การพัฒนาอุปกรณ์ให้บริการเครือข่ายเสมือนส่วนตัว

DEVELOPEMENT OF VIRTUAL PRIVATE NETWORK SERVER

โดย

เฉลิมศักดิ์ เครือวัลย์

CHALERMSAK KROURWAN

อาจารย์ที่ปรึกษา

ผศ. อัครินทร์ คุณกิตติ

รายงานนี้เป็นส่วนหนึ่งของวิชาโครงการพัฒนาระบบงาน
หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
คณะเทคโนโลยีสารสนเทศ
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ภาคเรียนที่ 2 ปีการศึกษา 2552

DEVELOPEMENT OF VIRTUAL PRIVATE NETWORK SERVER

CHALERMSAK KROURWAN

A REPORT SUBMITTED IN PARTIAL FULFILLMENT OF THE

REQUIREMENTS OF THE COURSE

SYSTEM DEVELOPMENT PROJECT

MASTER OF SCIENCE PROGRAM IN INFORMATION TECHNOLOGY

FACULTY OF INFORMATION TECHNOLOGY

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

2/ 2009

ใบรับรองโครงการพัฒนาระบบงาน (System Development Project)

เรื่อง

การพัฒนาอุปกรณ์ให้บริการเครือข่ายเสมือนส่วนตัว

DEVELOPMENT OF VIRTUAL PRIVATE NETWORK

เฉลิมศักดิ์ เครือวัลย์

รหัสประจำตัว 50066433

ขอรับรองว่ารายงานฉบับนี้ข้าพเจ้าไม่ได้คัดลอกมาจากที่ใด
รายงานฉบับนี้ได้รับการตรวจสอบและอนุมัติให้เป็นส่วนหนึ่งของ
การศึกษาวิชาโครงการพัฒนาระบบงาน หลักสูตรวิทยาศาสตรมหาบัณฑิต (เทคโนโลยีสารสนเทศ)
ภาคเรียนที่ 2 ปีการศึกษา 2552

.....อาจารย์ที่ปรึกษา
(ผศ. อัครินทร์ คุณกิตติ)

.....กรรมการสอบ
(ผศ. ดร. โอฬาร วงศ์วิรัตน์)

.....กรรมการสอบ
(ดร. สุขสันต์ พาณิชพาพิบูล)

หัวข้อ	การพัฒนาอุปกรณ์ให้บริการเครือข่ายเสมือนส่วนตัว
นักศึกษา	นายเฉลิมศักดิ์ เครือวัลย์
รหัสนักศึกษา	50066433
ปริญญา	วิทยาศาสตรมหาบัณฑิต
สาขาวิชา	เทคโนโลยีสารสนเทศ
แขนงวิชา	วิทยาการสารสนเทศ
ปีการศึกษา	2552
อาจารย์ที่ปรึกษา	ผศ.อัครินทร์ คุณกิตติ

บทคัดย่อ

เนื่องจากการติดต่อสื่อสารผ่านเครือข่ายคอมพิวเตอร์เป็นที่นิยมมากและการติดต่อสื่อสารผ่าน Internet เป็นที่นิยมอย่างแพร่หลาย เทคโนโลยีเครือข่ายเสมือนส่วนตัวก็เป็นอย่างหนึ่งที่ทำให้สามารถใช้ Internet จากบ้านหรือที่ไหนที่อยู่ไกลจากองค์กร เราสามารถใช้เทคโนโลยีนี้ในการเข้าถึงข้อมูลภายในองค์กรของได้และมีความปลอดภัยแต่ราคาของอุปกรณ์ให้บริการเครือข่ายเสมือนราคาสูงและปัจจุบันมี OPENSOURCE ดังนั้นการที่เอา OPENSOURCE ก็มีข้อจำกัดที่การจัดการค่อนข้างยากดังนั้นจึงมีการพัฒนา OPENSOURCE โดยทำการพัฒนาบน Unix และใช้ภาษาคอมพิวเตอร์ในการพัฒนาระบบจัดการเพื่อให้ได้ระบบที่สามารถให้บริการเครือข่ายเสมือนส่วนตัวแลสามารถจัดการได้อย่างสะดวกและง่าย

Title	A development of Virtual Private Network
Student	Mr.Chalermsak Krourwan
Student ID.	50066433
Degree	Master of Science in Information Technology
Program	Information Technology
Major	Information Science
Academic Year	2009
Advisor	Asst. Prof. Akharin Khunkitti

ABSTRACT

Communication Technology increase very high and Internet is the most famous in Communications. Technology Virtual Private Network can help you to access data where is in your Office from your home with the internet and VPN is security but VPN is very high cost so you can use OPENSOURCE but a limit of OPENSOURCE is very difficult so I developed system by use operation system is Unix and develop management system with computer language after that you will have management virtual private network system which can service VPN and easy to use with Client and Administrator

กิตติกรรมประกาศ

โครงการพัฒนาระบบงานนี้สำเร็จลุล่วงไปด้วยดี โดยได้รับความสนับสนุนจากบุคคลหลายฝ่าย ข้าพเจ้าจึงขอขอบคุณบุคคลดังต่อไปนี้

- บิดา มารดา พี่ที่ให้ความช่วยเหลือ ดูแล และให้กำลังใจตลอดมา
- อาจารย์อัครินทร์ คุณกิตติ อาจารย์ที่ปรึกษาโครงการที่ให้คำปรึกษา ชี้แนะแนวทาง ข้อบกพร่องในการพัฒนาระบบงานนี้
- คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง และคณาจารย์ทุกท่าน ที่ให้การอบรมสั่งสอนความรู้แก่ข้าพเจ้ามาโดยตลอด
- เพื่อนและพี่ร่วมรุ่น IS ที่ร่วมเรียนและให้คำปรึกษาพร้อมกับฝ่าฟันอุปสรรคมาด้วยกัน

เฉลิมศักดิ์ เครือวัลย์

ผู้จัดทำ

สารบัญ

หน้า

บทคัดย่อภาษาไทย..... I

บทคัดย่อภาษาอังกฤษ.....II

กิตติกรรมประกาศ.....III

สารบัญ.....IV

สารบัญตาราง.....VI

สารบัญรูป.....VII

บทที่ 1 บทนำ.....1

1.1 ความเป็นมาและความสำคัญของปัญหา..... 1

1.2 ความมุ่งหมายและวัตถุประสงค์ของการศึกษา.....1

1.3 ขอบเขตการวิจัย..... 1

1.4 ขั้นตอนการศึกษา..... 1

1.5 ประโยชน์ที่คาดว่าจะได้รับ.....2

บทที่ 2 พัฒนาอุปกรณ์ให้บริการเครือข่ายเสมือนส่วนตัว.....3

2.1 หลักการทำงานของอุปกรณ์ให้บริการเครือข่ายเสมือนส่วนตัว.....3

2.2 โปรแกรม OpenVPN 3

2.1.1 ขั้นตอนการสร้าง Tunneling และส่งข้อมูล.....4

2.3 SSL (Secure Socket Layer) 5

2.4 Encryption(การเข้ารหัสข้อมูล) 7

2.4.1 Symmetric Encryption 7

2.4.1.1 Data Encryption Standard (DES) 8

2.4.1.2 International Data Encryption Algorithm (IDEA) 8

2.4.2 Asymmetric Encryption 8

2.4.2.1 RSA 8

2.5 ระบบปฏิบัติการ FreeBSD (FreeBSD Operating System) 8

สารบัญ (ต่อ)

หน้า

บทที่ 3 การวิเคราะห์และออกแบบระบบ

3.1 ความต้องการของระบบงานใหม่.....10

3.2 กระบวนการทำงานโดยใช้ไฟล์ Configuration.....10

3.3 ระบบจัดการเครือข่ายเสมือนส่วนตัว.....13

3.4 การออกแบบฐานข้อมูลจากไฟล์ Configuration.....18

บทที่ 4 การทำงานของระบบ.....21

4.1 เครื่องมือที่ใช้ในการพัฒนาระบบ.....21

4.2 เครื่องมือที่ใช้ในการพัฒนาระบบ.....22

4.3 การพัฒนา Shell Script ของ OPENVPN.....23

4.4 การพัฒนาระบบจัดการเครือข่ายเสมือนผ่านเว็บไซต์.....30

4.4.1 การเพิ่มไฟล์ Configuration ของ Server.....30

4.4.2 การเพิ่มผู้ใช้งานระบบ.....33

4.4.3 การสร้าง Key ของ Server.....34

บทที่ 5 สรุปผลการทำงานของระบบ.....35

5.1 การทดสอบโครงการ.....35

5.2 ผลสรุปจากการทดสอบโครงการ.....37

5.3 ผลสรุปจากการพัฒนาโครงการ.....37

5.4 แนวทางการพัฒนาต่อ.....38

บรรณานุกรม.....39

ภาคผนวก.....40

ภาคผนวก ก. การติดตั้งโปรแกรมที่เกี่ยวข้อง.....40

ภาคผนวก ข. การคู่มือการใช้งานระบ.....43

ประวัติผู้เขียน.....64

สารบัญตาราง

ตารางที่ หน้า

3.1 รายละเอียดตาราง tb_user..... 18
3.2 รายละเอียดตาราง tb_authen..... 19
3.3 รายละเอียดตาราง tb_config 19
3.4 รายละเอียดตาราง tb_config_push 20
3.5 รายละเอียดตาราง tb_config_option 20

สารบัญรูป

รูปที่ หน้า

2.1 แสดงหลักการทำงานของอุปกรณ์ให้บริการเครือข่ายเสมือนส่วนตัว.....3

2.2 แสดง SSL HEADER 5

2.3 แสดง Packet ของ TUN 5

2.4 แสดง Packet ของ TAP.....5

2.5 แสดงการทำงานของ SSL 6

2.6 แสดงการทำงานของ Symmetric Encryption 7

2.7 แสดงการทำงานของ Asymmetric Encryption 8

3.1 แสดง Context Diagram 13

3.2 แสดง Data Flow Diagram Level 1.....13

3.3 แสดง Data Flow Diagram Level 2 ของ การสร้างไฟล์ Server's Configuration.....14

3.4 แสดง Data Flow Diagram Level 2 ของ การสร้างไฟล์ Client's Configuration 14

3.5 แสดง Data Flow Diagram Level 2 ของ การสร้าง Client's Key.....15

3.6 แสดง Data Flow Diagram Level 2 ของ การสร้าง Server's Key.....15

4.1 แสดง Flow Chart ของ การสร้าง Server's Key.....16

4.2 แสดง Flow Chart ของ การสร้าง Client's Key 17

4.3 แสดง ER Diagram.....18

5.1 แสดงแบบของการทดสอบ.....35

5.2 แสดง TAP Interface 36

5.3 แสดง TUN Interface.....36

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ในปัจจุบันเทคโนโลยีการติดต่อสื่อสารก้าวไกลไปมากและการสื่อสารกันโดย computer network ก็ได้รับความนิยมมากในปัจจุบัน ตัวอย่างเช่น พนักงานออกไปทำงานนอกองค์กรและต้องการใช้ทรัพยากรภายในองค์กรผ่าน Internet สามารถทำได้โดยใช้เทคโนโลยี VPN ในการทำงานเข้ามาใช้ในการทำงานซึ่งจะทำให้พนักงานสามารถเข้าถึงทรัพยากรภายในองค์กรได้และข้อมูลมีความปลอดภัยซึ่งเนื่องจากอุปกรณ์ให้บริการ VPN มีราคาสูงจึงพัฒนาอุปกรณ์ VPN เองเพื่อลดค่าใช้จ่าย

1.2 ความมุ่งหมายและวัตถุประสงค์ของการศึกษา

โครงการพัฒนาอุปกรณ์ให้บริการเครือข่ายเสมือนส่วนตัวมีวัตถุประสงค์ดังต่อไปนี้

- เพื่อพัฒนาเครื่องมือในการจัดการเทคโนโลยีเครือข่ายเสมือนส่วนตัวประเภท Software ที่มีชื่อว่า OpenVPN ซึ่งติดตั้งบนระบบปฏิบัติการ FreeBSD
- เพื่อลดขั้นตอนและความยุ่งยากในการจัดการและใช้งานเครือข่ายส่วนตัวเสมือนของ OpenVPN ให้ผู้ใช้มีความสะดวกสบาย
- เพื่อศึกษาเทคโนโลยีเครือข่ายเสมือนส่วนตัวประเภท Software ที่มีชื่อว่า OpenVPN

1.3 ขอบเขตของการศึกษา

โครงการพัฒนาอุปกรณ์ให้บริการเครือข่ายเสมือนส่วนตัวมีขอบเขตของการศึกษาดังต่อไปนี้

- ศึกษาหลักการทำงานของ VPN แบบ Client-to-Site
- ศึกษาในส่วนของระบบปฏิบัติการ FreeBSD
- ศึกษาในส่วนของการพัฒนาระบบด้วยภาษา PHP , MySQL , Java Script , Ajax
- ศึกษาในส่วนของ Openvpn's software

1.4 ขั้นตอนของการศึกษา

โครงการพัฒนาอุปกรณ์ให้บริการเครือข่ายเสมือนส่วนตัวมีขั้นตอนของการศึกษาดังต่อไปนี้

- ศึกษาการติดตั้งระบบปฏิบัติการ FreeBSD
- ศึกษาการติดตั้ง Openvpn บน FreeBSD
- ศึกษาการ Configuration Openvpn บน FreeBSD
- ศึกษาการติดตั้งและให้บริการ Web Service โดย Apache บน FreeBSD
- ศึกษาการพัฒนา Web Service โดย PHP,MySQL,Ajax,CSS,Java Script

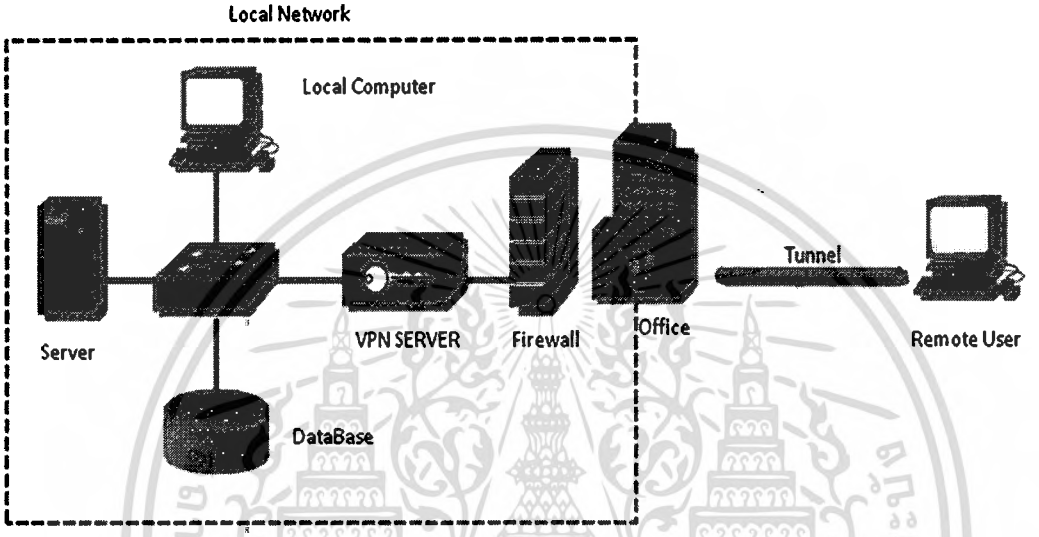
1.5 ประโยชน์ที่คาดว่าจะได้รับ

โครงการพัฒนาอุปกรณ์ให้บริการเครือข่ายเสมือนส่วนตัวมีประโยชน์ที่คาดว่าจะได้รับดังต่อไปนี้

- อุปกรณ์ให้บริการเครือข่ายเสมือนส่วนตัวแบบ Client-to-Site
- สามารถลดปัญหาในการจัดการไฟล์ Configuration ของ Remote User
- สามรถลดปัญหาเรื่องความยุ่งยากและซับซ้อนในการ Configuration OpenVPN ของผู้ดูแลระบบ
- ลดค่าใช้จ่ายในการซื้ออุปกรณ์ให้บริการเครือข่ายเสมือนส่วนตัว

บทที่ 2
พัฒนาอุปกรณ์ให้บริการเครือข่ายเสมือนส่วนตัว

2.1 หลักการทำงานของอุปกรณ์ให้บริการเครือข่ายเสมือนส่วนตัว



รูปที่ 2.1 แสดงหลักการทำงานของอุปกรณ์ให้บริการเครือข่ายเสมือนส่วนตัว

Remote User ต้องการเข้าถึงทรัพยากรภายในองค์กร โดยติดต่อผ่าน Internet มายัง VPN Server เพื่อทำการแลกเปลี่ยน KEY ที่ใช้ในการติดต่อระหว่าง VPN Server และ Remote User เมื่อแลกเปลี่ยนเสร็จแล้วการติดต่อระหว่าง Remote User และ Office จึงเสมือนมีท่อทำการห่อหุ้มเอาไว้หรือที่เรียกว่า Tunneling ซึ่งข้อมูลที่ถูกส่งภายในท่อนี้จะได้รับการเข้ารหัสจึงทำให้ข้อมูลมีความปลอดภัย ซึ่งเมื่อส่งข้อมูลมายัง VPN Server แล้ว VPN Server จะทำหน้าที่ในการส่งข้อมูลไปยัง Local Network ปลายทางที่มี Interface ติดต่อกับ VPN Server

2.2 โปรแกรม OpenVPN

โปรแกรม OpenVPN เป็นโปรแกรมให้บริการเครือข่ายเสมือนส่วนตัว(VPN)ซึ่งเป็น Open Source จึงไม่ต้องเสียค่าใช้จ่ายใดแต่การตั้งค่า Configuration ค่อนข้างยากซึ่งต้องทำทั้งฝั่งของ Server และ Client และก่อนจะทำการติดต่อนั้นจะต้องทำการสร้าง Key เพื่อใช้ในการติดต่อ

OpenVPN เป็น Software Based VPN ที่เป็น Open Source โดยที่ตอบสนองต่อจุดประสงค์หลักของความปลอดภัย คือ CIA (Confidentiality, Integrity, Availability) ข้อดีของ OpenVPN

- สามารถทำงานบน Layer 2 หรือ Layer 3 กล่าวคือ สามารถเลือกได้ว่าเราต้องการจะเข้ารหัสที่ Layer 2 (Ethernet Frame) หรือ Layer 3 (Transport Layer)

- สามารถทำงานร่วมกับ Firewall ถึงแม้ว่าระบบทำการสร้าง tunnel ไปแล้วแต่ firewall ก็สามารถตรวจสอบได้ผ่าน port และสามารถทำงานผ่าน Firewall ได้เกือบทุกๆประเภทและถ้าต้องการให้ OpenVPN สามารถผ่านได้ก็แค่เปิด port แค่ port ของ OpenVPN แค่ port เดียว
- สามารถใช้งานบน NAT ได้
- สามารถติดตั้งได้บนทุก platform

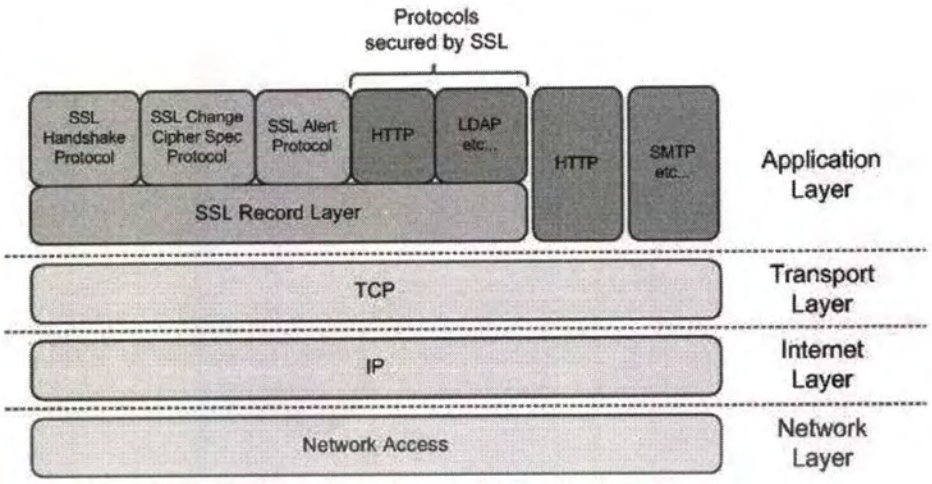
OpenVPN Version 2.0 เป็น Version ล่าสุดและได้เลือกมาใช้ในการพัฒนาระบบซึ่งมีส่วนที่เพิ่มเติมมาอีกดังต่อไปนี้

- สามารถรองรับการทำงานแบบ Multi-Client Support
- มีคำสั่ง pull/push ที่ช่วยจัดการตั้งค่า network ของ client หลังจากที่ได้ทำการเชื่อมต่อกับ server เรียบร้อยแล้ว
- มี Management Interface โดยใช้งานผ่าน Telnet ได้

OpenVPN ทำงานในระดับ Application Layer โดยการใช้ SSL (ต่อมาถูกพัฒนาจนเป็น TLS) และสร้าง Tunnel โดยใช้ TUN/TAP Adapter และใช้โปรโตคอล TCP/UDP ในการส่งข้อมูล

2.2.1 ขั้นตอนการสร้าง Tunneling และส่งข้อมูล

- Application จะทำการส่งข้อมูลไปที่ Private Network โดยใช้ IP ต้นทางเป็น Private IP และปลายทางเป็น IP ของ Host ที่อยู่ใน Private Network
- เมื่อเริ่ม Run Application นั้น OpenVPN จะทำการสร้างกุญแจใช้สำหรับการเข้ารหัสข้อมูลมา 2 อัน โดยอันแรกอยู่ที่ ไคลเอ็นต์ (Client) ส่วนอันที่ 2 อยู่ที่ VPN เซิร์ฟเวอร์ (Server) กุญแจที่ได้นั้นมาจาก Function ของ OpenSSL Library
- ในการส่งข้อมูลจาก ไคลเอ็นต์ (Client) ไปยัง เซิร์ฟเวอร์ (Server) นั้นจะทำการเข้ารหัสข้อมูลโดยเข้ารหัสแบบ RSA
- เมื่อข้อมูลถูกเข้ารหัสเสร็จก็จะถูกส่งโดยใช้ IP เป็น IP จริงที่อยู่ที่ ไคลเอ็นต์ (Client) และ เซิร์ฟเวอร์ (Server) ผ่านAdapter ที่ใช้ในการสร้าง Tunneling โดย Adapter นั้นมี 2 แบบคือ TUN และ TAP



