

ระบบป้องกันไอทีบนจอผู้ให้บริการอินเทอร์เน็ตคัดบัญชีดำ
PROTECTION SYSTEM IP OF INTERNET SERVICE PROVIDERS
(ISP) MOUNTED BLACKLIST



รายงานนี้เป็นส่วนหนึ่งของวิทยานิพนธ์ที่ภาวนิพนธ์ 2

หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ

คณะเทคโนโลยีสารสนเทศ

มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ภาคเรียนที่ 2 ปีการศึกษา 2557

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า

ไม่ว่าวิธีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้คัดลอกเนื้อหา และต้องอ้างถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ระบบป้องกันไอพีของผู้ให้บริการอินเทอร์เน็ตผิดบัญญัติ

PROTECTION SYSTEM IP OF INTERNET SERVICE PROVIDERS
(ISP) MOUNTED BLACKLIST



T144584

โดย

วีรวัฒน์ โพธิ์ระย้า

WEERAWAT PORAYA

อาจารย์ที่ปรึกษา

ดร. นล เปรมชัยเจียร

เลขหมู่.....
เลขทะเบียน.....144584

วัน,เดือน,ปี...2.5...๒๕๖๒...2559



รายงานนี้เป็นส่วนหนึ่งของวิชาการศึกษาระดับ 2

หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ

คณะเทคโนโลยีสารสนเทศ

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับ...ภาคเรียนที่ 2 ปีการศึกษา 2557...อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

**PROTECTION SYSTEM IP OF INTERNET SERVICE PROVIDERS
(ISP) MOUNTED BLACKLIST**



**A REPORT SUBMITTED IN PARTIAL FULFILLMENT OF THE
REQUIREMENTS OF THE COURSE
INDEPENDENT STUDY2
MASTER OF SCIENCE PROGRAM IN INFORMATION TECHNOLOGY
FACULTY OF INFORMATION TECHNOLOGY
KING MONKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG**

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



COPYRIGHT 2015

FACULTY OF INFORMATION TECHNOLOGY

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

เอกสารนี้เป็นเอกสารที่จัดทำขึ้นเพื่อใช้ในการเรียนการสอนเท่านั้น ไม่สามารถนำเอกสารนี้ไปเผยแพร่หรือใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ใบรับรองการศึกษาอิสระ 2 (Independent Study 2)

เรื่อง

ระบบป้องกันไอพีของผู้ให้บริการอินเทอร์เน็ตติดบัญชีดำ

PROTECTION SYSTEM IP OF INTERNET SERVICE PROVIDERS (ISP) MOUNTED BLACKLIST

นายวิวัฒน์ โพธิ์ระย้า

รหัสประจำตัว 56606080

ขอรับรองว่ารายงานฉบับนี้ ข้าพเจ้าไม่ได้คัดลอกมาจากที่ได้
รายงานฉบับนี้ได้รับการตรวจสอบและอนุมัติให้เป็นส่วนหนึ่งของ
การศึกษาอิสระ 2 หลักสูตรวิทยาศาสตรมหาบัณฑิต (เทคโนโลยีสารสนเทศ)
ภาคเรียนที่ 2 ปีการศึกษา 2557

นล เปร่มชัย

อาจารย์ที่ปรึกษา

(ดร.นล เปร่มชัย)

สุวรรณ อันนันหนับ

กรรมการสอบ

(ดร.สุวรรณ อันนันหนับ)

กนกวรรณ อัจฉริยะชาญวิช

กรรมการสอบ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับ (ดร.กนกวรรณ อัจฉริยะชาญวิช) อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

หัวข้อ	ระบบป้องกันไอพีของผู้ให้บริการอินเทอร์เน็ตฉบับลิขสิทธิ์
รหัสนักศึกษา	56606080
นักศึกษา	นายวิวัฒน์ โพธิ์ระยา
ปริญญา	วิทยาศาสตรมหาบัณฑิต
สาขาวิชา	เทคโนโลยีสารสนเทศ
แขนงวิชา	เทคโนโลยีเครือข่ายและระบบ
ปีการศึกษา	2557
อาจารย์ที่ปรึกษา	ดร.นลพร มัชฌิม

บทคัดย่อ

รายงานฉบับนี้เสนอวิธีการแก้ปัญหาไอพีของผู้ให้บริการอินเทอร์เน็ตฉบับลิขสิทธิ์ มีวัตถุประสงค์เพื่อศึกษาโปรโตคอลหลัก ๆ ที่ใช้ในการรับ-ส่งอีเมล คือ SMTP เป็นโปรโตคอลแบบ TCP/IP ที่ใช้ในการส่งอีเมลในเครือข่ายอินเทอร์เน็ตไปยังเครื่องบริการอื่น ๆ ซึ่งสามารถส่งอีเมลไปยังผู้ให้บริการได้ทั่วโลกมีข้อจำกัดในเรื่องของความสามารถในการส่งอีเมลว่าสามารถทำได้แบบเป็นคิว และ SMTP ส่วนใหญ่จะไม่ยอมให้คนภายนอกองค์กร หรือไอพีที่อยู่ภายนอกองค์กรใช้งาน SMTP ได้ แต่จดหมายนี้อยู่ในรูปแบบดิจิทัลไม่สามารถจับต้องได้ ดังนั้นผู้ให้บริการแต่ละที่จึงต้องตรวจสอบผู้ให้บริการก่อนว่าผู้ให้บริการเป็นลูกค้าหรืออยู่ในฐานข้อมูลภายในองค์กรหรือไม่ ถ้าผู้ให้บริการอยู่ในฐานข้อมูลระบบจะยินยอมให้ส่งอีเมลไปยังปลายทางได้

SMTP ส่วนใหญ่อยู่ในรูปแบบที่หลาย ๆ คนคุ้นเคย คือ smtp.company.com เป็นต้นซึ่งโดเมนเหล่านี้จะถูกมอบให้โดยผู้ให้บริการอีเมลเซิร์ฟเวอร์ (E-mailServer) ของคุณ เพราะผู้ให้บริการกลัวผู้ให้บริการส่ง Spam mail หรือโฆษณาไปรบกวนคนอื่นหรือผู้ให้บริการรายอื่น เพราะถ้ามีผู้ให้บริการสักคนส่งอีเมลไปหาผู้ให้บริการรายอื่นแทนที่ผู้รับอีเมลจะ Block E-mail ของคุณเพียงคนเดียว แต่กลับ Block SMTP ของผู้ให้บริการอีเมลเซิร์ฟเวอร์ทำให้ผู้ให้บริการคนอื่นเดือดร้อนไปด้วย เพราะใช้อีเมลเซิร์ฟเวอร์ติด Blacklist

Title	Protection System IP of Internet Service Providers (ISP) Mounted Blacklist
Student	Mr. Weerawat Poraya
Student ID.	56606080
Degree	Master of Science
Program	Information Technology
Major	Network Technologies and System
Academic Year	2014
Advisor	Dr. N. Premasathian

ABSTRACT

The report proposes how to solve the problem. IP Internet providers stick black Is intended to study the main Protocol used to transfer email is SMTP Protocol is a TCP/IP based network, send E-Mail to the Internet to other services that can send mail to users all over the world. There is a limit in terms of the ability to send e-mail if it can be done as most of the SMTP queue and will not allow people outside your organization or Enterprise outside the IP using this SMTP mail, but it is in a digital format must not handle so that each provider must examine you prior to that you as a customer or in the database layout or not. If it is allowed to export to.

SMTP usually is in a format that many people are familiar with. Is that smtp.company.com these values will be provided by your E-mail provider's server because service providers were afraid of you. Sending Spam mail or advertising to find somebody else, because if someone sends e-mail to find out everyone else, rather than the recipient will Block email you alone but Block SMTP E-mail server provider allows other users to troubling because E-mail server running Blacklist.

กิตติกรรมประกาศ

การจัดทำรายงานการศึกษาอิสระเรื่องระบบป้องกันไอพีของผู้ให้บริการอินเทอร์เน็ตติดบัญชีดำ สำเร็จลุล่วงไปด้วยดีด้วยความช่วยเหลืออย่างดียิ่งของอาจารย์ ดร.นลเปรมชัยเสีเยอร์ อาจารย์ที่ปรึกษาจัดทำรายงานการศึกษาอิสระ ที่ได้กรุณาให้คำปรึกษา ชี้แนะแนวทาง และช่วยตรวจสอบแก้ไขข้อบกพร่อง จนปัญหาพิเศษนี้สำเร็จลงได้

ขอขอบคุณคณาจารย์คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง ทุกท่านที่ได้ประสิทธิประสาทวิชาความรู้ในด้านต่างๆ ทำให้ผู้พัฒนาระบบสามารถนำความรู้ที่ได้มาประยุกต์ใช้ในการจัดทำรายงานการศึกษาอิสระนี้ได้อย่างมีประสิทธิภาพ

ขอขอบคุณผู้เชี่ยวชาญ ฝ่ายบริการอินเทอร์เน็ต บริษัท ทีทีแอนด์ที จำกัด (มหาชน) ทุกท่านที่ได้กรุณาสละเวลาอันมีค่าในการตรวจสอบ รวมทั้งให้คำปรึกษา ชี้แนะแนวทาง และช่วยตรวจสอบแก้ไขข้อบกพร่อง จนทำให้รายงานการศึกษาอิสระนี้มีความสมบูรณ์

สุดท้ายนี้ผู้จัดทำใครขอกราบขอบพระคุณ บิดา มารดา และครอบครัวที่เป็นกำลังใจให้การสนับสนุนในทุกเรื่อง ทำให้ผู้จัดทำรายงานการศึกษาอิสระนี้สามารถทำรายงานการศึกษาอิสระได้สำเร็จลุล่วงไปด้วยดี

วีรวัฒน์ โพธิ์ระยา

สารบัญ

	หน้า
บทคัดย่อภาษาไทย	I
บทคัดย่อภาษาอังกฤษ.....	II
กิตติกรรมประกาศ.....	III
สารบัญ.....	IV
สารบัญรูป	VI
บทที่ 1 บทนำ.....	1
1.1ความเป็นมาและความสำคัญ.....	1
1.2ความมุ่งมั่นและวัตถุประสงค์ของการศึกษา.....	2
1.3ขอบเขตของการพัฒนาระบบ.....	2
1.4นิยามศัพท์เฉพาะ	3
1.5แนวทางการศึกษา	3
1.6ผลที่คาดว่าจะได้รับ.....	3
บทที่ 2 เอกสารและงานวิจัยที่เกี่ยวข้อง	4
2.1แนวคิดเกี่ยวกับโปรโตคอล SMTP	4
2.2แนวคิดเกี่ยวกับการป้องกัน E-mail Virus และ E-mail Spam	6
2.3แนวคิดเกี่ยวกับความแตกต่างระหว่าง SMTP Proxy และ Mail Server	7
2.4ศึกษาผลกระทบและปัญหาขององค์กรผู้ให้บริการอินเทอร์เน็ต	9
2.5เครื่องมือที่ใช้ในการพัฒนาระบบ	9
บทที่ 3 ขั้นตอนการพัฒนาและออกแบบระบบ	12
3.1วิเคราะห์ระบบงานเดิม.....	12
3.2วิเคราะห์ระบบงานใหม่	14
บทที่ 4 การทดสอบและผลการทดสอบ	19
4.1บทนำ.....	19
4.2การทดสอบ	19
4.3ผลการทดสอบ	22
บทที่ 5 สรุปผลและข้อเสนอแนะ	26
5.1บทนำ.....	26
5.2สรุปผลและอภิปรายการดำเนินงาน.....	26

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญ (ต่อ)

	หน้า
5.3 ปัญหาและอุปสรรคในการทดลอง.....	26
5.4 ข้อเสนอแนะ	27
บรรณานุกรม	28
ประวัติผู้เขียน	29



สารบัญรูป

รูปที่	หน้า
2.1 กระบวนการส่งอีเมลล์ของโปรโตคอล SMTP.....	6
3. 1ภาพรวมของระบบงานเดิม.....	13
3. 2 ภาพรวมของระบบงานใหม่.....	15
3. 3 แอคทิวิตีไดอะแกรมการทำงานของระบบงานใหม่.....	16
3. 4แอคทิวิตีไดอะแกรมการเก็บข้อมูลค่าสถิติลงดาต้าเบส	17
3. 5แอคทิวิตีไดอะแกรมการนำค่าสถิติมาวาดกราฟแสดงผล	18
4. 1 ค่าสถิติก่อนการตรวจสอบ Found	20
4. 2 ค่าสถิติก่อนการตรวจสอบ Requests.....	20
4. 3 ค่าสถิติก่อนการตรวจสอบ Rejects.....	21
4. 4 ค่าสถิติก่อนการตรวจสอบ Authntication	22
4. 5 หน้าจอ Login สำหรับการเข้าใช้งานระบบ	22
4. 6 เลือเมนู Graphs.....	23
4. 7 เลือเงื่อนไขที่ต้องการ	23
4. 8 ตัวอย่างผลการทดสอบ Found.....	23
4. 9 ตัวอย่างผลการทดสอบ Requests	24
4. 10 ตัวอย่างผลการทดสอบ Reject.....	24
4. 11 ตัวอย่างผลการทดสอบ Authentication.....	25

บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญ

ปัจจุบันการให้บริการอินเทอร์เน็ตขององค์กรที่ให้บริการอินเทอร์เน็ต (Internet Service Provider : ISP) มีหลายรูปแบบเช่น Leased line, FTTX และ ADSL ในส่วนของ LeasedLine Internet จะทำการ Fixed-IP ให้ผู้ใช้บริการ แต่ FTTX , ADSL จะไม่มีการ Fixed-IP (Dynamic-IP) ในองค์กรที่ให้บริการอินเทอร์เน็ตที่มีไอพีในจำนวนมากๆ ซึ่งได้ทำการแจกจ่ายให้กับผู้ใช้บริการอินเทอร์เน็ตไปนั้น ผู้ใช้บริการมักไม่ทราบว่าคอมพิวเตอร์ของตัวเองนั้นมีไวรัสอยู่โดยในบางเครื่องที่มีไวรัสอยู่นั้นจะมีการส่งจดหมายขยะ (Spam Mail) ออกมาทำให้เกิดความเสียหายกับผู้ใช้บริการ, ผู้ให้บริการอินเทอร์เน็ต และผู้รับอีเมลปลายทาง สำหรับในส่วนผลกระทบต่อผู้ให้บริการอินเทอร์เน็ต คือ ทำให้ไอพีของผู้ให้บริการอินเทอร์เน็ตติดอยู่ใน Spam Blacklist ซึ่งส่งผลให้ไอพีเหล่านี้ไม่สามารถส่งอีเมลไปยังปลายทางได้ หากมีจำนวนไอพีที่ติด Blacklist มาก ๆ ส่งผลให้ไอพีติด Spam Blacklist และอาจส่งผลให้ไอพีอื่นๆที่อยู่ใน Subnet เดียวกัน หรือ AS Number เดียวกันส่งอีเมลออกไม่ได้

