

FreeBSD Üzerinde Mail Gateway

Beyhan Çalışkan

(2006)

beyhan@gazi.edu.tr

GİRİŞ	1
DONANIM SEÇİMİ	2
FreeBSD KURULUMU	2
POSTFIX + CLAMAV + RELAYDB + SPAMD	3
POSTFIX AYARLARI	3
CLAMSMTP AYARLARI	5
RELAYDB AYARLARI	5

GİRİŞ

Spam mail herkesin şikayetçi olduğu genel konu.Bu bağlamda mail trafiğinizi kuracağınız bir smtp gateway üzerinden geçirerek nasıl spam maillerden kurtulacağınızı anlatmaya çalışacağım.

İhtiyacımız olan işletim sistemi PF olan herhangi biri (OpenBSD, FreeBSD, NetBSD, DragonflyBSD) .Genel kullanım çokluğu göz önünde bulundurarak FreeBSD seçtim. PF 'in konuyla ne ilgisi var derseniz, Spamd OpenBSD tarafından geliştirilen ve PF ile birlikte çalışan bir uygulama.

Spamd uygulaması, bilinen iyi istemcileri mail sunucunuza yönlendirir. Aynı şekilde bilinen kötü istemcileri de tarpit'e. Son olarak gelen her yeni istemciye, iyi veya kötü istemci olduğunu bilmeksizin, sonra tekrar deneyin der.

Bunun sonucunda istemciler üç gruba ayrılır;

- Whitelist : iyi olarak bilinen istemciler
- Blacklist : kötü olarak bilinen istemciler

- Greylist : iyi mi kötü mü bilemiyoruz, ama zamanla kararımızı verecek.

Soru : Ben Postfix değil de Qmail kullanıyorum, sorun olur mu ?

Cevap : İstedığınızı kullanabilirsiniz, bu çözüm MTA bağımsızdır.

DONANIM SEÇİMİ

Spamd sistem kaynaklarını tüketmiyor ama Clamav için biraz ram ve P4 2.0 (dengi AMD de olur) veya daha üstü iyidir.

FreeBSD KURULUMU

FreeBSD kurulumunu bildiğinizi varsayarak, müsadenizle işin kolayına kaçıyorum. Kurlum için üstad Onur Bektaş'ın daha önce hazırladığı “FreeBSD Sunucu Optimizasyonu ve Güvenlik Ayarları” dökümanından faydalanabilirsiniz.

<http://csirt.ulakbim.gov.tr/dokumanlar/freebsdopguvenlik.pdf>

FreeBSD üzerinde PF için;

/etc/rc.conf dosyasına aşağıdaki satırları eklemeniz yeterli.

```
pf_enable="YES"
pflog_enable="YES"
pf_rules="/etc/pf.rules"
```

Çalışan sitem üzerinde PF 'i yüklemek için;

```
# kldload pf
# kldstat
Id Refs Address      Size      Name
1      8 0xc0400000 6721fc   kernel
2      1 0xc0a73000 58554    acpi.ko
3      1 0xc4eb5000 16000    linux.ko
4      1 0xc5e20000 2d000    pf.ko

# pfctl -e

# pfctl -s all
```

POSTFIX + CLAMAV + RELAYDB + SPAMD

Burada anlatılanlar postfix için , siz istediğiniz MTA 'yı kullanabilirsiniz. Eğer MySQL ile çalışan bir yapılandırmaya sahipseniz, postfix-mysql destekli kurmakta fayda var.

```
# cd /usr/ports/mail/postfix-current/ && make install clean
# cd /usr/ports/mail/clamav/ && make install clean
# cd /usr/ports/mail/clamsmtp/ && make install clean
# cd /usr/ports/mail/relaydb/ && make install clean
# cd /usr/ports/mail/spamd/ && make install clean
```

