ห้องสมุดคณะเทคโนโลยีสารสนเทศ สจล.

การพัฒนาโปรแกรมจัดการระบบเครือข่ายส่วนตัวเสมือนบนระบบปฏิบัติการ FreeBSD ผ่านทางเว็บ

The Development of Web-based Virtual Private Network Manager on FreeBSD Operating System



H002371

โดย

วิชัย เพียรดี

รหัส47066215

อาจารย์ที่ปรึกษา

ผศ.อัครินทร์ คุณกิตติ

วัน เดือน ปี 24 ก.พ. 2550
เลขทะเบียน 02371
เลขเรียกหนังสือ ลพ. 25391 2548
"ห้องสมุดคณะเทคโนโลยีสารสนเทศ สจล."

รายงานนี้เป็นส่วนหนึ่งของวิชาโครงการพัฒนาระบบงาน

หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ

ภาคเรียนที่ 2 ปีการศึกษา 2548

คณะเทคโนโลยีสารสนเทศ

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ชื่อหัวข้อ	การพัฒนาโปรแกรมจัดการระบบเครือข่ายส่วนตัวเสมือนบนระบบปฏิบัติการ FreeBSD ผ่านทางเว็บ
นักศึกษา	นายวิชัย เพียรดี
อาจารย์ที่ปรึกษา	ผศ.อัครินทร์ คุณกิตติ
ระดับการศึกษา	วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
แขนงวิชา	วิทยาการสารสนเทศ
ปีการศึกษา	2548

บทคัดย่อ

การจัดการระบบเครือข่ายส่วนตัวเสมือน(Virtual Private Network, VPN) ที่ใช้วิธีการติดตั้งแอพลิเคชั่นบนระบบปฏิบัติการ FreeBSD ส่วนใหญ่นั้นจะอยู่ในรูปแบบ Command line หรือการสร้างไฟล์คอนฟิกซึ่งมีความยุ่งยากในการจัดการ ดังนั้นในโครงงานนี้จึงได้ทำการศึกษาและวิเคราะห์ออกแบบพัฒนาโปรแกรมการจัดการเครือข่ายส่วนตัวเสมือนผ่านทางเว็บบราวเซอร์ซึ่งในส่วนการวิเคราะห์นั้นจะนำเสนอในรูปแบบ Data Flow Diagram, State Diagram และ Flowchart Diagram เป็นหลักในการแสดงขั้นตอนการทำงานของตัวโปรแกรม พร้อมทั้งได้แสดงรูปแบบของข้อมูลที่เกี่ยวข้อง (Data Format) ในโครงงานนี้เช่นกัน ส่วนหลักการทำงานของโปรแกรมนี้นั้นจะเข้าไปจัดการควบคุมแอพลิเคชั่นที่ใช้ในการสร้างเครือข่ายส่วนตัวเสมือนอีกทีหนึ่งโดยแอพลิเคชั่นที่นำมาใช้ในโครงงานนี้ก็คือ OpenVPN ซึ่งโปรแกรมที่พัฒนาขึ้นจะทำงานบนเว็บเซิร์ฟเวอร์พร้อมกับทำหน้าที่เป็น VPN เซิร์ฟเวอร์ โดยผู้ใช้จะทำการใช้โปรแกรมการจัดการเครือข่ายที่พัฒนาขึ้นนี้ผ่านเว็บบราวเซอร์จากฝั่งไคลเอ็นต์ โดยผู้ใช้จะสามารถทำการสร้างหรือลบไฟล์คอนฟิกที่เซิร์ฟเวอร์ที่ให้บริการเครือข่ายส่วนตัวเสมือนแทนการสร้างหรือลบไฟล์คอนฟิกที่เซิร์ฟเวอร์โดยตรงอีกทั้งสามารถทำการเพิ่มหรือลดการเชื่อมต่อ,ตรวจสอบสถานะ การเชื่อมต่อและตรวจสอบประวัติการเชื่อมต่อได้โดยไม่จำเป็นต้องอยู่ที่เครื่องเซิร์ฟเวอร์เพื่อจัดการระบบเครือข่าย ซึ่งผลจากการพัฒนาโครงงานนี้จะทำให้ลดความยุ่งยากในการจัดการเครือข่ายแบบเดิมอีกทั้งได้เข้าใจหลักการทำงานและการพัฒนาเครื่องมือที่ใช้ในการจัดการเครือข่ายส่วนตัวเสมือนบนระบบปฏิบัติการ FreeBSD

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Title	The Development of Web-based Virtual Private Network Manager on FreeBSD Operating System
Student	Mr. Wichai Peandee
Advisor	Asst.Prof Akharin Khunkitti
Level of Study	Master of Science in Information Technology
Major	Information Science
Academic Year	2005

ABSTRACT

In the present day, Virtual Private Network, VPN, which its applications are installed on FreeBSD operation system, almost bases on command line and configuration files which results in the difficulty in system management. As a result, this project will study, analyze and design the web-base VPN management program. In the analytic part, the presentation of the program working procedure will be mainly in the form of data flow diagram, state diagram and flowchart diagram. This project also presents data format of the related data. The principle of the program being introduced is to control the application which enables the virtual private network. The program introduced is the OpenVPN which VPN server is working on the web server. The management will be controlled through the web browser on a client side. Users from the client side are able to build or delete configuration file like those working on the server side. They are also able to add or delete connections, monitor the status and view the history file from both client side and server side. The benefits of this project is not merely to reduce the difficulty in system management but it is also to gain the understanding of the OpenVPN principle and the development of VPN management on FreeBSD operation system.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

กิตติกรรมประกาศ

โครงการพัฒนาระบบงานนี้สำเร็จลุล่วงไปด้วยดี โดยได้รับความสนับสนุนจากบุคคลหลายฝ่าย ข้าพเจ้าจึงขอขอบคุณบุคคลดังต่อไปนี้

- บิดา มารดา พี่ที่ให้ความช่วยเหลือ ดูแล และให้กำลังใจตลอดมา
- อาจารย์อัครินทร์ คุณกิตติ อาจารย์ที่ปรึกษาโครงการที่ให้คำปรึกษา ชี้แนะแนวทาง ข้อบกพร่องในการพัฒนาระบบงานนี้
- คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง และคณาจารย์ทุกท่าน ที่ให้การอบรมสั่งสอนความรู้แก่ข้าพเจ้ามาโดยตลอด
- เพื่อนร่วมรุ่น IS17 (ภาคสมทบ) ที่ร่วมเรียนและให้คำปรึกษาพร้อมกับฝ่าฟันอุปสรรคมาด้วยกัน

วิชัย เพียรดี
ผู้จัดทำ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญ

หน้า

บทคัดย่อภาษาไทย I

บทคัดย่อภาษาอังกฤษ II

กิตติกรรมประกาศ..... III

สารบัญ IV

สารบัญตาราง VI

สารบัญภาพ VII

บทที่

1. บทนำ 1

1.1 ความเป็นมา.....1

1.2 วัตถุประสงค์ของโครงการพัฒนาระบบงาน 2

1.3 ขอบเขตของโครงการพัฒนาระบบงาน 2

1.4 ขั้นตอนการดำเนินงาน 3

1.5 ประโยชน์ที่ได้รับ.....3

2. เครือข่ายส่วนตัวเสมือน.....4

2.1 ประเภทของเครือข่ายส่วนตัวเสมือน.....4

2.2.หลักการทำงานและโปรโตคอลของเครือข่ายส่วนตัวเสมือน.....7

2.3ระบบปฏิบัติการ FreeBSD 21

2.4 เครือข่ายส่วนตัวเสมือนบนระบบปฏิบัติการ FreeBSD 21

2.5 OpenVPN 22

2.6 สรุป 25

3.การวิเคราะห์และออกแบบโครงงานพัฒนาระบบ 26

3.1โครงสร้างการใช้งานของโอเพ่นวีพีเอ็น (OpenVPN) ของระบบเดิม.....26

3.2 โครงงานพัฒนาการใช้โอเพ่นวีพีเอ็น (OpenVPN) โดยผ่านเว็บเบส.....29

3.2.1 วัตถุประสงค์.....29

3.2.2 ความต้องการของระบบ.....30

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญ (ต่อ)

หน้า

3.2.3 การวิเคราะห์และออกแบบโครงร่างของโครงงานที่พัฒนา.....30
3.3 การออกแบบระบบงานส่วนข้อมูล.....39
4. การพัฒนาระบบงาน 43
4.1 เครื่องมือที่ใช้ในการพัฒนาโครงงาน..... 43
4.2 รูปแบบการใช้งานของ OpenVPN..... 43
4.3 การออกแบบฟังก์ชั่นการทำงาน.....43
4.4 การพัฒนาโครงงาน..... 54
5. การสรุปผลการทำงานของระบบ..... 72
5.1 การทดสอบโครงงาน..... 72
5.2 ผลสรุปจากการทดสอบโครงงาน..... 84
5.3 ผลสรุปการพัฒนาโครงงาน..... 84
5.4 แนวทางการพัฒนาต่อ..... 86
บรรณานุกรม 87
ภาคผนวก 88
ประวัตผู้เขียน 105

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญตาราง

หน้า

ตารางที่

3.1 ตารางที่ 3.1 รายละเอียดตาราง User..... 40
3.2 ตารางที่ 3.2 รายละเอียดตาราง IP 41
3.3 ตารางที่ 3.3 รายละเอียดตาราง Key..... 41

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญภาพ

หน้า

รูปที่

2.1 Remote Access จาก ไคลเอ็นต์ (Client) ไปยัง private network..... 5
2.2 การเชื่อมต่อแบบ Intranet (Site to Site)..... 5
2.3 แสดงการเชื่อมต่อรูปแบบต่าง คือ Remote Access, Intranet และ Extranet..... 6
2.4 Firewall based VPN..... 6
2.5 Hardware Based VPN..... 7
2.6 ลักษณะการส่งข้อมูลของ VPN 8
2.7 PPTP ติดต่อกันจากผู้รับไปจนถึงผู้ส่ง..... 9
2.8 PPTP ติดต่อกันจากไอเอสพี (ISP) ไปยัง เซิร์ฟเวอร์ (Server)..... 9
2.9 การผนึกเฟรมข้อมูล (Encapsulation) ของ PPTP 10
2.10 PPTP Control ใน TCP datagram 10
2.11 โครงสร้างของ Packet PPTP 11
2.12 สถานะขั้นการรับส่ง Message ของฝั่ง Originator..... 11
2.13 สถานะขั้นการรับส่ง Message ของฝั่ง Receiver 12
2.14 โครงสร้างของ Packet L2F 13
2.15 รูปแบบการเชื่อมต่อโดยใช้ L2F protocol 13
2.16 รูปกระบวนการส่งข้อมูลโดยใช้ L2F 14
2.17 รูปแบบการเชื่อมต่อโดยใช้ L2TP protocol 15
2.18 โครงสร้างของ Packet L2TP 15
2.19 Packet L2TP เมื่อใช้ร่วมกับ IPSec Protocol 15
2.20 การผนึกเฟรมข้อมูล (Encapsulation) ของ L2TP 16
2.21 Format of the L2TP control message 16
2.22 รูปแบบแพ็กเก็ตโปรโตคอล AH 17
2.23 รูปแบบแพ็กเก็ตโปรโตคอล ESP 17
2.24 รูปแบบแพ็กเก็ต IPSec SA 18

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญภาพ (ต่อ)

หน้า

2.25 รูปแบบแพ็กเก็ต IPSec Transport Mode 18

2.26 รูปแบบแพ็กเก็ต IPSec Tunneling Mode..... 19

2.27 Symmetric Encryption 20

2.28 Asymmetric Encryption 20

2.29 โครงสร้าง Packet ของ TUN 22

2.30 การเชื่อมต่อโดยใช้ TUN 23

2.31 การเชื่อมต่อโดยใช้ TAP 23

2.32การเชื่อมต่อโดยใช้ TUN 24

2.33 การรับส่งโดยใช้ OpenVPN..... 25

3.1 แสดงการจัดการเครือข่ายโดยการแก้ไขไฟล์คอนฟิก..... 27

3.2 แสดงการจัดการเครือข่ายโดยการส่ง Command Line..... 28

3.3 แสดงภาพรูปแบบการเชื่อมต่อโดยรวมของระบบว่ามีการเชื่อมต่ออย่างไร..... 31

3.4 แสดงองค์ประกอบการทำงานของระบบ..... 31

3.5 แสดงภาพรวม Function การทำงานของระบบ..... 32

3.6 แสดงสัญลักษณ์ของการไหลของข้อมูล..... 33

3.7 แสดง Context Diagram ของระบบจัดการVPN บน FreeBSD 33

3.8 แสดงการไหลของข้อมูลของระบบจัดการVPN บน FreeBSD ระดับ level 0 (DFD 0) 33

3.9 แสดงการไหลของข้อมูลของระบบจัดการVPN บน FreeBSD (DFD level 1 Process 1) 34

3.10 แสดงการไหลของข้อมูลของระบบจัดการVPN บน FreeBSD (DFD level 1 Process 2) 34

3.11แสดงการไหลของข้อมูลของระบบจัดการVPN บน FreeBSD (DFD level 1 Process 3) 35

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญภาพ (ต่อ)

หน้า

3.12 สเตทไดอะแกรม แสดงขั้นตอนการทำงานของ Function ADD 36
3.13 สเตทไดอะแกรม แสดงขั้นตอนการทำงานของ Function Delete..... 37
3.14 สเตทไดอะแกรม แสดงขั้นตอนการทำงานของFunction Historyและ Help..... 37
3.15 สเตทไดอะแกรม แสดงขั้นตอนการทำงานของ Function monitor.....38
3.16 สเตทไดอะแกรม แสดงขั้นตอนการทำงานของ Function Active 38
3.17 สเตทไดอะแกรมแสดงขั้นตอนการทำงานของFunction Stop Service..... 39
3.18 แบบจำลองความสัมพันธ์ระหว่างเอนทิตีส่วนข้อมูล.....40
3.19 แสดงรูปแบบข้อมูลภายในไฟล์คอนฟิก.....41
3.20 แสดงตัวอย่างข้อมูลภายในไฟล์คอนฟิก.....41
4.1 Flow Chart แสดงการเพิ่มผู้ใช้ในระบบ 45
4.2 Flow Chart แสดงการลบข้อมูลตลอดจนไฟล์คอนฟิกของผู้ใช้ในระบบ..... 46
4.3 Flow Chart แสดงกระบวนการของฟังก์ชั่น Help ในระบบ..... 47
4.4 Flow Chart แสดงกระบวนการของฟังก์ชั่น History 48
4.5 Flow Chart แสดงกระบวนการของฟังก์ชั่น Monitor ในกรณีตรวจสอบการให้บริการ (On Service) ทีละ 1 Username 49
4.6 Flow Chart แสดงกระบวนการของฟังก์ชั่น Monitor ในกรณีตรวจสอบการเชื่อมต่อ ทีละ 1 Username..... 50
4.7 Flow Chart แสดงกระบวนการของฟังก์ชั่น Monitor ในกรณีตรวจสอบการให้บริการ พร้อมกันทั้งหมด..... 51
4.8 Flow Chart แสดงกระบวนการของฟังก์ชั่นActive Service ในกรณีการสตาร์ทเซอร์วิส ทีละ 1 User.....52
4.9 Flow Chart แสดงกระบวนการของฟังก์ชั่นActive Service ในกรณีการสตาร์ทเซอร์วิส พร้อมกันทั้งหมด..... 53

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญภาพ (ต่อ)

หน้า

4.10 Flow Chart แสดงกระบวนการของฟังก์ชั่นStop Service ในกรณีหยุดให้บริการทีละ 1 User..... 53

4.11 Flow Chart แสดงกระบวนการของฟังก์ชั่นStop Service ในกรณีหยุดให้บริการ พร้อมกันทั้งหมด..... 54

4.12 แสดงส่วนติดต่อผู้ใช้ Login 61

4.13 แสดงส่วนติดต่อผู้ใช้ Main (Admin)..... 62

4.14 แสดงส่วนติดต่อผู้ใช้ Main Menu 62

4.15 แสดงส่วนติดต่อผู้ใช้ List Function 63

4.16 แสดงส่วนติดต่อผู้ใช้ ของ Generate Key..... 63

4.17 แสดงส่วนติดต่อผู้ใช้ ของ Add User 64

4.18 แสดงส่วนติดต่อผู้ใช้ ของ Delete/Change Status User 64

4.19 แสดงส่วนติดต่อผู้ใช้ ของ File Configure Management 65

4.20 แสดงส่วนติดต่อผู้ใช้ ของ Normal Create File (Simple)..... 65

4.21 แสดงส่วนติดต่อผู้ใช้ ของ Advance Create File 66

4.22 แสดงส่วนติดต่อผู้ใช้ ของ Export File Client /Secret Key ส่วน Admin..... 67

4.23 แสดงส่วนติดต่อผู้ใช้ ของ Status UseropenVPN..... 68

4.24 แสดงส่วนติดต่อผู้ใช้ ของ Log UseropenVPN..... 68

4.25 แสดงส่วนติดต่อผู้ใช้ ของ Admin OpenVPN 69

4.26 แสดงส่วนติดต่อผู้ใช้ ของการจัดการ OpenVPNโดยผู้ใช้ (User)..... 70

5.1 แสดง Topology ที่ใช้ในการทดสอบ..... 72

5.2 แสดงหน้าการ login โดยอยู่ใน Group Admin..... 73

5.3 แสดงหน้าแรกหลังจาก Login เข้ามาโดยอยู่ใน Group Admin..... 74

5.4 แสดงหน้าการเพิ่มรายชื่อเข้าไปในระบบ..... 74

5.5 แสดงผลจากการเพิ่มรายชื่อเข้าไปในระบบ..... 75

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญภาพ (ต่อ)

หน้า

5.6 แสดงการสร้างคีย์เพื่อใช้ในการเข้ารหัสของผู้ใช้..... 75
5.7 แสดงผลลัพธ์การสร้างคีย์เพื่อใช้ในการเข้ารหัสของผู้ใช้..... 76
5.8 แสดงการสร้างไฟล์คอนฟิกของผู้ใช้..... 76
5.9 แสดงการสร้างไฟล์คอนฟิกของผู้ใช้แบบ Normal 77
5.10 แสดงการสตาร์ทเซอร์วิสของผู้ใช้ 77
5.11 แสดงสถานะการให้บริการ 78
5.12 แสดงสถานการณ์ให้บริการและการเชื่อมต่อทั้งหมด..... 78
5.13 แสดงหน้าการ login โดยอยู่ใน Group User 79
5.14 แสดงหน้าการ Export File ของผู้ใช้ 80
5.15 แสดงสถานะการให้บริการและการเชื่อมต่อ ของผู้ใช้..... 81
5.16 แสดงการใช้โปรแกรม Telnet เข้าไปใช้บริการ..... 82
5.17 แสดงการใช้โปรแกรม Ethereal เพื่อตรวจจับ Packet ของข้อมูล..... 83
5.18 แสดงการใช้โปรแกรม Telnet เข้าไปใช้บริการผ่าน Tunneling 83
5.19 แสดงการใช้โปรแกรม Ethereal เพื่อตรวจจับ Packet ของข้อมูลที่ผ่าน Tunneling..... 84

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 1
บทนำ

1.1 ความเป็นมา

ในการเชื่อมต่อคอมพิวเตอร์จากระยะไกลเข้ามายังเครือข่ายบริษัทหรือองค์กรภายในนั้นมีได้หลายวิธีไม่ว่าจะเป็นการใช้โมเด็มเชื่อมต่อเข้ามายังเครือข่ายโดยผ่านสายโทรศัพท์หรือการใช้วงจรเช่าคู่สาย (Leased Line) ตลอดจนการใช้วิธีเชื่อมต่อผ่านเครือข่ายสาธารณะ (Public Network)เพื่อใช้ในการส่งผ่านข้อมูลระหว่างจุดสองจุดซึ่งแต่ละวิธีนั้นมีข้อดีข้อเสียแตกต่างกันออกไปเช่นการเช่าคู่สาย(Lease Line)หรือการใช้โมเด็มเชื่อมต่อเข้ามายังเครือข่ายโดยใช้สายโทรศัพท์แต่วิธีการดังกล่าวนั้นมีข้อจำกัดในเรื่องของค่าใช้จ่ายหรือความคล่องตัวในการเชื่อมต่อจากสถานที่ต่างๆ กล่าวคือการใช้โมเด็มนั้นระยะทางถ้ายิ่งไกลค่าใช้จ่ายก็ยิ่งมากส่วนวงจรเช่า (Leased Line) นั้นการเคลื่อนย้ายทำได้ลำบากอีกทั้งถ้าTraffic น้อยก็ไม่คุ้มค่า ส่วนวิธีการเชื่อมต่อเครือข่ายสาธารณะ (Public Network) นั้นจะมีปัญหาเกี่ยวกับระบบความปลอดภัยเนื่องจากเป็นการเชื่อมต่อผ่านเครือข่ายสาธารณะ (Public Network)ดังนั้นเพื่อเป็นการลดข้อจำกัดเกี่ยวกับความปลอดภัยในการส่งข้อมูลผ่านเครือข่ายสาธารณะ(Public Network)นั้นจึงมีคิดระบบเครือข่ายส่วนตัวเสมือน (Virtual Private Network) หรือที่เรียกว่า VPN ขึ้นเพื่อใช้ในการเชื่อมโยงคอมพิวเตอร์ที่อยู่ห่างไกลออกไปให้สามารถติดต่อรับส่งข้อมูลระหว่างเครือข่ายภายในองค์กรหรือบริษัทโดยผ่านเครือข่ายสาธารณะ (Public Network) แต่ยังคงมีความปลอดภัยในการใช้งานเสมือนเป็นโครงข่ายส่วนตัวโดยข้อดีของ VPNคือราคาถูกอีกทั้งสามารถเชื่อมต่อได้จากที่ไหนก็ได้ตราบเท่าที่เครือข่ายสาธารณะครอบคลุมอยู่ เครือข่ายสาธารณะที่จะกล่าวในที่นี้จะหมายถึง อินเตอร์เน็ต (Internet) นอกจากจะใช้เครือข่ายส่วนตัวเสมือนในการเชื่อมต่อผ่านเครือข่ายสาธารณะ(Public Network)แล้วยังสามารถนำไปใช้ในระบบที่เป็นวงจรเช่าคู่สาย(Leased Line) หรือ การเชื่อมต่อผ่านโมเด็ม (Modem) ได้อีกด้วย

แต่การจัดการระบบเครือข่ายส่วนตัวเสมือนที่ใช้บนระบบปฏิบัติการ FreeBSDส่วนใหญ่นั้นจะใช้อยู่ในรูปแบบ Command line หรือไฟล์คอนฟิก ซึ่งทำให้เกิดความไม่สะดวกในการจัดการระบบเครือข่ายดังนั้นในโครงงานนี้จึงนำเสนอแนวทางและหลักการพร้อมทั้งการวิเคราะห์ออกแบบเพื่อนำไปใช้ในการพัฒนาโปรแกรมการจัดการเครือข่ายส่วนตัวเสมือนผ่านทางเว็บบราวเซอร์ซึ่งโปรแกรมนี้จะเข้าไปจัดการควบคุมแอพลิเคชั่นที่ใช้ในการสร้างเครือข่ายส่วนตัวเสมือนอีกทีหนึ่งซึ่งแอพลิเคชั่นที่นำมาใช้ในโครงงานนี้ก็คือ OpenVPN ซึ่งการสร้างการเชื่อมต่อของ OpenVPN

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เดิมนั้นใช้ Command Line ร่วมกับไฟล์คอนฟิกเช่นเดียวกันกับแอพลิเคชั่นส่วนใหญ่ที่ใช้ในการสร้างเครือข่ายส่วนตัวเสมือนอื่นๆบนระบบปฏิบัติการ FreeBSD

โดยโครงงานพัฒนาระบบงานนี้มุ่งเน้นพัฒนาโปรแกรมเพื่อใช้ในการจัดการระบบการทำงานของเครือข่ายส่วนตัวเสมือน(VPN) โดยใช้แอพลิเคชั่น OpenVPN บนระบบปฏิบัติการ FreeBSD ซึ่งโครงงานที่พัฒนาขึ้นนี้จะทำงานเป็นส่วนติดต่อกับผู้ใช้ผ่านเว็บบราวเซอร์ซึ่งตัวโปรแกรมจะเข้าไปสร้างไฟล์คอนฟิกพร้อมกับส่ง Command Line ให้แทนการส่ง Command Line หรือสร้างไฟล์คอนฟิกโดยตรงซึ่งจะต้องอยู่ที่ตัวเซิร์ฟเวอร์แต่ด้วยความสามารถของโปรแกรมที่พัฒนาขึ้นนั้นจะสามารถทำการเพิ่มหรือลดการเชื่อมต่อ, ตรวจสอบสถานะ การเชื่อมต่อและตรวจสอบประวัติการเชื่อมต่อได้โดยไม่จำเป็นต้องอยู่ที่เครื่องเซิร์ฟเวอร์เพื่อจัดการระบบเครือข่าย

1.2 วัตถุประสงค์ของโครงการพัฒนาระบบงาน

1.2.1 เพื่อพัฒนาเครื่องมือในการจัดการเครือข่ายส่วนตัวเสมือน OpenVPNบนระบบปฏิบัติการ FreeBSD

1.2.2 เพื่อศึกษาการพัฒนาเครื่องมือที่ช่วยในการจัดการเครือข่ายส่วนตัวเสมือน OpenVPN บนระบบปฏิบัติการ FreeBSD

1.2.3 เพื่อศึกษาการทำงานตลอดจนวิธีการติดตั้งของระบบเครือข่ายส่วนตัวเสมือนบนระบบปฏิบัติการ FreeBSD

1.2.4 เพื่อลดความยุ่งยากในการจัดการเครือข่ายส่วนตัวเสมือนด้วย OpenVPN

1.3 ขอบเขตของโครงการพัฒนาระบบงาน

1.3.1โครงงานพัฒนาระบบงานนี้มุ่งเน้นการพัฒนาโปรแกรมที่ใช้ในการจัดการเครือข่ายส่วนตัวเสมือนบนระบบปฏิบัติการ FreeBSD โดยใช้แอพลิเคชั่น OpenVPN โครงงานที่พัฒนาขึ้นนี้จะทำงานโดยผ่านทางเว็บบราวเซอร์ ซึ่งโปรแกรมนี้จะเข้าไปจัดการควบคุมแอพลิเคชั่นที่ใช้ในการสร้างเครือข่ายส่วนตัวเสมือน (OpenVPN) โดยสามารถสร้างไฟล์คอนฟิกพร้อมกับส่ง Command Line ให้แทนการส่ง Command Line หรือสร้างไฟล์คอนฟิกโดยตรงซึ่งจะต้องอยู่ที่ตัวเซิร์ฟเวอร์อีกทั้งสามารถทำการเพิ่มหรือลดการเชื่อมต่อ,ตรวจสอบสถานะ การเชื่อมต่อและตรวจสอบประวัติการเชื่อมต่อได้

1.3.2 การพัฒนาโปรแกรมเพื่อใช้ในการจัดการระบบครือข่ายเสมือนผ่านทางเว็บนั้นจะเป็นการโปรแกรมโดยใช้ภาษา PHP, Perl รวมไปถึง Shell Script

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

1.3.3 สรุปผลที่ได้จากการทดสอบโปรแกรมว่า สามารถทำงานได้ตามความต้องการหรือไม่ดังนี้

- การทำงานของ Function Module Add, Delete ว่าสามารถเพิ่มหรือลดจำนวน User ในระบบงานได้หรือไม่

- การทำคอนฟิกพารามิเตอร์ของ User แต่ละคนเพื่อใช้ในการสร้าง Tunneling ระหว่าง Client และ Server ได้หรือไม่

- ทำการ Active หรือ Deactivate status ให้ On Service พร้อมกันทั้งหมดหรือทีละหนึ่ง User ได้หรือไม่

- สามารถตรวจสอบการเชื่อมต่อของ User ตลอดจนการ On Service ของระบบได้

- สามารถตรวจสอบประวัติการใช้งานจาก History (Log File) ได้

1.4 ขั้นตอนการดำเนินงาน

1.4.1 ศึกษาระบบการทำงานของเครือข่ายส่วนตัวเสมือน

1.4.2 ศึกษาการติดตั้งตลอดจนวิธีการใช้งานเครือข่ายส่วนตัวเสมือนบนระบบปฏิบัติการ FreeBSD ด้วยแอพลิเคชั่น OpenVPN

1.4.3 ศึกษาคุณสมบัติและวิธีการโปรแกรมด้วยภาษา PHP, Perl และ Shell Script

1.4.4 กำหนดความต้องการและออกแบบขั้นตอนการทำงานของโครงงานพัฒนาระบบการจัดการเครือข่ายส่วนตัวเสมือนผ่านทางเว็บ

1.4.5 พัฒนาโครงงาน

1.4.6 ทดสอบและปรับปรุงตัวโครงงาน

1.4.7 สรุปผลที่ได้จากการทดสอบว่าตัวโปรแกรมทำงานได้ตามความต้องการหรือไม่

1.5 ประโยชน์ที่ได้รับ

1.5.1 เข้าใจการทำงานของระบบเครือข่ายส่วนตัวเสมือนบนระบบปฏิบัติการ FreeBSD

1.5.2 เข้าใจคุณลักษณะการควบคุมโปรแกรมแอพลิเคชั่นผ่านทางเว็บ

1.5.3 เรียนรู้การโปรแกรมด้วยภาษา PHP, Perl และ Shell Script

1.5.4 สามารถนำความรู้ที่ได้จากการพัฒนาโครงงาน นำไปประยุกต์ใช้กับการพัฒนาการเขียนโปรแกรมเพื่อควบคุมแอพลิเคชั่นอื่นๆผ่านทางเว็บ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 2
เครือข่ายส่วนตัวเสมือน
(Virtual Private Network)

เครือข่ายส่วนตัวเสมือน (VPN) มีหลายประเภทซึ่งแต่ละประเภทนั้นก็จะมีวิธีแบ่งไปตามลักษณะการใช้งานแตกต่างกันขึ้นอยู่กับจะใช้หลักเกณฑ์อะไรในการแบ่งประเภทของเครือข่ายส่วนตัวเสมือน โดยหลักเกณฑ์ที่ใช้นั้นโดยส่วนใหญ่ที่ใช้นั้นมีอยู่ 2 อย่างคือ

1. ลักษณะการใช้งาน
2. ลักษณะของตัวอุปกรณ์

2.1 ประเภทของ Virtual Private Network (VPN)

VPN สามารถแบ่งวิธีการแบ่งชนิดของVPNได้2แบบ คือ [2]

2.1.1 แบ่งตามรูปแบบการใช้งาน

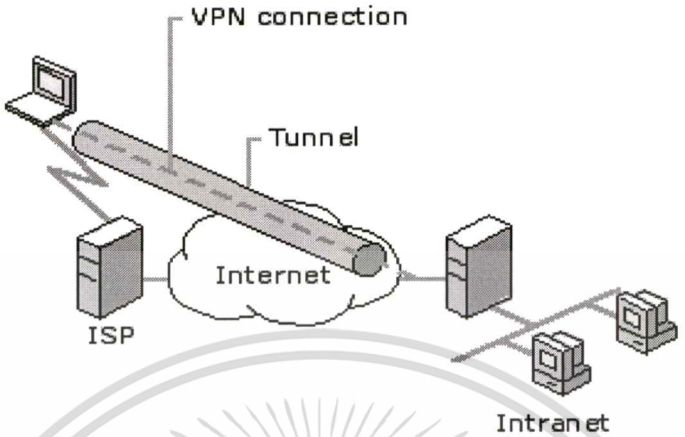
2.1.2 แบ่งตามลักษณะของผลิตภัณฑ์ที่ใช้งาน

โดยการแบ่งแบบแรกนั้นเป็นการแบ่งตามการเชื่อมต่อเพื่อใช้งานในขณะที่แบบที่สองนั้นเป็นการแบ่งตามลักษณะอุปกรณ์ที่มีแอพลิเคชั่น(Application) อยู่ภายในอุปกรณ์โดยที่แอพลิเคชั่น (Application) นั้นก็คือ ซอฟต์แวร์ (Software) ที่ใช้ติดตั้งระบบ VPN

2.1.1 แบ่งตามรูปแบบการใช้งาน ได้3ประเภทคือ [5]

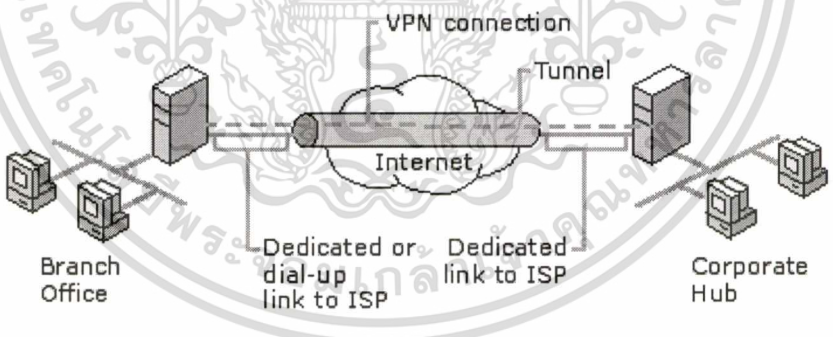
2.1.1.1 Remote Access เป็นการเชื่อมต่อเข้ามายังเครือข่ายจากภายนอกด้วยการใช้อุปกรณ์เคลื่อนที่ซึ่งมีลักษณะสองแบบคือแบบแรกเป็นการเชื่อมระหว่างHostของผู้ใช้เข้ามายังHostในเครือข่ายโดยผ่านอินเตอร์เน็ตกล่าวคือจะใช้อินเตอร์เน็ตเป็นตัวกลางในการติดต่อ ซึ่งจะมีการเข้ารหัส(สร้าง Tunneling) จากเครื่องไคลเอ็นต์(Client)ไปยังเซิร์ฟเวอร์(Server) ปลายทาง แบบที่สองเป็นการเชื่อมต่อมาที่เครื่องNAS(Network Access Server) โดยผ่านทางอินเตอร์เน็ต โดยเริ่มจาก ไคลเอ็นต์ (Client) Dial-up ผ่านโมเด็ม(Modem) มายัง ISP จากนั้นทาง ISP ก็จะสร้าง Tunneling ไปยังเซิร์ฟเวอร์ ปลายทาง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 2.1 Remote Access จาก ไคลเอ็นต์ (Client) ไปยัง private network

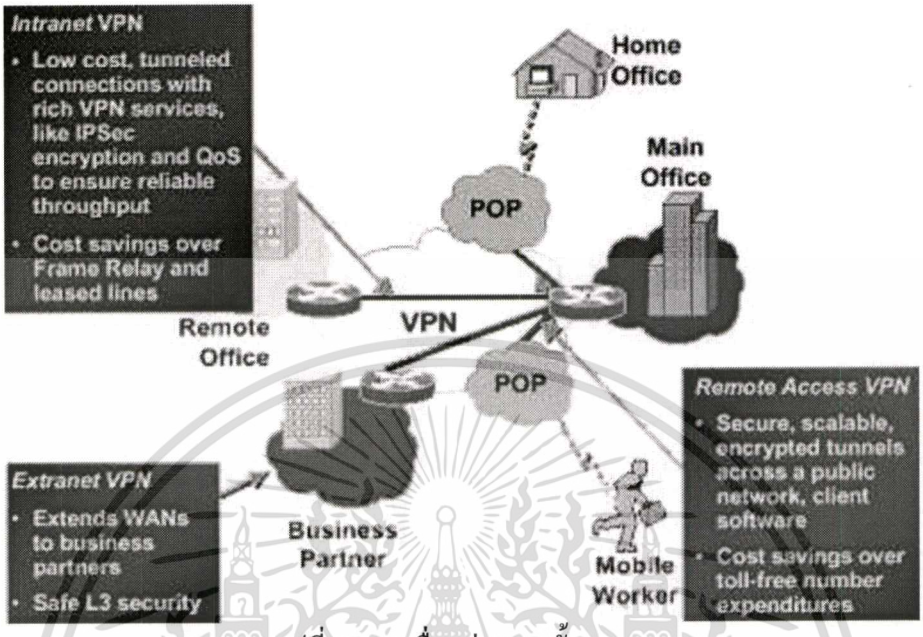
2.1.1.2 Intranet Base เป็นการเชื่อมต่อเครือข่ายภายในองค์กรหรือบริษัทเท่านั้นซึ่งองค์กรที่มีสาขาหรือสำนักงานหลายแห่งจะเชื่อมต่อเครือข่ายของแต่ละที่เข้ากับอินเตอร์เน็ตในท้องถิ่นของตนเพื่อเชื่อมต่อเข้ากับเครือข่าย VPN ขององค์กรอีกที



รูปที่ 2.2 การเชื่อมต่อแบบ Intranet (Site to Site)

2.1.1.3 Extranet Baseเป็นการเชื่อมต่อเครือข่ายระหว่างบริษัทหรือองค์เข้าด้วยกันซึ่งมีลักษณะคล้ายกับการเชื่อมต่อแบบ Intranet เพียงแต่ขยายการติดต่อไปยังองค์หรือบริษัทอื่นๆด้วยแทนที่จะเชื่อมต่อเฉพาะภายในองค์กรเท่านั้น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

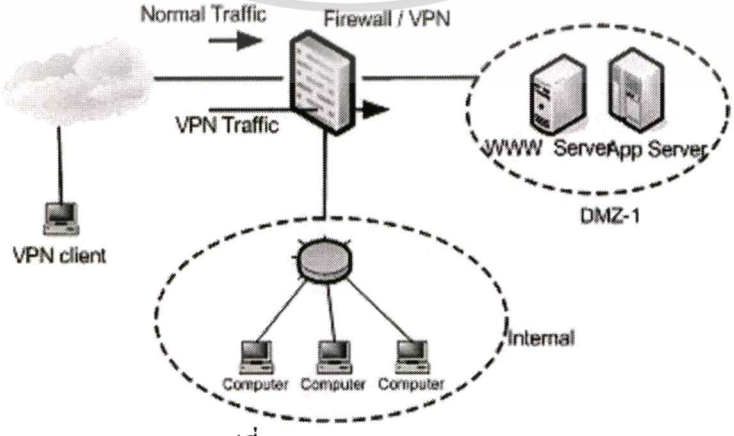


รูปที่2.3 การเชื่อมต่อVPNทั้ง 3แบบ

จากรูปที่ 2.3 แสดงการเชื่อมต่อรูปแบบต่าง คือ Remote Access, Intranet และ Extranet

2.1.2 แบ่งตามลักษณะของผลิตภัณฑ์ ได้3 ประเภท [2] คือ

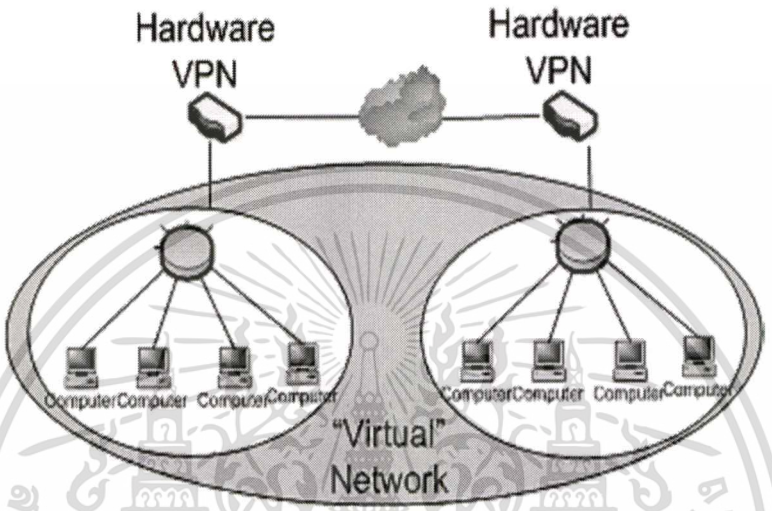
2.1.2.1. Firewall Based VPN เป็นการผนวกเพิ่มความสามารถในการทำ VPN ให้แก่อุปกรณ์ Firewall การรวมการทำให้ตัวอุปกรณ์ Firewall มีหน้าที่การทำงาน2ลักษณะคือ ควบคุมทราฟฟิคทั่วไปและหากทราฟฟิคนั้นเป็นของ VPN Firewall ก็จะทำหน้าที่เป็นVPN Gateway ทำหน้าที่ถอดรหัสข้อมูลที่ต้องการสื่อสารในVPN Packet ออกมาแล้วส่งต่อไปยังเครือข่ายที่ต่ออยู่หลังอุปกรณ์ Firewall ดังรูปที่2.4



รูปที่ 2.4 Firewall based VPN

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.1.2.2 Hardware Based VPN เป็นอุปกรณ์ที่ผลิตขึ้นเพื่อทำหน้าที่เป็น VPN โดยเฉพาะ ซึ่งในบางครั้งก็จะมีการรวม ความสามารถในการทำVPNเข้ากับ Router ด้วยอาจจะเรียกVPN ชนิดนี้ว่า Router-Based VPN ก็ได้



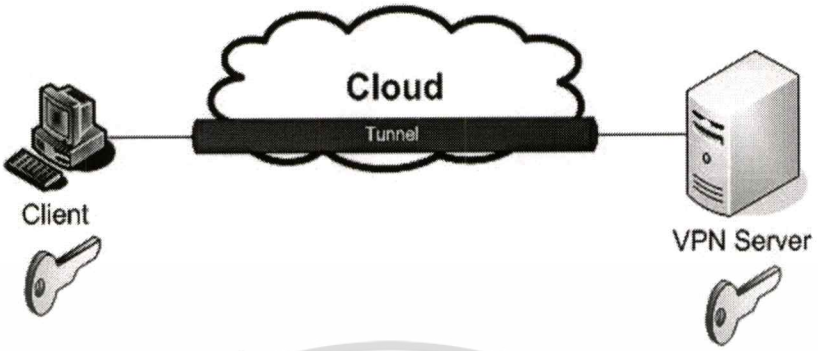
รูปที่ 2.5 Hardware Based VPN

2.1.2.3 Standalone VPN Application หรืออาจเรียกว่า Software based VPN ก็ได้ VPN ชนิดนี้เป็น ซอฟต์แวร์ (Software) ที่ทำหน้าที่เป็น VPN ทั้งส่วน เซิร์ฟเวอร์ (Server) และ ไคลเอ็นต์ (Client) ซึ่ง ซอฟต์แวร์ (Software) จะทำหน้าที่ทั้งสร้าง tunneling ในการส่งข้อมูลรวมถึงการเข้ารหัสถอดรหัสของข้อมูลโดยไม่เกี่ยวข้องกับ Hardware ใดๆจึงมีความยืดหยุ่นพอสมควร

2.2.หลักการทำงานและโปรโตคอล ของ VPN

VPN เป็นการเชื่อมโยงคอมพิวเตอร์ที่อยู่ห่างไกลออกไปโดยผ่านทางอินเตอร์เน็ตแต่ยังคงมีความปลอดภัยในการรับส่งข้อมูลการที่VPN มีคุณสมบัตินี้ได้นั้นเนื่องมาจากVPN ใช้เทคนิคการรับส่งข้อมูลที่เรียกว่า "Tunneling" ซึ่งเปรียบเสมือนท่อรับส่งข้อมูลระหว่างคอมพิวเตอร์สองระบบที่ผ่านเครือข่ายอินเตอร์เน็ต โดยที่ ท่อสำหรับรับส่งข้อมูลหรือ Tunnel เกิดจากการรับส่งข้อมูลเฟรม IP ระหว่างเครื่องด้วยการผนึกข้อมูลเฟรมIP (encapsulation) ที่ต้องการส่งด้วยโปรโตคอลพิเศษ ทำให้ผู้อื่นไม่สามารถอ่านได้ [1]

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 2.6 ลักษณะการส่งข้อมูลของ VPN

