# Adblocking NG

Michael Koerfer — 24.11.2017



## Overview

- Hardware
- Virtualization
- OS + Configuration
- Conclusion
- Credits



### Home

- Checkout out a Fujitsu Futro S550-2 Thin Client



- AMD Sempron 200U CPU
- 1 GB RAM
- $1 \times 1000 \text{ Mbit/s}$
- > 8 GB CF HDD \*extra
- 1 x USB Network 1000 Mbit/s \*extra
- Amazon \$40

### • S0H0

- Checkout out a PC Engines APU.1D Bundle



- AMD Embedded G-Series T40E APU
- 2 GB RAM
- 16 GB MicroSD HDD \*extra
- $3 \times 1000 \text{ MBit/s}$
- Amazon \$300

### Companies

- Checkout out a Netgate XG-1541 1U HA



- Intel Xeon-DE D-1541 8 Core
- 16 GB RAM
- 256GB m.2 SATA
- 2 x Intel 10GbE
- HA Professional 3 Years
- Netgate \$4168 + shipping



### VMWare or VirtualBox

- Pfsense
- > 1 CPU
- > 2 GB RAM
- > 10 GB VHD
- > 2 NIC's
- https://doc.pfsense.org/index.php/PfSense\_on\_VMware\_vSphere\_/\_ESXi
- http://samuraihacks.com/install-pfsense-in-virtualbox/
- Follow the next steps and enjoy

# OS + Configuration

### Installer ISO, Memstick or Memstick Serial?

- Optical disc image (ISO image, CD/DVD disc): Easy and familiar to many, if the target hardware has an optical drive it's a solid choice, especially if the BIOS will not boot from USB.

### • Memstick:

- Like the Memstick image, but runs using the serial console rather than VGA, for newer embedded systems.

### NanoBSD or NanoBSD+VGA

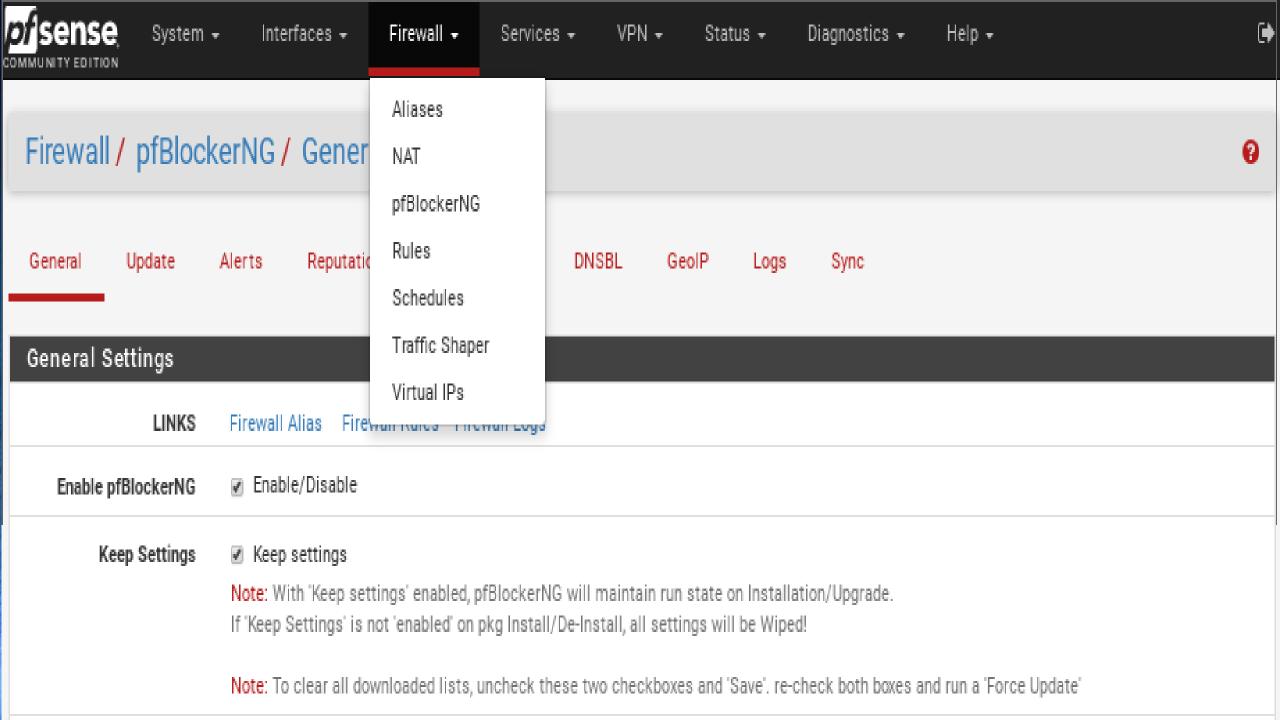
- IMPORTANT: NanoBSD will be deprecated with the pfSense 2.4-RELEASE! https://doc.pfsense.org/index.php/Installing\_pfSense

