

**FREEBSD VE OPENBSD İŞLETİM SİSTEMLERİ
ÜZERİNDE CLAMAV DESTEKLİ DANSGUARDIAN
KURULUMU**

/******\

* **Gökhan ALKAN**

* gokhan [at] enderunix [dot] org

* EnderUNIX Yazılım Gelistirme Takımı

* <http://www.enderunix.org>

*

* Sürüm : 1.0

* Tarih : 16.06.2007

* Belgenin en güncel haline

<http://www.enderunix.org/docs/clamavdansguardianonbsd.pdf> adresinden erişebilirsiniz

*****/

1.GİRİŞ.....	3
2.GEREKLİ YAZILIMLAR VE KURULUMLARI.....	3
Clamav Kurulumu:.....	3
Squid Kurulumu:.....	4
Dansguardian Kurulumu Ve Yapılandırması:.....	5
FreeBSD İşletim Sistemi İçin Kurulum Yönergeleri:.....	6
OpenBSD İşletim Sistemi İçin Kurulum Yönergeleri:.....	7
3.TEST AŞAMASI.....	8

1. GİRİŞ

Dansguardian güçlü bir web içerik filtreleme yazılımıdır. İnternet dünyasına her gün yeni katılan web sayfaları denetimi dahada zorlaştırmaktadır.Dansguardian ile kullanıcıların istenmeyen web içeriklerini ziyaret etmesi engellenebilir. Bunun yanında diğer bir tehlikede web sayfaları üzerinden sisteme bulaşabilecek virüslerdir. Kullanıcı bilgisayarında antivirüs yazılımı yoksa eğer virüs sisteme bulaşması içten bile değildir. Dansguardian ile web üzerinden akan trafik clamav ile bütünleşik bir şekilde çalıştırılarak kontrol edilebilir. Bu sayede kullanıcı bilgisayarlarına antivirüs yazılı kurmadan bu kontrol gerçekleştirilebilir.Bu makalede OpenBSD ve FreeBSD işletim sistemleri üzerinde Clamav ile bütünleşik Dansguardian kurulumu ile web üzerinden akan trafik kontrol edilecektir.

2. GEREKLİ YAZILIMLAR VE KURULUMLARI

Clamav Kurulumu:

Clamav acik kaynak kodlu antivirüs yazılımıdır. FreeBSD port ağacında */usr/ports/security/clamav* dizininde bulunur.FreeBSD işletim sistemi için kurulum kısaca aşağıdaki adımlar uygulanır.

```
# cd /usr/ports/security/clamav  
# make install clean
```

İkili (binary) kurulum için *pkg_add -rv clamav* kullanılabilir.

```
# pkg_add -rv clamav  
Açılıştta aktif etmek için /etc/rc.conf dosyasına satırları eklenir.
```

```
# clamav_freshclam_enable="YES"  
# clamav_clamd_enable="YES"
```

Gerekli servisleri başlatılır.

```
# /usr/local/etc/rc.d/clamav-freshclam start  
# /usr/local/etc/rc.d/clamav-clamd start
```

OpenBSD işletim sisteminde port ağacında */usr/ports/security/clamav/* dizininde bulunur kurulum için

```
# cd /usr/ports/security/clamav/  
# make install
```

Yada binary olarak kurulum gerçekleştirilebilir.

```
# pkg_add -rv clamav-0.90.3
```

Gerekli servisler çalıştırılmadan önce yapılandırmaları gerçekleştirilir.

`/etc/freshclam.conf` ve `vi /etc/clamd.conf` dosyalarındaki Example satırlarının başına `#` satırı eklenir.

```
# vi /etc/freshclam.conf
#Example
#
```

```
# vi /etc/clamd.conf
#Example
#
```

```
# /usr/local/bin/freshclam
# /usr/local/sbin/clamd
```

<http://www.enderunix.org/docs/Clamav.pdf> adresinden clamav ile ilgili daha detaylı bilgiye ulaşılabilir.

Squid Kurulumu:

Şu anki son versiyon olan 3.x sürümü FreeBSD port ağacında `/usr/ports/www/squid30` dizini altında bulunur. Kurulum için

```
# cd /usr/ports/www/squid30
# make install
```

Açılıştta aktif hale getirmek için ise `/etc/rc.conf` dosyasına aşağıdaki satırlar eklenir.

```
# vi /etc/rc.conf
squid_enable="YES"
#
```

Squid için gerekli cache izinleri squid başlatılmadan önce çalıştırılmalıdır.

```
# /usr/local/sbin/squid -z
```

Daha sonra squid başlatılabilir.

Yada kaynak koddan kurulum yapmak istenirse eğer aşağıdaki adresten istenilen sürüm <http://www.squid-cache.org/Versions/> adresinden temin edilip kurulum gerçekleştirilebilir.

