

ราสพ์เบอรี พาย ไฟร์วอลล์ สำหรับหน่วยงานธุรกิจขนาดกลางและขนาดเล็ก (SMEs)

Raspberry Pi firewall for Small and Medium Enterprise (SMEs)

นพดล จินตสุนทรอุไร¹, ตรีรัตน์ เมตต์การุณจิต²

สาขาเทคโนโลยีสารสนเทศ คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีไทย-ญี่ปุ่น

1771/1 ถ.พัฒนาการ แขวงสวนหลวง เขตสวนหลวง กรุงเทพฯ 10250 โทร 0-2763-2644

¹ ji.noppadol_st@tni.ac.th

² triratana@tni.ac.th

บทคัดย่อ

ในบทความนี้นำเสนอแนวคิดเกี่ยวกับการนำบอร์ด ราสพ์เบอรี พาย (raspberry pi : RPi) ที่เป็นบอร์ดสมองกลฝังตัว (embedded board) ชนิดหนึ่งที่เป็นที่นิยมใช้ในปัจจุบัน ประยุกต์การใช้งานเป็นอุปกรณ์ไฟร์วอลล์ (Firewall) ที่ได้เปรียบเทียบกับราสพ์เบอรี พายไฟร์วอลล์กับ บอร์ดสมองกลฝังตัวอื่นๆ ที่ใช้เป็นไฟร์วอลล์ และ ไฟล์วอลล์ของเราเตอร์ขนาดกลาง ซึ่งผลออกมานั้น เห็นได้ว่า ราสพ์เบอรี พายนั้น เมื่อเทียบกับ คิวบ์บอร์ดประสิทธิภาพการทำงาน ในแง่ของทราฟฟิค(throughput) กับจำนวนกฎของไฟร์วอลล์นั้น คิวบ์บอร์ด ไฟร์วอลล์ สามารถทำงานได้ดีกว่า ราสพ์เบอรี พายไฟร์วอลล์ แต่ก็ไม่ได้แตกต่างกันมาก นอกจากนี้ราสพ์เบอรีพายไฟร์วอลล์ มีความสามารถเทียบเคียงกับไฟร์วอลล์ของเราเตอร์ขนาดกลางในแง่ของการตั้งกฎของไฟร์วอลล์ รวมถึงการตรวจจับและป้องกันภัยคุกคาม โดยจุดเด่นของบอร์ดราสพ์เบอรี พาย ไฟร์วอลล์ คือมีราคาถูกกว่าเราเตอร์ขนาดกลางมาก ที่เป็นทางเลือกสำหรับธุรกิจขนาดกลางและเล็กที่จะนำไปใช้งานได้

คำสำคัญ : ราสพ์เบอรี พาย , ไฟร์วอลล์ , ความปลอดภัยของอินเทอร์เน็ต , หน่วยงานธุรกิจขนาดกลางและขนาดย่อม

1.บทนำ

การใช้งานอินเทอร์เน็ตในปัจจุบันนี้ มีหลากหลายรูปแบบด้วยกันทั้ง เข้าเพื่อไปหาข้อมูล อ่านข่าวสาร หรือเพื่อทำการ ดาวน์โหลด ข้อมูลเพื่อใช้ในการทำธุรกรรมต่าง ๆ ในการใช้งานดังกล่าวอาจจะมีภัยคุกคามทางอินเทอร์เน็ตต่าง ๆ มากมาย อาทิเช่น [1] การใส่คำสั่งข้อมูลผ่าน SQL (SQL injection) การเปิดช่องโหว่ของการยืนยันตัวตน (Broken Authentication) การปลอมแปลงหน้าเว็บเพจ (cross site scripting : XSS) จากการสำรวจข้อมูลทางสถิติของ Internet Security Threat Report ประจำปี 2014 [2] จำนวนการปิดกั้นเว็บไซต์ที่อันตรายนั้น มีจำนวนมากกว่าปีที่แล้วถึง 23% และ อัตราของการโจมตีของหน่วยงานธุรกิจขนาดกลางและขนาดย่อม เมื่อเทียบกับปีที่แล้ว มีสัดส่วนที่มากขึ้นจากเดิมถึง 11 % จะเห็นได้ว่าอันตรายของภัยคุกคามทางอินเทอร์เน็ตต่อหน่วยงานธุรกิจขนาดกลางและขนาดเล็กนั้นมีมากยิ่งขึ้น และเป็นสิ่งสำคัญที่จะต้องคำนึงถึงอย่างหลีกเลี่ยงไม่ได้

มาตรการความปลอดภัยของอินเทอร์เน็ตในหน่วยงานธุรกิจต่าง ๆ มีความแตกต่างกันไป ทั้งนี้ขึ้นอยู่กับประเภทของธุรกิจและลักษณะงานของธุรกิจนั้น ๆ ด้วย สำหรับองค์กรขนาดใหญ่ทั่วไป มีการป้องกันภัยคุกคามทางอินเทอร์เน็ตที่มีประสิทธิภาพที่ดี โดยการลงทุนกับอุปกรณ์ต่าง ๆ

