ผลกระทบจากการโจมตีด้วย DoS/DDoS ที่มีต่อโอเพนซอร์สไฟร์วอลล์

Impact of DoS/DDoS attacks on Open-source Firewalls

ไกรลาศ ศิลกุล[1]

ชัยพร เขมะภาตะพันธ์[2]

บทคัดย่อ

ไฟร์วอลล์นับเป็นองค์ประกอบสำคัญในการรักษาความปลอดภัยเครือข่ายคอมพิวเตอร์ ที่เชื่อมต่อสื่อสารกับภายนอก เช่น เครือข่ายอินเตอร์เน็ต ซึ่งผู้บุกรุกใช้เป็นช่องทางเข้าโจมตีระบบภายใน สารนิพนธ์นี้ศึกษาถึงผลกระทบเชิงประสิทธิภาพที่เกิดจากการโจมตีแบบ DoS/DDoS ทีมีต่อการทำงานของไฟร์วอลล์ที่นำมาทดสอบ 3 ผลิตภัณฑ์ได้แก่ pfSense, Endian และ OPNsense โดยไฟร์วอลล์ที่นำมาเพื่อทำการทดสอบเหล่านี้ได้ผ่านเกณฑ์การพิจารณาคัดเลือกจากซอฟท์แวร์ไฟร์วอลล์ชนิดฟรี โอเพนซอร์ส ภายใต้แพลตฟอร์มลินุกซ์ และเป็นผลิตภัณฑ์ปล่อยออกมาให้ใช้งานในช่วงเวลาใกล้เคียงกัน รวมไปถึงต้องเป็นที่นิยมใช้อย่างแพร่หลาย ในปัจจุบัน

การวัดผลกระทบจากการโจมตีแบบ DoS/DDoS พิจารณาปฏิกิริยาซึ่งเกิดขึ้นหลังจากถูกโจมตีจนกระทั่งไฟร์วอลล์นั้นไม่สามารถทำงานตามได้ตามปกติ นอกจากการศึกษาผลกระทบดังกล่าว ยังสามารถวัดจากประสิทธิภาพทางด้านต่างๆ ได้แก่ ปริมาณ Throughput การใช้ทรัพยากร CPU และ Memory

ผลการทดสอบได้แสดงให้เห็นว่า ไฟร์วอลล์ทั้งสามมีการตอบสนองต่อการโจมตีดังกล่าวแตกต่างกันจำแนกได้เป็นสองส่วน โดยส่วนแรกพิจารณาผลในแง่ของปริมาณ Throughput การใช้ทรัพยากร CPU และ Memory ซึ่งไฟร์วอลล์ pfSense ให้ประสิทธิภาพสูงสุดในด้านนี้ ในส่วนหลังวัดผลความทนทานต่อการโจมตี โดยวัดจากระยะเวลาที่ไฟร์วอลล์ยังคงทำงานตามได้ตามปกติเป็นระยะเวลานานที่สุดตั้งแต่ถูกโจมตี ไฟร์วอลล์ Endian มีความทนทานมากที่สุด อย่างไรก็ตามเหตุการณ์นี้ได้พบว่า ไฟร์วอลล์ทุกตัวตอบสนองไปในทิศทางเดียวกันคือ จะหยุดทำงานลงจนกระทั่งไม่สามารถส่งผ่านแพกเก็ตได้

คำสำคัญ: โอเพนซอร์สไฟร์วอลล์, การโจมตีแบบ DoS/DDoS, pfSense, Endien, OPNsense, Benchmarking

---

[1] นักศึกษาหลักสูตรวิศวกรรมคอมพิวเตอร์และโทรคมนาคม วิทยาลัยนวัตกรรมด้านเทคโนโลยีและวิศวกรรม มหาวิทยาลัยธุรกิจบัณฑิตย์

[2] ที่ปรึกษาวิทยานิพนธ์

Abstract

Firewalls are important components in network security that connects to external networks such as the Internet, which is an interface that allows intruders to attack an internal system. This thematic research studies and investigates the impact from DoS/DDoS attacks to performance of firewalls; pfSense, Endian and OPNsense. The firewalls that are used for these tests have passed the criteria of selecting free open source firewall software running on the Linux platform. They are also products that launched simultaneously, which are widely applied and still in use until now.

The impact from DoS/DDoS attacks can be measured from durability and reaction after an attack until the firewalls can not operate as normal. Moreover, the study of the impact is also involves benchmarking measurement of throughput, CPU utilization, memory usage of the firewalls.