โปรโตคอลที่ใช้ในการรับ-ส่งอีเมลคือ SMTP Protocol ซึ่งโดยปกติแล้ว SMTP Protocol ถูกออกแบบเพื่อใช้สำหรับการส่งอีเมลจากผู้ส่งไปยัง SMTP Server ต้นทางผ่านเครือข่ายอินเทอร์เน็ตไปยัง SMTP Server ของผู้รับปลายทางโดยผู้ใช้บริการสามารถส่งเมลไปยังผู้รับอื่นๆได้ทั่วโลก แต่อีเมลที่ส่งเข้าที่ SMTP Server ต้นทางมักมีอีเมลขยะส่งเข้ามาเสมอ ดังนั้นจึงมีความจำเป็นต้องกรองอีเมลขยะก่อนที่จะส่งไปยัง SMTP Server ปลายทาง ซึ่งโดยปกติแล้ว SMTP Server ต้นทาง จะอนุญาตให้ผู้ใช้ที่ Authenticate ผ่าน หรือ Source IP อยู่ในช่วงที่อนุญาตให้ส่งอีเมลได้เท่านั้น

สแปมเมอร์จะไม่สามารถส่งอีเมลผ่าน SMTP Server ต้นทางได้ เพราะอีเมลที่ส่งมักมีการปลอม Sender Address และสแปมเมอร์ไม่ทราบ Username และ Password สำหรับใช้ Authentication กับ SMTP Server ต้นทาง หรือ Source IP ที่ใช้ส่งไม่ได้อยู่ในช่วงที่อนุญาตให้ส่งผ่าน SMTP Server ต้นทางได้ ดังนั้นสแปมเมอร์จะแก้ปัญหานี้โดยการทำตัวเป็น SMTP Server ต้นทางเสียเอง และส่งอีเมลไปยัง SMTP Server ปลายทางโดยตรง ซึ่งจะส่งผลให้ไอพีที่ผู้ให้บริการอินเทอร์เน็ตแจกจ่ายให้ลูกค้าติด Spam Blacklist ซึ่งผู้ให้บริการอินเทอร์เน็ตหลายๆราย จะแก้ปัญหานี้โดยการปิดกั้นไม่ให้ลูกค้าส่งอีเมลออกไปยัง SMTP Server ต้นทางโดยตรง แต่บังคับให้ส่งผ่าน SMTP Gateway ของผู้ให้บริการอินเทอร์เน็ตเท่านั้น

เมื่อผู้ให้บริการอินเทอร์เน็ตบังคับให้ลูกค้าส่งอีเมลผ่าน SMTP Gateway ของผู้ให้บริการ เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาดูเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

อินเทอร์เน็ตเท่านั้น อีเมลที่ส่งผ่านจึงมีทั้งที่มาจาก Source IP ที่เป็น Dynamic และ Static แต่เมื่อผู้ให้บริการอินเทอร์เน็ตตรวจพบอีเมลขยะจาก Source IP ที่เป็น Dynamic IP กลับไม่สามารถปิดกั้นการส่งอีเมลจาก Source IP ได้เนื่องจากผู้ให้บริการรายนั้นใช้ไอพีที่เปลี่ยนแปลงได้ และ SMTP Gateway ไม่มีความสามารถในการปิดกั้นการส่งจาก ADSL Account

แม้ว่าการแก้ปัญหาโดยการบังคับให้ส่งอีเมลทั้งหมดผ่านทาง SMTP Gateway ของผู้ให้บริการอินเทอร์เน็ต จะสามารถแก้ปัญหาไอพีที่แจกจ่ายให้ผู้ให้บริการติด Blacklist ได้ แต่พบว่าไม่สามารถแก้ปัญหาไอพีของ SMTP Gateway ของผู้ให้บริการอินเทอร์เน็ตติด Blacklist ได้

ปัญหานี้สามารถแก้ไขให้หมดไปได้โดยวิธีการ แยกประเภทลูกค้าโดยอนุญาตให้ลูกค้าแบบ Static IP เท่านั้นที่จะสามารถส่งอีเมลผ่าน SMTP Gateway ของผู้ให้บริการได้ ส่วนลูกค้าประเภท Dynamic IP อนุญาตให้ส่งไปยัง SMTP Server ด้านทางแบบมีเงื่อนไข โดยการทำ SMTP Authentication เพราะมีเพียงผู้ส่งตัวจริงเท่านั้นที่สามารถทำได้ แต่สแปมเมอร์ไม่สามารถทำได้

สำหรับบริการส่งอีเมลผ่าน SMTP Sever ด้านทางนั้นมีทั้งที่มาจากผู้ให้บริการอีเมลในอินเทอร์เน็ต เช่น Hotmail, Yahoo, Google หรือผู้ดูแลระบบอีเมลของบริษัท โดยผู้ให้บริการอีเมลจะแจ้งให้ผู้ใช้บริการอีเมลทราบวิธีการตั้งค่า เพื่อใช้งานทั้งจากอีเมลไคลเอนต์และเว็บเมล

1.2 ความมุ่งมั่นและวัตถุประสงค์ของการศึกษา

- 1.2.1 เพื่อศึกษาการทำงานของการทำงานของการส่งอีเมลโดยใช้ SMTP Protocol
- 1.2.2 เพื่อศึกษาปัญหาที่มีผลกระทบต่อการส่งและรับอีเมล ในเรื่องวิธีป้องกันไม่ให้ไอพีของผู้ให้บริการผู้ให้บริการอินเทอร์เน็ตติด Blacklist
- 1.2.3 เพื่อศึกษาและทำการเปรียบเทียบความแตกต่างแตกต่างระหว่าง SMTP Proxy ต่างจาก Mail Server อย่างไร
- 1.2.4 เพื่อศึกษาปัญหาและแนวทางการเพิ่มประสิทธิภาพการให้กับผู้ให้บริการอินเทอร์เน็ต
- 1.2.5 เพื่อศึกษาวิธีการป้องกัน Virus และ Spam และการปลอมแปลง Sender E-mail โดยไม่ผ่านการ Authentication
- 1.2.6 เพื่อเพิ่มประสิทธิภาพการทำงานของ SMTP ให้มีประสิทธิภาพยิ่งขึ้น

1.3 ขอบเขตของการพัฒนาระบบ

สร้างระบบป้องกันไอพีของผู้ให้บริการอินเทอร์เน็ตติด Blacklist เพื่อแก้ไขปัญหาของการติด Blacklist ของผู้ให้บริการอินเทอร์เน็ตภายในองค์กรและเปรียบเทียบถึงความแตกต่างระหว่างก่อนหน้าและหลังมีการใช้ระบบเพื่อวัดประสิทธิภาพการทำงานของระบบ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

1.4 นิยามศัพท์เฉพาะ

Internet Service Provider (ISP) หรือผู้ให้บริการอินเทอร์เน็ตคือบริษัทที่ให้ลูกค้าสามารถเข้าถึงอินเทอร์เน็ตโดยผู้ให้บริการจะเชื่อมโยงลูกค้าเข้ากับเทคโนโลยีรับส่งข้อมูลที่เหมาะสมในการส่งผ่านอุปกรณ์โปรโตคอลอินเทอร์เน็ตอย่างเช่น โคอัล, ดีเอสแอล, เคเบิลโมเด็ม, อินเทอร์เน็ตไร้สายหรือการเชื่อมต่อระบบโฮสติ่งผู้ให้บริการอินเทอร์เน็ตอาจให้บริการเปิดบัญชีชื่อผู้ใช้ในอีเมลติดต่อสื่อสารกับผู้อื่นโดยรับ-ส่งผ่านเซิร์ฟเวอร์ของผู้ให้บริการ ในบางครั้งผู้ให้บริการทางอินเทอร์เน็ตอาจให้บริการเก็บไฟล์ข้อมูลระยะไกล รวมถึงเรื่องเฉพาะทางอื่นๆ เป็นต้น

Simple Mail Transfer Protocol (SMTP) คือโปรโตคอลแบบTCP/IPที่ใช้ในการส่งอีเมลในเครือข่ายอินเทอร์เน็ตไปยังเครื่องบริการอื่นๆซึ่งสามารถส่งเมลไปยังผู้ใช้ได้ทั่วโลกมีข้อจำกัดในเรื่องของความสามารถในการส่งอีเมลว่าสามารถทำได้แบบเป็นคิวเท่านั้น และ SMTP ส่วนใหญ่จะไม่ยอมให้คนภายนอกองค์กร หรือไอพีที่อยู่ภายนอกองค์กรใช้งาน SMTP

Leased Line เป็นเครือข่ายส่วนบุคคลใช้สำหรับการติดต่อสื่อสารด้วยเทคโนโลยีใยแก้วนำแสงรับ-ส่งสัญญาณ ภาพเสียงและข้อมูลระหว่างสถานที่ 2 แห่ง สามารถติดต่อถึงกันได้อย่างรวดเร็ว แม่นยำและปลอดภัยจากการละเมิดข้อมูลและยังสามารถเลือกใช้ความเร็วในการรับ-ส่งได้ตามความต้องการและลักษณะการใช้งานตั้งแต่ความเร็ว 9.6 Kbps จนถึงความเร็ว 155 Mbps ตามมาตรฐานของ ITU โดยมีศูนย์ควบคุมการทำงานของโครงข่ายด้วยระบบคอมพิวเตอร์

1.5 แนวทางการศึกษา

ศึกษาการทำงานของโปรโตคอลหลักๆที่ใช้ในการรับ-ส่งอีเมล คือ SMTP มาเพื่อวิเคราะห์หลักการทำงาน จุดเด่นและจุดด้อยของโปรโตคอล เพื่อที่จะนำ Filter ต่างๆที่มีส่วนช่วยในการเพิ่มประสิทธิภาพของ SMTP เพิ่มเข้าไปเพื่อลดจุดด้อยของ SMTP Proxy ให้มีประสิทธิภาพในการใช้งานมากยิ่งขึ้น รวมทั้งวิธีการป้องกัน Spam และไวรัสต่างๆ

1.6 ผลที่คาดว่าจะได้รับ

1.6.1 แก้ปัญหาไอพีของผู้ให้บริการอินเทอร์เน็ตติดBlacklist

1.6.2 แก้ปัญหาในการปลอม Sender E-mail เนื่องจากต้อง Authentication ทุกครั้งก่อนที่จะเริ่มใช้งาน

1.6.3 แก้ปัญหา Queue ค้างเพราะว่า SMTP Proxy ต่างจาก Mail Server เนื่องจาก SMTP Proxy มีการตรวจสอบ SMTP Conversation ทีละคำสั่งจึงสามารถตรวจสอบได้ตั้งแต่ก่อนที่จะมีการส่งอีเมลสมบูรณ์ทั้งฉบับแต่ Mail Server ต้องรับอีเมลมาก่อนทั้งฉบับก่อนแล้วถึงจะตรวจสอบ จึงทำให้เกิดปัญหาเรื่อง Disk และ Queue อยู่

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 2

เอกสารและงานวิจัยที่เกี่ยวข้อง

ในการศึกษาเพื่อทำระบบป้องกันไอพีของผู้ให้บริการอินเทอร์เน็ตคิดบัญชีค่า กรณีศึกษา บริษัท ทีทีเอ็นเคที จำกัด (มหาชน) ในครั้งนี้ได้แนวคิดและทฤษฎีในการวิจัยที่เกี่ยวข้องทั้งหมด ดังนี้

- 2.1 แนวคิดเกี่ยวกับโปรโตคอล SMTP
- 2.2 แนวคิดเกี่ยวกับการป้องกัน E-mail Virus และ E-mail Spam
- 2.3 แนวคิดเกี่ยวกับความแตกต่างระหว่าง SMTP Proxy และ Mail Server
- 2.4 ศึกษาผลกระทบและปัญหาขององค์กรผู้ให้บริการ
- 2.5 เครื่องมือที่ใช้ในการพัฒนาระบบ

2.1 แนวคิดเกี่ยวกับโปรโตคอล SMTP

Simple Mail Transfer Protocol (SMTP) เป็นมาตรฐานในการส่งจดหมายระหว่างเครื่อง Host ต่างๆ บน TCP/IP Protocol ซึ่งกำหนดอยู่ใน RFC 821 เป็นโปรโตคอลที่คู่กับ POP3 เพราะเป็นโปรโตคอลที่ใช้ส่งอีเมลล์จาก User Agent ของผู้ส่งไปยัง MTA ของผู้ส่งและส่งต่อไปยัง MTA เครื่องอื่นๆที่เป็นจุดผ่านในการเชื่อมต่อไปยังเครื่องของผู้รับ โปรโตคอล SMTP จะทำงานร่วมกับ โปรโตคอล TCP โดยใช้พอร์ต 25 โดยโปรโตคอล SMTP จะทำหน้าที่ในการส่งอีเมลล์และ โปรโตคอล POP3 จะทำหน้าที่ในส่วนของการรับอีเมลล์ของผู้ใช้บริการ

SMTPที่ใช้ในการส่งจดหมายนั้นได้พัฒนาขึ้นมาทำงานบน TCP/IP เพื่อความสะดวกในการรับ-ส่งอีเมลล์เป็นหลัก ทำให้การทำงานในส่วนของการรักษาความปลอดภัยน้อยกลายเป็นช่องโหว่ให้เกิดการส่งสแปมขึ้นจึงต้องมี Service อื่นๆเข้ามาช่วยในการจัดการการรับ-ส่งอีเมลล์และในการส่งอีเมลล์ของโปรโตคอล SMTP นั้นจะใช้วิธีอ้างอิงเซิร์ฟเวอร์อื่นๆตาม DNS (Domain Name System) เช่นเดียวกับระบบอื่นๆในอินเทอร์เน็ตและยังสามารถส่งอีเมลล์ไปยังผู้รับคนเดียวหรือหลายคนพร้อมกันได้ด้วย

องค์ประกอบที่สำคัญของ SMTP มีดังต่อไปนี้

1. Message User Agent (MUA) คือ โปรแกรมที่ติดต่อกับผู้ใช้บริการในการส่งอีเมลล์ ซึ่งเมื่อผู้ใช้บริการได้เขียนเนื้อหาอีเมลล์ที่ต้องการเรียบร้อยแล้ว โปรแกรมจะทำการจัดรูปแบบของข้อมูล และส่งออกไปยัง MTA ด้วยโปรโตคอล SMTP

2. Message Transfer Agent (MTA) คือ เซิร์ฟเวอร์ซึ่งทำหน้าที่เป็นตัวกลางรับข้อมูลเนื้อหาของจดหมายที่มาจาก MUA หรือ MTA เดียวกันก็ได้ และทำการส่งต่ออีเมลล์เหล่านั้นไปยัง

