RHCSA 系列（十一）：使用 firewalld 和 iptables 来控制网络流量

2015-9-29 10:11 收藏: 8

原文：http://www.tecmint.com/firewalld-vs-iptables-and-control-network-traffic-in-firewall/
译文：LCTT https://linux.cn/article-6315-1.html

作者： Gabriel Cánepa
译者： FSSlc

简单来说，防火墙就是一个基于一系列预先定义的规则（例如流量包的目的地或来源，流量的类型等）的安全系统，它控制着一个网络中的流入和流出流量。

RHCSA: 使用 FirewallD 和 Iptables 来控制网络流量 – Part 11

在本文中，我们将回顾 firewalld 和 iptables 的基础知识。前者是 RHEL 7 中的默认动态防火墙守护进程，而后者则是针对 Linux 的传统的防火墙服务，大多数的系统和网络管理员都非常熟悉它，并且在 RHEL 7 中也可以用。

FirewallD 和 Iptables 的一个比较

在后台， firewalld 和 iptables 服务都通过相同的接口来与内核中的 netfilter 框架相交流，这不足为奇，即它们都通过 iptables 命令来与 netfilter 交互。然而，与 iptables 服务相反， firewalld 可以在不丢失现有连接的情况下，在正常的系统操作期间更改设定。

在默认情况下， firewalld 应该已经安装在你的 RHEL 系统中了，尽管它可能没有在运行。你可以使用下面的命令来确认（firewall-config 是用户界面配置工具）：

```
# yum info firewalld firewall-config
```

检查 FirewallD 的信息

以及，

```
# systemctl status -l firewalld.service
```

检查 FirewallD 的状态

另一方面， iptables 服务在默认情况下没有被包含在 RHEL 系统中，但可以被安装上。

```
# yum update && yum install iptables-services
```

这两个守护进程都可以使用常规的 systemd 命令来在开机时被启动和开启：

```
# systemctl start firewalld.service | iptables-service.service
# systemctl enable firewalld.service | iptables-service.service
```

另外，请阅读：管理 Systemd 服务的实用命令 <https://linux.cn/article-5926-1.html>

至于配置文件， iptables 服务使用 `/etc/sysconfig/iptables` 文件（假如这个软件包在你的系统中没有被安装，则这个文件将不存在）。在一个被用作集群节点的 RHEL 7 机子上，这个文件看起来是这样：

Iptables 防火墙配置文件

而 firewalld 则在两个目录中存储它的配置文件，即 `/usr/lib/firewalld` 和 `/etc/firewalld` ：

```
# ls /usr/lib/firewalld /etc/firewalld
```

FirewallD 的配置文件

在这篇文章中后面，我们将进一步查看这些配置文件，在那之后，我们将在这两个地方添加一些规则。现在，是时候提醒你了，你总可以使用下面的命令来找到更多有关这两个工具的信息。

```
# man firewalld.conf
# man firewall-cmd
# man iptables
```

除了这些，记得查看一下当前系列的第一篇 RHCSA 系列（一）：回顾基础命令及系统文档 <https://linux.cn/article-6133-1.html>，在其中我描述了几种渠道来得到安装在你的 RHEL 7 系统上的软件包的信息。

使用 Iptables 来控制网络流量

在进一步深入之前，或许你需要参考 Linux 基金会认证工程师（Linux Foundation Certified Engineer,LFCE） 系列中的 配置 Iptables 防火墙 – Part 8 <http://www.tecmint.com/configure-iptables-firewall/> 来复习你脑中有关 iptables 的知识。

