

1. Configure your system so that the iptables and ip6tables services will not be accidentally started by an administrator.

```
[root@server ~]# systemctl status iptables
● iptables.service - IPv4 firewall with iptables
   Loaded: loaded (/usr/lib/systemd/system/iptables.service; enabled; vendor preset: disabled)
   Active: active (exited) since Tue 2024-12-03 20:47:53 EET; 1min 21s ago
   Main PID: 1758 (code=exited, status=0/SUCCESS)
   CGroup: /system.slice/iptables.service

Dec 03 20:47:53 server.mostafa.com systemd[1]: Sta...
Dec 03 20:47:53 server.mostafa.com iptables.init[1758]: ...
Dec 03 20:47:53 server.mostafa.com systemd[1]: Sta...
Hint: Some lines were ellipsized, use -l to show in full.
[root@server ~]# systemctl disable iptables
Removed symlink /etc/systemd/system/basic.target.wants/iptables.service.
[root@server ~]# systemctl status iptables
● iptables.service - IPv4 firewall with iptables
   Loaded: loaded (/usr/lib/systemd/system/iptables.service; disabled; vendor preset: disabled)
   Active: active (exited) since Tue 2024-12-03 20:47:53 EET; 1min 45s ago
   Main PID: 1758 (code=exited, status=0/SUCCESS)
   CGroup: /system.slice/iptables.service

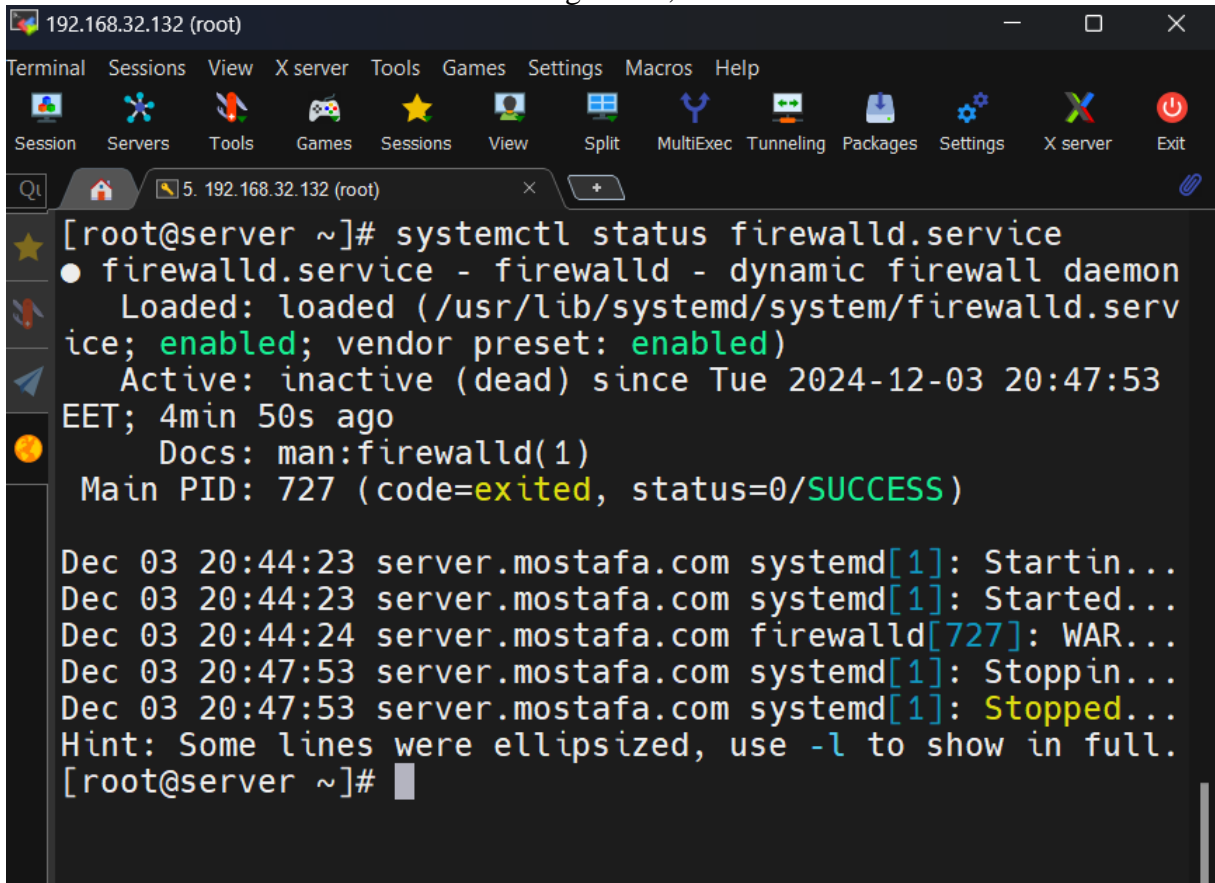
Dec 03 20:47:53 server.mostafa.com systemd[1]: Sta...
Dec 03 20:47:53 server.mostafa.com iptables.init[1758]: ...
