การปรับแต่งระบบอีเมล์ให้มี SPF บน DNS และบน Mail Server

โดย อดิศร ขาวสังข์

จัดทำเมื่อ 13 มิถุนายน 2553

อ้างอิง http://wiki.ubuntu.org.cn/UbuntuHelp:Postfix/SPF#SPF_Package_selection_and_installation ,
http://hosting.intermedia.net/support/kb/default.asp?id=1010

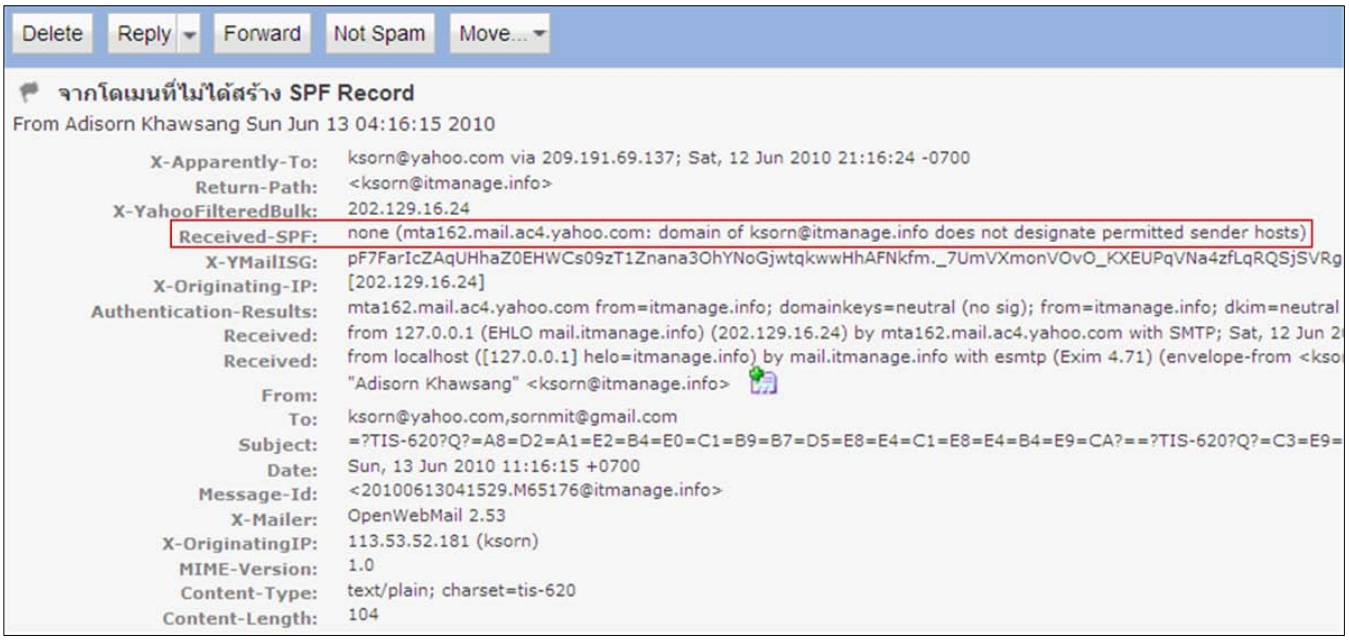
บทนำ

เนื่องจากมี Spam ที่เกิดจากการปลอม Address เกิดขึ้นจำนวนมาก ทำให้ ISP ได้ Implement มาตรฐานใหม่ขึ้นมาชื่อว่า Sender Policy Framework (SPF) ซึ่งเป็นมาตรฐานที่หลายๆ Provider (Hotmail, Yahoo, AOL, etc) ได้นำมาใช้งาน โดย Provider ดังกล่าวได้ใช้ SPF (มีการติดตั้ง SPF Package เพิ่มเติมบน Mail Server) เพื่อกำหนดว่าจะอนุญาตให้ email ต่างๆ สามารถผ่านหรือเข้ามาที่เครือข่ายของตนเองได้หรือไม่ ทำให้ระบบ mail ต่างๆ ที่ต้องการจะส่งเมล์ไปยัง Provider ดังกล่าวต้องมีการสร้าง SPF Record (การสร้าง list ไว้ใน DNS) เพื่อให้ Domain ของเขาได้รับการยอมรับจาก Provider ดังกล่าวนั้น

