Enhancing Your Network Security with pfBlockerNG-devel: A Quick Guide

I recently upgraded to pfSense Plus 24.03 and initially hoped to see improvements with pfBlockerNG-devel. However, it appears that pfBlockerNG-devel is facing stability issues in this version. On the other hand, the standard pfBlockerNG seems to be functioning more stably. If you're encountering similar issues with pfBlockerNG-devel, it might be worth switching back to the stable version of pfBlockerNG until further updates address these concerns.

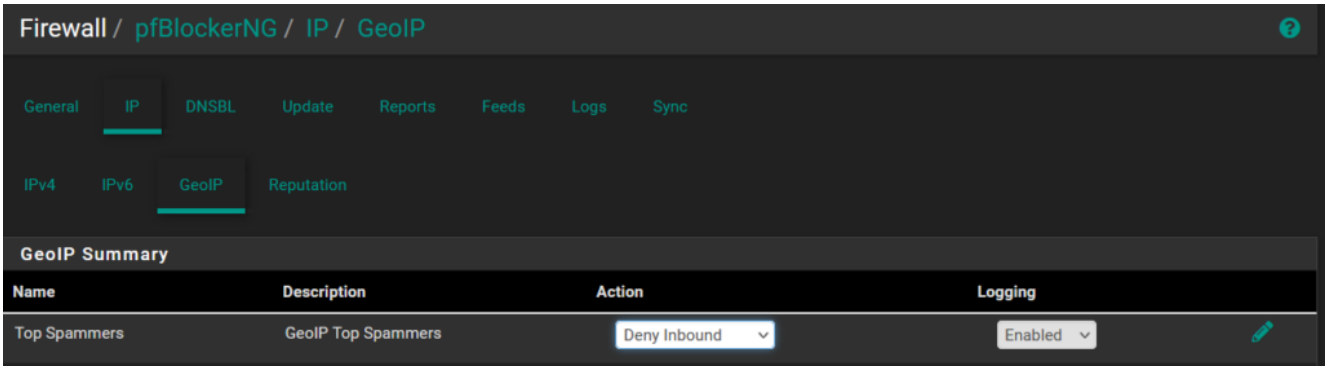
Are you concerned about the security of your home network? Worried about malicious websites, ads, and unwanted content infiltrating your online experience? Look no further than pfBlockerNG-devel, a powerful package for pfSense that allows you to take control of your network's security by implementing various blocking mechanisms. In this guide, we'll walk you through the installation and key configuration steps to get the most out of pfBlockerNG-devel without overwhelming you with technical details.

Installation

To get started, open up your pfSense dashboard and navigate to the System Package Manager. Here, you'll find a list of available packages. Search for "pfBlockerNG-devel" and install it. Once the installation is complete, you'll be guided through a wizard that will assist you in setting up pfBlockerNG.

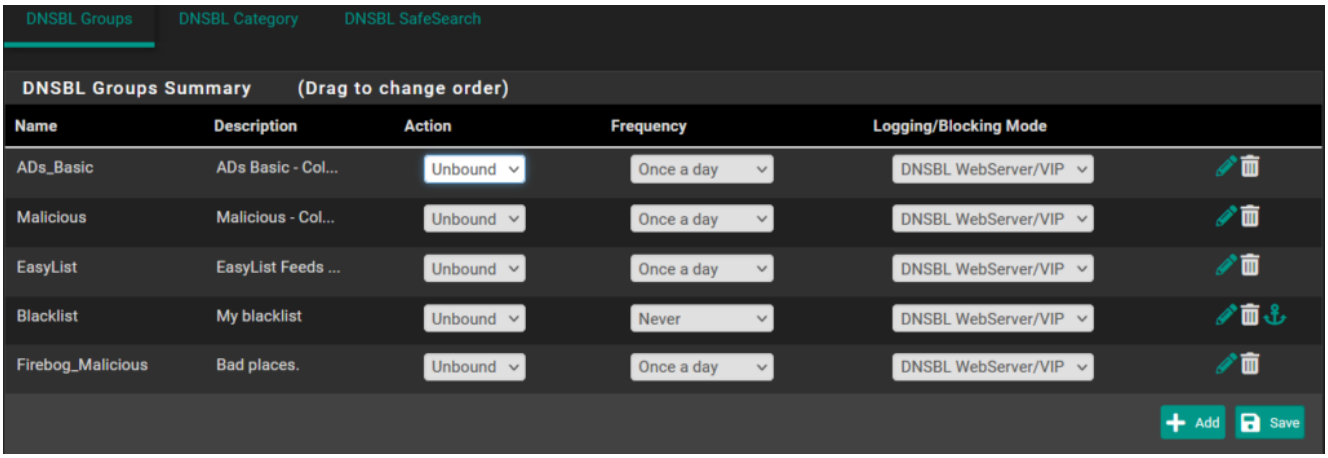
Initial Configuration

After installation, ensure that you enable “floating rules” and “kill states.” These settings are important for the proper functioning of pfBlockerNG.



