ted and may earn a commission when you buy through links on our site

nake a VPN kill switch in Linux with

Connecting to the internet through a VPN is steadily getting more mainstream as ISPs and governments take an increasing interest in your browsing habits. But what good is a VPN if you forget to use it? Or if the connection drops and you don't notice? If you're already committed to browsing the web anonymously, setting up a VPN kill switch on your Linux desktop will make sure your data is encrypted.

AARON PHILLIPS
December 4, 2020

A VPN kill switch is a set of firewall rules that will stop all internet traffic when your VPN isn't

Latest guides

Surveillance camera statistics: which cities have the most CCTV cameras?
August 15, 2019 / by Paul Bischoff

Guide to using public wifi safely and securely
October 9, 2018 / by Osman Husain

Popular Posts

connected. They're completely automated, with the kill switch only kicking in when there's a problem with your secure connection.

If you've ever kicked yourself for browsing while your VPN was down without even noticing, creating a VPN kill switch with UFW is a pretty easy fix.

What is UFW?

UFW is a set of scripts that act as a wrapper to the Linux iptables firewall. iptables is a powerful tool, but it's not very easy to use. UFW makes it much simpler to build a useful ruleset, especially if you're not a Linux power user who knows iptables by heart.

If you've ever struggled with Linux networking but still need a secure and user friendly firewall, I recommend UFW.

Before you begin

Before you get started, it's a good idea to make sure your system is up to date. I'll be using Ubuntu 18 LTS for this guide. As long as you're using a Debian-based Linux operating system, the steps will be identical.

Use the following commands to update your operating system and installed software:

```
sudo apt update

sudo apt upgrade -y
```

10 Best SFTP and FTPS Servers Reviewed 2021

February 27, 2019 / by Jon Watson

Best VPNs for Netflix: Get any version of Netflix anywhere

January 5, 2019 / by Paul Bischoff

10 Best VPNs for Torrenting Safely and Privately in 2021

January 1, 2019 / by Paul Bischoff

Die besten und schlechtesten VPNs für Torrent-Dateien und P2P-Filesharing 2018

September 25, 2018 / by Paul Bischoff

How to make your own free VPN with Amazon Web Services

May 15, 2018 / by Paul Bischoff

Latest Cloud and Online Backup

10 Best Secure File Sharing Tools & Software for Business in 2021

October 21, 2019 / by Tim Keary

Once the commands have finished executing, you're ready to get started setting up a VPN kill switch with UFW.

Disabling IPv6

Many VPN providers still don't have adequate IPv6 support, which can cause data leaks and other issues. I think it's a good idea to disable IPv6 entirely unless you're positive your provider supports it.

This step is optional, and you can skip it if necessary.

How to turn disable IPv6

You'll need to disable IPv6 for both the operating system and UFW to be sure that your VPN provider won't passthrough IPv6 traffic unencrypted. In Ubuntu, that means you'll need to edit the following files:

- **/etc/sysctl.conf** to disable IPv6 networking
- **/etc/default/ufw** to stop UFW from automatically creating IPv6 rules

Rapidshare is discontinued, try these alternatives
February 4, 2019 / by Aimee O'Driscoll

The 5 Best Edge Services Providers
October 15, 2018 / by Stephen Cooper

The best apps to encrypt your files before uploading to the cloud
October 11, 2018 / by Paul Bischoff

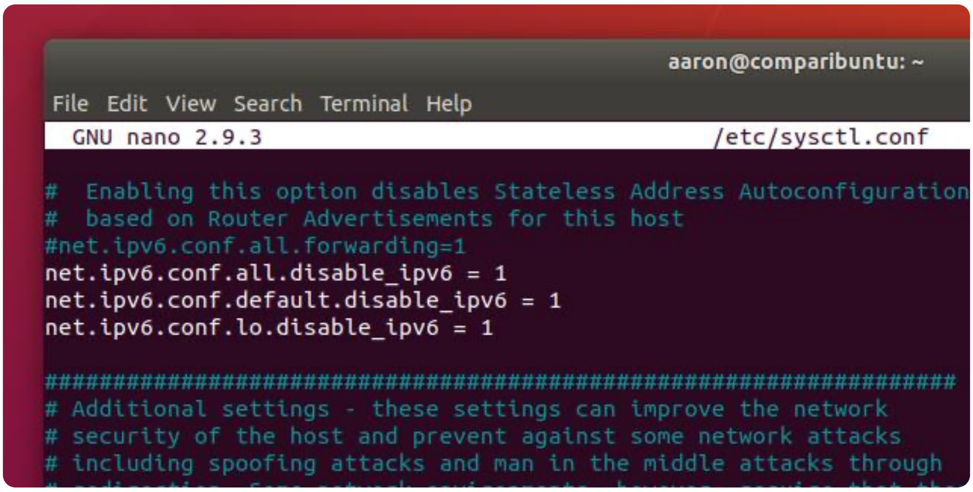
Is Dropbox Secure? 10 Ways To Make The File Sharing Service Safer To Use
December 28, 2017 / by David Gilbert

Latest Information Security

Canada cyber security and cyber crime statistics (2020-2021)
September 6, 2021 / by Aimee O'Driscoll

Ransomware attacks on US schools and colleges cost $6.62bn in 2020
August 31, 2021 / by Paul Bischoff

France cyber security and cyber crime statistics



```
GNU nano 2.9.3                                  /etc/sysctl.conf

#  Enabling this option disables Stateless Address Autoconfiguration
#  based on Router Advertisements for this host
#net.ipv6.conf.all.forwarding=1
net.ipv6.conf.all.disable_ipv6 = 1
net.ipv6.conf.default.disable_ipv6 = 1
net.ipv6.conf.lo.disable_ipv6 = 1

###################################################################
# Additional settings - these settings can improve the network
# security of the host and prevent against some network attacks
# including spoofing attacks and man in the middle attacks through
```

