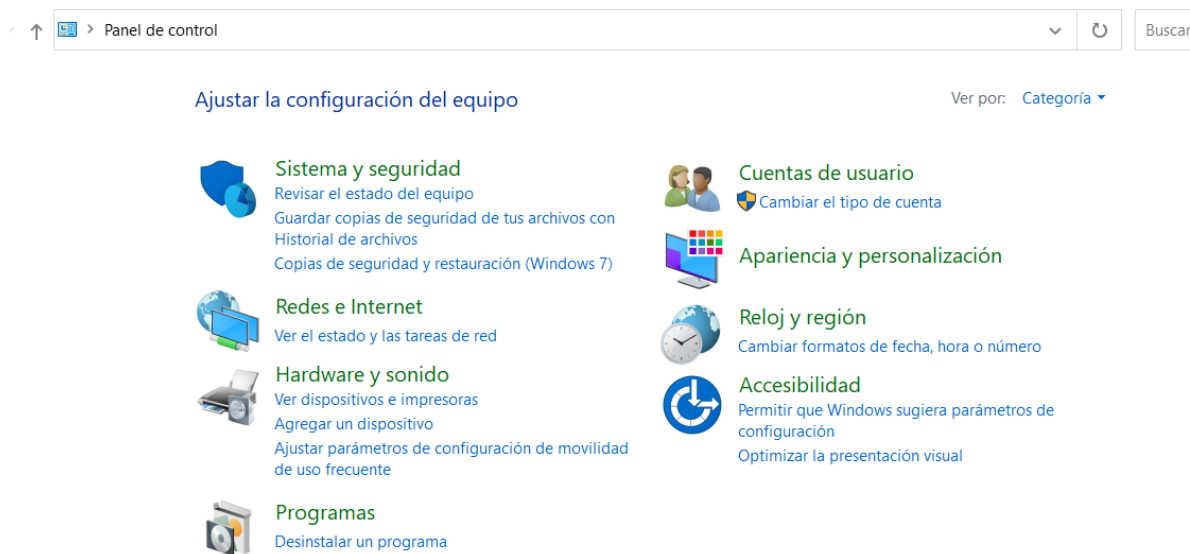


## Accedemos al panel de control



## Luego a sistema y seguridad y damos clic en firewall de Windows defender







## Le damos en desactivar el firewall del windows


Panel de control > Sistema y seguridad > Firewall de Windows Defender

### Ayudar a proteger el equipo con Firewall de Windows Defender

Firewall de Windows Defender puede ayudar a impedir que piratas informáticos o software malintencionado obtengan acceso al equipo a través de Internet o una red.

 <b>Redes privadas</b>	No conectado 
 <b>Redes públicas o invitadas</b>	Conectado 

Redes en lugares públicos como aeropuertos o cafeterías



Estado de Firewall de Windows Defender:	Activado
Conexiones entrantes:	Bloquear todas las conexiones a aplicaciones que no estén en la lista de aplicaciones permitidas
Redes públicas activas:	 Megacable_5G_B80C
Estado de notificación:	Notificarme cuando Firewall de Windows Defender bloquee una nueva aplicación

En un servidor no es recomendable desactivarlos, en su lugar se recomienda configurar permisos



### Personalizar la configuración de cada tipo de red

Puede modificar la configuración del firewall para cada tipo de red que use.

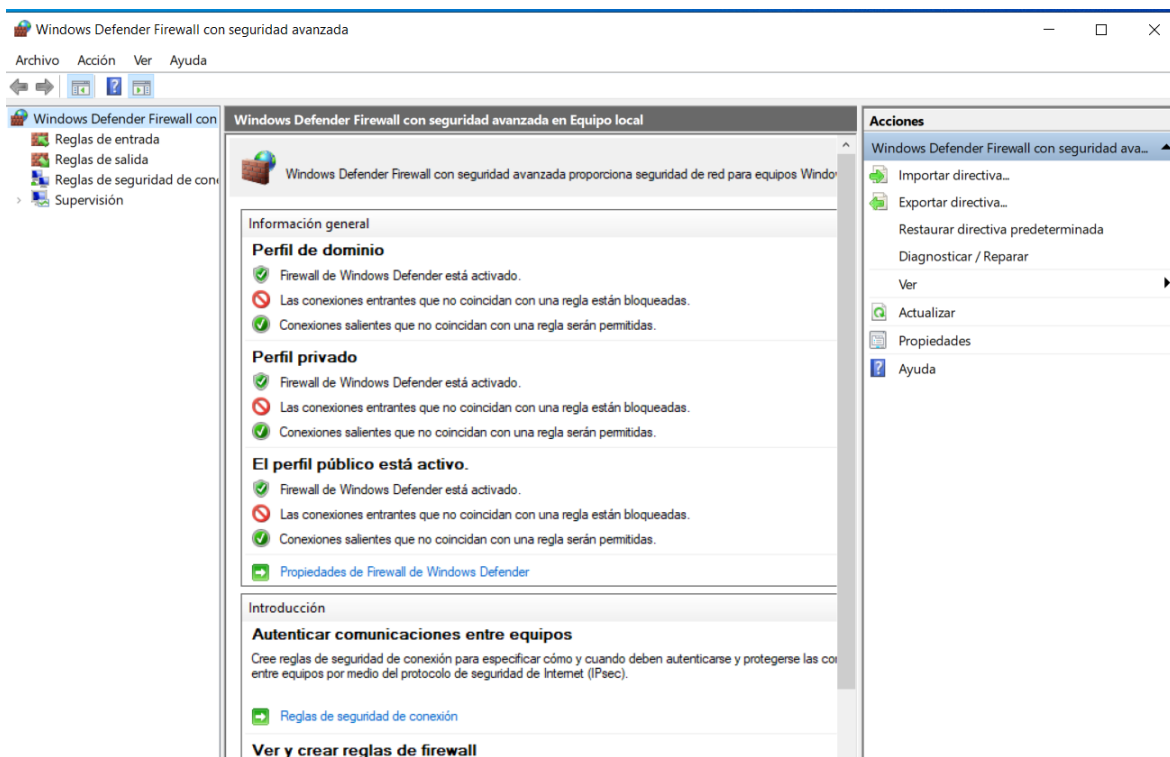
#### Configuración de red privada

-  ☒ Activar Firewall de Windows Defender
- ☐ Bloquear todas las conexiones entrantes, incluidas las de la lista de aplicaciones permitidas
  - ☒ Notificarme cuando Firewall de Windows Defender bloquee una nueva aplicación
-  ☐ Desactivar Firewall de Windows Defender (no recomendado)

