



คู่มือประกอบการฝึกอบรมเชิงปฏิบัติการ

การติดตั้ง Authentication

คำนำ

ตามที่พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มีผลบังคับใช้ตั้งแต่วันที่ 22 สิงหาคม 2550 นั้น มีผลทำให้หน่วยงานต่างๆ ซึ่งเป็นผู้ให้บริการเข้าถึงระบบเครือข่ายอินเทอร์เน็ต จำเป็นต้องเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Data) ไว้อย่างน้อย 90 วัน ปรากฏว่าหน่วยงานต่างๆ ส่วนใหญ่ยังขาดความรู้ความเข้าใจในเจตนารมณ์ของกฎหมาย และวิธีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Data) ที่ถูกต้องและครบถ้วนตามที่กฎหมายกำหนด

ดังนั้นเพื่อให้หน่วยงานต่างๆ สามารถเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Data) ได้ถูกต้องและครบถ้วนตามที่กฎหมายกำหนด และสามารถประหยัดงบประมาณในการจัดซื้อซอฟต์แวร์จากต่างชาติ โดยการนำซอฟต์แวร์ Open Source ไปใช้ในการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Data) สำนักงานส่งเสริมอุตสาหกรรมซอฟต์แวร์แห่งชาติ (องค์การมหาชน) จึงเห็นควรให้มีการจัดจ้างทำคู่มือ พร้อมชุดติดตั้ง (Software package), Slideบรรยายประกอบการฝึกอบรมปฏิบัติการ, Courseware สำหรับใช้ทบทวนหรือศึกษาค้นคว้าด้วยตนเอง ให้กับผู้ประกอบการและผู้ดูแลระบบของหน่วยงานภาครัฐ นอกจากนั้นจัดให้มีการสนับสนุนภายหลังการอบรมผ่านทางเว็บไซต์ และทางโทรศัพท์ ให้กับผู้เข้าร่วมโครงการ โดยในการจัดจ้างในครั้งนี้ จะเป็นประโยชน์ต่อ ผู้ประกอบการและผู้ดูแลระบบของหน่วยงานภาครัฐหน่วยงานต่างๆ ในการที่จะนำไปใช้ นอกจากนี้แล้วสำนักงานฯ จะกำหนดให้คู่มือและชุดติดตั้งต่างๆ มีการกำหนดสิทธิในการเผยแพร่แบบโอเพนซอร์ส ซึ่งจะช่วยให้หน่วยงานต่างๆ สามารถนำเอาคู่มือและชุดติดตั้งประกอบการฝึกอบรม ไปแก้ไขหรือพัฒนาต่อได้ ในกรณีที่มีการเปลี่ยน version ซึ่งจะเป็นการทำให้บุคลากรของผู้ประกอบการ และหน่วยงานต่างๆ ในประเทศไทยทันต่อการเปลี่ยนแปลงเทคโนโลยีอยู่เสมอ

เอกสารฉบับนี้เป็นคู่มือโครงการฝึกอบรมผู้ประกอบการในการติดตั้งและให้บริการคำปรึกษาระบบเก็บข้อมูลจราจร (Traffic Data) ตาม พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ด้วยซอฟต์แวร์โอเพนซอร์ส สนับสนุนโดย สำนักงานส่งเสริมอุตสาหกรรมซอฟต์แวร์แห่งชาติ (องค์การมหาชน) ซึ่งต่อไปนี้เป็น การสรุปวัตถุประสงค์ ผลที่คาดว่าจะได้รับ โครงสร้างของหลักสูตร และหลักสูตรการฝึกอบรมของโครงการ

วัตถุประสงค์

1. เพื่อช่วยให้ผู้ประกอบการและผู้ดูแลระบบเข้าใจวัตถุประสงค์ที่แท้จริงของการเก็บข้อมูลจราจร (Traffic Data) ตาม มาตรา 26 ของ พรบ. การกระทำผิดด้วยคอมพิวเตอร์ พ.ศ. 2550
2. เพื่อให้ผู้ประกอบการและผู้ดูแลระบบเข้าใจวิธีการเก็บข้อมูลจราจร (Traffic Data) ที่ถูกต้องตามมาตรา 26 ของ พรบ. การกระทำผิดด้วยคอมพิวเตอร์ พ.ศ. 2550
3. เพื่อให้ผู้ประกอบการและผู้ดูแลระบบสามารถเก็บข้อมูลจราจร (Traffic Data) ได้ด้วยซอฟต์แวร์โอเพนซอร์ส อย่างถูกต้องและครบถ้วนตามที่กฎหมายกำหนด
4. เพื่อให้ผู้ประกอบการสามารถให้คำปรึกษาแก่ผู้รับบริการอย่างถูกต้องและครบถ้วนตามที่กฎหมายกำหนด
5. เพื่อให้ผู้ประกอบการลดค่าใช้จ่ายในการจัดเก็บข้อมูลจราจร (Traffic Data)

ผลที่คาดว่าจะได้รับ

1. ได้หลักสูตร และระบบต้นแบบนำซอฟต์แวร์โอเพนซอร์สไปใช้เก็บข้อมูลจราจร (Traffic Data)
2. ประอบการสามารถนำความรู้ที่ได้รับไปให้บริการให้คำปรึกษาและติดตั้งระบบเก็บข้อมูลจราจร (Traffic Data) ด้วยซอฟต์แวร์โอเพนซอร์สอย่างถูกต้องและครบถ้วนตามที่กฎหมายกำหนด
3. System Admin ของหน่วยงานภาครัฐสามารถนำซอฟต์แวร์โอเพนซอร์สไปใช้เก็บข้อมูลจราจร (Traffic Data) ได้อย่างถูกต้องและครบถ้วนตามที่กฎหมายกำหนด

หลักสูตรการฝึกอบรม

ชื่อหลักสูตร หลักสูตรการติดตั้งระบบเก็บข้อมูลจราจร (Traffic Data) ตามพรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับด้วยคอมพิวเตอร์ พ.ศ. 2550 ด้วยซอฟต์แวร์โอเพนซอร์ส

วัตถุประสงค์ ฝึกอบรมโดยการบรรยาย สาธิต และฝึก Hands-on ตาม พรบ.ว่าด้วยการกระทำความผิดเกี่ยวกับด้วยคอมพิวเตอร์ พ.ศ. 2550 ด้วยซอฟต์แวร์โอเพนซอร์ส

จำนวนวัน 5 วัน

คุณสมบัติผู้เข้าฝึกอบรม

1. มีความรู้ทางด้านคอมพิวเตอร์และ Open Source
2. เป็นผู้ดูแลระบบคอมพิวเตอร์ให้กับหน่วยงาน
3. เป็นผู้ที่สนใจในระบบการติดตั้ง ระบบเก็บข้อมูลจราจร (Traffic Data) ตาม พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับด้วยคอมพิวเตอร์ พ.ศ. 2550 ด้วยซอฟต์แวร์โอเพนซอร์ส

ลักษณะการฝึกอบรม : บรรยาย สาธิต ฝึกปฏิบัติ แลกเปลี่ยนประสบการณ์

โครงสร้างหลักสูตร

วันที่ 1 Syslog-NG

เป็นการอธิบายถึง พรบ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 อธิบายถึงสถาปัตยกรรมของระบบให้ถูกต้องตาม พรบ. อธิบายถึงสถาปัตยกรรมของ Syslog-NG และวิธีการติดตั้ง

เป็นหลักสูตรที่ตรงกับข้อ 8 ของประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่องหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550

วันที่ 2 ปฏิบัติการการติดตั้งซอฟต์แวร์ Syslog-NG

เป็นการฝึกการปฏิบัติการติดตั้ง Syslog-NG โดยการสาธิต และให้ผู้เข้ารับการอบรมติดตั้ง มีผู้ช่วยฝึกให้การช่วยเหลือ

วันที่ 3 NTP Server และ NTP Client

ปฏิบัติการการติดตั้งซอฟต์แวร์ NTP Server และ NTP Client

เป็นการอธิบายถึงสถาปัตยกรรมของ NTP ทั้ง Server และ Client รวมทั้งเป็นการฝึกการปฏิบัติการติดตั้ง NTP Server และ NTP Client โดยการสาธิต และให้ผู้เข้ารับการอบรมติดตั้ง มีผู้ช่วยฝึกให้การช่วยเหลือ

เป็นหลักสูตรที่ตรงกับข้อ 9 ของประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่องหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550

วันที่ 4 Authentication

เป็นการอธิบายถึงสถาปัตยกรรมของ Authentication รวมทั้งเป็นการฝึกการปฏิบัติการติดตั้ง Authentication โดยการสาธิต และให้ผู้เข้ารับการอบรมติดตั้ง มีผู้ช่วยฝึกให้การช่วยเหลือ

เป็นหลักสูตรที่ตรงกับข้อ 2 ภาคผนวก ข แนบท้ายประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550

วันที่ 5 ปฏิบัติการการนำ Syslog-NG, NTP Server, NTP Client และ Authentication ทำงานร่วมกัน

ให้ผู้เข้ารับการอบรมทำการติดตั้ง Syslog-NG, NTP Server, NTP Client และ Authentication ทำงานร่วมกัน มีผู้ช่วยฝึกให้การช่วยเหลือ

การวัดผล : ผู้เข้าอบรมจะต้องสามารถทำการติดตั้ง Syslog-NG, NTP Server, NTP Client และ Authentication ได้

ประกาศนียบัตร : ผู้ที่ผ่านหลักสูตรตามเงื่อนไขการวัดผล จะได้ Certificate of Completion จาก SIPA หรือจาก ATSI หรือ SIPA ร่วมกับ ATSI



คู่มือประกอบการฝึกอบรมเชิงปฏิบัติการ
การติดตั้ง Authentication

ลิขสิทธิ์โดย

สำนักงานส่งเสริมอุตสาหกรรมซอฟต์แวร์แห่งชาติ (องค์การมหาชน)
89/2 หมู่ 3 อาคาร 9 ชั้น 11 บมจ. ทีไอที ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่
กรุงเทพฯ 10210
โทรศัพท์ 0-2554-0400
โทรสาร 0-2554-0401

ผู้ดำเนินการ

สมาคมอุตสาหกรรมซอฟต์แวร์ไทย
99/30 หมู่ 4 ชั้น 5 อาคารซอฟต์แวร์พาร์ค ถ.แจ้งวัฒนะ ข.ปากเกร็ด ต.คลองเกลือ
จ.นนทบุรี 11120
โทรศัพท์ 0-2583-9992, 0-2962-2900 ต่อ 1501 หรือ สายตรง 0-2962-1348
โทรสาร. 0-2962-1349
E-mail: info@atsi.or.th

ผู้บริหารโครงการ

บริษัท เบนซ์มาร์ค วิชั่น จำกัด
Mobile : 089 797 8262
e-mail: bv2551@gmail.com



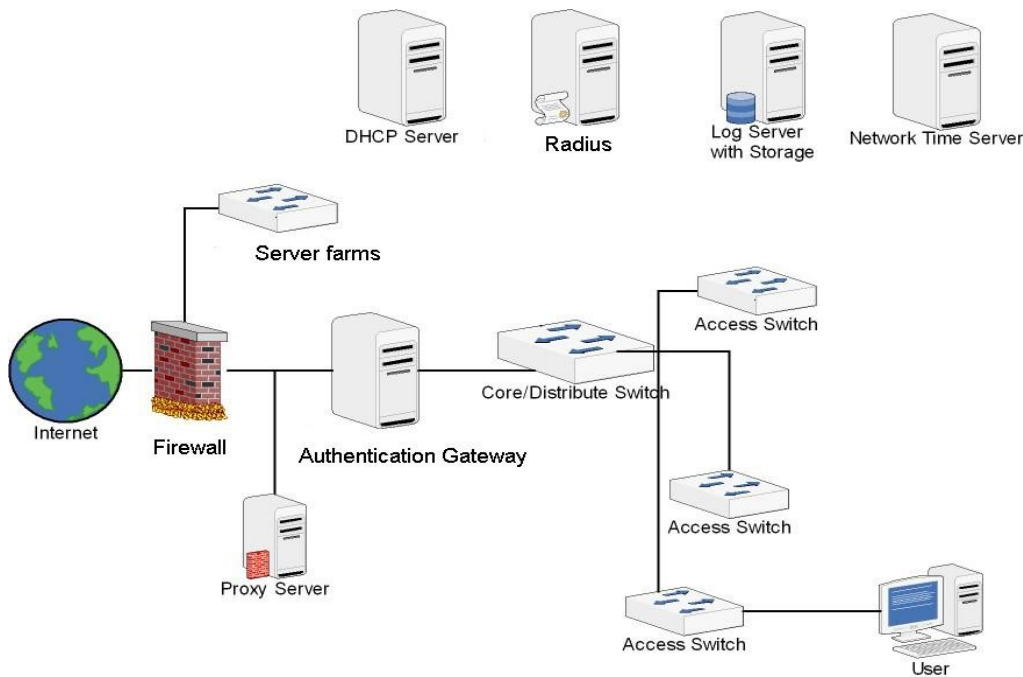
สารบัญ

1. Introduction	1
2. Software Requirement	4
3. Hardware Requirement	4
4. Install Ubuntu 8.04	5
1. Network setup	18
2. Enable TUN/TAP device driver support	18
3. Install OPENSSSH	19
5. Install Chillispot	22
6. Install Firewall	24
7. Install Apache	26
8. Install MySQL Database Server	29
9. Install PHP	31
● Install PhpMyAdmin	33
10. Install Radius Server	35
● Change authorization to sql	39
● SQL Logging	40
● Create login page	43
11. Setup SSL	45
12. Add User	53
13. Logging	60
● Install Time Server	61
● Install Transparent Proxy Squid	68
● Install logging Server	71
References	78

ระบบยืนยันตัวตน (Authentication)

Introduction

ปัจจุบันระบบเครือข่ายอินเทอร์เน็ตนับว่ามีความนิยมแพร่หลายและจากข้อมูลการสำรวจพบว่ามีผู้ใช้งานอินเทอร์เน็ตเพิ่มขึ้นเรื่อย ๆ ในประเทศไทย และสิ่งที่สำคัญคือการให้บริการระบบจะต้องดำเนินการตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ ซึ่งระบุว่าในการเก็บข้อมูลจราจรนั้นต้องสามารถระบุรายละเอียดผู้ใช้บริการระบบเครือข่ายอินเทอร์เน็ตเป็นรายบุคคลได้ (Identification and Authentication) เช่น ลักษณะการใช้บริการ Proxy Server, Network Address Translation(NAT) หรือ Proxy Cache หรือ Cache Engine หรือบริการ Free Internet หรือบริการ 1222 หรือ Wi-Fi Hotspot ต้องสามารถระบุตัวตนของผู้ใช้บริการเป็นรายบุคคลได้จริง

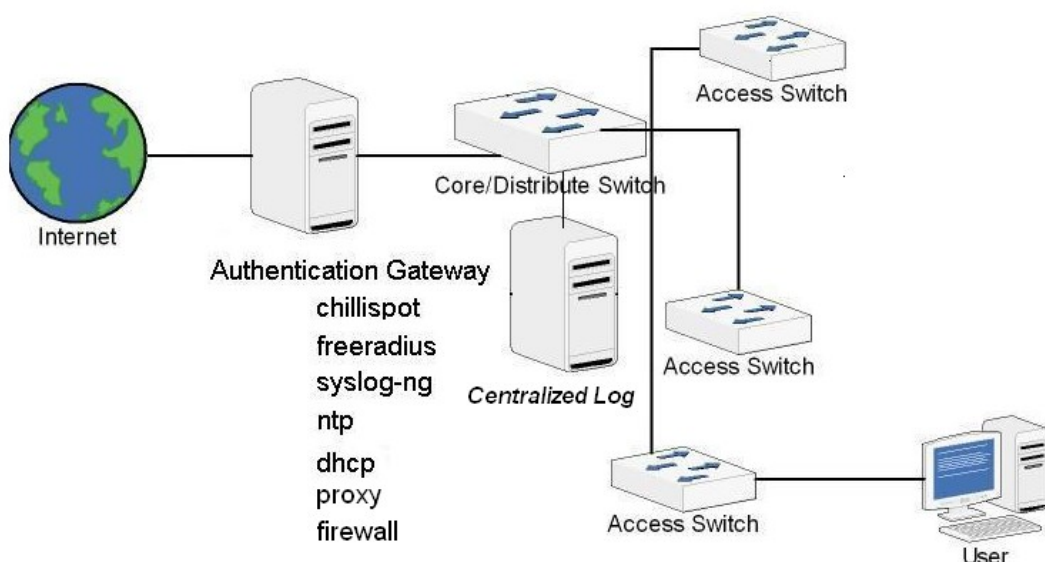


รูปที่ 1 ระบบเครือข่ายคอมพิวเตอร์โดยทั่ว ๆ ไป

ระบบเครือข่ายคอมพิวเตอร์ทั่ว ๆ ไปสามารถแสดงได้ดังรูปที่ 1 ปกติจะแบ่งโซนทั้งหมดของเครือข่ายออกเป็น 3 โซนด้วยกันคือ

1. โชน Demilitarized (DMZ)จะเป็น โชนที่ใช้เชื่อมต่อกับอุปกรณ์เครือข่ายทั้งหมดขององค์กร หรือเรียกว่า โชนของเซิร์ฟเวอร์ฟาร์ม ส่วนใหญ่จะเป็นพื้นที่ให้บริการเซอร์วิสต่าง ๆ ขององค์กร เช่น DHCP, Radius, Log Server, NTP เป็นต้นปกติจะเป็นที่ค่อนข้างจะปลอดภัยที่สุดสำหรับองค์กร
2. โชน Internet จะเป็น โชนที่เชื่อมต่อกับเครือข่ายอินเทอร์เน็ต ประกอบด้วย อุปกรณ์ Router, Firewall และ Proxy Server เป็นต้น
3. โชน Internal จะเป็น โชนที่อยู่ติดกับผู้ใช้บริการภายในองค์กรจะประกอบไปด้วย Core/Distribute Switch, Access Switch และ Authentication Gateway เป็นต้น

จากรูปจะสามารถอธิบายการทำงานได้ว่าเมื่อผู้ใช้บริการต้องการที่จะใช้งานเครือข่ายอินเทอร์เน็ต อุปกรณ์ Authentication Gateway จะบังคับให้ป้อนชื่อผู้ใช้และรหัสผ่านเพื่อเป็นการยืนยันตัวตนตามกฎหมาย โดยระบบบัญชีรายชื่อทั้งหมดจะถูกเก็บไว้ที่ Radius Server และขณะเดียวกันตัว Radius จะตรวจสอบสิทธิและบันทึกข้อมูลการเข้าใช้งานในระบบทั้งหมดไว้ เช่น ล็อกออนเวลาเท่าไรและได้หมายเลขไอพีอะไร รวมถึงเวลาที่เข้ามาใช้งานทั้งหมด เป็นต้น เมื่อผ่านขั้นตอนการตรวจสอบสิทธิการเข้าใช้งาน ผู้ใช้บริการก็จะสามารถใช้งานตามปกติทั่วไป โดยจะมี Time Server เป็นตัวขอเทียบเวลาให้กับเครือข่ายอื่น ๆ ในองค์กร รวมถึง Proxy Server จะช่วยบันทึกค่าให้ว่าผู้ใช้บริการไปใช้งานที่ไหนและเวลาเท่าใดเพื่อใช้จัดเก็บเป็นข้อมูลการจราจรคอมพิวเตอร์ตามพรบ. ว่าด้วยการทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐



รูปที่ 2 แสดงการติดตั้งซอฟต์แวร์ที่ตัวอุปกรณ์ Authentication Gateway เพื่อลดจำนวนเครื่องแม่ข่ายลง

