

Cómo instalar un Servidor VPN en 5 minutos

para una pequeña empresa

Elio Rojano



<https://sinologic.net>

```
hellc2@sinologic:~$ whoami
```

VoIP, SIP, WebRTC
Asterisk, Kamailio,
Python, Javascript, PHP
OpenSource



Elio Rojano

@hellc2

erojano@sinologic.net

```
hellc2@sinologic:~$ links
```

<https://www.sinologic.net/>

<https://es.slideshare.net/hellc2/>

<https://www.linkedin.com/in/rojano/>

<http://www.VOZ.com/>

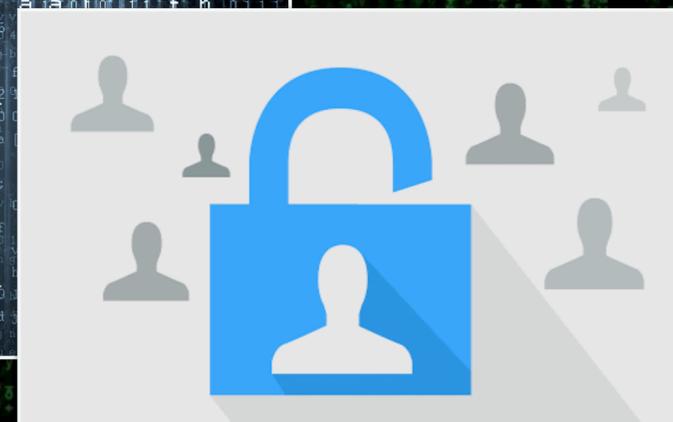
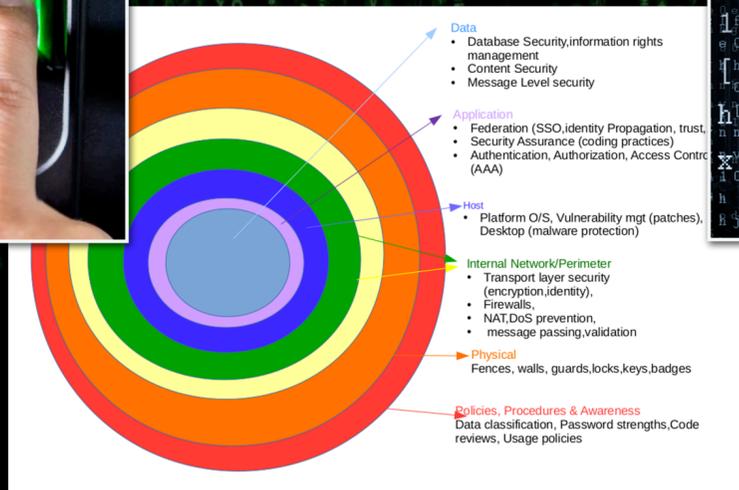


Motivación



La oficina es un “lugar seguro”

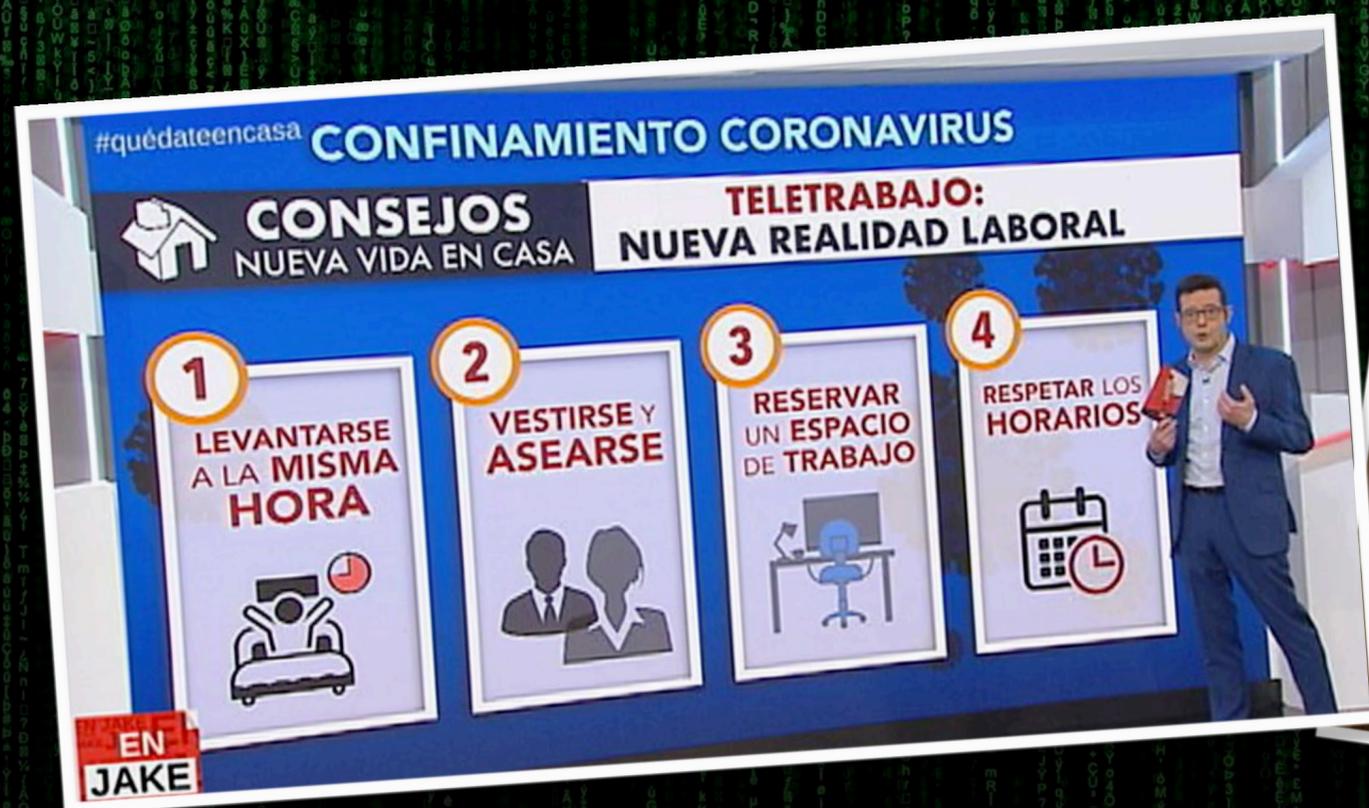
- Acceso restringido al interior de la oficina
- Datos confidenciales dentro de la red interna
- Firewall/SBC para control de acceso exterior
- Uso de protocolos y sistemas de cifrado para las comunicaciones internas y externas
- Departamento responsable de la seguridad informática
- etc...



El SARS-CoV2 ha obligado a “teletrabajar” a todos aquellos que podían

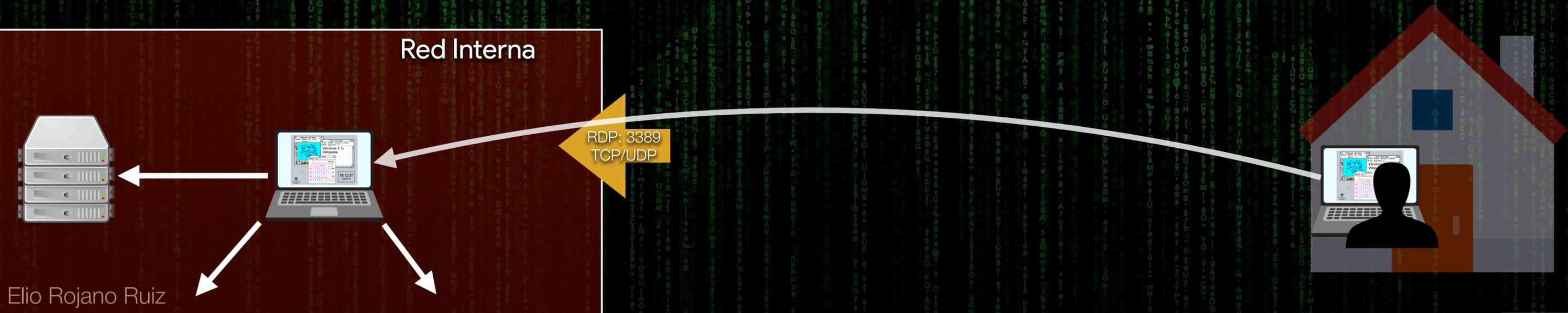


Todos los que podían trabajar desde sus casas han tenido que adaptarse de la noche a la mañana a esta situación para poder seguir trabajando



Muchas empresas tenían que seguir trabajando pero desde casa: ¿Solución?

Abrir puertos y hacer uso de sistemas remotos...
Teamviewer, RDP, Terminal Server, etc.





Herramientas básicas

Comunicaciones



- Sistema de **Correo electrónico**



- Sistema de **Mensajería instantánea**



- Sistema de **Telefonía VoIP**



- Sistema de **Videoconferencia**



Pero...

¿Cómo se accede a la información de la empresa?