อีกความหมายหนึ่ง SPF เป็นเทคโนโลยีขัดขวางการปลอมอีเมล์ (e-mail anti-forgery technology) ที่ยอมให้เจ้าของโดเมนต้นทางสร้างรายชื่อ (list) ไว้ใน Domain Name Service (DNS) ของตัวอง เพื่อให้โดเมนปลายทางยอมรับ (authorized) อีเมล์ที่มาจากโดเมนต้นทางของตัวเอง ในส่วนของผู้ที่เป็นโดเมนปลายทาง การตัดสินว่าจะรับหรือไม่รับอีเมล์ที่มาจากโดเมนต้นทางนั้นจะต้องมีการติดตั้งโปรแกรมเพิ่มเติมบน Mail Server ของตัวเอง

การปรับแต่ง DNS

เมื่อเราทดสอบส่งเมล์จากโดเมนที่ไม่มีการสร้าง SPF Record บน DNS ประจำโดเมน ซึ่งในที่นี้ผู้เขียนทดสอบการส่งเมล์จากโดเมน itmanage.info ไปยังเว็บเมล์ที่นิยมใช้กัน เช่น yahoo mail หรือ Gmail จะได้ผลการรับเมล์แบบ Full Header ดังรูปที่ 1 (เป็นตัวอย่างของ yahoo mail) ซึ่งจากรูปจะเห็นว่าในรายละเอียดที่เป็น Received-SPF เป็น none

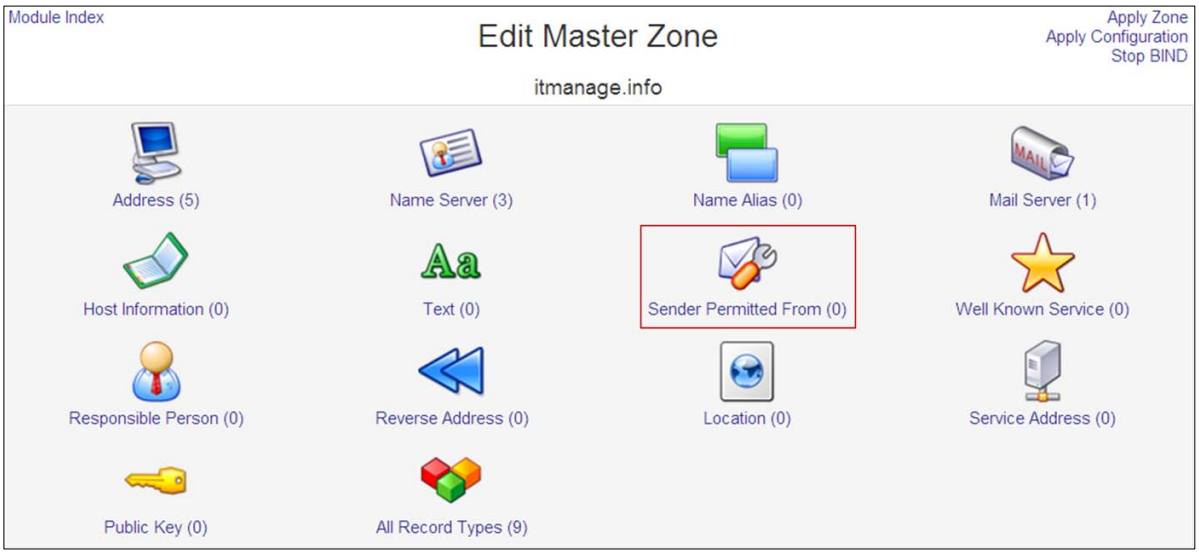


รูปที่ 1 แสดงตัวอย่างการรับของ Yahoo ที่รับจากโดเมนที่ไม่ได้สร้าง SPF record ไว้บน DNS ประจำโดเมน

การไม่สร้าง SPF Record บน DNS Server ประจำโดเมน itmanag.info อาจจะส่งผลให้ Yahoo ไม่รับอีเมล์จากโดเมนนี้ได้ ดังนั้นเพื่อความสมบูรณ์ของระบบอีเมล์ เราควรจำทำการสร้าง SPF Record บน DNS Server ประจำโดเมน ซึ่งในที่นี้

