







## Basic Network Security with m0n0wall in the SMB –By Phil Vogler NCS Idaho





Here are some of the basic firewall rules I use when deploying a m0n0wall in a small business ( 5 to 50 users)



Basic LAN security, these rules stop spam bots and DNS Hijack. These must be applied to the Wireless interface as well. In source check mark the “not” option and enter the IP of your internal Mail and DNS server. The internal DNS server should have Open DNS in in the forwarders

### Firewall: Rules







LAN WAN WIRELESS







	Proto	Source	Port	Destination	Port	Description	
<input type="checkbox"/> <input checked="" type="checkbox"/>	TCP	! 192.168.:	*	*	25 (SMTP)	SMTP LAN Block	 
<input type="checkbox"/> <input checked="" type="checkbox"/>	UDP	! 192.168.	*	*	53 (DNS)	DNS HiJack LAN Block	 
<input type="checkbox"/> <input checked="" type="checkbox"/>	*	LAN net	*	*	*	Default Lan -> any	 


   
 

 Internal Mail Server IP  
 Internal DNS Server

Home use, no internal servers, m0n0wall must be set as the DNS server with Open DNS as the forward

	Proto	Source	Port	Destination	Port	Description	
<input type="checkbox"/> <input checked="" type="checkbox"/>	TCP	*	*	*	25 (SMTP)	SMTP Lan Block	 
<input type="checkbox"/> <input checked="" type="checkbox"/>	TCP/UDP	! 192.168.	*	*	53 (DNS)	DNS HiJack Block	 
<input type="checkbox"/> <input checked="" type="checkbox"/>	*	LAN net	*	*	*	Default Lan --> Any	 

 m0n0wall IP Address

Make sure to check the DNS re-bind option under the Wan settingsDo this as well at Open DNS

**Block private networks**  
When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). You should generally leave this option turned on, unless your WAN network lies in such a private address space, too.

---

Do this as well in your Open DNS Account

**Malware/Botnet Protection**  **Enable basic malware/botnet protection**  
When certain Internet-scale botnets are discovered or particularly malicious malware hits, we offer protection to all our users so that as many people as possible can be protected from the threat. At this time, this feature blocks the Conficker virus and the Internet Explorer Zero Day Exploit, and is continually expanded to include other types of malicious sites.

---

**Phishing Protection**  **Enable phishing protection**  
By enabling phishing protection, you'll protect everyone on your network from known phishing sites using the best data available.

---

**Suspicious Responses**  **Block internal IP addresses**  
When enabled, DNS responses containing IP addresses listed in [RFC1918](#) will be filtered out. This helps to prevent [DNS Rebinding attacks](#). For example, if `badstuff.attacker.com` points to `192.168.1.1`, this option would filter out that response.

Also check the Adware setting in the Open DNS filtering settings.

Add these to the blocked Domains in the filtering settings at in Open DNS

It is a short list but it is a start

adtechus.com

advertising.com

burstnet.com

[creative.ak.facebook.com](https://creative.ak.facebook.com)

[doubleclick.net](https://doubleclick.net)

[eyewonder.com](https://eyewonder.com)

[ifstmedia.com](https://ifstmedia.com)

[linksynergy.com](https://linksynergy.com)

[media6degrees.com](https://media6degrees.com)

[questionmarket.com](https://questionmarket.com)

[yieldmanager.com](https://yieldmanager.com)