The test results show that the three firewalls respond differently to these attacks, which are observed from two perspectives. First, in term of performance, it can be noted that the pfSense firewall provides the highest performance. From the second perspective, durability from the attacks which is measured from the longest time that the firewalls still operate normally since the attack happened. Endian firewall has the highest durability. However, from this part of the study, it can be noted that all the firewalls will have the same reaction, i.e., they stop their operation yielding in stopping packet transfer and filtering.
Keywords: Open-source Firewall, DoS/DDoS attack, pfSence, Endien, OPNsense, Benchmarking.

1. บทนำ

การเชื่อมต่อคอมพิวเตอร์ต่างๆ เพื่อสื่อสารกับเครื่องในต่างพื้นที่กันนั้น บริการเครือข่ายที่นิยม เช่น อินเตอร์เน็ตมักเสี่ยงต่อการถูกเข้าโจมตีได้โดยง่ายเนื่องจากเป็นเครือข่ายสาธารณะ การสร้างมาตรการรักษาความปลอดภัยให้แก่ระบบจึงมีความจำเป็น ที่ทำได้หลากหลายแนวทาง แต่วิธีที่ได้รับความนิยม คือ การนำไฟร์วอลล์มาเป็นเครื่องมือปกป้องระบบ ซึ่งในปัจจุบันมีผลิตภัณฑ์ซอฟท์แวร์แบบโอเพนซอร์สให้นำมาใช้งานโดยไม่เสียค่าใช้จ่ายใดๆ อยู่มากมาย ต่างก็มีคุณสมบัติที่แตกต่างกันตามแนวทางการออกแบบของผู้พัฒนาแต่ละราย

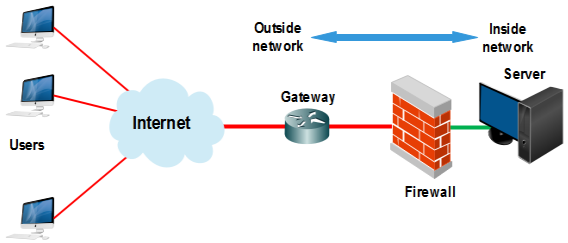
ช่องทางภัยคุกคามผ่านการใช้บริการของเครือข่ายสาธารณะนั้น การโจมตีแบบ DoS/DDoS นับเป็นภัยคุกคามซึ่งก่อให้เกิดความเสียหาย และลดความสามารถการทำงานของระบบลง ซึ่งการประเมินผลกระทบที่เกิดจากการโจมตีด้วย DoS/DDoS ที่มีต่อไฟร์วอลล์ดังกล่าว จึงนับเป็นสิ่งจำเป็น ทั้งนี้เพื่อให้สามารถระบุค่าพารามิเตอร์สำคัญที่สร้างผลกระทบต่อการทำงานของระบบที่นำไฟร์วอลล์มาติดตั้งใช้งาน ดังนั้นปัญหาในการสร้างเครื่องมือสำหรับการชี้วัดผลกระทบจากการโจมตีดังกล่าว ที่มีต่อโอเพนซอร์สไฟร์วอลล์ จึงนับว่ามีความน่าสนใจเป็นอย่างยิ่ง ซึ่งมีประโยชน์ทั้งช่วยในการพิจารณาเลือกไฟร์วอลล์

มาใช้ให้เหมาะสมกับงานแต่ละแบบ และช่วยให้สามารถออกแบบและพัฒนากระบวนการทดสอบและประเมินไฟร์วอลล์ทำได้อย่างมีลำดับและขั้นตอน

2. ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

2.1 ไฟร์วอลล์ [1]

