รายงานการใช้งานระบบเครือข่ายคอมพิวเตอร์ มหาวิทยาลัยเทคโนโลยีสุรนารี

ประจำเดือนกันยายน 2560

1. <u>รายงานการดำเนินงานของฝ่ายเครือข่าย</u>

1.1 สรุปการดำเนินการบนระบบเครือข่าย SUTnet

- Link Uninet Down วันที่ 10 ก.ย.60 เวลา 14.00-15.30 น. ทั้งนี้ไม่กระทบผู้ใชงาน
- เปลี่ยน link ผู้ให้บริการ internet service provider จากเดิม บริษัท 3BB ที่ความเร็ว (Domestic 2 Gbps/Inter 1Gbps) เป็นบริษัท AWN 3BB ที่ความเร็ว (Domestic 3 Gbps/Inter 1Gbps) ณ. วันที่ 26 ก.ย.60
- ทดสอบอุปกรณ์รักษาความปลอดภัยระบบเครือข่าย (Firewall) ในวันที่ 15 กันยายน 2560 เวลา 13.40-13.55 น. ทำให้ระบบเครือข่ายไม่สามารถใช้งานได้ในเวลาดังกล่าว
- แก้ไขปัญหาจุดเชื่อมต่อระบบเครือข่าย ตามที่ได้มีการแจ้งซ่อมดังนี้
  - รหัสใบงาน 600731-10-1 สำนักงานคณบดีสำนักวิชาพยาบาลศาสตร์ ชั้น 1 อาคารวิชาการ 1 แก้ไขสาย LAN โดนหนูกัดขาด และย้ายตำแหน่งติดตั้ง Outlet และจัดทำสาย LAN เพื่อเชื่อมต่อ จำนวน 1 เส้น
  - รหัสใบงาน 600905-23-1 สาขาวิชาการพยาบาลอนามัยชุมชน อาคารวิชาการ 1 ชั้น 3 จัดทำสาย LAN ความยาว 7 เมตร จำนวน 1 เส้นพร้อมติดตั้งให้
  - รหัสใบงาน 600906-16-1 อาคารเรียนรวม 2 ศูนย์บริการการศึกษา ห้อง สทศ. ย้าย Switch HUB ติดตั้งไว้ภายในห้อง และจัดทำสาย LAN จำนวน 5 เส้น
- ติดตั้ง Cisco switch HUB จำนวน 6 เครื่อง ดังนี้
  - ติดตั้ง Cisco switch HUB ที่หอพักนักศึกษา 15 ติดตั้งทั้งหมดจำนวน 2 เครื่อง
  - ติดตั้ง Cisco switch HUB ที่หอพักนักศึกษา 16 ติดตั้งทั้งหมดจำนวน 4 เครื่อง

1.2 สรุปการดำเนินการบนระบบเครือข่ายไร้สาย

- ติดตั้ง Access Point เพิ่มจำนวน 138 เครื่อง ดังนี้
  - ติดตั้ง Access Point ที่หอพักนักศึกษา 15 ติดตั้งทั้งหมดจำนวน 60 เครื่อง
  - ติดตั้ง Access Point ที่หอพักนักศึกษา 16 ติดตั้งทั้งหมดจำนวน 78 เครื่อง

1.3 สรุปการดำเนินการบนระบบ Internet Data Center

- เปลี่ยน harddisk storage netapp เสีย 1 ลูก นำลูกสำรองเปลี่ยนทดแทนเรียบร้อยแล้ว
- แก้ไขปัญหา vmserver 4 (vsan1) มี disk เสีย 1 ลูก แก้ไขโดยลบ diskgroup และสร้าง diskgroup.ใหม่ โดยไม่นำเอา disk ที่เสียเข้ามาใน diskgroup และ replace ลูกใหม่ และ join disk ลูกใหม่เข้า diskgroup
- ย้าย VMserver0 จากกลุ่ม vsan 2 ไปกลุ่ม vsan1
- เพิ่ม harddisk vmserver6 (vasn2) 6 ลูก ลูกละ 1 Tb

- เปลี่ยนพัดลม vmserver33,39 ทำให้สามารถใช้งานได้ตามปกติ
- แก้ไข vmserver : unicad_connector , unicad_gateway โดยเปลี่ยนระบบปฏิบัติการจากเดิม Ubuntu16 เป็น CentOS 7 , cpu 4 vcpu, ram 8 Gb, Hard disk 60 Gb, หมายเลข IP 203.158.7.112 , 203.158.7.113 โดยติดตั้ง webmin และ ssh เพิ่มเติม