จากรูปที่ 2 จะเห็นได้ว่าเครื่องแม่ข่ายตามรูปที่ 1 สามารถปรับลดลงให้เหลือเพียงเครื่องแม่ข่ายเพียงสองตัว เพื่อให้ประหยัดงบประมาณในองค์กรขนาดกลางถึงเล็ก คือเครื่องแม่ข่ายที่ทำหน้าที่เป็น Authentication Gateway และเครื่องแม่ข่ายที่ทำหน้าที่เป็น Centralized Log

Authentication เป็นวิธีการที่ใช้ในการตรวจสอบผู้ที่มาใช้งานระบบเครือข่ายอินเทอร์เน็ต โดยระบบจะทำการตรวจสอบจาก username และ password ว่าถูกต้องไหม จุดประสงค์หลักของการ Authentication คือพิสูจน์ตัวบุคคลว่าคน ๆ นั้นที่เข้าใช้งานระบบเครือข่ายอินเทอร์เน็ต คือใคร พร้อมทั้งทำการตรวจสอบสิทธิ์ว่าผู้ใช้งานระบบเครือข่ายอินเทอร์เน็ตของท่านนั้นมีสิทธิ์ใช้ได้นานเท่าไรและสามารถ upload หรือ download ได้ด้วยความเร็วเท่าไร ซึ่งระบบนั้นจะทำการตัดผู้ใช้ออกไปจากการให้บริการทันทีที่เวลาหมด อีกทั้งยังสามารถกำหนดเวลาและความเร็วได้ตามความเหมาะสมด้วย ต่อจากนั้นจะทำการบันทึกข้อมูลการใช้งานระบบเครือข่ายอินเทอร์เน็ต ซึ่งจุดประสงค์หลักของขบวนการนี้เพื่อทำรายงานการใช้ระบบเครือข่ายอินเทอร์เน็ต จะทำการยืนยันบันทึกข้อมูลในการใช้งานระบบเครือข่ายอินเทอร์เน็ตไว้อย่างละเอียดโดยสามารถทำรายงานสรุปและสถิติต่าง ๆ ได้ตามความต้องการ

จากเหตุผลดังกล่าวข้างต้นทำให้รู้ว่า การ Authentication ก็เป็นส่วนที่สำคัญและขาดไม่ได้ถ้าเราจะใช้งานระบบเครือข่ายอินเทอร์เน็ต เพราะเป็น“เครื่องพิสูจน์ว่าคุณคือใคร”

หลาย ๆ บริษัท พยายามขายอุปกรณ์ฮาร์ดแวร์และซอฟต์แวร์ โดยชูจุดเด่นเรื่องการตรวจสอบยืนยันบุคคลโดยวิธีการใช้ “MAC Address และ IP Address” ซึ่งเป็นวิธีที่ไม่ถูกต้องเพราะข้อมูลทั้งสองไม่สามารถระบุหรือยืนยันบุคคลได้ ขณะเดียวกัน โปรแกรมที่ใช้ปลอมแปลง MAC และ IP Address ก็มีอยู่มากมาย ที่สำคัญโดยเฉพาะเครื่องลูกข่ายที่มีการหมุนเวียนเข้ามาใช้งานภายในองค์กร เช่น เครื่องคอมพิวเตอร์ในห้องปฏิบัติการคอมพิวเตอร์ภายในสถานศึกษา เป็นต้น ทำให้ไม่สามารถตรวจสอบหาผู้ใช้บริการที่แท้จริง

สำหรับเนื้อหาสำหรับการเรียนในเอกสารนี้จะกล่าวถึงวิธีการสร้างเครื่องแม่ข่าย Authentication Gateway ดังรูปที่ 2 ให้มีหน้าที่ดังนี้ Authentication Gateway, Radius Server, NTP Server, Proxy Server, Logging Server และ Dhcp Server คิดว่าน่าจะทำให้องค์กรต่าง ๆ สามารถสร้างขึ้นมาเองได้ในราคาที่เหมาะสมกับงบประมาณขององค์กรนั้น ๆ และช่วยลดการนำเข้าอุปกรณ์ฮาร์ดแวร์และซอฟต์แวร์ราคาแพงจากต่างประเทศ อีกทั้งเชื่อว่าโดยพื้นฐานของคนไทยเป็นคนที่มีความสามารถแต่ขาดแนวทางในการดำเนินงาน

ผู้เขียนเชื่อเป็นอย่างยิ่งว่า “เอกสารฉบับนี้จะช่วยให้สามารถปฏิบัติตามขั้นตอนต่าง ๆ ตามลำดับและสามารถเข้าใจวิธีการสร้าง Authentication Server โดยไม่ยากจนเกินไป”



Software Requirement

ซอฟต์แวร์ที่ต้องการมีดังต่อไปนี้

- Ubuntu 8.04
- Chillispot
- FreeRadius
- Apache
- MySQL
- Putty

Hardware Requirement

ฮาร์ดแวร์ที่ต้องการมีดังต่อไปนี้

- เครื่อง PC สำหรับทำเป็น Server มี 2 interfaces
- เครื่อง PC สำหรับเป็นตัว test

Software Installation

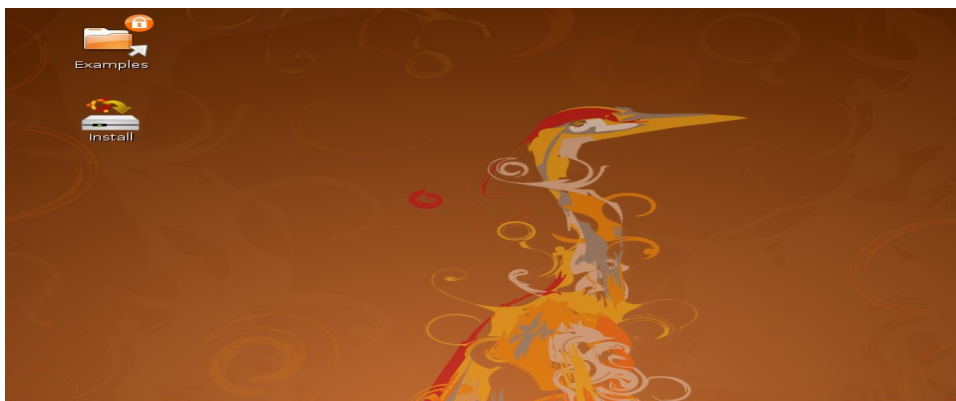
Install Ubuntu 8.04

1. ใส่แผ่น Ubuntu 8.04 แล้ว restart จากนั้นเข้า Bios ตั้งให้ boot จาก CD ก่อน...



รูปที่ 3 แสดงขั้นตอนการเลือกภาษาในการติดตั้ง

2. เลือก Install แล้ว Enter



รูปที่ 4 แสดงการ Install

3. ภาษา ให้เลือก English แล้วกด forward



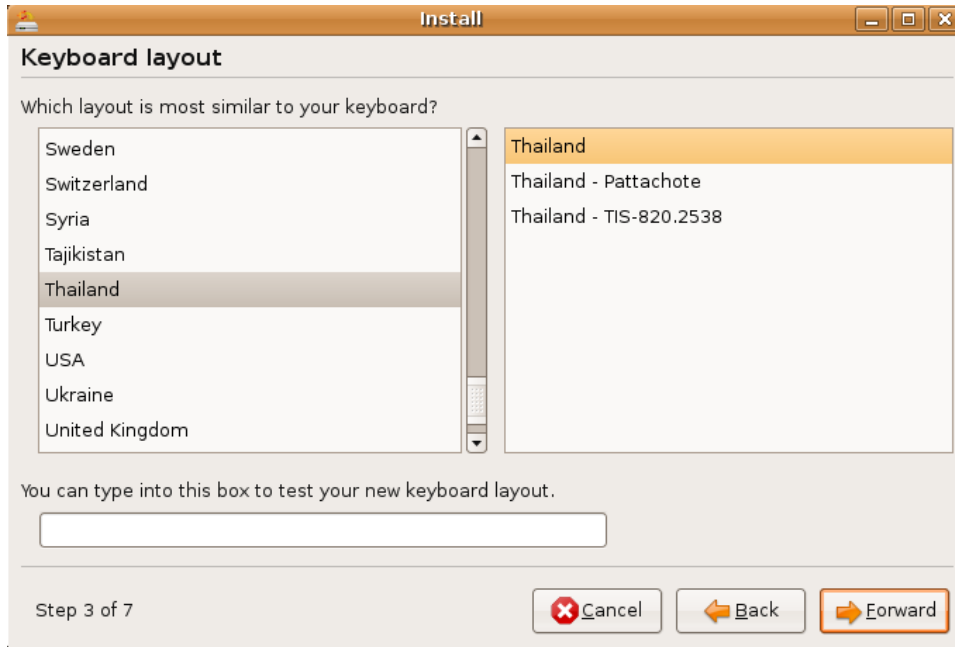
รูปที่ 5 แสดงการเลือกภาษาในขั้นตอนการ install

4. ระยะเวลา ให้เลือก Bangkok



รูปที่ 6 แสดงการตั้งโซนเวลา

5. Keyboard layout เลือก Thailand, Thailand - TIS-620-2538 จากนั้นให้กด forward



รูปที่ 7 แสดงขั้นตอนการกำหนดค่า Keyboard layout

6. จัดการ Partition เพื่อเตรียมลง Ubuntu แนะนำถ้ามีเนื้อที่เหลือจากการที่ถูกลง Windows XP มาให้เลือก Guided ง่ายที่สุด เดี่ยวมันจัดการให้



รูปที่ 8 แสดงการจัดการ Partition แบบ Guided

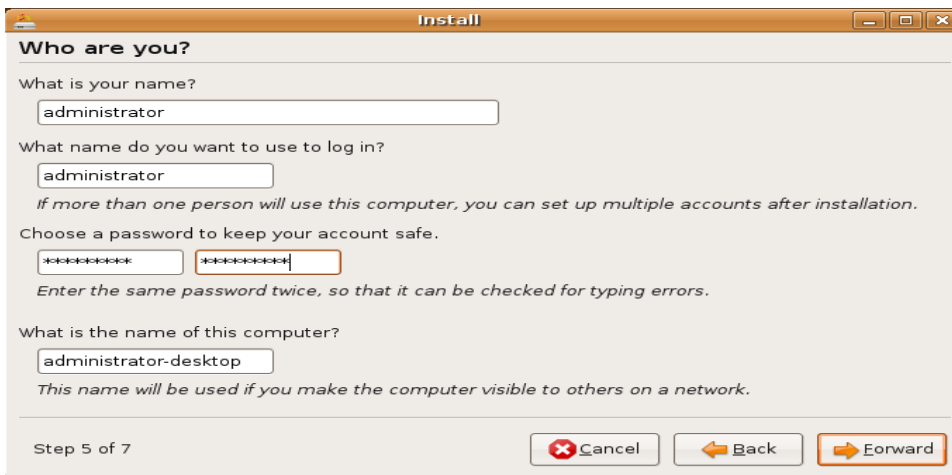
แต่ถ้าเลือกแบบ Manual มันจะให้เราทำการจัดการพาร์ติชันเอง ก็ให้เราสร้าง 2 พาร์ติชันไว้ มี
(1) สร้างเนื้อที่ขนาดไหนก็ได้ ขั้นต่ำ 5 GB เลือกไฟล์ระบบเป็น Ext3 จากนั้นกำหนด Mount point เป็น /



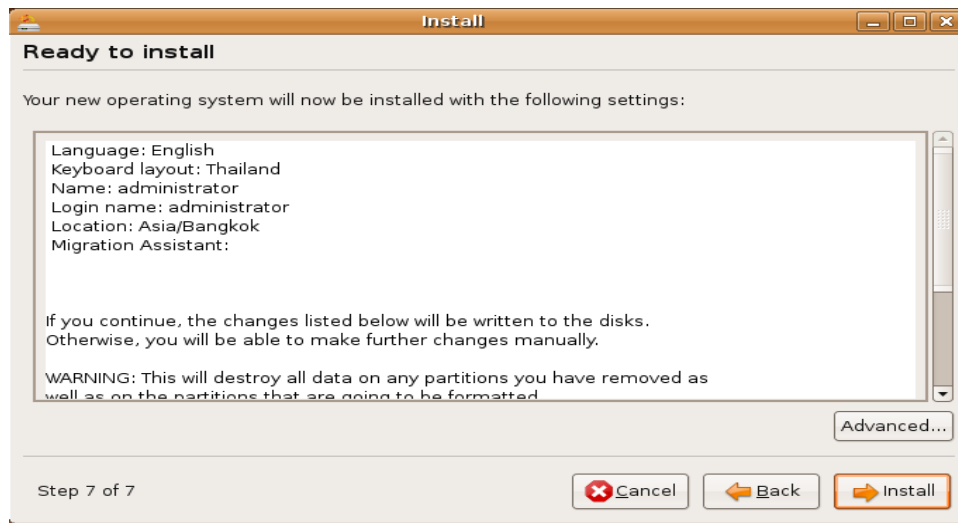
รูปที่ 9 แสดงการจัดการ Partition แบบ Manual

(2) สร้างพาร์ติชันอีก 1 พาร์ติชัน ให้ขนาดเป็น 2 เท่าของ RAM ที่มี (ถ้าใคร Ram 1 GB ไม่จำเป็นต้องสร้างก็ได้ ให้ข้ามขั้นตอนนี้ไปได้) ให้เลือกไฟล์ระบบเป็น Swap partition จากนั้นตรวจสอบความเรียบร้อยแล้วกด forward

7. ทำการสร้าง User และ password ของเราขึ้นมา และห้ามลืมโดยเด็ดขาด เมื่อทำการกรอกข้อมูลเสร็จแล้วกด forward



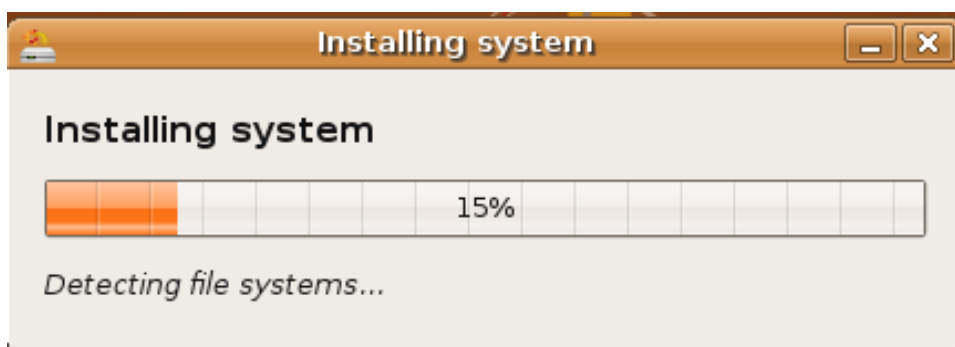
รูปที่ 10 แสดงการสร้าง User และ Password



รูปที่ 11 แสดงรายละเอียดของระบบ

8. ทำการตรวจสอบความถูกต้อง จากนั้นกด Install

แสดงสถานะความคืบหน้าของการ Installing system



รูปที่ 12 แสดงความคืบหน้าในการติดตั้ง

9. เมื่อทำการติดตั้งเสร็จแล้ว ให้ทำการ restart



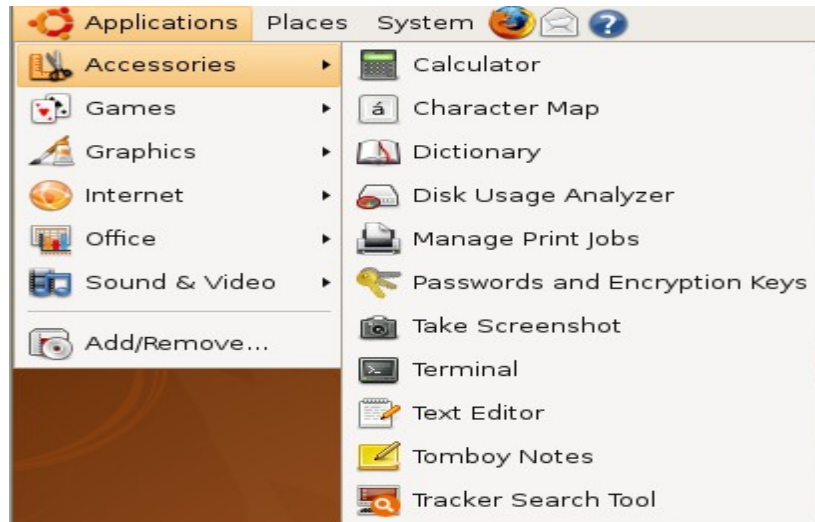
รูปที่ 13 แสดงการ Restart ระบบ

10. เริ่มใช้งาน Ubuntu ได้โดยทำการป้อน User และ password ที่เราได้ทำการกำหนดไว้ในขั้นตอนที่ 7



รูปที่ 14 แสดงการกรอก Username

11. จากนั้นเรียกใช้โปรแกรม Terminal เพื่อใช้ในการกำหนดค่า password ให้กับ root



รูปที่ 15 แสดงการเรียกใช้โปรแกรม Terminal

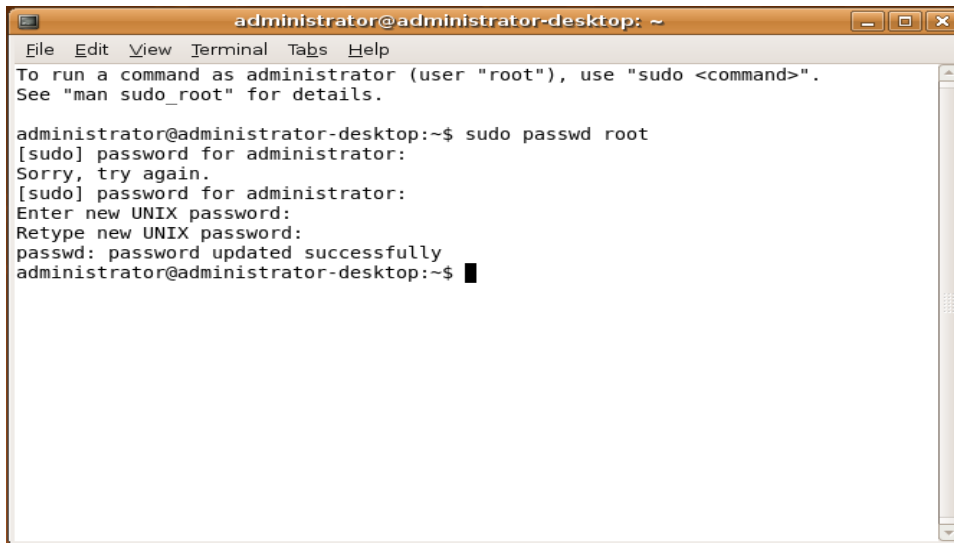
12. ทำการกำหนด password ให้กับ root account โดยใช้คำสั่ง

```
sudo passwd root   กด Enter
```

จากนั้นให้พิมพ์รหัสที่ได้กำหนดไว้ในขั้นตอนที่ 7 และกด Enter จะปรากฏข้อความ

Enter new UNIX password: (ใส่ password สำหรับ root แล้วกด Enter)

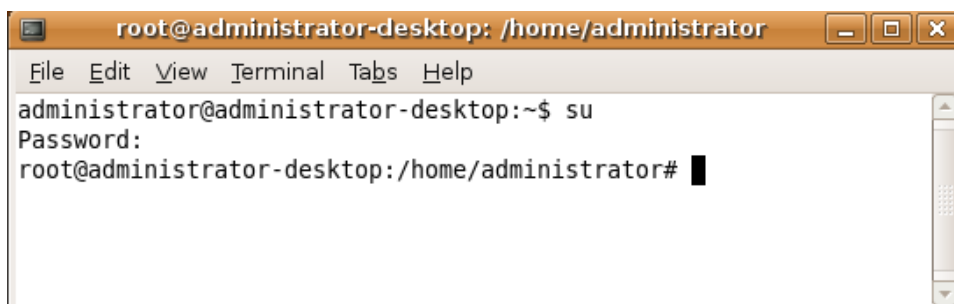
Retype new UNIX password: (ใส่ password อีกครั้ง แล้วกด Enter)



```
administrator@administrator-desktop: ~  
File Edit View Terminal Tabs Help  
To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo_root" for details.  
  
administrator@administrator-desktop:~$ sudo passwd root  
[sudo] password for administrator:  
Sorry, try again.  
[sudo] password for administrator:  
Enter new UNIX password:  
Retype new UNIX password:  
passwd: password updated successfully  
administrator@administrator-desktop:~$ █
```

