Configuración del Firewall de Windows y Windows Defender

Alfredo Abad

ISO-04-06a10_ConfigRed-WIN_Ext-FirewallWIN.pptx
http://www.flu-project.com/2014/06/el-firewall-de-windows-parte-1.html
http://www.flu-project.com/2014/06/el-firewall-de-windows-parte-2.html
http://www.flu-project.com/2014/07/el-firewall-de-windows-parte-3.html

UA: 22-jun-2019

1

Historia del firewall

- En Windows 2000 y XP el Firewall era muy rudimentario, con funcionalidades básicas de apertura y cierre de puertos, así cómo de unas pocas excepciones configuradas por defecto (escritorio remoto, compartición de impresoras, etc.)
  - Sin embargo, desde Windows Vista disponemos de un Firewall avanzado (más parecido a los firewall físicos)
- El nuevo cortafuegos de Windows dispone de la posibilidad de bloquear tanto conexiones entrantes como salientes
  - Algo muy necesario en la lucha contra los malware de tipo bot / troyanos reversos, que se conectan a un Panel de Control remoto (generalmente web)
- Actualmente, Windows ha integrado su firewall en Windows Defender

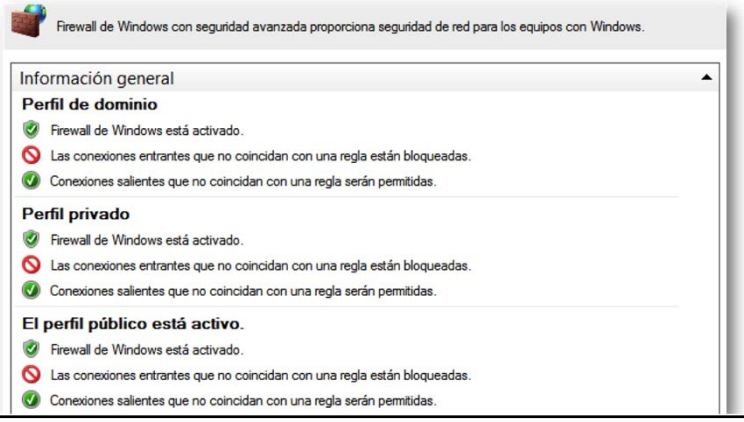
2

Podemos arrancarlo llamando al programa "wf.msc" como administrador

3

Cada interfaz se asociará a un perfil

- Desde el firewall podremos configurar varios tipos de perfiles:
  - Dominio: configurado para su uso en redes internas
  - Privado: destinado a un entorno privado (domicilio)
  - Público: configuración en redes desconocidas



4

Y la primera vez que se realice una conexión a una red, Windows nos preguntará el perfil que debe usar

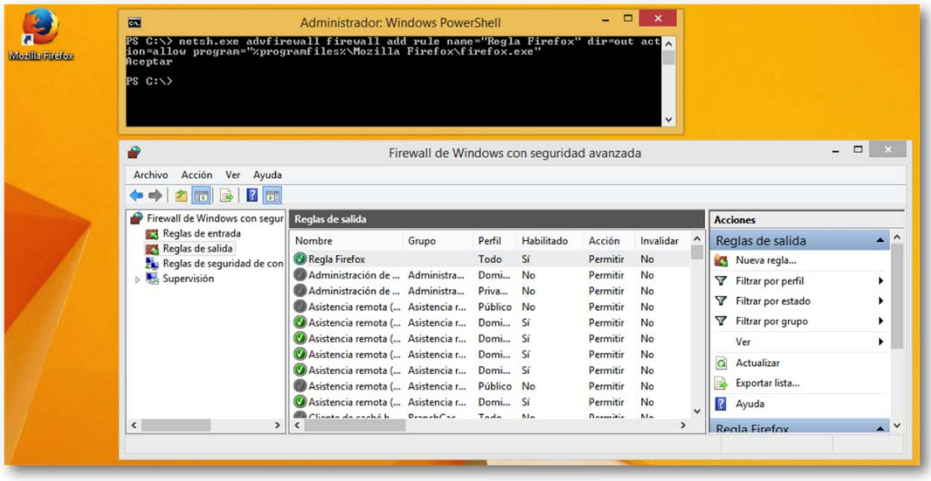
- En cada uno de estos perfiles se podrán configurar tanto conexiones entrantes como salientes. En ambas podremos filtrar:
  - Protocolos y puertos
  - Subredes
  - Usuarios
  - Equipos
  - Software, etc.
- Un punto interesante es la posibilidad de configurar el firewall de Windows para que únicamente salgan hacia Internet las aplicaciones que nos interesen.
- Será útil para protegernos frente a malware de tipo bot, downloaders y otro software malicioso, que se intente conectar "sin nuestro permiso" a paneles de control remoto, alojados en distintos puntos de Internet
- Lo malo, es que es bastante “engorroso” de configurar, porque se deben dar de alta una a una cada aplicación que deseamos que salga hacia Internet (lista blanca)