1.4 สรุปการดำเนินการบนระบบโทรคมนาคม

- จัดสรรหมายเลขโทรศัพท์ตามหนังสือขอใช้บริการ จำนวน 4 เลขหมาย
- ซ่อมบำรุงตู้สาขาโทรศัพท์ที่อาคารเครื่องมือฯ 7 เนื่องจากไฟเบอร์ออฟติกมีปัญหา ดำเนินการแก้ไขแล้วเสร็จ สามารถใช้งานได้ตามปกติ
- เพิ่มตำแหน่งสายสัญญาณโทรศัพท์ในห้องอธิการบดีจำนวน 3 จุด หลังจากปรับปรุงห้องทำงานใหม่ และติดตั้งเครื่องโทรศัพท์ไอพีโฟน จำนวน 3 เครื่อง
- เพิ่มตำแหน่งสายสัญญาณโทรศัพท์ในห้องผู้ช่วยรองอธิการดีที่อาคารบริหารจำนวน 8 จุด และติดตั้งเครื่องโทรศัพท์ไอพีโฟนเพิ่ม 8 เครื่อง พร้อมจัดสรรหมายเลขโทรศัพท์ใหม่
- ย้ายจุดสายสัญญาณตำแหน่งเครื่องโทรศัพท์โทรศัพท์ห้องรองอธิการบดีฝ่ายบริหารทั่วไป

