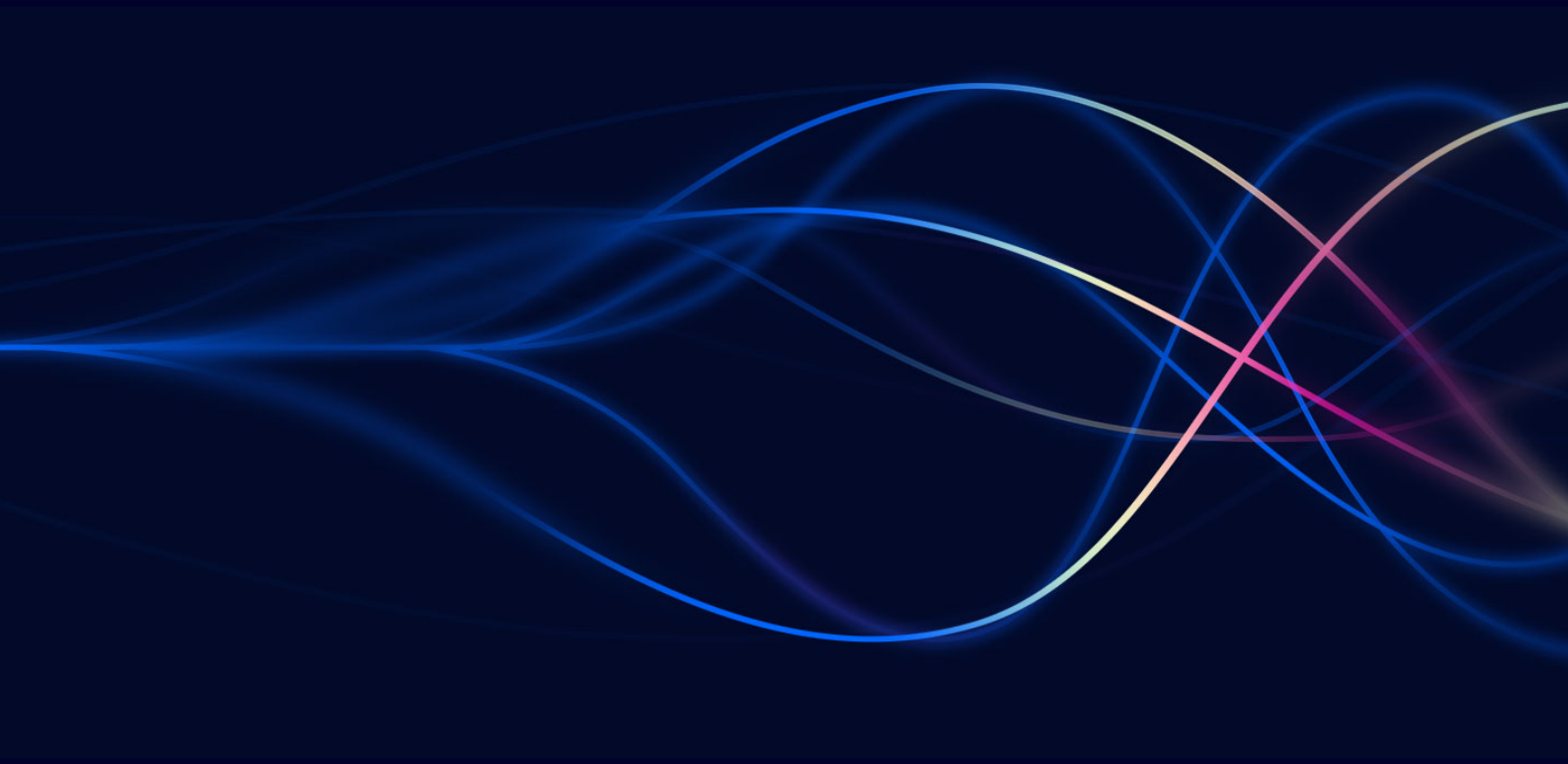
Q-FEEDS

Setup Guide
IPtables (Linux)

Public



Version 1.0 – 12 November 2024

Introduction

In today's world, keeping your network and devices secure is of upmost importance. On linux we can leverage Iptables to manage IP traffic on Linux hosts.

Q-Feeds provides dynamic, up-to-date lists of these IoCs, designed specifically for use with security controls like iptables. By integrating Q-Feeds into your iptables, you can improve your devices’s protection against new and emerging threats. This means your linux host 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, so you can get the best security possible. You'll learn how to use the Q-Feeds installer, 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.

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 SonicWall:

Name	Type	Description	URI
Malware IP	IP	List of dangerous IP addresses	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 and may overload the system.