รูปที่ 2.2 แสดง SSL HEADER

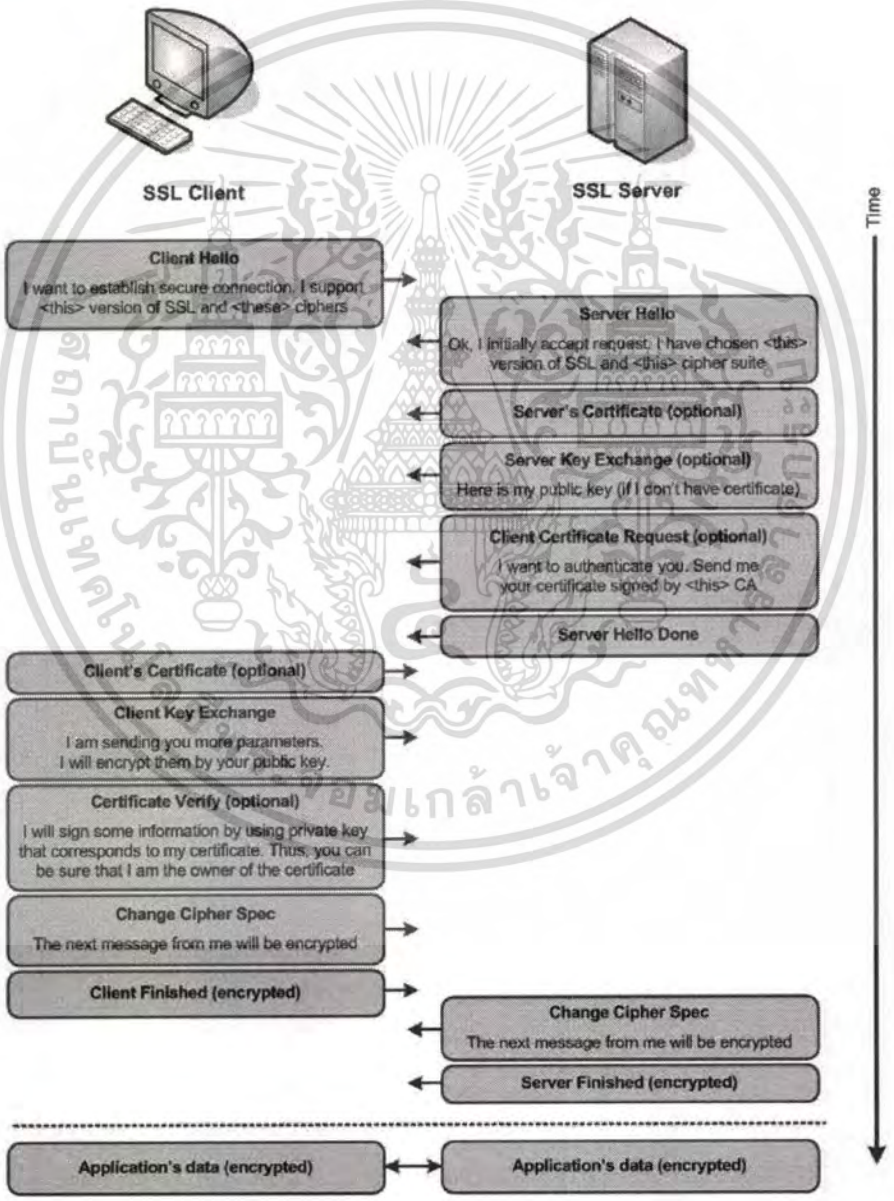
จากรูปแสดงรูปแบบการเข้ารหัสแบบ SSL ซึ่งอยู่บน TCP/IP Model ซึ่งแสดงให้เห็นว่า SSL ทำงานบน Application Layer เช่นเดียวกับ OpenVPN ที่ทำงานผ่าน Software

รูปที่ 2.3 แสดง Packet ของ TUN

รูปที่ 2.4 แสดง Packet ของ TAP

2.3 SSL (Secure Socket Layer)

เป็นโปรโตคอลที่ใช้สำหรับเข้ารหัสข้อมูลและการพิสูจน์ตัวตนระหว่าง เซิร์ฟเวอร์ (Server) กับ ไคลเอ็นต์ (Client) การทำงานของโปรโตคอลจะเริ่มจากการเจรจาเพื่อตกลงเกี่ยวกับอัลกอริทึมกับคีย์ที่จะใช้สำหรับการเข้ารหัสข้อมูลรวมถึงขั้นตอนการพิสูจน์ตัวตน และเมื่อตกลงกันเกี่ยวกับอัลกอริทึมและคีย์ได้แล้ว เซิร์ฟเวอร์ (Server) และ ไคลเอ็นต์ (Client) ก็เริ่มการติดต่อโดยใช้ข้อมูลที่ติดต่อกันไว้ SSLนั้นถูกพัฒนาโดยบริษัท Netscape ซึ่งต่อมาก็ถูกนำมาพัฒนาโดย IETF จนได้โปรโตคอล TLS (Transport Layer Security) นั่นเอง



รูปที่ 2.4 แสดงการทำงานของ SSL

อธิบายขั้นตอนการทำงานของ SSL

1. Client ทำการติดต่อไปยัง Server เพื่อร้องขอการติดต่อ
2. เมื่อ Server ได้รับการร้องขอแล้วจะตอบกลับไปว่าจะเลือกใช้ SSL Version ไหน
3. ทำการส่ง Public Key ของ Server ไปยัง Client
4. บอกให้ Client ทำการส่ง Public Key กลับมาให้ Server ด้วย
5. Client ได้รับข้อความจาก Server และทำการส่ง Public Key ของตัวเองกลับไปยัง Server โดยทำการเข้ารหัสโดย Public Key ของ Server
6. เมื่อทำการแลกเปลี่ยน Key เรียบร้อยแล้วแสดงว่า Application's data ได้ทำการเข้ารหัสเรียบร้อยแล้ว

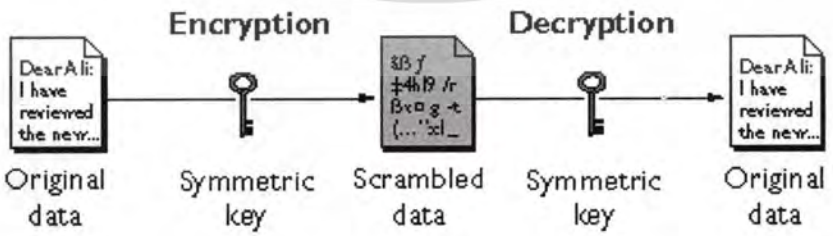
2.4 Encryption(การเข้ารหัสข้อมูล)

การเข้ารหัสข้อมูล (Data Encryption) การเข้ารหัสข้อมูล คือการนำข้อมูลปกติที่อยู่ในรูปของตัวอักษรธรรมดา มาผ่านการเข้ารหัสทำให้ได้ข้อมูลออกมาในอีกรูปแบบหนึ่งซึ่งจะไม่มีความหมาย อ่านไม่ออกและแปลกลับไปหาข้อมูลเดิมไม่ได้หากไม่มีรหัสลับที่ถูกต้อง ดังนั้นการเข้ารหัสข้อมูลจึงเป็นการรักษาความปลอดภัยของข้อมูลอย่างหนึ่งซึ่งการเข้ารหัสข้อมูลแบ่งออกได้เป็น 2 ประเภทคือ

- Symmetric Encryption
- Asymmetric Encryption

2.4.1 Symmetric Encryption

เป็นการเข้าและถอดรหัสข้อมูลโดยใช้รหัสลับตัวเดียวกันโดยคีย์ (Key) ที่ใช้จะมีความยาวคงที่ การไหลของข้อมูลเป็นเหมือนดังรูป



รูปที่ 2.5 แสดงการทำงานของ Symmetric Encryption

การเข้ารหัสข้อมูลแบบ Symmetric Encryption นี้มีหลายชนิดแต่ที่ยกมาอธิบายนี้ก็มี DES (Data Encryption Standard) และ IDEA (International Data Encryption Algorithm)

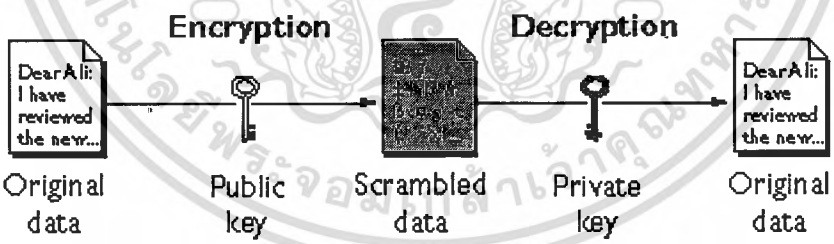
2.4.1.1 Data Encryption Standard (DES) เป็นการเข้ารหัสข้อมูลในชั้นที่มีความลับน้อย ซึ่ง DES นั้นถูกพัฒนาโดย IBM และเป็นอัลกอริทึมที่เคยนิยมกันอย่างแพร่หลาย DES นั้นประกอบด้วย 2 ส่วนคือ อัลกอริทึมและคีย์ (Key) โดย คีย์ จะมีขนาด 56 บิต และจะทำการเข้ารหัสข้อมูลทีละ 64 บิต โดยมีขั้นตอนการทำงานทั้งหมด 18 ขั้นตอนซึ่งขั้นตอนแรกกับขั้นตอนสุดท้ายนั้นเป็นการสลับบิต (Permutation) เท่านั้น

2.4.1.2 International Data Encryption Algorithm (IDEA) เป็นการเข้ารหัสและถอดรหัสข้อมูลประเภท Symmetric Encryption แบบ Block Cipher ชนิดหนึ่ง โดย IDEA จะใช้รหัสลับ 128 บิตในการเข้ารหัสข้อมูล ซึ่งมีผลให้การเข้ารหัสข้อมูลมีความปลอดภัยมากกว่า DES ที่ใช้ 56 บิตมาก

2.4.2 Asymmetric Encryption

เป็นการเข้าและถอดรหัสข้อมูลโดยใช้รหัสลับโดยใช้ คีย์คนละชุดกันโดย ชุดหนึ่งจะใช้ในการเข้ารหัสในขณะที่อีกตัวจะใช้ในการถอดรหัส ซึ่งคีย์ที่ใช้เรียกว่า Private Key และ Public Key โดยมีลักษณะดังรูปที่ 2.6 เทคนิคที่ใช้การเข้ารหัสแบบนี้ตัวอย่างที่มีก็เช่น RSA (ย่อมาจากชื่อของผู้ที่คิดค้นคือ Rivest, Shamir, Adleman)

2.4.2.1 RSA เป็นการเข้ารหัสแบบ Asymmetric ชนิดหนึ่ง โดยจะประกอบด้วยรหัส 2 ตัวคือ Public Key และ Private Key ซึ่ง Public Key นี้สามารถเปิดเผยได้แต่ Private Key นี้ไม่สามารถเปิดเผยได้รู้เฉพาะผู้ส่งเท่านั้น นอกจากนี้จะต้องเป็นคู่ของมันเท่านั้นจึงจะถอดรหัสได้



รูปที่ 2.6 แสดงการทำงานของ Asymmetric Encryption

2.5 ระบบปฏิบัติการ FreeBSD (FreeBSD Operating System)

ระบบปฏิบัติการ FreeBSD เป็นระบบปฏิบัติการที่มีเสถียรภาพอย่างสูง ระบบปฏิบัติการหนึ่ง สามารถนำมาประยุกต์ใช้งานได้ในหลายลักษณะ เช่น นำมาสร้างเป็น Web server, E-mail server, DNS server , รับการหมุนเข้าใช้งานจากโทรศัพท์ (Dial up), Database server และอื่นๆอีกมากมาย ในการศึกษานี้นำระบบปฏิบัติการ FreeBSD มาสร้างเป็น Router ด้วยโปรแกรม XORP (eXtensible Open Router Platform) นอกจากนี้ระบบปฏิบัติการ FreeBSD ยังมีความสามารถอีก

หลากหลาย สามารถ Download ตัวระบบปฏิบัติการมาใช้งานได้โดยไม่เสียค่าใช้จ่ายในการใช้งาน และยังมีเอกสารประกอบการใช้งานได้ที่เว็บไซต์ http://www.freebsd.org ผู้ใช้งานสามารถปรับปรุงและใช้งานตัวระบบปฏิบัติการ FreeBSD ได้ภายใต้ลิขสิทธิ์แบบ BSD

บทที่ 3

การวิเคราะห์และออกแบบระบบ

บทนี้จะกล่าวถึงวิธีการวิเคราะห์และออกแบบระบบเครือข่ายเสมือนส่วนตัวโดยใช้ระบบปฏิบัติการ Freebsd ที่ทำการติดตั้ง VPN Software ที่มีชื่อว่า OpenVPN และทำการพัฒนาระบบบน Web Base Application เพื่อใช้ในการจัดการ OpenVPN อย่างสะดวกสบายและมีประสิทธิภาพ

3.1 ความต้องการของระบบงานใหม่

- ผู้ดูแลระบบสามารถทำการสร้าง KEY ที่ใช้งานผ่านระบบได้
- ผู้ใช้งานสามารถ Download Key
- ผู้ใช้งานไม่ต้องทำการสร้างไฟล์ Configuration เอง
- ระบบทำการสร้างไฟล์ Configuration ให้กับ Server และ Client
- สามารถจัดการระบบผ่านหน้าจอ Interface ได้อย่างสะดวกและง่าย

3.2 กระบวนการทำงานโดยใช้ไฟล์ Configuration

การวิเคราะห์ระบบโดยเอาการทำงานของ OpenVPN โดยผ่านไฟล์ Configuration มาใช้ในการควบคุมและให้บริการ Server ดังนั้นเพื่อให้เราสามารถสร้างระบบที่สามารถจัดการ OpenVPN ได้จึงต้องเอาไฟล์ Basic Configuration มาทำการศึกษาและออกแบบทั้งของฝั่งของ Server และ Client มาศึกษาและทำการออกแบบและพัฒนาดังต่อไปนี้

ตัวอย่างไฟล์ Configuration ของ Server

```
;local a.b.c.d
port 1194
proto udp
dev tun
;dev-node MyTap
ca ca.crt
cert server.crt
key server.key  # This file should be kept secret
```

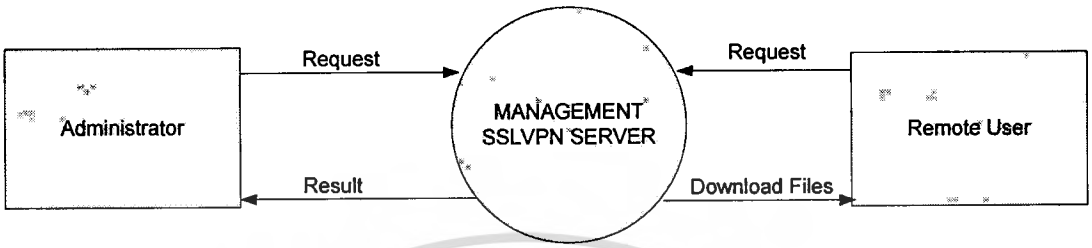
```
dh dh1024.pem
server 10.8.0.0 255.255.255.0
ifconfig-pool-persist ipp.txt
;server-bridge 10.8.0.4 255.255.255.0 10.8.0.50 10.8.0.100
;push "route 192.168.10.0 255.255.255.0"
;push "route 192.168.20.0 255.255.255.0"
;client-config-dir ccd
;route 192.168.40.128 255.255.255.248
;client-config-dir ccd
;route 10.9.0.0 255.255.255.252
;learn-address ./script
;push "redirect-gateway"
;push "dhcp-option DNS 10.8.0.1"
;push "dhcp-option WINS 10.8.0.1"
;client-to-client
;duplicate-cn
keepalive 10 120
;tls-auth ta.key 0 # This file is secret
;cipher BF-CBC        # Blowfish (default)
;cipher AES-128-CBC   # AES
;cipher DES-EDE3-CBC  # Triple-DES
comp-lzo
;max-clients 100
;user nobody
;group nobody
persist-key
persist-tun
status openvpn-status.log
;log         openvpn.log
;log-append  openvpn.log
verb 3
;mute 20
```

ตัวอย่างไฟล์ Configuration ของ Client

```
client
dev tun
;dev-node MyTap
proto udp
remote my-server-1 1194
;remote my-server-2 1194
;remote-random
resolv-retry infinite
nobind
;user nobody
;group nobody
persist-key
persist-tun
;http-proxy-retry # retry on connection failures
;http-proxy [proxy server] [proxy port #]
;mute-replay-warnings
ca ca.crt
cert client.crt
key client.key
;ns-cert-type server
;tls-auth ta.key 1
;cipher x
comp-lzo
verb 3
;mute 20
```

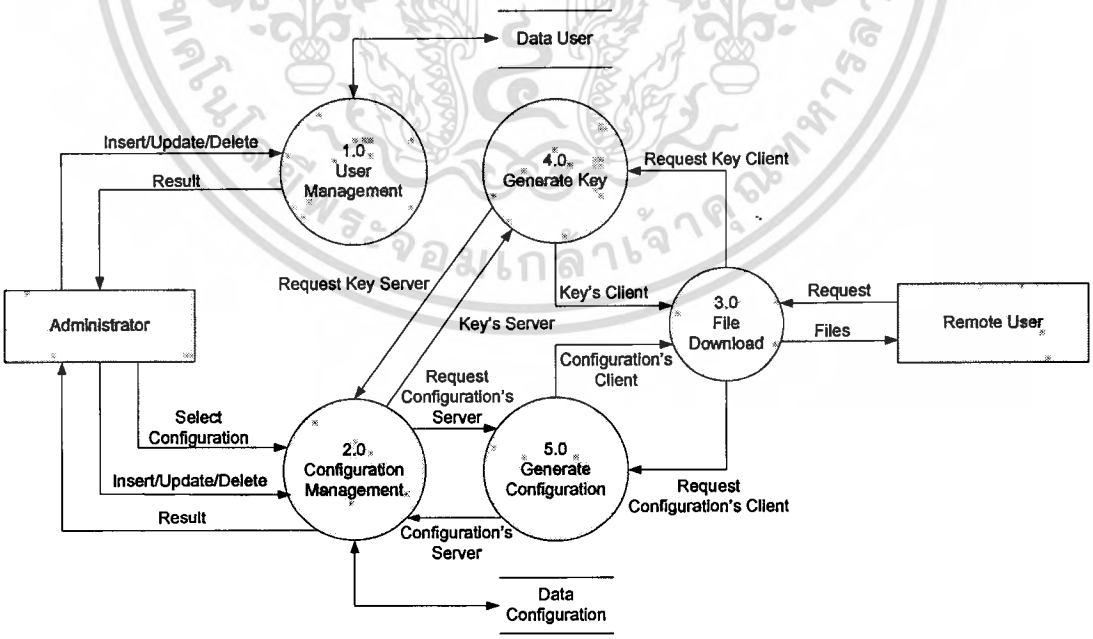
3.3 ระบบจัดการเครือข่ายเสมือนส่วนตัว

การออกแบบโดยใช้ Data Flow Diagram โดยเอาความต้องการของระบบมาทำการออกแบบเป็น Context Diagram ได้ดังนี้



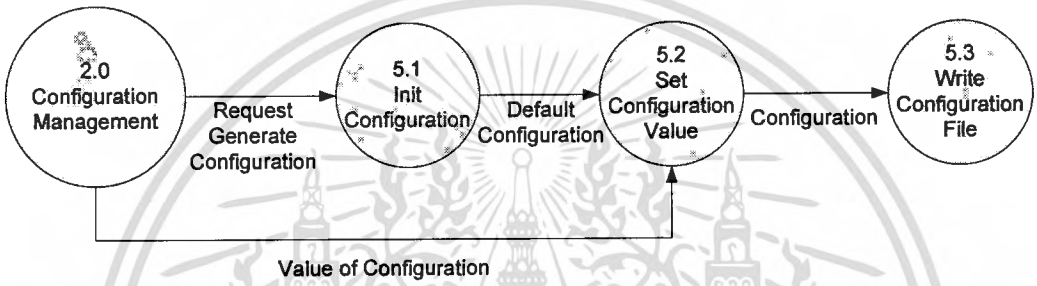
รูปที่ 3.1 แสดง Context Diagram

จากภาพ Context Diagram สามารถอธิบายได้ดังนี้ ระบบทำการติดต่อกับผู้ใช้งานสองกลุ่มคือ Administrator และ Remote User โดยที่ Administrator จะติดต่อกับระบบเพื่อทำการร้องขอให้ระบบทำการ สร้าง Key หรือเปิดปิดการให้บริการ Administrator สามารถทำการจัดการผู้ใช้งานใหม่ได้เช่น เพิ่ม ลบ แก้ไข และAdministrator สามารถจัดการเพิ่ม ลบ แก้ไขในส่วนไฟล์ Configuration ได้ส่วนกลุ่มของ Remote User จะติดต่อโดยการร้องขอให้ระบบทำการสร้าง Key และไฟล์ Configuration ที่ใช้ในการติดต่อและให้ทำการ Download



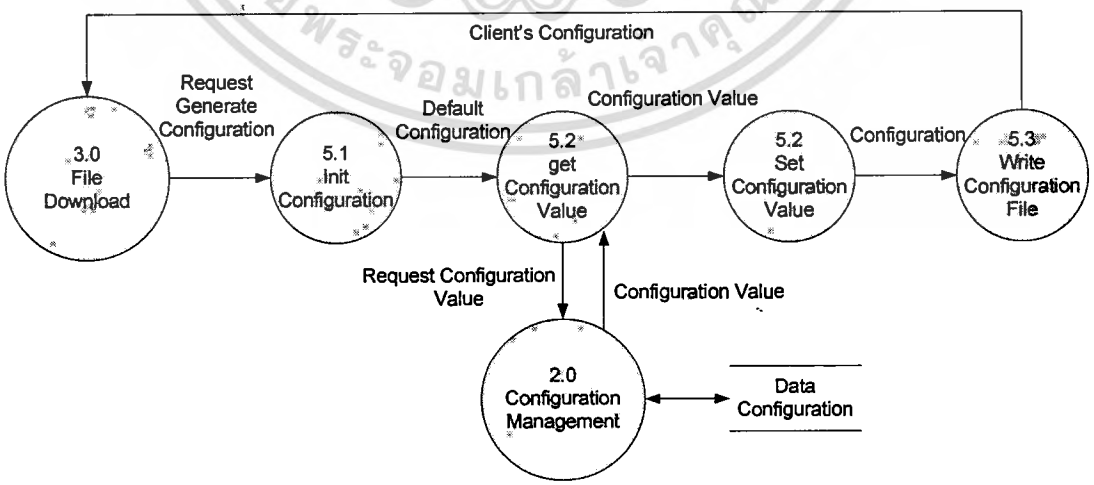
รูปที่ 3.2 แสดง Data Flow Diagram Level 1

