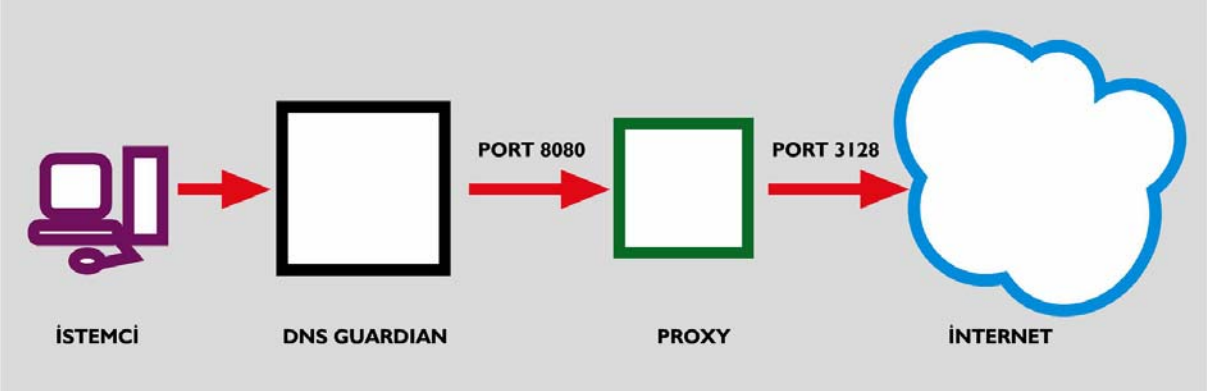
Gökhan ALKAN
gokhan [at] enderunix [dot] org
EnderUNIX Geliştirici
http://www.enderunix.org
Sürüm : 1.0
Tarih : 28.03.2006
Makalenin en yeni versiyonu http://www.enderunix.org/docs/dansguardian.pdf adresinde elde edilebilir.

1. Dansguardian Nedir?

Dansguardian Linux , FreeBSD ,OpenBSD , NetBSD , Mac OS X ve Solaris üzerinde çalışan web içerik filtreleme (http trafiğini filtreleme) yazılımıdır. Domain , kullanıcı ve ip bazlı filtreleme yeteneklerine sahip bir yazılım olan dansguardian'ın ana sayfasına

2. Dansguardian Nasıl Çalışır?

Dansguardian istemci internet tarayıcısı ile Proxy arasında bulunur ve aradaki trafik üzerinde gerekli işlemleri yapar. İstemci tarayıcısından çıkan web istekleri dansguardin'a ulaşır ve dansguardian filtreleme işlemlerini yaptıktan sonra isteği Proxy'ye gönderir. Aşağıda dansguardian çalışması şekillerle anlatılmıştır. Burada dansguardian'ın "8080" ve Proxy sunucusunun da "3128"'i posttan çalıştığı varsayılmıştır.



İstemciden web sunucusuna giden istek dansguardin'a gelir. Gerekli filtreleme işlemelerinden sonra paket Proxy'ye oradan da web sunucusuna iletilir. Web sunucusu paketi işleyip gerekli cevabı Proxy'ye gönderir ve oradan da tekrar dansguardin'a iletilir. Gerekli filtreleme işlemlerinden geçirildikten sonra paket istemciye geri döner. Dansguardian basit olarak bu şekilde çalışmaktadır.
Dansguardian Kurulumu

Kullanılan dağıtıma göre kurulum gerçekleştirilebilir. Burada kaynak koddan kurulumu anlatılacaktır. Kurulum için gerekli paket http://dansguardian.org/ adresinden temin edinilebilir. Burada dansguardian için şu anda son sürüm olan 2.9.6.1 sürümü kurulacaktır.

```
# cd /usr/local
# wget http://mirror2.dansguardian.org/downloads/2/Alpha/dansguardian-2.9.6.1.tar.gz
# tar –zxvf  dansguardian-2.9.6.1.tar.gz
```

Çalışma dizininde dansguardian-2.9.6.1 adından bir dizin oluşmaktadır. Kurulum için bu dizin içerisinde ./configure , make , make install , make clean betikleri çalıştırılarak kurulum temel olarak yapılabilir.

Özelleştirilmiş bir kurulum yapmak için ./configure betiğine çeşitli parametreler verilerek yapılabilir. ./configure –help ile bu parametreler öğrenilebilir.

