© ECTI-CARD 2009, May'09, Bangkok, Thailand. ISBN: 978-974-8285-62-7

NtopViewer ซอฟต์แวร์ตรวจสอบการใช้งานอินเทอร์เน็ตในโรงเรียน

พนิตา พงษ์ไพบูลย์
ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
panita@nectec.or.th

โสภณ มงคลลักษมี
ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
theohncom@gmail.com

สิริกานต์ พุกกะวรรณะ
ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
sirikarn.pukkawanna@nectec.or.th

บทคัดย่อ

บทความนี้นำเสนอซอฟต์แวร์ตรวจวัดและวิเคราะห์การใช้งานอินเทอร์เน็ตในโรงเรียน (NtopViewer) เพื่อช่วยในการวางแผน วิเคราะห์ความผิดปกติและบริหารจัดการทรัพยากรในเครือข่าย โดยเป้าหมายกลุ่มผู้ใช้หลักคือบุคคลากรในสถานศึกษา ที่ขาดความเชี่ยวชาญด้านเครือข่าย ซอฟต์แวร์ที่พัฒนาขึ้นจึงจำเป็นต้องใช้งานง่าย และสื่อข้อมูลที่สำคัญได้ชัดเจน

Abstract

This article presents NtopViewer, software for monitoring Internet usage in schools. Target users for NtopViewer are teachers or IT administrators in schools who may not have expertise in network management. The resulting software has user-friendly GUI and presents data in angles most suitable to teachers' needs.

คำสำคัญ

Network management, traffic classification, DoS attack

1. บทนำ ที่มา และแรงจูงใจของปัญหา

ในปัจจุบันเครือข่ายอินเทอร์เน็ตเข้ามามีบทบาทในชีวิตประจำวันมากขึ้น หน่วยงานต่างๆ ต่างมีเครือข่ายคอมพิวเตอร์เป็นของตนเองและเชื่อมโยงเข้าสู่อินเทอร์เน็ต ความท้าทายที่ตามมาจากการจัดตั้งเครือข่ายคอมพิวเตอร์ของหน่วยงาน ได้แก่ การบริหารจัดการเครือข่ายและการใช้ทรัพยากรที่มีในเครือข่ายอย่างมีประสิทธิภาพ ซึ่งเป็นปัญหาที่พบบ่อยในหน่วยงานขนาดกลางและขนาดเล็ก เช่น โรงเรียน สถาบันการศึกษา และหน่วยงานราชการ ส่วนใหญ่จะขาดบุคลากรที่มีความรู้ความสามารถในการดูแลจัดการเครือข่าย หนึ่งในองค์ประกอบสำคัญที่จะช่วยให้ผู้ดูแลเครือข่ายจัดการทรัพยากรเครือข่ายได้อย่างเต็มประสิทธิภาพ คือระบบที่ช่วยตรวจสอบปริมาณการใช้งานแบนด์วิดท์และตรวจสอบปริมาณการไหลเวียนของข้อมูลในเครือข่าย (Traffic monitoring system) ผู้ดูแลระบบจำเป็นต้องทราบว่าผู้ใช้ ใช้เครือข่ายอินเทอร์เน็ตมากน้อยแค่ไหน ปริมาณช่องสัญญาณที่เชื่อมต่ออยู่เพียงพอต่อการใช้งานหรือไม่ หากไม่เพียงพอเป็นเพราะสาเหตุอะไร เป็นเพราะมีผู้ใช้งานจำนวนมาก หรือเป็นเพราะมีผู้ใช้งานบางกลุ่มใช้แอปพลิเคชั่นที่ต้องการแบนด์วิดท์สูง หรือเป็นเพราะมีการแพร่กระจายของไวรัสคอมพิวเตอร์ภายในเครือข่าย ข้อมูลเหล่านี้จำเป็นต่อการบริหารจัดการทรัพยากรเครือข่ายให้มีประสิทธิภาพ

บทความนี้นำเสนอซอฟต์แวร์ตรวจวัดและวิเคราะห์การใช้งานอินเทอร์เน็ตในโรงเรียน (NtopViewer) ที่สามารถตอบคำถามทั้งหมดข้างต้น เพื่อช่วยในการวางแผนและบริหารจัดการทรัพยากรในเครือข่าย โดยเป้าหมายกลุ่มผู้ใช้หลักคือบุคคลากรในสถานศึกษา ที่ขาดความเชี่ยวชาญด้านเครือข่าย ซอฟต์แวร์ที่พัฒนาขึ้นจึงจำเป็นต้องใช้งานง่าย และสื่อข้อมูลที่สำคัญได้ชัดเจน