รูปที่ 16 แสดงการกำหนด Password ให้กับ User root

เมื่อทำการกำหนด password ให้กับ root เสร็จแล้ว ต่อไปเป็นการทดสอบ โดยให้พิมพ์ คำสั่ง su แล้วกด Enter แล้วให้ใส่ password ของ root ที่เราได้ทำการกำหนดไว้ จากนั้นกด Enter จะสังเกตเห็นได้ว่า ลำดับชื่อ เปลี่ยนไปจากเดิมเป็น administrator เป็น root ถือว่าเป็นอันเสร็จสิ้น



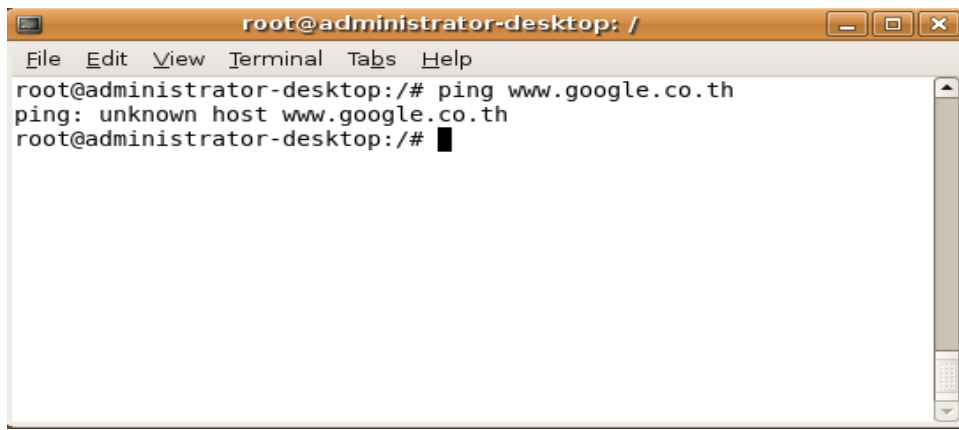
```
root@administrator-desktop: /home/administrator  
File Edit View Terminal Tabs Help  
administrator@administrator-desktop:~$ su  
Password:  
root@administrator-desktop:/home/administrator# █
```

รูปที่ 17 แสดงการทดสอบการกำหนด Password ให้กับ User root

ตรวจสอบว่าเครื่องสามารถใช้งานอินเทอร์เน็ตได้หรือไม่

1. ใช้คำสั่ง ping ในการตรวจสอบว่าเครื่องสามารถใช้งานอินเทอร์เน็ตได้หรือไม่ในที่นี้ได้ทำการ ping ไปยังเว็บไซต์ของ google แต่ในที่นี้เครื่องยังไม่สามารถใช้งานอินเทอร์เน็ตได้ จะปรากฏข้อความว่าไม่รู้จัก host ของ google

```
ping www.google.co.th
```



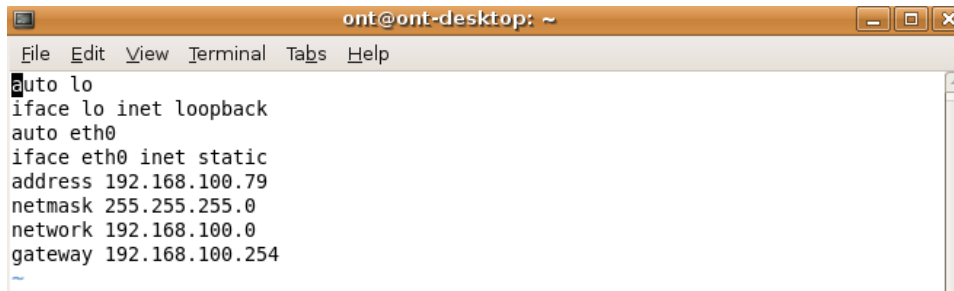
```
root@administrator-desktop: /
File Edit View Terminal Tabs Help
root@administrator-desktop:/# ping www.google.co.th
ping: unknown host www.google.co.th
root@administrator-desktop:/#
```

รูปที่ 18 แสดงการทดสอบการใช้งานอินเทอร์เน็ต

2. วิธีแก้ไขให้เครื่องสามารถใช้งานอินเทอร์เน็ตได้ คือ การกำหนด ip ให้กับเครื่องโดยทำการแก้ไขไฟล์ interfaces

```
vi /etc/network/interfaces
```

พิมพ์คำสั่งแล้วกด Enter จะปรากฏ Editor ให้ทำการแก้ไข เพิ่มเติม



```
ont@ont-desktop: ~  
File Edit View Terminal Tabs Help  
auto lo  
iface lo inet loopback  
auto eth0  
iface eth0 inet static  
address 192.168.100.79  
netmask 255.255.255.0  
network 192.168.100.0  
gateway 192.168.100.254  
~
```

รูปที่ 19 แสดงวิธีการแก้ไขไฟล์ interfaces

3. จากนั้นทำการ restart network

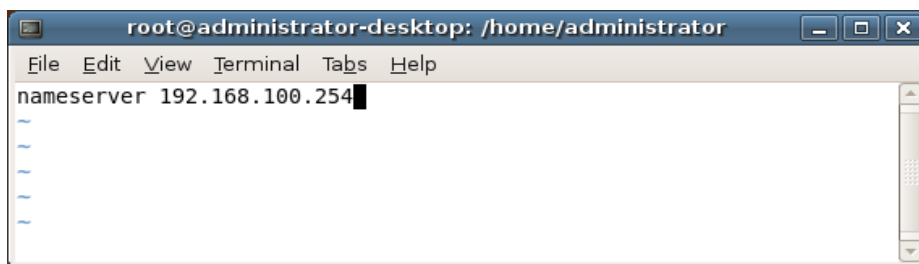
```
/etc/init.d/networking restart
```

จะปรากฏข้อความว่าไม่มี file resolv.conf

4. ทำการสร้างไฟล์ resolv.conf ขึ้นมาเพื่อกำหนดค่า nameserver โดยใช้คำสั่งดังต่อไปนี้

```
vi /etc/resolv.conf
```

ต่อจากนั้นทำการเพิ่ม nameserver



```
root@administrator-desktop: /home/administrator  
File Edit View Terminal Tabs Help  
nameserver 192.168.100.254  
~  
~  
~  
~
```

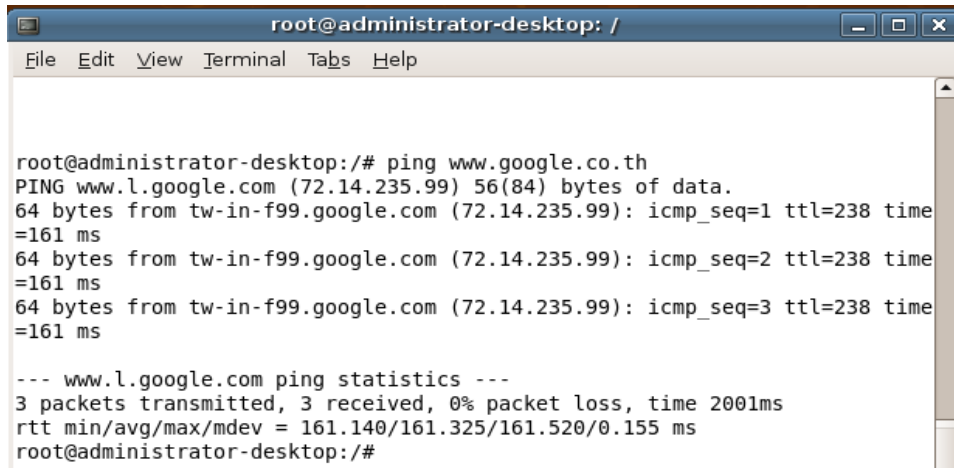
รูปที่ 20 แสดงการกำหนด NameServer

5. ทำการ restart network อีกครั้ง โดยใช้คำสั่งดังต่อไปนี้

```
/etc/init.d/networking restart
```

6. ทดสอบการใช้งานอินเทอร์เน็ตโดยใช้คำสั่ง ping ถ้าปรากฏข้อความตามภาพแสดงว่าสามารถทำการเชื่อมต่ออินเทอร์เน็ตได้สำเร็จ

```
ping www.google.co.th
```



```
root@administrator-desktop: /
File Edit View Terminal Tabs Help

root@administrator-desktop:/# ping www.google.co.th
PING www.l.google.com (72.14.235.99) 56(84) bytes of data.
64 bytes from tw-in-f99.google.com (72.14.235.99): icmp_seq=1 ttl=238 time
=161 ms
64 bytes from tw-in-f99.google.com (72.14.235.99): icmp_seq=2 ttl=238 time
=161 ms
64 bytes from tw-in-f99.google.com (72.14.235.99): icmp_seq=3 ttl=238 time
=161 ms

--- www.l.google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
rtt min/avg/max/mdev = 161.140/161.325/161.520/0.155 ms
root@administrator-desktop:/#
```

รูปที่ 21 แสดงการทดสอบการใช้งานอินเทอร์เน็ต

7. ทำการ update package ต่าง ๆ ที่จำเป็นของ Ubuntu โดยใช้คำสั่ง

```
apt-get update
```

จากนั้นระบบจะทำการ update package อัตโนมัติ

```
root@administrator-desktop: /
File Edit View Terminal Tabs Help
Get:10 http://security.ubuntu.com hardy-security/universe Sources [3308B]
Get:11 http://security.ubuntu.com hardy-security/multiverse Packages [3465B]
Get:12 http://security.ubuntu.com hardy-security/multiverse Sources [14B]
Ign http://th.archive.ubuntu.com hardy-updates/restricted Translation-en_US
Ign http://th.archive.ubuntu.com hardy-updates/universe Translation-en_US
Get:13 http://th.archive.ubuntu.com hardy Release [65.9kB]
Get:14 http://th.archive.ubuntu.com hardy-updates Release [58.5kB]
Get:15 http://th.archive.ubuntu.com hardy/main Packages [1178kB]
Get:16 http://th.archive.ubuntu.com hardy/restricted Packages [6986B]
Get:17 http://th.archive.ubuntu.com hardy/main Sources [338kB]
Get:18 http://th.archive.ubuntu.com hardy/restricted Sources [1488B]
Get:19 http://th.archive.ubuntu.com hardy/universe Packages [4297kB]
Get:20 http://th.archive.ubuntu.com hardy/universe Sources [1323kB]
Get:21 http://th.archive.ubuntu.com hardy/multiverse Packages [179kB]
Get:22 http://th.archive.ubuntu.com hardy/multiverse Sources [60.9kB]
Get:23 http://th.archive.ubuntu.com hardy-updates/main Packages [276kB]
Get:24 http://th.archive.ubuntu.com hardy-updates/restricted Packages [6626B]
Get:25 http://th.archive.ubuntu.com hardy-updates/main Sources [79.1kB]
Get:26 http://th.archive.ubuntu.com hardy-updates/restricted Sources [907B]
Get:27 http://th.archive.ubuntu.com hardy-updates/universe Packages [69.5kB]
Get:28 http://th.archive.ubuntu.com hardy-updates/universe Sources [15.0kB]
Get:29 http://th.archive.ubuntu.com hardy-updates/multiverse Packages [12.0kB]
Get:30 http://th.archive.ubuntu.com hardy-updates/multiverse Sources [1943B]
Fetched 8100kB in 1min21s (99.0kB/s)
Reading package lists... Done
root@administrator-desktop:/#
```

รูปที่ 22 แสดงการอัปเดต package

Network setup

1. ทำการ Enable packet forwarding โดยใช้คำสั่งดังต่อไปนี้

```
vi /etc/sysctl.conf
```

2. จากนั้นทำการเอาคอมเม้นท์หน้าข้อความ `net.ipv4.ip_forward=1` ออก เพื่อสั่งให้ packet forwarding ของ ipv4 ทำงาน

3. ทำการรันคำสั่งต่อไปนี้ เพื่อให้มีผลทันที เพื่อให้ forward packet ทำตัวเป็นเราเตอร์ได้

```
echo 1 | tee /proc/sys/net/ipv4/ip_forward
```

- ถ้าผลที่ได้เป็น 1 ถือว่าทำการ Enable packet forwarding สำเร็จ

4. ทำการ Restart network ด้วยคำสั่งดังต่อไปนี้

```
sysctl -p  
/etc/init.d/networking restart
```

Enable TUN/TAP device driver support

1. ทำการ Enable TUN/TAP device driver support โดยใช้คำสั่งดังต่อไปนี้ เพื่อแก้ไขไฟล์ modules

```
vi /etc/modules
```

2. จากนั้นทำการเพิ่ม tun ต่อท้ายข้อความเดิม

3. จากนั้นทำการ Enable โดยไม่ต้องทำการ Reboot ด้วยคำสั่งดังต่อไปนี้

```
modprobe tun
```


Install OPENSSSH

ประโยชน์ของ OpenSSH เพื่อจะใช้ remote เข้าไปทำงานบนเครื่อง Server แทนการนั่งหน้าเครื่อง และสามารถทำการคัดลอก และวางคำสั่งได้ง่ายขึ้นกว่าเดิม โดยเราจะต้องใช้คู่กับโปรแกรม putty เราสามารถทำได้ โดยติดตั้ง OpenSSH วิธีการติดตั้งมีดังนี้

1. ทำการ ติดตั้ง OpenSSH server โดยคำสั่งดังต่อไปนี้

```
apt-get install ssh openssh-server
```

หากมีคำถามให้ตอบ Y แล้วกด Enter

```
root@administrator-desktop: /
File Edit View Terminal Tabs Help
root@administrator-desktop:/# apt-get install openssh-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  libssl0.9.8 openssh-blacklist openssh-client
Suggested packages:
  keychain libpam-ssh molly-guard rssh
The following NEW packages will be installed:
  openssh-blacklist openssh-server
The following packages will be upgraded:
  libssl0.9.8 openssh-client
2 upgraded, 2 newly installed, 0 to remove and 213 not upgraded.
Need to get 5927KB of archives.
After this operation, 496KB of additional disk space will be used.
Do you want to continue [Y/n]? y
```

รูปที่ 23 แสดงการติดตั้ง OpenSSH

หากสามารถทำการติดตั้ง OpenSSH server สำเร็จ จะปรากฏข้อความตามภาพ

2. เมื่อทำการติดตั้ง OpenSSH server เสร็จแล้ว ก็ทำการเปิด sshd service โดยใช้คำสั่งดังต่อไปนี้

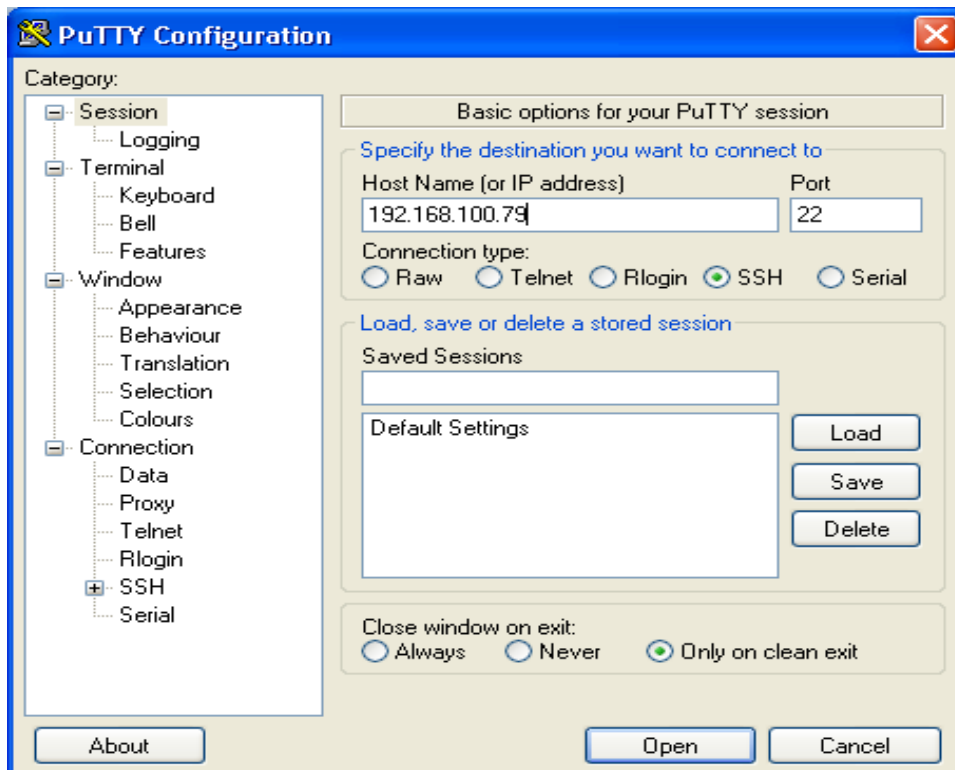
```
/etc/init.d/ssh restart
```

ถ้าสามารถเปิด service ได้ จะปรากฏข้อความตามภาพ

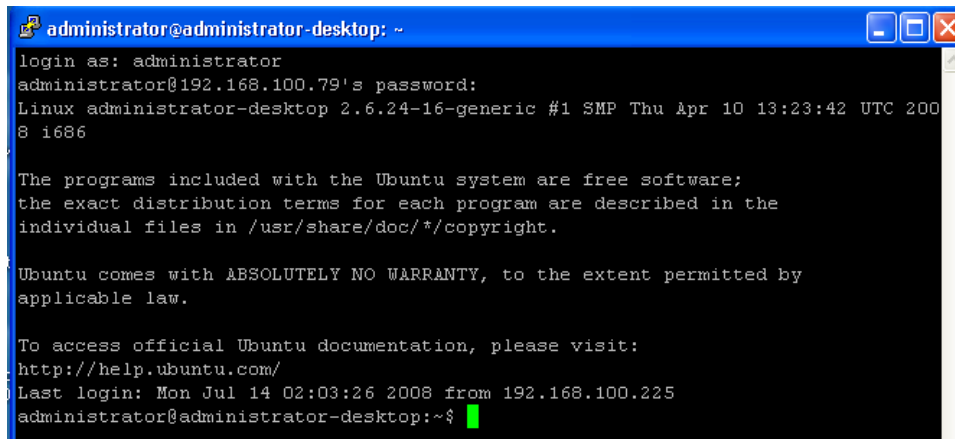
```
root@administrator-desktop: /
File Edit View Terminal Tabs Help
root@administrator-desktop:/# /etc/init.d/ssh start
* Starting OpenBSD Secure Shell server sshd
root@administrator-desktop:/# [ OK ]
```

รูปที่ 24 แสดงการ start service ssh

จากนั้นให้ใช้ติดตั้งโปรแกรม putty และเปิดทำการ remote ใช้เครื่อง server ซึ่งต่อไปนี้จะเราจะใช้โปรแกรม putty แทน เพราะง่ายต่อการคัดลอกคำสั่งต่าง ๆ



รูปที่ 25 แสดงการ remote ด้วยโปรแกรม putty
จากนั้นให้ทำการ Login ด้วย user และ password แทนการใช้งานผ่าน โปรแกรม Terminal



```
administrator@administrator-desktop: ~  
login as: administrator  
administrator@192.168.100.79's password:  
Linux administrator-desktop 2.6.24-16-generic #1 SMP Thu Apr 10 13:23:42 UTC 2008 1686  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
Last login: Mon Jul 14 02:03:26 2008 from 192.168.100.225  
administrator@administrator-desktop:~$
```