3. Dansguardian Yapılandırması Ve Çalıştırılması

languagedir = ''
Dil dosyalarının bulunduğu dizin. İsteğe göre languagedir ile belirtilen dizin altındaki turkish dizini içindeki dosyalar düzenlenebilir.
languagedir = '/usr/local/share/dansguardian/languages'

language = ''
Bu parametre ile hata mesajlarının gösterileceği dil belirlenir.
language='turkish'

logfileformat=''
1 = DansGuardian format 2 = CSV-style format
3 = Squid Log File Format 4 = Tab delimited
İsteğe göre bir değer verilebilir. Eğer log analiz programı olarak sarg kullanılması düşünülüyorsa bu değer squid log dosyası biçimi olmalıdır. Çünkü Sarg ile dansguardian log dosyası biçimini analiz edilememektedir.
logfileformat='3'

loglocation = ''
Bu parametre ile dansguardian'ın log tutacağı dosyanın yeri belirtilir.
loglocation = '/var/log/dansguardian/access.log'

filterip = ‘’

Dansguardian'ın dinleyeceği ip adresi belirtilir. Eğer boş bırakılırsa dansguardian bütün ipleri dinleyecektir.

filterip=’192.168.1.1’

filterport = ‘’

Dansguardian’ın çalışacağı port numarasını belirtir.

filterport=’8080’

proxyip = ‘’

Dansguardian ile beraber çalışacak Proxy’nin çalıştığı ip numarası. Eğer dansguardian ve Proxy aynı makine üzerinde hizmet veriyorlarsa buraya 127.0.0.1 yazılabilir.

proxyip=’127.0.0.1’

proxyport = ‘’

Proxy’nin çalışacağı port numarası. Dansguardian istemciden gelen isteği alıp değerlendirdikten sonra bağlanacağı Proxy’nin çalıştığı port numarası.

proxyport=3128

weightedphrasemode = “”

Sizden yada bağlanmak istediğiniz sitenin bulunduğu sunucudaki trafik yükünün yoğun olmasından dolayı dansguardian geç açılan siteleri engellemektedir.Bu seçenek “0”,”1”,”2” değerlerini alabilmektedir. Bu özelliği iptal etmek için bu değer “o” yapılır.

weightedphrasemode = 0

4. Dansguardian Filtreleme İçin Gerekli Ayar Dosyaları

Dansguardian için gerekli kısıtlamaların yapılacağı ayar dosyaları lists dizini altında bulunur. Genel olarak banned ile başlayanlar yasaklamaları exception ile başlayanlarsa filtrelemenin yapılmayacağı es geçileceği yönündedir.

Bannedextensionlist:

Engellenmek istenen dosya uzantıları belirtilir.

Örnek tanımlama

.exe

.tar

Bu tanımla ile exe ve tar uzantılı dosyaların indirilmesi engellenmiş olur.

Bannediplist:

Engellenmek istenen ip adresleri belirtilir.

Örnek Tanımlama

192.168.1.1

Bu tanımlama ile 192.168.1.1 ipsinin internet erişimi yasaklanır.

Bannedmimetypelist

Engellenmek istenen MIME tiplerinin belirtilir.

Örnek Tanımlama

audio/mpeg

Bannedregexpurllist

URL'de geçen kelimeler için düzenli ifade deyimleri ile url bazında filtreleme yapılır.Bannedurllist dosyasından farkı düzenli ifade deyimlerinin kullanılabilmesidir.

Örnek Tanımlama

(nix|rosoft|nux)

Örneğin bu dosya içinde yapılacak (nix|rosoft|nux) gibi bir tanımla www.unix.org www.chinaunix.net , www.microsoft.com gibi siteler engellenmiş olur. Ayrıca daha ileri düzeyde düzenli ifade terimleri kullanılabilmektedir.

Bannedsitelist

Domain bazında filtrelemenin yapıldığı dosya. Bu dosyaya yazılacak domain isimleri engellenir.

Örnek Tanımlama

google.com

Bu tanımlama ile sadece google.com domaini yasaklanır. Yani www.google.com yada mail.google.com yasaklanmış olur ancak www.google.com.tr için yasaklama söz konusu değildir.

Bannedurllist

İstenilen URL'lerin bir kısmını yada tamamının engellenmesi için filtrelemenin uygulandığı dosya.

Örnek Tanımlama

google.com/bsd

Bu tanımlama ile www.google.com/bsd adresine erişim yasaklanmış olur ancak www.google.com/linux adresine erişim yapılabilir.

