมต่อ
เหตุการณ์ที่เป็นทางเลือก	1)เมื่อตรวจสอบแล้วไม่มีบัญชีผู้ใช้งานระบบนั้นจากในฐานข้อมูลของเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Token หรือมีการใส่ข้อมูลที่ผิดให้ระบบทำการปฏิเสธการเชื่อมต่อ
เงื่อนไขภายหลัง	-

ตารางที่ 3.6 ยูสเคสแสดงการทำงานของฟังก์ชัน Generate Token Server

ชื่อยูสเคส	Generate Token Server
วัตถุประสงค์	สามารถสร้างและให้บริการรหัสตัวเลข 6 หลัก สำหรับใช้เป็นตัวประกอบที่ 2 เพื่อใช้ยืนยันตัวตนในส่วนของ Token เมื่อมีการ Login เข้าให้งานระบบ
Actor	ผู้ดูแลระบบ
เงื่อนไขก่อนหน้า	1)เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการที่ทำการติดตั้งฟังก์ชัน Token เปิดทำงานและพร้อมให้บริการ
ลำดับเหตุการณ์ปกติ	1)ผู้ดูแลระบบทำการ Login เข้าใช้งานที่เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Token หลังจากนั้นทำการเปิดการใช้งานฟังก์ชันเพื่อรอให้บริการการเชื่อมต่อจากเครื่องคอมพิวเตอร์ที่ต้องการใช้งานระบบพิสูจน์ตัวตนด้วย Token 2)เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Token รอรับการร้องขอการเชื่อมต่อจากผู้ใช้งานที่ต้องการเชื่อมต่อระบบพิสูจน์ตัวตันก่อนใช้งานเว็บอินทราเน็ต 3)เมื่อผู้ใช้งานระบบร้องขอการเชื่อมต่อเพื่อใช้งาน เครื่องคอมพิวเตอร์ที่ติดตั้งฟังก์ชันและทำหน้าที่เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Token ทำการตรวจสอบรหัสตัวเลขว่าตรงกันหรือไม่ก่อนอนุญาตใช้งาน 4)สร้างชุดรหัสตัวเลขไปเรื่อยๆใช้สำหรับเป็นตัวประกอบที่ 2 เพื่อเพิ่มความปลอดภัยไว้ตรวจสอบการพิสูจน์ตัวตน
เหตุการณ์ที่เป็นทางเลือก	-
เงื่อนไขภายหลัง	-

ตารางที่ 3.7 ยูสเคสแสดงการทำงานของฟังก์ชัน Generate Token Android

ชื่อยูสเคส	Generate Token Android
วัตถุประสงค์	สามารถสร้างและให้บริการรหัสตัวเลข 6 หลัก สำหรับใช้เป็นตัวประกอบที่ 2 เพื่อใช้ยืนยันตัวตนในส่วนของ Token เมื่อมีการ Login เข้าให้งานระบบ
Actor	ผู้ดูแลระบบและผู้ใช้งานระบบ
เงื่อนไขก่อนหน้า	1)เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการที่ทำการติดตั้งฟังก์ชัน Token เปิดทำงานและพร้อมให้บริการ 2)โทรศัพท์เคลื่อนที่ที่มีการติดตั้งฟังก์ชัน Token บนระบบปฏิบัติการแอนดรอยด์เปิดทำงานและพร้อมให้บริการ
ลำดับเหตุการณ์ปกติ	1)ผู้ดูแลระบบทำการ Login เข้าใช้งานที่เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Token หลังจากนั้นทำการเปิดการใช้งานฟังก์ชันเพื่อรอให้บริการการเชื่อมต่อจากเครื่องคอมพิวเตอร์ที่ต้องการใช้งานระบบพิสูจน์ตัวตนด้วย Token 2)ผู้ดูแลระบบติดตั้งและเปิดการทำงานของแอพพลิเคชัน Token บนระบบปฏิบัติการแอนดรอยด์ 3)Token ซึ่งติดตั้งบนระบบปฏิบัติการแอนดรอยด์ในโทรศัพท์เคลื่อนที่ทำการเชื่อมต่อกับเวลาทางอินเทอร์เน็ตและสร้างรหัสตัวเลข 6 หลัก 4)เมื่อผู้ใช้งานระบบเชื่อมต่อเข้ามาและทำการใส่รหัสตัวเลข ระบบจะทำการตรวจสอบคู่รหัสว่าข้อมูลถูกต้องตรงหรือไม่จึงจะอนุญาตให้ใช้งานได้ 5)สร้างชุดรหัสตัวเลขไปเรื่อยๆใช้สำหรับเป็นตัวประกอบที่ 2 เพื่อเพิ่มความปลอดภัยไว้ตรวจสอบการพิสูจน์ตัวตน
เหตุการณ์ที่เป็นทางเลือก	-
เงื่อนไขภายหลัง	-

ตารางที่ 3.8 ยูสเคสแสดงการทำงานของฟังก์ชัน Manage User Account

ชื่อยูสเคส	Manage User Account
วัตถุประสงค์	สามารถจัดการสร้าง ลบ แก้ไข ข้อมูลผู้ใช้งาน
Actor	ผู้ดูแลระบบ
เงื่อนไขก่อนหน้า	1)เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการที่ทำการติดตั้งฟังก์ชัน VPN เปิดทำงานและพร้อมให้บริการ 2)เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการที่ทำการติดตั้งฟังก์ชัน Token เปิดทำงานและพร้อมให้บริการ 3)ผู้ดูแลระบบมีสิทธิในการจัดการ
ลำดับเหตุการณ์ปกติ	1)ผู้ดูแลระบบทำการ Login เข้าใช้งานที่เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Token หลังจากนั้นทำการเปิดการใช้งานฟังก์ชันเพื่อรอให้บริการการเชื่อมต่อจากเครื่องคอมพิวเตอร์ที่ต้องการใช้งานระบบพิสูจน์ตัวตนด้วย Token 2)ผู้ดูแลระบบทำการ Login เข้าใช้งานที่เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ VPN หลังจากนั้นทำการเปิดการใช้งานฟังก์ชัน VPN เพื่อรอให้บริการการเชื่อมต่อจากเครื่องคอมพิวเตอร์ภายนอก 3)เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการทำการตรวจสอบข้อมูลและหลังจากทำการตรวจสอบชื่อผู้ใช้ รหัสผ่านแล้วอนุญาตให้ใช้งานระบบได้ 4)ผู้ดูแลระบบทำการสร้าง เพิ่ม ลบ แก้ไขรายการบัญชีผู้ใช้งานในเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Token 5)ผู้ดูแลระบบทำการสร้าง เพิ่ม ลบ แก้ไขรายการบัญชีผู้ใช้งานในเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ VPN 6)เมื่อผู้ดูแลระบบใช้งานเสร็จแล้วต้องการสิ้นสุดการทำงานจึงทำการยกเลิกการเชื่อมต่อและออกจากระบบ
เหตุการณ์ที่เป็นทางเลือก	1)เมื่อตรวจสอบแล้วไม่มีบัญชีผู้ใช้งานในฐานข้อมูลหรือมีการใส่ข้อมูลที่ผิดให้ระบบทำการปฏิเสธการเชื่อมต่อ
เงื่อนไขภายหลัง	-

ตารางที่ 3.9 ยูสเคสแสดงการทำงานของฟังก์ชัน Manage User Policy

ชื่อยูสเคส	Manage User Policy
วัตถุประสงค์	สามารถจัดการ กำหนดสิทธิการเข้าใช้งานระบบของผู้ใช้งาน
Actor	ผู้ดูแลระบบ
เงื่อนไขก่อนหน้า	1)เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการที่ทำการติดตั้งฟังก์ชัน VPN เปิดทำงานและพร้อมให้บริการ 2)เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการที่ทำการติดตั้งฟังก์ชัน Token เปิดทำงานและพร้อมให้บริการ 3)ผู้ดูแลระบบมีสิทธิในการจัดการ
ลำดับเหตุการณ์ปกติ	1)ผู้ดูแลระบบทำการ Login เข้าใช้งานที่เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Token หลังจากนั้นทำการเปิดการใช้งานฟังก์ชันเพื่อรอให้บริการการเชื่อมต่อจากเครื่องคอมพิวเตอร์ที่ต้องการใช้งานระบบพิสูจน์ตัวตนด้วย Token 2)ผู้ดูแลระบบทำการ Login เข้าใช้งานที่เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ VPN หลังจากนั้นทำการเปิดการใช้งานฟังก์ชัน VPN เพื่อรอให้บริการการเชื่อมต่อจากเครื่องคอมพิวเตอร์ภายนอก 3)เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการทำการตรวจสอบข้อมูลและหลังจากทำการตรวจสอบชื่อผู้ใช้ รหัสผ่านแล้วอนุญาตให้ใช้งานระบบได้ 4)ผู้ดูแลระบบทำการกำหนดสิทธิการเข้าใช้งาน เช่นช่วงระยะเวลาเชื่อมต่อ ที่สามารถใช้งานได้ การเข้าใช้งานพร้อมกันหลาย ผู้ใช้งานระบบ ทั้งเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Token และเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ VPN 5)เมื่อผู้ดูแลระบบใช้งานเสร็จแล้วต้องการสิ้นสุดการทำงานจึงทำการยกเลิกการเชื่อมต่อและออกจากระบบ
เหตุการณ์ที่เป็นทางเลือก	1)เมื่อตรวจสอบแล้วไม่มีบัญชีผู้ใช้งานในฐานข้อมูลหรือมีการใส่ข้อมูลที่ผิดให้ระบบทำการปฏิเสธการเชื่อมต่อ
เงื่อนไขภายหลัง	-

ตารางที่ 3.10 ยูสเคสแสดงการทำงานของฟังก์ชัน View Log User Token

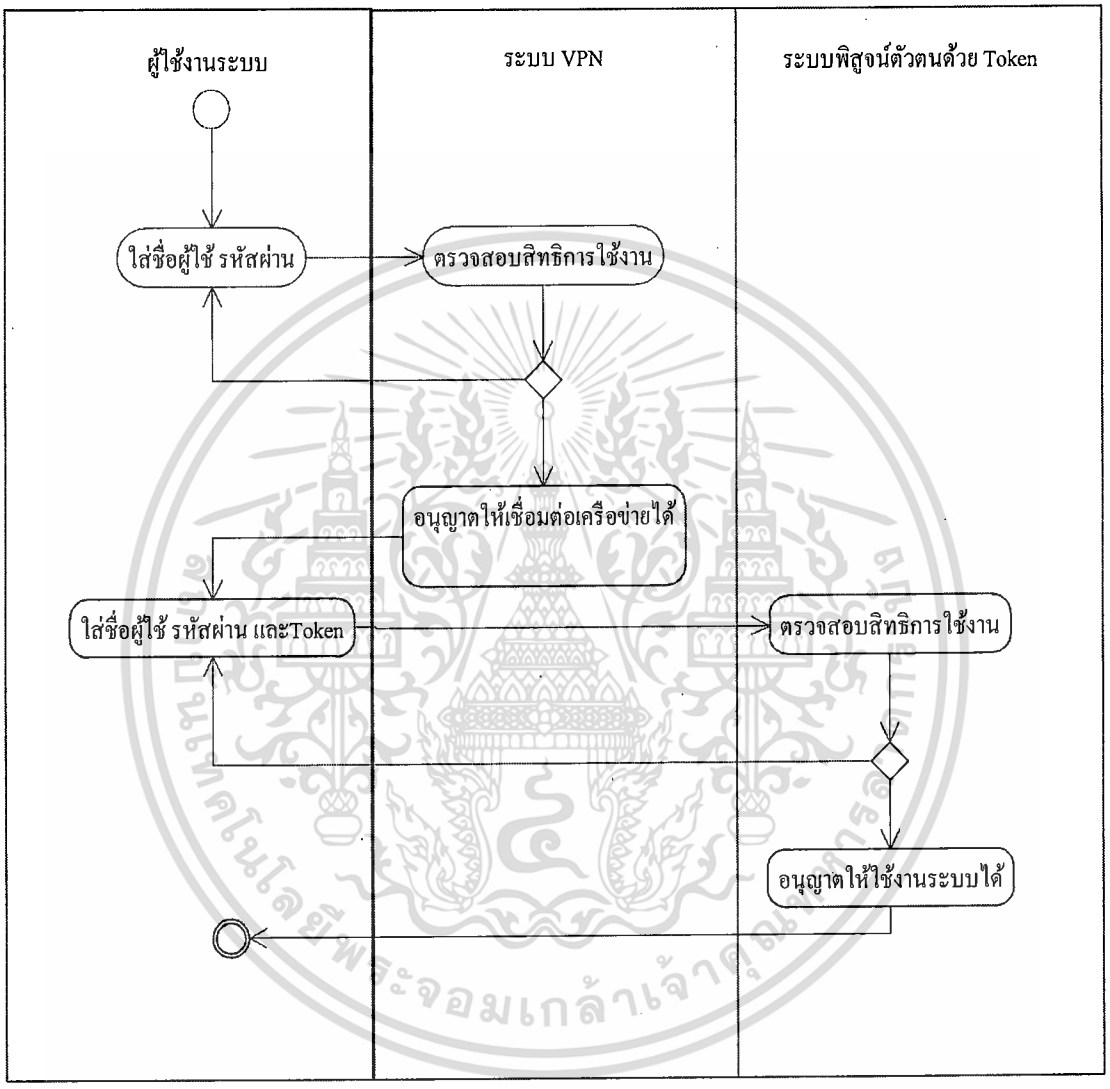
ชื่อยูสเคส	View Log User Token
วัตถุประสงค์	สามารถตรวจสอบและดึงข้อมูลผู้ใช้งานระบบ
Actor	ผู้ดูแลระบบ
เงื่อนไขก่อนหน้า	1)เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการที่ทำการติดตั้งฟังก์ชัน Token เปิดทำงานและพร้อมให้บริการ 2)ผู้ดูแลระบบมีสิทธิในการจัดการ
ลำดับเหตุการณ์ปกติ	1)ผู้ดูแลระบบทำการ Login เข้าใช้งานที่เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Token หลังจากนั้นทำการเปิดการใช้งานฟังก์ชันเพื่อรอให้บริการการเชื่อมต่อจากเครื่องคอมพิวเตอร์ที่ต้องการใช้งานระบบพิสูจน์ตัวตนด้วย Token 2)เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการทำการตรวจสอบข้อมูลและหลังจากทำการตรวจสอบชื่อผู้ใช้ รหัสผ่านแล้วอนุญาตให้ใช้งานระบบได้ 3)ผู้ดูแลระบบทำการดึงข้อมูลผู้ใช้งานระบบออกมาแสดงเป็นรายงานได้ 4)เมื่อผู้ดูแลระบบใช้งานเสร็จแล้วต้องการสิ้นสุดการทำงานจึงทำการยกเลิกการเชื่อมต่อและออกจากระบบ
เหตุการณ์ที่เป็นทางเลือก	1)เมื่อตรวจสอบแล้วไม่มีบัญชีผู้ใช้งานในฐานข้อมูลหรือมีการใส่ข้อมูลที่ผิดให้ระบบทำการปฏิเสธการเชื่อมต่อ
เงื่อนไขภายหลัง	-

ตารางที่ 3.11 ยูสเคสแสดงการทำงานของฟังก์ชัน Login Control

ชื่อยูสเคส	Login Control
วัตถุประสงค์	ผู้ใช้งานระบบ Login เข้าใช้งานระบบ
Actor	ผู้ดูแลระบบ
เงื่อนไขก่อนหน้า	1)เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการที่ทำการติดตั้งฟังก์ชัน VPN เปิดทำงานและพร้อมให้บริการ 2)เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการที่ทำการติดตั้งฟังก์ชัน Token เปิดทำงานและพร้อมให้บริการ 3)ผู้ดูแลระบบมีสิทธิในการจัดการ
ลำดับเหตุการณ์ปกติ	1)ผู้ดูแลระบบทำการ Login เข้าใช้งานที่เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Token หลังจากนั้นทำการเปิดการใช้งานฟังก์ชันเพื่อรอให้บริการการเชื่อมต่อจากเครื่องคอมพิวเตอร์ที่ต้องการใช้งานระบบพิสูจน์ตัวตนด้วย Token 2)ผู้ดูแลระบบทำการ Login เข้าใช้งานที่เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ VPN หลังจากนั้นทำการเปิดการใช้งานฟังก์ชัน VPN เพื่อรอให้บริการการเชื่อมต่อจากเครื่องคอมพิวเตอร์ภายนอก 3)เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการทำการตรวจสอบข้อมูลและหลังจากทำการตรวจสอบชื่อผู้ใช้ รหัสผ่านแล้วอนุญาตให้ใช้งานระบบได้ เพื่อจัดการบัญชีผู้ใช้งานระบบ 4)เมื่อผู้ดูแลระบบใช้งานเสร็จแล้วต้องการสิ้นสุดการทำงานจึงทำการยกเลิกการเชื่อมต่อและออกจากระบบ
เหตุการณ์ที่เป็นทางเลือก	1)เมื่อตรวจสอบแล้วไม่มีบัญชีผู้ใช้งานในฐานข้อมูลหรือมีการใส่ข้อมูลที่ผิดให้ระบบทำการปฏิเสธการเชื่อมต่อ
เงื่อนไขภายหลัง	-

3.4 แอคทิวิตีไดอะแกรม (Activity Diagram)

ภาพรวมการทำงานของระบบจะแบ่งเป็น 2 ส่วน โดยเริ่มต้นที่ผู้ใช้งานทำการ Login เข้าใช้งาน VPN ก่อนเมื่อสำเร็จจะต้องทำการ Login เข้าใช้งานระบบพิสูจน์ตัวตนด้วย Token อีกหนึ่งขั้นตอน ซึ่งรายละเอียดขั้นตอนการทำงานของระบบแสดงในแอคทิวิตีไดอะแกรม ดังรูป 3.2



รูปที่ 3.2 แอคทีวิตีไดอะแกรมการทำงานของระบบพิสูจน์ตัวตนผ่านเครือข่ายเสมือนด้วย Token

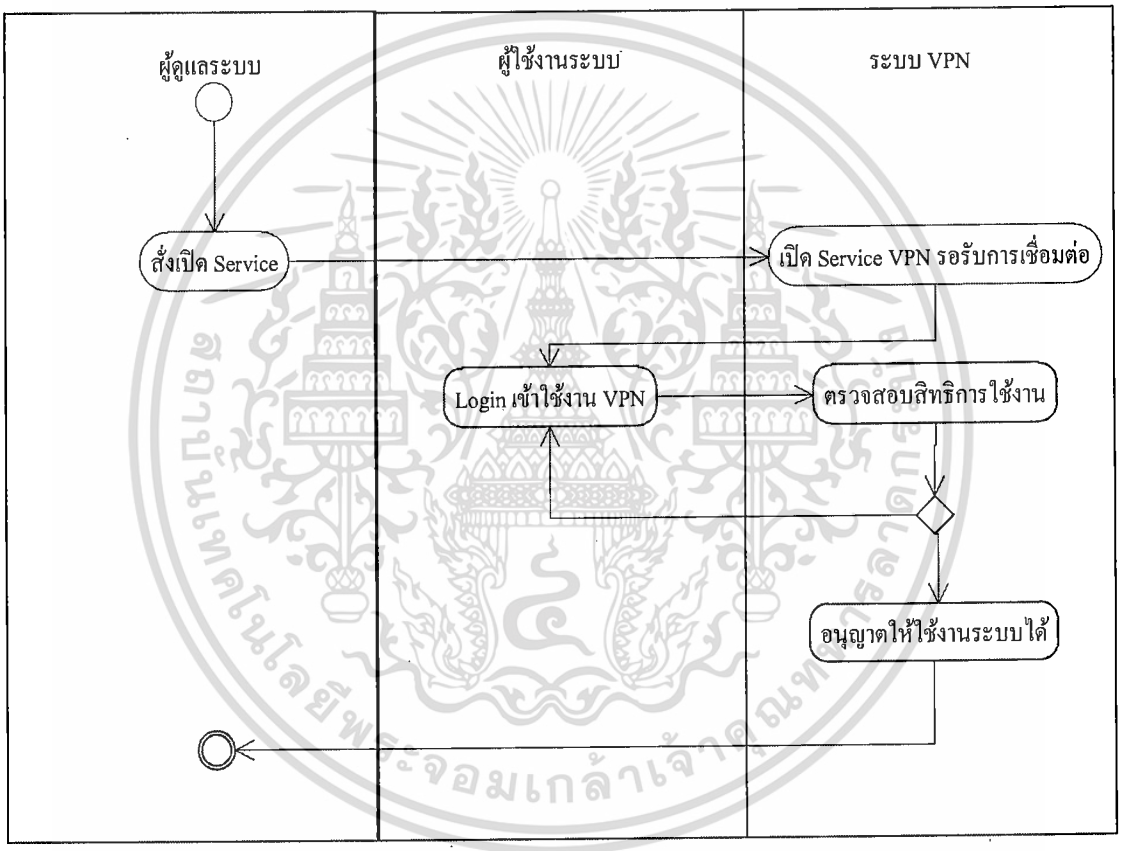
ฟังก์ชันการทำงานของ VPN มีขั้นตอนคือ

1. ผู้ดูแลระบบทำการเปิด Service ที่เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ VPN เพื่อรอรับการเชื่อมต่อเครือข่ายจากเครื่องคอมพิวเตอร์ผู้ใช้งานจากภายนอกเครือข่าย

2. ผู้ใช้งานจากภายนอกตรวจสอบการเชื่อมต่อระหว่างเครื่องคอมพิวเตอร์กับเครือข่ายอินเทอร์เน็ตหลังจากนั้นเปิดโปรแกรม VPN แล้วทำการ Login เข้าใช้งาน

3. เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ VPN ทำการตรวจสอบชื่อผู้ใช้งาน รหัสผ่าน สิทธิการใช้งานเมื่อข้อมูลถูกต้องจะอนุญาตให้ใช้งานได้โดยทำการสร้างการเชื่อมต่อเสมือนระหว่างคอมพิวเตอร์ภายนอกกับเครือข่ายภายใน

รายละเอียดขั้นตอนการทำงานของฟังก์ชัน VPN แสดงในแอคทิวิตีไดอะแกรมดังรูปที่ 3.3



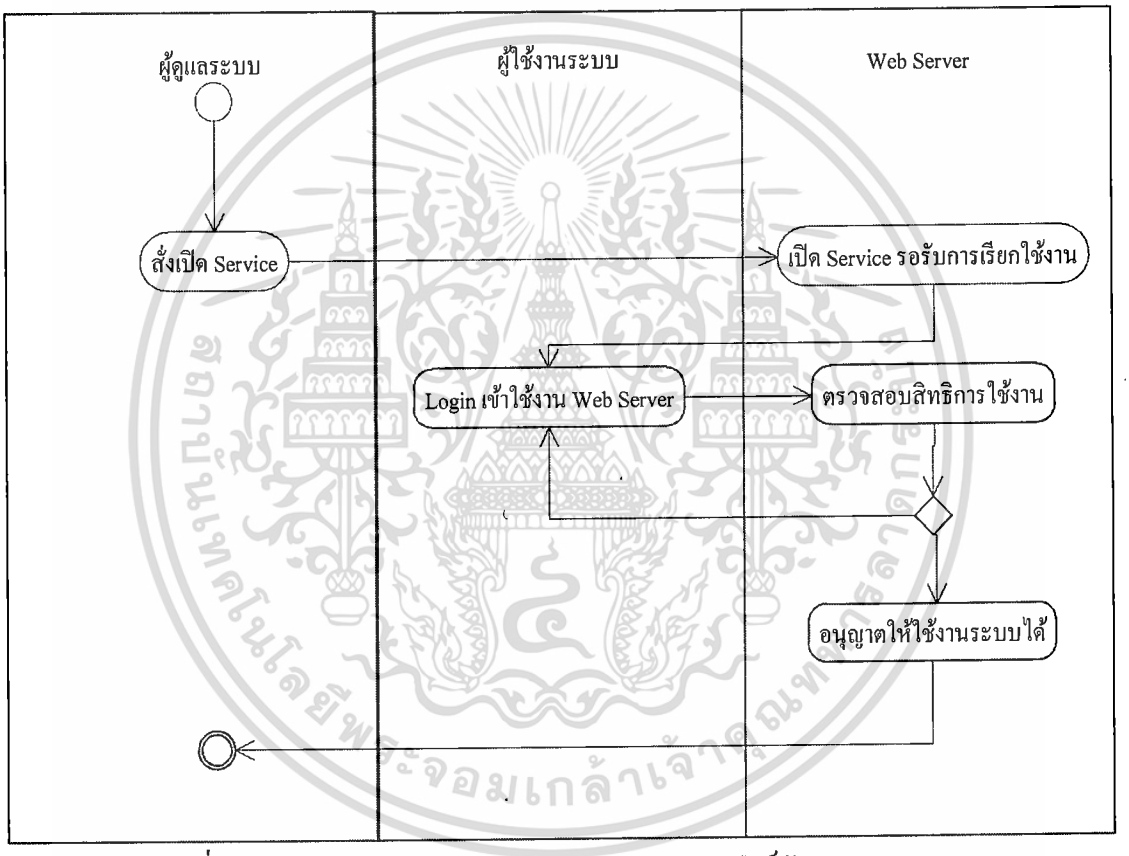
รูปที่ 3.3 แอคทิวิตีไดอะแกรมแสดงการทำงานของฟังก์ชัน VPN

ฟังก์ชันการทำงานของ Web Service มีขั้นตอนคือ

1. ผู้ดูแลระบบทำการเปิดฟังก์ชันการทำงานที่เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการเว็บเพื่อรอรับการเชื่อมต่อเครือข่ายจากเครื่องคอมพิวเตอร์ผู้ใช้งาน

