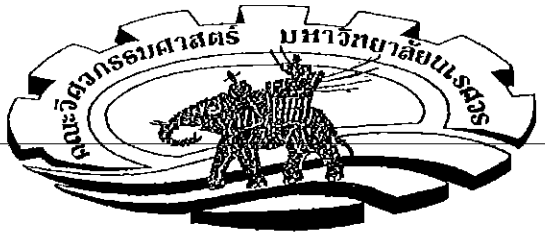
การใช้งานไฟร์วอลล์ผ่านเว็บแอปพลิเคชันบนระบบปฏิบัติการลินุกซ์

Using firewall via web application on Linux operating system

นายพรพนม นันทะเสน รหัส 48364821
นางสาวพลิตา สำเภาเงิน รหัส 48364845

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต
สาขาวิชาวิศวกรรมคอมพิวเตอร์ ภาควิชาวิศวกรรมไฟฟ้าและคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ มหาวิทยาลัยนเรศวร
ปีการศึกษา 2551



ใบรับรองโครงงาน

หัวข้อโครงงาน การใช้งานไฟร์วอลล์ผ่านเว็บแอปพลิเคชันบนระบบปฏิบัติการลินุกซ์

ผู้ดำเนินโครงงาน นายพรพนม นันทะเสน รหัส 48364821

นางสาวพลิตา สำเภาเงิน รหัส 48364845

อาจารย์ที่ปรึกษา นายภาณุพงศ์ สอนคม

สาขาวิชา วิศวกรรมคอมพิวเตอร์

ภาควิชา วิศวกรรมไฟฟ้าและคอมพิวเตอร์

ปีการศึกษา 2551

.....

คณะวิศวกรรมศาสตร์ มหาวิทยาลัยนเรศวร อนุมัติให้โครงงานฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมคอมพิวเตอร์

คณะกรรมการสอบโครงงานวิศวกรรม

.....ประธานกรรมการ

(นายภาณุพงศ์ สอนคม)

.....กรรมการ

(ดร.อัครพันธ์ วงศ์กังแห)

.....กรรมการ

(นายเศรษฐา ตั้งค้าวานิช)

หัวข้อโครงงาน	การใช้งาน Firewall ผ่านเว็บแอปพลิเคชันบนระบบปฏิบัติการลินุกซ์
ผู้ดำเนินโครงงาน	นายพรพนม นันทะเสน รหัส 48364821
	นางสาวพลิตา สำเภาเงิน รหัส 48364845
อาจารย์ที่ปรึกษา	นายภาณุพงศ์ สอนคม
สาขาวิชา	วิศวกรรมคอมพิวเตอร์
ภาควิชา	วิศวกรรมไฟฟ้าและคอมพิวเตอร์
ปีการศึกษา	2551

บทคัดย่อ

โครงงานนี้พัฒนาขึ้นเพื่อให้ระบบปฏิบัติการลินุกซ์ที่พัฒนาเป็น Firewall เพื่อใช้เป็นมาตรการป้องกันและรักษาความปลอดภัยภายในระบบเครือข่าย สามารถใช้งานได้ง่าย สะดวก และมีประสิทธิภาพการทำงานที่ดีขึ้น เพื่อรองรับต่อความต้องการใช้งานภายในสภาวกาลปัจจุบัน โดยโครงงานนี้มีการพัฒนาอยู่ 2 ส่วน คือ ส่วนติดต่อผู้ใช้ ได้มีการพัฒนาเว็บแอปพลิเคชันเพื่อใช้เป็นส่วนติดต่อระหว่างผู้ใช้กับ Firewall เพื่อให้ผู้ใช้สามารถปรับเปลี่ยนกฎการทำงานของ Firewall ได้อย่างสะดวกและง่ายดายตามต้องการ อีกส่วนหนึ่งก็คือส่วนของ Firewall ได้มีการพัฒนาให้มีความสามารถในการป้องกันการเข้าถึงเว็บไซต์ด้วยการบล็อก URL และสามารถปรับเปลี่ยน URL ที่ต้องการบล็อกได้อย่างง่ายดายผ่านทางเว็บแอปพลิเคชัน

Project Title	Using firewall via web application on Linux operating system		
Name	Mr. Pornpanom	Nanthasen	ID 48364821
	Miss. Phalita	Sampaongoen	ID 48364845
Project Advisor	Mr. Panupong	Sornkhom	
Major	Computer Engineering		
Department	Electrical and Computer Engineering		
Academic year	2008		

ABSTRACT

This project developed for creating the firewall of the Linux operating system, to manage the protection and security of the network, simple, conveniently and better efficient function that supported the need of work. We separated project into 2 parts are interface and firewall. Interface, development of the web application to connect between user and firewall that can be adapted with work conveniently and easily. Firewall, developed to protection of approaching to the improve website with block URL and can be changed URL so easily by web application.

กิตติกรรมประกาศ

โครงงานเรื่องการใช้ Firewall ผ่านเว็บแอปพลิเคชันบนระบบปฏิบัติการลินุกซ์สำเร็จได้ด้วยดี เนื่องจากได้รับความอนุเคราะห์จากอาจารย์ปรึกษาโครงงาน อาจารย์ภาณุพงศ์ สอนคม ซึ่งท่านได้กรุณาให้คำปรึกษา แนะนำวิธีการทำงาน พร้อมทั้งเสนอแนะแนวทางการแก้ไขปัญหามาตลอดระยะเวลาการทำโครงงาน

ดร.อัครพันธ์ วงศ์กังแห และ อาจารย์เศรษฐา ตั้งค้าวานิช ที่กรุณาสละเวลา เป็นอาจารย์สอบโครงงาน พร้อมทั้งให้คำแนะนำที่เป็นประโยชน์ในการทำโครงงานนี้

อาจารย์ทุกท่าน ที่ช่วยประสิทธิ์ประสาทวิชาความรู้ ทั้งในแง่วิชาการ และในแง่การดำรงชีวิต ช่วยอบรมสั่งสอนให้เป็นคนดี คงไว้ซึ่งความมีคุณธรรม ความซื่อสัตย์

บิดา มารดา เพื่อนพ้อง พี่น้อง ที่ช่วยเป็นกำลังใจ และช่วยสนับสนุนตลอดมา ทั้งในการเรียน และการจัดทำโครงงาน ให้สำเร็จลุล่วงไปได้เป็นอย่างดี

ผู้จัดทำโครงงานขอกราบขอบพระคุณเป็นอย่างสูง มา ณ โอกาสนี้

นายพรพนม นันทะเสน

นางสาวพลิตา สำเภาเงิน

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

สารบัญรูป

สารบัญรูป (ต่อ)

สารบัญรูป (ต่อ)

สารบัญรูป (ต่อ)

สารบัญรูป (ต่อ)

สารบัญรูป (ต่อ)

สารบัญรูป (ต่อ)

บทที่ 1
บทนำ

1.1 ที่มาและความสำคัญ

การปกป้องความมั่นคงและการรักษาความปลอดภัยภายในระบบเครือข่ายคอมพิวเตอร์ ถือเป็นสิ่งสำคัญอย่างยิ่ง เนื่องจากการถูกดุกคามโดยผู้ไม่ประสงค์ดี หรือจากโปรแกรมบางประเภท ได้มีอัตราเพิ่มขึ้นเรื่อยๆ ซึ่งอาจนำมาซึ่งความเสียหายต่อระบบภายในองค์กร ดังนั้นภายในองค์กรหรือสถานที่ให้บริการด้านคอมพิวเตอร์ในยุคปัจจุบัน จึงจำเป็นจะต้องมีระบบเครือข่ายคอมพิวเตอร์ที่มีประสิทธิภาพ ใช้งานง่าย สามารถป้องกันและรักษาความปลอดภัยให้แก่ระบบได้

การรักษาความปลอดภัยในระบบนั้นสามารถกระทำได้หลายวิธี ซึ่งการใช้ Firewall นั้นถือเป็นอีกหนึ่งวิธีที่มีประสิทธิภาพ และนำมาใช้กันอย่างกว้างขวาง โดยที่ Firewall เปรียบเสมือนกำแพงที่สามารถกั้นและกรอง Package ที่ไม่พึงประสงค์ด้วยการตรวจสอบค่า IP, Port และประเภทของ Protocol จากการพิจารณาสภาวะการเชื่อมต่อ อีกทั้งยังสามารถทำงานได้ในระดับ Application เช่น ตรวจดู Header ของ E-mail และสแกนไวรัส เป็นต้น

Firewall ที่ใช้อยู่ในปัจจุบันนั้นโดยส่วนใหญ่แล้ว หากต้องมีการปรับปรุง แก้ไข หรือเปลี่ยนแปลงการทำงานต่างๆ จะต้องพิมพ์คำสั่งซึ่งค่อนข้างยุ่งยากและไม่สะดวกต่อการใช้งาน ดังนั้นผู้จัดทำจึงได้พัฒนาเว็บแอปพลิเคชันเพื่อใช้ติดต่อกับ Firewall ทำให้ผู้ใช้สามารถใช้งาน Firewall ได้ง่ายและสะดวกสบายยิ่งขึ้น แต่ยังคงไว้ซึ่งความมีประสิทธิภาพในการป้องกันและรักษาความปลอดภัยในระบบเครือข่ายคอมพิวเตอร์

1.2 วัตถุประสงค์

1.2.1 พัฒนาให้ Firewall สามารถใช้งานได้ง่ายขึ้น

1.2.2 นำโปรแกรมและเทคโนโลยีที่มีอยู่แล้วมาพัฒนาให้เกิดประโยชน์

1.2.3 ประยุกต์ใช้งานทรัพยากรได้อย่างมีประสิทธิภาพและเกิดประสิทธิผล

1.2.4 นำความรู้ที่ได้ศึกษามาพัฒนาต่อยอด

1.3 ขอบข่ายของโครงงาน

1.3.1 สร้างและพัฒนาเว็บแอปพลิเคชันเพื่อใช้เป็นส่วนติดต่อระหว่างผู้ใช้กับ Firewall

1.3.2 พัฒนา Firewall ให้มีความสามารถในการป้องกันการเข้าถึงเว็บไซต์ที่ไม่เหมาะสม

1.4 ขั้นตอนการดำเนินงาน

1.4.1 ศึกษาทฤษฎีที่เกี่ยวข้อง

1.4.2 พัฒนาระบบและออกแบบโปรแกรม

1.4.3 เขียนโปรแกรมเพื่อทดสอบกับระบบ

1.4.4 ตรวจสอบหาข้อผิดพลาดและแก้ไข

1.4.5 สรุปผลการทดลองและจัดทำรูปเล่มรายงาน

1.5 แผนการดำเนินงาน

ตารางที่ 1.1 แผนการดำเนินงานโครงงานการใช้งาน Firewall ผ่านเว็บแอปพลิเคชันบนระบบปฏิบัติการลินุกซ์

กิจกรรม	ปี 2551							ปี 2552		
	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.
1. ศึกษาทฤษฎีที่เกี่ยวข้อง	←	—	→							
2. พัฒนาระบบและออกแบบโปรแกรม			←	—	→					
3. เขียนโปรแกรมเพื่อทดสอบกับระบบ						←	—	→		
4. ตรวจสอบหาข้อผิดพลาดและแก้ไข						←	—	—	→	
5. สรุปผลการทดลองและจัดทำรูปเล่มรายงาน			←	—	—	—	—	—	—	→

1.6 ผลที่คาดว่าจะได้รับ

1.6.1 ได้เว็บแอปพลิเคชันที่สามารถใช้เป็นส่วนติดต่อระหว่างผู้ใช้กับ Firewall

1.6.2 ได้ Firewall ที่มีความสามารถในการป้องกันการเข้าถึงเว็บไซต์ที่ไม่เหมาะสม

1.6.3 ได้ Firewall ที่มีระบบป้องกันและรักษาความปลอดภัยที่ดี โดยใช้ทรัพยากรได้อย่างมีประสิทธิภาพและเกิดประสิทธิผล

1.6.4 สามารถนำองค์ความรู้ที่ได้ศึกษามาพัฒนาต่อยอดได้อย่างมีประสิทธิภาพและก่อให้เกิดประโยชน์สูงสุด

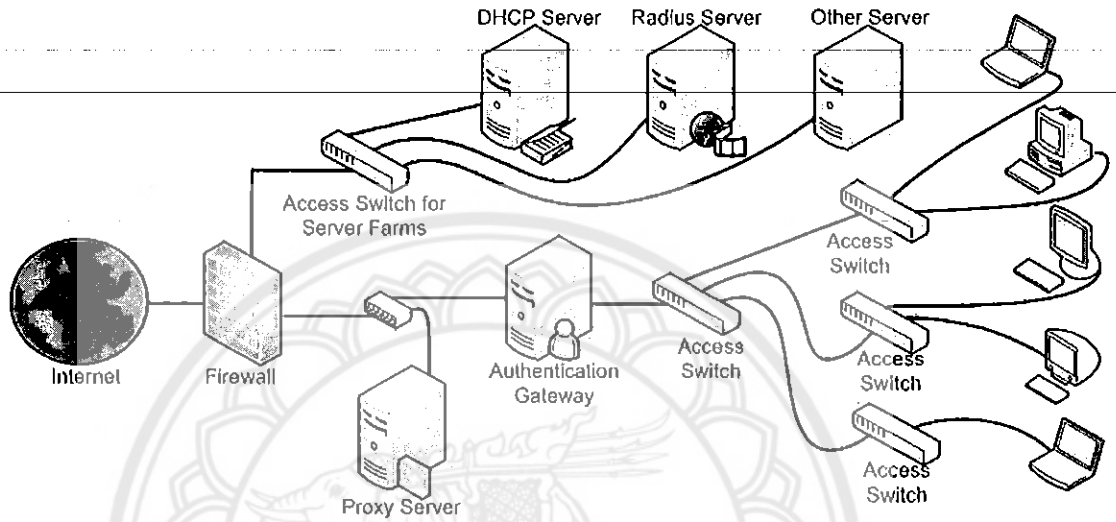
1.7 งบประมาณโครงงาน

1.7.1	ค่าวัสดุสำนักงาน	เป็นเงิน	300 บาท
1.7.2	ค่าวัสดุคอมพิวเตอร์	เป็นเงิน	200 บาท
1.7.1	ค่าจัดทำเอกสาร	เป็นเงิน	1,000 บาท
1.7.2	ค่าวัสดุอื่นๆ	เป็นเงิน	500 บาท
		รวมเป็นเงิน	2,000 บาท
			(สองพันบาทถ้วน)

หมายเหตุ ถัวเฉลี่ยทุกรายการ

บทที่ 2
หลักการและทฤษฎี

2.1 ระบบเครือข่ายคอมพิวเตอร์



รูปที่ 2.1 แสดงระบบเครือข่ายคอมพิวเตอร์ทั่วไป

ระบบเครือข่ายคอมพิวเตอร์ทั่วๆ ไปสามารถแสดงได้ดังรูปที่ 2.1 โดยมีส่วนประกอบที่สำคัญอยู่ 3 ส่วนใหญ่ๆ คือ

1. ส่วน Demilitarize (DMZ) เป็นส่วนที่ใช้เชื่อมต่อกับอุปกรณ์เครื่องแม่ข่ายทั้งหมดขององค์กร หรือเรียกว่าส่วนของเซิร์ฟเวอร์ฟาร์ม (Server Farms) ซึ่งหน้าที่โดยทั่วไปจะเป็นพื้นที่ให้บริการเซอร์วิสต่างๆ ขององค์กร เช่น DHCP Server, RADIUS Server, Log Server, NTP Server เป็นต้น โดยส่วนนี้จะเป็นส่วนที่ค่อนข้างจะปลอดภัยที่สุดสำหรับองค์กร

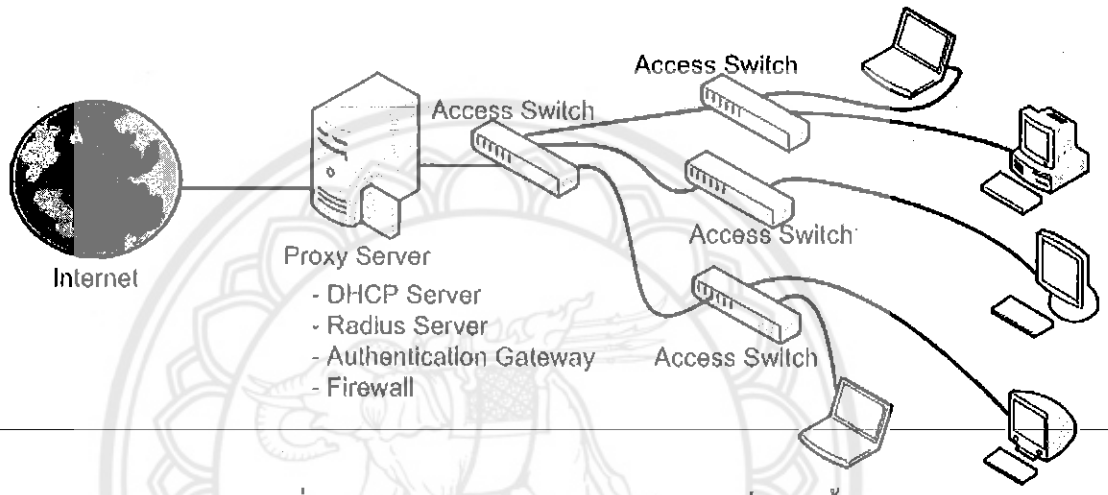
2. ส่วน Internet เป็นส่วนที่เชื่อมต่อกับเครือข่ายอินเทอร์เน็ต ประกอบด้วย อุปกรณ์ Router, Firewall และ Proxy Server เป็นต้น

3. ส่วน Internal จะเป็นส่วนที่ติดต่อกับผู้ใช้บริการภายในองค์กร ซึ่งประกอบไปด้วย Access Switch และ Authentication Gateway เป็นต้น

หลักการทำงานของระบบเครือข่ายคอมพิวเตอร์จากรูปที่ 2.1 มีหลักการทำงานคือ เมื่อผู้ใช้บริการมีการเชื่อมต่อเข้ากับระบบเครือข่ายคอมพิวเตอร์ DHCP Server ก็จะให้ IP Address แก่เครื่องนั้นๆ ซึ่งหากเครื่องนั้นต้องการใช้งานอินเทอร์เน็ต อุปกรณ์ที่เรียกว่า Authentication Gateway จะทำงานโดยการบังคับให้พิมพ์ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อเป็นการยืนยัน

ตัวตนว่าเป็นผู้มีสิทธิ์ในการเข้าใช้ระบบเครือข่ายคอมพิวเตอร์ ซึ่งการตรวจสอบสิทธิ์ในการใช้งานต่างๆ จะเป็นหน้าที่ของ RADIUS Server หลังจากผ่านขั้นตอนการยืนยันตัวตนแล้ว จะสามารถเข้าใช้งานในระบบเครือข่ายคอมพิวเตอร์ได้ภายใต้กฎของ Firewall

จากระบบเครือข่ายคอมพิวเตอร์ในรูปที่ 2.1 จะเห็นได้ว่ามีจำนวนอุปกรณ์ที่ค่อนข้างมาก ทำให้มีความยุ่งยากด้านการเชื่อมต่อและการติดตั้งเพื่อให้อุปกรณ์ในระบบเครือข่ายคอมพิวเตอร์สามารถทำงานร่วมกันได้ อีกทั้งยังมีค่าใช้จ่ายที่ค่อนข้างสูงในการซื้ออุปกรณ์แต่ละชิ้น ดังนั้นจึงได้พัฒนาระบบเครือข่ายคอมพิวเตอร์ดังแสดงในรูปที่ 2.2

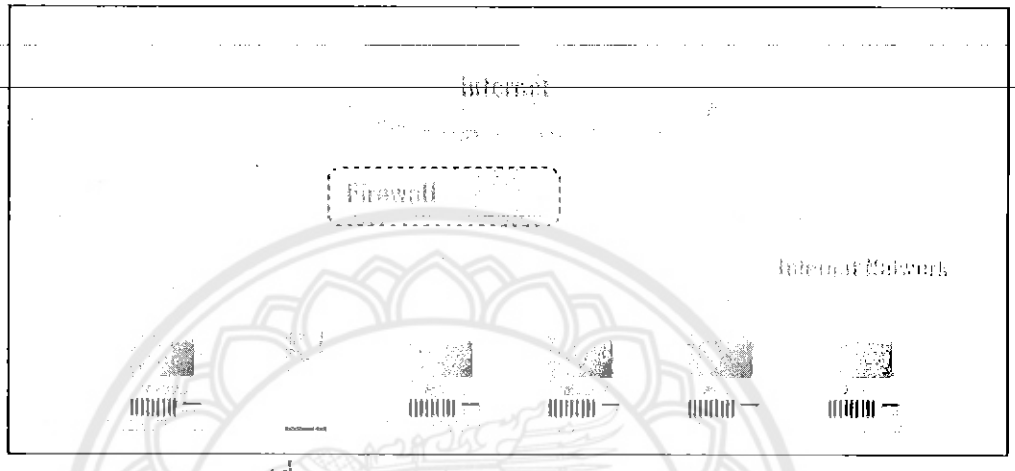


รูปที่ 2.2 แสดงระบบเครือข่ายคอมพิวเตอร์ที่จัดทำขึ้น

จากรูปที่ 2.2 จะเห็นได้ว่าใช้อุปกรณ์น้อยลง แต่ยังสามารถทำงานได้เช่นเดียวกับระบบเครือข่ายคอมพิวเตอร์ในรูปที่ 2.1 ซึ่งเป็นการลดการใช้อุปกรณ์ลง โดยรวมเอาส่วนต่างๆ ของระบบมาไว้ในอุปกรณ์ให้บริการเพียงเครื่องเดียวที่เรียกกว่า Proxy Server ซึ่งในโครงงานนี้ได้นำเอาระบบปฏิบัติการลินุกซ์ คือ Ubuntu desktop รุ่น 8.04 มาจัดทำเป็นเครื่องให้บริการด้วยการติดตั้งโปรแกรมต่างๆ เพื่อเพิ่มความสามารถ คือ Chillispot, Apache Web Server, MySQL Database Server, PHP5, PHPMyadmin, FreeRADIUS, SSL, และ Transparent Proxy Squid นำมาทำการปรับตั้งค่าต่างๆ เพื่อให้ทำงานได้อย่างมีประสิทธิภาพ สามารถใช้ได้กับองค์กรขนาดเล็ก และขนาดกลาง ทำให้ประหยัดค่าใช้จ่ายในการจัดทำระบบเครือข่ายคอมพิวเตอร์ได้เป็นอย่างมาก

2.2 Firewall

ในความหมายด้านการสร้างนั้น Firewall หมายถึง กำแพงที่มีไว้เพื่อป้องกันไม่ให้ไฟลุกลามไปยังส่วนอื่นๆ [5] ส่วนในทางด้านคอมพิวเตอร์ก็มีความหมายคล้ายคลึงกันนั่นก็คือ ระบบที่มีไว้ป้องกันและรักษาความปลอดภัยเพื่อมิให้สิ่งที่ไม่พึงประสงค์ที่มาจากระบบภายนอกรุกล้ำเข้ามาทำความเสียหายให้กับระบบภายใน



รูปที่ 2.3 แสดงรูปแบบการทำงานของ Firewall

Firewall เป็น Component หรือกลุ่มของ Component ซึ่งอาจจะเป็น เร้าท์เตอร์, คอมพิวเตอร์ หรือเครือข่ายประกอบกัน โดยทำหน้าที่ในการควบคุมการจราจรทางคอมพิวเตอร์และเทคโนโลยีสารสนเทศ ตัว Firewall นั้นจะช่วยป้องกันระบบภายในเพื่อไม่ให้ระบบเครือข่ายที่ไม่ปลอดภัยสามารถเข้ามาทำความเสียหายได้ และยังสามารถสร้างมาตรการหรือข้อกำหนดต่างๆ เพื่อเป็นมาตรฐานความปลอดภัยให้กับระบบภายใน

Firewall ในปัจจุบันนั้นแบ่งเป็นสองชนิดหลักๆ คือ Stateful Packet Filtering Firewall และ Proxy Server ซึ่งจะมีการตรวจสอบข้อมูลที่ไหลผ่านเข้าออกที่คนละ Layer กัน โดย Packet Filtering นั้นจะตรวจสอบข้อมูลที่ Network Layer และ Session Layer ในขณะที่ Proxy Server นั้นสามารถตรวจสอบข้อมูลที่ Application Layer ได้

ดังนั้นในโครงงานนี้จึงจัดทำ Proxy Server เพื่อมาใช้เป็น Firewall เพื่อให้สามารถป้องกันการเข้าถึงเว็บไซต์ที่ไม่เหมาะสมโดยการกำหนด URL (Uniform Resource Locator) ซึ่งเป็นการตรวจสอบข้อมูลที่ Application Layer และจัดทำเว็บแอปพลิเคชันขึ้นมาเพื่อใช้เป็นส่วนติดต่อกับ Firewall ทำให้การใช้งาน Firewall สามารถทำได้ง่ายและสะดวกมากยิ่งขึ้น

2.2.1 สิ่งที่ Firewall ช่วยได้

Firewall สามารถช่วยเพิ่มความปลอดภัยให้กับระบบได้โดย

- บังคับใช้นโยบายด้านความปลอดภัย โดยกำหนดกฎให้กับ Firewall เพื่อใช้ควบคุมการจราจรทางคอมพิวเตอร์และเทคโนโลยีสารสนเทศ
- ทำให้การจัดการดูและระบบมีความสะดวกและง่ายขึ้น เนื่องจากการติดต่อทุกชนิดจะต้องผ่าน Firewall ซึ่งถือว่าเป็นการดูแลความปลอดภัยในระดับเครือข่าย (Network-base Security)
- ป้องกันระบบเครือข่ายภายในบางส่วนที่ไม่ต้องการเปิดเผยแก่สาธารณะ โดยสามารถกำหนดได้ว่าอนุญาตหรือไม่ ในการเข้าถึงข้อมูลในแต่ละส่วน
- Firewall บางชนิดสามารถป้องกันไวรัสได้ โดยจะตรวจสอบข้อมูลที่โอนย้ายผ่านเข้ามาทางโปรโตคอล HTTP, FTP และ SMTP