To get started, open **/etc/sysctl.conf** for editing with the following console command:

```
sudo nano /etc/sysctl.conf
```

Scroll through the file until you see an entry for **net.ipv6.conf** and add the following three lines to the end of the configuration file:

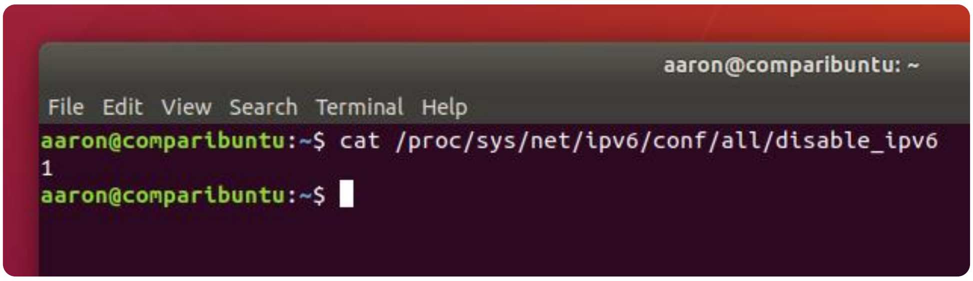
```
net.ipv6.conf.all.disable_ipv6=1

net.ipv6.conf.default.disable_ipv6=1

net.ipv6.conf.lo.disable_ipv6=1
```

Save your changes with **Ctrl+X**, **Y** and force the system to reload sysctl.conf and apply your changes using the command:

```
sudo sysctl -p
```



```
aaron@comparibuntu:~$ cat /proc/sys/net/ipv6/conf/all/disable_ipv6
1
aaron@comparibuntu:~$ 
```

You can confirm the changes were applied successfully by taking a look at files in the **/proc**

(2020-2021)

August 27, 2021 / by Aimee O'Driscoll

UK cyber security and cyber crime statistics (2021)

August 25, 2021 / by Aimee O'Driscoll

US cyber security and cyber crime statistics (2021)

August 25, 2021 / by Aimee O'Driscoll

Latest VPN & Privacy

The Ultimate Guide to Ad-Blocking Filter Lists

September 10, 2021 / by Josh Lake

Syria Cyber Profile

September 2, 2021 / by Stephen Cooper

North Korea Cyber Profile

August 27, 2021 / by Stephen Cooper

Egypt Cyber Profile

August 27, 2021 / by Stephen Cooper

India Cyber Profile

August 27, 2021 / by Stephen Cooper

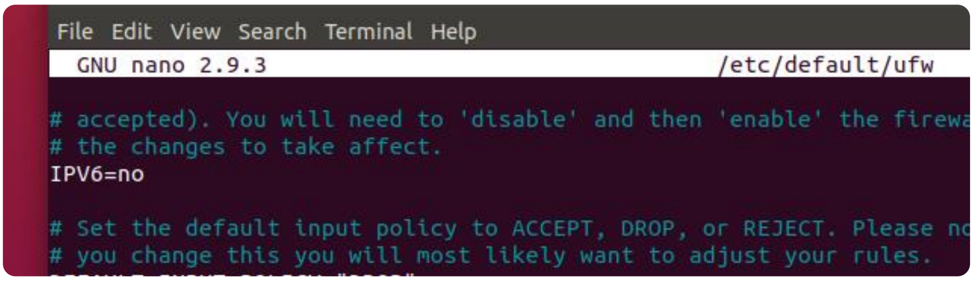
Latest Crypto

Bitcoin fraud, theft, and security

which contain information about your system. In this case, use the following command to make sure IPv6 is disabled at the operating system level:

```
cat /proc/sys/net/ipv6/conf/all/disable_ipv6
```

If your system displays a **1** as output, IPv6 has been disabled successfully.



```
  GNU nano 2.9.3                          /etc/default/ufw

# accepted). You will need to 'disable' and then 'enable' the firewa
# the changes to take affect.
IPV6=no

# Set the default input policy to ACCEPT, DROP, or REJECT. Please no
# you change this you will most likely want to adjust your rules.
```

Next, you'll want to stop UFW from automatically creating IPv6 firewall rules. Even through the protocol has been disabled at the operating system level, UFW stubbornly insists on adding IPv6 rules until it's been told to stop. Doing so will reduce clutter in your ruleset and might save you some confusion later on.

To turn off IPv6 in UFW, open the file **/etc/default/ufw** for editing using this command:

```
sudo nano /etc/default/ufw
```

Scroll through until you find the setting for IPv6 rules, and change it to read:

```
IPV6=no
```

Press **Ctrl+X**, **Y** to save your changes. **If you've**

statistics
May 6, 2021 / by Aimee O'Driscoll

Bitcoin Price History – the value of 1 BTC over time
April 19, 2021 / by Rebecca Moody

How Do People Feel About Cryptocurrencies?
July 31, 2019 / by Paul Bischoff

The Biggest Cryptocurrency Heists of All Time
June 28, 2019 / by Theo Tsihitas

Understanding cryptography's role in blockchains
April 10, 2019 / by Josh Lake

Latest Crypto Popular Posts

How to buy and pay with bitcoin anonymously
April 18, 2018 / by Aimee O'Driscoll

What is Bitcoin mining and how can you do it?
March 7, 2018 / by Aimee O'Driscoll

15 best bitcoin wallets for 2021 (that are safe and easy to use)
February 25, 2018 / by Aimee O'Driscoll

already enabled UFW prior to starting this project, **you'll need to disable it** with the following command:

```
sudo ufw disable
```

Now that IPv6 has been disabled system-wide, you can move on to collecting the information you need to set up the VPN kill switch with UFW.