2. ผู้ใช้งานระบบตรวจสอบการเชื่อมต่อระหว่างเครื่องคอมพิวเตอร์กับเครือข่ายอินเทอร์เน็ตหลังจากนั้นเปิดโปรแกรมเว็บเบราว์เซอร์แล้วทำการ Login เข้าใช้งาน

3. เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการเว็บทำการตรวจสอบชื่อผู้ใช้งาน รหัสผ่านและสิทธิการใช้งานเมื่อข้อมูลถูกต้องจะอนุญาตให้ใช้งานระบบงานภายในผ่านเว็บเบราว์เซอร์ได้ รายละเอียดขั้นตอนการทำงานของฟังก์ชันเว็บแสดงในแอคทิวิตีไดอะแกรมดังรูปที่ 3.4



รูปที่ 3.4 แอคทีวิตีไดอะแกรมแสดงการทำงานของฟังก์ชัน Web Service

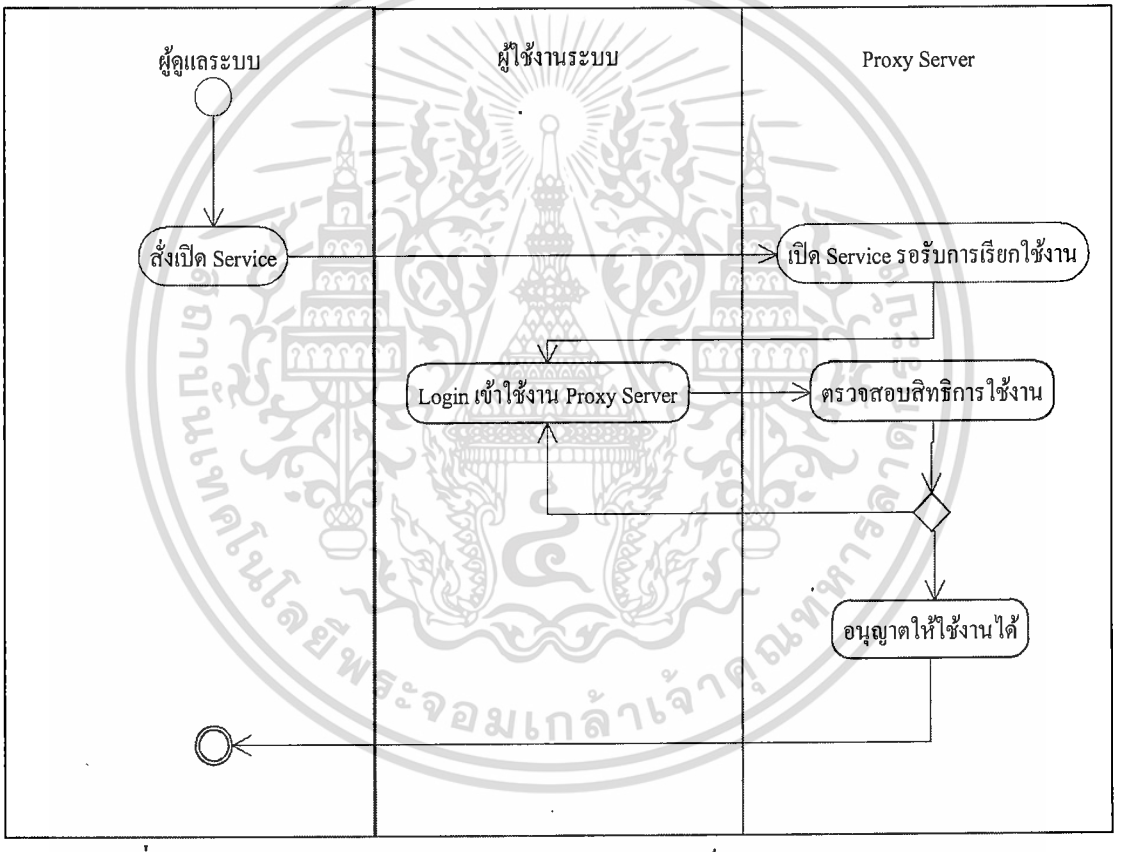
ฟังก์ชันการทำงานของ Authentication Internet มีขั้นตอนคือ

1. ผู้ดูแลระบบทำการเปิดฟังก์ชันการทำงานที่เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Proxy เพื่อรอรับการเชื่อมต่อเครือข่ายจากเครื่องคอมพิวเตอร์ผู้ใช้งานภายในก่อนทำการใช้งานอินเทอร์เน็ตเพื่อยืนยันตัวตน

2. ผู้ใช้งานภายในเครือข่ายเปิดโปรแกรมเว็บเบราว์เซอร์ แล้วทำการ Login เข้าใช้งาน

3. เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Proxy ทำการตรวจสอบชื่อผู้ใช้งาน รหัสผ่าน สิทธิการใช้งานเมื่อข้อมูลถูกต้องจะอนุญาตให้ใช้งานอินเทอร์เน็ตผ่านเว็บเบราว์เซอร์ได้

รายละเอียดขั้นตอนการทำงานของฟังก์ชัน Authentication Internet แสดงในแอคทิวิตีไดอะแกรมดังรูปที่ 3.5



รูปที่ 3.5 แอคทีวิตีไดอะแกรมแสดงการทำงานของฟังก์ชัน Authentication Internet

ฟังก์ชันการทำงานของ Log User Surf Website มีขั้นตอนคือ

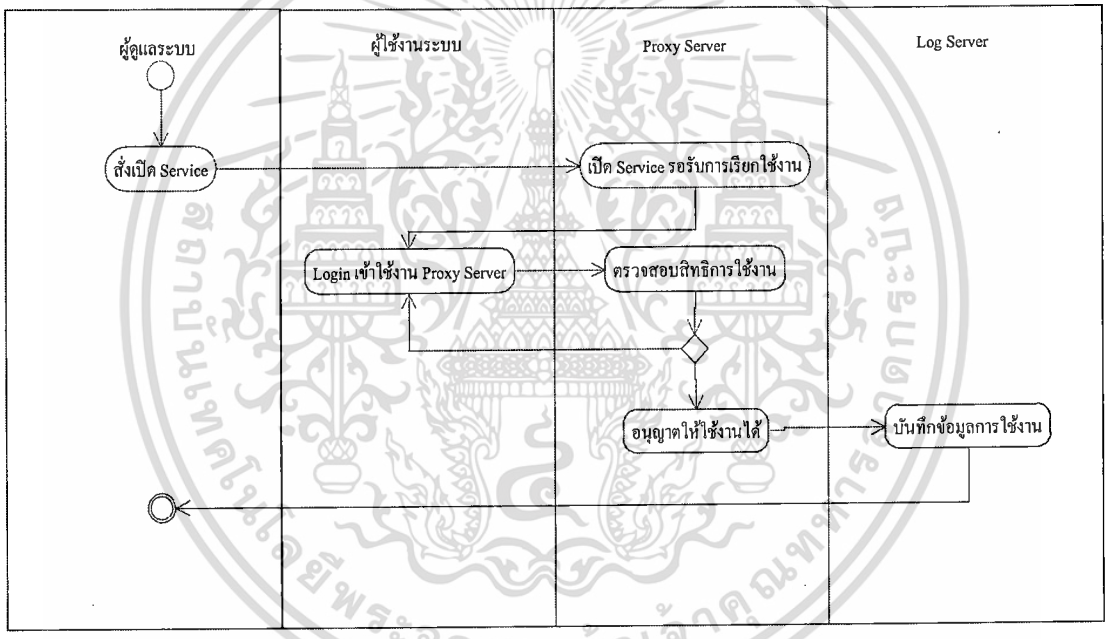
1. ผู้ดูแลระบบทำการเปิดฟังก์ชันการทำงานที่เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Proxy เพื่อรอรับการเชื่อมต่อเครือข่ายจากเครื่องคอมพิวเตอร์ผู้ใช้งาน

2. ผู้ใช้งานภายในเครือข่ายเปิดโปรแกรมเว็บเบราว์เซอร์ แล้วทำการ Login เข้าใช้งาน

3. เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Proxy ทำการตรวจสอบชื่อผู้ใช้งาน รหัสผ่าน สิทธิการใช้งานเมื่อข้อมูลถูกต้องจะอนุญาตให้ใช้งานระบบงานภายในผ่านเว็บเบราว์เซอร์ได้

4. เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Proxy ทำการบันทึกข้อมูลผู้ใช้งานในเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการสำหรับจัดเก็บข้อมูลผู้ใช้งาน

รายละเอียดขั้นตอนการทำงานของฟังก์ชัน Log User Surf Website แสดงในแอคทิวิตีไดอะแกรมดังรูปที่ 3.6



รูปที่ 3.6 แอคทีวิตีไดอะแกรมแสดงการทำงานของฟังก์ชัน Log User Surf Website

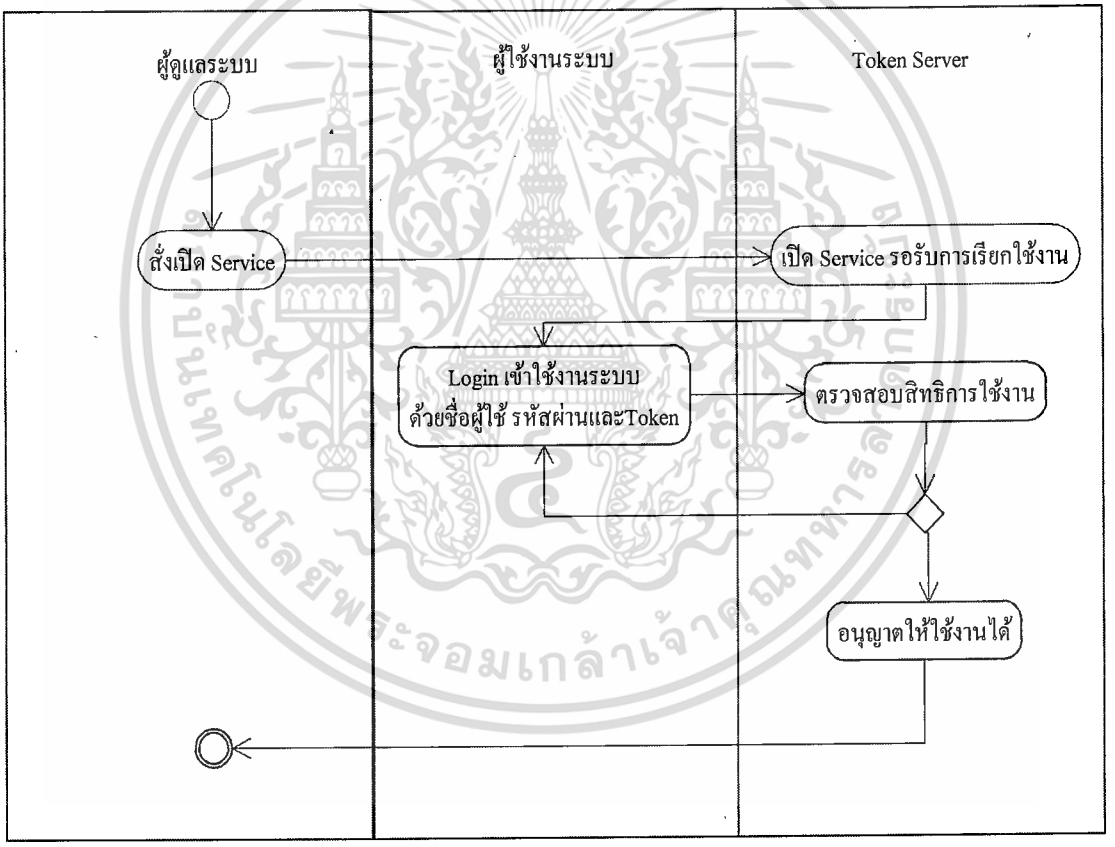
ฟังก์ชันการทำงานของ Authentication Token มีขั้นตอนคือ

1. ผู้ดูแลระบบทำการเปิดฟังก์ชันการทำงานที่เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Token เพื่อรอรับการเชื่อมต่อเครือข่ายจากเครื่องคอมพิวเตอร์ผู้ใช้งาน

2. ผู้ใช้งานระบบตรวจสอบการเชื่อมต่อระหว่างเครื่องคอมพิวเตอร์กับเครือข่ายอินเทอร์เน็ตหลังจากนั้นเปิดโปรแกรมเว็บเบราว์เซอร์แล้วทำการ Login เข้าใช้งาน

3. เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Token ทำการตรวจสอบชื่อผู้ใช้งาน รหัสผ่าน รหัส Token สิทธิการใช้งานเมื่อข้อมูลถูกต้องจะอนุญาตให้ใช้งานระบบงานภายในผ่านเว็บเบราว์เซอร์ได้

รายละเอียดขั้นตอนการทำงานของฟังก์ชัน Authentication Token แสดงในแอคทิวิตีไดอะแกรมดังรูปที่ 3.7



รูปที่ 3.7 แอคทิวิตีไดอะแกรมแสดงการทำงานของฟังก์ชัน Authentication Token

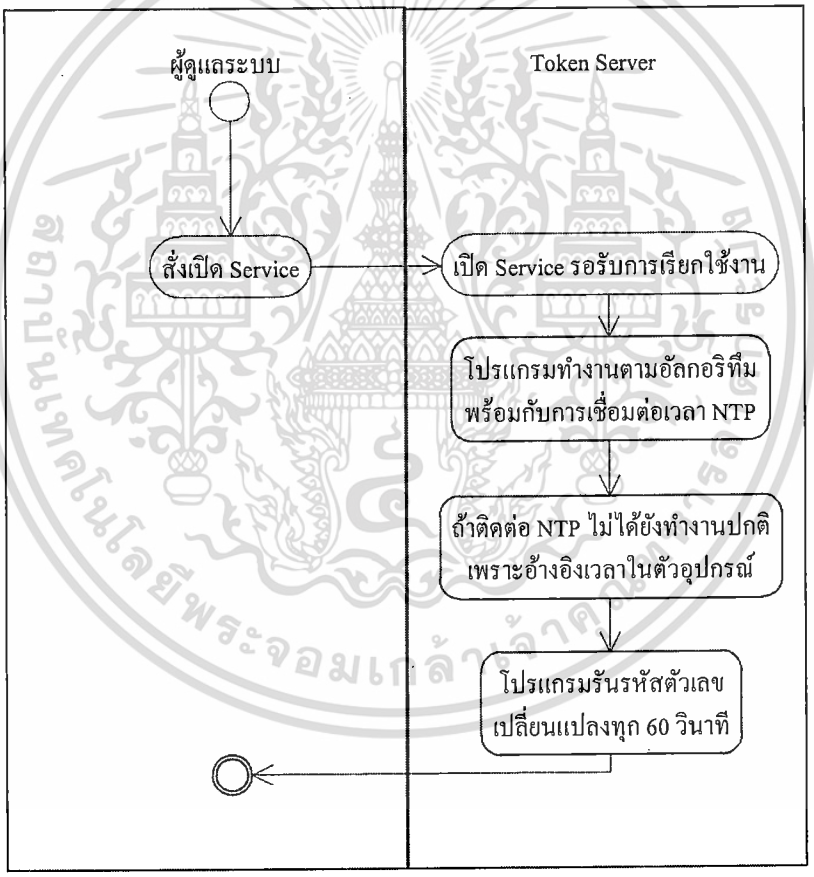
ฟังก์ชันการทำงานของ Generate Token Server มีขั้นตอนคือ

1. ผู้ดูแลระบบทำการเปิดฟังก์ชันการทำงานที่เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Token เพื่อรอรับการเชื่อมต่อเครือข่ายจากเครื่องคอมพิวเตอร์ผู้ใช้งาน

2. เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Token ทำการสร้างรหัสตัวเลขการอัลกอริทึม ซึ่งต้องเปลี่ยนแปลงชุดตัวเลขทุกๆ 60 วินาที

3. เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Token รอรับการเชื่อมต่อจากเครื่องผู้ใช้งาน เมื่อมีการ Login จะทำการตรวจสอบชื่อผู้ใช้งาน รหัสผ่าน รหัส Token สิทธิการใช้งานเมื่อข้อมูลถูกต้องจะอนุญาตให้ใช้งานระบบงานภายในผ่านเว็บเบราว์เซอร์ได้

รายละเอียดขั้นตอนการทำงานของฟังก์ชัน Generate Token Server แสดงในแอคทิวิตีไดอะแกรมดังรูปที่ 3.8



รูปที่ 3.8 แอคทีวิตีไดอะแกรมแสดงการทำงานของฟังก์ชัน Generate Token Server

ฟังก์ชันการทำงานของ Generate Token Android มีขั้นตอนคือ

1. ผู้ใช้งานระบบทำการเปิดแอพพลิเคชั่นที่เครื่องโทรศัพท์เคลื่อนที่สำหรับใช้งานเป็นอุปกรณ์ Token ในระบบปฏิบัติการแอนดรอยด์

2. Token แอนดรอยด์ทำการสร้างรหัสตัวเลขการอัลกอริทึมซึ่งต้องเปลี่ยนแปลงชุดตัวเลขทุกๆ 60 วินาที

3. ผู้ใช้งานทำการ Login ผ่านเว็บเบราว์เซอร์โดยใช้ชื่อผู้ใช้งาน รหัสผ่าน และรหัส Token หลังจากนั้นเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Token จะตรวจสอบความถูกต้องและสิทธิการใช้งานเมื่อข้อมูลถูกต้องจะอนุญาตให้ใช้งานระบบงานภายในผ่านเว็บเบราว์เซอร์ได้

รายละเอียดขั้นตอนการทำงานของฟังก์ชัน Generate Token Android แสดงในแอคทิวิตีไดอะแกรม ดังรูปที่ 3.9

รูปที่ 3.9 แอคทิวิตีไดอะแกรมแสดงการทำงานของฟังก์ชัน Generate Token Android

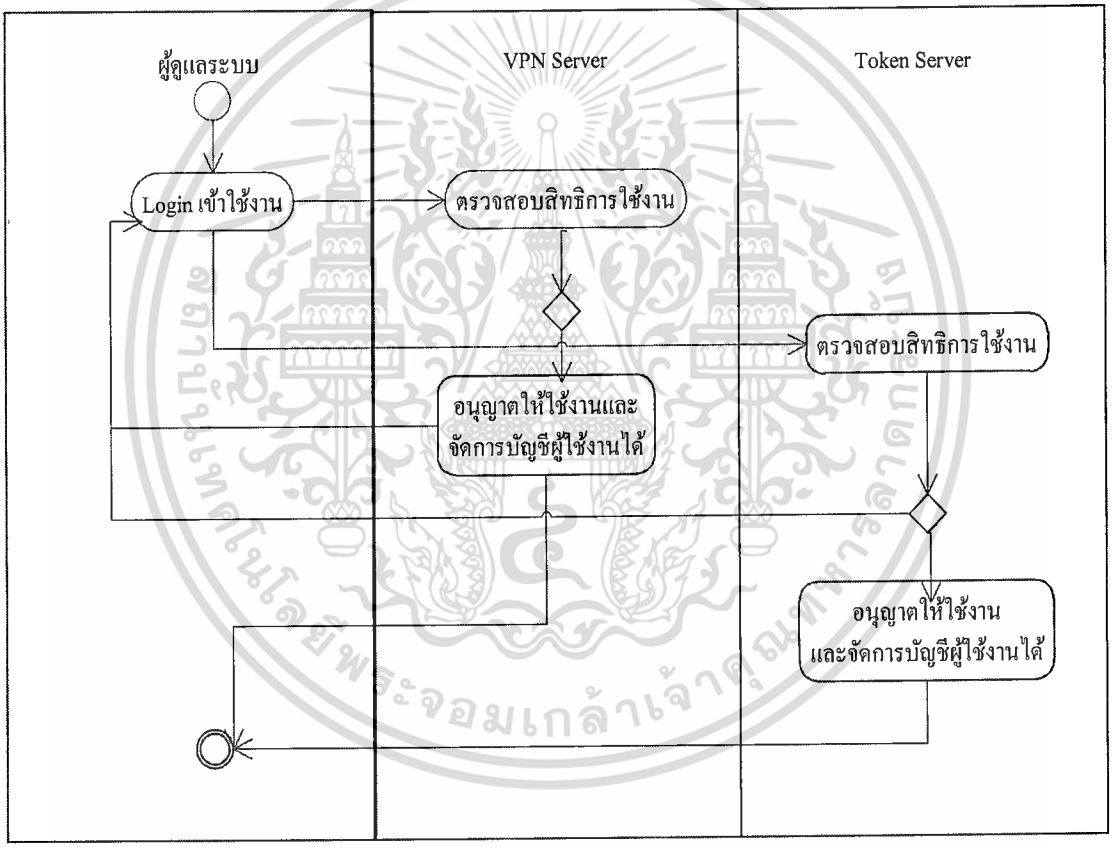
ฟังก์ชันการทำงานของ Login Control for Manage User Account and Policy มีขั้นตอนคือ

1. ผู้ดูแลระบบทำการ Login เข้าใช้งานเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ VPN และเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Token เพื่อบริหารจัดการระบบ

2. เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ VPN และเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Token ทำการตรวจสอบชื่อผู้ใช้งาน รหัสผ่าน สิทธิการใช้งานเมื่อข้อมูลถูกต้องจะอนุญาตให้ใช้งานระบบงานภายในผ่านเว็บเบราว์เซอร์ได้

3. ผู้ดูแลระบบทำการจัดการบัญชี และสิทธิผู้ใช้งานระบบได้

รายละเอียดขั้นตอนการทำงานของฟังก์ชัน Login Control for Manage User Account and Policy แสดงในแอคทิวิตีไดอะแกรมดังรูปที่ 3.10



รูปที่ 3.10 แอคทิวิตีไดอะแกรมแสดงการทำงานของฟังก์ชัน Login Control for Manage User Account and Policy

ฟังก์ชันการทำงานของ View Log User Token มีขั้นตอนคือ

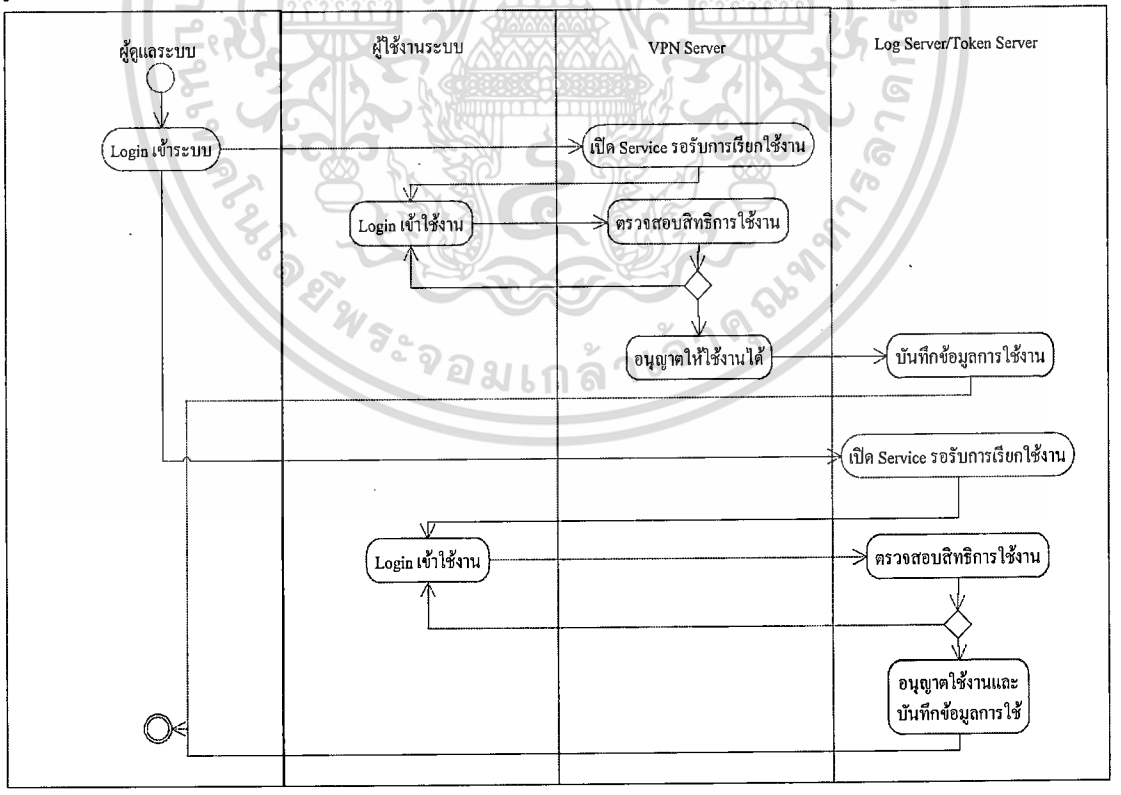
1. ผู้ดูแลระบบทำการ Login เข้าใช้งานเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ VPN และเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Token เพื่อบริหารจัดการระบบ

2. เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ VPN และเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Token ทำการตรวจสอบชื่อผู้ใช้งาน รหัสผ่าน สิทธิการใช้งานเมื่อข้อมูลถูกต้องจะอนุญาตให้ใช้งานระบบงานภายในผ่านเว็บเบราว์เซอร์ได้

3. ผู้ใช้ระบบทำการ Login เข้าใช้งานเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ VPN และเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Token เพื่อใช้งานระบบงานภายใน

4. เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ VPN และเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Token ทำการตรวจสอบชื่อผู้ใช้งาน รหัสผ่าน สิทธิการใช้งานเมื่อข้อมูลถูกต้องจะอนุญาตให้ใช้งานระบบงานภายในผ่านเว็บเบราว์เซอร์ได้