Dec 03 20:47:53 server.mostafa.com systemd[1]: Sta...
```

```
[root@server ~]# systemctl status ip6tables
● ip6tables.service - IPv6 firewall with ip6tables
   Loaded: loaded (/usr/lib/systemd/system/ip6tables.serv
  ice; enabled; vendor preset: disabled)
   Active: active (exited) since Tue 2024-12-03 20:48:35
  EET; 1min 58s ago
   Main PID: 1861 (code=exited, status=0/SUCCESS)

Dec 03 20:48:35 server.mostafa.com systemd[1]: Startin...
Dec 03 20:48:35 server.mostafa.com ip6tables.init[1861]:
...
Dec 03 20:48:35 server.mostafa.com systemd[1]: Started...
Hint: Some lines were ellipsized, use -l to show in full.
[root@server ~]# systemctl disable ip6tables
Removed symlink /etc/systemd/system/basic.target.wants/ip
6tables.service.
[root@server ~]# systemctl status ip6tables
● ip6tables.service - IPv6 firewall with ip6tables
   Loaded: loaded (/usr/lib/systemd/system/ip6tables.serv
  ice; disabled; vendor preset: disabled)
   Active: active (exited) since Tue 2024-12-03 20:48:35
  EET; 2min 11s ago
   Main PID: 1861 (code=exited, status=0/SUCCESS)

Dec 03 20:48:35 server.mostafa.com systemd[1]: Startin...
Dec 03 20:48:35 server.mostafa.com ip6tables.init[1861]:
...
Dec 03 20:48:35 server.mostafa.com systemd[1]: Started...
Hint: Some lines were ellipsized, use -l to show in full.
[root@server ~]# █
```