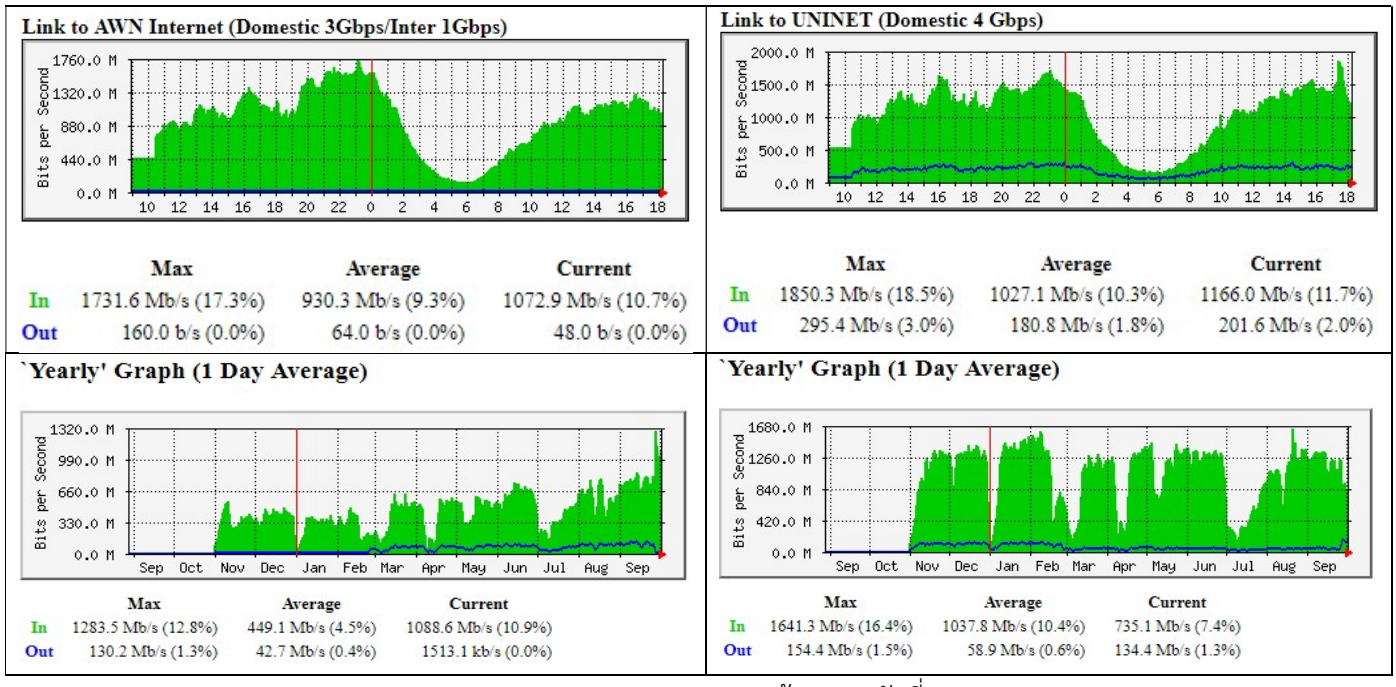
1.5 การดำเนินการอื่นๆ

- จัดสรรพื้นที่เว็บไซต์ส่วนบุคคล จำนวน 5 account
- จัดสรรพื้นที่เว็บไซต์ ชนิด intranet แก่สถาบันวิจัยและพัฒนา
- จัดสรรพื้นที่เว็บไซต์ สำหรับวิจิตรภาคีสถาน http://www.wps.sut.ac.th
- จัดสรร internet account สำหรับกิจกรรมอบรมเชิงปฏิบัติการ “การขายสินค้า otop ไปต่างประเทศผ่าน eBay” สำนักวิชาวิศวกรรมศาสตร์ จำนวน 200 account
- แจ้งเตือน ช่องโหว่ BlueBorne ถูกแฮกเครื่อง ฝังมัลแวร์ได้ผ่าน Bluetooth
- แก้ไข web server : web.sut.ac.th โดน hack ผ่านพื้นที่เว็บไซต์ science.sut.ac.th ที่มีการเปิด permission 777 ในบาง folder ทำให้มีการส่งคสริปเข้ามารันในระบบได้ แก้ไขโดยลบสคริปแปลกปลอม และปรับ permission ใหม่ให้มีความเหมาะสม และทำการวาง .htaccess ไฟล์เพื่อป้องกันการสั่งรันไฟล์ php ใน folder นั้น
- เว็บไซต์ http://ced.sut.ac.th/ โดนเปลี่ยนแปลงข้อมูล ในบางหน้า และไฟล์เอกสารโดนลบ ตรวจสอบพบว่า การ hack เกิดจากการที่เปิด permission 777 ของ file - folder เอาไว้ ทำให้สามารถ upload file hack หรือ เปลี่ยนแปลง code php ของไฟล์ที่เปิด 777 ตลอดจนสามารถลบไฟล์ออกจากระบบได้ ซึ่งมีการ hack มานานแล้วทำให้ไม่สามารถใช้วิธีการ recovery ข้อมูลได้ แต่ได้ให้คำแนะนำวิธีการแก้ไขและแนวทางแก้ไขแล้ว
- แจ้งเตือน-ตรวจสอบความปลอดภัยบนเว็บไซต์ http://web.sut.ac.th/2012 มีการเปิด permission 777 สำหรับ files-folder (ยอมให้มีการ read-write-execute) ไว้จำนวนมาก โดยจะเป็นช่องโหว่ให้ผู้ไม่หวังดีสามารถเข้ามาวาง file hack จากภายนอกได้
- Disable account น.ศ. ที่สำเร็จการศึกษารวม 1,256 account

- ตัดจำหน่ายครุภัณฑ์ฝ่ายเครือข่ายที่ชำรุด-ปลดระวาง ประจำปี 2560 จำนวน 353 รายการ
- เปิดตัวบริการ google drive file stream 27 ก.ย. 60 / ทำให้มีผู้ใช้งาน sutg.dot account รายใหม่เข้าสู่ระบบ 413 คน
- จัดกิจกรรม KM ประจำปี 2560 ของฝ่ายเครือข่าย เรื่อง การสร้างองค์ความรู้เรื่อง Wireless Security สำหรับเจ้าหน้าที่ฝ่ายเครือข่ายเพื่อให้บริการและการแก้ไขปัญหาได้อย่างมีประสิทธิภาพ

2.รายงานการใช้งานระบบเครือข่าย

Internet Gateway Traffic



*ทางออก Uninet 4Gbps / AWN Domestic 3 Gbps,Inter 1 Gbps) / ข้อมูล ณ วันที่ 3 ต.ค. 60

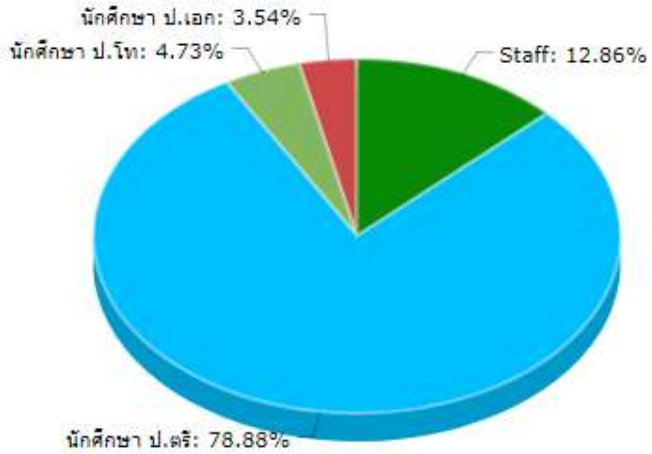
2.1 รายงานจำนวนผู้ใช้งานผ่านระบบเครือข่าย (LAN) (ไม่รวมห้องปฏิบัติการคอมฯ)

