

<b>PRÁCTICA : E6 – Instalar un cortafuegos en Windows y Linux</b> <b>MF0486_3 : Seguridad en Equipos Informáticos</b>			Fecha	21 / 03 / 2022
			Página 1 de 5	
Curso	7.1. MF0486_3 Seguridad en equipos informáticos	Plan de Formación	FC- 2021.1/II.000/1914256	

Nombre y Apellidos:	JHONATAN RODRIGUEZ FERREIRA	Firma del Alumno:	
DNI:	78644010H	Firma del Profesor:	

Apto: ☐

No Apto: ☐

Calificación:

### Instrucciones Generales

La puntuación máxima será de 10 puntos.  
Esta prueba tendrá una duración máxima de 1260 minutos  
( Temporalizados durante la Unidad de Aprendizaje )

El alumno/a deberá acatar las siguientes normas durante la duración de la práctica :

- Rellene el encabezado con su nombre, apellidos y D.N.I.
- Firme en todas y cada una de las hojas entregadas, incluidas las que estén en blanco.
- Usar exclusivamente bolígrafo azul o negro
- Guardar los ficheros generados en una carpeta con nombre **MF0486\_E6**
- El docente le indicará al final como entregar el contenido de dicha carpeta
- Al finalizar el ejercicio y antes de entregarlo **comprueba tus respuestas**, en caso de duda consulta al docente.

### Equipo y material

- Bolígrafo azul.
- Folios.
- Ordenadores.
- Conexión a Internet. ( Para buscar información a modo de ayuda )
- Pendrive.
- Bibliografía empleada en el Módulo.
- Sistema operativo Windows ( virtualizado )
- Sistema operativo Linux ( virtualizado )

<b>PRÁCTICA : E6 – Instalar un cortafuegos en Windows y Linux</b> <b>MF0486_3 : Seguridad en Equipos Informáticos</b>			<b>Fecha</b>	21 / 03 / 2022
			Página 2 de 5	
<b>Curso</b>	7.1. MF0486_3 Seguridad en equipos informáticos	<b>Plan de Formación</b>	FC- 2021.1/II.000/1914256	

## Instrucciones específicas

El objetivo de esta práctica guiada será que el alumno elabore un Plan de seguridad de una empresa ficticia o real, en el cual se plasmen diversas políticas de seguridad vistas durante el módulo formativo.

### Condiciones de realización:

La actividad se llevará a cabo en el aula y el alumnado contará en todo momento supervisión del docente.

El alumnado contará con una duración de 1260 minutos para realizar la práctica.

Se podrá realizar en varias partes con una duración cada una de 60 minutos aproximadamente.

El alumno podrá hacer uso de internet para su realización, y se detallan a continuación algunas webs de ayuda.

### Páginas webs :

[https://es.wikipedia.org/wiki/Cortafuegos\\_\(inform%C3%A1tica\)](https://es.wikipedia.org/wiki/Cortafuegos_(inform%C3%A1tica))

En ella se valorará la utilización de herramientas para la gestión del tiempo y secuenciación del uso de las aplicaciones necesarias. Y se observará especialmente la autonomía del alumnado a la hora de ejecutar y tomar decisiones. Como también la estructuración del ejercicio en donde se solicitará, orden, coherencia y limpieza.

Una vez terminado la práctica se le notificará al docente y pasará a su evaluación.

<b>PRÁCTICA : E6 – Instalar un cortafuegos en Windows y Linux</b> <b>MF0486_3 : Seguridad en Equipos Informáticos</b>			Fecha	21 / 03 / 2022
			Página 3 de 5	
Curso	7.1. MF0486_3 Seguridad en equipos informáticos	Plan de Formación	FC- 2021.1/II.000/1914256	