2. Check if the firewalld service is running. If not, start it.

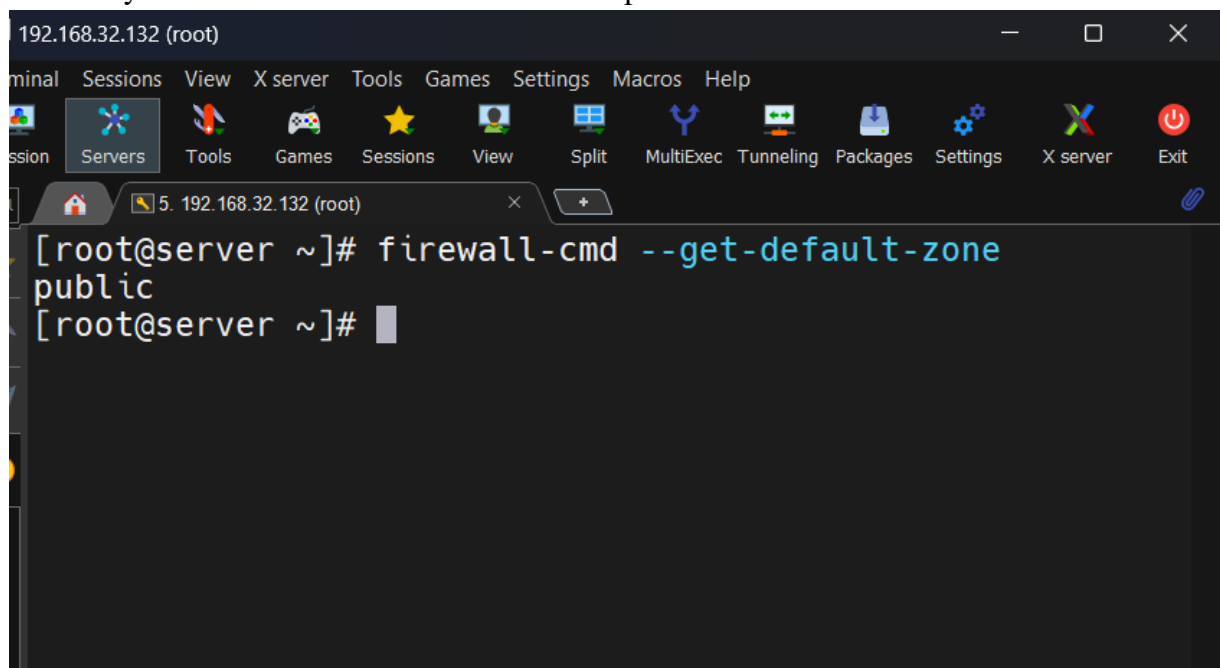


A terminal window titled "192.168.32.132 (root)" with a menu bar (Terminal, Sessions, View, X server, Tools, Games, Settings, Macros, Help) and a toolbar. The terminal shows the command `systemctl status firewalld.service` and its output. The output indicates that the service is loaded and enabled but is currently inactive (dead) since December 3, 2024, at 20:47:53 EET. It also shows the main PID as 727 and the status as "exited" with a success code. A log snippet shows the service starting and then stopping.

```
[root@server ~]# systemctl status firewalld.service
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset: enabled)
   Active: inactive (dead) since Tue 2024-12-03 20:47:53 EET; 4min 50s ago
     Docs: man:firewalld(1)
    Main PID: 727 (code=exited, status=0/SUCCESS)

Dec 03 20:44:23 server.mostafa.com systemd[1]: Starting...
Dec 03 20:44:23 server.mostafa.com systemd[1]: Started...
Dec 03 20:44:24 server.mostafa.com firewalld[727]: WARNING...
Dec 03 20:47:53 server.mostafa.com systemd[1]: Stopping...
Dec 03 20:47:53 server.mostafa.com systemd[1]: Stopped...
Hint: Some lines were ellipsized, use -l to show in full.
[root@server ~]#
```

