Extended Features of Sendmail

(SMTP AUTH and STARTTLS)

Bob Tanner <tanner@real−time.com>

Real Time Enterprises, Inc

Eden Prairie, MN

Why Sendmail?

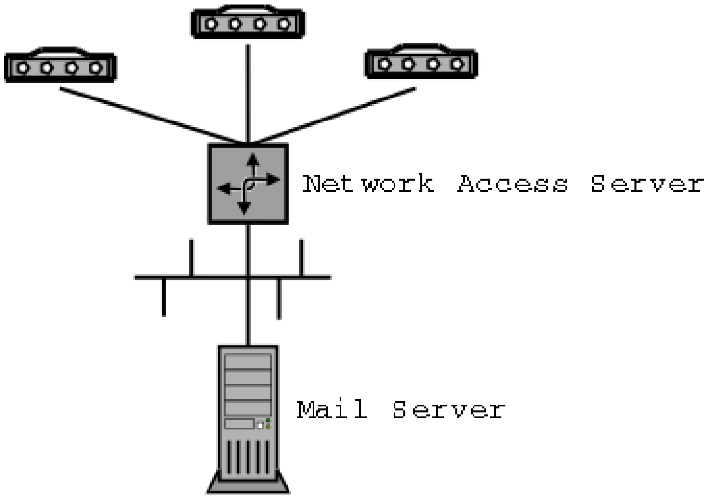
- Postfix
- Qmail
- Emix
- Exchange
- Familiarity and comfort
- "Best" known MTA
- Microsoft factor

Why RedHat?

- Personal preference
- Linux is Linux
- Use The Source!

Typical Setup

- All users are on your network
- Complete Control over IP allocation
- Complete Control over FQDN



Typical Setup Sendmail Configuration

- Sendmail m4 configuration
  - `MASQUERADE_AS(‘real−time.com’)dnl`
  - `FEATURE(‘masquerade_envelope’)dnl`
  - `FEATURE(‘virtusertable’,‘hash −o /etc/mail/virtusertable’)dnl`
  - `FEATURE(use_cw_file)dnl`
  - `FEATURE(‘access_db’)dnl`
- MUA configuration
  - Set incoming/POP/IMAP server to popmail.real−time.com
  - Set outgoing/SMTP server to mail.real−time.com

Configuration File Detail

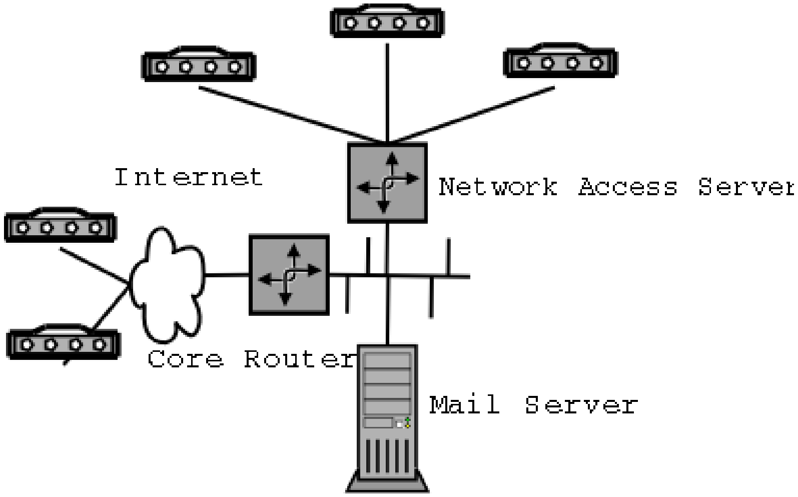
- /etc/mail/virtusertable
  - cfandre@mn-linux.org   cfandre@real-time.com
  - tanner@mn-linux.org   tanner@real-time.com
  - amy@tebbe.org   atebbe@real-time.com
  - rjt@tanners.org   rjt@real-time.com
- /etc/mail/local-host-names
  - mn-linux.org
  - tanners.org
  - tebbe.org

