PBXMONITOR

Central Blacklist Setup Guide for pfSense Firewalls

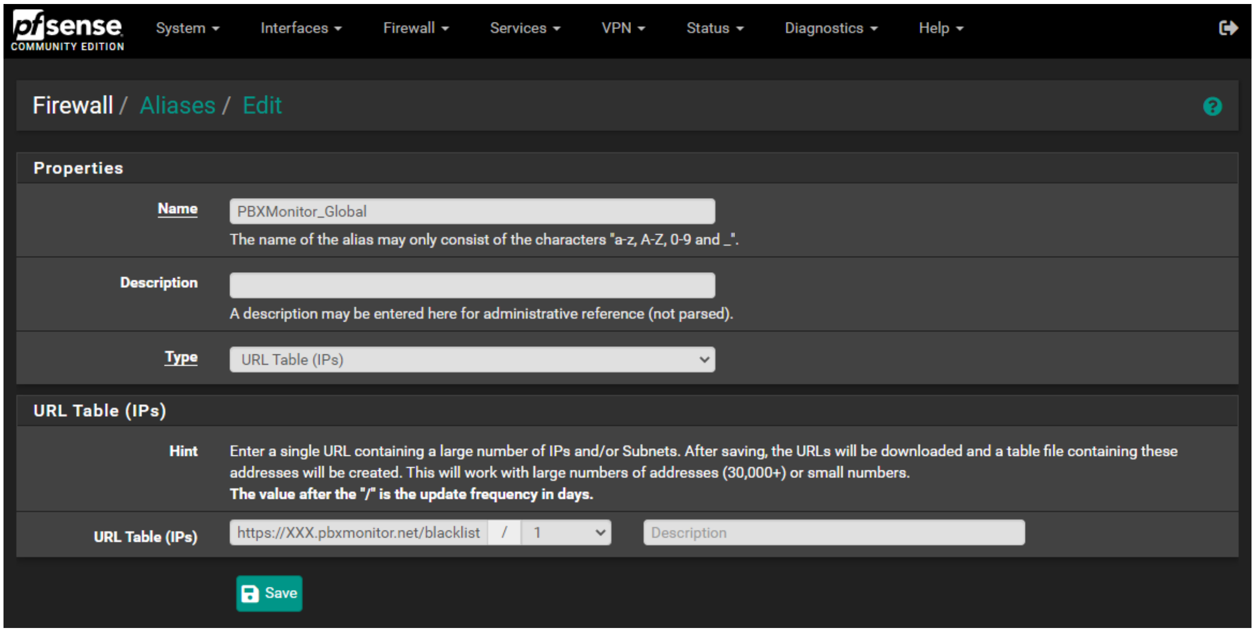
Created based on pfSense CE 2.5.2-RELEASE on 10-13-2021

Author: Brentt Graeb

DISCLAIMER: This guide does not assume you have CARP, Multi-WAN, Load Balancing, etc, enabled on the firewall, in those scenarios small differences in the setup will be needed, but the changes required should be self-evident. Contact support if you run into issues that this document does not cover.

Step 1: Login to pfSense as a full admin, and go to Firewall > Aliases, and Click the +Add button.

Step 2: Fill in the page as you see below, for the URL Table (IPs) Value, look in PBXMonitor under **Central Security > Distribution Log,** Copy the link displayed there, and paste it into the field, Ensure no leading or trailing spaces. Then ensure the Octet or Slash setting is set to 1, this tells the firewall to update the list daily. Click the Save Button. And then Click Apply Changes.



Firewall / Aliases / Edit

Properties

Name: PBXMonitor_Global
The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".

Description:
A description may be entered here for administrative reference (not parsed).

Type: URL Table (IPs)