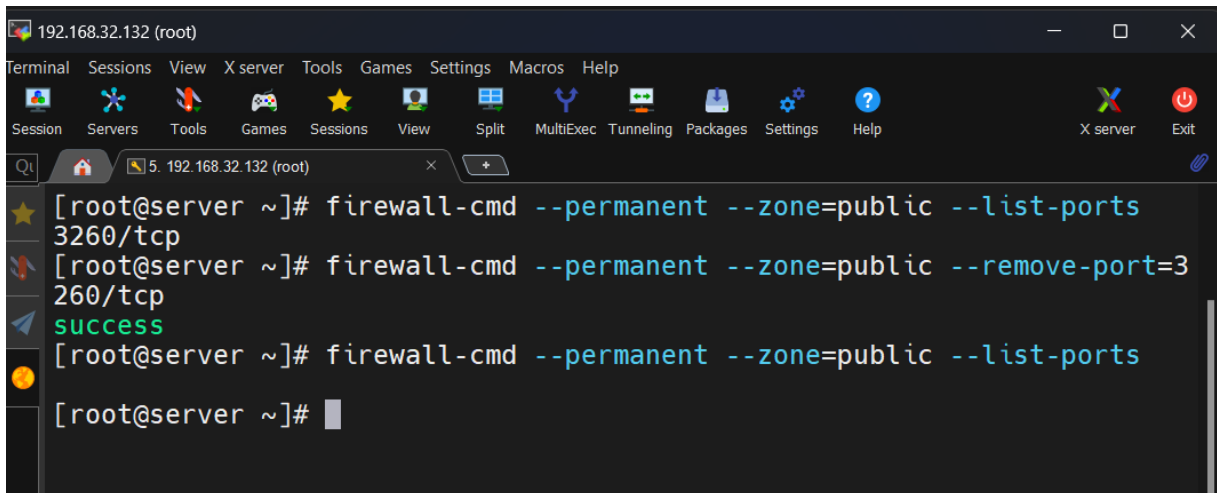
3. Verify that the default firewall zone is set to public.



A terminal window titled "192.168.32.132 (root)" with a menu bar (Terminal, Sessions, View, X server, Tools, Games, Settings, Macros, Help) and a toolbar. The terminal shows the command `firewall-cmd --get-default-zone` and its output, which is "public".

```
[root@server ~]# firewall-cmd --get-default-zone
public
[root@server ~]#
```

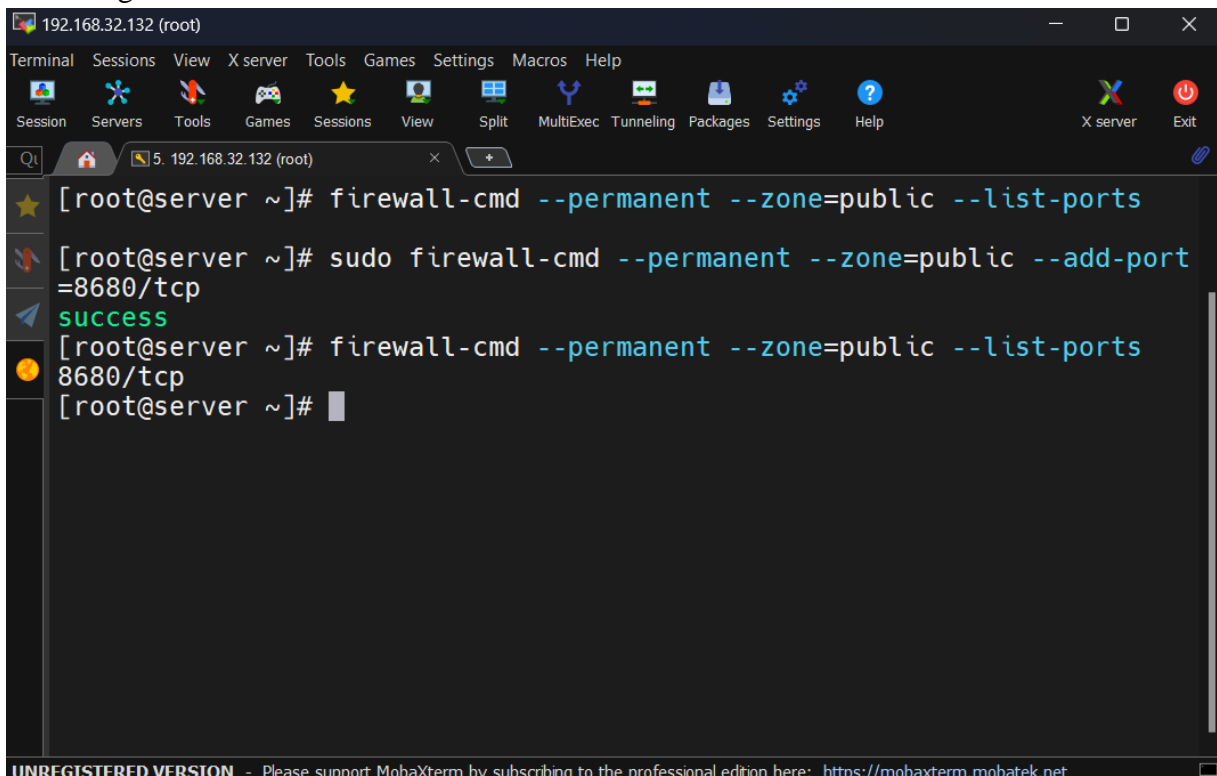
4. Verify that there are no unwanted ports open in the permanent configuration for the public zone.