Fichas de clientes

Aplicaciones

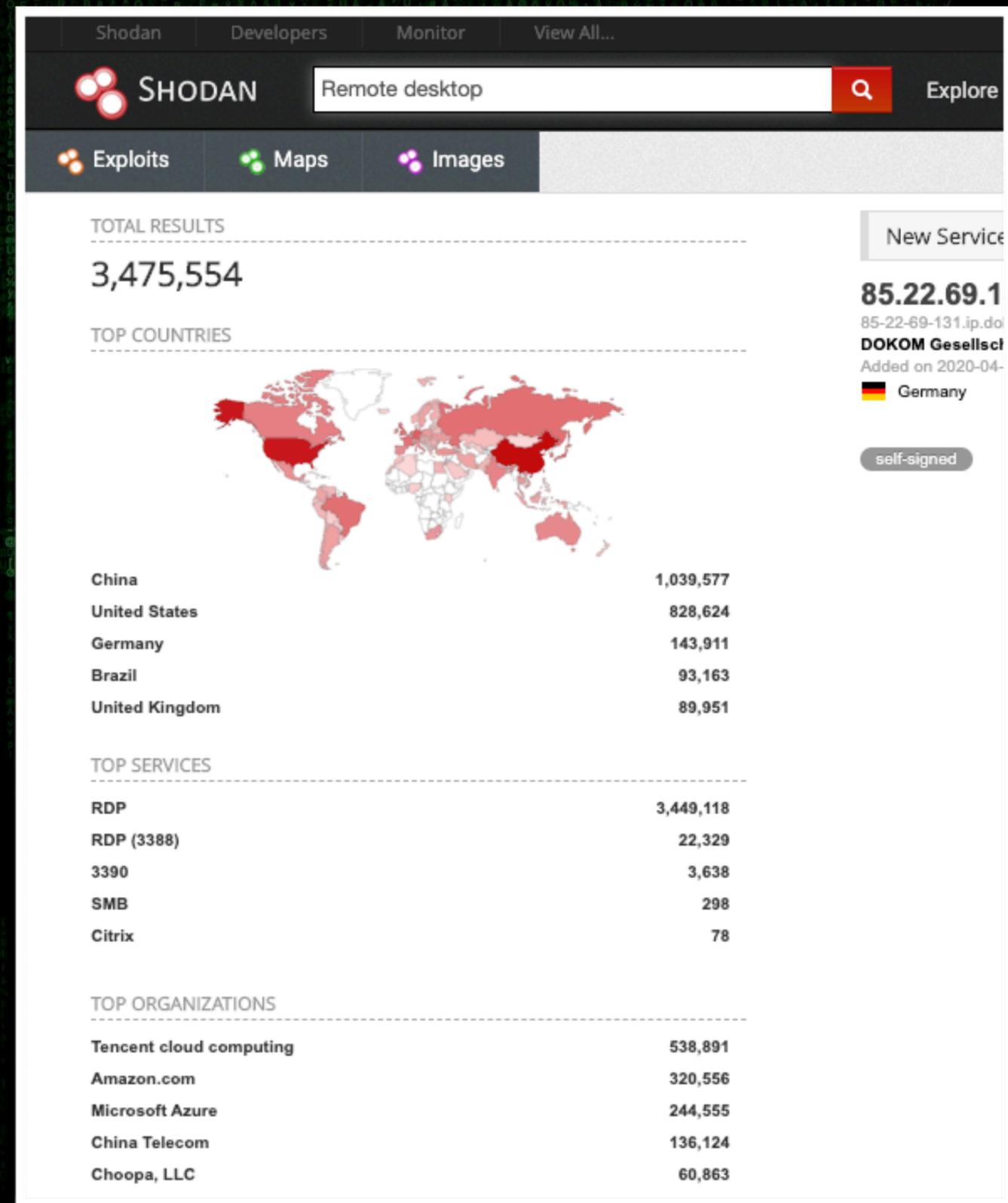
Facturas

Listados de proveedores

Tickets

Documentación

Esto ha dado
como resultado
un gran número
de sistemas
vulnerables en
Internet



The screenshot shows the Shodan search engine interface. At the top, there are navigation tabs for 'Shodan', 'Developers', 'Monitor', and 'View All...'. The search bar contains the text 'Remote desktop' and a search icon. Below the search bar, there are tabs for 'Exploits', 'Maps', and 'Images'. The main content area displays the following information:

- TOTAL RESULTS:** 3,475,554
- TOP COUNTRIES:** A world map with red highlights indicating the top countries. Below the map is a table:

Country	Count
China	1,039,577
United States	828,624
Germany	143,911
Brazil	93,163
United Kingdom	89,951

- TOP SERVICES:** A table showing the top services:

Service	Count
RDP	3,449,118
RDP (3388)	22,329
3390	3,638
SMB	298
Citrix	78

- TOP ORGANIZATIONS:** A table showing the top organizations:

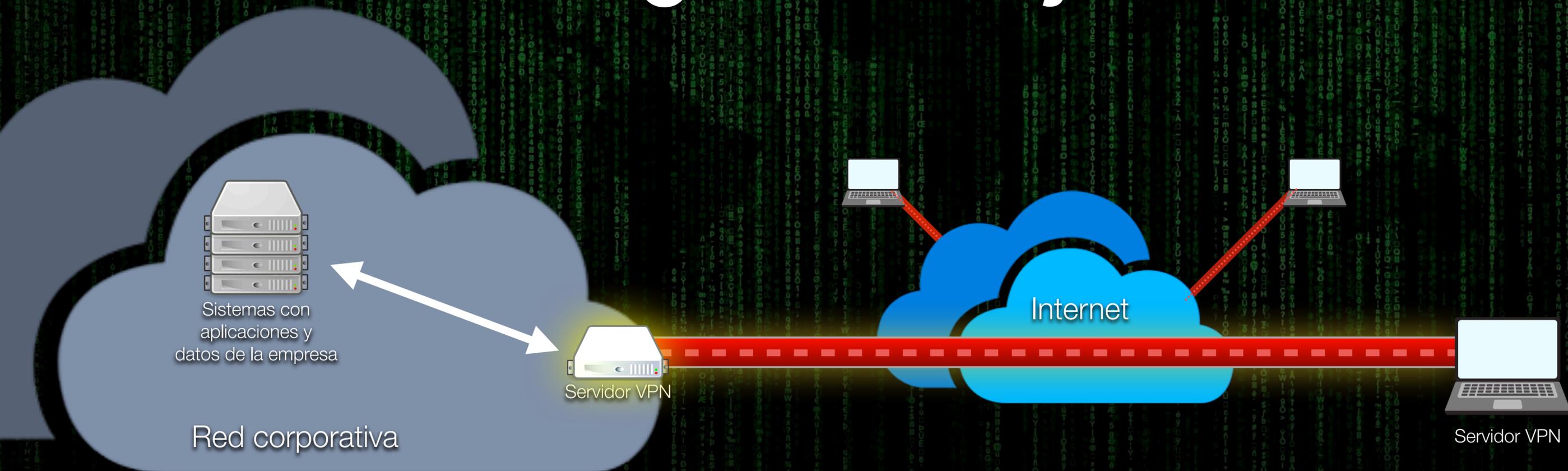
Organization	Count
Tencent cloud computing	538,891
Amazon.com	320,556
Microsoft Azure	244,555
China Telecom	136,124
Choopa, LLC	60,863

On the right side of the interface, there is a 'New Service' section with the following details:

- IP Address:** 85.22.69.1
- Domain:** 85-22-69-131.ip.dok
- Organization:** DOKOM Gesellscl
- Added on:** 2020-04-
- Country:** Germany
- Signature:** self-signed



Miles de administradores de sistemas empezaron a instalar VPN corporativas para las empresas y que éstas pudieran seguir trabajando.



¿Qué ocurre con las pequeñas empresas que no tienen esta posibilidad?