เป็นหนึ่งในเครื่องมือสำหรับสร้างมาตรการรักษาความปลอดภัยให้แก่คอมพิวเตอร์ที่เชื่อมต่อใช้งานอยู่บนเครือข่าย มีหน้าที่หลักในการป้องกันข้อมูล และระบบให้ปลอดภัยจากการคุกคามรูปแบบต่างๆ เครื่องมือนี้สามารถเป็นได้ทั้งซอฟท์แวร์ ฮาร์ดแวร์ หรือเป็นทั้งสองแบบรวมกัน ขึ้นอยู่กับจุดประสงค์ที่พัฒนาขึ้นมาเพื่อประยุกต์ใช้กับงานต่างๆ ที่มีความหลากหลายแตกต่างกันไป ไฟร์วอลล์จึงเป็นส่วนแรกของระบบเครือข่ายที่รับข้อมูลขาเข้า และยังเป็นส่วนสุดท้าย ที่จัดการข้อมูลขาออก เป็นส่วนทำหน้าที่ตัดสินใจเกี่ยวกับการอนุญาตให้มี หรือระงับการสื่อสารสำหรับส่งผ่านข้อมูลระหว่างกันของคอมพิวเตอร์ที่เชื่อมต่อใช้งานบนเครือข่าย โดยการตัดสินใจดังกล่าวนั้นเกิดจากการกำหนดนโยบาย (Policy) สำหรับสร้างกฎการคัดกรอง (Rules) ความถูกต้องของแพกเก็ตที่ใช้ในการสื่อสารระหว่างกัน โดยรูปแบบพื้นฐานการใช้งานที่ทำการจัดวางไฟร์วอลล์แทรกไว้ระหว่างเครือข่ายภายในและเครือข่ายภายนอก ทั้งนี้เพื่อประโยชน์ในการควบคุมการเข้าและออกของข้อมูลหรือบริการต่างๆ ที่ต้องผ่านการเปรียบเทียบตามกฎการคัดกรองของไฟร์วอลล์ในทุกครั้งเสียก่อน จึงจะมีสิทธิผ่านเข้าสู่การใช้บริการต่างๆ จากเครือข่ายภายในได้ ดังแสดงรูปแบบพื้นฐานไฟร์วอลล์ที่เชื่อมต่อใช้งานบนเครือข่ายในรูปที่ 1



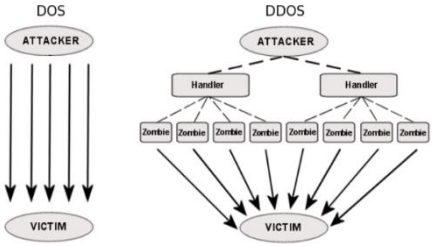
รูปที่ 1 โครงสร้างพื้นฐานระบบไฟร์วอลล์

เทคโนโลยีไฟร์วอลล์ [2],[3] เป็นรูปแบบที่เปลี่ยนแปลงไปตามความต้องการที่เกิดขึ้นอย่างรวดเร็ว ส่งผลให้ไฟร์วอลล์มีความหลากหลายยิ่งขึ้น ทั้งในเชิงการป้องกันภัยคุกคามต่างๆ และในเชิงการใช้งาน ซึ่งหากจำแนกไฟร์วอลล์ตามช่วงในการพัฒนานั้น สามารถเริ่มได้จากรูปแบบ Packet Filtering firewall ที่เป็นเทคโนโลยีรุ่นแรกๆ ของไฟล์วอลล์ ตรวจสอบคัดกรองข้อมูลในระดับเครือข่ายของ TCP/IP บนชั้นอินเตอร์เน็ต โดยพิจารณาจากข้อมูลส่วนที่อยู่ในเฮดเดอร์ของแพกเก็ตที่ผ่านเข้ามาเทียบกับกฎที่กำหนดไว้และตัดสินว่าควรจะทิ้งหรือยอมให้แพกเก็ตนั้นผ่านไปได้ รูปแบบ Application Gateway firewall ตรวจสอบการข้อมูลถึงระดับชั้นแอพพลิเคชัน โดยแอพลิเคชันแต่ละตัวเรียกว่า พร็อกซีเซิร์ฟเวอร์ (Proxy Server)

มีหลักการทำงานคือ เมื่อไคลเอนต์ต้องการรับบริการเพื่อเชื่อมต่อไปยังภายนอก จะต้องส่งคำขอไปยังแอพพลิเคชันเพื่อสั่งให้ พร็อกซี่เซิร์ฟเวอร์ทำการเชื่อมต่อเครือข่ายภายนอกกับภายใน รูปแบบ Stateful Inspection firewall ควบคุมการเชื่อมต่อที่เกิดระหว่างเครือข่ายภายนอกกับภายในเช่นเดียวกับที่มีในเทคโนโลยีรุ่นก่อน โดยได้เพิ่มตารางใช้ระบุสถานะ (State Table) เมื่อได้รับแพกเก็จเข้ามา หลักการการคัดกรองจะนำแพกเก็จปัจจุบันมาเปรียบเทียบแพกเก็จที่เก็บบันทึกไว้ หากพบว่าแพกเก็ตนั้นเคยระบุในตารางดังกล่าว ไฟร์วอลล์ก็จะอนุญาตให้แพกเก็ตผ่านไปได้โดยไม่ต้องตรวจสอบซ้ำอีก

2.2 การโจมตีแบบปฏิเสธการให้บริการ [4]