A screenshot of the MobaXterm terminal window. The title bar shows the IP address 192.168.32.132 (root). The terminal displays the following commands and output:

```
[root@server ~]# firewall-cmd --permanent --zone=public --list-ports
3260/tcp
[root@server ~]# firewall-cmd --permanent --zone=public --remove-port=3260/tcp
success
[root@server ~]# firewall-cmd --permanent --zone=public --list-ports
[root@server ~]#
```

5. Add port 8680/TCP to the permanent configuration for the public zone. Verify your configuration.

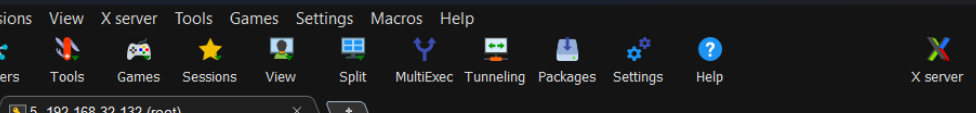


A screenshot of the MobaXterm terminal window. The title bar shows the IP address 192.168.32.132 (root). The terminal displays the following commands and output:

```
[root@server ~]# firewall-cmd --permanent --zone=public --list-ports
[root@server ~]# sudo firewall-cmd --permanent --zone=public --add-port=8680/tcp
success
[root@server ~]# firewall-cmd --permanent --zone=public --list-ports
8680/tcp
[root@server ~]#
```

At the bottom of the terminal window, there is a message: **UNREGISTERED VERSION** - Please support MobaXterm by subscribing to the professional edition here: <https://mobaxterm.mobatek.net>

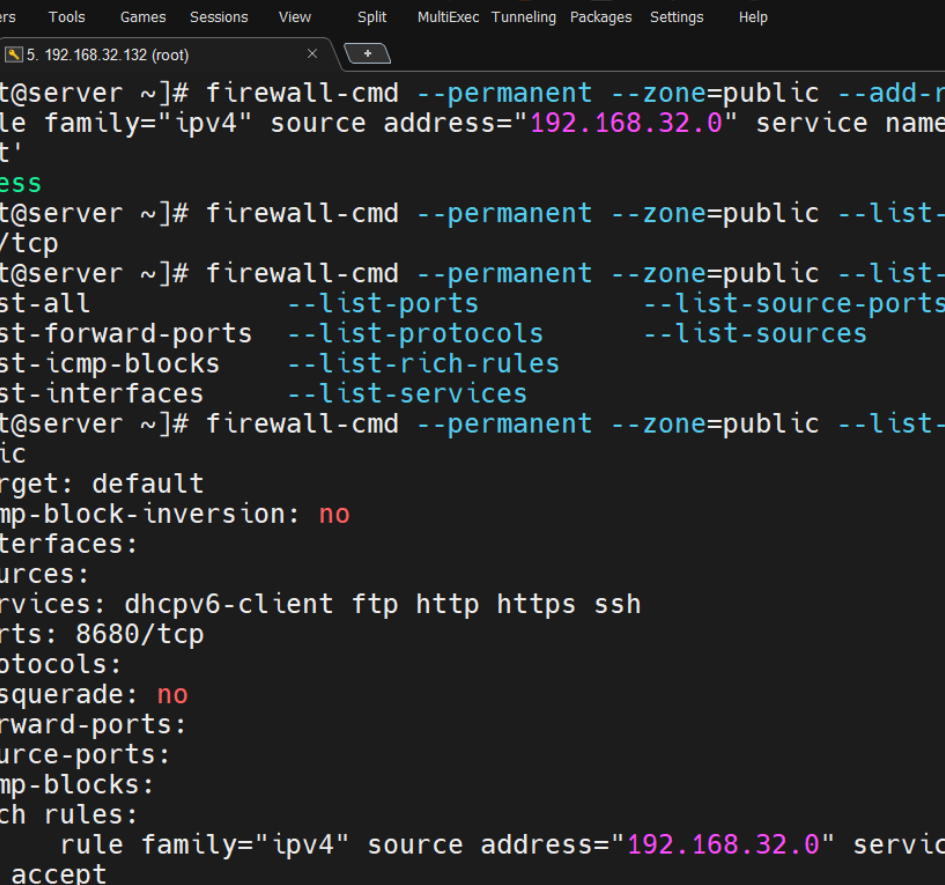
6. Reboot your serverX machine. (For a quick test, you can also use `sudo _firewall-cmd --reload`.)



