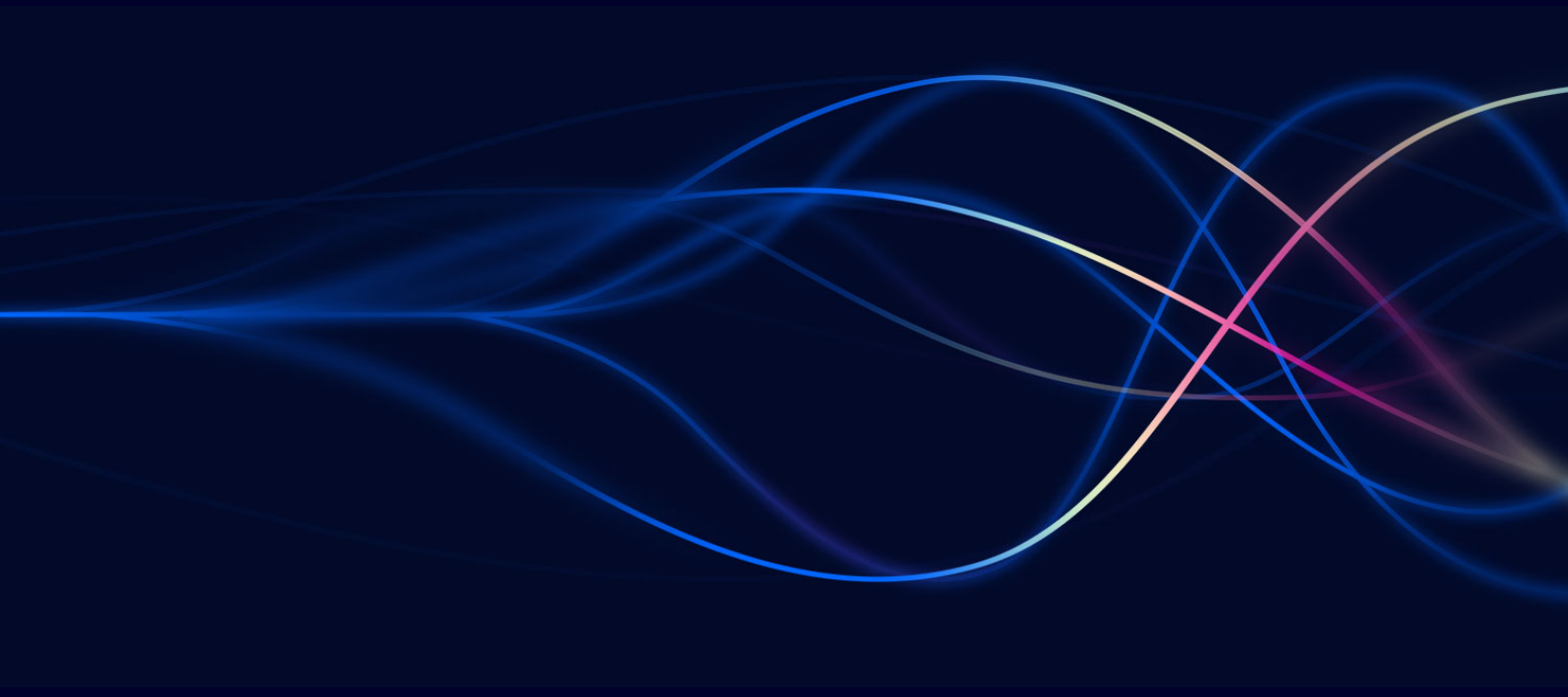
Q-FEEDS

Setup Guide
pfSense

Public



Version 1.0 - 9 February 2026

Introduction

In today's world, keeping your network secure is super important. Firewals are a great tools for protecting your network. They can filter domains and IP addresses using external dynamic lists of threat indicators, known as Indicators of Compromise (IoCs).

Q-Feeds provides dynamic, up-to-date lists of these IoCs, designed specifically for use with security controls like DNS blackholes. By integrating Q-Feeds into your pfSense installation, you can improve your network's protection against new and emerging threats. This means your firewall can automatically block harmful traffic and stay updated with the latest threat information.