Kurulum bittikten sonra */etc/rc.conf* dosyasına aşağıdaki satırları ekliyoruz;

```
postfix_enable="YES"
sendmail_submit_enable="NO"
sendmail_outbound_enable="NO"
sendmail_msp_queue_enable="NO"
clamsmtpd_enable="YES"
clamsmtpd_conf="/usr/local/etc/clamsmtpd.conf"
clamav_clamd_enable="YES"
clamav_freshclam_enable="YES"
pfspamd_enable="YES"
pfspamd_flags="-n smtpgw -g"
```

Spamd 'yi greylist modunda çalıştırmak için;

```
# mount -t fdescfs fdescfs /dev/fd
```

/etc/fstab aşağıdaki satırı da ekleyin;

```
fdescfs /dev/fd fdescfs rw 0 0
```

POSTFIX AYARLARI

/usr/local/etc/postfix/main.cf için ;

```
mail_owner = postfix
myhostname = mx.univeriste.edu.tr
myorigin = $myhostname
inet_interfaces = all
mydestination = $myhostname
unknown_local_recipient_reject_code = 550
relay_domains = universite.edu.tr
alias_maps = hash:/usr/local/etc/postfix/aliases
alias_database = hash:/usr/local/etc/postfix/aliases
unknown_address_reject_code = 550
unknown_client_reject_code = 550
unknown_hostname_reject_code = 450
content_filter = scan:127.0.0.1:10025
transport_maps = hash:/usr/local/etc/postfix/relay_transport

## Bundan sonra yazılanları Postfix ayarlarınız ve bilginiz doğrultusunda ekleyiniz.
smtpd_reject_unlisted_sender = yes
smtpd_helo_restrictions =check_helo_access hash:/usr/local/etc/postfix/helo_access,
                        reject_invalid_hostname,
                        reject_non_fqdn_hostname

smtpd_recipient_restrictions = permit_mynetworks,
                              reject_unknown_recipient_domain,
                              reject_non_fqdn_recipient,
                              reject_unauth_destination,
                              reject_rbl_client sbl.spamhaus.org

smtpd_client_restrictions =   permit_mynetworks,
                              reject_unknown_reverse_client_hostname,
                              permit

mime_header_checks = regexp: /usr/local /etc/postfix/maps/header_checks
header_checks = regexp: /usr/local /etc/postfix/maps/header_checks

show_user_unknown_table_name = no

## mysql'den user doğrulamak için kullanılacak
relay_recipient_maps = proxy:mysql: /usr/local/etc/postfix/mysql/aliases.cf,
                      proxy:mysql: /usr/local/etc/postfix/mysql/remote_aliases.cf

# Tuning
smtpd_soft_error_limit = 3
smtpd_error_sleep_time = 10s
default_process_limit = 200

minimal_backoff_time =1500s
maximal_backoff_time =6000s
maximal_queue_lifetime = 1d
bounce_queue_lifetime = 1d
```

```
# touch /usr/local/etc/postfix/relay_transport
# vi /usr/local/etc/postfix/relay_transport
```

```
universite.edu.tr smtp:ip adresi (smtp sunucunuzun ip adresi)
```

/usr/local/etc/postfix/master.cf için ;

```
# For virus..
scan    unix    -        -        n        -        16        smtp
        -o smtp_send_xforward_command=yes

127.0.0.1:10026 inet    n        -        n        -        16        smtpd
        -o content_filter=
        -o
receive_override_options=no_unknown_recipient_checks,no_header_body_checks
        -o smtpd_helo_restrictions=
        -o smtpd_client_restrictions=
        -o smtpd_sender_restrictions=
        -o smtpd_recipient_restrictions=permit_mynetworks,reject
        -o mynetworks_style=host
        -o smtpd_authorized_xforward_hosts=127.0.0.0/8
```

CLAMSMTP AYARLARI

/usr/local/etc/clamsmtpd.conf için ;

```
Listen: 0.0.0.0:10025
Action: drop
Quarantine: on
# en son satıra
VirusAction: /usr/local/sbin/virus/blackvirus
```