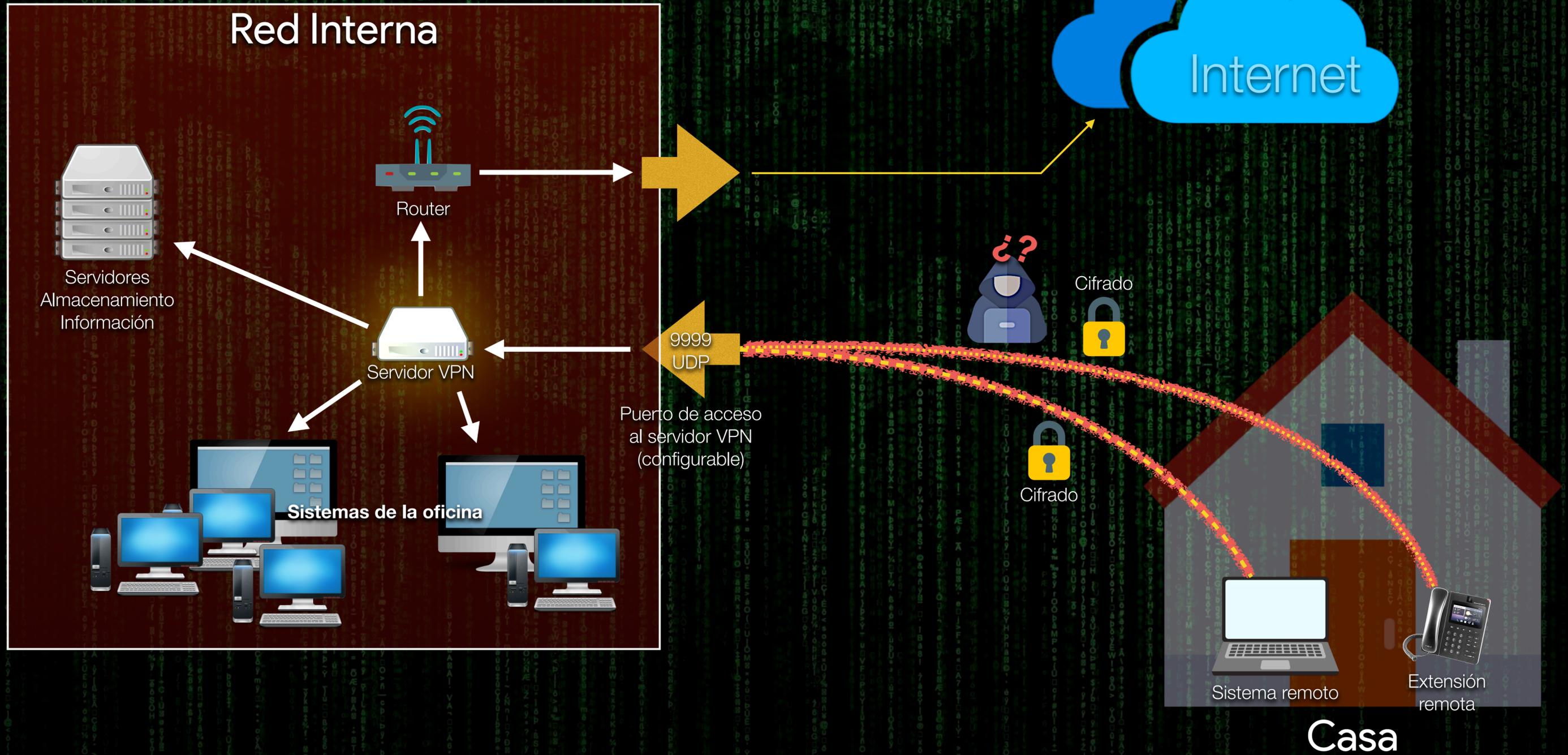


**Montar un servidor VPN corporativo
no es un sistema fácil e intuitivo
para una empresa sin recursos
específicos.**



Idea General

Esquema de la Idea General



Ingredientes:

- **Raspberry PI** (a ser posible RPI4)
- **Acceso a la configuración del Router**
- **Posibilidad de abrir puertos** (CG-NAT?) 😡
- **IP pública y fija** (muy recomendado)
- **Conexión estable y ancho de banda suficiente**
(Necesario para poder transmitir datos de entrada y salida)



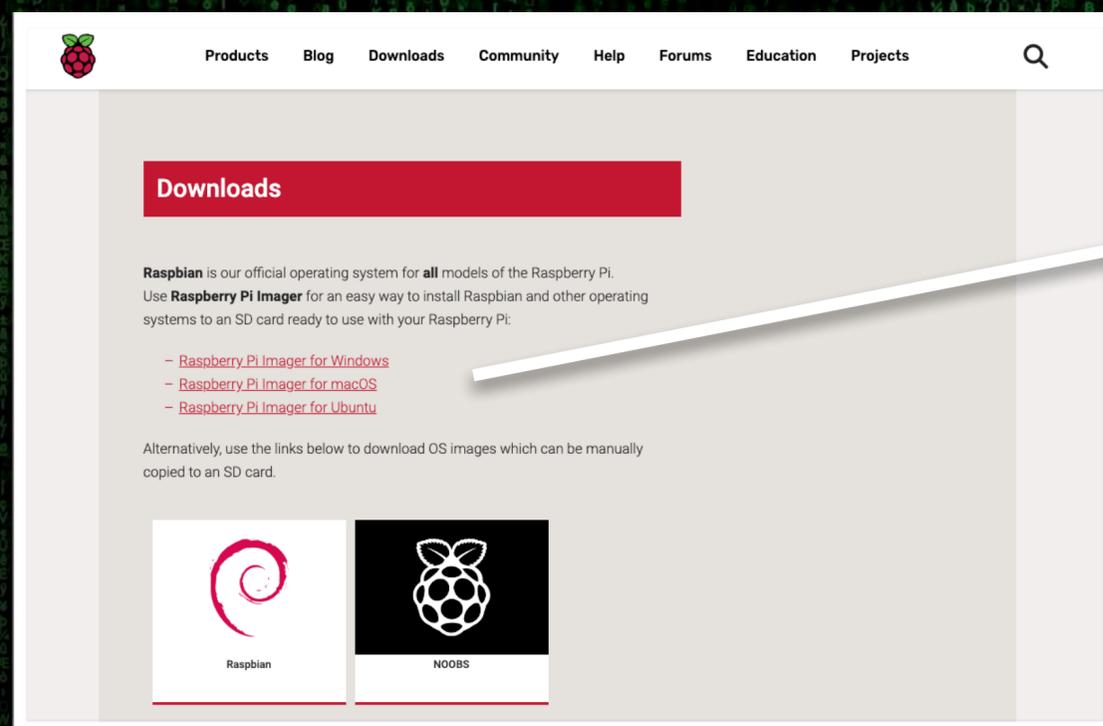
Recomendaciones:

- Uso de un **SAI** para el router y la RPI
- **Recomendable: Redundancia** (otra RPI en otro puerto, por si...)

Preparar servidor VPN:



- **Una tarjeta microSD** (8Gb aprox.)
- Instalar **Raspbian**: (No necesitamos escritorio, tan solo la versión mínima)



- [Raspberry Pi Imager for Windows](#)
- [Raspberry Pi Imager for macOS](#)
- [Raspberry Pi Imager for Ubuntu](#)

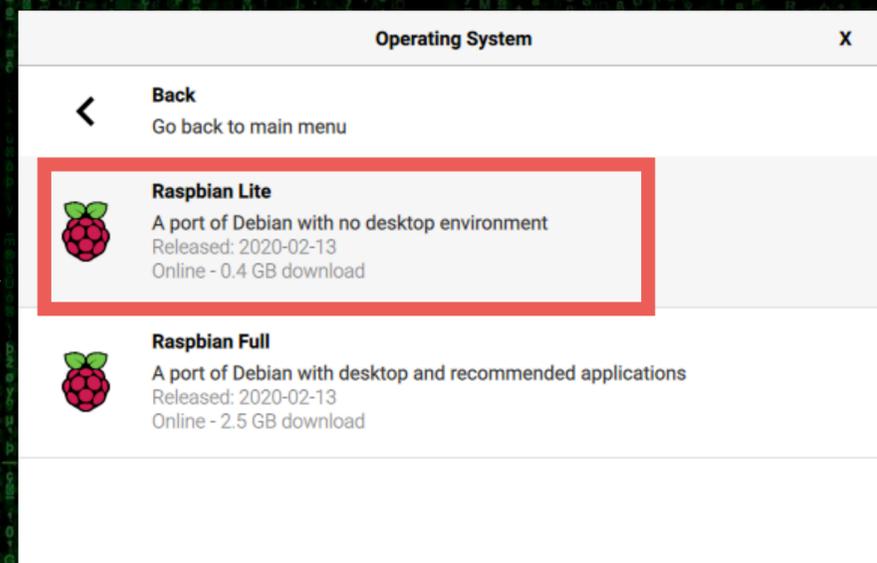
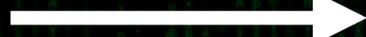
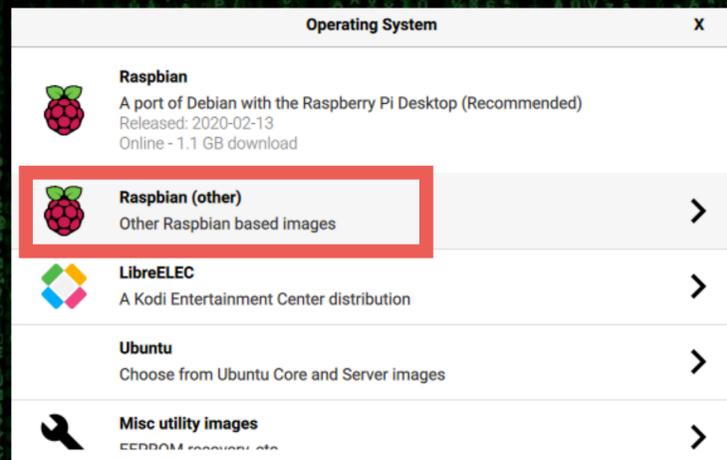
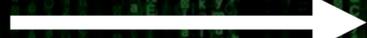
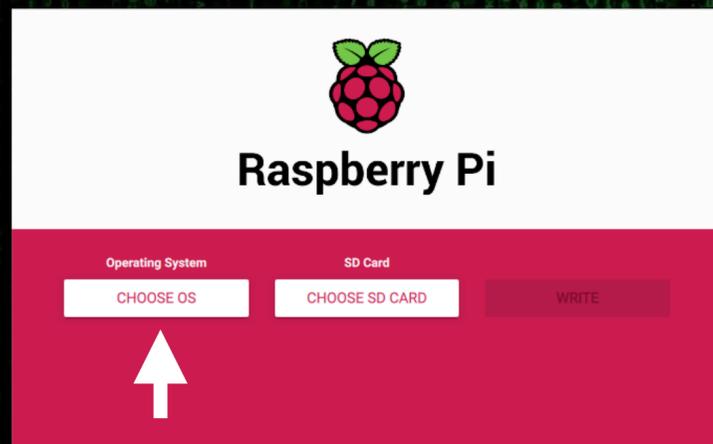
<https://www.raspberrypi.org/downloads/>