ซอฟต์แวร์ NtopViewer นี้พัฒนาต่อยอดจาก ntop [1] ซึ่งเป็นซอฟต์แวร์สนับสนุนการบริหารจัดการเครือข่ายแบบโอเพ่นซอร์ส ที่ได้รับความนิยมเป็นอย่างสูง ข้อดีของการใช้ ntop เป็นฐานในการพัฒนาคือ ntop มีความสามารถในการดักจับแพ็กเก็ต (Packet Sniffing) ที่มีจำนวนมากและความเร็วสูงอย่างมีประสิทธิภาพ และสามารถวิเคราะห์ปริมาณการใช้งานในเครือข่ายแยกตามผู้ใช้และแยกตามแอปพลิเคชั่นได้อย่างละเอียด นอกจากนี้เนื่องจากเป็นโอเพ่นซอร์ส ntop ได้ออกแบบโครงสร้างรองรับการพัฒนาเพิ่มเติมความสามารถใหม่ๆ ผ่านช่องทางที่เรียกว่า plugin ดังนั้นผู้ที่ต้องการพัฒนาปรับปรุง ntop สามารถเขียนโปรแกรมเข้าไปสวมกับ ntop ผ่านโครงสร้างของ plugin

อย่างไรก็ตามข้อจำกัดของ ntop มีหลายประเด็น เช่นไม่มีการเก็บข้อมูลลงฐานข้อมูลถาวร ทำให้การค้นคืนข้อมูลย้อนหลังลำบาก ความไม่ยืดหยุ่นของส่วนประสานต่อกราฟิกกับผู้ใช้ (GUI) เนื่องจากพัฒนาด้วยภาษาซี การเปลี่ยนแปลงแก้ไข GUI ทำได้ยาก จากการสำรวจความคิดเห็นของผู้ใช้งาน ntop ในสถานศึกษา พบว่า GUI เดิมของ ntop นั้นมีความซับซ้อนยากต่อการใช้งาน เนื่องจากเป็นภาษาอังกฤษ มีศัพท์เทคนิคมาก และมีข้อมูลการใช้เครือข่ายในเชิงลึกมากผู้ใช้ไม่เข้าใจรายละเอียดของข้อมูลที่โปรแกรมนำเสนอ

ทีมวิจัยได้พัฒนาซอฟต์แวร์ NtopViewer เพื่อลดข้อจำกัดข้างต้นของ ntop กล่าวคือ เพิ่มเติม plugin สำหรับเก็บข้อมูลลงฐานข้อมูล MySQL เพื่อการค้นคืนข้อมูลย้อนหลัง เพิ่ม plugin สำหรับตรวจจับการจู่โจมในเครือข่าย ซึ่งเทคนิคการวิเคราะห์หาการจู่โจมในเครือข่ายนี้เป็นเทคนิคที่ทางทีมวิจัยคิดค้นขึ้นมาใหม่ และมีผลการทดลองยืนยันความถูกต้องของเทคนิคนี้ดังแสดงใน [2-3] เพิ่มความสามารถในการค้นคืนข้อมูลย้อนหลัง และวิเคราะห์ข้อมูลย้อนหลังในแง่มุมที่ตรงความต้องการของผู้ใช้มากขึ้น และพัฒนา GUI ขึ้นใหม่ที่มีความยืดหยุ่น ง่ายต่อการเรียนรู้และใช้งาน โดย GUI ใหม่นี้จะติดต่อกับฐานข้อมูลโดยตรง โดยไม่ต้องแก้ไขการแสดงผลเดิมของ ntop

2. งานและทฤษฎีที่เกี่ยวข้อง

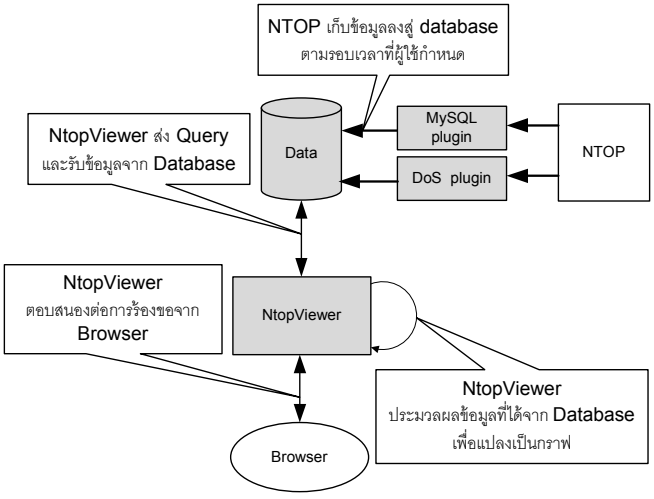
การตรวจวัดและวิเคราะห์ข้อมูลภายในเครือข่าย คือ กระบวนการดักจับการสัญจรไปมาของข้อมูลบนเครือข่าย หรือ Network traffic จากนั้นก็จะนำข้อมูลที่ได้มาวิเคราะห์ เพื่อดูว่าเกิดอะไรขึ้นบนเครือข่าย การตรวจวัดและวิเคราะห์ข้อมูลภายในเครือข่าย ทำให้เข้าใจพฤติกรรม และปริมาณการไหลเวียนของข้อมูลภายในเครือข่ายจริง ช่วยวิเคราะห์สาเหตุที่เครือข่ายช้าหรือไม่เสถียร เช่นตรวจสอบต้นตอของการโจมตี ผู้บุกรุก หรือสามารถตรวจสอบเครื่องคอมพิวเตอร์ที่น่าสงสัยบนเครือข่ายได้ รวมถึงช่วยวางแผนทรัพยากรทางด้านเครือข่าย

