Planificación y Administración de Redes – ASIR1

**Práctica 4: Nivel de transporte. Cortafuegos**

| Módulo profesional: Planificación y Administración de Redes  Ciclo Formativo: C.F.G.S. Administración de Sistemas Informáticos en Red Curso: 1º  Profesor: Anabel Serradilla Fernández |
| --- |

| Esta práctica se realizará de forma individual o en grupos de máximo dos personas  Todos los pasos deben ser documentados mediante capturas de pantalla y/o explicaciones que se incluirán en la entrega. |
| --- |

**Alumno1: Enrique Gonzalez de Anleo Aliaga**

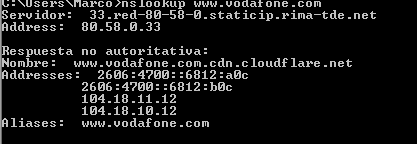
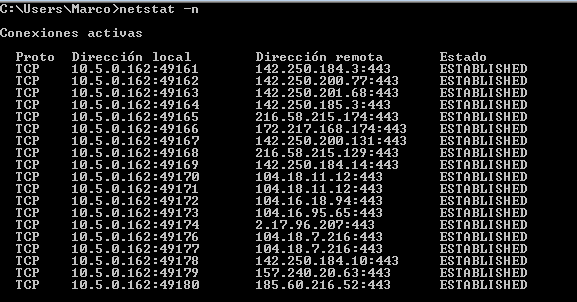
**Alumno2: Marco Batista Calado**

**1. Análisis de conexiones y puertos en Windows**

En una máquina virtual Microsoft Windows que tenga acceso a Internet, cierra todos los programas y aplicaciones que accedan a la red (navegadores, clientes FTP, de mensajería instantánea, etc.).

A continuación, ejecuta un navegador y accede a http://www.vodafone.com.

Mediante la orden "*netstat -n*" comprueba qué conexiones tiene establecidas tu PC. Realiza una captura de cada uno de los casos y responde:

1.1- Mediante "*ping*" o "*nslookup*" comprueba cuál es la dirección IP de www.vodafone.com. Aporta capturas de "*netstat -n*" en las que se vean conexiones de tu equipo con esta IP. Después, rellena esta tabla: 

| **IP de www.vodafone.com** | **Puertos usados en tu PC** | **Puerto/s usados en www.vodafone.com** |
| --- | --- | --- |
| 104.18.11.12 | 49170/49171 | 443 |
| 104.18.10.12 |  |  |

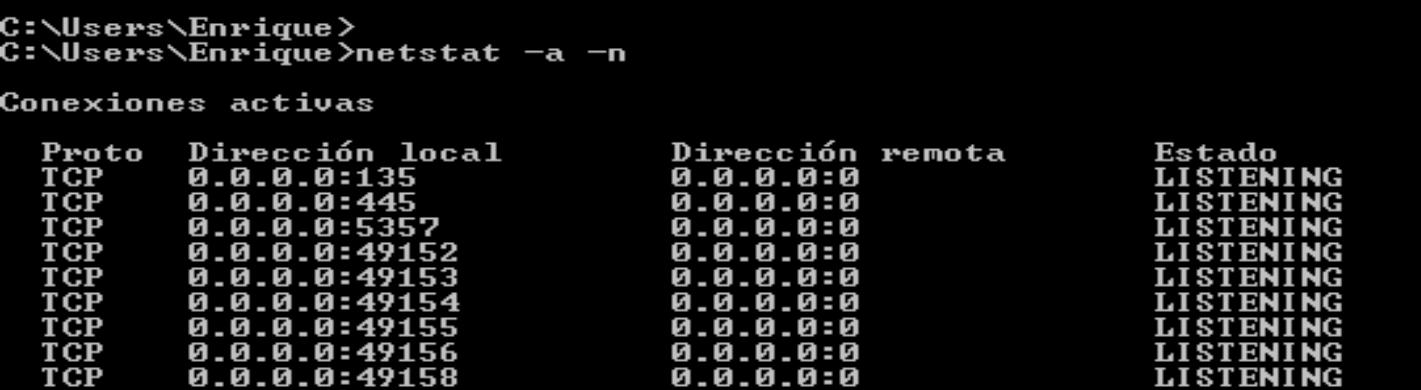
1.2- ¿Por qué aparecen conexiones a otras direcciones IP diferentes a la de www.vodafone.com?

Aparecen otras conexiones debido a que puede conectarse a vodafone por diferentes IP (utilizan varias IP para evitar sobrecargas).

1.3- Recarga la página http://www.vodafone.com y ejecuta "*netstat*" (sin la opción -n) ¿Qué diferencia obtienes entre la ejecución de "*netstat*" y "*netstat-n*"?

Con -n nos muestra el formato numérico

1.4- Cierra todos los programas y aplicaciones que accedan a Internet y ejecuta "netstat-a -n". - ¿Qué puertos están en escucha en tu PC? (LISTENING)



- Busca en internet 3 de los puertos que tienes en escucha e indica a qué servicios corresponden típicamente (FTP, carpetas compartidas de Windows, etc.)

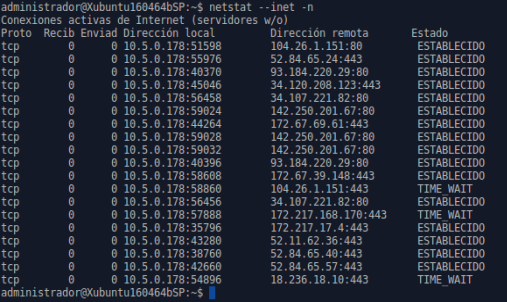
| Puerto | Servicio asociado |
| --- | --- |
| 135 | Servicio RPC |
| 445 | Acceso directo a redes TCP/IP MS |
| 5357 | Aplicaciones |

**2. Análisis de conexiones y puertos en Linux**

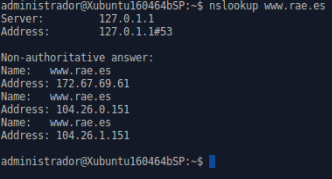
En una máquina virtual Linux que tenga acceso a Internet, cierra todos los programas y aplicaciones que accedan a la red (navegadores, clientes FTP, de mensajería instantánea, etc.).

A continuación ejecuta un navegador y accede a http://www.rae.es.

Mediante la orden "*netstat --inet -n*" compruebe qué conexiones tiene establecidas tu equipo. Realiza una captura y responde:

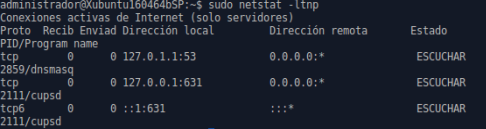


1.5- Mediante "*ping*" o "*nslookup*" comprueba cuál es la dirección IP de www.rae.es. Aporta capturas en las que se vean conexiones de tu equipo con esta IP. Rellena esta tabla:

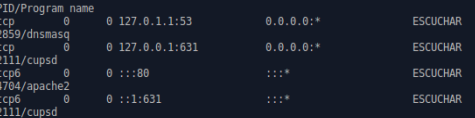


| IP de www.rae.es | Puertos usados en su PC | Puerto/s usados en www.rae.es |
| --- | --- | --- |
| 172.67.69.61 | 44264 | 443 |
| 104.26.0.151 |  |  |
| 104.26.1.151 | 51598 | 80 |

1.6- Cierra todos los programas y aplicaciones que accedan a Internet. A continuación, ejecuta "*netstat -ltnp*" como superusuario.

- ¿Qué puertos están en escucha en tu PC (LISTENING)? 

- Instala un servidor Web Apache (*sudo apt-get install apache2*) y vuelve a comprobar qué puertos tiene en escucha tu equipo con *netstat-ltnp*.

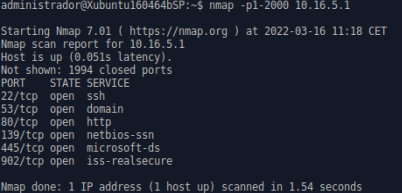


- ¿En qué puerto está escuchando Apache?

Puerto 80

- Instala la aplicación *nmap* (*sudo apt-get install nmap*).

- Escanea los primeros 2000 puertos del servidor de clase (*nmap -p1-2000 ip\_servidor*). ¿Qué puertos tiene abiertos este servidor? Probablemente, ¿Qué servicios está ofreciendo en Internet?



Puertos abiertos y servicios: 22(ssh: protocolo que nos da acceso remoto a un servidor por medio de un canal seguro en el que toda la información está cifrada), 53(dominio), 80(http: puerto de internet), 139(netbios-ssn: capa de software desarrollado para enlazar un sistema operativo de red con hardware específico),445(microsoft-ds: acceso directo a redes TCP / IP MS que no requiere el uso de una capa NetBIOS) y 902(iss-realsecure).

