/***\
* **Gökhan ALKAN**
* gokhan [at] enderunix [dot] org
* EnderUNIX Yazılım Gelistirme Takımı
* http://www.enderunix.org
*
* Sürüm : 1.0
* Tarih : 25.05.2007
***/

1 Simscan Nedir?

Simscan qmail-scanner yada qscand'e benzeyen qmail için çalışan basitleştirilmiş bir tarayıcıdır. Ayrıca ekli mailler için engelleme seçeneği de mevcuttur. Simscan C ile yazılmıştır.

2 Simscan Nasıl Çalışır?

- ✓ Simscan geçici bir çalışma dizini oluşturur. Bu dizin kurulum esnasında *"--enable-workdir="* ile belirtilebilir. Bu dizin için ön tanımlı değer *"/var/qmail/simscan"* dizinidir. Oluşturulan bu çalışma dizini altında "unix time in seconds" . "microseconds" , "process id" şeklinde geçici çalışma dizini oluşturulur. Email bu geçici çalışma dizini altında "msg.unixtime.micro.pid" adında dosyaya okunur.

- ✓ ripmime ile email başlık , veri kısmı ve dosya ekleri şeklinde parçalanır

- ✓ mail engellenmek istenen dosya eklerine karşı kontrol edilir.

- ✓ Clamd çalışma dizinideki bütün dosyaları tarar . Clamdscan'ın dönüş kodu kontrol edilir , eğer virüs varsa qmail-smtpd'e mailin bounce edileceğine dair kalıcı hata mesajı gönderilir

- ✓ Genellikle spamassassin spamc ile çağrılır. X-Spam-Flag başlığı kontrol edilir. Eğer başlık "YES" içeriyorsa mail reddedilir.

- ✓ Eğer bütün bu işlemler başarı ile gerçekleştirilmişse mail qmail-queue'e aktarılır. SIMSCAN_DEBUG çevre değişkeni aktif edilmedikçe çalışma dizini ve geçici bütün dosyalar silinir.

3 Kurulum İçin Gerekenler

- ✓ Ripmime
- ✓ qmail with qmail-queue patch
- ✓ Clamav
- ✓ Spamassassin

3.1 Ripmime Kurulumu

Ripmime PLDaniels tarafından ANSI/POSIX standartlarında yazılmış mime ayrıştırıcısıdır. Ripmime *http://www.pldaniels.com/ripmime/* adresinden elde edilebilir. Yada kullanılan dağıtıma göre isteğe bağlı olarak kurulumu gerçekleştirilebilir.

```
# wget  http://www.pldaniels.com/ripmime/ripmime-1.4.0.6.tar.gz
# tar -zxvf ripmime-1.4.0.6.tar.gz
```

Çalışma dizinininde *ripmime-1.4.0.*6 adından dizin oluşmaktadır . Bu dizin içerisinde

```
# make
# make install
```

komutları çalıştırılarak ripmime kurulumu gerçekleştirilir.

Yada isteğe göre FreeBSD port ağacından kurulumyapılabilir.

```
# cd /usr/src/qmail/ripmime-1.4.0.6
# make
# make install
```

3.2 Qmail Yamasının Uygulanması

Öncelikle *qmail-queue* yamasının uygulanıp uygulanmadığının anlaşılması gerekmektedir. Bunun için aşağıdaki adımlar uygulanır.

```
# cd /var/qmail/bin
# strings qmail-smtpd | grep QMAILQUEUE
QMAILQUEUE
#
```

Cıktısı alınıyorsa yama uygulanmış demektir.

Eğer qmail-queue yaması *http://www.qmail.org/qmailqueue-patch* adresinden yada istenen başka bir adresden temin edilip uygulanabilir.qmail-queue yamasını uygulamak için basit olarak

```
# cd /qmail/qmail-1.03
# fetch http://www.qmail.org/qmailqueue-patch
# patch < qmailqueue-patch
# make setup check
```

şeklinde uygulanabilir.

4 Simscan Kurulumu

Simcan Kurulum Seçenekleri

--enable-user=<kullanıcı>

Simscan'ın hangi kullanıcı hakları ile çalışacağını belirtir. Ön tanımlı değeri "simscan" 'dır.

--enable-clamav=y|n

Virüs tarayıcısı olarak clamav'ı aktif yada pasif hale getirmek için kullanılır. "y/n" seçeneklerini alabilir. Ön tanımlı olarak bu seçenek aktif halde gelmektedir

--enable-custom-smtp-reject=y|n

Bu özellik aktif olduğunda simscan , virüslü mailler bulunduğunda red mesajının içine virüs isminide koyar.

