

# Taller de Instalación y Configuración de Aplicaciones

## Guía de Trabajo 3.4 - Configuración de Firewall en Windows 10

En esta guía veremos cómo agregamos permisos a las aplicaciones en el firewall de Windows.

Esto funciona para las aplicaciones en general habilitando todos los puertos de entrada y salida utilizados por las mismas automáticamente.

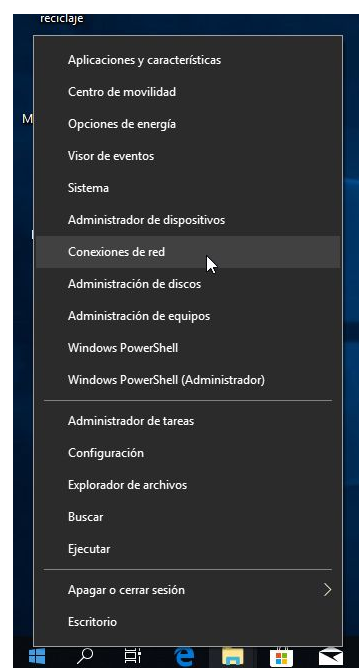
En el caso nuestro funcionará para FTP y todos su puertos, sin embargo en el caso de HTTP sólo habilita el puerto 80. Para poder utilizar otros puertos ver la parte 3 de esta guía.

### Parte 1 - Abrir la configuración de firewall de windows para luego permitir a aplicaciones

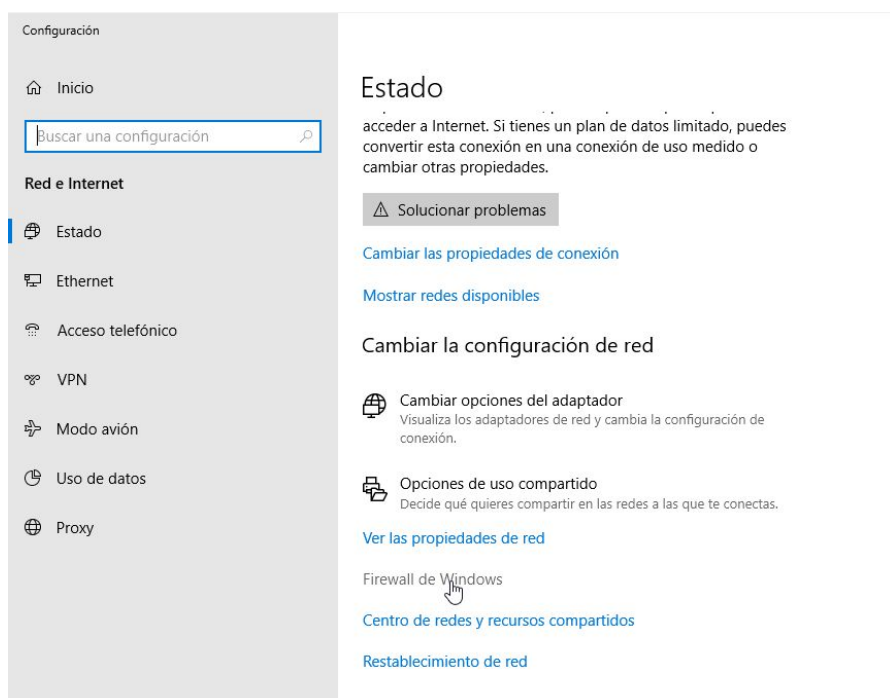
Para abrir la configuración del firewall:

- Desde el menú de Windows 10:

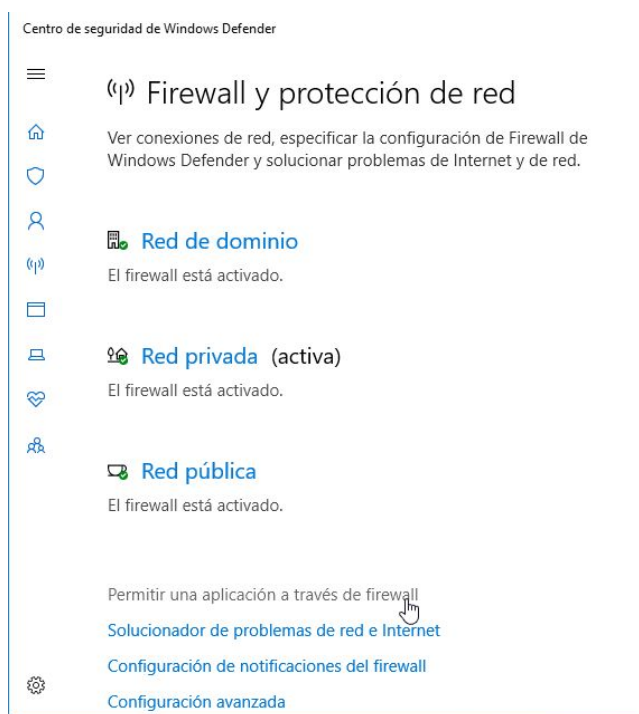
**Paso 1:** Dar click derecho en el botón Inicio. Y elegir “Conexiones de red”.  
Se abrirá la ventana de configuración, mostrando la opción de RED.



**Paso 2:** Ir a la parte inferior hasta encontrar “Firewall de Windows”

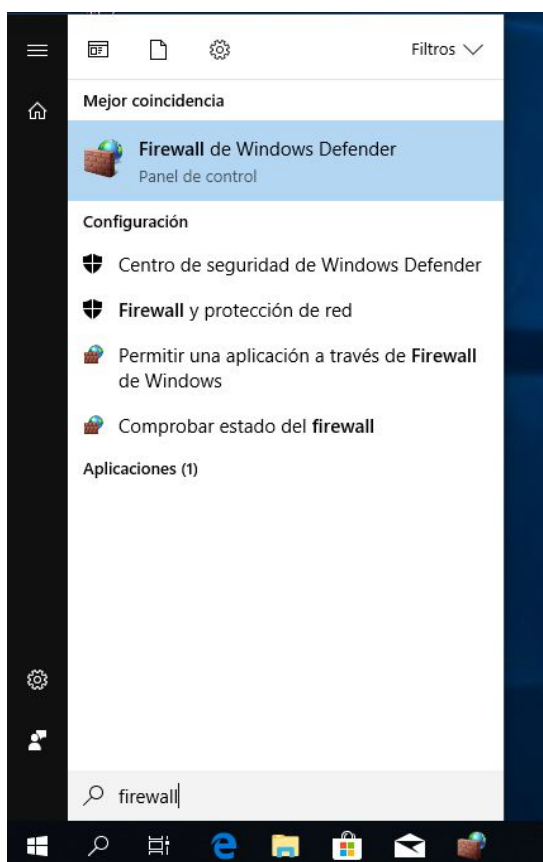


**Paso 3:** Se abrirá “Centro de seguridad de Windows Defender”, Debemos seleccionar la opción que está debajo: “Permitir una aplicación a través de firewall”.

