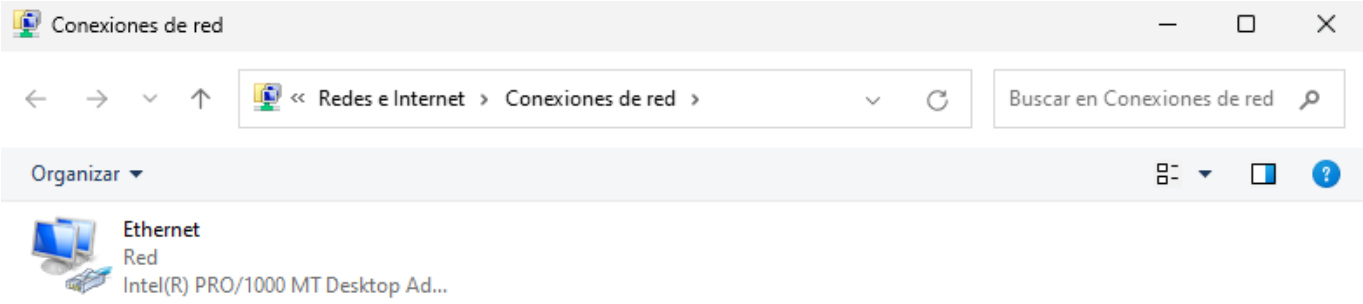
[FORT] Práctica 8: Fortificación de la Red de Windows 11

1. Verificar el listado de interfaces de red del sistema

a. Lista todas las interfaces de red que están disponibles en tu sistema

Podemos revisar esto dentro de “Panel de Control/Redes y recursos compartidos/cambiar configuración de adaptador”:



También podemos ver las interfaces con sus configuraciones de red usando el comando de CMD “ipconfig”:

```
Símbolo del sistema

Microsoft Windows [Versión 10.0.22631.5039]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\MCBS>ipconfig

Configuración IP de Windows


Adaptador de Ethernet Ethernet:

   Sufijo DNS específico para la conexión. . :
   Vínculo: dirección IPv6 local. . . : fe80::61b1:ee45:e3ca:9a56%7
   Dirección IPv4. . . . . . . . . . . . . . : 10.0.2.15
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : 10.0.2.2

C:\Users\MCBS>
```

b. Comprueba si tienes IPv6 Concebida

En la salida del comando “ipconfig” se puede observar si hay una dirección IP asociada:

```
Símbolo del sistema

Microsoft Windows [Versión 10.0.22631.5039]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\MCBS>ipconfig

Configuración IP de Windows


Adaptador de Ethernet Ethernet:

   Sufijo DNS específico para la conexión. . :
   Vínculo: dirección IPv6 local. . . : fe80::61b1:ee45:e3ca:9a56%7
   Dirección IPv4. . . . . . . . . . . . . . : 10.0.2.15
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : 10.0.2.2

C:\Users\MCBS>
```

Como se puede observar, esta máquina tiene una IPv6 Asociada

c. ¿Que tipo de dirección IPV6 es? ¿Como la obtienes?

Teniendo en cuenta que esta IPv6 comienza por fe80, es una dirección IP local. Esta IP se puede obtener a través de SLAAC (Stateless Address AutoConfiguration) si no hay servidor DHCPv6 o por

DHCPv6

d. Si haces ping al nombre de tu equipo, ¿responde antes la pila IPv6 o la pila IPv4?

Si hacemos ping al hostname responde antes la pila IPv6:

```
C:\Users\MCBS>hostname
MCBSW11

C:\Users\MCBS>ping MCBSW11

Haciendo ping a MCBSW11 [fe80::61b1:ee45:e3ca:9a56%7] con 32 bytes de datos:
Respuesta desde fe80::61b1:ee45:e3ca:9a56%7: tiempo<1m
Respuesta desde fe80::61b1:ee45:e3ca:9a56%7: tiempo<1m
Respuesta desde fe80::61b1:ee45:e3ca:9a56%7: tiempo<1m
Respuesta desde fe80::61b1:ee45:e3ca:9a56%7: tiempo<1m

Estadísticas de ping para fe80::61b1:ee45:e3ca:9a56%7:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

e. ¿Se puede modificar el orden de resolución de IPv6 o IPv4?

Se puede modificar el orden de resolución mediante el uso del comando netsh. Podemos revisar el estado actual de las políticas IPv6 con:

```
netsh interface ipv6 show prefixpolicies
```

```
netsh>interface ipv6 show prefixpolicies
Consultando el estado activo...

