

## Firewall Log'larını Anlık İzleme

(+) *Bu yazı birebir denenmiştir ve başarılı olunmuştur.*

Firewall paketlerin geçişini kontrol eden donanımdır. Paketlerin geçişine izin verip vermeme gibi kararlar alır ve her paket için verdiği kararı raporlar (log'lar). Bu yazıda firewall'ın log'larını iç ağdaki bir bilgisayara yönlendirip iç ağdaki bilgisayardan log'ların nasıl anlık olarak izlenebileceği gösterilecektir.

Firewall paketlerin geçişine izin verilip verilmeyeceğini (DROP ve ALLOW ile) tayin eden bir yazılımdır. Router içerisindeki firewall bu kontrolü yaparken log kaydı tutma özelliğine de sahiptir. Ancak router'ın belleği kısıtlı olduğu için log kaydı tutma işlemi router üzerinde yapılmamaktadır. Bu iş için log'ların depolanabileceği bir server makina kullanılmaktadır.

Diyelim ki Ubuntu 14.04 işletim sistemine sahip Asus Laptop'ımı server yapmak istiyorum. Böylece router'daki log'ları kendime yönlendirip depolayabileceğim. Kendi makinamı log sunucusu yapabilmek için syslog yazılımından faydalanabilirim. Bu yazıda anlatılan teknik işlemler tamamlandığında router, log'ları gönderen client hükmünde olacakken makinam ise log'ları kaydeden server konumunda olacaktır. O halde hadi başlayalım:

İlk olarak Ubuntu 14.04 işletim sistemini log sunucusu yapalım. Bunun için rsyslog daemon'ını yapılandırmamız gerekmektedir. O yüzden aşağıdaki gibi rsyslog daemon'ının dosyasını açalım.

```
> nano /etc/rsyslog.conf // rsyslog kurulu gelmezse > apt-get install rsyslog
```

Açılan dosyada yer alan aşağıdaki satırların başındaki diyez işaretlerini kaldıralım:

```
$ModLoad imudp  
$UDPServerRun 514
```

Daha sonra dosyanın en altına şu satırları koyalım:

```
$template TmplAuth,  
/var/log/firewall.log
```

NOT: Sistemimden kaynaklanan bir problem dolayısıyla bu yazıda bahsedilen tüm teknik işlemler tamamlandığında log dosyası kernel hatalarıyla dolup taşıtı. Bu işi çözebilmek için /etc/rsyslog.conf dosyasında yer alan aşağıdaki kodun başına diyez işareti koyarak kernel hatalarını kapatalım.

```
#$ModLoad imklog
```

Daha sonra /var/log klasörünün sahibini syslog yapalım:

```
> cd /var && sudo chown syslog:syslog log
```

En sonunda ise rsyslogd daemon'ını tekrar başlatalım:

```
sudo service rsyslog restart // root olsan bile sudo kullan. Aksi takdirde service bulunamıyor.
```

Böylece sistemimizi log sunucusu yapmış olduk ve router'dan log almaya hazır konuma getirdik. Şimdi router'ı log gönderir hale getirelim. Bunun için router'ın arayüzüne girip Firewall ayarlarından log gönderilecek IP adresi olarak kendi makinamızın IP adresini girelim.

<http://192.168.0.1>

// Router Arayüzüne Götürür



Yukarıdaki resimden görülebileceği üzere Güvenlik Duvarı -> Uzak Kütük sekmesine geçilerek log'ların gönderileceği adres olarak kendi makinamızın IP'si koyulmuştur. Uygula butonuna basıldıktan sonra router'ın içerisindeki firewall yazılımı log'ları makinamıza göndermeye başlayacaktır.