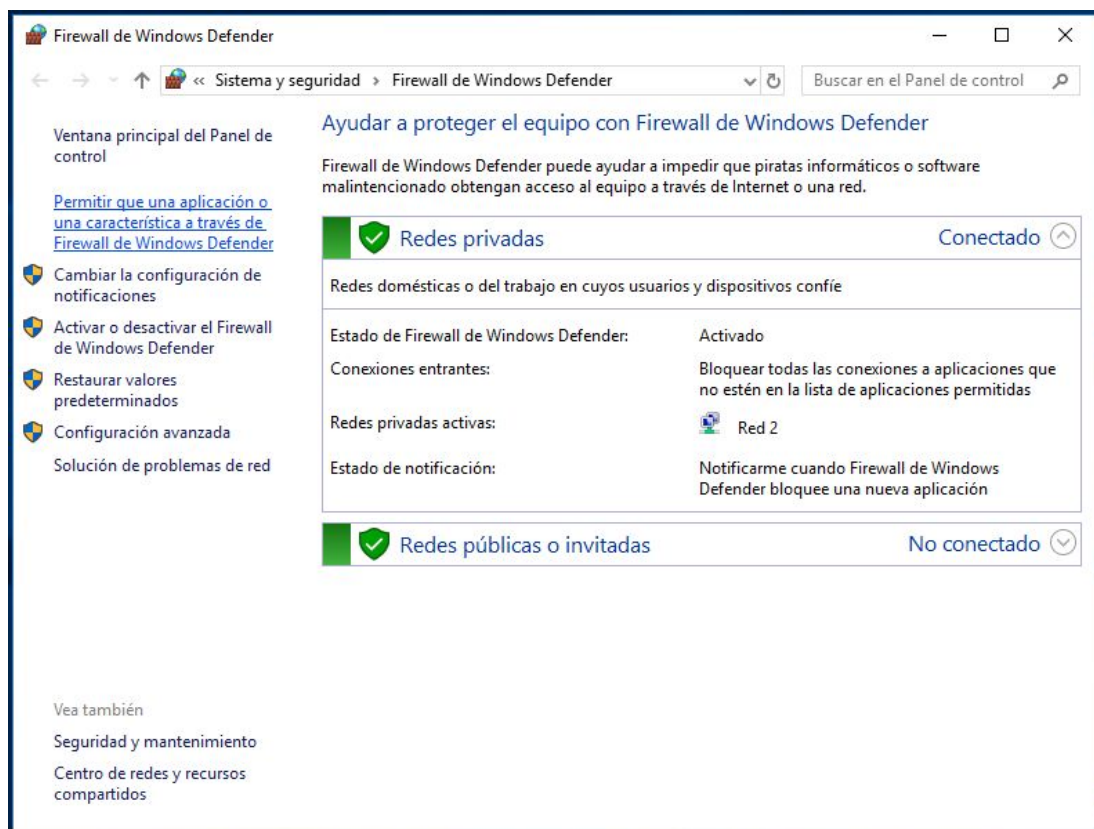


- Desde el buscador de Windows 10:

**Paso 1:** En el buscador escribir “firewall” y seleccionar Firewall de Windows Defender



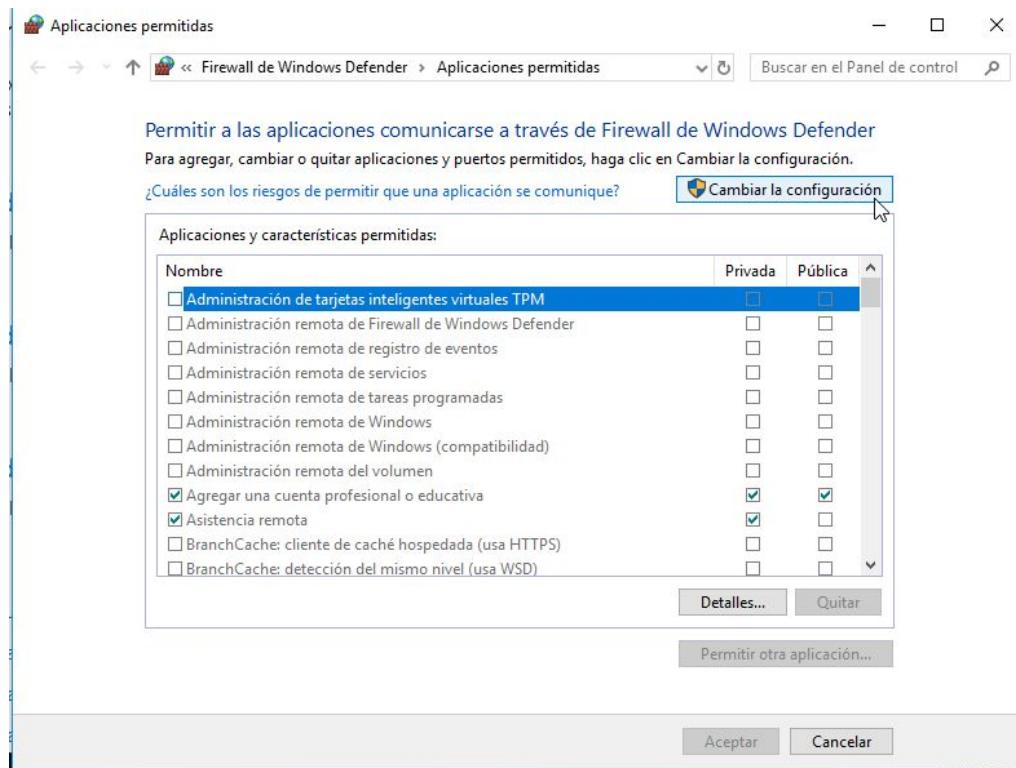
Paso 2: Seleccionar la opción: “Permitir que una aplicación o una característica...”



