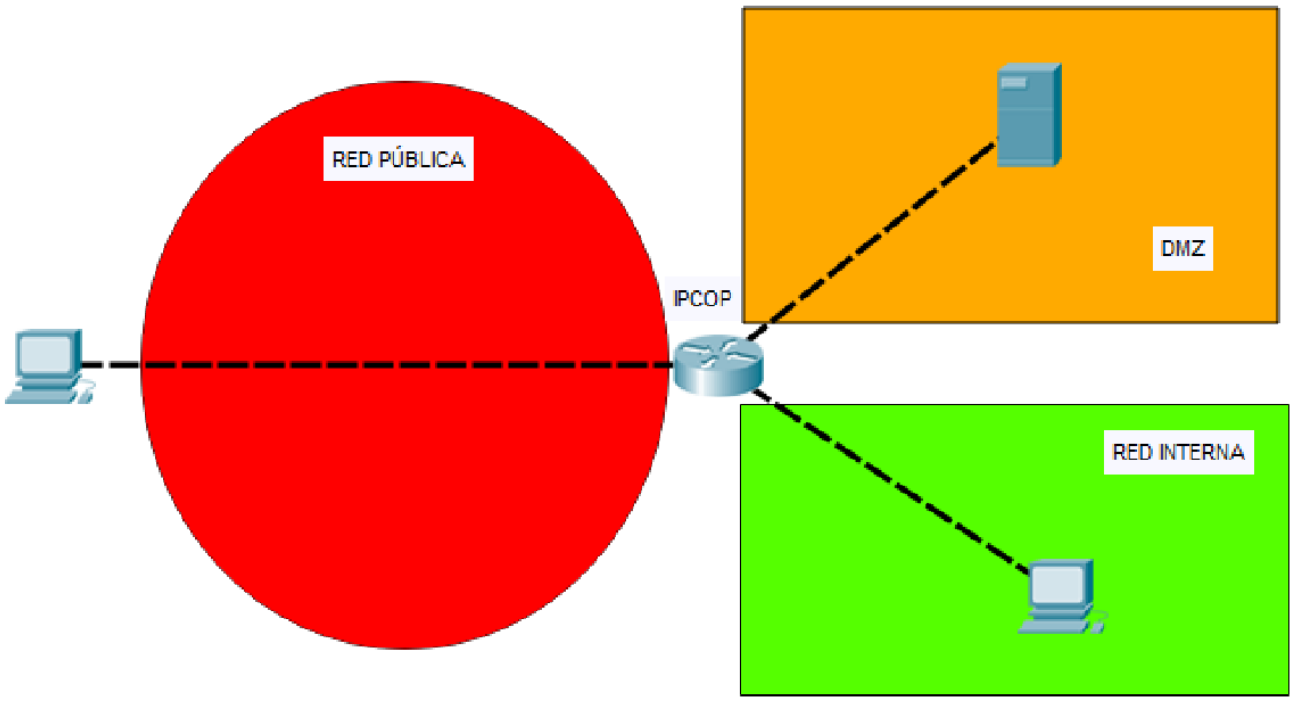
Instalación de IPCOP como *Firewall*

Ismael Macareno Chouikh

2025-02-07

Índice

1. Esquema de red



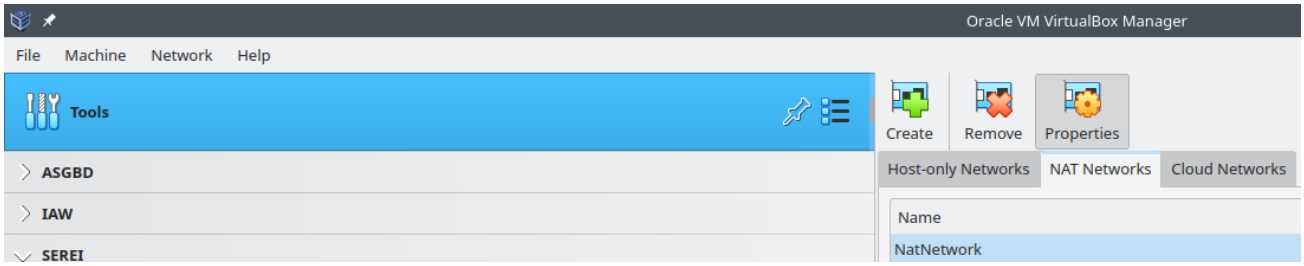
Máquina	Red	Dirección IP	Color
IPCOP	10.0.1.0/17	10.0.1.0/17	naranja
	192.168.1.0/24	192.168.1.1/24	verde
	172.26.0.0/16	172.26.0.0/16	roja
Windows 10 ltsc	192.168.1.0/24	192.168.1.4/24	verde
Windows 7 Ultimate	10.0.1.0/17	10.0.1.4/17	naranja