รูปที่ 26 แสดงการ Login เข้าใช้งาน

Install Chillispot

Chillispot เป็นซอฟต์แวร์ Opensource เป็นโปรแกรมที่ทำหน้าที่เป็นตัวจัดการการใช้งานระบบเครือข่าย อินเทอร์เน็ตของเครื่อง Client และ Chillispot จะทำหน้าที่เป็น dhcp server เอง ดังนั้นจะต้องทำการเช็คให้แน่ใจเสียก่อนว่าในเครื่องไม่มี dhcp server อยู่ ถ้ามีก็ให้ทำการหยุดเสียก่อน

ขั้นตอนการติดตั้ง Chillispot จาก

1. ทำการติดตั้ง chillispot โดยใช้คำสั่งดังต่อไปนี้

```
apt-get install chillispot
```

จากนั้นให้เติมรายละเอียดดังต่อไปนี้

IP address of radius server 1:

127.0.0.1

Radius shared secret:

radiussecert

Ethernet interface for DHCP to listen:

eth1

URL of UAM Server:

<https://192.168.182.1/cgi-bin/hotspotlogin.cgi>

URL of UAM homepage:

<https://192.168.182.1/welcome.html>

Shared password between chillispot and webserver:uamsecret

2. ต่อไปทำการ Enable captive portal ในไฟล์ chillispot โดยใช้คำสั่งดังต่อไปนี้

```
vi /etc/default/chillispot
```

จากนั้นทำการกำหนดค่าให้ ENABLED=1

3. ทำการคอนฟิกไฟล์ chilli.conf โดยใช้คำสั่ง

```
vi /etc/chilli.conf
```

จากนั้นทำการแก้ไขไฟล์ดังกล่าว ด้วยรายละเอียดข้างล่าง

```
net 192.168.182.0/24
dns1 192.168.100.254
dns2 192.168.100.254
radiusserver1 127.0.0.1
radiusserver2 127.0.0.1
radiussecret radiussecret
dhcpif eth1
uamserver https://192.168.182.1/cgi-bin/hotspotlogin.cgi
uamhomepage https://192.168.182.1/welcome.html
uamsecret uamsecret
uamlisten 192.168.182.1
uamallowed www.google.co.th,192.168.182.0/24
```

รูปที่ 27 แสดงการกำหนดค่าคอนฟิกไฟล์ของ chillispot

Install Firewall

ต่อจากนี้เราจะมาทำการกำหนดกฎไฟร์วอลล์ให้กับ Chillispot โดยใช้คำสั่งดังต่อไปนี้

1. ทำการกำหนดกฎไฟร์วอลล์ โดยทำการสร้างไฟล์ chilli.iptables โดยทำการคัดลอกมาจากไฟล์ firewall.iptables โดยใช้คำสั่งดังต่อไปนี้

```
cp /usr/share/doc/chillispot/firewall.iptables /etc/init.d/chilli.iptables
```

2. เมื่อทำการสร้างไฟล์ chilli.iptables เรียบร้อยแล้ว จากนั้นทำการกำหนดให้ chilli.iptables สามารถ Execute ได้ โดยใช้คำสั่งดังต่อไปนี้

```
chmod a+x /etc/init.d/chilli.iptables
```

3. จากนั้นทำการกำหนดให้ กฎของ Firewall ให้ทำการ start ทุกครั้งเมื่อมีการเปิดเครื่อง โดยใช้คำสั่งดังต่อไปนี้

```
ln -s /etc/init.d/chilli.iptables /etc/rcS.d/S41chilli.iptables
```

4. โดยค่าดีฟอลต์ไฟร์วอลล์จะทำการกำหนดค่าให้ etho=internet,eth1=LAN แต่ถ้าคุณต้องการเปลี่ยนแปลงค่าดังกล่าว คุณสามารถทำได้โดยการเปลี่ยนแปลงค่าดังกล่าวในไฟล์ chilli.iptables

5. ในขั้นตอนต่อมาให้ทำการ Enable firewall script โดยใช้คำสั่งดังต่อไปนี้

```
/etc/init.d/chilli.iptables
```

6. หากต้องการให้เครื่องลูกสามารถทดสอบการเชื่อมต่อโดยใช้โปรโตคอล icmp หรือคำสั่ง ping ให้เพิ่มกฎของ iptables ดังนี้

```
#Allow ping to myserver
SERVER_IP="192.168.182.1"
iptables -A INPUT -p icmp -icmp-type 8 -s 0/0 -d $SERVER_IP -m state --state
NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A OUTPUT -p icmp -icmp-type 0 -s $SERVER_IP -d 0/0 -m state --state
ESTABLISHED,RELATED -j ACCEPT
```

หมายเหตุ หากต้องการสร้างแพ็คเกจเองเราสามารถนำใช้ของ Coova-Chilli ได้ดังนี้
ดาวน์โหลดซอร์สโค้ดจาก Coova-Chilli

```
# wget http://ap.coova.org/chilli/coova-chilli-1.0.12.tar.gz
```

แตกไฟล์ออก

```
# tar xzvf coova-chilli-1.0.12.tar.gz
```

ติดตั้งไฟล์ที่จำเป็นต้องใช้คอมไพล์แพ็คเกจดังนี้

```
# apt-get install debhelper cmake libdaemon-dev libconfuse-dev fakeroot
# cd coova-chilli
# dpkg-buildpackage -rfakeroot
# cd ..
```

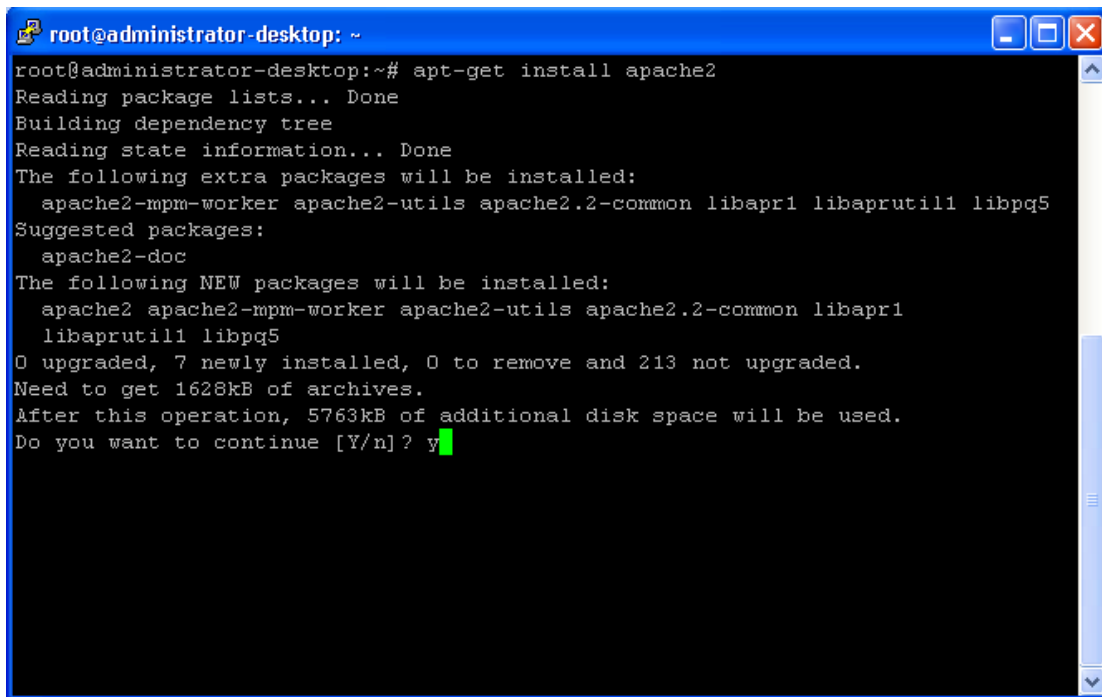
หลังจากนั้นจะได้แพ็คเกจที่พร้อมสำหรับการติดตั้ง coova-chilli_1.0.12-1_i386.deb

```
# dpkg -i coova-chilli_1.0.12-1_i386.deb
```

Install Apache

1. การติดตั้ง Apache Web Server โดยใช้คำสั่ง `apt-get install apache2` ถ้ามีคำถามให้ตอบ `y` แล้วกด Enter

```
apt-get install apache2
```



```
root@administrator-desktop: ~  
root@administrator-desktop:~# apt-get install apache2  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following extra packages will be installed:  
  apache2-mpm-worker apache2-utils apache2.2-common libapr1 libaprutil1 libpq5  
Suggested packages:  
  apache2-doc  
The following NEW packages will be installed:  
  apache2 apache2-mpm-worker apache2-utils apache2.2-common libapr1  
  libaprutil1 libpq5  
0 upgraded, 7 newly installed, 0 to remove and 213 not upgraded.  
Need to get 1628kB of archives.  
After this operation, 5763kB of additional disk space will be used.  
Do you want to continue [Y/n]? y
```

รูปที่ 28 แสดงการติดตั้ง Apache

ระบบจะแสดงความคืบหน้าของการติดตั้ง ตามภาพ


```
root@administrator-desktop: ~
Selecting previously deselected package apache2.
Unpacking apache2 (from ../apache2_2.2.8-1ubuntu0.3_all.deb) ...
Setting up libapr1 (1.2.11-1) ...

Setting up libpq5 (8.3.3-0ubuntu0.8.04) ...

Setting up libaprutil1 (1.2.12+dfsg-3) ...

Setting up apache2-utils (2.2.8-1ubuntu0.3) ...
Setting up apache2.2-common (2.2.8-1ubuntu0.3) ...
Module alias installed; run /etc/init.d/apache2 force-reload to enable.
Module autoindex installed; run /etc/init.d/apache2 force-reload to enable.
Module dir installed; run /etc/init.d/apache2 force-reload to enable.
Module env installed; run /etc/init.d/apache2 force-reload to enable.
Module mime installed; run /etc/init.d/apache2 force-reload to enable.
Module negotiation installed; run /etc/init.d/apache2 force-reload to enable.
Module setenvif installed; run /etc/init.d/apache2 force-reload to enable.
Module status installed; run /etc/init.d/apache2 force-reload to enable.
Module auth_basic installed; run /etc/init.d/apache2 force-reload to enable.
Module authz_default installed; run /etc/init.d/apache2 force-reload to enable.
Module authz_user installed; run /etc/init.d/apache2 force-reload to enable.
Module authz_groupfile installed; run /etc/init.d/apache2 force-reload to enable.
Module authn_file installed; run /etc/init.d/apache2 force-reload to enable.
Module authz_host installed; run /etc/init.d/apache2 force-reload to enable.

Setting up apache2-mpm-worker (2.2.8-1ubuntu0.3) ...
 * Starting web server apache2
apache2: Could not reliably determine the server's fully qualified domain name, using 127.0
.1.1 for ServerName
[ OK ]

Setting up apache2 (2.2.8-1ubuntu0.3) ...
Processing triggers for libc6 ...
ldconfig deferred processing now taking place
root@administrator-desktop:~#
```

รูปที่ 29 แสดงความคืบหน้าการติดตั้ง Apache

2. หลังจากติดตั้งเสร็จแล้ว ต้องทำการ config เล็กน้อย ไฟล์ configuration files ทั้งหมดอยู่ที่ /etc/apache2/apache2.conf สิ่งที่ต้องแก้ไขมีดังนี้

ไฟล์ apache2.conf ให้แก้ไขส่วนที่เป็น

- ServerName (โดยในที่นี้กำหนด ServerName 192.168.182.1)
- MaxKeepAliveRequests

ไฟล์ `sites-available/default` เลือกแก้ไขที่จำเป็น เช่น

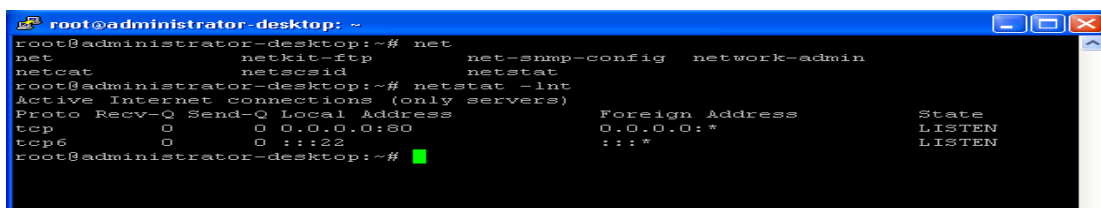
- ServerAdmin (ใส่ email address ของ webmaster)
- Document Root (ปกติจะเป็น `/var/www` แต่ถ้าต้องการเปลี่ยนเป็นที่อื่น ก็แก้ไขได้)

3. หลังจากทำการติดตั้งเสร็จแล้ว ให้ทำการ start apache โดยใช้คำสั่ง

```
/etc/init.d/apache2 start
```

4. ตรวจสอบว่า Apache ทำงานหรือไม่ โดยใช้คำสั่ง `netstat -lnt` ซึ่งถ้า apache สามารถทำงานได้ จะแสดงพอร์ต 80 สถานะเป็น LISTEN

```
netstat -lnt
```



```
root@administrator-desktop: ~  
root@administrator-desktop:~# net  
net          netkit-ftp      net-smmp-config  network-admin  
netcat       netcsid        netstat  
root@administrator-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  
tcp6       0      0 :::22                  :::*                     LISTEN  
root@administrator-desktop:~#
```

รูปที่ 30 แสดงการตรวจสอบ Apache

Install MySQL Database Server

1. ทำการติดตั้ง MySQL Database ด้วยคำสั่งดังต่อไปนี้ ถ้ามีคำถามให้ตอบ y แล้วกด Enter

```
apt-get install mysql-server
```

```
root@administrator-desktop: /
root@administrator-desktop:/# apt-get install mysql-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  mysql-server-5.0
Suggested packages:
  mysql-doc-5.0 tinyca
Recommended packages:
  libhtml-template-perl mailx
The following NEW packages will be installed:
  mysql-server mysql-server-5.0
0 upgraded, 2 newly installed, 0 to remove and 213 not upgraded.
Need to get 0B/27.5MB of archives.
After this operation, 86.2MB of additional disk space will be used.
Do you want to continue [Y/n]? y
```

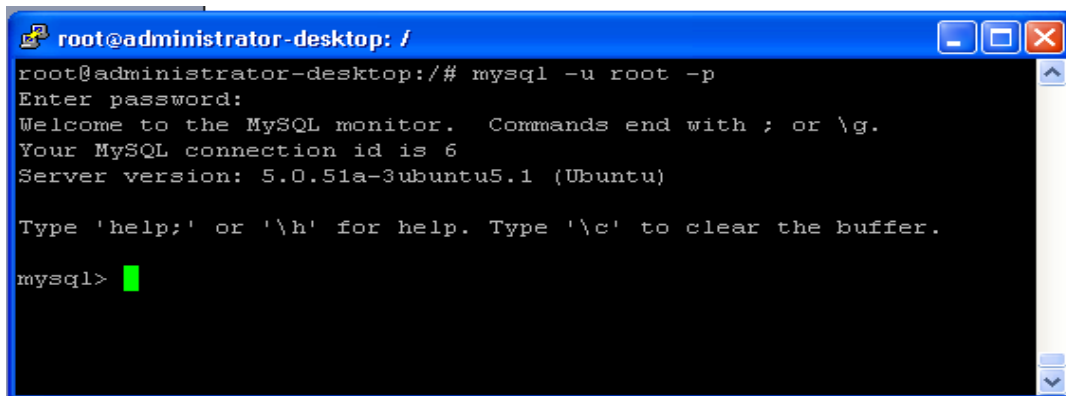
รูปที่ 31 แสดงการติดตั้ง MySQL Database Server

2. เมื่อทำการติดตั้งเสร็จ ระบบจะให้เรากำหนด password ของ root ทำการกำหนด password ให้กับ root หลังจากนั้นกด OK ทำการยืนยันรหัสอีกครั้ง จากนั้นกด OK ระบบจะทำการติดตั้งต่อ วิธีการเปลี่ยนค่ารหัสผ่านของ mysql ทำได้โดยพิมพ์ `mysqladmin password NEW-PASSWORD`

3. ทดสอบว่า MySQL สามารถใช้งานได้หรือไม่ โดยใช้คำสั่งดังต่อไปนี้

```
mysql -u root -p
```

จากนั้นกด Enter แล้วใส่รหัสผ่านของ root ถ้าปรากฏข้อความตามภาพถือว่าเป็นอันสำเร็จ



```
root@administrator-desktop: /
root@administrator-desktop:/# mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 6
Server version: 5.0.51a-3ubuntu5.1 (Ubuntu)

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

mysql>
```

รูปที่ 32 แสดงการทดสอบการเข้าใช้งาน mysql

Install PHP

1. การติดตั้ง PHP โดยใช้คำสั่งดังต่อไปนี้

```
apt-get install php5
```

ถ้ามีคำถามให้ตอบ y แล้วกด Enter

```
root@administrator-desktop: ~
root@administrator-desktop:~# sudo apt-get install php5
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  apache2-mpm-prefork libapache2-mod-php5 php5-common
Suggested packages:
  php-pear
The following packages will be REMOVED:
  apache2-mpm-worker
The following NEW packages will be installed:
  apache2-mpm-prefork libapache2-mod-php5 php5 php5-common
0 upgraded, 4 newly installed, 1 to remove and 213 not upgraded.
Need to get 3087kB of archives.
After this operation, 6443kB of additional disk space will be used.
Do you want to continue [Y/n]? y
```

รูปที่ 33 แสดงการติดตั้ง PHP

2. เมื่อทำการติดตั้ง PHP สำเร็จให้ทำการ restart apache ด้วยคำสั่ง

```
/etc/init.d/apache2 restart
```

3. เมื่อทำการ restart apache แล้วให้ทำการทดสอบว่า php ทำงานหรือไม่ ให้ทำการสร้างไฟล์ php ขึ้นมาทดสอบการทำงานโดยใช้ชื่อไฟล์ว่า test.php โดยใช้คำสั่งดังนี้ และพิมพ์ข้อความต่อไปนี้ <?php phpinfo(); ?>

```
vi /var/www/test.php
```

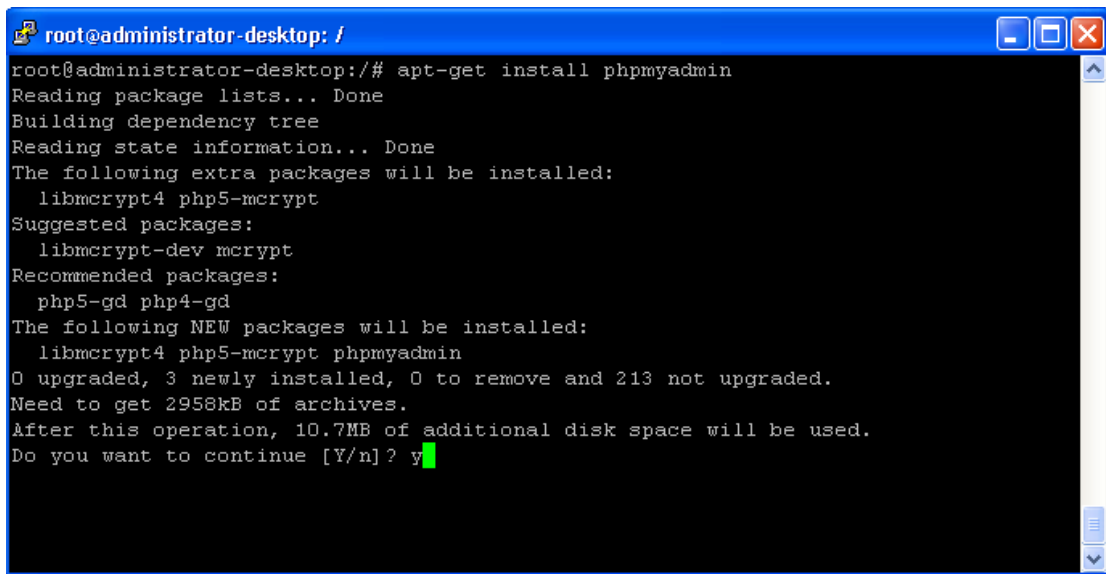

Install PhpMyAdmin

PhpMyAdmin เป็นส่วนต่อประสานที่สร้างโดยภาษาพีเอชพี ซึ่งใช้จัดการฐานข้อมูล MySQL ผ่านเว็บเบราว์เซอร์ โดยสามารถที่จะทำการสร้างฐานข้อมูลใหม่ หรือทำการสร้าง TABLE ใหม่ๆ และยังมี function ที่ใช้สำหรับการทดสอบการ query ข้อมูลด้วยภาษา SQL พร้อมกันนั้น ยังสามารถทำการ insert delete update หรือแม้กระทั่งใช้คำสั่งต่างๆ เหมือนกับกับการใช้ภาษา SQL ในการจัดการตารางข้อมูล เริ่มติดตั้งตามขั้นตอนดังต่อไปนี้ได้เลย