GeoIP Blocking

One powerful feature of pfBlockerNG-devel is the ability to block traffic based on geographical locations. If there are countries you prefer not to have contact with, you can easily set up inbound blocking rules for them. This adds an extra layer of security to your network.

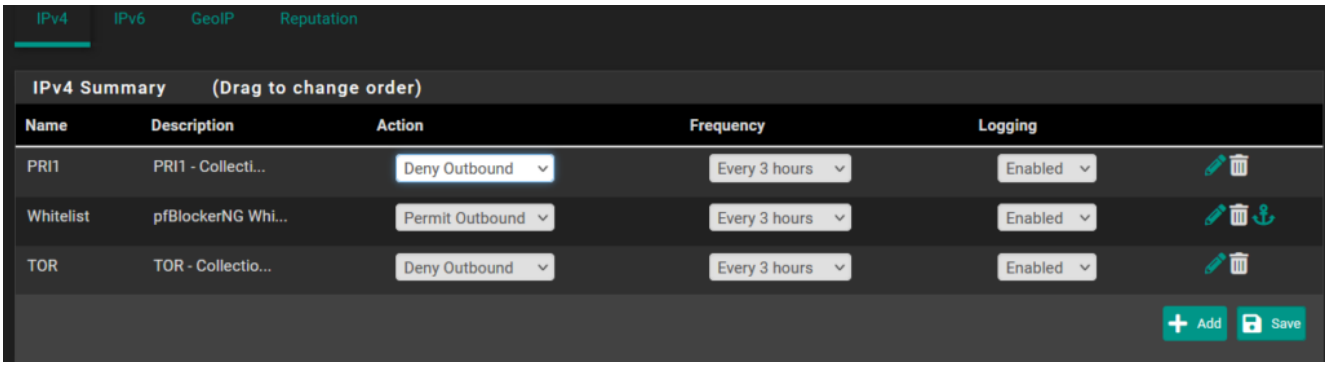


DNSBL (DNS Blocking)

DNSBL, or DNS Blocking, is an essential tool to prevent access to malicious, ads, and unwanted websites. pfBlockerNG-devel supports this feature by allowing you to add various

blacklists. However, it’s important not to go overboard, as blocking too much might hinder your internet usage. Consider enabling lists like “ads_basic,” “malicious,” “easylist,” and “firebog_malicious” under DNSBL groups.

Moreover, the “shalalist” category offers site-blocking options for aggressive, cost traps, drugs, finance, gambling, and spyware-related websites. The “ut1” category includes aggressive, dangerous sites, DDOS, drugs, gambling, malware, phishing, sects, and cheater-related sites. Be selective in your choices to maintain optimal internet usability.



IP Blocking

In the IP blocking section, you can prevent outbound traffic to specific IP addresses. This is useful for devices that may have IP addresses hardcoded in their software, bypassing your DNS. Prioritize blocking known malicious IPs by using the PRI1 and TOR deny outbound lists. Additionally, maintain a whitelist to permit outbound traffic to trusted IPs.

Regular Updates

Remember, changes you make within pfBlockerNG-devel need an update to take effect. Go to “Firewall” and select “pfBlockerNG Update” to ensure your settings are current.

DNS Provider and Security

For enhanced security, consider configuring your external DNS provider. One recommended option is Quad9, known for its comprehensive blocklists and secondary DNS service. Quad9 not only blocks potentially harmful sites but also secures your DNS requests against potential fakes. This extra layer of protection prevents malicious actors from redirecting you to counterfeit websites.

Conclusion

Enhancing your network security with pfBlockerNG-devel doesn’t have to be overwhelming. By following this quick guide, you can set up an effective security solution for your home network. Remember to strike a balance between protection and usability, and stay updated with the latest threat intelligence to keep your online experience safe and smooth.