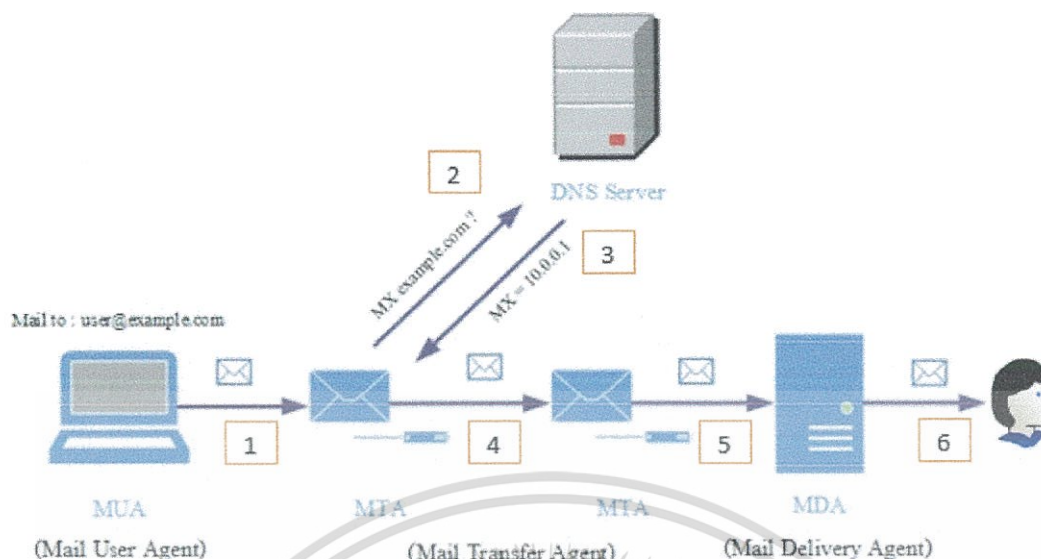
เอกสารนี้เป็นเอกสารที่สงวนลิขสิทธิ์สำหรับการใช้งานเพื่อการศึกษาเท่านั้น เมื่อผู้ใช้ได้พิมพ์เอกสารนี้ไปใช้โดยไม่ได้รับอนุญาต ถือว่าผิดกฎหมาย และหากมีการนำเอกสารนี้ไปใช้โดยไม่ได้รับอนุญาต ผู้ใช้จะต้องรับผิดชอบต่อเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ปลายทางที่กำหนดไว้ คือ MTA ของอีเมลปลายทางเพราะฉะนั้น MUA ต้องทราบว่าจะใช้เซิร์ฟเวอร์ใดเป็น MTA เพราะโปรแกรมไคลเอนต์ที่เป็น MUA ไม่สามารถส่งอีเมลออกไปยังปลายทางได้เอง

3. Message Delivery Agent (MDA) คือเซิร์ฟเวอร์ที่เป็นตัวเก็บเมลบ็อกซ์ของผู้ใช้งาน ทำหน้าที่รับจดหมายที่เข้ามาโดยโปรโตคอล SMTP และทำหน้าที่ในการตรวจสอบว่ามีเมลบ็อกซ์ (Mailbox) ของผู้ใช้ตรงตามที่ระบุในอีเมลหรือไม่ หากไม่ตรงกันก็จะแจ้งข้อผิดพลาด (Error) กลับไป แต่ถ้ามีเมลบ็อกซ์ตรงตามที่กำหนดจะรับจดหมายเข้ามาและนำไปเก็บยังเนื้อหาที่จัดสรรไว้สำหรับเมลบ็อกซ์นั้น และรอให้เจ้าของเมลบ็อกซ์มาเปิดอ่านต่อไป หรือจะเรียก MDA ว่าเป็นเมลเซิร์ฟเวอร์ที่มีไว้เก็บเมลบ็อกซ์ของผู้ใช้นั่นเอง

จากองค์ประกอบทั้ง 3 ส่วนที่กล่าวมาข้างต้นมีความสัมพันธ์ในกระบวนการส่งอีเมลของโปรโตคอล SMTP ดังแสดงรูปที่ 2.1 ซึ่งมีขั้นตอนดังนี้

1. ผู้ใช้อีเมลเขียนจดหมายบนโปรแกรมเมลไคลเอนต์ MUA เพื่อส่งไปยังอีเมลแอดเดรสปลายทาง จดหมายจะถูกส่งไปยัง MTA เพื่อให้ MTA ส่งต่อไปยังปลายทาง
2. MTA ได้รับจดหมายมาจากผู้ใช้บริการโปรโตคอล SMTP ทำการตรวจสอบโดเมนปลายทาง และสอบถาม DNS ว่าหากต้องการส่งอีเมลไปยังโดเมน example.com นั้นจะต้องส่งไปยัง MTA ไหน โดยภายใน DNS จะมีการกำหนด mx record เอาไว้
3. DNS จะตอบกลับมาเป็นไอพีแอดเดรสหรือชื่อโฮสต์ของเซิร์ฟเวอร์ที่ระบุอยู่ใน mx record กลับมายัง MTA
4. MTA จัดการส่งอีเมลออกไปยัง MTA ที่ DNS ระบุไว้
5. MTA ของโดเมน example.com ได้รับอีเมลเข้ามาและทำการตรวจสอบ ถ้าตรวจสอบแล้วพบว่าเป็นของโดเมนตัวเอง ก็จะทำการค้นหาต่อไปว่าชื่อผู้รับที่อยู่ในอีเมลนั้นเก็บไว้บน MDA ไດและส่งไปยัง MDA นั้นๆ
6. MDA เมื่อได้รับจดหมายเข้ามาก็จะทำการตรวจสอบชื่อผู้รับ และนำจดหมายไปเก็บยังเมลบ็อกซ์ของผู้รับ



รูปที่ 2.1 กระบวนการส่งอีเมลล์ของโปรโตคอล SMTP

2.2 แนวคิดเกี่ยวกับการป้องกัน E-mail Virus และ E-mail Spam

2.2.1 อีเมลไวรัส (E-mail Virus) คืออีเมลที่ถูกส่งเข้ามาด้วยความจงใจหรือไม่เจาจงซึ่งมีการพัฒนาและแพร่หลายอย่างต่อเนื่อง อาจพบไวรัสชนิดใหม่แทบทุกเดือนโดยมีความประสงค์ที่จะทำให้คอมพิวเตอร์ของคุณมีไวรัสเมื่อทำการเปิดคลิกไฟล์แนบที่ผู้ส่งนั้นส่งมา, ในบางกรณีเรายังพบว่า Hacker ได้ทำการสร้างอีเมลที่มีไวรัสและทำการแนบไฟล์โดยเฉพาะ ".exe" และทำการบีบอัดไฟล์ (ZIP File) เพื่อหลบหลีกการตรวจสอบของ E-Mail Hosting บางกรณี Hacker อาจจะมีการส่งอีเมลโดยมีการแนบ URL หรือ Website เพราะต้องการหลบหลีกการตรวจสอบของ Firewall E-Mail Hosting เพื่อหลอกให้คุณกดเข้าไปดาวน์โหลดไวรัสลงในเครื่องคอมพิวเตอร์ โดยไวรัสที่ Hacker จงใจส่งเข้ามาผ่านทางอีเมลนั้นจะมีจุดประสงค์หลักคือ โจรกรรมข้อมูล (Hack) เพื่อเอาข้อมูลที่เป็นความลับ หรือข้อมูลที่สำคัญทางธุรกิจของคุณไปใช้ในเชิงมิชอบ เช่น Username, Password ของอีเมลไปปลอมแปลงและสร้างเอกสารเลขบัญชีปลอมขึ้นมาซึ่งเป็นกรณีที่พบได้บ่อยมาก ทำให้เกิดความเสียหายต่อตัวเองและต่อธุรกิจได้ ช่องทางการแพร่กระจายของไวรัสจะอาศัยอีเมลและอินเทอร์เน็ตเป็นช่องทางหลัก การทำงานของไวรัสจะอยู่ในระดับแอปพลิเคชันเลเยอร์ (Application Layer) อาศัยการ Executed คำสั่งของผู้ใช้และระบบปฏิบัติการเป็นหลัก ไวรัสจะเกี่ยวข้องกับอินเทอร์เน็ตและไฟร์วอลล์ (Firewall) คือ ไวรัสจะอาศัยอินเทอร์เน็ตเป็นทางผ่านเท่านั้น หากไวรัสแพร่ระบาดโดยที่เราไม่เฝ้าระวังไว้อยู่และกำหนดให้ไฟร์วอลล์อนุญาตให้มีทราฟฟิกเพื่อการรับ-ส่งอีเมลได้ ไวรัสจะสามารถผ่านเข้ามาได้ในช่องทางเดียวกัน ไฟร์วอลล์ไม่สามารถป้องกันไวรัสได้เพราะการทำงานของไฟร์วอลล์อยู่คนละส่วนกัน ไฟร์วอลล์เป็นเพียงเครื่องมือในการป้องกันระดับเน็ตเวิร์กเลเยอร์ (Network Layer) ที่คอยควบคุมทราฟฟิกเป็นหลัก ซึ่งทำงานอยู่เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ในเลเยอร์ที่ต่ำกว่าการทำงานของไวรัสทำให้ไฟร์วอลล์รู้จักแต่เฉพาะ TCP, UDP, ICMP, PORT

2.2.2 อีเมลสแปม (E-Mail Spam) คือ ลักษณะของอีเมลที่สร้างความเสียหายแก่เครือข่ายอินเทอร์เน็ตและสร้างความเดือดร้อนให้แก่ผู้ใช้บริการอินเทอร์เน็ตนั้นแบ่งออกเป็นประเภทใหญ่ ๆ ได้สองประเภท คือ Chain Mail หรือจดหมายลูกโซ่ และ Spam Mail หรือการโจมตีด้วยอีเมล

1. Chain Mail หรือจดหมายลูกโซ่นั้นจะมีเนื้อหาเหมือนจดหมายทั่วไปแต่จะมีเนื้อหาเกี่ยวกับคำเตือนเรื่องไวรัส หรือเรื่องอื่น ๆ ให้ส่งต่อให้กับคนที่รู้จัก หากมีคนส่งต่อกันเป็นจำนวนมากส่งผลให้ Mail Server ของผู้ให้บริการอินเทอร์เน็ตเสียหายเกิด Server Down หรือทำงานช้าลง นอกจากนี้ยังเป็นตัวการทำให้ทราฟฟิกของเครือข่ายอินเทอร์เน็ตเกิดการติดขัดในส่วนของผู้ใช้บริการอินเทอร์เน็ตนั้น การได้รับอีเมลประเภทนี้บ่อย ๆ จะเกิดความรำคาญได้ ดังนั้นผู้ใช้บริการต้องหยุดการส่งอีเมลประเภทนี้เพื่อหยุดวงจรลูกโซ่

2. สแปมเมล (Spam Mail) หรืออีเมลขยะที่ได้รับมาโดยผู้ใช้อีเมลไม่ต้องการจำนวนมาก ๆ ในครั้งหนึ่ง หรือการทยอยส่งแต่ส่งจำนวนหลายฉบับ อาจจะเป็นโฆษณาชวนเชื่อ และไม่สามารถติดตามผู้ส่งตัวจริงได้ อาจจะไม่เป็นอันตรายมากแต่จะส่งผลกระทบต่อในเรื่องของความรำคาญให้แก่ผู้รับ และทำให้ประสิทธิภาพของการใช้ระบบอีเมลลดน้อยลงและสิ้นเปลืองทรัพยากรเพื่อจัดการกับอีเมลขยะพวกนี้ สำหรับวัตถุประสงค์นั้นมีหลากหลาย ตั้งแต่โฆษณาสินค้าการโจมตีระบบ การแกล้งแค้นส่วนตัว การกลั่นแกล้ง เป็นต้น ซึ่งผู้ใช้อีเมลอาจจะได้รับผลกระทบใน 2 กรณีดังต่อไปนี้

กรณีแรก ในฐานะเป็นผู้รับอีเมลผู้ส่งอีเมลเป็นคนที่ผู้รับอีเมลไม่เคยรู้จักมาก่อน แต่ได้ส่งอีเมลมาให้ผู้รับ โดยตรงโดยที่ผู้รับอีเมลไม่ต้องการรับอีเมลฉบับนั้นเลย จากนั้นผู้รับอีเมลต้องมาตามลบอีเมลฉบับนั้นๆทิ้งไป

กรณีที่สอง ในฐานะที่ถูกใช้เป็นตัวกลางในการส่งต่ออีเมลเป็นการส่งผลกระทบต่อเฉพาะกับเมลเซิร์ฟเวอร์เท่านั้น เนื่องจากเมลเซิร์ฟเวอร์กำหนดค่าไว้ไม่เหมาะสม ทำให้สามารถโดนถูกใช้เป็นตัวกลางในการกระจายอีเมลขยะ ไปหาผู้ใช้อีเมลอื่นๆได้

2.3 แนวคิดเกี่ยวกับความแตกต่างระหว่าง SMTP Proxy และ Mail Server

Mail Server คือเครื่องคอมพิวเตอร์ที่ให้บริการในการรับส่งเมลให้กับบุคคลหรือองค์กร โดยที่ Mail Server จะตั้งอยู่ที่ผู้ให้บริการอินเทอร์เน็ตหรือภายในองค์กร หรือแม้กระทั่งที่พักส่วนบุคคลก็ได้ ตัวอย่างผู้ให้บริการเมลที่เป็นที่รู้จักได้แก่ Hotmail.com, Gmail.com สำหรับการที่องค์กรมี Mail Server เป็นของตนเองจะมีประโยชน์ คือความสะดวกในการจัดการกล่องข้อความ (Mailbox) ของผู้ใช้บริการแต่ละคนในด้านความปลอดภัยและปริมาณเนื้อที่จัดเก็บข้อมูลซึ่งสามารถเพิ่มได้โดยไม่จำกัดการทำงานของการทำงานการรับส่งเมลนั้น จะประกอบไปด้วย 2 ส่วนหลักคือ Mail Server

และ Mail Client เมื่อผู้ใช้บริการต้องการใช้เมลจะต้องใช้งานผ่าน Mail Client ซึ่งอาจอยู่ในรูปแบบเอกสารและเอกสารเมื่อผู้ใช้บริการต้องการใช้เมลจะต้องใช้งานผ่าน Mail Client ซึ่งอาจอยู่ในรูปแบบเอกสารและไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