Precedencia Etiq.  Prefijo
----------- -----  ------------------------------
         50     0  ::1/128
         40     1  ::/0
         35     4  ::ffff:0:0/96
         30     2  2002::/16
          5     5  2001::/32
          3    13  fc00::/7
          1    11  fec0::/10
          1    12  3ffe::/16
          1     3  ::/96
```

El prefijo “::ffff:0:0/96” que se puede observar en la captura de pantalla, corresponde a las IPv4

mapeadas en IPv6, para darle prioridad de resolución a IPv4 tan solo tenemos que aumentar su nuvel de precedencia, en este caso a 60, haciéndolo el más alto, con el siguiente comando:

```
netsh interface ipv6 set prefixpolicy ::ffff:0:0/96 60 4
```

```
Administrador: Símbolo del sistema
Microsoft Windows [Versión 10.0.22631.5039]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Windows\System32>netsh interface ipv6 set prefixpolicy ::ffff:0:0/96 60 4
Aceptar


C:\Windows\System32>netsh interface ipv6 show prefixpolicies
Consultando el estado activo...

Precedencia Etiq.  Prefijo
----------- -----  ------------------------------
         60     4  ::ffff:0:0/96
         50     0  ::1/128
         40     1  ::/0
         30     2  2002::/16
          5     5  2001::/32
          3    13  fc00::/7
          1    11  fec0::/10
          1    12  3ffe::/16
          1     3  ::/96


C:\Windows\System32>_
```

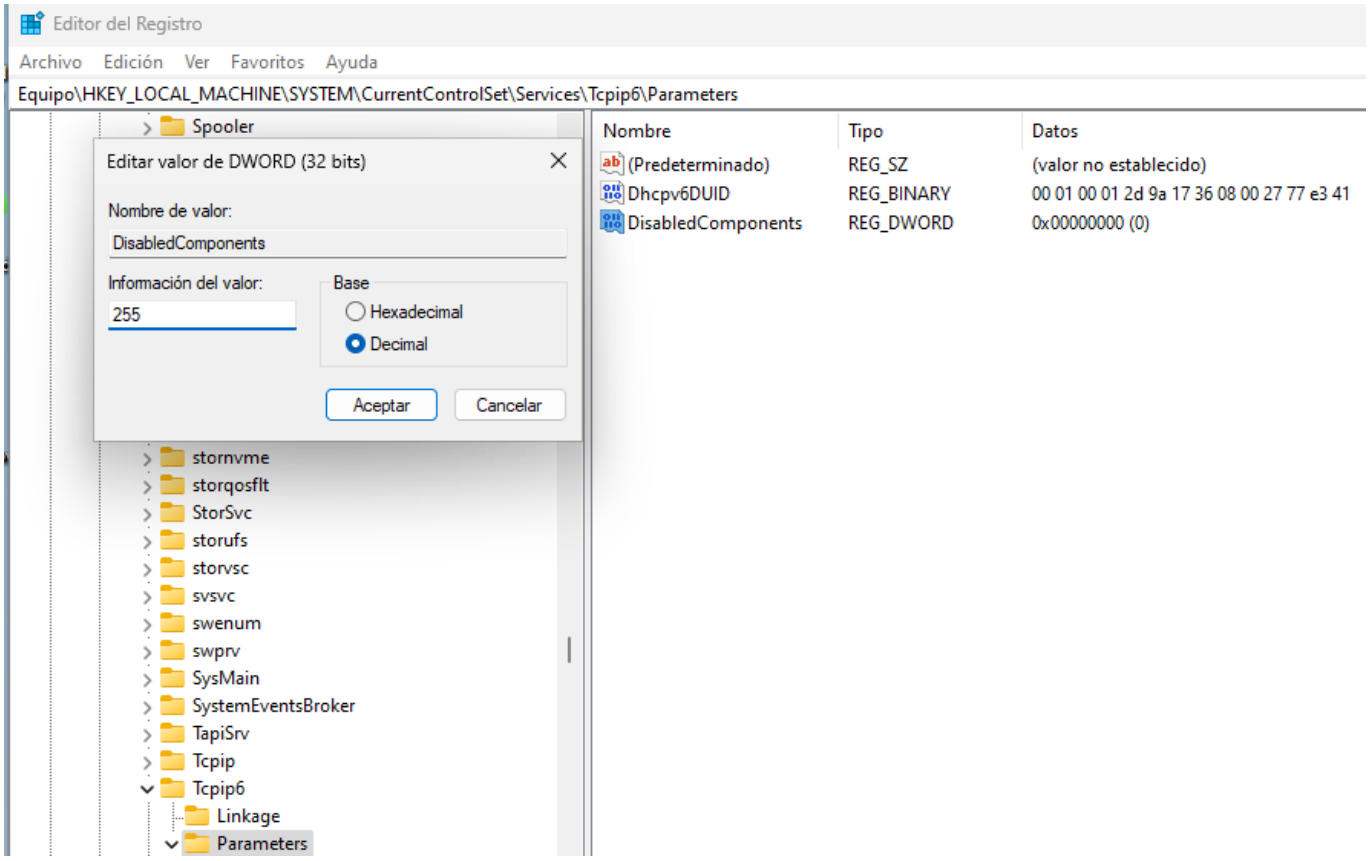
Una vez aplicada dicha configuración se puede observar como al hacer ping al nombre del host ahora responde primero IPv4:

```
C:\Users\MCBS>ping MCBSW11

Haciendo ping a MCBSW11 [10.0.2.15] con 32 bytes de datos:
Respuesta desde 10.0.2.15: bytes=32 tiempo<1m TTL=128
Respuesta desde 10.0.2.15: bytes=32 tiempo<1m TTL=128
Respuesta desde 10.0.2.15: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 10.0.2.15:
    Paquetes: enviados = 3, recibidos = 3, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

f. ¿Podemos eliminar la configuración de IPv6 de todas las interfaces?

Si, puede ser eliminada mediante el uso de claves de registro en

“HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/Tcpip6/Parameters/”, creando una nueva clave de registro de tipo REG_WORD llamada DisabledComponents con el valor 255:



Tras eso se reinicia el equipo y se puede comprobar con el comando “ipconfig” que ya no se está configurando IPv6:

```
C:\Users\MCBS>ipconfig

Configuración IP de Windows


Adaptador de Ethernet Ethernet:

   Sufijo DNS específico para la conexión. . :
   Dirección IPv4. . . . . . . . . . . . . . : 10.0.2.15
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : 10.0.2.2

C:\Users\MCBS>
```

g. ¿Es posible que al deshabilitar IPv6 se provoque una realentización del arranque de Windows? ¿Si es así como lo corregimos?

De acuerdo con microsoft esto puede ocurrir en sistemas windows antiguos situados entre Windows 7

y windows 8.1 y puede ser corregido mediante la descarga de ciertas actualizaciones.

2. Una vez eliminado IPv6 de todas las interfaces:

a. ¿Que tipo de perfiles tenemos en una interfaz de Microsoft Windows 11? ¿Qué diferencia tenemos entre ellos?

Generalmente hay 2 principales tipos:

- Privado: Pensado para redes que son de confianza como una casa o una pequeña oficina, bajo este perfil el dispositivo puede ser descubierto por otros equipos de la red. Algunas reglas del cortafuegos son más ligeras en este perfil.
- Público: Se usa en redes que no son de confianza, como redes públicas de bares y bibliotecas, el cortafuegos es mucho más restrictivo. Además también bloquea la compartición de recursos.

Si un equipo está unido a un Active Directory las configuraciones de red y seguridad son controladas por el administrador de dominio.

b. ¿Que perfil es recomendable para un equipo personal como el que estamos configurando?