Domain bazında değil url bazında filtreleme yapılır.

Örnek Tanımlama

yahoo.com

Bu tanımla yapıldığı takdirde www.yahoo.com adresine erişim yasaklanmış olur ancak mail.yahoo.com adresine erişim sağlanabilir.

Exceptionfilesitelist

Dosya indirilecek olan sitelerin isimlerinin bulunduğu dosya.

Örnek tanımlama

windowsupdate.microsoft.com

Exceptioniplist

Engellenmek istenen ip adreslerinin bulunduğu dosya.

Örnek Tanımlama

192.168.1.1

Bu tanımlama ile 192.168.1.1 ipsi için filtreleme uygulanmaz.

Exceptionregexpurllist
URL'de geçen kelimeler için filtreleme yapılmaması istenen adresler belirtilir.
Örnek Tanımlama
ender

Bu tanımlama ile URL'de ender geçen adresler filtrelenmez

Exceptionsitelist
Filtrelemenin yapılmayacağı domain isimleri belirtilir.
Örnek Tanımlama
yahoo.com

Bu tanımlama ile yahoo.com sitesi için filtreleme yapılmaz.

Exceptionurllist
Filtrelemenin yapılmayacağı site bölümleri belirtilir. google.com/bsd yada enderunix.org/openbsd doğru tanımlamalardır.
Örnek Tanımlama
google.com/bsd

Bu tanımlama ile google.com/bsd adresi için filtreleme uygulanmaz.

Blacklist
SquidGuard'dan alınan kara liste uygulamasının yapıldığı siteler ve URL'ler bulunur. İsteğe göre bu klasör içerisindeki dosyalara eklemeler yapılarak engellenmek istenen domain yada URL'ler yazılabilir.

Greysitelist
Dansguardian çalışma mantığına göre "grey" listeleri "banned" listelerinin üstüne yazar. Aynı şekilde "exception" listeleri de "banned" listelerinin üstüne yazar. Grey listesinin exception listesinden farkı url filtrelemesini es geçmek ve diğer filtreleme kurallarının yapılmasıdır.

Aşağıdaki dosyalarda gerekli belirtimler yapılsın

Bannedsitelist → enderunix.org
Bannedextensionlist → .tgz

Bu şekilde ne enderunix.org adresine nede http://www.enderunix.org/isoqlog/isoqlog-2.2.1.tar.gz dosyasına erişim yapılabilir. Eğer enderunix.org ile ilgili hiçbir filtrelememenin yapılmaması isteniyorsa enderunix.org exceptionsitelist dosyasında belirtilmelidir.

Exceptionsitelist → enderunix.org

Bu şekilde hem enderunix.org adresine hemde http://www.enderunix.org/isoqlog/isoqlog-2.2.1.tar.gz dosyasına erişim yapılabilir. Ancak enderunix.org adresine erişim sağlansın ancak

enderunix.org sitesi için gerekli diğer filtrelemeler yapılsın istenirse burada grey listeleri kullanılmalıdır.

Bannedsitelist → enderunix.org
Bannedextensionlist → .tgz

Greysitelist → enderunix.org

Bu şekilde yapılan bir tanımlama ile www.enderunix.org sitesine erişim yapılabilir ancak http://www.enderunix.org/isoqlog/isoqlog-2.2.1.tar.gz dosyası temin edilemez çünkü www.enderunix.org için gerekli filtrelemeler yapılmış ve bannedextensionlist dosyasında tgz uzantılı dosyalar yasaklandığı için isoqlog-2.2.1.tar.gz dosyasına erişim yapılamaz.

Greyurllist
Greysitelist dosyasında exception listeleri banned listelerinin üstüne yazar.grey listeleri de banned listelerinin üstüne yazar ancak exception listelerinden farkı; exception listeleri filtrelemeyi tamamen kaldırır.Grey listeleri ise filtrelemede istenilen bir bölümü kaldırır tüm filtrelemeyi değil.

Bannedsitelist → enderunix.org

Greyurllist → enderunix.org/isoqlog

Bu şekilde bir tanımlama ile www.enderunix.org/isoqlog için filtreleme yapılmaz ve www.enderunix.org/isoqlog adresine erişim yapılabilir.