รูปแบบการโจมตีโดยปฏิเสธให้บริการทั้งแบบ DoS (Denial of Service) และแบบ DDoS (Distribution Denial of Service) ล้วนแต่มีจุดมุ่งหมายเป็นเช่นเดียวกันคือ ทำให้เครื่องหรือระบบที่เป็นเป้าหมายไม่สามารถตอบสนองการให้บริการใดๆ แก่ผู้ใช้ได้ ซึ่งผลการโจมตีนี้จะทำให้ทรัพยากรของเครื่องเป้าหมายถูกใช้จนหมดไปอย่างรวดเร็ว จนกระทั่งไม่สามารถทำงานได้ตามปกติการ หรือมีระดับการให้บริการต่ำมาก



รูปที่ 2 รูปแบบพื้นฐานการโจมตีแบบ DoS และ DDoS
ที่มา: ภาพประกอบจากเว็บไซต์ https://www.securetia.com

กลวิธีการโจมตีแบบ DoS/DDoS [5] มักนิยมใช้การส่งแพกเก็ตในลักษณะที่ผิดไปจากรูปแบบปกติ ส่งผลให้เกิดการเปลี่ยนแปลงของข้อมูลสำคัญที่ใช้ควบคุมกลไกในการสื่อสาร และสร้างความสับสนต่อการจัดการระบบโดยรวม โดยวิธีการโจมตีที่นิยมใช้ เช่น Syn-flooding Attack โจมตีเพื่อเข้าควบคุมเครื่องที่ถูกระบุไว้ไม่ให้ส่งข้อมูลตอบกลับ สร้างให้เกิดสภาวะ half-open ขึ้นที่เครื่องเป้าหมาย ส่งผลให้ลำดับของบริการของเครื่องเป้าหมายเต็มทำให้ระบบล่มได้ ชนิด Smurf Attack ใช้วิธีการปลอม IP ด้านต้นทางให้เป็น IP ของเป้าหมาย โดยที่ผู้โจมตีจะส่ง ICMP Echo Request ไปยังส่วน Broadcast address ในเครือข่าย ทำไห้ให้เครือข่ายซึ่งเป็นตัวกลางส่ง ICMP Echo Reply กลับไปยัง IP ของเป้าหมายทันที ซึ่งส่งผลให้มีการใช้งานแบนด์วิดธ์จนเต็ม ชนิด Ping of Death Attack จะใช้วิธีการดัดแปลงแก้ไขความยาวของ IP แพกเก็ตที่ใช้ในการปิง (Ping) ให้มีความยาวกว่าปกติ ก่อนส่งไปโจมตียังเครื่องเป้าหมายที่ใช้โปรโตคอล TCP/IP ในการติดต่อสื่อสาร ซึ่งผลที่เกิดขึ้นนี้อาจทำให้ระบบของเครื่องคอมพิวเตอร์ล่ม (Crash) ได้

นอกจากรูปแบบต่างๆ ที่ได้กล่าวมาข้างต้นแล้ว ยังมีการโจมตีในรูปแบบ DoS/DDoS อื่นๆ ที่เป็นภัยคุกคามต่อระบบอีกหลากหลายแบบ เช่น Ping flood, UDP Flood, Mail Bomb และ Fraggle Attack เป็นต้น แต่ด้วยเทคโนโลยีที่มีในปัจจุบันมีประสิทธิภาพสูงขึ้น ทำให้ผู้โจมตีนำรูปแบบเหล่านี้มาใช้งานลดลง เนื่องจากมีโอกาสประสบความสำเร็จน้อยมาก

