

Re: Firewall: iptables rules for ssh, web, e-mail and DNS

Source: <http://linux.derkeiler.com/Mailing-Lists/RedHat/2003-12/0127.html>

From: Benjamin J. Weiss (*benjamin_at_weiss.name*)

Date: 12/02/03

To: <redhat-list@redhat.com>

Date: Tue, 2 Dec 2003 09:26:40 -0600

> *Hello:*

>

> *I'm trying to configure iptables (on RH 9) with a restrictive set of rules,*

> *to leave open only ssh, http, pop3 / imap, smtp and DNS ports and close all*

> *the rest.*

```
[root@mail root]# cat /etc/sysconfig/iptables
# Firewall configuration written by lokkit
# Manual customization of this file is not recommended.
# Note: ifup-post will punch the current nameservers through the
# firewall; such entries will *not* be listed here.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:RH-Lokkit-0-50-INPUT - [0:0]
-A INPUT -j RH-Lokkit-0-50-INPUT
-A RH-Lokkit-0-50-INPUT -p tcp -m tcp --dport 22 --syn -j ACCEPT
-A RH-Lokkit-0-50-INPUT -p tcp -m tcp --dport 25 --syn -j ACCEPT
-A RH-Lokkit-0-50-INPUT -p tcp -m tcp --dport 53 --syn -j ACCEPT
-A RH-Lokkit-0-50-INPUT -p udp -m udp --sport 53 -j ACCEPT
-A RH-Lokkit-0-50-INPUT -p tcp -m tcp --dport 80 --syn -j ACCEPT
-A RH-Lokkit-0-50-INPUT -p tcp -m tcp --dport 443 --syn -j ACCEPT
-A RH-Lokkit-0-50-INPUT -p tcp -m tcp --dport 993 --syn -j ACCEPT
-A RH-Lokkit-0-50-INPUT -i lo -j ACCEPT
-A RH-Lokkit-0-50-INPUT -p tcp -m tcp --syn -j REJECT
-A RH-Lokkit-0-50-INPUT -p udp -m udp -j REJECT
COMMIT
```

--

redhat-list mailing list

unsubscribe <mailto:redhat-list-request@redhat.com?subject=unsubscribe>

<https://www.redhat.com/mailman/listinfo/redhat-list>