

# OpenBSD PF CARP ve pfSync ile Redundancy Firewall

---

oucar@bga.com.tr

**Ozan UÇAR**

**30.03.2011**

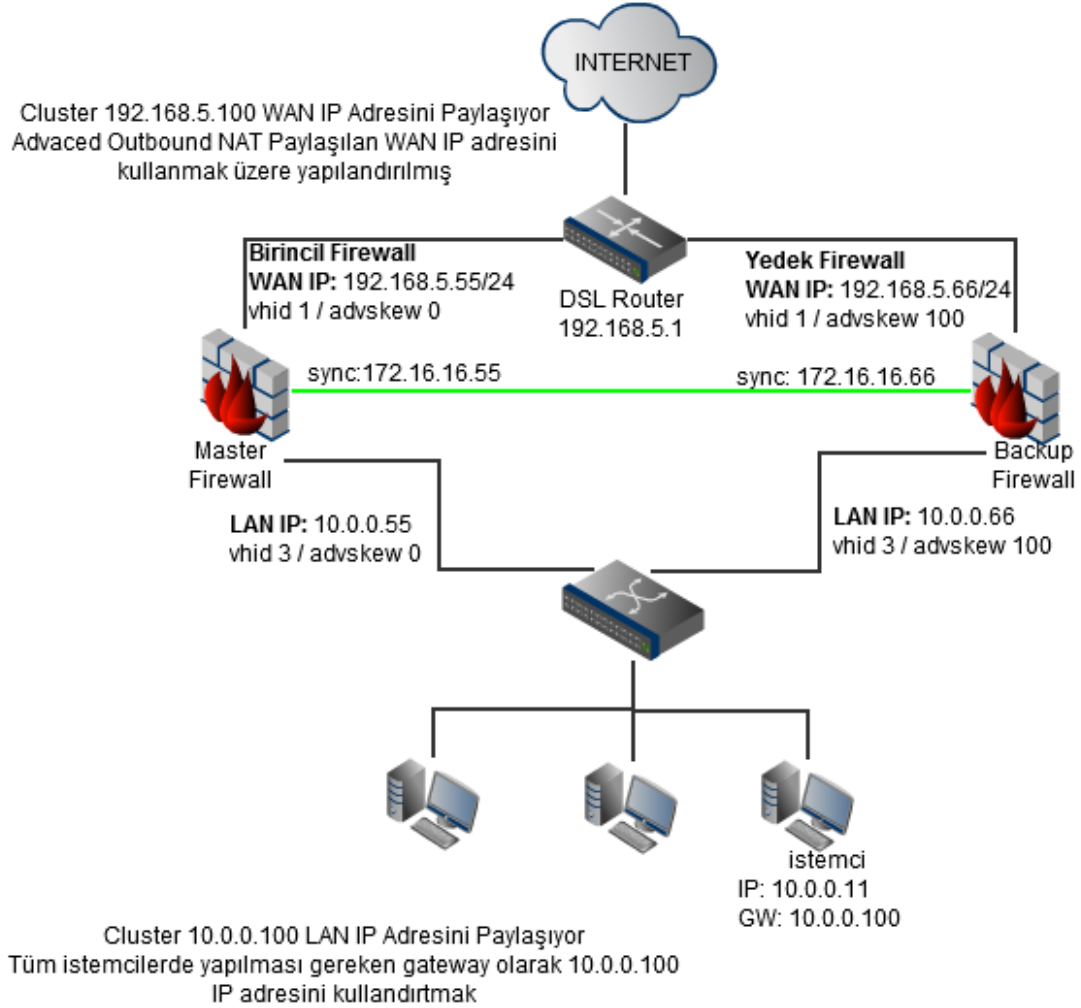
Firewall'lar ağ sınır güvenliğinin vazgeçilmezi ve en kritik seviyede çalışan sistemlerden biridir. Firewall donanımsal veya yazılımsal bir sorun yaşattığında, yerel ağı dünyaya bağlayan nokta kesilir, bu durumda iş yükü ve kazanç için düşünmek istemediğimiz tüm kabus senaryoları bir bir işlemeye başlar. Bu belge, iki OpenBSD PF firewall arasında cluster yapısı ve failover anlatılmıştır. Bir firewall hizmet dışı kalınca, anında diğerinin devreye girmesi ve senkronize çalışması bir senaryo üzerinden anlatılmıştır. Belge, uygulamaya yönelik olup pf kurallanımı ile ilgili fazla teknik detay içermemektedir. Geri bildirimlerde bulunarak katkı sağlayabilirsiniz.

