Ozan UÇAR 28.01.2010
mail@ozanucar.com
www.cehturkiye.com

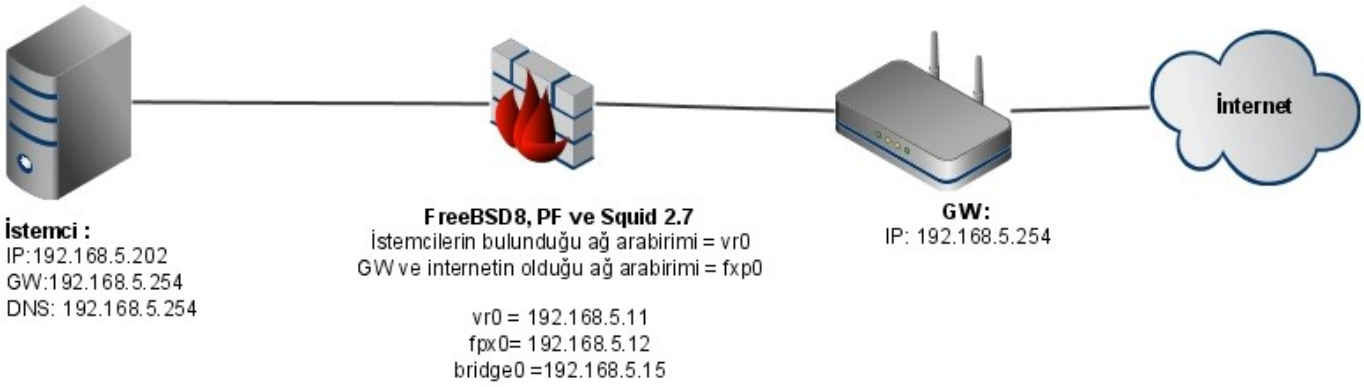
Bridge FreeBSD PF ve Transparent Squid

FreeBSD işletim sistemini bridge modda yapılandırıp üzerinde PF (packet filter) ile transparent squid kullanımı anlatılmıştır.

Nasıl Çalışır

FreeBSD PF fiziksel olarak gateway ile istemciler arasına yerleştirilir, mevcut network yapısı ve istemcilerin ağ ayarları değiştirilmeden (proxy, gateway vs.) layer 2 seviyesinde filtreleme yapılır.İstemciler bilinmeyenlerin çıkış noktası olarak yine gateway'lerini görürler ve internete çıkmak için tüm paketleri gateway'lerine iletirler fakat gateway'lerine paketler ulaşmadan bridge modda çalışan PF ve Squid bunları işlenen kural listesine göre süzüp ardından trafiği olduğu gibi (nat vs. yapmadan) gateway'e iletir.Bridge modda FreeBSD tıpkı bir switch gibi çalışır ...

Böylelikle görünmez modda PF ve Squid çalıştırmış oluyoruz.



İstenilen Network Yapısı

FreeBSD bridge yapılandırması

Ağ kartlarının "fxp0" ve "fxp1" olduğu düşünülmüştür.

```
# ifconfig bridge create
bridge0
# ifconfig bridge0
bridge0: flags=8802<BROADCAST,SIMPLEX,MULTICAST> metric 0 mtu 1500
        ether 96:3d:4b:f1:79:7a
        id 00:00:00:00:00:00 priority 32768 hellotime 2 fwddelay 15
        maxage 20 holdcnt 6 proto rstp maxaddr 100 timeout 1200
        root id 00:00:00:00:00:00 priority 0 ifcost 0 port 0


# ifconfig bridge0 addm fxp0 addm fxp1 up
# ifconfig fxp0 up
```

```
# ifconfig fxp1 up
```

Ayarların açılışta geçerli olması için `/etc/rc.conf` dosyasına aşağıdaki satırlar eklenir;

```
cloned_interfaces="bridge0"
ifconfig_bridge0="addm fxp0 addm fxp1 up"
ifconfig_fxp0="up"
ifconfig_fxp1="up"
```

Bridge interface için ip ataması yapılmak isteniliyorsa;

```
ifconfig bridge0 inet 192.168.0.1/24
```

