**OpenBSD SMTP Relay Server**

2012-02-23

Michael Spence

**Audience:**

At the time of writing this document, this document was intended for use by the APEagers System Engineer or System Administrator.

**Preamble:**

This document details the steps take to create a SMTP relay server for the purpose of relaying emails sent from devices within the WAN. Devices include: printers, scanners, ERA, and various manufacturer applications. Devices may also include: servers, RMMs, monitoring servers.

**Topics of Discussion**

1. System Requirements

2. OpenBSD Installation

3. Sendmail CF file

4. Access Database

5. Relay Domains

6. Start-up Configuration

7. PF Rules ???

**Topics in Detail**

**1. System Requirements**

The development machine, built as a Virtual Box Appliance on Michael's Slackware box, was given the following resources:

HDD: 1 GB

Mem: 256 MB

At no time was this machine put under any great stress, and it is recommended that the following resources are given to a mail relay server (this is the author's recommendations):

HDD: 20 GB

Mem: 512 MB

These specifications are recommended based on intuition primarily. Thought was given to the possibility of large emails (maximum size 50MB) being queued for up to a day, 15GB would allow for 300 such emails. Naturally it is not expected that emails would be of such a size, and if it is accepted that the average email size is 1 MB, then these specs will allow for fifteen thousand emails.

**2. OpenBSD Installation**

The development server used has been installed as a typical installation of OpenBSD as described in "Open BSD Installation Guide" by Michael Spence. No specific services were turned off after installation, including the packet filter, for which rules were not altered.

Two standard users accounts have been added: one for the engineer "mspence" and one for "issadmin"; both accounts have explicit sudoer rights. This was done in accordance

e with the mentioned documentation.

Setups for similar SMTP servers should follow this same installation procedure.

It is the author's recommendation that the IP address for all relay servers matches the following:

IP Address = 10.<site>.1.10   
where site is the 2nd octet value for the Campus

**3. Sendmail CF file**

The CF controls the way sendmail functions. This file cannot (or should not) be modified by hand, rather it should be built by using a compiler from a secondary configuration file. These secondary files reside at /usr/share/sendmail/cf and are named \*.mc.

The final MC file is based on the original "obenbsd-localhost.mc" file and adapted in the following way to produce an effective configuration file.

The following steps were taken to alter the original.

added:

- define(`confMAX\_MESSAGE\_SIZE', `50000000')dnl

- define(`confTO\_QUEUERETURN', `2h')dnl

- define(`confTO\_QUEUEWARN', `1h')dnl

- FEATURE(`access\_db')dnl

changed:

- DAEMON\_OPTIONS(`Family=inet, address=127.0.0.1, Name=MTA')dnl

to

- DAEMON\_OPTIONS(`Family=inet, address=10.32.77.10, Name=MTA')dnl

removed:

- DAEMON\_OPTIONS(`Family=inet6, address=::1, Name=MTA')dnl

- CLIENT\_OPTIONS(`Family=inet6, Address=::')dnl

The CF file can be compiled from the MC file using a command similar to the following:

m4 /usr/share/sendmail/m4/cf.m4 openbsd-mspence.mc > mspence.cf

\*\*\* Note: see Appendix Z for full configuration file \*\*\*

**4. Access Database**

The access database controls the clients allowed to access this relay server for the purpose of sending mail. This has been configured very loosely and allows all members with an IP address of 10.x.y.z to use this service. \*\*\* NOTE: any service, beneficial or not may use this service. Be forewarned of possible abuse of this system by spammers. \*\*\*

The access database file (located /etc/mail/access) was edited to configure the allowed relaying from the internal network.

added:

- Connect:10 RELAY

- Connect:127.0.0.1 RELAY

The configuration then needs to be compiled, which can be done using the following command, as stated in access file.

makemap hash /etc/mail/access < /etc/mail/access

**5. Relay Domains**

The configured relay domains allow particular source or target email domains to be passed through the relay server.

The /etc/mail/relay-domains file defines the set of allowed domains. The development server was configured to allow all domains (both target and source). This was achieved by adding "\*" as the last line of the file and removing all other configuration lines.

Further restrictions can be placed on these domains, if necessary, but this would require that specific email addresses are used from the configured senders.

