Postfix в качестве почтового шлюза организации

Черновик!

Список задач

- Postfix должен выступать шлюзом для Microsoft Exchange
- Должна проводиться проверка на существование почтового ящика перед приемом письма - как довольно простой этап отсеивания спама
- Серые списки - борьба со спамом
- Проверка антивирусом. Все зараженные письма блокировать
- Проверка и анализ на принадлежность к спаму: пометить письмо, но доставить пользователю
- Dualdelivery. Входящая почта должна доставляться на основной и дополнительный почтовые сервера

Используемое ПО

- postfix - почтовый сервер (MTA)
- postfix-ldap - для работы с MS Active Directory
- postgrey - серые списки
- amavis - анализатор, использует антивирус и антиспам
- clamav - антивирус
- spamassassin - оценка спама

Установка

```
Postfix & Active Directory integration
# apt-get install postfix

Postfix & Active Directory integration
# apt-get install postfix-ldap

Amavis
# apt-get install amavis amavisd-new

ClamAV
# apt-get install clamav clamav-daemon clamav-dreshclam

Архиваторы для распаковки вложений
```

```
# apt-get install zoo unzip bzip2 p7zip cpio cabextract tnef pax nomarch
lzop altermime arj lhasa ripole unrar
```

...

Интеграция с Microsoft Active Directory

Создаем файл ldap_mydomain.ru.cf с примерно таким содержимым:

```
# Проверка существования почтовых ящиков в Active Directory

server_host = ldap://mydomain.int
server_port = 3268
timeout = 60
search_base = DC=mydomain,DC=int
query_filter =
(&(proxyAddresses=smtp:%s)(!(userAccountControl:1.2.840.113556.1.4.803:=2))(
|(objectClass=user)(objectClass=group)(objectClass=contact)(objectClass=publ
icFolder)))
result_format = %s
result_attribute = cn
#result_attribute = sAMAccountName
special_result_attribute =
scope = sub
bind = yes
bind_dn = ldaplookup@mydomain.int
bind_pw = LDAPSecretPassword
dereference = 0
domain = mydomain.ru
version=3
debuglevel = 0
#debuglevel = 9
```

Проверяем как оно работает:

```
# postmap -q someuser@mydomain.ru ldap://etc/postfix/ldap_mydomain.ru.cf
```

Если все хорошо и правильно - должны показаться ФИО учетной записи someuser@mydomain.ru

Добавляем проверку в postfix/main.cf:

```
virtual_mailbox_maps = ldap:/etc/postfix/ldap_mydomain.ru.cf
```

Amavis

Настраиваем по очереди в /etc/amavis/conf.d/ (показаны только основные изменения)

01-debian

```
use strict;

$ENV{PATH} = $path =
'/usr/local/sbin:/usr/local/bin:/usr/sbin:/sbin:/usr/bin:/bin';
$file   = 'file';
$gzip   = 'gzip';
$bzip2  = 'bzip2';
$lzop   = 'lzop';
$rpm2cpio   = ['rpm2cpio.pl','rpm2cpio'];
$cabextract = 'cabextract';
$uncompress = ['uncompress', 'gzip -d', 'zcat'];
$unfreeze   = ['unfreeze', 'freeze -d', 'melt', 'fcat'];
$arc        = ['nomarch', 'arc'];
$unarj      = ['arj', 'unarj'];
$unrar      = ['rar', 'unrar']; #disabled (non-free, no security support)
$zoo    = 'zoo';
$lha    = 'lha';
$lha    = undef;
$pax    = 'pax';
$cpio   = 'cpio';
$ar     = 'ar';
$ripole = 'ripole';
$dspam  = 'dspam';

1;  # ensure a defined return
```

15-av_scanners

```

### http://www.clamav.net/
 ['ClamAV-clamd',
   \&ask_daemon, ["CONTSCAN {}\n", "/var/run/clamav/clamd.ctl"],
   qr/\bOK$/m, qr/\bFOUND$/m,
   qr/^.*?: (?!Infected Archive)(.*) FOUND$/m ],
```