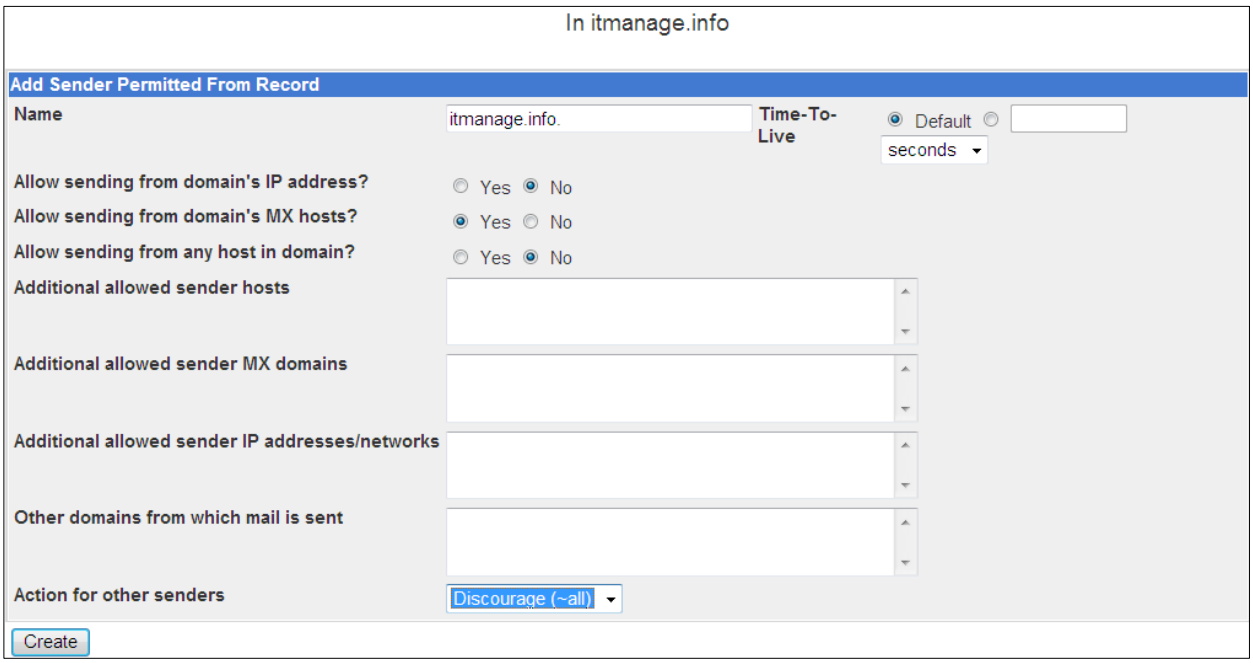
เพื่อความง่ายผู้เขียนขอใช้โปรแกรม Webmin ที่ได้ติดตั้งไว้บน DNS Server ที่เก็บข้อมูลโดเมนของ itmanage.info โดยมีขั้นตอนดังนี้

1. เลือกรายการ Sender Permitted From ในส่วน Edit Master Zone บนเครื่อง DNS Server ที่เป็น Master ดังรูปที่ 2



รูปที่ 2 ส่วนของ Edit Master Zone บน Master DNS Server ผ่านโปรแกรม Webmin

2. สร้าง SPF Record ดังตัวอย่างในรูปที่ 3 ซึ่งค่าหรือออฟชั่นต่าง ๆ สามารถเปลี่ยนแปลงได้ตามความเหมาะสม แล้วทำการบันทึกค่า



รูปที่ 3 ตัวอย่างการสร้าง SPF Record บน Master DNS Server

3. จากนั้นจะได้ค่า spf ดังรูปที่ 4

Name	TTL	SPF specification
itmanage.info.	Default	v=spf1 mx ~all

รูปที่ 4 ตัวอย่างค่า spf

4. ซึ่งเมื่อทำการเปิดไฟล์ /etc/bind/itmanage.info.hosts บน Master DNS Server ของโดเมนที่ผู้เขียนได้ทดลองแล้วจะเห็นว่ามีการเพิ่ม SPF Record เป็นชนิด txt ในบรรทัดสุดท้าย ดังรูปที่ 5

```
itmanage.info.   IN      NS      ns1.itmanage.info.
itmanage.info.   IN      NS      ns3.itmanage.info.
ns1.itmanage.info.       IN      A       202.129.16.32
ns2.itmanage.info.       IN      A       202.129.16.35
www.itmanage.info.       IN      A       202.129.16.28
itmanage.info.   IN      MX      5 mail.itmanage.info.
mail.itmanage.info.      IN      A       202.129.16.24
itmanage.info.   IN      NS      ns2.itmanage.info.
ns3.itmanage.info.       IN      A       202.129.16.17
itmanage.info.   IN      TXT     "v=spf1 mx ~all"
```