## Descripción de la práctica

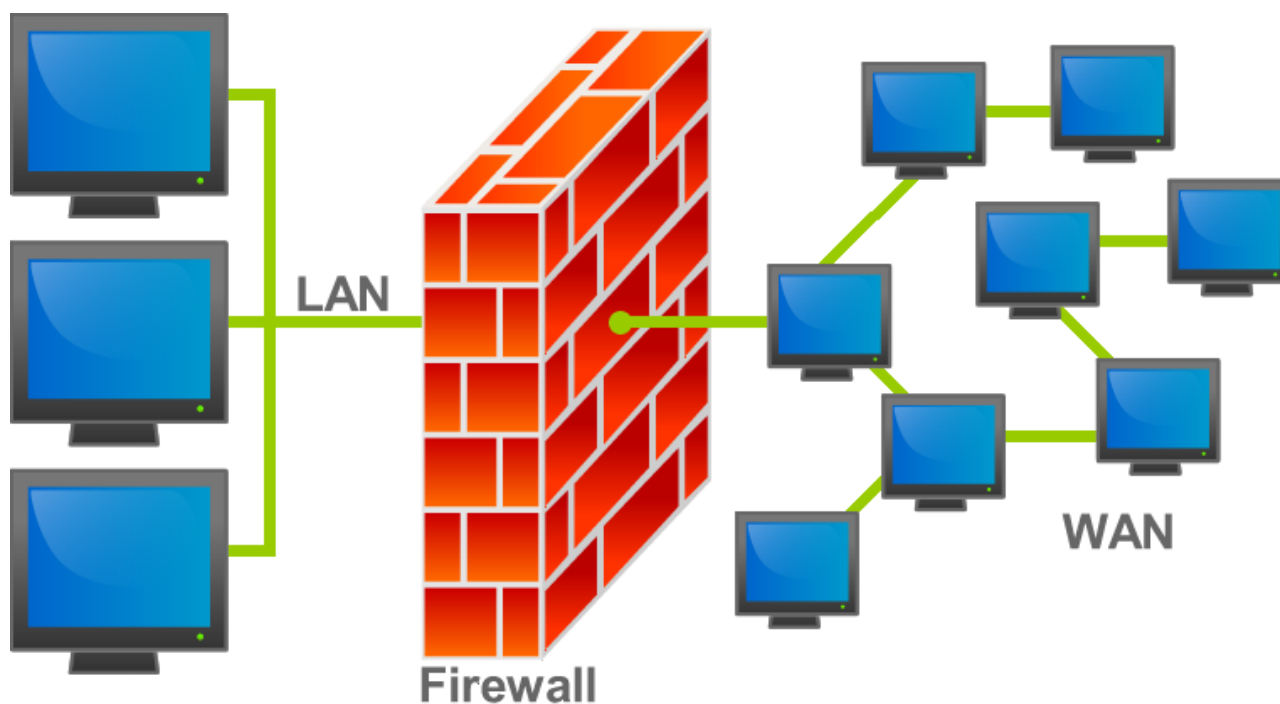
### El concepto de Cortafuegos

Un **cortafuegos (firewall)** es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

Los cortafuegos pueden ser implementados en hardware o software, o en una combinación de ambos. Los cortafuegos se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets. Todos los mensajes que entren o salgan de la intranet pasan a través del cortafuegos, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados. También es frecuente conectar el cortafuegos a una tercera red, llamada zona desmilitarizada o DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior.

Un cortafuegos correctamente configurado añade una protección necesaria a la red, pero que en ningún caso debe considerarse suficiente. La seguridad informática abarca más ámbitos y más niveles de trabajo y protección.



<b>PRÁCTICA : E6 – Instalar un cortafuegos en Windows y Linux</b> <b>MF0486_3 : Seguridad en Equipos Informáticos</b>			Fecha	21 / 03 / 2022
			Página 4 de 5	
Curso	7.1. MF0486_3 Seguridad en equipos informáticos	Plan de Formación	FC- 2021.1/II.000/1914256	

## PRÁCTICA

### 1ª Parte : Instalación y configuración de un cortafuegos en Windows

En esta primera parte de la práctica el alumno elegirá la configuración o programa de los que se citan a continuación u otra configuración que proponga el alumno y que crea conveniente para instalar y configurar un firewall en entornos basados en Windows.

Una vez el alumno haya finalizado tendrá que documentar y presentar todo en un informe, detallando los principales pasos que ha realizado.

#### Configurar un cortafuegos Windows con Zonealarm

<http://www.zonealarm.com/es/software/free-firewall/>

#### Otras alternativas

<http://www.xatakawindows.com/bienvenidoawindows8/este-es-el-firewall-de-windows-y-sus-mejores-alternativas>

<http://www.emezeta.com/articulos/10-firewalls-gratuitos-alternativos>

### 2ª Parte : Instalación y configuración de un cortafuegos en Linux

En esta segunda parte de la práctica el alumno elegirá la configuración o programa de los que se citan a continuación u otra configuración que proponga el alumno y que crea conveniente para instalar y configurar un firewall en entornos basados en Linux.

Una vez el alumno haya finalizado tendrá que documentar y presentar todo en un informe, detallando los principales pasos que ha realizado.

#### Configurar un cortafuegos en Ubuntu con Gufw

<https://es.wikipedia.org/wiki/Gufw>

<b>PRÁCTICA : E6 – Instalar un cortafuegos en Windows y Linux</b> <b>MF0486_3 : Seguridad en Equipos Informáticos</b>			Fecha	21 / 03 / 2022
			Página 5 de 5	
Curso	7.1. MF0486_3 Seguridad en equipos informáticos	Plan de Formación	FC- 2021.1/II.000/1914256	

El alumno además podrá elegir alguno de los siguientes programas para configurar el cortafuegos :

**CSF:** uno de los más conocidos sin lugar a dudas. CSF (ConfigServer Security & Firewall) es un software desarrollado por Configserver.com y se encuentra en constante actualización. No solamente es fácil de instalar, sino también de configurar y utilizar. CSF es compatible con muchos distros populares como CentOS, Ubuntu, Fedora, Debian y más.

**APF:** Advanced Policy Firewall es uno de los proyectos de R-fx Networks. APF es un cortafuegos que está basado en el conocido sistema iptables (que a su vez está construido sobre Netfilter). APF está diseñado con el fin de poder satisfacer las demandas más esenciales que hoy en día encontramos en la industria de Internet. Este software cuenta con un archivo de configuración bien detallado, de manera tal que configurar nuestro firewall se vuelve una tarea sencilla en la gran mayoría de sus aspectos.

**Shorewall:** su verdadero nombre es Shoreline Firewall. Es otra conocida herramienta y se encarga de simplificar en gran medida el uso de iptables, que para algunos usuarios puede resultar complejo. Podemos configurarlo fácilmente a partir de varias indicaciones según nuestros distintos requerimientos. La herramienta recibe actualizaciones periódicas y posee una detallada documentación.

**KISS Firewall:** también conocido como KISS My Firewall. Se trata de un firewall totalmente gratuito basado en iptables y creado por Steve Eschweiler. KISS Firewall está diseñado para ser usado en un típico servidor web e incluso tiene métodos preventivos para evitar ataques DDOS, escaneo de puertos e incluso IP spoofing/suplantación de IP.

