VPN

A **Virtual Private Network (VPN)** is a technology that creates a secure and encrypted connection over a less secure network, such as the internet. It enables users to send and receive data across shared or public networks as if their computing devices were directly connected to a private network.

By routing the network traffic through a VPN server located anywhere in the world, it not only secures data from eavesdropping but also allows for remote access to network resources and the bypassing of internet censorship or geo-restrictions. VPNs are widely used in both corporate and personal settings to protect sensitive data and enhance privacy.Aptos Narrow

VPN Protocols

- **IPSec (Internet Protocol Security) :** IPSec is a suite of protocols designed to secure Internet Protocol (IP) communications by authenticating and encrypting each IP packet in a data stream.

- **L2TP/IPSec (Layer 2 Tunneling Protocol with IPSec)** : L2TP/IPSec combines the Layer 2 Tunneling Protocol (L2TP) with IPSec encryption to provide a highly secure VPN connection.

- **IKEv2/IPSec (Internet Key Exchange version 2 with IPSec) :** IKEv2/IPSec is a VPN protocol that provides a secure key exchange session, establishing IPSec encryption parameters.

- **OpenVPN:** OpenVPN is an open-source VPN protocol known for its flexibility and strong security. It utilizes SSL/TLS for key exchange, allowing it to traverse firewalls and network address translators (NATs) more easily than some other protocols.

- **WireGuard:** WireGuard is a newer, open-source VPN protocol that aims for simplicity and high performance.

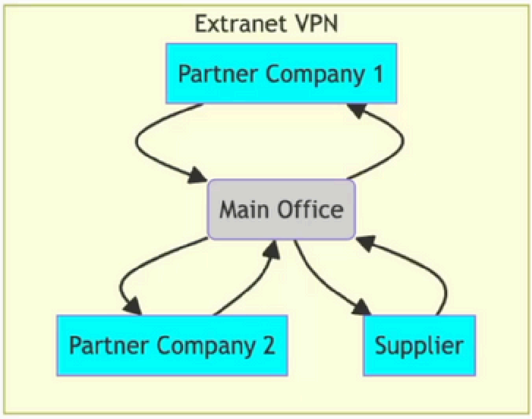
Site-to-Site VPN

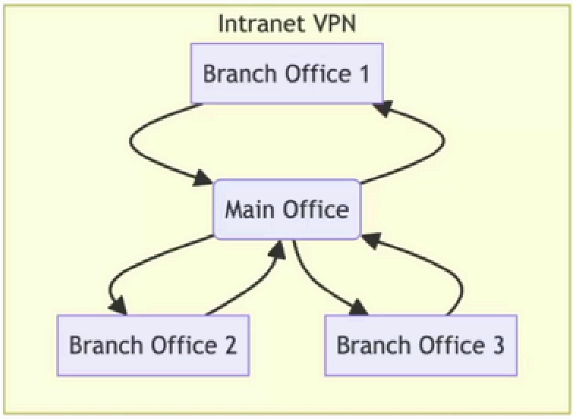
A **VPN site-to-site**, or site-to-site virtual private network, is a networking technology that allows the connection of multiple remote networks over a public network infrastructure, typically the internet. This setup enables secure communication between geographically distributed sites, such as branch offices, data centers, or partner locations, as if they were directly connected on the same local network. There are two main types of site-to-site VPNs:

Intranet and Extranet:

An intranet VPN connects networks belonging to a single organization, allowing seamless communication and resource sharing between various company locations. On the other hand, an extranet VPN extends this connectivity to include networks of external partners, suppliers, or customers, enabling controlled access to shared resources while maintaining security and privacy boundaries between different organizations. Both types of site-to-site VPNs employ encryption and tunneling protocols to ensure confidentiality, integrity, and authenticity of transmitted data across the interconnected networks.

Site-to-Site VPN





VPN types

- **P2P Network:** A P2P network enables direct device-to-device connections, facilitating decentralized and efficient data sharing.

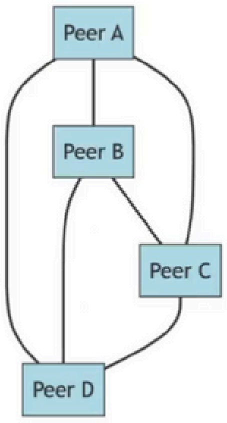
- **Remote Access Network:** Remote Access Networks provide secure access to a private network's resources from remote locations via the internet.

- **MPLS Network:** MPLS is a routing technique that speeds up data transmission by using short path labels rather than long network addresses.