- Realiza un escaneado de puertos de los equipos que tienen configuración automática en la clase (están en el rango 10.5.0.10 a 10.5.0.254). ¿Qué equipos ha detectado? ¿Qué puertos tienen abiertos?

Equipos: 102, 103, 104, 105, 111,112,113,115, 120, 122, 124, 126, 132, 135, 136, 138, 140, 141, 143, 149, 179, 180, 116

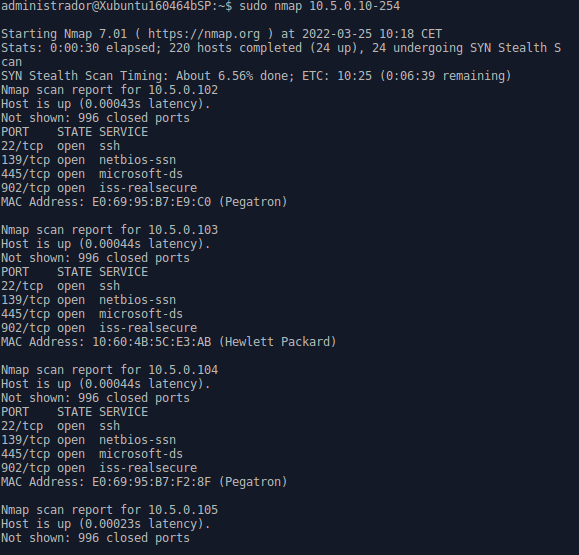
Puertos: 22, 139, 445, 902, 53, 4159

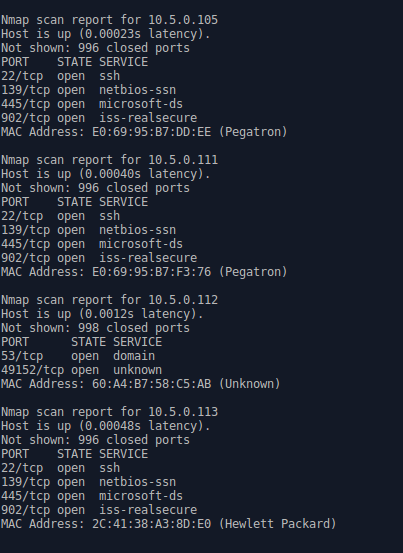
Instalar nmap: sudo apt-get install nmap (si no funciona), primero actualizamos:

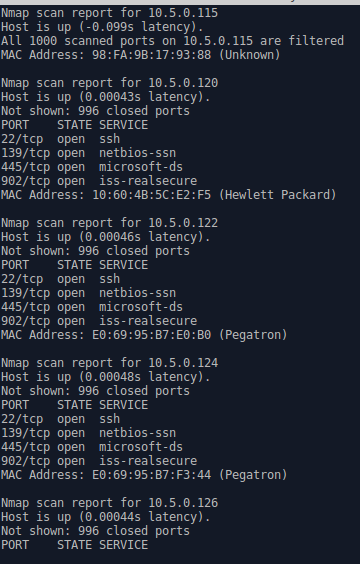
sudo apt-get update

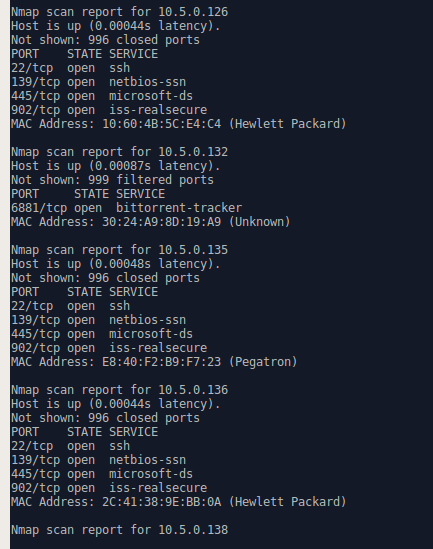
ejecutamos sudo rm -r /var/lib/dpkg/lock, y ya:

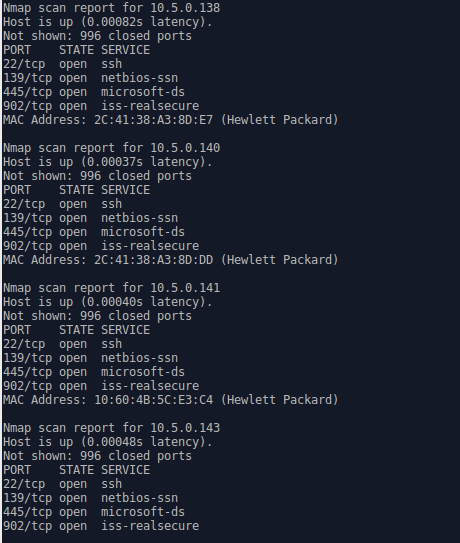
sudo nmap 10.5.0.10-254

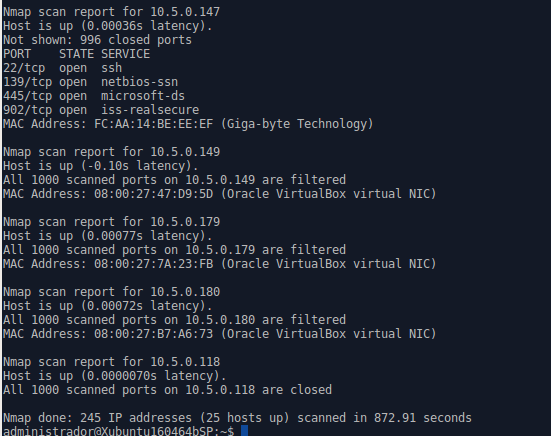












**3. Configuración de un servicio FTP en el puerto 21**

| El servicio FTP se estudiará a fondo en el próximo curso, pero con esta práctica se va a usar ese servicio para entender mejor el concepto de puerto y el funcionamiento del nivel de transporte, dejando la configuración avanzada para las prácticas del segundo curso.  Se proporcionan capturas para ayudar a configurar el servidor. |
| --- |

En una máquina virtual de Windows limpia (si es necesario restaura la última “snapshot inicial” disponible) asegúrate de que tiene una única tarjeta de red en modo puente.

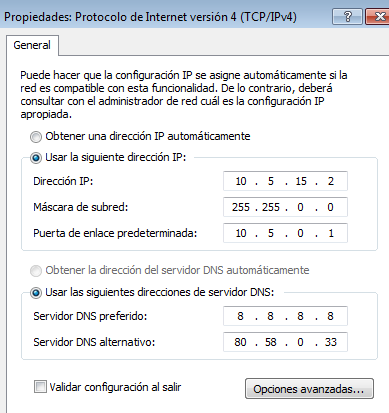
La configuración de red de esta máquina debe ser la siguiente:

• IP: 10.5.X.Y, con X= su número de clase e Y cualquier número libre.

• NM: 255.255.0.0

• GW: 10.5.0.1

• DNS: Cualquiera válido. Por ejemplo 80.58.0.33, 8.8.8.8, 80.58.32.97, 8.8.4.4, etc.

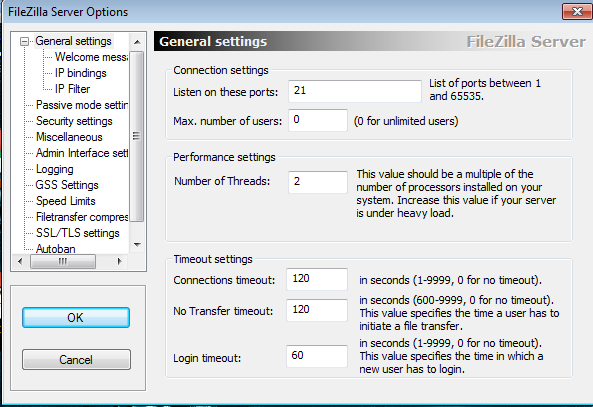


Descarga e instala el servidor FTP “Filezilla Server”. La URL desde la que se puede descargar el software es: https://filezilla-project.org/ .

IMPORTANTE: Durante la instalación **no se debe cambiar** el puerto de escucha que utiliza Filezilla Server para conectarse a la interfaz de configuración del Filezille Server.

- Una vez instalado, configura Filezilla para aceptar conexiones por el puerto 21 (FTP)





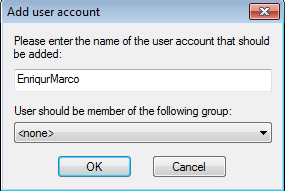
- Crea una carpeta en C: denominada "MiFTP”



- Crea un usuario en Filezilla Server con tu nombre (p.e. "juan", "ana", etc.)



