19th International Computer Science and Engineering Conference (ICSEC)
Chiang Mai, Thailand, 23-26 November, 2015

ระบบยืนยันตัวตนแบบอัตโนมัติสำหรับควบคุมการเข้าถึงเครือข่าย
A-NAC: An Automated Authentication System for Network Access Controls

ธงชัย เจือจันทร์[1], เอกพล นันทพันธ์[1], และ พิชิต อนุฤทธิ์[1]
[1]สาขาวิทยาการคอมพิวเตอร์ ภาควิชาวิทยาศาสตร์พื้นฐาน คณะวิทยาศาสตร์วิทยาศาสตร์และเทคโนโลยี
มหาวิทยาลัยราชภัฏสุรินทร์, สุรินทร์
E-mail: {thongchai336, slarkcomsci, pichit.anurit}@gmail.com

บทคัดย่อ

ระบบควบคุมการเข้าถึงเครือข่ายถูกพัฒนาอย่างแพร่หลายเพื่อใช้เป็นเครื่องมือควบคุมใช้งานอินเทอร์เน็ต เช่น RahuNAS JumboNet SNAC pfSense และ CoovaChilli แต่ระบบเหล่านี้ยังมีปัญหาแง่การใช้งานหลายด้าน งานวิจัยนี้จึงออกแบบและพัฒนาระบบควบคุมการเข้าถึงเครือข่ายอินเทอร์เน็ตที่มีความต่อเนื่อง ถึงแม้ผู้ใช้จะเปลี่ยนสับเน็ตที่ใช้เชื่อมต่ออินเทอร์เน็ตภายในองค์กร และพัฒนาระบบต้นแบบจากการใช้ซอฟต์แวร์โอเพนซอร์สด้านการจัดการเครือข่าย การระบุตัวตน และการเก็บล็อก ร่วมกับซอฟต์แวร์ที่พัฒนาขึ้น แล้วได้ทำการทดลองบนระบบเทสเบด ผลจากการทดลองของงานวิจัยนี้แสดงถึงประสิทธิภาพและประสิทธิผล โดยมีความยืดหยุ่นสำหรับการใช้งานในเครือข่ายที่ซับซ้อนได้

คำสำคัญ: ระบบยืนยันตัวตนอัตโนมัติ, หลายสับเน็ต, ยืนยันตัวตน

Abstract

Network Access Controls (NACs) have been developed as a tool for controlling network accesses. For example, RahuNAS, JumboNet, SNAC, pfSense and CoovaChilli are potential tools. However, such tools still have some drawbacks. In this research, we have designed and developed an automated authentication system for seamlessly using internal organization networks. We have prototyped and tested on network testbed. Experimental results illustrated that our design shows an effectiveness in complex networks.

Keywords: NAC, Network Access Control, Automated Authentication

1. บทนำ

การเชื่อมต่อสู่ระบบอินเทอร์เน็ตปัจจุบัน จำเป็นต้องผ่านระบบควบคุมการเข้าถึงเครือข่าย (Network Access Control: NAC) [1] ก่อนเข้าใช้อินเทอร์เน็ต เพื่อระบุและเก็บข้อมูลทางจราจรเครือข่าย (Traffic) ของผู้เข้าใช้ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดด้านคอมพิวเตอร์ พ.ศ. 2550 [2] โดยก่อนหน้านี้อุปกรณ์เครือข่ายส่วนใหญ่ ยังไม่มีการใช้แบบเคลื่อนที่สูงมากนัก ทั้งในการเชื่อมต่อแบบแบบสาย (Wired) และไร้สาย (Wireless)