Configuration File Detail (cont)

- /etc/mail/access
  - `localhost           RELAY`
  - `real-time.com        RELAY`
  - `206.10.252           RELAY`
  - `206.10.253           RELAY`
- Support
  - `Since you have control, support is pretty easy`

Common Setup

- Most users are on your network
- Some user are outside your network
- Users outside are trained on how to reconfigure MUA to use the appropriate SMTP Server
- Convince outside users to use web−mail software like IMP



Common Setup Sendmail Configuration

- Sendmail m4 configuration
  - `MASQUERADE_AS(‘real−time.com’)dnl`
  - `FEATURE(‘masquerade_envelope’)dnl`
  - `FEATURE(‘virtusertable’,‘hash −o /etc/mail/virtusertable’)dnl`
  - `FEATURE(use_cw_file)dnl`
  - `FEATURE(‘access_db’)dnl`
- MUA configuration
  - Outside users set outgoing/SMTP server to dial−in provider like AOL’s SMTP server
  - Inside/Outside users set incoming/POP/IMAP server to popmail.real−time.com
  - Inside users set outgoing/SMTP server to mail.real−time.com

Common Setup Sendmail Configuration (cont)

- Support headaches
  - Users can’t change MUA settings
  - Users won’t change MUA settings
  - Users don’t know HOW to change MUA setting
  - Lots of fustrating support time

Configuration File Detail

- /etc/mail/virtusertable
  - cfandre@mn-linux.org   cfandre@real-time.com
  - tanner@mn-linux.org   tanner@real-time.com
  - amy@tebbe.org   atebbe@real-time.com
  - rjt@tanners.org   rjt@real-time.com
- /etc/mail/local-host-names
  - mn-linux.org
  - tanners.org
  - tebbe.org

Configuration File Detail (cont)

- /etc/mail/access

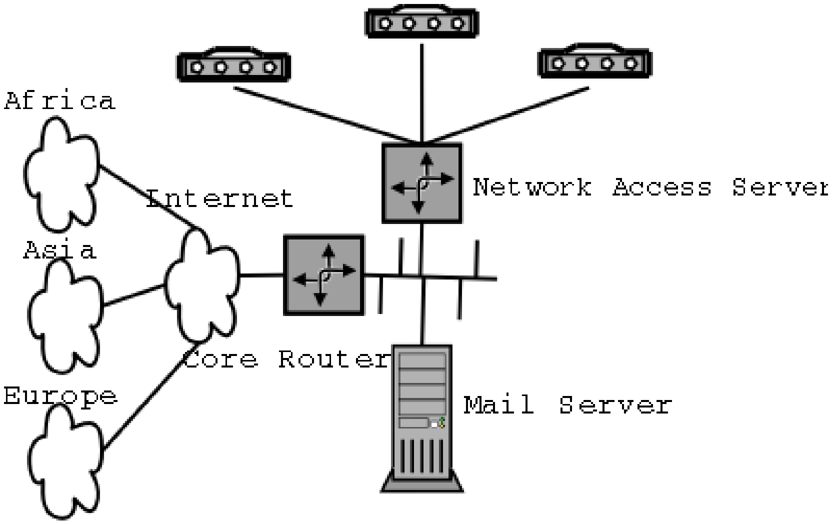
```
localhost               RELAY
real-time.com           RELAY
206.10.252              RELAY
206.10.253              RELAY
uu.net                  RELAY
ca.uu.net               RELAY
chicago.il.uu.net       RELAY
```

Nightmare Setup

- ALL user are NOT on your network
- Unknown IP addresses
  - Many of IP addresses are dynamic
- Unknown FQDN
  - Many hosts do not even have reverse name lookup
- Users are techincally challenged and can’t change outgoing SMTP Server
- Geographically located world−wide

Nightmare Setup (cont)

- Language Barriers
- Time Barrier
- Cultural Barriers
- Political Issues
  - Client internal policies
    - Mail must have headers that make it look like it’s from clientcomany.com
    - Minimal work to implement the change
    - Existing MUA (outlook) must work with the solution