**eBox Platform:** Algo más que un simple software cortafuegos.

**Monowall:** La más liviana de las propuestas de la entrada.

**PfSense:** Si desea un servidor de seguridad integral y nada más, no busques más.

**Smoothwall Advanced:** Y su versión de pago, con asistencia técnica y más opciones.

El alumno también podrá elegir algunas de las siguientes distribuciones Linux :

**ClearOS:** La distro que combina facilidad de uso con funcionalidad.

**IPCop:** Distribución versátil y rápida. Altamente configurable.

**Smoothwall Express:** Probablemente la distribución firewall con la mayor reputación.

<b>PRÁCTICA : E6 – Instalar un cortafuegos en Windows y Linux</b> <b>MF0486_3 : Seguridad en Equipos Informáticos</b>			Fecha	21 / 03 / 2022
			Página 6 de 5	
Curso	7.1. MF0486_3 Seguridad en equipos informáticos	Plan de Formación	FC- 2021.1/II.000/1914256	

## Firewall TinyWall

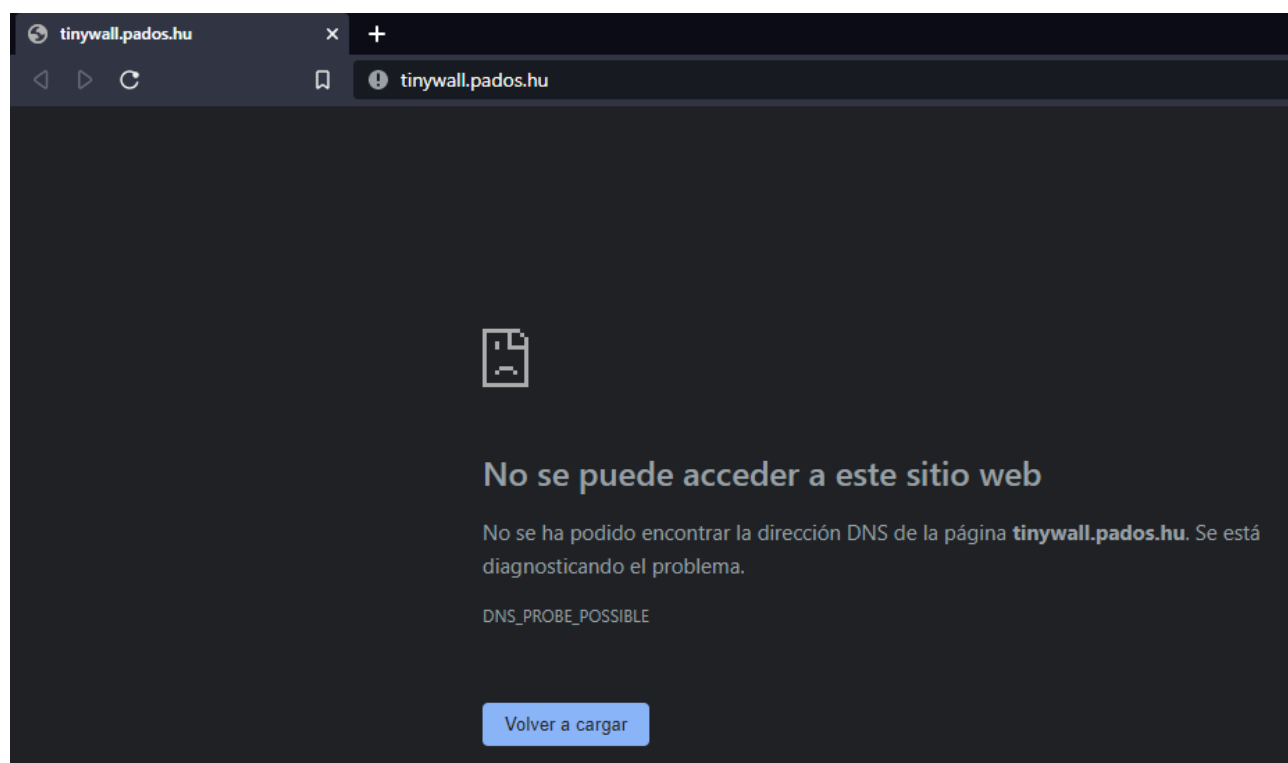
Para esta práctica utilizaremos Tinywall, es un cliente ligero pero muy potente a la hora de protegernos de conexiones externas o internas en nuestra misma red.

Descargamos el Firewall de Sophos. versátil y rápida. Altamente configurable.

Para esta práctica utilizaremos Tinywall, es un cliente ligero pero muy potente a la hora de protegernos de conexiones externas o internas de nuestra misma red, incluso tiene un apartado de virus para poder detectar malware en dado caso de que estemos en peligro

Paso 1. Lo descargamos desde la página <https://tinywall.pados.hu/> y lo instalamos posteriormente.

Al terminar la instalación hay que tener en cuenta que el tiny firewall ya empieza bloqueándote todos los accesos y puertos del pc. Lo comprobamos abriendo el navegador de internet y no nos abre la página.

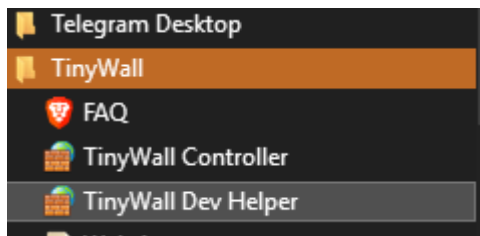



También en la señal wifi de nuestro PC.

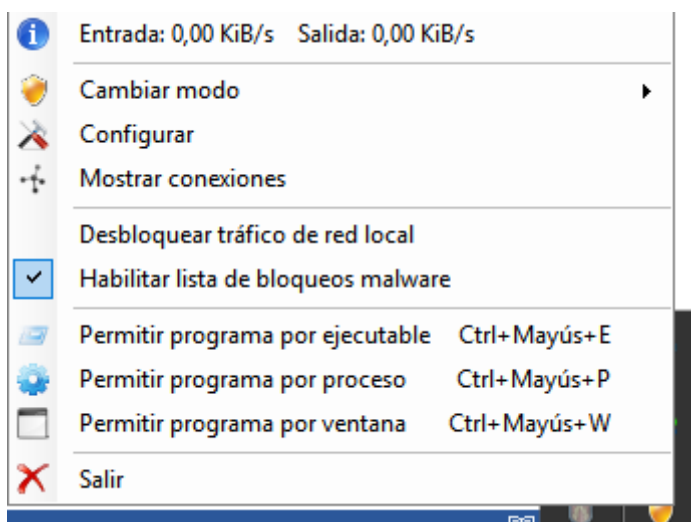


Paso 2. Localizamos el programa en el menú de Windows.