ในการสร้างเครือข่าย VPN นั้นมี โปรโตคอลที่ใช้สร้างระบบอยู่4โปรโตคอลหลักคือ [3]

- PPTP (Point – To – Point Tunneling Protocol)
- L2F (Layer-2 Forwarding)
- L2TP (Layer-2 Tunneling Protocol)
- IPSec (IP Security Protocol)

นอกเหนือจากโปรโตคอลทั้ง 4 นี้แล้วยังมีวิธีการสร้างเครือข่ายVPN ในรูปแบบอื่นได้อีก อาจจะเป็นรูปแบบเฉพาะหรือที่เรียกกันว่า “Proprietary” [6] เช่น

- PPP Over SSH
- VPND
- VTun
- Tinc

โดยรูปแบบลักษณะนี้มักเป็น Application ส่วนใหญ่ซึ่งอาจเป็น Freeware หรือ Commercial ก็ได้แต่ในที่นี้จะกล่าวถึงเฉพาะบางตัวเท่านั้น

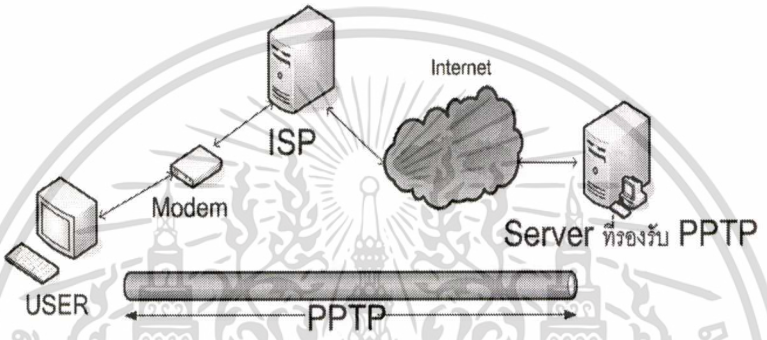
2.2.1. VPN PROTOCOL

2.2.1.1 PPTP (Point-to-Point Tunneling Protocol)

โปรโตคอล PPTP เป็นโปรโตคอลใน Layer ที่ 2 โดยโปรโตคอล PPTP จะใช้โปรโตคอล TCP ในการสร้าง Tunnel และใช้โปรโตคอลPPP เป็นตัวรับส่งข้อมูลที่ต้องการติดต่อระหว่างผู้รับและผู้ส่งซึ่งการเชื่อมต่อของโปรโตคอลชนิดนี้มีสองรูปแบบคือ วิธีแรก ใช้ PPTP ติดต่อกันจากผู้รับไปจนถึงผู้ส่ง ส่วนวิธีที่สองนั้นใช้ PPTPเฉพาะส่วนที่ติดต่อระหว่าง ISP ไปยังปลายทางเท่านั้น โดยวิธีแรกนั้นทั้ง ไคลเอ็นต์ (Client)และ เซิร์ฟเวอร์ (Server) จะต้องรองรับ โปรโตคอล PPTP ทั้งคู่ แต่ตอนเริ่มต้นนั้นจะใช้โปรโตคอลPPP เพื่อรับส่งข้อมูลเพื่อใช้ในการติดต่อจากนั้นเมื่อติดต่อได้

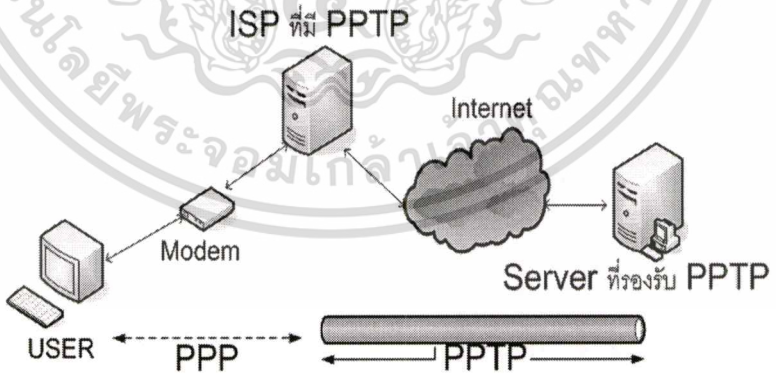
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

แล้วก็จะใช้โปรโตคอล PPTP วิธีนี้ ISP ไม่จำเป็นต้องรองรับ PPTP เลย ส่วนวิธีที่สองนั้นผู้รับส่งต้นทางนั้นไม่จำเป็นต้องมี ซอฟต์แวร์(Software) หรือ Application ที่รองรับการส่งข้อมูลของ PPTP แต่จะส่งข้อมูลไปยัง ISP โดยใช้ การส่งแบบ PPP แทน โดยที่ ISP นั้นจะทำหน้าที่ส่งข้อมูลนั้นไปยัง เซิร์ฟเวอร์ (Server) ปลายทางโดยใช้ PPTP โดยที่ เซิร์ฟเวอร์ (Server) นั้นก็ต้องรองรับ PPTP ด้วย



รูปที่ 2.7 PPTP ติดต่อกันจากผู้รับไปจนถึงผู้ส่ง

รูปที่ 2.7 แสดงการเชื่อมต่อการส่งผ่านข้อมูลผ่าน PPTPตลอดทาง โดยที่ ไคลเอ็นต์ (Client) และเซิร์ฟเวอร์ (Server) ปลายทางต้องรองรับ PPTP ทั้งคู่ (วิธีแรก)

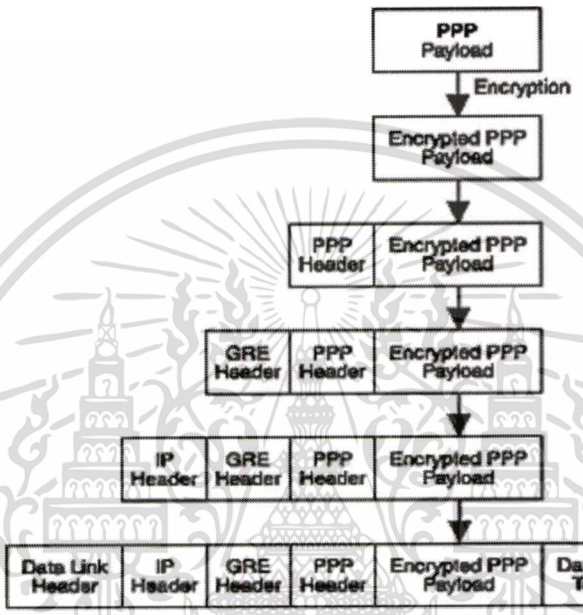


รูปที่ 2.8 PPTP ติดต่อกันจากไอเอสพี (ISP) ไปยัง เซิร์ฟเวอร์ (Server)

รูปที่ 2.8 แสดงการเชื่อมต่อการส่งผ่านข้อมูลผ่าน PPTP โดยที่ ไคลเอ็นต์ (Client) ไม่จำเป็นต้องรองรับ PPTP เลยโดยปล่อยให้เป็นหน้าที่ ของ ISP (Internet Service Provider) แทน ซึ่ง ISP จะต้องรองรับ PPTP

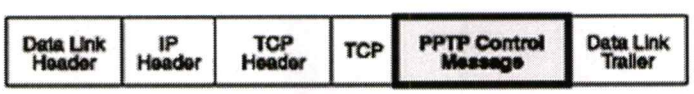
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ในการสร้าง Tunneling นั้น PPTP ใช้โปรโตคอล GRE (Generic Routing Encapsulation) ในการสร้าง Tunneling (RFC 2637) ดังนั้นในส่วนของ PPTP Header นั้นจะประกอบด้วย GRE Header กับ PPP Header ในหนังสือบางเล่มจะรวมเรียก PPTP Header



รูปที่ 2.9 การผนึกเฟรมข้อมูล (Encapsulation) ของ PPTP

จากรูปที่ 2.9 เฟรม ข้อมูลPayload จะถูกผนึก (Encapsulate) อยู่ในเฟรม PPP โดยจะเพิ่ม PPP Header ข้างหน้าเฟรมจากนั้นเฟรม PPP ก็จะถูกผนึกให้อยู่ในเฟรมGRE (Generic Routing Encapsulation) โดย มีGRE Header เพิ่มเข้ามาต่อจากนั้นจะมีการเพิ่ม IP Header เข้าไปซึ่ง IP Header นี้จะประกอบด้วยIP –ของ ไคลเอ็นต์ (Client) และ เซิร์ฟเวอร์ (Server) ปลายทางที่รองรับ PPTP เมื่อถึงขั้นตอนนี้เฟรมก็จะถูกผนึกอีกครั้งในส่วนของ Data Link ตามปกติแล้วจึงส่งออกไปยัง ISP (Public Network)

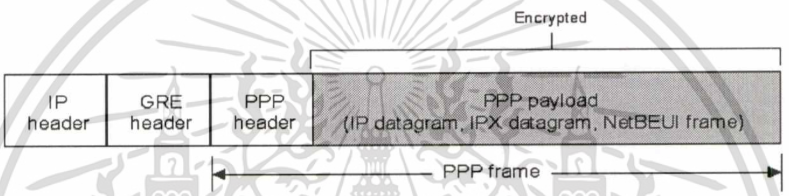


รูปที่ 2.10 PPTP Control ใน TCP datagram

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

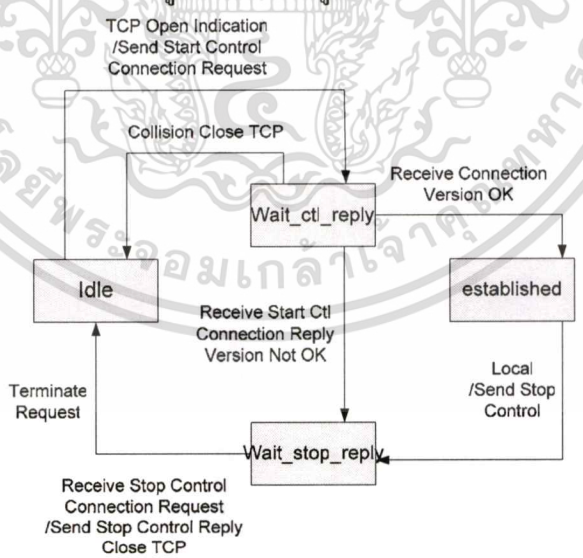
ส่วนรูปที่ 2.10 นั้นแสดง PPTP Control message ใน TCP datagram โดยที่ Control message จะใช้ในการติดต่อเพื่อสร้างการเชื่อมต่อกับปลายทาง Message ที่ใช้ก็มีเช่น Start-Control-Connection-Request ใช้Request จากฝั่ง ไคลเอ็นต์ (Client) เพื่อสร้างการเชื่อมต่อ, Start-Control-Connection-Replyใช้สำหรับResponse จากฝั่ง เซิร์ฟเวอร์ (Server) ไปยัง ไคลเอ็นต์ (Client) ว่าได้รับ Start-Control-Connection จาก ไคลเอ็นต์ (Client) แล้วเป็นต้น

และเนื่องจาก PPTP นั้นห่อหุ้ม packet ของ PPP อีกทีหนึ่งนั้นทำให้โปรโตคอล PPTP มีความยืดหยุ่นสามารถรองรับ โปรโตคอลอื่นๆนอกจาก โปรโตคอล IP เช่น IPX, NetBEUI เป็นต้น



รูปที่ 2.11 โครงสร้างของ Packet PPTP

ขั้นตอนการส่ง Message และสถานะของ ไคลเอ็นต์ (Client) หรือ เซิร์ฟเวอร์ (Server) ของโปรโตคอล PPTP สามารถแสดงได้ดังรูปที่ 2.12 และรูปที่ 2.13

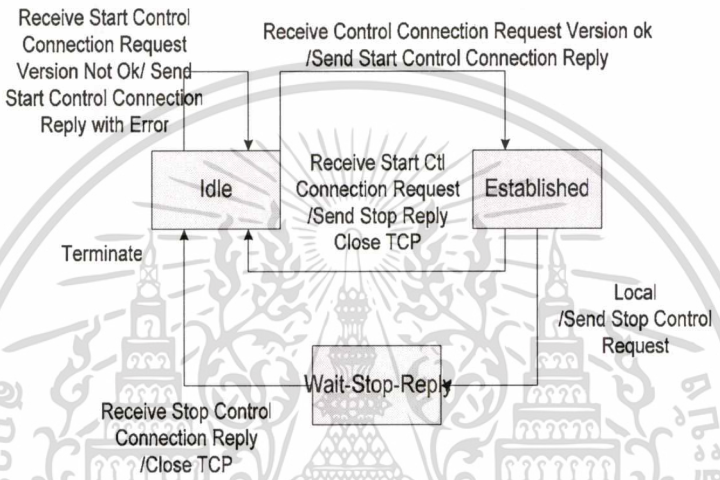


รูปที่2.12 สถานะขั้นการรับส่ง Message ของฝั่ง Originator

เริ่มจากฝั่งเริ่มสร้างการเชื่อมต่ออยู่ในสถานะ Idle ได้ส่ง Message Start Control Connection ไปยังฝั่งตรงข้ามเมื่อส่งเสร็จก็จะอยู่ในสถานะรอ Message Control ตอบกลับมาถ้าไม่มีการตอบกลับอาจเนื่องมาจากการชนกันของข้อมูลก็จะกลับสู่สภาวะ Idle เช่นเดิมแต่ถ้าได้รับ Message Start

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

กลับมาก็จะเปลี่ยนสถานะไปที่ Established ซึ่งเป็นสถานะที่ใช้สร้างและส่งข้อมูลตามปกติ และเมื่อต้องการจะปิด Tunneling ก็จะส่ง Message Send Stop Control ออกไปก่อนที่จะเปลี่ยนสถานะเป็น Wait_stop_reply และเมื่อได้รับ Message Send Stop Control กลับมาก็จะเปลี่ยนสถานะเป็น Idle ดังเดิม



รูปที่ 2.13 สถานะขั้นการรับส่ง Message ของฝั่ง Receiver

จากรูปที่ 2.13 เริ่มจากทางฝั่งรับได้รับ Message Control Connection Request ทางฝั่งรับก็จะส่ง Message Start Control Connection Reply ไปก่อนจะเปลี่ยนไปอยู่ในสถานะ Established เพื่อสร้างการเชื่อมต่อและรับส่งข้อมูล และเมื่อต้องการที่จะทำการปิดหรือจบการเชื่อมต่อก็จะส่ง Message Stop Control ไปยังฝั่งตรงข้ามเมื่อส่งเสร็จก็จะเปลี่ยนสถานะเป็น Wait _stop_reply และเมื่อได้รับ Message Stop Control Reply กลับมาก็จะปิดการเชื่อมต่อพร้อมกับเปลี่ยนสถานะไปเป็น Idle

ส่วนในเรื่องของการพิสูจน์ตัวตนนั้นโปรโตคอล PPTP จะอาศัย โปรโตคอลPPP ดังนั้น โปรโตคอล PPTP จะใช้กลไกการพิสูจน์ตัวตนของผู้ใช้ (Authentication) คือ โปรโตคอล PAP (Password Authentication Protocol) และ CHAP (Challenge Handshaking Authentication Protocol) ซึ่งต่อมาถูกพัฒนาเป็น MS-CHAP (Microsoft Challenge Handshaking Authentication Protocol) โดยบริษัท Microsoft ส่วนการเข้ารหัสนั้นโปรโตคอลสามารถใช้โปรโตคอล PPP ในการเข้ารหัสได้แต่ ทาง Microsoft ใช้ โปรโตคอล MPPE (Microsoft Point-to-Point Encryption) ซึ่งมีความปลอดภัยมากกว่า

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.2.1.2 L2F (Layer 2 Forwarding)

L2F หรือ Layer 2 Tunneling เป็นการเชื่อมต่อคอมพิวเตอร์จากระยะไกลผ่านอินเตอร์เน็ต โดยจะทำงานใน Layer ที่ 2 เช่นเดียวกับ PPTP โปรโตคอล L2F ถูกออกแบบมาใช้กับการสร้างการเชื่อมต่อที่ปลอดภัยระหว่างผู้ใช้กับเครือข่ายขององค์กร ข้อแตกต่างระหว่าง โปรโตคอล PPTP กับ L2F คือ

- PPTP ไม่มีการ Authentication (ต้องอาศัย PPP) ในขณะที่ L2F มีการ Authentication ที่ปลายสองด้าน อีกทั้งL2F ต้องการระบบที่สนับสนุนทั้งใน แอคเซสเซิร์ฟเวอร์ (Access Server) และ Router

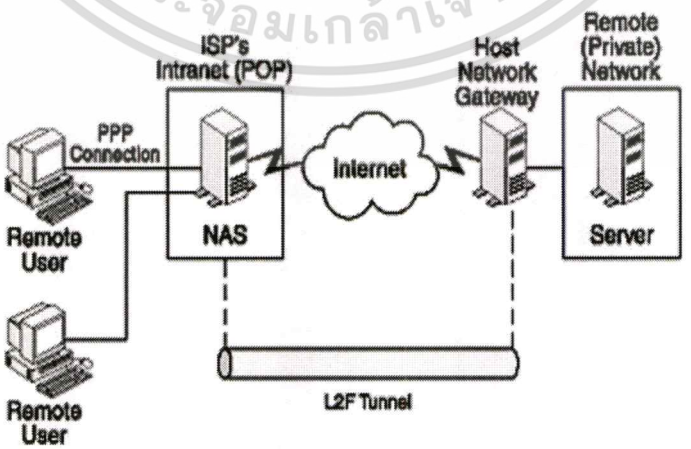
- การสร้าง "Tunneling" ของ L2F ไม่ขึ้นกับ Protocol IP ดังนั้น L2F สามารถทำงานร่วมกับโปรโตคอลอื่นโดยตรงได้เช่น เฟรมรีเลย์ และ ATM เป็นต้น

การตรวจสอบผู้ใช้ของโปรโตคอลL2Fแบ่งออกเป็น2ลำดับคือลำดับแรกจะตรวจสอบที่ISP ก่อนที่จะสร้างTunneling ลำดับที่สองจะทำเมื่อได้สร้างการเชื่อมต่อกับเกตเวย์ (Gateway) ของเครือข่ายขององค์กรแล้ว



รูปที่ 2.14 โครงสร้างของ Packet L2F

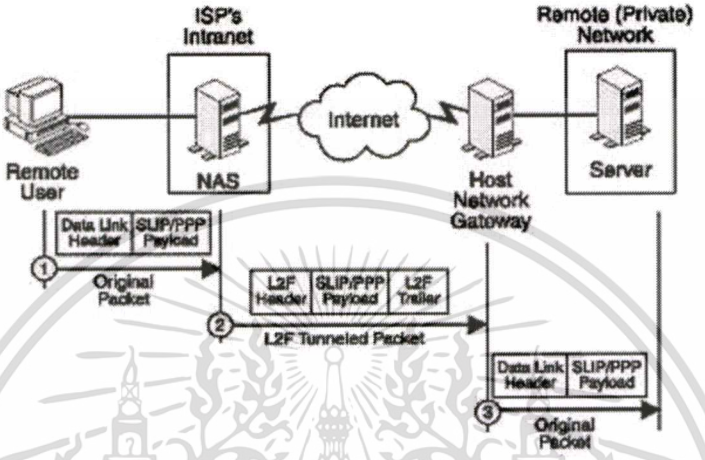
รูปที่ 2.14 แสดงถึงโครงสร้าง Packet ของโปรโตคอล L2F โดยส่วนของ L2F checksum นั้นอาจจะมีหรือไม่มีก็ได้



รูปที่ 2.15 รูปแบบการเชื่อมต่อโดยใช้ L2F protocol

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

รูปที่ 2.15 แสดงการเชื่อมต่อโดยใช้ L2F การเชื่อมต่อแบบนี้จะส่งข้อมูลผ่าน L2F ระหว่าง ISP (Internet Service Provider) กับ Gateway ปลายทางเท่านั้น



รูปที่ 2.16 รูปกระบวนการส่งข้อมูลโดยใช้ L2F

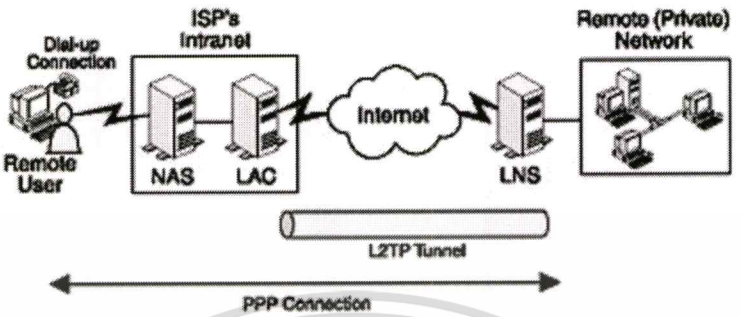
จากรูปที่ 2.16 เฟรมข้อมูลถูกส่งจากต้นทางโดย User หลังจากนั้นที่ NAS (Network Access เซิร์ฟเวอร์ (Server)) เฟรมข้อมูลจะถูกเพิ่ม L2F Header เข้ามาโดยอาจจะมี L2F checksum อยู่ด้วย ก่อนที่จะถูกถอดเอา L2F Header ออกที่ Host Network Gateway ปลายทางจากนั้นก็จะเหลือเฟรมข้อมูลส่งไปยัง เซิร์ฟเวอร์ (Server) (Private) ที่อยู่ในเครือข่ายที่ต้องการเข้าไปใช้ทรัพยากร

2.2.1.3 L2TP (Layer 2 Tunneling Protocol)

โปรโตคอล L2TP ถูกกำหนดให้เป็นมาตรฐานโดย IETF (Internet Engineering Task Force) เพื่อใช้แทนโปรโตคอล PPTP และ L2F เพื่อขจัดข้อบกพร่องของ โปรโตคอลทั้งสอง

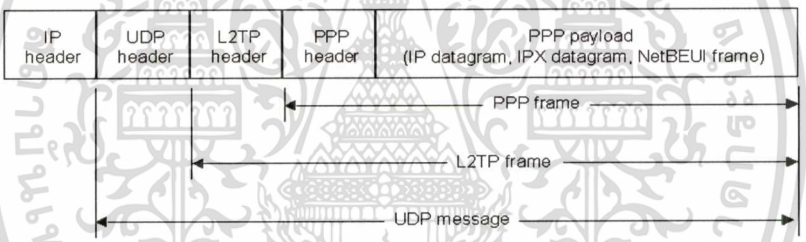
โปรโตคอลนี้เป็นการรวมความสามารถและข้อดีของโปรโตคอล PPP และ L2F เข้าด้วยกัน โดยการทำงานของโปรโตคอล L2TPนี้มีการทำงานคล้ายกับโปรโตคอลPPPแต่ต่างกันตรงที่ โปรโตคอลL2TP จะใช้โปรโตคอลUDP Port 1701 ในการตกลงรายละเอียดการรับส่งข้อมูลและ สร้างTunneling แทนการใช้โปรโตคอลTCP ส่วนตัวข้อมูลนั้นจะรับส่งโดยใช้ UDP/PPP ผ่าน Tunnel ที่สร้างขึ้นแทนการใช้TCP/IP ส่งไปกับ PPP โปรโตคอล L2TP ยังสามารถผนึก (Encapsulate)ข้อมูลเฟรม PPP แล้วส่งผ่านไปในเครือข่าย IP,X.25,Frame Relay หรือ ATM(Asynchronous Transfer Mode) ได้ ทำให้ L2TPมีความยืดหยุ่นสูงในการส่งผ่านข้อมูลข้อมูล ที่ส่งไปนั้นอาจมีการเข้ารหัสหรือบีบอัดข้อมูลก่อนส่งก็ได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



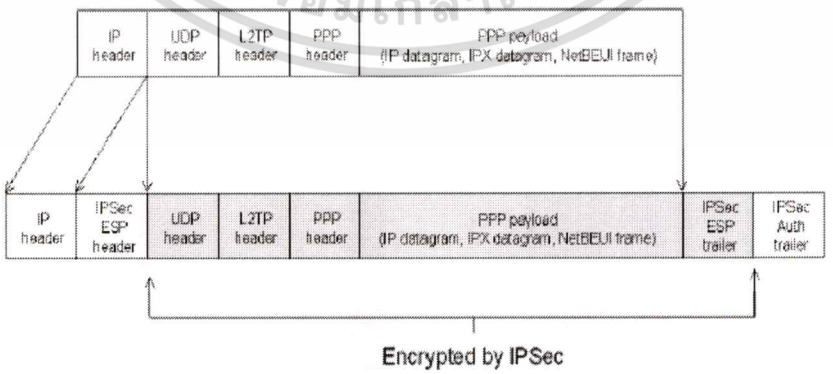
รูปที่ 2.17 รูปแบบการเชื่อมต่อโดยใช้ L2TP protocol

จากรูปที่2.17 เฟรมข้อมูลที่ส่งออกจาก LAC (L2TP Access Concentrators) จะถูกผนึกเฟรมโดยโปรโตคอล L2TP จากนั้นก็จะส่งไปยัง LNS (L2TP Network เซิร์ฟเวอร์ (Server)) โดยที่ LNS จะทำการถอดผนึกออกให้เหลือเฟรมข้อมูลแล้วส่งไปยัง Remote (Private) Network ปลายทางต่อไป



รูปที่ 2.18โครงสร้างของ Packet L2TP

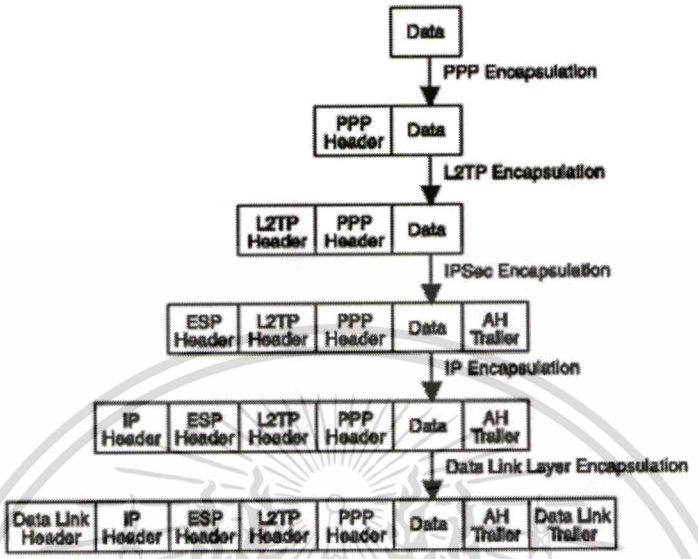
รูปที่ 2.18 แสดงโครงสร้างของ Packet L2TP ที่ไม่ได้ใช้ IPSec Protocolเข้ารหัส (encryption) ในการ ผนึกเฟรมข้อมูลแต่ในการใช้งานส่วนใหญ่แล้วมักจะใช้ โปรโตคอล L2TP ร่วมกับโปรโตคอล IPSec ในการผนึกข้อมูลเพื่อส่งไปยังปลายทางโดยจะมีรูปแบบดังรูปที่ 16



รูปที่ 2.19 Packet L2TP เมื่อใช้ร่วมกับ IPSec Protocol

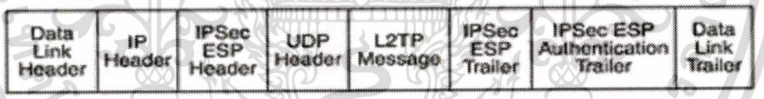
ในรูปแบบที่ 2.19 นี้เป็นรูปแบบที่มักจะใช้ในผลิตภัณฑ์ของ Microsoft เช่น Window 2000 เป็นต้น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 2.20 การผนึกเฟรมข้อมูล (Encapsulation) ของ L2TP

จากรูปที่2.20 เป็นรูปแบบ เฟรม ข้อมูลPayload จะถูกผนึก (Encapsulate) อยู่ในรูปของเฟรม PPP โดยมีการเพิ่ม PPP Header เข้ามาจากนั้นก็จะถูกผนึกให้อยู่ในเฟรม L2TP ก่อนที่จะถูกผนึกโดยโปรโตคอล IPsec หลังจากนั้นก็จะส่งไปในรูปของเฟรม IP ไปยังปลายทาง



รูปที่2.21 Format of the L2TP control message

รูปที่ 2.21 แสดงรูปแบบ Message Control ของโปรโตคอล L2TP โดยที่Control message จะใช้ในการติดต่อเพื่อสร้างการเชื่อมต่อกับปลายทาง Message ที่ใช้ก็มีเช่น Start-Control-Connection-Request ใช้ในการRequest จากฝั่ง ไคลเอ็นต์ (Client) เพื่อสร้างการเชื่อมต่อ, Start-Control-Connection-Reply ใช้ในการResponse จากฝั่ง เซิร์ฟเวอร์ (Server) ไปยัง ไคลเอ็นต์ (Client) ว่าได้รับ Start-Control-Connection จาก ไคลเอ็นต์ (Client) แล้วเป็นต้น โดย Message เหล่านี้มีความใกล้เคียงกับโปรโตคอล PPTPที่ได้นำเสนอไปในตอนต้น

ขั้นตอนการส่ง Message และสถานะของ ไคลเอ็นต์ (Client) หรือ เซิร์ฟเวอร์ (Server) ของโปรโตคอล L2TP นั้นมีคล้ายกับโปรโตคอล PPTP เพียงแต่ Message ที่L2TP ใช้ส่งนั้นอาจมี Message บางชนิดที่ไม่เหมือนกัน เนื่องจากโปรโตคอล L2TP นี้เป็นการรวมข้อดีของโปรโตคอล PPTP และโปรโตคอล L2F จึงทำให้มีบางส่วนคล้ายกับโปรโตคอลทั้งสองบางส่วน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.2.1.4 IPSec (IP Security)

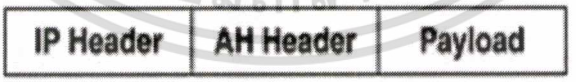
IPSec (IP Security) เป็นโปรโตคอลที่ให้บริการการรักษาความปลอดภัยข้อมูลในระดับเน็ตเวิร์คเลเยอร์ โดยโปรโตคอลนี้ได้ถูกออกแบบสำหรับการเข้ารหัสข้อมูลแพ็กเก็ต (Packet) ของโปรโตคอล IP โปรโตคอลนี้จะรับรองความลับของข้อมูล (Confidentiality), ความคงสภาพของข้อมูล (Integrity) และการพิสูจน์ตัวตนของฝ่ายส่ง (Authentication) มาตรฐานต่างๆที่ IPSec ใช้สำหรับการเข้ารหัสข้อมูลคือ

- การแลกเปลี่ยนคีย์ (Key) โดยใช้ เทคนิค Diffie-Hellman Key Exchange
- การเข้ารหัสแพ็กเก็ตที่แลกเปลี่ยน Secret Key และการพิสูจน์ตัวตนโดยใช้ Public-Key Cryptography
- การเข้ารหัสข้อมูลโดย DES (Data Encryption Stand)
- การใช้ Hash Algorithm เช่น HMAC, MD5, SHA ในการตรวจสอบความคงสภาพของแพ็กเก็ต (Packet)
- ใบรับรองดิจิตอล (Digital Certificate) สำหรับการตรวจสอบเจ้าของกุญแจสาธารณะ (Public Key) [3]

รูปแบบแพ็กเก็ตของ IPSec

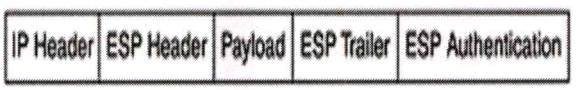
IPSec มีการกำหนดรูปแบบของแพ็กเก็ตโดยมีการเพิ่มข้อมูลเข้ากับ IP datagram เดิมและอาจมีการเข้ารหัสแพ็กเก็ตข้อมูลเดิมด้วย IPSec นั้นสามารถแบ่งได้2โปรโตคอลหลักๆคือ

- *AH (Authentication Header)*: โปรโตคอลนี้จะให้บริการรับรองความคงสภาพของข้อมูล (Integrity) และการพิสูจน์ตัวตนของฝ่ายส่ง (Authenticity) แต่ไม่รับรองความลับของข้อมูล (Confidentiality) โดยมีรูปแบบดังรูปที่ 2.22



รูปที่ 2.22 รูปแบบแพ็กเก็ตโปรโตคอล AH

- *ESP (Encapsulating Security Payload)*: โปรโตคอลนี้จะให้บริการรับรองความคงสภาพของข้อมูล (Integrity), การพิสูจน์ตัวตนของฝ่ายส่ง (Authenticity) และความความลับของข้อมูล (Confidentiality) โดยมีรูปแบบดังรูปที่ 2.23

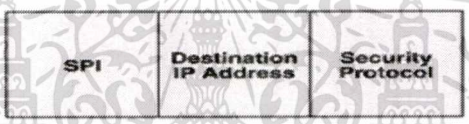


รูปที่ 2.23 รูปแบบแพ็กเก็ตโปรโตคอล ESP

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ทั้งสองโปรโตคอลสามารถใช้งานร่วมกันได้แต่แอพพลิเคชัน(Application) ส่วนใหญ่จะเลือกใช้อย่างใดอย่างหนึ่งเท่านั้น

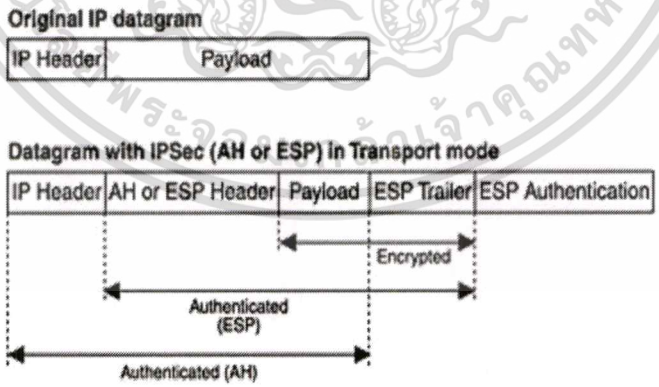
ก่อนส่ง IP datagram ทั้ง AH และ ESP จะสร้างการเชื่อมต่อเสมือนท่อส่งข้อมูลก่อน ซึ่งการเชื่อมต่อนี้เรียกว่า SA (Security Agreement) การเชื่อมต่อแบบนี้เป็นการเชื่อมต่อทางเดียว (Unidirectional) โดยการการเชื่อมต่อแต่ละครั้งนั้นจะต้องมีอย่างน้อย 2 ท่อ (Tunneling) สำหรับส่งข้อมูล คือจาก A ไป B และ B ไป A การเชื่อมต่อ SA จะมีหมายเลขประจำการเชื่อมต่อเรียกว่า SPI (Security Parameter Index) โดยการรับส่งแพ็กเก็ตนั้นก็จะใช้ SPI ร่วมกับหมายเลข IP ของเครื่องปลายในการส่งข้อมูลด้วย ดังนั้น SA จึงถือได้ว่าเป็นการรักษาความปลอดภัยอย่างหนึ่งของ IPSec รูปแบบของ SPI อยู่รวมกับแพ็กเก็ต เป็นดังรูปที่ 2.24



รูปที่ 2.24 รูปแบบแพ็กเก็ต IPSec SA

IPSec นั้นสามารถแบ่งการทำงานได้ 2 Mode คือ

- Transport Mode เป็นการที่เข้ารหัสเฉพาะส่วนที่เป็นข้อมูลเท่านั้นส่วน Header ยังคงไว้เช่นเดิม (IP ใช้ของเดิม)

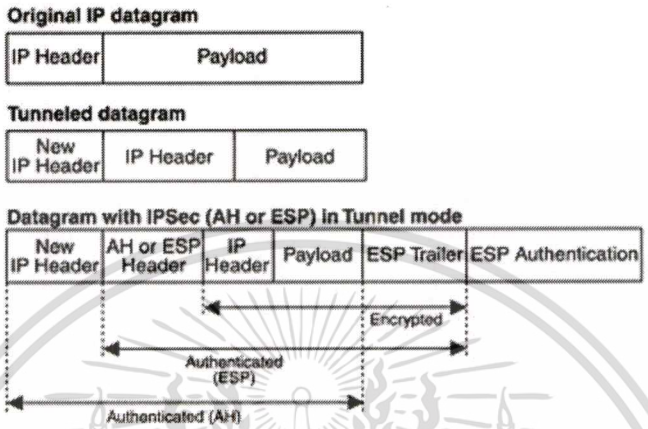


รูปที่ 2.25 รูปแบบแพ็กเก็ต IPSec Transport Mode

รูปที่2.25 แสดงแพ็กเก็ต IPSec ชนิด Transport Mode จะสังเกตได้ว่า Header (IP) จะไม่มีการเปลี่ยนแปลง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- Tunneling Mode นั้นแพ็กเก็ตไอพีเดิมจะถูกเข้ารหัสทั้งหมดและเพิ่มส่วน Header ใหม่ให้กับแพ็กเก็ต



รูปที่ 2.26 รูปแบบแพ็กเก็ต IPSec Tunneling Mode

รูปที่2.26 แสดงแพ็กเก็ต IPSec ชนิด Tunneling Mode จะสังเกตได้ว่า Header (IP) เดิมจะถูกเข้ารหัสและจะมีการเพิ่ม IP Header ตัวใหม่เข้าไป

Transport Mode นั้นสามารถโปรเซสข้อมูลแบบ QoS (Quality of Service) เนื่องจากเข้ารหัสเฉพาะข้อมูลเท่านั้นแต่ผู้บุกรุกจะสามารถตรวจสอบได้ง่ายกว่า Tunneling Mode ส่วน Tunneling Mode นั้น ไคลเอ็นต์ (Client) นั้นไม่จำเป็นต้องติดตั้ง Application เพิ่มเติม โดยการเข้า/ถอดรหัสนั้นให้เป็นหน้าที่ของ อุปกรณ์เครือข่ายแทน

2.2.2. Encryption

2.2.2.1 การเข้ารหัสข้อมูล (Data Encryption)

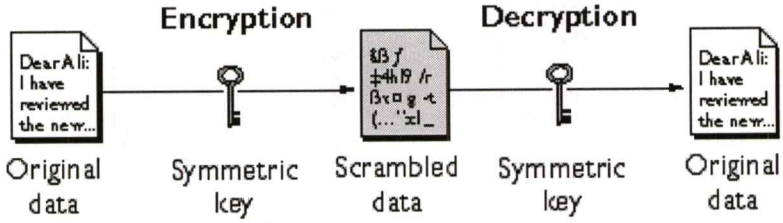
การเข้ารหัสข้อมูล คือการนำข้อมูลปกติที่อยู่ในรูปของตัวอักษรธรรมดา มาผ่านการเข้ารหัสทำให้ได้ข้อมูลออกมาในอีกรูปแบบหนึ่งซึ่งจะไม่มีความหมาย อ่านไม่ออกและแปลกลับไปหาข้อมูลเดิมไม่ได้หากไม่มีรหัสลับที่ถูกต้อง ดังนั้นการเข้ารหัสข้อมูลจึงเป็นการรักษาความปลอดภัยของข้อมูลอย่างหนึ่งซึ่งการเข้ารหัสข้อมูลแบ่งออกได้เป็น2 ประเภทคือ

Symmetric Encryption และ Asymmetric Encryption **[1]**

2.2.2.1.1 Symmetric Encryption

เป็นการเข้าและถอดรหัสข้อมูลโดยใช้รหัสลับตัวเดียวกันโดยคีย์ (Key) ที่ใช้จะมีความยาวคงที่ การไหลของข้อมูลเป็นเหมือนดังรูปที่ 2.27

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 2.27Symmetric Encryption

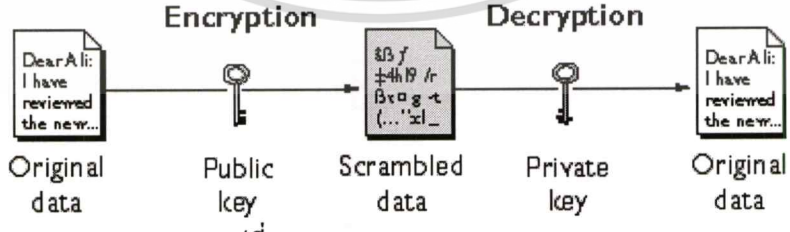
การเข้ารหัสข้อมูลแบบ Symmetric Encryption นี้มีหลายชนิดแต่ที่ยกมาอธิบายนี้ก็มี DES (Data Encryption Standard) และ IDEA (International Data Encryption Algorithm)

- ***Data Encryption Standard (DES):*** เป็นการเข้ารหัสข้อมูลในชั้นที่มีความลับน้อย ซึ่ง DES นั้นถูกพัฒนาโดย IBM และเป็นอัลกอริทึมที่เคยนิยมกันอย่างแพร่หลาย DES นั้นประกอบด้วย 2 ส่วนคือ อัลกอริทึมและคีย์ (Key) โดย คีย์ จะมีขนาด 56 บิต และจะทำการเข้ารหัสข้อมูลทีละ 64 บิต โดยมีขั้นตอน 18 ขั้นตอน แต่ขั้นตอนแรกกับขั้นตอนสุดท้ายนั้นเป็นการสลับบิต (Permutation) เท่านั้น

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

2.2.2.1.2 Asymmetric Encryption

เป็นการเข้าและถอดรหัสข้อมูลโดยใช้รหัสลับโดยใช้ คีย์คนละชุดกันโดย ชุดหนึ่งจะใช้ในการเข้ารหัสในขณะที่อีกตัวจะใช้ในการถอดรหัส ซึ่งคีย์ที่ใช้เรียกว่า Private Key และ Public Key โดยมีลักษณะดังรูปที่ 2.28 เทคนิคที่ใช้การเข้ารหัสแบบนี้ตัวอย่างที่มีก็เช่น RSA (ย่อมาจากชื่อของผู้ที่คิดค้นคือ Rivest, Shamir, Adleman)



รูปที่ 2.28Asymmetric Encryption

- ***RSA***: เป็นการเข้ารหัสแบบ Asymmetric ชนิดหนึ่ง โดยจะประกอบด้วยรหัส 2 ตัวคือ Public Key และ Private Key ซึ่ง Public Key นี้สามารถเปิดเผยได้แต่ Private Key นี้ไม่สามารถเปิดเผยได้รู้เฉพาะผู้ส่งเท่านั้น นอกจากนี้จะต้องเป็นคู่ของมันเท่านั้นจึงจะถอดรหัสได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.2.2.2 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

2.3ระบบปฏิบัติการ FreeBSD (FreeBSD Operating System)

FreeBSD (Free Berkeley Software Distribution) เป็นระบบปฏิบัติการขั้นสูงที่สามารถทำงานได้บนสถาปัตยกรรมหลายๆแบบเช่น x86 (Intel), DEC Alpha, Sun Sparc และ PPC(PowerPC) FreeBSD มีต้นกำเนิดมาจาก BSD ของมหาวิทยาลัย California, Berkeley FreeBSD มีคุณสมบัติที่โดดเด่นในด้านการจัดการเครือข่ายขั้นสูง มีความปลอดภัยอีกทั้งสามารถเข้ากันได้กับเครื่องคอมพิวเตอร์หลายสถาปัตยกรรม FreeBSD นั้นสามารถนำมาสร้างเป็น เซิร์ฟเวอร์ (Server) แบบ Intranet และ Internet ได้พร้อมทั้งยังสามารถรองรับการทำงานกับเครือข่ายที่มีการโหลดข้อมูลมากๆ และสามารถใช้หน่วยความจำได้อย่างมีประสิทธิภาพถึงแม้จะมี Process ของผู้ใช้เข้ามามากก็ตาม

คุณสมบัติที่มีในFreeBSDนั้นส่วนมากจะมีในระบบปฏิบัติการชั้นสูงที่ต้องเสียค่าใช้จ่ายแต่สำหรับ FreeBSDนั้นผู้ต้องการใช้งานนั้น สามารถ Download มาใช้งานได้โดยไม่เสียค่าใช้จ่ายใดๆทั้งสิ้น