จาก Data Flow Diagram Level 1 สามารถอธิบายได้ว่า Administrator ทำการเพิ่ม ลบ แก้ไข Administrator และทำการจัดการข้อมูลภายในฐานข้อมูลของ User และ Administrator สามารถจัดการเพิ่ม ลบ แก้ไข ไฟล์ Configuration ของ Server และทำการจัดการข้อมูลภายในของไฟล์ Configuration และถ้า Administrator ทำการร้องขอให้เลือกใช้ไฟล์ Configuration ไหนก็จะทำการสร้าง Configuration นั้นโดยรายละเอียดจะทำการเอาข้อมูลจากฐานข้อมูลและทำการสร้างไฟล์และหลังจากนั้นระบบจะทำการสร้าง Key ที่ใช้สำหรับ Server ส่วนกลุ่ม Remote User จะทำการร้องขอไฟล์ที่ใช้ในการติดต่อกับ Server เมื่อระบบได้รับการร้องขอจะทำการสร้างไฟล์และ Configuration หลังจากนั้นนำมารวมกันโดยการ Zip ไฟล์



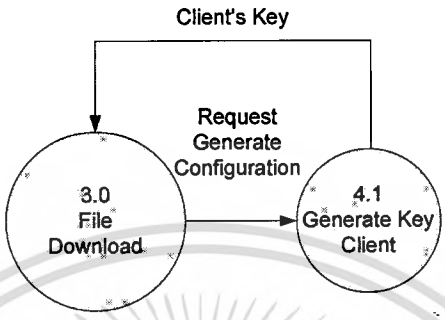
รูปที่ 3.3 แสดง Data Flow Diagram Level 2 ของ การสร้างไฟล์ Server's Configuration

จาก Data Flow Diagram Level 2 สามารถอธิบายได้ว่าการสร้างไฟล์ Configuration ของ Server นั้นขั้นแรกจะทำการกำหนดค่าเริ่มต้นขึ้นมาก่อนหลังจากนั้นทำการเอาค่าที่ใช้อยู่ปัจจุบันไปใช้งานและทำการเขียนลงไปในไฟล์ Configuration



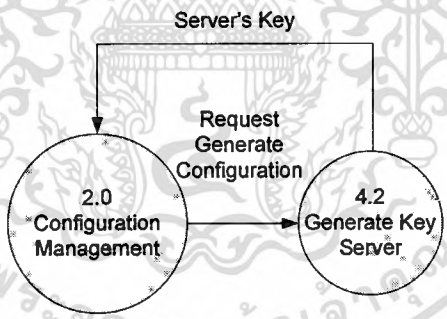
รูปที่ 3.4 แสดง Data Flow Diagram Level 2 ของ การสร้างไฟล์ Client's Configuration

- จาก Data Flow Diagram Level 2 สามารถอธิบายได้ว่าการสร้างไฟล์ Configuration ของ Client นั้นขั้นแรกจะทำการกำหนดค่าเริ่มต้นขึ้นมาก่อนหลังจากนั้นทำการเอาค่าที่ใช้อยู่ปัจจุบันของ Server มาเพื่อให้ได้ค่าที่ตรงกันระหว่าง Server และ Client หลังจากนั้นก็ทำเอาค่าเหล่านั้นไปใส่ใน format ของ Client และทำการสร้างไฟล์ Configuration ขึ้น



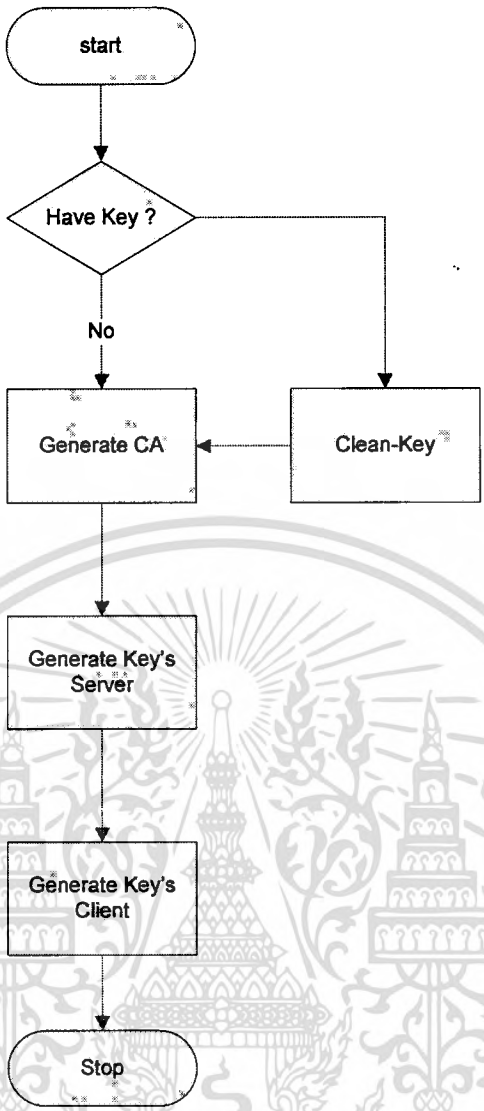
รูปที่ 3.5 แสดง Data Flow Diagram Level 2 ของ การสร้าง Client's Key

จาก Data Flow Diagram Level 2 สามารถอธิบายได้ว่าการสร้าง Key ของ Client หลังจากที่ Remote User ทำการ Request มายังระบบเพื่อขอทำการ Download Files เพื่อใช้ในการติดต่อหลังจากนั้นระบบจะทำการสร้าง Key



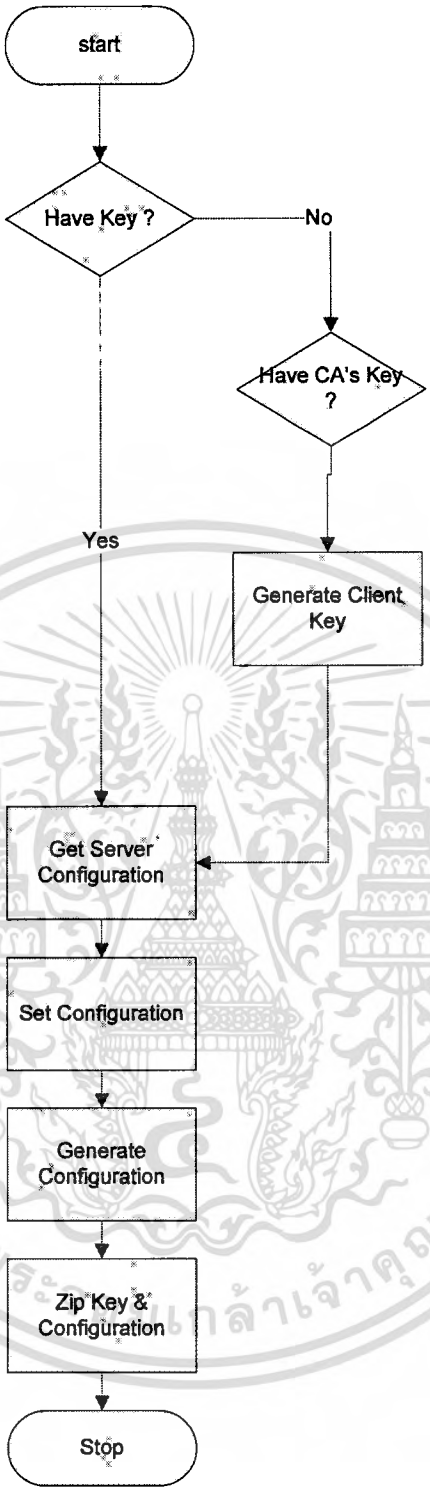
รูปที่ 3.6 แสดง Data Flow Diagram Level 2 ของ การสร้าง Server's Key

จาก Data Flow Diagram Level 2 สามารถอธิบายได้ว่าการสร้าง Key ของ Server หลังจากที่ Administrator ทำการร้องขอให้ระบบทำการสร้าง Key เพื่อไว้ใช้งานสำหรับ Server



รูปที่ 3.7 แสดง Flow Chart ของ การสร้าง Server's Key

โดยหลังจากที่ระบบได้รับการร้องขอให้สร้าง Key ขั้นแรกจะต้องทำการตรวจสอบว่ามี Key เก่าใช้งานอยู่หรือไม่ ถ้ามีอยู่แล้วจะทำการลบและทำการสร้าง Key ใหม่หลังจากนั้นค่อยทำการสร้าง Key ใหม่โดยเริ่มจากการสร้าง Certificate Authentication ซึ่งจะได้ ca.crt หลังจากนั้นจะทำการสร้าง Key สำหรับ Server ได้แก่ Server.key , Server.crt เมื่อทำการสร้าง Key สำหรับ Server เสร็จแล้วจากนั้นก็ทำการสร้าง dh ซึ่งจะได้ dh1024.pem



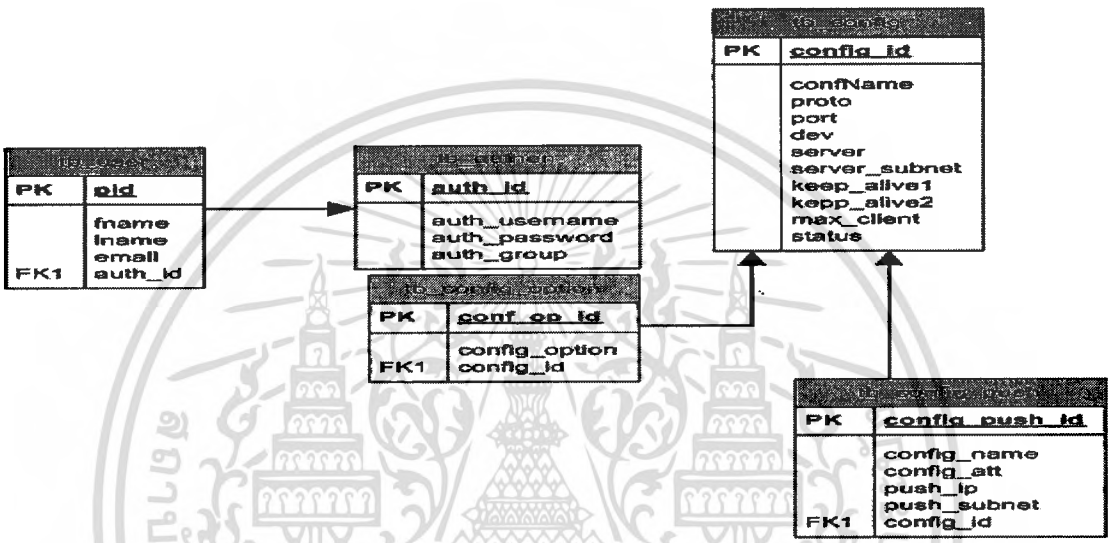
รูปที่ 3.8 แสดง Flow Chart ของ การสร้าง Client's Key

โดยหลังจากที่ระบบได้รับการร้องขอให้สร้าง Key ขั้นแรกจะต้องทำการตรวจสอบว่ามี Key เก่าใช้งานอยู่หรือไม่ ถ้ามีอยู่แล้วระบบจะไม่ทำการสร้าง Key แต่ถ้ายังไม่มี Key ก็จะทำการสร้าง Key ให้แต่ต้องตรวจสอบก่อนว่า Server ได้ทำการสร้าง Key แล้วหรือยังถ้าสร้างแล้วจะทำการทำการสร้าง Key หลังจากเสร็จสิ้นแล้วก็จะทำการสร้างไฟล์ Configuration โดยทำการเช็คจาก

Configuration ของ Server หลังจากนั้นจะทำการสร้างไฟล์ Configuration ของ Client และทำการ Zip ไฟล์รวมกับ Key

3.4 การออกแบบฐานข้อมูลจากไฟล์ Configuration

เนื่องจากการใช้งานระบบจำเป็นต้องทำงานผ่านไฟล์ Configuration ดังนั้นจึงจำเป็นต้องออกแบบให้สามารถเก็บข้อมูลของไฟล์ Configuration ได้เพื่อนำไปใช้ในการสร้างไฟล์ Configuration ของ Server และ Client



รูปที่ 3.9 แสดง ER Diagram

ตารางที่ 3.1 รายละเอียดตาราง tb_user

Field	Type	Null	Key	Detail	Ref .table
pid	Varchar(13)		PK	รหัสประจำตัวผู้ใช้งาน	
fname	Varchar(255)	n		ชื่อ	
lname	Varchar(255)	n		นามสกุล	
email	Varchar(255)	n		email	
auth_id			FK		tb_authen

ตารางที่ 3.2 รายละเอียดตาราง tb_authen

Field	Type	Null	Key	Detail	Ref .table
auth_id	Varchar(13)		PK	รหัสประจำตัวผู้ใช้งาน	
auth_username	Varchar(255)	n		ชื่อผู้ใช้งาน	
auth_password	Varchar(255)	n		รหัสผ่าน	
auth_group	Varchar(255)	n		กลุ่มผู้ใช้งาน	

ตารางที่ 3.3 รายละเอียดตาราง tb_config

Field	Type	Null	Key	Detail	Ref .table
config_id	Int(10)		PK	รหัสประจำตัวของ config	
confName	Varchar(255)			ชื่อ config	
proto	Varchar(255)	n		protocol	
port	Varchar(255)	n		port	
dev	Varchar(255)	n		Tun/tap	
server	Varchar(255)	n		Network ip	
server_subnet	Varchar(255)	n		Subnetmask	
keepalive1	Int(4)	n		ping	
keepalive2	Int(4)	n		timeout	
max_client	Int(2)	n		จำนวนผู้ใช้งาน	
status	Varchar(255)	n		สถานะของไฟล์ config ว่าถูกใช้งานหรือไม่	

ตารางที่ 3.4 รายละเอียดตาราง tb_config_push

Field	Type	Null	Key	Detail	Ref .table
config_push_id	Int(10)		PK	รหัสของคำสั่ง push	
config_name	Varchar(255)	n		ชื่อคำสั่งของ push	
config_att	Varchar(255)	n		ค่าของ push	
push_ip	Varchar(255)	n		Ip address	
push_subnet		n		subnetmask	
config_id			FK	รหัสประจำตัวของ config	tb_config

ตารางที่ 3.5 รายละเอียดตาราง tb_config_option

Field	Type	Null	Key	Detail	Ref .table
config_op_id	Int(10)		PK	รหัสประจำตัว Option	
config_option	Varchar(255)	n		ชื่อของ Option	
config_id	Varchar(255)		FK	รหัสประจำตัวของ config	tb_config

บทที่ 4
ขั้นตอนการพัฒนาระบบงาน

ในบทนี้จะกล่าวถึงรายละเอียดของการออกแบบโปรแกรม ขั้นตอนการพัฒนาระบบ เครื่องมือต่าง ๆ ที่ใช้ในการพัฒนาระบบ

4.1 การทำงานของระบบ

การทำงานของระบบแบ่งออกเป็น 2 ส่วนคือ ส่วนแรกคือส่วนการทำงานของผู้ดูแลระบบเครือข่ายเสมือนส่วนตัวซึ่งจะทำหน้าที่ในการดูแลการทำงานของระบบเช่น การจัดการไฟล์ Configuration เช่นการเพิ่ม ลบ แก้ไข และการจัดการ Key เช่นการสร้าง Key ใหม่การลบ Key ที่ใช้งานอยู่และการจัดการผู้ใช้งานระบบเช่น เพิ่ม ลบ แก้ไข และการจัดการการทำงานของระบบเช่นเปิดปิดการให้บริการเป็นต้นและอีกส่วนคือส่วนผู้ใช้งานจะต้องเข้ามาทำการระบุตัวตนกับตัวระบบหลังจากนั้นก็ทำงาน Download โปรแกรมและ Files ที่เอาไว้ใช้ในการติดต่อกับระบบ

การทำงานของการให้บริการเครือข่ายส่วนตัว นั้นจะถูกควบคุมด้วยไฟล์ Configuration ของ Server ซึ่งผู้ดูแลระบบทำการตั้งค่าต่างๆผ่านระบบ ดังนั้นจะต้องสามารถออกแบบให้ดูดูแลสามารถทำการเพิ่มรูปแบบการใช้งานได้หลายรูปแบบและสามารถเลือกใช้ได้ตามสถานะการณ์

การเตรียม Key สำหรับเครื่อง Server เพื่อให้บริการโดยคำสั่งที่ใช้สั่ง OpenVPN นั้นคือ Shell Script ซึ่งเดิมจะต้องถูกสั่งผ่าน Command Line ใน Shell ดังนั้นจึงทำการแก้ไขให้สามารถทำงานผ่านระบบได้

4.2 เครื่องมือที่ใช้ในการพัฒนาระบบ

เครื่องมือที่ใช้ในการพัฒนาระบบจัดการเครือข่ายเสมือนส่วนตัว

- FreeBSD 6.4
- PHP 5.0
- PHP mod SSH
- MySQL
- Apache22
- Ajax
- phpMyAdmin

4.2.1 FreeBSD 6.4

ระบบปฏิบัติการ FreeBSD เป็นฟรีเวอร์ชั่น ของ Berkeley UNIX เป็นระบบปฏิบัติการ UNIX ที่มีประสิทธิภาพสูงเหมาะสำหรับใช้เป็น Internet หรือ Intranet เซิร์ฟเวอร์ เนื่องจากมีความเสถียรภาพในการให้บริการทางด้านเครือข่ายสูง มีการจัดสรรการใช้หน่วยความจำที่ดี มีระบบรักษาความปลอดภัยสูง ให้เวลาในการตอบสนองต่อผู้ใช้ได้ดี นอกจากนี้ยังสามารถใช้ได้กับคอมพิวเตอร์ในหลายตระกูลเช่น x86 ,DEC Alpha, IA-64, PC-98 และ UltraSPARC เป็นต้น

4.2.2 Apache22

ต้นกำเนิดมาจากโปรแกรม NCSA httpd1.3 ได้รับการปรับปรุงและพัฒนาอย่างต่อเนื่อง จนอาจถือได้ว่าเป็นเว็บเซิร์ฟเวอร์ที่ดีที่สุดบน UNIX ในปัจจุบัน Apache เป็นเว็บเซิร์ฟเวอร์ที่ทำงานได้เร็ว มีความน่าเชื่อถือได้สูง และมีความสามารถอื่น

4.2.3 MySQL5.0

เป็น DBMS ที่ใช้ในการจัดการฐานข้อมูลเชิงสัมพันธ์ (Relational Database) ทำงานในรูปแบบไคลเอนต์/เซิร์ฟเวอร์ ซึ่งมีขนาดเล็กแต่มีประสิทธิภาพและความเร็วในการประมวลผลสูง ความสามารถโดยทั่วๆ ไปจะครอบคลุมความต้องการของโปรแกรมระบบงานนี้อย่างเพียงพอ จัดเป็นระบบฐานข้อมูลประเภท SQL-Base โดยที่ผู้ใช้สามารถใช้คำสั่ง SQL ในการสั่ง หรือใช้งานได้โดยไม่ต้องศึกษาคำสั่งเพิ่มเติมแต่อย่างใด นอกจากนี้ยังสนับสนุน API เพื่อใช้งานกับโปรแกรมอื่น ๆ มากมาย และยังสามารถรองรับข้อมูลขนาดใหญ่ได้อีกด้วย

ในการทำงานกับระบบงานนี้จำเป็นต้องมีการติดตั้งในส่วนของโปรแกรมที่เป็นเซิร์ฟเวอร์ก่อน หลังจากนั้นจึงทำการสร้างฐานข้อมูล, ตาราง และ กำหนดรูปแบบของข้อมูลที่ต้องการจัดเก็บในตารางรวมถึงคีย์หลักตามที่ได้ออกแบบไว้

4.2.4 PHP 5.0

ภาษา PHP จัดเป็นภาษา script ที่สามารถทำงานร่วมกับ HTML โดยสามารถเขียน script แทรกเข้าไปใน tag ภาษา HTML ได้ หรือสามารถเขียนเป็นไฟล์ PHP ก็ได้ โดย PHP เป็น open source ที่สามารถใช้งานได้กับหลายๆ ระบบปฏิบัติการ เช่น Windows , Linux , Unix เป็นต้น และยังสามารถรองรับการติดต่อกับฐานข้อมูลหลายๆ ชนิดด้วย

4.2.5 PHP Mod SSH

เพื่อให้ PHP สามารถใช้งาน SSH ได้โดยจะต้องทำการติดตั้งเพิ่มซึ่งสามารถดูรายละเอียดได้จาก www.php.net ได้ในหัวข้อ SSH2 เพื่อให้ใช้คำสั่งในการจัดการ SSH

4.2.6 AJAX

ภาษา Java Script ที่ทำงานฝั่ง Server โดยการทำการส่งไฟล์ที่ต้องการไปทำการประมวลผลฝั่ง Server และทำการส่งผลกลับมา นำมาใช้ในกรณีต้องการส่งไปเฉพาะบาง page ไปประมวลผลแล้วนำผมกลับมาโดยแสดงที่หน้าจอหลักโดยไม่ต้อง Refresh หน้าใหม่ทั้งหน้า

4.2.7 phpMyAdmin

ถูกเขียนภาษา PHP เพื่อใช้จัดการฐานข้อมูล MySQL โดยต้องทำการไปแก้ไขค่าใน inic.inc.php เพื่อให้สามารถติดต่อกับฐานข้อมูล MySQL ได้ซึ่ง phpMyADmin จะทำหน้าที่เหมือน DBMS เพื่อใช้ในการสร้างตาราง

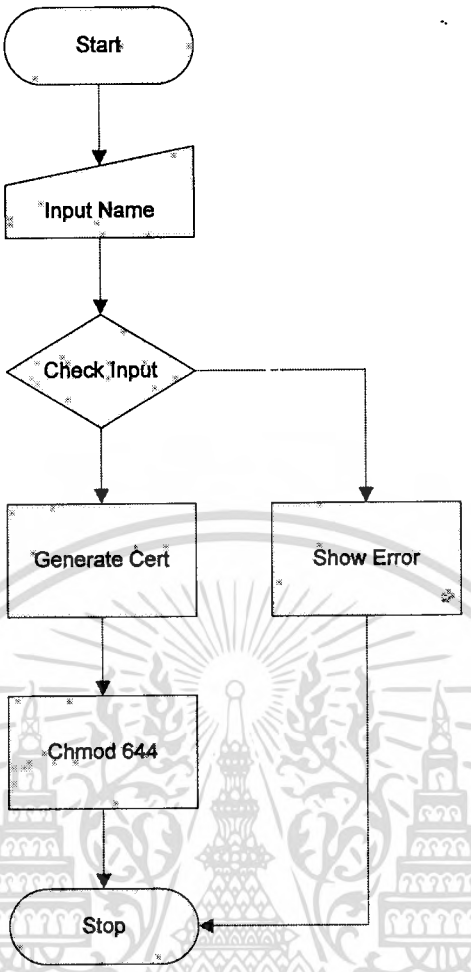
4.3 การพัฒนา Shell Script ของ OPENVPN

การพัฒนา Shell Script ของ OpenVPN ให้ทำงานผ่านระบบได้ก่อนอื่นการทำงานแบบเดิมไม่ใช่แบบ batch แต่จะเป็นการทำงานที่ interactive กับผู้ใช้งานดังนั้นจึงต้องทำการเปลี่ยนแปลง shell script ให้สามารถทำงานแบบ batch ได้