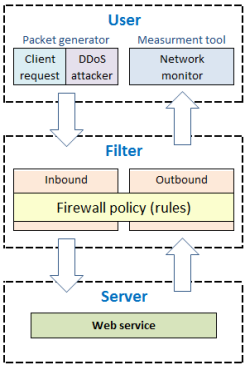
2.3 งานวิจัยที่เกี่ยวข้อง

[6] Muhammad Zeeshan Ahmad ดำเนินการทดสอบประสิทธิภาพโอเพ่นซอร์ส ไฟร์วอลล์ 2 แบบคือ IPtables และ Shorewall ซึ่งพบว่า Shorewall มีประสิทธิภาพโดยรวมสูงกว่า IPtables ในทุกด้านที่ทดสอบ [7] Wenhui Su และ Junjie Xu ทดสอบไฟร์วอลล์ที่ทำงานบนแพลตฟอร์มต่างชนิดกันที่ได้แก่ Cisco ASA5505 เป็นชนิดฮาร์ดแวร์และ Linux IPtables ที่เป็นซอฟท์แวร์ พบว่าแบบฮาร์ดแวร์มีประสิทธิภาพโดยรวมสูงกว่า [8] Chirag Sheth และ Rajesh Thakker ทดสอบไฟร์วอลล์แบบฮาร์ดแวร์ Cisco ASA และแบบซอฟท์แวร์ 2 ผลิตภัณฑ์ได้แก่ CP SPLAT แบบต้องมีค่าใช้จ่าย และ OpenBSD PF ที่สามารถนำมาใช้ได้ฟรี ทดลองใช้การโจมตีด้วยวิธีแบบ DDoS ผ่านทางโปรโตคอล http พบว่า ไฟร์วอลล์แบบฮาร์ดแวร์สามารถแสดงประสิทธิภาพได้สูงสุด รองลงมาคือซอฟท์แวร์แบบมีค่าใช้จ่าย และแบบไม่มีค่าใช้จ่าย [9] Thaier Hayajneh, Bassam J. Mohd, Awni Itradat และ Ahmad Nahar ทดสอบไฟร์วอลล์ทำงานบนแพลตฟอร์มที่ต่างกันได้แก่ Cisco ASA 5510 แบบมีค่าใช้จ่าย และ Cisco Router 2811 ผลการทดสอบแสดงให้เห็นว่า ไฟร์วอลล์ Cisco ASA 5510 สามารถแสดงประสิทธิภาพโดยรวมได้สูงมากกว่าไฟร์วอลล์ Cisco Router 2811

3. ขั้นตอนการดำเนินงานวิจัย

3.1 ภาพรวมของระบบ

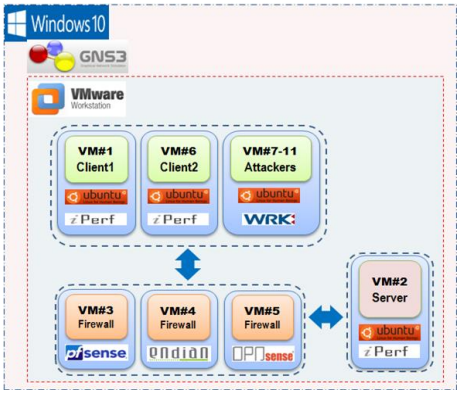
องค์ประกอบส่วนต่างๆ ดำเนินการด้วยวิธีจำลองสร้างเป็นระบบเสมือน (Virtual machine) แบ่งตามหน้าที่การทำงานได้เป็น 3 ส่วนหลักได้แก่ ส่วนผู้ใช้งาน (User) ทำหน้าที่ร้องขอใช้บริการ (Request) ส่งแพกเก็ตการใช้งานแบบปกติ และการจำลองให้มีการโจมตีแบบ DoS/DDoS รวมไปถึงการแสดงผล (Monitor) ข้อมูลจากที่ดำเนินการขอรับบริการดังกล่าว ส่วนทำหน้าที่คัดกรอง (Filter) แพกเก็ตที่ส่งมาจากผู้ใช้งาน กำหนดให้ต้องผ่านการตรวจสอบโดยไฟร์วอลล์ เพื่อพิสูจน์ความถูกต้องตรงตามนโยบายควบคุมการเข้าถึงข้อมูล ส่วนเครื่องให้บริการ (Services) กำหนดหน้าที่ให้บริการประเภท Web service โดยภาพรวมของระบบแสดงในรูปที่ 3



รูปที่ 3 ภาพรวมของระบบการวัดประสิทธิภาพไฟล์วอลล์

3.2 การดำเนินงานจัดสร้างระบบ

จัดวางองค์ประกอบส่วนต่างๆ เพื่อสร้างเครื่องมือการทดลองบนเครื่องคอมพิวเตอร์ ASUS GL752V, 2.7 GHz. Intel Core i7 6700HQ, Ram 16 GB BUS 2133MHz. สร้างเครือข่ายเสมือนผ่านโปรแกรม VMware โดยมีรายละเอียดในส่วนของซอฟท์แวร์ที่ติดตั้งดังรูปที่ 4