## Parte 2 - Habilitar las aplicaciones que necesitamos.

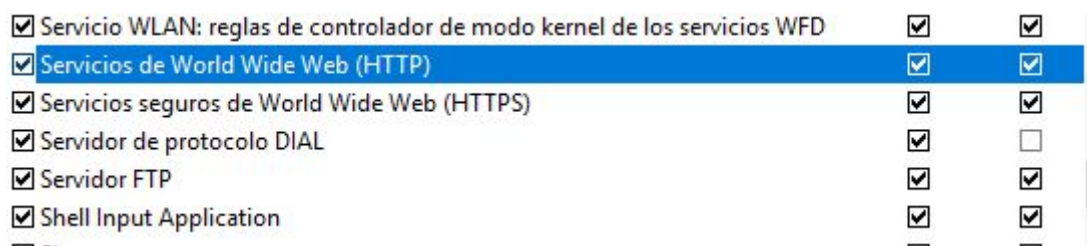
Una vez tenemos abierto el panel de configuración del firewall, debemos seguir los siguientes pasos:

Paso 1: Dar click en “Cambiar la configuración”, se habilitará la lista para realizar modificaciones.



Paso 2: Buscar la aplicación que corresponda en nuestro caso deberemos habilitar:

- Servicios de World Wide Web(HTTP)