This manual will show you how to set up and use Q-Feeds with your pfSense setup, so you can get the best security possible. You'll learn how to configure the pfSense, import Q-Feeds, and ensure everything is working correctly. With these steps, you'll be able to enhance your network's defenses and keep your data safe from cyber threats.

Q-FEEDS

Table of Contents

Introduction *1*

Using Q-Feeds for Enhanced Network Security *3*

Available Lists of Indicators 3

Obtain API-token **3**

1. Install and setup pfBlockerNG *4*

1.1 Installation **4**

1.2. Configuration **4**

2. Configure IP addresses blocklist *5*

3. Domain (DNSBL) configuration *6*

4. Fetch latest intelligence *7*

Using Q-Feeds for Enhanced Network Security

Q-Feeds provides dynamic lists of Indicators of Compromise (IoCs) to enhance your network security controls. These lists, based on Q-Feeds Threat Intelligence Data Feeds, are regularly updated with various types of IoCs such as IP addresses and domains. By using these lists, you can monitor and block user access to dangerous network resources effectively.

Available Lists of Indicators

Q-Feeds offers the following types of indicators for pfSense:

Name	Type	Description	URI
Malware Domains	Domain	List of malicious domains	https://api.qfeeds.com/api?feed_type=malware_domains&api_token=XXXXXX&limit= XXXXXX
Malware IPs	IP	List of malicious IPs	https://api.qfeeds.com/api?feed_type=malware_ip&api_token=XXXXXX&limit= XXXXXX

To optimize system performance and prevent unnecessary strain on our infrastructure, please schedule updates at the standard interval of 20 minutes. Setting the interval to less than 20 minutes is not beneficial.

Obtain API-token

Accessing the lists—including direct downloads into your network security solutions—requires an API token from Q-Feeds. You can request this token through your account manager or by registering at **https://tip.qfeeds.com/**

We have multiple types of keys available from Free (community edition) to Plus and Premium. You can find more information on **https://qfeeds.com/licenses**

To test downloading the lists, you can use the cURL utility. Here is the syntax for Linux systems:

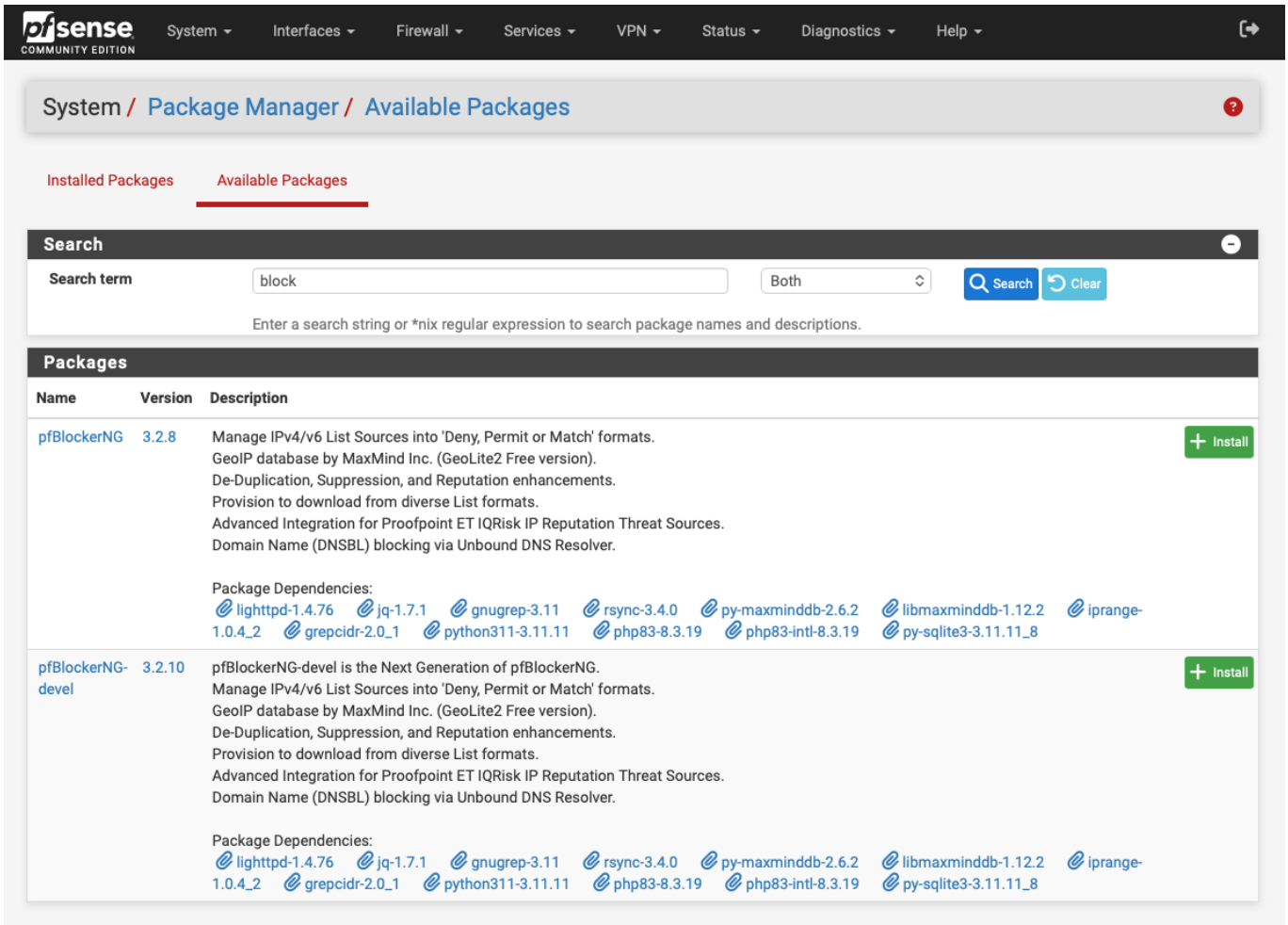
curl -v -u api_token:XXXXX https://api.qfeeds.com/api?feed_type=malware_domains&limit=XXXXX

