

# Full Mail Server solution w/ vDomains & vUsers

Contributed by Mikie

This guide describes how to setup a full email solution in Debian Linux (all code is from Debian Etch). I was asked to design a secure, scalable, portable solution for a small company. While the guide references many 'servers', the company only had 4 physical machines, Xen was used to virtualize the entire solution. That particular aspect of the system is not discussed in this guide, although I will try to get it into the next revision.

This tutorial is Copyright (c) 2007 by Justin Refice. It is derived from various guides and original material, listed at the end of the document. You are free to use this tutorial under the Creative Commons license 2.5 or any later version.I.

## Introduction

Just a note on the server names used below: If it doesn't need to be accessed by the internet, don't let it be. Domain names ending in internal.example.com are internal NIC/IP Addresses... there is no way to access them directly from the internet, nor should there be. Any server that ONLY has an internal.example.com domain name is a pure-internal server, and can't be accessed directly from the internet. All non-internal servers have two NICS (These can be two real NICs, or virtual). The first NIC has access to the internet, and is strictly firewalled. The second NIC has access to the internal network, and has a little less security as a result. The details of how to setup these NICs are outside the scope of this document, but I may update it to include them in the future.

The general layout of the servers is:

Primary MX: NIC1 = Insecure/Internet = mx-1.example.com  
NIC2 = Secure/Intranet = mx-1.internal.example.com  
MTA: Postfix  
Greylist Filter: Postgrey

Secondary MX: NIC1 = Insecure/Internet = mx-2.example.com  
NIC2 = Secure/Intranet = mx-2.internal.example.com  
MTA: Postfix  
Greylist Filter: Postgrey

SMTP+TLS & IMAPS: NIC1 = Insecure/Internet = secure-mail.example.com  
NIC2 = Secure/Intranet = secure-mail.internal.example.com  
MTA: Postfix (+TLS/SSL)  
IMAP: Dovecot (IMAPS)

Mail Delivery Server: postman.internal.example.com  
MTA (lmt): DSPAM  
Antivirus: ClamAV  
IMAP: Dovecot

Database Server: sql-1.internal.example.com  
MySQL

File Server: files-1.internal.example.com  
NFS

Temporary Build Server: build.internal.example.com  
<Various Tools>

Mail works in the following way:

Internet mail to your domains:

- Mail comes in to Primary or Secondary MX on port 25
- MX queries MySQL server to see if mail recipient & destination are valid:
- Recipient is unauthorized - Mail is rejected (550 Error)
- Recipient is authorized - Mail is allowed to continue
- MX checks greylist policy:
- This is the first time email is tried - Mail is rejected (Retry)
- This is not the first time email is tried - Mail is allowed to continue
- MX checks for quota violations
- The user's quota is full - Mail is bounced
- The user has room - Mail is delivered
- MX Sends mail to Internal Delivery Server (via LMTP)
- Internal Delivery Server checks for Virus/SPAM
- This is SPAM - SPAM is marked, and given to LDA for delivery.
- This is a virus - Mail is rejected
- This is NOT SPAM and NOT VIRUS - Mail is given to LDA
- LDA Delivers mail
- The mail is marked as SPAM - Delivered to "SPAM" directory in Maildir
- The mail is NOT marked as SPAM - Delivered to inbox.

Internet mail from your domains:

- User initiates connection to SMTP Relay on port 25
- SMTP Relay offers TLS:
- User does not use TLS - Mail is rejected
- User does use TLS - Session is allowed to continue
- SMTP Relay offers AUTH (PLAIN):
- User does not authenticate/Fails Authentication - Mail is rejected
- User does authenticate - Session completes as usual

Remote users access mail via IMAPS (Secure IMAP)

Local users access mail via IMAP

If the user detects a false positive SPAM detection, they forward the email to "ham-<username>@<domain>.<tld>"

If the user detects a false negative SPAM detection, they forward the email to "spam-<username>@<domain>.<tld>"

II. Important Notes

All this may be installed in either Debian 4.0 Etch or Ubuntu Feisty Fawn, since both systems are quite similar. Note however that there may be some minor issues if you use the default version of Dovecot and Postfix, but I will try to note them down for you when they arise.

If you are a Ubuntu user, note that I will not use "sudo" in front of every command. Instead, I will launch a root shell using the command "sudo -s".

Installing software in Ubuntu & Debian is very easy, so whenever possible we'll be using the build in apt-get utility. The less we have to build ourselves, the easier it is to maintain later.

So, let's get started!