



Setup Guide pfSense

Public



Introduction

In today's world, keeping your network secure is super important. Firewalls are a great tool 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.

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:

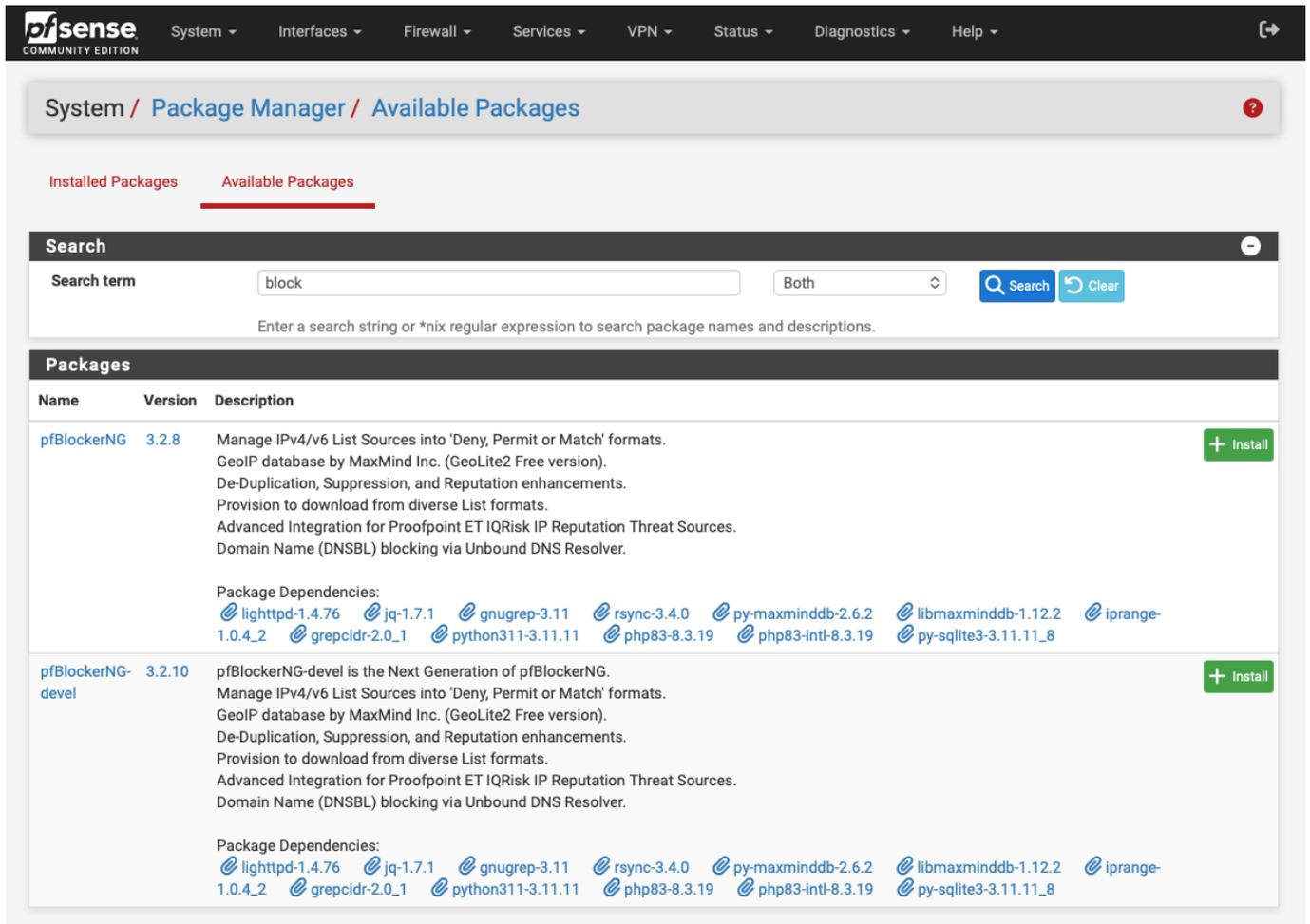
```
curl -v -u api_token:XXXXX https://api.qfeeds.com/api?feed_type=malware_domains&limit=XXXXX
```

