**Zack Pelka**

Configure iptables to Allow Access to Common Services on Linux

|  |  |
| --- | --- |
| Prepared By: | Zachary Pelka |
| Document Version: | 1.1 |
| Last Updated On: | 29NOV2020 |
| Document Classification: | Public Domain |

The information in the document may contain proprietary and confidential information that is intended for the employees of ZP Enterprises only. If you are not an employee of ZP Enterprises, you are hereby notified that any disclosure, copying, distribution, retention or use of the contents of this information is prohibited in an altered form. This is for public use without modification.

## **Purpose**

This article gives the steps to open firewall ports on CentOS 6.x in Iptables IPv4.

## **Basics**

* Iptables rules can be changed on the fly by using the **iptables** binary.
* The rules that are set using iptables command are in memory only and will vanish when the daemon is restarted.
* The firewall rules added on the fly can be saved to the configuration file easily in CentOS/RHEL with the command **service iptables save**
  + This is no need to edit the configuration file unless you really want to.
* The following examples are aimed at hardening the inbound traffic, but allowing all outbound traffic.
  + You can completely lock down all inbound, outbound and forwarded traffic if needed. It generally just causes a lot more administration and usually isn't necessary.

## **Basic Commands**

* **iptables --flush** delete all firewall rules from memory.
* **iptables --list** List current firewall policies
* **service iptables save** (CentOS/RHEL) save current rules in memory to configuration file (/etc/sysconfig/iptables)
* **service iptables restart** restart iptables daemon and load firewall rules from configuration file.
* **iptables-save > /root/firwallrules.fw** save firewall rules in memory to a specific configuration file.
* **iptables-restore > /root/firwallrules.fw** restore firewall rules from a specific configuration file to memory.

## **Basic iptables Command Parameters**

* **-A** append to policy chain
* **INPUT | OUTPUT | FORWARD** policy chain identifiers
* **-p** protocol
* **-m** match
* **-s** source
* **--dport** destination port
* **--state** connection state
* **-j** jump target **ACCEPT | DROP**

## **Backup Current Iptables Configuration to File**

Before you begin, it is recommended to backup your current firewall rules.

iptables-save > /path/to/somewhere/filename

**Example:**

iptables-save > /home/user1/iptable-rules-25NOV2020.fw

## **Remove All Current Rules**

iptables --flush

## **Set Policy Chains Default Rule**

iptables -P INPUT DROP

iptables -P OUTPUT ACCEPT

iptables -P FORWARD ACCEPT

## **Allow Loopback**

iptables -A INPUT -i lo -j ACCEPT

## **Allow All Established and Related Connections**

iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT

## **Allow ICMP "ping" from LAN (TCP Port 22)**

iptables -A INPUT -p icmp -m icmp -s 192.168.0.0/24 --icmp-type echo-request -j ACCEPT

## **Allow SSH from LAN (TCP Port 22)**

iptables -A INPUT -p tcp -m tcp -s 192.168.0.0/24 --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT

## **Allow RSYNC from LAN (TCP Port 873)**

iptables -A INPUT -p tcp -m tcp -s 192.168.0.0/24 --dport 873 -m state --state NEW,ESTABLISHED -j ACCEPT

## **Allow HTTP (TCP Port 80)**

iptables -A INPUT -p tcp -m tcp --dport 80 -m state --state NEW,ESTABLISHED -j ACCEPT

## **Allow HTTPS (TCP Port 443)**

iptables -A INPUT -p tcp -m tcp --dport 443 -m state --state NEW,ESTABLISHED -j ACCEPT

## **Allow MySQL Server Access from LAN (TCP Port 3306)**

iptables -A INPUT -p tcp -m tcp -s 192.168.0.0/24 --dport 3306 -m state --state NEW,ESTABLISHED -j ACCEPT

## **Allow Nagios NRPE Client Access from Nagios Server (TCP Port 5666)**

iptables -A INPUT -s <NAGIOSSERVERIP> -p tcp -m tcp --dport 5666 -m state --state NEW,ESTABLISHED -j ACCEPT

## **Allow VNC Inbound Access**

VNC server listens on the following TCP ports:

=> VNC server on display 0 will listen on TCP ports 5800, 5900 and 6000

=> VNC server on display 1 will listen on TCP ports 5801, 5901 and 6001  
=> VNC server on display N will listen on TCP ports 580N, 590N and 600N

In other words, a VNC server listens for a VNC client on TCP ports 5800+N, 5900+N, and 6000+N where N is the display which starts at zero. So,

5800+N – Java-based vncviewer;

5900+N – VNC Client Port;

6000+N – X Server port.