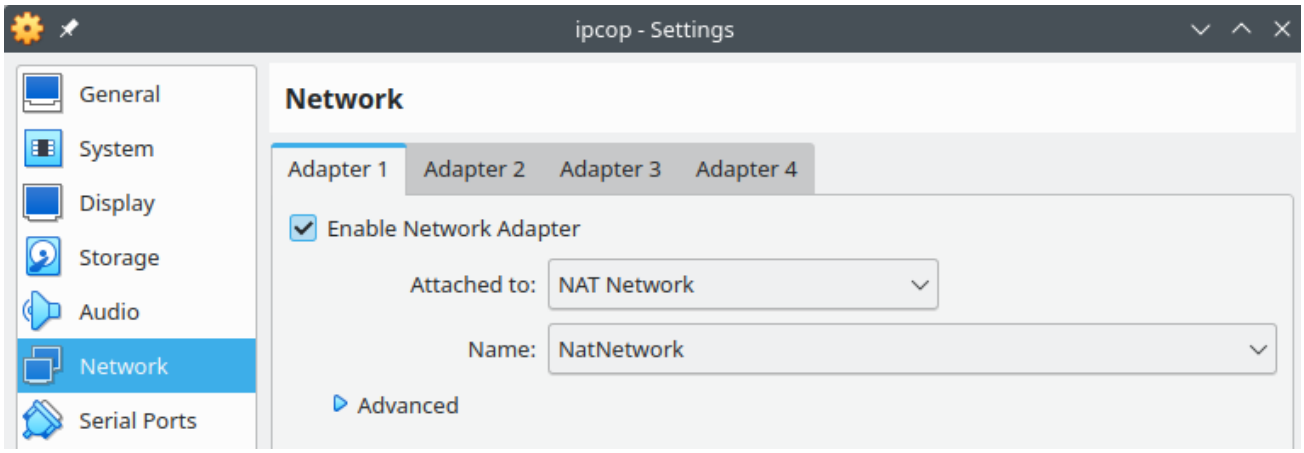
2. Entorno

- Máquina Virtual ipcop
  - RAM: 4096
  - Almacenamiento: 30 GiBi
  - Procesador: 1
  - Tarjetas de red:
    - 1 ->Red NAT
    - 2 ->Red Interna
    - 3 ->Red Interna

A la hora de habilitar la **red nat** es posible que nos de fallo la configuración de la MV, para solucionar este problema lo que tendremos que hacer será lo siguiente:

1. Clic derecho en **herramientas**
2. Tools ->*network manager*
3. Crear





3. Instalación de IPCOP

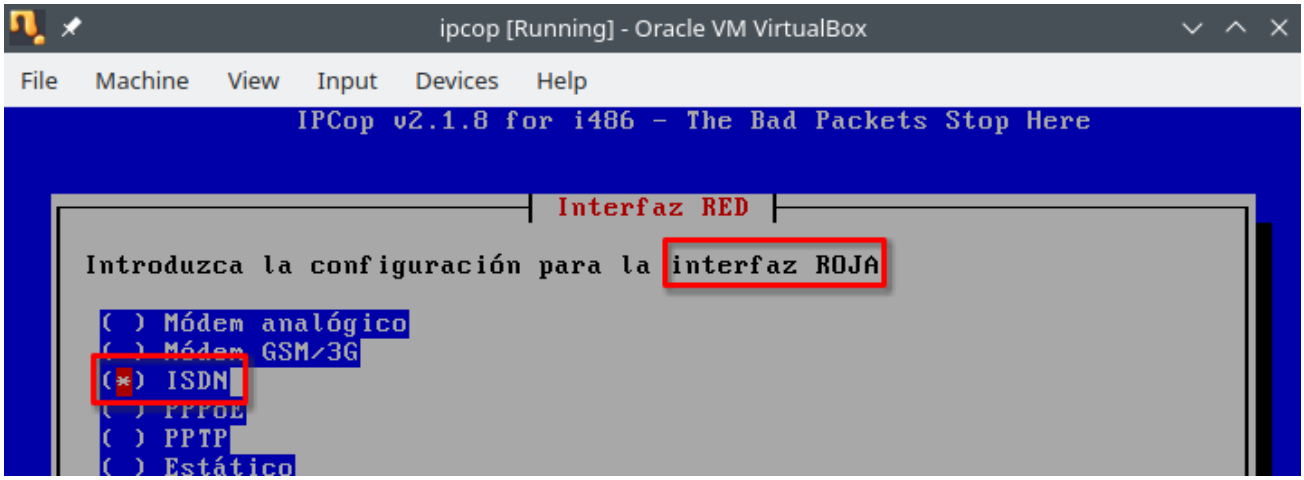
Los primeros pasos de la instalación son similares a los de cualquier otra máquina instalada:

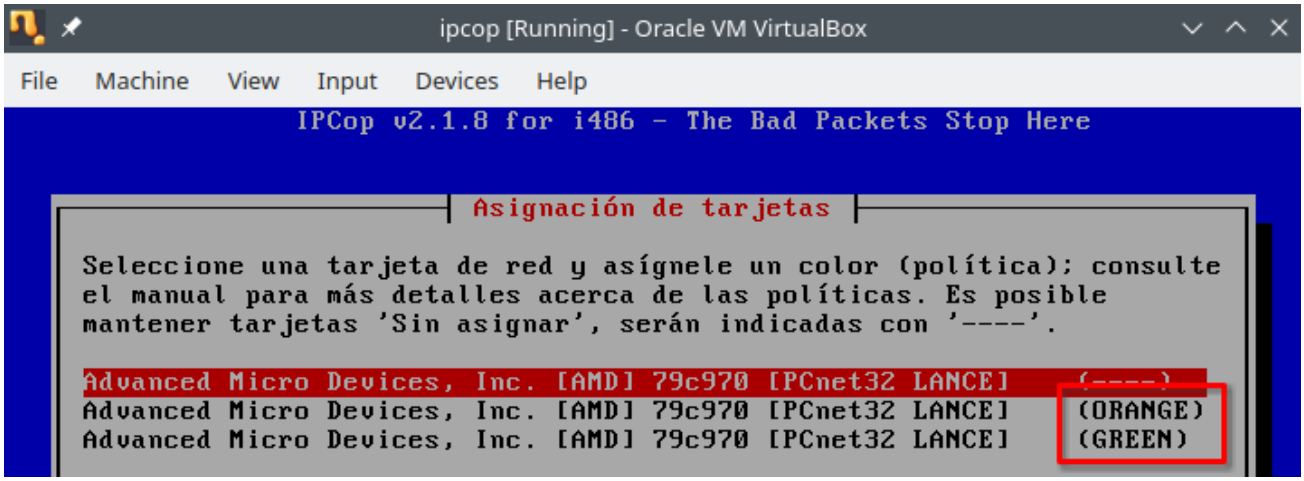
- Selección de idioma del sistema
- Selección de idioma del teclado
- Selección de disco donde se va a instalar el S.O