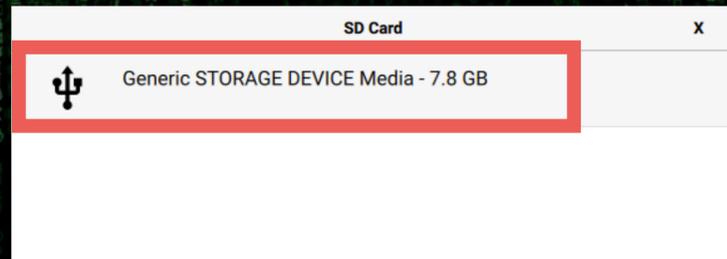
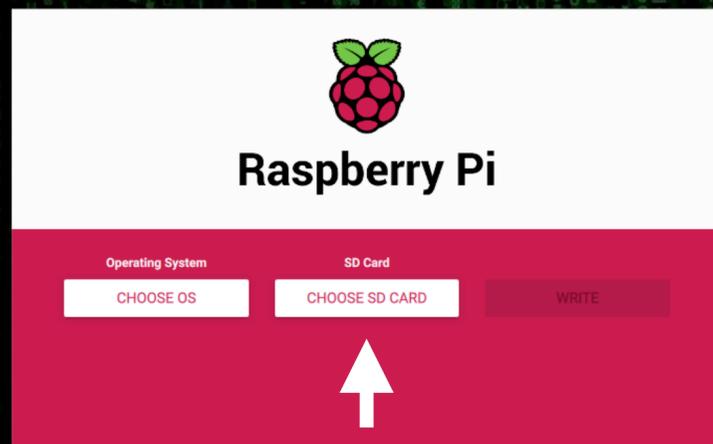
Preparar servidor VPN:



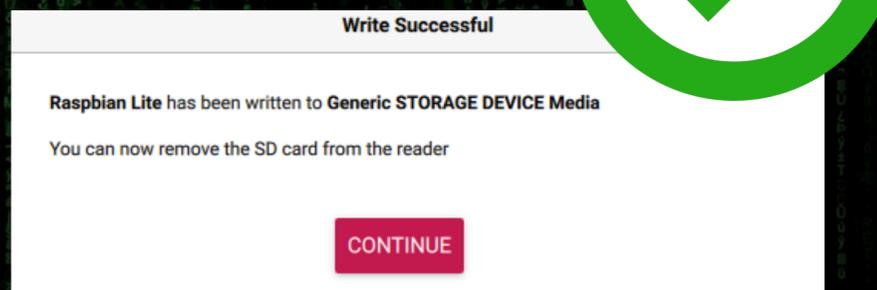
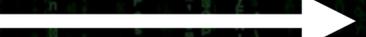
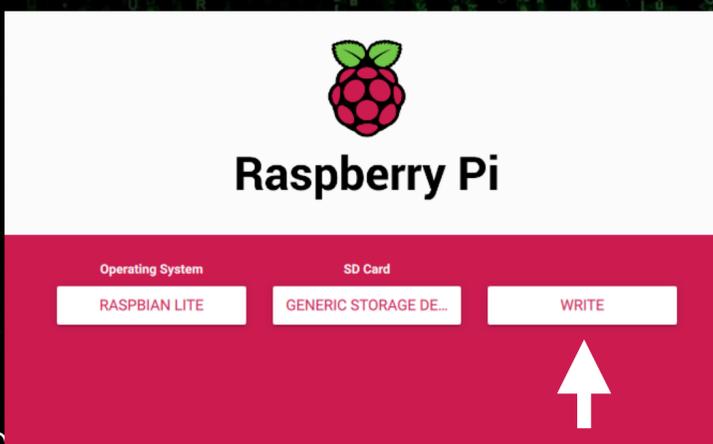
1º



2º



3º



Preparar servidor VPN:



1º. Accedemos a la Raspberry Pi

usuario: **pi**
contraseña: **raspberrry**



2º. Ejecutar **raspi-config** y activar el servidor SSH

```
4 Localisation Options Set up language and regional settings
5 Interfacing Options Configure connections to peripherals
6 Overclock Configure overclocking for your Pi
```



```
P1 Camera Enable/Disable connection to the Raspberry Pi Camera
P2 SSH Enable/Disable remote command line access to your Pi using SSH
P3 VNC Enable/Disable graphical remote access to your Pi using RealVNC
```

3º. Actualizamos repositorio:

```
pi@raspberrry:~$ sudo apt-get update
pi@raspberrry:~$ sudo apt-get upgrade
pi@raspberrry:~$ sudo reboot
```

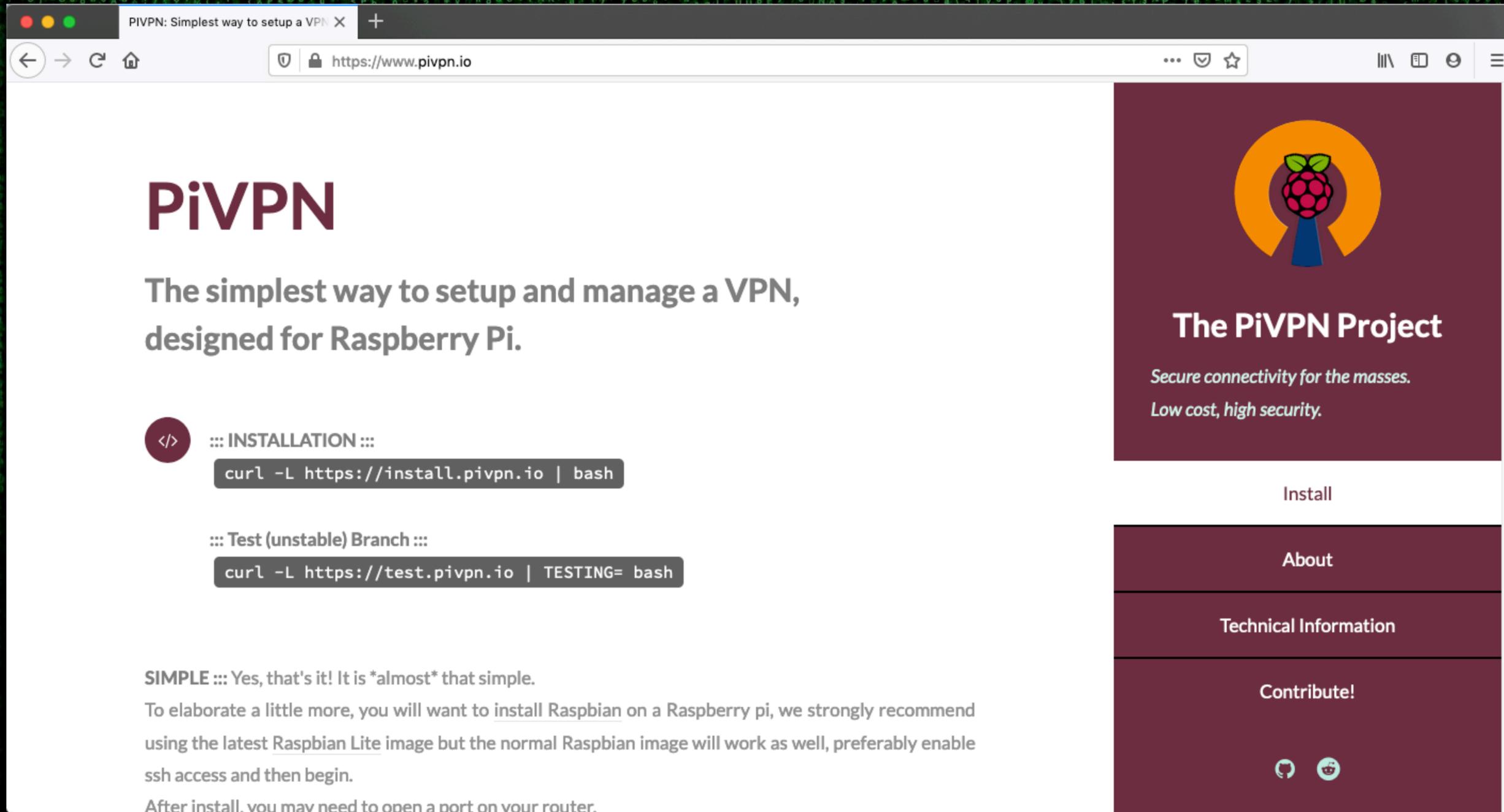


Preparar el servidor VPN

Preparar el servidor VPN

c0r0n4con

Esto lo paramos hackeando



PIVPN: Simplest way to setup a VPN X +

← → ↻ 🏠 <https://www.pivpn.io> ... 🛡️ ☆ 🗑️ 📄 ⌵ ☰

PIVPN

The simplest way to setup and manage a VPN, designed for Raspberry Pi.