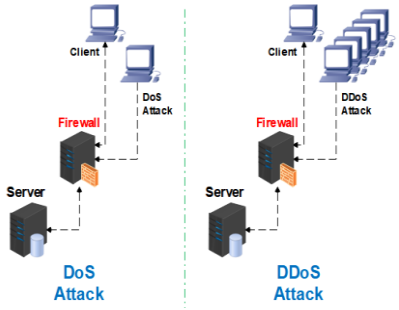
รูปที่ 4 ผังการติดตั้งซอฟท์แวร์

การติดตั้งในส่วนของซอฟท์แวร์ อ้างอิงตามที่ระบุไว้ในการออกแบบได้แก่ ส่วน Users กำหนดจัดตั้ง VM#1 และ VM#6 ทำหน้าที่ เป็น Client ที่ติดตั้งซอฟท์แวร์สำหรับจำลองสร้างแพกเก็ตเพื่อวัดผลด้าน Throughput และให้ VM#7 เป็น Attackers จำลองการโจมตีด้วย http แพกเก็ตเพื่อทดสอบด้าน Unreachable timeout และ Action response ในส่วนของ Filter ทำการติดตั้งไฟร์วอลล์ pfSense, Endian และ OPNsense บน VM#3, VM#4 และ VM#5 ตามลำดับ ซึ่งในส่วนนี้ใช้ชี้วัดค่า CPU utilization และ Memory usage ส่วนสุดท้ายทำหน้าที่เป็น Server ติดตั้งบน VM#2 ใช้สำหรับให้บริการ Web service เมื่อมีการร้องขอจาก Users

3.3 วิธีการทดลอง

การดำเนินงานครั้งนี้มีตัวอย่างไฟร์วอลล์ใช้สำหรับการทดสอบ 3 ผลิตภัณฑ์ที่ได้แก่ pfSense, Endian และ OPNsense ทำการวัดผลเพื่อเป็นเกณฑ์สำหรับประเมินไฟร์วอลล์ที่นำมาทดสอบ แบ่งเป็นสองกลุ่มคือ กลุ่มวัดผลเชิงประสิทธิภาพการทำงานได้แก่ Throughput เป็นจำนวน Transaction/Request ที่สร้างขึ้นหรือทำงานได้ในช่วงเวลาทดสอบหนึ่งๆ ที่ใช้ชี้วัดถึงระบบงานที่มีความสามารถการจัดการกับจำนวนงานสำเร็จ ในหนึ่งหน่วยเวลานั้นๆ การวัดค่า Resource consumption ซึ่งเป็นผลรวมการใช้ทรัพยากรเพื่อการ

ทำงานของระบบทั้งด้าน CPU และ Memory คำนึงถึงการใช้ประโยชน์จากทรัพยากรเหล่านี้ และอีกกลุ่มเป็นการวัดผลด้าน Unreachable timeout พิจารณาความทนทานต่อการโจมตี ชี้วัดจากระยะเวลาที่ไฟร์วอลล์ยังคงทำงานตามปกติ ตั้งแต่เริ่มต้นโจมตี จนกระทั่งหยุดการทำงานลงอย่างสมบูรณ์ และทดสอบด้าน Action response ที่พิจารณาผลตอบสนองที่ไฟร์วอลล์แสดงออกหลังจากการโจมตีดังกล่าวประสบความสำเร็จ โดยออกแบบการจัดวางเครือข่ายไว้สองแบบคือ เครือข่ายแบบ DoS และ DDoS ดังแสดงในรูปที่ 5

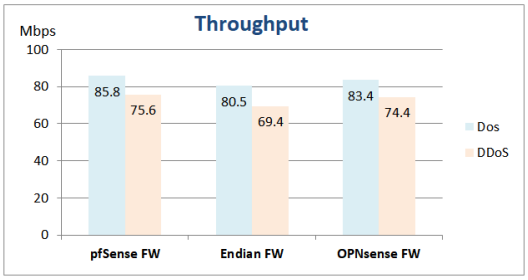


รูปที่ 5 การจัดรูปแบบตั้งเครือข่ายสำหรับการทดสอบ

4. ผลการวิจัย

แสดงการเปรียบเทียบผลการทดลองของไฟร์วอลล์ทั้งสาม ซึ่งสามารถแบ่งการรายงานผลและการวิเคราะห์ผลออกได้เป็นสองส่วนทั้งที่ทดสอบด้วยการโจมตีแบบ DoS และแบบ DDoS ดังแสดงด้วยแผนภูมิดังต่อไปนี้

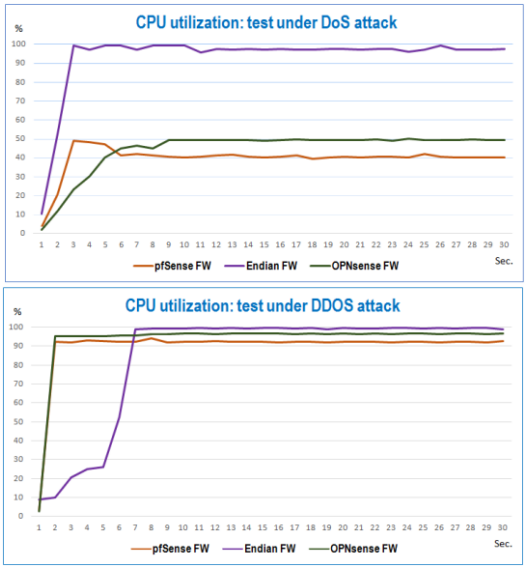
4.1 ผลการทดสอบด้าน Throughput



รูปที่ 6 เปรียบเทียบผลการทดลองด้าน Throughput

การทดสอบพบว่า ไฟร์วอลล์ pfSence มีคุณสมบัติการคัดกรองแพกเก็ตในเชิงปริมาณ Throughput สูงกว่าไฟร์วอลล์อีกสองแบบ ทั้งทดสอบโดยการโจมตีแบบ DoS และ DDoS