5. Dansguardian İle Filtre Gruplarının Oluşturulması

Dansguardian'da filtreleme grupları oluşturarak istenilen kullanıcıları belirlenen gruplara atayarak gruplara özgü filtreleme seçenekleri oluşturulabilir.
Öncelikle dansguardian.conf dosyası içerisindeki değişikliklerin yapılması gerekiyor.

```
#  vi dansguardian.conf
filtergroups = 4
filtergroupslist = '/usr/local/etc/dansguardian/lists/filtergrouplist'
#
```

"filtergroups"
değişkeni ile kaç tane filtre grubu oluşturulacağı belirleniyor. Burada 4 tane filtreleme grubu oluşturularak örnekler verilecek.

"*filtergroupslist = '/usr/local/etc/dansguardian/lists/filtergrouplist' "*
ile de filtreleme gruplarının tanımlarının yapılacağı yer belirtiliyor.

```
192.168.195.159=filter1
192.168.193.47=filter2
192.168.195.250=filter3
81.213.183.239=filter4
```

"authplugin = '/usr/local/etc/dansguardian/authplugins/ip.conf'"

bu değer ile de ip bazlı tanımlamlamaların yapılacağı belirtiliyor .

“/usr/local/etc/dansguardian/authplugins/ip.conf”

ip bazlı tanımlamalar yapılırken oluşturulacak grupların bulunacağı dosya belirtiliyor.

```
plugname = 'ip'
ipgroups = '/usr/local/etc/dansguardian/lists/authplugins/ipgroups'
```

filtreleme grupları oluşturuluyor. İsteğe göre düzenlenip gruplar oluşturulabilir.

```
192.168.195.159=filter1
192.168.193.47=filter2
192.168.195.250=filter3
81.213.183.239=filter4
```

6. Dansguardian Çalıştırılması

Kurulum esnasında ./configure betiğine verilen sysvdir seçeneğine göre scripts dizini altında başlangıç için hazır betikler bulunur. Kullanılan sisteme göre buradaki hazır betikler kullanılabilir yada özelleştirilebilir. Burada OpenBSD üzerine kurulum gerçekleştirildiği için

```
# cp bsd-init /usr/bin/dansguardian-hazir-betik
# chmod 755 cp bsd-init /usr/bin/dansguardian-hazir-betik
# dansguardian-hazir-betik start
# dansguardian-hazir-betik stop
```

başlangıç için kullanılacak hazır betik dosyası PATH değişkeninin tanımlı olduğu bir dizine kopyalanır ve çalıştırılabilir olması için gerekli izinler chmod komutuyla verilir. PATH değişkenin tanımlı olduğu dizinleri öğrenmek için env kullanılabilir.

```
# env | grep ‘PATH’
PATH=/sbin:/usr/sbin:/bin:/usr/bin:/usr/X11R6/bin:/usr/local/sbin:/usr/local/bin
#
```

Ardından betiğe verilerek start ve stop komutlarıyla dansguardian başlatılır yada durdurulur.

ps ile dansguardian çalışması kontrol edilebilir.

```
# ps –auwx | grep ‘dansguardian’
nobody   29716  0.0  0.4 23604  1856 ??  Ss    12:23PM    0:00.08
/usr/local/sbin/dansguardian
nobody    6783  0.0  0.3 23688  1740 ??  I     12:31PM    0:00.03
/usr/local/sbin/dansguardian
….
….
#
```

Ayar dosyalarında gerekli değişiklikler yapıldıktan sonra değişikliklerin etkin olabilmesi için ya dansguardian durdurulup yeniden başlatılmalıdır yada dansguardian –r parametresi verilerek çalıştırmalıdır. which komutuyla dansguardian tam yolu bulunmalıdır.

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

ardından ***–r*** parametresi ile değişikliklerin etkin olması sağlanır.

```
# /usr/local/sbin/dansguardian -r
```

Aynı şekilde dansguardianı durdurmak için –q parametresi verilebilir yada hazır betikleri ile de aynı işlem gerçekleştirilebilir.

```
# dansguardian -q
```

7. Dansguardian Log Takibi

Dansguardian.conf dosyası içinde "loglocation " parametresiyle belirtilen değişkene verilen dizinde dansguardian log'ları tutulur. Buradan erişim yapılan adresler takip edilebilir.

```
# tail -f /var/log/dansguardian/access.log
  1143025442.897   1196 192.168.195.250 TCP_MISS/200 17529 GET
http://www.enderunix.org/ - DEFAULT_PARENT/127.0.0.1 -
…
#
```