5

Uso de la consola para gestionar el firewall

- Podemos habilitar estas reglas desde consola. Por ejemplo, si quisiéramos que saliese hacia Internet el navegador “Firefox”, podríamos añadir la siguiente regla:
  - **netsh.exe advfirewall firewall add rule name=“Regla Firefox” dir=out action=allow program=“%programfiles%\Mozilla Firefox\firefox.exe”**
- Y para el caso contrario, evitar que salga hacia Internet, simplemente deberíamos cambiar "allow", por "deny“ (diapo siguiente)

6



7

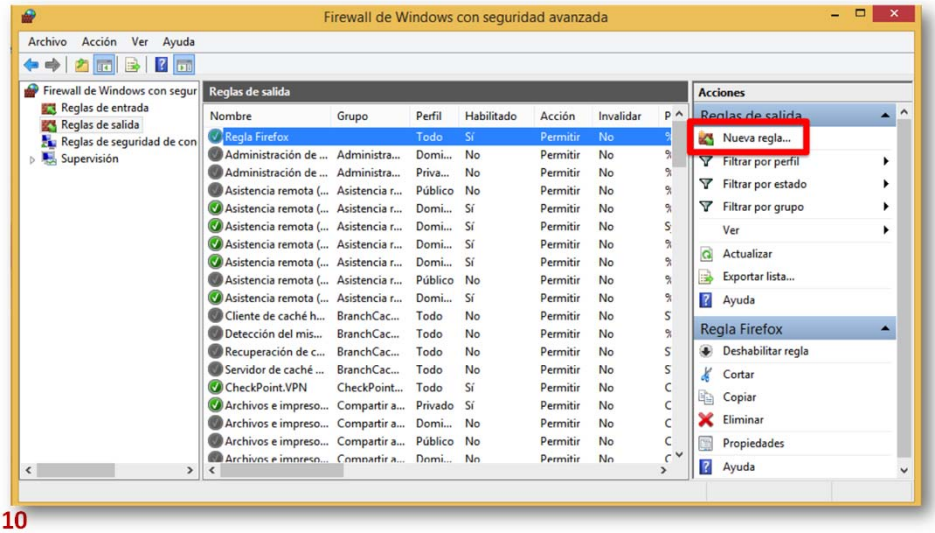
Windows Defender en W10

8

CREACIÓN DE REGLAS

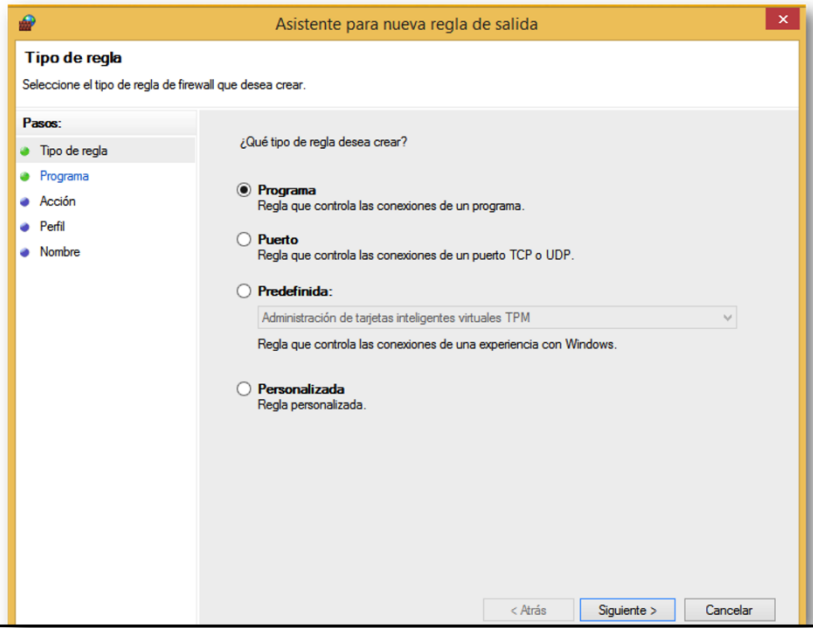
9

Creamos una nueva regla



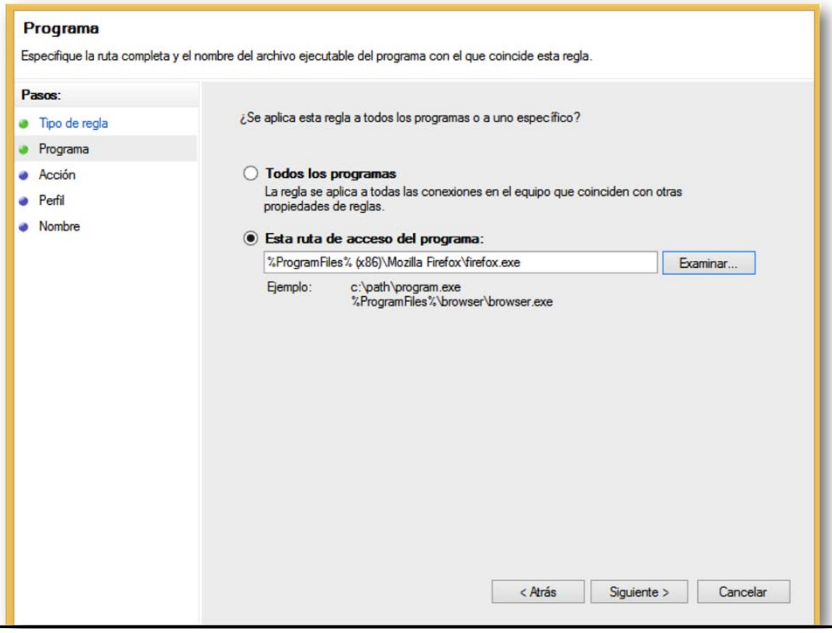
10

A continuación tendremos que indicar a qué objeto queremos bloquear (programa, puerto, etc.)



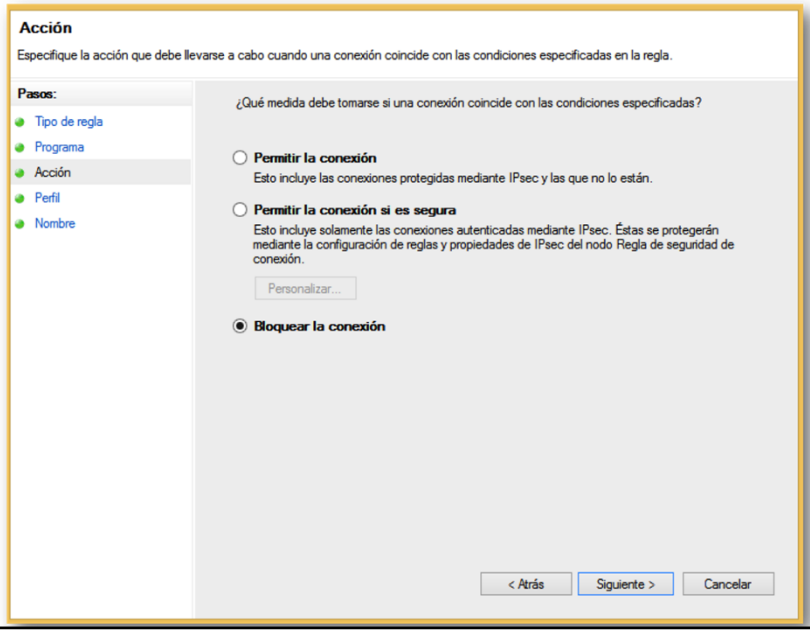
11

Seleccionamos el programa o los programas que queremos que se vean afectados por la presente regla