5. การใช้งานระบบผ่านเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ VPN และการใช้งานผ่านเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Token จะมีการบันทึกข้อมูลลงเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการสำหรับจัดเก็บข้อมูลผู้ใช้งานซึ่งสิทธิของผู้ดูแลระบบสามารถเรียกดูข้อมูลได้ รายละเอียดขั้นตอนการทำงานของฟังก์ชัน View Log User Token แสดงในแอคทิวิตีไดอะแกรมดังรูปที่ 3.11



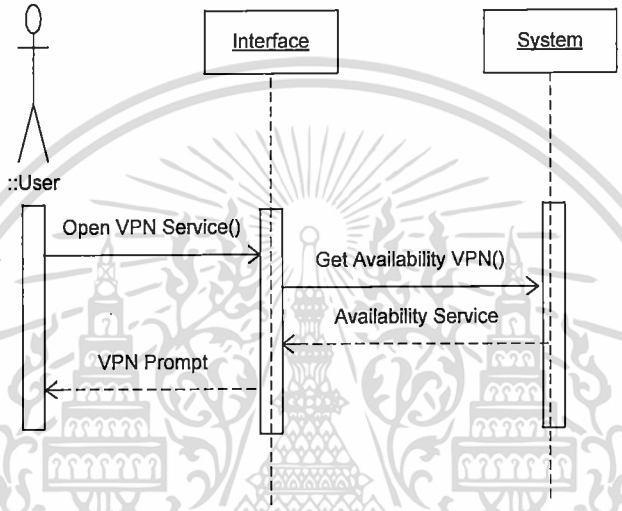
รูปที่ 3.11 แอคทิวิตีไดอะแกรมแสดงการทำงานของฟังก์ชัน View Log User Token

3.5 ซีเควนซ์ไดอะแกรม (Sequence Diagram)

ซีเควนซ์ไดอะแกรมเป็นแผนภาพสำหรับแสดงการปฏิสัมพันธ์กันระหว่างออบเจ็กต์ตามลำดับการทำงานของเหตุการณ์ที่เกิดขึ้น โดยแต่ละออบเจ็กต์จะถูกกระตุ้นให้ทำงานผ่านทางข้อความ ซึ่งได้อธิบายการทำงานทั้ง 11 ซีเควนซ์ไดอะแกรม ตามแต่ละยูสเคส ดังรูปที่ 3.12 – 3.22

1) VPN แสดงการทำงานเมื่อ ผู้ใช้งานระบบ ภายนอกจะทำการ VPN เข้าใช้งานระบบงานภายในองค์กร ผู้ใช้งานระบบเปิดฟังก์ชัน VPN ดังรูปที่ 3.12

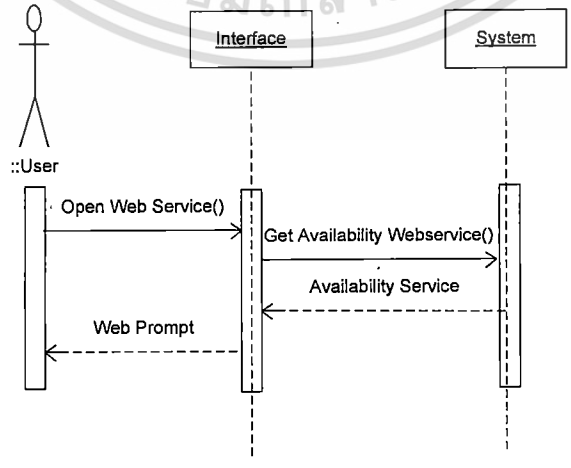
ผู้ดูแลระบบ ->Interface->System



รูปที่ 3.12 ซีเควนซ์ไดอะแกรมแสดงการทำงานของฟังก์ชัน VPN

2) Web Service แสดงการทำงานของเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการเว็บที่ทำการเปิดบริการรอรับการเชื่อมต่อจากผู้ใช้งาน โดยผู้ดูแลระบบเปิดฟังก์ชันเว็บ ดังรูปที่ 3.13

ผู้ดูแลระบบ ->Interface->System

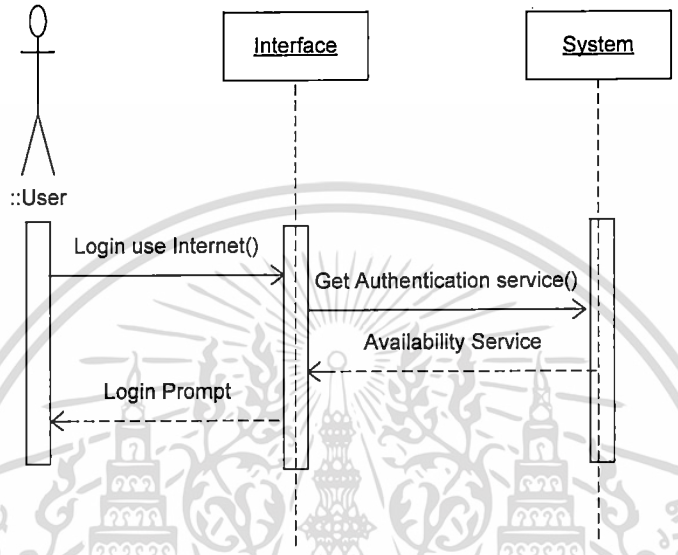


รูปที่ 3.13 ซีเควนซ์ไดอะแกรมแสดงการทำงานของฟังก์ชัน Web Service

3) Authentication Internet แสดงการทำงานของระบบที่ผู้ดูแลระบบทำการเปิดบริการส่วนสำหรับพิสูจน์ตันตนไว้เพื่อให้ผู้ใช้งานระบบภายในใช้ยืนยันตัวตนก่อนใช้งานอินเทอร์เน็ต ดังรูปที่ 3.14

ผู้ใช้งานระบบเปิดฟังก์ชันพิสูจน์ตัวตนก่อนการใช้งานอินเทอร์เน็ต

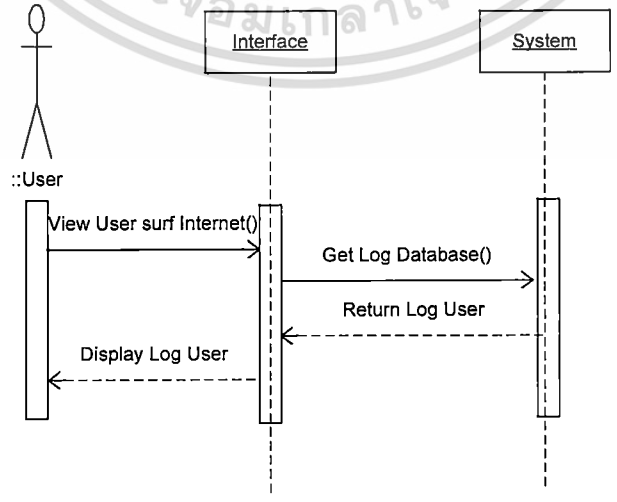
ผู้ดูแลระบบ ->Interface->System



รูปที่ 3.14 ซีเควนซ์ไดอะแกรมแสดงการทำงานของฟังก์ชัน Authentication Internet

4) Log User Surf Website แสดงระบบที่ผู้ดูแลระบบเปิดใช้บริการเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Proxy และมีการบันทึกข้อมูลการใช้งานเว็บไซต์ดังรูปที่ 3.15

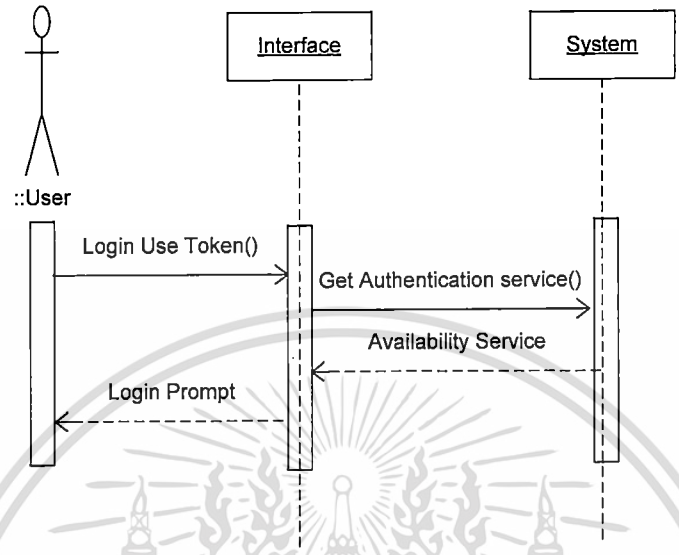
ผู้ดูแลระบบ ->Interface->System



รูปที่ 3.15 ซีเควนซ์ไดอะแกรมแสดงการทำงานของฟังก์ชัน Log User Surf Website

5) Authentication Token แสดงระบบที่ผู้ดูแลระบบทำการเปิดบริการ การยืนยันตัวตนด้วย Token ผู้ดูแลระบบเปิดฟังก์ชันพิสูจน์ตัวตนก่อนการใช้งานอินทราเน็ต ดังรูปที่ 3.16

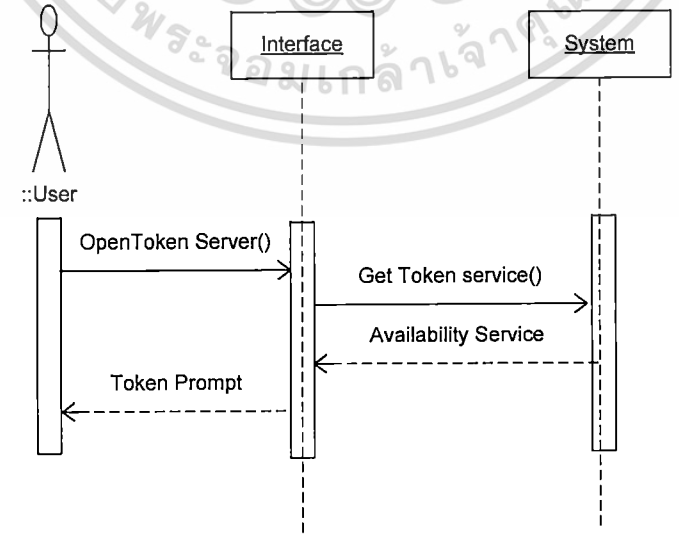
ผู้ดูแลระบบ ->Interface->System



รูปที่ 3.16 ซีเควนซ์ไดอะแกรมแสดงการทำงานของฟังก์ชัน Authentication Token

6) Generate Token Server แสดงระบบที่ผู้ดูแลระบบทำการเปิดบริการเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Token เพื่อรอรับการเชื่อมต่อจากผู้ใช้งาน โดยผู้ดูแลระบบเปิดฟังก์ชันการพิสูจน์ตัวตนด้วย Token ก่อนการใช้งานอินทราเน็ต ดังรูปที่ 3.17

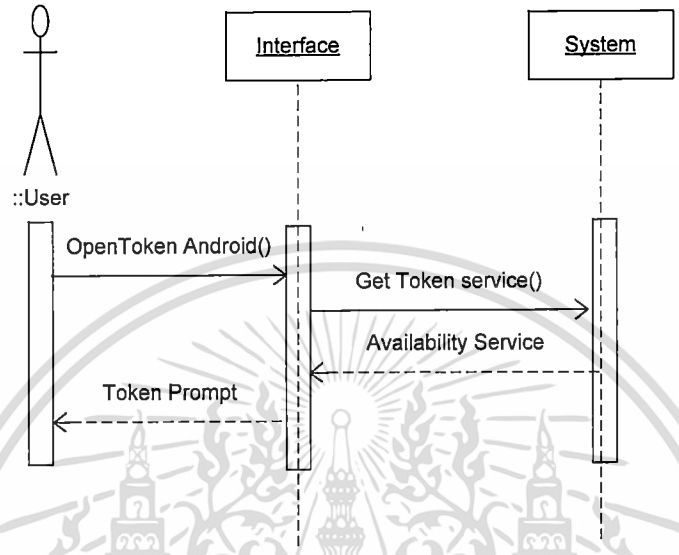
ผู้ดูแลระบบ ->Interface->System



รูปที่ 3.17 ซีเควนซ์ไดอะแกรมแสดงการทำงานของฟังก์ชัน Generate Token Server

7) Generate Token Android แสดงระบบที่ผู้ใช้งานระบบติดตั้งและใช้งานแอพพลิเคชัน Token บนระบบปฏิบัติการแอนดรอยด์ ซึ่งผู้ใช้งานระบบทำเปิดฟังก์ชันสร้างชุดรหัสตัวเลขในระบบปฏิบัติการแอนดรอยด์บนโทรศัพท์เคลื่อนที่ ดังรูปที่ 3.18

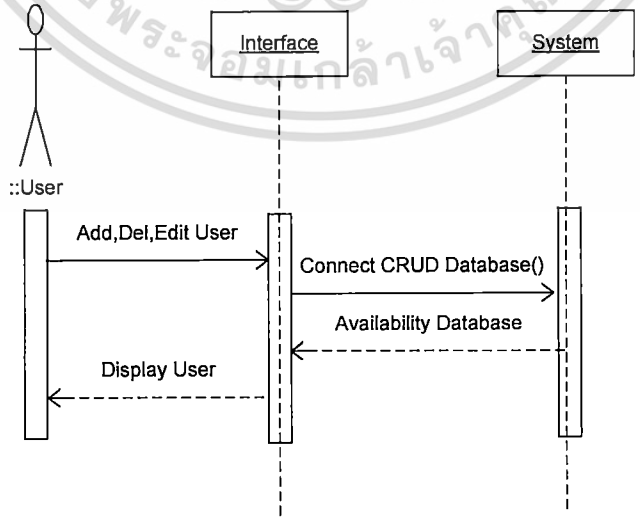
ผู้ดูแลระบบ ->Interface->System



รูปที่ 3.18 ซีเควนซ์ไดอะแกรมแสดงการทำงานของฟังก์ชัน Generate Token Android

8) Manage User Account แสดงระบบที่ผู้ดูแลระบบบริหารจัดการข้อมูลผู้ใช้งานระบบ ซึ่งติดตั้งในส่วนของ Pfsense และไมโครซอฟท์ วินโดวส์เอกซ์พี ดังรูปที่ 3.19

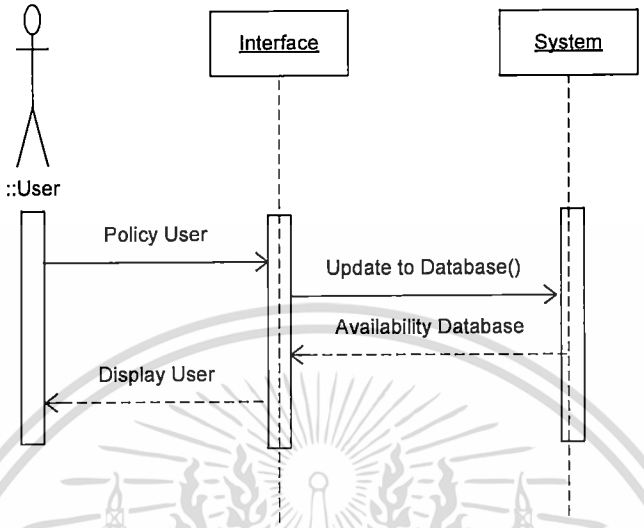
ผู้ดูแลระบบ ->Interface->System



รูปที่ 3.19 ซีเควนซ์ไดอะแกรมแสดงการทำงานของฟังก์ชัน Manage User Account

9) Manage User Policy แสดงระบบที่ผู้ดูแลระบบกำหนดสิทธิ ผู้ใช้งาน สำหรับการเข้าใช้งานระบบ ซึ่งติดตั้งในส่วนของ Pfsense และไมโครซอฟท์ วินโดวส์เอกซ์พี ดังรูปที่ 3.20

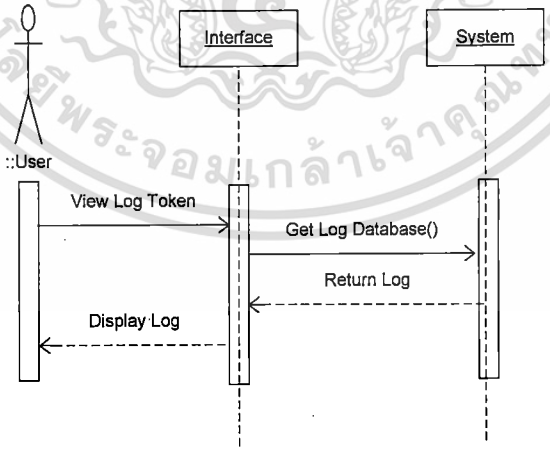
ผู้ดูแลระบบ ->Interface->System



รูปที่ 3.20 ซีเควนซ์ไดอะแกรมแสดงการทำงานของฟังก์ชัน Manage User Policy

10) View Log User Token แสดงระบบที่ผู้ดูแลระบบดูข้อมูลการเข้าใช้งานของผู้ใช้งานระบบ ซึ่งติดตั้งในส่วนของไมโครซอฟท์ วินโดวส์เอกซ์พี ดังรูปที่ 3.21

ผู้ดูแลระบบ ->Interface->System

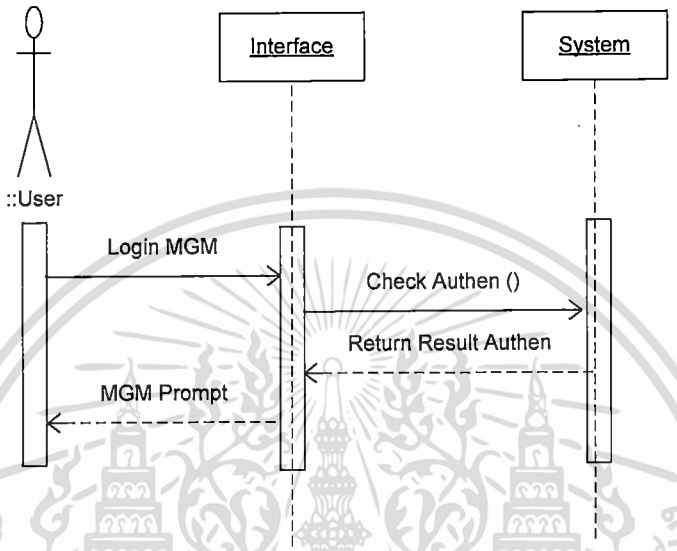


รูปที่ 3.21 ซีเควนซ์ไดอะแกรมแสดงการทำงานของฟังก์ชัน View Log User Token

11) Login Control แสดงระบบที่ ผู้ใช้งานระบบ ต้องมีการ Login ก่อนใช้งาน และผู้ดูแลระบบ เข้าสู่ระบบเพื่อจัดการข้อมูลผู้ใช้งานระบบในส่วนของการใช้งานอินเทอร์เน็ตและอินทราเน็ตที่จะต้องทำการ Login ก่อน ดังรูปที่ 3.22

ผู้ดูแลระบบ ->Interface->System

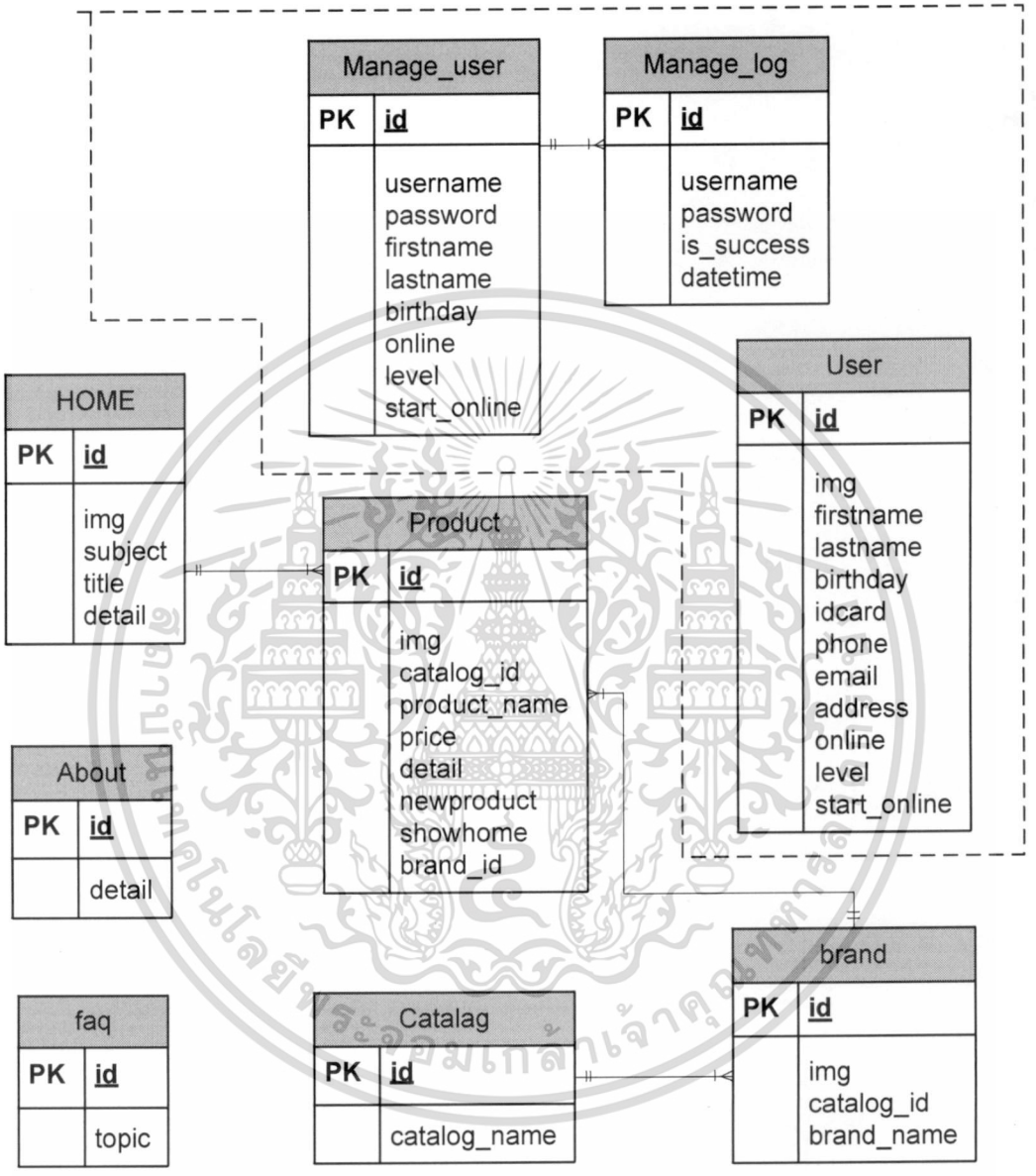
ผู้ใช้งานระบบ->Interface->System



รูปที่ 3.22 ซีเควนซ์ไดอะแกรมแสดงการทำงานของฟังก์ชัน Login Control

3.6 แผนภาพแสดงความสัมพันธ์ระหว่างเอนทิตี (E-R Diagram)

เอนทีตีที่อยู่ภายในกรอบเส้นประคือส่วนที่เป็นการพัฒนาเพิ่มเติมขึ้นเพื่อใช้ในการพิสูจน์ตัวตนและเอนทีติที่อยู่นอกเส้นประคือระบบสำหรับทดสอบซึ่งเป็นระบบของเดิมที่มีอยู่แล้ว ดังรูปที่ 3.23



รูปที่ 3.23 แผนภาพแสดงความสัมพันธ์ระหว่างเอนทิตี

พจนานุกรมข้อมูล (Data Dictionary)

พจนานุกรมข้อมูลแสดงการอธิบายรายละเอียดแอททริบิวต์ในตารางของฐานข้อมูลของระบบซึ่งประกอบไปด้วยชื่อแอททริบิวต์ คำอธิบาย ชนิดข้อมูล คีย์ และตารางอ้างอิง ตามตารางที่ 3.12 – 3.20

ตารางที่ 3.12 Manage_user ข้อมูลสำหรับจัดการผู้ใช้งานระบบ

ชื่อแอททริบิวต์	คำอธิบาย	ชนิดข้อมูล	คีย์	ตารางอ้างอิง
Id	รหัส	int	PK	
Username	ผู้ใช้งาน	varchar		
password	รหัสผ่าน	varchar		
firstname	ชื่อ	varchar		
lastname	นามสกุล	varchar		
birthday	วันเกิด	date		
Online	กำหนดเวลาออนไลน์	varchar		
Level	ระดับผู้ใช้งาน	int		
start_online	เวลาเริ่มออนไลน์	datetime		

ตารางที่ 3.13 Manage_log ข้อมูลสำหรับจัดการการใช้งานระบบ

ชื่อแอททริบิวต์	คำอธิบาย	ชนิดข้อมูล	คีย์	ตารางอ้างอิง
id	รหัส	int	PK	
Username	ผู้ใช้งาน	varbinary		
password	รหัสผ่าน	varchar		
is_success	สถานภาพการเข้าใช้งาน	int		
datetime	วันเวลาใช้งาน	datetime		

ตารางที่ 3.14 About คำอธิบายเกี่ยวกับเว็บไซต์

ชื่อแอททริบิวต์	คำอธิบาย	ชนิดข้อมูล	คีย์	ตารางอ้างอิง
Id	รหัส	int	PK	
Detail	รายละเอียด	text		

ตารางที่ 3.15 Brand กลุ่มแบรนด์ข้อมูลสินค้า

ชื่อแอททริบิวต์	คำอธิบาย	ชนิดข้อมูล	คีย์	ตารางอ้างอิง
Id	รหัส	int	PK	
Img	รูป	varchar		
catalog_id	รหัสแคตาล็อก	int		
brand_name	ชื่อแบรนด์	varchar		

ตารางที่ 3.16 Catalog กลุ่มแคตาล็อกสินค้า

ชื่อแอททริบิวต์	คำอธิบาย	ชนิดข้อมูล	คีย์	ตารางอ้างอิง
Id	รหัส	int	PK	
catalog_name	ชื่อแคตาล็อก	varchar		