(ข้อมูล ณ วันที่ 3 ต.ค. 60)

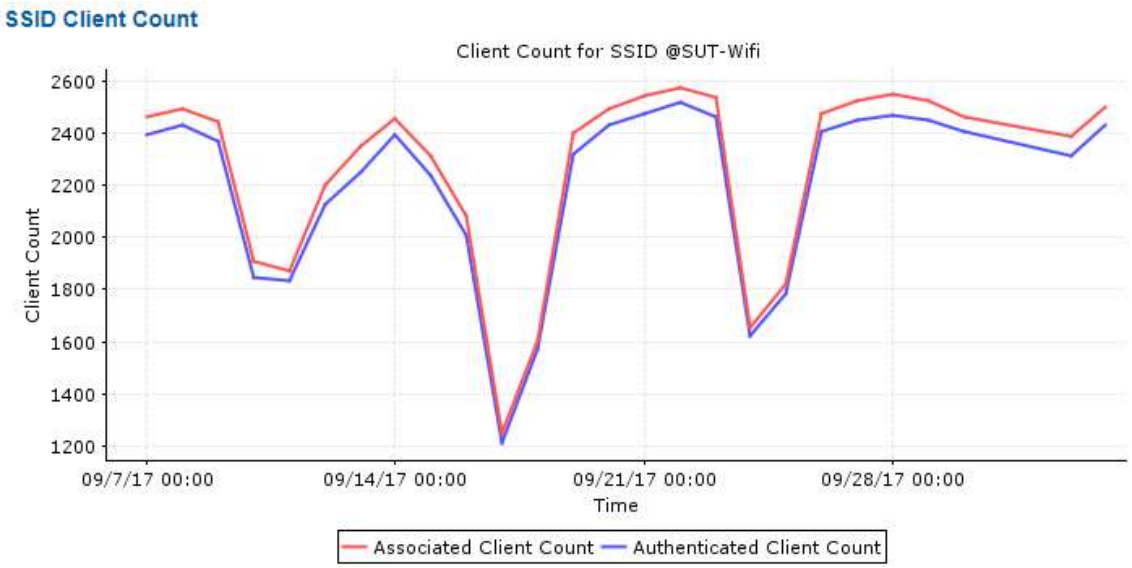
วิธีการ	จำนวน
วิธีการแบบ NAC In-Band	256 คน
วิธีการแบบ ISE	1,655 คน
รวมทั้งหมด	**1,911 คน**

2.2 รายงานจำนวนผู้ใช้งานผ่านระบบเครือข่ายไร้สาย

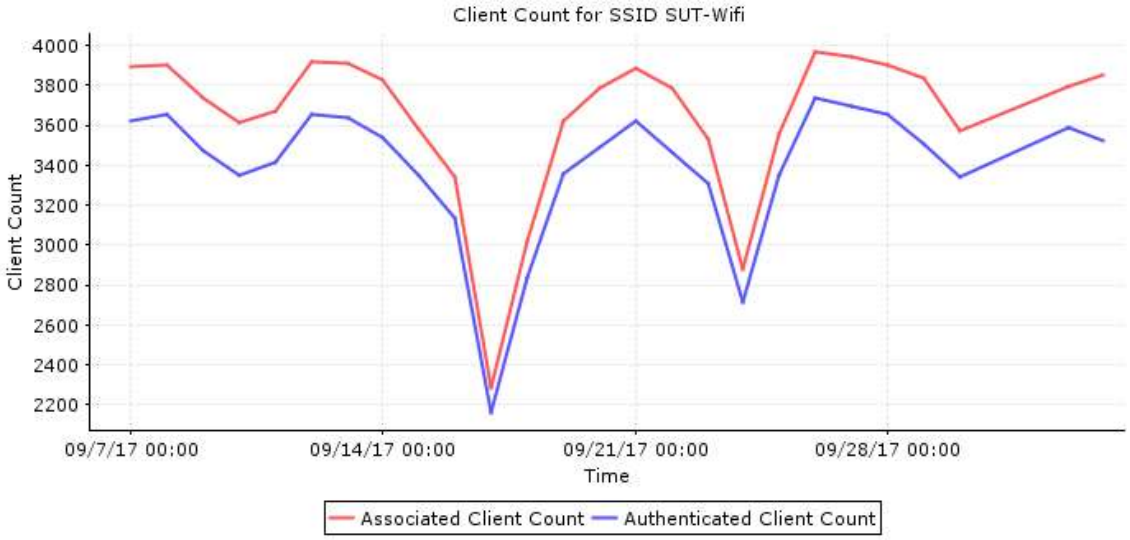
2.2.1 จำนวนผู้ใช้งานเครือข่ายไร้สาย @SUT-Wifi



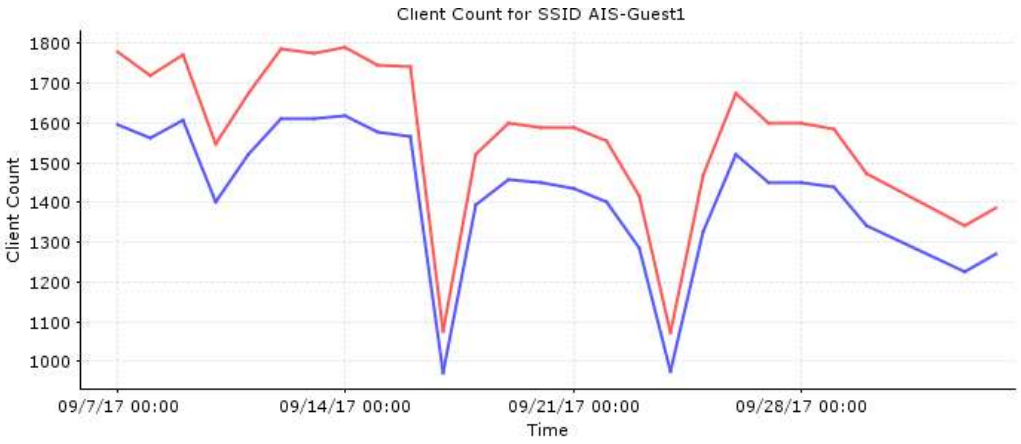
จำนวนผู้ใช้งานเครือข่ายไร้สาย @SUT-Wifi (ที่มา https://203.158.4.211) (ข้อมูล 1 เดือนย้อนหลัง)

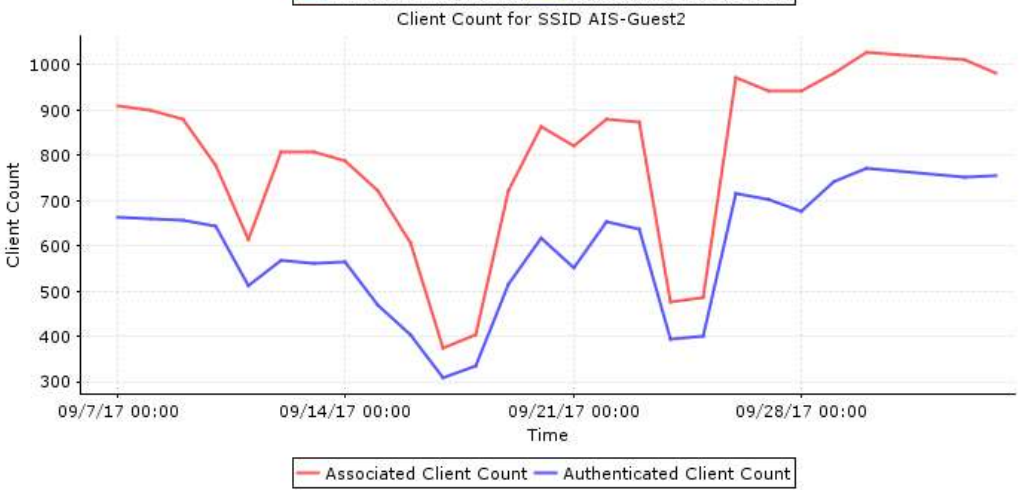


2.2.2 จำนวนผู้ใช้งานเครือข่ายไร้สาย SUT-Wifi

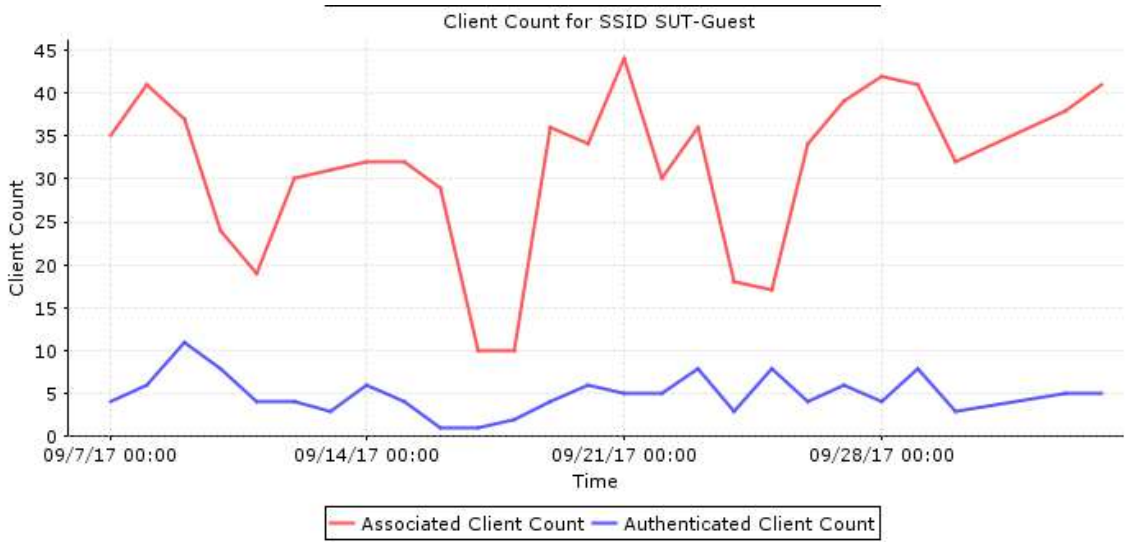


2.2.3 จำนวนผู้ใช้งานเครือข่ายไร้สาย SUT-AIS

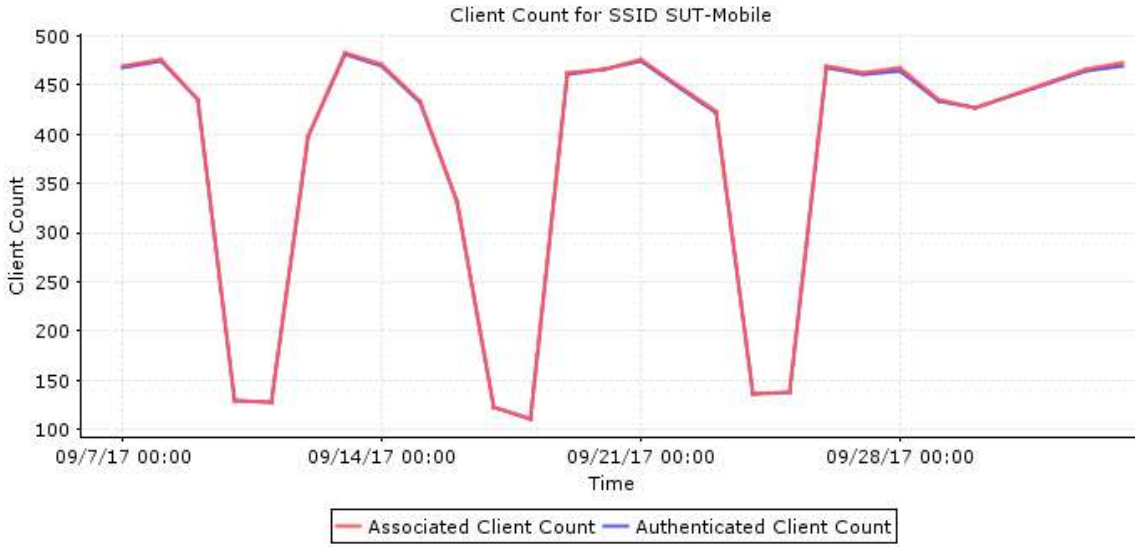




2.2.4 จำนวนผู้ใช้งานเครือข่ายไร้สาย SUT-Guest



2.2.5 จำนวนผู้ใช้งานเครือข่ายไร้สาย SUT-Mobile

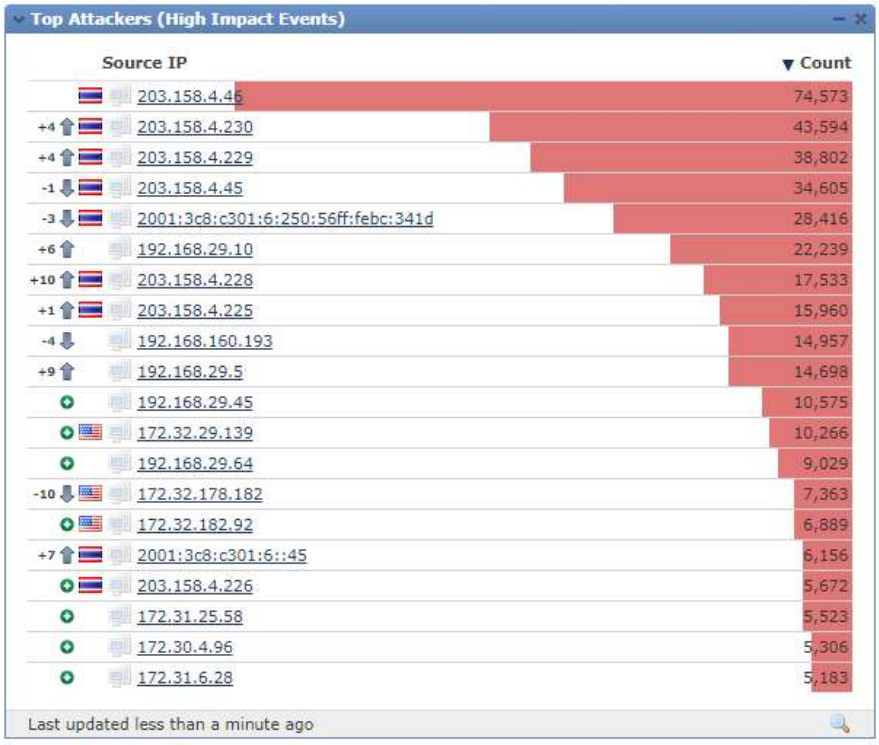


2.2.6 สรุปสถิติจำนวนผู้ใช้งานผ่านระบบ wireless ทั้งหมด

- ผู้ใช้งานผ่านระบบ wireless สูงสุด 7,802 คน/วัน
- ผู้ใช้งานผ่านระบบ wireless ต่ำสุด 4,387 คน/วัน
- ผู้ใช้งานผ่านระบบ wireless เฉลี่ย 6,762 คน/วัน

3. ภัยคุกคามระบบเครือข่าย

- **สถานะการณ์ไวรัสและมัลแวร์ที่แพร่ระบาดในมหาวิทยาลัย** (ข้อมูล 1 เดือนย้อนหลัง)
  (ที่มา : Sourcefire 203.158.4.43)



Malware Intrusions

Message	Count
MALWARE-CNC Win.Trojan.Zeus variant outbound connection (1:35030:1)	143,668
MALWARE-CNC Win.Trojan.Zeus variant outbound connection (1:35549:1)	92,949
+1 BLACKLIST suspicious .bit dns query (1:41083:1)	78,951
+2 MALWARE-CNC Win.Trojan.Zeus variant outbound connection (1:35746:1)	61,267
MALWARE-CNC Win.Trojan.Njrat variant outbound connection (1:25100:5)	39,417
+1 MALWARE-CNC Win.Trojan.Glupteba.M initial outbound connection (1:30288:2)	38,244
+1 MALWARE-CNC Win.Trojan.Nvbpass variant outbound connection (1:19864:5)	38,084
+4 BLACKLIST DNS request for known malware domain ltc.give-me-coins.com (1:31660:1)	36,942
-6 BLACKLIST suspicious .bit tcp dns query (1:42841:4)	33,411
MALWARE-CNC Win.Trojan.Zbot variant in.php outbound connection (1:26023:3)	22,075
-2 BLACKLIST DNS request for known malware domain chickenkiller.com (1:28283:1)	19,470
+4 BLACKLIST DNS request for known malware domain rterybrstutnrsbberve.com	18,921
+1 BLACKLIST DNS request for known malware domain erwbtkidthetcwerc.com (1:28058:1)	18,589
-3 MALWARE-CNC Win.Trojan.Jaktinier outbound connection (1:31459:3)	17,589
BLACKLIST DNS request for known malware domain rvbwtbeitwjeitv.com (1:28060:1)	16,861
-3 MALWARE-CNC Win.Trojan.Pmabot outbound connection (1:37213:3)	16,255
+1 MALWARE-CNC Win.Trojan.Andromeda variant outbound connection (1:33496:1)	15,146
-1 BLACKLIST DNS request for known malware domain xa.yessearches.com -	13,540
MALWARE-CNC Win.Trojan.Njrat variant outbound connection (1:36506:2)	7,508
BLACKLIST DNS request for known malware domain restless.su - Gamarue Trojan	7,473

Last updated 1 minute ago

- **การยับยั้งการโจมตีบนระบบเครือข่าย โดย อุปกรณ์ IPS** (ข้อมูล 1 เดือนย้อนหลัง)
  (ที่มา : Sourcefire 203.158.4.43)