## İçindekiler

Gereksinimler .....	3
OpenBSD PF Master Firewall Yapılandırması .....	4
OpenBSD Master Ağ Arabirimleri .....	4
Ağ Ayarlarını Yapılandırmak.....	4
OpenBSD MASTER Ağ Ayarlarının Çıktısı .....	5
WAN arabirimine (em1) bağlı carp1 sanal interface.....	6
LAN arabirimine (em0) bağlı carp1 sanal interface .....	6
CARP işlemi için ihtiyacımız olan sistem ayarları.....	6
OpenBSD PF Backup Firewall Yapılandırması .....	7
OpenBSD Backup Ağ Arabirimleri .....	7
Ağ Ayarlarını Yapılandırmak.....	7
OpenBSD Backup Ağ Ayarlarının Çıktısı .....	8
WAN arabirimine (em1) bağlı carp1 sanal interface.....	9
LAN arabirimine (em0) bağlı carp1 sanal interface .....	9
CARP işlemi için ihtiyacımız olan sistem ayarları.....	9
Minimum pf.conf ayarları .....	9
pf.conf kuralları.....	10
Failover cluster Sistemin Test Edilmesi .....	10
Master Firewall üzerinden,bakalım trafik geçiyor mu ?.....	11
Hostname i backup.bga.com.tr olan Backup Firewall durumu.....	11
Bacup Firewall üzerinden,bakalım trafik geçiyor mu ? .....	12
Eklenecekler.....	12

## Gereksinimler

Bu belgede kullanılan işletim sistemleri OpenBSD 4.7 , diğer \*BSD istemlerde pf aktif edilerek aynı mantıkla carp işlemini yapabilirsiniz.



### OpenBSD CARP Network Şeması

*Dikkat: Aşağıdaki bilgileri kendi sisteminize ve ağ yapınıza göre düzenleyiniz aksi taktirde bire bir yaptığınız ayarlar çalışmayabilir.*

## OpenBSD PF Master Firewall Yapılandırması

```
# uname -a
OpenBSD master.bga.com.tr 4.7 GENERIC#558 i386
# cat /etc/mygate
192.168.5.254
# cat /etc/myname
master.bga.com.tr
```

## OpenBSD Master Ağ Arabirimleri

```
lan:em0
wan:em1
pfsync:em2
```

## Ağ Ayarlarını Yapılandırmak

```
# cat /etc/hostname.em0
inet 10.0.0.55 255.255.255.0 NONE
# cat /etc/hostname.em1
inet 192.168.5.55 255.255.255.0
# cat /etc/hostname.em2
inet 172.16.16.55 255.255.255.0 NONE
# cat /etc/hostname.pfsync0
up syncdev em2
```

## OpenBSD MASTER Ağ Ayarlarının Çıktısı

```
# ifconfig
lo0: flags=8049 mtu 33200
priority: 0
groups: lo
inet6 ::1 prefixlen 128
inet6 fe80::1%lo0 prefixlen 64 scopeid 0x5
inet 127.0.0.1 netmask 0xff000000
em0: flags=8b43 mtu 1500
lladdr 00:0c:29:b4:d4:59
priority: 0
media: Ethernet autoselect (1000baseT full-duplex, master)
status: active
inet6 fe80::20c:29ff:feb4:d459%em0 prefixlen 64 scopeid 0x1
inet 10.0.0.55 netmask 0xfffff00 broadcast 10.0.0.255
em1: flags=8b43 mtu 1500
lladdr 00:0c:29:b4:d4:63
priority: 0
groups: egress
media: Ethernet autoselect (1000baseT full-duplex, master)
status: active
inet6 fe80::20c:29ff:feb4:d463%em1 prefixlen 64 scopeid 0x2
inet 192.168.5.55 netmask 0xfffff00 broadcast 192.168.5.255
em2: flags=8843 mtu 1500
lladdr 00:0c:29:b4:d4:6d
priority: 0
media: Ethernet autoselect (1000baseT full-duplex, master)
status: active
inet6 fe80::20c:29ff:feb4:d46d%em2 prefixlen 64 scopeid 0x3
inet 172.16.16.55 netmask 0xfffff00 broadcast 172.16.16.255
enc0: flags=0<> mtu 1536
priority: 0
pfsync0: flags=41 mtu 1500
priority: 0
pfsync: syncdev: em2 maxupd: 128 defer: off
groups: carp pfsync
pflog0: flags=141 mtu 33200
priority: 0
groups: pflog
carp1: flags=8843 mtu 1500
lladdr 00:00:5e:00:01:01
priority: 0
carp: MASTER carpdev em1 vhid 1 advbase 20 advskew 0
groups: carp
inet6 fe80::200:5eff:fe00:101%carp1 prefixlen 64 scopeid 0x6
inet 192.168.5.100 netmask 0xfffff00 broadcast 192.168.5.255
```

```
carp2: flags=8843 mtu 1500
lladdr 00:00:5e:00:01:02
priority: 0
carp: MASTER carpdev em0 vhid 2 advbase 20 advskew 0
groups: carp
inet6 fe80::200:5eff:fe00:102%carp2 prefixlen 64 scopeid 0x7
inet 10.0.0.100 netmask 0xfffff00 broadcast 10.0.0.255
```

