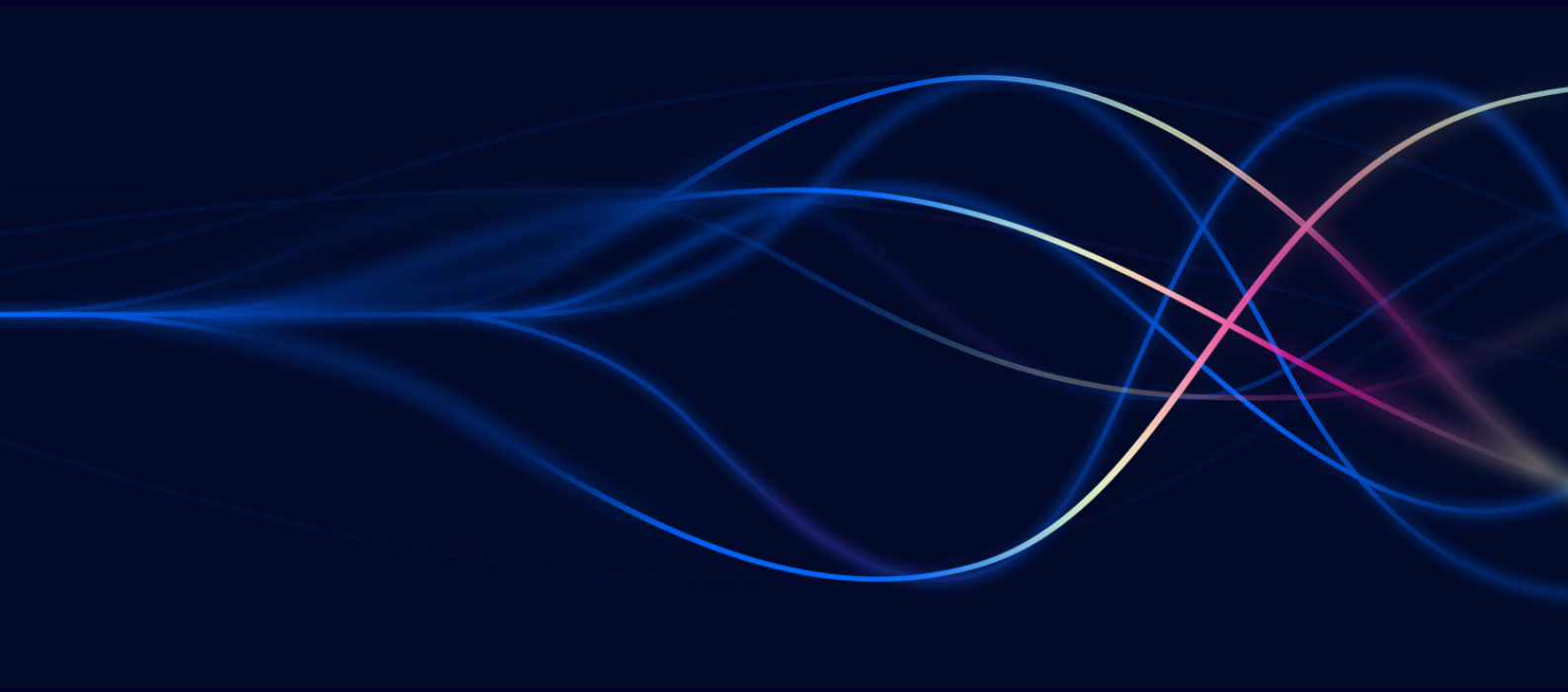
Q-FEEDS

OPNsense®
Securing networks made easy

Setup Guide
OPNsense

Public



Version 1.7 - 16 December 2025

Introduction

In today's world, keeping your network secure is super important. Next Generation Firewalls (NGFWs) are essential tools for protecting your network. They can filter DNS and web traffic 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 NGFWs. By integrating Q-Feeds into your OPNsense firewall, 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 OPNsense firewall, so you can get the best security possible. You'll learn how to configure the firewall, 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.