แอปพลิเคชันหรือเว็บแอปพลิเคชัน เมื่อผู้ใช้บริการทำการส่งอีเมลข้อมูลอีเมลจะถูกส่งจากไปยัง Mail Server ส่วนในกรณีที่ผู้ใช้ต้องการอ่านอีเมล ผู้ใช้บริการเพียงอ่านข้อมูลผ่านทางกล่องข้อความของ Mail Server สำหรับกรณีที่ส่งอีเมลข้ามกลุ่มหรือองค์กรเช่น ต้องการส่งจากอีเมล Hotmail.com ไปยัง Yahoo.com จะคล้ายหลักการส่งอีเมลเหมือนที่กล่าวมาข้างต้น เพียงแต่อีเมลที่ส่งไปยัง Mail Server ของ Hotmail จะถูกส่งผ่านไปยัง Mail Server ของ Yahoo อีกครั้งหนึ่ง

นอกจาก Mail Server และ Mail Client แล้วยังมีส่วนที่สำคัญอีกอย่าง คือ DNS Server ซึ่งจะต้องจัดเก็บข้อมูล Public-IP และ URL ของ Mail Server ทำให้ Mail Client ส่งข้อมูลไปยัง Mail Server ได้อย่างถูกต้องและใช้โปรโตคอล SMTP ในการส่งเมลไปยังกล่องข้อความของผู้รับปลายทางที่ Mail Server ซึ่งในบางครั้งเครื่องที่ให้บริการในส่วนนี้จะเรียกว่า SMTP Server ซึ่งในกรณีที่ส่งอีเมลต่างกลุ่มหรือต่างองค์กร อีเมลจะมีการส่งต่อระหว่าง SMTP Server นั้นเอง

Simple Mail Transfer Protocol Server หรือ SMTP Server คือเครื่องบริการส่งอีเมลไปยังเครื่องบริการอื่น ๆ เพราะปกติผู้ใช้อินเทอร์เน็ตมักจะประสบปัญหาในการส่งอีเมลเมื่อเชื่อมต่ออินเทอร์เน็ตของผู้ให้บริการรายหนึ่ง แต่ใช้อีเมลของผู้ให้บริการอินเทอร์เน็ตอีกรายหนึ่ง ทำให้ไม่สามารถส่งอีเมลไปยังปลายทางได้จะเกิดข้อผิดพลาดในขณะที่ทำการส่ง หรือมีอีเมลตีกลับ โดยแจ้งข้อความเช่น Relaying denied ที่เป็นเช่นนี้เพราะผู้ให้บริการอินเทอร์เน็ตจะอนุญาตเฉพาะผู้บริการที่ใช้เครือข่ายของตนเท่านั้นส่งอีเมลผ่าน SMTP Server ของตนเองได้ แต่จะไม่อนุญาตให้ผู้บริการจากเครือข่ายรายอื่น ถึงแม้ว่าผู้บริการจะใช้อีเมลของตนเองก็ไม่สามารถส่งอีเมลผ่าน SMTP Server ของตนได้ ทั้งนี้เพื่อป้องกันผู้ไม่ประสงค์ดีเข้ามาใช้อีเมลเซิร์ฟเวอร์ของตนในการส่งสแปมหรืออีเมลที่ไม่พึงประสงค์ออกไปซึ่งจะทำให้ SMTP ติด Blacklist ทำให้ผู้บริการไม่สามารถส่งอีเมลไปถึงผู้รับรายอื่น ๆ ได้ แต่ว่า SMTP มี Feature Authentication เพื่ออำนวยความสะดวกให้แก่ผู้บริการอีเมลสามารถส่งอีเมลจากนอกเครือข่ายได้ หากผู้บริการต้องการจะส่งอีเมลผ่าน SMTP Server นี้จะต้องผ่านกระบวนการพิสูจน์สิทธิ์ก่อน นั่นคือ ต้อง Authentication ในการส่งอีเมลก่อนทุกครั้ง ในปัจจุบันโปรแกรมมีอีเมลเวอร์ชันใหม่ ๆ ที่สนับสนุนระบบ SMTP Authentication กันหมดแล้ว จึงไม่ใช่เรื่องยากที่จะทำการตั้งค่า SMTP Authentication สำหรับ E-mail Client SMTP Proxy เข้ามาช่วยเสริมความสามารถ ทำให้แก้ปัญหาหลักๆ ของระบบงานแบบเดิมได้ 3 เรื่อง

1. แก้ปัญหา IP ของผู้ให้บริการติด Blacklist
2. แก้ปัญหาในการปลอม Sender E-mail เนื่องจากต้อง Authentication ทุกครั้ง
3. แก้ปัญหา Queue ค้างเพราะว่า SMTP Proxy ต่างจาก Mail Server เนื่องจาก SMTP

Proxy มีการตรวจสอบ SMTP Conversation ที่ละคำตั้งจึงสามารถตรวจสอบได้ตั้งแต่ก่อนที่จะมีการถูกส่งอีเมลสมบูรณ์ทั้งฉบับแต่ Mail Server ต้องรับอีเมลมาก่อนทั้งฉบับแล้วค่อยตรวจสอบจึงทำให้เกิดปัญหาเรื่อง Disk Queue อยู่

เอกสารนี้เป็นเอกสารที่สงวนลิขสิทธิ์ไว้เพื่อใช้ในการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.4 ศึกษาผลกระทบและปัญหาขององค์กรผู้ให้บริการอินเทอร์เน็ต

ผลกระทบที่มีต่อผู้ให้บริการอินเทอร์เน็ตการทำระบบป้องกันไอพีของผู้ให้บริการติด Blacklistเนื่องจากการให้บริการอินเทอร์เน็ตขององค์กรที่ให้บริการอินเทอร์เน็ตมีหลายแบบเช่น Leased Line , FTTX และ ADSL ในส่วนของ Leased Line Internet จะทำการ Fixed-IP แต่ FTTX , ADSL จะไม่มีการ Fixed-IP (Dynamic-IP) จึงทำให้ผู้พัฒนาถึงเห็นว่าองค์กรที่ให้บริการอินเทอร์เน็ตที่มีไอพีเยอะมากๆ และได้แจกจ่ายให้กับผู้ใช้บริการอินเทอร์เน็ตแต่ผู้ใช้บริการส่วนใหญ่ไม่ทราบว่าคอมพิวเตอร์ของตัวเองนั้นมีไวรัสอยู่หรือไม่โดยในบางเครื่องที่มีไวรัสอยู่นั้นจะมีการส่งสแปมเกิดขึ้นและทำการโจมตี รวมถึงการรบกวนผู้อื่นทำให้เกิดความเสียหายต่าง ๆ อาจส่งผลกระทบโดยการโดน Block-IP เนื่องจากไอพีติด Blacklist และถ้าติด Blacklist มากขึ้นเรื่อย ๆ อาจจะโดน Block-IP ทั้ง As Number ซึ่งจะส่งผลกระทบให้ผู้ให้บริการ Static-IP ได้รับผลกระทบด้วยเนื่องจากอยู่ใน As number เดียวกัน

ผู้ให้บริการอินเทอร์เน็ตบางรายแก้ปัญหาโดยการ Block Destination Port 25 และให้ส่งผ่าน Mail Gateway ของผู้ให้บริการแทนแต่ก็ยังมีความปัญหาอื่นตามมาเช่นมีการจงใจส่งสแปมของ Hacker หรือคอมพิวเตอร์พนักงานบริษัทติดไวรัสจะมีการส่งสแปมเกิดขึ้นในจำนวนมากๆ ส่งผลให้ Mail gateway ของผู้ให้บริการเกิด Queue ค้างในจำนวนมาก, User ปลอม Sender E-mail, ไอพีของ Mail Gateway ถูก Block เนื่องจากมีอีเมลบางฉบับที่ Mail Gateway ตรวจสอบไม่พบสแปมทำให้สามารถส่งออกไปยังปลายทางได้ , ทำงานไม่ทัน , รับโทรศัพท์ไม่ไหวจึงเกิด Throughput เยอะส่งผลให้ผู้ให้บริการเปลือง Bandwidth ไปกับสแปมเป็นต้นเหตุให้ Mail Gateway Outgoing เกิดการ Overload ใช้งานไม่ทัน

2.5 เครื่องมือที่ใช้ในการพัฒนาระบบ

เครื่องมือต่างๆเป็นจุดประสงค์หลักของการรวบรวม Open Source เพื่อให้โปรแกรมหรือคุณสมบัติต่างๆใช้งานร่วมกันได้

2.5.1 Linux Server

ลินุกซ์เป็นโปรแกรมคอมพิวเตอร์ประเภทระบบปฏิบัติการตระกูลหนึ่ง เป็นระบบปฏิบัติการประเภท Unix หรือยูนิกซ์โคลนที่ใช้งานบนเครื่อง PC แต่ปัจจุบันไม่ได้ใช้งานบนเครื่อง PC เพียงอย่างเดียวสามารถใช้งานได้บนเครื่อง Server ต่างๆได้ เช่น SUN SPARC เป็นต้น ซอฟต์แวร์ระบบปฏิบัติการลินุกซ์เป็น Open Source ซึ่งสามารถใช้ลินุกซ์ได้โดยไม่ต้องเสียค่าลิขสิทธิ์เป็น Unix เต็มรูปแบบในระบบ Multi User Multi Task คือการใช้งานได้ครั้งละหลายๆคน และทำงานได้ครั้งละหลายๆงานที่มีระบบการติดต่อกับผู้ใช้งานแบบกราฟิกหรือที่เรียกว่า X-Windows เป็นมาตรฐานสนับสนุนโปรโตคอลแบบ TCP/IP, SLIP, PPP, UUCP เป็น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ระบบปฏิบัติการ 32บิตมีประสิทธิภาพสูงมาก ทั้งที่ลินุกซ์เป็นเพียงเคอร์เนล (Kernel) ของระบบปฏิบัติการ ซึ่งจะทำหน้าที่ในด้านของการจัดสรรและบริหารโพรเซสงานการจัดการไฟล์และอุปกรณ์ I/O ต่าง ๆ ใช้งานผ่านทางแอปพลิเคชันและระบบอินเทอร์เน็ตเฟส เช่น Shell หรือ X วินโดวส์

2.5.2 Spam Assassin

Spam Assassin เป็นระบบที่ช่วยคัดกรอง ป้องกันจดหมายขยะหรืออีเมลที่ไม่พึงประสงค์ อีกทั้งยังสามารถกำหนด E-mail White list และ Email Blacklist ซึ่งสามารถระบุชื่ออีเมลหรืออีเมลทั้งหมดที่ถูกส่งมาจากโดเมนใดๆได้

2.5.3 ClamAV

Clam Antivirus (ClamAV) คือ Antivirus สำหรับติดตั้งบนเซิร์ฟเวอร์ที่ใช้ระบบปฏิบัติการ Linux ClamAV เป็นแหล่งเปิด (GPL) เครื่องมือป้องกันไวรัสที่ออกแบบมาสำหรับการตรวจสอบโทรจันไวรัสมัลแวร์และภัยคุกคามที่เป็นอันตรายอื่น ๆ มีประสิทธิภาพสูงเพื่อป้องกันมัลแวร์และป้องกันไวรัสที่เปิดให้ใช้งานมากที่สุดทั่วโลกมีที่อยู่ไอพีเกือบหนึ่งล้านไอพีที่ทำการอัปเดต ClamAV ในแต่ละวันจากมิเรอร์เซิร์ฟเวอร์ 120 แห่งที่ตั้งอยู่ใน 38 ประเทศทั่วโลก ClamAV มีชื่อเสียงทางด้านความเร็วและความแม่นยำจากการใช้งานผ่านโซลูชันด้านความปลอดภัยเครือข่ายและผู้ให้บริการทั่วโลกและในปัจจุบันได้มีการนำไปผนวกรวมกับโซลูชันสำหรับองค์กรชั้นนำต่างๆ ได้แก่ Secure Mail Gateways เพื่อตรวจหาภัยคุกคามที่ฝังตัวอยู่ในระดับลึก เช่น ไวรัส โทรจัน สปายแวร์และมัลแวร์รูปแบบอื่นๆ

2.5.4 SNMP

Simple network management protocols (SNMP) เป็นเซอร์วิสที่ให้ผู้ดูแลระบบสามารถตรวจสอบสถานะของการทำงานหรือจัดการเกี่ยวกับค่าคอนฟิกต่างๆของอุปกรณ์ได้ ซึ่ง SNMP จะมีประโยชน์ในการนำมาใช้มอนิเตอร์การทำงานการวิ่งเข้า-ออกของทราฟฟิกที่ผ่านเครื่อง Linux ที่ทำงานในลักษณะเป็น Gateway โดยใช้ snmpwalk เพื่อใช้ในการตรวจสอบสถานะ

การทำงานของ SNMP เริ่มจากฝั่งไคลเอนต์ต้องส่งคำสั่ง SNMP Request ไปยังอุปกรณ์ที่ได้ทำการเป็นเซอร์วิสของการทำงาน SNMP ไว้แล้วพร้อมทั้งส่ง Community String เข้าไปด้วย จากนั้นอุปกรณ์จะทำการตรวจสอบ Community String ว่าถูกต้องหรือไม่ ถ้าถูกต้องจะส่งข้อมูลต่างๆที่ไคลเอนต์ร้องขอส่งกลับไปยังไคลเอนต์ ส่วนใหญ่ผู้ให้บริการอินเทอร์เน็ตที่ใช้ Linux มาทำเป็น Internet Gateway จะนำ SNMP มาใช้เพื่อตรวจสอบสถานะการทำงานของอุปกรณ์โดยทำการติดตั้ง SNMP บน Server Linux เครื่องนั้น

2.5.5 CACTI

CACTI คือ CACTI Traffic Graph หรือเรียกกันสั้นๆว่า “CACTI” เป็น Open Source Software ซึ่งทำหน้าที่ในการแสดงปริมาณข้อมูลทั้งขาเข้า/ออกในเครือข่ายโดยจะแสดงผลออกมาในรูปแบบของกราฟสามารถเข้าใจและเปรียบเทียบระดับการใช้งานได้ง่ายขึ้น อีกทั้งยังมี

เอกสารเป็นเอกสารที่ลงนามไว้สำหรับใช้เพื่อการศึกษาเท่านั้น เมื่อผู้ใดเห็นประโยชน์ในการนำเอกสารนี้ไปใช้ กรุณาแจ้งให้ทราบถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ประสิทธิภาพเพิ่มขึ้นจาก กราฟในรูปแบบเดิมCACTIเป็น web-based application ประเภทที่ทำงานร่วมกับ RRDTTool สำหรับการสร้างกราฟ เพื่อใช้สำหรับการวิเคราะห์ และติดตามการทำงานของระบบไม่ว่าจะเป็นสถิติด้านการใช้งาน CPU, Memoryจำนวนผู้ใช้บริการในเครือข่าย, จำนวนการเชื่อมต่อข้อมูลภายในเครือข่าย, อัตราการรับ/ส่งข้อมูลผ่านเครือข่าย ซึ่ง CACTIมีความพร้อมและสะดวกในการจัดการเกี่ยวกับเรื่องดังกล่าว และสำหรับ CACTIรุ่นที่มีการปรับปรุงให้สามารถเพิ่มเติมPlug-in ได้ ก็สามารถที่จะเขียน Plug-in หรือดึง Plug-in ที่มีผู้พัฒนาอยู่แล้วมาใช้งานเพิ่มเติมได้อีก เป็นการขยายความสามารถของ CACTIออกไปได้อย่างไม่จำกัด



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 3

ขั้นตอนการพัฒนาและออกแบบระบบ

3.1 วิเคราะห์ระบบงานเดิม

ระบบงานเดิมของ Mail Gateway ของบริษัท ทีทีแอนด์ที จำกัด (มหาชน) คือ ไม่ได้มีการแบ่งแยก User ระหว่าง User ที่เป็นแบบ StaticIP และ DynamicIP ก่อนการศึกษาภาพรวมของระบบงานเดิม ผู้พัฒนาได้ทำการศึกษาความแตกต่างของ IP Address ทั้งสอง

3.1.1 ศึกษา IP Address แบบ Static และ แบบ Dynamic

1. IP Address แบบ Static คือ IP Address ที่ผู้ให้บริการอินเทอร์เน็ตแจก IP Address ให้กับผู้ใช้บริการอินเทอร์เน็ตแต่ละคนอย่างถาวร ทำให้ IP Address เหล่านี้ไม่มีการเปลี่ยนแปลงไม่ว่าจะใช้งานไปนานเท่าไร อย่างไรก็ตาม ถ้ามีการใช้บริการ IP Address แบบ Static IP ไปให้ผู้ให้บริการแล้วถ้า IP address นั้นไม่ได้ถูกใช้งาน จะทำให้สูญเสีย IP address นั้นไปโดยเปล่าประโยชน์ เนื่องจากผู้ให้บริการอินเทอร์เน็ตแต่ละรายมีจำนวน IP Address ที่ให้ใช้งานจำกัดจึงจำเป็นจะต้องทำให้เกิดประโยชน์ให้สูงที่สุดในการใช้งาน

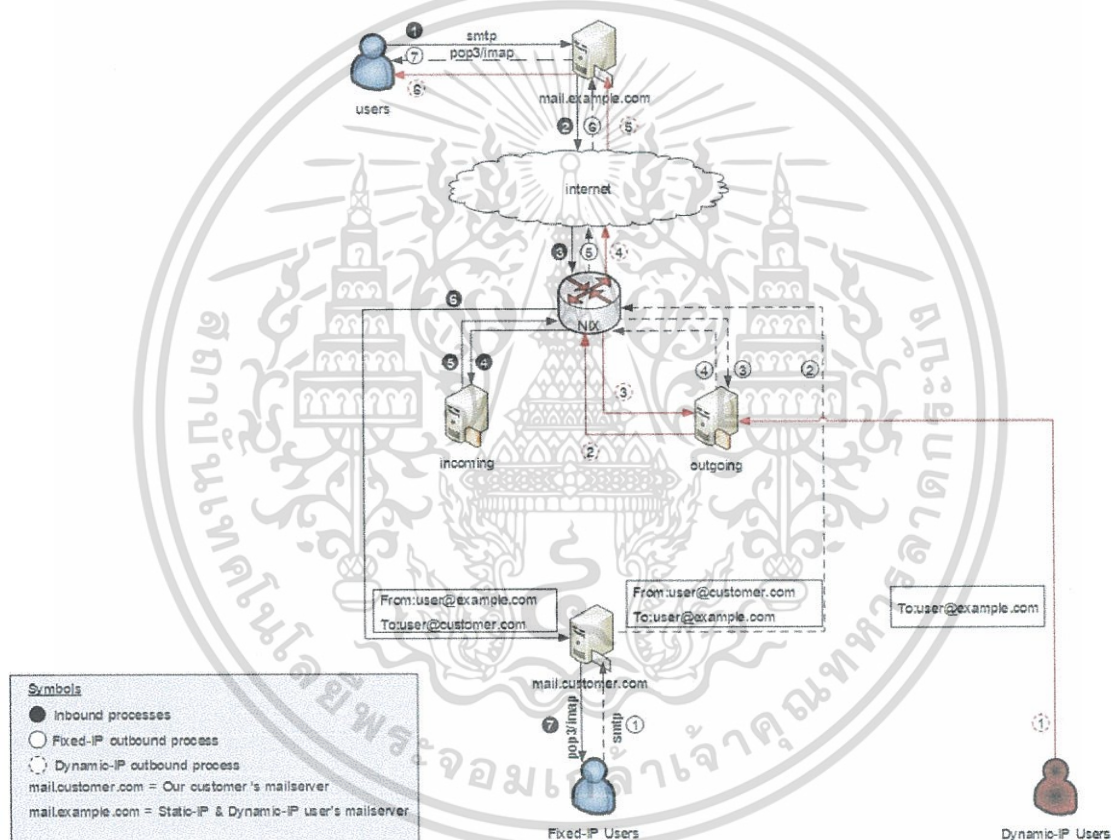
2. IP Address แบบ Dynamic คือ IP Address ที่ทำให้ผู้ให้บริการอินเทอร์เน็ตใช้ประโยชน์จาก IP Address ได้มากที่สุด เนื่องจากระบบ IP address แบบ Dynamic จะทำให้ IP Address ของคอมพิวเตอร์ผู้ใช้บริการอินเทอร์เน็ตแต่ละคนเปลี่ยนแปลงไปตามระยะเวลา ถ้าหาก IP Address ใดไม่ถูกใช้งานก็จะสามารถนำไปแจกต่อให้กับเครื่องคอมพิวเตอร์เครื่องอื่นที่ต้องการใช้งานต่อไปได้ และถ้าคอมพิวเตอร์เครื่องนั้นกลับมาใช้งานก็จะได้ IP Address อันแทนไป ไม่มีการฟิคว่าของ IP Address คายตัวเหมือนกัน IP Address แบบ Static IP

3.1.2 ภาพรวมของระบบงานเดิม

จากที่กล่าวมาข้างต้น บริษัท ทีทีแอนด์ที จำกัด (มหาชน) นั้นไม่มีการแยกแยะระหว่างผู้ใช้บริการแบบ StaticIP และ DynamicIP ทำให้เกิดปัญหาในส่วนของ Leased Line Internet จะทำการ Fixed-IP แต่ว่า FTTX , ADSL จะไม่มีการ Fixed-IP (Dynamic-IP) จึงทำให้ผู้พัฒนามองเห็นว่าองค์กรที่มีไอพีจำนวนมากและได้แจกจ่ายให้กับ User ผู้ใช้บริการอินเทอร์เน็ตแต่ไอพีติด Blacklist มากขึ้นเรื่อยๆ จากการที่ผู้ใช้บริการมักไม่เคยทราบว่าคอมพิวเตอร์ของตัวเองนั้นมีไวรัสอยู่หรือไม่ โดยในบางเครื่องที่มีไวรัสอยู่นั้นจะมีการส่งสแปมเกิดขึ้นและทำการโจมตีและรบกวนผู้อื่นทำให้เกิดความเสียหายต่างๆขึ้นจึงอาจส่งผลกระทบโดยการโดน Block-IP เนื่องจากไอพีติด Blacklist และถ้าติด Blacklist มากขึ้นจนโดน Block IP นั้นไปหรืออาจโดนทั้ง As Number ซึ่งอาจจะส่งผลกระทบต่อผู้ใช้บริการ Static IP ได้รับผลกระทบด้วยเนื่องจากอยู่ใน As number เดียวกันวิธีการแก้ปัญหาเบื้องต้น โดย Block Destination Port 25 และให้ส่งผ่าน Mail Gateway ของ ISP แทนแต่ก็

เอกสารนี้เป็นเอกสารลิขสิทธิ์ของบริษัท ทีทีแอนด์ที จำกัด (มหาชน) ไม่อนุญาตให้เผยแพร่โดยไม่ได้รับอนุญาต
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ยังมีปัญหาอื่นตามมาเช่นมีการโจมตีส่งสแปมของ Hacker หรือคอมพิวเตอร์พนักงานบริษัทติดไวรัส ก็จะมีการส่งสแปมเกิดขึ้นในจำนวนมากๆแล้วนั้นจะทำให้ Mail gateway ขององค์กรเกิดคิวค้างในจำนวนมาก, User ปลอม Sender E-mail, ไอพีของ Mail Gateway ถูก block เนื่องจากมีอีเมลบางฉบับที่ Mail Gateway ตรวจสอบไม่พบสแปมทำให้สามารถส่งออกไปยังปลายทางได้, ทำงานไม่ทัน, รับโทรศัพท์ไม่ไหวจึงเกิด Throughput เยอะ ส่งผลให้ผู้ให้บริการเปลือง Bandwidth ไปกับสแปมซึ่งเป็นต้นเหตุให้ Mail Gateway Outgoing เกิดการ Overload ใช้งานไม่ทัน สืบเนื่องมาจากปัญหาหลักของ Dynamic IP ไม่สามารถ Block IP Address ได้เนื่องจาก Reset Router หรือ ปิด – เปิด Router ทุกครั้ง IP Address ก็จะเปลี่ยนไปทุกครั้ง



รูปที่ 3.1 ภาพรวมของระบบงานเดิม

การส่งอีเมลขาออก

1. ส่วนของ Leased Line User การส่งออกอีเมลของผู้ใช้งาน Leased Line จะส่งผ่านเมล์เซิร์ฟเวอร์ของผู้ให้บริการอินเทอร์เน็ต แล้วผ่าน Mail gateway ก่อนที่จะส่งออกไปยังปลายทาง
2. ส่วนของ ADSL User การส่งออกอีเมลของผู้ใช้งาน ADSL จะไม่มีเมล์เซิร์ฟเวอร์และถูกบล็อก Smtip Connection ที่ส่งไปยังเมล์เซิร์ฟเวอร์อื่น ๆ แต่ให้ส่งผ่าน Mail Gateway ของผู้ให้บริการอินเทอร์เน็ตแทน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

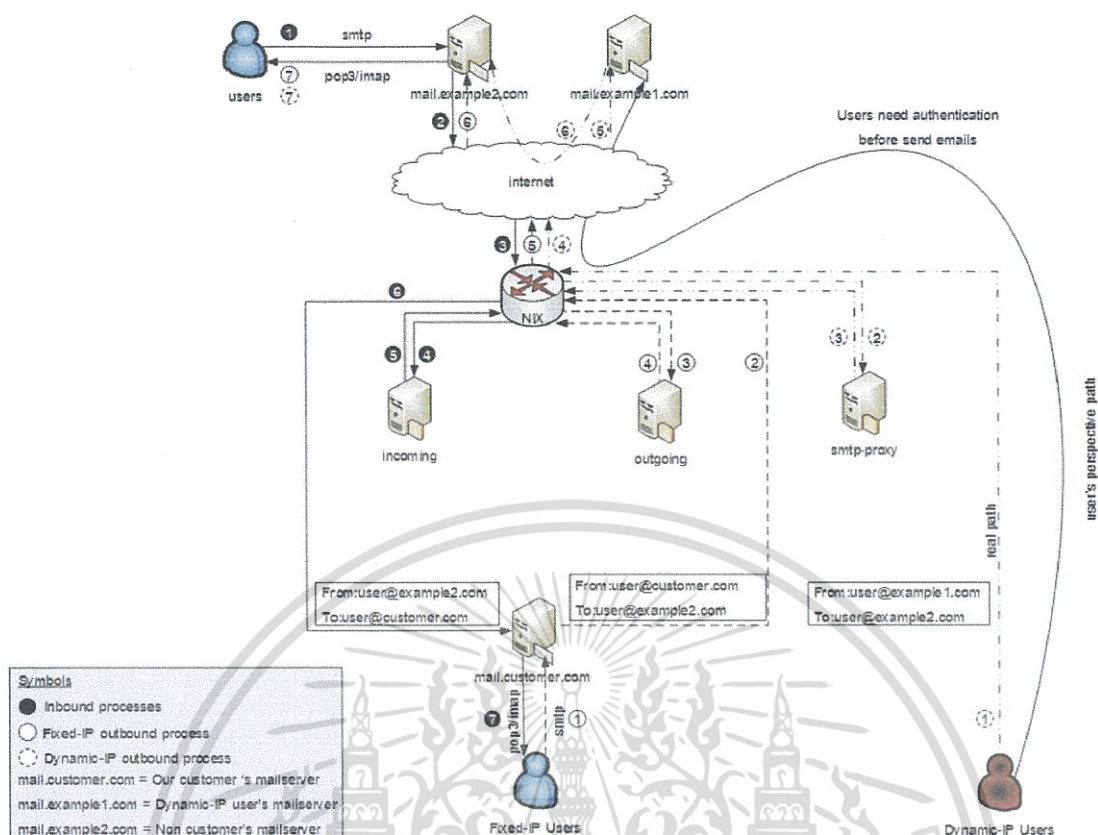
การรับอีเมลเข้า

1. ผู้ใช้บริการที่มีเมลเซิร์ฟเวอร์เป็นของตัวเองหรือให้ผู้ให้บริการกรองอีเมลให้ แล้วส่งต่อไปยังเซิร์ฟเวอร์ลูกค้า โดยจะมีการตั้งค่า MX Record เป็น Mail Gateway ของผู้ให้บริการอินเทอร์เน็ต
2. ลูกค้าที่มีเมลเซิร์ฟเวอร์ และรับอีเมลเองได้โดยไม่ใช้บริการในส่วนของการคัดกรองอีเมลของผู้ให้บริการอินเทอร์เน็ต โดยจะมีการตั้งค่า MX Record เป็นของผู้ใช้บริการเอง เช่น เมลเซิร์ฟเวอร์ของผู้ใช้บริการ หรือ Mail Gateway ของผู้ให้บริการ

3.2 วิเคราะห์ระบบงานใหม่

จากที่ผู้พัฒนาได้ศึกษาแนวทางและแนวคิดต่างๆที่เกี่ยวข้องกับระบบงานใหม่และปัญหาต่างๆของระบบงานเดิมจึงมีแนวคิดที่จะพัฒนาระบบขึ้นมาใหม่เพื่อแก้ไขปัญหของระบบงานเดิมดังกล่าวปัญหานี้สามารถแก้ไขให้หมดไปได้โดยวิธีการ แยกประเภทลูกค้าโดย อนุญาตให้ลูกค้าแบบ Static IP เท่านั้นที่จะสามารถส่งอีเมลผ่าน SMTP Gateway ของผู้ให้บริการได้ ส่วนลูกค้าประเภท Dynamic IP อนุญาตให้ส่งไปยัง SMTP Server ต้นทางแบบมีเงื่อนไขโดยจะต้องมีการทำ SMTP Authentication เพราะ มีเพียงผู้ส่งตัวจริงเท่านั้นที่ทำได้ แต่สแปมเมอร์ทำไม่ได้ การแยก Mail Gateway กันระหว่าง Static-IP และ Dynamic-IP และคุณสมบัติต่างๆของ Protocol SMTP ในการแก้ปัญหาต่างๆได้ เช่น SMTP Authentication และเพิ่ม Filter ต่างๆเพื่อเข้าไปช่วยในการจัดการในด้านป้องกัน Virus และ Spam เช่น Spam Assassin, Clam AV และประยุกต์ใช้ Protocol SNMP ในการดึงค่า Stat ต่างๆออกมา พร้อมทั้ง ใช้โปรแกรมประยุกต์ CACTI เพื่อแสดงปริมาณข้อมูลทั้งขาเข้า/ออกในเครือข่าย โดยจะแสดงผลออกมาในรูปแบบของกราฟสามารถเข้าใจและเปรียบเทียบระดับการใช้งานได้ง่ายขึ้นเพื่อวัดประสิทธิภาพของการทำงานเพราะฉะนั้นระบบงานใหม่ จะสามารถป้องกันการโดน Block IP เนื่องจากผู้ใช้ที่เป็น Dynamic-IP จะต้องวิ่งผ่านทาง Mail Proxy หรือ Proxy Server ที่เราสร้างขึ้นมานี้เพราะฉะนั้น Hacker จะไม่สามารถปลอมแปลง User และนำ Account ของผู้ให้บริการไปส่ง Spam ได้ เพราะจะต้องผ่านการ Authentication ของระบบงานก่อน ในระบบงานใหม่นี้ก็ยังสามารถ Scan Virus และ Check Spam ต่างๆได้ สามารถดึงค่า Stat ต่างๆ พร้อมทั้ง Monitor Graph ดู Traffic ต่างๆได้ เช่น Memory , CPU ระบบงานใหม่ที่กำลังสร้างขึ้นนี้จะทำงานบน Platform ที่เป็น Linux Server และในส่วนของการ Plot Graph สามารถใช้งานผ่าน Web Application ได้เนื่องจาก Cacti เป็น Web-Based Application

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 3. ภาพรวมของระบบงานใหม่

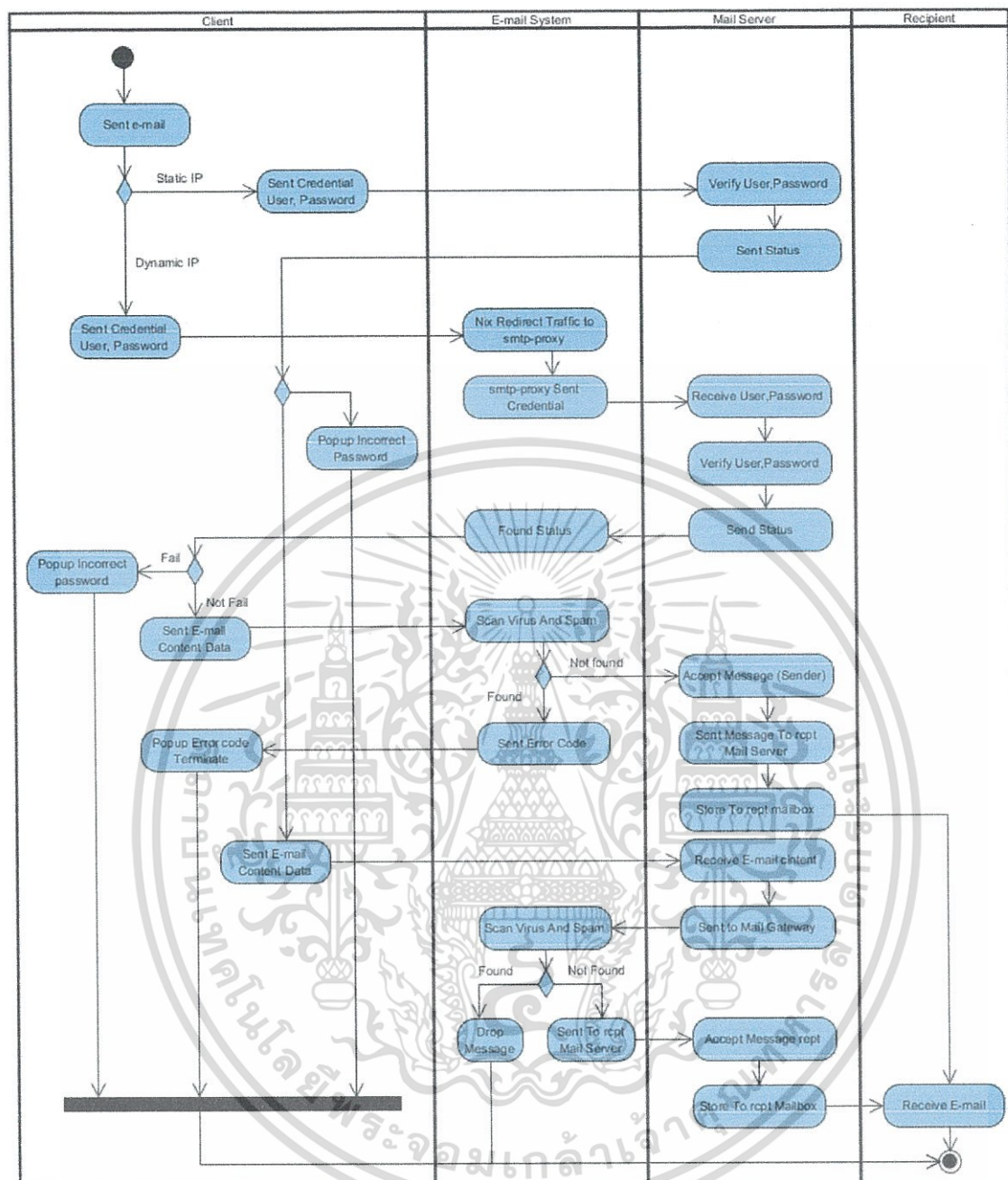
การส่งอีเมลขาออก

1. ส่วนของ Leased Line User การส่งออกอีเมลของผู้ใช้งาน Leased Line จะส่งผ่านเมลเซิร์ฟเวอร์ของผู้ให้บริการอินเทอร์เน็ต แล้วผ่าน Mail gateway ก่อนที่จะส่งออกไปยังปลายทาง
2. ส่วนของ ADSL User การส่งออกอีเมลของผู้ใช้งาน ADSL ไม่ใช้วิธีการ block ใดๆ smtp connection เหมือนระบบงานเดิม แต่ใช้ smtp proxy block เฉพาะ smtp connection ที่ไม่มีการ authenticate เท่านั้นและไม่อนุญาตให้ส่งผ่าน mail gateway เหมือนระบบงานเดิม

การรับอีเมลขาเข้า

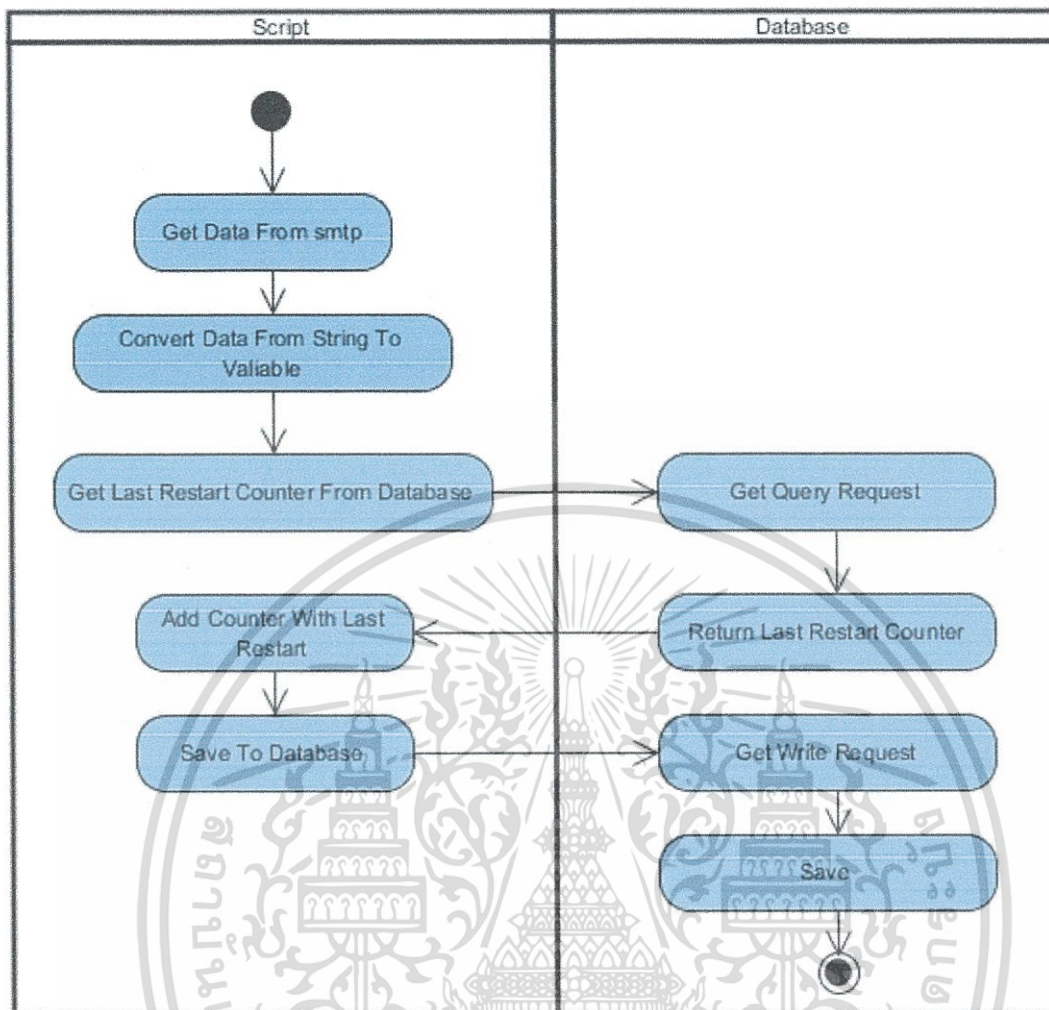
1. ผู้ใช้บริการที่มีเมลเซิร์ฟเวอร์เป็นของตัวเองหรือให้ผู้ให้บริการกรองอีเมลให้แล้วส่งต่อไปยังเซิร์ฟเวอร์ลูกค้า โดยจะมีการตั้งค่า MX Record เป็น Mail Gateway ของผู้ให้บริการอินเทอร์เน็ต
2. ลูกค้าที่มีเมลเซิร์ฟเวอร์ และรับอีเมลเองได้โดยไม่ใช้บริการในส่วนของการคัดกรองอีเมลของผู้ให้บริการอินเทอร์เน็ต โดยจะมีการตั้งค่า MX Record เป็นของผู้ใช้บริการเอง เช่นเมลเซิร์ฟเวอร์ของผู้ใช้บริการ หรือ Mail Gateway ของผู้ให้บริการ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

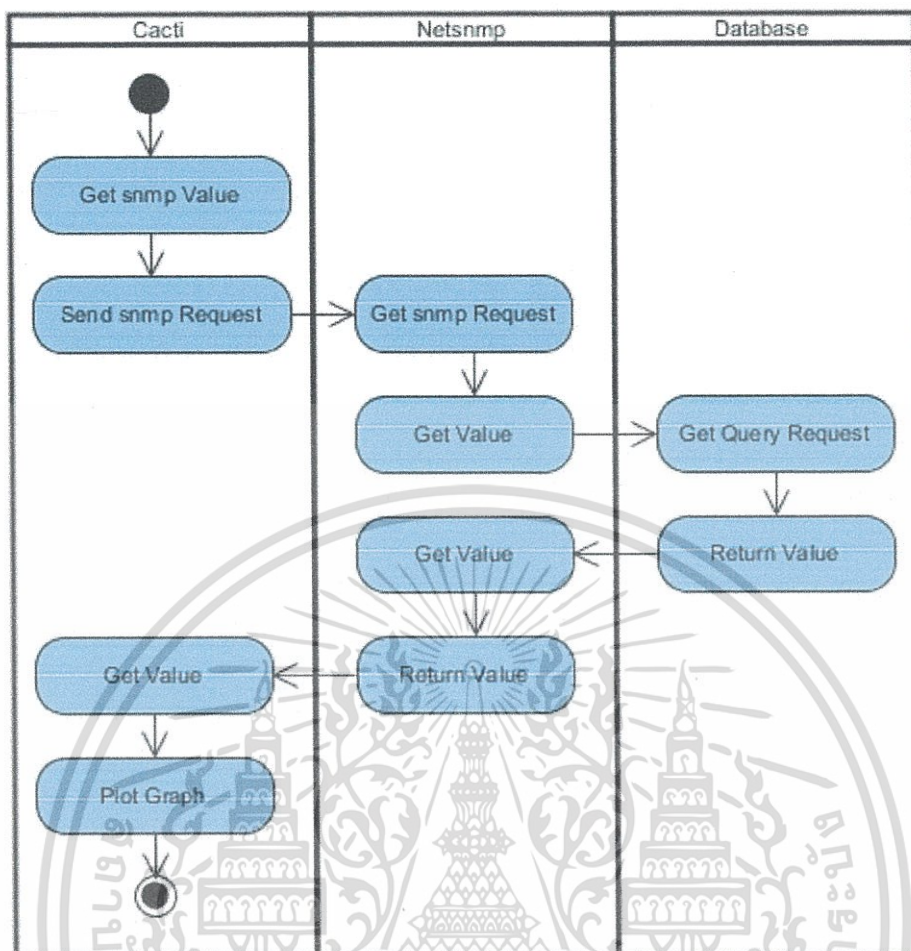


รูปที่ 3. 3 แอคทิวิตีไดอะแกรมการทำงานของระบบงานใหม่

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 3. 4 เอกวิวัติไคอะแกรมการเก็บข้อมูลค่าสถิติลงดาต้าเบส



รูปที่ 3. 5 แอคทิวิตีไดอะแกรมการนำค่าสถิติมาวาดกราฟแสดงผล

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 4

การทดสอบและผลการทดสอบ

4.1 บทนำ

จากการวิเคราะห์และออกแบบระบบงานในบทที่ 3 ในบทนี้จะกล่าวถึงการทดลองและผลการทดลองระบบป้องกันไอพีของผู้ให้บริการอินเทอร์เน็ตบัญชีดำโดยมีรายละเอียดดังนี้

- การทดสอบ
- ผลการทดสอบ

4.2 การทดสอบ

การทดสอบการทำงานของระบบป้องกันไอพีของผู้ให้บริการอินเทอร์เน็ตบัญชีดำจะทำการทดสอบการทำงานโดยการทดสอบจัดทำทดสอบโดยผู้จัดทำปัญหาพิเศษเองซึ่งเป็นการทดสอบโดยรวมทั้งหมดว่าระบบงานมีกระบวนการทำงานที่ถูกต้องตามวัตถุประสงค์ที่กำหนดไว้หรือไม่ เพื่อทำการหาข้อบกพร่องของระบบงานและนำไปสู่การปรับปรุงแก้ไขให้ระบบงานดีขึ้น โดยการทดสอบจะแบ่งออกเป็นหัวข้อย่อยๆดังนี้

4.2.1 การทดสอบ Found ประกอบไปด้วย Viruses, Spam, No-Authentication

ทดสอบโดยทำการพิมพ์คำสั่ง service smtp-gated status ในเครื่อง Server เพื่อตรวจสอบค่าสถิติก่อนทำการทดสอบ Found ซึ่งประกอบไปด้วย Viruses, Spam, No-Authentication ก่อนการส่งอีเมลเพื่อทำการวิเคราะห์ว่า มีการส่งอีเมลที่เป็น Viruses, Spam หรือไม่

กรณีที่ 1 กรณีที่ส่ง Viruses ในอีเมลส่งต่อไปยังผู้อื่นค่าสถิติก็จะเพิ่มในส่วนของ Viruses

กรณีที่ 2 กรณีที่ส่ง Spam ในอีเมลส่งต่อไปยังผู้อื่นค่าสถิติก็จะเพิ่มในส่วนของ Spam

กรณีที่ 3 กรณีที่ No-Authenticationการส่งอีเมลโดยไม่ผ่านการเข้ารหัส ค่าสถิติก็จะเพิ่มในส่วน of No-Auth


```
[root@SMTPProxy etc]# service smtp-gated status
smtp-gated (pid 18163) is running...
Version: 1.4.20.0
Compile date: Nov 26 2014 15:42:31
Dump time: Sat Apr 25 23:04:35 2015
Start time: Fri Apr 24 15:17:24 2015
Restart time: Sat Apr 25 14:13:05 2015
Last crash: Thu Jan 1 07:00:00 1970
Last BUG: Thu Jan 1 07:00:00 1970
Uptime: 1d 7h 47m 11s
Resource: 1072/0/0/0 (maxrss/ixrss/idrss/isrss)
Children: 0/7/0/0 (current/max/crashed/bugs)
Found: 1/1/122/0/0 (viruses/spam/no-auth/spf/regex/earlytalk)
Requests: 6254869/6/472 (total/direct/empty)
Rejects: 7189/0/6247026/0/0/0/0 (host/ident/lock/dnsbl/rate/ratelimit/other)
Errors: 0 (pipeline)
Auth: 114/43 (accepted/rejected)
```

รูปที่ 4.1 ค่าสถิติก่อนการตรวจสอบ Found

4.2.2 การทดสอบ Request ประกอบไปด้วย Total, Direct, Empty

ทดสอบโดยทำการพิมพ์คำสั่ง service smtp-gated status ในเครื่อง Server เพื่อตรวจสอบค่าสถิติก่อนทำการทดสอบการ Request ซึ่งประกอบไปด้วย Total, Direct, Empty

กรณีที่ 1 การ RequestTotal เป็นการ Traffic ที่ขอใช้บริการรวมทั้งหมดผ่าน Server นี้ค่าสถิติก็จะเพิ่มในส่วนของ RequestTotal

กรณีที่ 2 การ Request Direct เป็น Section ที่ถูก Encryption โดย TLS Protocols โดยที่ smtp จะปล่อยผ่าน เนื่องจากการถูกเข้ารหัส ค่าสถิติก็จะเพิ่มในส่วนของ Request Direct

กรณีที่ 3 การ Request Empty เป็นการร้องขอแต่ไม่ได้ใช้บริการ รวมทั้งการส่งอีเมลล์ไม่สำเร็จและ Transaction ไม่ครบค่าสถิติก็จะเพิ่มในส่วนของ Request Empty

```
[root@SMTPProxy etc]# service smtp-gated status
smtp-gated (pid 18163) is running...
Version: 1.4.20.0
Compile date: Nov 26 2014 15:42:31
Dump time: Sat Apr 25 23:04:35 2015
Start time: Fri Apr 24 15:17:24 2015
Restart time: Sat Apr 25 14:13:05 2015
Last crash: Thu Jan 1 07:00:00 1970
Last BUG: Thu Jan 1 07:00:00 1970
Uptime: 1d 7h 47m 11s
Resource: 1072/0/0/0 (maxrss/ixrss/idrss/isrss)
Children: 0/7/0/0 (current/max/crashed/bugs)
Found: 1/1/122/0/0 (viruses/spam/no-auth/spf/regex/earlytalk)
Requests: 6254869/6/472 (total/direct/empty)
Rejects: 7189/0/6247026/0/0/0/0 (host/ident/lock/dnsbl/rate/ratelimit/other)
Errors: 0 (pipeline)
Auth: 114/43 (accepted/rejected)
```

รูปที่ 4.2 ค่าสถิติก่อนการตรวจสอบ Requests

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

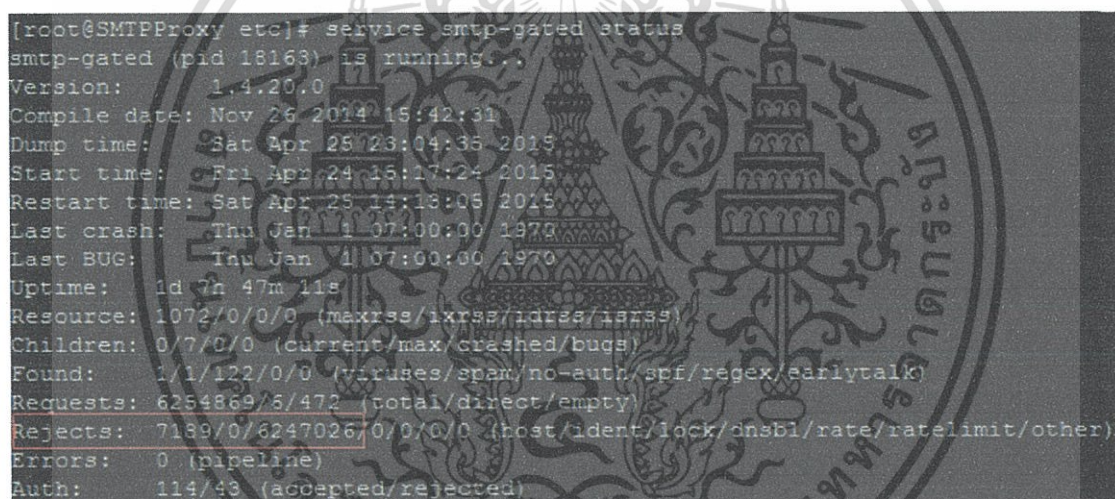
4.2.3 การทดสอบ Reject ประกอบไปด้วย Host, Ident, Lock, Other

ทดสอบโดยทำการพิมพ์คำสั่ง service smtp-gated status ในเครื่อง Server เพื่อตรวจสอบค่าสถิติก่อนทำการทดสอบการ Reject ซึ่งประกอบไปด้วย Host, Lock, Other

กรณีที่ 1 การ Reject Host การปฏิเสธ Host ที่ขอใช้บริการเนื่องจากการมีขอใช้บริการติดต่อกันเกินเวลาที่ตั้งไว้ค่าสถิติก็จะเพิ่มในส่วนของ Reject Host

กรณีที่ 2 การ Reject Lock โดยการ Lock IP-Address ของผู้ที่โจมตีผู้ใช้บริการรายอื่นไม่ว่าจะเป็นการโจมตีด้วยรูปแบบ Viruses หรือการส่ง Request ขอใช้บริการต่อกันในจำนวนมากๆ ระบบก็จะทำการ Lock IP-address ไว้ทำให้ไม่สามารถส่ง Viruses ให้ผู้ใช้บริการรายอื่นได้อีกค่าสถิติก็จะเพิ่มในส่วนของ Reject Lock

กรณีที่ 3 การ Reject Other เป็นการปฏิเสธในช่องทางอื่นๆ ค่าสถิติก็จะเพิ่มในส่วนของ Reject Other



```
[root@SMTPProxy etc]# service smtp-gated status
smtp-gated (pid 18163) is running...
Version: 1.4.20.0
Compile date: Nov 26 2014 15:42:31
Dump time: Sat Apr 25 23:04:35 2015
Start time: Fri Apr 24 15:17:24 2015
Restart time: Sat Apr 25 13:13:05 2015
Last crash: Thu Jan 1 07:00:00 1970
Last BUG: Thu Jan 1 07:00:00 1970
Uptime: 1d 7h 47m 11s
Resource: 1072/0/0/0 (maxrss/ixrss/idrss/isrss)
Children: 0/7/0/0 (current/max/crashed/bugs)
Found: 1/1/122/0/0 (viruses/spam/no-auth/spf/regex/earlytalk)
Requests: 6254869/5/472 (total/direct/empty)
Rejects: 7189/0/6247026/0/0/0/0 (host/ident/lock/dnsbl/rate/ratelimit/other)
Errors: 0 (pipeline)
Auth: 114/43 (accepted/rejected)
```

รูปที่ 4.3 ค่าสถิติก่อนการตรวจสอบ Rejects

4.2.4 การทดสอบ Authentication ประกอบไปด้วย Accepted, Rejected

ทดสอบโดยทำการพิมพ์คำสั่ง service smtp-gated status ในเครื่อง Server เพื่อตรวจสอบค่าสถิติก่อนทำการทดสอบการ Authentication ซึ่งประกอบไปด้วย Accepted, Rejected ในการส่งอีเมลเพื่อทำการวิเคราะห์ดูว่าผู้ลงชื่อเข้าใช้ระบบทำการ Login และส่งอีเมลด้วย Username และ Password ที่ถูกต้องหรือไม่

กรณีที่ 1 ผ่านการ Authentication เพื่อทำการส่งอีเมลอย่างถูกต้องค่าสถิติก็จะเพิ่มในส่วนของ Accepted

กรณีที่ 2 ไม่ผ่านการ Authentication เพื่อทำการส่งอีเมลไม่ว่าจะเป็นการใส่รหัสผู้ผลิตหรือมีเจตนาไม่ใส่ก็ตามค่าสถิติก็จะเพิ่มในส่วนของ Rejected

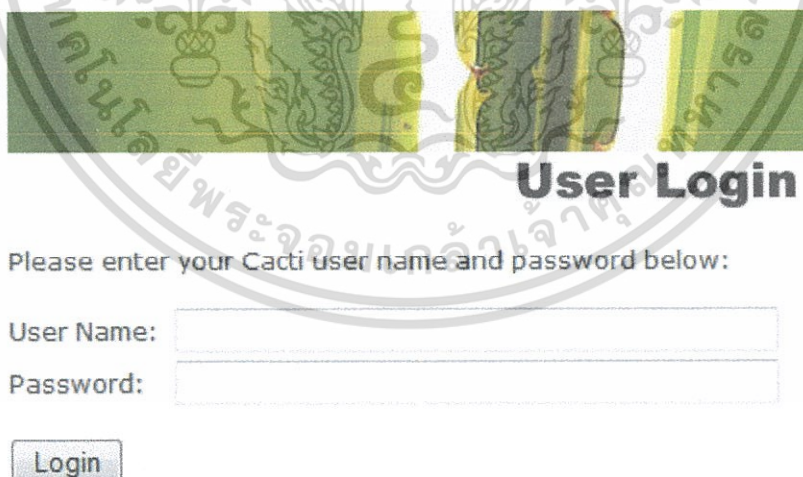
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้


```
[root@SMTPProxy log]# service smtp-gated status
smtp-gated (pid 18163 7892) is running...
Version:      1.4.20.0
Compile date: Nov 26 2014 15:42:31
Dump time:    Sat Apr 25 21:11:47 2015
Start time:   Fri Apr 24 15:17:24 2015
Restart time: Sat Apr 25 14:13:05 2015
Last crash:   Thu Jan  1 07:00:00 1970
Last BUG:     Thu Jan  1 07:00:00 1970
Uptime:       1d 5h 54m 23s
Resource:     1072/0/0/0 (maxrss/ixrss/idrss/iarss)
Children:     1/7/0/0 (current/max/crashed/bugs)
Found:        1/1/122/0/0 (viruses/spam/no-auth/spf/regex/earlytalk)
Requests:     6254573/4/464 (total/direct/empty)
Rejects:      7187/0/6246754/0/0/0/0 (host/ident/lock/dnsbl/rate/ratelimit/other)
Errors:       0 (pipeline)
Auth:         100/41 (accepted/rejected)
```

รูปที่ 4.4 ค่าสถิติก่อนการตรวจสอบ Authentication

4.3 ผลการทดสอบ

ผลของการทดสอบระบบป้องกันไอพีของผู้ให้บริการอินเทอร์เน็ตรายละเอียดยังคงจะมีส่วนติดต่อสำหรับผู้ใช้งาน โดยผู้ใช้งานจะเป็นเจ้าหน้าที่ในหน่วยงานบริการอินเทอร์เน็ต เพื่อ Monitor ดูการเปลี่ยนแปลงของระบบงานให้เข้าใจได้ง่ายขึ้น โดยผ่าน Web Application ที่แสดงผลออกมาในรูปแบบของกราฟ การเข้าสู่ระบบ ผู้ใช้งานจะต้องระบุรหัสผู้ใช้งานและรหัสผ่านให้ถูกต้องเพื่อใช้งานระบบ แสดงดังภาพที่ 4.5



รูปที่ 4.5 หน้าจอ Login สำหรับการเข้าใช้งานระบบ

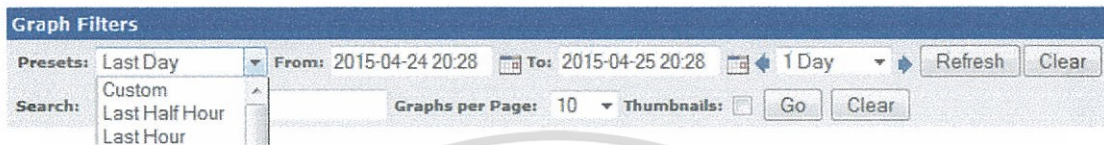
เมื่อเข้ามาสู่ระบบแล้วจะต้องทำการเลือกที่เมนู Graphs เพื่อทำการ Monitor สถานะของ Graphs แต่ละประเภทแสดงดังภาพ 4.6

