ipset

ipset (https://ipset.netfilter.org/) is a companion application for the **iptables** Linux **firewall**. It allows you to setup rules to quickly and easily block a set of IP addresses, among other things.

Related articles

Firewall

iptables

1 Installation

Install the **`ipset (https://archlinux.org/packages/?name=ipset)`** package.

2 Configuration

2.1 Blocking a list of networks

Start by creating a new "set" of network addresses. This creates a new "hash" set of "net" network addresses named "myset".

```
# ipset create myset hash:net
```

or

```
# ipset -N myset nethash
```

Add any IP address that you would like to block to the set.

```
# ipset add myset 14.144.0.0/12
# ipset add myset 27.8.0.0/13
# ipset add myset 58.16.0.0/15
# ipset add myset 1.1.1.0/24
```

Finally, configure **iptables** to block any address in that set. This command will add a rule to the top of the "INPUT" chain to "-m" match the set named "myset" from ipset (--match-set) when it is a "src" packet and "DROP", or block, it.

```
# iptables -I INPUT -m set --match-set myset src -j DROP
```

2.2 Blocking a list of IP addresses

Start by creating a new "set" of ip addresses. This creates a new "hash" set of "ip" addresses named "myset-ip".

```
# ipset create myset-ip hash:ip
```

or

```
# ipset -N myset-ip iphash
```

Add any IP address that you would like to block to the set.

```
# ipset add myset-ip 1.1.1.1
# ipset add myset-ip 2.2.2.2
```

Finally, configure **iptables** to block any address in that set.

```
# iptables -I INPUT -m set --match-set myset-ip src -j DROP
```

2.3 Making ipset persistent

The ipset you have created is stored in memory and will be gone after reboot. To make the ipset persistent you have to do the followings:

First, save the ipset to `/etc/ipset.conf`:

```
# ipset save > /etc/ipset.conf
```

Then **enable** `ipset.service`, which works similarly to `iptables.service` for restoring **iptables rules**.

Warning: A (rare) bug **FS#79674 (https://bugs.archlinux.org/task/79674)** has been observed once which resulted in `iptables.service` failing due to missing ipsets despite `ipset.service` succeeding. Use redundant security and consider a monitoring script if you need 100% assurance that your firewall is intact.

2.4 Blocking with PeerGuardian and other blocklists

The **`pg2ipset-git` (https://aur.archlinux.org/packages/pg2ipset-git/)**[AUR] tool by the author of Maeyanie.com, coupled with the **ipset-update.sh (https://github.com/ilikenwf/pg2ipset/blob/master/ipset-update.sh)** script, can be used with cron to automatically update various blocklists. Currently, by default, blocking of: country, tor exit node and Bluetrack pg2 list are implemented.

3 Other commands

To view the sets:

```
# ipset list
```

or

```
# ipset -L
```

To delete a set:

```
# ipset destroy myset
```

or

```
# ipset -X myset
```

To delete all sets:

```
# ipset destroy
```

Please see the **ipset(8) (https://man.archlinux.org/man/ipset.8)** for further information.

4 Optimization

The **iprange (https://aur.archlinux.org/packages/iprange/)**[AUR] tool can help to reduce entries in ipset.conf by merging adjacent ranges or eliminating overlapped ranges. This can improve the router/firewall performance if the table size is huge. This tool can also convert a list of hostnames to IPs.

Although ipset is designed to be able to scale well, that does not mean infinitely. In particular, some nations have very large IP address spaces, which will cause geoblocking to be inefficient.