การทำงานโดยใช้ Shell Script ของ OpenVPN นั้นแต่ละไฟล์จะต้องมีการเรียกใช้ไฟล์ openssl.cnf และมีการตั้งค่าดังต่อไปนี้

ตัวอย่างไฟล์ build-ca.sh

```
. /usr/local/etc/openvpn/rsa/vars

export KEY_CNAME="server"

if test $KEY_DIR; then

cd $KEY_DIR && \
openssl req -batch -days 100 -nodes -new -x509 -keyout ca.key -out ca.crt -config $KEY_CO$
chmod 600 ca.key

else
    echo you must define KEY_DIR
fi
```



รูปที่ 4.1 แสดง Flow Chart แสดงขั้นตอนการทำงานของไฟล์ build-ca

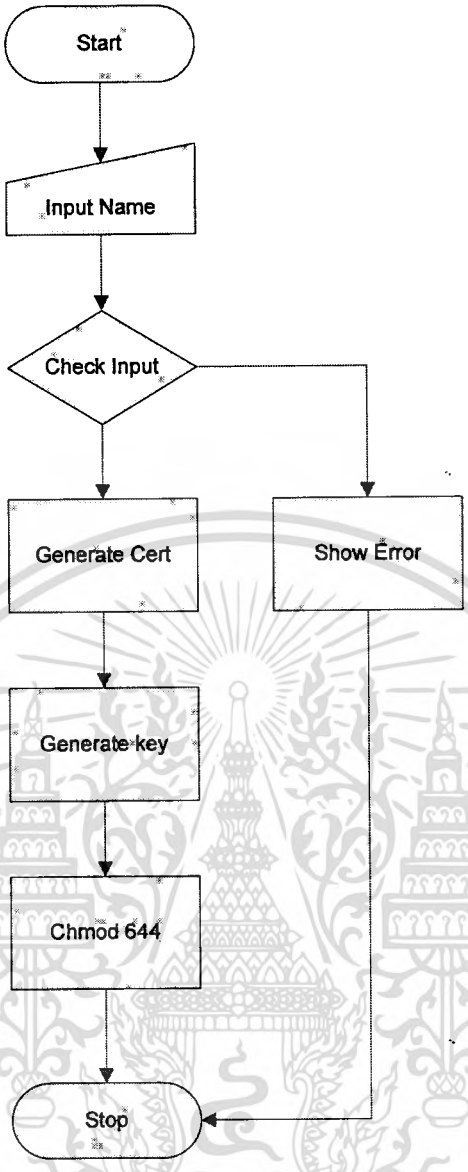
ขั้นตอนการทำงานของ build-ca

- ทำการใส่ชื่อ common name
- ทำการตรวจสอบว่าได้ใส่ชื่อมาหรือไม่ ถ้าไม่ก็จะแจ้งเตือนและออก
- ทำการสร้าง ca.cert
- ทำการเปลี่ยน mode เป็น 644

ตัวอย่างไฟล์ build-key-server.sh

```
. /usr/local/etc/openvpn/rsa/vars

export KEY_CNAME="server"

if test $# -ne 1; then
    echo "usage: build-key-server <name>";
```

```
    exit 1
fi
if test $KEY_DIR; then

cd $KEY_DIR && \
openssl req -days 100 -batch -nodes -new -keyout $1.key -out $1.csr -extensions server -config
$KEY_CONFIG && \
openssl ca  -days 100 -batch -out $1.crt -in $1.csr -extensions server -config $KEY_CONFIG
&& \
chmod 600 $1.key

else
    echo you must define KEY_DIR
fi
```



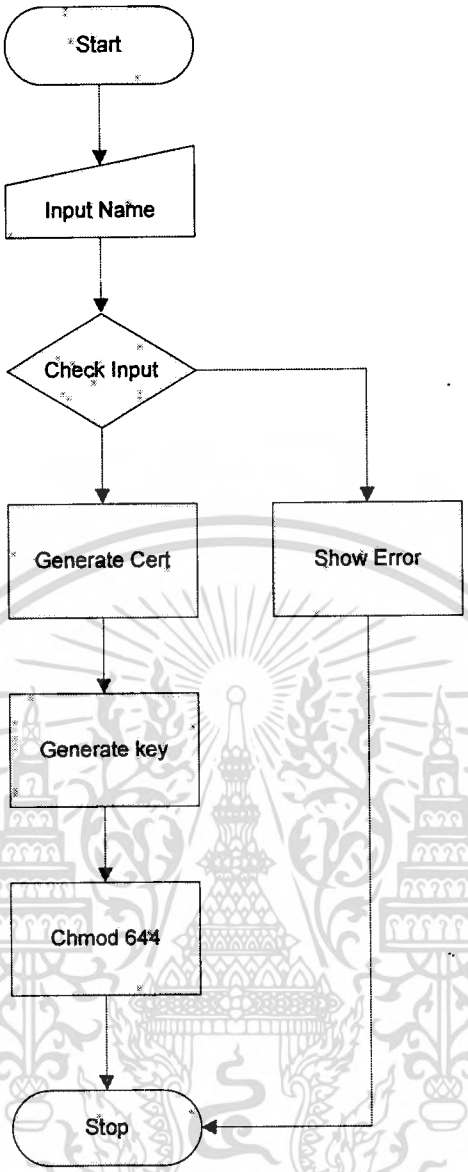
รูปที่ 4.2 แสดง Flow Chart แสดงขั้นตอนการทำงานของไฟล์ build-key-server

ขั้นตอนการทำงานของ build-key-server

- ทำการใส่ชื่อ common name
- ทำการตรวจสอบว่าได้ใส่ชื่อมาหรือไม่ ถ้าไม่ก็จะแจ้งเตือนและออก
- ทำการสร้าง cert
- ทำการสร้าง key
- ทำการเปลี่ยน mode เป็น 644

ตัวอย่างไฟล์ build-key.sh

```
. /usr/local/etc/openvpn/rsa/vars
if test $# -ne 1; then
    echo "usage: build-key <name>";
    exit 1
fi
export KEY_CNAME=$1

if test $KEY_DIR; then

cd $KEY_DIR && \
openssl req -days 100 -batch -nodes -new -keyout $1.key -out $1.csr -config $KEY_CONFIG
&& \
openssl ca -days 100 -batch -out $1.crt -in $1.csr -config $KEY_CONFIG && \
chmod 0775 $1.key

else
    echo you must define KEY_DIR
fi
```



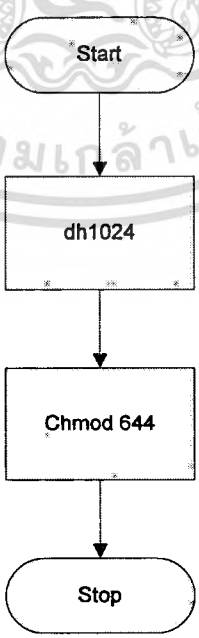
รูปที่ 4.3 แสดง Flow Chart แสดงขั้นตอนการทำงานของไฟล์ build-key

ขั้นตอนการทำงานของ build-key

- ทำการใส่ชื่อ common name
- ทำการตรวจสอบว่าได้ใส่ชื่อมาหรือไม่ ถ้าไม่ก็จะแจ้งเตือนและออก
- ทำการสร้าง cert
- ทำการสร้าง key
- ทำการเปลี่ยน mode เป็น 644

ตัวอย่างไฟล์ build-dh.sh

```
. /usr/local/etc/openvpn/rsa/vars

if test $# -ne 1; then
    echo "usage: build-key <name>";
    exit 1
fi
export KEY_CNAME=$1
if  test $KEY_DIR; then

cd $KEY_DIR && \
openssl req -days 100 -batch -nodes -new -keyout $1.key -out $1.csr -config $KEY_CONFIG
&& \
openssl ca -days 100 -batch -out $1.crt -in $1.csr -config $KEY_CONFIG && \
chmod 0775 $1.key

else
    echo you must define KEY_DIR
fi
```



รูปที่ 4.4 แสดง Flow Chart แสดงขั้นตอนการทำงานของไฟล์ build-key

ขั้นตอนการทำงานของ build-dh

- ทำการสร้าง dh1024.pem
- ทำการเปลี่ยน mode เป็น 644

ตัวอย่างไฟล์ vars.sh

```
export D="/usr/local/etc/openvpn/rsa"
export KEY_DIR=$D/keys
export KEY_SIZE=1024
export KEY_COUNTRY=TH
export KEY_PROVINCE=BANGKOK
export KEY_CITY=LADKRABANG
export KEY_ORG="DIPAC@KMITL"
export KEY_EMAIL="admin@admin.com"
```

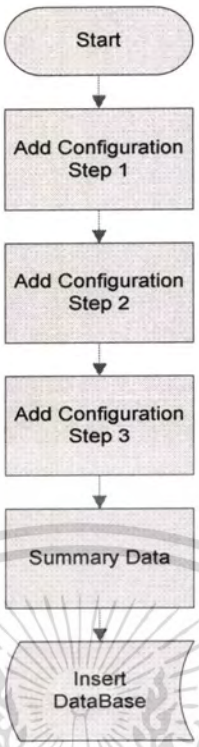
ใช้ในการทำการตั้งค่าของตัวแปรที่ใช้ในการทำการสร้าง Key ซึ่งจะเอาค่าตัวแปรไปใส่ให้ไฟล์ openssl.cnf เพื่อใช้ในการสร้าง Key โดยใช้คำสั่งสร้าง Key ของ Openssl ในการสร้าง Key แบบ RSA

4.4 การพัฒนาระบบจัดการเครือข่ายเสมือนผ่านเว็บไซต์

การทำงานในส่วนของการผู้ดูแลระบบสามารถทำการสร้างไฟล์ configuration ใหม่ได้และสามารถลบและแก้ไขได้และผู้ดูแลระบบจะต้องสามารถทำการเพิ่มลบแก้ไขผู้ใช้งานระบบได้และผู้ดูแลระบบสามารถสร้าง Key ไว้สำหรับ Server สำหรับผู้ใช้งานระบบจะต้องทำการสร้างให้เอง ซึ่งผู้ดูแลระบบสามารถสั่งการได้โดยผ่าน web browser และทำการ connect มายัง Server โดยผ่าน Internet หรือ intranet

4.4.1 การเพิ่มไฟล์ Configuration ของ Server

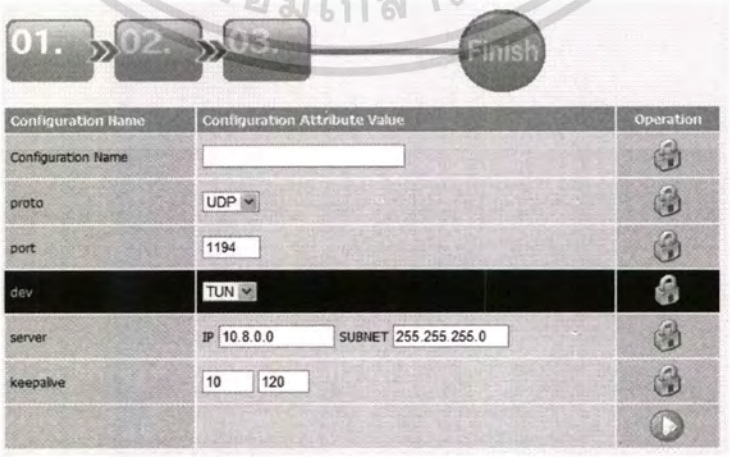
ผู้ดูแลระบบทำการเพิ่มไฟล์ Configuration ของ Server และทำการเก็บไว้ในฐานข้อมูลซึ่งจะนำมาใช้ในกรณีสร้างไฟล์ Configuration ของ Client โดยจะดึงเอาค่าที่จำเป็นต้องเหมือนกันระหว่าง Server และ Client และแต่ละบรรทัดของไฟล์ Configuration สามารถใส่ได้เฉพาะบางค่าเท่านั้นดังนั้นจึงได้ทำการออกแบบและพัฒนาเพื่อลดปัญหาการที่ผู้ดูแลระบบทำการใส่ค่าที่ผิดด้วย GUI ที่เข้าใจง่ายและขั้นแบ่งเป็นขั้นตอนดังต่อไปนี้



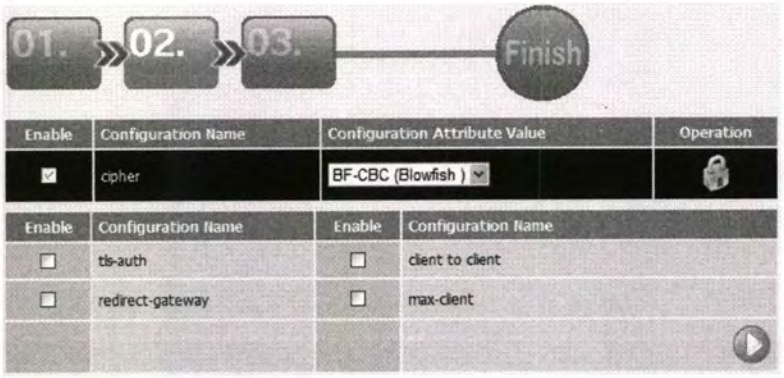
รูปที่ 4.5 แสดง Flow Chart แสดงขั้นตอนการทำงานของไฟล์ build-key-server

ขั้นตอนการทำงานของการเพิ่มไฟล์ Configuration

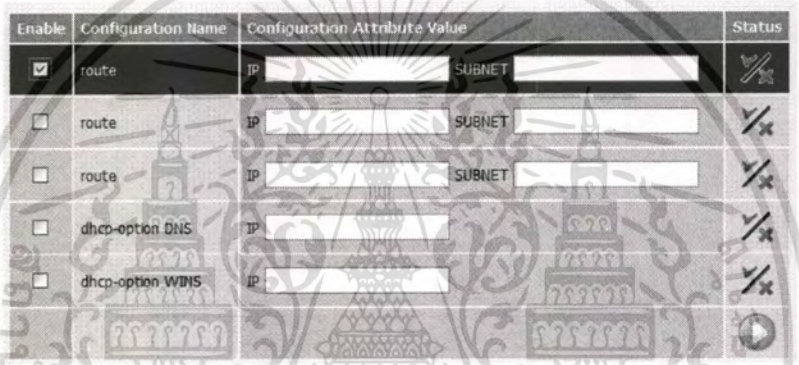
- ทำการเพิ่มไฟล์ configuration step 1
- ทำการเพิ่มไฟล์ configuration step 2
- ทำการเพิ่มไฟล์ configuration step 3
- ทำการรวมข้อมูล
- ทำการเพิ่มข้อมูลลงฐานข้อมูล



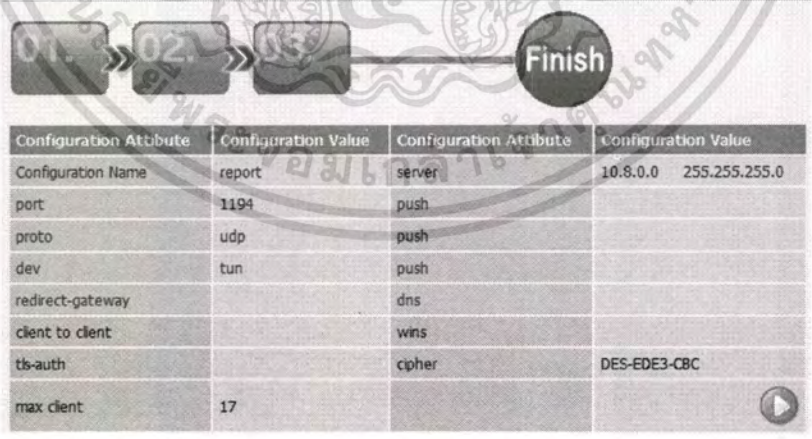
รูปที่ 4.6 แสดง add configuration step 1



รูปที่ 4.7 แสดง add configuration step 2



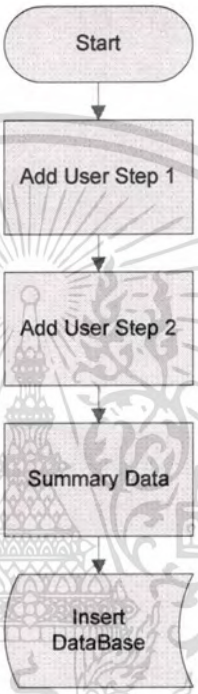
รูปที่ 4.8 แสดง add configuration step 3



รูปที่ 4.9 แสดง Summary Data

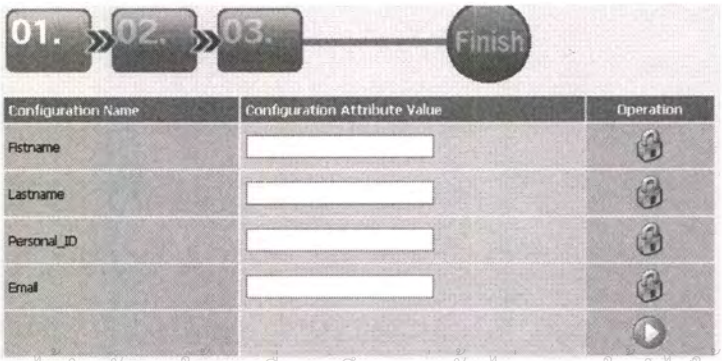
4.4.2 การเพิ่มผู้ใช้งานระบบ

ผู้ดูแลระบบทำการเพิ่มผู้ใช้งานเพื่อให้คนที่จะใช้งานทำการระบุตัวตนตามที่ผู้ดูแลระบบได้ทำการสร้างให้ตนเองและหลังจากที่ทำการระบุตัวตนแล้วทำการโหลดไฟล์ที่ใช้ของตนเองไปใช้งาน ซึ่งเพื่อให้สะดวกกับผู้ดูแลระบบในการเพิ่มผู้ใช้งานดังนั้นจึงทำการแบ่งเป็นขั้นตอนเช่นเดียวกับไฟล์ Configuration

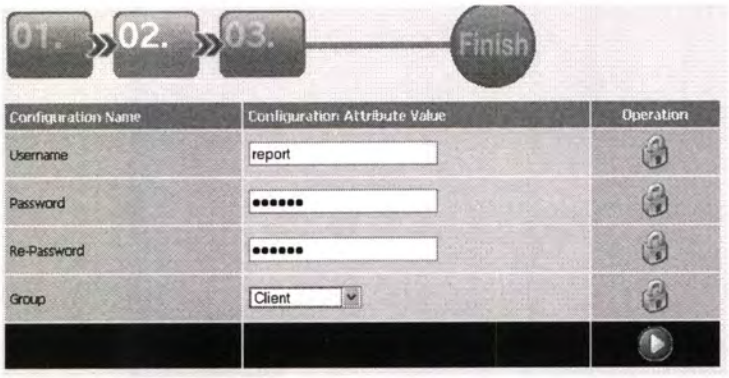


ขั้นตอนการทำงานของการเพิ่มผู้ใช้งาน

- ทำการเพิ่มผู้ใช้งาน step 1
- ทำการเพิ่มผู้ใช้งาน step 2
- ทำการรวมข้อมูล
- ทำการเพิ่มข้อมูลลงฐานข้อมูล



รูปที่ 4.10 แสดง add user step 1

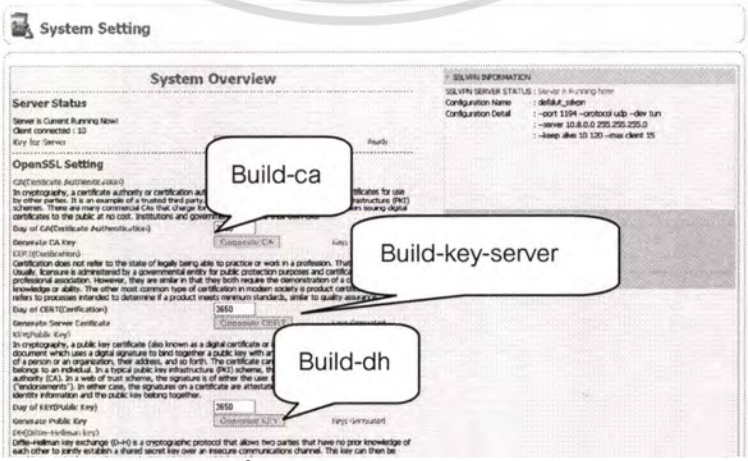


รูปที่ 4.11 แสดง add user step 2

รูปที่ 4.12 แสดง summary user

4.4.3 การสร้าง Key ของ Server

ผู้ดูแลระบบทำการสร้าง Key ที่เอาไว้ใช้งานสำหรับเครื่อง Server วิ่งได้แก่การสั่ง run คำสั่งดังต่อไปนี้ build-ca , build-key-server , build-dh และหลังจากนั้นทำการ start service



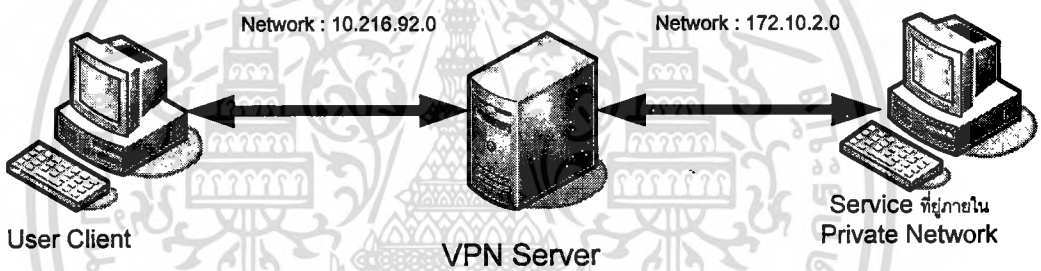
รูปที่ 4.13 แสดง การสร้าง Key

บทที่ 5
สรุปผลการทำงานของระบบ

ในบทนี้จะกล่าวถึงการทดสอบโครงงานโดยจะกำหนดวิธีการทดสอบออกเป็นสถานการณ์รูปแบบต่างๆ เพื่อนำมาวิเคราะห์สรุปผลการทำงานของโครงงานต่อไป