Squid OpenBSD port ağacında `/usr/ports/www/squid30` dizini altında bulunur. Transparan olarak kurulumu gerçekleştirmek için

```
# cd /usr/ports/www/squid30
# env FLAVOR=transparent make install
```

Ardından cache izinleri oluşturulmalıdır .

Squid'in açılışta aktif hale gelebilmesi için aşağıdaki satırlar */etc/rc.local* dosyasına eklenmelidir.

```
# /usr/local/sbin/squid -zX
...
...
2007/06/16 13:30:38| /var/squid/cache/0F/E9 created
2007/06/16 13:30:38| /var/squid/cache/0F/EA created
2007/06/16 13:30:38| /var/squid/cache/0F/EB created
2007/06/16 13:30:38| /var/squid/cache/0F/EC created
...
...
#

# vi /etc/rc.local
if [ -x /usr/local/sbin/squid ]; then
    echo -n 'squid';    /usr/local/sbin/squid
fi
#
```

Ardından squid başlatılabilir.

```
# /usr/local/sbin/squid

# ps auwx | grep "squid"
_squid 30665 11.6 0.5 4488 6580 ?? S 1:32PM 0:00.50 (squid) (squid)
root 26632 0.0 0.0 1352 584 ?? Ss 1:32PM 0:00.00 /usr/local/sbin/squid
_squid 9484 0.0 0.0 268 308 ?? Ss 1:32PM 0:00.01 (unlinkd) (unlinkd)
root 30946 0.0 0.0 340 508 p1 S+ 1:32PM 0:00.01 grep squid
#
```

Daha detaylı bilgiye <http://www.enderunix.org/docs/squid.html> adresinden erişim sağlanabilir.

Dansguardian Kurulumu Ve Yapılandırması:

Dansguardianı FreeBSD ve OpenBSD işletim sistemleri üzerinde kurulumunda bazı farklılıklar olmaktadır. Bundan dolayı burada anlatılacak olan dansguardian kurulumu FreeBSD ve OpenBSD işletim sistemleri için ayrı ayrı anlatılacaktır.

Dansguardian için şu anda bulunan son versiyonuna <http://dansguardian.org/downloads/2/Beta/dansguardian-2.9.8.5.tar.gz> adresinden ulaşılabilir.

```
# wget http://dansguardian.org/downloads/2/Beta/dansguardian-2.9.8.5.tar.gz
# tar -zxvf dansguardian-2.9.8.5.tar.gz
```

FreeBSD İşletim Sistemi İçin Kurulum Yönergeleri:

Dansguardianı clamav ile entegre biçimde çalıştırabilmek için en kolay yol, dansguardianı *clamav* kullanıcısı ve grubunun hakları ile çalıştırmaktır. Ayrıca derlenme esnasında *--enable-clamav --enable-clamd* verilecek parametreler ilede clamav entegrasyonu gerçekleştirilmiş olur. Burada isteğe göre *--enable-clamav* desteği verilmedende kurulum gerçekleştirilebilir.

Öncelikle dansguardian için ön tanımlı olarak gerekli pcre paketinin kurulumu gerçekleştirilmelidir.

```
# cd /usr/ports/devel/pcre
# make install
```

```
# cd dansguardian-2.9.8.5
```

```
# ./configure --prefix=/usr/local/dansguardian --enable-clamav --enable-clamd --with-proxyuser=clamav --with-proxygroup=clamav
```

```
# make
# make install
```

/usr/local/dansguardian/etc/dansguardian/dansguardian.conf dosyasında clamav entegrasyonu için gerekli satırların başından # işareti kaldırılır.

```
# vi /usr/local/dansguardian/etc/dansguardian/dansguardian.conf
contentscanner = '/usr/local/dansguardian/etc/dansguardian/contentscanners/clamav.conf'
contentscanner =
'/usr/local/dansguardian/etc/dansguardian/contentscanners/clamdsan.conf'
#
```

/usr/local/dansguardian/etc/dansguardian/contentscanners/clamav.conf dosyası içerisinde antivirüs taraması için gerekli geçiçi izin oluşturulmalıdır. Ön tanımlı olarak */tmp* dizini kullanılmaktadır.

```
# vi /usr/local/dansguardian/etc/dansguardian/contentscanners/clamav.conf
scanbuffdir = '/istenilen_dizin'
#
```

/usr/local/dansguardian/etc/dansguardian/contentscanners/clamdsan.conf dosyası içerisinde clamd için kullanılan socket bilgisi verilmektedir. Bu netstat komutu ile öğrenilebilir.

```
# netstat -na | grep "clamd"
c597aec4 stream 0 0 c7293550 0 0 0 /var/run/clamav/clamd
#
```