### DNSBL (DNS Blacklist)

- Login WebUI
- System -> Package Manager -> Available Packages
- pfBlockerNG (Manage IPv4/6 list sources into "Deny Permit or Match")

### After Install

- Firewall -> pfBlockerNG



### DNSBL Tab

- Enter the DNSBL VIP as 10.10.10.1
- Enter the DNSBL Listening Port as 8081
- Enter the DNSBL SSL Listening port as 8443
- Select the DNSBL Listening Interface as LAN

DNSBL Configuration	
LINKS	Firewall Alias Firewall Rules Firewall Logs
Info	<b>6</b>
Enable DNSBL	This will enable DNS Block List for Malicious and/or unwanted Adverts Domains To Utilize, <b>Unbound DNS Resolver</b> must be enabled.
Enable TLD	BETA This is an Advanced process to determine if all Sub-Domains should be blocked for each listed Domain.  Click infoblock before enabling this feature!
DNSBL Virtual IP	Example (10.10.10.1) Enter a single IPv4 VIP address that is RFC1918 Compliant.  This address should be in an Isolated Range than what is used in your Network. Rejected DNS Requests will be forwarded to this VIP (Virtual IP) RFC1918 Compliant - (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16)
DNSBL Listening Port	Example (8081) Enter a single PORT that is in the range of 1 - 65535 This Port must not be in use by any other process.
DNSBL SSL Listening Port	Example (8443) Enter a single PORT that is in the range of 1 - 65535 This Port must not be in use by any other process.
DNSBL Listening Interface	LAN  Select the interface you want DNSBL to Listen on.  Default: LAN - Selected Interface should be a Local Interface only.
DNSBL Firewall Rule	✓ LAN Å

- For the DNSBL Firewall Rule select all of the LAN subnets that access the DNS Resolver. Ensure als use only the DNS Resolver.

### DNSBL IP Firewall Rules

- Select Deny outbound or as per your requirements
- Select Enable logging
- Alexa (is optional, you can skip this until later if you wish)
- Select Top 1K
- Select the TLD Inclusions as ca,co,com,io,me,net,org or as required.
- In the Custom List you may enter any domain you wish to Whitelist.
- Save your settings

DNSBL IP Firewall Rule Settings				
	Configure settings for Firewall Rules when any DNSBL Feed contain IP Addresses			
List Action	Deny Outbound ▼			
	Default: Disabled 1			
Enable Logging	Enable ▼			
	Default: Enable			
	Select - Logging to Status: System Logs: FIREWALL ( Log ) This can be overriden by the 'Global Logging' Option in the General Tab.			
Advanced Inbound Fi	rewall Rule Settings	Ð		
Advanced Outbound I	Firewall Rule Settings	0		
Alexa Whitelist		0		
Alexa Wilitelist				
Custom Domain Whitelist		0		
TLD Exclusion List		0		
TLD Blacklist		0		
TLD Whitelist		0		

### DNSBL Feeds Tab

Create a new DNSBL AliasEnter DNS Group Name as ADsEnter Description as DNSBL ADverts