ระบบตรวจวัดและวิเคราะห์ข้อมูลในเครือข่ายมีทั้งระบบที่เป็นฮาร์ดแวร์และซอฟต์แวร์ ในเครือข่ายความเร็วสูงขนาดใหญ่จำเป็นต้องใช้ฮาร์ดแวร์เพื่อดักจับและวิเคราะห์แพ็กเก็ต แต่ในเครือข่ายขนาดกลางและเล็ก เช่นเครือข่ายภายในโรงเรียน ระบบที่เป็นซอฟท์แวร์นั้นเพียงพอ ซอฟท์แวร์โอเพ่นซอร์สที่น่าสนใจได้แก่ ntop, tcpdump, wireshark, MRTG [1,4-6] นอกจากนี้ยังมีซอฟท์แวร์เชิงพาณิชย์อีกหลายตัว ได้แก่ Colasoft Capsa, Network Probe, Netflow Analyzer, IP Traffic Monitor, PRTG, SoftPerfect Traffic Meter, และ Ultra Network Analyzer [7-14] ผลการสำรวจพบว่าซอฟต์แวร์ NtopViewer มีคุณสมบัติที่เทียบได้ซอฟท์แวร์เชิงพาณิชย์ และเด่นกว่าในด้านของการรายงานข้อผิดพลาดและความเสี่ยงจากการถูกจู่โจมในเครือข่าย และการบันทึกข้อมูลลงฐานข้อมูลเพื่อความสะดวกในการค้นคืนข้อมูลย้อนหลังในมิติต่างๆ นอกจากนี้ พบว่าซอฟท์แวร์เชิงพาณิชย์สำหรับตรวจวัดและวิเคราะห์ข้อมูลในเครือข่ายนั้นมีค่าลิขสิทธิ์ที่แพงมาก หากนำมาใช้งานในระดับหน่วยงานที่มีคอมพิวเตอร์ในเครือข่ายมากกว่า 10 ชุดขึ้นไป จะมีค่าลิขสิทธิ์แบบ site license ขั้นต่ำ US$300 หรือมากกว่า 10,000 บาท

3. รายละเอียดการพัฒนา

3.1 ภาพรวมของระบบ

NtopViewer เป็น web application ที่ทำหน้าที่วิเคราะห์และประมวลผลการใช้งานเครือข่ายจากฐานข้อมูล และจัดแสดงผลข้อมูลในรูปแบบที่เข้าใจง่าย ข้อมูลที่นำเสนอผ่านการวิเคราะห์และสังเคราะห์ในมิติที่แตกต่างจาก ntop รวมทั้งผนวกเทคนิคการตรวจจับการจู่โจมบนเครือข่ายแบบใหม่ ช่วยให้ผู้ใช้ทราบถึงสาเหตุความผิดปกติบนเครือข่าย กระบวนการทำงานของ NtopViewer แสดงดังรูปที่ 1

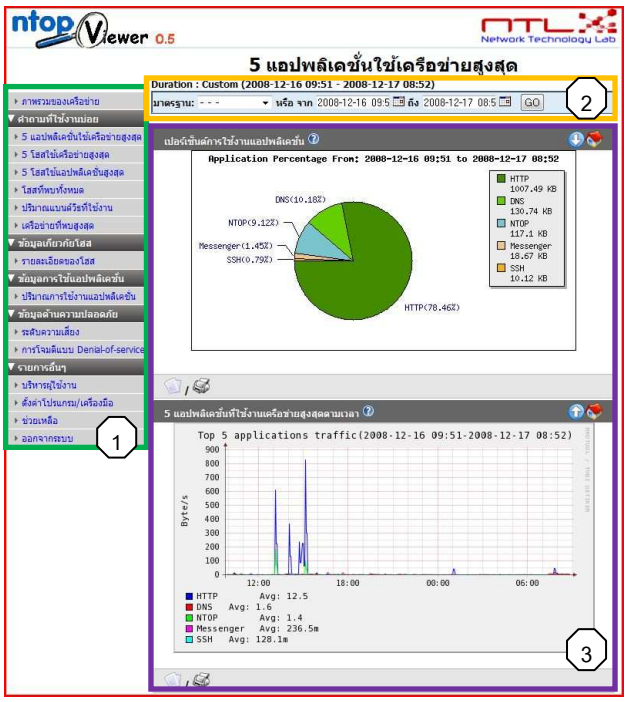


รูปที่ 1 ภาพรวมการทำงานของ NtopViewer

เมื่อเริ่มใช้งานผู้ใช้งานจะพบกับหน้าจอ login เมื่อทำการ login ผ่านแล้วจึงจะสามารถเข้าใช้งานได้ ส่วนรายการเมนูหลักประกอบด้วย 5 เมนู คือ