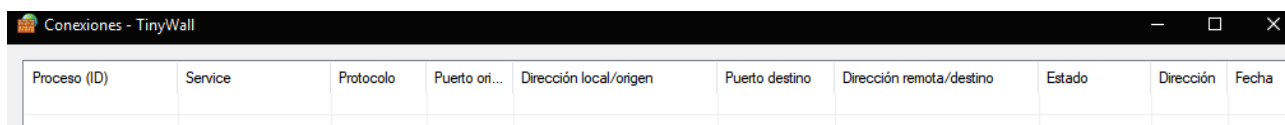
<b>PRÁCTICA : E6 – Instalar un cortafuegos en Windows y Linux</b> <b>MF0486_3 : Seguridad en Equipos Informáticos</b>			Fecha	21 / 03 / 2022
			Página 7 de 5	
Curso	7.1. MF0486_3 Seguridad en equipos informáticos	Plan de Formación	FC- 2021.1/II.000/1914256	




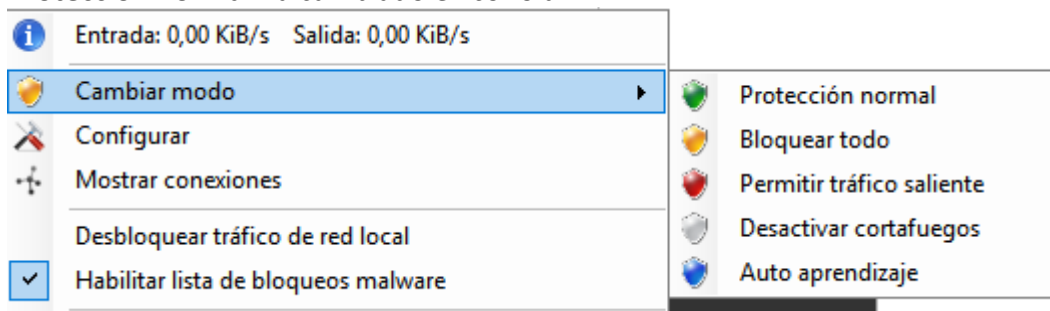
Pinchamos y no nos aparece nada, debemos ir a la barra de herramientas y en la parte de abajo pinchar en este icono para que nos aparezca las opciones. 



Vemos que entrada y salida esta en 0 kbps, pinchamos en **mostrar conexiones**



No existe nada abierto. Cambiamos la configuración a **cambiar modo** y elegimos **Protección normal** ha cambiado el icono a 