ตารางที่ 3.17 Faq รายการคำถามคำตอบ

ชื่อแอททริบิวต์	คำอธิบาย	ชนิดข้อมูล	คีย์	ตารางอ้างอิง
Id	รหัส	int	PK	
Topic	ชื่อหัวข้อ	text		

ตารางที่ 3.18 Home หน้าหลักสำหรับแสดงผล

ชื่อแอททริบิวต์	คำอธิบาย	ชนิดข้อมูล	คีย์	ตารางอ้างอิง
Id	รหัส	int	PK	
Img	รูป	text		
subject	หัวข้อ	varchar		
Title	เรื่อง	varchar		
Detail	รายละเอียด	text		

ตารางที่ 3.19 Product ข้อมูลรายการสินค้า

ชื่อแอททริบิวต์	คำอธิบาย	ชนิดข้อมูล	คีย์	ตารางอ้างอิง
Id	รหัส	int	PK	
Img	รูป	varchar		
catalog_id	รหัสแคตาล็อก	int		
brand_id	รหัสแบรนด์	int		
product_name	ชื่อสินค้า	varchar		
Price	ราคา	varchar		
Detail	รายละเอียดสินค้า	text		
Newproduct	สินค้าใหม่	int		
Showtime	ตารางแสดงสินค้า	int		

ตารางที่ 3.20 User ข้อมูลผู้ใช้งานระบบ

ชื่อแอททริบิวต์	คำอธิบาย	ชนิดข้อมูล	คีย์	ตารางอ้างอิง
Id	รหัส	int	PK	
Img	รูป	varchar		
firstname	ชื่อ	varchar		
lastname	นามสกุล	varchar		
birthday	วันเกิด	date		
idcard	รหัสบัตร	varchar		
phone	เบอร์โทรศัพท์	varbinary		
email	เมล	varchar		
address	ที่อยู่	text		
online	ตรวจสอบการออนไลน์	varchar		
level	ระดับผู้ใช้งาน	int		
start_online	เวลาเริ่มออนไลน์	datetime		

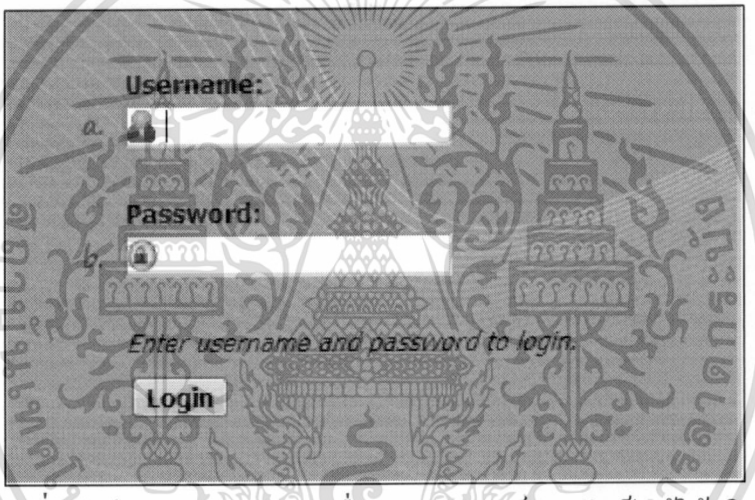
บทที่ 4
การจัดสร้างระบบ

4.1 การออกแบบหน้าจอการทำงาน

1) ผู้ดูแลระบบ Login เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ VPN โดยผู้ดูแลระบบทำการ Login เพื่อเข้าจัดการเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ VPN ซึ่งมีการติดตั้งฟังก์ชันสำหรับเป็นผู้ให้บริการ Proxy ไว้ในเครื่องเดียวกันด้วย ดังนั้นจะต้องทำการยืนยันตัวตนก่อนเข้าบริหารจัดการ ซึ่งได้มีการนำระบบโอเพนซอร์สเดิมมาช่วยในการพัฒนา ดังรูป 4.1

a) ลงชื่อเข้าใช้งานด้วยชื่อผู้ใช้

b) ใส่รหัสผ่านผู้ใช้งาน

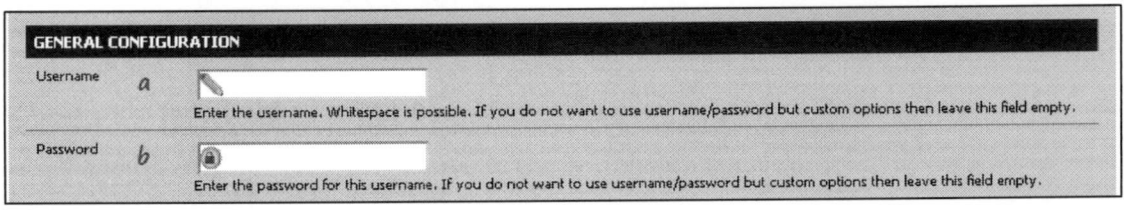


รูปที่ 4.1 ผู้ดูแลระบบ Login เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ VPN

2) ผู้ดูแลระบบ เพิ่มหรือแก้ไขข้อมูลผู้ใช้งานระบบในเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ VPN โดยผู้ดูแลระบบเข้าจัดการสร้าง แก้ไข ผู้ใช้งานระบบ ที่จะใช้งานระบบ VPN และ Proxy ซึ่งได้มีการนำระบบโอเพนซอร์สเดิมมาช่วยในการพัฒนา ดังรูป 4.2

a) สร้างบัญชีผู้ใช้งานระบบโดยกำหนดชื่อผู้ใช้งานไว้สำหรับในการ Login

b) กำหนดรหัสผ่านของบัญชีผู้ใช้งานระบบ



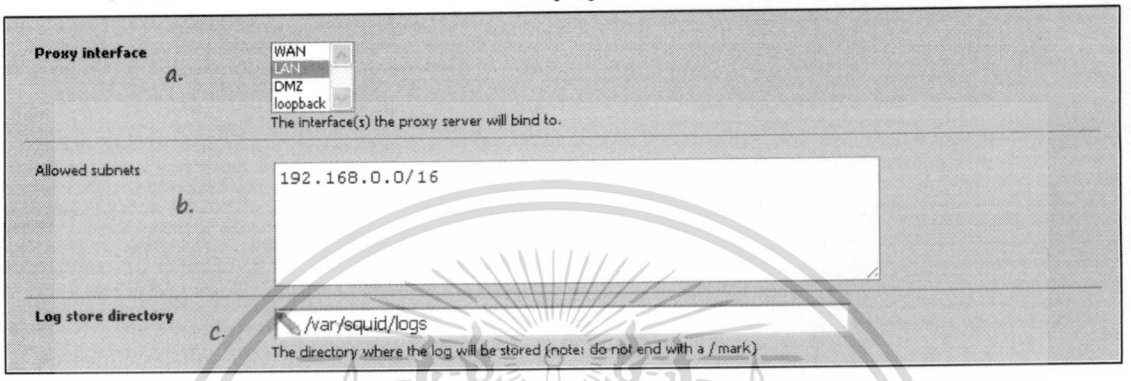
รูปที่ 4.2 เพิ่มผู้ใช้งาน VPN และ Proxy บัญชีผู้ใช้งานระบบ

3) ผู้ดูแลระบบตั้งค่าการทำงานของเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Proxy โดยผู้ดูแลระบบกำหนด IP Address กลุ่มของผู้ใช้งานสำหรับการใช้ Proxy ซึ่งได้มีการนำระบบโอเพนซอร์สเดิมมาช่วยในการพัฒนา ดังรูป 4.3

a) กำหนด Interface ของกลุ่มผู้ใช้งานที่จะเข้าใช้งาน Proxy

b) กำหนดช่วง IP Address ของเครื่องผู้ใช้งานที่จะทำการใช้งาน Proxy

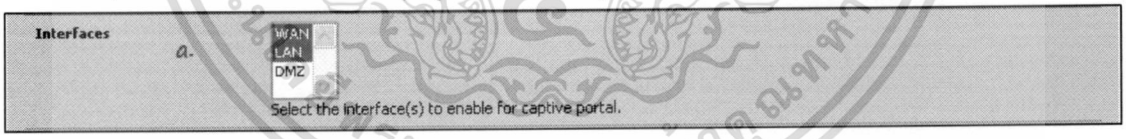
c) กำหนดตำแหน่งที่จะทำการบันทึกข้อมูลผู้ใช้งาน Proxy



รูปที่ 4.3 ตั้งค่าเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Proxy

4) ผู้ดูแลระบบตั้งค่าการพิสูจน์ตัวตน โดยกำหนด Interface เพื่อควบคุมกลุ่มผู้ใช้งานระบบก่อนใช้งานอินเทอร์เน็ตผ่าน Proxy ซึ่งได้มีการนำระบบโอเพนซอร์สเดิมมาช่วยในการพัฒนา ดังรูป 4.4

a) กำหนด Interface ของกลุ่มผู้ใช้งานที่จะพิสูจน์ตัวตนก่อนเข้าใช้งาน Proxy

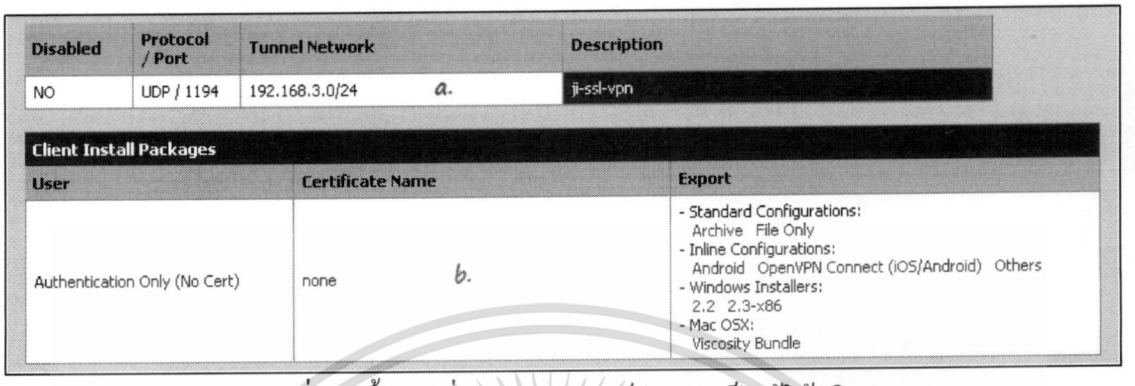


รูปที่ 4.4 ตั้งค่าการพิสูจน์ตัวตนก่อนการใช้งาน Proxy

5) ผู้ดูแลระบบตั้งค่าเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ VPN และสร้างโปรแกรม VPN สำหรับติดตั้งบนเครื่องคอมพิวเตอร์ผู้ใช้งานระบบภายนอก ซึ่งได้มีการนำระบบโอเพนซอร์สเดิมมาช่วยในการพัฒนา ดังรูป 4.5

a) กำหนดกลุ่ม IP Address ของคอมพิวเตอร์ภายนอกเมื่อทำการเชื่อมต่อผ่าน VPN แล้วจะได้ IP Address ตามที่เราได้ตั้งค่าไว้

b) สามารถเลือกโปรแกรม VPN สำหรับติดตั้งบนเครื่องลูกข่ายแล้วนำไปติดตั้งบนคอมพิวเตอร์ภายนอกเครือข่ายตามชนิดของระบบปฏิบัติการที่ใช้งานได้



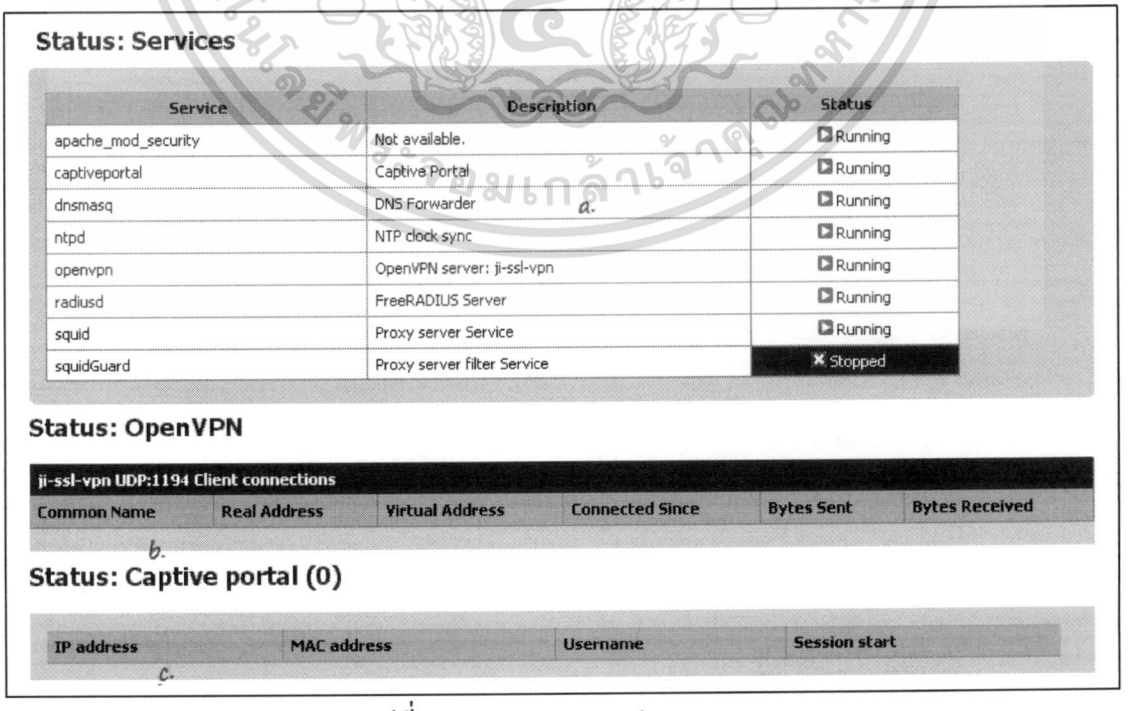
รูปที่ 4.5 ตั้งค่าเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ VPN

6) ผู้ดูแลระบบดูสถานภาพการทำงานของฟังก์ชันต่างๆ โดยเป็นหน้าต่างแสดงสถานการณ์ของการทำงานในแต่ละ Service ซึ่งได้มีการนำระบบโอเพนซอร์สเดิมมาช่วยในการพัฒนา ดังรูป 4.6

a) แสดงสถานภาพการทำงานของ Service ต่างๆ

b) แสดงสถานภาพเมื่อมีเครื่องคอมพิวเตอร์ผู้ใช้งานจากภายนอกเชื่อมต่อ VPN เข้ามาใช้งานระบบภายใน

c) แสดงสถานภาพเมื่อมีเครื่องคอมพิวเตอร์ผู้ใช้งานภายในใช้งานอินเทอร์เน็ตหรือระบบงานภายใน



รูปที่ 4.6 สถานภาพการทำงานของ Services

7) ผู้ดูแลระบบดูข้อมูลผู้ใช้งานภายในซึ่งเป็นการใช้งานอินเทอร์เน็ต จะทำการติดตั้งบนเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Token ซึ่งได้มีการนำระบบโอเพนซอร์สเดิมมาช่วยในการพัฒนา ดังรูป 4.7

a) แสดง IP Address ของเครื่องผู้ใช้งานภายในเครือข่าย วันเวลาที่ใช้งาน และเว็บไซต์ที่เข้าใช้บริการ เมื่อมีการใช้งานอินเทอร์เน็ต

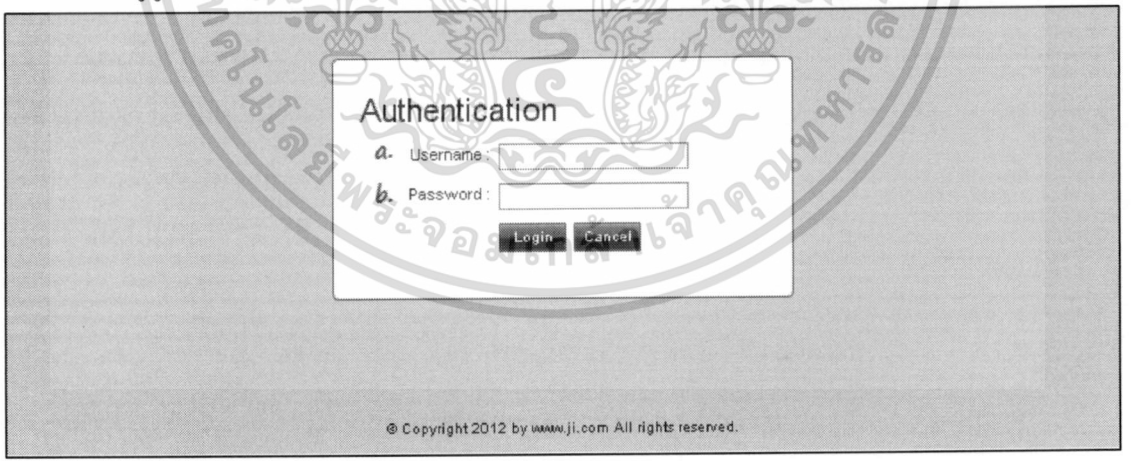
Received	Source IP	S.	F..	Severity	Timestamp	Tag	O. Message
7/28/2013 9:49:55.671 PM	192.168.2.99		l...	Info	Jul 28 13:39:33	pf	192.168.119.1.138 > 192.168.119.255.138: NBT UDP PACKET(138)
7/28/2013 9:51:53.765 PM	192.168.2.99		s...	Info	Jul 28 13:41:31	squid[39062]	192.168.1.2 - - [28/Jul/2013:13:41:31 +0000] "POST http://safebrowsing.clients.google.com
7/28/2013 9:51:53.765 PM	192.168.2.99		s...	Info	Jul 28 13:41:31	squid[39062]	a.
7/28/2013 9:51:53.984 PM	192.168.2.99		s...	Info	Jul 28 13:41:32	squid[39062]	192.168.1.2 - - [28/Jul/2013:13:41:32 +0000] "GET http://safebrowsing-cache.google.com/s
7/28/2013 9:51:53.984 PM	192.168.2.99		s...	Info	Jul 28 13:41:32	squid[39062]	
7/28/2013 9:51:54.093 PM	192.168.2.99		s...	Info	Jul 28 13:41:32	squid[39062]	192.168.1.2 - - [28/Jul/2013:13:41:32 +0000] "GET http://safebrowsing-cache.google.com/s
7/28/2013 9:51:54.093 PM	192.168.2.99		s...	Info	Jul 28 13:41:32	squid[39062]	
7/28/2013 9:51:54.171 PM	192.168.2.99		s...	Info	Jul 28 13:41:32	squid[39062]	192.168.1.2 - - [28/Jul/2013:13:41:32 +0000] "GET http://safebrowsing-cache.google.com/s
7/28/2013 9:51:54.171 PM	192.168.2.99		s...	Info	Jul 28 13:41:32	squid[39062]	
7/28/2013 9:51:54.265 PM	192.168.2.99		s...	Info	Jul 28 13:41:32	squid[39062]	192.168.1.2 - - [28/Jul/2013:13:41:32 +0000] "GET http://safebrowsing-cache.google.com/s
7/28/2013 9:51:54.265 PM	192.168.2.99		s...	Info	Jul 28 13:41:32	squid[39062]	
7/28/2013 9:51:54.390 PM	192.168.2.99		s...	Info	Jul 28 13:41:32	squid[39062]	192.168.1.2 - - [28/Jul/2013:13:41:32 +0000] "GET http://safebrowsing-cache.google.com/s

รูปที่ 4.7 ข้อมูลผู้ใช้งานเว็บไซต์

8) ผู้ดูแลระบบ Login เพื่อจัดการเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการเว็บและเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Token ซึ่งติดตั้งบนเครื่องเดียวกันบนระบบปฏิบัติการไมโครซอฟท์ วินโดวส์เอกซ์พี ดังรูป 4.8

a) ผู้ดูแลระบบใส่ชื่อผู้ใช้งานเพื่อยืนยันตัวตนก่อนเข้าใช้งานระบบ

b) ผู้ดูแลระบบใส่รหัสผ่านเพื่อยืนยันตัวตนก่อนเข้าใช้งานระบบ



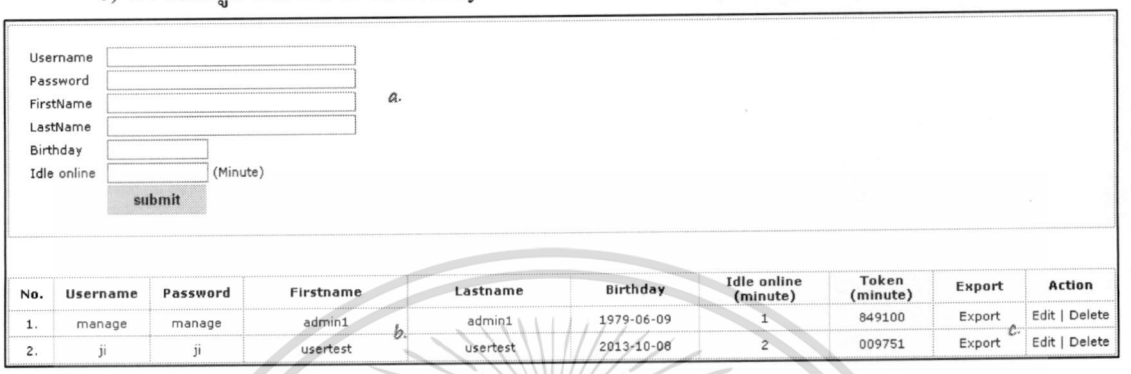
รูปที่ 4.8 ผู้ดูแลระบบ Login สำหรับจัดการเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Token

9) ผู้ดูแลระบบบริหารจัดการเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Token โดยผู้ดูแลระบบจัดการสร้างและกำหนดระยะเวลาใช้งานระบบของผู้ใช้งานได้ ดังรูป 4.9

a) สร้างข้อมูลบัญชีผู้ใช้งานโดยกำหนดข้อมูลต่างๆของผู้ใช้งานระบบสำหรับใช้ Token

b) เมื่อสร้างบัญชีผู้ใช้งานเสร็จแล้วจะแสดงตารางข้อมูลผู้ใช้งานตามรูป

c) สร้างเมนูสำหรับส่งออกค่า Key เพื่อใช้สร้างรหัสสำหรับแอพพลิเคชันบนแอนดรอยด์



รูปที่ 4.9 ผู้ดูแลระบบใช้งานเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Token

10) ผู้ใช้งานระบบ Login ด้วย ชื่อผู้ใช้งาน รหัสผ่าน และ Token ซึ่งหน้า Login การเข้าใช้งานระบบสำหรับผู้ใช้งานที่จะทำการเชื่อมต่อเข้าสู่ระบบงานภายในดังรูป 4.10

a) ก่อนการเข้าใช้งานผ่าน เว็บเบราว์เซอร์ให้พิมพ์โพรโตคอล HTTPS ด้วย

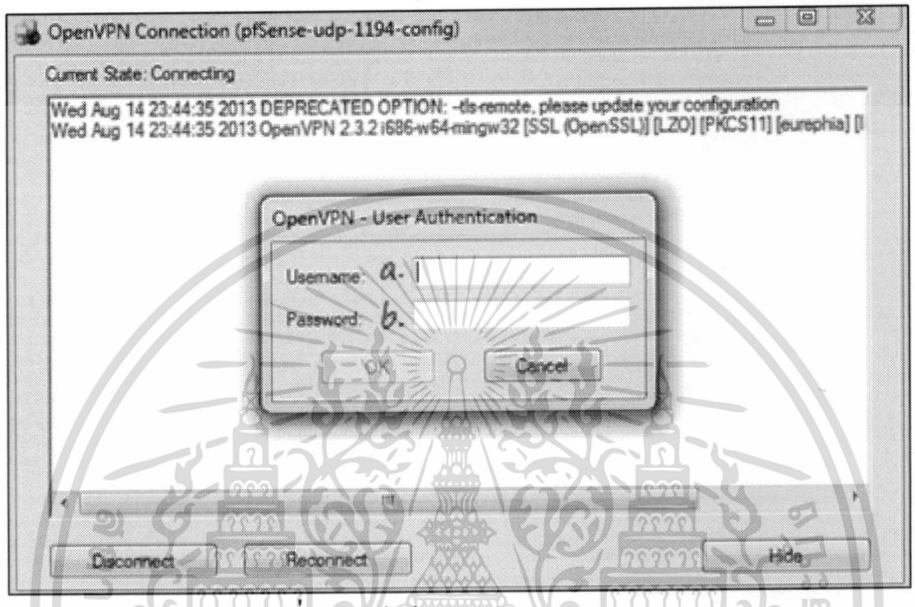
b) กำหนดช่องสำหรับใส่ ชื่อผู้ใช้งาน รหัสผ่าน และ Token Key ก่อนเข้าใช้งานระบบงานภายใน

รูปที่ 4.10 ผู้ใช้งานระบบ Login เว็บเบราว์เซอร์พร้อม Token

11) ผู้ใช้งานภายนอก Login VPN เป็นส่วนแสดงโปรแกรม VPN ของเครื่องลูกข่ายที่ผู้ใช้งานระบบต้องทำการพิสูจน์ตัวตนก่อนเชื่อมต่อเครือข่ายภายใน ซึ่งได้มีการนำระบบโอเพนซอร์สเดิมมาช่วยในการพัฒนา ดังรูป 4.11

a) แสดงหน้า Login ของโปรแกรม VPN ที่เครื่องลูกข่ายเมื่อผู้ใช้งานระบบภายนอกเครือข่ายจะทำการเชื่อมต่อกับเครือข่ายภายใน

b) แสดงช่องสำหรับใส่รหัสผ่านของผู้ใช้งานภายนอก

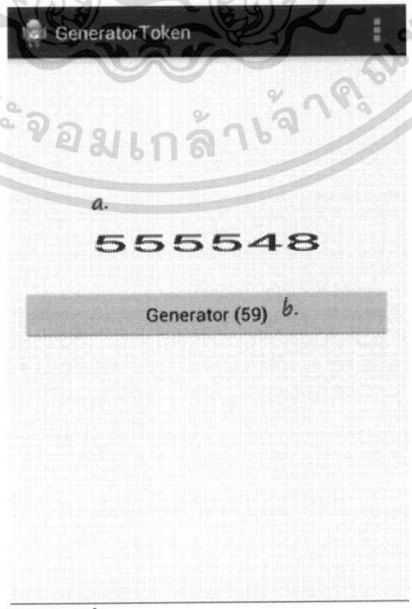


รูปที่ 4.11 ผู้ใช้งานระบบภายนอก Login VPN

12) Token ที่เป็นแอพพลิเคชันบนระบบปฏิบัติการแอนดรอยด์ ดังรูป 4.12

a) แสดงรหัสตัวเลข 6 ตัว ที่จะใช้ทำการเป็นตัวประกอบที่ 2 ในระบบการพิสูจน์ตัวตน

b) แสดงเวลาที่จะนับถอยหลังทุก 60 วินาทีและทำการเปลี่ยนรหัสตัวเลข



รูปที่ 4.12 แอนดรอยด์ Token

4.2 การพัฒนาระบบ (System Development)

