

Adblocking NG

Michael Koerfer – 24.11.2017



Overview

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

The background is a deep blue gradient. On the left, there's a faint grid of small squares. On the right, there are several concentric, curved lines that create a sense of depth and movement, resembling a tunnel or a stylized eye.

Hardware

- Home

- Checkout out a Fujitsu Futro S550-2 Thin Client



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

- SOHO

- Checkout out a PC Engines APU.1D Bundle



- AMD Embedded G-Series T40E APU
- 2 GB RAM
- 16 GB MicroSD HDD *extra
- 3 x 1000 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

The background is a deep blue gradient. On the left side, there is a faint, light blue grid pattern. On the right side, there are several concentric, curved lines that create a sense of depth and movement, resembling a tunnel or a stylized eye.

Virtualization

- 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

The background is a deep blue gradient. On the left, there's a faint grid of small squares. On the right, there are several concentric, curved lines that create a sense of depth and movement, resembling a tunnel or a stylized eye.

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

pfSense

COMMUNITY EDITION

System ▾

Interfaces ▾

Firewall ▾

Services ▾

VPN ▾

Status ▾

Diagnostics ▾

Help ▾

Firewall / pfBlockerNG / General

General

Update

Alerts

Reputation

DNSBL

GeoIP

Logs

Sync

General Settings

LINKS

Firewall Alias

Firewall Rules

Firewall Logs

Aliases

NAT

pfBlockerNG

Rules

Schedules

Traffic Shaper

Virtual IPs

Enable pfBlockerNG

☒ Enable/Disable

Keep Settings

☒ Keep settings

Note:

With 'Keep settings' enabled, pfBlockerNG will maintain run state on Installation/Upgrade.
If 'Keep Settings' is not 'enabled' on pkg Install/De-Install, all settings will be Wiped!

Note:

To clear all downloaded lists, uncheck these two checkboxes and 'Save'. re-check both boxes and run a 'Force Update'

- 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



Enable DNSBL

☐

This will enable DNS Block List for Malicious and/or unwanted Adverts Domains
To Utilize, **Unbound DNS Resolver** 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

Select the interface you want DNSBL to Listen on.
Default: **LAN** - Selected Interface should be a Local Interface only.

DNSBL Firewall Rule

☒

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

Enable Logging

Enable

Default: Enable

Select - Logging to Status: System Logs: FIREWALL (Log)

This can be overridden by the 'Global Logging' Option in the General Tab.

Advanced Inbound Firewall Rule Settings



Advanced Outbound Firewall Rule Settings



Alexa Whitelist



Custom Domain Whitelist



TLD Exclusion List



TLD Blacklist



TLD Whitelist



- DNSBL Feeds Tab

- Create a new DNSBL Alias

Enter DNS Group Name as ADs

Enter Description as DNSBL ADverts



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	
				Add

Save

- 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](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/comeleon/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

Enter DNS Group Name. Example: Ads

Description

DNSBL Settings



DNSBL

 ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼

Format

State

Source

Header/Label

Add



List Action

 ▼Default: **Disabled**Select **Unbound** to enable 'Domain Name' blocking for this Alias.

Update Frequency

 ▼Default: **Never**Select how often List files will be downloaded. **This must be within the Cron Interval/Start Hour settings.**

Weekly (Day of Week)

 ▼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

DNSBL Configuration

LINKS

[Firewall Alias](#) [Firewall Rules](#) [Firewall Logs](#)

Info



Enable DNSBL



This will enable DNS Block List for Malicious and/or unwanted Adverts Domains
To Utilize, **Unbound DNS Resolver** 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

Select the interface you want DNSBL to Listen on.

Default: **LAN** - Selected Interface should be a Local Interface only.

DNSBL Firewall Rule



• 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 :)



- General
- Update
- Alerts
- Reputation
- IPv4
- IPv6
- DNSBL
- GeoIP
- Logs
- Sync

Update Settings

[Firewall Alias](#) [Firewall Rules](#) [Firewall Logs](#)

Status NEXT Scheduled CRON Event will run at 17:00 with 00:57:24 time remaining.
Refresh to update current status and time remaining.

Force Options ** AVOID ** Running these "Force" options - when CRON is expected to RUN!

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.

GeneralUpdateAlertsReputationIPv4IPv6DNSBLGeoIPLogsSync

Update Settings

[Firewall Alias](#) [Firewall Rules](#) [Firewall Logs](#)

Status

NEXT Scheduled CRON Event will run at 17:00 with 00:57:24 time remaining.
Refresh to update current status and time remaining.

Force Options

**** AVOID **** Running these "Force" options - when CRON is expected to RUN!

Select 'Force' option

☒ Update

☐ Cron

☐ Reload

Run

View

- Dashboard

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

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










DNSBL:64557



Alias	Count	Packets	Updated	
pfB_DNSBLIP	1	0	Nov 22 16:00	
DNSBL_ADverts	64557	0	Nov 21 00:00:08	

The background is a deep blue gradient. On the left side, there is a faint, light blue grid pattern. On the right side, there are several concentric, curved lines that create a sense of depth and movement, resembling a tunnel or a stylized eye.

Conclusion

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

The background is a deep blue gradient. On the left, there's a faint grid of small squares. On the right, there are several concentric, curved lines that create a sense of depth and movement, resembling a tunnel or a stylized eye.

Credits

- @BBcan177
- @pfsense
- @freebsd
- @The_Pi_Hole

and the whole community for the support

Questions ?????????

Thank you

Author: Michael Koerfer

E-mail: michael_koerfer@posteo.de

Twitter: [@D_70WN](https://twitter.com/D_70WN)