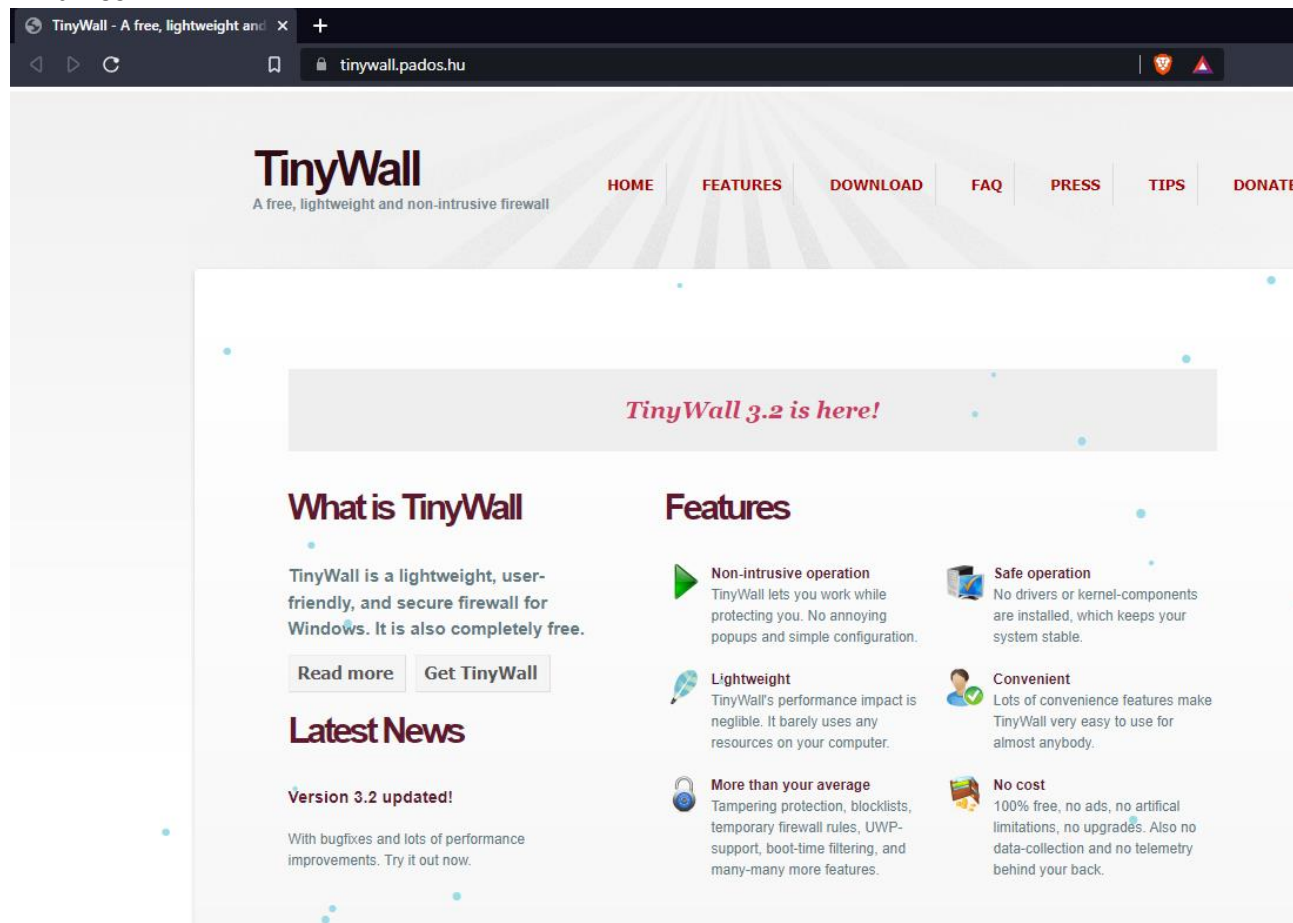


Abrimos el internet y ahora si podemos navegar



<b>PRÁCTICA : E6 – Instalar un cortafuegos en Windows y Linux</b> <b>MF0486_3 : Seguridad en Equipos Informáticos</b>			Fecha	21 / 03 / 2022
			Página 8 de 5	
Curso	7.1. MF0486_3 Seguridad en equipos informáticos	Plan de Formación	FC- 2021.1/II.000/1914256	

Miramos



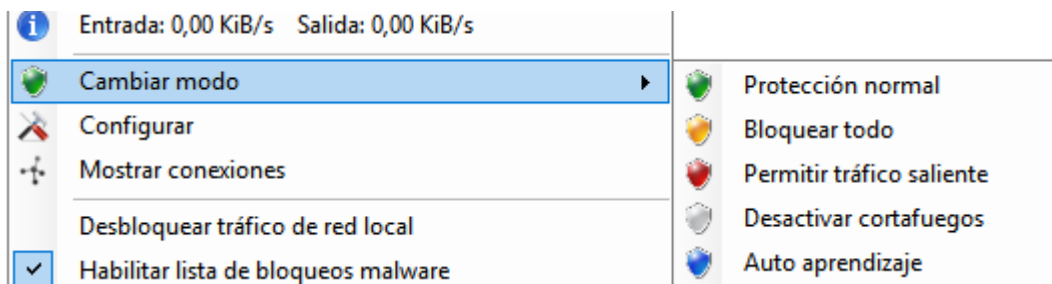
Miramos el cuadro de conexiones y vemos que ya tenemos dos servicios con salida.

Proceso (ID)	Service	Protocolo	Puerto ori...	Dirección local/origen	Puerto destino	Dirección remota/destino	Estado	Dirección	Fecha
brave.exe (8028)	BITS	TCP	63701	127.0.0.1	52242	127.0.0.1	SynSent		2022/04
svchost.exe (7312)	BITS	TCP	63720	172.168.1.117	443	2.17.153.3	SynSent		2022/04

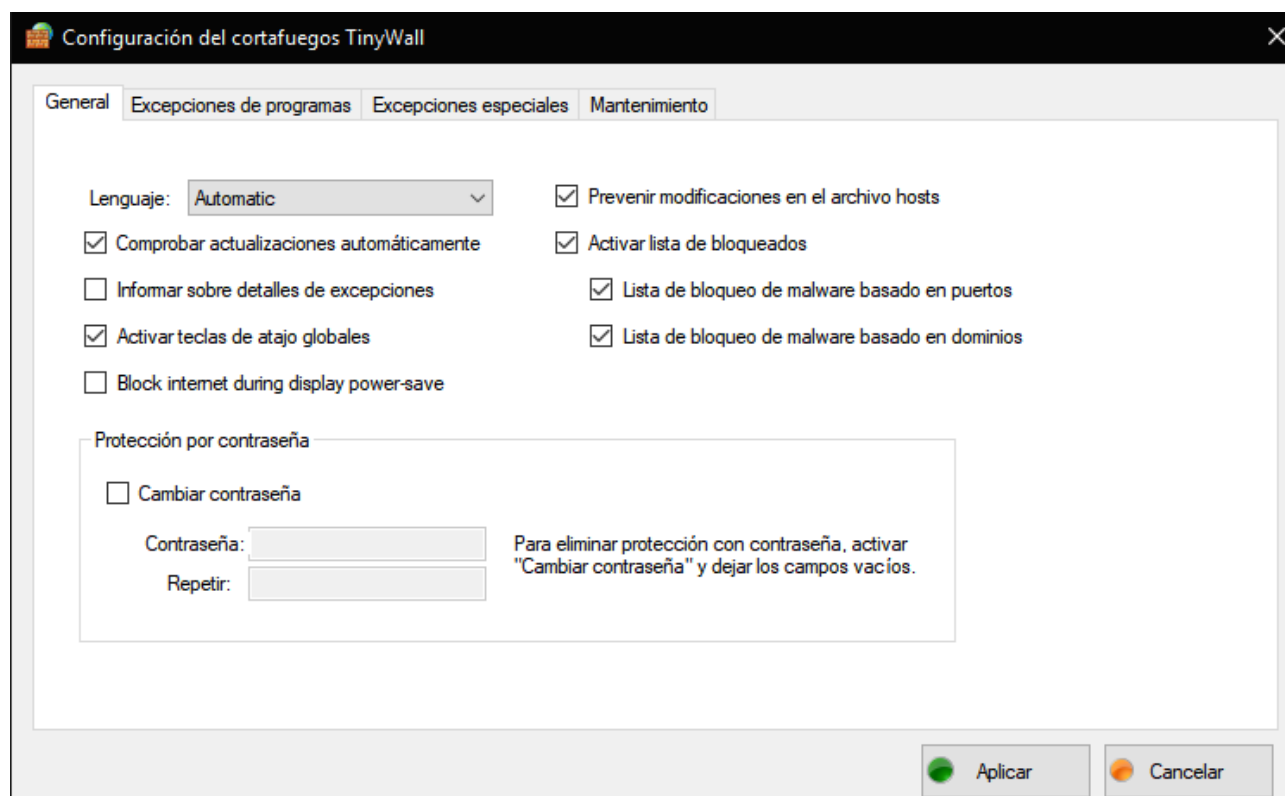
Podemos configurar nuestro Firewall de manera sencilla pinchando en cualquier de las 5 modalidades que ya vienen preconfiguradas