This manual is written for the latest version of OPNsense in December 2025, **V25.7.9**

Q-FEEDS

Table of Contents

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:

Name	Type	Description
Malware IP	IP	List of dangerous IP addresses
Malware Domains	Domains	List of malicious domains

Update intervals

The type of license determines the update schedule of the IOCs. With our community edition the refresh time is 7 days, for the Plus license every 4 hours and for our Premium offer it's every 20 minutes.

		COMMUNITY EDITION	PLUS	PREMIUM
SERVICES	Active Support	✗	✓	✓
	Easy Integration	✓	✓	✓
	Curated data	✓	✓	✓
	Update Frequency	delayed by **7 days**	delayed by **4 hours**	every **20 minutes**
	IoC Lookup	✗	✓	✓
OSINT	IP	✓	✓	✓
	DNS	✓	✓	✓
PAID	IP	✗	✓	✓
	DNS	✗	✗	✓

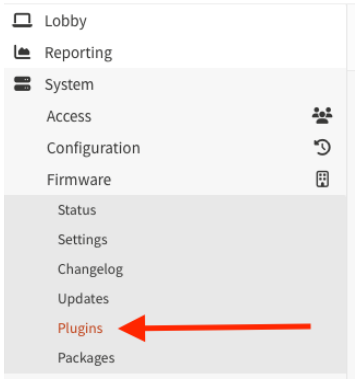
Services

With certain types of licenses you're eligible for some extra functionality on our Threat Intelligence Portal. This includes IoC lookup giving you the possibility to lookup certain IoCs and learn why they're included in our data feeds. It also provides you information like a threat score, geo locations, DNS and NS records etc.

Setup Q-Feeds

To setup Q-Feeds, first make sure your firewall is updated to the latest firmware. Prior versions might work but are not guaranteed supported.

Step 1. Install Q-Feeds plugin



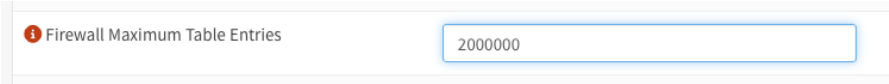
Installing the Q-Feeds plugin is easy. In the menu go to **System → firmware → plugins**

On the page which opens on the left you can use the search function to install the Q-Feeds plugin by pressing the little **+** icon on the right.

After the installation continue to step 2.

Step 2. Increase Maximum table size. (Optional on older OPNsense versions)

After the setup you may need to increase the maximum table size to a minimum of 2.000.000. This can be done via the menu **Firewall → Settings → Advanced**



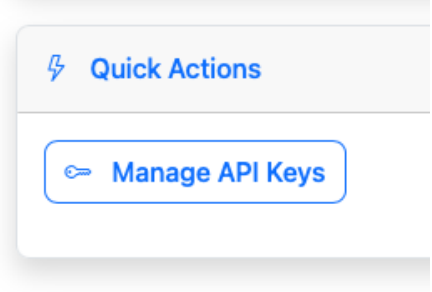
Scroll down until you see the field '**Firewall Maximum Table Entries**'. Most likely if you've never changed this field its empty. Please fill in a minimum of **2.000.000.** You can check your Maximum Table Entries by going to Firewall -> Aliases and check the counter in the top right. On the screenshot below you see an example of the Maximum Table Size set to 5.000.000.

Step 3. Activate the plugin

To activate the plugin please go to **Security → Q-Feeds Connect**. The settings page of the Q-Feeds plugin will now open and it asks for an API token. You can obtain this token by register an account on our Threat Intelligence Portal (https://tip.qfeeds.com) .

After you've registered an account and logged in, on the dashboard you will find the '**Manage API Keys**' page. On this page click **'Create Free API Key'.** Copy the API token into the settings page of the plugin on your OPNsense appliance.

Click Apply and the plugin will start fetching the Threat Intelligence and create firewall aliases.



Step 4. Create firewall rules for IP based blocking

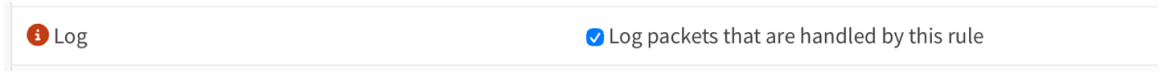
Depending on your setup you can create firewall rules which includes our Threat Intelligence. In order to do so go to **Firewall → Rules**. Depending on your needs you can select an interface, or you can create a Floating rule to target multiple interfaces at once.