1. ทำการติดตั้ง PhpMyAdmin โดยใช้คำสั่ง ดังต่อไปนี้

```
apt-get install phpmyadmin
```

ถ้ามีคำถามตอบ Y แล้วกด Enter



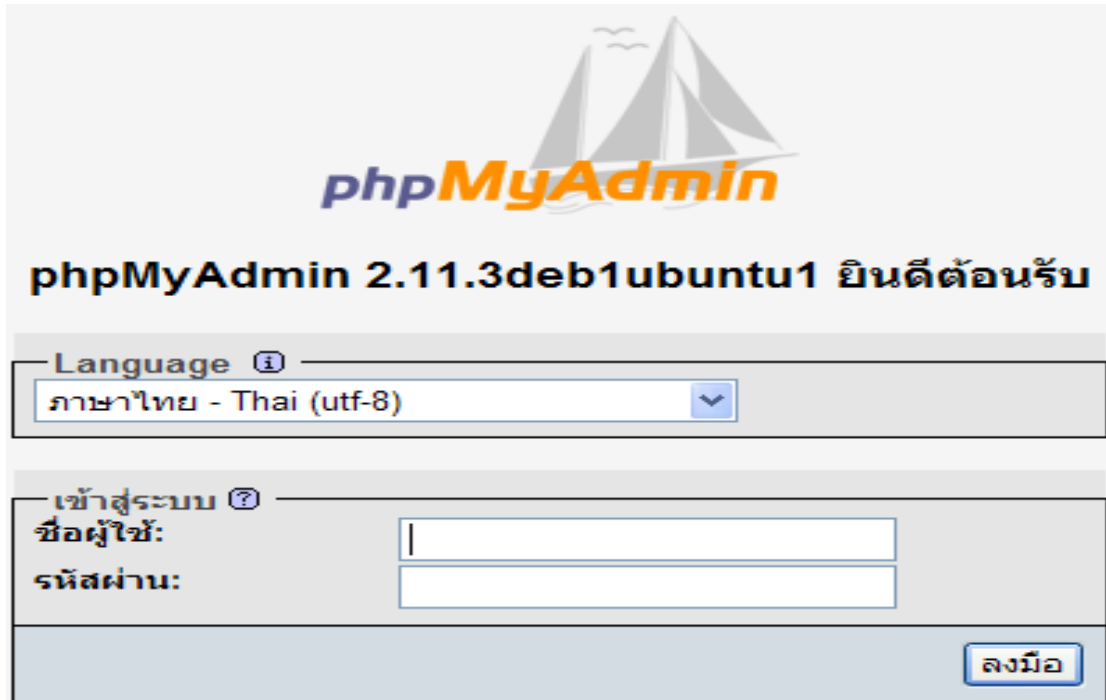
```
root@administrator-desktop: /
root@administrator-desktop:/# apt-get install phpmyadmin
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  libmcrypt4 php5-mcrypt
Suggested packages:
  libmcrypt-dev mcrypt
Recommended packages:
  php5-gd php4-gd
The following NEW packages will be installed:
  libmcrypt4 php5-mcrypt phpmyadmin
0 upgraded, 3 newly installed, 0 to remove and 213 not upgraded.
Need to get 2958kB of archives.
After this operation, 10.7MB of additional disk space will be used.
Do you want to continue [Y/n]? y
```

รูปที่ 35 แสดงการติดตั้ง PhpMyAdmin

2. ทำการกำหนดค่า PhpMyAdmin ให้ติดต่อกับ web server apache2 จากนั้นกด OK ระบบจะทำการติดตั้งต่อ

3. ทดสอบการทำงานของ PhpMyAdmin โดยการใช้ browser เปิด

<http://192.168.100.79/phpmyadmin> ถ้าปรากฏข้อความตามภาพถือว่าการติดตั้งสำเร็จ



phpMyAdmin

phpMyAdmin 2.11.3deb1ubuntu1 ยินดีต้อนรับ

Language ⓘ

ภาษาไทย - Thai (utf-8)

เข้าสู่ระบบ ⓘ

ชื่อผู้ใช้:

รหัสผ่าน:

ลงมือ

รูปที่ 36 แสดงการทดสอบการใช้งาน PhpMyAdmin

Install Radius Server

RADIUS (Remote Authentication Dial in User Services) เป็นอีกบริการหนึ่งที่ทำให้เครื่อง Server สามารถที่จะตรวจสอบสิทธิ์การใช้งาน Internet คล้ายๆ กับศูนย์ให้บริการ Internet ต่างๆ ที่จะมี Radius Server ไว้เพื่อตรวจสอบสิทธิ์การใช้งาน ซึ่งเราสามารถที่จะสร้าง User Account ขึ้นมาเองได้ และสามารถที่จะจำกัดจำนวนชั่วโมงการใช้งานของ Users ขั้นตอนการติดตั้ง Radius Server และ Database มีดังต่อไปนี้

1. ทำการ Install radius server ด้วยคำสั่งต่อไปนี้ ถ้ามีคำถามให้ตอบ Y

```
apt-get install freeradius freeradius-mysql
```

2. ทำการ start freeradius โดยใช้คำสั่งดังต่อไปนี้

```
/etc/init.d/freeradius start
```

```
root@administrator-desktop: /var/log/apache2
root@administrator-desktop:/var/log/apache2# /etc/init.d/freeradius start
* Starting FreeRADIUS daemon freeradius
Tue Jul 8 00:30:51 2008 : Info: Starting - reading configuration files ...
[ OK ]
root@administrator-desktop:/var/log/apache2#
```

รูปที่ 37 แสดงการ start freeradius

3. ทำการสร้าง Database ชื่อว่า radius เพื่อใช้ในการเก็บบัญชีรายผู้ใช้งาน ด้วยคำสั่งต่อไปนี้ หรือจะใช้ phpmyadmin เป็นเครื่องมือในการช่วยสร้างก็ได้

```
mysql -u root -p (เพื่อใช้งาน mysql) จากนั้นใส่รหัสที่เรากำหนดไว้ในขั้นตอนการลง mysql ต่อจากนั้นทำการสร้าง Database ด้วยคำสั่งดังต่อไปนี้
CREATE DATABASE radius;
```

```
root@administrator-desktop:/# mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 13
Server version: 5.0.51a-3ubuntu5.1 (Ubuntu)

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

mysql> CREATE DATABASE radius;
Query OK, 1 row affected (0.06 sec)

mysql>
```

รูปที่ 38 แสดงการสร้าง Database radius

เมื่อทำการสร้างฐานข้อมูลเรียบร้อยแล้วให้ใช้คำสั่ง quit เพื่อออกจากการใช้งาน mysql

4. จากนั้นทำการสร้างตารางให้กับฐานข้อมูล Radius โดยใช้เทมเพลตของโปรแกรม FreeRadius

```
zcat /usr/share/doc/freeradius/examples/mysql.sql.gz | mysql -u root -p radius
```

5. ทำการสร้าง user ที่มีสิทธิ์ใน Database radius โดยใช้คำสั่งต่อไปนี้ ในที่นี้กำหนด user เท่ากับ radius และ password เท่ากับ mysqlsecret

```
mysql -u root -p (เพื่อใช้งาน mysql) จากนั้นใส่รหัสที่เรากำหนดไว้ในขั้นตอนการ  
ลง mysql จากนั้นพิมพ์คำสั่งดังต่อไปนี้  
mysql> GRANT ALL PRIVILEGES ON radius.* TO 'radius'@'localhost'  
IDENTIFIED BY 'mysqlsecret'; (กด Enter)  
mysql> FLUSH PRIVILEGES;  
mysql> quit;
```

6. กำหนดค่าไฟล์คอนฟิกของ FreeRadius ให้เชื่อมต่อกับฐานข้อมูล โดยใช้คำสั่งดังต่อไปนี้

```
vi /etc/freeradius/sql.conf
```

แล้วทำการกำหนด ชื่อ login และ password ตามภาพ

```
root@administrator-desktop: /
#
# Configuration for the SQL module, when using MySQL.
#
# The database schema is available at:
#
#     doc/examples/mysql.sql
#
# If you are using PostgreSQL, please use 'postgresql.conf', instead.
# If you are using Oracle, please use 'oracle.conf', instead.
# If you are using MS-SQL, please use 'mssql.conf', instead.
#
# $Id: sql.conf,v 1.41.2.2.2.6 2007/07/17 08:35:34 pnixon Exp $
#
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 = "mysqlsecret"

    # Database table configuration
}
: wC
```

รูปที่ 39 แสดงการกำหนด username และ password ในการเข้าใช้ฐานข้อมูล

7. ทำการกำหนด password ให้กับเครื่อง Client ที่จะเข้าใช้งาน FreeRadius โดยใช้คำสั่งดังต่อไปนี้

```
vi /etc/freeradius/clients.conf
```

จากนั้นทำการกำหนดให้ Client 127.0.0.1 มีค่า secret=radiussecret

```
client 127.0.0.1 {
    secret = radiussecret
}
```

8. ทำการ Test default file setup โดยทำการแก้ไขไฟล์ users โดยใช้คำสั่ง

```
vi /etc/freeradius/users
```

จากนั้นค้นหา “John Doe” เมื่อพบแล้วให้เอาคอมเมนต์หน้าชื่อออกจากรายชื่อแก้ไขข้อความให้เหมือนภาพด้านล่าง เมื่อทำการแก้ไขเสร็จให้ทำการ stop service

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

รูปที่ 40 แสดงการกำหนดค่าให้กับ user “John Doe”

หมายเหตุ กรณีติดตั้งซอฟต์แวร์ freeradius > 2.0.4 ให้เปลี่ยนค่าของไฟล์ users ขึ้นการทดสอบและดีบั๊กให้ใช้ดังนี้ freeradius -XXX

```
DEFAULT      Service-Type == Framed-User  
              Service-Type = Framed-User,  
              Fall-Through = Yes  
"john woo"    Cleartext-Password := "testing"  
              Service-Type = Framed-User,
```

9. จากนั้นเปิดทำการ stop freeradius

```
/etc/init.d/freeradius stop (Enter) และตามด้วยคำสั่งเพื่อทำการดีบั๊ก  
freeradius -XXX -A
```

10. จากนั้นให้เปิด โปรแกรม putty เพิ่มขึ้นอีก 1 ตัว เพื่อที่ทำหน้าที่เสมือนเป็นเครื่อง Client โดยเปิดโปรแกรม putty ในข้อ 9 ทั่วไป เสมือนเป็นเครื่อง Server จากนั้นใช้ putty ที่เปิดขึ้นมาใหม่ทำการ Test โดยใช้คำสั่งดังต่อไปนี้

```
radtest "John Doe" hello 127.0.0.1 0 radiussecert
```

ถ้าทุกอย่างเรียบร้อย ในเครื่อง Client จะปรากฏข้อความตามภาพ

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
Last login: Tue Jul  8 02:13:25 2008 from 192.168.100.225
administrator@administrator-desktop:~$ sudo -s
[sudo] password for administrator:
root@administrator-desktop:~# radtest "John Doe" hello 127.0.0.1 0 radiussecret
Sending Access-Request of id 46 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=46, length=37
  Reply-Message = "Hello, John Doe"
root@administrator-desktop:~#
```

รูปที่ 41 แสดงการตรวจสอบการทำงานของ FreeRadius

Change authorization to sql

เป็นการเปลี่ยนกระบวนการตรวจสอบคุณสมบัติของผู้ใช้งาน(Authorization) ของ Client radius จากเดิมเป็นไฟล์ให้เปลี่ยนไปเป็น SQLServer แทน โดยมีขั้นตอนดังต่อไปนี้คือ

1. ทำการเปลี่ยน authorization จาก file ไปเป็น sql โดยใช้คำสั่งดังต่อไปนี้

```
vi /etc/freeradius/radiusd.conf
```

จากนั้นให้หาล็อก authorize{ ..} ซึ่งเมื่อ radius server ได้รับการติดต่อจากผู้ใช้ (radius client) วิธีการตรวจสอบคุณสมบัติของผู้ใช้จะอยู่ในส่วนของ authorize{...} และทำการเอาคอมเม้นท์หน้า sql ออก และทำการคอมเม้นท์หน้า files แทน ซึ่งเป็นการกำหนดวิธีตรวจสอบคุณสมบัติของผู้ใช้จากเดิมเป็น files เปลี่ยนไปเป็น sql ตามภาพ

```
root@administrator-desktop: ~
# suffix
# ntdomain
#
# This module takes care of EAP-MD5, EAP-TLS, and EAP-LEAP
# authentication.
#
# It also sets the EAP-Type attribute in the request
# attribute list to the EAP type from the packet.
eap
#
# Read the 'users' file
# 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
```

รูปที่ 42 การเปลี่ยน authorization จาก file ไปเป็น sql

SQL Logging

SQL logging ทำหน้าที่ในการเก็บค่าการใช้งานต่าง ๆ ของ Client radius ดังนั้นต้องทำการคอนฟิกค่าต่าง ๆ ให้ทำงานสอดคล้องกับ FreeRadius Server โดยมีขั้นตอนดังต่อไปนี้

1. เป็นการกำหนดการเก็บค่าการใช้งานของผู้ใช้งานในระบบ โดยใช้คำสั่งดังต่อไปนี้ เพื่อทำการแก้ไขไฟล์ sql.conf

```
vi /etc/freeradius/sql.conf
```

จากนั้นตรวจสอบว่า readclient=yes หรือยัง ถ้ายังให้ทำกำหนดให้ readclient=yes เพื่อที่จะทำให้ radius client อ่านค่าจาก database

2. ต่อจากนั้นทำการคอนฟิกไฟล์ radiusd.conf โดยใช้คำสั่งดังต่อไปนี้

```
vi /etc/freeradius/radiusd.conf
```

ต่อจากนั้น ยกเลิกการ Comment #sql ออก เพื่อเรียกใช้ข้อมูลจาก database ในการตรวจสอบ UserName

password ในการทำ accounting

```
accounting {
```

```
...
```

```
sql
```

```
...
```

```
}
```

ต่อจากนั้นยกเลิกการ Comment #sql ออก เพื่อเรียกใช้ข้อมูลจาก database ในการตรวจสอบ UserName
password ในการทำ session

```
session {
```

```
...
```

```
sql
```

```
...
```

```
}
```

หมายเหตุ ถ้าเป็น freeradius-2.0.4 ของ Debian lenny ให้แก้ไฟล์ /etc/freeradius/radiusd.conf และไฟล์
/etc/freeradius/site-avaliabile/default

```
modules {
```

```
....
```

```
$INCLUDE sql.conf
```

```
....
```

```
}
```

```
authorize {
```

```
...
```

```
# files
```

```
sql
```

```
...
```

```
}  
accounting {  
    ...  
    sql  
    ...  
}  
session {  
    ...  
    sql  
}
```

3. ทำการเพิ่ม user เพื่อทดสอบการทำงาน โดยพิมพ์คำสั่งดังต่อไปนี้ ให้อยู่ในบรรทัดเดียวกัน เพื่อทำการเพิ่ม user mysqltest และมีรหัสผ่านเป็น testsecret ในตาราง radcheck

```
echo "INSERT INTO radcheck (UserName,Attribute,op,Value) VALUES  
( 'mysqltest', 'User-Password', '=', 'testsecret');" | mysql -u radius -p radius
```

4. ทำการ start radius โดยใช้คำสั่งดังต่อไปนี้

```
/etc/init.d/freeradius start
```

จากนั้นทำการทดสอบ โดยพิมพ์คำสั่งดังต่อไปนี้

```
radtest mysqltest testsecret 127.0.0.1 0 radiussecret
```

ถ้าทุกอย่างเรียบร้อยจะแสดงข้อความการ Access สำเร็จ


```
root@administrator-desktop: ~
Tue Jul 8 16:01:47 2008 : Info: Starting - reading configuration files ...
root@administrator-desktop:~# radtest mysqltest testsecret 127.0.0.1 0 radiussecret
Sending Access-Request of id 174 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=174, length=20
root@administrator-desktop:~#
```

รูปที่ 43 แสดงการทดสอบใช้งาน User จากฐานข้อมูล

Create login page

การสร้างหน้าจอสําหรับใช้ในการ login เข้าใช้งานในระบบเครือข่ายอินเทอร์เน็ต

1. ทำการสร้างไดเรกทอรี /var/www/cgi-bin

```
mkdir -p /var/www/cgi-bin
```

2. ทำการสร้างไฟล์ hotspotlogin.cgi ไปวางในไดเรกทอรีที่ได้ทำการสร้างไว้ในข้อที่ 1.