Router makinasından gelen log kayıtlarını /var/log dizini altında yer alan firewall.log dosyasına bakarak görüntüleyebiliriz.

```
> tail -f /var/log/firewall.log
```

Output:

```
root@hefese-N61Jq: /var/log
root@hefese-N61Jq: /var/log# tail -f routerTraffic.log
Nov 25 15:56:33 2016 SYSLOG[0]: message repeated 5 times: [ [Host 192.168.0.1] UDP 192.168.0.11,137 --> 192.168.0.255,137 ALLOW: Inbound access request ]
Nov 25 15:56:33 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 61.182.87.144,62908 --> 178.233.170.175,23 DENY: Firewall interface access request
Nov 25 15:56:33 2016 SYSLOG[0]: [Host 192.168.0.1] UDP 192.168.0.11,55662 --> 178.233.140.110,53 ALLOW: Outbound access request [DNS query for ki2542080031.sgk.intra.]
Nov 25 15:56:33 2016 SYSLOG[0]: [Host 192.168.0.1] UDP 192.168.0.11,137 --> 192.168.0.255,137 ALLOW: Inbound access request
Nov 25 15:56:33 2016 SYSLOG[0]: message repeated 2 times: [ [Host 192.168.0.1] UDP 192.168.0.11,137 --> 192.168.0.255,137 ALLOW: Inbound access request ]
Nov 25 15:56:34 2016 SYSLOG[0]: [Host 192.168.0.1] UDP 192.168.0.11,49154 --> 10.204.96.40,161 ALLOW: Outbound access request
Nov 25 15:56:34 2016 SYSLOG[0]: [Host 192.168.0.1] UDP 192.168.0.11,49154 --> 10.37.101.22,161 ALLOW: Outbound access request
Nov 25 15:56:34 2016 SYSLOG[0]: [Host 192.168.0.1] UDP 192.168.0.11,49154 --> 10.37.101.26,161 ALLOW: Outbound access request
Nov 25 15:56:34 2016 SYSLOG[0]: [Host 192.168.0.1] UDP 192.168.0.11,49154 --> 10.38.100.27,161 ALLOW: Outbound access request
Nov 25 15:56:34 2016 SYSLOG[0]: [Host 192.168.0.1] UDP 192.168.0.11,49154 --> 10.43.101.197,161 ALLOW: Outbound access request
Nov 25 15:56:44 2016 SYSLOG[0]: [Host 192.168.0.1] UDP 192.168.0.11,49154 --> 10.204.96.40,161 ALLOW: Outbound access request
Nov 25 15:56:44 2016 SYSLOG[0]: [Host 192.168.0.1] UDP 192.168.0.11,49154 --> 10.37.101.22,161 ALLOW: Outbound access request
Nov 25 15:56:44 2016 SYSLOG[0]: [Host 192.168.0.1] UDP 192.168.0.11,49154 --> 10.37.101.26,161 ALLOW: Outbound access request
Nov 25 15:56:44 2016 SYSLOG[0]: [Host 192.168.0.1] UDP 192.168.0.11,49154 --> 10.38.100.27,161 ALLOW: Outbound access request
Nov 25 15:56:44 2016 SYSLOG[0]: [Host 192.168.0.1] UDP 192.168.0.11,49154 --> 10.43.101.197,161 ALLOW: Outbound access request
Nov 25 15:57:01 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 177.71.63.253,40802 --> 178.233.170.175,23 DENY: Firewall interface access request
Nov 25 15:57:22 2016 SYSLOG[0]: [Host 192.168.0.1] UDP 192.168.0.15,31278 --> 178.233.140.110,53 ALLOW: Outbound access request [DNS query for ww.w.netmaster.com.tr.]
Nov 25 15:57:22 2016 SYSLOG[0]: [Host 192.168.0.1] UDP 192.168.0.15,31278 --> 176.240.150.250,53 ALLOW: Outbound access request [DNS query for ww.w.netmaster.com.tr.]
Nov 25 15:57:22 2016 SYSLOG[0]: [Host 192.168.0.1] UDP 192.168.0.15,31278 --> 46.197.15.60,53 ALLOW: Outbound access request [DNS query for www.netmaster.com.tr.]
Nov 25 15:57:23 2016 SYSLOG[0]: [Host 192.168.0.1] ICMP (type 3) 192.168.0.15 --> 178.233.140.110 ALLOW: Outbound access request
Nov 25 15:57:23 2016 SYSLOG[0]: [Host 192.168.0.1] ICMP (type 3) 192.168.0.15 --> 176.240.150.250 ALLOW: Outbound access request
Nov 25 15:57:23 2016 SYSLOG[0]: [Host 192.168.0.1] UDP 192.168.0.11,49154 --> 10.204.96.40,161 ALLOW: Outbound access request
Nov 25 15:57:23 2016 SYSLOG[0]: [Host 192.168.0.1] UDP 192.168.0.11,49154 --> 10.37.101.22,161 ALLOW: Outbound access request
Nov 25 15:57:23 2016 SYSLOG[0]: [Host 192.168.0.1] UDP 192.168.0.11,49154 --> 10.37.101.26,161 ALLOW: Outbound access request
Nov 25 15:57:23 2016 SYSLOG[0]: [Host 192.168.0.1] UDP 192.168.0.11,49154 --> 10.38.100.27,161 ALLOW: Outbound access request
Nov 25 15:57:23 2016 SYSLOG[0]: [Host 192.168.0.1] UDP 192.168.0.11,49154 --> 10.43.101.197,161 ALLOW: Outbound access request
Nov 25 15:57:32 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.13,38954 --> 183.61.49.155,8080 DENY: Inbound or outbound access request
Nov 25 15:57:32 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.13,39533 --> 203.205.151.193,8080 DENY: Inbound or outbound access request
Nov 25 15:57:33 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.13,39533 --> 203.205.151.193,8080 DENY: Inbound or outbound access request
Nov 25 15:57:34 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.13,38954 --> 183.61.49.155,8080 DENY: Inbound or outbound access request
Nov 25 15:57:34 2016 SYSLOG[0]: [Host 192.168.0.1] UDP 192.168.0.11,49154 --> 10.204.96.40,161 ALLOW: Outbound access request
Nov 25 15:57:34 2016 SYSLOG[0]: [Host 192.168.0.1] UDP 192.168.0.11,49154 --> 10.37.101.22,161 ALLOW: Outbound access request
```

