การออกแบบ และ การวัดประสิทธิภาพของระบบเครือข่าย: กรณีศึกษา วิทยาลัยพลศึกษานครหลวงเวียงจันทน์

มัยสุข ยางเจยมัว

งานนิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรมหาบัณฑิต
สาขาวิชาเทคโนโลยีสารสนเทศ
คณะวิทยาการสารสนเทศ มหาวิทยาลัยบูรพา
เมษายน 2559

คณะกรรมการควบคุมงานนิพนธ์และคณะกรรมการสอบงานนิพนธ์ได้พิจารณางานนิพนธ์ของ นายมัยสุข ยางเจยมัว ฉบับนี้แล้ว เห็นสมควรรับเป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ ของมหาวิทยาลัยบูรพาได้

คณะกรรมการควบคุมงานนิพนธ์

..... อาจารย์ที่ปรึกษา
(ดร. ณัฐนนท์ ลีลาตระกูล)

คณะกรรมการสอบวิทยานิพนธ์

..... ประธานกรรมการ
(ดร.ภารุจ รัตนวรพันธุ์)

..... กรรมการ
(ผู้ช่วยศาสตราจารย์ ดร. สุนิสา ริมเจริญ)

..... กรรมการ
(ดร. ณัฐนนท์ ลีลาตระกูล)

คณะวิทยาการสารสนเทศ อนุมัติให้รับงานนิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ ของมหาวิทยาลัยบูรพา

..... คณบดีคณะวิทยาการสารสนเทศ
(ผู้ช่วยศาสตราจารย์ ดร.กฤษณะ ชินสาร)

วันที่ ๒๓ เดือน สิงหาคม พ.ศ. ๒๕๕๙

กิตติกรรมประกาศ

งานนิพนธ์ฉบับนี้สำเร็จลุล่วงอย่างสมบูรณ์เนื่องด้วยความเมตตากรุณา และ คำแนะนำอันมีค่ายิ่งจาก ดร.ณัฐนนท์ ลีลาตระกูล อาจารย์ที่ปรึกษา ที่กรุณาให้คำปรึกษาแนะนำแนวทางที่ถูกต้องตลอดจนแก้ไขข้อบกพร่องต่าง ๆ ด้วยความละเอียดถี่ถ้วน และ เอาใจใส่ด้วยดีเสมอมา ผู้ทำงานนิพนธ์รู้สึกซาบซึ้งเป็นอย่างยิ่งจึงขอบกราบขอบพระคุณเป็นอย่างสูงไว้ ณ โอกาสนี้

ขอกราบขอบพระคุณ สำนักงานความร่วมมือเพื่อการพัฒนาระหว่างประเทศ (สพร.) กระทรวงการต่างประเทศที่ได้สนับสนุนทุนการศึกษาให้แก่ผู้ทำงานวิทยานิพนธ์ และ มอบความรักความห่วงใยรวมทั้งความเข้าใจเสมอมา

ขอกราบขอบพระคุณ ขอขอบคุณผู้อำนวยการวิทยาลัยพละศึกษา ดร.อินตอง เลิศสินไชย และ ครูอาจารย์ทุกท่านที่สังกัดอยู่วิทยาลัยพละศึกษานครหลวงเวียงจันทน์ที่ได้สนับสนุนทุนและ สถานที่การศึกษาให้แก่ทำงานวิทยานิพนธ์ และ มอบความรัก ความห่วงใย รวมทั้งความเข้าใจเสมอมา

ขอกราบขอบพระคุณวิทยาลัยครูคังไขที่ประเทศลาวที่ได้สนับสนุนทุนการศึกษาให้โอกาส ได้ทำงานนิพนธ์ และ มอบความรัก ความห่วงใยรวมทั้งความเข้าใจเสมอมา

ขอกราบขอบพระคุณ อาจารย์ และ พนักงานวิขาการที่คณะวิทยาการสารสนเทศทุก ๆ คน ให้การสนับสนุนการทำงานนิพนธ์เสมอมา

ขอกราบขอบพระคุณ พี่ ๆ เพื่อน และ น้อง ๆ หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ ๆ คน ให้การสนับสนุนการทำงานนิพนธ์เสมอมา

ขอกราบขอบพระคุณ สำนักงานเอกอัครราชทูตลาวประจำประเทศไทยที่ได้ดูแล และ อำนวยความสะดวกให้แก่ข้าพเจ้าทุกประการในระยะเวลาการศึกษาครั้งนี้

ขอกราบขอบพระคุณ คุณพ่อ วันนี ยางเจยมัว และ คุณแม่ ซ้งหมี ยางเจยมัว อันเป็นที่รักยิ่ง ที่ได้ให้กำเนิดชีวิต และ สนับสนุนการศึกษาแก่ข้าพเจ้าด้วยความรักความห่วงใยเสมอมา ขอขอบคุณ น้อง จันทนู วันนียางเจยมัว และ ทิดประเจิด ยางเจยมัว ทั้งสองพร้อมด้วยครอบครัว และญาติพี่น้องที่ได้ดูแลครอบครัวของข้าพเจ้ารวมทั้งคอยให้ความช่วยเหลือมาตลอดระยะเวลาการศึกษา โดยเฉพาะภรรยา นาง นวนอินดาว จ้งตัวมัว สำหรับความรัก ความห่วงใย ความเข้าใจเสมอมา เป็นแรงใจให้ต่อสู้และสนับสนุนการศึกษา

คุณค่าและประโยชน์ของการศึกษาครั้งนี้ขอมอบเป็นกตัญญูแด่ บุพการี บูรพาจารย์ และ ผู้มีพระคุณทุกท่าน ที่ทำให้แก่ผู้ทำงานนิพนธ์เป็นผู้มีการศึกษาและประสบความสำเร็จมาจนตราบเท่าทุกวันนี้

มัยสุข ยางเจยมัว

57910239: สาขาวิชา: เทคโนโลยีสารสนเทศ; วท.ม. (เทคโนโลยีสารสนเทศ)
คำสำคัญ: การออกแบบเครือข่ายคอมพิวเตอร์/ การติดตั้ง/ ตั้งค่า pfSense/
การวัดประสิทธิภาพของเครือข่าย

มัยสุข ยางเจยมัว: การออกแบบ และ การวัดประสิทธิภาพของระบบเครือข่าย: กรณีศึกษาวิทยาลัยพลศึกษานครหลวงเวียงจันทน์ (NETWORK DESIGN AND PERFORMANCE MEASUREMENT FOR PHYSICAL EDUCATION COLLEGE AT VIENTIANE)
คณะกรรมการควบคุมงานนิพนธ์: ณัฐนนท์ ลีลาตระกูล, Ph.D. 165 หน้า. ปี พ.ศ. 2559

ในงานนิพนธ์นี้ผู้ทำงานนิพนธ์ได้ออกแบบเครือข่ายคอมพิวเตอร์ให้กับวิทยาลัยพลศึกษา ตามความต้องการของวิทยาลัยพลศึกษา ซึ่งมี 3 ระบบเครือข่าย 1) ระบบเครือข่ายภายในอาคาร A, 2) ระบบเครือข่ายภายในอาคาร B, C, และ D, และ 3) ระบบเครือข่ายไร้สาย (Wi-Fi หรือ Wireless) (โดยอาคาร D มี ระบบ LAN สำหรับปฏิบัติการ 2 ห้อง) นอกจากนั้น ผู้ทำงานนิพนธ์ยังได้ ติดตั้ง pfSense, DHCP server, DNS, เครื่องแม่ข่าย Proxy, Captive Portal, เครื่องแม่ข่าย RADIUS, พร้อมกำหนดค่าจำกัดแบนด์วิดท์(Download และ Upload), บล็อก YouTube และ Facebook, ทำ NAT และ Port Forwarding, ติดตั้ง IPsec VPN, OpenVPN, ทำเว็บไซต์ของวิทยาลัยพลศึกษา และ ติดตั้งซอฟต์แวร์ป้องกันไวรัสให้แก่วิทยาลัย หลังจากการติดตั้ง และการตั้งค่าต่าง ๆ ในเครือข่าย ผู้ทำงานนิพนธ์ได้ทดสอบการวัดประสิทธิภาพของเครือข่าย และสำรวจความพึงพอใจของผู้ใช้จำนวน 37 คน พบว่าความพึงพอใจของอาจารย์ที่มีต่อสัญญาณ Wireless อยู่ในระดับกลาง และ การความพึงพอใจของอาจารย์ที่ใช้งานเครือข่ายคอมพิวเตอร์ที่เป็นระบบสาย (LAN)อยู่ในระดับดี

57910239: MAJOR: INFORMATION TECHNOLOGY; M.Sc.
(INFORMATION TECHNOLOGY)
KEYWORD: COMPUTER NETWORK DESIGN/INSTALLATION/
PFSENSE CONFIGURATION/NETWORK PERFORMANCE MEASUREMENT
MAISOUK YANGCHIAMOUA: NETWORK DESIGN AND PERFORMANCE
MEASUREMENT FOR PHYSICAL EDUCATION COLLEGE AT VIENTIANE.
ADVISORY COMMITTEE: NUTTHANON LEELATHAKUL, Ph.D. 165 P. 2016

In this thesis work, we design a computer network for a physical education college. According to the college, we design three network systems: 1) one for Building A 2) one for Building B, C and D 3) Wireless network. (There are 2 computer laboratories in Building D). In addition, we also install pfSense, DHCP server, DNS, Proxy server, captive portal, RADIUS server, configure download and upload bandwidth limitation, block YouTube and Facebook, NAT and port forwarding, install IPsec VPN, Open VPN, create website for the college of physical education, and install antivirus software. After installation the network system, we measure the performance of the network and conduct satisfaction survey with 37 users. We see that the satisfaction level of teachers for the wireless network is medium, and the satisfaction level of teachers who use the cable network (LAN) is good.

สารบัญ

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

สารบัญภาพ

สารบัญภาพ (ต่อ)

สารบัญภาพ (ต่อ)

ภาพที่ หน้า

สารบัญภาพ (ต่อ)

ภาพที่ หน้า

บทที่ 1
บทนำ

หลักการและเหตุผล

วิทยาลัยพลศึกษาเป็นวิทยาลัยของรัฐและเป็นวิทยาลัยพลศึกษาแห่งแรกของประเทศลาว ตั้งอยู่ที่ บ้านท่งบ้ง เมืองสีโคตระบอง นครหลวงเวียงจันทน์วิทยาลัยพลศึกษาได้เปิดการเรียนการสอน 4 หลัก สูตร ดังนี้

1. หลักสูตรระบบ 12+2 ชั้นสูงปกติ
2. หลักสูตรระบบ 12+4 ชั้นปริญญาตรีปกติ
3. หลักสูตรระบบ 11+3+2 ชั้นสูง ต่อเนื่อง
4. หลักสูตรระบบ 11+3+1+3 ชั้นปริญญาตรีต่อเนื่อง

เพื่อให้การเรียนการสอนมีประสิทธิภาพมากขึ้นวิทยาลัยพลศึกษา จึงได้มีการนำเอาอินเทอร์เน็ตเข้ามาใช้ในวิทยาลัยฯ เนื่องจากว่าประเทศลาวกำลังมีการพัฒนาและขยายตัวมากขึ้น อินเทอร์เน็ตจึงมีบทบาทสำคัญต่อการพัฒนาการศึกษาและเป็นสื่อสำหรับการเรียนการสอนรวมถึงวิธีการค้นหาข้อมูลการประมวลผล และ การเพิ่มศักยภาพด้านการสื่อสารและด้านความรู้จากแหล่งเรียนรู้ได้มากขึ้น

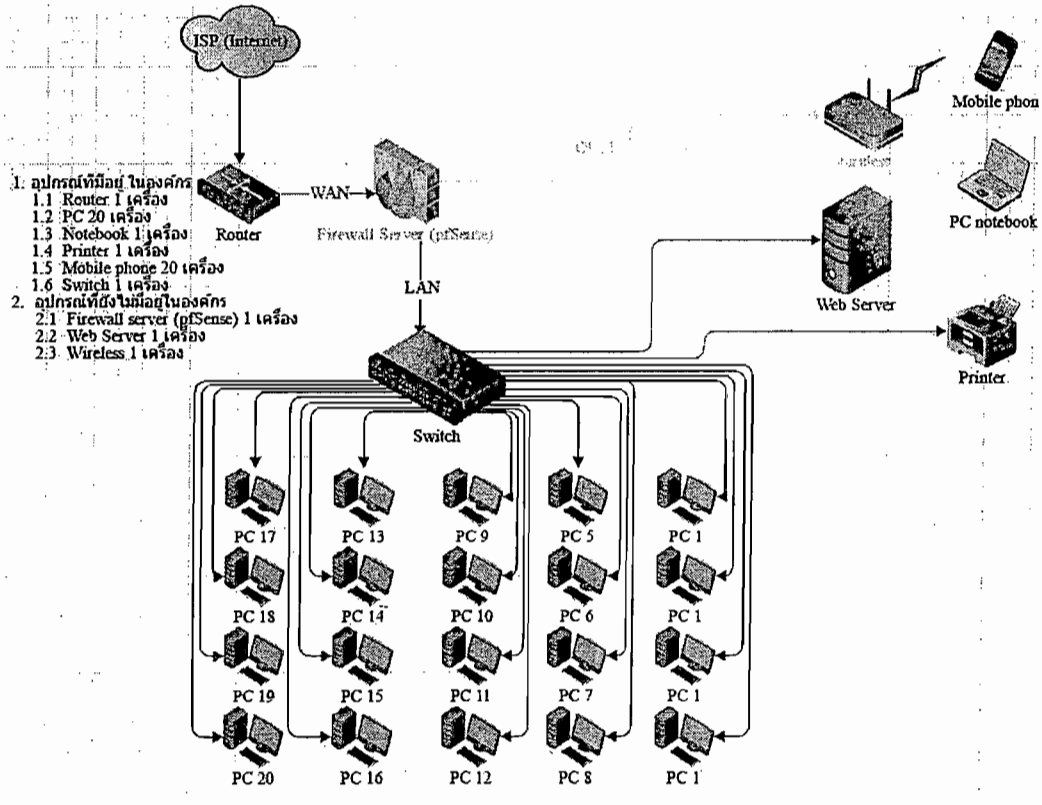
ในปัจจุบันการใช้อินเทอร์เน็ตยังมีปัญหาในการเข้าถึงข้อมูลต่างๆ ไม่ว่าจะเป็นฐานข้อมูล อีเมล์ เว็บไซต์ ไฟล์ภาพ เพลง ผู้ใช้งานอาจรู้เท่าไม่ถึงการณ์ อาจจะดาวน์โหลดไฟล์เหล่านั้นมา ซึ่งจะเป็นการสร้างปัญหาและนำความเสียหายมาสู่ในระบบเครือข่ายเช่น เป็นการกระทบต่อการทำงานของแอพพลิเคชั่นหลักของผู้ใช้งาน ทำให้การทำงานมีความล่าช้า หรือคอมพิวเตอร์ติดไวรัส ผลมาจากการเข้าใช้งานเว็บไซต์ที่ไม่มีความน่าเชื่อถือ จะนำความเสียหายมาให้ผู้ใช้งานอื่นๆ ด้วย เพราะฉะนั้นงานนิพนธ์นี้ได้เลือก pfSense มาเพื่อแก้ไขปัญหาที่กล่าวมา

งานนิพนธ์นี้ทำ pfSense ให้กับวิทยาลัยฯ เป็นกรณีศึกษา โดยที่วิทยาลัยฯ นี้การใช้ระบบไม่มีการติดตั้งระบบความปลอดภัยของระบบเครือข่ายภายในวิทยาลัยฯ อย่าง เช่น ความเสี่ยงต่อความปลอดภัยจากบุคคลภายนอกที่เข้ามาใช้งานระบบเครือข่าย ไม่มีการกำหนดการเข้าถึงข้อมูลไม่มีการจัดการและการควบคุมระบบในการเข้าใช้งานเว็บไซต์ต่าง ๆ ไม่มีการจัดเก็บ log file ของผู้ใช้งาน ปัญหาการดาวน์โหลดโปรแกรมหรือไฟล์ภาพ เพลงต่าง ๆ ที่ผิดกฎหมาย ทำให้สิ้นเปลืองแบนด์วิดท์ (Bandwidth) และในวิทยาลัยฯ ไม่มีการทำเว็บไซต์ให้บริการของวิทยาลัยฯ

วัตถุประสงค์

วัตถุประสงค์งานนิพนธ์นี้ จะมุ่งเน้นการจัดการและการบริหารโดยการสร้างความปลอดภัยให้กับระบบสารสนเทศภายในวิทยาลัยฯ โดยได้ออกแบบจัดทำระบบเครือข่ายและการบริหารระบบเพื่อสารสนเทศภายในวิทยาลัยฯ ให้สอดคล้องกับนโยบายของวิทยาลัยฯ โดยมีวัตถุประสงค์งานนิพนธ์ดังนี้

1. เพื่อให้ครู และ นักเรียนมีระบบเครือข่ายที่มีความปลอดภัยสำหรับใช้ในการเรียนการสอน
2. เพื่อการปรับปรุงนโยบายทางด้านความปลอดภัยให้สอดคล้องกับการใช้งานภายในวิทยาลัยฯ
3. สามารถควบคุมการทำงานของเครื่องคอมพิวเตอร์ที่อยู่บนเครือข่ายได้
4. สามารถแลกเปลี่ยนข้อมูลกันได้ เช่น การโอนย้ายแฟ้มข้อมูลจากคอมพิวเตอร์เครื่องหนึ่ง ไปยังอีกเครื่องหนึ่งรวมถึงสามารถส่งข่าวสารไปมาระหว่างคอมพิวเตอร์ได้



ภาพที่ 1-1 รายละเอียดระบบเครือข่าย

ประโยชน์ที่คาดว่าจะได้รับ

ในงานนิพนธ์นี้ผู้จัดทำงานนิพนธ์ได้ศึกษาและตระหนักถึงการจัดการ และ การบริหารความปลอดภัยของข้อมูลภายในวิทยาลัยฯ ที่มีความสำคัญในการดำเนินการศึกษาและให้ผู้ใช้งานภายในสถาบันการศึกษารู้ถึงความปลอดภัยในการใช้งานระบบสารสนเทศ โดยการนำเอาเครื่องมือหรือซอฟต์แวร์การรักษาความปลอดภัยมาใช้ภายในวิทยาลัยฯ พร้อมทั้งรู้วิธีการในการวางแผนเพื่อดูแลระบบสารสนเทศภายในวิทยาลัยฯ ให้มีประสิทธิภาพต่อไป ประโยชน์ที่คาดว่าจะได้รับมีดังนี้:

1. วิทยาลัยพลศึกษามีเว็บไซต์เป็นของตนเองในการให้บริการ
2. การใช้อินเทอร์เน็ตมีความสะดวกมากขึ้นอย่าง เช่น ผู้ใช้สามารถแลกเปลี่ยนข้อมูลกับเพื่อนร่วมงานที่อยู่คนละที่ ได้อย่างสะดวก และ รวดเร็วประกอบกับปริมาณการใช้ (Traffic) สามารถนำความรู้ที่ได้รับไปให้บริการให้คำปรึกษาและติดตั้งระบบเก็บข้อมูลระบบเครือข่าย
3. บุคลากรที่เกี่ยวข้องมีความรู้ความเข้าใจในกรอบการทำงานและกระบวนการของ pfSense กับการบริหารจัดการเทคโนโลยีสารสนเทศให้ปลอดภัย
4. สำหรับเป็นแบบอย่างและเป็นแนวทางในการนำ pfSense ไปใช้กับบริการเทคโนโลยีสารสนเทศอื่น ๆ ที่มีในองค์กร

ขอบเขตของงานนิพนธ์

งานนิพนธ์นี้มุ่งเน้นการจัดการ และ การบริหาร โดยสร้างความปลอดภัยให้กับระบบสารสนเทศภายในวิทยาลัยฯ ตามวัตถุประสงค์ข้างต้น ผู้จัดทำงานนิพนธ์ได้ออกแบบระบบรักษาความปลอดภัย และ บริหารระบบสารสนเทศภายในวิทยาลัยฯ ให้สอดคล้องกับนโยบายของวิทยาลัยฯ โดยมีขอบเขตดังนี้

1. ติดตั้ง pfSense
2. การกำหนดค่า pfSense โดยใช้ Wizard
3. การตั้งค่า DHCP server, DNS servers
4. การตั้งค่าเครื่องแม่ข่าย Proxy บริการเก็บแคชของข้อมูลเว็บไซต์
5. การตั้งค่า Captive Portal Network บริการหน้าเว็บไซต์เริ่มต้นเมื่อเข้าสู่เครือข่าย LAN และ Wireless LAN และ ตั้งเวลาการออก Internet ให้เวลางานไม่ให้ใช้ Internet
6. การตั้งค่าเครื่องแม่ข่าย RADIUS บริการกำหนดรายชื่อผู้ใช้ในการเข้าถึงเครือข่าย

7. ตั้งค่า Log Server บริการเก็บประวัติการใช้งานเครือข่าย
8. การตั้งค่าจำกัดแบนด์วิดท์ Download และ Upload
9. การตั้งการค่าบล็อก YouTube และ Facebook ใน pfSense บริการกำหนดสิทธิ์การเข้าถึงเว็บไซต์และบริการต่างๆ
10. การตั้งค่า NAT และ Port Forwarding เพื่อส่งข้อมูลไปยังเครื่องแม่ข่าย pfSense และ web บริการ IP ภายในองค์กร
11. การตั้งค่า Dynamic DNS บริการแปลชื่อโดเมน
12. การสร้างกฎไฟร์วอลล์ (Rule: WAN และ LAN): บริการไฟร์วอลล์
13. การตั้งค่า Multi-WAN Load Balancing: บริการจัดการความคับคั่งของเครือข่าย
14. การตั้งค่า IPsec VPN บริการการเพิ่มความปลอดภัยของการส่งผ่านข้อมูล
15. การติดตั้ง และ ตั้งค่า OpenVPN บริการเชื่อมต่อเครือข่ายเสมือน
16. ติดตั้ง และ การตั้งค่า Organization Website: เว็บไซต์ขององค์กร
17. บริการป้องกัน Antivirus

บทที่ 2
พื้นฐานและทฤษฎีที่เกี่ยวข้อง

ผู้จัดทำงานนิพนธ์เล็งเห็นความสำคัญการบริหาร และ การจัดการระบบสารสนเทศในแต่ละสถาบัน ไม่ว่าจะเป็นเรื่องการใช้ระบบฐานข้อมูล การใช้อินเทอร์เน็ตภายในสถาบัน ซึ่งจะมักมีประเด็นสำคัญหลายประเด็น เช่น การเข้าใช้งานภายในเครือข่ายอินเทอร์เน็ต การเข้าใช้งานอีเมล์และเว็บไซต์ที่ไม่มีความปลอดภัย ซึ่งส่งผลร้ายให้ระบบเครือข่ายภายในสถาบัน ดังนั้นระบบสารสนเทศจำเป็นจะ ต้องมีการรักษาความปลอดภัยภายในเครือข่ายจากการบุกรุกจากภายนอกและพร้อมที่จะรับมือกับภัยคุกคามต่าง ๆ โดยงานนิพนธ์นี้ได้ใช้ pfSense ช่วยจัดการในประเด็นต่าง ๆ

ทำความรู้จักกับ pfSense

(นภดล สุขศรี, 2012). คู่มือติดตั้ง และการใช้งาน pfSense ปี พ.ศ. 2555 ได้กล่าวเกี่ยวกับ pfSense ดังนี้

"pfSense ระบบปฏิบัติการ Open source ที่มีประสิทธิภาพ และคุ้มค่า โดยเฉพาะในด้านการทำหน้าที่เป็นเครื่องผู้ให้บริการ (Server) สำหรับบริการงานต่าง ๆ

pfSense ถูกพัฒนาต่อยอดมาจาก monowall โดยที่ pfSense จะมีตัวเลือกการติดตั้งและการตั้งค่าที่ยืดหยุ่นมากกว่า monowall โดย pfSense รวมเอาคุณสมบัติและฟีเจอร์ที่สำคัญ ๆ ของไฟร์วอลล์ที่ใช้ในเชิงธุรกิจมาไว้ด้วยกันเหมาะสำหรับใช้เป็นไฟร์วอลล์ (firewall) อุปกรณ์จัดเส้นทาง (Router) เกตเวย์ (Gateway), เครื่องผู้ให้บริการ Proxy โดยมี Free BSD ยูนิกซ์ (Unix) เป็นพื้นฐานหลักในการพัฒนา"

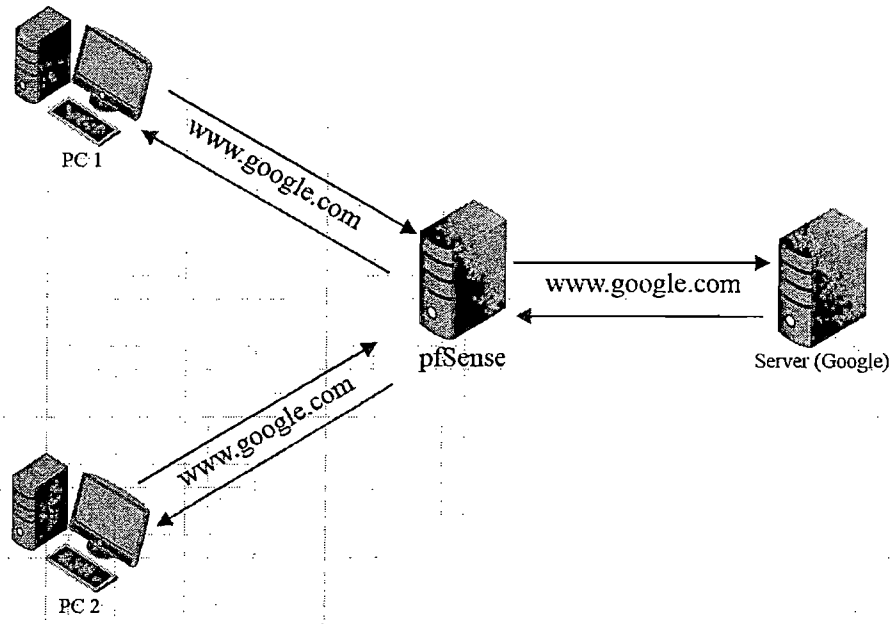
การจัดการและบริหารระบบเครือข่ายภายในสถาบัน

การจัดการและบริหารระบบเครือข่ายภายในสถาบันให้มีประสิทธิภาพดีจำต้องมีการวางแผน การออกแบบ การติดตั้ง การตั้งค่าในเรื่องของระบบความปลอดภัย และ การจัดการส่วนประกอบต่าง ๆ ของเครือข่ายรวมไปถึงพนักงานไอที และ อุปกรณ์ต่าง ๆ ที่เชื่อมต่อเข้ากับระบบเพื่อให้การบริหารมีประสิทธิภาพสูงสุดโดยทั่วไปเครือข่ายภายในสถาบันประกอบไปด้วยส่วนประกอบต่าง ๆ ดังตัวอย่างต่อไปนี้

1. เครื่องผู้ให้บริการ Proxy: บริการเก็บข้อมูลเว็บไซต์ไว้ในแคช (Cache)

ให้บริการเก็บข้อมูลหรือจำข้อมูลของเว็บไซต์และเป็นตัวกลางที่ให้บริการระหว่างเครื่องเว็บแม่ข่ายและไคลเอนต์ ดังภาพที่ 2-1 เมื่อ PC-1 ต้องการเข้าใช้งานเว็บไซต์ Google.com PC-1 ส่งคำร้องขอหน้าเว็บไปยังเครื่องผู้ให้บริการ Proxy ถ้าหากว่าเป็นการร้องขอหน้าเว็บที่เครื่อง

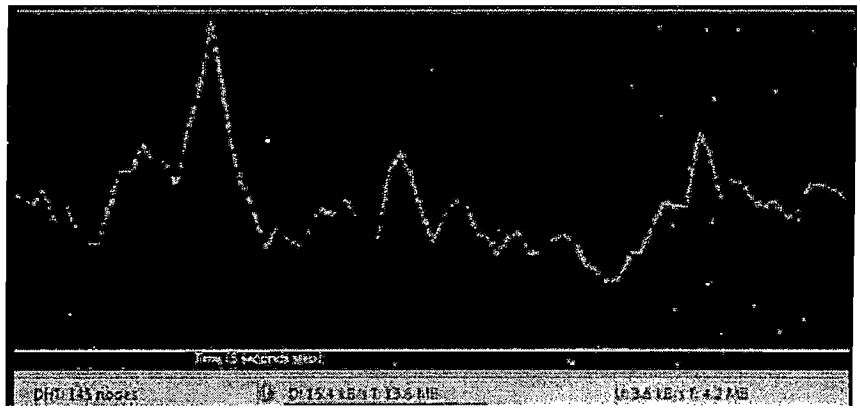
ผู้ให้บริการ Proxy ยังไม่มีไว้การเก็บหรือจำไว้เครื่องผู้ให้บริการ Proxy ก็จะถามไปยังเครื่อง ผู้ให้บริการเว็บพอเครื่องผู้ให้บริการ Proxy ได้รับข้อมูลหน้าเว็บจากเครื่องผู้ให้บริการเว็บแล้วก็จะจำหน้าเว็บนั้นไว้แล้วส่งข้อมูลดังกล่าวต่อไปที่ PC-1 ตามที่ร้องขอมา เมื่อ PC-2 เข้าใช้งานหน้าเว็บเดิม เครื่องผู้ให้บริการ Proxy ก็ไปนำเอาหน้าเว็บที่เก็บไว้ในแคชมาส่งให้ PC-2 ได้เลย โดยไม่ต้องร้องขอไปยังเครื่องผู้ให้ บริการเว็บอีกครั้ง



ภาพที่ 2-1 กระบวนการทำงานของเครื่องผู้ให้บริการ Proxy

2. Traffic Shaper บริการจัดการช่องสัญญาณสำหรับบริการที่แตกต่างกัน

Traffic Shaper คือ เครื่องมือควบคุมปริมาณการใช้เครือข่าย เช่น กำหนดปริมาณการ upload และ download ของแต่ละผู้ใช้ ภาพที่ 2-2 แสดงถึงปริมาณข้อมูลก่อน และหลังการใช้ Traffic Shaper

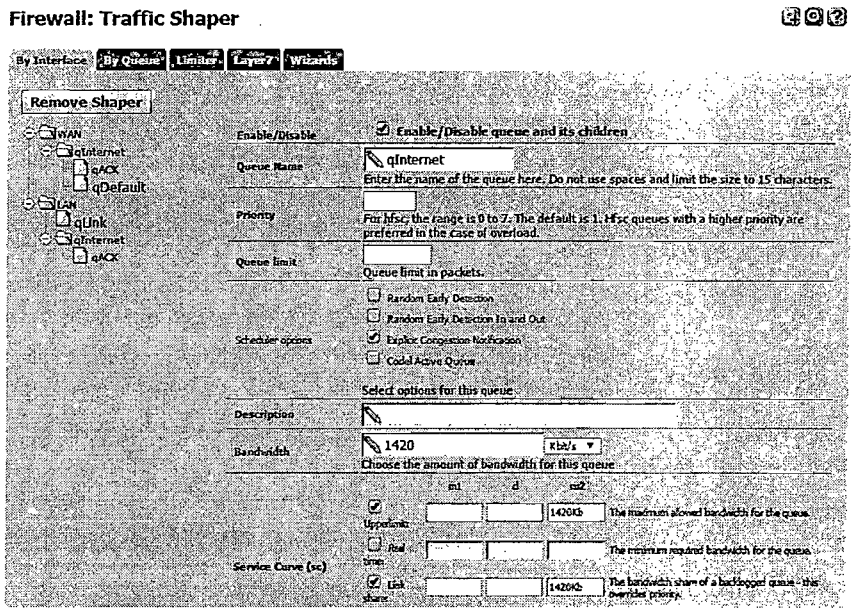


ภาพที่ 2-2 กราฟเปรียบเทียบข้อมูลปริมาณการใช้เครือข่ายก่อนและหลังใช้ Traffic shaper

(ที่มา: youtube.com/watch?v=1QjWJCimXlE)

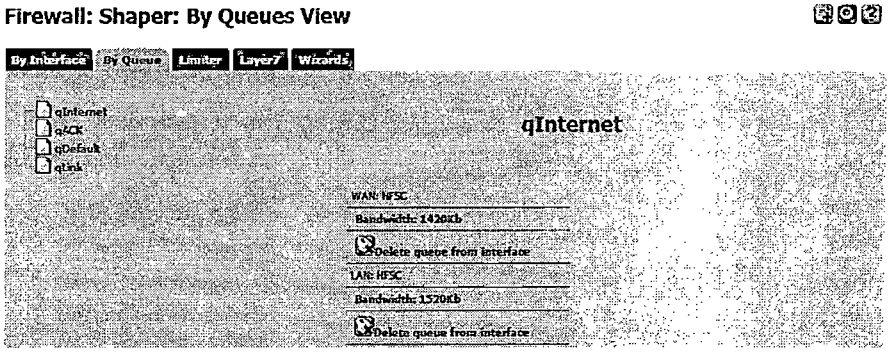
ผู้ดูแลระบบสามารถใช้ Traffic Shaper ได้ 4 รูปแบบดังต่อไปนี้

1. ใช้ Traffic Shaper แบบ “By Interface” เป็นการแสดงกฎของแต่ละ Interface (เช่น WAN และ LAN) ดังภาพที่ 2-3 ด้านซ้ายมือแสดงกฎทั้งหมดของ Interface (WAN และ LAN) ส่วนด้านขวามือแสดงรายละเอียดของกฎ qACK ที่ Interface WAN ใน Traffic Shaper และสามารถยกเลิกการกำหนด Traffic Shaper ที่ปุ่ม Remove shaper



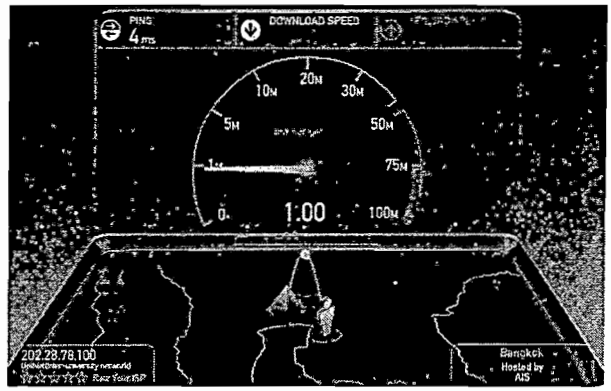
ภาพที่ 2-3 การแสดงกฎใน Interface (WAN LAN)

2. ใช้ “Traffic Shaper”แบบ“By Queue” เป็นการแสดงกฎของแต่ละคิว ดังภาพที่ 2-4 แสดงกฎของแต่ละคิวที่กำหนดใน Traffic Shaper



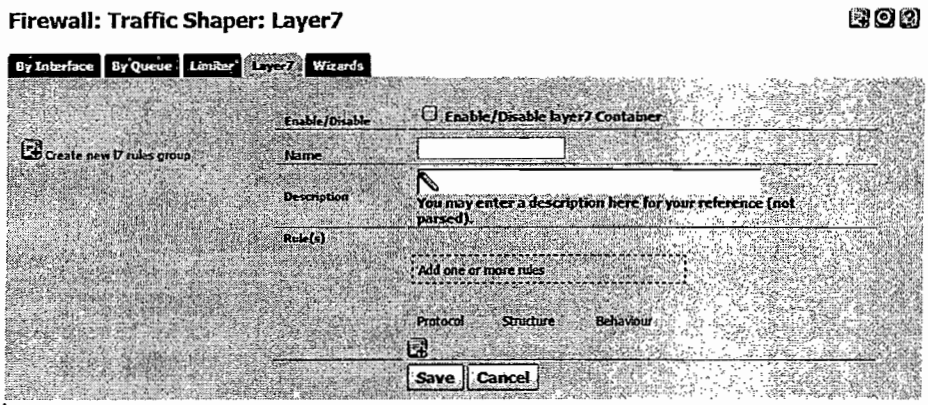
ภาพที่ 2-4 คิวของแต่ละกฎที่กำหนดใน Traffic Shaper

3. ใช้ “Limiter” เพื่อจำกัดแบนด์วิดท์ (จำกัดความเร็วทั้งการ upload และ การ download) pfSense ช่วยผู้ดูแลระบบโดยให้บริการเฝ้าใช้แบนด์วิดท์ และ ให้ผู้ดูแลระบบจำกัดการใช้แบนด์วิดท์ได้ด้วย ภาพที่ 2-5 แสดงผลการวัดความเร็วของอินเทอร์เน็ตโดยใช้เครื่องมือได้จากเว็บ www.Speedtest.net



ภาพที่ 2-5 กระบวนการวัดความเร็วของ Bandwidth

4. ใช้ “Layer7” เป็นการสร้างกฎใหม่ที่เกี่ยวกับ Application และสามารถ upload file รูปแบบการรับส่งข้อมูลของ Application เพื่อสร้างกฎได้ ดังภาพที่ 2-6 เป็นตัวอย่างการสร้างกฎในกลุ่ม layer 7 ใน Traffic shaper



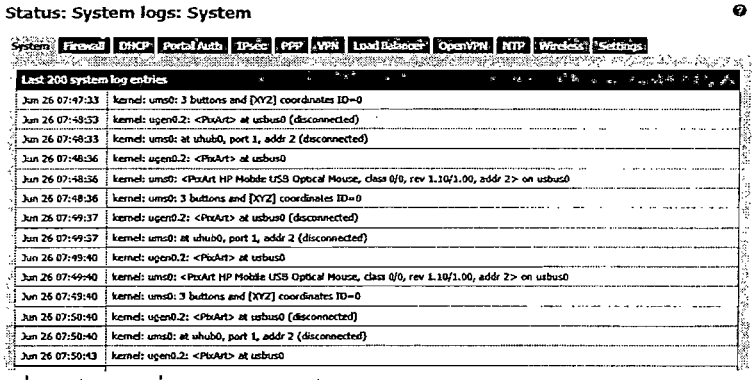
ภาพที่ 2-6 สร้างกฎในกลุ่ม layer 7 ใน Traffic shaper

3. เครื่องผู้ให้บริการ Radius กำหนดรายชื่อผู้ใช้ที่มีสิทธิ์ในการเข้าถึงเครือข่าย

เครื่องผู้ให้บริการ Radius ให้บริการการพิสูจน์ตัวตน เพื่อเป็นการควบคุม และ ตรวจสอบสิทธิ์การเข้าใช้อินเทอร์เน็ตของผู้ใช้ให้มีประสิทธิภาพ เช่น การใช้งานของผู้ใช้งานเป็นจำนวนชั่วโมง และ ตรวจสอบผู้ใช้ที่กำลังใช้งานเครือข่ายอยู่

4. เครื่องผู้ให้บริการล็อก (log) บริการเก็บประวัติการใช้งานเครือข่าย

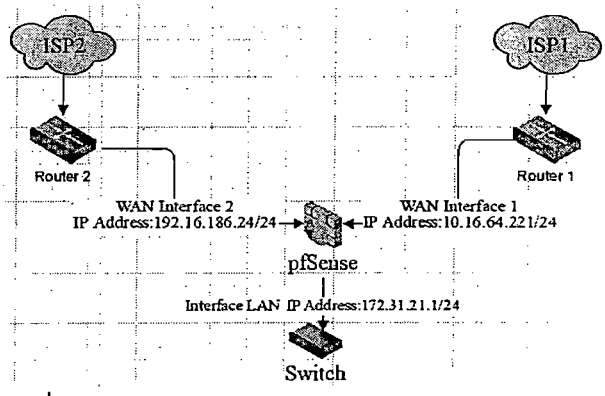
เครื่องผู้ให้บริการล็อกเป็นระบบที่ทำหน้าที่จัดเก็บและรักษาข้อมูลการใช้งานระบบเครือข่ายส่วนต่าง ๆ ดังภาพที่ 2-7 ที่แสดงถึงรายละเอียดข้อมูลการใช้ระบบ (แสดงรายการที่ระบบจัดเก็บไว้ 200 รายการสุดท้าย) และ แถบด้านบนใช้สำหรับแสดงบล็อกประเภทต่าง ๆ



ภาพที่ 2-7 รายการที่ถูกเก็บในเครื่องผู้ให้บริการล็อก

5. การกระจายภาระงานให้สมดุล (Load balance): บริการจัดการความคับคั่งของเครือข่าย

เพื่อเป็นการจัดการระบบเครือข่ายให้มีประสิทธิภาพสูง และ สามารถรองรับปริมาณของผู้ใช้ งานให้ได้จำนวนมากขึ้น ผู้ดูแลระบบจึงกระจายภาระงานให้สมดุล (Load balance) ตามสิทธิ์ที่กำหนดไว้ ดังภาพที่ 2-8 แสดงถึงการเชื่อมต่อสำหรับการทำ Load Balancing

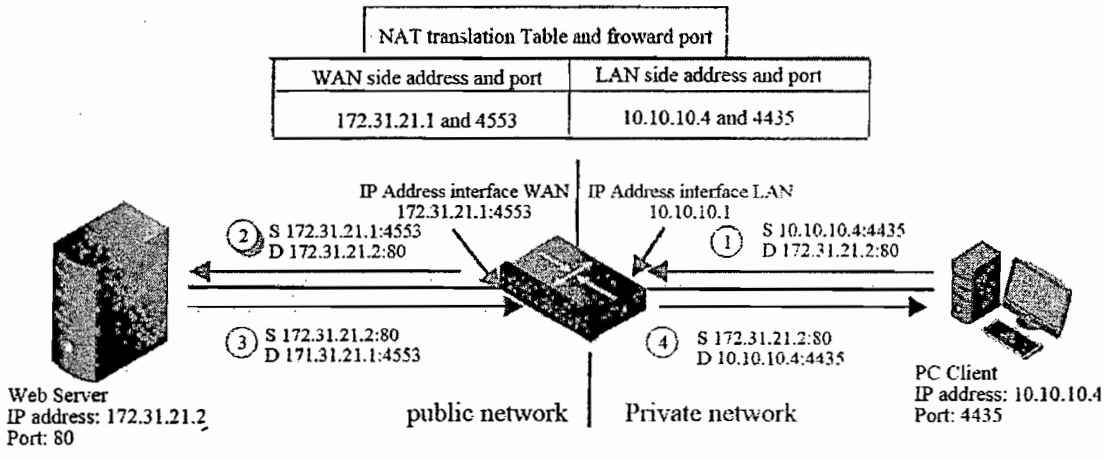


ภาพที่ 2-8 แสดงถึงการเชื่อมต่อสำหรับการทำ Load Balancing ใน pfSense

6. การส่งต่อพอร์ตที่ NAT (NAT Port Forwarding)

การส่งต่อพอร์ตที่ NAT คือ การกำหนดเส้นทางของข้อมูลที่ติดต่อเข้ามายังอุปกรณ์จัดเส้นทาง (Router) ที่มี NAT ทำงานอยู่ โดยหลังจากกำหนดเส้นทางแล้ว เมื่อข้อมูลจากภายนอกมาถึง NAT จะให้ส่งต่อข้อมูลไปยังเครื่องที่อยู่หลังอุปกรณ์จัดเส้นทาง โดยอาศัยตาราง NAT ที่ช่วยแปลง

ไอพีภายนอก (Public IP address) ไปเป็นไอพีภายในระบบ (Private IP address) ส่วนในกรณีที่เครื่องที่อยู่หลังอุปกรณ์จัดเส้นทางต้องการส่งข้อมูลไปยังเครื่องภายนอก เมื่อข้อมูลจากภายในมาถึง NAT จะแปลงไอพีภายในระบบไปเป็นไอพีภายนอกระบบ ภาพที่ 2-9 แสดงถึงขั้นตอนในการทำงานของ NAT เมื่อไคลเอนต์ร้องขอข้อมูลไปยังเครื่องผู้ให้บริการเว็บ ไคลเอนต์ส่งข้อมูลไปยังหมายเลขไอพีปลายทางซึ่งเป็นของเว็บเครื่องผู้ให้บริการเว็บ โดยข้อมูลมีหมายเลขไอพีและพอร์ตต้นทาง (เป็นหมายเลขไอพีภายใน) เป็นของไคลเอนต์ พอข้อมูลผ่านอุปกรณ์จัดเส้นทางซึ่งมี NAT ทำงานอยู่ NAT จะอาศัยตาราง NAT เพื่อแปลงไอพีภายในระบบไปเป็นไอพีภายนอกระบบ ก่อนที่ NAT จะส่งข้อมูลไปยังเครื่องผู้ให้บริการเว็บ (ตอนนี้ ข้อมูลมีที่อยู่ปลายทางเป็นไอพีและพอร์ตของเครื่องผู้ให้บริการเว็บ และ มีที่อยู่ต้นทางที่มีไอพี และพอร์ตของอุปกรณ์จัดเส้นทาง) จากนั้นเมื่อเครื่องผู้ให้บริการเว็บได้รับข้อมูลดังกล่าวแล้ว เครื่องผู้ให้บริการเว็บก็จะส่งข้อมูลกลับไปให้ไคลเอนต์ โดยข้อมูลดังกล่าวมีหมายเลขไอพีปลายทาง และ พอร์ตที่เป็นของอุปกรณ์จัดเส้นทาง และมีหมายเลขไอพีและพอร์ตต้นทางเป็นของเครื่องผู้ให้บริการเว็บ พอข้อมูลผ่านอุปกรณ์จัดเส้นทาง NAT ที่อุปกรณ์จัดเส้นทางจะแปลงไอพีปลายทางที่เป็นที่อยู่ภายนอกระบบไปเป็นไอพีภายในระบบ หลังจากที่แปลงที่อยู่แล้วอุปกรณ์จัดเส้นทางก็ส่งข้อมูลต่อไปให้ ไคลเอนต์ โดยหมายเลขไอพีปลายทาง เป็นหมายเลขไอพีและพอร์ตของ ไคลเอนต์ และ หมายเลขไอพีต้นทางเป็นหมายเลขไอพีและพอร์ตของเครื่องผู้ให้บริการเว็บ

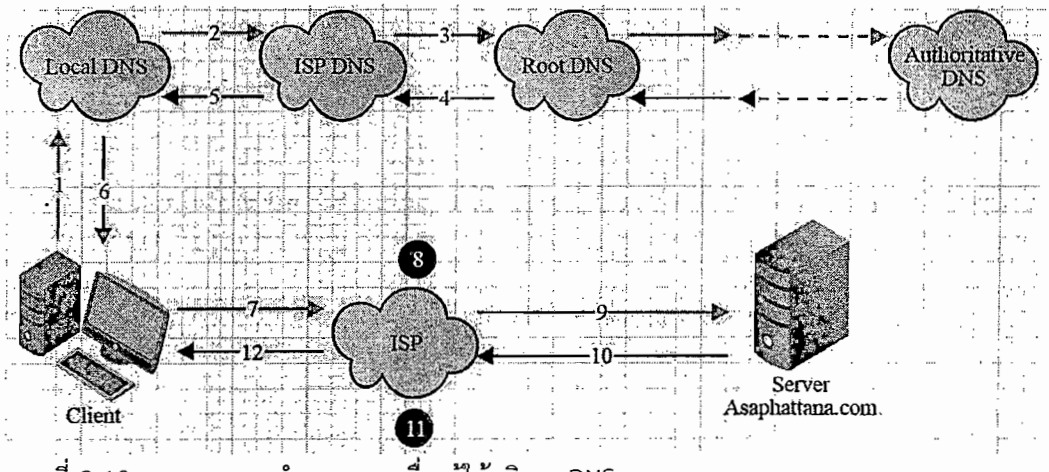


ภาพที่ 2-9 ขั้นตอนในการทำงานของ NAT

7. เครื่องผู้ให้บริการ DNS: บริการแปลชื่อโดเมน

เครื่องผู้ให้บริการ DNS ย่อมาจาก Domain Name System ซึ่งให้บริการแปลงชื่อโดเมนเป็นหมายเลขไอพี เพราะว่าหมายเลขไอพีจำได้ยาก ด้วยเหตุนี้คนจึงเลือกที่จะจำชื่อโดเมนแทนเพราะจดจำได้ง่ายกว่า ระบบ DNS จะช่วยบริการแปลงชื่อโดเมนให้ไปเป็นเลขไอพี ภาพที่ 2-10 แสดงกระบวนการทำงานของ DNS เครื่องผู้ให้บริการ โดยมีรายละเอียดดังต่อไปนี้: 1. ไคลเอนต์ส่งข้อมูลไป

ถามผู้ให้บริการท้องถิ่น (Local DNS) ว่า asaphattana.com มีหมายเลขไอพีอะไร 2. ถ้าผู้ให้บริการท้องถิ่น NDS ไม่รู้หมายเลขไอพีของ assaphattana.com ผู้ให้บริการท้องถิ่น DNS จะถามต่อไปยังเครื่องผู้ให้บริการ DNS ของ ISP ว่า asaphattana.com มีไอพีอะไร 3. ถ้าเครื่องผู้ให้บริการ DNS ของ ISP ไม่รู้หมายเลขไอพีที่ไคลเอนต์ร้องขอ มันจะต้องส่งคำร้องขอไปยังเครื่องผู้ให้บริการ DNS ที่เป็น Root, TLD, และ Authoritative DNS ตามลำดับ จนกว่าจะได้รับหมายเลขไอพีที่ต้องการ 4. เมื่อเครื่องผู้ให้บริการ Root DNS ได้รับหมายเลขไอพี ก็ส่งหมายเลขไอพีของ asaphattana.com ไปยัง DNS ของ ISP 5-6. พอเครื่องผู้ให้บริการ DNS ของ ISP ได้รับหมายเลขไอพี หมายเลขไอพีก็จะถูกส่งต่อไปยัง Local DNS ซึ่งจะส่งหมายเลขไอพีต่อไปยังไคลเอนต์ 7-8-9. พอไคลเอนต์ได้รับหมายเลขไอพีของ asaphattana.com มาแล้วก็ทำการเชื่อมต่อไปยังหมายเลขไอพีที่ได้รับมา 10-11-12. พอ เครื่องผู้ให้บริการเว็บ ได้รับร้องข้อแล้ว เครื่องผู้ให้บริการเว็บก็ส่งหน้าเว็บกลับไปยังไคลเอนต์เป็นทอด ๆ



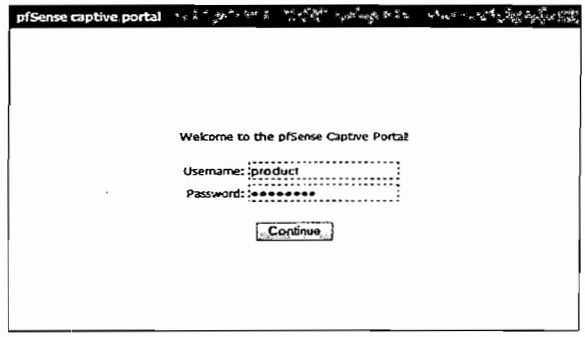
ภาพที่ 2-10 กระบวนการทำงานของเครื่องผู้ให้บริการ DNS

8. บริการแปลชื่อโดเมนแบบพลวัต Dynamic DNS

Dynamic Domain Name system คือ ระบบที่ให้บริการการแปลงชื่อโดเมนเป็นหมายเลขไอพี ซึ่งต่างจากระบบ DNS ทั่วไปที่หมายเลขไอพีของเครื่องผู้ให้บริการต้องคงที่ หากหมาย เลขไอพีมีการเปลี่ยนแปลง ระบบ DNS ทั่วไปจะไม่สามารถแปลงชื่อโดเมนให้เป็นเลขไอพีใหม่ได้ โดยอัตโนมัติในขณะที่ Dynamic DNS สามารถทำได้

9. Captive portal

Captive portal เป็นการกำหนดผู้สิทธิ์ให้ผู้ใช้เข้าถึงระบบ และ ให้บริการยืนยันตัวตน แก่ผู้ที่จะเข้ามาใช้งานระบบในเครือข่าย ดังภาพที่ 2-11 ก่อนที่ผู้ใช้จะเข้าใช้งานอินเทอร์เน็ต ผู้ใช้ต้องป้อนชื่อผู้ใช้ และ รหัสผ่านเพื่อยืนยันตัวตนก่อน



ภาพที่ 2-11 หน้าสำหรับล็อกอินเข้าใช้อินเทอร์เน็ตในระบบ Captive portal ของ pfSense

10. บล็อกเว็บไซต์ (Block Facebook)

เว็บไซต์ Facebook เป็นเว็บไซต์ที่ใช้พูดคุย สื่อสาร ซึ่งกำลังเป็นที่นิยมในกลุ่มวัยรุ่น ดังนั้นเพื่อป้องกันไม่ให้นักเรียนและบุคลากรใช้ Facebook ในเวลาเรียน ผู้ดูแลระบบอาจต้องบล็อกเว็บไซต์ไม่ให้ผู้ใช้บางคนถึงได้ (ขณะเดียวกัน ผู้ใช้บางประเภทก็อาจไม่ถูกบล็อก)

การเพิ่มความปลอดภัยของเครือข่าย

การใช้อินเทอร์เน็ตสามารถส่งผลกระทบต่อเครือข่ายได้ เช่น ไฟล์ที่ส่งติดไวรัสทำให้ส่งผลกระทบต่อความปลอดภัยของเครื่องคอมพิวเตอร์ และ เครือข่ายโปรแกรมไวรัสในเครื่องคอมพิวเตอร์อาจส่งข้อมูลข้ามเครือข่ายเป็นจำนวนมากจนทำให้เครือข่ายต้องหยุดทำงาน เพราะฉะนั้นในระบบเครือข่ายจึงต้องมีระบบการป้องกันความปลอดภัย

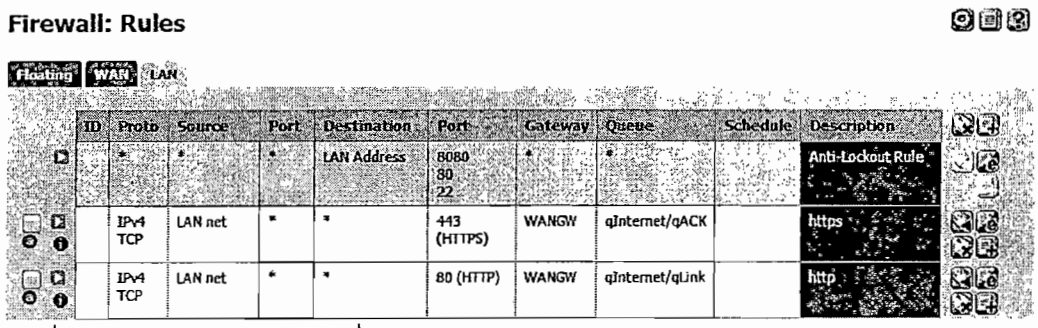
1. เครื่องผู้ให้บริการไฟร์วอลล์ (Firewall) กำหนดกฎสำหรับ interface (WAN, LAN, Wireless)

ไฟร์วอลล์เป็นเครื่องมือที่สามารถสร้างกฎ เป็นเสมือนกำแพงหน้าบ้านที่สำคัญที่สุดของระบบเครือข่าย ทำหน้าที่ป้องกันการโจมตีจากบุคคลภายนอก และ กำหนดสิทธิ์การเข้าใช้ระบบเครือข่าย ภาพที่ 2-12 แสดงกฎไฟร์วอลล์ที่ Interface LAN ซึ่งมีรายละเอียดดังนี้

1. Interface LAN อนุญาตให้มีการส่งข้อมูลของทุกโปรโตคอล โดยเครื่องผู้ส่งจะมีหมายเลขไอพีใดก็ได้และมี port ใดก็ได้ แต่เครื่องผู้รับจะต้องอยู่ภายใน LAN และ รับข้อมูลที่พอร์ตหมายเลข 8080, 80, หรือ 22 เท่านั้น ส่วน Gateway จะเป็นหมายเลขไอพีอะไรก็ได้และทุกคิวอะไรก็ได้

2. Interface LAN อนุญาตให้มีการส่งข้อมูลของทุกโปรโตคอล (IPv4 TCP) โดยเครื่องผู้ส่งจะมีหมายเลขไอพีใน LAN และมี port ใดก็ได้ เครื่องผู้รับจะอยู่ที่ไหนก็ได้ และ รับข้อมูลที่พอร์ตหมายเลข 443 (HTTPS) เท่านั้น ส่วน Gateway จะเป็น WANGW และ คิว เป็น qInternet/qACK

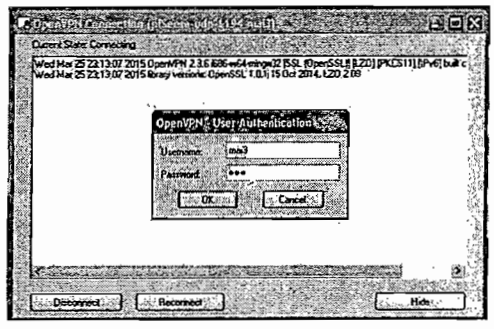
3. Interface LAN อนุญาตให้มีการส่งข้อมูลของทุกโปรโตคอล (IPv4 TCP) โดยเครื่องผู้ส่งจะมีหมายเลขไอพีใน LAN และมี port ใดก็ได้ เครื่องผู้รับจะอยู่ที่ไหนก็ได้ และ รับข้อมูลที่พอร์ตหมายเลข 80 (HTTP) เท่านั้น ส่วน Gateway จะเป็น WANGW และ คิวเป็น qInternet/qLink



ภาพที่ 2-12 ตัวอย่างกฎไฟร์วอลล์ที่ Interface ต่าง ๆ

2. OpenVPN บริการเครื่องภายนอกเครือข่ายเชื่อมต่อกับเครือข่ายขององค์กร

เป็นการให้ผู้ใช้งานสามารถติดต่อเข้าใช้งานเครือข่ายของสถาบัน ในเวลาผู้ใช้ออกไปทำงานนอกสถานที่ได้ เช่น พนักงานวิชาการ หรือ ฝ่ายไอทีที่ออกไปทำงานนอกสถานที่สามารถเชื่อมต่อเข้าเครือข่ายของสถาบันเพื่อเรียกดูข้อมูลของสถาบัน โดยผู้ใช้เปิด VPN ไคลเอนต์เพื่อเชื่อมต่อกับระบบเครือข่ายของสถาบัน ทำให้เกิดความสะดวกและปลอดภัยในการทำงาน ภาพที่ 2-13 แสดงถึงการพิสูจน์ตัวตนของผู้ใช้โดยมีการระบุชื่อผู้ใช้และรหัสผ่านที่ไคลเอนต์ ของ OpenVPN



ภาพที่ 2-13 การระบุชื่อผู้ใช้และรหัสผ่านที่ไคลเอนต์ OpenVPN

3. IPSec VPN

IPSec VPN ย่อมาจาก Internet Protocol security เป็นโปรโตคอลสำหรับการส่งข้อมูลผ่านอินเทอร์เน็ตอย่างปลอดภัย โดยการพิสูจน์ตัวตน และ การเข้ารหัสของผู้ใช้ในขณะที่ทำการติดต่อ นอกจากนี้โปรโตคอลยังเป็นผู้ตรวจสอบความถูกต้อง และการรักษาความปลอดภัยของข้อมูล เช่น การเชื่อมต่อระหว่าง ไคลเอนต์ OpenVPN และ OpenVPN จะมี IPsec เป็นตัวกลางในการสื่อสารข้อมูลของไคลเอนต์ OpenVPN และ OpenVPN

บทที่ 3

การดำเนินงาน

งานนิพนธ์นี้มุ่งเน้นการจัดการ การบริหาร และ ความปลอดภัยให้กับระบบสารสนเทศภายในวิทยาลัยฯ โดยมีวิธีและขั้นตอนการดำเนินงานดังต่อไปนี้

- การออกแบบเครือข่ายในสถานที่ทดลอง
- การศึกษา ติดตั้ง และ ตั้งค่า pfSense ในสถานที่ทดลอง
- การออกแบบเครือข่ายในสถานที่จริง
- การติดตั้งและตั้งค่า pfSense ในสถานที่จริง

การออกแบบเครือข่ายในสถานที่ทดลอง

ผู้ทำงานนิพนธ์ได้มีการออกแบบระบบเครือข่ายในสถานที่ทดลอง เพื่อทดสอบการติดตั้งและการเข้าใช้งาน ก่อนการติดตั้งที่สถานที่จริงที่ประเทศสาธารณรัฐประชาธิปไตยประชาชนลาว ดังรายละเอียดในตารางที่ 3-1

ตารางที่ 3-1 Software และ Hardware ที่ใช้ในสถานที่ทดลอง

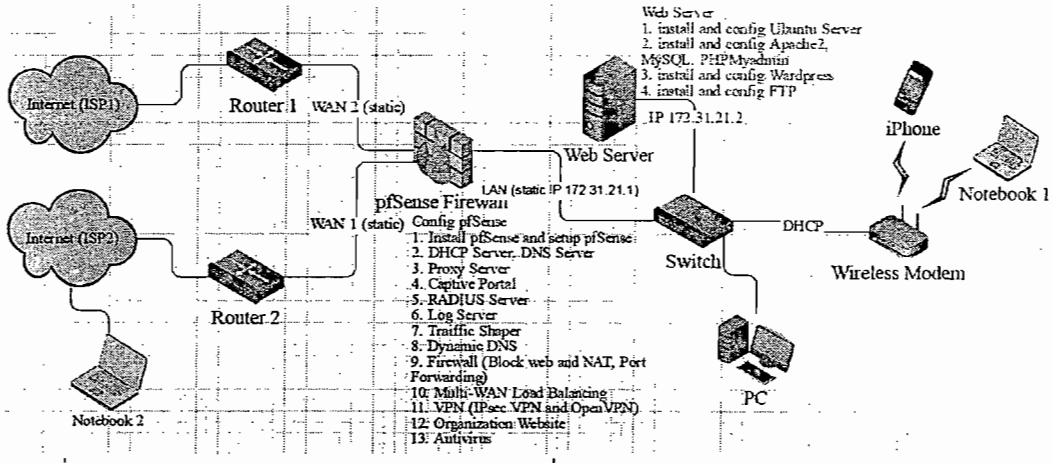
รายการที่ต้องการทดลอง	Software ที่ใช้	Hardware ที่ใช้
DHCP Server, DNS Server	pfSense, cmd	PC, Netbook, iPhone, Switch, Wireless Modem , pfSense Firewall
Proxy Server, Radius Server	pfSense (ใช้ Packages Squid and Lightsquid) Web browser	PC, Netbook, iPhone, Switch, Wireless Modem , pfSense Firewall, Router1, Internet (ISP1)
Bandwidth limit	pfSense, Web browser. www.speedtest.net	PC, Netbook, iPhone, Switch, Wireless Modem , pfSense Firewall, Router1, Internet (ISP1)
Captive Portal, Dynamic DNS, NAT Porforward, Block website Facebook and YouTube, Firewall	pfSense, Web browser	PC, Netbook, iPhone, Switch, Wireless Modem , pfSense Firewall, Router1, Internet (ISP1)