例 1：同时允许流入和流出的网络流量

TCP 端口 80 和 443 是 Apache web 服务器使用的用来处理常规（HTTP）和安全（HTTPS）网络流量的默认端口。你可以像下面这样在 enp0s3 接口上允许流入和流出网络流量通过这两个端口：

```
# iptables -A INPUT -i enp0s3 -p tcp --dport 80 -m state --state NEW,ESTABLISHED -j ACCEPT
# iptables -A OUTPUT -o enp0s3 -p tcp --sport 80 -m state --state ESTABLISHED -j ACCEPT
# iptables -A INPUT -i enp0s3 -p tcp --dport 443 -m state --state NEW,ESTABLISHED -j ACCEPT
# iptables -A OUTPUT -o enp0s3 -p tcp --sport 443 -m state --state ESTABLISHED -j ACCEPT
```

例 2：从某个特定网络中阻挡所有（或某些）流入连接

或许有时你需要阻挡来自于某个特定网络的所有（或某些）类型的来源流量，比方说 192.168.1.0/24：

```
# iptables -I INPUT -s 192.168.1.0/24 -j DROP
```

上面的命令将丢掉所有来自 192.168.1.0/24 网络的网络包，而

```
# iptables -A INPUT -s 192.168.1.0/24 --dport 22 -j ACCEPT
```

将只允许通过端口 22 的流入流量。

例 3：将流入流量重定向到另一个目的地

假如你不仅使用你的 RHEL 7 机子来作为一个软件防火墙，而且还将它作为一个硬件防火墙，使得它位于两个不同的网络之间，那么在你的系统上 IP 转发一定已经被开启了。假如没有开启，你需要编辑 `/etc/sysctl.conf` 文件并将 `net.ipv4.ip_forward` 的值设为 1，即：

```
net.ipv4.ip_forward = 1
```

接着保存更改，关闭你的文本编辑器，并最终运行下面的命令来应用更改：

```
# sysctl -p /etc/sysctl.conf
```

例如，你可能在一个内部的机子上安装了一个打印机，它的 IP 地址为 192.168.0.10，CUPS 服务在端口 631 上进行监听（同时在你的打印服务器和你的防火墙上）。为了从防火墙另一边的客户端传递打印请求，你应该添加下面的 iptables 规则：

```
# iptables -t nat -A PREROUTING -i enp0s3 -p tcp --dport 631 -j DNAT --to 192.168.0.10:631
```

请记住 iptables 会逐条地读取它的规则，所以请确保默认的策略或后面的规则不会重载上面例子中那些规则。

FirewallD 入门

firewalld 引入的一个变化是区域（zone）（注：翻译参考了 https://fedoraproject.org/wiki/FirewallD/zh-cn <https://fedoraproject.org/wiki/FirewallD/zh-cn> ）。这个概念允许将网路划分为拥有不同信任级别的区域，由用户决定将设备和流量放置到哪个区域。

要获取活动的区域，使用：

```
# firewall-cmd --get-active-zones
```

在下面的例子中，public 区域是激活的，并且 enp0s3 接口被自动地分配到了这个区域。要查看有关一个特定区域的所有信息，可使用：

```
# firewall-cmd --zone=public --list-all
```

列出所有的 Firewalld 区域

由于你可以在 RHEL 7 安全指南 <https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Security_Guide/sec-Using_Firewalls.html> 中阅读到更多有关区域的知识，这里我们将仅列出一些特别的例子。

例 4：允许服务通过防火墙

要获取受支持的服务的列表，可以使用：

```
# firewall-cmd --get-services
```

列出所有受支持的服务

要立刻生效且在随后重启后都可以让 http 和 https 网络流量通过防火墙，可以这样：

```
# firewall-cmd --zone=MyZone --add-service=http
# firewall-cmd --zone=MyZone --permanent --add-service=http
# firewall-cmd --zone=MyZone --add-service=https
# firewall-cmd --zone=MyZone --permanent --add-service=https
# firewall-cmd --reload
```

假如 `--zone` 被忽略，则使用默认的区域（你可以使用 `firewall-cmd –get-default-zone` 来查看）。

若要移除这些规则，可以在上面的命令中将 `add` 替换为 `remove` 。

例 5：IP 转发或端口转发

首先，你需要查看在目标区域中，伪装（masquerading）是否被开启：

```
# firewall-cmd --zone=MyZone --query-masquerade
```