5.1 การทดสอบโครงการ

การทดสอบโครงงานจะกระทำโดยให้ผู้ดูแลระบบทำการเพิ่ม ผู้ใช้ในระบบพร้อมกับสร้างไฟล์คอนฟิกขึ้นก่อนที่จะทำการสตาร์ทเซอร์วิสนี้พร้อมกับตรวจสอบสถานะการเชื่อมต่อและการให้บริการจากฝั่งเซิร์ฟเวอร์ นอกจากนี้ยังต้องตรวจสอบการเข้ารหัสข้อมูลว่าในกรณีที่ยังไม่ได้ใช้บริการผ่านเครือข่ายส่วนตัวเสมือนกับกรณีที่ได้ใช้บริการผ่านเครือข่ายส่วนตัวเสมือนนั้นว่ามีความแตกต่างกันหรือไม่โดยกำหนด Topology เป็นดังรูปที่ 5.1

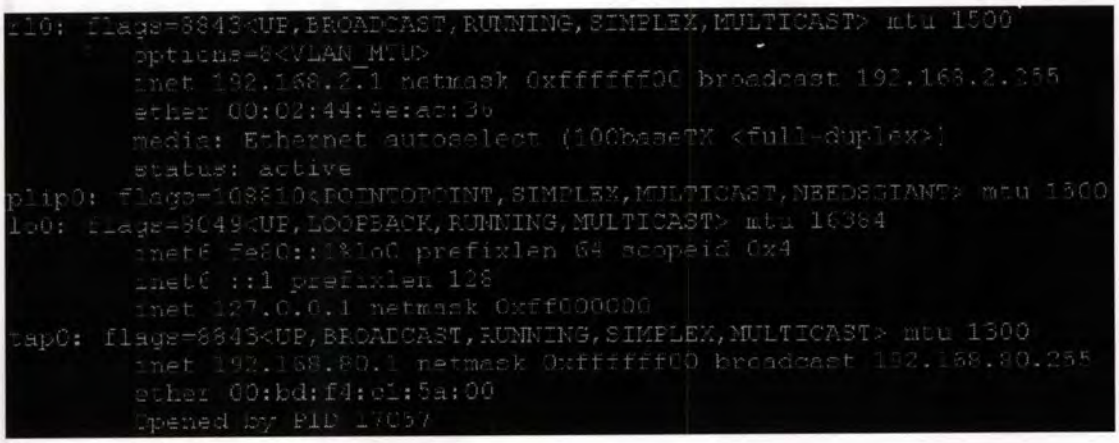


รูปที่ 5.1 แสดงแบบของการทดสอบ

รูปที่ 5.1 แสดง Topology ที่ใช้ในการทดสอบโดยกำหนดให้ User Client นั้นอยู่ในส่วนของเครือข่ายสาธารณะ (Public Network) แล้วต้องการติดต่อผ่านเข้าไปใช้บริการที่อยู่เครือข่ายภายใน

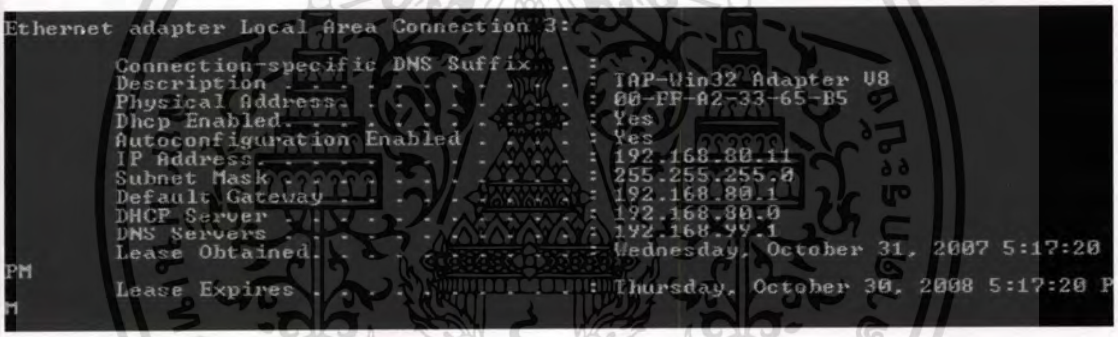
การตรวจสอบว่า Server และ Client สามารถให้บริการได้

โดยการแบ่งการตรวจสอบทั้ง 2 ฝั่งโดยการว่า Server สามารถทำงานได้และ Client สามารถทำงานได้โดยถ้าฝั่ง Server สามารถทำงานได้ก็จะขึ้น Interface ใหม่ขึ้นมาอันหนึ่งซึ่งจะเป็น TUN หรือ TAP ขึ้นอยู่กับการตั้งค่าของไฟล์ Configuration พร้อมกับ IP ADDRESS ขึ้นอยู่กัยการตั้งค่าของไฟล์ Configuration ฝั่งของ Client ก็เช่นกันถ้าสามารถติดต่อได้ก็จะมี Interface ใหม่พร้อมกับ IP ADDRESS ที่ได้จาก Server



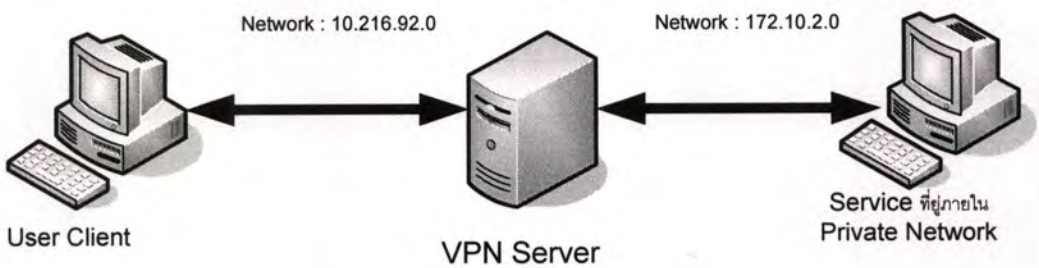
รูปที่ 5.2 แสดง TAP Interface

จากรูปจะมี Interface Tap0 ขึ้นมาใหม่อันหนึ่งซึ่งเกิดจากการเปิด Service ของ Openvpn ในฝั่งของ Server



รูปที่ 5.3 แสดง TUN Interface

จะมี Interface Ethernet ขึ้นมาอันใหม่อันหนึ่งและ IP ADDRESS ที่ได้รับนั้นมาจาก Server เป็นอันแสดงว่าเราสามารถติดต่อกับ SSLVPN Server ได้แล้วและสามารถ Access เข้าไปยังเครือข่ายภายในองค์กรได้



รูปที่ 5.4 แสดงการทดสอบเข้าไปใช้งานของผู้ใช้งาน

หลังจากทำการติดตั้ง openvpn software ที่ฝั่ง client และทำการ download key และ ไฟล์ configuration ไปแล้วทำการติดต่อผ่าน openvpn's software เรียบร้อยแล้วจะสามารถเข้าถึงเครื่อง PC ภายใน Private Network ได้

5.2 ผลสรุปจากการทดสอบโครงการ

จากตัวอย่างที่แสดงมาทั้งหมดนั้นแสดงให้เห็นถึงผลลัพธ์การทำงานของตัวโครงงานที่พัฒนาขึ้นนั้นสามารถเข้าไปจัดการตัวแอพลิเคชั่นที่ใช้ในการสร้างเครือข่ายส่วนตัวเสมือน (Virtual Private Network) โอเพ่นวีพีเอ็น (OpenVPN) โดยตัวโครงงานที่พัฒนาขึ้นนั้นจะทำการจัดการเพิ่มหรือลดจำนวนผู้ใช้ในระบบ, การติดตั้งค่าพารามิเตอร์ของผู้ใช้แต่ละคนและการตรวจสอบการให้บริการว่าได้ทำการสตาร์ทเซอร์วิส (Start Service) ของผู้ใช้แต่ละคนแล้วหรือไม่ อีกทั้งรวมไปถึงการตรวจสอบสถานะเชื่อมต่อของผู้ใช้ในระบบด้วย นอกจากนี้ยังได้ทำการตรวจสอบการเข้ารหัสข้อมูลโดยใช้โปรแกรม Ethereal ว่ามีความแตกต่างระหว่างการส่งข้อมูลผ่านเครือข่ายส่วนตัวเสมือน (Virtual Private Network) กับการส่งข้อมูลโดยไม่ผ่านเครือข่ายส่วนตัวเสมือน (Virtual Private Network) หรือไม่ โดยผลที่ได้คือข้อมูลที่ส่งผ่านเครือข่ายส่วนตัวเสมือน (Virtual Private Network) นั้นจะไม่สามารถอ่านค่าได้ต่างจากข้อมูลที่ไม่ส่งผ่านเครือข่ายส่วนตัวเสมือน (Virtual Private Network) ซึ่งสามารถใช้โปรแกรม Ethereal ตรวจจับข้อมูลแล้วอ่านข้อความที่ตรวจจับได้โดยข้อมูลที่ส่งผ่านเครือข่ายส่วนตัวเสมือนนั้นเป็นข้อความที่ถูกเข้ารหัส (Cipher Text)ไว้โดยใช้คีย์ (Key) ที่เรียกว่า คีย์ลับ (Secret Key) ของผู้ใช้แต่ละคน

5.3 ผลสรุปจากการพัฒนาโครงการ

จากการพัฒนาโครงงานทำให้เข้าใจหลักการทำงานของเครือข่ายส่วนตัวเสมือน (Virtual Private Network) ว่ามีหลักการทำงานอย่างไร มีรูปแบบในการใช้งานกี่ประเภทอีกทั้งได้เข้าใจถึงความสามารถของฟังก์ชั่นของโปรแกรม โอเพ่นวีพีเอ็น (OpenVPN) และการนำฟังก์ชั่นนี้มาใช้ในประโยชน์ในโครงงานรวมถึงการพัฒนาฟังก์ชั่นการทำงานเพิ่มเติมในส่วนของโครงงานเพื่อให้สามารถจัดการการเชื่อมต่อของผู้ใช้แต่ละคนผ่านทางเว็บบราวเซอร์ซึ่งในปัจจุบันนี้การใช้งานผ่านทางเว็บบราวเซอร์เป็นที่นิยมมากในการใช้งานผ่านทางอินเทอร์เนต (Internet) ซึ่งเป็นเครือข่ายสาธารณะ (Public Network) ในการพัฒนาโครงงานนี้นั้นสามารถจะสรุปความสามารถได้ดังนี้

- สามารถเพิ่มหรือลดจำนวนผู้ใช้ในระบบ
- สามารถเพิ่มหรือลดจำนวนผู้ดูแลระบบ
- ผู้ดูแลสามารถเปลี่ยนรหัสและสถานะเข้า Login เพื่อใช้งานในระบบของผู้ใช้ได้
- ผู้ดูแลสามารถลบไฟล์คอนฟิกหรือเปลี่ยนคีย์ (Key) ของผู้ใช้
- ผู้ดูแลสามารถสามารถสตาร์ทเซอร์วิส (Start Service)

- ผู้ดูแลสามารถตรวจสอบสถานะการให้บริการ
- ผู้ดูแลสามารถสามารถหยุดเซอร์วิส (Stop Service) เพื่อหยุดให้บริการ
- ผู้ดูแลสามารถสร้างไฟล์ Configuration ของ Server
- ระบบสามารถสร้างไฟล์ Configuration ของ Client
- ผู้ดูแลสามารถตรวจสอบประวัติการใช้งานของผู้ใช้แต่ละคนได้
- ผู้ใช้สามารถเปลี่ยนรหัสผ่านของตนเองได้
- ผู้ใช้สามารถตรวจสอบการให้บริการและสถานะการเชื่อมต่อของตนได้

จากการทดสอบโปรแกรมนี้พบว่าสามารถทำงานได้ตามฟังก์ชั่นที่ต้องการซึ่งเป็นความต้องการขั้นพื้นฐานในการจัดการเครือข่ายส่วนตัวเสมือน แต่อย่างไรก็ตามตัวโปรแกรมนี้สามารถนำไปพัฒนาต่อได้เพื่อให้ได้ระบบที่สมบูรณ์มากยิ่งขึ้นและเกิดประโยชน์ได้มากที่สุด

5.4 แนวทางการพัฒนาต่อ

การพัฒนาโปรแกรมจัดการเครือข่ายส่วนตัวเสมือนบนระบบปฏิบัติการ FreeBSD ผ่านทางเว็บ สามารถที่จะนำไปพัฒนาต่อเพื่อให้มีความสามารถมากขึ้นกว่าเดิมได้โดยการเพิ่มฟังก์ชั่นการทำงานให้สามารถสร้างการเชื่อมต่อที่ซับซ้อนมากขึ้นเช่น

- การเพิ่มพารามิเตอร์ลงไปในระบบงานที่ซับซ้อนเช่น พารามิเตอร์ที่เกี่ยวข้องกับการสร้าง Tunneling ผ่าน Proxy Server
- การทำงานในรูปแบบ Bridged Ethernet Tunnels ซึ่งเหมาะสำหรับการใช้งานบน Protocol อื่นๆ ที่ไม่ใช่ IP หรือการใช้งานที่ต้องมีการ Broadcast ด้วย หรือต้องการใช้ IP ใน network เดียวกันกับ network ปลายทาง โดยที่ VPN Server จะทำหน้าที่เป็น Bridge ให้นั่นเองซึ่งในโครงงานนี้ยังไม่สามารถทำได้

บรรณานุกรม

กิตติพงษ์ สุวรรณราช. 2547. **การบริหารและจัดการเครือข่ายอินเทอร์เนตด้วยระบบปฏิบัติการ FreeBSD,** ออฟเซ็ท เพรส.

จตุชัย แพงจันทร์ และ อนุโชต วุฒิพรพงษ์. 2546. **เจาะระบบ Network ฉบับสมบูรณ์,** ไอดีซี อินโฟ ดิสทริบิวเตอร์ เซ็นเตอร์.

เรืองไกร รังสิพล. 2545. **เปิดโลก Firewall และ Internet Security** ,โปรวิชั่น.

สุวัฒน์ ปุณณชัยยะและคณะ. 2545. **เปิดโลก TCP/IP และโปรโตคอล ของอินเทอร์เน็ต 2nd Ed** , โปรวิชั่น.

Meeta Gupta. 2003. **Building a Virtual Private Network**, Premier Press, a division of Course Technology.

Microsoft. 2004. **"Virtual Private Networking in Windows2000"** [Online]. Available:http://www.microsoft.com/windows2000/technologies/communications/vpn/default.asp

Microsoft. 2004. **"Virtual Private Networking and Intranet Security"** [Online]. Available:http://www.microsoft.com/windows2000/technologies/communications/vpn/default.asp

OpenVPN. 2010. **"OpenVPN"** [Online]. Available: http://openvpn.net

ภาคผนวก ก
การติดตั้งโปรแกรมที่เกี่ยวข้อง

ขั้นตอนการติดตั้งระบบต่าง ๆ ที่เกี่ยวข้องกับโปรแกรมหาอายุและขนาดของเว็บออบเจ็กต์ โดยเป็นการติดตั้งในระบบปฏิบัติการ FreeBSD 5.5 ปกติแล้วจะติดตั้งโปรแกรมได้หลายรูปแบบเช่นการดาวน์โหลดซอสโค้ดมาคอมไพล์ก็ได้ หรือจะทำการเลือกเพ็กเก็จต่าง ๆ จากคำสั่ง /stand/sysinstall แล้วเลือกเมนู configure แล้วเลือกเมนูย่อย Packages ก็ได้ แต่ในระบบปฏิบัติการ FreeBSD มีระบบ Ports ซึ่งจะช่วยให้การติดตั้งสะดวกและมีความยืดหยุ่นมากกว่า โดย Ports จะทำการดาวน์โหลดโปรแกรมต่าง ๆ ที่มีสัมพันธ์กันมาติดตั้งให้โดยอัตโนมัติ ซึ่งในที่นี้จะเป็นการติดตั้งโปรแกรมต่าง ๆ กับโปรแกรมหาอายุและขนาดของเว็บออบเจ็กต์ด้วย Port โดยโปรแกรมที่ต้องจะติดตั้งคือ Perl, php5, MySQL Server , Apache2.2 ส่วนที่เหลือจะเป็นโปรแกรมที่สัมพันธ์กับโปรแกรมทั้งหมดนี้ Portsจะดาวน์โหลดโปรแกรมที่เหลือมาติดตั้งให้โดยอัตโนมัติ

การติดตั้ง php5 จาก Ports

```
# cd /usr/ports/lang/php5
# make config
เลือกค่าต่างๆตามที่จะใช้งาน
#make install clean
```

config file php.ini

```
# cp /usr/local/etc/php.ini-recommended /usr/local/etc/php.ini
www # vi /usr/local/etc/php.ini
แก้ไขให้เป็นเหมือนข้างล่าง
default_charset = "tis-620"
upload_tmp_dir = "/tmp/uptmp"
session.save_patch = "/tmp/sesstmp"
```

จากนั้น

```
www # mkdir /tmp/uptmp
ww # mkdir /tmp/sesstmp
www # chmod 777 /tmp/uptmp
www # chmod 777 /tmp/sesstmp
www # cd /usr/ports/lang/php4-extensions
```

```
www # make install clean
www # /usr/local/etc/rc.d/apache22.sh restart
```

การติดตั้ง Extensions ต่างๆของ PHP5

```
# cd /usr/ports/lang/php5-extensions
# make config
```

เลือก extention ต่างๆตามที่จะใช้งาน

```
# make install clean
```

พอเสร็จก็สั่ง restart apache อีกครั้ง

```
# /usr/local/etc/rc.d/apache22.sh restart
```

ลองเรียกหน้า test.php ดู

http://www.my-office.com/test.php

จะมีรายละเอียดต่างๆของ Extensions เพิ่มเข้ามาเป็นอันเรียบร้อย

ติดตั้ง Apache 2

```
www # cd /usr/ports/www/apache2
?WITH_LDAP_MODULES=yes\
?WITH_MYSQL=yes\
?WITH_SSL_MODULES=yes\
?WITH_THREADS=yes\
?install && make clean
```

รอจนระบบติดตั้งเสร็จแล้วทำการแก้ไขไฟล์ rc.conf

```
www # vi /etc/rc.conf
```

เพิ่มคำสั่ง apache2_enable="YES"

ทำการแก้ไขไฟล์ httpd.conf

```
www # cd /usr/local/etc/apache2/httpd.conf
```

แก้ให้เหมือนดังตัวอย่างข้างล่าง

```
AddHandler cgi-script .cgi .pl
```

แก้ Document Root

```
DocumentRoot "/usr/local/www/data"
<Directory "/usr/local/www">
```

โดย "/usr/local/www/data" คือไดเรกทอรีที่ติดตั้งโปรแกรมสร้างรายงาน หรืออาจจะติดตั้งโปรแกรมสร้างรายงานไว้ใน User Directory แทนก็ได้ โดยทั่วไปก็จะต้องสร้างไดเรกทอรี public_html ไว้ในโฮมไดเรกทอรีของผู้ใช้ ก็ให้ทำการติดตั้งโปรแกรมไว้ในไดเรกทอรีนี้

เมื่อติดตั้งโปรแกรมเสร็จแล้วทำการสั่งให้ apache เริ่มทำงานด้วยคำสั่ง

```
# /usr/local/etc/rc.d/apache start
```

การติดตั้งโปรแกรม MySQL Server 5 จาก Ports

```
www # cd /usr/ports/databases/mysql50-server
www # make \
? WITH_CHARSET=tis620 \
? WITH_XCHARSET=all \
? WITH_COLLATION=tis620_thai_ci \
? make  install with_db_dir=/usr/local/db-mysql && make clean
```

โดยที่ /usr/local/db-mysql เป็นไดเรกทอรีที่ต้องการติดตั้งฐานข้อมูล หากไม่มีการกำหนด ฐานข้อมูลจะถูกติดตั้งที่ /var/db/mysql ซึ่งโดยปกติจะมีพื้นที่น้อยเกินไป หรืออาจเข้าไปแก้ไขไฟล์ Makefile ในส่วน db_dir แทนก็ได้ จากนั้น Ports ก็จะทำการตรวจสอบดูว่าโปรแกรมที่เกี่ยวข้องกับ mysql323-server ติดตั้งในระบบหรือยัง ถ้ายังไม่ได้ติดตั้งจะไปทำการดาวน์โหลดโปรแกรมเหล่านั้นมาติดตั้งให้โดยอัตโนมัติ หากไม่มีข้อผิดพลาดแจ้งขึ้นมาในระหว่างการทำงานแสดงว่าโปรแกรม MySQL ได้ถูกติดตั้งและสามารถใช้งานได้ เมื่อมีการเริ่มระบบใหม่(restart) หรือสามารถสั่งให้ MySQL Server เริ่มทำงานทันทีโดยไม่ต้องเริ่มระบบใหม่ด้วยคำสั่ง

ปรับแต่งไฟล์ my.cnf

```
www # cp /usr/local/share/mysql/my-medium.cnf /etc/my.cnf
www # chown root:sys /etc/my.cnf
www # chmod 644 /etc/my.cnf
www # rehash
www # /usr/local/etc/rc.d/mysql-server.sh start
```

เพิ่มผู้ใช้งานระบบฐานข้อมูล

```
www # mysqladmin –u root password 1234
```

ตัวอีกษรแดงๆ ให้เปลี่ยนเป็น Username + password ของตัวเอง

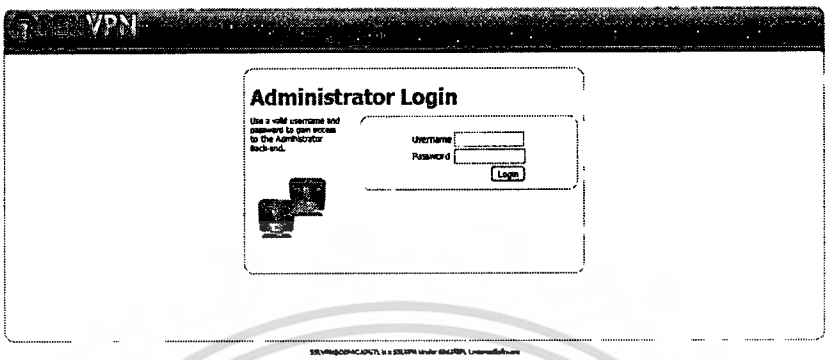
และปรับแต่งไฟล์ /etc/rc.conf โดยเพิ่มคำสั่ง mysql_enable="YES"