The screenshot shows a terminal window with a dark theme. The title bar at the top reads "192.168.32.132 (root)". Below the title bar is a menu bar with options: Terminal, Sessions, View, X server, Tools, Games, Settings, Macros, and Help. A toolbar with various icons is located below the menu bar. The terminal content shows the user is at the root prompt [root@server ~] and has entered the command firewall-cmd --reload. The output is success. The user then enters the command reboot, and the cursor is at the end of the command.

```
192.168.32.132 (root)
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
5. 192.168.32.132 (root)
[root@server ~]# firewall-cmd --reload
success
[root@server ~]# reboot
```

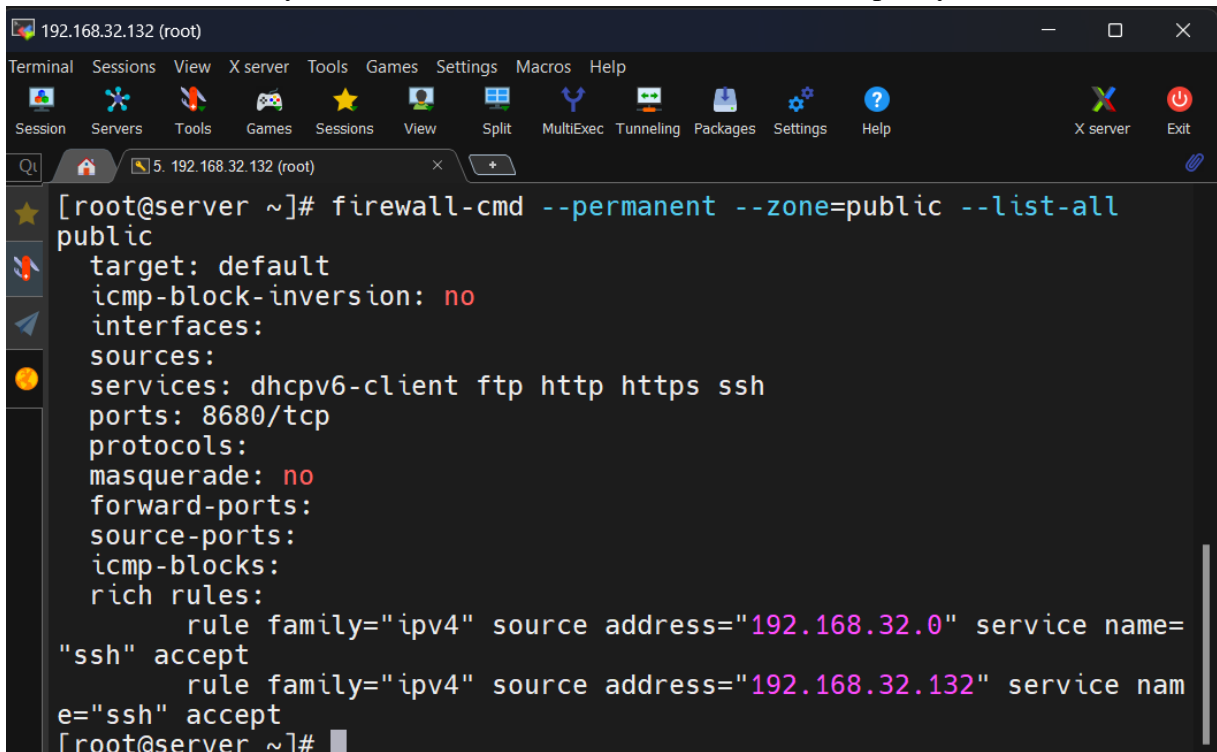
7. add a rule that only allows access to the `sshd` service from one subnet only