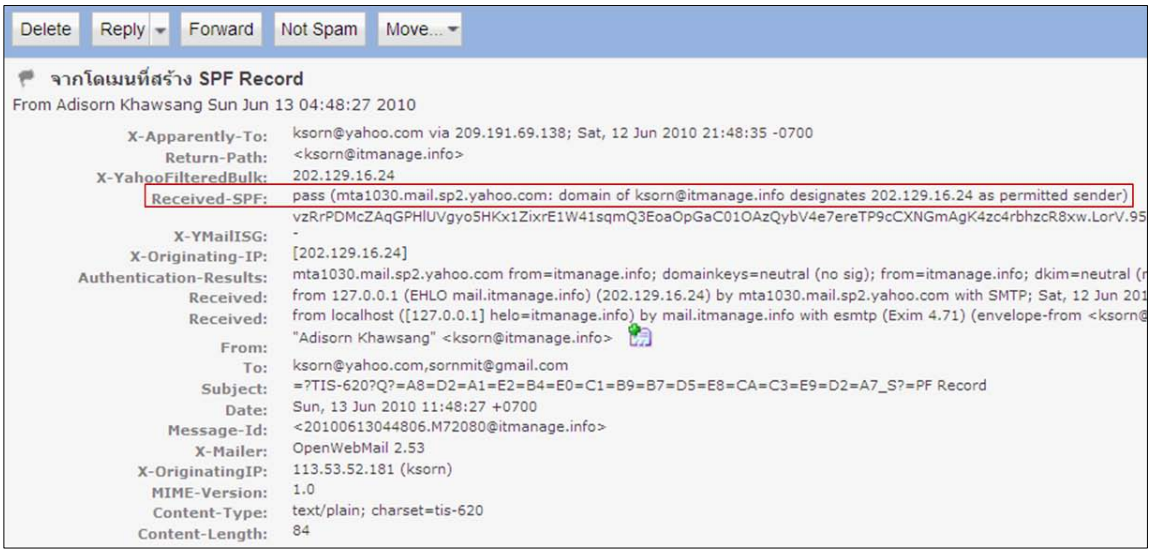
รูปที่ 5 SPF Record ที่ถูกเพิ่มให้กับไฟล์ hosts บน DNS Server

5. เมื่อทำการตรวจสอบด้วยคำสั่ง nslookup จะได้ค่าของ type=txt เป็น spf ดังรูปที่ 6

```
C:\Users\adisorn.k>nslookup
Default Server:  UnKnown
Address:  192.168.1.1

> set type=txt
> itmanage.info
Server:  UnKnown
Address:  192.168.1.1

Non-authoritative answer:
itmanage.info    text =

        "v=spf1 mx ~all"
>
```

รูปที่ 6 การใช้คำสั่ง nslookup ทำการตรวจสอบ SPF record

6. และเมื่อทดลองส่งเมล์จาก Mail Server ของโดเมน itmanage.info อีกครั้งไปยัง Yahoo จะได้ผลการรับเมล์แบบ Full Header ดังรูปที่ 7 ซึ่งจะเห็นว่าค่า Received-SPF จะผ่านการตรวจสอบจากระบบเมล์ของ Yahoo ซึ่งมีค่าเป็น pass



รูปที่ 7 แสดงตัวอย่างการรับของ Yahoo ที่รับจากโดเมนที่มีการสร้าง SPF record ไว้บน DNS ประจำโดเมน

การติดตั้ง SPF บน Postfix Mail Server (สำหรับ Ubuntu)

จากที่กล่าวมาแล้ว ในส่วนของ Mail Server ถ้าต้องการจะกลั่นกรองการรับเมล์โดยอาศัยมาตรฐาน SPF ก็จะต้องมีการติดตั้ง SPF Package เพิ่มเติมบน Mail Server ซึ่งขั้นตอนการติดตั้งและการใช้งานบน Postfix (Ubuntu) มีดังนี้

1. การเลือก SPF Package และการติดตั้ง : ใน Ubuntu 7.04 และ 7.10 มีสอง RFC 4408 compliant package sets ที่สามารถใช้งานได้ อันหนึ่งถูกเขียนด้วย Python อีกอันถูกเขียนด้วย perl สำหรับ perl package เป็นความต้องการพื้นฐานที่พบเห็นโดยทั่วไป ในเวอร์ชันใหม่ ๆ ของ Python package มีความทันสมัยมากกว่า (มีชุด default ที่ไม่ซับซ้อนในการเซ็ตอัพ)