ด้วยความซับซ้อนและจำนวนของผู้ใช้อินเทอร์เน็ตที่มีมากขึ้น เช่น ผู้ใช้หนึ่งคนจะมีอุปกรณ์ที่เชื่อมต่ออินเทอร์เน็ตได้จำนวนมาก เป็นต้น และพื้นที่ความต้องการใช้อินเทอร์เน็ตเพิ่มขึ้น การจัดการให้อินเทอร์เน็ตมีพื้นที่ครอบคลุมมากขึ้นจึงเป็นสิ่งจำเป็นสำหรับองค์กรต่าง ๆ ซึ่งต้องออกแบบเครือข่ายให้เหมาะสมทั้งในแง่ของจำนวนอุปกรณ์และพื้นที่การให้บริการ โดยส่วนใหญ่จะใช้วิธีเพิ่มจำนวนสับเน็ต (Subnet) แล้วกระจายไปยังพื้นที่ต่าง ๆ การเพิ่มสับเน็ตดังกล่าวนำมาซึ่งความยุ่งยากในกระบวนการระบุตัวตนก่อนเข้าใช้อินเทอร์เน็ตจากอุปกรณ์เครือข่าย โดยเฉพาะการเปลี่ยนสับเน็ตเพื่อเข้าใช้อินเทอร์เน็ต ซึ่งจะทำให้หมายเลข Media Access Control (MAC) ถูกจับคู่กับหมายเลข IP ในสับเน็ตใหม่ ผู้ใช้จึงถูกบังคับให้ยืนยันตัวตนใหม่ภายใต้เครือข่ายในองค์กรเดียวกัน และยากต่อการคงสถานะการยืนยันตัวตนและการเก็บล็อก (Log) ตาม พ.ร.บ. ว่าด้วยการกระทำความผิดด้านคอมพิวเตอร์ได้

ถึงแม้ก่อนหน้านี้จะมีระบบควบคุมการเข้าถึงเครือข่ายถูกพัฒนาขึ้นเป็นจำนวนมาก [3]–[10] แต่ระบบเหล่านี้ไม่สามารถแก้ปัญหาที่กล่าวมาแล้วได้ โดยมีเพียง JumboNet [6] เท่านั้นที่สามารถยืนยันตัวตนเมื่อมีการย้ายสับเน็ต แต่ระบบดังกล่าวไม่ถูกเปิดเผยซอร์ซโค้ด และใช้เพียงหมายเลข MAC เป็นเครื่องมือในการระบุตัวตน จึงยากในการจัดการข้อมูลหมายเลข MAC และยากต่อองค์กรขนาดกลางและขนาดเล็กที่จะพัฒนาระบบขึ้นมาใช้ตามแนวคิดนี้ได้ งานวิจัยนี้จึงต้องการพัฒนาระบบควบคุมการเข้าถึงเครือข่ายที่ยืนยันตัวตนแบบอัตโนมัติและสามารถคงสถานะการยืนยันตัวตนหลังจากการข้ามสับเน็ตแบบโอเพนซอร์ส

การออกแบบระบบควบคุมการเข้าถึงเครือข่ายเพื่อแก้ไขปัญหาข้างต้นแบ่งระบบออกเป็น 2 ส่วน คือ การยืนยันตัวตนด้วยหมายเลข MAC และ การใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) โดย *แบบที่ (1)* จะมีการเข้าถึงข้อมูลผู้ใช้ในระดับกายภาพ (Physical Access) ก่อนที่จะนำเข้าหมายเลข MAC สู่ระบบ เมื่อผู้ใช้แบบแรกเข้ามาในระบบเครือข่ายขององค์กร ระบบ A-NAC จะยืนยันตัวตนให้กับผู้ใช้และสามารถเข้าใช้เครือข่ายอินเทอร์เน็ตได้โดยอัตโนมัติ และ *แบบที่ (2)* ผู้ใช้จะยืนยันตัวตนด้วย Username และ Password ขององค์กร ซึ่งหลังจากการยืนยันตัวตนแล้วการย้ายสับเน็ตระบบจะยืนยันตัวตนได้โดยอัตโนมัติ

การพัฒนาระบบใช้วิธีต่อยอดจากโอเพนซอร์สทางเครือข่ายและระบบการยืนยันตัวตน ซึ่งประกอบด้วย iptables, ipset,

FreeRadius, MySQL และ Apache และได้ทำการทดลองด้วยวิธี testbed เทียบกับระบบ Fortinet แล้วประเมินค่า Authentication Delay (AD), AD เมื่อมีการย้ายสับเน็ต และ Overhead ซึ่งผลการทดลองแสดงให้เห็นถึง A-NAC มีค่า AD ต่ำกว่า Fortinet และค่า AD เมื่อย้ายสับเน็ตค่าเฉลี่ยอยู่ในระดับต่ำกว่า 6 วินาที ซึ่งอยู่ในระดับที่ยอมรับได้ต่อการยืนยันตัวตนโดยปกติ ซึ่งยืดหยุ่นต่อการใช้งานของผู้ใช้ในเครือข่ายขององค์กรและเก็บข้อมูลจราจรคอมพิวเตอร์เพื่อใช้ดำเนินการทางกฎหมายได้