การติดตั้งโปรแกรม OpenVPN จาก Ports

```
# cd /usr/ports/security/openvpn
# make && make install
```

ภาคผนวก ข

การคู่มือการใช้งานระบบ



รูป แสดงหน้าจอ Login ของ Administrator

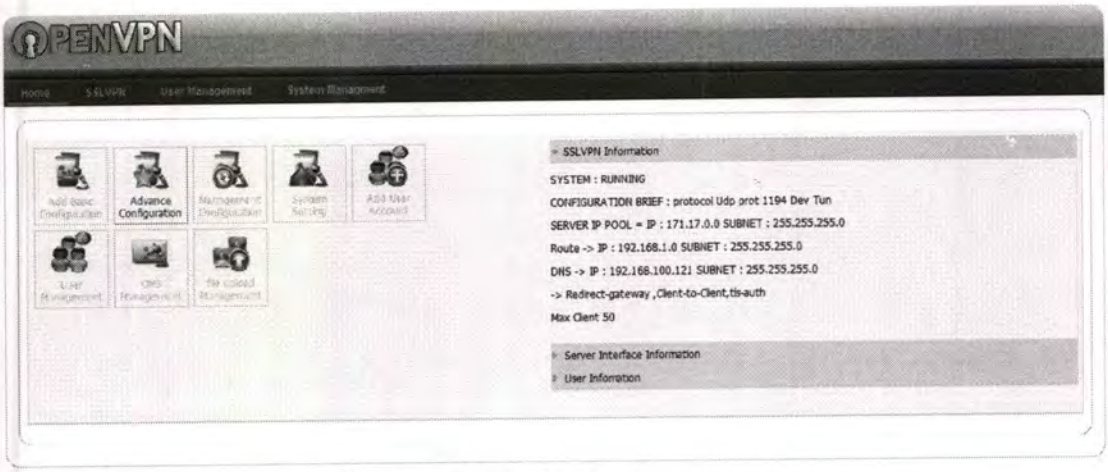
หน้าจอแสดงหน้าการเข้าไปใช้งานระบบของผู้ดูแลระบบ

รูป แสดงเตือนว่าผู้ใช้งานถูกต้อง

ถ้าทำการกรอกชื่อผู้ใช้งานเรียบร้อยแล้วและเมื่อทำการตรวจสอบว่าสามารถผ่านเข้าไปใช้งานได้ ก็จะแสดงรายระเลียดดังภาพข้างบน

รูป แสดงเตือนว่าผู้ใช้งานไม่ถูกต้อง

ภาพแสดงในกรณีที่ผู้ใช้งานทำการกรอกข้อมูลและรหัสผ่านไม่ถูกต้องระบบจะทำการแจ้ง



รูป แสดงหน้าจอหลักของ Administrator

ภาพแสดงหน้าจอหลักของการจัดการหลักของหน้าจอการจัดการระบบให้บริการเครือข่ายเสมือนส่วนตัว

เมนูแสดงรายการดังต่อไปนี้

- Add Basic Configuration
- Management Configuration
- System Setting
- Add user Account
- User Management

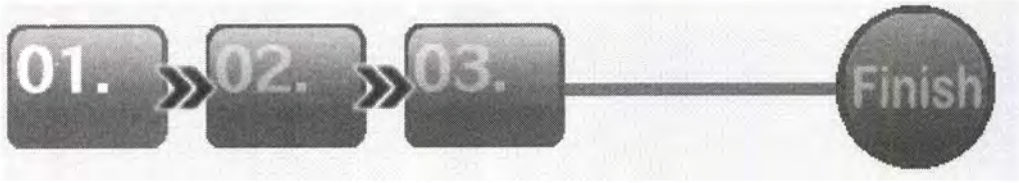
ภาพดังต่อไปนี้เป็นสัญลักษณ์ที่ใช้ส่วนของการสร้าง Configuration และเพิ่มผู้ใช้งาน รวมทั้งการแก้ไขในส่วนของ Configuration และ การแก้ไขผู้ใช้งาน

 ภาพแสดงเพื่อบอกว่า จำเป็นต้องทำการกรอกข้อมูลให้เรียบร้อย

 ภาพแสดงปุ่มที่มช้ในการ submit ระบบ

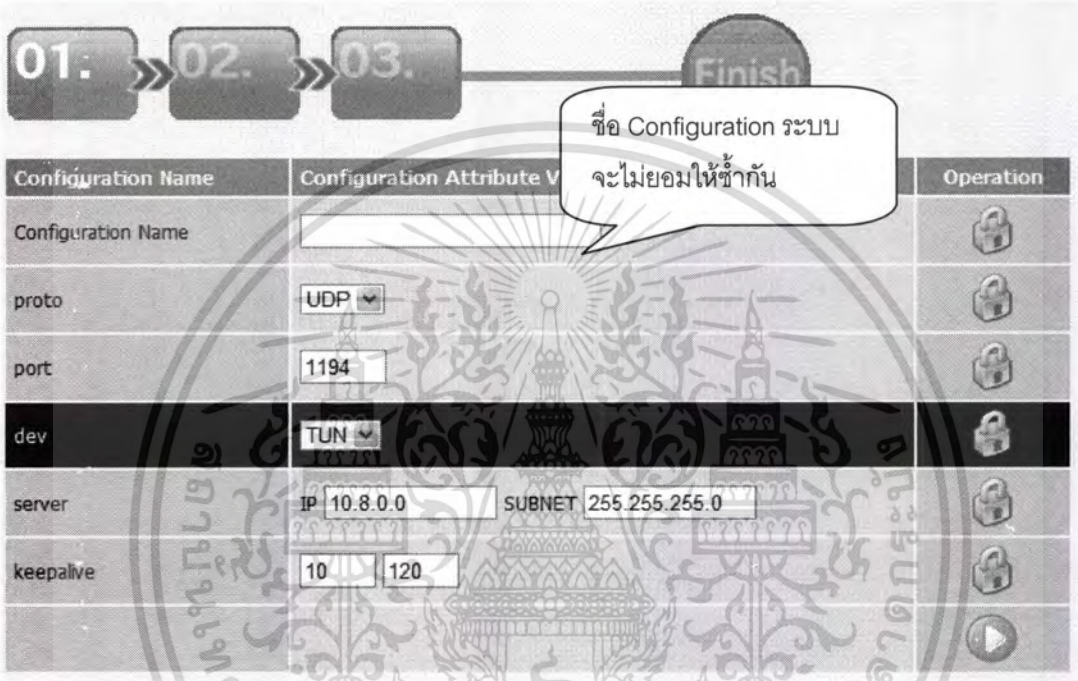
 ภาพแสดงเพื่อบอกว่า ไม่จำเป็นต้องกรอกข้อมูลให้เรียบร้อย

ส่วนการจัดการไฟล์ Configuration เบื้องต้น (Add Basic Configuration) ใช้ในการเพิ่มไฟล์ Configuration ที่นำมาใช้ในการตั้งค่าการใช้งานของ SSLVPN Server โดยจะมีการแบ่งขั้นตอนในการเพิ่ม Configurations



รูป สัญลักษณ์ลำดับในการทำงาน

จากภาพแสดงสัญลักษณ์เพื่อบอกว่ากำลังดำเนินการอยู่ในขั้นตอนไหนของขั้นตอนจากตัวอย่าง คือ ขั้นตอนแรก



รูป หน้าจอในการทำงานเพิ่มไฟล์ Configuration

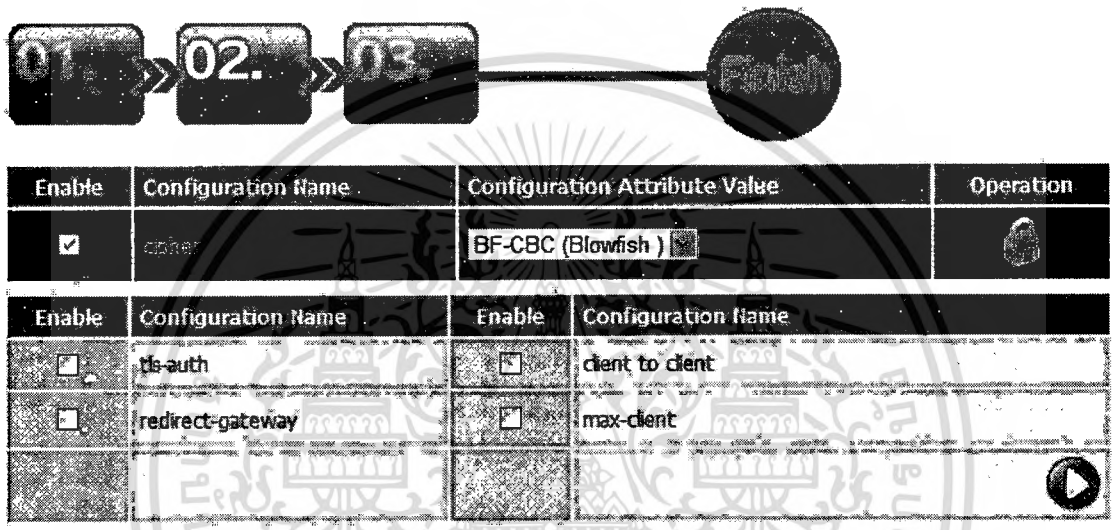
จากภาพแสดงขั้นตอนแรกในการเพิ่มไฟล์ configuration

รูป หน้าจอในการทำงานเพิ่มไฟล์ Configuration

ภาพแสดงตัวเลือกของ proto ซึ่งหมายถึง ว่าต้องการให้ server รับส่งข้อมูลด้วย protocol ไหน ระหว่าง TCP หรือ UDP

รูป หน้าจอในการทำงานเพิ่มไฟล์ Configuration

ภาพแสดงตัวเลือกของ Dev ซึ่งหมายถึงว่าต้องการให้ระบบทำการห่อหุ้มข้อมูลใน Layer ไหน ภายใน OSI Mode ระหว่าง TUN ทำงานใน Layer 3 ซึ่งจะทำการห่อหุ้มแค่ IP หรือ TAP ที่ทำงานใน Layer 2 ซึ่งจะทำการห่อหุ้มทั้ง Frame

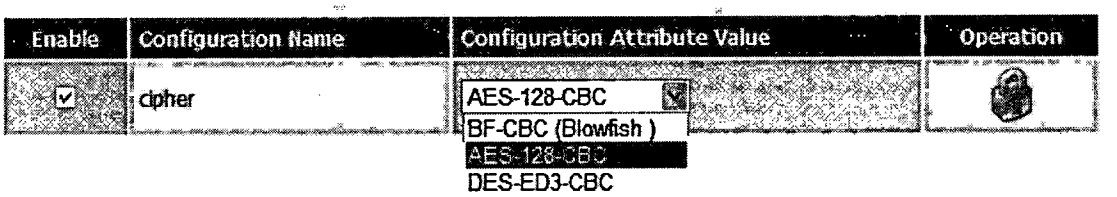


รูป หน้าจอในการทำงานเพิ่มไฟล์ Configuration

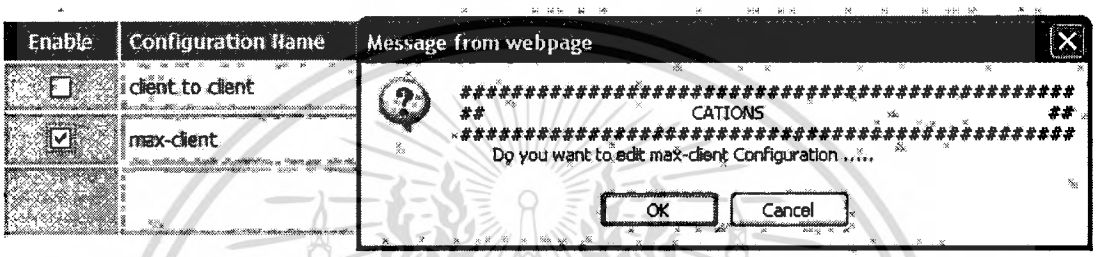
ภาพแสดงขั้นตอนที่สองในการเพิ่ม Configuration

มีรายการดังนี้

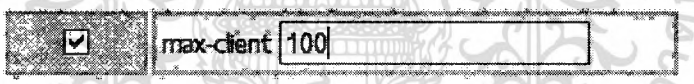
Cipher	คือการเข้ารหัสข้อมูล
TLS-AUTH	การให้มีส่วนของการระบุตัวตนโดยใช้ ta.key
Client-to-Client	การให้ Client สามารถติดต่อกับ Client ด้วยกันได้
Redirect-gateway	การให้ Client ทำการเปลี่ยน Gateway มาใช้ Gateway ของ SSLVPN Server



รูป หน้าจอในการทำงานเพิ่มไฟล์ Configuration
ภาพแสดงตัวเลือกของการเข้ารหัสโดยจะมีให้เลือกดังนี้ คือ Blowfish , AES , 3DES ตามรายการที่แสดงให้เห็นบนภาพข้างบน



รูป หน้าจอในการทำงานเพิ่มไฟล์ Configuration
ภาพแสดงตัวเลือกของการกำหนดจำนวนผู้ใช้งาน

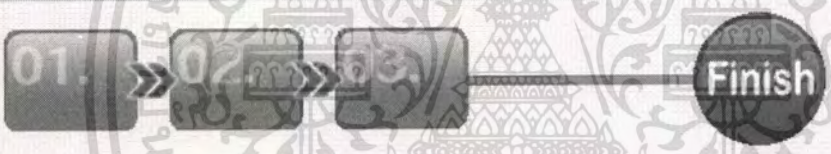


รูป หน้าจอในการทำงานเพิ่มไฟล์ Configuration
ภาพแสดงตัวเลือกของการกำหนดจำนวนผู้ใช้งาน

Enable	Configuration Name	Configuration Attribute Value	Status
☑	route	IP SUBNET	
☐	route	IP SUBNET	
☐	route	IP SUBNET	
☐	dhcp-option DNS	IP	
☐	dhcp-option WINS	IP	

รูป หน้าจอในการทำงานเพิ่มไฟล์ Configuration

ภาพแสดงขั้นตอนที่สามในการเพิ่ม Configuration โดยขั้นตอนนี้จะให้ทำการกรอกข้อมูลที่ใช้ในการ Route ไปยัง Subnet อื่นหรือทำการตั้งค่าในให้ไปหา DNS Server ในกรณีที่ทำ Redirect Gateway เพื่อให้สามารถเชื่อมต่อ Internet ได้



Configuration Attibute	Configuration Value	Configuration Attibute	Configuration Value
Configuration Name	report	server	10.8.0.0 255.255.255.0
port	1194	push	
proto	udp	push	
dev	tun	push	
redirect-gateway		dns	
client to client		wins	
tls-auth		cipher	DES-EDE3-CBC
max client	17		

รูป หน้าจอในการทำงานเพิ่มไฟล์ Configuration

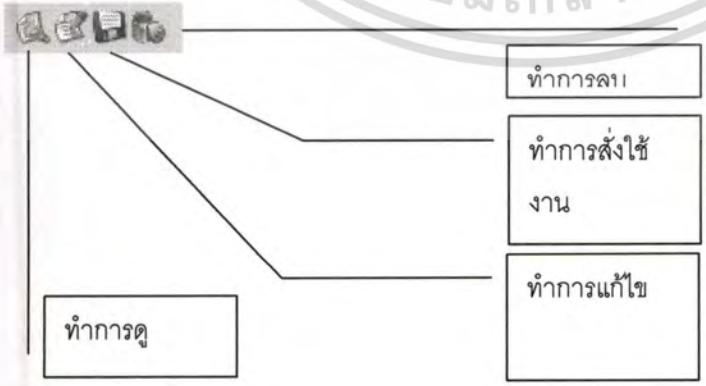
ภาพแสดงขั้นตอนสุดท้ายในการเพิ่ม Configuration โดยขั้นตอนนี้จะให้ทำการเช็คดูข้อมูลว่ามีผิดพลาดหรือไม

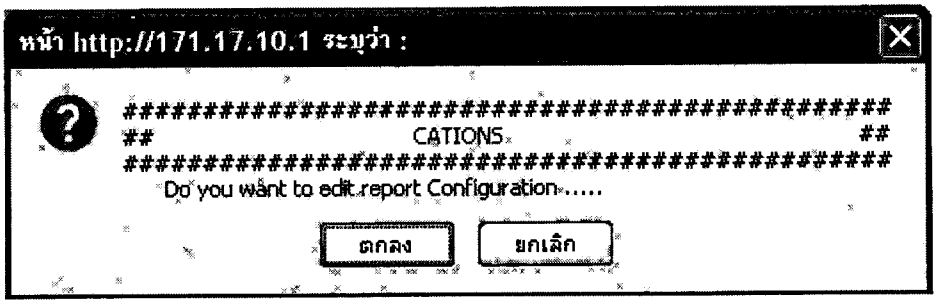
รูป หน้าจอในการทำงานเพิ่มไฟล์ Configuration
ภาพแสดงเมื่อทำการกดปุ่ม Submit ระบบจะถามอีกทีเพื่อความมั่นใจ

การจัดการไฟล์ Configuration (Management Configuration)ใช้ในการแก้ไข ลบ และทำการดูรายละเอียดของไฟล์ configuration และสามารถทำการกำหนดได้ว่าจะเลือกใช้ไฟล์ Configuration ตัวไหนในการ run service

Configuration Name	Status	Operator
sslvpn	disable	
ex1	disable	
defalut_sslvpn	enable	
testtest	disable	
uiui	disable	
report	disable	

รูป หน้าจอในการทำงานจัดการไฟล์ Configuration
ภาพแสดงส่วนของการจัดการไฟล์ Configuration



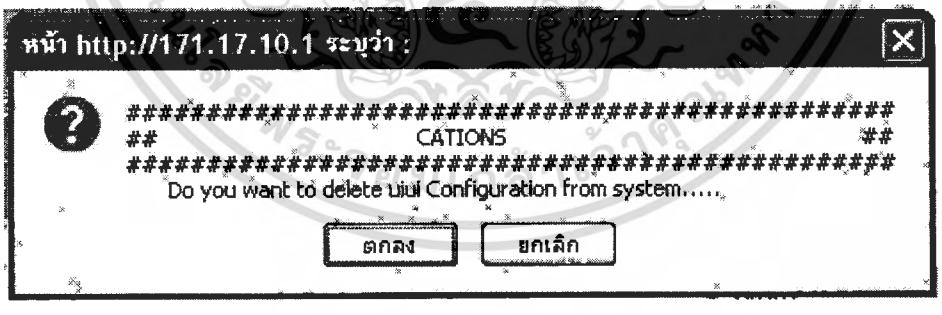


รูป หน้าจอในการทำงานจัดการไฟล์ Configuration

ภาพแสดงการยืนยันการแก้ไขไฟล์ Configuration

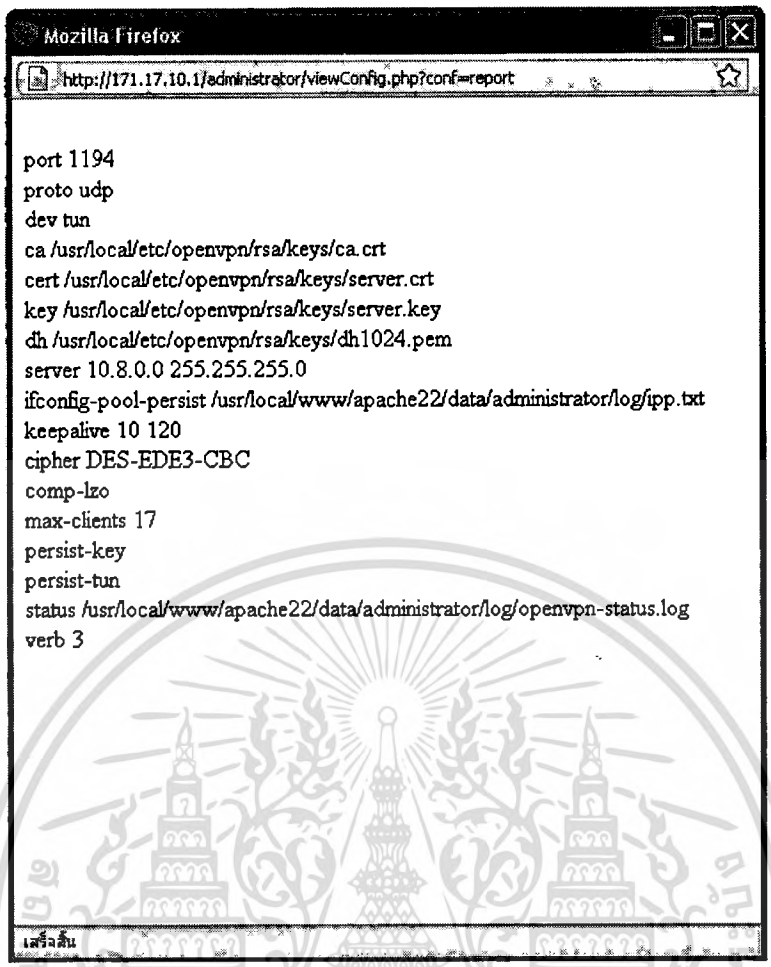
รูป หน้าจอในการทำงานจัดการไฟล์ Configuration

ภาพแสดงการยืนยันการเลือกใช้งานไฟล์ Configuration นี้ให้เป็นไฟล์หลัก



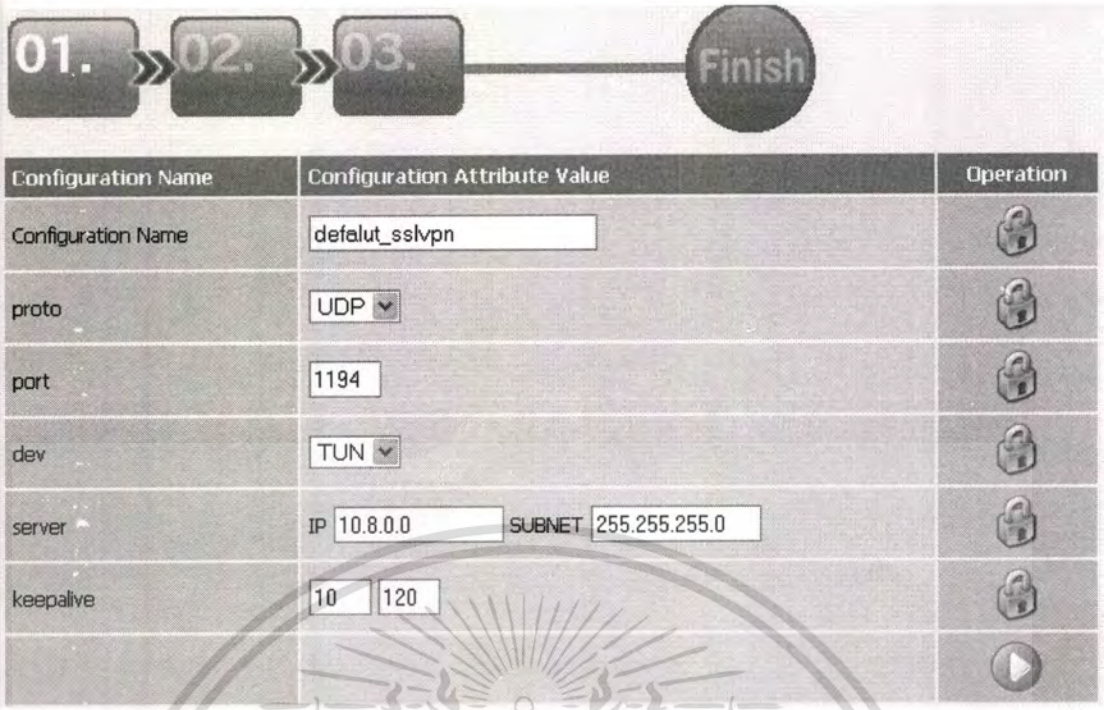
รูป หน้าจอในการทำงานจัดการไฟล์ Configuration