ตัวอย่างเช่น ไฟร์วอลล์ ระบบการป้องกันการบุกรุก (intrusion prevention systems : IPS) แอปพลิเคชันเกตเวย์ (application gateway) เป็นต้น โดยอุปกรณ์ดังกล่าวมีราคาค่อนข้างสูง เมื่อเทียบกับ ลักษณะของรายได้ของหน่วยงานธุรกิจขนาดกลางและขนาดย่อม โดยเฉพาะธุรกิจขนาดเล็กจะไม่ลงทุนในส่วนนี้ อีกทั้งต้องเพิ่มบุคลากรในการจัดการอุปกรณ์ดังกล่าว ซึ่งค่อนข้างซับซ้อน และเป็นการสิ้นเปลืองจนเกินไป

บทความนี้จะให้เห็นถึงทางเลือกหนึ่งของหน่วยงานขนาดกลางและขนาดเล็ก ที่สามารถใช้ไฟร์วอลล์ ในราคาถูกได้ โดยการประยุกต์ใช้ บอร์ดสมองกลฝังตัว ที่มีราคาถูก เช่น ราสพ์เบอรี พาย มาใช้เป็น ไฟร์วอลล์ ซึ่งเป็นอุปกรณ์หลักในการป้องกันภัยคุกคามในอินเทอร์เน็ตให้กับหน่วยงานธุรกิจขนาดกลางและขนาดย่อม ให้สามารถเลือกซื้ออุปกรณ์ป้องกันความปลอดภัยของอินเทอร์เน็ต ในราคาย่อมเยา และมีประสิทธิภาพที่เทียบเคียงกับ ไฟร์วอลล์ในระดับองค์กร โดยส่วนแรกจะกล่าวถึงการแนะนำอุปกรณ์ ราสพ์เบอรี พาย ในปัจจุบันนี้ว่ามีอะไรบ้าง และในส่วนที่สอง จะนำราสพ์เบอรี พาย ดังกล่าวนั้นมาเปรียบเทียบกับ ไฟร์วอลล์ ในระดับองค์กรที่มีใช้อยู่ ณ ปัจจุบัน เพื่อหาความแตกต่างในด้านต่าง ๆ เช่น ประสิทธิภาพในการทำงาน ความเร็วในการป้องกัน และความสามารถในการรองรับข้อมูล

2.ราสพ์เบอรี พาย ไฟร์วอลล์ (RPi Firewall)

ราสพ์เบอรี พาย (raspberry pi : RPi) [3] เป็นบอร์ดระบบฝังตัว ที่มีลักษณะคล้ายคอมพิวเตอร์ขนาดเล็ก มีขนาดเท่ากับบัตรเครดิต ซึ่งพัฒนาจาก มหาวิทยาลัยเคมบริดจ์ เมื่อปี 2012 โดยราคาอยู่ที่ประมาณ 35 เหรียญสหรัฐ โดยบอร์ด ราสพ์เบอรี พาย นั้น ประกอบด้วย หน่วยประมวลผลสถาปัตยกรรมแบบอาร์ม (advance RISC machine : ARM) และมีหน่วยประมวลผลภาพ 3 มิติ สำหรับการฉายภาพวิดีโอ ขนาดความละเอียดสูง มีหน่วยความจำชั่วคราว (random access memory : RAM) ที่แตกต่างกันไปในแต่ละรุ่น ซึ่งจะกล่าวต่อไป และสามารถเพิ่มหน่วยความจำโดยใช้เอสดีการ์ด(SD card) ได้ พอร์ตการเชื่อมต่อประกอบด้วย เฮชดีเอ็มไอ(HDMI) ยูเอสบี(USB) และ พอร์ต อีเทอร์เน็ต(ethernet) ซึ่งมีความนิยมอย่างมากในหน่วยอุตสาหกรรมระบบโครงข่ายอัจฉริยะ โดยที่ ราสพ์เบอรี พาย นั้นทำงานด้วยระบบ ลินุกซ์ ซึ่งก็หมายความว่า สามารถใช้ติดตั้งโปรแกรม ทำเป็นเว็บเซิร์ฟเวอร์ หรือจะเป็นหน่วยควบคุมอื่นๆได้ โดยที่ระบบปฏิบัติการนั้นจะเก็บไว้ในเอสดีการ์ด (SD card) เมื่อทำการติดตั้งเสร็จเรียบร้อย ทุกหน่วยประมวลผลของ ราสพ์เบอรี พาย ก็จะเริ่มทำงานทันที

2.1 คุณสมบัติของ ราสพ์เบอร์รี่ พาย โมเดล บี (rasberry pi model B) [4]

เป็นรุ่นของบอร์ดที่ได้รับความนิยมและใช้กันมากที่สุดในขณะนี้ ซึ่งในรุ่นนี้ได้รับการพัฒนาจากรุ่น เอ และมีส่วนที่สำคัญดังต่อไปนี้

- หน่วยประมวลผล ARM 700 MHz แขนเดียว
- RAM 512 MB
- พอร์ตยูเอสบี 2 ช่อง
- พอร์ตอีเทอร์เน็ต 100 Mb ใช้สำหรับเสียบสายแลน
- กำลังส่งไฟฟ้าอยู่ที่ 700 mA

2.2 คุณสมบัติของ ราสพ์เบอร์รี่ พาย 2 (rasberry pi 2) [4]

เป็นรุ่นของบอร์ดที่พัฒนาจากโมเดล บี พลัส ในปัจจุบัน ซึ่งในรุ่นนี้ มีคุณสมบัติหลักเหมือนกับ โมเดล บี พลัส เหมือนกันทั้งหมด แต่จะพัฒนาเรื่องของประสิทธิภาพการทำงาน รวมถึงเพิ่ม ความหลากหลายเพื่อรองรับเทคโนโลยีในอนาคต เช่น รองรับการทำงานกับ วินโดวส์ 10 และลักษณะที่ใช้กับกราฟฟิคระดับสูง เป็นต้น ซึ่งรายละเอียดของคุณสมบัติมีดังนี้