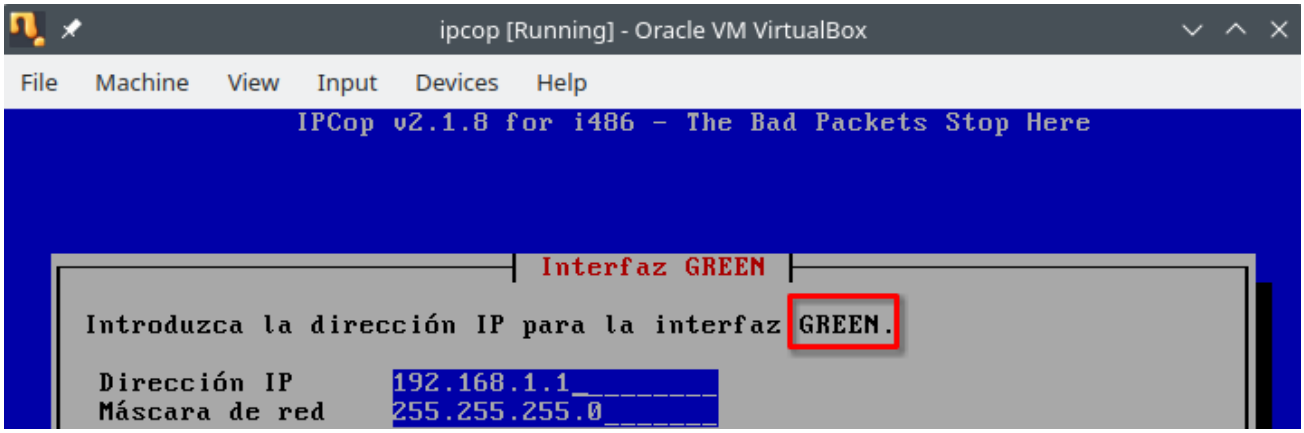
Pero llegados a un punto es donde la instalación cambia con muchísima diferencia, este punto es en el que se nos pregunta por las interfaces de la MV, como bien sabemos tenemos tres interfaces de red

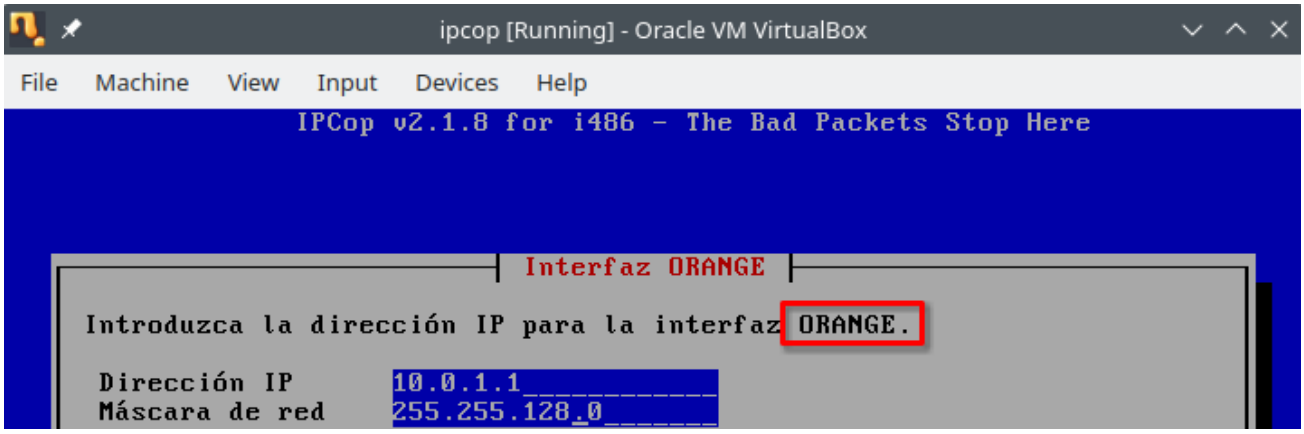
1. Red NAT
2. Red interna (*switch* ipcop)
3. Red interna (*switch* ipcop)