PF (Packet Filter) ile istemcilerden gelen ve hedef port 80 olan isteklerin squid'e yönlendirilmesi

```
PF aktif edilmesi ;

kldload pf.ko

/etc/rc.conf;
pf_enable="YES"
pf_rules="/etc/pf.conf"
pf_flags=""
pflog_enable="YES"
pflog_logfile="/var/log/pflog"
pflog_flags=""

Servisin başlatılması
#/etc/rc.d/pf start
```

Kural dosyası

 # touch /etc/pf.conf

İstemcilerden gelen herhangi bir hedefin 80. Portuna giden istekler squid e yönlendirilir

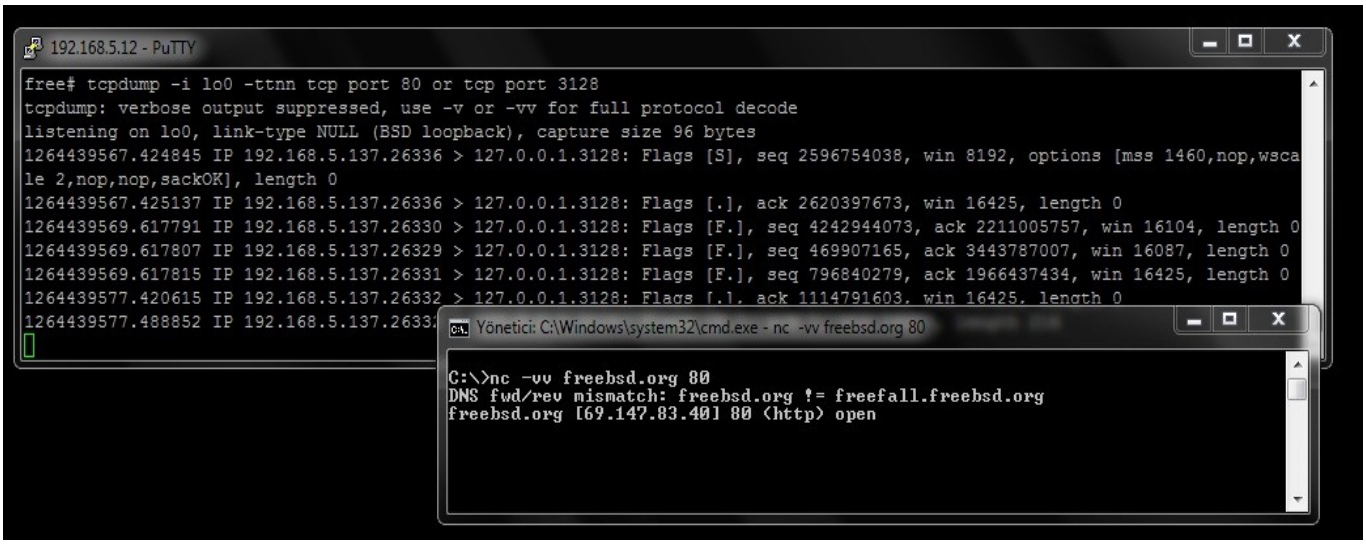
pf.conf ;

int_if="vr0"

ext_if="fxp0"

rdr on $int_if inet proto tcp from $lan to any port { 80 443 } -> 127.0.0.1 port 3128

pass in quick on $int_if route-to lo0 inet proto tcp from $lan to 127.0.0.1 port 3128 keep state



Not: $lan = yerel network aralığınız. Örnek : 192.168.5.0/24

Squid Kurulumu;
-Port ağacından kurulumu ;
 # cd /usr/ports/www/squid && make install clean

Not: squid port ağacından kurarken PF desteğini aktif etmenizde fayda var.

- Depodan kurulumu
 # pkg_add –rv ftp://ftp.freebsd.org/pub/FreeBSD/ports/i386/packages-7-stable/Latest/squid.tbz

Transparent olarak çalışması için squid.conf dosyasına eklenecek satır ;
http_port 127.0.0.1:3128 transparent

Eğer herşey yolunda gittiyse squid.conf dosyasına aşağıdaki gibi bir kural tanımlayıp test edebilirsiniz ;

acl yasakli dstdomain .yahoo.com
http_access deny yasakli

www.yahoo.com adresine erişiminiz squid tarafından engellenir.

Daha fazla bilgi;
Bridge: http://www.freebsd.org/doc/handbook/network-bridging.html
Pf ve Squid : http://www.benzedrine.cx/transquid.html