ทำการติดตั้งฟังก์ชันการทำงานต่างๆ ตามรายการด้านล่าง ดังนี้

1) ติดตั้งระบบปฏิบัติการ Pfsense เพื่อสร้างระบบพิสูจน์ตัวตนด้วย Token ในส่วนของ VPN เพื่อเชื่อมต่อเครือข่าย และ Proxy สำหรับการใช้งานอินเทอร์เน็ต เราได้ทำการพัฒนาบนระบบปฏิบัติการ Pfsense

2) ติดตั้งฟังก์ชัน Open VPN วิธีการลงดูในภาคผนวก

3) ติดตั้งฟังก์ชันพิสูจน์ตัวตน วิธีการลงดูในภาคผนวก

4) ติดตั้งฟังก์ชัน Proxy วิธีการลงดูในภาคผนวก

5) ติดตั้งฟังก์ชัน Free Radius วิธีการลงดูในภาคผนวก

6) ติดตั้งไมโครซอฟท์ วินโดวส์เอกซ์พีในการสร้างระบบพิสูจน์ตัวตนด้วย Token และทำหน้าที่เป็นเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการเว็บด้วย โดยเป็นลักษณะเว็บอินทราเน็ตและต้องทำการลงโปรแกรมซิงโครนัสเวลากับ NTP ด้วย

7) ติดตั้งฟังก์ชันเว็บคือ Apache & Mod SSL และ PHP โดยทำการลงโปรแกรมที่เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการเว็บซึ่งทำการติดตั้งบนระบบปฏิบัติการไมโครซอฟท์ วินโดวส์เอกซ์พีที่มีระบบพิสูจน์ตัวตนด้วย Token ด้วย โดยใช้โอเพนซอร์ส Appserv 2.5.9

8) ติดตั้งฐานข้อมูล MySQL โดยลงฐานข้อมูล MySQL และทำการสร้างฐานข้อมูลที่เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการเว็บซึ่งเป็นส่วนของไมโครซอฟท์ วินโดวส์เอกซ์พีที่มีระบบพิสูจน์ตัวตนด้วย Token โดยใช้โอเพนซอร์ส Appserv 2.5.9

9) ติดตั้งฟังก์ชันสร้างชุดรหัสตัวเลขโดยติดตั้งในส่วนของเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Token ที่สร้างชุดรหัสตัวเลขโดยใช้ PHP และ MySQL ในการเก็บข้อมูลการนำไปใช้ให้วางในส่วนของเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการเว็บซึ่งการทำงานเราได้พัฒนาบนเครื่องคอมพิวเตอร์เดียวกัน และนำไปใช้งานร่วมกับ Apache SSL เพื่อใช้งานผ่านโพรโตคอล HTTPS

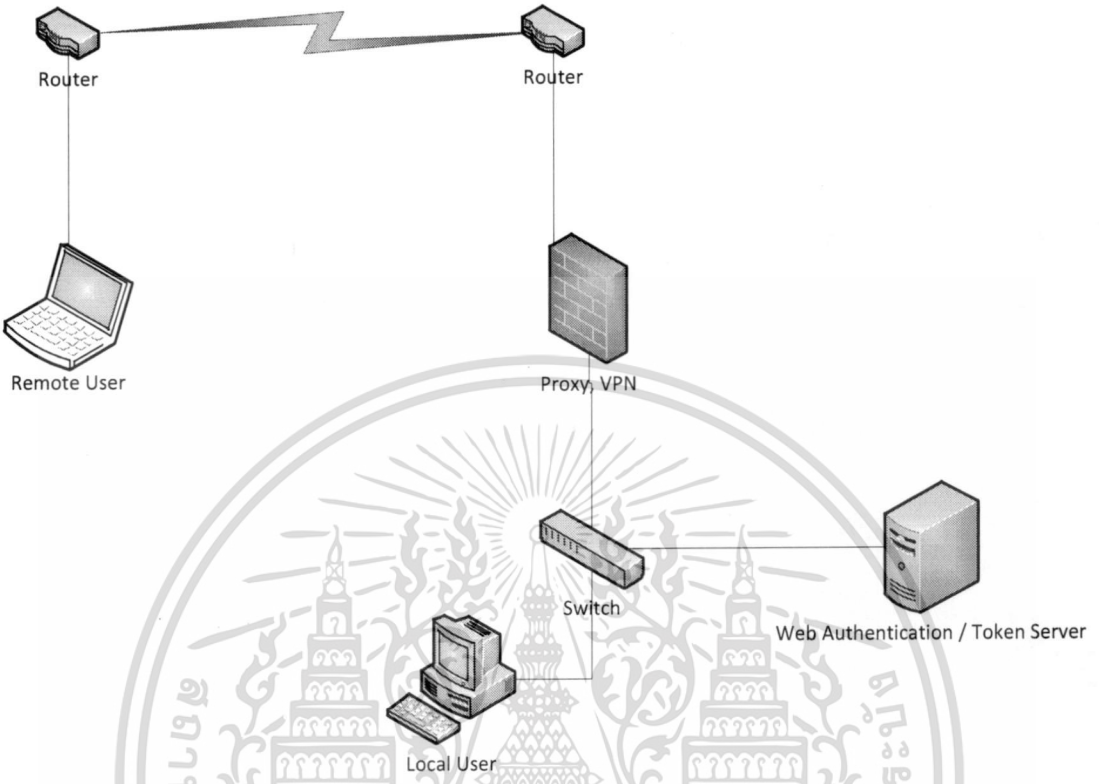
10) สร้าง Token หรือซอฟต์แวร์แอพพลิเคชันบนระบบปฏิบัติการแอนดรอยด์ ซึ่งได้พัฒนาและทดลองใช้กับแอนดรอยด์ 4.2 Jelly Bean และต้องทำการลงแอพพลิเคชันเพื่อซิงโครนัสเวลากับ NTP ด้วย

11) ผู้ดูแลระบบทำการตั้งค่าการใช้งานโดย Login สำหรับจัดการเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ VPN และเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Proxy ให้ใช้งานผ่านเว็บเบราว์เซอร์และทำการตั้งค่าฟังก์ชันบัญชีผู้ใช้งาน โดยไปที่ Menu: Service -> Free Radius โดยสามารถเข้าไป สร้าง ลบ แก้ไข ผู้ใช้งานระบบ สำหรับการใช้งานส่วนของอินเทอร์เน็ต และ VPN

12) เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Token และ เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการเว็บ สามารถใช้งานผ่านเว็บเบราว์เซอร์และทำการยืนยันตัวตนก่อนเข้าทำการตั้งค่าจึงจะ

สามารถเพิ่ม ลบ แก้ไข และส่งออกค่ารหัสเพื่อนำไปใช้ในการสร้างชุดรหัสตัวเลขบนระบบปฏิบัติการแอนดรอยด์ได้

13) เชื่อมต่อ Network แสดงแผนภาพการเชื่อมต่ออุปกรณ์กับระบบเครือข่าย



รูปที่ 4.13 แผนผังแสดงการเชื่อมต่อเครือข่าย (Network Diagram)

4.3 การทดสอบระบบ

ในการทดสอบระบบ Token ได้ทำการใช้งานระบบโดยโปรแกรมสามารถทำงานทั้งในส่วนเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการและส่วนที่ติดตั้งในระบบปฏิบัติการแอนดรอยด์บนโทรศัพท์เคลื่อนที่ให้ทำการสร้างชุดรหัสตัวเลข 6 หลักโดยมีเวลาเข้ามาเกี่ยวข้องคือ โปรแกรมจะทำงานไปเรื่อยๆ โดยเปลี่ยนแปลงค่าทุกๆ 60 วินาที ในการซิงโครนัสรหัสตัวเลขจะใช้เวลาอ้างอิงเหมือนกันในที่นี้ใช้การเชื่อมต่อกับเวลาทางอินเทอร์เน็ตตัวเดียวกัน ซึ่งจากการทดสอบรหัสตัวเลขระหว่างระบบปฏิบัติการแอนดรอยด์บนโทรศัพท์เคลื่อนที่กับเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการรหัสตรงกันแม้ในบางช่วงเวลาจะไม่ได้เชื่อมต่อกับเวลาทางอินเทอร์เน็ต ซึ่งเมื่อเปรียบเทียบกับระบบที่ขายอยู่ตามท้องตลาดคือระบบอาร์เอสเอที่ต้องใช้อุปกรณ์ฮาร์ดแวร์ SecurID Token ทำการสร้างชุดรหัสตัวเลขทุกๆ 60 วินาที เพื่อที่จะซิงโครนัสกับเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการอาร์เอสเอ อีกทั้งจำเป็นต้องมีการลงทุนค่าเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการอาร์เอสเอ อุปกรณ์ฮาร์ดแวร์อาร์เอสเอ SecurID Token และ Radius Server เพื่อสนับสนุนการทำงานของระบบด้วย ระบบสามารถทำงานได้เหมือนกันจะต่างกันที่อัลกอริทึมที่ใช้ซึ่งอาร์เอสเอมี

อัลกอริทึมเฉพาะเป็นความลับขององค์กร ส่วนระบบที่พัฒนาใช้การเข้ารหัสแบบ MD5 และ ASCHII Code มาช่วยในการสร้างอัลกอริทึมและโปรแกรมของระบบ

ตารางที่ 4.1 แสดงการเปรียบเทียบและประสิทธิภาพของระบบ

เรื่อง	2 Factor Authentication with Token	อาร์เอสเอ Token
ฐานข้อมูลผู้ใช้งาน	MySQL เป็นโอเพนซอร์สซึ่งสามารถรองรับปรับเปลี่ยนได้ง่าย	Radius ต้องทำการติดตั้งเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการสำหรับจัดการ นิยมใช้งานกับฐานข้อมูลผู้ใช้งานทั้งขนาดเล็กและใหญ่ขึ้นอยู่กับการออกแบบและราคาจะแพงตามไปด้วย
การใช้งาน	พัฒนาให้ใช้กับเว็บเบราว์เซอร์	รองรับการใช้งานเว็บเบราว์เซอร์ได้
ความเที่ยงตรงในการสร้างชุดรหัสตัวเลข	ขึ้นอยู่กับอุปกรณ์ปลายทางเนื่องจาก Token ที่สร้างขึ้นนั้นเป็นซอฟต์แวร์บนระบบปฏิบัติการแอนดรอยด์จะต้องทำการซิงโครนัสกับเวลาทางอินเทอร์เน็ตใหม่ถ้ามีการตั้งค่าเวลาบนอุปกรณ์เอง	ถูกต้องน่าเชื่อถือ การใช้งานมีประสิทธิภาพสูงและรับประกันจากผู้ผลิต
อัลกอริทึมและความปลอดภัยของระบบ	MD5 และประยุกต์ใช้ ASCHII Code ช่วยในการพัฒนาระบบ ซึ่งมีความปลอดภัยสูง	ใช้การเข้ารหัสและถอดรหัสอาร์เอสเอและใช้อัลกอริทึมเฉพาะเป็นความลับของผู้ผลิต
ความสะดวกในการใช้งาน	ใช้งานง่ายรองรับอุปกรณ์การทำงานที่หลากหลายเนื่องจากเป็นซอฟต์แวร์ Token	ราคาแพง ต้องใช้งานและติดตั้งตามระบบที่ผู้ผลิตจำหน่ายให้

ในการนำ Open VPN ซึ่งเป็นโปรแกรมโอเพนซอร์สที่มีการใช้งานอย่างแพร่หลาย และมีการใช้ SSL เพื่อเพิ่มความปลอดภัยจำเป็นต้องทำการลงซอฟต์แวร์ VPN บนเครื่องลูกข่ายทในเครื่องคอมพิวเตอร์ปลายทางที่จะทำการเชื่อมต่อกับเครือข่ายภายในผ่านเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ VPN นั้นระบบมีความปลอดภัยในการใช้งานแต่ยุ่งยากในการใช้งานกว่าแบบ SSL เว็บเบราว์เซอร์ VPN ที่ใช้งานผ่านเว็บไซต์โดยตรงเนื่องจากไม่ต้องทำการลงโปรแกรมที่เครื่องคอมพิวเตอร์ปลายทาง ส่วนการเปรียบเทียบกับ Cisco ASA ซึ่งมีการใช้งานแบบ IPSec VPN ที่มีความปลอดภัยและประสิทธิภาพสูงแต่จำเป็นต้องซื้ออุปกรณ์ที่ราคาสูงและเหมาะสมในการใช้งานแบบการเชื่อมต่อเครือข่ายส่วนตัวระหว่างองค์กรกับองค์กร

บทที่ 5
สรุปผลการพัฒนาโครงการและข้อเสนอแนะ

5.1 สรุปโครงการพัฒนาระบบงาน

1) มีระบบ Two Factor Authentication ที่สามารถนำมาใช้งานในองค์กรโดยพัฒนาในลักษณะคอมพิวเตอร์ที่ให้บริการผ่านทางเว็บไซต์ที่จะต้องทำการใส่ชื่อผู้ใช้ รหัสผ่านก่อนเพื่อยืนยันตัวตนก่อนเข้าใช้งานระบบพร้อมกับเพิ่ม Token ซึ่งพัฒนาบนระบบปฏิบัติการแอนดรอยด์เข้ามาเป็นอีกตัวประกอบในการยืนยันตัวตน

2) ระบบมีขั้นตอนการพิสูจน์ตัวตนที่มากขึ้นจึงมีความปลอดภัยสำหรับระบบที่มากขึ้น เพราะเพียงแค่ชื่อผู้ใช้และรหัสผ่านสามารถถูกขโมยได้และเรานำ Token ซึ่งเป็นการสร้างซอฟต์แวร์ที่สะดวกและยืดหยุ่นต่อการใช้งานในระบบปฏิบัติการแอนดรอยด์บนโทรศัพท์เคลื่อนที่ ส่วนเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Token ได้พัฒนาโปรแกรมและใช้อัลกอริทึม MD5 ช่วยในการสร้างดังนั้นแม้จะถูกขโมยชื่อผู้ใช้ หรือรหัสผ่านไป ก็จะไม่สามารถเข้าใช้งานระบบได้

3) ได้ทำการศึกษาการสร้างเครือข่ายเสมือนเพื่อเชื่อมต่อระหว่างเครือข่ายสาธารณะที่มีการใช้งานอยู่ต่างสถานที่กับระบบเครือข่ายภายในองค์กรที่มีระบบงานภายในเมื่อพนักงานองค์กรจะใช้งานจะต้องทำการเชื่อมต่อ VPN ก่อนเพื่อเพิ่มระบบความปลอดภัยในการใช้งาน โดยได้มีการนำโอเพนซอร์ส Open VPN มาช่วยในการพัฒนาระบบขึ้น

5.2 ผลการดำเนินการพัฒนาระบบ

1) สามารถนำระบบ Two Factor Authentication ไปใช้งานผ่านเว็บเบราว์เซอร์และมีส่วนประกอบต่างๆในระบบคือ ระบบจัดเก็บข้อมูลผู้ใช้งานระบบเว็บอินทราเน็ต ระบบ Proxy ระบบพิสูจน์ตัวตนด้วย Token ระบบ VPN และมีการเพิ่มความปลอดภัยผ่านเว็บไซต์ด้วยโพรโตรคอล HTTPS

2) มีระบบ Two Factor Authentication สามารถนำไปใช้กับหน่วยงานต่างๆได้ ค่าใช้จ่ายในการดำเนินการติดตั้งและลงทุนในตัวอุปกรณ์ถูกเมื่อเปรียบเทียบกับระบบที่มีขายตามท้องตลาด

3) ระบบที่ได้พัฒนาขึ้นสามารถบริหารจัดการบัญชีผู้ใช้งานระบบและมี Token ซึ่งเป็นแอพพลิเคชันในระบบปฏิบัติการแอนดรอยด์ที่สามารถนำไปติดตั้งกับอุปกรณ์ฮาร์ดแวร์ที่หลากหลายได้

5.3 ข้อจำกัดและข้อเสนอแนะ

ในการพัฒนาระบบมีองค์ประกอบที่เกี่ยวข้องมากเนื่องจากเป็นการสร้างที่เกี่ยวข้องกับระบบเครือข่ายเน็ตเวิร์ค จึงต้องมีความรู้ทางด้านเน็ตเวิร์คและระบบปฏิบัติการต่างๆพอสมควร สำหรับการสร้าง Token ที่เป็นลักษณะแอพพลิเคชันบนระบบปฏิบัติการแอนดรอยด์นั้นมีข้อจำกัด

ในเรื่องข้องค่าชุดรหัสตัวเลขทั้งในส่วนของเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการและ Token ให้ตรงกันเนื่องจากติดตั้งอยู่ต่างสถานที่จึงจำเป็นต้องติดตั้งการซิงโครนัสเวลา NTP ซึ่งได้ใช้วิธีเชื่อมต่อกับเวลาทางอินเทอร์เน็ตด้วยซึ่งถ้าไม่มีการซิงโครนัสเวลาแล้วเมื่อทำการตั้งค่านาฬิกาบนอุปกรณ์ที่ไม่ตรงกันทำให้ค่าชุดรหัสตัวเลขที่ได้ระหว่างเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการและ Token ไม่ตรงกันด้วย อีกทั้งหน้าต่างอินเทอร์เฟสต่างๆเนื่องจากมีการนำซอฟต์แวร์โอเพนซอร์สมาช่วยจึงปรับแต่งได้ไม่มากนัก

ในส่วนของข้อเสนอแนะคืออาจจะทำการปรับปรุงและพัฒนาการเชื่อมต่อระบบในส่วนของ VPN และการพิสูจน์ตัวตนให้อยู่ในขั้นตอนเดียวกัน อีกทั้งในส่วนของ Token ที่เป็นซอฟต์แวร์อาจจะเพิ่มฟังก์ชันการทำงาน เช่น ระบบกำหนดตำแหน่งบนโลก (GPS) และพัฒนาให้รองรับกับระบบปฏิบัติการที่หลากหลายมากยิ่งขึ้น

บรรณานุกรม

กรมตรวจบัญชีสหกรณ์. 2556. **เทคโนโลยี VPN คืออะไร.** [Online] Available: http://www.cad.go.th /ewtadmin/ewt/netgrp/download/VPN.pdf

พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550. 2556. **ราชกิจจานุเบกษา เล่ม 124 ตอนที่ 27 ก.** [Online] Available: http://www.mof.go.th/home/contact/19072550.pdf

สิริพร จิตต์เจริญธรรม, เสาวภา ปานจันทร์ และเลอศักดิ์ ลิ้มวิวัฒน์กุล. 2547. **ความรู้เบื้องต้นเกี่ยวกับการพิสูจน์ตัวตน**. [Online] Available: http://www.eco.ru.ac.th/MBE/boonkij/group3/Interconnection%20and%20Multicast%20Economics/security.htm

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน). 2554. **Secure Socket Layer Virtual Private Network.** [Online] Available: http://www.etda.or.th/etda_website/mains/display/209

Electric Sheep Fencing LLC. 2556. **Pfsense Documentation**. [Online] Available: https://doc.Pfsense.org/ index.php/Tutorials

EMC Corporation. 2556. **อาร์เอสเอ SECURID®AUTHENTICATORS: The gold standard in two-factor authentication.** [Online] Available: http://www.emc.com/collateral/data-sheet/ h9061-sid-ds.pdf

Thaicreate.com. 2556. **Android.** [Online] Available: http://www.thaicreate.com/ mobile/ Android.html

ภาคผนวก

ภาคผนวก ก
ขั้นตอนการติดตั้งระบบ

1.1 การติดตั้ง Pfsense

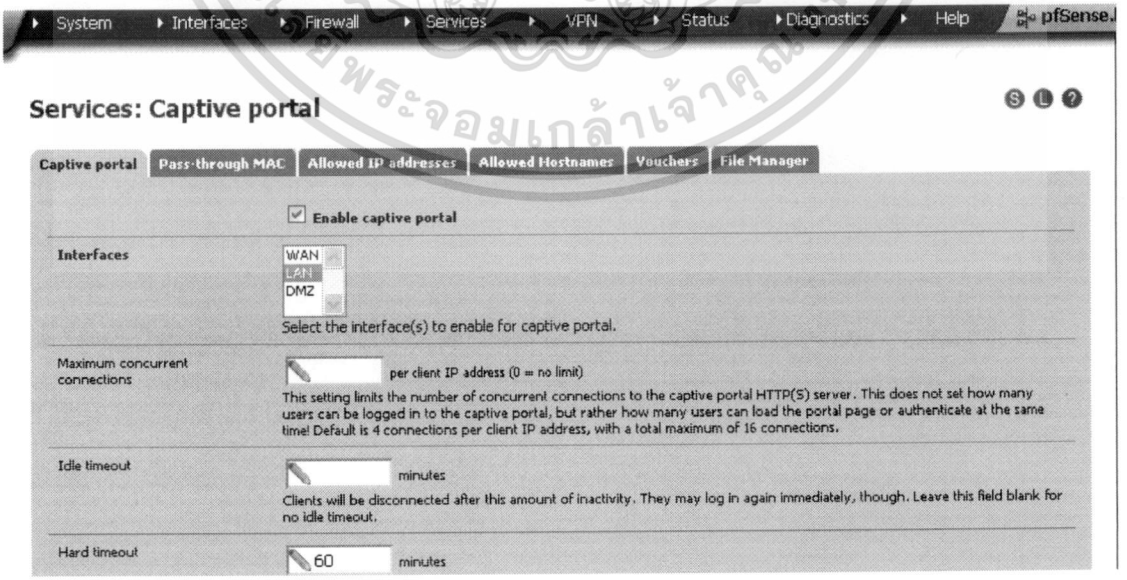
ดาวน์โหลดโอเพนซอร์ส Pfsense หลังจากนั้นทำการติดตั้งระบบลงในคอมพิวเตอร์ที่มีพอร์ตสำหรับเชื่อมต่อเครือข่าย 3 ช่องทาง

1.2 การติดตั้ง Captive portal Open VPN Free Radius และ Proxy (Squid)

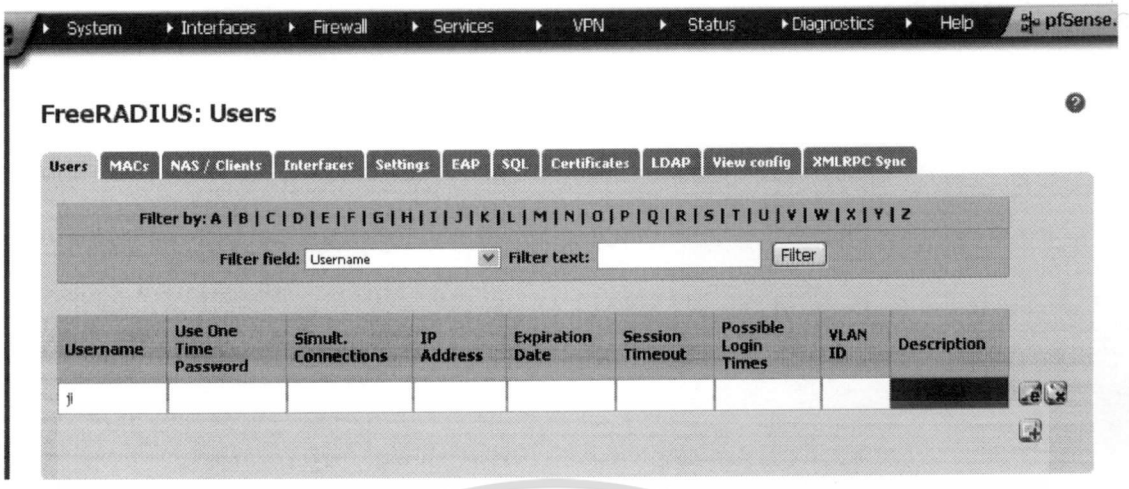
หลังจากทำการเชื่อมต่ออินเทอร์เน็ตแล้ว ไปที่ System-> Package แล้วทำการเลือก Open VPN Free Radius และ Squid แล้วสั่ง Install