### WAN arabirimine (em1) baęlı carp1 sanal interface

```
# cat /etc/hostname.carp1
inet 192.168.5.100 255.255.255.0 192.168.5.255 vhid 1 advbase 20 advskew 0 carpdev
em1 pass benimgizliparolam
```

### LAN arabirimine (em0) baęlı carp1 sanal interface

```
inet 10.0.0.100 255.255.255.0 10.0.0.255 vhid 2 advbase 20 advskew 0 carpdev em0
pass benimgizliparolam
```

### CARP iřlemi iin ihtiyacımız olan sistem ayarları

```
# sysctl net.inet.ip.forwarding=1
net.inet.ip.forwarding: 0 -> 1
# sysctl -w net.inet.carp.allow=1
net.inet.carp.allow: 1 -> 1
# sysctl -w net.inet.carp.preempt=1
net.inet.carp.preempt: 0 -> 1
# sysctl -w net.inet.carp.log=1
net.inet.carp.log: 0 -> 1
```

## OpenBSD PF Backup Firewall Yapılandırması

```
# uname -a
OpenBSD backup.bga.com.tr 4.7 GENERIC#558 i386
# cat /etc/mygate
192.168.5.254
# cat /etc/myname
backup.bga.com.tr
```

## OpenBSD Backup Ağ Arabirimleri

```
lan:em0
wan:em1
pfsync:em2
```

## Ağ Ayarlarını Yapılandırmak

```
# cat /etc/hostname.em0
inet 10.0.0.66 255.255.255.0 NONE
# cat /etc/hostname.em1
inet 192.168.5.66 255.255.255.0
# cat /etc/hostname.em2
inet 172.16.16.66 255.255.255.0 NONE
# cat /etc/hostname.pfsync0
up syncdev em2
```

## OpenBSD Backup Ağ Ayarlarının Çıktısı

```
# ifconfig
lo0: flags=8049 mtu 33200
priority: 0
groups: lo
inet6 ::1 prefixlen 128
inet6 fe80::1%lo0 prefixlen 64 scopeid 0x5
inet 127.0.0.1 netmask 0xff000000
em0: flags=8b02 mtu 1500
lladdr 00:0c:29:83:49:fc
priority: 0
media: Ethernet autoselect (none)
status: no carrier
inet 10.0.0.66 netmask 0xfffff00 broadcast 10.0.0.255
inet6 fe80::20c:29ff:fe83:49fc%em0 prefixlen 64 duplicated scopeid 0x1
em1: flags=8b43 mtu 1500
lladdr 00:0c:29:83:49:06
priority: 0
groups: egress
media: Ethernet autoselect (1000baseT full-duplex,master)
status: active
inet6 fe80::20c:29ff:fe83:4906%em1 prefixlen 64 scopeid 0x2
inet 192.168.5.66 netmask 0xfffff00 broadcast 192.168.5.255
em2: flags=8843 mtu 1500
lladdr 00:0c:29:83:49:10
priority: 0
media: Ethernet autoselect (1000baseT full-duplex,master)
status: active
inet 172.16.16.66 netmask 0xfffff00 broadcast 172.16.16.255
inet6 fe80::20c:29ff:fe83:4910%em2 prefixlen 64 duplicated scopeid 0x3
enc0: flags=0<> mtu 1536
priority: 0
pflog0: flags=141 mtu 33200
priority: 0
groups: pflog
carp1: flags=8843 mtu 1500
lladdr 00:00:5e:00:01:01
priority: 0
carp: BACKUP carpdev em1 vhid 1 advbase 20 advskew 0
groups: carp
inet6 fe80::200:5eff:fe00:101%carp1 prefixlen 64 scopeid 0x7
inet 192.168.5.100 netmask 0xfffff00 broadcast 192.168.5.255
carp2: flags=8803 mtu 1500
lladdr 00:00:5e:00:01:02
priority: 0
carp: INIT carpdev em0 vhid 2 advbase 20 advskew 0
```

```
groups: carp
inet6 fe80::200:5eff:fe00:102%carp2 prefixlen 64 scopeid 0x8
inet 10.0.0.100 netmask 0xfffff00 broadcast 10.0.0.255
```

