davydany / **IPTABLES-CHEATSHEET.md**

IP Tables (iptables) Cheat Sheet

IPTABLES-CHEATSHEET.md

IP Tables (iptables) Cheat Sheet

IPTables is the Firewall service that is available in a lot of different Linux Distributions. While modifiying it might seem daunting at first, this Cheat Sheet should be able to show you just how easy it is to use and how quickly you can be on your way mucking around with your firewall.

Resources

The following list is a great set of documentation for `iptables`. I used them to compile this documentation.

- **How-To Geek: The Beginner's Guide to iptables, the Linux Firewall**: https://www.howtogeek.com/177621/the-beginners-guide-to-iptables-the-linux-firewall/
- **IPTables Essentials: Common Firewall Rules and COmmands** https://www.digitalocean.com/community/tutorials/iptables-essentials-common-firewall-rules-and-commands
- **List and Delete `iptable` rules:** https://www.digitalocean.com/community/tutorials/how-to-list-and-delete-iptables-firewall-rules

The Theory

NOTE: The commands below must be run as the root user or user with privileges to access `iptables`.

There are 3 CHAINS. These are INPUT, FORWARD and OUTPUT.

- **INPUT** - Used to control the behavior of INCOMING connections.
- **FORWARD** - Used to control the behavior of connections that aren't delivered locally but sent immediately out. (i.e.: router)
- **OUTPUT** - Used to control the behavior of OUTGOING connections.

NOTE: A lot of connections might require inbound and outbound rules, so bear that in mind while making changes to the firewall.

Before we determine the individual rules for each of the chain, we need to determine the default policy for each chain. This can be shown by typing:

```
sudo iptables -L | grep policy
```

Change the default policy for a Chain

To change the default policy of a chain, run: `iptables --policy <ACCEPT/DROP>

If we want to ACCEPT all connections (on all Chains), run the following:

```
iptables --policy INPUT ACCEPT
iptables --policy OUTPUT ACCEPT
iptables --policy FORWARD ACCEPT
```

If we want to DROP all connections (on all chains), run the following:

```
iptables --policy INPUT DROP
iptables --policy OUTPUT DROP
iptables --policy FORWARD DROP
```

Actions: ACCEPT vs DROP vs REJECT

- **ACCEPT**: Allow the connection
- **DROP**: Drop the connection (as if no connection was ever made; Useful if you want the system to 'disappear' on the network)

- **REJECT**: Don't allow the connection but send an error back.

The Commands (Examples)

List Entries in `iptables`

```
$ iptables -L
```

Set Default Policy for INPUT to ACCEPT

```
iptables --policy INPUT ACCEPT
```

Set Default Policy for OUTPUT to DROP

```
iptables --policy OUTPUT DROP
```

Set Default Policy for FORWARD to REJECT

```
iptables --policy FORWARD REJECT
```

ACCEPT Connections From a Single IP Address

```
$ iptables -A INPUT -s 10.10.10.10 -j ACCEPT

# Explanation:
# ACCEPTS all INCOMING Connections from 10.10.10.10.
# -A <CHAIN>  : Append a Rule to the chain that is specified (INPUT in this
scenario)
# -s <SOURCE> : Source - The Source IP of the connection (10.10.10.10)
# -j <ACTION> : (jump) - Defines what to do when the Packet matches this rule. We
can either ACCEPT, DROP or REJECT it. (ACCEPT)
```

DROP Connections for an IP Range

```
$ iptables -A INPUT -s 10.10.10.0/24 -j DROP

# Explanation:
# BLOCKS all INCOMING connections from 10.10.10.0 to 10.10.10.255
# -A <CHAIN>  : Append a Rule to the chain that is specified (INPUT in this
```

```
scenario)
# -s <SOURCE> : Source - The Source IP of the connection (10.10.10.0 to
10.10.10.255)
# -j <ACTION> : (jump) - Defines what to do when the Packet matches this rule. We
can either ACCEPT, DROP or REJECT it. (DROP)
```

REJECT OUTBOUND Connections for an IP on a Specific Port (SSH)

```
$ iptables -A OUTPUT -p tcp --dport ssh -s 10.10.10.10 -j REJECT

# Explanation:
# REJECTs all OUTPUT connections to 10.10.10.10 on TCP Port
# -A <CHAIN>  : Append a Rule to the chain that is specified (OUTPUT in this
scenario)
# -s <SOURCE> : Source - The Source IP of the connection (10.10.10.10)
# -j <ACTION> : (jump) - Defines what to do when the Packet matches this rule. We
can either ACCEPT, DROP or REJECT it. (REJECT)
```

DROP All OUTGOING Connections; ALLOW only CONNECTIONS to 192.168.1.1

```
$ iptables --policy OUTPUT DROP
# Explanation:
# DROP all OUTPUT connections.

$ iptables -A OUTPUT -d 192.168.1.1 -j ACCEPT
# Explanation:
# Allow connections to the destination port 192.168.1.1
```

Saving Changes Made to `iptables`

The changes you made to your iptables rules will not be saved unless it is called explicitly to be saved. The next time the service starts, any unsaved changes will be wiped away. The following are examples on how to save on different platforms

Ubuntu: `sudo /sbin/iptables-save`

RedHat / Centos: `/sbin/service iptables save`

Others: `/etc/init.d/iptables save`

**Clearing All the Rules*

To clear all the rules that are configured, you can flush it with the *Flush* command.

```
iptables -F
```

Deleting Individual Rules

You can delete rules based on what they're doing:

```
iptables -D INPUT -s 127.0.0.1 -p tcp -dport 111 -j ACCEPT
# Explanation
# -D <CHAIN>    : The Rule to delete (INPUT -s 127.0.0.1 -p tcp -dport 111 -j
ACCEPT)
# -s <SOURCE>   : Source - The Source IP of the connection (127.0.0.1)
# -p <protocol> : Protocol - THe protocol of the rule or of the packet to check
# --dport <port>: Destination Port: The Destination port or port range
specification
# -j <ACTION>   : (jump) - Defines what to do when the Packet matches this rule.
We can either ACCEPT, DROP or REJECT it. (REJECT)
```

You can also delete base don the rule number:

```
iptables -D INPUT 4
```

Universal155 commented on Sep 12, 2019

commit:
Set Default Policy for FORWARD to REJECT

iptables --policy FORWARD REJECT

davydany commented on Sep 12, 2019 Author

> commit:
> **Set Default Policy for FORWARD to REJECT**
>
> iptables --policy FORWARD REJECT

Thank you **@Universal155** ... Good eye! Fixed now.

domdom82 commented on May 26, 2020

```
  You can also delete base don the rule number:
```

typo `base don`
fix:

```
  You can also delete based on the rule number:
```

upsangel commented on Jan 12

Thank you! It will be great if it covers NAT and stateful firewall rule~