หลังจากนั้น ระบบจะทำการติดตั้งโดยอัตโนมัติ พอติดตั้งเสร็จจะปรากฏเมนูดังนี้

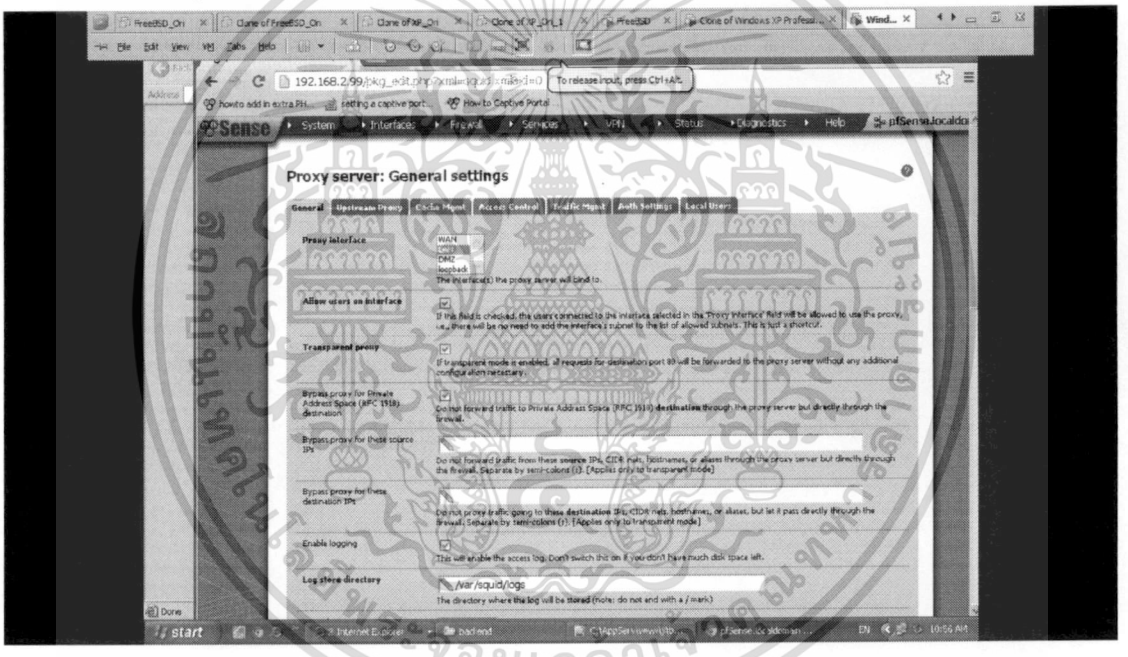
Services->Captive Portal



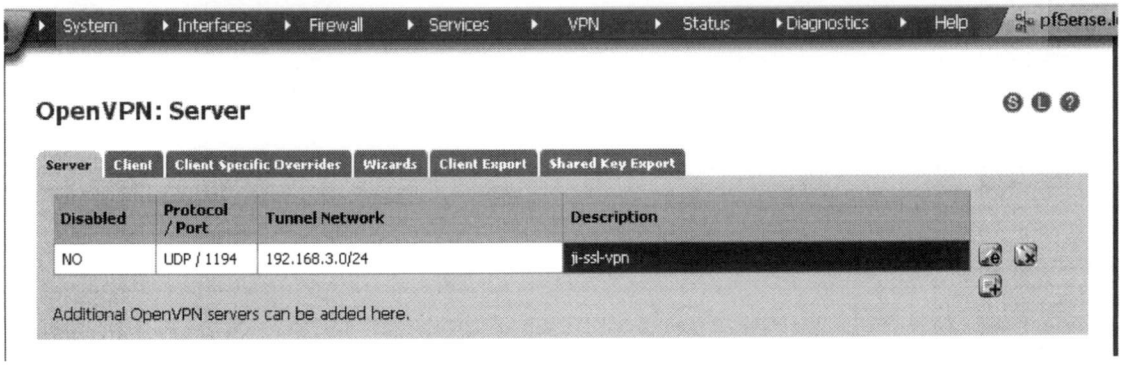
Services-> Free Radius



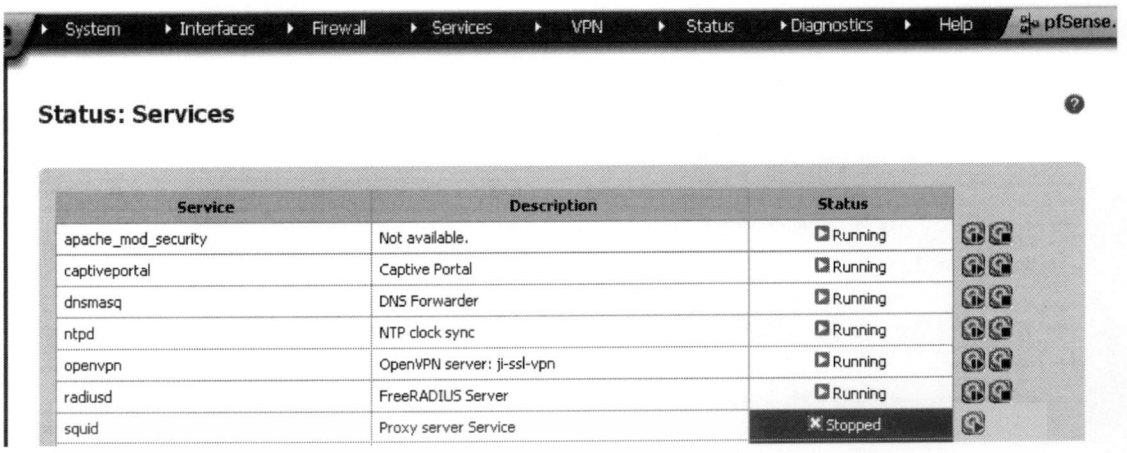
Services ->Proxy Server



VPN->Open VPN



Status->Service



1.3 การติดตั้งเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการเว็บ สำหรับระบบพิสูจน์ตัวตนด้วย Token

ติดตั้ง Appserv 2.5.9

ตั้งค่า Apache and SSL (HTTPS)

นำโปแกรมที่เขียนเสร็จไปวางไว้ที่ C:\Appserv\www\ และสร้างฐานข้อมูล

1.4 การติดตั้งโปรแกรมแอพพลิเคชัน Token บนระบบปฏิบัติการแอนดรอยด์

ดาวน์โหลดแอพพลิเคชัน Generate Token จากเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ และทำการติดตั้ง หลังจากนั้นใส่ Key ที่ได้จากการนำออกมาจากเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Token แล้วจึงจะทำให้แอพพลิเคชันใช้งานและทำการสร้างชุดรหัสตัวเลขได้

1.5 การตั้งค่าการเชื่อมต่อระบบ

ระบบพิสูจน์ตัวตนผ่านเครือข่ายเสมือนโดยใช้ Token จะถูกติดตั้งและจัดการโดยส่วนเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการโดยติดตั้งระบบปฏิบัติการและชุดซอฟต์แวร์ที่ทำหน้าที่บริการต่างๆตามหัวข้อด้านบนและทำการตั้งค่าการทำงานตัวเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการหลังจากนั้นจึงทำกาบริหารจัดการผู้ใช้งานระบบ

1.5.1 เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ VPN และเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Proxy

- ทำการตั้งค่า IP Address ในส่วนของ WAN เพื่อเชื่อมต่อกับ Router
- ทำการตั้งค่า IP Address ในส่วนของ LAN เพื่อเชื่อมต่อกับผู้ใช้งานระบบภายใน
- ทำการตั้งค่า IP Address ในส่วนของ DMZ เพื่อเชื่อมต่อกับกลุ่มของเครื่องคอมพิวเตอร์แม่ข่าย
- ทำการเปิดไฟร์วอลล์เป็น Any ทั้งหมด

- ทำการ Enable Captive portal และ เชื่อมต่อผู้ใช้งานระบบ กับฐานข้อมูลบัญชี Radius

- ทำการสร้าง Radius Client เพื่อรองรับการเชื่อมต่อกับ Captive portal และ VPN

- ทำการ Enable Proxy เพื่อใช้ในการเก็บข้อมูลผู้ใช้งานด้วย

- ทำการตั้งค่า IP Address ที่ System Log สำหรับส่งข้อมูลผู้ใช้งานเว็บไซต์ให้ส่งไปที่ Syslog Server (เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Token)

- ทำการสร้าง Open VPN เพื่อกำหนดชุด IP Address สำหรับการเชื่อมต่อจากผู้ใช้งานระบบภายนอก

1.5.2 เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Token ซึ่งติดตั้งเป็นเว็บอินทราเน็ตด้วยในเครื่องคอมพิวเตอร์ระบบปฏิบัติการไมโครซอฟท์ วินโดวส์เอกซ์พี

- ทำการติดตั้งชุดโปรแกรมไว้ที่ Apache เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการเว็บ

- เรียกใช้งานโปรแกรมผ่านเว็บเบราว์เซอร์

- ติดตั้งโปรแกรม Syslog watcher เพื่อใช้ช่วยในการดูข้อมูลผู้ใช้งานเว็บไซต์ง่ายขึ้น

ภาคผนวก ข

คู่มือการใช้งานระบบ

หลังจากทำการติดตั้งระบบเสร็จแล้วสามารถใช้งานฟังก์ชันต่างๆได้ ดังนี้

1. การใช้งาน VPN โดยผู้ดูแลระบบ

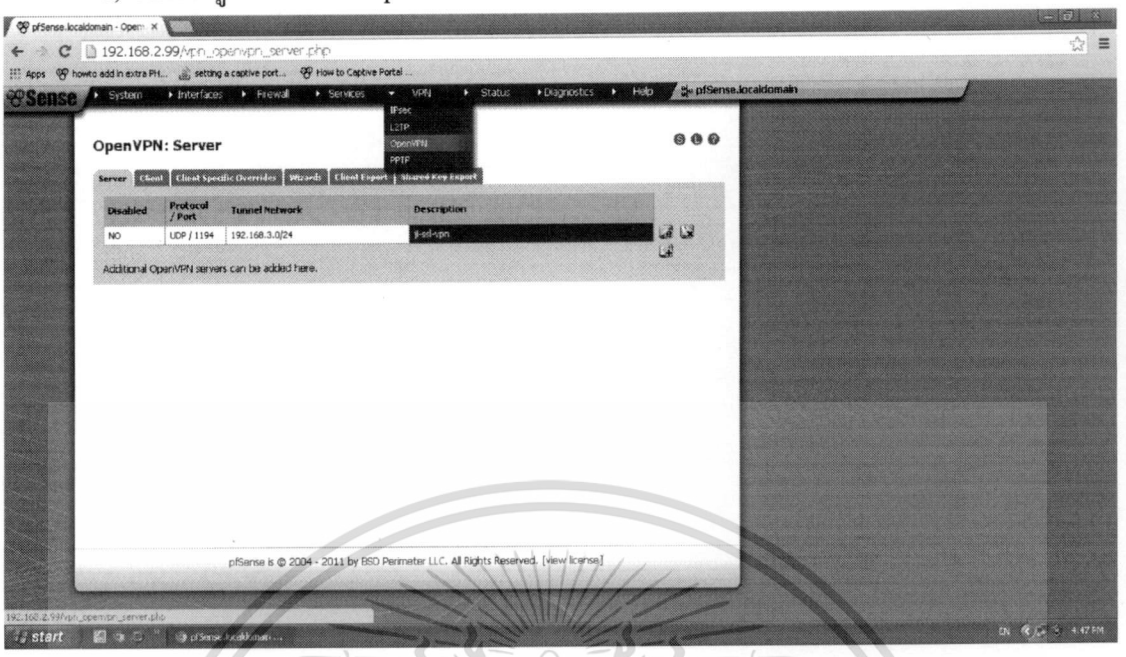
1) เชื่อมต่อคอมพิวเตอร์เข้าสู่ระบบเครือข่ายเดียวกับคอมพิวเตอร์ที่ทำการติดตั้งระบบปฏิบัติการ Pfsense ที่เราได้ทำการใช้เป็นเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ VPN

2) เปิดเว็บเบราว์เซอร์และพิมพ์ IP Address ของเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ VPN เช่นในตัวอย่าง 192.168.2.99

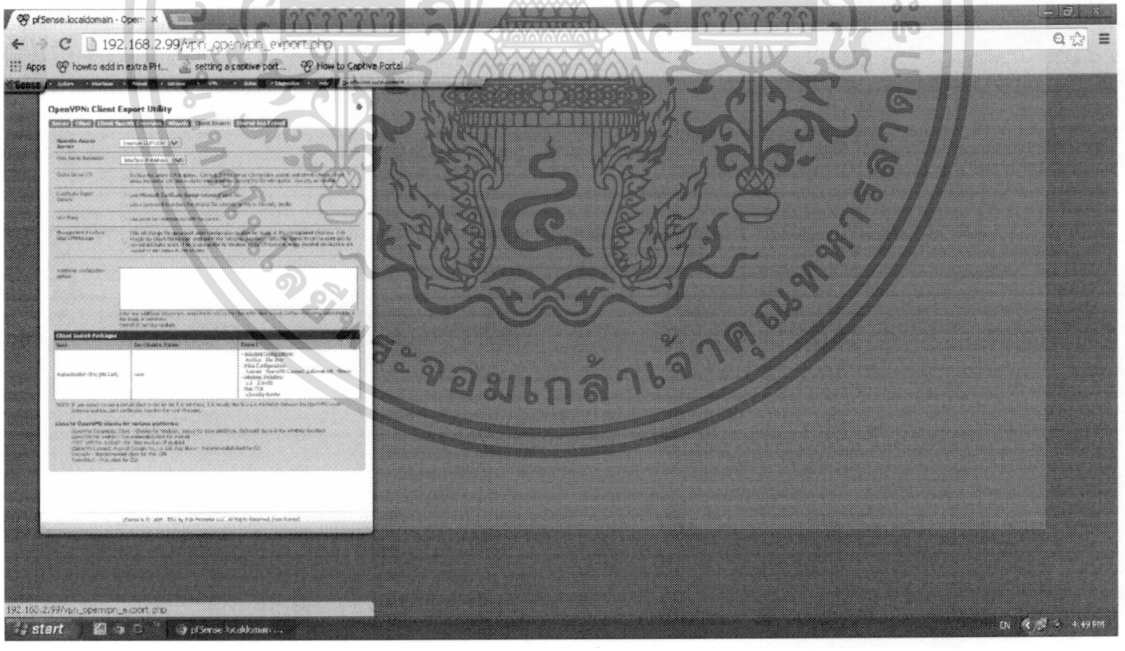
3) หลังจากนั้นจะปรากฏหน้า Login เพื่อทำการยืนยันตัวตนก่อนเข้าใช้งาน

4) ใส่ชื่อผู้ใช้และรหัสผ่าน

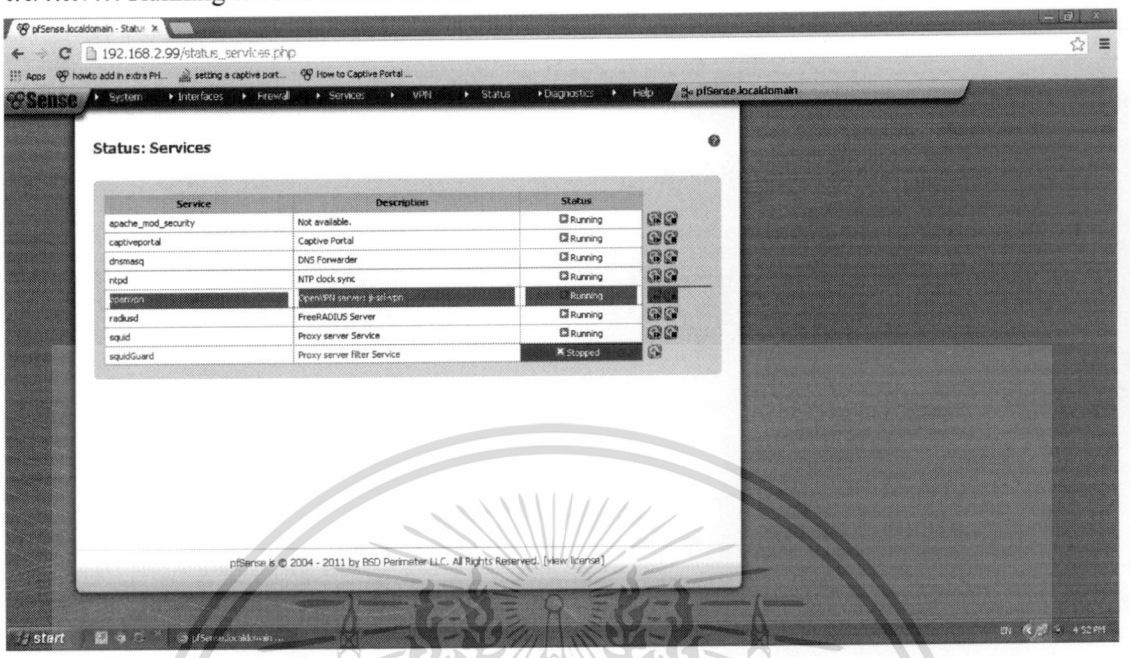
5) ไปที่เมนู VPN เลือก Open VPN จะเห็นว่าได้ตั้งการไว้แล้ว



6) เลือกไปที่ Client Export เพื่อทำการสร้างโปรแกรม VPN ของเครื่องลูกข่ายไว้สำหรับติดตั้งในเครื่องคอมพิวเตอร์จากภายนอกโดยสามารถคลิกเลือกตามระบบปฏิบัติการที่ใช้ได้



7) ตรวจสอบสถานการณ์ทำงานของ Open VPN โดยไปที่เมนู Status -> Services ว่าอยู่ในสถานภาพ Running หมายถึงพร้อมใช้งาน



2. การใช้งาน Proxy โดยผู้ดูแลระบบ

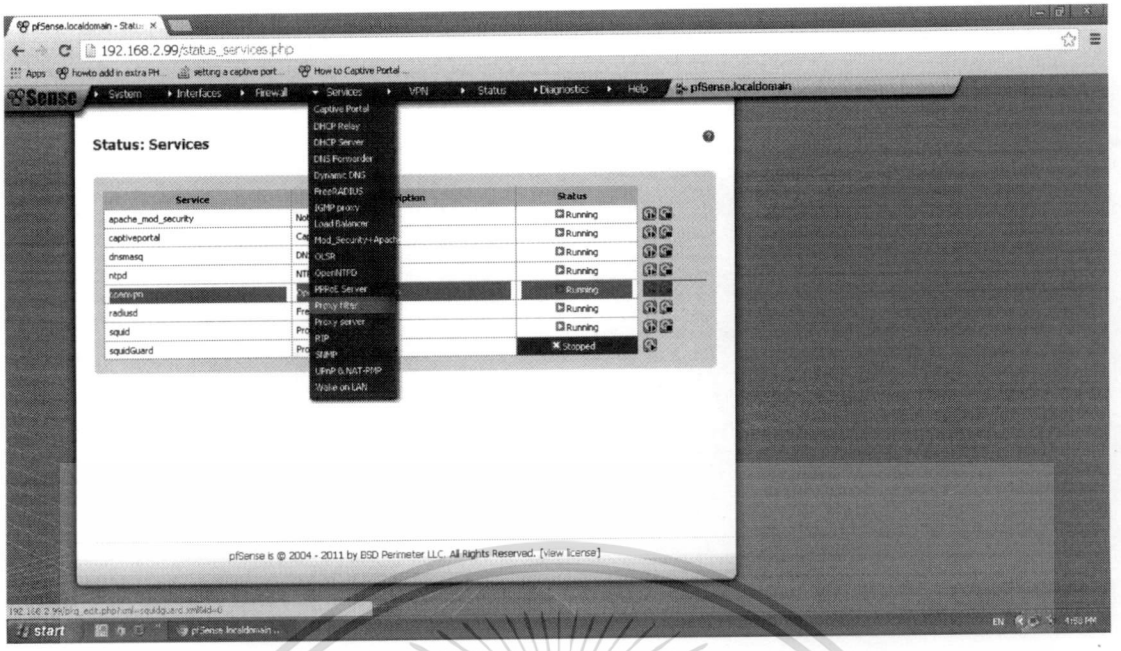
1) เชื่อมต่อคอมพิวเตอร์เข้าสู่ระบบเครือข่ายเดียวกับคอมพิวเตอร์ที่ทำการติดตั้งระบบปฏิบัติการ Pfsense ที่เราได้ทำการใช้เป็นเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Proxy ซึ่งเป็นเครื่องเดียวกับเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ VPN

2) เปิดเว็บเบราว์เซอร์และพิมพ์ IP Address ของเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Proxy เช่นในตัวอย่าง 192.168.2.99

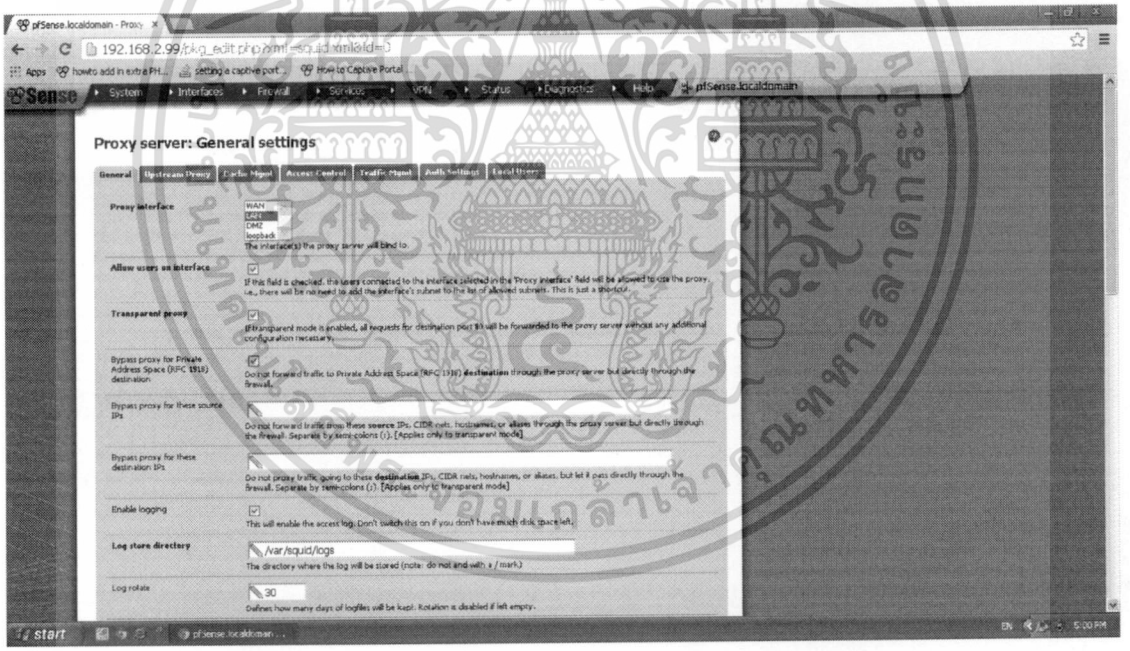
3) หลังจากนั้นจะปรากฏหน้า Login เพื่อทำการยืนยันตัวตนก่อนเข้าใช้งาน

4) ทำการใส่ชื่อผู้ใช้และรหัสผ่าน

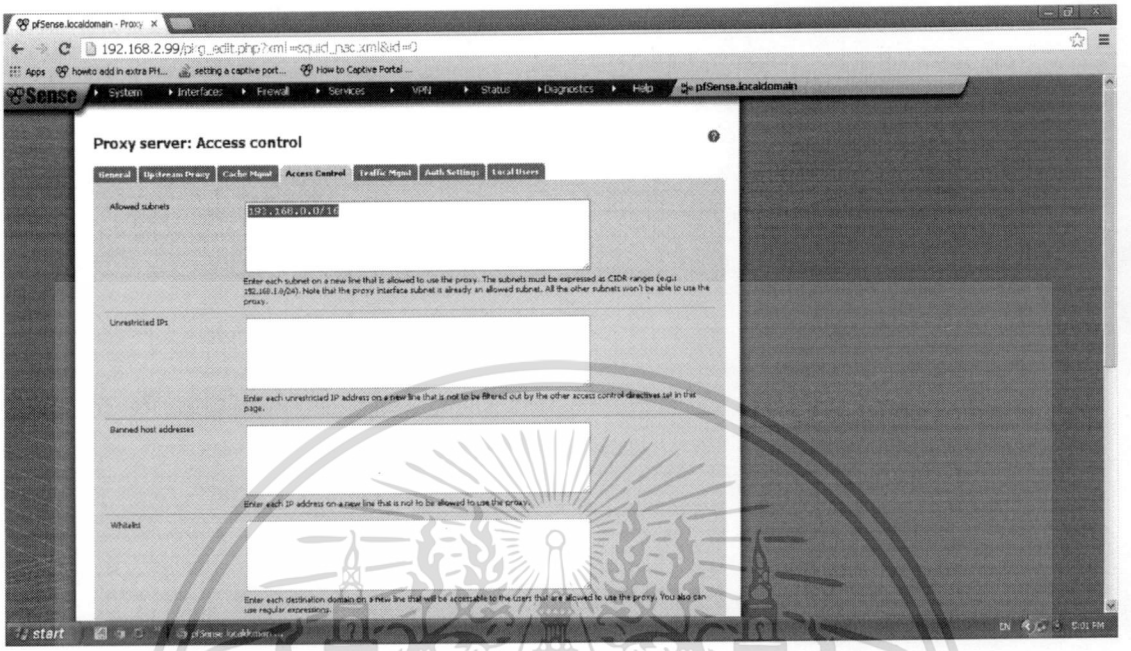
5) หลังจากนั้นไปที่เมนู Services -> Proxy Server