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 visiting our website at https://qfeeds.com/start-trial-license/.

With the trial token, you will receive 30 days of free and full access to all our indicators of compromise. If you need assistance, please contact your account manager or email us at sales@qfeeds.com.

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_ip&limit=XXXXX
```

Setup Q-Feeds

The **Q-Feeds Blocklist** is a security solution that provides the latest threat intelligence data to protect your system from malicious IP addresses associated with malware, botnets, and other cyber threats. This installer script automates the installation and configuration process, ensuring your system is up-to-date with the latest blocklists provided by Q-Feeds.

Note: Before using this software, you must accept the Terms & Conditions and End-User License Agreement (EULA) as published on https://qfeeds.com/terms.

Prerequisites

- **Operating System:** Linux
- **Supported Distributions:** Ubuntu, Debian, CentOS, RHEL, AlmaLinux, Rocky Linux, Fedora, openSUSE Leap, SLES, Arch Linux
- **Privileges:** Root access is required to run the installer script and configure system settings.
- **Network Access:** Ability to connect to https://api.qfeeds.com to fetch the blocklist data.
- **API Token:** A valid Q-Feeds API Token. Obtain one from your Q-Feeds account or contact Q-Feeds support.

Installation Steps

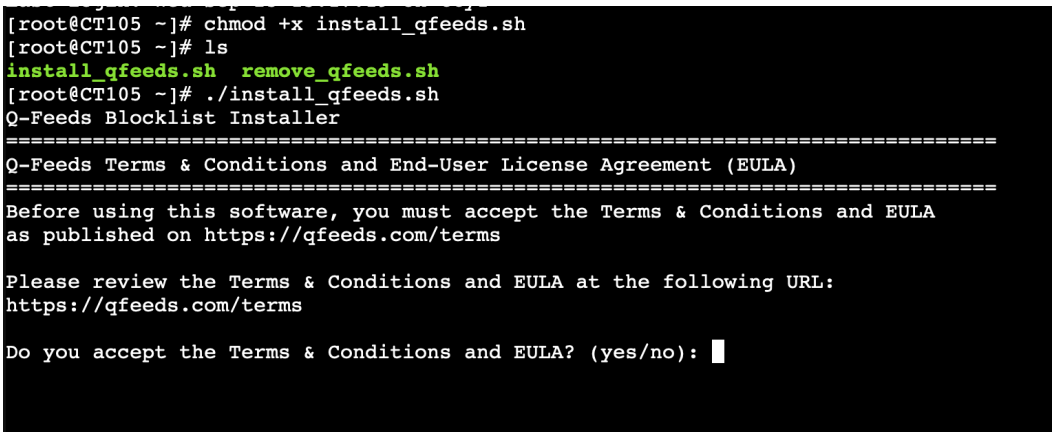
1. Download the Installer Script

First, download the install_qfeeds.sh installer script to your system.
You can obtain the script by contacting your distributor or Q-Feeds representative.

2. Run the Installer Script

Make the installer script executable and run it as the root user:

```
chmod +x install_qfeeds.sh
sudo ./install_qfeeds.sh
```



Important: The script must be run with root privileges to install dependencies and configure system settings.

3. Accept the Terms & Conditions and EULA

Upon running the script, you will be prompted to accept the Terms & Conditions and EULA. Type `**yes**` to accept and proceed with the installation.

4. Configure the Script

a. Enter Your Q-Feeds API Token

Input your API Token obtained from Q-Feeds.

```
Do you accept the Terms & Conditions and EULA? (yes/no): yes
Thank you for accepting the Terms & Conditions and EULA.
Detected Linux distribution: almalinux 9.4
Installing required packages...
Last metadata expiration check: 18:10:09 ago on Tue 24 Sep 2024 09:09:42 PM UTC.
Package iptables-nft-1.8.10-4.el9_4.x86_64 is already installed.
Package ipset-7.11-8.el9.x86_64 is already installed.
Package curl-7.76.1-29.el9_4.1.x86_64 is already installed.
Package util-linux-2.37.4-18.el9.x86_64 is already installed.
Dependencies resolved.
Nothing to do.
Complete!
Last metadata expiration check: 18:10:12 ago on Tue 24 Sep 2024 09:09:42 PM UTC.
Package iptables-services-1.8.10-2.2.el9.noarch is already installed.
Dependencies resolved.
Nothing to do.
Complete!
Dependencies installed.
Configuring Q-Feeds Blocklist Script...
Enter your Q-Feeds API Token:
```

b. Optional Settings

You can customize the following settings or press Enter to accept the defaults:
Feed Type: The type of threat intelligence feed you wish to use (default: malware_ip).
Limit: The maximum number of IP addresses to fetch (default: 130000).

c. Cron Job Schedule

Set how frequently the blocklist should be updated. (default: */20 * * * *)