<b>PRÁCTICA : E6 – Instalar un cortafuegos en Windows y Linux</b> <b>MF0486_3 : Seguridad en Equipos Informáticos</b>			Fecha	21 / 03 / 2022
			Página 9 de 5	
Curso	7.1. MF0486_3 Seguridad en equipos informáticos	Plan de Formación	FC- 2021.1/II.000/1914256	



Tenemos la opción de crear nuestras propias reglas e indicarles que deseamos que se conecte o no como lo vemos en **Configurar**



<b>PRÁCTICA : E6 – Instalar un cortafuegos en Windows y Linux</b> <b>MF0486_3 : Seguridad en Equipos Informáticos</b>			Fecha	21 / 03 / 2022
			Página 10 de 5	
Curso	7.1. MF0486_3 Seguridad en equipos informáticos	Plan de Formación	FC- 2021.1/II.000/1914256	

Tenemos excepciones especiales

**Configuración del cortafuegos TinyWall**

General Excepciones de programas **Excepciones especiales** Mantenimiento

Seleccionar los servicios o programas especiales que se permitirán en este equipo. Cuidado al desactivar excepciones recomendadas ya que puede limitar la seguridad del equipo.

**Recomendado**

- ☒ Actualizaciones de Windows
- ☒ Actualizaciones de Windows Store
- ☒ Cliente DHCP de Windows
- ☒ Cliente DNS de Windows
- ☒ Descubrimiento de redes de Windows
- ☒ Filtrar tráfico ICMP
- ☒ Sincronización del reloj de Windows

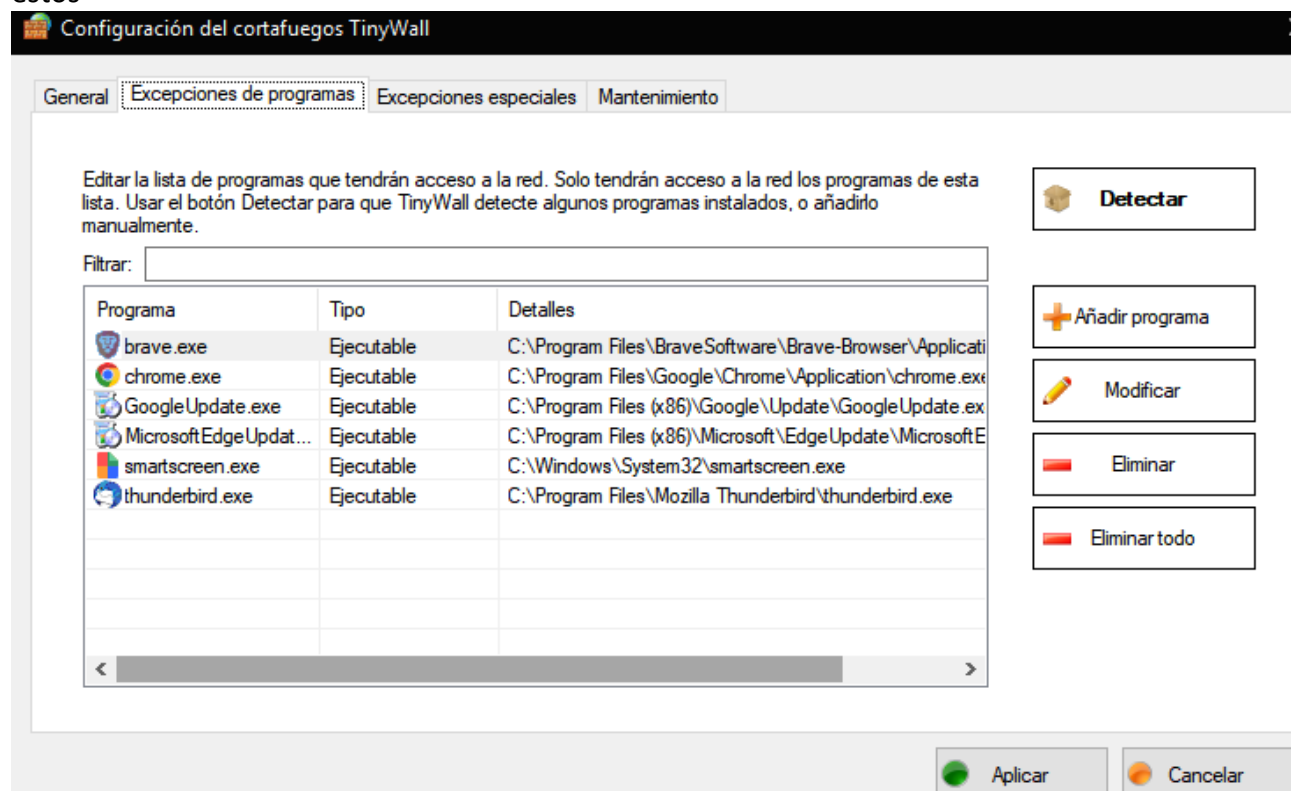
**Opcional**

- ☐ Archivos e impresoras compartidas
- ☐ Asistencia remota de Windows
- ☐ Escritorio remoto de Windows
- ☐ Ping máquina local
- ☐ VPN L2TP/IPSec
- ☐ VPN PPTP
- ☐ Windows Defender
- ☐ WSL 2

Aplicar Cancelar

<b>PRÁCTICA : E6 – Instalar un cortafuegos en Windows y Linux</b> <b>MF0486_3 : Seguridad en Equipos Informáticos</b>			Fecha	21 / 03 / 2022
			Página 11 de 5	
Curso	7.1. MF0486_3 Seguridad en equipos informáticos	Plan de Formación	FC- 2021.1/II.000/1914256	

Y en programas podemos configurar lo que queremos en mi caso he puesto estos



<b>PRÁCTICA : E6 – Instalar un cortafuegos en Windows y Linux</b> <b>MF0486_3 : Seguridad en Equipos Informáticos</b>			Fecha	21 / 03 / 2022
			Página 12 de 5	
Curso	7.1. MF0486_3 Seguridad en equipos informáticos	Plan de Formación	FC- 2021.1/II.000/1914256	

Añadir/modificar excepción del cortafuegos - TinyWall

Reconocido brave.exe

Duración excepción: Permanente

Programa: C:\Program Files\BraveSoftware\Brave-Brow

Tipo: Ejecutable

Seleccionar proceso...