ส่วนถัดไปของเอกสารจะเป็นส่วนระบบและกลไกก่อนหน้า ในส่วนที่ 3 นำเสนอการออกแบบและพัฒนาระบบ ส่วนที่ 4 คือ การทดลองและประเมินผล และส่วนที่ 5 สรุปผลจากงานวิจัยนี้

2. ระบบและกลไกก่อนหน้า

มีระบบและกลไกที่ถูกพัฒนาเพื่อใช้สำหรับระบุตัวตน ก่อนเข้าถึงอินเทอร์เน็ตจำนวนมาก แต่ระบบเหล่านั้นยังมีข้อจำกัดหลายประการ ซึ่งในงานวิจัยแบ่งได้เป็น กลุ่มซอฟต์แวร์โอเพนซอร์ส กลุ่มการพัฒนาเฉพาะองค์กร และกลุ่มอุปกรณ์เชิงพาณิชย์ดังนี้

2.1 ซอฟต์แวร์โอเพนซอร์ส

NAC ในกลุ่มซอฟต์แวร์โอเพนซอร์สที่ถูกพัฒนาขึ้น มีหลายระบบด้วยกัน เช่น RahuNAS [9], SNAC [3], pfSense [8], CoovaChilli [4] และ WifiDog [10] เป็นต้น ซึ่งซอฟต์แวร์เหล่านี้ถูกนำไปใช้ในองค์กรทั้งขนาดเล็กและขนาดกลางได้อย่างมีศักยภาพ และยังมีส่วนช่วยที่สำคัญในการลดการนำเข้าอุปกรณ์จากต่างประเทศ แต่อย่างไรก็ตามซอฟต์แวร์โอเพนซอร์สเหล่านี้ ยังไม่มีกลไกที่จะช่วยให้ระบบการยืนยันตัวตนมีความยืดหยุ่นเพียงพอ สำหรับเครือข่ายในปัจจุบัน เช่น การคงสถานะการยืนยันตัวตนเมื่อผู้ใช้ย้ายสับเน็ต เป็นต้น จึงเป็นที่มาของงานวิจัยนี้ที่จะปรับปรุงวิธีการยืนยันตัวตนแบบอัตโนมัติได้

2.2 กลุ่มเฉพาะสำหรับองค์กร

JumboNet [6] เป็น NAC ที่มีความสามารถระบุตัวตนของผู้ใช้จากหมายเลข MAC เพียงอย่างเดียว เก็บ Log ได้ตาม พ.ร.บ. ว่าด้วยการกระทำความผิดด้านคอมพิวเตอร์ และสามารถระบุตัวตนได้โดยอัตโนมัติเมื่ออุปกรณ์เคลื่อนที่ข้ามสับเน็ต แต่ JumboNet ถูกพัฒนาสำหรับใช้เฉพาะภายในหน่วยงาน ซึ่ง NAC ต้นแบบจากงานวิจัยนี้ จะมีความสามารถทัดเทียมกับ JumboNet และใช้ปัจจัยการระบุตัวตนมากกว่า จึงยืดหยุ่นและเหมาะกับการนำไปใช้กับเครือข่ายที่มีหลายสับเน็ตมากกว่า

2.3 กลุ่มผลิตภัณฑ์เชิงพาณิชย์

อุปกรณ์เชิงพาณิชย์สำหรับองค์กรขนาดใหญ่ เช่น Fortinet [5] ถูกพัฒนาให้สนับสนุนการใช้งานกับองค์กรขนาดใหญ่ ซึ่งอาจต้องมีการควบคุมการเข้าถึงเครือข่ายจากหลายสับเน็ตรวมกัน และถึงแม้ Fortinet จะเป็นอุปกรณ์ที่มีราคาแพง แต่ยังไม่สามารถรองรับกับการใช้อุปกรณ์เครือข่ายที่มีการเคลื่อนที่ข้ามสับเน็ตได้ สำหรับระบบควบคุมการเข้าถึงเครือข่ายขนาดเล็ก เช่น Mikrotik [7] มีความสะดวกอย่างมากกับเครือข่ายขนาดเล็ก มีหน้าต่างการใช้งานที่สะดวก ขนาดเล็กกะทัดรัด และง่ายต่อการจัดการ ถึงแม้ Mikrotik จะเป็นอุปกรณ์ที่สะดวกและใช้งานง่าย แต่ไม่สนับสนุนการขยายตัวของเครือข่ายสำหรับองค์กรได้ ซึ่งต้นแบบจากงานวิจัยสามารถยืดหยุ่นรองรับทั้งองค์กรขนาดใหญ่และขนาดเล็กได้