Nightmare Setup (cont)

- Political Issues
  - Country politics
    - Keep originating ISP hidden
- Privacy Issues
  - Keep the contents of email private without use of an external tool

Nightmare Setup Sendmail Configuration (and why this does not work)

- Sendmail m4 configuration
  - `MASQUERADE_AS(‘real−time.com’)dnl`
  - `FEATURE(‘masquerade_envelope’)dnl`
  - `FEATURE(‘virtusertable’,‘hash −o /etc/mail/virtusertable’)dnl`
  - `FEATURE(use_cw_file)dnl`
  - `FEATURE(‘access_db’)dnl`
- MUA configuration
  - Outside users set outgoing/SMTP server to dial−in provider like AOL’s SMTP server
  - Inside/Outside users set incoming/POP/IMAP server to popmail.real−time.com
  - Inside users set outgoing/SMTP server to mail.real−time.com

Nightmare Setup Sendmail Configuration (Cont)

- Support headaches
  - Users can’t/won’t change MUA settings
  - Users won’t change MUA settings
  - Users don’t know HOW to change MUA setting
  - Lots of fustrating support time
  - Maintaining /etc/mail/access file is impossible
  - Maintaining /etc/mail/virtuserstable is impossible
  - Major administrator headaches

Configuration File Detail

- /etc/mail/virtusertable
  - `cfandre@mn-linux.org      cfandre@real-time.com`
  - `tanner@mn-linux.org       tanner@real-time.com`
  - `amy@tebbe.org             atebbe@real-time.com`
  - `rjt@tanners.org           rjt@real-time.com`
- /etc/mail/local-host-names
  - `mn-linux.org`

Configuration File Detail (cont)

- /etc/mail/access (that does not work)
  - `localhost              RELAY`
  - `real-time.com          RELAY`
  - `206.10                 RELAY`
  - `202.14                 RELAY`
  - `Many, many more entries here`

Client's Initial Solution

- promiscuous_relay By default, the sendmail configuration files do not permit mail relaying (that is, accepting mail from outside your local host (class {w}) and sending it to another host than your local host). This option sets your site to allow mail relaying from any site to any site. In almost all cases, it is better to control relaying more carefully with the access map, class {R}, or authentication. Domains can be added to class {R} by the macros RELAY_DOMAIN or RELAY_DOMAIN_FILE (analogously to MASQUERADE_DOMAIN and MASQUERADE_DOMAIN_FILE, see below).
- Spammers found the open relay
  - Compaq PIII 500, 256Mb RAM
  - At Above.net in Washington, DC
  - ORB
  - RSS

The Sendmail Solution

- Closed down the open relay
  - FEATURE(‘blacklist_recipients’)dnl
  - FEATURE(‘relay_based_on_MX’)dnl
  - FEATURE(dnsbl, ‘rbl.maps.vix.com’, ‘Mail from $&{client_addr} Rejected – see http://www.mail-abuse.org/rbl/’)dnl
  - FEATURE(dnsbl, ‘dialups.mail-abuse.org’, ‘Dialup – see http://www.mail-abuse.org/dul/’)dnl
  - FEATURE(dnsbl, ‘relays.mail-abuse.org’, ‘Open spam relay at $&{client_addr} – see http://www.mail-abuse.org/rss/’)dnl
  - FEATURE(‘delay_checks’)dnl
- Use SMTP AUTH instead of the access file
  - SMTP AUTH allows relaying for senders who have successfully authenticated themselves.

The Sendmail Solution

- Make sendmail LDAP aware
  - virtusers database
- Make sendmail SASL aware
  - Simple Authentication and Security Layer
- Make sendmail SSL aware

How’d you do that?