Getting the information you need

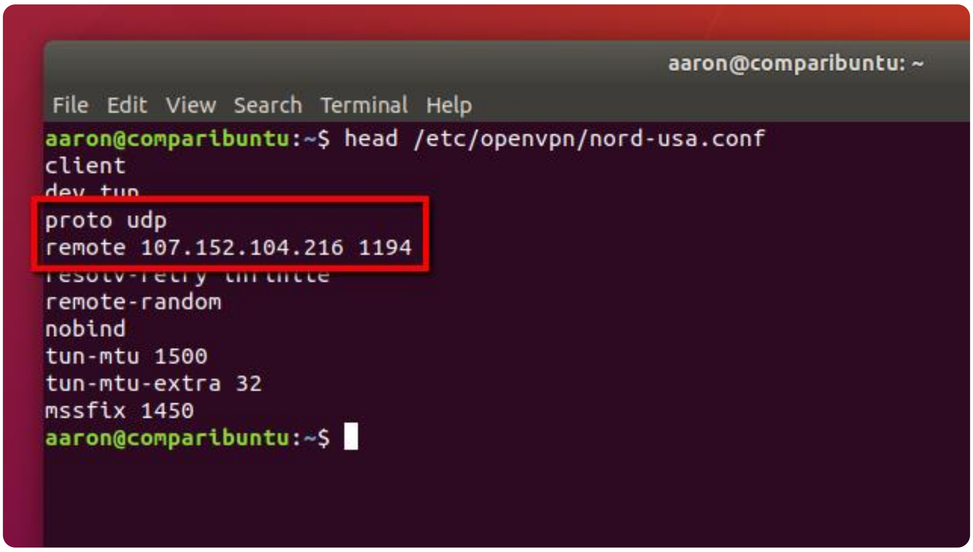
In order to setup a VPN kill switch in UFW, you need three pieces of information:

- The **public IP address** of the VPN server you connect to
- The **port and protocol** your server uses to communicate
- The **subnet** of your local network

Those settings can be found in the config file for your VPN server. In order to get information about your connection, you'll have to look through the config and make a note of your settings.

Display the VPN server settings

In most cases, your VPN config will be stored in **/etc/openvpn**, but it's possible to set it up in any location. If you don't see an ***.ovpn** or ***.conf** file in **/etc/openvpn**, check your home directory.



```
aaron@comparibuntu:~$ head /etc/openvpn/nord-usa.conf
client
dev tun
proto udp
remote 107.152.104.216 1194
resolv-retry infinite
remote-random
nobind
tun-mtu 1500
tun-mtu-extra 32
mssfix 1450
aaron@comparibuntu:~$
```

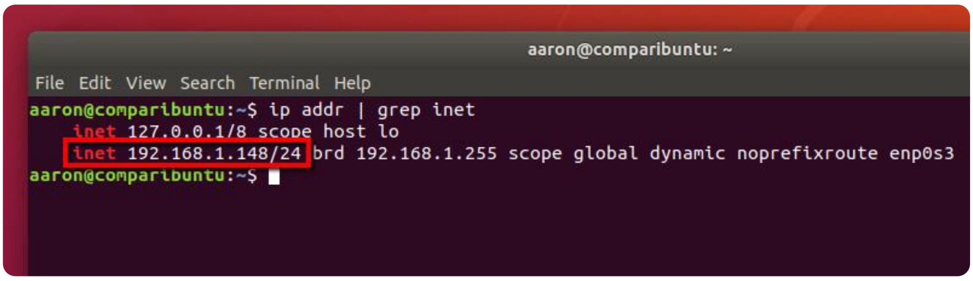
The **port, protocol, and public IP address** you need will be near the top of the config file. I used this command to display mine, as above:

```
head /etc/openvpn/config.ovpn
```

Make a note of all three, since you will need them to setup UFW.

Display the subnet

You'll also need to know the LAN subnet your computer is on. In many cases, it will be **192.168.1.0/24** but if you're not sure it's a good idea to confirm before setting up a VPN kill switch with UFW.



```
aaron@comparibuntu:~$ ip addr | grep inet
    inet 127.0.0.1/8 scope host lo
    inet 192.168.1.148/24 brd 192.168.1.255 scope global dynamic noprefixroute enp0s3
aaron@comparibuntu:~$
```

There are a handful of different ways to get the information you need, but I recommend this command:

June 11, 2019 / by Sam Cook

How to set up IPTV on Perfect Player

January 31, 2019 / by Tom Blackstone

Kodi Solutions IPTV: What is Kodi Solutions? Is it your next IPTV?

September 24, 2018 / by Tom Blackstone

Area 51 IPTV: What is Area 51 IPTV and should you use it?

September 23, 2018 / by Tom Blackstone

Terrarium TV shut down: Use these top 10 Terrarium TV alternatives

September 18, 2018 / by Sam Cook

Latest Identity Theft Protection

How to delete online accounts and reduce your security risks

February 3, 2020 / by Sam Cook

Identity fraud on Upwork and other freelance sites threatens gig economy integrity

July 30, 2019 / by Sam Cook

Consumer interest in

```
ip addr | grep inet
```

You'll see an **inet** entry for each network adapter on your system. In most cases, there will only be two entries; one for your loopback adapter, and one for your LAN adapter. **Ignore the loopback adapter**, which will always have a subnet of **127.0.0.1/8**, and make a note of the other entry.

Setting up a VPN kill switch with UFW

Once you have the information you need, you'll be able to setup the VPN kill switch with UFW. There are three steps to this process:

- Explicitly allow LAN traffic, so network services will work even when the VPN is down
- Disallow all other traffic unless it is running through the encrypted connection
- Enable UFW to activate the ruleset

Once you're finished, the VPN kill switch will be active. All of the settings will stay active even if you reboot your computer.