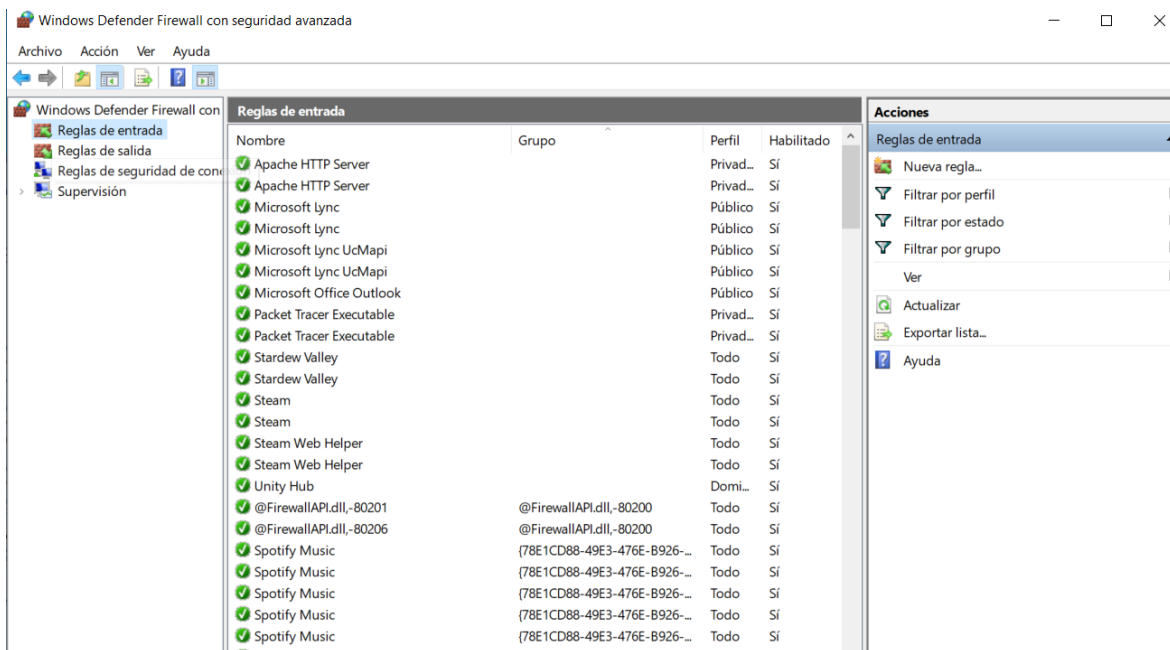
#### Configuración de red pública

-  ☒ Activar Firewall de Windows Defender
- ☐ Bloquear todas las conexiones entrantes, incluidas las de la lista de aplicaciones permitidas
  - ☒ Notificarme cuando Firewall de Windows Defender bloquee una nueva aplicación
-  ☐ Desactivar Firewall de Windows Defender (no recomendado)

Nos regresamos y damos clic en configuración avanzada, y entramos directamente al cortafuegos



Creamos una regla



Para este caso le damos en personalizada

Asistente para nueva regla de entrada

X

Tipo de regla

Seleccione el tipo de regla de firewall que desea crear.

Pasos:

Tipo de regla

Programa

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.

No cambiamos nada

## Programa

Especifique la ruta completa y el nombre del archivo ejecutable del programa con el que coincide esta regla.

### Pasos:

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

¿Se aplica esta regla a todos los programas o a uno específico?

☒ **Todos los programas**

La regla se aplica a todas las conexiones en el equipo que coinciden con otras propiedades de reglas.

☐ **Esta ruta de acceso del programa:**

Examinar...

Ejemplo: c:\path\program.exe  
%ProgramFiles%\browser\browser.exe

### Servicios

Especifique los servicios a los que se aplica esta regla.

Personalizar...

< Atrás

Siguiente >

Cancelar

El tipo de protocolo le cambiamos a ICMPv4

### Protocolo y puertos

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

#### Pasos:

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

¿A qué puertos y protocolos se aplica esta regla?

Tipo de protocolo: Cualquiera

Número de protocolo: 0

Puerto local: Todos los puertos

Ejemplo: 80, 443, 5000-5010

Puerto remoto: Todos los puertos

Ejemplo: 80, 443, 5000-5010

Configuración ICMP: Personaliz...

< Atrás

Siguiente >

Cancelar

¿A qué puertos y protocolos se aplica esta regla?

Tipo de protocolo: ICMPv4

Número de protocolo: 1

Puerto local: Todos los puertos


Ejemplo: 80, 443, 5000-5010


Puerto remoto: Todos los puertos

Ejemplo: 80, 443, 5000-5010

Configuración ICMP: Personaliz...

Aquí podemos admitir o bloquear ciertas direcciones.

 Asistente para nueva regla de entrada



### Ámbito

Especifique las direcciones IP local y remota a las que se aplica esta regla.

**Pasos:**

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

**¿A qué direcciones IP locales se aplica esta regla?**

- ☒ Cualquier dirección IP
- ☐ Estas direcciones IP:

Agregar...

Editar...

Quitar

Personalizar los tipos de interfaz a los que se aplica esta regla: 

Personalizar...

**¿A qué direcciones IP remotas se aplica esta regla?**

- ☒ Cualquier dirección IP
- ☐ Estas direcciones IP:

Agregar...

Editar...


Quitar

< Atrás

Siguiente >

Cancelar

Aquí podemos configurar 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
- Programa
- Protocolo y puertos
- Ámbito
- 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.

☐ **Bloquear la conexión**

< Atrás

Siguiente >

Cancelar



Aquí no cambiamos nada



Asistente para nueva regla de entrada



## Perfil

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

### Pasos:

- Tipo de regla
- Programa
- Protocolo y puertos
- Ámbito
- 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

Nombramos la regla

### Nombre

Especifique el nombre y la descripción de esta regla.