Buscar archivo...

Elegir servicio...

Elegir aplicación UWP...

☐ Restringir a red local

☐ Aplicar mismas reglas a procesos hijo

☐ Bloquear siempre todo el tráfico

☐ Permitir sólo los puertos especificados

☐ Permitir tráfico saliente de UDP y TCP

☐ Sin restricciones de tráfico UDP y TCP

☒ Sin restricciones

Abrir los siguientes puertos, además de las restricciones de arriba. (Lista separada por comas)

Salida TCP: \*

Salida UDP: \*

Entrada TCP: \*

Entrada UDP: \*

Aplicar

Cancelar

Ahora lo único que tenemos que hacer es elegir más programas y servicios o procesos que no queramos que tenga salida y creamos las reglas, por ejemplo, para bloquear el proceso de update adobe haríamos lo siguiente. Pinchamos en **Añadir programa** luego **Seleccionar servicio** elegimos el proceso y luego **bloqueamos todo el trafico**

<b>PRÁCTICA : E6 – Instalar un cortafuegos en Windows y Linux</b> <b>MF0486_3 : Seguridad en Equipos Informáticos</b>		Fecha	21 / 03 / 2022
		Página 13 de 5	
Curso	7.1. MF0486_3 Seguridad en equipos informáticos	Plan de Formación	FC- 2021.1/II.000/1914256

Servicios			
Descripción	Nombre	Ejecutable	
Actualizador de zona horaria automática	tzaupdate	C:\Windows\system32\svchost.exe	
Adaptador de rendimiento de WMI	wmiApSrv	C:\Windows\system32\wbem\WmiA...	
Administración de aplicaciones	AppMgmt	C:\Windows\system32\svchost.exe	
Administración de autenticación de Xbox Live	XblAuthManager	C:\Windows\system32\svchost.exe	
Administración de capas de almacenamiento	TieringEngineService	C:\Windows\system32\TieringEngine...	
Administración de máquinas virtuales de Hyper-V	vmms	C:\Windows\system32\vmms.exe	
Administración remota de Windows (WS-Management)	WinRM	C:\Windows\System32\svchost.exe	
Administrador de conexiones automáticas de acceso re...	RasAuto	C:\Windows\System32\svchost.exe	
Administrador de conexiones de acceso remoto	RasMan	C:\Windows\System32\svchost.exe	
Administrador de conexiones de Windows	Wcmsvc	C:\Windows\system32\svchost.exe	
Administrador de configuración de dispositivos	DsmSvc	C:\Windows\system32\svchost.exe	
Administrador de credenciales	VaultSvc	C:\Windows\system32\lsass.exe	
Administrador de cuentas de seguridad	SamSs	C:\Windows\system32\lsass.exe	
Administrador de cuentas web	TokenBroker	C:\Windows\system32\svchost.exe	
Administrador de identidad de redes de mismo nivel	p2pimsvc	C:\Windows\System32\svchost.exe	
Administrador de mapas descargados	MapsBroker	C:\Windows\System32\svchost.exe	
Administrador de pagos y NFC/SE	SEMGrSvc	C:\Windows\system32\svchost.exe	
Administrador de sesión local	LSM	C:\Windows\system32\svchost.exe	
Administrador de usuarios	UserManager	C:\Windows\system32\svchost.exe	
Adobe Acrobat Update Service	AdobeARMService	C:\Program Files (x86)\Common Files...	
Adquisición de imágenes de Windows (WIA)	stisvc	C:\Windows\system32\svchost.exe	
Agente de conexión de red	NcbService	C:\Windows\System32\svchost.exe	
Agente de detección en segundo plano de DevQuery	DevQueryBroker	C:\Windows\system32\svchost.exe	
Agente de directiva IPsec	PolicyAgent	C:\Windows\system32\svchost.exe	
Agente de eventos de tiempo	TimeBrokerSvc	C:\Windows\system32\svchost.exe	
Agente de eventos del sistema	SystemEventsBroker	C:\Windows\system32\svchost.exe	
Agente de supervisión en tiempo de ejecución de Prote...	SgmBroker	C:\Windows\system32\SgmBroker.e...	
Agrupación de red del mismo nivel	p2psvc	C:\Windows\System32\svchost.exe	
Aislamiento de claves CNG	KeyIso	C:\Windows\system32\lsass.exe	
Aplicación auxiliar de NetBIOS sobre TCP/IP	lmhosts	C:\Windows\System32\svchost.exe	
Aplicación auxiliar IP	iphlpvc	C:\Windows\System32\svchost.exe	
Aplicación del sistema COM+	COMSysApp	C:\Windows\system32\dlhhost.exe	
Archivos sin conexión	CscService	C:\Windows\System32\svchost.exe	
Asignador de detección de topologías de nivel de vínculo	ltdsvc	C:\Windows\System32\svchost.exe	
Asignador de extremos de RPC	RpcEptMapper	C:\Windows\system32\svchost.exe	
Asistente para la conectividad de red	NcaSvc	C:\Windows\System32\svchost.exe	
ASUS Com Service	asComSvc	C:\Program Files (x86)\ASUS\AXSP\...	
Audio de Windows	Audiosrv	C:\Windows\System32\svchost.exe	
Autenticación natural	NaturalAuthentication	C:\Windows\system32\svchost.exe	

Seleccionar Cancelar

<b>PRÁCTICA : E6 – Instalar un cortafuegos en Windows y Linux</b> <b>MF0486_3 : Seguridad en Equipos Informáticos</b>			Fecha	21 / 03 / 2022
			Página 14 de 5	
Curso	7.1. MF0486_3 Seguridad en equipos informáticos	Plan de Formación	FC- 2021.1/II.000/1914256	

Añadir/modificar excepción del cortafuegos - TinyWall

**Reconocido AdobeARMservice (armsvc.exe)**

Duración excepción: Permanente

Programa: AdobeARMservice (C:\Program Files (x86)\C...