- หน่วยประมวลผล ARM Cortex-v7 900 MHz 4 แขน
- RAM 1 GB LPDDR2 SDRAM หน่วยความจำ 2 ตัว
- พอร์ตยูเอสบี 4 ช่อง
- พอร์ตอีเทอร์เน็ต 100 Mb ใช้สำหรับเสียบสายแลน
- กำลังส่งไฟฟ้าสูงสุดอยู่ที่ 1000 mA

2.3 ซอฟต์แวร์ ราสพ์เบอร์รี่ พาย ไฟร์วอลล์

2.3.1 ซอฟต์แวร์ IPFire [5]

IPFire เป็นซอฟต์แวร์ที่ออกแบบเพื่อทำการปรับปรุงและพัฒนาเกี่ยวกับความปลอดภัยทางด้านเครือข่าย ซึ่งใช้ได้ตั้งแต่ในระดับองค์กรธุรกิจขนาดเล็ก จนถึง ธุรกิจขนาดใหญ่ ซึ่งซอฟต์แวร์ดังกล่าวนี้มีลักษณะการทำงานที่ง่าย และมีหน้าจการทำงานในส่วนของผู้ใช้งานค่อนข้างสะดวกต่อการใช้งาน โดยใน คุณสมบัติการทำงานในด้านไฟร์วอลล์ จะอ้างอิงจากการทำงานของ การตรวจสอบแพ็คเกจแบบสถานะสัมพันธ์ (serial peripheral interface : SPI) ซึ่งจะสร้างการทำงานบนเฟรมเวิร์ก ที่ชื่อว่า เนตฟิลเตอร์ (netfilter) โดยลักษณะการทำงานของส่วนนี้จะแจ้งเตือนการทำงานถึง 4 ระดับด้วยกัน ซึ่งเปรียบเทียบได้ถึง 4 ระดับของความปลอดภัย

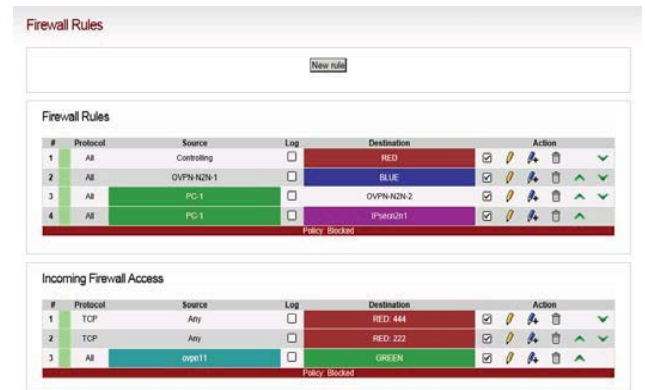
สีเขียว แสดงถึง ระดับปลอดภัย (safe area)

สีแดง แสดงถึง ระดับอันตราย (danger area)

สีน้ำเงิน แสดงถึง ระดับของพื้นที่ไร้สาย หมายความว่า เป็นส่วนหนึ่งของเครือข่ายภายใน (wireless network)

สีส้ม แสดงถึง เขตของการควบคุมของไฟร์วอลล์ (demilitarized zone : DMZ)

ซึ่งในระดับที่กล่าวมาข้างต้นนั้น จะเอาไปใช้ในการตั้งกฎไฟร์วอลล์ (firewall rules) ที่สามารถกำหนดให้อุปกรณ์ดังกล่าวนี้สามารถจัดการกับ IP ที่เข้าข่ายอันตรายได้ อย่างเช่นการลบทิ้ง หรือปิดกั้นไม่ให้ผ่าน เป็นต้น หน้าจการทำงานของการตั้งกฎไฟร์วอลล์ เป็นไปตามรูปที่ 1



#	Protocol	Source	Log	Destination	Action
1	All	Controlling	<input type="checkbox"/>	RED	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
2	All	OVPN-NON-1	<input type="checkbox"/>	BLUE	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
3	All	PC-1	<input type="checkbox"/>	OVPN-NON-2	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
4	All	PC-1	<input type="checkbox"/>	IPsec021	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

Policy blocked

#	Protocol	Source	Log	Destination	Action
1	TCP	Any	<input type="checkbox"/>	RED:444	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
2	TCP	Any	<input type="checkbox"/>	RED:322	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
3	All	open11	<input type="checkbox"/>	GREEN	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

Policy blocked

รูปที่ 1 หน้าจการทำงานของการตั้งกฎไฟร์วอลล์ของ IPFire [5]

2.3.2 ซอฟต์แวร์ Utangle Firewall [6]

เป็นซอฟต์แวร์ที่รวมอยู่ในตัวอุปกรณ์เซิร์ฟเวอร์ของ Utangle ซึ่งสามารถดาวน์โหลดซอฟต์แวร์ตัวแยกออกมาเพื่อทำแยกออกมาต่างหากได้ ซึ่งคุณสมบัติการทำงานนั้น สามารถกำหนดกฎของไฟร์วอลล์เพิ่มปิดกั้นไม่ให้ไอพีแอดเดรส ที่ไม่พึงประสงค์สามารถเข้ามาในเครือข่ายได้ และสามารถสร้าง DMZ เพื่อทำการป้องกันกฎที่เพิ่มออกมาได้ ซึ่งสามารถดาวน์โหลดผ่านเว็บไซต์ได้