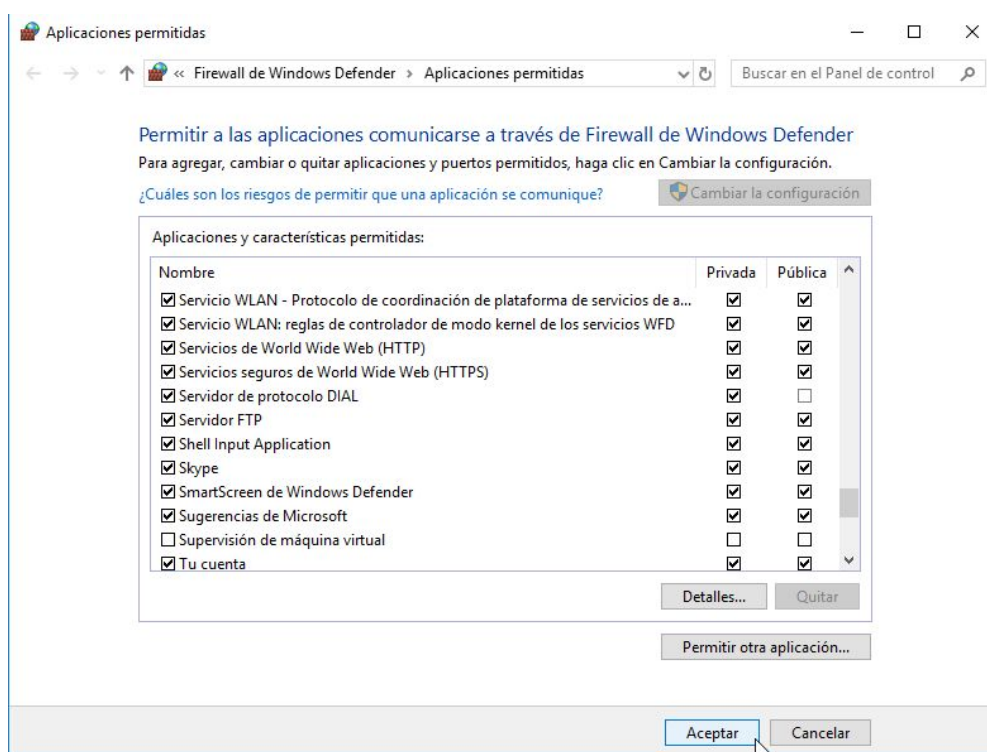


- Servidor FTP



Tener en cuenta que podremos habilitar para ambientes “Públicos” o “Privados” de nuestra red.

**Paso 3:** Una vez elegidos daremos click en “Aceptar” y cerramos las ventanas del “Centro de seguridad de Windows”



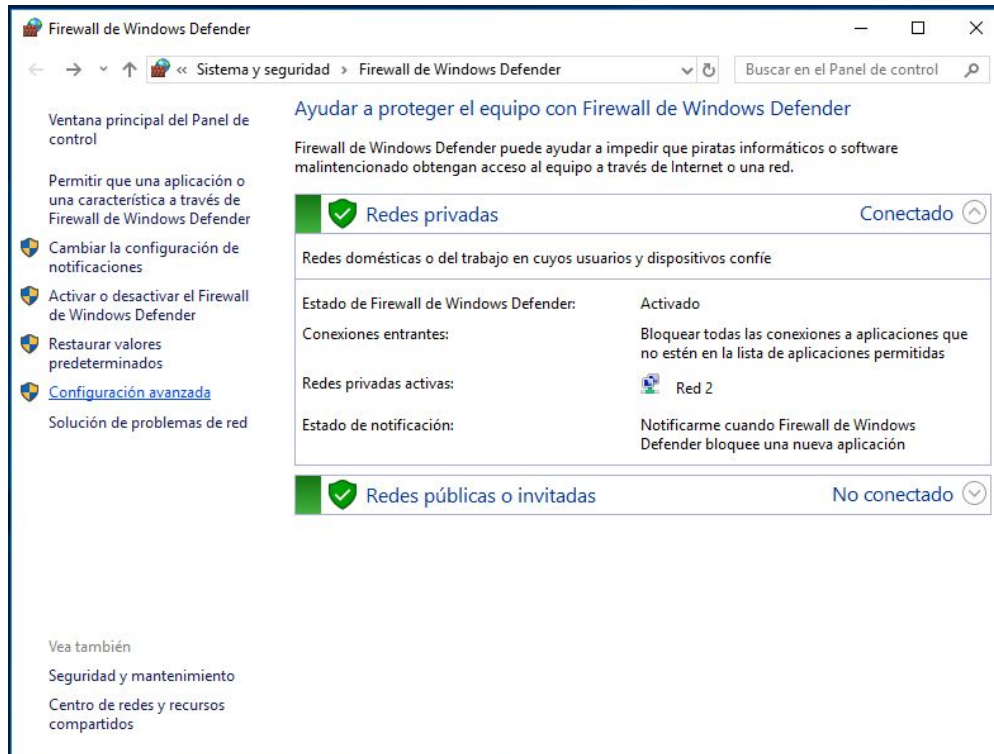
**Paso 4:** Verificar el acceso desde un explorador web del Host, colocando la **ip** de la VM precedida por http://. Por ej: “http://192.168.212.5”

**Paso 5:** Verificar el acceso desde Winscp del Host, colocando la **ip** de la VM, el **puerto** elegido para nuestro SitioFTP y , el usuario y contraseña correspondientes.