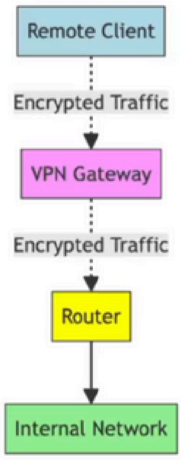
- **Hybrid VPN:** A Hybrid VPN combines traditional VPN elements with direct cloud connections to optimize access to both private network and public cloud resources.

- **SD-WAN VPN:** SD-WAN technology uses software to control connectivity, management, and services between data centers and branches, enhancing network performance and reducing operational costs.

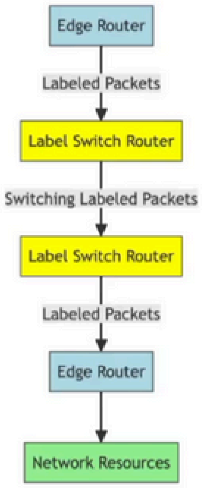
VPN Types



P2P



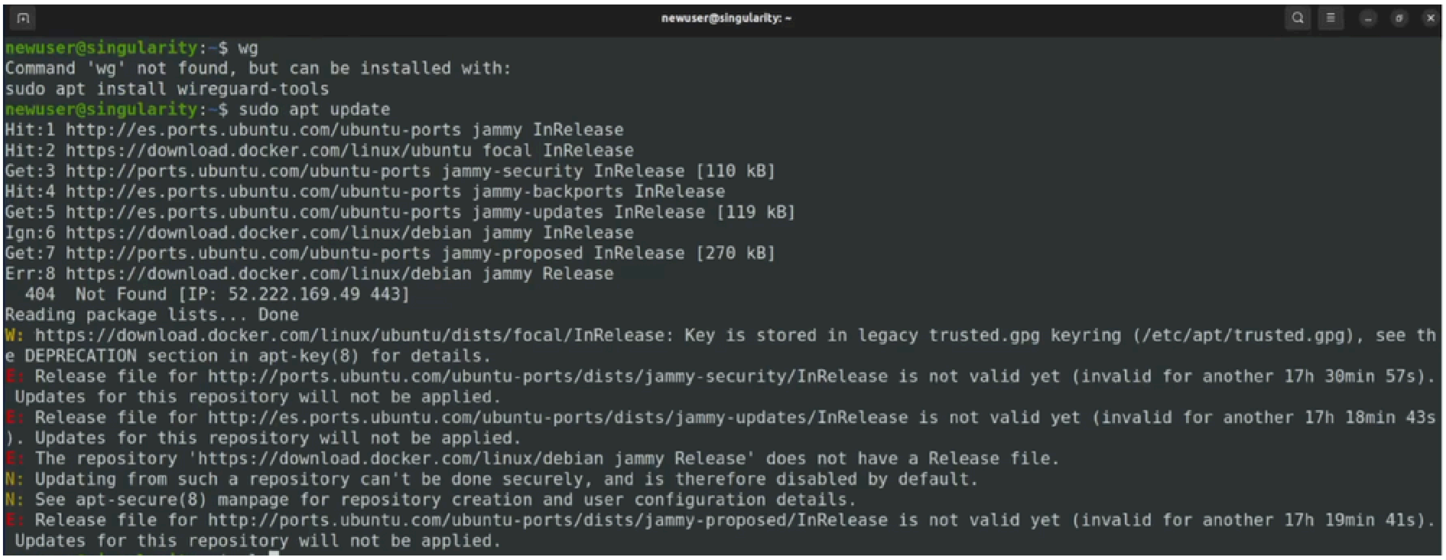
Remote Access VPN



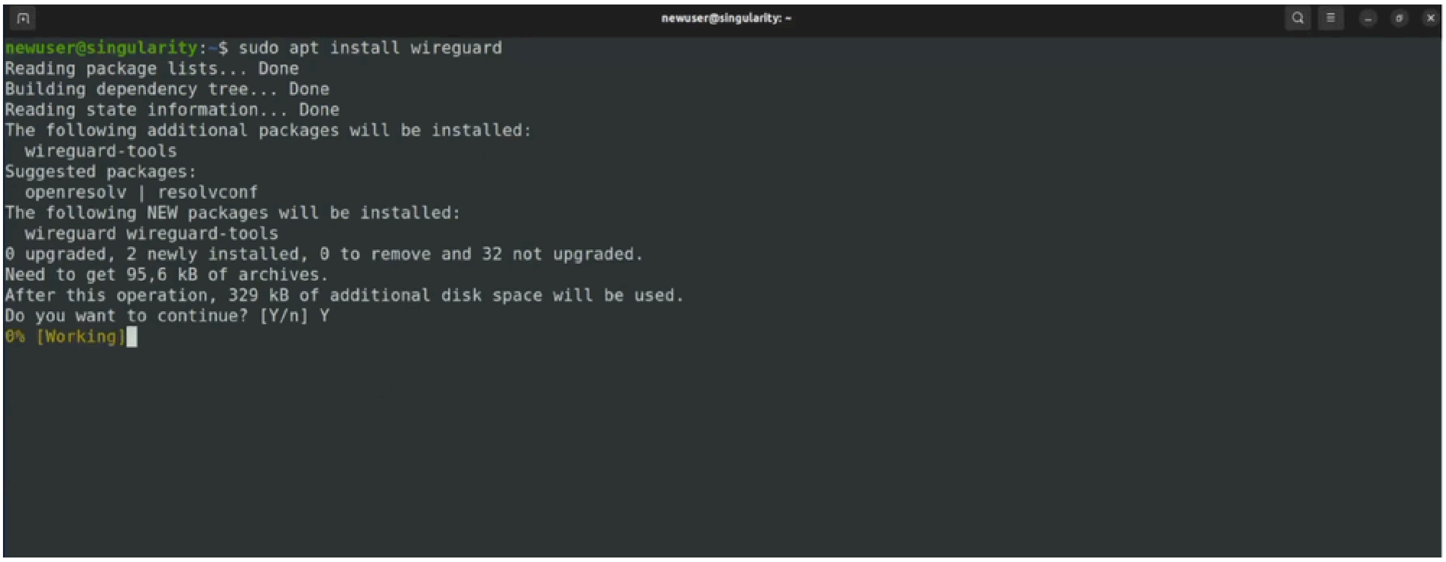
MPLS

WireGuard

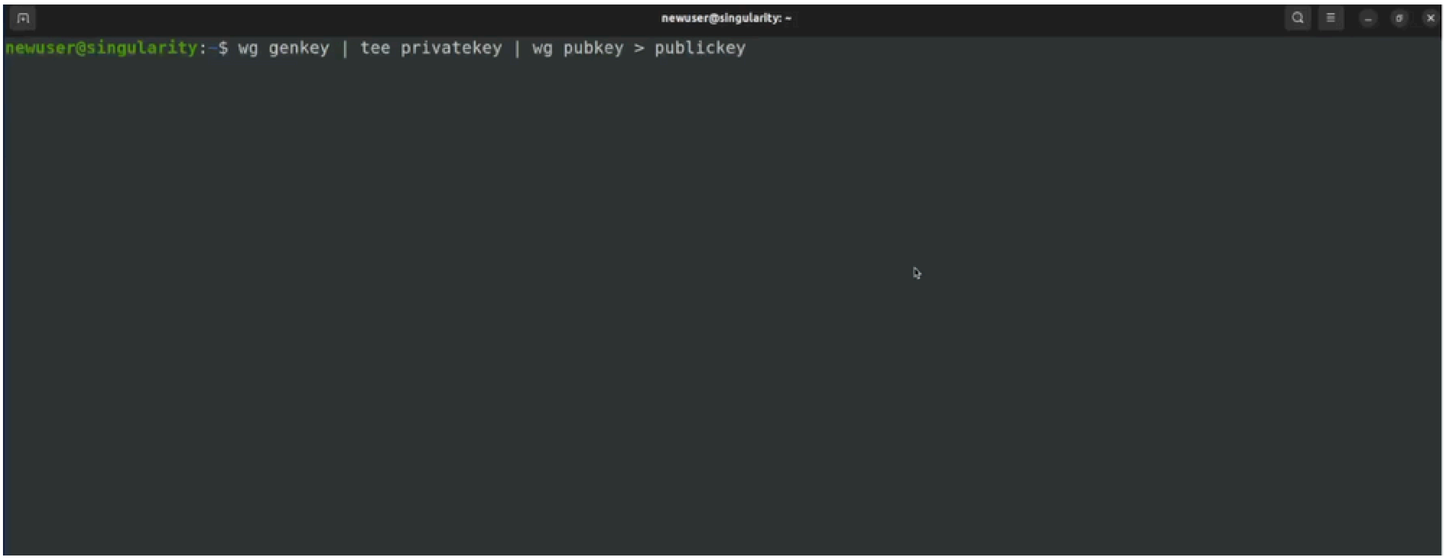
WireGuard stands out as a modern and efficient VPN protocol renowned for its simplicity, speed, and strong security features. Its importance lies in offering a streamlined and secure solution for establishing encrypted connections, catering to the growing demands of privacy-conscious users and organizations in today's digital landscape.