- There are lots of packages to make this all work
- Install openssl−0.9.6
- Install openldap−1.2.11
- Install cyrus−sasl−1.5.24
- Install sendmail−8.11.1

OpenSSL

- Stock RPM
- http://www.openssl.org
- No configuration necessary

OpenLDAP

- Stock RPM
- http://www.openldap.org
- Ummm, lots of configuration, but that’s another talk

Cyrus SASL

- Couple of patches
  - SASL by default uses "login"
  - Login default is /etc/sasldb
  - We want it to use PAM
  - Small patch to make SASL use openssl
- ftp://ftp.andrew.cmu.edu/pub/cyrus−mail
- Cyrus SASL needs /etc/sasldb
- /etc/sasldb is some hash DBM file format

Cyrus SASL (cont)

- Hard to make this secure in an RPM
- Use saslpasswd and a random username and password to create /etc/sasldb
- /etc/sasldb is not used, but cyrus wants it

Sendmail

- Use RedHat’s base sendmail rpm
- redhat.config.m4
  - `define(‘confMAPDEF’, ‘–DNEWDB –DNIS –DLDAPMAP –DSTARTTLS’)`
  - `define(‘confENVDEF’, ‘$(RPM_OPT_FLAGS) –D_FFR_SASL_OPTS –DXDEBUG=0 –DSASL –DSFIO –I/usr/include/sfio’)`
  - `define(‘confLIBS’, ‘–lnsl –lldap –llber –lsasl –lsfio –lssl –lcrypto’)`
- Compile and Install

Sendmail

- Initial test
  - `/usr/lib/sendmail -d0.1 -bv root | grep SASL`
  - `Make sure SASL appears in the output`

Sendmail

- Start Sendmail
  - Connect to it and see if 250-AUTH appears in the output
  - % telnet localhost 25
  - 220 local.sendmail.ORG ESMTP Sendmail 8.10.0/8.10.0; Thu, 9 Sep 1999 10:48:44 -0700 (PDT)
  - ehlo localhost
  - 250-local.sendmail.ORG Hello localhost [127.0.0.1], pleased to meet you
  - 250-ENHANCEDSTATUSCODES
  - 250-DSN
  - 250-AUTH DIGEST-MD5 CRAM-MD5
  - 250 HELP
  - quit

Sendmail

- Troublshooting
  - `LogLevel = 14 is your friend`
  - `http://www.sendmail.org/~ca/email/auth.html`

The Configuration File

- README.cf is your friend
- http://www.sendmail.org search for STMP AUTH
- Create your keys

  -
    ```
    openssl genrsa -rand /lib/libc-2.1.3.so:/usr/bin/emacs -out sendmail.key 1024
    ```

  -
    ```
    openssl req -new -key sendmail.key -out sendmail.csr
    ```

  -
    ```
    openssl x509 -req -days 1825 -in sendmail.csr -signkey sendmail.key -out sendmail.crt
    ```

The Configuration File (cont)

- Define the location for your certs
  - `Use m4 macros to keep it platform independent`
  - `define(‘CERT_DIR’, ‘MAIL_SETTINGS_DIR‘’certs’)dnl`
- Define the location for your Certificate Authority (CA)
  - `define(‘confCACERT_PATH’, ‘CERT_DIR’)dnl`
- Define Server Cert and Key
  - `define(‘confSERVER_CERT’, ‘CERT_DIR/sendmail.crt’)dnl`
  - `define(‘confSERVER_KEY’, ‘CERT_DIR/sendmail.key’)dnl`

The Configuration File (cont)

- Define Client Cert and Key
  - `define('confCLIENT_CERT', 'CERT_DIR/sendmail.crt')dnl`
  - `define('confCLIENT_KEY', 'CERT_DIR/sendmail.key')dnl`
- Using same key for server and client
  - `Self signed keys`

The Magic of SMTP AUTH

- Only do SMTP AUTH if the client ask for it
  - define(‘confAUTH_OPTIONS’, ‘p’)
- Activate Relaying via SMTP AUTH
  - TRUST_AUTH_MECH(‘LOGIN PLAIN DIGEST−MD5 CRAM−MD5’)dnl
  - Per default, relaying is allowed for any user who authenticated via a "trusted" mechanism, i.e., one that is defined via TRUST_AUTH_MECH
- /etc/mail/access can still be used
  - Will try SMTP AUTH first, fails will look in /etc/mail/access

Activate TLS

- You get it almost for free
  - `define(‘confAUTH_MECHANISMS’, ‘LOGIN PLAIN DIGEST−MD5 CRAM−MD5’)dnl`
- Encrypts SMTP session
- Allows end−point to end−point encryption
- Addresses privacy concerns

Configuring MUA (outlook)

- http://www.real–time.com/support
  - Click Email Config
- Quick–n–dirty config
  - Tools->Accounts
  - Choose your ISPs account
  - Click Properties
  - Click the Server Tab
  - Check the "My Server Requires Authentication"
  - Click the Setting... button
  - Check the "Use same settings as my incoming mail server"

Log files

- Syslog