1) คำถามที่ใช้งานบ่อย แสดงข้อมูล 5 อันดับแรกของโฮสต์ แอปพลิเคชั่น หรือเครือข่ายที่ใช้งานสูงสุด
2) ข้อมูลเกี่ยวกับโฮสต์แสดงข้อมูลเจาะลึกรายละเอียดของแต่ละโฮสต์ที่สนใจ
3) ข้อมูลการใช้แอปพลิเคชั่น แสดงข้อมูลโฮสต์ที่ใช้แอปพลิเคชั่นที่สนใจ
4) ข้อมูลด้านความปลอดภัย แสดงข้อมูลความเสี่ยงต่างๆ และการโจมตีแบบ Denial of service ที่เกิดกับเครือข่าย
5) รายการอื่นๆ ใช้ตั้งค่าของโปรแกรมและบริหารบัญชีผู้ใช้งาน

หน้าจอแสดงผลถูกแบ่งออกเป็นสามส่วนหลัก ประกอบด้วย 1) ส่วนของเมนูหลักอยู่ทางด้านซ้ายของหน้า 2) ส่วนของเมนูในการเลือกช่วงเวลาเรียกดูข้อมูล 3) ส่วนของการแสดงผล ตามรูปที่ 2 โดยผู้ใช้สามารถเลือกการแสดงผลเป็นภาษาไทยหรือภาษาอังกฤษตามต้องการ



รูปที่ 2 หน้าจอแสดงผล

ในการควบคุมการแสดงผล ผู้ใช้สามารถเลือกช่วงเวลาของข้อมูลที่ต้องการเรียกดูได้สองแบบ แบบแรกเลือกจากช่วงเวลามาตรฐานที่ระบบจัดเตรียมไว้ให้ ประกอบด้วยช่วงเวลาย้อนหลังไป 1 ชั่วโมง 24 ชั่วโมง 7 วัน และ 30 วันนับจากปัจจุบัน แบบที่สอง กำหนดช่วงเวลาตามความต้องการของผู้ใช้เอง โดยกำหนดวันเวลาเริ่มต้นสิ้นสุดจากปฏิทิน

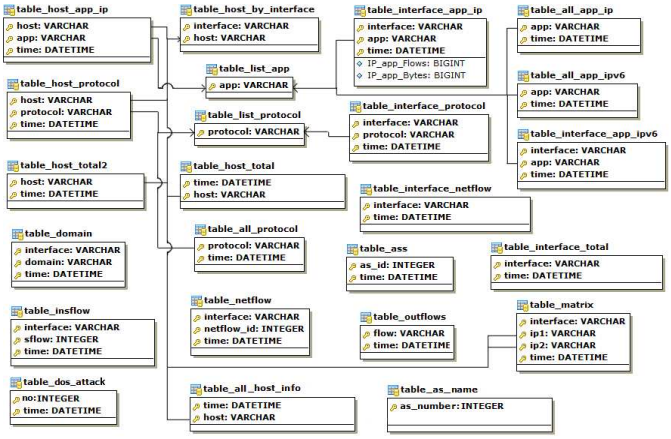
ในส่วนการแสดงผลจะวิเคราะห์ข้อมูลในมิติต่างๆ เช่น โฮสต์ที่ใช้งานเครือข่ายสูงสุดโดยรวม แยกตามทิศทางการรับส่งข้อมูล แยกตามโฮสต์ภายในภายนอก หรือแยกตามชนิดของแอปพลิเคชั่น เป็นต้น ผลลัพธ์ถูกแสดงในรูปแบบกราฟวงกลม กราฟแท่ง กราฟเส้น และตารางขึ้นอยู่กับลักษณะข้อมูล แต่ละกราฟหรือแต่ละตารางจะถูกจัดแสดงอยู่ในกรอบของตัวเองอย่างเป็นสัดส่วน ซึ่งแต่ละกรอบข้อมูลจะมีคำอธิบายความหมายของกราฟโดยละเอียด เหมาะสำหรับผู้ใช้ทั่วไปซึ่งไม่เชี่ยวชาญศัพท์เทคนิคทางเครือข่าย นอกจากนี้ผู้ใช้สามารถที่จะส่งข้อมูลของกราฟหรือตารางสู่เครื่องพิมพ์หรือออกมาเป็นไฟล์ข้อมูล