2.3.3 ซอฟต์แวร์ IPTable [7]

IPTable เป็น ซอฟต์แวร์ไฟร์วอลล์ของระบบปฏิบัติการลินุกซ์ ที่สามารถสร้างกฎของไฟร์วอลล์ ได้โดยใช้เวลาการตอบสนองรวดเร็ว ซึ่งคุณสมบัติการทำงานนั้น ซอฟต์แวร์ดังกล่าวสามารถสร้างกฎไฟร์วอลล์ได้ จัดการการจราจรของข้อมูลที่เข้ามาได้ และสามารถจัดการ ไอพีแอดเดรส ต่างๆได้ เช่น การจัดการไอพี โปรโตคอล พอร์ต เป็นต้น ซึ่งหน้าจการทำงานนั้น เป็นไปตามรูปที่ 2

```

table: nat
Chain PREROUTING (policy ACCEPT)
num target prot opt source destination
Chain POSTROUTING (policy ACCEPT)
num target prot opt source destination
1 MASQUERADE all -- 10.8.0.0/24 0.0.0.0/0
2 SNAT all -- 10.8.0.0/24 0.0.0.0/0 to:10.168.5.145
Chain OUTPUT (policy ACCEPT)
num target prot opt source destination

table: filter
Chain INPUT (policy ACCEPT)
num target prot opt source destination
1 ACCEPT udp -- 0.0.0.0/0 0.0.0.0/0 udp dpt:1194
Chain FORWARD (policy ACCEPT)
num target prot opt source destination
Chain OUTPUT (policy ACCEPT)
num target prot opt source destination

```

รูปที่ 2 หน้าจการทำงานของการตั้งกฎไฟร์วอลล์ของ IPTable [8]

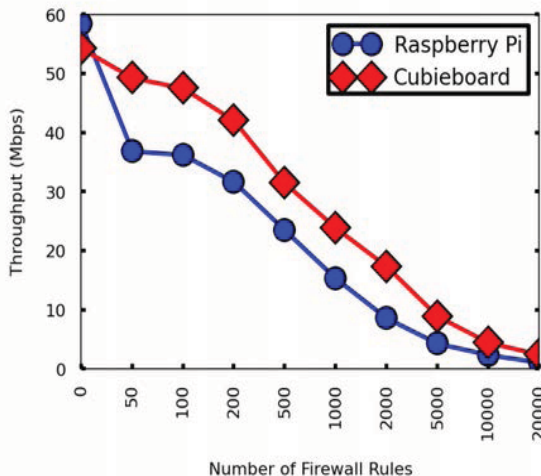
3. ราชพีเบอร์รี่ พาย ไฟร์วอลล์ กับ ไฟร์วอลล์ตัวอื่น ๆ

3.1 ราชพีเบอร์รี่ พาย ไฟร์วอลล์ กับ บอร์ดสมองกลฝังตัวอื่น ๆ

งานวิจัยของ Zubair Nabi [9] ที่นำเสนอเรื่อง A \$35 Firewall for the Developing World ได้สรุปใจความเกี่ยวกับการเปรียบเทียบ บอร์ด ราชพีเบอร์รี่ พาย ที่ประยุกต์การใช้งานในด้านของอุปกรณ์ไฟร์วอลล์ เทียบกับ บอร์ดระบบฝังตัวชนิดอื่น ๆ ซึ่งในงานวิจัยเทียบกับ คิวบ์บอร์ด (cubieboard) โดยที่งานวิจัยนี้จะวัดความสามารถในด้านต่างๆของการทำงานของไฟร์วอลล์ อย่างเช่น การตั้งกฎไฟร์วอลล์ ประสิทธิภาพในการทำงาน รวมถึง องค์ประกอบในด้านอื่น ๆ อย่างเช่นการแปลงที่อยู่ของเครือข่าย (network address translation : NAT) หรือการ ดูข้อมูลที่เข้ามา เป็นต้น ซึ่งจะอธิบายเป็นส่วน ๆ ดังนี้

3.1.1 ความสามารถในการสร้างกฎไฟร์วอลล์

ความสามารถในการสร้าง กฎไฟร์วอลล์ ของ ราชพีเบอร์รี่ พาย ไฟร์วอลล์ มีปริมาณข้อมูลอยู่ที่ 58 Mbps แตกต่างจาก คิวบ์บอร์ดไฟร์วอลล์ (cubieboard firewall) ที่ทำงานอยู่ที่ 54Mbps และเมื่อทำการเพิ่มจำนวนกฎเพิ่มขึ้น จำนวนทรูพุท (throughput) คิวบ์บอร์ด ไฟร์วอลล์ จะสูงกว่าเมื่อเทียบกับ ราชพีเบอร์รี่ พาย ไฟร์วอลล์ ซึ่งลักษณะความสามารถจะเป็นไปตามรูปที่ 3



รูปที่ 3 ประสิทธิภาพของการสร้างกฎของไฟร์วอลล์ ระหว่าง ราชพีเบอร์รี่ พาย ไฟร์วอลล์ มาเทียบกับ คิวบ์บอร์ด ไฟร์วอลล์ [9]