在下面的图片中，我们可以看到对于外部区域，伪装已被开启，但对于公用区域则没有：

查看伪装状态

你可以为公共区域开启伪装：

```
# firewall-cmd --zone=public --add-masquerade
```

或者在外部区域中使用伪装。下面是使用 firewalld 来重复例 3 中的任务所需的命令：

```
# firewall-cmd --zone=external --add-forward-
  port=port=631:proto=tcp:toport=631:toaddr=192.168.0.10
```

不要忘了重新加载防火墙。

在 RHCSA 系列的 第九部分 <https://linux.cn/article-6286-1.html> 你可以找到更深入的例子，在那篇文章中我们解释了如何允许或禁用通常被 web 服务器和 ftp 服务器使用的端口，以及在针对这两个服务所使用的默认端口被改变时，如何更改相应的规则。另外，你或许想参考 firewalld 的 wiki 来查看更深入的例子。

- 延伸阅读：在 RHEL 7 中配置防火墙的几个实用的 firewalld 例子 <http://www.tecmint.com/firewalld-rules-for-centos-7/>

总结

在这篇文章中，我们已经解释了防火墙是什么，介绍了在 RHEL 7 中用来实现防火墙的几个可用的服务，并提供了可以帮助你入门防火墙的几个例子。假如你有任何的评论，建议或问题，请随意使用下面的评论框来让我们知晓。这里就事先感谢了！

---

via: http://www.tecmint.com/firewalld-vs-iptables-and-control-network-traffic-in-firewall/ <http://www.tecmint.com/firewalld-vs-iptables-and-control-network-traffic-in-firewall/>

作者：Gabriel Cánepa <http://www.tecmint.com/author/gacanepa/> 译者：FSSlc <https://github.com/FSSlc> 校对：wxy <https://github.com/wxy>

本文由 LCTT <https://github.com/LCTT/TranslateProject> 原创翻译，Linux中国 <file:///root/github/my-notes/Manual/Linux.cn/RHCSA/RHCSA%E7%B3%BB%E5%88%9711%E4%BD%BF%E7%94%A8%20firewalld%20%E5%92%8C.html> 荣誉推出

原文：http://www.tecmint.com/firewalld-vs-iptables-and-control-network-traffic-in-firewall/

<http://www.tecmint.com/firewalld-vs-iptables-and-control-network-traffic-in-firewall/>

作者： Gabriel Cánepa

译文：LCTT <http://lctt.github.io/> https://linux.cn/article-6315-1.html <https://linux.cn/article-6315-1.html> 译者： FSSlc

发表评论

评论

本文导航

- FirewallD 和 Iptables 的一个比较
- 使用 Iptables 来控制网络流量
  - 例 1：同时允许流入和流出的网络流量
  - 例 2：从某个特定网络中阻挡所有（或某些）流入连接
  - 例 3：将流入流量重定向到另一个目的地
- FirewallD 入门
  - 例 4：允许服务通过防火墙
  - 例 5：IP 转发或端口转发

相关阅读

RHCSA

- RHCSA 系列（十）：Yum 包管理、Cron 自动任务计划和监控系统日志 2015-9-26
- RHCSA 系列（十二）：使用 Kickstart 完成 RHEL 7 的自动化安装 2015-10-2
- RHCSA 系列（七）：使用 ACL（访问控制列表）和挂载 Samba/NFS 共享 2015-9-22
- RHCSA 系列（八）：加固 SSH，设定主机名及启用网络服务 2015-9-23
- RHCSA 系列（九）：安装、配置及加固一个 Web 和 FTP 服务器 2015-9-24
- RHCSA 系列（十三）： 在 RHEL 7 中使用 SELinux 进行强制访问控制 2015-10-3