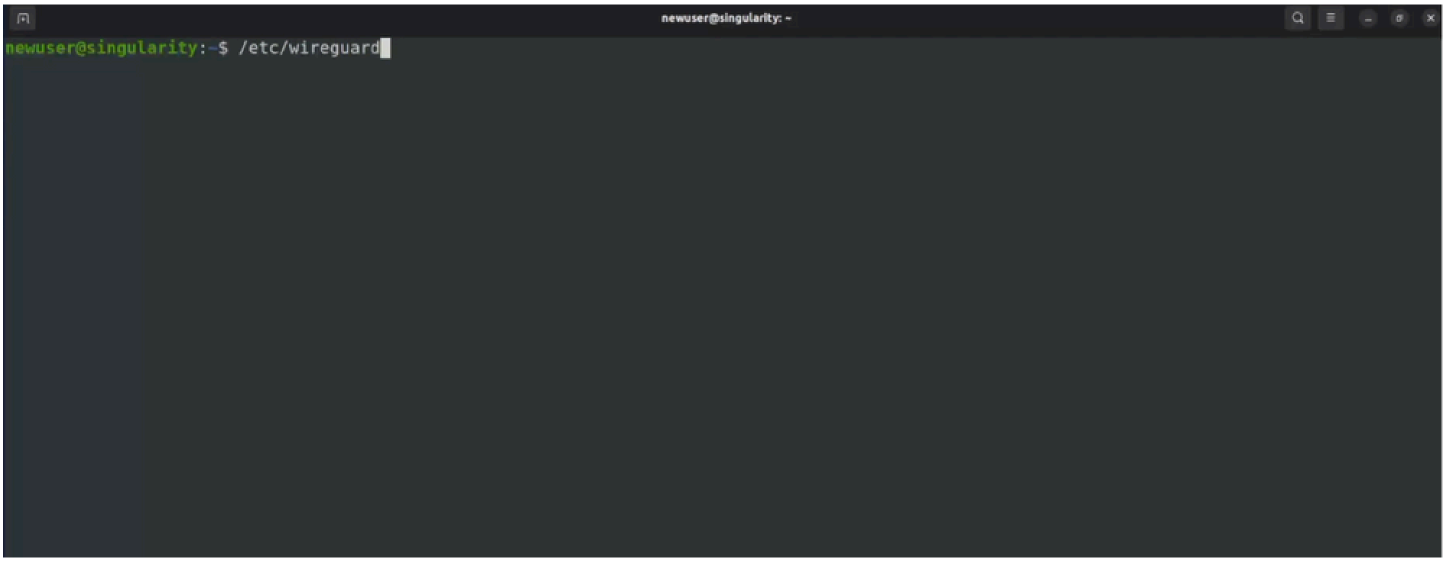
```
newuser@singularity:~$ wg
Command 'wg' not found, but can be installed with:
sudo apt install wireguard-tools
newuser@singularity:~$ sudo apt update
Hit:1 http://es.ports.ubuntu.com/ubuntu-ports jammy InRelease
Hit:2 https://download.docker.com/linux/ubuntu focal InRelease
Get:3 http://ports.ubuntu.com/ubuntu-ports jammy-security InRelease [110 kB]
Hit:4 http://es.ports.ubuntu.com/ubuntu-ports jammy-backports InRelease
Get:5 http://es.ports.ubuntu.com/ubuntu-ports jammy-updates InRelease [119 kB]
Ign:6 https://download.docker.com/linux/debian jammy InRelease
Get:7 http://ports.ubuntu.com/ubuntu-ports jammy-proposed InRelease [270 kB]
Err:8 https://download.docker.com/linux/debian jammy Release
  404  Not Found [IP: 52.222.169.49 443]
Reading package lists... Done
W: https://download.docker.com/linux/ubuntu/dists/focal/InRelease: Key is stored in legacy trusted.gpg keyring (/etc/apt/trusted.gpg), see th
e DEPRECATION section in apt-key(8) for details.
E: Release file for http://ports.ubuntu.com/ubuntu-ports/dists/jammy-security/InRelease is not valid yet (invalid for another 17h 30min 57s).
 Updates for this repository will not be applied.
E: Release file for http://es.ports.ubuntu.com/ubuntu-ports/dists/jammy-updates/InRelease is not valid yet (invalid for another 17h 18min 43s
). Updates for this repository will not be applied.
E: The repository 'https://download.docker.com/linux/debian jammy Release' does not have a Release file.
N: Updating from such a repository can't be done securely, and is therefore disabled by default.
N: See apt-secure(8) manpage for repository creation and user configuration details.
E: Release file for http://ports.ubuntu.com/ubuntu-ports/dists/jammy-proposed/InRelease is not valid yet (invalid for another 17h 19min 41s).
 Updates for this repository will not be applied.
```