Not-1: Bu seçenek aktif hala getirmek için qmail qmail-queue-custom-error.patch yaması ile derlenmesi gerekmektedir

Not-2: Bu seçenek aktif hale getirildiğinde --enable-dropmsg=n olmalıdır.

--enable-per-domain=y|n

Sistemde birden fazla domain bulunduğunda her bir domain için ayrı ayrı tarama seçenekleri kullanılabilir. Ayrıca istenilen dosya eklerini engelleme , spam taraması gibi seçenekler her bir domain için aktif/pasif hale getirilebilir yada özelleştirilebilir.

Not: Bu seçenek aktif olduğunda --enable-spam-passthru değeri göz ardı edilir.

--enable-attach=y|n

/var/qmail/control/ssattach dosyasında belirtilen dosya eklerine sahip mailler engellenir. Ön tanımlı olarak bu değer aktif değildir.

--enable-dropmsg=y|n

Bu seçenek aktif olduğunda virüs yada spamli mail bulunduğunda maili düşürür. Kullanıcıya hata mesajı döndermez.

--enable-spam=y|n

Spam taramasını aktif yada pasif hale getirir. Ön tanımlı olarak bu değer aktif değildir.

--enable-spam-passthru=y|n

Mail spam olarak algılandığında kullanıcıya red mesajı göndermek yerine maili kullanıcıya iletir.

Not: Bu seçeneğin kullanılabilmesi için "spam-hits" değerinin kullanılmaması gerekmektedir.

--enable-spamc-user=y|n

Mail bir kullanıcı için gelmişse simscan spamc'yi –u kullanıcı@domain şeklinde çağırır. Bu şekilde spamassassin kullanıcı için özelleştirilmiş kurallar sistem geneilndeki kuralların üstüne yazar.

--enable-spam-hits=<sayı>

Belirtilen değerin üzerinde olan mailler kullanıcıya iletilmeden engellenir. Ön tanımlı değeri "10"'dur.

Not: Bu seçeneğin kullanılabilmesi için --enable-spam-passthru değerinin "n" olması gerekmektedir.

--enable-spamc-args=<Değer>

Spamc için verilebilecek değerler belirtilir.

--enable-spam-auth-user=y|n

Sistemdeki kullanıcılar için mail gönderimi sırasında spam taramasının yapılıp yapılmayacağını belirtir. Ön tanımlı olarak aktif değildir.

--enable-dropmsg=y|n

mail'in virüs içermesi yada spam olarak algılandığı durumlarda kullanıcıya 5xx içeren mesajlar gönderilmesi yerine mail engellenir ve kullanıcıya iletilmez.

Not-1: Bu seçenek Custom Reject seçeneğine baskın gelir.

Not-2: Eğer --enable-spam-passthru= seçeneği "y" ise spam-hits değeri aktif olmadıkca spam engellenmez.

--enable-quarantinedir=<dizin_yolu>

spam yada virüslü maillerin tutulacağı dizinini yolunu belirtir. Ön tanımlı olarak aktif halde değildir. Bu seçenek aktif hale getirilerek mailler belirtilen dizine yazılır.

--enable-workdir=<dizin_yolu>

simscan çalışma dizininin yolunu belirtir. Ön tanımlı olarak */var/qmail/simscan* dır.

4.1 Simscan Kurulumu

Öncelikle gerekli paketler teminedilmelidir.

```
# fetch http://www.inter7.com/simscan/simscan-1.3.1.tar.gz
# tar -zxvf simscan-1.3.tar.gz
# cd simscan-1.3
```

```
# ./configure --enable-user=clamav --enable-clamav=y --enable-attach=y --
enable-spam=y --enable-spam-passthru=y --enable-spamc-user=y --enable-
quarantinedir=/var/qmail/quarantine
```

```
# ./configure --enable-user=clamav --enable-clamav=y --enable-attach=y --
enable-spam=y --enable-spamc-user=y --enable-per-domain=y --enable-
quarantinedir=/var/qmail/control/quarantine --enable-spam-hits=6
```

Burada iki farklı kurulum gerçekleşmektedir aslında tek fark --enable-per-domain=y değeri ve **--enable-spam-passthru=y** degerinin kullanılmayip spam-hit'i 6 ve üzerinde olan mailleri düşürmesi icin eklenen **--enable-spam-hits=6** değeridir.

```
# make
# make install-strip
```