2.2.2 สิ่งที่ Firewall ช่วยไม่ได้

- อันตรายที่เกิดจากระบบเครือข่ายภายใน ไม่สามารถป้องกันได้เนื่องจากอยู่ภายในระบบเครือข่าย ไม่ได้ผ่าน Firewall เข้ามา
- อันตรายจากภายนอกที่ไม่ได้ผ่านเข้ามาทาง Firewall เช่น การ Dial-up เข้ามายังระบบเครือข่ายภายในโดยตรงโดยไม่ได้ผ่าน Firewall
- อันตรายจากวิธีใหม่ๆ ที่อาจเกิดขึ้น เนื่องจากปัจจุบันมีการพบช่องโหว่อยู่ตลอด จึงไม่สามารถไว้ใจ Firewall ที่ติดตั้งเพียงครั้งเดียวแล้วคาดหวังว่าจะปลอดภัยตลอดไป ต้องมีการดูแลอย่างต่อเนื่องและสม่ำเสมอ
- ไวรัส ถึงแม้ว่าจะมี Firewall บางชนิดที่สามารถป้องกันไวรัสได้ แต่ก็ไม่มี Firewall ใดที่สามารถตรวจสอบไวรัสได้ทุกๆ โปรโตคอล

2.3 IPTABLES

IPTABLES คือ ชุดคำสั่งชนิดหนึ่งซึ่งทำงานอยู่บนระบบปฏิบัติการลินุกซ์ [7]โดยมีหน้าที่ในการตรวจสอบ Packet ต่างๆ ที่เข้ามายังระบบปฏิบัติการตัวนั้นๆ อีกทั้งยังสามารถทำหน้าที่ในการส่งต่อและเปลี่ยนแปลง Packet ต่างๆ ดังนั้นจึงสามารถใช้ IPTABLES มาใช้เป็นชุดคำสั่งสำหรับสร้างกฎต่างๆให้กับ Firewall ได้

2.2.1 รูปแบบการใช้งาน iptables เบื้องต้น

iptables จะมีรูปแบบการใช้งานดังนี้คือ

iptables [table] <command> <match> <target/jump>

โดยกฎที่เขียนขึ้นจะเป็นเป็นตัวบอกเคอร์เนล (Kernel) ว่าให้กระทำอย่างไร ในกรณีที่พบ Packet ตรงตามที่ระบุไว้

- **[table]** หมายถึง ตารางหรือ table ที่ต้องการระบุ เช่น iptables -t nat หมายถึงให้ทำงานกับ NAT Table ในกรณีที่ไม่ได้ระบุตาราง iptables จะถือว่าคำสั่งดังกล่าวระบุถึง Filter Table โดยอัตโนมัติ
- **<command>** จะเป็นตัวสั่งให้ iptables ทำในสิ่งที่ต้องการ เช่น iptables -A INPUT ซึ่งหมายถึงให้สร้าง Rule ต่อท้าย Input Chain ใน Filter Table
- **<match>** เป็นส่วนที่ใช้ตรวจสอบว่า Packet มีข้อมูลตรงกับที่ระบุไว้หรือไม่ เช่น มี Source IP Address เป็น 1.2.3.4
- <target/jump> เป็นตัวระบุว่าเมื่อเจอ Packet ที่ตรงกับที่ระบุไว้ก็จะกระทำ ตามที่ระบุไว้ เช่น ถ้า Packet ใดมี Source IP Address เป็น 1.2.3.4 ให้ DROP Packet นั้นทิ้งไป

2.2.2 Table

iptables สามารถทำงานได้กับตาราง 3 ตารางหลัก สามารถระบุตารางได้โดยใช้ออปชัน -t ตามด้วยชื่อ Table คือ

- **Filter table** ใช้สำหรับกรอง Packet มี 3 built-in chain คือ INPUT, OUTPUT, FORWARD ซึ่งจะได้อธิบายรายละเอียดต่อไป
- **NAT table** ใช้สำหรับการแปลงแอดเดรส (Network Address Translation) มี 3 built-in chain คือ PREROUTING, POSTROUTING, OUTPUT
- **Mangle table** เป็นตารางที่ใช้เปลี่ยนแปลงหรือแก้ไข packet เช่น เปลี่ยนค่า TTL, MARK ซึ่งปกติจะใช้ในการทำ Routing ที่มีความซับซ้อนสูง มี 2 Built-in Chain คือ PREROUTING Chain (ใช้แก้ไข Packet ก่อนที่จะเข้าสู่ไฟร์วอลล์และก่อนเข้าสู่ routing decision) และ OUTPUT Chain (ใช้แก้ไข Packet ที่ถูกสร้างโดยไฟร์วอลล์ก่อนที่มันจะถูกส่งไปยัง Routing Decision) ทั้งนี้ไม่สามารถทำ Network Address Translation หรือ Masquerading ที่ Table นี้ได้

2.2.3 Command

- **-A** เพิ่ม Rule ใหม่ต่อท้าย Chain (Append Rule) เช่น

 # iptables -A INPUT -p ALL -i eth0 -j ACCEPT

- **-D** ลบ Rule (Delete Rule) เช่น

  # iptables -D INPUT --dport 80 -j DROP

- **-I** เพิ่ม Rule ใหม่ ใน Chain (Insert Rule) เช่น

  # iptables -I OUTPUT -p ALL -s 127.0.0.1/32 -j ACCEPT

- **-R** แทนที่ Rule เดิม ด้วย Rule ใหม่ (Replace Rule)
- **-L** แสดง Rule ทั้งหมดใน Chain (ถ้าไม่ระบุ Chain จะแสดง Rule ทั้งหมดใน Filter Table ทั้งสาม Built-in Chain) เช่น

  # iptables –L

  # iptables -L -t nat

  # iptables -L INPUT

- **-F** ลบ Rule ทั้งหมดใน Chain ทิ้ง เช่น

  # iptables -F INPUT

  # iptables -F mychain

- **-Z** ใช้ Reset Byte Counter สำหรับทุก Rule ใน Chain ที่กำหนด เช่น

  # iptables -Z INPUT

- **-N** ใช้สร้าง Chain ใหม่ เช่น

  # iptables -N mychain

- **-X** ลบ Chain ที่ไม่มี Rule ซึ่งสามารถลบ User-defined Chain ที่ไม่มี Rule ได้ แต่ไม่สามารถลบ Built-in Chain ได้ เช่น

  # iptables -X emptychain

- **-P** เปลี่ยน Default Policy ของ Chain ค่าที่ใช้ได้คือ ACCEPT, DROP ทั้งนี้ค่านี้มีความสำคัญอย่างมากเพราะหาก Packet ถูกส่งเข้ามาใน Chain แล้ว และไม่ ตรงตามเงื่อนไขกับ Rule ใดๆ เลย Packet นั้นก็ต้องถูกตัดสินใจโดย Policy ของ Chain นั้นๆ เช่น

  # iptables -P FORWARD DROP

  ซึ่งหาก Packet ถูกส่งเข้ามายัง FORWARD Chain และไม่ตรงตามเงื่อนไขกับ Rule ใดๆ ใน FORWARD Chain นี้เลย มันก็จะถูก DROP ทันที

- **-E** ใช้เปลี่ยนชื่อ Chain ใหม่ เช่น

  # iptables -E myoldchain mynewchain

การใช้ Command ด้านบนนั้นสามารถใช้ร่วมกับออปชันบางอย่างได้ คือ

- **-V, --verbose** ใช้ร่วมกับ -L, -A, -I, -D, -R เพื่อให้แสดงจำนวน Byte ที่ตรงกับ Rule ออกมาด้วย (หน่วยเป็นได้ทั้ง K(x1,000),M(x1,000,000),G(x1,000,000,000)) เช่น

  # iptables -L -v

- **-x, --exact** ใช้ร่วมกับ -L และ -v เพื่อให้แสดงจำนวน Packet และจำนวนของ Byte ข้อมูลที่ตรงกัน โดยไม่ให้แสดงผลในหน่วยของ K,M,G เช่น

  # iptables -L OUTPUT -v -x

- **-n, --numeric** ใช้ร่วมกับ -L เพื่อสั่งให้ iptables แสดงข้อมูลไอพีแอดเดรสและ Port เป็นตัวเลขเท่านั้น เช่น

  # iptables -L OUTPUT -n

- **--line-numbers** ใช้ร่วมกับ -L เพื่อแสดงเลขบรรทัดของ Rule ซึ่งตัวเลขที่แสดงนี้จะสามารถใช้ได้กับคำสั่ง INSERT Rule ที่ระบุเป็นลำดับที่ของ Rule เช่น

  # iptables -L --line-numbers

- **--modprobe=*command*** เพื่อโหลด Module ที่เกี่ยวข้อง

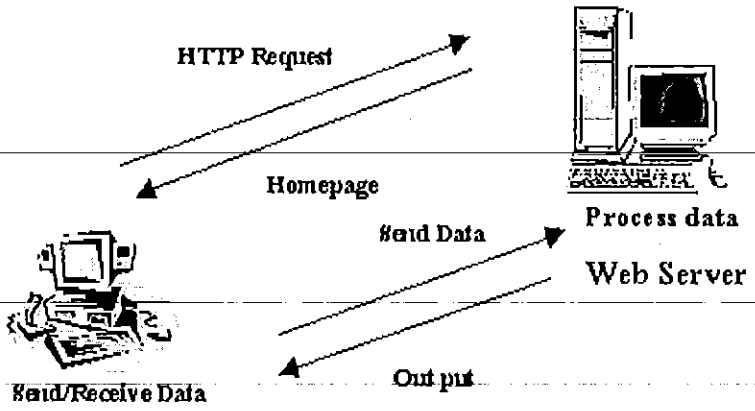
2.4 Common Gateway Interface (CGI)

มีการเข้าใจผิดกันว่า CGI เป็นภาษาหนึ่ง หรือเข้าใจว่าเป็นโปรแกรมหนึ่ง และเมื่อกล่าวถึง CGI ก็จะนึกถึงภาษา Perl แต่ความจริงแล้ว CGI เป็นเพียงหลักการหรือวิธีการเท่านั้น ซึ่งนอกจากภาษา Perl แล้วก็สามารถใช้ภาษาอื่นๆเขียนได้ เช่น PHP [8], ASP, CFM, C, C++ เป็นต้น

ตารางที่ 2.1 ภาษาที่ตรงกับ Plateform ของแต่ละระบบปฏิบัติการ

ระบบปฏิบัติการ	ภาษาที่ใช้ได้
Unix/Linux	C, C++, Perl, PHP
Windows	Perl, PHP, ASP, CFM

CGI เป็นโปรโตคอลที่ใช้ในการติดต่อระหว่าง Browser ของตัว Server กับตัวโปรแกรม Gateway [1] (หรือที่เรียกกันว่า CGI script) ซึ่งอาจจะเขียนขึ้นด้วยภาษาอะไรก็ได้ที่สามารถติดต่อกับ stdin, stdout และ ตัวแปรของระบบได้ ดังนั้น CGI จึงเป็นวิธีการ Interface ระหว่าง Server กับ Client โดยรับเอาข้อมูลจาก Client ไปประมวลผลที่ Server ผ่านทาง Browser [6]



รูปที่ 2.4 แสดงการติดต่อด้วยวิธี Common Gateway Interface (CGI)

จากรูปที่ 2.4 จะแสดงให้เห็นถึงวิธีการของ CGI ในการติดต่อสื่อสารระหว่าง Client กับ Server ซึ่งมีหลักการทำงานดังนี้

- Client เรียกข้อมูล HTTP จาก Server เช่นเรียก http://192.168.182.1
- Server ส่งข้อมูล เป็น Homepage หรือ HTML Format มายัง Client
- Client ส่งข้อมูลที่ต้องการประมวลผลไปยัง Server เช่น สั่งให้มีการปิด Port 80
- Server ประมวลผล มีการปิด Port 80 และบันทึกลงบนฐานข้อมูล

2.5 Message-Digest Algorithm 5 (MD5)

MD5 เป็นการ Hashing แบบทางเดียว (One-way Encryption) [3] ซึ่งถือเป็นการเข้ารหัสข้อมูลที่นิยมนำมาใช้ในการสื่อสารบนอินเทอร์เน็ตเป็นอย่างมาก เพื่อให้การสื่อสารนั้นมีความปลอดภัยสูงกว่าปกติ โดยผลลัพธ์ของการเข้ารหัสจะได้เป็นตัวอักษร ASCII ขนาด 32 ตัวอักษรตามมาตรฐาน RFC1321 เช่น <? echo md5("apple"); ?> จะได้เป็น 1f3870be274f6c49b3e31a0c6728957f ซึ่งเห็นได้ชัดว่าเป็นชุดตัวอักษรที่ไม่สามารถแปรออกมาได้

แต่การเข้ารหัสแบบ MD5 นี้เป็นมาตรฐานซึ่ง Cracker สามารถเขียนโปรแกรม MD5 Brute force ขึ้นมาตามมาตรฐานเพื่อให้ได้มาซึ่งข้อความก่อนเข้ารหัส โดยการแก้ปัญหานี้สามารถทำได้ 2 วิธีหลักๆ ดังนี้

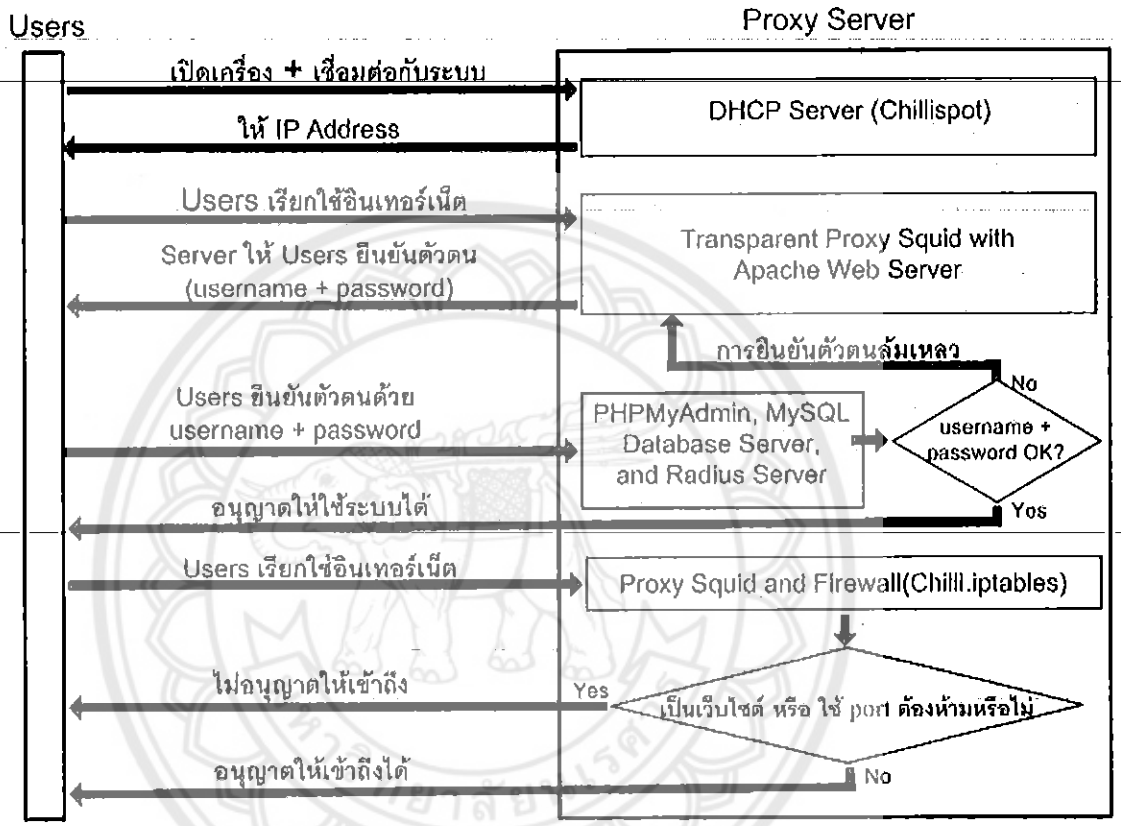
2.5.1 เข้ารหัสด้วย MD5 มากกว่า 1 ครั้ง เช่น <? echo md5(md5("apple")); ?> ซึ่งการใช้วิธีนี้จะทำให้การถอดรหัสออกมาทำได้ยากขึ้น เนื่องจากจะต้องมีการ Brute force ที่มากยิ่งขึ้น

2.5.2 เข้ารหัสพร้อมด้วย Public Key ซึ่งจะช่วยให้การถอดรหัสมีความยุ่งยากมากขึ้น เช่น

<? $key = "modoeye.com"; echo md5("apple".$key); ?>

บทที่ 3
ขั้นตอนการดำเนินงาน

3.1 ออกแบบโครงงาน



รูปที่ 3.1 แสดงการทำงานของระบบคอมพิวเตอร์ที่พัฒนาขึ้น

Proxy Server ที่พัฒนาขึ้นมานี้แบ่งเป็นส่วนใหญ่ๆ ได้ 3 ส่วนดังนี้

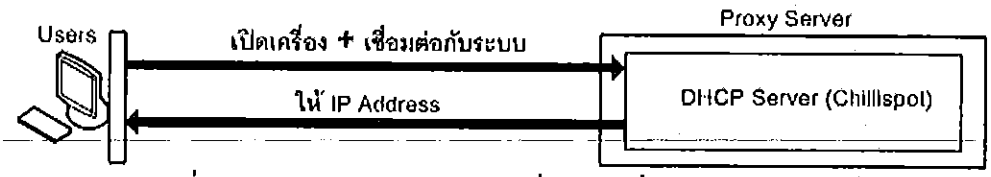
3.1.1 ส่วนที่ทำหน้าที่เป็น DHCP Server ทำหน้าที่ให้บริการแจกหมายเลข IP ให้กับเครื่องลูกข่าย (Users)

3.1.2 ส่วนที่ทำหน้าที่เป็น Authentication Gateway ทำหน้าที่ในการบังคับให้ Users ยืนยันตัวตนและตรวจสอบสิทธิ์ที่มีในระบบคอมพิวเตอร์ ก่อนมีการเข้าใช้งาน

3.1.3 ส่วนที่ทำหน้าที่เป็น Transparent Proxy Squid และ Firewall เป็นส่วนที่ตรวจสอบเว็บไซต์ หรือการกระทำต่างๆ ของ Users ซึ่งหากนอกเหนือจากกฎของ Proxy Squid และ Firewall แล้ว Proxy Server จะไม่อนุญาตให้มีกระทำนั้น แต่หากการกระทำไม่ได้ฝืนหรือผิดกฎของ Proxy Squid และ Firewall แล้ว Proxy Server จะอนุญาตให้มีการกระทำนั้นๆ ได้

3.2 การทำงานของระบบแต่ละส่วน

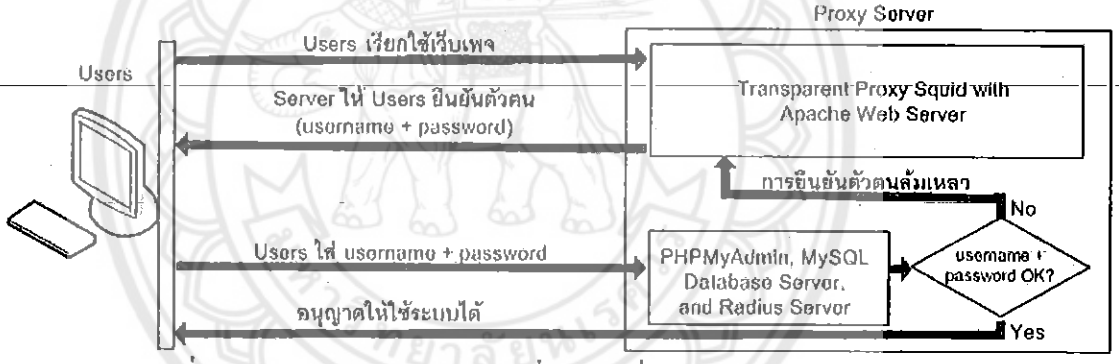
3.2.1 DHCP Server



รูปที่ 3.2 แสดงการทำงานในส่วนที่ทำหน้าที่เป็น DHCP Server

เมื่อเปิดเครื่องลูกข่าย (Users) ที่มีการเชื่อมต่อกับ Proxy Server เครื่องลูกข่ายก็จะได้รับหมายเลข IP (IP address) ซึ่งโปรแกรมที่ทำหน้าที่เป็นผู้แจกหมายเลข IP หรือที่เรียกว่า "DHCP Server" ก็คือโปรแกรม ChilliSpot ที่ได้ติดตั้งไว้ในเครื่อง Proxy Server นั่นเอง

3.2.2 Authentication Gateway

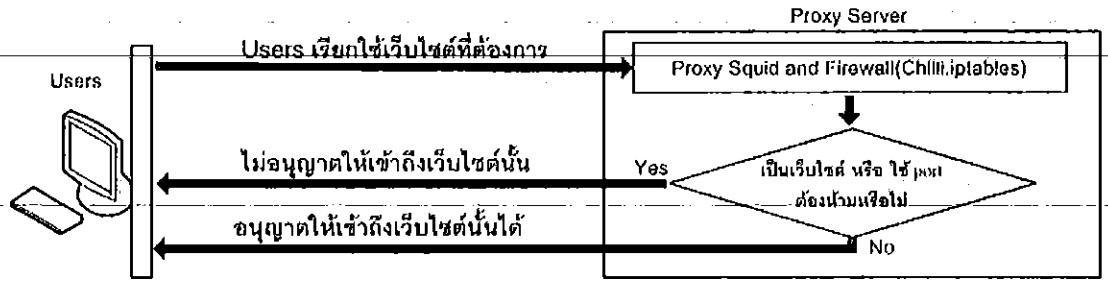


รูปที่ 3.3 แสดงการทำงานในส่วนที่ทำหน้าที่เป็น Authentication Gateway

เมื่อ Users ต้องการที่จะใช้งานอินเทอร์เน็ต การเรียกใช้ดังกล่าวก็จะถูกส่งไปยัง Proxy Server แล้วโปรแกรม Transparent Proxy Squid ที่ติดตั้งไว้ ก็ทำงาน โดยจะมีการส่งหน้าเว็บไปให้ Users เพื่อยืนยันตัวตนโดยให้ใส่ Username และ Password [4]

เมื่อ Users ทำการยืนยันตัวตนแล้ว ข้อมูลการยืนยันตัวตนจะถูกส่งมายัง Proxy Server โดยจะมีการตรวจเทียบกับข้อมูลการยืนยันตัวตนนั้นกับข้อมูลจากตารางของโปรแกรม PHPMyAdmin ซึ่งติดต่อกับฐานข้อมูลใน MySQL Database Server และมีการตรวจสอบสิทธิ์การใช้งานในระบบเครือข่ายคอมพิวเตอร์นี้ด้วยโปรแกรม FreeRADIUS ซึ่งทำหน้าที่เป็น RADIUS Server ซึ่งหากข้อมูลการยืนยันตัวตนถูกต้องก็จะอนุญาตให้มีการเข้าใช้ระบบคอมพิวเตอร์นี้ได้ แต่ถ้าไม่ถูกต้องก็จะมีการแสดงผลให้ทราบว่าการยืนยันตัวตนเกิดข้อผิดพลาด และให้ยืนยันตัวตนใหม่อีกครั้ง

3.2.3 Proxy Squid, Firewall, and Log Server



รูปที่ 3.4 แผนภาพการทำงานในส่วนที่ทำหน้าที่เป็น Foxy Squid, Firewall

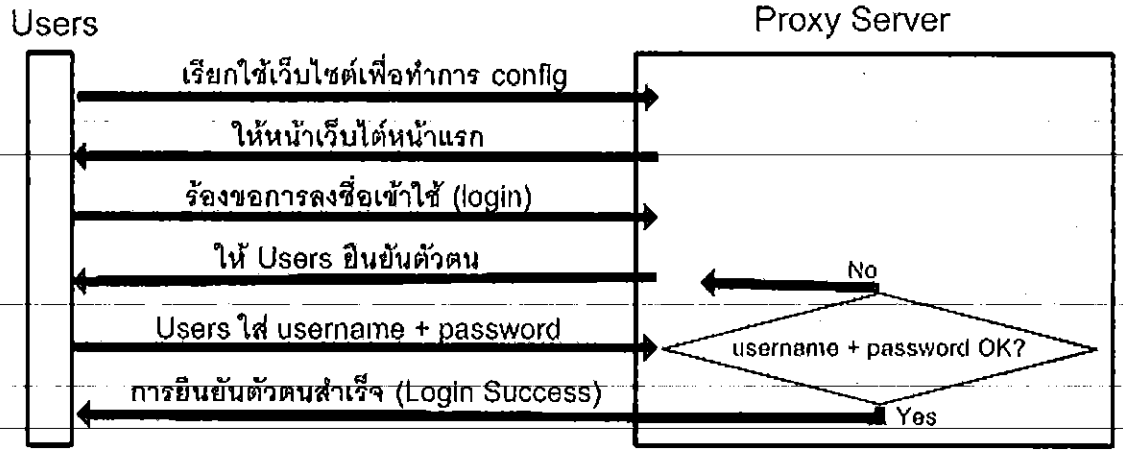
เมื่อผ่านขั้นตอนการยืนยันตัวตนแล้ว หาก Users มีการเรียกใช้เว็บไซต์ ข้อมูลการเรียกใช้ดังกล่าวจะถูกส่งผ่านมายัง Gateway Server จากนั้นโปรแกรม Squid ซึ่งทำหน้าที่เป็น Transparent Proxy Squid จะทำงานตามคำสั่งที่ได้กำหนดไว้ในไฟล์ที่ชื่อว่า "squid.conf" โดยตรวจสอบ URL ที่มีการเรียกใช้กับ URL ที่เก็บไว้ในไฟล์ที่ชื่อว่า "blacklists" ซึ่งหาก URL ที่มีการเรียกใช้มีอยู่ในไฟล์นี้ Proxy Server ก็จะไม่อนุญาตให้มีการเข้าถึงเว็บไซต์ดังกล่าว แต่ถ้าไม่มีก็จะอนุญาตให้มีการเข้าถึงเว็บไซต์นั้นได้ภายใต้กฎที่กำหนดไว้ในไฟล์ที่ชื่อว่า chilli.iptables ซึ่งทำหน้าที่เป็นกฎของ Firewall ด้วยความสามารถของโปรแกรม ChilliSpot