1. Install and setup pfBlockerNG

1.1 Installation

In order to use Q-Feeds on your firewall we need to install the plugin pfBlockerNG (externally maintained). You can find the plugin in the package manager under

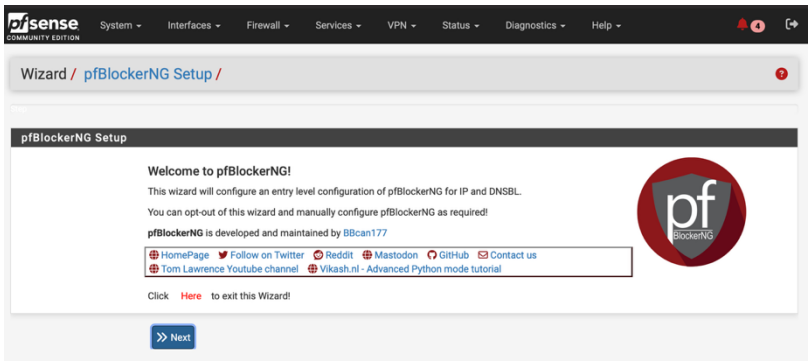
System -> Package manager -> available packages



Click install next to the **pfBlockerNG** line and follow the instructions

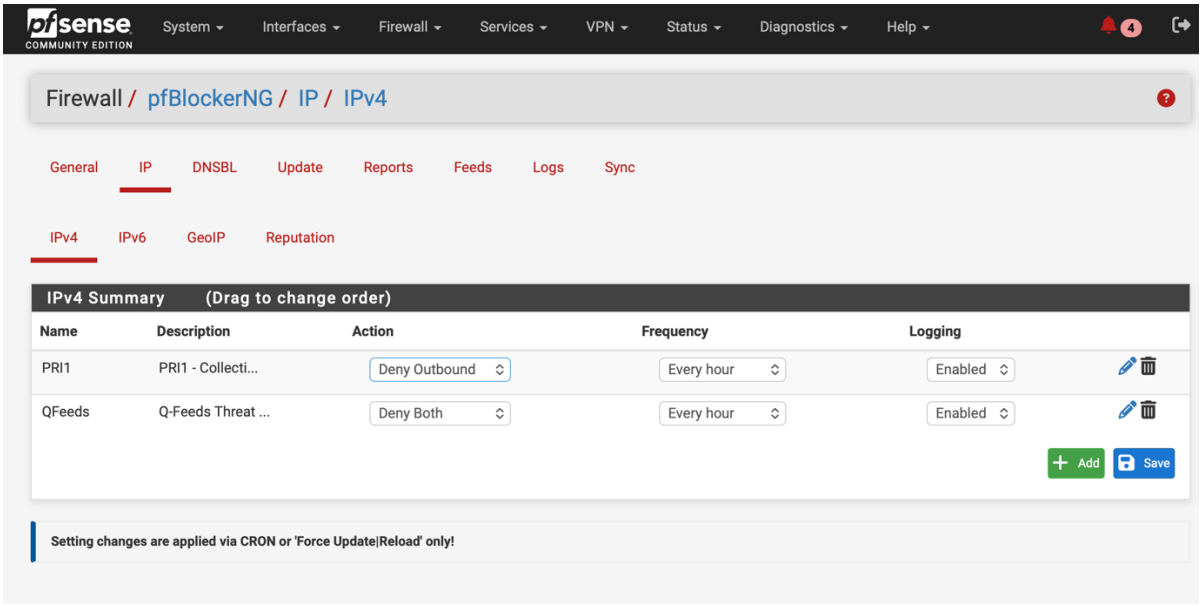
1.2. Configuration

Access pfBlockerNG via **Firewall -> pfBlockerNG.