3.1.2 คุณสมบัติและความสามารถของการทำงานทั่วไป

ในงานวิจัยนี้จะกล่าวคุณสมบัติภายในของ ระหว่าง ราชพีเบอร์รี่ พาย ไฟร์วอลล์ มาเทียบกับ คิวบ์บอร์ด ไฟร์วอลล์ โดยที่ ราชพีเบอร์รี่ พาย ไฟร์วอลล์ ทำงานด้วยหน่วยประมวลผล สถาปัตยกรรม ARM ความเร็ว 700MHz เก็บข้อมูลด้วย มัลติมีเดียการ์ด (multimedia card : MMC) ภายนอก หรือผ่าน เอสดีการ์ด (SD card) ซึ่งมีอินเตอร์เฟสการใช้งาน พอร์ทเอนกประสงค์ (general-purpose input/output : GPIO) และ พอร์ทสื่อสารข้อมูลแบบ

อนุกรม (universal asynchronous receiver/transmitter : UART) รวมอยู่ในซอฟต์แวร์ด้วย ซึ่งเป็นที่นิยมมากในการพัฒนาอุปกรณ์ด้วยระบบปฏิบัติการลินุกซ์

ส่วน คิวบ์บอร์ด ไฟร์วอลล์ ทำงานด้วยสถาปัตยกรรม ARM เช่นเดียวกับ ราชพีเบอร์รี่ พาย ไฟร์วอลล์ ความเร็ว 1 GHz และเก็บข้อมูลด้วยหน่วยจัดเก็บภายในขนาด 4 GB NAND Flash และสามารถเพิ่มหน่วยความจำผ่าน เอสดีการ์ด (SD card) ได้ และอินเตอร์เฟสการใช้งานเพิ่มเติม อย่างเช่น ช่องเสียบยูเอสบี , ช่องการสื่อสารแบบอนุกรมแบบซิงโครนัส (inter-integrated circuit : I2C) , พอร์ทสถานะสัมผัส (serial peripheral interface : SPI) และ พอร์ทช่องแรงดันไฟฟ้าที่แตกต่างกัน (low-voltage differential signaling : LVDS)

ในตารางที่ 1 เป็นการเปรียบเทียบคุณสมบัติระหว่าง ราชพีเบอร์รี่ พาย ไฟร์วอลล์ มาเทียบกับ คิวบ์บอร์ด ไฟร์วอลล์

ตารางที่ 1 คุณสมบัติการใช้งานระหว่าง ราชพีเบอร์รี่ พาย ไฟร์วอลล์ กับ คิวบ์บอร์ด ไฟร์วอลล์ [9]

คุณสมบัติ	Raspberry Pi	Cubieboard
หน่วยประมวลผล(MHz)	700	1000
GPU	24	7.2
ความจำ	512	1024
Ethernet	10/100	10/100
ราคา (\$)	35	59

3.2 ราชพีเบอร์รี่ พาย ไฟร์วอลล์ กับ เราท์เตอร์ในระดับกลางในแง่ไฟร์วอลล์

โดยในที่นี้จะใช้ เราท์เตอร์ยี่ห้อ Cisco 1900 series มาเป็นตัวแทนของ เราท์เตอร์ในระดับกลางเพื่อทำการเปรียบเทียบประสิทธิภาพในด้านคุณสมบัติ และความสามารถในการทำงานของไฟร์วอลล์

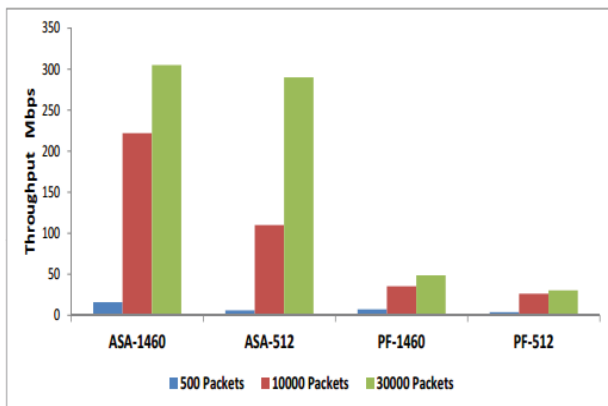
3.2.1 การเปรียบเทียบในแง่ของไฟร์วอลล์

ในเราท์เตอร์ดังกล่าวนี้การที่จะสามารถมีคุณสมบัติในการป้องกันความปลอดภัยของอินเทอร์เน็ตได้ จะต้องทำการลงซอฟต์แวร์เพิ่มเติมเพื่อเพิ่มความสามารถในการทำงานของเราท์เตอร์ ซึ่ง ซอฟต์แวร์นั้นมีชื่อว่า Cisco IOS Firewall [10] ซึ่งคุณสมบัติในการทำงานมีดังนี้

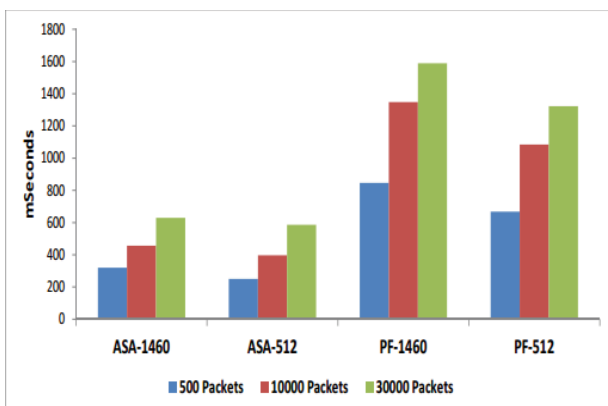
- ตรวจสอบแพ็คเกจ สเตตฟูล (stateful) สำหรับการใช้งานไฟร์วอลล์จริง
- การตรวจสอบ พร็อกซี่ (proxy) เพื่อควบคุมการเข้าถึงทรัพยากร
- การขอตรวจสอบการป้องกันโปรโตคอลทั่วไปและโปรแกรม
- สนับสนุน ไฟร์วอลล์โปร่งแสง (transparent firewall)
- ป้องกันการกระจายปฏิเสธบริการ (DDOS)
- บันทึกการติดต่อและสนับสนุนการตรวจสอบและแจ้งเตือน