 **INSTALLATION**

```
curl -L https://install.pivpn.io | bash
```

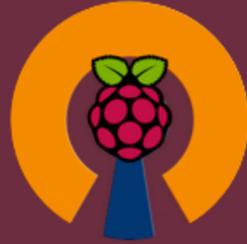
Test (unstable) Branch

```
curl -L https://test.pivpn.io | TESTING= bash
```

SIMPLE ::: Yes, that's it! It is **almost** that simple.

To elaborate a little more, you will want to install Raspbian on a Raspberry pi, we strongly recommend using the latest Raspbian Lite image but the normal Raspbian image will work as well, preferably enable ssh access and then begin.

After install, you may need to open a port on your router.



The PiVPN Project

Secure connectivity for the masses.
Low cost, high security.

Install

About

Technical Information

Contribute!

Preparar el servidor VPN



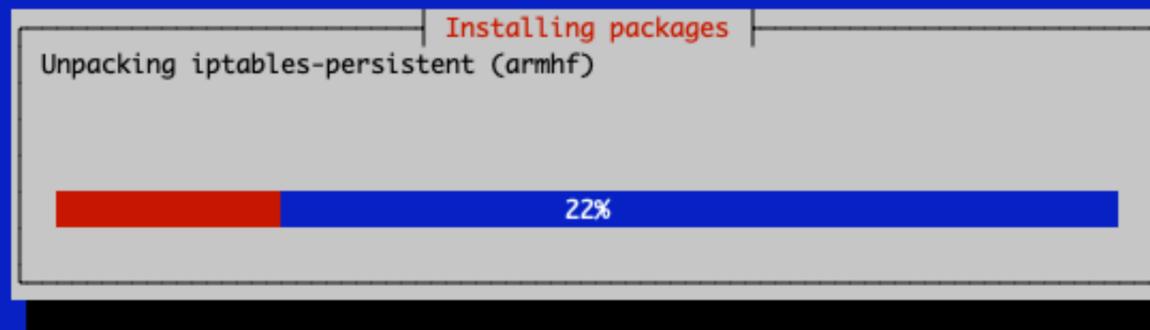
```
pi@raspberrypi:~# curl -L https://install.pivpn.io | bash
```

Preparar el servidor VPN

c0r0n4con

Esto lo paramos hackeando

Package configuration



Preparar el servidor VPN

c0r0n4con

Esto lo paramos hackeando

Welcome

PiVPN Automated Installer

This installer will transform your Raspberry Pi into an OpenVPN or WireGuard server!

<Ok

Preparar el servidor VPN

c0r0n4con

Esto lo paramos hackeando

Initiating network interface

Static IP Needed

The PiVPN is a SERVER so it needs a STATIC IP ADDRESS to function properly.

In the next section, you can choose to use your current network settings (DHCP) or to manually edit them.



Preparar el servidor VPN

c0r0n4con

Esto lo paramos hackeando

Calibrating network interface

DHCP Reservation

Are you Using DHCP Reservation on your Router/DHCP Server?
These are your current Network Settings:

IP address: 10.10.0.234/16
Gateway: 10.10.0.1

Yes: Keep using DHCP reservation
No: Setup static IP address
Don't know what DHCP Reservation is? Answer No.

Preparar el servidor VPN

c0r0n4con

Esto lo paramos hackeando

Parsing User List

Local Users

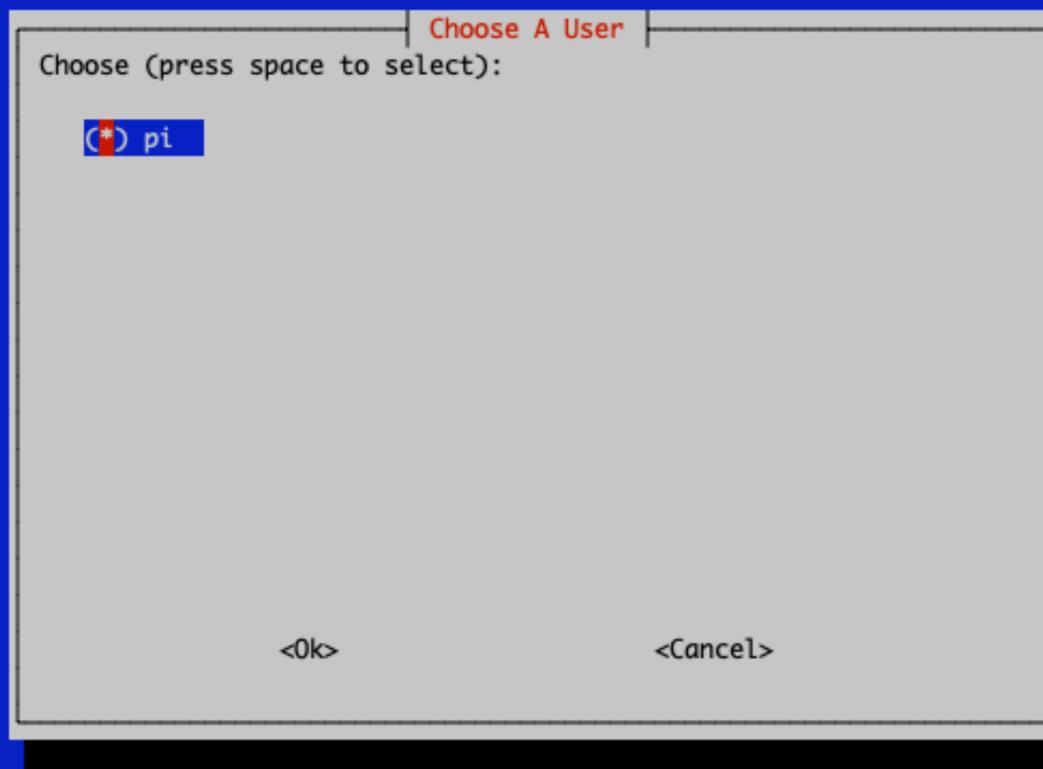
Choose a local user that will hold your ovpn configurations.



Preparar el servidor VPN

c0r0n4con

Esto lo paramos hackeando





Setup PiVPN

Installation mode

WireGuard is a new kind of VPN that provides near-istantaneous connection speed, high performance, modern cryptography.

It's the recommended choice especially if you use mobile devices where WireGuard is easier on battery than OpenVPN.

OpenVPN is still available if you need the traditional, flexible, trusted VPN protocol. Or if you need features like TCP and custom search domain.

Choose a VPN (press space to select):

- WireGuard
- OpenVPN

<Ok> <Cancel>

Preparar el servidor VPN

c0r0n4con

paramos hackeando

```

::: You are root.
::: Hostname length OK
::: Verifying free disk space...
:::
::: Checking apt-get for upgraded packages.... done!
:::
::: Your system is up to date! Continuing with PiVPN installation...
update-alternatives: using /usr/sbin/iptables-legacy to provide /usr/sbin/iptables (iptables) in manual mode
update-alternatives: using /usr/sbin/ip6tables-legacy to provide /usr/sbin/ip6tables (ip6tables) in manual mode
::: Checking for git... not installed!
::: Checking for tar... already installed!
::: Checking for wget... already installed!
::: Checking for curl... already installed!
::: Checking for grep... already installed!
::: Checking for dnsutils... not installed!
::: Checking for whiptail... already installed!
::: Checking for net-tools... already installed!
::: Checking for bsdmainutils... already installed!
::: Checking for dhcpcd5... already installed!
::: Checking for iptables-persistent... not installed!
::: Package git successfully installed!
::: Package dnsutils successfully installed!
::: Package iptables-persistent successfully installed!
::: Using User: pi
:::
::: Checking for existing base files...
::: Checking /etc/.pivpn is a repo...::: Cloning https://github.com/pivpn/pivpn.git into /etc/.pivpn... done!
::: Using VPN: WireGuard
::: Installing WireGuard from Debian package...
::: Adding Raspbian repository...
::: Updating package cache...

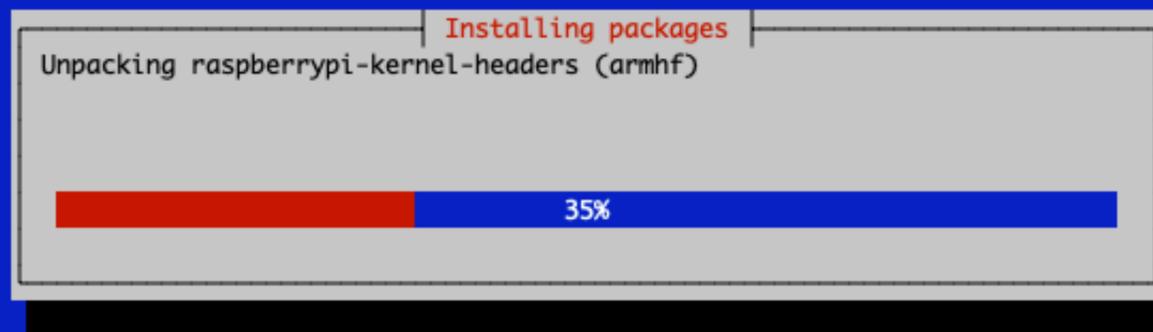
```