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4. 6เลือกเมนู Graphs

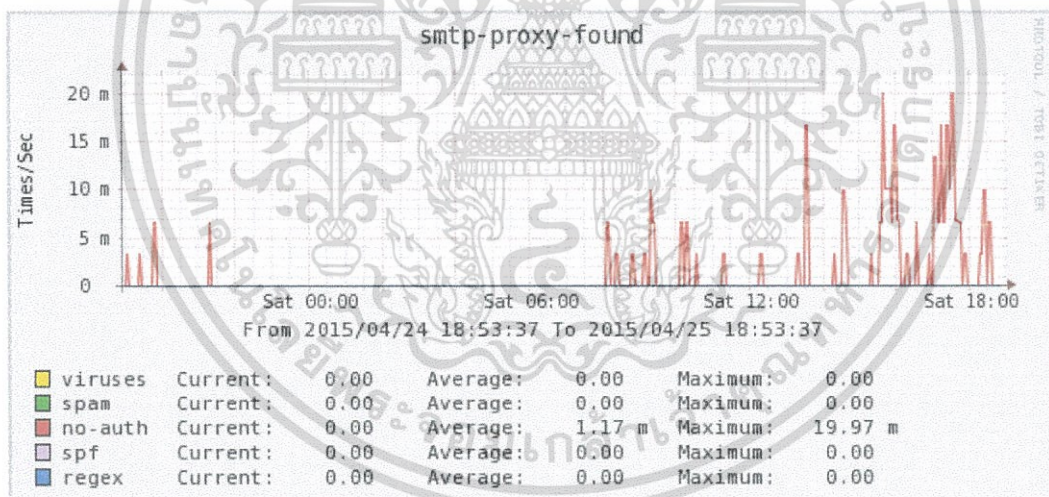
หน้าจอสำหรับเลือกเงื่อนไขที่ต้องการเฉพาะเจาะจงมากยิ่งขึ้น สามารถเลือกช่วงเวลาที่ต้องการดูกราฟได้ตามต้องการ และสามารถเลือกจำนวนที่ต้องการแสดงผลได้ แสดงดังภาพ 4.7



รูปที่ 4. 7เลือกเงื่อนไขที่ต้องการ

ดังนั้นผลการทดลองที่เกิดขึ้นจะประกอบไปด้วยผลการทดสอบตามวัตถุประสงค์ที่กำหนดดังนี้

4.3.1 ผลการทดสอบ Found

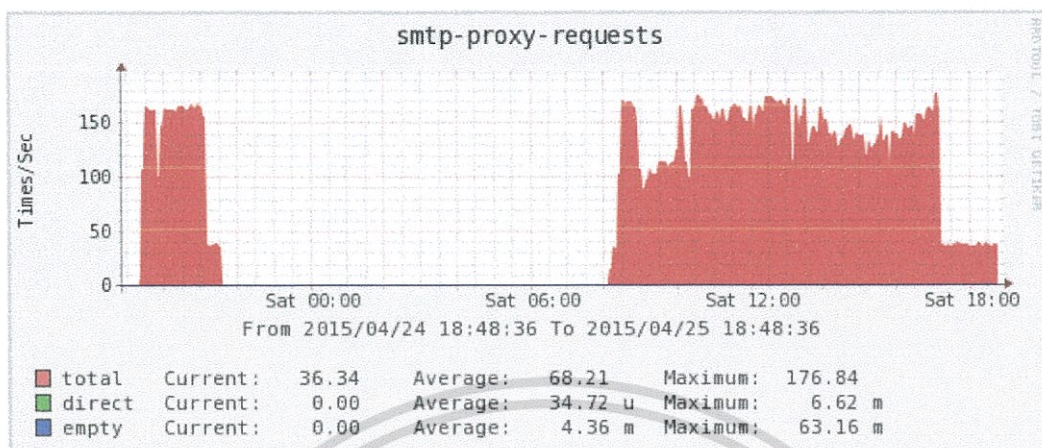


รูปที่ 4. 8ตัวอย่างผลการทดสอบ Found

จากกราฟแสดงข้อมูลของผู้ที่ไม่ได้ทำการ Authentication เข้ามาใช้งานอย่างถูกต้องทำให้ในช่วงเวลาดังกล่าวมีกราฟที่เป็นสีแดงมาก แต่ในขณะเดียวกันนั้นยังไม่พบ Viruses และ Spam

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

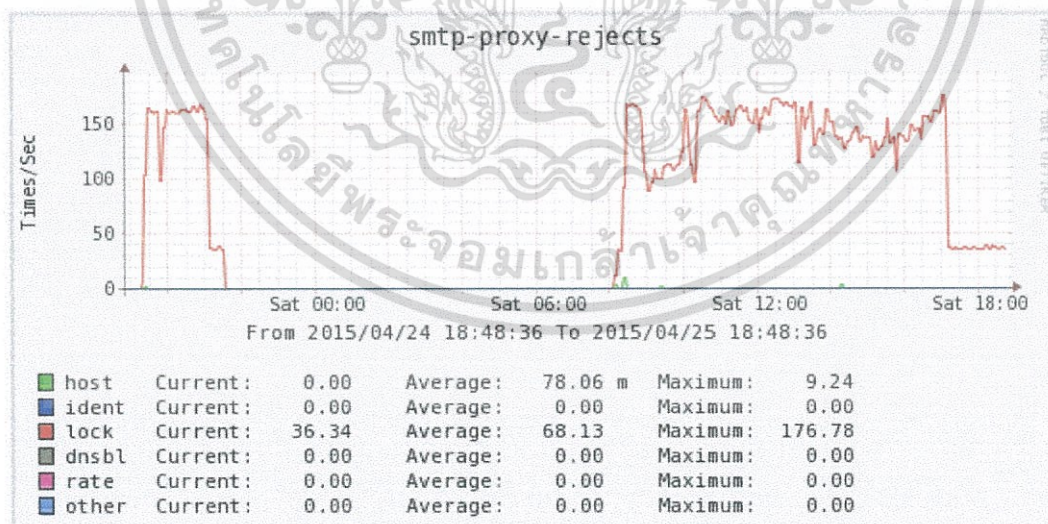
4.3.2 ผลการทดสอบ Requests



รูปที่ 4. 9 ตัวอย่างผลการทดสอบ Requests

จากกราฟแสดงข้อมูลของการ Requests ขอใช้บริการเป็นจำนวนมาก จึงทำให้เวลาดังกล่าวมรกราฟเป็นสีแดง ในส่วนของ RequestsDirect, Requests Empty นั้นมีจำนวนที่น้อยมากจึงทำให้กราฟที่ออกมาไม่สามารถแสดงภาพได้อย่างชัดเจน

4.3.3 ผลการทดสอบ Rejects

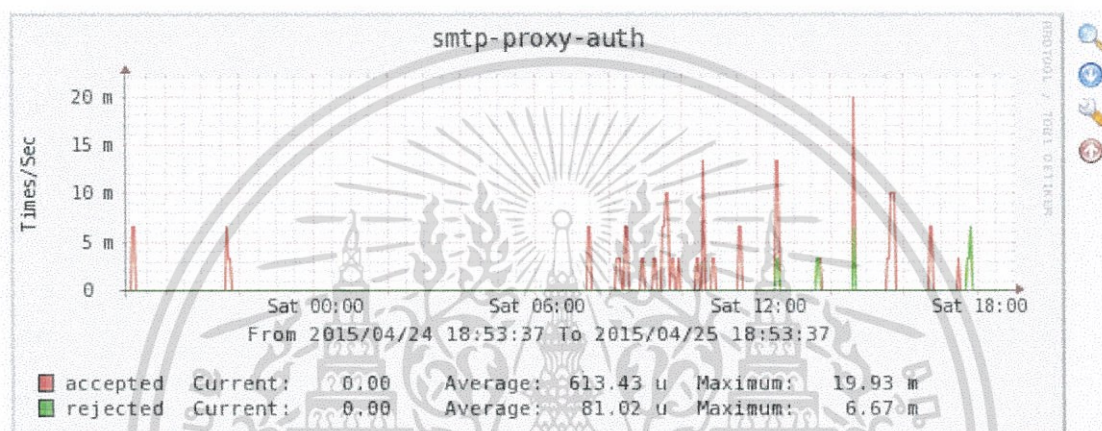


รูปที่ 4. 10 ตัวอย่างผลการทดสอบ Reject

จากกราฟแสดงข้อมูลของการ Reject พบว่าระบบงานมีการ RejectLock อย่างมากในเวลาดังกล่าวจึงทำให้กราฟเป็นสีแดงอย่างเห็นได้ชัดเนื่องจากในช่วงเวลาดังกล่าวโดยการมีการ Lock IP Address ของผู้ที่โจมตีผู้ใช้บริการรายอื่นด้วยรูปแบบการคุกคามต่างๆ ไม่ว่าจะเป็นโดน Lock เอกสารใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

จากการส่ง Viruses, Spam หรือการการส่ง Request ขอใช้บริการต่อกันในจำนวนมากๆระบบก็จะทำการ Lock IP-address ไว้ทำให้ไม่สามารถส่ง Viruses, Spam ให้ผู้ให้บริการรายอื่นได้ทั้งนี้ถ้าผู้ให้บริการอินเทอร์เน็ตต้องการปลดล็อคเพื่อทำการใช้งานต้องติดต่อเจ้าหน้าที่ผู้ให้บริการอินเทอร์เน็ตโดยตรงเพื่อทำการแก้ไขในลำดับต่อไปในส่วนของการ Reject Host มีข้อมูลเพียงเล็กน้อยเท่านั้น

4.3.4 ผลการทดสอบ Authentication



รูปที่ 4. 11 ตัวอย่างผลการทดสอบ Authentication

จากกราฟแสดงข้อมูลของการ Authentication จะพบว่า กราฟ Accepted จะมีจำนวนที่สูงมากเนื่องจาก ผู้ที่ทำการส่งอีเมลส่วนใหญ่จะเป็นผู้ส่งที่ถูกต้องผ่านการ Authentication มาเป็นส่วนใหญ่ และไม่ทำการ Authentication เพื่อทำการส่งอีเมลหรือการใส่รหัสผู้ใช้ผิดหรือมีเจตนาไม่ใส่รหัสผู้ใช้ที่ถูกต้อง เพียงเล็กน้อยเท่านั้น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 5

สรุปผลและข้อเสนอแนะ

5.1 บทนำ

จากการดำเนินงานที่กล่าวมา เป็นการจัดทำระบบป้องกันไอพีของผู้ให้บริการอินเทอร์เน็ตติดบัญชีดำ เพื่อสนับสนุนการปฏิบัติงานของ บริษัท ทีทีแอนด์ที จำกัด (มหาชน) ซึ่งจากการจัดทำระบบและทดสอบการใช้งานภายในองค์กรจึงสามารถสรุปผลและอภิปรายการดำเนินงานได้ดังนี้

5.2 สรุปผลและอภิปรายการดำเนินงาน

จากผลการดำเนินงานพบว่า การนำโปรโตคอลหลักที่ใช้ในการรับ-ส่งอีเมล คือ SMTP มาใช้เพื่อวิเคราะห์หลักการทำงาน เพื่อนำจุดเด่นมาใช้งาน และปรับปรุงจุดด้อยของโปรโตคอล โดยการนำ Filter ต่างๆ อย่างเช่น Clamav, Spamassassin, Snmp ที่มีส่วนช่วยในการเพิ่มประสิทธิภาพของ SMTP เพิ่มเข้าไปเพื่อลดจุดด้อยของ SMTP Proxy ให้มีประสิทธิภาพและป้องกัน Spam และ Virus ต่างๆ ที่จะส่งผลกระทบต่อการทำงานของ IP-Address ซึ่งจะส่งผลกระทบต่อองค์กร รวมทั้งยังใช้เทคโนโลยี Web Applications ในการพัฒนาระบบให้สอดคล้องกับกระบวนการทางธุรกิจการให้บริการอินเทอร์เน็ตในการแก้ไขปัญหา ทำให้สามารถวิเคราะห์หาสาเหตุและเปรียบเทียบได้อย่างแท้จริงและวัดผลได้จากการที่ IP-Address ของผู้ให้บริการอินเทอร์เน็ตติดบัญชีดำได้น้อยลง ซึ่งสิ่งต่างๆ เหล่านี้เป็นผลดีต่อผู้ให้บริการอินเทอร์เน็ตโดยตรง

5.3 ปัญหาและอุปสรรคในการทดลอง

ปัญหาและอุปสรรคที่พบระหว่างการพัฒนากระบวนการ คือ การนำ Range Dynamic IP จริงของผู้ใช้งานอินเทอร์เน็ตมาทดสอบต้องมีความระมัดระวังอย่างมากเพราะอาจส่งผลกระทบต่อผู้ใช้งานและผู้ให้บริการอินเทอร์เน็ตได้ เนื่องจากระบบยังใหม่อยู่อาจจะมีการทำงานบางส่วนที่ยังไม่ครอบคลุมดีพอ จึงต้องนำไปปรับปรุงแก้ไขและพัฒนาต่อไปในอนาคตต่อไปรวมถึงช่วงเวลาในการทดสอบที่สั้นอาจทำให้ผลลัพธ์ที่ออกมาไม่ชัดเจนมากพอ แต่ก็เพียงพอที่จะสามารถทดสอบสมรรถภาพของระบบงานได้

5.4 ข้อเสนอแนะ

การจัดทำระบบป้องกันไอพีของผู้ให้บริการอินเทอร์เน็ตฉบับนี้ มีข้อเสนอแนะสำหรับการพัฒนาเพิ่มเติมดังนี้ ควรพัฒนาเพิ่มเติมในส่วนของ SPF Record (Sender Policy Framework) ซึ่งเป็นระบบที่ช่วยป้องกันการดักจับ Spam Mail อีกวิธีหนึ่งซึ่งเป็นที่นิยมใช้กันมาก ซึ่งจะช่วยให้ระบบงานที่จัดทำมีประสิทธิภาพที่ดียิ่งขึ้น



บรรณานุกรม

เรืองไกร รังสิพล.2545, เปิดโลก Firewall และ Internet Security.พิมพ์ครั้งที่ 1.กรุงเทพฯ: โปรวิชั่น
 รัชชชัย ชมศิริ.2547,ติดตั้ง/ดูแล ระบบเครือข่ายคอมพิวเตอร์อย่างมืออาชีพ.พิมพ์ครั้งที่ 1.กรุงเทพฯ:
 ซีเอ็ดยูเคชั่น



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
 ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ประวัติผู้เขียน

ชื่อ-นามสกุล นายวีรวัฒน์ โพธิ์ระย้า
วัน เดือน ปีเกิด 9 พฤษภาคม 2534
สถานที่เกิด สระบุรี
ที่อยู่ สระบุรี
ประวัติการศึกษา วิทยาศาสตร์บัณฑิต เทคโนโลยีสารสนเทศ
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
ประสบการณ์ทำงาน
พ.ศ. 2556- ปัจจุบัน ตำแหน่งวิศวกรระบบ
บริษัท ทีทีแอนด์ที จำกัด มหาชน



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้