ตารางที่ 3-1 Software และ Hardware ที่ใช้ในสถานที่ทดลอง (ต่อ)

รายการที่ต้องการทดลอง	Software ที่ใช้	Hardware ที่ใช้
Radius Server	pfSense (ใช้ Packages freeradius2), putty	PC, Netbook, iPhone, Switch, Wireless Modem , pfSense Firewall, Router1, Internet (ISP1)
Log Server	pfSense, System Watcher	PC, Netbook, iPhone, Switch, Wireless Modem , pfSense Firewall, Router1, Internet (ISP1)
IPsec	pfSense, Web browser, vpn-client-2.2.2-release	PC, Netbook, iPhone, Switch, Wireless Modem , pfSense Firewall, Router1, Internet (ISP1), Netbook3
OpenVPN	pfSense, Web browser, Packages OpenVPN Client Export, install program OpenVPN Client	PC, Netbook, iPhone, Switch, Wireless Modem , pfSense Firewall, Router1, Internet (ISP1), Netbook3
Load Balance (Bandwidth-Session Management)	pfSense, Web browser	PC, Netbook, iPhone, Switch, Wireless Modem , pfSense Firewall, Router1, Router2, Internet (ISP1), Internet (ISP2), Netbook3
Web Server	pfSense, Web browser, Ubuntu Server, wordpress	PC, Netbook, iPhone, Switch, Wireless Modem , pfSense Firewall, Router, Internet (ISP1), Netbook3

ผู้ทำงานนิพนธ์ได้ออกแบบระบบเครือข่ายเพื่อศึกษา pfSense ในเรื่องต่าง ๆ ดังภาพที่ 3-1 ซึ่งเป็นแผนภาพเครือข่าย (หรือเรียกว่าแผนที่เครือข่าย) แสดงให้เห็นส่วนประกอบต่าง ๆ ของ

เครือข่ายคอมพิวเตอร์ ซึ่งแผนภาพช่วยให้ผู้จัดการเครือข่ายสามารถติดตามแก้ไขปัญหาของระบบเครือข่าย



ภาพที่ 3-1 ถึงโครงสร้างของระบบเครือข่ายในสถานที่จำลอง

การศึกษา ติดตั้ง และ ตั้งค่า pfSense ในสถานที่ทดลอง

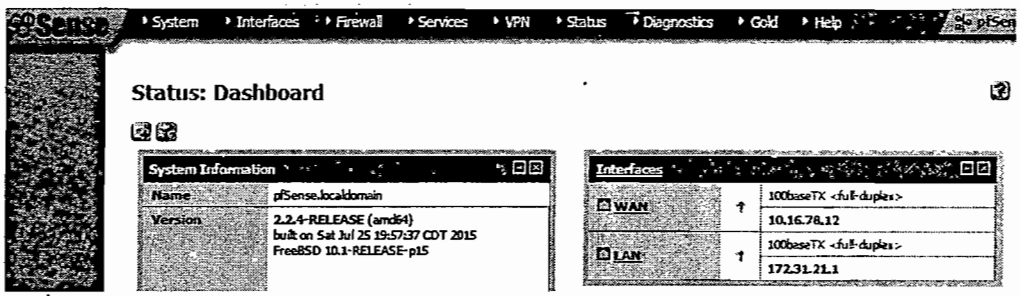
ผู้ทำงานนิพนธ์ได้ศึกษาขั้นตอนการติดตั้ง pfSense (รุ่น 2.2.4-RELEASE-pfSense (amd64)) ในสถานที่ทดลอง โดยติดตั้งใน Dell (Vostro Intel core i3) และ มีการกำหนดค่า card LAN ของ Interface WAN และ LAN (โดยรายละเอียดของการติดตั้ง และ การกำหนดค่า interface ทั้งสองอยู่ใน ภาคผนวก ก.1) และ ผลลัพธ์ของการกำหนดค่า card LAN ของ Interface WAN และ LAN ที่สำเร็จแล้วแสดงผลได้ ดังภาพที่ 3-2

```
*** Welcome to pfSense 2.2.4-RELEASE-pfSense (i386) on pfSense ***

 WAN (wan)       -> le0        -> v4: 10.16.78.12/24
 LAN (lan)       -> le1        -> v4: 172.31.21.1/24
 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) pfSense Developer Shell
 4) Reset to factory defaults         13) Upgrade from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option:
```

ภาพที่ 3-2 ผลลัพธ์ของการกำหนดค่าของ Interface WAN LAN

1. **การใช้ Wizard เพื่อกำหนดค่าเริ่มต้นของ pfSense**

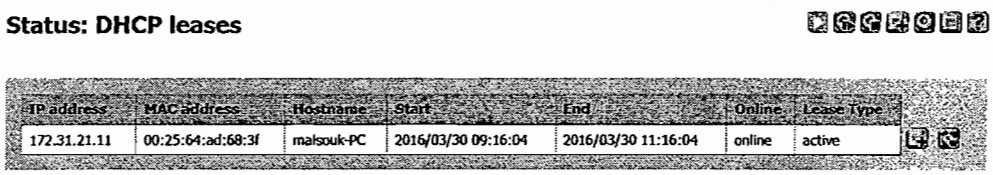
ผู้ทำงานนิพนธ์เปิด Web browser เพื่อ login เข้าในระบบ pfSense หน้า Wizard จะปรากฏขึ้น จากนั้นผู้ทำงานนิพนธ์ได้เข้าไปกำหนดค่า hostname, Domain, Time Server hostname, Time zone กำหนดหมายเลขไอพีใน Interface WAN และ LAN และ รหัสของ admin รายละเอียดของการตั้งค่าอยู่ในภาคผนวก ก.2 และ หลังจากการตั้งค่าแล้ว pfSense จะแสดงหน้าเว็บ ดังภาพที่ 3-3



ภาพที่ 3-3 ผลลัพธ์ของการใช้ Wizard

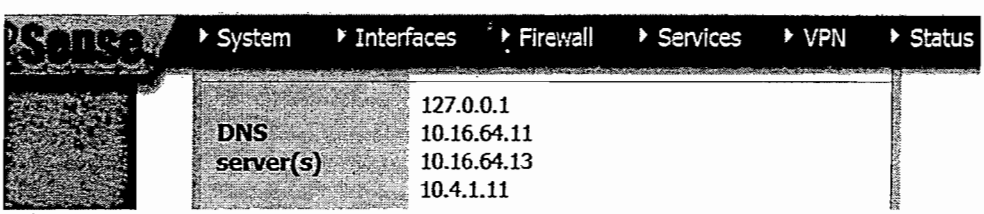
2. **การตั้งค่า DHCP Server, DNS Server**

DHCP เป็นโปรโตคอลที่ใช้ในการแจกไอพีอัตโนมัติในรูปแบบของไคลเอนต์กับเครื่องแม่ข่าย DHCP โดยที่ไคลเอนต์จะต้องส่งคำขอไปยังเครื่องแม่ข่าย DHCP เพื่อขอไอพี ผู้ทำงานนิพนธ์ได้กำหนดค่าที่อยู่หมายเลขไอพีเริ่มตั้งแต่หมายเลขไอพี 172.31.21.10 - 172.31.21.245 ใน interface LAN รายละเอียดของการตั้งค่าอยู่ในภาคผนวก ก.3.1 และ หลังจากสำเร็จการตั้งค่าแล้วจะได้ผลลัพธ์ ดังภาพที่ 3-4



ภาพที่ 3-4 การแสดงถึงผู้เข้าใช้งาน DHCP Server

นอกจากนี้ยังมีการตั้งค่า DNS Server ซึ่ง DNS Server ช่วยแปลง Domain name เป็นหมายเลขไอพีโดยผู้ทำงานนิพนธ์ได้กำหนด DNS Server อยู่ที่ General Setup ของ pfSense รายละเอียดของการตั้งค่าอยู่ในภาคผนวก ก.3.2 และ หลังจากตั้งค่าแล้วผู้ติดตั้งจะได้ผลลัพธ์ ดังภาพที่ 3-5



ภาพที่ 3-5 ผลลัพธ์ของการกำหนดค่า DNS Server

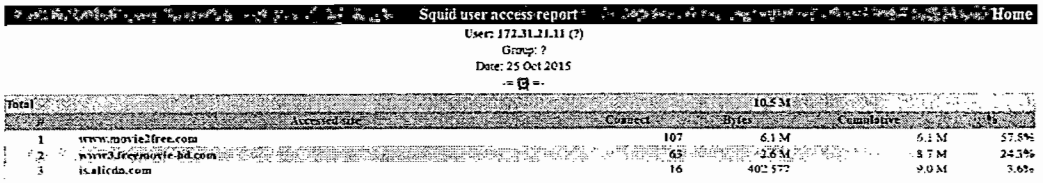
3. การตั้งค่าเครื่องแม่ข่าย Proxy

1. ผู้ทำงานนิพนธ์ได้กำหนดค่าในเครื่องแม่ข่าย Proxy ซึ่งเครื่องแม่ข่าย Proxy เป็นเครื่องแม่ข่ายที่เก็บหน้าเว็บเพจที่ถูกเรียกใช้ไปแล้วเพื่อให้ไคลเอนต์เข้ามาใช้ได้ภายหลัง โดยที่ pfSense ให้บริการดาวน์โหลดแพ็กเกจเครื่องแม่ข่าย Proxy เพื่อติดตั้ง โดยผู้ติดตั้งต้องกำหนดค่าต่าง ๆ ดังนี้

- เลือก Interface ที่จะใช้ตั้งค่า Proxy
- อนุญาตผู้ใช้ให้ใช้ Interface ได้โดยไม่ต้องเพิ่ม Subnet ที่จะอนุญาตให้กับ Interface (Allow users on interface)
- สั่งข้อมูลที่จะไป port 80 ทั้งหมดไปที่ port proxy โดยไม่ต้องตั้งค่าใดอีก (Transparent proxy)
- บันทึกการเข้าถึง proxy (Enable logging)
- ตั้งขนาดของ cache (Hard disk cache size)

2. เพิ่มหมายเลขไอพีของ cache managers ภายนอกที่ผู้ติดตั้งยอมให้เข้ามาควบคุมจากภายนอก รายละเอียดของการตั้งค่าอยู่ในภาคผนวก ก.4.1

3. นอกจากนี้ เครื่องแม่ข่าย Proxy ยังมีแพ็กเกจ Lightsquid ซึ่งเป็นเครื่องมือที่ใช้เก็บบันทึก URL เข้าใช้แต่ละเว็บเพจ โดยผู้ติดตั้งต้องกำหนดค่ารูปแบบรายงาน (Report Template) และ ช่วง เวลาการ Refresh (Refresh Scheduler) ดังรายละเอียดของการตั้งค่าอยู่ในภาคผนวก ก. 4.3-4.4 และ หลังจากตั้งค่าแล้วจะได้ผลลัพธ์การบันทึก URL ดังภาพที่ 3-6



ภาพที่ 3-6 ผลลัพธ์การเก็บ log URL แต่ละเว็บเพจของผู้ใช้ 172.31.21.11

4. การตั้งค่า Captive Portal

Captive portal เป็นระบบยืนยันตัวตน (Authentication) ก่อนที่จะใช้งานอินเทอร์เน็ต ระบบ Captive portal ให้เข้าไปยังหน้าเว็บที่ให้เราป้อน username และ password เพื่อตรวจสอบตัวตนก่อนการเข้าใช้งาน โดยมีการตั้งค่า Captive Portal และ สร้าง User ตามขั้นตอนดังต่อไปนี้

1. การกำหนดค่าอยู่ที่ Captive Portal มีดังนี้
   - เปิดใช้ (captive portal) ☑ Enable captive portal
   - เลือก Interface LAN ที่ต้องการใช้ Captive Portal (Interface)

- กำหนดจำนวนการเชื่อมต่อพร้อมกันในเวลาผู้ใช้เข้า login เพื่อเข้าใช้ Internet (Maximum concurrent connections)

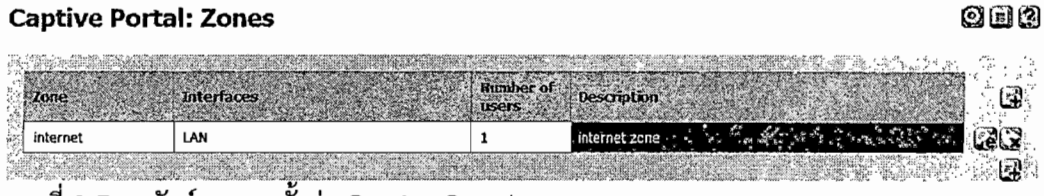
- กำหนดช่วงเวลาที่ผู้ใช้ต้องการ login ใหม่ในกรณีที่ผู้ใช้ไม่ได้ใช้ Internet เป็นเวลาต่อเนื่องกัน Idle timeout

- ใส่ URL ของหน้าของที่เว็บเบราว์เซอร์ต้องแสดงหลังจาก login สำเร็จแล้ว (After authentication redirection URL)

- กำหนดจำนวนผู้ใช้ในการเข้า login พร้อมกันหลายเครื่อง (Concurrent user logins)

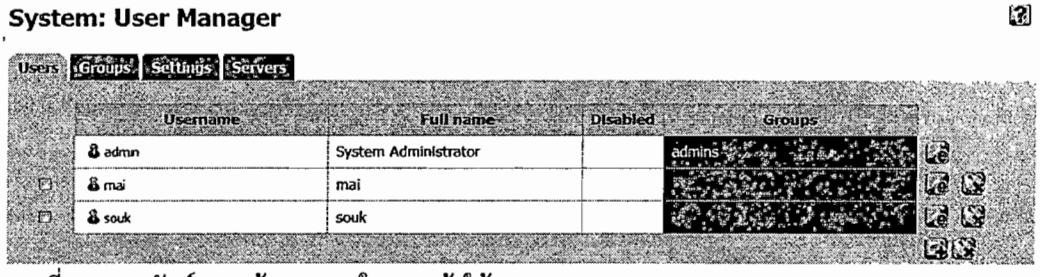
- เลือกการยืนยันตัวตน หรือ ผู้จัดการระบบ (ท้องถิ่น) (Authentication)

รายละเอียดของการตั้งค่าอยู่ในภาคผนวก ก.5.1 และ หลังจากการตั้งค่าแล้วจะได้ผลลัพธ์ ดังภาพที่ 3-7



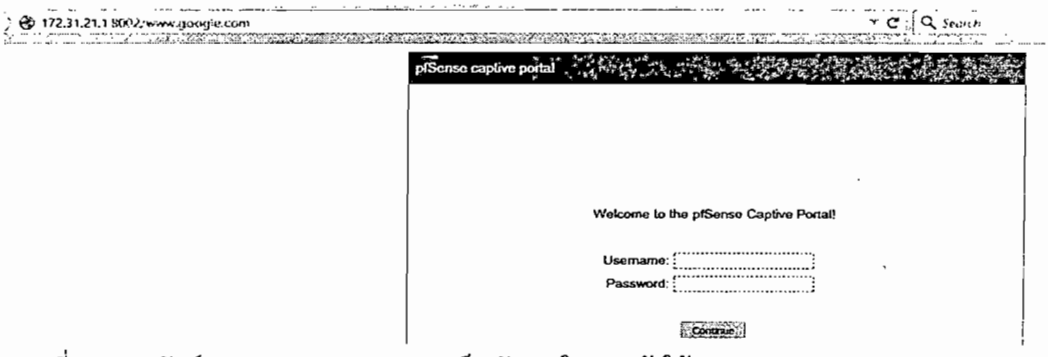
ภาพที่ 3-7 ผลลัพธ์ของการตั้งค่า Captive Portal

2. ถ้าเลือกการยืนยันตัวตนโดยใช้ระบบจัดผู้ใช้ (ท้องถิ่น) ในข้อ 2.4.1 ผู้ติดตั้งต้องสร้างผู้ใช้ที่จะยอมให้เข้าไปใช้งานเครือข่าย Internet โดยกำหนด User, Password และ Full name รายละเอียดของการตั้งค่าอยู่ในภาคผนวก ก.5.2 และ หลังการตั้งค่าแล้วจะได้ผลลัพธ์ ดังภาพที่ 3-8



ภาพที่ 3-8 ผลลัพธ์ของสร้าง User ในการเข้าใช้งาน Captive Portal

3. ผลการตรวจสอบใช้งานระบบ Captive Portal เมื่อไคลเอนต์ต้องการเข้าใช้ Internet โดยเข้าเว็บ www.Google.com จะมีหน้ายืนยันตัวตน (Authentication) ให้ผู้ใช้ป้อน username และ password ดังภาพที่ ภาพที่ 3-9



ภาพที่ 3-9 ผลลัพธ์ของการตรวจสอบความเป็นตัวตน ในการเข้าใช้งาน Captive Portal

4. ถ้าไคลเอนต์ยืนยันตัวตนสำเร็จ ระบบจะบันทึกการเข้าถึง โดยแสดงหมายเลขไอพี หมายเลข MAC และ username ของผู้ใช้งาน ดังภาพที่ 3-10

Captive Poital status

IP address	MAC address	Username	Session start
172.31.21.11	00:25:64:ad:68:3f	mai	03/30/2016 06:35:30

ภาพที่ 3-10 บันทึกการยืนยันตัวตนของผู้ใช้

5. **การตั้งค่าเครื่องแม่ข่าย Free RADIUS**

เครื่องแม่ข่าย Free RADIUS เป็น package ที่ใช้ในการตรวจสอบสิทธิ์ในการใช้งานของผู้ใช้ (User) เช่น เมื่อมีการใช้งานของระบบ VPN Server หรือ Captive Portal จะมีการตรวจสอบสิทธิ์ก่อนการเข้าใช้งาน ผู้ทำงานนิพนธ์ได้ 1) ติดตั้ง package ของ Free RADIUS2 2) กำหนดชื่อและรหัสของผู้ใช้งาน 3) กำหนดที่อยู่ไอพี และ รหัสของไคลเอนต์ใน NAS/Clients และ 4) กำหนดค่า Interfaces ที่กำลังรอข้อมูล RADIUS listening interface และรหัสของไคลเอนต์ รายละเอียดของการตั้งค่าอยู่ในภาคผนวก ก.6.1-ก.6.2 หลังจากตั้งค่าแล้วจะได้ผลลัพธ์ ดังภาพที่ 3-11

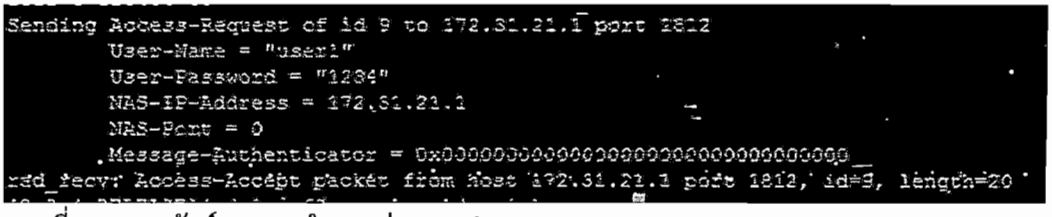
FreeRADIUS: Interfaces

Users | MACs | NAS / Clients | Interfaces | Settings | EAP | SQL | Certificates | LDAP | View config | XMLRPC Sync

Interface IP Address	Port	Interface Type	IP Version	Description
172.31.21.1	1812	auth	ipaddr	interface LAN

ภาพที่ 3-11 ผลลัพธ์ของการกำหนดค่า Interfaces

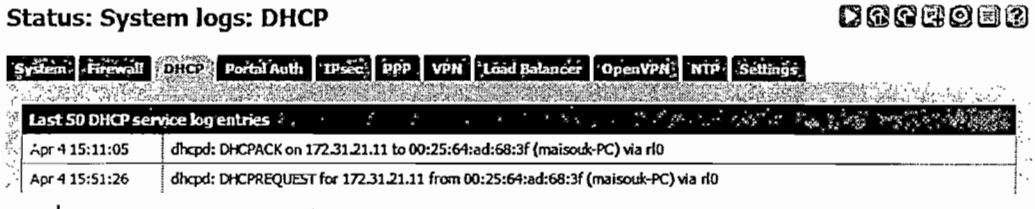
จากนั้นผู้ทำงานนิพนธ์ได้ทดสอบการทำงาน Free RADIUS2 package โดยเข้าไปที่หน้า command line ของเครื่องแม่ข่าย pfSense ผ่านช่องทาง SSH จากโปรแกรม Putty โดยใช้ คำสั่ง redtest user1 user1 192.168.254.1 :1812 0 123456789 โดยระบบจะแสดงคำว่า Access-Accept ในบรรทัดสุดท้ายต่อหน้าคำ rad_recv รายละเอียดของการตั้งค่าอยู่ในภาคผนวก ก.6.3 หลังจากตั้งค่าแล้วจะได้ผลลัพธ์ ดังภาพที่ 3-12



ภาพที่ 3-12 ผลลัพธ์ของการกำหนดค่า Interfaces

6. การตั้งค่า Log Server

pfSense มีระบบ System logs ที่ใช้ในการเก็บ log file ต่าง ๆ ที่ทำงานอยู่บน pfSense เช่น การเก็บ log DHCP, log firewall, log OpenVPN และ อื่น ๆ ดังภาพที่ 3-13

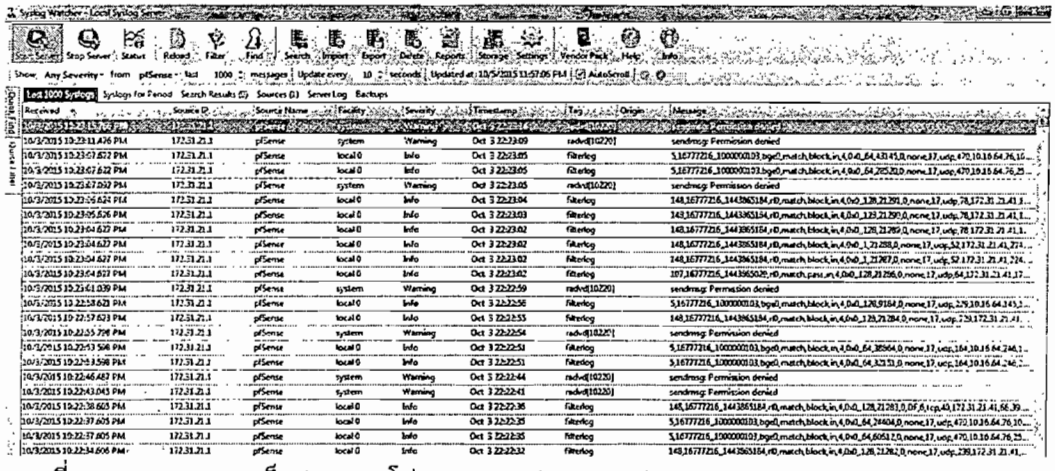


ภาพที่ 3-13 การแสดงระบบเก็บ logs ของ DHCP

นอกจากนี้ยังตั้งค่าให้ pfSense ส่ง log ไปยัง log Server เครื่องอื่น โดยใช้โปรแกรม (Syslog Watcher) เพื่อเก็บ logs ต่าง ๆ ที่ส่งมาจาก pfSense ผู้ทำงานนิพนธ์ได้กำหนดค่าดังรายละเอียดต่อไปนี้

- เปิดใช้การบันทึกระยะไกล (Enable Remote Logging: ☑ Send log messages to remote syslog server)
- ระบุหมายเลขไอพีของ Server ที่มีโปรแกรม Syslog Watcher (Remote Syslog Servers: Server: xxx.xxx.xxx.xxx)
- ดาวน์โหลดโปรแกรม Syslog Watcher ที่เว็บไซต์ http://syslogwatcher.soft32.com เพื่อติดตั้ง

รายละเอียดของการตั้งค่าอยู่ในภาคผนวก ก.7.1-ก.7.3 หลังจากตั้งค่าแล้วจะได้ผลลัพธ์ดังภาพที่ 3-14



ภาพที่ 3-14 ผลของการเก็บ log ของโปรแกรม Syslog Watcher

7. การจำกัดแบนด์วิดท์การดาวน์โหลด และ การอัพโหลดให้แก่เครื่องบางเครื่อง

ผู้ทำงานนิพนธ์ได้ใช้ “Limiter” เพื่อจำกัดแบนด์วิดท์ (จำกัดความเร็วได้ทั้งการ upload และ การ download) โดยจำกัดแบนด์วิดท์การดาวน์โหลด (InlimiterLAN=60Mbit/s) และ การอัพโหลด (QotlimiterLAN=30Mbit/s) ให้กับเครื่องที่ใช้หมาย เลขไอพีที่กำหนด โดยมีขั้นตอนดังนี้

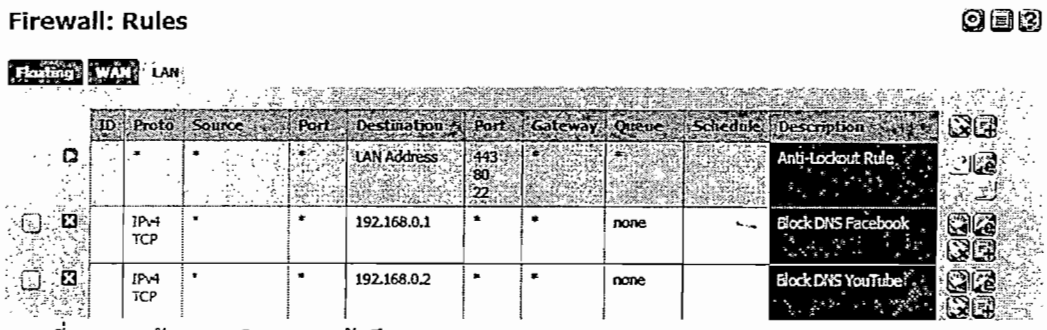
- อนุญาตให้เปิด limiter ของลูกเครือข่าย (Enable: ☑ Enable limiter and its....
- ใส่ชื่อ (Name: OutlimiterLAN)
- กำหนดแบนด์วิดท์ (Bandwidth: 30 Mbit/s)

รายละเอียดของการตั้งค่าอยู่ในภาคผนวก ก.8.1-ก.8.2 หลังจากตั้งค่าแล้วจะได้ผลลัพธ์ดังภาพที่ 3-15

ภาพที่ 3-15 ผลการทดสอบปริมาณแบนด์วิดท์สำหรับอัพโหลด และ ดาวน์โหลด โดยใช้เครื่องมือจากเว็บไซต์ www.speedtest.net

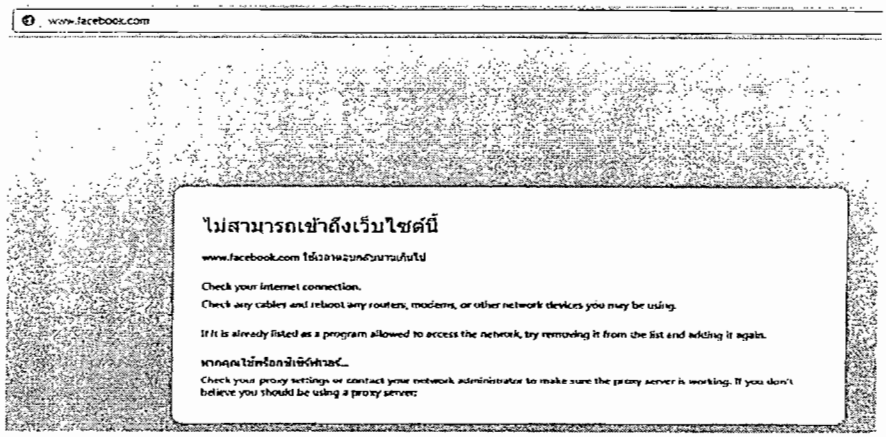
8. การตั้งค่าบล็อก Facebook และ YouTube ใน pfSense

การบล็อก Facebook และ YouTube เป็นการสร้างกฎไฟร์วอลล์ปฏิเสธให้มีการเข้าถึง Facebook และ YouTube โดยผู้ทำงานนิพนธ์จำลอง DNS Resolver อยู่ที่ Host Overrides ของ Facebook และ YouTube เพื่อนำไปสร้างกฎไฟร์วอลล์ไม่อนุญาตให้มีการเข้าถึงตัว DNS Resolver รายละเอียดของการตั้งค่าอยู่ในภาคผนวก ก.9.1-ก.9.2 หลังจากตั้งค่าแล้วจะได้ผลลัพธ์ ดังภาพที่ 3-16



ภาพที่ 3-16 สร้างกฎปฏิเสธการเข้าถึง Facebook และ YouTube

หลังจากสร้างกฎแล้วผู้ทำงานนิพนธ์ได้ทดสอบการเข้าถึง Facebook ได้ผลดังภาพที่ 3–17

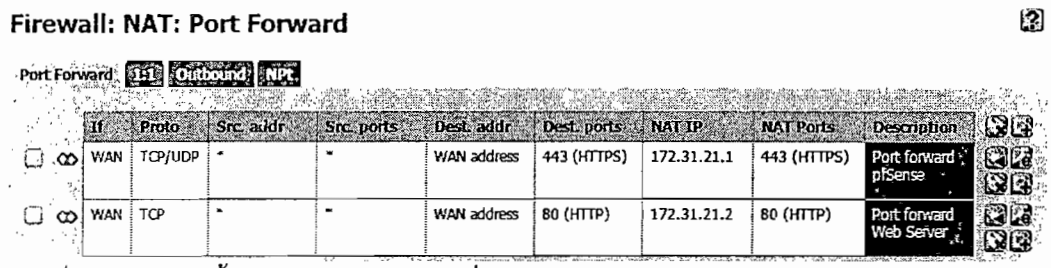


ภาพที่ 3-17 ผลการเข้าถึงตัว Facebook

9. การตั้งค่า NAT และ Port Forward ไปที่ Web server ใน pfSense

การส่งต่อพอร์ตที่ NAT คือ การกำหนดเส้นทางของข้อมูลที่ติดต่อเข้ามายังอุปกรณ์จัดเส้นทาง (Router หรือ มาที่เครื่องแม่ข่าย pfSnese) โดยอาศัยตาราง NAT ที่ช่วยแปลงไอพีภายนอก (Public IP address) ไปเป็นไอพีภายในระบบ (Private IP address) ผู้ทำงานนิพนธ์ได้ตั้งค่า NAT ใน pfSense เพื่อแปลง IP ของ Interface WAN (10.16.64.92) ให้เป็นหมายเลข IP ของ Interface LAN (172.31.21.1 ของ pfSense และ 172.31.21.2 ของ Web server)

Port forwarding เป็นการกำหนดเส้นทางของข้อมูลไปยังเครื่องปลายทาง เช่น การทำ Port forwarding ไปที่ Port 443 ของเครื่อง pfSense และ Port 80 ของ Web Server รายละเอียดของการตั้งค่าอยู่ในภาคผนวก ก.10 หลังจากตั้งค่าแล้วจะได้ผลลัพธ์ดังภาพที่ 3-18



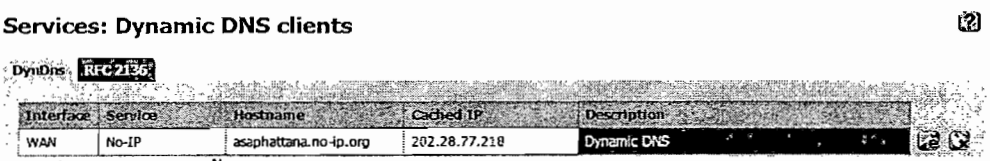
ภาพที่ 3-18 ผลการตั้งค่า port forward ไปที่ pfSense และ Web Server

10. การตั้งค่า Dynamic DNS

Dynamic Domain Name System เป็นระบบที่ให้บริการการแปลงชื่อโดเมนเป็นหมายเลขไอพี (ซึ่งต่างจากระบบ DNS ทั่วไปที่หมายเลขไอพีของเครื่องผู้ให้บริการจำเป็นต้องคงที่) โดยขั้นตอนการกำหนดค่าบริการ DNS แบบไดนามิกใน pfSense ต้องมีการสมัคร Free Dynamic DNS และ ตั้งค่า Dynamic DNS ใน pfSense ดังนี้

- เลือกประเภทบริการ (Service type: No-IP)
- เลือกอินเตอร์เฟส (Interface to monitor: WAN)
- รูปแบบการบริการที่สมัครชื่อโฮสต์ (Service type: No-IP)
- ใส่ชื่อโฮสต์ที่สมัคร (Hostname: asaphatthana.no-ip.org)
- ใส่ E-mail ที่ใช้สมัคร (Username: msycm2015@gmail.com)
- ใส่รหัส (Password: xxxxxxx)
- คำอธิบายสิ่งที่เราจะทำ (Description: asathattana.no-ip.org)

รายละเอียดของการตั้งค่าอยู่ในภาคผนวก ก.11.1-ก.11.2 หลังจากตั้งค่าแล้วจะได้ผลลัพธ์ดังภาพที่ 3-19



ภาพที่ 3-19 ผลการตั้งค่า Dynamic DNS

11. การสร้างกฎไฟร์วอลล์

ไฟร์วอลล์เป็นเครื่องมือสร้างกฎทำหน้าที่เสมือนกำแพงหน้าบ้านที่สำคัญของระบบเครือข่ายทำหน้าที่ป้องกันการโจมตีจากบุคคลภายนอก และ กำหนดสิทธิ์การเข้าใช้ระบบเครือข่ายโดยผู้ใช้ pfSense สร้างกลุ่มที่ต้องการอนุญาตใช้ในกฎของกฎไฟร์วอลล์ เช่น EmailPort, LocalNetworkPort, และ RomoteAccessPorts และการสร้างกฎไฟร์วอลล์ มีขั้นตอนดังนี้

1. สร้างกลุ่ม Alias port ของ EmailPorts, LocalNetworkPort, และ RomoteAccessPorts

- ใส่ชื่อกลุ่ม Alias port (Name: EmailPorts, LocalNetworkPort, หรือ RomoteAccessPorts)
- คำอธิบาย (Description: Permit only important ports to client local net)
- เลือกรูปแบบเป็น Port (Type: Port(S))
- ใส่ port ที่ต้องการอนุญาต (Port (S): 20, 21, 53.....)

รายละเอียดของการตั้งค่าอยู่ในภาคผนวก ก.12.1 หลังจากตั้งค่าแล้วจะได้ผลลัพธ์ดังภาพที่ 3-20

Firewall: Aliases

IP Ports URLs All

Name	Values	Description
EmailPorts	25, 80, 110, 143, 465, 993, 995	General email port
LocalNetworkPort	20, 21, 67, 68, 80, 123, 389, 443, 445, 563...	Permit only important ports to client local net
RomoteAccessPorts	22, 23, 1194, 1389, 4500	Allow client to use the port for remote access

ภาพที่ 3-20 ผลของการสร้างกลุ่ม Alias port ของ EmailPorts, LocalNetworkPort, และ RomoteAccessPorts

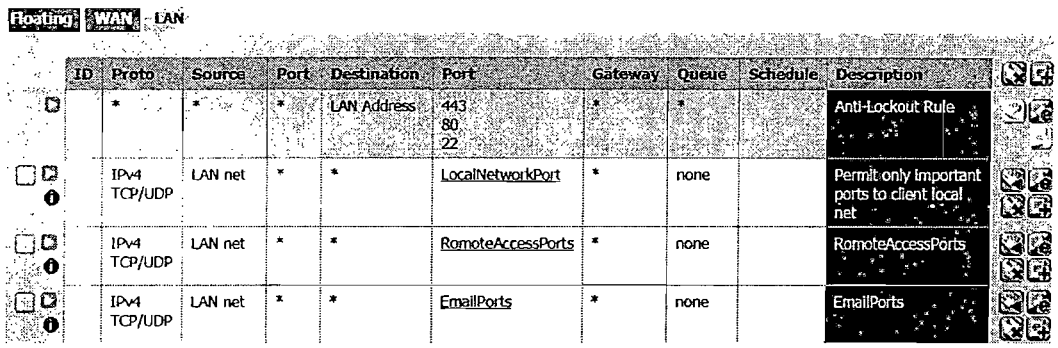
2. สร้างกฎไฟร์วอลล์สำรับการอนุญาตใช้ LocalNetworkPort, RomoteAccessPorts, และEmailPorts

- รูปแบบการกระทำ (Action: Pass)
- เลือกอินเตอร์เฟส (Interface: LAN)
- กำหนด Protocol (Protocol: TCP/UDP)
- รูปแบบต้นทาง (Source: Type: LAN net)
- รูปแบบปลายทาง (Destination: type: any)

- เลือกกลุ่ม port ปลายทาง (Destination port range: from: (other): LocalNetworkPort RomoteAccessPorts EmailPorts และ to: (other): LocalNetworkPort RomoteAccessPorts EmailPorts

- คำอธิบายสิ่งที่เราจะทำ (Description: Permit only important ports to ....)

รายละเอียดของการตั้งค่าอยู่ในภาคผนวก ก.12.2 หลังจากตั้งค่าแล้วจะได้ผลลัพธ์ ดังภาพที่ 3-21

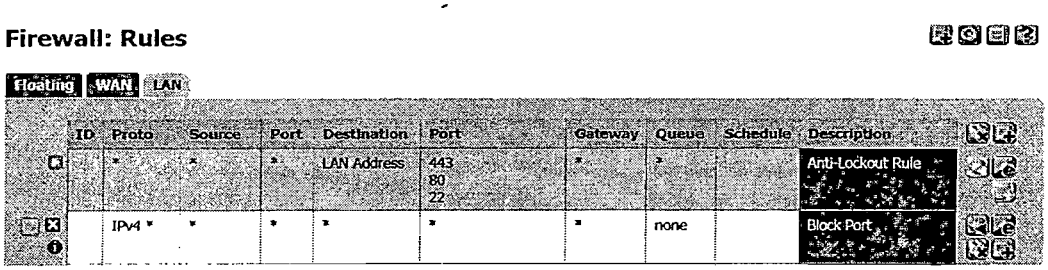


ภาพที่ 3-21 ผลของการสร้างกฎไฟร์วอลล์สำหรับการอนุญาตใช้ LocalNetworkPort, RomoteAccessPorts, และ EmailPorts

3. การสร้างกฎไฟร์วอลล์ไม่อนุญาตให้มีการเข้าถึง Port

- Action: block
- Interface: LAN
- Protocol: any
- Source: Type: LAN net
- Destination: type: any
- Log: ☑ Log packets that are handled by this rule
- Description: block port แล้วคลิก Save

รายละเอียดของการตั้งค่าอยู่ในภาคผนวก ก.12.3 หลังจากตั้งค่าแล้วจะได้ผลลัพธ์ ดังภาพที่ 3-22

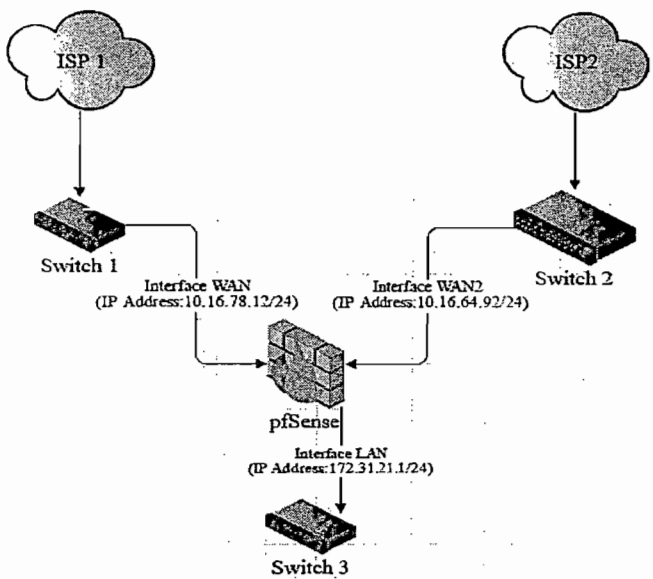


ภาพที่ 3-22 ผลของสร้างกฎไฟร์วอลล์ไม่อนุญาตให้มีการเข้าถึง Port

12. การตั้งค่า Multi-WAN Load Balancing

Load Balancing เป็นตัวช่วยแบ่งกระจายงานของ WAN1 และ WAN2 กรณีที่ WAN1 หรือ WAN2 down pfSense สามารถไปใช้อีกทางได้ นอกจากนี้ load balancing มีการแบ่งทราฟฟิกจากเครื่องภายในเครือข่ายไปยัง WAN ทั้งสองในมีอัตราที่เหมาะสม โดยมีขั้นตอนในการกำหนดค่าดังนี้

- การออกแบบแผนภาพ (Diagram) ของ Multi-WAN Load Balancing ดังภาพที่ 3-23



ภาพที่ 3-23 การแสดงถึงโครงสร้างของ Multi-WAN Load Balancing

- กำหนดหมายเลขไอพีของ interface WAN และ interface WAN2 เป็น Static
- สร้าง Group สำหรับ Load balancing สำหรับ Failover จำนวน 2 Group
- ตรวจสอบการทำงานของ Gateway WAVGW และ Gateway OPTGW ทั้งสอง

รายละเอียดของการตั้งค่าอยู่ในภาคผนวก ก.13 หลังจากตั้งค่าแล้วจะได้ผลลัพธ์ดังภาพที่ 3-24

Status: Gateways

Gateways | Gateway Groups

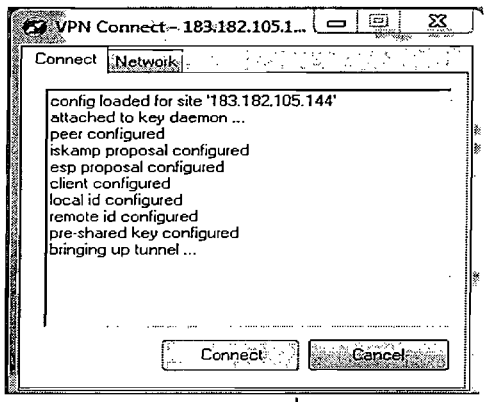
Name	Gateway	Monitor	RTT	Loss	Status	Description
WANGW	10.16.78.1	10.16.78.12	0.4ms	0%	Online Last check: Wed, 07 Oct 2015 00:53:53 +0700	WAN Gateway
OPT1GW	10.16.64.1	10.16.64.92	0.1ms	0%	Online Last check: Wed, 07 Oct 2015 00:53:53 +0700	WAN2

ภาพที่ 3-24 ผลของการตรวจสถานะของ Gateway WAVGW และ OPTGW ทั้งสองสถานะ online

13. การตั้งค่า IPsec VPN

IPSec VPN เป็นเทคโนโลยีที่ให้ผู้ใช้สามารถเข้าถึงทรัพยากรเครือข่ายของสถาบันได้โดยผ่าน IPsec

IPSec ย่อมาจาก Internet Protocol Security เป็นโปรโตคอลสำหรับการส่งข้อมูลผ่านอินเทอร์เน็ตอย่างปลอดภัย โดยการพิสูจน์ตัวตน และ การเข้ารหัสของผู้ใช้ในขณะที่ทำการติดต่อ นอกจากนี้โปรโตคอลยังตรวจสอบความถูกต้อง และการรักษาความปลอดภัยของข้อมูล โดยการตั้งค่า IPsec VPN มีขั้นตอนดังนี้ 1) กำหนดค่า IPsec VPN และ ค่าฝั่ง client 2) สร้างกฎไฟร์วอลล์สำหรับ Interface WAN and IPsec รายละเอียดของการตั้งค่าอยู่ในภาคผนวก ก.14 หลังจากการตั้งค่าแล้ว ผู้ทำงานนิพนธ์ได้ทดสอบการเชื่อมต่อของ VPN ไปที่ pfSense ดังภาพที่ 3-25



ภาพที่ 3-25 ผลของการเชื่อมต่อของ PVN connect ไปที่ pfSense

ผู้ทำงานนิพนธ์ได้ทดสอบโดยได้ ping ไปหาไอพีของ Interface LAN Server ที่อยู่ภายในเครือข่ายของสถาบัน หลังจากได้เชื่อมต่อ IPsec VPN สำเร็จจะแสดงได้ตามผลตอบกับ ping ดังภาพที่ 3-26

```
C:\Users\maisouk>ping 192.168.254.1

Pinging 192.168.254.1 with 32 bytes of data:
Reply from 192.168.254.1: bytes=32 time=51ms TTL=64
Reply from 192.168.254.1: bytes=32 time=20ms TTL=64

Ping statistics for 192.168.254.1:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 20ms, Maximum = 51ms, Average = 35ms
```

ภาพที่ 3-26 ผลของการ ping ไปหาไอพีของ Interface LAN Server

14. การตั้งค่า OpenVPN

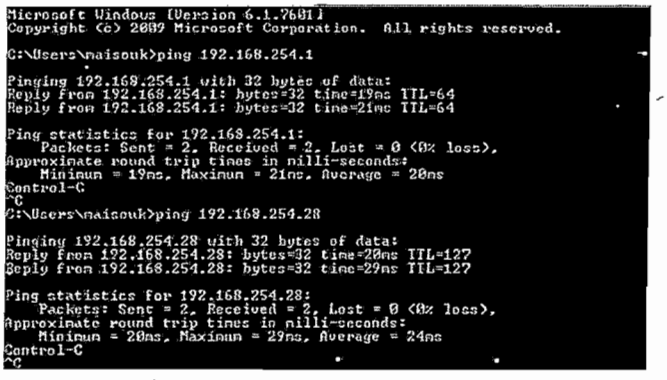
ผู้ใช้งานสามารถติดต่อเข้าใช้งานเครือข่ายของสถาบัน ในเวลาผู้ใช้ออกไปทำงานนอกสถานที่ได้ผ่าน OpenVPN โดยมีขั้นตอนการกำหนดค่าดังนี้

- ติดตั้ง Packages ของ OpenVPN
- ใช้ Wizard กำหนดค่า OpenVPN
- สร้าง User สำหรับใช้ในการเข้า Login OpenVPN
- การกำหนดค่า OpenVPN Client Export โดยการนำเอาค่า config ไปใส่ใน directory ของ OpenVPN Client

รายละเอียดของการตั้งค่าอยู่ในภาคผนวก ก.15 และหลังจากการตั้งค่าแล้ว ผู้ทำงานนิพนธ์ได้ทำการทดสอบการเชื่อมต่อ OpenVPN Connection ไปที่ pfSense ผลได้ดังภาพที่ 3-27

ภาพที่ 3-27 ผลการเชื่อมต่อของ OpenVPN ไปที่ pfSense

ผลทดสอบ ping ไปหาไอพีของ interface LAN Server ที่อยู่ในเครือข่ายของสถาบันเมื่อเชื่อมต่อ OpenVPN สำเร็จเป็น ดังภาพที่ 3-28

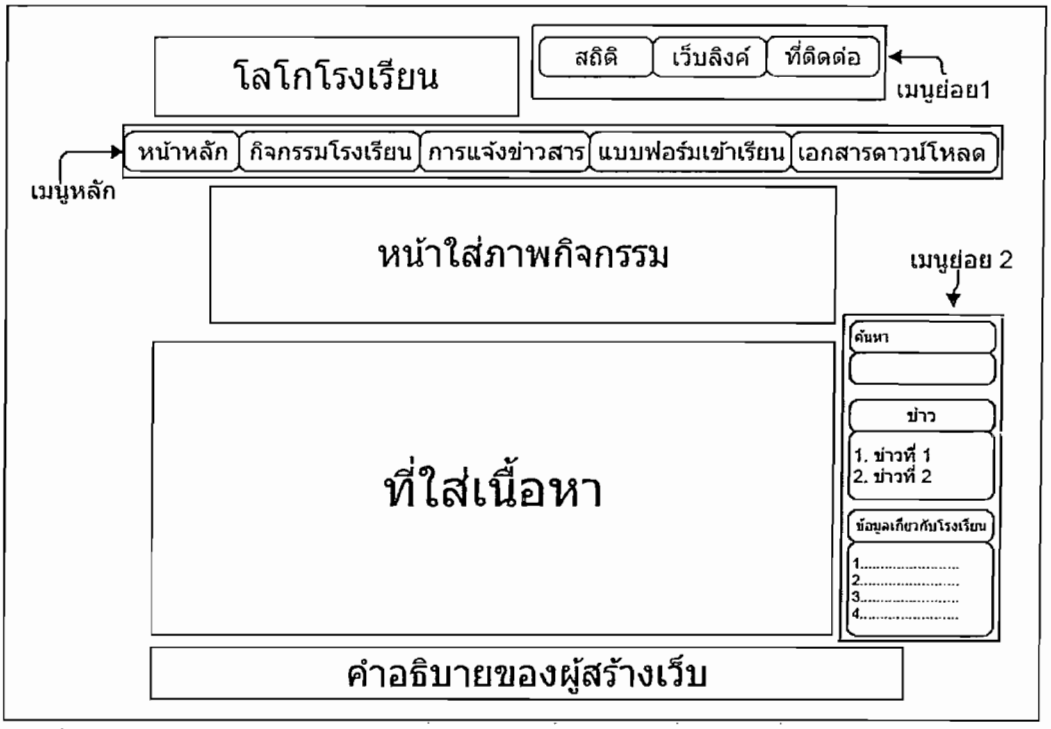


ภาพที่ 3-28 ผลของการ ping ไปหาไอพีของ interface LAN Server

15. การติดตั้งเครื่องแม่ข่าย และ การสร้างเว็บไซต์ขององค์กร

1. การออกแบบหน้าเว็บของวิทยาลัยพลศึกษา

การออกแบบแผนภาพหน้าหลักของเว็บไซต์ของวิทยาลัยพลศึกษา ดังภาพที่ 3-29



ภาพที่ 3-29 การออกแบบแผนภาพหน้าเว็บของวิทยาลัยพลศึกษา

2. ส่วนประกอบมีรายละเอียดของเว็บมีดังนี้
   - โลโก้ของโรงเรียน
   - เมนูหลัก (หน้าหลัก กิจกรรมโรงเรียน การแจ้งข่าวสาร แบบฟอร์มเข้าเรียน เอกสารดาวน์โหลด
   - เมนูย่อย 1 สถิติ (สถิตินักเรียน และ สถิติครู) เว็บลิงค์ และ ที่ติดต่อ
   - เมนูย่อย 2 (ค้นหา ข่าว ข้อมูลเกี่ยวกับโรงเรียน ระบบการจัดตั้ง องค์กรจัดตั้ง มหาชน ห้องการที่ขึ้นกับโรงเรียน หลักสูตรการเรียน-การสอน คะแนนของนักเรียน รายชื่อนักเรียน)
   - หน้าใส่ภาพกิจกรรม
   - ที่ใส่เนื้อหา
   - คำอธิบายของผู้สร้างเว็บ

3. ผู้ทำงานนิพนธ์ข้อกล่าวถึงการติดตั้ง Ubuntu Server ในงานนิพนธ์นี้แนะนำให้ผู้อ่านไปศึกษาที่เว็บไซต์ (https://www.youtube.com/watch?v=EMla0SHfXSs)

4. ผู้ทำงานนิพนธ์ข้อกล่าวถึงการติดตั้งและตั้งค่า Word press ในงานนิพนธ์นี้แนะนำให้ผู้อ่านไปศึกษาที่เว็บไซต์ https://www.youtube.com/watch?v=_0zKdNDYEI0&spfreload=10

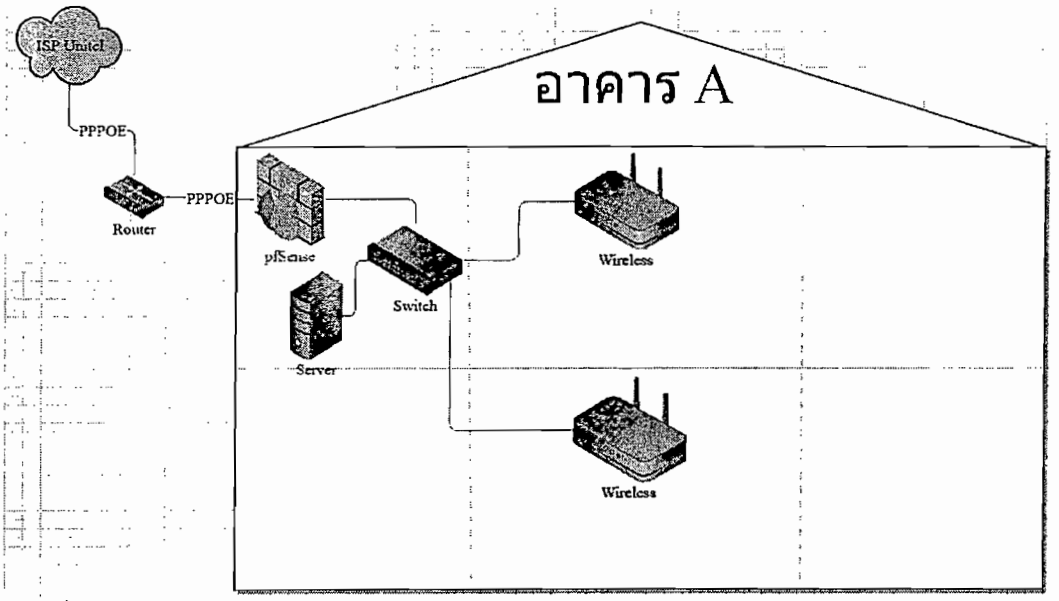
ผลของการสร้าง website วิทยาลัยพลศึกษา เป็นไปตามที่ออกแบบไว้ แสดงดังภาพที่ 3-30

ภาพที่ 3-30 หน้าเว็บไซต์ของวิทยาลัยพลศึกษา

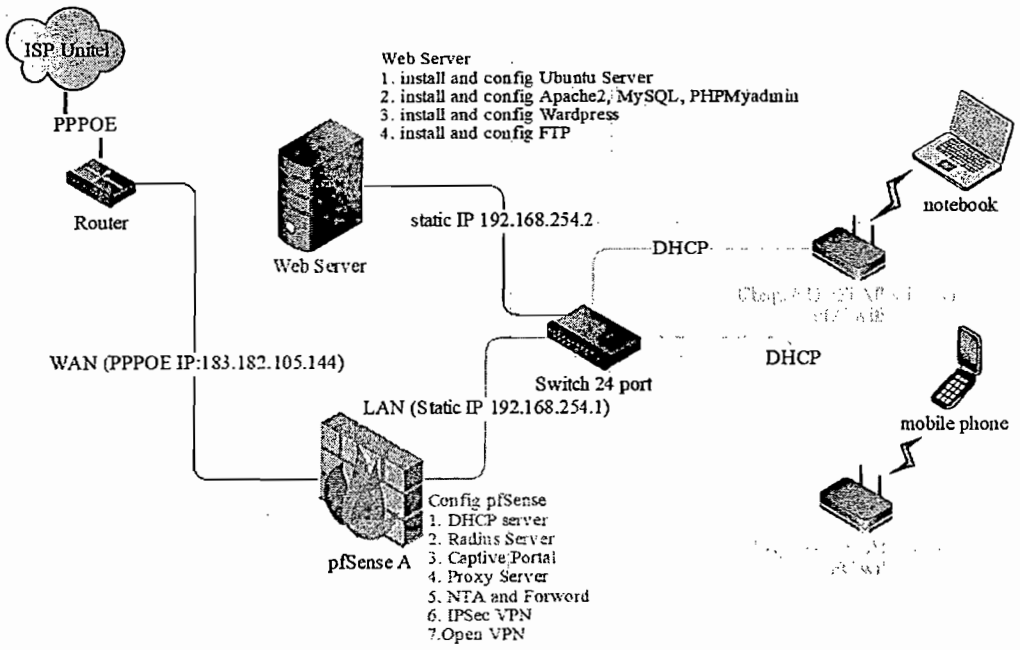
การออกแบบเครือข่ายในสถานที่จริง

ผู้ทำงานนิพนธ์ได้มีการออกแบบระบบเครือข่ายในสถานที่จริง เพื่อการติดตั้งและการเข้าใช้งานที่ประเทศสาธารณรัฐประชาธิปไตยประชาชนลาว ได้มีการออกแบบระบบเครือข่ายในแต่ละอาคาร

1. การออกแบบแผนภาพระบบเครือข่ายในอาคาร A แสดงดังภาพที่ 3-31, 3-32

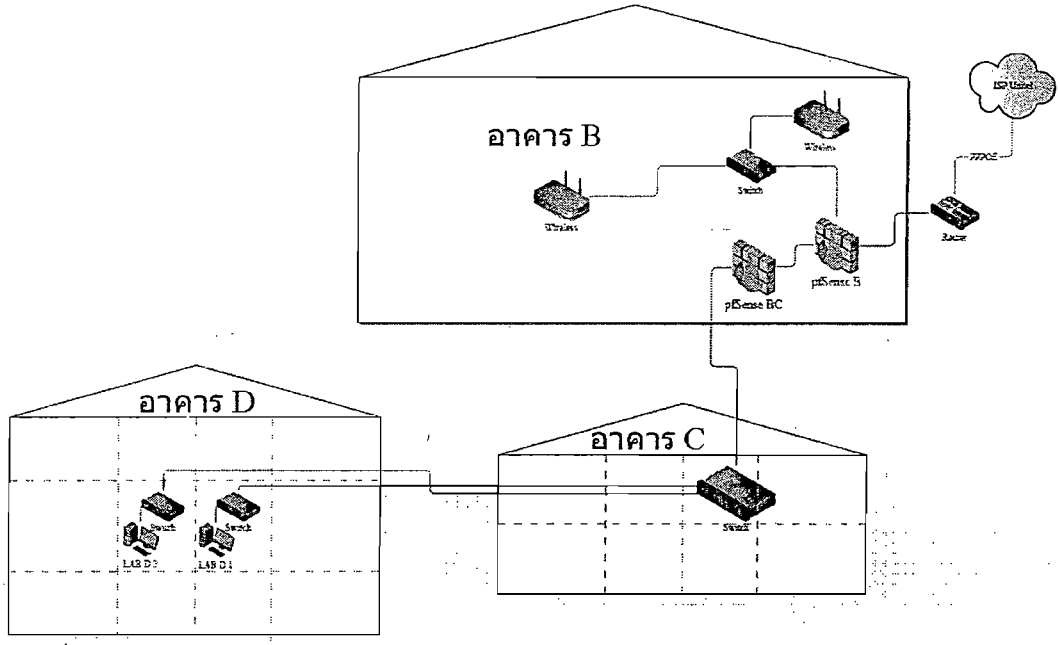


ภาพที่ 3-31 การออกแบบแผนภาพระบบเครือข่ายในอาคาร A

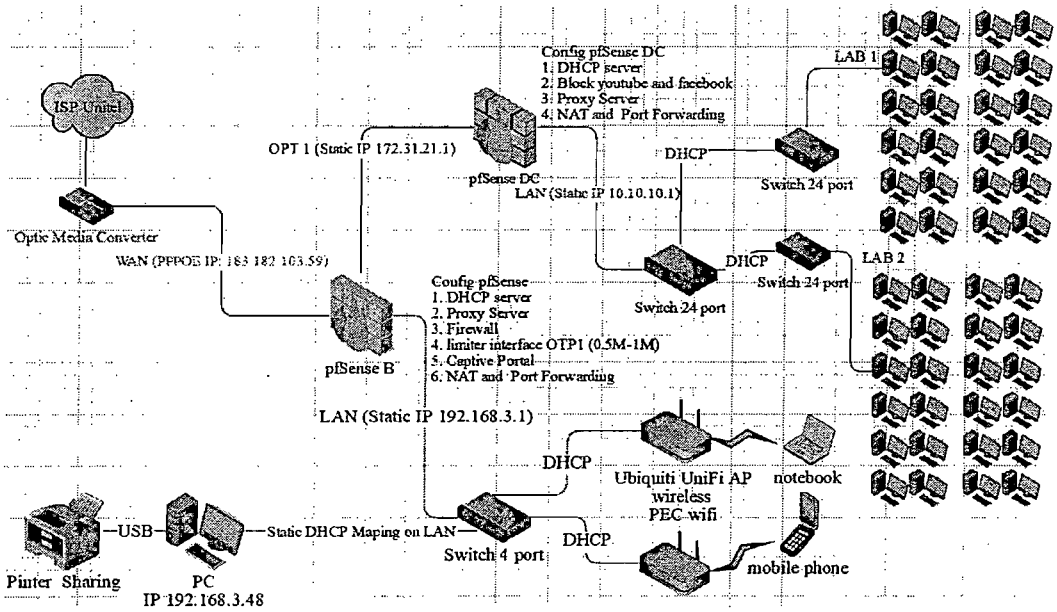


ภาพที่ 3-32 รายละเอียดระบบเครือข่ายในอาคาร A

2. การออกแบบระบบเครือข่ายในอาคาร B และ C, D แสดงดังภาพที่ 3-33, 3-34



ภาพที่ 3-33 การออกแบบระบบเครือข่ายในอาคาร B และ C, D



ภาพที่ 3-34 รายละเอียดระบบเครือข่ายในอาคาร B และ C, D

การติดตั้งและตั้งค่า pfSense, เว็บไซต์, และ Antivirus ในสถานที่จริง

การติดตั้ง pfSense ในสถานที่จริงมันคล้ายกับการติดตั้งในสถานที่จำลองต่างกันเพียงแค่หมายเลขไอพี และ Hardware บางส่วน ดังนี้