3.3 การพัฒนาเว็บแอปพลิเคชัน

3.3.1 การพัฒนาเว็บแอปพลิเคชันเพื่อใช้ เปิด/ปิด Port ใน Firewall

ในการพัฒนาเว็บแอปพลิเคชั่นเพื่อใช้เป็นส่วนติดต่อระหว่างผู้ใช้กับ Firewall นั้น ในโครงงานนี้จะมุ่งเน้นไปในด้านความสามารถในการ เปิด/ปิด Port ของ Firewall เป็นหลัก โดยพัฒนาเว็บไซต์ให้มีความสามารถในการเพิ่มกฎเข้าไปใน Firewall ได้ สามารถแก้ไข เปลี่ยนแปลง หรือลบกฎที่ตั้งไว้ได้ ทำให้ผู้ใช้ที่ไม่มีความรู้ในคำสั่ง iptables สามารถใช้ Firewall ผ่านเว็บแอปพลิเคชั่นเพื่อเพิ่มกฎในการ เปิด/ปิด Port ของ Firewall ได้อย่างสะดวกและง่ายดาย

การปรับเปลี่ยนกฎของ Firewall จะมีการพัฒนาเว็บแอปพลิเคชันเพื่อใช้ติดต่อเพื่อปรับเปลี่ยน และแก้ไขข้อมูลคำสั่งต่างๆ ในไฟล์ที่ชื่อว่า "chilli.iptables" ซึ่งเป็นไฟล์ที่เก็บกฎต่างๆ ของ Firewall ไว้



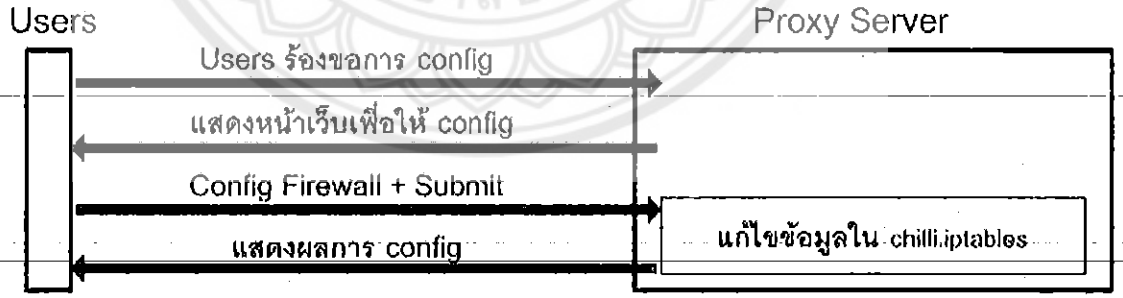
รูปที่ 3.5 แสดงการยืนยันตัวตนก่อนปรับเปลี่ยนการทำงานของ Proxy Server

จากรูปที่ 3.5 มีขั้นตอนการทำงานต่างๆ ดังนี้

1. เมื่อมีการร้องขอเพื่อทำการปรับเปลี่ยนกฎของ Firewall แล้ว Proxy Server จะแสดงเว็บไซต์หน้าแรกให้กับผู้ร้องขอ

2. Users ร้องขอการลงชื่อเข้าใช้โดยคลิกที่คำว่า "Login" แล้ว Proxy Server จะแสดงหน้าเว็บไซต์เพื่อให้แสดงตัวตน

3. เมื่อ Gateway Server ได้รับการยืนยันตัวตนจาก Users ยืนยันตัวตน ด้วยการพิมพ์ Username และ Password แล้ว Gateway Server จะทำการเทียบ Username กับ Password กับฐานข้อมูล ถ้าหากมีอยู่จริงและถูกต้อง จะแสดงผลให้ทราบว่าการยืนยันตัวตนสำเร็จ (Login Success) แต่ถ้าหากไม่มีอยู่จริงหรือไม่ถูกต้อง จะให้มีการยืนยันตัวตนใหม่



รูปที่ 3.6 แสดงขั้นตอนการปรับเปลี่ยนกฎของ Firewall

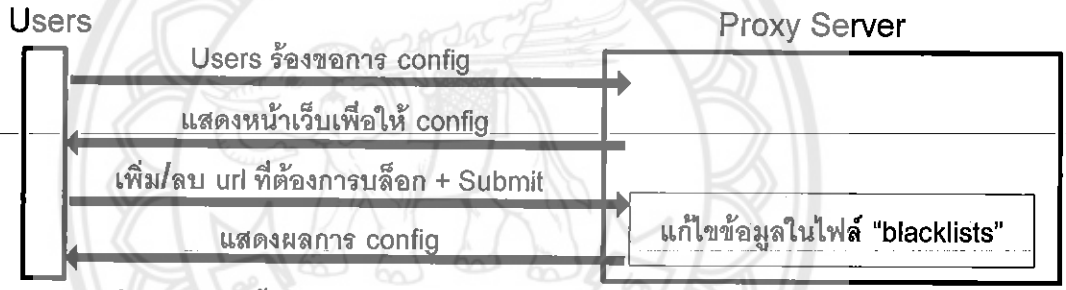
จากรูปที่ 3.6 มีขั้นตอนการในการปรับเปลี่ยนกฎของ Firewall ดังนี้

1. เมื่อผ่านขั้นตอนการยืนยันตัวตนแล้ว Users จะมีการร้องขอการปรับเปลี่ยนกฎของ Firewall โดยคลิกที่คำว่า "Config" แล้ว Gateway Server จะแสดงหน้าเว็บไซต์เพื่อให้ Users ปรับเปลี่ยนกฎของ Firewall

2. เมื่อ Users ได้ทำการปรับเปลี่ยนกฎของ Firewall แล้ว Gateway Server จะมีการปรับเปลี่ยนกฎตามความต้องการของ Users โดยแก้ไขข้อมูลคำสั่งในไฟล์ "chilli.iptables" และแสดงข้อความว่าการปรับเปลี่ยนกฎนั้นสำเร็จ เช่น Add Service Success เป็นต้น

3.3.2 การพัฒนาเว็บแอปพลิเคชันเพื่อใช้กำหนดเว็บไซต์ที่ต้องการห้ามไม่ให้มีการเข้าถึง

การพัฒนาเว็บแอปพลิเคชั่นเพื่อใช้กำหนดเว็บไซต์ที่ต้องการบล็อกเพื่อไม่ให้ Users สามารถเข้าถึงได้นั้น จะมีหลักการทำงานคล้ายๆ กับการพัฒนาเว็บแอปพลิเคชันเพื่อให้ Users สามารถใช้ในการปรับเปลี่ยนกฎของ Firewall [2] แต่แตกต่างกันตรงที่ต้องเขียนเพิ่มคำสั่งลงในไฟล์ "squid.conf" เพื่อให้มีการบล็อก URL ที่เก็บไว้ในไฟล์ๆ หนึ่งที่ได้สร้างไว้โดยเฉพาะ ซึ่งในโครงงานนี้ได้สร้างไฟล์ชื่อว่า "blacklists" และเขียนคำสั่งเพื่อให้เว็บแอปพลิเคชันสามารถแก้ไขข้อมูลในไฟล์นี้ได้ เพื่อเป็นการปรับเปลี่ยน URL ที่ต้องการบล็อกนั่นเอง ซึ่งเว็บแอปพลิเคชั่นที่ได้พัฒนาขึ้นนี้มีขั้นตอนการทำงานดังรูปที่ 3.7



รูปที่ 3.7 แสดงขั้นตอนการปรับเปลี่ยนเว็บไซต์ที่ต้องการห้ามไม่ให้มีการเข้าถึง

ขั้นตอนการทำงานสามารถอธิบายได้ดังนี้

1. เมื่อผ่านขั้นตอนการยืนยันตัวตนแล้ว Users จะมีการร้องขอการปรับเปลี่ยน URL ที่ต้องการบล็อกโดยคลิกคำว่า "Block" แล้ว Gateway Server จะแสดงหน้าเว็บไซต์เพื่อให้ปรับเปลี่ยน URL ที่ต้องการบล็อก

2. เมื่อ Users ได้ทำการปรับเปลี่ยน URL ที่ต้องการบล็อกแล้ว Gateway Server จะมีการปรับเปลี่ยนข้อมูลตามการปรับเปลี่ยนของ Users โดยแก้ไขข้อมูลในไฟล์ "blacklists" และแสดงข้อความว่าการปรับเปลี่ยนนั้นสำเร็จ

3.3.3 การพัฒนาเว็บแอปพลิเคชั่นเพื่อใช้ในการจัดการบัญชีรายชื่อผู้ใช้และผู้ดูและระบบ

3.3.3.1 การติดต่อฐานข้อมูลจะใช้ฟังก์ชันสำหรับใช้ติดต่อฐานข้อมูล ซึ่งมีรูปแบบการใช้งานดังนี้

mysql_connect($host,$user,$Password);

$host คือ IP Address ของเครื่องที่เก็บฐานข้อมูล

$user คือ ชื่อผู้ใช้งานในการติดต่อฐานข้อมูล

$Password คือ รหัสผ่านในการติดต่อฐานข้อมูล

3.3.3.2 เลือกฐานข้อมูล เมื่อติดต่อฐานข้อมูลได้แล้ว ให้เลือกฐานข้อมูลโดยใช้คำสั่ง

mysql_select_db("$db_name");

$db_name คือ ชื่อของฐานข้อมูลที่ต้องการเรียกใช้ เมื่อติดต่อฐานข้อมูลได้แล้วสามารถเข้าไปจัดการข้อมูลได้ทันที

3.3.3.3 การเพิ่มข้อมูลลงในฐานข้อมูล

ในการเพิ่มข้อมูลจะต้องสร้างคำสั่งไว้ในตัวแปร แล้วใช้คำสั่งที่อยู่ในตัวแปรนั้นผ่านฟังก์ชันที่ใช้สำหรับเพิ่มข้อมูล

$sql = "INSERT INTO $tb_user_name VALUES('$usr','$passwd')";

$usr คือ ชื่อผู้ใช้

$tb_name คือ ชื่อของตาราง

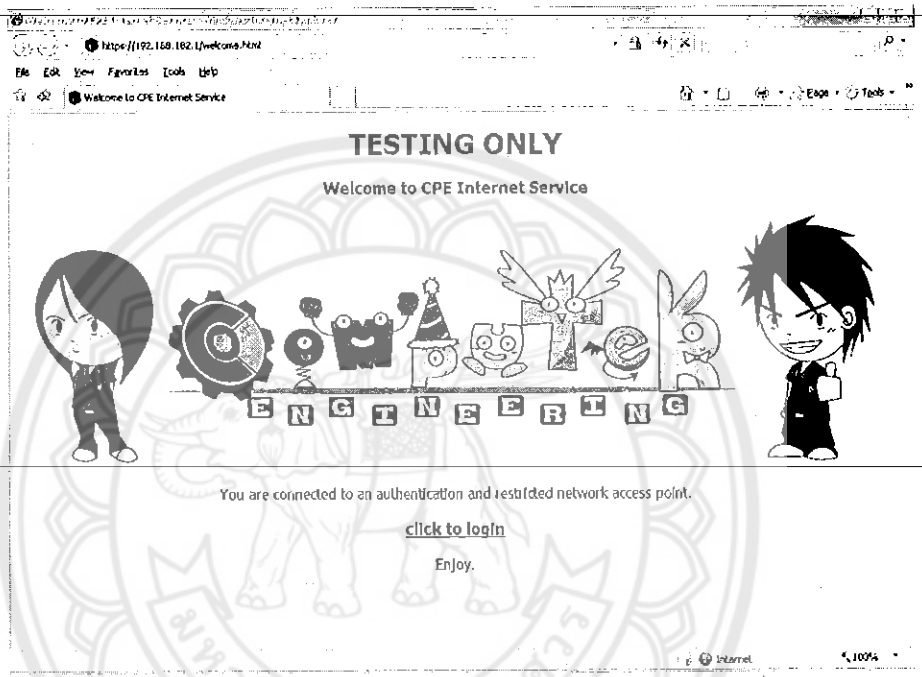
โครงงานนี้จะมีการใช้การเข้ารหัส Password แบบ MD5 เพื่อให้ระบบมีความปลอดภัยมากยิ่งขึ้นด้วยคำสั่ง $passwd = md5($pwd);

บทที่ 4

การทดลอง

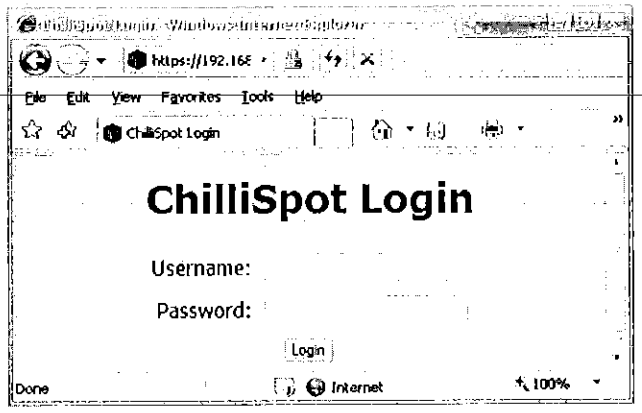
4.1 การแสดงผลในส่วนของ Authentication

เมื่อมีการเรียกใช้เว็บไซต์ต่างๆ Proxy Server แสดงหน้าเว็บไซต์แสดงข้อความต้อนรับ ดังรูปที่ 4.1 ซึ่งหากต้องการใช้งานระบบ ให้คลิกคำว่า “click to login”



รูปที่ 4.1 แสดงลักษณะหน้าเว็บแรกเมื่อมีการเรียกใช้ระบบ

หลังจากนั้น จะมีหน้าเว็บเพื่อให้ใส่ Username กับ Password ซึ่งเป็นการยืนยันตัวตนก่อนเข้าใช้ระบบ ดังรูปที่ 4.2



รูปที่ 4.2 แสดงลักษณะหน้าเว็บที่มีการยืนยันตัวตน

ถ้าหากมีข้อผิดพลาดในการยืนยันตัวตนเกิดขึ้น เช่น Username หรือ Password ไม่ถูกต้อง Proxy Server จะมีการแสดงหน้าเว็บไซต์เพื่อแสดงข้อผิดพลาด และให้มีการยืนยันตัวตนอีกครั้ง

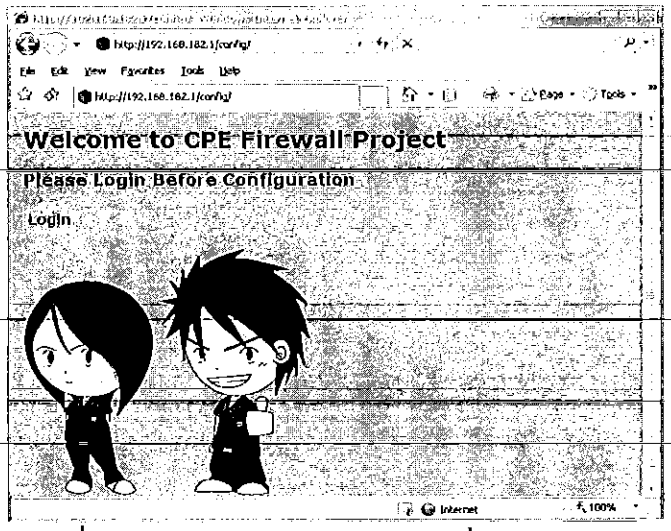
รูปที่ 4.3 แสดงลักษณะหน้าเว็บที่เกิดข้อผิดพลาดในการยืนยันตัวตน

ถ้าหากการยืนยันตัวตนมีความถูกต้อง Proxy Server จะแสดงข้อความว่าได้เข้าใช้ระบบแล้ว และมีข้อความว่า "Logout" สำหรับคลิกเมื่อไม่ต้องการใช้งานระบบ

รูปที่ 4.4 แสดงลักษณะหน้าเว็บที่มีการยืนยันตัวตนสำเร็จ

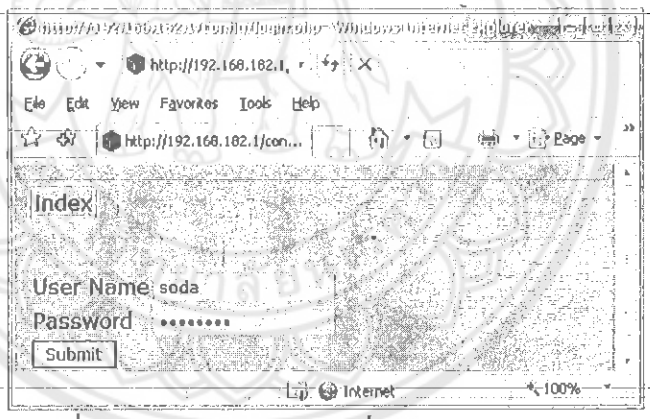
4.2 ลักษณะการแสดงผลของเว็บแอปพลิเคชันก่อนการปรับเปลี่ยนการทำงานของ Proxy Server

การเริ่มทำงานของเว็บแอปพลิเคชันที่พัฒนาขึ้นเพื่อใช้ปรับเปลี่ยนการทำงานของ Proxy Server นี้ จะเริ่มจากการใช้ Web Browser เปิด http://192.168.182.1/config แล้วจะมีการแสดงผลดังรูปที่ 4.5

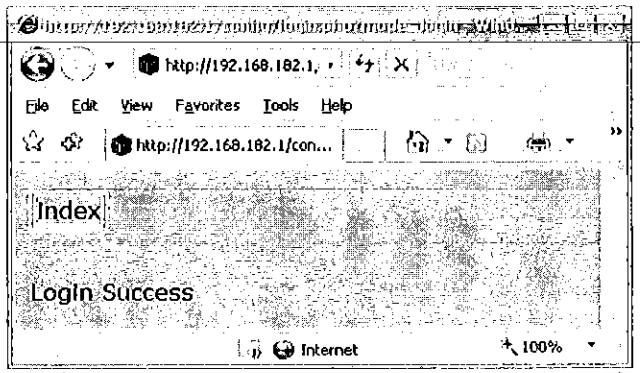


รูปที่ 4.5 แสดงหน้าเว็บไซต์หน้าแรกเมื่อมีการเรียกใช้เพื่อปรับเปลี่ยนการทำงานของ Proxy Server

Users ต้องมีการลงชื่อเข้าใช้โดยการคลิก "Login" แล้วจะมีการแสดงผลดังรูปที่ 4.6 ซึ่งหากการลงชื่อเข้าใช้ไม่สำเร็จ หรือมีข้อผิดพลาด จะแสดงผลดังรูปที่ 4.6 แต่ถ้าหากสำเร็จจะแสดงผลดังรูปที่ 4.7

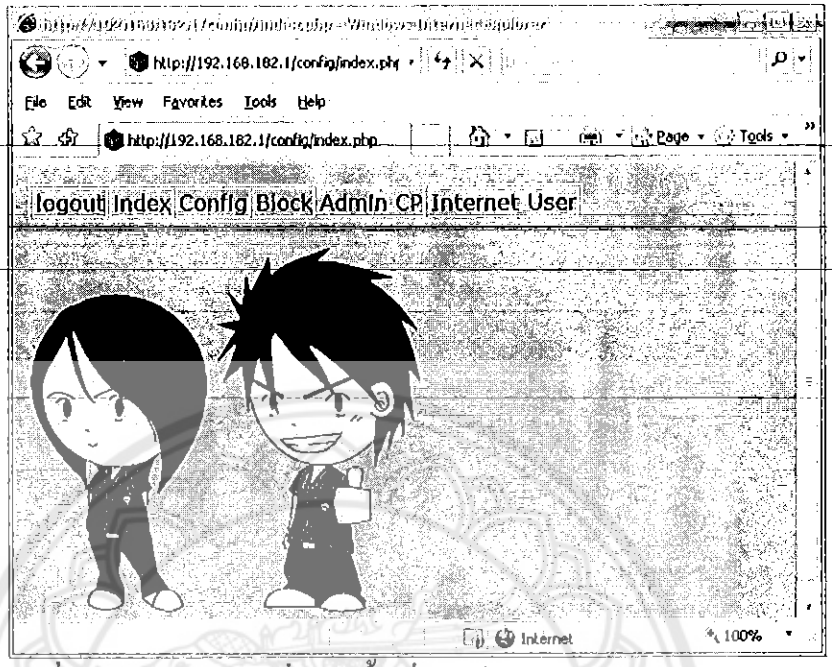


รูปที่ 4.6 แสดงหน้าเว็บไซต์เพื่อให้มีการยืนยันตัวตน



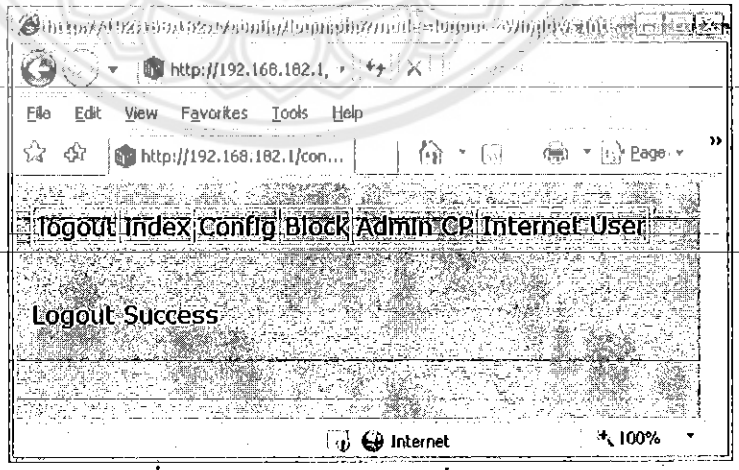
รูปที่ 4.7 แสดงหน้าเว็บไซต์เมื่อการยืนยันตัวตนสำเร็จ

หลังจากผ่านการยืนยันตัวตนเสร็จแล้ว เมื่อคลิกคำว่า “index” จะมีตัวเลือกที่จัดทำขึ้นเพื่อใช้เป็นส่วนติดต่อกับ Proxy Server ดังรูปที่ 4.8



รูปที่ 4.8 แสดงตัวเลือกที่จัดทำขึ้นเพื่อใช้เป็นส่วนติดต่อกับ Proxy Server

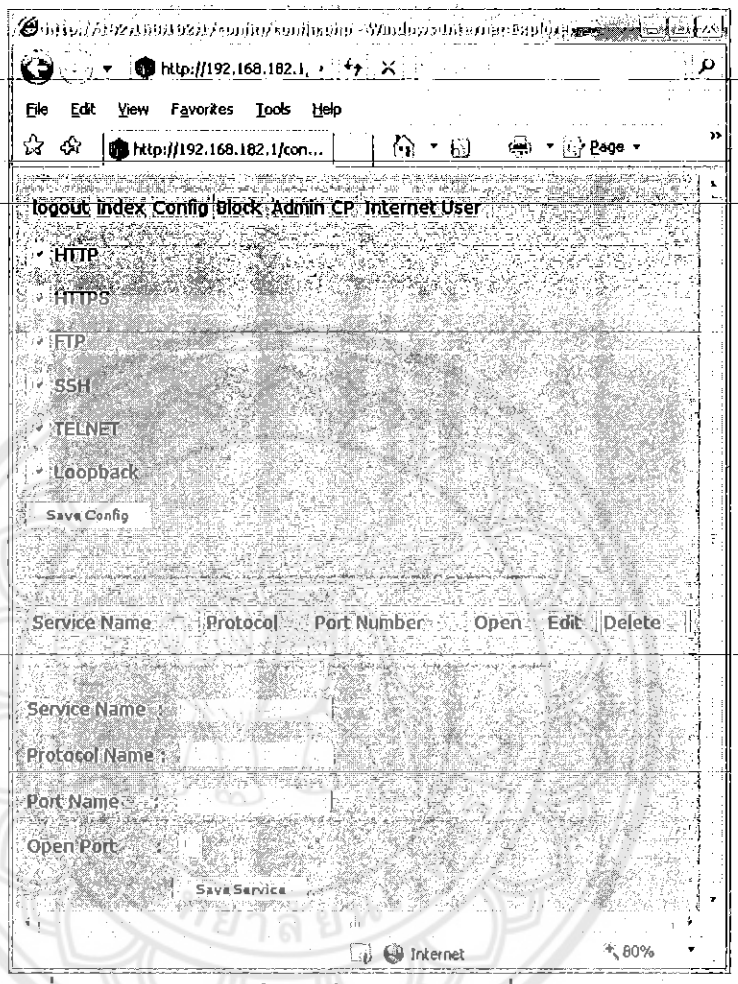
เมื่อ Users ใช้เว็บแอปพลิเคชันเพื่อปรับเปลี่ยนการทำงานของ Proxy Server เสร็จแล้ว ควรออกจากการใช้งาน โดยทำการคลิกที่คำว่า “logout” แล้วจะมีการแสดงผลว่าการออกจากการใช้งานสำเร็จ “Logout Success” ดังรูปที่ 4.9