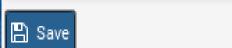
### Firewall / pfBlockerNG / DNSBL Feeds



General Update Alerts Reputation IPv4 IPv6 DNSBL GeoIP Logs Sync

DNSBL DNSBL Feeds DNSBL EasyList

DNS Group Name	DNS Group Description	Action	Frequency	
ADverts	DNSBL ADverts	unbound	EveryDay	<b>₽</b> 🗓
				+ Add



### DNSBL Feeds

- Enter the Header/Label and Source URL as follows (Use copy/paste as plain text), set format Auto and State ON
- yoyo

```
http://pgl.yoyo.org/adservers/serverlist.php?
hostformat=hosts&mimetype=plaintext
```

- hpHosts\_ads
http://hosts-file.net/ad\_servers.txt

- Adaway
https://adaway.org/hosts.txt

- Cameleon

http://sysctl.org/cameleon/hosts

- Select List Action as Unbound
- Select Update Frequency as Once a day

### Alexa

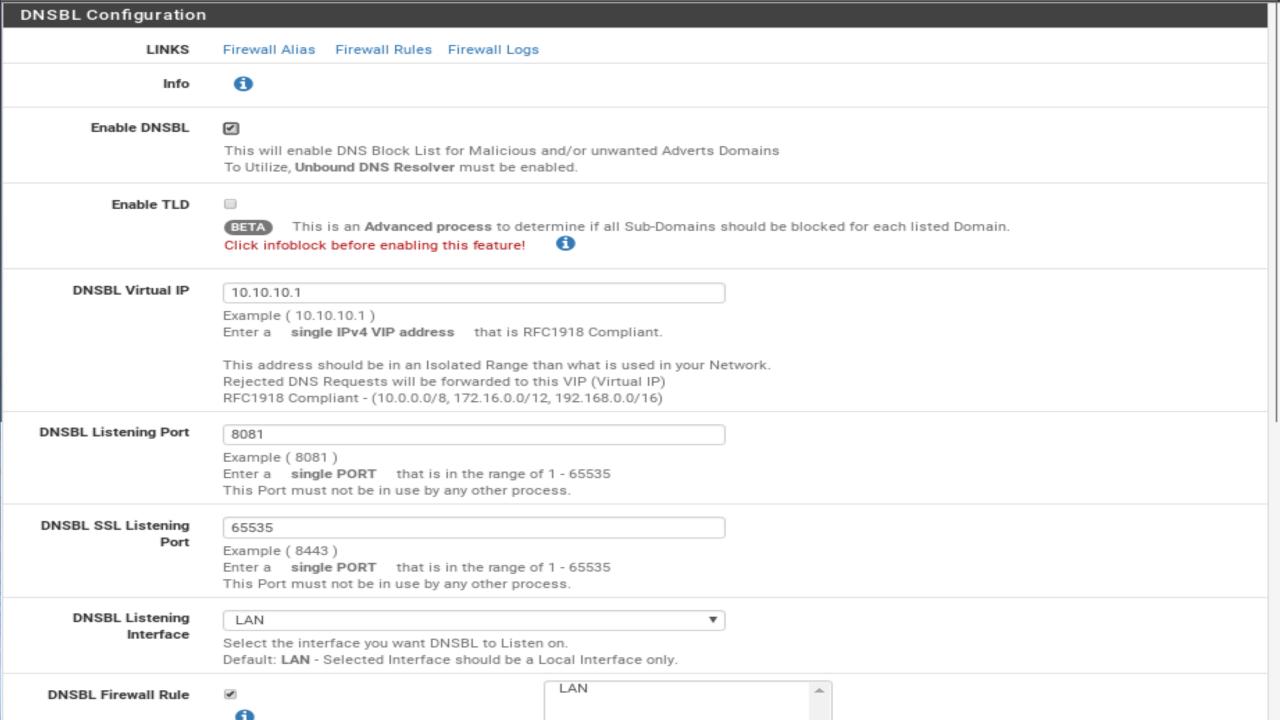
- Do not enable the Alexa Whitelist for this ADverts based alias, as Alexa also posts the top ADvert servers. So using Alexa whitelist, will interfere with ADvert Blocking.
- Add any other domains that you wish to block in the Custom List.