#### Pasos:

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

Nombre:

Jaime

Descripción (opcional):

Regla en cortafuegos

< Atrás

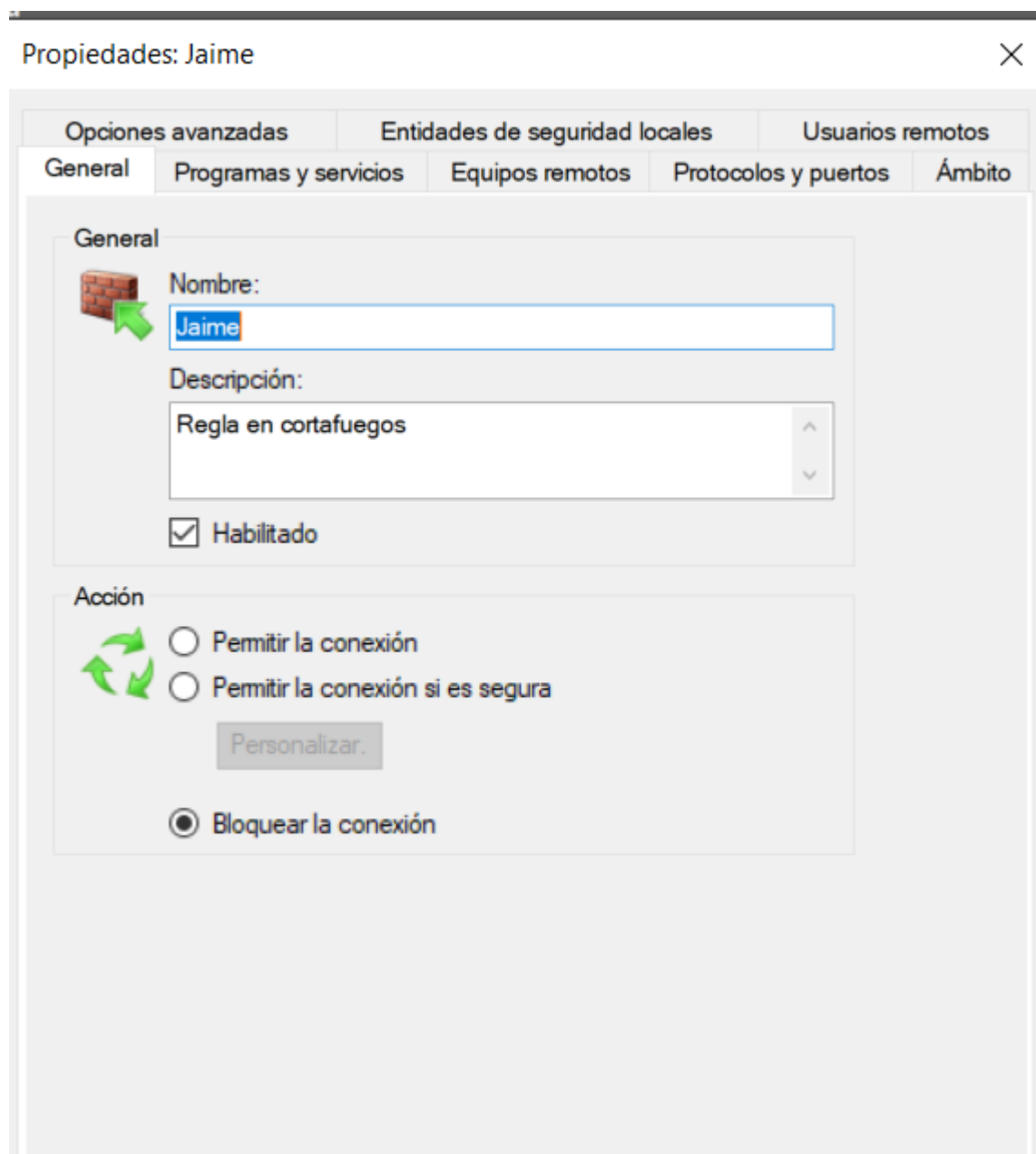
Finalizar

Cancelar

Ya nos aparece la regla

Reglas de entrada				Acciones	
Nombre	Grupo	Perfil	Habilitado	Reglas de entrada	
✓ Jaime		Todo	Sí	Nueva regla...	
✓ Apache HTTP Server		Privad...	Sí	Filtrar por perfil	
✓ Apache HTTP Server		Privad...	Sí	Filtrar por estado	
✓ Microsoft Lync		Público	Sí	Filtrar por grupo	
✓ Microsoft Lync		Público	Sí	Ver	
✓ Microsoft Lync UcMapi		Público	Sí	Actualizar	
✓ Microsoft Lync UcMapi		Público	Sí	Exportar lista...	
✓ Microsoft Office Outlook		Público	Sí	Ayuda	
✓ Packet Tracer Executable		Privad...	Sí	Jaime	
✓ Packet Tracer Executable		Privad...	Sí	Deshabilitar regla	
✓ Stardew Valley		Todo	Sí	Cortar	
✓ Stardew Valley		Todo	Sí	Copiar	
✓ Steam		Todo	Sí	Eliminar	
✓ Steam		Todo	Sí	Propiedades	
✓ Steam Web Helper		Todo	Sí	Ayuda	
✓ Steam Web Helper		Todo	Sí		
✓ Unity Hub		Domi...	Sí		
✓ @FirewallAPI.dll,-80201	@FirewallAPI.dll,-80200	Todo	Sí		
✓ @FirewallAPI.dll,-80206	@FirewallAPI.dll,-80200	Todo	Sí		
✓ Spotify Music	{78E1CD88-49E3-476E-B926-...	Todo	Sí		

Le damos clic derecho en propiedades y cambiamos la conexión



Hacemos ping a una IP de la red

```
C:\Users\Jaime>ping 192.168.1.10

Haciendo ping a 192.168.1.10 con 32 bytes de datos:
Respuesta desde 192.168.1.10: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.10: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.10: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.10: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.1.10:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

Cuando hacemos el cambio ya no llegan los mensajes

```
Haciendo ping a 192.168.1.10 con 32 bytes de datos:
Respuesta desde 192.168.207.254: Host de destino inaccesible.
Respuesta desde 192.168.207.254: Host de destino inaccesible.
Respuesta desde 192.168.207.254: Host de destino inaccesible.
Respuesta desde 192.168.207.254: Host de destino inaccesible.