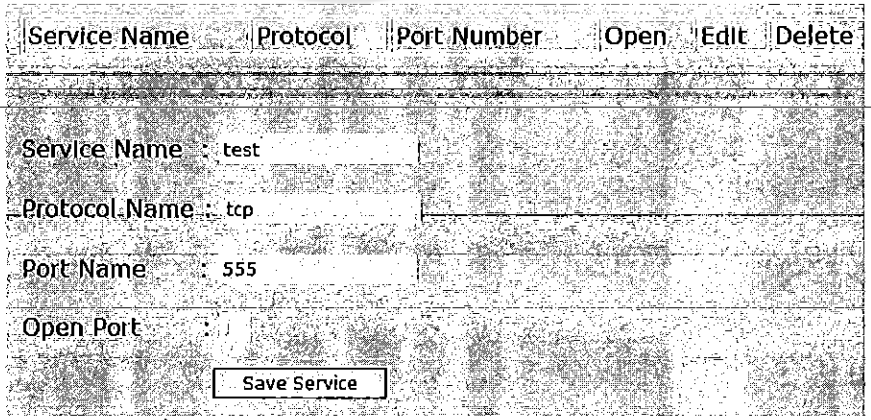
รูปที่ 4.9 แสดงหน้าเว็บไซต์เมื่อออกจากระบบ

4.3 การใช้งาน Firewall ผ่านเว็บแอปพลิเคชันเพื่อ เปิด/ปิด Port

หลังจากผ่านการยืนยันตัวตนแล้ว เมื่อคลิกคำว่า "index" แล้วคลิกคำว่า "Config" ก็จะมีการแสดงหน้าเว็บไซต์ ให้สามารถปรับเปลี่ยนกฎต่างๆ ของ Firewall ดังรูปที่ 4.10

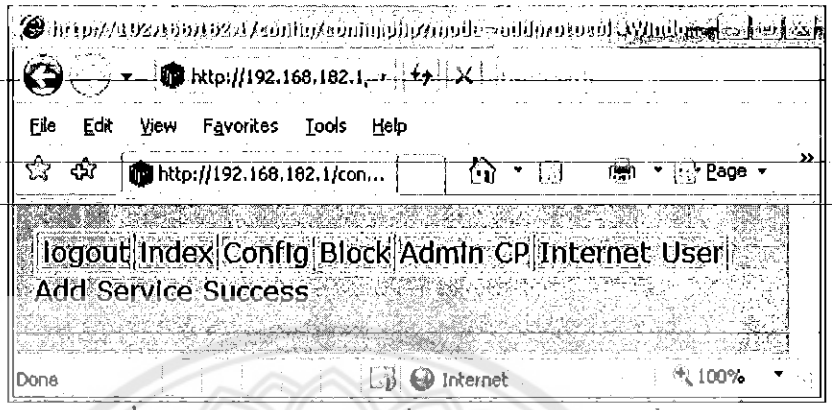


รูปที่ 4.10 แสดงหน้าเว็บไซต์สำหรับปรับเปลี่ยนกฎของ Firewall

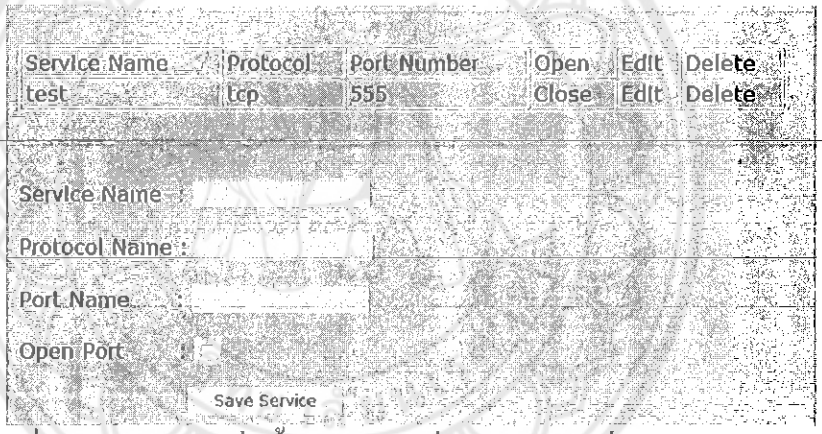


รูปที่ 4.11 แสดงตัวอย่างการปรับเปลี่ยนกฎของ Firewall

จากการปรับเปลี่ยนกฎของ Firewall ในรูปที่ 4.11 แล้วคลิกคำว่า “Save Service” ก็จะมีการแสดงผลว่าการปรับเปลี่ยนกฎของ Firewall สำเร็จ ดังรูปที่ 4.12 และเมื่อคลิกคำว่า “Config” จะมีตารางเพิ่มขึ้นตามข้อมูลที่ได้เพิ่มเข้าไป ดังรูปที่ 4.13



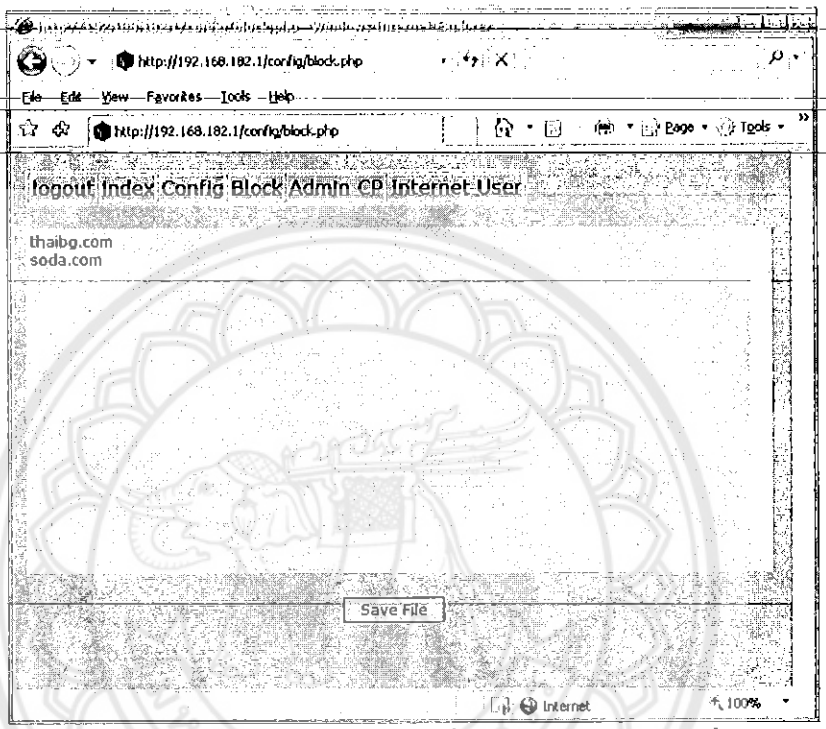
รูปที่ 4.12 แสดงการปรับเปลี่ยนกฎของ Firewall เมื่อสำเร็จ



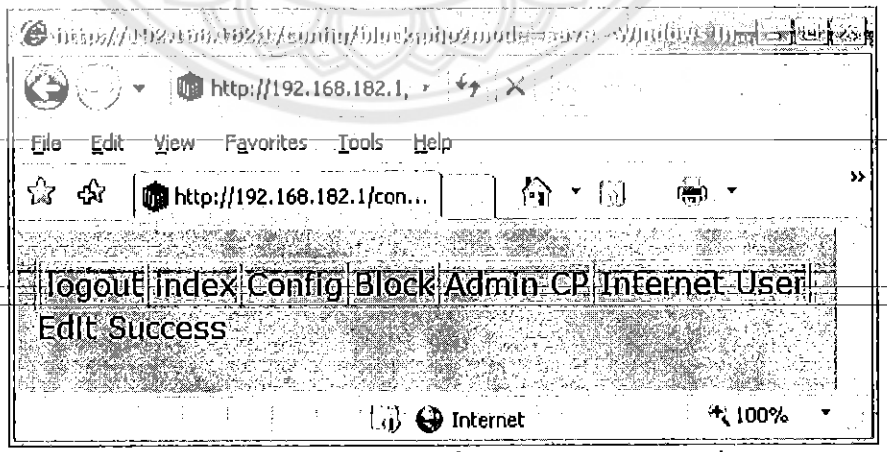
รูปที่ 4.13 แสดงการเพิ่มขึ้นของตารางเมื่อมีการปรับเปลี่ยนกฎของ Firewall

4.4 การใช้งาน Squid ผ่านเว็บแอปพลิเคชันเพื่อบล็อกการเข้าถึงเว็บไซต์

หลังจากผ่านการยืนยันตัวตนแล้ว เมื่อคลิกคำว่า "index" แล้วคลิกคำว่า "Block" ก็จะมีการแสดงหน้าเว็บไซต์ ให้สามารถเพิ่มหรือลบ URL ของเว็บไซต์ที่ต้องการบล็อก ดังรูปที่ 4.14 และเมื่อคลิกคำว่า "Submit" ก็จะแสดงการแก้ไขข้อมูลสำเร็จ "Edit Success" ดังรูปที่ 4.15



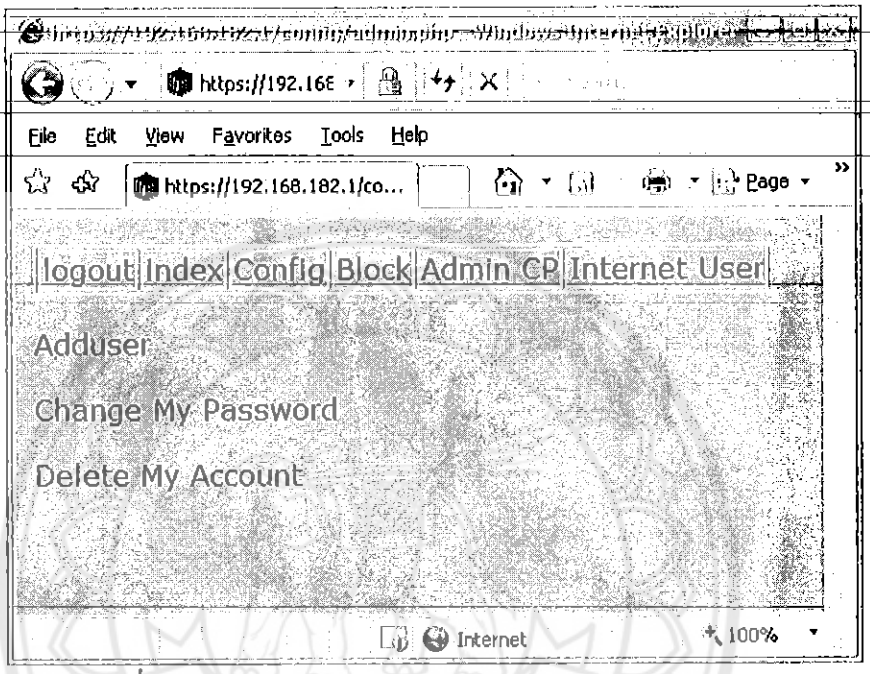
รูปที่ 4.14 แสดงหน้าเว็บไซต์สำหรับปรับเปลี่ยน URL ของเว็บไซต์ที่ต้องการบล็อก



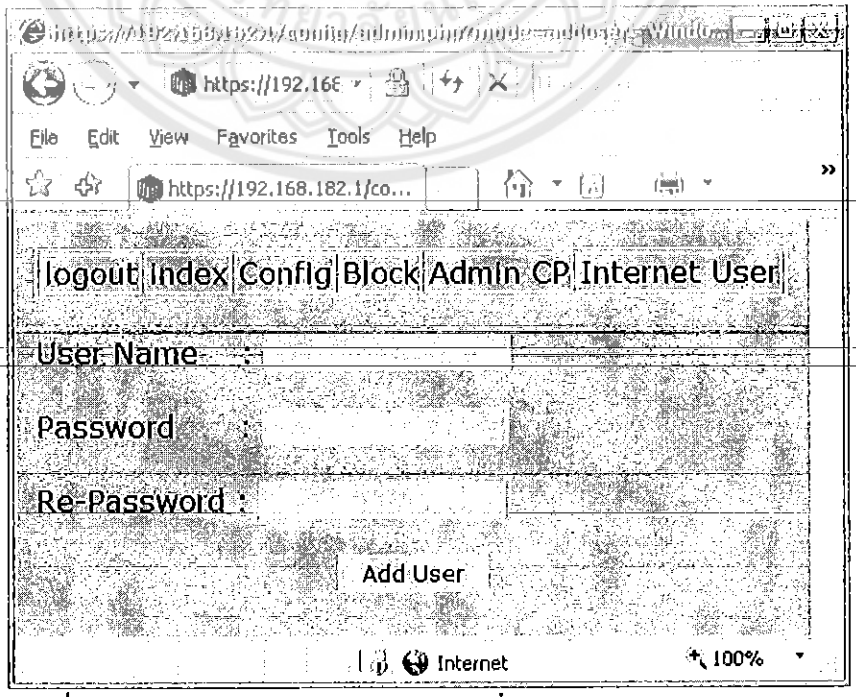
รูปที่ 4.15 แสดงหน้าเว็บไซต์เมื่อมีการปรับเปลี่ยน URL ของเว็บไซต์ที่ต้องการบล็อกสำเร็จ

4.5 การใช้เว็บแอปพลิเคชันในการจัดการกับบัญชีผู้ดูแลระบบ

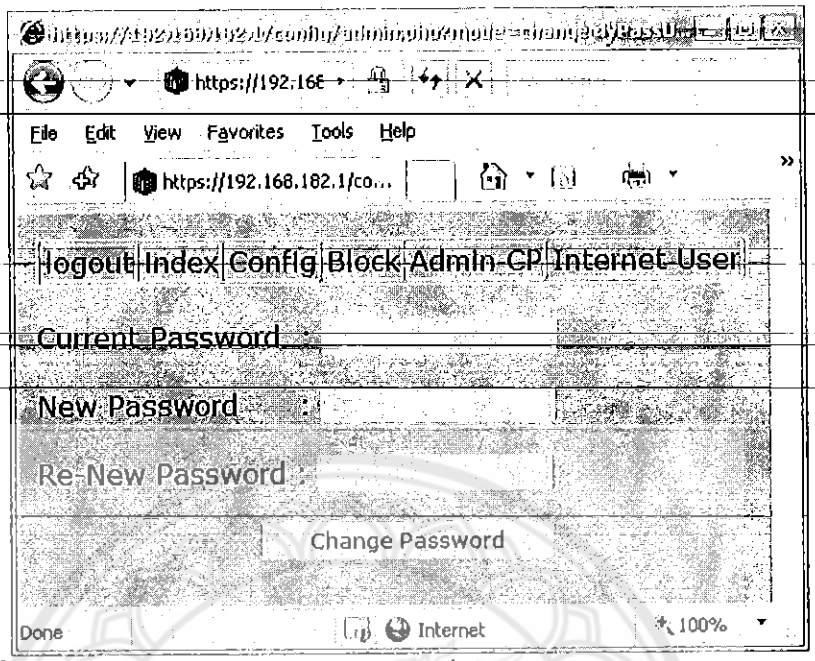
หลังจากผ่านการยืนยันตัวตนแล้ว เมื่อต้องการจัดการกับบัญชีผู้ดูแลระบบให้คลิกคำว่า "Admin CP" โดยจะมีให้เลือกว่าจะเพิ่มผู้ใช้ (Adduser), เปลี่ยนรหัสผ่าน (Change My Password) และลบผู้ใช้ (Delete My Account) โดยแต่ละตัวเลือกจะมีรูปแบบการแสดงผลดังต่อไปนี้



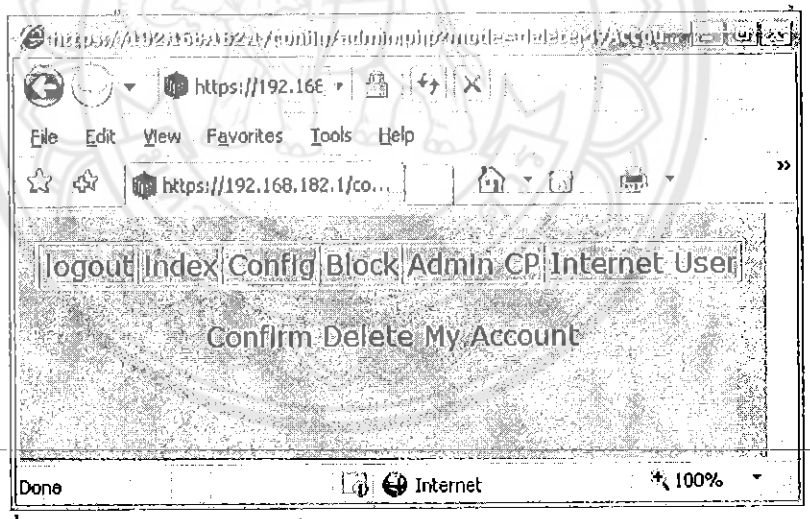
รูปที่ 4.16 แสดงหน้าเว็บไซต์สำหรับจัดการบัญชีผู้ดูแลระบบ



รูปที่ 4.17 แสดงหน้าเว็บไซต์สำหรับการเพิ่มบัญชีผู้ดูแลระบบ (Adduser)



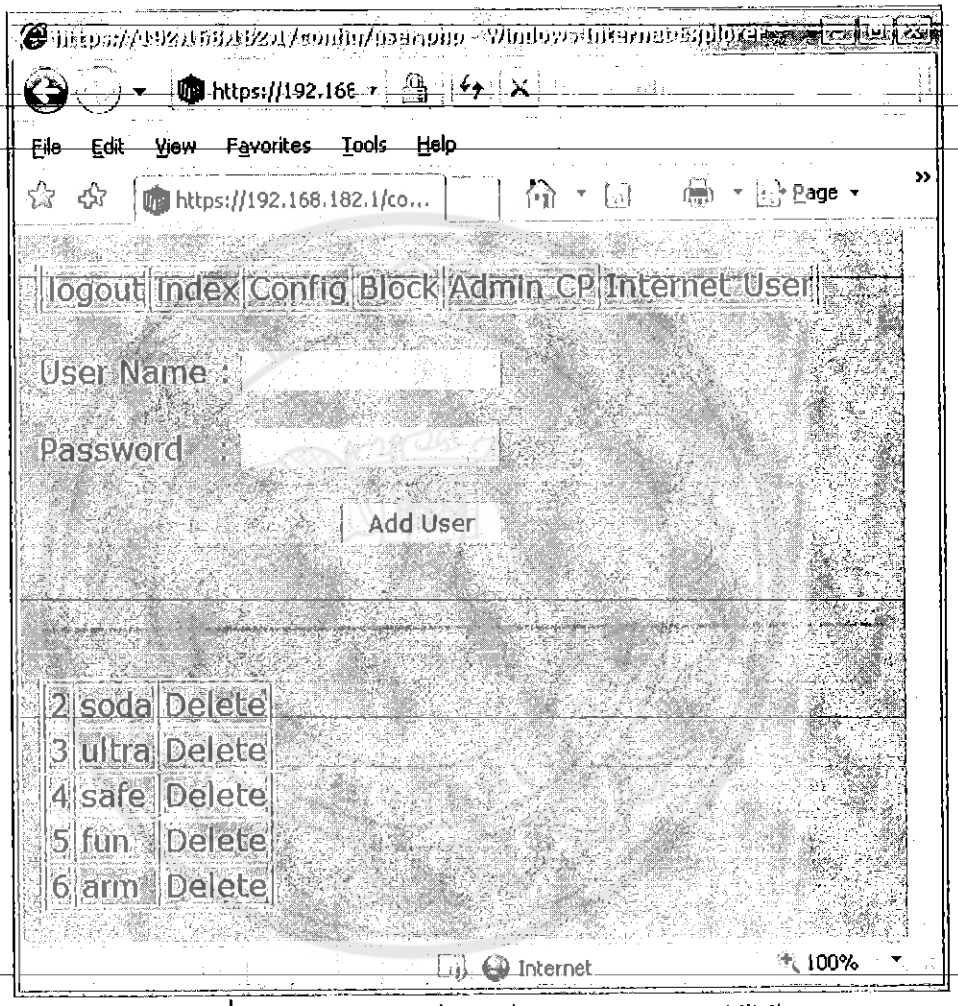
รูปที่ 4.18 แสดงหน้าเว็บไซต์สำหรับการเปลี่ยนรหัสผ่าน (Change My Password)



รูปที่ 4.19 แสดงหน้าเว็บไซต์สำหรับการลบผู้ดูแลระบบ (Delete My Account)

4.6 การใช้เว็บแอปพลิเคชันในการจัดการกับบัญชีผู้ใช้

หลังจากผ่านการยืนยันตัวตนแล้ว เมื่อต้องการจัดการกับบัญชีผู้ใช้ให้คลิกคำว่า "Internet User" โดยจะแบ่งส่วนการทำงานออกเป็น 2 ส่วน คือ ส่วนแรกจะมีช่องว่างสำหรับพิมพ์ชื่อผู้ใช้ (User Name) และรหัสผ่าน (Password) เพื่อเพิ่มจำนวนผู้ใช้ อีกส่วนหนึ่งจะแสดงรายชื่อผู้ใช้ทั้งหมดซึ่งสามารถลบผู้ใช้ออกได้เพียงคลิกคำว่า "Delete"



รูปที่ 4.20 แสดงหน้าเว็บไซต์สำหรับจัดการบัญชีผู้ใช้

บทที่ 5
สรุปและข้อเสนอแนะ

5.1 สรุปผลการทดลองและแนวทางในการพัฒนาต่อ

จากการทดลองของโครงงานนี้สรุปได้ว่า Proxy Server ที่พัฒนาขึ้นสามารถทำหน้าที่เป็น DHCP Server, Radius Server, Authentication Gateway และ Firewall สามารถใช้เว็บแอปพลิเคชันเพื่อปรับเปลี่ยนการทำงานของ Firewall ได้ แต่รูปแบบการใช้งานของเว็บเอปพลิเคชันยังไม่ครอบคลุมทุกฟังก์ชันการปรับเปลี่ยนการทำงานของ Firewall ทำได้เพียงเปิด/ปิด Port เท่านั้น ส่วนการใช้งานอื่นที่ได้เพิ่มขึ้นมา นั่นก็คือการเพิ่มความสามารถในการการจำกัดการเข้าถึงเว็บไซต์ต่างๆ ด้วยการบล็อก URL และสามารถเพิ่มหรือลบ URL ที่ไม่ต้องการให้มีการเข้าถึงผ่านทางเว็บแอปพลิเคชันได้

ดังนั้นแนวทางการพัฒนาต่อก็คือการพัฒนาให้เว็บแอปพลิเคชันให้สามารถปรับเปลี่ยนการทำงานของ Firewall ได้หลากหลายมากกว่านี้ และสามารถจำกัดการเข้าถึงเว็บไซต์ต่างๆ ด้วยการกำหนดคำสำคัญที่ปรากฏอยู่บนหน้าเว็บไซต์ที่ไม่ต้องการให้มีการเข้าถึงได้ โดยเว็บแอปพลิเคชันที่จะพัฒนาต่อควรมีรูปแบบการนำเสนอที่น่าสนใจขึ้น มีการแสดงสถานะของฟังก์ชั่นการทำงานต่างๆ ของ Proxy Server นอกจากนี้แล้วยังสามารถพัฒนา Proxy Server นี้ให้สามารถจัดเก็บข้อมูลการจราจรทางคอมพิวเตอร์ได้ ตามมาตรา 26 ภายในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 โดยการติดตั้งและตั้งค่าการใช้งานโปรแกรม Syslog-ng ซึ่งเป็นโปรแกรมฟรีสำหรับระบบปฏิบัติการลินุกซ์ ที่ทำหน้าที่เป็น Logging Server เพื่อใช้สำหรับจัดเก็บข้อมูลการจราจรคอมพิวเตอร์โดยเฉพาะ

5.2 ปัญหาข้อเสนอแนะและแนวทางแก้ไข

5.2.1 การติดตั้งระบบปฏิบัติการ รวมถึงการติดตั้งโปรแกรมต่างๆ ให้กับเครื่อง Proxy Server ควรมีการศึกษาข้อมูลการทำงานของโปรแกรมต่างๆ ให้เกิดความเข้าใจ เพื่อให้การติดตั้งและการปรับตั้งค่าต่างๆ ของโปรแกรมเหมาะสมกับการใช้งาน และระบบภายในองค์กร

5.2.2 ควรมีการตรวจเช็คอุปกรณ์ต่างๆ รวมทั้งสภาพความสามารถในการใช้งานให้ดีก่อนติดตั้งระบบปฏิบัติการ และโปรแกรมต่างๆ เพื่อไม่เกิดข้อผิดพลาดจากปัญหาด้าน Hardware

5.2.3 ในการกำหนดรหัสผ่านต่างๆ ควรจะเป็นรหัสที่ผู้ติดตั้งหรือผู้ดูแลระบบจำได้ดี เนื่องจากมีการติดตั้งหลายโปรแกรมลงบน Proxy Server ซึ่งในบางโปรแกรมต้องมีรหัสผ่านในการใช้งาน จึงอาจนำมาซึ่งความสับสนของผู้ใช้งานหรือผู้ดูแลระบบได้ในภายหลัง

เอกสารอ้างอิง

[1] Dream Group 2542. "ถาม-ตอบ เรื่อง Common Gateway Interface (FAQ)." [Online]. Available. http://tutor.dserver.org/perl/cgi_faq.html. 1999.

[2] Kridsana Meesuk. "ตัวอย่างการบล็อกเว็บไม่พึงประสงค์ (ลามก)." [Online]. Available : http://www.thaislack.com/tips/block_squid.html. 2006.