Debido a esto tendremos que seguir lo siguiente:


ipcop [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
IPCop v2.1.8 for i486 - The Bad Packets Stop Here
Interfaz RED
Introduzca la configuración para la interfaz ROJA
( ) Módem analógico
( ) Módem GSM/3G
(*) ISDN
( ) PPPoE
( ) PPTP
( ) Estático


ipcop [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
IPCop v2.1.8 for i486 - The Bad Packets Stop Here
Asignación de tarjetas
Seleccione una tarjeta de red y asígnele un color (política); consulte el manual para más detalles acerca de las políticas. Es posible mantener tarjetas 'Sin asignar', serán indicadas con '----'.
Advanced Micro Devices, Inc. [AMD] 79c970 [PCnet32 LANCE] (----)
Advanced Micro Devices, Inc. [AMD] 79c970 [PCnet32 LANCE] (ORANGE)
Advanced Micro Devices, Inc. [AMD] 79c970 [PCnet32 LANCE] (GREEN)

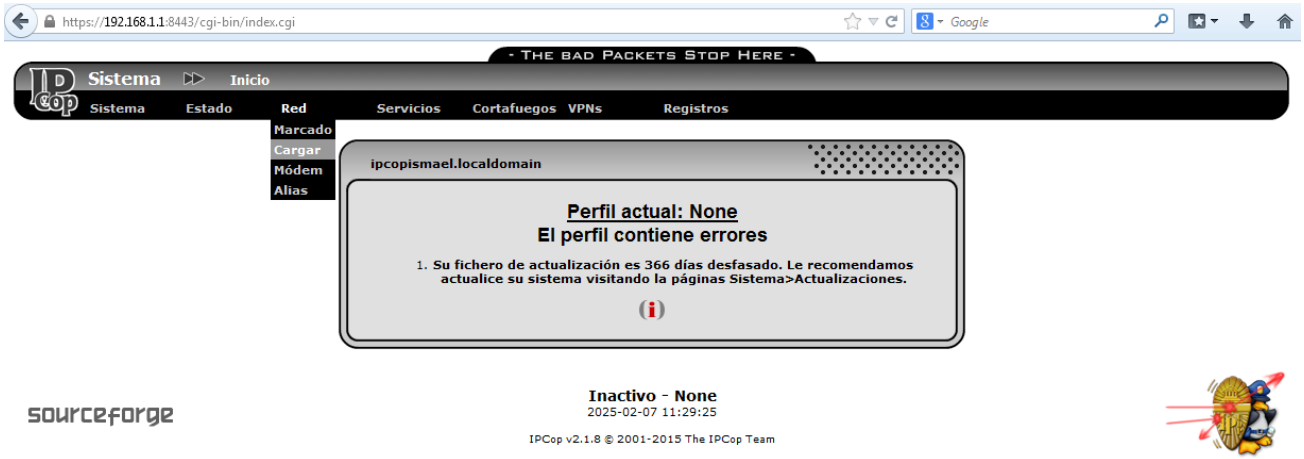

ipcop [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
IPCop v2.1.8 for i486 - The Bad Packets Stop Here
Interfaz GREEN
Introduzca la dirección IP para la interfaz GREEN.
Dirección IP 192.168.1.1
Máscara de red 255.255.255.0



4. Configuración de OpenVPN en IPCOP

Para configurar una VPN en IPCOP tendremos que acceder a su interfaz GUI web la cuál es accesible desde:

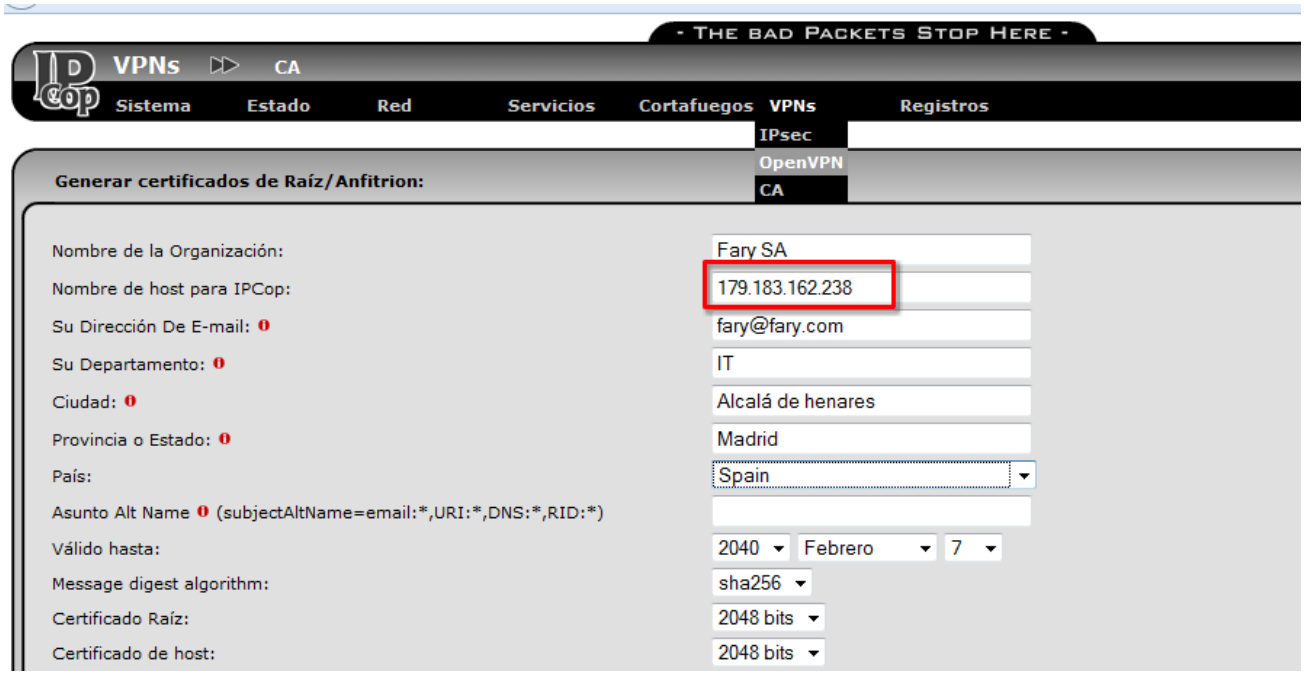
- https://DIRECCIONIP:8443



Una vez estemos en la interfaz web de IPCOP lo que tendremos que hacer será seguir la ruta:

1. VPNs
2. CA
3. Generar certificado de Raíz/Anfitrión

Configuraremos el nuevo certificado de la siguiente manera:



AVISO

Poner como nombre de host para IPCOP la dirección 179.183.162.238

Luego de haber creado el nuevo certificado raíz lo que tendremos que hacer será activar OpenVPN. Para ello tendremos que acceder a:

1. VPNs
2. OpenVPN

Lo único que tendremos que hacer será:

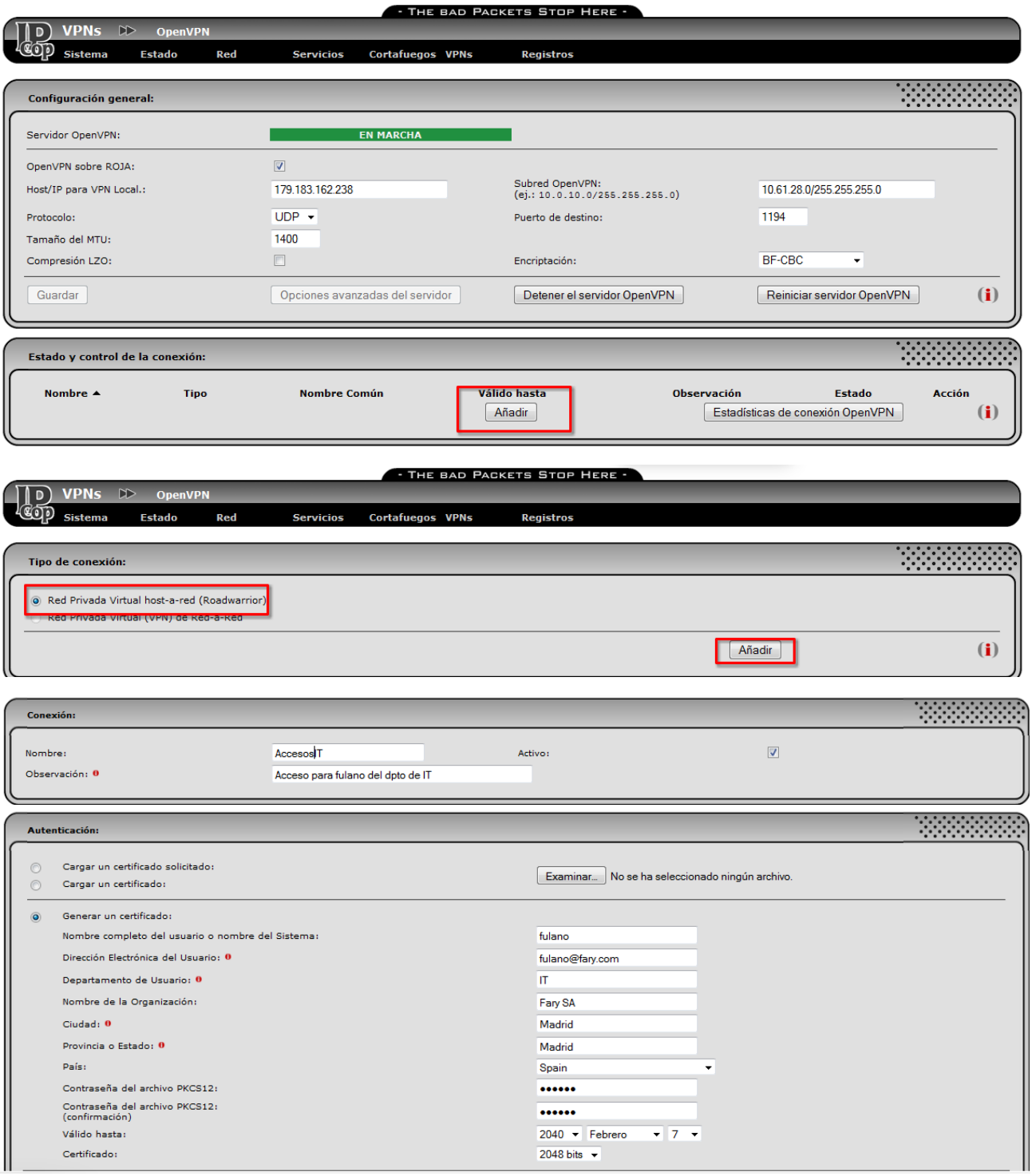
- Activar **OpenVPN sobre roja**
- Poner como **Host/IP para VPN local** la dirección 179.183.162.238
- Guardar los cambios
- Encender el servidor OpenVPN

Luego de haber iniciado el servicio OpenVPN lo que tendremos que hacer será crear un certificado para poder dárselo a otra máquina y que se pueda conectar a la VPN.