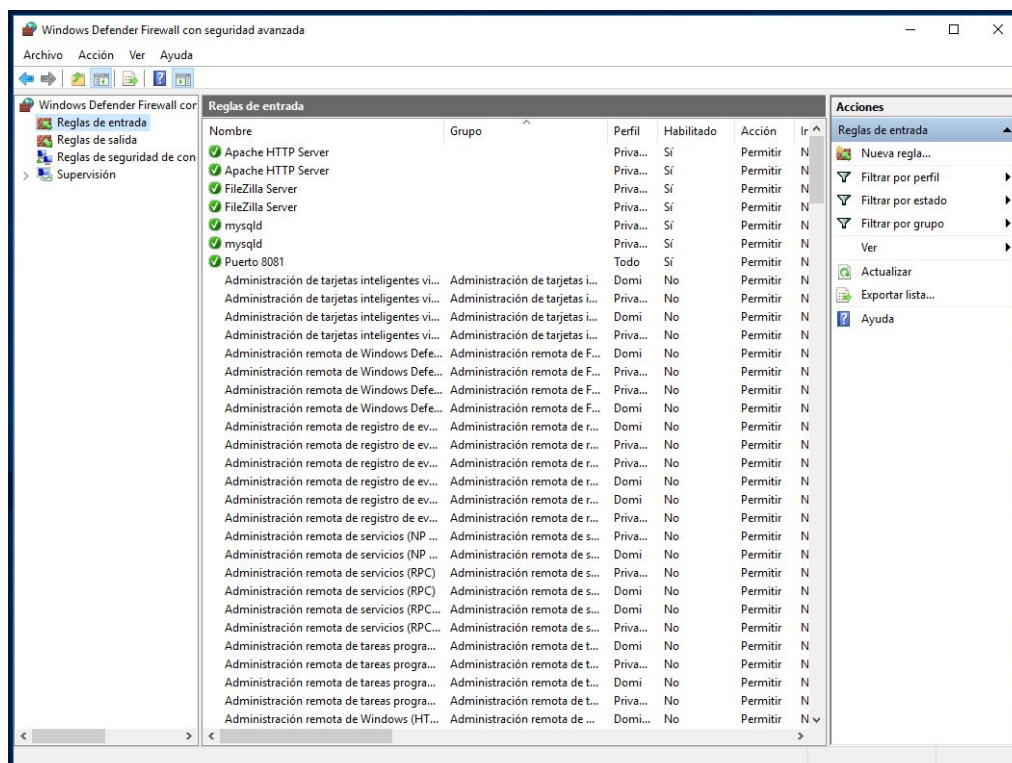
### Parte 3 - Habilitar otros puertos en el Firewall. Útil para nosotros para HTTP

Si nuestros sitios web utilizan puertos diferentes al 80, además de la configuración de la parte 1, deberemos agregar reglas en el firewall que permitan el tráfico a través de dichos puertos. Por ejemplo, para habilitar la comunicación a través del puerto 8081, deberíamos hacer lo siguiente:

Paso 1: En el panel del Firewall de Windows, elegir la opción Configuración Avanzada:



Paso 2: Seleccionar en el panel de la izquierda "Reglas de Entrada":





**Paso 3:** Seleccionar en el panel de la derecha “Nueva regla...” y en tipo de regla seleccionar “Puerto”:

**Paso 4:** Seleccionar el protocolo TCP y como puerto local específico el 8081:

**Paso 5:** En Acción, seleccionar Permitir la conexión:

Asistente para nueva regla de entrada

**Acción**

Especifique la acción que debe llevarse a cabo cuando una conexión coincide con las condiciones especificadas en la regla.