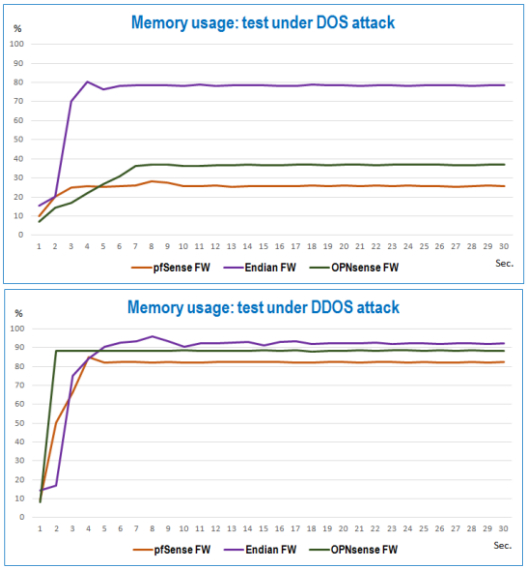
4.2 ผลการทดสอบด้าน CPU utilization



รูปที่ 7 เปรียบเทียบผลการทดลองด้าน CPU utilization

การทดสอบพบว่าไฟร์วอลล์ pfSence มีการใช้ทรัพยากรสำหรับการประมวลผลน้อยกว่าไฟร์วอลล์อีกสองแบบ ทั้งที่ทดสอบโดยการโจมตี DoS และ DDoS

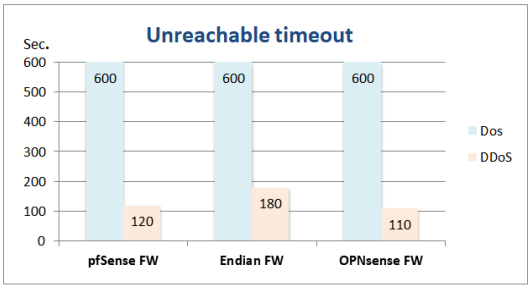
4.3 ผลการทดสอบด้าน Memory usage



รูปที่ 8 เปรียบเทียบผลการทดลองด้าน Memory usage

การทดสอบพบว่าไฟร์วอลล์ pfSence มีการใช้ประโยชน์จากหน่วยความจำน้อยกว่าไฟร์วอลล์อีกสองแบบ ทั้งทดสอบโดยการโจมตี DoS และ DDoS

4.4 ผลการทดสอบด้าน Unreachable timeout



รูปที่ 9 เปรียบเทียบผลการทดลองด้าน Unreachable timeout

การทดสอบพบว่า ไฟร์วอลล์ Endian สามารถทนต่อการโจมตีแบบ DDoS ได้เป็นเวลานานมากกว่าไฟร์วอลล์อีกสอง แบบ อย่างไรก็ตามหากทดสอบโดยใช้ DoS พบว่าไม่ส่งผลให้ไฟร์วอลล์หยุดการทำงานได้ จึงไม่สามารถนำมาเปรียบเทียบไฟร์วอลล์ทั้งสามในกรณีนี้ได้

4.5 ผลการทดสอบด้าน Action response

การทดสอบผลด้าน Action response เป็นผลต่อเนื่องจากการโจมตีจนกระทั่งระบบ (ไฟร์วอลล์) ปฏิเสธการให้บริการลง จึงวัดผลจากปฏิกิริยาที่เกิดขึ้นจากไฟร์วอลล์แต่ละตัวสรุปได้ว่า ไฟร์วอลล์ทั้งสามผลิตภัณฑ์ที่นำมาทดสอบ แสดงผลตอบรับที่เป็นไปในทิศทางเดียวกันคือ ยุติการทำงานลงและไม่สามารถส่งผ่านแพกเก็ตออกไปได้