Tipo: Servicio

☐ Restringir a red local  
☐ Aplicar mismas reglas a procesos hijo  
☒ Bloquear siempre todo el tráfico  
☐ Permitir sólo los puertos especificados  
☐ Permitir tráfico saliente de UDP y TCP  
☐ Sin restricciones de tráfico UDP y TCP  
☐ Sin restricciones

Abrir los siguientes puertos, además de las restricciones de arriba. (Lista separada por comas)

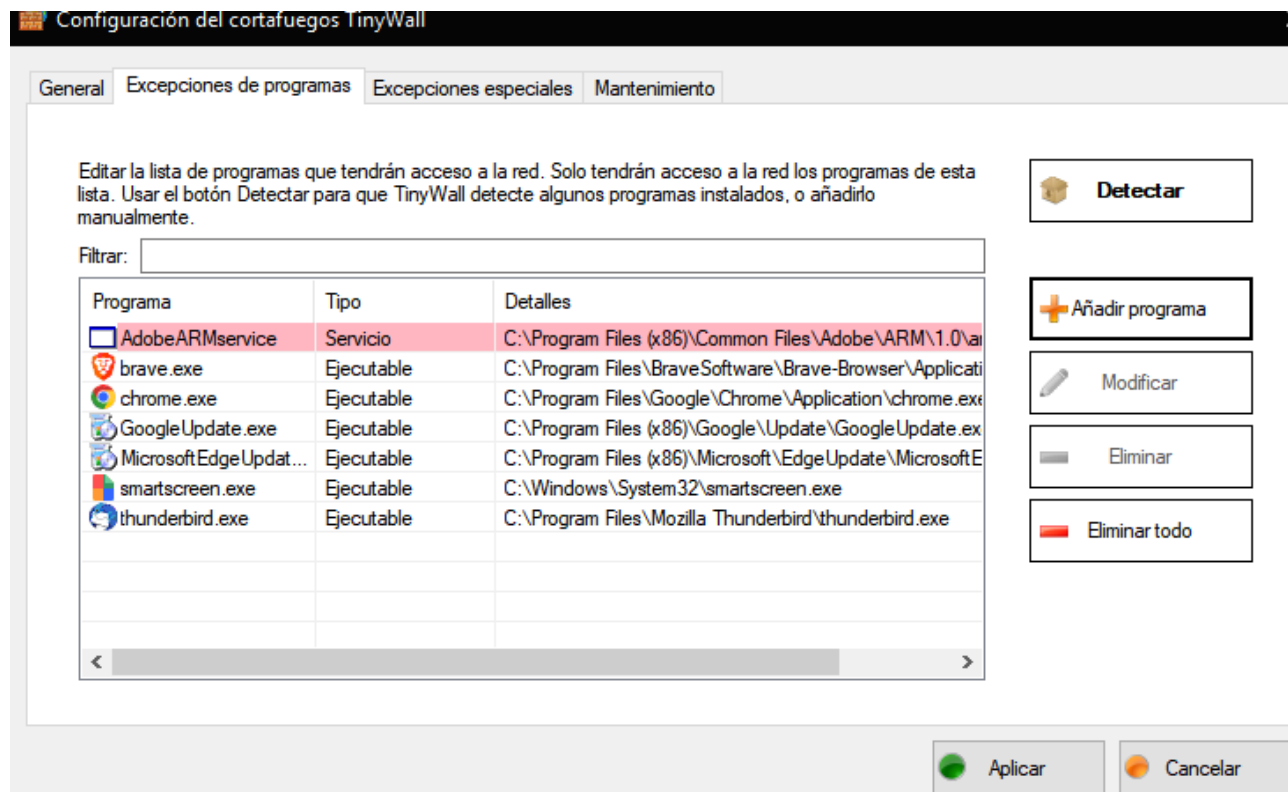
Salida TCP:  Salida UDP:

Entrada TCP:  Entrada UDP:

Y ahora vemos como me indica lo que tengo bloqueado y no, marcando en rojo los elementos que no tienen salida a internet.



<b>PRÁCTICA : E6 – Instalar un cortafuegos en Windows y Linux</b> <b>MF0486_3 : Seguridad en Equipos Informáticos</b>		<b>Fecha</b>	21 / 03 / 2022
		Página 15 de 5	
<b>Curso</b>	7.1. MF0486_3 Seguridad en equipos informáticos	<b>Plan de Formación</b>	FC- 2021.1/II.000/1914256



La ventaja de Tinyfirewall es que es un cliente ligero que se puede instalar en cualquier ordenador tanto antiguo como nuevo que hace exactamente lo que necesitamos y es protegernos y poder decidir que elementos queremos que tengan conexión o no a nuestro equipo y como agregado puede cotejar mediante una lista que esta en internet si existe o hay posibilidad de que una conexión sea maliciosa mediante los puertos.

- ☒ Prevenir modificaciones en el archivo hosts
- ☒ Activar lista de bloqueados
  - ☒ Lista de bloqueo de malware basado en puertos
  - ☒ Lista de bloqueo de malware basado en dominios