[3] Modoeye Administrator. "เทคนิคการใช้งาน MD5 เพื่อเข้ารหัสข้อมูล." [Online]. Available : http://forum.modoeye.com/26/98/เทคนิคการใช้งาน_MD5_เพื่อเข้ารหัสข้อมูล. 2005.

[4] SiPA and ATSI. "คู่มือประกอบการฝึกอบรมเชิงปฏิบัติการ การติดตั้ง Authentication." [Online]. Available : http://61.7.253.244/syslog-ng. 2007.

[5] ปราการ โกลากุล. "ความรู้พื้นฐานเกี่ยวกับไฟร์วอลล์ (Firewall)." [Online]. Available : http://www.thaicert.org/paper/firewall/fwbasics.php. 2001.

[6] ผู้ช่วยศาสตราจารย์ ดร.ภาสกร เรืองรอง. "Common Gateway Interface (CGI)." [Online]. Available : http://www.thaiwbi.com/course/asp/introduc.html. 2007.

[7] ภูวดล ด่านระหาญ. "Linux 2.4 Stateful Firewall : IPTABLES." [Online]. Available : http://www.thaicert.nectec.or.th/paper/firewall/iptables.php. 2001

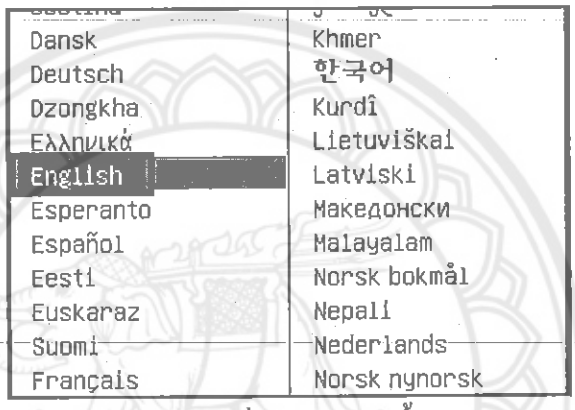
[8] สมศักดิ์ โชคชัยชุติกุล. **PHP5**. 1st Ed. กรุงเทพฯ : บริษัท โปรวิชั่น จำกัด. 2547.

ภาคผนวก ก

การติดตั้งและตั้งค่าการใช้งาน ระบบปฏิบัติการ Linux

ก.1. การติดตั้งระบบปฏิบัติการ Linux

ก.1.1 เมื่อใส่แผ่นสำหรับติดตั้งระบบปฏิบัติการ Linux แล้ว Restart จะมีการแสดงผล ดังรูปที่ ก.1 ให้เลือกภาษาที่จะใช้ในการติดตั้ง โดยในที่นี้จะเลือกภาษาอังกฤษ แล้วกดปุ่ม Enter บนแป้นพิมพ์

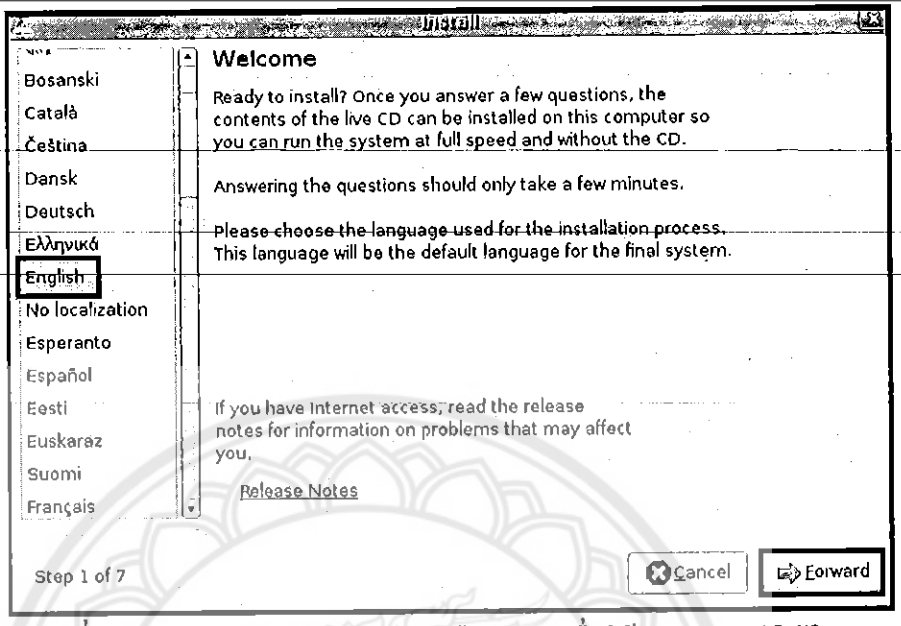


รูปที่ ก.1 แสดงการเลือกภาษาที่ใช้ในการติดตั้ง ระบบปฏิบัติการ Linux

ก.1.2 หลังจากการเลือกภาษาแล้ว จะมีการแสดงผลดังรูปที่ ก.2 ให้ทำการเลือก Install Ubuntu แล้วกดปุ่ม Enter ที่แป้นพิมพ์

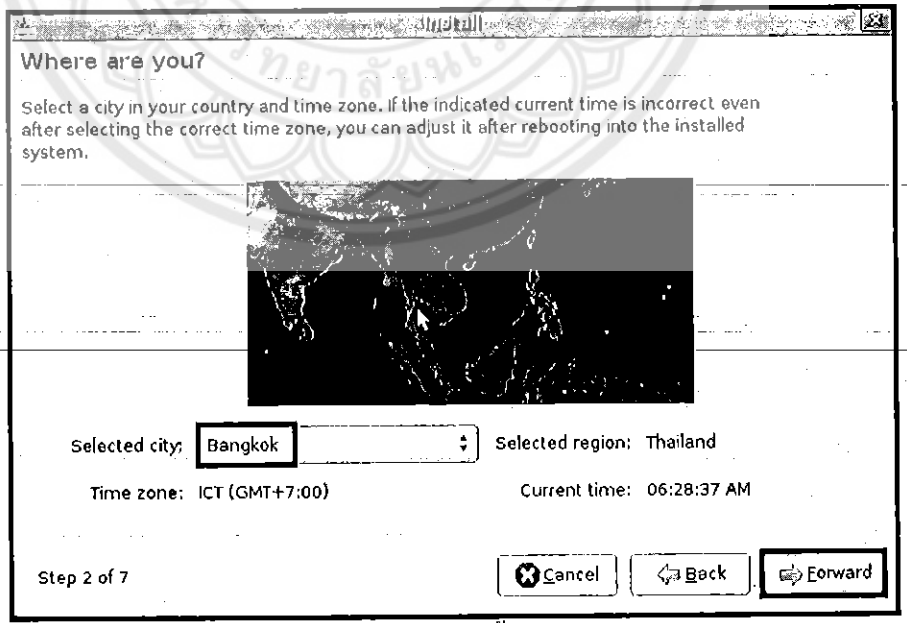
รูปที่ ก.2 แสดงหน้าต่างสำหรับเข้าสู่การติดตั้งโปรแกรม

ก.1.3 เลือกภาษาหลักสำหรับการใช้งานระบบปฏิบัติการ โดยเลือกเป็นภาษาอังกฤษ หลังจากนั้น คลิกที่ Forward ดังรูปที่ ก.3



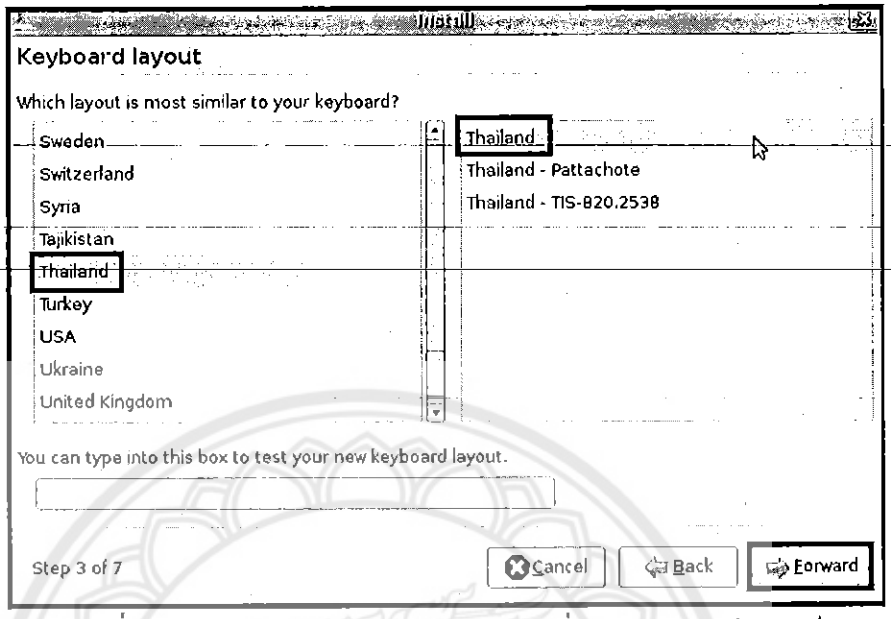
รูปที่ ก.3 แสดงหน้าต่างสำหรับการเลือกภาษาเพื่อใช้งานระบบปฏิบัติการ

ก.1.4 เลือกเขตพื้นที่ให้เหมาะกับช่วงเวลาสากล โดยหากเป็นประเทศไทยจะเลือกที่ Bangkok จากนั้นคลิกที่ Forward ดังรูปที่ ก.4



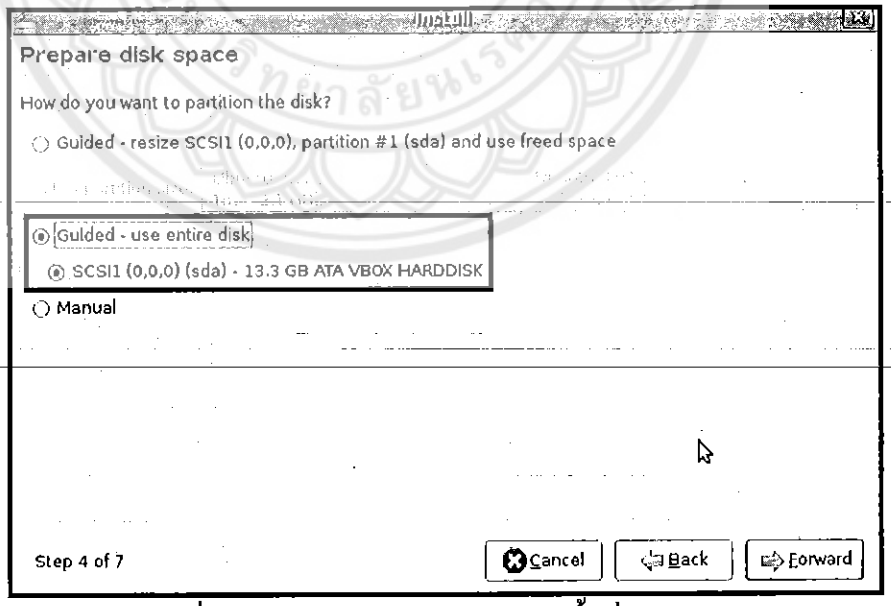
รูปที่ ก.4 แสดงหน้าต่างสำหรับเลือกเขตพื้นที่เพื่อให้เหมาะกับช่วงเวลาสากล

ก.1.5 ภาษาที่ได้กำหนดไว้อัตโนมัติจะเป็นภาษาอังกฤษ ดังนั้นจึงให้เลือกภาษาที่สอง เพื่อให้สามารถใช้งานได้สะดวกขึ้น จึงเลือกภาษาไทย (Thailand) จากนั้นคลิก Forward ดังรูปที่ ก.5



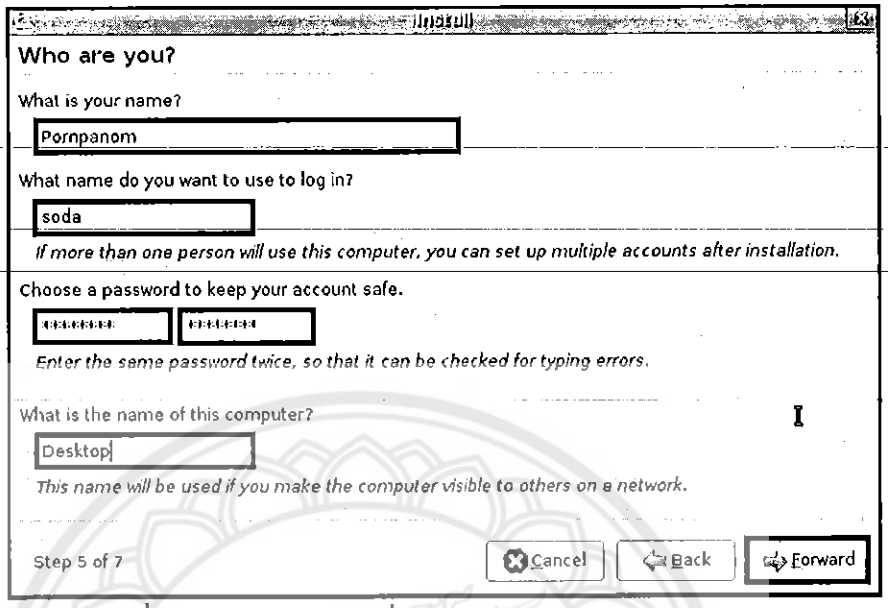
รูปที่ ก.5 แสดงหน้าต่างสำหรับเลือกภาษาที่สองสำหรับแป้นพิมพ์

ก.1.6 เลือกพื้นที่ Hard disk สำหรับติดตั้งระบบปฏิบัติการ เพื่อความง่ายและลดขั้นตอนในการติดตั้งควรเลือกแบบ Use entire disk แล้วคลิก Forward ดังรูปที่ ก.6



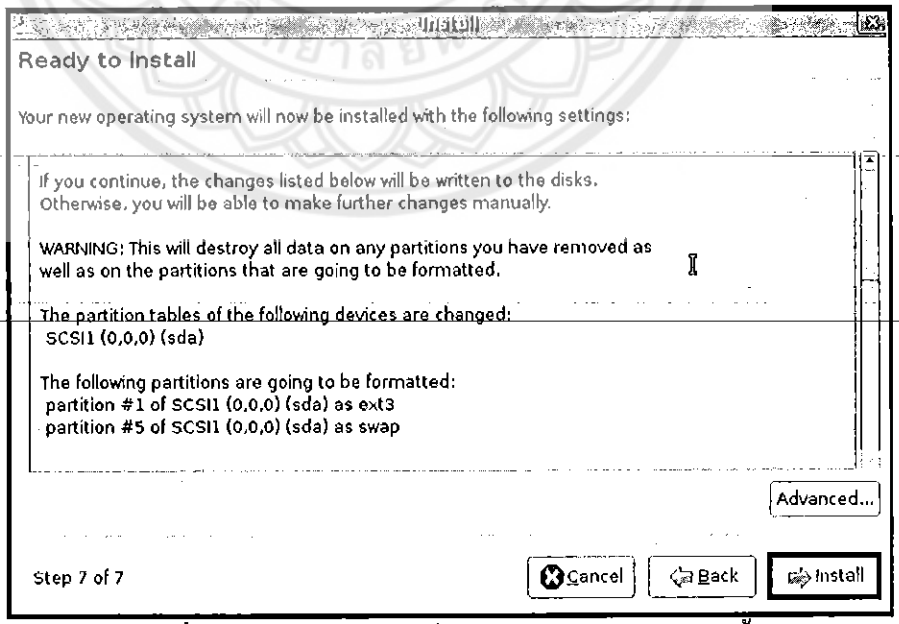
รูปที่ ก.6 แสดงหน้าต่างสำหรับเลือกพื้นที่ Hard disk

ก.1.7 พิมพ์ข้อมูลต่างๆ ตามความเหมาะสม ตามรูปที่ ก.7 โดยสิ่งสำคัญที่สุดคือ Password เมื่อพิมพ์ไปแล้วนั้นต้องจำได้ และตรงกันทั้งสองช่อง จากนั้นคลิก Forward



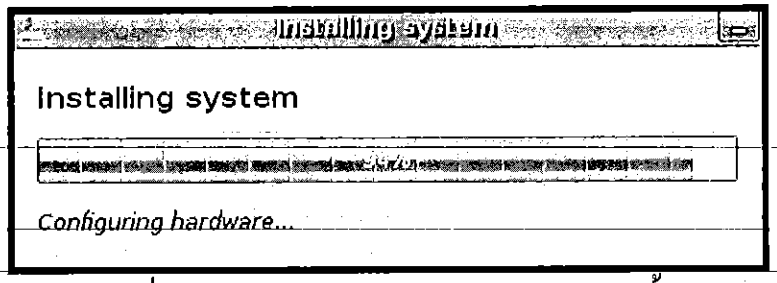
รูปที่ ก.7 แสดงหน้าต่างเพื่อกำหนด Username และ Password

ก.1.8 ในขั้นตอนนี้จะแสดงข้อมูลต่างๆ ที่ได้กำหนดไว้ เพื่อให้ผู้ติดตั้งได้ตรวจสอบดูให้แน่ใจอีกครั้ง หากมีข้อผิดพลาดสามารถกลับไปแก้ไขโดยคลิกที่ Back แต่หากแน่ใจว่าไม่มีข้อผิดพลาดให้คลิกที่ Install เพื่อติดตั้ง ดังรูปที่ ก.8

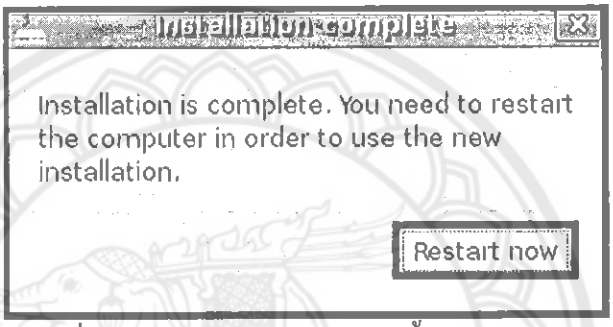


รูปที่ ก.8 แสดงหน้าต่างเพื่อตรวจสอบข้อมูลก่อนติดตั้ง

ก.1.9 หลังจากคลิก Install เพื่อเริ่มติดตั้ง จะมีการแสดงความคืบหน้าในการติดตั้ง ดังรูปที่ ก.9 และเมื่อการติดตั้งเสร็จสมบูรณ์ จะมีหน้าต่างแสดงผลดังรูปที่ ก.10



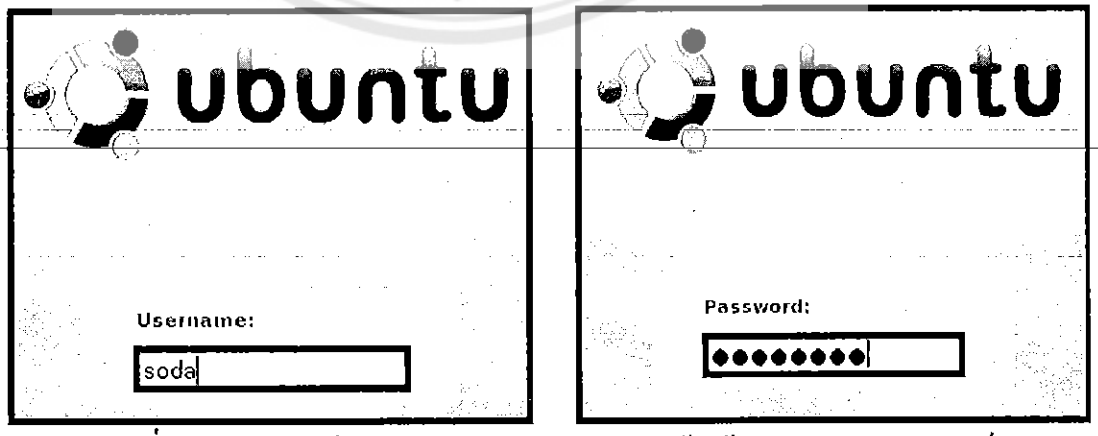
รูปที่ ก.9 แสดงหน้าต่างความคืบหน้าในการติดตั้ง



รูปที่ ก.10 แสดงหน้าต่างการติดตั้งเสร็จสมบูรณ์

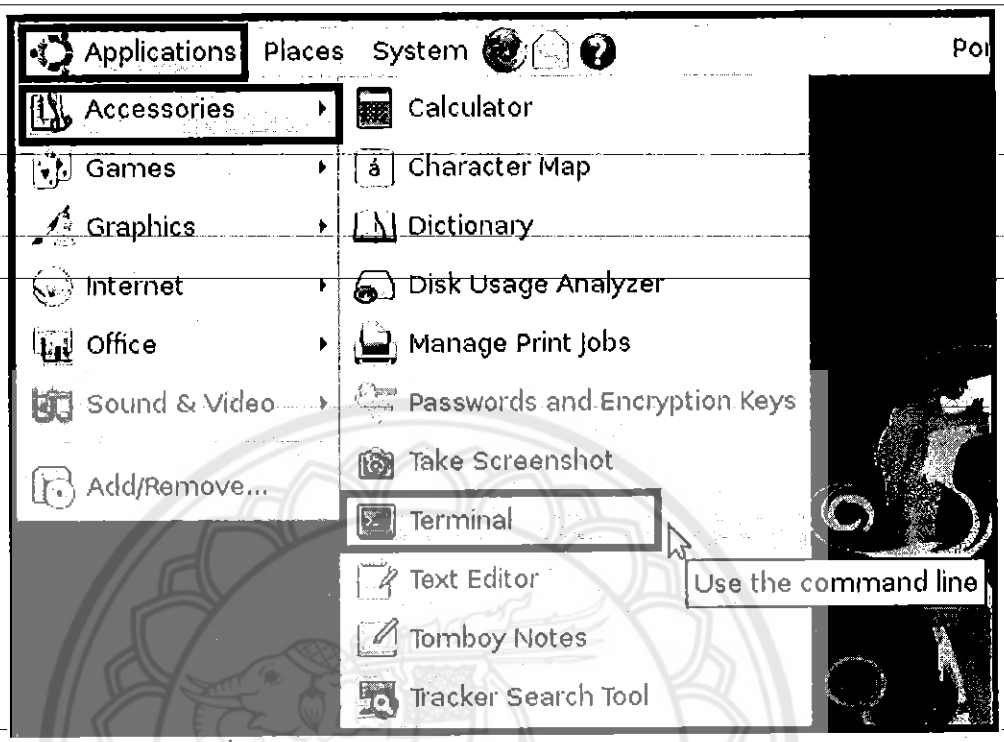
ก.2. การตั้งค่าการเชื่อมต่อและการ Updateระบบปฏิบัติการ Linux

ก.2.1 ทำการยืนยันตัวตน (Authentication) โดยการพิมพ์ Username และ Password ดังรูปที่ ก.11



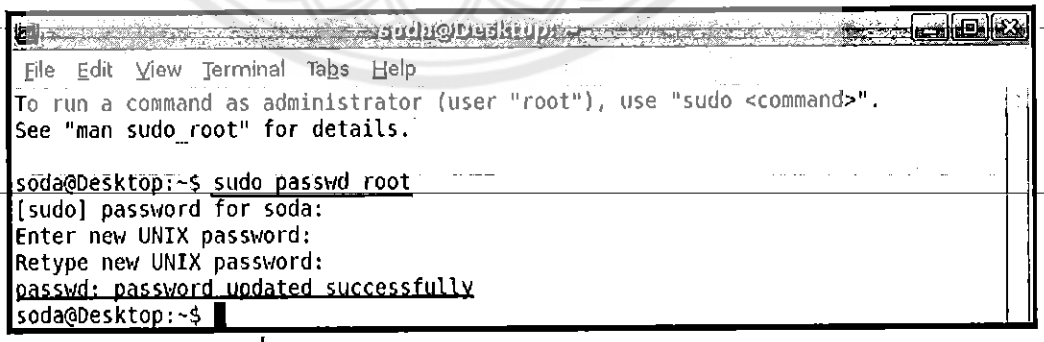
รูปที่ ก.11 แสดงหน้าต่างสำหรับยืนยันตัวตนก่อนเข้าใช้ระบบปฏิบัติการลินุกซ์

ก.2.2 เมื่อผ่านการลงชื่อเข้าใช้แล้ว คลิกที่ Applications จากนั้นเลือกที่ Accessories แล้วคลิกที่ Terminal ดังรูปที่ ก.12



รูปที่ ก.12 แสดงการเข้าสู่ root ของระบบปฏิบัติการลินุกซ์

ก.2.3 พิมพ์คำสั่ง "sudo passwd root" แล้วกดปุ่ม Enter ที่แป้นพิมพ์ เพื่อกำหนดรหัสผ่านของ root หลังจากนั้นให้พิมพ์รหัสผ่าน และยืนยันรหัสผ่านอีกครั้ง ถ้าหากการกำหนดรหัสผ่านเสร็จสมบูรณ์จะมีข้อความแสดงผลว่า "passwd: password updated successfully" ดังรูปที่ ก.13



รูปที่ ก.13 แสดงหน้าต่างการกำหนดรหัสผ่านของ root

ก.2.4 การเข้าถึงในส่วนของ root เพื่อให้การปรับตั้งค่าต่างๆ ของ root สามารถทำได้ โดยการพิมพ์ "su" แล้วกดปุ่ม Enter ที่แป้นพิมพ์ หลังจากนั้นให้พิมพ์ Password แล้วกดปุ่ม Enter อีกครั้งหากการเข้าใช้สำเร็จจะเปลี่ยนจาก "[ชื่อผู้ใช้]@[ชื่อเครื่อง]:..." เป็น "root@[ชื่อเครื่อง]:..." ดังรูปที่ ก.14

```
passwd: password updated successfully
soda@Desktop:~$ su
Password:
root@Desktop:/home/soda#
```