2.4. VPN บนระบบปฏิบัติการ FreeBSD

การติดตั้ง VPN บนระบบปฏิบัติการ FreeBSD นั้นจะทำได้โดยการติดตั้ง Application โดย Application มีหลายชนิดดังนั้น โดยในโครงงานพัฒนาระบบนี้ได้ใช้ OpenVPN เป็นหลักในการพัฒนาโปรแกรมการจัดการเครือข่ายส่วนตัวเสมือน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.5. OpenVPN

OpenVPN เป็น Application ที่สามารถนำใช้โดยไม่เสียค่าใช้จ่ายใดๆทั้งสิ้น OpenVPN มีหลาย Version สามารถทำงานบนระบบปฏิบัติการได้หลายชนิดเช่น Linux, FreeBSD และWindows เป็นต้น

หลักการทำงานของ OpenVPN

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

ขั้นตอนการสร้าง Tunneling และส่งข้อมูล

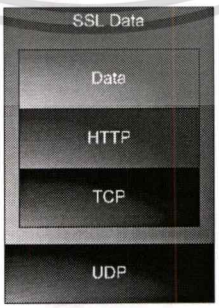
-Application จะทำการส่งข้อมูลไปที่ Private Network โดยใช้ IP ต้นทางเป็น Private IP และปลายทางเป็น IP ของ Host ที่อยู่ใน Private Network

- เมื่อเริ่มRun Application นั้น OpenVPN จะทำการสร้างกุญแจใช้สำหรับการเข้ารหัสข้อมูลมา2อันโดยอันแรกอยู่ที่ ไคลเอ็นต์ (Client) ส่วนอันที่ 2 อยู่ที่ VPN เซิร์ฟเวอร์ (Server) กุญแจที่ได้นั้นมาจาก Function ของ OpenSSL Library

- ในการส่งข้อมูลจาก ไคลเอ็นต์ (Client) ไปยัง เซิร์ฟเวอร์ (Server) นั้นจะทำการเข้ารหัสข้อมูลโดยเข้ารหัสแบบ RSA

- เมื่อข้อมูลถูกเข้ารหัสเสร็จก็จะถูกส่งโดยใช้IP เป็น IP จริงที่อยู่ที่ ไคลเอ็นต์ (Client) และเซิร์ฟเวอร์ (Server) ผ่านAdapter ที่ใช้ในการสร้าง Tunneling โดย Adapter นั้นมี 2แบบคือ TUN และ TAP

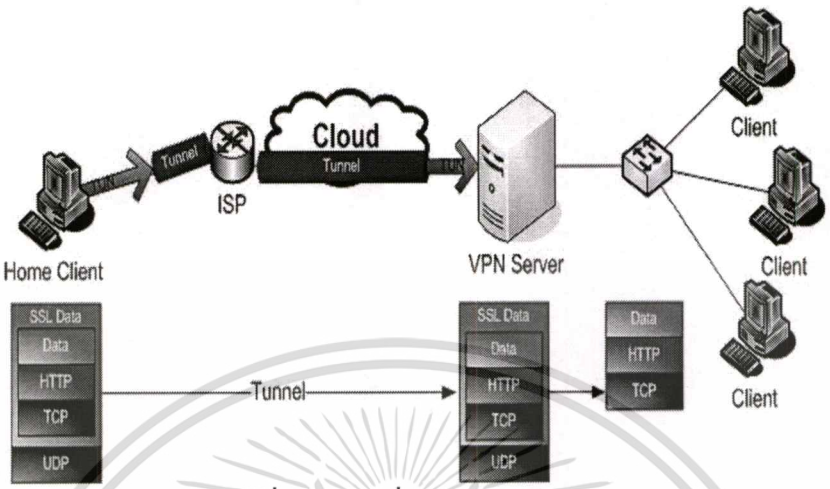
TUN เป็น Virtual network adapter ที่ทำการเขียนข้อมูลลงไปใน TCP/UDP ดังรูปที่ 2.29



รูปที่ 2.29 โครงสร้าง Packet ของ TUN

สามารถแสดงรูปแบบการส่งและรับข้อมูลได้ดังรูปที่ 2.29

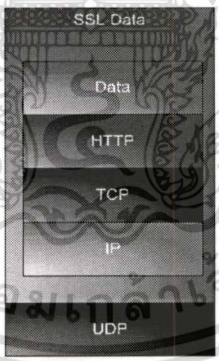
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 2.30 การเชื่อมต่อโดยใช้ TUN

โดยจากรูปที่ 2.30 ข้อมูลจะถูกส่งจาก ไคลเอ็นต์ (Client) ไปยัง เซิร์ฟเวอร์ (Server) โดยใช้ Tunneling ที่สร้างโดยAdapter ชนิด TUN

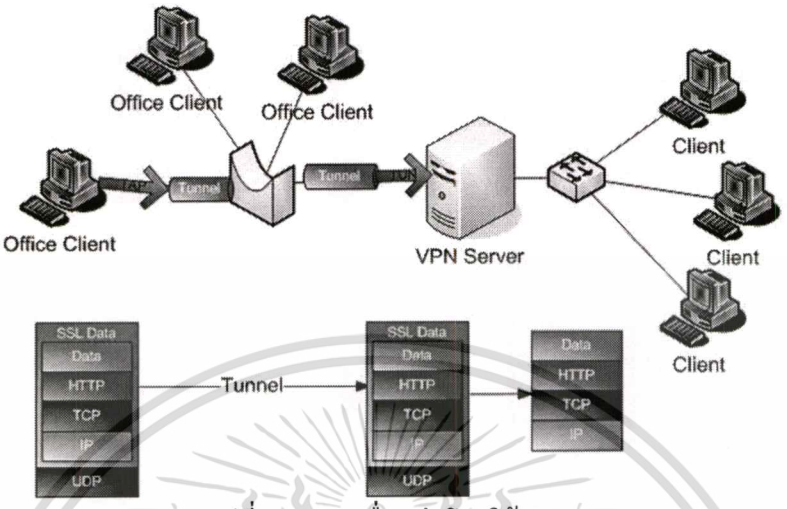
TAP เป็น Virtual network adapter อีกชนิดหนึ่งโดยจะมีลักษณะเหมือน Ethernet Network โดยจะทำงานกับ Bridge (Layer2) จะเขียนข้อมูลบน Frame ของ Ethernet ดังรูปที่ 2.30



รูปที่ 2.31 การเชื่อมต่อโดยใช้ TAP

สามารถแสดงรูปแบบการส่งและรับข้อมูลได้ดังรูปที่ 2.31

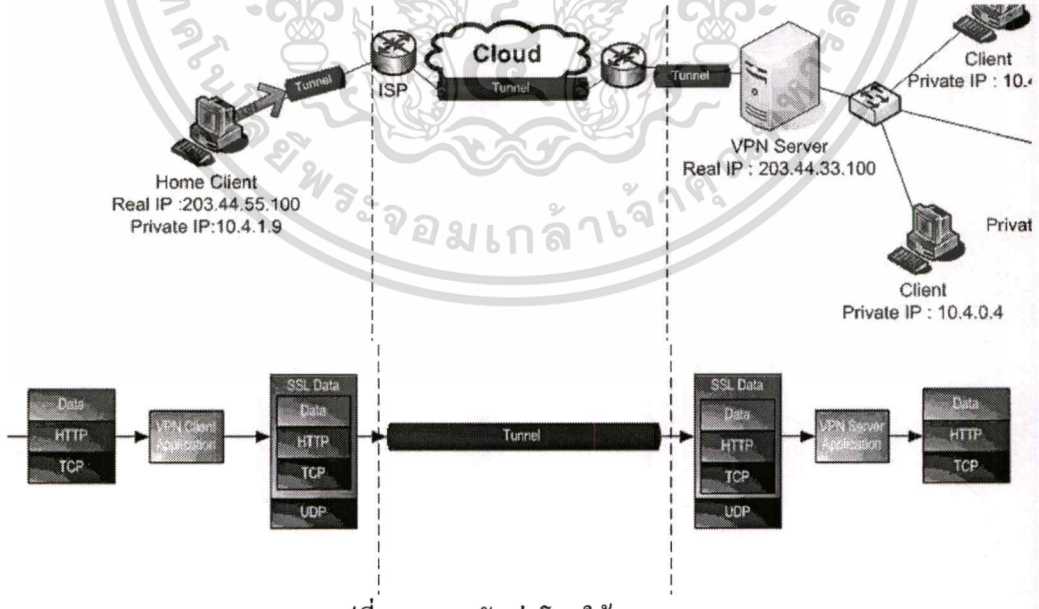
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 2.32 การเชื่อมต่อโดยใช้ TUN

โดยจากรูปที่ 2.32 ข้อมูลจะถูกส่งจาก ไคลเอ็นต์ (Client) ไปยัง เซิร์ฟเวอร์ (Server) โดยใช้ Tunneling ที่สร้างโดยAdapter ชนิด TAP

การส่งข้อมูลโดยใช้ OpenVPN นั้นสามารถใช้ Adapterได้ทั้ง 2 แบบ ส่วนการส่งข้อมูลโดยใช้ OpenVPN นั้นสามารถแสดงได้ดังรูปที่ 2.33



รูปที่ 2.33 การรับส่งโดยใช้ OpenVPN

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.6 สรุป

ระบบเครือข่ายส่วนตัวเสมือน(Virtual Private Network) สามารถแบ่งโดยใช้หลักเกณฑ์ได้ 2 แบบคือ 1.แบ่งตามรูปแบบการใช้งาน 2.แบ่งตามลักษณะของผลิตภัณฑ์ที่ใช้งาน โดยการแบ่งตามรูปแบบที่ใช้งานนั้นสามารถแบ่งได้ 3 ชนิดคือ Remote Access, Intranet Base และ Extranet Base ส่วนการแบ่งตามลักษณะของผลิตภัณฑ์ที่ใช้งานแบ่งได้ 3 ชนิดเช่นกัน คือ Firewall Based VPN, Hardware Based VPN และ Software based VPN โดยที่โปรโตคอลที่ใช้ในเครือข่ายส่วนตัวเสมือนนั้นหลักๆมี4 โปรโตคอลคือ PPTP (Point-to-Point Tunneling Protocol), L2F (Layer 2 Forwarding), L2TP (Layer 2 Tunneling Protocol) และ IPSec (IP Security)

การติดตั้ง VPN บนระบบปฏิบัติการ FreeBSD นั้นจะทำได้โดยการติดตั้ง Application โดยในโครงงานพัฒนาระบบนี้ได้ใช้ OpenVPN เป็นหลักในการพัฒนาโปรแกรมการจัดการเครือข่ายส่วนตัวเสมือนโดยตัวโครงงานจะเป็นการจัดการ Application นี้ผ่านทางเว็บบราวเซอร์ ไม่ว่าจะเป็นการเพิ่ม, ลด ดูสถานการณ์เชื่อมต่อรวมไปถึงการ Active Service ทั้งหมดหรือทีละหนึ่ง User

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 3

การวิเคราะห์และออกแบบโครงงานพัฒนาระบบ

ในบทนี้จะกล่าวถึงรูปแบบการใช้งานเครือข่ายส่วนตัวเสมือนโดยใช้แอพลิชั่นโอเพ่นวีพีเอ็น(OpenVPN) บนระบบปฏิบัติการ FreeBSD ในระบบเดิม โดยจะกล่าวรวมไปถึงปัญหาที่เกิดขึ้นจากการใช้งานในระบบเดิมด้วย อีกทั้งการนำเสนอการวิเคราะห์การออกแบบโครงงานว่ามีรูปแบบอย่างไรตลอดจนความสามารถของโครงงานเพื่อนำมาใช้ในการจัดการเครือข่ายส่วนตัวเสมือนบนระบบปฏิบัติการFreeBSD

3. 1โครงสร้างการใช้งานของโอเพ่นวีพีเอ็น (OpenVPN) ของระบบเดิม

รูปแบบการจัดการใช้งานโอเพ่นวีพีเอ็น (OpenVPN) นั้นในปัจจุบันสามารถทำได้ 2 วิธี วิธีแรกคือการเข้าไปแก้ไขไฟล์คอนฟิก (File Configure) วิธีที่สองก็คือการใช้ Command Line ในการแก้ไขคอนฟิก (Configure) หรือจัดการระบบเครือข่ายส่วนตัวเสมือน (Virtual Private Network: VPN)

3.1.1 การจัดการระบบเครือข่ายส่วนตัวเสมือนโดยใช้วิธีแก้ไขไฟล์คอนฟิก (Configure) นั้นมักเป็นที่นิยมเนื่องจากง่ายและสามารถตรวจสอบได้ก่อนที่จะรันไฟล์คอนฟิก (Run File Configure) ดังนั้นในกรณีที่ผู้ดูแลยังไม่มีคุ้นเคยกับโอเพ่นวีพีเอ็น (OpenVPN) จึงมักใช้วิธีการนี้ในการจัดการระบบเครือข่าย ซึ่งการสร้างติดตั้งระบบเครือข่ายส่วนตัวเสมือน (VPN) ที่เซิร์ฟเวอร์ (Server) นั้นจะทำการสร้างไฟล์ (File) /etc/openvpn/server.conf โดย 1 ไฟล์ใช้แทน 1 อินเทอร์เฟต (Interface) ถ้าเป็นโอเพ่นวีพีเอ็นเวอร์ชั่นที่ต่ำกว่า2.00ลงมาแต่ถ้าเป็นเวอร์ชั่นตั้งแต่ 2.00 ขึ้นไปก็จะสามารถใช้อินเทอร์เฟตเดียวกันได้โดยปัจจุบันโอเพ่นวีพีเอ็น (OpenVPN) นั้นมีถึงเวอร์ชั่นที่ 2.00 ส่วนไฟล์คอนฟิกนั้นสามารถแสดงส่วนหนึ่งได้ดังตัวอย่างดังนี้

```
# Which local IP address should OpenVPN
# listen on? (optional)
;local a.b.c.d

# Which TCP/UDP port should OpenVPN listen on?
# If you want to run multiple OpenVPN instances
# on the same machine, use a different port
# number for each one.  You will need to
# open up this port on your firewall.
port 1194

# TCP or UDP server?
;proto tcp
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

proto udp

ฯลฯ

หลังจากได้คอนฟิก (Configure) ค่าในไฟล์ Server.conf แล้วจึงเซฟไฟล์ (Save File) ก่อนจะทำการรีสตาร์ทเครื่องเซิร์ฟเวอร์ (Server) อีกครั้งเพื่อให้ระบบรันค่าคอนฟิกในไฟล์ขึ้นมา

ส่วนที่ ไคลเอนต์ (Client) ก็จะสร้างไฟล์ (File) Client.ovpn (กรณีระบบปฏิบัติการวินโดวส์ Window) ตัวอย่างดังข้างล่างนี้เป็นส่วนหนึ่งของไฟล์ Client.ovpn

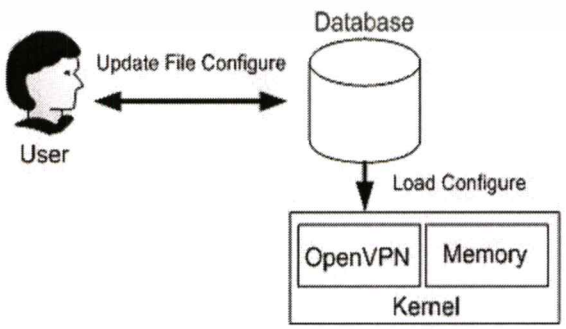
```
# Specify that we are a client and that we
# will be pulling certain config file directives
# from the server.
client