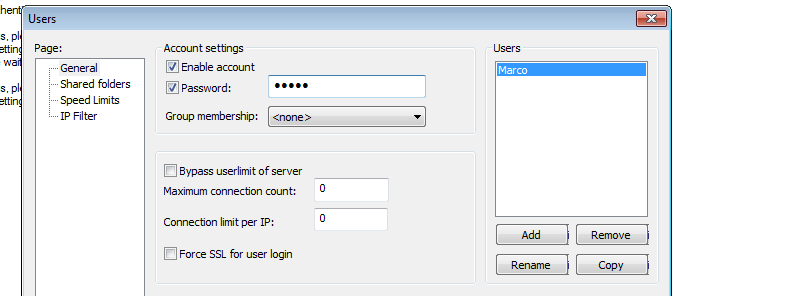




- Asigna a ese usuario un password.

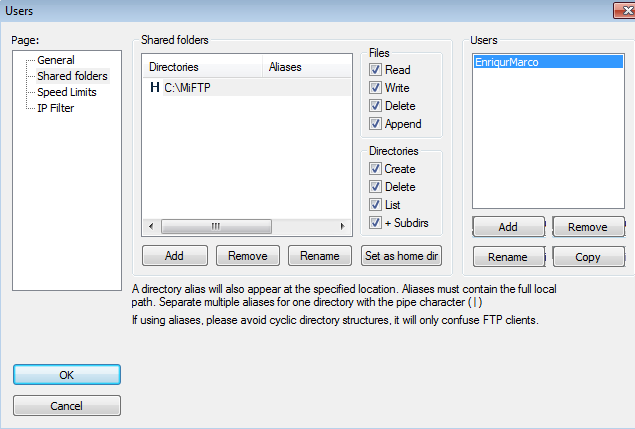


**EJEMPLO MEJOR VISTO**

****

- Asigna a ese usuario permisos de lectura, escritura, etc.. sobre el directorio C:\MiFTP





No olvides desactivar el cortafuegos de Windows provisionalmente para que el servidor FTP sea accesible. Más adelante, se configurará adecuadamente el cortafuegos y se podrá volver a activar. **Desactivar el cortafuegos es una mala práctica que pone en peligro la seguridad del sistema.**



- Comprueba mediante "*netstat -a -n*" que tu servidor FTP está escuchando en el puerto 21.



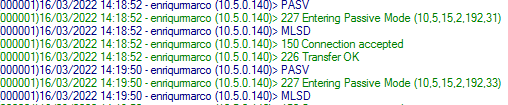
- Desde otra máquina virtual (Windows o Linux) que hará las funciones de cliente, instala e inicia Filezilla Client y accede al servidor FTP de la M.V.



- Envía y descarga algún fichero de más de 1 KB para comprobar que el servidor FTP funciona correctamente.



- Al enviar un fichero, se establece una conexión adicional para el canal de datos. En este caso se utiliza "FTP pasivo". Observando los logs de Filezilla o mediante Wireshark, indica a través de qué puertos en el servidor FTP se realizan estas conexiones.



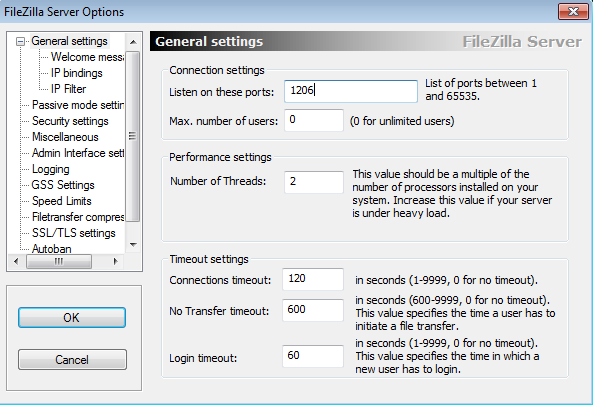
Puertos se pasan los dos últimos números de la línea Entering PAssive MOde (10.5.2.192.31) [en este caso el 192 y el 31] y unirlos 192=11000000,31=00011111->1100000000011111=49183

Puertos se pasan los dos últimos números de la línea Entering PAssive MOde (10.5.2.192.33) [en este caso el 192 y el 33] y unirlos 192=11000000,33=00100001->1100000000100001=49185

**4. Modificación de puertos en un servicio FTP**

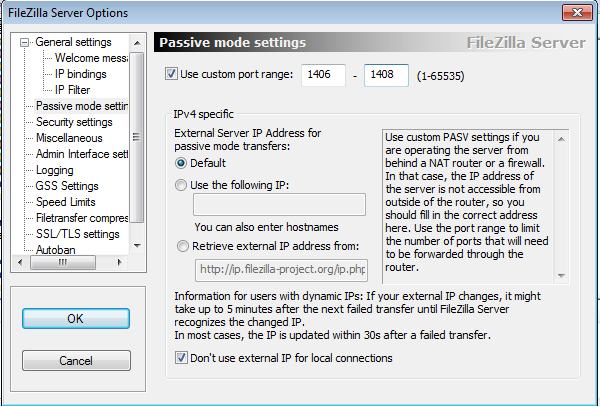
- Modifica el puerto del servidor FTP para que las conexiones se acepten por el puerto 1206





- Fuerza que las conexiones para las transferencias en modo pasivo se realicen por los puertos del 1406 al 1408





- Comprueba mediante "*netstat -a -n*" que tu servidor FTP está escuchando en el puerto 1206.

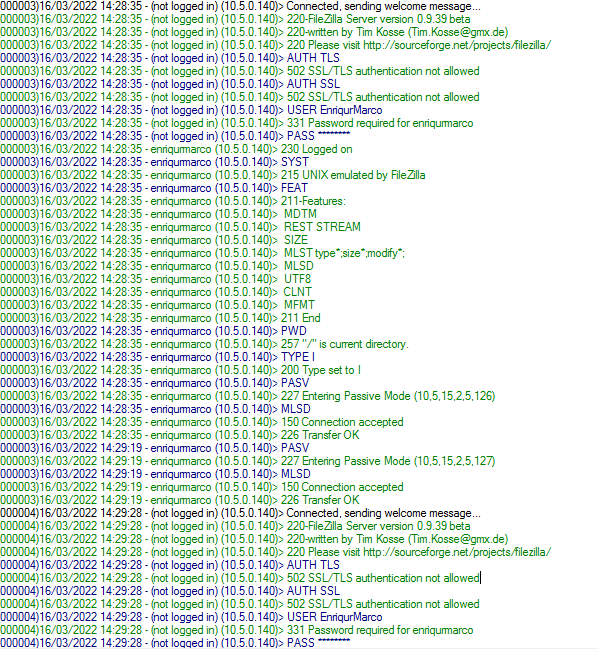


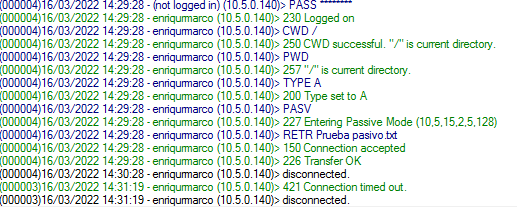
- Accede con Filezilla Client desde tu PC cliente con la nueva configuración.



- Comprueba, enviando varios ficheros, que se usan los puertos configurados para FTP pasivo.







Deben salir por los puertos entre el 1406 y el 1408,

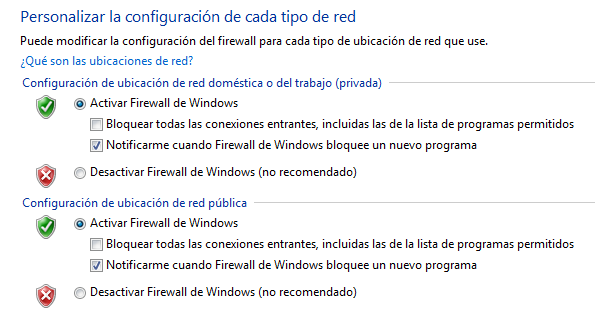
(10.5.15.2.5.126)->5=00000101 y 126=01111110->10101111110=1406

**5. Configuración del cortafuegos de Windows**

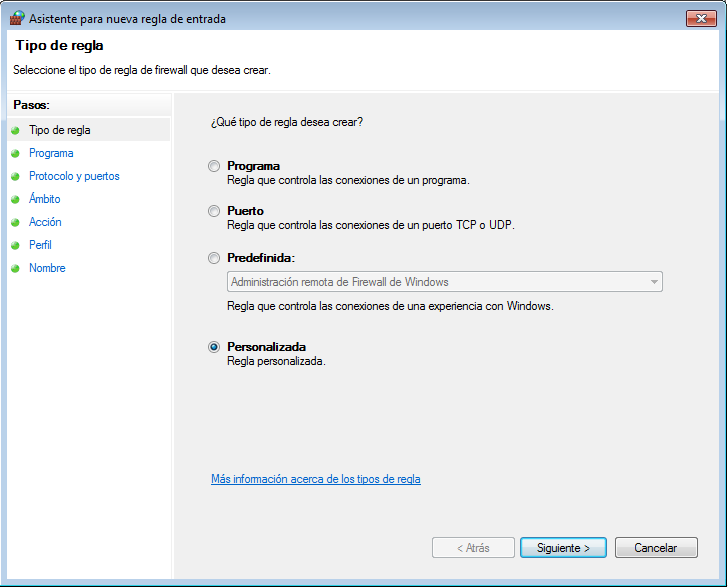
Desactivar el cortafuegos para que funcionen los servicios es una mala práctica que pone en riesgo la seguridad del sistema. Por eso en este apartado se configurará adecuadamente el cortafuegos de forma que pueda estar activado sin que el servicio FTP deje de estar operativo.

