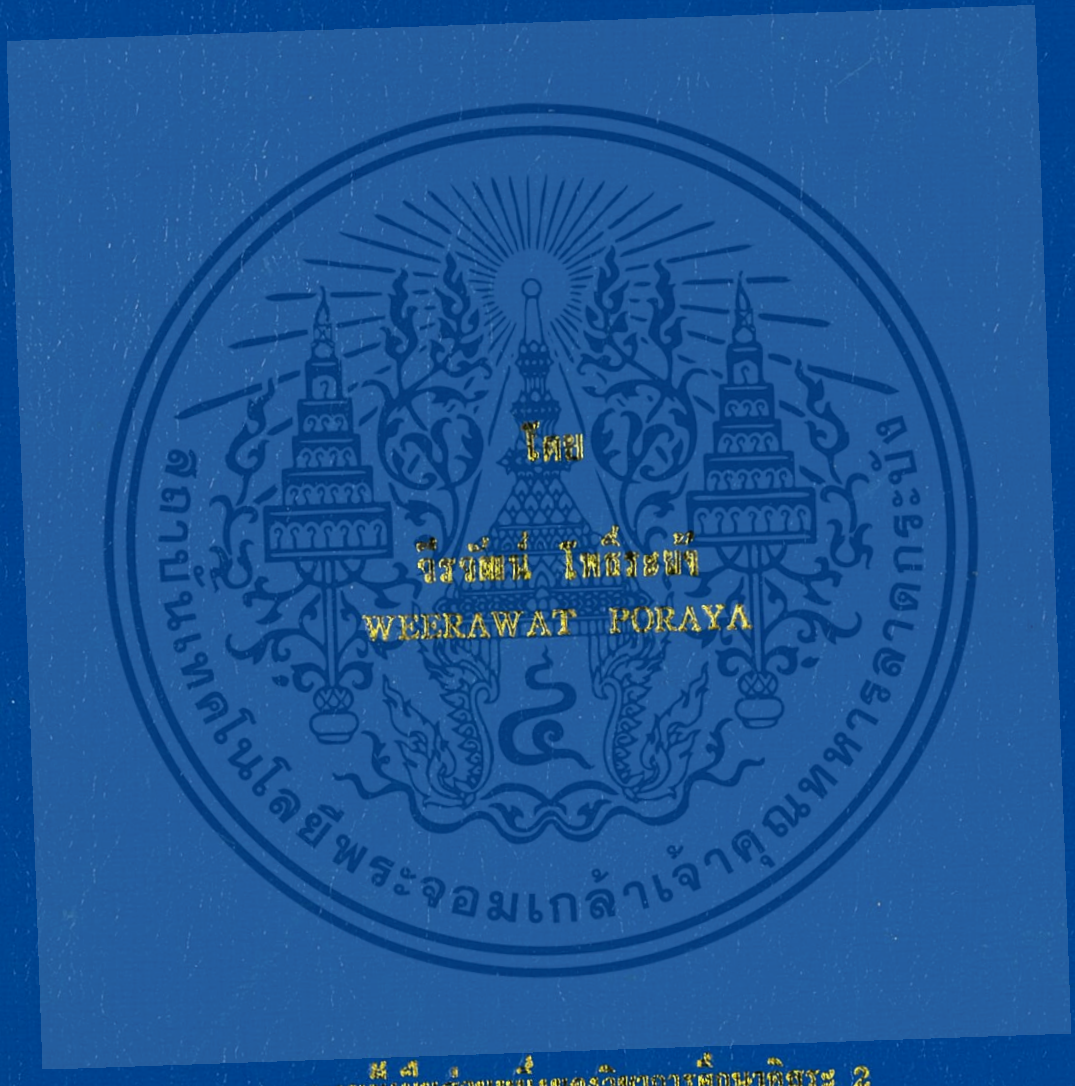
ระบบป้องกันไอพีบล็อกผู้ให้บริการอินเทอร์เน็ตติดบัญชีดำ
PROTECTION SYSTEM IP OF INTERNET SERVICE PROVIDERS (ISP) MOUNTED BLACKLIST



โดย

วีรวัฒน์ โพธิ์รัชฟ้า

WEERAWAT PORAYA

รายงานนี้เป็นส่วนหนึ่งของวิชาการศึกษาอิสระ 2

หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ

คณะเทคโนโลยีสารสนเทศ

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ภาคเรียนที่ 2 ปีการศึกษา 2557

ระบบป้องกันไอพีของผู้ให้บริการอินเทอร์เน็ตติดบัญชีดำ

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

โดย

วีรวัฒน์ โพธิ์ระย้า

WEERAWAT PORAYA

อาจารย์ที่ปรึกษา

ดร. นล เปรมัษเฐียร

รายงานนี้เป็นส่วนหนึ่งของวิชาการศึกษาอิสระ 2
หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
คณะเทคโนโลยีสารสนเทศ
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ภาคเรียนที่ 2 ปีการศึกษา 2557

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

WEERAWAT PORAYA

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

2/2014

ใบรับรองการศึกษาอิสระ 2 (Independent Study 2)

เรื่อง

ระบบป้องกันไอพีของผู้ให้บริการอินเทอร์เน็ตติดบัญชีดำ

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

นายวีรวัฒน์ โพธิ์ระย้า

รหัสประจำตัว 56606080

ขอรับรองว่ารายงานฉบับนี้ ข้าพเจ้าไม่ได้คัดลอกมาจากที่ใด

รายงานฉบับนี้ได้รับการตรวจสอบและอนุมัติให้เป็นส่วนหนึ่งของ

การศึกษาอิสระ 2 หลักสูตรวิทยาศาสตรมหาบัณฑิต (เทคโนโลยีสารสนเทศ)

ภาคเรียนที่ 2 ปีการศึกษา 2557

.....อาจารย์ที่ปรึกษา

(ดร.นล เปรมัษเฐียร)

.....กรรมการสอบ

(ดร.สุภวรรณ อันนันหนับ)

.....กรรมการสอบ

(ดร.กนกวรรณ อัจฉริยะชาญวณิช)

หัวข้อ	ระบบป้องกันไอพีของผู้ให้บริการอินเทอร์เน็ตติดบัญชีดำ
รหัสนักศึกษา	56606080
นักศึกษา	นายวีรวัฒน์ โพธิ์ระย้า
ปริญญา	วิทยาศาสตรมหาบัณฑิต
สาขาวิชา	เทคโนโลยีสารสนเทศ
แขนงวิชา	เทคโนโลยีเครือข่ายและระบบ
ปีการศึกษา	2557
อาจารย์ที่ปรึกษา	ดร.นลเปรมัษเฐียร

บทคัดย่อ

รายงานฉบับนี้เสนอวิธีการแก้ปัญหาไอพีของผู้ให้บริการอินเทอร์เน็ตติดบัญชีดำ มีวัตถุประสงค์เพื่อศึกษาโปรโตคอลหลัก ๆ ที่ใช้ในการรับ-ส่งอีเมล์ คือ SMTP เป็นโปรโตคอลแบบ TCP/IP ที่ใช้ในการส่งอีเมล์ในเครือข่ายอินเทอร์เน็ตไปยังเครื่องบริการอื่น ๆซึ่งสามารถส่งอีเมล์ไปยังผู้ใช้บริการได้ทั่วโลกมีข้อจำกัดในเรื่องของความสามารถในการส่งอีเมล์ว่าสามารถทำได้แบบเป็นคิว และ SMTP ส่วนใหญ่จะไม่ยอมให้คนภายนอกองค์กร หรือไอพีที่อยู่ภายนอกองค์กรใช้งาน SMTPได้ แต่จดหมายนี้อยู่ในรูปแบบดิจิตอลไม่สามารถจับต้องได้ ดังนั้นผู้ให้บริการแต่ละที่จึงต้องตรวจสอบผู้ใช้บริการก่อนว่าผู้ใช้บริการเป็นลูกค้าหรืออยู่ในฐานข้อมูลภายในองค์กรหรือไม่ ถ้าผู้ใช้บริการอยู่ในฐานข้อมูลระบบจะยินยอมให้ส่งอีเมล์ไปยังปลายทางได้

SMTP ส่วนใหญ่อยู่ในรูปแบบที่หลาย ๆ คนคุ้นเคย คือ smtp.company.com เป็นต้นซึ่งโดเมนเหล่านี้จะถูกมอบให้โดยผู้ให้บริการอีเมล์เซิร์ฟเวอร์ (E-mailServer) ของคุณ เพราะผู้ให้บริการก็กลัวผู้ใช้บริการส่ง Spam mail หรือโฆษณาไปรบกวนคนอื่นหรือผู้ใช้บริการรายอื่น เพราะถ้ามีผู้ใช้บริการสักคนส่งอีเมล์ไปหาผู้ใช้บริการรายอื่นแทนที่ผู้รับอีเมล์จะ Block E-mail ของคุณเพียงคนเดียว แต่กลับ Block SMTP ของผู้ให้บริการอีเมล์เซิร์ฟเวอร์ทำให้ผู้ใช้บริการคนอื่นเดือดร้อนไปด้วย เพราะว่าอีเมล์เซิร์ฟเวอร์ติดBlacklist

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

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.นลเปรมัษเฐียร 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 โพธิ์ระย้า

สารบัญ

สารบัญ (ต่อ)

หน้า

สารบัญรูป

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญ

ปัจจุบันการให้บริการอินเทอร์เน็ตขององค์กรที่ให้บริการอินเทอร์เน็ต (Internet Service Provider : ISP) มีหลายรูปแบบเช่น Leased line, FTTX และ ADSLในส่วนของ LeasedLine Internet จะทำการ Fixed-IPให้ผู้ใช้บริการ แต่ FTTX , ADSLจะไม่มีการ Fixed-IP (Dynamic-IP) ในองค์กรที่ให้บริการอินเทอร์เน็ตที่มีไอพีในจำนวนมากๆซึ่งได้ทำการแจกจ่ายให้กับผู้ใช้บริการอินเทอร์เน็ตไปนั้น ผู้ใช้บริการมักไม่ทราบว่าคอมพิวเตอร์ของตัวเองนั้นมีไวรัสอยู่โดยในบางเครื่องที่มีไวรัสอยู่นั้นจะมีการส่งจดหมายขยะ(Spam Mail) ออกมาทำให้เกิดความเสียหายกับผู้ใช้บริการ, ผู้ให้บริการอินเตอร์เน็ต และผู้รับอีเมล์ปลายทาง สำหรับในส่วนผลกระทบต่อผู้ให้บริการอินเตอร์เน็ต คือ ทำให้ไอพีของผู้ให้บริการอินเตอร์เน็ตติดอยู่ใน Spam Blacklist ซึ่งส่งผลให้ไอพีเหล่านี้ไม่สามารถส่งอีเมล์ไปยังปลายทางได้ หากมีจำนวนไอพีที่ติด Blacklist มาก ๆส่งผลให้ไอพีติด Spam Blacklist และอาจส่งผลให้ไอพีอื่นๆที่อยู่ใน Subnet เดียวกัน หรือ AS Number เดียวกันส่งอีเมล์ออกไม่ได้

โปรโตคอลที่ใช้ในการรับ-ส่งอีเมล์ คือSMTP Protocol ซึ่งโดยปกติแล้วSMTP Protocol ถูกออกแบบเพื่อใช้สำหรับการส่งอีเมล์จากผู้ส่งไปยัง SMTP Server ต้นทางผ่านเครือข่ายอินเทอร์เน็ตไปยังSMTP Server ของผู้รับปลายทางโดยผู้ใช้บริการสามารถส่งเมล์ไปยังผู้รับอื่นๆได้ทั่วโลก แต่อีเมล์ที่ส่งเข้าที่ SMTP Server ต้นทางมักมีอีเมล์ขยะส่งเข้ามาเสมอดังนั้นจึงมีความจำเป็นต้องกรองอีเมล์ขยะก่อนที่จะส่งไปยัง SMTP Server ปลายทาง ซึ่งโดยปกติแล้ว SMTP Server ต้นทาง จะอนุญาตให้ผู้ใช้ที่ Authenticate ผ่าน หรือ Source IPอยู่ในช่วงที่อนุญาตให้ส่งอีเมล์ได้เท่านั้น