# Use the same setting as you are using on
# the server.
# On most systems, the VPN will not function
# unless you partially or fully disable
# the firewall for the TUN/TAP interface.
;dev tap
dev tun
# Windows needs the TAP-Win32 adapter name
# from the Network Connections panel
# if you have more than one.  On XP SP2,
# you may need to disable the firewall
# for the TAP adapter.
;dev-node MyTap
# Are we connecting to a TCP or
# UDP server?  Use the same setting as
# on the server.
;proto tcp
proto udp
```

ฯลฯ

บรรทัดที่มีเครื่องหมาย # นั้นเป็นคำอธิบายหรือแนะนำ

โดยรูปที่ 3.1 จะแสดงการทำงานของการจัดการเครือข่ายโดยใช้วิธีการแก้ไขไฟล์คอนฟิก (File Configure)



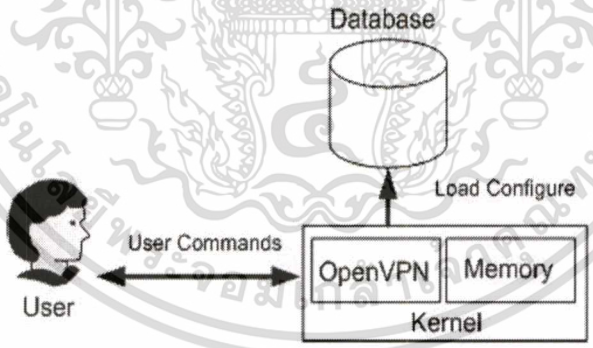
รูปที่ 3.1 แสดงการจัดการเครือข่ายโดยการแก้ไขไฟล์คอนฟิก

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

จากรูปที่ 3.1 ผู้ใช้งานหรือผู้ดูแล (Administrator) เครือข่ายส่วนตัวเสมือนจะทำการแก้ไขเปลี่ยนแปลงค่าในไฟล์คอนฟิก (File Configure) เมื่อแก้ไขเสร็จก็จะทำการเซฟไฟล์ (save file) จากนั้นก็จะทำการรีสตาร์ทเครื่องเซิร์ฟเวอร์อีกครั้งเพื่อให้ระบบทำการ Load Configure จากไฟล์ที่เซตไว้

3.1.2 การจัดการระบบเครือข่ายส่วนตัวเสมือนโดยใช้ Command Line วิธีการนี้จะเป็นการส่ง Command Line เพื่อจัดการระบบเครือข่ายส่วนตัวเสมือนโดยตรงซึ่งค่าของพารามิเตอร์ที่ใช้จะมีระบุไว้ที่http://openvpn.net/man.html หรือสามารถใช้คำสั่ง man ตามด้วย openvpn (man openvpn) ก็จะมีรายละเอียดของรูปแบบ Command Line ให้ดู การใช้วิธีนี้นั้นมักใช้ในกรณีที่จะแก้ไขหรือเพิ่มออปชั่น (Option) เป็นส่วนใหญ่ ส่วนกรณีติดตั้งระบบเครือข่ายนั้นมักใช้วิธีการแก้ไขไฟล์คอนฟิก (File Configure) ในการติดตั้ง

รูปที่3.2 จะแสดงการทำงานของการจัดการเครือข่ายโดยใช้วิธีการส่ง Command Line เพื่อแก้ไขเปลี่ยนแปลงค่าพารามิเตอร์ของระบบเครือข่ายส่วนตัวเสมือน



รูปที่ 3.2 แสดงการจัดการเครือข่ายโดยการส่ง Command Line

จากรูปที่ 3.2 เมื่อ ผู้ใช้งานหรือผู้ดูแล (Administrator) เครือข่ายส่วนตัวเสมือนต้องการแก้ไขเปลี่ยนแปลงค่าพารามิเตอร์ในระบบเครือข่ายก็จะทำการส่ง Command Line โดยผ่านโปรแกรมโอเพ่นวีพีเอ็น (OpenVPN) ใน Kernel จากนั้นระบบก็จะทำการอัพเดท (Update) ไฟล์คอนฟิก (File Configure) ในหน่วยความจำสำรอง

ส่วนรูปแบบของการใช้คำสั่งของโอเพ่นวีพีเอ็น (OpenVPN) มีตัวอย่างดังนี้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

openvpn [**--genkey**] [**--secret** *file*]

openvpn [**--config** *file*]

จากตัวอย่างที่แสดงนั้นคือรูปแบบของคำสั่ง Command Line ที่ใช้ในการส่งเพื่อปรับเปลี่ยนค่าหรือแสดงค่าที่ต้องการ โดยที่

openvpn คือ คำสั่งหลักของซอฟต์แวร์โอเพ่นวีพีเอ็น(OpenVPN)

genkey คือ การเจนเนอร์เรท (Generate) ค่าคีย์ (Key)ซึ่งใช้อยู่ใน โมด (Mode) Pre-Shared-Static-Key พารามิเตอร์นี้ใช้คู่กับพารามิเตอร์ Secret

secret คือ เป็นการนำค่าคีย์ (Key) ที่เจนเนอร์เรท(Generate)
ขึ้นมาไปเก็บที่ ไฟล์ (file)

Config คือ การนำคำสั่งที่เขียนไว้เป็นชุดเก็บไว้ในไฟล์ (file) ขึ้นมารัน (run) คล้ายกับ Batch File ในระบบปฏิบัติการ DOSจากตัวอย่างที่นำมานั้นเป็นเพียงส่วนหนึ่งของพารามิเตอร์ที่โอเพ่นวีพีเอ็น (OpenVPN) มีให้ใช้ในการจัดการระบบ

สามารถแสดงรูปแบบทั่วไปของ Command Line ของโอเพ่นวีพีเอ็นได้ดังนี้

openvpn [--option1] [--option2] [--option3]

ส่วนค่าที่อยู่ในวงเล็บ [ ] นั้นเป็นค่าออปชั่น (Option) ซึ่งค่านี้จะต้องมีเครื่องหมาย – นำก่อนที่จะใส่ค่าลงไป เช่น [-- genkey] [--secret file] เป็นต้น

3.1.3 ข้อเสียที่พบในการใช้วิธีการจัดการระบบเครือข่ายในปัจจุบันคือ

- ในการจัดการระบบเครือข่ายนั้นเป็นแบบปัจจุบันนั้นค่อนข้างยากดังนั้นผู้ใช้หรือผู้ดูแลจำเป็นต้องมีความคุ้นเคยกับโอเพ่นวีเอ็น (OpenVPN) พอสมควรจึงสามารถจัดการระบบได้ไม่ว่าจะเป็นการแก้ไขไฟล์คอนฟิก(File Configure) หรือการใช้ Command Line
- การจัดการโดยใช้ Command Line นั้นไม่ค่อยสะดวกในการทำงานเนื่องจากจะต้องเข้าใจในค่าพารามิเตอร์ที่ใช้ในการส่ง

3.2 โครงงานพัฒนาการใช้โอเพ่นวีพีเอ็น (OpenVPN) โดยผ่านเว็บเบส

3.2.1 วัตถุประสงค์

- เพื่อให้เข้าใจการทำงานของระบบเครือข่ายส่วนตัวเสมือน
- เพื่อเรียนรู้เข้าการออกแบบวิเคราะห์ตลอดจนการพัฒนาโปรแกรมเพื่อจัดการ Application ผ่านทางเว็บ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- เพื่อเรียนรู้และศึกษาการโปรแกรมด้วยภาษา PHP, Shell Script เพื่อใช้ในการพัฒนาโครงงานการจัดการระบบผ่านทางเว็บ

3.2.2 ความต้องการของระบบ

โครงงานหรือระบบที่จะพัฒนาขึ้นนั้นจะเป็นโปรแกรมที่ใช้ เว็บบราวเซอร์(Web browser) ในการที่จะเข้าไป Setup ระบบเครือข่ายส่วนตัวเสมือน (VPN) ได้โดยไม่จำเป็นต้องอยู่ที่เครื่องเซิร์ฟเวอร์ ซึ่งการ Setup นั้นจะประกอบด้วยฟังก์ชั่นเพิ่มหรือลด User, ตรวจสอบ log file,ดูค่า Configure, แก้ไขไฟล์ Configure ตลอดจนการ Monitor ระบบเพื่อดูสถานะภาพการเชื่อมต่อเป็นต้น โดยผู้ที่จะเข้าไปแก้ไขหรือเพิ่ม User ได้นั้นจะต้องเป็น Administrator หรือผู้มีสิทธิ์ในการเข้าใช้ได้เท่านั้นดังนั้นก่อนที่จะทำการเข้าใช้ระบบจะมีการตรวจสอบสิทธิ์ก่อนที่จะเข้าไปใช้งานเพื่อป้องกันไม่ให้บุคคลไม่มีสิทธิ์เข้ามา Setup ระบบได้ โครงงานนี้เป็นการช่วยให้การจัดการระบบเครือข่ายนั้นทำได้สะดวกมากขึ้นแต่ก็อาจจะไม่สามารถจะทำการ Setup ได้ทุกอย่างที่ Command Line นั้นทำได้อยู่ในรูปแบบเว็บบราวเซอร์(Web Browser)หรือรูปแบบ GUI(Graphic User Interface) ทั้งหมด ดังนั้นเพื่อที่จะให้ Administrator นั้นยังสามารถทำการ Setup ค่าในส่วนที่ระบบไม่ได้ทำให้เป็น GUI(Graphic User Interface) นั้นระบบได้เพิ่มส่วนที่เป็นการใส่ค่า Command Line ไปด้วยเพื่อเพิ่มความสะดวกในการ Setup ระบบโดยไม่จำเป็นต้องเปิดโปรแกรมที่ใช้รีโมทเข้ามายังเซิร์ฟเวอร์เพื่อใช้ส่ง Command Line อีกทั้งระบบได้เพิ่มในส่วนความช่วยเหลือ(Help) ในกรณีต้องการทราบความหมายหรือโครงสร้าง(Syntax) ของ Command Line ด้วย

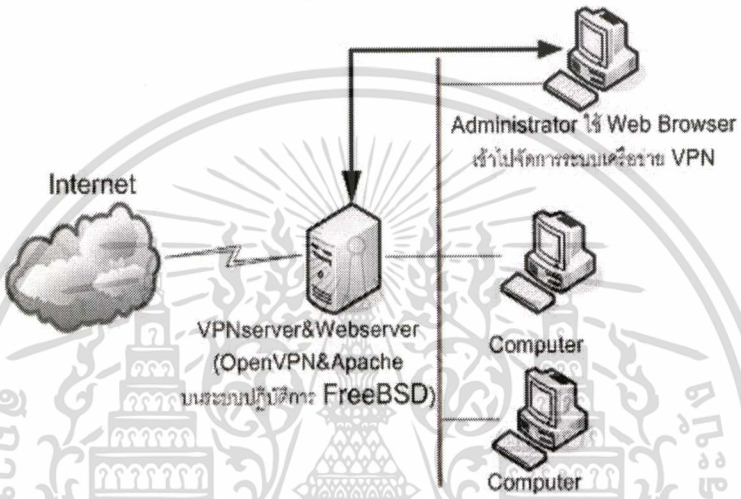
การทำงานของตัวโครงงานนั้นจะต้องทำงานอยู่บนระบบปฏิบัติงานฟรีบีเอสดี(FreeBSD) ซึ่งรูปแบบของตัวโครงงานนี้จะเป็นเว็บเบส (Web Base) โดยตัวโครงงานนี้จะทำงานอยู่บนเว็บเซิร์ฟเวอร์ที่ทำหน้าทีเป็น VPN เซิร์ฟเวอร์ด้วยในตัวเดียวกันซึ่งทำให้การจัดการระบบนั้นไม่จำเป็นต้องอยู่ที่เดียวกับตัวเซิร์ฟเวอร์เพื่อจัดการระบบอีกทั้งโปรแกรมจะต้องมีความสามารถในการเพิ่มจำนวนรายชื่อ Administrator และพร้อมกับสามารถเปลี่ยนแปลงแก้ไข รหัส (Password) ของแต่ละคนได้ซึ่งตรงจุดนี้จะยอมให้ Administrator แต่ละคนสามารถลดหรือเพิ่มรายชื่อ Administratorของคนอื่นได้ เพื่อเข้าไปทำการจัดการระบบได้ โดยในโครงงานนี้ถือว่า Administrator เป็น level สูงสุดในการจัดการระบบ

3.2.3 การวิเคราะห์และออกแบบโครงร่างของโครงงานที่พัฒนา

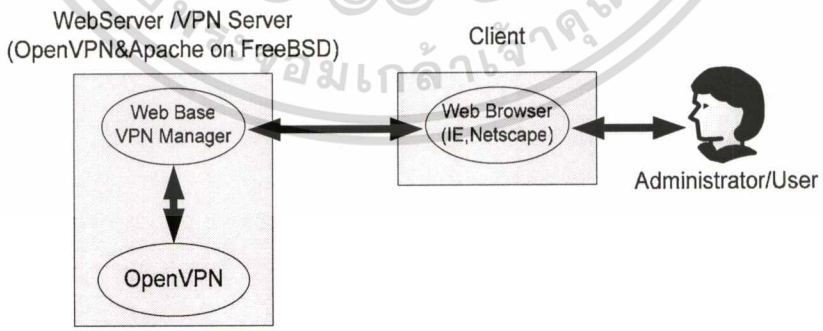
ตัวโครงงานนั้นเป็นการจัดการเครือข่ายส่วนตัวเสมือน (Virtual Private Network: VPN) โดยผ่านทางเว็บซึ่งจะพยายามจัดการให้อยู่ในรูปแบบ GUI (Graphic User Interface) มากที่สุดเพื่อให้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ทำงานได้ง่ายซึ่งอาจจะมีบางส่วนอนุญาตให้สามารถป้อนคำสั่ง Command Line ได้ แต่ยังคงไว้ซึ่งการใช้งานที่ง่าย ตัวระบบจัดการของโครงงานนั้นจะทำงานอยู่บนระบบปฏิบัติการฟรีบีเอสดี (FreeBSD) โดยจะทำงานผ่านซีจีไอ (Common Gateway Interface: CGI) ซึ่งพัฒนาด้วยภาษา Perl (Practical Extraction and Report Language) หรืออาจจะเป็นภาษาPHP(Personal Home Page)ก็ได้ ส่วนตัวเว็บเซิร์ฟเวอร์ของโครงงานจะใช้ Apache เป็นเว็บเซิร์ฟเวอร์ (Web server)



รูปที่3.3 จะแสดงภาพรูปแบบการเชื่อมต่อโดยรวมของระบบว่ามีการเชื่อมต่ออย่างไร โดยรูปที่3.3 จะแสดงรูปแบบโดยรวมของระบบของโครงงานซึ่งจะประกอบด้วยเซิร์ฟเวอร์ที่เป็นเว็บและวีพีเอ็น (VPN) เซิร์ฟเวอร์โดยที่Administratorสามารถเข้ามาจัดการเครือข่ายส่วนตัวเสมือนได้โดยใช้เว็บราวเซอร์



รูปที่3.4 แสดงองค์ประกอบการทำงานของระบบ

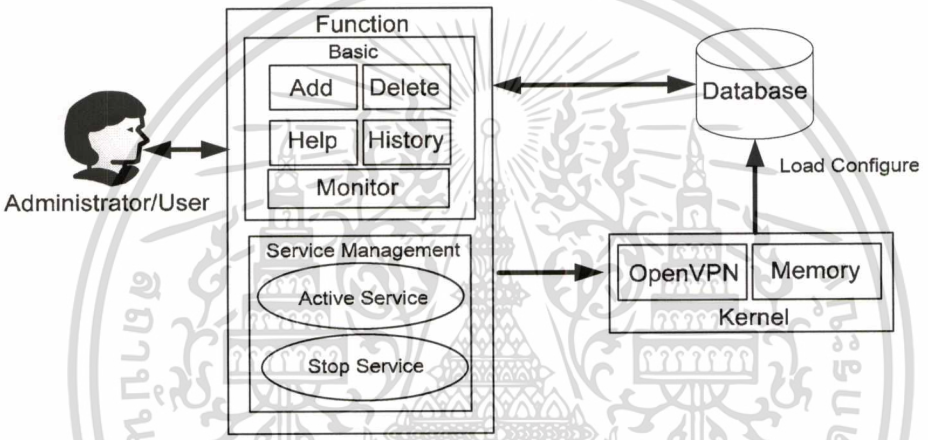
จากรูปที่ 3.4 จะแสดงองค์ประกอบการทำงานของระบบโดยตัวโครงงานนั้นจะอยู่บนฝั่ง Server ที่ทำงานเป็น Web Base และ VPN เซิร์ฟเวอร์ด้วย โดยAdministrator/User จะสามารถจัดการ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เครือข่ายส่วนตัวเสมือน (VPN) ได้จากฝั่ง Client ด้วยการจัดการผ่านเว็บบราวเซอร์เพื่อเรียกใช้ VPN Manager ที่อยู่ฝั่งเซิร์ฟเวอร์ได้

ผลจากการวิเคราะห์และออกแบบ

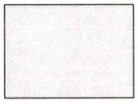
ตัวโครงงานนั้นจะประกอบด้วยฟังค์ชั่นที่ใช้ในการจัดการระบบเครือข่าย 2 แบบคือ Basic Function และ Management Function แสดงดังรูปที่ 3.5



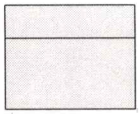
รูปที่3.5 แสดงภาพรวม Function การทำงานของระบบ

โดย Basic Function นั้นจะประกอบด้วย ฟังค์ชั่น(Function) ที่ทำงานในส่วนของการจัดการเกี่ยวกับ เพิ่ม (Add) , ลบ(Delete) ผู้ใช้งาน (User) ,การเรียกดูข้อมูล (History) ประวัติการใช้งานในระบบ และฟังค์ชั่นการขอข้อมูลขอความช่วยเหลือ (Help) ในการจัดการระบบด้วย Command Line ส่วน Management Function นั้นจะประกอบด้วย function ที่ใช้ในการจัดการเครือข่ายส่วนที่เชื่อมต่อ เรียกว่า Active Service และ Stop Service

3.2.3.1 ผังการไหลของข้อมูลโปรแกรมการจัดการระบบเครือข่ายส่วนตัวเสมือนบนระบบปฏิบัติการ FreeBSD

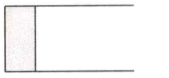


สัญลักษณ์แสดงเอ็นทิตี (Entity)

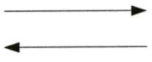


สัญลักษณ์แสดงกระบวนการ (Process)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



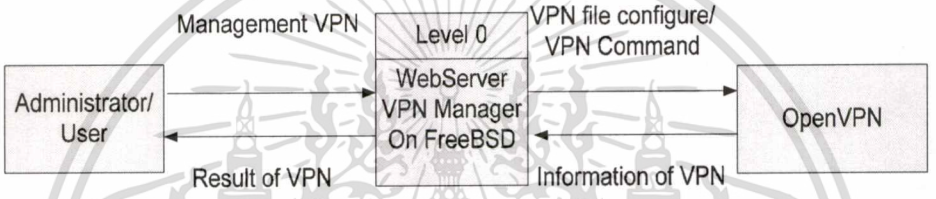
สัญลักษณ์แสดงฐานข้อมูลหรือแฟ้มข้อมูล



สัญลักษณ์แสดงทิศทางการไหลของข้อมูล

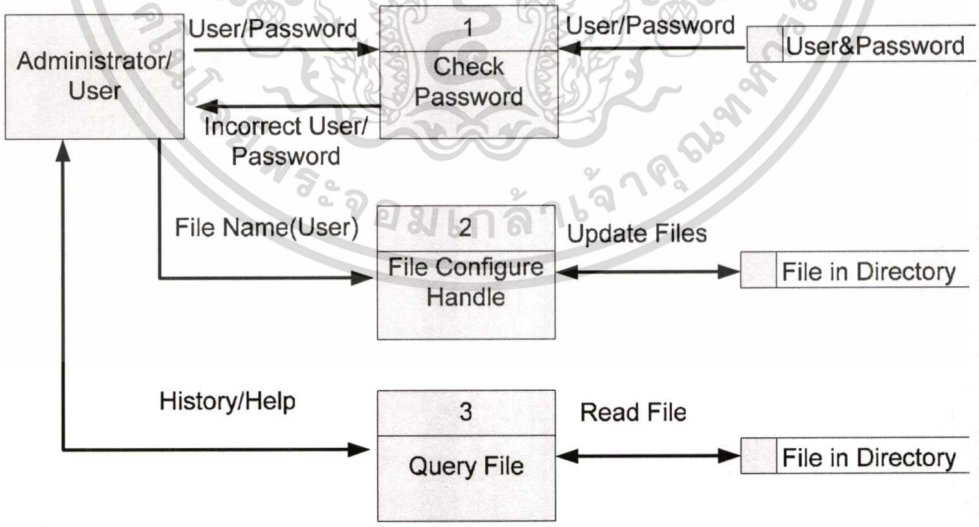
รูปที่ 3.6 แสดงสัญลักษณ์ของการไหลของข้อมูล

สามารถแสดงการไหลของข้อมูลในระบบที่เกิดขึ้นได้ดังนี้



รูปที่ 3.7แสดง Context Diagram ของระบบจัดการVPN บน FreeBSD

รูปที่3.7แสดงการจัดการระบบโดยที่ Administrator/User จะเข้าใช้ตัวโปรแกรมที่พัฒนาขึ้นแทนที่จะเข้าไปจัดการตัว OpenVPN โดยตรง

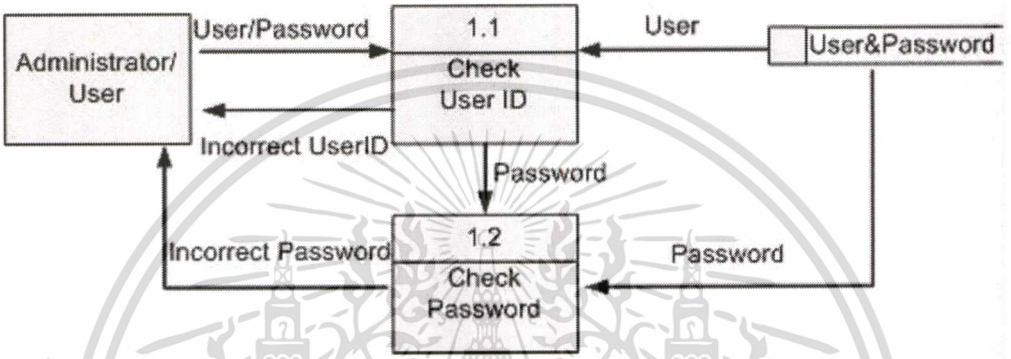


รูปที่ 3.8แสดงการไหลของข้อมูลของระบบจัดการVPN บน FreeBSD ระดับ level 0 (DFD 0)

จากรูปที่ 3.8แสดงการไหลขอข้อมูลในระดับที่ 0 โดยระบบได้แบ่งการไหลข้อมูลออกเป็น3 ส่วน คือ Check Password ใช้ในการตรวจสอบ User/Password ส่วนที่สอง File Configure Handle ใช้ใน

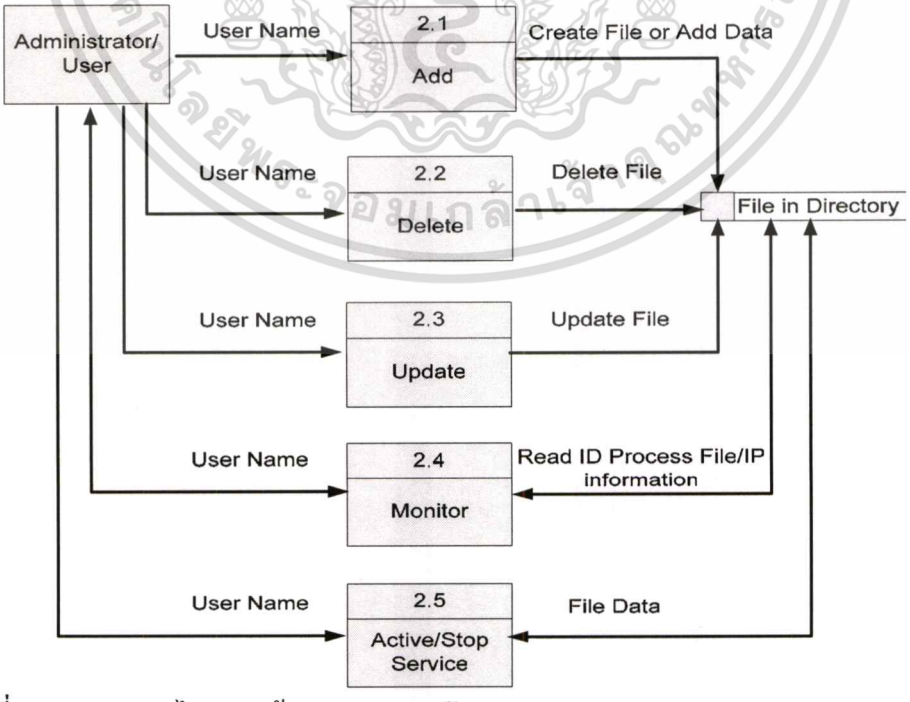
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

การจัดการไฟล์คอนฟิกเมื่อมีการเปลี่ยนแปลง, เพิ่มและลด (ในกรณีของAdministratorเท่านั้น) รวมไปถึงการตรวจสอบสถานะไฟล์ เพื่อใช้ในการตรวจสอบสถานการณ์เชื่อมต่อ สุดท้าย Query File ใช้ในการดึงข้อมูลจากไฟล์เพื่อใช้ในการตรวจสอบคอนฟิก, การดึงข้อมูลจาก Log File เพื่อใช้ในการดูประวัติ (Log File) รวมไปถึงการดึงไฟล์ขอความช่วยเหลือ (Help)



รูปที่ 3.9 แสดงการไหลของข้อมูลของระบบจัดการVPN บน FreeBSD (DFD level 1 Process 1)

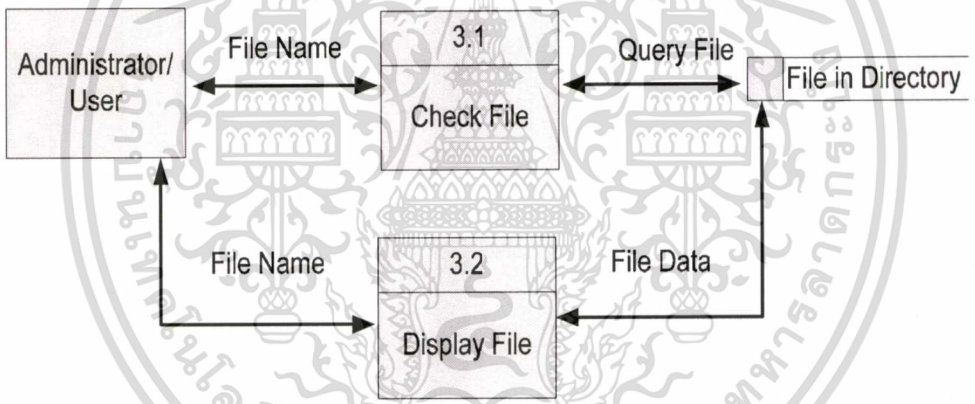
รูปที่3.9 เป็นการแสดงการไหลของข้อมูลของ Process การตรวจสอบ Check Password โดยฟังก์ชั่น Check Password จะแบ่งเป็นสองส่วนคือ Check User ID ใช้ตรวจสอบ User ID เทียบกับ Database ส่วนที่สองคือ Check Password ใช้ตรวจสอบว่า Password นั้นถูกต้องหรือไม่



รูปที่ 3.10 แสดงการไหลของข้อมูลของระบบจัดการVPN บน FreeBSD (DFD level 1 Process 2)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

จากรูปที่ 3.10 นั้นเป็นการแสดงการไหลของข้อมูลของ Process File Configure Handle ซึ่งได้แบ่งออกเป็น 5 ส่วนคือ เริ่มจาก Add ใช้ในการเพิ่มไฟล์และข้อมูลของผู้ใช้เมื่อมีการเพิ่ม จำนวนผู้ใช้ ส่วนที่สองคือ Delete ซึ่งใช้ในการลบไฟล์รวมไปถึงข้อมูลในระบบที่เกี่ยวข้องกับผู้ใช้นั้นๆ เมื่อมีการลดผู้ใช้ ในระบบ ส่วนที่สาม Update ใช้ในการเปลี่ยนแปลงไฟล์หรือข้อมูลที่เกี่ยวข้องกับผู้ใช้ ส่วนที่4 Monitor ใช้ในการตรวจสอบสถานะการเชื่อมต่อโดยจะไปดึง (Query) ข้อมูลเฟรมว่ามีการเขียนPacketส่งผ่าน Tunneling หรือไม่โดยข้อมูลเฟรมนั้นจะถูกเขียนลงไฟล์ Status ทุก 5 วินาทีและถ้าไม่มีการเขียน Packet ลงไปในเฟรม 20 วินาที ไฟล์ Status จะถูก Reset ให้มีค่าเป็นศูนย์ดังนั้นการตรวจสอบสถานะจะมีความถูกต้องในช่วง 20 วินาที ส่วนสุดท้าย Active/Stop Service มีหน้าที่ในการทำการ Start หรือ Stop Service ให้กับผู้ใช้ในระบบโดยสามารถจะทำได้ทีละ 1 ผู้ใช้หรือทำพร้อมกันทั้งหมดก็ได้



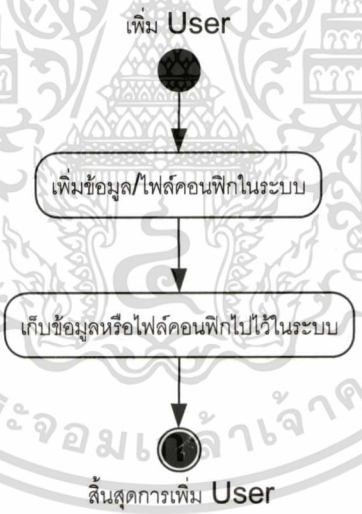
รูปที่ 3.11 แสดงการไหลของข้อมูลของระบบจัดการVPN บน FreeBSD (DFD level 1 Process 3)

จากรูปที่ 3.11 นั้นเป็นการแสดงการไหลของข้อมูลของ Process Query File ซึ่งได้แบ่งออกเป็น 2 ส่วนคือ เริ่มจาก Check File ใช้ในการในการตรวจสอบไฟล์คอนฟิก, ไฟล์ข้อมูลว่ามีอยู่ในระบบหรือไม่โดยถ้ามีไฟล์ที่ต้องการอยู่ในระบบก็จะสามารถทำ กระบวนการต่อไปแต่ถ้าไม่พบไฟล์ที่ต้องการก็จะแจ้งกลับมาว่าไม่พบไฟล์ดังกล่าว ส่วนสุดท้ายคือ Display File โดยเมื่อผ่านการตรวจสอบจากส่วน Check File ระบบก็จะแสดงข้อมูลซึ่งอาจจะเป็นการ Download หรือ แสดงทางหน้าจอขึ้นอยู่กับประเภทของไฟล์ เช่นถ้าเป็นไฟล์คอนฟิกก็จะให้ Download ไปเก็บไว้ที่เครื่อง Client เพื่อใช้ในการ Start Service ด้านฝั่ง Client แต่ถ้าเป็นไฟล์ช่วยเหลือก็จะแสดงทางหน้าจอคอมพิวเตอร์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ฟังค์ชั่นการทำงานพื้นฐาน (Basic Function)

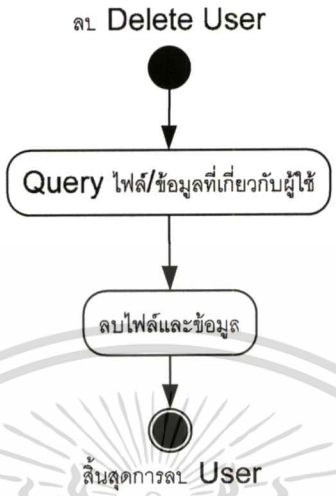
ADD การเพิ่มผู้ใช้หรือเพิ่มการเชื่อมต่อระหว่างระบบเครือข่ายภายในองค์กรกับเครือข่ายสาธารณะภายนอกโดยโปรแกรมจะทำการเพิ่มข้อมูลของผู้ใช้หรือจะทำการสร้างไฟล์คอนฟิกขึ้นก่อนที่จะทำการเก็บไว้ในระบบ ซึ่งในระบบเครือข่ายส่วนตัวเสมือน (Virtual Private Network: VPN) นั้นจะกำหนดให้ไฟล์คอนฟิก 1 ไฟล์ต่อ 1 การเชื่อมต่อ (1 File: 1 Interface) จากนั้นเมื่อกำหนดค่าต่างๆในไฟล์เรียบร้อยก็จะทำการเซฟ (Save) กลับไปที่ตัววีพีเอ็นเซิร์ฟเวอร์ (VPN Server) เมื่อต้องการที่จะสตาร์ทเซอร์วิส (Start Service) ก็จะทำการสตาร์ทโดยใช้ Command Line เพื่อให้ระบบ load ไฟล์ขึ้นเข้าไปในระบบ ไฟล์ที่สร้างจะใช้นามสกุล .conf (ในโครงงานนี้จะเน้นการใช้คีย์แบบ Symmetric Key ซึ่งทาง Clientจึงต้องมีคีย์ที่มีค่าเหมือนกันดังนั้นเมื่อทาง Administrator ได้ Setup เสร็จก็ต้องส่ง File ที่เป็นคีย์ไปให้ User เพื่อใช้ในการ Setup ทางฝั่ง Client) การทำงานของฟังก์ชั่น ADD แสดงดังรูปที่ 3.12



รูปที่ 3.12 สเตทไดอะแกรม แสดงขั้นตอนการทำงานของ Function ADD

Delete การลดผู้ใช้นั้นจะทำโดยการ Query File ที่เกี่ยวข้องของUser นั้นแล้วทำการลบออกจากระบบ User นั้นก็จะไม่สามารถใช้งานเครือข่ายส่วนตัวเสมือนได้ โดยแสดงดังรูปที่ 3.13

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

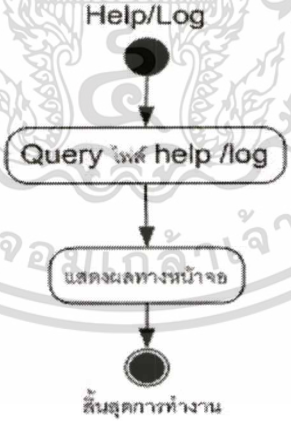


รูปที่ 3.13 สเตทไดอะแกรม แสดงขั้นตอนการทำงานของ Function Delete

จากรูปที่ 3.13 นั้นจะเริ่มจากการ Query File ก่อนที่จะทำการลบไฟล์ออก

Help ใช้ในการเรียกดูการติดตั้งและพารามิเตอร์ที่มีในโอเพ่นวีพีเอ็น (OpenVPN) โดยเป็นการเรียก File ที่เก็บไว้ในตัวเซิร์ฟเวอร์ขึ้นมาให้ Administrator ดูว่าพารามิเตอร์ที่จะใช้นั้นมี Option อะไรและแต่ละ Option นั้นมีความหมายอย่างไร

History ใช้ในการเรียกดู Log File เพื่อตรวจสอบการใช้งานโดยทั่วไปของ User ทั้งหมด

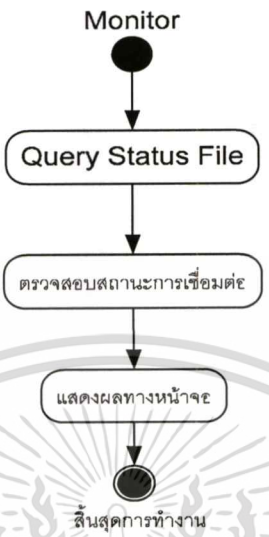


รูปที่ 3.14 สเตทไดอะแกรม แสดงขั้นตอนการทำงานของFunction Historyและ Help

จากรูปที่ 3.14 นั้นแสดงให้เห็นว่า Help/Log นั้นมีพื้นฐานหลักการทำงานที่คล้ายเหมือนกัน

Monitor ตรวจสอบการเชื่อมต่อในแต่ละส่วนได้ซึ่งจะตรวจสอบจากไฟล์ Status ว่า User นั้นยังคงสถานะภาพการเชื่อมต่ออยู่หรือไม่

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

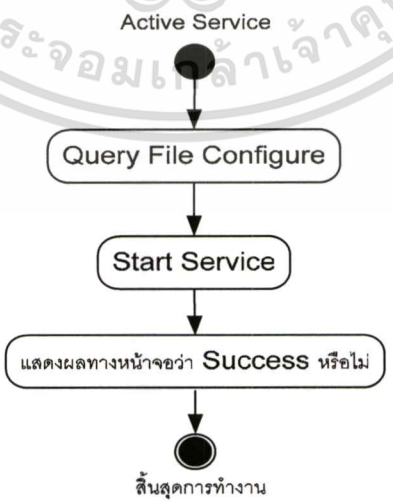


รูปที่ 3.15 สเตทไดอะแกรม แสดงขั้นตอนการทำงานของ Function monitor

รูปที่ 3.15 แสดงการทำงานของ Monitor โดยจะเริ่มจากการตรวจสอบข้อมูลในไฟล์ Status ว่ามีการเขียน Packet ลงไปใน Tunneling หรือไม่โดยจะมีการเขียนลงไปในไฟล์ Status ทุก 5 วินาทีแต่ถ้าไม่มีการเขียนหรือส่ง Packet ใน Tunneling เป็นเวลา 20 วินาที ระบบจะ Reset ค่าในไฟล์ Status ให้เป็นศูนย์ หลังจากตรวจสอบค่าในไฟล์ Status จะแจ้งผลทางหน้าจอ

ฟังค์ชั่นการจัดการการให้บริการ (Service Management Function)

Active Service เป็นฟังก์ชั่นสำหรับ start service ของ User โดยเริ่มจากการตรวจสอบไฟล์คอนฟิกว่ามีอยู่ในระบบหรือไม่ถ้าพบว่ามีอยู่ก็จะทำการ Start Service ซึ่งสามารถจะ start service ทั้งหมดพร้อมกันหรือจะเป็นทีละ user ก็ได้

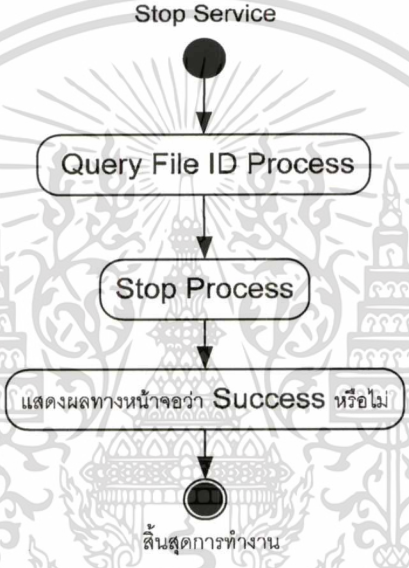


รูปที่ 3.16 สเตทไดอะแกรม แสดงขั้นตอนการทำงานของ Function Active Service

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

จากรูปที่ 3.16 แสดงให้เห็นพื้นฐานหลักการทำงานของ Function Active Service โดยในรูปเป็นการแสดงให้เห็นขั้นตอนการทำงานคร่าวๆของ Function นี้

Stop Service เป็นฟังก์ชั่นสำหรับ stop service ของ User โดยเริ่มจากการตรวจสอบไฟล์Id Process ว่าค่า Process ID ของ Service นั้นๆ เป็นค่าอะไรจากนั้นก็จะทำการ Kill Process เพื่อเป็นการ Stop Service นั้นๆ โดยการ Stop Service นั้นสามารถทำได้ทั้งหมดพร้อมกันหรือจะ Stop Service เพียงหนึ่ง User ก็ได้



รูปที่ 3.17 สเตทไดอะแกรม แสดงขั้นตอนการทำงานของ Function Stop Service

จากรูปที่ 3.17 แสดงให้เห็นพื้นฐานหลักการทำงานของ Function Stop Service โดยในรูปเป็นการแสดงให้เห็นขั้นตอนการทำงานคร่าวๆของ Function นี้

3.3 การออกแบบระบบงานส่วนข้อมูล

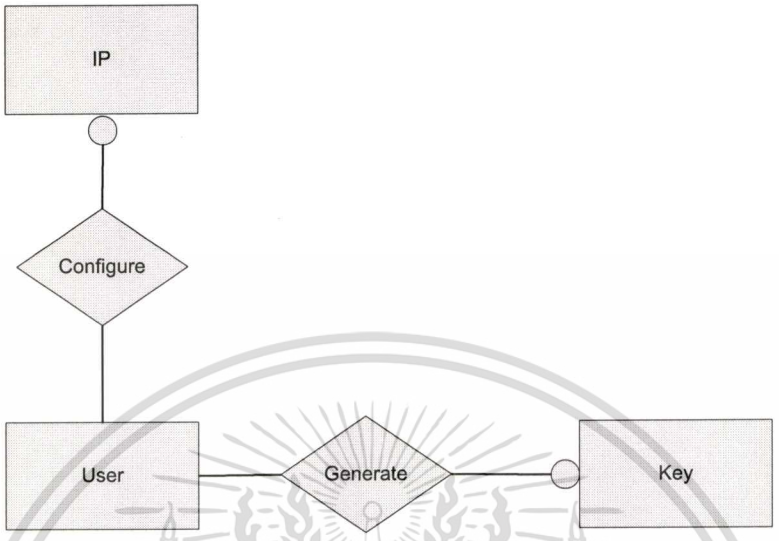
ในหัวข้อนี้จะอธิบายการออกแบบระบบเกี่ยวกับงานส่วนข้อมูลโดยแบ่งเป็น 2 ส่วนหลัก คือ

3.3.1 กลุ่มของข้อมูลที่เป็นระบบฐานข้อมูลที่สัมพันธ์กัน

3.3.2 กลุ่มของข้อมูลที่เป็นไฟล์ข้อความ (Text File)

3.3.1 กลุ่มของข้อมูลที่สัมพันธ์กันนั้นจะแสดงด้วยแบบจำลองข้อมูล โดยเครื่องมือที่จะนำมาใช้ในการวิเคราะห์คือแผนภาพแสดงความสัมพันธ์ระหว่างเอนทิตี (Entity Relationship Diagram) ดังภาพที่ 3.18

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 3.18 แบบจำลองความสัมพันธ์ระหว่างเอนทิตีส่วนข้อมูล

รูปที่ 3.18 แสดงความสัมพันธ์ระหว่างเอนทิตีส่วนข้อมูลภายในโครงงาน

รายละเอียดของเอนทิตีมีดังนี้

User เก็บข้อมูลเกี่ยวกับรายละเอียดของผู้ใช้ภายในระบบ

IP เก็บข้อมูลไอพีเพื่อใช้ในการสร้างไฟล์คอนฟิกของผู้ใช้ภายในระบบ

Key เก็บข้อมูลรายชื่อไฟล์คีย์ของผู้ใช้แต่ละคนภายในระบบ

พจนานุกรมข้อมูล

หลังจากที่ได้ทำการวิเคราะห์และออกแบบฐานข้อมูล แล้ว สามารถกำหนดคุณลักษณะของแอททริบิวต์ในแต่ละเอนทิตีได้ดังนี้

- เอนทิตี User

ตารางที่ 3.1 รายละเอียดตาราง User

Field	Type	Null	Key	Detail	Ref. Table
User_Open	Varchar(20)	N	PK	ชื่อที่ใช้ในระบบ	
User_ID	Varchar (4)	N		รหัสผู้ใช้งาน	
User_Name	Varchar (80)	N		ชื่อผู้ใช้งาน	
User_Email	Varchar (40)	N		อีเมล	
User_Status	Char(1)	N		สถานะผู้ใช้งาน	
User_Pwd	Varchar (8)	N		รหัสผ่าน	

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- เอนทิตี IP

ตารางที่ 3.2 รายละเอียดตาราง IP

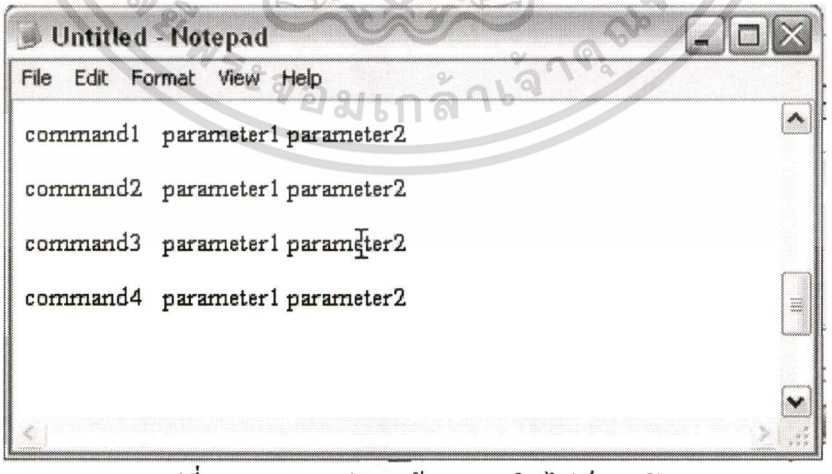
Field	Type	Null	Key	Detail	Ref. Table
User_Open	Varchar(15)	N	PK,FK	ชื่อที่ใช้ในระบบ	User
IP_1	Varchar(15)	N		ไอพีเซิร์ฟเวอร์	
IP_2	Varchar(15)	N		ไอพีไคลเอนต์	
Port	Int(5)	N		Port ของผู้ใช้	

- เอนทิตี Key

ตารางที่ 3.3 รายละเอียดตาราง Key

Field	Type	Null	Key	Detail	Ref. Table
User_Open	Varchar(8)	N	PK, FK	ชื่อที่ใช้ในระบบ	User
Key_Filename	Varchar(15)	N		ชื่อ ไฟล์คีย์ของผู้ใช้	

3.3.2 กลุ่มของข้อมูลที่เป็นไฟล์ข้อความ (Text File) นั้นมีลักษณะของBatch file ซึ่งเป็นการเก็บชุดของ Command Line ไว้เป็นบรรทัดสามารถแสดงได้ดังรูปที่ 3.19

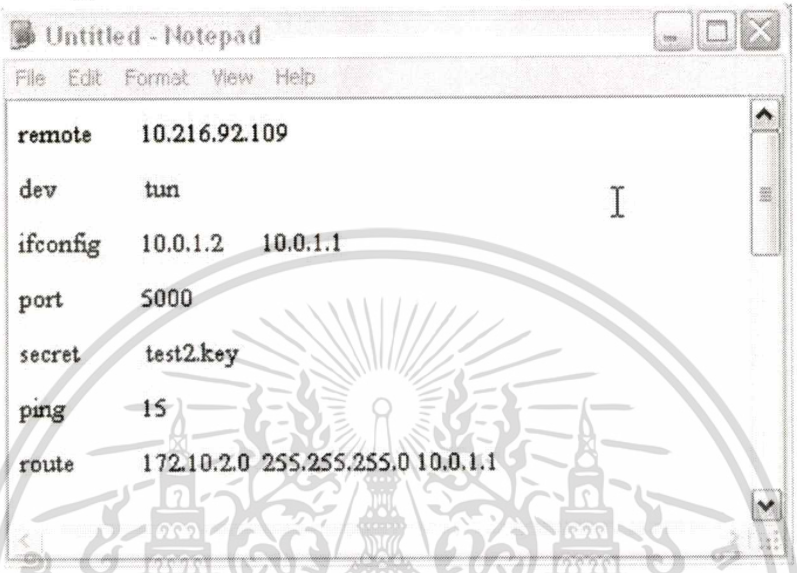


รูปที่ 3.19 แสดงรูปแบบข้อมูลภายในไฟล์คอนฟิก

รูปที่ 3.19 แสดงรูปแบบข้อมูลภายในไฟล์คอนฟิกซึ่งมีรูปแบบเป็นลักษณะ Batch File โดยในฟิลด์ (Filed) ที่ 1 นั้นเป็นคำสั่ง Command Line ที่ใช้ในการสั่งงานให้เป็นไปตามความต้องการของระบบ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ส่วนฟิลด์ที่ 2 และ3 หรือถัดมานั้นคือค่าพารามิเตอร์ของคำสั่งนั้นๆที่ต้องการเซตให้เป็นไปตามความต้องการของผู้ดูแลในการสร้างการเชื่อมต่อ ตัวอย่างเช่นรูปที่ 3.20



รูปที่ 3.20 แสดงตัวอย่างข้อมูลภายในไฟล์คอนฟิก

จากรูปที่ 3.20 นั้นจะเห็นว่าฟิลด์แรกนั้นเป็นคำสั่งที่ใช้จัดการระบบส่วนฟิลด์ถัดมานั้นเป็นพารามิเตอร์

สรุป

จากการวิเคราะห์และออกแบบในบทนี้นั้นสามารถแบ่งฟังก์ชั่นการทำงานได้เป็น 2 ส่วนหลักๆคือ ฟังค์ชั่นการทำงานพื้นฐาน (Basic Function) และฟังค์ชั่นการจัดการการให้บริการ (Service Management Function) โดยฟังก์ชั่นพื้นฐานนั้นเป็นการจัดการในกรณีของการเพิ่มหรือลดจำนวนผู้ใช้เป็นหลัก ในขณะที่ฟังค์ชั่นการจัดการการให้บริการนั้นจะเป็นการจัดการการให้บริการแก่ผู้ใช้ โดยแต่ละฟังก์ชั่นนั้นก็แบ่งย่อยลงตามรายละเอียดการทำงานของแต่ละฟังก์ชั่นย่อยซึ่งจะนำผลจากการวิเคราะห์และออกแบบนี้ไปพัฒนาโครงงานต่อไป

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 4

การพัฒนาระบบงาน

ในบทนี้จะกล่าวถึงการพัฒนาโครงงาน , ตัวโปรแกรม, การใช้งาน, เครื่องมือที่ใช้ในการพัฒนาโครงงานตลอดจนความสามารถของตัวโปรแกรมการจัดการเครือข่ายส่วนตัวเสมือนบนระบบปฏิบัติการ FreeBSD และหลักการทำงานของตัวโปรแกรมโดยละเอียด

4.1 เครื่องมือที่ใช้ในการพัฒนาโครงงาน

- EditPlus อิดิเตอร์ที่ใช้ในการเขียนโปรแกรม
- Microsoft Word ใช้ในการเขียนเอกสารประกอบการพัฒนาโครงงาน
- Visio ใช้ในการออกแบบวาดภาพประกอบคำอธิบาย
- VM Ware ใช้ในการสร้างสภาพแวดล้อมการทำงานของระบบปฏิบัติการ FreeBSD
- Apache Web server ใช้เป็นเว็บเซิร์ฟเวอร์บนระบบปฏิบัติการ FreeBSD
- PHP, Shell Script และ Java Script เป็นภาษาที่ใช้ในการพัฒนาโครงงาน
- Internet Explorer ใช้เป็นบราวเซอร์หลักในการทดสอบโครงงาน

4.2 รูปแบบการใช้งานของ OpenVPN

Application OpenVPN นั้นมีรูปแบบการใช้งานหลักอยู่2 แบบคือ

1. ใช้งานลักษณะ Bridge ซึ่งเป็นการสร้าง Tunneling อยู่บน Layer ที่ 2
2. ใช้งานลักษณะ Router ในรูปแบบนี้เป็นการสร้าง Tunneling อยู่ Layer ที่ 3 โดยตัว VPN Server นั้นจะทำหน้าที่ Forward Packet ส่งต่อให้ไปใน Private Network ที่อยู่หลัง VPN Server นั้นเอง

จากการศึกษาความเป็นไปได้ของโครงงานในระดับนี้จะใช้รูปแบบที่ 2 เนื่องจากเป็นรูปแบบที่ใช้มากกว่ารูปแบบแรกอีกทั้งไม่ซับซ้อนมากนัก

4.3 การออกแบบฟังก์ชั่นการทำงาน

ในการพัฒนาโครงงานได้แบ่งฟังก์ชั่นการทำงานเป็น 2 ส่วนคือ

1. ฟังก์ชันการทำงานพื้นฐาน (Basic Function) ซึ่งเป็นฟังก์ชั่นที่ใช้ในการเพิ่มลดจำนวนผู้ใช้งานตลอดจนการตรวจสอบสถานะและรวมไปถึงประวัติการเข้าใช้งานของ User

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2. ฟังก์ชั่น Service Management เป็นฟังก์ชั่นใช้ในการจัดการเกี่ยวกับการ Start และ Stop Service

4.3.1 ฟังก์ชั่นการทำงานพื้นฐาน (Basic Function)

เป็นฟังก์ชั่นที่ใช้ในการจัดการเกี่ยวกับผู้ใช้เป็นหลักมี 5 ฟังก์ชั่นคือ

1. ADD
2. Delete
3. Help
4. History
5. Monitor

4.3.1.1 ADD

ฟังก์ชั่น ADD ทำหน้าที่เกี่ยวกับการเพิ่มผู้ใช้และผู้ดูแลในระบบ, สร้างไฟล์คอนฟิก และสร้างคีย์ที่ใช้ในการเข้ารหัสข้อมูลของผู้ใช้แต่ละคน

ขั้นตอนการเพิ่มผู้ใช้ในระบบมีดังนี้

1.เลือกหัวข้อ Add User ที่อยู่ในส่วนของ Basic Function

2.ให้ใส่ข้อมูล Useropenvpn (ซึ่งใช้ในการ Login), Password, Name-Lastname, E-mail และ ID (สามารถตรวจสอบได้ว่ามีอยู่ในระบบแล้วโดยเลือก view) เมื่อใส่ข้อมูลครบแล้วให้เลือก Submit

3.จากนั้นให้เลือกหัวข้อ Generate Key ที่อยู่ในส่วนของ Basic Function

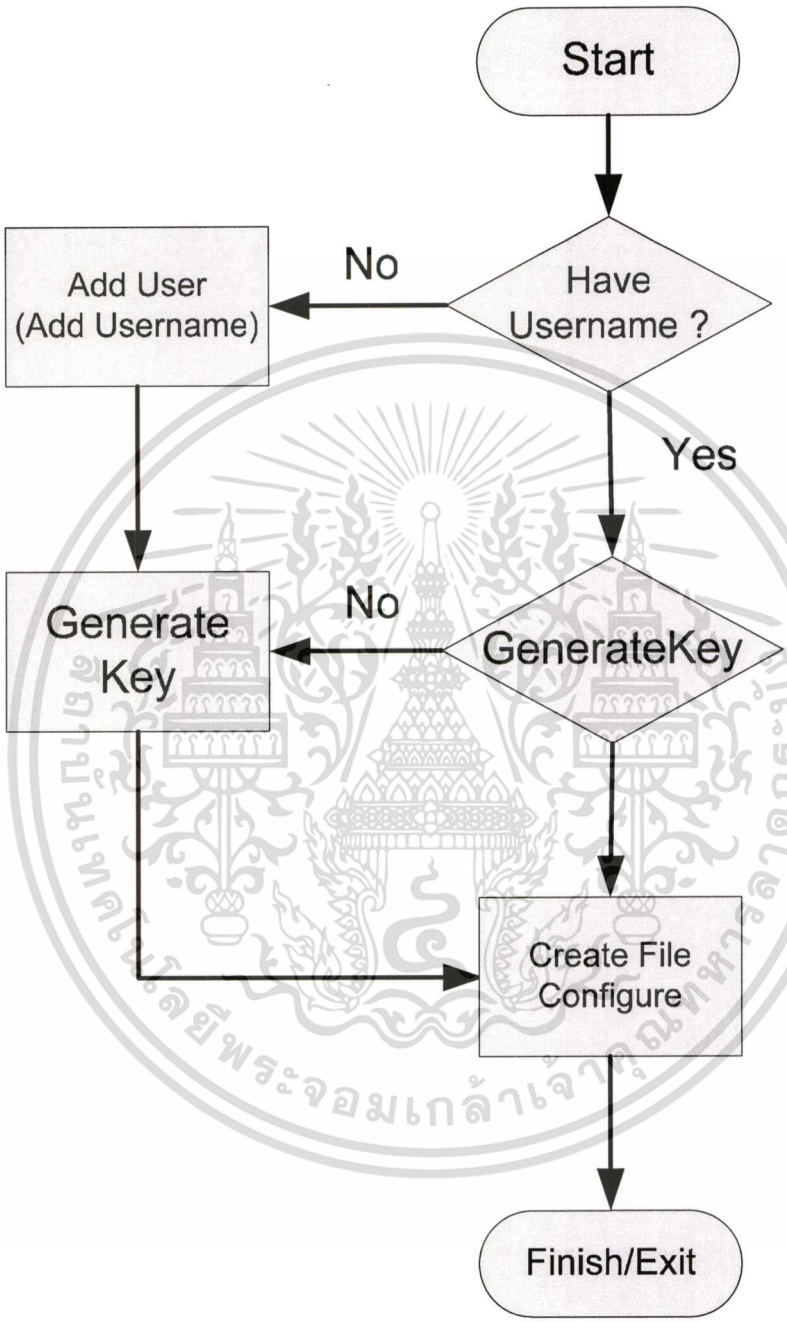
4. ให้ใส่ Useropenvpn ที่ได้ทำการเก็บไว้ในระบบก่อนหน้านี้แล้วเลือก GenerateKey โดยระบบจะแจ้งออกมาว่า “Genkey Complete” เมื่อทำการ Generate Key สำเร็จ

5. จากนั้นเลือกหัวข้อ Create/Delete File Configure เพื่อ Create File Configure

6.ใส่ค่า Useropenvpn ก่อนจะเลือกว่าจะ Create File Configure แบบใด โดยมีให้เลือก 2 ประเภทคือ Normal และ Advance ซึ่งการใช้ Advance นั้นจำเป็นต้องมีความเชี่ยวชาญในการใส่พารามิเตอร์อีกทั้งการใช้ Advanceนั้นจะ Create File ได้ทีละด้านกล่าวคือ Client และ Server นั้นเอง ดังนั้นถ้าไม่มีการเพิ่มพารามิเตอร์ที่พิเศษให้เลือก Normal แทนจากนั้นเลือกปุ่ม Configure

7. ใส่ค่าตามที่ช่องที่กำหนดไว้ก่อนกดปุ่ม Submit ระบบจะแจ้งออกมาว่า “Create File Complete” เป็นอันเสร็จกระบวนการเพิ่มผู้ใช้ในระบบ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.1 Flow Chart แสดงการเพิ่มผู้ใช้ในระบบ

จากรูปที่ 4.1 แสดงการทำงานของฟังก์ชั่น Add ในการเพิ่มผู้ใช้ในระบบโดยเริ่มจากการตรวจสอบว่ามีรายชื่ออยู่ในระบบแล้วหรือไม่ถ้ายังไม่มีก็จะให้ทำการเพิ่มรายชื่อในระบบก่อนที่จะให้ Generate Key โดยผู้ใช้แต่ละคนจะมีคีย์ได้ 1 คีย์เท่านั้น และเมื่อทำการเพิ่มรายชื่อและคีย์แล้วจึงจะสามารถจะสร้างไฟล์คอนฟิกเพื่อใช้ในการ Start Service ต่อไป

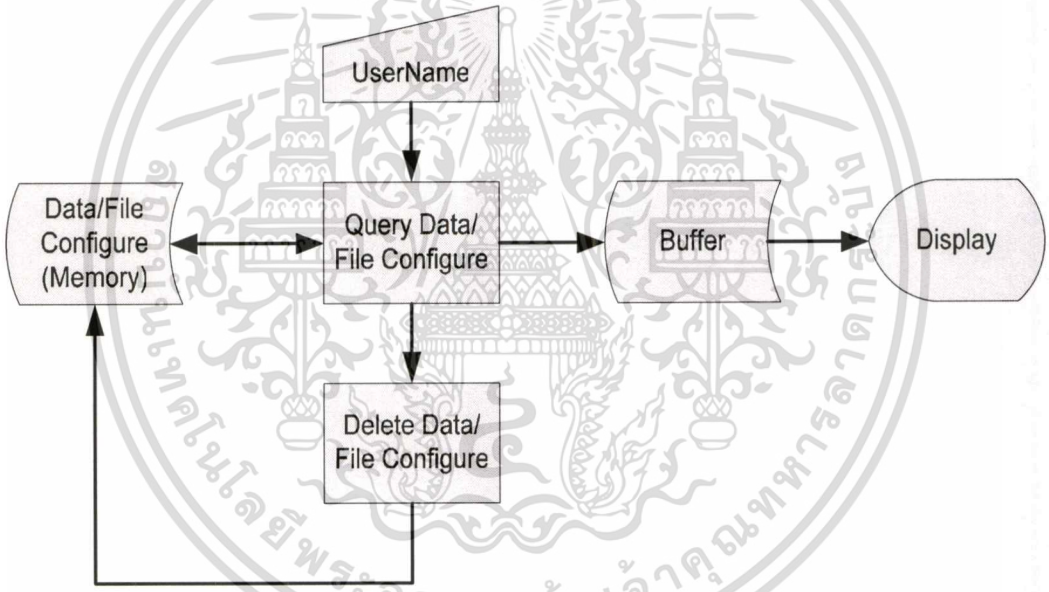
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4.3.1.2 Delete

ฟังก์ชั่น Delete ทำหน้าที่เกี่ยวกับการลบผู้ใช้ในระบบ โดยจะลบไฟล์คอนฟิก และคีย์ที่ใช้ในการเข้ารหัสข้อมูลของผู้ใช้แต่ละคนตลอดจน ไฟล์ประวัติการใช้งานในระบบด้วยเช่นกัน

ขั้นตอนการลบผู้ใช้ในระบบมีดังนี้

1. เลือกหัวข้อ Delete/Change
2. ใส่ค่า Useropenvpn ลงไป (ในกรณีที่ไม่ทราบให้เลือกปุ่ม ViewUser&ID เพื่อดูรายชื่อทั้งหมด)
3. เมื่อใส่ค่า Useropenvpn เรียบร้อยให้กดปุ่ม ConfirmDelete เพื่อลบผู้ใช้ในระบบ



รูปที่ 4.2 Flow Chart แสดงการลบข้อมูลตลอดจนไฟล์คอนฟิกของผู้ใช้ในระบบ

จากรูปที่ 4.2 แสดงการทำงานของฟังก์ชั่น Delete ในการลบผู้ใช้ออกจากระบบนั้นจะเริ่มจากใส่รายชื่อ (Username) จากนั้นระบบจะทำการค้นหาว่าผู้ใช้รายนี้มีข้อมูลหรือไฟล์ที่เกี่ยวข้องกับผู้ใช้รายนี้ในระบบหรือไม่ และเมื่อค้นพบก็จะทำการลบออกจากหน่วยความจำและฐานข้อมูลซึ่งถือเป็นการเสร็จกระบวนการทำงานของฟังก์ชั่น Delete

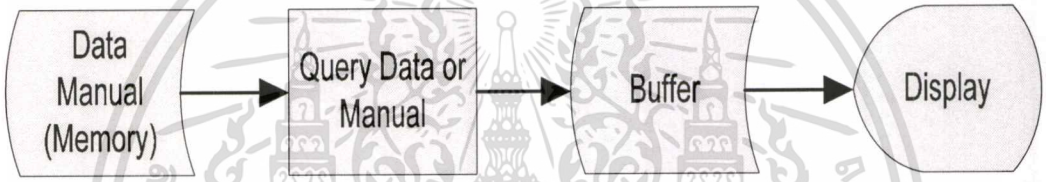
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4.3.1.3 Help

ฟังก์ชั่น Help ทำหน้าที่เกี่ยวกับการให้ข้อมูลในการใช้งานกับผู้ดูแลระบบ โดยผู้ใช้สามารถตรวจสอบว่าพารามิเตอร์ที่ใช้นั้นมีคุณสมบัติอย่างอะไรและใช้ทำอะไร นอกจากนี้ฟังก์ชั่น Help นี้ยังรวมไปถึงการให้ข้อมูลที่มีอยู่ในระบบเพื่อทำให้การเพิ่มค่า, เปลี่ยนแปลงสถานะทำได้ง่ายยิ่งขึ้น ขั้นตอนใช้งานฟังก์ชั่น Help ของระบบมีดังนี้

1.เลือกหัวข้อ Help ที่อยู่ในส่วนของ Main Menu

2.ระบบจะ Display Manual ของ OpenVPN



รูปที่ 4.3 Flow Chart แสดงกระบวนการของฟังก์ชั่น Help ในระบบ

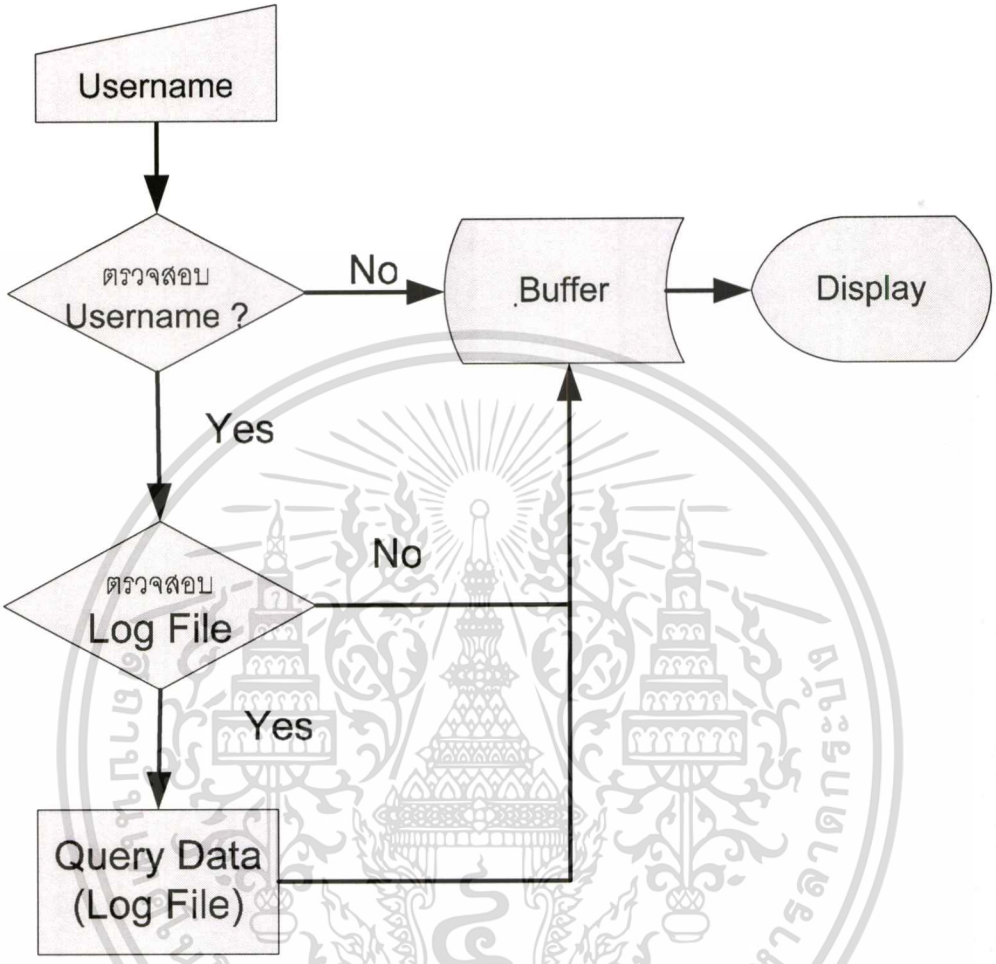
จากรูปที่ 4.3 แสดงการทำงานของฟังก์ชั่น Help ในการให้ข้อมูลในการใช้งานแก่ผู้ดูแลระบบ เริ่มจากระบบจะไป Query ข้อมูลหรือคู่มือที่เก็บไว้ในตัวเซิร์ฟเวอร์แล้วนำไปแสดงผลที่หน้าจอ (Display)

4.3.1.4 History

ฟังก์ชั่น History ทำหน้าที่เกี่ยวกับแสดงข้อมูลการใช้งานตลอดจนข้อผิดพลาดที่เกิดขึ้นในการสร้างการเชื่อมต่อ โดยผู้ดูสามารถตรวจสอบว่าผู้ใช้ในระบบแต่ละคนมีการเข้าใช้งานอย่างไร ขั้นตอนใช้งานฟังก์ชั่น History ของระบบมีดังนี้

1. เลือกหัวข้อ Log User
2. ใส่ค่า Useropenvpn ลงไปก่อนกดปุ่ม CheckLog ระบบจะทำการแสดงผลออกมาทางหน้าจอ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.4 Flow Chart แสดงกระบวนการของฟังก์ชั่น History

จากรูปที่ 4.4 แสดงการทำงานของฟังก์ชั่น History เพื่อใช้ในการตรวจสอบประวัติการเชื่อมต่อของผู้ใช้ในระบบโดยเมื่ออินพุทค่า Usernameลงไประบบจะทำการตรวจสอบว่ามีรายชื่อ (Username) นี้ในระบบหรือไม่ซึ่งถ้ามีรายชื่อนี้ในระบบ ระบบก็จะทำการตรวจสอบว่ามี Log file อยู่หรือไม่แล้วจะแสดงผลทางหน้าจอให้ผู้ดูแลระบบทราบ

4.3.1.5 Monitor

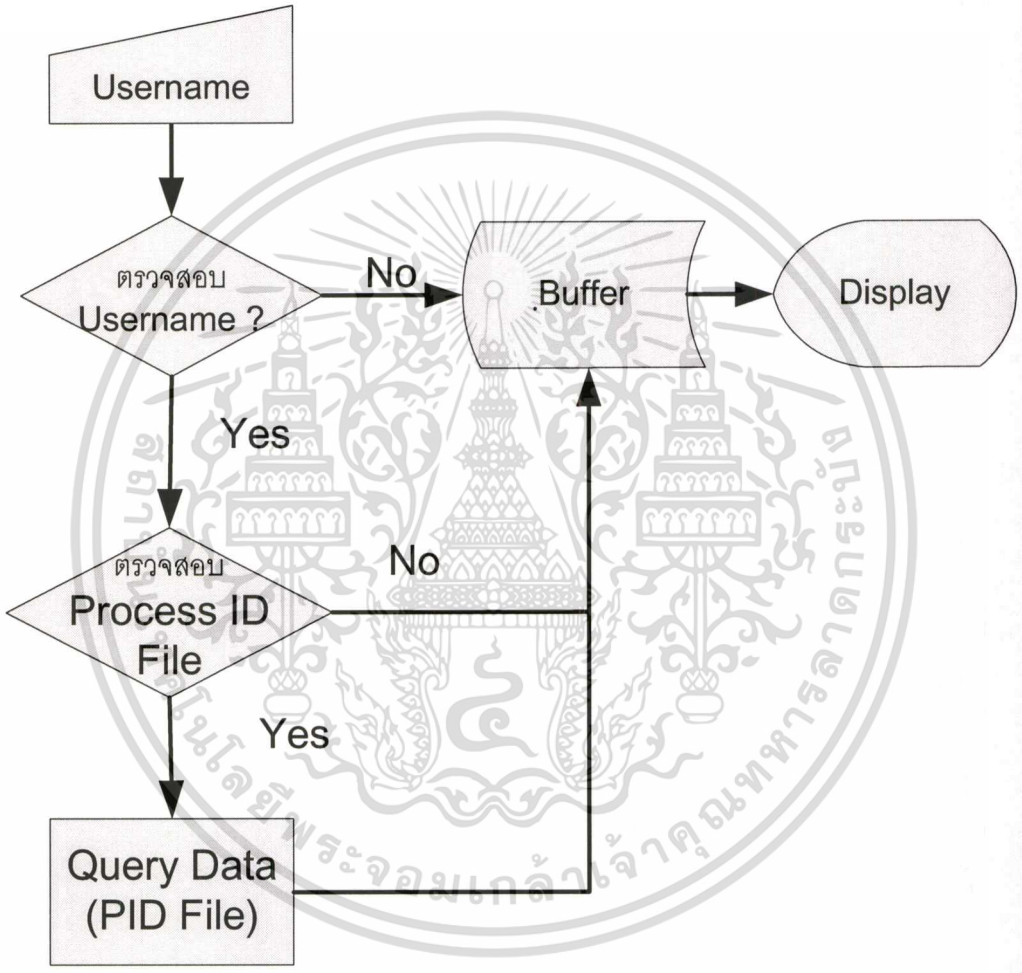
ฟังก์ชั่น Monitor ใช้ในการตรวจสอบสถานะการเชื่อมต่อรวมไปถึงการให้บริการ (On Service) ของระบบซึ่งสามารถแสดงผลได้ทั้งหมดพร้อมกันหรือแสดงผลเพียงรายเดียว

ขั้นตอนใช้งานฟังก์ชั่น Monitor (ทีละ 1 Connection)

1. เลือกหัวข้อ Status

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2. ใส่ Useropenvpn ก่อนที่จะเลือกดูสถานการณ์เชื่อมต่อ(Status) หรือ สถานการณ์ให้บริการ (Process ID)
3. กดปุ่ม Check เพื่อดูผล

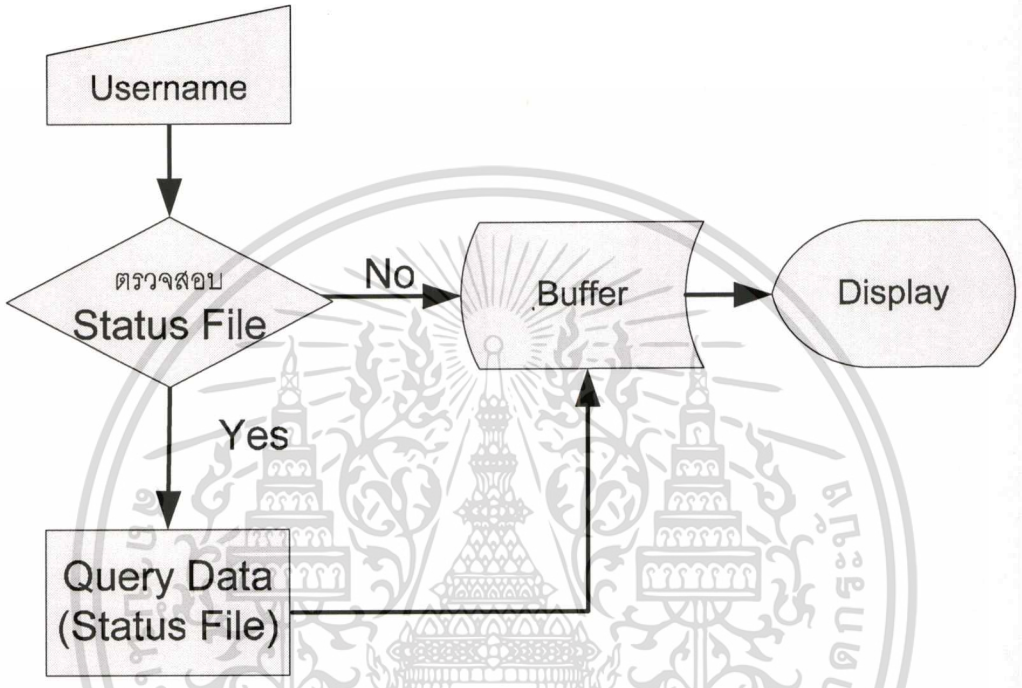


รูปที่ 4.5 Flow Chart แสดงกระบวนการของฟังก์ชั่น Monitor ในกรณีตรวจสอบการให้บริการ (On Service) ทีละ 1 Username

จากรูปที่ 4.5 แสดงการทำงานของฟังก์ชั่น Monitor เพื่อใช้ในการตรวจสอบการให้บริการ (On Service) การเชื่อมต่อของระบบโดยเมื่ออินพุทค่า Usernameลงไประบบจะทำการตรวจสอบว่ามีรายชื่อ (Username) นี้ในระบบหรือไม่ซึ่งถ้ามีรายชื่อนี้ในระบบ ระบบก็จะทำการตรวจสอบว่ามี PID File อยู่หรือไม่แล้วจะแสดงผลทางหน้าจอให้ผู้ดูแลระบบทราบ (PID File คือ ไฟล์ที่เก็บค่า

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Process ID ของการเชื่อมต่อไว้ซึ่งไฟล์นี้จะถูกสร้างขึ้นพร้อมกับการสตาร์ทเซอร์วิสของแต่ละ Username)



รูปที่ 4.6 Flow Chart แสดงกระบวนการของฟังก์ชั่น Monitor ในกรณีตรวจสอบการเชื่อมต่อ ทีละ 1 Username

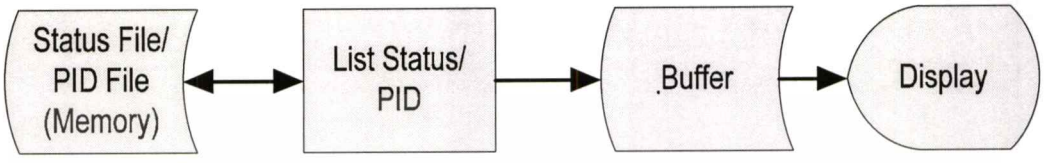
จากรูปที่ 4.6 แสดงการทำงานของฟังก์ชั่น Monitor เพื่อใช้ในการตรวจสอบการเชื่อมต่อ ระหว่างผู้ใช้กับระบบว่าได้เชื่อมต่อกันแล้วหรือไม่โดยใส่อินพุทค่า Usernameลงไป แล้วระบบจะทำการตรวจสอบว่ามีไฟล์สถานะ (Status File) หรือไม่ ซึ่งถ้ามี ระบบจะแสดงผลทางหน้าจอให้ผู้ดูแลระบบทราบ

หมายเหตุ ไฟล์สถานะ (Status File) นั้นจะถูก Update โดยระบบทุก 5 วินาที ซึ่งค่าที่เก็บไว้ภายในไฟล์คือค่าจำนวน Packet ที่ส่งผ่าน Tunneling ภายหลังจากมีการเชื่อมต่อระหว่างผู้ใช้แล้วนั้นจะมีการตรวจสอบจากระบบโดยการส่ง Ping Packet (ICMP) เข้าไปในการเชื่อมต่อนั้นหมายความว่า Packet ที่ส่งไปนั้นจะถูกเข้ารหัสเปรียบเสมือนเป็นข้อมูลเพียงแต่ต้องมีการตอบรับจากปลายทางแต่ถ้าไม่มีการส่ง packet กลับมาเป็นระยะเวลา 10 วินาที หรือ 20 วินาทีระบบจะทำการรีเซต(Reset)ค่าจำนวน packet ในไฟล์สถานะให้เป็นศูนย์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ขั้นตอนใช้งานฟังก์ชั่น Monitor เพื่อตรวจสอบการเชื่อมต่อและการให้บริการทั้งหมด

-กดปุ่ม ALLProcess ระบบจะแสดงผลทางหน้าจอ



รูปที่ 4.7 Flow Chart แสดงกระบวนการของฟังก์ชั่น Monitor ในกรณีตรวจสอบการให้บริการพร้อมกันทั้งหมด

จากรูปที่ 4.7 แสดงการทำงานของฟังก์ชั่น Monitor เพื่อใช้ในการตรวจสอบการเชื่อมต่อและการให้บริการ (On Service) พร้อมกันทั้งหมด โดยระบบจะตรวจสอบไฟล์สถานะ (Status File) และ PID File ก่อนที่จะแสดงผลทางหน้าจอ

4.3.2 ฟังก์ชั่นการจัดการการให้บริการ (Service Management Function)

เป็นฟังก์ชั่นที่ใช้ในการจัดการเกี่ยวกับผู้ใช้เป็นหลักมี 2 ฟังก์ชั่นคือ

1. Active Service
2. Stop Service

4.3.2.1 Active Service

เป็นฟังก์ชั่นที่ใช้ในการสตาร์ทเซอร์วิส (Start Service) โดยสามารถจะสตาร์ทเซอร์วิสพร้อมกันทั้งหมดที่ได้ทำการสร้างไฟล์คอนฟิกไว้แล้วหรือจะเลือกที่จะสตาร์ทเซอร์วิสทีละ 1 User ก็ได้

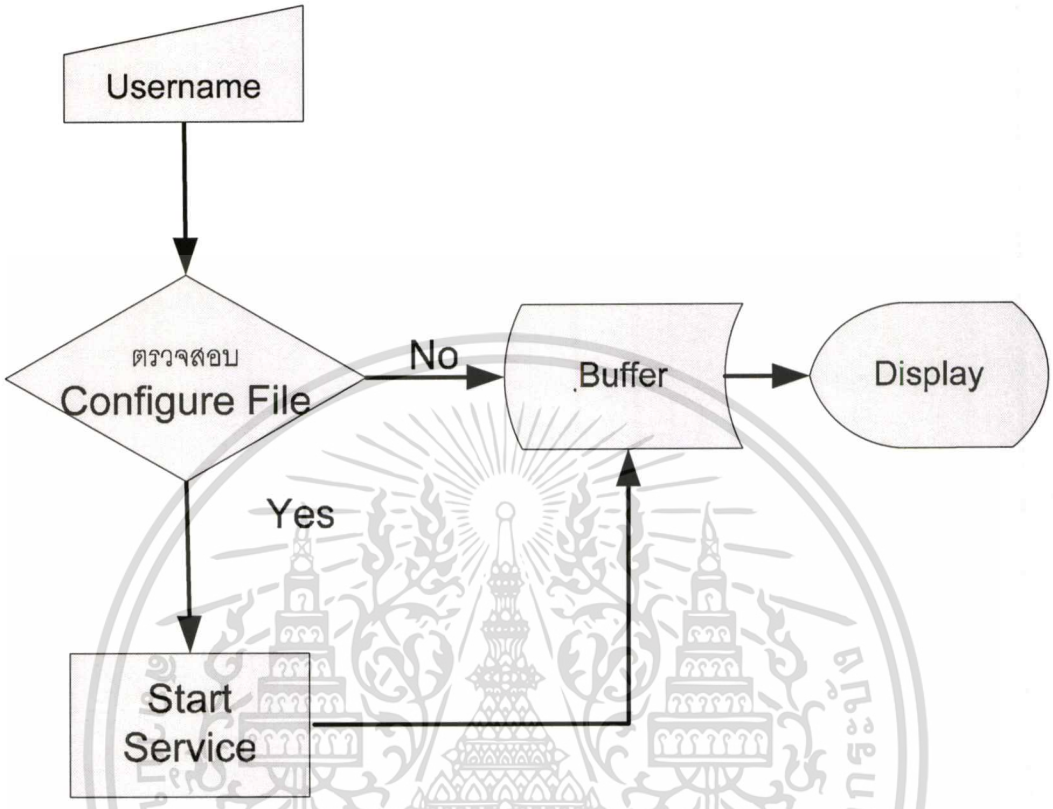
ขั้นตอนใช้งานฟังก์ชั่น Active Service (ทีละ 1 User)

1. เลือกหัวข้อ Status
2. ใส่ค่า Useropenvpn ก่อนเลือกค่าในส่วนของ One Connection เป็น Start
3. กดปุ่ม Change เพื่อให้สตาร์ทเซอร์วิส

Start - ใช้ในการสตาร์ทเซอร์วิส

Reload-ใช้ในการรีสตาร์ทเซอร์วิส

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.8 Flow Chart แสดงกระบวนการของฟังก์ชั่นActive Service ในกรณีการสตาร์ทเซอร์วิสทีละ 1 User

จากรูปที่ 4.8 แสดงการทำงานของฟังก์ชั่น Active Service เพื่อใช้ในการสตาร์ทเซอร์วิสทีละ 1 User โดยเริ่มจากการใส่ค่า Username ระบบจะทำการตรวจสอบไฟล์คอนฟิก (Configure File) ก่อนที่จะสตาร์ทเซอร์วิสนั้นๆ

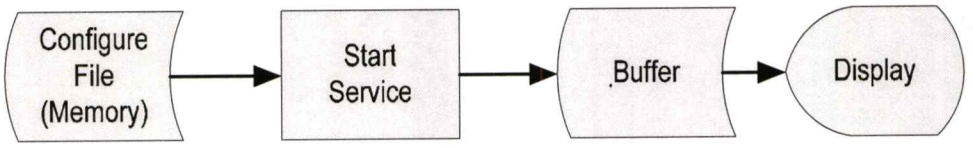
ขั้นตอนใช้งานฟังก์ชั่น Active Service (ทั้งหมด)

1. เลือกหัวข้อ Status
2. เลือกค่าในส่วนของ All Connection เป็น Start
3. กดปุ่ม ALLStatus เพื่อให้สตาร์ทเซอร์วิส

Start - ใช้ในการสตาร์ทเซอร์วิส

Reload-ใช้ในการรีสตาร์ทเซอร์วิส

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.9 Flow Chart แสดงกระบวนการของฟังก์ชั่นActive Service ในกรณีการสตาร์ทเซอร์วิสพร้อมกันทั้งหมด

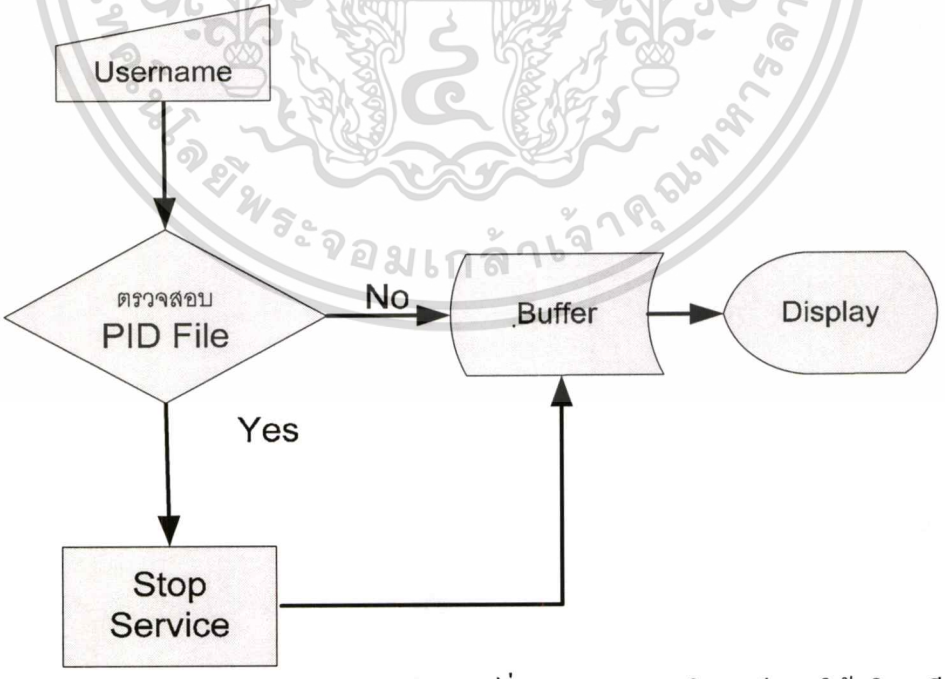
จากรูปที่ 4.9 แสดงการทำงานของฟังก์ชั่น Active Service เพื่อใช้ในการสตาร์ทเซอร์วิสทั้งหมดโดยเริ่มจากระบบจะทำการอ่านข้อมูลไฟล์คอนฟิก (Configure File) ทั้งหมดก่อนที่จะสตาร์ทเซอร์วิสนั้นๆ พร้อมกันทั้งหมด

4.3.2.2 Stop Service

เป็นฟังก์ชั่นที่ใช้ในการหยุดให้บริการ (Stop Service) โดยสามารถจะหยุดพร้อมกันทั้งหมดหรือจะเลือกที่จะหยุดให้บริการทีละ 1 User ก็ได้

ขั้นตอนใช้งานฟังก์ชั่น Stop Service (ทีละ 1 User)

1. เลือกหัวข้อ Status
2. ใส่ค่า Useropenvpn ก่อนเลือกค่าในส่วนของ One Connection เป็น Stop
3. กดปุ่ม Change เพื่อให้สตาร์ทเซอร์วิส



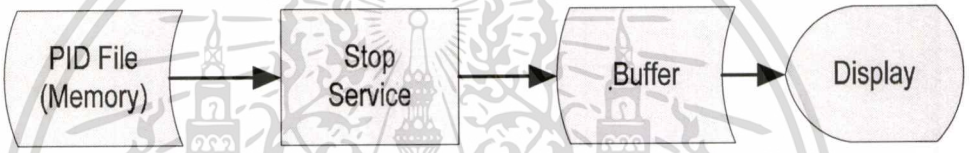
รูปที่ 4.10 Flow Chart แสดงกระบวนการของฟังก์ชั่นStop Service ในกรณีหยุดให้บริการทีละ 1 User

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

จากรูปที่ 4.10 แสดงการทำงานของฟังก์ชั่น Stop Service เพื่อใช้ในการหยุดให้บริการทีละ 1 User โดยเริ่มจากการใส่ค่า Username ระบบจะทำการตรวจสอบค่า Process ID ในPID File ก่อนที่จะหยุดให้บริการ Process ID นั้นๆ

ขั้นตอนใช้งานฟังก์ชั่น Stop Service (ทั้งหมด)

1. เลือกหัวข้อ Status
2. เลือกค่าในส่วนของ All Connection เป็น Stop
3. กดปุ่ม ALLStatus เพื่อหยุดการให้บริการทั้งหมด



รูปที่ 4.11 Flow Chart แสดงกระบวนการของฟังก์ชั่นStop Service ในกรณีหยุดให้บริการพร้อมกันทั้งหมด

จากรูปที่ 4.11 แสดงการทำงานของฟังก์ชั่น Stop Service เพื่อใช้ในการหยุดให้บริการทั้งหมด โดยระบบจะทำการตรวจสอบค่า Process ID ในPID File ก่อนที่จะหยุดให้บริการ Process ID

4.4 การพัฒนาโครงงาน

หัวข้อนี้จะกล่าวถึงตัวโครงงานที่ได้พัฒนาขึ้นโดยจะแบ่งเป็น 2 ส่วนคือ

1. การทำงานของโปรแกรมหลักๆที่ใช้ในการพัฒนา (เฉพาะส่วนของ Shell Script)
2. ส่วนที่ติดต่อกับผู้ใช้ (User Interface)

4.4.1 การทำงานของโปรแกรมหลัก

โครงงานนี้จะเน้นการโปรแกรมโดยใช้ภาษา Shell Script เป็นหลักในการจัดการส่วนที่เรียกว่า Back End และจะใช้ภาษา PHP ในส่วนที่ติดต่อกับผู้ใช้ (Web) โดยในที่นี้จะกล่าวถึงส่วนที่เป็น Back End เท่านั้น ส่วนที่สำคัญของ Back End มีดังนี้คือ

1. การ Generate Key
2. การ Start/Stop/Reload Service
3. การตรวจสอบสถานการณ์เชื่อมต่อ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

1.ไฟล์ Gen.sh ทำหน้าที่ Generate Key