### WAN arabirimine (em1) baęlı carp1 sanal interface

```
# cat /etc/hostname.carp1
inet 192.168.5.100 255.255.255.0 192.168.5.255 vhid 1 advbase 20 advskew 0 carpdev
em1 pass benimgizliparolam
```

### LAN arabirimine (em0) baęlı carp1 sanal interface

```
inet 10.0.0.100 255.255.255.0 10.0.0.255 vhid 2 advbase 20 advskew 0 carpdev em0
pass benimgizliparolam
```

### CARP iřlemi iin ihtiyacımız olan sistem ayarları

```
# sysctl net.inet.ip.forwarding=1
net.inet.ip.forwarding: 0 -> 1
# sysctl -w net.inet.carp.allow=1
net.inet.carp.allow: 0 -> 1
# sysctl -w net.inet.carp.preempt=1
net.inet.carp.preempt: 0 -> 1
# sysctl -w net.inet.carp.log=1
net.inet.carp.log: 0 -> 1
```

### Minimum pf.conf ayarları

```
# cat /etc/pf.conf
# $OpenBSD: pf.conf,v 1.49 2009/09/17 06:39:03 jmc Exp $
# C | EH TURKIYE
# See pf.conf(5) for syntax and examples.
# Remember to set net.inet.ip.forwarding=1 and/or net.inet6.ip6.forwarding=1
# in /etc/sysctl.conf if packets are to be forwarded between interfaces.

# Aę Arabirimleri
IntIf="em0"
ExtIf="em1"
CarpIf="em2"
PFSync="em2"

#Network Tanımları
CarpExt="{192.168.5.55, 192.168.5.66}"
CarpInt="{10.0.0.55, 10.0.0.66}"
IntNet="10.0.0.0/24"
```

## pf.conf kuralları

```
# CARP firewall failover kuralları
pass quick log on $PFSSync proto pfsync keep state (no-sync)
pass in quick log on $ExtIf proto carp from $CarpExt to 224.0.0.18 keep state
pass in quick log on $IntIf proto carp from $CarpInt to 224.0.0.18 keep state

### Network Address Translation
match out log on egress from (self) to any tag EGRESS nat-to ($ExtIf:0) port
1024:65535
match out log on egress from $IntNet to any received-on $IntIf tag EGRESS nat-to
carp1 port 1024:65535

set skip on lo

in log (all) all # keep-state baglanti kur
pass out log (all) all

# varsayilan block kurali
block in on ! lo0 proto tcp to port 6000:6010
```

*Not: Minimum pf.conf ayarları ve kuralları her iki pf için yazılmalıdır.*

## Failover cluster Sistemin Test Edilmesi

İstemciden [www.bga.com.tr](http://www.bga.com.tr) adresine bağlantı kuruyoruz. Bağlantı istekleri MASTER sunucu tarafından yönlendiriliyor.

Şu an Master Firewall olarak [master.bga.com.tr](http://master.bga.com.tr) firewall' u devrede ;

```
# ifconfig carp
carp1: flags=8843 mtu 1500
lladdr 00:00:5e:00:01:01
priority: 0
carp: MASTER carpdev em1 vhid 1 advbase 20 advskew 0
groups: carp
inet6 fe80::200:5eff:fe00:101%carp1 prefixlen 64 scopeid 0x6
inet 192.168.5.100 netmask 0xfffff00 broadcast 192.168.5.255
carp2: flags=8843 mtu 1500
lladdr 00:00:5e:00:01:02
priority: 0
carp: MASTER carpdev em0 vhid 2 advbase 20 advskew 0
groups: carp
inet6 fe80::200:5eff:fe00:102%carp2 prefixlen 64 scopeid 0x7
inet 10.0.0.100 netmask 0xfffff00 broadcast 10.0.0.255
pfsync0: flags=41 mtu 1500
priority: 0
pfsync: syncdev: em2 maxupd: 128 defer: off
groups: carp pfsync
```