ตารางที่ 3-2 รายละเอียดการติดตั้ง และ ตั้งค่า (แสดงเฉพาะส่วนที่ตั้งค่าต่างกัน)

รายละเอียดในการติดตั้ง	ค่าที่ใช้สำหรับการติดตั้งในส่วนที่ต่างกัน	
	สถานที่ทดลอง	สถานที่จริง
4.1 ติดตั้ง pfSense และ การกำหนดค่า interface	IP Interface WAN (10.16.72.12) IP Interface LAN (172.31.21.1)	IP Interface WAN 1. อาคาร A (183.182.105.144) 2. อาคาร B (183.182.103.59) 3.อาคาร C, D (172.31.21.2) IP Interface LAN 1. อาคาร A (192.168.254.1) 2. อาคาร B (192.168.3.1) 3.อาคาร C, D (10.10.10.1) IP Interface OPT 1.อาคาร B (172.31.21.1)
4.2 กำหนดค่า pfSense โดยใช้ wizard	IPv4 Configuration Type (ใน interface WAN): Static	IPv4 Configuration Type (ใน interface WAN): PPPoE
4.3 กำหนดค่า DHCP server	DHCP server (172.31.21.10- 172.31.21.245)	DHCP server อาคาร A (192.168.254.10-192.168.254.32) DHCP server อาคาร B (192.168.3.10-192.168.3.245) DHCP server อาคาร C,D (10.10.10.10-10.10.10.70)
4.7 ตั้งค่าจำกัดแบนด์วิดท์ Download และ Upload ของ interface OTP1 (0.5M-1M)	การจำกัดเฉพาะหมายเลขโดยกำหนดให้ Download และ Upload (60M-30M)	การจำกัดแบนด์วิดท์ใน interface OTP1 ของอาคาร A โดยกำหนดให้ Download และ Upload (0.5M-1M)

ในตารางด้านล่างนี้ผู้ทำงานนิพนธ์สรุปการติดตั้งเครื่องแม่ข่าย pfSense และ Web Server รวมถึงเครือข่ายไร้สายในสถานที่จริง (รายละเอียดขั้นตอน และ วิธีการติดตั้งอยู่ในภาคผนวก)

ตารางที่ 3-3 รายละเอียดการติดตั้ง และ ตั้งค่า ในสถานที่จริง

รายละเอียดในการติดตั้ง และ ตั้งค่า	อาคาร	ภาคผนวก
1. ติดตั้ง pfSense และ การกำหนดค่า interface	A, B, และ C, D	ก.1
2. กำหนดค่า pfSense โดยใช้ Wizard	A, B, และ C, D	ก.2
3. กำหนดค่า DHCP server	A, B, และ C, D	ก.3.1
4. ตั้งค่าเครื่องแม่ข่าย Proxy บริการเก็บแคชของข้อมูลเว็บไซต์	A, B, และ C, D	ก.4
5. การตั้งค่า Captive Portal Network บริการหน้าเว็บไซต์เริ่มต้นเมื่อเข้าสู่เครือข่าย LAN และ Wireless LAN เพื่อยืนยันตัวตน	A และ B	ก.5
6. ตั้งค่าเครื่องแม่ข่าย RADIUS เพื่อกำหนดรายชื่อผู้ใช้ที่สามารถเข้าถึงเครือข่าย	A	ก.6
7. ตั้งค่าจำกัดแบนด์วิดท์ Download และ Upload ของ interface OTP1 (0.5M-1M)	B	ก.8
8. ตั้งการค่าบล็อก YouTube และ Facebook ใน pfSense เพื่อกำจัดเข้าถึงเว็บไซต์	C และ D	ก.9
9. ตั้งค่า NAT และ Port Forwarding เพื่อส่งข้อมูลไปยังเครื่องแม่ข่าย pfSense และ web บริการ IP ภายในวิทยาลัย	A, B, และ C, D	ก.10
10. ตั้งค่า IPsec VPN เพื่อเพิ่มความปลอดภัยของการส่งผ่านข้อมูล	A	ก.14
11. ติดตั้ง และ ตั้งค่า OpenVPN เพื่อบริการเครือข่ายเสมือน	A	ก.15
12. การติดตั้งเครื่องแม่ข่าย และ การสร้างเว็บไซต์ขององค์กร	A	ให้อ่านตาม ข้อ 2.16.2-2.16.4 ของบทที่ 3

13. บริการป้องกัน Virus (Antivirus)

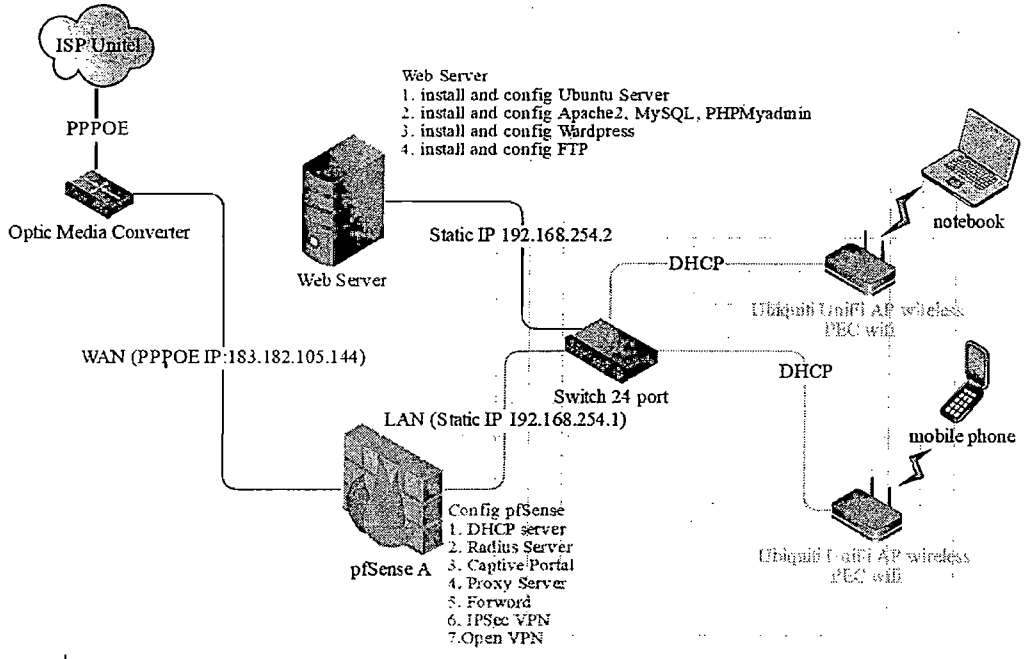
เพื่อเป็นการป้องกัน virus เบื้องต้นให้กับเครื่อง computer ต่าง ๆ ของอาจารย์ในวิทยาลัย ดังนั้นผู้ทำงานนิพนธ์ ได้ติดตั้ง Antivirus รุ่น avast_free_antivirus_setup_online ให้กับอาจารย์ในวิทยาลัย

บทที่ 4

ผลการดำเนินการติดตั้งและกำหนดค่าของ pfSense

หลังจากการติดตั้งและกำหนดค่าระบบเครือข่ายให้กับวิทยาลัยพละศึกษา ผู้ทำงานนิพนธ์ได้ทดสอบประสิทธิภาพของเครือข่ายในอาคารต่าง ๆ โดยมีรายละเอียดดังนี้

โครงสร้างระบบเครือข่ายที่ 1 (ภายในอาคาร A)



ภาพที่ 4-1 โครงสร้างของระบบเครือข่ายอาคาร A

ผู้ทำงานนิพนธ์ได้ออกแบบการทดสอบในส่วนต่าง ๆ 8 ส่วนต่อไปนี้

1.1 การวัดความล่าช้าสำหรับการส่งข้อมูลภายในเครือข่ายอาคาร A

1.2 การวัดแบนด์วิดท์ของอินเทอร์เน็ต (อัพโหลดและดาวน์โหลด)

1.3 การทดสอบ Port forwarding และ กฎไฟร์วอลล์

1.4 การทดสอบยืนยันตัวตนก่อนการเข้าใช้ Internet (Authentication) โดยใช้ Captive Portal

1.5 การทดสอบเครื่องแม่ข่าย RADIUS

1.6 การทดสอบ IPsec VPN

1.7 การทดสอบ OpenVPN

1.8 การทดสอบเครื่องแม่ข่าย proxy

1. **การวัดความล่าช้าของของระบบเครือข่ายภายในอาคาร A**

การทดสอบเครือข่าย Wi-Fi ภายในอาคาร A รายละเอียดดังต่อไปนี้

1. ผู้ทำงานนิพนธ์ทดสอบโดยใช้ ไคลเอนต์ 10 ไคลเอนต์ ping ไปยังเครื่องแม่ข่าย pfSense โดยใช้คำสั่ง ping –n 50 192.168.254.1 แต่ละไคลเอนต์จะส่ง ping ไป 50 pingแล้วรอการตอบกลับมา จากผลการทดลองสรุปได้ว่าเครื่องแม่ข่ายตอบ pfSense ตอบกลับมา 100% ไม่มีแพ็กเกจสูญหาย โดยค่าเฉลี่ยของเวลาที่ ping เดินทางไปกลับ คือ 20.7 มิลลิวินาที ค่าเวลาที่ ping เดินทางไปกลับน้อยสุดเป็น 0 และ มากสุดที่ 454 มิลลิวินาทีดังรายละเอียดที่แสดงด้วยตาราง 4-1

ตารางที่ 4-1 การ ping จาก ไคลเอนต์ ไปที่ pfSense ping -n 50 192.168.254.1

การ ping จาก ไคลเอนต์ ไปที่ pfSense ping -n 50 192.168.254.1	เวลาที่เดินทางไปกับ (Round Trip Time) (ms)					
	Sent	Received	lost	Minimum	Maximum	Average
ไคลเอนต์ 1	50	50	0	0	11	1
ไคลเอนต์ 2	50	50	0	0	282	61
ไคลเอนต์ 3	50	50	0	2	10	3
ไคลเอนต์ 4	50	50	0	1	454	91
ไคลเอนต์ 5	50	50	0	1	41	2
ไคลเอนต์ 6	50	50	0	1	9	1
ไคลเอนต์ 7	50	50	0	1	6	1
ไคลเอนต์ 8	50	50	0	1	256	45
ไคลเอนต์ 9	50	50	0	1	5	1
ไคลเอนต์ 10	50	50	0	1	35	1

2. ผู้ทำงานนิพนธ์ทดสอบโดยใช้ไคลเอนต์ 10 ไคลเอนต์ ping ไปยัง Web Server โดยใช้คำสั่ง ping –n 50 192.168.254.2 แต่ละไคลเอนต์จะส่ง ping ไป 50 ping แล้ว รอการตอบกลับมา จากผลการทดลองสรุปได้ว่า Web Server ตอบกลับมา 100% ไม่มีแพ็กเกจสูญหาย โดยค่าเฉลี่ยของเวลาที่ ping เดินทางไปกลับ คือ 3.8 มิลลิวินาที ค่าเวลาที่ ping เดินทางไปกลับน้อยสุดเป็น 0 และมากสุดที่ 121 มิลลิวินาทีดังรายละเอียดที่แสดงด้วยตาราง 4-2

ตารางที่ 4-2 การ ping จาก ไคลเอนต์ ไปที่ web server ping -n 50 192.168.254.2

การ ping จาก ไคลเอนต์ ไปที่ web server ping -n 50 192.168.254.2	เวลาที่เดินทางไปกับ (Round Trip Time) (ms)					
	Sent	Received	lost	Minimum	Maximum	Average
ไคลเอนต์ 1	50	50	0	0	4	1
ไคลเอนต์ 2	50	50	0	0	4	1
ไคลเอนต์ 3	50	50	0	1	121	9
ไคลเอนต์ 4	50	50	0	0	117	15
ไคลเอนต์ 5	50	50	0	1	10	2
ไคลเอนต์ 6	50	50	0	1	40	2
ไคลเอนต์ 7	50	50	0	1	82	4
ไคลเอนต์ 8	50	50	0	0	4	1
ไคลเอนต์ 9	50	50	0	0	5	1
ไคลเอนต์ 10	50	50	0	0	34	2

3. ผู้ทำงานนิพนธ์ทดสอบโดยใช้ไคลเอนต์ 10 ไคลเอนต์ ping ไปยัง Google โดยใช้คำสั่ง ping –n www.Google .com แต่ละไคลเอนต์จะส่ง ping ไป 50 ping แล้วรอการตอบกลับมา จากผลการทดลองสรุปได้ว่า Google ตอบกลับมา 99% มีแพ็กเกจสูญหาย 5 แพ็กเกจ โดยค่าเฉลี่ยของเวลาที่ ping เดินทางไปกลับ คือ 88.998 มิลลิวินาที ค่าเวลาที่ ping เดินทางไปกลับน้อยสุดเป็น 56 และ มากสุดที่ 394 มิลลิวินาทีดังรายละเอียดที่แสดงด้วยตาราง 4-3

ตารางที่ 4-3 การ ping จาก ไคลเอนต์ ไปที่ Google ping -n 50 www.Google .com

การ ping จาก ไคลเอนต์ ไปที่ Google ping -n 50 www.Google .com	เวลาที่เดินทางไปกับ (Round Trip Time) (ms)					
	Sent	Received	lost	Minimum	Maximum	Average
ไคลเอนต์ 1	50	47	3	56	146	62
ไคลเอนต์ 2	50	50	0	56	179	82
ไคลเอนต์ 3	50	50	0	56	111	61
ไคลเอนต์ 4	50	49	1	299	394	304
ไคลเอนต์ 5	50	50	0	56	107	61
ไคลเอนต์ 6	50	50	0	57	71	59
ไคลเอนต์ 7	50	50	0	56	248	94
ไคลเอนต์ 8	50	50	0	56	83	58
ไคลเอนต์ 9	50	49	1	56	111	61
ไคลเอนต์ 10	50	50	0	56	80	59

4. ผู้ทำงานนิพนธ์ทดสอบโดยใช้ไคลเอนต์ 10 ไคลเอนต์ ping ไปยัง YouTube โดยใช้คำสั่ง ping –n www. YouTube.com แต่ละไคลเอนต์จะส่ง ping ไป 50 ping แล้วรอการตอบกลับมา จากผลการทดลองสรุปได้ว่า YouTube ตอบกลับมา 99.4% มีแพ็กเกจสูญหาย 3 แพ็กเกจ โดยค่าเฉลี่ยของ เวลาที่ ping เดินทางไปกลับ คือ 48.84 มิลลิวินาทีค่าเวลาที่ ping เดินทาง ไปกลับน้อยสุดเป็น 4 และ มากสุดที่ 311 มิลลิวินาทีดังรายละเอียดที่แสดงด้วยตาราง 4-4

ตารางที่ 4-4 การ ping จาก ไคลเอนต์ ไปที่ YouTube ping -n 50 www.YouTube.com

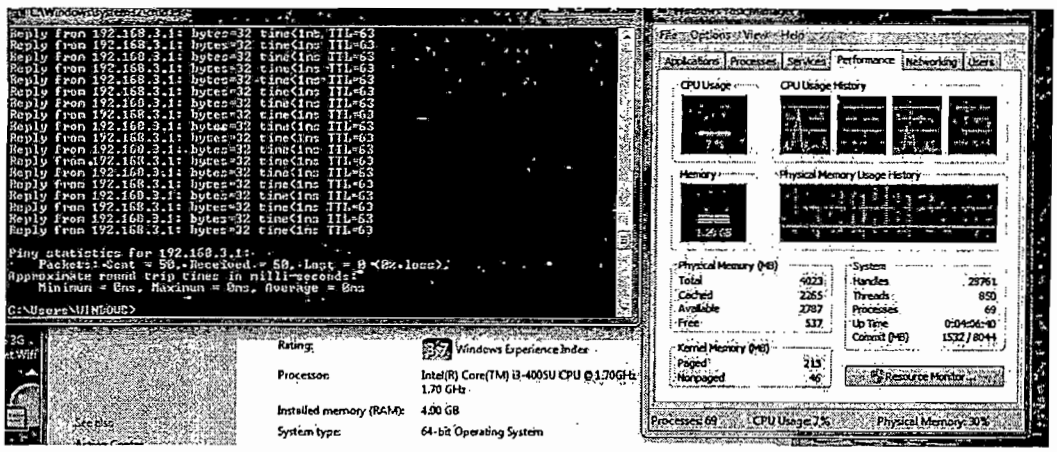
การ ping จาก ไคลเอนต์ ไปที่ YouTube ping -n 50 www.YouTube.com	เวลาที่เดินทางไปกับ (Round Trip Time) (ms)					
	Sent	Received	lost	Minimum	Maximum	Average
ไคลเอนต์ 1	50	47	3	4	27	6
ไคลเอนต์ 2	50	50	0	4	158	17
ไคลเอนต์ 3	50	50	0	300	311	302
ไคลเอนต์ 4	50	50	0	4	32	8
ไคลเอนต์ 5	50	50	0	4	43	8
ไคลเอนต์ 6	50	50	0	4	238	39
ไคลเอนต์ 7	50	50	0	4	39	8
ไคลเอนต์ 8	50	50	0	4	79	8
ไคลเอนต์ 9	50	50	0	12	256	86
ไคลเอนต์ 10	50	50	0	4	22	7

5. ผู้ทำงานนิพนธ์ทดสอบโดยใช้ไคลเอนต์ 10 ไคลเอนต์ ping ไปยัง Facebook โดยใช้คำสั่ง ping –n www. Facebook.com แต่ละไคลเอนต์จะส่ง ping ไป 50 ping แล้วรอการตอบกลับมา จากผลการทดลองสรุปได้ว่า Facebook ตอบกลับมา 99.4% มีแพ็กเกจสูญหาย 3 แพ็กเกจโดยค่าเฉลี่ยของเวลาที่ ping เดินทางไปกลับ คือ 254.526 มิลลิวินาที ค่าเวลาที่ ping เดินทางไปกลับน้อยสุดเป็น 198 และ มากสุดที่ 744 มิลลิวินาทีดังรายละเอียดที่แสดงด้วยตาราง 4-5

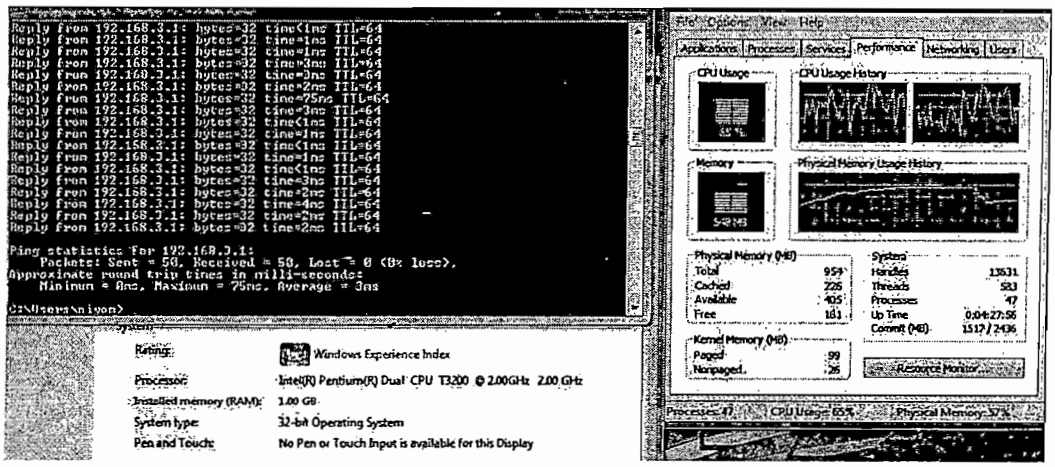
ตารางที่ 4-5 การ ping จาก ไคลเอนต์ ไปที่ Facebook ping -n 50 www.Facebook.com

การ ping จาก ไคลเอนต์ ไปที่ Facebook ping -n 50 www.Facebook.com	เวลาที่เดินทางไปกับ (Round Trip Time) (ms)					
	Sent	Received	lost	Minimum	Maximum	Average
ไคลเอนต์ 1	50	47	3	223	297	229
ไคลเอนต์ 2	50	50	0	223	345	233
ไคลเอนต์ 3	50	50	0	223	461	255
ไคลเอนต์ 4	50	50	0	223	268	228
ไคลเอนต์ 5	50	50	0	221	251	225
ไคลเอนต์ 6	50	50	0	222	744	392
ไคลเอนต์ 7	50	50	0	221	511	321
ไคลเอนต์ 8	50	50	0	222	251	225
ไคลเอนต์ 9	50	50	0	221	290	224
ไคลเอนต์ 10	50	50	0	198	381	227

สรุป ผลการทดสอบ ping ไปที่เครื่องแม่ขาย pfSense, Web Server, Google, YouTube, และ Facebook พบว่า แต่ละไคลเอนต์ได้รับ ping reply กลับมาในระยะเวลาแตกต่างกัน เพราะว่า เครื่อง computer ของแต่ละเครื่องจะมีสมรรถนะต่างกัน และ ขณะทดสอบ CPU ของแต่ละเครื่องทำงานไม่เท่ากัน ภาพที่ 4-2 และ 4-3 แสดงผลการทดสอบของไคลเอนต์ตัวอย่าง



ภาพที่ 4-2 ผลการทดสอบ ping ไปที่ Server จากไคลเอนต์ตัวที่ 1 (Intel (R) Core (TM) i3 และ RAM 4GB) ได้ค่าเฉลี่ย และ ค่ามากที่สุดที่ 0 มิลลิวินาที



ภาพที่ 4-3 ผลการทดสอบ ping ไปที่ Server จากไคลเอนต์ตัวที่ 1 (Intel (R) Pentium (R) และ RAM 1GB) ได้ค่าค่าเฉลี่ย ที่ 3 มิลลิวินาที และ ค่ามากที่สุดที่ 75 มิลลิวินาที

จากภาพ 4-2 และ 4-3 ความล่าช้า (Round trip time) ที่พบในการทดสอบ pingเกือบทั้งหมดมีค่าประมาณ 0-3 มิลลิวินาที เท่านั้น แต่ ในเครื่องที่มี RAM น้อย และ มีการใช้ CPU มาก ความล่าช้าที่ได้จากการทดสอบ ping มีค่า Maximum มากดัง 75 มิลลิวินาที (เหตุการณ์ลักษณะนี้เกิดขึ้นประมาณ 1-2 ครั้งในการทดสอบ ping 50 ครั้ง)

สรุป การเปรียบเทียบค่าเฉลี่ยที่ได้จากผลการทดสอบ ping ของไคลเอนต์ไปที่ pfSense, Web Server, www. Google.com, www.YouTube.com, และ www.Facebook.com จะเห็นว่าความล่าช้าเฉลี่ย (Round Trip Tine) ที่เกิดจากการ ping Facebook YouTube Google ซึ่งเป็น Server อยู่ภายนอกจะมีค่ามากกว่าเวลาที่ใช้สำหรับ ping pfSense และ Web Server ประมาณ 30-200 มิลลิวินาที

โดย Facebook จะใช้เวลาตอบ ping นานกว่า YouTube และ Google จากการทดสอบ tracert ไปที่เครื่องแม่ข่ายของ Facebook จากไคลเอนต์ที่อยู่ในเครือข่ายในอาคาร A พบว่าเส้นทางประกอบด้วย 15 router โดยเครื่องแม่ข่าย ของ Facebook อยู่ที่ประเทศ United States ตามข้อมูลจากเว็บไซต์ http://www.speedguide.net/ip/66.220.146.36/ ดังภาพที่ 4-4

```
C:\Users\yangchiamoua>tracert www.facebook.com

Tracing route to star-mini.c10r.facebook.com [66.220.146.36]
over a maximum of 30 hops:

  1    1 ms    <1 ms    <1 ms  pfSense.localdomain [192.168.254.1]
  2   40 ms     5 ms     5 ms  unitel.com.la [183.182.97.229]
  3    5 ms     4 ms     *     unitel.com.la [183.182.97.35]
  4    9 ms     5 ms     *     183.182.96.109
  5  292 ms   313 ms   297 ms  ge-1-2-3-xcr1.hkg.cw.net [203.169.57.1]
  6  300 ms   221 ms   265 ms  ae44.pr01.hkg3.tfbnw.net [103.4.96.114]
  7  264 ms     *      328 ms  ae0.bb01.hkg1.tfbnw.net [31.13.28.216]
  8  341 ms   406 ms.  304 ms  ae13.bb01.hnd1.tfbnw.net [31.13.26.21]
  9    *        *      328 ms  be6.bb02.lax1.tfbnw.net [31.13.24.153]
 10  258 ms   305 ms   304 ms  ae7.bb03.prn2.tfbnw.net [31.13.24.3]
 11  239 ms   392 ms     *     ae43.dr08.prn2.tfbnw.net [31.13.31.127]
 12    *        *        *     Request timed out.
 13    *        *        *     Request timed out.
 14    *        *        *     Request timed out.
 15  277 ms     *        *     unitel.com.la [183.182.105.144]
 16  293 ms   303 ms   304 ms  edge-star-mini-shv-18-prn1.facebook.com [66.220.146.36]

Trace complete.

C:\Users\yangchiamoua>
```

ภาพที่ 4-4 ผลการ tracert ไปที่เครื่องแม่ข่ายของ Facebook

ส่วนผลทดสอบ tracert www. YouTube.com พบว่าเส้นทางประกอบด้วย 8 router โดยเครื่องแม่ข่ายของ Google อยู่ที่ประเทศ Lao People's Democratic Republic ตามข้อมูลจากเว็บไซต์ (http://www.speedguide.net/ip/183.182.96.154 /) ดังภาพที่ 4-5 ด้านล่าง

```
C:\Users\yangchiamoua>tracert www.youtube.com

Tracing route to youtube-ui.l.google.com [183.182.96.154]
over a maximum of 30 hops:

  1    1 ms     1 ms     1 ms  pfSense.localdomain [192.168.254.1]
  2    9 ms     4 ms     6 ms  unitel.com.la [183.182.97.229]
  3    9 ms     8 ms     8 ms  unitel.com.la [183.182.97.35]
  4   10 ms     *       94 ms  unitel.com.la [183.182.97.121]
  5    9 ms     4 ms     4 ms  183.182.96.5
  6   10 ms     5 ms     4 ms  183.182.96.154

Trace complete.
```

ภาพที่ 4-5 ผลการ tracert ไปที่เครื่องแม่ข่ายของ YouTube

ตารางที่ 4-6 ด้านล่างสรุปค่าเฉลี่ยความล่าช้าไปยังเครื่องแม่ข่ายต่าง ๆ

เครื่องแม่ข่าย	ค่าเฉลี่ย Round Trip Time
เครื่องแม่ข่าย web	3.8
เครื่องแม่ข่าย pfSense	20.7
เครื่องแม่ข่าย YouTube	48.84
เครื่องแม่ข่าย Google	88.998
เครื่องแม่ข่าย Facebook	254.526

ส่วนการ ping ไปที่ pfSense และ Web Serve เป็นการ ping ภายในเครือข่ายใช้เวลาตอบกลับน้อย เพราะว่าไม่ได้ออกไปข้างนอก และ ไม่ได้ผ่านไฟร์วอลล์

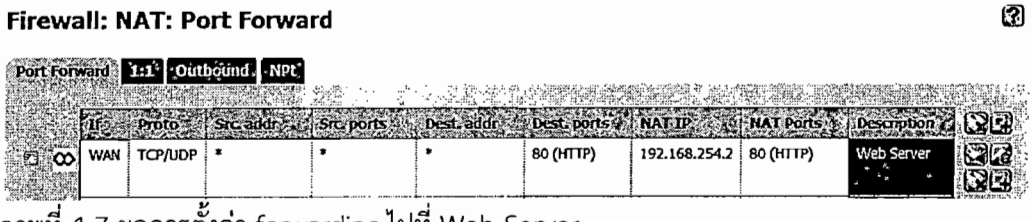
2. การวัดแบนด์วิดท์ของอินเทอร์เน็ต (อัพโหลดและดาวน์โหลด)

วิทยาลัยพลศึกษา ใช้บริการของ Unitel ซึ่งให้บริการ Internet ที่ความเร็วสูงสุดในการอัพโหลด สูงสุด 6 Mbps และ ที่ความเร็วในการดาวน์โหลดสูงสุดที่ 6 Mbps การทดสอบโดยใช้ www.speedtest.net พบว่า ปริมาณแบนด์วิดท์ในการอัพโหลด 5.58 Mbps และดาวน์โหลดอยู่ที่ 5.93 Mbps ซึ่งใกล้เคียงกับแบนด์วิดท์ที่คาดว่าจะรับจาก ISP ดังภาพที่ 4-6

ภาพที่ 4-6 ผลการทดสอบปริมาณแบนด์วิดท์สำหรับอัพโหลด และ ดาวน์โหลด

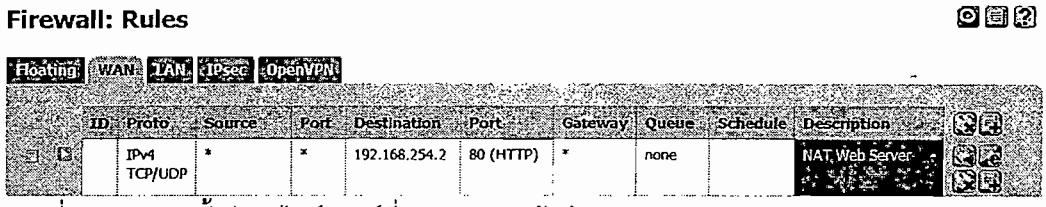
3. การทดสอบ Port forwarding และ กฎไฟร์วอลล์

1. การทดสอบ Port forwarding เพื่ออนุญาตให้ผู้ใช้เข้าถึง Web Server โดยมีการทำ Port forwarding ที่กฎไฟร์วอลลของ pfSense โดยเครื่องไคลเอนต์ภายในและภายนอกที่มีหมายเลขไอพีและ Port ต้นทางอะไรก็ได้ สามารถเข้าถึง Web Server ที่ และ Port 80 (HTTP) และ NTA จะส่งข้อมูลไปที่ Web Server ที่หมายเลขไอพี 192.168.254.2 ดังภาพที่ 4-7



ภาพที่ 4-7 ผลการตั้งค่า forwarding ไปที่ Web Server

หลังการกำหนด Port forwarding สำเร็จ pfSense จะสร้างกฎไฟร์วอลล์ (โดยอัตโนมัติ) ที่อนุญาตให้มีการเข้าถึง Web Server กฎนี้อนุญาตให้เครื่องใดก็ได้ทั้งภายในและภายนอก จาก Port อะไรก็ได้ ให้สามารถเข้าถึง Web Server ที่อยู่หมายเลขไอพีปลายทาง 192.168.254.2 และ Port 80 (HTTP) ดังภาพ 4-8

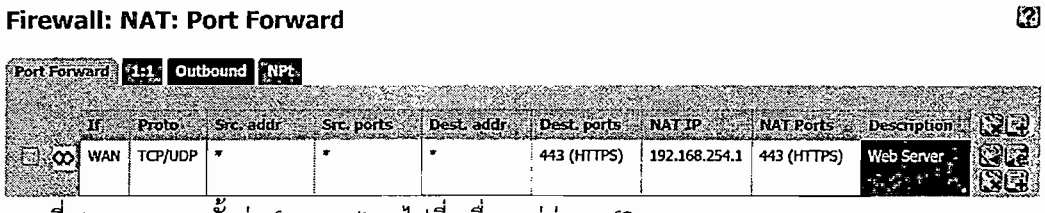


ภาพที่ 4-8 ผลการตั้งค่ากฎไฟร์วอลล์ที่อนุญาตการเข้าถึง Web Server

ผู้ใช้สามารถเข้าถึง web Server ได้โดยใช้ชื่อโดเมน www.pec29052009.edu.la หมายเลขไอพี 183.182.105.144 ซึ่งผู้ทำงานนิพนธ์ได้จดทะเบียนกับ Internet แห่งประเทศลาวดังภาพที่ 4-9

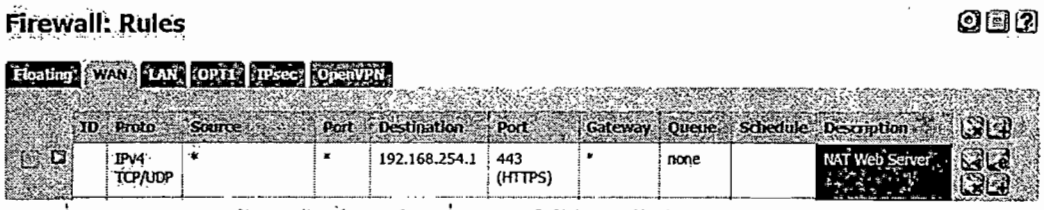
ภาพที่ 4-9 ผลการทดสอบเข้าเว็บไซด์หลังจากมีการอนุญาตกฎไฟร์วอลล์

2. การทดสอบ Port forwarding ที่เข้าถึงเครื่องแม่ข่าย pfSense มีการทำ Port forwarding ที่ pfSense เพื่อกำหนดเงื่อนไขของไฟร์วอลล์ โดยอนุญาตให้เครื่องไคลเอนต์ภาย ในและภายนอกที่มีหมายเลขไอพีและ Port ต้นทางอะไรก็ได้ สามารถเข้าถึงเครื่องแม่ข่าย pfSense ที่ Port 443 (HTTPS) โดย NAT จะ forward ข้อมูลไปที่หมายเลขไอพี 192.168.254.1 ดังภาพที่ 4-10



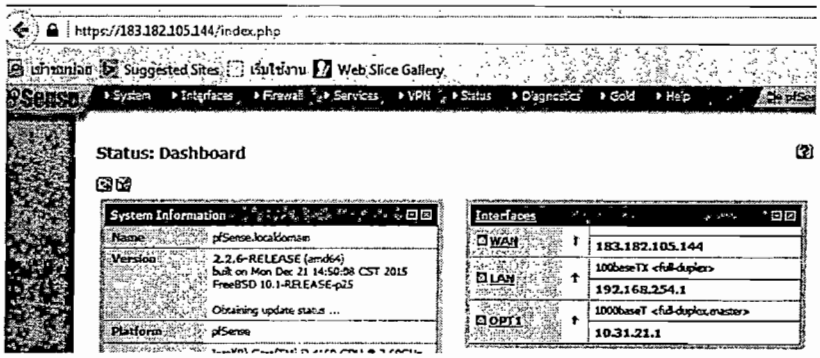
ภาพที่ 4-10 ผลการตั้งค่า forwarding ไปที่เครื่องแม่ข่าย pfSense

หลังกำหนด Port forwarding สำเร็จแล้ว pfSense จะสร้างกฎไฟร์วอลล์ (โดยอัตโนมัติ) ใน Interface WAN โดยอนุญาตให้มีการเข้าถึงเครื่องแม่ข่าย pfSense กฎนี้อนุญาตให้เครื่องใดก็ได้ทั้งภายในและภายนอก จาก Port ต้นทางอะไรก็ได้ ให้สามารถเข้าถึงเครื่องแม่ข่าย pfSense ที่อยู่หมายเลขไอพีปลายทาง 192.168.254.1 และ Port 443 (HTTPS) ดังภาพ 4-11



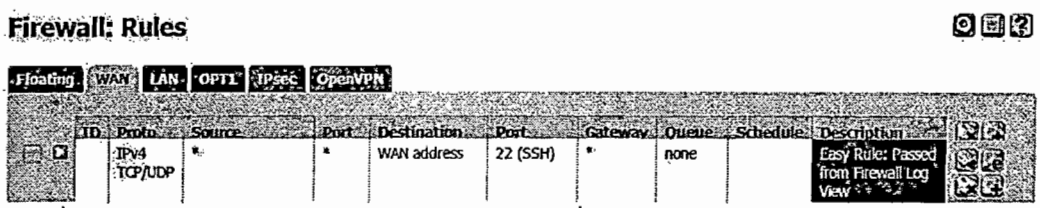
ภาพที่ 4-11 ผลการ สร้างกฎไฟร์วอลล์อยู่ที่อนุญาตให้มีการเข้าถึงตัว pfSense

การทดสอบกฎข้างต้นโดยให้ไคลเอนต์ที่อยู่ข้างนอกเครือข่าย (เช่น ไคลเอนต์อยู่ในมหาวิทยาลัยบูรพา) พบว่าไคลเอนต์สามารถเข้าถึงหน้าเว็บ pfSense โดยใช้ URL https://183.182.105.144 ดังภาพ 4-12



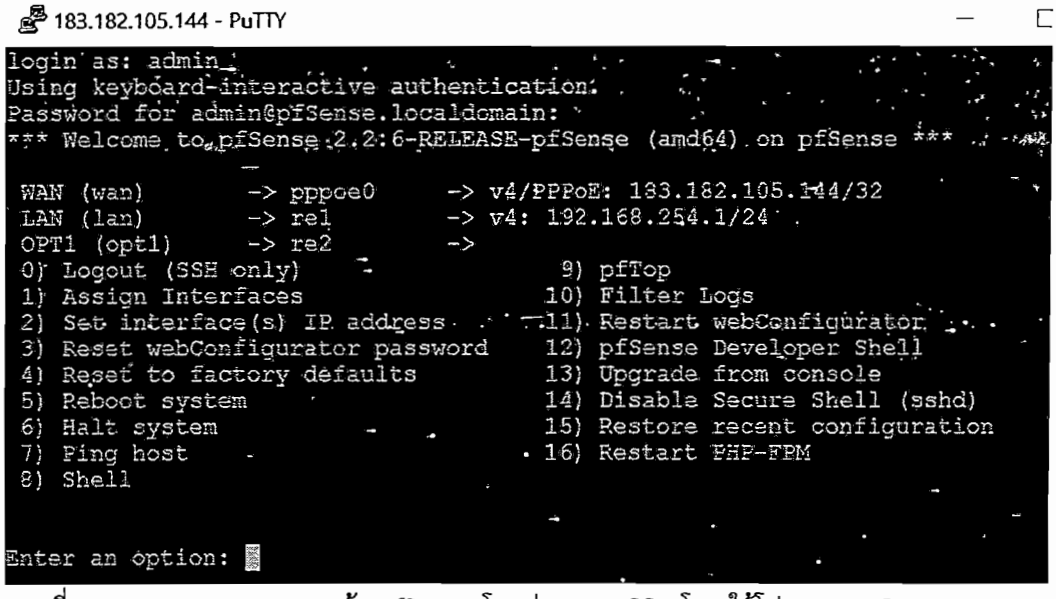
ภาพที่ 4-12 ผลการทดสอบการให้เข้าถึง pfSense หลังจากทำ Port forwarding

3. ผู้ทำงานนิพนธ์นี้ได้ทดสอบการเข้าถึง pfSense ผ่านช่องทาง SSH จากเครื่องที่อยู่นอกเครือข่ายโดยใช้โปรมแกรม Putty โดยผู้ทำงานนิพนธ์ได้สร้างกฎไฟร์วอลล์ที่อนุญาตให้เข้าถึงตัว SSH daemon ของ pfSense โดยกฎในภาพที่ 4-10 จะอนุญาตให้เครื่องใดก็ได้ทั้งภายในและภายนอก จาก Port ต้นทางอะไรก็ได้ ให้สามารถเข้าถึงที่อยู่หมายเลขไอพีปลายทางเป็น WAN address และ Port 22 (ssh) ดังภาพที่ 4-13



ภาพที่ 4-13 ผลการกำหนดค่าในการสร้างกฎไฟร์วอลล์ที่อนุญาตให้เข้าถึงตัว SSH ของ pfSense

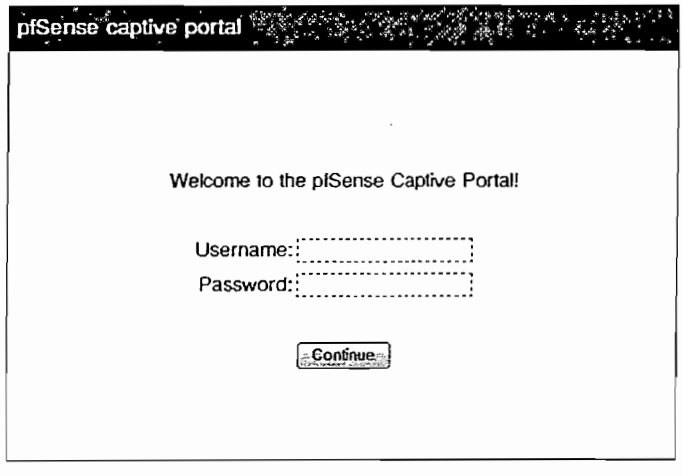
การทดสอบกฎข้างต้น พบว่าไคลเอนต์สามารถเข้าถึง pfSense โดยใช้โปรมแกรม Putty ดังภาพที่ 4-14



ภาพที่ 4-14 ผลการทดสอบการเข้า pfSense โดยช่องทางง SSH โดย ใช้โปรมแกรม Putty

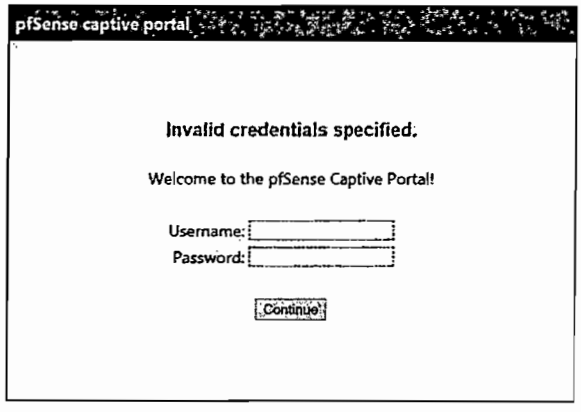
4. **การทดสอบยืนยันตัวตนก่อนการเข้าใช้ Internet (Authentication) โดยใช้ Captive Portal**

ผู้ทำงานนิพนธ์ ได้ใช้ Notebook ที่อยู่ภายในเครือข่ายทำการทดสอบระบบการยืนยันตัวตน โดยการเข้าถึงใดเว็บหนึ่ง (เช่น เข้าเว็บ Google) จากนั้นก็ปรากฏหน้าเว็บบราวเซอร์ที่มีช่องให้ใส่ชื่อผู้ใช้ และ รหัสผู้ใช้เพื่อให้ผู้ใช้ยืนยันตัวตน ดังภาพที่ 4-15



ภาพที่ 4-15 ผลการแสดงหน้าเว็บบราวเซอร์ที่มีช่องให้ใส่ชื่อผู้ใช้ และ รหัสผู้ใช้

เมื่อทดสอบใส่รหัสผิด Captive Portal จะแจ้งเตือนว่าชื่อผู้ใช้ และ รหัสไม่ถูกต้องให้ระบุใหม่ ดังภาพ 4-16



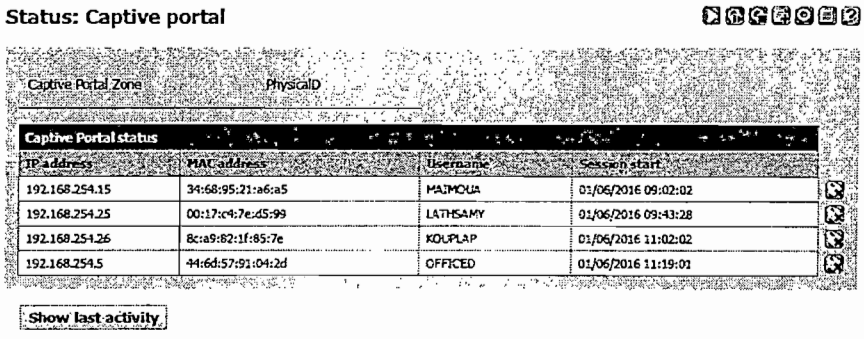
ภาพที่ 4-16 ผลการแสดงหน้าเว็บบราวเซอร์ที่ใส่ชื่อผู้ใช้และรหัสผู้ใช้ผิด

ถ้าใส่รหัสถูกต้องเราก็สามารถเข้าใช้ Internet ได้ ดังภาพที่ 4-17

ภาพที่ 4-17 ผลการทดสอบระบบ Authentication หลังจากผู้ใช้ใส่ชื่งผู้ใช้ และ รหัสผ่านถูกต้อง

หลังจากผู้ใช้ยืนยันตัวตนเข้าในระบบแล้ว ผู้ดูแลระบบสามารถตรวจสอบว่ามีผู้ใช้ใดบ้างที่กำลังใช้งานมีหมายเลขไอพีและหมายเลข MAC อะไรบ้าง เข้าเมื่อเวลาและวันที่เท่าไร เช่น ในเวลา 09:02:02 ของวันที่ 10/06/2015 มีผู้ใช้ MAIMOUA ที่มีหมายเลขไอพี 192.168.254.15 และ

หมายเลข MAC 34:68:95:21:a6:a5 กำลังใช้งานอยู่ ดังที่แสดงดังภาพที่ 4-18

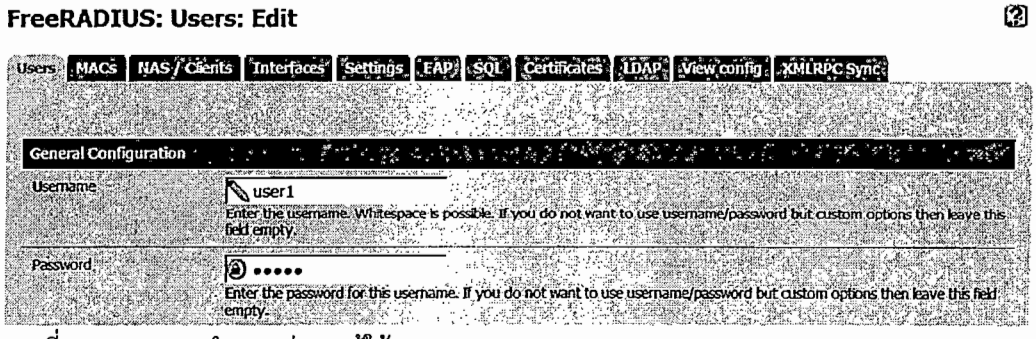


ภาพที่ 4-18 ผลการแสดงผู้ใช้ที่กำลังเข้าใช้งานเครือข่ายด้วยระบบ Authentication โดย Captive Portal

5. การทดสอบ RADIUS Server

ผู้ทำงานนิพนธ์ไม่ได้เลือกใช้เครื่องแม่ข่าย RADIUS ที่ pfSense ได้เตรียมไว้ให้เพื่อให้บริการการยืนยันตัวตน อย่างไรก็ตามผู้ทำงานนิพนธ์ได้ติดตั้ง และ ทดสอบการใช้งานเบื้องต้นเพื่อรองรับการใช้งานในอนาคต

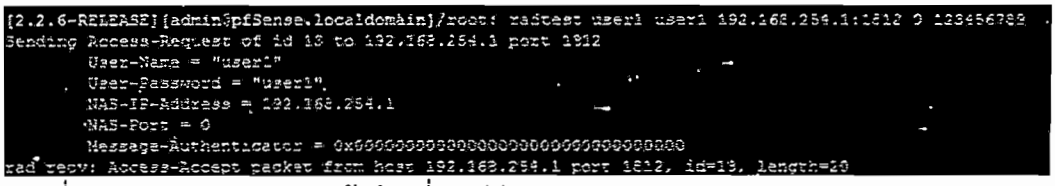
เครื่องแม่ข่าย RADIUS ช่วยให้ผู้ดูแลระบบกำหนดชื่อและรหัสให้แก่ผู้ใช้เวลาล็อกอิน หรือ Authentication เข้าระบบ ในการทดสอบนี้ ผู้ทำงานนิพนธ์ทดลองใช้เครื่องแม่ข่าย RADIUS โดยกำหนด ชื่อ user1 และ รหัสผ่าน user1 ดังภาพ 4-19



ภาพที่ 4-19 ผลการกำหนดค่าของผู้ใช้งาน RADIUS

ผู้ทำงานนิพนธ์ได้ตรวจสอบชื่อผู้ใช้และรหัสของผู้ใช้ที่เครื่องแม่ข่าย RADIUS โดยผู้ทำงานนิพนธ์เข้าถึงบรรทัดคำสั่ง (command line) ของ pfSense แล้วกดเลข 8 เพื่อเข้าไปเขียนคำสั่งตรวจเช็คว่า user1 มีสิทธิ์เข้าถึงเครื่องแม่ข่าย RADIUS โดยใช้คำสั่ง redtest user1 user1 192.168.254.1:1812 0 123456789 โดย user1 คือชื่อผู้ใช้ และ รหัสผ่าน 192.168.254.1 คือ หมายเลขไอพีของเครื่องแม่ข่าย 1812 คือ Port ของเครื่องแม่ข่าย RADIUS และ 123456789 คือ

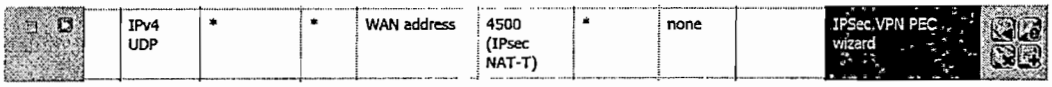
รหัสผ่านของเครื่องแม่ข่าย RADIUS ผู้เข้าใช้ user1 ที่มีสิทธิ์เข้าถึงเครื่องแม่ข่าย RADIUS ระบบจะแสดงคำว่า Access-Accept ดังภาพที่ 4-20



ภาพที่ 4-20 ผลการทดสอบการเข้าถึงเครื่องแม่ข่าย RADIUS

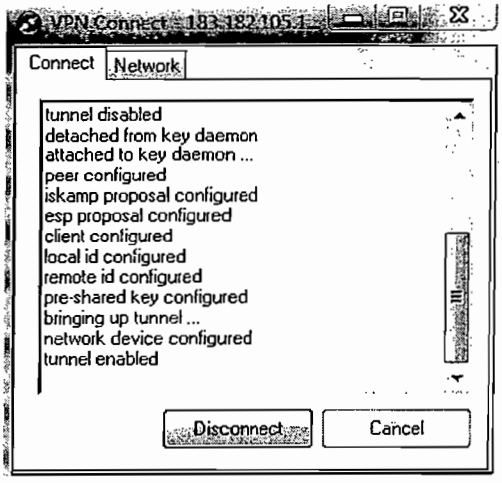
6. การทดสอบ IPsec VPN

ผู้ทำงานนิพนธ์นี้ ได้ใช้ Notebook ที่อยู่ข้างนอกเครือข่ายเพื่อทดสอบการเข้าถึงเครือข่ายภายในวิทยาลัยผ่าน VPN โดยใช้ซอฟต์แวร์ชื่อ IPsec VPN ที่ต้องมีการกำหนดค่าระหว่าง IPsec VPN Client และ IPsec VPN ที่ pfSense (ตามที่ระบุไว้ในบทที่ 3) ต้องอนุญาตให้ให้ผู้ใช้ทั่วไปเข้าถึง IPsec VPN ผ่านไฟร์วอลล์ เช่น อนุญาตให้เครื่องที่มีโปรโตคอล UDP จาก Port ต้นทางอะไรก็ได้ ให้ไปที่จุดหมายปลายทางหมายไอพี WAN ที่ Port 4500 (IPsec NAT-T) ดังภาพที่ 4-21



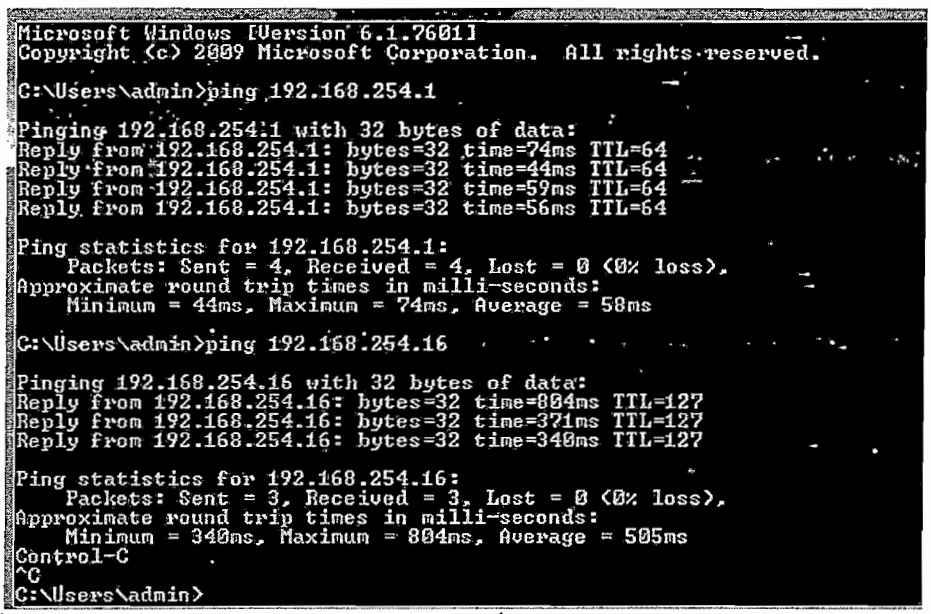
ภาพที่ 4-21 ผลการสร้างกฎไฟร์วอลล์เพื่ออนุญาตให้ไคลเอนต์ เข้าถึง pfSense ผ่าน IPsec VPN

ผลการเชื่อมต่อ IPsec VPN โดยที่ใช้ Notebook ที่อยู่ข้างนอกเครือข่าย (เช่น เราอยู่ในมหาวิทยาลัยบูรพา) และใช้ IPsec VPN ไคลเอนต์ (โปรแกรมชื่อ VPN connect) เข้าถึง pfSense ได้ ดังภาพที่ 4-22



ภาพที่ 4-22 แสดงเวลาที่ทำการเชื่อมต่อไปที่ pfSense ผ่าน IPsec VPN

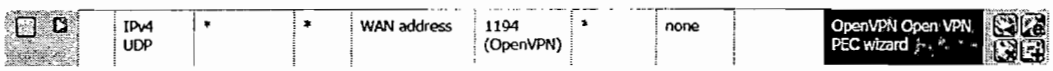
เราสามารถ ping ไปเครื่องภายในเครือข่ายข้างในได้เช่น ping ไปหาไอพีของ pfSense และ หมายเลขไอพีของเครื่อง PC ที่กำลังทำงานอยู่ ดังภาพที่ 4-23



ภาพที่ 4-23 ผลการทดสอบในเวลาการ ping ไปยังเครื่องภายในเครือข่าย

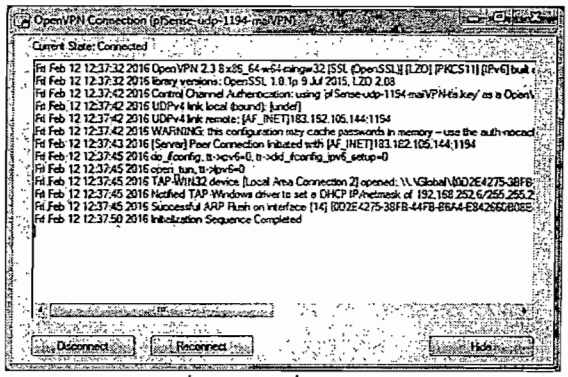
7. การทดสอบ OpenVPN

OpenVPN เป็นอีกทางเลือกหนึ่งที่ผู้จัดทำได้เลือกมาใช้บริการVPN โดยผู้ทำงานนิพนธ์ได้ใช้ Notebook ที่อยู่ข้างนอกเครือข่ายทำการทดสอบการเข้าถึงเครือข่ายภายในโดยใช้ OpenVPN โดยต้องมีการกำหนดค่าที่ pfSense ก่อน จากนั้นผู้ทำงานนิพนธ์จะต้องนำค่า Config ที่ได้จาก pfSense ไปใส่ในไคลเอนต์ของ OpenVPN เพื่อให้ไคลเอนต์เชื่อมต่อกับ OpenVPN (ตามที่ระบุไว้ในบทที่ 3) และกำหนดกฎเพื่ออนุญาตใช้ OpenVPN ผ่านไฟร์วอลล์ เช่น อนุญาตให้เครื่องที่ใช้โปรโตคอล UDP จาก Port ต้นทางอะไรก็ได้ ให้ไปที่จุดหมายปลายทางหมายไอพี WAN ที่ Port 1194 (OpenVPN) ดังภาพที่ 4-24



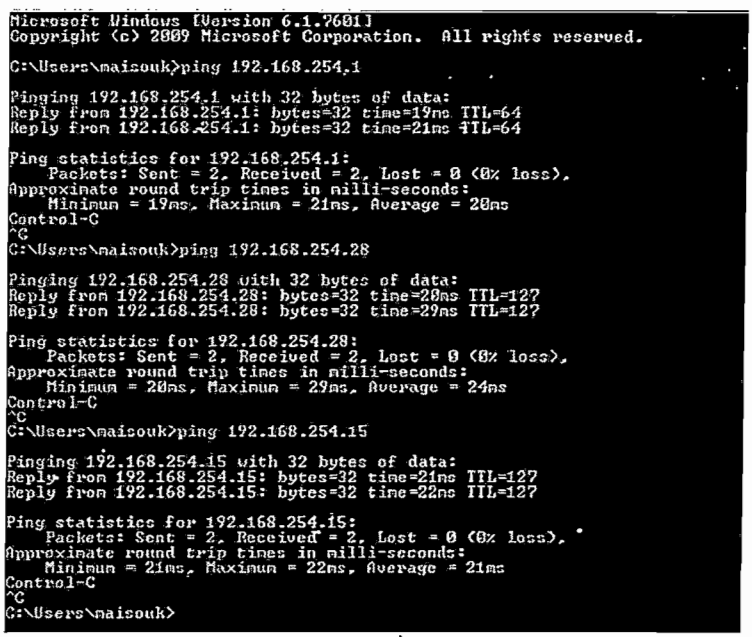
ภาพที่ 4-24 ผลการสร้างกฎไฟร์วอลล์เพื่ออนุญาตให้ OpenVPN เข้าถึง pfSense ได้

ผลการเชื่อมต่อ Open VPN โดยที่ใช้ Notebook ที่อยู่ข้างนอกเครือข่าย (เช่น เราอยู่ในมหาวิทยาลัยบูรพา) และ ใช้ OpenVPN ไคลเอนต์ (โปรแกรมชื่อ OpenVPN Client) พบว่า OpenVPN ไคลเอนต์สามารถเข้าถึง pfSense ได้ ดังภาพที่ 4-25



ภาพที่ 4-25 OpenVPN Client ทำการเชื่อมต่อไปที่ pfSense

เราสามารถ ping ไปเครื่องภายในเครือข่ายข้างในได้เช่น ping ไปหาไอพีของ pfSense และ หมายเลขไอพีของเครื่องที่กำลังทำงานอยู่ ดังภาพที่ 4-26



ภาพที่ 4-26 ผลการทดสอบในเวลาการ ping เข้าไปที่ภายในเครือข่าย

8. การทดสอบเครื่องแม่ข่าย proxy

เมื่อกำหนดค่าที่เครื่องแม่ข่าย proxy ใน pfSense แล้ว เครื่องแม่ข่าย proxy จะเก็บ (cache) ข้อมูลหน้าเว็บที่ไคลเอนต์เคยเรียกใช้งานไว้ เมื่อมีไคลเอนต์ใหม่เรียกใช้หน้าเว็บเดิมเครื่องแม่ข่าย proxy จะทำหน้าที่แทน Web Server และส่งต่อหน้าเว็บที่เก็บไว้ใน cache ให้กับไคลเอนต์ นอกจากนี้ เครื่องแม่ข่าย proxy ยังสามารถเก็บ log ข้อมูลของผู้ใช้เครือข่าย ภาพที่ 4-27 แสดงตัวอย่างของ Squid user access report ของวันที่ 22 มีนาคม 2559 ซึ่งมีเครื่องใช้หมายเลขไอพี 92.168.254.21 (มี host name คือ Tech Good) เข้าเชื่อมต่อเครือข่าย 171 ครั้ง ใช้แบนด์วิดท์ 327.8 Mbps (คิดเป็น 42.2 % แบนด์วิดท์ทั้งหมด) Tech Good อยู่ในกลุ่มผู้ใช้ Teacher2

Squid user access report — Home

Date: 22 Mar 2016 (update :: 21:56 :: 22 Mar 2016)

Top Sites Report

Big Files Report

#	Time	User	Real Name	Connect	Bytes	%	Group
1		192.168.254.21	Tech Good	171	327.8 M	42.2%	02. Teacher2
2		192.168.254.27	?	1 789	122.7 M	15.8%	02. Teacher2
3		192.168.254.30	?	143	93.1 M	12.0%	?
4		192.168.254.20	?	1 270	69.7 M	8.9%	?
5		192.168.254.23	?	675	65.3 M	8.4%	02. Teacher2
6		192.168.254.25	?	4 739	37.8 M	4.8%	02. Teacher2
7		192.168.254.16	?	1 762	35.9 M	4.6%	01. Teacher1

ภาพที่ 4-27 รายงานการเข้าใช้งานเครือข่ายของ Squid

นอกจากการเก็บ log หมายเลขไอพีแล้วเครื่องแม่ข่าย proxy ยังเก็บเว็บไซต์ที่ผู้ใช้เข้าไปใช้ ดังภาพที่ 4-28 เครื่องที่มีหมายเลขไอพี 192.168.254.21 ได้เข้าไปเว็บไซต์มีชื่อ products.kaspersk y-labs.com เป็นจำนวน 1 ครั้ง มีแบนด์วิดท์ที่ใช้ 169.6 M และ คิดเป็น 51.7 % ของจำนวนแบนด์วิดท์ที่เข้าใช้ทั้งหมด

Squid user access report — Home

User: 192.168.254.21 (Tech Good)

Group: 02. Teacher2

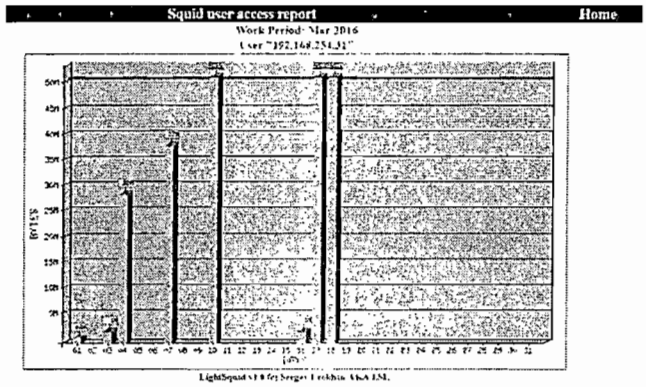
Date: 22 Mar 2016

User download "Big Files"