สแปมเมอร์จะไม่สามารถส่งอีเมล์ผ่าน SMTP Server ต้นทางได้ เพราะอีเมล์ที่ส่งมักมีการปลอมSender Address และสแปมเมอร์ไม่ทราบ Username และ Password สำหรับใช้Authenticationกับ SMTP Server ต้นทาง หรือ Source IPที่ใช้ส่งไม่ได้อยู่ในช่วงที่อนุญาตให้ส่งผ่านSMTP Server ต้นทางได้ ดังนั้นแสปมเมอร์จะแก้ปัญหานี้โดยการทำตัวเป็น SMTP Server ต้นทางเสียเอง และส่งอีเมล์ไปยัง SMTP Server ปลายทางโดยตรง ซึ่งจะส่งผลให้ไอพีที่ผู้ให้บริการอินเตอร์เน็ตแจกจ่ายให้ลูกค้าติด Spam Blacklist ซึ่งผู้ให้บริการอินเตอร์เน็ตหลายๆราย จะแก้ปัญหานี้โดยการปิดกั้นไม่ให้ลูกค้าส่งอีเมล์ออกไปยัง SMTP Server ต้นทางโดยตรง แต่บังคับให้ส่งผ่านSMTP Gateway ของผู้ให้บริการอินเตอร์เน็ตเท่านั้น

เมื่อผู้ให้บริการอินเตอร์เน็ตบังคับให้ลูกค้าส่งอีเมล์ผ่าน SMTP Gateway ของผู้ให้บริการ

อินเตอร์เน็ตเท่านั้น อีเมล์ที่ส่งผ่านจึงมีทั้งที่มากจาก Source IPที่เป็น Dynamic และ Static แต่เมื่อผู้ให้บริการอินเตอร์เน็ตตรวจพบอีเมล์ขยะจาก Source IPที่เป็น Dynamic IPกลับไม่สามารถปิดกั้นการส่งอีเมล์จาก Source IPได้เนื่องจากผู้ใช้บริการรายนั้นใช้ไอพีที่เปลี่ยนแปลงได้ และ SMTP Gateway ไม่มีความสามารถในการปิดกั้นการส่งจาก ADSL Account

แม้ว่าการแก้ปัญหาโดยการบังคับให้ส่งอีเมล์ทั้งหมดผ่านทาง SMTP Gateway ของผู้ให้บริการอินเตอร์เน็ต จะสามารถแก้ปัญหาไอพีที่แจกจ่ายให้ผู้ใช้บริการติด Blacklistได้ แต่พบว่าไม่สามารถแก้ปัญหาไอพีของ SMTP Gateway ของผู้ให้บริการอินเตอร์เน็ตติด Blacklist ได้

ปัญหานี้สามารถแก้ให้หมดไปได้โดยวิธีการ แยกประเภทลูกค้าโดยอนุญาตให้ลูกค้าแบบ Static IPเท่านั้นที่จะสามารถส่งอีเมล์ผ่าน SMTP Gateway ของผู้ให้บริการได้ ส่วนลูกค้าประเภท Dynamic IPอนุญาตให้ส่งไปยัง SMTP Server ต้นทางแบบมีเงื่อนไข โดยการทำ STMP Authencationเพราะมีเพียงผู้ส่งตัวจริงเท่านั้นที่สามารถทำได้ แต่สแปมเมอร์ไม่สามารถทำได้

สำหรับบริการส่งอีเมล์ผ่าน SMTP Sever ต้นทางนั้นมีทั้งที่มาจากผู้ให้บริการอีเมล์ในอินเตอร์เน็ต เช่น Hotmail,Yahoo,Google หรือผู้ดูแลระบบอีเมล์ของบริษัทโดยผู้ให้บริการอีเมล์จะแจ้งให้ผู้ใช้บริการอีเมล์ทราบวิธีการตั้งค่า เพื่อใช้งานทั้งจากอีเมล์ไคลเอนต์และเว็บเมล์

1.2 ความมุ่งมั่นและวัตถุประสงค์ของการศึกษา

1.2.1 เพื่อศึกษาการการทำงานของการส่งอีเมล์โดยใช้SMTP Protocol

1.2.2 เพื่อศึกษาปัญหาที่มีผลกระทบต่อการส่งและรับอีเมล์ ในเรื่องวิธีป้องกันไม่ให้ไอพีของผู้ให้บริการผู้ให้บริการอินเทอร์เน็ตติดBlacklist

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

สร้างระบบป้องกันไอพีของผู้ให้บริการอินเทอร์เน็ตติดBlacklist เพื่อแก้ไขปัญหาของการติด Blacklist ของผู้ให้บริการอินเทอร์เน็ตภายในองค์กรและเปรียบเทียบถึงความแตกต่างระหว่างก่อนหน้าและหลังมีการใช้ระบบเพื่อวัดประสิทธิภาพการทำงานของระบบ

1.4 นิยามศัพท์เฉพาะ

Internet Service Provider (ISP) หรือผู้ให้บริการอินเทอร์เน็ตคือบริษัทที่ให้ลูกค้าสามารถเข้าถึงอินเทอร์เน็ตโดยผู้ให้บริการจะเชื่อมโยงลูกค้าเข้ากับเทคโนโนยีรับส่งข้อมูลที่เหมาะสมในการส่งผ่านอุปกรณ์โปรโตคอลอินเทอร์เน็ตอย่างเช่นไดอัล, ดีเอสแอล, เคเบิลโมเด็ม, อินเทอร์เน็ตไร้สายหรือการเชื่อมต่อระบบไฮสปีดผู้ให้บริการอินเทอร์เน็ตอาจให้บริการเปิดบัญชีชื่อผู้ใช้ในอีเมล์ติดต่อสื่อสารกับผู้อื่นโดยรับ-ส่งผ่านเซิร์ฟเวอร์ของผู้ให้บริการ ในบางครั้งผู้ให้บริการทางอินเทอร์เน็ตอาจให้บริการเก็บไฟล์ข้อมูลระยะไกล รวมถึงเรื่องเฉพาะทางอื่นๆ เป็นต้น

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

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

1.5 แนวทางการศึกษา

ศึกษาการทำงานของโปรโตคอลหลักๆที่ใช้ในการรับ-ส่งอีเมล์ 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 ทีละคำสั่งจึงสามารถตรวจสอบได้ตั้งแต่ก่อนที่อีเมล์จะมีการส่งอีเมล์สมบูรณ์ทั้งฉบับแต่ Mail Server ต้องรับอีเมล์มาก่อนทั้งฉบับก่อนแล้วถึงจะตรวจสอบ จึงทำให้เกิดปัญหาเรื่อง Disk และ Queue อยู่

บทที่ 2
เอกสารและงานวิจัยที่เกี่ยวข้อง

ในการศึกษาเพื่อทำระบบป้องกันไอพีของผู้ให้บริการอินเทอร์เน็ตติดบัญชีดำ กรณีศึกษา บริษัท ทีทีแอนด์ที 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 เพราะเป็นโปรโตคอลที่ใช้ส่งอีเมล์จาก User Agent ของผู้ส่งไปยัง MTA ของผู้ส่งและส่งต่อไปยังMTA เครื่องอื่นๆที่เป็นจุดผ่านในการเชื่อมต่อไปยังเครื่องของผู้รับโปรโตคอล SMTP จะทำงานร่วมกับโปรโตคอล TCP โดยใช้พอร์ต25โดยโปรโตคอล SMTP จะทำหน้าที่ในการส่งอีเมล์และโปรโตคอล POP3 จะทำหน้าที่ในส่วนของการรับอีเมล์ของผู้ใช้บริการ

SMTPที่ใช้ในการส่งจดหมายนั้นได้พัฒนาขึ้นมาทำงานบน TCP/IP เพื่อความสะดวกในการรับ-ส่งอีเมล์เป็นหลัก ทำให้การทำงานในส่วนของการรักษาความปลอดภัยน้อยกลายเป็นช่องโหว่ให้เกิดการส่งสแปมขึ้นจึงต้องมี Service อื่นๆเข้ามาช่วยในการจัดการการรับ-ส่งอีเมล์และในการส่งอีเมล์ของโปรโตคอล SMTP นั้นจะใช้วิธีอ้างถึงเซิร์ฟเวอร์อื่นๆตาม DNS (Domain Name System) เช่นเดียวกับระบบอื่นๆในอินเทอร์เน็ตและยังสามารถส่งอีเมล์ไปยังผู้รับคนเดียวหรือหลายๆคนพร้อมกันได้ด้วย

องค์ประกอบที่สำคัญของ SMTP มีดังต่อไปนี้

1. Message User Agent(MUA) คือโปรแกรมที่ติดต่อกับผู้ใช้บริการในการส่งอีเมล์ ซึ่งเมื่อผู้ใช้บริการได้เขียนเนื้อหาอีเมล์ที่ต้องการเรียบร้อย โปรแกรมจะทำการจัดรูปแบบของข้อมูลและส่งออกไปยัง MTA ด้วยโปรโตคอล SMTP

2. Message Tranfer Agent (MTA) คือ เซิร์ฟเวอร์ซึ่งทำหน้าที่เป็นตัวกลางรับข้อมูลเนื้อหาของจดหมายที่มาจากMUA หรือ MTA เดียวกันก็ได้ และทำการส่งต่ออีเมล์เหล่านั้นไปยัง

ปลายทางที่กำหนดไว้ คือ MTA ของอีเมล์ปลายทางเพราะฉะนั้น MUA ต้องทราบว่าจะใช้เซิร์ฟเวอร์ใดเป็น MTA เพราะโปรแกรมไคลเอนต์ที่เป็น MUA ไม่สามารถส่งอีเมล์ออกไปยังปลายทางได้เอง

3. Message Delivery Agent (MDA) คือเซิร์ฟเวอร์ที่เป็นตัวเก็บเมล์บ็อกของผู้ใช้งาน ทำหน้าที่รับจดหมายที่เข้ามาโดยโปรโตคอล SMTP และทำหน้าที่ในการตรวจสอบว่ามีเมล์บ็อก (Mailbox) ของผู้ใช้ตรงตามที่ระบุในอีเมล์หรือไม่ หากไม่ตรงกันก็จะแจ้งข้อผิดพลาด (Error) กลับไป แต่ถ้ามีเมลล์บ็อกตรงตามที่กำหนดจะรับจดหมายเข้ามาและนำไปเก็บยังเนื้อหาที่จัดสรรไว้สำหรับเมล์บ็อกนั้น และรอให้เจ้าของเมล์บ็อกมาเปิดอ่านต่อไป หรือจะเรียก MDA ว่าเป็นเมล์เซิร์ฟเวอร์ที่มีไว้เก็บเมล์บ็อกของผู้ใช้นั่นเอง

จากองค์ประกอบทั้ง 3 ส่วนที่กล่าวมาข้างต้นมีความสัมพันธ์ในกระบวนการส่งอีเมล์ของโปรโตคอล SMTP ดังแสดงรูปที่ 2.1 ซึ่งมีขั้นตอนดังนี้

1. ผู้ใช้อีเมล์เขียนจดหมายบนโปรแกรมเมล์ไคลเอนต์ MUA เพื่อส่งไปยังอีเมล์แอดเดรสปลายทาง จดหมายจะถูกส่งไปยัง MTA เพื่อให้ MTA ส่งต่อไปยังปลายทาง