5. สรุปผลการวิจัย

การวิเคราะห์ผลการทดสอบด้านต่างๆ พบว่า ไฟร์วอลล์ทั้ง3 มีการตอบสนองต่อผลกระทบจากการโจมตีด้วย DoS/ DDoS ที่แตกต่างกันซึ่งหากพิจารณาผลในแง่ของปริมาณ Throughput การใช้ทรัพยากร CPU และ Memory ไฟร์วอลล์ pfSense ให้ผลด้านประสิทธิภาพสูงที่สุด แต่หากพิจารณาวัดผลความทนทานต่อการโจมตี ไฟร์วอลล์ Endian สามารถทนทานได้นานที่สุด และยังพบว่า ไฟร์วอลล์ทุกตัวไม่สามารถป้องกันการโจมตีด้วย DoS/ DDoS ได้ และมีผลตอบสนองในทิศทางเดียวกันคือ หยุดทำงานจนไม่สามารถส่งผ่านแพกเก็ตออกไปได้

อย่างไรก็ตามยังมีวิธีการอีกมากมายที่สามารถขัดขวางการทำงานของระบบถึงแม้ว่าจะมีการจัดการทรัพยากรที่ดีแล้ว ซึ่งแนวทางการแก้ไขอาจใช้การจำกัด Bandwidth สำหรับแต่ละบริการ หรือใช้การจำกัดการเข้าถึงโดยระบุเป็นจำนวนผู้ใช้ที่สามารถเข้าถึงงานได้ และรวมไปถึงการพิจารณาติดตั้งระบบสำรอง เพื่อป้องกันความสูญเสียการทำงาน ให้ระบบสามารถรักษาเสถียรภาพของการให้บริการ

6. การพัฒนาในอนาคต

แนวทางเพื่อนำงานทดสอบไฟร์วอลล์มาพัฒนาต่อยอดอาจเป็นไปได้หลายแนวทาง เช่น การปรับปรุงองค์ประกอบต่างๆ ของระบบที่มีอยู่เดิมให้มีประสิทธิภาพสูงขึ้น อาทิเพิ่มความเร็วการประมวลผล หรือเพิ่มกฎการคัดกรองเป็นต้น ทั้งนี้ก็เพื่อการจำลองสถานการณ์ให้ใกล้เคียงกับการใช้งานจริงมากที่สุด หรือเพิ่มการวัดประสิทธิภาพจากตัวชี้วัดอื่นๆ เพื่อระบุลักษณะการทำงานของไฟร์วอลล์ซึ่งไม่ได้ใช้ในโครงการนี้ เช่น วัดอัตราการสูญเสียแพกเก็ต การวัดการกระจายตัวของ IP และการวัดอัตราการเชื่อมต่อสูงสุดเป็นต้น อีกแนวทางอาจยึดโครงสร้างระบบเดิมแต่ปรับเพิ่มเติมให้ระบบสามารถนำมาใช้ทดสอบไฟร์วอลล์แต่ละแบบเช่นไฟร์วอลล์แบบฮาร์ดแวร์ รวมไปถึงการปรับปรุงให้สามารถนำมาทดสอบกับไฟร์วอลล์ที่ออกแบบให้ทำงานบนแพลตฟอร์มต่างชนิดกันได้ จุดประสงค์ก็เพื่อให้เกิดความหลากหลายของแบบจำลองการทดสอบ โดยแนวทางที่กล่าวมายังคงมีรูปแบบและจุดมุ่งหมายเช่นเดิมคือ การสร้างเครื่องมือวัดประสิทธิภาพไฟร์วอลล์ที่มีความแม่นยำในการทดสอบให้มากที่สุด

เอกสารอ้างอิง

Karen M. Goertzel. **Firewalls**, IATAC: the Department of Defend. May 2011.

John Wack and Ken Cutler. **Guidelines on Firewall and policy**. National Institute of Standard and Technology. Jan 2002.

Elizabeth D. Zwicky and Simon Cooper. **Building of the Internet Firewalls**. O'Reilly Network. Jun 2001.

Gary C. Kessler. **Computer Security Handbook.** John Wiley & Sons, Inc. Wiley Online Library. Aug 2015.

Sílvia Farraposol, Laurent Gallon and Philipp Owezarski. **DDoS Servival Handbook**, 2013.

Muhammad Zeeshan Ahmad, **Comparative Analysis of Iptable and Shorewall**. Blekinge Institute of Technology, Aug 2012.

Wenhui Su and Junjie Xu, “Performance Evaluation of CISCO ASA & Lnux IPtable Firewall Solutions”, Halmstad University, May 2013.

Chirag Sheth and Rajesh Thakker, “**Performance Evaluation and Comparison of Network Firewalls under DDoS Attack**”, MECS, Oct 2013.

Thaier Hayajneh, Bassam J. Mohd, Awni D. Itradat and Ahmad Nahar. **Performance and Information Security Evaluation with Firewalls**. Hashemite University, Jan 2013.