```
#!/bin/sh
# Path ของ Directory ตัว Application ของ OpenVPN
openvpn="/usr/local/sbin/openvpn"
# Path ของ Directory ที่ใช้เก็บค่าคีย์
key1="/etc/openvpn/key/"
# Path ของ PID directory โดยไฟล์นี้ทำหน้าที่เก็บค่า Process ID
piddir="/var/run/openvpn"
# Path ของ Directory ที่ใช้เก็บค่าไฟล์คอนฟิกที่สร้างขึ้น
work=/etc/openvpn
# ใช้ Case เพื่อสร้างรายการฟังก์ชั่น
case "$1" in
#เรียก Application OpenVPN เพื่อให้ Generate Key ไปเก็บไว้ที่ Path ที่กำหนดไว้
        start)
                $openvpn  --cd /etc/openvpn/key/  --genkey --secret  $2.key
                echo -n $"Generate Secret Key for openvpn:"
                ;;

                *)
#ใช้แสดงการใส่ค่า argument ของ shell script
                echo "Usage: gen.sh {start filename}"
                exit 1
                ;;
# จบ Function Case
esac
# ออกจะระบบ
exit 0
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.ไฟล์ Openv.sh ทำหน้าที่ Start/Stop/Restart/Reload

```
#!/bin/sh
# Path ของ Directory ตัว Application ของ OpenVPN
openvpn="/usr/local/sbin/openvpn"
# Path ของ Status directory โดยไฟล์นี้ทำหน้าที่เก็บค่าจำนวน Packet ที่ส่งผ่าน Tunneling
lock="/etc/openvpn/subsys"
# Path ของ PID directory โดยไฟล์นี้ทำหน้าที่เก็บค่า Process ID
piddir="/var/run/openvpn"
# Path ของ Directory ที่ใช้เก็บค่าไฟล์คอนฟิกที่สร้างขึ้น
work=/etc/openvpn
# Path ของ Directory ที่ใช้เก็บ Log File ที่ใช้เก็บประวัติการเข้าใช้ระบบ
log=/etc/openvpn/log

[ -f  $openvpn ] || exit 0

# ใช้  Function Case เพื่อสร้างรายการการทำงานเริ่มจาก Start/Stop/Restart/Reload
case "$1" in
 start)
        echo -n $"Start openvpn: All Connection <br>"

        /sbin/modprobe tun >/dev/null 2>&1
# ถ้าไม่มี Path ของ PID directory ส่วนนี้ก็จะทำการสร้าง Path พร้อมกับ Directory
        if [ ! -d  $piddir ]; then
           mkdir $piddir
        fi
# ก่อนจะ Start Service ทุกไฟล์คอนฟิกในระบบ นั้น จะทำการตรวจสอบว่ามี Service ค้างไว้
หรือไม่ถ้ามีจะทำการ Kill Process ก่อนที่จะ Start Service ในส่วนต่อไป
            for pidf in `/bin/ls $piddir/*.pid 2>/dev/null`; do
              if [ -s $pidf ]; then
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
            kill `cat $pidf` >/dev/null 2>&1
          fi
          rm -f $pidf
        done
        rm -rf $lock/*.status
        sleep 2
      rm -f $piddir/*.pid
      cd $work
      errors=0
      successes=0
# ก่อนจะ Start Service ทุกไฟล์คอนฟิกในระบบนั้นจะทำการตรวจสอบว่ามี Configure File อยู่
หรือไม่เพื่อใช้เป็นค่าตัวแปรในการวนรอบ Start Service
      for c in `/bin/ls *.conf 2>/dev/null`; do

        bn=${c%%.conf}
        rm -f $piddir/$bn.pid
# ในการ Start Service นั้นจะเพิ่มพารามิเตอร์ส่วนที่ใช้ในการสร้าง log file, Status File และการ
กำหนดค่าการตรวจสอบการส่งข้อมูลผ่าน Tunneling
        $openvpn --daemon --writepid $piddir/$bn.pid --config $c --cd $work --log-append
$log/$bn.log --status $lock/$bn.status 2 --ping-restart 20
# ถ้าไม่มี Error จะแสดงข้อความ " Already to Run Service"
        if [ $? = 0 ]; then
          successes=1
        else
          errors=1
        fi
      done

                                    if [ $successes = 1 ]; then
                                      echo " Already to Run Service"
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
fi
;;
```

#ใช้ Stop Service ทุก Connection โดยอ่านค่าจาก PID File แล้ว Kill เพื่อ Stop Service โดยเมื่อทำการ Stop Service เรียบร้อยก็จะทำการลบไฟล์ PID และ Status ออกจากระบบ

```
stop)
        echo -n $"Shutting down openvpn:All Connection <br> "
        for pidf in `/bin/ls $piddir/*.pid 2>/dev/null`; do
         if [ -s $pidf ]; then
           kill `cat $pidf` >/dev/null 2>&1
         fi
         rm -f $pidf
        done
        rm -f $lock/*.status
        ;;
```

#restart เป็นการใช้ 2 function มาต่อกันคือ stop และ start ผลที่ได้นั้น Process ID จะไม่เป็นค่าเดิม การทำงานของ Code คือจะประวิงเวลาไว้ 2 วินาทีหลังจาก Stop Service ทั้งหมดก่อนที่จะทำการ Start Service ใหม่

```
restart)
        $0 stop
        sleep 2
        $0 start
;;
```

#reload นั้นใช้ Kill โดยใช้พารามิเตอร์ –HUP เพื่อเป็นการ Reload Process โดยยังคงใช้ค่า Process ID ตัวเดิม

```
reload)
        echo -n $"Reload openvpn:All Connection "
           for pidf in `/bin/ls $piddir/*.pid 2>/dev/null`; do
                if [ -s $pidf ]; then
                   kill -HUP `cat $pidf` >/dev/null 2>&1
                fi
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
        done
    ;;
#ใช้แสดงการใส่ค่า argument ของ shell script
 *)
    echo "Usage: openvp.sh {start|stop|restart| reload}"
    exit 1
esac
exit 0
```

3. การตรวจสอบสถานะของระบบจะแบ่งเป็นการเปิดรอให้บริการ (On Service) และการเชื่อมต่อ

โดยจะแบ่งการทำงานเป็น 2 โปรแกรมคือ

1. ส่วนตรวจสอบสถานะการให้บริการ
2. ส่วนตรวจสอบสถานะการเชื่อมต่อว่าในเวลา ณ ขณะนั้นมีการเชื่อมต่อหรือไม่

3.1ไฟล์ Read.sh ทำหน้าที่ ตรวจสอบสถานะให้บริการของเซิร์ฟเวอร์

```
#!/bin/sh
# Path ของ PID directory โดยไฟล์นี้ทำหน้าที่เก็บค่า Process ID
piddir="/var/run/openvpn"
# เริ่มจากจะตรวจสอบว่ามีค่า Process ID อยู่หรือไม่โดยจะ List ค่าเหล่านี้ส่งไปยังหน้าจอซึ่งถ้าค่า
Process ID นั้นแสดงว่าระบบได้ทำการสตาร์ทเซอร์วิสขึ้นมาให้แล้ว รอการเชื่อมต่อจากฝั่ง
ไคลเอนต์ (Client)
case "$1" in
                pidn)
                    for pidf in `/bin/ls $piddir/$2.pid 2>/dev/null`; do
                    if [ -s $pidf ]; then
                        echo  `cat $pidf`
                    fi
                done
    ;;
                *)
                    echo "Usage: read.sh {pidn username}"
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
                exit 1
        ;;
esac
exit 0
```

3.2 ไฟล์ Conn.sh สอบสถานะการเชื่อมต่อว่าในเวลา ณ ขณะนั้นมีผู้ใช้ใดบ้างที่ทำการเชื่อมต่ออยู่