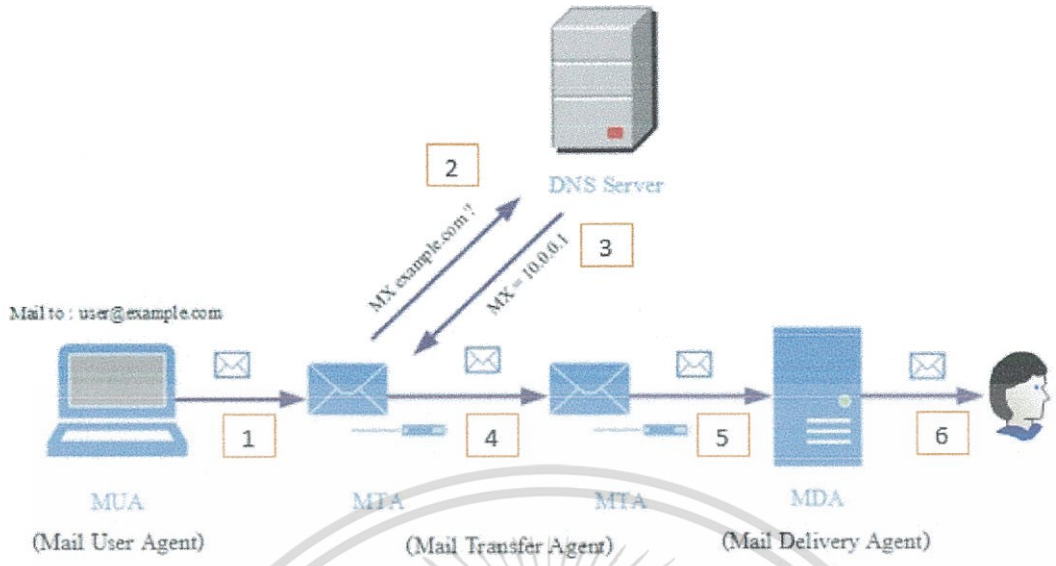
2. MTA ได้รับจดหมายมาจากผู้ใช้บริการโปรโตคอล SMTP ทำการตรวจสอบโดเมนปลายทาง และสอบถาม DNS ว่าหากต้องการส่งอีเมล์ไปยังโดเมน example.com นั้นจะต้องส่งไปยัง MTA ไหน โดยภายใน DNS จะมีการกำหนด mx record เอาไว้

3. DNS จะตอบกลับมาเป็นไอพีแอดเดรสหรือชื่อโฮสต์ของเซิร์ฟเวอร์ที่ระบุอยู่ใน mx record กลับมายัง MTA

4. MTA จัดการส่งอีเมล์ออกไปยัง MTA ที่ DNS ระบุไว้

5. MTA ของโดเมน example.com ได้รับอีเมล์เข้ามา และทำการตรวจสอบ ถ้าตรวจสอบแล้วพบว่าเป็นของโดเมนตัวเอง ก็จะทำการค้นหาต่อไปว่าชื่อผู้รับที่อยู่ในอีเมล์นั้นเก็บไว้บน MDA ใดและส่งไปยัง MDA นั้นๆ

6. MDA เมื่อได้รับจดหมายเข้ามาก็จะทำการตรวจสอบชื่อผู้รับ และนำจดหมายไปเก็บยังเมล์บ็อกของผู้รับ



รูปที่ 2.1กระบวนการส่งอีเมล์ของโปรโตคอล SMTP

2.2 แนวคิดเกี่ยวกับการป้องกัน E-mail Virus และ E-mail Spam

2.2.1 อีเมล์ไวรัส (E-mail Virus) คืออีเมล์ที่ถูกส่งเข้ามาด้วยความจงใจหรือไม่เจาะจงซึ่งมีการพัฒนาและแพร่หลายอย่างต่อเนื่อง อาจพบไวรัสชนิดใหม่แทบทุกเดือนโดยมีความประสงค์ที่จะทำให้คอมพิวเตอร์ของคุณมีไวรัสเมื่อทำการเปิดคลิกไฟล์แนบที่ผู้ส่งนั้นส่งมา, ในบางกรณีเรายังพบว่า Hacker ได้ทำการสร้างอีเมล์ที่มีไวรัสและทำการแนบไฟล์โดยเฉพาะ ".exe" และทำการบีบอัดไฟล์(ZIP File)เพื่อหลบหลีกการตรวจสอบของ E-Mail Hosting บางกรณี Hacker อาจจะทำการส่งอีเมล์โดยมีการแนบ URL หรือ Website เพราะต้องการหลบหลีกการตรวจสอบของ Firewall E-Mail Hosting เพื่อหลอกให้คุณกดเข้าไปดาวน์โหลดไวรัสลงในเครื่องคอมพิวเตอร์ โดยไวรัสที่ Hacker จงใจส่งเข้ามาผ่านทางอีเมล์นั้นจะมีจุดประสงค์หลักคือ โจรกรรมข้อมูล (Hack) เพื่อเอาข้อมูลที่เป็นความลับ หรือข้อมูลที่สำคัญทางธุรกิจของคุณไปใช้ในเชิงมิชอบ เช่น Username, Password ของอีเมล์ไปปลอมแปลงและสร้างเอกสารเลขบัญชีปลอมขึ้นมาซึ่งเป็นกรณีที่พบได้บ่อยมาก ทำให้เกิดความเสียหายต่อตัวเองและต่อธุรกิจได้ ช่องทางการแพร่กระจายของไวรัสจะอาศัยอีเมล์และอินเทอร์เน็ตเป็นช่องทางหลัก การทำงานของไวรัสจะอยู่ในระดับแอพพลิเคชั่นเลเยอร์ (Application Layer) อาศัยการ Executed คำสั่งของผู้ใช้และระบบปฏิบัติการเป็นหลัก ไวรัสจะเกี่ยวข้องกับอินเทอร์เน็ตและไฟร์วอลล์(Firewall) คือไวรัสจะอาศัยอินเทอร์เน็ตเป็นทางผ่านเท่านั้น หากไวรัสแพร่ระบาดโดยที่เรามีเมล์เซิร์ฟเวอร์อยู่และกำหนดให้ไฟร์วอลล์อนุญาติให้มีทราฟฟิคเพื่อการรับ-ส่งอีเมล์ได้ ไวรัสจะสามารถผ่านเข้ามาได้ในช่องทางเดียวกัน ไฟร์วอลล์ไม่สามารถป้องกันไวรัสได้เพราะการทำงานของไฟร์วอลล์อยู่คนละส่วนกัน ไฟว์วอลล์เป็นเพียงเครื่องมือในการป้องกันระดับเน็ตเวิร์กเลเยอร์(Network Layer)ที่คอยควบคุมทราฟฟิคเป็นหลัก ซึ่งทำงานอยู่

ในเลเยอร์ที่ต่ำกว่าการทำงานของไวรัสทำให้ไฟร์วอลล์รู้จักแต่เฉพาะ TCP, UDP, ICMP, PORT

2.2.2 อีเมล์สแปม (E-Mail Spam) คือ ลักษณะของอีเมล์ที่สร้างความเสียหายแก่เครือข่ายอินเทอร์เน็ตและสร้างความเดือดร้อนให้แก่ผู้ใช้บริการอินเทอร์เน็ตนั้นแบ่งออกเป็นประเภทใหญ่ ๆ ได้สองประเภท คือ Chain Mail หรือจดหมายลูกโซ่ และ Spam Mail หรือการโจมตีด้วยอีเมล์

1. Chain Mail หรือจดหมายลูกโซ่นั้นจะมีเนื้อหาเหมือนจดหมายทั่วไปแต่จะมีเนื้อหาเกี่ยวกับคำเตือนเรื่องไวรัส หรือเรื่องอื่น ๆให้ส่งต่อให้กับคนที่รู้จัก หากมีคนส่งต่อกันเป็นจำนวนมากส่งผลให้Mail Server ของผู้ให้บริการอินเทอร์เน็ตเสียหายเกิด Server Down หรือทำงานช้าลง นอกจากนี้ยังเป็นตัวการทำให้ทราฟฟิคของเครือข่ายอินเทอร์เน็ตเกิดอาการติดขัดในส่วนของผู้ใช้บริการอินเทอร์เน็ตนั้น การได้รับอีเมล์ประเภทนี้บ่อย ๆ จะเกิดความรำคาญได้ ดังนั้นผู้ใช้บริการต้องหยุดการส่งอีเมล์ประเภทนี้เพื่อหยุดวงจรลูกโซ่

2. สแปมเมล์ (Spam Mail) หรืออีเมล์ขยะที่ได้รับมาโดยผู้ใช้อีเมล์ไม่ต้องการจำนวนมาก ๆ ในครั้งหนึ่ง หรือการทยอยส่งแต่ส่งจำนวนหลายฉบับ อาจจะเป็นโฆษณาชวนเชื่อและไม่สามารถติดตามผู้ส่งตัวจริงได้ อาจจะไม่เป็นอันตรายมากแต่จะส่งผลกระทบในเรื่องของความรำคาญให้แก่ผู้รับ และทำให้ประสิทธิภาพของการใช้ระบบอีเมล์ลดน้อยลงและสิ้นเปลืองทรัพยากรเพื่อจัดเก็บอีเมล์ขยะพวกนี้ สำหรับวัตถุประสงค์นั้นมีหลากหลาย ตั้งแต่โฆษณาสินค้าการโจมตีระบบ การแก้แค้นส่วนตัว การกลั่นแกล้ง เป็นต้น ซึ่งผู้ใช้อีเมล์อาจจะได้รับผลกระทบใน 2 กรณีดังต่อไปนี้

กรณีแรก ในฐานะเป็นผู้รับอีเมล์ผู้ส่งอีเมล์เป็นคนที่ผู้รับอีเมล์ไม่เคยรู้จักมาก่อนแต่ได้ส่งอีเมล์มาให้ผู้รับโดยตรงโดยที่ผู้รับอีเมล์ไม่ต้องการรับอีเมล์ฉบับนั้นเลย จากนั้นผู้รับอีเมล์ต้องมาตามลบอีเมล์ฉบับนั้นๆทิ้งไป

กรณีที่สอง ในฐานะที่ถูกใช้เป็นตัวกลางในการส่งต่ออีเมล์เป็นการส่งผลกระทบเฉพาะกับเมล์เซิร์ฟเวอร์เท่านั้น เนื่องจากเมล์เซิร์ฟเวอร์กำหนดค่าไว้ไม่เหมาะสม ทำให้สามารถโดนถูกใช้เป็นตัวกลางในการกระจายอีเมล์ขยะไปหาผู้ใช้อีเมล์อื่นๆได้

2.3 แนวคิดเกี่ยวกับความแตกต่างระหว่าง SMTP Proxy และ Mail Server

Mail Server คือเครื่องคอมพิวเตอร์ที่ให้บริการในการรับส่งเมล์ให้กับบุคคลหรือองค์กร โดยที่ Mail Server จะตั้งอยู่ที่ผู้ให้บริการอินเทอร์เน็ตหรือภายในองค์กร หรือแม้กระทั่งที่พักส่วนบุคคลก็ได้ ตัวอย่างผู้ให้บริการเมล์ที่เป็นที่รู้จักได้แก่ Hotmail.com, Gmail.com สำหรับการที่องค์กรมี Mail Serverเป็นของตนเองจะมีประโยชน์ คือความสะดวกในการจัดการกล่องข้อความ (Mailbox)ของผู้ใช้บริการแต่ละคนในด้านความปลอดภัยและปริมาณเนื้อที่จัดเก็บข้อมูลซึ่งสามารถเพิ่มได้โดยไม่จำกัดการทำงานของการรับส่งเมล์นั้น จะประกอบไปด้วย 2 ส่วนหลักคือ Mail Server และ Mail Client เมื่อผู้ใช้บริการต้องการใช้เมล์จะต้องใช้งานผ่าน Mail Client ซึ่งอาจอยู่ในรูปแบบ

แอปพลิเคชันหรือเว็ปแอปพลิเคชัน เมื่อผู้ใช้บริการทำการส่งอีเมล์ข้อมูลอีเมล์จะถูกส่งจากไปยัง Mail Server ส่วนในกรณีที่ผู้ใช้ต้องการอ่านอีเมล์ ผู้ใช้บริการเพียงอ่านข้อมูลผ่านทางกล่องข้อความของ Mail Server สำหรับกรณีที่ส่งอีเมล์ข้ามกลุ่มหรือองค์กรเช่น ต้องการส่งจากอีเมล์ Hotmail.com ไปยัง Yahoo.com จะคล้ายหลักการส่งอีเมล์เหมือนที่กล่าวมาข้างต้น เพียงแต่อีเมล์ที่ส่งไปยัง Mail Server ของ Hotmail จะถูกส่งผ่านไปยัง Mail Serverของ Yahooอีกครั้งหนึ่ง

นอกจาก Mail Serverและ Mail Client แล้วยังมีส่วนที่สำคัญอีกอย่าง คือDNS Server ซึ่งจะต้องจัดเก็บข้อมูล Public-IP และ URL ของMail Server ทำให้ Mail Client ส่งข้อมูลไปยัง Mail Serverได้อย่างถูกต้องและใช้โปรโตคอล SMTP ในการส่งเมล์ไปยังกล่องข้อความของผู้รับปลายทางที่ Mail Server ซึ่งในบางครั้งเครื่องที่ให้บริการในส่วนนี้จะเรียกว่า SMTP Server ซึ่งในกรณีที่ส่งอีเมล์ต่างกลุ่มหรือต่างองค์กร อีเมล์จะมีการส่งต่อระหว่าง SMTP Server นั่นเอง