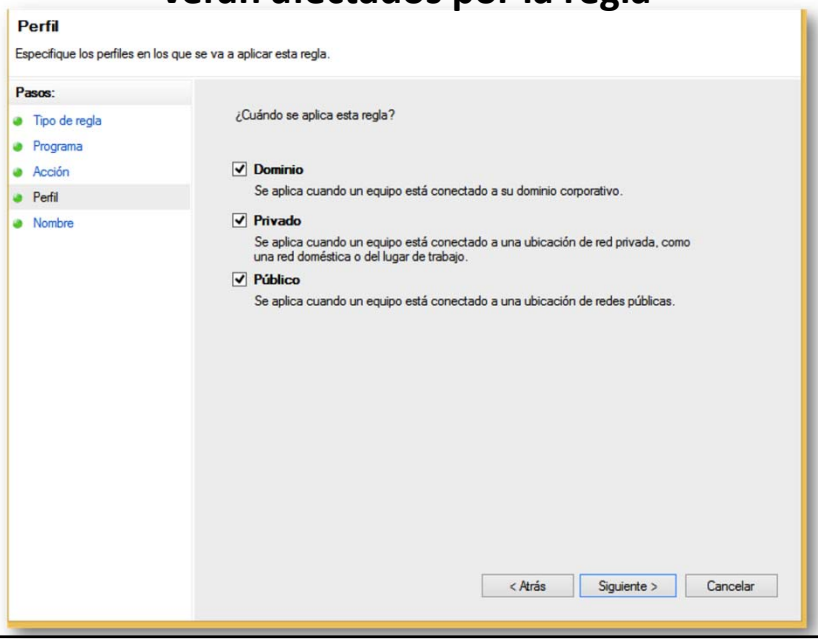
12

Seleccionamos la acción a tomar (permitir, bloquear, o permitir siempre y cuando la conexión sea segura)



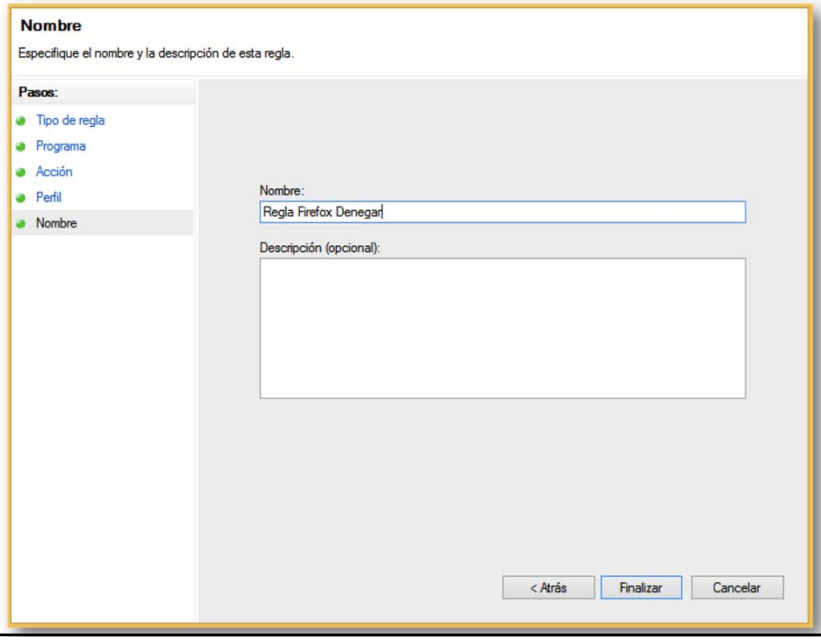
13

El penúltimo paso será indicar los perfiles que se verán afectados por la regla



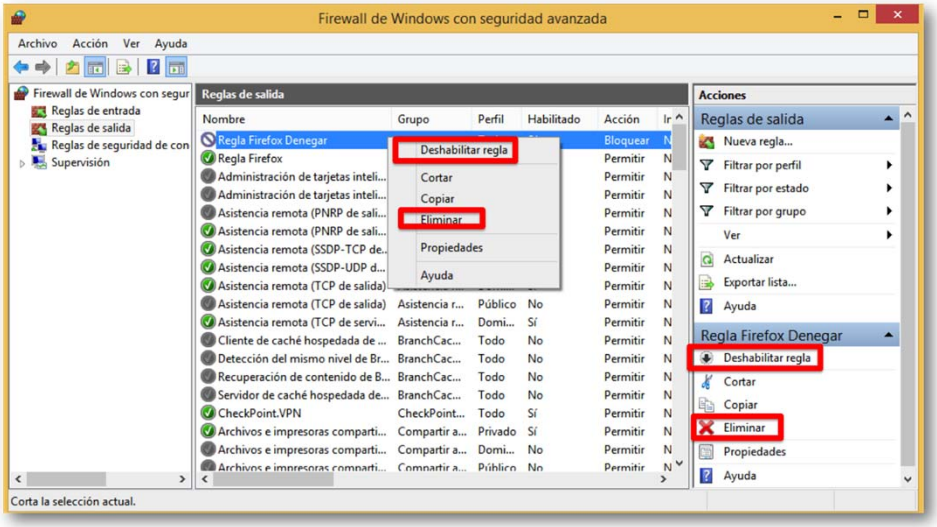
14

Finalmente le daremos un nombre y una descripción, para facilitar a los admins el trabajo, mientras gestionan esta y otras futuras reglas