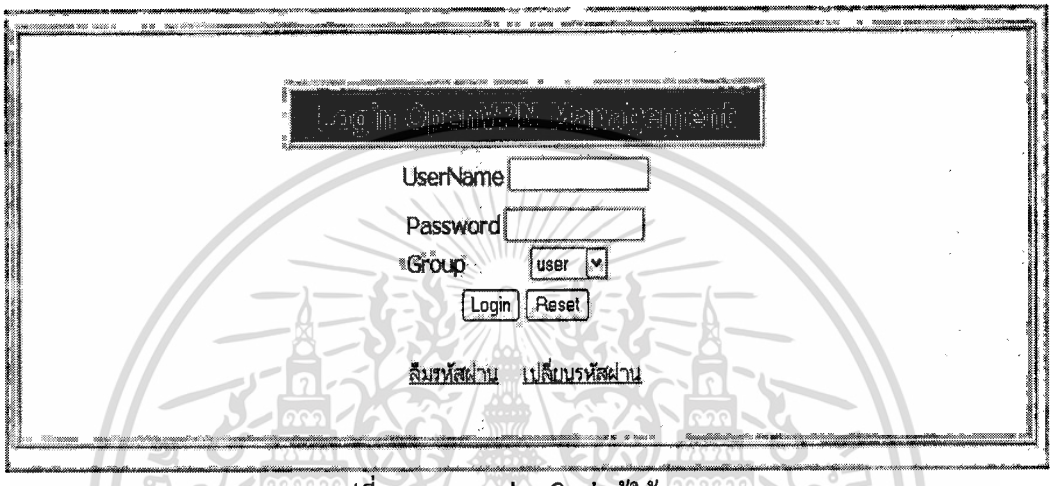
```
#!/bin/sh
# Path ของ PID directory โดยไฟล์นี้ทำหน้าที่เก็บค่า Process ID
piddir="/var/run/openvpn"
# Path ของ Status directory โดยไฟล์นี้ทำหน้าที่เก็บค่าจำนวน Packet ที่ส่งผ่าน Tunneling
lock="/etc/openvpn/subsys"
case "$1" in
# เริ่มจากจะตรวจสอบว่ามีไฟล์สถานะ (Status File) อยู่หรือไม่จากนั้นจะทำการอ่านค่าจำนวน
Packet ที่อยู่ในไฟล์โดยจะส่งผลแสดงเฉพาะค่าจำนวนที่รับมาจากไคลเอนต์ (Receive Packet) ซึ่งนี้
จะนำไปประมวลผลต่อบนตัวโปรแกรมที่ทำงานบนเว็บเซิร์ฟเวอร์อีกที
                conn)
                        for stat in `/bin/ls $lock/$2.status 2>/dev/null`; do
                                if [ -s $stat ]; then
                                        echo `cat $stat |awk  'NR==5' |cut -c20-`
                                fi
                        done
        ;;
                        *)

                                echo "Usage: conn.sh {conn  username}"
                                exit 1
        ;;
esac
exit 0
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4.4.2 ส่วนติดต่อกับผู้ใช้ (User Interface)

ในส่วนนี้จะเป็นการนำเสนอตัวโครงงานที่ได้พัฒนาขึ้นว่ามีลักษณะอย่างไรรูปแบบการจัดการของส่วนที่ใช้ติดต่อกับผู้ใช้เป็นอย่างไรเป็นหลัก



รูปที่ 4.12 แสดงส่วนติดต่อผู้ใช้ Login

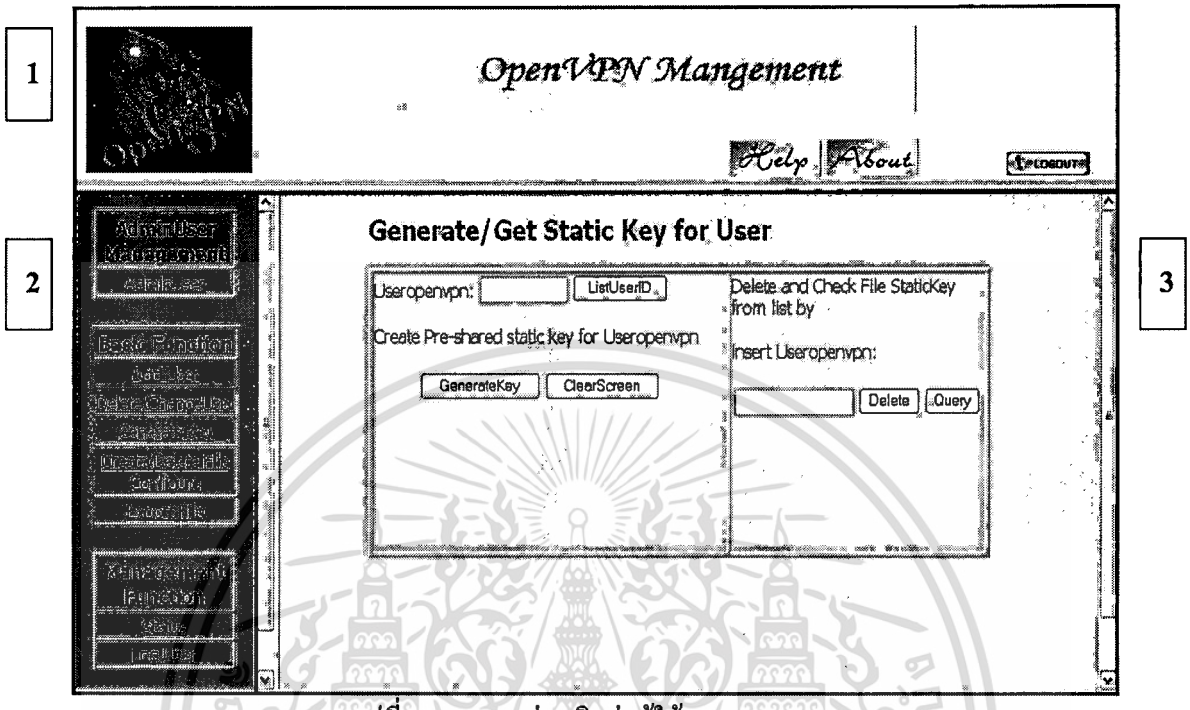
รูปที่ 4.12 แสดงส่วนติดต่อผู้ใช้ Login ประกอบด้วยช่องอินพุท UserName, Password และ Group โดยจะแบ่งเป็น Admin กับ User

4.4.2.1 ส่วนติดต่อกับผู้ใช้ (User Interface) ในส่วนของผู้ดูแลระบบ (Admin)

เป็นส่วนที่ผู้ดูแลระบบเท่านั้นสามารถเข้าไปใช้งานเพื่อจัดการระบบเครือข่ายส่วนตัวเสมือนได้โดยผู้ดูแลระบบจะสามารถทำรายการได้ดังต่อไปนี้

1. เพิ่มรายชื่อผู้ใช้หรือผู้ดูแลในระบบ
2. แก้ไขข้อมูลผู้ดูแลตลอดจนการเปลี่ยนรหัสผ่านด้วยเช่นกัน
3. สร้างไฟล์คอนฟิก (File Configure) ของผู้ใช้ (User) แต่ละคนในระบบ
4. สตาร์ทเซอร์วิส (Start Service) และ หยุดการให้บริการ (Stop Service) ได้พร้อมกันทั้งหมดหรือทีละ 1 User
5. ตรวจสอบการให้บริการตลอดจนสถานการณ์เชื่อมต่อของผู้ใช้งานในระบบ
6. สามารถตรวจสอบประวัติการใช้งานของผู้ใช้แต่ละคนได้

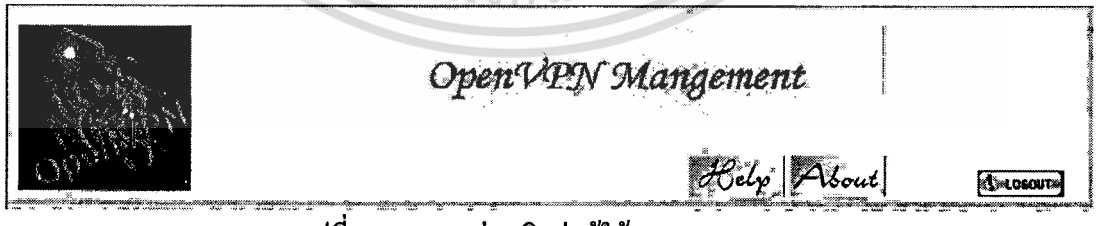
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.13 แสดงส่วนติดต่อผู้ใช้ Main (Admin)

รูปที่ 4.13 แสดงส่วนติดต่อผู้ใช้ Main ประกอบด้วย 3 ส่วนหลักๆคือโดยจะแบ่งเป็น

1. ส่วนเมนเมนู (Main Menu) หมายเลขที่ 1 ส่วนเรียกอ่านคู่มือ, ข้อมูลโครงงานและ Logout
2. ส่วนรายการฟังก์ชั่น (List Function Menu) หมายเลขที่ 2 เป็นส่วนที่รวมฟังก์ชั่นที่มีในระบบ
3. ส่วนเมนหลัก (Main) หมายเลขที่ 3 เป็นส่วนที่ใช้ในการทำรายการต่างๆ



รูปที่ 4.14 แสดงส่วนติดต่อผู้ใช้ Main Menu

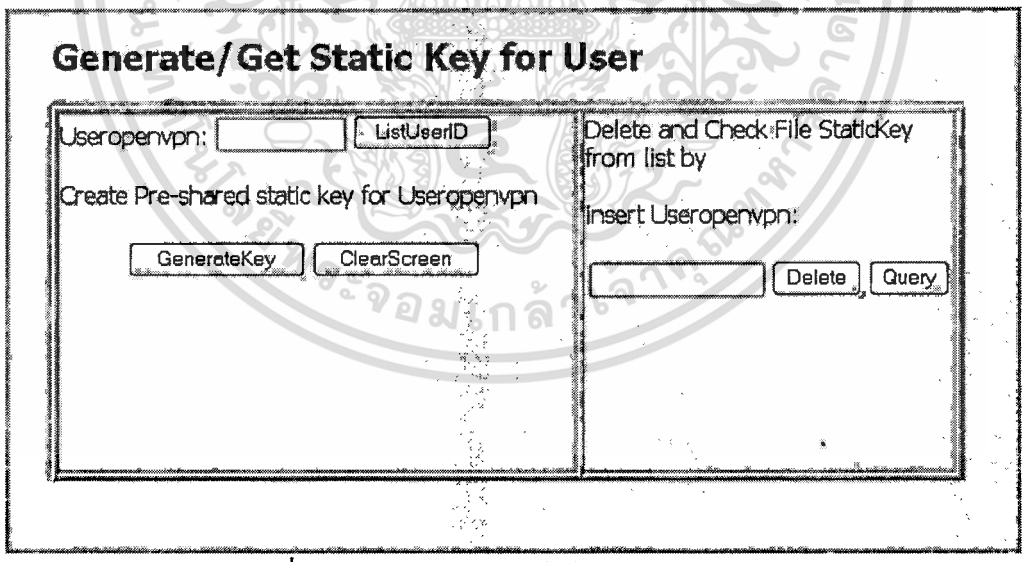
รูปที่ 4.14 แสดงส่วนติดต่อผู้ใช้ Main Menu ใช้ในการเรียกอ่านคู่มือ, ข้อมูลโครงงานและ Logout

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.15 แสดงส่วนติดต่อผู้ใช้ List Function

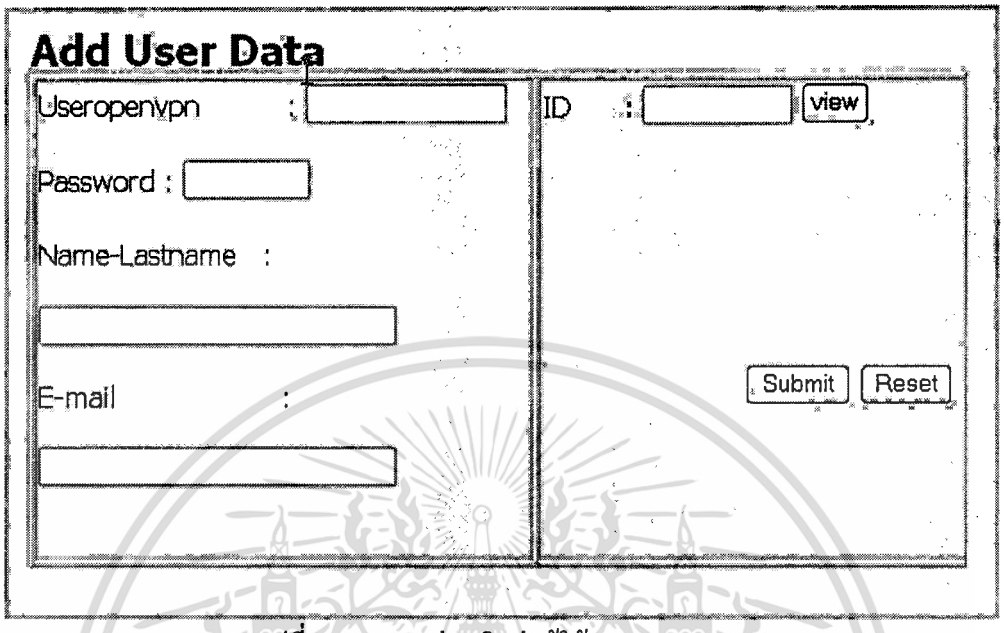
รูปที่ 4.15 แสดงส่วนติดต่อผู้ใช้ List Function ใช้ในการรวมฟังก์ชั่นที่มีในระบบของโครงงาน



รูปที่ 4.16 แสดงส่วนติดต่อผู้ใช้ ของ Generate Key

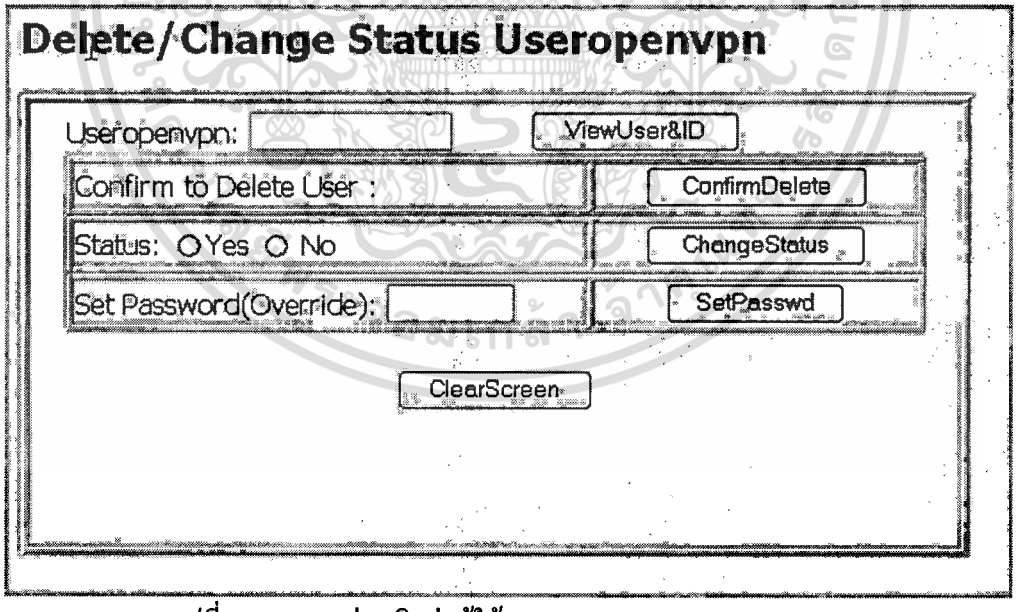
รูปที่ 4.16 แสดงส่วนติดต่อผู้ใช้ Generate Key ใช้ในการสร้างคีย์ของแต่ละผู้ใช้ในระบบโดยแบ่งเป็นส่วนที่ใช้ในการสร้างคีย์กับส่วนที่ใช้ในการลบคีย์ของแต่ละคน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.17 แสดงส่วนติดต่อผู้ใช้ ของ Add User

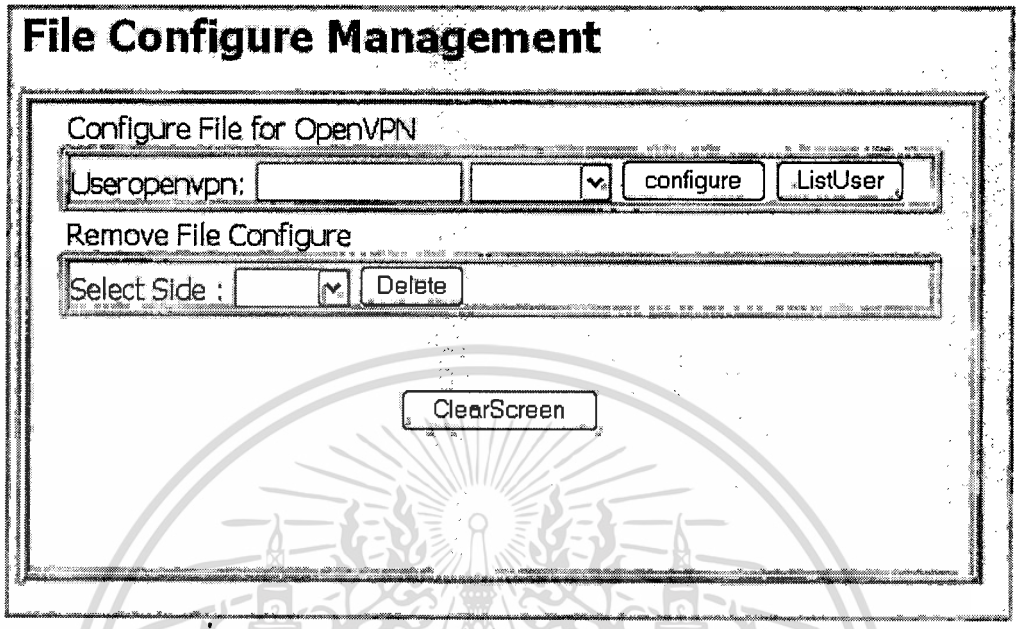
รูปที่ 4.17 แสดงส่วนติดต่อผู้ใช้ Add User ใช้ในการเพิ่มผู้ใช้ในระบบ



รูปที่ 4.18 แสดงส่วนติดต่อผู้ใช้ ของ Delete/Change Status User

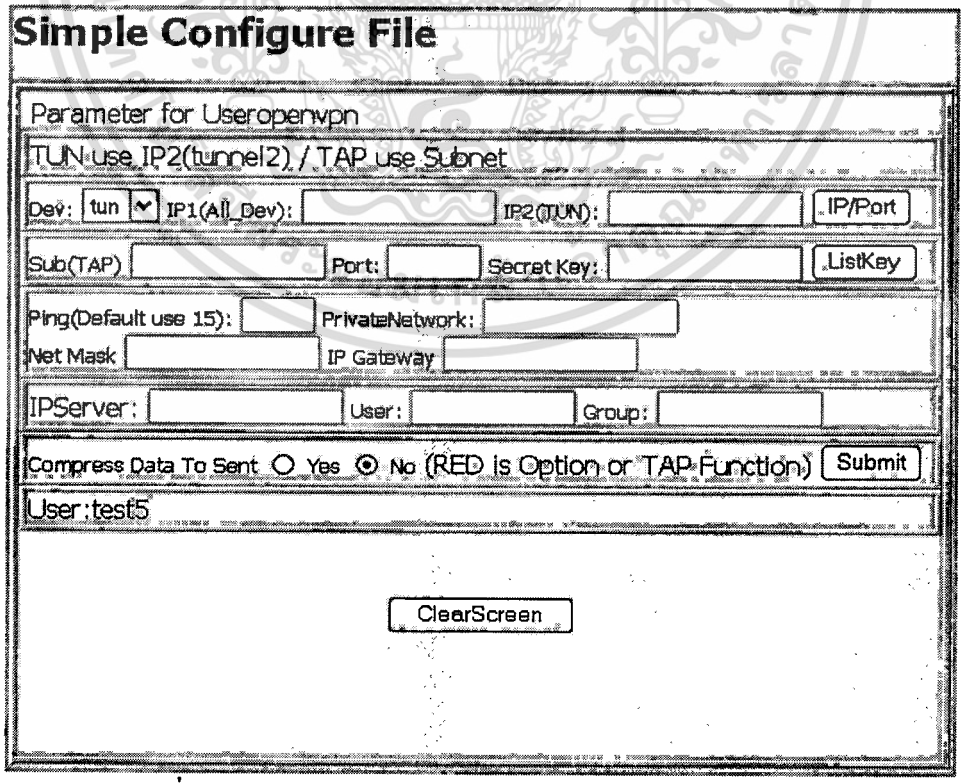
รูปที่ 4.18 แสดงส่วนติดต่อผู้ใช้ Delete User, เปลี่ยนสถานะการใช้งานตลอดจนการตั้งรหัสผ่านของผู้ใช้โดยผู้ดูแลระบบ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.19 แสดงส่วนติดต่อผู้ใช้ ของ File Configure Management

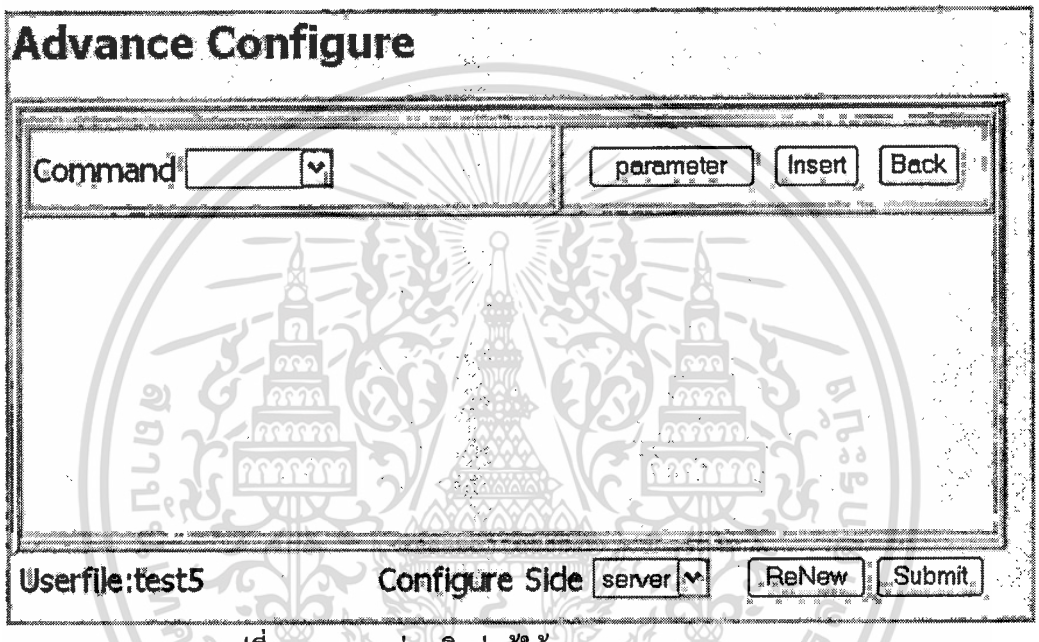
รูปที่ 4.19 แสดงส่วนติดต่อผู้ใช้ File Configure Management โดยฟังก์ชั่นนี้ใช้ในการสร้างหรือลบไฟล์คอนฟิกโดยผู้ดูแลระบบซึ่งการสร้างไฟล์คอนฟิกสามารถทำได้ 2 รูปแบบคือ Normal และ Advance



รูปที่ 4.20 แสดงส่วนติดต่อผู้ใช้ ของ Normal Create File (Simple)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

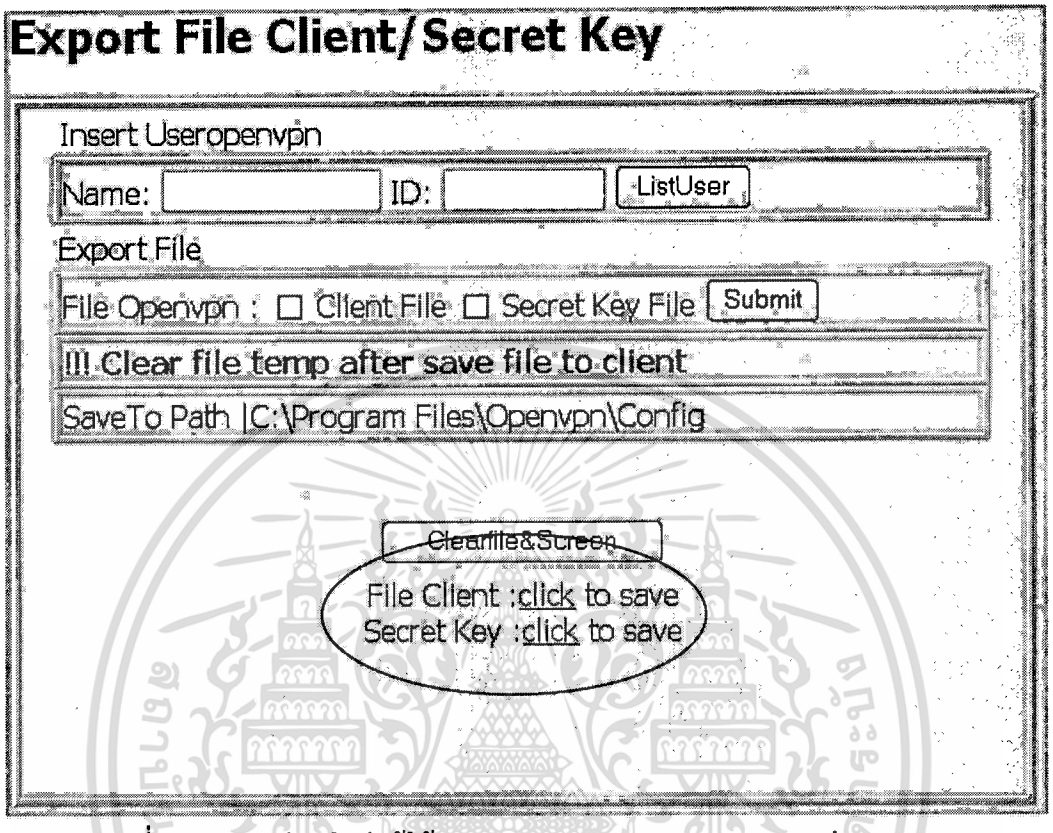
รูปที่ 4.20 แสดงส่วนติดต่อผู้ใช้ Normal Create File (Simple) โดยฟังก์ชั่นนี้เป็นส่วนต่อเนื่องจากการเลือก Normal Create File จากฟังก์ชั่น File Configure Management ซึ่งฟังก์ชั่น Normal Create File นี้จะใช้ในการสร้างไฟล์คอนฟิกโดยผู้ดูแลระบบซึ่งจะใช้พามิเตอร์ที่เป็น Default



รูปที่ 4.21 แสดงส่วนติดต่อผู้ใช้ ของ Advance Create File

รูปที่ 4.21 แสดงส่วนติดต่อผู้ใช้Advance Create File โดยฟังก์ชั่นนี้เป็นส่วนต่อเนื่องจากการเลือก Advance Create File จากฟังก์ชั่น File Configure Management เช่นเดียวกับ Normal File Configure ซึ่งฟังก์ชั่น Advance Create File นี้จะใช้ในการสร้างไฟล์คอนฟิกโดยผู้ดูแลระบบซึ่งสามารที่จะกำหนดค่าพามิเตอร์เองได้ซึ่งต่างจาก Normal Create File ที่จะใช้พารามิเตอร์เป็น Default แต่การสร้างไฟล์ของ Advance นั้นจะทำได้ทีละด้าน (Client File และ Server File) ในขณะที่ Normal Create นั้นจะสร้างไฟล์พร้อมกันทั้ง 2 ด้าน

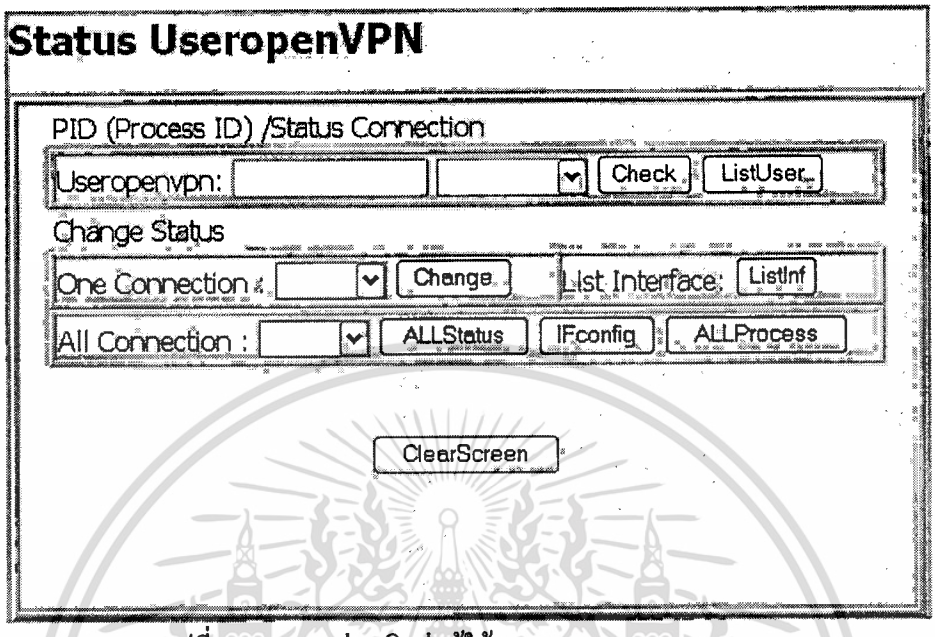
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.22 แสดงส่วนติดต่อผู้ใช้ ของ Export File Client /Secret Key ส่วน Admin

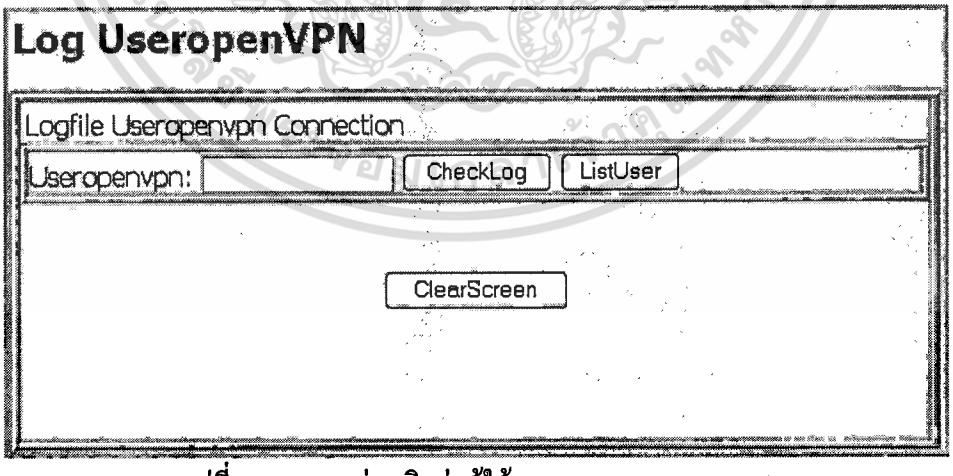
รูปที่ 4.22 แสดงส่วนติดต่อผู้ใช้ Export File Client /Secret Key ของ Admin โดยฟังก์ชั่นนี้จะใช้ในการ Download File ของไฟล์คีย์และไฟล์คอนฟิกของฝั่งไคลเอนต์ โดยลิงค์ (Link) ที่ระบบสร้างให้สำหรับ Download นั้นแสดงดังรูป 4.22 ในวงรี

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.23 แสดงส่วนติดต่อผู้ใช้ ของ Status UseropenVPN

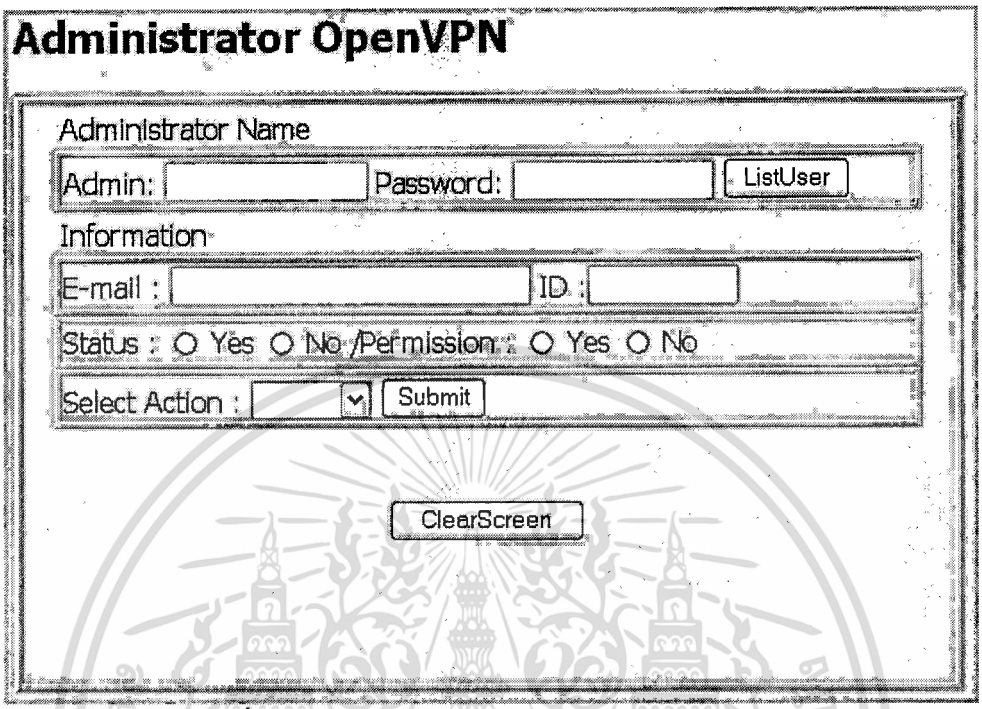
รูปที่ 4.23แสดงส่วนติดต่อผู้ใช้ Status UseropenVPN โดยฟังก์ชั่นนี้จะใช้ในการตรวจสถานะการให้บริการรวมไปถึงตรวจสอบการเชื่อมต่อของผู้ใช้ซึ่งฟังก์ชั่นนี้สามารถจะตรวจพร้อมกันทั้งหมดหรือทีละ 1 User นอกจากใช้ในการตรวจสอบสถานะและการเชื่อมต่อแล้วยังสามารถตรวจสอบข้อมูล Interface ได้เช่นกัน



รูปที่ 4.24 แสดงส่วนติดต่อผู้ใช้ ของ Log UseropenVPN

รูปที่ 4.24 แสดงส่วนติดต่อผู้ใช้ Log UseropenVPN โดยฟังก์ชั่นนี้จะใช้ในการตรวจสอบประวัติการใช้งานของผู้ใช้แต่ละคน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.25 แสดงส่วนติดต่อผู้ใช้ ของ Admin OpenVPN

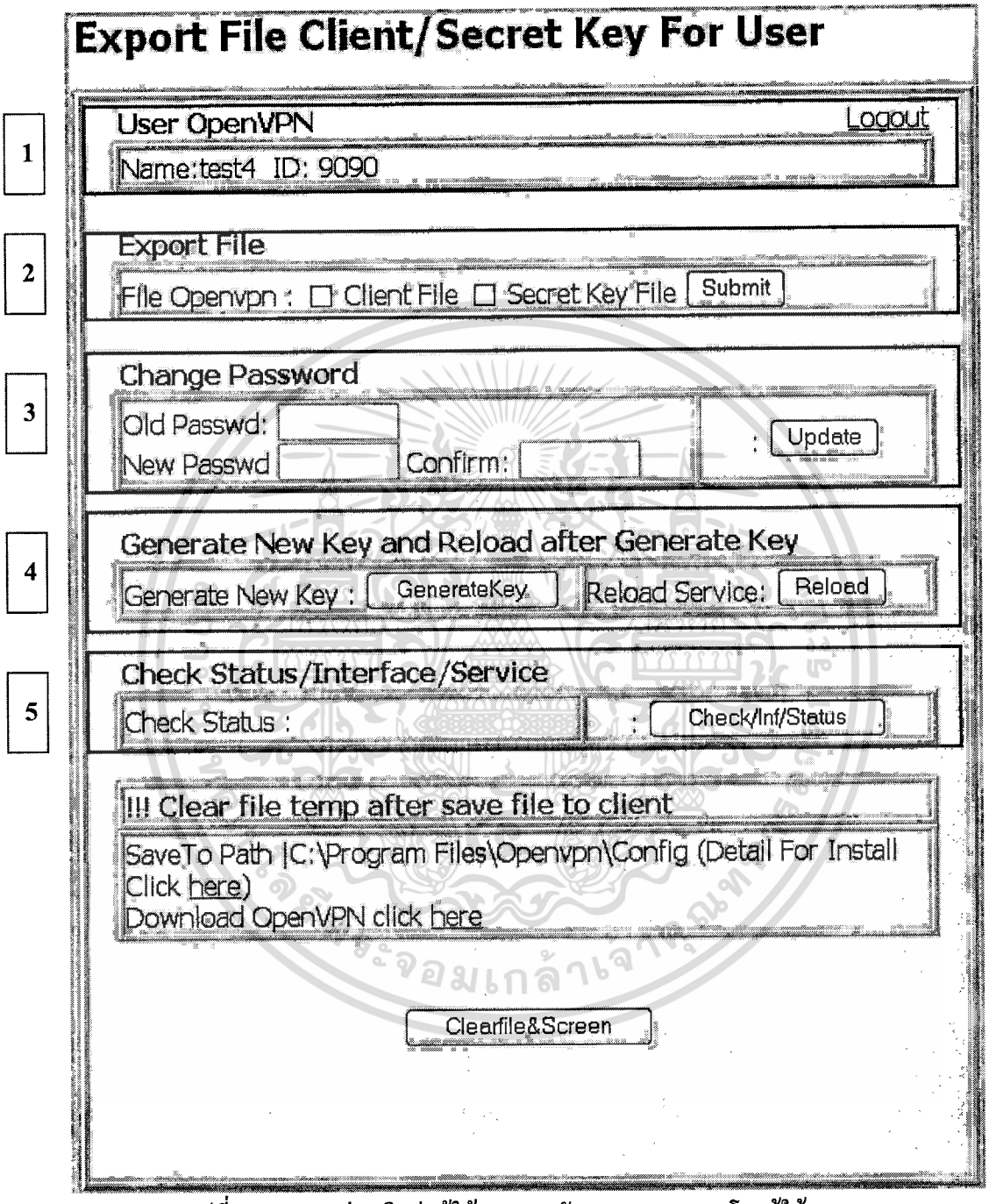
รูปที่ 4.25 แสดงส่วนติดต่อผู้ใช้ Admin OpenVPN โดยฟังก์ชั่นนี้จะใช้ในการจัดการเกี่ยวกับผู้ดูแลระบบเช่นการเพิ่ม, การลบ, แก้ไขข้อมูลตลอดจนการเปลี่ยนรหัสผ่านเป็นต้น

4.4.2.2 ส่วนติดต่อกับผู้ใช้ (User Interface) ในส่วนของผู้ใช้งานในระบบ (User)

เป็นส่วนที่ผู้ใช้งานสามารถเข้าไปใช้งานได้โดยผู้ใช้งานจะสามารถทำรายการได้ดังต่อไปนี้

1. Download ข้อมูลไฟล์คอนฟิกของผู้ใช้งานนั้นๆ
2. ตรวจสอบสถานการณ์เชื่อมต่อและการใช้บริการของผู้ใช้นั้นได้
3. เปลี่ยนรหัสผ่านเข้าระบบการจัดการเครือข่ายส่วนตัวเสมือน
4. เปลี่ยนคีย์ที่ใช้ในการเข้ารหัสข้อมูลได้พร้อมกับ Reload การให้บริการในส่วนของผู้ใช้นั้นได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.26 แสดงส่วนติดต่อผู้ใช้ ของการจัดการ OpenVPN โดยผู้ใช้ (User)

รูปที่ 4.26 แสดงส่วนติดต่อผู้ใช้ ของการจัดการ OpenVPN โดยผู้ใช้ โดยแบ่งเป็น 5 ส่วนตามหมายเลข 1-5

หมายเลขที่ 1 เป็นส่วนแสดงรายชื่อของผู้ใช้งาน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

หมายเลขที่ 2 เป็นส่วน Export File โดยสามารถเลือกได้ว่าจะ Export ข้อมูล คีย์ หรือไฟล์คอนฟิกได้

หมายเลขที่ 3 เป็นส่วนที่ใช้ในการเปลี่ยนรหัสผ่านของผู้ใช้งาน

หมายเลขที่ 4 เป็นส่วนเปลี่ยนคีย์ในการเข้ารหัสข้อมูลของผู้ใช้งานและเมื่อเปลี่ยนคีย์เสร็จจะต้องทำการ Reload ก่อนเพื่อให้ระบบนำคีย์ใหม่ไปใช้งาน

หมายเลขที่ 5 เป็นส่วนที่ใช้ตรวจสอบการให้บริการและสถานะการเชื่อมต่อของผู้ใช้งาน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

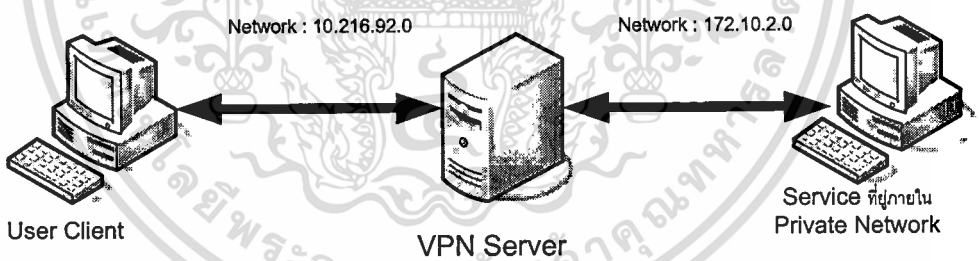
บทที่ 5

การสรุปผลการทำงานของระบบ

ในบทนี้จะกล่าวถึงการทดสอบโครงงานโดยจะกำหนดวิธีการทดสอบออกเป็นสถานการณ์รูปแบบต่างๆ เพื่อนำมาวิเคราะห์สรุปผลการทำงานของโครงงานต่อไป

5.1 การทดสอบโครงงาน

การทดสอบโครงงาน จะกระทำโดยให้ผู้ดูแลระบบทำการเพิ่ม ผู้ใช้ในระบบพร้อมกับสร้างไฟล์คอนฟิกขึ้นก่อนที่จะทำการสตาร์ทเซอร์วิสนี้พร้อมกับตรวจสอบสถานะการเชื่อมต่อและการให้บริการจากฝั่งเซิร์ฟเวอร์ นอกจากนี้ยังต้องตรวจสอบการเข้ารหัสข้อมูลว่าในกรณีที่ยังไม่ได้ใช้บริการผ่านเครือข่ายส่วนตัวเสมือนกับกรณีที่ได้ใช้บริการผ่านเครือข่ายส่วนตัวเสมือนนั้นว่ามีความแตกต่างกันหรือไม่โดยกำหนด Topology เป็นดังรูปที่ 5.1



รูปที่ 5.1 แสดง Topology ที่ใช้ในการทดสอบ

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

สถานการณ์กรณีที่ 1 (Admin)

- เพิ่มผู้ใช้ในระบบพร้อมกับสร้างไฟล์คอนฟิกของผู้ใช้รายนี้
- ทำการสตาร์ทเซอร์วิสของผู้ใช้ที่เพิ่มขึ้นใหม่นี้
- ตรวจสอบการให้บริการ

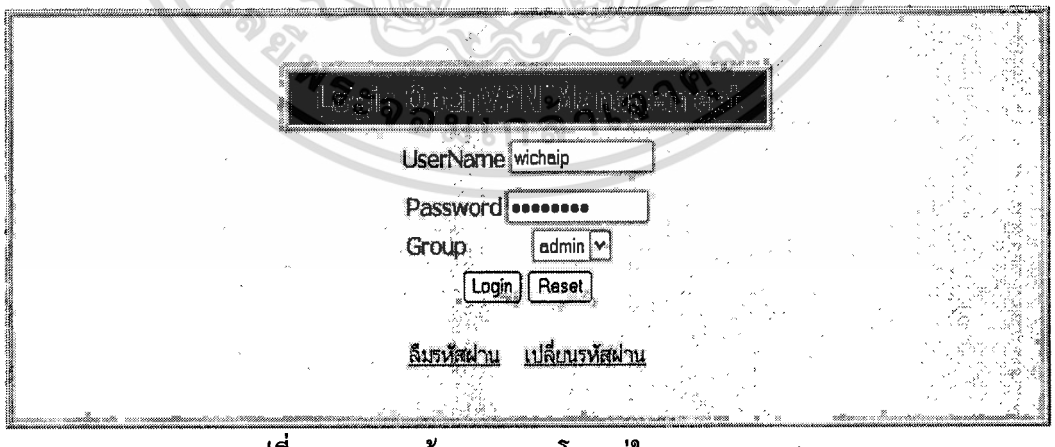
ขั้นตอนการทดสอบ

1. Login เข้าระบบใน Group Admin
2. เลือกฟังก์ชั่น Add User แล้วใส่รายละเอียดให้ครบ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3. เลือก Submit เพื่อให้ระบบทำการเพิ่มรายชื่อเข้าไปในระบบ
4. ระบบแจ้งผลกลับมาว่า "Add user Complete" ก่อนที่จะเลือก Generate Key เพื่อสร้างคีย์ที่ใช้ในการเข้ารหัส
5. ใส่รายชื่อลงไปก่อนที่จะเลือก Generate Key ซึ่งเมื่อระบบทำงานเสร็จก็จะแจ้งผลกลับมา
6. เมื่อเสร็จขั้นตอนที่ 5 แล้วจึงเลือกฟังก์ชั่น Create/Delete File เพื่อที่จะสร้างไฟล์คอนฟิกต่อไป
7. ใส่รายชื่อลงไปแล้วเลือกการ Create แบบ Normal แล้วเลือก Configure เพื่อทำรายการต่อไป
8. ใส่ค่าพามิเตอร์ลงไปในช่องพารามิเตอร์ให้ครบตามที่กำหนด
9. จากนั้นเลือกฟังก์ชั่น Status ก่อนที่จะใส่ค่ารายชื่อแล้วเลือก Start ที่อยู่ในส่วนของ One Connection แล้วเลือก Change เพื่อสตาร์ทเซอร์วิสของผู้ใช้นี้
10. ตรวจสอบสถานการณ์ให้บริการโดยใส่ค่ารายชื่อแล้วเลือก Process ID ก่อนที่จะเลือกฟังก์ชั่น Check ที่อยู่ในส่วนถัดมา ซึ่งระบบจะแสดงผลเป็นหมายเลข Process ID ออกมาให้นั่นแสดงว่าระบบได้ทำการสตาร์ทเซอร์วิสให้เรียบร้อยแล้ว

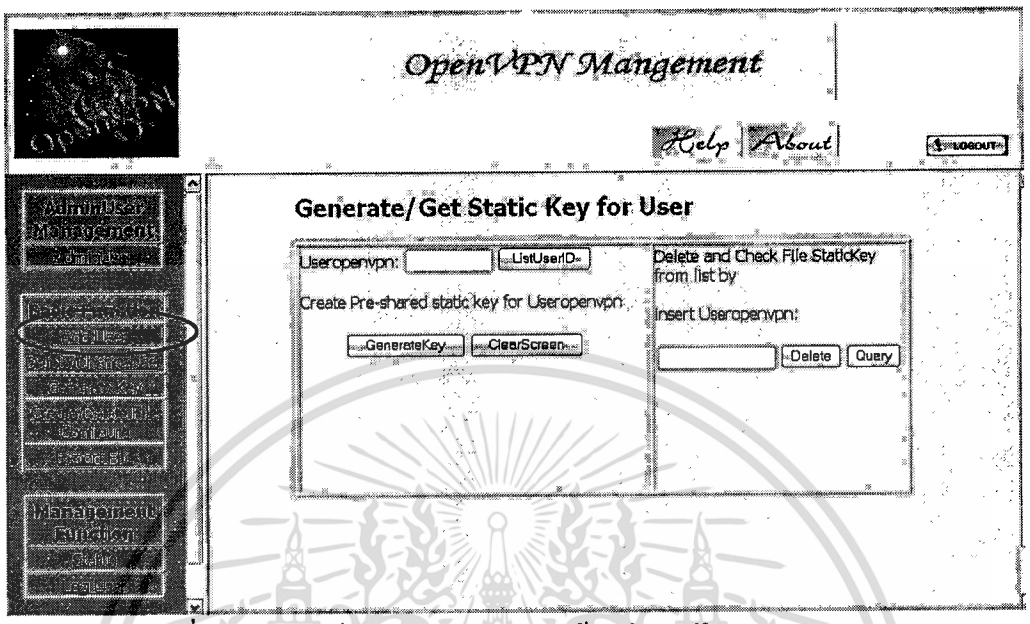
ภาพแสดงขั้นตอนการทดสอบกรณีที่ 1



รูปที่ 5.2 แสดงหน้าการ login โดยอยู่ใน Group Admin

รูปที่ 5.2 แสดงขั้นตอนการ Login ซึ่งอยู่ในขั้นตอนที่ 1

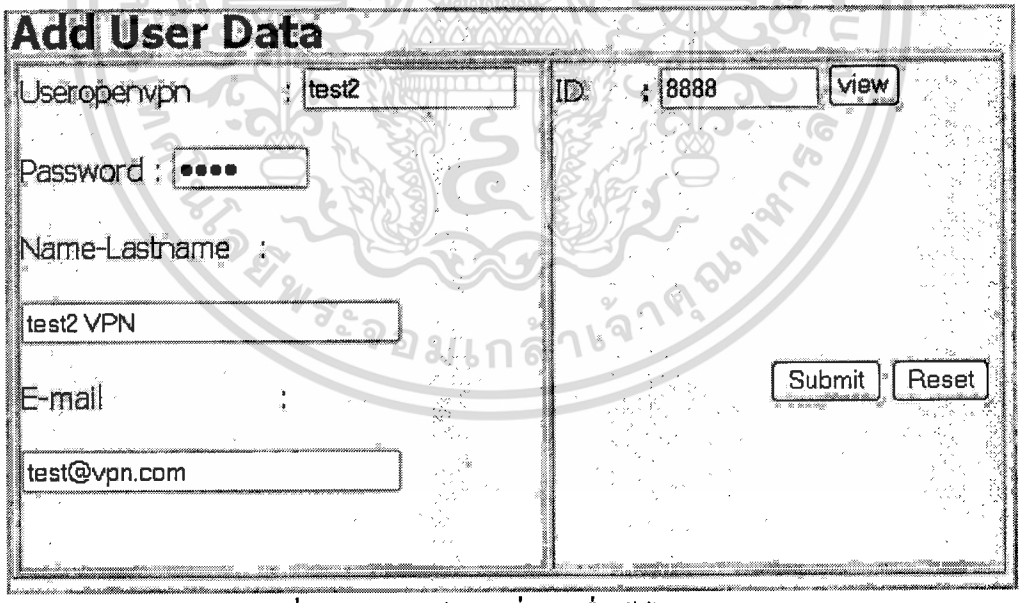
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



Add User

รูปที่ 5.3 แสดงหน้าแรกหลังจาก Login เข้ามาโดยอยู่ใน Group Admin

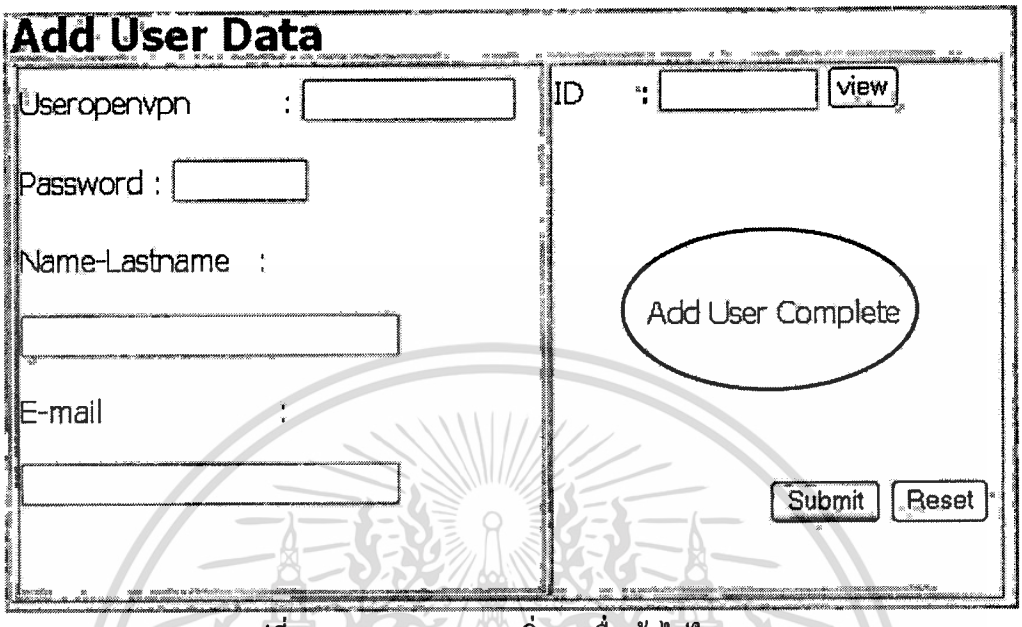
รูปที่ 5.3 แสดงหน้าแรกหลังจาก Login เข้ามาก่อนที่จะเลือก ฟังก์ชั่น “Add User”



รูปที่ 5.4 แสดงหน้าการเพิ่มรายชื่อเข้าไปในระบบ

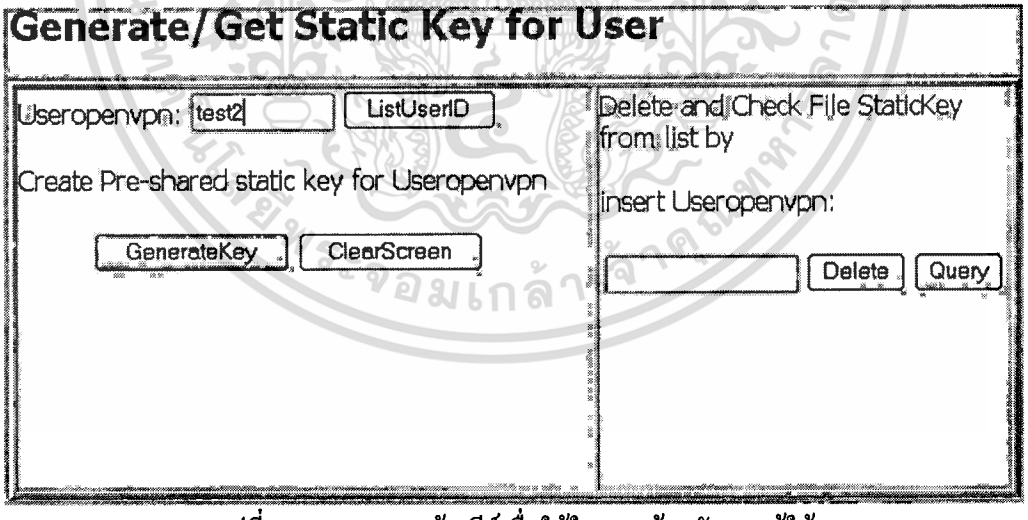
รูปที่ 5.4 แสดงหน้าการเพิ่มรายชื่อเข้าไปในระบบโดยในที่นี้ใช้ชื่อ “test 2” โดยเมื่อระบบทำการเพิ่มเรียบร้อยจะแสดงผลว่า “Add User Complete” ดังรูปที่ 5.5

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 5.5 แสดงผลจากการเพิ่มรายชื่อเข้าไปในระบบ

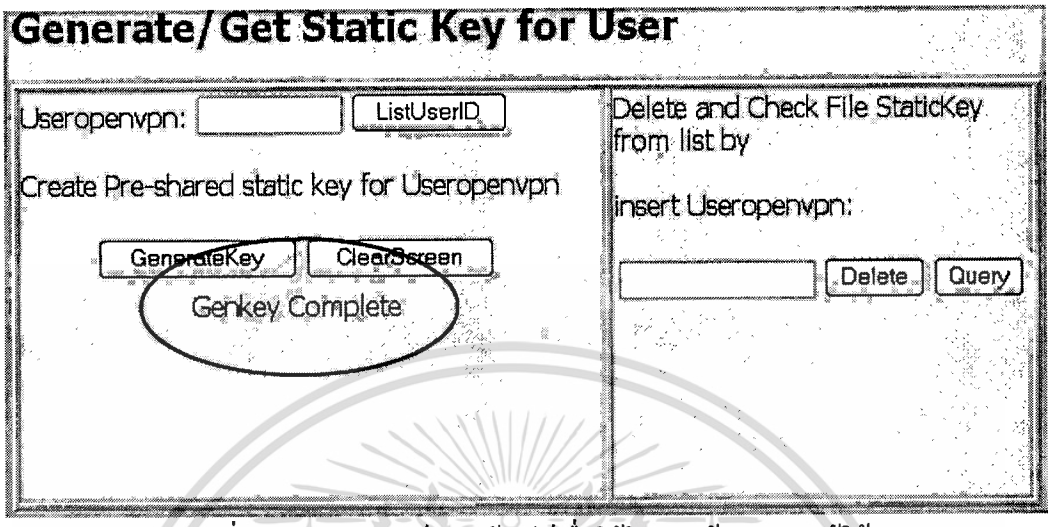
รูปที่ 5.5 แสดงผลจากการเพิ่มรายชื่อเข้าไปในระบบโดยจะส่งผลเป็นค่า "Add User Complete"



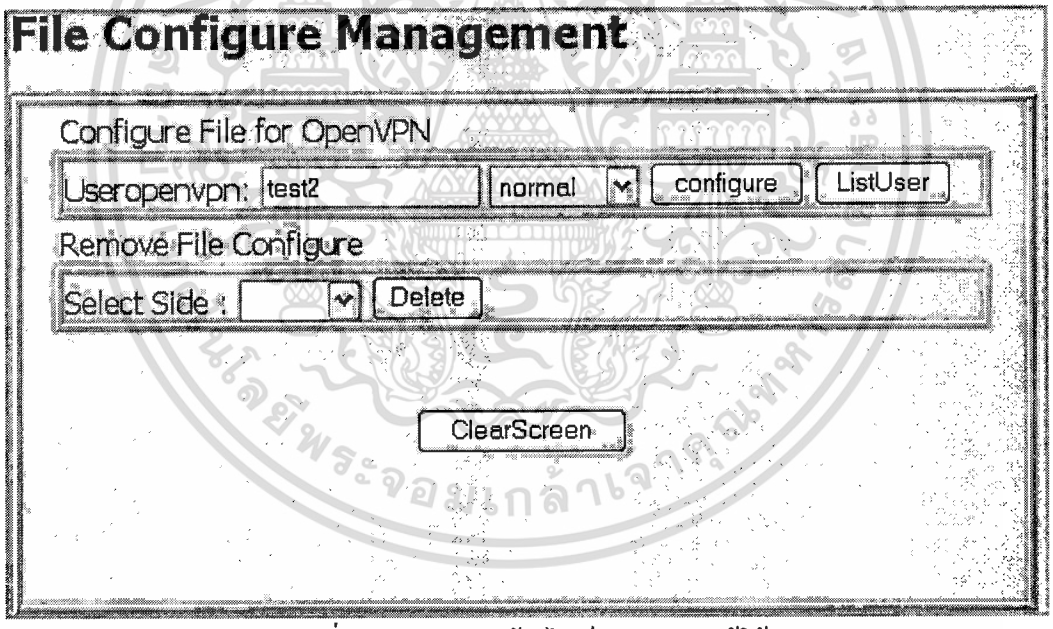
รูปที่ 5.6 แสดงการสร้างคีย์เพื่อใช้ในการเข้ารหัสของผู้ใช้

รูปที่ 5.6 แสดงการสร้างคีย์เพื่อใช้ในการเข้ารหัสของผู้ใช้ โดยในที่นี้คือ "test2" ซึ่งอยู่ในขั้นตอนที่ 5 และเมื่อระบบทำการสร้างคีย์ให้เสร็จเรียบร้อยจะแสดงผลเป็นข้อความ "Genkey Complete" ดังรูปที่ 5.7

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



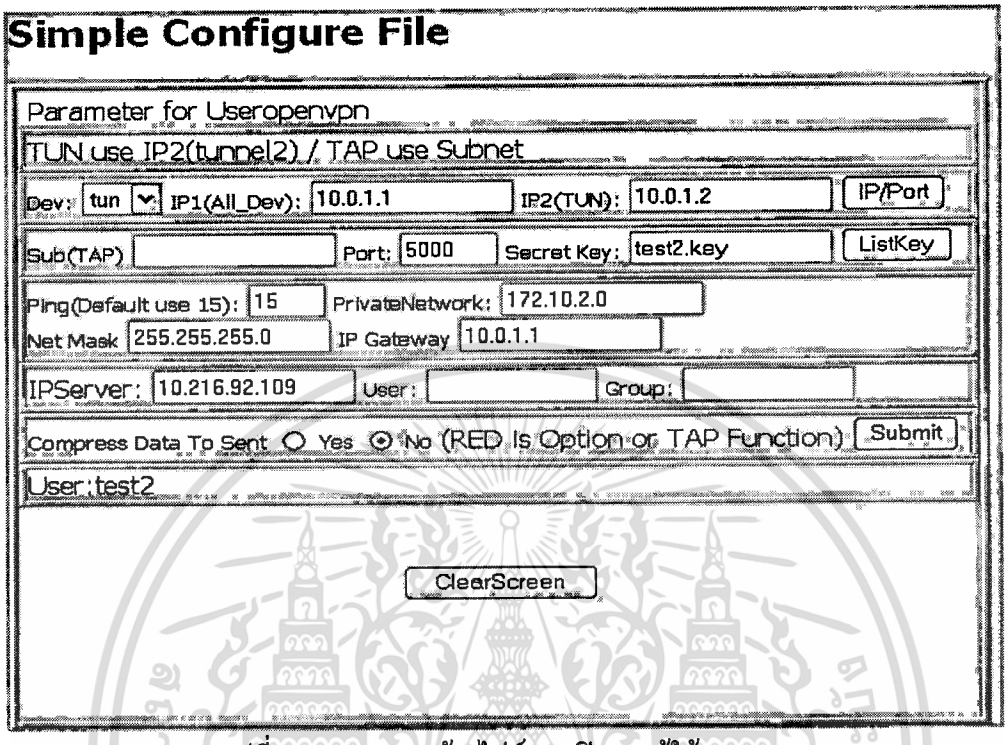
รูปที่ 5.7 แสดงผลลัพธ์การสร้างคีย์เพื่อใช้ในการเข้ารหัสของผู้ใช้



รูปที่ 5.8 แสดงการสร้างไฟล์คอนฟิกของผู้ใช้

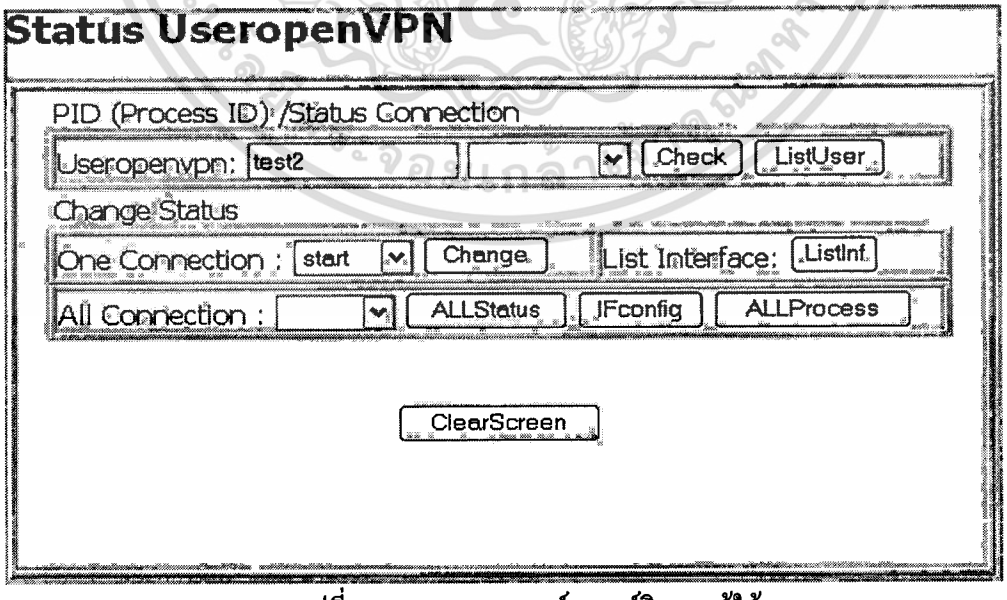
รูปที่ 5.8 แสดงการสร้างไฟล์คอนฟิกของผู้ใช้ซึ่งอยู่ในขั้นตอนที่ 6-7 โดยในการทดสอบนี้จะใช้การสร้างไฟล์คอนฟิกแบบ Normal

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 5.9 แสดงการสร้างไฟล์คอนฟิกของผู้ใช้แบบ Normal

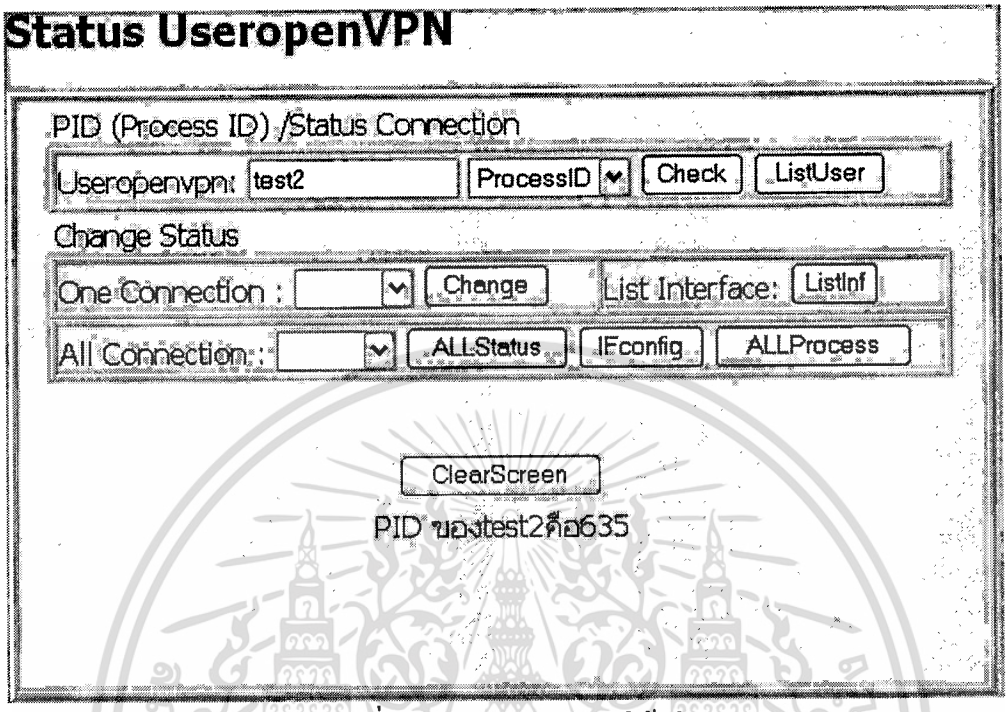
รูปที่ 5.9 แสดงการสร้างไฟล์คอนฟิกของผู้ใช้แบบ Normal โดยพารามิเตอร์ที่ใช้จะเป็นแบบ Default รูปนี้อยู่ในขั้นตอนที่ 8



รูปที่ 5.10 แสดงการสตาร์ทเซอร์วิสของผู้ใช้

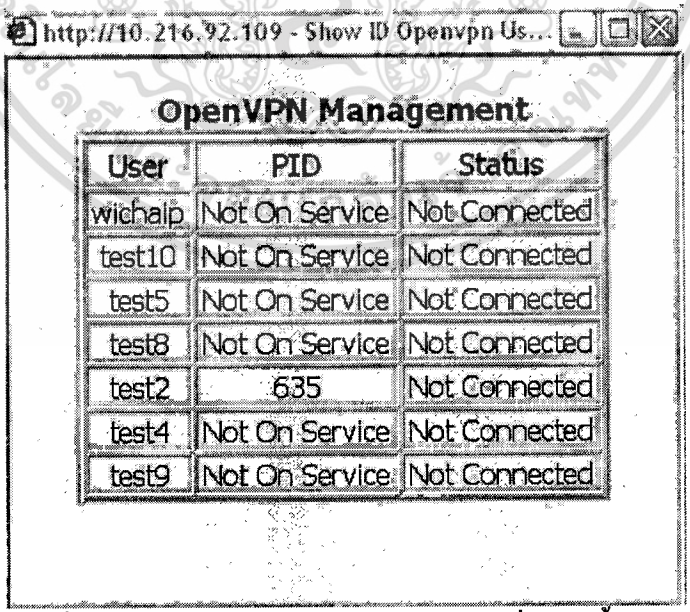
รูปที่ 5.10 แสดงการสตาร์ทเซอร์วิสของผู้ใช้ "test2" ขั้นตอนที่ 9

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 5.11 แสดงสถานะการให้บริการ

รูปที่ 5.11 แสดงสถานะการให้บริการ ของ User "test2" โดยแสดงเป็น Process ID แต่ถ้าต้องการตรวจสอบทั้งหมดให้เลือก "ALLProcess" ระบบจะทำการแสดงผลออกมาทุก User ดังรูปที่ 5.12



รูปที่ 5.12 แสดงสถานะการให้บริการและการเชื่อมต่อทั้งหมด

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

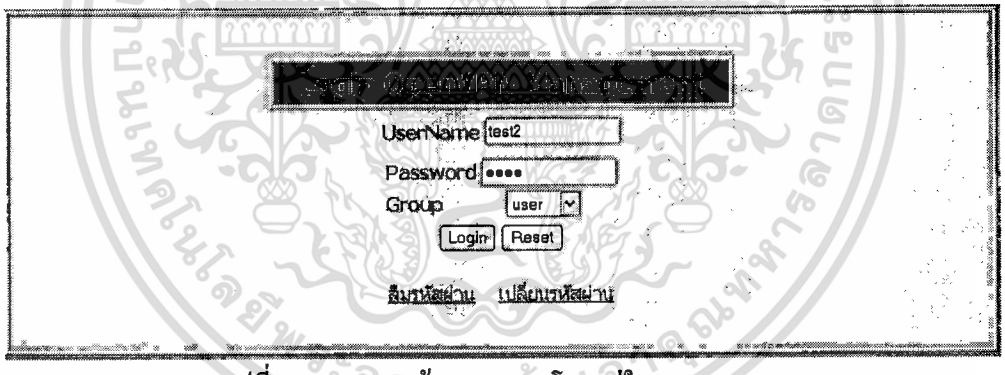
สถานการณ์กรณีที่ 2 (User)

- ผู้ใช้ในระบบต้องการสร้างการเชื่อมต่อเครือข่ายส่วนตัวเสมือนระหว่าง VPN เซิร์ฟเวอร์กับ ไคลเอนต์
- ผู้ใช้ต้องการตรวจสอบการให้บริการและสถานการณ์เชื่อมต่อ

ขั้นตอนการทดสอบ

1. เริ่มจากผู้ใช้ Login เข้าระบบใน Group User
2. ทำการ Export File ทั้ง Configure File และ Key File ไปไว้ใน Directory ที่ OpenVPN กำหนดบนฝั่งไคลเอนต์
3. จากนั้นก็ทำการรันโปรแกรม OpenVPN ฝั่งไคลเอนต์
4. เมื่อเสร็จก็สามารถตรวจสอบด้วยการเลือก Check/Inf/Status เพื่อตรวจสอบว่าได้เชื่อมต่อกับระบบแล้วหรือยัง

ภาพแสดงขั้นตอนการทดสอบกรณีที่ 2

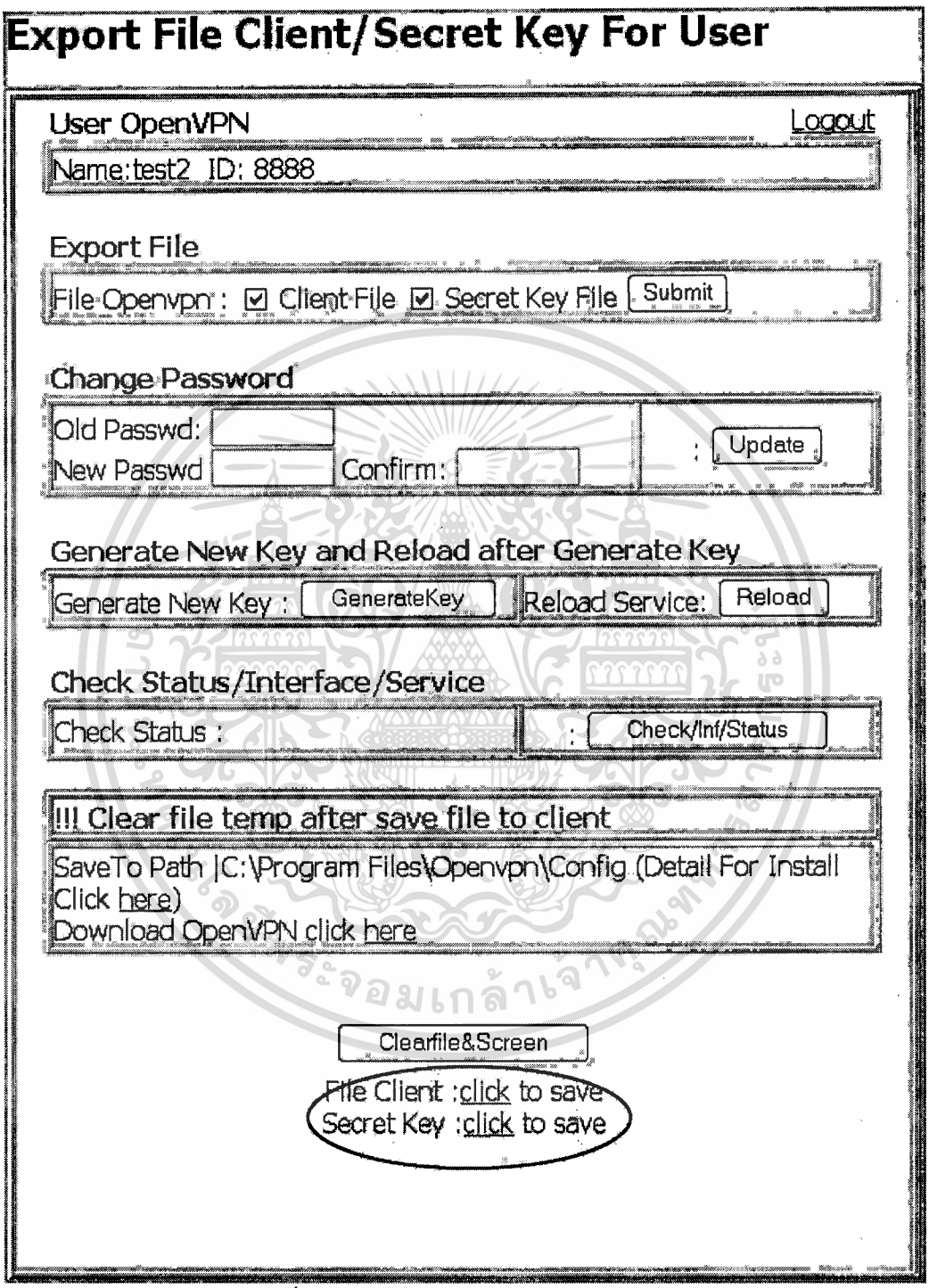


รูปที่ 5.13 แสดงหน้าการ login โดยอยู่ใน Group User

รูปที่ 5.13 แสดงหน้าการ Login เข้าไปใช้งานของ Group User ในที่นี้คือ ผู้ใช้ “test2”

ส่วนในรูปที่ 5.14 นั้นจะแสดงการ Export File ออกมาจากระบบซึ่งสามารถที่จะเลือก Export File ออกมาพร้อมกันทั้งไฟล์คอนฟิกและไฟล์คีย์ที่ใช้ในการเข้ารหัสข้อมูลก็ได้หรือจะ Export File ออกมาเพียงไฟล์ใดไฟล์หนึ่งก็ได้แต่ในการจะสร้างการเชื่อมต่อนั้นจะต้องประกอบด้วยทั้งสองไฟล์ โดยไฟล์คีย์นั้นสามารถที่จะเปลี่ยนหรือ Generate ค่าขึ้นมาใหม่ได้แต่เมื่อ Generate ขึ้นมาใหม่ก็ต้องทำการ Reload อีกครั้งเพื่อให้ระบบนำคีย์ใหม่ไปใช้งานทันที

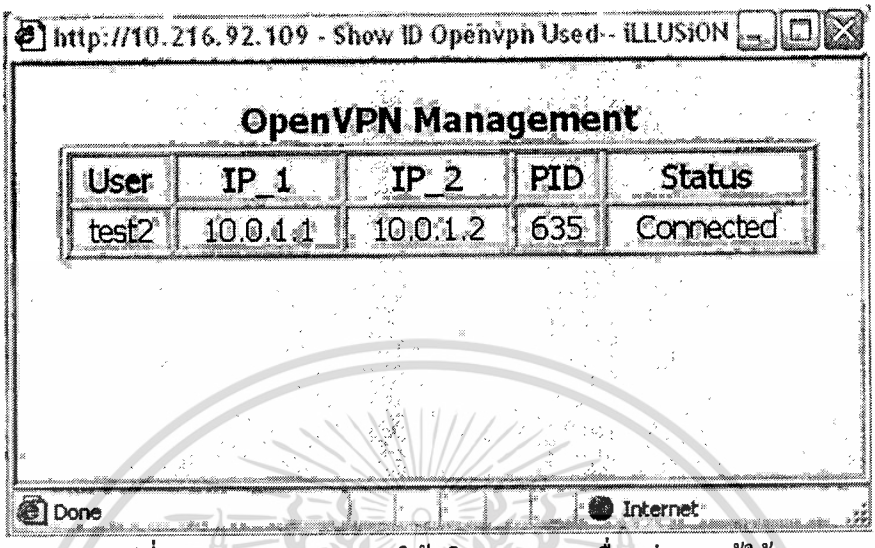
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 5.14 แสดงหน้าการ Export File ของผู้ใช้

รูปที่ 5.14 แสดงหน้าการ Export File ของผู้ใช้ โดยระบบจะสร้างลิงค์ (Link) ให้เพื่อใช้ในการ Export File ซึ่งในรูปนี้อยู่ขั้นตอนที่ 2

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

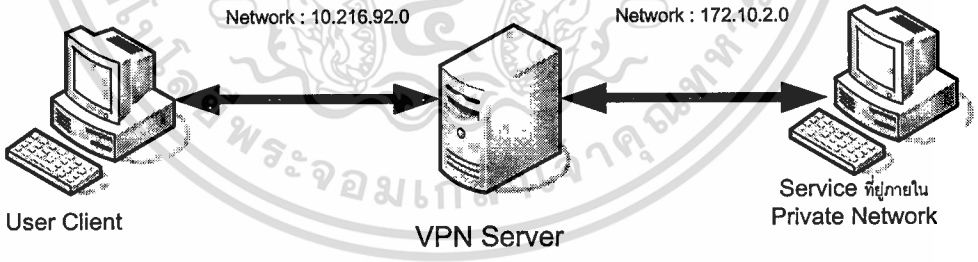


รูปที่ 5.15 แสดงสถานะการให้บริการและการเชื่อมต่อ ของผู้ใช้

รูปที่ 5.15 แสดงสถานะการให้บริการและการเชื่อมต่อ ของผู้ใช้โดยจะแจ้งเป็นค่า Process ID และ "Connected" ว่าได้เชื่อมต่อกับระบบแล้ว

การตรวจสอบการเข้ารหัสของข้อมูล

โดยแบ่งเป็น 2 กรณีคือในกรณีที่ไม่ใช้เครือข่ายส่วนตัวเสมือนและกรณีที่ใช้ผ่านเครือข่ายส่วนตัวเสมือนซึ่งเป็นการเข้าไปให้บริการที่อยู่ภายใน Private Network โดยบริการที่เข้าไปใช้นั้นคือ Telnet Service



ขั้นตอนการตรวจสอบ

1. ใช้โปรแกรม Telnet จากฝั่งผู้ใช้ที่อยู่บนเครือข่ายสาธารณะ (Public Network) ในที่นี้คือ Network ID: 10.216.92.0 ไปยังเซิร์ฟเวอร์ที่ ที่อยู่ในเครือข่ายภายใน (Private Network) ซึ่งในที่นี้คือ Network ID: 172.10.2.0
2. ใช้โปรแกรม Ethereal ตรวจจับ Packet Data เพื่อตรวจสอบว่ามีลักษณะข้อมูลอย่างไร
3. logout ออกจากเซอร์วิส (Service)
4. สร้างการเชื่อมต่อผ่านเครือข่ายส่วนตัวเสมือน (Virtual Private Network)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

5. ใช้โปรแกรม Telnet จากฝั่งผู้ใช้ที่อยู่บนเครือข่ายสาธารณะ (Public Network) ไปยังเซิร์ฟเวอร์ที่ ที่อยู่ในเครือข่ายภายใน (Private Network) ซึ่งครั้งนี้จะเป็นการเชื่อมต่อผ่าน Tunneling ของเครือข่ายส่วนตัวเสมือน(Virtual Private Network)
6. ใช้โปรแกรม Ethereal ตรวจจับ Packet Data เพื่อตรวจสอบลักษณะข้อมูลโดยเทียบกับข้อมูลที่ได้จากขั้นตอนที่ 2 ว่าแตกต่างหรือเหมือนกันอย่างไร

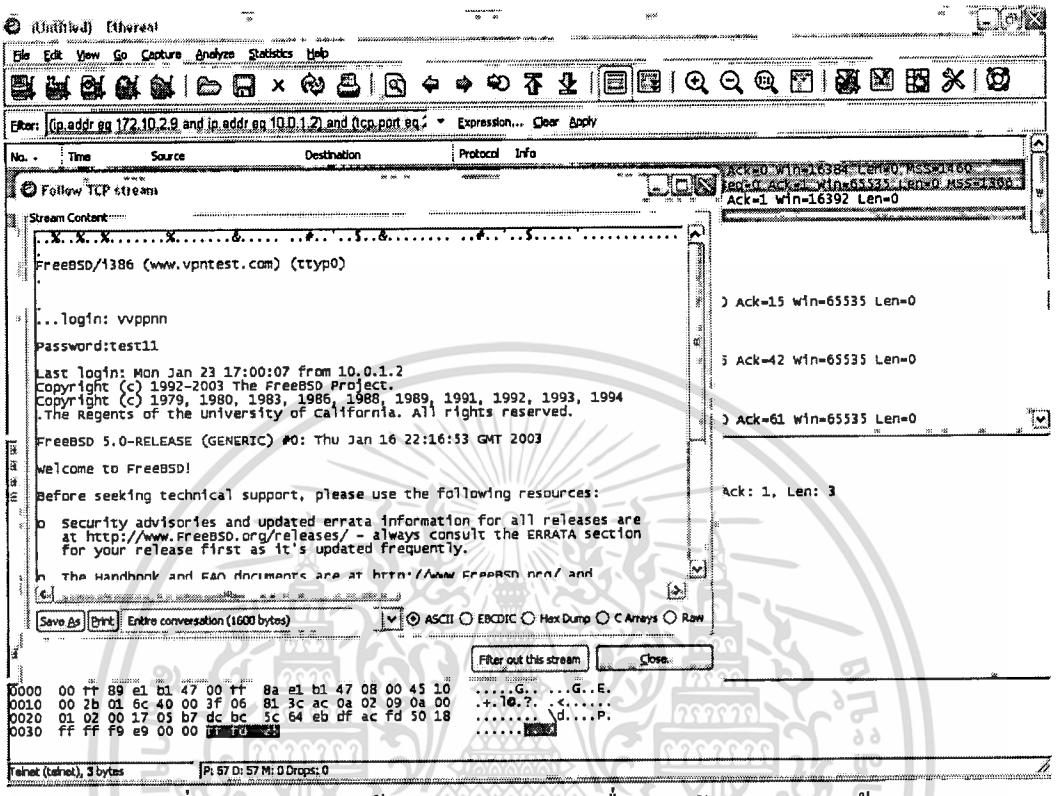
ภาพแสดงขั้นตอนการตรวจสอบการเข้ารหัส



รูปที่ 5.16 แสดงการใช้โปรแกรม Telnet เข้าไปใช้บริการ

รูปที่ 5.16 แสดงการใช้โปรแกรม Telnet เข้าไปหาเซิร์ฟเวอร์ที่ให้บริการ Telnet ในเครือข่ายภายใน (Private Network) โดยในรูปนี้อยู่ในขั้นตอนการทดสอบที่ 1

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 5.17 แสดงการใช้โปรแกรม Ethereal เพื่อตรวจจับ Packet ของข้อมูล

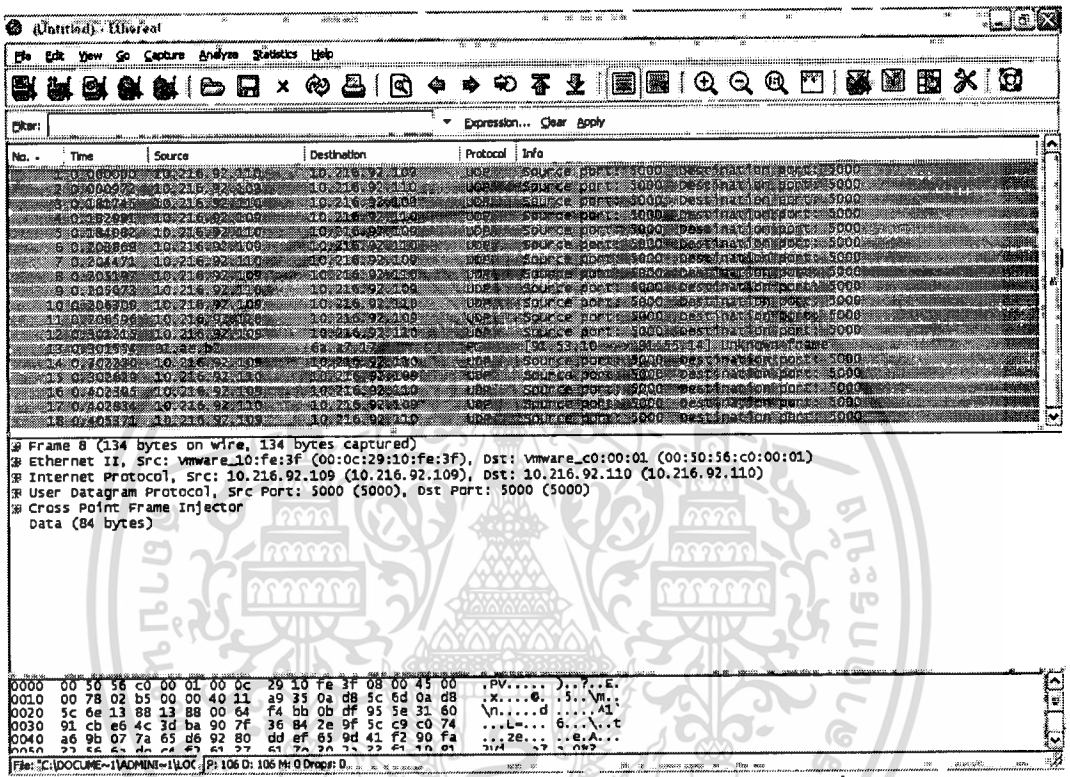
รูปที่ 5.17 แสดงการใช้โปรแกรม Ethereal เพื่อตรวจจับ Packet ของข้อมูลในกรณีที่ยังไม่ได้ส่งข้อมูลผ่าน Tunneling ของเครือข่ายส่วนตัวเสมือน โดยข้อมูลที่ตรวจพบสามารถทำการถอดรหัส (Decode) ออกมาได้ทำให้เห็นว่าข้อมูลที่ส่งนั้นมีค่าอะไรซึ่งจะไม่ปลอดภัย (รูปนี้แสดงขั้นตอนที่ 2)



รูปที่ 5.18 แสดงการใช้โปรแกรม Telnet เข้าไปใช้บริการผ่าน Tunneling

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

รูปที่ 5.18 แสดงการใช้โปรแกรม Telnet เข้าไปใช้บริการผ่าน Tunneling ซึ่งเป็นการส่งข้อมูลผ่านเครือข่ายส่วนตัวเสมือน (Virtual Private Network) (อยู่ในขั้นตอนที่ 5 หลังได้ผ่านขั้นตอนที่ 3-4)



รูปที่ 5.19 แสดงการใช้โปรแกรม Ethereal เพื่อตรวจจับ Packet ของข้อมูลที่ผ่าน Tunneling

รูปที่ 5.19 แสดงการใช้โปรแกรม Ethereal เพื่อตรวจจับ Packet ของข้อมูลที่ผ่านเครือข่ายส่วนตัวเสมือน (Virtual Private Network) ซึ่งผลที่ได้คือข้อมูลถูกเข้ารหัสแล้วส่งไปยังปลายทางด้วยโปรโตคอล UDP ดังนั้นโปรแกรม Ethereal นั้นไม่สามารถถอดรหัสเพื่อดูข้อความที่อยู่ภายในได้

5.2 ผลสรุปจากการทดสอบโครงงาน

จากตัวอย่างที่แสดงมาทั้งหมดนั้นแสดงให้เห็นถึงผลลัพธ์การทำงานของตัวโครงงานที่พัฒนาขึ้นนั้นสามารถเข้าไปจัดการตัวแอพลิเคชั่นที่ใช้ในการสร้างเครือข่ายส่วนตัวเสมือน (Virtual Private Network) โอเพ่นวีพีเอ็น (OpenVPN) โดยตัวโครงงานที่พัฒนาขึ้นนั้นจะทำการจัดการเพิ่มหรือลดจำนวนผู้ใช้ในระบบ, การติดตั้งค่าพารามิเตอร์ของผู้ใช้แต่ละคนและการตรวจสอบการให้บริการว่าได้ทำการสตาร์ทเซอร์วิส (Start Service) ของผู้ใช้แต่ละคนแล้วหรือไม่อีกทั้งรวมไปถึงการตรวจสอบสถานะเชื่อมต่อของผู้ใช้ในระบบด้วย นอกจากนี้ยังได้ทำการตรวจสอบการเข้ารหัสข้อมูลโดยใช้โปรแกรม Ethereal ว่ามีความแตกต่างระหว่างการส่งข้อมูลผ่านเครือข่ายส่วนตัว

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เสมือน (Virtual Private Network) กับการส่งข้อมูลโดยไม่ผ่านเครือข่ายส่วนตัวเสมือน (Virtual Private Network) หรือไม่ โดยผลที่ได้คือข้อมูลที่ส่งผ่านเครือข่ายส่วนตัวเสมือน (Virtual Private Network) นั้นจะไม่สามารถอ่านค่าได้ต่างจากข้อมูลที่ไม่ส่งผ่านเครือข่ายส่วนตัวเสมือน (Virtual Private Network) ซึ่งสามารถใช้โปรแกรม Ethereal ตรวจจับข้อมูลแล้วอ่านข้อความที่ตรวจจับได้ โดยข้อมูลที่ส่งผ่านเครือข่ายส่วนตัวเสมือนนั้นเป็นข้อความที่ถูกเข้ารหัส (Cipher Text)ไว้โดยใช้คีย์ (Key) ที่เรียกว่า คีย์ลับ (Secret Key) ของผู้ใช้แต่ละคน

5.3 ผลสรุปการพัฒนาโครงงาน

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) เพื่อให้บริการแก่ผู้ใช้ได้ทั้งแบบทีละคนหรือพร้อมกันทั้งหมดได้
- ผู้ดูแลสามารถตรวจสอบสถานะการให้บริการแก่ผู้ใช้ได้ทั้งแบบทีละคนหรือพร้อมกันทั้งหมดได้
- ผู้ดูแลสามารถสามารถหยุดเซอร์วิส (Stop Service) เพื่อหยุดให้บริการแก่ผู้ใช้ได้ทั้งแบบทีละคนหรือพร้อมกันทั้งหมดได้
- ผู้ดูแลสามารถตรวจสอบสถานะการเชื่อมต่อของผู้ใช้ว่าได้เชื่อมต่อเข้ากับระบบได้ทั้งแบบทีละคนหรือพร้อมกันทั้งหมดได้
- ผู้ดูแลสามารถ Export File ของผู้ใช้แต่ละคนได้
- ผู้ดูแลสามารถตรวจสอบประวัติการใช้งานของผู้ใช้แต่ละคนได้
- ผู้ใช้สามารถเปลี่ยนรหัสผ่านของตนเองได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- ผู้ใช้สามารถ Export File ของตนได้
- ผู้ใช้สามารถเปลี่ยนคีย์ (Key) ที่ใช้ในการเข้ารหัสข้อมูลได้ด้วยตนเอง
- ผู้ใช้สามารถตรวจสอบการให้บริการและสถานะการเชื่อมต่อของตนได้

จากการทดสอบโปรแกรมนี้พบว่าสามารถทำงานได้ตามฟังก์ชั่นที่ต้องการซึ่งเป็นความต้องการขั้นพื้นฐานในการจัดการเครือข่ายส่วนตัวเสมือน แต่อย่างไรก็ตามตัวโปรแกรมนี้สามารถนำไปพัฒนาต่อได้เพื่อให้ได้ระบบที่สมบูรณ์มากยิ่งขึ้นและเกิดประโยชน์ได้มากที่สุด

5.4 แนวทางการพัฒนาต่อ

การพัฒนาโปรแกรมจัดการเครือข่ายส่วนตัวเสมือนบนระบบปฏิบัติการ FreeBSD ผ่านทางเว็บ สามารถที่จะนำไปพัฒนาต่อเพื่อให้มีความสามารถมากขึ้นกว่าเดิมได้โดยการเพิ่มฟังก์ชั่นการทำงานให้สามารถสร้างการเชื่อมต่อที่ซับซ้อนมากขึ้นเช่น

1. เพิ่มฟังก์ชั่น VPN Gateway Pool กล่าวคือให้มีเซิร์ฟเวอร์ให้บริการเครือข่ายส่วนตัวเสมือนหลายตัวในลักษณะ Share Load
2. การทำงานในลักษณะ TLS คือ เป็นการควบคุมการเข้าใช้งานส่งผ่านข้อมูลโดยใช้คีย์ที่เป็นสาธารณะและส่วนตัวที่เรียกว่า Public Key และPrivate Key ซึ่งจะต้องมีเซิร์ฟเวอร์ตัวหนึ่งที่ทำหน้าที่จัดการ Certificate (โดยอาจจะเป็น Server เดียวกับ VPN Server ก็ได้) เพื่อใช้ในการแลกเปลี่ยนคีย์นั้นเอง
3. การเพิ่มพารามิเตอร์ลงไปในระบบงานที่ซับซ้อนเช่น พารามิเตอร์ที่เกี่ยวข้องกับการสร้าง Tunneling ผ่าน Proxy Server
4. 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

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ภาคผนวก

ก. ความต้องการของระบบ

1. ระบบปฏิบัติการ FreeBSD Version 5.0
2. Apache Web Server
3. PHP Version 4.4.0
4. Mysql 4.5
5. OpenVPN Version 2.05 และ OpenSSL

ข. การติดตั้งโปรแกรม

1. ระบบปฏิบัติการ FreeBSD นั้นสามารถศึกษาวิธีการได้จากเว็บไซต์ของ FreeBSD ได้ตามลิงค์นี้ http://www.freebsd.org/

2. การติดตั้ง Apache Web Server และ PHP นั้นสามารถทำได้ดังนี้

2.1 เริ่มจาก Download โปรแกรม Apache Web Server จากเว็บไซต์ตามลิงค์นี้ http://www.apache.org/ และ โปรแกรมจาก PHP จาก http://www.php.net/ มาเก็บไว้ที่ Directory /tmp

2.2 Unzip ไฟล์ apache และทำการติดตั้งโปรแกรม Apache Web Server ดังนี้