4.1. Generación de certificado para conexión a VPN

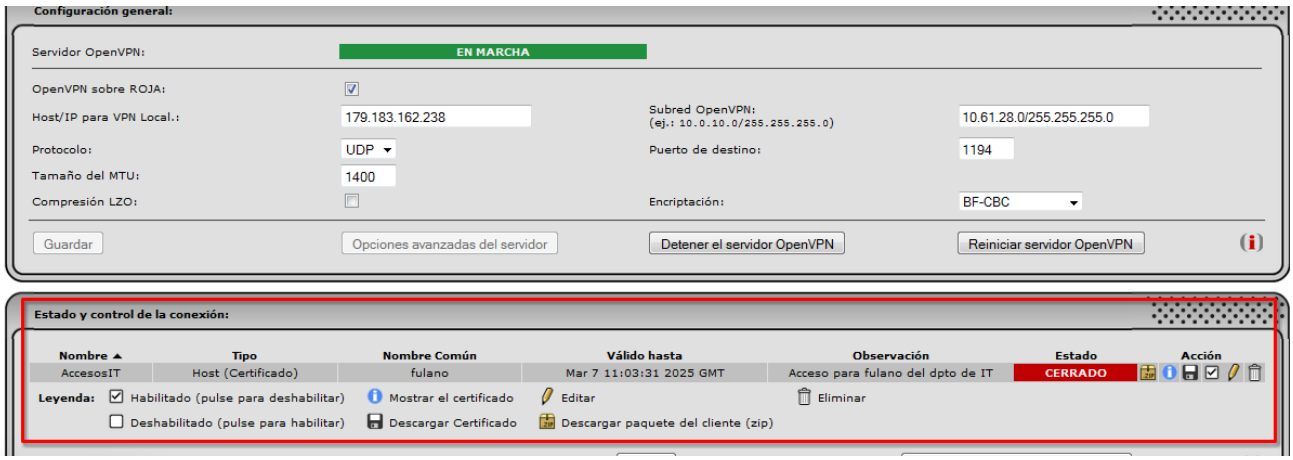
Para esto lo que tendremos que hacer será acceder a:

1. VPNs
2. OpenVPN
3. Estado y control de la conexión
   a) Válido hasta ->añadir



AVISO

El nombre no puede contener espacios, todo junto o falla



4.2. Comprobación de VPN

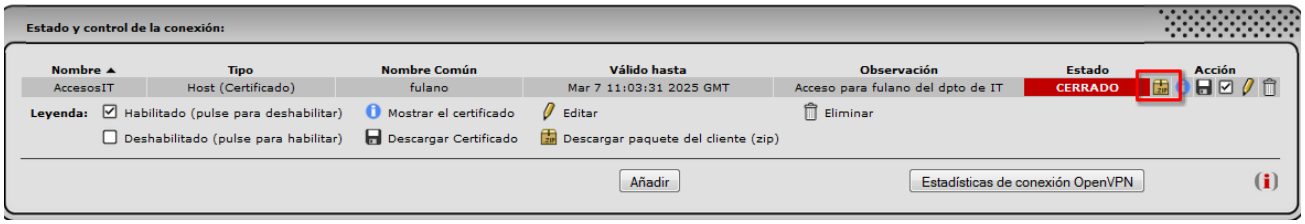
Para comprobar el funcionamiento de la VPN voy a hacer uso de otra MV con un S.O Windows 10 Pro LTSC.

Lo primero que habrá que hacer para comprobar la VPN será descargar el `.zip` con los ficheros

- `x.p12`
- `x.ovpn`

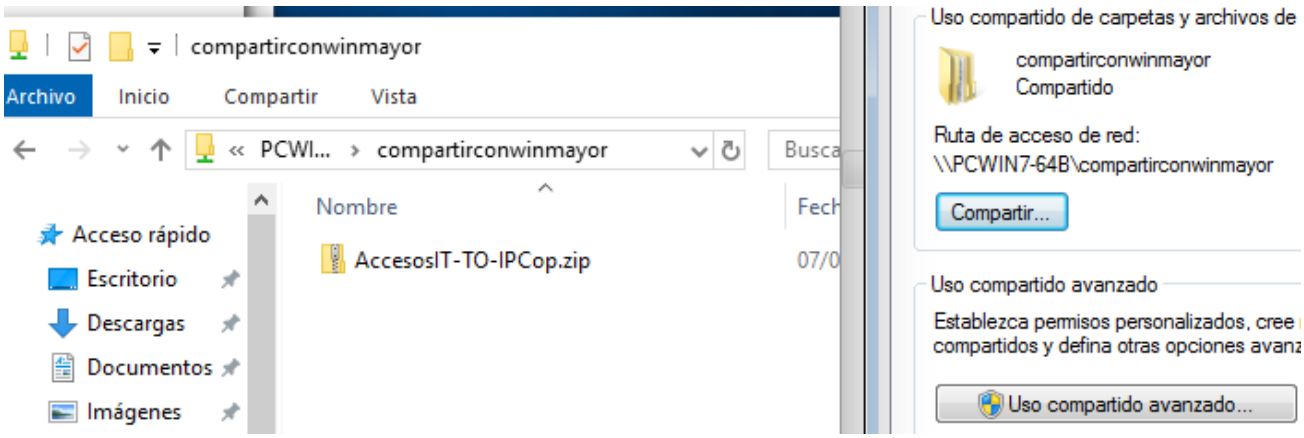
Para esto lo que tendremos que hacer será desde:

1. VPNs
2. OpenVPN
3. Estado y control de la conexión
   a) Descargar ficheros comprimidos en `.zip`



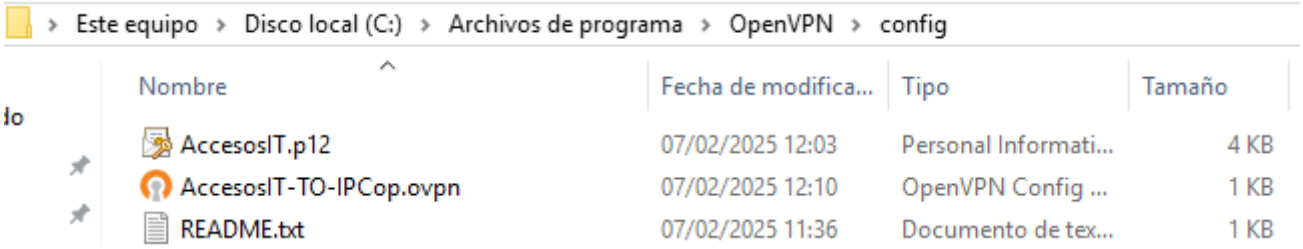
Luego lo que haremos será pasar ese `.zip` a la MV Windows 10 a través de la red con cualquiera de las herramientas que ya conocemos (`scp`, mobaXterm, etc.)

Yo en mi caso como las dos MV están en red interna y odio el `scp` de *Windows* lo que hago es compartir el `.zip` a través de una carpeta compartida de *Windows*

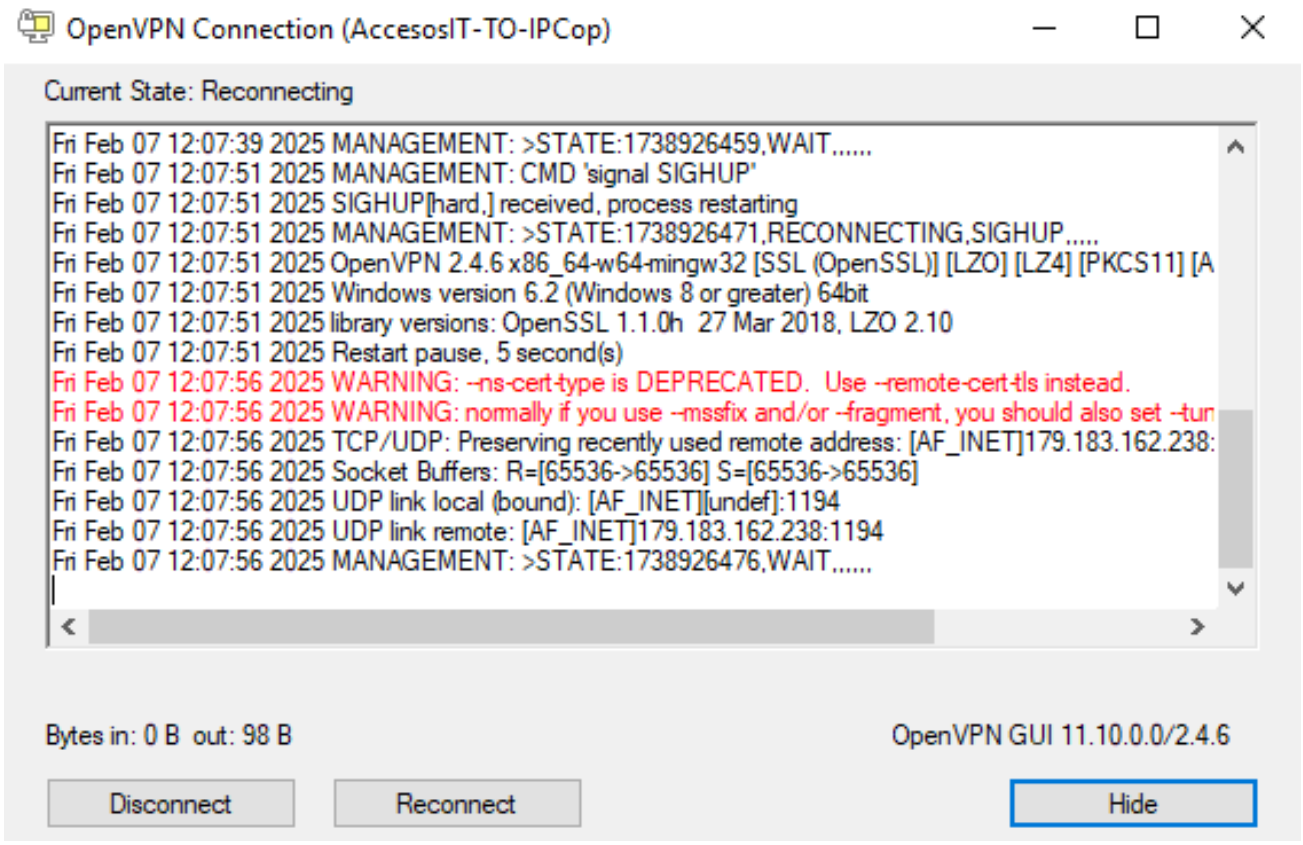


Una vez tengamos el fichero `.zip` en la MV de *Windows 10* lo que tendremos que hacer será descargar openvpn-install-2.4.6-I602.exe en la MV de *Windows 10*.