Total			327.8 M		
#	Accessed site	Connect	Bytes	Cumulative	%
1	products.kaspersky-labs.com	1	169.6 M	169.6 M	51.7%
2	dm.kaspersky-labs.com	16	144.1 M	313.7 M	43.9%
3	au.v4.download.windowsupdate.com	22	10.3 M	324.0 M	3.1%
4	download.cdn.mozilla.net	9	2.6 M	326.5 M	0.7%
5	safebrowsing-cache.google.com	11	1 011 049	327.5 M	0.2%
6	www.google.com	4	75 249	327.6 M	0.0%
7	v4.download.windowsupdate.com	4	29 911	327.6 M	0.0%
8	cdn.content.prod.cms.msn.com	18	29 394	327.6 M	0.0%
9	tile-service.weather.microsoft.com	6	28 610	327.7 M	0.0%
10	wscont.apps.microsoft.com	1	22 139	327.7 M	0.0%

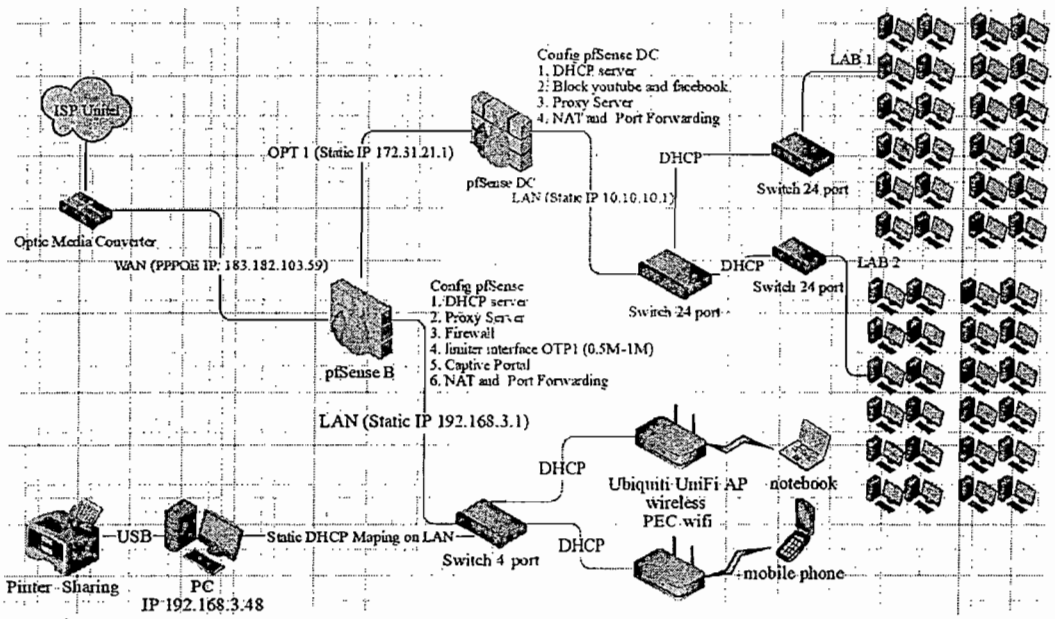
ภาพที่ 4-28 รายงานเว็บไซต์ที่ผู้ใช้เครื่องที่มีหมายเลขไอพี 192.168.254.21 ได้เข้าถึงในวันที่ 22 มีนาคม 2559

นอกจากนี้ เครื่องแม่ข่าย proxy ยังสามารถแสดงผลเป็นรูปแบบ chart ดังภาพที่ 4-29 ที่แสดงจำนวนแบนด์วิดท์ที่ถูกใช้ไปในแต่ละวัน เช่น วันที่ 01 มีการใช้ แบนด์วิดท์ 68 KB



ภาพที่ 4-29 รายงานการใช้แบนด์วิดท์ในแต่ละวันของเครื่องที่ใช้ไอพีหมายเลข 192.168.254.31

โครงสร้างระบบเครือข่ายที่ 2 (ภายในอาคาร B, C,และD)



ภาพที่ 4-30 โครงสร้างของระบบเครือข่ายอาคาร B, C, และ D

ผู้ทำงานนิพนธ์ได้ออกแบบการทดสอบในส่วนต่าง ๆ 4 ส่วนต่อไปนี้

2.1 การวัดความล่าช้าสำหรับการส่งข้อมูลภายในเครือข่ายอาคาร B, C, และ D

2.2 การวัดแบนด์วิดท์ของอินเทอร์เน็ต (อัพโหลดและดาวน์โหลด)

2.3 การทดสอบกฎไฟร์วอลล์ สำหรับการ block Facebook and YouTube

2.4 การทดสอบกฎไฟร์วอลล์ สำหรับการในการอัพโหลด และดาวน์โหลด ไม่เกิน 1 M

2.5 การวัดความล่าช้าสำหรับการส่งข้อมูลภายในเครือข่ายอาคาร B, C, และ D

1. การทดสอบเครือข่ายในห้อง LAB1 ภายในอาคาร D ที่เป็นระบบสายแลนรายละเอียดมีดังต่อไปนี้

1. ผู้ทำงานนิพนธ์ทดสอบโดยใช้ไคลเอนต์ 15 ไคลเอนต์ ping ไปยังเครื่องแม่ข่าย pfSense B โดยใช้คำสั่ง ping –n 35 192.168.3.1 แต่ละไคลเอนต์จะส่ง ping ไป 35 ping แล้วรอการตอบกลับมา จากผลการทดลองสรุปได้ว่าเครื่องแม่ข่าย pfSense ตอบกลับมา 99.61% มีแพ็กเกจสูญหาย 2 แพ็กเกจโดยค่าเฉลี่ยของเวลาที่ ping เดินทางไปกลับ คือ 0 มิลลิวินาทีค่าเวลาที่ ping เดินทางไปกลับน้อยสุดเป็น 0 และ มากสุดที่ 1 มิลลิวินาทีดังรายละเอียดที่แสดงด้วยตาราง 4-7

ตารางที่ 4-7 การ ping จาก ไคลเอนต์ ไปที่ Server ping -n 35 192.168.3.1

การ ping จาก ไคลเอนต์ ไปที่ Server ping -n 35 192.168.3.1	เวลาที่เดินทางไปกับ (Round Trip Time) (ms)					
	Sent	Received	lost	Minimum	Maximum	Average
ไคลเอนต์ 1	35	35	0	0	0	0
ไคลเอนต์ 2	35	35	0	0	1	0
ไคลเอนต์ 3	35	35	0	0	0	0
ไคลเอนต์ 4	35	35	0	0	0	0
ไคลเอนต์ 5	35	35	0	0	0	0
ไคลเอนต์ 6	35	35	0	0	0	0
ไคลเอนต์ 7	35	33	2	0	1	0
ไคลเอนต์ 8	35	35	0	0	1	0
ไคลเอนต์ 9	35	35	0	0	0	0
ไคลเอนต์ 10	35	35	0	0	0	0
ไคลเอนต์ 11	35	35	0	0	0	0
ไคลเอนต์ 12	35	35	0	0	0	0
ไคลเอนต์ 13	35	35	0	0	1	0
ไคลเอนต์ 14	35	35	0	0	1	0
ไคลเอนต์ 15	35	35	0	0	0	0

2. ผู้ทำงานนิพนธ์ทดสอบโดยใช้ไคลเอนต์ 15 ไคลเอนต์ ping ไปยังเครื่องแม่ข่าย Google โดยใช้คำสั่ง ping –n 35 www.Google.com แต่ละไคลเอนต์จะส่ง ping ไป 35 ping แล้วรอการตอบกลับมา จากผลการทดลองสรุปได้ว่าเครื่องแม่ข่าย Google ตอบกลับมา 100% ไม่มีแพ็กเกจสูญหาย โดยค่าเฉลี่ยของเวลาที่ ping เดินทางไปกลับ คือ 3.6 มิลลิวินาทีค่าเวลาที่ ping เดินทางไปกลับน้อยสุดเป็น 3 และ มากสุดที่ 38 มิลลิวินาทีดังรายละเอียดที่แสดงด้วยตาราง 4-8

ตารางที่ 4-8 การ ping จาก ไคลเอนต์ ไปที่ Google ping -n 35 www.Google .com

การ ping จาก ไคลเอนต์ ไปที่ Google ping -n 35 www.Google .com	เวลาที่เดินทางไปกับ (Round Trip Time) (ms)					
	Sent	Received	lost	Minimum	Maximum	Average
ไคลเอนต์ 1	35	35	0	3	16	4
ไคลเอนต์ 2	35	35	0	3	17	4
ไคลเอนต์ 3	35	35	0	3	14	3
ไคลเอนต์ 4	35	35	0	3	12	4
ไคลเอนต์ 5	35	35	0	3	10	3
ไคลเอนต์ 6	35	35	0	3	8	3
ไคลเอนต์ 7	35	35	0	3	38	4
ไคลเอนต์ 8	35	35	0	3	7	3
ไคลเอนต์ 9	35	35	0	3	14	4
ไคลเอนต์ 10	35	35	0	3	32	4
ไคลเอนต์ 11	35	35	0	3	9	3
ไคลเอนต์ 12	35	35	0	3	26	4
ไคลเอนต์ 13	35	35	0	3	11	4
ไคลเอนต์ 14	35	35	0	3	11	4
ไคลเอนต์ 15	35	35	0	3	10	3

3. ผู้ทำงานนิพนธ์ทดสอบโดยใช้ไคลเอนต์ 15 ไคลเอนต์ ping ไปยัง เครื่องแม่ข่าย YouTube โดยใช้คำสั่ง ping –n 35 www. YouTube.com แต่ละไคลเอนต์จะส่ง ping ไป 35 ping แล้วรอการตอบกลับมา จากผลการทดลองสรุปได้ว่าเครื่องแม่ข่าย YouTube ตอบกลับมา 100% ไม่มีแพ็กเกจสูญหาย โดยค่าเฉลี่ยของเวลาที่ ping เดินทางไปกลับ คือ 4 มิลลิวินาที ค่าเวลาที่ ping เดินทางไปกลับน้อยสุดเป็น 3 และ มากสุดที่ 30มิลลิวินาทีดังรายละเอียดที่แสดงด้วยตาราง 4-9

ตารางที่ 4-9 การ ping จาก ไคลเอนต์ ไปที่ Server ping -n 35 www.YouTube.com

การ ping จาก ไคลเอนต์ ไปที่ Server ping -n 35 www.YouTube.com	เวลาที่เดินทางไปกับ (Round Trip Time) (ms)					
	Sent	Received	lost	Minimum	Maximum	Average
ไคลเอนต์ 1	35	35	0	3	14	3
ไคลเอนต์ 2	35	35	0	3	12	3
ไคลเอนต์ 3	35	35	0	3	19	4
ไคลเอนต์ 4	35	35	0	3	21	6
ไคลเอนต์ 5	35	35	0	3	21	6
ไคลเอนต์ 6	35	35	0	3	13	4
ไคลเอนต์ 7	35	35	0	3	22	4
ไคลเอนต์ 8	35	35	0	3	8	4
ไคลเอนต์ 9	35	35	0	3	15	3
ไคลเอนต์ 10	35	35	0	3	30	5
ไคลเอนต์ 11	35	35	0	3	19	4
ไคลเอนต์ 12	35	35	0	3	13	4
ไคลเอนต์ 13	35	35	0	3	14	3
ไคลเอนต์ 14	35	35	0	3	15	3
ไคลเอนต์ 15	35	35	0	3	17	4

4. ผู้ทำงานนิพนธ์ทดสอบโดยใช้ ไคลเอนต์ 15 ไคลเอนต์ ping ไปยัง เครื่องแม่ข่าย Facebook โดยใช้คำสั่ง ping –n www.Facebook.com แต่ละไคลเอนต์จะส่ง ping ไป 35 ping แล้วรอการตอบกลับมา จากผลการทดลองสรุปได้ว่าเครื่องแม่ข่าย Facebook ตอบกลับมา 99.61% มีแพ็กเกจสูญหาย 2 แพ็กเกจ โดยค่าเฉลี่ยของเวลาที่ ping เดินทางไปกลับ คือ 223.6 มิลลิวินาที ค่าเวลาที่ ping เดินทางไปกลับน้อยสุดเป็น 220 และ มากสุดที่ 232 มิลลิวินาทีดังรายละเอียดที่แสดงด้วยตาราง 4-10

ตารางที่ 4-10 การ ping จาก ไคลเอนต์ ไปที่ Server ping -n 35 www.Facebook.com

การ ping จาก ไคลเอนต์ ไปที่ Server ping -n 35 www.Facebook.com	เวลาที่เดินทางไปกับ (Round Trip Time) (ms)					
	Sent	Received	lost	Minimum	Maximum	Average
ไคลเอนต์ 1	35	35	0	220	229	224
ไคลเอนต์ 2	35	35	0	220	230	223
ไคลเอนต์ 3	35	35	0	220	230	223
ไคลเอนต์ 4	35	35	0	220	230	224
ไคลเอนต์ 5	35	34	1	220	232	225
ไคลเอนต์ 6	35	34	1	221	232	224
ไคลเอนต์ 7	35	35	0	221	232	224
ไคลเอนต์ 8	35	35	0	221	231	223
ไคลเอนต์ 9	35	35	0	220	229	224
ไคลเอนต์ 10	35	35	0	220	231	223
ไคลเอนต์ 11	35	35	0	220	232	223
ไคลเอนต์ 12	35	35	0	221	231	224
ไคลเอนต์ 13	35	35	0	221	227	223
ไคลเอนต์ 14	35	35	0	220	230	223
ไคลเอนต์ 15	35	35	0	221	228	224

สรุป การเปรียบเทียบค่าเฉลี่ยที่ได้จากผลการทดสอบ ping ของไคลเอนต์ไปที่ pfSense, Web Server, www. Google.com, www.YouTube.com, www.Facebook.com จะเห็นว่าความล่าช้า (Round Trip Tine) ที่เกิดจากการ ping Facebook YouTube Google ซึ่งเป็น Server อยู่ภายนอกจะมีค่ามากกว่าผลต่างของค่าเฉลี่ยประมาณ 3-223 มิลลิวินาที

โดย Facebook จะใช้เวลาตอบ ping นานกว่า YouTube และ Google โดยการทดสอบ tracert ไปที่เครื่องแม่ข่ายของ Facebook จากไคลเอนต์ที่อยู่ในเครือข่ายในอาคาร B พบว่าเส้นทางประกอบด้วย 15 router โดยเครื่องแม่ข่ายของ Facebook อยู่ที่ประเทศ United States ตามข้อมูลจากเว็บไซต์ http://www.speedguide.net/ip/66.220.146.36/ ดังภาพที่ 4-31

```
C:\Users\yangchiamoua>tracert www.facebook.com

Tracing route to star-mini.c10r.facebook.com [66.220.146.36]
over a maximum of 30 hops:

  1     2 ms     1 ms     2 ms  pfSense.localdomain [192.168.3.1]
  2    10 ms     6 ms     6 ms  unitel.com.la [183.182.103.1]
  3    10 ms     4 ms     5 ms  unitel.com.la [183.182.97.35]
  4    15 ms     6 ms     5 ms  183.182.96.109
  5   289 ms   304 ms   304 ms  ge-1-2-3-xcr1.hkg.cw.net [203.169.57.1]
  6   301 ms   311 ms   296 ms  ae44.pr01.hkg3.tfbnw.net [103.4.96.114]
  7   317 ms   304 ms   304 ms  ae0.bb01.hkg1.tfbnw.net [31.13.28.216]
  8   297 ms   317 ms   295 ms  ae13.bb01.hnd1.tfbnw.net [31.13.26.21]
  9   269 ms   303 ms   303 ms  be10.bb01.lax1.tfbnw.net [31.13.29.63]
 10   296 ms   303 ms   304 ms  ae19.bb03.prn2.tfbnw.net [31.13.25.217]
 11   298 ms   303 ms   304 ms  ae43.dr01.prn2.tfbnw.net [31.13.31.119]
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15   284 ms   303 ms   303 ms  unitel.com.la [183.182.103.59]
 16   295 ms   303 ms   305 ms  edge-star-mini-shv-18-prn1.facebook.com [66
.220.146.36]

Trace complete.

C:\Users\yangchiamoua>
```

ภาพที่ 4-31 ผลการ tracert ไปที่เครื่องแม่ข่ายของ Facebook

ส่วนผลทดสอบ tracert www. YouTube.com พบว่าเส้นทางประกอบด้วย 8 router เครื่องแม่ข่าย ของ Google อยู่ที่ประเทศ Lao People's Democratic Republic ตามข้อมูลจากเว็บไซต์ (http://www.speedguide.net/ip/183.182.96.165)ดังภาพที่ 4-32 ด้านล่าง

```
C:\Users\yangchiamoua>tracert www.youtube.com

Tracing route to youtube-ui.l.google.com [183.182.96.165]
over a maximum of 30 hops:

  1     1 ms     2 ms     2 ms  pfSense.localdomain [192.168.3.1]
  2     9 ms     7 ms     4 ms  unitel.com.la [183.182.103.1]
  3   124 ms     4 ms     4 ms  unitel.com.la [183.182.97.35]
  4     9 ms     8 ms     5 ms  unitel.com.la [183.182.97.121]
  5     9 ms     5 ms     5 ms  183.182.96.5
  6    10 ms     8 ms     4 ms  183.182.96.165

Trace complete.
```

ภาพที่ 4-32 ผลการ tracert ไปที่เครื่องแม่ข่ายของ YouTube

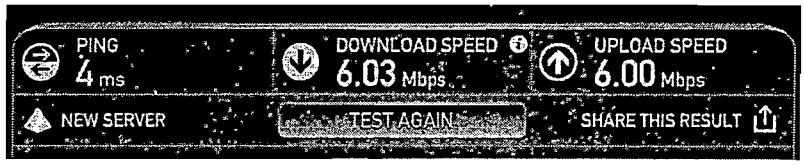
ตารางที่ 4-11 สรุปค่าเฉลี่ยความล่าช้าไปยังเครื่องแม่ข่ายดังรายละเอียดแสดงด้วยตารางด้านล่าง

เครื่องแม่ข่ายต่างๆ	ค่าเฉลี่ย Round Trip Time
เครื่องแม่ข่าย pfSense	0
เครื่องแม่ข่าย Google	3.6
เครื่องแม่ข่าย YouTube	4
เครื่องแม่ข่าย Facebook	223.6

ส่วนการ ping ไปที่ pfSense และ Web Serve เป็นการ ping ภายในเครือข่ายใช้เวลาตอบกลับน้อย เพราะว่าไม่ได้ออกไปข้างนอก และ ไม่ได้ผ่านไฟร์วอลล์

2. การวัดแบนด์วิดท์ของอินเทอร์เน็ต (อัพโหลดและดาวน์โหลด)

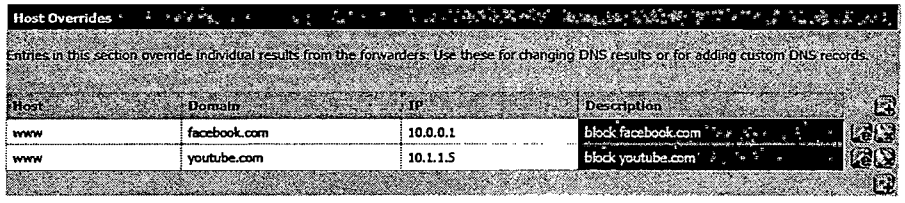
การทดสอบโดยใช้ www.speedtest.net พบว่า ปริมาณแบนด์วิดท์ในการอัพโหลด 6.00 Mbps และดาวน์โหลดอยู่ที่ 6.00 Mbps ซึ่งใกล้เคียงกับแบนด์วิดท์ที่คาดว่าจะรับจาก ISP ดังแสดงดังภาพที่ 4-33



ภาพที่ 4-33 ผลการทดสอบปริมาณแบนด์วิดท์ สำหรับอัพโหลด และ ดาวน์โหลด

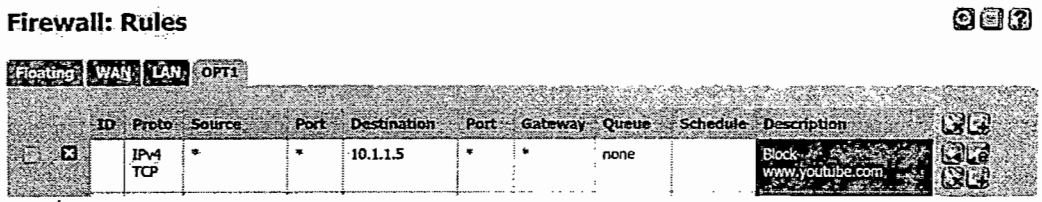
3. การทดสอบกฎไฟร์วอลล์ สำหรับการ block Facebook and YouTube

ผู้จัดทำงานนิพนธ์ได้สร้างหมายเลขไอพี (ปลอม) สำหรับ www.YouTube.com และ www.Facebook.com ขึ้น และ นำไปใส่ที่บริการ "Host Overrides" ของ pfSense ดังภาพ 4-34



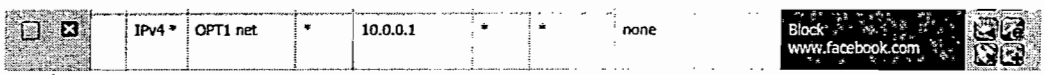
ภาพที่ 4-34 การจำลองหมายเลขไอพีของ YouTube และ Facebook

ผู้ทำงานนิพนธ์สร้างกฎปฏิเสธการเข้าถึง YouTube (ที่ไอพี 10.1.1.5) จากทุกไคลเอนต์ที่อยู่ภายในเครือข่ายอาคาร D (ทุก ๆ Port ต้นทางของทั้ง TCP และ UDP) ดังภาพ 4-35



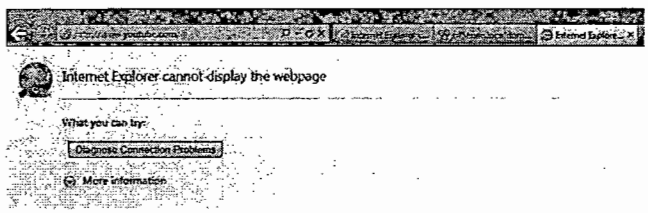
ภาพที่ 4-35 กฎไฟร์วอลล์ไม่อนุญาตให้มีการเข้าถึงตัว YouTube ได้

ผู้ทำงานนิพนธ์ปฏิเสธการเข้าถึง Facebook (ที่ไอพี 10.0.0.1) จากทุกไคลเอนต์ที่อยู่ภายในเครือข่าย อาคาร D จากทุก ๆ TCP/UDP ทุก ๆ Port ต้นทาง ดังภาพ 4-36



ภาพที่ 4-36 ผลการ สร้างกฎไฟร์วอลล์ไม่อนุญาตให้มีการเข้าถึงตัว Facebook ได้

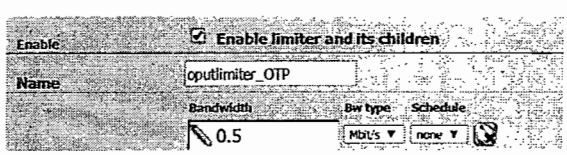
ผู้ทำงานนิพนธ์ใช้ Notebook ที่อยู่ภายในเครือข่ายอาคาร D ทดสอบเข้าใช้เว็บ YouTube และ พบว่าไม่สามรถเข้าใช้ YouTube (เพราะฉะนั้น Facebook ก็เข้าไม่ได้) ดังภาพ 4-37



ภาพที่ 4-37 ผลการ แสดงถึง client ไม่สามารถเข้าใช้เว็บ YouTube

4. การทดสอบกฎไฟร์วอลล์สำหรับการในการอัพโหลดและดาวน์โหลดไม่เกิน 1 Mpbs

ผู้ทำงานนิพนธ์ได้กำหนดใช้ “Limiter” เพื่อจำกัดแบนด์วิดท์ที่ผู้ใช้จะใช้ได้ในอาคาร D โดยจะกำหนดแบนด์วิดท์ในการอัพโหลด 0.5 Mbps และ กำหนดชื่อ Limiter “oputlimiter_OTP” ดังภาพที่ 4-38

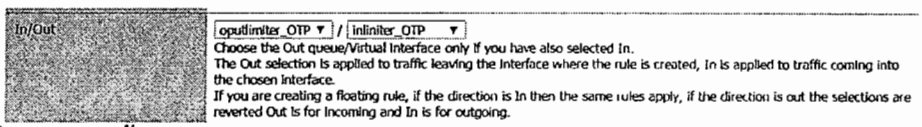


ภาพที่ 4-38 การตั้งค่า “Limiter” เพื่อจำกัดแบนด์วิดท์ให้แก่ผู้ใช้ในการอัพโหลด

ผู้ทำงานนิพนธ์ได้กำหนดใช้ “Limiter” เพื่อจำกัดแบนด์วิดท์ที่ผู้ใช้จะใช้ได้ในอาคาร D โดยจะกำหนดแบนด์วิดท์ในการดาวน์โหลด 1 Mbps และ กำหนดชื่อ Limiter “intlimiter_OTP” ดังภาพที่ 4-39

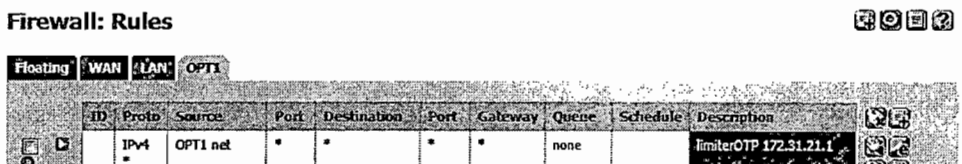
ภาพที่ 4-39 การตั้งค่า “Limiter” เพื่อจำกัดแบนด์วิดท์ให้แก่ผู้ใช้ในการดาวน์โหลด

หลังจากนั้นผู้ทำงานนิพนธ์ตั้งค่าไฟร์วอลล์อนุญาตให้ผู้ใช้สามารถอัพโหลด 0.5 Mbps (โดยใส่ Limiter “oputlimiter_OTP”) และดาวน์โหลด 1 Mbps (โดยใส่ Limiter “intlimiter_OTP”) ใน Interface OTP1 ดังภาพ 4-40



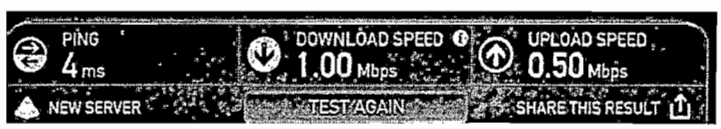
ภาพที่ 4-40 การตั้งค่าให้ผู้ใช้สามารถอัพโหลด 0.5M และดาวน์โหลด 1M

การสร้างกฎโดยอนุญาตให้ทุก ๆ ไคลเอนต์ที่อยู่ในเครือข่ายภายในอาคาร D โดยให้อัพโหลดไม่เกิน 0.5 Mbps และดาวน์โหลดไม่เกิน 1 Mbps (สังเกตเครื่องหมาย ด้านซ้ายที่บ่งบอกว่ากฎนี้ได้ใส่ Limiter แล้ว) ดังภาพ 4-41



ภาพที่ 4-41 กฎอนุญาตให้ผู้ใช้สามารถอัพโหลด 0.5M และดาวน์โหลด 1M

หลังจากการสร้างกฎอนุญาตให้ผู้ใช้สามารถอัพโหลดข้อมูลที่ 0.5 Mbps และ ดาวน์โหลดที่ 1 Mbps แล้วผู้ทำงานนิพนธ์ ได้ใช้ Notebook ที่อยู่ภายในเครือข่ายอาคาร D เพื่อทดสอบปริมาณแบนด์วิดท์โดยใช้ www.speedtest.net พบว่า ปริมาณแบนด์วิดท์ในการอัพโหลด 1.00 Mbps และดาวน์โหลดอยู่ที่ 0.50 Mbps ซึ่งตรงกับแบนด์วิดท์ได้กำหนดไว้ ดังภาพที่ 4-42



ภาพที่ 4-42 ปริมาณแบนด์วิดท์ ในการอัพโหลดและดาวน์โหลด

แบบสำรวจความพึงพอใจของอาจารย์ที่ใช้ Internet ในวิทยาลัยพลศึกษา

ผู้ทำงานนิพนธ์ได้ออกแบบระบบและติดตั้งระบบเครือข่ายให้วิทยาลัยพลศึกษา เพื่อให้ได้ระบบเครือข่ายที่มีประสิทธิภาพ ซึ่งมีบทบาทสำคัญต่อการพัฒนาการศึกษาและใช้ระบบเครือข่ายคอมพิวเตอร์ เป็นสื่อสำหรับการเรียนการสอน รวมถึงใช้ค้นหาข้อมูล ประมวลผล และ เพิ่มศักยภาพด้านการสื่อสารจากแหล่งเรียนรู้ได้มากขึ้นที่หลากหลาย เพราะฉะนั้นผู้ทำงานนิพนธ์จึงได้สร้างแบบสำรวจความพึงพอใจของอาจารย์ที่ใช้ Internet ในวิทยาลัยพลศึกษา ผลการวิเคราะห์มี 2 ส่วนดังนี้

ส่วนที่ 1 แบบสอบถามข้อมูลเบื้องต้นของผู้ทำแบบสำรวจ

ในงานนิพนธ์เล่มนี้ ผู้ทำงานนิพนธ์ได้ศึกษาข้อมูลพื้นฐานเกี่ยวกับแบบสำรวจของอาจารย์ในวิทยาลัยพลศึกษา ที่ใช้ Internet โดยแบ่งข้อมูลออกเป็น 13 ชนิดได้แก่

1. เพศ
2. อายุ
3. ระดับการศึกษา
4. สถานภาพ
5. ความถี่ในการใช้อินเทอร์เน็ต/วัน
6. ความถี่ในการใช้งานอินเทอร์เน็ต/สัปดาห์
7. ท่านมักจะใช้บริการในช่วงเวลาใดมากที่สุด
8. สถานที่ที่ใช้บริการอินเทอร์เน็ตเป็นประจำ
9. เว็บไซต์ที่เข้าใช้มากที่สุด
10. ท่านรู้จักเว็บไซต์ของวิทยาลัยจากที่ใด
11. ท่านเข้าชมเว็บไซต์ของวิทยาลัยบ่อยแค่ไหน
12. ท่านเข้าชมเว็บไซต์ของวิทยาลัยเพื่อวัตถุประสงค์ใด
13. ท่านคิดว่าเว็บไซต์ของวิทยาลัยเป็นประโยชน์ต่อท่านหรือไม่

จากการศึกษาข้อมูลพื้นฐานเกี่ยวกับแบบสำรวจของอาจารย์ในวิทยาลัยพลศึกษา ในการใช้ Internet มีจำนวน 37 คน โดยเป็นเพศชาย 16 คน หญิง 21 หญิง ส่วนใหญ่มีอายุระหว่าง 21-30 ปี ระดับการศึกษาส่วนใหญ่อยู่ระดับปริญญาตรี โดยมีรายละเอียดดังแสดงในตารางที่ 4-12

ตาราง 4-12 ข้อมูลพื้นฐานของอาจารย์ในวิทยาลัยที่ใช้งาน Internet

ลำดับ	ข้อมูล	จำนวน(คน)	ร้อยละ
1. เพศ			
	ชาย	16	43.24324
	หญิง	21	56.75676
รวม		37	100
2. อายุ			
	21-30 ปี	26	70.27027
	31-40 ปี	7	18.91892
	41-50 ปี	2	5.405405
	51-60 ปี	2	5.405405
ร่วม		37	100
3. ระดับการศึกษา			
	กำลังศึกษาปริญญาตรี	5	13.51351
	กำลังศึกษาปริญญาโท	5	13.51351
	ปริญญาตรี	26	70.27027
	ปริญญาโท	1	2.702703
รวม		37	100
4. สถานภาพ			
	นักวิชาการ/อาจารย์	19	51.35135
	บุคลากร	11	29.72973
	ผู้บริหาร	7	18.91892
รวม		37	100
5. ความถี่ในการใช้อินเทอร์เน็ต/วัน			
	จำนวน 1-3 ชม./วัน	23	62.16216
	จำนวน 3-6 ชม./วัน	10	27.02703
	จำนวน 6-9 ชม./วัน	4	10.81081
รวม		37	100

ตาราง 4-12 ข้อมูลพื้นฐานของอาจารย์ในวิทยาลัยที่ใช้งาน Internet (ต่อ)

ลำดับ	ข้อมูล	จำนวน(คน)	ร้อยละ
6. ความถี่ในการใช้งานอินเทอร์เน็ต/สัปดาห์			
	น้อยกว่า 1 วัน/สัปดาห์	2	5.405405
	1 วัน/สัปดาห์	1	2.702703
	2 วัน/สัปดาห์	4	10.81081
	3 วัน/สัปดาห์	5	13.51351
	4 วัน/สัปดาห์	8	21.62162
	5 วัน/สัปดาห์	8	21.62162
	ใช้ทุกวัน	9	24.32432
	รวม	37	100
7. ท่านมักจะใช้บริการในช่วงเวลาใดมากที่สุด			
	8.00 – 12.00 น.	12	32.43243
	12.00 – 13.00 น.	9	24.32432
	13.00 – 16.00 น.	8	21.62162
	16.00 – 20.00 น	2	5.405405
	20.00 – 24.00 น.	6	16.21622
	รวม	37	100
8. สถานที่ที่ใช้บริการอินเทอร์เน็ตเป็นประจำ			
	ห้องสมุด	2	5.405405
	สำนักงาน ที่สังกัด	27	72.97297
	หอพักของวิทยาลัย	2	5.405405
	จุดให้บริการ Wireless บริเวณ (โปรดระบุ)	6	16.21622
	รวม	37	100

ตาราง 4-12 ข้อมูลพื้นฐานของอาจารย์ในวิทยาลัยที่ใช้งาน Internet (ต่อ)

ลำดับ	ข้อมูล	จำนวน(คน)	ร้อยละ
9. เว็บไซต์ที่เข้าใช้มากที่สุด			
	YouTube	8	17.02128
	Facebook	15	31.91489
	LINE	2	4.255319
	Google	20	42.55319
	Yahoo	2	4.255319
	รวม	47	100
10. ท่านรู้จักเว็บไซต์ของวิทยาลัยจากที่ใด			
	จากเว็บค้นหา เช่น Google	18	48.64865
	เพื่อนแนะนำ	7	18.91892
	แผ่นพับที่วิทยาลัยแจก	4	10.81081
	ลิงค์จากเว็บอื่น	3	8.108108
	อื่น ๆ (โปรดระบุ)	5	13.51351
	รวม	37	100
11. ท่านเข้าชมเว็บไซต์ของวิทยาลัยบ่อยแค่ไหน			
	1-2 ครั้งต่อสัปดาห์	6	17.64706
	1-2 ครั้งต่อเดือน	3	8.823529
	น้อยกว่า 1 ครั้งต่อเดือน	2	5.882353
	ไม่เคย	23	67.64706
	รวม	34	100
12. ท่านเข้าชมเว็บไซต์ของวิทยาลัยเพื่อวัตถุประสงค์ใด			
	อ่านข่าวสารใหม่ๆของวิทยาลัย	11	47.82609
	ค้นหาเอกสาร แบบฟอร์ม หรือ บทความ	1	4.347826
	เพื่อหาข้อมูลเกี่ยวกับรายวิชาเรียน	3	13.04348
	อื่น ๆ (โปรดระบุ)	8	34.78261
รวม	23		

ตาราง 4-12 ข้อมูลพื้นฐานของอาจารย์ในวิทยาลัยที่ใช้งาน Internet (ต่อ)

ลำดับ	ข้อมูล	จำนวน(คน)	ร้อยละ
13. ท่านคิดว่าเว็บไซต์ของวิทยาลัยเป็นประโยชน์ต่อท่านหรือไม่			
	ค่อนข้างเป็นประโยชน์	7	25.92593
	เป็นประโยชน์ แต่ยังไม่เพียงพอ	16	59.25926
	ไม่เป็นประโยชน์เลย	4	14.81481
	รวม	27	100

จากตารางที่ 4-12 พบว่าผู้ตอบแบบสำรวจความพึงพอใจมีจำนวนทั้งหมด 37 คน โดยมีข้อมูลสรุปได้ดังนี้

เพศ ผู้ตอบแบบสำรวจความพึงพอใจส่วนใหญ่เป็นเพศหญิง จำนวน 21 คน คิดเป็นร้อยละ 56.75676 และ เพศชาย จำนวน 16 คน คิดเป็นร้อยละ 43.24324

อายุ ผู้ตอบแบบสำรวจความพึงพอใจส่วนใหญ่มีอายุระหว่าง 21-30 ปี จำนวน 21 คน คิดเป็นร้อยละ 70.27027 รองลงมามีอายุระหว่าง 31-40 ปี มีจำนวน 7 คน คิดเป็นร้อยละ 17.91892 รอง ลงมาอีกก็มีอายุระหว่าง 41-50 ปี มีจำนวน 2 คน คิดเป็นร้อยละ 5.405405
ส่วนอายุสูงกว่า 51-60 ปี มีจำนวน 2 คน คิดเป็นร้อยละ 5.405405

ระดับการศึกษา ผู้ตอบแบบสำรวจความพึงพอใจส่วนใหญ่จะมีระดับการศึกษาปริญญาตรี จำนวน 26 คน คิดเป็นร้อยละ 70.27027 รองลงมาเป็นกำลังศึกษาปริญญาโท จำนวน 5 คน คิดเป็นร้อยละ 13.51351 รองลงมาอีกเป็นกำลังศึกษาปริญญาตรีจำนวน 5 คน คิดเป็นร้อยละ 13.51351 และ ปริญญาโท มีจำนวน 1 คน คิดเป็นร้อยละ 2.702703

สถานภาพ ผู้ตอบแบบสำรวจความพึงพอใจส่วนใหญ่จะมีสถานภาพเป็นนักวิชาการ/อาจารย์ มีจำนวน 19 คน คิดเป็นร้อยละ 51.35135 รองลงมาเป็นบุคลากร มีจำนวน 11 คน คิดเป็นร้อยละ 29.72973 และ ผู้บริหาร มีจำนวน 7 คน คิดเป็นร้อยละ 18.91892

ความถี่ในการใช้อินเทอร์เน็ต/วัน ผู้ตอบแบบสำรวจความพึงพอใจส่วนใหญ่เป็นจำนวน 1-3 ชม./วัน มีจำนวน 23 คน คิดเป็นร้อยละ 62.16216 รองลงมาเป็นจำนวน 3-6 ชม./วัน มีจำนวน 10 คน คิดเป็นร้อยละ 27.02703 และ จำนวน 6-9 ชม./วัน มีจำนวน 4 คน คิดเป็นร้อยละ10.81081

ความถี่ในการใช้งานอินเทอร์เน็ต/สัปดาห์ ผู้ตอบแบบสำรวจความพึงพอใจส่วนใหญ่เป็นใช้ทุกวัน มีจำนวน 9 คน คิดเป็นร้อยละ 24.32432 รองลงมาเป็น 5 วัน/สัปดาห์ มีจำนวน 8 คน คิดเป็นร้อยละ 21.62162 รองลงมาอีกเป็น 4 วัน/สัปดาห์ มีจำนวน 8 คน คิดเป็นร้อยละ 21.62162 ต่ำกว่า 3 วัน/สัปดาห์ มีจำนวน 5 คน คิดเป็นร้อยละ 13.51351 และ 2 วัน/สัปดาห์ มีจำนวน 4 คน คิดเป็นร้อยละ 10.81081 และ 1 วัน/สัปดาห์ มีจำนวน 1 คน คิดเป็นร้อยละ 2.702703 และน้อยกว่า 1 วัน/สัปดาห์ มีจำนวน 2 คน คิดเป็นร้อยละ 5.405405

ท่านมักจะใช้บริการในช่วงเวลาใดมากที่สุด ผู้ตอบแบบสำรวจความพึงพอใจส่วนใหญ่เป็นจะใช้ในช่วงเวลา 8.00 – 12.00 น. คิดเป็นร้อยละ 32.43243 มีจำนวน 12 คน รองลงมาเป็น 12.00 – 13.00 น. มีจำนวน 9 คน คิดเป็นร้อยละ 24.32421 รองลงมาอีกเป็น 13.00 – 16.00 น. มีจำนวน 8 คน คิดเป็นร้อยละ 21.62162 และ ช่วงเวลา 16.00 – 20.00 น มีจำนวน 2 คน คิดเป็นร้อยละ 5.405405 และ ช่วงเวลา 20.00 – 24.00 น. มีจำนวน 6 คน คิดเป็นร้อยละ 16.21622

สถานที่ที่ใช้บริการอินเทอร์เน็ตเป็นประจำ ผู้ตอบแบบสำรวจความพึงพอใจส่วนใหญ่เป็นสำ นักงาน ที่สังกัด มีจำนวน 27 คน คิดเป็นร้อยละ 72.97297 รองลงมาเป็นจุดให้บริการ Wireless บริเวณ (โปรดระบุ) มีจำนวน 6 คิดเป็นร้อยละ 16.21622 ต่ำสุด ห้องสมุด มีจำนวน 2 คน คิดเป็นร้อยละ 5.405405 และหอพักของวิทยาลัย มีจำนวน 2 คน คิดเป็นร้อยละ 5.405405

เว็บไซต์ที่เข้าใช้มากที่สุด ผู้ตอบแบบสำรวจความพึงพอใจส่วนใหญ่เป็น Google มีจำนวน 20 คน คิดเป็นร้อยละ 42.55319 รองลงมาเป็น Facebook มีจำนวน 15 คน คิดเป็นร้อยละ 31.91486 YouTube มีจำนวน 8 คน คิดเป็นร้อยละ 170.2128 ส่วนคนที่เข้าน้อยที่สุด LINE มีจำนวน 2 คน คิดเป็นร้อยละ 4.255319 และ Yahoo มีจำนวน 2 คน คิดเป็นร้อยละ 4.255319

ท่านรู้จักเว็บไซต์ของวิทยาลัยจากที่ใด ผู้ตอบแบบสำรวจความพึงพอใจส่วนใหญ่จะเป็นการค้นหาจากเว็บไซต์ Google มีจำนวน 18 คน คิดเป็นร้อยละ 48.64865 รองลงมาเป็นการแนะนำจากเพื่อน มีจำนวน 7 คน คิดเป็นร้อยละ 18.91892 และ รองลงมาอีกเป็นแห่งที่อื่น ๆ (โปรดระบุ) มีจำนวน 5 คน คิดเป็นร้อยละ 13.51351 และ จากแผ่นพับที่วิทยาลัยแจก มีจำนวน 4 คน คิดเป็นร้อยละ 10.81081 และ จากลิงค์จากเว็บอื่นมีจำนวน 3 คน คิดเป็นร้อยละ 8.108108

ท่านเข้าชมเว็บไซต์ของวิทยาลัยบ่อยแค่ไหน ผู้ตอบแบบสำรวจความพึงพอใจส่วนใหญ่จะไม่เคยเข้า มีจำนวน 23 คน คิดเป็นร้อยละ 67.64706 รองลงมาความพึงพอใจเข้าใช้เว็บไซต์ของวิทยาลัยมากสุด 1-2 ครั้งต่อสัปดาห์ มีจำนวน 6 คน คิดเป็นร้อยละ 17.64706 และ รองลงมาอีกเป็น

1-2 ครั้งต่อเดือน มีจำนวน 3 คน คิดเป็นร้อยละ 8.823529 และ น้อยกว่า 1 ครั้งต่อเดือน มีจำนวน 2 คน คิดเป็นร้อยละ 2.882353

ท่านเข้าชมเว็บไซต์ของวิทยาลัยเพื่อใด ผู้ตอบแบบสำรวจความพึงพอใจส่วนใหญ่เป็นการอ่านข่าวสารใหม่ๆของวิทยาลัย มีจำนวน 11 คน คิดเป็นร้อยละ 47.82609 รองลงมาเพื่อวัตถุประสงค์อื่น ๆ (โปรดระบุ) ..... มีจำนวน 8 คน คิดเป็นร้อยละ 34.78261 และ รองลงมาอีกเพื่อหาข้อมูลเกี่ยวกับรายวิชาเรียน จำนวน 3 คน คิดเป็นร้อยละ 13.04348 และ ค้นหาเอกสารแบบฟอร์ม หรือบทความ มีจำนวน 1 คน คิดเป็นร้อยละ 4.347826

ท่านคิดว่าเว็บไซต์ของวิทยาลัยเป็นประโยชน์ต่อท่านหรือไม่ ผู้ตอบแบบสำรวจความพึงพอใจส่วนใหญ่เห็นว่าเป็นประโยชน์ แต่ยังไม่เพียงพอ มีจำนวน 16 คน คิดเป็นร้อยละ 59.25926 รองลงมาค่อนข้างเป็นประโยชน์ มีจำนวน 7 คน คิดเป็นร้อยละ 25.92593 และ ไม่เป็นประโยชน์เลย มีจำนวน 4 คน คิดเป็นร้อยละ 14.81481

ส่วนที่ 2 แบบสอบถามความพึงพอใจของอาจารย์ที่ใช้งาน Internet ในวิทยาลัยพลศึกษาของผู้ทำแบบสำรวจ

งานนิพนธ์ครั้งนี้ผู้ทำงานนิพนธ์ได้ดำเนินการทดสอบการใช้งานระบบเครือข่ายในวิทยาลัยพลศึกษา เพื่อวัดความพึงพอใจของการใช้งาน ผู้ทำงานนิพนธ์จึงได้ทำแบบสำรวจความพึงพอใจต่อการใช้งานใน 11 ด้าน ดังนี้

1. สัญญาณ Wireless ครอบคลุมทั่วถึง
2. ความสะดวกความเร็วในการเชื่อมต่อสัญญาณ Wireless ก่อนเข้าใช้งาน
3. ความเร็วของการส่งข้อมูล และ ใช้อินเทอร์เน็ต ได้รวดเร็วหรือไม่
4. สามารถตอบสนองความต้องการของผู้ใช้บริการมีระบบ Authentication เวลาเครือข่ายไร้ สายเพื่อตรวจสอบสิทธิ์ผู้ใช้
5. ท่านคิดว่า Authentication เครือข่ายไร้สายของวิทยาลัยเป็นประโยชน์ต่อท่านหรือไม่
6. ท่านคิดว่า Authentication เครือข่ายไร้สายของวิทยาลัยจะมีความปลอดภัยต่อท่านหรือไม่
7. ท่านคิดว่า Authentication ของวิทยาลัยจะมีความล่าช้าต่อท่านหรือไม่
8. ความมีเสถียรภาพของระบบฯ Authentication เวลาเครือข่ายไร้สาย
9. ความสะดวกในการเข้าถึงระบบ Authentication เครือข่ายคอมพิวเตอร์ที่เป็นระบบสาย (LAN) ของวิทยาลัย (LAN)
10. ความเร็วในการใช้งาน Internet ผ่านระบบเครือข่ายคอมพิวเตอร์ของวิทยาลัย (LAN)

11. ความมีเสถียรภาพของระบบฯ สามารถใช้งาน Internet ได้อย่างต่อเนื่อง (LAN)

ผู้ทำงานนิพนธ์ได้ทำการวิเคราะห์ข้อมูลความพึงพอใจในภาพรวมของแบบสำรวจความพึงพอใจต่อการใช้งานระบบเครือข่ายของผู้ใช้งานในวิทยาลัยพลศึกษา โดยมีรายละเอียดดังแสดงในตารางที่ 4-13

ตาราง 4-13 ความพึงพอใจของอาจารย์ที่ใช้งานระบบเครือข่ายในวิทยาลัยพลศึกษา

รายการ	ระดับความพึงพอใจ					
	แย่มาก	แย่	ปานกลาง	ดี	ดีมาก	X
1. สัญญาณ Wireless ครอบคลุมทั่วถึง	3	9	14	8	1	35
ร้อยละ	8.571	25.71	40	22.85	2.85	100
2. ความสะดวกความเร็วในการเชื่อมต่อสัญญาณ Wireless ก่อนเข้าใช้งาน	2	6	19	7	1	35
ร้อยละ	5.71	17.14	54.28	20	2.85	100
3. ความเร็วของสัญญาณในการส่งข้อมูลและ ใช้อินเทอร์เน็ต ได้รวดเร็วหรือไม่	2	4	20	9	0	35
ร้อยละ	5.71	11.43	57.14	25.71	0	100
4. สามารถตอบสนองความต้องการของผู้ใช้บริการมีระบบ Authentication เวลาเครือข่ายไร้สายเพื่อตรวจสอบสิทธิ์ผู้ใช้	1	4	23	6	1	35
ร้อยละ	2.85	11.43	65.71	17.14	2.85	100
5. ท่านคิดว่า Authentication เครือข่ายไร้สายของวิทยาลัยเป็นประโยชน์ต่อท่านหรือไม่	0	1	6	25	3	35
ร้อยละ	0	2.85	17.14	71.42	8.57	100
6. ท่านคิดว่า Authentication เครือข่ายไร้สายของวิทยาลัยจะมีความปลอดภัยต่อท่านหรือไม่	0	2	14	19	0	35

ตาราง 4-13 ความพึงพอใจของอาจารย์ที่ใช้งานระบบเครือข่ายในวิทยาลัยพลศึกษา (ต่อ)

ร้อยละ	ระดับความพึงพอใจ					
	แย่มาก	แย่	ปานกลาง	ดี	ดีมาก	X
ร้อยละ	0	5.71	40	54.28	0	100
7. ท่านคิดว่า Authentication ของวิทยาลัยจะมีความล่าช้าต่อท่านหรือไม่	0	1	9	23	2	35
ร้อยละ	0	2.85	25.71	65.71	5.71	100
8. ความมีเสถียรภาพของระบบฯ Authentication เวลาเครือข่ายไร้สาย	0	2	19	13	1	35
ร้อยละ	0	5.71	54.28	37.14	2.85	100
9. ความสะดวกในการเข้าถึงระบบ Authentication เครือข่ายคอมพิวเตอร์ที่เป็นระบบสาย (LAN) ของวิทยาลัย (LAN)	0	0	0	2	0	2
ร้อยละ	0	0	0	100	0	100
10. ความเร็วในการใช้งาน Internet ผ่านระบบเครือข่ายคอมพิวเตอร์ของวิทยาลัย (LAN)	0	0	0	1	1	2
ร้อยละ	0	0	0	50	50	100
11. ความมีเสถียรภาพของระบบฯ สามารถใช้งาน Internet ได้อย่างต่อเนื่อง (LAN)	0	0	0	2	0	2
ร้อยละ	0	0	0	100	0	100

จากตาราง 4-13 พบว่าผลการวิเคราะห์แบบสำรวจความพึงพอใจของอาจารย์ที่ใช้งานระบบเครือข่ายในวิทยาลัยพลศึกษา ส่วนใหญ่แล้วจะอยู่ในระดับพอ ใจในระดับกลาง โดยมีข้อมูลสรุปความพึงพอใจของอาจารย์ที่ใช้งานสัญญาณ Wireless ครอบคลุมทั่วถึงอยู่ในระดับกลาง และการความพึงพอใจของอาจารย์ที่ใช้งานเครือข่ายคอมพิวเตอร์ที่เป็นระบบสาย (LAN) อยู่ในระดับด

บทที่ 5

สรุปผลการติดตั้ง

ผู้ทำงานนิพนธ์มีวัตถุประสงค์ที่จะศึกษาระบบเครือข่ายที่มีประสิทธิภาพ โดยผู้ทำงานนิพนธ์ได้เลือกศึกษา pfSense เพื่อใช้ระบุสิทธิ์การเข้าถึงข้อมูลต่าง ๆ ไม่ว่าจะเป็นฐานข้อมูล อีเมล์ เว็บไซต์ ไฟล์ภาพ เพลง ซึ่งผู้ใช้งานที่รู้เท่าไม่ถึงการณ์อาจดาวน์โหลดไฟล์ที่มีความเสี่ยงด้านความปลอดภัย ทำให้เกิดปัญหาและนำความเสียหายมาสู่ในระบบเครือข่าย เช่น กระทบต่อการทำงานของแอพพลิเคชั่นหลักของผู้ใช้งาน ทำให้การทำงานมีความล่าช้า หรือ คอมพิวเตอร์ติดไวรัส เป็นผลให้การเข้าใช้งานเว็บไซต์ไม่มีความน่าเชื่อถือ และ นำความเสียหายมาให้ผู้ใช้งานอื่นๆ

วัตถุประสงค์อีกด้านหนึ่ง คือ ผู้ทำงานนิพนธ์ต้องการช่วยออกแบบเครือข่ายคอมพิวเตอร์ให้กับวิทยาลัยพลศึกษา ซึ่งมีบทบาทสำคัญต่อการพัฒนาการศึกษา และ ใช้ระบบเครือข่ายคอมพิวเตอร์เป็นสื่อสำหรับการเรียนการสอน รวมถึงใช้ค้นหาข้อมูล ประมวลผลและเพิ่มศักยภาพด้านการสื่อสารจากแหล่งเรียนรู้ได้มากขึ้นที่หลากหลาย

ในงานนิพนธ์นี้ผู้ทำงานนิพนธ์ได้ไปติดตั้งระบบเครือข่ายให้วิทยาลัยพละศึกษาบ้านท่งบัง เมืองสีโคตระบอง นครหลวงเวียงจันทน์ ประเทศลาว ในขั้นแรก ผู้ทำงานนิพนธ์ได้ไปสำรวจสถานที่เพื่อออกแบบระบบเครือข่ายตามความต้องการของวิทยาลัยพลศึกษาซึ่งมีสามระบบเครือข่าย 1) ระบบเครือข่ายภายในอาคาร A, 2) ระบบเครือข่ายภายในอาคาร B, C, และ D, และ 3) ระบบเครือข่ายไร้สาย (Wi-Fi หรือ Wireless) 4 จุด โดยวิทยาลัยพลศึกษา มีสองห้อง LAB

หลังจากออกแบบแล้ว ผู้ทำงานนิพนธ์ได้ออกแบบระบบเครือข่ายทั้งแบบใช้สาย และแบบไร้สาย โดยได้ติดตั้ง pfSense ในสถานที่ทดลอง ก่อนที่จะติดตั้งระบบจริง ให้กับวิทยาลัยฯ เพื่อให้วิทยาลัยฯ มีระบบเครือข่ายที่มีความปลอดภัย โดยระบบที่ติดตั้งในสถานที่จริงมีดังนี้

ผู้ทำงานนิพนธ์ได้ออกแบบ และ ติดตั้งระบบเครือข่ายท้องถิ่นและเครือข่ายไร้สายในอาคาร A, และ B, C, D นอกจากนั้น ผู้ทำงานนิพนธ์ยังได้ ติดตั้ง pfSense, DHCP server, DNS, เครื่องแม่ข่าย Proxy, Captive Portal, เครื่องแม่ข่าย RADIUS, พร้อมกำหนดค่าจำกัดแบนด์วิดท์ (Download และ Upload), บล็อก YouTube และ Facebook, ทำ NAT และ Port Forwarding , ติดตั้ง IPsec VPN, OpenVPN, ทำเว็บไซต์ของวิทยาลัยพลศึกษา , และ การติดตั้งซอฟต์แวร์ป้องกัน VIRUS

ผลการทดลองในสถานที่จริงเป็นไปตามผลการทดลองในบทที่ 4 ซึ่งสามารถสรุปได้ว่าการติดตั้งระบบเครือข่ายที่ออกแบบมีประสิทธิภาพในการใช้งานจริงได้พอสมควร กล่าวคือ ค่าล่าช้าที่ได้รับจากการ ping มีค่าน้อยเป็นที่พึงพอใจของผู้ใช้แบนด์วิดท์ของอินเทอร์เน็ต (อัพโหลดและดาวน์โหลด) เป็นไปตามที่คาดว่าจะรับจาก ISP ผู้ทำงานนิพนธ์สามารถเข้าไปที่เครื่องแม่ขาย pfSense และ

เครื่องแม่ข่าย Web Server ได้โดยการกำหนดค่า Port forwarding และ กฎไฟร์วอลล์ สามารถยืนยันตัวตนก่อนการเข้าใช้อินเทอร์เน็ต (Authentication) โดยใช้ Captive Portal สามารถตรวจสอบชื่อผู้ใช้และรหัสของผู้ใช้ที่เครื่องแม่ข่าย RADIUS, และ จำกัดแบนด์วิดท์ให้กับเครื่องในห้อง Lab (เครื่องในห้อง Lab สามารถดาวน์โหลด YouTube ได้พร้อมกัน) โดยผู้ทำงานนิพนธ์กำหนดแบนด์วิดท์ให้สามารถการอัพโหลด 1.00 Mbps และดาวน์โหลดอยู่ที่ 0.50 Mbps นอกจากนั้นบุคคลากรยังสามารถทำรีโมทล็อกอิน ใช้ทรัพยากรในเครือข่ายของวิทยาลัย ได้จากภายนอกเครือข่าย (VPN) และสามารถดูรายการเข้าใช้งานเครือข่ายของ Squid ที่ผู้ใช้เข้าใช้งานเว็บต่าง ๆ ได้จริง และผลการวิเคราะห์แบบสำรวจความพึงพอใจของอาจารย์ที่ใช้งานระบบเครือข่ายในวิทยาลัยพลศึกษาส่วนใหญ่แล้วจะอยู่ในระดับพึงพอใจในระดับกลาง โดยมีความพึงพอใจต่อความครอบคลุมของสัญญาณ Wireless อยู่ในระดับกลาง และ ความพึงพอใจที่ใช้งานเครือข่ายคอมพิวเตอร์ที่เป็นระบบสาย (LAN) อยู่ในระดับดี

บรรณานุกรม

นภดล สุขศรี. (2012). *คู่มือติดตั้งและใช้งาน pfSense*. กรุงเทพ: ซีเอ็ดยูเคชั่น.

น.ท.ภาณุฤทธิ์ ยุกตะทัต. (2544). *กลยุทธ์การวางระบบเครือข่ายฉบับ SME*. กรุงเทพ: โรงพิมพ์ DLS.

ธวัชชัย ชมศิริ. (2547). *ติดตั้ง/ดูแลระบบเครือข่ายคอมพิวเตอร์ย่างมืออาชีพ*. กรุงเทพ: บริษัท เอช.เอ็น. กรุ๊ป จำกัด.

อธิพงศ์ คำสีลา, สมนึก พ่วงพรพิทักษ์และสุชาติ คุ้มมะณี. (2557). การปรับปรุงการจัดการฏไฟร์วอลล์ด้วยแนวคิดการตัดสินใจแบบโดเมนเดี่ยว. *วารสารเทคโนโลยีสารสนเทศ (Information Technology Journal) คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ*, 10(2), 7-14.

Chris Buechler, Scott Ullrich. (2004). *pfSense*. ค้นเมื่อ 12 กุมภาพันธ์ 2559, จากเว็บไซต์ https://www.pfsense.org/.

Christopher M. Buechler, Jim Pingle. (2009). *pfSense The Definitive Guide to the Open Source Firewall and Router Distribution*. Publisher: Reed Media Services.

James F. Kurose, Keith W. Ross. (2012). *Computer Networking: A Top-Down Approach*. Publisher: Pearson.

Jeffrey A.Hoffer, Joey F. George & Joseph S. Vatacich. (2547). *การวิเคราะห์ และ ออกแบบระบบ (Modem Systems Analysis & Design)*. กรุงเทพ: บริษัท เอช.เอ็น. กรุ๊ป จำกัด.

Matt Williamson. (2011). *pfSense 2 Cookbook Mar*. Publisher: Packet Publishing.

Poramays T. (2011). *ตอนที่ 3 การติดตั้ง pfSense Squid Proxy Configuration*. ค้นเมื่อ 30 มีนาคม 2559 จากเว็บไซต์ https://www.youtube.com/watch?v=ejxClHbF0u0.

Supawish Tanacharoenpradit. (2010). *การติดตั้ง pfSense ตอนที่ 1*. ค้นเมื่อ 22 มีนาคม 2559 จากเว็บไซต์ https://www.youtube.com/watch?v=Ur7oSvEofrk.