```
zcat -c /usr/share/doc/chillispot/hotspotlogin.cgi.gz | tee /var/www/cgi-bin/hotspotlogin.cgi
```

3. ต่อจากนั้นทำการ chmod ให้ไฟล์ hotspotlogin.cgi สามารถ execute ได้

```
chmod a+x /var/www/hotspot/cgi-bin/hotspotlogin.cgi
```

4. ต่อไปทำการแก้ไขไฟล์ hotspotlogin.cgi

```
vi /var/www/cgi-bin/hotspotlogin.cgi
```

จากนั้นทำการเอาคอมเมนต์หน้า \$uamsecret และ \$userpassword ออก และทำการแก้ไข password ของ \$uamsecret ให้มีค่าเท่ากับ uamsecret

```
$uamsecret="uamsecret";
$userpassword=1:
```

เมื่อแก้ไขเสร็จแล้วให้ทำการ start chillispot ด้วยคำสั่ง

```
/etc/init.d/chillispot start
```

5. ต่อจากนั้นทำการสร้างไฟล์ welcome.html

```
vi /var/www/welcome.html
```

ทำการเพิ่มข้อมูลเหล่านี้ลงไปไฟล์ welcome.html

```
<html>
<head><title> Welcome to Our Hotspot, Wireless Network </title>
</head>
<body>
<center>
<H1><font color="red">TESTING ONLY</font></H1>

<H3><font color="blue">Welcome to Our Hotspot, Wireless Network.</font></H3>
<p>You are connected to an authentication and restricted network access point.
<H3><a href="http://192.168.182.1:3990/prelogin">Click here to login</a></H3>
<p>
<p>Enjoy.
</center>
</body>
</html>
```

รูปที่ 44 แสดงตัวอย่างไฟล์ welcome.html

ถ้าต้องการรูป chillispot.png ให้ทำการดาวน์โหลดโดยใช้คำสั่ง

```
wget
http://mamboeasy.psu.ac.th/~wiboon.w/images/stories/chillispot/chillispot.png

cp chillispot.png /var/www
```

Setup SSL

ก่อนทำการติดตั้ง SSL ต้องแน่ใจว่าได้ทำการติดตั้ง LAMP เป็นที่เรียบร้อยแล้ว ถ้าไม่แน่ใจก็ให้ใช้คำสั่งในการตรวจสอบ นั่นก็คือคำสั่ง `tasksel` แล้วตรวจสอบว่าคุณยังไม่ได้ติดตั้งโปรแกรมตัวใด ก็ให้ทำการติดตั้งให้เรียบร้อย การติดตั้ง SSL มีขั้นตอนดังต่อไปนี้

1. ทำการติดตั้ง SSL โดยใช้คำสั่งดังต่อไปนี้ ถ้ามีคำถามตอบ Y แล้วกด Enter

```
apt-get install ssl-cert
```

ถ้ามีคำถามให้ตอบ y แล้วกด Enter

```
root@administrator-desktop: /
root@administrator-desktop:/# apt-get install ssl-cert
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  openssl openssl-blacklist
Suggested packages:
  openssl-doc
The following NEW packages will be installed:
  openssl-blacklist
The following packages will be upgraded:
  openssl ssl-cert
2 upgraded, 1 newly installed, 0 to remove and 211 not upgraded.
Need to get 6731kB of archives.
After this operation, 12.5MB of additional disk space will be used.
Do you want to continue [Y/n]? y
```

รูปที่ 45 แสดงการติดตั้ง SSL

2. เมื่อทำการติดตั้งเสร็จ ในขั้นตอนต่อไปให้สร้างไดเรกทอรี `ssl` ขึ้นมาเพื่อเก็บ Certificate ที่ถูกสร้างขึ้น โดยใช้คำสั่งดังต่อไปนี้

```
mkdir /etc/apache2/ssl
จากนั้นใช้คำสั่ง ls เพื่อดูว่ามี ไดเรกทอรี ssl หรือยัง
```

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

รูปที่ 46 แสดงการสร้างไดเรกทอรี ssl

3. ทำการสร้าง self-signed certificates ด้วยคำสั่งดังต่อไปนี้

```
make-ssl-cert /usr/share/ssl-cert/ssleay.cnf /etc/apache2/ssl/apache.pem
```

คุณจะถูกถามด้วยคำถามดังต่อไปนี้

Country Name

ป้อน TH

State or Province Name

สามารถที่จะเว้นว่างได้

Locality Name

สามารถที่จะเว้นว่างได้

Organization Name

ชื่อบริษัท

Host

ป้อน ip address หรือ domain address ของคุณก็ได้

Email

ป้อน Email

4. ทำการ install module ssl ด้วยคำสั่งดังต่อไปนี้

```
a2enmod ssl
```

แล้วทำการ reload apache ด้วยคำสั่งดังต่อไปนี้

```
/etc/init.d/apache2 force-reload
```

5. ต่อไปทำการสร้าง Virtual Host ชื่อ hotspot ขึ้นมาด้วยคำสั่งดังต่อไปนี้

```
vi /etc/apache2/sites-available/hotspot
```

จากนั้นให้ทำการพิมพ์ข้อความต่อไปนี้ลงไป

```
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>
```

รูปที่ 47 แสดงตัวอย่างคอนฟิกไฟล์ของ hotspot

6. ต่อจากนั้นทำการ Enable SSL virtualhost ด้วยคำสั่งดังต่อไปนี้

```
a2ensite hotspot
```

ต่อจากนั้นทำการ reload apache ด้วยคำสั่งดังต่อไปนี้

```
/etc/init.d/apache2 reload
```

7. การ Listen Port โดยค่า default ของ https จะทำงานที่พอร์ต 443 แก้ไขคอนฟิกได้ที่ไฟล์ ports.conf ด้วยคำสั่งดังต่อไปนี้

```
vi /etc/apache2/ports.conf
```

ทำการแก้ไข ให้เหมือนภาพด้านล่าง

```
root@administrator-desktop: /etc/apache2/sites-available
Listen 192.168.182.1:80
Listen 192.168.182.1:443
#<IfModule mod_ssl.c>
# Listen 443
#</IfModule>
~
~
~
```

รูปที่ 48 แสดงการ Listen ports 443

8. เปลี่ยนแปลงค่าให้มีการ Listen พอร์ตที่เป็น default http port(80) ด้วยคำสั่งดังต่อไปนี้

```
vi /etc/apache2/sites-available/default
```

โดยส่วนบนของไฟล์จะเป็นดังนี้ :

```
NameVirtualHost *
```

```
<VirtualHost *>
```

```
...
```

```
...
```

```
</VirtualHost>
```

ทำการเปลี่ยนแปลงค่าให้มีการ Listen พอร์ตที่เป็น default http port(80) โดยการเพิ่ม :80 ต่อท้าย *

```
NameVirtualHost *:80
```

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

```
...
```

```
...
```

```
</VirtualHost>
```

9. ทำการกำหนด Server Root โดยการคอนฟิกที่ไฟล์ apache2.conf

```
vi /etc/apache2/apache2.conf
```

ทำการกำหนดค่าให้กับ ServerName (ในกรณีที่ยังไม่ได้ทำการกำหนด)

```
ServerName 192.168.182.1
```

10. ทำการแก้ไข host file ด้วยคำสั่งดังต่อไปนี้

```
vi /etc/hosts
```

แก้ไขชื่อ host ได้ตามความต้องการ

```
root@administrator-desktop: /etc/apache2/sites-available
127.0.0.1          localhost
192.168.182.1     administrator-desktop
```

รูปที่ 49 แสดงการแก้ไขชื่อ host

11. ทำการ restart apache ด้วยคำสั่ง

```
/etc/init.d/apache2 restart
```

12. ทดสอบโดยใช้ browser เปิด <https://192.168.182.1> ถ้าสามารถดู Certificate ที่เราได้สร้างไว้ได้ ถือว่าเป็นอันสำเร็จ ตามรูปข้างล่างนี้

General Details

Could not verify this certificate for unknown reasons.

Issued To

Common Name (CN)	192.168.182.1
Organization (O)	NANA IT CO.LTD.
Organizational Unit (OU)	NANA
Serial Number	00:E7:2C:5A:15:06:6B:0F:FB

Issued By

Common Name (CN)	192.168.182.1
Organization (O)	NANA IT CO.LTD.
Organizational Unit (OU)	NANA

Validity

Issued On	07/21/2008
Expires On	08/20/2008

Fingerprints

SHA1 Fingerprint	97:0D:C1:BC:F0:5B:2F:EA:5C:7C:67:50:52:CD:A6:38:84:E4:D1:08
MD5 Fingerprint	56:64:E6:A4:72:1A:BF:64:36:80:4F:A8:CC:8B:ED:0E

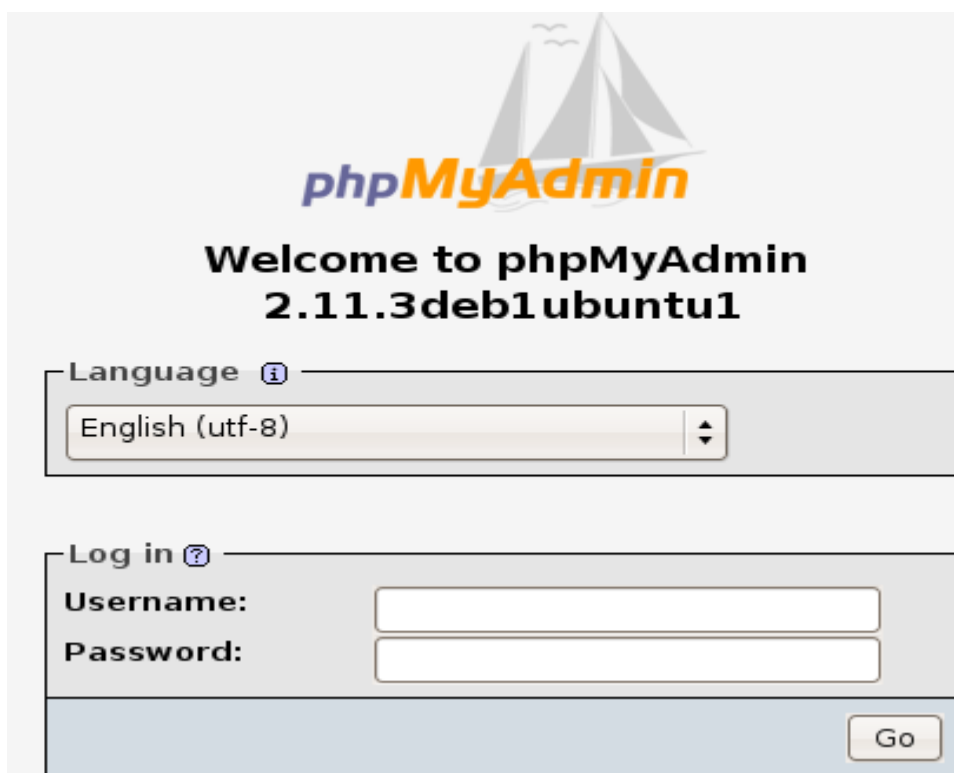
Close

รูปที่ 50 แสดง Certificate

Add User

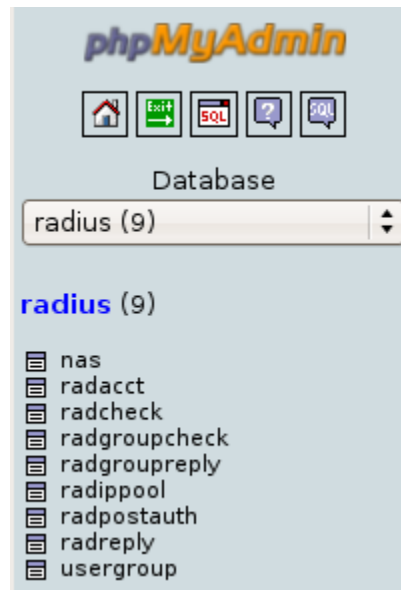
วิธีการเพิ่มรายชื่อผู้ใช้งานในระบบ นั้น สามารถทำได้หลายวิธี แต่ในที่นี้จะเสนอวิธีใช้ phpmyadmin และการ import text file ในการสร้างรายชื่อผู้ใช้งาน

1. ใช้ Browser เรียกใช้งาน PhpMyAdmin จากนั้นทำการ login เข้าใช้งานจากนั้นเลือกใช้งาน ฐานข้อมูล Radius



รูปที่ 51 แสดงการเรียกใช้งาน PhpMyAdmin

2. เมื่อทำการเลือกฐานข้อมูลเป็นที่เรียบร้อยแล้วจะปรากฏรายชื่อตารางต่าง ๆ ที่อยู่ในฐานข้อมูล Radius



รูปที่ 52 แสดงรายชื่อตารางในฐานข้อมูล radius

ซึ่งในที่นี่ตารางที่เราจะใช้มีอยู่ 2 ตารางคือ ตาราง radcheck ซึ่งตารางนี้มีไว้เพื่อกำหนดเงื่อนไขตรวจสอบการเข้าใช้งานระบบเครือข่ายอินเทอร์เน็ตของผู้ใช้งานในแต่ละราย ตารางนี้จะถูกเรียกใช้งานก็ต่อเมื่อผู้ใช้งานทำการ Login เข้าใช้งานระบบเครือข่ายอินเทอร์เน็ต ส่วนตารางที่ 2 คือ ตาราง radreply ตารางนี้มีไว้เพื่อกำหนดเงื่อนไขของผู้ใช้งานในแต่ละรายในการที่ผู้ใช้งานจะถูกตัดออกจากการใช้งานระบบเครือข่ายอินเทอร์เน็ต

โครงสร้างของตาราง radcheck

ฟิลด์	ชนิด	การเรียงลำดับ	แอดทริบิวต์	ว่างเปล่า (null)	ค่าปริยาย	เพิ่มเติม
<u>id</u>	int(11)		UNSIGNED	ไม่		auto_increment
UserName	varchar(64)	latin1_swedish_ci		ไม่		
Attribute	varchar(32)	latin1_swedish_ci		ไม่		
op	char(2)	latin1_swedish_ci		ไม่	==	
Value	varchar(253)	latin1_swedish_ci		ไม่		

รูปที่ 53 แสดงโครงสร้างตาราง radcheck

โครงสร้างของตาราง radreply

ฟิลด์	ชนิด	การเรียงลำดับ	แอดทริบิวต์	ว่างเปล่า (null)	ค่าปริยาย	เพิ่มเติม
id	int(11)		UNSIGNED	ไม่		auto_increment
UserName	varchar(64)	latin1_swedish_ci		ไม่		
Attribute	varchar(32)	latin1_swedish_ci		ไม่		
op	char(2)	latin1_swedish_ci		ไม่	=	
Value	varchar(253)	latin1_swedish_ci		ไม่		

รูปที่ 54 แสดงโครงสร้างตาราง radreply

เมื่อสังเกตจะพบว่า 2 ตารางนี้มีโครงสร้างตารางเหมือนกัน แต่ที่จะแตกต่างกันนั้นอยู่ที่ค่าที่จะใส่ลงไป

3. เพิ่มรายชื่อผู้ใช้งาน โดยเริ่มจากตาราง radcheck ก่อน ทำการเลือกตาราง radcheck

The screenshot shows the phpMyAdmin interface for the 'radius' database. The 'radcheck' table structure is displayed with the following fields:

Field	Type	Collation	Attributes	Null	Default	Extra
<input type="checkbox"/> id	int(11)		UNSIGNED	No		auto_increment
<input type="checkbox"/> UserName	varchar(64)	latin1_swedish_ci		No		
<input type="checkbox"/> Attribute	varchar(32)	latin1_swedish_ci		No		
<input type="checkbox"/> op	char(2)	latin1_swedish_ci		No	==	
<input type="checkbox"/> Value	varchar(253)	latin1_swedish_ci		No		

รูปที่ 55 แสดงเพิ่มรายชื่อผู้ใช้งานในตาราง radcheck

ต่อจากนั้นเลือกเมนูแทรกเพื่อทำการเพิ่มรายชื่อผู้ใช้งาน จากนั้นทำการเพิ่มรายชื่อผู้ใช้งานตามตารางที่ 1

ตารางที่ 1 radcheck ตัวอย่างการสร้างฐานข้อมูลสำหรับกำหนดบัญชีรายชื่อผู้ใช้งานในองค์กร

Radcheck Table			
UserName	Attribute	op	Value
Somsak Jaidee	User-Password	==	dHIIC2c
Somchai Rakkarndee	User-Password	==	e45DiZ83

ทดสอบชื่อและรหัสผ่านที่สร้างไว้ดังนี้

```
radtest "Somsak jaidee" dHIIC2c localhost 0 radiussecret
```

```
root@SIPAAUTH: /usr/local/simple-cdd
root@SIPAAUTH:/usr/local/simple-cdd# radtest "Somsak Jaidee" dHIIC2c localhost 0 radiussecret
Sending Access-Request of id 120 to 127.0.0.1 port 1812
  User-Name = "Somsak Jaidee"
  User-Password = "dHIIC2c"
  NAS-IP-Address = 255.255.255.255
  NAS-Port = 0
rad recv: Access-Accept packet from host 127.0.0.1:1812, id=120, length=20
root@SIPAAUTH:/usr/local/simple-cdd#
```

รูปที่ 56 แสดงผลการทดสอบเพิ่มรายชื่อผู้ใช้งาน

ตัวอย่างข้อมูลในตาราง Radreply

id	UserName	Attribute	op	Value
1	Somchai Rakkarndee	Session-Timeout	:=	10800
2	Somchai Rakkarndee	Idle-Timeout	:=	1200

รูปที่ 57 แสดงข้อมูลในตาราง Radreply

จากตารางตัวอย่าง Radreply เป็นการกำหนดค่าให้กับตาราง Radreply เพื่อให้ Somchai Rakkarndee สามารถใช้งานได้ครั้งละ 10800 วินาที (3 ชั่วโมง) และหากไม่ใช้งานอินเทอร์เน็ต 1200 วินาที (20 นาที) จะทำการตัดออกจากระบบโดยอัตโนมัติ

ในการทำงานเดียวกันหากเราต้องการกำหนดให้การใช้งานเป็นแบบใช้งานเพียงครั้งเดียว 3 ชั่วโมงก็ให้เปลี่ยนค่า Attribute จากตาราง radreply จาก Session-Timeout เป็น Max-All-Session แทน

วิธีการสร้างรายชื่อผู้ใช้งานด้วยการ import text file

1. สร้าง Text file เพื่อสร้างรายชื่อผู้ใช้งานในตาราง radcheck และตาราง radreply เมื่อสร้างข้อมูลรายชื่อผู้ใช้งานที่เราต้องการใน Text file เป็นที่เรียบร้อยแล้วให้ทำการบันทึกข้อมูลเป็นชื่อ radcheck.sql หรือจะบันทึกเป็นชื่อใหม่ก็ได้แต่นามสกุลต้องเป็น *.sql

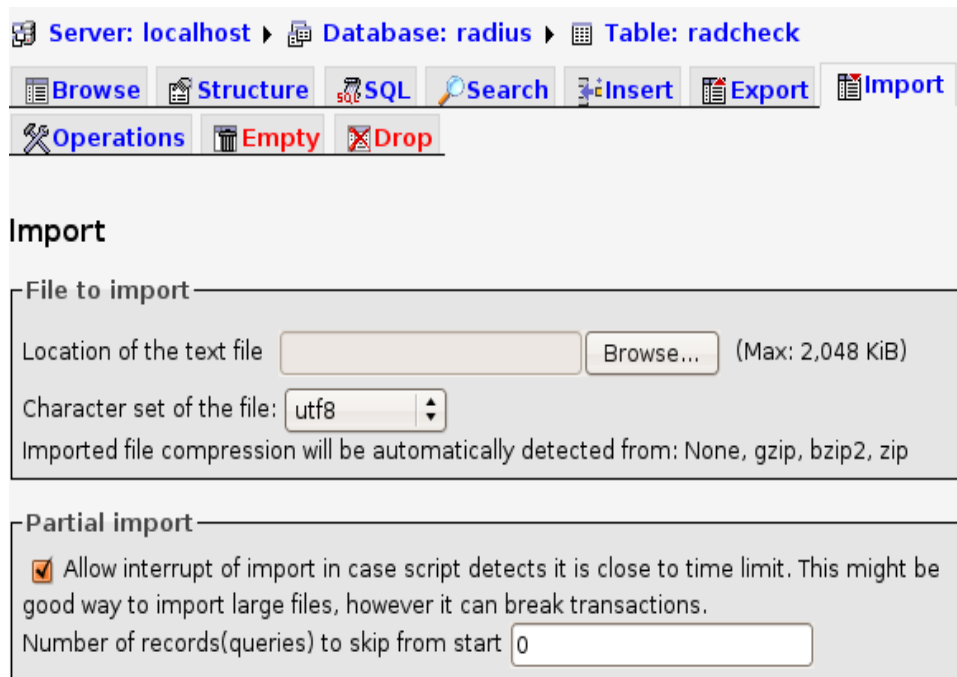
ตัวอย่างการเพิ่มรายชื่อผู้ใช้งานในตาราง radcheck

```
INSERT INTO radcheck VALUES ("', 'Somsak Jaidee', 'User-Password', '=', 'dHIIC2c'),  
('', 'Somchai Rakkarndee', 'User-Password', '=', 'e45DiZ83');
```

ตัวอย่างการเพิ่มรายชื่อผู้ใช้งานในตาราง radreply