```
Enter your Q-Feeds API Token: YOURTOKEN
Enter feed type [default: malware_ip]:
Enter the limit of IPs to fetch [default: 130000]:
Configuration file created at /etc/qfeeds/qfeeds_config.conf
Installing main script...
Main script installed at /usr/local/bin/update_qfeeds_blocklist.sh
Setting up cron job...
Enter cron schedule (e.g., '*/20 * * * *' for every 20 minutes) [default: */20 * * * *]:
```

5. Finalize Installation

The installer will install necessary dependencies, create configuration files, set up cron jobs, and run the main script once to verify installation.

Note: you might get a few warnings while pulling the feeds. This is due incompatibility with CIDR notations. You can ignore these.

```
2024-09-25 15:24:45 : Warning: Invalid IP format skipped - 194.165.16.72/31
2024-09-25 15:24:45 : Warning: Invalid IP format skipped - 194.26.135.26/31
2024-09-25 15:24:45 : Warning: Invalid IP format skipped - 62.204.41.8/31
2024-09-25 15:24:45 : Warning: Invalid IP format skipped - 62.204.41.44/31
2024-09-25 15:24:45 : Warning: Invalid IP format skipped - 196.92.1.190/31
2024-09-25 15:24:45 : Warning: Invalid IP format skipped - 141.98.11.194/31
2024-09-25 15:24:47 : ipset sets updated with latest IPs.
2024-09-25 15:24:47 : Configuring iptables to block IPs in qfeeds_blacklist_v4
2024-09-25 15:24:48 : Added iptables rule to drop traffic from qfeeds_blacklist_v4.
2024-09-25 15:24:48 : Configuring ip6tables to block IPs in qfeeds_blacklist_v6
2024-09-25 15:24:48 : Added ip6tables rule to drop traffic from qfeeds_blacklist_v6.
2024-09-25 15:24:48 : Note: Install netfilter-persistent to ensure iptables rules persist on reboot.
2024-09-25 15:24:48 : Q-Feeds blocklist update completed successfully.
2024-09-25 15:24:48 : Cleaned up temporary files.
Installation and initial run completed.
Q-Feeds Blocklist setup is complete!
[root@CT105 ~]#
```

Verification

1. Check the Blocklist Update

Verify that the blocklist has been fetched and ipset lists are populated by running the following commands:

```
sudo ipset list qfeeds_blacklist_v4
sudo ipset list qfeeds_blacklist_v6
```

2. Verify iptables Rules

```
sudo iptables -L INPUT -v -n | grep qfeeds_blacklist_v4
sudo ip6tables -L INPUT -v -n | grep qfeeds_blacklist_v6
```

3. Review Logs

```
sudo tail /var/log/qfeeds_blocklist.log
```

File and Directory Locations

- Configuration File: /etc/qfeeds/qfeeds_config.conf
- Log File: /var/log/qfeeds_blocklist.log
- Main Script Executable: /usr/local/bin/update_qfeeds_blocklist.sh
- Installer Script: /usr/local/bin/install_qfeeds.sh
- Lock File: /var/lock/qfeeds_blocklist.lock
- ipset Restore Rules: /etc/iptables/ipset.rules
- Systemd Service for ipset restore: /etc/systemd/system/ipset-restore.service
- Cron Job: Root's crontab

Uninstallation

To remove the Q-Feeds Blocklist from your system:
We provide a uninstaller script which will automatically remove the cron job, iptables rules etc.

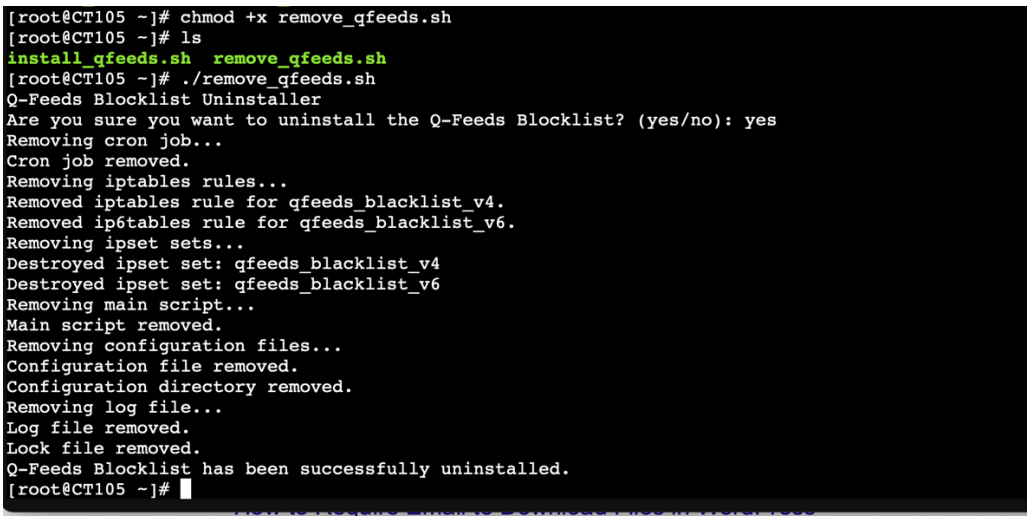
In order to delete make the “remove_qfeeds.sh” file executable:

```
Chmod +x remove_qfeeds.sh
```

Continue executing the script:

```
sudo ./remove_qfeeds.sh
```

Type **Yes** as confirmation. And let the script work its magic.



The script does not automatically remove its dependencies. If you want you can remove them with the following commands:

Ubuntu/Debian:

```
sudo apt-get -y remove iptables ipset netfilter-persistent flock
```

Centos/RHEL/Almalinux/Rocky

```
sudo yum -y remove iptables ipset
```

Fedora

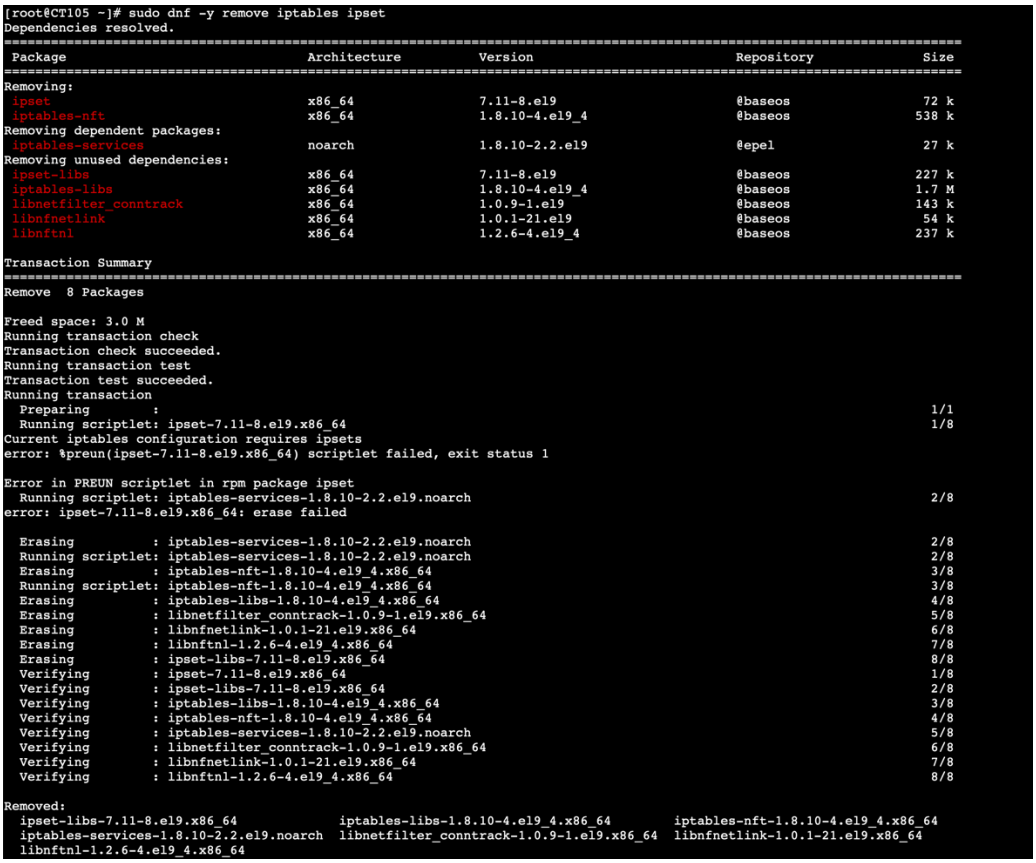
```
sudo dnf -y remove iptables ipset
```

Opensuse-leap/SLES