15-content_filter_mode

```
use strict;

# You can modify this file to re-enable SPAM checking through spamassassin
# and to re-enable antivirus checking.

#
# Default antivirus checking mode
# Please note, that anti-virus checking is DISABLED by
# default.
# If You wish to enable it, please uncomment the following lines:

@bypass_virus_checks_maps = (
```

```
   \%bypass_virus_checks, \@bypass_virus_checks_acl,
\$bypass_virus_checks_re);

#
# Default SPAM checking mode
# Please note, that anti-spam checking is DISABLED by
# default.
# If You wish to enable it, please uncomment the following lines:

@bypass_spam_checks_maps = (
   \%bypass_spam_checks, \@bypass_spam_checks_acl, \$bypass_spam_checks_re);

1;  # ensure a defined return
```

20-debian_defaults

```
use strict;
$QUARANTINEDIR = "$MYHOME/virusmails";
$quarantine_subdir_levels = 1; # enable quarantine dir hashing
$log_recip_templ = undef;    # disable by-recipient level-0 log entries
$DO_SYSLOG = 1;              # log via syslogd (preferred)
$syslog_ident = 'amavis';    # syslog ident tag, prepended to all messages
$syslog_facility = 'mail';
$syslog_priority = 'debug';  # switch to info to drop debug output, etc
$enable_db = 1;              # enable use of BerkeleyDB/libdb (SNMP and
nanny)
$enable_global_cache = 1;    # enable use of libdb-based cache if
$enable_db=1
$inet_socket_port = 10024;   # default listening socket
$sa_spam_subject_tag = '***SPAM*** ';
$sa_tag_level_deflt  = -999;  # add spam info headers if at, or above that
level
$sa_tag2_level_deflt = 6.0; # add 'spam detected' headers at that level
$sa_kill_level_deflt = 21.0; # triggers spam evasive actions
$sa_dsn_cutoff_level = 7;   # spam level beyond which a DSN is not sent
$sa_mail_body_size_limit = 200*1024; # don't waste time on SA if mail is
larger
$sa_local_tests_only = 0;    # only tests which do not require internet
access?
$MAXLEVELS = 14;
$MAXFILES = 1500;
$MIN_EXPANSION_QUOTA =      100*1024;  # bytes
$MAX_EXPANSION_QUOTA = 300*1024*1024;  # bytes
$final_virus_destiny      = D_DISCARD;  # (data not lost, see virus
quarantine)
$final_banned_destiny     = D_BOUNCE;   # D_REJECT when front-end MTA
$final_spam_destiny       = D_DISCARD;
$final_bad_header_destiny = D_PASS;     # False-positive prone (for spam)
$enable_dkim_verification = 1;
$virus_admin = "postmaster\@$mydomain"; # due to D_DISCARD default
$X_HEADER_LINE = "$myproduct_name at $mydomain";
```

```
@viruses_that_fake_sender_maps = (new_RE(
  [qr'\bEICAR\b'i => 0],           # av test pattern name
  [qr/.*/ => 1],  # true for everything else
));
@keep_decoded_original_maps = (new_RE(
  qr'^MAIL-UNDECIPHERABLE$', # recheck full mail if it contains
undecipherables
  qr'^(ASCII(?! cpio)|text|uuencoded|xxencoded|binhex)'i,
));
$banned_filename_re = new_RE(
  # block certain double extensions anywhere in the base name
  qr'\.[^./]*\.(exe|vbs|pif|scr|bat|cmd|com|cpl|dll)\.?$'i,
  qr'\{[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}\}?$'i, # Windows Class ID
CLSID, strict
  qr'^application/x-msdownload$'i,                # block these MIME types
  qr'^application/x-msdos-program$'i,
  qr'^application/hta$'i,
  qr'.\.(exe|vbs|pif|scr|bat|cmd|com|cpl)$'i, # banned extension - basic
  qr'^\.(exe-ms)$',                      # banned file(1) types
);
@score_sender_maps = ({ # a by-recipient hash lookup table,
                        # results from all matching recipient tables are
summed
  ## site-wide opinions about senders (the '.' matches any recipient)
  '.' => [  # the _first_ matching sender determines the score boost