Allow local traffic

It's important to allow your computer to access the LAN even when the VPN is down if you rely on any local network resources. Since most people use network printing, and many Linux users rely on SSH, I really recommend you don't skip this step.

Please note that this will only allow traffic in or out on your LAN. Your internet connection will be

checking credit scores jumped 230 percent in a decade. Here's why that's a dangerous trend
February 20, 2019 / by Sam Cook

Latest Kodi

Can You Watch Tyson vs Jones on Kodi?
August 13, 2020 / by Sam Cook

How to install the PBS Kids Kodi addon
September 25, 2019 / by Ian Garland

How to watch AEW – All Out Free on Kodi with a VPN
August 30, 2019 / by William Elcock

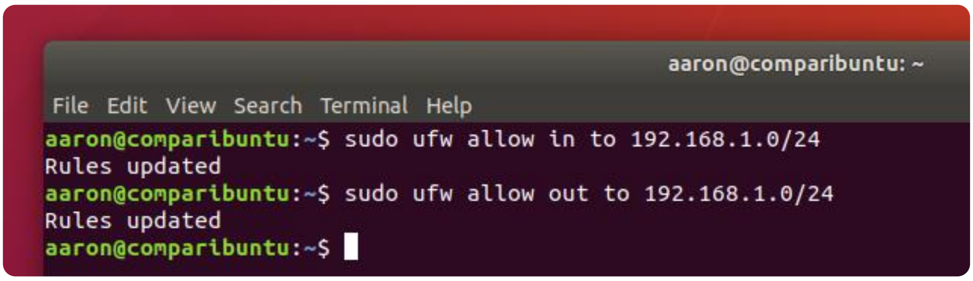
How to watch the US Tennis Open 2021 on Kodi – free livestream
August 16, 2019 / by William Elcock

How to download and install Kodi Leia 18.3 on Firestick
August 13, 2019 / by Ian Garland

Latest Kodi Popular Posts

Can you watch Bellator 223: Mousasi vs.

disabled when the VPN is down as intended.



```
aaron@comparibuntu:~$ sudo ufw allow in to 192.168.1.0/24
Rules updated
aaron@comparibuntu:~$ sudo ufw allow out to 192.168.1.0/24
Rules updated
aaron@comparibuntu:~$
```

You'll need to know your LAN subnet from the previous step, and use that subnet in place of mine at **192.168.1.0/24**.

Use the following commands to allow LAN access to your computer:

```
sudo ufw allow in to 192.168.1.0/24

sudo ufw allow out to 192.168.1.0/24
```

You should get confirmation when each rule is added, as above.

Configure the VPN kill switch

Next, you'll set up the kill switch itself. There are only 4 or 5 commands you'll need to enter, but this will completely shut down your internet connection when the VPN is disconnected.

To start, set the default policy to deny all traffic using these two commands:

```
sudo ufw default deny outgoing
sudo ufw default deny incoming
```

Next, add an exception to the ruleset allowing you to connect to the VPN server. Without this line, you'll be unable to authenticate and your VPN

Lovato on Kodi?
June 21, 2019 / by Sam Cook

How to watch the 2021 French Open on Kodi
May 21, 2019 / by Sam Cook

How to watch the NCAA Frozen Four 2021 on Kodi
April 10, 2019 / by Sam Cook

How to watch the 2021 NCAA Final Four and Championship game on Kodi
April 5, 2019 / by Sam Cook

30+ Best Kodi Addons working in August 2021 (of 130+ tested)
March 15, 2019 / by Ian Garland

Latest Net Admin

Threat Modeling Guide
September 13, 2021 / by Amakiri Welekwe

7 Best Static Code Analysis Tools
September 5, 2021 / by Liku Zelleke

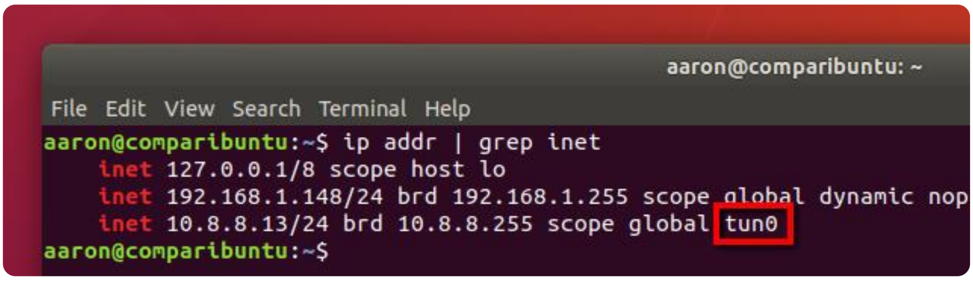
4 Best PII Scanning Tools
September 5, 2021 / by Stephen Cooper

session won't be able to start successfully. Use the VPN **port, protocol, and public IP address** you made a note of in a previous step.

Once you're sure you've got the information you need, run this command with your own settings in place of mine:

```
sudo ufw allow out to 107.152.104.216 port 1194
proto udp
```

Now that you're able to connect to the VPN through your firewall, you'll have to write a rule or two forcing all outbound traffic to move through that connection. For this guide I'm assuming your VPN connects using the network device **tun0**, since that is the default.



```
aaron@comparibuntu:~$ ip addr | grep inet
    inet 127.0.0.1/8 scope host lo
    inet 192.168.1.148/24 brd 192.168.1.255 scope global dynamic nop
    inet 10.8.8.13/24 brd 10.8.8.255 scope global tun0
aaron@comparibuntu:~$
```

If you need to confirm, you can **connect to your VPN** and run **ip addr | grep inet** again. You'll see an additional entry for the VPN connection, and you can pick out the name of your VPN tunnel adapter from the information listed.