Simple Mail Transfer Protocol Server หรือ SMTP Server คือเครื่องบริการส่งอีเมล์ไปยังเครื่องบริการอื่น ๆ เพราะปกติผู้ใช้อินเทอร์เน็ตมักจะประสบปัญหาในการส่งอีเมล์เมื่อเชื่อมต่ออินเทอร์เน็ตของผู้ให้บริการรายหนึ่ง แต่ใช้อีเมล์ของผู้ให้บริการอินเทอร์เน็ตอีกรายหนึ่ง ทำให้ไม่สามารถส่งอีเมล์ไปยังปลายทางได้จะเกิดข้อผิดพลาดในขณะที่ทำการส่ง หรือมีอีเมล์ตีกลับ โดยแจ้งข้อความเช่นRelaying denied ที่เป็นเช่นนี้เพราะผู้ให้บริการอินเทอร์เน็ตจะอนุญาตเฉพาะผู้ใช้บริการที่ใช้เครือข่ายของตนเท่านั้นส่งอีเมล์ผ่าน SMTP Server ของตนเองได้ แต่จะไม่อนุญาตให้ผู้ใช้บริการจากเครือข่ายรายอื่น ถึงแม้ว่าผู้ใช้บริการจะใช้อีเมล์ของตนเองก็ไม่สามารถส่งอีเมล์ผ่าน SMTP Server ของตนได้ ทั้งนี้เพื่อป้องกันผู้ไม่ประสงค์ดีเข้ามาใช้อีเมล์เซิร์ฟเวอร์ของตนในการส่งสแปมหรืออีเมล์ที่ไม่พึงประสงค์ออกไปซึ่งจะทำให้ SMTP ติดBlacklistทำให้ผู้ใช้บริการไม่สามารถส่งอีเมล์ไปถึงผู้รับรายอื่นๆได้ แต่ว่า SMTP มี FeatureAuthentication เพื่ออำนวยความสะดวกให้แก่ผู้ใช้บริการอีเมล์สามารถส่งอีเมล์จากนอกเครือข่ายได้ หากผู้ใช้บริการต้องการจะส่งอีเมล์ผ่าน SMTP Server นี้จะต้องผ่านกระบวนการพิสูจน์สิทธิ์ก่อน นั่นคือ ต้องAuthenticationในการส่งอีเมล์ก่อนทุกครั้ง ในปัจจุบันโปรแกรมมีอีเมล์เวอร์ชันใหม่ ๆ ที่สนับสนุนระบบ SMTP Authentication กันหมดแล้ว จึงไม่ใช่เรื่องยากที่จะทำการตั้งค่า SMTP Authentication สำหรับ E-mail ClientSMTP Proxy เข้ามาช่วยเสริมความสามารถ ทำให้แก้ปัญหาหลักๆของระบบงานแบบเดิมได้ 3 เรื่อง

1. แก้ปัญหาIP ของผู้ให้บริการติดBlacklist
2. แก้ปัญหาในการปลอม Sender E-mail เนื่องจากต้อง Authentication ทุกครั้ง
3. แก้ปัญหา Queue ค้างเพราะว่า SMTP Proxy ต่างจาก Mail Server เนื่องจาก SMTP Proxy มีการตรวจสอบ SMTP Conversation ทีละคำสั่งจึงสามารถตรวจสอบได้ตั้งแต่ก่อนที่จะมีการถูกส่งอีเมล์สมบูรณ์ทั้งฉบับแต่ Mail Server ต้องรับอีเมล์มาก่อนทั้งฉบับแล้วค่อยตรวจสอบจึงทำให้เกิดปัญหาเรื่อง Disk, Queue อยู่

2.4 ศึกษาผลกระทบและปัญหาขององค์กรผู้ให้บริการอินเทอร์เน็ต

ผลกระทบที่มีต่อผู้ให้บริการอินเทอร์เน็ตการทำระบบป้องกันไอพีของผู้ให้บริการติด Blacklistเนื่องจากการให้บริการอินเทอร์เน็ตขององค์กรที่ให้บริการอินเทอร์เน็ตมีหลายแบบเช่น Leased Line , FTTX และ ADSLในส่วนของ Leased Line Internet จะทำการ Fixed-IP แต่ FTTX , ADSLจะไม่มีการ Fixed-IP (Dynamic-IP) จึงทำให้ผู้พัฒนาเล็งเห็นว่าองค์กรที่ให้บริการอินเทอร์เน็ตที่มีไอพีเยอะมากๆและได้แจกจ่ายให้กับผู้ใช้บริการอินเทอร์เน็ตแต่ผู้ใช้บริการส่วนใหญ่มักไม่ทราบว่าคอมพิวเตอร์ของตัวเองนั้นมีไวรัสอยู่หรือไม่โดยในบางเครื่องที่มีไวรัสอยู่นั้นจะมีการส่งสแปมเกิดขึ้นและทำการโจมตี รวมถึงการรบกวนผู้อื่นทำให้เกิดความเสียหายต่าง ๆ อาจส่งผลกระทบโดยการโดน Block-IP เนื่องจากไอพีติดBlacklistและถ้าติดBlacklistมากขึ้นเรื่อย ๆ อาจจะโดน Block -IP ทั้ง As Number ซึ่งจะส่งผลกระทบให้ผู้ใช้บริการ Static -IP ได้รับผลกระทบด้วยเนื่องจากอยู่ใน As number เดียวกัน

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

2.5 เครื่องมือที่ใช้ในการพัฒนาระบบ

เครื่องมือต่างๆเป็นจุดประสงค์หลักของการรวบรวม Open Source เพื่อทำให้โปรแกรมหรือคุณสมบัติต่างๆใช้งานร่วมกันได้

2.5.1 Linux Server

ลีนุกซ์เป็นโปรแกรมคอมพิวเตอร์ประเภทระบบปฏิบัติการตระกูลหนึ่ง เป็นระบบปฏิบัติการประเภท Unix หรือยูนิกซ์โคลนที่ใช้งานบนเครื่อง PC แต่ปัจจุบันไม่ได้ใช้งานบนเครื่อง PC เพียงอย่างเดียวสามารถใช้งานได้บนเครื่อง Server ต่างๆได้ เช่นSUN SPARCเป็นต้น ซอฟต์แวร์ระบบปฏิบัติการลีนุกซ์เป็นOpen Source ซึ่งสามารถใช้ลีนุกซ์ได้โดยไม่ต้องเสียค่าลิขสิทธิ์เป็น Unix เต็มรูปแบบในระบบ Multi User Multi Task คือการใช้งานได้ครั้งละหลายๆคน และทำงานได้ครั้งละหลายๆ งานที่มีระบบการติดต่อกับผู้ใช้งานแบบกราฟิกหรือที่เรียกว่าX-Windwowเป็นมาตรฐานสนับสนุนโปรโตคอลแบบ TCP/IP, SLIP, PPP, UUCP เป็น

ระบบปฏิบัติการ 32บิทมีประสิทธิภาพสูงมาก ทั้งที่ลีนุกซ์เป็นเพียงเคอร์เนล (Kernel) ของระบบปฏิบัติการ ซึ่งจะทำหน้าที่ในด้านของการจัดสรรและบริหารโพรเซสงานการจัดการไฟล์และอุปกรณ์ I/O ต่าง ๆ ใช้งานผ่านทางแอพพลิเคชั่นและระบบอินเทอร์เฟส เช่น Shell หรือ X วินโดวส์

2.5.2 Spam Assassin

Spam Assassin เป็นระบบที่ช่วยคัดกรอง ป้องกันจดหมายขยะหรืออีเมล์ที่ไม่พึงประสงค์ อีกทั้งยังสามารถกำหนด E-mail While list และEmail Blacklistซึ่งสามารถระบุชื่ออีเมล์หรืออีเมล์ทั้งหมดที่ถูกส่งมาจากโดเมนใดๆได้

2.5.3 ClamAV

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

2.5.4 SNMP

Simple network management protocols (SNMP) เป็นเซอร์วิสที่ให้ผู้ดูแลระบบสามารถตรวจสอบดูสถานะของการทำงานหรือจัดการเกี่ยวกับค่าคอนฟิคต่างๆของอุปกรณ์ได้ ซึ่ง SNMP จะมีประโยชน์ในการนำมาใช้มอนิเตอร์ดูการทำงานการวิ่งเข้า-ออกของทราฟฟิคที่ผ่านเครื่อง Linux ที่ทำงานในลักษณะเป็น Gateway โดยใช้ snmpwalkเพื่อใช้ในการตรวจสอบสถานะ

การทำงานของ SNMPเริ่มจากฝั่งไคลเอนต์ต้องส่งคำสั่ง SNMP Request ไปยังอุปกรณ์ที่ได้ทำการเป็นเซอร์วิสของการทำงาน SNMP ไว้แล้วพร้อมทั้งส่ง Community String เข้าไปด้วยจากนั้นอุปกรณ์จะทำการตรวจสอบ Community String ว่าถูกต้องหรือไม่ ถ้าถูกต้องจะส่งข้อมูลต่างๆที่ไคลเอนต์ร้องขอส่งกลับไปยังไคลเอนต์ ส่วนใหญ่ผู้ให้บริการอินเทอร์เน็ตที่ใช้Linux มาทำเป็น Internet Gateway จะนำ SNMPมาใช้เพื่อดูสถานะการทำงานของอุปกรณ์โดยทำการติดตั้ง SNMP บน Server Linux เครื่องนั้น

2.5.5 CACTI

CACTIคือCACTI Traffic Graph หรือเรียกกันสั้นๆว่า “CACTI”เป็น Open Source Softwareซึ่งทำหน้าที่ในการแสดงปริมาณข้อมูลทั้งขาเข้า/ออกในเครือข่ายโดยจะแสดงผลออกมาในรูปแบบของกราฟสามารถเข้าใจและเปรียบเทียบระดับการใช้งานได้ง่ายขึ้นอีกทั้งยังมี

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

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

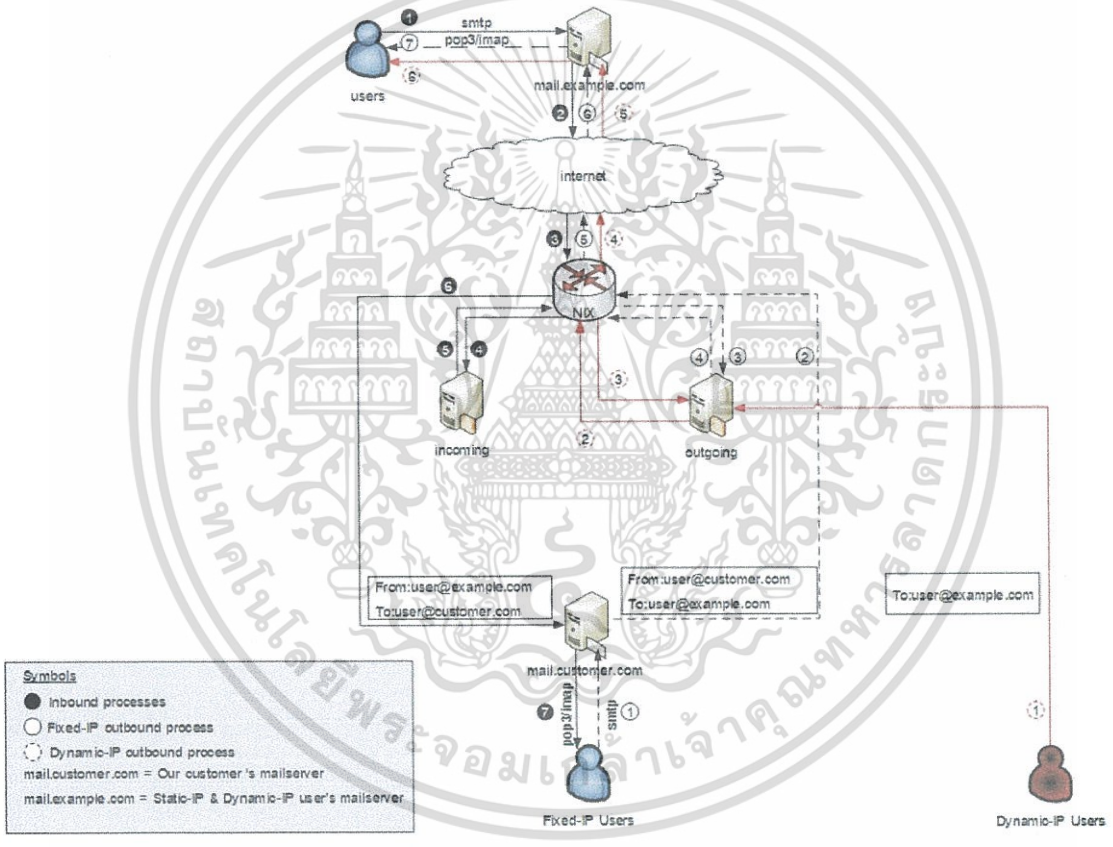
1. IP Address แบบ Static คือ IP Address ที่ผู้ให้บริการอินเทอร์เน็ตแจก IP Address ให้กับผู้ใช้บริการอินเทอร์เน็ตแต่ละคนอย่างถาวร ทำให้IP Address เหล่านี้ไม่มีการเปลี่ยนแปลงไม่ว่าจะใช้งานไปนานเท่าไหร่ อย่างไรก็ตาม ถ้ามีการใช้บริการIP Address แบบ Static IP ไปให้ผู้ใช้บริการแล้วถ้าIP address นั้นไม่ได้ถูกใช้งาน 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 Addressใดไม่ถูกใช้งานก็จะสามารถนำไปแจกต่อให้กับเครื่องคอมพิวเตอร์เครื่องอื่นที่ต้องการใช้งานต่อไปได้ และถ้าคอมพิวเตอร์เครื่องนั้นกลับมาใช้งานก็จะได้ IP Address อื่นแทนไป ไม่มีการฟิคค่าของ IP Address ตายตัวเหมือนกันIP Address แบบ Static IP