  Save your settings

DNSBL Feeds						
LINKS	Firewall Alias Firewall Rules Firewall Logs					
DNS GROUP Name	ADverts					
	Enter DNS Group Name. Example: Ads					
Description	DNSBL ADverts					
DNSBL Settings	•					
DNSBL	Auto ▼ ON ▼ http://pgl.yoyo.org/adservers/serverlist.php?hostformat=hosts&mimel	yoyo Delete				
	Auto ▼ ON ▼ http://hosts-file.net/ad_servers.txt	hpHosts_ads Delete				
	Auto ▼ ON ▼ https://adaway.org/hosts.txt	Adaway Delete				
	Auto ▼ ON ▼ http://sysctl.org/cameleon/hosts	Cameleon Till Delete				
	Format State Source	Header/Label				
Add	+ Add					
List Action	Unbound ▼					
	Default: Disabled Select Unbound to enable 'Domain Name' blocking for this Alias.					
Update Frequency	Once a day ▼					
	Default: Never Select how often List files will be downloaded. This must be within the Cron Interval/Start Hour settings.					
Weekly (Day of Week)	Monday ▼					
recitly (buy or recitly	Default: Monday					
	Select the 'Weekly' ( Day of the Week ) to Update					
	This is only required for the 'Weekly' Frequency Selection. The 24 Hour Download 'Time' will be used.					
Enable Alexa Whitelist	☐ Filter Alias via Alexa					

### DNSBL Tab

- Click DNSBL Enable checkbox.
- Save your settings



### Update Tab

- Select Force Update
- You should now see the DNSBL Feeds being downloaded and parsed. Once that is complete, goto the Dashboard, and confirm that the widget is populated correctly.
- Even an update takes time, so be patient :)

### Firewall / pfBlockerNG / Update IPv6 Reputation General Update Alerts IPv4 DNSBL GeoIP Logs Sync **Update Settings** Firewall Alias Firewall Rules Firewall Logs NEXT Scheduled CRON Event will run at 17:00 with 00:57:24 time remaining. Status Refresh to update current status and time remaining. Force Options \*\* AVOID \*\* Running these "Force" options - when CRON is expected to RUN! Q Select 'Force' option Update Cron Reload

### pfBlockerNG Alerts Tab

- Any domain that is blocked will be reported here. For HTTPS alerts, the SRC IP and URL are not captured due to Browser security measures.
- As a test, goto www.aol.com and www.yahoo.com and see some alerts populate.

- There are several other DNSBL Feeds that can be used with pfBNG DNSBL. I will post that at a later date, once users get their basic configurations working. There is also an ADBlock Easylist tab, which is pretty self-explanatory.

### Firewall / pfBlockerNG / Update IPv6 Reputation General Update Alerts IPv4 DNSBL GeoIP Logs Sync **Update Settings** Firewall Alias Firewall Rules Firewall Logs NEXT Scheduled CRON Event will run at 17:00 with 00:57:24 time remaining. Status Refresh to update current status and time remaining. Force Options \*\* AVOID \*\* Running these "Force" options - when CRON is expected to RUN! Q Select 'Force' option Update Cron Reload

### Dashboard

- Is it possible to view the DNSBL Adblocker status on the dashboard?

# pfBlockerNG











MaxMind: Last-Modified: Mon, 06 Nov 2017 19:15:47 GMT

**Packets** 





Alias

pfB\_DNSBLIP

DNSBL\_ADverts





Count

64557



Nov 21 00:00:08

Updated











- No additional hardware
- Easy to set up
- Quick to configure
- Easy to virtualize
- Extended and subsequent analysis



- @BBcan177
- @pfsense
- @freebsd
- @The\_Pi\_Holeand the whole community for the support

Questions ???????

# Thank you

Author: Michael Koerfer

E-mail: michael\_koerfer@posteo.de

Twitter: @D\_70WN