Estadísticas de ping para 192.168.1.10:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
```

Comando netstat para observar las conexiones activas en nuestro servidor

```
C:\Users\Jaime>netstat

Conexiones activas

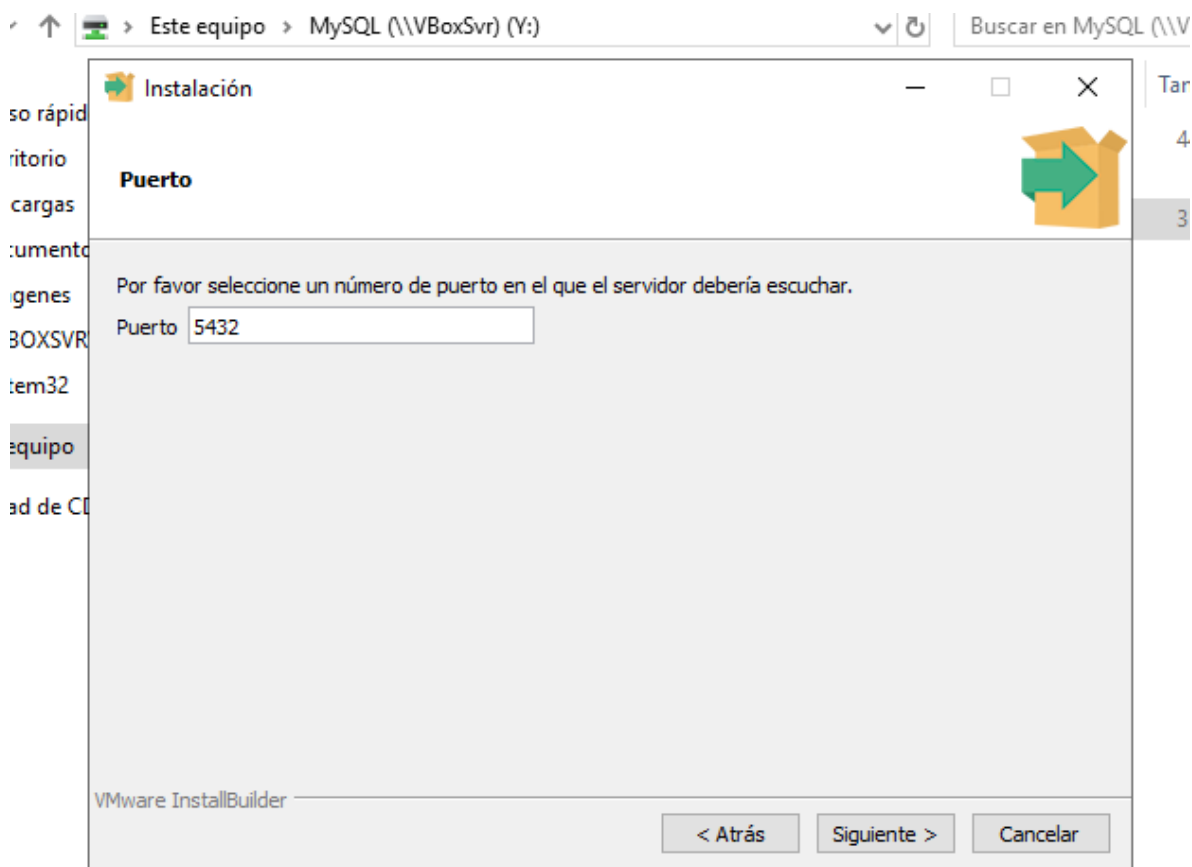
    Proto  Dirección local      Dirección remota      Estado
    TCP    192.168.207.22:7680   10.150.2.203:59714    TIME_WAIT
    TCP    192.168.207.22:51085  20.42.65.84:https     TIME_WAIT
    TCP    192.168.207.22:51086  52.109.20.80:https     TIME_WAIT
    TCP    192.168.207.22:60519  20.10.31.115:https     ESTABLISHED
    TCP    192.168.207.22:60526  20.10.31.115:https     ESTABLISHED

C:\Users\Jaime>
```

Instalamos el PostgreSQL

Contraseña admin123

Puerto 5432






Instalación



### Opciones Avanzadas



Seleccione la configuración regional a ser usada por el nuevo clúster de base de datos.

Configuración Regional [Configuración Regional por defec 

VMware InstallBuilder

< Atrás

Siguiente >

Cancelar

**preinstall.summary**



The following settings will be used for the installation::

