Cómo instalar un Servidor VPN en 5 minutos

para una pequeña empresa

Elio Rojano

https://sinologic.net

c0r0n4con

Esto lo paramos hackeando

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/

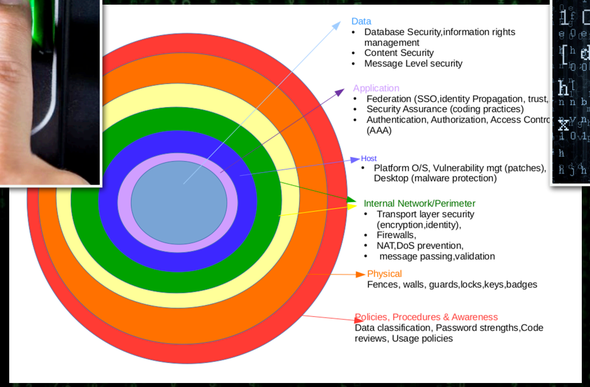
https://www.linkedin.com/in/rojano/

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...



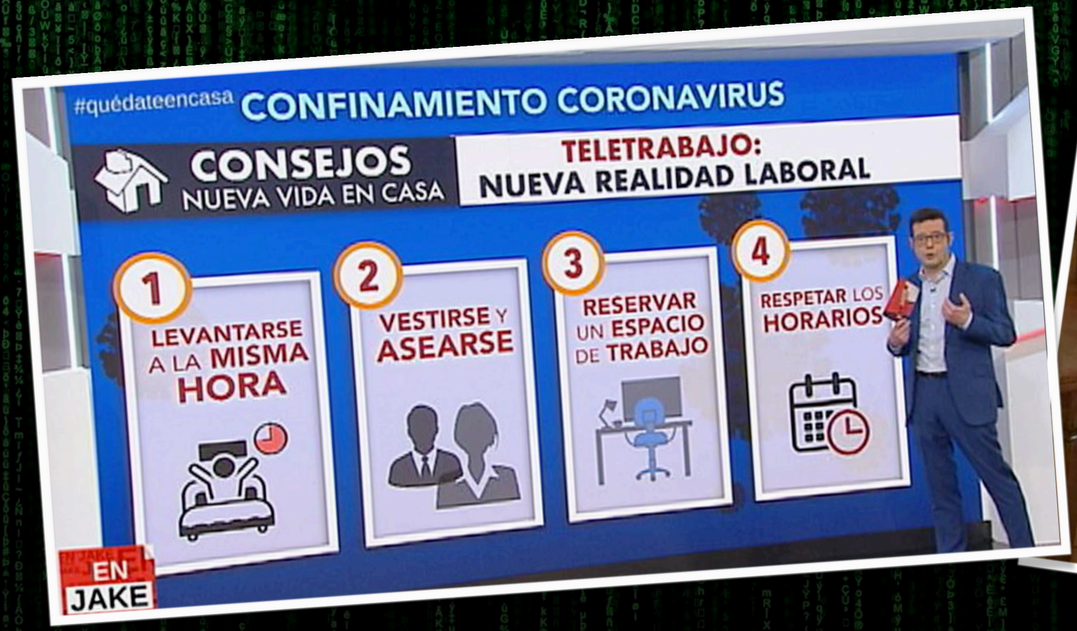
c0r0n4con

Esto lo paramos hackeando

El *SARS-CoV2* ha obligado a *"teletrabajar"* a todos aquellos que podían

Elio Rojano Ruiz

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



Elio Rojano Ruiz

c0r0n4con

Esto lo paramos hackeando

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

Elio Rojano Ruiz

Comunicaciones

- Sistema de Correo electrónico 
- Sistema de Mensajería instantánea 
- Sistema de Telefonía VoIP 
- Sistema de Videoconferencia 

c0r0n4con

Esto lo paramos hackeando

Pero...
¿Cómo se accede a la información de la empresa?

Fichas de clientes

Aplicaciones

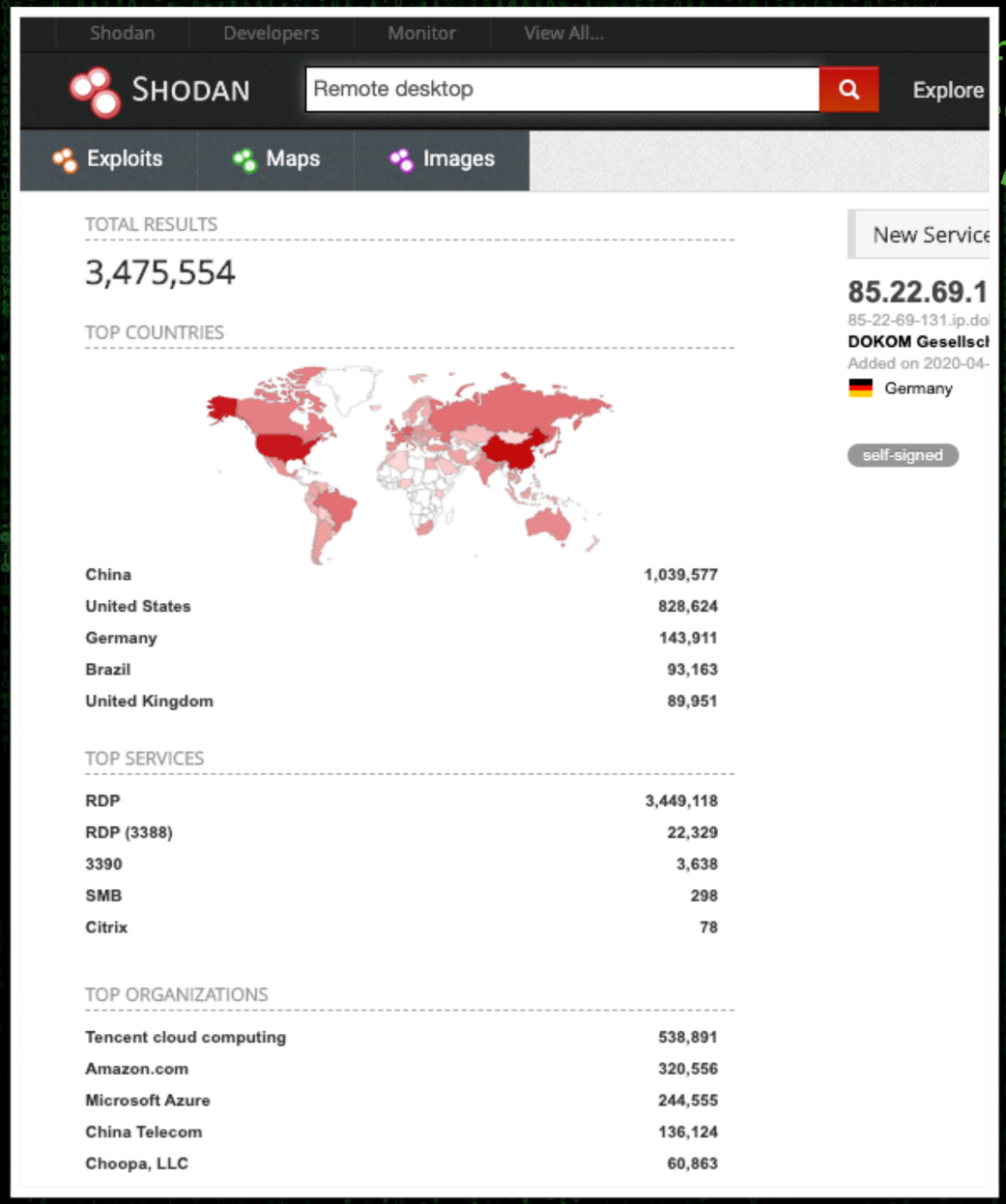
Facturas

Listados de proveedores

Tickets

Documentación

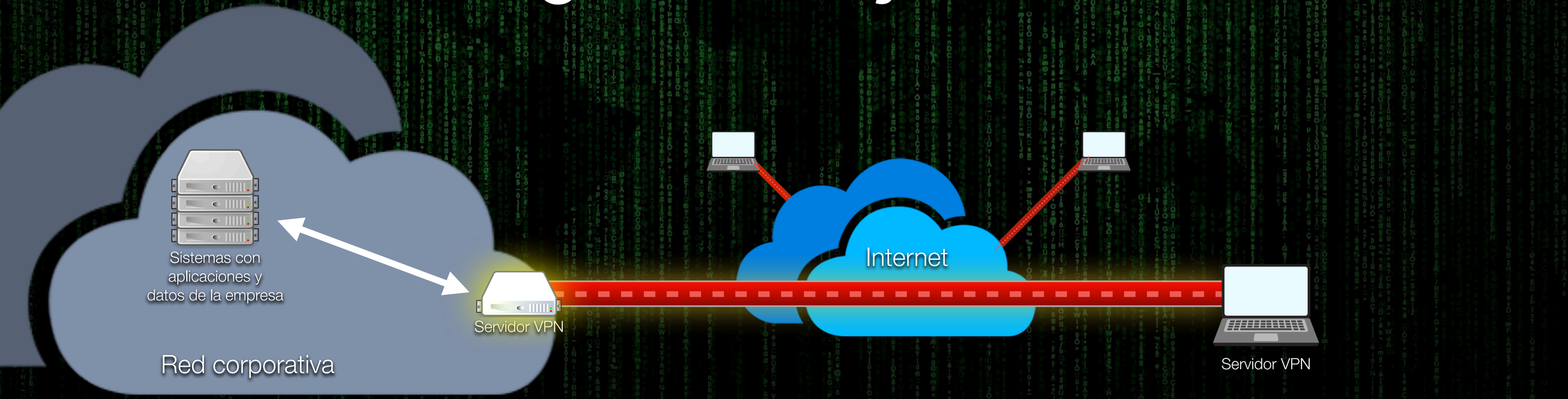
Esto ha dado como resultado un gran número de sistemas vulnerables en Internet



c0r0n4con

Esto lo paramos hackeando

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



Elio Rojano Ruiz

c0r0n4con

Esto lo paramos hackeando

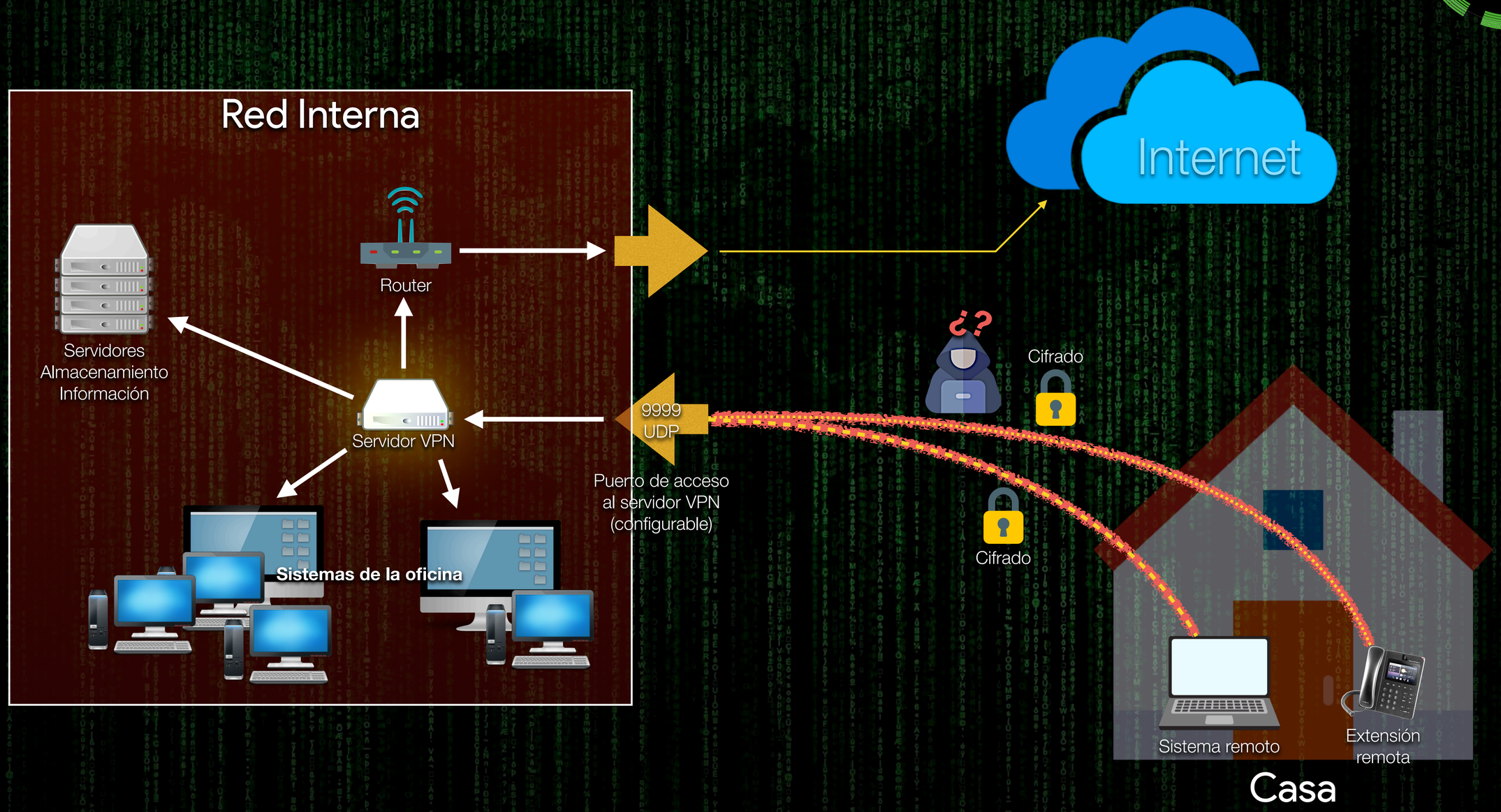
¿Qué ocurre con las pequeñas empresas que no tienen esta posibilidad?

Elio Rojano Ruiz

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



Elio Rojano Ruiz

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:

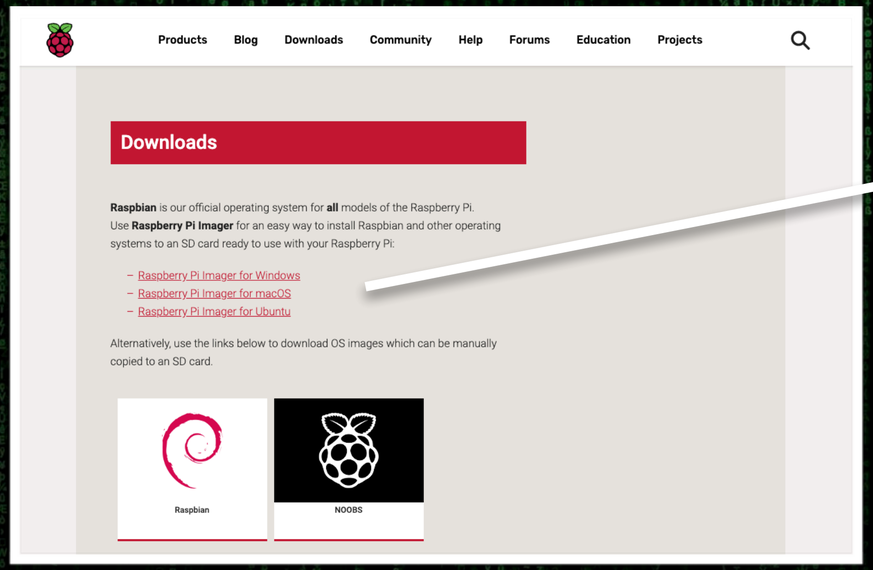
- **Uso de un SAI para el router y la RPI**
- **Recomendable: Redundancia** (otra RPI en otro puerto, por si...)

Preparar servidor VPN:

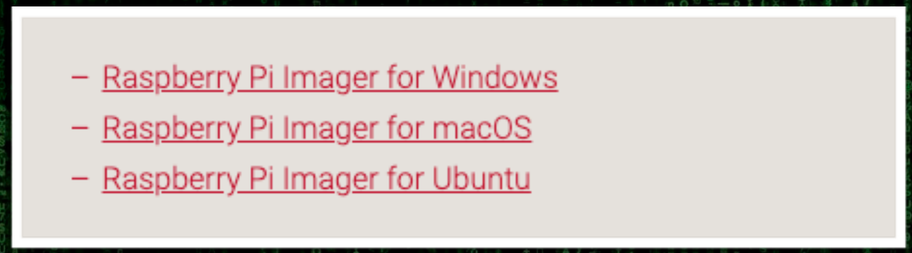
c0r0n4con

Esto lo paramos hackeando

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



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

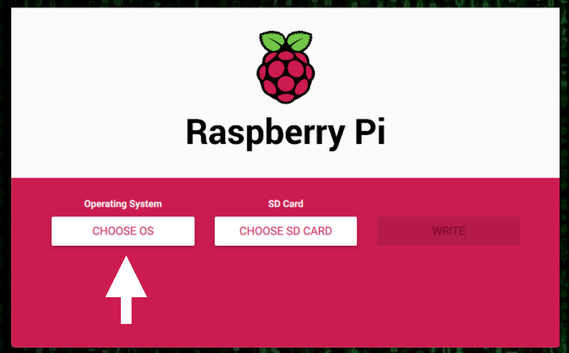


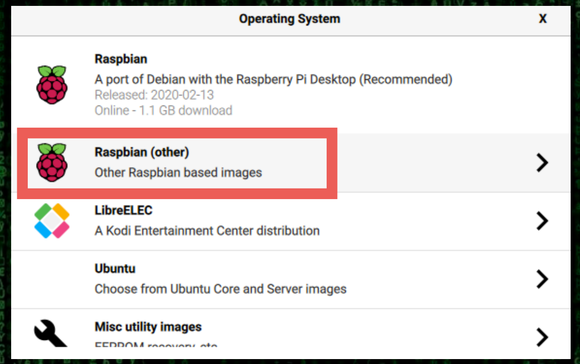
Preparar servidor VPN:

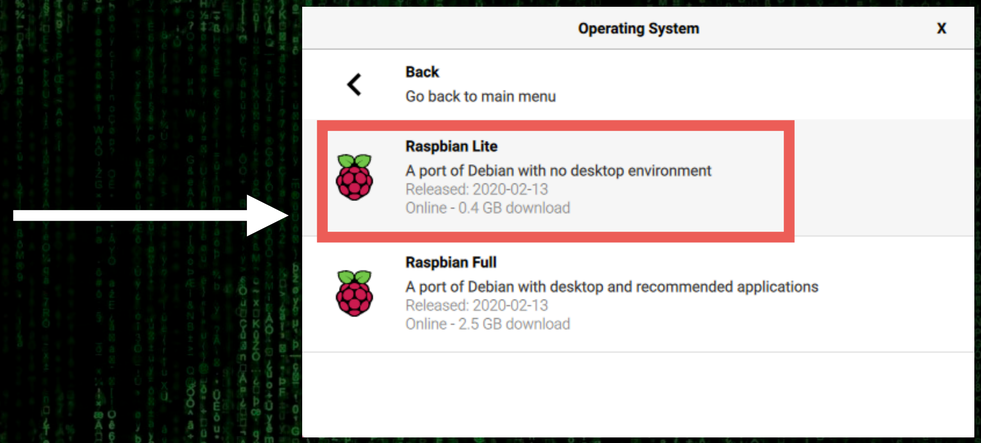
c0r0n4con

Esto lo paramos hackeando

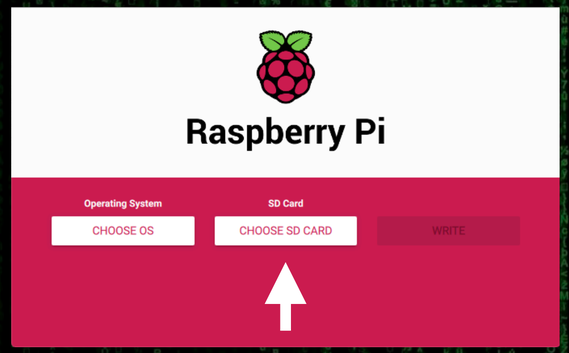
1º

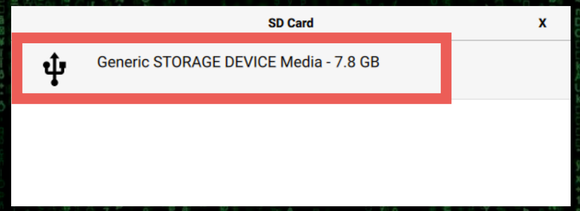




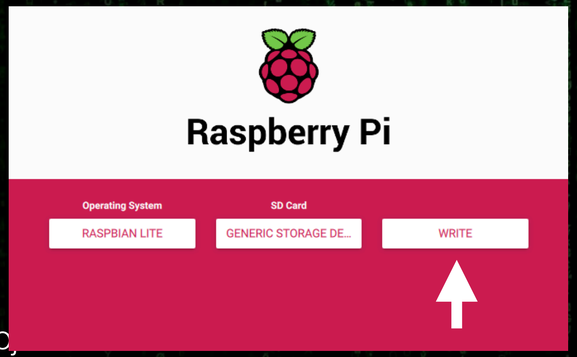


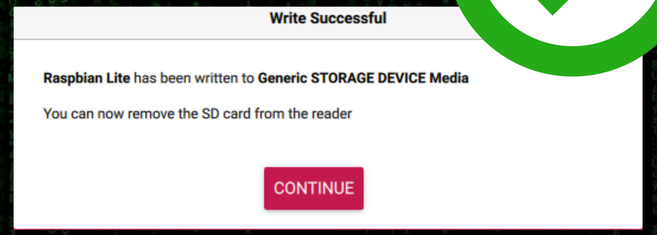
2º





3º





Elio Ro

Preparar servidor VPN:

c0r0n4con

Esto lo paramos hackeando

1º. Accedemos a la Raspberry PI

usuario: pi
contraseña: raspberry

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
```

→

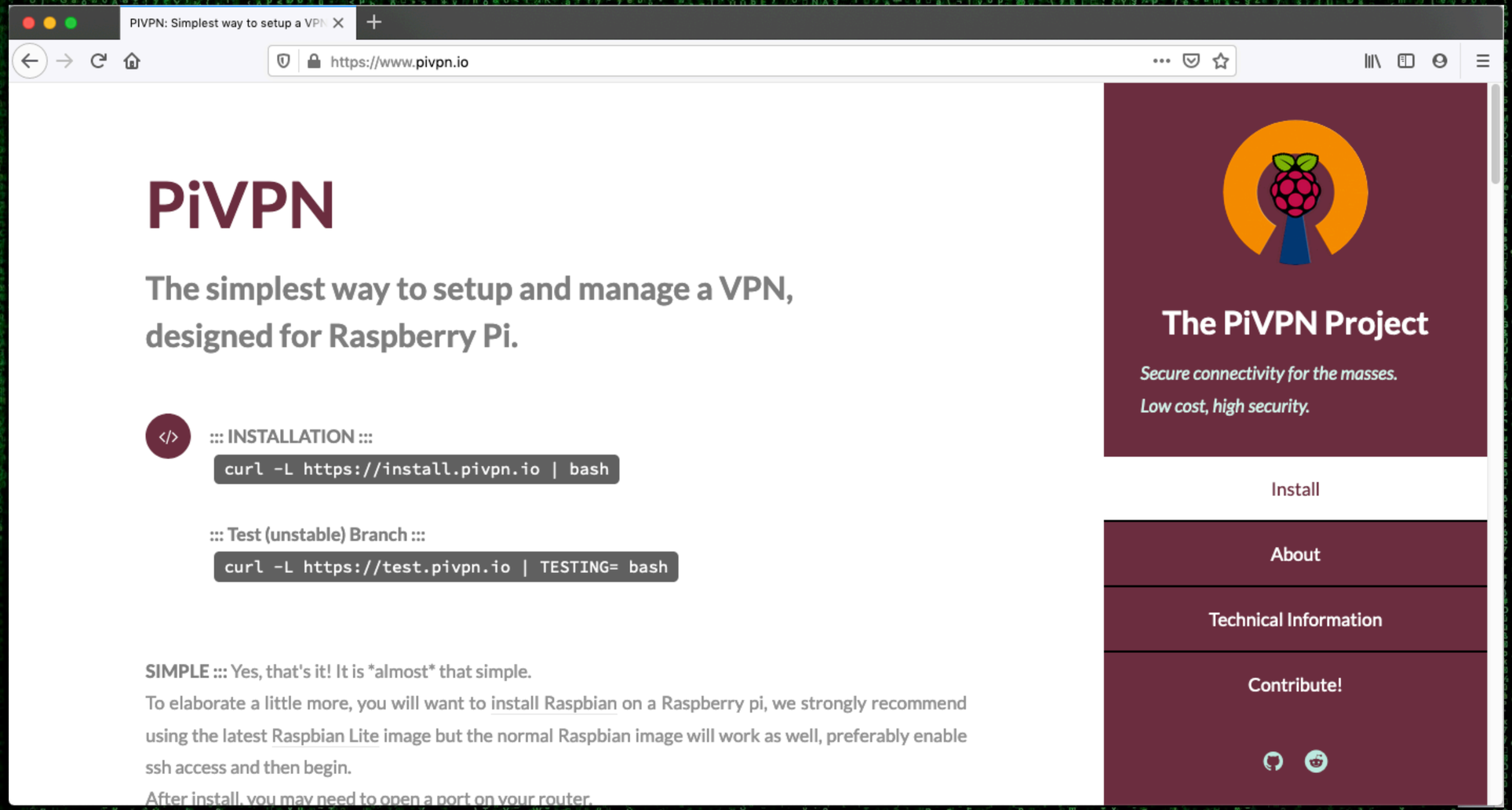
```
P1 Camera       Enable/Disable connection to the Raspberry Pi Camera
P2 SSH          Enable/Disable remote command line access to your Pi using SSH
P3 VNC          Enable/Disable graphical remote access to your Pi using RealVNC
```

3º. Actualizamos repositorio:

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

Preparar el servidor VPN

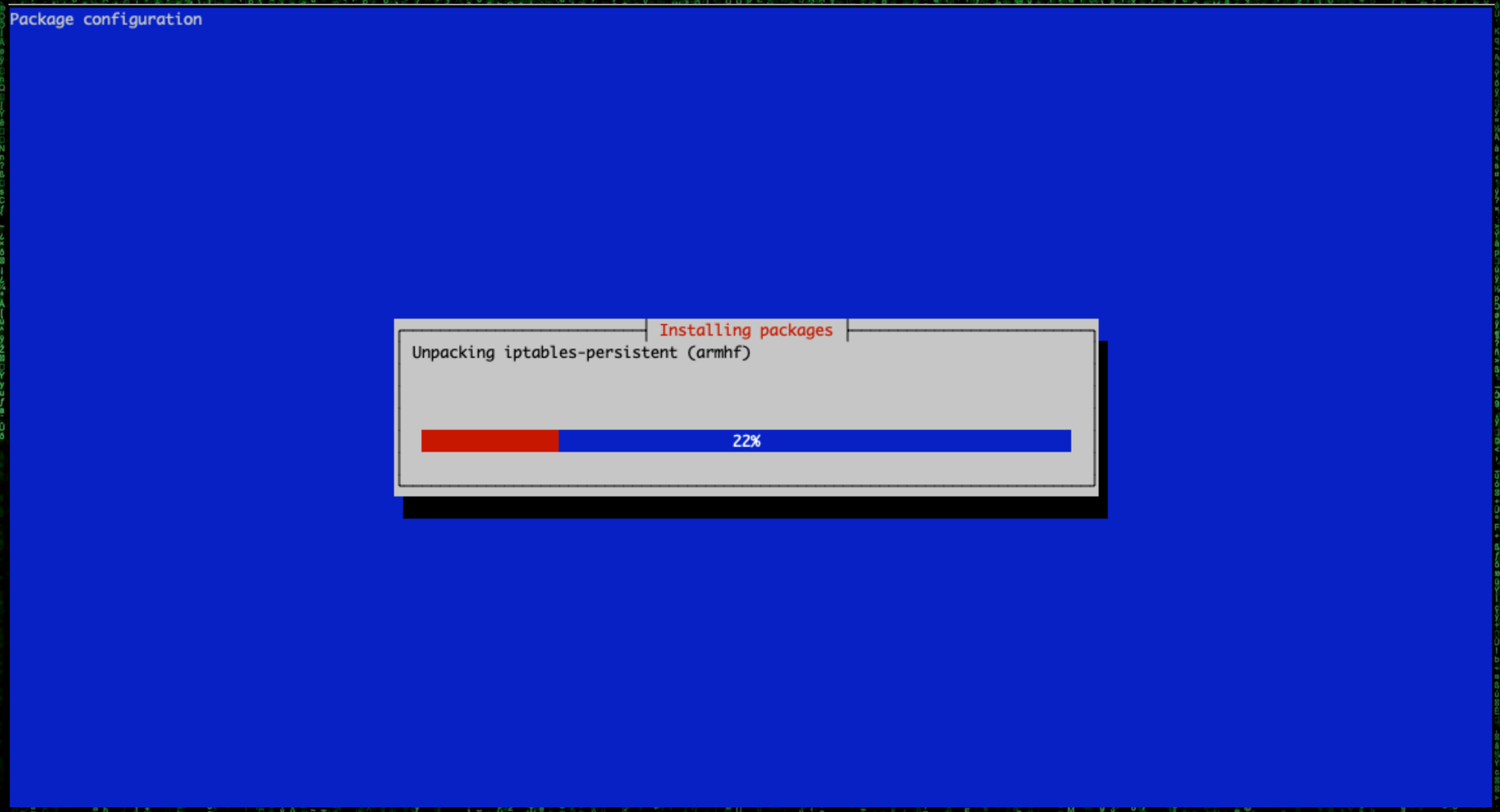
Preparar el servidor VPN



Preparar el servidor VPN


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

Preparar el servidor VPN



Elio Rojano Ruiz

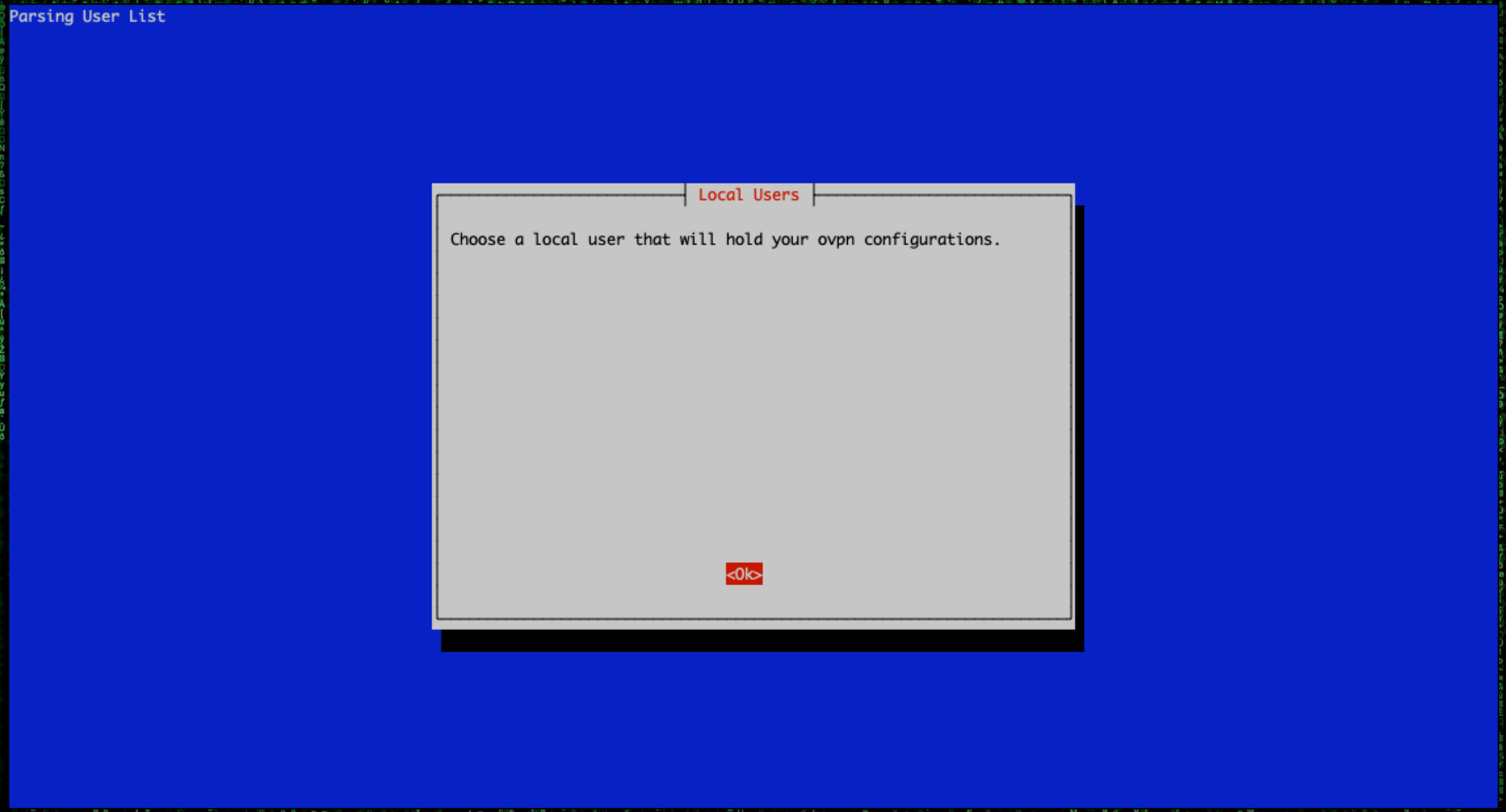
Preparar el servidor VPN

Preparar el servidor VPN

Elio Rojano Ruiz

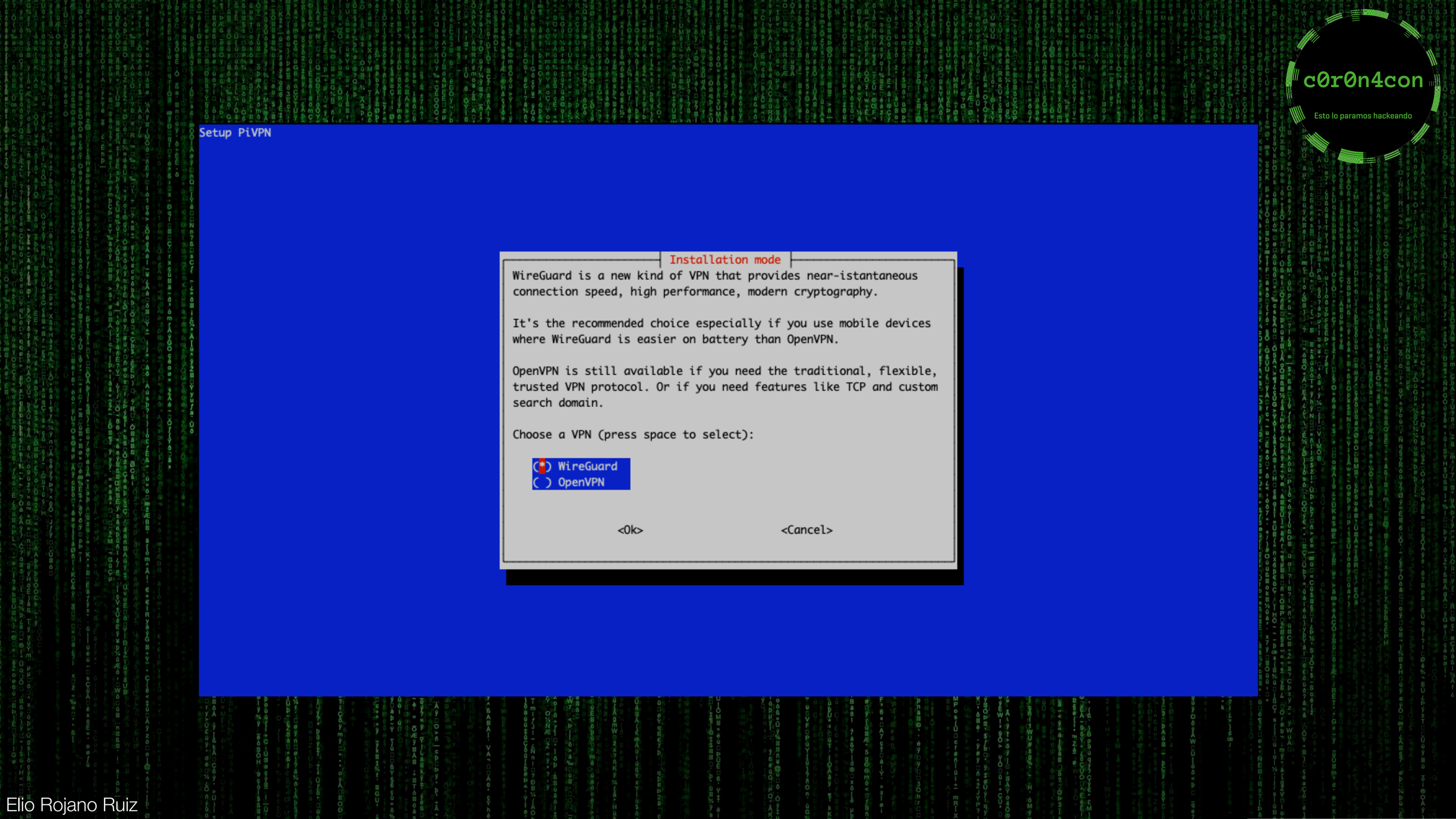
Preparar el servidor VPN

Preparar el servidor VPN



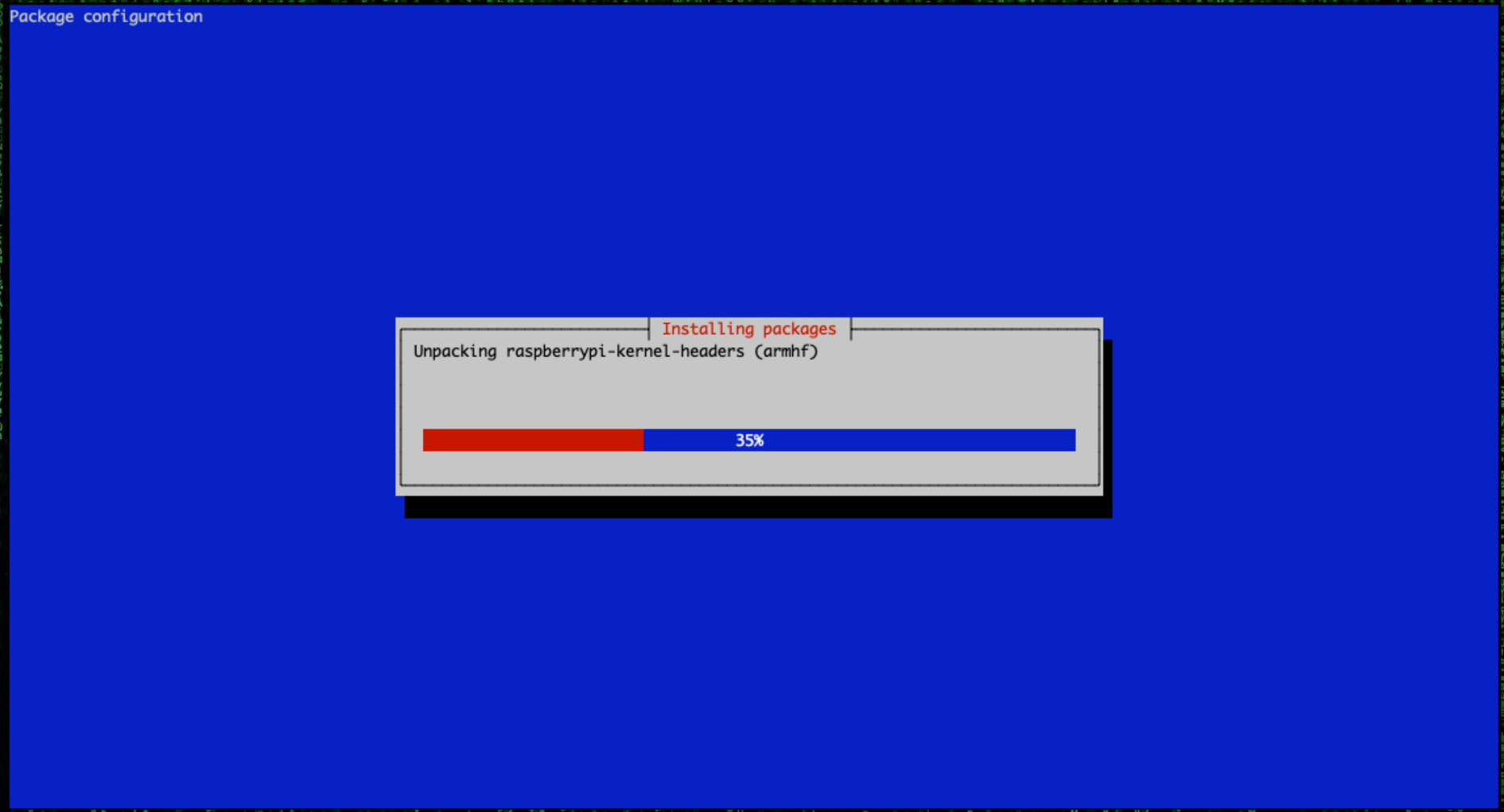
Elio Rojano Ruiz

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>
Elio Rojano Ruiz

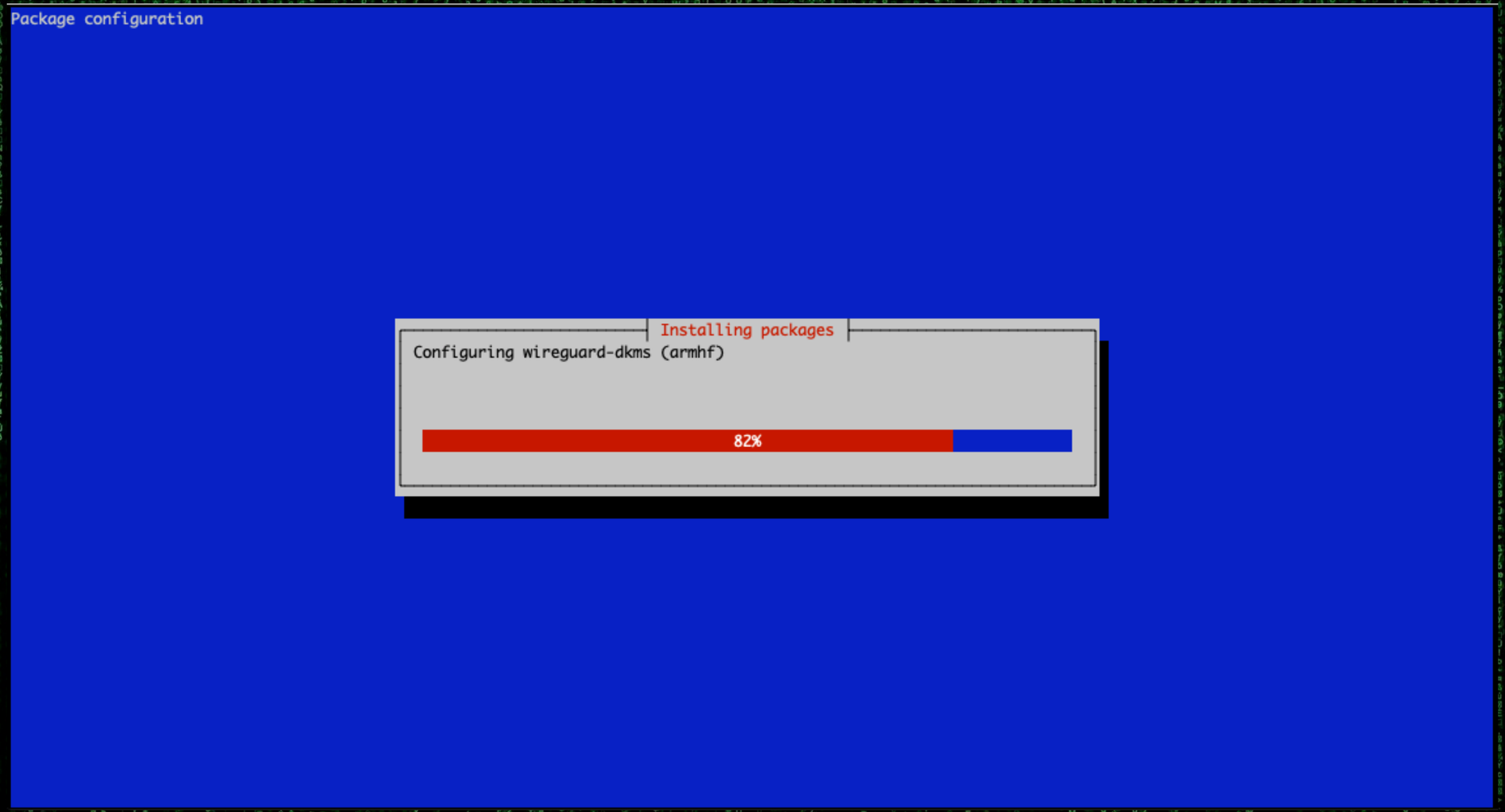
Preparar el servidor VPN

Preparar el servidor VPN

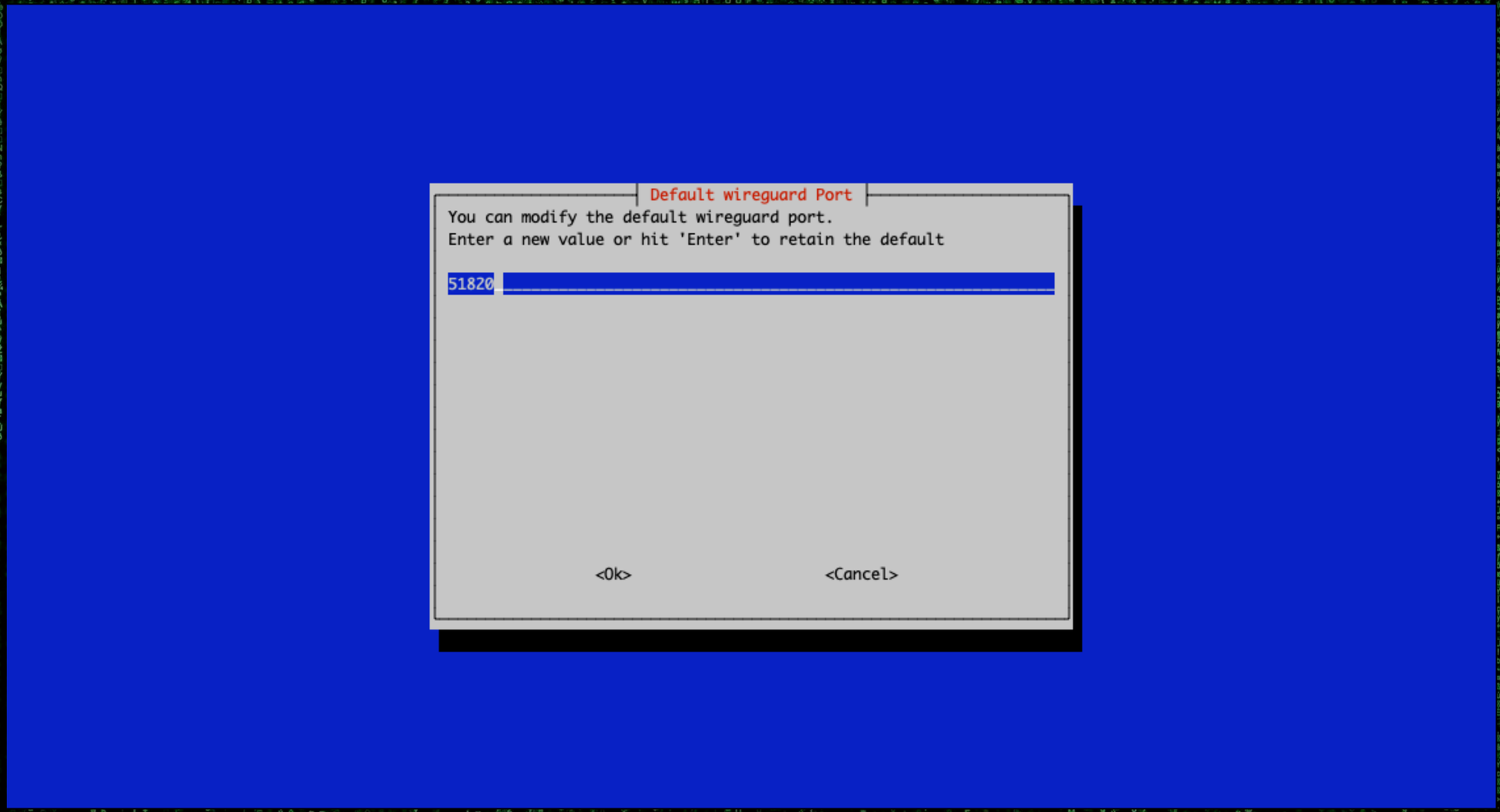


Elio Rojano Ruiz

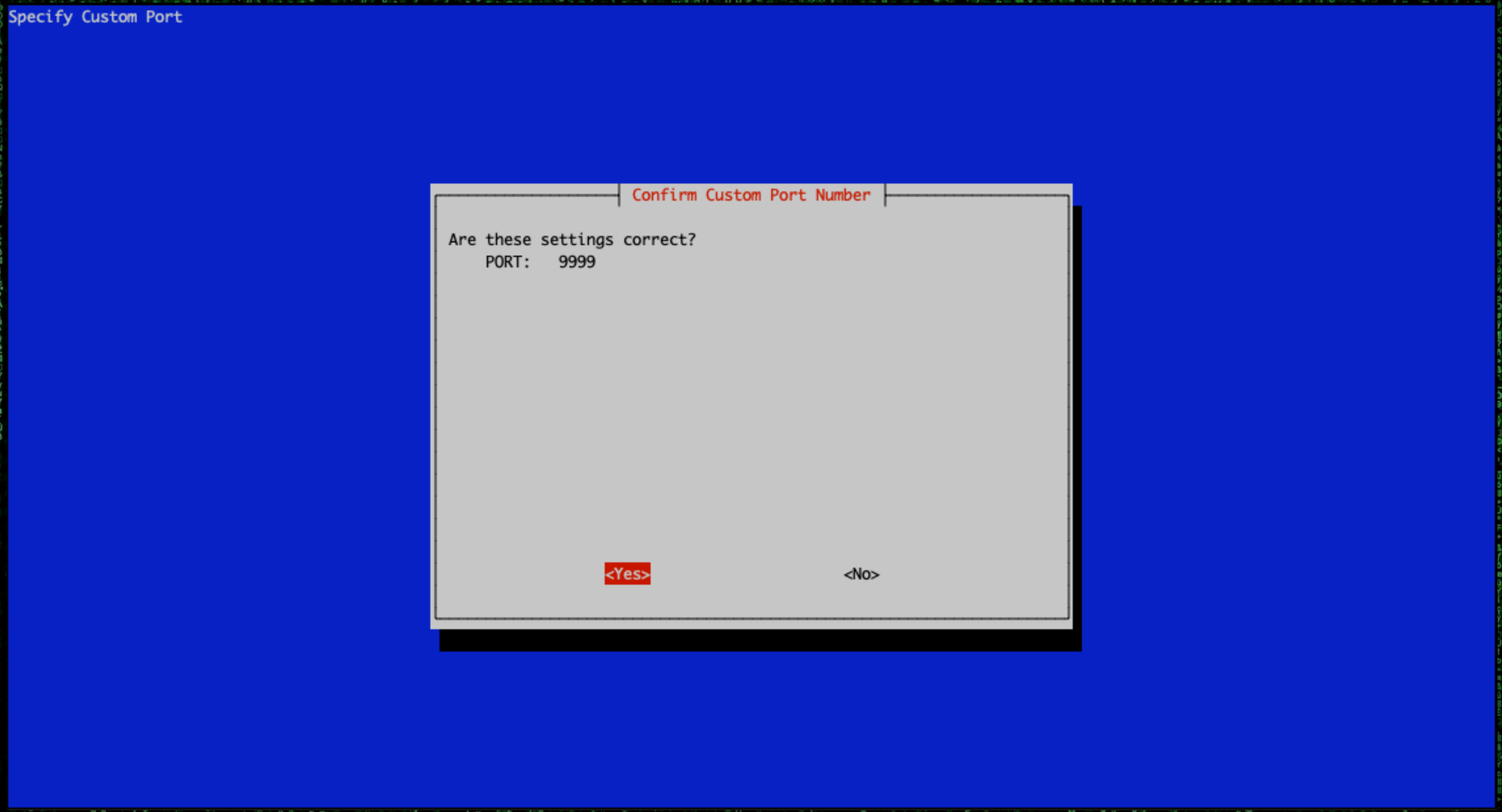
Preparar el servidor VPN



Preparar el servidor VPN



Preparar el servidor VPN



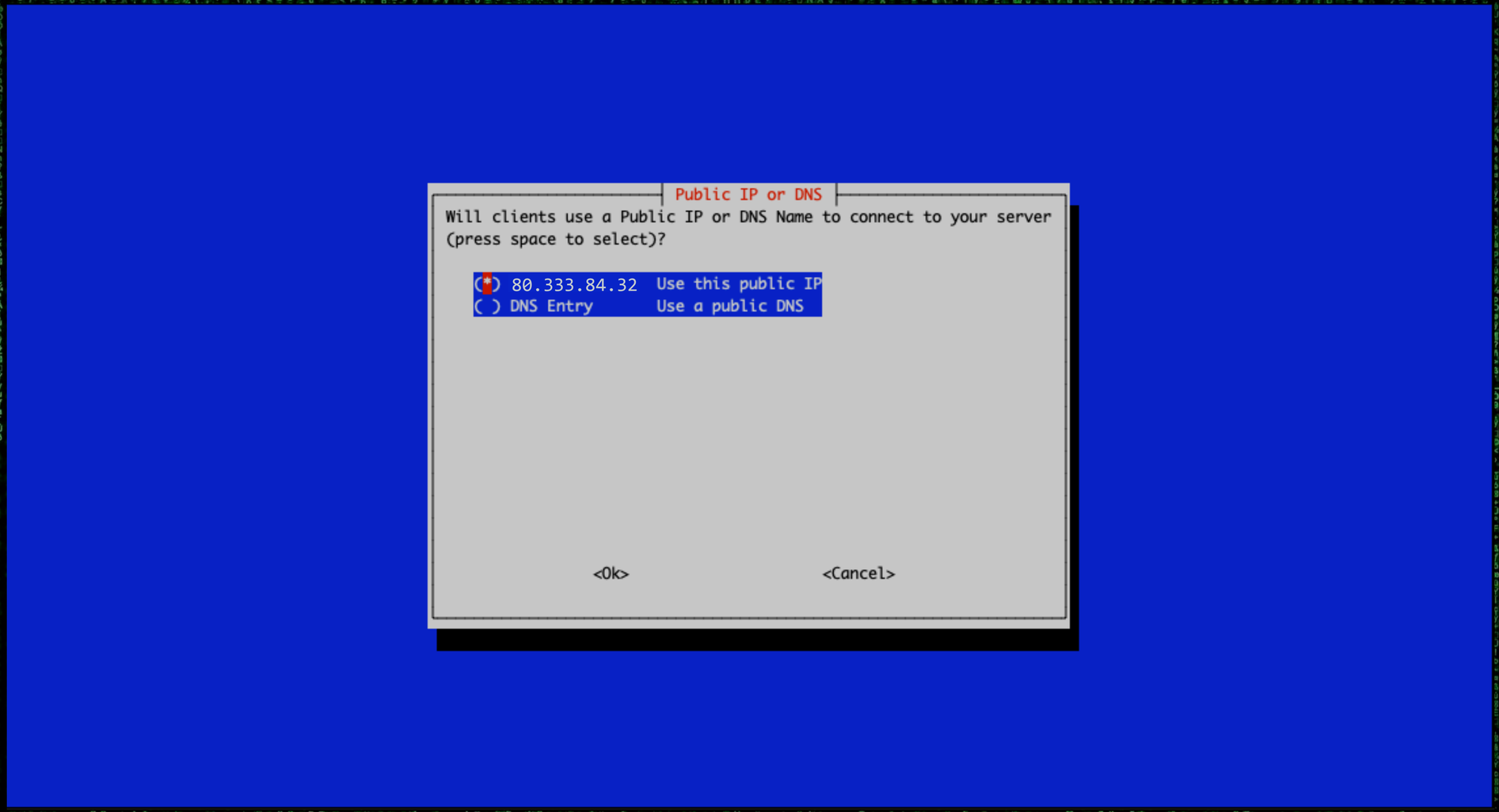
Elio Rojano Ruiz

Preparar el servidor VPN

c0r0n4con

Esto lo paramos hackeando

Preparar el servidor VPN



c0r0n4con

Esto lo paramos hackeando

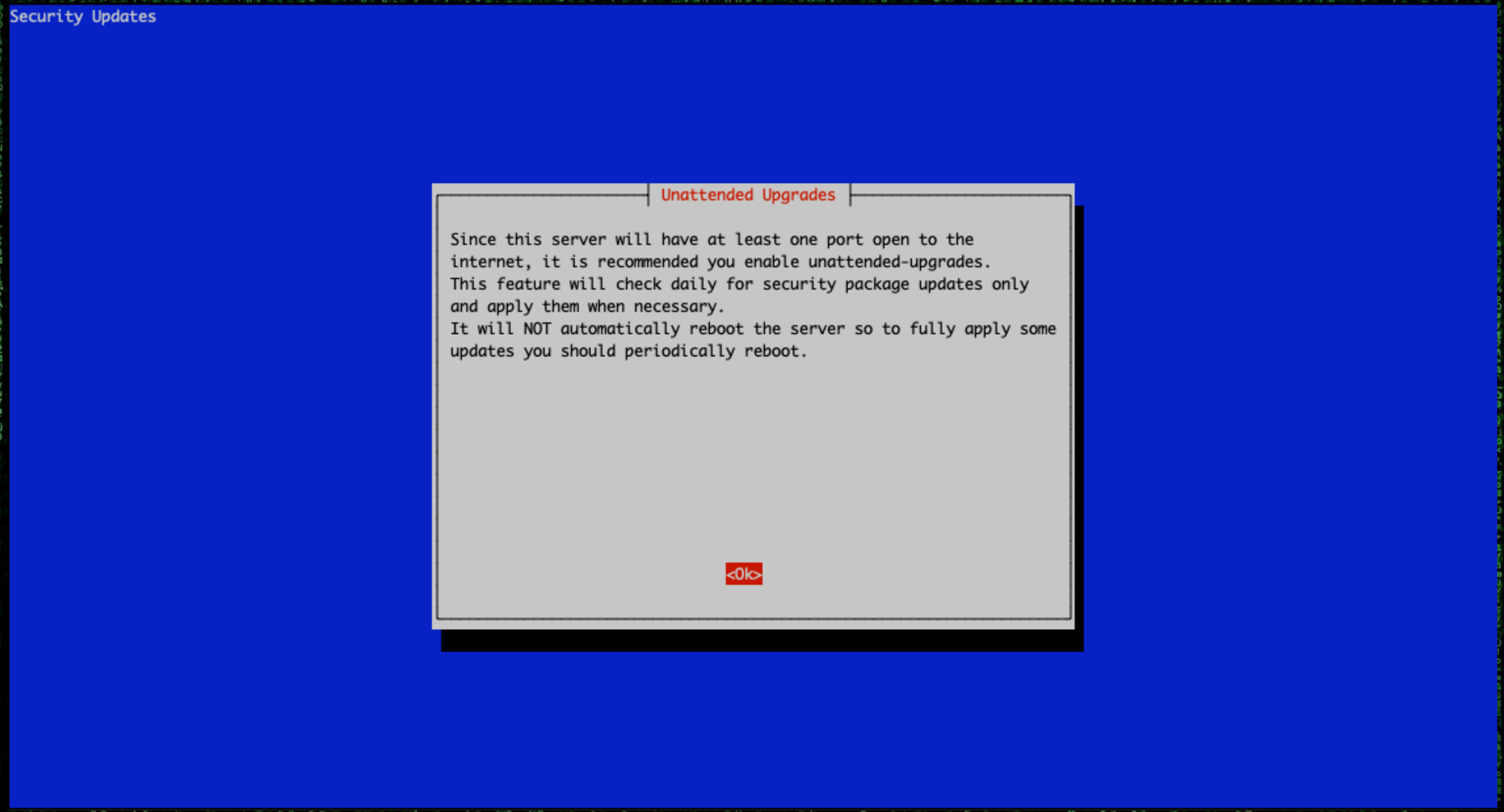
Preparar el servidor VPN

c0r0n4con

Esto lo paramos hackeando

Preparar el servidor VPN

Preparar el servidor VPN



c0r0n4con

Esto lo paramos hackeando

Preparar el servidor VPN

Elio Rojano Ruiz

Preparar el servidor VPN

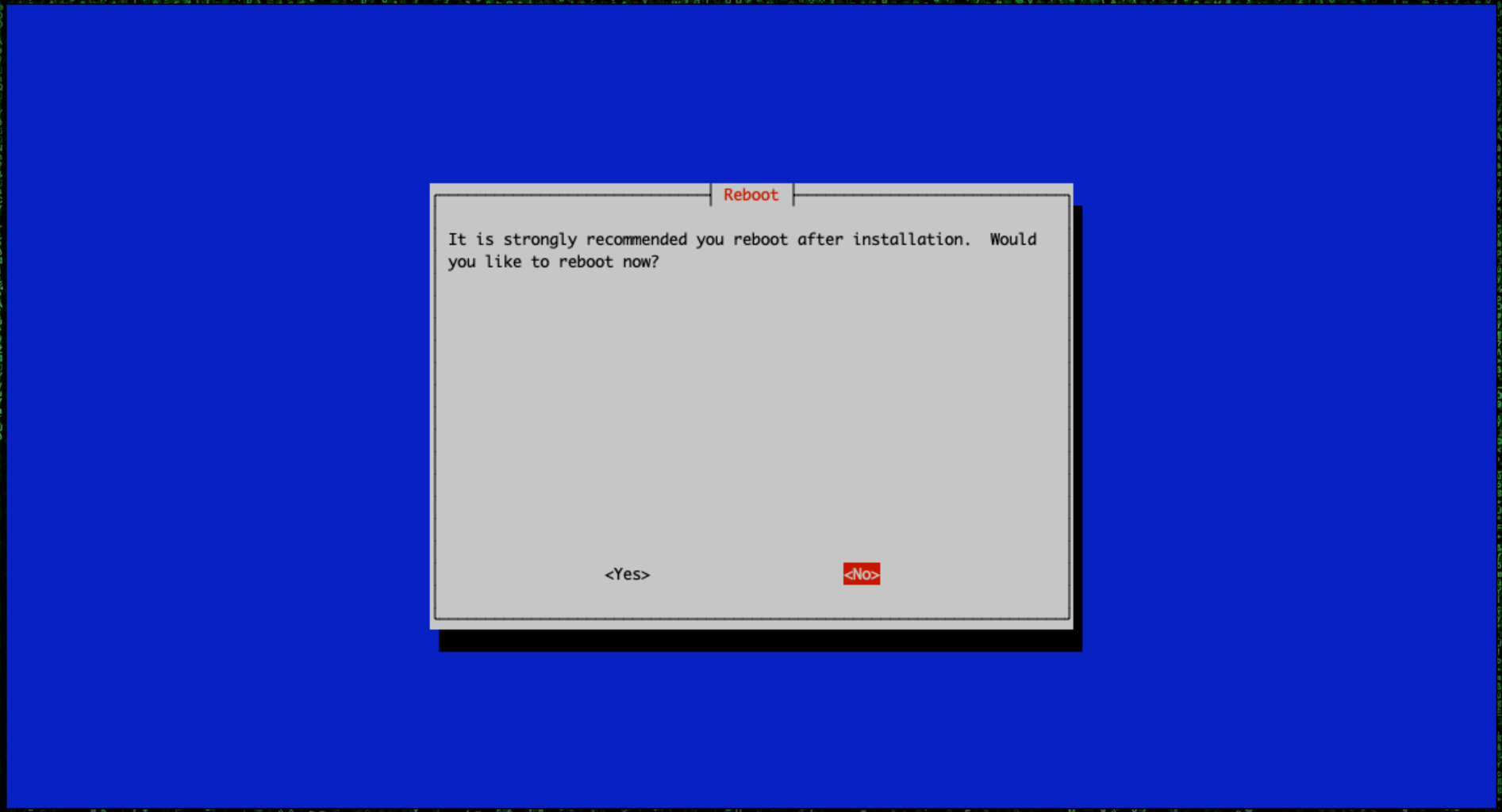

```
:::    Checking for dhcpcd5... already installed!
:::    Checking for iptables-persistent... not installed!
:::    Package git successfully installed!
:::    Package dnsutils successfully installed!
:::    Package iptables-persistent successfully installed!
::: Using User: pi
:::
::: Checking for 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

Preparar el servidor VPN



Preparar el servidor VPN


```
::: 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

c0r0n4con

Esto lo paramos hackeando

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

c0r0n4con

Esto lo paramos hackeando

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+XXFDNbOcHnYigyn0Um/4eaP3Y0LxUxw8E+MbiG0=
Address = 10.6.0.2/24
DNS = 208.67.222.222, 208.67.220.220

[Peer]
PublicKey = 3kQQFy+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_pPplStUJLKmrBgrr name
cipher AES-256-CBC
auth SHA256
auth-nocache
verb 3
<ca>
-----BEGIN CERTIFICATE-----
MIIBnjCCAUWgAwIBAgIJAOSbId/PyrQiMAoGCCqGSM49BAMCMBMxETAPBgNVBAMM
CENoYW5nZU1IMB4XDTE5MDIxMTIwMTAxNloXDTI5MDIwODIwMTAxNlowEzERMA8G
A1UEAwwIQ2hhbmdlTWUwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAASmBfFpYpIc
IkOhhiPpyeCmtb7+XbkryfNhQ36P3kldmBqW4ew4B262dbtdqNAYMt12uiy0688iVa7D/xotVqTWL
Ur39aCBQkeGWo4GBMH8wHQYDVR0OBBYEFKa0awzTxhTYna19/AHQJ5NM+x5FMEMG
A1UdIwQ8MDqAFKa0awzTxhTYna19/AHQJ5NM+x5FoRekFTATMREwDwYDVQQDDAhD
aGFuZ2VNZYIJAOSbId/PyrQiMAwGA1UdEwQFMAMBAf8wCwYDVR0PBAQDAgEGMAoG
CCqGSM49BAMCA0cAMEQCICNOAV3UD2pUKaQMc1Q/1UyuZ3KjuCssX+fTgvRYoXY2
AiAy6Plw9e01tjmhkEOEPkM62+CBz3jsp+rqgwTgOHKZpQ==
-----END CERTIFICATE-----
</ca>
<cert>
-----BEGIN CERTIFICATE-----
```

Configurar el Router

Configurar el Router

c0r0n4con
Esto lo paramos hackeando

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

- Overview
- Router
- Routing
- Access Points
- SSIDs
- Clients
- VPN
- Firewall
  - Basic
  - Traffic Rules
  - Advanced
- Captive Portal
- Alert/Notification

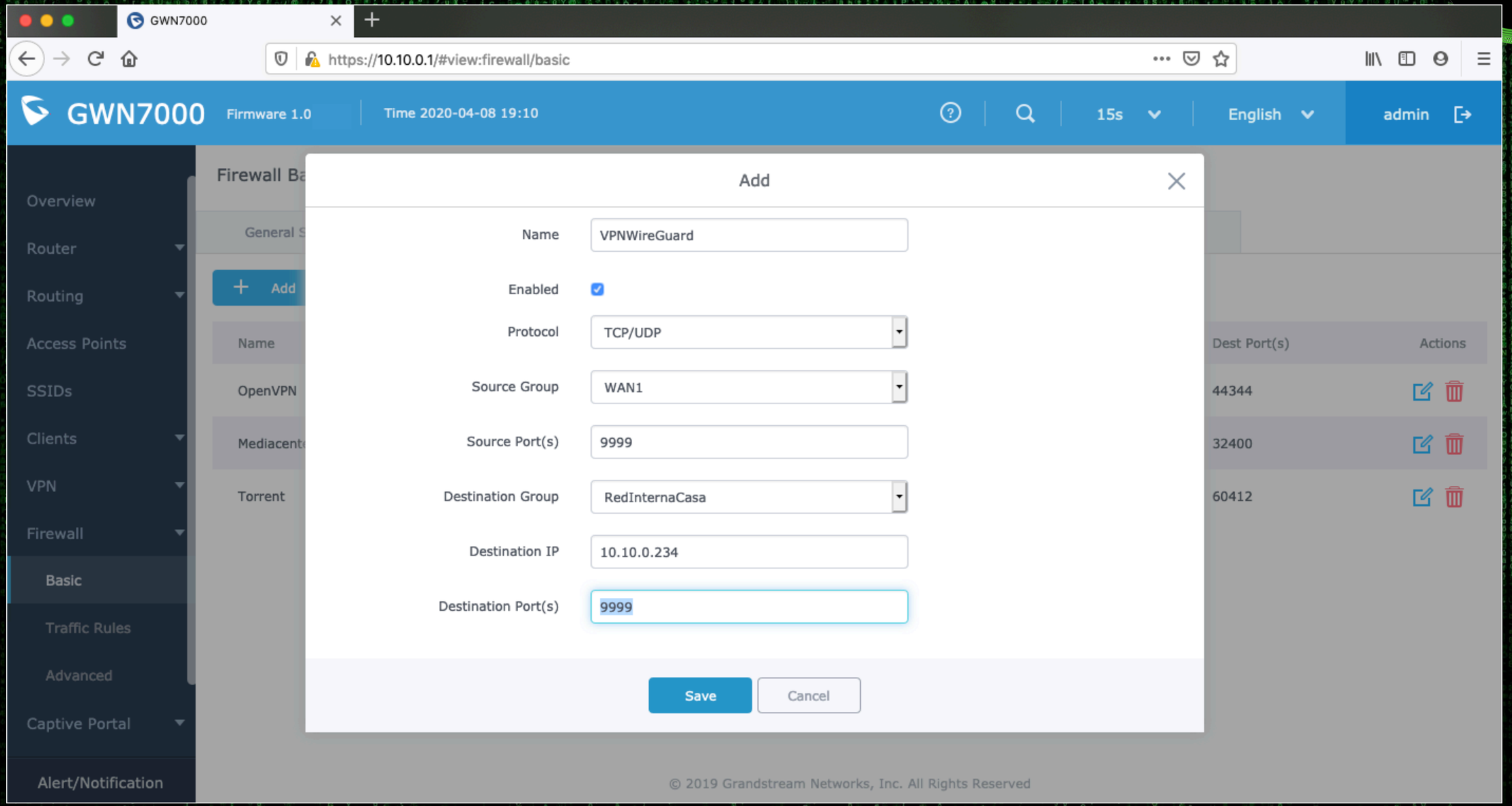
Firewall Basic Settings

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

+ Add

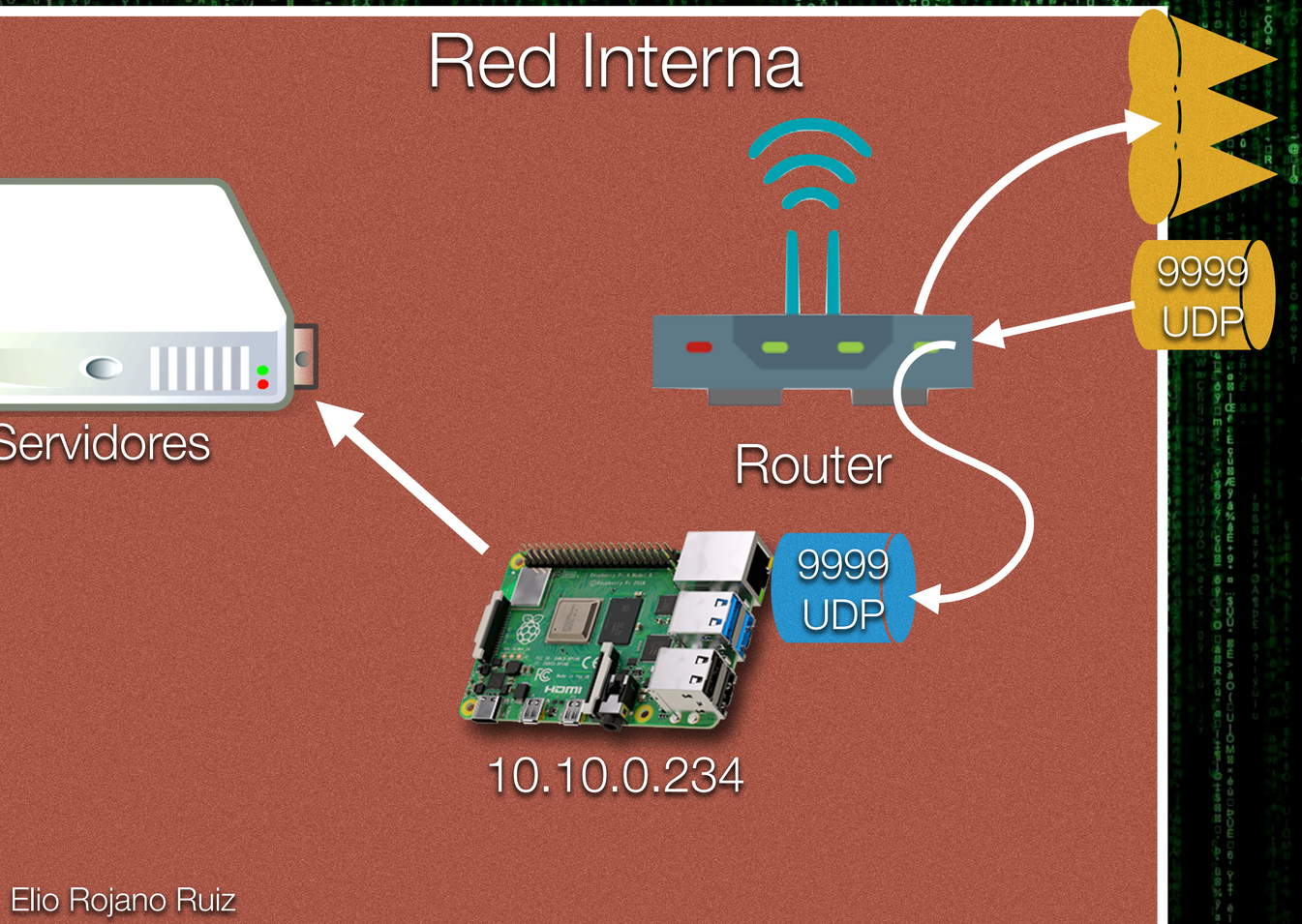
Name	Enabled	Protocol	Src Group	Src Port(s)	Dest Group	Dest IP	Dest Port(s)	Actions
OpenVPN	✗	UDP	WAN1	44344	RedInternaCasa	10.10.0.4	44344	
Mediacenter	✓	TCP/UDP	WAN1	56035	RedInternaCasa	10.10.0.7	32400	
Torrent	✓	TCP/UDP	WAN1	60412	RedInternaCasa	10.10.0.7	60412	