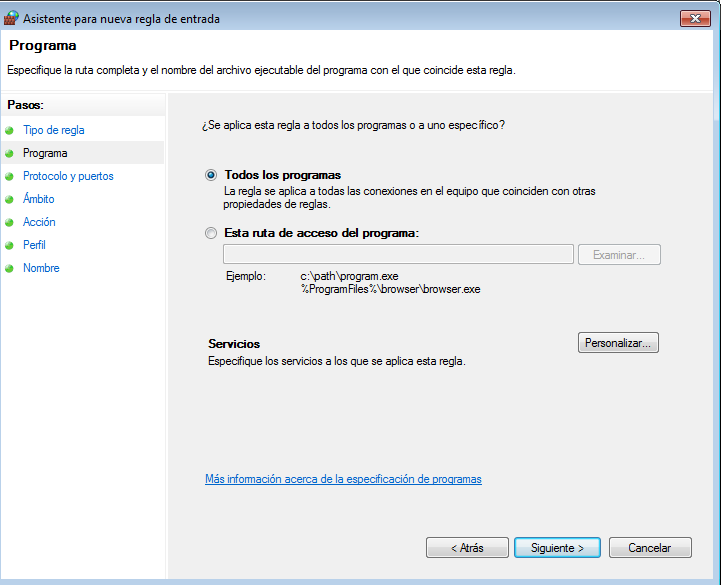
***Tener en cuenta que El cortafuegos de WIndows no permite el bloqueo del paso de direcciones,solo en Linux***

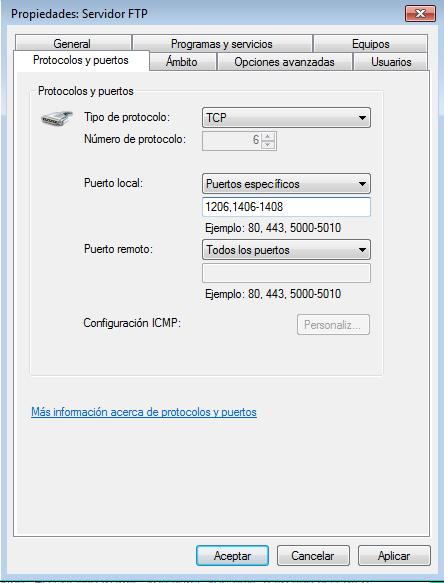
- Activa el cortafuegos de Windows en la M.V. y configúralo de forma que tu servidor FTP siga funcionando, aunque el cortafuegos esté activado.

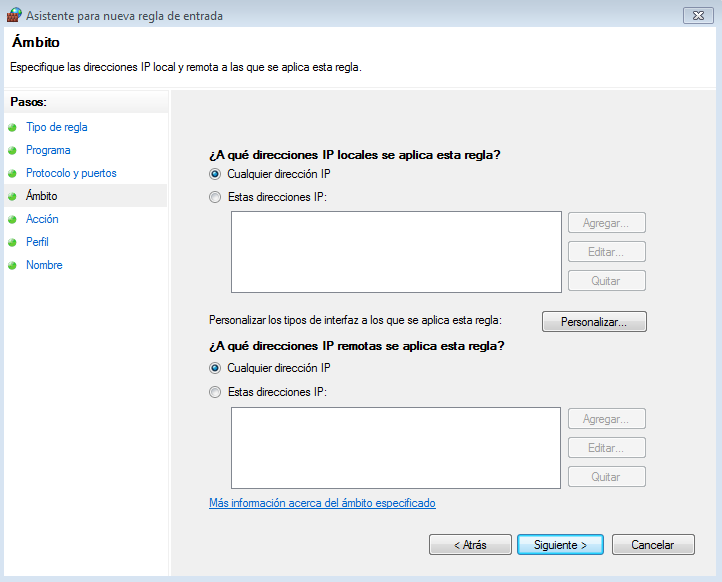


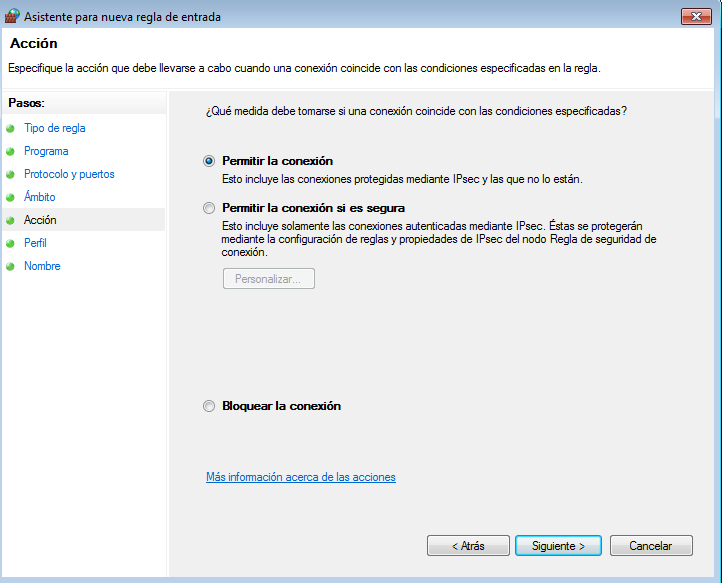


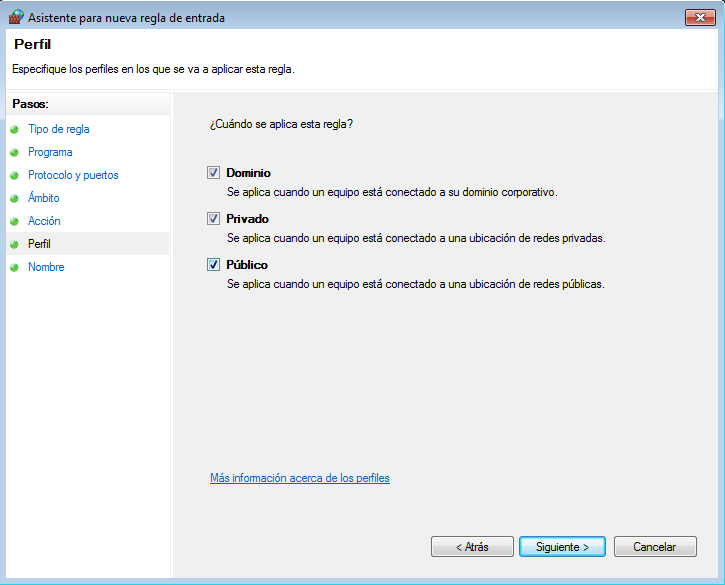


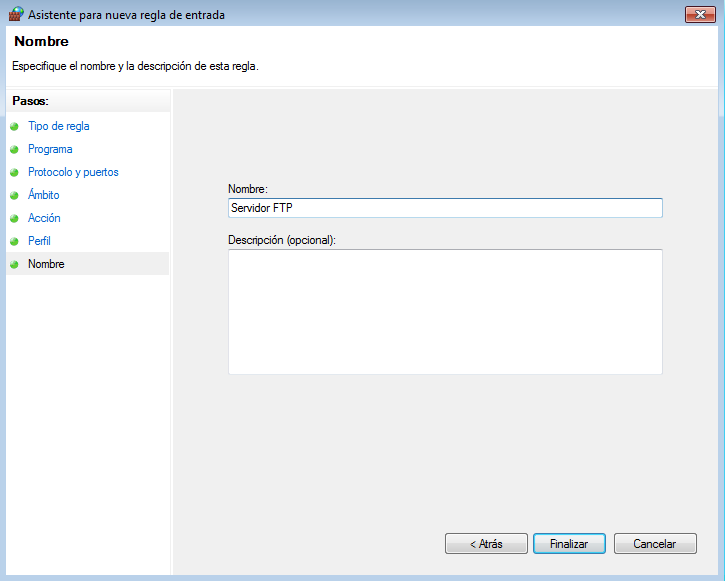




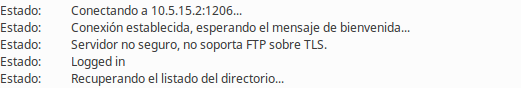








- Comprueba desde tu máquina física que todo sigue operativo (conectándote al servidor FTP, descargando un fichero, etc.).



