

# Beveiligingstool onder de loep

# m0n0wall

**In het kader van security mag de firewall niet ontbreken. In dit artikel bekijkt Adri Mathlener de statefull software firewall m0n0wall. Dit is een open source firewall die is gebaseerd op FreeBSD.**

We onderscheiden drie firewall types:

- Packet filter: aan de hand van een set regels, die je zelf opstelt, wordt er uitsluitend gekeken naar de ip-header van ieder afzonderlijk ip-pakketje en aan de hand daarvan wordt het ip-pakketje doorgelaten of tegengehouden. Je kunt hiermee prima ip-adressen blokkeren en poorten voor de buitenwereld afsluiten.
- Statefull: werkt ook op basis van ip-headers, met dit verschil dat er nu wordt gekeken of het ip-pakketje de start van een nieuwe connectie is, of deel uit maakt van een reeds gemaakte connectie of ongeldig is.
- Application layer: dit type firewall kijkt naar de application layer van een ip-pakketje. Het is in staat te 'snappen' wat bepaalde applicaties en protocollen (zoals FTP, DNS web browsing) doen en kan daar dan gepaste acties op loslaten. Dit wordt gerealiseerd middels een proxy.

Zoals gezegd, m0n0wall [1] is van het Statefull-type. Je kunt m0n0wall draaien op een pc, maar ook op een ALIX board [2] of een net45xx board [3]. Het voordeel van de laatste twee is dat het stroomverbruik van dit soort devices over het algemeen zeer laag is. Ook laat m0n0wall zich prima virtualiseren met de bekende tools, zoals VMware en VirtualBox.

De functionaliteit die m0n0wall biedt is uitgebreid, waarvan dit wel de kenmerkendste zijn: webinterface, wireless support, captive portal, 802.1Q VLAN support, statefull packet filtering, logging, NAT, DHCP client & server, Ipsec VPN tunnels, static routes, caching DNS forwarder, DynDNS client, SNMP client en traffic shaper.

Installatie is simpel; download de iso [1] van nog geen 6 Mb en bak hier een cd van. Na het booten kom je terecht in de console setup.

```
--- This is m0n0wall, version 1.235
built on Thu Sep 4 21:49:51 CEST 2008 for generic-pc-odrom
Copyright (C) 2002-2008 by Manuel Kasper. All rights reserved.
Visit http://m0n0.ch/wall for updates.

LAN IP address: 192.168.1.1

Port configuration:
LAN -> eth0
WAN -> eth1

m0n0wall console setup
=====
1) Interfaces: assign network ports
2) Set up LAN IP address
3) Reset webGUI password
4) Reset to factory defaults
5) Reboot system
6) Ping host
Enter a number: █
```

Als eerste configureer je nu de nic's voor de LAN en WAN connectie. Zorg dat je een diskette in de drive hebt zitten, want daar wordt de configuratie op weggeschreven. Voor VirtualBox heb ik hier [4] een virtual floppy disk gevonden. Daarna reboot m0n0wall zichzelf. De volgende stap is het toewijzen van een ip-adres. Als je m0n0wall in gaat zetten, vergeet dan niet om het admin wachtwoord aan te passen. Voer in je browser dit adres in als url en je kunt dan inloggen met user

admin met wachtwoord mono. Onderstaande gui wordt vervolgens gepresenteerd:



In General Setup stel je de tijdzone in en laat de webGUI via https werken. We willen tenslotte secure werken daar waar het kan nietwaar. Dan is nu de weg vrij om de gewenste firewall regels in te voeren en je firewall is klaar voor gebruik. Dat je met Captive Portal leuke dingen kunt doen, laat Danne [5] ons zien. Op de site van m0n0wall is uitgebreide documentatie te vinden en daarnaast ook de nodige screencasts. De onderliggende firewall van m0n0wall is ipfw en via <http://<m0n0wall-ip>/status.php> is die te bekijken.

[1] <http://m0n0.ch/wall>

[2] [www.pcengines.ch/](http://www.pcengines.ch/)

[3] [www.soekris.com/](http://www.soekris.com/)

[4] [www.allbootdisks.com/download/dos.html](http://www.allbootdisks.com/download/dos.html)

[5] [www.djesigns.com/archives/400](http://www.djesigns.com/archives/400)