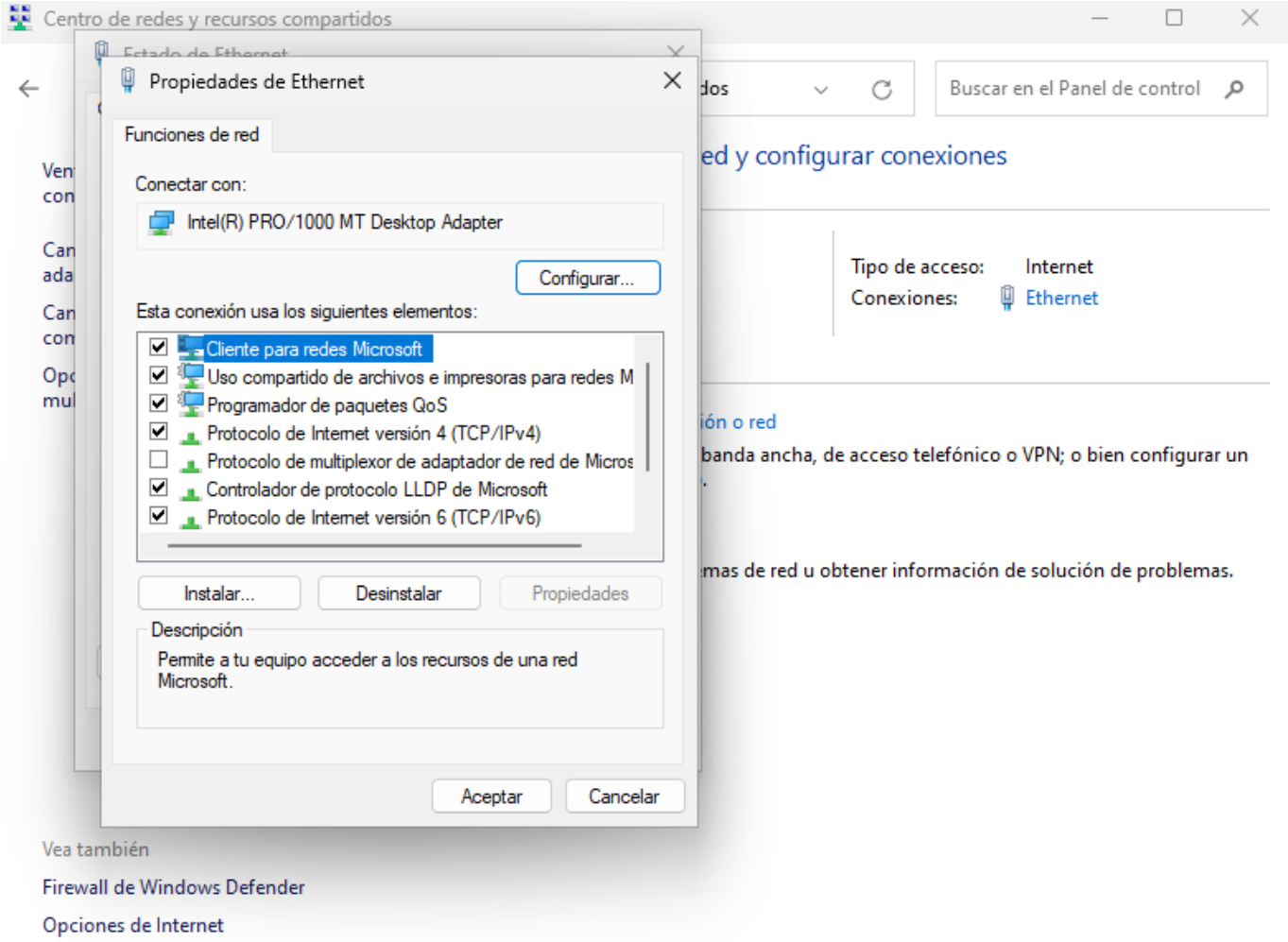
En este caso como el equipo se encuentra en una red que se podría considerar hasta cierto punto pública (Munics o Eduroam) lo recomendable sería establecer el perfil público por seguridad.

c. ¿La configuración del perfil afecta en algo a la seguridad?

Si ya que dependiendo del perfil que se configure el equipo puede estar oculto o no en la red, dificultando su localización por parte de un atacante , además el firewall se puede volver más restrictivo y se bloquea la compartición de archivos, reduciendo la cantidad de posibles agujeros de seguridad del sistema. Además con perfiles como el del dominio pueden haber directivas de seguridad más contundentes que incrementen considerablemente la seguridad.

d. ¿Que componentes tiene instalados cada interfaz?¿Es necesario tener instalados todos los componentes?¿Cuáles se pueden eliminar?

Para revisar esto, volvemos a la parte de configuración del adaptador del panel de control y revisamos las propuedades del adaptador:



En este caso se encuentran instalado los siguientes componentes:

- Cliente para Redes Microsoft
- uso compartido de archivos e impresoras para redes Microsoft
- Programador de Paqquetes QoS
- Protocolo de internet versión 4
- Controlador de protocolo LLDP de Microsoft
- Protocolo de Internet Versión 6
- Respondedor de detección de topologías de nivel de v…
- Controlador de E/S de asignador de deteción de topología…

No todos estos componentes serían necesarios, por ejemplo, como hemos desactivado IPv6 perfectamente se podría retirar el componete de “Protocolo de Internet Versión 6” Los protocolos que se podrían retirar si problemas serían:

- uso compartido de archivos e impresoras para redes Microsoft: Si no se van a compartir recursos no tiene sentido tenerlo habilitado
- Programador de Paqquetes QoS: Se usa para gestionar la prioridad del tráfico, no es esencial, porlo que puede ser deshabilitado.
- Protocolo de Internet Versión 6: IPv6 se encuentra deshabilitado en este equipo
- Controlador de protocolo LLDP de Microsoft: Se usa para descibrir dispositivos en redes empresariales, en este caso no estamos en una así que no es necesario.
- Respondedor de detección de topologías de nivel de v.: Solo es útil si queremos un mapa de red.