```
www#cd /tmp
www#gzip –cd apache_1.3.33.tar.gz|tar xvf –
www#cd apache_1.3.33
www#./configure
www#cd ..
```

2.3 Unzip ไฟล์ php และทำการติดตั้งโปรแกรม PHP ดังนี้

```
www#cd /tmp
www#gzip –cd php-4.4.0.tar.gz|tar xvf –
www#cd  php-4.4.0
www#./configure –with-mysql –with-apache=../apache_1.3.33
www#make
www#make install
```

2.4 กลับไปที่ Directory ของ Apahce

```
www#cd /tmp/apache_1.3.33
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

www#./configure –prefix=/usr/local/apache –active-module=src/modules

/php4/libphp4.a

www#make

www#make install

2.5 กลับไปที่ Directory ของ PHP อีกครั้งโดยใช้คำสั่งดังนี้

www#cd/tmp/php-4.4.0

www#cp php.ini-dist /usr/local/lib/php.ini

2.6 จากนั้นให้เพิ่มบรรทัด “AddType Application/x-httpd-php .php” ลงไปในไฟล์ httpd.conf ซึ่งอยู่ที่ /usr/local/apache/conf เป็นอันจบกระบวนการติดตั้ง Apache Web Server และ PHP

3. การติดตั้ง MySQL Database

3.1 เริ่มจาก Download โปรแกรม MySQL จากเว็บไซต์ตามลิงค์นี้ http://www.mysql.com/ มาเก็บไว้ที่ Directory /tmp

3.2 Unzip ไฟล์ MySQL และทำการติดตั้งโปรแกรม MySQL ดังนี้

www#cd /tmp

www#gzip –cd mysql-3.23.56.tar.gz|tar xvf –

www#cd mysql-3.23.56

www#./configure

www#make

www#make install

4. การติดตั้ง OpenVPN 2.0.5 โดยก่อนทำการติดตั้งต้องทำการติดตั้ง OpenSSL ก่อน

4.1 เริ่มจาก Download โปรแกรม OpenSSL จาก http://www.openssl.org/ มาเก็บไว้ที่ Directory /tmp

4.2 Unzip ไฟล์ OpenSSL และทำการติดตั้งโปรแกรม OpenSSL ดังนี้

www#gzip –cd openssl-0.9.7d.tar.gz | tar xvf –

www#cd openssl-0.9.7d

www#./config

www# make

www#make install

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4.3 ซึ่งเมื่อติดตั้ง OpenSSL เสร็จก็จะทำการติดตั้ง OpenVPN โดยหลังจาก Download โปรแกรม OpenVPN จากเว็บไซต์ตามลิงค์นี้http://www.openvpn.net/ มาเก็บไว้ที่ Directory /tmp เสร็จก็จะทำการ Unzip ไฟล์ OpenVPN และทำการติดตั้งโปรแกรม OpenVPN ดังขั้นตอนนี้

```
www# gzip –cd openvpn-2.0.5.tar.gz | tar xvf –
www# cd openvpn-2.0.5
www# ./configure
www# make
www# make install
```

5. หลังการติดตั้งโปรแกรมต่างๆเสร็จจึงสามารถติดตั้งตัวโครงงานให้สามารถทำงานได้

ค. การติดตั้งโครงงาน

ตัวไฟล์ของโครงงานแบ่งเป็นสองส่วนหลักๆคือ

1. ส่วนที่เป็นภาษา PHP
2. ส่วนที่เป็น Shell Script

โดยส่วนที่เป็นภาษา PHP นั้นจะติดตั้งไว้ที่ Directory /usr/local/apache/htdocs/openvpn ส่วนไฟล์ที่เป็น Shell Script นั้นจะติดตั้งไว้ที่ Directory /etc/openvpn/shell หลังการติดตั้งไฟล์เหล่านี้แล้วให้ทำการสร้าง Directory เหล่านี้ขึ้นเพื่อรองรับการทำงานของโปรแกรม ดังนี้

/etc/openvpn/subsys

/etc/openvpn/status

/etc/openvpn/log

/etc/openvpn/key

/etc/openvpn/client

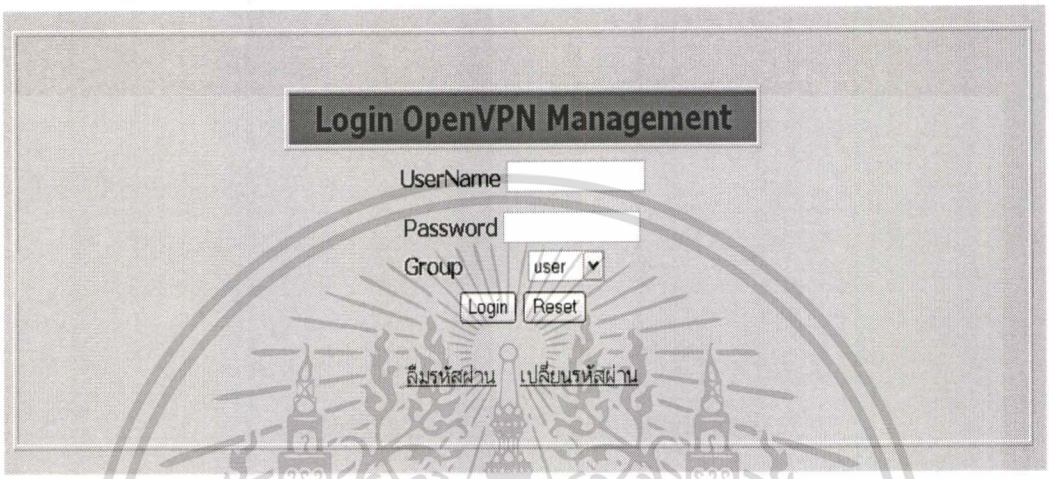
เมื่อต้องการเรียกใช้การทำงานนั้นให้เรียกไปที่

http://ip serverที่ให้บริการ/openvpn/form_login.php

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

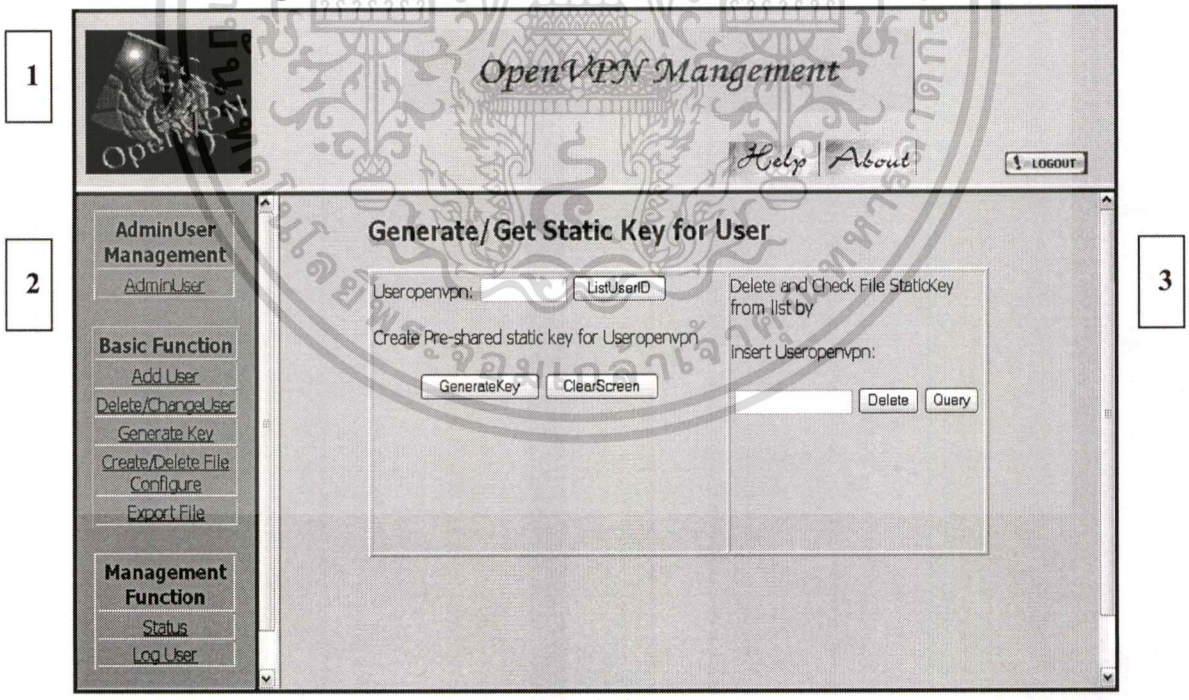
ง. การใช้งานโปรแกรม

1. หน้า Login ประกอบด้วยช่องอินพุท UserName, Password และ Group โดยจะแบ่งเป็น Admin กับ User



แสดงส่วนติดต่อผู้ใช้ Login

2. หน้าหลังการ Login ของ Admin (Main)



แสดงส่วนติดต่อผู้ใช้ Main (Admin)

Main ประกอบด้วย 3 ส่วนหลักๆคือโดยจะแบ่งเป็น

1. ส่วนเมนเมนู (Main Menu) หมายเลขที่ 1 ส่วนเรียกอ่านคู่มือ, ข้อมูลโครงงานและ Logout