3.2 การออกแบบและพัฒนาระบบ

ส่วนประกอบหลักของการพัฒนา NtopViewer ประกอบด้วยการพัฒนา MySQL plugin ส่วนขยายเพื่อเก็บข้อมูลลงฐานข้อมูล DoS plugin ส่วนขยายเพื่อวิเคราะห์การจู่โจมบนเครือข่าย และ NtopViewer เวบอินเทอร์เฟสที่วิเคราะห์และแสดงผลข้อมูลผ่านเวบ (ส่วนประกอบสีเทาตามรูปที่ 1)

3.2.1 MySQL plugin

หนึ่งในข้อจำกัดของ ntop คือไม่มีการเก็บข้อมูลลงฐานข้อมูลถาวร ทำให้การค้นคืนข้อมูลย้อนหลังทำไม่ได้ แม้ว่า ntop มี RRD plugin สำหรับเก็บข้อมูลลง round-robin database (RRD) [15] ซึ่งเป็นฐานข้อมูลลักษณะ time series แต่ว่า RRD ไม่เป็นที่รู้จักกันอย่างแพร่หลาย การสืบค้นข้อมูลทำได้ยาก ข้อมูลมีการอ้างอิงตามเวลาอย่างเดียว ไม่สามารถเลือกดูข้อมูลมิติอื่น อีกทั้งข้อมูลจะเก็บทับซ้ำข้อมูลเดิม จึงทำให้ยากต่อการนำข้อมูลมาประยุกต์ใช้งาน ทีมวิจัยจึงได้พัฒนาวิธีเก็บข้อมูล ลงฐานข้อมูล MySQL ในรูปแบบของ plugin ขึ้นเพื่อตอบสนองความต้องการค้นคืนและวิเคราะห์ข้อมูลสำหรับผู้ใช้



รูปที่ 3 ตารางทั้งหมดในฐานข้อมูลและความสัมพันธ์

ฐานข้อมูล MySQL สำหรับเก็บข้อมูลจาก ntop มีทั้งหมด 24 ตาราง ดังรูปที่ 3 ตัวอย่างเช่น ตาราง Table_host_app_IP เก็บข้อมูลแอปพลิเคชั่นที่แต่ละโฮสต์ใช้งาน เพื่อนำมาวิเคราะห์ว่าโฮสต์ใดใช้งานเวบหรือแอปพลิเคชั่นอื่นๆ มากที่สุด หรือตาราง Table_host_total เก็บข้อมูลชนิดของแพ็กเก็ตและปริมาณไบต์รับส่งของแต่ละโฮสต์ เพื่อหาโฮสต์ที่รับส่งข้อมูลมากที่สุด ตาราง Table_all_host_info เก็บรายละเอียด ชื่อ IP MAC address ที่ตั้ง และบทบาทของทุกโฮสต์ เพื่อช่วยวิเคราะห์ความผิดปกติ เช่น 1 MAC address พบที่หลายโฮสต์ อาจบ่งชี้ว่าเกิดการปลอมแปลง MAC address สังเกตว่าตารางส่วนใหญ่ใช้วันเวลาเป็นดรรชนีสำหรับค้นคืน

MySQL plugin พัฒนาด้วยภาษาซี เป็นกระบวนการย่อย (Thread) ที่ทำงานไปพร้อมกับกระบวนการหลักของ ntop ซึ่ง plugin นี้จะวนรอบด้วยความถี่ตามตัวแปรที่ตั้งไว้ และบันทึกข้อมูลลงฐานข้อมูลตามรอบการเก็บ ซึ่งข้อมูลทุกชนิดที่เก็บนั้นเป็น global variable ของ ntop อยู่แล้ว จึงง่ายต่อการดึงมาใช้

3.2.2 Denial-of-service (DoS) plugin

DoS plugin ถูกพัฒนาขึ้นเพื่อช่วยวิเคราะห์หาเหตุการณ์จู่โจมบนเครือข่าย โดยเน้นไปที่การจู่โจมชนิด Denial-of-Service ห้าชนิด ได้แก่ port scan, host scan, SYN flood, UDP flood, และ ICMP flood ทีมวิจัยได้พัฒนาเทคนิคใหม่ในการวิเคราะห์หา DoS attack รายละเอียดตาม [2-3]