3.1.2 ภาพรวมของระบบงานเดิม

จากที่กล่าวมาข้างต้น บริษัท ทีทีแอนด์ที จำกัด (มหาชน) นั้นไม่มีการแยกระหว่างผู้ใช้บริการแบบ StaticIP และ DynamicIPทำให้เกิดปัญหาในส่วนของ Leased Line Internet จะทำการ Fixed-IPแต่ว่า FTTX , ADSLจะไม่มีการ Fixed-IP (Dynamic-IP) จึงทำให้ผู้พัฒนามองเห็นว่าองค์กรที่มีไอพีจำนวนมากและได้แจกจ่ายให้กับ User ผู้ใช้บริการอินเทอร์เน็ตแต่ไอพีติดBlacklistมากขึ้นเรื่อย ๆจากการที่ผู้ใช้บริการมักไม่เคยทราบว่าคอมพิวเตอร์ของตัวเองนั้นมีไวรัสอยู่หรือไม่ โดยในบางเครื่องที่มีไวรัสอยู่นั้นจะมีการส่งสแปมเกิดขึ้นและทำการโจมตีและรบกวนผู้อื่นทำให้เกิดความเสียหายต่างๆขึ้นจึงอาจส่งผลกระทบโดยการโดน Block-IPเนื่องจากไอพีติดBlacklistและถ้าติดBlacklistมากขึ้นๆจนโดน Block IP นั้นไปหรืออาจโดนทั้งAs Number ซึ่งอาจจะส่งผลกระทบให้ผู้ใช้บริการ Static IPได้รับผลกระทบด้วยเนื่องจากอยู่ใน As number เดียวกันวิธีการแก้ปัญหาเบื้องต้นโดย Block Destination Port 25 และให้ส่งผ่าน Mail Gateway ของISP แทนแต่ก็

ยังมีปัญหาอื่นตามมาเช่นมีการจงใจส่งสแปมของ Hacker หรือคอมพิวเตอร์พนักงานบริษัทติดไวรัส ก็จะมีการส่งสแปมเกิดขึ้นในจำนวนมากๆแล้วนั้นจะทำให้ Mail gateway ขององค์กรเกิดคิวค้างในจำนวนมาก, User ปลอม Sender E-mail, ไอพีของ Mail Gateway ถูก block เนื่องจากมีอีเมล์บางฉบับที่ Mail Gateway ตรวจสอบไม่พบสแปมทำให้สามารถส่งออกไปยังปลายทางได้, ทำงานไม่ทัน, รับทราฟฟิคไม่ไหวจึงเกิด 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 3.1ภาพรวมของระบบงานเดิม

การส่งอีเมล์ขาออก

1. ส่วนของ Leased Line User การส่งออกอีเมล์ของผู้ใช้งาน Leased Line จะส่งผ่านเมล์เซิร์ฟเวอร์ของผู้ให้บริการอินเทอร์เน็ต แล้วผ่าน Mail gateway ก่อนที่จะส่งออกไปยังปลายทาง

2. ส่วนของ ADSL User การส่งออกอีเมล์ของผู้ใช้งาน ADSL จะไม่มีเมล์เซิร์ฟเวอร์และถูกบล็อคSmtp Connection ที่ส่งไปยังเมล์เซิร์ฟเวอร์อื่น ๆ แต่ให้ส่งผ่าน Mail Gatewatของผู้ให้บริการอินเทอร์เน็ตแทน

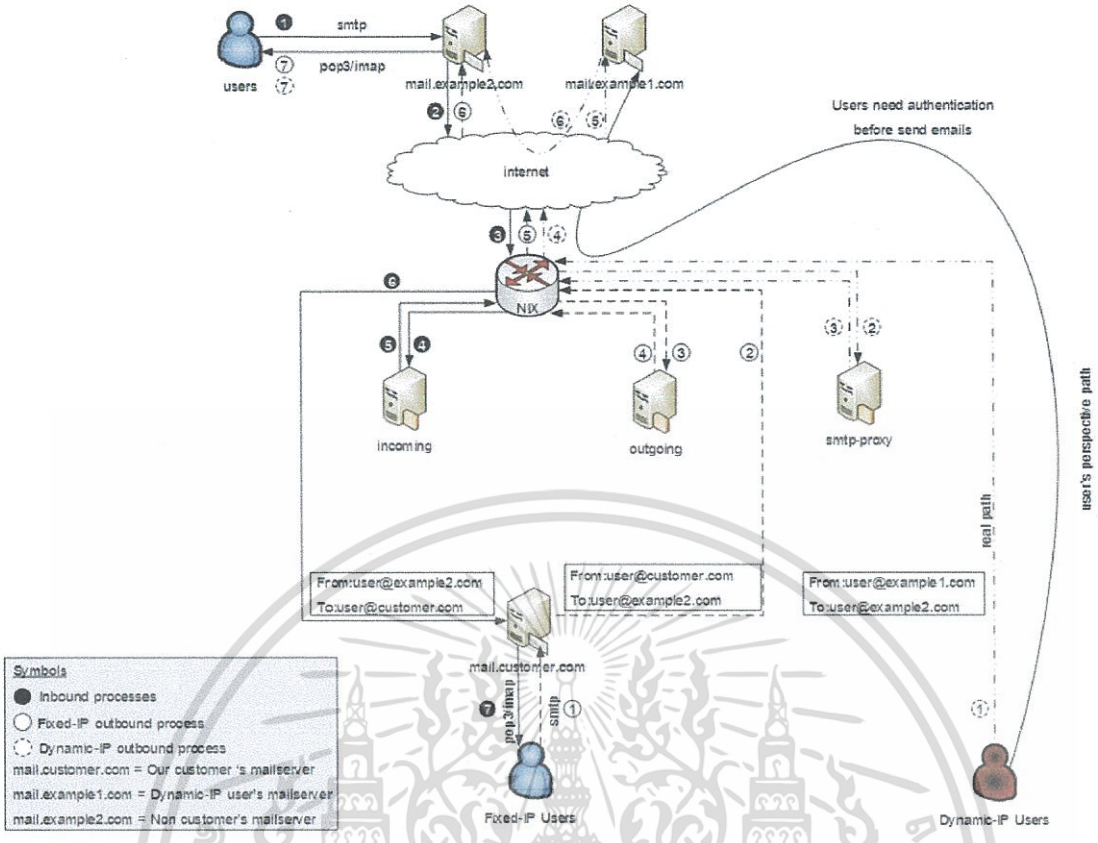
การรับอีเมล์ขาเข้า

1. ผู้ใช้บริการที่มีเมล์เซิร์ฟเวอร์เป็นของตัวเองหรือให้ผู้ให้บริการกรองอีเมล์ให้ แล้วส่งต่อไปยังเซิร์ฟเวอร์ลูกค้า โดยจะมีการตั้งค่า MX Record เป็น Mail Gateway ของผู้ให้บริการอินเทอร์เน็ต

2. ลูกค้าที่มีเมล์เซิร์ฟเวอร์ และรับอีเมล์เองได้โดยไม่ใช้บริการในส่วนของการคัดกรองอีเมล์ของผู้ให้บริการอินเทอร์เน็ตโดยจะมีการตั้งค่า MX Record เป็นของผู้ใช้บริการเอง เช่น เมล์เซิร์ฟเวอร์ของผู้ใช้บริการ หรือ Mail Gateway ของผู้ใช้บริการ

3.2 วิเคราะห์ระบบงานใหม่

จากที่ผู้พัฒนาได้ศึกษาแนวทางและแนวคิดต่างๆที่เกี่ยวข้องกับระบบงานใหม่และปัญหาต่างๆของระบบงานเดิมจึงมีแนวคิดที่จะพัฒนาระบบขึ้นมาใหม่เพื่อแก้ไขปัญหาของระบบงานเดิม ดังกล่าวปัญหานี้สามารถแก้ให้หมดไปได้โดยวิธีการ แยกประเภทลูกค้าโดย อนุญาตให้ลูกค้าแบบ Static IP เท่านั้นที่จะสามารถส่งอีเมล์ผ่าน SMTP Gateway ของผู้ให้บริการได้ ส่วนลูกค้าประเภท Dynamic IP อนุญาตให้ส่งไปยัง SMTP Server ต้นทางแบบมีเงื่อนไขโดยจะต้องมีการทำ STMP Authencationเพราะ มีเพียงผู้ส่งตัวจริงเท่านั้นที่ทำได้ แต่แสปมเมอร์ทำไม่ได้ การแยก Mail Gateway กันระหว่าง Static-IP และ Dynamic-IP และคุณสมบัติต่างๆของ Protocol SMTP ในการแก้ปัญหาต่างๆ ได้ เช่น SMTP Authentication และเพิ่ม Filter ต่างๆเพื่อเข้าไปช่วยในการจัดการในด้านป้องกัน Virus และ Spam เช่น Spam Assassin, Clam AV และประยุกต์ใช้ Protocol SNMP ในการดึงค่า Stat ต่างๆออกมา พร้อมทั้ง ใช้โปรแกรมประยุกต์ CACTIเพื่อแสดงปริมาณข้อมูลทั้งขาเข้า/ออกในเครือข่ายโดยจะแสดงผลออกมาในรูปแบบของกราฟสามารถเข้าใจและเปรียบเทียบระดับการใช้งานได้ง่ายขึ้นเพื่อวัดประสิทธิภาพของการทำงานเพราะฉะนั้นระบบงานใหม่ จะสามารถป้องกันการโดน Block IP เนื่องจากผู้ใช้ที่เป็น Dynamic-IP จะต้องวิ่งผ่านทาง Mail Proxy หรือ Proxy Server ที่เราสร้างขึ้นมาใหม่นี้เพราะฉะนั้น Hacker จะไม่สามารถปลอมแปลง User และนำ Account ของผู้ใช้บริการไปส่ง Spam ได้ เพราะว่าต้องผ่านการ Authentication ของระบบงานก่อน ในระบบงานใหม่นี้ก็ยังสามารถ Scan Virus และ Check Spam ต่างๆได้ สามารถดึงค่า Stat ต่างๆ พร้อมทั้ง Monitor Graph ดู Traffic ต่างๆได้ เช่น Memory , CPU ระบบงานใหม่ที่สร้างขึ้นนี้จะทำงานบน Platform ที่เป็น Linux Server และในส่วนของการ Plot Graph สามารถใช้งานผ่าน Web Application ได้เนื่องจาก Cacti เป็น Web-Based Application