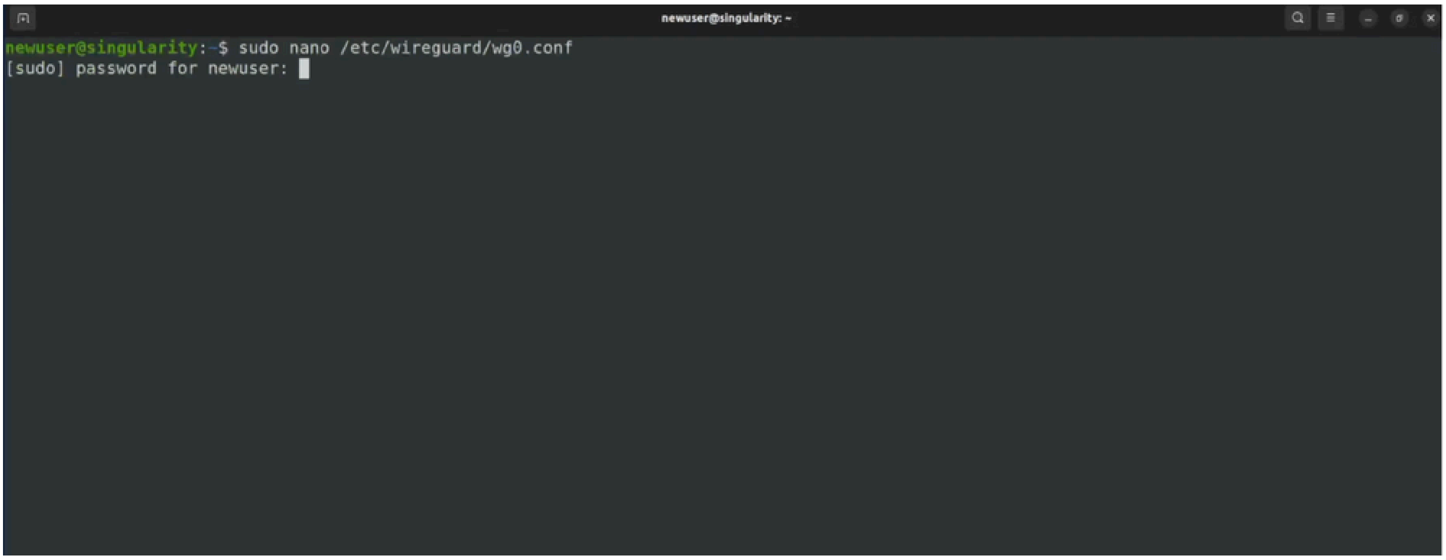
```
newuser@singularity:~$ sudo apt install wireguard
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  wireguard-tools
Suggested packages:
  openresolv | resolvconf
The following NEW packages will be installed:
  wireguard wireguard-tools
0 upgraded, 2 newly installed, 0 to remove and 32 not upgraded.
Need to get 95,6 kB of archives.
After this operation, 329 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
0% [Working]
```