** If you open this plugin for the first time you're presented with a wizard. For this manual we click 'here' to exit this wizard but feel free to follow the wizard to setup other feeds.



2. Configure IP addresses blocklist

Go to **IP -> IPv4** and click the green Add button



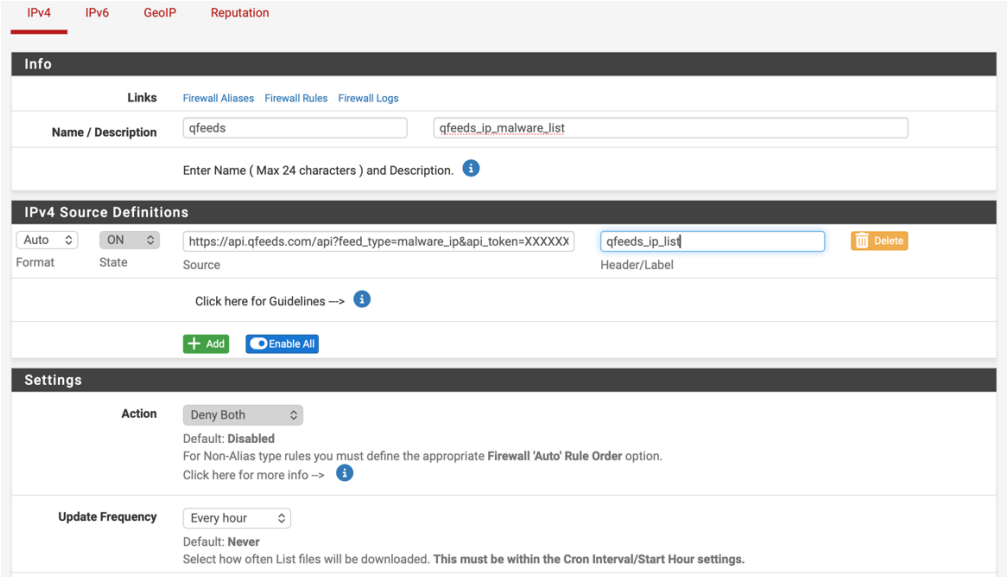
On this page you need to fill in a name and description of the collection. In the IPV4 source definitions you select ‘ON” in the state field and copy the following URL in the source field:

https://api.qfeeds.com/api?feed_type=malware_ip&api_token=XXXXXX

Don’t forget to replace the red XXX with your own api_token.