Log kayıtlarına göre firewall yazılımının paket geçişine izin verdiği ve vermediği durumların ekrana düştüğü görülmektedir. (ALLOW, DENIED).

Sonuç olarak router makinasındaki firewall kendinde tanımlı kurallara göre iç ağ ve dış ağ arasındaki her paketin geçişine müdahil olmaktadır (DROP, ALLOW, DENIED) ve bu müdahalelerinin hepsini log'lamaktadır. Biz bu yazıda yaptığımız işlem ile router makinasının ürettiği log kayıtlarını iç ağdaki log sunucusuna (sistemimize) yönlendirmiş olduk. Böylece sistemimizden router makinasında dönen olayları izleyebilir hale gelmiş olduk.

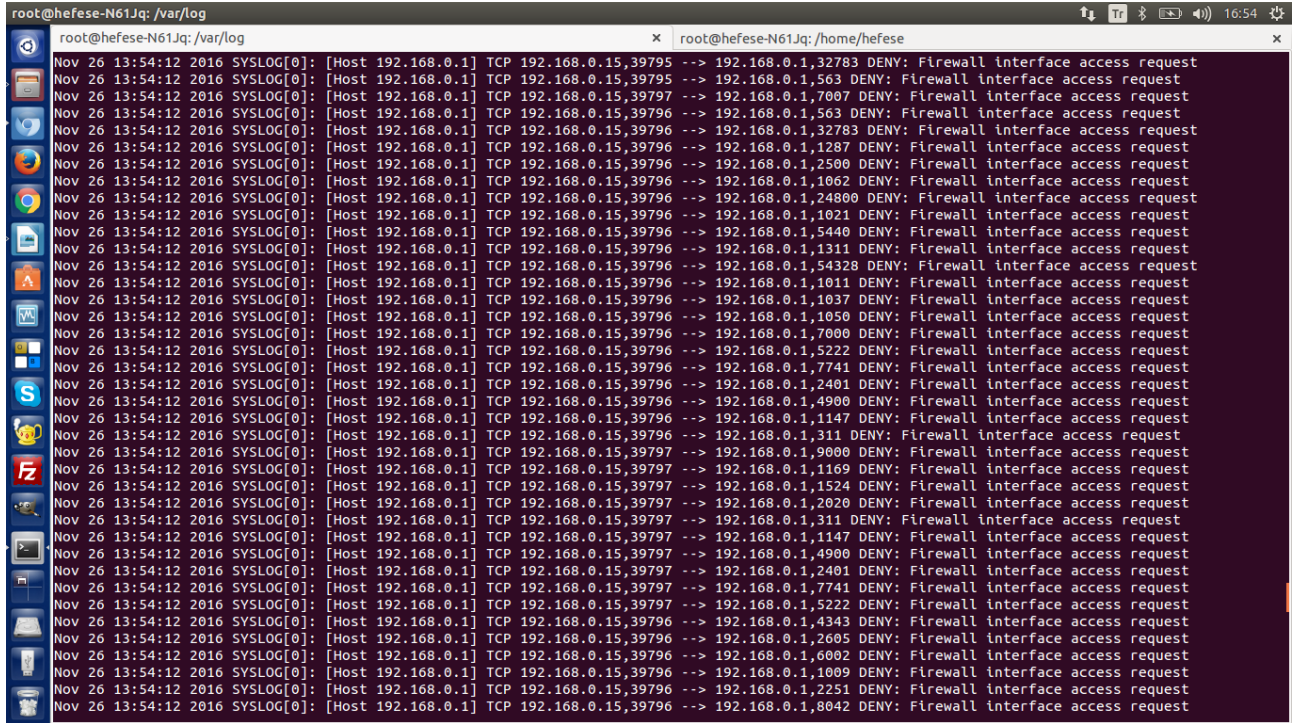
NOT: Router makinası paket gelip geçtikçe sürekli log üreteceğinden sistemimizdeki (log sunucumuzdaki) log dosyası sürekli güncellenecektir. Gelen her yeni log kaydı log dosyasına append olacaktır. Dolayısıyla tail tool'unun -f parametresi ile sürekli güncellenen log dosyasının güncel bir şekilde ekrana basılmasını sağlamış olduk. Yani -f parametresi ile log dosyasına eklenen her yeni kayıt anlık olarak ekrana verilebilmektedir.