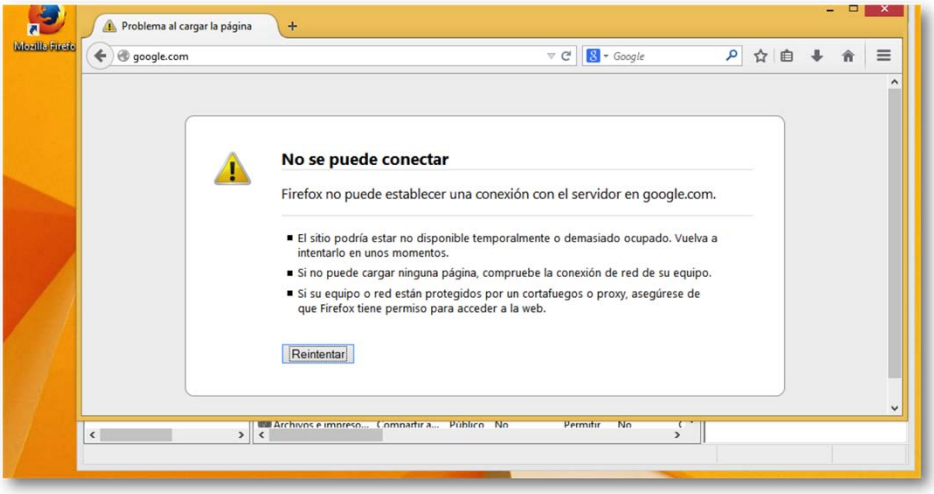
15

Una vez aplicada la regla, podremos deshabitar o eliminarla desde el menú de acciones, o pulsando con el botón derecho sobre la regla



16

Si todo ha ido correctamente, veremos si surte efecto o no la regla. En nuestro caso, bloquear el acceso a Internet del navegador Firefox