```
zipper remove iptables ipset
```

ARCH

```
pacman -Sy –noconfirm iptables ipset
```



```
[root@CT105 ~]# sudo dnf -y remove iptables ipset
Dependencies resolved.
================================================================================
 Package                 Architecture    Version                 Repository  Size
================================================================================
Removing:
 ipset                   x86_64          7.11-8.el9              @baseos     72 k
 iptables-nft            x86_64          1.8.10-4.el9_4          @baseos    538 k
Removing dependent packages:
 iptables-services       noarch          1.8.10-2.2.el9          @epel       27 k
Removing unused dependencies:
 ipset-libs              x86_64          7.11-8.el9              @baseos    227 k
 iptables-libs           x86_64          1.8.10-4.el9_4          @baseos    1.7 M
 libnetfilter_conntrack  x86_64          1.0.9-1.el9             @baseos    143 k
 libnfnetlink            x86_64          1.0.1-21.el9            @baseos     54 k
 libnftnl                x86_64          1.2.6-4.el9_4           @baseos    237 k

Transaction Summary
================================================================================
Remove  8 Packages

Freed space: 3.0 M
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing        :                                                        1/1
  Running scriptlet: ipset-7.11-8.el9.x86_64                                1/8
Current iptables configuration requires ipsets
error: %preun(ipset-7.11-8.el9.x86_64) scriptlet failed, exit status 1

Error in PREUN scriptlet in rpm package ipset
  Running scriptlet: iptables-services-1.8.10-2.2.el9.noarch                2/8
error: ipset-7.11-8.el9.x86_64: erase failed

  Erasing          : iptables-services-1.8.10-2.2.el9.noarch                2/8
  Running scriptlet: iptables-services-1.8.10-2.2.el9.noarch                2/8
  Erasing          : iptables-nft-1.8.10-4.el9_4.x86_64                     3/8
  Running scriptlet: iptables-nft-1.8.10-4.el9_4.x86_64                     3/8
  Erasing          : iptables-libs-1.8.10-4.el9_4.x86_64                    4/8
  Erasing          : libnetfilter_conntrack-1.0.9-1.el9.x86_64              5/8
  Erasing          : libnfnetlink-1.0.1-21.el9.x86_64                       6/8
  Erasing          : libnftnl-1.2.6-4.el9_4.x86_64                          7/8
  Erasing          : ipset-libs-7.11-8.el9.x86_64                           8/8
  Verifying        : ipset-7.11-8.el9.x86_64                                1/8
  Verifying        : ipset-libs-7.11-8.el9.x86_64                           2/8
  Verifying        : iptables-libs-1.8.10-4.el9_4.x86_64                    3/8
  Verifying        : iptables-nft-1.8.10-4.el9_4.x86_64                     4/8
  Verifying        : iptables-services-1.8.10-2.2.el9.noarch                5/8
  Verifying        : libnetfilter_conntrack-1.0.9-1.el9.x86_64              6/8
  Verifying        : libnfnetlink-1.0.1-21.el9.x86_64                       7/8
  Verifying        : libnftnl-1.2.6-4.el9_4.x86_64                          8/8

Removed:
  ipset-libs-7.11-8.el9.x86_64            iptables-libs-1.8.10-4.el9_4.x86_64        iptables-nft-1.8.10-4.el9_4.x86_64
  iptables-services-1.8.10-2.2.el9.noarch libnetfilter_conntrack-1.0.9-1.el9.x86_64  libnfnetlink-1.0.1-21.el9.x86_64
  libnftnl-1.2.6-4.el9_4.x86_64
```

Manual uninstallation

1. Remove iptables Rules:

```
sudo iptables -D INPUT -m set --match-set qfeeds_blacklist_v4 src -j DROP
sudo ip6tables -D INPUT -m set --match-set qfeeds_blacklist_v6 src -j DROP
```

2. Delete ipset Lists:

```
sudo ipset destroy qfeeds_blacklist_v4
sudo ipset destroy qfeeds_blacklist_v6
```

3. Remove Cron Job:

```
sudo crontab -e
```

4. Delete Files and Directories:

```
sudo rm -f /usr/local/bin/update_qfeeds_blocklist.sh
sudo rm -f /usr/local/bin/install_qfeeds.sh
sudo rm -f /var/log/qfeeds_blocklist.log
sudo rm -f /var/lock/qfeeds_blocklist.lock
sudo rm -rf /etc/qfeeds
```

Troubleshooting

1. Missing Dependencies: Ensure that iptables, ipset, curl, and other necessary dependencies are installed.

2. Blocklist Not Updating: Check the log file `s/var/log/qfeeds_blocklist.log` for errors.

Support

For any issues or further assistance, contact Q-Feeds support:
Email: support@qfeeds.com
Website: https://qfeeds.com/support
Documentation: https://qfeeds.com/docs