2.4 งานวิจัยก่อนหน้า

งานวิจัยก่อนหน้า [3], [11], [12] มุ่งพัฒนาแก้ไขปัญหาด้านความมั่นคง ซึ่งเป็นแนวทางพัฒนาระบบ NAC ที่ช่วยให้ผู้ใช้มีความปลอดภัย เช่น การพัฒนา Agent เพื่อป้องกันการปลอมแปลงหมายเลข MAC แต่ระบบดังกล่าวยังไม่มีการคำนึงถึงความสะดวกของผู้ใช้งาน และความพร้อมของอุปกรณ์ของผู้ใช้ที่มีความหลากหลาย และมีความซับซ้อนมากขึ้น งานวิจัยนี้จึงคำนึงถึงความหลากหลายของอุปกรณ์เครือข่ายที่เพิ่มสูงขึ้น และช่วยให้ระบบ NAC มีความยืดหยุ่น ใช้งานได้ต่อเนื่อง เหมาะสมกับรูปแบบการเชื่อมต่อเครือข่ายในปัจจุบัน

3. การออกแบบและพัฒนาระบบ

ในส่วนนี้จะกล่าวถึงการออกแบบระบบจากแนวคิดของงานวิจัยนี้

3.1 การออกแบบระบบ

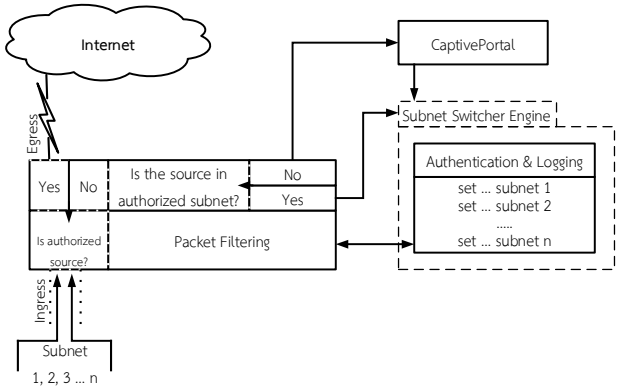
ระบบ A-NAC ถูกออกแบบเพื่อมุ่งเน้นให้ระบบสามารถยังคงสถานะการยืนยันตัวตนให้ผู้ใช้ได้ ถึงแม้ผู้ใช้จะเคลื่อนที่และมีการเข้าใช้อินเทอร์เน็ตจากสับเน็ตใด ๆ ในเครือข่ายขององค์กรเดียวกัน จากรูปที่ 1 เป็นโครงสร้างทั้งหมดของระบบ A-NAC โดยผู้ดูแลระบบจะต้องกำหนดและแบ่ง IP ให้กับสับเน็ตที่ 1 ถึง n และหมายเลข MAC ที่เชื่อถือได้จะถูกนำไปเก็บไว้ที่รายการ *<trusted_mac>* และเข้าสู่ขั้นตอนต่อไปนี้

(1) Subnet Switcher Engine (SSE) เป็นหน่วยที่ใช้สำหรับการระบุตัวตน และเก็บ Log ทั้ง n สับเน็ต โดยแบ่งออกเป็นกลุ่ม ซึ่งในงานวิจัยนี้เรียกว่า set แต่ละ set จะมี 2 คอลัมน์ *<name>* และ *<subnet_id>* สำหรับแยกแต่ละสับเน็ตออกจากกัน ในแต่ละ *<subnet_id>* จะประกอบด้วย *<ip_address>* และ *<mac_address>* เพื่อเก็บหมายเลข IP และ MAC ตามลำดับ สำหรับผู้ใช้ที่ทำการล็อกอินเข้าสู่ระบบใหม่ SSE จะใช้หมายเลข MAC ตรวจสอบสับเน็ตที่ 1 ถึง n หากยังไม่พบจะเก็บหมายเลข IP และ MAC เข้าไปยังกลุ่ม set ที่ผู้ใช้กำลังใช้งานอยู่ (Reside) แต่ถ้าหาก MAC ของผู้ใช้เคยอยู่ใน set อื่นแล้ว (ผู้ใช้เคยผ่านการระบุตัวตนในสับเน็ตอื่นแล้ว) ระบบจะลบหมายเลข IP และ MAC จากสับเน็ตเดิม แล้วทำการยืนยันตัวตนใหม่และเพิ่มหมายเลข IP และ MAC เข้าสู่สับเน็ตใหม่