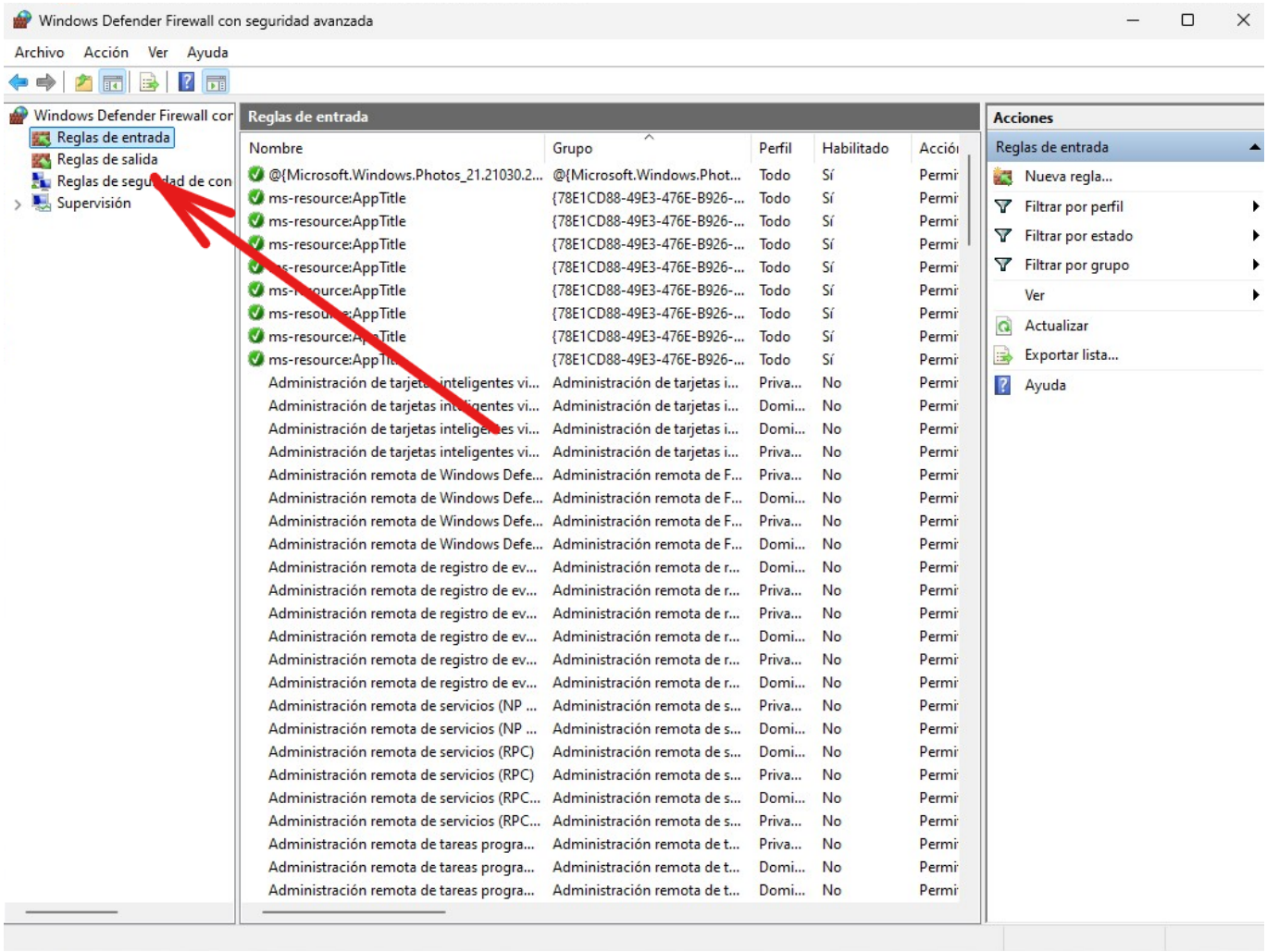
e. ¿Hasta que nivel de la capa OSI nos protege el FireWall de Windows?

El firewall de WIndows protege en las capas 3 y 4:

- Capa 3: Filtra basándose en origen, destino, puerto y protocolo
- Capa 4: Puede filtrar tráfico en función del estado de las sesiones.

f. ¿El Firewall de Windows permite gestionar el tráfico de entrada y salida? ¿Cuál es la configuración más restrictiva que se puede aplicar?