**Pasos:**

- Tipo de regla
- Protocolo y puertos
- Acción**
- Perfil
- Nombre

¿Qué medida debe tomarse si una conexión coincide con las condiciones especificadas?

☒ **Permitir la conexión**  
Esto incluye las conexiones protegidas mediante IPsec y las que no lo están.

☐ **Permitir la conexión si es segura**  
Esto incluye solamente las conexiones autenticadas mediante IPsec. Éstas se protegerán mediante la configuración de reglas y propiedades de IPsec del nodo Regla de seguridad de conexión.

Personalizar...

☐ **Bloquear la conexión**

< Atrás    Siguiendo >    Cancelar

**Paso 6:** Seleccionar los perfiles a los que se aplica la regla:

Asistente para nueva regla de entrada

**Perfil**

Especifique los perfiles en los que se va a aplicar esta regla.

**Pasos:**

- Tipo de regla
- Protocolo y puertos
- Acción
- Perfil**
- Nombre

¿Cuándo se aplica esta regla?

☒ **Dominio**  
Se aplica cuando un equipo está conectado a su dominio corporativo.

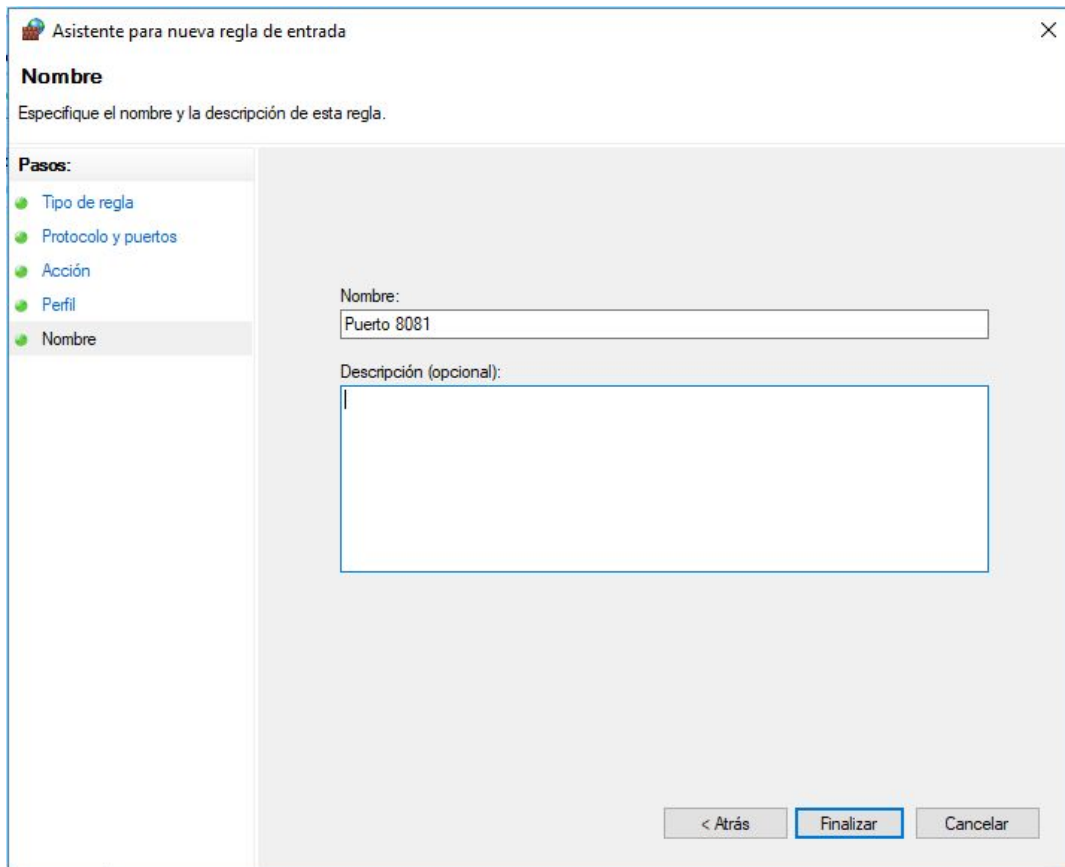
☒ **Privado**  
Se aplica cuando un equipo está conectado a una ubicación de red privada, como una red doméstica o del lugar de trabajo.

