Firewall Rules For Virtual Mail Server

This page is supplemental to main article: Creating a Virtual Mail Server with Postfix, Dovecot and MySQL

A firewall is simply a set of kernel routing rules, iptables rules, that selectively block or allow network traffic into and out of your machine. A web facing email server must be secured by a suitable set of firewall rules or it will quickly be overwhelmed and compromised!

If you already have a firewall in place for other services then you will need to add to it the rules necessary to support mail server traffic. If you do not have a firewall currently in place, then you may use the example below as a good starting point!

Loading *only* the rules below as your firewall will close other access that may be important to you such as http and ssh! You should first use iptables -L to check for pre-existing rules and merge those below into your existing firewall. If you have no existing firewall and/or need to allow http and ssh, uncomment the –policy lines and those for http and ssh as necessary to meet your requirements.

Following is a **minimal** set of iptables rules to provide a firewall for your email server. While

```
#--policy INPUT DROP
#--policy FORWARD DROP
#--policy OUTPUT ACCEPT

-A INPUT -m state --state INVALID -j DROP
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

# Postfix SMTP, SMTPS, SUBMISSION
-A INPUT -p tcp --dport 25 -m state --state NEW -j ACCEPT
-A INPUT -p tcp --dport 465 -m state --state NEW -j ACCEPT
-A INPUT -p tcp --dport 587 -m state --state NEW -j ACCEPT

# Imap and ImapS
#-A INPUT -p tcp --dport 143 -m state --state NEW -j ACCEPT
-A INPUT -p tcp --dport 993 -m state --state NEW -j ACCEPT

# Pop3 and Pop3S
#-A INPUT -p tcp --dport 110 -m state --state NEW -j ACCEPT
-A INPUT -p tcp --dport 995 -m state --state NEW -j ACCEPT

#  Allow HTTP and HTTPS connections from anywhere on normal ports
#-A INPUT -p tcp --dport 80 -j ACCEPT
#-A INPUT -p tcp --dport 443 -j ACCEPT

#  Allow SSH connections on normal port 22
#-A INPUT -p tcp -m state --state NEW --dport 22 -j ACCEPT
```

```
#  Respond to ping requests
#-A INPUT -p icmp --icmp-type echo-request -j ACCEPT

#  Drop all other inbound
-A INPUT -j DROP
```

Port 25, SMTP, must be enabled in order to accept incoming email for delivery to your virtual mail boxes.

Port 465, SMTPS, must be enabled for secure SMTP connections.

Port 587, SUBMISSION, is used by Mail User Agents (MUAs) such as Thunderbird to allow submission of outgoing email from your virtual users.

Ports 143 and 110 provide plain text Imap and POP3 connections, rescpectively. It is probably best not to use these and to force all Imap and Pop3 connections to be secure, as we will do in this article. If not used it is best to comment them out of your iptables rules as is shown here.

Ports 993 and 995 provide secure Imap and Pop3, respectively. These must be open in order for your virtual users to be able to send and receive email.

To install these rules as your firewall save them to a text file using

```
iptables-save >/etc/firewall.rules
```

then load that file using iptables-restore as shown below. This will replace any currently existing iptables rules with those in the file.

There are many preferences for saving and loading firewall scripts. I generally use /etc/firewall.rules for my own systems and will use that for this example.

```
iptables-restore </etc/firewall.rules
```

To see all currently active rules:

```
iptables -L
```

To flush all current rules:

```
iptables -F
```

To load your firewall rules at each boot, you will need to create a start script and save it to /etc/rc.d/rc.firewall and make it executable. This file will then be started by /etc/rc.d/rc.inet2 when your system boots, before your network devices are started.

You may choose to create a more complete script with start and stop options, but the following simple script is sufficient to load your firewall rules at boot.

```
vi /etc/rc.d/rc.firewall
```

```
# add the following lines #
if [ -e /etc/firewall.rules ]; then
        iptables-restore </etc/firewall.rules
fi
```

Make sure rc.firewall is executable...

```
chmod +x /etc/rc.d/rc.firewall
```

Load your firewall rules and make sure they are as you expect them to be before continuing. Also, be certain that your firewall actually loads at boot to prevent accidentally running without it!

```
iptables-restore </etc/firewall.rules
iptables -L
```

Return to main article page

Sources

- Originally written by astrogeek

howtos, email, postfix, dovecot, firewall