   new_RE(  # regexp-type lookup table, just happens to be all soft-
blacklist
    [qr'^(bulkmail|offers|cheapbenefits|earnmoney|foryou)@'i         =>
5.0],
    [qr'^(greatcasino|investments|lose_weight_today|market\.alert)@'i=>
5.0],
    [qr'^(money2you|MyGreenCard|new\.tld\.registry|opt-out|opt-in)@'i=>
5.0],
    [qr'^(optin|saveonlsmoking2002k|specialoffer|specialoffers)@'i   =>
5.0],
    [qr'^(stockalert|stopsnoring|wantsome|workathome|yesitsfree)@'i  =>
5.0],
    [qr'^(your_friend|greatoffers)@'i                                =>
5.0],
    [qr'^(inkjetplanet|marketopt|MakeMoney)\d*@'i                    =>
5.0],
   ),
   { # a hash-type lookup table (associative array)
     #'nobody@cert.org'                       => -3.0,
     #'cert-advisory@us-cert.gov'             => -3.0,
     #'owner-alert@iss.net'                   => -3.0,
     #'slashdot@slashdot.org'                 => -3.0,
     #'securityfocus.com'                     => -3.0,
     #'ntbugtraq@listserv.ntbugtraq.com'      => -3.0,
     #'security-alerts@linuxsecurity.com'     => -3.0,
     #'mailman-announce-admin@python.org'     => -3.0,
```

```
    #'amavis-user-admin@lists.sourceforge.net'=> -3.0,
    #'amavis-user-bounces@lists.sourceforge.net' => -3.0,
    #'spamassassin.apache.org'                => -3.0,
    #'notification-return@lists.sophos.com'   => -3.0,
    #'owner-postfix-users@postfix.org'        => -3.0,
    #'owner-postfix-announce@postfix.org'     => -3.0,
    #'owner-sendmail-announce@lists.sendmail.org'   => -3.0,
    #'sendmail-announce-request@lists.sendmail.org' => -3.0,
    #'donotreply@sendmail.org'                => -3.0,
    #'ca+envelope@sendmail.org'               => -3.0,
    #'noreply@freshmeat.net'                  => -3.0,
    #'owner-technews@postel.acm.org'          => -3.0,
    #'ietf-123-owner@loki.ietf.org'           => -3.0,
    #'cvs-commits-list-admin@gnome.org'       => -3.0,
    #'rt-users-admin@lists.fsck.com'          => -3.0,
    #'clp-request@comp.nus.edu.sg'            => -3.0,
    #'surveys-errors@lists.nua.ie'            => -3.0,
    #'emailnews@genomeweb.com'                => -5.0,
    #'yahoo-dev-null@yahoo-inc.com'           => -3.0,
    #'returns.groups.yahoo.com'               => -3.0,
    #'clusternews@linuxnetworx.com'           => -3.0,
    #lc('lvs-users-admin@LinuxVirtualServer.org')    => -3.0,
    #lc('owner-textbreakingnews@CNNIMAIL12.CNN.COM') => -5.0,
    # soft-blacklisting (positive score)
    #'sender@example.net'                     =>  3.0,
    #'.example.net'                           =>  1.0,
   },
  ],  # end of site-wide tables
});
1;  # ensure a defined return
```

21-ubuntu_defaults

```
use strict;

#
# These are Ubuntu specific defaults for amavisd-new configuration
#
# DOMAIN KEYS IDENTIFIED MAIL (DKIM)
$enable_dkim_verification = 1;
# Don't be verbose about sending mail:
@whitelist_sender_acl = qw( .$mydomain );
$final_virus_destiny      = D_DISCARD; # (defaults to D_BOUNCE)
$final_banned_destiny     = D_DISCARD;  # (defaults to D_BOUNCE)
$final_spam_destiny       = D_DISCARD;  # (defaults to D_REJECT)
$final_bad_header_destiny = D_PASS;  # (defaults to D_PASS), D_BOUNCE
suggested
#$bad_header_quarantine_to = undef # use this for not quarantine mails with
bad_header

$virus_admin = undef;
```

```
$spam_admin = undef;

#------------ Do not modify anything below this line -------------
1;  # insure a defined return
```

Ну и все остальное по желанию

Dualdelivery - двойная доставка

Для некоторых целей требуется чтобы входящая почта пересылалась на несколько серверов: основной и резервный.