Karantina için gerekli dizin oluşturulmalı ve gerekli izinler verilmelidir.

```
# mkdir /var/qmail/control/quarantine
# chown clamav  /var/qmail/control/quarantine
```

qmail-smtpd dosyasına aşağıdaki şekilde olmalıdır.

```
QMAILQUEUE="/var/qmail/bin/simscan"
export QMAILQUEUE
```

```
# cat /var/qmail/supervise/qmail-smtpd/run

#!/bin/sh
QMAILQUEUE="/var/qmail/bin/simscan"
export QMAILQUEUE
..
..
#
```

qmail-smtpd yeniden başlatılmalıdır.

```
# svc -d  /service/qmail-smtpd/log
# svc -d  /service/qmail-smtpd

# svc -u  /service/qmail-smtpd/log
# svc -u /service/qmail-smtpd
```

tcp.smtp dosyasına aşağıdaki satır eklenmelidir.

```
:allow,QMAILQUEUE="/var/qmail/bin/simscan"

# cat /etc/tcp.smtp
127.:allow,RELAYCLIENT=""
:allow,QMAILQUEUE="/var/qmail/bin/simscan"
#

# /usr/local/bin/tcprules /etc/tcp.smtp.cdb /etc/tcp.smtp.tmp <
/etc/tcp.smtp
```

Eğer birden fazla domain için kurulum yapılmışsa *(--enable-per-domain=y)* simcontrol dosyası oluşturulmalıdır. İsteğe göre gerekli değerler verilmelidir.

```
# vi /var/qmail/control/simcontrol
:clam=yes,spam=no,attach=.scr:.pif:
#
```

Burada ön ön tanımlı değerler verilmiştir. Virüs taraması yapan ekli maillerden uzantısı .scr ve .pif olanları engellenmiş ve spam taraması yapılmamıştır. Bu bölümün ayrıntıları Birden Fazla Domain İçin Spam Ve Virüs Kontrolü bölümünde anlatılmıştır.

Değişikliklerin aktif olabilmesi için *simcontrol.cdb* oluşması gerekmektedir. Bunun için simscanmk komutu verilmelidir.

```
# /var/qmail/bin/simscanmk
```

4.2 Dosya Uzantısı Engelleme

Simscan ile dosya uzantısı engelleyebilmek için ripmime kurulu olmalı ve "--enable-attach" değeri "y" olmalıdır. Ripmime /usr/local/bin/ripmime dizininden başka bir dizine kurulmuş ise --enable-ripmime= paremetresi ile bu dizinin yeri belirtilmelidir. Simscan'de bu özellik ön tanımlı olarak aktif değildir. Engdellenmek istenen uzantılar /var/qmail/control/ssattach dosyasının içerisine her bir satıra bir uzantı gelecek şekilde yazılır.

```
[gokhan@enderunix galkan]$ cat /var/qmail/control/ssattach
 .exe
 .mp3
 .bat
```

Eğer simscan "--enable-per-domain=y" seçeneği ile derlenmişse bu şekilde dosya uzantısı engelleme yapılamaz. İleriki bölümlerde birden fazla domain bulunan sistemler için nasıl dosya uzantısı engellemesi yapılacağı anlatılacaktır.

4.3 Birden Fazla Domain İçin Spam Ve Virüs Kontrolü

Bu özelliğin aktif olabilmesi için --enable-per-domain=y seçeneği ile derlenmiş olması gerekmektedir.

/var/qmail/control/simcontrol dosyası istenilen tarama seçeneklerine göre düzenlenebilir. Belli bir domain için , belli bir kullanıcı için yada bütün bir domain için ön tanımlı olarak

clam/spam/attachments aktif pasif duruma getirilebilir yada istenilen kritelerlere göre tarama seçenekleri oluşturulabilir. Aşağıda örnek olarak oluşturulmuş bir simcontrd dosyası mevcuttur.

```
# cat  /var/qmail  /contr ol/si mcontr ol
 galkan@enderunix.org:clam=yes,spam=no,attach=.txt:.com
 enderunix.org:clam=no,spam=yes,attach=.mp3
 :clam=yes,spam=yes,spam_hits=15
#
```

Birinci satır ile galkan@enderunix.org kullanıcısı için spam taraması aktif değil virüs taraması aktif ve .txt ve .com uzantılı dosya uzantılarına sahip maillerde engellenecektir.

İkinci satır ile enderunix.org domaini için spam taraması aktif virüs taraması aktif değil ve .mp3 uzantılı dosya eklerine sahip maillerde engellenecektir.

Üçüncü satır ile makine üzerindeki bütün domainler için geçerli olacak şekilde virüs ve spam taraması aktif ve spam hiti olarak 15 in üzerinde olan mailler engellenecek şekilde konfigüre edilmiştir.