```
INSERT INTO radreply VALUES ("', 'Somsak Jaidee', 'Session-Timeout', ':=', 10800),  
('', 'Somsak Jaidee', 'Idle-Timeout', ':=', 1200);
```

2. เมื่อสร้าง Text file แล้ว ให้เปิด PhpMyAdmin เลือกเมนู import เพื่อทำการ import text file จากนั้นกดปุ่ม Browse เพื่อเลือก text file ที่เราได้สร้างไว้จากนั้นกดปุ่ม Go เพื่อทำการ import text file



The screenshot shows the phpMyAdmin interface for the 'radcheck' table in the 'radius' database on 'localhost'. The 'Import' tab is selected. Under the 'Import' section, there is a 'File to import' section with a text input field for the file location, a 'Browse...' button, and a note '(Max: 2,048 KiB)'. Below this is a 'Character set of the file:' dropdown menu set to 'utf8'. A note states: 'Imported file compression will be automatically detected from: None, gzip, bzip2, zip'. Under the 'Partial import' section, there is a checked checkbox for 'Allow interrupt of import in case script detects it is close to time limit. This might be good way to import large files, however it can break transactions.' and a text input field for 'Number of records(queries) to skip from start' with the value '0'.

รูปที่ 58 แสดงการ import text file

3. จากนั้นทำการตรวจสอบการเพิ่มรายชื่อผู้ใช้งานด้วยโปรแกรม PhpMyAdmin โดยเลือกตาราง radcheck แล้วเลือกเมนู Browse จะแสดงรายชื่อผู้ใช้งานที่เราได้ทำการเพิ่มไว้ด้วย text file

SQL query: `SELECT * FROM `radcheck` LIMIT 0, 30`

Profiling [Edit] [Explain SQL] [Create PHP Code] [Refresh]

Show : row(s) starting from record #

in mode and repeat headers after cells

Sort by key:

	id	UserName	Attribute	op	Value
<input type="checkbox"/>	1	mysqltest	Password	==	testsecret
<input type="checkbox"/>	2	joy	Password	==	joy
<input type="checkbox"/>	3	Somsak Jaidee	Password	==	dHlIC2c
<input type="checkbox"/>	4	Somchai Rakkarndee	Password	==	e45DiZ83

Check All / Uncheck All With selected:

รูปที่ 59 แสดงรายชื่อผู้ใช้งานจาก text file

หลังจากทำการเพิ่มรายชื่อผู้ใช้งานเสร็จแล้วให้ทำการทดสอบโดยใช้ browser เปิด <https://192.168.182.1/welcome.html> จะปรากฏภาพของ Chillispot และมีลิงค์ให้ทำการ login

TESTING ONLY



Welcome to Our Hotspot, Wireless Network.

You are connected to an authentication and restricted network access point.

[Click here to login](#)

Enjoy.

รูปที่ 60 แสดงหน้าจอ welcome.html



The image shows a login form titled "ChilliSpot Login" on a light blue background. It contains two input fields: "Username:" and "Password:". Below the password field is a "Login" button.

รูปที่ 61 แสดงหน้าจอสำหรับการ Login เข้าใช้งานในระบบ

Logging

กลไกสำคัญอีกส่วนหนึ่ง ตามพรบ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ก็คือการจัดเก็บข้อมูลการจราจรคอมพิวเตอร์นั่นเอง สิ่งที่เกี่ยวข้องแม่ข่าย Authentication สามารถทำได้ก็คือการเลือกเฉพาะส่วนสำคัญของกฎหมายแล้วทำการส่งต่อไปยังอุปกรณ์ centralized log เหตุผลที่เราต้องมีการคัดเลือกเฉพาะส่วนที่จำเป็นก็คือ เพื่อไม่ให้ปริมาณแพ็คเกจของข้อมูลการจราจรทำให้การใช้งานระบบเครือข่ายคอมพิวเตอร์ช้าลง หรือ เปลืองแบนวิดธ์ของระบบนั่นเอง

สำหรับเซิร์ฟเวอร์ที่สำคัญที่จะต้องส่งต่อข้อมูลการจราจรคอมพิวเตอร์ ได้แก่ squid และ radius ขณะเดียวกันเราก็จะใช้หลักการของ IPTABLES เพื่อทำการคัดลอกข้อมูลเบื้องต้นสำหรับการใช้งานผ่านพอร์ตต่าง ๆ ที่เป็นเซิร์ฟเวอร์พื้นฐานเพื่อจัดเก็บข้อมูลการจราจรคอมพิวเตอร์ เช่น http, https, ftp, smtp, imap, pop3, IM เป็นต้น โดยการใช้วิธีนี้เป็นวิธีที่ปลอดภัยสำหรับทุก ๆ องค์กร

ข้อสังเกต อุปกรณ์บางชิ้นในท้องตลาด ติดตั้งซอฟต์แวร์พิเศษ เช่น dsniiff เป็นต้นทำการ mirror port ของอุปกรณ์สวิตช์แล้วทำการจัดเก็บข้อมูลการจราจรคอมพิวเตอร์ การใช้ซอฟต์แวร์ประเภทนี้สามารถดักจับแพ็คเกจซึ่งมีเนื้อหาของข้อความได้เช่น รหัสบัตรเครดิต รหัสจดหมายอิเล็กทรอนิกส์ เป็นต้น นับว่าเป็นอุปกรณ์ที่ไม่ควรอย่างยิ่งที่จะใช้เก็บข้อมูลการจราจรคอมพิวเตอร์

เนื้อหาต่อไปนี้จะเป็นส่วนอธิบายเนื้อหาต่าง ๆ ต่อไปนี้

การติดตั้ง Time server และการขอเทียบเวลาโดยใช้ Linux (ที่มา เอกสารการอบรมการเก็บข้อมูลจราจร ตาม พรบ.ว่าด้วยการกระทำผิดด้วยคอมพิวเตอร์ พ.ศ. 2550 ของอ.บุญลือ อยู่คง)

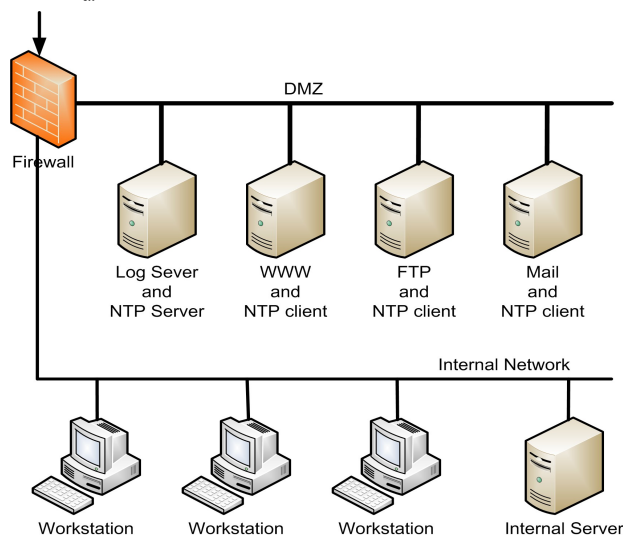
ขั้นตอนการติดตั้ง Transparent Proxy Squid

การติดตั้ง logging server เพื่อทำการส่งข้อมูลการจราจรคอมพิวเตอร์ไปยังเครื่องแม่ข่าย centralized log

Install Time Server

โปรแกรมที่ใช้สำหรับการเทียบเวลาและการตั้งเครื่องแม่ข่ายฐานเวลาที่นิยมใช้กันคือ ntp โดยขั้นตอนการตั้งฐานเวลาที่สำคัญ (ที่มา เอกสารการอบรมการเก็บข้อมูลจราจร ตาม พรบ. ว่าด้วยการกระทำผิดด้วยคอมพิวเตอร์ พ.ศ. 2550 ของอ.บุญลือ อยู่คง)

1. ขั้นตอนการติดตั้ง NTP Server (Network Time Protocol) ก่อนอื่นต้องดูหลักเกณฑ์ในข้อ ๕ ตรงข้อความที่ว่า ต้องตั้งนาฬิกา ของอุปกรณ์บริการทุกชนิดให้ตรงกับเวลาอ้างอิง ingsากล (Stratum 0) และแนะนำให้ใช้วิธีการติดตั้ง NTP Server ไว้ในระบบหนึ่งเครื่องน่าจะเอาไว้ที่เครื่อง Log Server เพื่อจ่ายสัญญาณนาฬิกาให้กับเครื่อง Server และเครื่อง Workstation ทั้งหมดในระบบเป็นลำดับที่ 1 ส่วนลำดับที่ 2 และ 3 ให้อ้างอิงไปยังฐานเวลาภายนอก เพราะถ้าให้ Server แต่ละตัวไปร้องขอ sync สัญญาณนาฬิกาจากภายนอกเวลาอาจมีปัญหาได้เพราะระบบ Network ในบ้านเราการให้บริการยังมีปัญหาติดขัดเป็นประจำที่แน่ ๆ คือแทบจะวิ่งออกไปท่องใน Internet กันไม่ได้เลยอาจเป็นปัญหาในการอ้างอิงเวลาให้กับ Server และ Workstation แต่ละตัวได้ สำหรับโปรแกรม ntp สามารถกำหนดค่า Configure ให้เป็นได้ทั้ง Server และ Client ตัวอย่างต่อไปนี้จะติดตั้ง Server เพียงเครื่องเดียว นอกนั้นทั้ง Server และ Workstation ในระบบจะทำ configure ให้เป็น Client เพื่อร้องขอเทียบฐานเวลาจาก Server ดังภาพ



รูปที่ 62 แสดงการอ้างอิงฐานเวลาและ Log Server

ขั้นที่ 1 ให้ติดตั้งโปรแกรม ntp บน Server (ในภาพเป็นเครื่อง Log Server) ดังนี้

```
apt-get install ntp
```

คงไม่ต้องอธิบายรายละเอียดมากเกินไปเพราะผู้ดูแลระบบที่จะทำขั้นนี้ได้คงไม่ต้องบอกวิธีการ mount cd หรือการติดตั้งผ่าน Internet และก่อนที่จะทำการแก้ไข Configuration ให้ทำการตรวจสอบวันเวลาที่ server ที่อ้างอิงในประเทศไทยตามตาราง NTP Server ที่แนะนำตามตาราง

ตารางที่ 2 แสดงการอิงเวลามาตรฐานของประเทศไทย

NTP Server Address	หน่วยงาน	Clock Strata	อุปกรณ์อ้างอิง
203.185.69.60	สถาบันมาตรวิทยาแห่งชาติ	Stratum-1	นาฬิกาซีเซียม Stratum-0 เทียบด้วยค่า TAI โดย BIPM (precision ~50 nSec)
time.navy.mi.th	กรมอุทกศาสตร์ กองทัพเรือ	Stratum-1	นาฬิกาซีเซียม Stratum-0 ทำ MOU กับสถาบันมาตรฯ เพื่อส่งค่าเทียบกับ BIPM
time.nist.gov	National Institute of Standards and TechnoLogy, US	Stratum-1	นาฬิกาซีเซียม Stratum-0 เทียบด้วยค่า TAI โดย BIPM

ขั้นที่ 2 หลังจากทำการตรวจสอบเรียบร้อยแล้ว ให้ไปแก้ไขค่า configure ให้มีค่าดังนี้

```
cp /etc/ntp.conf /etc/ntp.conf.bak
```

```
vi /etc/ntp.conf
```

```
restrict default kod nomodify notrap noquery nopeer
restrict 127.0.0.1
# อนุญาตให้ internal network เข้าใช้
restrict 192.168.1.0 mask 255.255.255.0 nomodify notrap
server 203.185.69.60 dynamic
server time.navy.mi.th dynamic
server time.nist.gov dynamic
server 127.127.1.0 # local clock
fudge 127.127.1.0 stratum 10
driftfile /var/lib/ntp/drift
broadcastdelay 0.008
keys /etc/ntp/keys
เมื่อตรวจสอบแก้ไขค่าให้มิตามนี้แล้วบันทึก
:wq
```

ขั้นที่ 3 ตรวจสอบ Remote Server ที่ต้องการใช้อ้างอิงฐานเวลา ใช้คำสั่งดังนี้

```
apt-get install ntpdate
```

```
ntpdate -b 203.185.69.60
```

```
ntpdate -b time.navy.mi.th
```

```
ntpdate -b time.nist.gov
```

28 Jan 14:28:20 ntpdate[2693]: step time server 192.43.244.18 offset **-0.092687** sec

ตัวอย่าง NTP Server ของ Nectec

```
ntpdate -b clock.nectec.or.th
```

```
ntpdate -b clock2.nectec.or.th
```

```
ntpdate -b clock.thaicert.nectec.or.th
```

ที่ต้องให้ทำการทดสอบค่าเวลาระหว่างเครื่องของเรากับ Server ภายนอกเพื่อให้เลือกหา Server ที่เวลาอ้างอิงใกล้เคียงกันมากที่สุด (ดูผลค่า **offset** ต้องมีค่าน้อยที่สุดถ้าเป็นไปได้ควรเลือก Server ในประเทศไทย เลือกมาจัดอันดับที่ 1, 2, 3 ใน configuration) และต้องไม่พบปัญหา `no server suitable for synchronization found` เพราะถ้าไม่มี host ที่อ้างอิงก็จะไม่สามารถใช้เป็นมาตรฐานเวลาได้

ขั้นที่ 4 ก่อนสั่ง restart service ให้ตรวจสอบ server อ้างอิงอีกครั้ง

```
ntpdate -b 203.185.69.60
```

สั่ง restart service

```
/etc/init.d/ntpd restart
```

ขั้นที่ 5 ตรวจสอบการทำงานจาก Log file

```
grep ntpd /var/log/syslog จะได้ค่าคล้าย ๆ กับตัวอย่างข้างล่าง
```

```
Jan 28 15:47:49 ns1 ntpd[3838]: ntpd 4.2.4p2@1.1495-o Thu Jun 21 12:57:41 UTC 2007 (1)
```

```
Jan 28 15:47:49 ns1 ntpd[3839]: precision = 2.000 usec
```

```
Jan 28 15:47:49 ns1 ntpd[3839]: Listening on interface #2 lo, ::1#123 Enabled
```

```
Jan 28 15:47:49 ns1 ntpd[3839]: Listening on interface #5 eth0, 192.168.1.10#123 Enabled
```

```
Jan 28 15:47:49 ns1 ntpd[3839]: kernel time sync status 0040
```

```
Jan 28 15:47:50 ns1 ntpd[3839]: frequency initialized 80.586 PPM from /var/lib/ntp/drift
```

ขั้นที่ 6 หลังจาก Server ทำงานปกติไม่มีการแจ้ง Error ใด ๆ สามารถตรวจสอบตารางการทำงานของ Server ได้ด้วยคำสั่ง

```
ntpq -pn
```

```
remote      refid      st t when poll reach  delay  offset  jitter
=====
203.185.69.60 .PPS.      1 u 49 64 3 49.263 577.356 40.539
122.154.11.67 .GPS.      1 u 50 64 3 50.387 568.011 4.886
192.43.244.18 .ACTS.     1 u 111 64 2 607.213 463.669 0.002
127.127.1.0   .LOCL.     101 48 64 3 0.000 0.000 0.002
```

สามารถใช้เครื่อง Linux เครื่องอื่นในระบบทดสอบการทำงานของ Server ได้ด้วยคำสั่ง

```
ntpdate <ip address> ใส่ ip address ของเครื่อง NTP Server
```

ขั้นที่ 7 สำหรับเครื่อง **Server Linux** ที่เหลือทั้งหมดของระบบให้ทำการแก้ไขค่า configuration ของโปรแกรม ntp ให้ร้องขอเวลาจาก NTP Server ดังนี้

```
vi /etc/ntp.conf
```

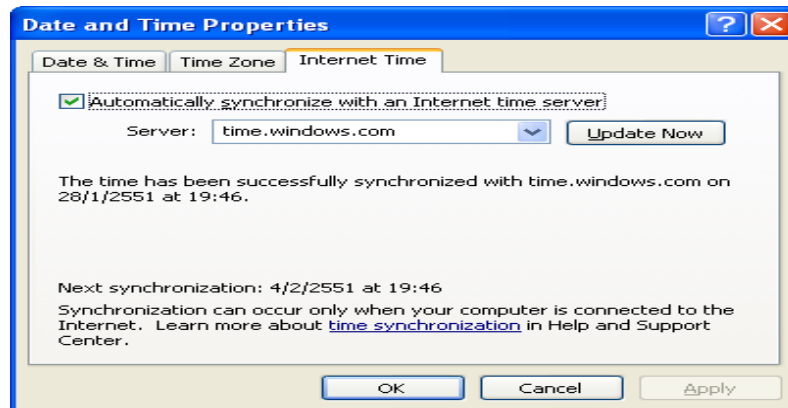
```
server 192.168.1.1          <- ip address ของ NTP Server
restrict default ignore
restrict 127.0.0.1
restrict 192.168.1.1 mask 255.255.255.255 nomodify notrap noquery
driftfile /var/lib/ntp/drift
:wq
```

```
/etc/init.d/ntpd restart
```

ใช้คำสั่งตรวจสอบการทำงานเหมือนกับการตั้ง NTP Server ตามตัวอย่างข้างบนที่ผ่านมาแล้วเพื่อให้แน่ใจว่ามีการอ้างอิงเวลาจาก NTP Server ของเราหรือยัง

ขั้นที่ 8 ต่อไปให้จัดการกับเครื่องลูกข่ายในองค์กรหรือหน่วยงาน ซึ่งผู้เขียนจะยกตัวอย่างเฉพาะลูกข่ายที่

เป็น Microsoft Windows เพราะเป็นผู้ใช้ส่วนใหญ่ของประเทศ ถ้าเป็น OS ค่ายอื่นต้องศึกษาจากคู่มือของค่ายนั้น ๆ
ขั้นตอนนี้นำไปแก้ไขค่า Internet time ของเครื่องลูกข่ายโดยไปดับเบิลคลิกที่ นาฬิกาด้านล่างขวาของ Task bar จะ
ได้หน้าจอดังนี้



รูปที่ 63 แสดงการแก้ไขค่า Internet time

จากภาพจะเห็นว่าที่เครื่องลูกข่ายจะมีส่วนของการตั้งเวลาอัตโนมัติ นั่นคือมีการให้กรอกค่า Network Time Server (NTP) เพื่อให้เครื่องสามารถตั้งเวลาตรงกับเวลาสากลได้อย่างถูกต้อง แต่ค่าหลัก (Default) ที่ Microsoft Windows XP กำหนดให้มาเป็นการ Update เวลาทุก ๆ 7 วัน ทำให้เวลาที่ตั้งไว้อาจไม่ตรงหรือคลาดเคลื่อนได้เมื่อเครื่องลูกข่ายมีเวลาไม่ตรงกับเวลามาตรฐานทำให้การบันทึก Log file การใช้งานคลาดเคลื่อนไม่เป็นไปตามกฎหมาย คงไม่สามารถไปบังคับลูกข่ายว่าก่อนเล่นต้องคลิกที่ Update Now คงไม่มีใครยอมทำตามเป็นแน่ให้จัดการกับเครื่องลูกข่ายทุกเครื่อง โดยการไปแก้ไข Registry (คิดเองว่าจะใช้วิธีอะไรแก้ไขทุกเครื่อง) ดังนี้

ไปที่เมนู Start -> Run -> regedit กด Enter เข้าไปที่ตำแหน่ง

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\w32time\TimeProviders\NtpClient]

จอกภาพด้านขวามือจะมีคำว่า SpecialPollInterval เมื่อดับเบิลคลิกจะปรากฏค่าเป็นเลขฐานสิบหก (Hex) "SpecialPollInterval"=dword:00093a80 ให้เลือกเป็น decimal จะเปลี่ยนจาก 93a80 เป็น 604800 ค่านี้มีหน่วยเป็นวินาทีที่มีค่าเท่ากับ 7 วัน (1 วัน = 86400 วินาที) ต้องการให้มีการ Update ที่วินาที ที่นาที หรือที่ชั่วโมง ก็ให้แก้ไขเลขนี้ได้เลยตามต้องการและที่สำคัญคือให้พิมพ์ลงไปช่อง Server ของเดิมเป็น time.windows.com เปลี่ยนเป็นเลข IP Address ของเครื่อง NTP Server ที่ตั้งขึ้นเองแล้วทดลองคลิก Update Now ถ้าทำสำเร็จบรรทัดต่อลงมาจะเป็นรายงานว่าเวลาได้ Sync กับ Server เรียบร้อยแล้ว และต้องไม่ลืมเป็นสิ่งที่สุดท้ายคือต้องตั้งให้ Windows Time



Service อยู่ที่ Automatic เพื่อให้ start service ทุกครั้งที่เครื่อง Boot

Tip & Trick

สำหรับการทำ NTP Server จะมีการใช้งานโปรโตคอล NTP หมายเลข **Port = 123** ต้องไปดูเรื่อง **Firewall** อนุญาตให้ลูกข่ายสามารถเข้าใช้ Port และ Protocol ให้ตรงกันจึงจะใช้งานได้

Install Transparent Proxy Squid

ความหมายของ Transparent Proxy คือทำให้เครื่องลูกข่ายทุกเครื่องที่ใช้งานอินเทอร์เน็ตผ่านเกตเวย์ของเรา ไม่ต้องทำการตั้งค่า Internet proxy ที่ตัวเว็บเบราว์เซอร์ของเครื่องลูกข่ายเอง จริง แล้วซอฟต์แวร์ squid เองมีการให้บริการการทำ authentication ผ่านตัวเองอยู่เหมือนกัน แต่มีข้อจำกัดคือทำได้เฉพาะโปรโตคอล http เท่านั้น อีกทั้งไม่สามารถทำงานร่วมกับ transparent proxy ได้ ทำให้ไม่สะดวกเป็นอย่างมากในการกำหนดค่าพร็อกซีเซิร์ฟเวอร์ให้เว็บเบราว์เซอร์ ทุก ๆ ตัว โดยเนื้อหาในบทนี้ผู้เขียนจะไม่ขอกล่าวละเอียดมากนักเพราะไม่ใช่จุดประสงค์หลักของการสร้างเครื่องแม่ข่าย Authentication Gateway อย่างไรก็ตามรายละเอียดเพิ่มเติมสามารถศึกษาได้จากเว็บไซต์ทั่ว ๆ ไป รวมถึงเว็บไซต์ของผู้ผลิตซอฟต์แวร์นี้ <http://www.squid-cache.org>

โดยขั้นตอนการติดตั้งและการกำหนดค่าสามารถทำได้ง่าย ๆ ดังนี้

ทำการติดตั้งซอฟต์แวร์ squid ก่อน