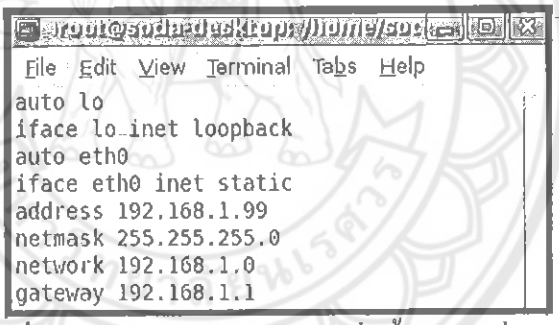
รูปที่ ก.14 แสดงหน้าต่างการเข้าสู่ root

ก.2.5 พิมพ์คำสั่ง "vi /etc/network/interfaces" เพื่อทำการตั้งค่าการเชื่อมต่อ ดังรูปที่ ก.15

```
root@Desktop:/home/soda# vi /etc/network/interfaces
```

รูปที่ ก.15 แสดงการใช้คำสั่งเพื่อเข้าสู่ไฟล์ข้อมูลที่ใช้ในการตั้งค่าการเชื่อมต่อ

ก.2.6 พิมพ์ข้อมูลดังรูปที่ ก.16 เพื่อกำหนด IP Address ให้เป็นแบบ Static แล้วบันทึก



รูปที่ ก.16 แสดงการพิมพ์ข้อมูลเพื่อตั้งค่าการเชื่อมต่อ

ก.2.7 พิมพ์คำสั่ง "/etc/init.d/networking restart" เพื่อ Restart Network ดังรูปที่ ก.17

```
root@Desktop:/home/soda# /etc/init.d/networking restart
 * Reconfiguring network interfaces...
grep: /etc/resolv.conf: No such file or directory
                                                    [ OK ]
```

รูปที่ ก.17 แสดงการ Restart Network

ก.2.8 พิมพ์คำสั่ง "vi /etc/resolv.conf" เพื่อกำหนดค่า Server Name ดังรูปที่ ก.18

```
root@Desktop:/home/soda# vi /etc/resolv.conf
```

รูปที่ ก.18 แสดงการใช้คำสั่งเพื่อเข้าสู่ไฟล์ข้อมูลที่ใช้ในการตั้งค่า Server Name

ก.2.9 พิมพ์ข้อความ "nameserver 192.168.1.1" ลงในไฟล์ แล้วบันทึก เพื่อกำหนดค่า Server Name ดังรูปที่ ก.19

```
nameserver 192.168.1.1
```

รูปที่ ก.19 แสดงการกำหนดค่า Server Name

ก.2.10 พิมพ์คำสั่ง "/etc/init.d/networking restart" เพื่อให้มีการเชื่อมต่อใหม่อีกครั้ง

```
root@Desktop:/home/soda# /etc/init.d/networking restart
 * Reconfiguring network interfaces...                              [ OK ]
```

รูปที่ ก.20 แสดงการ Restart Network อีกครั้ง

ก.2.11 พิมพ์คำสั่ง "ifconfig" แล้วกดปุ่ม Enter ที่แป้นพิมพ์ เพื่อตรวจสอบค่าของการเชื่อมต่อของระบบเครือข่าย แสดงให้เห็นดังรูปที่ ก.21

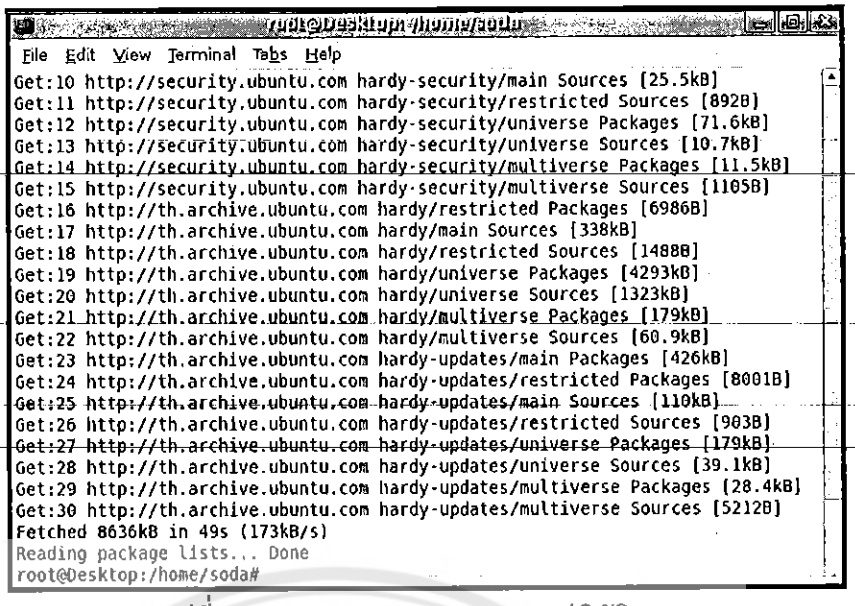
```
root@Desktop:/home/soda# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:55:56:dc
          inet addr:192.168.1.99  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe55:56dc/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4699 errors:1 dropped:0 overruns:0 frame:0
          TX packets:131 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:397210 (387.9 KB)  TX bytes:16902 (16.5 KB)
          Interrupt:11 Base address:0xc020

eth1      Link encap:Ethernet  HWaddr 08:00:27:c6:10:61
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:89 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:11256 (10.9 KB)
          Interrupt:10 Base address:0xc060

eth1:avahi Link encap:Ethernet  HWaddr 08:00:27:c6:10:61
          inet addr:169.254.4.198  Bcast:169.254.255.255  Mask:255.255.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          Interrupt:10 Base address:0xc060

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
```

รูปที่ ก.21 แสดงรายละเอียดข้อมูลต่างๆ ของการเชื่อมต่อระบบเครือข่าย

ก.2.12 พิมพ์คำสั่ง "apt-get update" ดังรูปที่ ก.22 แล้วกดปุ่ม Enter ที่แป้นพิมพ์ เพื่อ Update ระบบปฏิบัติการ โดยกระบวนการในการ Update นั้นแสดงให้เห็นดังรูปที่ ก.23

```
root@Desktop:/home/soda# apt-get update
```

รูปที่ ก.22 แสดงการใช้คำสั่งเพื่อ Update ระบบปฏิบัติการ



รูปที่ ก.23 แสดงการ Update ระบบปฏิบัติการ

ก.3. การตั้งค่าเครือข่าย

ก.3.1 พิมพ์คำสั่งดังรูปที่ ก.24 เพื่อเปิดไฟล์ที่ชื่อว่า "sysctl.conf

```
root@Desktop:/home/soda# vi /etc/sysctl.conf
```

รูปที่ ก.24 แสดงคำสั่งเปิดไฟล์ sysctl.conf

ก.3.2 ทำการแก้ไขข้อความในไฟล์ "sysctl.conf" โดยการลบคอมเม้นหน้าข้อความ "net.ipv4.ip_forward=1" ออกดังรูปที่ ก.25 เพื่อทำการเปิดใช้งาน Packet Forwording

```
###############################################################3
# Functions previously found in netbase
#

# Comment the next two lines to disable Spoof protection (reverse-p
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
net.ipv4.conf.default.rp_filter=1
net.ipv4.conf.all.rp_filter=1

# Uncomment the next line to enable TCP/IP SYN cookies
# This disables TCP Window Scaling (http://lkml.org/lkml/2008/2/5/1
#net.ipv4.tcp_syncookies=1

# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1

# Uncomment the next line to enable packet forwarding for IPv6
#net.ipv6.ip_forward=1


###################################################################
```

รูปที่ ก.25 แสดงการแก้ไขข้อความในไฟล์ sysctl.conf

ก.3.3 พิมพ์คำสั่งดังรูปที่ ก.26 เพื่อตรวจสอบผลการเปิดใช้งาน Packet Forwarding หากผลเป็น 1 แสดงว่าการเปิดใช้งานสำเร็จ

```
root@Desktop:/home/soda# echo 1 | tee /proc/sys/net/ipv4/ip_forward
1
root@Desktop:/home/soda#
```

รูปที่ ก.26 แสดงผลการเปิดใช้งาน Packet Forwarding

ก.3.4 พิมพ์คำสั่ง "sysctl -p" และ "/etc/init.d/networking restart" เพื่อให้มีการ Restart Network ดังรูปที่ ก.27

```
root@Desktop:/home/soda# sysctl -p
kernel.printk = 4 4 1 7
kernel.maps_protect = 1
fs.inotify.max_user_watches = 524288
vm.mmap_min_addr = 65536
net.ipv4.conf.default.rp_filter = 1
net.ipv4.conf.all.rp_filter = 1
net.ipv4.ip_forward = 1
root@Desktop:/home/soda# /etc/init.d/networking restart
 * Reconfiguring network interfaces...                    [ OK ]
root@Desktop:/home/soda#
```

รูปที่ ก.27 แสดงการ Restart Network หลังจากเปิดใช้งาน Packet Forwarding

ก.4. การเปิดใช้งาน TUN/TAP Device Driver Support

ก.4.1 พิมพ์คำสั่ง "vi /etc/modules" เพื่อเปิดไฟล์ที่ชื่อว่า "Modules" แล้วเพิ่มข้อความโดยการพิมพ์คำว่า "tun" ต่อท้ายข้อความเดิม ดังรูปที่ ก.28 เพื่อเปิดการใช้งาน TUN/TAP Device Driver Support

```
File  Edit  View  Terminal  Tabs  Help
# /etc/modules: kernel modules to load at boot time.
#
# This file contains the names of kernel modules that should be load
# at boot time, one per line. Lines beginning with "#" are ignored.

fuse
lp
tun
```

รูปที่ ก.28 แสดงการแก้ไขข้อความในไฟล์ Modules

ก.4.2 ทำการ Enable ด้วยคำสั่ง "modprobe tun" ดังรูป

```
root@Desktop:/home/soda# modprobe tun
root@Desktop:/home/soda#
```

รูปที่ ก.29 แสดงการ Enable Tunnel

ภาคผนวก ข

การติดตั้งโปรแกรมต่างๆ

ข.1. การติดตั้ง OpenSSH Server

โปรแกรม OpenSSH ทำให้สามารถ Remote เข้าไปทำงานบน Proxy Server ได้ ทำให้สามารถทำการคัดลอกและวางคำสั่งต่างๆ ได้ง่ายขึ้น โดยในที่นี้จะใช้ร่วมกับโปรแกรม PuTTY

ข.1.1 พิมพ์คำสั่งติดตั้งโปรแกรม OpenSSH Server ดังรูปที่ ข.1 แล้วกดปุ่ม Enter ที่แป้นพิมพ์ เพื่อเริ่มการติดตั้ง หากมีคำถามให้ทำการพิมพ์ Y แล้วกดปุ่ม Enter ดังรูปที่ ข.2

```
root@Desktop:/home/soda# apt-get install ssh openssh-server
```

รูปที่ ข.1 แสดงคำสั่งติดตั้ง OpenSSH Server

```
The following NEW packages will be installed:
  openssh-blacklist openssh-server ssh
0 upgraded, 3 newly installed, 0 to remove and 67 not upgraded.
Need to get 2379kB of archives.
After this operation, 4903kB of additional disk space will be used
Do you want to continue [Y/n]? y ←
Get:1 http://th.archive.ubuntu.com hardy-updates/main openssh-blac
```

รูปที่ ข.2 แสดงการตอบคำถามขณะติดตั้ง OpenSSH Server

ข.1.2 หลังจากการติดตั้งโปรแกรม OpenSSH Server เสร็จสมบูรณ์ จากนั้นให้ทำการเปิด SSH Service ด้วยคำสั่งดังรูปที่ ข.3

```
root@Desktop:/home/soda# /etc/init.d/ssh restart
 * Restarting OpenBSD Secure Shell server sshd                    [ OK ]
root@Desktop:/home/soda#
```

รูปที่ ข.3 แสดงการเปิด SSH Service

ข.2. การติดตั้ง ChilliSpot

โปรแกรม ChilliSpot เป็นซอฟต์แวร์ Open Source ซึ่งทำหน้าที่จัดการด้านระบบเครือข่ายอินเตอร์เน็ตโดยจะทำหน้าที่เป็น DHCP Server แจก IP Address ให้กับเครื่องลูกข่าย และทำหน้าที่เป็น Firewall โดยเก็บกฎต่างๆ ของการใช้อินเตอร์เน็ต

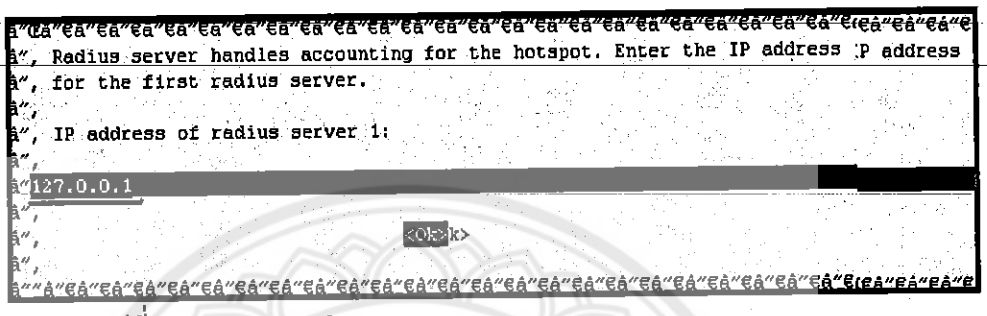
ตั้งแต่ภาคผนวก ข.2 เป็นต้นไป จะเป็นการติดตั้งโปรแกรมต่างๆ โดยใช้โปรแกรม PuTTY มาช่วยในการติดตั้งเพื่อให้ง่ายต่อการคัดลอกคำสั่งต่างๆ ซึ่งการใช้งานโปรแกรม PuTTY จะแสดงไว้ในภาคผนวก ค.1

ข.2.1 ทำการพิมพ์คำสั่งดังรูปที่ ข.4 เพื่อติดตั้งโปรแกรม ChilliSpot

```
root@Desktop:~# apt-get install chillispot
```

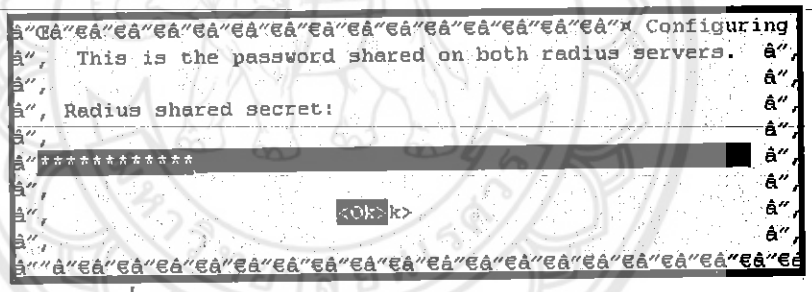
รูปที่ ข.4 แสดงการใช้คำสั่งติดตั้งโปรแกรม ChilliSpot

ข.2.2 ทำการพิมพ์หมายเลข IP Address ของ RADIUS Server แล้วเลือก OK



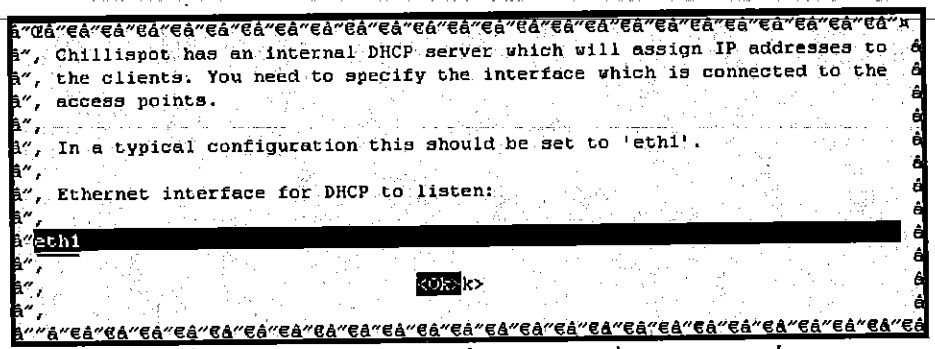
รูปที่ ข.5 แสดงการกำหนด หมายเลข IP Address ของ RADIUS Server

ข.2.3 พิมพ์รหัสผ่านของ RADIUS Server ตามต้องการ แล้วเลือก OK



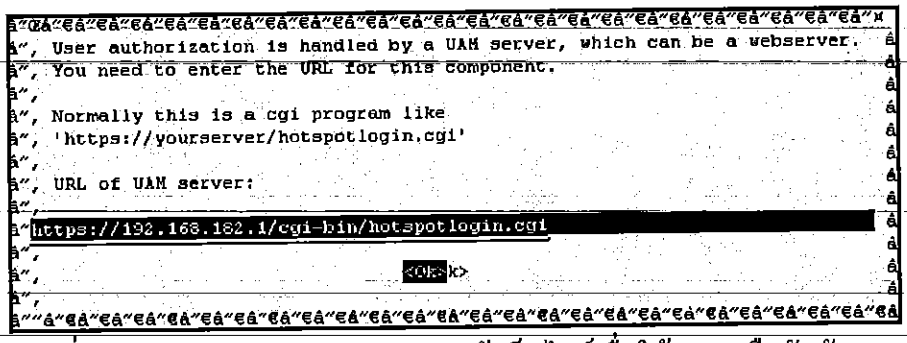
รูปที่ ข.6 แสดงการกำหนดรหัสผ่านของ RADIUS Server

ข.2.4 เลือก LAN Card ที่จะให้มีการเชื่อมต่อไปสู่เครื่องลูกข่าย โดยจะกำหนดให้เป็น eth1 แล้วเลือก OK ดังรูปที่ ข.7



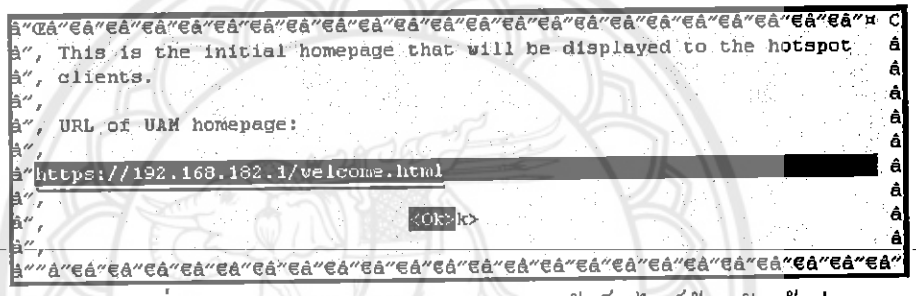
รูปที่ ข.7 แสดงการเลือกจุดที่จะให้มีการเชื่อมต่อไปสู่เครื่องลูกข่าย

ข.2.5 กำหนด URL ของหน้าเว็บไซต์เพื่อให้ Users ยืนยันตัวตน แล้วเลือก OK



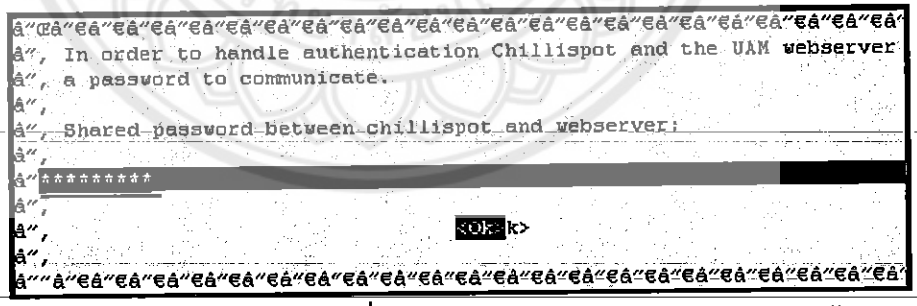
รูปที่ ข.8 แสดงการกำหนด URL ของหน้าเว็บไซต์เพื่อให้ Users ยืนยันตัวตน

ข.2.6 กำหนด URL ของหน้าเว็บไซต์ต้อนรับเข้าสู่ระบบ แล้วเลือก OK



รูปที่ ข.9 แสดงการกำหนด URL ของหน้าเว็บไซต์ต้อนรับเข้าสู่ระบบ

ข.2.7 กำหนดรหัสผ่านที่ใช้ร่วมกันระหว่างโปรแกรม ChilliSpot กับ Webserver เลือก OK



รูปที่ ข.10 แสดงการกำหนดรหัสผ่านที่ใช้ร่วมกันระหว่างโปรแกรม ChilliSpot กับ Webserver

ข.2.8 ทำการเปิดไฟล์ชื่อ "chillispot" ด้วยคำสั่งดังรูปที่ ข.11 แล้วทำการแก้ไขข้อความภายในไฟล์โดยกำหนดค่า ENABLED = 1 ดังรูปที่ ข.12 แล้วทำการบันทึก

```
root@Desktop:~# vi /etc/default/chillispot
```

รูปที่ ข.11 แสดงการใช้คำสั่งเพื่อเปิดไฟล์ ChilliSpot

```
# /etc/default/chillispot
#
# Enable on system start?
# Change to 1 if you want it to be enabled.
# Please make sure you have configured chillispot first.
ENABLED=1
#
# chillispot default configuration
```

รูปที่ ข.12 แสดงการแก้ไขข้อความในไฟล์ ChilliSpot

ข.2.9 ทำการเปิดไฟล์ชื่อ "chilli.conf" ด้วยคำสั่งดังรูปที่ ข.13 แล้วทำการตรวจสอบและแก้ไขข้อมูลต่างๆ ดังรูปที่ ข.14 – ข.24 แล้วทำการบันทึก

```
root@Desktop:~# vi /etc/chilli.conf
```

รูปที่ ข.13 แสดงการใช้คำสั่งเพื่อเปิดไฟล์ chilli.conf

```
# TAG: net
# IP network address of external packet data network
# Used to allocate dynamic IP addresses and set up routing.
# Normally you do not need to uncomment this tag.
#net 192.168.182.0/24
```

รูปที่ ข.14 แสดงการกำหนดค่า net (ในไฟล์ chilli.conf)

```
# TAG: dns1
# Primary DNS server.
# Will be suggested to the client.
# If omitted the system default will be used.
# Normally you do not need to uncomment this tag.
#dns1 192.168.9.9
```

รูปที่ ข.15 แสดงการกำหนดค่า dns1 (ในไฟล์ chilli.conf)

```
# TAG: dns2
# Secondary DNS server.
# Will be suggested to the client.
# If omitted the system default will be used.
# Normally you do not need to uncomment this tag.
#dns2 192.168.9.9
```

รูปที่ ข.16 แสดงการกำหนดค่า dns2 (ในไฟล์ chilli.conf)

```
# TAG: radiusserver1
# IP address of radius server 1
# For most installations you need to modify this tag.
radiusserver1 127.0.0.1

# TAG: radiusserver2
# IP address of radius server 2
# If you have only one radius server you should set radiusserver2 to the
# same value as radiusserver1.
# For most installations you need to modify this tag.
radiusserver2 127.0.0.1
```

รูปที่ ข.17 แสดงการกำหนดค่า RADIUS Server 1 และ RADIUS Server 2 (ในไฟล์ chilli.conf)

```
# TAG: radiussecret
# Radius shared secret for both servers
# For all installations you should modify this tag.
radiussecret radiussecret
```

รูปที่ ข.18 แสดงรหัสผ่านสำหรับ RADIUS Server (ในไฟล์ chilli.conf)

```
# DHCP Parameters

# TAG: dhcpif
# Ethernet interface to listen to.
# This is the network interface which is connected to the access points.
# In a typical configuration this tag should be set to eth1.
dhcpif eth1
```

รูปที่ ข.19 แสดงจุดที่กำหนดให้มีการเชื่อมต่อกับเครื่องลูกข่าย (ในไฟล์ chilli.conf)

```
# Universal access method (UAM) parameters

# TAG: uamserver
# URL of web server handling authentication.
uamserver https://192.168.182.1/cgi-bin/hotspotlogin.cgi
```

รูปที่ ข.20 แสดง URL ของหน้าเว็บไซต์เพื่อให้ Users ยืนยันตัวตน (ในไฟล์ chilli.conf)

```
# TAG: uamhomepage
# URL of welcome homepage.
# Unauthenticated users will be redirected to this URL. If not specified
# users will be redirected to the uamserver instead.
# Normally you do not need to uncomment this tag.
uamhomepage https://192.168.182.1/welcome.html
```

รูปที่ ข.21 แสดงผล URL ของหน้าเว็บไซต์ต้อนรับเข้าสู่ระบบ (ในไฟล์ chilli.conf)

```
# TAG: uamsecret
# Shared between chilli and authentication web server
uamsecret uamsecret
```

รูปที่ ข.22 แสดงรหัสผ่านที่ใช้ระหว่าง โปรแกรม ChilliSpot กับ Web Server (ในไฟล์ chilli.conf)

```
# TAG: uamlisten
# IP address to listen to for authentication requests
# Do not uncomment this tag unless you are an experienced user
#uamlisten 192.168.182.1
```

รูปที่ ข.23 แสดง IP Address ของ Proxy Server (ในไฟล์ chilli.conf)

```
# TAG: uamalloved
# Comma separated list of domain names, IP addresses or network segments
# the client can access without first authenticating.
# It is possible to specify this tag multiple times.
# Normally you do not need to uncomment this tag.
#uamalloved www.google.co.th,192.168.182.0/24
```

รูปที่ ข.24 แสดงเว็บไซต์ที่อนุญาตให้เข้าถึงได้โดยไม่ต้องยืนยันตัวตน (ในไฟล์ chilli.conf)

ข.3. การติดตั้ง Firewall

การสร้าง Firewall นั้น ทำได้โดยกำหนดกฎต่างๆ ไว้ในไฟล์ chilli.iptables เพื่อให้ ChilliSpot ทำหน้าที่เป็น Firewall ของระบบ และสามารถปรับเปลี่ยนกฎต่างๆ ของ Firewall ได้ โดยการเปลี่ยนข้อมูลในไฟล์ chilli.iptables