DoS plugin มีลักษณะเป็น thread และพัฒนาด้วยภาษาซีเช่นเดียวกับ MySQL plugin โดย DoS plugin คัดลอกข้อมูลแพ็กเก็ตจาก packet analyzer ของ ntop จึงไม่จำเป็นต้องทำหน้าที่ดักจับ แพ็กเก็ตเอง DoS plugin สร้าง flow record สำหรับทุกแพ็กเก็ตแยกตามโพรโทตอล ได้แก่ TCP flow, UDP flow และ ICMP flow และนำข้อมูล Flow ของทุกโพรโทตอลมาจับคู่กับรูปแบบการจู่โจมที่เรียกว่าattack graphlet หากรูปแบบตรงกันจะตรวจสอบว่าเป็นการจู่โจมประเภท DoS จริงหรือไม่ โดยใช้ค่าThreshold ซึ่งกำหนดเป็นค่ามาตรฐานไว้ก่อนหน้านี้ ผู้ใช้สามารถตั้งค่า default threshold ผ่านหน้าเวบดังรูปที่ 4 หลังจากวิเคราะห์แล้วว่ามีการจู่โจมเกิดขึ้น DoS plugin จะแจ้งเตือนบนหน้าเวบของ ntop และบันทึกเหตุการณ์ลงตาราง Table_dos_attack ในฐานข้อมูล

DoS Detection Preferences

Item	Description and Notes
Analysis Interval	50 seconds
Threshold of Port Scan	629 destination ports
Threshold of Host Scan	7 hosts
Threshold of SYN Flood	1826 source ports
Threshold of UDP Flood	26714 hosts
Threshold of ICMP Flood	22300 hosts

Save Config Cancel

รูปที่ 4 หน้าจอสำหรับตั้งค่า Default thresholds

3.2.3 ส่วนแสดงผล NtopViewer

NtopViewer คือเวบอินเทอร์เฟสที่วิเคราะห์และแสดงผลข้อมูลปริมาณการใช้งานเครือข่ายในรูปแบบที่เข้าใจง่ายกว่า ntop การพัฒนาใช้ PHP5 ร่วมกับ Javascript การแสดงผลในรูปแบบกราฟใช้ JPGraph สำหรับกราฟแท่งและกราฟวงกลม และใช้ RRDtool สำหรับกราฟเส้นที่มีแกนนอนเป็นเวลา สาเหตุที่ใช้ RRDtool วาดกราฟเส้นเนื่องจาก RRDtool จัดการข้อมูลจำนวนมากได้อย่างมีประสิทธิภาพ สามารถจัดการกับกราฟในกรณีข้อมูลไม่สม่ำเสมอได้ สามารถแปลงข้อมูลดิบที่เป็น counter มาเป็นค่าเฉลี่ย เช่นการคำนวณแบนด์วิดท์จากปริมาณไบต์เข้าออก ได้อย่างถูกต้องรวดเร็ว

3.3 ข้อจำกัดของระบบ

ซอฟต์แวร์ NtopViewer ผ่านการทดสอบประสิทธิภาพการทำงานบนเครือข่ายที่มีแบนด์วิดท์ไม่เกิน 10 Mbps และเครื่องลูกข่ายไม่เกิน 150 เครื่อง ผ่านการทดสอบติดตั้งบน

ระบบปฏิบัติการ Linux (Fedora Core 7-8, LinuxSIS 5.5-6.0) ต้องการหน่วยความจำอย่างน้อย 128 MB และพื้นที่ฮาร์ดดิสก์อย่างน้อย 1 GB (ขึ้นอยู่กับจำนวนคอมพิวเตอร์ที่ดูแล) ซอฟต์แวร์ที่จำเป็น ได้แก่ MySQL, Web server, PHP, JPGraph, JavaScript, และ RRDtool

ข้อจำกัดในการพัฒนาและการใช้งาน NtopViewer ในด้านอื่นๆ ได้แก่ ส่วนขยาย MySQL plugin และ DoS plugin ต้องใช้งานกับ ntop เวอร์ชั่น 3.3 ขึ้นไปเท่านั้น ส่วน DoS plugin สามารถตรวจจับการจู่โจมได้เพียงห้าชนิด (ตามหัวข้อ 3.2.2) MySQL plugin อ้างอิงการทำงานและใช้ช่วงความถี่การเก็บข้อมูลเดียวกับช่วงความถี่ของ RRD plugin

4. การทดสอบการใช้งาน

4.1 สภาพแวดล้อมในการทดสอบ

ทีมพัฒนานำซอฟต์แวร์ NtopViewer ไปทดสอบกับโรงเรียนสองช่วง มิ.ย.-ธ.ค. 2550 และก.ค.-ก.ย. 2551 บทความนี้จะกล่าวถึงผลการทดสอบในช่วงที่สองซึ่งไปทดสอบใช้งานจริงกับเครือข่ายภายในโรงเรียน 3 แห่ง ได้แก่ โรงเรียนธรรมศาสตร์คลองหลวงวิทยาคม จังหวัดปทุมธานี โรงเรียนนวมราชานุสรณ์ จังหวัดนครนายก และโรงเรียนบางลี่วิทยา จังหวัดสุพรรณบุรี รายละเอียดการทดสอบดูได้ที่ [16]