Cuando hayamos instalado openVPN en la MV de *Windows 10* lo que tendremos que hacer será descomprimir el fichero `.zip` en el directorio `C\Archivos de programa\OpenVPN\config`



Luego de haber hecho lo anterior ya podremos inciar el programa GUI de openVPN



5. Conectividad entre máquinas

Para realizar esta parte de la práctica lo primero que hay que hacer es configuar las redes de las MV de tal manera que cada máquina este conectada a la red correspondiente

- MV *Windows 10 LTSC* –>192.168.1.5/24 (lan-1)
- MV *Windows 7 Ultimate* –>10.0.0.4/17 (dmz-1)

```
Adaptador de Ethernet Ethernet:

   Sufijo DNS específico para la conexión. . :
   Vínculo: dirección IPv6 local. . . : fe80::7421:7308:bb14:e1d6%14
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.1.5
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : 192.168.1.1

Adaptador de Ethernet Ethernet 3:

   Estado de los medios. . . . . . . . . . . : medios desconectados
   Sufijo DNS específico para la conexión. . :
```

```
Adaptador de Ethernet Conexión de área local:

   Sufijo DNS específico para la conexión. . :
   Vínculo: dirección IPv6 local. . . : fe80::849b:8cf:26d3:6c84%11
   Dirección IPv4. . . . . . . . . . . . . . : 10.0.1.4
   Máscara de subred . . . . . . . . . . . . : 255.255.128.0
   Puerta de enlace predeterminada . . . . . : 10.0.1.0

Adaptador de túnel isatap.{E59ABE27-93E1-446A-9AC9-3BA0A5CD9EC6}:

   Estado de los medios. . . . . . . . . . . : medios desconectados
   Sufijo DNS específico para la conexión. . :

Adaptador de túnel Conexión de área local* 3:

   Estado de los medios. . . . . . . . . . . : medios desconectados
   Sufijo DNS específico para la conexión. . :
```

5.1. `icmp` red verde a la naranja permitido

Para realizar esta parte lo que tendremos que hacer será primeramente en la MV IPCOP añadir unas reglas `iptables`

- `iptables -t nat -A POSTROUTING -s 10.0.0.0/17 -o <INTERFACE>-j MASQUERADE`
- `iptables -A FORWARD -s 10.0.1.4/32 -d 192.168.1.4/32 -p icmp --icmp-type echo-request -j ACCEPT`
- `iptables -A FORWARD -s 192.168.1.4/32 -d 10.0.1.4/32 -p icmp --icmp-type echo-reply -j ACCEPT`

Una vez hecho esto ya podremos hacer `ping` desde la MV *Windows 10 LTSC* (lan) a la DMZ

```
C:\Users\alumno>ping 10.0.1.4

Haciendo ping a 10.0.1.4 con 32 bytes de datos:
Respuesta desde 10.0.1.4: bytes=32 tiempo=3ms TTL=127
Respuesta desde 10.0.1.4: bytes=32 tiempo=2ms TTL=127
Respuesta desde 10.0.1.4: bytes=32 tiempo=2ms TTL=127
Respuesta desde 10.0.1.4: bytes=32 tiempo=2ms TTL=127

Estadísticas de ping para 10.0.1.4:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 2ms, Máximo = 3ms, Media = 2ms
```

5.2. `icmp` red verde a la roja permitido

- `iptables -A FORWARD -s 192.168.1.0/24 -d 172.26.0.0/16 -p icmp --icmp-type echo-request -j ACCEPT`

```
C:\Users\alumno>ping 172.26.0.0

Haciendo ping a 172.26.0.0 con 32 bytes de datos:
Respuesta desde 172.26.0.0: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.26.0.0: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.26.0.0: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.26.0.0: bytes=32 tiempo=1ms TTL=64

Estadísticas de ping para 172.26.0.0:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 1ms, Media = 1ms
```

5.3. `icmp` red naranja a la verde denegado

- `iptables -A FORWARD -s 10.0.0.0/17 -d 192.168.1.0/24 -p icmp --icmp-type echo-request -j REJECT`

```
C:\Users\alumno>ping 192.168.1.4

Haciendo ping a 192.168.1.4 con 32 bytes de datos:
Respuesta desde 10.0.1.0: Puerto de destino inaccesible.
Respuesta desde 10.0.1.0: Puerto de destino inaccesible.
Respuesta desde 10.0.1.0: Puerto de destino inaccesible.
Respuesta desde 10.0.1.0: Puerto de destino inaccesible.

Estadísticas de ping para 192.168.1.4:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
```

5.4. `icmp` red naranja a la roja denegado

- `iptables -A FORWARD -s 10.0.0.0/17 -d 172.26.0.0/16 -p icmp --icmp-type echo-request -j REJECT`

```
C:\Users\alumno>ping 172.26.0.0

Haciendo ping a 172.26.0.0 con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 172.26.0.0:
    Paquetes: enviados = 4, recibidos = 0, perdidos = 4
    (100% perdidos),
```

6. Bibliografía

- Vídeo Configuración OpenVPN
  - https://youtu.be/0VJzdindSS8?si=lhiAFVuz-QYRJ0Di

- Vídeo IPCOP
  - https://youtu.be/M_r0vEq_heY?si=3Rmjg-l7lVoriGyd
- zeppelinux
  - https://www.zeppelinux.es/configurar-ipcop-como-encaminador-nat-router/

Adjunto PDF Universidad del Azuay