```
apt-get install squid
```

หลังจากติดตั้งซอฟต์แวร์ squid แล้วให้ทำการกำหนดค่าไฟล์ `/etc/squid/squid.conf` ต้องทำการคอมเมนต์ข้อความ `#http_port 3128` และเพิ่มค่าเข้าไป 4 บรรทัด โดยต้องคำนึงถึงตำแหน่งของไฟล์ด้วยดังนี้

```
vi /etc/squid/squid.conf
```

```
# Squid normally listens to port 3128
```

```
# http_port 3128
```

```
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
```

```
acl chillispot src 192.168.182.0/255.255.255.0
```

```
http_port 192.168.182.1:3128 transparent
```

```
http_access allow chillispot
```

บรรทัดล่างสุดเพิ่มข้อความ

```
visible_hostname administrator-desktop
```

คำอธิบาย

http_port 3128เป็นการยกเลิกการทำงานของโปรแกรมแบบไม่ทำ transparent
visible_hostname ต้องกำหนดชื่อเครื่องให้กับระบบหากไม่ใส่จะทำให้ไม่สามารถสตาร์ทเซอร์วิสได้
acl chillspot src เป็นการกำหนดค่าเน็ตเวิร์คของเครื่องข่ายคอมพิวเตอร์ที่จะอนุญาตให้ใช้งานผ่านโปรแกรม squid
http_port x.x.x.x.3128 transparent เป็นการกำหนดให้พอร์ต 3128 เป็น transparent proxy
http_access allow กำหนดค่า access control ให้เน็ตเวิร์ควง chillspot สามารถใช้งานผ่าน transparent proxy squid
ได้

สั่งให้โปรแกรม squid ทำงาน

```
/etc/init.d/squid start
```

ตรวจสอบเซอร์วิสของ squid ว่าทำงานหรือไม่ดังนี้

```
ps -ef | grep "squid"
```

หรือคำสั่ง

```
netstat -lnt
```

สุดท้ายเป็นการกำหนดค่ากฎไฟร์วอลล์ โดยต้องทำการตั้งค่าทั้งหมดดังนี้

1. ให้ทำการส่งต่อแพ็กเก็ตที่เข้ามาทางพอร์ต 80 ไปยัง squid พอร์ต 3128

```
iptables -t nat -A PREROUTING -i tun0 -p tcp -m tcp --dport 80 -j REDIRECT --to-ports 3128
```

2. ต้องอนุญาตให้ใช้งาน INPUT ที่เป็นแพ็ก syn

```
iptables -A INPUT -i tun0 -p tcp -m tcp --dport 3128 --syn -j ACCEPT
```

3. ต้องเพิ่ม rule ต่อไปนี้เพื่อป้องกันการเข้าใช้งานระบบโดยการแอบตั้งค่า proxy เอง

```
Iptables -t nat -I PREROUTING -p tcp -m tcp --dport 3128 -j DROP
```



หมายเหตุ ในข้อที่ 3 หากเราต้องการป้องกันการเข้าใช้งานโดยการตั้งค่าพรีอ็อกซีเอง เช่น dansguardian ที่พอร์ต 8080 หรือ frox ที่พอร์ต 2121 ให้เพิ่มคำสั่งข้างล่างดังนี้

```
iptables -t nat -I PREROUTING -p tcp -m tcp --dport 8080 -j DROP
```

```
Iptables -t nat -I PREROUTING -p tcp -m tcp --dport 2121 -j DROP
```

Install logging server

เริ่มการติดตั้งโปรแกรม syslog-ng

เพื่อทำการส่งข้อมูลการจราจรคอมพิวเตอร์ไปยังเครื่องแม่ข่าย centralized log ซอฟต์แวร์ที่นิยมใช้กันก็คือ syslog-ng ของบริษัท BalaBit IT Security <http://www.balabit.com> ซึ่งมีความสามารถสูงกว่าระบบ syslog ทั่วไป เช่น สามารถรับส่งข้อมูลผ่าน โปรโตคอล tcp , สามารถฟิลเตอร์ข้อความทั้งก่อนส่งและก่อนการจัดเก็บ, สามารถจัดเก็บข้อความลงในโปรแกรมฐานข้อมูลเพื่อให้สะดวกในการเรียกดู และแม้แต่สามารถทำต่อระหว่างเครื่องส่งและเครื่องรับได้ด้วยแต่จะมีเฉพาะในส่วนของ commercial

```
apt-get install syslog-ng
```

หลังจากนั้นกำหนดค่าเพิ่มให้กับไฟล์ syslog-ng.conf ดังนี้ โดยให้พิมพ์ต่อจากไฟล์คอนฟิกเดิมของระบบ

```
destination remote {  
    udp("192.168.20.104" port(514));  
};  
log {source(s_all); filter(f_messages); destination(remote); };  
log {source(s_all); filter(f_kern); destination(remote); };
```

ค่าที่ต้องการตั้งคือค่าหมายเลขไอพีแอดเดรสของเครื่องแม่ข่าย centralized log ในระบบ
สั่งให้โปรแกรม syslog-ng ทำงาน

```
/etc/init.d/syslog-ng start
```

ต่อไปเป็นการกำหนดค่าให้กับ iptables ทำการส่งข้อมูลการจราจรคอมพิวเตอร์ไปยังตัว syslog-ng agent

```
vi rc.iptablescapture
```

```
#!/bin/bash
```

```
iptables -t nat -N logging
```

```
iptables -t nat -A PREROUTING -j logging
```



```
iptables -t nat -A POSTROUTING -j logging
iptables -A INPUT -j LOG --log-level info --log-prefix "INPUT "
iptables -A OUTPUT -j LOG --log-level info --log-prefix "OUTPUT "
iptables -A FORWARD -j LOG --log-level info --log-prefix "FORWARD "
# HTTP:
iptables -t nat -A logging -p tcp --dport 80 -j LOG --log-prefix "HTTP: " \
--log-level info
# HTTPS:
iptables -t nat -A logging -p tcp --dport 443 -j LOG --log-prefix "HTTPS: " \
--log-level info
# SMTP:
iptables -t nat -A logging -p tcp --dport 25 -j LOG --log-prefix "SMTP: " \
--log-level info
# FTP:
iptables -t nat -A logging -p tcp --dport 21 -j LOG --log-prefix "FTP: " \
--log-level info
# IMAP:
iptables -t nat -A logging -p tcp --dport 143 -j LOG --log-prefix "IMAP: " \
--log-level info
# POP3:
iptables -t nat -A logging -p tcp --dport 110 -j LOG --log-prefix "POP3: " \
--log-level info
# MSN:
iptables -t nat -A logging -p tcp --dport 1863 -j LOG --log-prefix "MSN: " \
--log-level info
# JABBER:
iptables -t nat -A logging -p tcp --dport 5222 -j LOG --log-prefix "JABBER: " \
--log-level info
```

```
# JABBERS
```

```
iptables -t nat -A logging -p tcp --dport 5223 -j LOG --log-prefix "JABBERS: " \
--log-level info
```

```
# ICQ/AIM
```

```
iptables -t nat -A logging -p tcp --dport 5190 -j LOG --log-prefix "ICQ/AIM: " \
--log-level info
```

```
# Yahoo
```

```
iptables -t nat -A logging -p tcp --dport 5050 -j LOG --log-prefix "YAHOO: " \
--log-level info
```

```
# IRC
```

```
iptables -t nat -A logging -p tcp --dport 6667 -j LOG --log-prefix "IRC: " \
--log-level info
```

```
# Gadu-Gadu
```

```
iptables -t nat -A logging -p tcp --dport 8074 -j LOG --log-prefix "GADU-GADU: " \
--log-level info
```

```
Chain logging (2 references)
pkts bytes target      prot opt in     out    source            destination
14  672 LOG          tcp  --  *     *     0.0.0.0/0         0.0.0.0/0         tcp dpt:80 LOG flags 0 level 6 prefix `HTTP: '
0    0 LOG          tcp  --  *     *     0.0.0.0/0         0.0.0.0/0         tcp dpt:443 LOG flags 0 level 6 prefix `HTTPS: '
0    0 LOG          tcp  --  *     *     0.0.0.0/0         0.0.0.0/0         tcp dpt:25 LOG flags 0 level 6 prefix `SMTP: '
0    0 LOG          tcp  --  *     *     0.0.0.0/0         0.0.0.0/0         tcp dpt:21 LOG flags 0 level 6 prefix `FTP: '
0    0 LOG          tcp  --  *     *     0.0.0.0/0         0.0.0.0/0         tcp dpt:143 LOG flags 0 level 6 prefix `IMAP: '
0    0 LOG          tcp  --  *     *     0.0.0.0/0         0.0.0.0/0         tcp dpt:110 LOG flags 0 level 6 prefix `POP3: '
0    0 LOG          tcp  --  *     *     0.0.0.0/0         0.0.0.0/0         tcp dpt:1863 LOG flags 0 level 6 prefix `MSN: '
0    0 LOG          tcp  --  *     *     0.0.0.0/0         0.0.0.0/0         tcp dpt:5222 LOG flags 0 level 6 prefix `JABBER: '
0    0 LOG          tcp  --  *     *     0.0.0.0/0         0.0.0.0/0         tcp dpt:5223 LOG flags 0 level 6 prefix `JABBERS: '
0    0 LOG          tcp  --  *     *     0.0.0.0/0         0.0.0.0/0         tcp dpt:5190 LOG flags 0 level 6 prefix `ICQ/AIM: '
0    0 LOG          tcp  --  *     *     0.0.0.0/0         0.0.0.0/0         tcp dpt:5050 LOG flags 0 level 6 prefix `Yahoo: '
0    0 LOG          tcp  --  *     *     0.0.0.0/0         0.0.0.0/0         tcp dpt:6667 LOG flags 0 level 6 prefix `IRC: '
0    0 LOG          tcp  --  *     *     0.0.0.0/0         0.0.0.0/0         tcp dpt:8074 LOG flags 0 level 6 prefix `GADU-GADU: '
```

รูปที่ 64 แสดงผลการรันสคริป rc.iptablescapture

ตัวอย่างต่อไปเป็นขั้นตอนที่ใช้ส่งค่าข้อมูลการจราจรคอมพิวเตอร์จากเซิร์ฟเวอร์ของ squid และ radius ไปยัง syslog โดยอาศัยหลักการเปลี่ยนข้อมูลล็อกไฟล์ให้เป็นสตรีมมิ่งโดยใช้คำสั่ง tail ของยูนิกซ์ช่วยดังนี้

- การส่งค่าจาก squid ไปยัง syslog

```
tail -F /var/log/squid/access.log | logger -t squid -p local3.info
```

- การส่งค่าจาก radius ไปยัง syslog ต้องไปแก้ค่าที่ไฟล์ radiusd.conf

```
#detailfile = ${radacctdir}/%{Client-IP-Address}/detail-%Y%m%d  
detailfile = ${radacctdir}/%{Client-IP-Address}/details
```

จากนั้นทำการส่งค่าจาก radiusd ไปยัง syslog ดังนี้

```
tail -F /var/log/radius/radacct/127.0.0.1/details | logger -t radiusd -p local3.info
```

หมายเหตุ คำสั่ง logger -t จะใช้กำหนดชื่อข้อมูลการจราจรคอมพิวเตอร์ ในที่นี้เราจะใช้แทนว่าข้อมูลการจราจรคอมพิวเตอร์มาจากเซิร์ฟวิสใด เช่น squid และ radius เป็นต้น และต้องห้ามลืมใช้ tail -F เพราะจะเป็นการกำหนดให้ tail ทำงานไม่ว่าไฟล์ต้นทางจะมีการสร้างไฟล์ใหม่หรือไม่ก็ตาม

สำหรับวิธีการแก้ปัญหาไฟล์ที่อาจจะใหญ่เกินไปสำหรับข้อมูลล็อกไฟล์ของ radius เซิร์ฟเวอร์เราสามารถใช้งานร่วมกับ logrotate โดยสร้างไฟล์ชื่อว่า /etc/logrotate.d/radius เพื่อจัดการกับไฟล์ดังกล่าว

```
/var/log/radius/radacct/127.0.0.1/details {  
  
    rotate 13  
  
    weekly  
  
    missingok  
  
    notifempty  
  
    compress  
  
}
```


การตั้งค่าให้ส่งข้อมูลการจราจรคอมพิวเตอร์จาก squid และ radius โดยให้ทำงานทุกครั้งหลังเปิดเครื่องดังนี้

vi /etc/init.d/rc.capture

```
#!/bin/bash
tail -F /var/log/squid/access.log | logger -t squid -p local3.info &
tail -F /var/log/radius/radacct/127.0.0.1/details | logger -t radiusd -p local3.info &
```

จากนั้นสั่งให้สามารถรันได้และสร้างลิงค์ให้ทำงานทุกครั้งหลังเปิดเครื่อง

```
chmod a+x /etc/init.d/rc.capture
ln -s /etc/init.d/rc.capture /etc/rcS.d/S88rccapture
```

ตัวอย่างค่าคอนฟิกูเลชันของ syslog-ng.conf สำหรับเครื่องแม่ข่าย centralized log

- สำหรับการตั้งค่าเป็นเครื่อง centralized log

```
source s_sys {  
    file ("/proc/kmsg" log_prefix("kernel: "));  
    unix-stream ("/dev/log");  
    internal();  
    udp(ip(0.0.0.0) port(514));  
    tcp(ip(0.0.0.0) port(514) keep-alive(yes));  
};
```

- สำหรับฟิลเตอร์โปรแกรม squid

```
filter f_squid { match("squid"); };  
destination d_squid {  
    file("/var/log/$HOST/$YEAR/$MONTH/squid.$YEAR-$MONTH-$DAY"  
    owner(root) group(adm) perm(665)  
    create_dirs(yes) dir_perm(0775));  
};  
log { source(s_sys); filter(f_squid); destination(d_squid); };
```

- สำหรับฟิลเตอร์โปรแกรม radiusd

```
filter f_radius { match("radiusd"); };  
destination d_radius {  
    file("/var/log/$HOST/$YEAR/$MONTH/radius.$YEAR-$MONTH-$DAY"  
    owner(root) group(adm) perm(665)  
    create_dirs(yes) dir_perm(0775));  
};  
log { source(s_sys); filter(f_radius); destination(d_radius); };
```

ขั้นตอนเพิ่มเติมการติดตั้งจากแผ่นติดตั้งพิเศษ AUTHENTICATION

INTERNET(dhcp) ---|eth0 SIPAAUTH eth1|-- Local Network (192.168.182.0/24)

ขั้นตอนที่ 1 ติดตั้งจากแผ่น debian-804-i386-CD-1.iso ซึ่งมีข้อจำกัดอยู่ที่ต้องต่อสายแลนด้านอินเทอร์เน็ตเข้ากับ eth0 และต้องสามารถใช้งานอินเทอร์เน็ตด้วย dhcp ได้ ส่วนสายด้าน eth1 ยังไม่ต้องเสียบสายก่อน จากนั้นดำเนินการติดตั้งตามขั้นตอนปกติ และเลือกโปรไฟล์ชื่อว่า “AUTH”

ขั้นตอนที่ 2 หลังจากเริ่มสตาร์ทเครื่องครั้งที่สอง ป้อนชื่อผู้ใช้และรหัสผ่านแล้ว ให้ทำการใส่แผ่นติดตั้งอีกครั้งหนึ่งแล้วทำการ mount แผ่นดังนี้ และตั้งรันสคริปเพื่อเตรียมการติดตั้งแพ็คเกจส่วนที่เหลือให้กับเครื่องดังนี้

```
# mount -t iso9660 /dev/cdrom /media/cdrom
# cp /media/cdrom/simple-cdd/* /usr/local/simple-cdd/
# chmod 755 /usr/local/simple-cdd/*
# /usr/local/simple-cdd/AUTH.postinst
```

เอาแผ่นออกแล้วทำการรีสตาร์ทเครื่องใหม่อีกครั้งหนึ่ง

```
# umount /dev/cdrom
# shutdown -r now
```

ขั้นตอนที่ 3 หลังจากเครื่องสตาร์ทใหม่ครั้งที่สามให้ทำตามขั้นตอนที่เหลือ ต้องตอบ “Y” syslog-ng และ ssl กำหนดค่าให้กับ CA และต้องให้ตั้งชื่อเครื่องว่า “SIPAAUTH” จากนั้นล๊อคออนแล้วรันสคริปเพื่อสร้างฐานข้อมูลต่อไปนี้

```
# mysqladmin password mysqlsecret
# /usr/local/simple-cdd/auth-mysql.sh
```

จากนั้นต้องสั่งรีสตาร์ทเซอร์วิส freeradius และทดสอบโดยใช้คำสั่ง

```
# /etc/init.d/freeradius restart
# radtest “Somsak Jaidee” dHIIC2c 127.0.0.1 0 radiussecret
```

สุดท้ายต่อสายแลน eth1 ด้านเครื่องลูกข่ายเข้ากับสวิตช์ ระบบเครื่องแม่ข่าย Authentication ก็พร้อมที่จะใช้งานได้



References

- <https://help.ubuntu.com/community/WifiDocs/ChillispotHotspot>
- <http://mamboeasy.psu.ac.th/~wiboon.w/>
- <http://www.ubuntu.com/>
- <http://www.ubuntuclub.com/>