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



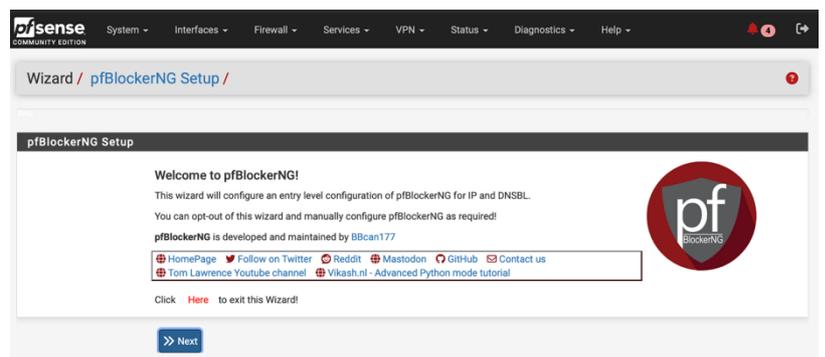
The screenshot shows the pfSense Package Manager interface. The search term is 'block'. Two packages are listed:

Name	Version	Description	Action
pfBlockerNG	3.2.8	Manage IPv4/v6 List Sources into 'Deny, Permit or Match' formats. GeoIP database by MaxMind Inc. (GeoLite2 Free version). De-Duplication, Suppression, and Reputation enhancements. Provision to download from diverse List formats. Advanced Integration for Proofpoint ET IQRisk IP Reputation Threat Sources. Domain Name (DNSBL) blocking via Unbound DNS Resolver. Package Dependencies: lighttpd-1.4.76 jq-1.7.1 gnugrep-3.11 rsync-3.4.0 py-maxminddb-2.6.2 libmaxminddb-1.12.2 iprange-1.0.4_2 grepclidr-2.0_1 python311-3.11.11 php83-8.3.19 php83-intl-8.3.19 py-sqlite3-3.11.11_8	+ Install
pfBlockerNG-devel	3.2.10	pfBlockerNG-devel is the Next Generation of pfBlockerNG. Manage IPv4/v6 List Sources into 'Deny, Permit or Match' formats. GeoIP database by MaxMind Inc. (GeoLite2 Free version). De-Duplication, Suppression, and Reputation enhancements. Provision to download from diverse List formats. Advanced Integration for Proofpoint ET IQRisk IP Reputation Threat Sources. Domain Name (DNSBL) blocking via Unbound DNS Resolver. Package Dependencies: lighttpd-1.4.76 jq-1.7.1 gnugrep-3.11 rsync-3.4.0 py-maxminddb-2.6.2 libmaxminddb-1.12.2 iprange-1.0.4_2 grepclidr-2.0_1 python311-3.11.11 php83-8.3.19 php83-intl-8.3.19 py-sqlite3-3.11.11_8	+ Install

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

1.2. Configuration

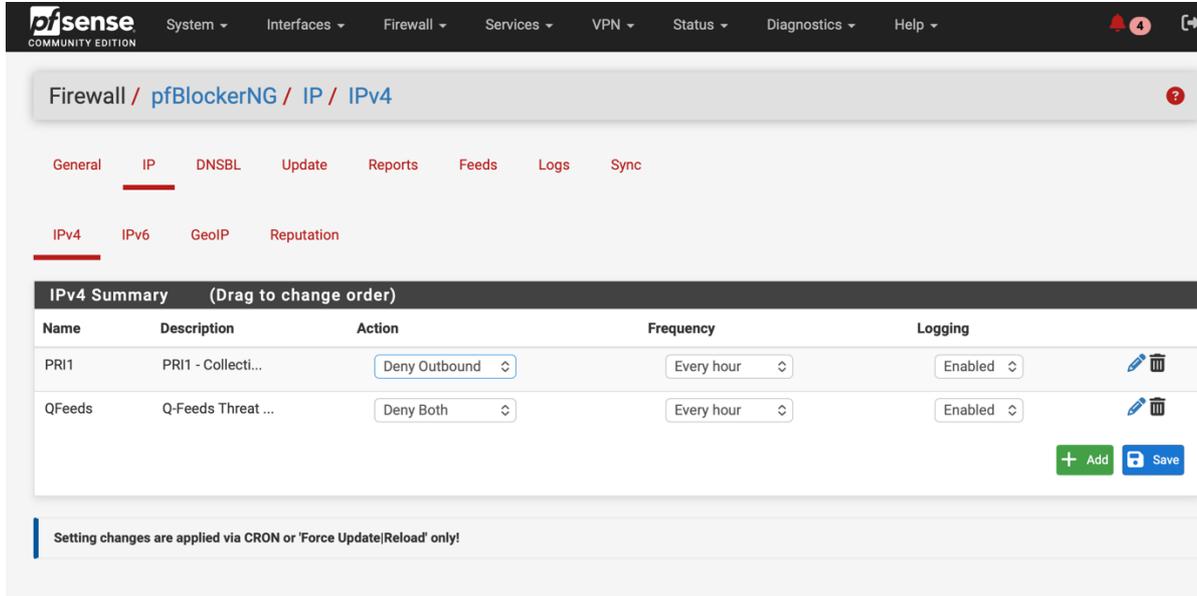
Access pfBlockerNG via **Firewall -> pfBlockerNG**. If you open this plugin for the first time you're presented with a wizard. For this manual we click 'here' to exit this wizard but feel free to follow the wizard to setup other feeds.