ตารางที่ 1 สภาพแวดล้อมที่ทดสอบ NtopViewer

โรงเรียน	ช่วงเวลาทดสอบ	Network bandwidth	จำนวนลูกข่าย
ธรรมศาสตร์คลองหลวงวิทยาคม	30 ก.ค. - 30 ส.ค. 51	2 Mbps	150
บางลี่วิทยา	22 ก.ค. - 15 ก.ย. 51	8 Mbps	80
นวมราชานุสรณ์	15 ก.ค. - 17 ก.ย. 51	2 Mbps	40
NECTEC	15 ก.ค. - 30 ก.ย. 51	10 Mbps	20

การติดตั้ง Ntop server เพื่อการทดสอบในทุกโรงเรียนจะติดตั้ง Hub คั่นอยู่ระหว่าง Internet Gateway และอุปกรณ์ Ethernet Switch โดยเชื่อมต่อ NtopViewer server เข้ากับ Hub เพื่อเฝ้าดูข้อมูลที่วิ่งเข้าออกเครือข่าย

4.2 ผลการทดสอบและการวิจารณ์ผล

กลุ่มตัวอย่างที่ประเมินผลการใช้งาน ประกอบด้วยบุคคลากรในโรงเรียนต่างๆ ที่ติดตั้งทดลองใช้ NtopViewer และผู้ดูแลเครือข่ายของ NECTEC รวม 19 คน กลุ่มตัวอย่างได้ทดลองใช้ NtopViewer บนระบบปฏิบัติการ Windows XP 17 คน และบน Windows Vista 2 คน เว็บบราวเซอร์ที่ใช้ ได้แก่ Internet Explorer 14 คน Firefox 5 คน

ตารางที่ 2 ตารางเปรียบเทียบระดับความพึงพอใจระหว่าง NtopViewer และ ntop

ประเด็น	NtopViewer ดีกว่ามาก	NtopViewer ดีกว่า	เท่ากัน	NtopViewer แย่กว่า	NtopViewer แย่กว่ามาก	ไม่มีความเห็น
ความสะดวกในการหาข้อมูลที่ต้องการ	7.14%	78.57 %	14.29 %			
ความง่ายในการเรียนรู้เพื่อใช้งานโปรแกรม	28.57 %	57.14 %	14.29 %			
ความถูกต้องของข้อมูล	7.14%	42.86 %	42.86 %			7.14%
ความเร็วในการแสดงผล		35.71 %	50%	7.14%	7.14%	
ประโยชน์ของข้อมูลที่นำเสนอ	7.14%	85.71 %	7.14%			
ความเพียงพอของข้อมูลที่นำเสนอ	7.14%	71.43 %	14.29 %			7.14%
ความง่ายในการทำความเข้าใจกับข้อมูล	7.14%	78.57 %	14.29 %			
ความง่ายในการตั้งค่าต่างๆ	7.14%	85.71 %	7.14%			
ความพึงพอใจในภาพรวม	14.29 %	78.57 %	7.14%			

การประเมินผลใช้แบบสอบถามสำรวจความสามารถในการใช้ซอฟต์แวร์ในห้ามุมมอง ได้แก่ 1) ความถูกต้องของข้อมูล 2) ประโยชน์ของข้อมูล 3) ความเข้าใจในการใช้งานโปรแกรม 4) ความเร็วในการแสดงผล 5) ความสะดวกและง่ายในการใช้งาน โดยเปรียบเทียบ NtopViewer กับ ntop เวอร์ชั่น 3.3 ก่อนการแก้ไข ระดับความพึงพอใจของผู้ใช้แสดงในตารางที่ 2 ซึ่งจะเห็นได้ว่าผลส่วนใหญ่มีความเห็นว่า NtopViewer นั้นสามารถใช้งานและทำความเข้าใจกับข้อมูลที่จัดแสดงได้สะดวกและง่ายกว่า ntop แต่ในเรื่องของความเร็วในการแสดงผลนั้นพบว่ายังมีปัญหาความล่าช้าในการแสดงกราฟ โดยเฉพาะอย่างยิ่งหากผู้ใช้เลือกช่วงเวลาที่ยาว ทำให้ต้องประมวลผลข้อมูลจำนวนมากที่ฐานข้อมูล อย่างไรก็ตาม

ในภาพรวมผู้ใช้พึงพอใจกับ NtopViewer มากกว่า ntop 3.3 แสดงว่าการพัฒนา NtopViewer นั้นบรรลุวัตถุประสงค์