As Action select Deny Both and select the Update Frequency according to your license:

- Community = daily
- Plus = 4 hours
- Premium = 1 hour



Hit Save IPV4 settings on the bottom of the page

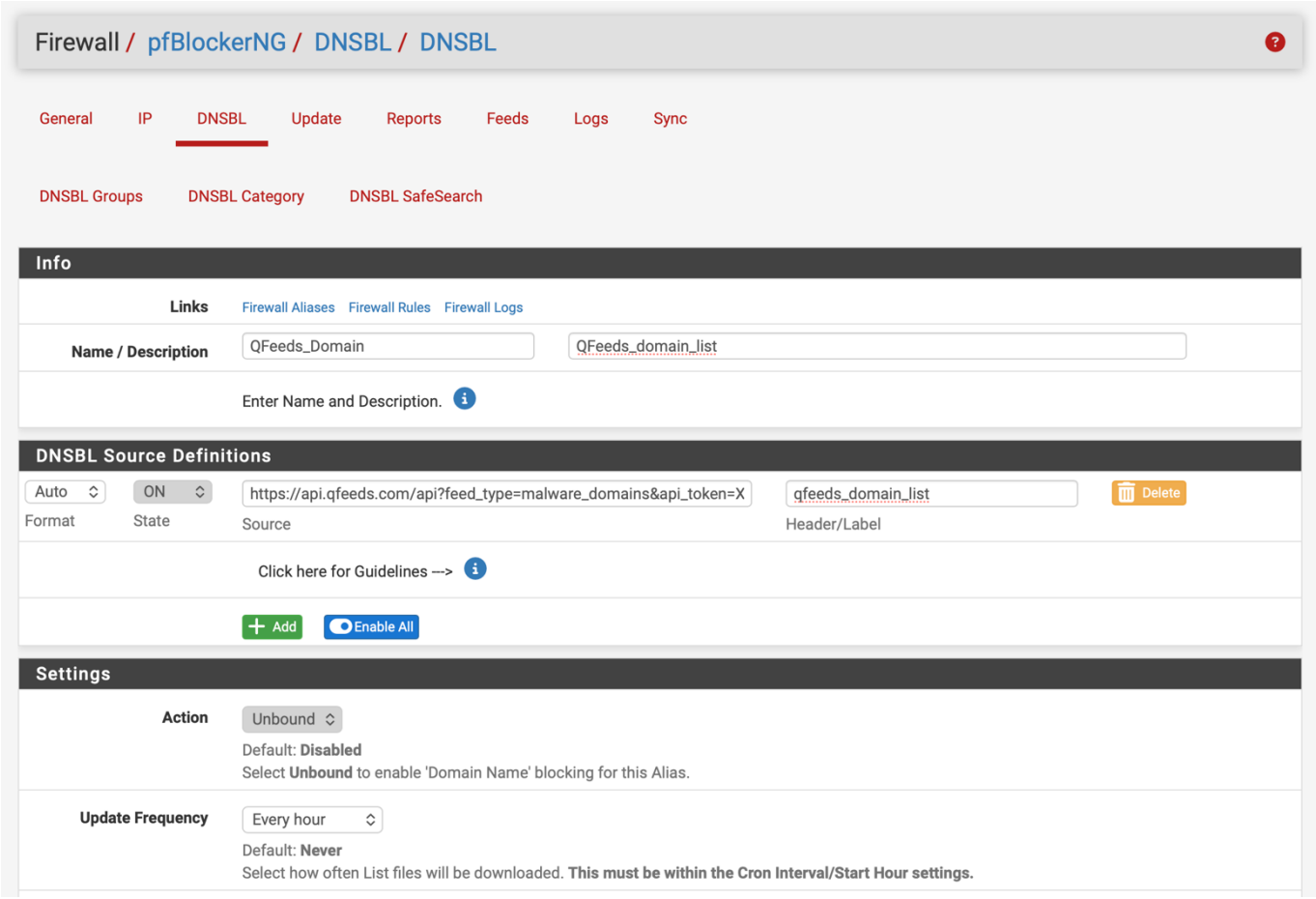
3. Domain (DNSBL) configuration

Exactly the same as the IP list but in the DNSBL tab:

With this URL:

https://api.qfeeds.com/api?feed_type=malware_domains&api_token=XXXXXX

Select State “on” and Action Unbound:



Hit Save DNSBL Settings on the bottom of the page

4. Fetch latest intelligence

On the Update tab you can force download the latest threat intelligence from Q-Feeds. Select Reload and hit Run:

Do not run force update when cron is running or about to run (like in the screenshot below)