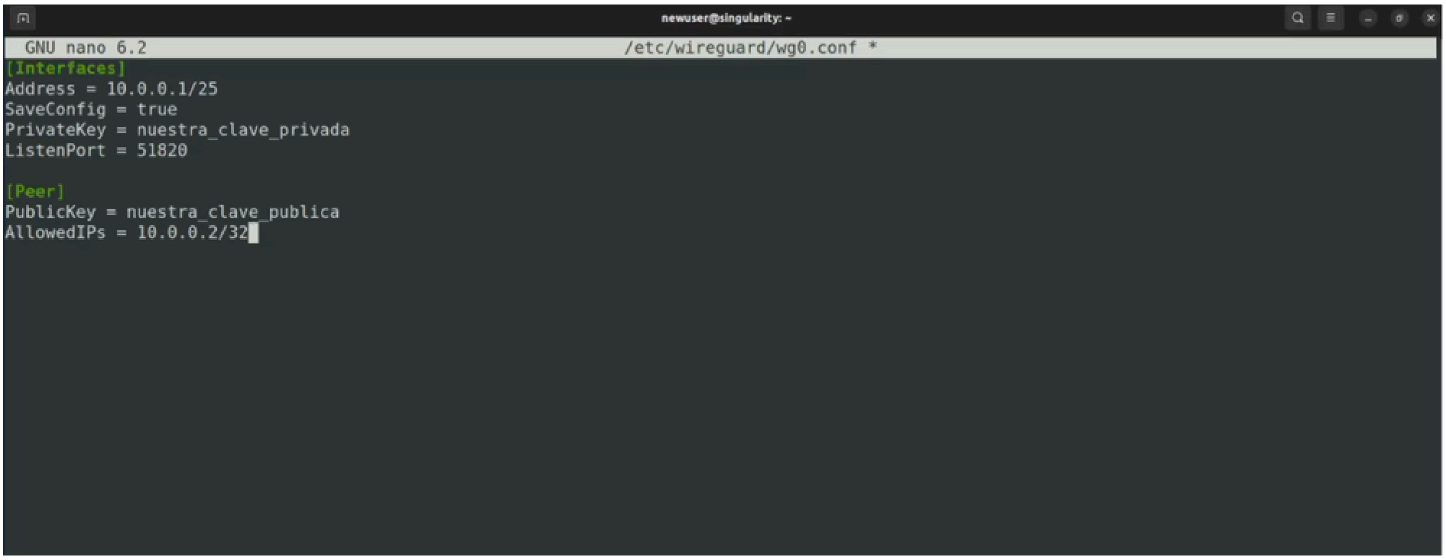
```
newuser@singularity:~$ wg genkey | tee privatekey | wg pubkey > publickey
```



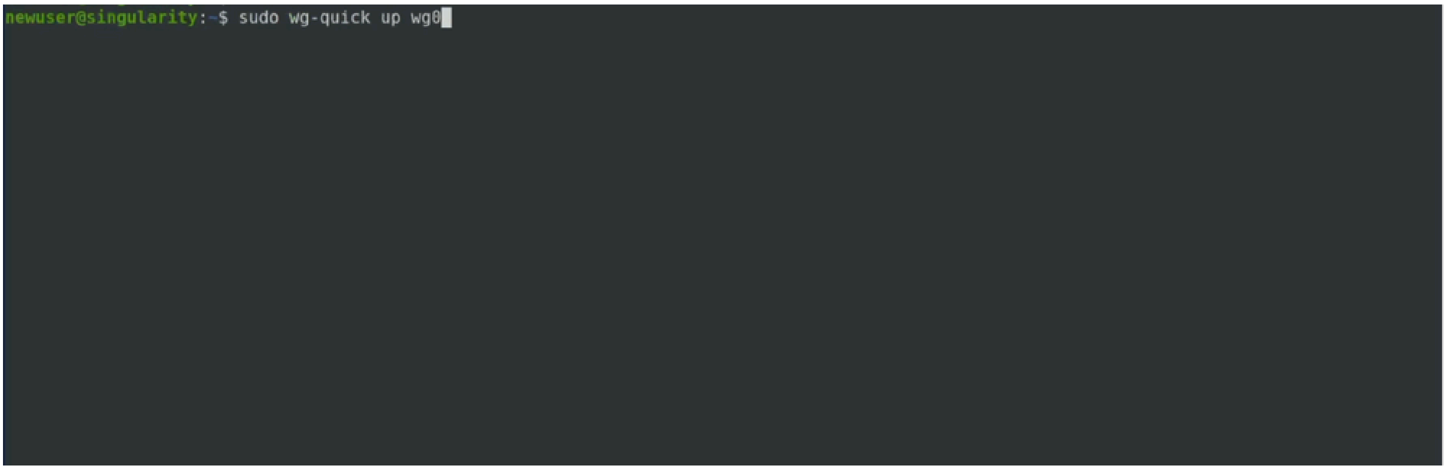
```
newuser@singularity:~$ /etc/wireguard
```