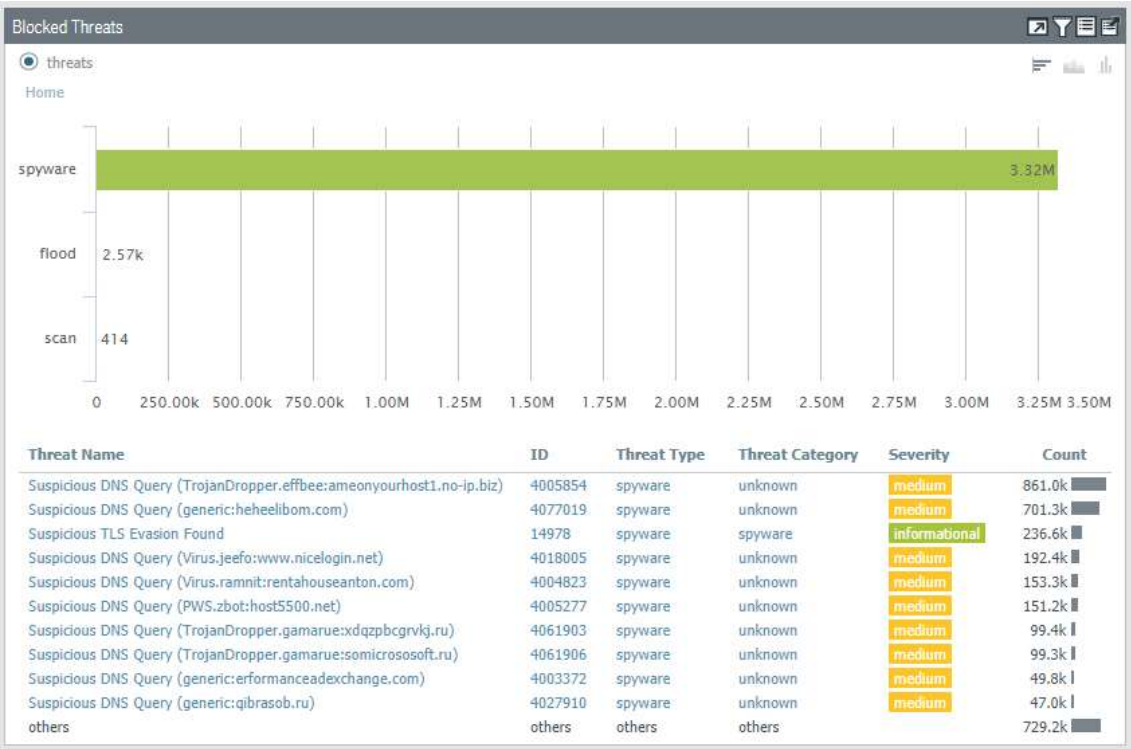
Dropped Intrusion Events

Classification	Count
A Network Trojan was Detected	773,130
Attempted Administrator Privilege Gain	11,017
Web Application Attack	4,577
Misc Activity	2,601
Attempted Information Leak	328
Potential Corporate Policy Violation	315
Attempted User Privilege Gain	74

Last updated 2 minutes ago

- **การยับยั้งการโจมตีบนระบบเครือข่าย โดย อุปกรณ์ Firewall** (ข้อมูล 1 เดือนย้อนหลัง)

  (ที่มา Paloalto:203.158.4.110)



Threat Name	ID	Threat Type	Threat Category	Severity	Count
Suspicious DNS Query (TrojanDropper.effbee:ameonyourhost1.no-ip.biz)	4005854	spyware	unknown	medium	861.0k
Suspicious DNS Query (generic:heheelibom.com)	4077019	spyware	unknown	medium	701.3k
Suspicious TLS Evasion Found	14978	spyware	spyware	informational	236.6k
Suspicious DNS Query (Virus.jeefo:www.nicelogin.net)	4018005	spyware	unknown	medium	192.4k
Suspicious DNS Query (Virus.ramnit:rentahouseanton.com)	4004823	spyware	unknown	medium	153.3k
Suspicious DNS Query (PWS.zbot:host5500.net)	4005277	spyware	unknown	medium	151.2k
Suspicious DNS Query (TrojanDropper.gamarue:xdqzpbcgrvkj.ru)	4061903	spyware	unknown	medium	99.4k
Suspicious DNS Query (TrojanDropper.gamarue:somicrososoft.ru)	4061906	spyware	unknown	medium	99.3k
Suspicious DNS Query (generic:erformanceadexchange.com)	4003372	spyware	unknown	medium	49.8k
Suspicious DNS Query (generic:qibrasob.ru)	4027910	spyware	unknown	medium	47.0k
others	others	others	others		729.2k