```
– Jan 31 17:10:50 transmuter sendmail[27466]: f0VNAnt27464: SMTP outgoing connect on
  dagger.real-time.com

– Jan 31 17:10:50 transmuter sendmail[27466]: TLS: init(clt)=1

– Jan 31 17:10:50 transmuter sendmail[27466]: f0VNAnt27464: TLS: start client

– Jan 31 17:10:50 transmuter sendmail[27466]: TLS cert verify: depth=0
  /C=US/ST=MN/L=Eden Prairie/O=Real Time Enterprises, Inc./CN=mail.real-
  time.com/Email=postmaster@real-time.com, state=0, reason=self signed certificate

– Jan 31 17:10:50 transmuter sendmail[27466]: f0VNAnt27464: TLS: get_verify in clt:
  18 get_peer: 0x81105b0

– Jan 31 17:10:50 transmuter sendmail[27466]: TLS: connection to mail.real-
  time.com., version=TLSv1/SSLv3, verify=SUCCUSS, cipher=EDH-RSA-DES-CBC3-SHA,
  bits=168

– Jan 31 17:10:50 transmuter sendmail[27466]: TLS: server cert
  subject:/C=US/ST=MN/L=Eden+20Prairie/O=Real+20Time+20Enterprises,+20Inc./CN=mail.r
  eal-time.com/Email=postmaster@real-time.com, cert
  issuer=/C=US/ST=MN/L=Eden+20Prairie/O=Real+20Time+20Enterprises,+20Inc./CN=mail.re
  al-time.com/Email=postmaster@real-time.com

– Jan 31 17:10:50 transmuter sendmail[27466]: SASL: outgoing connection to mail.real
  time.com.: mech=DIGEST-MD5, bits=56
```

Log files

- /usr/lib/sendmail −q −v

```
250-enchanter.real-time.com Hello IDENT:njFouiGhki8iB+cRrfh6VW9yNGnkX2MD@dagger.real-time.com [206.10.252.103], pleased to meet you
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-SIZE
250-DSN
250-ONEX
250-ETRN
250-XUSR
250-AUTH CRAM-MD5 DIGEST-MD5
250-STARTTLS
250 HELP
>>> STARTTLS
220 2.0.0 Ready to start TLS
```

Recap

- Unknown IP addresses
  - IP address is a non−issue
  - We can identify each user via their username and password
- Unknown FQDN
  - SMTP AUTH removes need for this info
  - This info was used in the /etc/mail/access file
  - We are using username and password now
- Users are techincally challenged and can’t change outgoing SMTP Server

Recap (cont)

- Geographically located world−wide
- Language, time, Cultural Barriers
  - Will still have to explain re−configuration of MUA
  - Only have to do it once
- Political Issues
  - Client internal policies
    - All mail comes from clientdomain.com
    - Very little work necessary to convert to this new system
    - Existing MUA works with solution
  - Country polictics
    - TLS keeps originating ISP’s mail OUT of the picture totally

Recap (cont)

- Privacy Issues
  - TLS keeps the contents of email private without the use of an external tool

Q & A on SMTP AUTH and TLS

- Questions
- NIH syndrome

Not Invented Here Syndrome

- Don’t re−invent the wheel
- The power of open source is sharing
- SourceForge project "Real Time Enterprises"
- http://sourceforge.net/projects/rte/
- All RPM packages are available

Break

- MAPS
- ORBS
- Miscelleous Sendmail things
- Q & A

MAPS

- Realtime Blackhole List (RBL)
- Dialup Users List (DUL)
- Relay Spam Stopper (RSS)
- Anti−spam tools
- Very easy to setup in Sendmail
- Fairly effective

MAPS and Sendmail

- Default setup uses Mail Abuse’s DNS server
- m4 configuration files