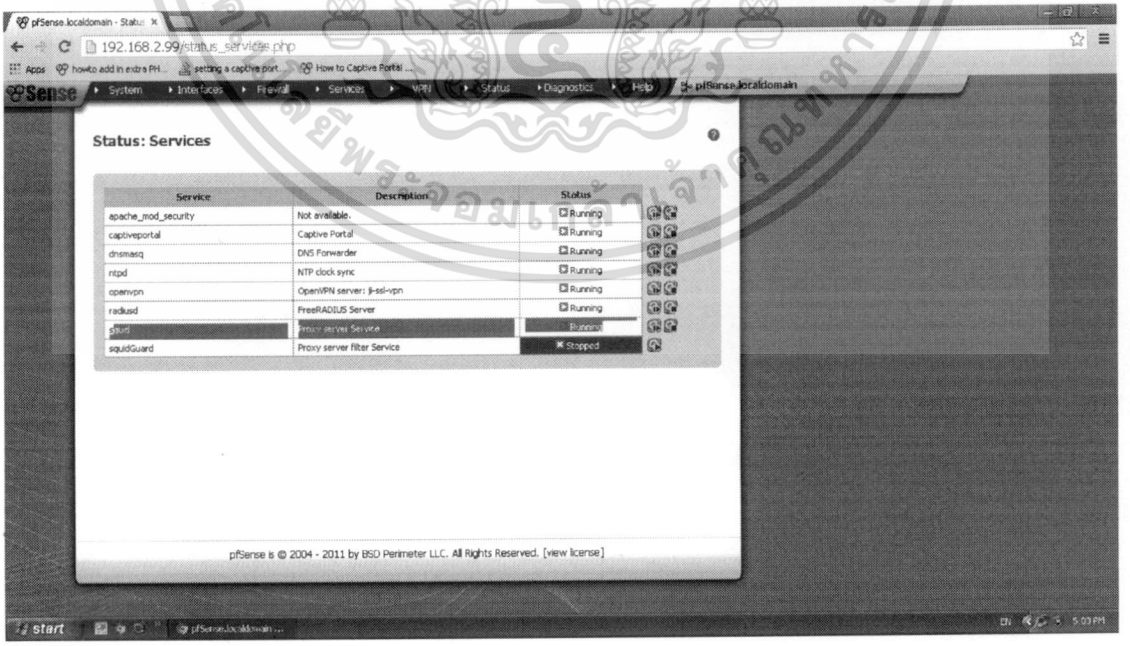
6) เลือก Interface กลุ่มผู้ใช้งานที่ต้องการใช้ Proxy ในที่นี้เลือก LAN



7) ไปที่เมนู Access Control เพื่อตรวจสอบกลุ่ม IP Address ของเครื่องคอมพิวเตอร์ภายในที่ต้องการใช้งาน Proxy

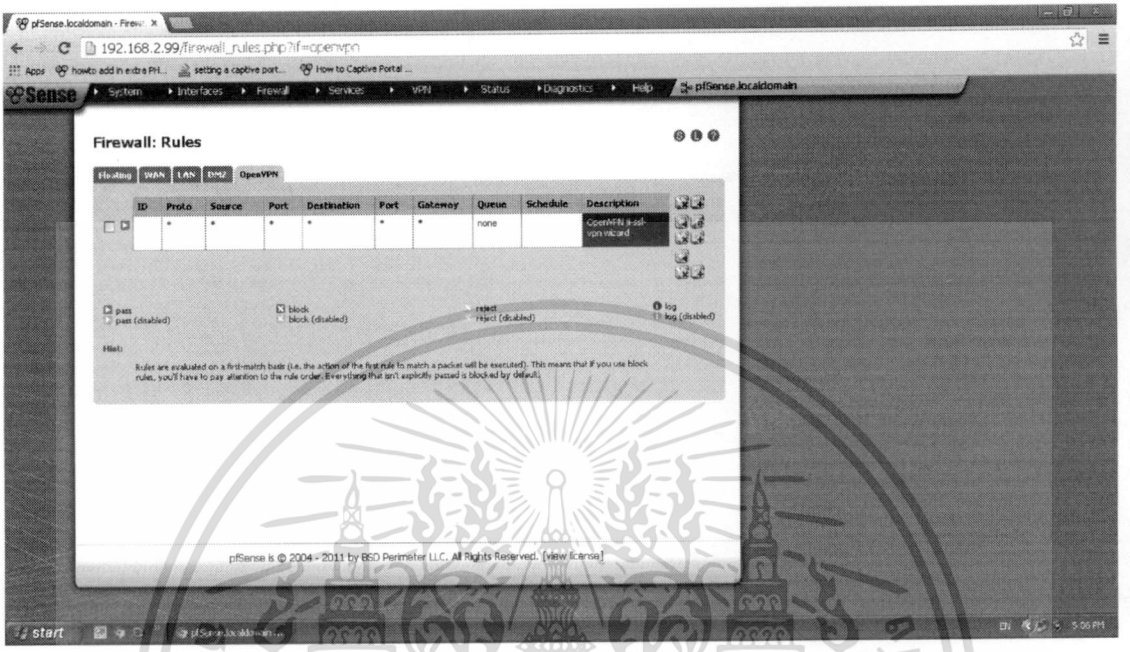


8) ตรวจสอบสถานการณ์ทำงานของเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Proxy โดยไปที่เมนู Status -> Services ว่าสถานภาพ Squid อยู่ในสถานภาพ Running หมายถึงพร้อมใช้งานหรือไม่

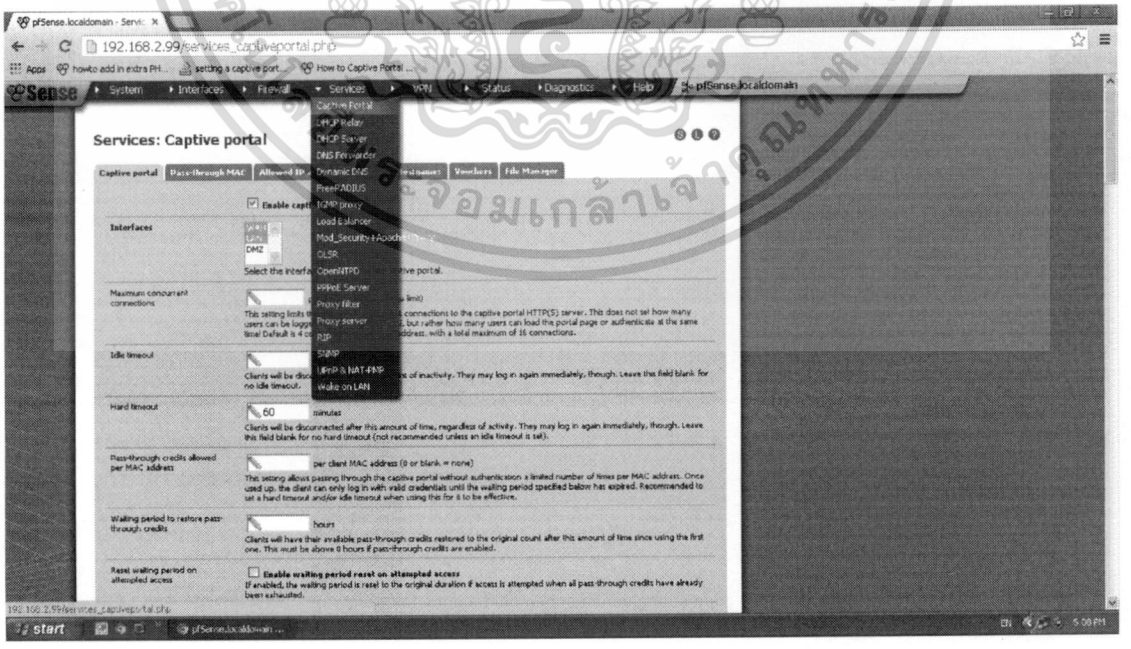


3. การใช้งานการยืนยันตัวตนในฟังก์ชัน VPN และ Proxy โดยผู้ดูแลระบบ

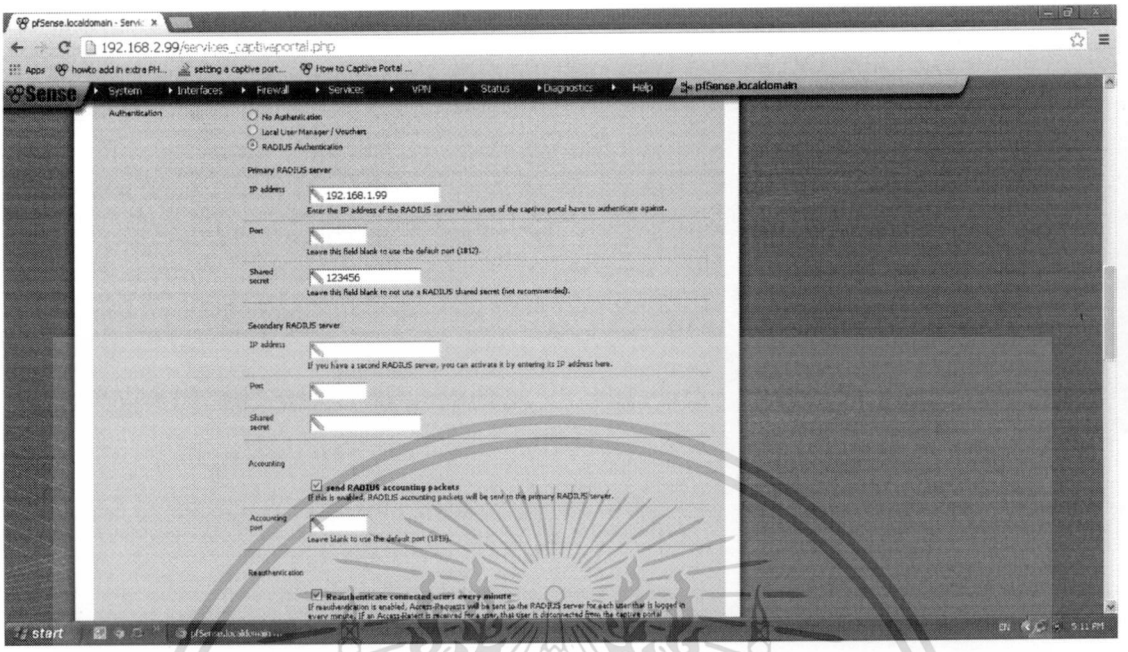
1) สำหรับ VPN สามารถใช้งานได้เลยเพียงแค่ตรวจสอบการตั้งค่าในไฟร์วอลล์โดยไปที่เมนู Firewall -> Rules -> OpenVPN ทำการเปิดใช้งาน any ทั้งหมดผลที่ได้จะเป็น *



2) สำหรับการใช้งานการยืนยันตัวตนในฟังก์ชัน Proxy ไปที่เมนู Services -> Captive Portal เลือก Enable กำหนดกลุ่ม Interface ของเครื่องภายในที่ต้องการยืนยันตัวตน

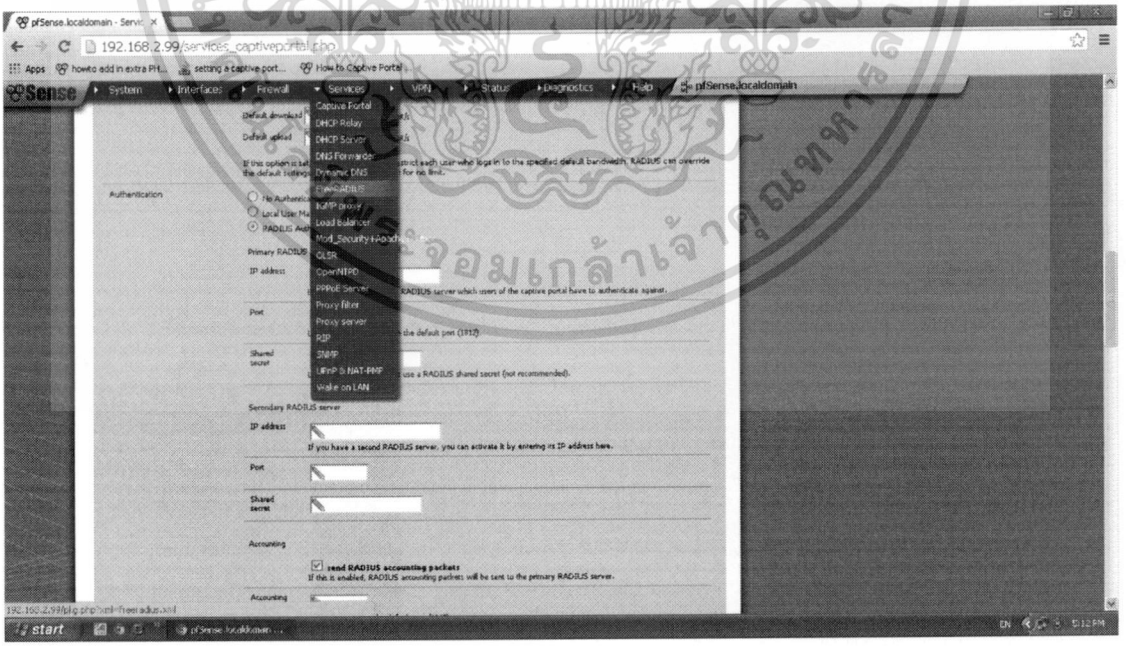


3) กำหนดตำแหน่งที่จะตรวจสอบบัญชีผู้ใช้งาน ซึ่งในที่นี้เก็บไว้ที่ Radius

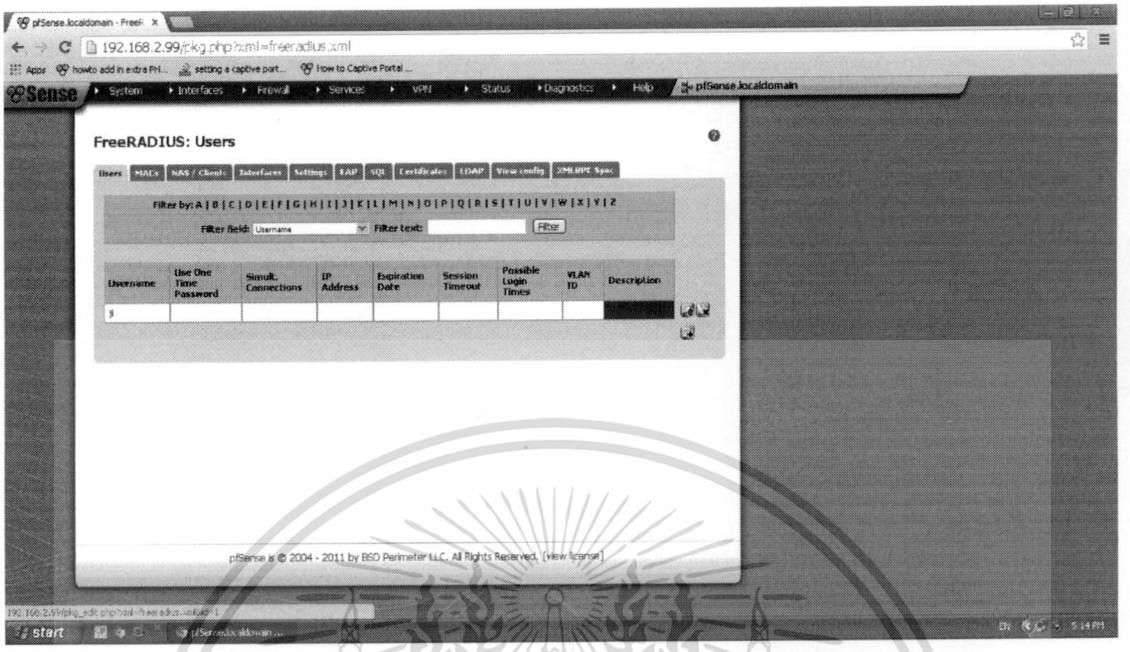


4. การจัดการผู้ใช้งานฟังก์ชัน VPN และ Proxy โดยผู้ดูแลระบบ

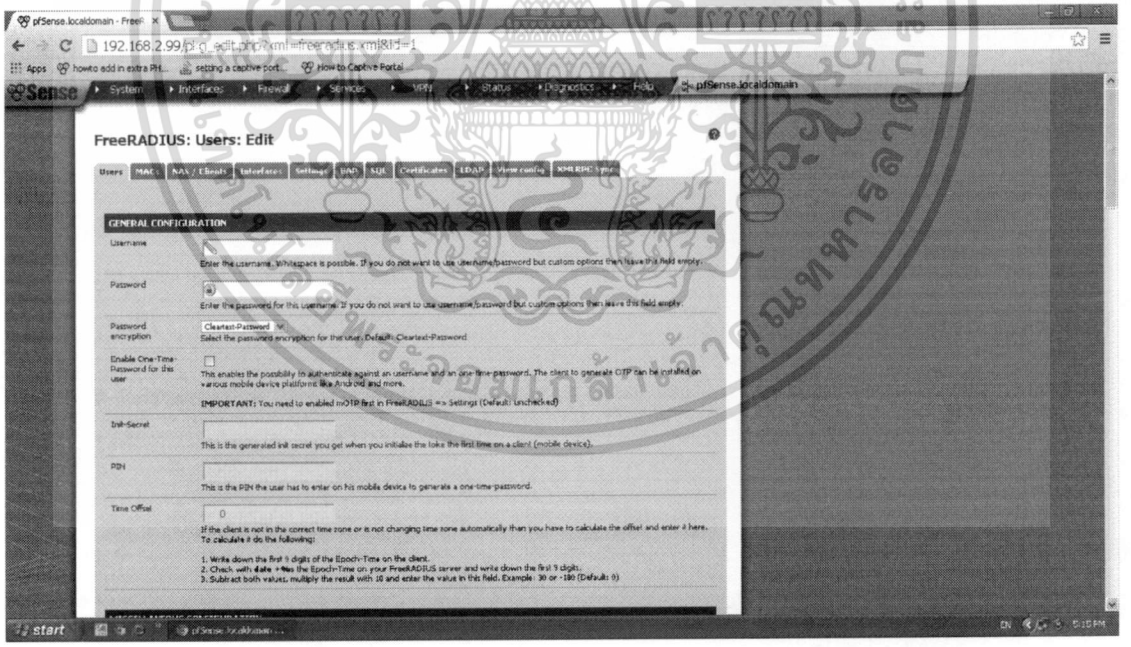
1) บัญชีผู้ใช้งานทำสร้างและบันทึกลงในฐานข้อมูล Free Radius ดังนั้นให้ไปที่เมนู Services -> FreeRADIUS



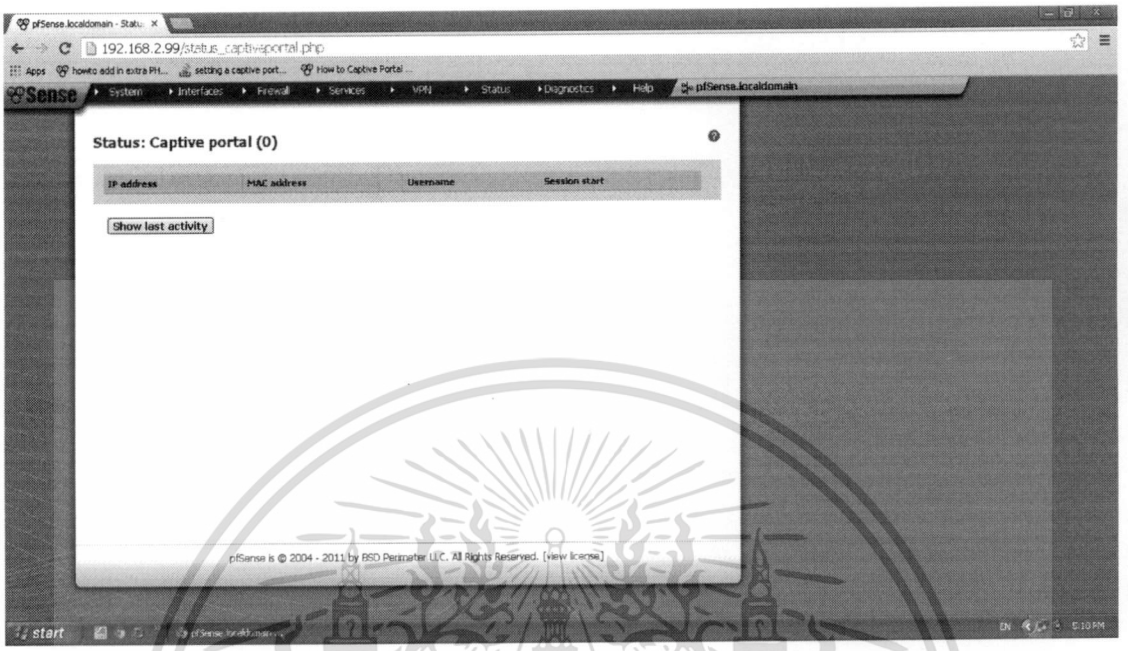
2) คลิก + เพื่อเพิ่มบัญชีผู้ใช้งาน



3) กำหนดชื่อผู้ใช้งานและรหัสผ่านเสร็จแล้วทำการคลิก Save

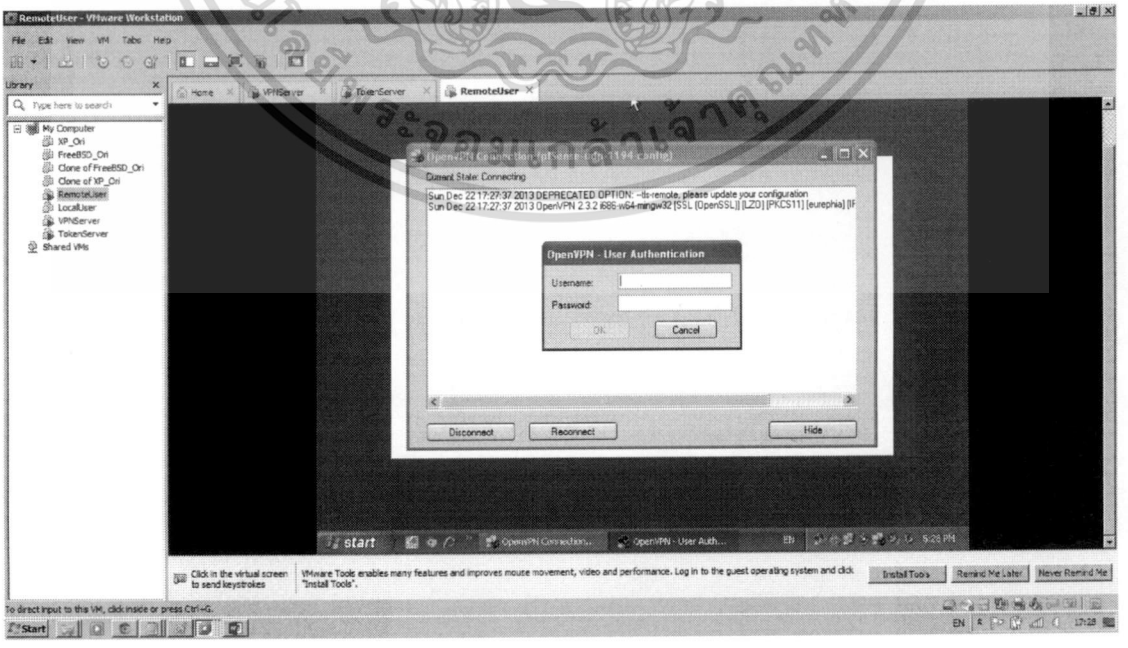


4) สามารถตรวจสอบรายการผู้ใช้งานเมื่อมีการ Login เข้าสู่ระบบที่เมนู Services -> Captive Portal

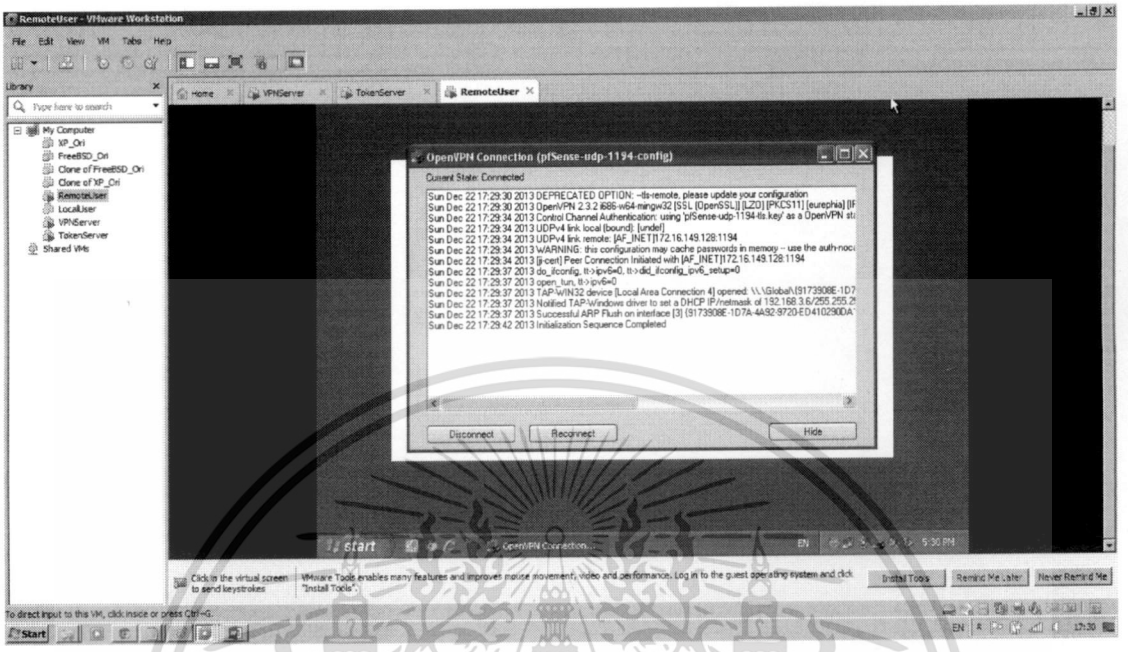


5. การเชื่อมต่อเครือข่ายด้วย VPN Client โดยผู้ใช้งานภายนอก

1) หลังจากทำการติดตั้ง VPN Client ที่คอมพิวเตอร์ภายนอกเครือข่ายแล้วตรวจสอบการเชื่อมต่ออินเทอร์เน็ต และทำการเปิดโปรแกรม OpenVPN GUI