Example

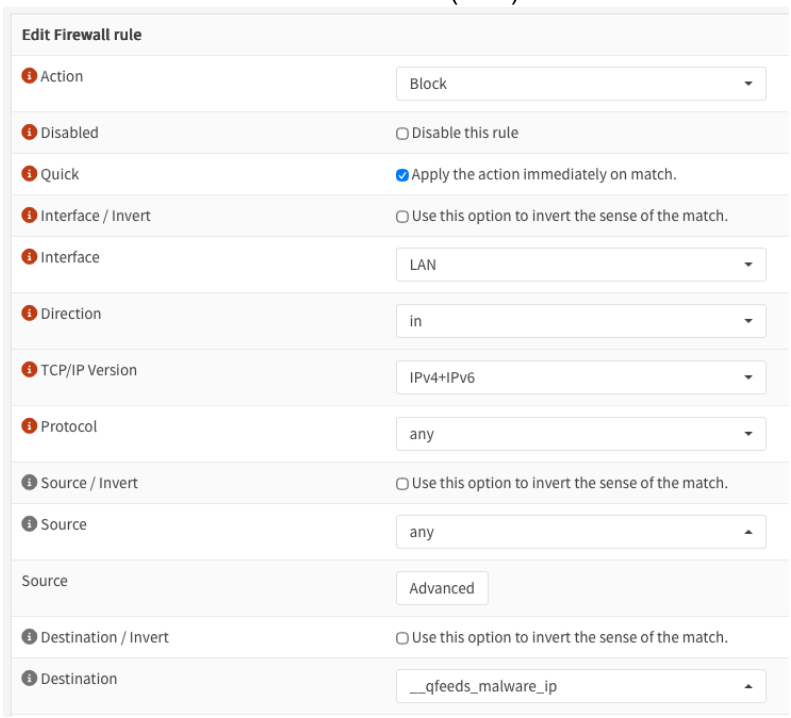
For this example we will setup floating rules to block both incoming and outgoing connections, regardless the interface, which are known by Q-Feeds for being malicious. To do so select **Floating**. You need to create two firewall rules in order to block both connections from- and to the malicious IP addresses.

Click on the "**+**" Icon to create a new rule.

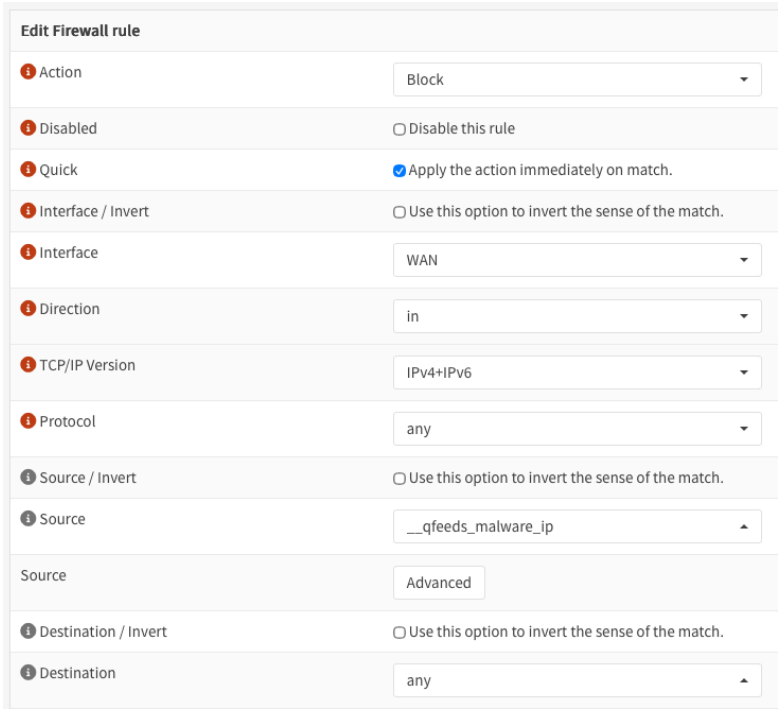
- **Action**
  - Select block or reject depending on your preferences. We advise to use block so the malicious IP won't get notified that you've actively blocked it using a firewall. For your LAN (Rule 1 in the example below) rule you could use Reject.
- **Interface**
  - Select the interfaces on which you would like to block the connections. While you could select multiple interfaces, in this example we chose to use both LAN (towards Q-feeds destination) & WAN (from Q-feeds source) for INBOUND blocking.
- **TCP/IP Version:**
  - Select IPV4/IPV6. Obviously, it depends on which versions you use. Our threat intelligence contains both.
- **Direction**
  - Using "any", traffic originating from the firewall (for example a local proxy) is additionally not allowed. By default, we select "in" for rules as traffic usually originates from a network connected to the firewall.
- **Logging**
  - We advise you to enable the log for the rules in order to use the Events page within the plugin. Without any logs this page will not show any results although there are blocked anyway.