ภาคผนวก

ภาคผนวก ก

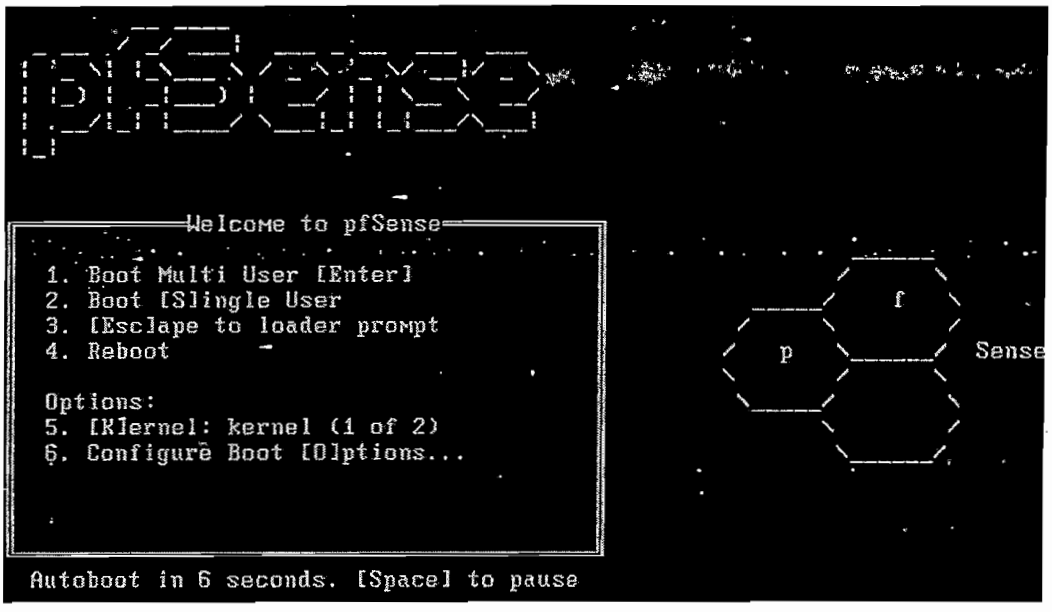
การติดตั้ง และ การตั้งค่า pfSense

ก. การติดตั้ง และ ตั้งค่าระบบ pfSense

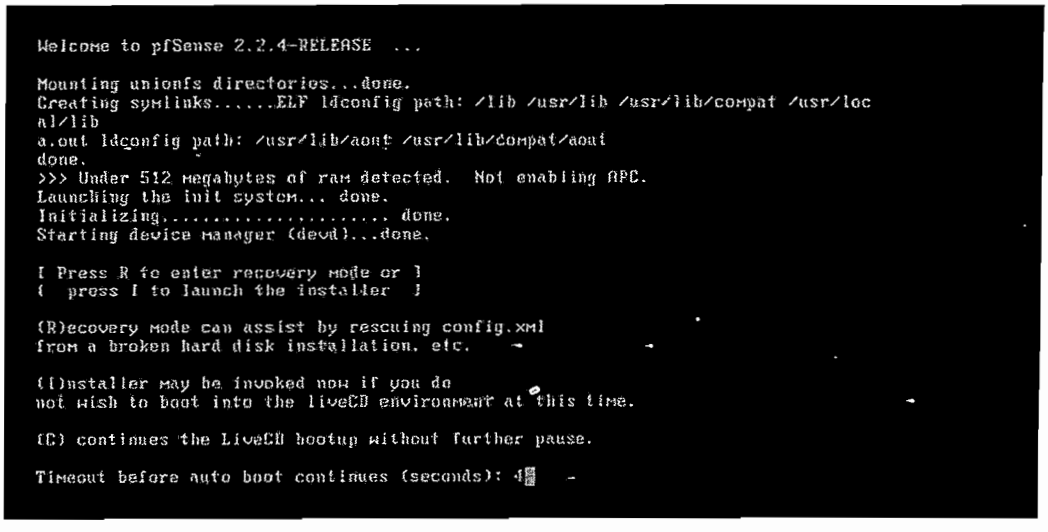
ก.1 ขั้นตอนการติดตั้ง pfSense

ก.1.1 ติดตั้ง BIOS ให้ Boot CD/DVD

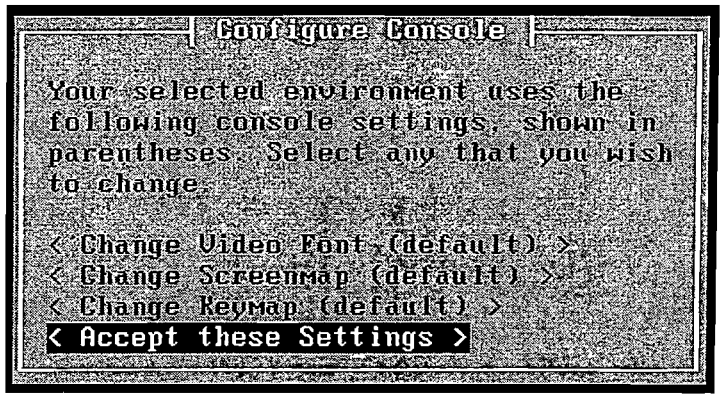
ก.1.2 หน้าแสดงเมนูการติดตั้ง ดังภาพข้างล่าง



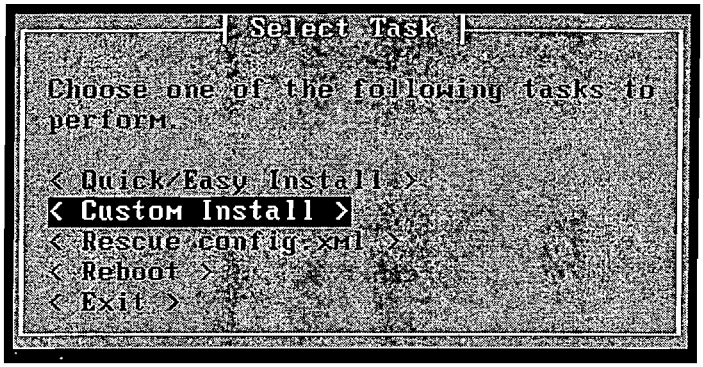
ก.1.3 ให้กด I เพื่อทำการติดตั้ง (Installer)



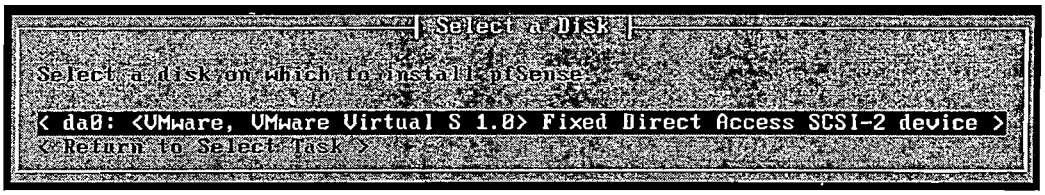
ก.1.4 เลือก Accept these Settings แล้วกด Enter



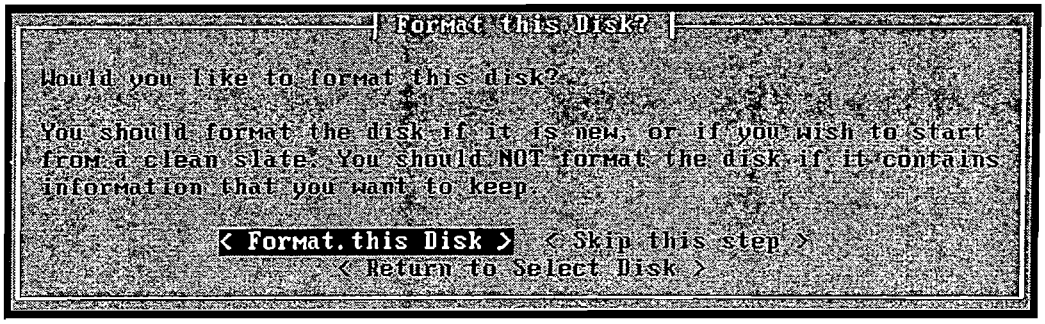
ก.1.5 เลือกการติดตั้งด้วยตนเอง Custom Install แล้วกด Enter



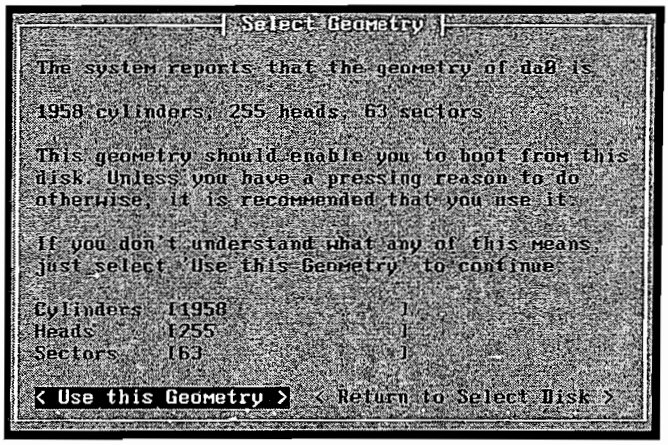
ก.1.6 เลือก Hard disk ที่ต้องการติดตั้ง <ad0: 2048MB <VBOX HARDDISK 1.0> at ata0-mater UDMA33> แล้วกด enter



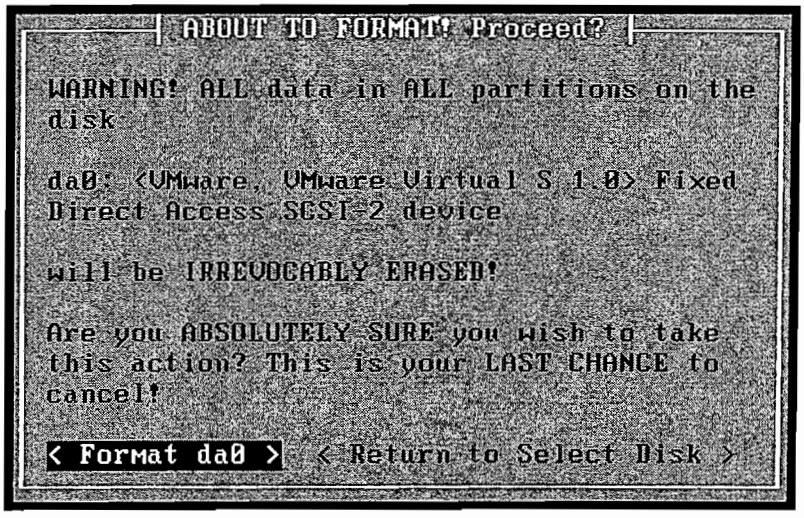
ก.1.7 เลือก Format ข้อมูลที่อยู่ใน Hard disk <Format this Disk> แล้วกด enter



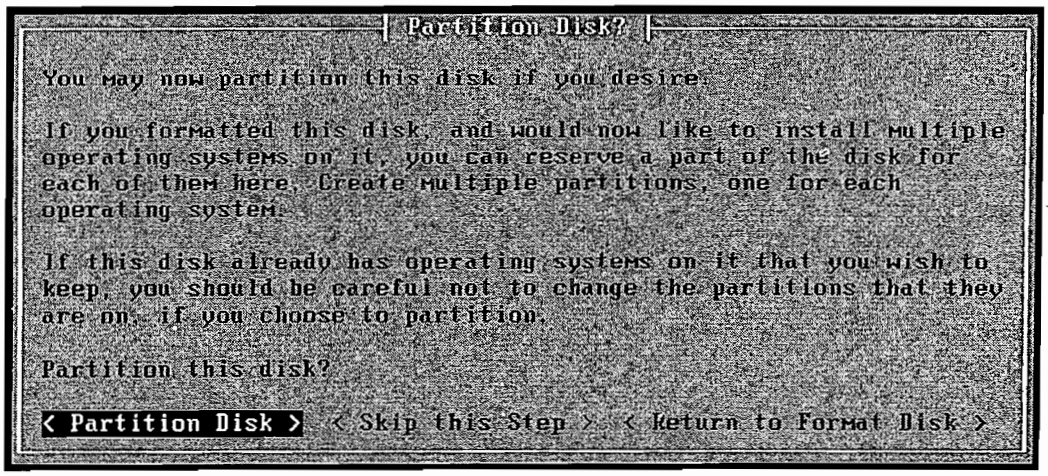
ก.1.8 เลือกโดยสร้างการแบ่งฮาร์ดดิสต์ <Use the Geometry> แล้วกด enter



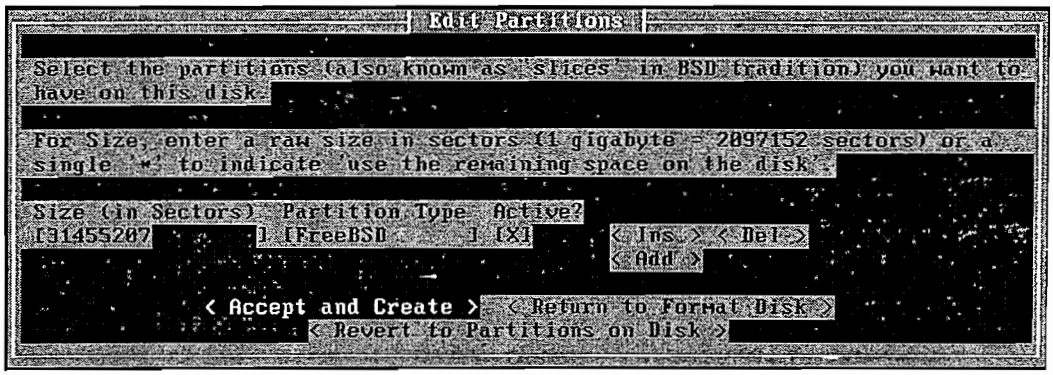
ก.1.9 เลือก <Format da0> แล้วกด enter



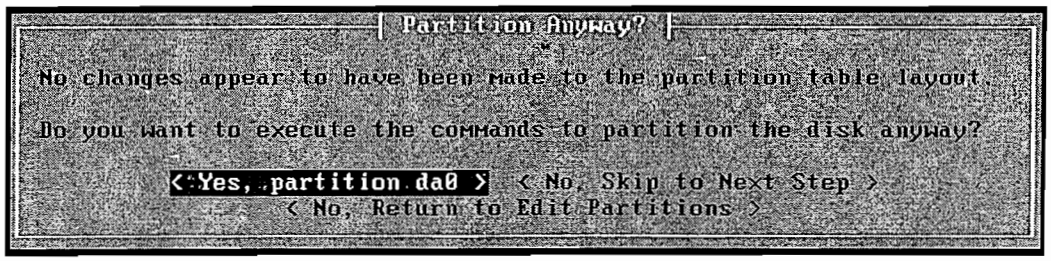
ก.1.10 การเข้าไปกำหนดพื้นที่ของ Disk โดย เลือก <Partition Disk> แล้วกด Enter



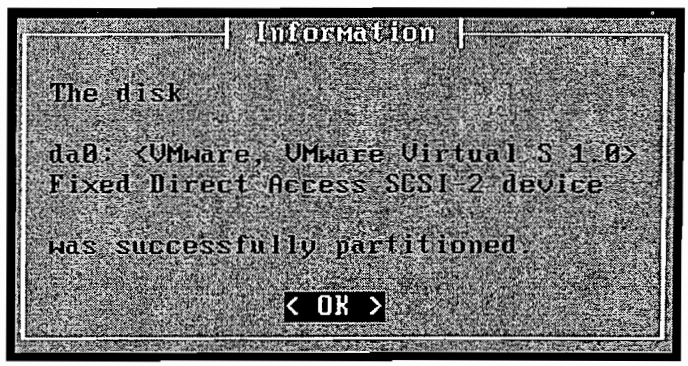
ก.1.11 การกำหนดพื้นที่ของ Disk เลือก <Accept and Create> แล้วกด Enter



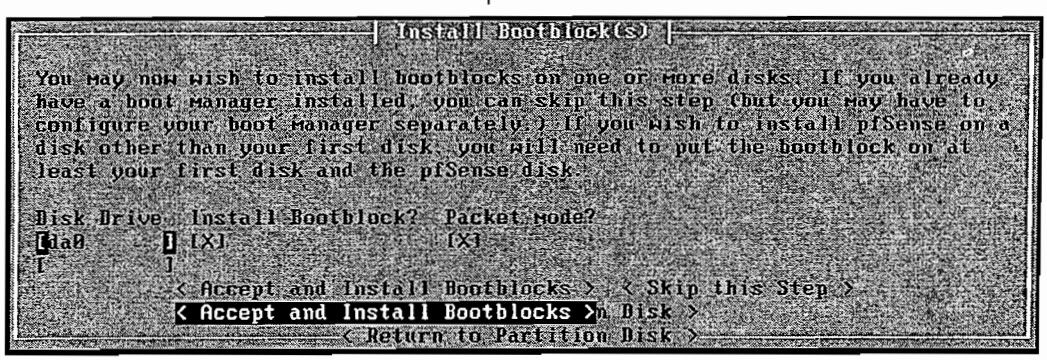
ก.1.12 เลือก <Yes, Partition da0> แล้วกด Enter



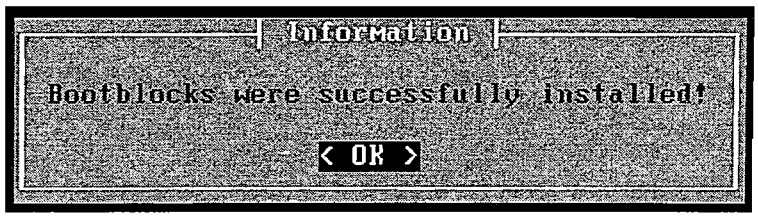
ก.1.13 เลือก <OK> แล้วกด Enter



ก.1.14 เริ่มทำการติดตั้ง เลือก <Accept and install Boot blocks> แล้วกด Enter

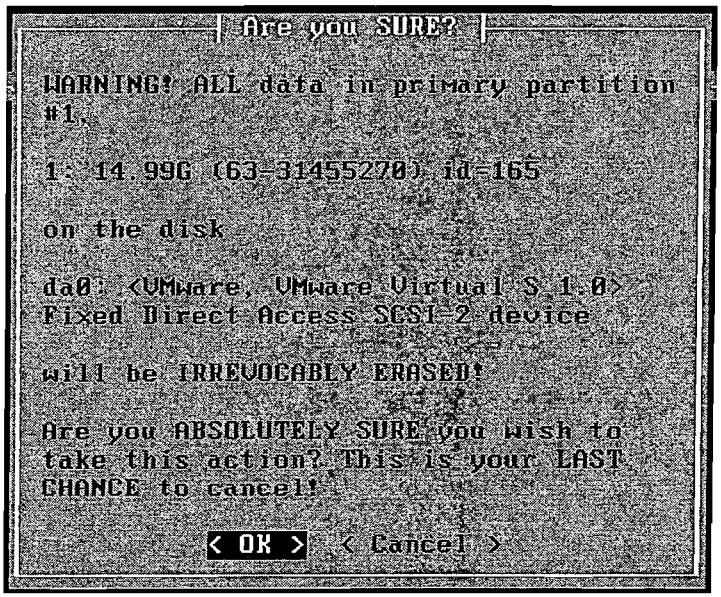


ก.1.15 เลือก <OK> แล้วกด Enter

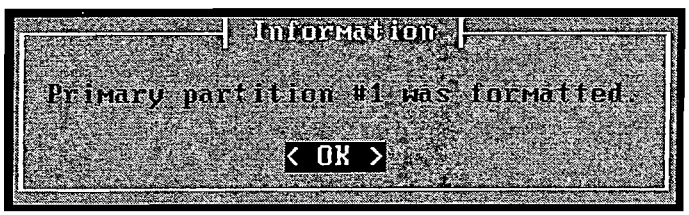


ก.1.16 เลือก Primary partition <1: 19.99G (63-41929650) id=165> แล้วกด Enter

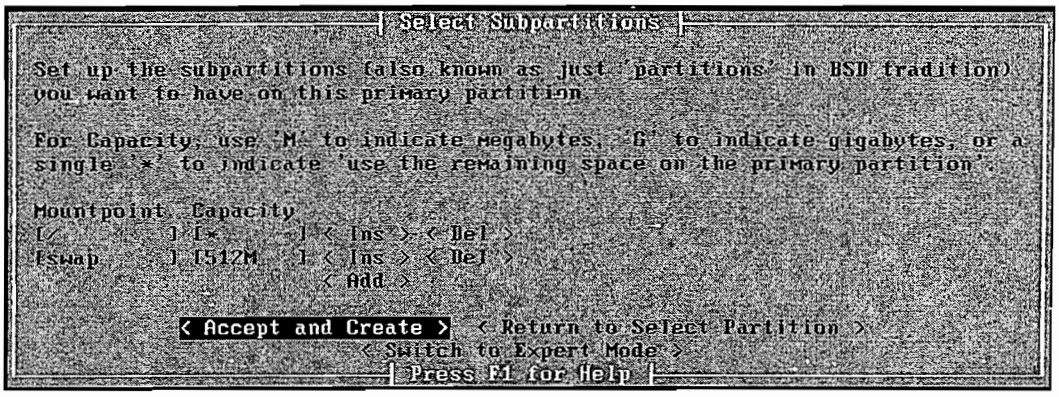
ก.1.17 เลือกยืนยันการ format (<OK>) แล้วกด Enter



ก.1.18 เลือก <OK> แล้วกด Enter

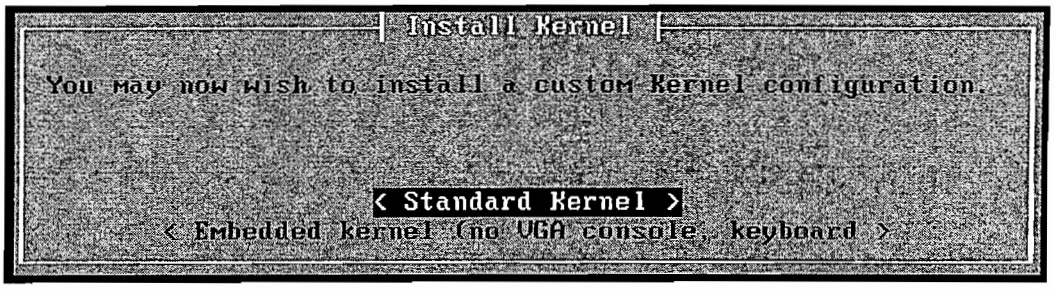


ก.1.19 เลือก <Accept and Create> เพื่อสร้าง Sub partitions ใน primary partition แล้วกด Enter

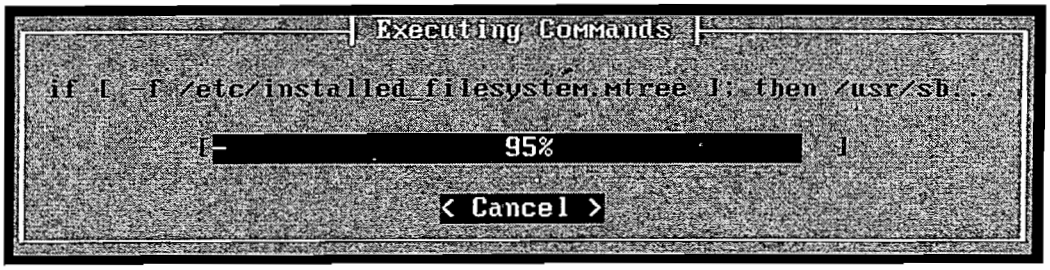


ก.1.20 รอจนกว่าจะถึง 100 %

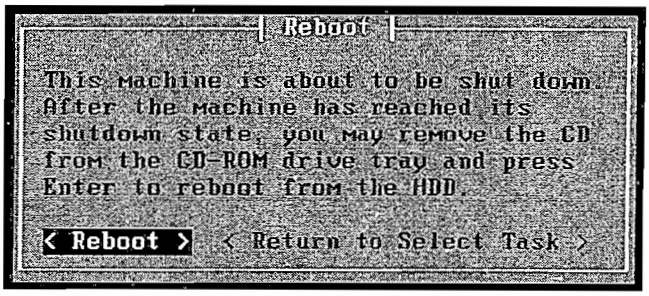
ก.1.21 เลือก < Standard Kernel > แล้วกด Enter



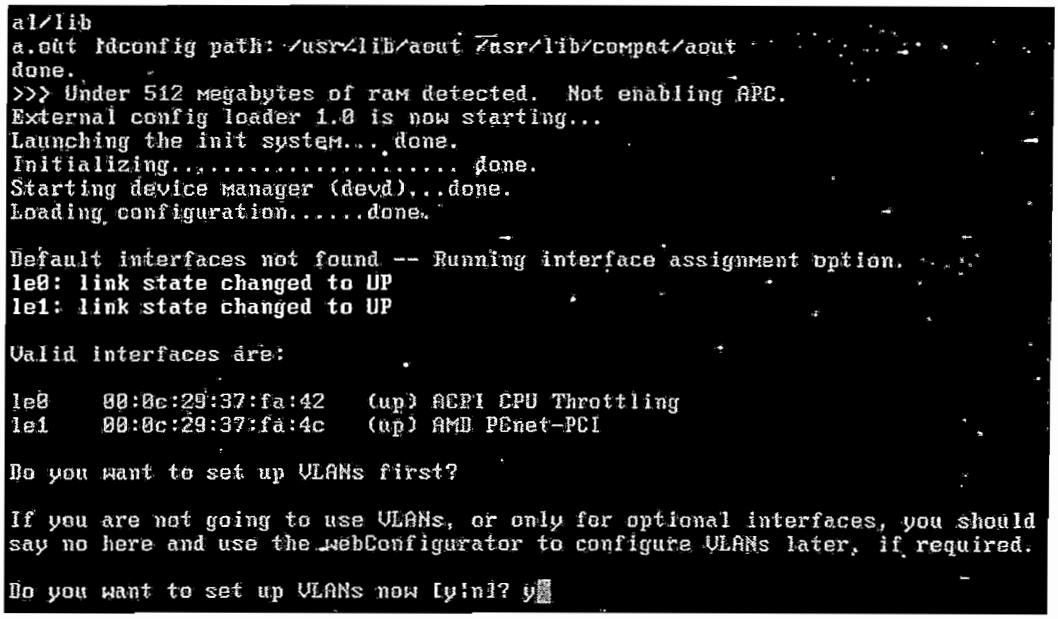
ก.1.22 รอจนกว่าถึง 100 %



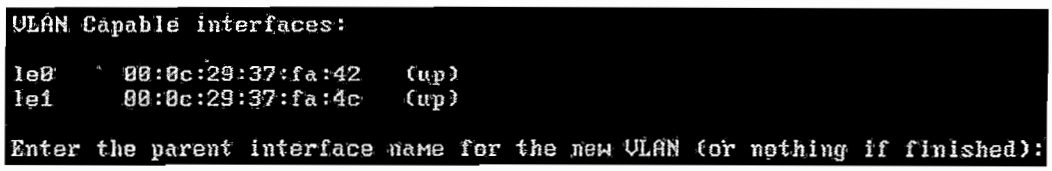
ก.1.23 เลือก <Reboot> แล้ว กด Enter

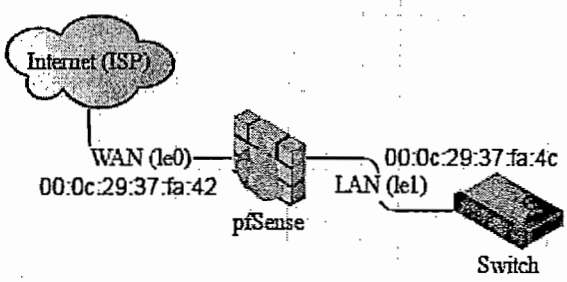


ก.1.24 หลังจาก reboot แล้วจะปรากฏหน้าจอดังนี้ หลังจากนั้นกด y แล้วกด Enter

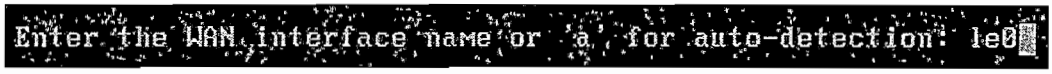


ก.1.25 กด Enter เพื่อกำหนด Interface ตามรายละเอียดในภาพด้านล่าง



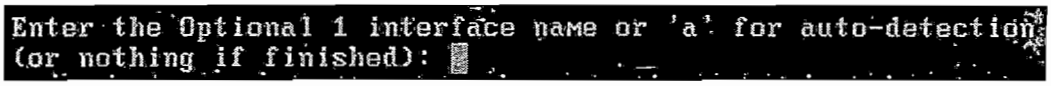


ก.1.26 พิมพ์ le0 สำหรับ Interface WAN แล้วกด Enter

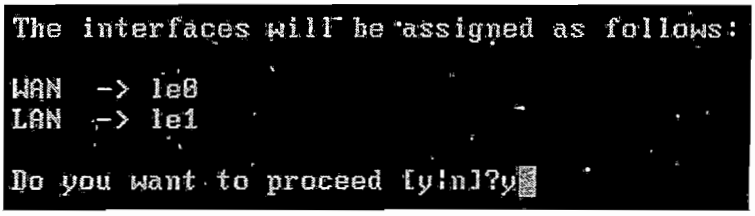


ก.1.27 พิมพ์ le1 สำหรับ Interface LAN แล้วกด Enter

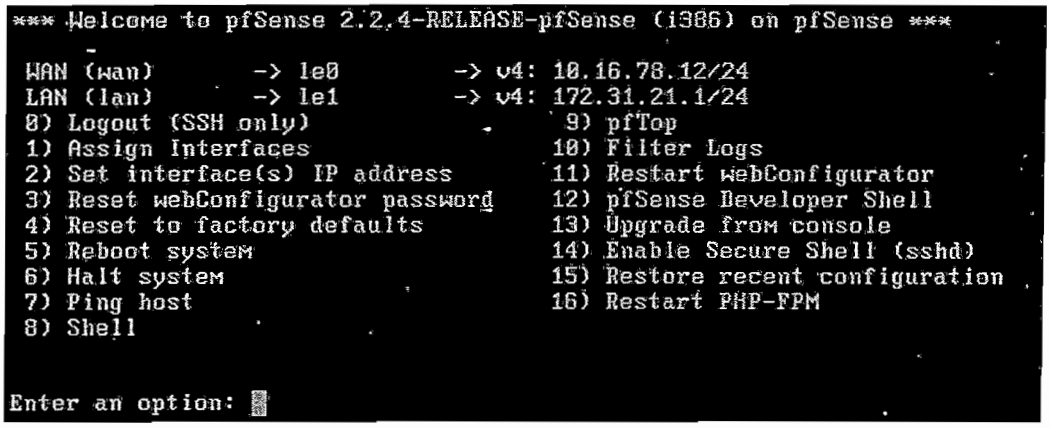
ก.1.28 กด Enter



ก.1.29 กด y แล้วกด Enter



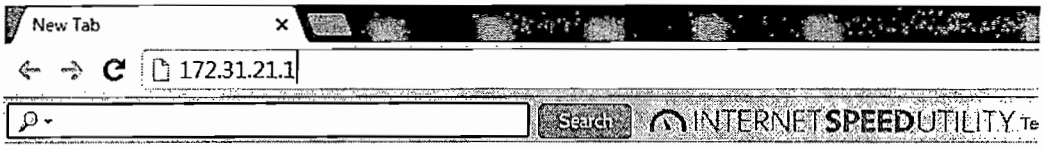
ก.1.30 จะได้หน้าจอดังนี้



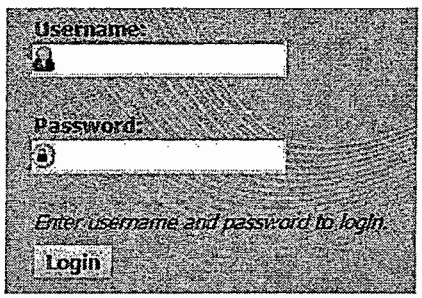
ก.2 การกำหนดค่า pfSense โดยใช้ Wizard

การตั้งค่า pfSense โดยใช้ Wizard เพื่อตั้งค่าใน Interface WAN และ LAN

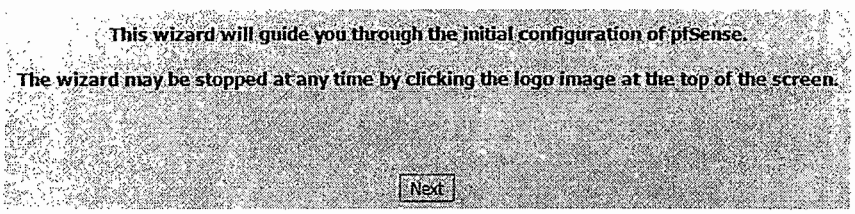
ก.2.1 เข้าระบบโดยใช้ 172.31.21.1



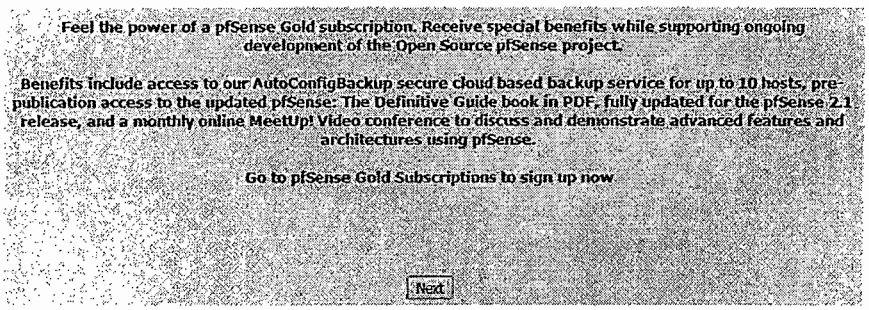
ก.2.2 ใส่ชื่อ (User: admin) และรหัสผ่าน (password: pfSense) เพื่อ login



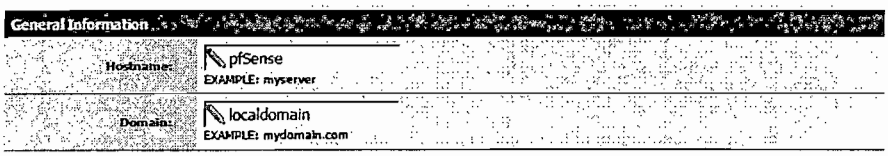
ก.2.3 คลิกที่ Next



ก.2.4 คลิกที่ Next



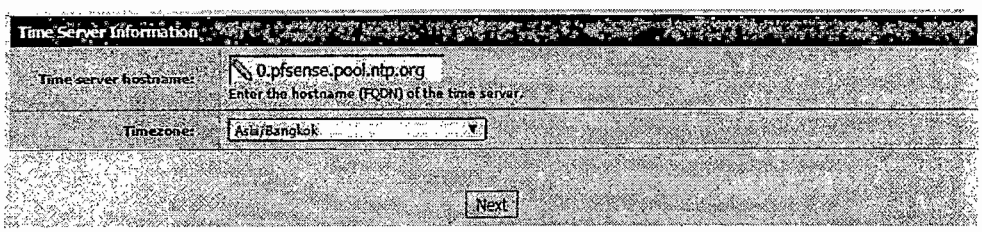
ก.2.5 กำหนดค่า Host และ Domain แล้ว คลิกที่ Next



ก.2.6 กำหนดค่า Time Server Information

1) Time zone: Asia/Bangkok (ใส่โซนของเวลา)

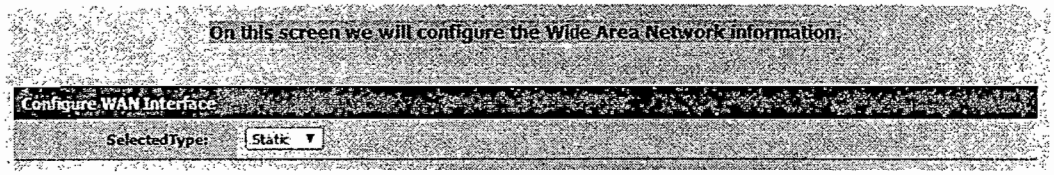
2) คลิกที่ Next



ก.2.7 กำหนดค่าเกี่ยวกับ Wide Area Network

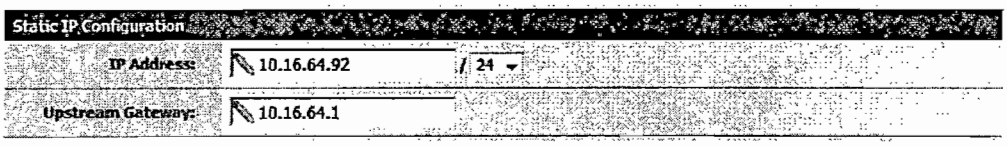
1) Configure WAN Interface: (ตั้งค่าอินเตอร์เฟส WAN)

- Selected Type: Static (เลือกที่อยู่หมายเลขไอพีแบบคงที่)



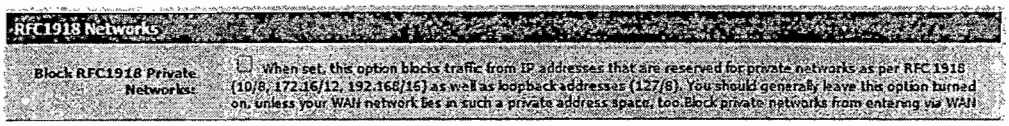
2) Static IP Configuration (ตั้งค่าไอพีในรูปแบบ Static)

- IP Address: 10.16.64.92 (ใส่ค่าหมายเลขไอพี)
- Upstream Gateway: 10.16.64.1



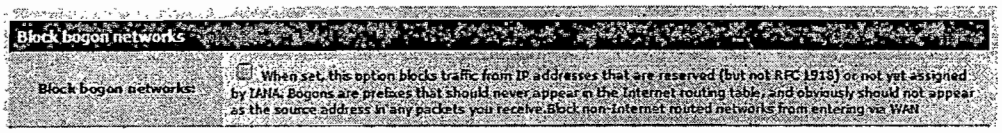
3) ยกเลิกการบล็อกข้อมูลที่มาจากที่อยู่หมายเลขไอพีแบบ Private

Block RFC1918 Private Networks: ☐ (When set...



4) ยกเลิกการบล็อกข้อมูลที่มาจากที่อยู่หมายเลขไอพีที่ถูกจองไว้ โดย IANA

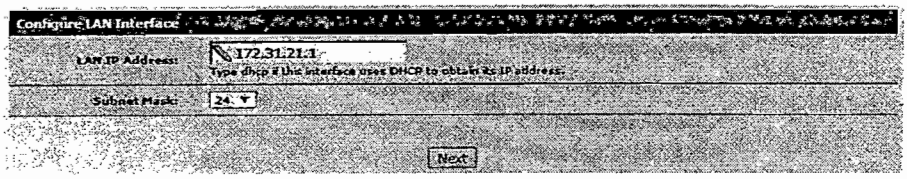
- Block bog on networks: ☐ (When set, this ...) แล้วคลิกที่ Next



ก.2.8 ตั้งค่าที่อยู่หมายเลขไอพี Interface LAN (Configure LAN Interface's IP address)

1) LAN IP Address: 172.31.21.1 (ใส่ค่าหมายเลขไอพีแอดของ LAN)

2) Subnet Mask: 24 (ใส่ค่าซับเน็ตมาส์ค) แล้วคลิก Next

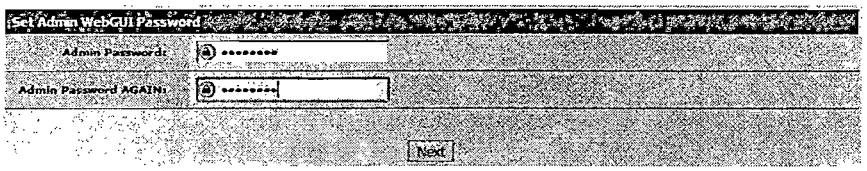


ก.2.9 กำหนด Set Admin Web GUI Password

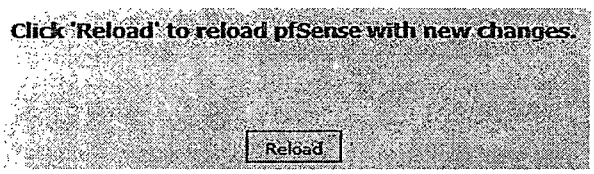
1) Admin Password: xxxxxxxxxx (ใส่รหัสของผู้ดูแลระบบ)

2) Admin Password AGAIN: xxxxxxxxxx (ยืนยันรหัสผู้ใช้ระบบ)

แล้ว คลิกที่ Next

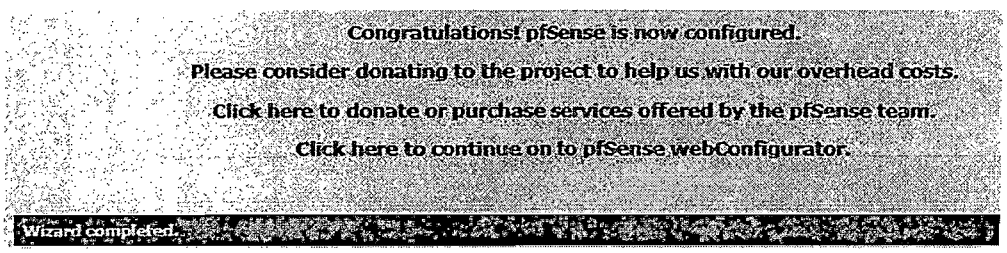


ก.2.10 คลิกที่ Reload

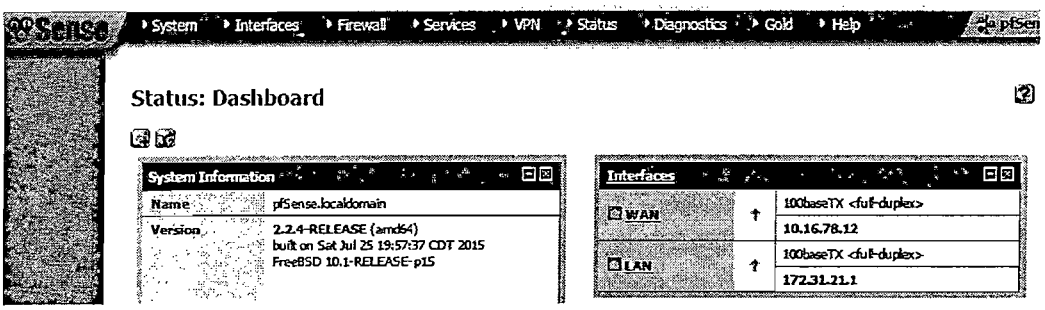


ก.2.11 รอโหลด pfSense

ก.2.12 คลิกที่ here



ก.2.13 ผลลัพธ์ของการตั้งค่า pfSense โดยใช้ Wizard



ก.3 การตั้งค่า DHCP server, DNS servers

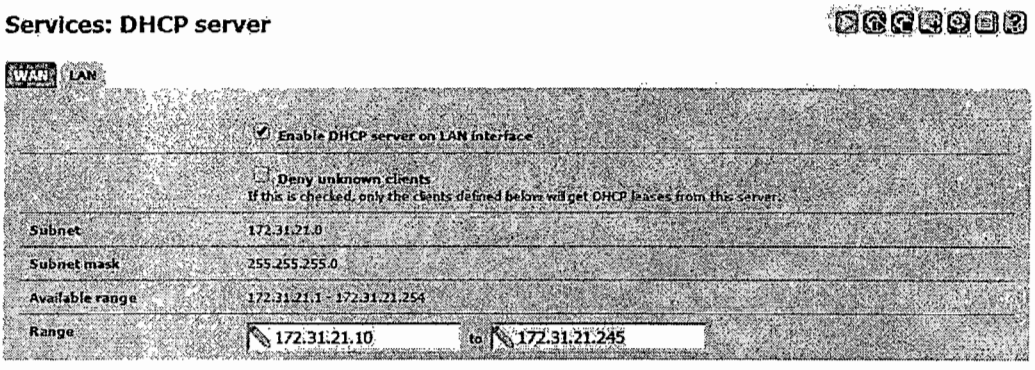
ก.3.1 การกำหนดตั้งค่า DHCP Server

1) ไปที่ Services | DHCP Server

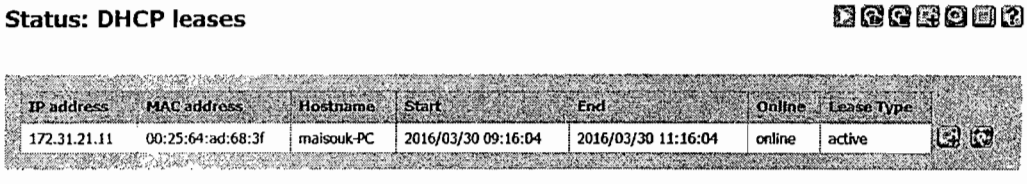
2) เข้าไปที่ LAN

☑ Enable DHCP server on LAN interface

- Range: 172.31.21.10 to 172.31.21.245 (กำหนดช่วงที่อยู่หมายเลขไอพีที่เครื่องแม่ข่าย DHCP จะแจกไปยังไคลเอนต์) แล้วคลิก Save



3) การแสดงผู้เข้าใช้งาน DHCP Server

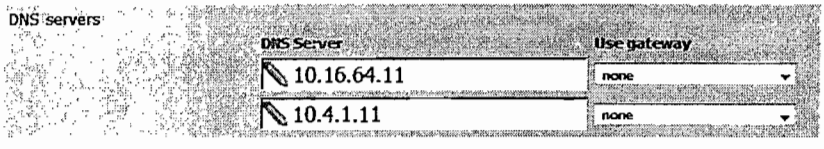


ก.3.2 การกำหนดตั้งค่า DNS Server

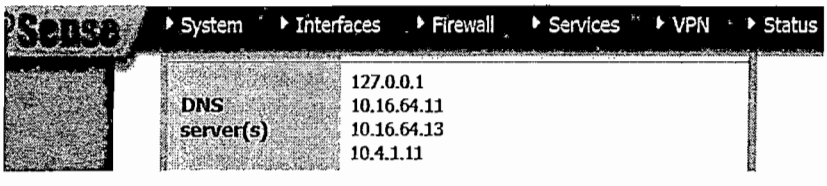
1) เข้าไปที่ System | General Setup

2) กำหนดค่าที่ System

- DNS Server: 10.16.64.11 และ 10.4.1.11 แล้วคลิก Save



3) ผลของการตั้งค่า DNS Server แสดงได้ดังนี้



ก.4 การตั้งค่าเครื่องแม่ข่าย Proxy

ขั้นตอนการกำหนดค่าที่เครื่องผู้ให้บริการเครื่องแม่ข่าย Proxy มีดังนี้

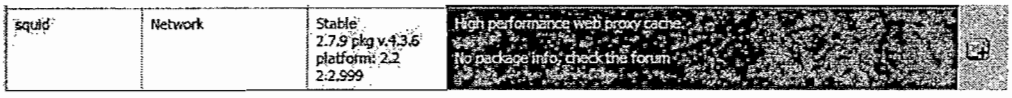
- ติดตั้งแพ็กเกจของ Proxy Server
- ตั้งค่า Proxy Server
- ติดตั้งแพ็กเกจในการตรวจสอบของการใช้งาน Proxy Server
- ตั้งค่า Lightsquid และ ตรวจสอบไคลเอนต์ที่เข้าไปเว็บต่าง ๆ

ก.4.1 การติดตั้งแพ็กเกจของ Proxy Server

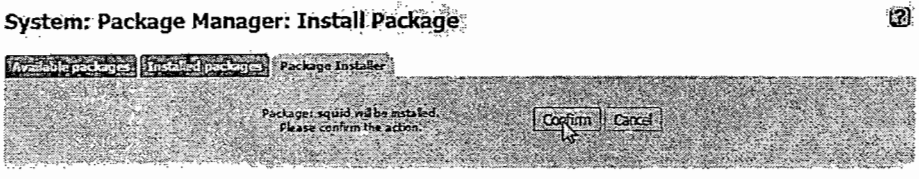
1) คลิก System | แพ็กเกจ

2) เข้าไปที่ Available แพ็กเกจ

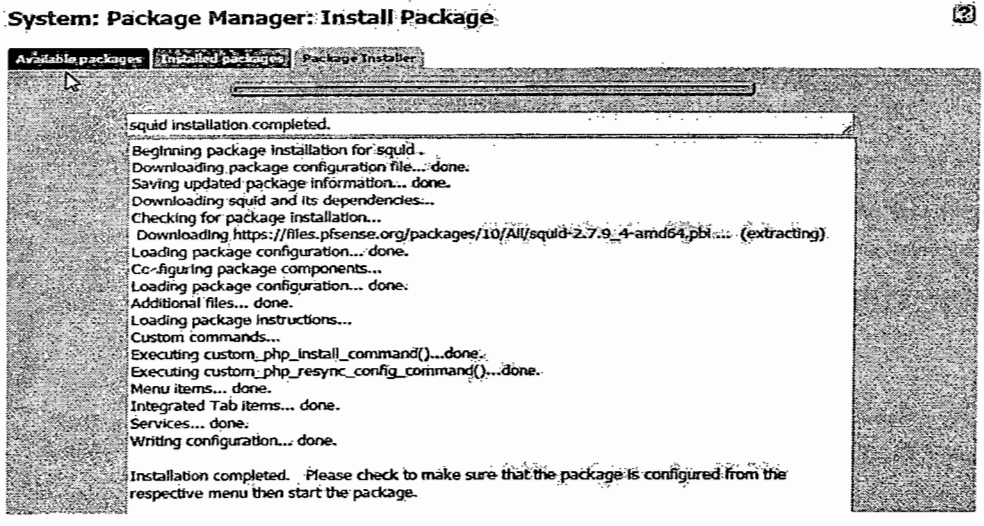
3) เลือกหาแพ็กเกจที่มีชื่อว่า Squid แล้วคลิกที่เครื่องหมาย 



4) คลิกไปที่ Config



5) รอการดาวน์โหลดและติดตั้ง Squid จนให้ติดตั้งเสร็จ ดังภาพด้านล่าง

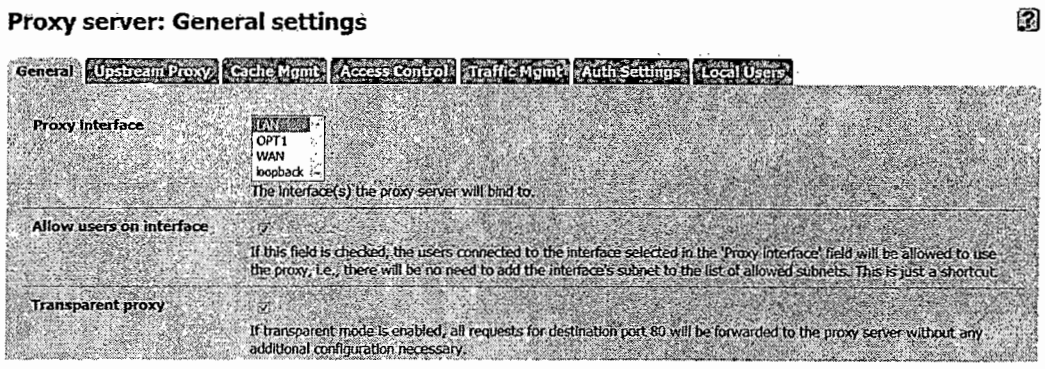


ก.4.2 การตั้งค่าเครื่องแม่ข่าย Proxy

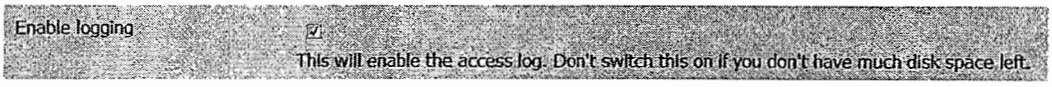
1) คลิก Service | Proxy Server

2) ทำการกำหนดที่ General

- Proxy interface: LAN
- Allow users on interface: ☑ If this field is checked...
- Transparent proxy: ☑ If transparent mode is enabled.....



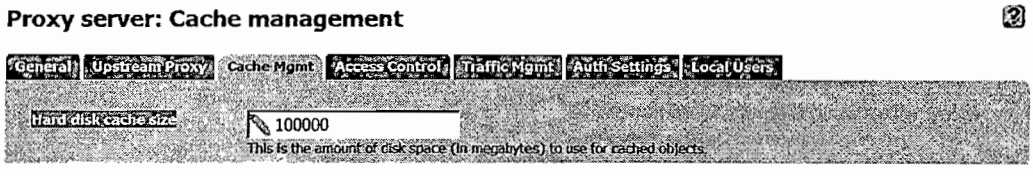
- Enable logging: ☑ This will enable the access log. Don't...



- Save

3) การตั้งค่าที่ Cache Mgmt

- Hard disk cache size: 100000
- Save



4) การตั้งค่าที่ Access Control

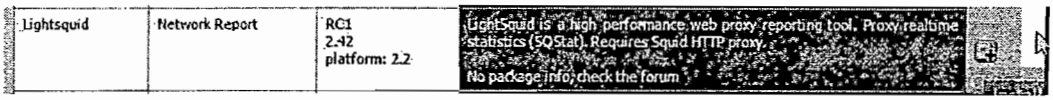
- External Cache-Managers: 127.0.0.1
- Save

ก.4.3 การติดตั้งแพ็กเกจ Lightsquid เพื่อตรวจสอบของการใช้งาน Proxy Server

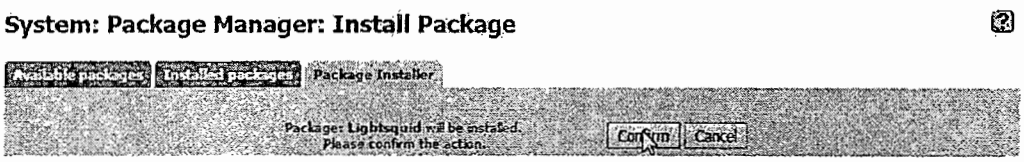
1) คลิก System | แพ็กเกจ

2) เข้าไปที่ Available แพ็กเกจ

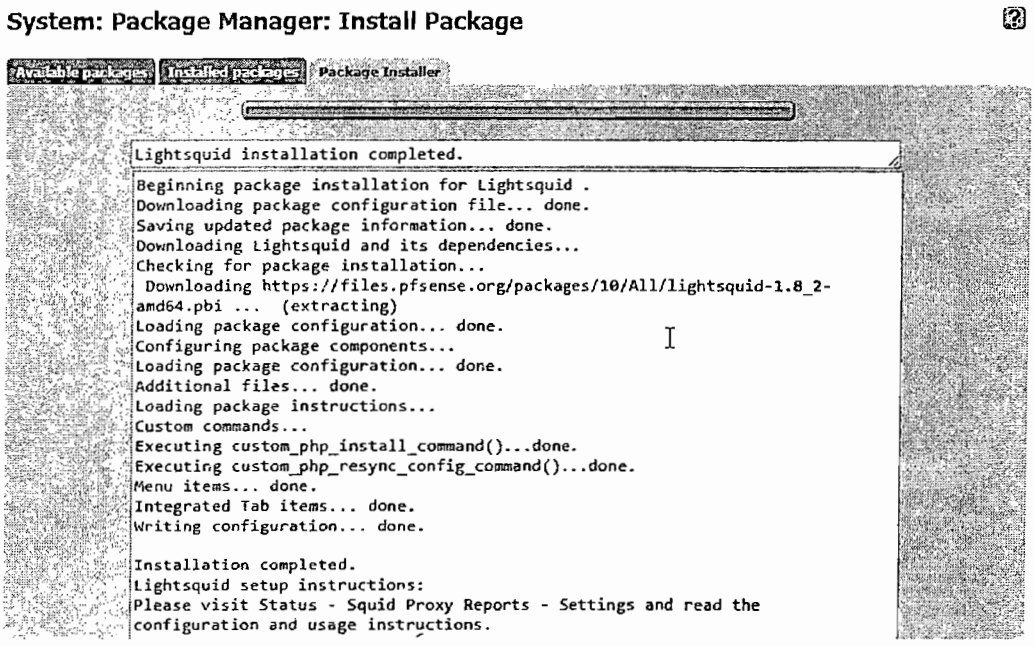
3) เลือกหาแพ็กเกจที่มีชื่อว่า Lightsquid แล้วก่อ คลิกที่เครื่องหมาย 



4) คลิกไปที่ Config



5) รอการดาวน์โหลด และติดตั้ง, ของ Lightsquid จนให้ติดตั้งเสร็จแล้วดั่งรูป



ก.4.4 ทำการตั้งค่า Lightsquid

1) คลิก Status | squid proxy Reports

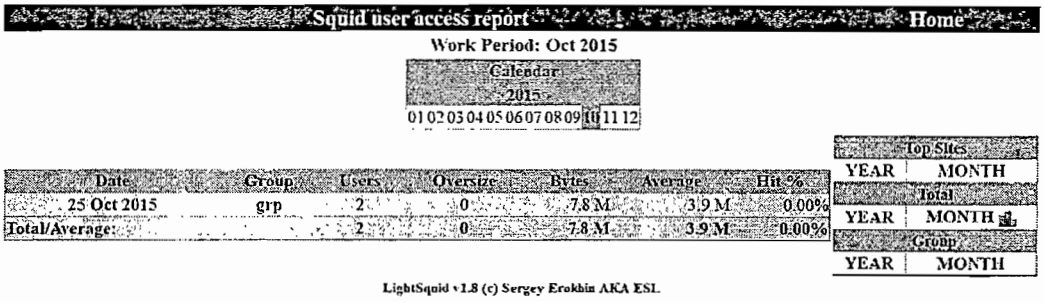
2) ทำการกำหนดที่ Settings

- Report Template: Novopf

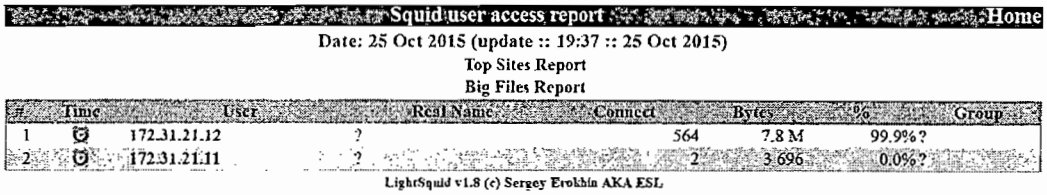
- Refresh Scheduler: 8h แล้วคิก Save

3) ทำการตรวจดูว่า Client เข้าไปเว็บอะไรบาง

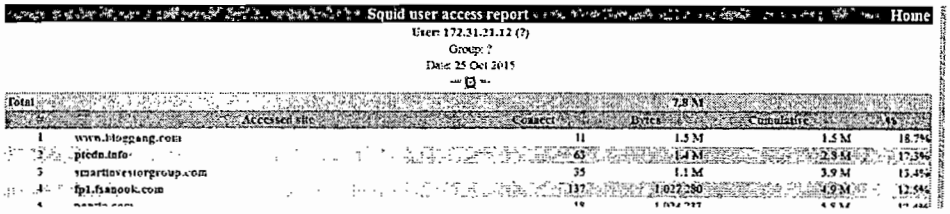
- เข้าไปที่ Lightsquid reports



- เข้าไปในวันที่ 25 oct 2015



- เข้าไปที่หมายเลขไอพี 172.31.21.12 เพื่อดูบันทึก URL



ก.5 การตั้งค่า Captive Portal มีสองขั้นตอนดังนี้

การกำหนดค่า Captive Portal และ การสร้าง User ให้สามารถเข้าใช้งานในระบบ Captive Portal

ก.5.1 การตั้งค่า Services Captive Portal

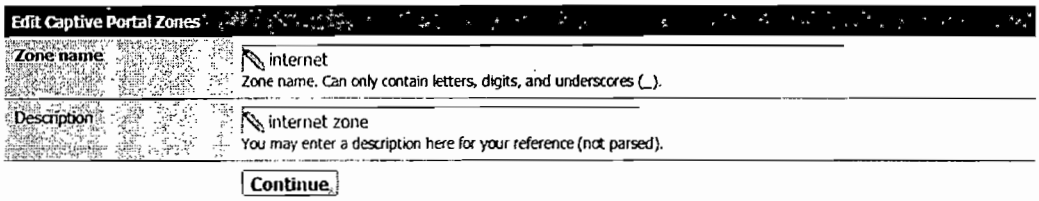
1) เข้าไปที่ Service | Captive Portal

2) ตั้งชื่อโซนของ Captive Portal (ตั้งค่าที่ Edit Captive Portal Zone name)

- Zone name: Lab

- Description: User Authentication แล้วคลิก Continue

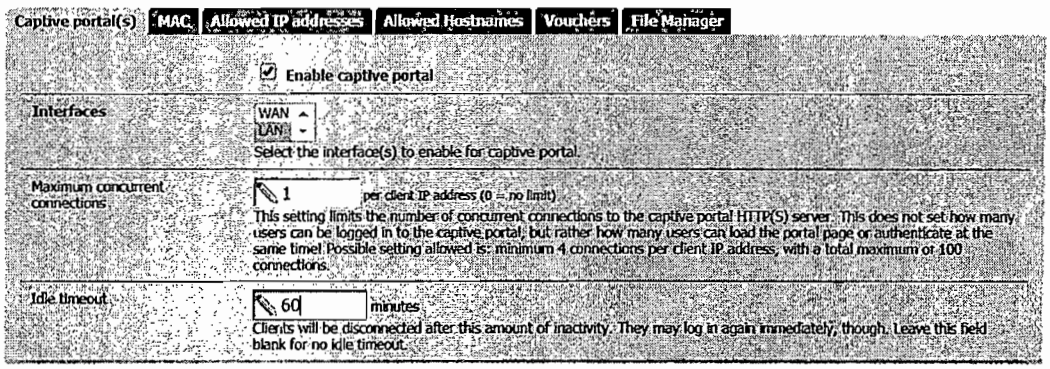
Services: Captive portal: Edit Zones



3) ที่แท็บ Captive Portal (s)

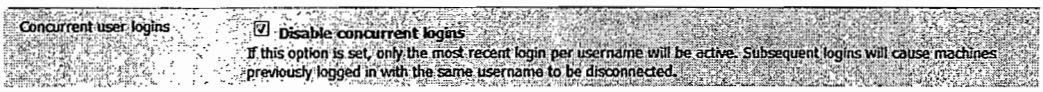
- ☑ Enable captive portal: เปิดใช้ captive portal
- Interface: เลือก Interface LAN
- Maximum concurrent connections: 1
- Idle timeout: 60 minutes กำหนดเวลาที่ใช้ในการ login

Services: Captive portal: Lab

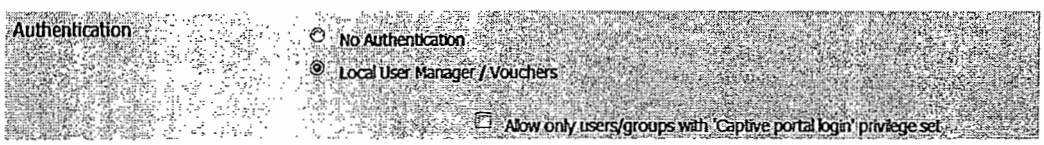


- After authentication Redirection URL: www.google.com

- Concurrent user logins: ☑ Disable concurrent logins กำหนดให้ client ใช้ได้หนึ่งเครื่องต่อหนึ่งผู้ใช้