รูปที่ 3. 2ภาพรวมของระบบงานใหม่

การส่งอีเมล์ขาออก

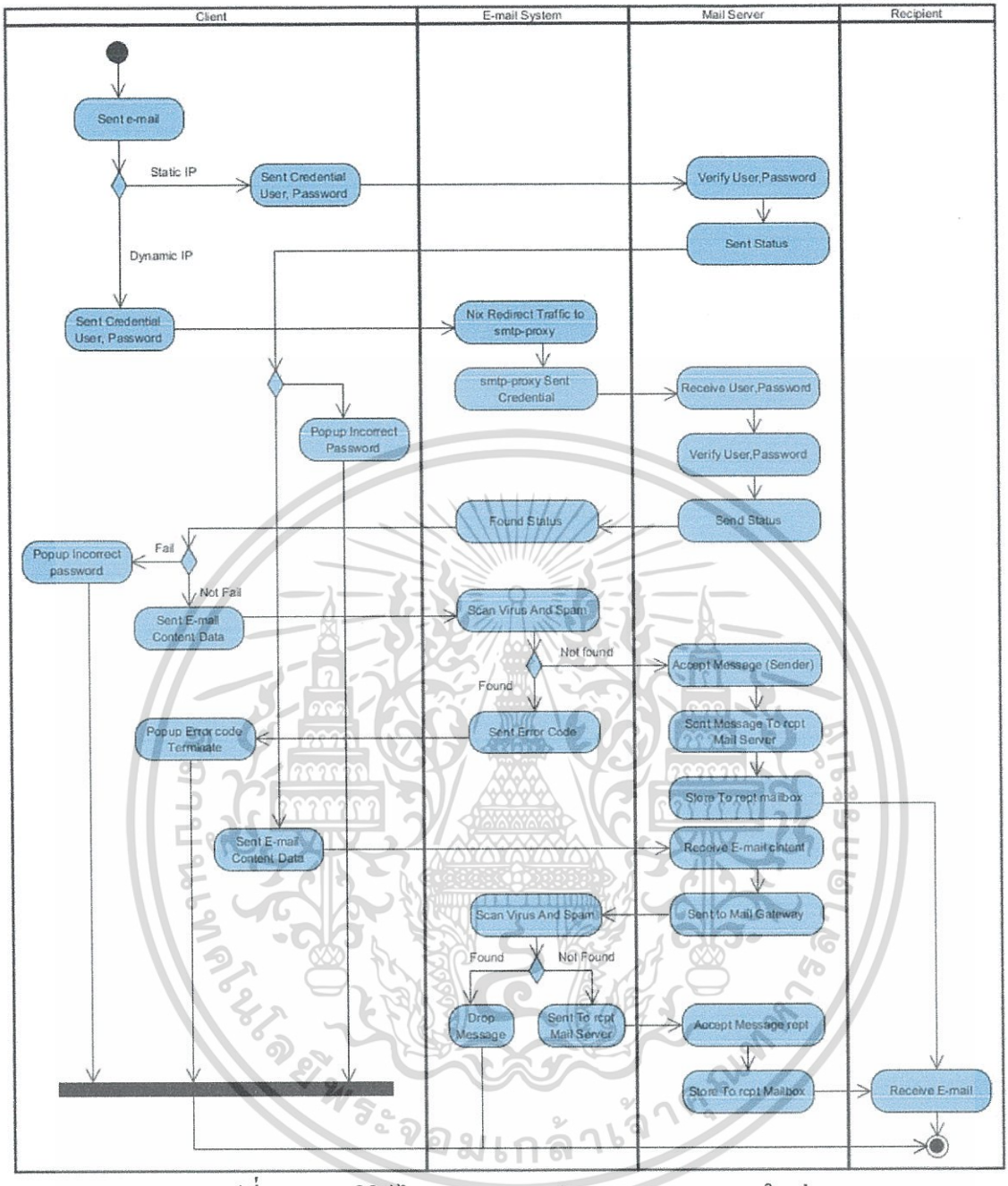
1. ส่วนของ Leased Line User การส่งออกอีเมล์ของผู้ใช้งาน Leased Line จะส่งผ่านเมล์เซิร์ฟเวอร์ของผู้ให้บริการอินเทอร์เน็ต แล้วผ่าน Mail gateway ก่อนที่จะส่งออกไปยังปลายทาง

2. ส่วนของ ADSL User การส่งออกอีเมล์ของผู้ใช้งาน ADSL ไม่ใช้วิธีการ block ทุกๆ smtp connection เหมือนระบบงานเดิม แต่ใช้ smtp proxy block เฉพาะ smtp connection ที่ไม่มีการ authenticate เท่านั้นและไม่อนุญาตให้ส่งผ่าน mail gateway เหมือนระบบงานเดิม

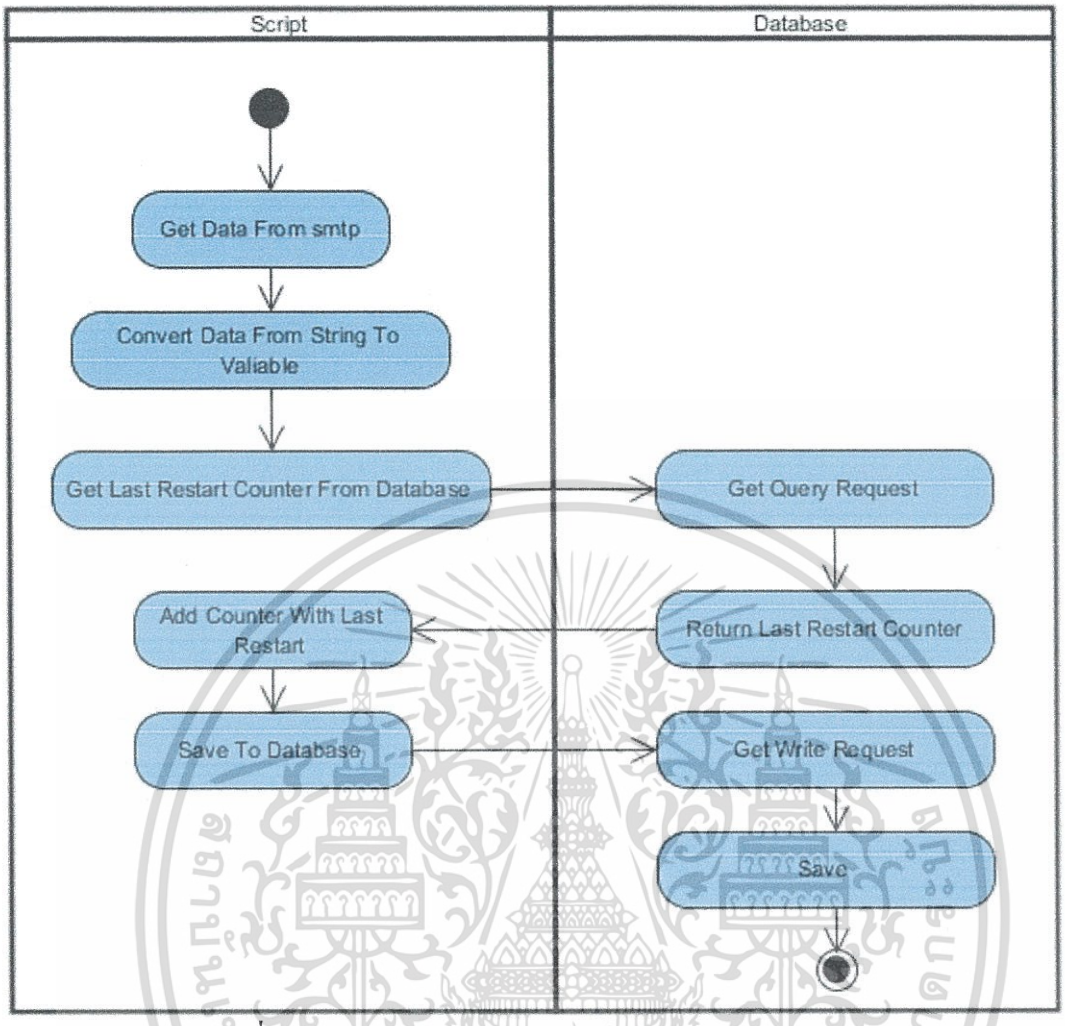
การรับอีเมล์ขาเข้า

1. ผู้ใช้บริการที่มีเมล์เซิร์ฟเวอร์เป็นของตัวเองหรือให้ผู้ให้บริการกรองอีเมล์ให้ แล้วส่งต่อไปยังเซิร์ฟเวอร์ลูกค้า โดยจะมีการตั้งค่า MX Record เป็น Mail Gateway ของผู้ให้บริการอินเทอร์เน็ต

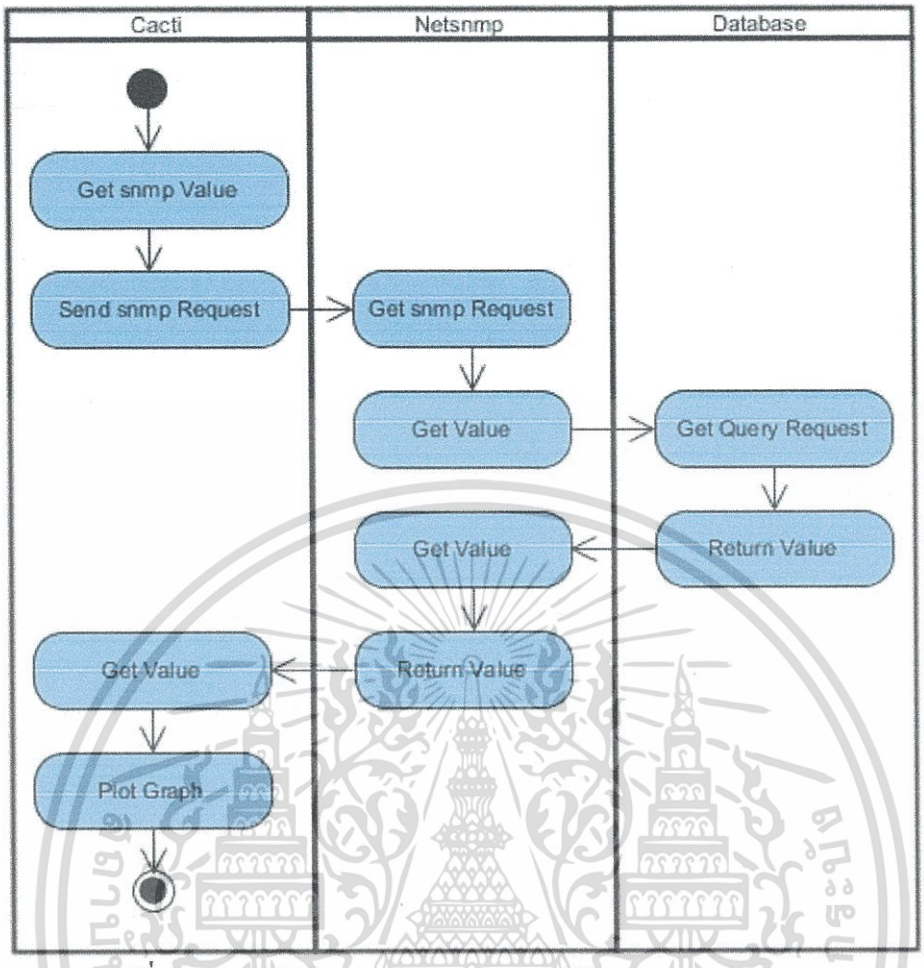
2. ลูกค้าที่มีเมล์เซิร์ฟเวอร์ และรับอีเมล์เองได้โดยไม่ใช้บริการในส่วนของการคัดกรองอีเมล์ของผู้ให้บริการอินเทอร์เน็ต โดยจะมีการตั้งค่า MX Record เป็นของผู้ใช้บริการเอง เช่น เมล์เซิร์ฟเวอร์ของผู้ใช้บริการ หรือ Mail Gateway ของผู้ใช้บริการ



รูปที่ 3. 3แอคทิวิตีไดอะแกรมการทำงานของระบบงานใหม่



รูปที่ 3. 4แอคทิวิตีไดอะแกรมการเก็บข้อมูลค่าสถิติลงดาต้าเบส



รูปที่ 3. 5แอคทิวิตี้ไดอะแกรมการนำค่าสถิติมาวาดกราฟแสดงผล

บทที่ 4
การทดสอบและผลการทดสอบ

4.1 บทนำ

จากการวิเคราะห์และออกแบบระบบงานในบทที่ 3 ในบทนี้จะกล่าวถึงการทดลองและผลการทดลองระบบป้องกันไอพีของผู้ให้บริการอินเทอร์เน็ตติดบัญชีดำโดยมีรายละเอียดดังนี้