## Firewall Log'larını Analiz Etme

Kendi bilgisayarımın nmap ile router'ımı aşağıdaki gibi port taramasına tabi tuttuğumda

```
> nmap -sS 192.168.0.1
```

log dosyasına şöyle kayıtlar düşüvermiştir:



```
root@hefese-N61Jq: /var/log
root@hefese-N61Jq: /home/hefese
Nov 26 13:54:12 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.15,39795 --> 192.168.0.1,32783 DENY: Firewall interface access request
Nov 26 13:54:12 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.15,39795 --> 192.168.0.1,563 DENY: Firewall interface access request
Nov 26 13:54:12 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.15,39797 --> 192.168.0.1,7007 DENY: Firewall interface access request
Nov 26 13:54:12 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.15,39796 --> 192.168.0.1,563 DENY: Firewall interface access request
Nov 26 13:54:12 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.15,39796 --> 192.168.0.1,32783 DENY: Firewall interface access request
Nov 26 13:54:12 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.15,39796 --> 192.168.0.1,1287 DENY: Firewall interface access request
Nov 26 13:54:12 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.15,39796 --> 192.168.0.1,2500 DENY: Firewall interface access request
Nov 26 13:54:12 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.15,39796 --> 192.168.0.1,1062 DENY: Firewall interface access request
Nov 26 13:54:12 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.15,39796 --> 192.168.0.1,24800 DENY: Firewall interface access request
Nov 26 13:54:12 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.15,39796 --> 192.168.0.1,1021 DENY: Firewall interface access request
Nov 26 13:54:12 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.15,39796 --> 192.168.0.1,5440 DENY: Firewall interface access request
Nov 26 13:54:12 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.15,39796 --> 192.168.0.1,1311 DENY: Firewall interface access request
Nov 26 13:54:12 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.15,39796 --> 192.168.0.1,54328 DENY: Firewall interface access request
Nov 26 13:54:12 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.15,39796 --> 192.168.0.1,1011 DENY: Firewall interface access request
Nov 26 13:54:12 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.15,39796 --> 192.168.0.1,1037 DENY: Firewall interface access request
Nov 26 13:54:12 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.15,39796 --> 192.168.0.1,1050 DENY: Firewall interface access request
Nov 26 13:54:12 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.15,39796 --> 192.168.0.1,7000 DENY: Firewall interface access request
Nov 26 13:54:12 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.15,39796 --> 192.168.0.1,5222 DENY: Firewall interface access request
Nov 26 13:54:12 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.15,39796 --> 192.168.0.1,7741 DENY: Firewall interface access request
Nov 26 13:54:12 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.15,39796 --> 192.168.0.1,2401 DENY: Firewall interface access request
Nov 26 13:54:12 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.15,39796 --> 192.168.0.1,4900 DENY: Firewall interface access request
Nov 26 13:54:12 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.15,39796 --> 192.168.0.1,1147 DENY: Firewall interface access request
Nov 26 13:54:12 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.15,39796 --> 192.168.0.1,311 DENY: Firewall interface access request
Nov 26 13:54:12 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.15,39797 --> 192.168.0.1,9000 DENY: Firewall interface access request
Nov 26 13:54:12 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.15,39797 --> 192.168.0.1,1169 DENY: Firewall interface access request
Nov 26 13:54:12 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.15,39797 --> 192.168.0.1,1524 DENY: Firewall interface access request
Nov 26 13:54:12 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.15,39797 --> 192.168.0.1,2020 DENY: Firewall interface access request
Nov 26 13:54:12 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.15,39797 --> 192.168.0.1,311 DENY: Firewall interface access request
Nov 26 13:54:12 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.15,39797 --> 192.168.0.1,1147 DENY: Firewall interface access request
Nov 26 13:54:12 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.15,39797 --> 192.168.0.1,4900 DENY: Firewall interface access request
Nov 26 13:54:12 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.15,39797 --> 192.168.0.1,2401 DENY: Firewall interface access request
Nov 26 13:54:12 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.15,39797 --> 192.168.0.1,7741 DENY: Firewall interface access request
Nov 26 13:54:12 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.15,39797 --> 192.168.0.1,5222 DENY: Firewall interface access request
Nov 26 13:54:12 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.15,39796 --> 192.168.0.1,4343 DENY: Firewall interface access request
Nov 26 13:54:12 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.15,39796 --> 192.168.0.1,2605 DENY: Firewall interface access request
Nov 26 13:54:12 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.15,39796 --> 192.168.0.1,6002 DENY: Firewall interface access request
Nov 26 13:54:12 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.15,39796 --> 192.168.0.1,1009 DENY: Firewall interface access request
Nov 26 13:54:12 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.15,39796 --> 192.168.0.1,2251 DENY: Firewall interface access request
Nov 26 13:54:12 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.15,39796 --> 192.168.0.1,8042 DENY: Firewall interface access request
```

