

SYSLOG SERVER KURULUMU

Ubuntu Web Sitesinden,
Virtualbox üzerine
kurulum yapmak için .iso
dosyası indirilerek
kurulum gerçekleştirilir.

WAN tarafında, pfsense
ile aynı subnette olması
ve SSH Server'ı
yüklenmesine dikkat edilir.

```
apt-get install syslogd
apt-get install syslog-ng
cp /etc/syslog.conf /etc/syslog.conf.backup
/etc/default/syslogd >> SYSLOGD="-r"
/etc/init.d/syslogd restart
pico /etc/syslog-ng/syslog-ng.conf
---
source s_net { udp(ip(0.0.0.0) port(514)); };
destination d_net { file("/var/log/22902.log"); };
log { source(s_net); destination(d_net); };
---
/etc/init.d/syslog-ng restart
```

Diagnostics: System logs: Settings

System	Firewall	DHCP	Portal Auth	IPsec VPN	PPTP VPN	Load Balancer	OpenVPN	OpenNTPD	Settings
--------	----------	------	-------------	-----------	----------	---------------	---------	----------	-----------------

Show log entries in reverse order (newest entries on top)

Number of log entries to show:

Log packets blocked by the default rule
Hint: packets that are blocked by the implicit default block rule will not be logged anymore if you uncheck this option. Per-rule logging options are not affected.

Show raw filter logs
Hint: If this is checked, filter logs are shown as generated by the packet filter, without any formatting. This will reveal more detailed information.

Enable syslog'ing to remote syslog server

Disable writing log files to the local ram disk

Remote syslog server	<input type="text" value="192.168.1.7"/> IP address of remote syslog server
	<input type="checkbox"/> system events
	<input type="checkbox"/> firewall events
	<input type="checkbox"/> DHCP service events
	<input type="checkbox"/> Portal Auth
	<input type="checkbox"/> VPN events
	<input checked="" type="checkbox"/> Everything

Note:
syslog sends UDP datagrams to port 514 on the specified remote syslog server. Be sure to set syslogd on the remote server to accept syslog messages from pfSense.

Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
Interface	WAN ▾ Choose on which interface packets must come in to match this rule.
Protocol	UDP ▾ Choose which IP protocol this rule should match. Hint: in most cases, you should specify <i>TCP</i> here.
Source	<input type="checkbox"/> not Use this option to invert the sense of the match. Type: Single host or alias ▾ Address: 192.168.1.7 / 31 ▾ Advanced - Show source port range
Source OS	OS Type: any ▾ Note: this only works for TCP rules
Destination	<input type="checkbox"/> not Use this option to invert the sense of the match. Type: WAN address ▾ Address: [redacted] / 31 ▾
Destination port range	from: (other) ▾ 514 to: (other) ▾ 514 Specify the port or port range for the destination of the packet for this rule. Hint: you can leave the 'to' field empty if you only want to filter a single port

Sunucudan tail -f /var/log/22902.log ile gelen bilgiler kontrol edilir.
Pfsense'dan istenilen Kurallar seçilerek loglanabilir.

İstenilen verileri grep ile düzenli olarak ayıklayabilirsiniz.
(bash script ve crontab kullanabilirsiniz)

```
cat /var/log/syslog_coder/r229syslog.log | grep "79.123.229.42 pf:" > hedefdosya
```

Log dosyasının şişmemesi için (log rotation)

```
find /var/log/sys -type f -name *.log -mtime +150 -print | xargs rm
```

MRTG Kurulumu

Services: SNMP



The changes have been applied successfully. You can also [monitor](#) the filter reload progress.

SNMP Daemon

Enable

Polling Port	<input type="text" value="161"/> Enter the port to accept polling events on (default 161)
System location	<input type="text"/>
System contact	<input type="text"/>
Read Community String	<input type="text" value="public"/> In most cases, "public" is used here

SNMP Traps

Enable

Trap server	<input type="text"/> Enter trap server name
Trap server port	<input type="text" value="162"/> Enter the port to send the traps to (default 162)
Enter the SNMP trap string	<input type="text"/> Trap string

Modules

SNMP Modules	<input checked="" type="checkbox"/> MibII <input checked="" type="checkbox"/> Netgraph <input checked="" type="checkbox"/> PF <input checked="" type="checkbox"/> Host Resources
---------------------	---