***Si quieres permitir que entre solo un equipo, tienes que especificar la ip remota***

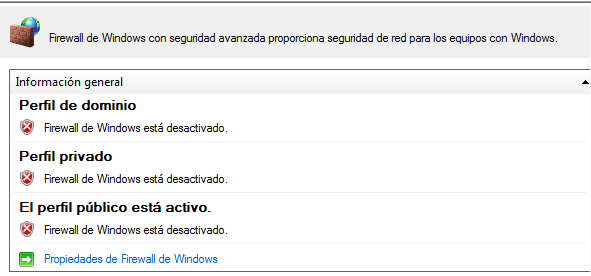
**6. Configuración de un cortafuegos comercial**

El cortafuegos incluido con las versiones de escritorio de Windows es un cortafuegos de entrada válido, pero muy limitado en cuanto a las opciones que ofrece. No se puede comparar con otros cortafuegos avanzados como Zone Alarm Pro o Comodo Firewall en Windows o las reglas de iptables en Linux (las iptables las veréis en otro módulo).

En este apartado se realizará una configuración básica a nivel 3 y 4 del cortafuegos comercial Comodo Firewall.

Este apartado se realizará **sobre la M.V. Windows 7**, en la que ya está instalado el Filezilla Server, configurado tal cual lo dejamos en el apartado 4 (Puerto de escucha el 1206, modo pasivo 1406-1408)

- Desactiva el cortafuegos de Windows en esa M.V. e instala la versión gratuita de *Comodo Firewall* (https://personalfirewall.comodo.com/).



- En la primera pantalla que aparece pulsar sobre el botón Opciones para indicar al programa de instalación que instale solo el firewall (no es necesario instalar ni el

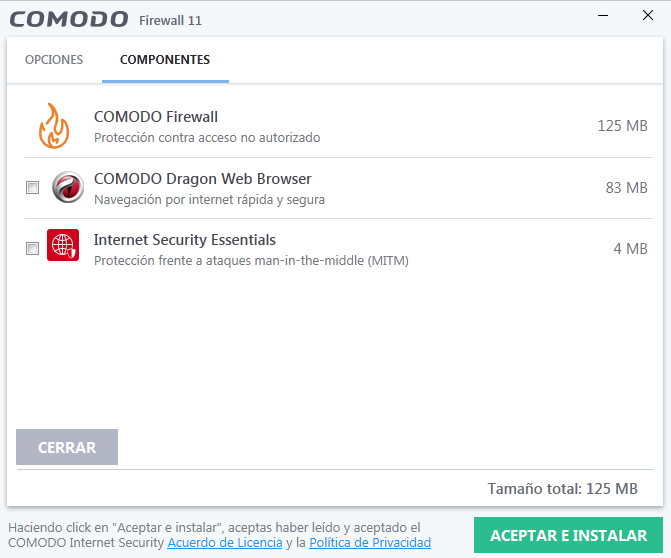
browser ni los componentes adicionales que aparecen)



- Al finalizar la instalación desactivar las opciones que aparecen:



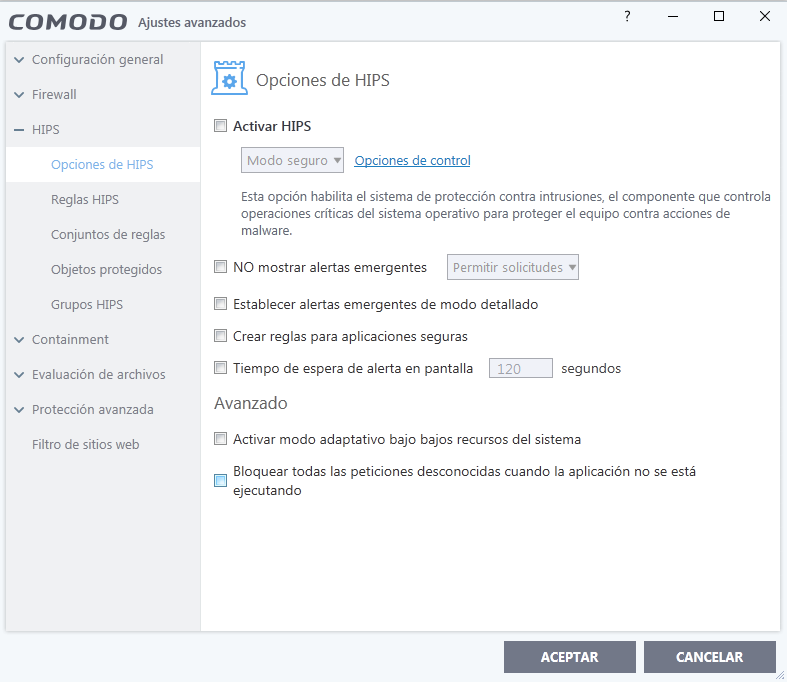
ç

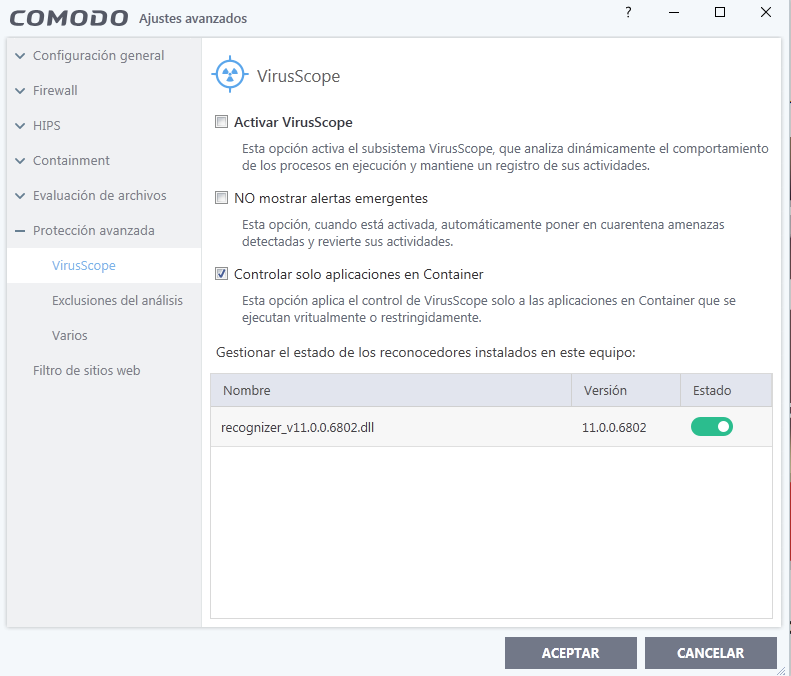


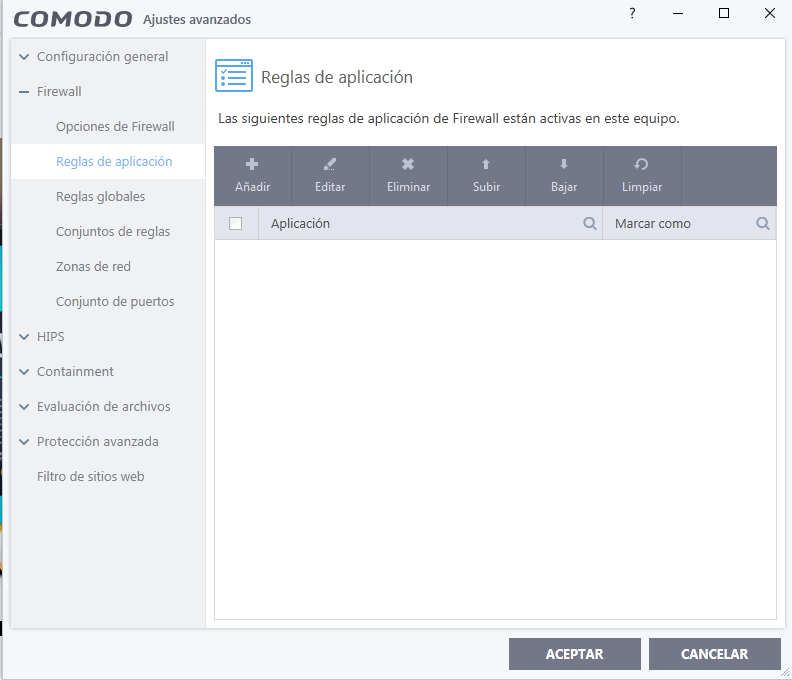


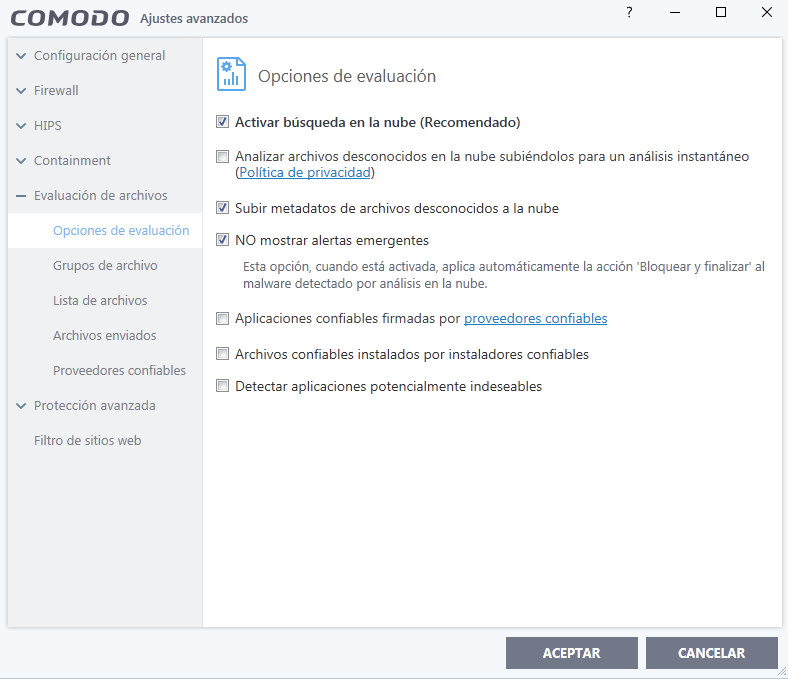
- Configura Comodo Firewall para que:

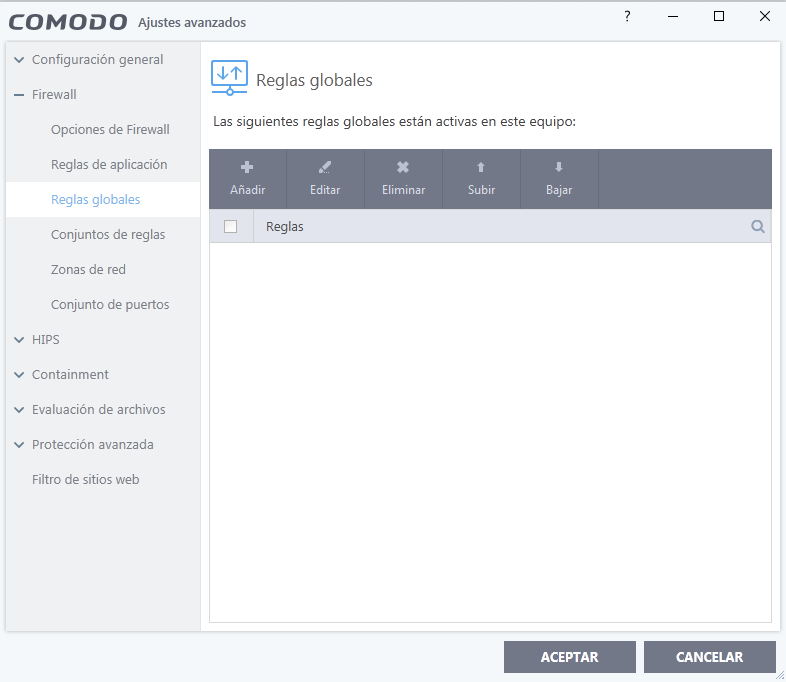
o Estén desactivadas todas las funcionalidades extra y sólo opere como cortafuegos







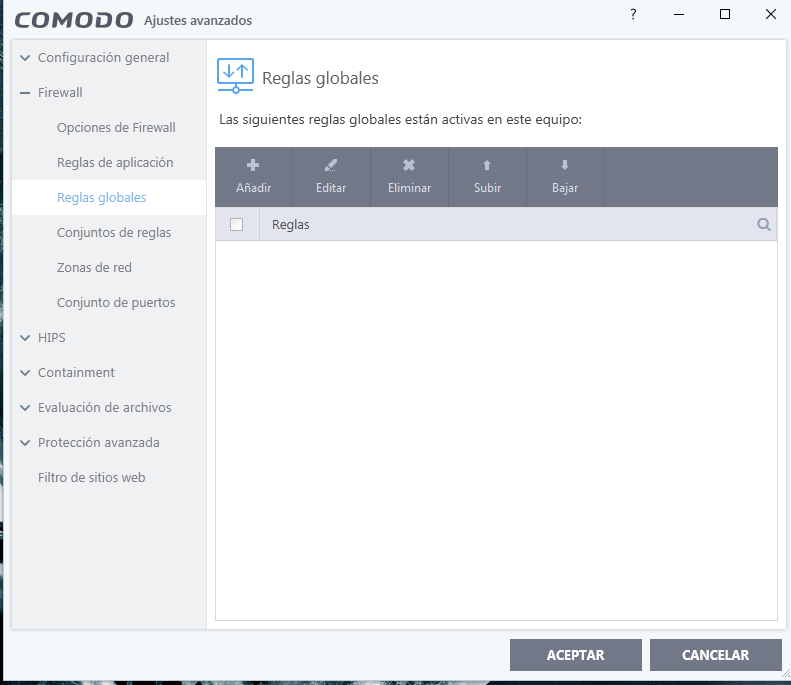


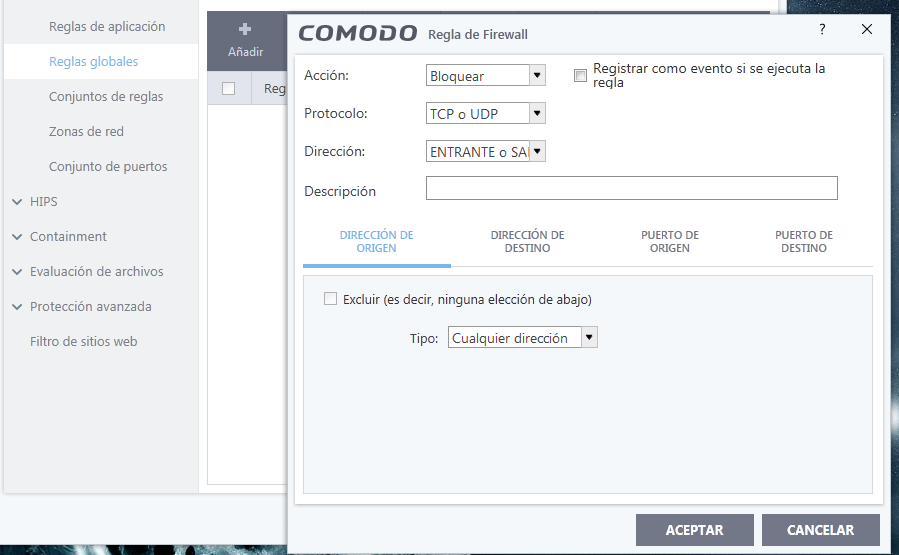


o La M.V. esté completamente protegida cerrando todos los puertos en entrada y salida.

***Primero debemos de saber que este firewall no trabaja como el de windows, es decir, el de windows trabaja respecto al equipo y cómodo respecto al paquete por eso no encontramos dirección local y remota, sí no qué dirección origen, destino y puerto origen, destino.***

***Tener en cuenta la jerarquía de cómodo, cuanto más alto más prioridad.***

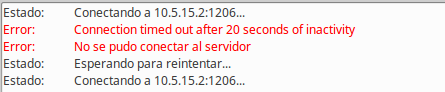




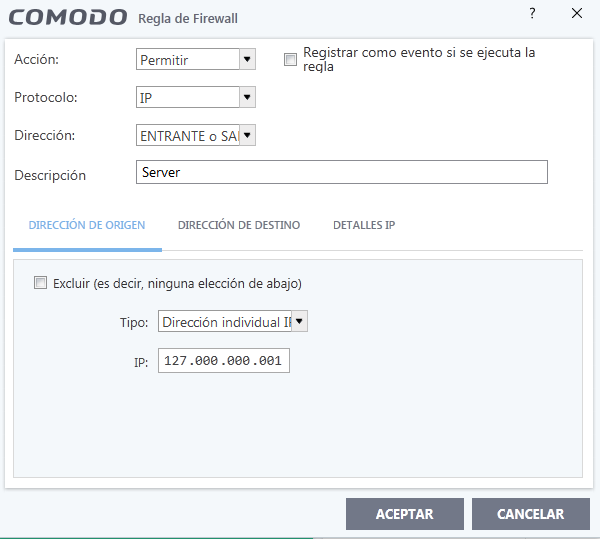
Hemos usado el protocolo TCP o UDP pero el protocolo IP es más restrictivo así que es mejor utilizar ese protocolo.

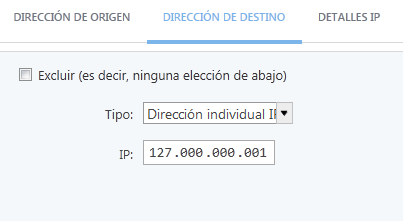
- Comprueba que tu M.V. no tiene acceso a Internet y no es accesible desde la red. El servidor FTP tampoco debería ser accesible (intenta conectarte desde la máquina real). - Configura Comodo Firewall para que el servidor FTP sea accesible y pueda transferir ficheros.