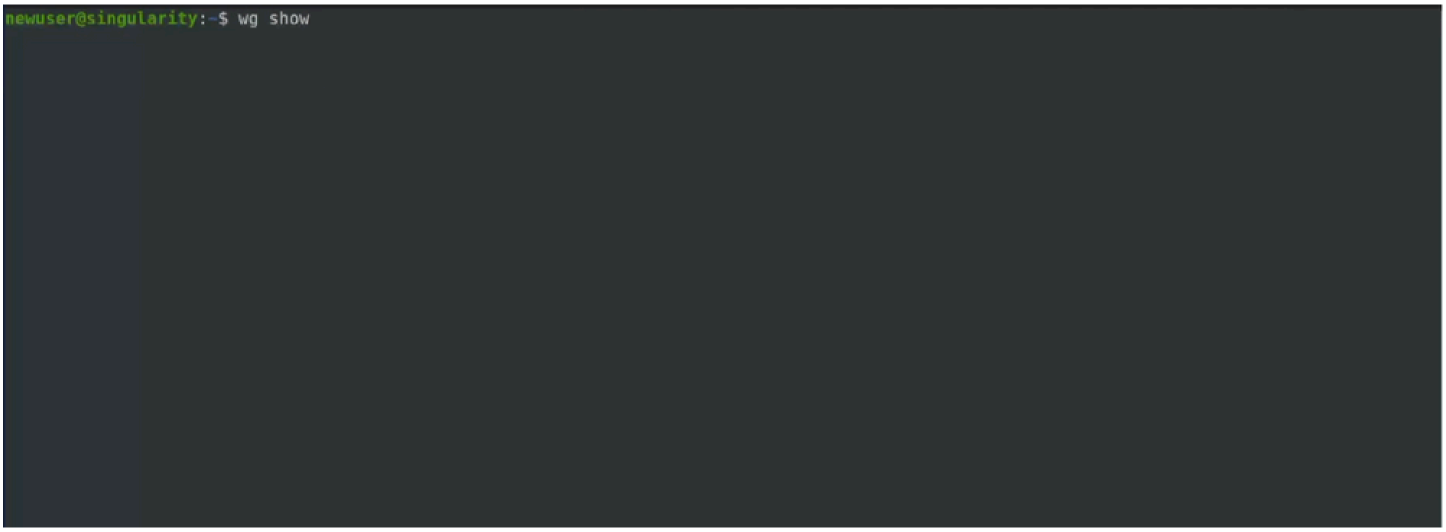
```
newuser@singularity:~$ sudo nano /etc/wireguard/wg0.conf
[sudo] password for newuser:
```



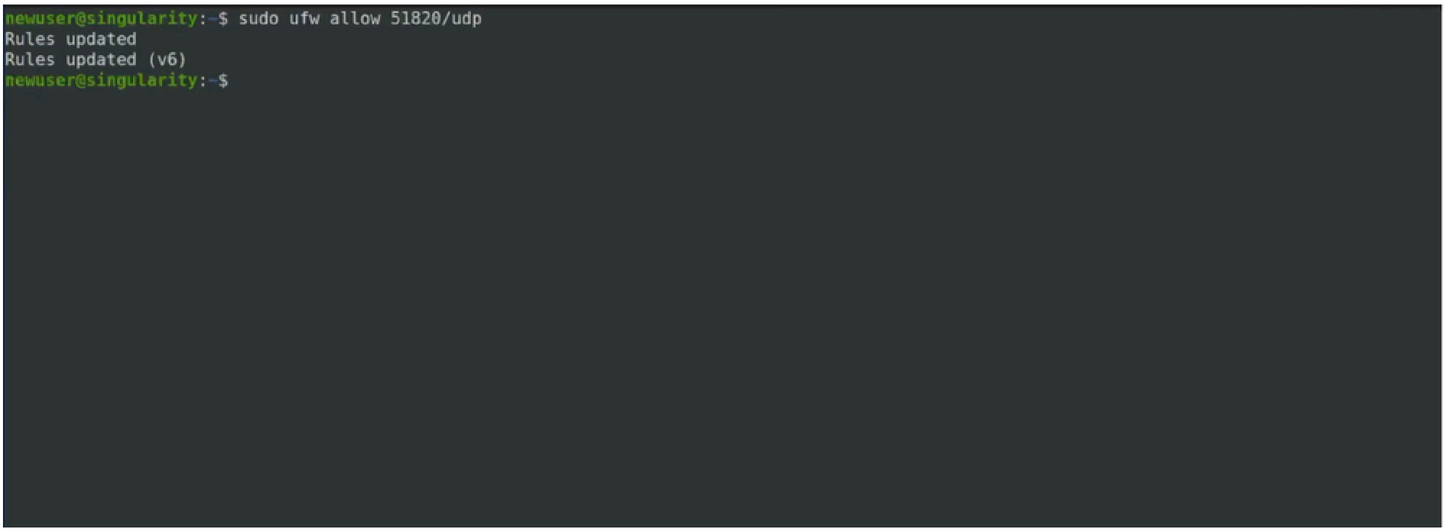
```
  GNU nano 6.2                                          /etc/wireguard/wg0.conf *
[Interfaces]
Address = 10.0.0.1/25
SaveConfig = true
PrivateKey = nuestra_clave_privada
ListenPort = 51820

[Peer]
PublicKey = nuestra_clave_publica
AllowedIPs = 10.0.0.2/32
```