(2) Captive Portal (CP) เป็นหน้าต่างสำหรับการล็อกอินเข้าสู่ระบบ ซึ่งหน้าต่าง CP จะปรากฏให้ผู้ใช้ล็อกอินจาก 2 กรณีคือ (1) หมายเลข MAC ไม่อยู่ในรายการ *<trusted_mac>* และ

(2) หมายเลข IP และ MAC ยังไม่เคยมีการล็อกอินจากสับเน็ตใดสับเน็ตหนึ่งมาก่อน

(3) Packet Filtering (PF) เป็นขั้นตอนการตรวจสอบแพ็กเก็ตที่มาจากสับเน็ตต่าง ๆ ภายใน (Ingress) และมีปลายทางไปยังเครือข่ายภายนอก (Egress) โดย PF จะดึงข้อมูลทั้ง n set และ รายการ *<trusted_mac>* มาตรวจสอบ โดยใช้หมายเลข IP และ MAC ต้นทาง (Is authorized source? ในรูปที่ 1) ถ้าหากมีอยู่แล้ว A-NAC จะส่งต่อ (Forward) แพ็กเก็ตดังกล่าวเข้าสู่ Egress หากไม่พบใน set ระบบจะตรวจสอบว่าต้นทางที่ได้รับเคยถูกยืนยันตัวตนในสับเน็ตอื่นหรือไม่ (Is source is in authorized subnet? ใน รูปที่ 1) หากไม่พบแพ็กเก็ตจะถูกส่งไปยังส่วนของ CP แต่หากมีอยู่ใน set ระบบจะส่งต่อแพ็กเก็ตไปในยัง SSE เพื่อระบุตัวตนแบบอัตโนมัติและปรับปรุง (update) ต้นทางให้อยู่ใน set ของสับเน็ตใหม่ของผู้ใช้



รูปที่ 1 โครงสร้างของระบบ A-NAC

3.1 การพัฒนาระบบ

A-NAC ถูกพัฒนาโดยนำซอฟต์แวร์โอเพนซอร์สหลายส่วนมาประกอบกัน และเพิ่มกลไก SSE CP และ PF เพื่อให้เชื่อมโยงกันอย่างเป็นระบบ โดย SSE จะใช้ ipset ทำงานร่วมกับ FreeRadius จัดเก็บข้อมูลด้วย MySQL และใช้ Engine ที่พัฒนาขึ้นมาเพิ่มเติม สำหรับจัดการเมื่อผู้ใช้เปลี่ยนสับเน็ตเพื่อใช้อินเทอร์เน็ต ส่วนระบบ CP เป็นหน้าต่างเว็บอย่างง่าย ให้บริการโดย Apache เพื่อรอรับการป้อน Username และ Password จากผู้ใช้ แล้วเชื่อมโยงเข้าสู่ SSE ต่อไป สำหรับ PF จะใช้ iptables ทำงานร่วมกับ ipset