ซึ่งคุณสมบัติดังกล่าวจะเป็นส่วนที่เพิ่มเติม (add-ons) ของเราเตอร์ เพื่อให้อุปกรณ์ดังกล่าวสามารถทำงานเป็นไฟร์วอลล์ป้องกันการโจมตีของอินเทอร์เน็ตได้

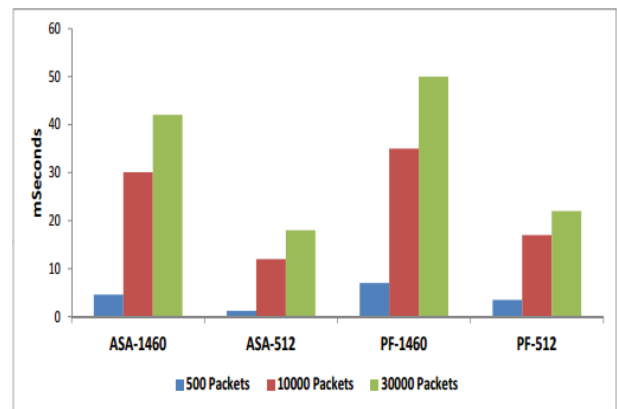
โดยจากงานวิจัยของ Thajer Hayajneh, Bassam J. Mohd , Awni Itradat, และ Ahmad Nahar Quttoum [11] ที่นำเสนอเรื่อง Performance and Information Security Evaluation with Firewalls ได้นำเสนอเกี่ยวกับประสิทธิภาพการทำงานของไฟร์วอลล์ในเชิงสถิติ ของอุปกรณ์ที่เป็นไฟร์วอลล์โดยตรงกับเราเตอร์ที่เพิ่มซอฟต์แวร์ โดยในที่นี้จะให้ความสำคัญในส่วนที่เป็นเราเตอร์ที่เพิ่มซอฟต์แวร์ ผลลัพธ์ที่ได้นั้น เมื่อทำการใส่ ข้อมูลแพ็คเกจ (packets) ที่เพิ่มมากขึ้น จะทำให้ จำนวนข้อมูลที่เข้ามา (throughput) มากขึ้น มี สัดส่วนความล่าช้า (delay) ที่เพิ่มขึ้น และค่าความแปรปรวนของความล่าช้า (jitter delay) ที่เพิ่มมากขึ้น ตามสถิติในรูป 4 , 5 และ 6 ซึ่งจะสังเกตว่าไฟร์วอลล์โดยตรงนั้น สามารถทำประสิทธิภาพได้มากกว่า เราเตอร์ที่ทำการเพิ่มซอฟต์แวร์เข้าไป



รูปที่ 4 ประสิทธิภาพของ throughput เมื่อส่งแพ็คเกจในขนาดต่าง ๆ [11]



รูปที่ 5 ประสิทธิภาพของเวลาในการล่าช้าเมื่อส่งแพ็คเกจในขนาดต่าง ๆ [11]



รูปที่ 6 ประสิทธิภาพของความแปรปรวนในการล่าช้าเมื่อส่งแพ็คเกจในขนาดต่าง ๆ [11]

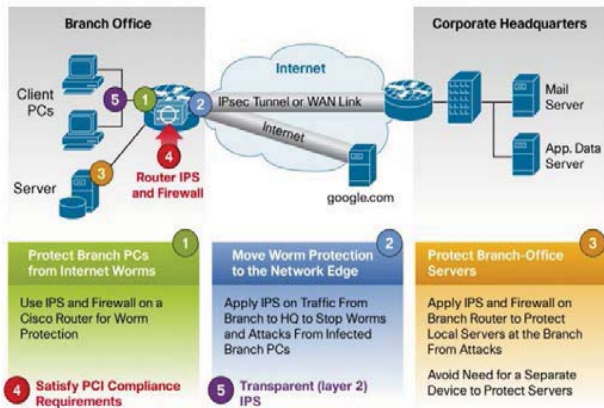
แต่ทั้งนี้อาจจะสรุปได้ว่า คุณสมบัติดังกล่าวนี้ เราเตอร์เมื่อทำการเพิ่มซอฟต์แวร์ที่สามารถทำงานเกี่ยวกับไฟร์วอลล์ได้ จะมีความสามารถในการตรวจสอบและป้องกันภัยคุกคามทางอินเทอร์เน็ตได้ ซึ่งในแต่ละรุ่นนั้น จะมีความสามารถในการรองรับประสิทธิภาพที่แตกต่างกันออกไป ทั้งนี้เนื่องจากปัจจัยในด้านคุณสมบัติภายในต่างๆ ซึ่งจะกล่าวในข้อต่อไป