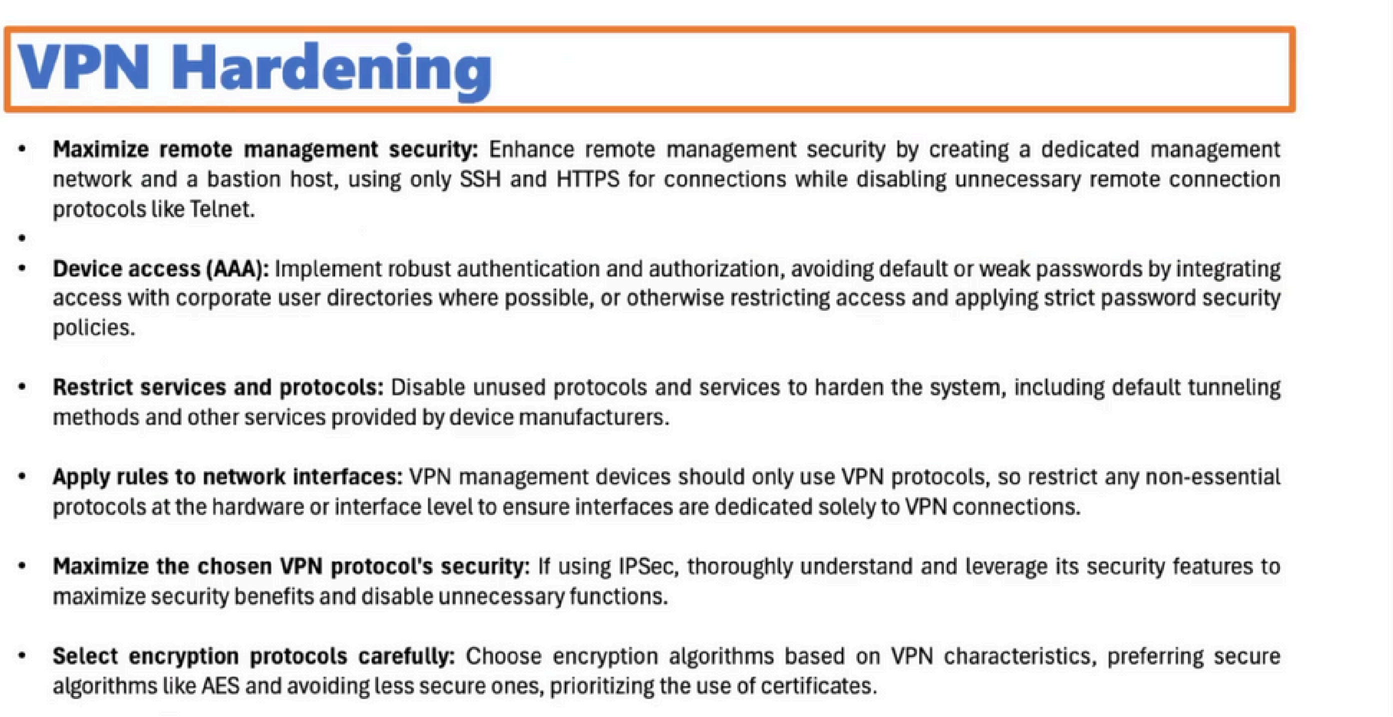
```
newuser@singularity:~$ sudo wg-quick up wg0
```



```
newuser@singularity:~$ wg show
```



```
newuser@singularity:~$ sudo ufw allow 51820/udp
Rules updated
Rules updated (v6)
newuser@singularity:~$
```



VPN Hardening

- **Maximize remote management security:** Enhance remote management security by creating a dedicated management network and a bastion host, using only SSH and HTTPS for connections while disabling unnecessary remote connection protocols like Telnet.
-
- **Device access (AAA):** Implement robust authentication and authorization, avoiding default or weak passwords by integrating access with corporate user directories where possible, or otherwise restricting access and applying strict password security policies.
- **Restrict services and protocols:** Disable unused protocols and services to harden the system, including default tunneling methods and other services provided by device manufacturers.
- **Apply rules to network interfaces:** VPN management devices should only use VPN protocols, so restrict any non-essential protocols at the hardware or interface level to ensure interfaces are dedicated solely to VPN connections.
- **Maximize the chosen VPN protocol's security:** If using IPSec, thoroughly understand and leverage its security features to maximize security benefits and disable unnecessary functions.
- **Select encryption protocols carefully:** Choose encryption algorithms based on VPN characteristics, preferring secure algorithms like AES and avoiding less secure ones, prioritizing the use of certificates.