192.168.0.15

// Benim bilgisayarımın IP Adresi

192.168.0.1

// Router'ın IP Adresi

Kayıtlardan görülebileceği üzere 192.168.0.15 adresinden 192.168.0.1 adresine paketler gitmektedir ve bu paketler router'a vardığında DENY edilmektedir. Bilgisayarımın router'a yapılan nmap port tarama işlemi bitene kadar bu tür log kayıtları firewall'dan gelmeye devam etmiştir ve bilgisayarımın nmap port taraması bittiği an firewall'dan bu kayıtların gelişi de bitmiştir. Dolayısıyla diyebiliriz ki nmap port tarama paketleri firewall log'larında "Firewall interface access request" olarak işaretlenmektedir. Bu bilgiden hareketle firewall log'larına bakmaya devam ettiğimizde port tarama paketlerinin dışarıdan da geldiği görülmüştür:



```
root@hefese-N61Jq: /var/log
root@hefese-N61Jq: /var/log
hefese@hefese-N61Jq: ~
Nov 25 20:53:46 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.26,54934 --> 37.157.2.26,443 DENY: Inbound or outbound access request
Nov 25 20:53:47 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.13,38223 --> 172.217.23.238,443 DENY: Inbound or outbound access request
Nov 25 20:53:48 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.13,60790 --> 64.233.166.188,5228 DENY: Inbound or outbound access request
Nov 25 20:53:48 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.26,54936 --> 37.252.172.39,443 DENY: Inbound or outbound access request
Nov 25 20:53:48 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.26,54934 --> 37.157.2.26,443 DENY: Inbound or outbound access request
Nov 25 20:53:48 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.26,54937 --> 37.157.2.26,443 ALLOW: Outbound access request
Nov 25 20:53:48 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.26,54934 --> 37.157.2.26,443 DENY: Inbound or outbound access request
Nov 25 20:53:48 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.26,54936 --> 37.252.172.39,443 DENY: Inbound or outbound access request
Nov 25 20:53:49 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.26,54934 --> 37.157.2.26,443 DENY: Inbound or outbound access request
Nov 25 20:53:49 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.26,54936 --> 37.252.172.39,443 DENY: Inbound or outbound access request
Nov 25 20:53:49 2016 SYSLOG[0]: [Host 192.168.0.1] UDP 192.168.0.11,49154 --> 10.204.96.40,161 ALLOW: Outbound access request
Nov 25 20:53:49 2016 SYSLOG[0]: [Host 192.168.0.1] UDP 192.168.0.11,49154 --> 10.37.101.22,161 ALLOW: Outbound access request
Nov 25 20:53:49 2016 SYSLOG[0]: [Host 192.168.0.1] UDP 192.168.0.11,49154 --> 10.37.101.26,161 ALLOW: Outbound access request
Nov 25 20:53:49 2016 SYSLOG[0]: [Host 192.168.0.1] UDP 192.168.0.11,49154 --> 10.38.100.27,161 ALLOW: Outbound access request
Nov 25 20:53:49 2016 SYSLOG[0]: [Host 192.168.0.1] UDP 192.168.0.11,49154 --> 10.43.101.197,161 ALLOW: Outbound access request