4. การทดลองและประเมินผล

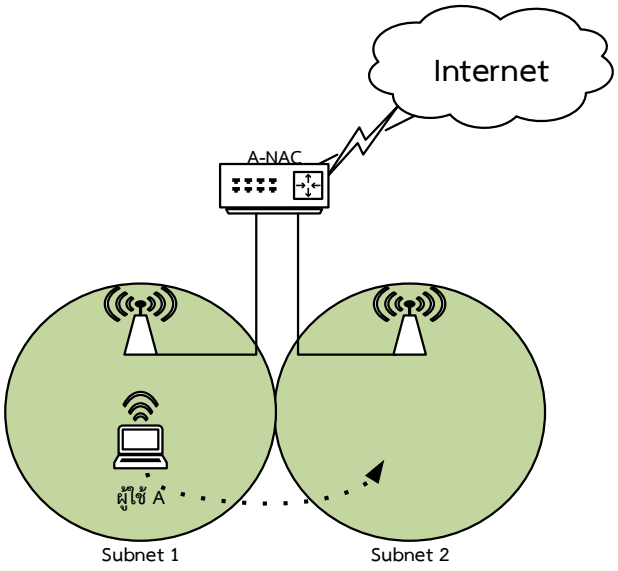
4.1 การออกแบบการทดลอง

การทดลองเพื่อประเมินต้นแบบจากงานวิจัยนี้ ได้ประเมินโดยใช้ระบบ testbed และทำการทดลองซ้ำจำนวน 30 ครั้ง ดังแสดงในรูปที่ 2 A-NAC ทำหน้าที่ควบคุมการเข้าถึงอินเทอร์เน็ตจากสับเน็ตภายในจำนวน 2 สับเน็ต คือ Subnet 1 และ Subnet 2 เมื่อเริ่มการทดลองผู้ใช้จะเริ่มยืนยันตัวตนจาก Subnet 1 แล้วย้ายเข้าสู่ Subnet 2 ตามลำดับ ในการทดลองแต่ละครั้งได้ควบคุม DHCP และ DNS ให้ถูกใช้จากแหล่งเดียวกันเพื่อป้องกัน Delay จากปัจจัยการกำหนดไอพีให้ end-user โดยระหว่างการทดลองจะมีการเก็บผลตามเมตริกต่อไปนี้

(1) ค่า Authentication Delay (AD) เทียบกับอุปกรณ์เชิงพาณิชย์ Fortinet เพราะ Fortinet เป็นอุปกรณ์ที่ต้องนำเข้าจากต่างประเทศและมีราคาสูง ซึ่งถูกใช้จริงในหลายหน่วยงาน การนำ มาเทียบเคียงกับ Fortinet จะช่วยแสดงให้เห็นถึงประเด็นด้านประสิทธิภาพของ A-NAC ได้ดีกว่าการเทียบเคียงกับซอฟต์แวร์โอเพนซอร์สอื่น ๆ

(2) ค่า AD ที่เกิดจากการระบุตัวตนโดยอัตโนมัติหลังจากผู้ใช้ย้ายสับเน็ต เนื่องจากคุณสมบัติ (Feature) การระบุตัวตนโดยอัตโนมัตินี้ มีอยู่เพียงในระบบนี้และ JumboNet จึงไม่สามารถเปรียบเทียบค่า Delay ได้จากปัญหาที่กล่าวไปแล้วข้างต้น จึงได้ทดสอบด้วยการตรวจสอบค่า ค่า Delay ที่เกิดขึ้นจากการเข้าถึงเว็บไซต์ปลายทาง (Target Site) เทียบกับขั้นตอนระบุตัวตนอัตโนมัติของ A-NAC รวมกับการเข้าเว็บไซต์ปลายทางโดย Target Site จากงานวิจัยนี้อยู่ห่างจากผู้ใช้จำนวน 4 hop

(3) Overhead ใช้วิธีเก็บค่าสะสมการประมวลผล (Cumulative CPU) ซึ่งได้เปรียบเทียบระหว่างสถานการณ์ปกติของเครื่องทดลองกับ Overhead ที่เกิดขึ้นหลังจาก A-NAC เริ่มทำงาน



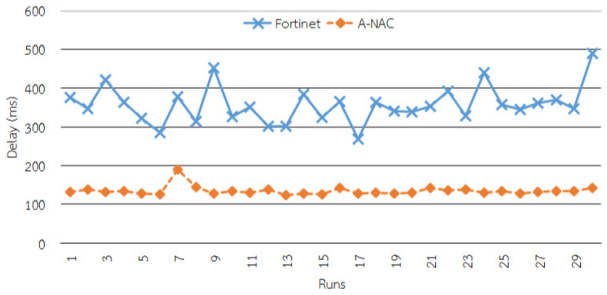
รูปที่ 2 แผนผังการทดลอง

4.2 ผลการทดลอง

4.2.1 ผลการวัด Authentication Delay

รูปที่ 3 เป็นผลจากการทดลองเปรียบเทียบ AD ระหว่าง Fortinet กับ A-NAC โดยแกน x คือการทดลองแต่ละครั้งและแกน y คือ Delay ที่เกิดขึ้น จากกราฟ Fortinet จะมี Delay อยู่ระหว่าง 356.7±48.3 ms ส่วน A-NAC จะมี Delay อยู่ระหว่าง 134.2±11.7 ดังนั้น A-NAC มี Delay ต่ำกว่า Fortinet ในแง่ของ Payload ที่ใช้