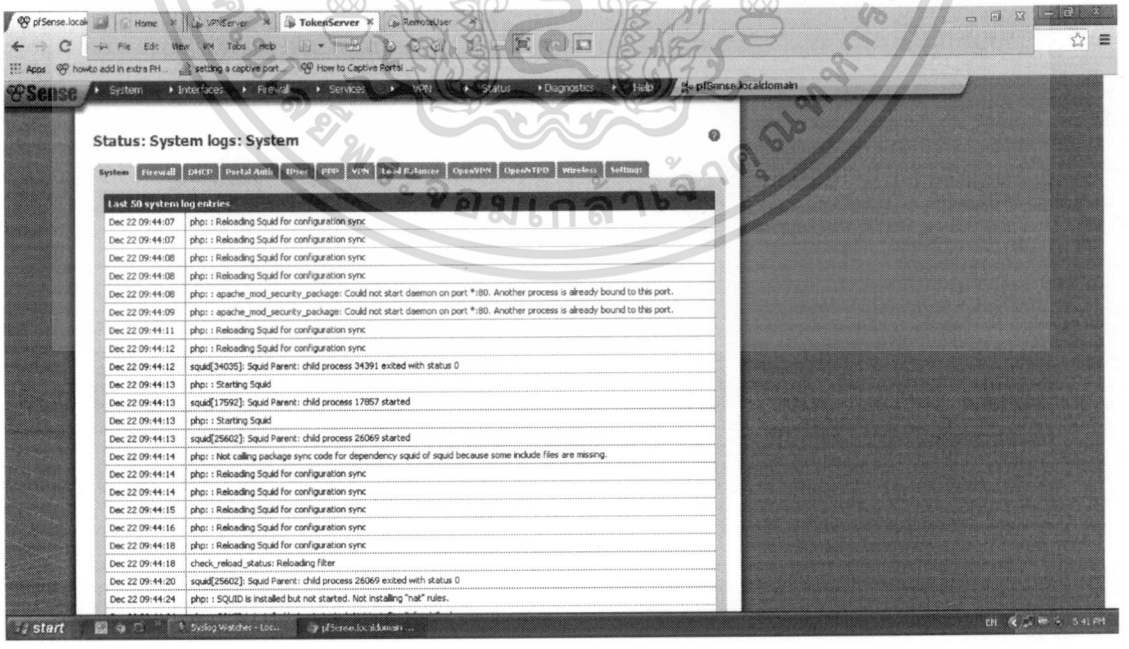


2) ใส่ชื่อผู้ใช้งานและรหัสผ่านซึ่งเป็นบัญชีเดียวกับการใช้งาน Proxy หลังจากนั้นคลิก OK หลังจากนั้นปรากฏ Initialization Sequence Completed และจะได้ IP Address อีกชุดหนึ่ง

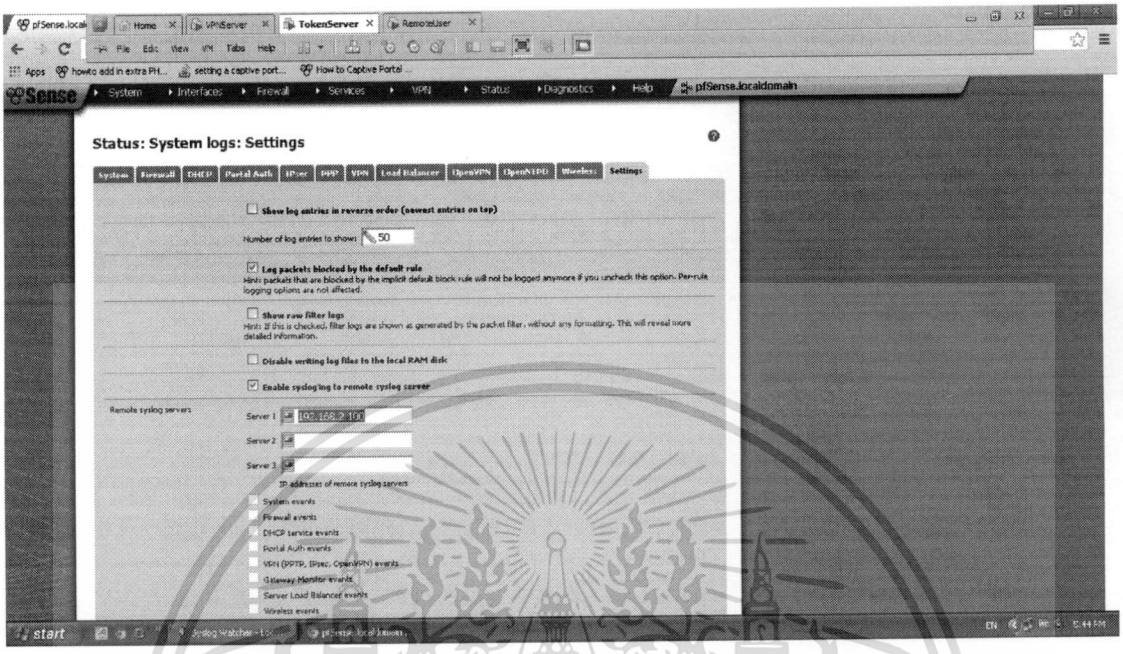


6. การใช้งานฟังก์ชันจัดเก็บข้อมูลผู้ใช้งานของการใช้งานระบบผ่าน Proxy โดยผู้ดูแลระบบ

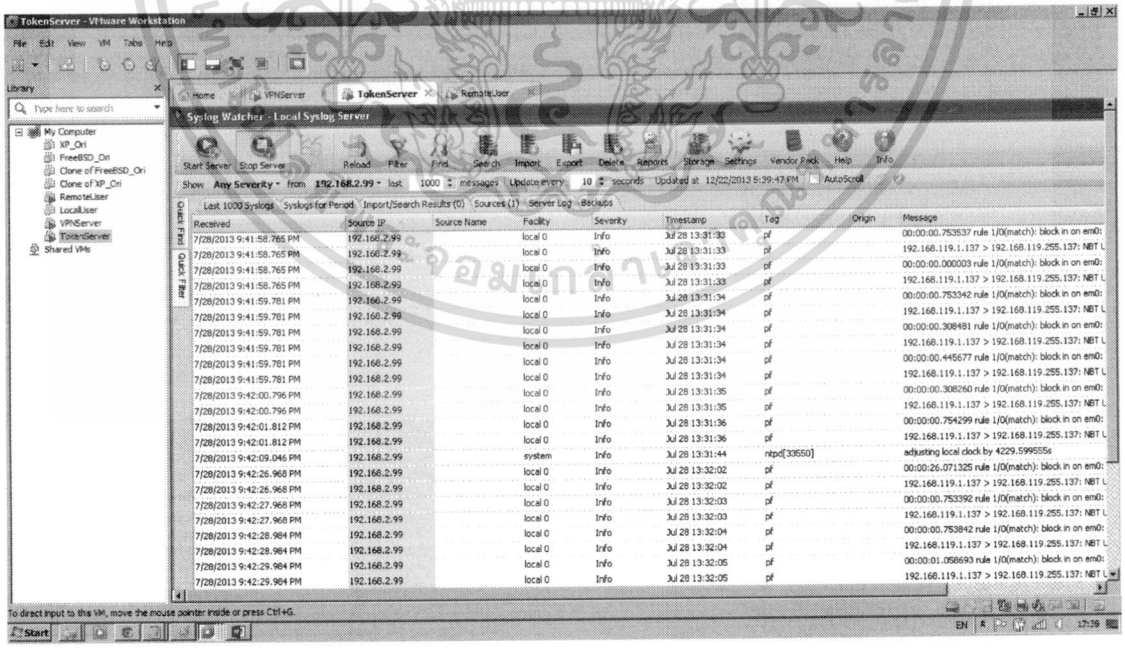
1) ทำการตั้งค่า Syslog โดยเปิดใช้งานเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Proxy และไปที่เมนู Status -> System logs



2) ทำการตั้งค่าโดยไปที่เมน Settings ใส่ IP Address เครื่องที่จะทำการเก็บข้อมูลผู้ใช้งาน ในที่นี้ใช้เครื่องเดียวกับเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ VPN

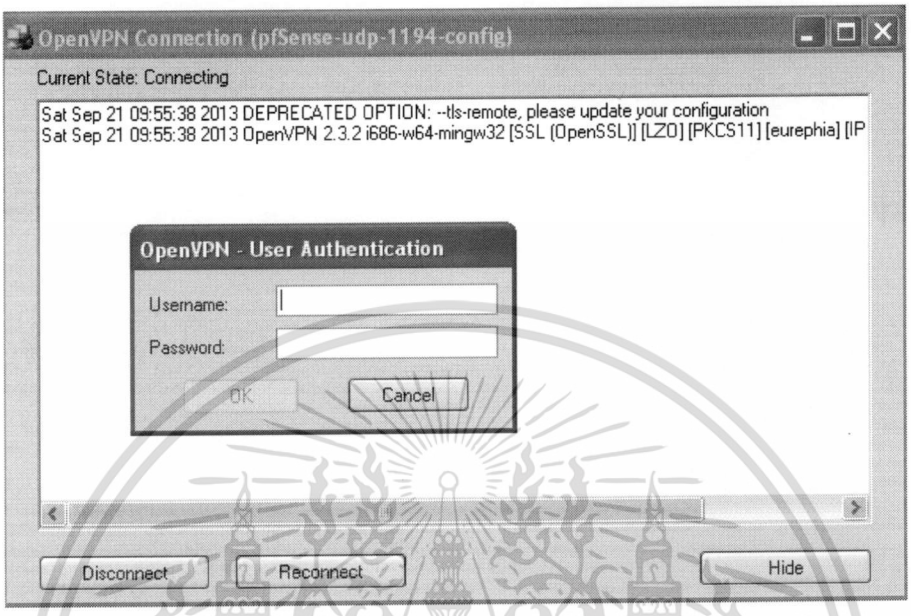


3) หลังจากทำการตั้งค่าเสร็จแล้ว เปิดโปรแกรม Syslog watcher สามารถดูสถานการณ์ใช้งานได้

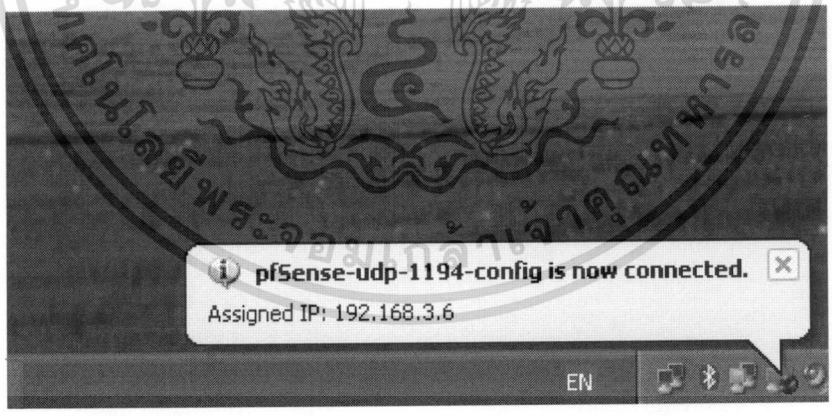


7. การใช้งานระบบพิสูจน์ตัวตนด้วย Token โดยเข้าใช้งานผ่านเว็บอินทราเน็ต โดยผู้ใช้งาน

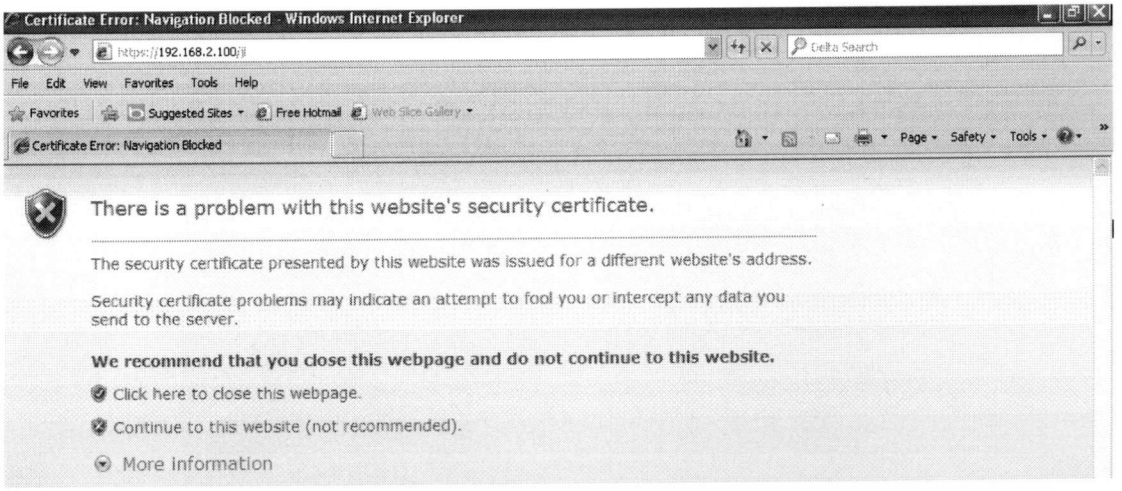
1) ผู้ใช้งานภายนอกเครือข่ายจะต้องทำการเชื่อมต่อเครือข่ายภายในด้วย VPN Client ก่อน จะยืนยันตัวตนเพื่อใช้งานระบบงานภายในได้



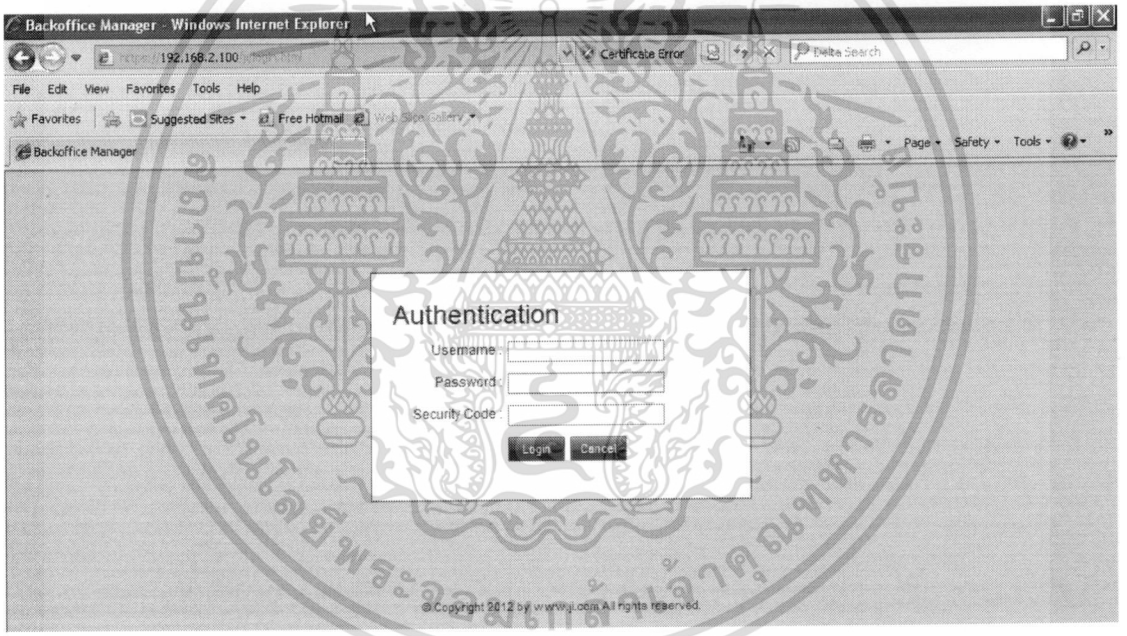
2) เมื่อ VPN สำเร็จจะ ได้ Connection IP Address อีกชุด แล้วจึงสามารถเข้าใช้งานระบบเว็บอินทราเน็ต โดยการพิสูจน์ตัวตนด้วยชื่อผู้ใช้ รหัสผ่าน และ Token



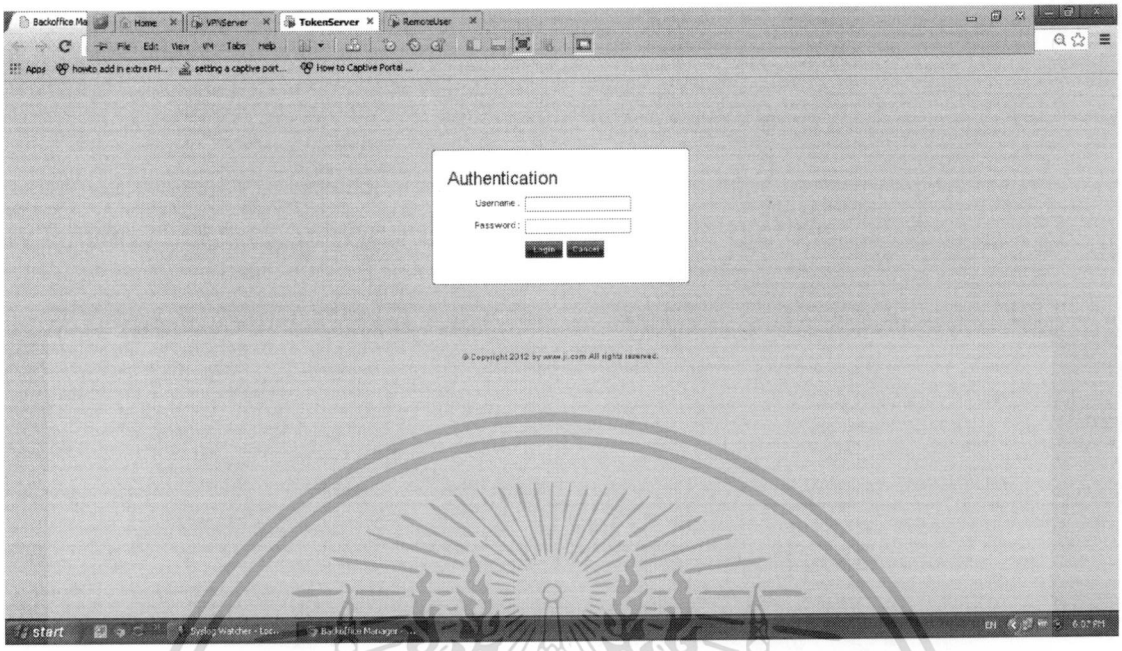
3) การใช้ระบบงานเว็บอินทราเน็ต สามารถเข้าใช้งานได้ โดยการผ่านเว็บเบราว์เซอร์และทำการ พิมพ์ IP Address ของเครื่องที่ทำการติดตั้งเว็บอินทราเน็ต ซึ่งในที่นี้ติดตั้งที่เครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Token เนื่องจากมีการเพิ่มความปลอดภัยด้วยโพรโตคอล HTTPS จึงต้องพิมพ์ https://ตาม ด้วย IP Address ด้วย



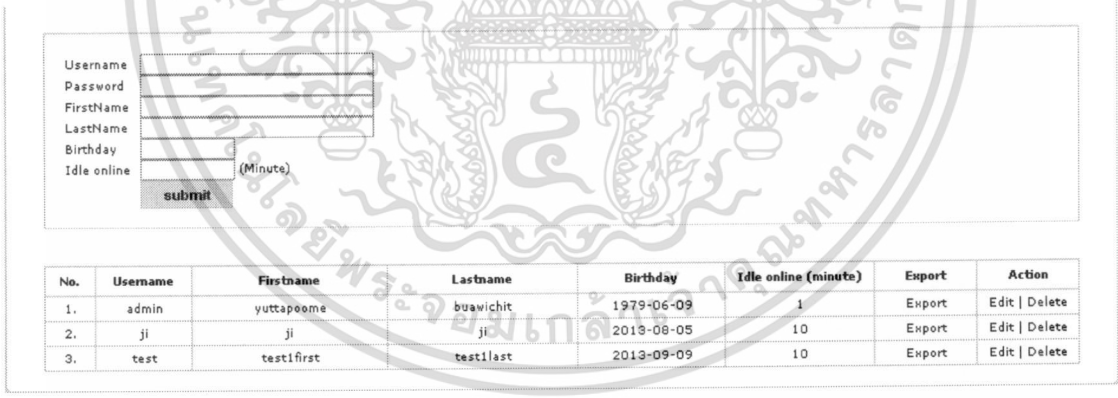
4) หลังจากนั้นทำการพิสูจน์ตัวตนก่อนการจะใช้งานเว็บอินทราเน็ต โดยใช้ชื่อผู้ใช้ รหัสผ่านและToken ที่ได้รับจากแอพพลิเคชันในระบบปฏิบัติการแอนดรอยด์บนโทรศัพท์เคลื่อนที่



5) สำหรับผู้ดูแลระบบสามารถ Login เข้าใช้งานระบบผ่านเว็บเบราว์เซอร์



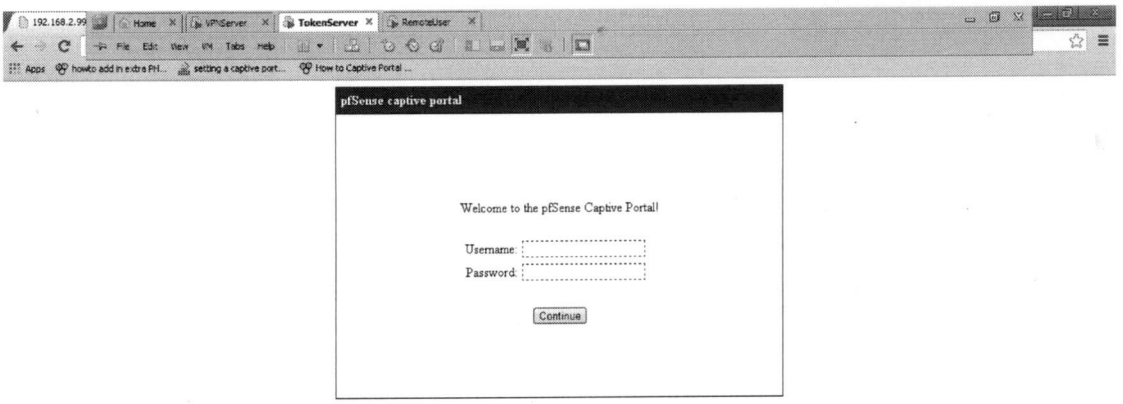
6) จะปรากฏเมนูไว้สำหรับให้ผู้ใช้งานระบบสร้างบัญชีผู้ใช้ และส่งออกค่าไว้สำหรับใช้งาน Token ได้



No.	Username	Firstname	Lastname	Birthday	Idle online (minute)	Export	Action
1.	admin	yuttapoome	buawichit	1979-06-09	1	Export	Edit | Delete
2.	ji	ji	ji	2013-08-05	10	Export	Edit | Delete
3.	test	test1first	test1last	2013-09-09	10	Export	Edit | Delete

8. การใช้งานระบบพิสูจน์ตัวตนก่อนการใช้งานอินเทอร์เน็ต ผ่าน Proxy

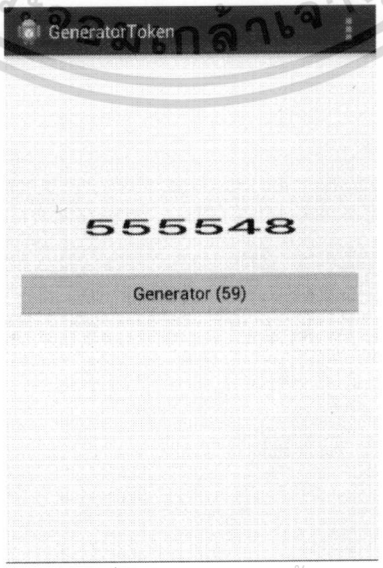
1) เมื่อเครื่องคอมพิวเตอร์ภายในเครือข่ายจะทำการใช้งานอินเทอร์เน็ตจะทำการเปิดเว็บเบราว์เซอร์ และทำการพิมพ์ชื่อเว็บไซต์ต่างๆที่ต้องการจะใช้งานแต่ในที่นี้จะไม่สามารถใช้งานได้ทันทีเพราะระบบจะกำหนดให้ยืนยันตัวตนก่อนการใช้งาน



2) หลังจากยืนยันตัวตนผ่านแล้วระบบจะยอมให้ใช้งานเว็บไซต์ตามที่ร้องขอผ่านเครื่องคอมพิวเตอร์สำหรับเป็นผู้ให้บริการ Proxy โดยระบบจะมีการเก็บข้อมูลของผู้ใช้งานเว็บไซต์ต่างๆ ด้วย ตาม พ.ร.บ. คอมพิวเตอร์ 2550

9. การใช้งาน Token ในระบบปฏิบัติการแอนดรอยด์ผ่านโทรศัพท์เคลื่อนที่

1) หลังจากทำการติดตั้งแอพพลิเคชัน Token ในโทรศัพท์เคลื่อนที่เรียบร้อยแล้วให้ตรวจสอบการเชื่อมต่อเวลาโดยให้ตั้งค่ารับเวลาจากอินเทอร์เน็ต หลังจากนั้นเปิดแอพพลิเคชันเพื่อเริ่มการทำงานซึ่งจะได้รหัสตัวเลข 6 หลักไว้สำหรับการยืนยันตัวตนเป็นตัวประกอบที่ 2 ในระบบพิสูจน์ตัวตนผ่านเครือข่ายเสมือนด้วย Token



ประวัติผู้เขียน

ชื่อผู้จัดทำโครงงาน	นายวิวรรธน์ โกพลรัตน์
วันเดือนปีเกิด	24 กุมภาพันธ์ 2528
สถานที่เกิด	นครพนม
ประวัติการศึกษา	
มัธยมศึกษาตอนต้น	โรงเรียนจุฬาภรณราชวิทยาลัย มุกดาหาร
มัธยมศึกษาตอนปลาย	โรงเรียนแก่นนครวิทยาลัย ขอนแก่น
อุดมศึกษา	วศ.บ. วิศวกรรมคอมพิวเตอร์ มหาวิทยาลัยนเรศวร
ประวัติการทำงาน	
พ.ศ. 2556 – ปัจจุบัน	นักวิชาการคอมพิวเตอร์ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร