

pfSense

เป็นโปรเจกต์ที่พัฒนาโดย **Chris Buechler** และ **Scott Ullrich** ถูกพัฒนาขึ้นจาก **Linux** สายพันธ์ **FreeBSD** เมื่อปี 2004 จุดประสงค์เพื่อใช้งานเป็นไฟร์วอลล์ และเราเตอร์ และสามารถจัดการตัวอุปกรณ์ได้ผ่านหน้า **Browser (IE, Firefox, Chrome, etc.)** ได้ และด้วยเนื่องจากตัว **pfSense** ถูกพัฒนามาจาก **Linux** ทำให้เราสามารถใช้งานมันได้ฟรี แบบไม่ต้องกังวลเรื่อง **License**

Hardware สำหรับการติดตั้ง pfSense

- ❖ เครื่องคอมพิวเตอร์ CPU แนะนำว่าควรจะเป็น Core 2 Duo ขึ้นไป
- ❖ Ram ขั้นต่ำควรอยู่ที่ 512 MB ขึ้นไป
- ❖ การ์ดแลน 2 การ์ด (ขั้นต่ำ)
- ❖ ฮาร์ดดิสก์ ขั้นต่ำ 1GB

Feature เด่น ของ pfSense

- ❖ Firewall
- ❖ State Table
- ❖ Network Address Translation
- ❖ Captive Portal

Firewall

- ❖ สามารถจำกัดจำนวนการเชื่อมต่อ (Connection) ต่อ Rule ได้
- ❖ สามารถ Filter โดยใช้ระบบปฏิบัติการเป็นเงื่อนไขได้ เช่น อนุญาตให้เครื่องคอมพิวเตอร์ที่เป็น Linux ใช้งานอินเทอร์เน็ตได้ แต่ไม่อนุญาตให้เครื่องที่เป็น Windows ใช้งานอินเทอร์เน็ต
- ❖ สามารถเซ็ตแต่ละ Rule ให้เก็บหรือไม่เก็บ Log ได้
- ❖ มีความยืดหยุ่นสูงในการทำ Policy Routing โดยสามารถเลือก Gateway ของแต่ละ Rule ได้ (สำหรับ Load balancing, Fail Over, Multi-WAN เป็นต้น)
- ❖ สามารถตั้งชื่อกลุ่มของ IP, เน็ตเวิร์ค หรือ พอร์ต ได้ ทำให้เข้าใจง่ายและสะดวกต่อการจัดการ Rule ต่างๆ โดยเฉพาะอย่างยิ่งสำหรับระบบที่มีหลายๆ Public IP และมีเครื่องเซิร์ฟเวอร์หลายๆเครื่อง
- ❖ มีความสามารถทำ Transparent Layer 2 สามารถทำ Bridge และ Filter ระหว่าง Interface ได้

State Table

State Table ของไฟร์วอลล์ เป็นการคงไว้ของการเชื่อมต่อของในเน็ตเวิร์ค

- ❖ จำกัดจำนวนการเชื่อมต่อ (**Connection**) ต่อเครื่อง
- ❖ จำกัดจำนวน **state** ต่อ **Host**
- ❖ จำกัดการเชื่อมต่อใหม่ (**new connection**) ต่อวินาที
- ❖ กำหนดการหมดเวลาของ **state** (**state timeout**)
- ❖ กำหนดชนิดของ **state**

Network Address Translation (NAT)

❖ การทำ Port forwarding แบบช่วงและแบบหลายๆ Public IP

❖ 1:1 NAT สำหรับ IP เดียว หรือ สำหรับทั้ง Subnet

❖ Outbound NAT

- ค่า NAT ปกติสำหรับ Outbound traffic ทั้งหมด ถูก NAT ไปยัง IP ที่อยู่ฝั่ง WAN ในรูปแบบที่มีหลาย WAN ค่า NAT ปกติ จะถูก NAT ไปยัง IP ที่กำลังใช้งานฝั่ง WAN

- การทำ Outbound NAT ขั้นสูง ทำให้ค่า NAT ปกติถูกปิดการใช้งาน และเปิดการใช้งานการสร้าง NAT ที่มีความยืดหยุ่นมากขึ้นกว่าเดิม (คือสามารถกำหนด Rule ที่ไม่ให้ทำ NAT ได้)

❖ NAT Reflection – ในการตั้งค่าบางครั้ง เป็นไปได้ที่ Service ที่เข้าถึงโดย Public IP สามารถเข้าได้จากเน็ตเวิร์คข้างใน

Captive Portal

Captive Portal อนุญาตให้คุณบังคับให้ **Authenticate** หรือทำการ **Redirect** ไปยังเว็บเพจเพื่อให้คุณคลิกเพื่อที่จะผ่านเน็ตเวิร์คออกไปได้ ซึ่งส่วนใหญ่ใช้กับ **Hot Spot** แต่ก็สามารถนำไปใช้ได้กับเน็ตเวิร์คขององค์กรเพื่อระดับความปลอดภัยบนเครือข่ายไร้สาย หรือ การเข้าถึงอินเทอร์เน็ต ข้อมูลเพิ่มเติมเกี่ยวกับเทคโนโลยีของ **Captive Portal** สามารถอ่านเพิ่มเติมได้ที่ **Wikipedia** รายการดังต่อไปนี้ เป็นความสามารถของ **Captive Portal** ใน **pfSense**

-**Maximum concurrent connection** — จำกัดจำนวนการเชื่อมต่อของ **IP** ของเครื่องลูกข่าย คุณสมบัตินี้เป็นการป้องกัน **Denial of Service** จากเครื่องลูกข่ายที่ส่ง **traffic** อย่างต่อเนื่องปราศจากการ **authenticate** หรือคลิกที่เว็บเพจที่ **Redirect** ไป

-**Idle timeout** — ตัดการเชื่อมต่อเมื่อไม่มีการใช้งานในเวลาที่กำหนด

-**Hard timeout** — ตัดการเชื่อมต่อโดยอัตโนมัติเมื่อถึงเวลาที่กำหนด

-**Logon pop up window** — เป็น **pop up window** ที่มีปุ่ม **log off**

-**URL Redirection** — หลังจากการ **Authenticate** หรือคลิกบนเว็บเพจเป็นที่เรียบร้อยแล้ว เราสามารถ **Redirect** ไปยังเว็บเพจที่เรากำหนดไว้ได้

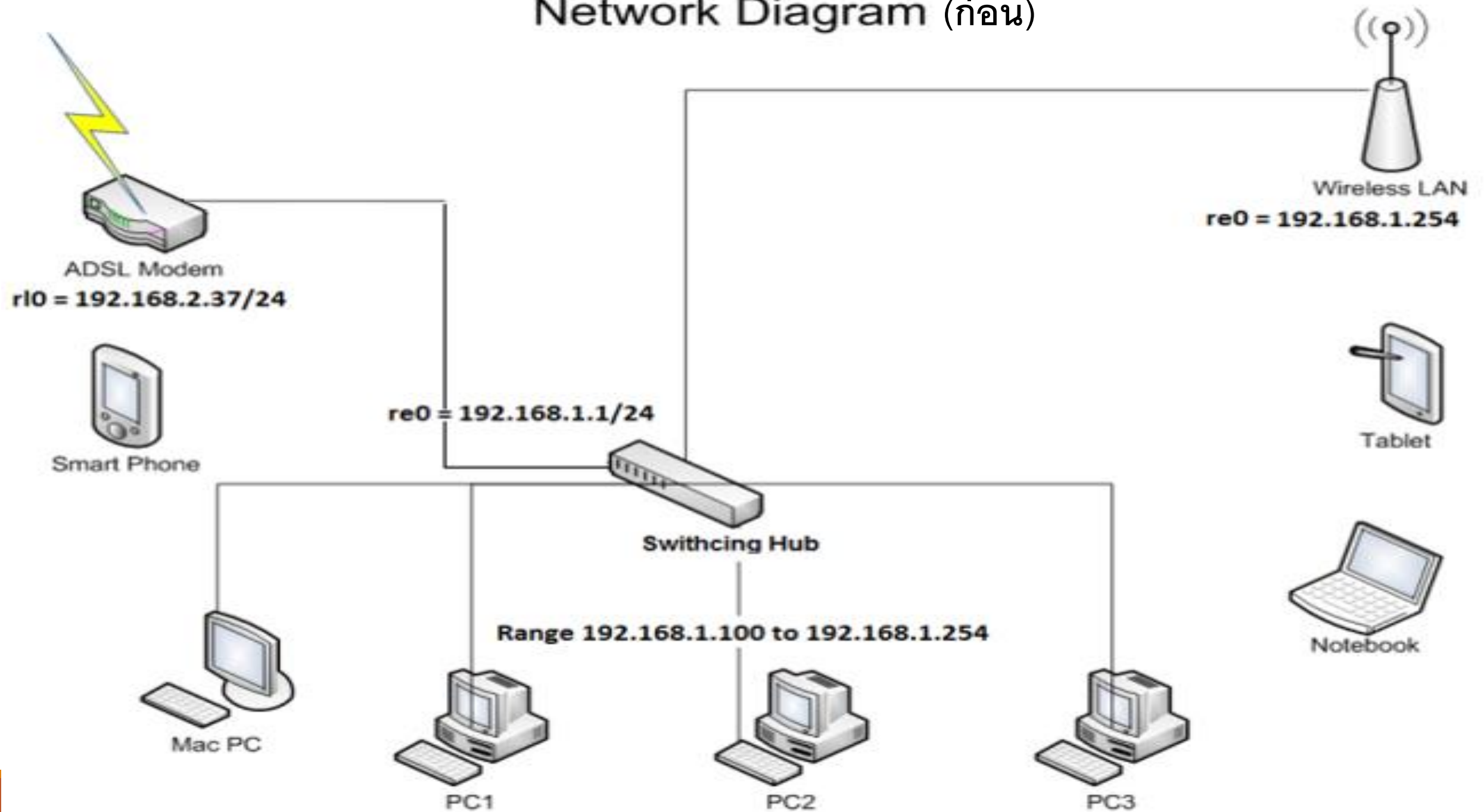
-**MAC Filter** — สามารถ **filter** โดยใช้ **MAC Address**

Authentication Option

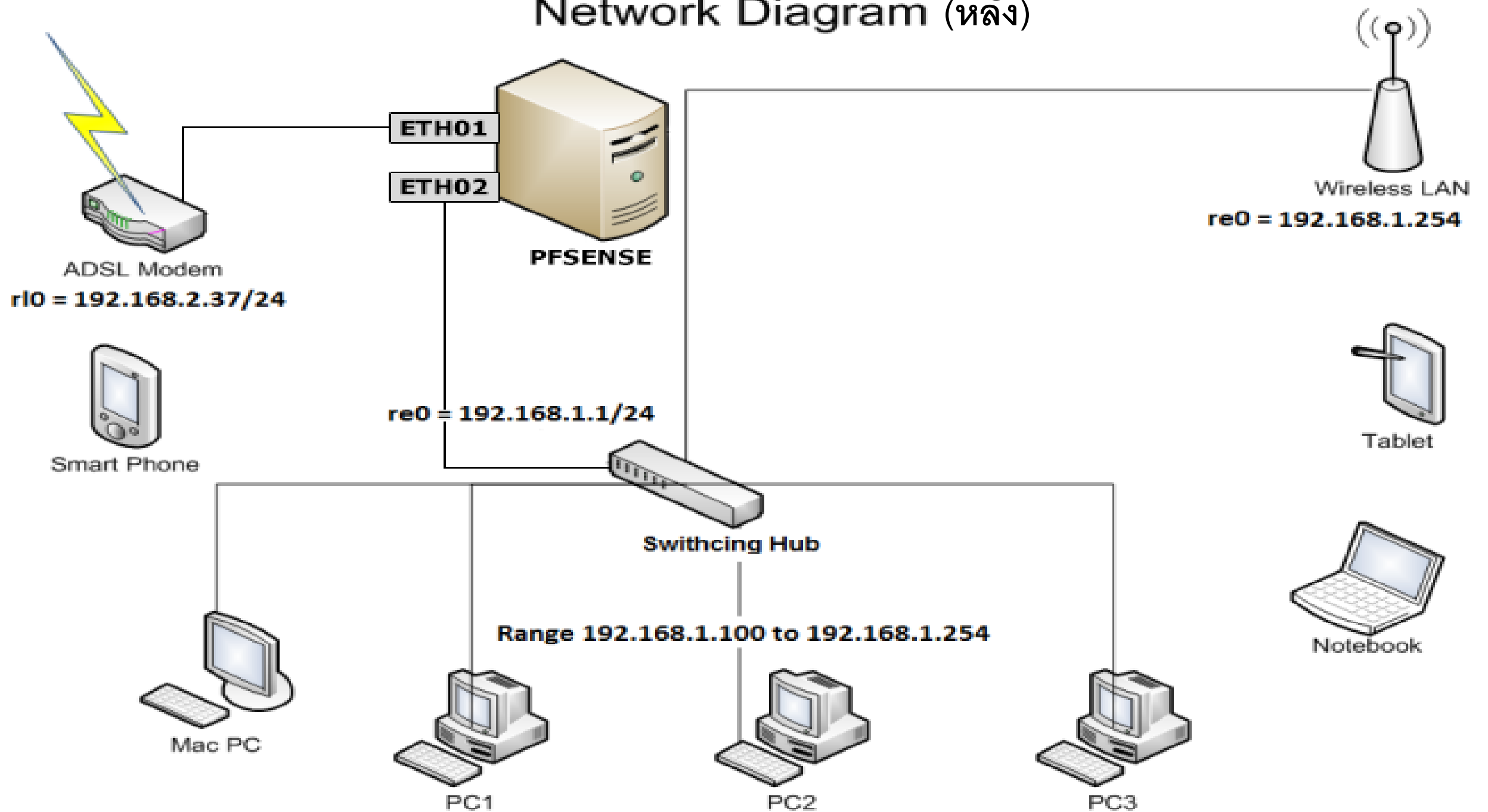
มีสามตัวเลือกในการทำ

- **authenticationNo authentication** – หมายความว่า ผู้ใช้เพียงแค่คลิกในหน้าที่ **Redirect** ไป โดยที่ไม่ต้องให้รหัสผ่านแต่อย่างใด
- **Local user manager** – สามารถใช้ฐานข้อมูลผู้ใช้ใน **pfSense** ได้
- **RADIUS authentication** – เป็นวิธีการที่แนะนำสำหรับผู้ใช้ในองค์กรและ **ISP** สามารถ **Authenticate** กับ **Microsoft Active Directory** และ **RADIUS Server** หลายๆตัว

Network Diagram (ก่อน)



Network Diagram (หลัง)



ข้อดีในการใช้งาน

- ❖ สร้างง่าย เจาะ ยาก เพราะระบบ ที่ไม่ซับซ้อน จึงมีช่องโหว่น้อยมาก
- ❖ ควบคุมการใช้งานระบบ **internet** ภายในองค์กรได้โดยระบบยืนยันตัวตน
- ❖ เหมาะกับองค์กรที่ต้องการเก็บ **log** การใช้งานจากผู้ใช้งานตาม พรบ. คอมพิวเตอร์
- ❖ เหมาะกับ **administrator** มือใหม่ **config** ง่าย จัดการระบบง่าย และ ระบบ แข็งแรง
- ❖ เหมาะกับการควบคุมการจราจรในระบบ และการทำ **Routing**
- ❖ เหมาะกับการใช้งานในองค์กรระดับเล็กถึงระดับกลาง

ข้อเสีย

- ❖ เนื่องจากเป็นซอฟต์แวร์แบบ **Open source** จึงไม่มีการซัพพอร์ตใดๆ เวลาเกิดปัญหา
- ❖ ความสามารถด้าน **firewall** ไม่สูงเทียบเท่า **next generation firewall** ที่มีในปัจจุบัน
- ❖ ไม่เหมาะกับการใช้งานในองค์กรระดับใหญ่

ตัวอย่างการใช้งานระบบการยืนยันตัวตน

หน้าจอล็อกอินเพื่อเข้าใช้งานอินเทอร์เน็ต

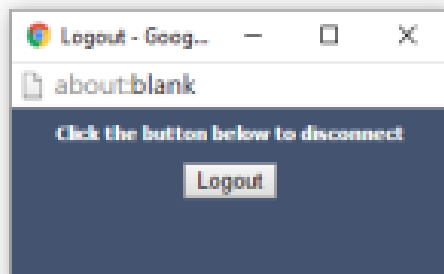
ระบบพิสูจน์ตัวตน

ชื่อใช้งาน : USERNAME
test

พาสวอร์ด : PASSWORD

ลงชื่อเข้าใช้ →

← → ↻ https://www.google.co.th/?gws_rd=ssl



หน้าจอเมื่อล็อกอินสำเร็จและหน้าต่าง Pop-Up logout เมื่อต้องการออกจากระบบ

ฟังก์ชันการเพิ่มผู้ใช้แบบทีละคน

← → ↻ 192.168.1.1/admin/index2.php?option=register2

ระบบจัดการการพิสูจน์ตัวตนผู้ใช้งานอินเทอร์เน็ต

Registration [2]

เพิ่มผู้ใช้รายคน

เลือกกลุ่ม : Student *ระบุกลุ่มไฟท์กอล์ฟ

ชื่อ : นายจิรพัฒน์ * นายของพ่อ

นามสกุล : นสจจรณ * ศรีสวัสดิ์

อีเมล : kidgleam@gmail.com * tongtoth@hotmail.com

ชื่อผู้ใช้ : test1 * รหัสหรือเลขประชาชน 13 หลัก

กรอกเป็นตัวเลขภาษาอังกฤษและตัวเลขเท่านั้น

รหัสผ่าน : ***** -

ความยาวอย่างน้อย 4 อักขระ

ยืนยันรหัสผ่าน : ***** -

ส่งข้อมูล

ฟังก์ชันการเพิ่มผู้ใช้แบบเป็นกลุ่ม

← → ↻ 192.168.1.1/admin/index2.php?option=add_user&group=office&username=&numadd=

Authent!cation For Admin

ระบบจัดการการพิสูจน์ตัวตนผู้ใช้งานอินเทอร์เน็ต

Generate Users

เพิ่มผู้ใช้รายใหม่เข้าสู่ระบบ **บันทึก** **ยกเลิก**

ตารางแสดงรายชื่อสมาชิกที่จะเพิ่มใหม่ในกลุ่มOffice ทั้งหมด **10** คน

| ลำดับที่ | ชื่อผู้ใช้งาน | รหัสผ่าน | วันหมดอายุ | ความจุเริ่มต้น (ความจุไฟล์ / อีเมล) |
|----------|---------------|----------|------------|--|
| 1 | KE12 | ugj08d | 0000-00-00 | 2048/2048 KB |
| 2 | KE13 | m3wyl9 | 0000-00-00 | 2048/2048 KB |
| 3 | KE14 | c46mfz | 0000-00-00 | 2048/2048 KB |
| 4 | KE15 | cbmihe | 0000-00-00 | 2048/2048 KB |
| 5 | KE16 | pi0nbh | 0000-00-00 | 2048/2048 KB |
| 6 | KE17 | 2wmdj4 | 0000-00-00 | 2048/2048 KB |
| 7 | KE18 | opnlhm | 0000-00-00 | 2048/2048 KB |
| 8 | KE19 | gut89 | 0000-00-00 | 2048/2048 KB |
| 9 | KE20 | wl2gpx | 0000-00-00 | 2048/2048 KB |
| 10 | KE21 | rpm82e | 0000-00-00 | 2048/2048 KB |

192.168.1.1/admin/index2.php?option=manage_group&action=add

Group Manager

จัดการกลุ่มผู้ใช้งานอินเทอร์เน็ต

เพิ่มกลุ่ม

กรุณาระบุค่าของฟิลด์ด้านล่างแล้วคลิกปุ่มเพื่อเพิ่มกลุ่มใหม่

| ลำดับที่ | ชื่อกลุ่ม | ความเร็วเน็ต Down : Up (Kbps) | วันหมดอายุ ค.ศ.-เดือน-วัน | สถานะ | ดำเนินการ |
|----------|---------------|----------------------------------|------------------------------|-------|-----------|
| 1 | Administrator | 10240 : 10240 | 0000-00-00 | 🔒 | 🔧 ✖ |
| 2 | Register | 1024 : 512 | 0000-00-00 | 🔒 | 🔧 ✖ |
| 3 | Office | 2048 : 2048 | 0000-00-00 | 🔒 | 🔧 ✖ |
| 4 | Student | 2048 : 1024 | 0000-00-00 | 🔒 | 🔧 ✖ |
| 388 | | 105C : 105C | 2016-04-05 | | 🗑 |

login 1 ครั้งหมดใช้งานเวลา : 1 hour

หมดอายุ : 1 hour

ถ้าไม่ใช้งานเป็นเวลา จะตัดการใช้งาน : 5 minutes

ระยะเวลาสถานะพัก : 1 minute

เว็บไซต์การ login เครื่องใช้ : http://www.google.com

ฟังก์ชันการจัดการกลุ่มผู้ใช้อินเทอร์เน็ต

ฟังก์ชันดูประวัติการใช้งานอินเทอร์เน็ต

192.168.1.1/admin/index2.php?option=user_history

Authent!cation For Admin

ระบบจัดการการพิสูจน์ตัวตนผู้ใช้งานอินเทอร์เน็ต

History

ประวัติการใช้งานอินเทอร์เน็ต

วันที่เริ่มต้น : 2016-03-06 วันที่สิ้นสุด : 2016-03-07 แสดงทั้งหมด

จำนวนการใช้งานภายในช่วงเวลาดังกล่าว มีทั้งสิ้น 7 ครั้ง

| ลำดับ | ชื่อผู้ใช้ | ชื่อ - นามสกุล | เริ่มต้น-สิ้นสุดใช้งาน | หมายเลขไอพี | เป็นเวลา | Upload | Download |
|-------|------------|---------------------|--|---------------|----------|-----------|------------|
| 1 | admin | นายชัยวัฒน์ แสงอรุณ | 06-03-2559 00:07:14 06-03-2559 01:27:27 | 192.168.1.100 | 1:20:13 | 25.87 MB. | 176.34 MB. |
| 2 | admin | นายชัยวัฒน์ แสงอรุณ | 06-03-2559 01:31:17 06-03-2559 01:36:38 | 192.168.1.100 | 0:05:21 | 2.32 MB. | 2.26 MB. |
| 3 | admin | นายชัยวัฒน์ แสงอรุณ | 06-03-2559 15:48:41 06-03-2559 16:07:29 | 192.168.1.100 | 0:18:48 | 5.42 MB. | 7.51 MB. |
| 4 | admin | นายชัยวัฒน์ แสงอรุณ | 06-03-2559 16:11:10 06-03-2559 16:54:01 | 192.168.1.200 | 0:42:51 | 14.59 MB. | 399.58 MB. |
| 5 | admin | นายชัยวัฒน์ แสงอรุณ | 06-03-2559 16:57:34 06-03-2559 18:34:11 | 192.168.1.200 | 1:36:37 | 2.38 MB. | 11.89 MB. |

ฟังก์ชันสถิติการใช้งานระบบ

← → ↻ 192.168.1.1/admin/index2.php?option=user_statistic

Authent!cation For Admin

ระบบจัดการการพิสูจน์ตัวตนผู้ใช้ผ่านลินเชอร์เน็ท



Statistic

สถิติการใช้งานระบบ



Squid user access report

User: 192.168.1.100 (?)

Group: ?

Date: 06 Mar 2016

| Total | | 5.3 M | | |
|-------|--|-------------|-------|--------------|
| # | Accessed site | Connect | Bytes | Cumulative % |
| 1 | www.servethehome.com | 52 | 1.1 M | 1.1 M 20.0% |
| 2 | pantip.com | 27 623 981 | | 1.7 M 11.2% |
| 3 | www.overclockzone.com | 61 584 331 | | 2.3 M 10.5% |
| 4 | documents.tips | 13 545 031 | | 2.7 M 9.7% |
| 5 | hosxp.net | 26 481 689 | | 3.2 M 8.6% |
| 6 | ercaservice.samsungmobile.com | 102 393 360 | | 3.8 M 7.0% |
| 7 | reader11.documents.tips | 11 292 713 | | 3.8 M 5.2% |
| 8 | www.teenewareless.com | 51 205 895 | | 4.0 M 3.7% |
| 9 | www.thaiseoboard.com | 48 137 884 | | 4.2 M 2.4% |
| 10 | pagead2.google syndication.com | 6 129 612 | | 4.3 M 2.3% |
| 11 | cdn.garenanow.com | 82 123 668 | | 4.4 M 2.2% |
| 12 | www.thaiadmin.org | 13 121 542 | | 4.5 M 2.1% |
| 13 | fonts.gstatic.com | 8 116 752 | | 4.5 M 2.0% |
| 14 | upic.me | 3 100 237 | | 4.7 M 1.8% |
| 15 | www.thaibsd.com | 46 56 212 | | 4.8 M 1.0% |
| 16 | 192.168.2.51 | 13 51 648 | | 4.8 M 0.9% |
| 17 | ung.tarad.com | 18 44 789 | | 4.9 M 0.8% |
| 18 | www.taradplaza.com | 14 43 407 | | 4.9 M 0.7% |
| 19 | updateres.garenanow.com | 12 39 294 | | 5.0 M 0.7% |
| 20 | ptcdn.info | 46 38 390 | | 5.0 M 0.6% |
| 21 | staticxx.facebook.com | 1 35 196 | | 5.0 M 0.6% |
| 22 | www.mangaforum.org | 1 28 812 | | 5.1 M 0.5% |
| 23 | www.linuxthai.org | 3 27 989 | | 5.1 M 0.5% |