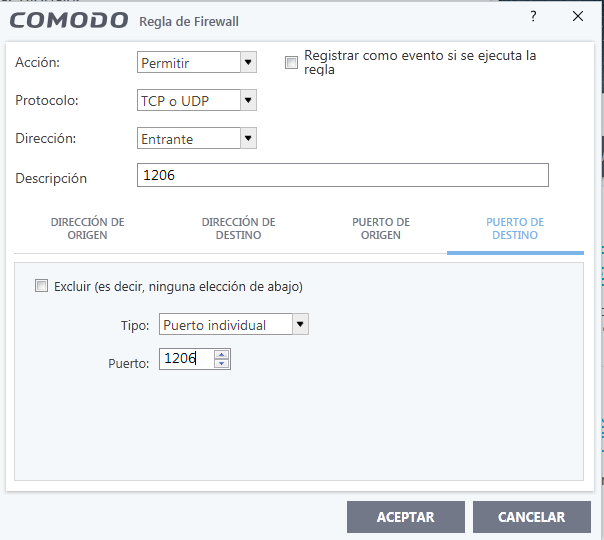


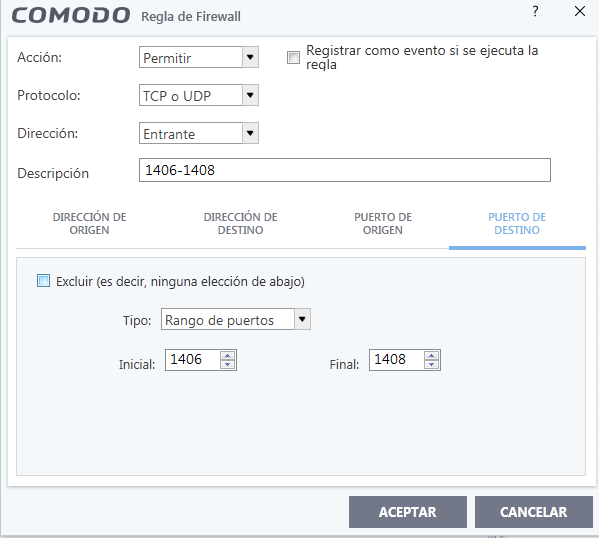
Ahora procedemos a configurar el Comodo para el servidor FTP:



￼￼

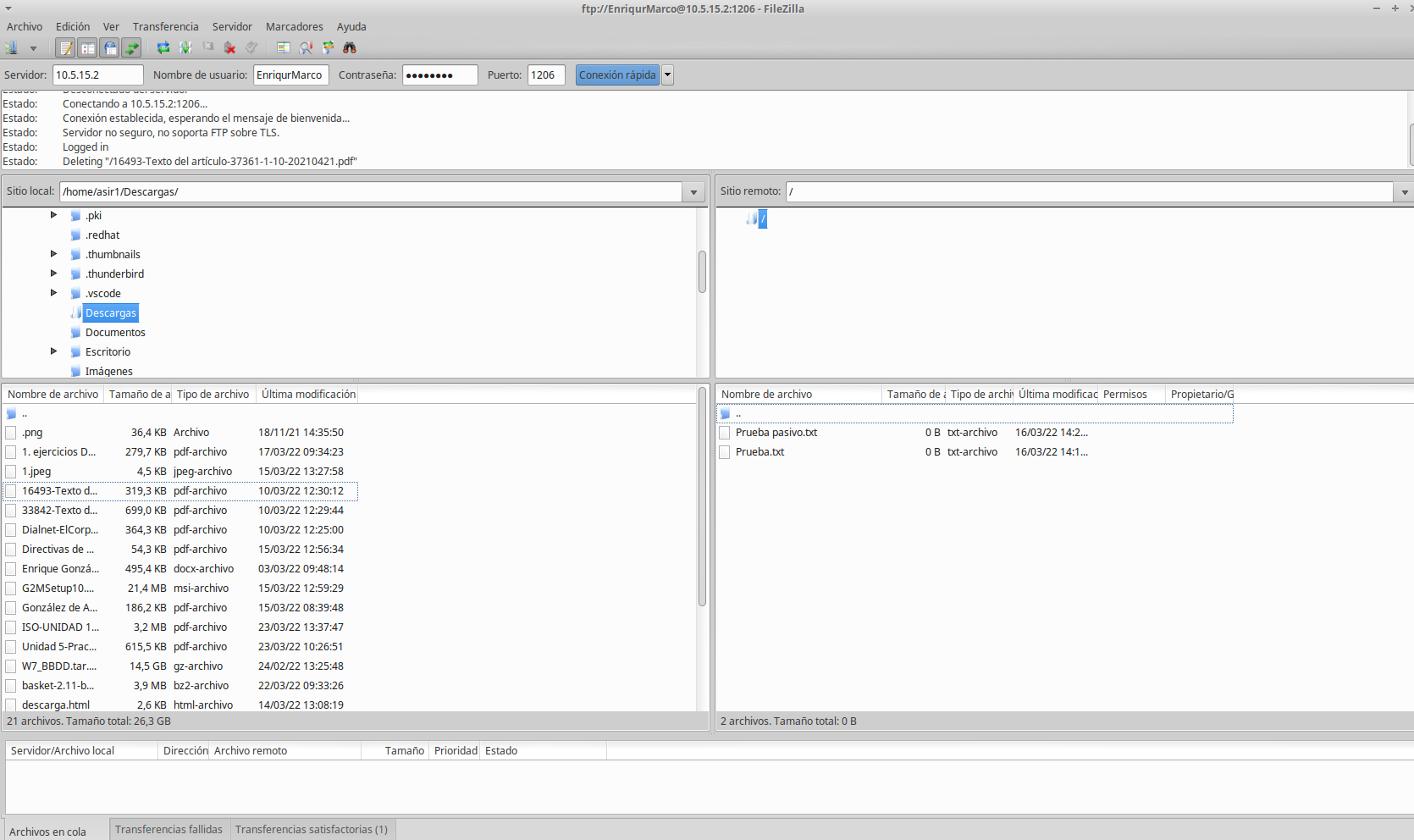
***También se puede hacer abriendo el puerto destino 14147***