Для этого был найдена интересная статейка:
http://pjrlost.blogspot.ru/2012/11/smtp-delivery-to-two-mail-servers-via.html

Осталось только немного заменить настройку чтобы почта шла таким путем: Internet → Postfix → Amavis(Antivirus → AntiSpam) → Postfix → Dualdelivery → Мои почтовые сервера

- Устаналиваем msmtp

  ```
  # apt-get install msmtp
  ```

- Создаем пользователя smtpdd, создаем папки и даем на них права этому пользователю
  - /opt/smtpdd
  - /var/spool/smtpdd
  - /var/tmp/smtpdd
- Скачиваем файл https://dl.dropbox.com/u/49959760/smtpdd.tar.gz и разворачиваем содержимое в /opt/smtpdd
- Создаем задание cron

  ```
  # crontab -e -u smtpdd
  ```

  со следующим содержимым:

  ```
  0 * * * * /opt/smtpdd/smtpdd.sh  /var/spool/smtpdd/ qrun > /dev/null
  2>&1
  ```

- Добавляем в /etc/postfix/main.cf строчки

  ```
  relay_domains = domain.whatever
  transport_maps = hash:/etc/postfix/domain.whatever.transport
  ```

- Создаем файл /etc/postfix/domain.whatever.transport и прописываем в него адрес нашего основного почтового сервера

  ```
   domain.whatever smtp:[192.168.1.1]
  ```

- Даем команду

  ```
  # postmap /etc/postfix/domain.whatever.transport
  ```

- Изменяем postfix/master.cf следующим образом:

```
#
#
==========================================================================
===
smtp      inet  n       -       -       -       -       smtpd
## Отправляем письмо в Amavis
        -o content_filter=amavis:[127.0.0.1]:10024
        -o receive_override_options=no_address_mappings

## Dualdelivery - пересылаем письмо на основной и резервный почтовые сервера
dualdelivery    unix    - n n - 5 pipe
        user=smtpdd argv=/opt/smtpdd/smtpdd.sh /var/spool/smtpdd/
${sender} ${recipient}
# Options:
#  q - deliver and queue if fail
#  d - deliver and delete if fail
#  o - deliver and only queue the mail
        192.168.102.10:25:q 192.168.102.234:25:d

# Amavis
amavis     unix    -       -       n       -       2       lmtp
        -o disable_dns_lookups=yes
        -o lmtp_send_xforward_command=yes
        -o smtp_data_done_timeout=1200
        -o max_use=20

## Получаем письма с Amavis и обрабатываем дальше
127.0.0.1:10025 inet    n       -       n       -       2       smtpd
        -o content_filter=dualdelivery
        -o local_recipient_maps=
        -o relay_recipient_maps=
        -o smtpd_restriction_classes=
        -o smtpd_delay_reject=no
        -o smtpd_client_restrictions=permit_mynetworks,reject
        -o smtpd_helo_restrictions=
        -o smtpd_sender_restrictions=
        -o smtpd_recipient_restrictions=permit_mynetworks,reject
        -o smtpd_data_restrictions=reject_unauth_pipelining
        -o smtpd_end_of_data_restrictions=
        -o mynetworks=127.0.0.0/8
        -o smtpd_error_sleep_time=0
        -o smtpd_soft_error_limit=1001
        -o smtpd_hard_error_limit=1000
        -o smtpd_client_connection_count_limit=0
        -o smtpd_client_connection_rate_limit=0
        -o
receive_override_options=no_header_body_checks,no_unknown_recipient_che
cks
```