Görüldüğü üzere */usr/local/dansguardian/etc/dansguardian/contentscanners/clamdsan.conf* dosyası içerisinde *clamdufsfile* değeri */var/run/clamav/clamd* olmalıdır.

```
# vi /usr/local/dansguardian/etc/dansguardian/contentscanners/clamdsan.conf
```

```
clamdudsfile = '/var/run/clamav/clamd'  
#
```

ipc dosyaları barındırmak için gerekli hafıza diski tanımlı olarak /tmp dizini altında tutulur. Başka bir dizin altında bu dosyalar barındırılmak istenirse eğer ;

```
# mkdir /usr/dansguardian  
# mdmfs -s 128m md /usr/dansguardian/
```

Açılıştta kalıcı olarak aktif olabilmesi için /etc/fstab dosyası içerisinde aşağıdaki satır girilmelidir.

```
# vi /etc/fstab  
md /usr/dansguardian mfs rw,-s128m 0 0  
#
```

Clamav kullanıcısı ile çalıştırıldığı için dizinin hakları clamav kullanıcısına ait olmalıdır.

```
# chown clamav:clamav /usr/dansguardian
```

dansguardian.conf dosyası içerisinde yeni dizin *ipcfilename* ve *urlipcfilename* parametreleri için belirtilmelidir.

```
# vi /usr/local/dansguardian/etc/dansguardian/dansguardian.conf  
ipcfilename = '/usr/dansguardian/.dguardianipc'  
ipipcfilename = '/tmp/.dguardianipipc'  
#
```

Dansguardian yeniden başlatılarak clamav entegrasyonu tamamlanmış olur.

```
# /usr/local/dansguardian/sbin/dansguardian
```

OpenBSD İşletim Sistemi İçin Kurulum Yönergeleri:

Clamav 0.90 surumu ile bazı fonksiyonlarda değişiklikler yapılmıştır. FreeBSD ve Linux sistemler için gerekli yamayı yapabilir yada direkt <http://ipucu.enderunix.org/view.php?id=1551%E2%8C%A9=tr> adresindeki şekilde sorunu çözülebilir.

OpenBSD üzerine dansguardiani clamav ile entegre bir biçimde kullanmak için dansguardiani *--enable-clamd* ile derlenmelidir. *--enable-clamav* seçeneğini kullanılmamalıdır.

--enable-clamav ile libClamAV desteği veriliyor.
--enable-clamd ile ClamD içerik tarayıcı desteği veriliyor.

Belirtildiği üzere "*--enable-clamav*" libClamAV desteği ile dansguardin derlenmiş oluyor.

Öncelikle dansguardian clamav desteği verilerek derlenip kurulumu gerçekleştirilmelidir.

```
# ./configure --enable-clamd --with-proxyuser=_clamav --with-proxygroup=_clamav
# make
# make install
```

/usr/local/dansguardian/etc/dansguardian/dansguardian.conf dosyasında clamav entegrasyonu için gerekli satırın başından # işareti kaldırılır.

```
# vi /usr/local/dansguardian/etc/dansguardian/dansguardian.conf
contentscanner ='/usr/local/dansguardian/etc/dansguardian/contentscanners/clamdscan.conf'
#
```

port ağacından kurduysanız muhtemelen */tmp/clamd* olacak şekilde, degilsede netstat ile öğrenilebilir. Yada yapılandırma dosyasından istenildiği şekilde yapılabilir.

```
# netstat -na | grep "clamd"
0xd879084c stream 0 0 0xd86f6a5c 0x0 0x0 0x0 /tmp/clamd
#
```

```
# vi /usr/local/dansguardian/etc/dansguardian/contentscanners/clamdscan.conf
clamdudsfile = "/tmp/clamd"
#
```

Bu şekilde OpenBSD üzerinde dansguardian clamav entegre bir biçimde çalıştırılabilir.

3. TEST AŞAMASI

Antivirüs testi için http://www.eicar.org/anti_virus_test_file.htm sayfası kullanılabilir. Aşağıda virüslü bir dosya sisteme indirilmeye çalışılmış ve **Virus or bad content detected** mesaj ile içeriğinde virüs bulundurduğu mesajı gösterilmiştir.

Access has been Denied!

Access to the page:

<http://www.eicar.org/download/eicar.com.txt>

... has been denied for the following reason:

Virus or bad content detected. Eicar-Test-Signature

Categories:

Content scanning

You are seeing this error because what you attempted to access appears to contain, or is labeled as containing, material that has been deemed inappropriate.

If you have any queries contact your ICT Coordinator or Network Manager.

YOUR ORG NAME

Powered by [DansGuardian](#)

Dansguardian ile ilgili daha detaylı bilgiye www.enderunix.org/docs/dansguardian.pdf adresinden ulaşılabilir.