The screenshot shows a terminal window with a dark background and a light-colored text. The window title is "192.168.32.132 (root)". The terminal displays the following commands and output:

```
[root@server ~]# firewall-cmd --permanent --zone=public --add-rich-rule='rule family="ipv4" source address="192.168.32.0" service name="ssh" accept'
success
[root@server ~]# firewall-cmd --permanent --zone=public --list-ports
8680/tcp
[root@server ~]# firewall-cmd --permanent --zone=public --list-
--list-all                --list-ports                --list-source-ports
--list-forward-ports      --list-protocols            --list-sources
--list-icmp-blocks        --list-rich-rules
--list-interfaces         --list-services
[root@server ~]# firewall-cmd --permanent --zone=public --list-all
public
target: default
icmp-block-inversion: no
interfaces:
sources:
services: dhcpv6-client ftp http https ssh
ports: 8680/tcp
protocols:
masquerade: no
forward-ports:
source-ports:
icmp-blocks:
rich rules:
    rule family="ipv4" source address="192.168.32.0" service name=
ssh" accept
[root@server ~]#
```

8. add a rule that only allows access to the sshd service from one ip only

A screenshot of a terminal window titled "192.168.32.132 (root)". The window has a menu bar with "Terminal", "Sessions", "View", "X server", "Tools", "Games", "Settings", "Macros", and "Help". Below the menu bar is a toolbar with icons for Session, Servers, Tools, Games, Sessions, View, Split, MultiExec, Tunneling, Packages, Settings, Help, X server, and Exit. The terminal shows the command "firewall-cmd --permanent --zone=public --list-all" being executed. The output lists various firewall settings: target: default, icmp-block-inversion: no, interfaces: (empty), sources: (empty), services: dhcpv6-client ftp http https ssh, ports: 8680/tcp, protocols: (empty), masquerade: no, forward-ports: (empty), source-ports: (empty), icmp-blocks: (empty), and rich rules: (empty). The rich rules section shows two rules: "rule family='ipv4' source address='192.168.32.0' service name='ssh' accept" and "rule family='ipv4' source address='192.168.32.132' service name='ssh' accept". The prompt "[root@server ~]#" is visible at the bottom.

```
[root@server ~]# firewall-cmd --permanent --zone=public --list-all
public
target: default
icmp-block-inversion: no
interfaces:
sources:
services: dhcpv6-client ftp http https ssh
ports: 8680/tcp
protocols:
masquerade: no
forward-ports:
source-ports:
icmp-blocks:
rich rules:
    rule family="ipv4" source address="192.168.32.0" service name=
"ssh" accept
    rule family="ipv4" source address="192.168.32.132" service nam
e="ssh" accept
[root@server ~]#
```