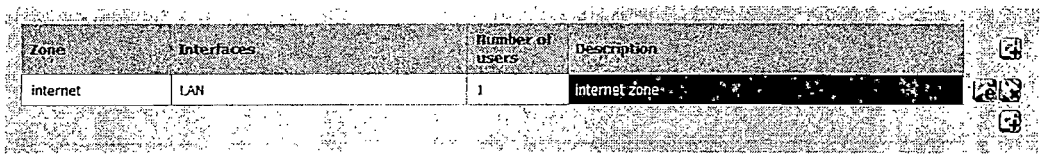


- Authentication: ⊙ Local User Manager แล้ว ก่อ Save



4) ผลของการค่า Captive Portal

Captive Portal: Zones



ก.5.2 การสร้าง User ให้สามารถเข้าใช้งานในระบบ Captive Portal

1) เข้าไปที่ System | User Manager

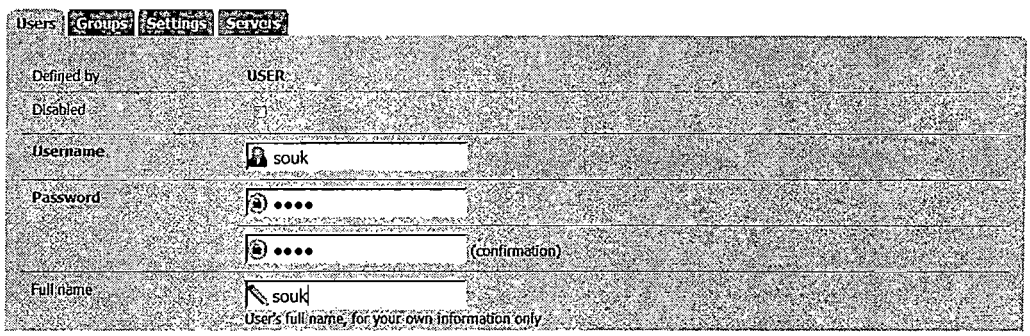
2) ตั้งค่าที่ User | เข้าไปที่ Add user 

- Username: souk
- Password: souk

: souk ใส่ Password ยืนยันอีกครั้ง

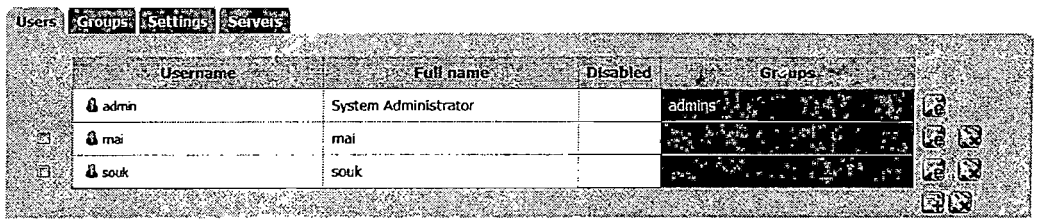
- Full name: souk แล้วคลิกSave

System: User Manager

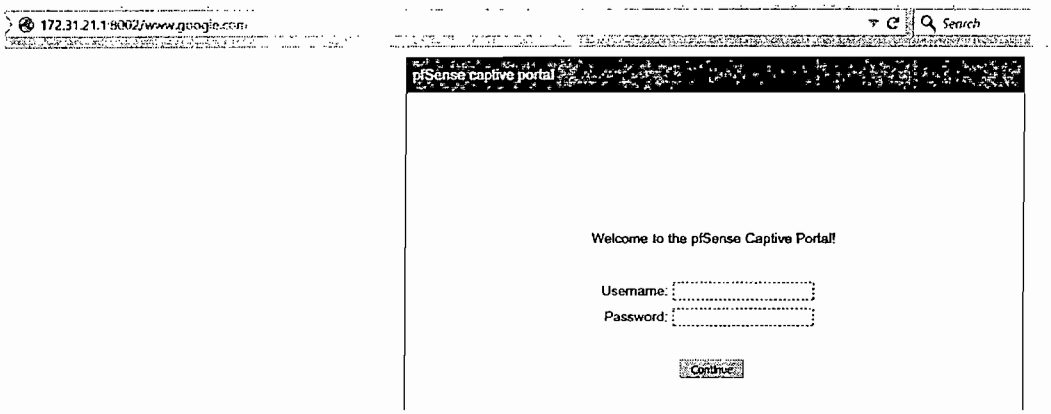


3) ผลของการสร้าง User

System: User Manager



ก.5.3 ผลการตรวจสอบ Captive Portal หลังจากผู้ใช้ต้องการเข้าเว็บ www.Google.com



ก.5.4 ถ้าไคลเอนต์ยืนยันตัวตนสำเร็จ ระบบจะบันทึกการเข้าถึง ดังภาพข้างล่าง

Captive Portal status

IP address	MAC address	Username	Session start
172.31.21.11	00:25:64:ad:68:3f	mai	03/30/2016 06:35:30

ก.6 การตั้งค่าเครื่องแม่ข่าย RADIUS

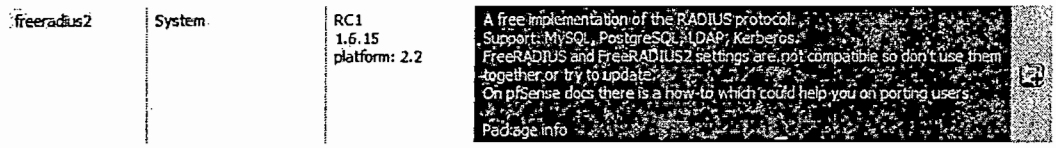
การกำหนดค่าเครื่องแม่ข่าย RADIUS ประกอบด้วยขั้นตอนการติดตั้งแพ็กเกจของ Free RADIUS2 ขั้นตอนการตั้งค่า Free RADIUS และ ขั้นตอนการทดสอบ Free RADIUS

ก.6.1 การติดตั้งแพ็กเกจ Free Radius2

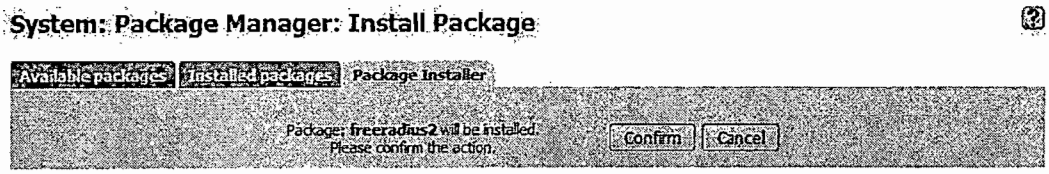
1) เข้าไปที่ System | Package

2) เข้าไปที่ Available Packages

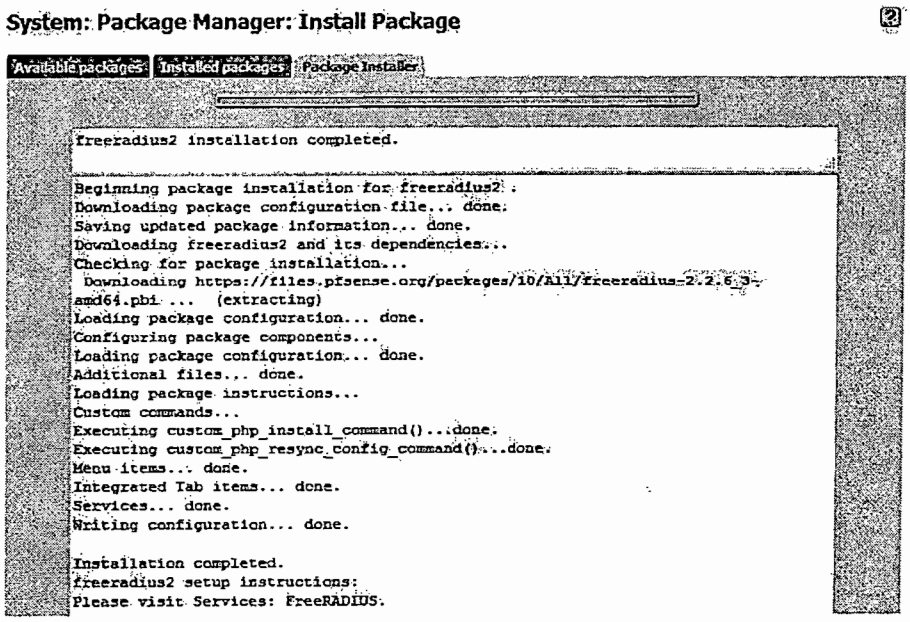
3) เข้าไปหาชื่อ Free RADIUS | แล้วคลิกที่ Add (Free RADIUS2) 



4) เข้าไปที่ confirm เพื่อติดตั้ง freeradius2

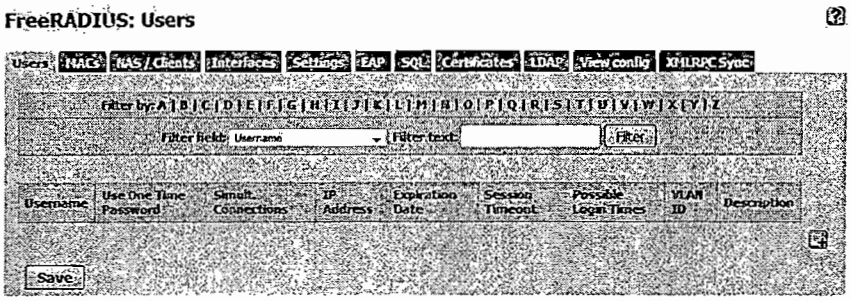


5) หลังจากติดตั้งเสร็จแล้วจะมีข้อความแสดงดังภาพด้านล่าง



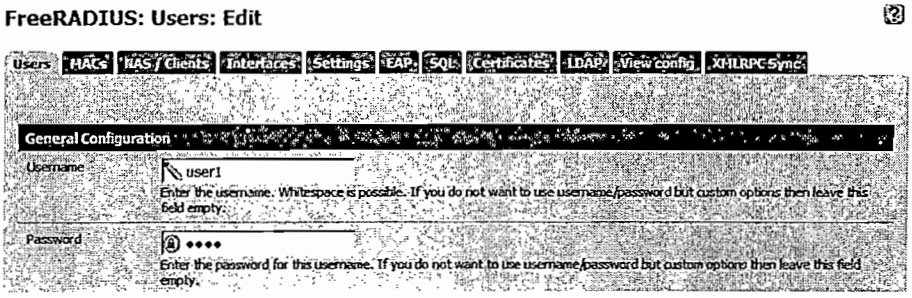
ก.6.2 การตั้งค่า Free RADIUS

1) เข้าไปที่ Service | Free RADIU | User | 

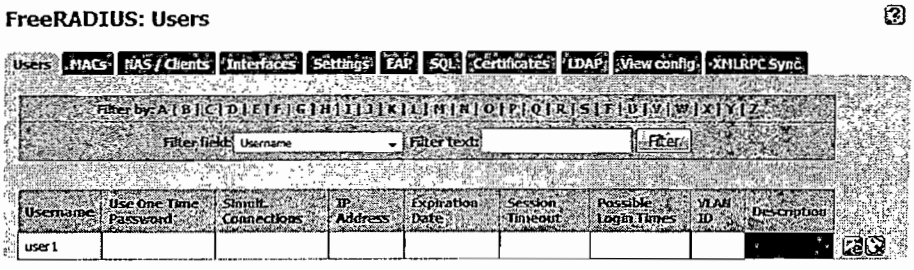


2) เข้าไปตั้งค่าชื่อ และ รหัสของผู้ใช้งานอยู่ที่ Users

- Username: user1
- Password: 1234 แล้วคลิก Save

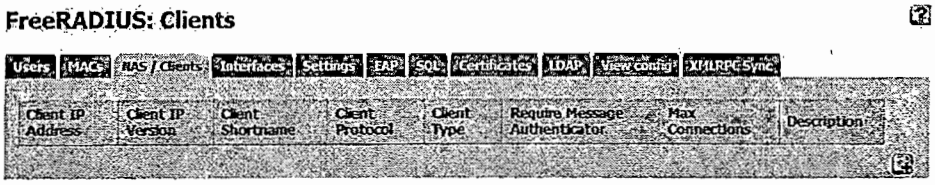


- ผลหรับที่ได้จากการตั้งค่าชื่อ และ รหัสของผู้ใช้งาน Free RADIU

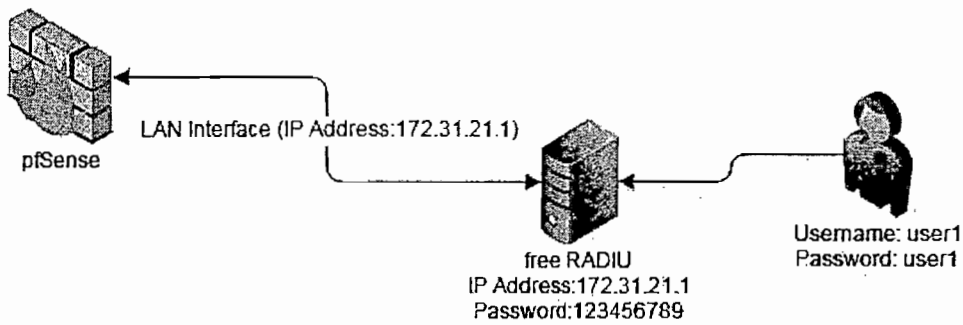


3) เข้าตั้งค่าที่ NAS/Clients

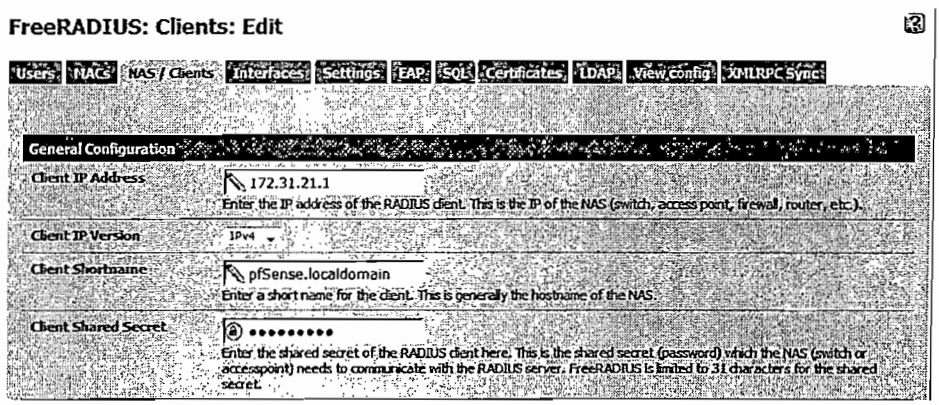
- เข้าไปที่ NAS/Clients | 



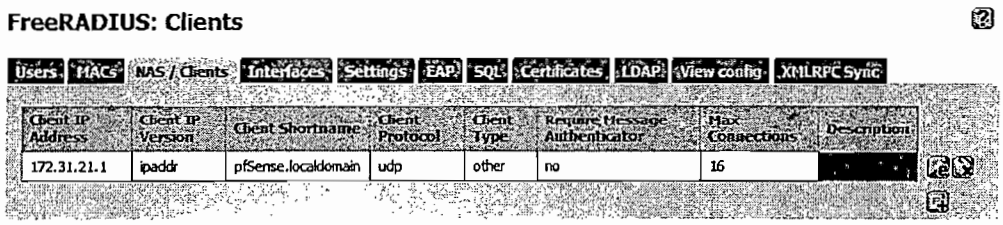
- Client IP Address: 172.31.21.1 (กำหนดหมายเลขไอพีของ RADIU)
- Client Shared Secret: 123456789 (ใส่รหัสของ RADIU)



- แล้วคลิก Save

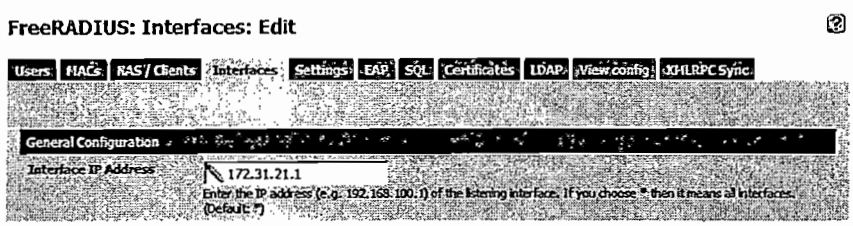


- ผลรับที่ได้จากการตั้งค่า NAS/Clients



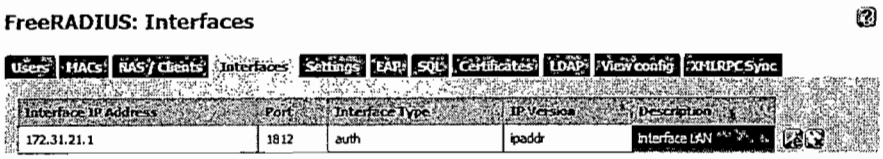
4) กำหนดค่า Interfaces

- Interface IP Address: 172.31.21.1 (กำหนด interface ที่เชื่อมต่อกับ RADIU)



- Description: Interface NAT (คำอธิบาย) แล้ว คลิก Save

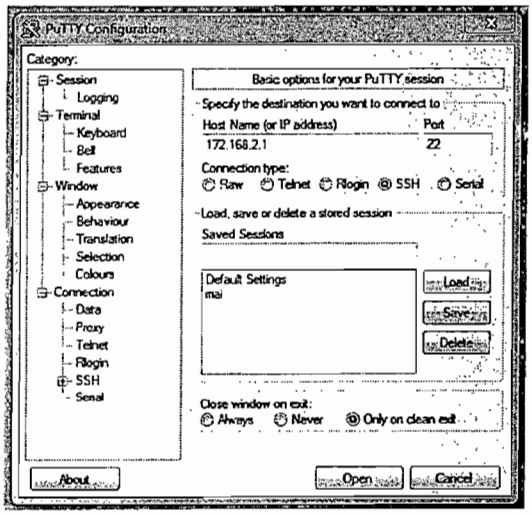
- ผลรับที่ได้จากการตั้งค่า Interfaces



ก.6.3 การทดสอบ Free RADIUS

1) เข้าไปที่หน้า command line ของ pfSense ช่องทาง SSH จากโปรแกรม Putty

- Host Name (or IP address): 172.31.21.1 (ใส่หมายเลขไอพีของ pfSense (Interface LAN))
- Port: 22 (ใส่พอร์ท)
- Connection type: ⦿ SSH (รูปแบบเป็น SSH) แล้ว คลิกใส่ Open



2) ใส่ชื่อ admin login: admin แล้ว กด Enter

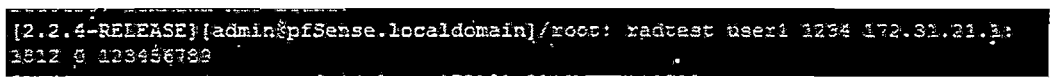
```
login as: admin
```

3) ใส่รหัสของ Admin: XXXXXXX

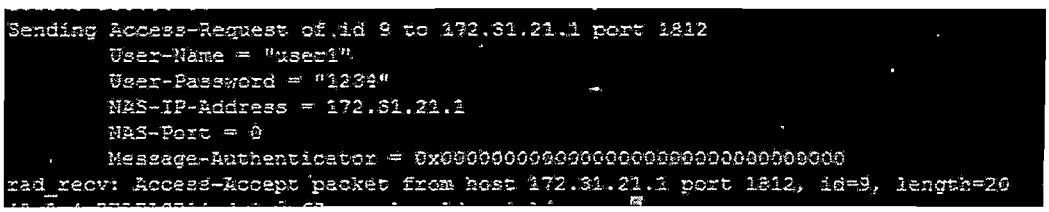
```
Using keyboard-interactive authentication.
Password for admin@pfsense.localdomain:
```

4) อยู่ในระบบ command line ของ pfSense แล้วเข้าไปที่ shell กด 8 แล้ว Enter

5) เขียนคำสั่งในการตรวจสอบ: radtest user1 1234 172.31.21.1:1812 0 1 123456789 แล้วกด Enter



6) จะปรากฏคำว่า Access-Accept ในบรรทัดสุดท้ายต่อหน้าคำ rad_recv: แสดงว่า user นี้สามารถ login เข้าถึงเครื่องแม่ข่าย Free RADIUS ได้



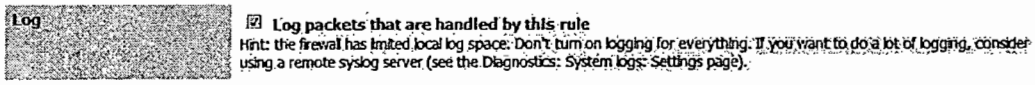
ก.7 ตั้งค่า Log Server

ขั้นตอนในการกำหนดค่าที่ System logs มีดังนี้

- การกำหนดค่าที่กฎไฟร์วอลล์เพื่อให้มีการเก็บ log
- การกำหนดค่าที่ System logs (pfSense) ให้ส่ง log ไปยังเครื่องแม่ข่ายเก็บ log เครื่องอื่น (Syslog Watcher)
- การดาวน์โหลด และ ติดตั้งโปรแกรม Syslog Watcher จากเว็บไซต์ http://syslogwatcher.soft32.com

ก.7.1 เนื่องจาก pfSense สามารถเก็บ log ได้หลายชนิด ซึ่งวิธีการกำหนดค่าให้เก็บ log แต่ละชนิดคล้ายกัน ผู้ทำงานนิพนธ์จึงเลือกแสดงขั้นตอนการกำหนดค่าที่ Interface LAN เพื่อให้เก็บ log ของกฎไฟร์วอลล์ เป็นตัวอย่าง

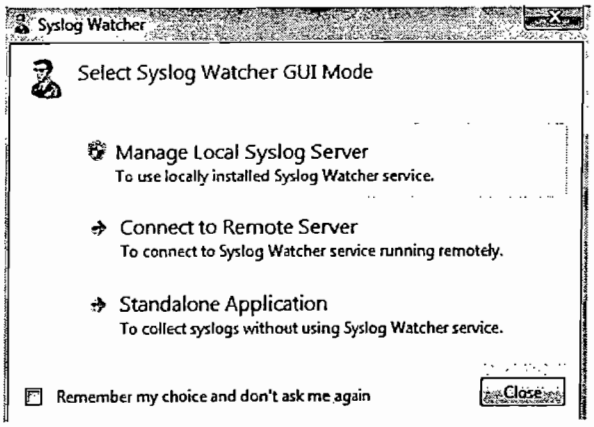
1) เข้าไปที่ Firewall | rule | LAN
2) กำหนดค่า log: ☑ Log packets that are handled by this rule



3) Save

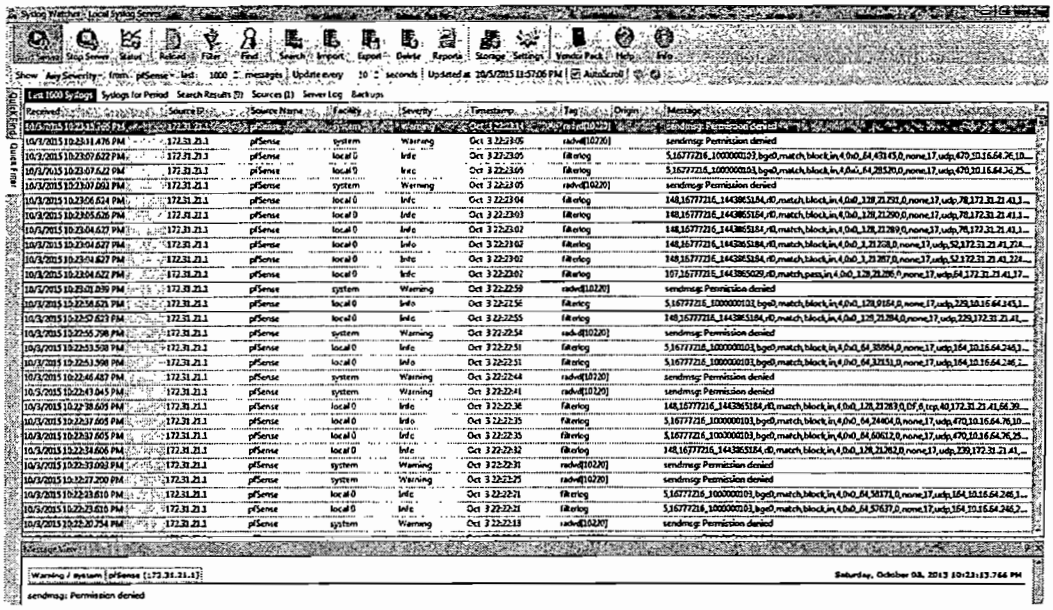
ก.7.2 การดาวน์โหลด และ ติดตั้งโปรแกรม Syslog Watcher

1) ดาวน์โหลด โปรแกรม Syslog Watcher จากเว็บไซต์ (http://syslog-watcher.soft32.com/free-download/) และ ติดตั้ง
2) เปิดโปรแกรม Syslog Watcher ที่ติดตั้งและเข้าไปที่ Manage Local Syslog Server



3) เข้าไปที่ Start Server

4) ผลของการการเก็บ log ของ System Watcher

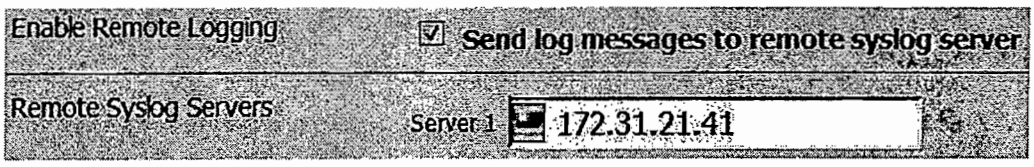


ก.7.3 กำหนดค่าให้ส่ง log ไปยัง log Server เครื่องอื่น (System Watcher)

1) เข้าไปที่ Status | system log

2) กำหนดค่าที่ Remote Logging Options

- Enable Remote Logging: ☑ Send log messages to remote Syslog Server
- Remote Syslog Servers Server1: 172.31.21.41 ละบุไอพีของ server ที่ติดตั้งโปรแกรม Syslog Watcher



- Remote Syslog Contents: ☑ Everything แล้วคลิก Save

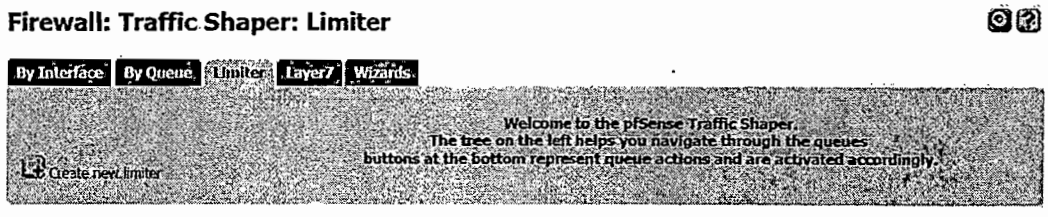
ก.8 การตั้งค่าจำกัดแบนด์วิดท์ Download และ Upload

pfSense ผู้ดูแลระบบสามารถกำหนด limit แบนด์วิดท์การอัพโหลดและดาวน์โหลด โดยสร้างกฎให้กับบางหมายเลขไอพี เช่น บอมให้อัพโหลด 30 Mbit/s และ ดาวน์โหลด 60 Mbit/s

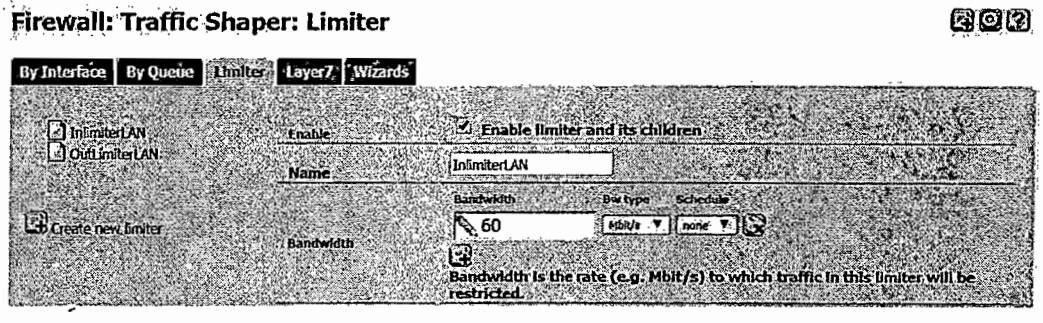
ก.8.1 การตั้งค่า limit การอัพโหลด และ ดาวน์โหลดใน pfSense

1) เข้าไปที่ Firewall | Traffic Shaper

2) เข้าไปที่ Limiter | Create new limiter (เพื่อกำหนดชื่อ และ ขนาดแบนด์วิดท์ของการอัพโหลด)



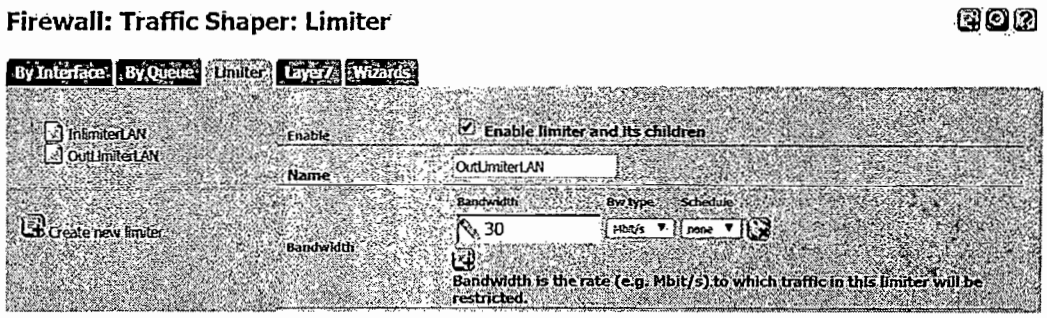
- Enable: ☑ Enable limiter and its children (อนุญาตให้เปิด limiter ของลูกเครือข่าย)
- Name: LnlimiterLAN (ใส่ชื่อ)
- กำหนดแบนด์วิดท์ โดยคลิกที่  แล้ว ใส่ Bandwidth: 60 Mbit/s
- Save



3). เข้าไปที่ Create new limiter (เพื่อกำหนดชื่อ และ ขกาดแบนด์วิดท์ของการดาวน์โหลด)

- Enable: ☑ Enable limiter and its children (อนุญาตให้เปิด limiter ของลูกเครือข่าย)
- Name: OutlimiterLAN (ใส่ชื่อ)
- กำหนดแบนด์วิดท์ โดยคลิกที่  แล้ว ใส่ Bandwidth: 30 Mbit/s

- Save

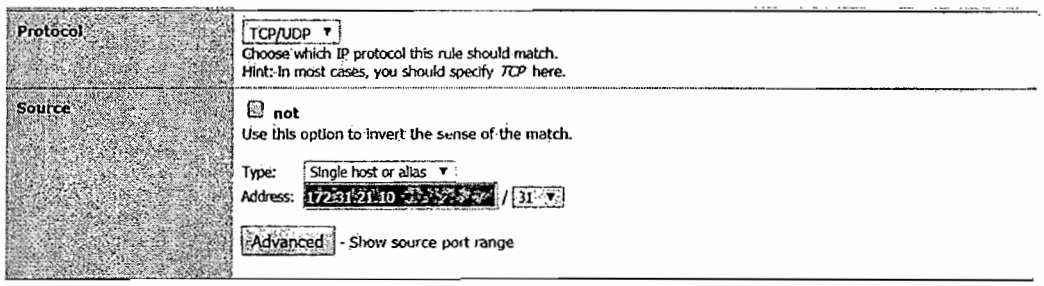


ก.8.2 สร้างกฎจำกัดบางหมายเลขไอพีสามารถอัพโหลดที่ความเร็ว 60 Mbit/s และดาวน์โหลด 30 Mbit/s

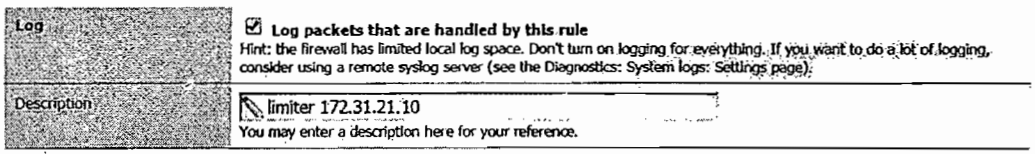
1) เข้าไปที่ Firewall | Rule | LAN | Add rule ()

3) กำหนดค่าที่ Edit Firewall rule

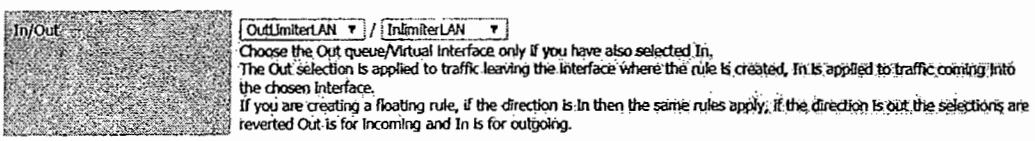
- Protocol: TCP/UDP
- Source: Type: Single host or alias และ Address: 172.31.21.10



- Log: ☑ Log packets that are handled by this rule
- Description: Limiter 172.31.21.10



- In/out: OutlimiterLAN to InlimiterLAN แล้วคลิก Save



3) ผลการทดสอบแบนด์วิดท์ในการอัพโหลด และ ดาวน์โหลด ของเครื่องที่มีหมายเลขไอพี 172.31.21.10 (ทดสอบโดยใช้ www.speedtest.net)

ก.9 การตั้งการค่าบล็อก YouTube และ Facebook ใน pfSense

การบล็อก YouTube และ Facebook ใน pfSense โดยมีการจำลอง DNS Resolver เพื่อนำไปสร้างกฎปฏิเสรกฎไฟร์วอลล์ไม่อนุญาตให้มีการเข้าถึงตัว DNS Resolver

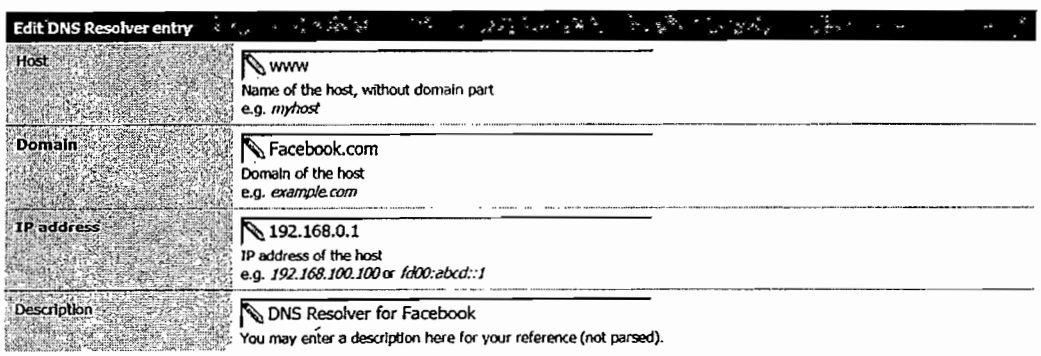
ก.9.1 การกำหนดค่า DNS Resolver ของ YouTube และ Facebook

1) เข้าไปที่ Services | DNS resolver

2) เข้าไปกำหนดค่าที่ Host Overrides | Add () เพื่อสร้าง DNS resolver ของ Facebook

- Host: www
- Domain: facebook.com
- IP Address: 192.168.0.1
- Description: DNS Resolver for Facebook แล้วคลิก Save

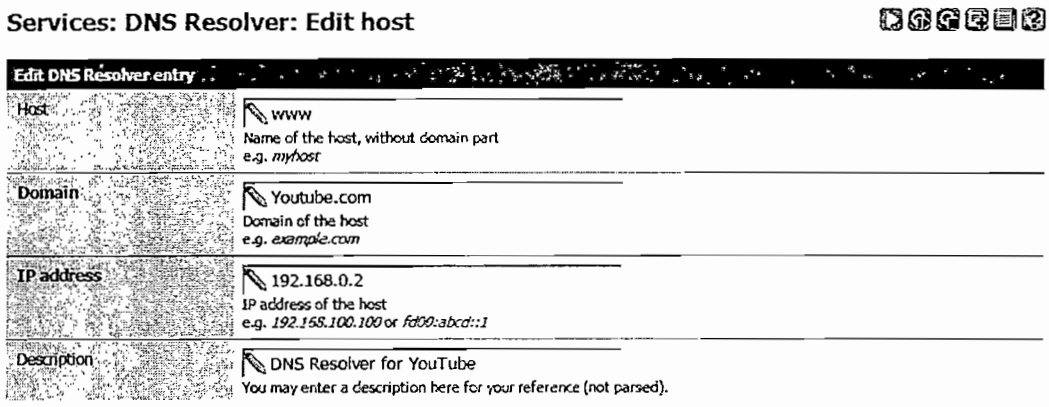
Services: DNS Resolver: Edit host



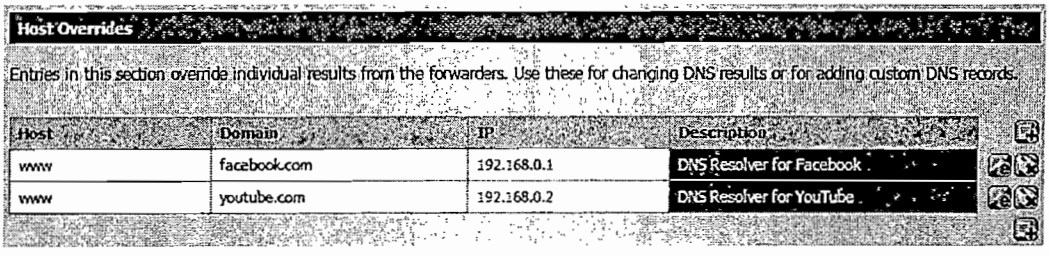
3) เข้าไปกำหนดค่าที่ Host Overrides | Add () เพื่อสร้าง DNS resolver ของ YouTube

- Host: www
- Domain: youtube.com
- IP Address: 192.168.0.2

- Description: DNS Resolver for YouTube แล้วคลิก Save



4) ผลของกำหนดค่าหมายเลขไอพีของ YouTube และ Facebook ใน DNS Resolver



ก.9.2 สร้างกฎไฟร์วอลล์ไม่อนุญาตให้มีการเข้าถึง Facebook และ YouTube

1) เข้าไปที่ firewall | rule | LAN

2) เข้าไปที่ Add rule New ( ) (เพื่อสร้างกฎปฏิเสรกฎไฟร์วอลล์ไม่อนุญาตให้มีการเข้าถึงตัว DNS Resolver ของ Facebook)

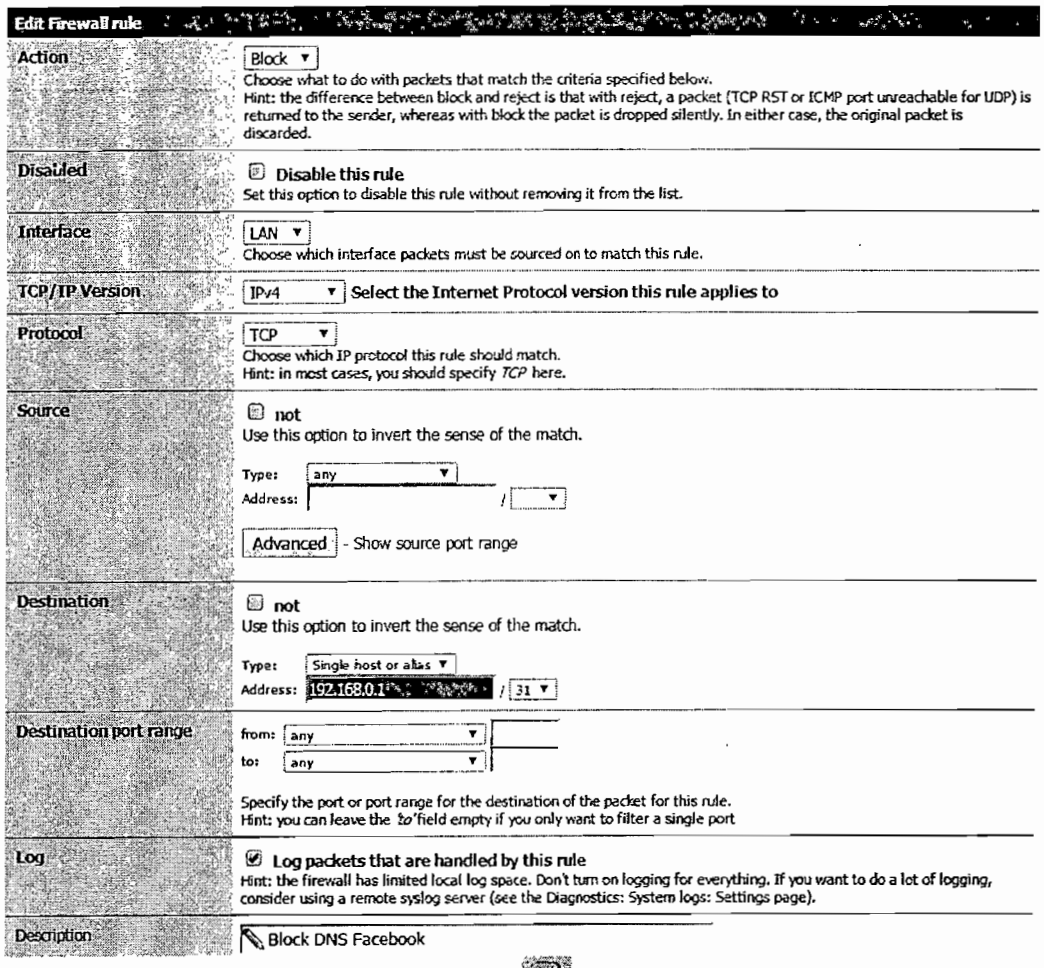
- Action: block
- Interface: LAN
- Protocol: any
- Source: Type: LAN net (รูปแบบต้นทาง)
- Destination: Type: Singe host or (รูปแบบปรายทาง)

Alias Address: 192.168.0.1 (ใส่หมายเลขไอพีของ Facebook ใน DNS Resolver)

- Destination port range: from: nay และ to: any
- Log: ☑ Log packets that are handled by this Rule

- Description: คำอธิบาย block Facebook interface LAN
- แล้วคลิก Save

Firewall: Rules: Edit



4) เข้าไปที่ Add rule New () (เพื่อสร้างกฎไฟร์วอลล์ไม่อนุญาตให้มีการเข้าถึง YouTube)

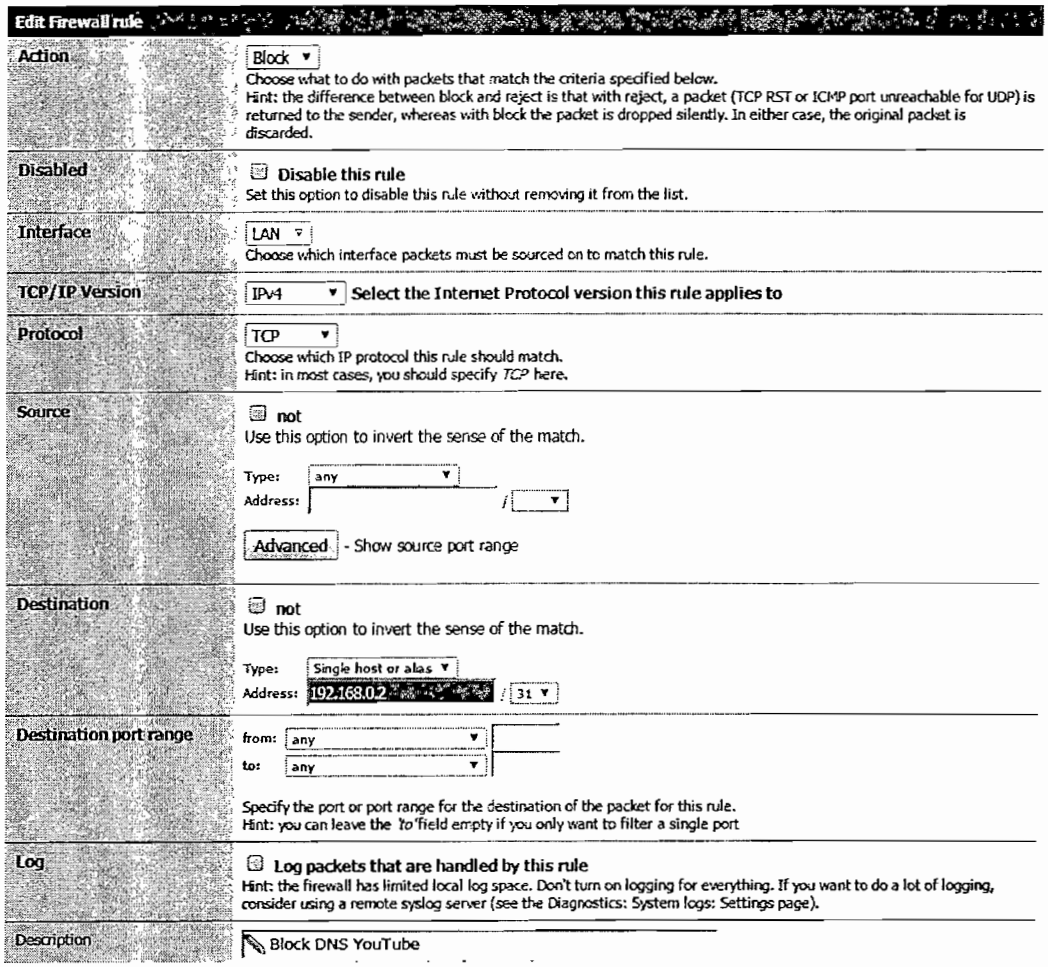
- Action: block
- Interface: LAN
- Protocol: any
- Source: Type: LAN net (รูปแบบต้นทาง)
- Destination: Type: Singe host or (รูปแบบปรายทาง)

Alias Address: 192.168.0.2 (ใส่หมายเลขไอพีของ YouTube ใน DNS Resolver)

- Destination port range: from: nay และ to: any

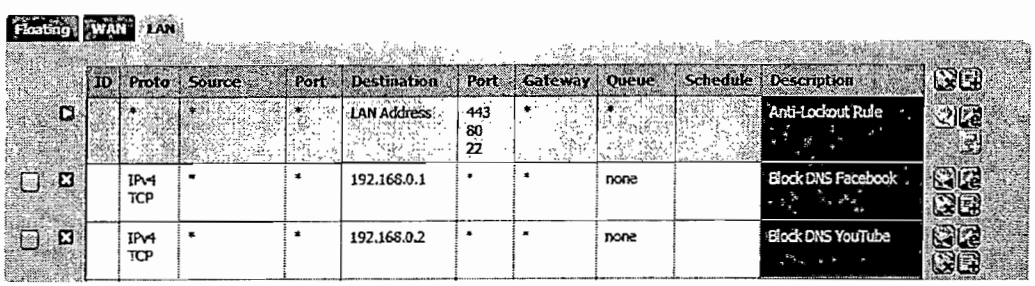
- Log: ☑ Log packets that are handled by this Rule
- Description: คำอธิบาย block Facebook interface LAN
- แล้วคลิก Save

Firewall: Rules: Edit

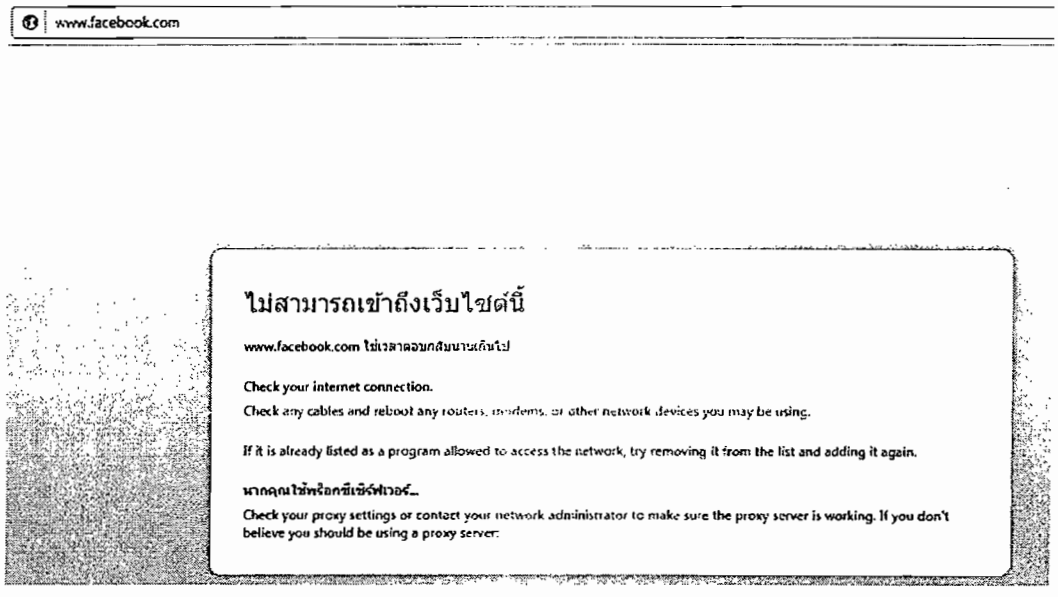


5) ผลของการสร้างกฎไฟร์วอลล์ไม่อนุญาตให้มีการเข้าถึงตัว Facebook และ YouTube ได้

Firewall: Rules



6) ผู้ทำงานนิพนธ์การทดสอบการเข้าถึง Facebook ได้ผลดังภาพด้านล่าง

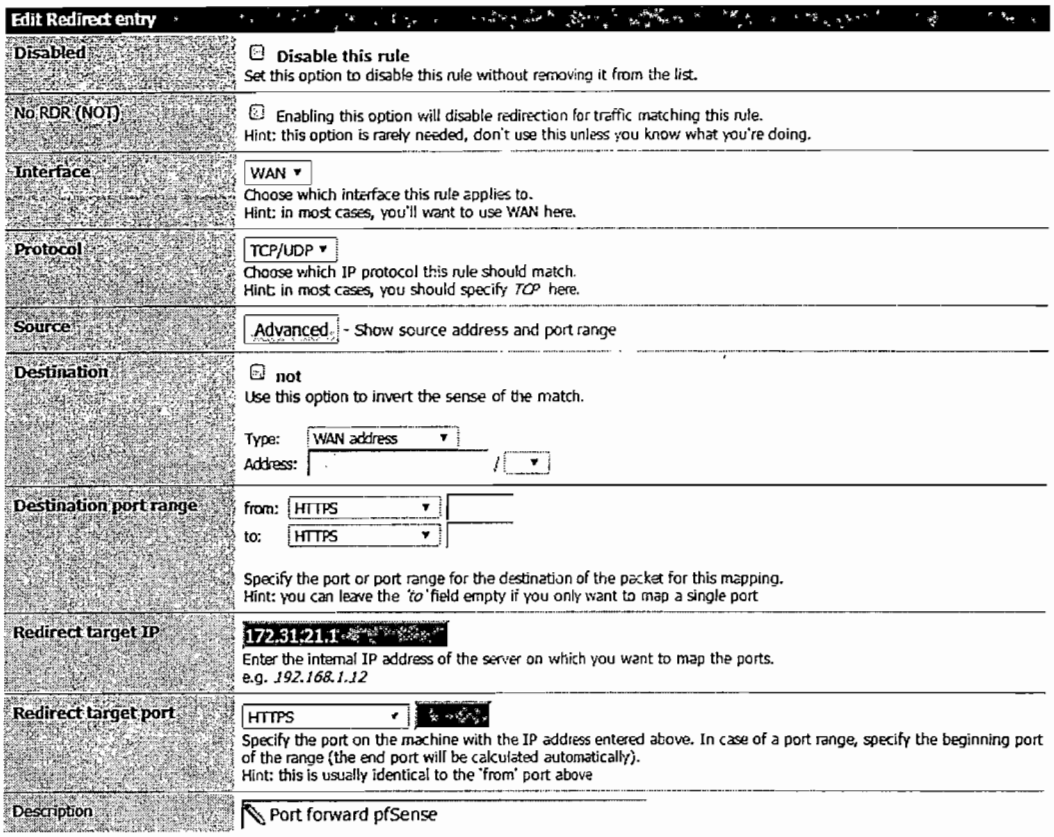


ก.10 การตั้งค่า NAT และ Port Forwarding เพื่อส่งข้อมูลไปยังเครื่องแม่ข่าย pfSense และ web

ขั้นตอนในการกำหนดค่า NAT ให้แปลงหมายเลขไอพีที่เป็น Interface WAN ไปเป็นหมายเลขไอพีของ Interface LAN (pfSense และ web server) และ การตั้งค่า Port Forward ไปที่ port 443 (pfSense) และ Port 80 (Web Server) มีรายละเอียดดังนี้

1) เข้าไปที่ไฟร์วอลล์ Firewall | NAT
2) เข้าไปที่ Port Forward | New rule ()
3) กำหนดค่าที่ Edit Redirect entry (เพื่อ Forward ไปที่ port 443 (pfSense))
   - Interface: WAN (เลือกอินเตอร์เฟส)
   - Protocol: TCP/UDP (โพรโทคอลเป็น TCP/UDP)
   - Destination: Type: WAN address (รูปแบบ)
   - Destination Port range: เลือก From และ To เป็น HTTPS
   - Redirect target IP:172.31.21.1 (ใส่หมายเลขไอพีปลายทาง)
   - Redirect target Port: HTTPS (ใส่พอร์ทปลายทาง)
   - Description: Port Forward pfSense (คำอธิบายสิ่งที่เราจะทำ)

- แล้วคลิก Save

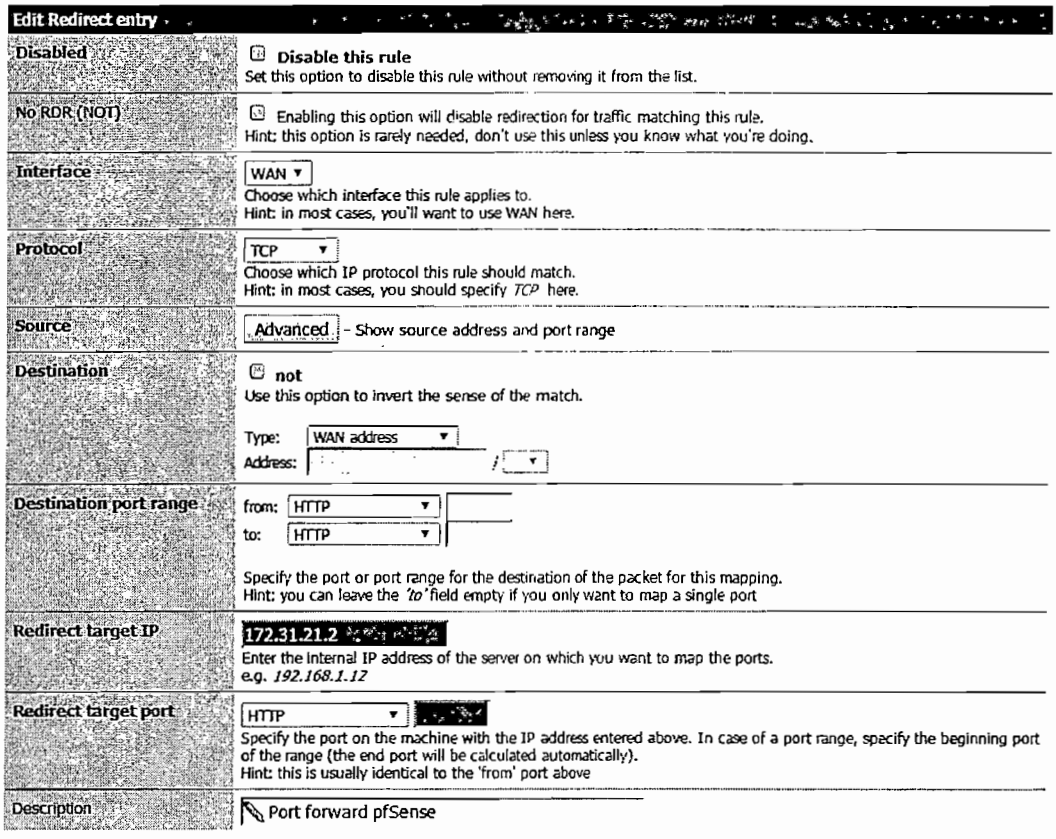


4) เข้าไปที่ New rule ( )

5) กำหนดค่าที่ Edit Redirect entry (เพื่อ Forward ไปที่ port 80 (Web Server))

- Interface: WAN (เลือกอินเตอร์เฟส)
- Protocol: TCP/UDP (โพรโทคอลเป็น TCP/UDP)
- Destination:Type: WAN address (รูปแบบ)
- Destination Port range: เลือก From และ To เป็น HTTP
- Redirect target IP:172.31.21.2 (ใส่หมายเลขไอพีปลายทาง)
- Redirect target Port: HTTP (ใส่พอร์ทปลายทาง)
- Description: Port Forward Web Server (คำอธิบายสิ่งที่เราจะทำ)

- Save



6) ผลของการกำหนด Port Forward ไปที่ port 443 (pfSense) และ Port 80 (Web Server) แสดงดังภาพด้านล่าง

Firewall: NAT: Port Forward

Port Forward | 1:1 | Outbound | NPt

	IF	Proto	Src. addr	Src. ports	Dest. addr	Dest. ports	NAT IP	NAT Ports	Description
	WAN	TCP/UDP	*	*	WAN address	443 (HTTPS)	172.31.21.1	443 (HTTPS)	Port forward pfSense
	WAN	TCP	*	*	WAN address	80 (HTTP)	172.31.21.2	80 (HTTP)	Port forward Web Server

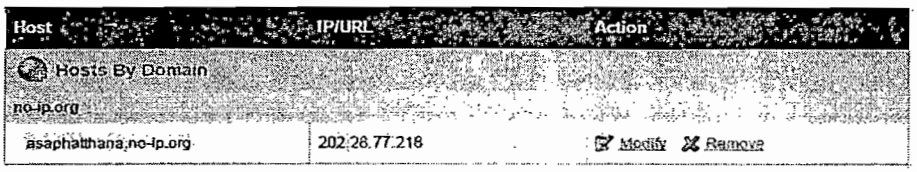
ก.11 การตั้งค่า Dynamic DNS

ในขั้นตอนการกำหนดค่าบริการ Dynamic DNS ใน pfSense ผู้ตั้งค่าต้องสมัคร Dynamic DNS และกำหนดค่า Dynamic DNS ใน pfSense ดังนี้

ก.11.1 ขั้นตอนในการเข้าไปสมัคร Domain Name System ของผู้ให้บริการ NOIP

1) เข้าไปที่เว็บ https://www.noip.com

2) ผลของการสมัคร Hosts By Domain (asaphatthana.no-ip.org) แสดงดังภาพด้านล่าง



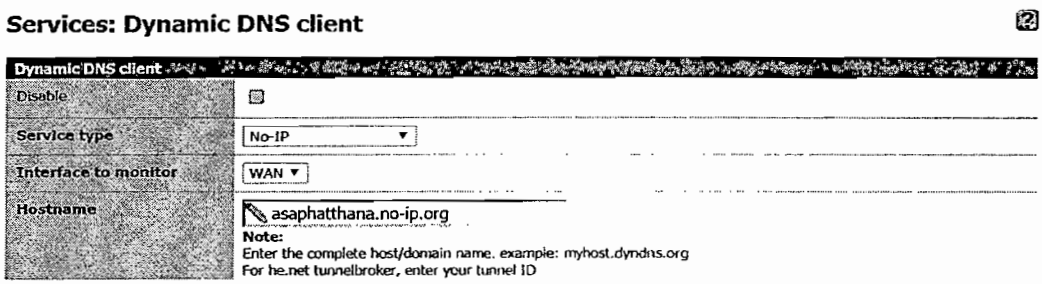
ก.11.2 การกำหนดค่า Dynamic DNS ใน pfSense

1) เข้าไปที่ Services | Dynamic DNS

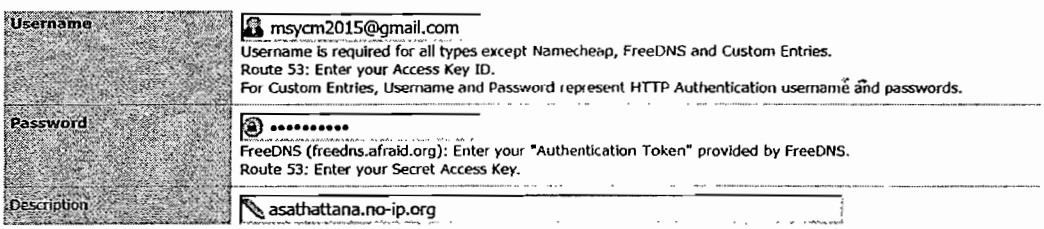
2) เข้าไปที่ DynDns | Add ()

3) การกำหนดค่าที่ Services: Dynamic DNS client

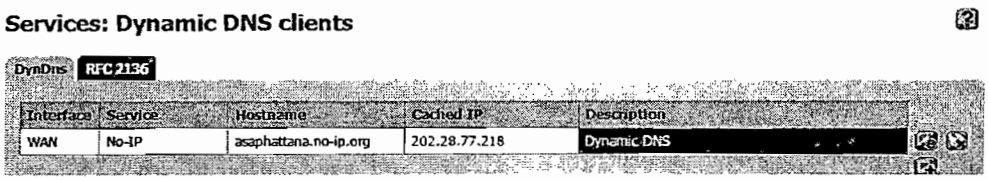
- Service type: No-IP (เลือก DNS ที่ให้ประเภทบริการ)
- Interface to monitor: WAN (เลือกอินเตอร์เฟส)
- Hostname: asaphatthana.no-ip.org (ใส่ชื่อโฮสต์ที่สมัคร)



- Username: msycm2015@gmail.com (ใส่ E-mail)
- Password: xxxxxxx (ใส่รหัส)
- Description: asathattana.no-ip.org (ใส่คำอธิบาย) แล้วคิก Save



4) ผลการตั้งค่า Dynamic DNS (Domain Name System) ใน pfSense

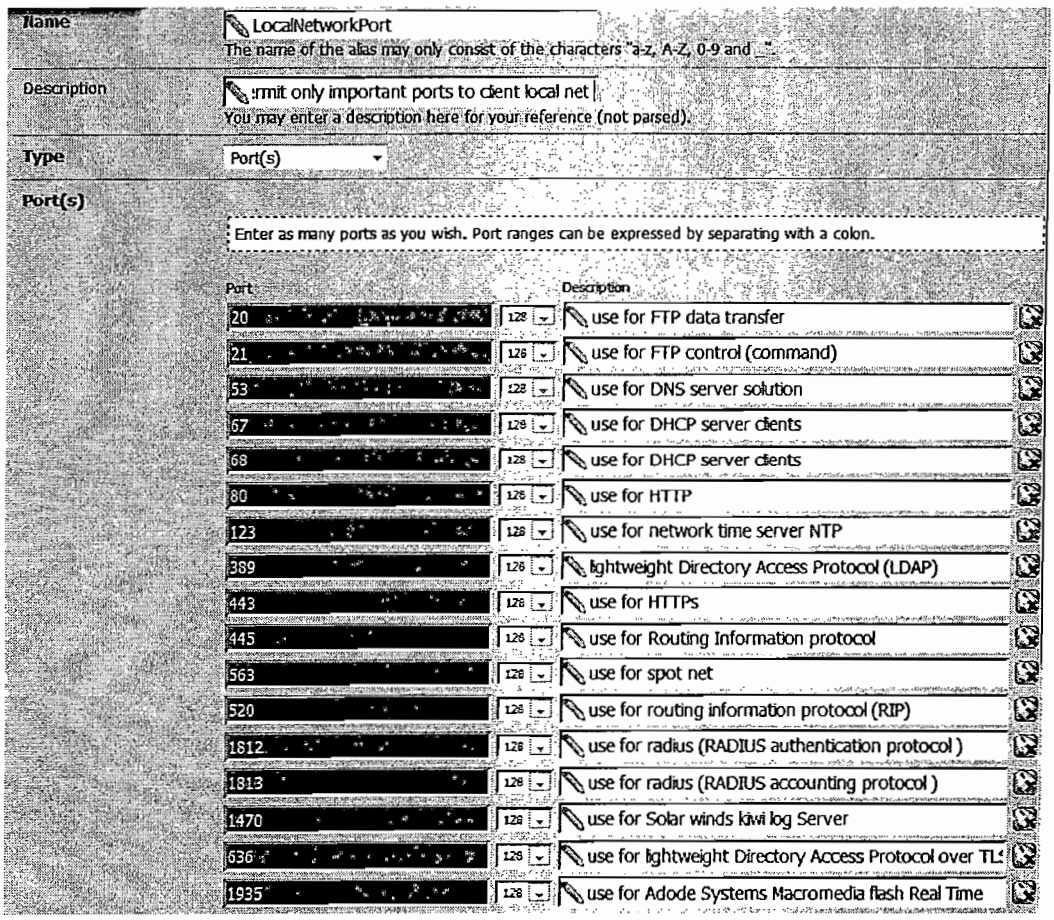


ก.12 การสร้างกฎไฟร์วอลล์

การสร้างกฎไฟร์วอลล์สำหรับการอนุญาตใช้ Port ที่จำเป็น และ สร้างกฎไฟร์วอลล์ไม่อนุญาตให้มีการเข้าถึง Port โดยมีการสร้างกลุ่ม Alias ของ Port ที่ต้องการใช้ เช่น LocalNetworkPort, RomoteAccessPorts, EmailPorts เพื่อนำเอาไปสร้างกฎไฟร์วอลล์สำหรับการอนุญาตการเข้าถึง Port ต่าง ๆ และ ไม่อนุญาตให้มีการเข้าถึง Port ที่ไม่ได้ใช้

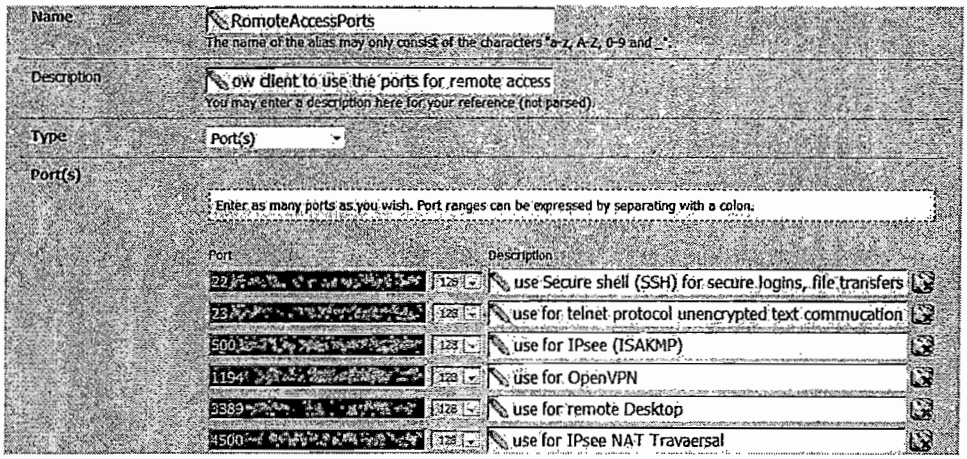
ก.12.1 การสร้างกลุ่ม Alias port

1) เข้าไปที่ Firewall | Alias | port
2) เข้าไปที่ Add New Alias (⊞) (เพื่อสร้าง Alias port ของ LocalNetworkPort)
   - Name: LocalNetworkPort
   - Description: Permit only important ports to client local net
   - Type: Port(S)
   - Port (S): ที่ต้องการอนุญาตดังภาพด้านล่าง แล้วคลิก Save



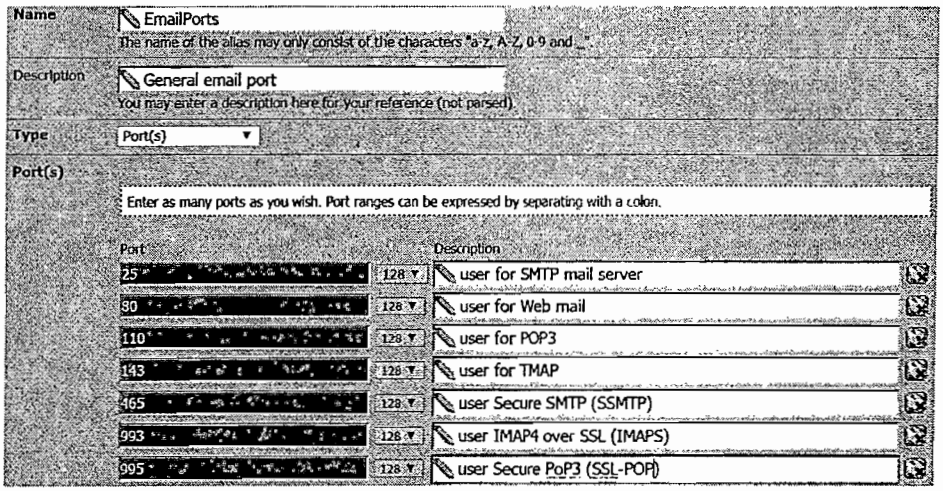
3) เข้าไปที่ Add New Alias (+) (เพื่อสร้าง Alias port ของ RomoteAccessPorts)

- Name: RomoteAccessPorts
- Description: Allow client to use the port for remote access
- Type: Port(S)
- Port (S): ที่ต้องการอนุญาตดังภาพด้านล่าง แล้วคลิก Save



4) เข้าไปที่ Add New Alias (+) (เพื่อสร้าง Alias port ของ EmailPorts)

- Name: EmailPorts
- Description: General email port
- Type: Port(S)
- Port (S): ที่ต้องการอนุญาตดังภาพด้านล่าง แล้วคลิก Save



5) ผลของการสร้างกลุ่ม Alias port ของ LocalNetworkPort, RomoteAccessPorts, EmailPorts

Firewall: Aliases

IP Ports URLs All

Name	Values	Description
EmailPorts	25, 80, 110, 143, 465, 993, 995	General email port
LocalNetworkPort	20, 21, 67, 68, 80, 123, 389, 443, 445, 563...	Permit only important ports to client local net
RomoteAccessPorts	22, 23, 1194, 1389, 4500	Allow client to use the port for remote access

ก.12.2 การสร้างกฎไฟร์วอลล์อนุญาตการเข้าถึง Port ต่าง ๆ

1) เข้าไปที่ Firewall | rule | LAN
2) เข้าไปที่ Add New rule ( ) (เพื่อสร้างกฎไฟร์วอลล์สำหรับการอนุญาตการเข้าถึง Port ของ LocalNetworkPort)
   - Action: Pass
   - Interface: LAN

Firewall: Rules: Edit

Edit Firewall rule

Action	Pass Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.
Disabled	Disable this rule Set this option to disable this rule without removing it from the list.
Interface	LAN Choose which interface packets must be sourced on to match this rule.