The screenshot shows the pfBlockerNG Setup Wizard. The title is 'Wizard / pfBlockerNG Setup /'. The main content says: 'Welcome to pfBlockerNG! This wizard will configure an entry level configuration of pfBlockerNG for IP and DNSBL. You can opt-out of this wizard and manually configure pfBlockerNG as required! pfBlockerNG is developed and maintained by BBcan177'. There are links for 'HomePage', 'Follow on Twitter', 'Reddit', 'Mastodon', 'GitHub', 'Contact us', 'Tom Lawrence Youtube channel', and 'Vikash.ni - Advanced Python mode tutorial'. A 'Next' button is at the bottom.

2. Configure IP addresses blacklist

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



Firewall / pfBlockerNG / IP / IPv4

General **IP** DNSBL Update Reports Feeds Logs Sync

IPv4 **IPv6** GeoIP Reputation

IPv4 Summary (Drag to change order)

Name	Description	Action	Frequency	Logging
PRI1	PRI1 - Collecti...	Deny Outbound	Every hour	Enabled
QFeeds	Q-Feeds Threat ...	Deny Both	Every hour	Enabled

+ Add Save

Setting changes are applied via CRON or 'Force Update|Reload' only!

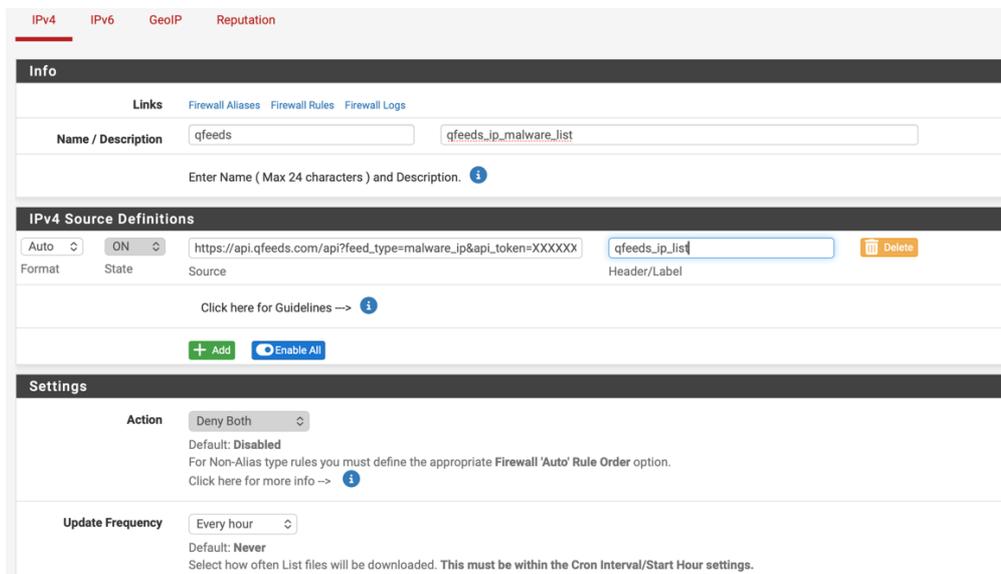
On this page you need to fill in a name and description of the collection. In the IPV4 source definitions you select 'ON' in the state field and copy the following URL in the source field:

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



IPv4 **IPv6** GeoIP Reputation

Info

Links Firewall Aliases Firewall Rules Firewall Logs

Name / Description qfeeds qfeeds_ip_malware_list

Enter Name (Max 24 characters) and Description.

