



Habilitar puerto de Pentaho en servidor



Objetivo:

El objetivo de esta guía es habilitar en el firewall de Windows el puerto utilizado por Pentaho BI, esto para dar solución al caso de que en Pentaho solamente se puede acceder desde el mismo servidor donde está instalado, no desde fuera.

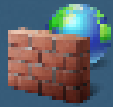


Índice:

1.	Abrir Windows Defender Firewall.....	1
2.	Seleccionar Reglas de entrada.....	2
3.	Seleccionar Nueva Regla.....	3
4.	Tipo de Regla.....	4
5.	Protocolo y Puertos.....	5
6.	Acción.....	6
7.	Perfil.....	7
8.	Nombre.....	8



1. Abrir Windows Defender Firewall.

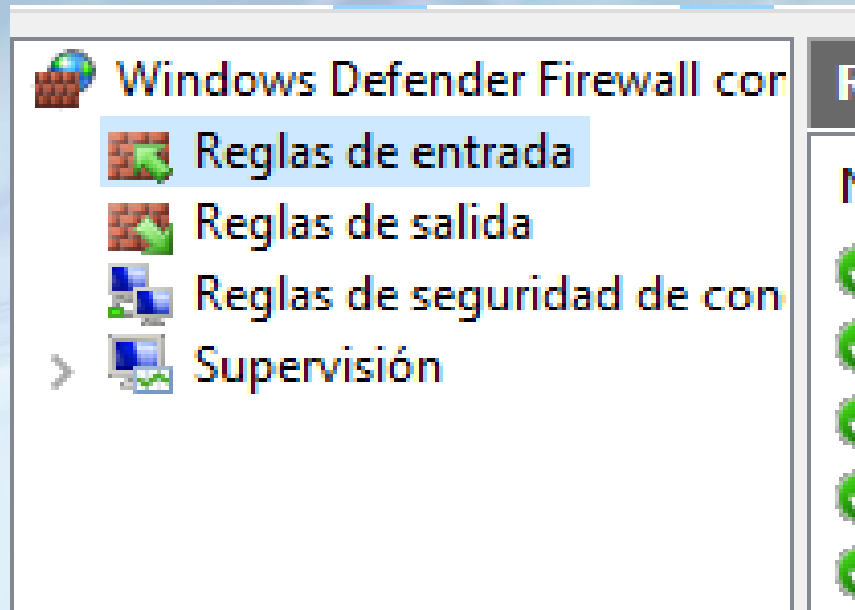


Windows Defender Firewall con
seguridad avanzada

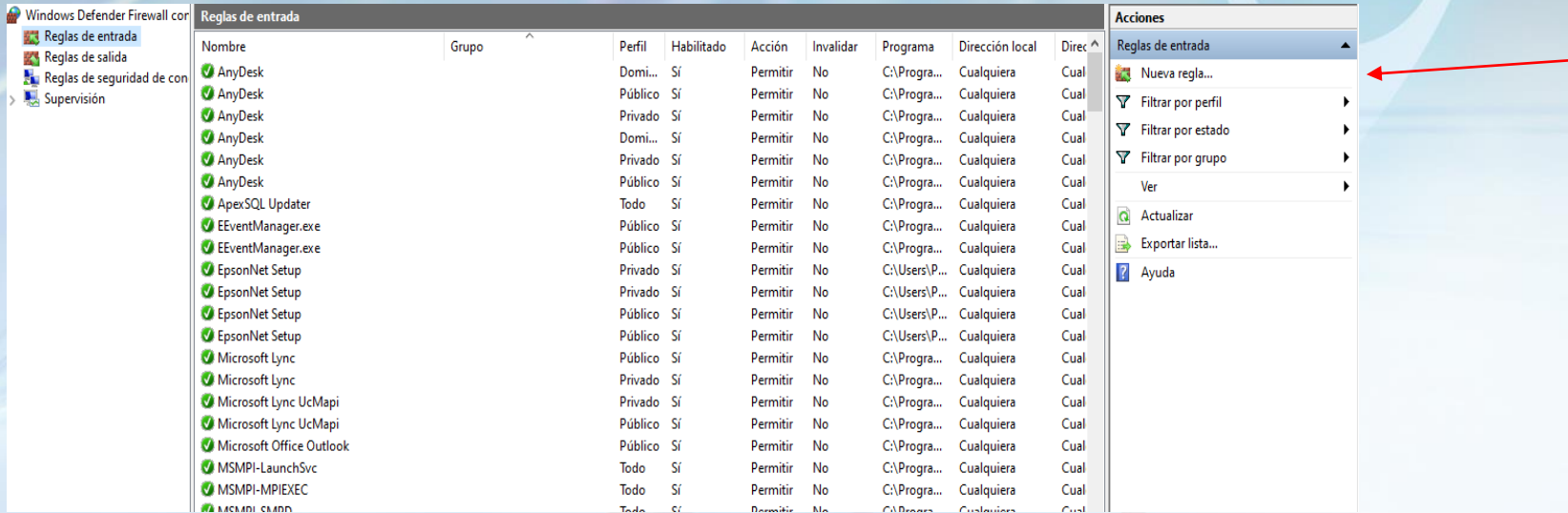
Aplicación



2. Seleccionar Reglas de entrada.



3. Seleccionar Nueva Regla



Windows Defender Firewall control panel showing the 'Reglas de entrada' (Inbound Rules) list. The 'Acciones' (Actions) dropdown menu is open, highlighting 'Nueva regla...' (New rule...). A red arrow points to this option.

Nombre	Grupo	Perfil	Habilitado	Acción	Invaldar	Programa	Dirección local	Direc
AnyDesk		Dom...	Sí	Permitir	No	C:\Progra...	Cualquiera	Cual
AnyDesk		Público	Sí	Permitir	No	C:\Progra...	Cualquiera	Cual
AnyDesk		Privado	Sí	Permitir	No	C:\Progra...	Cualquiera	Cual
AnyDesk		Dom...	Sí	Permitir	No	C:\Progra...	Cualquiera	Cual
AnyDesk		Privado	Sí	Permitir	No	C:\Progra...	Cualquiera	Cual
AnyDesk		Público	Sí	Permitir	No	C:\Progra...	Cualquiera	Cual
ApexSQL Updater		Todo	Sí	Permitir	No	C:\Progra...	Cualquiera	Cual
EEventManager.exe		Público	Sí	Permitir	No	C:\Progra...	Cualquiera	Cual
EEventManager.exe		Público	Sí	Permitir	No	C:\Progra...	Cualquiera	Cual
EpsonNet Setup		Privado	Sí	Permitir	No	C:\Users\P...	Cualquiera	Cual
EpsonNet Setup		Privado	Sí	Permitir	No	C:\Users\P...	Cualquiera	Cual
EpsonNet Setup		Público	Sí	Permitir	No	C:\Users\P...	Cualquiera	Cual
EpsonNet Setup		Público	Sí	Permitir	No	C:\Users\P...	Cualquiera	Cual
EpsonNet Setup		Privado	Sí	Permitir	No	C:\Progra...	Cualquiera	Cual
