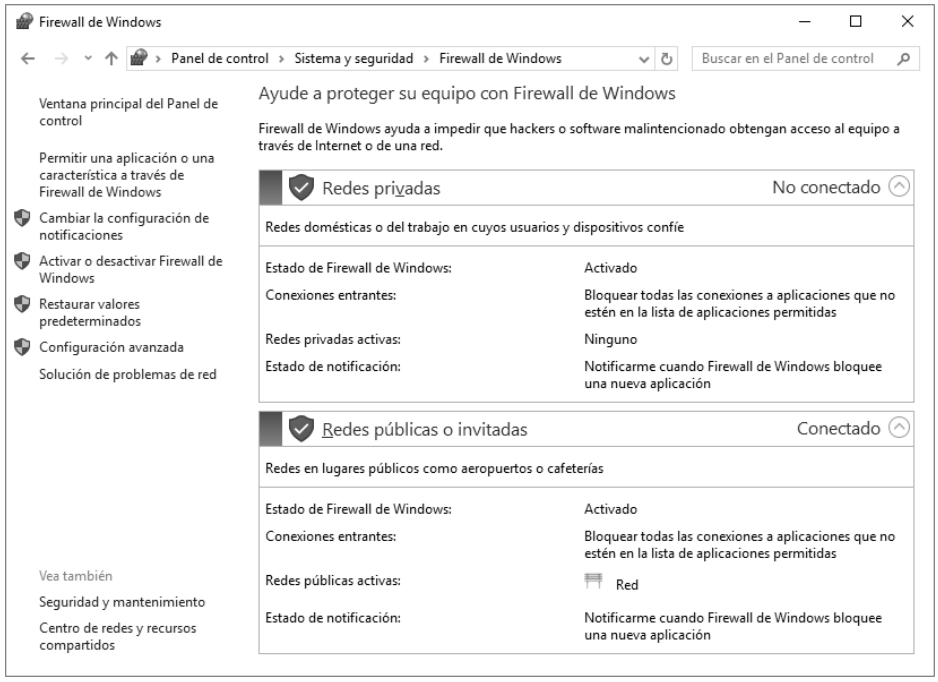
Capítulo 5
Seguridad y protección

1. La seguridad y el Firewall de Windows

Microsoft ha integrado un firewall con el Service Pack 2 de Windows XP. Si bien era más que bienvenido, rápidamente resultó poco fiable, pues era poco configurable. Desde Windows Vista, el firewall integrado de manera nativa se ha repensado por completo y ahora es posible definir de una forma mucho más específica los parámetros de protección. Veremos cmdlets que nos permitirán interactuar con el firewall.



Página de configuración del Firewall de Windows

He aquí la lista de los cmdlets estudiados:

– **`Get-NetFirewallProfile`**: recuperar la configuración del firewall (perfil).

– **`Set-NetFirewallProfile`**: modificar la configuración del firewall (perfil).

– **`New-NetFirewallRule`**: crear una nueva regla.

– **`Set-NetFirewallRule`**: modificar una regla existente.

1.1 Activar el Firewall de Windows

El Firewall de Windows está, por supuesto, habilitado por defecto tras una instalación no personalizada de Windows. Sin embargo, según la política de seguridad y las soluciones implementadas en la empresa, es posible desactivar el Firewall de Windows. En caso de tener que reactivarlo, he aquí cómo hacerlo mediante cmdlets de PowerShell.

La activación se lleva a cabo en dos etapas: la primera consiste en asegurarse de que el servicio de Firewall de Windows se ejecuta correctamente. Para ello, utilice **`Get-Service`**:

```
PS C:\Windows\system32> If ((Get-Service -Name MpsSvc).Status -eq
"Stopped")
>> {
>>     Set-Service -Name MpsSvc -StartupType Automatic
>>     Start-Service -Name MpsSvc
>> }
```

La segunda etapa consiste en activar el Firewall para los distintos perfiles deseados. Para ello, utilice **`Set-NetFirewallProfile`**. Este cmdlet admite varios parámetros, pero veremos los correspondientes a la activación y desactivación.

Parámetro	Descripción
`-AllowInboundRules` <GpoBoolean>	Especifica al firewall que bloquee las conexiones entrantes.
`-Enabled` <GpoBoolean>	Activa o desactiva el Firewall de Windows con seguridad avanzada para el perfil especificado.
`-LogAllowed`	Indica si los paquetes autorizados deben escribirse en los logs o no.
`-LogBlocked`	Indica si los paquetes bloqueados deben escribirse en los logs o no.

Parámetro	Descripción
-LogFileName <String>	Indica la ruta de acceso al archivo para escribir los logs.
-LogMaxSizeKilobytes	Especifica el tamaño máximo del archivo de log (en kilobytes).
-Name <String[]>	Especifica uno o varios nombres de perfil de firewall para modificar.
-NotifyOnListen <GpoBoolean>	Autoriza la notificación.