ภาพแสดงการยืนยันการลบไฟล์ Configuration

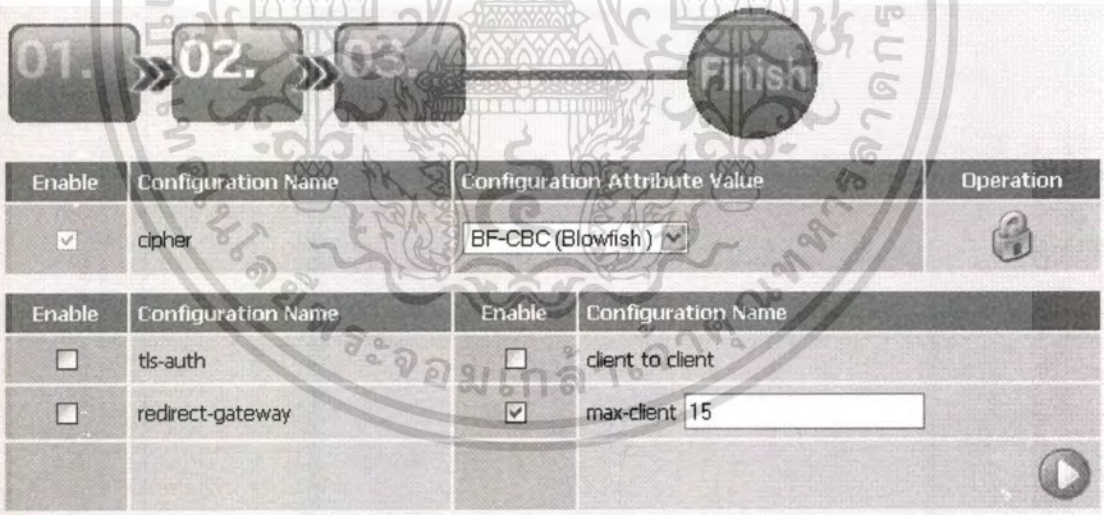


รูป หน้าจอในการทำงานจัดการไฟล์ Configuration

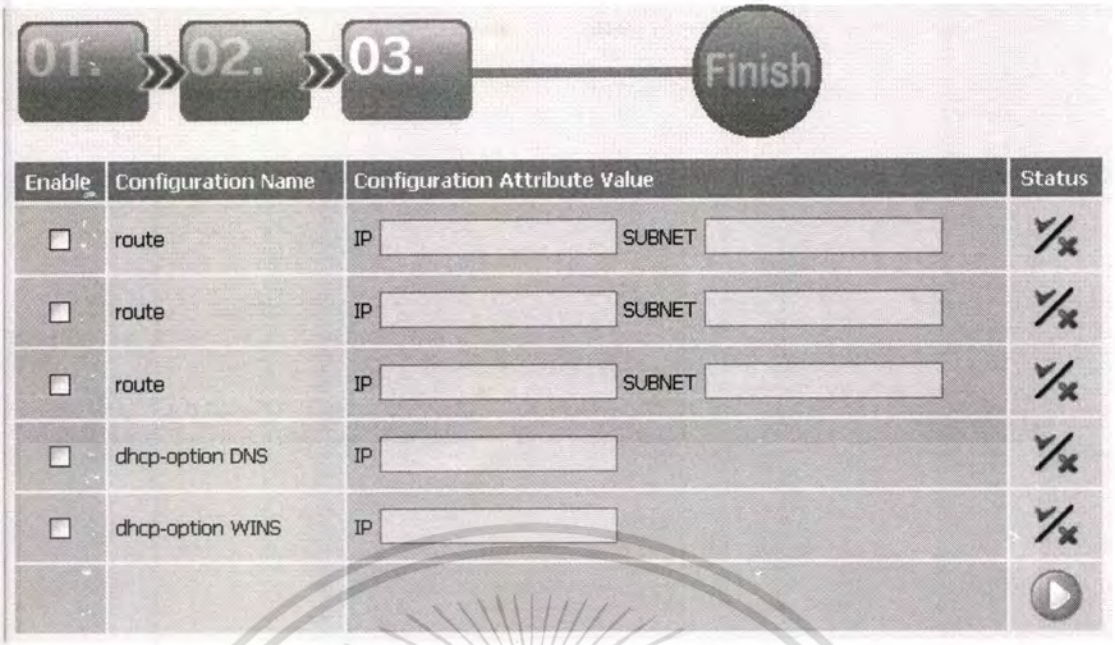
ภาพแสดงเมื่อทำการคลิ๊กที่ปุ่มดูรายละเอียดไฟล์ Configuration จะแสดงผลดังภาพข้างบนการแก้ไขไฟล์ Configuration จะเริ่มจากการที่กดที่ปุ่มแก้ไขที่หน้าการจัดการไฟล์ Configuration เพื่อทำการแก้ไขข้อมูล โดยระบบจะอนุญาติให้ผู้ใช้งานแก้ไขได้เฉพาะบางส่วนเท่านั้น



รูป หน้าจอในการทำงานจัดการผู้ใช้งาน
ภาพแสดงหน้าจอการแก้ไขซึ่งจะมีขั้นตอนเหมือนการเพิ่มไฟล์ Configuration

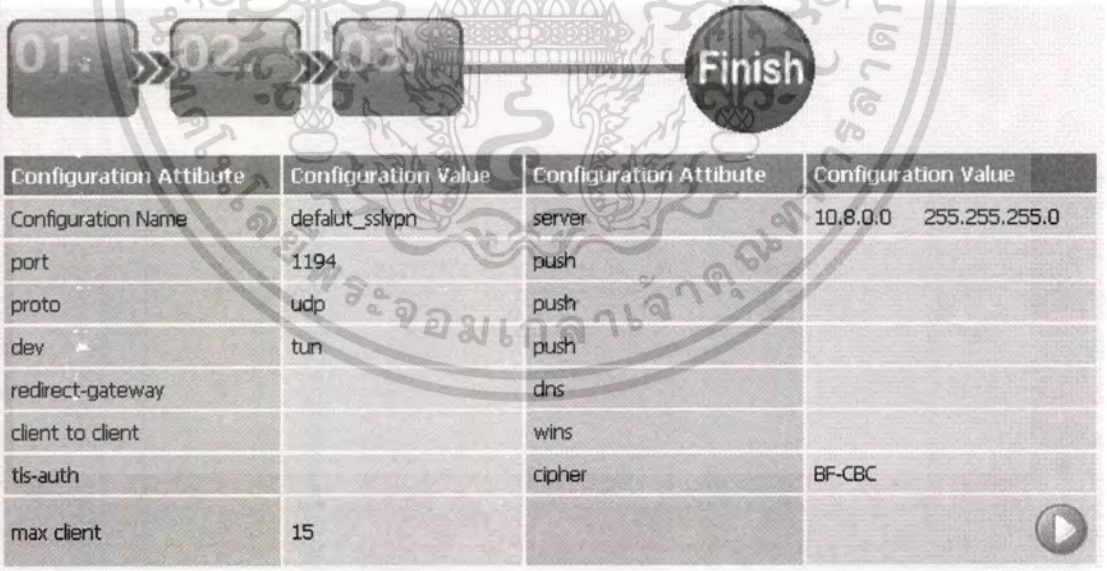


รูป หน้าจอในการทำงานจัดการผู้ใช้งาน
ภาพแสดงหน้าจอการแก้ไขซึ่งจะมีขั้นตอนเหมือนการเพิ่มไฟล์ Configuration



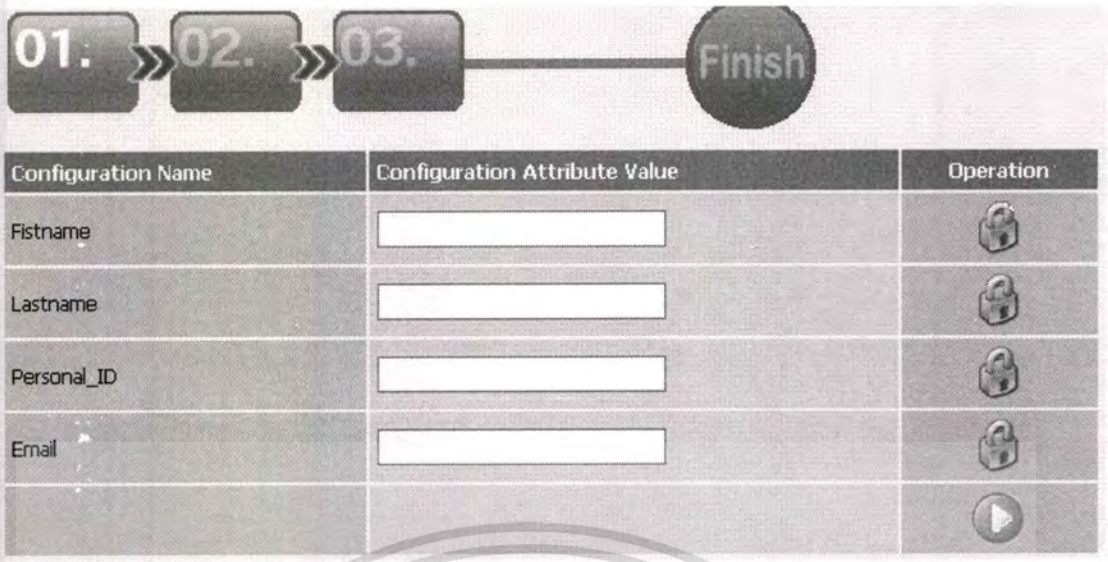
รูป หน้าจอในการทำงานจัดการผู้ใช้งาน

ภาพแสดงหน้าจอการแก้ไขซึ่งจะมีขั้นตอนเหมือนการเพิ่มไฟล์ Configuration ซึ่งถ้ามีการเพิ่มโดยการเลือก หรือ ไม่เลือกระบบจะไปทำการ เพิ่ม และ ลบให้จากไฟ Configuration



รูป หน้าจอในการทำงานจัดการผู้ใช้งาน

ภาพแสดงหน้าจอการแก้ไขซึ่งจะมีขั้นตอนเหมือนการเพิ่มไฟล์ Configuration และเมื่อการแก้ไขเสร็จก็จะทำการแสดงรายการเพื่อให้ผู้ใช้งานตรวจสอบและยืนยัน

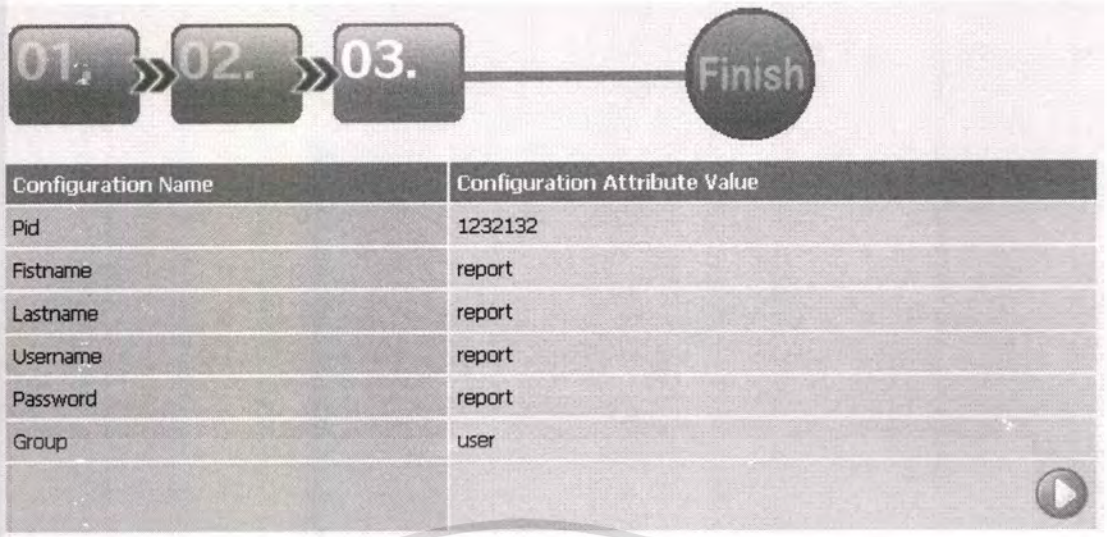


รูป หน้าจอในการทำงานจัดการผู้ใช้งาน

ภาพแสดงหน้าจอการเพิ่มผู้ใช้งานขั้นตอนแรกจะเป็นกรอกข้อมูลเกี่ยวกับข้อมูลของผู้ใช้งาน

รูป หน้าจอในการทำงานจัดการผู้ใช้งาน

ภาพแสดงหน้าจอการเพิ่มข้อมูลผู้ใช้งานขั้นตอนที่สอง จะเป็นการกรอกชื่อผู้ใช้งานและรหัสผ่าน และกลุ่มเพื่อกำหนดสิทธิการใช้งาน

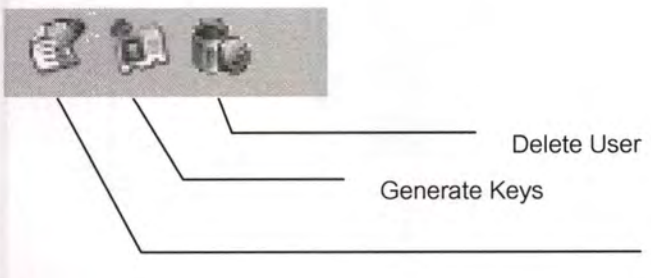


รูป หน้าจอในการทำงานจัดการผู้ใช้งาน

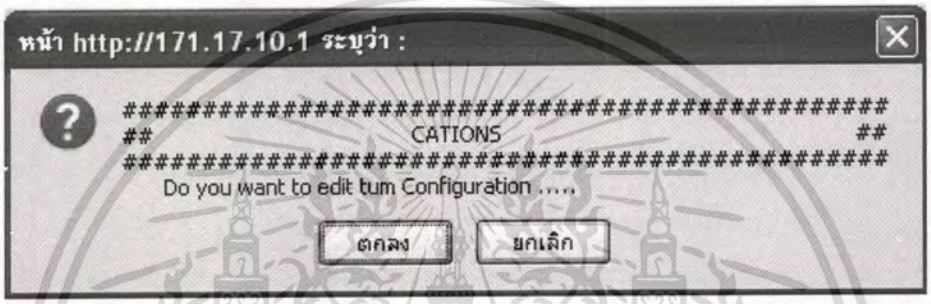
ภาพแสดงหน้าจอการเพิ่มข้อมูลผู้ใช้งานขั้นตอนสุดท้าย จะเป็นการตรวจเช็คการเพิ่มข้อมูล

รูป หน้าจอในการทำงานจัดการผู้ใช้งาน

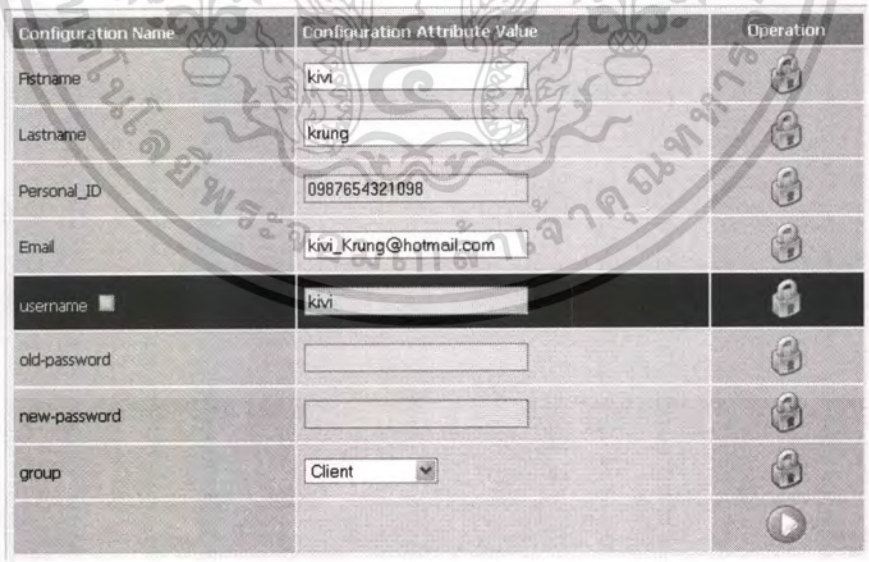
ภาพแสดงหน้าจอการจัดการข้อมูลผู้ใช้งานหลังจากที่ได้ทำการเพิ่มผู้ใช้งานเรียบร้อยแล้ว ซึ่งสามารถเลือกทว่าจะแก้ไข ลบ หรือ ทำการ Generate Key



รูป หน้าจอในการทำงานจัดการผู้ใช้งาน
ภาพแสดงหน้าจอการเพื่อยืนยันการลบผู้ใช้งาน

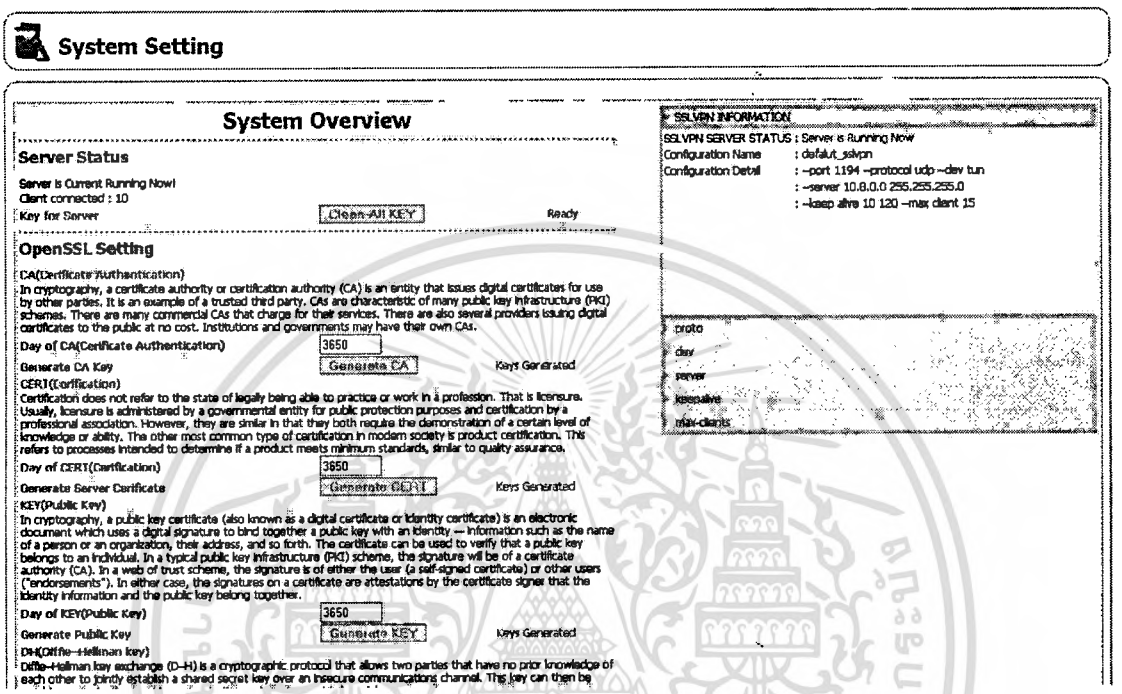


รูป หน้าจอในการทำงานจัดการผู้ใช้งาน
ภาพแสดงหน้าจอการเพื่อยืนยันการแก้ไขผู้ใช้งาน



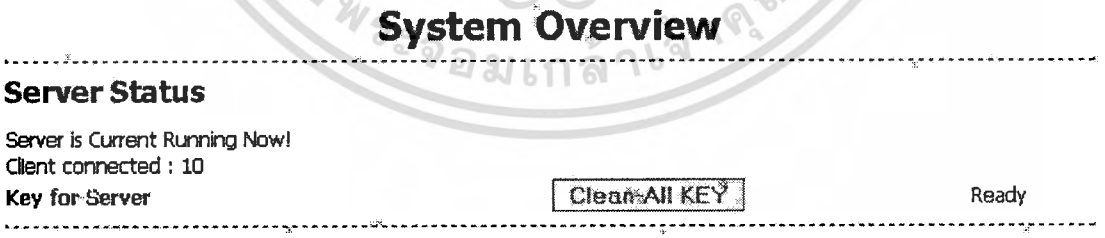
รูป หน้าจอในการทำงานแก้ไขผู้ใช้งาน
ภาพแสดงหน้าจอการแก้ไขข้อมูลผู้ใช้งานระบบ

การตั้งค่าเครือข่าย (Setting Server) เป็นการตั้งค่าต่างๆที่ใช้ในการทำงานของระบบ เช่น การสร้าง Key ที่ใช้การกำหนดระยะเวลาที่ใช้งานของแต่ละ Key การลบ Key การกำหนดค่าของ IP ADDESS ของแต่ละ Interface ที่ต้องนำไปติดต่อกับอุปกรณ์อื่น และสามารถตรวจสอบสภาพการให้บริการชองระบบว่ามีสิ่งผิดปกติหรือไม่