**6. Startup Configuration**

The /etc/rc.conf file configures many of the services which run at start-up. The sendmail\_flags option is of particular importance in this case for the configuration of APEagers particular needs

The following is the proposed settings for the sendmail flags:

sendmail\_flags="-L sm-mta -C/etc/mail/mspence.cf -bd -q10m"

These options configure sendmail to run as a daemon, use "mspence.cf" for configuration settings, set the syslog tag to "sm-mta" and process saved and queued messages every 10 minutes.

**7. PF Rules ???**

This is assumed to be the default, but here is the configuration on the dev box

pass

block in on ! lo0 proto tcp to port 6000:6010

**Y. Original Notes from EMAIL**

Notes on build of SMTP Server:

- OpenBSD 4.8 server (standard install with Xwindows items included (should remove))

- No PF rules needed

- IP address of server 10.32.77.10

- Compiled sendmail configuration file based on openbsd-localhost.mc (/usr/share/sendmail/cf/.)

- added FEATURE(`access\_db')dnl

- changed DAEMON\_OPTIONS(`Family=inet, address=127.0.0.1, Name=MTA')dnl to 10.32.77.10

- removed DAEMON\_OPTIONS(`Family=inet6, address=::1, Name=MTA')dnl

- Compiled access\_db configuration file

- editted /etc/mail/access

- added Connect:10 RELAY which relays for all IP's 10.0.0.0/8

- also added Connect:127.0.0.1 RELAY which probably isn't needed

- compiled with makemap hash /etc/mail/access < /etc/mail/access as stated in access file

- Altered relay-domains (/etc/mail/relay-domains)

- added \*

- Restarted sendmail

- command kill -HUP <pid of sendmail> (can get this from examining output of "ps aux" and finding sendmail)

I think it needs a stress test before putting into production. Would also like to see if it has any issues with sending attachements. Also like to see if I can set the limit of mail size; not aware of current limit, but do recall possibility to set limit.

I also noted that there is a mail queue for sendmail. Items can be added to the queue under certain circumstances (most notably when destination is unavailable). Queue is re-examined by sendmail every 30 minutes (as configured at the moment; can easily be changed). Also queue can be examined using "mailq", which has options to filter output based on recipient or sender or domain etc.

**Z. OpenBSD-MSpence.mc**

divert(-1)

#

# FILE: openbsd-mspence.mc

# DATE: 2012-01-04

# AUTTHOR: Michael Spence

#

# This configuration runs sendmail on the external interface

#

# To make .cf file run following command

#

# m4 /usr/share/sendmail/m4/cf.m4 openbsd-mspence.mc > mspence.cf

#

# Default configuration of sendmail uses /etc/mail/localhost.cf.

# Simply copy mspence.cf to localhost.cf and restart sendmail.

#

# OR

#

# Edit rc.conf and change flags for sendmail to reflect new file.

# (Also suggest '-q10m' for small queue processing interval)

#

#

divert(0)dnl

VERSIONID(`@(#)openbsd-mspence.mc $Revision: 0.2 $')

OSTYPE(openbsd)dnl

define(`confMAX\_MESSAGE\_SIZE', `50000000')dnl

define(`confTO\_QUEUERETURN', `2h')dnl

define(`confTO\_QUEUEWARN', `1h')dnl

FEATURE(`access\_db')dnl

FEATURE(nouucp, `reject')dnl

FEATURE(`accept\_unresolvable\_domains')dnl

FEATURE(`no\_default\_msa')dnl

MAILER(local)dnl

MAILER(smtp)dnl

DAEMON\_OPTIONS(`Family=inet, address=10.32.77.10, Name=MTA')dnl

DAEMON\_OPTIONS(`Family=inet, address=127.0.0.1, Port=587, Name=MSA, M=E')dnl

DAEMON\_OPTIONS(`Family=inet6, address=::1, Port=587, Name=MSA6, M=O, M=E')dnl

CLIENT\_OPTIONS(`Family=inet, Address=0.0.0.0')dnl

dnl

dnl Some broken nameservers will return SERVFAIL (a temporary failure)

dnl on T\_AAAA (IPv6) lookups.

define(`confBIND\_OPTS', `WorkAroundBrokenAAAA')dnl