Once you're satisfied you know which network device your VPN is using, run this command to force all outbound traffic to use the VPN:

```
sudo ufw allow out on tun0 from any to any
```

What is PII Compliance?
September 5, 2021 / by Stephen Cooper

Burp Suite Review & Alternatives
September 5, 2021 / by Stephen Cooper

Latest Net Admin Popular Posts

11 Best Free TFTP Servers for Windows, Linux and Mac
February 28, 2019 / by Jon Watson

13 Best NetFlow Analyzers & Collector Tools for 2021
January 23, 2019 / by John Kimball

Best Bandwidth Monitoring Tools – Free Tools to Analyze Network Traffic Usage
December 21, 2018 / by John Kimball

Latest Plex

Watch your Plex library in Kodi with the Plex Kodi addon
December 24, 2017 / by Aaron Phillips

How to set up Plex on Chromecast and get the

Optionally, you may want to allow connections back in through the VPN. For instance, you might have a BitTorrent client with a web interface you need to connect to from the web, or a service like Plex that requires inbound connections through the VPN. Run this command to allow inbound connections if desired:

```
sudo ufw allow in on tun0 from any to any
```

Once you've executed the final command, your VPN kill switch is ready to enable.

Enable UFW

Enabling UFW with your custom ruleset is simple. Run this command, and UFW will start on boot:

```
sudo ufw enable
```

If you need to disable your kill switch, you can use this command:

```
sudo ufw disable
```

UFW remembers the ruleset you created, so feel free to enable and disable the firewall whenever you like. Just remember, when UFW is disabled your internet traffic is not guaranteed to be encrypted.

most out of it
December 7, 2017 / by Aaron Phillips

Plex vs Kodi: Which streaming software is right for you?
November 1, 2017 / by Aaron Phillips

Installing and using the Fire TV Plex app
October 31, 2017 / by Aaron Phillips

The best Plex plugins: 25 of our favorites (Updated)
September 20, 2017 / by Aaron Phillips

Latest Plex Popular Posts

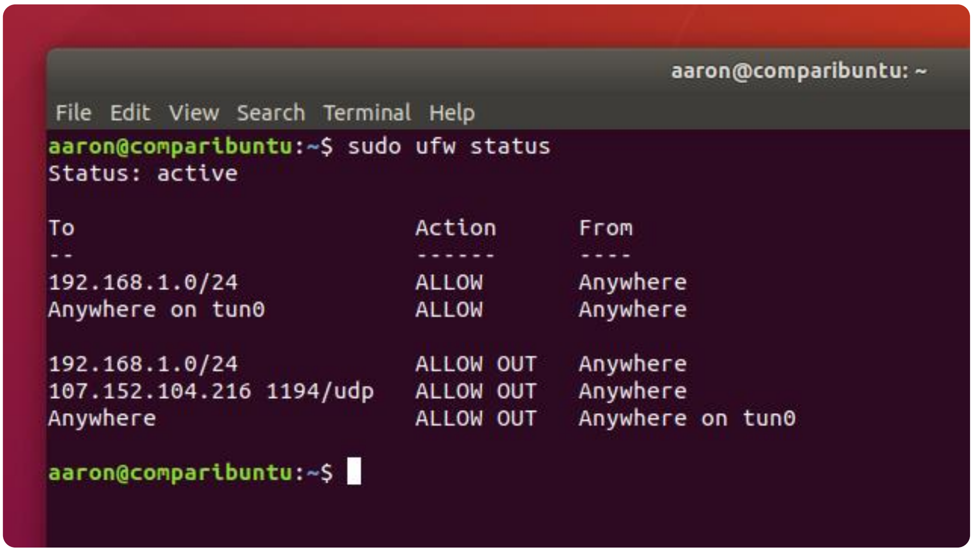
How to get started streaming with Plex media server
September 20, 2017 / by Aaron Phillips

Selectively routing Plex through your VPN
September 20, 2017 / by Aaron Phillips

Latest Sports Streaming

How to watch the Solheim Cup (2021) online from anywhere
September 3, 2021 / by Mark Gill

How to watch Manny



```
aaron@comparibuntu:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
192.168.1.0/24             ALLOW       Anywhere
Anywhere on tun0           ALLOW       Anywhere

192.168.1.0/24             ALLOW OUT   Anywhere
107.152.104.216 1194/udp   ALLOW OUT   Anywhere
Anywhere                   ALLOW OUT   Anywhere on tun0

aaron@comparibuntu:~$ 
```

Of course, it’s easy to check and see whether UFW is active or not, and which rules are being applied to your network. Check the status of UFW using this command:

```
sudo ufw status
```

That’s all there is to setting up UFW, but there are a few additional steps I recommend you take to make using OpenVPN with a kill switch a little easier.

Configuring your VPN to connect automatically

Although this step is optional, setting up a kill switch won’t be useful unless you connect to your VPN automatically. OpenVPN is notoriously unwieldy out of the box, but there are a few tricks you can use to streamline connecting to your VPN.