- การทดสอบ
- ผลการทดสอบ

4.2 การทดสอบ

การทดสอบการทำงานของระบบป้องกันไอพีของผู้ให้บริการอินเทอร์เน็ตติดบัญชีดำจะทำการทดสอบการทำงานโดยการทดสอบจัดทำการทดสอบโดยผู้จัดทำปัญหาพิเศษเองซึ่งเป็นการทดสอบโดยรวมทั้งหมดว่าระบบงานมีกระบวนการทำงานที่ถูกต้องตามวัตถุประสงค์ที่กำหนดไว้หรือไม่ 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 ก่อนการส่งอีเมล์เพื่อทำการวิเคราะห์ว่า มีการส่งอีเมล์ที่เป็น Viruses, Spam หรือไม่

กรณีที่ 1 กรณีที่ส่ง Viruses ในอีเมล์ส่งต่อไปยังผู้อื่นค่าสถิติก็จะเพิ่มในส่วนของ Viruses

กรณีที่ 2 กรณีที่ส่ง Spam ในอีเมล์ส่งต่อไปยังผู้อื่นค่าสถิติก็จะเพิ่มในส่วนของ Spam

กรณีที่ 3 กรณีที่ No-Authenticationการส่งอีเมล์โดยไม่ผ่านการเข้ารหัส ค่าสถิติก็จะเพิ่มในส่วนของ 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. 1ค่าสถิติก่อนการตรวจสอบ 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 RequestTotalเป็นการ Traffic ที่ขอใช้บริการรวมทั้งหมดผ่าน Server นี้ค่าสถิติก็จะเพิ่มในส่วนของ RequestTotal

กรณีที่ 2 การ Request Directเป็น Section ที่ถูก Encryption โดย TLS Protocols โดยที่ smtpจะปล่อยผ่าน เนื่องจากเป็นการถูกเข้ารหัส ค่าสถิติก็จะเพิ่มในส่วนของ Request Direct

กรณีที่ 3 การ RequestEmptyเป็นการร้องขอแต่ไม่ได้ใช้บริการ รวมทั้งการส่งอีเมล์ไม่สำเร็จและ Transaction ไม่ครบค่าสถิติก็จะเพิ่มในส่วนของ RequestEmpty

```
[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)
```

รูปที่4. 2ค่าสถิติก่อนการตรวจสอบRequests

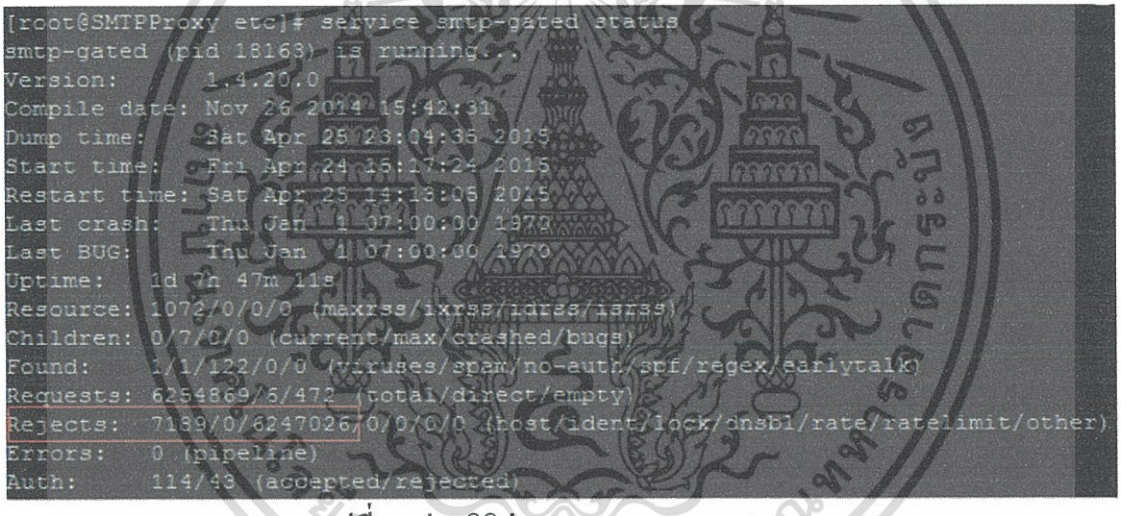
4.2.3 การทดสอบ Reject ประกอบไปด้วย Host, Ident, Lock,Other

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

กรณีที่ 1 การ Reject Hostการปฏิเสธ Host ที่ขอใช้บริการเนื่องจากมีการขอใช้บริการติดต่อกันเกินลิมิตที่ตั้งไว้ค่าสถิติก็จะเพิ่มในส่วนของReject Host

กรณีที่ 2 การ Reject Lockโดยการ Lock IP-Address ของผู้ที่โจมตีผู้ใช้บริการรายอื่นไม่ว่าจะเป็นการโจมตีด้วยรูปแบบ Viruses หรือการส่ง Request ขอใช้บริการต่อๆกันในจำนวนมากๆระบบก็จะทำการ Lock IP-address ไว้ทำให้ไม่สามารถส่ง Viruses ให้ผู้ใช้บริการรายอื่นได้อีกค่าสถิติก็จะเพิ่มในส่วนของ Reject Lock

กรณีที่ 3 การ Reject Otherเป็นการปฏิเสธในช่องทางอื่นๆ ค่าสถิติก็จะเพิ่มในส่วนของ Reject Other



รูปที่4. 3ค่าสถิติก่อนการตรวจสอบRejects

4.2.4 การทดสอบAuthenticationประกอบไปด้วย Accepted, Rejected

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

กรณีที่ 1 ผ่านการ Authentication เพื่อทำการส่งอีเมล์อย่างถูกต้องค่าสถิติก็จะเพิ่มในส่วนของ Accepted

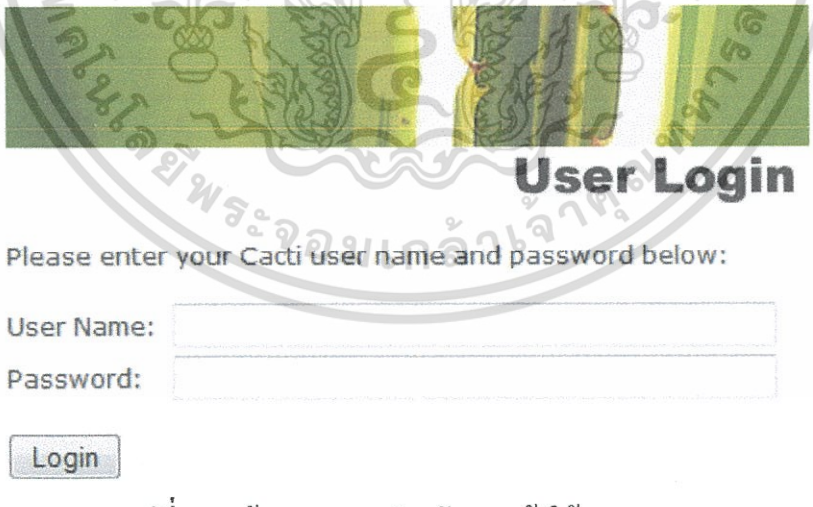
กรณีที่ 2 ไม่ผ่านการ Authentication เพื่อทำการส่งอีเมล์ ไม่ว่าจะเป็นการใส่รหัสผู้ใช้ผิดหรือมีเจตนาไม่ใส่ก็ตามค่าสถิติก็จะเพิ่มในส่วนของ Rejected

```
[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/isrss)
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)
```

รูปที่4. 4ค่าสถิติก่อนการตรวจสอบAuthtication

4.3 ผลการทดสอบ

ผลของการทดสอบระบบป้องกันไอพีของผู้ให้บริการอินเทอร์เน็ตติดบัญชีดำ จะมีส่วนติดต่อสำหรับผู้ใช้งานโดยผู้ใช้งานจะเป็นเจ้าหน้าที่ในหน่วยงานบริการอินเทอร์เน็ต เพื่อ Monitor ดูการเปลี่ยนแปลงของระบบงานให้เข้าใจได้ง่ายขึ้น โดยผ่านWeb Application ที่แสดงผลออกมาในรูปแบบของกราฟ การเข้าสู่ระบบ ผู้ใช้งานจะต้องระบุรหัสผู้ใช้งานและรหัสผ่านให้ถูกต้องเพื่อเข้าใช้งานระบบ แสดงดังภาพที่ 4.5

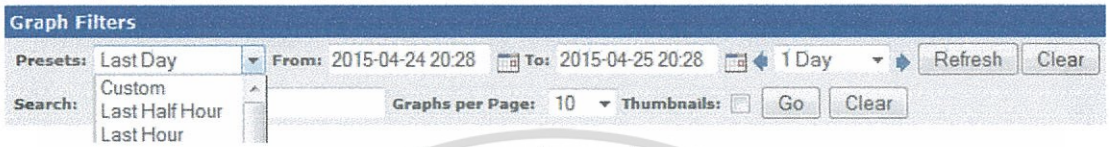


รูปที่4. 5หน้าจอ Login สำหรับการเข้าใช้งานระบบ

เมื่อเข้ามาสู่ระบบแล้วจะต้องทำการเลือกที่เมนู Graphs เพื่อทำการ Monitor สถานะของ Graphs แต่ละประเภทแสดงดังภาพ 4.6

รูปที่4. 6เลือกเมนู Graphs

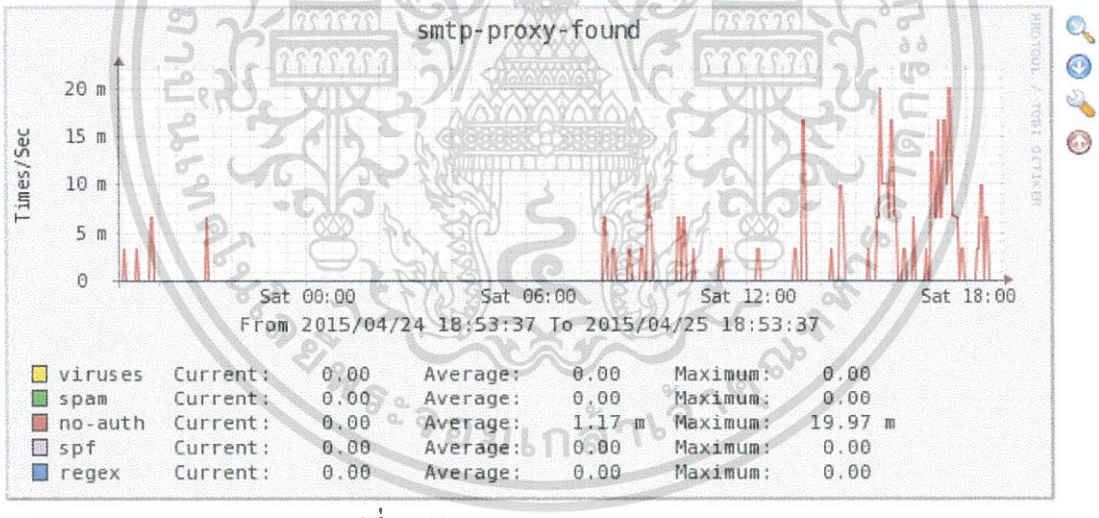
หน้าจอสำหรับเลือกเงื่อนไขที่ต้องการเฉพาะเจาะจงมากยิ่งขึ้น สามารถเลือกช่วงเวลาที่ต้องการดูกราฟได้ตามต้องการ และสามารถเลือกจำนวนที่ต้องการแสดงผลได้ แสดงดังภาพ 4.7



รูปที่4. 7เลือกเงื่อนไขที่ต้องการ

ดังนั้นผลการทดลองที่เกิดขึ้นจะประกอบไปด้วยผลการทดสอบตามวัตถุประสงค์ที่กำหนดดังนี้