3.2.2. การเปรียบเทียบคุณสมบัติของระบบตรวจสอบและป้องกันการบุกรุก

ในส่วนของ Cisco 1900 Series นั้น เมื่อทำการติดตั้ง Cisco IOS Firewall แล้วเมื่อทำการติดตั้งคุณสมบัติของระบบตรวจสอบการบุกรุก (intrusion detection system : IDS) นั้น ทำให้การทำงานของเราเตอร์นั้นมีประสิทธิภาพลดลง [12] และทำให้สูญเสียหน่วยความจำส่วนหนึ่งไปกับการทำงานนี้ โดยคุณสมบัติของ IOS Firewall IDS นั้น มีการทำงานดังนี้

- สามารถส่งการแจ้งเตือนไปยังหน่วยงานกลางได้
- สามารถทั้งแพ็คเกจที่ไม่พึงประสงค์ได้
- สามารถรีเซตการเชื่อมต่อโปรโตคอล ทีซีพี (TCP) ได้

ส่วนระบบป้องกันการบุกรุก [13] (intrusion prevention system : IPS) นั้น เป็นส่วนที่ต้องทำการเพิ่มซอฟต์แวร์ต่างหากเข้ามาเพื่อเพิ่มคุณสมบัติในการป้องกันการบุกรุกของภัยคุกคามต่างๆได้ ซึ่งคุณสมบัติต่างๆนั้น แสดงในรูปที่ 7



รูปที่ 7 คุณสมบัติการทำงานของระบบป้องกันการบุกรุกของเราเตอร์

Cisco [13]

ส่วนของ ราสเบอร์รี่ พาย ไฟร์วอลล์ การทำงานของระบบตรวจสอบและระบบป้องกันการบุกรุกนั้น จะต้องทำการเพิ่มเฟิร์มแวร์เพิ่มเติม (add-on) [5] เพื่อทำการเพิ่มคุณสมบัติดังกล่าวเข้ามา ซึ่งในบาง add-on นั้น สามารถทำงานได้ทั้งการตรวจสอบและการป้องกันการบุกรุกในตัวเดียวกันได้ เช่น Guardian ,Snort เป็นต้น

3.3 การเปรียบเทียบในเชิงราคาของอุปกรณ์

ในส่วนของราคานั้น เนื่องด้วยราคาของ Cisco Router 1900 Series นั้น เป็น เราเตอร์ในหน่วยงานธุรกิจขนาดกลาง ราคาของอุปกรณ์ก็อยู่ในขอบเขตของหน่วยงานธุรกิจขนาดกลางสามารถยอมรับได้ ช่วงราคาจะอยู่ที่ [14] 21,000 – 52,000 บาท แต่ในส่วนของบริษัท ราสเบอร์รี่ พาย นั้น ในส่วนของต้นทุนบริษัท ราคาจะอยู่ที่ ประมาณ 35 \$ หรือคือเป็นเงินไทยอยู่ที่ประมาณ 1,050 บาท โดยราคานี้ไม่รวมอุปกรณ์เสริมอื่นๆ ซึ่งราคานั้นเหมาะสมสำหรับ ธุรกิจขนาดเล็กที่มีงบประมาณค่อนข้างจำกัด แต่ทั้งนี้ทั้งนั้นเอง เมื่อราคาสูงมากขึ้น คุณภาพของตัวอุปกรณ์ก็จะดีขึ้นตามไป แต่ทั้งนี้ก็ต้องขึ้นอยู่กับความเหมาะสมกับข้อมูลที่รับเข้ามา และองค์ประกอบอื่นๆที่ต้องพิจารณาด้วย

3.4 ข้อจำกัดบางประการ

ในส่วนของคุณลักษณะการทำงานเบื้องต้นนั้น เนื่องจาก ราสเบอร์รี่ พาย ไฟร์วอลล์ เป็นบอร์ดสมองกลที่มีขนาดเล็กและราคาถูก คุณสมบัติบางอย่างก็ไม่สามารถทำได้เหมือนกับเราเตอร์ขนาดกลางในแง่ของไฟร์วอลล์ได้ทั้งหมด อย่างเช่น ข้อจำกัดในเรื่องของ แบนด์วิธ (Bandwidth) การใช้งานที่ ราสเบอร์รี่ พาย ไฟร์วอลล์ ทำงานในแบนด์วิธ ที่น้อยกว่า ทั้งนี้เพราะมาจากอีเทอร์เน็ต พอร์ต ที่รองรับได้สูงสุดแค่ 100 Mbps[4] ซึ่งไม่เหมือนกับเราเตอร์ขนาดกลางที่สามารถทำได้สูงสุด 1 Gbps[10] ซึ่งวิธีการแก้ปัญหานี้สามารถทำได้โดยการเพิ่มบอร์ดดังกล่าวเพื่อเป็น โหลดบาลานซ์ (Load Balance) หลายๆตัวยืดหยุ่นกับความต้องการของแต่ละธุรกิจ และคุณสมบัติภายนอก ถ้านำไปใช้ในแง่ของไฟร์วอลล์นั้น เนื่องจาก

พีเบอร์รี่ พาย ไฟร์วอลล์ มีพอร์ต อีเทอร์เน็ต (LAN) แค่ 1 พอร์ตเท่านั้น แต่เนื่องด้วยคุณสมบัติของไฟร์วอลล์ที่จะต้อง มี พอร์ต อย่างน้อย 2 พอร์ตขึ้นไป