IPv4 Source Definitions

Auto ON https://api.qfeeds.com/api?feed_type=malware_ip&api_token=XXXXXX qfeeds_ip_list Delete

Format State Source Header/Label

Click here for Guidelines -->

+ Add Enable All

Settings

Action Deny Both

Default: Disabled
For Non-Alias type rules you must define the appropriate Firewall 'Auto' Rule Order option.
Click here for more info -->

Update Frequency Every hour

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

Hit Save IPV4 settings on the bottom of the page

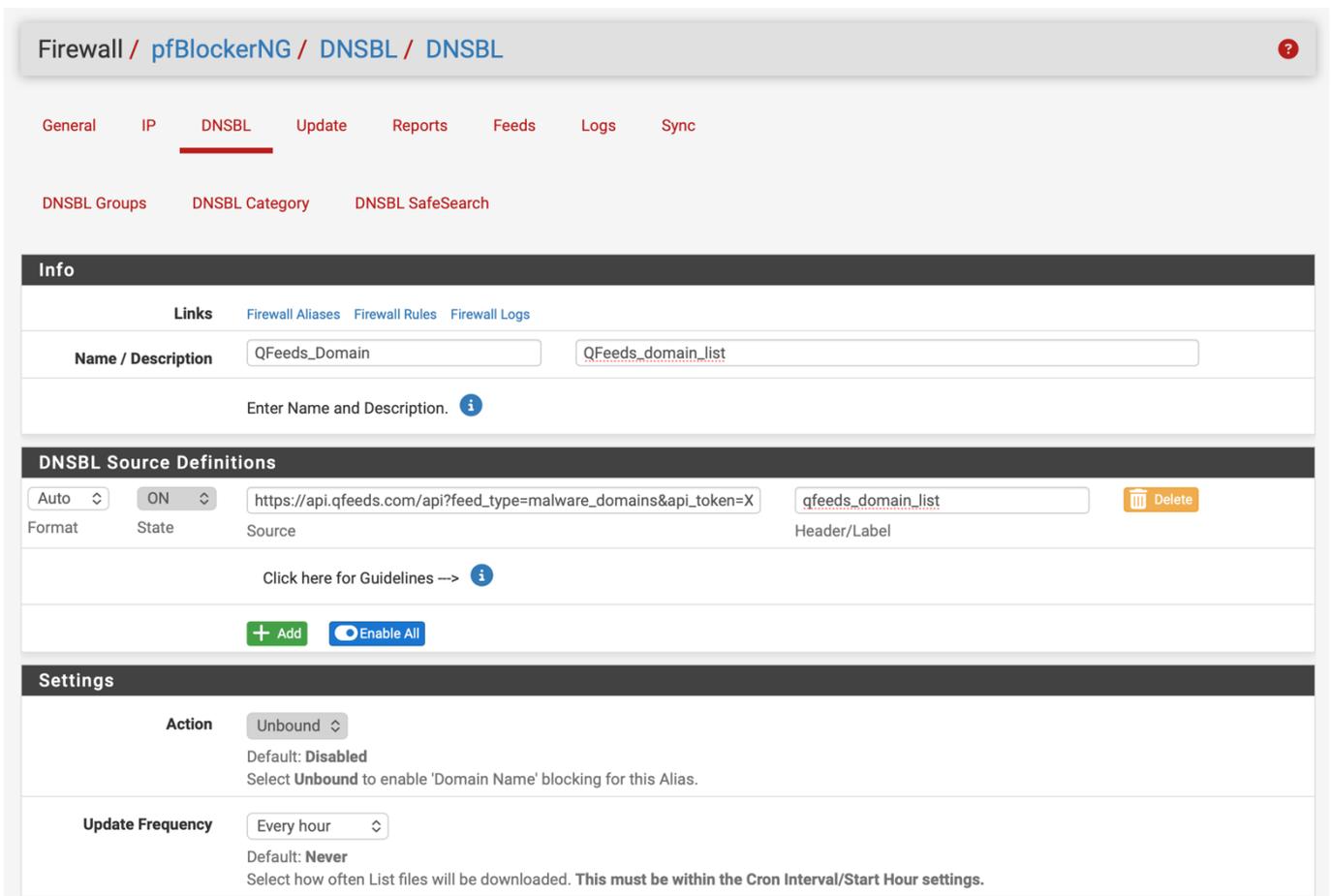
3. Domain (DNSBL) configuration

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:



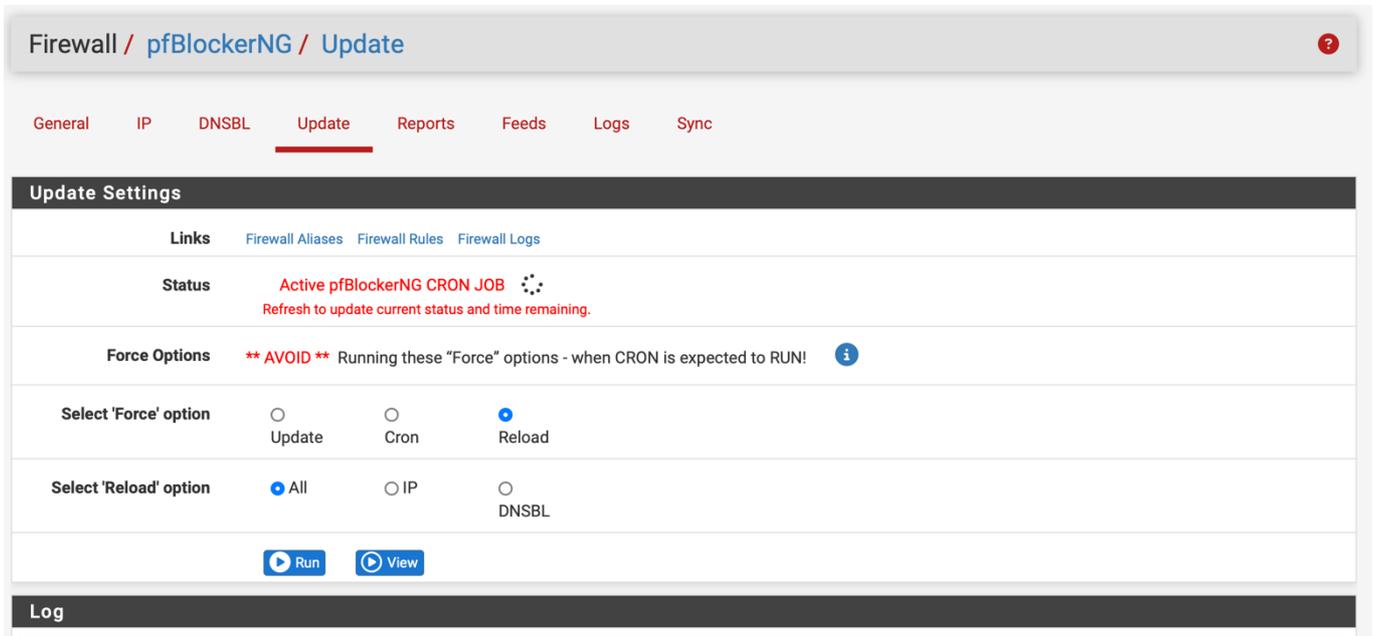
The screenshot shows the pfBlockerNG DNSBL configuration page. The breadcrumb trail is Firewall / pfBlockerNG / DNSBL / DNSBL. The 'DNSBL' tab is selected. Below the tabs are sub-sections: DNSBL Groups, DNSBL Category, and DNSBL SafeSearch. The 'Info' section shows links for Firewall Aliases, Firewall Rules, and Firewall Logs. The 'Name / Description' section has two input fields: 'QFeeds_Domain' and 'QFeeds_domain_list'. Below this is a prompt to 'Enter Name and Description'. The 'DNSBL Source Definitions' section contains a table with columns for Format, State, Source, and Header/Label. The current entry has Format 'Auto', State 'ON', Source 'https://api.qfeeds.com/api?feed_type=malware_domains&api_token=X', and Header/Label 'qfeeds_domain_list'. There is a 'Delete' button next to the entry. Below the table are buttons for '+ Add' and 'Enable All'. The 'Settings' section has an 'Action' dropdown set to 'Unbound' and an 'Update Frequency' dropdown set to 'Every hour'. The 'Action' section includes a note: 'Default: Disabled. Select Unbound to enable 'Domain Name' blocking for this Alias.' The 'Update Frequency' section includes a note: 'Default: Never. Select how often List files will be downloaded. This must be within the Cron Interval/Start Hour settings.'

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)



The screenshot shows the 'Update Settings' page in pfBlockerNG. The breadcrumb navigation is 'Firewall / pfBlockerNG / Update'. The 'Update' tab is selected in the top navigation bar. The page content includes:

- Links:** Firewall Aliases, Firewall Rules, Firewall Logs
- Status:** Active pfBlockerNG CRON JOB (with a refresh icon) and a note: 'Refresh to update current status and time remaining.'
- Force Options:** A warning: '** AVOID ** Running these "Force" options - when CRON is expected to RUN!' with an information icon.
- Select 'Force' option:** Radio buttons for Update, Cron, and Reload (selected).
- Select 'Reload' option:** Radio buttons for All (selected), IP, and DNSBL.
- Buttons:** 'Run' and 'View' buttons.
- Log:** A section header for the log area.