```
summary.installation.directory: C:\Program Files\PostgreSQL\15
summary.server.installation.directory: C:\Program Files\PostgreSQL\15
summary.data.directory: C:\Program Files\PostgreSQL\15\data
summary.database.port: 5432
summary.database.superuser: postgres
summary.serviceaccount: NT AUTHORITY\NetworkService
summary.databaseservice: postgresql-x64-15
summary.dt.installation.directory: C:\Program Files\PostgreSQL\15
summary.pgadmin.installation.directory: C:\Program Files\PostgreSQL\15\pgAdmin 4
summary.sbp.installation.directory: C:\Program Files\PostgreSQL\15
summary.installation.logfile: C:\Users\Administrador\AppData\Local\Temp\install-postgresql.log
```

VMware InstallBuilder

< Atrás

Siguiente >

Cancelar

**Listo para Instalar**



El programa está listo para iniciar la instalación de PostgreSQL en su ordenador.

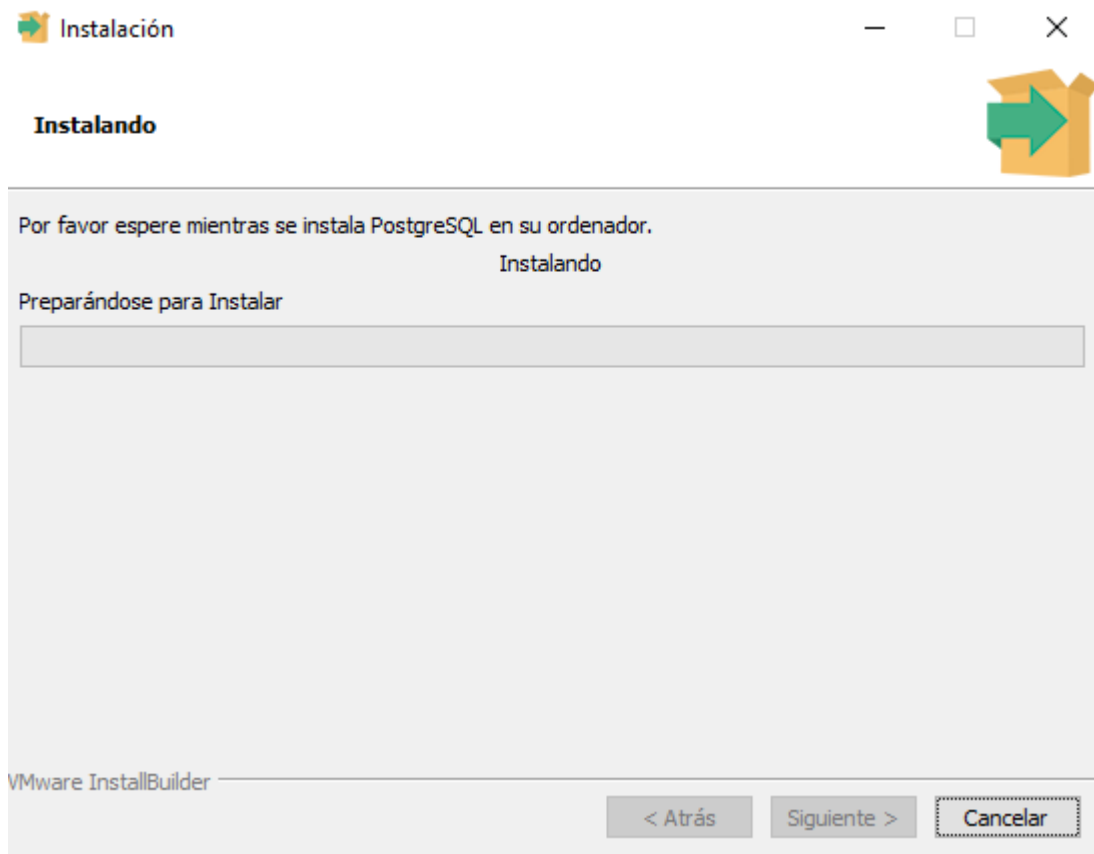
VMware InstallBuilder

< Atrás

Siguiente >

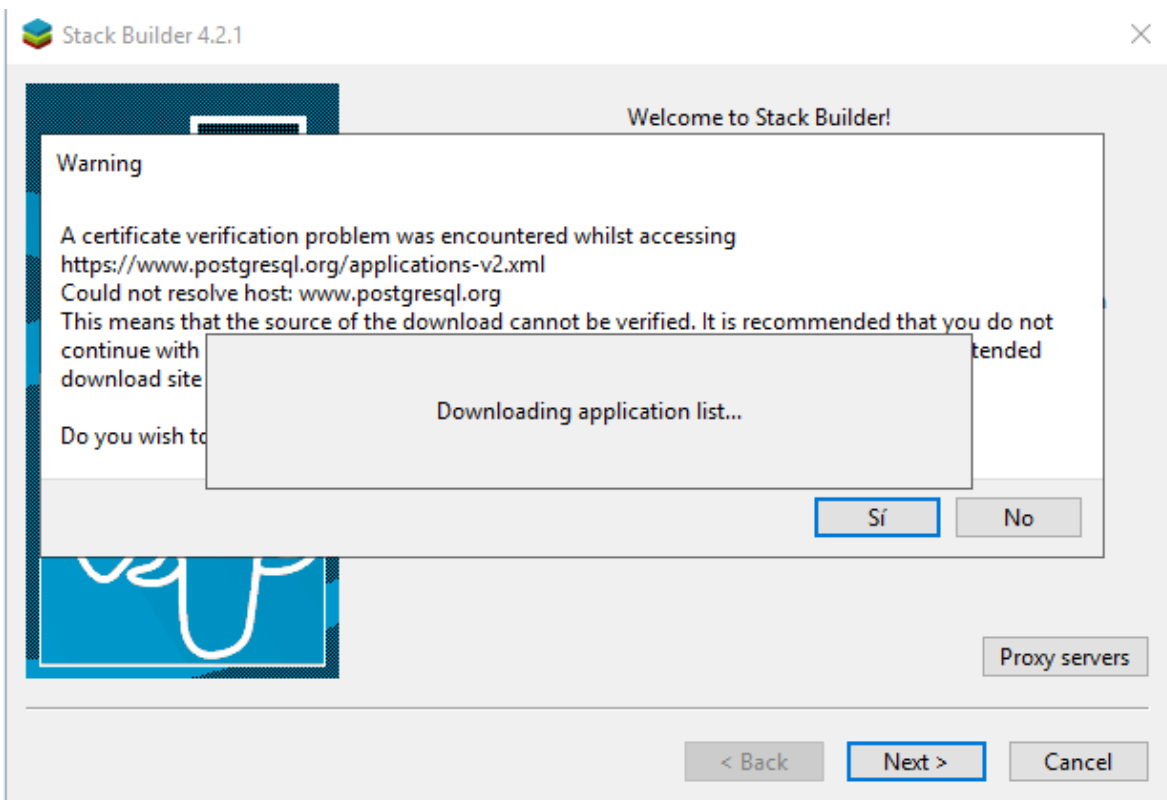
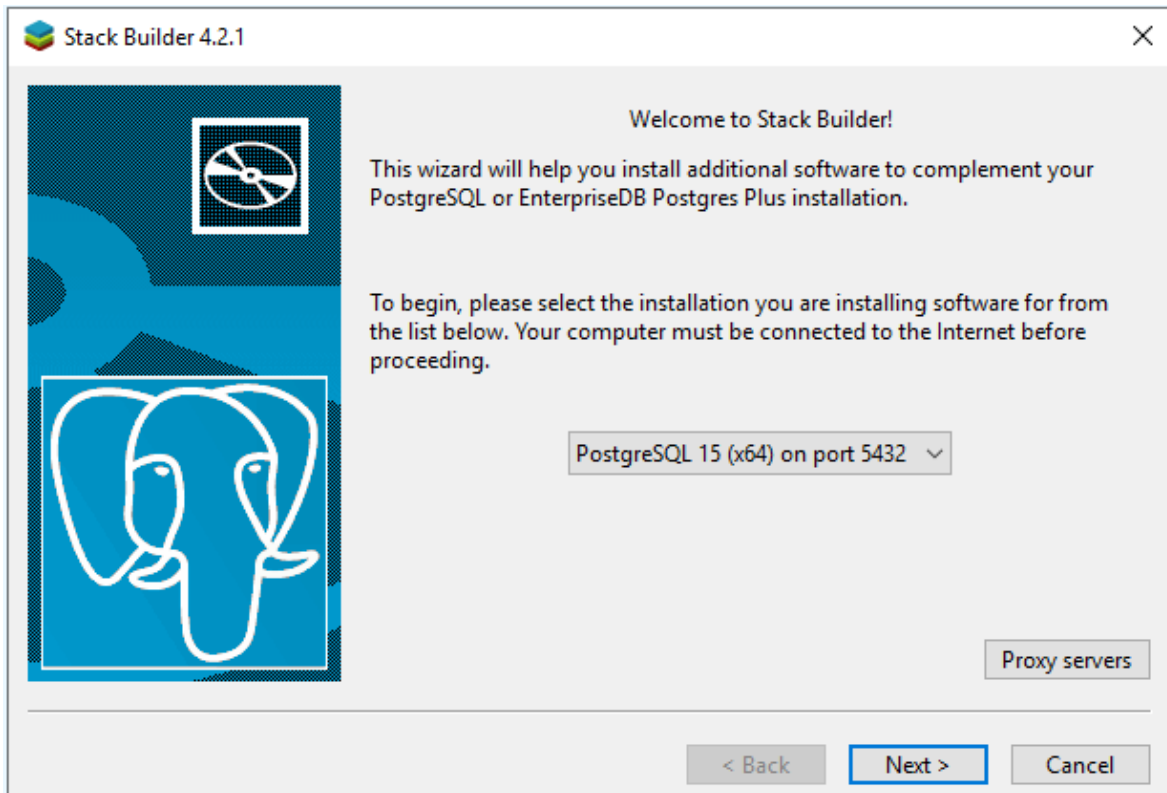
Cancelar



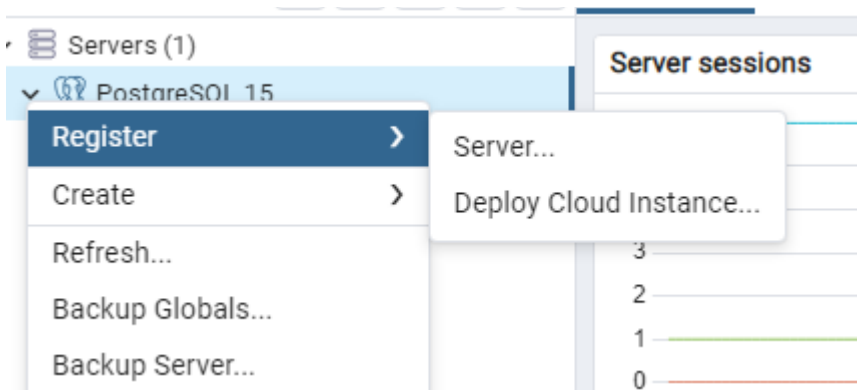
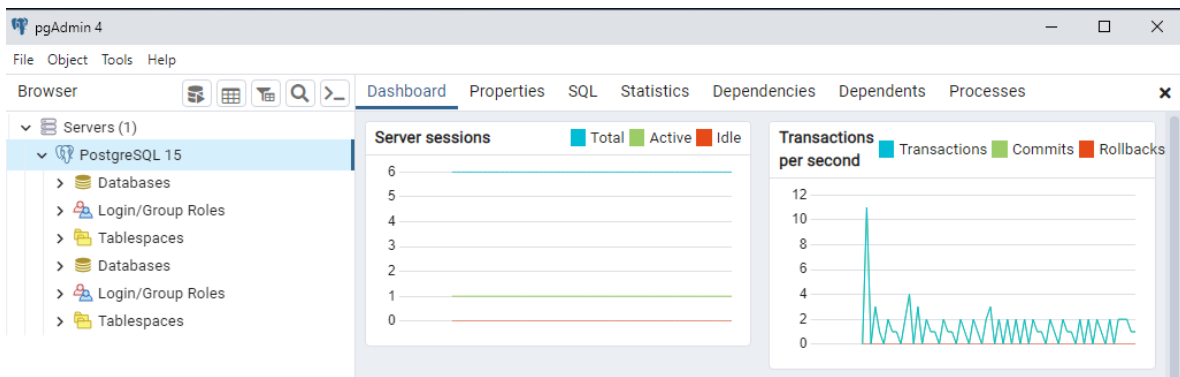


No descargamos el StackBuilder y finalizamos

Abrimos esta aplicación



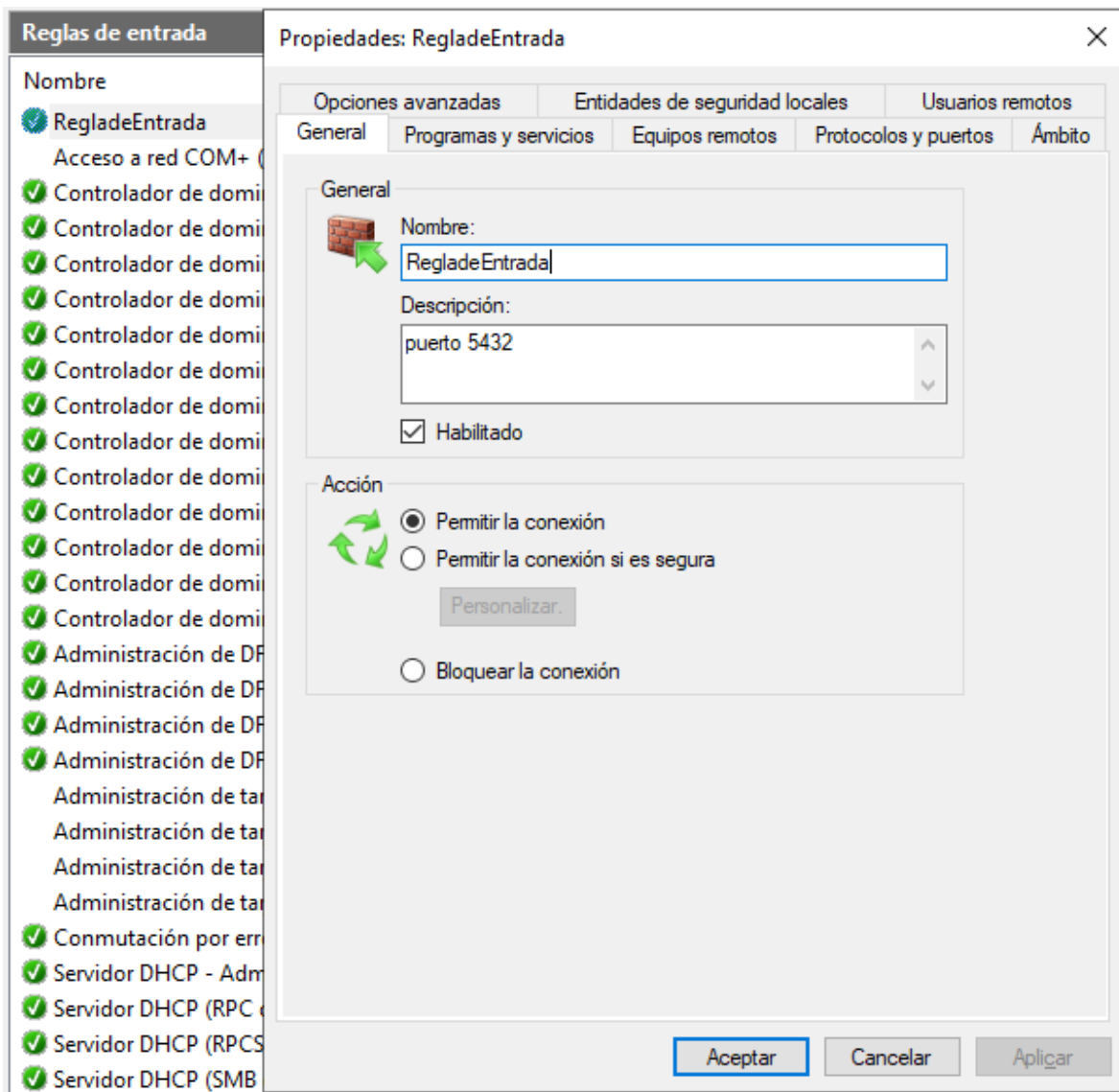
Abrimos e ingresamos las contraseñas



Creamos reglas de entrada y salida para el puerto 5432 y para verificar