เพื่อที่รองรับเส้นทาง สำหรับ ข้อมูลขาเข้า (Inbound Port) และ ข้อมูลขาออก (Outbound port) ที่จะเข้าไปยังเราเตอร์นั้น วิธีการแก้ปัญหานี้ของ ราสเบอร์รี่ พาย ไฟร์วอลล์ นั้น จะต้องใช้ พอร์ตยูเอสบี ในการที่จะแปลงเป็น อีเทอร์เน็ตพอร์ตาอกให้ซึ่งจะต้องเสียทรัพยากรของพอร์ตยูเอสบีไป 1 ช่องเพื่อรองรับคุณสมบัติดังกล่าว แต่ทั้งนี้เนื่องจากความต้องการพื้นฐานของหน่วยงานธุรกิจขนาดเล็ก ซึ่งไม่จำเป็นต้องใช้ข้อมูลที่มาก การใช้ ราสเบอร์รี่ พาย ไฟร์วอลล์ เพียงตัวเดียวเพื่อป้องกันภัยคุกคามอินเทอร์เน็ต เพียงพอสำหรับหน่วยงานธุรกิจดังกล่าว

4.บทสรุป

ในบทความนี้ได้เสนอแนวคิดเกี่ยวกับการเอาบอร์ด ราสเบอร์รี่ พาย มาประยุกต์ใช้กับไฟร์วอลล์ ที่ได้แสดงให้เห็นถึงคุณสมบัติของราสเบอร์รี่ พาย ไฟร์วอลล์ และซอฟต์แวร์ที่นำมาใช้เป็นไฟร์วอลล์ และได้เปรียบเทียบประสิทธิภาพการทำงานในแง่ของทรัพยากรกับการตั้งกฎของไฟร์วอลล์ เทียบกับคิมบอร์ด ไฟร์วอลล์ โดยประสิทธิภาพของคิมบอร์ดไฟร์วอลล์ ดีกว่า ราสเบอร์รี่ พายไฟร์วอลล์เล็กน้อย ราสเบอร์รี่ พายไฟร์วอลล์ มีความสามารถและการทำงานเทียบเคียงกับเราเตอร์ขนาดกลางในแง่ของการทำงานไฟร์วอลล์ ได้ อย่างเช่น การตั้งกฎของไฟร์วอลล์ รวมถึงการตรวจจับและป้องกันภัยคุกคาม แต่ทั้งนี้ ในส่วนของการทำงานนั้น ราสเบอร์รี่ พาย ไฟร์วอลล์นั้น อาจจะมีย่อจำกัดต่างอย่างเช่น แบนด์วิธในการใช้งาน รวมถึงประสิทธิภาพที่ลดลงเมื่อเปรียบเทียบกับเราเตอร์ในระดับกลางในแง่ไฟร์วอลล์ ส่วนในด้านของราคานั้น ราคาของบริษัท ราสเบอร์รี่ พายมีราคาขายอยู่ที่ ไม่เกินสองพันบาท นั้น มีราคาถูกมาก เมื่อเทียบกับเราเตอร์ขนาดกลางที่มีราคาขายอยู่ที่ 21,000 – 52,000 บาท ทำให้ราสเบอร์รี่ พาย ไฟร์วอลล์ เป็นทางเลือกของ หน่วยงานธุรกิจขนาดกลางและขนาดเล็ก ที่ต้องการประหยัดต้นทุนของไฟร์วอลล์ได้

เอกสารอ้างอิง

- [1] The OWASP Foundation, "The OWASP Top 10 - 2013," 2013.
- [2] Paul Wood, Ed., "INTERNET SECURITY THREAT REPORT 2014," Symantec Corporation, 2014, vol. 19, p. 18.
- [3] Monika Joshi and Chirag Gohel, "Agent Base Network Traffic Monitoring," *International Journal of Innovative Research in Science, Engineering and Technology*, vol. 2, no. 5, pp. 1799–1803, May 2013.
- [4] Raspberry Pi Foundation, "Raspberry Pi Hardware", Available : <https://www.raspberrypi.org/documentation/hardware/raspberrypi/>
- [5] IPFire, "About IPFire", Available : <http://www.ipfire.org/features>
- [6] Karen Mercedes Goertzel, "Information Assurance Tools Report – Firewalls. Seventh Edition," IATAC, Report, Feb. 2011.
- [7] Bhisham Sharma and Karan Bajaj, "Packet Filtering using IP Tables in Linux", *IJCSI International Journal of Computer Science Issues*, Vol. 8, Issue 4, No 2, July 2011



[8] IBM, "Developing IBM PureData System for Hadoop applications with the Eclipse IDE", Available :

<http://www.ibm.com/developerworks/library/bd-openvpn>

[9] Zubair Nabi, "A \$35 Firewall for the Developing World," IBM Research, 2014.

[10] Cisco System Inc., "Cisco IOS Firewall", 2011

[11] Thaier Hayajneh, Bassam J. Mohd , Awni Itradat, and Ahmad Nahar Quttoum, "Performance and Information Security Evaluation with Firewalls", International Journal of Security and Its Applications Vol.7, No.6 (2013), pp.355-372

[12] Cisco System Inc., "Cisco IOS Security Configuration Guide", 2001-2006, pp.sc271-290

[13] Cisco System Inc., "Cisco IOS Inline Intrusion Prevention System (IPS)", 2010.

[14] Networksure Limited Partnership, "Router Cisco Price", Available: <http://www.networksure.co.th/products/router/cisco-1900-series>