   - Protocol: TCP/UDP
   - Source: Type: LAN net

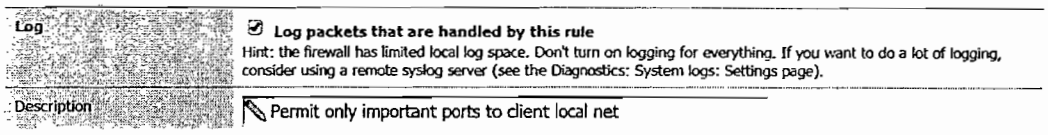
Protocol	TCP/UDP Choose which IP protocol this rule should match. Hint: in most cases, you should specify *TCP* here.
Source	not Use this option to invert the sense of the match. Type: LAN net

   - Destination port range: from: (other); LocalNetworkPorAlias และ to: (other); LocalNetworkPorAlia

Destination port range	from: (other) LocalNetv to: (other) LocalNetv Specify the port or port range for the destination of the packet for this rule. Hint: you can leave the *to* field empty if you only want to filter a single port

   - Log: ☑ Log packets that are handled by this rule

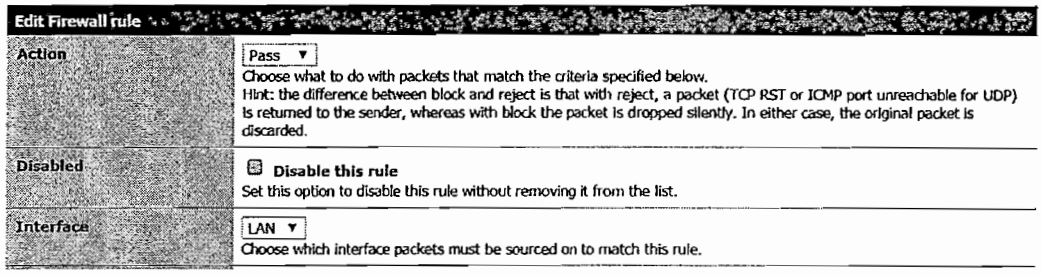
- Description: Permit only important ports ..... แล้วคลิก Save



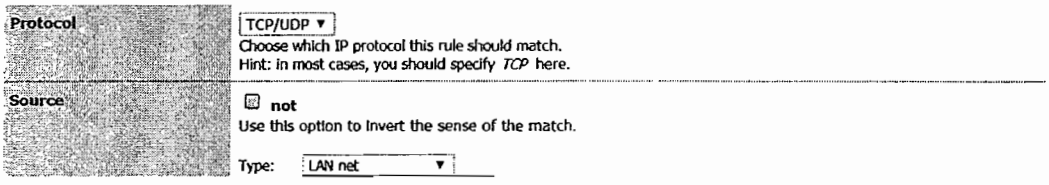
3) เข้าไปที่ Add New rule () (เพื่อสร้างกฎไฟร์วอลล์สำหรับการอนุญาตการเข้าถึง Port ของ RomoteAccessPorts)

- Action: Pass
- Interface: LAN

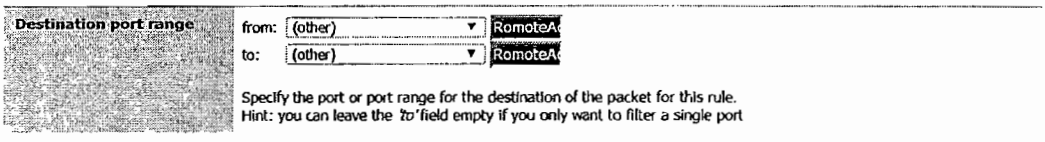
Firewall: Rules: Edit



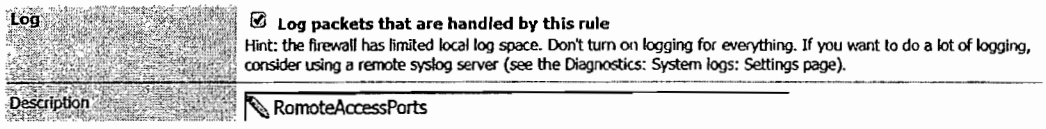
- Protocol: TCP/UDP
- Source: Type: LAN net



- Destination port range: from: (other); RomoteAccessPorts และ to: (other); RomoteAccessPorts



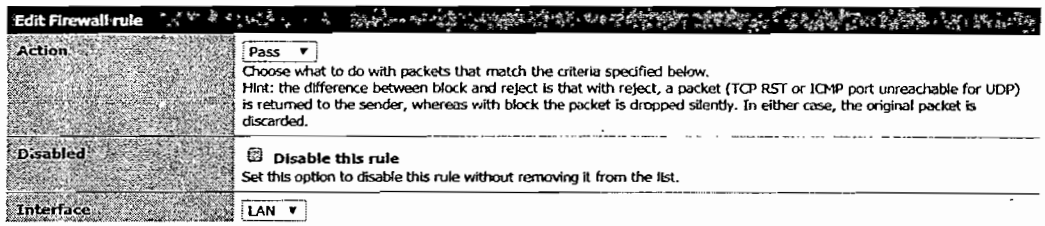
- Log: ☑ Log packets that are handled by this rule
- Description: RomoteAccessPorts แล้วคลิก Save



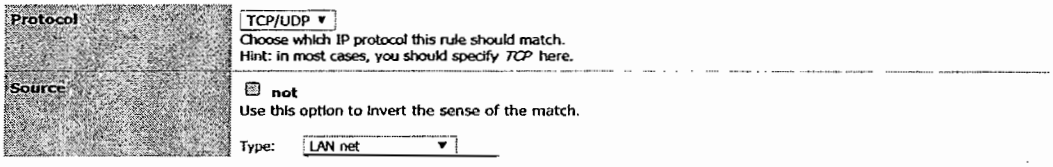
4) เข้าไปที่ Add New rule () (เพื่อสร้างกฎไฟร์วอลล์สำหรับการอนุญาตการเข้าถึง Port ของ EmailPorts)

- Action: Pass
- Interface: LAN

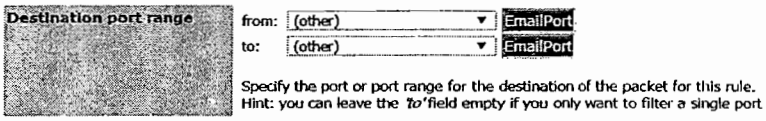
Firewall: Rules: Edit



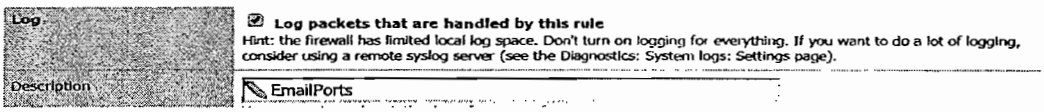
- Protocol: TCP/UDP
- Source: Type: LAN net



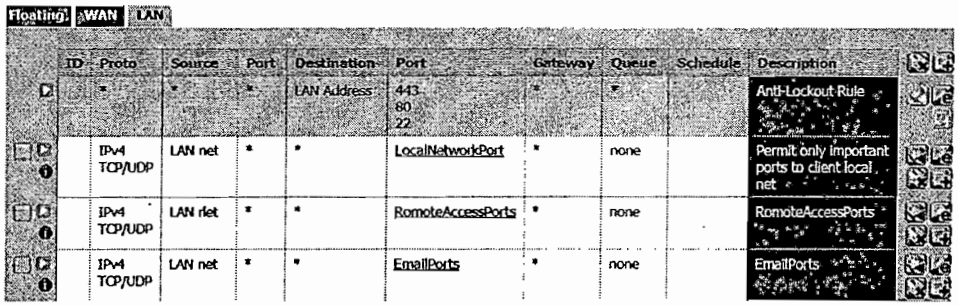
- Destination port range: from: (other); EmailPorts และ to: (other); EmailPorts



- Log: ☑ Log packets that are handled by this rule
- Description: EmailPorts แล้วคลิก Save



5) หลังการสร้างกฎไฟร์วอลล์สำหรับการอนุญาตการเข้าถึง Port ต่าง ๆ ได้ผลลัพธ์ ดังภาพด้านล่าง

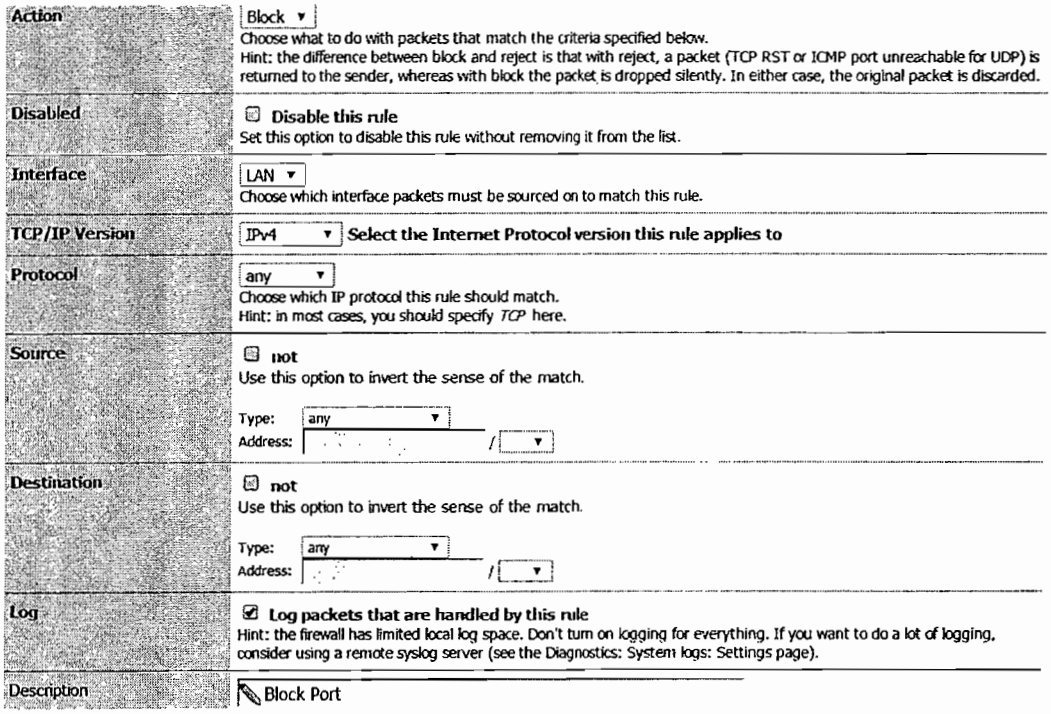


ก.12.3 การสร้างกฎไฟร์วอลล์ไม่อนุญาตให้มีการเข้าถึง Port

1) เข้าไปที่ Firewall | rule | LAN

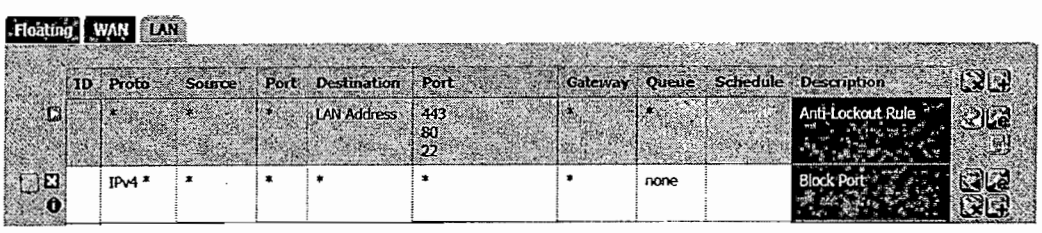
2) เข้าไปที่ Add New rule ()

- Action: block
- Interface: LAN
- Protocol: any
- Source: Type: LAN net
- Destination: type: any
- Log: ☑ Log packets that are handled by this rule
- Description: block port แล้วคลิก Save



3) ผลของการสร้างกฎไฟร์วอลล์ไม่อนุญาตให้มีการเข้าถึง Port

Firewall: Rules

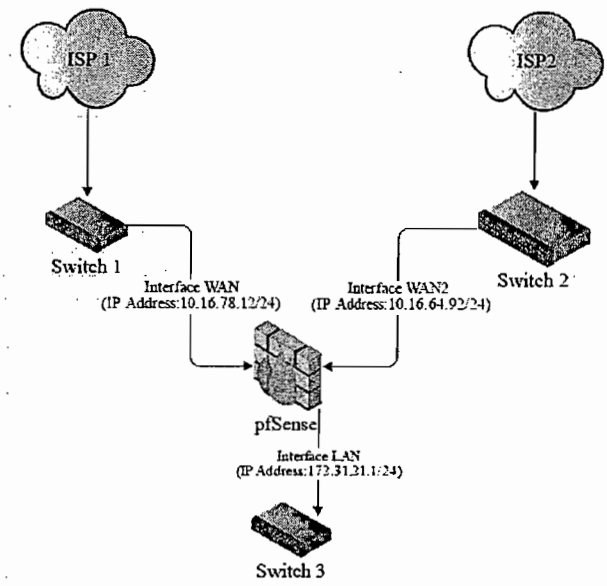


ก.13 การตั้งค่า Multi-WAN Load Balancing

ขั้นตอนการกำหนดค่า Multi-WAN Load มีดังนี้

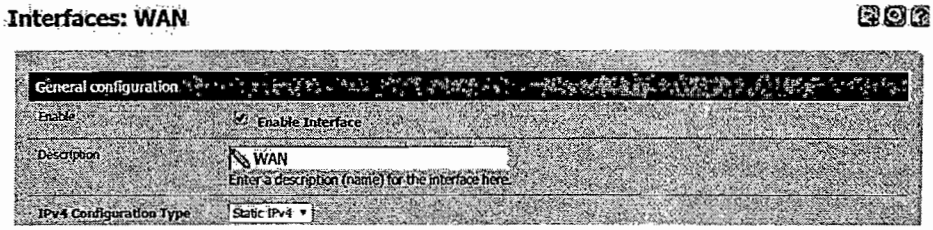
- การออกแบบแผนภาพ(Diagram) ของ Multi-WAN Load Balancing
- ตั้งค่าหมายเลขไอพีของ interface WAN เป็น Static
- ตั้งค่าหมายเลขไอพีของ interface OPT1 เป็น Static
- สร้าง Group สำหรับ Load balancing
- ใส่ Gateway ของ WAN และ WAN2
- ดูสถานะของ Gateway ทั้งสองว่า online หรือไม่

ก.13.1 การออกแบบแผนภาพ (Diagram) ของ Multi-WAN load Balancing



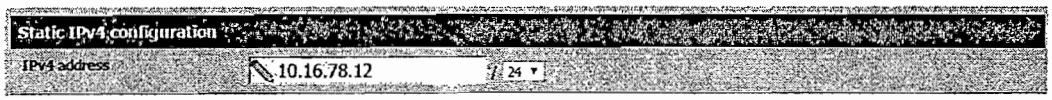
ก.13.2 การกำหนดค่าหมายเลขไอพีของ Interface WAN เป็นรูปแบบ Static

1) เข้าไปที่ Interfaces | WAN
2) กำหนดค่า General configuration
   - Enable: ☑ Enable Interface (เปิดใช้ interfaces WAN)
   - IPv4 Configuration Type: Static IPv4 (กำหนดเป็น Static IPv4)

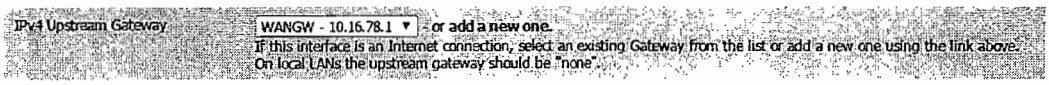


3) เข้าไปกำหนด Static IPv4 configuration

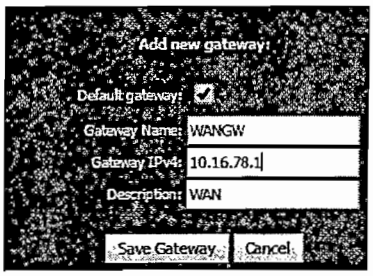
- IPv4 address: 10.16.78.12/24 (ใส่หมายเลขไอพี Interfaces WAN)



- คลิกเข้าไปที่ Add a new one เพื่อสร้าง Gateway

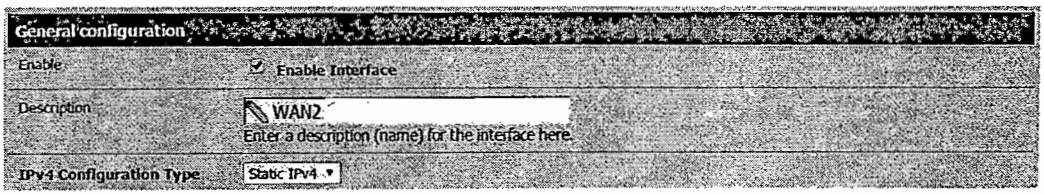


- คลิกเข้าไปที่ Gateway IPv4: 10.16.78.1
- Description: WAN (คำอธิบายสิ่งที่เราจะทำ)
- Save Gateway แล้วคลิก Save



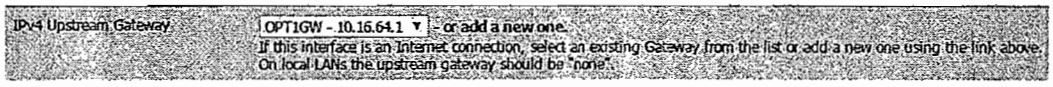
ก.13.3 การกำหนดค่าหมายเลขไอพีของ Interface WAN2 เป็นรูปแบบ Static

1) เข้าไปที่ Interfaces | WAN
2) กำหนดค่า General configuration
   - Enable: ☑ Enable Interface (เปิดใช้ interface WAN2)
   - Description: WAN2 (เปลี่ยน OPT1 เป็น WAN 2)
   - IPv4 Configuration Type: Static IPv4 (กำหนดเป็น Static IPv4)

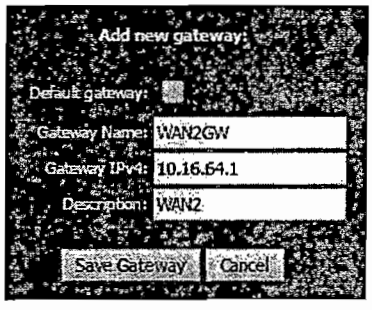


3) เข้าไปกำหนด Static IPv4 configuration
   - IPv4 address: 10.16.64.92/24 (ใส่หมายเลขไอพี Interfaces WAN2)

- คลิกเข้าไปที่ Add a new one เพื่อสร้าง Gateway ใหม่



- ใส่ Gateway IPv4: 10.16.64.1
- Description: WAN2 (คำอธิบายสิ่งที่เราจะทำ)
- Save Gateway แล้วคลิก Save

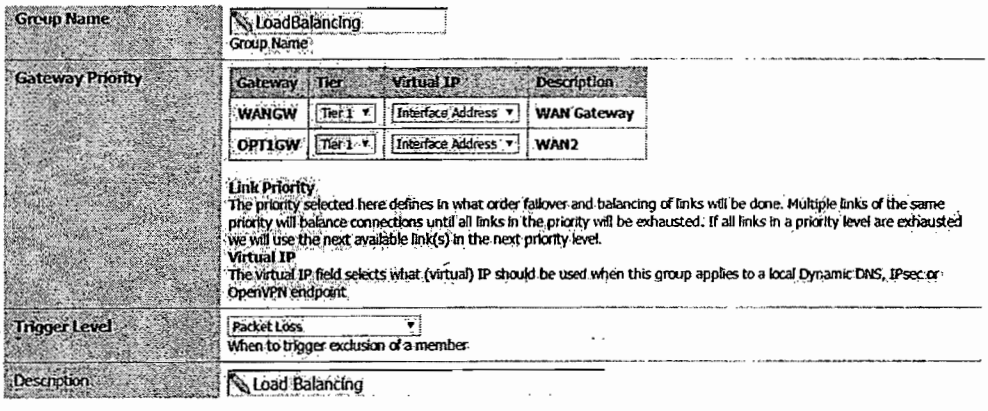


ก.13.4 สร้าง Group สำหรับ Load balancing

1) เข้าไปที่ System | Routing | Group |

2) เข้าไปกำหนดค่าที่ Edit gateway group entry

- Group Name: LoadBalancing (ใส่ชื่อ Group)
- Gateway Priority: WANGW เป็น **Tier 1** และ OPT1GW เป็น **Tier 1**
- Trigger Level: Packet Loss
- Description: Load Balancing แล้วคลิก Save

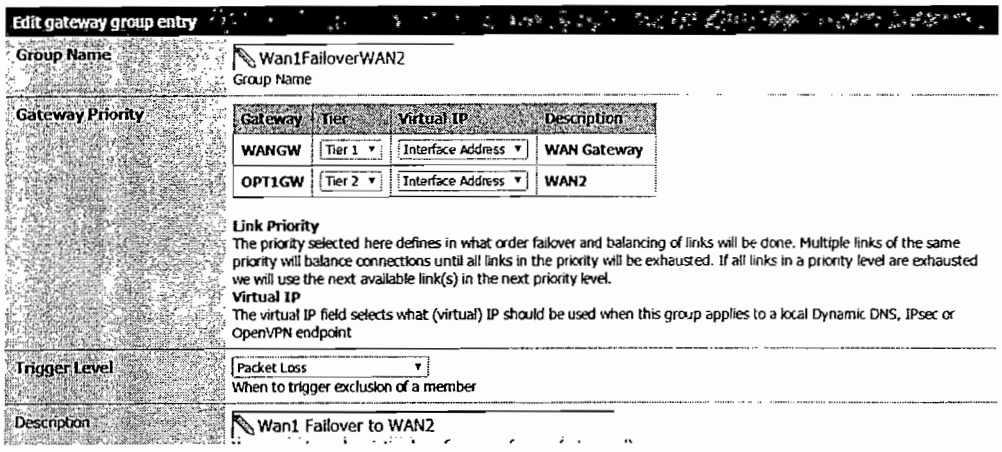


3) เข้าไปกำหนดค่าที่ Edit gateway group entry

- Group Name: Wan1FailoverWAN2 (ใส่ชื่อ Group)
- Gateway Priority: WANGW เป็น **Tier 1** และ OPT1GW เป็น **Tier 2**

- Trigger Level: Packet Loss
- Description: Wan1Failover to WAN2 (ใส่คำอธิบาย) แล้วคลิก Save

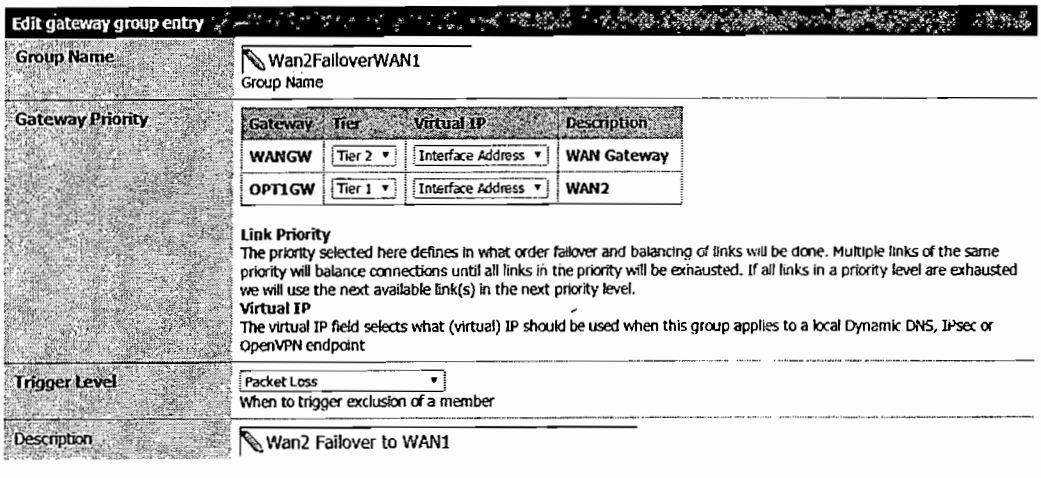
System: Gateways: Edit gateway group



4) เข้าไปกำหนดค่าที่ Edit gateway group entry

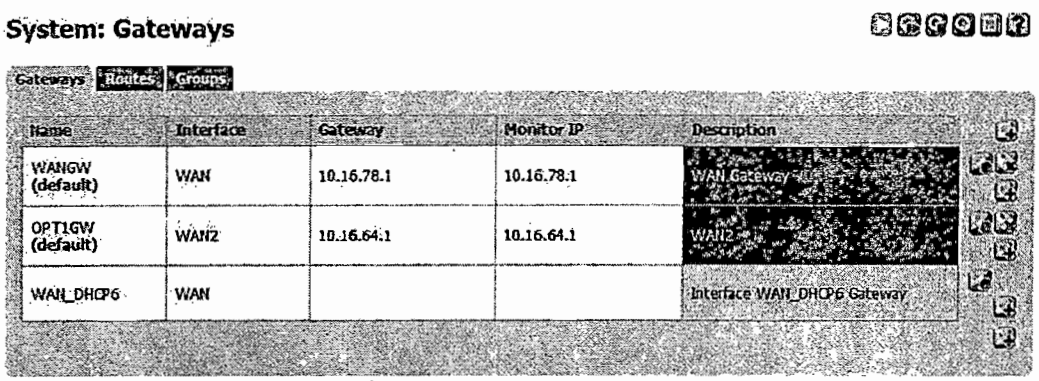
- Group Name: Wan2FailoverWAN1 (ใส่ชื่อ Group)
- Gateway Priority: WANGW เป็น Tier 2 และ OPT1GW เป็น Tier 1
- Trigger Level: Packet Loss
- Description: Wan2Failover to WAN1 (ใส่คำอธิบาย) แล้วคลิก Save

System: Gateways: Edit gateway group



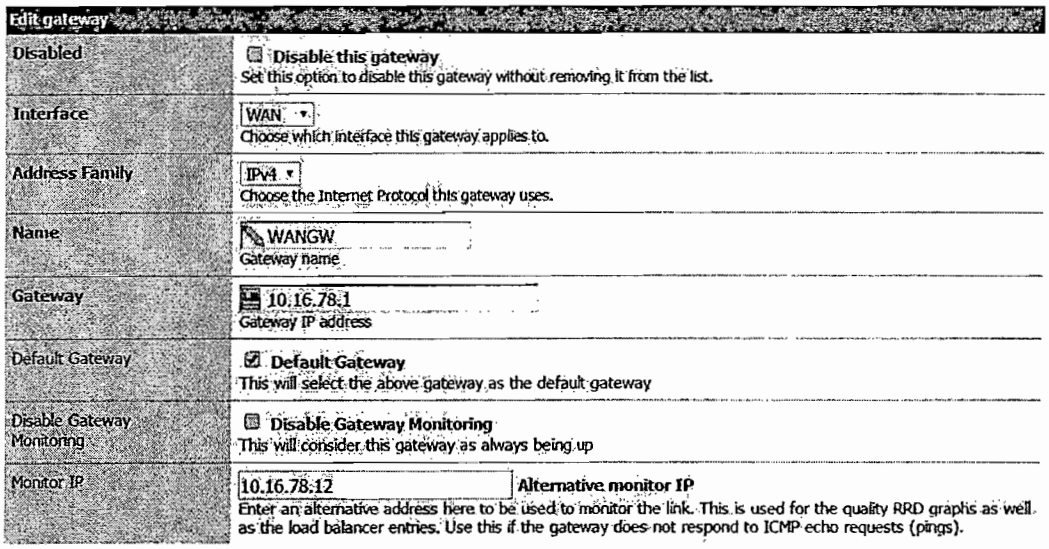
ก.13.5 ใส่หมายเขไอพีของ Gateway ของ WAN และ WAN2

1) เข้าไปที่ System | Routing | Gateway | (Edit Interface WAN)

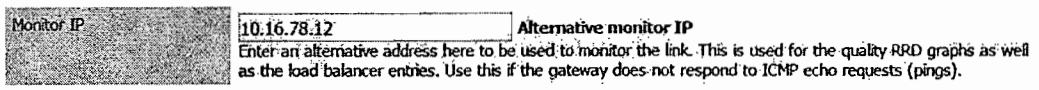


2) กำหนดค่าที่ Edit Gateway

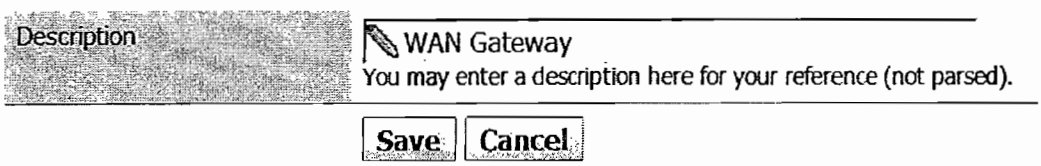
- Interface: WAN เลือกเป็น WAN
- Gateway: 10.16.78.1



- Monitor IP: 10.16.78.12 (ใส่หมายเลขไอพีของ Interface WAN)

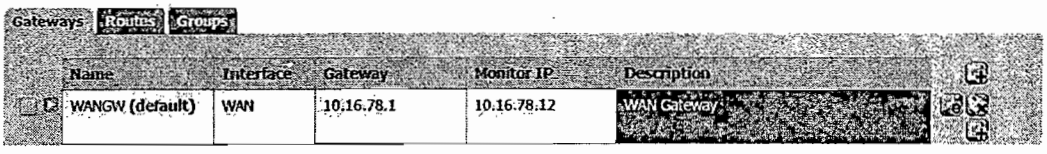


- Description: WAN Gateway (ใส่คำอธิบาย) แล้วคลิก Save



- ผลการตั้งค่า Gateway ของ WAN ได้ข้อมูลดังภาพด้านล่าง

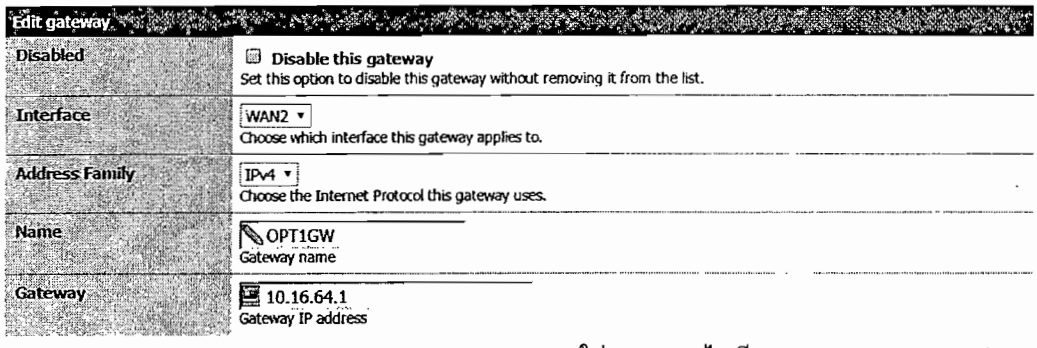
System: Gateways



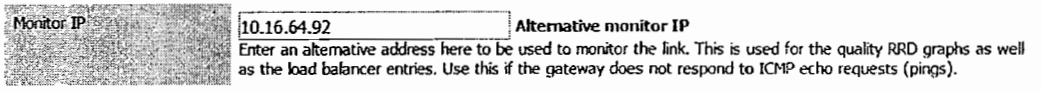
3) กำหนดค่าที่ Edit Gateway

- Interface: WAN เลือกเป็น WAN2
- Gateway: 10.16.64.1

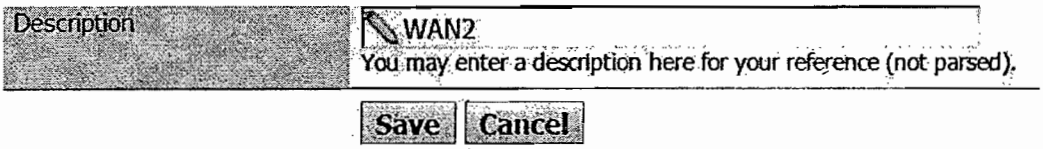
System: Gateways: Edit gateway



- Monitor IP: 10.16.64.92 (ใส่หมายเลขไอพีของ Interface WAN2)

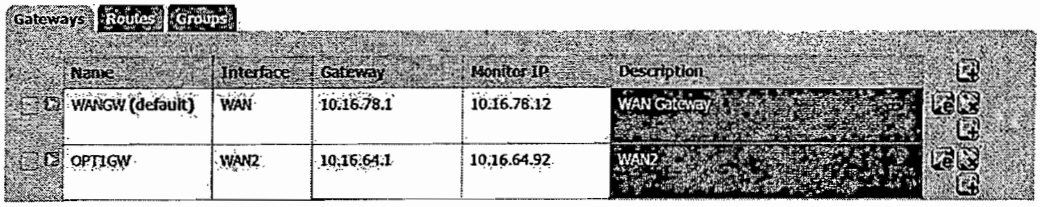


- Save



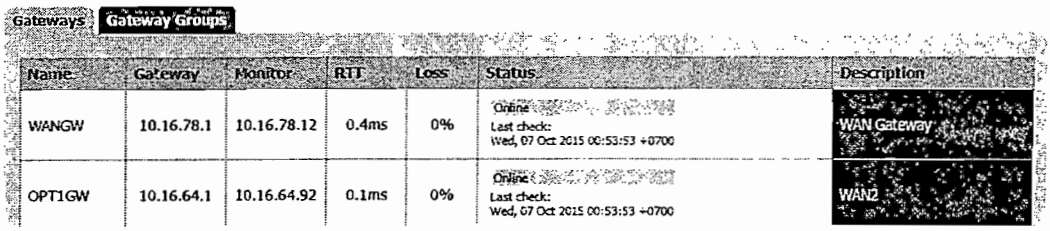
- ผลการตั้งค่า Gateway ของ WAN1 และ WAN2

System: Gateways



ก.13.6 ตรวจสอบสถานะ online ของ Gateways ที่ Interface WAVGW และ OPTGW โดยเข้าไปที่ Status | Gateways

Status: Gateways



ก.14 การตั้งค่า IPsec VPN

ขั้นตอนการกำหนดค่า IPsec VPN มีดังนี้

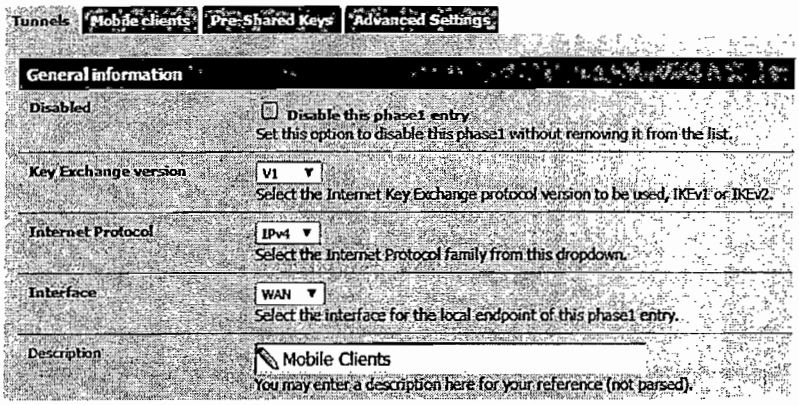
- การกำหนดค่า IPsec VPN
- การสร้างกฎ firewall สำหรับ Interface WAN and IPsec
- กำหนดค่าฝัง client

ก.14.1 การกำหนดค่า IPsec VPN

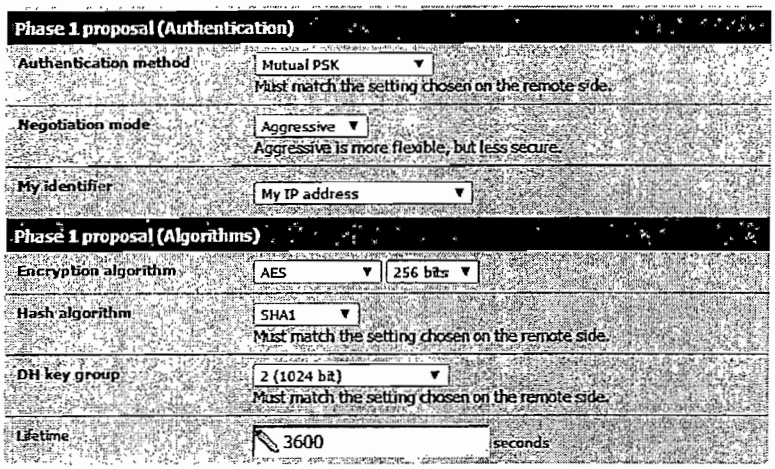
1) เข้าไปที่ Open VPN | IPsec VPN | Tunnels
   - Enable IPsec แล้วคลิก Save

VPN: IPsec

2) ไปที่ add new phase 1 ( )
   - Key Exchange version: v1
   - Internet Protocol: IPv4
   - Interface: WAN
   - Description: Mobile Clients



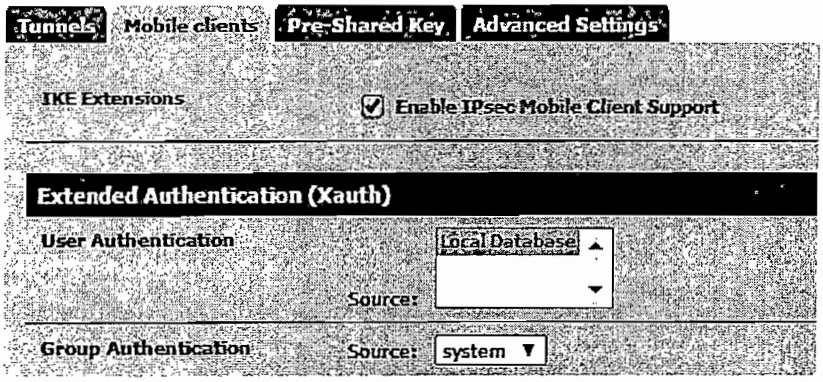
- Authentication method: Mutual SK
- Negotiation mode: Aggressive
- My identifier: My IP address
- Encryption algorithm: AES : 256 bits
- Hash algorithm: SHA1
- DH key group: 2 (1024 bit)
- Lifetime: 3600 seconds แล้วคลิก Save



3) เข้าไปตั้งค่าที่ Mobile clients

- IKE Extensions: ☑ Enable IPsec Mobile Client Support
- User Authentication: Local Database

- Group Authentication: system

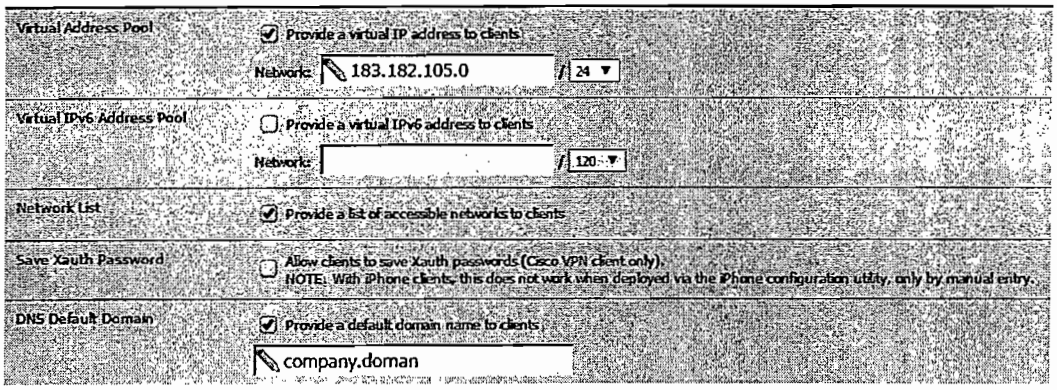


- Virtual Address Pool ☑ Provide a virtual IP address to clients

Network: 13.182.105.0/24

- Network List ☑ Provide a list of accessible networks to Clients
- DNS Default Domain: ☑ Provide a default domain name to clients

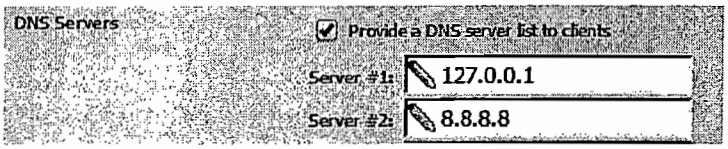
  Company. Doman



- DNS Servers: ☑ Provide a DNS server list to clients

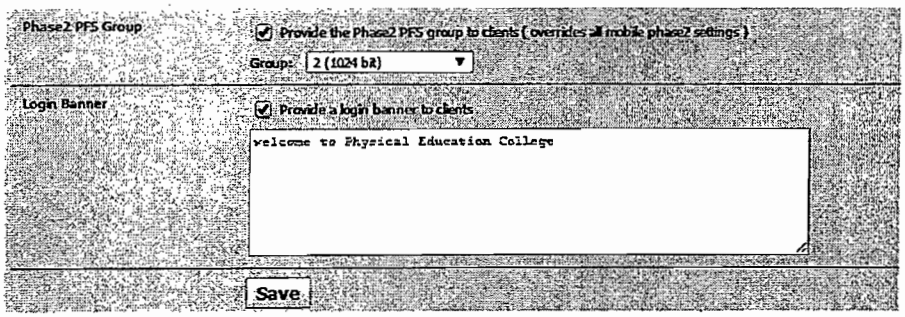
  Server #1: 127.0.0.1

  Server #2: 8.8.8.8

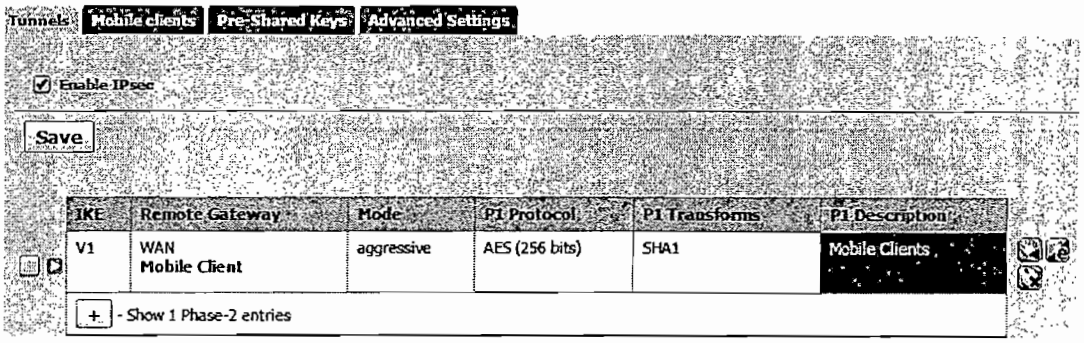


- Phase2 PFS Group: ☑ Provide the Phase2 PFS group to clients (Overrides all) Mobile phase2 settings)
- Group: 2 (1024 bit)
- Login Banner: ☑ Provide a login banner to clients

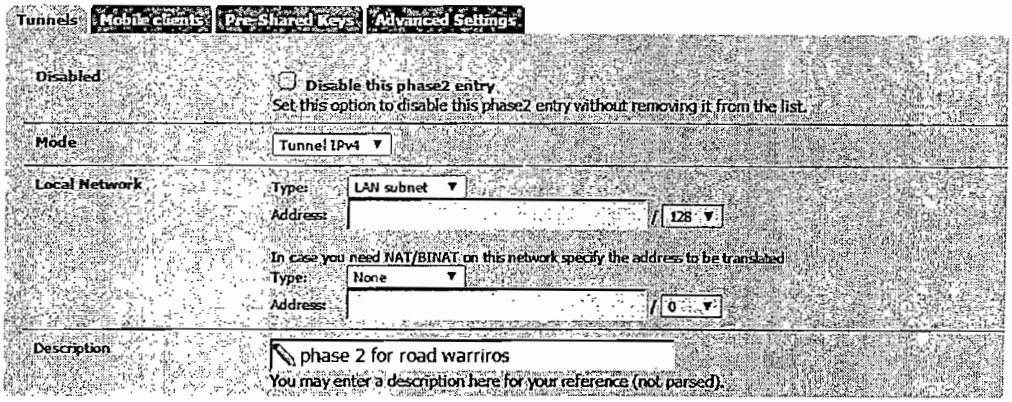
  Welcome to Physical Education College แล้วคลิก Save



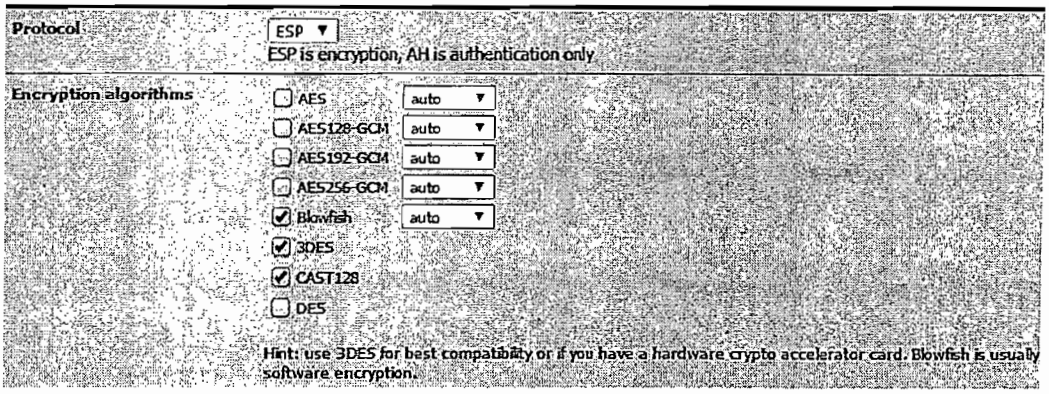
4) สร้าง phase 2 โดยเข้าไปที่ Tunnels | + -Show 0 Phase -2 entries | add new phase ( )



- Mode: Tunnel IPv4
- Local Network: Type: LAN subnet
- Description: phase 2 for road warriors

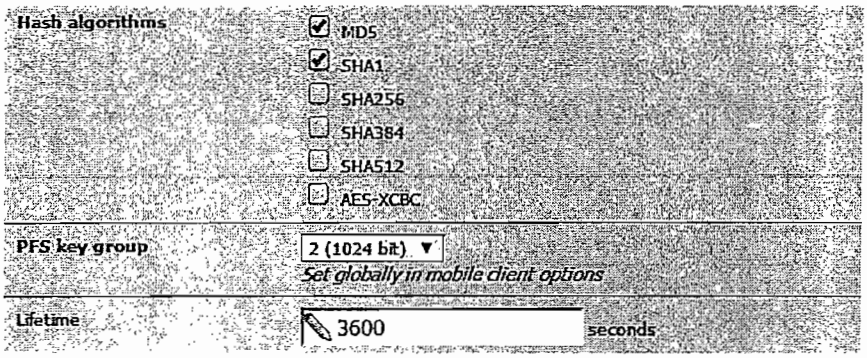


- Protocol: ESP
- Encryption algorithms: ☑ Blowfish ☑ 3DES ☑ CAST128

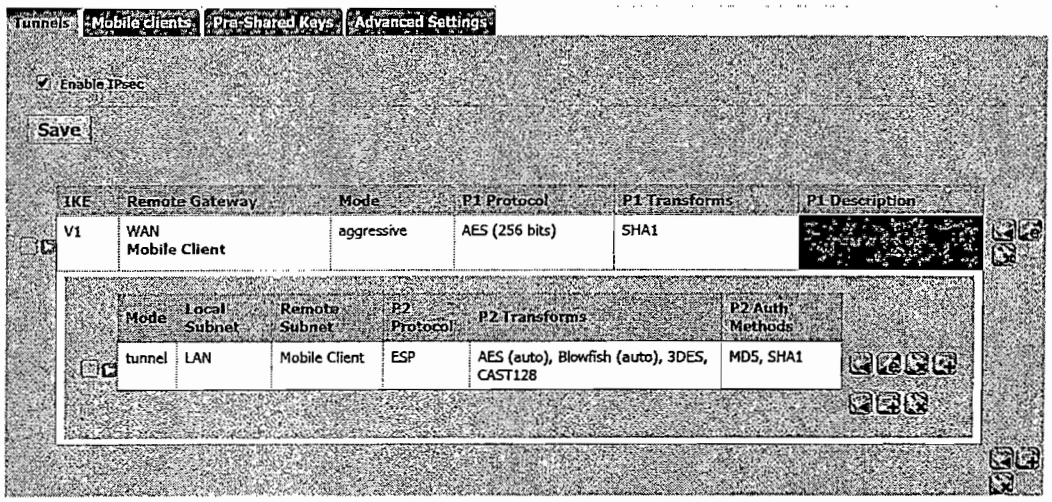


- Hash algorithms: ☑ MD5 ☑ SHA1

- Lifetime: 3600 Seconds แล้วคลิก Save



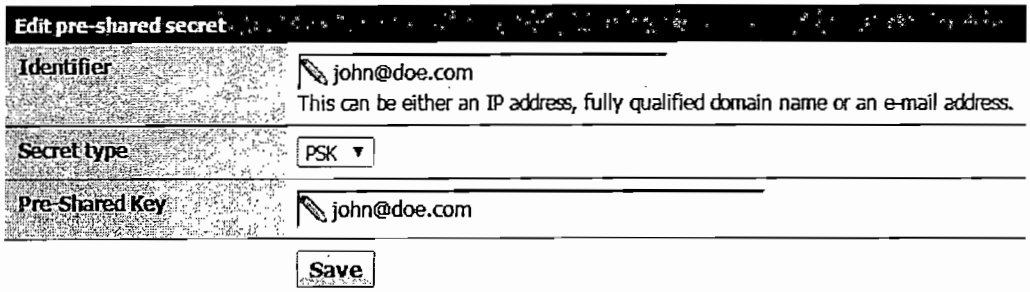
- ผลที่ได้จากการตั้งค่า



5) เข้าไปกำหนดค่าที่ Pre-Shared Keys | add key ( )

- Identifier: john@doe.com
- Secret type: PSK
- Pre-Shared Key: john@doe.com แล้วคลิก Save

VPN: IPsec: Edit Pre-Shared Key



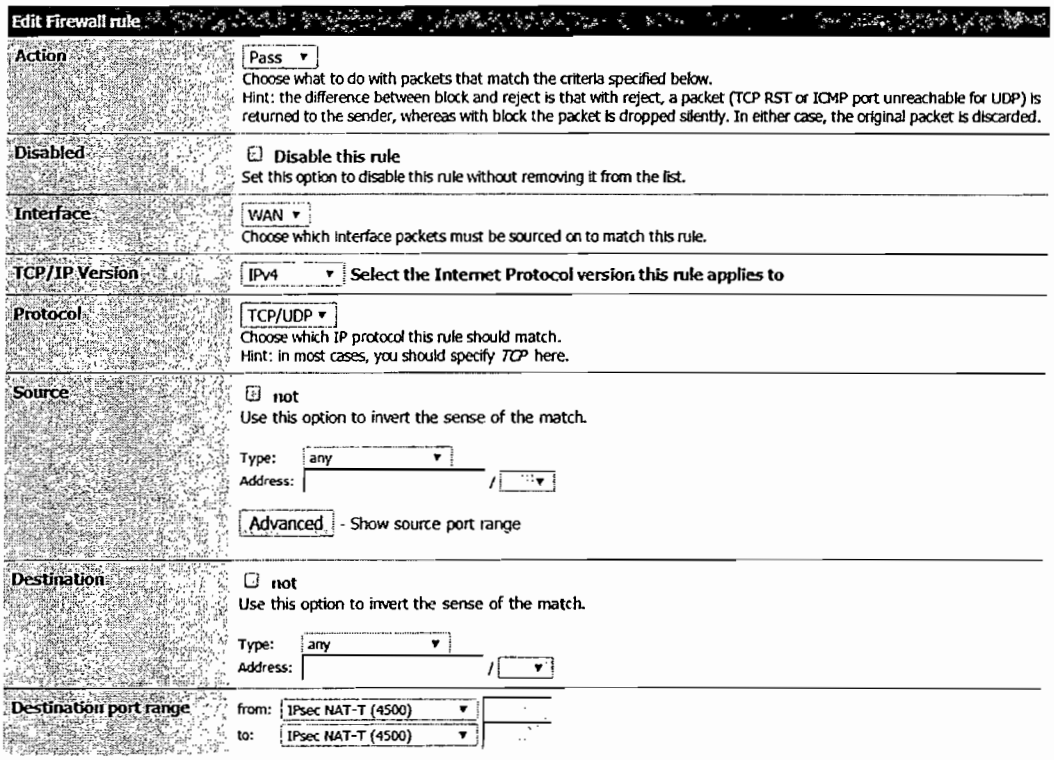
- ผลที่ได้จากการตั้งค่า Pre-Shared Keys ได้ข้อมูลดังภาพด้านล่าง

ก.14.2 การสร้างกฎ firewall สำหรับ Interface WAN and IPsec

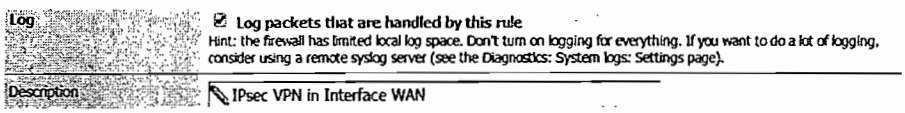
1) เข้าไปที่ Firewall | rule | WAN | add rule ( ) (เพื่ออนุญาตให้ IPsec ผ่าน Interface WAN)

- Action: Pass
- Interface: WAN
- Protocol: TCP/UDP
- Destination port range: from: IPsec NAT-T (4500)

  To: IPsec NAT-T (4500)

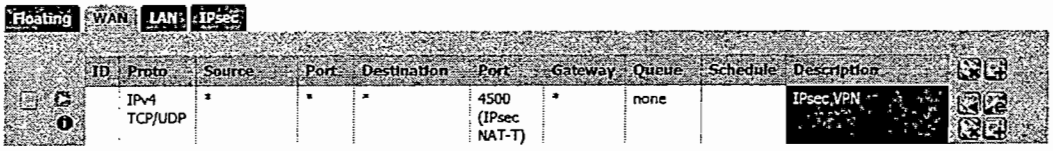


- Log: ☑ Log packets that are handled by this rule
- Description: IPsec VPN in Interface WAN แล้วคลิก Save