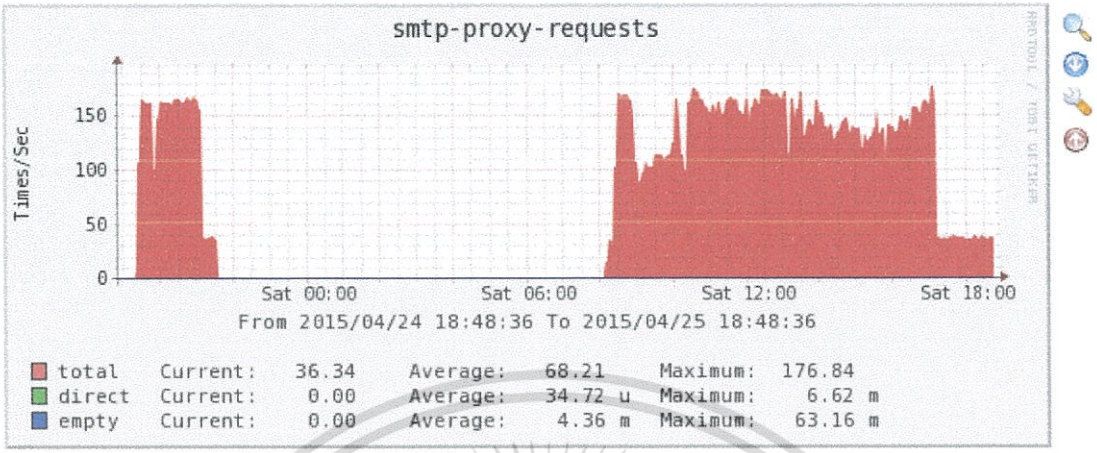
4.3.1 ผลการทดสอบ Found



รูปที่4. 8ตัวอย่างผลการทดสอบ Found

จากกราฟแสดงข้อมูลของผู้ที่ไม่ได้ทำการ Authentication เข้ามาใช้งานอย่างถูกต้องทำให้ในช่วงเวลาดังกล่าวมีกราฟที่เป็นสีแดงมาก แต่ในขณะเดียวกันนั้นยังไม่พบ Viruses และ Spam

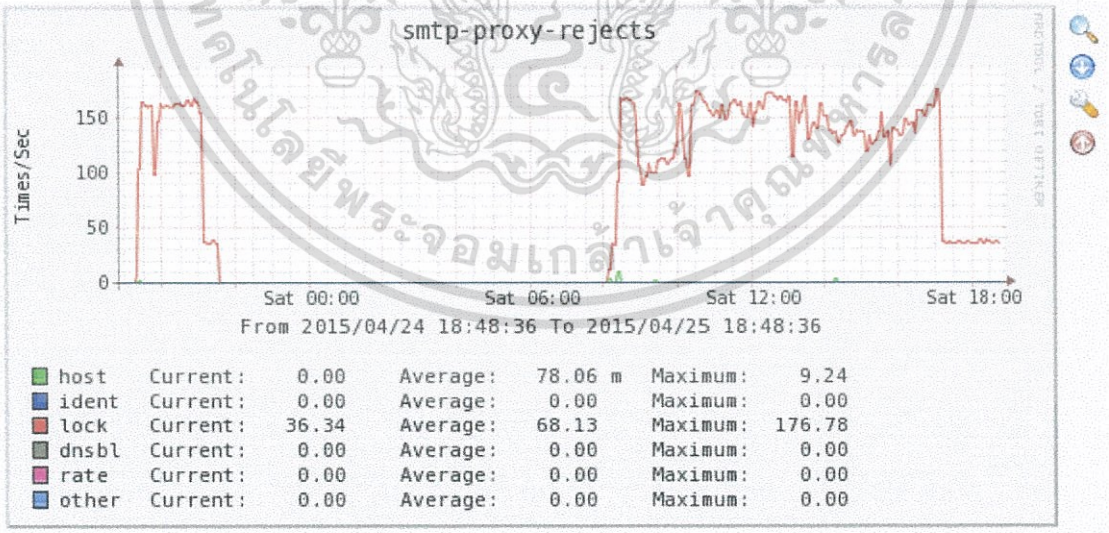
4.3.2 ผลการทดสอบ Requests



รูปที่ 4. 9ตัวอย่างผลการทดสอบ Requests

จากกราฟแสดงข้อมูลของการ Requests ขอใช้บริการเป็นจำนวนมาก จึงทำให้เวลาดังกล่าวมรกราฟเป็นสีแดง ในส่วนของ RequestsDirect,Requests Empty นั้นมีจำนวนที่น้อยมากจึงทำให้กราฟที่ออกมาไม่สามารถแสดงภาพได้อย่างชัดเจน

4.3.3 ผลการทดสอบ Rejects

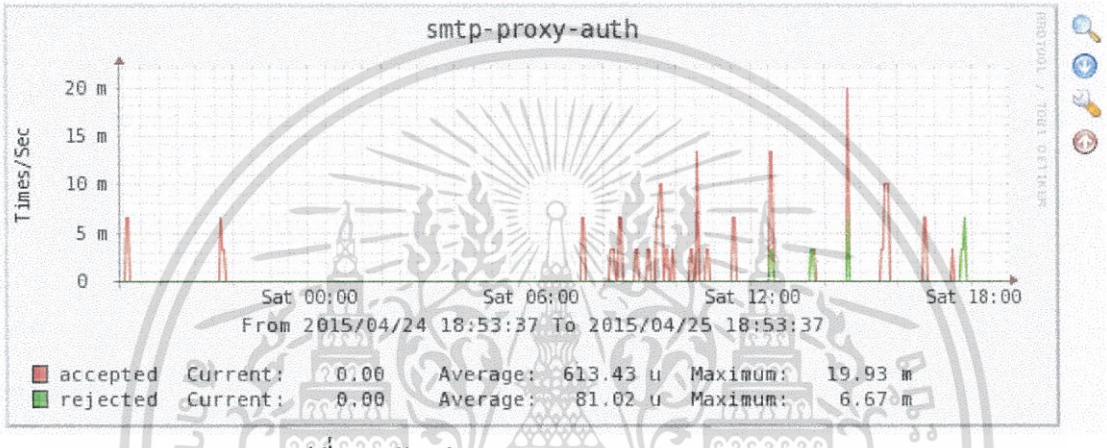


รูปที่4. 10ตัวอย่างผลการทดสอบ Reject

จากกราฟแสดงข้อมูลของการ Reject พบว่าระบบงานมีการ RejectLock อย่างมากในเวลาดังกล่าวจึงทำให้กราฟเป็นสีแดงอย่างเห็นได้ชัดเนื่องจากในช่วงเวลาดังกล่าวโดยการมีการ Lock IP-Address ของผู้ที่โจมตีผู้ใช้บริการรายอื่นด้วยรูปแบบการคุกคามต่างๆ ไม่ว่าจะเป็นโดน Lock

จากการส่ง Viruses, Spam หรือการการส่ง Request ขอใช้บริการต่อๆกันในจำนวนมากๆระบบก็จะทำการ Lock IP-address ไว้ทำให้ไม่สามารถส่ง Viruses, Spam ให้ผู้ใช้บริการรายอื่นได้ทั้งนี้ถ้าผู้ใช้บริการอินเทอร์เน็ตต้องการปลดล็อคเพื่อทำการใช้งานต้องติดต่อเจ้าหน้าที่ผู้ให้บริการอินเทอร์เน็ตโดยตรงเพื่อทำการแก้ไขในลำดับต่อไปในส่วนของการ Reject Host มีข้อมูลเพียงเล็กน้อยเท่านั้น

4.3.4 ผลการทดสอบ Authentication



รูปที่4. 11ตัวอย่างผลการทดสอบAuthentication

จากกราฟแสดงข้อมูลของการ Authentication จะพบว่า กราฟ Accepted จะมีจำนวนที่สูงมากเนื่องจาก ผู้ที่ทำการส่งอีเมล์ส่วนใหญ่จะเป็นผู้ส่งที่ถูกต้องผ่านการ Authentication มาเป็นส่วนใหญ่ และไม่ทำการAuthentication เพื่อทำการส่งอีเมล์หรือการใส่รหัสผู้ใช้ผิดหรือมีเจตนาไม่ใส่รหัสผู้ใช้ที่ถูกต้อง เพียงเล็กน้อยเท่านั้น

บทที่ 5
สรุปผลและข้อเสนอแนะ

5.1 บทนำ

จากการดำเนินงานที่กล่าวมา เป็นการจัดทำระบบป้องกันไอพีของผู้ให้บริการอินเทอร์เน็ตติดบัญชีดำ เพื่อสนับสนุนการปฏิบัติงานของ บริษัท ทีทีแอนด์ที จำกัด (มหาชน) ซึ่งจากการจัดทำระบบและทดสอบการใช้งานภายในองค์กรจึงสามาถสรุปผลและอภิปลายการดำเนินงานได้ดังนี้

5.2 สรุปผลและอภิปลายการดำเนินงาน

จากผลการดำเนินงานพบว่าการนำโปรโตคอลหลักที่ใช้ในการรับ-ส่งอีเมล์ คือ SMTP มาใช้เพื่อวิเคราะห์หลักการทำงาน เพื่อนำจุดเด่นมาใช้งาน และปรับปรุงจุดด้อยของโปรโตคอล โดยการนำ Filter ต่างๆ อย่างเช่น Clamav, Spamassassin, Snmpที่มีส่วนช่วยในการเพิ่มประสิทธิภาพของ SMTP เพิ่มเข้าไปเพื่อลดจุดด้อยของ SMTP Proxy ให้มีประสิทธิภาพและป้องกัน Spam และ Virus ต่างๆ ที่จะส่งผลกระทบต่อการติดบัญชีดำของ IP-Address ซึ่งจะส่งผลกระทบต่อองค์กร รวมทั้งยังใช้เทคโนโลยี Web Applications ในการพัฒนาระบบให้สอดคล้องกับกระบวนการทางธุรกิจการให้บริการอินเทอร์เน็ตในการแก้ไขปัญหา ทำให้สามารถดูวิเคราะห์หาสาเหตุและเปรียบเทียบได้อย่างแท้จริงและวัดผลได้จากการที่ IP-Address ของผู้ให้บริการอินเทอร์เน็ตติดบัญชีดำได้น้อยลง ซึ่งสิ่งต่างๆเหล่านี้เป็นผลดีต่อผู้ให้บริการอินเทอร์เน็ตโดยตรง

5.3 ปัญหาและอุปสรรคในการทดลอง

ปัญหาและอุปสรรคที่พบระหว่างการพัฒนาระบบงาน คือ การนำ Range Dynamic IP จริงของผู้ใช้งานอินเทอร์เน็ตมาทดสอบต้องมีความระมัดระวังอย่างมากเพราะอาจส่งผลกระทบต่อผู้ใช้งานและผู้ให้บริการอินเทอร์เน็ตได้ เนื่องจากระบบยังใหม่อยู่อาจจะมีการทำงานบางส่วนที่ยังไม่ครอบคลุมดีพอ จึงต้องนำไปปรับปรุงแก้ไขและพัฒนาต่อไปในอนาคตต่อไปรวมถึงช่วงเวลาในการทดสอบที่สั้นอาจทำให้ผลลัพธ์ที่ออกมาไม่ชัดเจนมากพอ แต่ก็เพียงพอที่จะสามารถทดสอบสมรรถภาพของระบบงานได้

5.4 ข้อเสนอแนะ

การจัดทำระบบป้องกันไอพีของผู้ให้บริการอินเทอร์เน็ตติดบัญชีดำในครั้งนี้มีข้อเสนอแนะสำหรับการพัฒนาเพิ่มเติมดังนี้ ควรพัฒนาเพิ่มเติมในส่วนของ SPF Record (Sender Policy Framework) ซึ่งเป็นระบบที่ช่วยป้องกันการดักจับ Spam Mail อีกวิธีหนึ่งซึ่งเป็นที่นิยมใช้กันมาก ซึ่งจะช่วยทำให้ระบบงานที่จัดทำมีสมรรถภาพที่ดียิ่งขึ้น

บรรณานุกรม

เรืองไกร รังสิพล.2545, **เปิดโลก Firewall และ Internet Security.**พิมพ์ครั้งที่ 1.กรุงเทพฯ: โปรวิชั่น

ธวัชชัย ชมศิริ.2547,**ติดตั้ง/ดูแล ระบบเครือข่ายคอมพิวเตอร์อย่างมืออาชีพ.**พิมพ์ครั้งที่ 1.กรุงเทพฯ: ซีเอ็ดยูเคชั่น

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