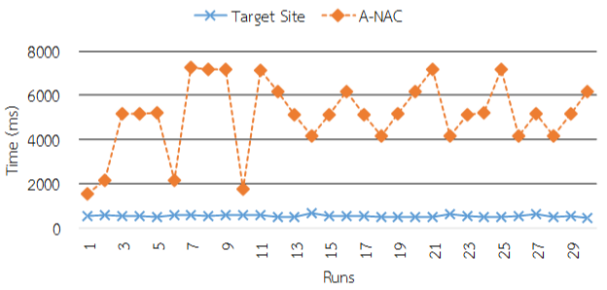
หลังจากยืนยันตัวตนแล้ว A-NAC มีขนาด 3676 ไบต์ ส่วน Fortinet มีขนาด 5751 ไบต์ ซึ่งอาจมีผลต่อ Delay ที่เกิดขึ้นได้ แต่อยู่ในสัดส่วนต่ำและไม่ส่งผลให้ผลการทดลองนี้มีผลเปลี่ยนแปลงแต่อย่างใด



รูปที่ 3 Authentication Delay

4.2.2 ผลการวัด AD ที่เกิดจากการระบุตัวตนโดยอัตโนมัติหลังจากผู้ใช้ย้ายสับเน็ต

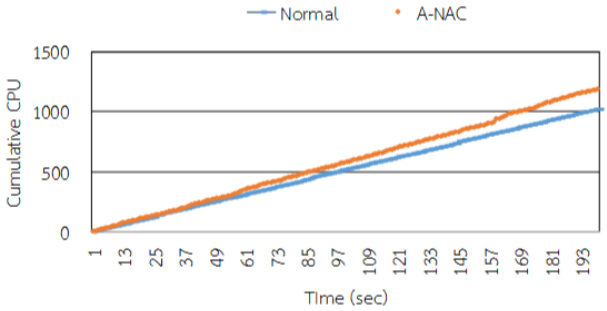
การประเมิน Delay ที่เกิดขึ้นเมื่อผู้ใช้ย้ายสับเน็ตแสดงในรูปที่ 4 โดยแกน x คือ ครั้งที่ทดสอบ และแกน y คือ Delay ที่เกิดขึ้นในหน่วยมิลลิวินาที (millisecond) จากผลการทดลองโดยเฉลี่ยการเข้าเว็บไซต์ปลายทาง (Target Site) ในสถานการณ์ปกติจะมี Delay อยู่ระหว่าง 540.4±43.5 ms ส่วน A-NAC จะมี Delay อยู่ระหว่าง 5089.2±1616.7 ms หรือประมาณ 5 วินาที ซึ่ง Delay ที่เกิดขึ้นของ ของ A-NAC เกิดจากกลไกภายในจึงต้องตรวจสอบถึง 3 ขั้นตอนโดยใช้ iptables ipset FreeRadius และการพัฒนาซอฟต์แวร์เพิ่มเติมจากงานวิจัยนี้



รูปที่ 4 Authentication Delay จากการระบุตัวตนเมื่อผู้ใช้ย้ายสับเน็ต

4.2.3 ผลการตรวจสอบ Overhead

การประเมินด้านประสิทธิภาพของระบบดังรูปที่ 4 โดยแกน x คือ เวลาที่เก็บข้อมูล และแกน y คือ อัตราการใช้ CPU สะสม จะเห็นว่า A-NAC มีสัดส่วนการใช้ทรัพยากรณ์เครื่องสูงกว่าเครื่องทดลอง ตอนที่อยู่ในสภาวะปกติ แต่อยู่ในระดับที่ใกล้เคียงกับเครื่องทดลอง