Nov 25 20:53:50 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.26,54934 --> 37.157.2.26,443 DENY: Inbound or outbound access request
Nov 25 20:53:50 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.26,54936 --> 37.252.172.39,443 DENY: Inbound or outbound access request
Nov 25 20:53:52 2016 SYSLOG[0]: [Host 192.168.0.1] UDP 192.168.0.26,50428 --> 8.8.8.8,53 ALLOW: Outbound access request [DNS query for pagead2.googleSyndication.com.]
Nov 25 20:53:52 2016 SYSLOG[0]: [Host 192.168.0.1] UDP 192.168.0.26,50429 --> 216.58.208.98,443 ALLOW: Outbound access request
Nov 25 20:53:52 2016 SYSLOG[0]: [Host 192.168.0.1] UDP 84.43.212.99,64148 --> 178.233.170.175,18211 DENY: Firewall interface access request
Nov 25 20:53:52 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.26,54934 --> 37.157.2.26,443 DENY: Inbound or outbound access request
Nov 25 20:53:52 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.26,54936 --> 37.252.172.39,443 DENY: Inbound or outbound access request
Nov 25 20:53:52 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.12,52829 --> 107.21.18.47,443 ALLOW: Outbound access request
Nov 25 20:53:54 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 111.121.193.195,58504 --> 178.233.170.175,2433 DENY: Firewall interface access request
Nov 25 20:53:57 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.26,54934 --> 37.157.2.26,443 DENY: Inbound or outbound access request
Nov 25 20:53:57 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.26,54936 --> 37.252.172.39,443 DENY: Inbound or outbound access request
Nov 25 20:53:59 2016 SYSLOG[0]: [Host 192.168.0.1] UDP 192.168.0.11,49154 --> 10.204.96.40,161 ALLOW: Outbound access request
Nov 25 20:53:59 2016 SYSLOG[0]: [Host 192.168.0.1] UDP 192.168.0.11,49154 --> 10.37.101.22,161 ALLOW: Outbound access request
Nov 25 20:53:59 2016 SYSLOG[0]: [Host 192.168.0.1] UDP 192.168.0.11,49154 --> 10.37.101.26,161 ALLOW: Outbound access request
Nov 25 20:53:59 2016 SYSLOG[0]: [Host 192.168.0.1] UDP 192.168.0.11,49154 --> 10.38.100.27,161 ALLOW: Outbound access request
Nov 25 20:53:59 2016 SYSLOG[0]: [Host 192.168.0.1] UDP 192.168.0.11,49154 --> 10.43.101.197,161 ALLOW: Outbound access request
Nov 25 20:54:01 2016 SYSLOG[0]: [Host 192.168.0.1] TCP 192.168.0.12,52830 --> 151.101.36.84,443 ALLOW: Outbound access request
Nov 25 20:54:01 2016 SYSLOG[0]: [Host 192.168.0.1] UDP 192.168.0.11,137 --> 192.168.0.255,137 ALLOW: Inbound access request
Nov 25 20:54:01 2016 SYSLOG[0]: message repeated 2 times: [ [Host 192.168.0.1] UDP 192.168.0.11,137 --> 192.168.0.255,137 ALLOW: Inbound access request ]
Nov 25 20:54:02 2016 SYSLOG[0]: [Host 192.168.0.1] UDP 192.168.0.26,63782 --> 8.8.8.8,53 ALLOW: Outbound access request [DNS query for 1.0.168.192.in-addr.arpa.]
Nov 25 20:54:02 2016 SYSLOG[0]: [Host 192.168.0.1] UDP 192.168.0.26,137 --> 192.168.0.1,137 DENY: Firewall interface access request
```