EpsonNet Setup		Privado	Sí	Permitir	No	C:\Progra...	Cualquiera	Cual
Microsoft Lync		Público	Sí	Permitir	No	C:\Progra...	Cualquiera	Cual
Microsoft Lync		Privado	Sí	Permitir	No	C:\Progra...	Cualquiera	Cual
Microsoft Lync UcMapi		Privado	Sí	Permitir	No	C:\Progra...	Cualquiera	Cual
Microsoft Lync UcMapi		Público	Sí	Permitir	No	C:\Progra...	Cualquiera	Cual
Microsoft Office Outlook		Público	Sí	Permitir	No	C:\Progra...	Cualquiera	Cual
MSMPI-LaunchSvc		Todo	Sí	Permitir	No	C:\Progra...	Cualquiera	Cual
MSMPI-MPIEXEC		Todo	Sí	Permitir	No	C:\Progra...	Cualquiera	Cual
MSMPI-SMPD		Todo	Sí	Permitir	No	C:\Progra...	Cualquiera	Cual



4. Tipo de Regla

Asistente para nueva regla de entrada

Tipo de regla

Seleccione el tipo de regla de firewall que desea crear.

Pasos:

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

¿Qué tipo de regla desea crear?

Programa
Regla que controla las conexiones de un programa.

Puerto
Regla que controla las conexiones de un puerto TCP o UDP.

Predefinida:
@FirewallAPI.dll,-80200
Regla que controla las conexiones de una experiencia con Windows.

Personalizada
Regla personalizada.

< Atrás **Siguiente >** Cancelar

5. Protocolo y Puertos

Asistente para nueva regla de entrada

Protocolo y puertos

Especifique los puertos y protocolos a los que se aplica esta regla.

Pasos:

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

¿Se aplica esta regla a TCP o UDP?

TCP
 UDP

¿Se aplica esta regla a todos los puertos locales o a unos puertos locales específicos?

Todos los puertos locales
 Puertos locales específicos:

Ejemplo: 80, 443, 5000-5010

< Atrás Siguiete > Cancelar

6. Acción

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 **Siguiente >** Cancelar

7. Perfil

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 **Siguiente >** Cancelar

8. Nombre

Asistente para nueva regla de entrada

Nombre

Especifique el nombre y la descripción de esta regla.

Pasos:

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

Nombre:

Descripción (opcional):

< Atrás Finalizar Cancelar



SPN

SPN