5. บทสรุป

บทความนี้นำเสนอรายละเอียดการพัฒนาและการทดสอบ ซอฟต์แวร์ตรวจวัดการใช้งานอินเทอร์เน็ตในโรงเรียน (NtopViewer) ซึ่งเป็นการพัฒนาต่อยอดจากซอฟต์แวร์โอเพ่นซอร์ส ntop เป้าหมายของ NtopViewer คือแก้ไขข้อบกพร่องของ ntop ที่ไม่มีการเก็บข้อมูลลงฐานข้อมูลถาวร ทำให้ไม่สามารถเรียกดูประวัติการใช้งานเครือข่ายในอดีตได้ ส่งผลต่อการวิเคราะห์ปัญหาในเครือข่ายย้อนหลัง และปรับปรุง GUI ของ ntop ที่ซับซ้อน แสดงข้อมูลเชิงลึกและละเอียดมากเกินความเข้าใจของผู้ดูแลระบบที่ไม่เชี่ยวชาญด้านเครือข่าย

NtopViewer ผ่านการทดสอบและประเมินผลโดยผู้ดูแลระบบในสถานศึกษา เพื่อขอคำแนะนำและข้อเสนอแนะ เพื่อมาปรับปรุง จนได้ซอฟต์แวร์ที่ใช้งานได้ตรงตามวัตถุประสงค์ และผู้ดูแลระบบมีความพึงพอใจในการใช้งานมากกว่าซอฟต์แวร์ ntop เดิม เริ่มตั้งแต่ 29 สิงหาคม 2551 ทางทีมวิจัยเปิดให้ผู้สนใจทั่วไปดาวน์โหลดและใช้งาน NtopViewer ได้ฟรีที่ http://wiki.nectec.or.th/ntl/Project/NtopViewer พร้อมทั้งเผยแพร่ซอฟต์แวร์นี้ร่วมกับระบบปฏิบัติการ LinuxSiS 6.0 [17]

5.1 แนวทางการพัฒนาต่อ

สิ่งที่ควรปรับปรุงในการพัฒนาโปรแกรม NtopViewer ในลำดับต่อไป ได้แก่ ปรับปรุงประสิทธิภาพการติดต่อฐานข้อมูล เช่น ลดปริมาณข้อมูลที่เก็บ ปรับปรุงโครงสร้าง เพื่อให้การค้นคืนเร็วขึ้น เพิ่มความยืดหยุ่นในการเลือกดูข้อมูล เช่น สามารถเลือก x ลำดับแรกที่แสดงผล (ปัจจุบันแสดงเพียง 5 ลำดับแรก) และเชื่อมโยงเข้ากับระบบ Firewall หรือระบบควบคุมแบนด์วิดท์เมื่อพบการใช้งานเครือข่ายที่ไม่เหมาะสม เป็นต้น

6. กิตติกรรมประกาศ

ซอฟต์แวร์ NtopViewer นี้ได้รับทุนสนับสนุนจากโปรแกรมวิศวกรรมความรู้ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.)

7. เอกสารอ้างอิง

[1] Network Top, http://www.ntop.org.

[2] S.Pukkawanna, V.Visoottiviseth, and P.Pongpaibool, "Lightweight Detection of DoS Attacks," in *Proc. of IEEE ICON 2007*, Adelaide, Australia, Nov. 2007.

[3] S.Pukkawanna, P.Pongpaibool, and V.Visoottiviseth, "LD^2: A System for Lightweight Detection of Denial-of-Service Attacks," in *Proc. of IEEE MILCOM 2008*, San Diego, CA, USA, Nov. 2008.

[4] Tcpdump, http://www.tcpdump.

[5] Wireshark, http://www.wireshark.org.

[6] Multi Router Traffic Grapher, http://www.mrtg.org.

[7] NetFlow Analyzer, http://manageengine.adventnet.com/products/netflow.

[8] SoftPerfect Traffic Meter, http://www.softperfect.com/products/trafficmeter.

[9] Network Probe, http://www.objectplanet.com/probe.

[10] Colasoft Capsa, http://www.colasoft.com/capsa.

[11] NetLimiter, http://www.netlimiter.com.

[12] Ultra Network Analyzer, http://www.gjpsoft.com/UltraNetSniffer.

[13] IP Traffic Monitor, http://www.skyward-soft.com/mambo/index.php.

[14] PRTG, http://www.paessler.com/prtg.

[15] RRDtool, http://oss.oetiker.ch/rrdtool.

[16] การทดสอบ NtopViewer ภาคสนาม. [อ อ น ไ ล น์]. http://wiki.nectec.or.th/ntl/Project/NtopViewerFieldTest.

[17] โครงการพัฒนาและส่งเสริมการใช้ซอฟต์แวร์โอเพนซอร์ส LinuxSIS. [อ อ น ไ ล น์]. http://www.opentle.org. สืบค้น 18 ธันวาคม 2251