ข.3.1 พิมพ์คำสั่งคัดลอกไฟล์ที่ชื่อว่า "chilli.iptables" ไว้ในส่วนที่มีการใช้งานอัตโนมัติ เมื่อเครื่อง Server ทำงาน ดังรูปที่ ข.25

```
root@Desktop:~# cp /usr/share/doc/chillispot/firewall.iptables  /etc/init.d/chilli.iptables
```

รูปที่ ข.25 แสดงคำสั่งคัดลอกไฟล์ chilli.iptables

ข.3.2 พิมพ์คำสั่งเพื่อให้ chilli.iptables สามารถ Execute ได้ ดังรูป แล้วกด Enter

```
root@Desktop:~# chmod a+x /etc/init.d/chilli.iptables
```

รูปที่ ข.26 แสดงคำสั่งเพื่อให้ chilli.iptables สามารถ Execute ได้

ข.3.3 พิมพ์คำสั่งเพื่อให้ Firewall ทำงานทุกครั้งเมื่อเครื่อง Server เปิดใช้งาน แล้วกด Enter

```
root@Desktop:~# ln -s /etc/init.d/chilli.iptables /etc/rcS.d/S41chilli.iptables
```

รูปที่ ข.27 แสดงคำสั่งเพื่อให้ Firewall ทำงานทุกครั้งเมื่อเครื่อง Server เปิดใช้งาน

ข.3.4 พิมพ์คำสั่งเพื่อทำการเปิดใช้งาน Firewall Script ดังรูป แล้วกด Enter

```
root@Desktop:~# /etc/init.d/chilli.iptables
```

รูปที่ ข.28 แสดงคำสั่งเพื่อทำการเปิดใช้งาน Firewall Script

ข.4. การติดตั้ง Apache Web Server

ข.4.1 พิมพ์คำสั่งติดตั้ง Apache Web Server ดังรูปที่ ข.29 แล้วกดปุ่ม Enter ที่แป้นพิมพ์เพื่อเริ่มการติดตั้ง หากมีคำถามให้ทำการพิมพ์ Y แล้วกดปุ่ม Enter ดังรูปที่ ข.30

```
root@Desktop:~# apt-get install apache2
```

รูปที่ ข.29 แสดงคำสั่งติดตั้ง Apache Web Server

```
Need to get 1646kB of archives.
After this operation, 5784kB of additional disk space will be used.
Do you want to continue [Y/n]? y
```

รูปที่ ข.30 แสดงการตอบคำถามขณะติดตั้ง Apache Web Server

ข.4.2 ทำการเปิดไฟล์ชื่อ "apache2.conf" ด้วยคำสั่งดังรูปที่ ข.31 แล้วกำหนดค่า Server Name ดังรูปที่ ข.32

```
root@Desktop:~# vi /etc/apache2/apache2.conf
```

รูปที่ ข.31 แสดงการใช้คำสั่งเพื่อเปิดไฟล์ apache2.conf

```
### Section 1: Global Environment
#
# The directives in this section affect the overall operation of Apache,
# such as the number of concurrent requests it can handle or where it
# can find its configuration files.
#
ServerName 192.168.182.1
```

รูปที่ ข.32 แสดงการกำหนดค่า Server Name (ในไฟล์ apache2.conf)

ข.4.3 ทำการพิมพ์คำสั่งเพื่อเปิดใช้งาน Apache Web Server ด้วยคำสั่งดังรูปที่ ข.33

```
root@Desktop:~# /etc/init.d/apache2 start
 * Starting web server apache2
httpd (pid 5656) already running
                                                          [ OK ]
root@Desktop:~#
```

รูปที่ ข.33 แสดงคำสั่งเพื่อเปิดใช้งาน Apache Web Server

ข.4.4 ทำการพิมพ์คำสั่งเพื่อตรวจสอบว่า Apache Web Server สามารถใช้งานได้หรือไม่ ด้วยคำสั่งดังรูป ซึ่งหากสามารถทำงานได้จะแสดงผลออกมาว่า Port 80 มีสถานะเป็น LISTEN

```
root@Desktop:~# netstat -lnt
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
tcp        0      0 192.168.182.1:3990      0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
```

รูปที่ ข.34 แสดงคำสั่งเพื่อตรวจสอบการทำงานของ Apache Web Server

ข.5. การติดตั้ง MySQL Database Server

ข.5.1 พิมพ์คำสั่งติดตั้ง MySQL Database Server ดังรูปที่ ข.35 แล้วกดปุ่ม Enter ที่แป้นพิมพ์ เพื่อเริ่มการติดตั้ง หากมีคำถามให้ทำการพิมพ์ Y แล้วกดปุ่ม Enter ดังรูปที่ ข.36

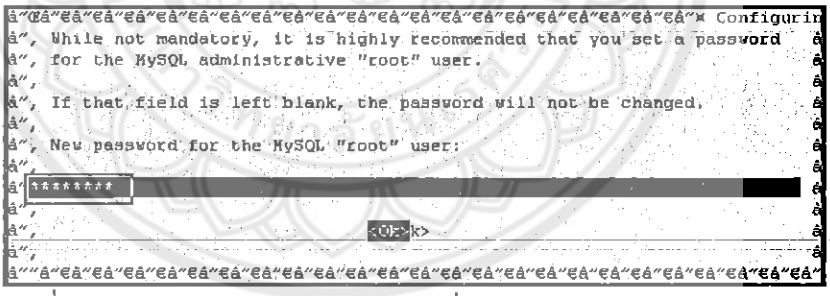
```
root@Desktop:~# apt-get install mysql-server
```

รูปที่ ข.35 แสดงคำสั่งติดตั้ง MySQL Database Server

```
Need to get 38.2MB of archives.
After this operation, 112MB of additional disk space will be used
Do you want to continue [Y/n]? (y) <---
```

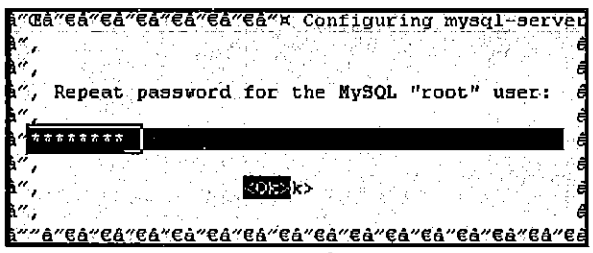
รูปที่ ข.36 แสดงการตอบคำถามขณะติดตั้ง MySQL Database Server

ข.5.2 ทำการกำหนดรหัสผ่านเข้าสู่ MySQL Database Server แล้วเลือก OK ดังรูปที่ ข.37



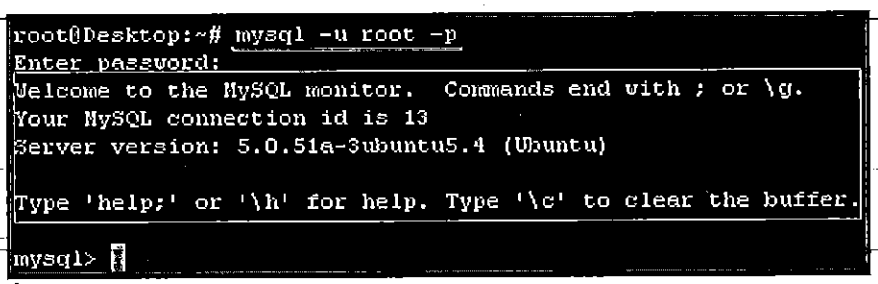
รูปที่ ข.37 แสดงการกำหนดรหัสผ่านเพื่อเข้าสู่ MySQL Database Server

ข.5.3 ทำการยืนรหัสผ่านเข้าสู่ MySQL Database Server แล้วเลือก OK ดังรูปที่ ข.38



รูปที่ ข.38 แสดงการยืนยันรหัสผ่านเพื่อเข้าสู่ MySQL Database Server

ข.5.4 ทดสอบว่า MySQL Database Server สามารถใช้งานได้หรือไม่ด้วยคำสั่ง "mysql -u root –p" แล้วพิมพ์รหัสผ่าน หากใช้งานได้จะมีการแสดงผลดังรูปที่ ข.39



รูปที่ ข.39 แสดงการทดสอบว่า MySQL Database Server สามารถใช้งานได้หรือไม่

ข.6. การติดตั้ง PHP5

ข.6.1 พิมพ์คำสั่งติดตั้ง PHP5 ดังรูปที่ ข.40 แล้วกดปุ่ม Enter ที่แป้นพิมพ์ เพื่อเริ่มการติดตั้ง หากมีคำถามให้ทำการพิมพ์ Y แล้วกดปุ่ม Enter ดังรูปที่ ข.41

รูปที่ ข.40 แสดงคำสั่งติดตั้ง PHP5

รูปที่ ข.41 แสดงการตอบคำถามขณะติดตั้ง PHP5

ข.6.2 เมื่อการติดตั้ง PHP5 สำเร็จ ให้พิมพ์คำสั่งเพื่อ Restart Apache Web Server ดังรูปที่ ข.42

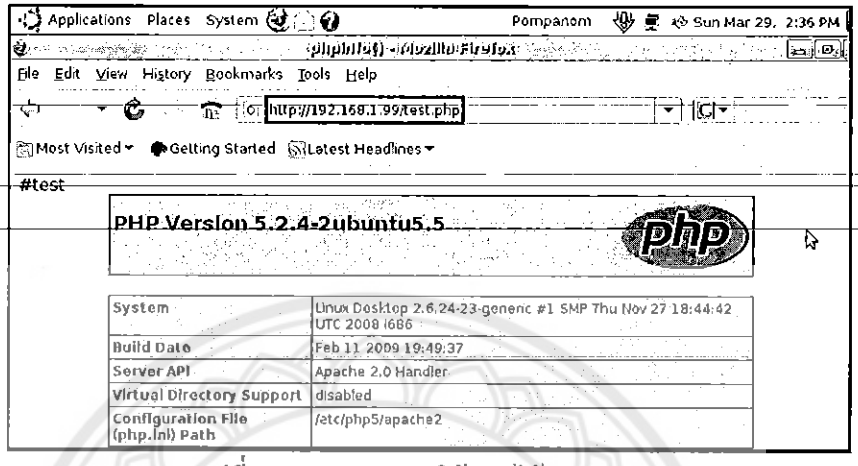
รูปที่ ข.42 แสดงคำสั่งเพื่อ Restart Apache Web Server

ข.6.3 ทดสอบว่า PHP5 สามารถใช้งานได้หรือไม่ โดยการสร้างไฟล์ที่ชื่อว่า "test.php" ดังรูปที่ ข.43 แล้วพิมพ์ข้อความลงในไฟล์ ดังรูปที่ ข.44 แล้วบันทึก ซึ่งเมื่อใช้ Browser เปิด http://192.168.1.99/test.php แล้วมีการแสดงผลดังรูปที่ ข.45 แสดงว่า PHP5 สามารถใช้งานได้

รูปที่ ข.43 แสดงการใช้คำสั่งเพื่อสร้างไฟล์ test.php

```
#test
<?php phpinfo(); ?>
```

รูปที่ ข.44 แสดงการใช้คำสั่งเพื่อสร้างไฟล์ test.php



รูปที่ ข.45 แสดงการใช้งานได้ของ PHP5

ข.7. การติดตั้ง PHPMyAdmin

PHPMyAdmin เป็นโปรแกรมที่ใช้สำหรับต่อประสานเพื่อใช้จัดการฐานข้อมูล MySQL ผ่าน Web Browser โดยสามารถทำการสร้างฐานข้อมูลใหม่ มีฟังก์ชันสำหรับการทดสอบการ Query ข้อมูลด้วยภาษา SQL และยังสามารถดำเนินการต่างๆ บนฐานข้อมูลได้เหมือนกับการใช้ภาษา SQLอีกด้วย

ข.7.1 พิมพ์คำสั่งติดตั้ง PHPMyAdmin ดังรูปที่ ข.46 แล้วกดปุ่ม Enter ที่แป้นพิมพ์ เพื่อเริ่มการติดตั้ง หากมีคำถามให้ทำการพิมพ์ Y แล้วกดปุ่ม Enter ดังรูปที่ ข.47

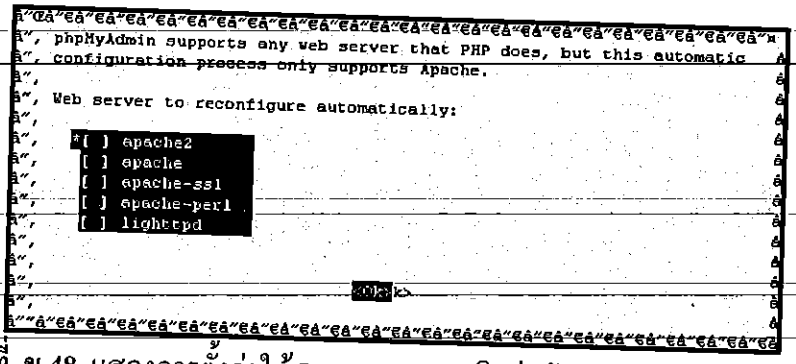
```
root@Desktop:~# apt-get install phpmyadmin
```

รูปที่ ข.46 แสดงคำสั่งติดตั้ง PHPMyAdmin

```
After this operation, 11.0MB of additional disk space will be used.
Do you want to continue [Y/n]? y
```

รูปที่ ข.47 แสดงการตอบคำถามขณะติดตั้ง PHPMyAdmin

ข.7.2 ทำการตั้งค่าให้ PHPMyAdmin ติดต่อกับ Web Server Apache2 ดังรูป แล้วเลือก OK



รูปที่ ข.48 แสดงการตั้งค่าให้ PHPMyAdmin ติดต่อกับ Web Server Apache2

ข.7.3 ทดสอบว่า PHPMyAdmin สามารถใช้งานได้หรือไม่ โดยการใช้ Browser เปิด http://192.168.1.99/phpmyadmin หากมีการแสดงผลดังรูปที่ ข.49 แสดงว่า PHPMyAdmin สามารถใช้งานได้

รูปที่ ข.49 แสดงการใช้งานได้ของ PHPMyAdmin

ข.8. การติดตั้ง RADIUS Server

RADIUS Server (Remote Authentication Dial in User Service Server) เป็นเครื่องบริการที่สามารถตรวจสอบสิทธิ์ในการใช้งาน Internet สามารถสร้าง User Account และสามารถจำกัดชั่วโมงการใช้งานของ Users ได้

ข.8.1 พิมพ์คำสั่งติดตั้ง RADIUS Server ดังรูปที่ ข.50 แล้วกดปุ่ม Enter ที่แป้นพิมพ์ เพื่อเริ่มการติดตั้ง

```
root@Desktop:~# apt-get install freeradius freeradius-mysql
```

รูปที่ ข.50 แสดงคำสั่งติดตั้ง RADIUS Server

ข.8.2 พิมพ์คำสั่งเพื่อเริ่มการทำงานของ RADIUS Server ดังรูปที่ ข.51

```
root@Desktop:/var/log/apache2# /etc/init.d/freeradius start
 * Starting FreeRADIUS daemon freeradius
Mon Mar 30 00:28:24 2009 : Info: Starting - reading configuration files ...
                                                                    [ OK ]
```

รูปที่ **ข.51** แสดงคำสั่งเพื่อเริ่มการทำงานของ RADIUS Server

ข.8.3 ทำการสร้างฐานข้อมูล ชื่อว่า "radius" เพื่อใช้ในการเก็บบัญชีรายชื่อผู้ใช้งานด้วยคำสั่งดังรูปที่ ข.52 หรือจะใช้ PHPMyAdmin เป็นเครื่องมือในการช่วยสร้างได้

```
root@Desktop:~# mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 21
Server version: 5.0.51a-3ubuntu5.4 (Ubuntu)

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> CREATE DATABASE radius;
Query OK, 1 row affected (0.08 sec)
```

รูปที่ **ข.52** แสดงการสร้างฐานข้อมูล

ข.8.4 ทำการสร้างตารางให้กับฐานข้อมูล RADIUS ที่ได้สร้างขึ้น ด้วยคำสั่งดังรูปที่ ข.53

```
mysql> quit;
Bye
root@Desktop:~# zcat /usr/share/doc/freeradius/examples/mysql.sql.gz | mysql -u root -p radius
Enter password:
```

รูปที่ ข.53 แสดงการสร้างตารางให้กับฐานข้อมูล RADIUS

ข.8.5 ทำการสร้าง Users ที่มีสิทธิ์ในฐานข้อมูล RADIUS โดยกำหนด Username Password ด้วยคำสั่งดังรูปที่ ข.54

```
root@Desktop:~# mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 23
Server version: 5.0.51a-3ubuntu5.4 (Ubuntu)

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> GRANT ALL PRIVILEGES ON radius.* TO 'radius'@'localhost' IDENTIFIED BY 'mysqlsecret';
Query OK, 0 rows affected (0.03 sec)

mysql> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.03 sec)

mysql> quit;
Bye
```

รูปที่ ข.54 แสดงการสร้าง Users ที่มีสิทธิ์ในฐานข้อมูล RADIUS

ข.8.6 ทำการเปิดไฟล์ชื่อ "sql.conf" ด้วยคำสั่งดังรูปที่ ข.55 แล้วกำหนดชื่อ Login และ Password ดังรูปที่ ข.56 แล้วทำการบันทึก

```
root@Desktop:~# vi /etc/freeradius/sql.conf
```

รูปที่ ข.55 แสดงคำสั่งเปิดไฟล์ sql.conf

```
sql {
        # Database type
        # Current supported are: rlm_sql_mysql, rlm_sql_postgresql,
        # rlm_sql_iodbc, rlm_sql_oracle, rlm_sql_unixodbc, rlm_sql_freetds
        driver = "rlm_sql_mysql"

        # Connect info
        server = "localhost"
        login = "radius"
        password = "radiussecret"
```

รูปที่ ข.56 แสดงการกำหนดชื่อ Login และ Password (ในไฟล์ sql.conf)

ข.8.7 ทำการเปิดไฟล์ชื่อ "clients.conf" ด้วยคำสั่งดังรูปที่ ข.57 แล้วกำหนดรหัสผ่านเพื่อเข้าใช้งาน RADIUS Server ดังรูปที่ ข.58 แล้วทำการบันทึก

```
root@Desktop:~# vi /etc/freeradius/clients.conf
```

รูปที่ ข.57 แสดงคำสั่งเปิดไฟล์ clients.conf

```
client 127.0.0.1 {
        #
        #  The shared secret use to "encrypt" and "sign" packets be
        #  the NAS and FreeRADIUS.  You MUST change this secret fro
        #  default, otherwise it's not a secret any more!
        #
        #  The secret can be any string, up to 31 characters in len
        #
        secret          = radiussecret
```

รูปที่ ข.58 แสดงการกำหนดรหัสผ่านเพื่อเข้าใช้งาน RADIUS Server (ในไฟล์ clients.conf)

ข.8.8 ทำการเปิดไฟล์ชื่อ "users" ด้วยคำสั่งดังรูปที่ ข.59 แล้วนำคอมเม้นท์หน้าชื่อ "john Doe" ออก และแก้ไขข้อความ ดังรูปที่ ข.60 แล้วทำการบันทึก เพื่อเป็นการเตรียมไฟล์สำหรับตรวจสอบการทำงานของ RADIUS Server

```
root@Desktop:~# vi /etc/freeradius/users
```

รูปที่ ข.59 แสดงคำสั่งเปิดไฟล์ Users

```
#
"John Doe"        Auth-Type :=Local, User-Password := "hello"
                  Reply-Message = "Hello, %u"
```

รูปที่ ข.60 แสดงการเตรียมไฟล์เพื่อทดสอบการทำงานของ RADIUS Server

ข.8.9 ทำการปิดการทำงานของ RADIUS Server ด้วยคำสั่งดังรูปที่ ข.61 และแก้ไขข้อผิดพลาด ด้วยคำสั่งดังรูปที่ ข.62

```
root@Desktop:~# /etc/init.d/freeradius stop
 * Stopping FreeRADIUS daemon freeradius                    [ OK ]
```

รูปที่ ข.61 แสดงคำสั่งปิดการทำงานของ RADIUS Server

```
root@Desktop:~# freeradius -XXX -A
```

รูปที่ ข.62 แสดงคำสั่งดีบัก RADIUS Server

ข.8.10 ทำการเปิดโปรแกรม PuTTY ให้ติดต่อไปยัง Sever อีก 1 ตัว (เปิดโปรแกรม PuTTY ใน ข.8.9 ทิ้งไว้) แล้วพิมพ์คำสั่ง ดังรูปเพื่อเป็นการทดสอบการทำงานของ RADIUS Server ในการตรวจสอบคุณสมบัติผู้ใช้จากไฟล์ ด้วยคำสั่งดังรูปที่ ข.63 ซึ่งหาก RADIUS Server ใช้งานได้จะมีข้อความ "Access-Accept"

```
soda@Desktop:~$ su
Password:
root@Desktop:/home/soda# radtest "John Doe" hello 127.0.0.1 0 radiussecret
Sending Access-Request of id 24 to 127.0.0.1 port 1812
        User-Name = "John Doe"
        User-Password = "hello"
        NAS-IP-Address = 255.255.255.255
        NAS-Port = 0
rad_recv: Access-Accept packet from host 127.0.0.1:1812, id=24, length=37
        Reply-Message = "Hello, John Doe"
```

รูปที่ ข.63 แสดงการทดสอบการอ่านข้อมูลจากไฟล์ของ RADIUS Server

ข.8.11 ทำการเปิดไฟล์ชื่อ "radiusd.conf" ด้วยคำสั่งดังรูปที่ ข.64 แล้วแก้ไขในส่วน ต่างๆ ดังนี้ คือ

```
root@Desktop:~# vi /etc/freeradius/radiusd.conf
```

รูปที่ ข.64 แสดงคำสั่งเปิดไฟล์ radiusd.conf

- authorize{...} แก้ไขโดยการนำคอมเม้นหน้า SQL ออก และใส่คอมเม้นหน้า file แทน ดังรูปที่ ข.65 เพื่อเป็นการกำหนดให้ RADIUS Server ตรวจสอบคุณสมบัติผู้ใช้จากฐานข้อมูล SQL แทนการตรวจสอบจากไฟล์ข้อมูล

- accounting{...} แก้ไขโดยการนำคอมเม้นหน้า SQL ออก ดังรูปที่ ข.66 เพื่อให้ RADIUS Server เรียกใช้ข้อมูลจากฐานข้อมูล

- session{...} แก้ไข โดยการนำคอมเม้นหน้า SQL ออก ดังรูปที่ ข.67 เพื่อให้ RADIUS Server เรียกใช้ข้อมูลจากฐานข้อมูล

```
#       files

        #
        #  Look in an SQL database.  The schema of the database
        #  is meant to mirror the "users" file.
        #
        #  See "Authorization Queries" in sql.conf
        sql

        #
        #  If you are using /etc/smbpasswd, and are also doing
        #  mschap authentication, the un-comment this line, and
        #  configure the 'etc_smbpasswd' module, above.
```

รูปที่ ข.65 แสดงการแก้ไขข้อมูลในส่วนของ authorize{...} ในไฟล์ radiusd.conf

```
        #  See "Accounting queries" in sql.conf
        sql

        #
        #  Instead of sending the query to the SQL server,
```

รูปที่ ข.66 แสดงการแก้ไขข้อมูลในส่วนของ accounting{...} ในไฟล์ radiusd.conf

```
session {
        radutmp

        #
        #  See "Simultaneous Use Checking Querie" in sql.conf
        sql
}
```

รูปที่ ข.67 แสดงการแก้ไขข้อมูลในส่วนของ session{...} ในไฟล์ radiusd.conf

ข.8.12 ทำการเปิดไฟล์ชื่อ "sql.conf" ด้วยคำสั่งดังรูปที่ ข.68 แล้วแก้ไขข้อความ readclients โดยการนำคอมเม้นออก แล้วกำหนดให้เท่ากับ yes ดังรูป ที่ ข.69

```
root@Desktop:~# vi /etc/freeradius/sql.conf
```

รูปที่ ข.68 แสดงคำสั่งเปิดไฟล์ sql.conf

```
        #
        # Set to 'yes' to read radius clients from the database ('nas'
        readclients = yes
}
```

รูปที่ ข.69 แสดงการแก้ไขข้อความในไฟล์ sql.conf

ข.8.13 ทำการเพิ่ม Users เพื่อใช้ในการทดสอบ โดยในที่นี้จะมี Users เป็น mysqltest และ Password เป็น testsecret ดังรูปที่ ข.70

```
root@Desktop:~# echo "INSERT INTO radcheck (UserName,Attribute,op,Value) VALUES
 ('mysqltest','User-Password','==','testsecret');" | mysql -u radius -p radius
Enter password:
```

รูปที่ ข.70 แสดงการเพิ่ม Users เพื่อใช้ในการทดสอบ

ข.8.14 ทำการ restart RADIUS Server ด้วยคำสั่งดังรูป

```
root@Desktop:~# /etc/init.d/freeradius start
 * Starting FreeRADIUS daemon freeradius
Mon Mar 30 05:41:51 2009 : Info: Starting - reading configuration files ...
                                                                    [ OK ]
```

รูปที่ ข.71 แสดงการ Restart RADIUS Server

ข.8.15 ทำการทดสอบการทำงานของ RADIUS Server ในการตรวจสอบผู้ใช้จากฐานข้อมูล ด้วยคำสั่งดังรูป หากการทดสอบสำเร็จจะแสดงข้อความ "Access-Accept"

```
root@Desktop:/home/soda# radtest mysqltest testsecret 127.0.0.1 0 radiussecret
Sending Access-Request of id 130 to 127.0.0.1 port 1812
        User-Name = "mysqltest"
        User-Password = "testsecret"
        NAS-IP-Address = 255.255.255.255
        NAS-Port = 0
rad_recv: Access-Accept packet from host 127.0.0.1:1812, id=130, length=20
```