รูปที่ 5 Overhead ของ A-NAC กับสภาวะปกติของเครื่องทดลอง

5. สรุป

ระบบควบคุมการเข้าถึงเครือข่าย เป็นเครื่องมือที่สำคัญสำหรับการยืนยันตัวตนผู้เข้าใช้อินเทอร์เน็ตสำหรับองค์กร โดยจำนวนของผู้ใช้ จำนวนอุปกรณ์เครือข่าย และรูปแบบการใช้เครือข่ายแบบเคลื่อนที่ในปัจจุบันมีสูงขึ้น แต่การออกแบบและพัฒนาระบบควบคุมการเข้าถึงเครือข่ายยังใช้การระบุตัวตนแยกตามสับเน็ต ทำให้ยุ่งยากต่อการใช้งานสำหรับอุปกรณ์เครือข่ายเคลื่อนที่ต่าง ๆ งานวิจัยนี้จึงออกแบบและพัฒนาระบบต้นแบบสำหรับควบคุมการเข้าถึงเครือข่ายแบบอัตโนมัติ เมื่อผู้ใช้ที่มีการย้ายสับเน็ตในเครือข่ายเดียวกัน จากการออกแบบและพัฒนาต้นแบบตามแนวคิดของงานวิจัยนี้ ได้ทำการทดลองบนระบบ testbed ผลการทดลองแสดงให้เห็นถึงความสามารถในการยืนยันตัวตนของผู้ใช้ได้ ถึงแม้ผู้ใช้จะใช้อุปกรณ์เครือข่ายและเคลื่อนย้ายการใช้อินเทอร์เน็ตระหว่างสับเน็ต ผู้ใช้ยังคงได้รับการเชื่อมต่ออินเทอร์เน็ตอย่างปกติ ในขณะที่ระบบสามารถยืนยันตัวตนให้ได้โดยอัตโนมัติ และสามารถเก็บ Log ได้ถูกต้องตามรูปแบบที่กำหนดได้

เอกสารอ้างอิง

[1] J. Kelley, R. Campagna, and D. Wessels, *Network Access Control For Dummies*. 2009.

[2] กระทรวงมหาดไทย, “พ.ร.บ. ว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550,” สำนักงานปลัดกระทรวงมหาดไทย, ถนนอัษฎางค์ เขตพระนคร กรุงเทพฯ 10200, พระราชบัญญัติ, 2550.

[3] S. Puangpronpitag and A. Suwannasa, “A Lightweight Agent-based Egress NAC on Wireless LAN,” in Proceedings of International Conference on Computer & Information Science, Kuala Lumpur, Malaysia, 12 June 2012.

[4] Coova Team, “CoovaChilli,” 2015. [Online]. Available: http://coova.org/CoovaChilli. Last Accessed: 01 Jun 2015.

[5] K. Xie and M. Xie, “Fortinet,” *Network security company*, 2015. [Online]. Available: www.fortinet.com. Last Accessed: 01 Jun 2015.

[6] สำนักบริการเทคโนโลยีสารสนเทศมหาวิทยาลัยเชียงใหม่ , “JumboNet,” *เครือข่ายไร้สายมหาวิทยาลัยเชียงใหม่ Jumbo Net*. [Online]. Available: https://jumbo.cmu.ac.th/. Last Accessed: 29 Jul 2015.

[7] MikroTik Company, “MikroTik,” *Network security company*, 2015. [Online]. Available: http://www.mikrotik.com/. Last Accessed: 05 Jun 2015.

[8] Electric Sheep Fencing, “pfSense,” *Open Source Security*, 2015. [Online]. Available: https://www.pfsense.org/. Last Accessed: 12 May 2015.

[9] N. Soutmun, “RahuNAS - Rahu Network Access Server,” 2011. [Online]. Available: https://github.com/neutronth/rahunas. Last Accessed: 12 May 2015.

[10] F. Prouls, “Wifidog,” 2015. [Online]. Available: http://dev.wifidog.org/. Last Accessed: 01 Jun 2015.

[11] A.-S. Ehab, “Automated management of network access control from design to enforcement,” in Proceedings of 15th ACM symposium on Access control models and technologies, Pittsburgh, Pennsylvania, USA, 2010.

[12] A. Nayak, A. Reimers, N. Feamster, and R. Clark, “Resonance: dynamic access control for enterprise networks,” in Proceedings of ACM workshop on Research on enterprise networking, NY, USA, 2009, pp. 11–18.