```
ca. Administrador: Símbolo del sistema
TCP [fe80::841a:fa22:131d:e617%5]:49751 Jaime:49668 ESTABLISHED
C:\Users\Administrador>netstat -a -n -t
Conexiones activas
Proto Dirección local Dirección remota Estado
Estado de descarga
TCP 0.0.0.0:88 0.0.0.0:0 LISTENING EnHost
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING EnHost
TCP 0.0.0.0:389 0.0.0.0:0 LISTENING EnHost
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING EnHost
TCP 0.0.0.0:464 0.0.0.0:0 LISTENING EnHost
TCP 0.0.0.0:593 0.0.0.0:0 LISTENING EnHost
TCP 0.0.0.0:636 0.0.0.0:0 LISTENING EnHost
TCP 0.0.0.0:3268 0.0.0.0:0 LISTENING EnHost
TCP 0.0.0.0:3269 0.0.0.0:0 LISTENING EnHost
TCP 0.0.0.0:3389 0.0.0.0:0 LISTENING EnHost
TCP 0.0.0.0:5357 0.0.0.0:0 LISTENING EnHost
TCP 0.0.0.0:5432 0.0.0.0:0 LISTENING EnHost
TCP 0.0.0.0:5985 0.0.0.0:0 LISTENING EnHost
TCP 0.0.0.0:9389 0.0.0.0:0 LISTENING EnHost
TCP 0.0.0.0:47001 0.0.0.0:0 LISTENING EnHost
TCP 0.0.0.0:49664 0.0.0.0:0 LISTENING EnHost
TCP 0.0.0.0:49665 0.0.0.0:0 LISTENING EnHost
TCP 0.0.0.0:49666 0.0.0.0:0 LISTENING EnHost
```

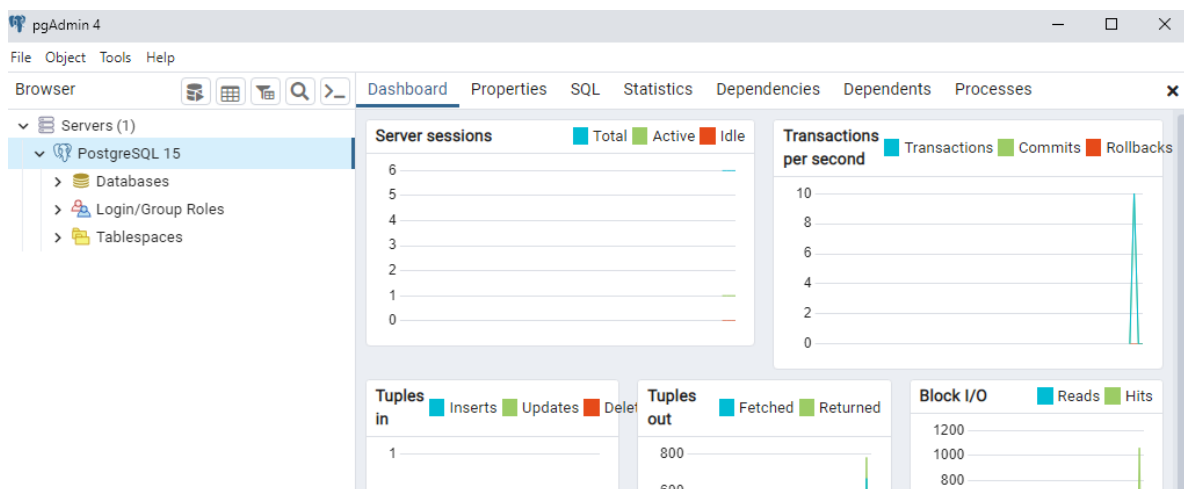
Creamos las reglas de entrada y salida del puerto que utiliza la BD



Abrimos la BD



Termina de abrir




Ahora bloqueamos la conexión

Propiedades: RegladeEntrada



Opciones avanzadas	Entidades de seguridad locales	Usuarios remotos
General	Programas y servicios	Equipos remotos
Protocolos y puertos	Ámbito	


General

 Nombre:

Descripción:

☒ Habilitado

Acción

 ☐ Permitir la conexión

☐ Permitir la conexión si es segura

☒ Bloquear la conexión

Creamos un server

Register - Server

General

Connection

SSL

SSH Tunnel

Advanced

Name

server2

Server group

Servers

Background

Foreground

Connect now?

Comments

i

?

Close

Reset

Save



pg\_hba.conf: Bloc de notas

Archivo Edición Formato Ver Ayuda