Yeşil renkli log kayıtlarına bakalım.

... 84.43.212.99,64148 --> 178.233.170.175,18211 DENY: Firewall interface access request

... 111.121.193.195,58504 --> 178.233.170.175,2433 DENY: Firewall interface access request

Paketin geldiği adreslere bakacak olursak paketin yabancı adreslerden geldiği görülmektedir. 178.233.170.175 adresi ise benim public IP'mdir. Çünkü What is My IP Address siteleri bu adresin benim public IP'im olduğunu söylemektedir. Bu log kayıtlarının açıklamaları ise "Firewall interface access request" şeklindedir. Demek ki dışarıdan router'ıma port tarama paketleri gelmiş. Yani birisi dışarıdan benim router'ımı taramış. Saldırgan bu tür port tarama işlemlerini nmap aracı ile belli bir IP aralığını tarayarak yapabilir. Yani illa beni tek hedef seçmiş olması gerekmez. Taranan IP aralığına denk geliyorsa ben de taranmış olurum. O yüzden saldırı belli bir IP aralığını tararken benim router'ımın IP'si de denk geldiği için firewall log'larına yukarıdaki gibi saldırı paketleri düşmüştür.

NOT: Aşağıda tüm interneti tarayan nmap kullanımını görmekteyiz.

```
> nmap -sS 0-255.0-255.0-255.0-255
```

Ancak bu bitmek bilmeyen bir tarama olacağından daha efektif ve hızlı sonuç almak için spesifik bir IP bloğu taranabilir. Örneğin;

```
> nmap -sS 178.1-255.0/16
```

Yukarıdaki tarama ile 178.x.0.0/16 network'ündeki her makina taranacaktır. x değıştiğçe network adresi de değışeceğinden birçok network taranacaktır. Bu tarama sonucunda benim router'ım da tarananlar arasında yer alacaktır. Çünkü IP adresim 178.233.170.175. Böylece saldırı hiç tanımadığı makinaları nmap ile tarayarak zafiyet arayabilecektir.

Böylece log takibi ile dışarıdan gelen bir saldırıyı tespit etmiş olduk. Saldırı kaydının oluştuğu tarihe bakarak saldırının gerçekleştiği zamanı öğrenebiliriz. Bu tip saldırıları tespit etmek için illaki ekranda akan log kayıtlarına sürekli bakmamız gerekmez. log dosyasını belli aralıklarla grep ile işleme sokarak da saldırı mahiyetinde kayıt olup olmadığını anlayabiliriz. Böylece saldırıya maruz kaldık mı kalmadık mı sorusuna cevap bulabiliriz.

### **Firewall Hakkında**

Firewall donanım olabileceği gibi işletim sistemlerimizde yüklü yazılım da olabilir. Her ikisi de aynı işi yapar. Yani paketlerin geçişini kontrol eder. Paketlerin geçip geçmeyeceği kararlarını alır ve her paket için aldığı kararı raporlar (log'lar).

Firewall donanımı da yazılımı da kurallara sahiptir ve o kurallara göre paketlerin geçişine dair kararlar alırlar. Firewall'a kendi kuralımızı ekleyebilmekteyiz.

### Yararlanılan Kaynaklar

[https://community.spiceworks.com/how\\_to/65683-configure-ubuntu-server-12-04-lts-as-a-syslog-server](https://community.spiceworks.com/how_to/65683-configure-ubuntu-server-12-04-lts-as-a-syslog-server)

<http://superuser.com/questions/803996/no-kernel-messages-are-logged-to-kern-log>

<http://serverfault.com/questions/176747/how-to-restart-rsyslog-daemon-on-ubuntu>