Here’s what I recommend:

- Run OpenVPN as a service using a ***.conf** file instead of an ***.ovpn** profile
- Save your username and password so

Pacquiao vs Yordenis Ugas online from anywhere
August 20, 2021 / by Mark Gill

How to watch the MLB Draft live online from anywhere
July 10, 2021 / by Mark Gill

How to watch Italy vs England live online (EURO 2020 final)
July 9, 2021 / by Ian Garland

How to watch Berrettini vs Hurkacz live online free (Wimbledon)
July 8, 2021 / by Ian Garland

Latest Sports Streaming Popular Posts

How to watch Gervonta Davis vs Leo Santa Cruz live online
October 20, 2020 / by Sam Cook

How to watch Vasiliy Lomachenko vs Teofimo Lopez live online
October 16, 2020 / by Sam Cook

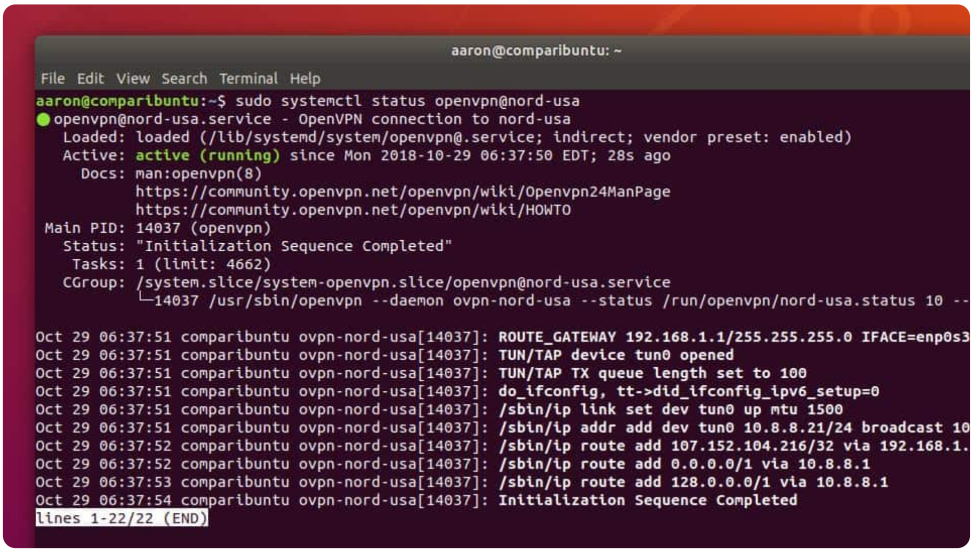
How to watch Deontay Wilder vs Tyson Fury 2 heavyweight

OpenVPN can connect automatically
- Use chmod to lock down your VPN config

If you implement those three suggestions, you'll be able to connect to your VPN automatically with the knowledge that your login credentials are secure. You'll also be able to control your VPN connection from the system console, which makes stopping and restarting the VPN connection much simpler.

Run OpenVPN as a service

Most people have their VPN configuration saved with an ***.ovpn** file extension. But if you change the extension to ***.conf**, and make sure the file is located in **/etc/openvpn**, you'll be able to manage the connection like you do any other system service.



```
aaron@comparibuntu:~$ sudo systemctl status openvpn@nord-usa
● openvpn@nord-usa.service - OpenVPN connection to nord-usa
   Loaded: loaded (/lib/systemd/system/openvpn@.service; indirect; vendor preset: enabled)
   Active: active (running) since Mon 2018-10-29 06:37:50 EDT; 28s ago
     Docs: man:openvpn(8)
           https://community.openvpn.net/openvpn/wiki/Openvpn24ManPage
           https://community.openvpn.net/openvpn/wiki/HOWTO
 Main PID: 14037 (openvpn)
   Status: "Initialization Sequence Completed"
    Tasks: 1 (limit: 4662)
   CGroup: /system.slice/system-openvpn.slice/openvpn@nord-usa.service
           └─14037 /usr/sbin/openvpn --daemon ovpn-nord-usa --status /run/openvpn/nord-usa.status 10 --

Oct 29 06:37:51 comparibuntu ovpn-nord-usa[14037]: ROUTE_GATEWAY 192.168.1.1/255.255.255.0 IFACE=enp0s3
Oct 29 06:37:51 comparibuntu ovpn-nord-usa[14037]: TUN/TAP device tun0 opened
Oct 29 06:37:51 comparibuntu ovpn-nord-usa[14037]: TUN/TAP TX queue length set to 100
Oct 29 06:37:51 comparibuntu ovpn-nord-usa[14037]: do_ifconfig, tt->did_ifconfig_ipv6_setup=0
Oct 29 06:37:51 comparibuntu ovpn-nord-usa[14037]: /sbin/ip link set dev tun0 up mtu 1500
Oct 29 06:37:51 comparibuntu ovpn-nord-usa[14037]: /sbin/ip addr add dev tun0 10.8.8.21/24 broadcast 10
Oct 29 06:37:52 comparibuntu ovpn-nord-usa[14037]: /sbin/ip route add 107.152.104.216/32 via 192.168.1.
Oct 29 06:37:52 comparibuntu ovpn-nord-usa[14037]: /sbin/ip route add 0.0.0.0/1 via 10.8.8.1
Oct 29 06:37:53 comparibuntu ovpn-nord-usa[14037]: /sbin/ip route add 128.0.0.0/1 via 10.8.8.1
Oct 29 06:37:54 comparibuntu ovpn-nord-usa[14037]: Initialization Sequence Completed
lines 1-22/22 (END)
```

Setting up your OpenVPN connection to run as a service is as easy as renaming a file. First, move your existing ***.ovpn** profile to **/etc/openvpn** if it isn't there already.