```
# Put your actual configuration here
# -----
#
# If you want to allow non-local connections, you need to add more
# "host" records. In that case you will also need to make PostgreSQL
# listen on a non-local interface via the listen_addresses
# configuration parameter, or via the -i or -h command line switches.


# TYPE DATABASE USER ADDRESS METHOD

# "local" is for Unix domain socket connections only
local all all scram-sha-256
# IPv4 local connections:
host all all 127.0.0.1/32 scram-sha-256
# IPv6 local connections:
host all all ::1/128 scram-sha-256
# Allow replication connections from localhost, by a user with the
# replication privilege.
local replication all scram-sha-256
host replication all 127.0.0.1/32 scram-sha-256
host replication all ::1/128 scram-sha-256
host all all 192.168.1.16/24 md5
```

Windows (CRLF) Línea 95, columna 1 100%

postgresql: Bloc de notas

Archivo Edición Formato Ver Ayuda

```
# - Authentication -

#authentication_timeout = 1min # 1s-600s
#password_encryption = md5 # scram-sha-256 or md5
#db_user_namespace = off

# GSSAPI using Kerberos
#krb_server_keyfile = 'FILE:${sysconfdir}/krb5.keytab'
#krb_caseins_users = off

# - SSL -

#ssl = off
#ssl_ca_file = ''
#ssl_cert_file = 'server.crt'
#ssl_crl_file = ''
#ssl_crl_dir = ''
#ssl_key_file = 'server.key'
#ssl_ciphers = 'HIGH:MEDIUM:+3DES:!aNULL' # allowed SSL ciphers
#ssl_prefer_server_ciphers = on
#ssl_ecdh_curve = 'prime256v1'
#ssl_min_protocol_version = 'TLSv1.2'
#ssl_max_protocol_version = ''
#ssl_dh_params_file = ''
```

Windows (CRLF) Línea 97, columna 25 100%

## Register - Server



General Connection SSL SSH Tunnel Advanced

Host  
name/addresses

localhost

Port

5432

Maintenance  
database

postgres

Username

postgres

Kerberos  
authentication?



Password

.....

Save  
password?



Role

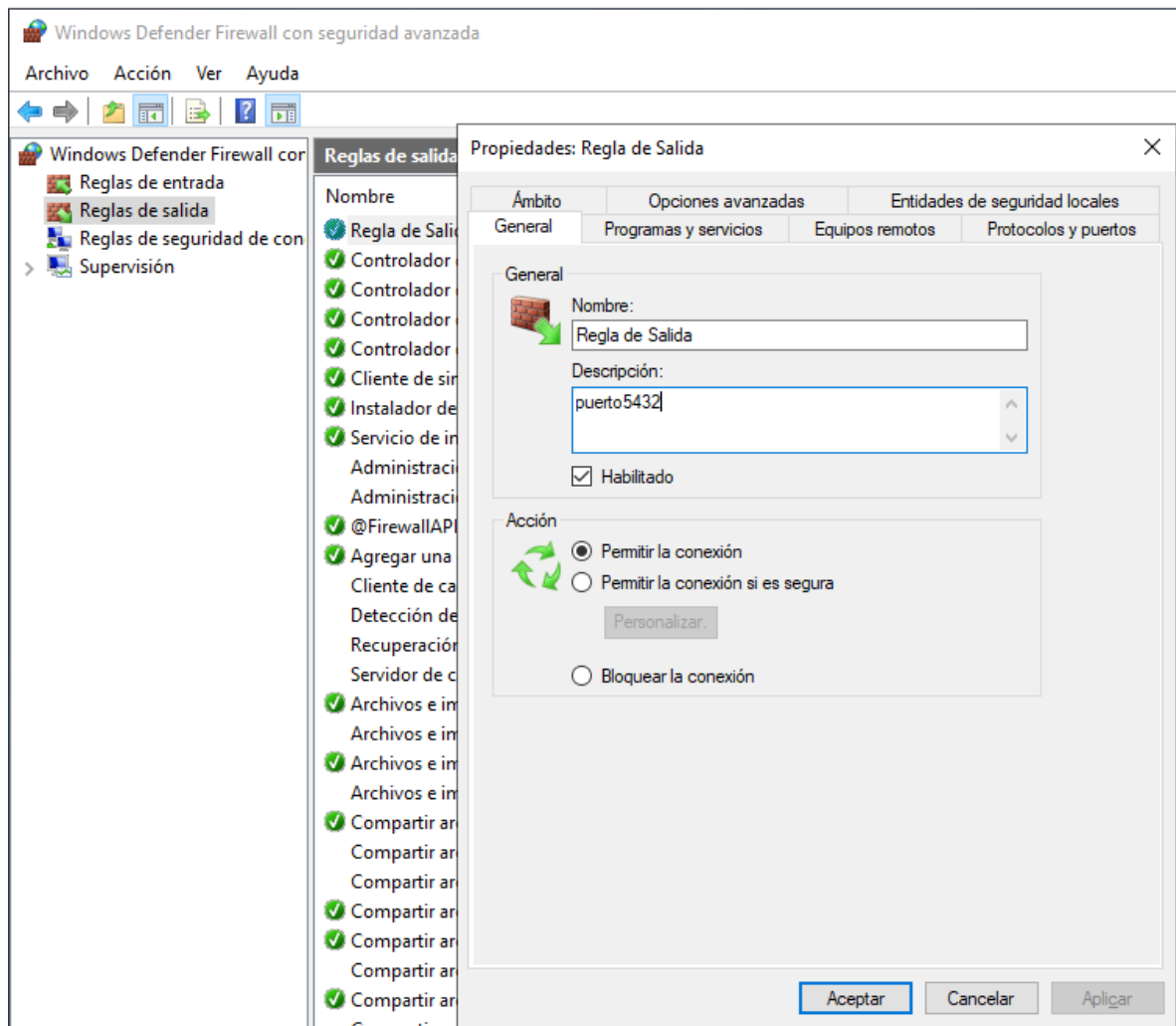
Service



✕ Close

↺ Reset

💾 Save



En el cliente ingresado al postgresql

FileObjectToolsHelp

Browser

▼

Servers (1)

▼

server1

>

Databases

>

Login/Group Roles

>

Tablespaces

Dashboard

Properties

SQL

Server sessions

6

5

4

3

2

1

0