รูปที่ ข.72 แสดงการทดสอบการทำงานของ RADIUS Server ในการตรวจสอบผู้ใช้จากฐานข้อมูล

ข.9. การติดตั้ง SSL

ก่อนติดตั้ง SSL ต้องมีการตรวจสอบให้แน่ใจเสียก่อนว่าได้มีการติดตั้ง LAMP (Linux, Apache, MySQL, PHP) เป็นที่เรียบร้อยแล้ว หากไม่แน่ใจให้ใช้คำสั่ง "tasksel" เพื่อตรวจสอบ ถ้าหากแน่ใจแล้วว่ามีการติดตั้งครบหมดทุกตัว สามารถทำการติดตั้ง SSL ได้

ข.9.1 พิมพ์คำสั่งติดตั้ง SSL ดังรูปที่ ข.73 แล้วกดปุ่ม Enter ที่แป้นพิมพ์ เพื่อเริ่มการติดตั้ง หากมีคำถามให้ทำการพิมพ์ Y แล้วกดปุ่ม Enter ดังรูปที่ ข.74

```
root@Desktop:~# apt-get install ssl-cert
```

รูปที่ ข.73 แสดงคำสั่งติดตั้ง SSL

```
After this operation, 12.5MB of additional disk space will be used.
Do you want to continue [Y/n]? y
Get:1 http://th.archive.ubuntu.com hardy-updates/main openssl-blacklist 0.3.3-
```

รูปที่ ข.74 แสดงการตอบคำถามขณะติดตั้ง SSL

ข.9.2 ทำการสร้างไดเรกทอรี่ SSL ขึ้นมาเพื่อเก็บ Certificate ที่ถูกสร้างขึ้นโดยใช้คำสั่ง ดังรูปที่ ข.75 แล้วทำการตรวจสอบว่ามีไดเรกทอรี่ SSL หรือยัง ด้วยคำสั่ง ดังรูปที่ ข.76

```
root@Desktop:~# mkdir /etc/apache2/ssl
```

รูปที่ ข.75 แสดงคำสั่งสร้างไดเรกทอรี่ SSL เพื่อเก็บ Certificate

```
root@Desktop:~# cd /etc/apache2
root@Desktop:/etc/apache2# ls
apache2.conf  envvars     mods-available  ports.conf       sites-enabled
conf.d        httpd.conf  mods-enabled    sites-available  ssl
```

รูปที่ ข.76 แสดงการตรวจสอบหาไดเรกทอรี่ SSL

ข.9.3 ทำการสร้าง Self-signed Certificates ด้วยคำสั่งดังรูปที่ ข.77

```
root@Desktop:/etc/apache2/ssl# make-ssl-cert /usr/share/ssl-cert/ssleay.cnf
/etc/apache2/ssl/apache.pem
```

รูปที่ ข.77 แสดงการสร้าง Self-signed Certificates

ข.9.4 ทำการติดตั้ง Module SSL ด้วยคำสั่งดังรูปที่ ข.78

```
root@Desktop:/etc/apache2/ssl# a2enmod ssl
Module ssl installed; run /etc/init.d/apache2 force-reload to enable.
```

รูปที่ ข.78 แสดงการติดตั้ง Module SSL

ข.9.5 ทำการ Reload Apache ด้วยคำสั่งดังรูปที่ ข.79

```
root@Desktop:~# /etc/init.d/apache2 force-reload
 * Reloading web server config apache2                              [ OK ]
```

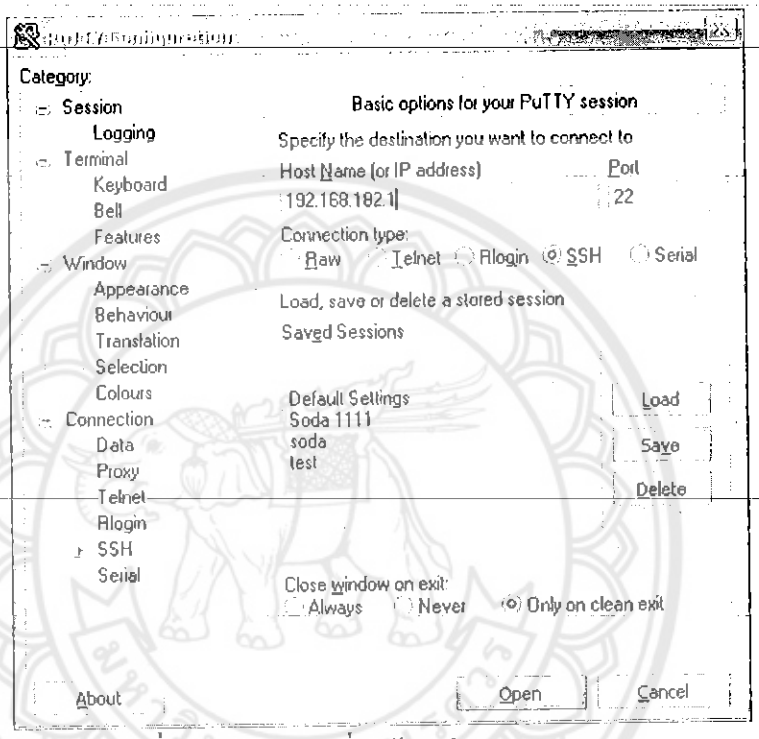
รูปที่ ข.79 แสดงการ Reload Apache

ภาคผนวก ค

การใช้งานโปรแกรมที่เกี่ยวข้อง

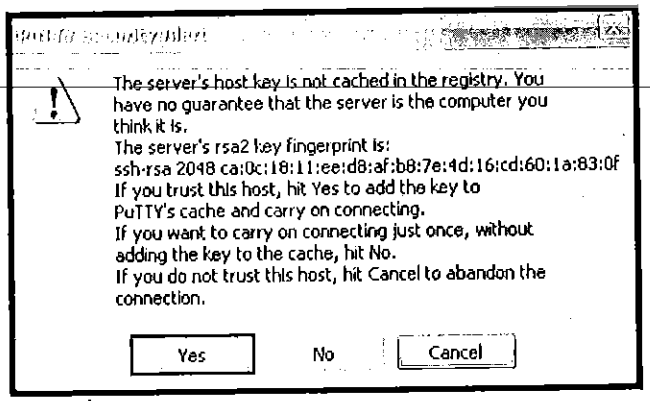
ค.1. การใช้งานโปรแกรม PuTTY

ค.1.1 ทำการดับเบิ้ลคลิกที่โปรแกรม PuTTY ก็จะมีการแสดงผลดังรูปที่ ค.1 หลังจากนั้นให้ทำการพิมพ์หมายเลขไอพีของ Proxy Server และพิมพ์หมายเลข Port เป็น 22 แล้วคลิก Open



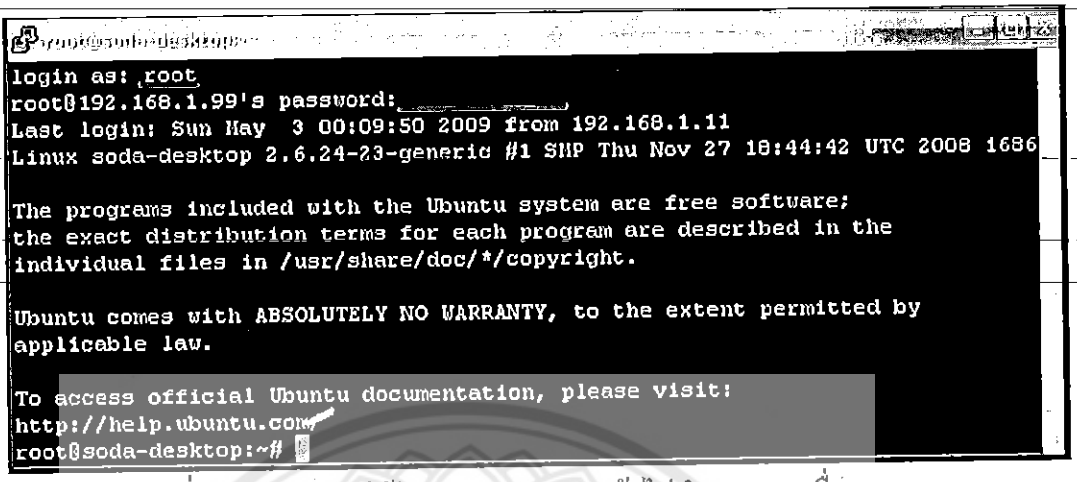
รูปที่ ค.1 แสดงการเริ่มใช้งานโปรแกรม PuTTY

ค.1.2 หากมีคำถามให้ทำการคลิกที่ Yes เพื่อเป็นการยืนยันการใช้งานโปรแกรม PuTTY



รูปที่ ค.2 แสดงการยืนยันใช้งานโปรแกรม PuTTY

ค.1.3 เมื่อโปรแกรม PuTTY ทำงานก็จะมีการแสดงผลดังรูป ให้ใส่ login as เป็น root แล้วก็พิมพ์รหัสผ่านตามที่กำหนดไว้ แล้วกดปุ่ม Enter

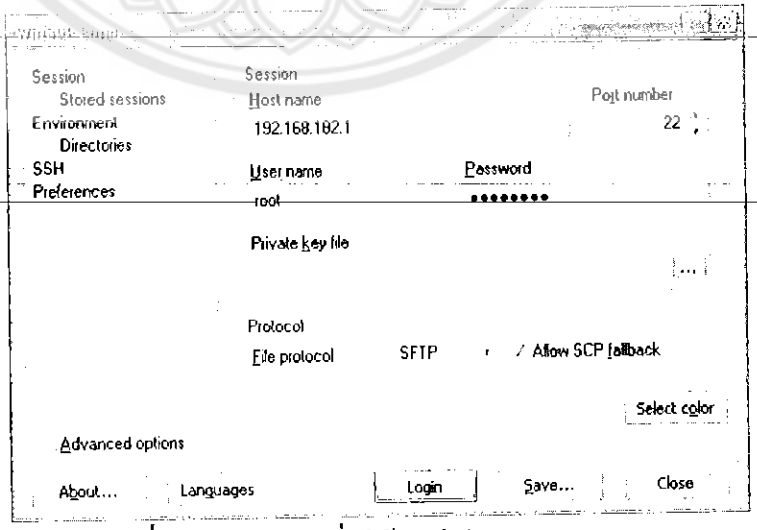


รูปที่ ค.3 แสดงการใช้โปรแกรม PuTTY เข้าไปทำงานบนเครื่อง Server

ค.2. การใช้งานโปรแกรม WinSCP

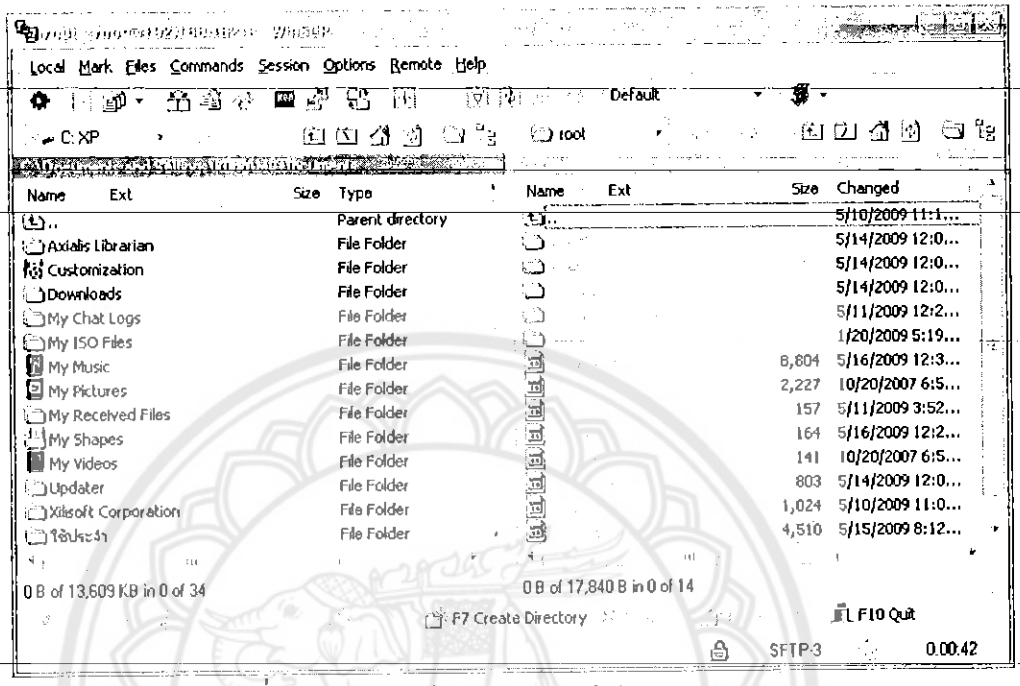
WinSCP เป็นโปรแกรมที่มีการทำงานคล้ายๆ กับโปรแกรม PuTTY โดยมีความสามารถแตกต่างกันคือ โปรแกรม PuTTY เป็นโปรแกรมที่ใช้คัดลอกคำสั่งเข้าสู่อุปกรณ์ที่เชื่อมต่อ แต่โปรแกรม WinSCP เป็นโปรแกรมที่ทำหน้าที่ช่วยจัดการแฟ้มข้อมูลระหว่างอุปกรณ์ที่ทำการเชื่อมต่อ ซึ่งโปรแกรม WinSCP มีวิธีการใช้ดังนี้

ค.2.1 เมื่อเปิดโปรแกรม WinSCP ก็จะมีการแสดงผลดังรูปที่ ค.4 หลังจากนั้นให้ทำการพิมพ์หมายเลขไอพีของ Proxy Server พร้อมทั้งพิมพ์หมายเลข Port เป็น 22 และ User name เป็น "root" ส่วน Password ให้พิมพ์รหัสผ่านของ root แล้วคลิกคำว่า "Login"



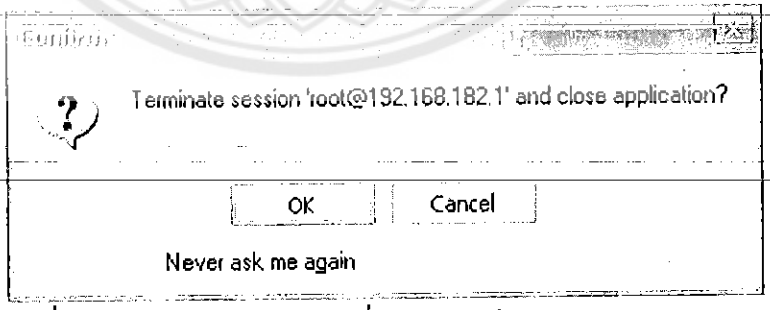
รูปที่ ค.4 แสดงการเริ่มใช้งานโปรแกรม WinSCP

ค.2.2 เมื่อเข้าถึง root สำเร็จ โปรแกรม WinSCP จะแสดงผลดังรูปที่ ค.5 ซึ่งจะแบ่งออกเป็น 2 ฝั่ง โดยที่ฝั่งซ้ายมือจะเป็นแฟ้มข้อมูลทั้งหมดที่อยู่ในอุปกรณ์ที่ใช้เชื่อมต่อ Proxy Server ส่วนฝั่งขวามือจะเป็นแฟ้มข้อมูลทั้งหมดที่มีอยู่ใน Proxy Server



รูปที่ ค.5 แสดงหน้าต่างหลักของโปรแกรม WinSCP

ค.2.3 เมื่อไม่ต้องการใช้งานโปรแกรม WinSCP แล้ว ควรจะปิดโปรแกรมโดยการคลิกที่เครื่องหมายกากบาท ที่มุมขวาด้านบนของหน้าต่างแสดงผลโปรแกรม แล้วจะมีการแสดงผลดังรูปที่ ค.6 ให้คลิกที่คำว่า "OK" เพื่อยืนยันการเลิกใช้งานโปรแกรม



รูปที่ ค.6 แสดงหน้าต่างยืนยันเพื่อปิดการใช้งานโปรแกรม WinSCP

ภาคผนวก ง

การใช้งานอื่นๆ

ง.1. การสร้างหน้าเว็บสำหรับลงชื่อเข้าใช้

ง.1.1 ทำการสร้างไดเรกทอรี่ /var/www/cgi-bin ด้วยคำสั่งดังรูปที่ ง.1

```
root@Desktop:~# mkdir -p /var/www/cgi-bin
```

รูปที่ ง.1 แสดงคำสั่งสร้างไดเรกทอรี่ /var/www/cgi-bin

ง.1.2 ทำการสร้างไฟล์ hotspotlogin.cgi ไปวางในไดเรกทอรี่ที่ได้สร้างไว้ก่อนหน้า

```
root@Desktop:~# zcat -c /usr/share/doc/chillispot/hotspotlogin.cgi.gz | tee
 /var/www/cgi-bin/hotspotlogin.cgi
```

รูปที่ ง.2 แสดงการสร้างไฟล์ hotspotlogin.cgi

ง.1.3 ทำการพิมพ์คำสั่งดังรูปที่ ง.3 เพื่อให้ไฟล์ hotspotlogin.cgi สามารถ Execute ได้

```
root@Desktop:~# chmod a+x /var/www/cgi-bin/hotspotlogin.cgi
```

รูปที่ ง.3 แสดงคำสั่งเพื่อให้ไฟล์ hotspotlogin.cgi สามารถ Execute ได้

ง.1.4 ทำการพิมพ์คำสั่งเปิดไฟล์ hotspotlogin.cgi ดังรูปที่ ง.4 แล้วทำการเอาคอมเม้นหน้า $uamsecret และ $userpassword ออก และแก้ไขรหัสผ่านของ $uamsecret ให้เหมือนกับที่ได้ตั้งไว้ขณะติดตั้ง ChilliSpot ดังรูปที่ ง.5

```
root@Desktop:~# vi /var/www/cgi-bin/hotspotlogin.cgi
```

รูปที่ ง.4 แสดงคำสั่งสร้างไฟล์ hotspotlogin.cgi

```
# Shared secret used to encrypt challenge with. Prevents dictionary attacks.
# You should change this to your own shared secret.
$uamsecret = "uamsecret";

# Uncomment the following line if you want to use ordinary user-password
# for radius authentication. Must be used together with $uamsecret.
$userpassword=1;
```

รูปที่ ง.5 แสดงการแก้ไขข้อมูลในไฟล์ hotspotlogin.cgi

ง.1.5 ทำการเปิดใช้งาน ChilliSpot ด้วยคำสั่ง ดังรูปที่ ง.6

```
root@Desktop:~# /etc/init.d/chillispot start
```

รูปที่ ง.6 แสดงการใช้คำสั่งเพื่อเปิดใช้งาน ChilliSpot

ง.1.6 ทำการสร้างไฟล์ welcome.html ด้วยคำสั่งดังรูปที่ ง.7 แล้วทำการพิมพ์คำสั่งภาษา HTML ดังรูปที่ ง.8 แล้วทำการบันทึก

```
root@Desktop:~# vi /var/www/welcome.html
```

รูปที่ ง.7 แสดงคำสั่งสร้างไฟล์ welcome.html

```
<html>
<head><title> Welcome to Mr.Soda Internet Service </title>
</head>
<body>
<center>
<H1><font color="red">TESTING ONLY</font></H1>
<img src="chillispot.png">
<H3><font color="blue">Welcome to Mr.soda Internet Service.</font></H3>
<p>You are connected to an authentication and restricted network access point.
<H3><a href="http://192.168.182.1:39990/prelogin">Click here to login</a><H/3>
<p>
<p>Enjoy.
</center>
</body>
</html>
```

รูปที่ ง.8 แสดงการเขียนคำสั่งภาษา HTML ในไฟล์ welcome.html

ง.2. การสร้าง Virtual Host

ง.2.1 ทำการสร้าง Virtual Host ชื่อ “hotspot” ด้วยคำสั่งดังรูปที่ ง.9 แล้วเพิ่มข้อมูลลงไป ดังรูปที่ ง.10 แล้วทำการบันทึก

```
root@Desktop:~# vi /etc/apache2/sites-available/hotspot
```

รูปที่ ง.9 แสดงคำสั่งสร้างการสร้าง Virtual Host

```
NameVirtualHost 192.168.182.1:443
<VirtualHost 192.168.182.1:443>
        ServerAdmin webmaster@domain.org
        DocumentRoot "/var/www"
        ServerName "192.168.182.1"
        <Directory "/var/www/">
                Options Indexes FollowSymLinks MultiViews
                AllowOverride None
                Order allow,deny
                Allow from all
        </Directory>
        ScriptAlias /cgi-bin/ /var/www/cgi-bin/
        <Directory "/var/www/cgi-bin/">
                AllowOverride None
                Options ExecCGI -MultiViews +SymLinksIfOwnerMatch
                Order allow,deny
                Allow from all
        </Directory>
        ErrorLog /var/log/apache2/hotspot-error.log
        LogLevel warn
        CustomLog /var/log/apache2/hotspot-access.log combined
        ServerSignature On
        SSLEngine On
        SSLCertificateFile /etc/apache2/ssl/apache.pem
</VirtualHost>
:wq
```

รูปที่ ง.10 แสดงการเพิ่มข้อมูลลงในไฟล์ hotspot

ง.2.2 ทำการ Enable SSL Virtualhost ด้วยคำสั่งดังรูปที่ ง.11

```
root@Desktop:~# a2ensite hotspot
Site hotspot installed; run /etc/init.d/apache2 reload to enable.
```

รูปที่ ง.11 แสดงการ Enable SSL Virtualhost

ง.2.3 ทำการ Reload Apache Web Server ด้วยคำสั่งดังรูป

```
root@Desktop:~# /etc/init.d/apache2 reload
 * Reloading web server config apache2                              [ OK ]
```

รูปที่ ง.12 แสดงคำสั่งเพื่อ Reload Apache Web Server

ง.2.4 ทำการพิมพ์คำสั่งเปิดไฟล์ ports.conf ดังรูปที่ ง.13 แล้วทำการแก้ไขข้อมูลในไฟล์ ดังรูปที่ ง.14 เพื่อปรับตั้งค่าการ Listen Port

```
root@Desktop:~# vi /etc/apache2/ports.conf
```

รูปที่ ง.13 แสดงคำสั่งเปิดไฟล์ ports.conf

```
Listen 192.168.182.1:80
Listen 192.168.182.1:443

#<IfModule mod_ssl.c>
#    Listen 443
#</IfModule>
```

รูปที่ ง.14 แสดงการแก้ไขข้อมูลในไฟล์ ports.conf

ง.2.5 ทำการพิมพ์คำสั่งเปิดไฟล์ที่ชื่อว่า "default" ดังรูปที่ ง.15 แล้วทำการแก้ไขข้อมูลในไฟล์ ดังรูปที่ ง.16 เพื่อให้มีการ Listen Port ที่ Port 80

```
root@Desktop:~# vi /etc/apache2/sites-available/default
```

รูปที่ ง.15 แสดงคำสั่งเปิดไฟล์ Default

```
NameVirtualHost *:80
<VirtualHost *:80>
```

รูปที่ ง.16 แสดงการแก้ไขข้อมูลในไฟล์ Default

ง.2.6 ทำการพิมพ์คำสั่งเปิดไฟล์ที่ชื่อว่า "hosts" ดังรูปที่ ง.17 แล้วทำการแก้ไขข้อมูลในไฟล์ ดังรูปที่ ง.18 โดยกำหนดชื่อและ IP Address ของ Hosts ได้ตามต้องการ

```
root@Desktop:~# vi /etc/hosts
```

รูปที่ ง.17 แสดงคำสั่งเปิดไฟล์ Default

```
127.0.0.1       localhost
192.168.182.1   Desktop
```

รูปที่ ง.18 แสดงการแก้ไขข้อมูลในไฟล์ Default

ง.2.7 ทำการพิมพ์คำสั่ง ดังรูปที่ ง.17 เพื่อ Restart Apache Web Server

```
root@Desktop:~# /etc/init.d/apache2 restart
```

รูปที่ ง.19 แสดงคำสั่งเพื่อ Restart Apache Web Server

ประวัติผู้เขียนโครงงาน

ชื่อ นายพรพนม นันทะเสน

ภูมิลำเนา 200 หมู่ 1 ต.ออย อ.ปง จ.พะเยา 56140

ประวัติการศึกษา

- จบระดับมัธยมศึกษาจากโรงเรียนปงพัฒนาวิทยาคม
- ปัจจุบันกำลังศึกษาในระดับปริญญาตรีชั้นปีที่ 4 สาขาวิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยนเรศวร

E-mail : mr.soda@msn.com, mr.soda@live.com

ชื่อ นางสาวพลิตา สำเภาเงิน

ภูมิลำเนา 1/34 ถ.สนามบิน ต.ในเมือง อ.เมือง จ.พิษณุโลก 65000

ประวัติการศึกษา

- จบระดับประถมศึกษาจากโรงเรียนอนุบาลโรจนวิทย์
- จบระดับมัธยมศึกษาตอนต้น จากโรงเรียนเฉลิมขวัญสตรี
- จบระดับมัธยมศึกษาตอนปลาย จากโรงเรียนเฉลิมขวัญสตรี
- เข้าศึกษาระดับอุดมศึกษา ปีการศึกษา 2548
- ประธานชมรม Computer & IT สโมสรนิสิตคณะวิศวกรรมศาสตร์ ปีการศึกษา 2550
- นิสิตทุนกิจกรรม คณะวิศวกรรมศาสตร์ ปีการศึกษา 2551
- ปัจจุบันกำลังศึกษาในระดับปริญญาตรีชั้นปีที่ 4 สาขาวิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยนเรศวร

E-mail : ps_pupe@hotmail.com, poupee_doll@windowlives.com