How to disable IPv6 rules in UFW to increase firewall security on Linux

When you add firewall rules using UFW, Uncomplicated Firewall, it adds both IPv4 and IPv6 rules by default. However, in most cases you will only need IPv4 rules because it is the most used.

IPv6 (Internet Protocol version 6) is the next generation Internet protocol following the success of IPv4. It solves the challenges associated with having a unique IP address available for each IoT-enabled device.

When you add firewall rules using UFW, Uncomplicated Firewall, it adds both IPv4 and IPv6 rules by default. However, in most cases you will only need IPv4 rules because it is the most used.

Here's how you can disable IPv6 rules in UFW to increase PC security.

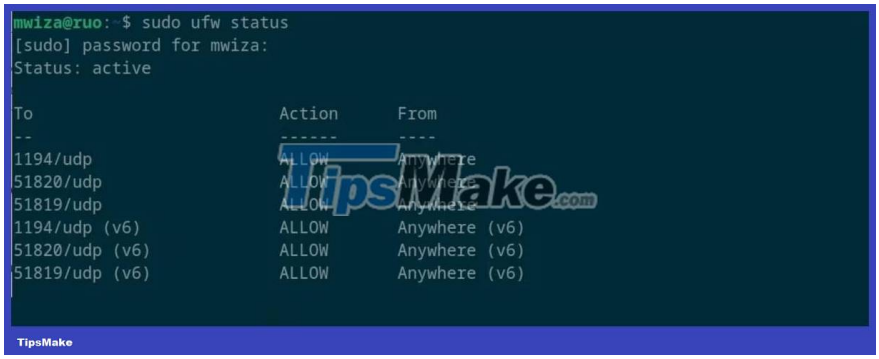
See UFW rules on Linux

UFW is a popular firewall tool on Linux because it is relatively easy to use and set up. It is available by default on Ubuntu and other Debian-based distributions, and you can easily install it on all major Linux distributions.

You can view the UFW rules on your Linux PC by running:

```
sudo ufw status
```

For security purposes, you will need elevated or administrative privileges to run UFW commands.



From the previous output, you can see that both IPv4 and IPv6 rules are enabled.

Enabling services or connections that should not be enabled is a security risk because it increases the attack surface and does not provide any security benefits.

Disable IPv6 rules using UFW on Linux

Disabling IPv6 rules in UFW is relatively easy. Just open the following UFW configuration file with your favorite text editor:

```
sudo vim /etc/default/ufw
```

Look at line **IPv6=yes** , line number 7 in this case. Change **yes** to **no** , then save the file. The file now looks like this:

In some cases you may need to restart the firewall for the changes to take effect, you can do this using:

```
sudo ufw reload
```

You can review the firewall status with the **sudo ufw status** command . This time, there will be only IPv4 rules.

Firewalls play an important role in protecting your PC from cyber threats. To enhance information security, it is best to have multiple layers of protection to prevent any intruders who may want to attack your PC.

Remember, only enable the connections or services you need in your firewall, everything else will be disabled by default.

You finished reading the article "**How to disable IPv6 rules in UFW to increase firewall security on Linux**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