- ผลของการสร้างกฎไฟร์วอลล์อนุญาตให้ IPsec ผ่าน Interface WAN ดังภาพด้านล่าง

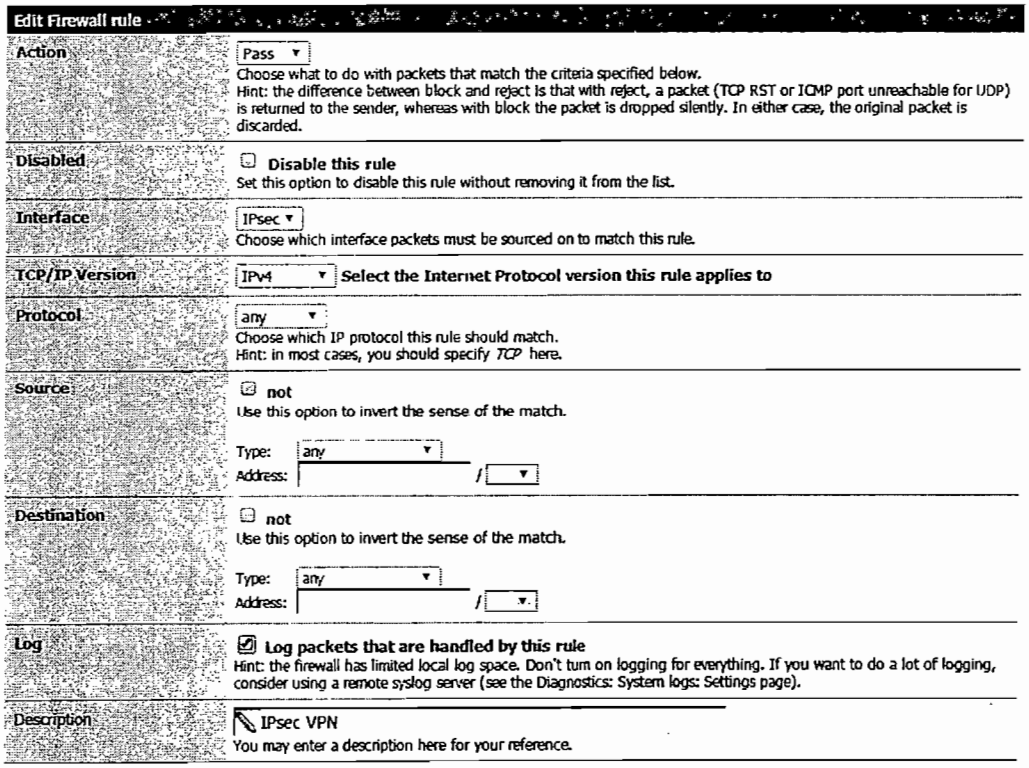
Firewall: Rules



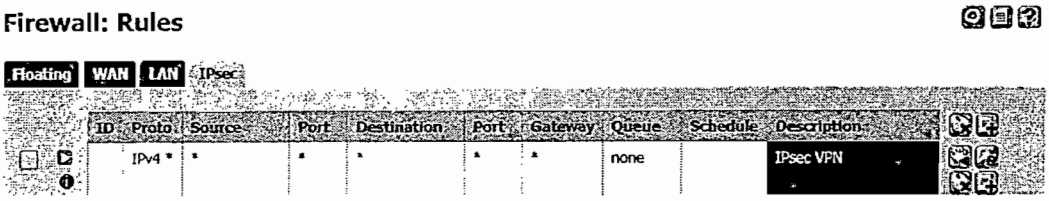
2) เข้าไปที่ Firewall | rule | IPsec | add rule ( ) (เพื่อสร้างกฎใน Interface IPsecVPN)

- Interface: IPsec
- Protocol: any
- Source: any
- Destination: any
- Description: IPsec VPN แล้วคลิด Save

Firewall: Rules: Edit

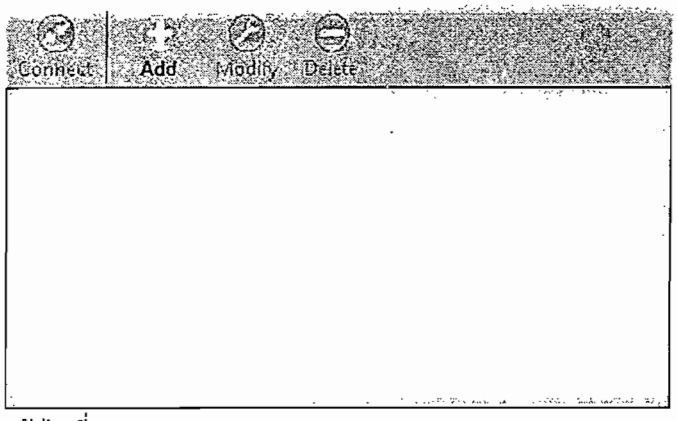


- ผลของการสร้างกฎไฟร์วอลล์ใน Interface IPsec ดังภาพด้านล่าง



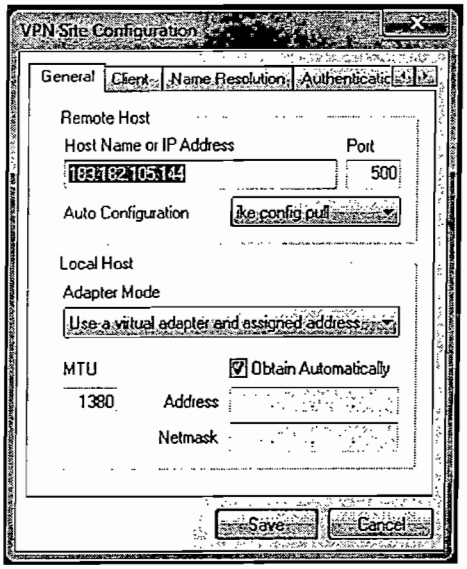
ก.14.3 การติดตั้ง โปรแกรม (vpn-client-2.2.2-release) https://www.shrew.net

1) ทำตั้งค่า vpn-client โดยเข้าไปที่ Add



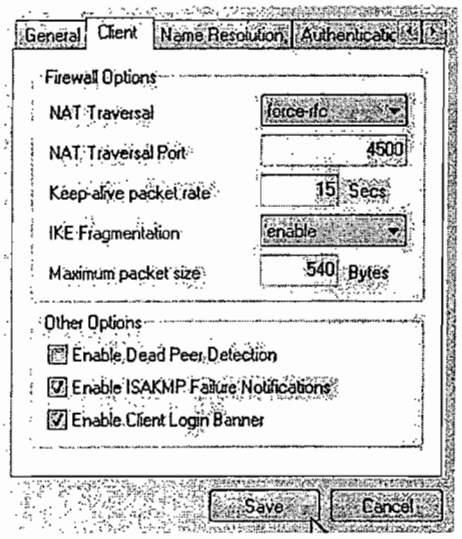
2) เข้าไปที่ General

- Host Name or IP Address: 183.182.105.144
- Port: 500
- Auto Configuration: ike config pull
- Adapter Mode: Use a virtual adapter and assigned address
- MTU: 1380 ☑ Obtain Automatically



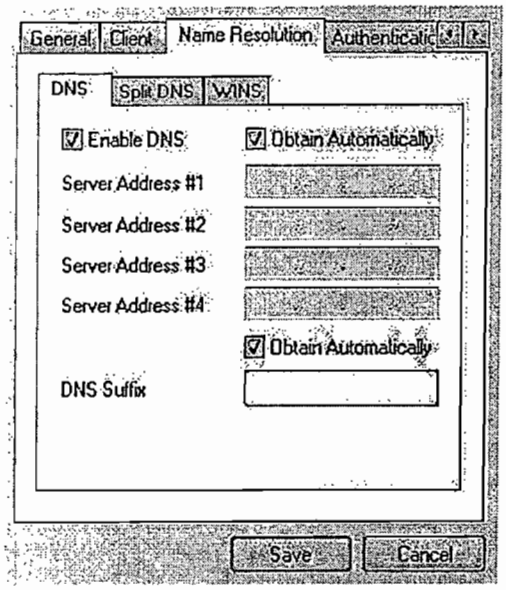
3) เข้าไปที่ Client

- NAT Traversal: force-rfc
- NAT Traversal post: 4500
- Keep-alive packet rate: 15 Secs
- IKE Fragmentation: enable
- Maximum packet size: 540 Bytes
- ☑ Enable ISAKMP Failure Notifications
- ☑ Enable Client Login Banner



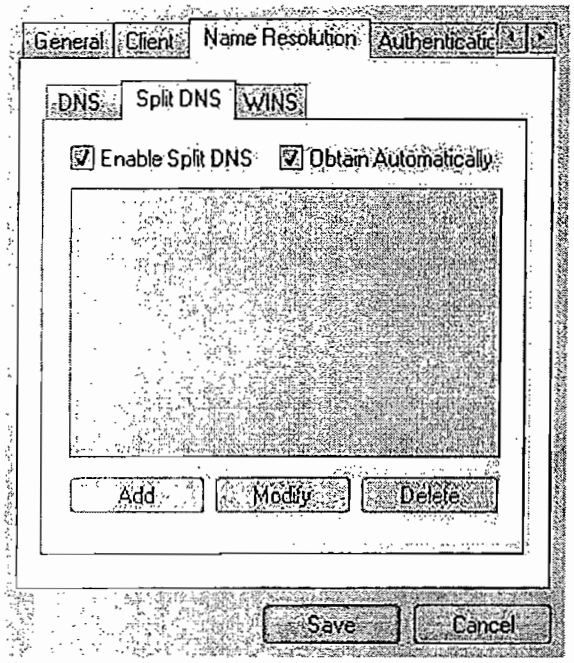
4). เข้าไปที่ Name Resolution | DNS

- ☑ Enable ☑ Obtain Automatically ☑ Obtain Automatically



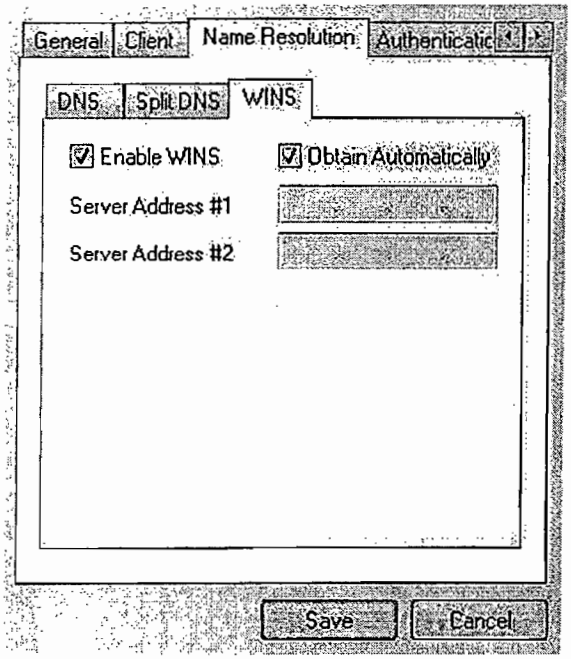
5) เข้าไปที่ Name Resolution | Split DNS

- ☑ Enable Split DNS ☑ Obtain Automatically



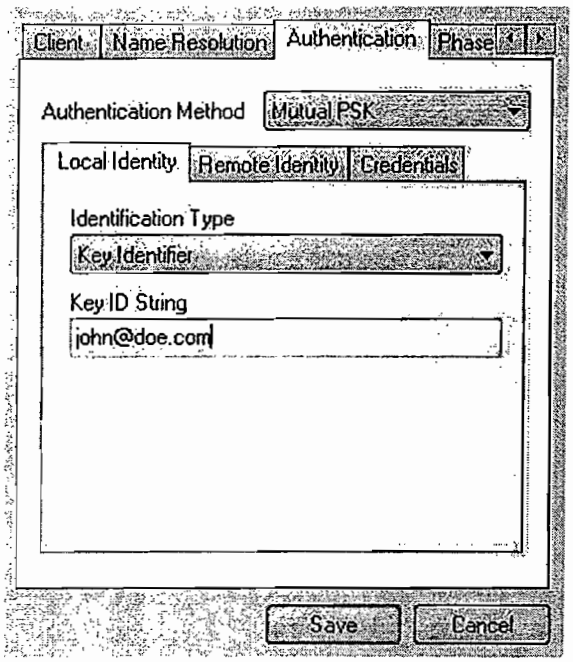
6) เข้าไปที่ Name Resolution | Split DNS

- ☑ Enable WINS ☑ Obtain Automatically



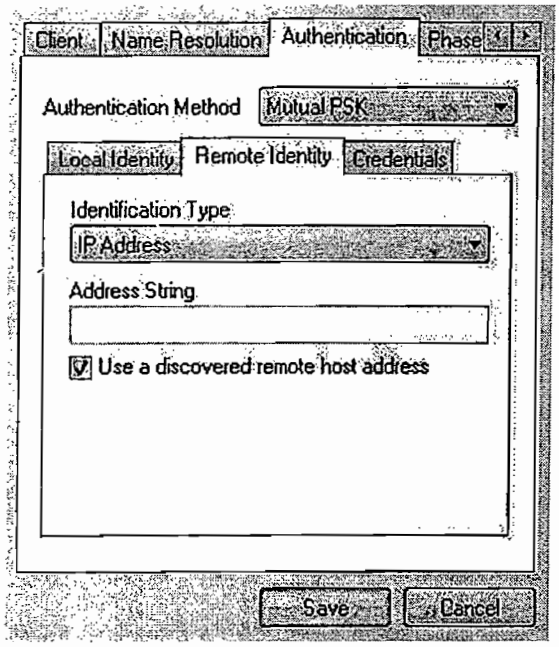
7) เข้าไปที่ Authentication | Local identity

- Identification Type: key Identifier
- Key ID String: john@doe.com



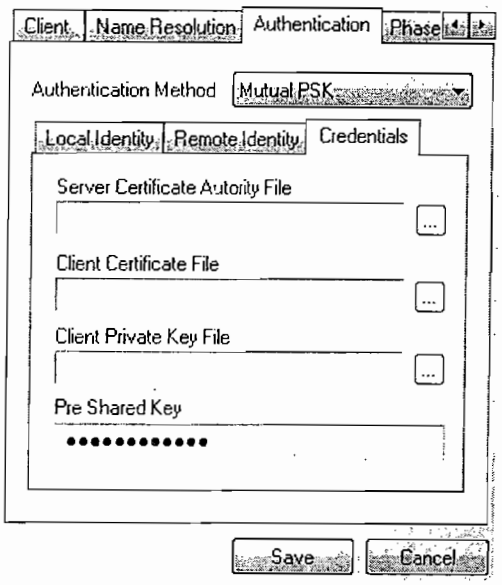
8) เข้าไปที่ Authentication | Remote identity

- Identification Type: IP Address
- ☑ Use a discovered remote host address



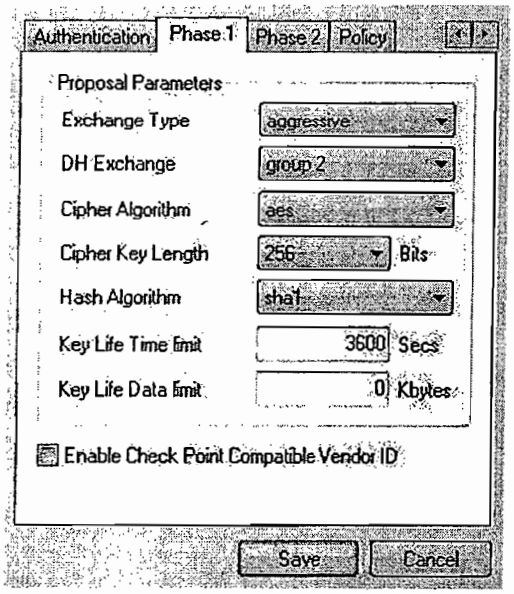
9) เข้าไปที่ Authentication | Remote identity

- Pre Shared Key: john@doe.com



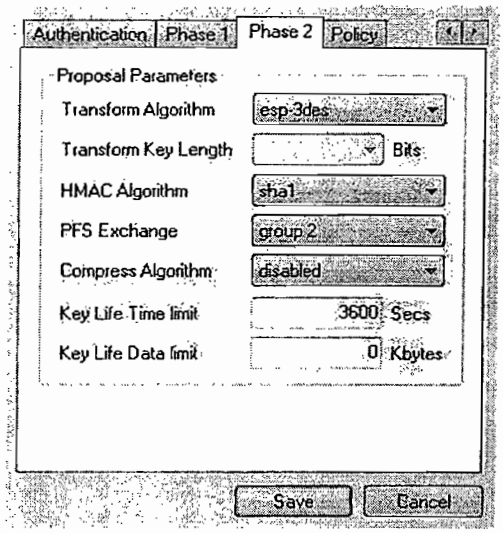
10) เข้าไปที่ phase 1

- Exchange Type: aggressive
- DH Exchange: group 2
- Cipher Algorithm: aes
- Cipher Key Length: 256
- Hash Algorithm: 3600



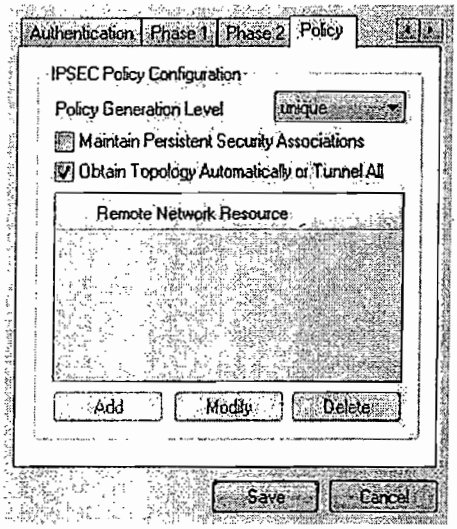
11) เข้าไปที่ phase 2

- Transform Algorithm: esp-3des
- Transform Key Length: sha1
- PFS Exchange: Group 2
- Compress Algorithm: disabled
- Key Life Time Limit: 3600

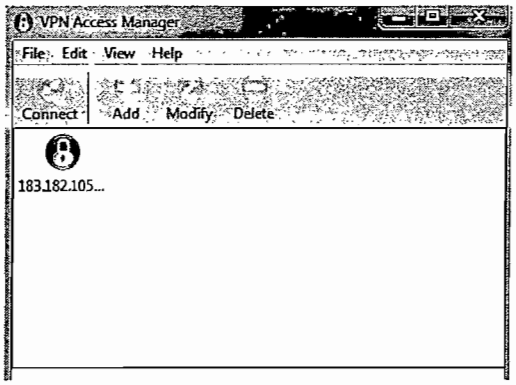


12) เข้าไปที่ Policy

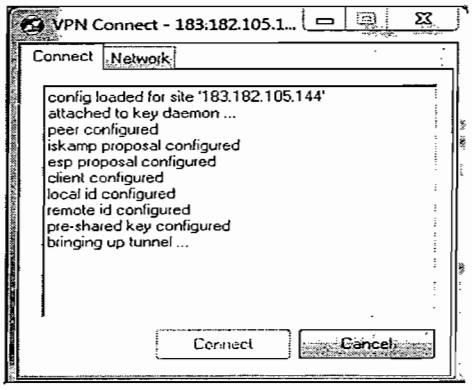
- Policy Generation Level: unique
- ☑ Obtain Topology automatically or tunnel all แล้วคลิก Save



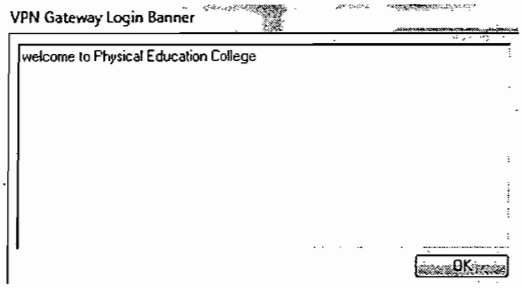
13) ผลของการตั้งค่า



14) การเชื่อมต่อ IPsec VPN



15) ถ้าหากมีการเชื่อมต่อสำเร็จผลก็จะแสดงคังภาพด้านล่าง



16) จากนั้นเราสามารถ ping ไปหาไอพีของ interface LAN Server ได้ ดังภาพด้านล่าง

```
C:\Users\maisouk>ping 192.168.254.1

Pinging 192.168.254.1 with 32 bytes of data:
Reply from 192.168.254.1: bytes=32 time=51ms TTL=64
Reply from 192.168.254.1: bytes=32 time=20ms TTL=64

Ping statistics for 192.168.254.1:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 20ms, Maximum = 51ms, Average = 35ms
```

ก.15 การติดตั้ง และ ตั้งค่า OpenVPN

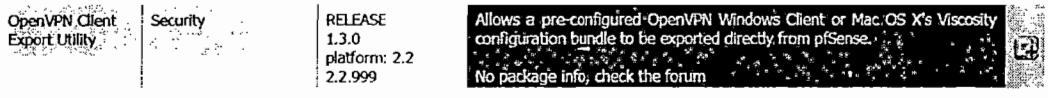
ขั้นตอนการกำหนดค่า OpenVPN มีดังนี้

- ติดตั้ง Packages ของ OpenVPN
- ใช้ Wizard กำหนดค่า OpenVPN
- การสร้าง User
- การกำหนดค่า OpenVPN Client Export

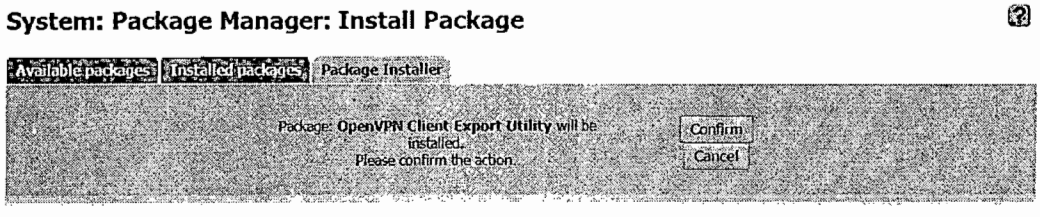
ก.15.1 การติดตั้ง Packages ของ OpenVPN Client Export

1) คลิก System | Packages

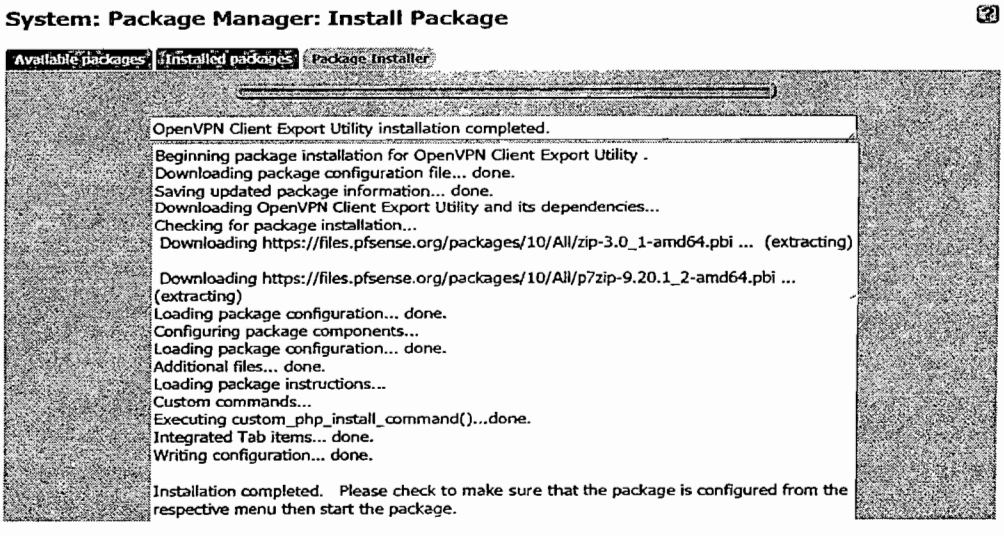
2) เข้าไปที่ Available Packages | แล้วคลิกที่ Add



3) คลิกไปที่ Config



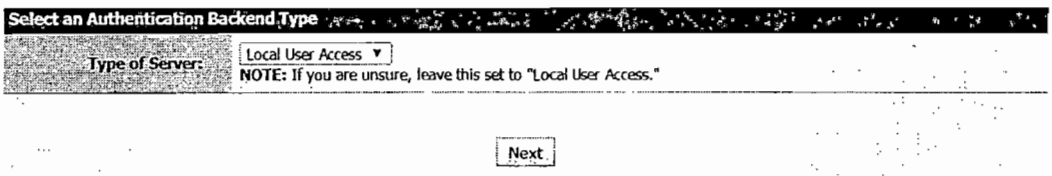
5) การติดตั้ง OpenVPN Client เมื่อติดตั้งเสร็จแล้ว แสดงดังภาพด้านล่าง



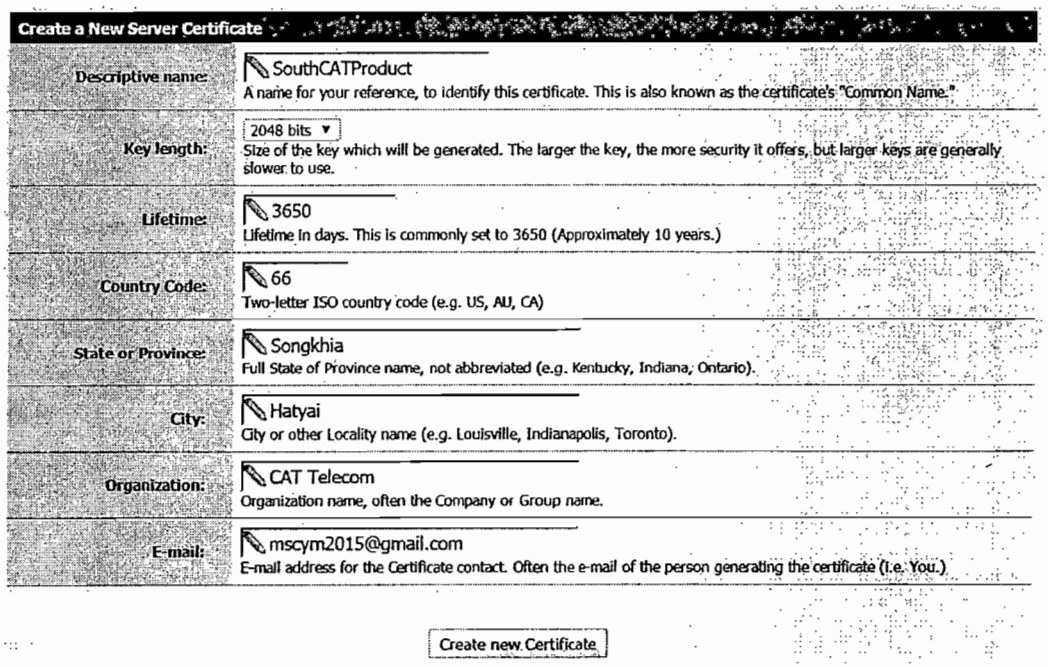
ก.15.2 ใช้ Wizard สำหรับการกำหนดค่า OpenVPN

1) คลิกเข้าไปที่ VPN | OpenVPN | Wizard

2) คลิกเลือก Local User Access แล้วคลิก Next

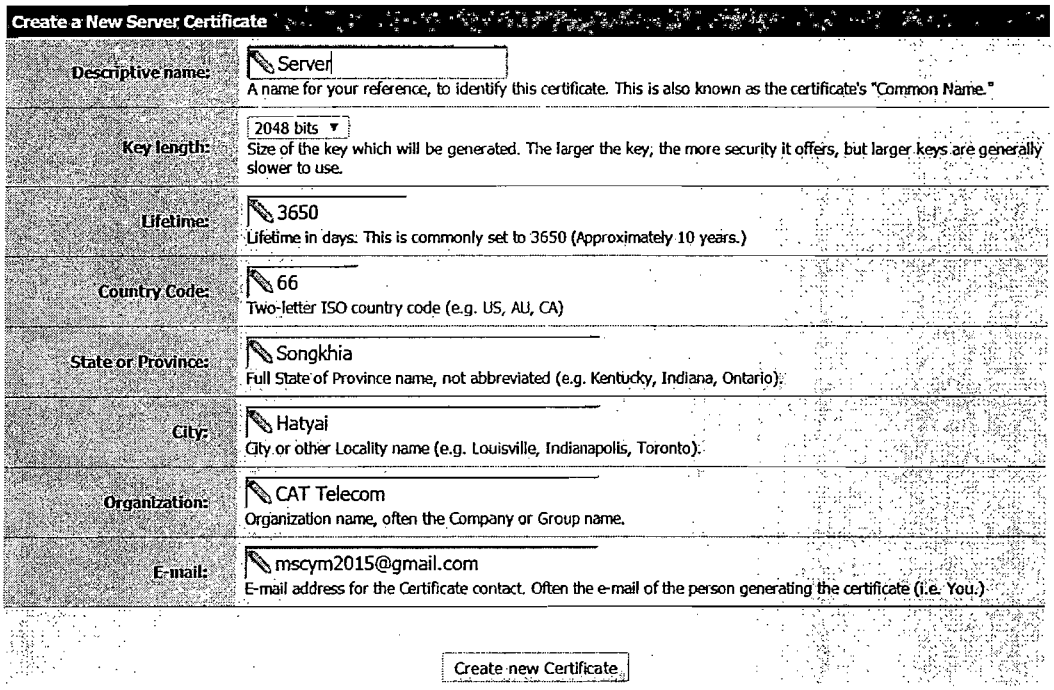


- Descriptive name: SouthCATProduct
- Key Length: 2048 bit
- Lifetime: 3650
- Country Code : laos
- State or Province: khaikhang
- City: venting
- Organization: My company
- E-mail: kuvkhubkoj2014@gmail.com แล้วคลิก Add new CA

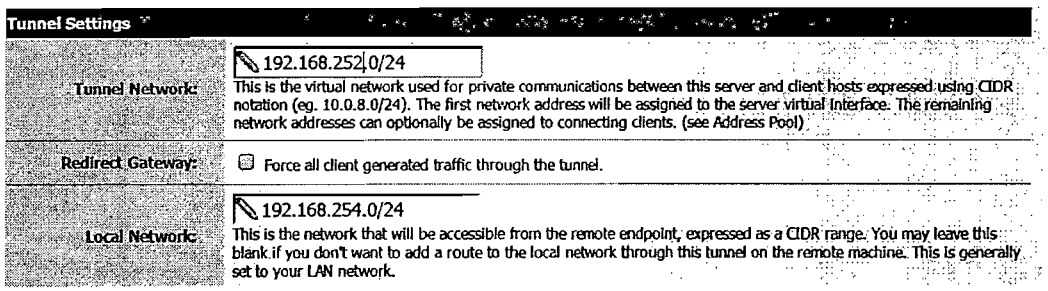


- Descriptive name: Sever แล้ว กด Create New Certificate
- Key Length: 2048 bit

- Lifetime: 3650
- Country Code : laos
- State or Province: khaikhang
- City: venting
- Organization: My company
- E-mail: kuvkhubkoj2014@gmail.com แล้วคลิก Add new CA

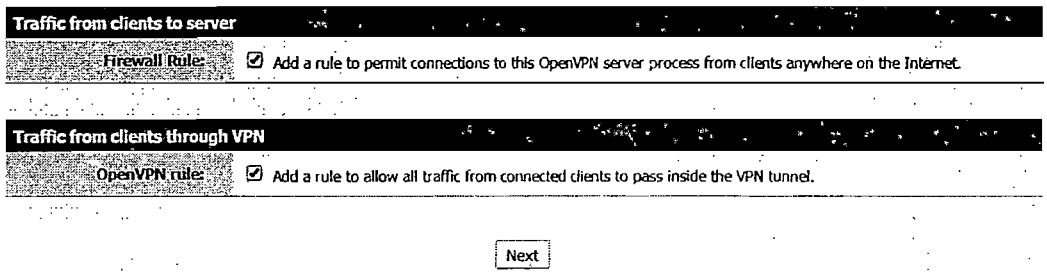


- Tunnel Network: 1192.168.252.0/24
- Local network: 192.168.254.0/24 แล้ว ก่อกด next



- Firewall rule: ☑ Add a rule to permit connections to this Open VPN Server process from clients anywhere on the Internet
- Open VPN rule: ☑ Add a rule to all traffic connected clients

to pass inside the VPN tunnel. แล้วคลิก Next และ คลิก Finish

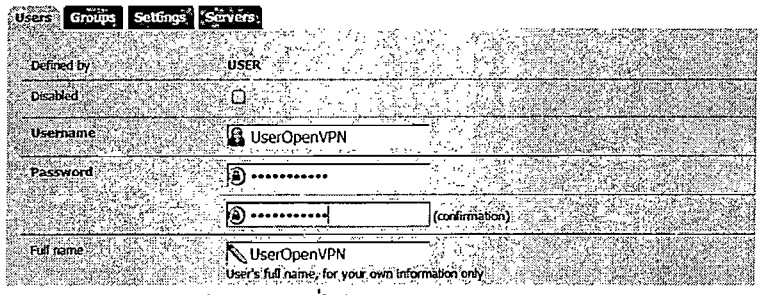


ก.15.3 การสร้าง User ของ Client

1) คลิกเข้าไปที่ System | User Manager | คลิกเพิ่มผู้ใช้ใหม่ที่ 

- Username: maisoukPVN
- Username: maisoukPVN
- Full name: yangchiamoua
- Save.

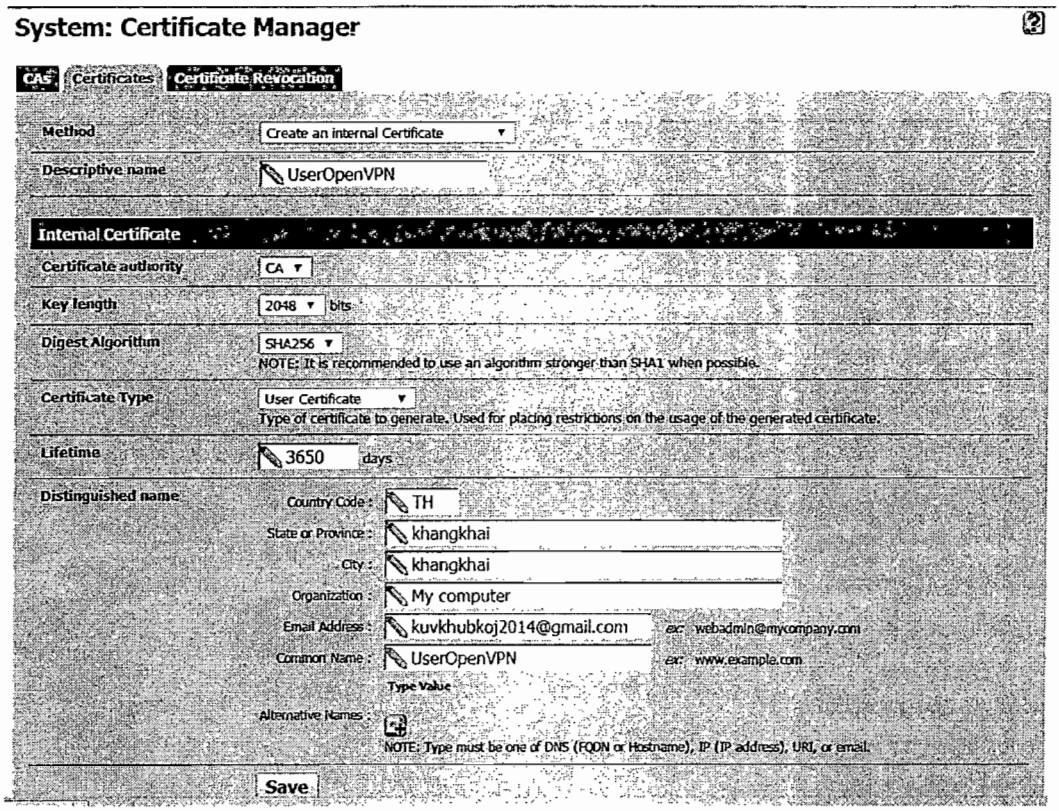
System: User Manager



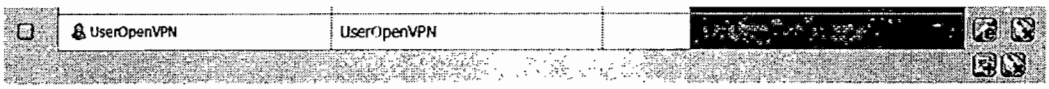
2) ทำการแก้ไข User ที่ใช้ login OpenVPN

- Method: Create an internal certificate
- Descriptive name: UserOpenVPN
- Certificate authority: CA
- Key length: 2048 bit
- Digest Algorithm: SHA256
- Certificate Type: User Certificate
- Lifetime: 3650 days
- Country Code : TH
- State or Province: khangkhai
- City: khangkhai
- Organization: My computer

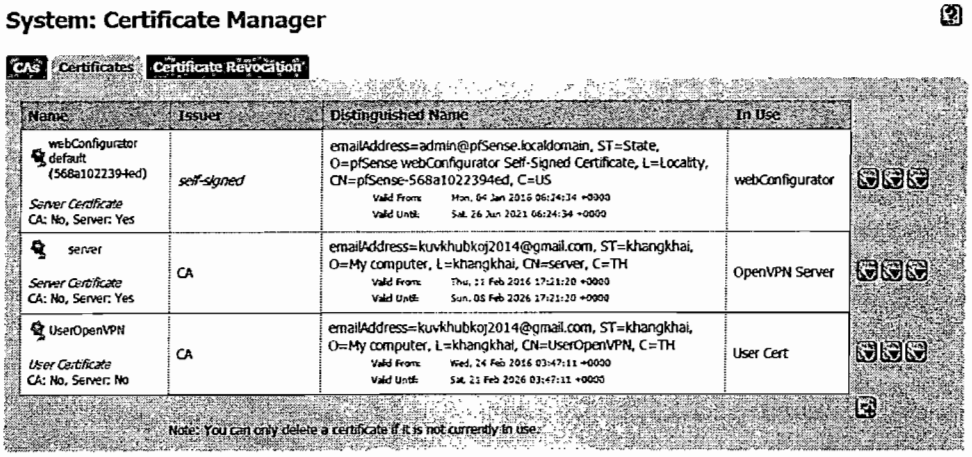
- Email Address: kuvkhubkoj2014@gmail.com
- Common Name: UserOpenVPN แล้วคลิก Save



- ผลที่ได้จากการตั้งค่า

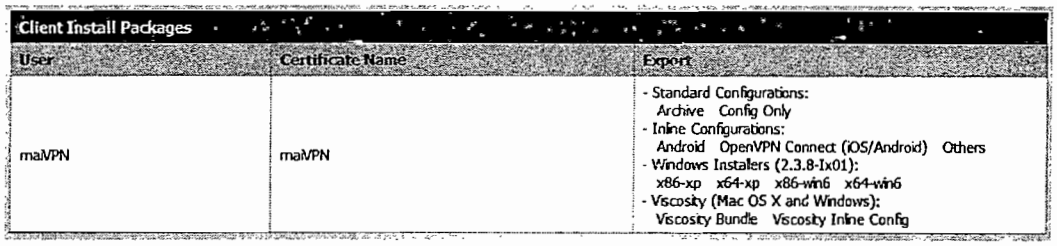


- และให้เข้าไปตรวดดูที่ certificate ว่าผลการสร้าง User ให้เข้าไปที่ System | Certificate Manager | certificate



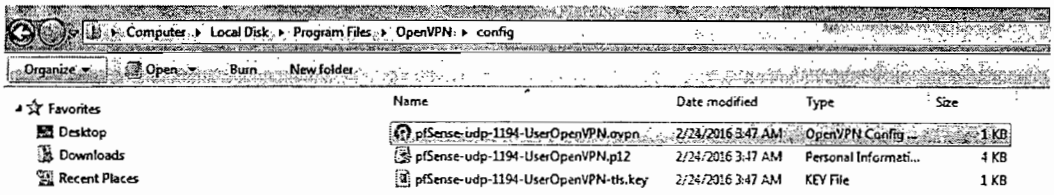
3) การดาวน์โหลดไฟล์ Config และ โปรแกรม OpenVPN เข้าไปที่

- การติดตั้งโปรแกรม OpenVPN Client เข้าไปที่เครื่อง computer
- เข้าไปที่ VPN | OpenVPN | Client Export



- คลิกที่ Archive เพื่อดาวน์โหลดไฟล์ Config ไปใส่ที่

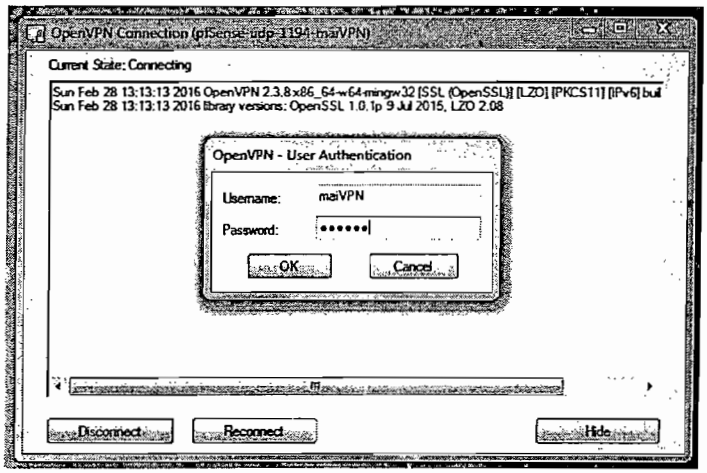
My computer | Local Disk | Program File | OpenVPN | Config



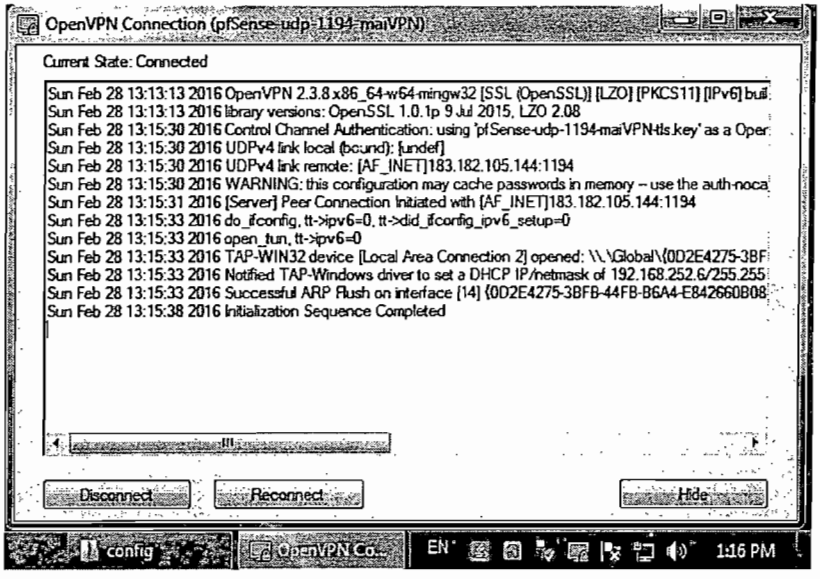
- ลบไฟล์ Config เดิมของโปรแกรม OpenVPN ทิ้งแล้ววาง File Config ที่ดาวน์โหลดไฟล์มาใหม่ใส่

4) การเชื่อมต่อ OpenVPN Client

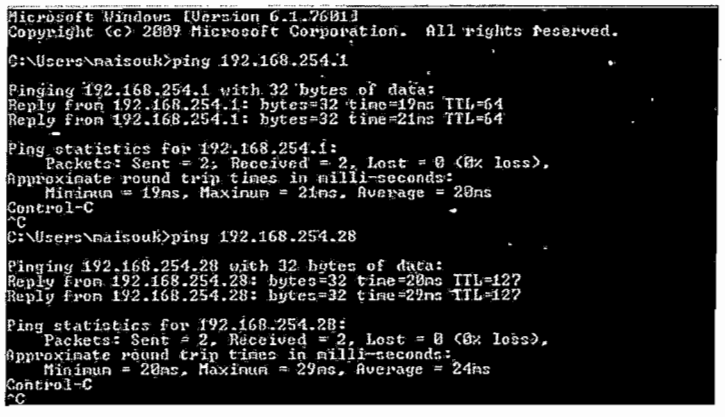
- ใส่ Username: maiVPN
- ใส่ Password: maiVPN แล้งคลิก OK



- การเชื่อมต่อสำเร็จ



5) จากนั้นเราสามารถทำกาน ping ไปหาไอพีของ interface LAN Server ได้ ดังภาพด้านล่าง



ภาคผนวก ข

แบบสอบถามความพึงพอใจการให้บริการระบบเครือข่ายคอมพิวเตอร์

แบบสอบถามความพึงพอใจการให้บริการระบบเครือข่ายคอมพิวเตอร์ วิทยาลัยพละศึกษา (ภาษาไทย)

คำชี้แจง : กรุณาเลือกช่องคำตอบ ตามความเป็นจริงหรือใกล้เคียงกับความคิดเห็นของท่านให้มากที่สุด

1. เพศ

☐ ชาย ☐ หญิง

2. อายุ

☐ ต่ำกว่า 20 ปี ☐ 21-30 ปี ☐ 31-40 ปี ☐ 41-50 ปี ☐ 51-60 ปี ☐ 61 ปีขึ้นไป

3. ระดับการศึกษา

☐ กำลังศึกษาปริญญาตรี ☐ กำลังศึกษาปริญญาโท ☐ กำลังศึกษาปริญญาเอก

☐ ปริญญาตรี ☐ ปริญญาโท ☐ ปริญญาเอก

4. สถานภาพ

☐ นักศึกษา ☐ นักวิชาการ/อาจารย์ ☐ บุคลากร ☐ ผู้บริหาร ☐ อื่น ๆ (โปรดระบุ)

5. ความถี่ในการใช้อินเทอร์เน็ต/วัน

☐ จำนวน 1-3 ชม./วัน ☐ จำนวน 3-6 ชม./วัน ☐ จำนวน 6-9 ชม./วัน ☐ มากกว่า 9 ชม./วัน

6. ความถี่ในการใช้งานอินเทอร์เน็ต/สัปดาห์

☐ น้อยกว่า 1 วัน/สัปดาห์ ☐ 1 วัน/สัปดาห์ ☐ 2 วัน/สัปดาห์ ☐ 3 วัน/สัปดาห์ ☐ 4 วัน/สัปดาห์

☐ 5 วัน/สัปดาห์ ☐ 6 วัน/สัปดาห์ ☐ ใช้ทุกวัน

7. ท่านมักจะใช้บริการในช่วงเวลาใดมากที่สุด

☐ 8.00 – 12.00 น. ☐ 12.00 – 13.00 น. ☐ 13.00 – 16.00 น.

☐ 16.00 – 20.00 น ☐ 20.00 – 24.00 น. ☐ หลังเวลา 24.00 น.

8. สถานที่ที่ใช้บริการอินเทอร์เน็ตเป็นประจำ

☐ ห้องเรียนคอมพิวเตอร์ชั้น 2 ☐ ห้องสมุด ☐ สำนักงาน ที่สังกัด

☐ หอพักของวิทยาลัย ☐ จุดให้บริการ Wireless บริเวณ (โปรดระบุ)

9. เว็บไซต์ที่เข้าใช้มากที่สุด

☐ YouTube ☐ Facebook ☐ LINE ☐ Google ☐ Gmail ☐ Yahoo

☐ เว็บไซต์อื่น .....

10. ท่านรู้จักเว็บไซต์ของวิทยาลัยจากที่ใด

☐ จากเว็บค้นหา เช่น Google ☐ เพื่อนแนะนำ ☐ แผ่นพับที่วิทยาลัยแจก

☐ ลิงค์จากเว็บอื่น ☐ อื่น ๆ (โปรดระบุ)

11. ท่านเข้าชมเว็บไซต์ของวิทยาลัยบ่อยแค่ไหน

☐ ทุกวัน ☐ 1-2 ครั้งต่อสัปดาห์ ☐ 1-2 ครั้งต่อเดือน ☐ น้อยกว่า 1 ครั้งต่อเดือน

☐ ไม่เคย

12. ท่านเข้าชมเว็บไซต์ของวิทยาลัยเพื่อวัตถุประสงค์ใด

☐ อ่านข่าวสารใหม่ๆของวิทยาลัย

☐ ค้นหาเอกสาร แบบฟอร์ม หรือบทความ

☐ ส่งข้อคิดเห็นติชมให้วิทยาลัย

☐ เพื่อหาข้อมูลเกี่ยวกับรายวิชาเรียน

☐ อื่น ๆ (โปรดระบุ) .....

13. ท่านคิดว่าเว็บไซต์ของวิทยาลัยเป็นประโยชน์ต่อท่านหรือไม่

☐ ค่อนข้างเป็นประโยชน์

☐ เป็นประโยชน์ แต่ยังไม่เพียงพอ

☐ ไม่เป็นประโยชน์เลย

14. สัญญาณ Wireless ครอบคลุมทั่วถึง

☐ มากที่สุด ☐ มาก ☐ ปานกลาง ☐ น้อย ☐ น้อยที่สุด

15. ความสะดวกความเร็วในการเชื่อมต่อสัญญาณ Wireless ก่อนเข้าใช้งาน

☐ แย่มาก ☐ แย่ ☐ ปานกลาง ☐ ดี ☐ ดีมาก

16. ความเร็วของสัญญาณในการส่งข้อมูล และ ใช้อินเทอร์เน็ต ได้รวดเร็วหรือไม่

☐ แย่มาก ☐ แย่ ☐ ปานกลาง ☐ ดี ☐ ดีมาก

17. สามารถตอบสนองความต้องการของผู้ใช้บริการมีระบบ Authentication เวลาเครือข่ายไร้สายเพื่อตรวจสอบสิทธิ์ผู้ใช้

☐ แย่มาก ☐ แย่ ☐ ปานกลาง ☐ ดี ☐ ดีมาก

18. ท่านคิดว่า Authentication เวลาเครือข่ายไร้สายของวิทยาลัยเป็นประโยชน์ต่อท่านหรือไม่

☐ แย่มาก ☐ แย่ ☐ ปานกลาง ☐ ดี ☐ ดีมาก

19. ท่านคิดว่า Authentication เวลาเครือข่ายไร้สายของวิทยาลัยจะมีความปลอดภัยต่อท่านหรือไม่

☐ แย่มาก ☐ แย่ ☐ ปานกลาง ☐ ดี ☐ ดีมาก

20. ท่านคิดว่า Authentication ของวิทยาลัยจะมีความล่าช้าต่อท่านหรือไม่

☐ แย่มาก ☐ แย่ ☐ ปานกลาง ☐ ดี ☐ ดีมาก

21. ความมีเสถียรภาพของระบบฯ Authentication เวลาเครือข่ายไร้สาย

☐ แย่มาก ☐ แย่ ☐ ปานกลาง ☐ ดี ☐ ดีมาก

22. ความสะดวกในการเข้าถึงระบบ Authentication เครือข่ายคอมพิวเตอร์ที่เป็นระบบสาย (LAN) ของวิทยาลัย (LAN)

☐ แย่มาก ☐ แย่ ☐ ปานกลาง ☐ ดี ☐ ดีมาก

23. ความเร็วในการใช้งานอินเทอร์เน็ต (Internet) ผ่านระบบเครือข่ายคอมพิวเตอร์ของวิทยาลัย (LAN)

☐ แย่มาก ☐ แย่ ☐ ปานกลาง ☐ ดี ☐ ดีมาก

24. ความมีเสถียรภาพของระบบฯ สามารถใช้งานอินเทอร์เน็ต (Internet) ได้อย่างต่อเนื่อง (LAN)

☐ แย่มาก ☐ แย่ ☐ ปานกลาง ☐ ดี ☐ ดีมาก

กรุณาให้ความคิดเห็นหรือคำแนะนำอื่นๆ

.....

.....

.....

.....

.....

.....

.....

.....

.....

ແບບສອບຖາມ (ภาษาลาว)

ຄວາມເພິ່ງພໍໃຈການໃຫ້ບໍລິການລະບົບເຄືອຂ່າຍຄອມພິວເຕີໃນວິທະຍາໄລພະລະສົງສາ

ຄຳຊີ້ແຈງ: ກະລຸນາເລືອກຄຳຕອບຕາມຄວາມເປັນຈິງ ຫຼື ໃກ້ຄຽງທີ່ສຸດຂອງທ່ານເຫັນ

1. ເພດ*

   ☐ ຊາຍ

   ☐ ຍິງ

2. ອາຍຸ*

   ☐ ຕ່ຳກວ່າ 20 ປີ ☐ 21-30 ປີ ☐ 31-40ປີ

   ☐ 41-50 ປີ ☐ 51-60 ປີ ☐ 61 ປີຂຶ້ນໄປ

3. ລະດັບການສຶກສາ*

   ☐ ສຶກສາຕ່ຳປະລິນຍາຕີ ☐ ສຶກສາຕ່ຳປະລິນຍາໂທ ☐ ສຶກສາຕ່ຳປະລິນຍາເອກ ☐ ປະລິນຍາຕີ ☐ ປະລິນຍາໂທ ☐ ປະລິນຍາເອກ

4. ສະຖານະພາບ*

   ☐ ນັກສຶກສາ ☐ ນັກວິຊາການ/ອາຈານ ☐ ບຸກຄະລາກອນ

   ☐ ຜູ້ບໍລິຫານ ☐ ອື່ນໆ

5. ຄວາມຖີ່ໃນການໃຊ້ອິນເຕີເນັດ/ວັນ*

   ☐ ຈຳນວນ 1-3 ຊມ/ວັນ ☐ ຈຳນວນ 3-6 ຊມ/ວັນ ☐ ຈຳນວນ 6-9 ຊມ/ວັນ

   ☐ ຫຼາຍກວ່າ 9 ຊມ/ວັນ

6. ຄວາມຖີ່ໃນການໃຊ້ງານອິນເຕີເນັດ/ອາທິດ*

   ☐ ໜ້ອຍກວ່າ 1 ວັນ/ອາທິດ ☐ 1 ວັນ/ອາທິດ ☐ 2 ວັນ/ອາທິດ

   ☐ 3 ວັນ/ອາທິດ ☐ 4 ວັນ/ອາທິດ ☐ 5 ວັນ/ອາທິດ

   ☐ 6 ວັນ/ອາທິດ ☐ ໃຊທຸກວັນ

7. ທ່ານມັກໃຊ້ຊ່ວງເວລາໃດຫຼາຍທີ່ສຸດ*

   ☐ 8:00-12:00ໂມງ ☐ 12:00-13:00 ໂມງ ☐ 13:00-16:00 ໂມງ

   ☐ 16:00-20:00ໂມງ ☐ 20:00-24:00 ໂມງ ☐ ຫຼັງຈາກ 24:00 ໂມງ

8. ສະຖານທີ່ໃຊ້ບໍລິການອິນເຕີເນັດເປັນປະຈຳ*

   ☐ ຫ້ອງຮຽນຄອມພິວເຕີຊັ້ນ 2☐ ຫ້ອງສະໝຸດ ☐ ຫ້ອງການທີ່ສັງກັດ

   ☐ ຫໍພັກຂອງວິທະຍາໄລ ☐ ຈຸດໃຫ້ບໍລິການ Wireless ບໍລິເວນ

9. ເວບໄຊທີ່ເຂົ້າໃຊ້ຫຼາຍທີ່ສຸດ*

   ☐ Youtube ☐ Facebook ☐ Line ☐ Google

   ☐ Gmail ☐ Yahoo ☐ Websize

10. ທ່ານຮູ້ຈັກເວບໄຊຂອງມະຫາວິທະຍາໄລທີ່ໃດ*

☐ ຈາກເວບຄົ້ນຫາເຊັ່ນ Google ☐ ເພື່ອນແນະນຳ

☐ ແຜນພັບທີ່ວິທະຍາໄລແຈກ ☐ ລິ້ງຈາກເວບອື່ນ

☐ ແລະ ອື່ນໆ ກະລຸນາລະບຸ.....

11. ທ່ານເຂົ້າຊົມເວບໄຊຂອງວິທະຍາໄລຫຼາຍປານໃດ*

☐ ທຸກວັນ ☐ 1-2 ຄັ້ງຕໍ່ອາທິດ ☐ 1-2 ຄັ້ງຕໍ່ເດືອນ

☐ ໜ້ອຍກວ່າ 1 ຄັ້ງຕໍ່ເດືອນ ☐ ບໍ່ເຄີຍ

12. ທ່ານ ເຂົ້າຊົມເວບໄຊຂອງວິທະຍາໄລເພື່ອຈຸດປະສົງຫຍັງ*

☐ ອ່ານຂ່າວສານໃໝ່ໆ ຂອງວິທະຍາໄລ

☐ ຄົ້ນຫາເອກະສານ ແບບຟອມ ຫຼື ບົດຄວາມ

☐ ສົ່ງຂໍ້ຄວາມຄິດເຫັນໃຫ້ແກ່ວິທະຍາໄລ

☐ ເພື່ອຫາຂໍ້ຄວາມກ່ຽວກັບລາຍວິຊາຮຽນ

☐ ແລະ ອື່ນໆ (ກະລຸນາລະບຸ).....

13. ທ່ານຄິດວ່າເວບໄຊຂອງວິທະຍາໄລເປັນປະໂຫຍດຕໍ່ທ່ານ ຫຼື ບໍ່*

☐ ຄອນຂ້າງເປັນປະໂຫຍດ

☐ ເປັນປະໂຫຍດແຕ່ຍັງບໍ່ພຽງພໍ

☐ ບໍ່ເປັນປະໂຫຍດເລີຍ

14. ສັນຍານ Wireless ຄອບຄຸມທົ່ວເຖິງ*

☐ ອ່ອນຫຼາຍ ☐ ອ່ອນ☐ ປານກາງ ☐ ດີ ☐ ດີຫຼາຍ

15. ຄວາມສະດວກຄວາມໄວໃນການເຊື່ອມຕໍ່ສັນຍານ Wireless ກ່ອນເຂົ້າໃຊ້ງານ*

☐ ອ່ອນຫຼາຍ ☐ ອ່ອນ☐ ປານກາງ ☐ ດີ ☐ ດີຫຼາຍ

16. ຄວາມໄວຂອງສັນຍານໃນການສົ່ງຂໍ້ມູນ ແລະ ໃຊ້ອິນເຕີເນັດໄດ້ຢ່າງໄວວາ ຫຼື ບໍ່*

☐ ອ່ອນຫຼາຍ ☐ ອ່ອນ☐ ປານກາງ ☐ ດີ ☐ ດີຫຼາຍ

17. ສາມາດຕອບສະໜອງຄວາມຕ້ອງການຂອງຜູ້ໃຊ້ບໍລິການມີລະບົບ Authentication ເວລາ ເຄື່ອຂ່າຍໄລ່ສາຍ ເພື່ອກວດກາສິດຜູ້ໃຊ້*

☐ ອ່ອນຫຼາຍ ☐ ອ່ອນ☐ ປານກາງ ☐ ດີ ☐ ດີຫຼາຍ

18. ທ່ານຄິດວ່າ Authentication ເວລາເຄື່ອຂ່າຍ ໄລ່ສາຍຂອງວິທະຍາໄລເປັນປະໂຫຍດຕໍ່ ທ່ານ ຫຼື ບໍ່*

☐ ອ່ອນຫຼາຍ ☐ ອ່ອນ☐ ປານກາງ ☐ ດີ ☐ ດີຫຼາຍ

19. ທ່ານຄິດວ່າ Authentication ເວລາເຄື່ອຂ່າຍໄລ່ສາຍຂອງວິທະຍາໄລຈະມີຄວາມປອດໄພ ຕໍ່ທ່ານ ຫຼື ບໍ່*

☐ ອ່ອນຫຼາຍ ☐ ອ່ອນ☐ ປານກາງ ☐ ດີ ☐ ດີຫຼາຍ

20. ທ່ານຄິດວ່າ Authentication ເວລາເຄື່ອຂ່າຍໄລ່ສາຍຂອງວິທະຍາໄລຈະມີຄວາມສຳຄັນຕໍ່ທ່ານ ຫຼື ບໍ່*

☐ ອ່ອນຫຼາຍ ☐ ອ່ອນ☐ ປານກາງ ☐ ດີ ☐ ດີຫຼາຍ

21. ຄວາມມີສະຖຽນລະພາບຂອງລະບົບ Authentication ເວລາເຄື່ອຂ່າຍໄລ່ສາຍ*

☐ ອ່ອນຫຼາຍ ☐ ອ່ອນ☐ ປານກາງ ☐ ດີ ☐ ດີຫຼາຍ

22. ຄວາມສະດວກໃນການເຂົ້າເຖິງລະບົບ Authentication ເວລາເຄື່ອຂ່າຍຄອມພິວເຕີທີ່ເປັນລະບົບສາຍ (LAN) ຂອງວິທະຍາໄລ (LAN) *

☐ ອ່ອນຫຼາຍ ☐ ອ່ອນ☐ ປານກາງ ☐ ດີ ☐ ດີຫຼາຍ

23. ຄວາມໄວໃນການໃຊ້ງານອິນເຕີເນັດ (Internet) ຜ່ານລະບົບເຄື່ອຂ່າຍຄອມພິວເຕີຂອງວິທຍາໄລ (LAN) *

☐ ອ່ອນຫຼາຍ ☐ ອ່ອນ☐ ປານກາງ ☐ ດີ ☐ ດີຫຼາຍ

24. ຄວາມມີສະຖຽນລະພາບຂອງລະບົບ ສາມາດໃຊ້ງານອິນເຕີເນັດ (Internet) ໄດ້ຢ່າງຕໍ່ເນື່ອງ (LAN) *

☐ ອ່ອນຫຼາຍ ☐ ອ່ອນ☐ ປານກາງ ☐ ດີ ☐ ດີຫຼາຍ

ກະລຸນາໃຫ້ຄວາມຄິດເຫັນ ຫຼື ຄຳແນະນຳອື່ນໆເພີ່ມເຕີມ

.....

.....

.....

.....

.....