รายงานสหกิจศึกษาฉบับสมบูรณ์

การพัฒนาระบบความปลอดภัยของเครือข่ายในองค์กร

NETWORK SECURITY FOR SMB

สิรวิชญ์ อมรกิตติสาร

SIRAVIT AMORNKITTISARN

ภาควิชา วิศวกรรมสารสนเทศ

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2559

รายงานสหกิจศึกษาฉบับสมบูรณ์

การพัฒนาระบบความปลอดภัยของเครือข่ายในองค์กร

NETWORK SECURITY FOR SMB

สิรวิชญ์ อมรกิตติสาร

SIRAVIT AMORNKITTISARN

ภาควิชา วิศวกรรมสารสนเทศ

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2559

ชื่อโครงงานสหกิจศึกษา	การพัฒนาระบบความปลอดภัยของเครือข่ายในองค์กร
ชื่อ-สกุลนักศึกษา	นายสิรวิชญ์ อมรกิตติสาร
คณะ	วิศวกรรมศาสตร์บัณฑิต **ภาควิชา** วิศวกรรมสารสนเทศ
ชื่อ-สกุลอาจารย์นิเทศน์	ผศ.มยุรี เลิศเวชกุล
ชื่อ-สกุล ผู้นิเทศน์งาน	คุณนฤดล รุ่งวีรกุลอนันต์
ชื่อสถานประกอบการ	บริษัท ไดเมนชั่นดาต้า (ประเทศไทย) จำกัด

บทคัดย่อ

บริษัท ไดเมนชั่นดาต้า (ประเทศไทย) จำกัดเป็นบริษัทที่ให้บริการโซลูชั่นทางด้านไอที มีความต้องการที่จะใช้งานซอฟต์แวร์โอเพนซอร์สไฟร์วอลเพื่อรักษาความปลอดภัยระบบเครือข่าย (Network Security) ให้กับลูกค้า ทั้งนี้การดำเนินการโครงงานนี้จำเป็นต้องใช้ความรู้ทางด้านความปลอดภัยระบบเครือข่าย และการออกแบบ ติดตั้ง และตั้งค่าการทำงานอุปกรณ์เครือข่าย รวมทั้งต้องมีการวิเคราะห์ปัญหาหรือจุดบกพร่องต่างๆ ของระบบ และนำเสนอแนวทางในการแก้ปัญหาให้กับลูกค้า เพื่อให้ระบบเครือข่ายของลูกค้านั้นมีความปลอดภัยมากที่สุดและสามารถทำงานได้อย่างมีประสิทธิภาพ

Co-operative Title Network security for SMB

Student Intern Name Siravit Amornkittisarn

Faculty Engineering **Department** Information Engineering

Advisor Name Asst.Prof. Mayuree Lertwatechakul

Mentor Name Narudol Rungveerakulanan

Company Dimension Data (Thailand) Limited

ABSTRACT

Dimension Data (Thailand) Limited is a company whose main business is to provide IT business solutions. Recently, there are needs to use the open source firewalls for implementing the customers' network security. It is required to have knowledge in network security as well as how to design, install and configure networking equipment. The problem analysis is also needed before a design phase as to deliver the most security and efficient network solution to the customer.

กิตติกรรมประกาศ

ข้าพเจ้าได้รับผิดชอบและปฏิบัติหน้าที่ในบริษัท ไดเมนชั่นดาต้า จำกัด ระหว่างวันที่ 8 สิงหาคม ถึงวันที่ 25 พฤศจิกายน พ.ศ.2559 ในโครงการวิชาสหกิจศึกษาที่ทางคณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง และบริษัทฯร่วมมือกันจัดตั้งขึ้นในหัวข้อโครงการ การพัฒนาระบบความปลอดภัยของเครือข่ายในองค์กร ซึ่งข้าพเจ้าได้รับความรู้ ความเข้าใจและประสบการณ์ในการทำงานที่เป็นประโยชน์อย่างมาก อีกทั้งการดูแลและการช่วยเหลือต่าง ๆ ตลอดเวลาการทำงาน โดยการปฏิบัติงานสหกิจศึกษาในครั้งนี้สำเร็จลุล่วงได้ เพราะมีการชี้แนะและได้รับความร่วมมือจากบุคคลต่าง ๆ ดังต่อไปนี้

พนักงานแผนก Managed Service

- คุณนฤดล รุ่งวีรกุลอนันต์
- คุณทรงพล เล็กเพชร
- คุณภาคภูมิ พรประทานเวช
- คุณปรัชสิทธิ์ วงศ์วิเศษกิจ
- คุณอำพล จงทวีสุข

พนักงานแผนกทรัพยากรบุคคล

- คุณอรียา จารุภูมิ

และข้าพเจ้าขอขอบคุณอาจารย์ที่ปรึกษา ผศ.มยุรี เลิศเวชกุล ที่คอยให้คำแนะนำ คำปรึกษาและคอยรับฟังและช่วยเหลือปัญหาต่าง ๆ ในการทำโครงการครั้งนี้ และท้ายที่สุดข้าพเจ้าขอขอบคุณครอบครัวที่คอยให้กำลังใจที่ดีแก่ข้าพเจ้าเสมอมาทำให้ปริญญานิพนธ์ฉบับนี้ให้สำเร็จลุล่วงไปได้ด้วยดี

สิรวิชญ์ อมรกิตติสาร

สารบัญ

หน้า

สารบัญรูป

สารบัญตาราง

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญ

เนื่องจาก บริษัท ไดเมนชั่นดาต้า (ประเทศไทย) จำกัด ได้จัดโครงการสหกิจศึกษาระหว่างบริษัท ไดเมนชั่นดาต้า (ประเทศไทย) จำกัด กับ คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง โดยในส่วนงานของแผนกติดตั้งนั้น ได้จัดทำโครงการการศึกษาเรื่องการรักษาความปลอดภัยของระบบเครือข่ายด้วยซอฟต์แวร์โอเพนซอร์สไฟร์วอล (Open Source Firewall) จึงมอบหมายงานให้นักศึกษาทำการศึกษาหาความรู้เกี่ยวกับเทคโนโลยีของไฟร์วอล รวมถึงการออกแบบและวิธีการติดตั้ง เพื่อให้นักศึกษามีความรู้สามารถออกแบบและติดตั้งไฟร์วอลให้กับลูกค้าได้

1.2 วัตถุประสงค์ของการปฏิบัติงาน

เนื่องจากบริษัท ไดเมนชั่นดาต้า (ประเทศไทย) จำกัด เป็นบริษัทที่ให้บริการโซลูชั่นทางด้านไอทีแก่ธุรกิจต่างๆ มีความต้องการที่จะขยายขอบเขตของผลิตภัณฑ์ที่จะให้บริการแก่ลูกค้าเพื่อให้ลูกค้านั้นได้มีตัวเลือกมากยิ่งขึ้นในการใช้บริการของไดเมนชั่นดาต้าและเพื่อประสิทธิภาพของระบบเครือข่ายของลูกค้านั้น จำเป็นต้องมีการศึกษาในตัวผลิตภัณฑ์ก่อนที่จะนำไปติดตั้งหรือให้บริการกับลูกค้า

1.3 วิธีการดำเนินงาน

- ศึกษาระบบและเทคโนโลยีของอุปกรณ์ไฟร์วอลรวมถึงคุณสมบัติการทำงานต่างๆ ตามเป็นความต้องการ (Requirement)
- วิเคราะห์ ระบบเครือข่ายของลูกค้าที่จะต้องการนำ Firewall ไปติดตั้ง
- ออกแบบและแก้ไขระบบเครือข่ายเพื่อให้ได้ตรงตาม Requirement
- ทดสอบระบบ
- วิเคราะห์ปัญหาที่เกิดขึ้น
- เสนอแนะแนวทางการเพิ่มประสิทธิภาพ
- สรุปผล

1.4 ขอบเขตของงาน

- เรียนรู้การทำงานและศึกษาโครงสร้างระบบความปลอดภัยของเครือข่ายที่จะนำ Firewall ไปติดตั้ง
- วิเคราะห์เปรียบเทียบและอธิบายเหตุผลในการเลือกใช้ Firewall แต่ละยี่ห้อในการนำไปติดตั้งให้ลูกค้า
- ออกแบบและติดตั้ง Firewall
- เสนอแนะแนวทางการเพิ่มประสิทธิภาพให้กับระบบเครือข่าย

1.5 ประโยชน์ที่คาดว่าจะได้รับ

- นักศึกษาได้รับความรู้และเข้าใจในเรื่องของ Network Security และการ Design ตาม Requirement ที่ได้รับ
- บริษัทฯได้รับแนวทางในการติดตั้ง Firewall ตาม Requirement ที่ได้รับ

บทที่ 2

ทบทวนวรรณกรรม

2.1 Firewall Technology

ในอดีตนั้น Firewall อาจไม่ใช่เครื่องมือที่สำคัญในการช่วยป้องกันระบบเนื่องจากเร้าเตอร์นั้นก็สามารถทำได้โดยการใช้ Access List แต่ในปัจจุบันนั้นการที่จะบล็อคเพียงไอพีแอดเดรสของต้นทางหรือปลายทางนั้นคงไม่เพียงพอต่อความปลอดภัยในเครือข่าย จึงมีการพัฒนา Firewall ออกมา นั่นคือระบบการป้องกันเครือข่ายทั้งจากภายนอกและภายใน ถ้าแปลเป็นภาษาไทยจะหมายถึงกำแพงไฟ โดยมีหน้าที่คอยควบคุมการส่งผ่านของข้อมูลทั้งขาเข้าและขาออกรวมถึงตรวจสอบสิทธิ์ในการเข้า-ออกของเครือข่ายทั้งจากบุคคลภายนอกหรือภายในด้วยกฎเกณฑ์ที่มีการระบุไว้

2.2 Traditional Firewall

คือเครื่องมือที่มีความสามารถในการควบคุมการส่งผ่านของข้อมูลทั้งเข้า-ออกจากเครือข่ายโดยมีสองรูปแบบคือ Stateless และ Stateful การที่จะเลือกใช้สองวิธีนี้ขึ้นอยู่กับโปรโตคอลที่ใช้ในการทำงาน การทำงานแบบ Stateless นั้นจะไม่มีการมอนิเตอร์เส้นทางของแพ็คเก็ตที่ผ่านเครือข่าย กล่าวคือจะไม่มีการเก็บสถานะของแพ็คเก็ตนั้นๆไว้ จะต้องมีการตรวจสอบแพ็คเก็ตใหม่ทุกครั้งที่มีการผ่านเครือข่าย และการทำงานแบบ Stateful นั้นก็คือมีการเก็บสถานะของแพ็คเก็ตนั้นไว้นั่นคือระบบจะรับรู้ว่าแพ็คเก็ตนี้ส่งผ่านไปยังที่ไหนหรือมีการติดตามไปจนถึงปลายทางและเมื่อมีการส่งแพ็คเก็ตชนิดเดิมเข้ามาในเครือข่ายก็จะไม่จำเป็นที่จะต้องตรวจสอบอีกครั้งนั่นเอง

เห็นได้ชัดว่าไฟร์วอลที่ทำงานแบบ Stateful นั้นมีประสิทธิภาพมากกว่าแบบ Stateless และ Traditional Firewall นั้นสามารถทำงานการตรวจสอบแพ็คเก็ตได้เพียงเลเยอร์ 2 ถึงเลเยอร์ 4 เท่านั้น

2.3 Next Generation Firewall

คือ ไฟร์วอลที่ได้มีการพัฒนามาจาก Traditional Firewall โดยมีการเพิ่มคุณสมบัติ (feature) ต่างๆ เข้าไปเพื่อให้สามารถทำงานได้อย่างมีประสิทธิภาพมากยิ่งขึ้นยกตัวอย่างเช่น

- Application Awareness
- Stateful Inspection

- Integrated Intrusion Protection System (IPS)
- Identity Awareness (การระบุตัวตนในการเข้าใช้งาน)
- Bridged and Routed Modes
- ความสามารถในการตรวจสอบความผิดปกติจากภายนอก

2.3.1 Application Awareness

สิ่งที่แตกต่างที่สุดระหว่าง traditional firewall กับ NGFW นั่นคือ NGFW สามารถตรวจสอบได้ถึงเลเยอร์ 7 หรือ แอพพลิเคชั่นเลเยอร์โดยที่ traditional firewall นั้นสามารถระบุได้มากสุดเพียงแค่พอร์ตที่ใช้ในการเชื่อมต่อหรือได้เพียงในชั้น Transport Layer ยกตัวอย่างที่เห็นได้ชัดนั่นก็คือในกรณีของ HTTP ที่ใช้พอร์ต 80 ในการเชื่อมต่อ ในปัจจุบันไม่ได้มีการกำหนดว่ามีเพียงแค่ HTTP เท่านั้นที่สามารถใช้พอร์ต 80 ได้นั่นหมายความว่าแอพพลิเคชั่นต่างๆ ก็สามารถใช้พอร์ตนี้ได้เช่นกัน ถ้าเป็นในมุมมองของ traditional firewall จะไม่สามารถรับรู้ได้ว่าเป็น Application ใดก็จะปล่อยผ่านไปเพราะคิดว่าเป็น HTTP นั่นเอง ข้อบกพร่องนี้จะเป็นจุดที่สามารถทำให้ระบบเครือข่ายเกิดความเสี่ยงได้

2.3.2 Identity Awareness

อีกหนึ่งความแตกต่างที่สำคัญนั่นก็คือการระบุตัวตนในการเข้างานของผู้ใช้งาน ใน traditional firewall นั้นอาจต้องมีการระบุตัวตนของผู้ใช้งานผ่านหมายเลขไอพีแอดเดรสแต่ใน NGFW นั้นสามารถระบุได้ผ่านระบบยืนยันตัวขององค์กรที่มีมาก่อนอยู่แล้วยกตัวอย่างเช่น Active Directory หรือ LDAP วิธีการนี้จะไม่เพียงสามารถควบคุมได้แค่ทราฟฟิกที่ผ่านเครือข่ายยังสามารถควบคุมได้ถึงการอนุญาตผู้ใช้งานในการเข้าถึงและสามารถจำกัดสิทธิ์ในการรับหรือส่งข้อมูลนอกเครือข่ายได้ด้วย

2.3.3 Stateful Inspection

ในฟีเจอร์ส่วนนี้จะไม่มีความแตกต่างมากนักจาก traditional firewall ซึ่งจากที่สามารถติดตามได้เพียง Layer 2 – Layer 4 นั้นก็จะสามารถติดตามได้ถึง Layer 7 นั่นเองและยังอนุญาตให้สามารถควบคุมและกำหนดข้อบังคับการใช้งานได้มากยิ่งขึ้น

2.3.4 Integrated IPS

Intrusion Prevention System (IPS) นั้นมีหน้าที่ในการตรวจจับหาการโจมตีที่อาจเกิดขึ้นได้ในเครือข่ายซึ่งมีหลายรูปแบบด้วยกันยกตัวอย่างเช่น ตรวจจับจากลายเซ็นต์ดิจิตอล, รูปแบบการโจมตีที่เกิดขึ้นบ่อย, พฤติกรรมที่ผิดปกติของแพ็คเก็ตและทำการวิเคราะห์รูปแบบพฤติกรรมของแพ็คเก็ตที่มีการรับ-ส่งระหว่างเครือข่าย

ในสภาพแวดล้อมที่มีการติดตั้ง traditional firewall นั้นส่วนมากจะมีการใช้งาน Intrusion Detection System (IDS) หรือ IPS โดยทั้งสองส่วนนี้มีการทำงานที่แตกต่างกันและส่วนมากมักจะถูกติดตั้งแยกกันเปรียบเสมือนเป็นคนละเครื่องมือ แต่ใน NGFW นั้นทั้ง IDS และ IPS จะถูกรวมกันอย่างสมบูรณ์ ในส่วนของการทำงานนั้น IPS จะทำงานได้สมบูรณ์ปกติแต่ที่แตกต่างเพิ่มขึ้นมานั่นก็คือประสิทธิภาพในการทำงานและการเข้าถึงข้อมูลจากทุกๆ เลเยอร์ของทราฟฟิก

2.3.5 Bridged and Routed Modes

ฟีเจอร์นี้ไม่ได้เป็นฟีเจอร์ที่ใหม่มากนัก แต่ถือเป็นฟีเจอร์ที่มีความสำคัญหรือจำเป็นอย่างมากในการใช้งาน เนื่องจากในปัจจุบันนี้ในองค์กรหลายๆองค์กรส่วนมากนั้นยังคงมีการใช้ traditional firewall อยู่นั่นเอง เมื่อมีการติดตั้ง NGFW จึงจำเป็นต้องมีการทำ Bridged mode หรือทำให้เป็น transparent นั่นเอง NGFW จะไม่แสดงเส้นทาง routed จะมีหน้าที่แค่ส่งต่อแพ็คเก็ตเท่านั้นจะไม่ได้ข้องเกี่ยวกับตารางเส้นทาง เมื่อองค์กรใดๆนั้นต้องการที่จะนำ traditional firewall ออกและทดแทนด้วย NGFW นั้นก็จะมีการปรับจาก Bridged mode เป็น Routed mode นั่นเอง

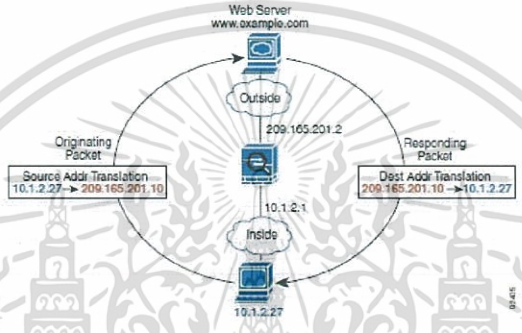
2.4 รูปแบบการติดตั้ง Firewall

ในการออกแบบหรือการวางตำแหน่งของ firewall ในเครือข่ายนั้นสามารถแบ่งออกเป็น 2 รูปแบบนั่นคือ Transparent mode และ Routed mode

2.4.1 Routed mode

ในรูปแบบของการติดตั้ง firewall ใน Routed mode นั้น ตัวอุปกรณ์เองจะถูกมองเห็นเป็นเร้าเตอร์ฮอปหนึ่งของเครือข่าย ซึ่งสามารถให้บริการการทำ NAT ระหว่างเครือข่ายได้และยังสามารถใช้โปรโตคอลค้นหาเส้นทางเช่น OSPF หรือ RIP ในโหมดนี้ยังรองรับการทำงานหลายอินเตอร์เฟสโดยแต่ละอินเตอร์เฟสจำเป็นที่จะต้องอยู่กันคนละซับเนตด้วย

- **IP Routing Support** หมายถึง firewall สามารถทำงานเป็นเร้าเตอร์ได้ด้วยและเป็นตัวกลางเชื่อมระหว่างระบบเครือข่ายต่างๆเข้าด้วยกัน รวมถึงยังรองรับโปรโตคอลค้นหาเส้นทางทั้ง OSPF และ RIP ใน single context mode และรองรับ static routes ในการทำงานแบบ multiple context mode
- **Network Address Translation (NAT)** หมายถึงการแปลงเลขไอพีแอดเดรสจาก local ไปเป็น global ที่สามารถใช้ในการค้นหาเส้นทางไปยังปลายทางที่อยู่กันคนละเน็ตเวิร์คได้ โดยทั่วไปแล้ว NAT นั้นไม่ได้ถูกกำหนดว่าจะต้องมีการใช้งานบน firewall



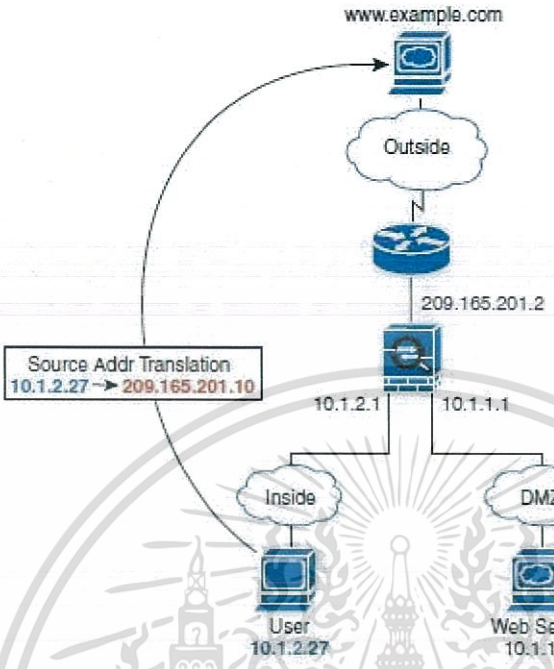
รูปที่ 2. 1 การทำ NAT

การทำงานของ Firewall ใน Routed mode

ในหัวข้อนี้สามารถแบ่งย่อยออกได้เป็นกรณีย่อยๆได้ดังนี้

1. ผู้ใช้งานภายในต้องการที่จะใช้งานเว็บเซิร์ฟเวอร์ภายนอก
2. ผู้ใช้งานภายนอกต้องการที่จะใช้งานเว็บเซิร์ฟเวอร์ใน DMZ
3. ผู้ใช้งานภายในต้องการที่จะใช้งานเว็บเซิร์ฟเวอร์ใน DMZ
4. โปรโตคอลค้นหาเส้นทางใช้งานภายนอกต้องการที่จะติดต่อกับผู้ใช้งานภายใน
5. ผู้ใช้งานที่ DMZ ต้องการที่จะติดต่อกับโปรโตคอลค้นหาเส้นทางใช้งานภายใน

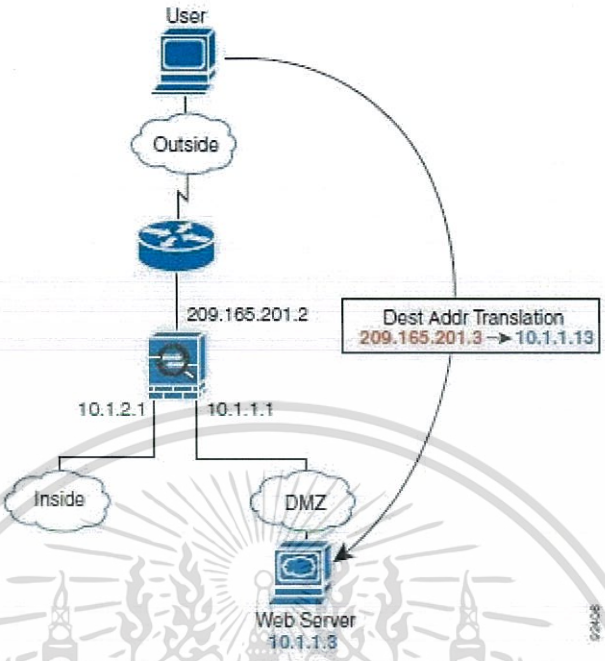
ผู้ใช้งานภายในต้องการที่จะใช้งานเว็บเซิร์ฟเวอร์ภายนอก



รูปที่ 2. 2 Inside to Outside

1. ผู้ใช้งานที่อยู่ภายในเน็ตเวิร์กต้องทำการร้องขอเว็บเพจจาก www.example.com
2. ไฟร์วอลจะได้รับแพ็คเก็ตเนื่องจากเป็นการเปิดเซสชั่นการทำงานใหม่และจะทำการตรวจสอบแพ็คเกตโดยอ้างอิงจากข้อกำหนดที่ได้ระบุไว้ (Access lists, Filters, AAA)
3. ไฟร์วอลจะทำหน้าที่ในการแปลงหมายเลขไอพีจาก 10.1.2.27 เป็น 209.165.201.10
4. ไฟร์วอลจะเก็บข้อมูลของเซสชั่นที่ได้ทำการเปิดไว้และส่งแพ็คเกตออกไปยังอินเตอร์เฟสที่เชื่อมต่อกับเน็ตเวิร์กภายนอก
5. เมื่อ www.example.com ได้ตอบรับการร้องขอจากผู้ใช้ แพ็คเกตจะวิ่งกลับโดยผ่านไฟร์วอลและเนื่องจากมีการเชื่อมต่ออยู่แล้วเพราะไฟร์วอลได้เก็บข้อมูลไว้ แพ็คเกตจะข้ามขั้นตอนในการตรวจสอบต่างๆออกไปและแปลงเลขไอพีที่เป็น global กลับเป็น local 10.1.2.27
6. ไฟร์วอลจะส่งแพ็คเกตออกไปยังอินเตอร์เฟสที่เชื่อมต่อกับผู้ใช้งานภายใน

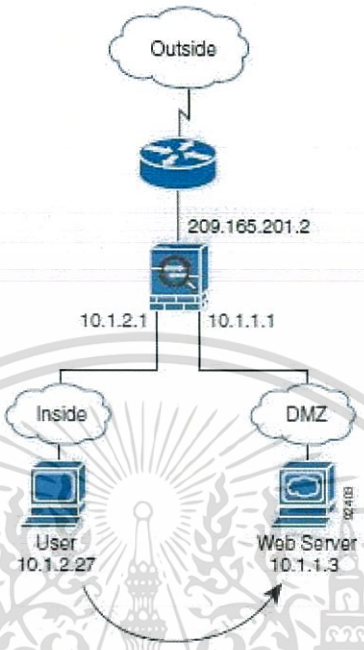
โปรโตคอลค้นหาเส้นทางใช้งานภายนอกต้องการที่จะใช้งานเว็บเซิร์ฟเวอร์ใน DMZ



รูปที่ 2. 3 Outside to DMZ

1. โปรโตคอลค้นหาเส้นทางใช้งานที่อยู่ภายนอกจะทำการร้องขอหน้าเว็บเพจจากเว็บเซิร์ฟเวอร์ที่ตั้งอยู่ใน DMZ โดยใช้เลขหมายไอพีที่ร้องขอเป็น global address 209.165.201.3 ซึ่งเป็นไอพีแอดเดรสของขาอินเตอร์เฟสที่อยู่ภายนอก
2. ไฟร์วอลจะทำการตรวจสอบแพ็คเกตที่วิ่งเข้ามาเนื่องจากเป็นเซสชั่นที่เพิ่งมีการเปิดใหม่ โดยจะทำการตรวจสอบตามข้อกำหนดต่างๆ (Access lists, Filter, AAA)
3. ถ้าหากผ่านการตรวจสอบทั้งหมดแล้วจะทำการแปลงหมายเลขไอพีแอดเดรสให้เป็น local address 10.1.1.13
4. ไฟร์วอลจะทำการเก็บบันทึกเซสชั่นนี้ไว้และทำการส่งต่อแพ็คเกตออกไปยังอินเตอร์เฟสที่เชื่อมต่อกับเว็บเซิร์ฟเวอร์
5. เมื่อเว็บเซิร์ฟเวอร์ทำการตอบกลับการร้องขอจากผู้ใช้งาน แพ็คเกตจะวิ่งกลับออกมาทางเดิมซึ่งจะต้องผ่านไฟร์วอล แต่เนื่องจากไฟร์วอลมีการเก็บเซสชั่นการทำงานไว้จึงจำได้ว่าเป็นแพ็คเกตที่มีการตรวจสอบไปแล้วก็จะทำการส่งต่อไปยังขาอินเตอร์เฟสที่เชื่อมต่อกับเน็ตเวิร์กภายนอกต่อไปและแปลงหมายเลขไอพีแอดเดรสเป็น global 209.165.201.3
6. ไฟร์วอลจะส่งต่อออกไปยังขาอินเตอร์เฟสที่เชื่อมต่อไปยังเน็ตเวิร์กของผู้ใช้งานภายนอก

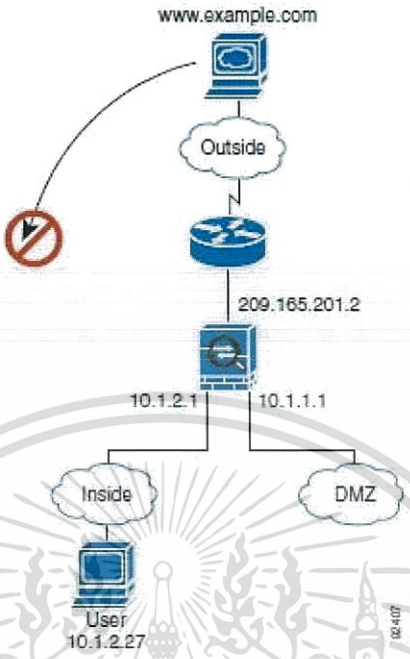
ผู้ใช้งานภายในต้องการที่จะใช้งานเว็บเซิร์ฟเวอร์ใน DMZ



รูปที่ 2. 4 Inside to DMZ

1. ผู้ใช้งานภายในร้องขอเว็บเพจจากเซิร์ฟเวอร์ในDMZโดยใช้หมายเลขไอพีแอดเดรสเป็นlocal 10.1.1.3
2. ไฟร์วอลจะทำการตรวจสอบแพ็คเกตที่วิ่งเข้ามาเนื่องจากเป็นเซสชั่นที่เพิ่งมีการเปิดใหม่ โดยจะทำการตรวจสอบตามข้อกำหนดต่างๆ (Access lists, Filter, AAA)
3. ไฟร์วอลจะทำการเก็บบันทึกเซสชั่นที่ได้ทำการเชื่อมต่อไว้และส่งแพ็คเกตออกไปยอินเตอร์เฟสที่เชื่อมต่อกับ DMZ
4. เมื่อเว็บเซิร์ฟเวอร์ทำการตอบกลับการร้องขอจากผู้ใช้งานแพ็คเกตจะวิ่งกลับออกมาทางเดิมซึ่งจะต้องผ่านไฟร์วอลแต่เนื่องจากไฟร์วอลมีการเก็บเซสชั่นการทำงานไว้จึงจำได้ว่าเป็นแพ็คเกตที่มีการตรวจสอบไปแล้วจึงข้ามขั้นตอนนี้ไป
5. ไฟร์วอลส่งแพ็คเกตกลับไปยังโปรโตคอลค้นหาเส้นทางใช้งานภายใน

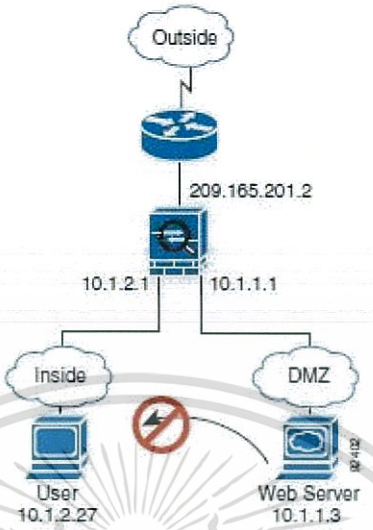
โปรโตคอลค้นหาเส้นทางใช้งานภายนอกต้องการที่จะติดต่อกับผู้ใช้งานภายใน



รูปที่ 2. 5 Outside to Inside

1. โปรโตคอลค้นหาเส้นทางใช้งานภายนอกต้องการที่จะเข้าถึงผู้ใช้งานภายใน (สมมติว่าโปรโตคอลค้นหาเส้นทางใช้งานภายในมีไอพีเป็นของตัวเอง) ถ้าเน็ตเวิร์กภายในเป็นไพรเวท จะไม่มีโปรโตคอลค้นหาเส้นทางใช้งานภายนอกใดๆสามารถเข้าถึงได้นอกจากจะมีการทำ NAT ก่อน
2. ไฟร์วอลจะทำการตรวจสอบแพ็คเกตที่เข้ามาเนื่องจากเป็นเซสชั่นใหม่โดยจะตรวจสอบจากข้อกำหนดต่างๆ
3. แพ็คเกตจะถูกดรอปทิ้งไปเนื่องจากไม่อนุญาตให้เข้าถึงผู้ใช้งานภายในได้และไฟร์วอลจะทำการเก็บข้อมูลของเซสชั่นนี้ไว้ ถ้าหากมีการพยายามที่จะโจมตีเน็ตเวิร์กภายในอีกไฟร์วอลจะมีมาตรการในการจัดการกับคอนเนคชั่นที่จะเกิดขึ้นได้อาจเป็นการบล็อคไอพีนั้นๆที่พยายามโจมตีเข้ามา

ผู้ใช้งานที่ DMZ ต้องการที่จะติดต่อกับโปรโตคอลค้นหาเส้นทางใช้งานภายใน



รูปที่ 2. 6 DMZ to Inside

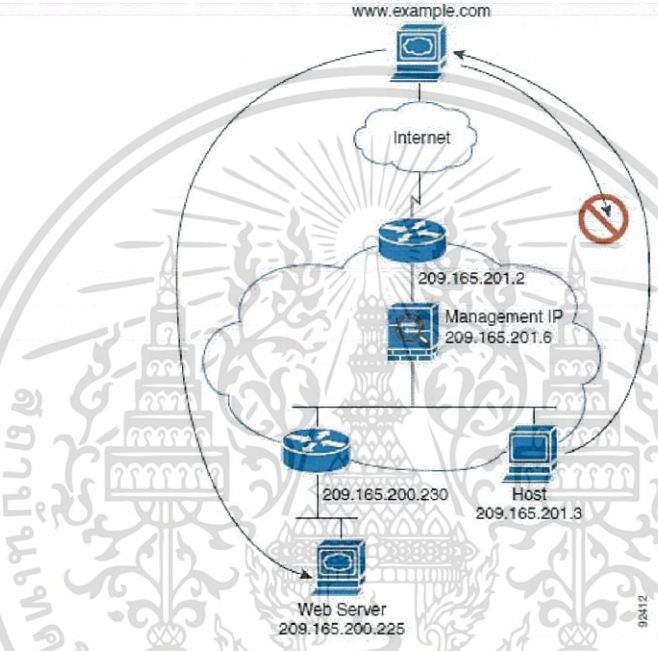
1. โปรโตคอลค้นหาเส้นทางใช้งานที่ DMZ พยายามที่จะติดต่อกับเน็ตเวิร์คของผู้ใช้ภายใน เนื่องจาก DMZ นั้นไม่มีความจำเป็นที่จะส่งทราฟฟิคหรือข้อมูลออกสู่อินเทอร์เน็ต ดังนั้นหมายเลขไอพีแอดเดรสที่เป็นไพรเวทสามารถส่งข้ามระบบเครือข่ายย่อยได้เช่นกัน
2. ไฟร์วอลจะทำการตรวจสอบแพ็คเกตที่เข้ามาเนื่องจากเป็นเซสชั่นใหม่โดยจะตรวจสอบจากข้อกำหนดต่างๆ
3. แพ็คเกตจะถูกดรอปทิ้งไปเนื่องจากไม่อนุญาตให้เข้าถึงผู้ใช้งานภายในได้และไฟร์วอลจะทำการเก็บข้อมูลของการพยายามเชื่อมต่อไว้

2.4.2 Transparent mode

โดยทั่วไปแล้ว Firewall จะมีหน้าที่เปรียบเสมือนกับเร้าเตอร์ กล่าวคืออาจทำหน้าที่เป็น default gateway สำหรับโฮสที่อยู่ในซับเนตเดียวกัน แต่ในโหมด transparent นั้นจะกลายเป็น Layer 2 Firewall และทำหน้าที่เป็นเหมือน Stealth firewall เหมือนกับการล่องหนหรือโฮสต์ไม่รู้ว่ามีไฟร์วอลอยู่บนเครือข่ายนั่นเองและไม่จะถูกมองว่าเป็นเร้าเตอร์ตัวที่เชื่อมต่อกับอุปกรณ์ต่างๆหรือโฮสต์นั่นเอง ในการใช้โหมด transparent ในการทำงานของไฟร์วอลนั้นไม่มีความจำเป็นที่จะต้องมีการ NAT เนื่องจากไม่ได้เป็น routed hop จึงสามารถนำไปเพิ่มในองค์กรได้อย่างง่ายโดยไม่ต้องมีการเปลี่ยนแปลงระบบภายในมากนัก

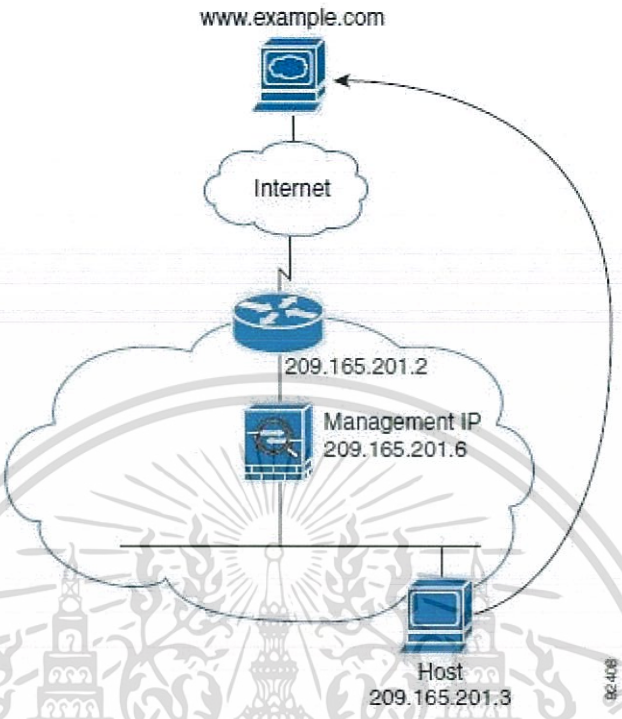
การทำงานของ Firewall ใน Transparent mode

1. โปรโตคอลค้นหาเส้นทางใช้งานภายในต้องการที่จะใช้งานเว็บเซิร์ฟเวอร์ภายนอก
2. โปรโตคอลค้นหาเส้นทางใช้งานภายนอกต้องการที่จะใช้งานเว็บเซิร์ฟเวอร์ภายใน
3. โปรโตคอลค้นหาเส้นทางใช้งานภายนอกพยายามที่จะเชื่อมต่อกับโปรโตคอลค้นหาเส้นทางใช้งานภายใน



รูปที่ 2. 7 การทำงานทั่วไปของโหมด Transparent

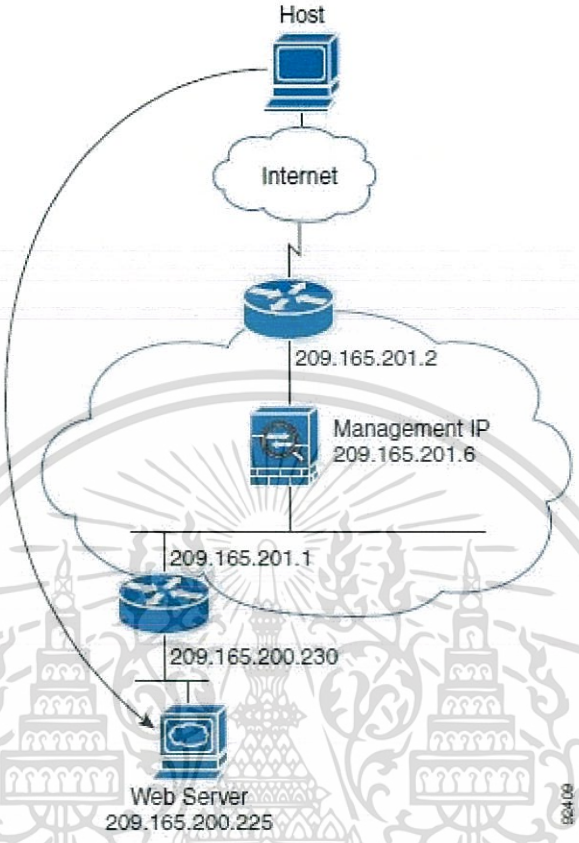
โปรโตคอลค้นหาเส้นทางใช้งานภายในต้องการที่จะใช้งานเว็บเซิร์ฟเวอร์ภายนอก



รูปที่ 2. 8 Inside to Outside

1. โปรโตคอลค้นหาเส้นทางใช้งานภายในร้องขอเว็บเพจจาก ww.example.com
2. ไฟร์วอลจะได้รับแพ็คเกตและเพิ่ม MAC address ของต้นทางไปยังตาราง MAC address เนื่องจากเป็นเซสชั่นใหม่จะต้องมีการตรวจสอบตามข้อกำหนดที่ได้ตั้งไว้ (Access lists, filters, AAA)
3. ไฟร์วอลจะทำการเก็บบันทึกเซสชั่นนี้ไว้
4. ถ้าหาก MAC address ปลายทางนั้นมีอยู่ในตาราง MAC address ไฟร์วอลจะทำการส่งต่อไปยังอินเตอร์เฟสนั้นๆที่ได้ระบุไว้ในตาราง ถ้าหากไม่มีอยู่ในตารางไฟร์วอลจะทำการดรอปแพ็คเกตนั้นทิ้งไป
5. เว็บเซิร์ฟเวอร์จะตอบกลับการร้องขอและเนื่องจากไฟร์วอลได้ทำการเปิดเซสชั่นไว้อยู่แล้วนั้น แพ็คเกตจะข้ามขั้นตอนในการตรวจสอบออกไป
6. ไฟร์วอลจะส่งต่อแพ็คเกตไปยังโปรโตคอลค้นหาเส้นทางใช้งานตามอินเตอร์เฟสที่เหมาะสม

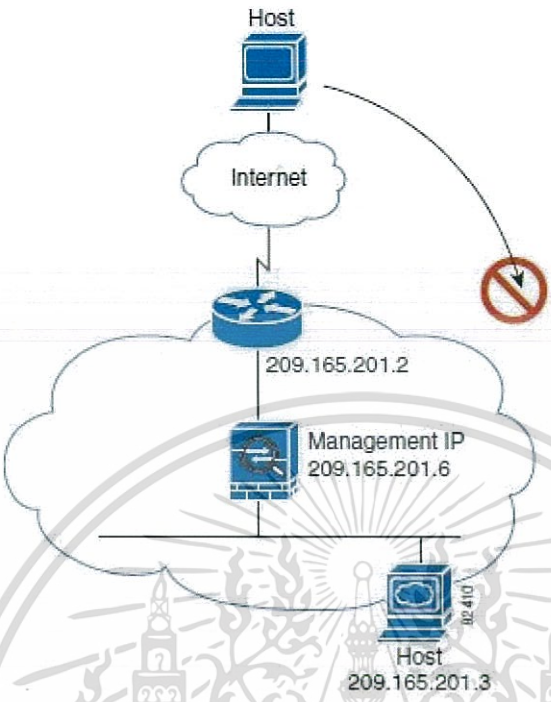
โปรโตคอลค้นหาเส้นทางใช้งานภายนอกต้องการที่จะใช้งานเว็บเซิร์ฟเวอร์ภายใน



รูปที่ 2.9 Outside to Inside

1. โปรโตคอลค้นหาเส้นทางใช้งานภายนอกร้องขอเว็บเพจจากเว็บเซิร์ฟเวอร์ที่อยู่ภายใน
2. ไฟร์วอลจะได้รับแพ็คเกตและเพิ่ม MAC address ของต้นทางไปยังตาราง MAC address เนื่องจากเป็นเซสชั่นใหม่จะต้องมีการตรวจสอบตามข้อกำหนดที่ได้ตั้งไว้ (Access lists, filters, AAA)
3. ไฟร์วอลจะทำการเก็บบันทึกเซสชั่นนี้ไว้
4. ถ้าหาก MAC address ปลายทางนั้นมีอยู่ในตาราง MAC address ไฟร์วอลจะทำการส่งต่อไปยังอินเตอร์เฟสนั้นๆที่ได้ระบุไว้ในตาราง ถ้าหากไม่มีอยู่ในตารางไฟร์วอลจะทำ ARP Request และ Ping เพื่อค้นหา
5. เว็บเซิร์ฟเวอร์จะตอบกลับการร้องขอและเนื่องจากไฟร์วอลได้ทำการเปิดเซสชั่นไว้อยู่แล้วนั้น แพ็คเกตจะข้ามขั้นตอนในการตรวจสอบออกไป
6. ไฟร์วอลจะส่งต่อแพ็คเกตไปยังโปรโตคอลค้นหาเส้นทางใช้งานตามอินเตอร์เฟสที่เหมาะสม

โปรโตคอลค้นหาเส้นทางใช้งานภายนอกพยามที่จะเชื่อมต่อกับโปรโตคอลค้นหาเส้นทางใช้งานภายใน



รูปที่ 2. 9 Outside to Inside hosts

1. โปรโตคอลค้นหาเส้นทางใช้งานภายนอกพยายามที่จะเชื่อมต่อกับโปรโตคอลค้นหาเส้นทางใช้ภายใน
2. ไฟร์วอลจะได้รับแพ็คเกตและเพิ่ม MAC address ของต้นทางไปยังตาราง MAC address เนื่องจากเป็นเซสชั่นใหม่จะต้องมีการตรวจสอบตามข้อกำหนดที่ได้ตั้งไว้ (Access lists, filters, AAA)
3. ไฟร์วอลจะทำการดรอปแพ็คเกตทิ้งไป
4. ถ้าหากโปรโตคอลค้นหาเส้นทางใช้ภายนอกพยายามที่จะเข้าถึงหรือโจมตีเน็ตเวิร์กภายในอีก ไฟร์วอลจะมีฟีเจอร์ที่ใช้ในการป้องกันไม่ให้เกิดขึ้น

2.5 รู้จักกับ Failover

การใช้งาน failover นั้นมีความจำเป็นที่ต้องมีไฟร์วอลอย่างน้อย 2 ตัวและเชื่อมต่อซึ่งกันและกันโดยผ่านลิ้งค์ failover หรือลิ้งค์ failover ที่เป็น stateful จะมีการคอยมอนิเตอร์อินเตอร์เฟสที่ active เพื่อคอยตรวจสอบว่าตรงกับเงื่อนไข failover หรือไม่ ถ้าหากสถานะนั้นตรงกับเงื่อนไขแล้วนั้น จะเกิดการทำ failover ขึ้นนั่นเอง

ไฟร์วอลนั้นสนับสนุนการทำงานของ failover ด้วยกันสองรูปแบบนั่นคือ Active/Active failover และ Active/Stand-by failover แต่ละรูปแบบก็จะมีการคอนฟิกและรูปแบบการทำงานที่แตกต่างกันออกไป

ในแบบ Active/Active failover นั้นทราฟฟิคสามารถทำงานหรือวิ่งผ่านได้ทั้งสองเน็ตเวิร์คหรือกล่าวคือทราฟฟิคจากภายนอกสามารถวิ่งผ่านไฟร์วอลได้ทั้งสองตัว สิ่งนี้ทำให้เกิดการทำ Load balancing ซึ่งจะพูดถึงในหัวข้อถัดๆไป

ในแบบ Active/Stand-by failover นั้นทราฟฟิคจะสามารถวิ่งผ่านไฟร์วอลได้เพียงตัวเดียวที่ตั้งค่าเป็น Active ไว้ส่วนอีกตัวหนึ่งนั้นจะถูกกำหนดให้ Stand-by รอ ถ้าหากไฟร์วอลตัวแรกนั้นเกิดดาวน์ลงไปไฟร์วอลอีกตัวจะขึ้นมาทำหน้าที่แทนนั้นเอง

2.5.1 Failover Link

ไฟร์วอลทั้งสองตัวที่จับคู่กับทำ failover นั้นจะต้องมีการติดต่อสื่อสารกันผ่าน failover link เพื่อแลกเปลี่ยนสถานะการทำงานของกันโดยจะมีการแลกเปลี่ยนข้อมูลกันดังต่อไปนี้

- สถานะของการทำงาน (Active or Stand-by)
- Power status
- Hello messages (keep-alive)
- สถานะของลิ้งค์เน็ตเวิร์ก
- MAC address
- การตั้งค่าและความสัมพันธ์ของข้อมูลภายในอุปกรณ์

2.5.2 LAN-Based Failover Link

ในการเชื่อมต่อระหว่างอินเตอร์เฟสของไฟร์วอลทั้งสองตัวนั้นสามารถใช้อีเธอร์เนตอินเตอร์เฟสเท่วไปในการเชื่อมต่อกันได้ อย่างไรก็ตามการคอนฟิก failover link อินเตอร์เฟสนั้นจะไม่คอนฟิกเหมือนอินเตอร์เฟสที่เชื่อมต่อกับเน็ตเวิร์กทั่วไป ลิ้งค์นี้จะใช้สำหรับสื่อสารของ failover เท่านั้น สามารถทำได้สองวิธีนั่นคือ

1. ใช้สวิตซ์เป็นตัวกลางโดยจะไม่ต้องไม่มีอุปกรณ์อื่นๆอยู่ในวงของเน็ตเวิร์กเดียวกัน (บรอดแคสโดเมนเดียวกันหรือ VLAN เดียวกัน)
2. ใช้สาย Crossover ในการเชื่อมต่อโดยตรงระหว่างไฟร์วอลทั้งสองตัวโดยไม่มีสวิตซ์เป็นตัวกลางในการเชื่อมต่อกันนน

2.5.3 สาเหตุที่ส่งผลให้เกิด Failover

อุปกรณ์สามารถทำงานผิดพลาดได้หากเกิดกรณีใดกรณีหนึ่งดังนี้

- ฮาร์ดแวร์นั้นเกิดความผิดพลาดหรือหน่วยจ่ายไฟทำงานล้มเหลว
- ซอฟท์แวร์นั้นเกิดความผิดพลาด
- อินเตอร์เฟสที่ใช้ในการมอนิเตอร์ทำงานผิดพลาด
- มีการใช้คำสั่ง no failover active ที่อุปกรณ์ที่อยู่ในสถานะ active หรือใช้คำสั่ง failover active ที่อุปกรณ์ที่อยู่ในสถานะ Stand-by

2.5.4 Regular Failover

เมื่อเกิด Failover ขึ้นทุกๆการเชื่อมต่อจะถูกปิดลงไป และไคลเอนต์จำเป็นต้องทำการเชื่อมต่อใหม่เมื่อมีสถานะของอุปกรณ์ตัวใดๆเป็น active ขึ้นมา

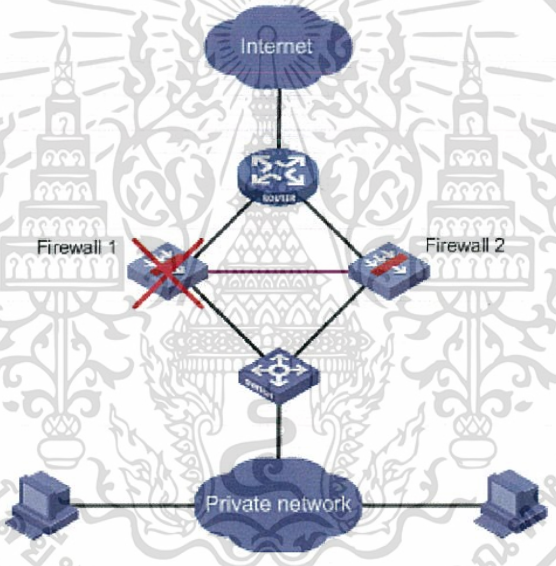
2.5.5 Stateful Failover

เมื่อใดก็ตามที่มีการเปิดใช้งาน Stateful Failover อุปกรณ์ที่เป็น Active จะทำการส่งข้อมูลของแต่ละการเชื่อมต่อไปยังอุปกรณ์ที่ Stand-by และหลังจากเกิด failover ขึ้นสถานะหรือข้อมูลของแต่ละการเชื่อมต่อจะพร้อมใช้งานที่อุปกรณ์ที่ Stand-by อยู่ โดยจะมีการส่งข้อมูลของการเชื่อมต่อดังต่อไปนี้

- NAT Translation table
- TCP connection states

- UDP connection states
- ARP table
- HTTP connection states
- ISAKMP และ IPSec SA table

  และจะไม่ทำการแลกเปลี่ยนข้อมูลต่อไปนี้กับอุปกรณ์ที่ Stand-by
- User Authentication table
- Routing table
- DHCP server address lease
- L2TP over IPSec sessions



รูปที่ 2. 10 ตัวอย่างการทำ Failover

2.6 รู้จักกับ AAA (triple A)

AAA ทำให้ไฟร์วอลสามารถระบุได้ว่ายูสเซอร์ที่เข้ามาใช้งานนั้นเป็นใคร (Authentication), ยูสเซอร์นั้นสามารถทำอะไรหรือเข้าถึงข้อมูลได้มากแค่ไหน (Authorization) และยูสเซอร์นั้นทำอะไรไปบ้างในการเข้ามาใช้งานเครือข่าย (Accounting)

AAA ให้บริการในการเพิ่มมาตรการความปลอดภัยของเครือข่ายและควบคุมการเข้าถึงข้อมูลหรือเซิร์ฟเวอร์ของยูสเซอร์แทนที่จะใช้แค่เพียง Access lists อย่างเดียว ยกตัวอย่างเช่น สามารถสร้าง access list เพื่ออนุญาตให้โปรโตคอลค้นหาเส้นทางใช้งานภายนอกนั้นสามาถ Telnet

มายังเซิร์ฟเวอร์ที่อยู่ในโซน DMZ ได้นแต่ถ้าต้องการแค่เพียงบางยูสเซอร์เท่านั้นที่จะสามารถใช้งาน Telnet มายัง DMZ ได้ก็จำเป็นที่จะต้องมีการใช้งาน AAA Server เพื่อที่จะระบุตัวตนของยูสเซอร์นั้นๆเนื่องจากการระบุเป็นเลขไอพีแอดเดรสโดยตรงอาจทำได้ยากเพราะมีการเปลี่ยนแปลงตลอดเวลาหรือเปลี่ยนแปลงเป็นระยะๆนั่นเอง

2.6.1 Authentication

การทำ Authentication หรือในภาษาไทยคือการยืนยันตัวตนนั้นจะควบคุมการเข้าถึงต่างๆโดยจะต้องมีการยืนยันโดยทั่วไปแล้วนั้นจะเป็น username และ password โดยสามารถให้เซอร์วิสดังต่อไปนี้มีการยืนยันตัวตนก่อนที่จะเข้าใช้งานได้เช่น Telnet , SSH , Serial console , VPN และ Network access

2.6.2 Authorization

Authorization หรือการระบุสิทธิ์ในการเข้าถึงจะเป็นการควบคุมแต่ละยูสเซอร์หลังจากได้ทำการยืนยันตัวตนแล้ว ทุกๆยูสเซอร์อาจมีสิทธิ์ในการเข้าใช้งานเน็ตเวิร์กเหมือนกันแต่สิทธิ์ในการเข้าถึงอาจไม่เท่ากันยกตัวอย่างเช่น ผู้ดูแลระบบเครือข่ายอาจมีสิทธิ์ในการปรับหรือหรือแก้ไขการตั้งค่าต่างๆของเครือข่ายแต่ยูสเซอร์ทั่วไปนั้นมีสิทธิ์แค่เข้าใช้งานเท่านั้นเป็นต้น

2.6.3 Accounting

เป็นการติดตามทราฟฟิกที่ผ่านตัวอุปกรณ์นั้นๆเช่นไฟร์วอลหรือเปรียบเสมือนการเก็บ log ของแต่ละยูสเซอร์ จำเป็นต้องมีการยืนยันตัวตนก่อนถึงจะสามารถเก็บทราฟฟิกที่ยูสเซอร์ใช้งานได้ เนื่องจากอาจเป็นการเก็บข้อมูลตามไอพีแอดเดรส จะเก็บข้อมูลเกี่ยวกับเซสชั่นที่มีการเปิดใช้งาน เซอร์วิสที่ใช้บริการ ระยะเวลาการใช้งานและปริมาณข้อมูลที่ใช้งาน

2.7 รู้จักกับ Virtual Machine

Virtual Machine คือระบบปฏิบัติการที่จะจำลองการทำงานของเครื่องคอมพิวเตอร์หรือซอฟท์แวร์ต่างๆลงบนเครื่องคอมพิวเตอร์อีกทีหนึ่ง เปรียบกับว่าเราสามารถแบ่งทรัพยากรของเครื่องคอมพิวเตอร์ 1 เครื่องออกเป็นหลายๆเครื่องได้นั่นเอง ประโยชน์จากการจำลองแบบนี้นั่นก็คือเราจะสามารถประหยัดงบประมาณหรือใช้ทรัพยากรของคอมพิวเตอร์ได้อย่างคุ้มค่าและสะดวกต่อการทดลองทางคอมพิวเตอร์ต่างๆ ยกตัวอย่างเช่น ต้องการที่จะจำลองระบบเครือข่ายขึ้นมา 1 ระบบ เมื่อใช้งาน Virtual Machine ก็ไม่มีความจำเป็นที่จะต้องใช้จำนวนคอมพิวเตอร์ตาม

จำนวนของอุปกรณ์หรือระบบนั้นๆ อาจใช้เพียง 1 เครื่องและทำการแบ่งทรัพยากรออกเป็นหลายๆ ส่วนเพื่อให้เพียงพอต่อทุกๆระบบปฏิบัติการนั่นเอง

รูปที่ 2. 11 ตัวอย่างหลักการทำงานของ Virtual Machine

2.8 รู้จักกับ QoS (Quality of Service)

ในระบบเครือข่ายสมัยใหม่นั้นได้มีการรวมเทคโนโลยีต่างๆเข้าไว้ด้วยกันรวมถึงมีการพัฒนาระบบโทรศัพท์จากอนาล็อคเป็นดิจิตอลโดยมีการสื่อสารผ่านไอพีแอดเดรส ซึ่งถือเป็นจุดสำคัญในการออกแบบระบบเครือข่าย เนื่องจากจำเป็นจะต้องมีการจัดลำดับความสำคัญของแพ็คเกตที่ทำงานอยู่บนระบบเครือข่าย ซึ่งแต่ละเซอร์วิสก็จะมีความสำคัญมากน้อยแตกต่างกันออกไป ในบางเซอร์วิสต้องการให้มีการการันตีในการส่งข้อมูล มีการควบคุมปริมาณแบนวิทธ์และอัตราที่แพ็คเกตนั้นสูญหายไม่ควรจะต่ำมากเกินไปเพราะจะส่งผลกระทบต่อประสิทธิภาพของเซอร์วิสนั้นๆ ยกตัวอย่างเช่นระบบโทรศัพท์ไอพีที่เป็นการสื่อสารแบบเรียลไทม์ มีความจำเป็นที่จะต้องมีการการันตีว่าจะไม่เกิดการสูญหายของแพ็คเกตมาเกินไปและเรื่องของความล่าช้าที่อาจเกิดขึ้นได้ ก็จะส่งผลให้การสื่อสารของทั้งสองฝั่งนั้นเกิดความผิดพลาดได้เช่นกัน

ปัจจัยสำคัญที่จะส่งผลกระทบต่อประสิทธิภาพของระบบเครือข่ายมีดังนี้

- Bandwidth capacity : ภาพกราฟฟิคที่มีขนาดใหญ่,การใช้งานมัลติมีเดียออนไลน์รวมถึงการดาวน์โหลดไฟล์ต่างๆที่มีขนาดใหญ่ส่งผลให้ความจุของแบนวิทธ์นั้นลดน้อยลงและทำให้เครือข่ายทำงานช้าลง
- End-to-End delay : ดีเลย์คือเวลาที่ใช้ในการส่งแพ็คเกตจากต้นทางไปยังปลายทาง
- Variation of delay (Jitter) คือความแตกต่างของดีเลย์แต่ละแพ็คเกตในเครือข่าย
- Packet loss : แพ็คเกตสูญหายนั้นโดยส่วนมากจะเกิดจากการที่เครือข่ายแวนนั้นเกิดความคับคั่งทำให้มีการดรอปแพ็คเกตนั้นๆทิ้งไป

รูปแบบของ QoS นั้นสามารถแบ่งได้เป็น 3 รูปแบบในการนำไปใช้งานจริงดังนี้

1. Best Effort : ด้วยรูปแบบการทำงานในลักษณะนี้จะไม่มีการกำหนดลำดับความสำคัญให้กับแต่ละแพ็คเกต ถ้าในเครือข่ายนั้นไม่ได้มีข้อกำหนดลำดับความสำคัญให้กับแต่ละเซอร์วิส การติดตั้งแบบนี้ก็ถือว่าเป็นแบบที่เหมาะสมแก่การใช้งาน

2. IntServ : ชื่อเต็มคือ Integrated Services สามารถให้บริการการจัดลำดับความสำคัญของแพ็คเกตได้อย่างเต็มที่โดยจะมีการจองแบนวิทธ์เป็นช่วงเลาให้กับแอพพลิเคชั่นที่ต้องการใช้งานในช่วงเวลานั้นๆแต่จะมีข้อจำกัดคือเรื่องของความยืดหยุ่นของระบบเครือข่ายเนื่องจากจะมีการจองแบนวิทธ์อาจส่งผลต่อแอพพลิเคชั่นอื่นๆในระบบได้

3.DiffServ : ชื่อเต็มคือ Differentiated Services จะให้ความยืนหยุ่นมากกว่าในการจัดการกับลำดับความสำคัญของแพ็คเกตในระบบเครือข่าย อุปกรณ์เครือข่ายจะจดจำรูปแบบของทราฟฟิคและจะมีการแบ่งเป็นคลาสของเซอร์วิสไม่เท่ากันจึงทำให้หลายๆเซอร์วิสสามารถทำงานพร้อมกันได้ ไม่ใช่การจองแบนวิทธ์ทั้งหมดเพื่อเซอร์วิสเพียงเซอร์วิสเดียว

บทที่ 3
ขั้นตอนการดำเนินงาน

วิธีการดำเนินสามารถแบ่งออกได้เป็น 3 ส่วนด้วยกันคือ

- จัดเตรียมเครื่องมือและอุปกรณ์ที่ใช้
- ศึกษาข้อมูลการใช้งานของอุปกรณ์และโปรแกรม
- การออกแบบ วิเคราะห์ และติดตั้งระบบ

3.1 จัดเตรียมเครื่องมือและอุปกรณ์ที่ใช้

3.1.1 Pfsense

เป็นโอเพ่นซอร์สเร้าเตอร์และไฟร์วอลซึ่งมีการพัฒนามาจาก FreeBSD จะต้องมีการติดตั้งลงบนเครื่องคอมพิวเตอร์หรือบน Virtual Machine สำหรับในการใช้งานและทำหน้าที่เป็นไฟร์วอลหรือเร้าเตอร์สำหรับเนตเวิร์กใดๆ ซอฟท์แวร์ pfSense นั้นมีหลากหลายฟีเจอร์ต่างๆให้เลือกใช้งานในทุกๆด้านเพื่อตอบสนองกับธุรกิจในปัจจุบันไม่ว่าจะเป็นในเรื่องของความปลอดภัยของระบบเครือข่าย การกำหนดลำดับความสำคัญของแต่ละเซอร์วิสต่างๆของธุรกิจ ในการติดตั้งและใช้งานนั้นจะทำผ่านหน้าเว็ปไซต์และไม่จำเป็นต้องมีพื้นฐานของ FreeBSD ก็สามารถใช้งานได้ โดยประสิทธิภาพการทำงานนั้นถือว่าดีในระดับนึง และในการติดตั้งก็มีค่าใช้จ่ายไม่สูงมากด้วย ในปัจจุบันมีการนำมาติดตั้งใช้งานจริงอย่างแพร่หลาย จากข้อมูลในปี 2013 มี pfSense ติดตั้งไปแล้วมากกว่า 200,000 เครื่องทั่วโลก

รูปที่ 3. 1 โอเพ่นซอร์ส Pfsense

3.1.2 VMware Workstation

โปรแกรม VMware เป็นโปรแกรมซึ่งใช้ในการสร้าง Virtual Machine (VM) หรือเครื่องคอมพิวเตอร์เสมือน คือ เป็นการสร้างเครื่องคอมพิวเตอร์ขึ้นมาอีกเครื่อง(หรือหลายๆเครื่อง ถ้าแรมมากพอ)ภายในเครื่องของเราเอง ดังนั้นจึงทำให้เราสามารถทดลองใช้งาน OS หรือโปรแกรมอื่นๆที่เราสนใจโดยไม่ต้องทำการ format เครื่องหรือใช้ PC อีกเครื่องหนึ่งมาเพื่อทดสอบระบบที่เราสนใจ และ virtual machine ที่กำลังมีการใช้งานอยู่บน VMware สามารถที่จะนำมาใช้งานภายนอกได้จริงในทันที(โดยใช้การ Bridge(Default) หรือ NATออกมาที่ Host ที่ได้ทำการ Run VMware อยู่) ดังนั้นประโยชน์อีกอย่างหนึ่งของ VMware คือสามารถทำการจำลองการทำงานของระบบ Network ได้โดยใช้คอมพิวเตอร์เพียงเครื่องเดียว

รูปที่ 3. 2 ซอฟต์แวร์วีเอ็มแวร์ (VMware)

3.1.3 โน๊ตบุ๊คใช้สำหรับจำลองระบบเครือข่าย(Simulator) ก่อนที่จะนำไปติดตั้งจริง

รูปที่ 3. 3 คอมพิวเตอร์โน๊ตบุ๊ค

3.2 ศึกษาข้อมูลการใช้งานของอุปกรณ์และโปรแกรม

3.2.1 ศึกษาการใช้งานซอฟท์แวร์ VMware

การใช้งานนั้นมีหลากหลายรูปแบบให้เลือกใช้ตามความเหมาะสมของเครือข่ายที่เราต้องการที่จะจำลองขึ้นมา ซึ่งในโครงงานนี้ได้สนใจเพียงบางส่วนนั้นคือ

- ศึกษาวิธีการติดตั้งโปรแกรม
- ศึกษาวิธีการเพิ่มเวอร์ชัวอินเตอร์เฟส (Virtual Interface)
- ศึกษาวิธีการจำลอง OS ต่างๆ
- ศึกษาวิธีการทำงานของเน็ตเวิร์กอินเตอร์เฟสเมื่อใช้ DHCP
- ศึกษาวิธีการทำงานของเน็ตเวิร์กอินเตอร์เฟสเมื่อใช้ NAT
- ศึกษาวิธีการทำงานของเน็ตเวิร์กอินเตอร์เฟสเมื่อใช้ host-only
- ศึกษาวิธีการเชื่อมต่อ virtual machine กับเครือข่ายภายนอก

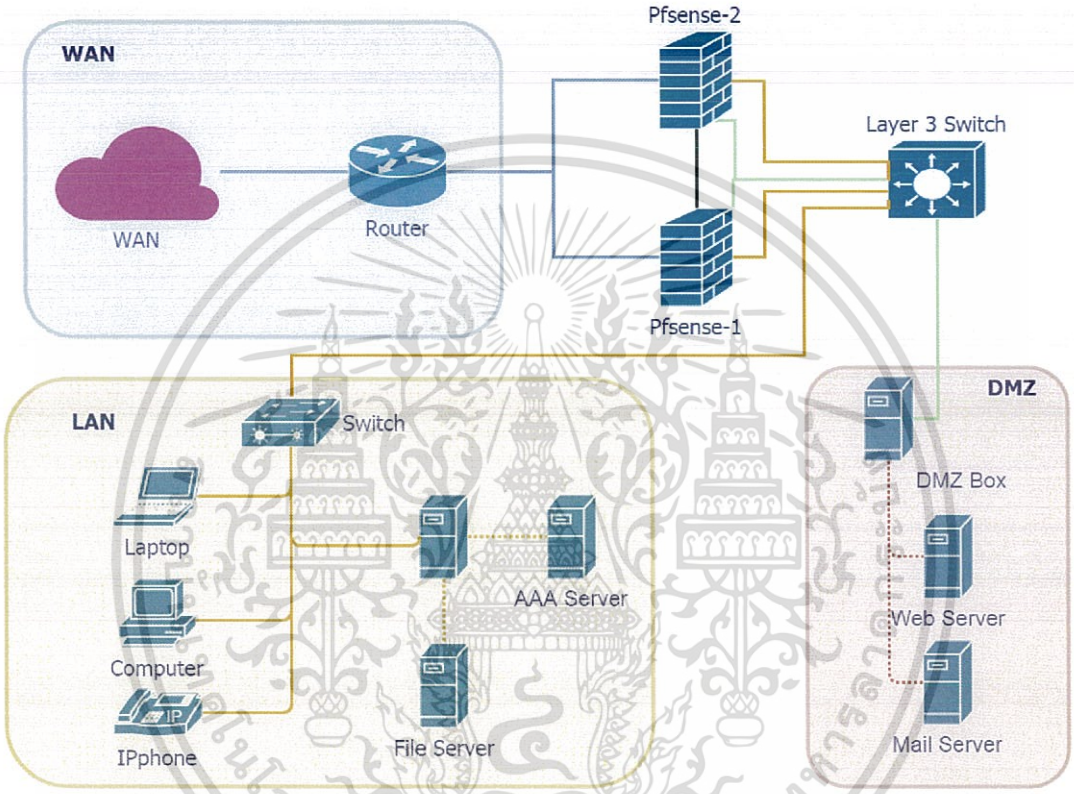
3.2.2 ศึกษาการใช้งาน Pfsense

Pfsense นั้นมีฟีเจอร์ที่สามารถนำมาประยุกต์ให้เกิดประโยชน์กับเครือข่ายได้อย่างมากมายแต่ในโครงงานนี้จะนำมาเพียงบางฟีเจอร์หรือบางคุณสมบัติที่จำเป็นเท่านั้นคือ

- ศึกษาการติดตั้ง Pfsense บน VMware
- ศึกษาการตั้งค่า WAN และ LAN Interfaces
- ศึกษาการตั้งค่า Secure Shell (SSH)
- ศึกษาการตั้งค่า Firewall rule
- ศึกษากาตั้งค่า Traffic-shaping (QoS, Quality of Service)
- ศึกษาการสร้าง Captive portal
- ศึกษาการสร้าง CARP failover
- ศึกษาการสร้าง Load-balancing
- ศึกษาการมอนิเตอร์ทราฟฟิกและทำรีพอร์ท

3.3 วิเคราะห์และออกแบบระบบ

โครงงานนี้เป็นการเพิ่มความปลอดภัยให้กับระบบเครือข่ายที่มีอยู่เดิมแล้ว โดยการติดตั้งไฟร์วอลที่เป็นโอเพ่นซอร์สเข้าไปตามความต้องการของลูกค้า โดยจะต้องวิเคราะห์ระบบเครือข่ายเดิมที่มีอยู่ก่อนแล้วจึงนำเสนอแล้วทางในการพัฒนาให้ดียิ่งขึ้นแก่ลูกค้า โดยในส่วนของโครงงานนี้นั้นรับผิดชอบในการติดตั้งไฟร์วอลและตั้งค่าในบางส่วน



รูปที่ 3. 4 ไดอะแกรมของเครือข่ายที่ได้ออกแบบ

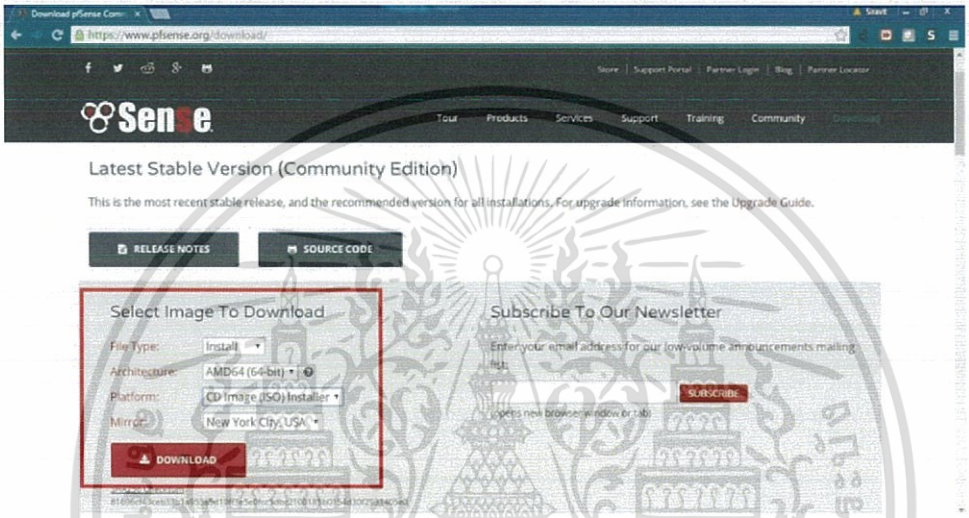
IP Address	Pfsense-1	Pfsense-2
WAN Interface	161.246.1.1/24	161.246.1.2/24
LAN Interface	192.168.1.1/24	192.168.1.2/24
SYNC Interface (failover)	10.0.0.1/24	10.0.0.02/24
DMZ Interface	200.1.1.1/24	200.1.1.2/24

ตารางที่ 3.1 ไอพีแอดเดรสของอุปกรณ์ต่างๆ

3.4 ติดตั้ง Pfsense บน VMware

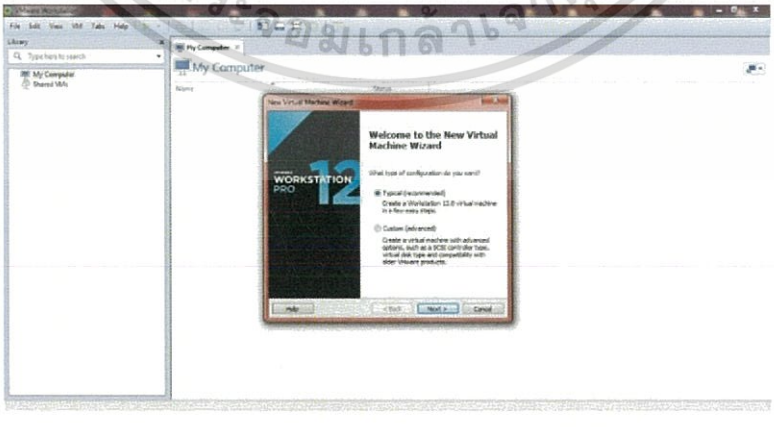
เนื่องจากในโครงงานนี้ก่อนที่จะมีการนำไปติดตั้งจริงจำเป็นที่จะต้องมีการทดสอบก่อน จึงจำลองการติดตั้งนี้ขึ้นมาบน Virtual machine

3.4.1 ทำการดาวน์โหลดซอฟท์แวร์ Pfsense ได้จาก www.pfsense.org/download โดยในช่อง Select Image To Download ให้เลือกตามกรอบสีแดงดังภาพที่ 3.4.2



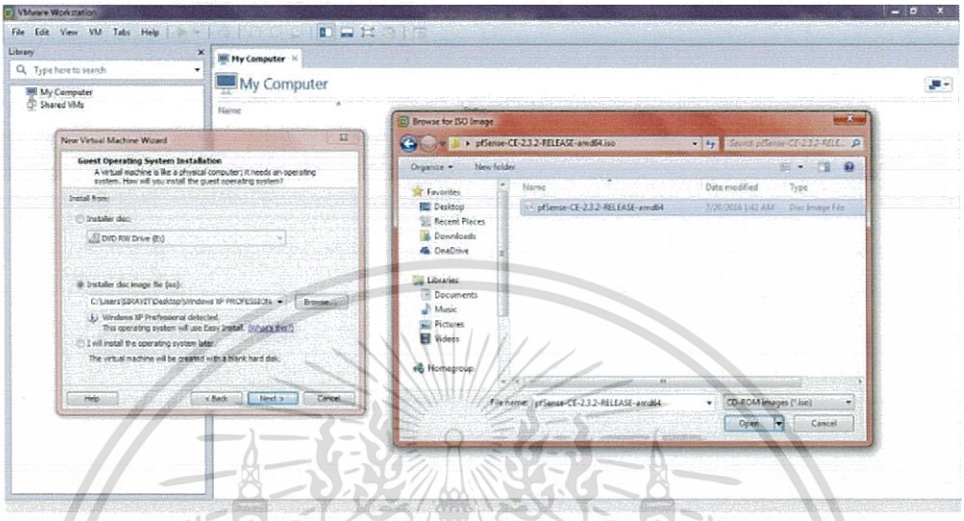
รูปที่ 3. 5 เว็บดาวน์โหลด Pfsense

3.4.2 หลังจากดาวน์โหลดเสร็จเรียบร้อยแล้ว จะได้ไฟล์ที่เป็น .iso ในกรณีที่จะติดตั้งจริงจำเป็นที่จะต้องโหลดใส่ลงแผ่น DVD เพื่อทำการติดตั้ง แต่ในกรณีศึกษานี้เราจะใช้โปรแกรม VMware ในการทำ virtual machine เริ่มจาก File > new virtual machine > typical > next



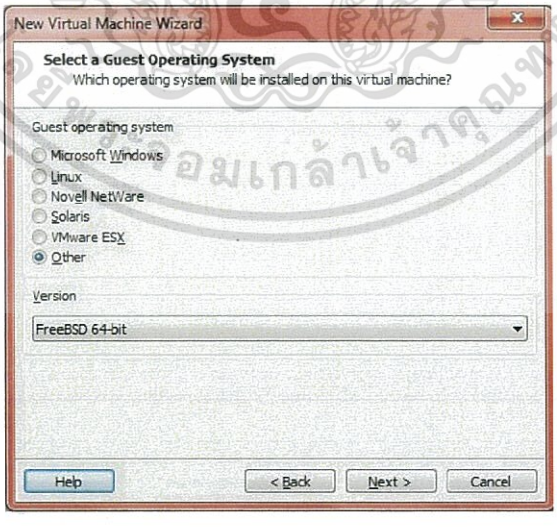
รูปที่ 3. 6 สร้าง virtual machine ใหม่

3.4.3 หลังจากทำการกด Next มาแล้วนั้นให้ทำการเลือกไฟล์อิมเมจที่เราได้ดาวน์โหลดมาในตอนแรกโดยเลือกในช่องของ Installer disc image file(iso) และทำการกด open และกด next



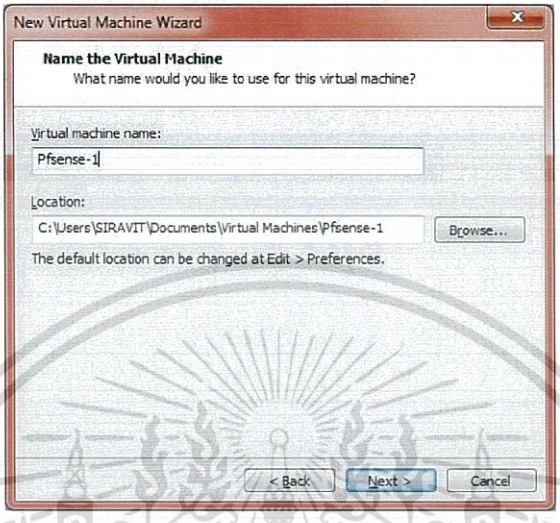
รูปที่ 3. 7 เลือกไฟล์อิมเมจ pfsense

3.4.4 หลังจากนั้นจะเป็นการเลือกระบบปฏิบัติการ pfsense นั้นจะทำงานบน FreeBSD ให้เราเลือก Other และ Version เป็น FreeBSD 64-bit และกด next



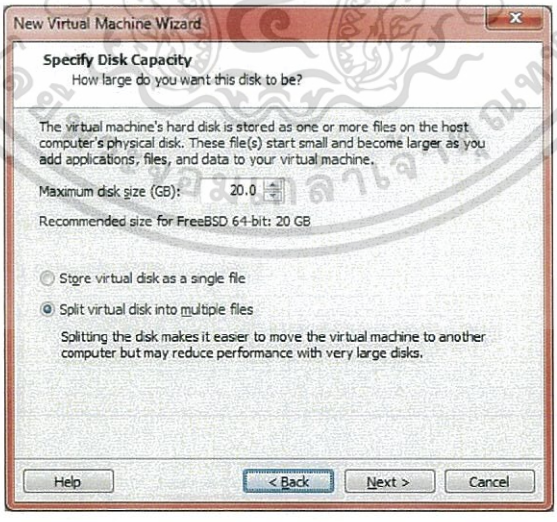
รูปที่ 3. 8 เลือกระบบปฏิบัติการ

3.4.5 หลังจากนั้นให้ทำการตั้งชื่อในช่อง Virtual machine name ในที่นี้จะตั้งชื่อเป็น Pfsense-1 เนื่องจากจะให้เป็นตัวแรกจากทั้งหมด 2 ตัวเพื่อเอามาทำ failover กันและ Location คือที่เก็บไฟล์ของ Virtual machine นี้และกด next



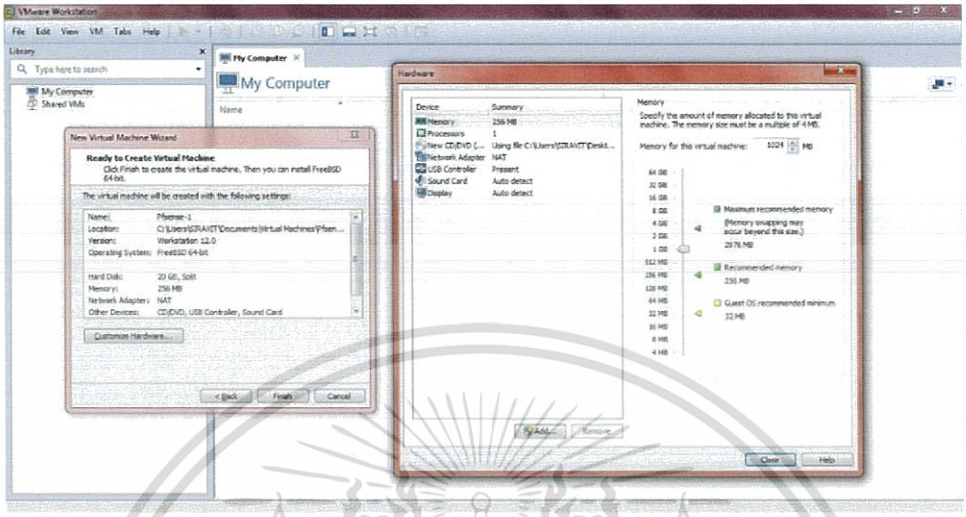
รูปที่ 3. 9 ตั้งชื่อ Virtual machine และกำหนดที่เก็บไฟล์

3.4.6 ทำการเลือกขนาดของฮาดดิสท์โดยจะเป็นการจองล่วงหน้าขนาดจะสามารถขยายไปเรื่อยๆจนถึงที่เรากำหนดไว้และเลือกเป็น Spilt virtual disk into multiple files



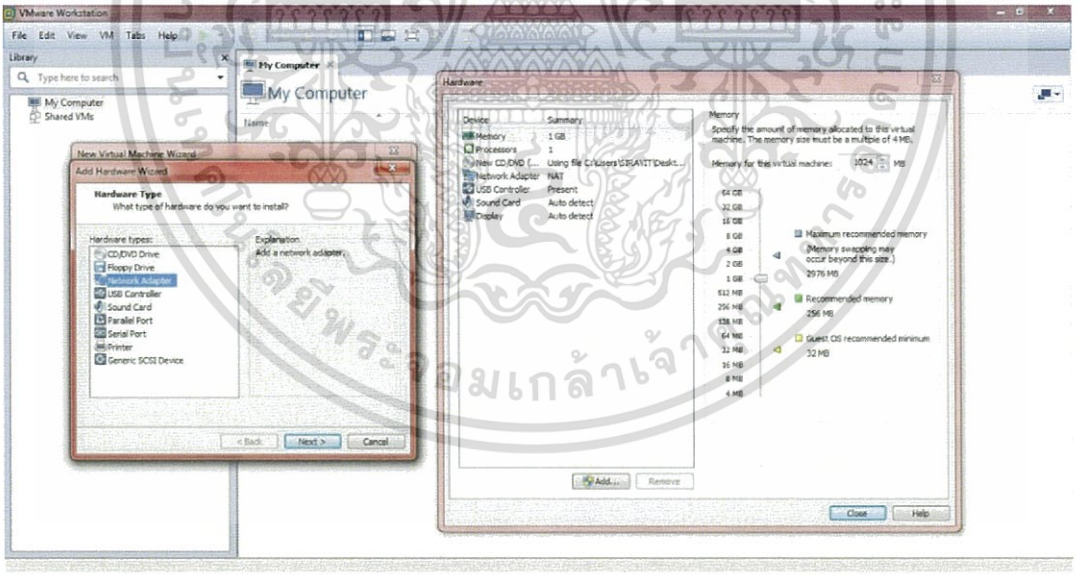
รูปที่ 3. 10 เลือกขนาดของฮาดดิสท์และรูปแบบการเก็บไฟล์

3.4.7 กำหนดสเปคของคอมพิวเตอร์ที่เราจะใช้ในการจำลอง pfsense โดยทำการเพิ่มแรมเป็น 1024 MB และเพิ่ม Network adapter ดังภาพต่อไปนี้



รูปที่ 3. 11 เพิ่มแรมและเน็ตเวิร์กอินเตอร์เฟส

3.4.8 เพิ่ม Network adapter โดยการกด Add และเลือก Network Adapter



รูปที่ 3. 12 การเพิ่มเน็ตเวิร์กอแดปเตอร์

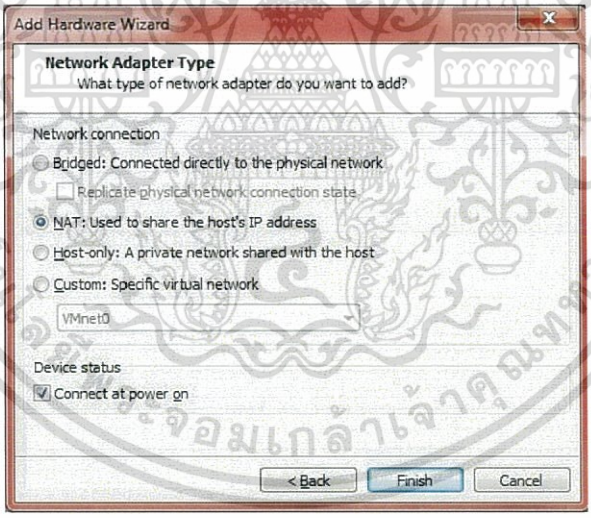
3.4.9 หลังจากกด next มานั้นจะเป็นการเลือกโหมดการทำงานของ Network adapter โดยจะอธิบายได้คร่าวๆดังนี้

1. Bridge mode จะเป็นการเชื่อมต่อโดยตรงกับเน็ตเวิร์กที่คอมพิวเตอร์ที่รัน VMware ทำงานอยู่โดยจะมีการแจกไอพีแอดเดรสมาให้ตัว virtual machine นี้ด้วย เปรียบเสมือนเป็นคอมอีก 1 เครื่องที่อยู่บนเน็ตเวิร์ก

2. NAT จะทำการแปลงหมายเลขไอพีแอดเดรสจากเน็ตเวิร์กของคอมพิวเตอร์ที่ได้รับมาให้เป็นไอพีแอดเดรสที่เราต้องการยกตัวอย่างเช่นคอมพิวเตอร์เราใช้ 192.168.1.3/24 เราสามารถตั้งค่า NAT ให้เปลี่ยนจาก 192.168.1.3/24 เป็น 10.0.0.3/24 ได้

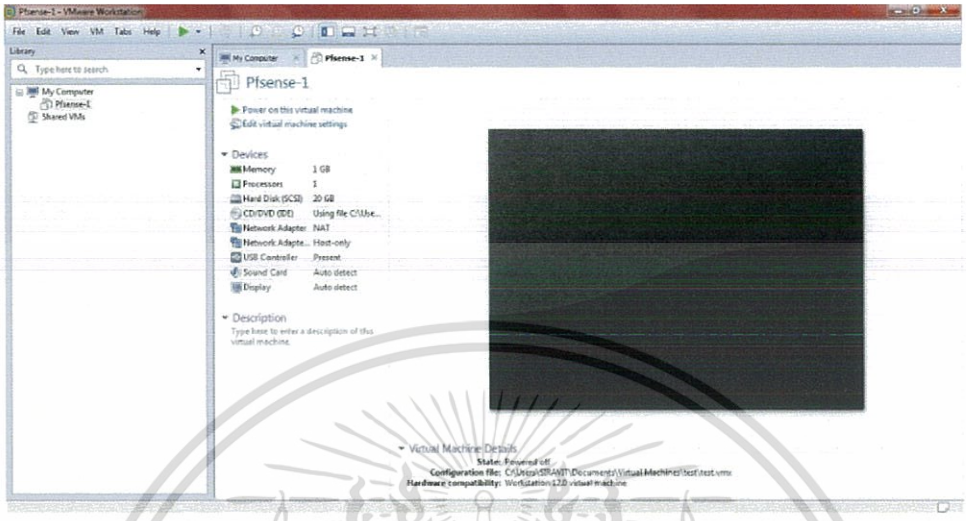
3. Host-only เป็นการสร้างเน็ตเวิร์กภายในซึ่งจะไม่เกี่ยวข้องกับเน็ตเวิร์กภายนอกที่เชื่อมต่อกับคอมพิวเตอร์ของเครื่องเรา

ในที่นี้ให้เลือกเป็น NAT โดยเราจะทำการตั้งค่า NAT หลังจากนี้ต่อไป



รูปที่ 3. 13 เลือกโหมดการทำงานของเนตเวิร์กอะแดปเตอร์

3.4.10 เสร็จสิ้นการสร้าง virtual machine บน VMware ต่อไปจะเป็นการติดตั้ง Pfsense ลงบน virtual machine ที่เราได้สร้างไว้

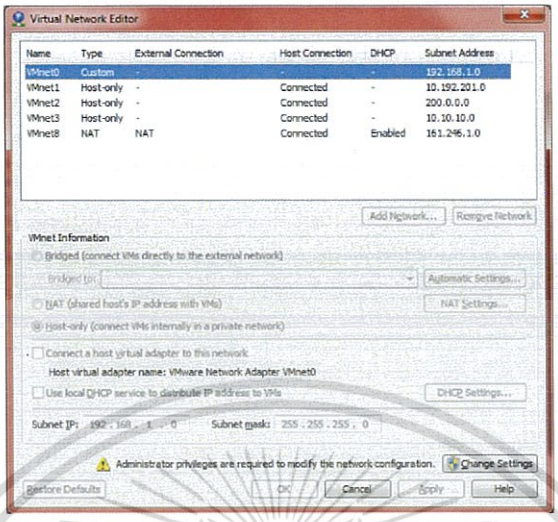


รูปที่ 3. 14 การจำลอง Virtual machine เสร็จสมบูรณ์

3.5 ตั้งค่า Virtual Network Interfaces

ก่อนที่เราจะทำการจำลองการทำงานของ Pfsense นั้น จำเป็นต้องมีการตั้งค่าอินเตอร์เฟสต่างๆให้กับ Vmware ก่อน หลังจากนั้นเราจะสามารถนำไปใช้กับ Pfsense ได้ จากไดอะแกรมข้างต้นที่ได้มีการออกแบบไว้ จะเห็นได้ว่ามีไอพีแอดแดรสอยู่ทั้งหมด 3 เน็ตเวิร์กด้วยกัน ได้แก่ ไอพีแอดเดรสที่เป็นพับบลิตไอพี 161.246.1.0/24 ไอพีแอดเดรสที่เป็นไพรเวทที่ใช้เชื่อมระหว่างไฟร์วอล 10.0.0.0/24 และไอพีแอดเดรสของเน็ตเวิร์กภายใน 192.168.1.0/24

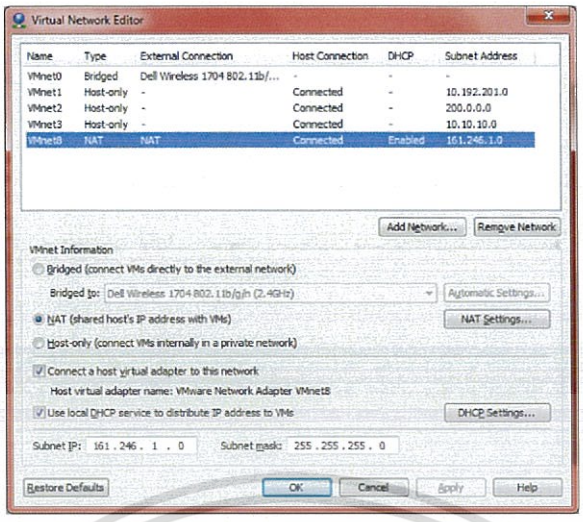
3.5.1 กำหนดอินเตอร์เฟสใน VMware ดังนี้ Edit > Virtual Netowrk Editor



รูปที่ 3. 15 หน้าต่าง Virtual Network Editor

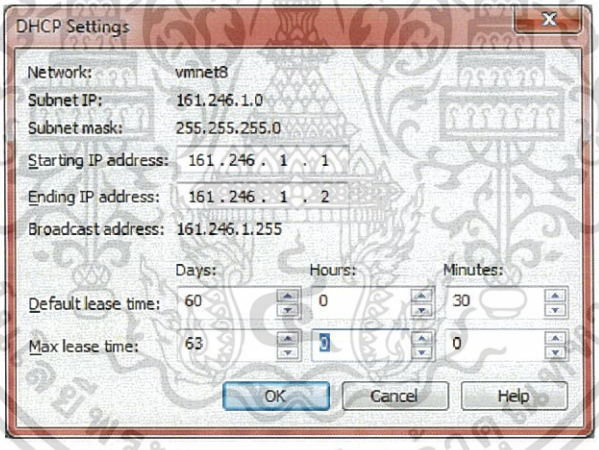
จากรูปให้สังเกตุตรงช่อง Name ที่จะมี VMnet0 , Vmnet1... นี่คืออินเตอร์เฟสของ VMware ที่สร้างไว้เพื่อรองรับให้ Virtual machine นำไปใช้นั่นเอง ในที่นี้เราจำเป็นที่จะต้องจำลองทั้งหมด 3 อินเตอร์เฟสได้แก่ WAN , LAN และ OPT

3.5.2 สร้างอินเตอร์เฟส WAN ก่อนเนื่องจากเราจำเป็นที่จะต้องให้ Virtual Machine ของเรานั้นสามารถออกสู่อินเทอร์เนตได้จริงๆ จึงจะต้องทำการ NAT ไอพีแอดเดรสของเครื่องคอมพิวเตอร์ที่ได้รับไอพีจากเร้าเตอร์จริงๆนั้นให้เสมือนว่า Pfsense ได้รับพับบลิคไอพีแอดเดรสมาโดยจะใช้เป็นเน็ตเวิร์กวง 161.246.1.0/24 โดยจะให้ VMware นั้นแจกเป็น DHCP มาให้ Virtual machine ให้ตั้งค่า Subnet IP และ Subnet mask โดยคลิกที่ VMnet8 และตั้งค่าดังรูป



รูปที่ 3. 16 ตั้งค่า Subnet IP และ Subnet mask

3.5.3 หลังจากนั้นกดที่ DHCP Setting เพื่อตั้งค่า range ของการแจกไอพีแอดเดรสและ

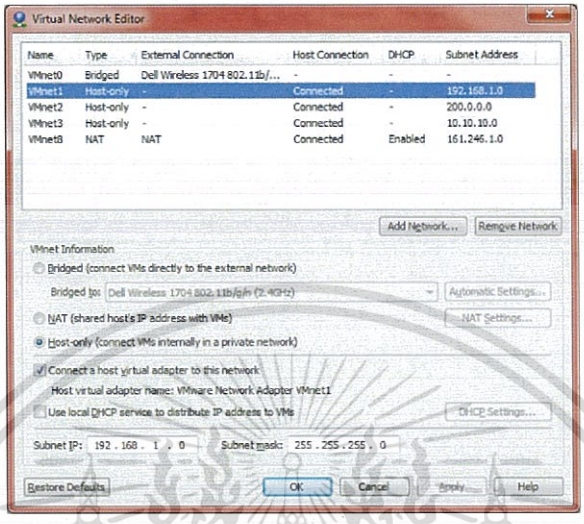


รูปที่ 3. 17 หน้าต่าง DHCP Setting

ทำการตั้งค่า เนื่องจากมี Pfsense 2 ตัวจึงได้มีการกำหนดให้มีการแจกเพียง 2 ไอพีเท่านั้นดังรูป

ดังนั้นตอนนี้เราจะได้อินเตอร์เฟสสำหรับ Pfsense ที่จะใช้ในขา WAN ลำดับต่อไปจะทำการตั้งค่าสำหรับขา LAN และ OPT ตามลำดับ

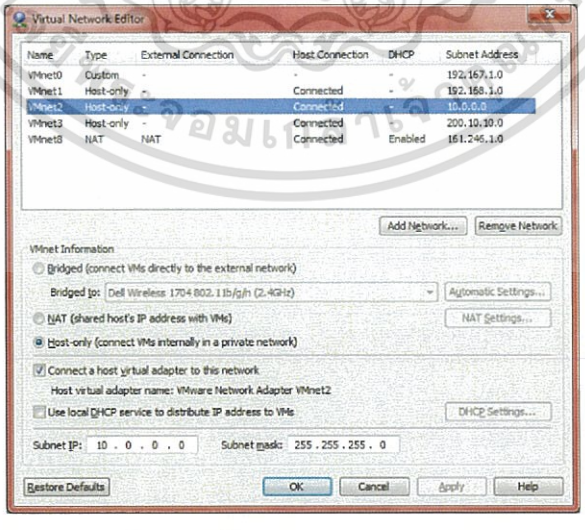
3.5.4 สำหรับ LAN นั้นจะใช้ไอพีเป็นไพรเวทไอพีแอดเดรส 192.168.1.0/24 ให้ทำการเข้าไปที่ Virtual Network Editor เลือก VMnet1 ในส่วนของ VMnet Information เลือกเป็น



รูปที่ 3. 18 ตั้งค่า Virtual Interface ของ LAN

Host-only ในส่วนของ Subnet IP และ Subnet mask ให้ตั้งค่าดังรูป

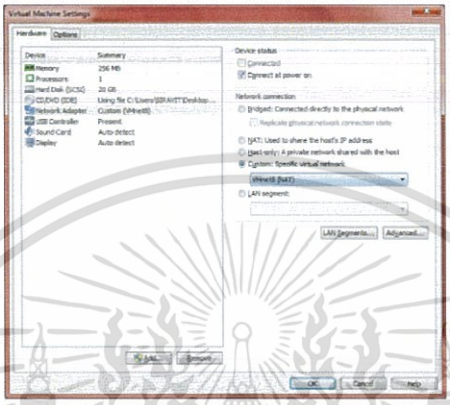
3.5.5 สำหรับ OPT นั้นเป็นอินเตอร์เฟสที่ใช้เชื่อมต่อระหว่าง Pfsense ด้วยกันดังนั้นจึงจะใช้เป็นไพรเวทไอพีแอดเดรสเช่นกัน 10.0.0.0/24 โดยเลือก VMnet2 ในส่วนของ VMnet Information เลือกเป็น Host-only ในส่วนของ Subnet IP และ Subnet mask ให้ตั้งค่าดังรูป



รูปที่ 3. 19 รูปที่ 3.5.5 ตั้งค่า Virtual Interface ของ SYNC

3.5.6 หลังจากที่เราได้เพิ่มอินเตอร์เฟสที่จำเป็นทั้งหมดบน VMware แล้วนั้นเราจะเพิ่ม Network Adapter ให้กับ Pfsense และทำการเลือกรูปแบบการเชื่อมต่อของแต่ละอินเตอร์เฟสให้กับ Pfsense โดยไปที่ Setting ของ Pfsense-1 แล้วตั้งค่าดังรูปต่อไปนี้

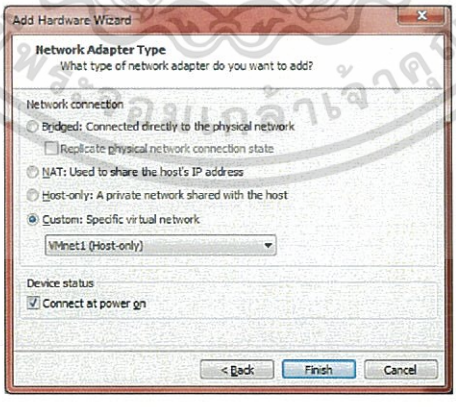
Wan > VMnet8 LAN > Vmnet1 OPT > VMnet2



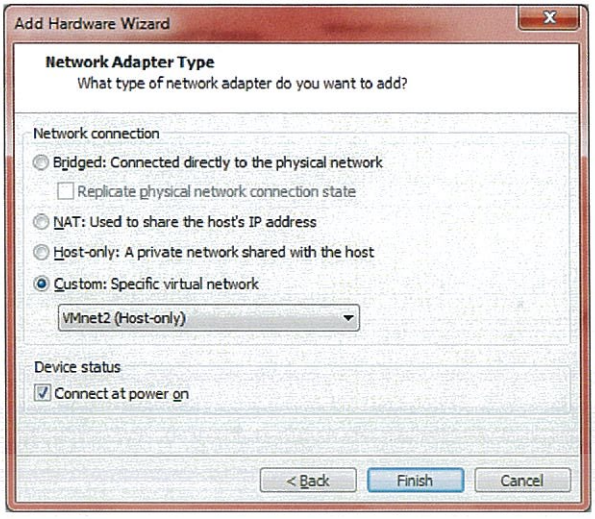
รูปที่ 3. 20 กำหนดโหมดการเชื่อมต่อของ Network adapter

จากรูปจะสังเกตเห็นได้ว่าในค่าเริ่มต้นนั้นมี Network adapter เพียง 1 การ์ดเท่านั้นเราจำเป็นที่จะต้องเพิ่มอีก 2 เพื่อที่จะนำไปใช้กับ LAN และ OPT

3.5.7 เพิ่ม Network adapter โดยที่หน้าต่าง Virtual machine setting เลือก add > network adapter > next > Custom > VMnet1(LAN)



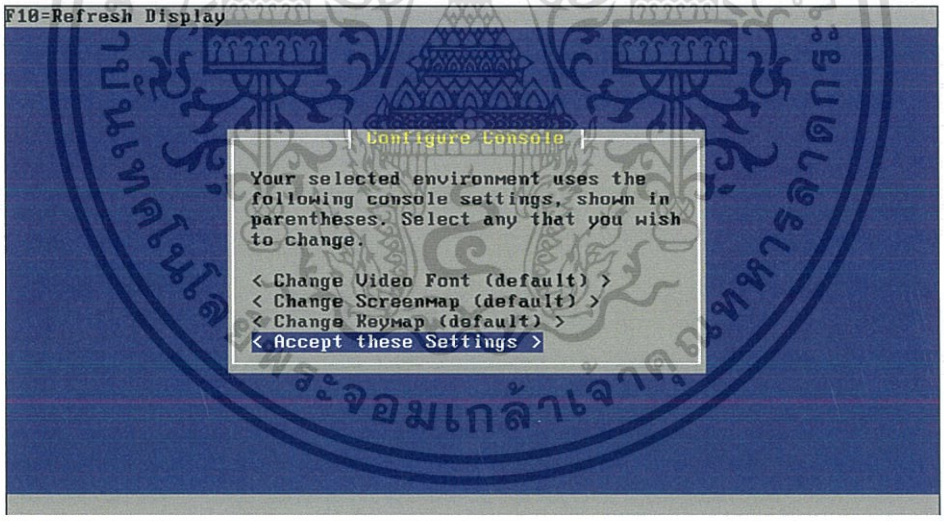
รูปที่ 3. 21 กำหนดโหมดการเชื่อมต่อของ Network adapter (LAN)



รูปที่ 3. 22 กำหนดโหมดการเชื่อมต่อของ Network adapter (SYNC)

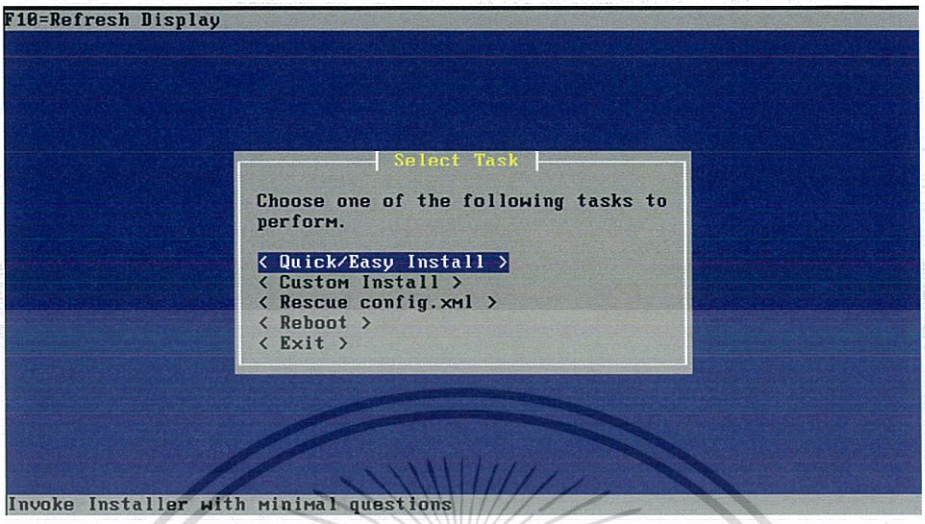
3.6 ติดตั้ง Pfsense สำหรับการใช้งาน

3.6.1 เลือก Pfsense-1 และกดปุ่ม Power on this virtual machine และรอการบูท จากนั้นpfsense จะนำไปสู่หน้าต่างนี้ เลือก Accept These Setting



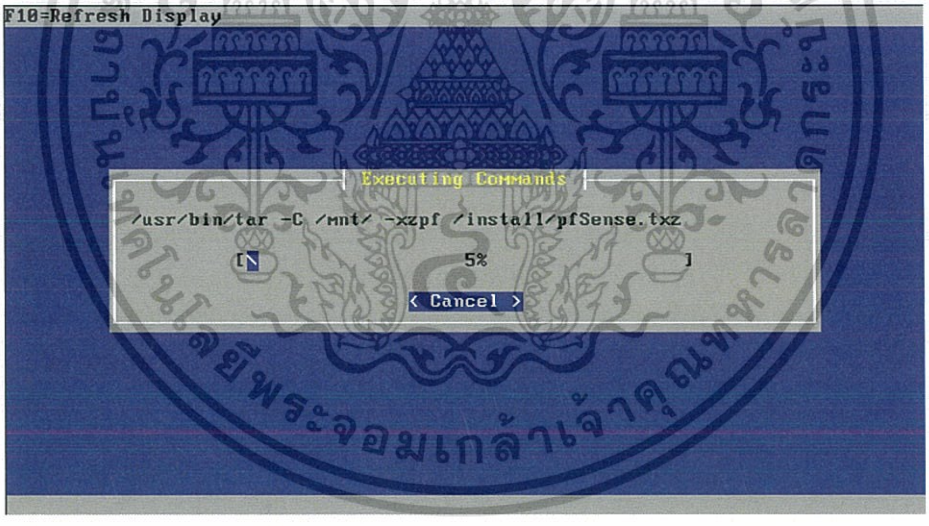
รูปที่ 3. 23 หน้าเริ่มต้นการติดตั้ง Pfsense

3.6.2 เลือก Quick/Easy Install



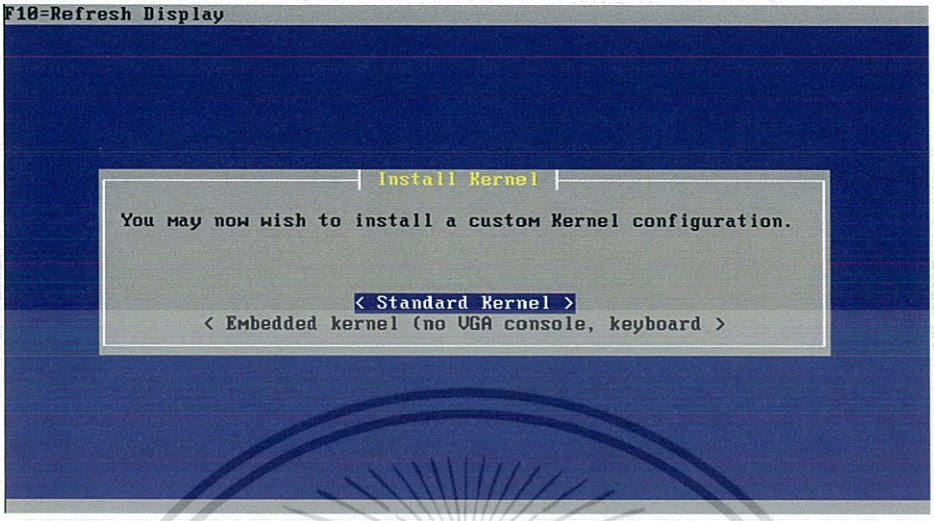
รูปที่ 3. 24 เลือกโหมดของการติดตั้ง

3.6.3 รอการติดตั้ง



รูปที่ 3. 25 รอการติดตั้ง Pfsense

3.6.4 เลือก Kernel

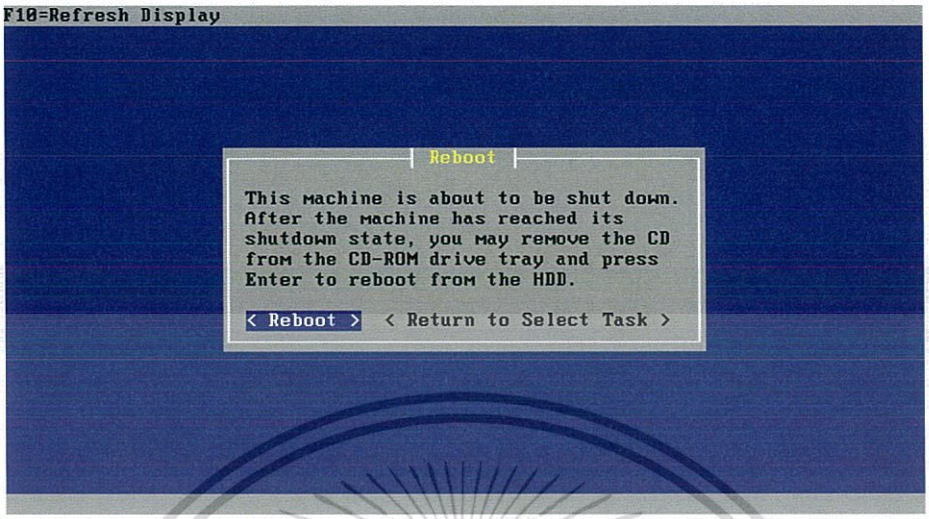


รูปที่ 3. 26 เลือก Kernel ในการทำงาน

3.6.5 รอการติดตั้ง

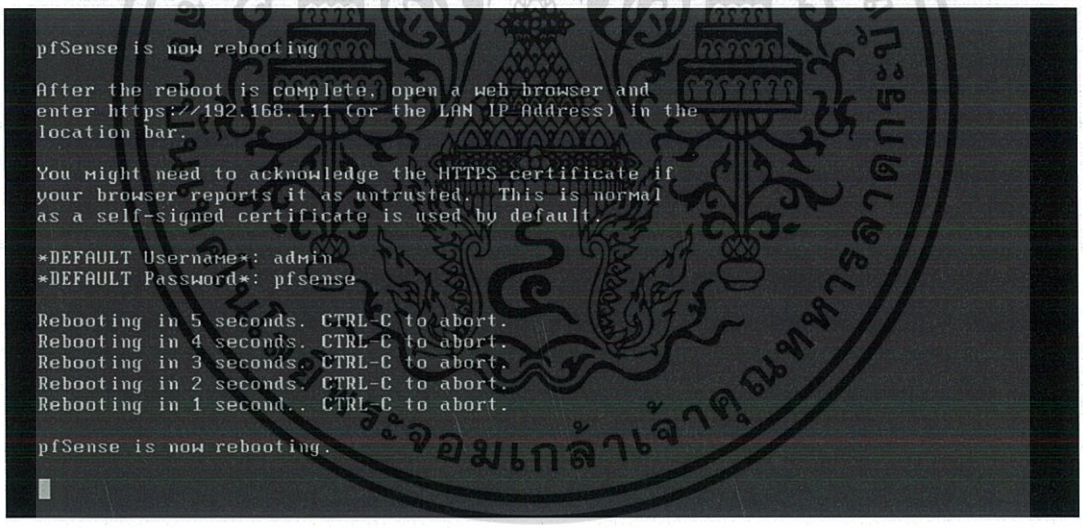
รูปที่ 3. 27 รอการติดตั้ง Kernel

3.6.6 Reboot



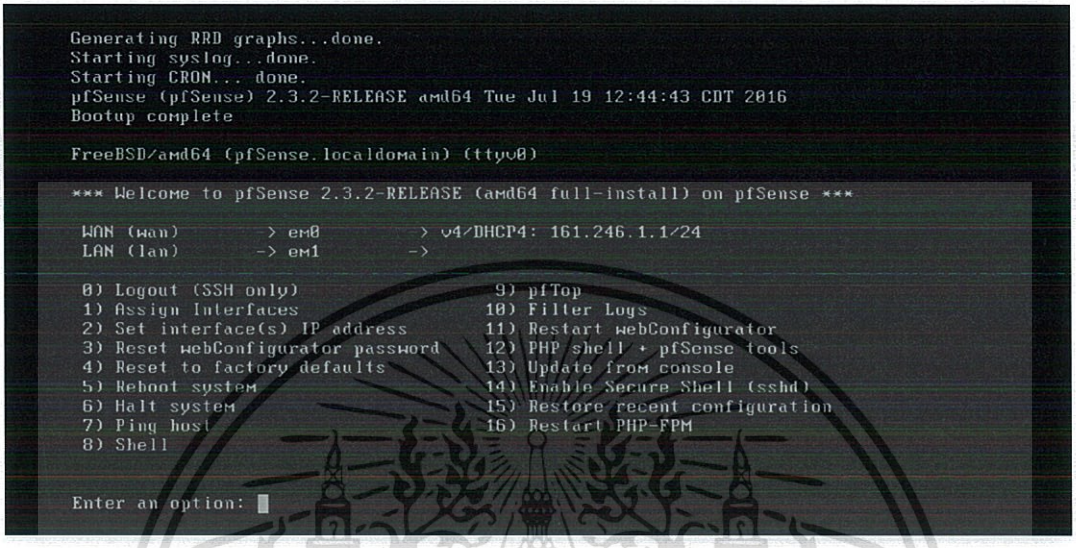
รูปที่ 3. 28 Reboot การทำงาน Pfsense

3.6.7 ยูสเซอร์เนมและรหัสผ่านเริ่มต้นของ Pfsense



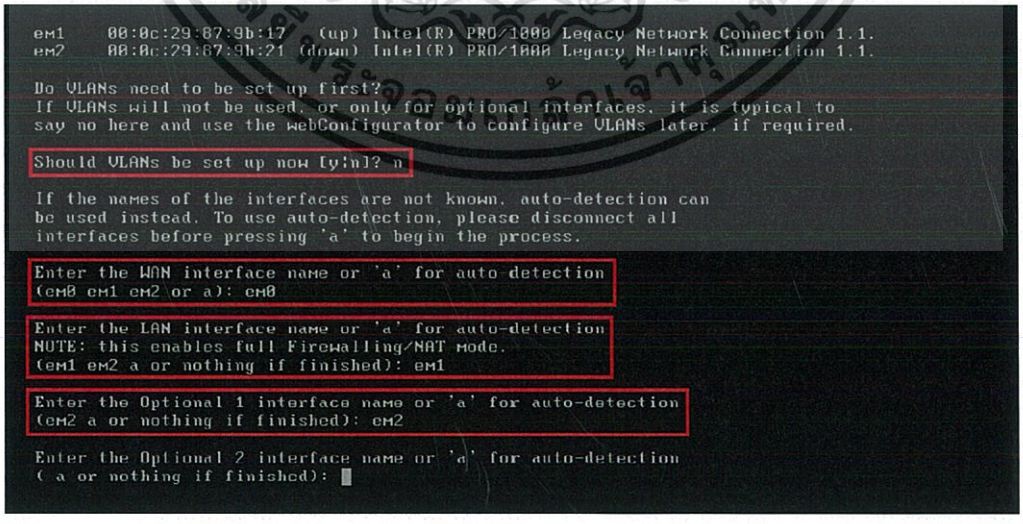
รูปที่ 3. 29 ยูสเซอร์เนมและรหัสผ่านในการคอนฟิก

3.6.8 หน้าแรกของการทำงาน Pfsense ในรูปแบบ Console จะสังเกตุเห็นว่าอินเตอร์เฟส WAN นั้นได้รับไอพีแอดเดรสแบบ DHCP เป็น 161.246.1.1/24 ตามที่ได้ตั้งค่าไว้ในด้านบน ดังรูป



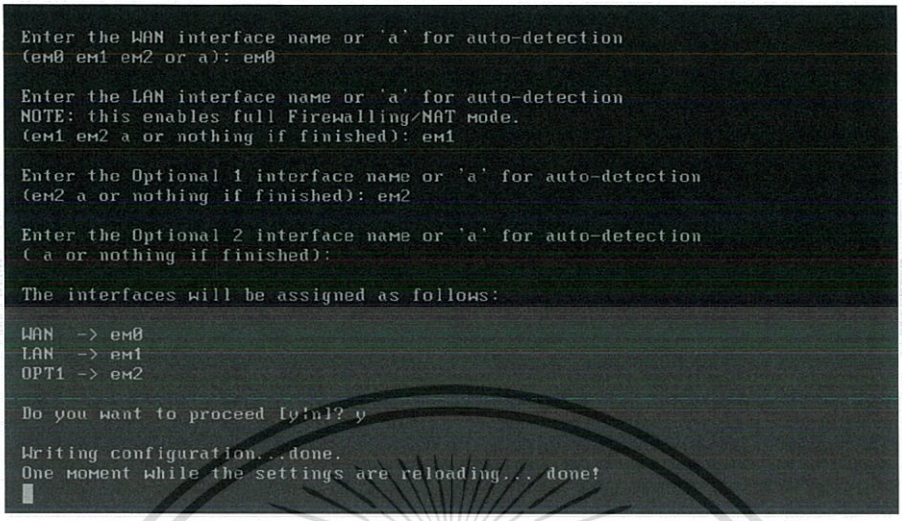
รูปที่ 3. 30 หน้าแรกของการทำงานโหมด Console

3.6.9 ทำการเพิ่มอินเตอร์เฟสโดยใช้คำสั่ง Assign Interfaces (1) โดยในสี่เหลี่ยมสีแดงแรกเป็นการถามว่าต้องการสร้าง Vlan หรือไม่ให้พิม n แล้ว enter หลังจากนั้นจะถาม WAN interface ให้ใช้ em0 และ LAN กับ OPT ให้เลือกเป็น em1 และ em2 ตามลำดับ หลังจากนั้น enter



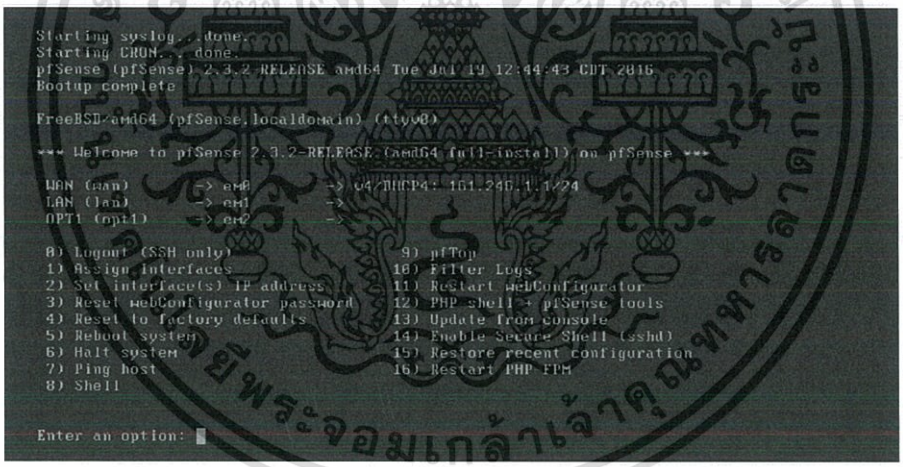
รูปที่ 3. 31 Assign Interfaces

3.6.10 ยืนยันการตั้งค่าอินเตอร์เฟส



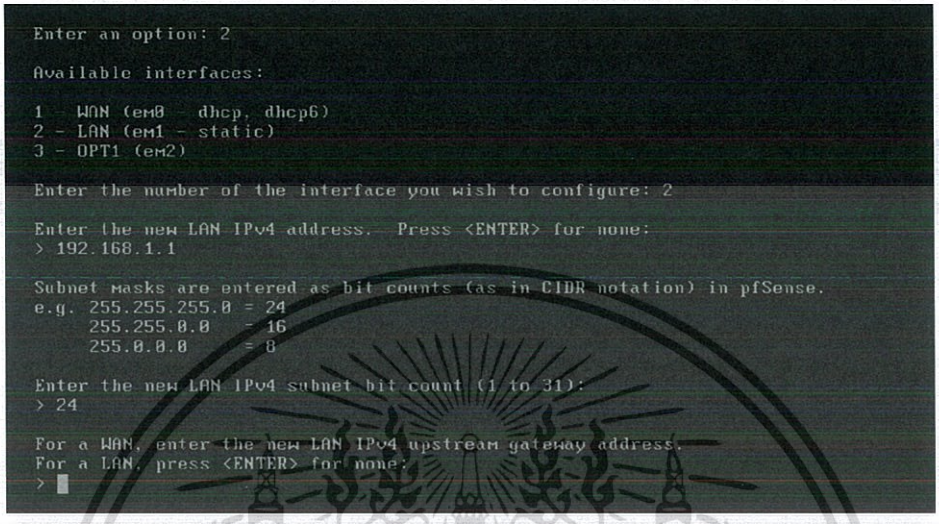
รูปที่ 3. 32 ยืนยันการตั้งค่าอินเตอร์เฟส

3.6.11 อินเตอร์เฟสทั้งหมดหลังจากทำการเพิ่มแล้ว



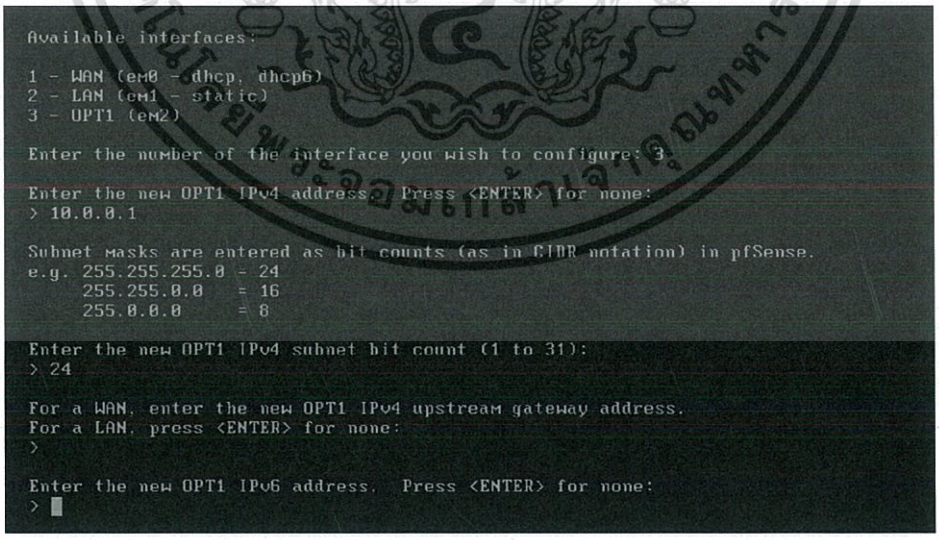
รูปที่ 3. 33 อินเตอร์เฟสทั้งหมดบน Pfsense

3.6.12 ทำการตั้งค่าไอพีแอดเดรสให้กับอินเตอร์เฟส LAN โดยใช้ไอพีเป็น 192.168.1.1 และมีซับเนตมาคเป็น 255.255.255.0 หลังจากนั้นทำการ enter และไม่ต้องเลือ DHCP ให้พิม n ดังรูป



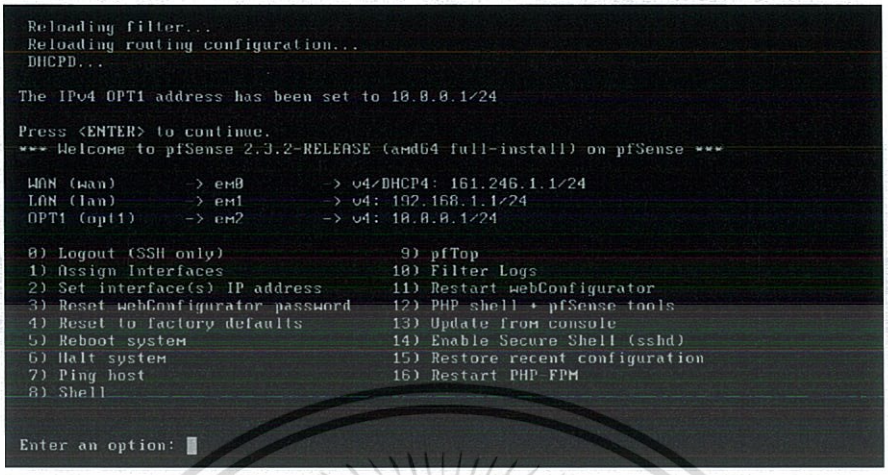
รูปที่ 3. 34 ตั้งค่าไอพีแอดเดรสให้อินเตอร์เฟส LAN

3.6.13 ทำการตั้งค่าไอพีแอดเดรสให้กับอินเตอร์เฟส OPT โดยใช้ไอพีเป็น 10.0.0.1 และมีซับเนตมาคเป็น 255.255.255.0 หลังจากนั้นทำการ enter และไม่ต้องเลือก DHCP โดยพิมพ์ n ดังรูป



รูปที่ 3. 35 ตั้งค่าไอพีแอดเดรสให้อินเตอร์เฟส SYNC

3.6.14 อินเตอร์เฟสทั้งหมดหลังเพิ่มและกำหนดไอพีแอดเดรสให้

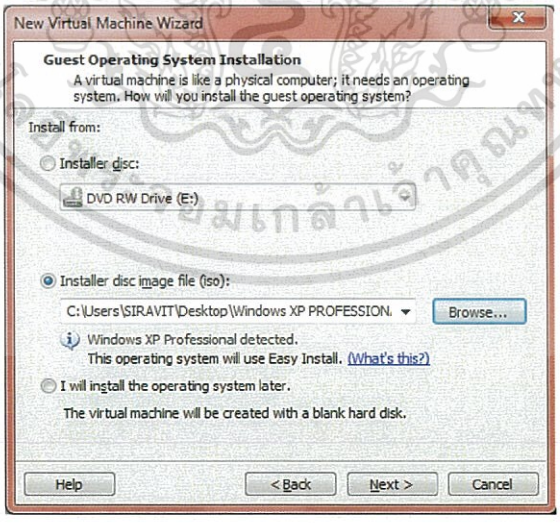


รูปที่ 3. 36 อินเตอร์เฟสทั้งหมดของ Pfsense หลังทำการกำหนดไอพีแอดเดรส

3.7 ติดตั้ง Windows XP เพื่อใช้สำหรับการตั้งค่า Pfsense

หลังจากติดตั้ง Pfsense บน VMware แล้วนั้นจำเป็นที่จะต้องมีเวิร์กสเตชั่นสำหรับตั้งค่า Pfsense เนื่องจากต้องทำการตั้งค่าหรือคอนฟิกผ่าน Web browser โดยในโครงงานนี้จะใช้ Window XP โดยจะทำการติดตั้งบน VMware โดยมีขั้นตอนดังต่อไปนี้

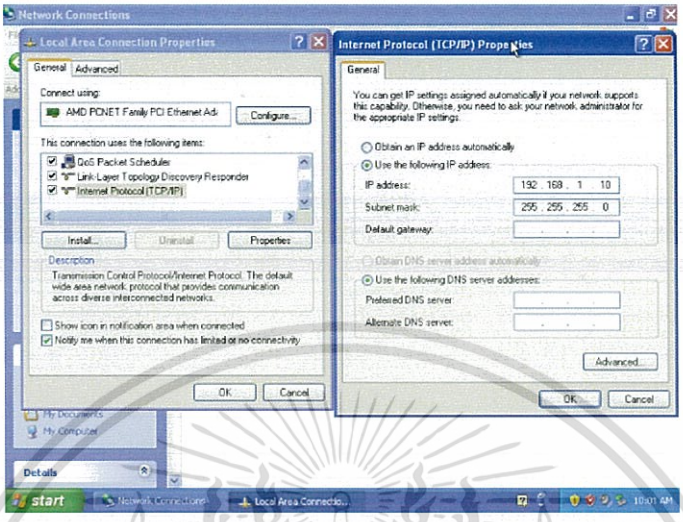
3.7.1 ทำการเพิ่มอิมเมจเหมือนในหัวข้อ 3.4



รูปที่ 3. 37 เพิ่มอิมเมจของ Windows XP

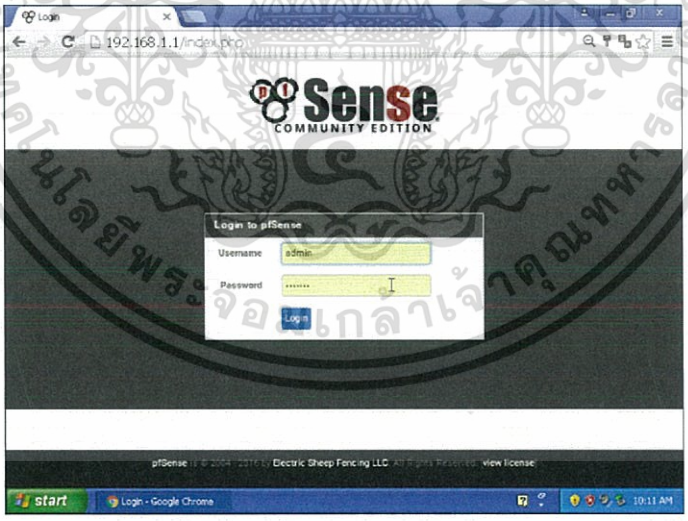
หลังจากทำเพิ่มอิมเมจแล้วนั้นก็ทำการติดตั้งเหมือนกับการติดตั้ง Windows ทั่วไป จากนั้นให้ทำการแก้ไขที่ Network adapter ของ Windows XP ให้เป็น VMnet1 (Host-only)

เนื่องจากต้องการให้มีไอพีแอดเดรสที่อยู่ในเน็ตเวิร์กเดียวกันกับ Pfsense ที่เป็น LAN Interface (192.168.1.0/24) โดยให้ทำการตั้งค่า Static IP โดยใช้เป็น 192.168.1.10/24 ดังรูป



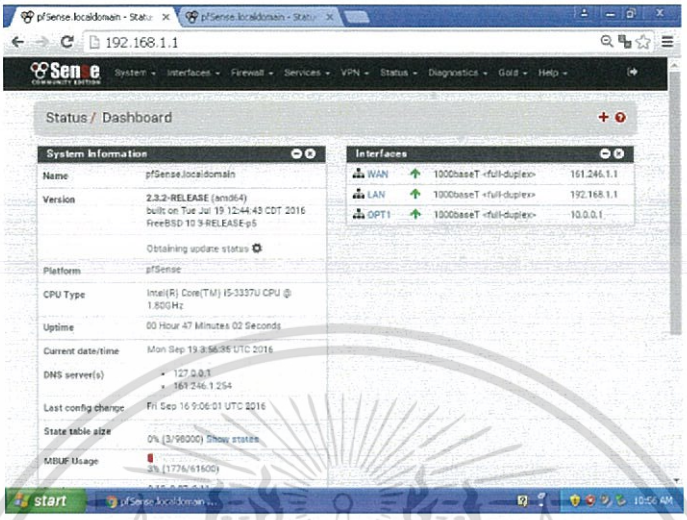
รูปที่ 3. 38 ตั้งค่าไอพีแอดเดรสบน Windows XP

3.7.3 ทำการทดลองเข้าหน้าคอนฟิกของ Pfsense ผ่าน Chrome โดยเข้าผ่านไอพีแอดเดรส 192.168.1.1 โดย Username คือ **admin** และ Password คือ **pfsense**



รูปที่ 3. 39 หน้าล็อกอินของ Pfsense

3.7.4 หลังจากทำการล็อกอินเข้ามาแล้ว หน้าแรกของ Pfsense จะเป็น dashboard ซึ่งจะแสดงข้อมูลของระบบและอินเตอร์เฟสต่างๆที่มีบน Pfsense

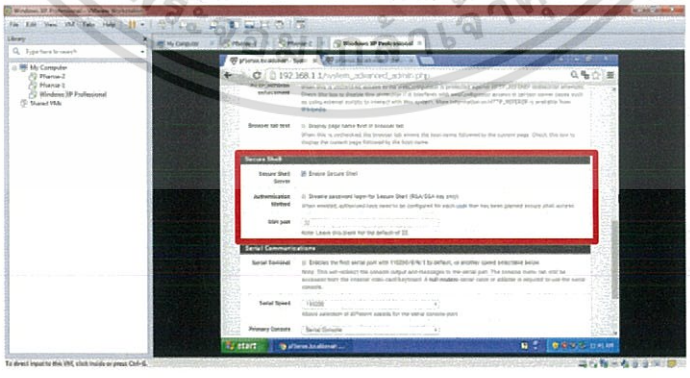


รูปที่ 3. 40 หน้าแรกของ Pfsense

3.8 ใช้งาน Secure Shell Service (SSH)

SSH เป็นโปรโตคอลทางเน็ตเวิร์กที่อนุญาตให้มีการเชื่อมต่อกันระหว่างสอง device โดยมีการเข้ารหัสข้อมูลก่อนทำการส่งไปยังปลายทาง การเปิดใช้งาน SSH บน Pfsense เป็นการอนุญาตให้เข้าใช้งานหน้า Console ทางไกลได้

3.8.1 เข้าไปที่หน้า **Browse > Advanced > Secure Shell** และติ๊กที่ช่อง **Enable Secure Shell** ในช่อง SSH Port เว้นว่างไว้โดย default จะเป็น Port 22 และกด Save



รูปที่ 3. 41 การเปิดใช้งาน SSH Service

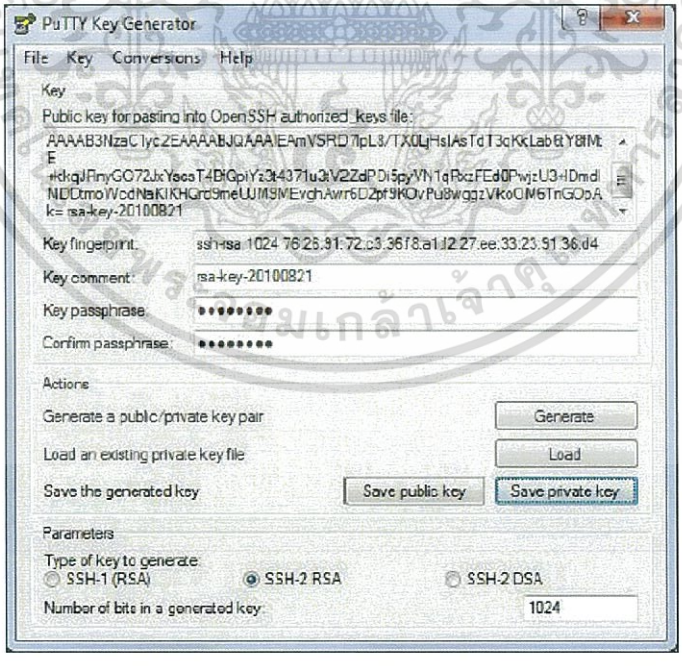
3.8.2 หลังจากทำการเปิด SSH Service ของ Pfsense แล้วนั้นเราจะทำการสร้าง RSA Key สำหรับการเข้าใช้งานหน้า console ของ Pfsense ผ่านโปรแกรม Putty โดยเริ่มจากทำการดาวน์โหลดโปรแกรม Puttygen และ Putty จาก http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html และทำการติดตั้งลงบนเครื่อง

For Windows on Intel x86

PuTTY:	putty.exe	(or by FTP)	(signature)
PuTTYtel:	puttytel.exe	(or by FTP)	(signature)
PSCP:	pscp.exe	(or by FTP)	(signature)
PSFTP:	psftp.exe	(or by FTP)	(signature)
Plink:	plink.exe	(or by FTP)	(signature)
Pageant:	pageant.exe	(or by FTP)	(signature)
PuTTYgen:	puttygen.exe	(or by FTP)	(signature)

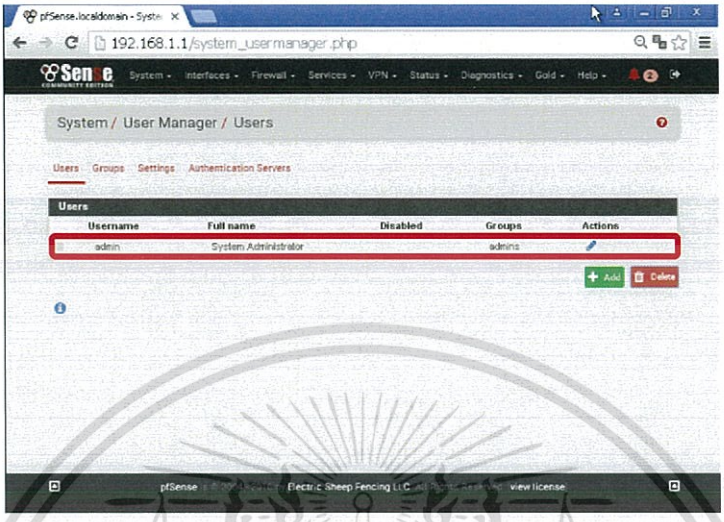
รูปที่ 3. 42 ดาวน์โหลด PuTTY และ PuTTYgen

3.8.3 เปิดโปรแกรม PuTTYgen คลิก generate และใส่ Key passphrase เป็น pfsense (optional) หรือใส่เป็นค่าอื่นก็ได้ หลังจากนั้นคลิก save private key และตั้งชื่อไฟล์เป็น Myprivatekey.ppk



รูปที่ 3. 43 สร้าง RSA Key

3.8.4 เข้าไปที่หน้าเว็บ pfsense ไปที่ **System > User Management > Users** ที่แถบของ Admin ในส่วนของ Actions เลือก **Edit user**

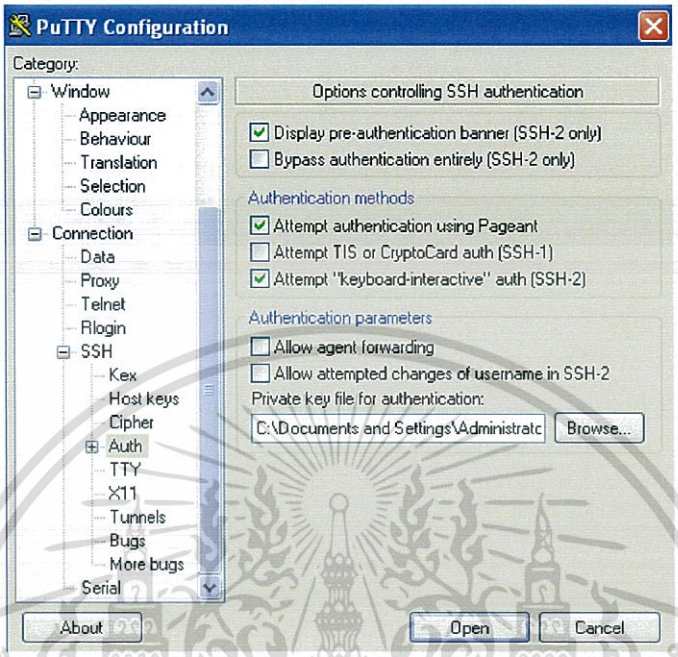


รูปที่ 3. 44 หน้าของ User management

3.8.5 เลื่อนลงมาที่แถบล่างสุดในส่วนของ Authorized SSH keys ให้ copy key ที่ได้จากการ generate มาใส่ไว้ในส่วนนี้และพิมพ์ ssh-rsa ไว้ข้างหน้าโดยข้อความที่ copy มานั้นให้นำมาแค่ส่วน public line โดยเปิดไฟล์ myprivatekey.ppk โดยใช้โปรแกรม Notepad

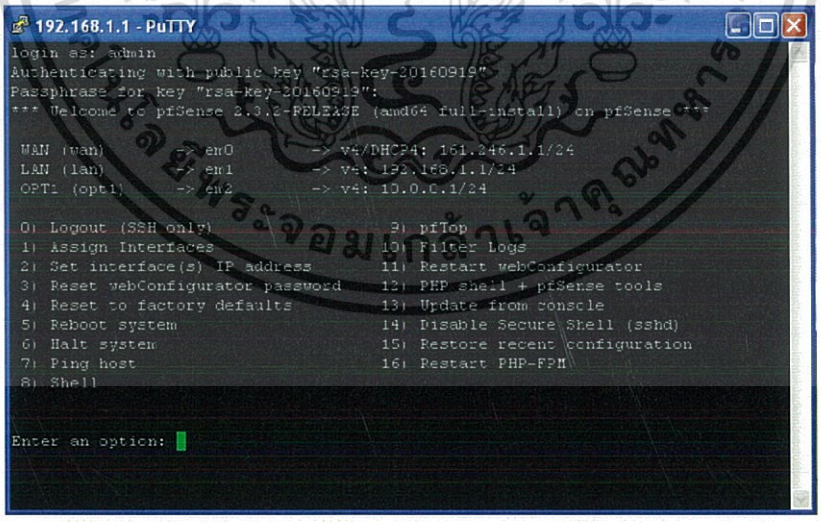
รูปที่ 3. 45 เพิ่ม Authorzied SSH Keys

3.8.6 ทดสอบการทำงาน SSH ด้วย PuTTY โดยใส่เลขไอพีแอดเดรสของ Pfsense คือ 192.168.1.1 และเพิ่มไฟล์ myprivatekey.ppk เพื่อจะข้ามส่วนของการใส่ password ใน SSH



รูปที่ 3. 46 เพิ่มไฟล์ myprivatekey.ppk

3.8.7 เข้า Pfsense ผ่าน PuTTY



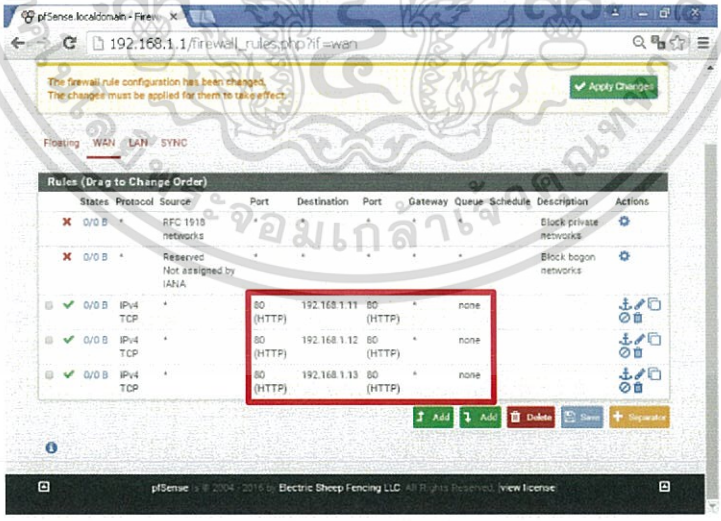
รูปที่ 3. 47 ทดสอบการทำงานผ่าน SSH

3.9 ตั้งค่า Firewall rule

ก่อนที่เราจะทำการตั้งค่า Firewall rule นั้น เราจะมาทำความรู้จักกับ Aliases Aliases คือคำสั้นๆที่ใช้ในการอ้างอิงกลุ่มของ IP, Port หรือ Network ต่างๆ ในการจัดการกับ Rule ต่างๆบน Firewall เป็นเรื่องที่ค่อนข้างจะซับซ้อนและละเอียดอ่อน ในระบบเล็กๆนั้นอาจมีไอพีแอดเดรสแค่ไม่กี่เบอร์เราอาจจะไม่ใช้ Aliases ได้ ถ้าระบบเราใหญ่ขึ้นแล้วเราไม่ใช้ Aliases จะทำให้เกิดความสับสนอย่างมากต่อโปรโตคอลค้นหาเส้นทางดูแลระบบ (Administrator) อาจจะส่งผลให้เกิดการคอนฟิกที่ผิดพลาด เป็นช่องโหว่ระบบที่ทำให้ Hacker อาศัยช่องโหว่นี้มาโจมตีระบบเรา ซึ่งแบบนี้ไม่ดีแน่ เราจะใช้ Aliases เพื่อลดความยุ่งยากในการบริหารจัดการ Rule บน Firewall ลงไป จากโครงงานนี้เราจะมี DMZ Zone ซึ่งเป็นโซนที่มีเซิร์ฟเวอร์ที่ภายนอกสามารถเข้าถึงได้อยู่ เราจะทำการรวมเซิร์ฟเวอร์ในโซนนี้ให้เป็น Aliases เดียวกันคือพวก Web server และ Mail server ในที่นี้เรามีไอพีแอดเดรสใน DMZ ดังนี้

Server name	IP Address / Subnet mask
Web Server 1	192.168.1.11 / 255.255.255.0
Web Server 2	192.168.1.12 / 255.255.255.0
Mail Server	192.168.1.13 / 255.255.255.0

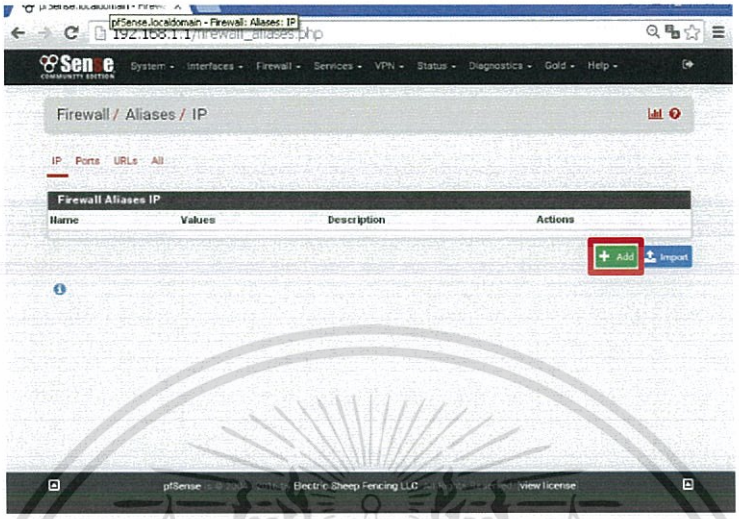
ตารางที่ 3.2 หมายเลขไอพีแอดเดรสของ DMZ



รูปที่ 3. 48 ก่อนทำการเพิ่ม Aliases

จากรูป 3.48 กรณีที่เรามีเซิร์ฟเวอร์มากกว่า 1 ตัวนั้นเราจำเป็นต้องอ้างอิงไอพีแอดเดรสของทุกตัว แต่ถ้าเราใช้งาน Aliases ก็ไม่จำเป็นที่จะต้องอ้างอิงทั้งหมดนั่นเอง

3.9.2 ต่อไปเราจะทำการใช้ Aliases ในการรวมเซิร์ฟเวอร์ทั้งสามตัวนี้ เพื่อง่ายต่อการเปลี่ยนแปลงหรือแก้ไข rules ของ Pfsense เข้าไปที่ Firewall > Aliases > Add ดังรูป



รูปที่ 3. 49 หน้าต่างเพิ่ม Aliases

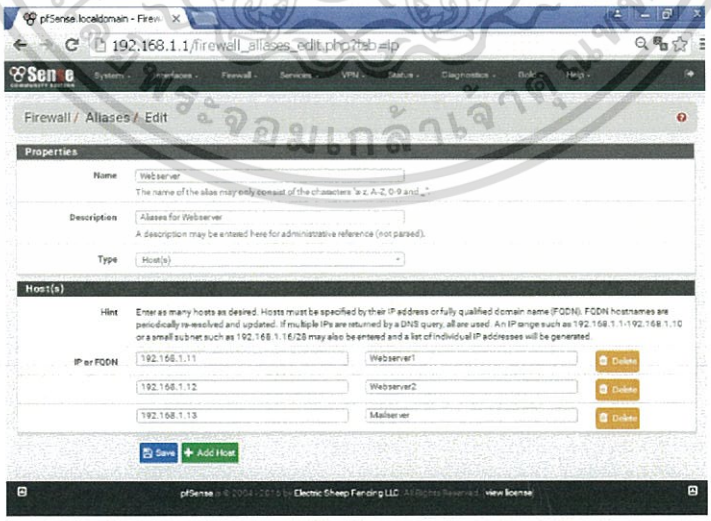
3.9.3 หลังจากเข้ามาแล้วนั้นให้ใส่ค่าดังรูปที่ 3.9.3 แล้วคลิก Save

Name : ตั้งชื่อสำหรับ Aliases

Description : ใส่คำอธิบาย

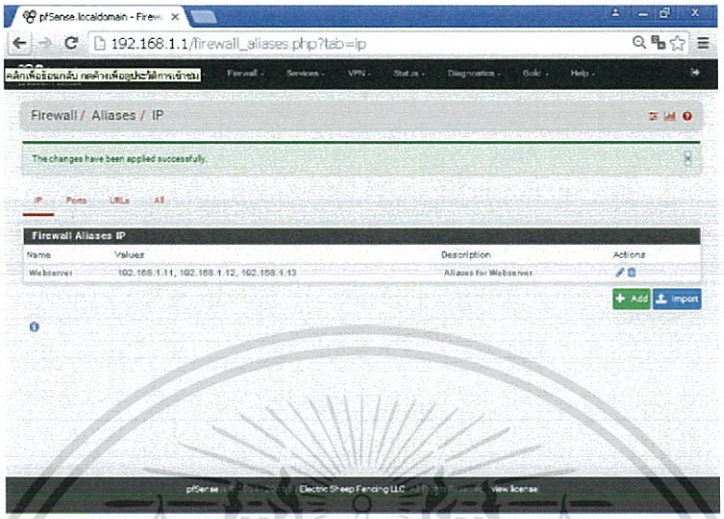
Type : ประเภทของ Aliases ในที่นี้ใช้เป็น host สามารถเพิ่มไอพีได้โดยการคลิกปุ่ม add host

Host(s) : เป็นรายการของไอพีแอดเดรสที่เราจะใช้ในกลุ่ม Aliases นี้



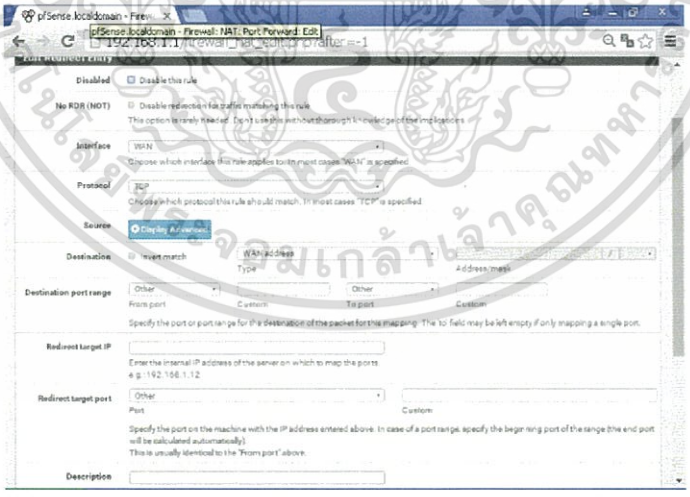
รูปที่ 3. 50 การตั้งค่า Aliases ให้กับเซิร์ฟเวอร์

3.9.4 หน้าต่างหลังจากทำการเพิ่ม Aliases แล้ว เราสามารถนำ Aliases ไปใช้ในแต่ละ rules ต่างๆได้อย่างสะดวก



รูปที่ 3. 51 เพิ่ม Aliases เสร็จสิ้น

3.9.5 หลังจากทำการเพิ่ม Aliases ให้กับ Webserver ก็จะทำกับกลุ่มของยูสเซอร์ด้วยตามขั้นตอนที่ 3.9.2-3.9.4 หลังจากนั้นเราจะทำ NAT port forward โดยจะทำการฟอเวิดทุกๆรีเควสที่เป็นเว็บรีเควส(HTTP) ไปยังเว็บเซิร์ฟเวอร์ โดยเริ่มจากเข้าไปที่ Firewall > NAT > Add



รูปที่ 3. 52 หน้าต่างตั้งค่า NAT port forward

3.9.6 ในการตั้งค่า NAT port forward ให้ตั้งค่าดังต่อไปนี้ และคลิก Save and Apply

Interface > WAN

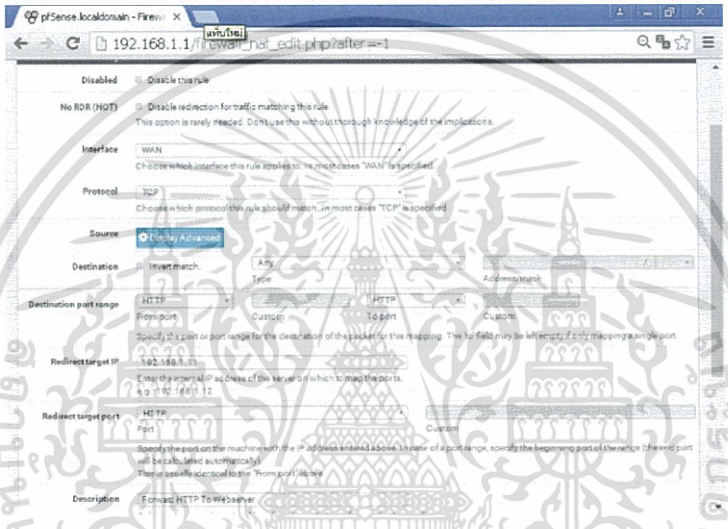
Protocol > TCP

Destination > Any

Destination port range > HTTP (From and To)

Redirect target IP > 192.168.1.11

Description > Forward HTTP to Webserver



รูปที่ 3. 53 ตัวอย่างการตั้งค่า NAT port forward

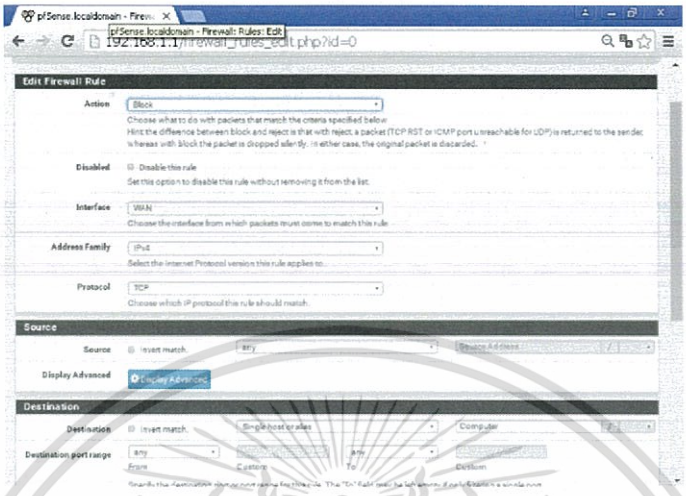
3.9.7 หลังจากที่เราเพิ่ม Aliases และ NAT port forward แล้วนั้น สุดท้ายจะเป็นการเพิ่ม firewall rules ซึ่งถือเป็นส่วนสำคัญในการทำงานของ Pfsense โดยมี Requirements ดังนี้

- อนุญาตให้ LAN เชื่อมต่อกับ WAN ได้
- อนุญาตให้ LAN บางส่วนเชื่อมต่อกับ WAN ได้
- บล็อค WAN ในการเข้าถึง LAN
- อนุญาตให้ LAN เชื่อมต่อกับ DMZ ได้เพียง HTTP
- อนุญาตให้ WAN เชื่อมต่อกับ DMZ ได้เพียง HTTP
- บล็อค DMZ ในการเข้าถึง LAN

จากกฎข้างต้นทั้งหมด สามารถทำการตั้งค่าได้ดังนี้ ไปที่ Firewall > rules > add

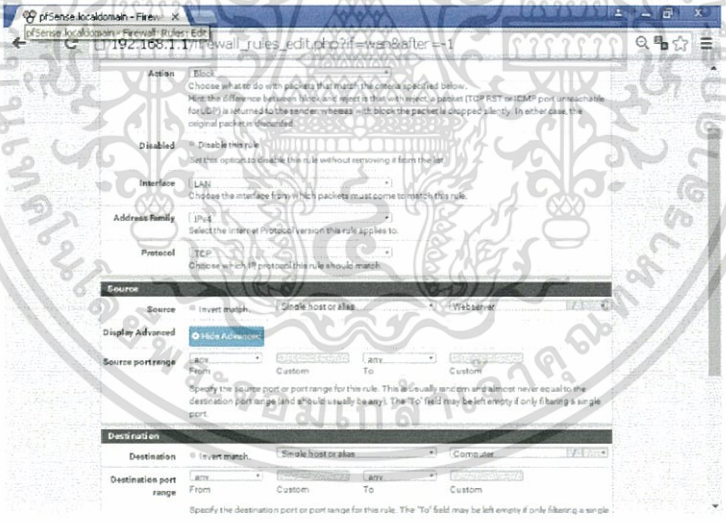
ในการกำหนด rules นั้นควรนำการบล็อคไว้บนสุดเสมอ ดังนี้

-บล็อค WAN ในการเข้าถึง LAN และตั้งค่าดังรูป



รูปที่ 3. 54 ตั้งค่า Block WAN to LAN

-บล็อค DMZ ในการเข้าถึง LAN ตั้งค่าดังรูป

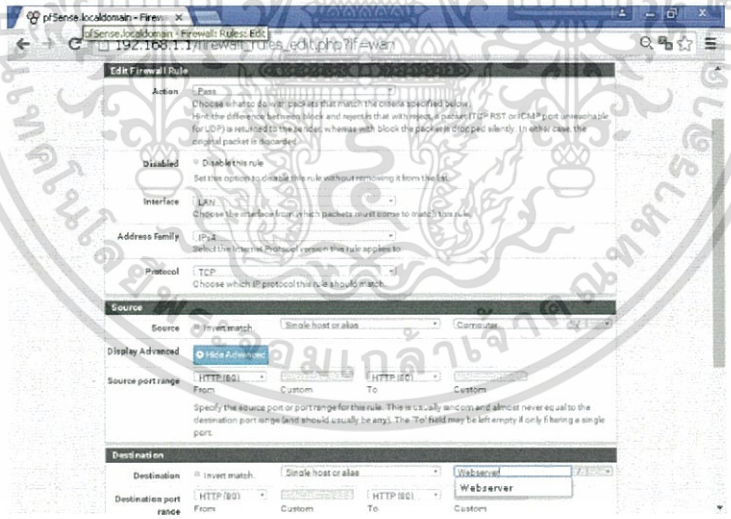


รูปที่ 3. 55 Block DMZ to LAN

-อนุญาตให้ WAN เชื่อมต่อกับ DMZ ได้

รูปที่ 3. 56 Allow WAN to DMZ

-อนุญาตให้ LAN เชื่อมต่อกับ DMZ ได้



รูปที่ 3. 57 Allow LAN to DMZ

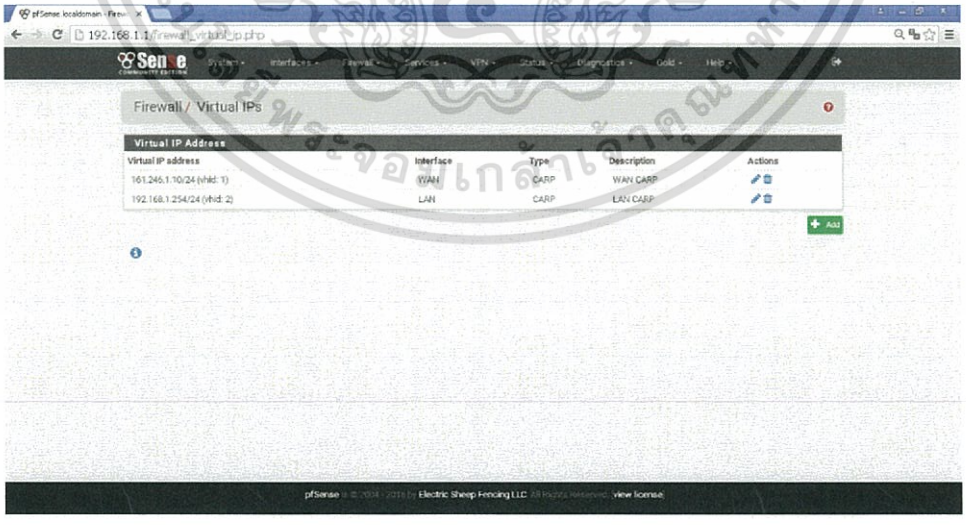
-อนุญาต LAN ทั้งหมดสำหรับทุกกฎ

รูปที่ 3. 58 Allow LAN to any rules

3.10 ติดตั้ง Failover

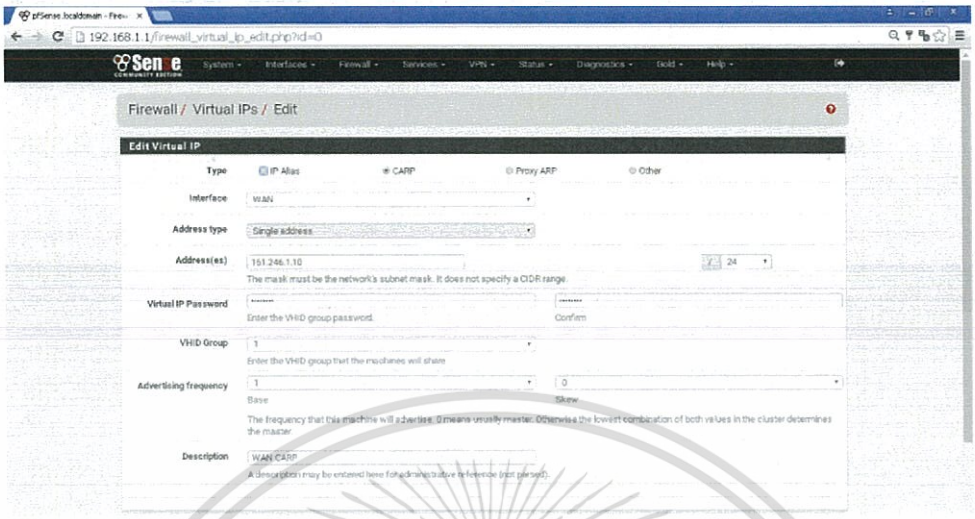
การทำ Failover นั้นมีจุดประสงค์เพื่อเพิ่ม High Availability ของการทำงานเนื่องจากอุปกรณ์ใดๆนั้นสามารถเกิดความผิดพลาดได้และอาจทำให้ระบบเครือข่ายเสียหายไปด้วย จึงต้องมีการสำรองในกรณีที่อุปกรณ์ตัวใดๆนั้นเสียหายลงไป จึงเกิดแนวคิดในการทำ Failover ขึ้นมานั่นเอง

3.10.1 เริ่มจากสร้าง Virtual IP address โดยไปที่ Firewall > Virtual IPs



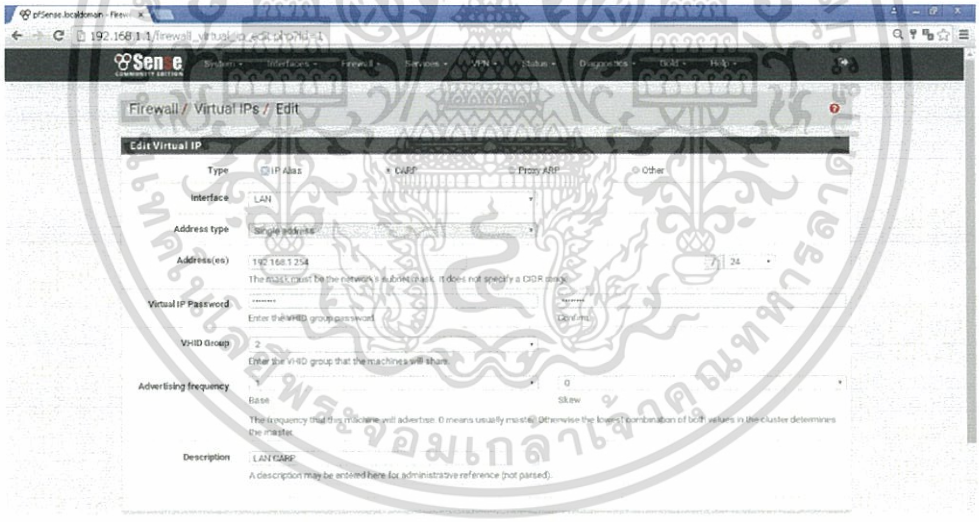
รูปที่ 3. 59 สร้าง Virtual IPs

3.10.2 สร้าง Virtual IP ให้กับอินเตอร์เฟส WAN โดยทำการกำหนดค่าต่างๆดังภาพ



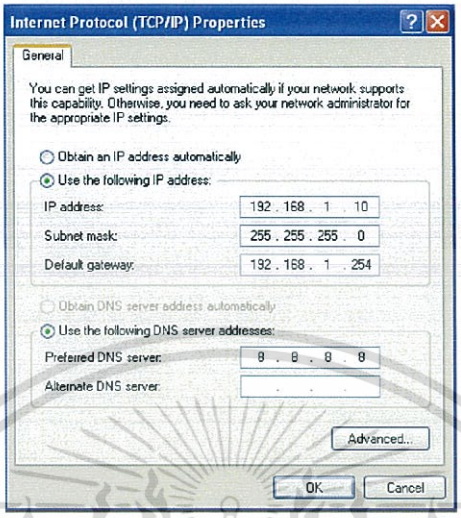
รูปที่ 3. 60 ตั้งค่า Virtual IP ของ WAN

3.10.3 สร้าง Virtual IP ให้กับอินเตอร์เฟส LAN โดยทำการกำหนดค่าต่างๆดังภาพ



รูปที่ 3. 61 ตั้งค่า Virtual IP ของ LAN

3.10.4 หลังจากที่เราทำการสร้าง Virtual IP เสร็จแล้วนั้นที่คอมพิวเตอร์จะต้องไปเปลี่ยน default gateway ให้เป็น Virtual IP ของ LAN คือ 192.168.1.254



รูปที่ 3. 62 ตั้งค่า default gateway เป็น Virtual IP LAN

3.10.5 หลังจากนั้นไปที่หน้าต่าง System > High Avail. SYNC ตั้งค่าดังนี้

Synchronize Interface > SYNC

pfsync Synchronize Peer IP > 10.0.0.2 (ไอพีแอดเดรสของ Pfsense-2)

Synchronize Config to IP > 10.0.0.2

รูปที่ 3. 63 หน้าต่าง High Avail. SYNC

3.10.6 ตั้งค่า High Avail. SYNC (ต่อ)

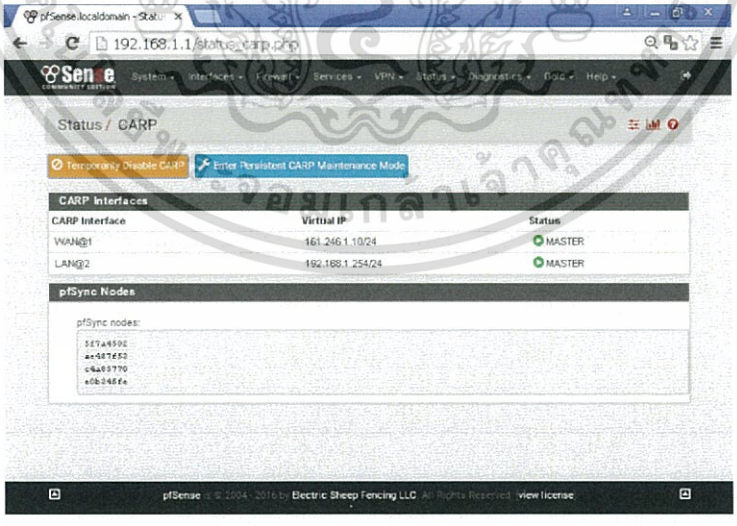
Remote System Username > admin (username webconfig pfsense-2)

Remote System Password > pfsense (password webconfig pfsense-2)

Select option to sync > check box ดังรูป 3.10.6

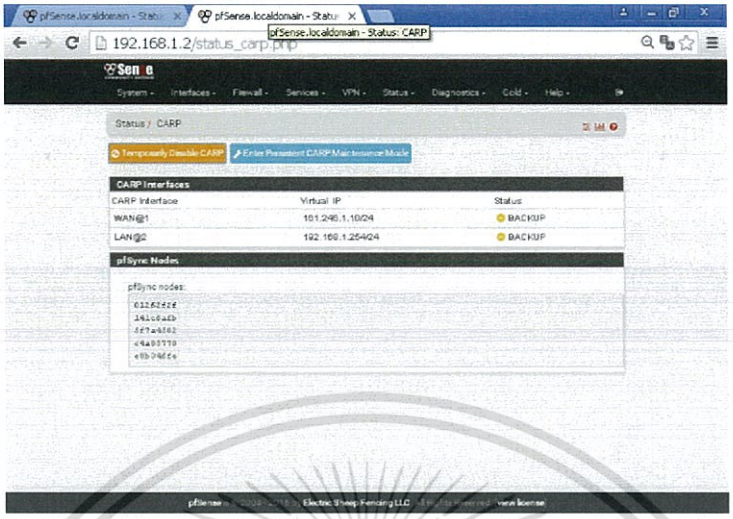
รูปที่ 3. 64 ตั้งค่า High Availa. Sync

3.10.7 ไปที่หน้าต่าง Status > CARP (failover) จะสังเกตเห็นว่าตอนนี้มีสถานะเป็น Master แล้วนั่นเอง และทำการตั้งค่าเดียวกันกับ Pfsense-2 สถานะที่ได้จะต้องเป็น Backup



รูปที่ 3. 65 สถานะของ CARP (failover)

3.10.8 สถานะ Failover ของ Pfsense-2

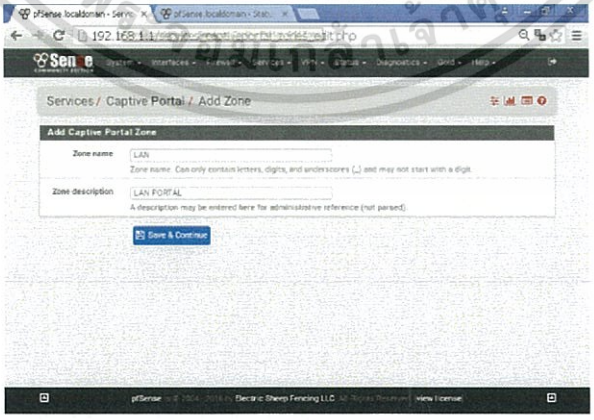


รูปที่ 3. 66 สถานะ Failover ของ Pfsense-2

3.11 สร้าง Captive Portal

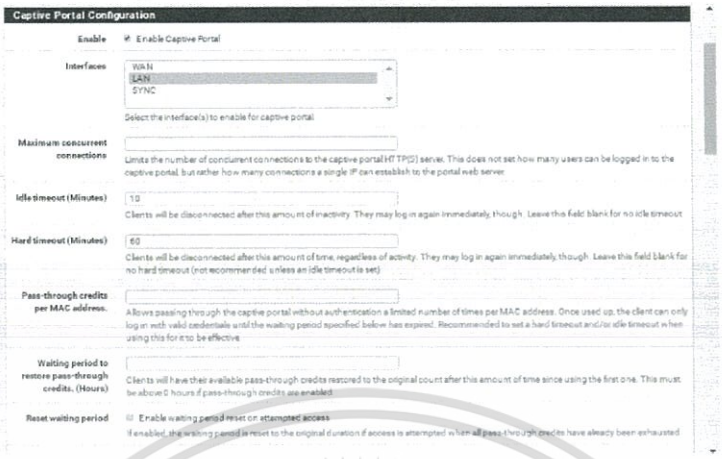
เพื่อเพิ่มความปลอดภัยให้กับระบบเครือข่าย ควรจะมีการยืนยันตัวตนก่อนการเข้าใช้งานเครือข่ายภายในนั่นเอง Captive Portal นั้นเป็นเสมือนหน้าต่างที่ต้องมีการยืนยันตัวตนก่อนการเข้าใช้งานเครือข่ายโดยสามารถเพิ่มข้อมูลของ user ที่สามารถเข้าใช้งานได้จาก local database หรือ Active Directory โดยจะสามารถทำการกำหนดเวลาการเข้าใช้งาน สิทธิ์ในการเข้าถึงอินเตอร์เนตหรือแหล่งข้อมูลต่างๆของเครือข่ายได้ด้วย สามารถทำได้ดังนี้

3.11.1 ไปที่หน้าต่าง Service > Captive Portal > Add



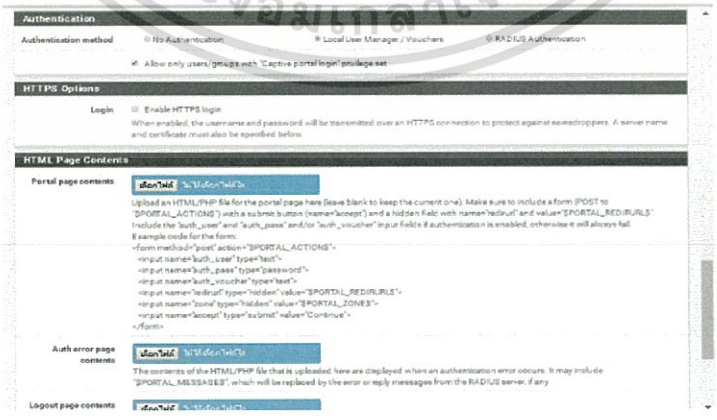
รูปที่ 3. 67 Zone name และ Description

3.11.2 ตั้งค่า Captive Portal ในการทำงาน



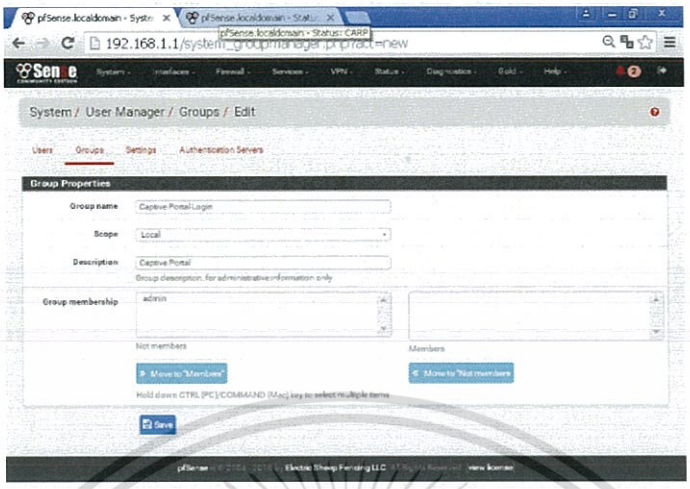
รูปที่ 3. 68 ตั้งค่า Captive Portal

รูปที่ 3. 69 ตั้งค่า Captive Portal (2)



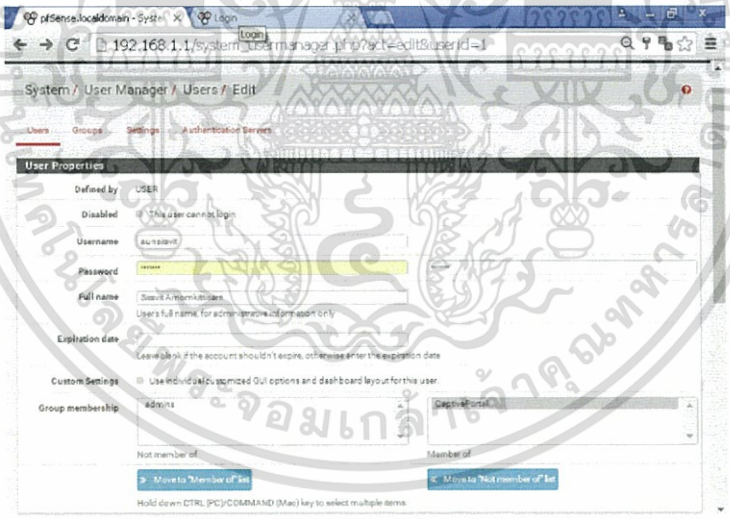
รูปที่ 3. 70 ตั้งค่า Captive Portal (3)

3.11.5 ไปที่ System > User manager > Groups < Add และทำการตั้งค่าดังรูป



รูปที่ 3. 71 ตั้งค่า Groups สำหรับ Captive Portal

3.11.6 เพิ่ม user ใน local database สำหรับการ login บน Captive Portal ในส่วนของ Group membership นั้นให้เพิ่มไปเป็น CaptivePortal



รูปที่ 3. 72 เพิ่ม user ใน local database

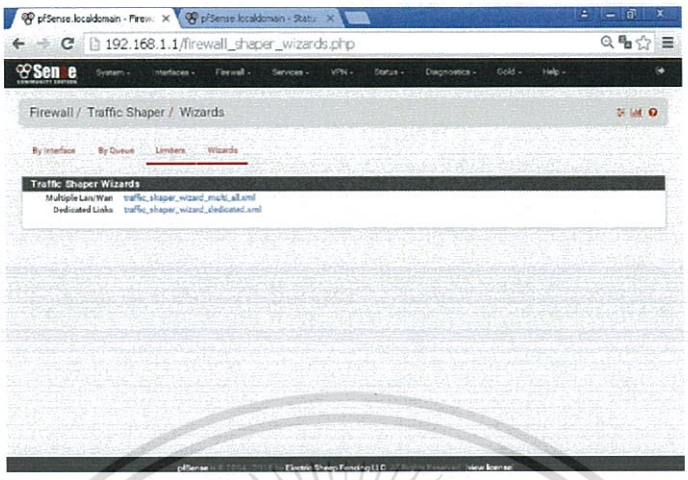
3.11.7 หลังจากทำการตั้งค่าทั้งหมดเสร็จสิ้นแล้ว ให้ลองเข้า browser จะพบว่าต้องทำการ login ก่อนถึงจะสามารถเข้าใช้งานอินเตอร์เนตได้ ดังรูป

รูปที่ 3. 73 หน้า login ของ Captive Portal

3.12 ใช้งาน Traffic-Shaping (QoS, Quality of Service)

Traffic-Shaping หรือเรียกอีกอย่างหนึ่งว่า Quality of Service เป็นการจัดลำดับความสำคัญของแพ็คเกตภายในระบบเครือข่าย การจัดลำดับความสำคัญของแพ็คเกตในเครือข่ายนั้นเป็นการระบุว่าแพ็คเกตไหนมีความสำคัญมากกว่าแพ็คเกตอื่นๆ ยกตัวอย่างเช่น โปรโตคอลค้นหาเส้นทางดูแลระบบเครือข่ายอาจต้องการให้ VoIP แพ็คเกตนั้นมีความสำคัญมากที่สุด เนื่องจากระหว่างการคุยโทรศัพท์นั้นไม่ควรจะมีการดรอปของแพ็คเกตหรือแพ็คเกตควรจะได้รับผลกระทบน้อยที่สุดขณะที่ทราฟฟิคภายในสูงมาก นอกจากนี้ VoIP แพ็คเกตนั้นจำเป็นต้องการใช้ throughput เพียง 100 kbps เท่านั้นก็เพียงพอต่อการใช้งานและนี่คือกรณีศึกษาการทำ QoS ให้กับระบบ VoIP ในส่วนต่อไปจะเป็นการคอนฟิก QoS ใน Pfsense โดยจะมีการให้ความสำคัญกับ Remote Access และ VoIP เป็นลำดับแรก ทำได้ดังนี้

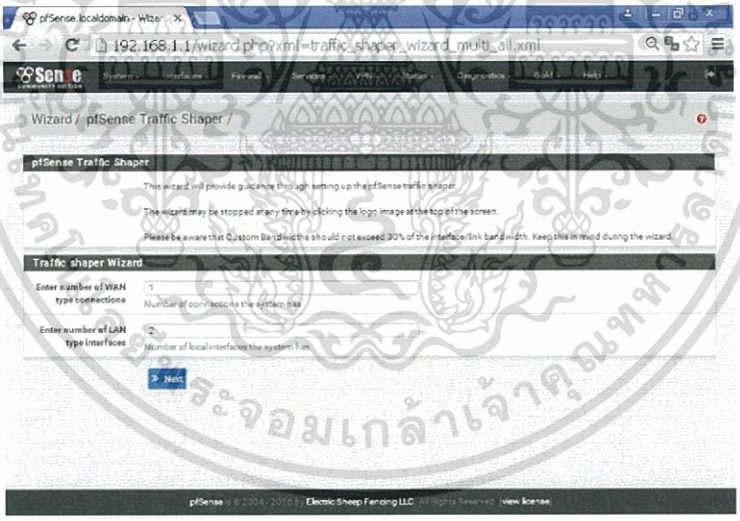
3.12.1 ไปที่ Firewall > Traffic Shaper > Wizards > Multiple LAN/WAN ดังรูป



รูปที่ 3. 74 หน้าต่าง Traffic Shaper

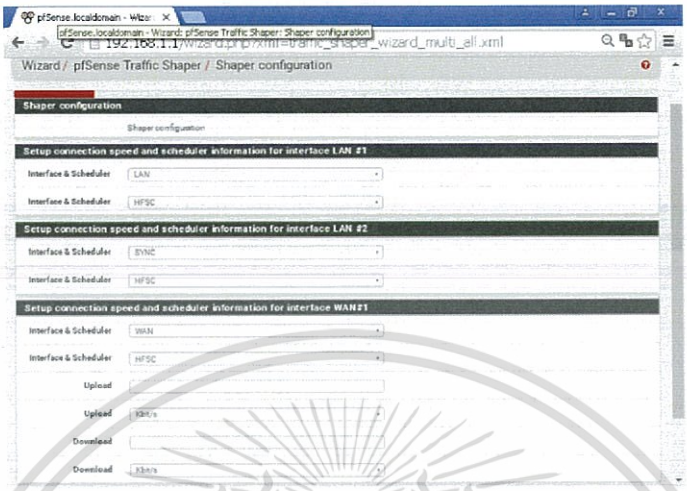
3.12.2 ตั้งค่าจำนวนของอินเตอร์เฟส WAN และ LAN

Enter number of WAN = 1 และ Enter number of LAN = 2 ดังรูป



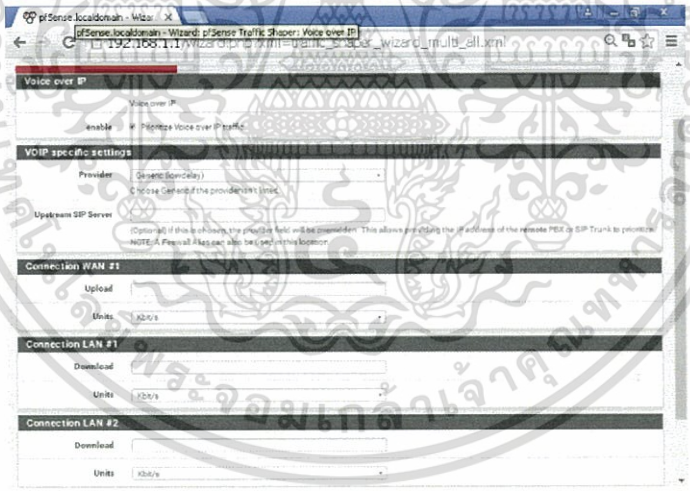
รูปที่ 3. 75 ตั้งค่าจำนวนอินเตอร์เฟส LAN/WAN สำหรับ Traffic-Shaper

3.12.3 ตั้งค่าแบนวิทธ์เบื้องต้นของแต่ละอินเตอร์เฟส ในส่วนของช่อง Upload และ Download นั้นให้ใส่ความเร็วของอินเทอร์เน็ตของเราที่ใช้งาน



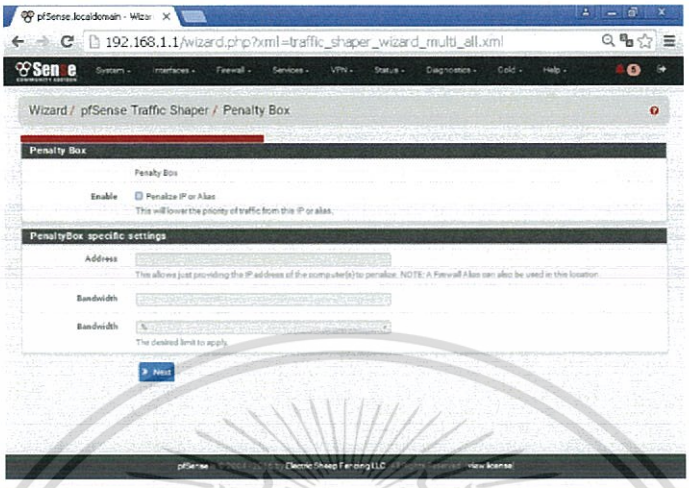
รูปที่ 3. 76 ตั้งค่าแบนวิทธ์เบื้องต้น

3.12.4 ตั้งค่า QoS สำหรับแพ็คเกต Voice over IP



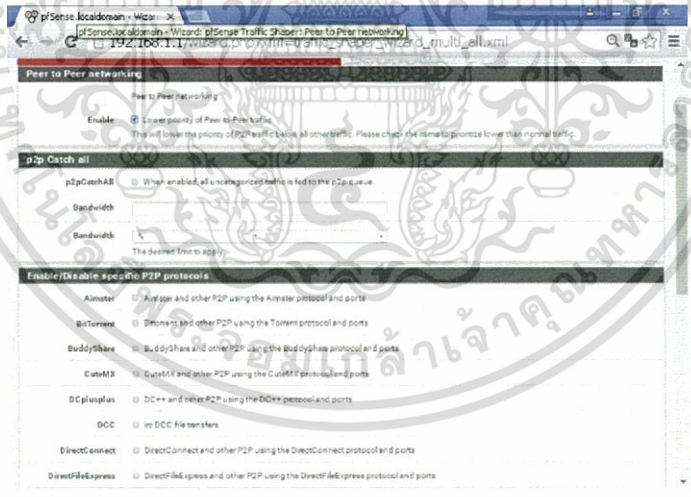
รูปที่ 3. 77 การตั้งค่าสำหรับ VoIP

3.12.5 Penalize IP box คือการลดระดับความสำคัญของแต่ละไอพีแอดเดรสโดย สามารถเพิ่มไอพีแอดเดรสที่เราต้องการได้ในช่องของ Address และติ๊กถูกที่ช่อง Enable



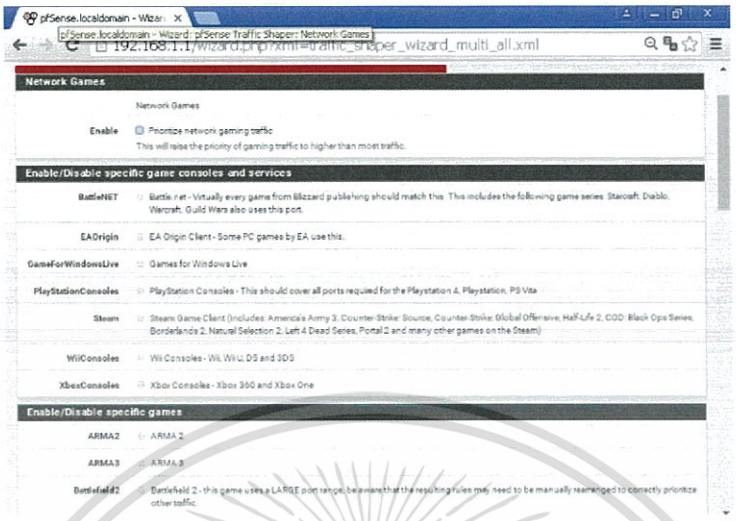
รูปที่ 3. 78 การตั้งค่า Penalty box

3.12.6 ในกรณีที่เราต้องการจำกัดการใช้งาน Bittorrent ให้ติ๊กที่ช่อง Lower priority of Peer-Peer traffic



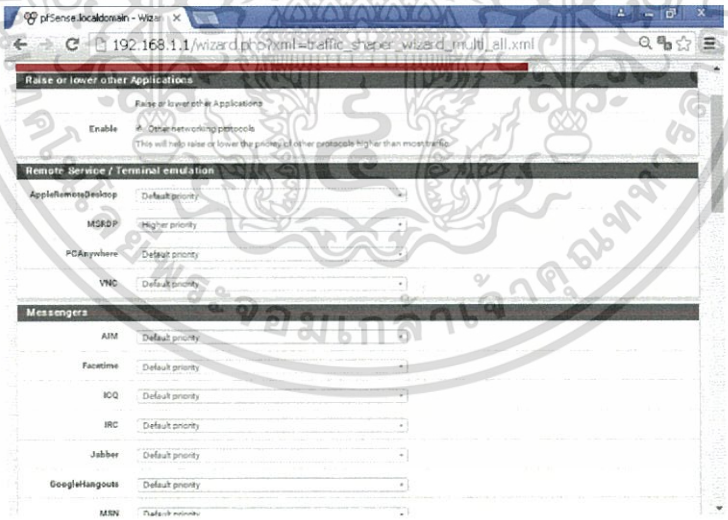
รูปที่ 3. 79 จำกัดการใช้งาน Bittorrent

3.12.7 กำหนดลำดับความสำคัญให้กับแพ็คเก็ตของแต่ละหมวดการใช้งาน



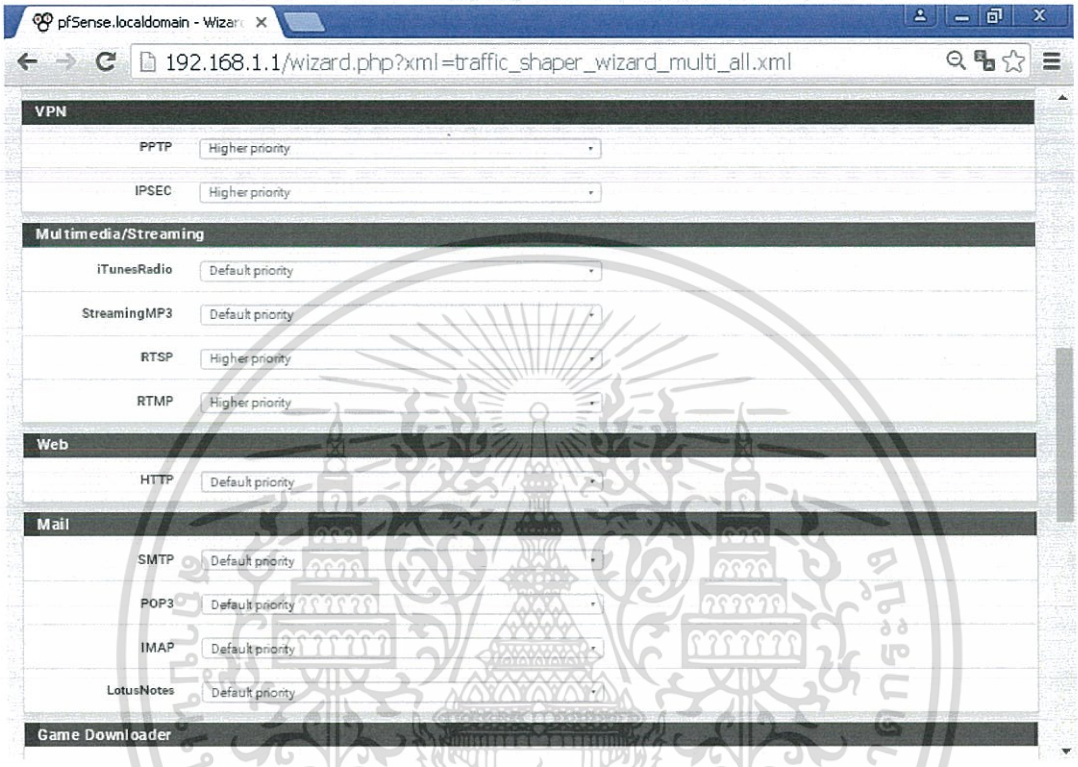
รูปที่ 3. 80 จัดลำดับความสำคัญของแพ็คเก็ตหมวดเกม

3.12.8 กำหนดลำดับความสำคัญให้กับแต่ละเน็ตเวิร์กโปรโตคอลและโปรแกรมแชทต่างๆ ในที่นี้จะเปลี่ยน MSRDP ให้เป็น Higher Priority เนื่องจากเป็นโปรโตคอลสำหรับควบคุมคอมพิวเตอร์ระยะไกลควรจะมีความเสถียรมากที่สุด



รูปที่ 3. 81 จัดลำดับความสำคัญของแต่ละโปรโตคอล

3.12.9 จัดลำดับความสำคัญให้กับการ VPN และมัลติมีเดียประเภทที่เป็นเรียลไทม์คอมมูนิเคชั่น ในส่วนของ VPN ให้เปลี่ยนเป็น Higher priority ทั้งหมดและMultimedia/Streaming เปลี่ยนเป็น High priority ที่ RTSP และ RTMP (Streaming and Message) หลังจากนั้นกด Next และ Finished



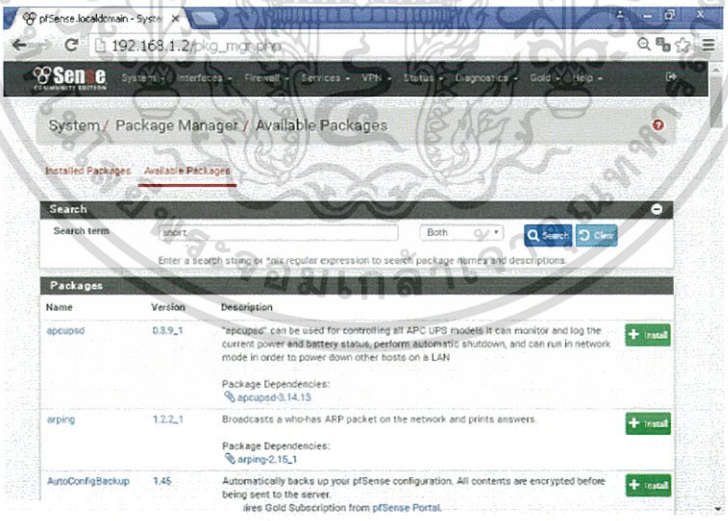
รูปที่ 3. 82 จัดลำดับความสำคัญของแต่ละเซอร์วิส

3.13 การใช้งาน SNORT เพื่อเพิ่มประสิทธิภาพในการทำงานของ Pfsense

3.13.1 Snort คือซอฟท์แวร์สำหรับตรวจจับโปรโตคอลค้นหาเส้นทางบุกรุกและป้องกันในระบบเครือข่าย หรือที่เรียกว่า Network Intrusion Detection System & Prevention System ซึ่งเป็นซอฟท์แวร์ที่เป็น Open Source สามารถทำให้นำมาใช้งานได้โดยไม่เสียค่าใช้จ่าย โดยการที่นำ SNORT มาใช้งานควบคู่ไปกับ Pfsense นั้นจะเป็นการเพิ่มความแข็งแกร่งและความปลอดภัยของระบบมากยิ่งขึ้น

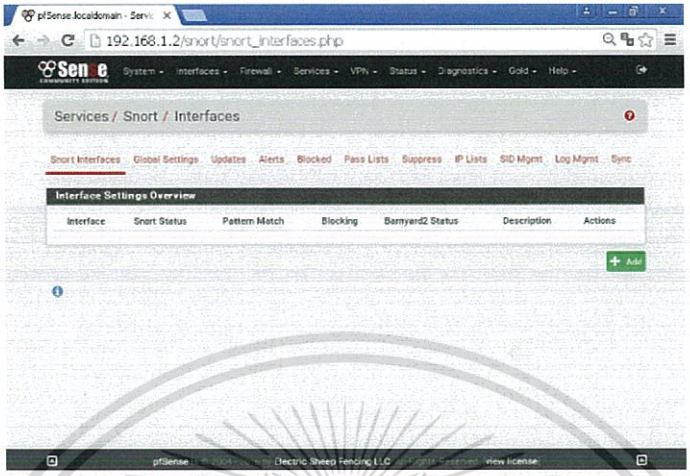
รูปที่ 3. 83 โลโก้ของ SNORT

3.13.2 ติดตั้ง SNORT โดยเข้าไปที่แถบ System > Package Manager > Available Packages ค้นหา snort แล้วกด Install ดังรูป



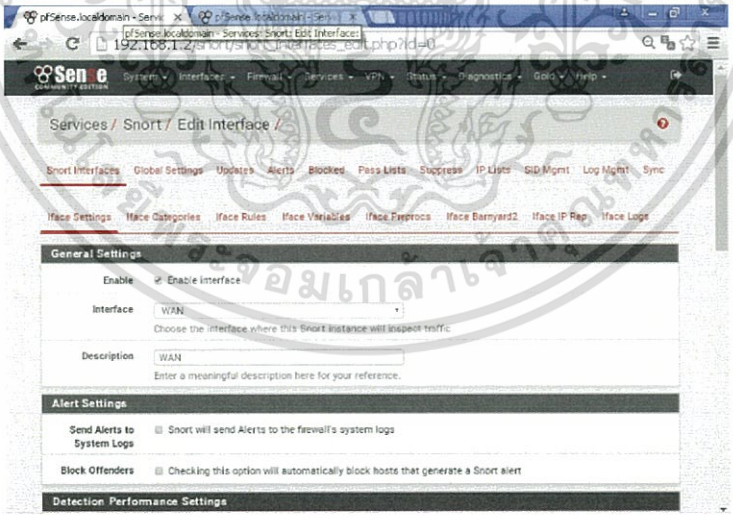
รูปที่ 3. 84 ติดตั้ง SNORT บน Pfsense

3.13.3 ไปที่ Service > Snort เพิ่มอินเตอร์เฟสที่จะใช้งาน SNORT โดยจะเป็น WAN และ LAN



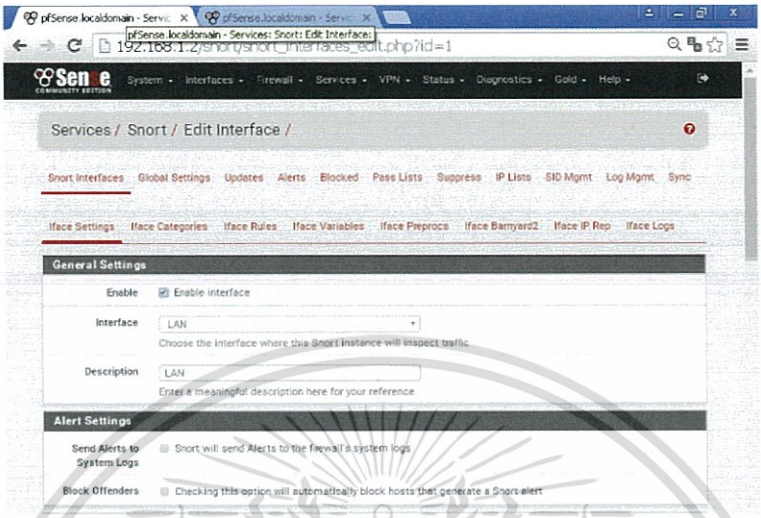
รูปที่ 3. 85 หน้าต่างของ SNORT

3.13.4 ติ๊กที่ Enable Interface และใส่ช่องของ Interface เลือกเป็น WAN หลังจากนั้นกด save



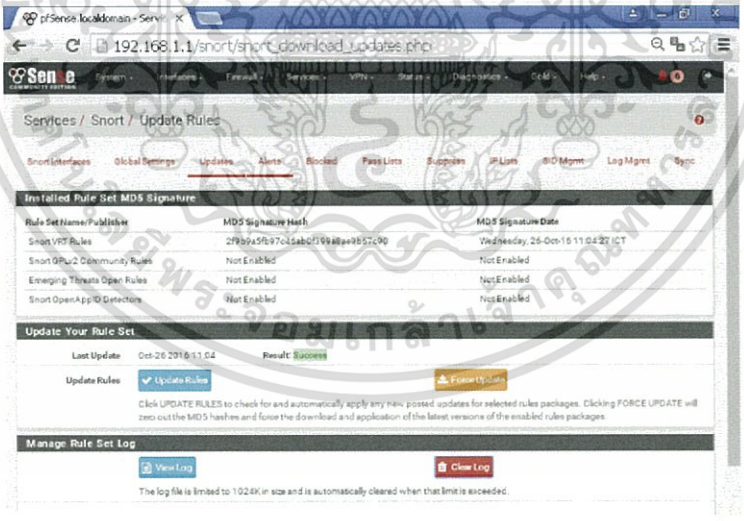
รูปที่ 3. 86 เพิ่มอินเตอร์เฟส WAN

3.13.5 ติ๊กที่ Enable Interface และใส่ช่องของ Interface เลือกเป็น LAN หลังจากนั้น กด save



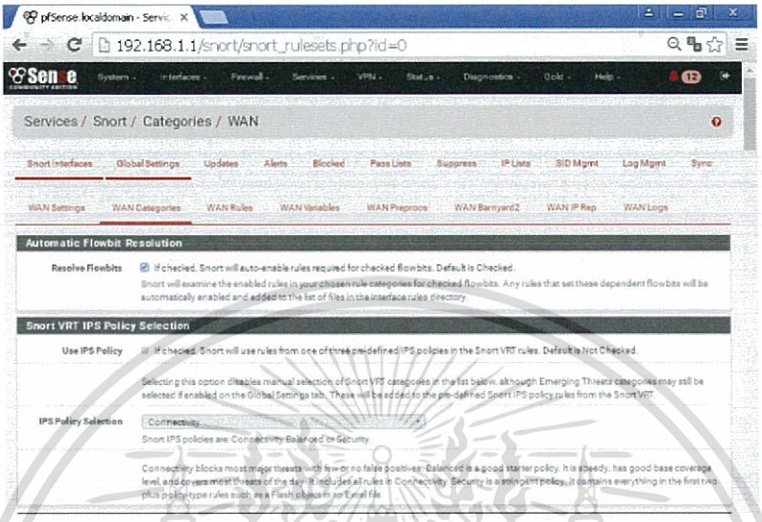
รูปที่ 3. 87 เพิ่มอินเตอร์เฟส LAN

3.13.6 อัพเดทข้อบังคับที่จะนำไปใช้ในการทำงาน โดยค่าเริ่มต้นนั้นจะยังไม่มีการดาวน์โหลดไว้ จึงจำเป็นที่จะต้องทำการดาวน์โหลดใหม่ โดยไปที่แถบ Updates และเลือก Update rules



รูปที่ 3. 88 การอัพเดทข้อบังคับสำหรับนำไปใช้งาน

3.13.7 หลังจากทำการอัพเดทข้อบังคับต่างๆของ SNORT สามารถไปเลือกใช้ข้อบังคับต่างๆได้ที่อินเตอร์เฟสที่เราต้องการ ตัวอย่างเช่นในอินเตอร์เฟส WAN โดยไปที่ WAN > WAN Categories ดังภาพ

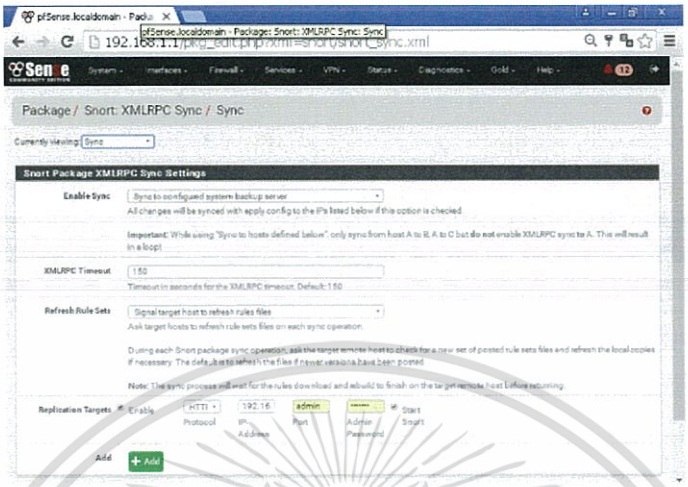


รูปที่ 3. 89 หน้าต่างการทำงานของ WAN Categories

3.13.8 รายการของข้อบังคับต่างๆที่สามารถนำไปใช้กับอินเตอร์เฟสใดๆที่ต้องการได้ ในตัวอย่างนี้จะเลือกข้อบังคับดังนี้ snort_botnet-cnc.rules, snort_ddos.rules, snort_scan.rules, snort_virus.rules

รูปที่ 3. 90 รายการของข้อบังคับต่างๆ

3.13.9 ในกรณีที่เราต้องต้องการให้ SNORT นั้นมีการแลกเปลี่ยนข้อมูลกันกับไฟร์วอลอีกตัวหนึ่งนั้นจะต้องมีการซิ้งค์ข้อมูลกัน โดยสามารถทำได้ดังนี้



รูปที่ 3. 91 หน้าต่างของการ SYNC SNORT

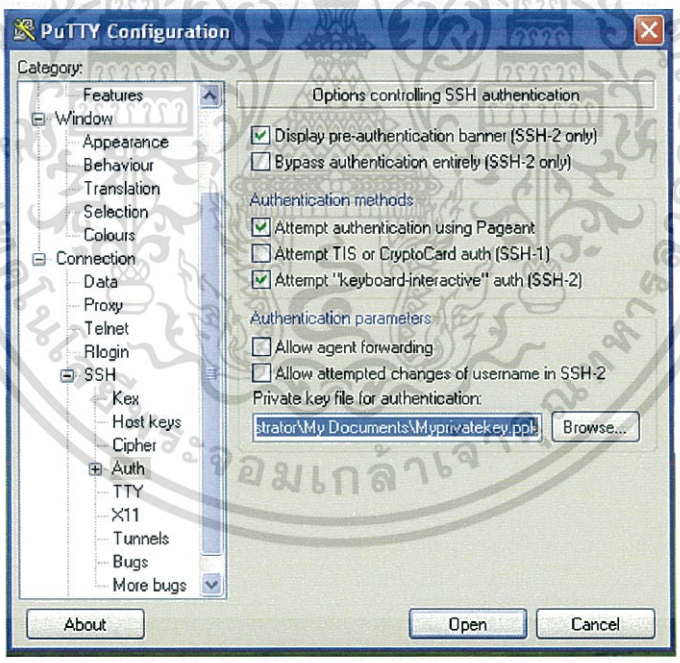
บทที่ 4

ผลการทดลอง

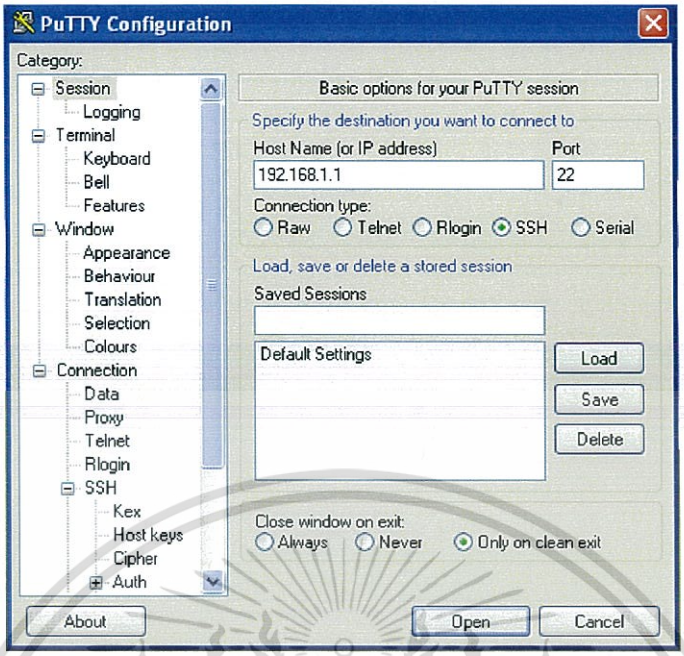
หลังจากที่ได้ทำการติดตั้งและตั้งค่าต่างๆให้กับ Pfsense แล้วนั้นจำเป็นจะต้องมีการทดสอบการทำงานของแต่ละฟีเจอร์เพื่อตรวจสอบว่าจะให้ผลลัพธ์ตรงตามความต้องการเพื่อประสิทธิภาพสูงสุดในการทำงาน โดยจะมีการตรวจสอบตามรายการดังนี้

1. การเข้าใช้งานผ่าน Secure Shell Service
2. การทำงานของข้อบังคับของไฟร์วอล
3. การทำงานของเฟลโอเวอร์
4. การทำงานของ Captive Portal
5. การทำงานของ Traffic-Shaping
6. การทำงานของ SNORT

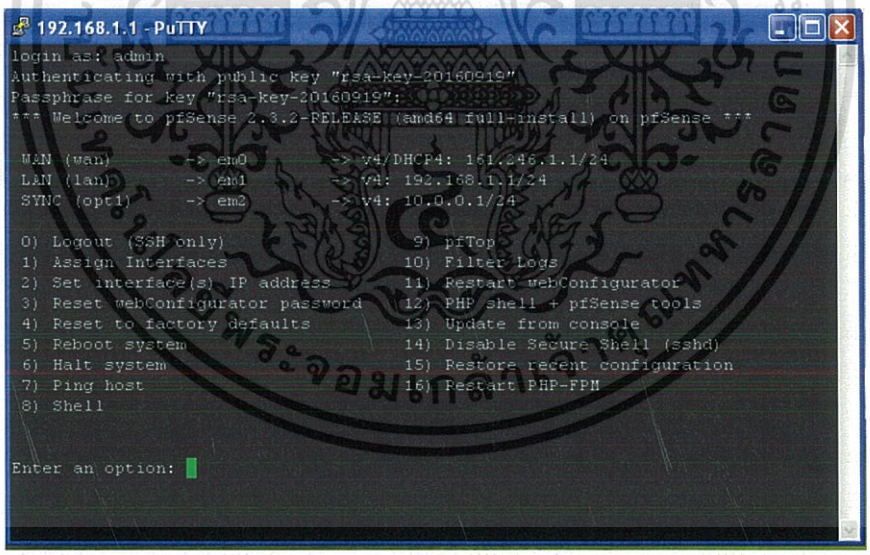
4.1 ทดสอบการเข้าใช้งานผ่าน Secure Shell Service



รูปที่ 4. 1 เพิ่มไพรเวทคีย์สำหรับ SSH



รูปที่ 4. 2 ใส่ไอพีแอดเดรสของ Pfsense

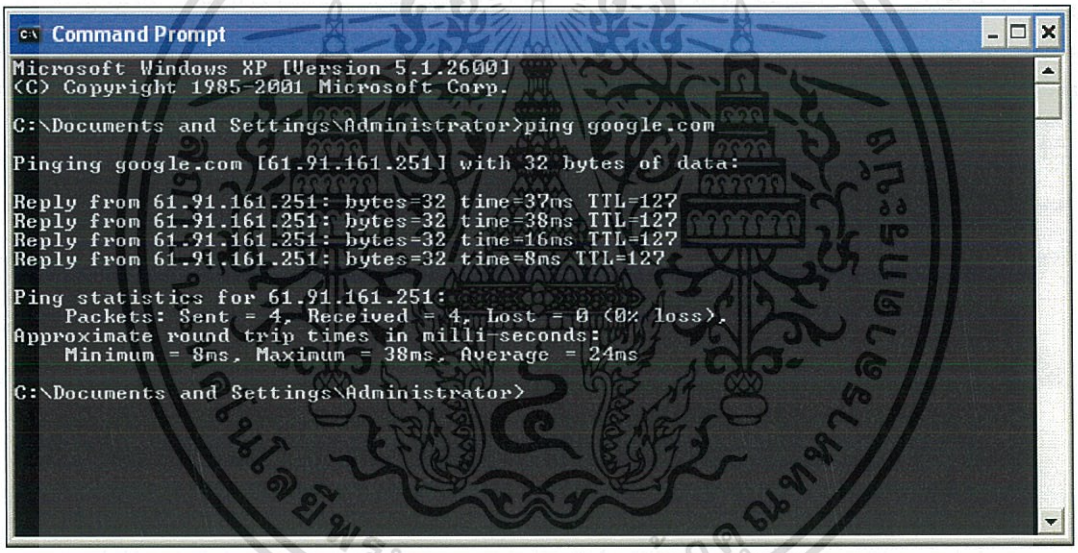


รูปที่ 4. 3 กรอกยูสเซอร์เนมและรหัสผ่านในการเข้าใช้งาน

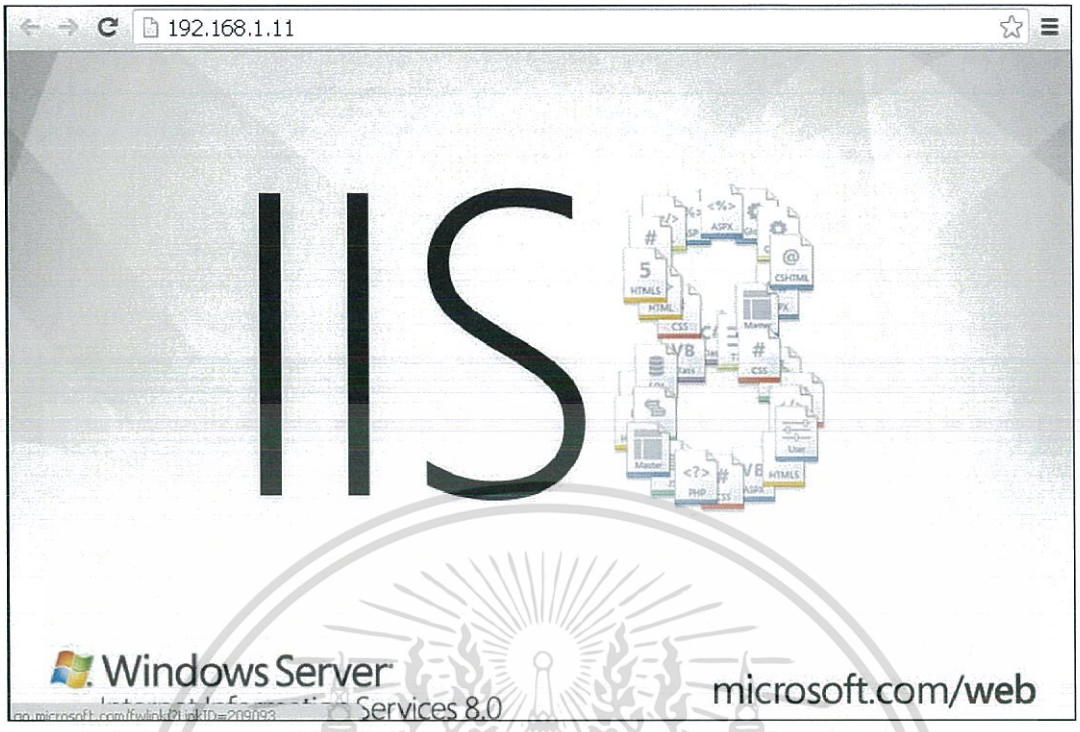
4.2 การทำงานของข้อบังคับไฟร์วอล

ในการทดสอบกระบวนการทำงานของข้อบังคับของไฟร์วอล จะทำการทดสอบโดยการ Ping จากต้นทางไปยังปลายทางต่างๆตามข้อตกลงที่ได้กำหนดไว้ในข้อบังคับโดยมีดังนี้

- อนุญาตให้ LAN เชื่อมต่อกับ WAN ได้
- อนุญาตให้ LAN บางส่วนเชื่อมต่อกับ WAN ได้
- บล็อค WAN ในการเข้าถึง LAN
- อนุญาตให้ LAN เชื่อมต่อกับ DMZ ได้เพียง HTTP
- อนุญาตให้ WAN เชื่อมต่อกับ DMZ ได้เพียง HTTP
- บล็อค DMZ ในการเข้าถึง LAN



รูปที่ 4. 4 LAN Ping WAN



รูปที่ 4. 5 LAN to DMZ

4.3 การทำงานของ Failover

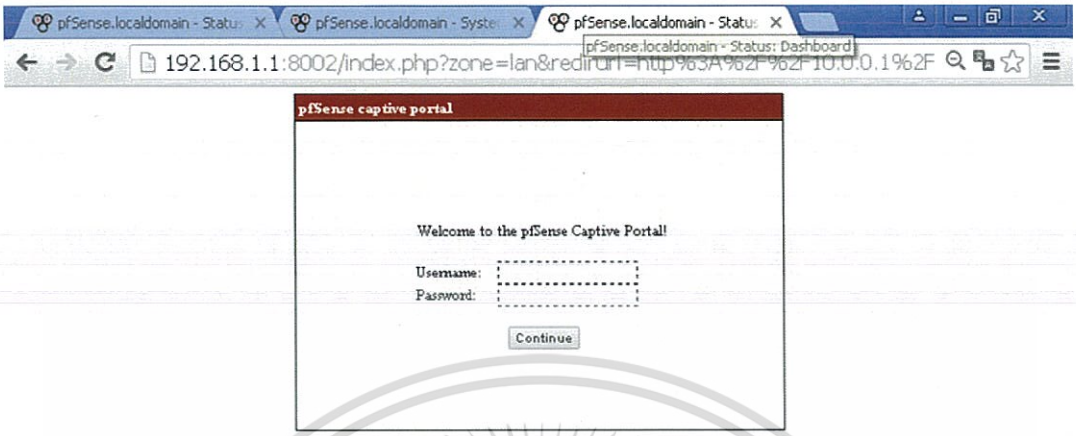
CARP Interfaces		
CARP Interface	Virtual IP	Status
WAN@1	161.246.1.10/24	MASTER
LAN@2	172.16.10.254/24	MASTER

รูปที่ 4. 6 สถานะของไฟร์วอลตัว Primary

CARP Interfaces		
CARP Interface	Virtual IP	Status
WAN@1	161.246.1.10/24	BACKUP
LAN@2	172.16.10.254/24	BACKUP

รูปที่ 4. 7 สถานะของไฟร์วอลตัว Secondary

4.4 การทำงานของ Captive Portal

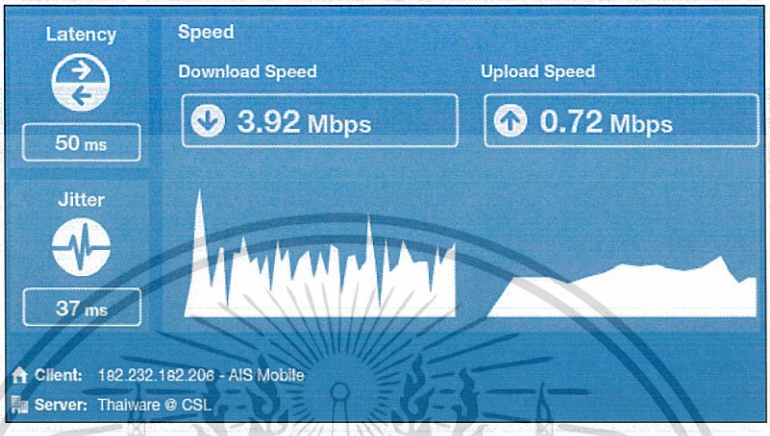


รูปที่ 4. 8 หน้าต่างของ Captive portal

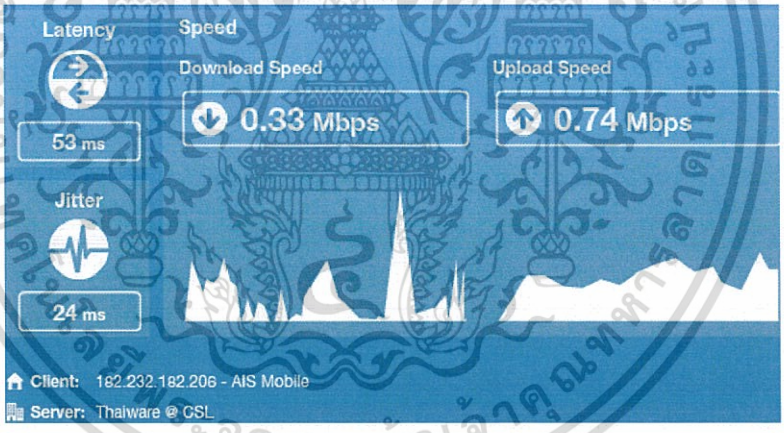
รูปที่ 4. 9 สเตตัสการเชื่อมต่อของแต่ละยูสเซอร์

4.5 การทำงานของ Traffic Shaping

ในส่วนของการวัดผลการทำงาน QoS นั้นเราจะทำการปรับแบนวิทธ์ของการเชื่อมต่อให้เหลือเพียง 10% จากแบนวิทธ์ทั้งหมดและสามารถเลือกให้บางเซอร์วิสมีแบนวิทธ์ที่มากกว่าปกติได้ดังรูป



รูปที่ 4. 10 ความเร็วทั่วไปก่อนทำการจำกัดแบนวิทธ์



รูปที่ 4. 11 ความเร็วหลังการจำกัดแบนวิทธ์

บทที่ 5
สรุปผลการทดลอง

ระบบความปลอดภัยระดับองค์กรในรูปแบบการติดตั้งไฟร์วอลสามารถนำมาประยุกต์ใช้ได้จริงในปัจจุบันและด้วยความที่เป็นโอเพ่นซอร์สไฟร์วอลนั่นหมายถึงไม่มีค่าใช้จ่ายในการนำมาใช้ ในปัจจุบันมีหลายองค์กรในไทยที่นำ Pfsense มาใช้งานจริงร่วมกับอุปกรณ์เครือข่ายอื่นๆ ซึ่งการที่ไม่มีค่าใช้จ่ายทำให้ได้เปรียบคู่แข่งที่ใช้ระบบที่มีการจัดการแบบเสียค่าลิขสิทธิ์ โดยสามารถทำงานได้ในระดับธุรกิจขนาดเล็กไปจนถึงกลาง อีกทั้งระบบยังสามารถทำหน้าที่เป็นเร้าเตอร์ได้ด้วยและยังมีอีกหลายฟีเจอร์ที่เป็นประโยชน์อย่างมากในการจัดการกับระบบเครือข่ายอาทิเช่น การควบคุมทราฟฟิคในระบบเครือข่าย การจำกัดแบนวิทธ์รวมถึงการควบคุมการเข้าใช้งานระบบเครือข่าย ในการวิเคราะห์และออกแบบระบบเครือข่ายเดิมที่มีอยู่แล้วเพื่อที่จะนำไฟร์วอลไปติดตั้งเพิ่มนั้นสำหรับ Pfsense นั้นไม่ถือว่าเป็นปัญหาในการออกแบบเนื่องจากสามารถเพิ่มได้เลยโดยไม่จำเป็นที่จะต้องเปลี่ยนแปลงใดๆกับระบบเครือข่ายเดิมและยังเป็นการเพิ่มประสิทธิภาพด้านความปลอดภัยให้แก่ระบบเครือข่ายอีกด้วย

เอกสารอ้างอิง

[1] Cisco systems, **Introduction to Cisco ASA Firewall Services**

[2] Cisco systems, **Cisco Security Appliance Command Line Configuration Guide, Version 7.2**

[3] Matt Williamson, **Pfsense 2 Cookbook**

[4] pfSense. (n.d.). *pfsense*. **Retrieved from https://www.pfsense.org/about-pfsense/features.html**