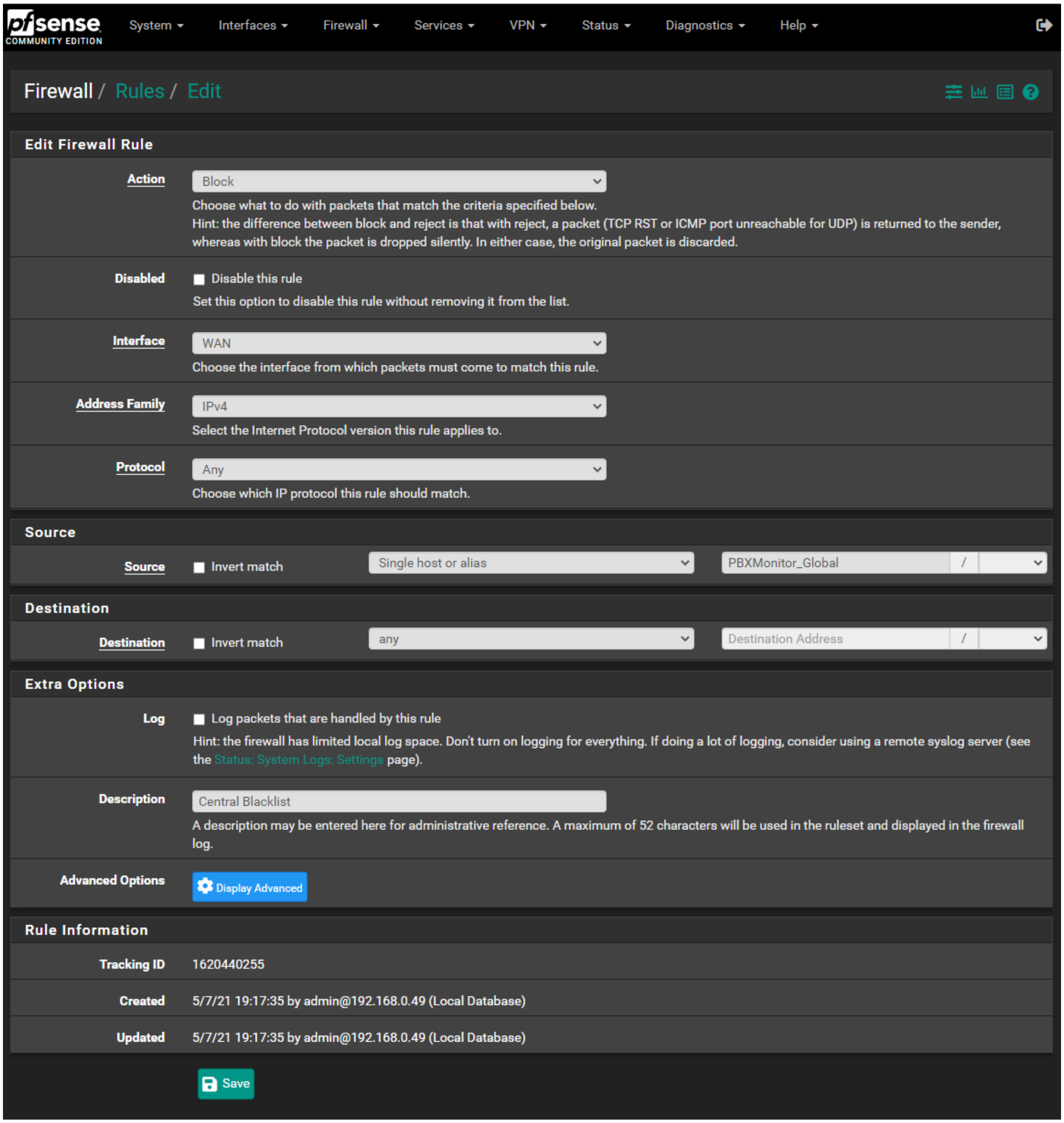
URL Table (IPs)

Hint: Enter a single URL containing a large number of IPs and/or Subnets. After saving, the URLs will be downloaded and a table file containing these addresses will be created. This will work with large numbers of addresses (30,000+) or small numbers.
The value after the "/" is the update frequency in days.

URL Table (IPs): https://XXX.pbxmonitor.net/blacklist / 1 Description

If you receive an Error Message, Check that your firewall has proper DNS Servers on the System > General Setup, page, and ensure all fields were filled out properly, if the problem persists contact support.

Step 3: Navigate to **Firewall > Rules > WAN**, and click the Add button with the Arrow Up on it. And fill in the page as you see below, and then click save. Note again that if you have a CARP, Multi-WAN, or Load Balancing setup in pfSense, minor differences may be required.



Firewall / Rules / Edit

Edit Firewall Rule

Action: Block
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled: □ Disable this rule
Set this option to disable this rule without removing it from the list.

Interface: WAN
Choose the interface from which packets must come to match this rule.

Address Family: IPv4
Select the Internet Protocol version this rule applies to.

Protocol: Any
Choose which IP protocol this rule should match.

Source

Source: □ Invert match | Single host or alias | PBXMonitor_Global /

Destination

Destination: □ Invert match | any | Destination Address /

Extra Options

Log: □ Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description: Central Blacklist
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options: Display Advanced

Rule Information

Tracking ID: 1620440255

Created: 5/7/21 19:17:35 by admin@192.168.0.49 (Local Database)

Updated: 5/7/21 19:17:35 by admin@192.168.0.49 (Local Database)

Save

STEP 4: Re-Verify all Settings are correct, and ensure that the new rule is the top rule on the **Firewall > Rules > WAN** page, any rules that are above this rule, would be exempted from its effects, and while some environments may have a need for this, this is outside of the scope of this document and not a situation we consider supported. If everything looks correct, you can now click the Apply Changes button. All IPs you place on PBXMonitors Central Blacklist will now feed into your firewall and be blocked at the firewall daily.