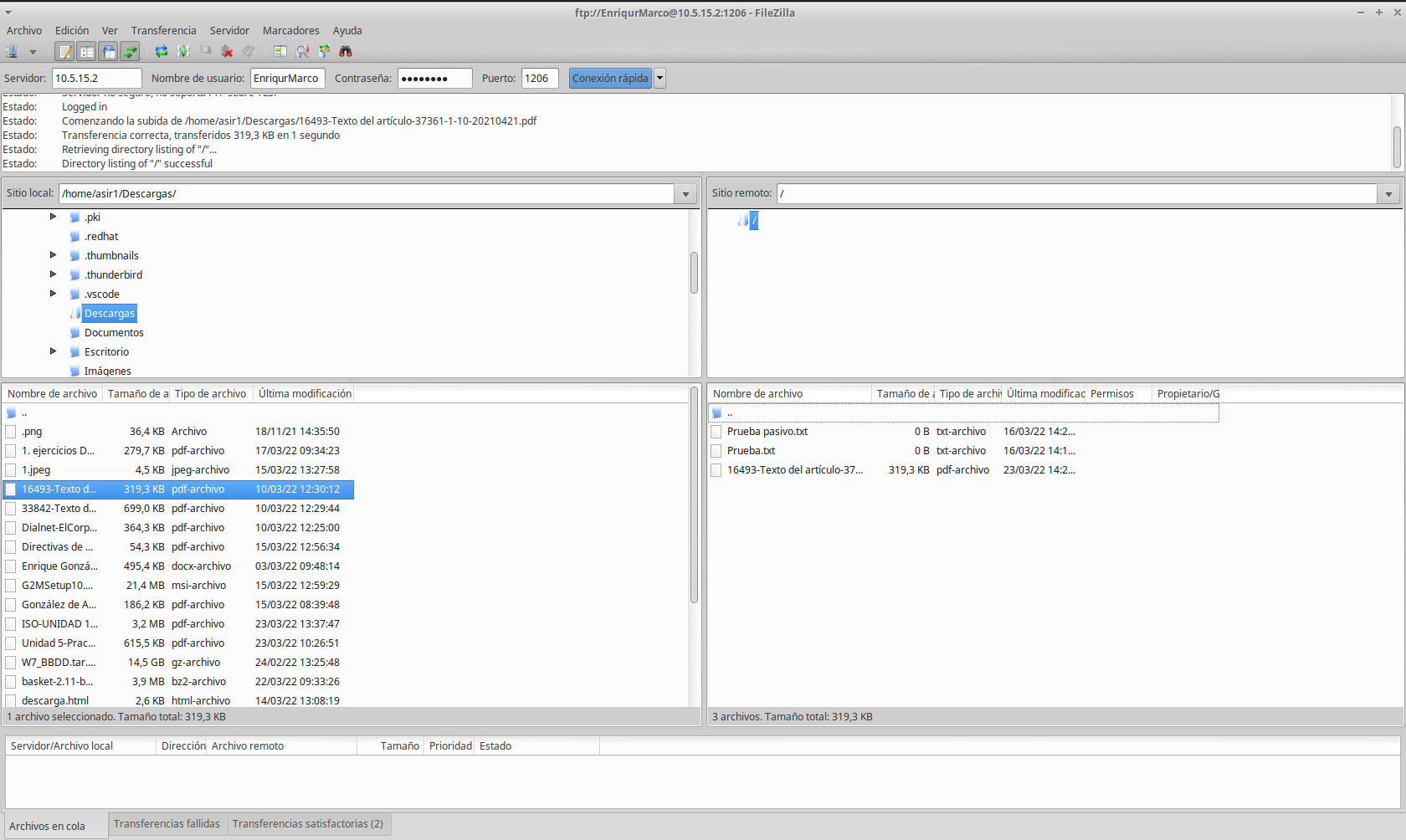




***Activamos la navegación pasiva y solo se puede acceder a partir de estos puertos***.

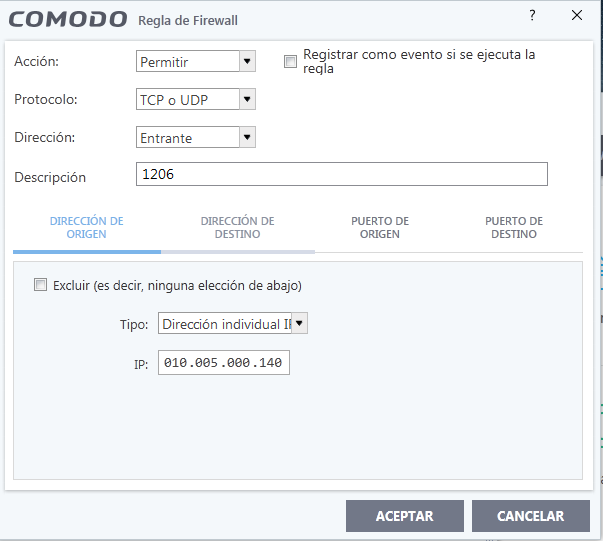
- Comprueba desde tu máquina física que el servidor FTP vuelve a estar operativo (conectándote al servidor FTP, descargando un fichero, etc…)





- ¿Serías capaz de modificar las reglas del cortafuegos para que tu servidor FTP sea accesible sólo desde tu máquina cliente (y no desde las de tus compañeros)? Hazlo y comprueba que las reglas funcionan adecuadamente con ayuda de un compañero.

***Modificamos las reglas de 1206 y 1406-1408 poniendo que la dirección origen es la del cliente.***



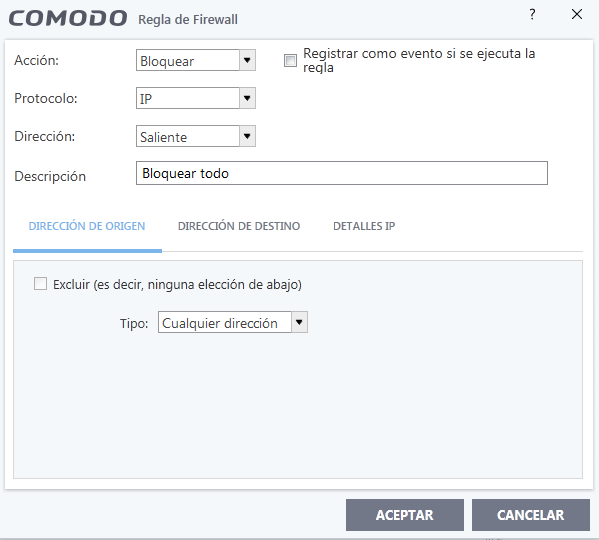


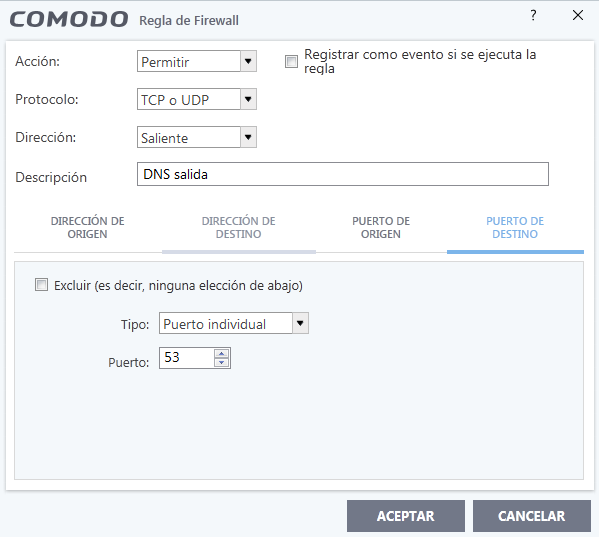
Debes aportar todas las capturas necesarias para la configuración de Comodo Firewall. El resultado, con las explicaciones y las capturas, debe ser un manual de configuración de este cortafuegos.

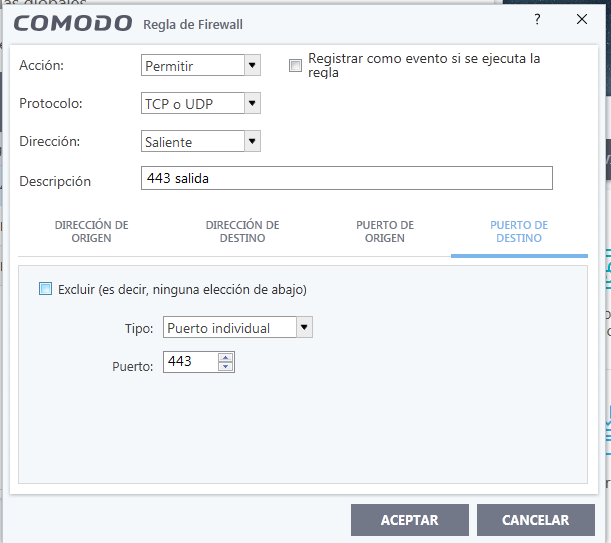
EXTRA: Practica configurando las siguientes reglas:

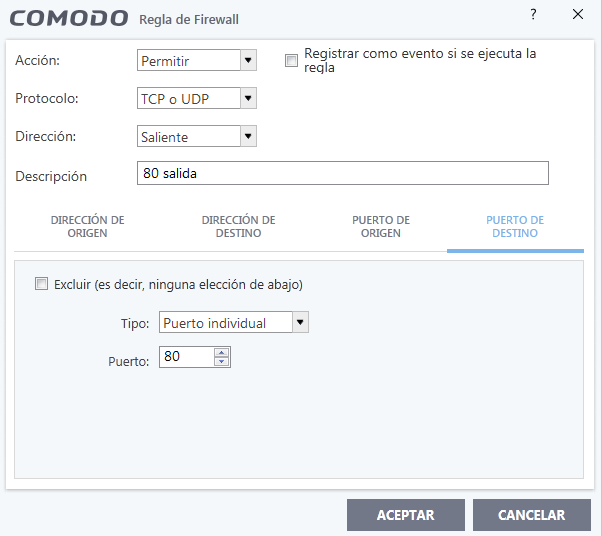
- Permitir la navegación web

**Quitamos el resto de reglas para evitar fallos.**



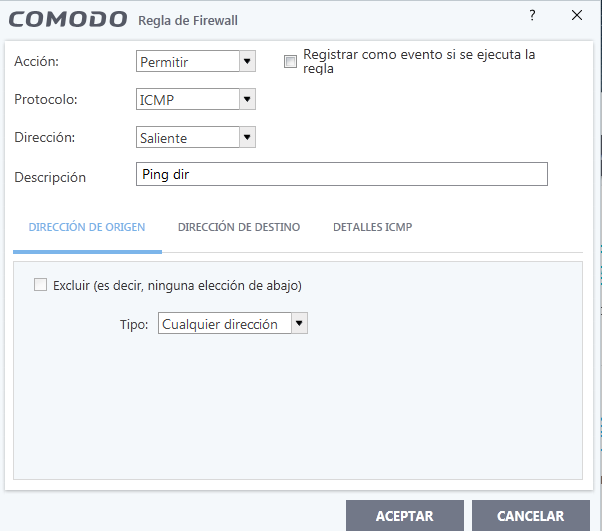
Dns

https

http

- Permitir la ejecución del comando ping a cualquier máquina

**Quitamos el resto de reglas para evitar fallos.**



***ICMP es el protocolo que utiliza ping, en este caso hemos hecho que podamos hacer ping pero no nos puedan hacer ping ya que no nos especifica.***

Profesora: Anabel Serradilla 9