Burada belli kriterler daha baskın çıkmaktadır. Baskınlık sırası olarak;

email adresi
bütün bir domain
bütün makine üzerindeki tüm domainler

Email adresi diğer kurallara göre baskındır. Örneğin burada enderunix.org için virüs taraması pasif halde olsada galkan@enderunix.org kullanıcısı için virüs taraması aktif halde olacaktır.

Sistem üzerindeki bütün domainler için virüs taraması aktif ancak enderunix.org için virüs taraması aktif olmadığı için virüs taraması gerçekleşmeyecektir

Yazılan kuralların aktif olabilmesi için /var/qmail/bin/simscanmk'ın çalıştırılması gerekmektedir.

4.4 Simscan'ın Test Edilmesi

Basit olarak şu şekilde simscan komut satırından kontrol edilebilir.

```
# echo "www.enderunix.org" > simscan.txt

# env QMAILQUEUE=/var/qmail/bin/simscan SIMSCAN_DEBUG=2
/var/qmail/bin/qmail-inject gonderbaba@enderunix.org <  simscan.txt
```

env ile başlayan satır tek bir satırdan oluşmaktadır.

Ekrana basılan mesajlardan kontrol edilebilir. Her şey yolundaysa log analizi yapılabilir.

5 Simscan Log Analizi Ve Olası Hatalar

Simscan debug moda çalıştırılmak isteniyorsa eğer qmail-smtpd dosyası aşağıdaki şekilde olmalıdır

```
# cat /var/qmail/supervise/qmail-smtpd/run

#!/bin/sh
SIMSCAN_DEBUG=2
export SIMSCAN_DEBUG
QMAILQUEUE="/var/qmail/bin/simscan"
export QMAILQUEUE
..
..
#
```

Simscan logları qmail-smtpd dosyasına yazar.

```
# tail -f /var/log/qmail/qmail-smtpd/current
…
…
@4000000044b54410295cdff4 simscan: .pif is attachment number 0
@4000000044b54410295ce7c4 simscan: starting: work dir:
/var/qmail/simscan/1152730118.693812.9306
@4000000044b544103973060c simscan: pelookup: called with
marketing@louisianaindians.com
@4000000044b544103976f9c4 simscan: pelookup: domain is louisianaindians.com
@4000000044b544103977057c simscan: cdb looking up louisianaindians.com
@4000000044b5441039770d4c simscan: pelookup: local part is marketing
@4000000044b544103977151c simscan: cdb looking up marketing@louisianaindians.com
@4000000044b5441039771cec simscan: pelookup: called with gonderbaba@enderunix.org
@4000000044b54410397724bc simscan: pelookup: domain is enderunix.org
@4000000044b5441039773074 simscan: cdb looking up enderunix.org
@4000000044b5441039773844 simscan: cdb for enderunix.org found
clam=yes,spam=no,attach=.pif
@4000000044b54410397d3f3c simscan: pelookup clam = yes
@4000000044b54410397d4af4 simscan: pelookup spam = no
@4000000044b54410397d52c4 simscan: pelookup attach = .pif
@4000000044b54410397d5a94 simscan: attachment flag attach = .pif
@4000000044b54410397d6264 simscan: .pif is attachment number 0
….
…

#
```

Simscan kurumlu gerçekleştikten sonra çıkabilecek hatalar ve çözüm yolları anlatılmıştır.

simscan error:2 hatasi:

Simcan + clamav + qmail kurulumu yapildi ve gerekli yapilandirmalar gerceklestirildi fakat qmail-smtpd loglarinda "simcan connect error 2 " hatasi aliniyorsa sebebi izin problemi olabilir. Simcan icin secilen kullanici clamav kullanicisi ise muhtemelen clamav /var/qmail/simscan dizininde yazma hakki bulunmamaktadir. Bunun icin dizinin grup haklari clamav grubu yapilir ve sticky bit aktif hale getirilir.

```
# chgrp clamav /var/qmail/simscan
# chmod g+s /var/qmail/simscan
```

Yada "NOPOFCHECK" degeri "0" yapilmalidir.

```
127.:allow,NOPOFCHECK="0",RELAYCLIENT=""
:allow,NOPOFCHECK="0",QMAILQUEUE="/var/qmail/bin/simscan"
```

Squirrelmail "server reply : sim" hatasi:

Simscan ile mail gondermeye calisildiginda mail gonderiliyor fakat "Server Reply : sim" hatasi aliniyor ise squirrelmail yapilandirma dosyasi olan config.php icerisinde $smtp_auth_mech degeri none yapilmalidir

```
$smtp_auth_mech = 'none';
```