   3.1 สำหรับ Python ให้ติดตั้งด้วยคำสั่งดังนี้

   apt-get install python-policyd-spf python-spf

   3.2 สำหรับ Perl System ให้ติดตั้งด้วยคำสั่งดังนี้

   apt-get install postfix-policyd-spf-perl libmail-spf-perl

2. การทำงานร่วมกับ Postfix : จะต้องมีการแก้ไขเปลี่ยนแปลง Postfix บางอย่าง เพื่อรวม SPF checking เข้ากับ Postfix ในคำแนะนำชุดนี้ การรวมกับโปรแกรม Python จะได้อธิบายต่อไป ส่วนการรวมกับโปรแกรม Perl ก็คล้ายกันมาก ทั้งนี้สำหรับรายละเอียดสามารถได้ด้วย man postfix-policyd-spf-perl

3. Enabling the Policy Service

   3.1 ในไฟล์ /etc/postfix/main.cf คุณจำเป็นต้องเพิ่มบรรทัดต่อไปนี้ (จะเพิ่มที่ส่วนไหนของไฟล์ก็ได้ แต่มักจะเพิ่มที่ส่วนท้ายของไฟล์)

   spf-policyd_time_limit = 3600s

   3.2 การเพิ่มค่าของ policy time limit จะทำให้ Server ไม่เกิดหมดเวลาในขณะที่ message ยังคงถูกโปรเซส และให้ทำการเพิ่มข้อความต่อไปนี้เข้าไปยังไฟล์ /etc/postfix/master.cf สำหรับ python script

   policy-spf unix - n n - - spawn
   user=nobody argv=/usr/bin/policyd-spf

   หรือสำหรับ Perl Script ให้เพิ่มข้อความต่อไปนี้

   policy-spf unix - n n - - spawn
   user=nobody argv=/usr/sbin/postfix-policyd-spf-perl

   3.3 สุดท้ายคุณจำเป็นต้องทำการเพิ่ม policy service เข้าไปยัง smtpd_recipient_restrictions ในไฟล์ /etc/postfix/main.cf ด้วยค่าต่อไปนี้

   smtpd_recipient_restrictions =
   .....
   permit_sasl_authenticated
   permit_mynetworks
   reject_unauth_destination
   check_policy_service unix:private/policy-spf

   หมายเหตุ การวาง policy server หลัง reject_unauth_destination จะป้องกันความเสี่ยงที่อาจจะเกิดผลที่ไม่คาดหมายขึ้นได้จาก policy server กับระบบของคุณ และอาจจะทำให้เกิดการหน่วง (ตรงนี้ขอแนะนำให้สำหรับทุก policy server) การวาง policy server หลัง permit local sender เป็นการต้องการเพียงแค่ให้ SPF ทำการตรวจสอบ inbound mail จากอินเตอร์เน็ตเท่านั้น ไม่มีผลต่อ outbound mail จาก user ของคุณ

4. Reload Postfix : ทำการ reload postfix ด้วยคำสั่ง

   /etc/init.d/postfix reload

5. <u>พิสูจน์การทำงาน</u> : ทำการตรวจสอบ mail logs ของคุณ ซึ่ง Python server logs mail จะถูกปฏิเสธหรือหน่วงโดย SPF ถ้าีมีปัญหาเกี่ยวข้อง policy server หรือการรวมกันกับ postfix ก็มีการบันทึก log ไว้ โดยตรวจสอบโดยใช้คำสั่ง

   tail -f /var/log/mail.log

   หรือ

   less /var/log/mail.log

การติดตั้ง SPF บน Exim Mail Server (สำหรับ Ubuntu)

การกลั่นกรองเมล์ให้เป็นไปตามมาตรฐาน SPF บน Exim (Ubuntu) จะต้องมีการติดตั้ง SPF Package เพิ่มเติม ซึ่งมีขั้นตอนการติดตั้งดังนี้

1. ติดตั้ง SPF librady ด้วยคำสั่ง

   apt-get install libmail-spf-query-perl

2. สร้างไฟล์ใหม่ชื่อว่า /etc/exim4/conf.d/acl/25_spf_check และมีเนื้อหาในไฟล์ดังนี้

```
# Use "spfquery" to obtain SPF status for this particular sender/host.
# If the return code of that command is 1, this is an unauthorized sender.
#

deny
  message     = [SPF] $sender_host_address is not allowed to send mail \
                from $sender_address_domain.
  log_message = SPF check failed.
  set acl_m9  = -ipv4=$sender_host_address \
                -sender=$sender_address \
                -helo=$sender_helo_name
  set acl_m9  = ${run{/usr/bin/spfquery $acl_m9}}
  condition   = ${if eq {$runrc}{1}{true}{false}}
```

จบครับ