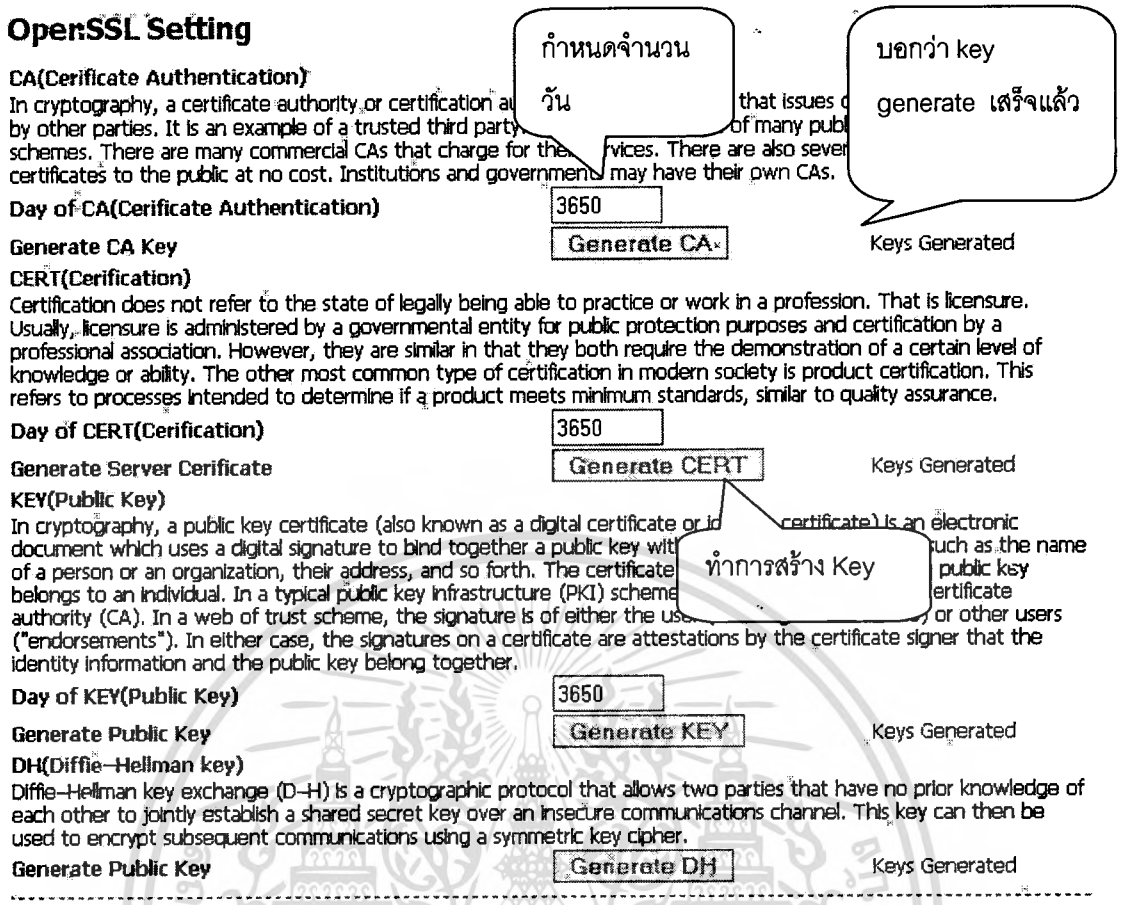
รูป หน้าจอในการตั้งค่าระบบ

ภาพแสดงหน้าการตั้งค่าของระบบโดยภาพรวม



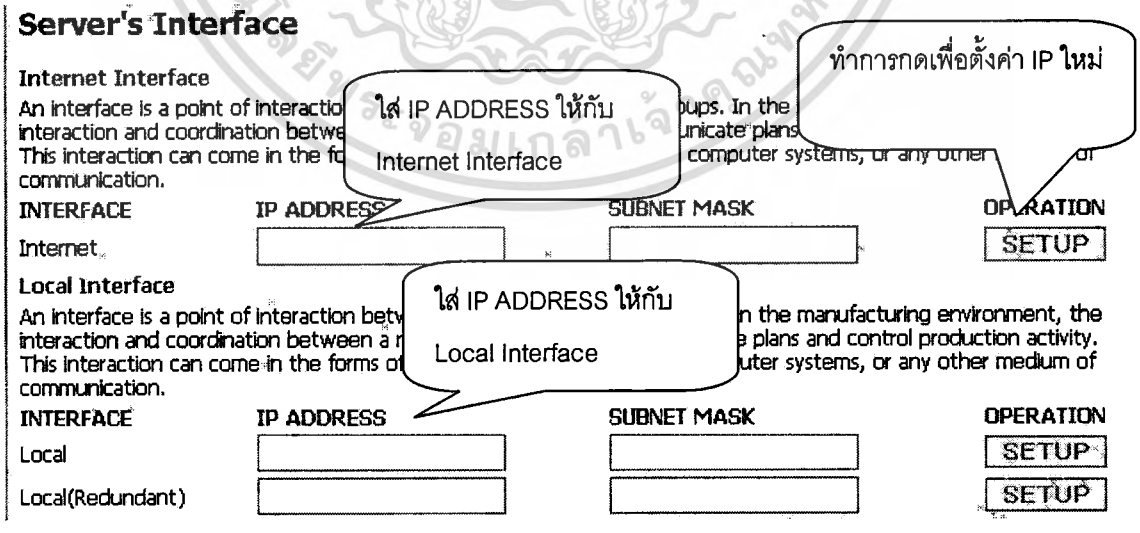
รูป หน้าจอในการตั้งค่าระบบ

ภาพแสดงหน้าแสดงสถานะของระบบ และสามารถทำการลบ key ที่ใช้อยู่ตอนนี้ทิ้งได้หมด



รูป หน้าจอในการตั้งค่าระบบ

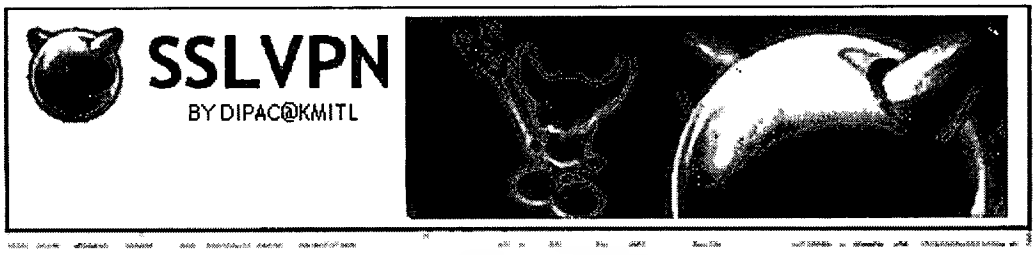
ภาพแสดงหน้าการตั้งค่าของระบบ

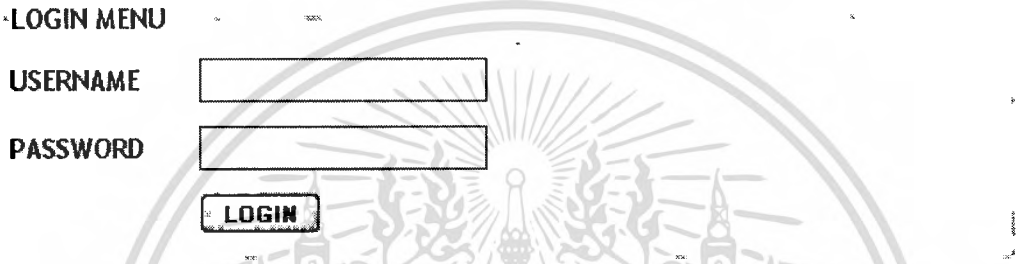


รูปที่ หน้าจอในการตั้งค่าระบบ

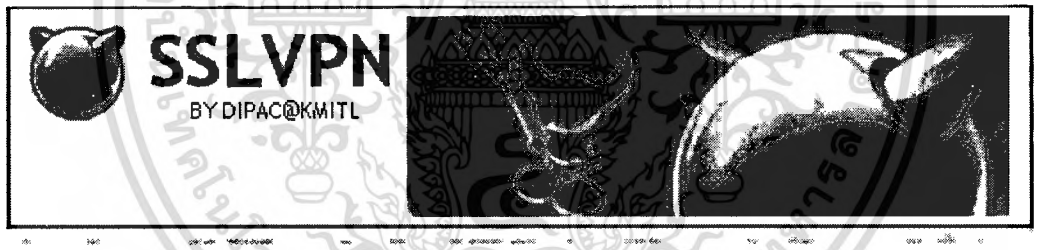
ภาพแสดงหน้าการตั้งค่าของระบบ

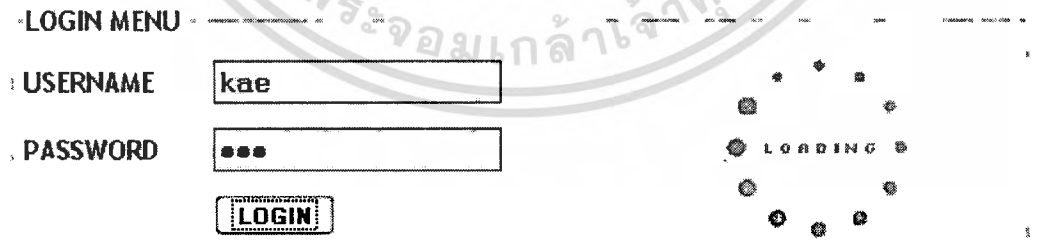
หน้าแรกของฝั่งผู้ใช้งานซึ่งจะต้องทำการ ระบุตัวตนก่อนโดยการใส่รหัสผู้ใช้งาน เพื่อให้ผู้ใช้งานสามารถเข้ามาทำการ Download Key และ ไฟล์ Configuration ของผู้ใช้งาน และรับข่าวต่างๆของ Server



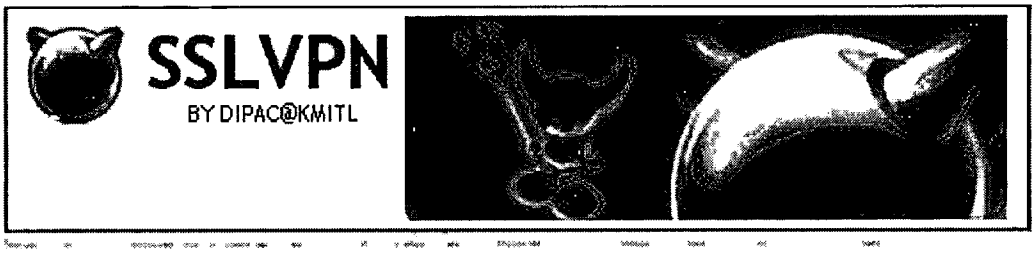


รูป หน้าจอหลักของผู้ใช้งาน

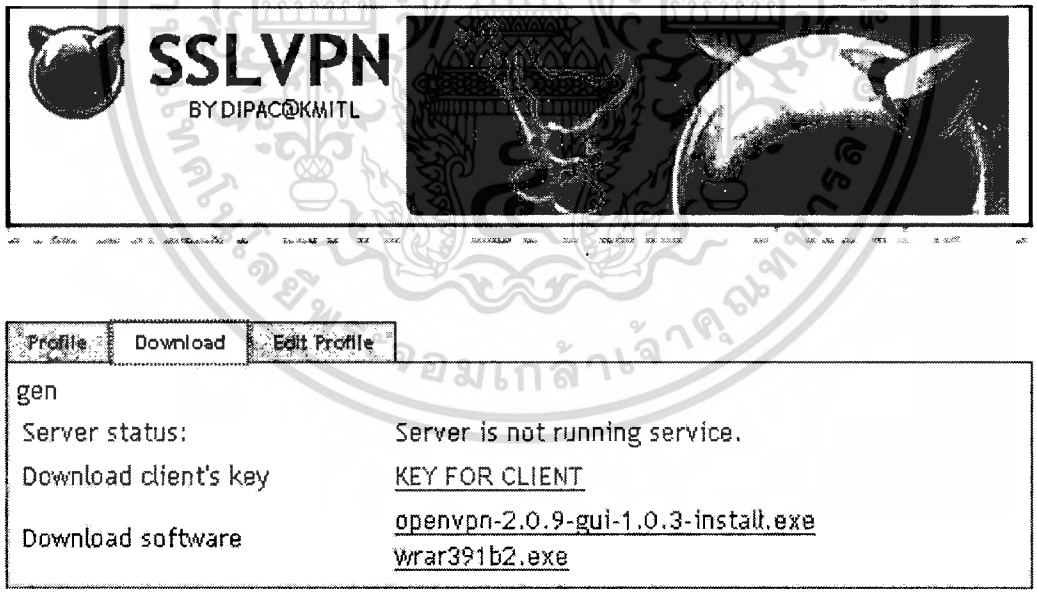




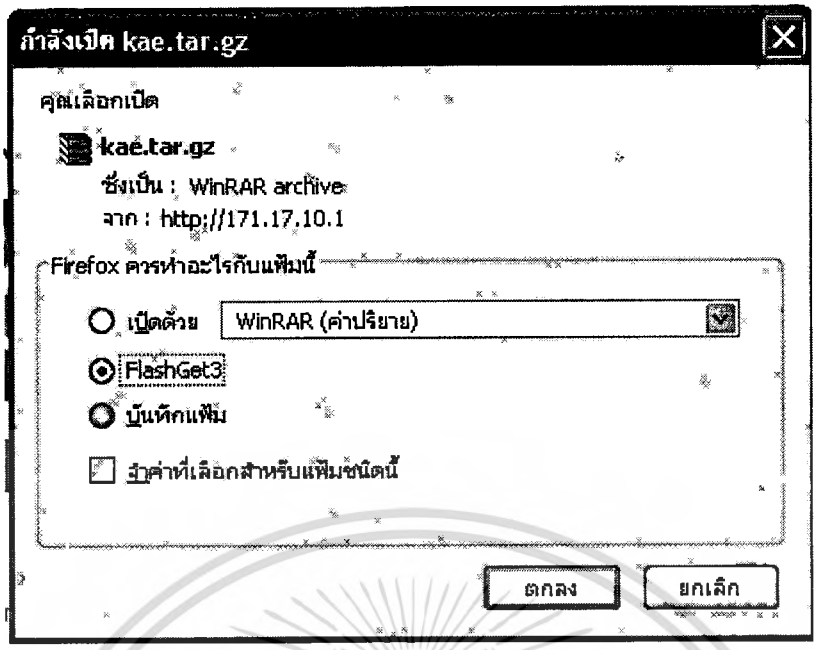
รูป หน้าจอแสดงเวลาทำการตรวจสอบผู้ใช้งาน



รูป หน้าจอหลักของผู้ใช้งานหลังจากผ่านการตรวจสอบ
ภาพแสดงส่วนผู้ใช้งานเมื่อทำการ Authentication เรียบร้อยแล้ว

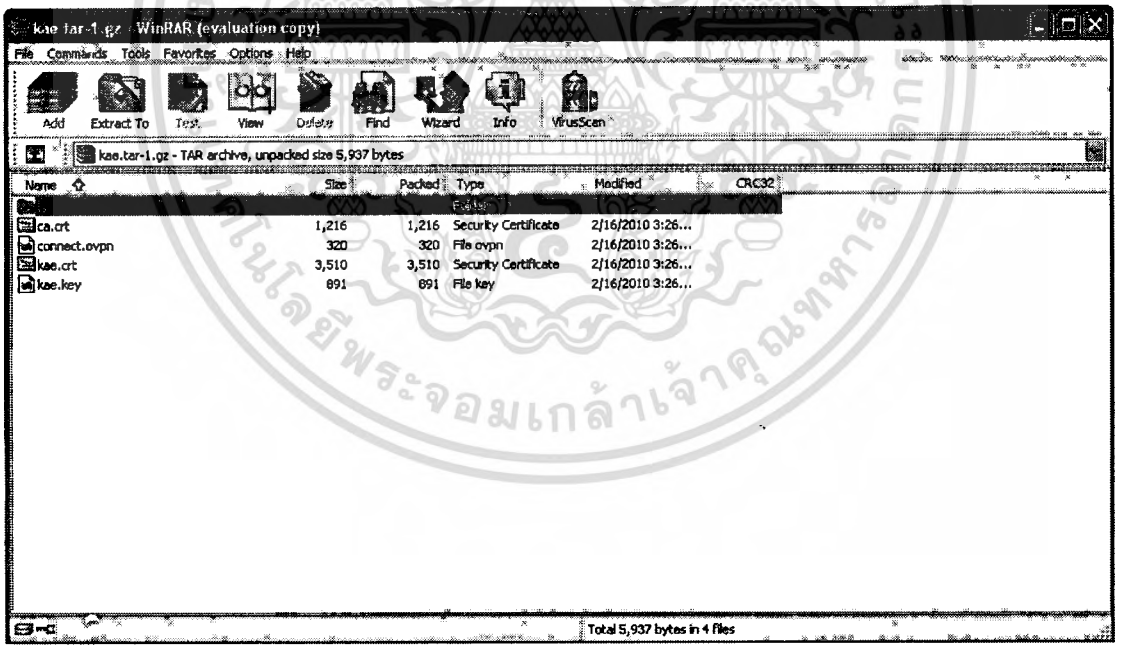


รูป หน้าจอหลักของผู้ใช้งานในกสน Download file
หลังจากทำการสร้างไฟล์ config และ key ให้ผู้ใช้งานแล้วระบบจะทำการ zip และเพื่อสะดวกแก่การนำไปติดตั้งของผู้ใช้งาน



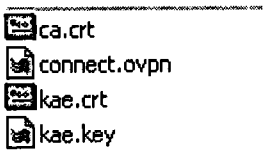
รูป ไฟล์ .ZIP ของ Client

ภาพแสดงส่วนผู้ใช้งานเมื่อทำการ Download ไฟล์ Key ของ client



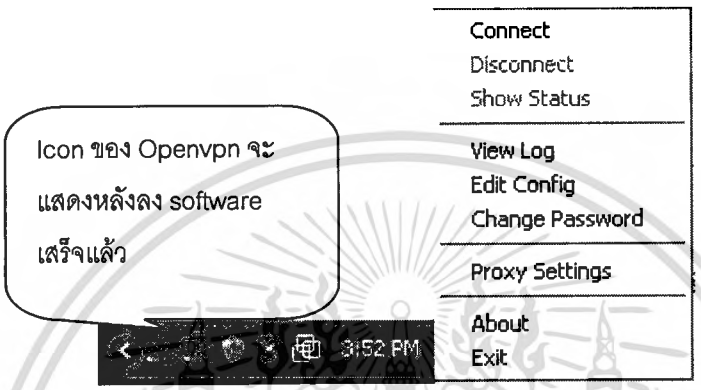
รูป ไฟล์ .ZIP ของ Client

ภาพแสดงส่วนของ Key ที่นำมา zip รวมกันไว้ในไฟล์ tar.gz



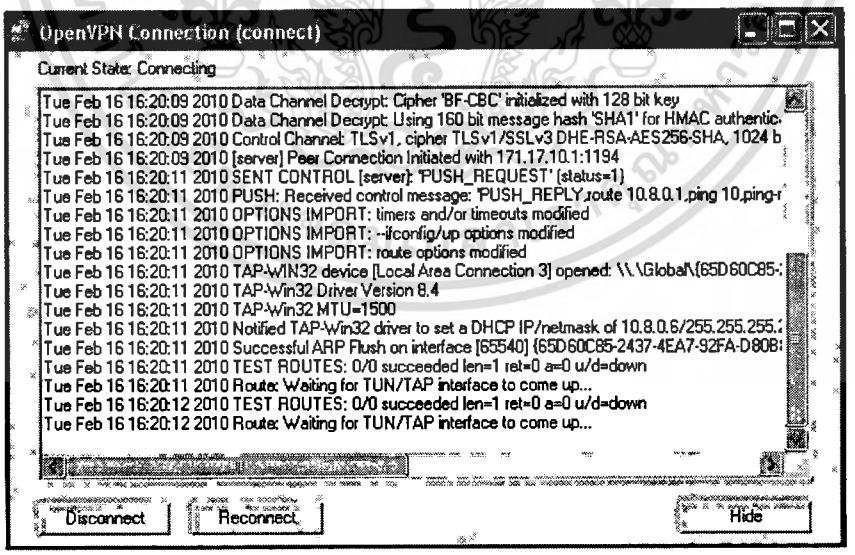
รูป ไฟล์ .ZIP ของ Client

ภาพแสดง Key ของ Client



รูป Openvpn Application ก่อนทำการเชื่อมต่อ

ภาพแสดง Taskbar ของ Client เมื่อทำการลงโปรแกรทเสร็จแล้วและเมื่อกดเมาส์ขวาที่ไอคอนดังสัญลักษณ์ แล้วกดไปที่ Connect เพื่อติดต่อกับ Server

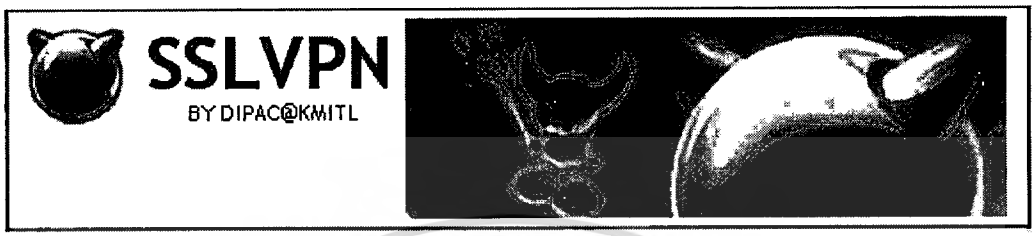


รูป Openvpn Application ตอนทำการเชื่อมต่อ

ภาพแสดงส่วนเมื่อผู้ใช้งานกดปุ่ม Connect ระบบจะทำการเชื่อมต่อและแสดง log การเชื่อมต่อดังกล่าว ถ้ามีการ Error ก็จะแสดงรายการที่ Error ออกมา

รูป Openvpn Application หลังการเชื่อมต่อสำเร็จ

ภาพแสดงส่วนทำการเชื่อมต่อกับ Server สำเร็จแล้ว



LOGIN MENU

USERNAME

PASSWORD

LOGIN

!!! Access Denial !!!
you have not permission

รูป แสดงกรณีที่ Login ไม่ผ่าน

ภาพแสดงของกรณีที่ผู้ใช้งานกรอกข้อมูลผู้ใช้งานและรหัสผ่านไม่ถูกต้อง

ประวัติผู้เขียน

ชื่อผู้เขียน	นายเฉลิมศักดิ์ เครือวัลย์
วัน เดือน ปีเกิด	18 เมษายน 2528
สถานที่เกิด	จังหวัดภูเก็ต
วุฒิระดับการศึกษา	สารสนเทศศาสตร์บัณฑิต
สถาบันที่สำเร็จการศึกษา	มหาวิทยาลัยวลัยลักษณ์
ปีที่สำเร็จการศึกษา	2550