Then rename the profile to give it a ***.conf** file

world title fight

February 21, 2020 / by Sam Cook

How to watch the Stanley Cup Final 2021 live online from anywhere

May 26, 2019 / by Sam Cook

How to watch Super Bowl LV (55) free online anywhere in the world

February 2, 2019 / by Sam Cook

Latest TV Streaming

How to watch American Crime Story season 3 online from anywhere

September 6, 2021 / by Mark Gill

How to watch Robot Chicken Season 11 online from anywhere

September 5, 2021 / by Ian Garland

How to watch A.P. Bio season 4 online from anywhere

September 1, 2021 / by Mark Gill

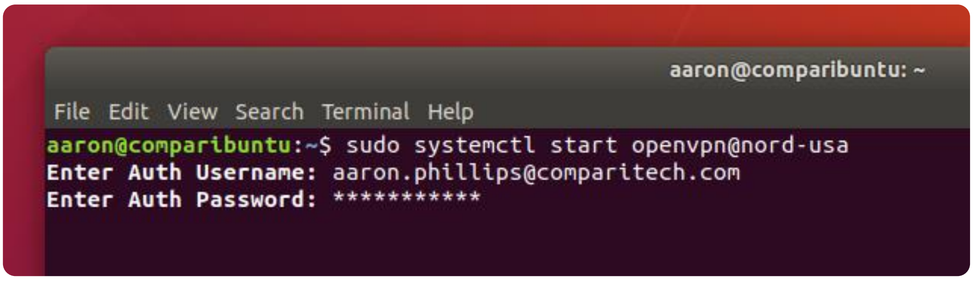
How to watch Coronation Street online abroad for free

August 18, 2021 / by Mark Gill

How to watch

extension. In my case, I saved the OpenVPN profile as **nord-usa.ovpn**, so I'll use the following command to rename it:

```
sudo mv /etc/openvpn/nord-usa.ovpn
/etc/openvpn/nord-usa.conf
```



```
aaron@comparibuntu:~$ sudo systemctl start openvpn@nord-usa
Enter Auth Username: aaron.phillips@comparitech.com
Enter Auth Password: ***********
```

Once it's renamed, you can start and stop OpenVPN just like any other systemd service. For instance, I'd use this command to connect:

```
sudo systemctl start openvpn@nord-usa
```

And this command to disconnect:

```
sudo systemctl stop openvpn@nord-usa
```

You'll notice that OpenVPN prompts you for a username and password each time, though. That's not ideal, but you can fix it by saving your username and password.

Save your username and password

In your OpenVPN profile, there's a line that tells your client how to authenticate. Some organizations use RSA keys, but nearly every consumer VPN requires a username and password. With a single change to that line, you can store your password and never be prompted to login again.

Bachelor in Paradise season 7 online
August 15, 2021 / by Mark Gill

Latest TV Streaming Popular Posts

How to watch Love Island 2021 online from abroad (stream it free)
May 30, 2019 / by Ian Garland

How to watch Game of Thrones Season 8 free online
April 14, 2019 / by Sam Cook

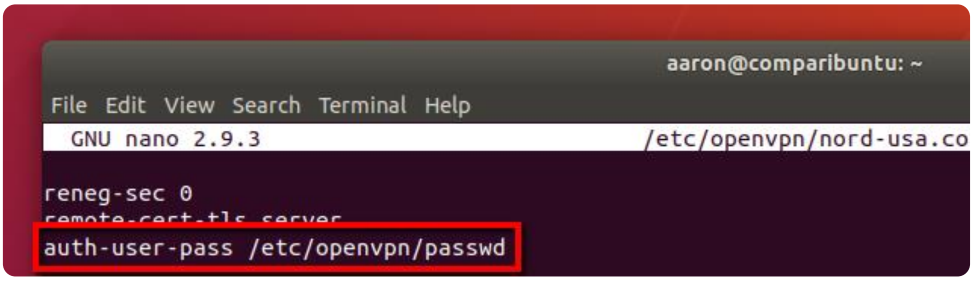
Latest Utilities

6 Best PC tune up software: How to tune up your PC
March 22, 2021 / by Aimee O'Driscoll

How to convert YouTube to MP3
February 18, 2021 / by Aimee O'Driscoll

How to convert SoundCloud to MP3
February 9, 2021 / by Aimee O'Driscoll

6 Best screen recorders for Windows 10 in 2021
June 23, 2020 / by Aimee O'Driscoll



```
  GNU nano 2.9.3                    /etc/openvpn/nord-usa.co

reneg-sec 0
remote-cert-tls server
auth-user-pass /etc/openvpn/passwd
```

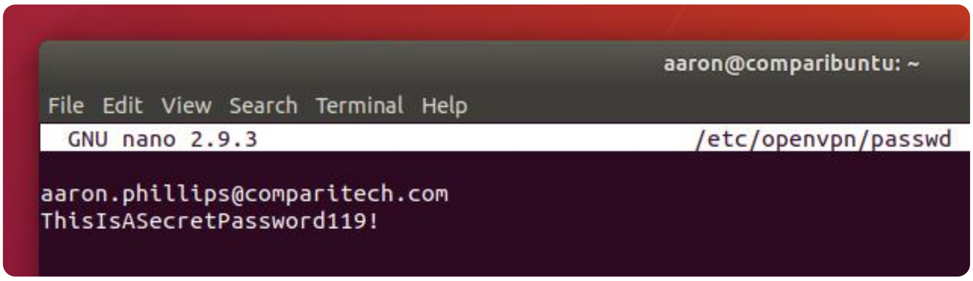
Best video downloaders for Windows 10 in 2021
June 16, 2020 / by Aimee O'Driscoll

Start by opening your OpenVPN profile for editing. You'll want to substitute the proper filename, but I used this command:

```
sudo nano /etc/openvpn/nord–usa.conf
```

Scroll until you find the line that says **auth-user-pass**, and change it to read like this:

```
auth–user–pass /etc/openvpn/passwd
```



```
  GNU nano 2.9.3                    /etc/openvpn/passwd

aaron.phillips@comparitech.com
ThisIsASecretPassword119!
```

That tells OpenVPN to look at **/etc/openvpn/passwd** for your credentials. All you need to do is create that file with your username and password and OpenVPN will connect automatically. Use this command to create the file and open it for editing:

```
sudo nano /etc/openvpn/passwd
```

The structure is very simple, your username is on the first line and your password is on the second. Make sure it looks like mine above, then save with **Ctrl+X**, **Y**.