Configurar el Router



Elio Rojano Ruiz

Configurar el Router



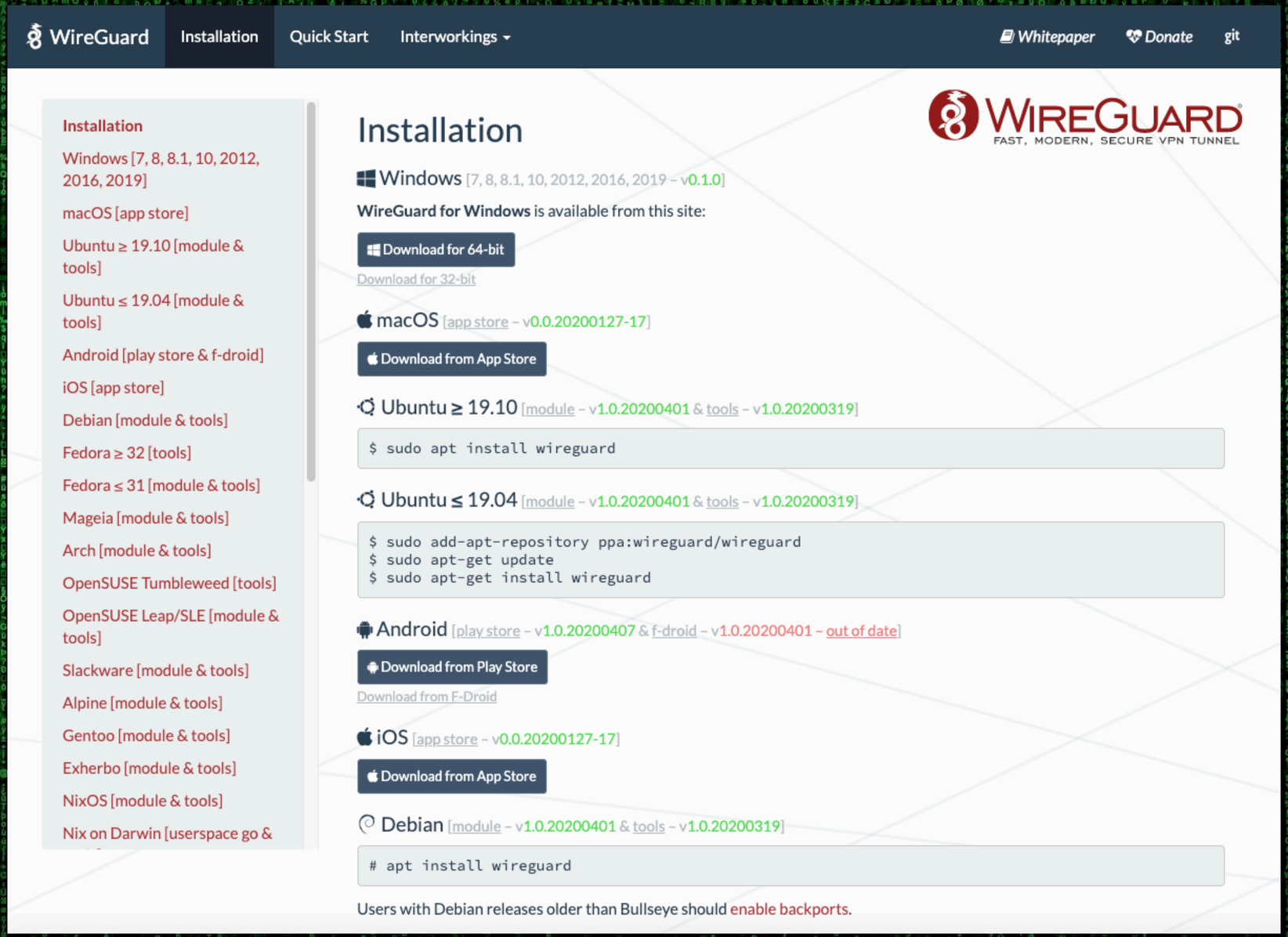
Elio Rojano Ruiz

Configurar los clientes

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

c0r0n4con

Esto lo paramos hackeando



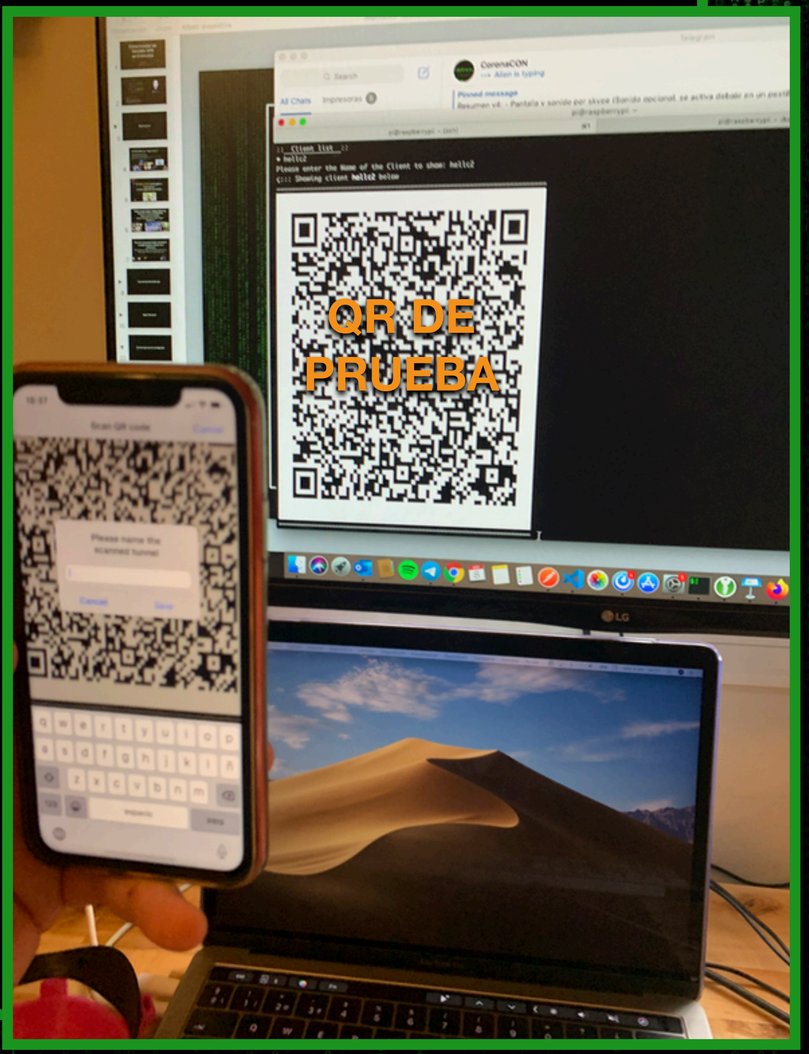
pivpn -qr

c0r0n4con

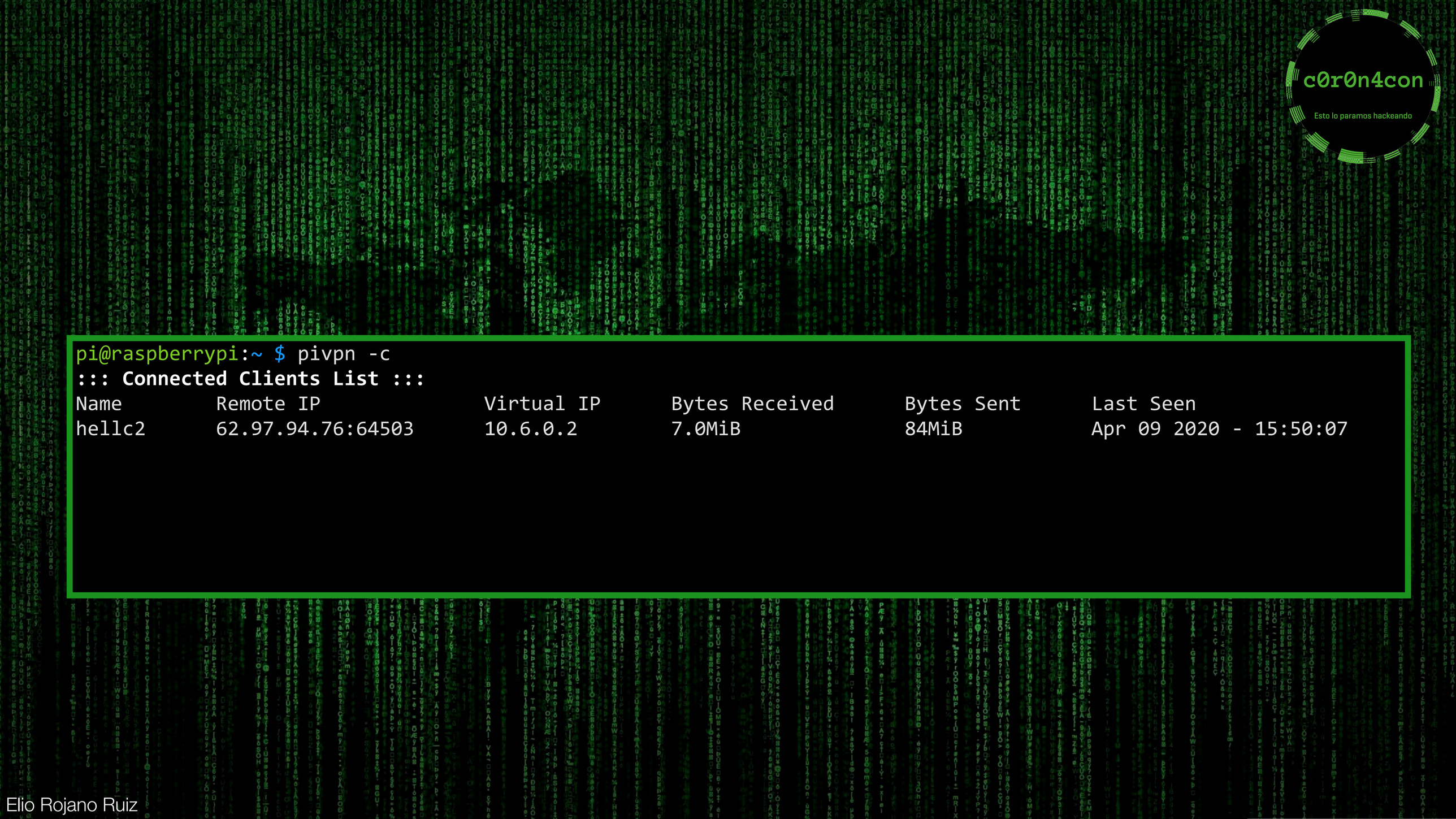
Esto lo paramos hackeando

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

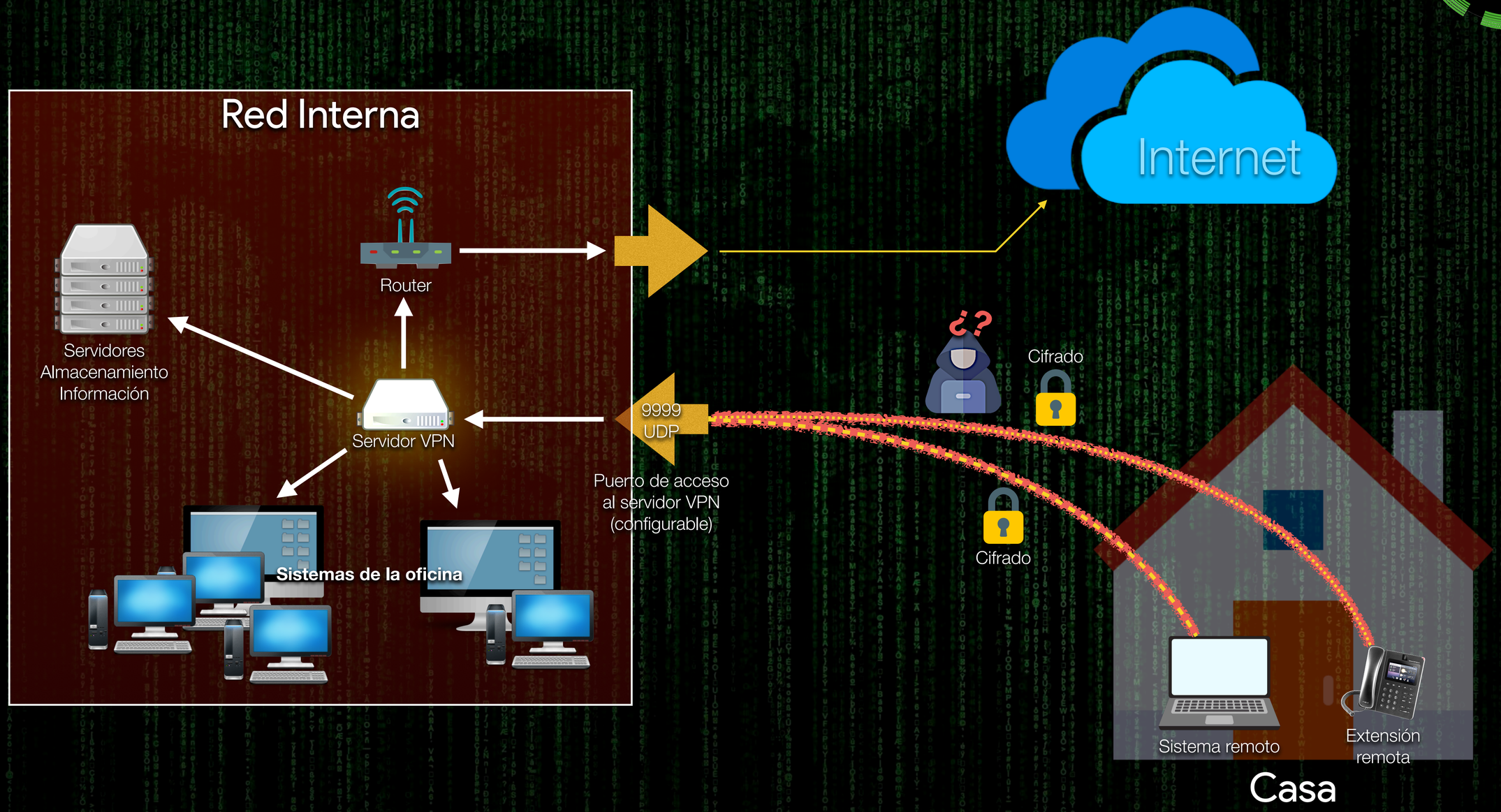
QR DE PRUEBA



Elio Rojano Ruiz


c0r0n4con
Esto lo paramos hackeando
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



Elio Rojano Ruiz

c0r0n4con

Esto lo paramos hackeando

¿Preguntas?

Gracias

c0r0n4con

Esto lo paramos hackeando

Cruz Roja

Elio Rojano Ruiz