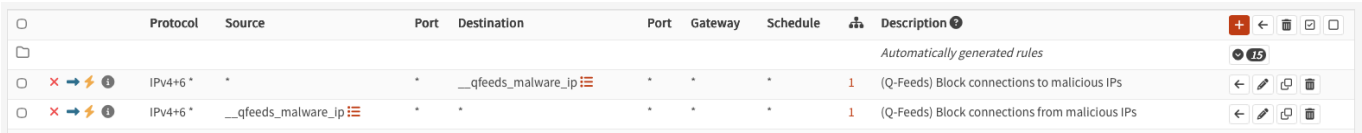
- ***Rule 1:***
  - **Destination Malware IPs**
    - Select the alias created by our plugin in the destination field. This rule ensures clients connected with the selected interface (LAN) cannot reach out to the addresses in our list.



- ***Rule 2:***
  - **Source**
    - Select an alias created by our plugin. This ensures traffic originating from these addresses is not allowed. This rule is optional as in most cases inbound traffic from external addresses is only selectively allowed.



Your rules should look like this:



These rules are just some simple examples on how to setup a firewall rule blocking IP addresses which are marked malicious by **Q-Feeds**. Yet it is an example and different rule setups might be required for different setups.

IPV6

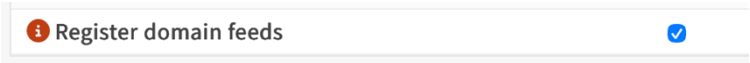
If you have an IPV6 enabled setup you can create the firewall rules for IPV6 as well. Keep in mind that IPv6 addresses are very dynamic—cybercriminals often rotate them quickly—so IPv6 blocking is only a smaller part of our intelligence set.

Setup DNS/Domain blocking with Unbound

Note: In order to make us of DNS based logging you need to configure Unbound as your primary DNS server. More information on how to configure this can be found here: https://docs.opnsense.org/manual/unbound.html

Step 1. Enable DNS in the Q-Feeds plugin

Go to the plugin settings page via the menu **Security → Q-Feeds Connect.** On the settings page you'll find the 'Register domain feeds' option.



Step 2. (only for older versions <25.7.9) Enable Unbound and enable the blocklist functionality.

Go to **Services → Unbound DNS → General.** And enable the unbound DNS server if it's not active.

You also need to enable the blocklist functionality within Unbound by going to **Services → Unbound DNS → Blocklist.** Optionally you can select additional blocklists for Ad blocking for example. Now you're all set.

Step 3. Check blocklist population.

Go to **Reporting → Unbound DNS** to check if the blocklist got populated with the actual domain names. On the details tab you can also see the DNS requests and possible blocks.

Purchase and configure Q-Feeds Plus or Premium

Step 1. Acquire a Plus or Premium license

In order to further improve the efficiency of the plugin and your security posture you can purchase a Plus or Premium license in our webstore. Head to http://qfeeds.com/opnsense/ to choose your package of choice and follow along on the webstore steps.

Note: For extra convenience use the same email address as you did when registering on the threat intelligence portal. This way your license will be added to your account automatically after your order.

Step 2. (optional) Activate your plus or Premium license

In case you did not or couldn't use the same email address on the Threat intelligence Portal you will receive an activation key. You can fill in this activation key under **Top right <your account name> → Licenses →Activate new license.** Here you can fill in the activation key you've received. When this is done you can assign the license to your API-key under API-Key management.