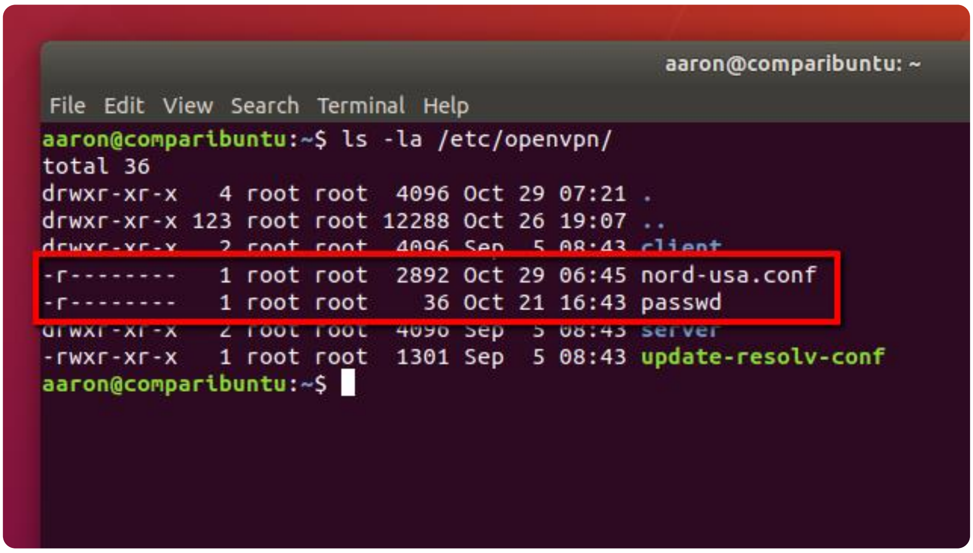
Now try to connect again using this command, substituting the name of your config:

```
sudo systemctl start openvpn@nord-usa
```

You'll notice there are no more username and password prompts and your VPN session starts immediately.

Lock down the config

Anytime you store a username and password in a plaintext file, you'll want to lock it down to make sure unauthorized users can't get access. It's also a good idea to ensure that the file in question is owned by the root user. Note that this represents the minimum amount of security—hashing the file is a better option, but it's beyond the scope of this guide.



```
aaron@comparibuntu:~$ ls -la /etc/openvpn/
total 36
drwxr-xr-x   4 root root  4096 Oct 29 07:21 .
drwxr-xr-x 123 root root 12288 Oct 26 19:07 ..
drwxr-xr-x   2 root root  4096 Sep  5 08:43 client
-r--------   1 root root  2892 Oct 29 06:45 nord-usa.conf
-r--------   1 root root    36 Oct 21 16:43 passwd
drwxr-xr-x   2 root root  4096 Sep  5 08:43 server
-rwxr-xr-x   1 root root  1301 Sep  5 08:43 update-resolv-conf
aaron@comparibuntu:~$ 
```

To lock down the config, you'll want to take the following steps:

- Change ownership of /etc/openvpn/passwd and your VPN profile to the root user

- Change permissions on both files to restrict access

When you’ve finished, your directory listing should look like mine above.

In order to change ownership, you’ll use the **chown** command like this, substituting the name of your OpenVPN profile for mine:

```
sudo chown root:root /etc/openvpn/nord-usa.conf

sudo chown root:root /etc/openvpn/passwd
```

Setting the ownership to root will prevent users from changing the permissions to something less secure. The correct permissions will only allow the root user to read the file, which is all OpenVPN needs to be able to connect when it’s being run as a service. No other users on your system will be able to see the plaintext credentials.

To change permissions, use these commands:

```
sudo chmod 400 /etc/openvpn/nord-usa.conf

sudo chmod 400 /etc/openvpn/passwd
```

Once you’re finished, list the contents of the OpenVPN directory with this command:

```
ls -la /etc/openvpn/
```

You’ll see that the owner is now root, and only root has read access to the files. Once you’re finished locking down the file permissions, it’s safe to set OpenVPN to automatically start on boot.

Connecting to your VPN automatically

All that’s left is to tell systemd that you’d like OpenVPN to connect when your computer boots up. You can do that with a single command, substituting the name of your profile for **nord-usa**:

```
sudo systemctl enable openvpn@nord-usa
```

You’re finished, and OpenVPN will now connect every time you start your computer. It’s fully protected by the UFW kill switch, and you can be sure that no unencrypted traffic will leave the network from your workstation.

Top image licensed for reuse by Codeproject.com

1 Comment

Leave a comment

Alex
August 22, 2021 at 6:29 pm

Thank you for the guide.

I'm having troubles trying to set the firewall rule
sudo ufw allow out to 107.152.104.216 port 1194 proto udp

I don't have IP address in my VPN's config. There is a usual internet address instead:

proto udp
remote at-vie.prod.surfshark.com 1194

So the command "sudo ufw allow…" fails.

What can I do?
Thanks.

Reply ▸

Leave a Reply

Comment

Name *

Leave Comment

This site uses Akismet to reduce spam. Learn how your comment data is processed.

comparitech

Home | Blog | Authors | Privacy policy | Cookies Policy | Terms of use | Disclosure | About Comparitech | Contact Us

Comparitech.com is owned and operated by Comparitech Limited, a registered company in England and Wales (Company No. 09962280), Suite 3 Falcon Court Business Centre, College Road, Maidstone, Kent, ME15 6TF, United Kingdom. Telephone +44(0)333 577 0163