Preparar el servidor VPN

c0r0n4con

Esto lo paramos hackeando

Package configuration

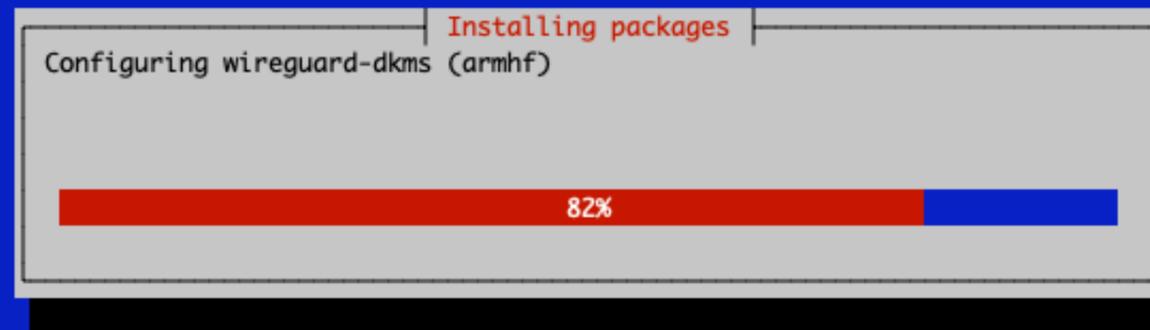


Preparar el servidor VPN

c0r0n4con

Esto lo paramos hackeando

Package configuration



Preparar el servidor VPN

c0r0n4con

Esto lo paramos hackeando

Default wireguard Port

You can modify the default wireguard port.
Enter a new value or hit 'Enter' to retain the default

51820

<Ok> <Cancel>

Preparar el servidor VPN

c0r0n4con

Esto lo paramos hackeando

Specify Custom Port

Confirm Custom Port Number

Are these settings correct?
PORT: 9999

<Yes> <No>

Preparar el servidor VPN

c0r0n4con

Esto lo paramos hackeando

Select the DNS Provider
for your VPN Clients (press space to select). To use your own,
select

Custom.

In case you have a local resolver running, i.e. unbound, select
"PiVPN-is-local-DNS" and make sure your resolver is
listening on

- Quad9
- OpenDNS
- Level3
- DNS.WATCH
- Norton
- FamilyShield

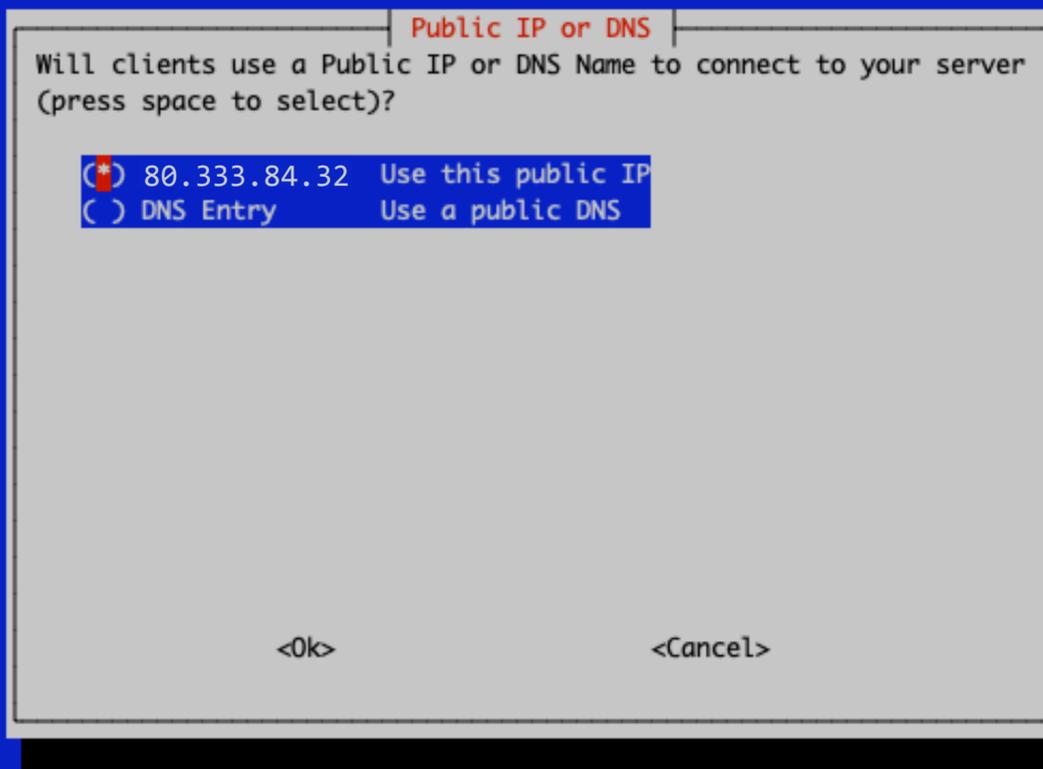
<Ok>

<Cancel>

Preparar el servidor VPN

c0r0n4con

Esto lo paramos hackeando



Preparar el servidor VPN

c0r0n4con

Esto lo paramos hackeando

PiVPN Setup

Confirm DNS Name

Is this correct?

Public DNS Name: vpn.sinologic.net

<Yes> <No>

Preparar el servidor VPN

c0r0n4con

Esto lo paramos hackeando

Server Information

The Server Keys and Pre-Shared key will now be generated.



Preparar el servidor VPN

c0r0n4con

Esto lo paramos hackeando

Security Updates

Unattended Upgrades

Since this server will have at least one port open to the internet, it is recommended you enable unattended-upgrades. This feature will check daily for security package updates only and apply them when necessary. It will NOT automatically reboot the server so to fully apply some updates you should periodically reboot.

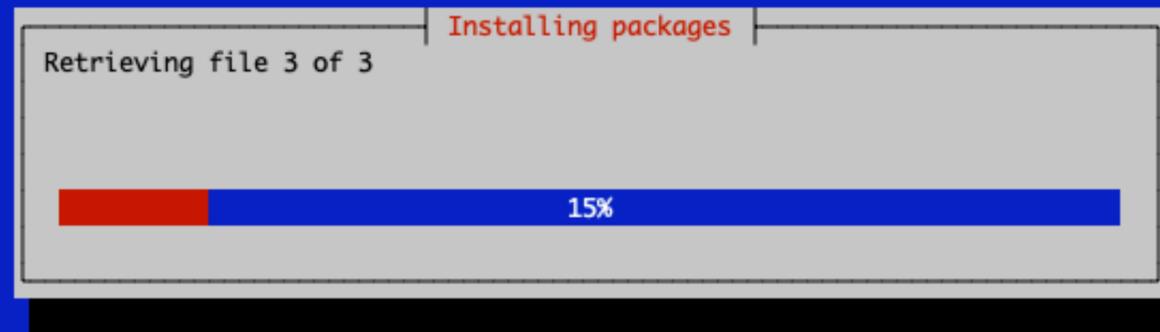


Preparar el servidor VPN

c0r0n4con

Esto lo paramos hackeando

Package configuration



Preparar el servidor VPN

c0r0n4con

Esto lo paramos hackeando

```
::: Checking for dhcpcd5... already installed!
::: Checking for iptables-persistent... not installed!
::: Package git successfully installed!
::: Package dnsutils successfully installed!
::: Package iptables-persistent successfully installed!
::: Using User: pi
:::
::: Checking for existing base files...
::: Checking /etc/.pivpn is a repo...::: Cloning https://github.com/pivpn/pivpn.git into /etc/.pivpn... done!
::: Using VPN: WireGuard
::: Installing WireGuard from Debian package...
::: Adding Raspbian repository...
::: Updating package cache...
::: Checking for raspberrypi-kernel-headers... not installed!
::: Checking for wireguard... not installed!
::: Checking for wireguard-tools... not installed!
::: Checking for wireguard-dkms... not installed!
::: Checking for qrencode... not installed!
::: Package raspberrypi-kernel-headers successfully installed!
::: Package wireguard successfully installed!
::: Package wireguard-tools successfully installed!
::: Package wireguard-dkms successfully installed!
::: Package qrencode successfully installed!
::: Using OpenDNS servers.
::: Backing up the wireguard folder to /etc/wireguard_2020-04-08-173322.tar.gz
::: Server Keys and Pre-Shared Key have been generated.
::: Server config generated.
::: Install Complete...
::: Restarting services...
::: Checking for unattended-upgrades... not installed!
::: Package unattended-upgrades successfully installed!
:::
::: Installing scripts to /opt/pivpn...
done.
::: Flushing writes to disk...
```

Preparar el servidor VPN

c0r0n4con

Esto lo paramos hackeando

Make it so.