  -
    ```
    FEATURE(dnsbl, ‘rbl.maps.vix.com’, ‘Mail from $&{client_addr} Rejected - see http://www.mail-abuse.org/rbl/’)dnl
    ```

  -
    ```
    FEATURE(dnsbl, ‘dialups.mail-abuse.org’, ‘Dialup - see http://www.mail-abuse.org/dul/’)dnl
    ```

  -
    ```
    FEATURE(dnsbl, ‘relays.mail-abuse.org’, ‘Open spam relay at $&{client_addr} - see http://www.mail-abuse.org/rss/’)dnl
    ```

MAPS and DNS

- Better to slave the zones

```
– zone "relays.mail-abuse.org" {
–         type slave;
–         file "slave/relays.mail-abuse.org";
–         masters { 204.152.184.64; };
–         allow-transfer { none; };
–         allow-query { any; };
–         allow-update { none; };
– };
```

MAPS and DNS (cont)

- Better to slave the zones

```
– zone "dialups.mail-abuse.org" {
–         type slave;
–         file "slave/dialups.mail-abuse.org";
–         masters { 204.152.184.74; };
–         allow-transfer { none; };
–         allow-query { any; };
–         allow-update { none; };
– };
```

MAPS RBL

- Creates intentional network outages for the purpose of limiting the transport of know−to−be−unwanted mass email
- Subscription service
- MAPS is not the network police force, but rather a method to identify likely spam origin
- Throwing the baby out with the bath water
- http://mail−abuse.org/rbl/

MAPS RSS

- A database of verified SMTP servers that all promiscious relaying
- Subscription service
- Baby and the water again
- http://mail−abuse.org/rss/

MAPS DUL

- Encourages good email behavior and accountability
- Prevents traspassing by spammers who offload unsolicited email using direct SMTP connections without using their ISP’s mail server as a relay
- Subscription based
- Need to register your network
- http://mail−abuse.org/dul/

ORBS

- Facist MAPS?
- Validated database of open mail relays
- Nomination of open relays (like MAPS)
- Scans the Internet for open relays
- Can be brutal
- Ran it for 1 month and got no spam
- http://www.orbs.org/

Misc things about Sendmail

- Prevent user harvesting
  - `define(‘confPRIVACY_FLAGS’,‘goaway’)dnl`
- Remove version info from SMTP greeting
  - `define(‘confSMTP_LOGIN_MSG’, ‘$j server ready at $b’)dnl`
- Yeah, security by obscurity

Misc things about Sendmail

- Change the helpfile too

```
-smtp   This is sendmail version $v
-smtp   Topics:
-smtp           HELO    EHLO    MAIL    RCPT    DATA
-smtp           RSET    NOOP    QUIT    HELP    VRFY
-smtp           EXPN    VERB    ETRN    DSN     AUTH
-smtp           STARTTLS
-smtp   For more info use "HELP <topic>".
-smtp   To report bugs in the implementation send email to
-smtp           sendmail-bugs@sendmail.org.
-smtp   For local information send email to Postmaster at your site.
+smtp   I’m sorry, Dave, I’m afraid I can’t do that.
```

Q&A

- Sendmail
- SMTP AUTH
- STARTTLS
- MAPS
- ORBS
- TCLUG