Action	Pass ▼ Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded. Reject only works when the protocol is set to either TCP or UDP (but not "TCP/UDP") below.
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
Interface	WAN ▼ Choose on which interface packets must come in to match this rule.
Protocol	UDP ▼ Choose which IP protocol this rule should match. Hint: in most cases, you should specify <i>TCP</i> here.
Source	<input type="checkbox"/> not Use this option to invert the sense of the match. Type: Single host or alias ▼ Address: 192.168.1.7 / 31 ▼ <input type="button" value="Advanced"/> - Show source port range
Source OS	OS Type: any ▼ Note: this only works for TCP rules
Destination	<input type="checkbox"/> not Use this option to invert the sense of the match. Type: WAN address ▼ Address: [redacted] / 31 ▼
Destination port range	from: (other) ▼ [redacted] to: (other) ▼ [redacted]

MRTG Server temel kurulum ;

```
apt-get update  
apt-get install build-essential  
apt-get install apache2  
apt-get install snmp  
apt-get install mrtg
```

MRTG Server temel kurulum ;

```
apt-get update  
apt-get install build-essential  
apt-get install apache2  
apt-get install snmp  
apt-get install mrtg
```

```
snmpwalk -v 2c -c public 192.168.1.15
```

public > community string

Config Dosyası Oluşturalım;

önce /var/www/mrtg dizinini oluşturun.
Konfigürasyon dosyasını oluşturmak için komutu girin;

```
/usr/bin/cfgmaker --global "Options[_]:growright,bits"  
--global "WorkDir: /var/www/mrtg" public@192.168.1.15  
> /usr/local/etc/mrtg.conf
```

Index Dosyası Oluşturalım;

önce `/var/www/mrtg` dizinini oluşturun.
Konfigürasyon dosyasını oluşturmak için komutu girin;

```
/usr/bin/indexmaker --title "Pfsense Test"  
/usr/local/etc/mrtg.conf --output /var/www/mrtg/index.html
```

Index Dosyası Oluşturalım;

önce /var/www/mrtg dizinini oluşturun.
Konfigürasyon dosyasını oluşturmak için komutu girin;

```
/usr/bin/indexmaker --title "Pfsense Test"  
/usr/local/etc/mrtg.conf --output /var/www/mrtg/index.html
```

Çalıştıralım; (Birkaç kere tekrarlayarak hata almayana kadar devam edin.)

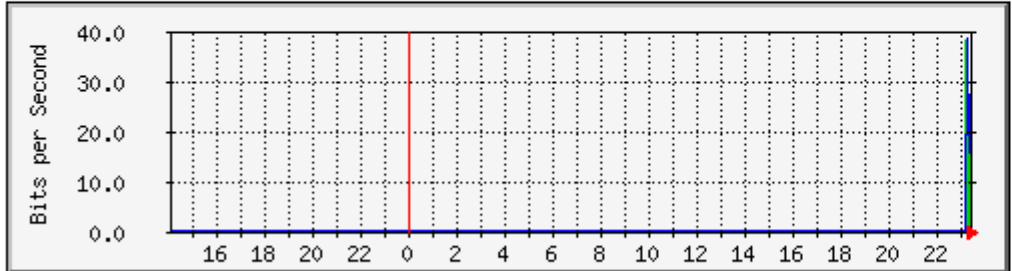
```
env LANG=C /usr/bin/mrtg /usr/local/etc/mrtg.conf
```

Son olarak crontab'a gir;

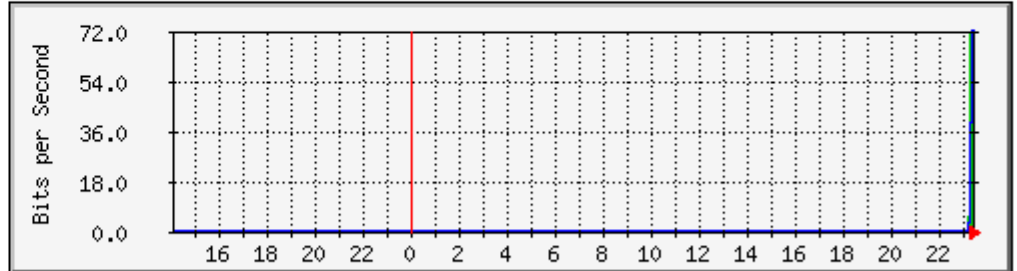
```
5,10,15,20,25,30,35,40,45,50,55 * * * * env LANG=C  
/usr/bin/mrtg /usr/local/etc/mrtg.conf
```

Pfsense Test

Traffic Analysis for em0 – pfSense.local



Traffic Analysis for em1 – pfSense.local



MRTG MULTI ROUTER TRAFFIC GRAPHER
version 2.16.3
[Tobias Oetiker <tobi@oetiker.ch>](mailto:tobi@oetiker.ch)
and [Dave Rand <dlr@bungj.com>](mailto:dlr@bungj.com)



nazim@sinop.edu.tr
inosci@gmail.com

Teşekkürler....