RELAYDB AYARLARI

```
# mkdir /usr/local/sbin/virus
# vi /usr/local/sbin/virus/blackvirus
```

```
#!/bin/sh

cat $EMAIL | /usr/local/bin/relaydb -b -f /var/db/virusdb/virus_ip
rm -f $EMAIL
```

```
# vi /usr/local/sbin/virus/clear_virusip_whitelist
```

```
#!/bin/sh
for erase in ` /usr/local/bin/relaydb -4lb -B +10 -f
/var/db/virusdb/virus_ip`
do
/usr/sbin/spamdb -d $erase
done
```

yazıp kaydedin.

```
# chmod +x /usr/local/sbin/virus/blackvirus
# chmod +x vi /usr/local/sbin/virus/clear_virusip_whitelist
# mkdir /var/db/virusdb
# touch /var/db/virusdb/virus_ip
# touch /var/db/virusdb/whitelist
# touch /var/db/virusdb/blacklist
# chown clamav virus_ip
```

SPAMD AYARLARI

```
# cp /usr/local/etc/spamd.conf.sample /usr/local/etc/spamd.conf
```

/usr/local/etc/spamd.conf dosyasının en altına eklenecek ;

```
relaydbvirus:\
    :black:\
    :msg="VIRUS. Your address %A is in my virus database list.":\
    :method=exec:\
    :file=/usr/local/bin/relaydb -4lb -m -3 -B +10 -f
/var/db/virusdb/virus_ip:

relaydbblack:\
    :black:\
    :msg="Your address %A is in my blacklist database.You don't allowed to
send message to our domain.":\
    :method=file:\
    :file=/var/db/virusdb/blacklist:

whitelist:\
    :white:\
    :method=file:\
    :file=/var/db/virusdb/whitelist:
```

CRONJOB

```
# crontab -e
```

```
29,59 * * * * /usr/local/sbin/virus/clear_virusip_whitelist 2> /dev/null
0,30 * * * * /usr/local/sbin/spamd-setup
# her pazar virus databaseini temizle
0 0 * * 6 /usr/local/bin/relaydb -db -W 0 -B -20 -m +7 -f
/var/db/virusdb/virus_ip
# 30 gün sonra girdileri sil
0 0 1 * * /usr/local/bin/relaydb -db -W 0 -m +30 -f /var/db/virusdb/virus_ip
58 * * * * /usr/sbin/ntpdate tr.pool.ntp.org | logger -t NTP
```

pf.conf AYARLARI

```
ext_if="bge0" (dc0,fxp0 yada herneyse)
table <spamd> persist
table <myblack> persist
table <spamd-white> persist file "/var/db/virusdb/whitelist"

rdr pass on $ext_if proto tcp from <spamd-white> to port smtp \
    -> 127.0.0.1 port smtp
rdr pass on $ext_if proto tcp from <spamd> to port smtp \
    -> 127.0.0.1 port spamd
rdr pass on $ext_if proto tcp from !<spamd-white> to port smtp \
    -> 127.0.0.1 port spamd

set skip on lo0

block in log all
block in quick on $ext_if proto tcp from <myblack> to port smtp
pass in on $ext_if proto tcp from any to $ext_if port 22 keep
state
pass in on $ext_if proto tcp from any to $ext_if port 25 keep
state
pass out keep state
```

SPAMD LOG

/etc/syslog.conf eklenecek;

```
!spamd
daemon.err;daemon.warn;daemon.info /var/log/spamd
```

touch /var/log/spamd

Sunucu kurulumunu bu şekilde bitirmiş olduk.

İşinize yarayacak birkaç komut;

```
# spamdb | grep 193.140.83.6
WHITE|193.140.83.6|||1170417031|1170425845|1173536269|3|0

# pfctl -t spamd-white -T show
# spamdb | grep GREY
# man spamd
# man spamdb
# man relaydb
# man pf
```