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

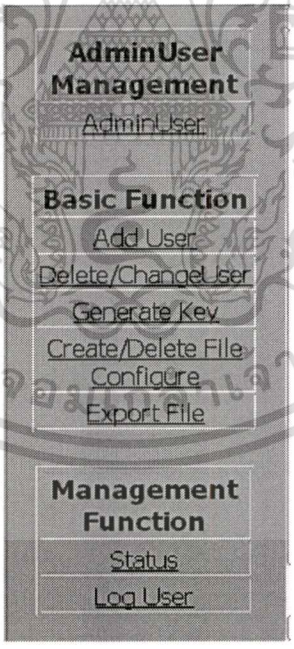
2. ส่วนรายการฟังก์ชั่น (List Function Menu) หมายเลขที่ 2 เป็นส่วนที่รวมฟังก์ชั่นที่มีในระบบ
3. ส่วนเมนหลัก (Main) หมายเลขที่ 3 เป็นส่วนที่ใช้ในการทำรายการต่างๆ

2.1 ส่วนเมนเมนู (Main Menu) ใช้ในการเรียกอ่านคู่มือ, ข้อมูลโครงงานและ Logout



Main Menu

2.2 ส่วนรายการฟังก์ชั่น (List Function Menu) ใช้ในการรวมฟังก์ชั่นที่มีในระบบของโครงงาน



List Function

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.3ส่วนเมนหลัก (Main) เป็น Area ที่ใช้สำหรับจัดการระบบเครือข่ายส่วนตัวเสมือนตามฟังก์ชั่นของโครงงานที่พัฒนาขึ้น

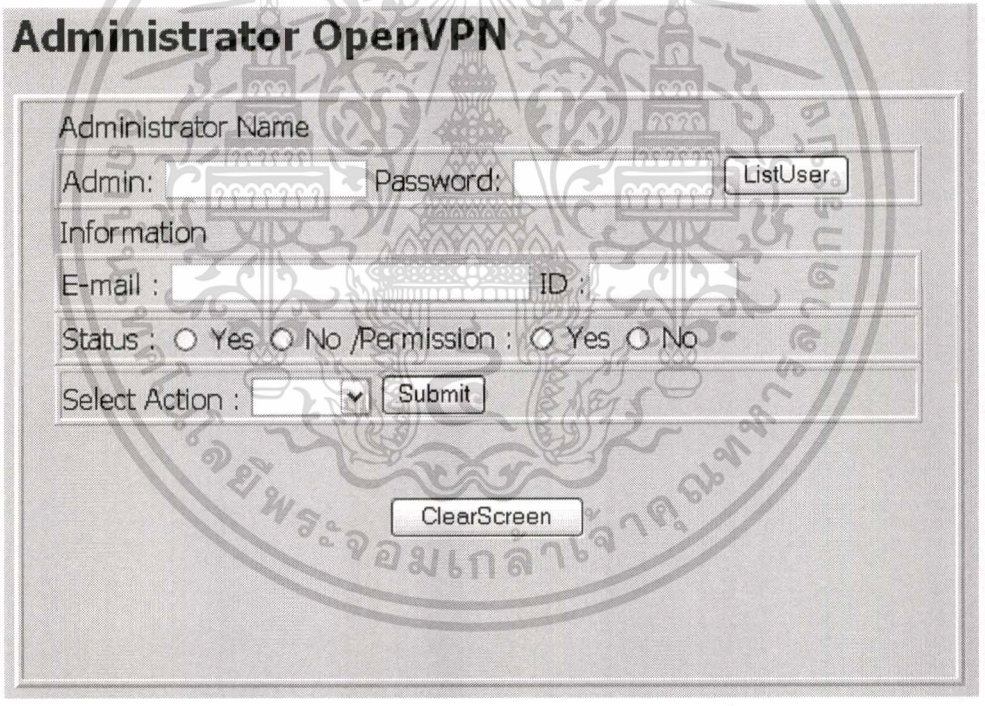
3.ฟังก์ชั่นการทำงานต่างใน List Function นั้นมี 3 ส่วนคือ

3.1 AdminUser Management ใช้ในการจัดการรายชื่อผู้ดูแลระบบ

3.2 Basic Function

3.3 Management Function

3.1 AdminUser Management ประกอบด้วยฟังก์ชันเดียวคือ AdminUser ใช้ในการจัดการเกี่ยวกับผู้ดูแลระบบเช่นการเพิ่ม, การลบ, แก้ไขข้อมูลตลอดจนการเปลี่ยนรหัสผ่านเป็นต้น



Function AdminUser

3.2 Basic Function ประกอบด้วยฟังก์ชัน

-Add User

-Delete/Change User

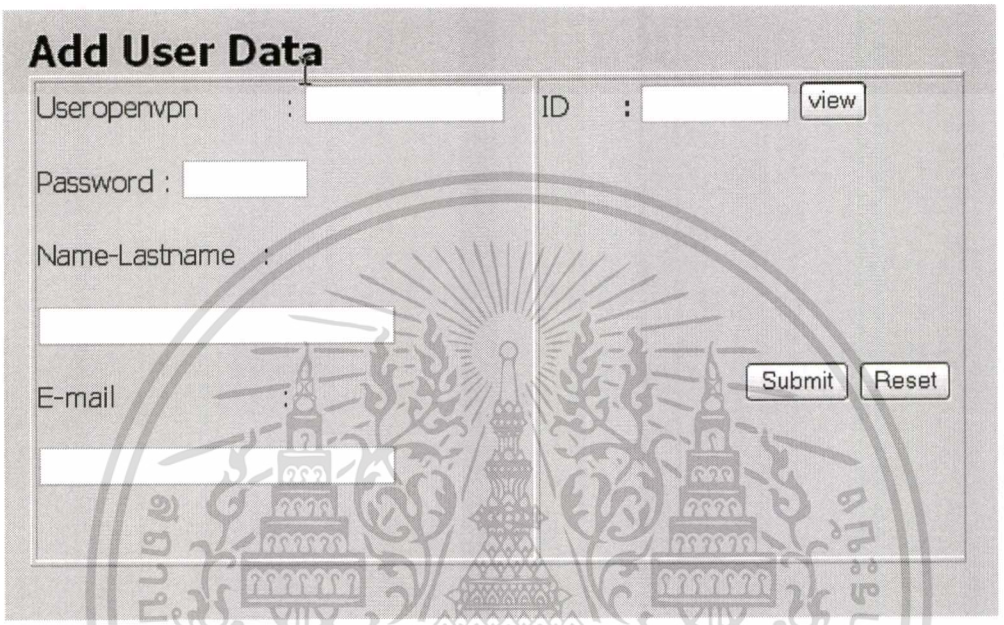
-Generate Key

-Create / Delete File Configure

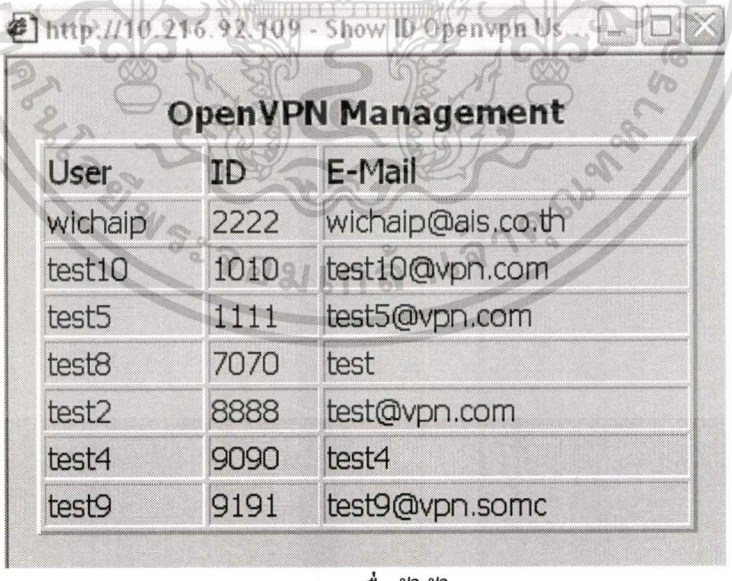
-Export File

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Add User ใช้ในการเพิ่มผู้ใช้ในระบบโดยเริ่มจากการใส่ชื่อ Useropenvpn ซึ่งห้ามซ้ำและสามารถตรวจสอบก่อนโดยใช้ “View” โดย View จะแสดงรายชื่อที่มีอยู่ในระบบทั้งหมดและเมื่อใส่ค่าครบทั้งหมดแล้วก็ให้เลือก “Submit” เพื่อเพิ่มรายชื่อในระบบ



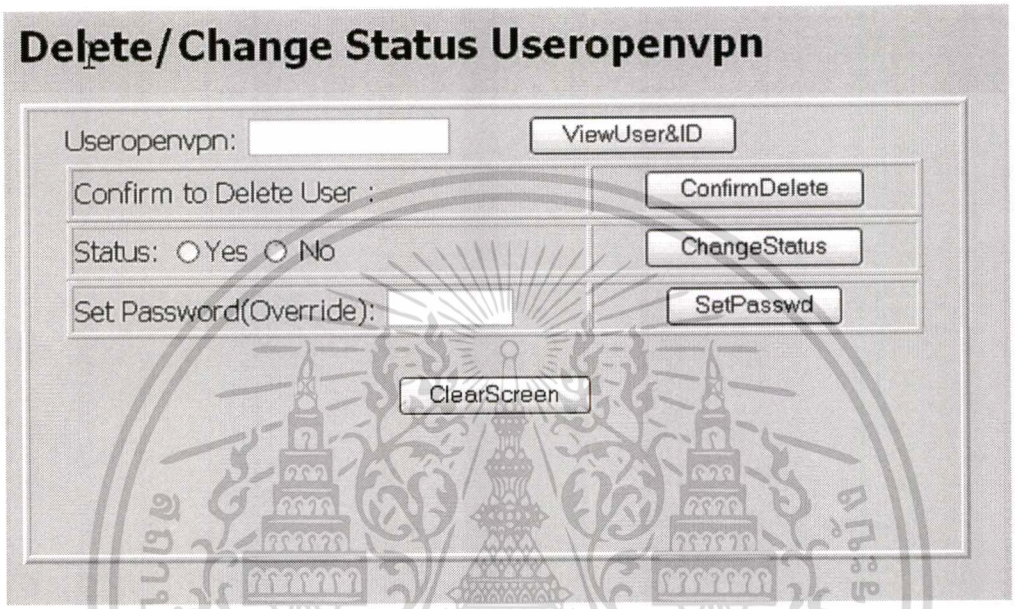
Add User



View แสดงรายชื่อผู้ใช้ในระบบ

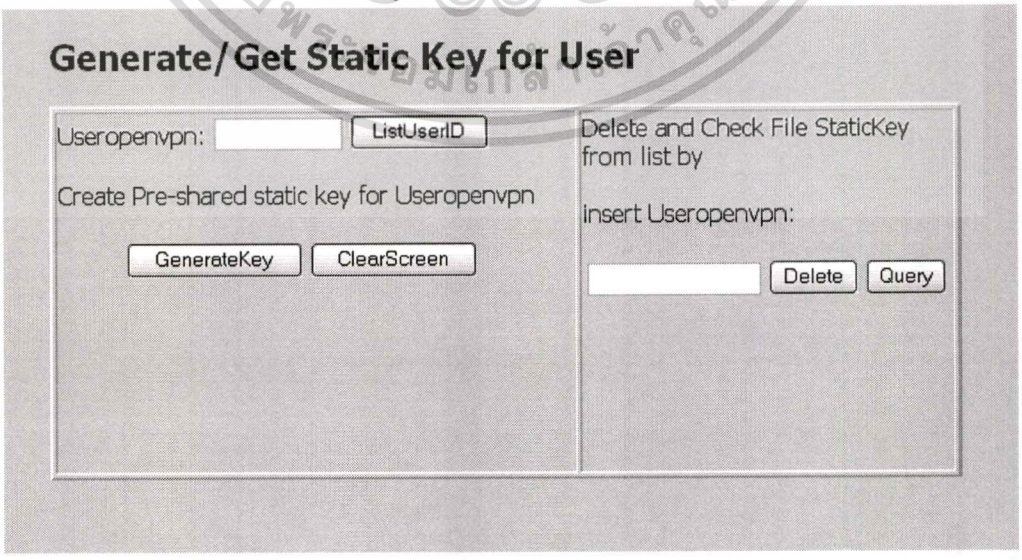
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Delete/Change User ใช้ Delete User, เปลี่ยนสถานะการใช้งานตลอดจนการตั้งรหัสผ่านของผู้ใช้โดยผู้ดูแลระบบ



Delete/Change Status User

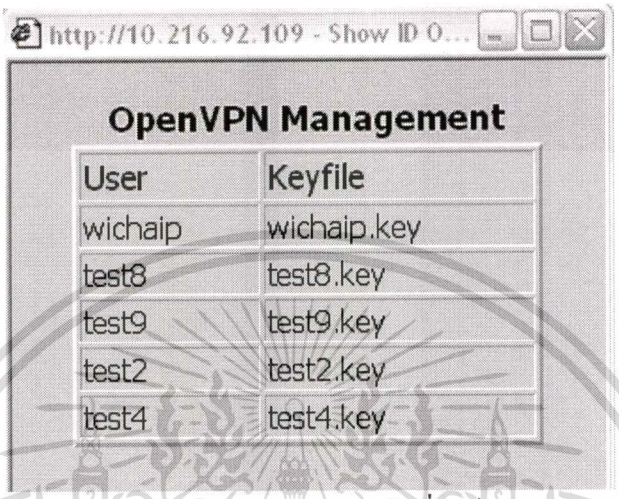
Generate Key ใช้ในการสร้างคีย์ของแต่ละผู้ใช้ในระบบโดยแบ่งเป็นส่วนที่ใช้ในการสร้างคีย์กับส่วนที่ใช้ในการลบคีย์ของแต่ละคนโดยจะสามารถสร้างคีย์ได้ก็ต่อเมื่อมีรายชื่อผู้ใช้ในระบบมิฉะนั้นจะไม่สามารถสร้างคีย์สำหรับผู้ใช้รายนั้นได้ โดยเราจะสามารถตรวจสอบว่าผู้ใช้รายนี้มี



Generate Key

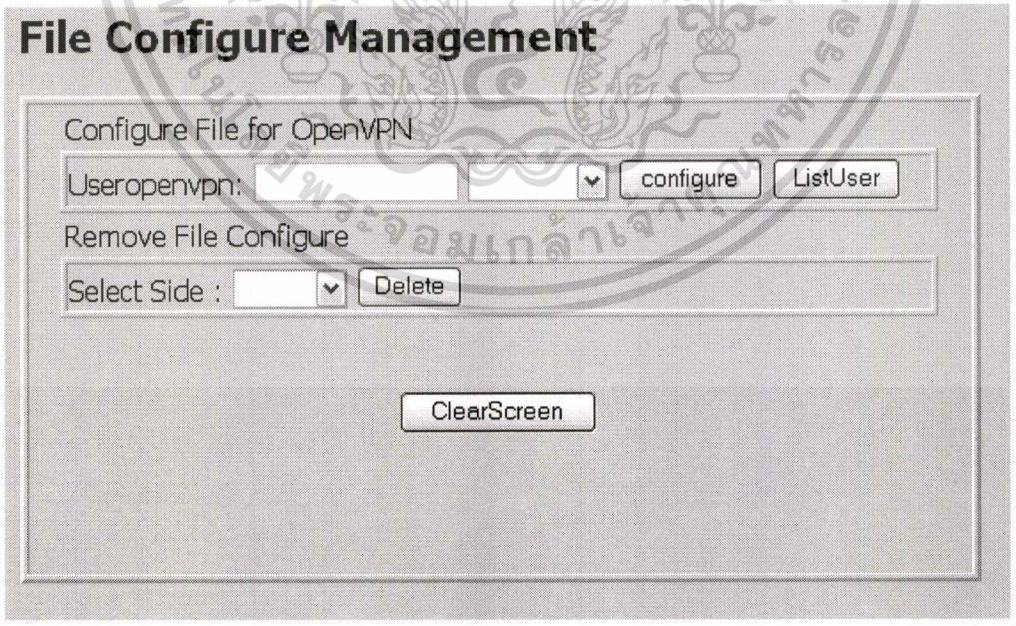
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

คีย์ในระบบหรือไม่สามารถตรวจสอบจาก “Query” ซึ่งจะแสดงผลออกมาดังรูป



ผลจาก “Query” แสดงรายชื่อคีย์

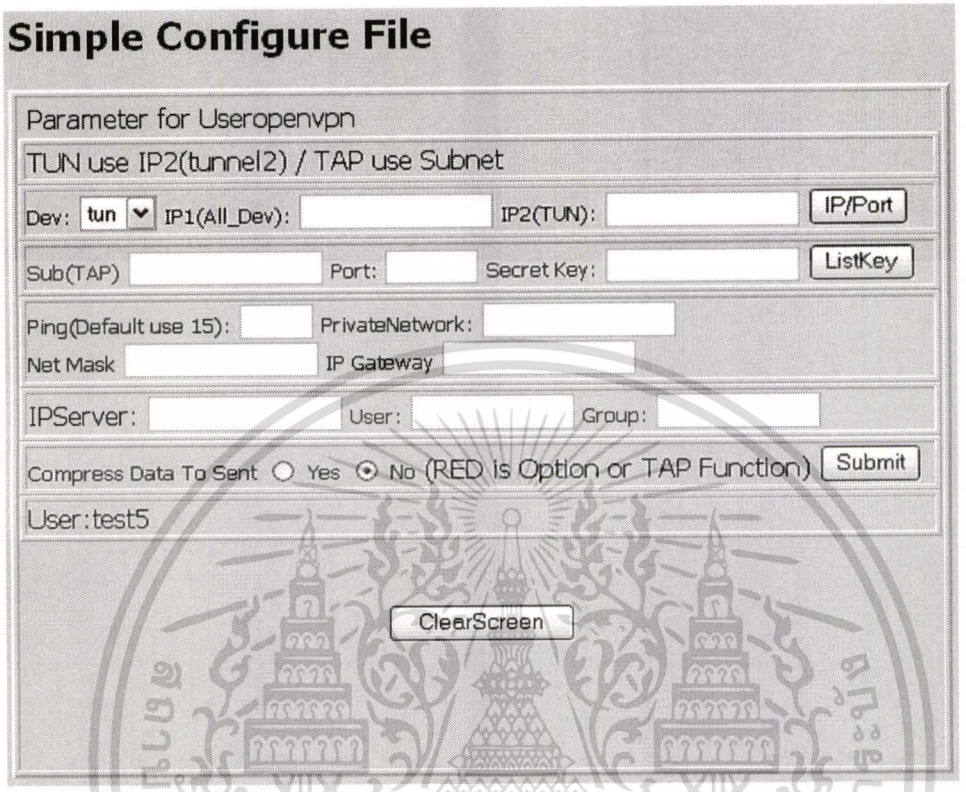
Create / Delete File Configure ใช้ในการสร้างหรือลบไฟล์คอนฟิกโดยผู้ดูแลระบบซึ่งการสร้างไฟล์คอนฟิกสามารถทำได้ 2 รูปแบบคือ Normal และ Advance



File Configure Management

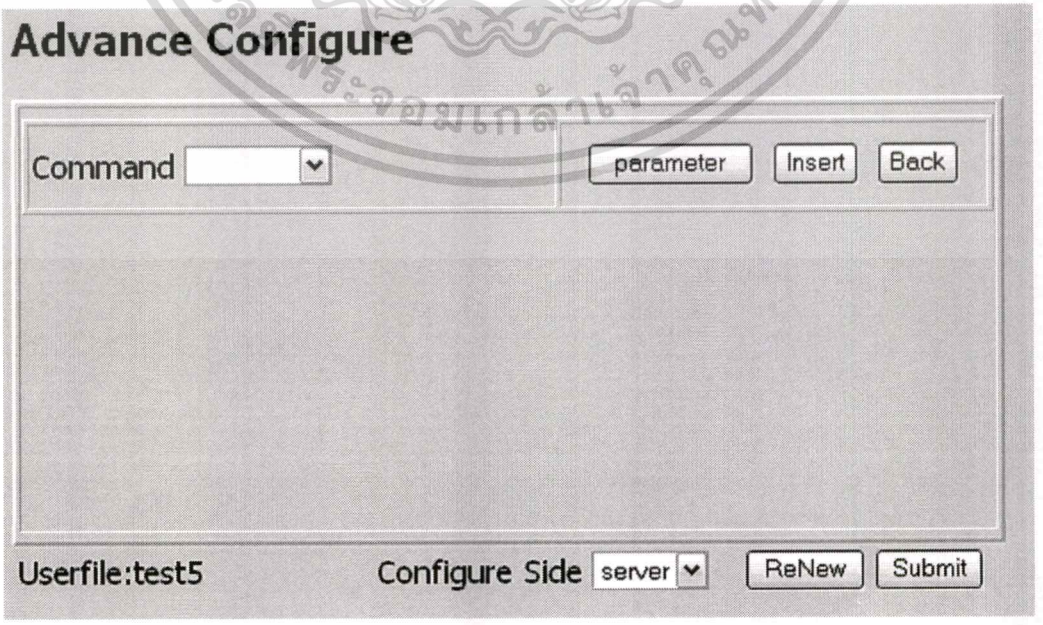
และเมื่อทำการเลือกลักษณะรูปแบบการ Configure แล้วให้เลือก “Configure” ระบบจะเปลี่ยนเข้าสู่รูปแบบที่ได้ทำการเลือกไว้ (Normal หรือ Advance)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



Normal Create File (Simple)

Normal Create File นี้จะใช้ในการสร้างไฟล์คอนฟิกโดยผู้ดูแลระบบซึ่งจะใช้พามิเตอร์ที่เป็น Default

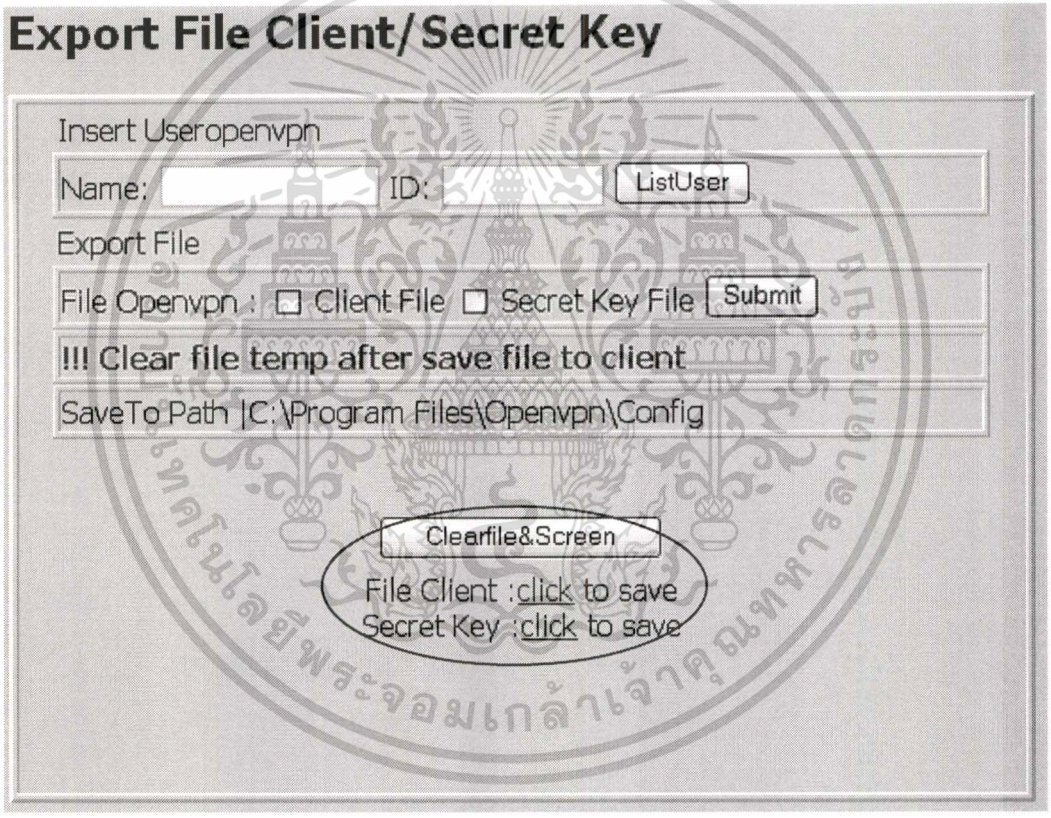


Advance Create File

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Advance Create File นี้จะใช้ในการสร้างไฟล์คอนฟิกโดยผู้ดูแลระบบซึ่งสามารที่จะกำหนดค่าพารามิเตอร์เองได้ซึ่งต่างจาก Normal Create File ที่จะใช้พารามิเตอร์เป็น Default แต่การสร้างไฟล์ของ Advance นั้นจะทำได้ทีละด้าน (Client File และ Server File) ในขณะที่ Normal Create นั้นจะสร้างไฟล์พร้อมกันทั้ง 2 ด้าน

Export File ใช้ในการ Download File ของไฟล์คีย์และไฟล์คอนฟิกของฝั่งไคลเอนต์ โดยลิงค์ (Link) ที่ระบบสร้างให้สำหรับ Download นั้นแสดงดังรูป โดยในวงรีนั้นเป็นลิงค์ที่ใช้สำหรับ Download File



Export File Client /Secret Key ส่วน Admin

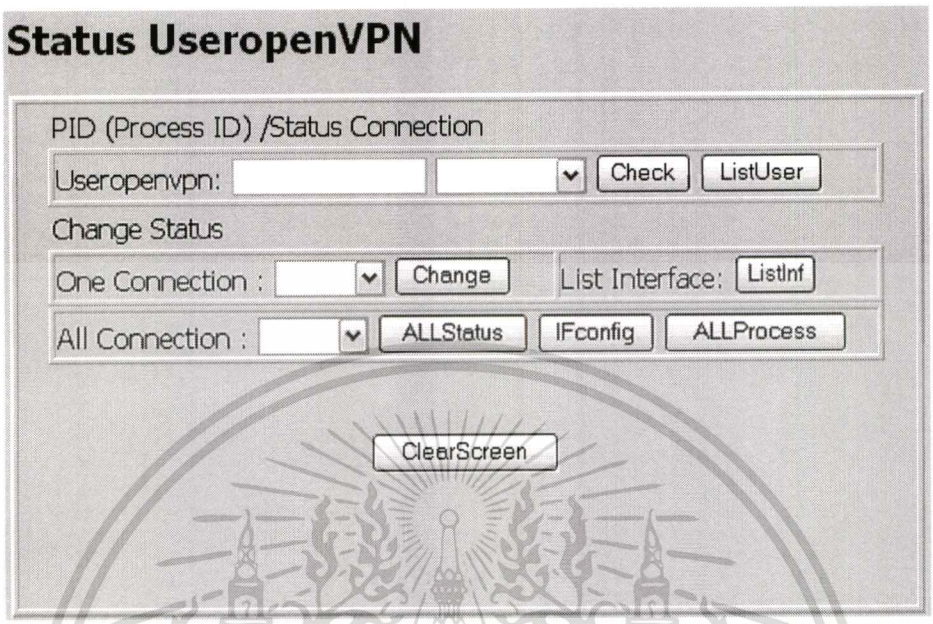
3.3 Management Function ประกอบด้วยฟังก์ชัน

-Status

-Log User

Status ใช้ในการตรวจสถานะการให้บริการรวมไปถึงตรวจสอบการเชื่อมต่อของผู้ใช้ซึ่งฟังก์ชั่นนี้สามารถจะตรวจพร้อมกันทั้งหมดหรือทีละ 1 User นอกจากใช้ในการตรวจสอบสถานะและการเชื่อมต่อแล้วยังสามารถตรวจสอบข้อมูล Interface ได้เช่นกัน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



Status UseropenVPN

จากรูป Status UseropenVPN

Check: ใช้สำหรับการตรวจสอบสถานะการให้บริการ (Process) หรือสถานะการเชื่อมต่อทีละ 1 User (Useropenvpn)

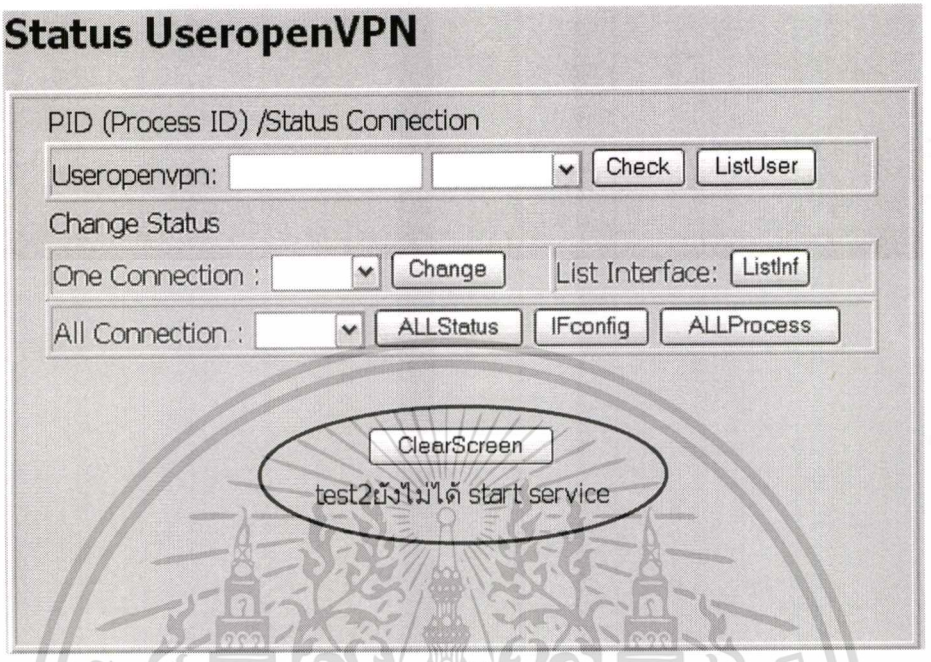
ALL Process: ใช้สำหรับการตรวจสอบสถานะการให้บริการ (Process) หรือสถานะการเชื่อมต่อพร้อมกันทั้งหมด

OneConnection: ใช้สำหรับเปลี่ยนสถานะการให้บริการทีละ 1 User

All Connection: ใช้สำหรับเปลี่ยนสถานะการให้พร้อมกันทั้งหมด

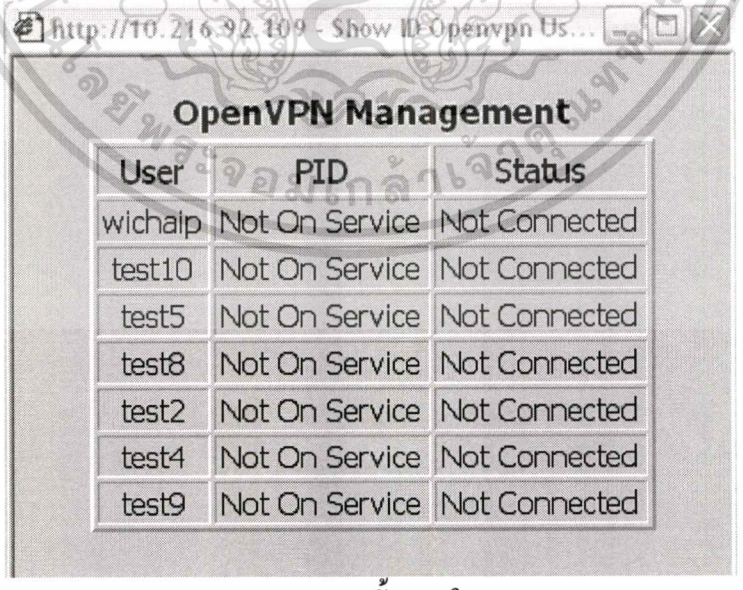
List Interface: ใช้สำหรับตรวจสอบข้อมูลไอพีตลอดจน Interface device ของผู้ใช้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



การแสดงผลทีละ 1 User

ในกรณีที่แสดงผลทีละ 1 Userนั้นจะแสดงผลที่ตัว Main โดยตรงในขณะที่แสดงผลทั้งหมดนั้นจะแสดงเป็นป๊อปอัพขึ้นมาให้เป็นตารางซึ่งการแสดงผลทั้งหมดนั้นให้เลือก “ALLProcess”

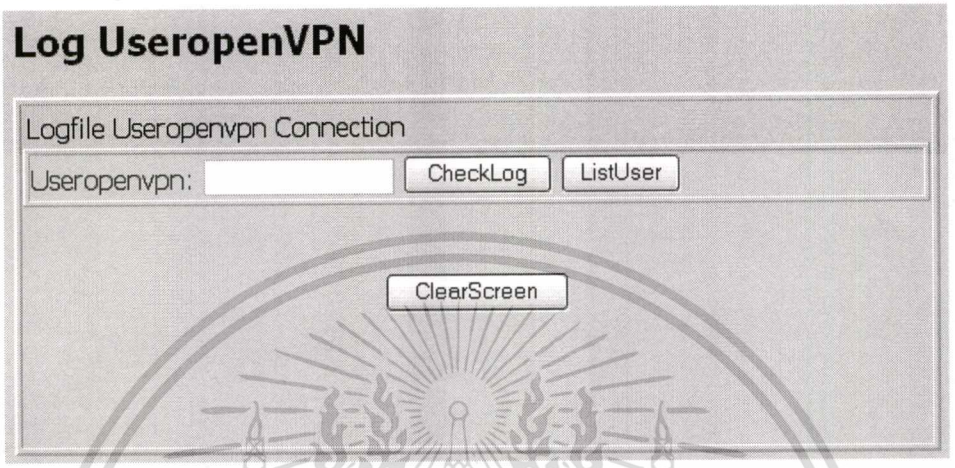


User	PID	Status
wichaip	Not On Service	Not Connected
test10	Not On Service	Not Connected
test5	Not On Service	Not Connected
test8	Not On Service	Not Connected
test2	Not On Service	Not Connected
test4	Not On Service	Not Connected
test9	Not On Service	Not Connected

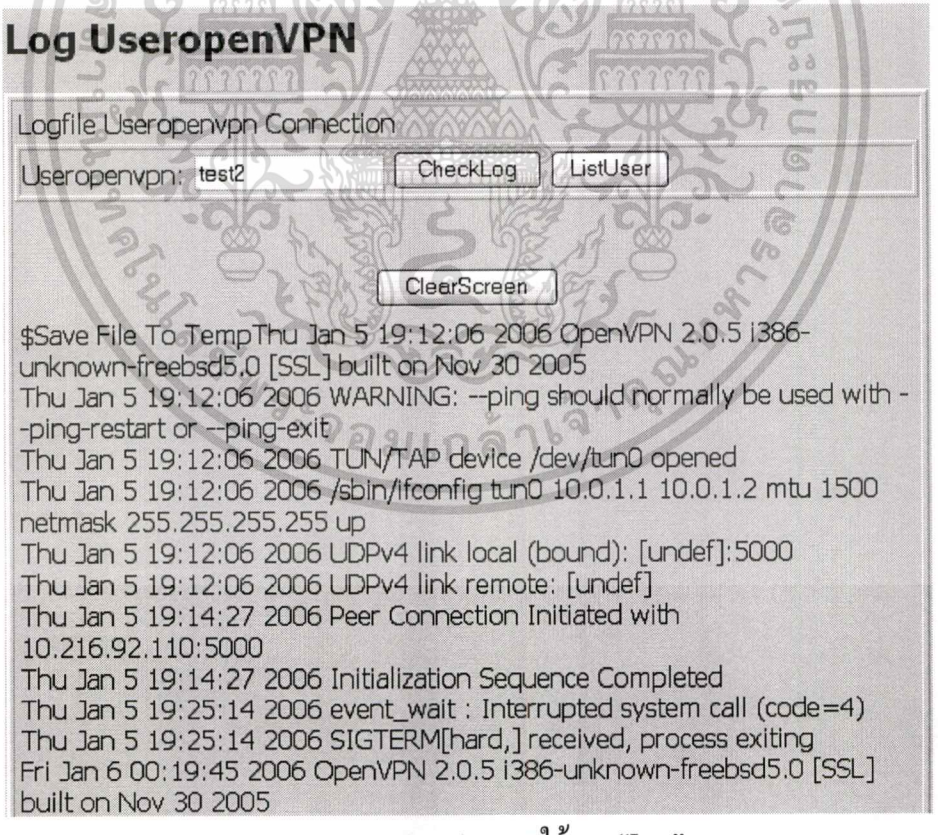
แสดงผลสถานะทั้งหมดในระบบ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Log User ใช้ในการตรวจสอบประวัติการใช้งานของผู้ใช้แต่ละคน โดยใส่ค่า Useropenvpn แล้วเลือก CheckLog



Log UseropenVPN



แสดงผลการตรวจสอบการใช้งาน “Log”

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4. หน้าหลังการ Login ของ User (Main) เป็นส่วนที่ผู้ใช้งานสามารถเข้าไปใช้งานได้โดยผู้ใช้งานจะสามารถทำรายการได้ดังต่อไปนี้

1. Download ข้อมูลไฟล์คอนฟิกของผู้ใช้งานนั้นๆ
2. ตรวจสอบสถานการณ์เชื่อมต่อและการใช้บริการของผู้ใช้นั้นได้
3. เปลี่ยนรหัสผ่านเข้าระบบการจัดการเครือข่ายส่วนตัวเสมือน
4. เปลี่ยนคีย์ที่ใช้ในการเข้ารหัสข้อมูลได้พร้อมกับ Reload การให้บริการในส่วนของผู้ใช้นั้นได้

การจัดการ OpenVPN โดยผู้ใช้ โดยแบ่งเป็น 5 ส่วนตามหมายเลข 1-5

หมายเลขที่ 1 เป็นส่วนแสดงรายชื่อของผู้ใช้งาน

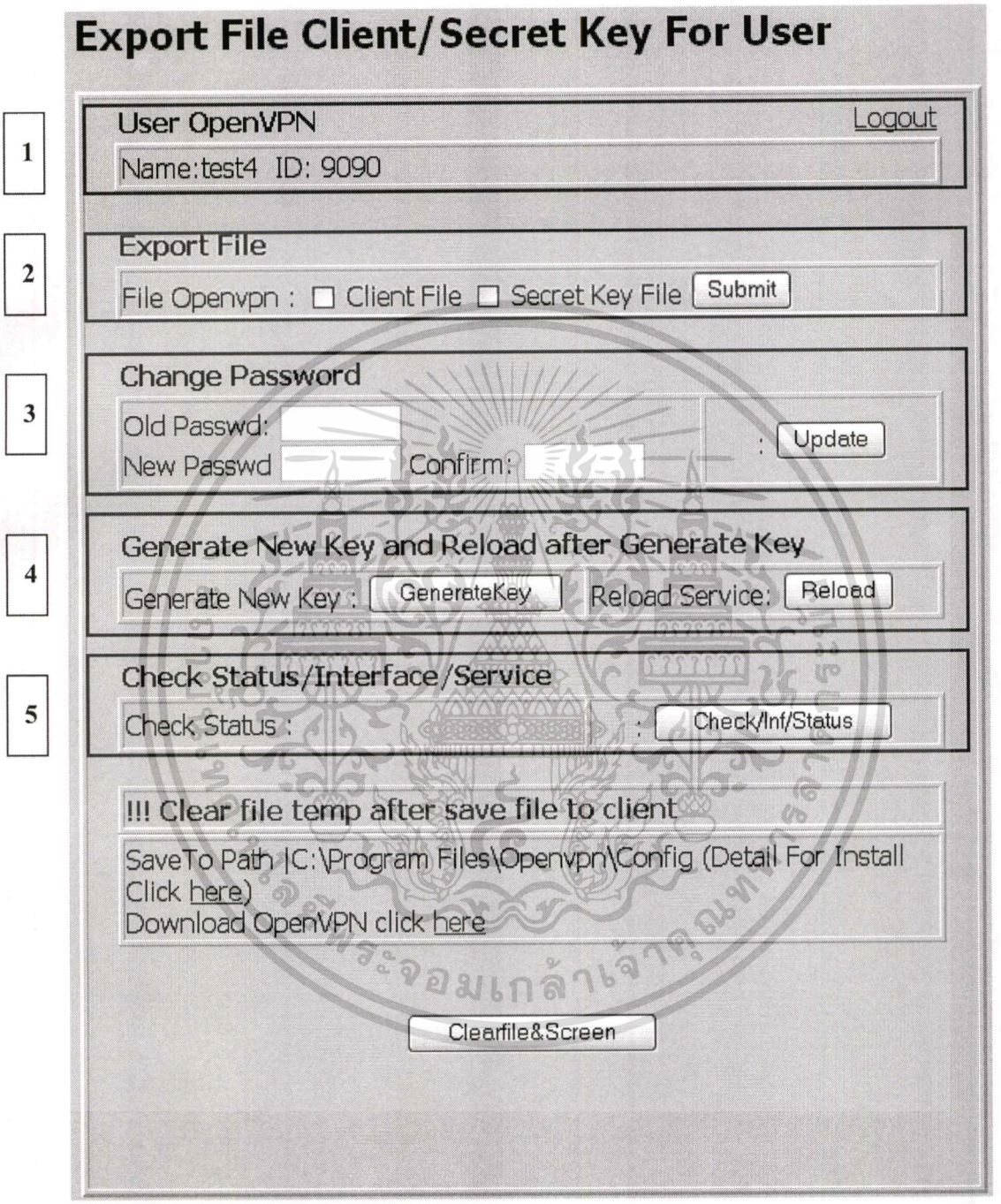
หมายเลขที่ 2 เป็นส่วน Export File โดยสามารถเลือกได้ว่าจะ Export ข้อมูล คีย์ หรือไฟล์คอนฟิกได้

หมายเลขที่ 3 เป็นส่วนที่ใช้ในการเปลี่ยนรหัสผ่านของผู้ใช้งาน

หมายเลขที่ 4 เป็นส่วนเปลี่ยนคีย์ในการเข้ารหัสข้อมูลของผู้ใช้งานและเมื่อเปลี่ยนคีย์เสร็จจะต้องทำการ Reload ก่อนเพื่อให้ระบบนำคีย์ใหม่ไปใช้งาน

หมายเลขที่ 5 เป็นส่วนที่ใช้ตรวจสอบการให้บริการและสถานะการเชื่อมต่อของผู้ใช้งาน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



แสดงส่วนติดต่อผู้ใช้ Main (User)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

จ. Parameter ของ OpenVPN ที่สามารถตั้งค่าได้ในโครงงานนี้

--config file

--local host

--remote host [port]

--proto p [p can be udp or tcp]

--dev tunX

--route network/IP [netmask] [gateway] [metric]

--route-gateway gw

--mtu-test

--ping n

--ping-restart n

--keepalive n m

--user user

--group group

--cd dir

--daemon [progname]

--chroot dir

--log file

--log-append file

--writepid file

--status file [n]

--mute n

--comp-lzo

--secret file [direction]

--port port

--ifconfig l rn [l :IP address local VPN, rn : IP address remote VPN]

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ประวัติผู้เขียน

ชื่อผู้เขียน	นายวิชัย เพียรดี
สถานที่เกิด	จังหวัดกรุงเทพมหานคร
ระดับประถมศึกษา	โรงเรียนสมฤทัย จังหวัดกรุงเทพฯ
ระดับมัธยมศึกษาตอนต้น	โรงเรียนเซนต์จอห์น จังหวัดกรุงเทพฯ
ระดับมัธยมศึกษาตอนปลาย	โรงเรียนเทพศิรินทร์ จังหวัดกรุงเทพฯ
วุฒิการศึกษาระดับปริญญาตรี	คณะวิศวกรรมศาสตร์ สาขาวิศวกรรมไฟฟ้า มหาวิทยาลัยเกษตรศาสตร์
ประสบการณ์การทำงาน	บริษัท แอดวานดซ์ อินโฟ เซอร์วิส (มหาชน)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้