Your Milage may vary, 0 is usually console, so probably only allow on display 1, 2, etc.

iptables -A INPUT -m state –-state NEW -m tcp -p tcp –dport 5801 -j ACCPET

iptables -A INPUT -m state –-state NEW -m tcp -p tcp –dport 5901 -j ACCPET

iptables -A INPUT -m state –-state NEW -m tcp -p tcp –dport 6001 -j ACCPET

## **Prevent a Denial of Service Attack**

*## Prevent HTTP DoS Attack*

*#> -m limit: This uses the limit iptables extension*

*#> --limit 25/minute: This limits only maximum of 25 connection per minute. Change this value based on your specific requirement*

*#> --limit-burst 100: This value indicates that the limit/minute will be enforced only after the total number of connection have reached the limit-burst level.*

iptables -A INPUT -p tcp --dport 80 -m limit --limit 25/minute --limit-burst 100 -j ACCEPT

## **Save Current Rules in Memory to Configuration File**

service iptables save

## **Restart Service**

service iptables restart

## **Script**

I create a BASH script to rewrite the firewall rules how I prefer. Then run the script and test. If everything tests good, then I save the configuration.

**Assumes all commands are executed with suitable privilege**

**Example:**

*#!/bin/sh*

*# Delete All Existing Rules for a fresh start, but you might want to backup the existing rules to be safe.*

*# Backup first*

Iptables-save >/some.file

iptables --flush

*# Set Default Chain Policies*

iptables -P INPUT DROP

iptables -P OUTPUT ACCEPT

iptables -P FORWARD ACCEPT

*## Allow Loopback*

iptables -A INPUT -i lo -j ACCEPT

*## Allow Established and Related Connections*

iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

*## Allow SSH (From LAN)*

iptables -A INPUT -s 192.168.0.0/24 -p tcp -m tcp --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT

*## Allow ICMP "ping" (From LAN)*

iptables -A INPUT -s 192.168.0.0/24 -p icmp -m icmp --icmp-type echo-request -j ACCEPT

*## Allow RSYNC (From LAN)*

iptables -A INPUT -s 192.168.0.0/24 -p tcp -m tcp --dport 873 -m state --state NEW,ESTABLISHED -j ACCEPT

*## Allow HTTP*

iptables -A INPUT -p tcp -m tcp --dport 80 -m state --state NEW,ESTABLISHED -j ACCEPT

*## Allow HTTPS*

iptables -A INPUT -p tcp -m tcp --dport 443 -m state --state NEW,ESTABLISHED -j ACCEPT

*## Allow MySQL (From LAN)*

iptables -A INPUT -s 192.168.0.0/24 -p tcp -m tcp --dport 3306 -m state --state NEW,ESTABLISHED -j ACCEPT

*## Allow NRPE Client Access (From Nagios Server)*

iptables -A INPUT -s <NAGIOSSERVERIP> -p tcp -m tcp --dport 5666 -m state --state NEW,ESTABLISHED -j ACCEPT

*## Allow VNC Access*

iptables -A INPUT -m state –-state NEW -m tcp -p tcp –dport 5801 -j ACCPET

iptables -A INPUT -m state –-state NEW -m tcp -p tcp –dport 5901 -j ACCPET

iptables -A INPUT -m state –-state NEW -m tcp -p tcp –dport 6001 -j ACCPET

*## Prevent HTTP DoS Attack*

*#> -m limit: This uses the limit iptables extension*

*#> --limit 25/minute: This limits only maximum of 25 connection per minute. Change this value based on your specific requirement*

*#> --limit-burst 100: This value indicates that the limit/minute will be enforced only after the total number of connection have reached the limit-burst level.*

iptables -A INPUT -p tcp --dport 80 -m limit --limit 25/minute --limit-burst 100 -j ACCEPT

## **Restore Iptables Rules from Backup File**

If you made a backup file or pulling a copy of rules from another system and wish to restore/replace the rules then use the following command.

iptables-restore < /path/to/somewhere/filename

**Example:**

iptables-restore < /home/user1/iptable-rules-25NOV2020.fw

## **Save IP tables**

service iptables save

## **Restart Service**

service iptables restart

## **Sources**

* <http://www.thegeekstuff.com/2011/06/iptables-rules-examples/>
* <http://www.cyberciti.biz/tips/linux-iptables-how-to-specify-a-range-of-ip-addresses-or-ports.html>

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **By** | **Changes** |
| **1.0** | 25NOV2020 | Zachary Pelka | Initial Draft |
| **1.1** | 29NOV2020 | Zachary Pelka | Typo Corrections + VNC rules |
|  |  |  |  |