Ejemplo: activación del Firewall de Windows para todos los perfiles

```
PS C:\Windows\system32> Set-NetFirewallProfile -Name * -Enabled True
```

Existen tres perfiles (tipos de red) en el Firewall de Windows:

– **Public**: este perfil se utiliza en los lugares públicos, como cafés, hoteles, etc. Bloquea por defecto el conjunto de conexiones y la detección de redes.
– **Private**: este perfil se utiliza generalmente cuando se trabaja en una red local privada, como por ejemplo en casa.
– **Domain**: si el puesto de trabajo está asociado a un dominio de Windows Server, entonces el perfil Domain está activo automáticamente. Este perfil se utiliza cuando el equipo está conectado a la red de una empresa.

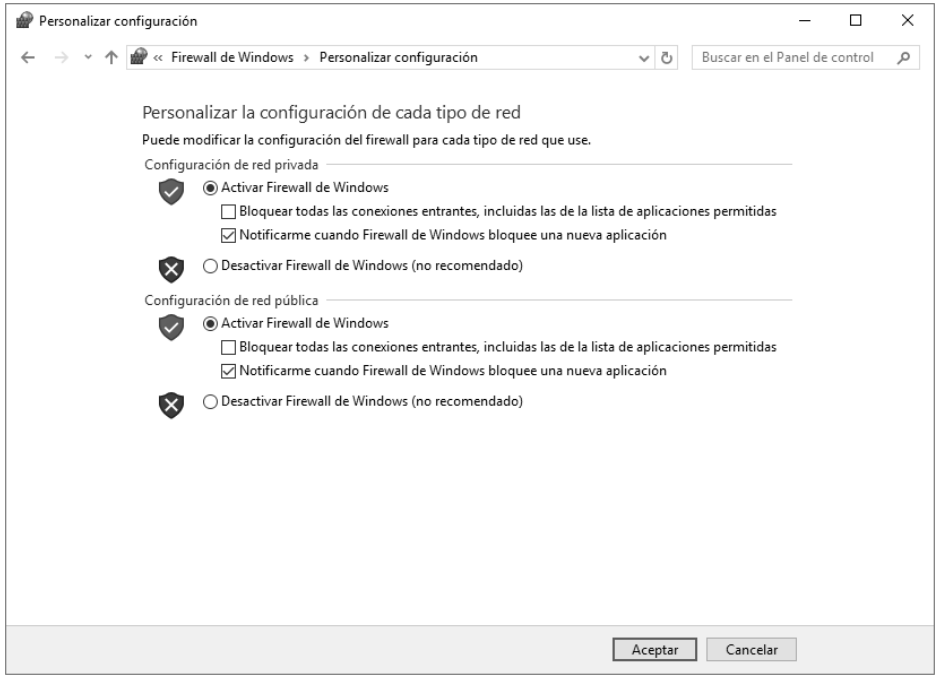
En cada perfil es posible, a su vez, jugar con un parámetro de seguridad en las conexiones entrantes, y un parámetro que gestiona las notificaciones.

El primer parámetro, **-AllowInboundRules**, permite definir qué comportamiento se desea en caso de producirse una conexión entrante. Puede tomar los siguientes valores:

Valor	Descripción
True	Bloquea todas las conexiones entrantes salvo aquellas que estén autorizadas mediante una regla de seguridad específica.
False	Bloquea absolutamente todas las conexiones entrantes.

El segundo parámetro, **`-NotifyOnListen`**, permite que se le notifique si el Firewall de Windows bloquea una nueva aplicación. Puede tomar los siguientes valores:

Valor	Descripción
`True`	Se muestra una notificación por pantalla en caso de que el Firewall de Windows bloquee una conexión y se le pide decidir si autoriza o no las futuras conexiones.
`False`	No se muestra ningún mensaje si el Firewall de Windows bloquea la conexión de alguna nueva aplicación.



Personalización de los parámetros del Firewall de Windows

Ejemplo: activación del firewall para un perfil con los parámetros

En el siguiente ejemplo, **Set-NetFirewallProfile** activa el firewall para el perfil Public, rechaza todas las conexiones entrantes y no se muestra ningún mensaje de advertencia cuando el firewall bloquea la conexión de alguna nueva aplicación.

```
PS C:\Windows\system32> Set-NetFirewallProfile -Name Public
-Enabled True -AllowInboundRules False -NotifyOnListen False
```

1.2 Desactivar el Firewall de Windows

Para desactivar el Firewall de Windows, basta simplemente con detener el servicio Firewall de Windows, cuyo efecto provoca que se permitan todas las conexiones de red entrantes y salientes del puesto de trabajo:

```
PS C:\Windows\system32> Stop-Service -Name MpsSvc
PS C:\Windows\system32> Set-Service -Name MpsSvc -StartupType
Disabled
```

Si simplemente desea desactivar el firewall para un perfil en particular, puede utilizar el cmdlet **Set-NetFirewallProfile**:

```
PS C:\Windows\system32> Set-NetFirewallProfile -Name
Public,Private -Enabled False
```

El ejemplo anterior desactiva el Firewall de Windows para los perfiles de conexión Public y Private.

1.3 Crear una nueva regla de seguridad

Pero la configuración del Firewall de Windows no se limita solamente a activarlo o desactivarlo según los perfiles de red. El modo avanzado del Firewall de Windows permite definir reglas de seguridad en función de las conexiones de red (protocolos, puertos) y también conexiones específicas de algún servicio o aplicación.