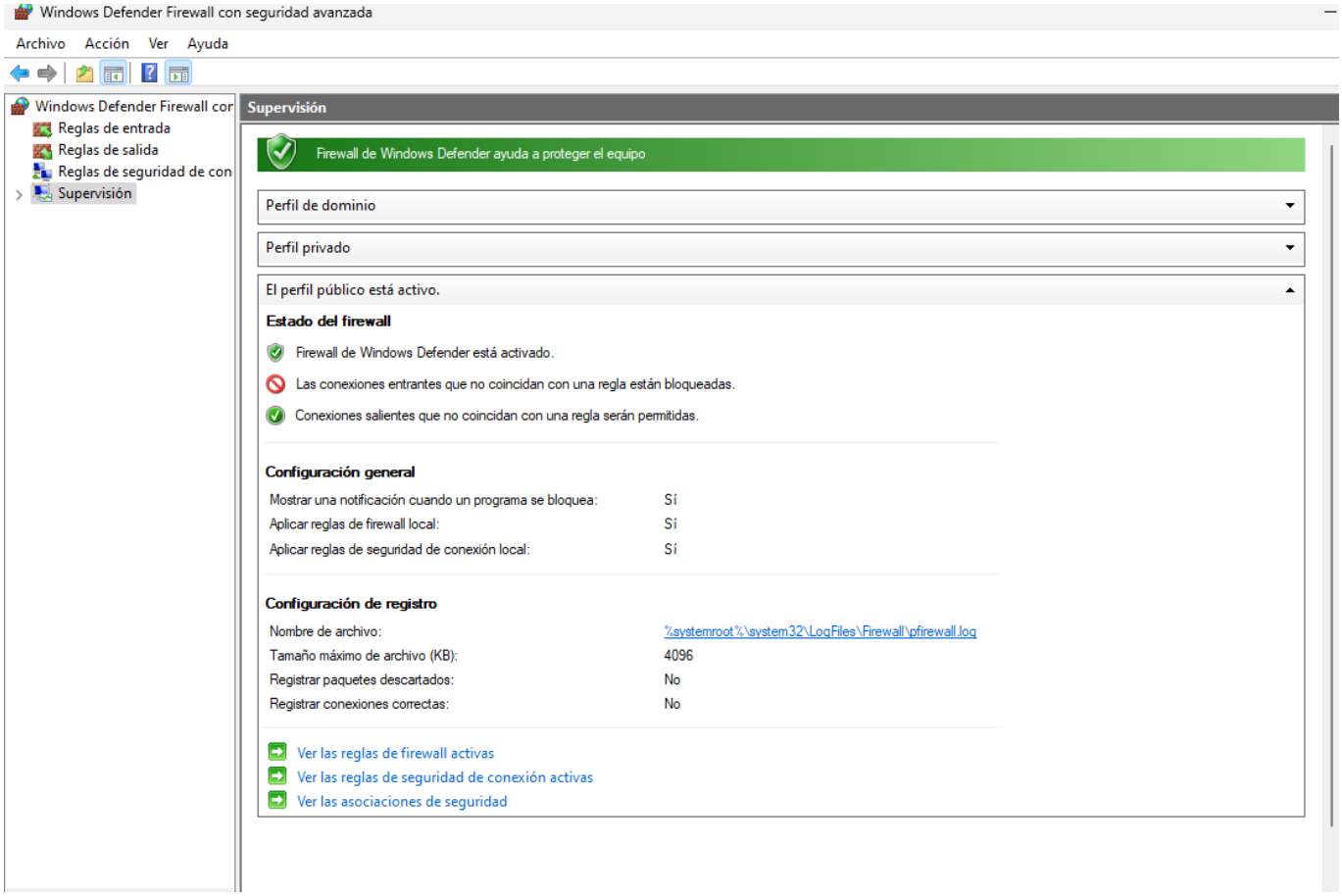
Si, el firewall puede gestionarl el tráfico de entrada y salida mediante el uso de reglas como se puede observar en la siguiente captura:



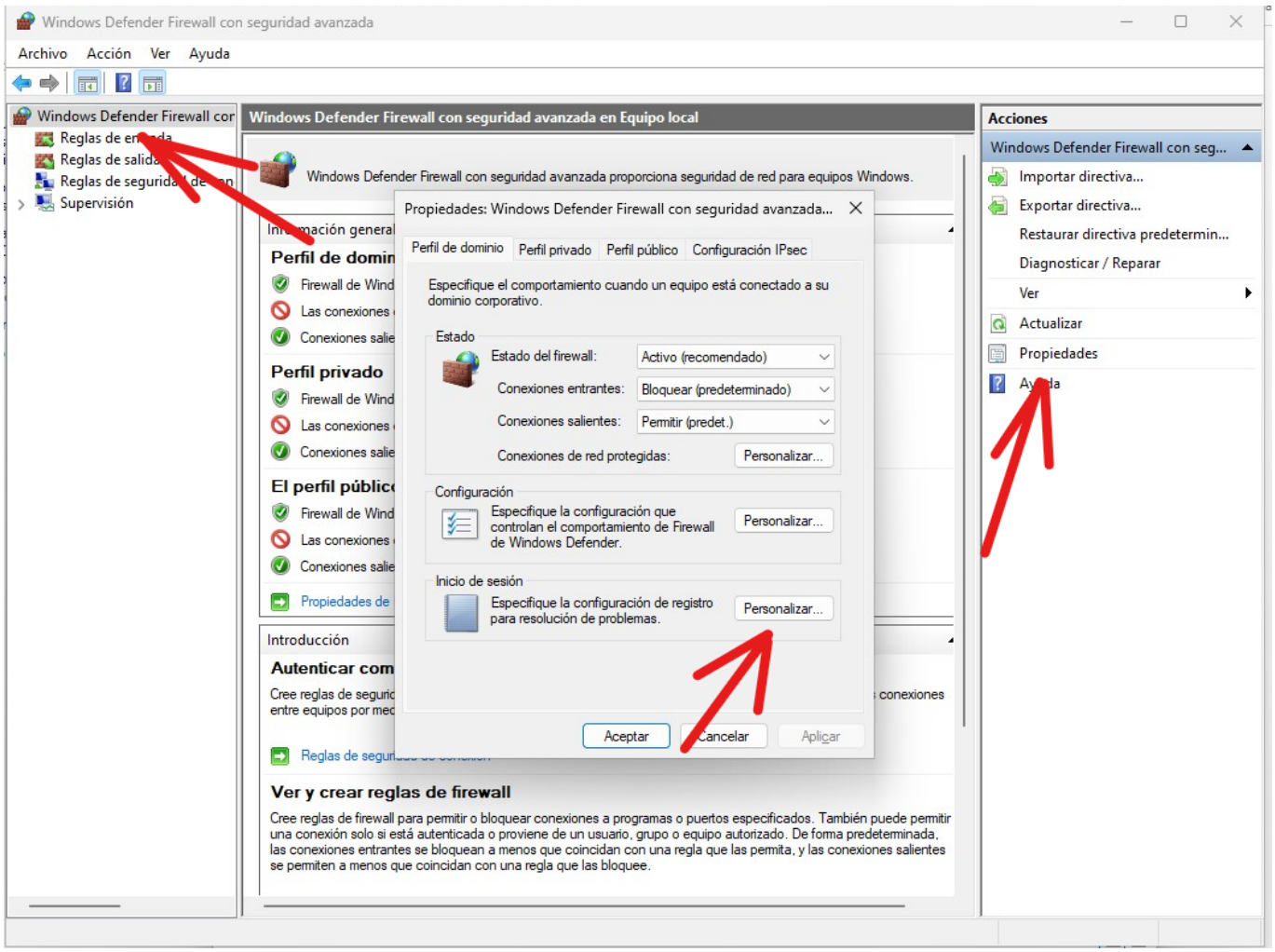
La configuración más restrictiva que se puede hacer es la poner el perfil público, que bloquea todo el tráfico de entrada y bloquear todo el tráfico de salida, eliminando las reglas predeterminadas de entrada y salida del firewall.

g. ¿Existe un sistema de Logs?¿En que carpetas se encuentras?¿Como se puede hacer debug de las reglas aplicadas?

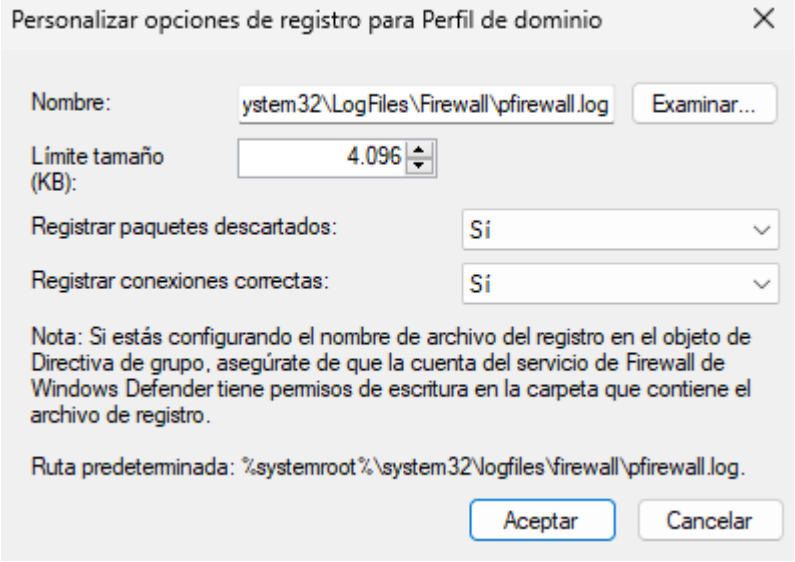
Los logs del firewall se almacenan en la ruta: “C:\Windows\System32\LogFiles\Firewall\pfirewall.log” como se peude observar dentr de opciones avanzadas del firewall:



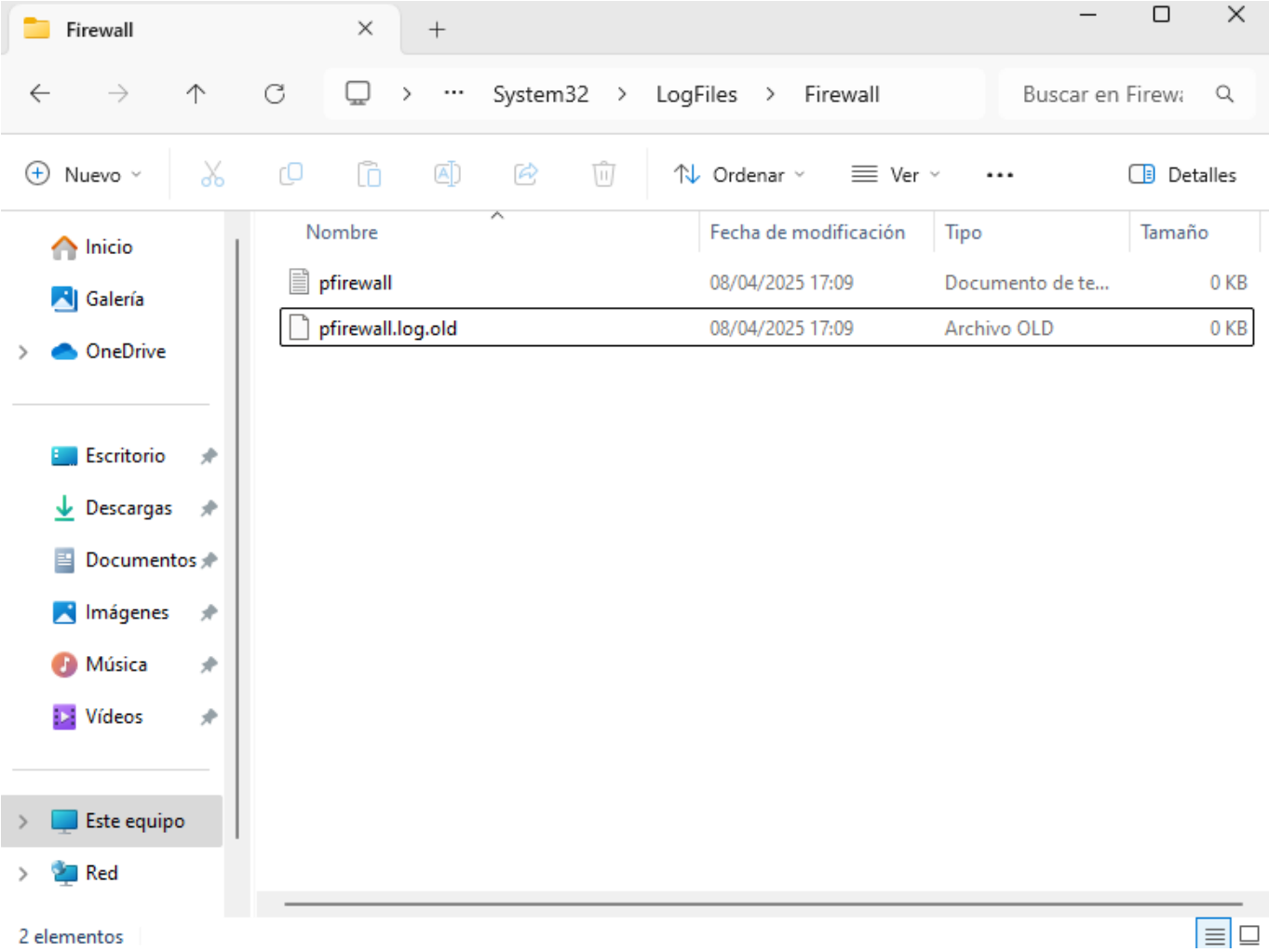
En este caso como se puede observar en la captura no se están registrando eventos de paquetes descartados o conexiones correctas en el log del firewall, por lo que se deben habilitar estas configuraciones. para ello seleccionamos Windows Defender Firewall en configuración avanzada del Firewall y le damos a propiedades, tras eso, en la sección de iniciar sesión se pulsa en personalizar:



Y dentro marcamos la opción de Registrar paquetes descartados como SI y hacemos lo mismo con registrar conexiones correctas:



Tras eso se puede observar que se han creado los archivos de log en la carpeta antes mencionada:



Se puede ver el contenido del log usando el siguiente comando como adminsitrador en PowerShell:

```
Get-Content C:\Windows\System32\LogFiles\Firewall\pfirewall.log
```

From:
https://www.knoppia.net/ - **Knoppia**

Permanent link:
https://www.knoppia.net/doku.php?id=master_cs:fortificacion:p8&rev=1744125231

Last update: **2025/04/08 15:13**