☒ **Público**  
Se aplica cuando un equipo está conectado a una ubicación de redes públicas.

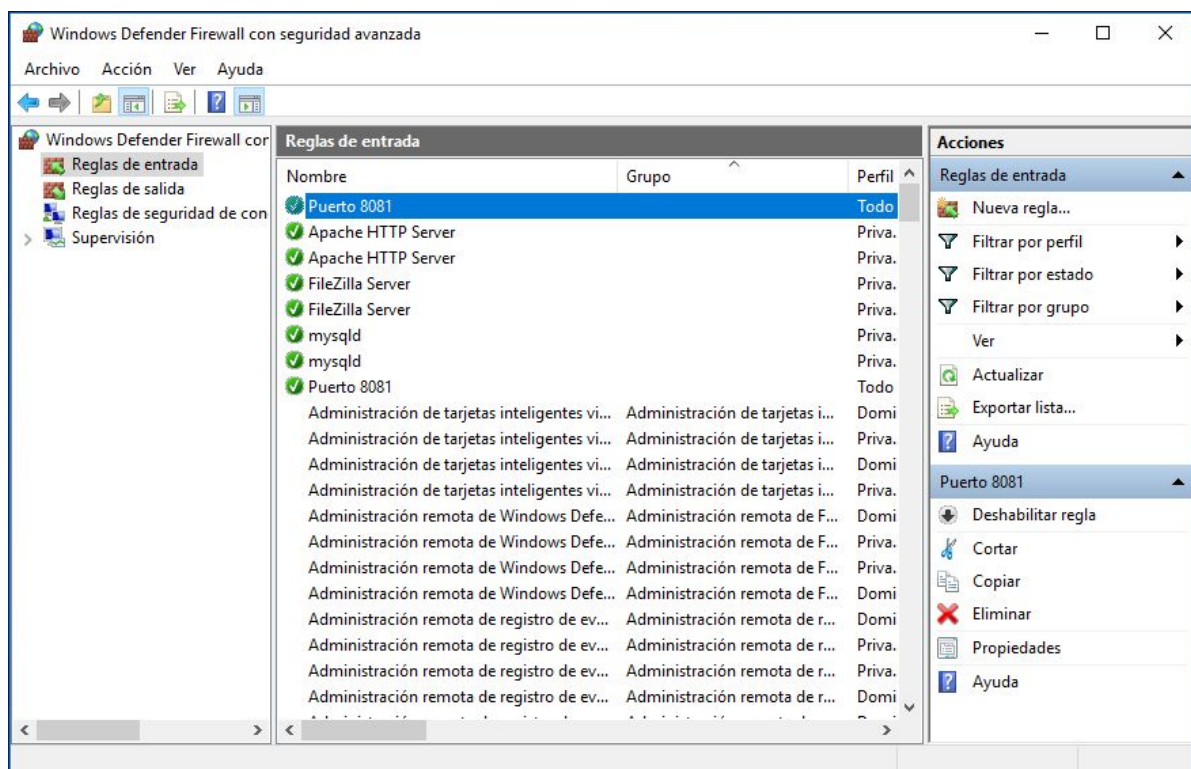
< Atrás    Siguiendo >    Cancelar



Paso 7: Poner un nombre descriptivo a la regla y finalizar:



Ahora la regla debería aparecer habilitada (con un visto de color verde) en el firewall:



Paso 8: Volver a probar desde el host para verificar que ahora sí podemos ver el sitio web.