Installation Complete!

Now run 'pivpn add' to create the ovpn profiles.
Run 'pivpn help' to see what else you can do!

If you run into any issue, please read all our documentation
carefully.
All incomplete posts or bug reports will be ignored or deleted.

Thank you for using PiVPN.



Preparar el servidor VPN

c0r0n4con

Esto lo paramos hackeando



Preparar el servidor VPN

c0r0n4con

ckeando

```
::: Using User: pi
:::
::: Checking for existing base files...
:::   Checking /etc/.pivpn is a repo...:::   Cloning https://github.com/pivpn/pivpn.git into /etc/.pivpn... done!
::: Using VPN: WireGuard
::: Installing WireGuard from Debian package...
::: Adding Raspbian repository...
::: Updating package cache...
:::   Checking for raspberrypi-kernel-headers... not installed!
:::   Checking for wireguard... not installed!
:::   Checking for wireguard-tools... not installed!
:::   Checking for wireguard-dkms... not installed!
:::   Checking for qrencode... not installed!
:::   Package raspberrypi-kernel-headers successfully installed!
:::   Package wireguard successfully installed!
:::   Package wireguard-tools successfully installed!
:::   Package wireguard-dkms successfully installed!
:::   Package qrencode successfully installed!
::: Using OpenDNS servers.
::: Backing up the wireguard folder to /etc/wireguard_2020-04-08-173322.tar.gz
::: Server Keys and Pre-Shared Key have been generated.
::: Server config generated.
::: Install Complete...
::: Restarting services...
:::   Checking for unattended-upgrades... not installed!
:::   Package unattended-upgrades successfully installed!
:::
::: Installing scripts to /opt/pivpn...
done.
::: Flushing writes to disk...
::: done.
```

Rebooting system...

Connection to 10.10.0.234 closed by remote host.

Connection to 10.10.0.234 closed.

Preparar el servidor VPN



pivpn

```
pi@raspberrypi:~ $ pivpn
::: Control all PiVPN specific functions!
:::
::: Usage: pivpn <command> [option]
:::
::: Commands:
::: -a, add          Create a client conf profile
::: -c, clients      List any connected clients to the server
::: -d, debug        Start a debugging session if having trouble
::: -l, list         List all clients
::: -qr, qrcode      Show the qrcode of a client for use with the mobile app
::: -r, remove       Remove a client
::: -h, help         Show this help dialog
::: -u, uninstall    Uninstall pivpn from your system!
::: -up, update      Updates PiVPN Scripts
::: -bk, backup      Backup VPN configs and user profiles
pi@raspberrypi:~ $
```

Preparar el servidor VPN



pivpn add

```
pi@raspberrypi:~ $ pivpn add
Enter a Name for the Client: hellc2
::: Client Keys generated
::: Client config generated
::: Updated server config
::: WireGuard restarted

=====

::: Done! hellc2.conf successfully created!
::: hellc2.conf was copied to /home/pi/configs for easy transfer.
::: Please use this profile only on one device and create additional
::: profiles for other devices. You can also use pivpn -qr
::: to generate a QR Code you can scan with the mobile app.

=====
```

Preparar el servidor VPN



Ejemplo de archivo de configuración

hellc2.conf
para **WireGuard**

```
pi@raspberrypi:~ $ cd configs/  
pi@raspberrypi:~/configs $ ls -la  
total 12  
drwxr-x--- 2 pi pi 4096 Apr  8 17:36 .  
drwxr-xr-x 5 pi pi 4096 Apr  8 17:36 ..  
-rw-r----- 1 pi pi  319 Apr  8 17:36 hellc2.conf  
pi@raspberrypi:~/configs $  
pi@raspberrypi:~/configs $ cat hellc2.conf  
[Interface]  
PrivateKey = MLN+XXFDNb0cHnYigyn0Um/4eaP3Y0LxUxw8E+MbiG0=  
Address = 10.6.0.2/24  
DNS = 208.67.222.222, 208.67.220.220 Irivjiri  
Irivjiri  
[Peer]  
PublicKey = 3κϒϒFy+Z4ZqMqJRJurAVqXI2q9N3nA67fLeUSSDUe0A=  
PresharedKey = sqigqLq/ndRz/qfS31QNLuQZMR72XPnEiskHSCgVbTU=  
Endpoint = casa.sinologic.net:9999  
AllowedIPs = 0.0.0.0/0, ::0/0  
pi@raspberrypi:~/configs $  
pi@raspberrypi:~/configs $ █
```



Preparar el servidor VPN



Ejemplo de archivo de configuración *hellc2.ovpn* para **OpenVPN**

```
client
dev tun
proto udp
remote vpn.sinologic.net 9999
resolv-retry infinite
nobind
persist-key
persist-tun
remote-cert-tls server
tls-version-min 1.2
verify-x509-name server_pPpIStUJLKmrBgrr name
cipher AES-256-CBC
auth SHA256
auth-nocache
verb 3
<ca>
-----BEGIN CERTIFICATE-----
MIIBnjCCAUWgAwIBAgIJAOSbld/PyrQiMAoGCCqGSM49BAMCMBMxETAPBgNVBAMM
CENoYW5nZU11MB4XDTE5MDIxMTIwMTAxNjowXDTI5MDIwODIwMTAxNjowEzERMA8G
A1UEAwlQ2hhbmdITWUwWTATBgcqhkiOQIBBgqhkiOPQMBBwNCAASmBfFpYplc
lkOhhiPpyeCmtb7+XbkryfNhQ36P3klDmBqW4ew4B262dbtdqNAYMt12uiy0688iVa7D/xotVqTWL
Ur39aCBQkeGwo4GBMH8wHQYDVR0OBBYEFKa0awzTxhTYna19/AHQJ5NM+x5FMEMG
A1UdlwQ8MDqAFKa0awzTxhTYna19/AHQJ5NM+x5FoRekFTATMREwDwYDVQQDDAhd
aGFuZ2V2bnZlYiJAOSbld/PyrQiMAwGA1UdEwQFMAMBAf8wCwYDVR0PBAQDAgEGMAoG
CCqGSM49BAMCA0cAMEQCICNOAV3UD2pUKaQMclQ/1UyuZ3KjuCssX+fTgvRYoXY2
AiAy6Plw9e01tjmhkEOEPkM62+CBz3jsp+rqgwTgOHKZpQ==
-----END CERTIFICATE-----
</ca>
<cert>
-----BEGIN CERTIFICATE-----
```





Configurar el Router

Configurar el Router



GWN7000 Firmware 1.0 | Time 2020-04-08 19:26 | 15s | English | admin

Firewall Basic Settings

General Settings | **Port Forward** | DMZ | UPnP Settings | UPnP Status

[+ Add](#)

Name	Enabled	Protocol	Src Group	Src Port(s)	Dest Group	Dest IP	Dest Port(s)	Actions
OpenVPN	✗	UDP	WAN1	44344	RedInternaCasa	10.10.0.4	44344	✎ 🗑️
Mediacenter	✓	TCP/UDP	WAN1	56035	RedInternaCasa	10.10.0.7	32400	✎ 🗑️
Torrent	✓	TCP/UDP	WAN1	60412	RedInternaCasa	10.10.0.7	60412	✎ 🗑️

© 2019 Grandstream Networks, Inc. All Rights Reserved

Configurar el Router



GWN7000 Firmware 1.0 | Time 2020-04-08 19:10 | English | admin

https://10.10.0.1/#view:firewall/basic

Firewall Basic

General Settings

- + Add
- Name
- OpenVPN
- Mediacenter
- Torrent

Add

Name: VPNWireGuard

Enabled:

Protocol: TCP/UDP

Source Group: WAN1

Source Port(s): 9999

Destination Group: RedInternaCasa

Destination IP: 10.10.0.234

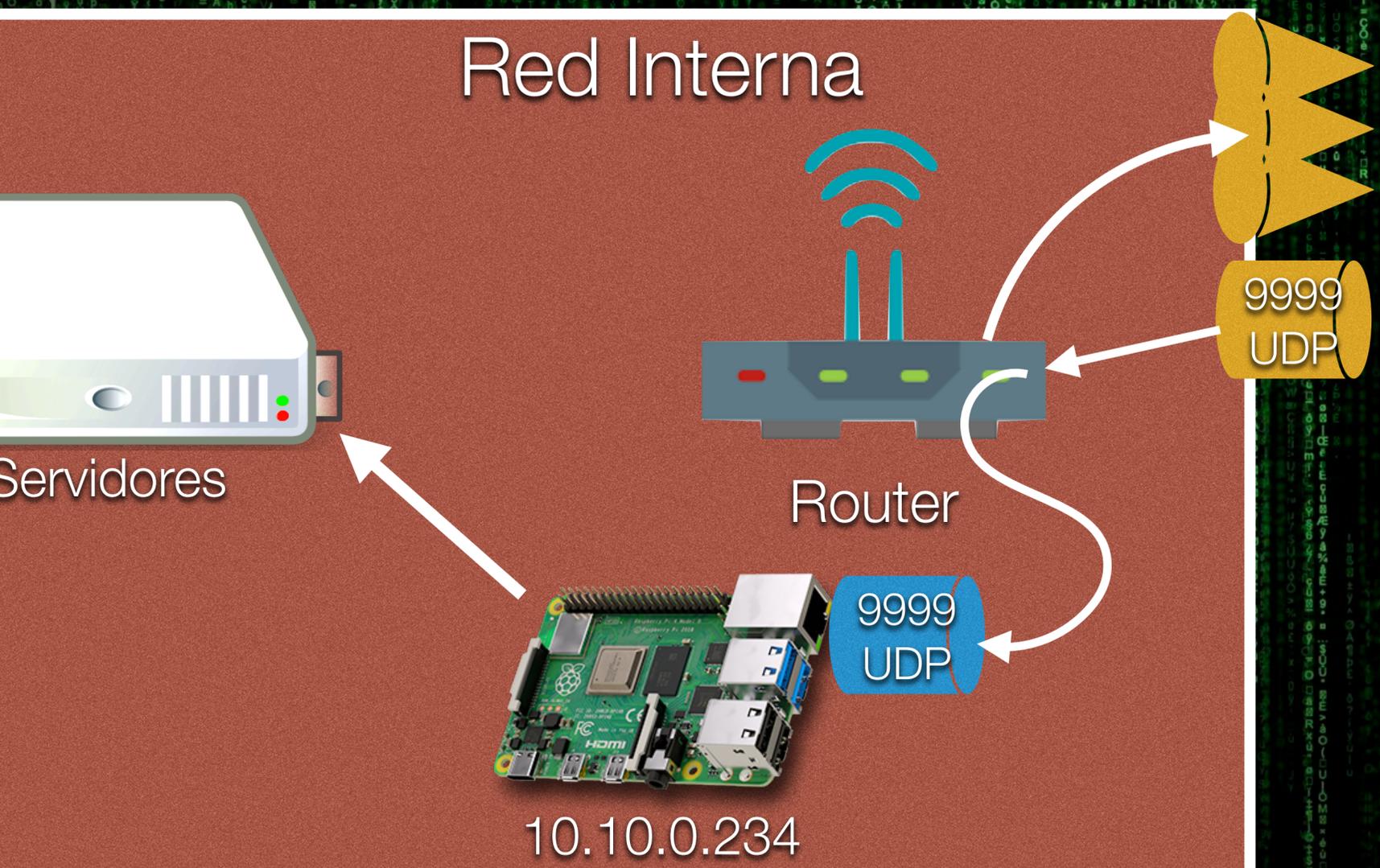
Destination Port(s): 9999

Save Cancel

Dest Port(s)	Actions
44344	
32400	
60412	

© 2019 Grandstream Networks, Inc. All Rights Reserved

Configurar el Router





Configurar los clientes

https://www.wireguard.com/install/

c0r0n4con

Esto lo paramos hackeando

WireGuard Installation Quick Start Interworkings Whitepaper Donate git

Installation

Windows [7, 8, 8.1, 10, 2012, 2016, 2019]
macOS [app store]
Ubuntu ≥ 19.10 [module & tools]
Ubuntu ≤ 19.04 [module & tools]
Android [play store & f-droid]
iOS [app store]
Debian [module & tools]
Fedora ≥ 32 [tools]
Fedora ≤ 31 [module & tools]
Mageia [module & tools]
Arch [module & tools]
OpenSUSE Tumbleweed [tools]
OpenSUSE Leap/SLE [module & tools]
Slackware [module & tools]
Alpine [module & tools]
Gentoo [module & tools]
Exherbo [module & tools]
NixOS [module & tools]
Nix on Darwin [userspace go &

Installation

Windows [7, 8, 8.1, 10, 2012, 2016, 2019 – v0.1.0]
WireGuard for Windows is available from this site:
Download for 64-bit
Download for 32-bit
macOS [app store – v0.0.20200127-17]
Download from App Store
Ubuntu ≥ 19.10 [module – v1.0.20200401 & tools – v1.0.20200319]
\$ sudo apt install wireguard
Ubuntu ≤ 19.04 [module – v1.0.20200401 & tools – v1.0.20200319]
\$ sudo add-apt-repository ppa:wireguard/wireguard
\$ sudo apt-get update
\$ sudo apt-get install wireguard
Android [play store – v1.0.20200407 & f-droid – v1.0.20200401 – out of date]
Download from Play Store
Download from F-Droid
iOS [app store – v0.0.20200127-17]
Download from App Store
Debian [module – v1.0.20200401 & tools – v1.0.20200319]
apt install wireguard
Users with Debian releases older than Bullseye should enable backports.

pivpn - qr



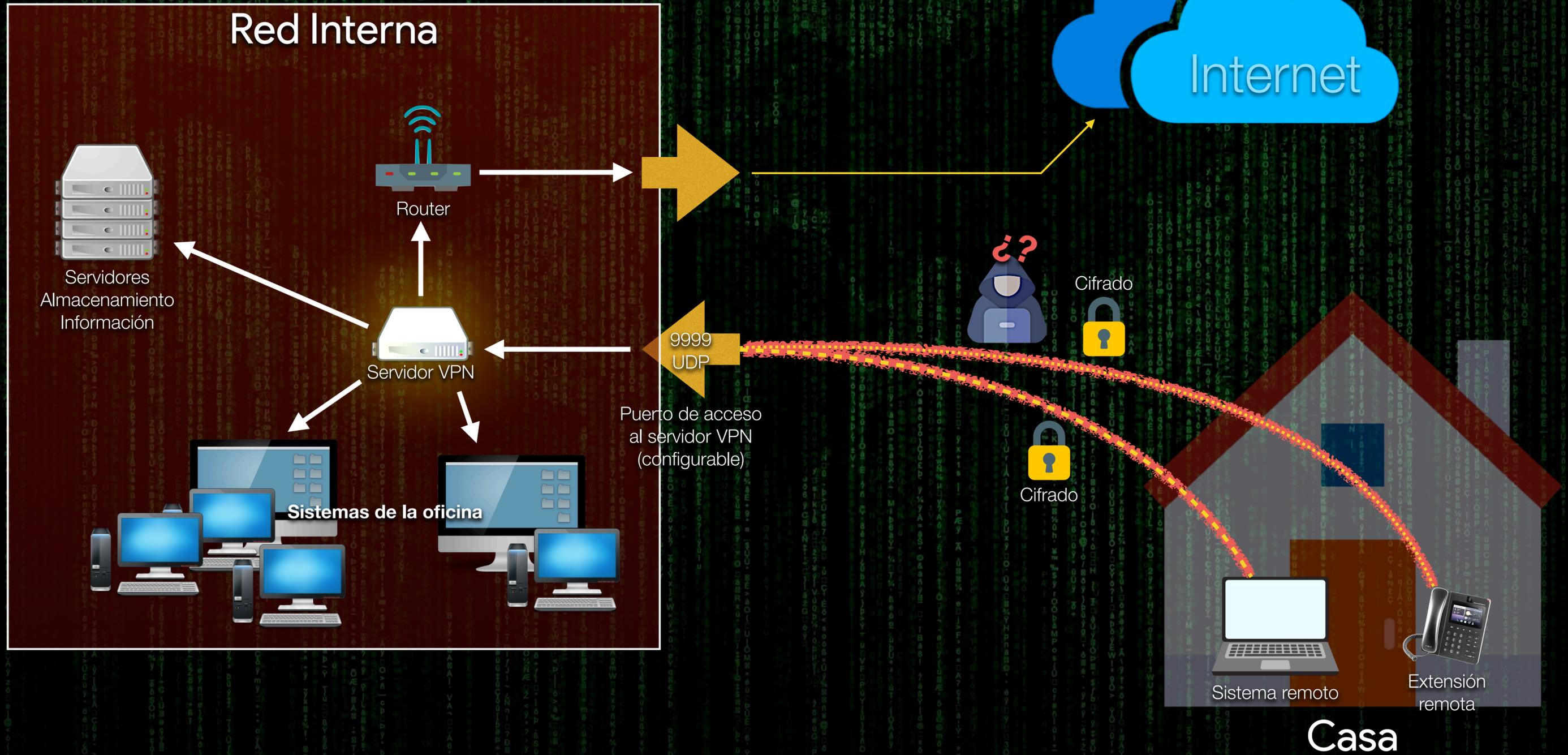
```
pi@raspberrypi:~ $ pivpn -qr
:: Client list ::
• hellc2
Please enter the Name of the Client to show: hellc2
c::: Showing client hellc2 below
```





```
pi@raspberrypi:~ $ pivpn -c
::: Connected Clients List :::
Name           Remote IP      Virtual IP     Bytes Received Bytes Sent     Last Seen
hellc2         62.97.94.76:64503 10.6.0.2      7.0MiB        84MiB         Apr 09 2020 - 15:50:07
```

Esquema de la Idea General





¿Preguntas?



Gracias