## Master Firewall üzerinden,bakalım trafik geçiyor mu ?

```
# tcpdump -nn -ttt -i em0 host 10.0.0.11 and tcp port 80
tcpdump: listening on em0, link-type EN10MB
Aug 16 17:20:16.736101 10.0.0.11.1477 > 83.66.140.10.80: P
3434076927:3434077718(791) ack 3491673519 win 64901 (DF)
Aug 16 17:20:16.736107 10.0.0.11.1477 > 83.66.140.10.80: P 0:791(791) ack 1 win 64901
(DF)
Aug 16 17:20:16.737067 83.66.140.10.80 > 10.0.0.11.1477: . ack 791 win 64909 (DF)
Aug 16 17:20:16.737074 83.66.140.10.80 > 10.0.0.11.1477: . ack 791 win 64909 (DF)
Aug 16 17:20:16.737079 83.66.140.10.80 > 10.0.0.11.1477: . ack 791 win 64909 (DF)
Aug 16 17:20:16.737092 83.66.140.10.80 > 10.0.0.11.1477: . ack 791 win 64909 (DF))
Aug 16 17:20:16.916555 10.0.0.11.1477 > 83.66.140.10.80: . ack 4206 win 65535 (DF)
```

Şimdi Master Firewall kapatıp, BACKUP Firewall durumunu gözlemleyelim. Master Firewall devre dışı kalınca, Backup firewall yaklaşık 20 saniye içerisinde otomatik olarak devreye girip **carp: MASTER** olarak hizmet vermeye başlayacak.

*master.bga.com.tr* devre dışı bırakıyoruz;

```
# ifconfig em0 down
# ifconfig em1 down
```

## Hostname i backup.bga.com.tr olan Backup Firewall durumu

```
# ifconfig carp
carp1: flags=8843 mtu 1500
lladdr 00:00:5e:00:01:01
priority: 0
carp: MASTER carpdev em1 vhid 1 advbase 20 advskew 0
groups: carp
inet6 fe80::200:5eff:fe00:101%carp1 prefixlen 64 scopeid 0x7
inet 192.168.5.100 netmask 0xfffff00 broadcast 192.168.5.255
carp2: flags=8803 mtu 1500
lladdr 00:00:5e:00:01:02
priority: 0
carp: INIT carpdev em0 vhid 2 advbase 20 advskew 0
groups: carp
inet6 fe80::200:5eff:fe00:102%carp2 prefixlen 64 scopeid 0x8
inet 10.0.0.100 netmask 0xfffff00 broadcast 10.0.0.255
```

## Bacup Firewall üzerinden,bakalım trafik geçiyor mu ?

```
# tcpdump -nn -ttt -i em0 host 10.0.0.11 and tcp port 80
tcpdump: listening on em0, link-type EN10MB
Aug 16 17:20:16.736101 10.0.0.11.1477 > 83.66.140.10.80: P
3434076927:3434077718(791) ack 3491673519 win 64901 (DF)
Aug 16 17:20:16.736107 10.0.0.11.1477 > 83.66.140.10.80: P 0:791(791) ack 1 win 64901
(DF)
Aug 16 17:20:16.737067 83.66.140.10.80 > 10.0.0.11.1477: . ack 791 win 64909 (DF)
Aug 16 17:20:16.737074 83.66.140.10.80 > 10.0.0.11.1477: . ack 791 win 64909 (DF)
Aug 16 17:20:16.737079 83.66.140.10.80 > 10.0.0.11.1477: . ack 791 win 64909 (DF)
```

Görüldüğü gibi Master Firewall devre dışı kalınca istemcilerin trafiği, Backup Firewall üzerinden devam ediyor.Cluster yapımız bu haliyle muhteşem çalışmakta, bir firewall gidince bir kaç saniye içerisinde yerini diğeri alıyor.

### Eklenecekler

OpenBSD PF Layer 2 Firewall ile CARP, pfsync yapılabilir mi ?

### Referanslar;

[www.openbsd.org/faq/pf/carp.htm](http://www.openbsd.org/faq/pf/carp.htm)

[www.countersiege.com/doc/pfsync-carp/](http://www.countersiege.com/doc/pfsync-carp/)