

firewalld exercise.

1. firewalld works with zones. A zone is a collection of rules that determines what is allowed and what is not.

2. What zone are my interfaces connected to?

```
# firewall-cmd --get-active-zones
public
interfaces: ens32
```

3. How do I list all available zones?

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

4. What services are allowed in a specific zone?

```
# firewall-cmd --zone=public --list-services
dhcpv6-client ssh
```

5. You cannot run a webserver because you see that http is not allowed.

6. We are going to create a webserver host first. This means that you install httpd and other tools by a yum groups install.

```
# yum groups install "Basic Web Server"
```

7. Put your name in the file /var/www/html/index.html

```
# echo "MS.GRONINGEN" > /var/www/index.html
```

8. Start the webserver

```
# systemctl start httpd
```

9. Make sure that httpd is running

```
# systemctl status httpd
```

10. Now ask a colleague to connect to your webserver. Your colleague installs elinks, which is a textmode webserver so you need no graphical environment.

```
(install elinks)
# yum install -y elinks
(connect to your webserver)
# elinks http://192.168.4.??? ← fill in the address of the webserver.
```

This will fail with the following message:

```
"Unable to retrieve http://....."
"No route to host"
"OK"
```

11. On the webserver host, you allow http packets.

```
# firewall-cmd --zone=public --add-service=http
```

Note: if you want to make this change permanent, you add the --permanent flag.

```
# firewall-cmd --zone=public --permanent --add-service=http
```

12. Your friend tries to connect again with elinks.

```
# elinks http://192.168.4.??? ← fill in the address of the webserver  
(success)
```

13. You can change your default zone.

```
# firewall-cmd --set-default-zone=home  
For the sake of the exercise we change it back to public:
```

```
# firewall-cmd --set-default-zone=public
```

14. If you have applications listening to ports that are closed, you can open specific ports.

```
# firewall-cmd --zone=public --add-port=5000/tcp
```

And you can open a range of ports.

```
# firewall-cmd --zone=public --add-port=4990-4999/udp
```

And then you can list the open ports.

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