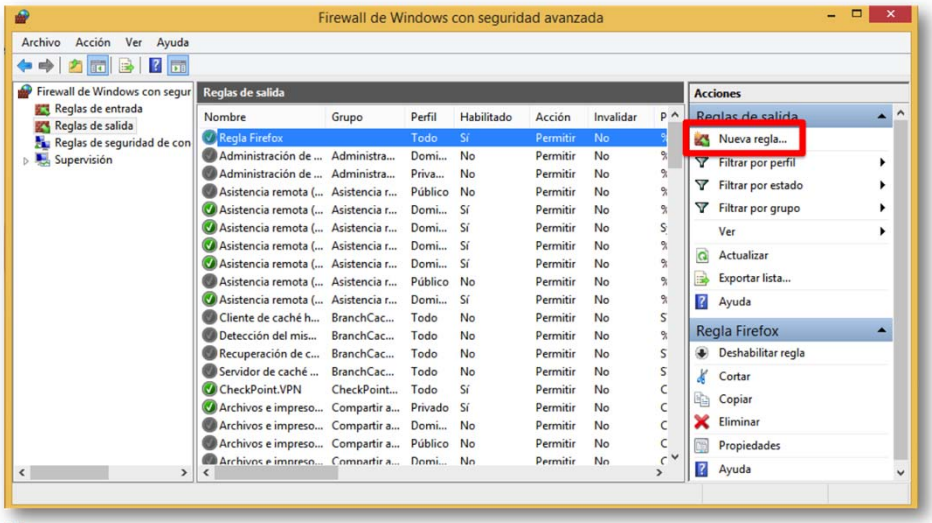


17

REGLAS PERSONALIZADAS

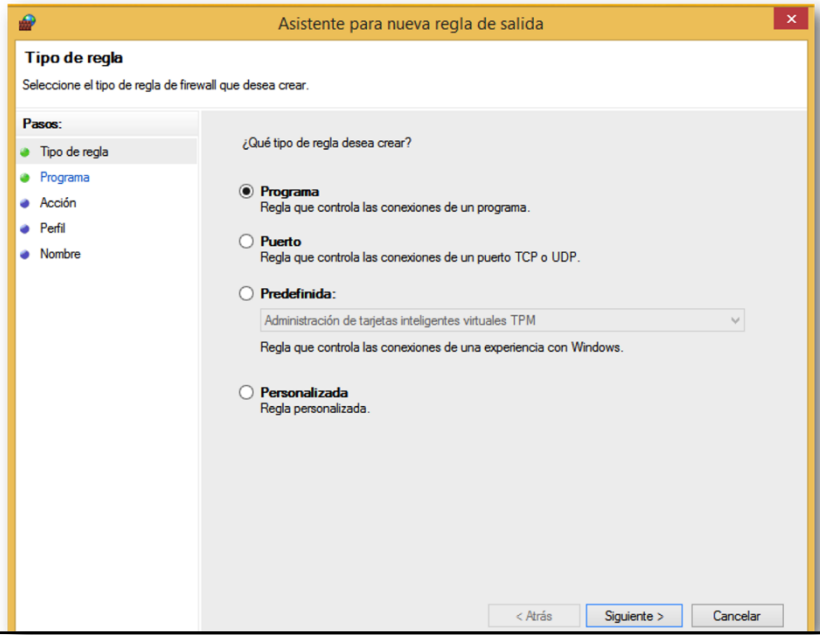
18

Desde esta pantalla podremos gestionar tanto reglas de entrada, como de salida



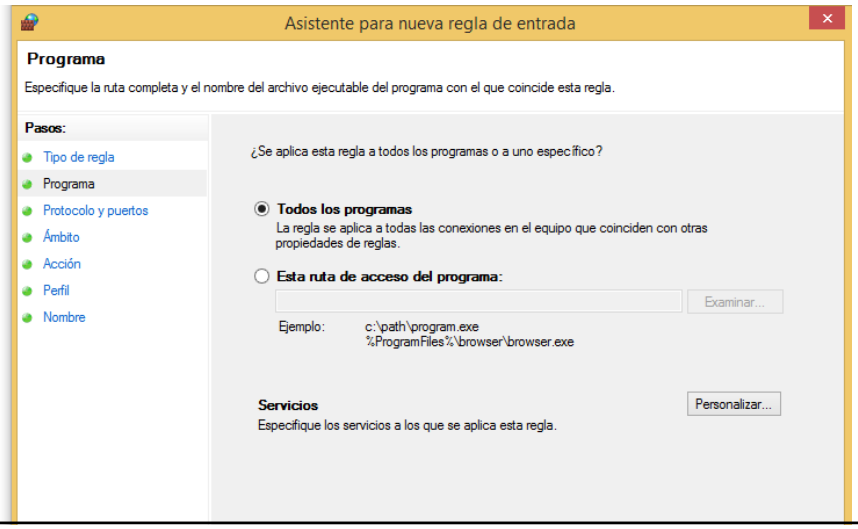
19

Una vez que pulsamos sobre la opción de creación de nuevas reglas, deberemos pulsar sobre "Personalizada“



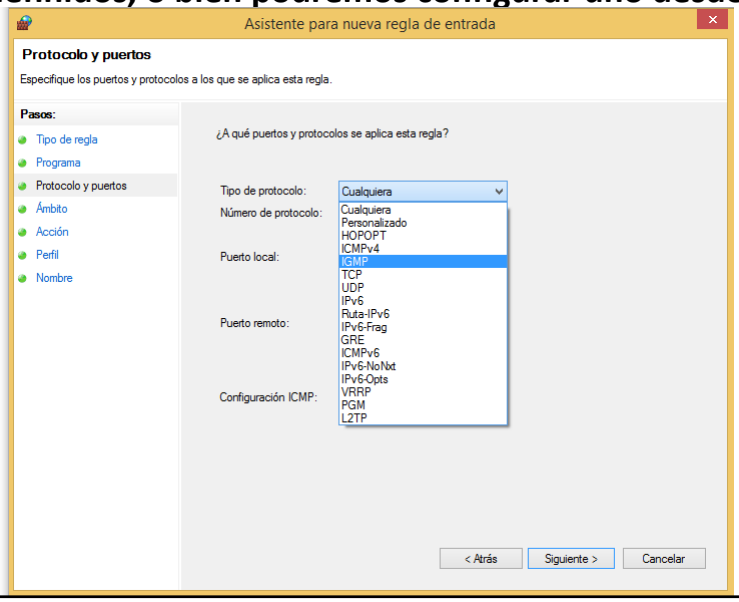
20

En este punto el asistente cambiará para mostrarnos todas las posibles configuraciones del Firewall. En el primer menú podremos gestionar los programas a los que afectará la regla que estamos diseñando

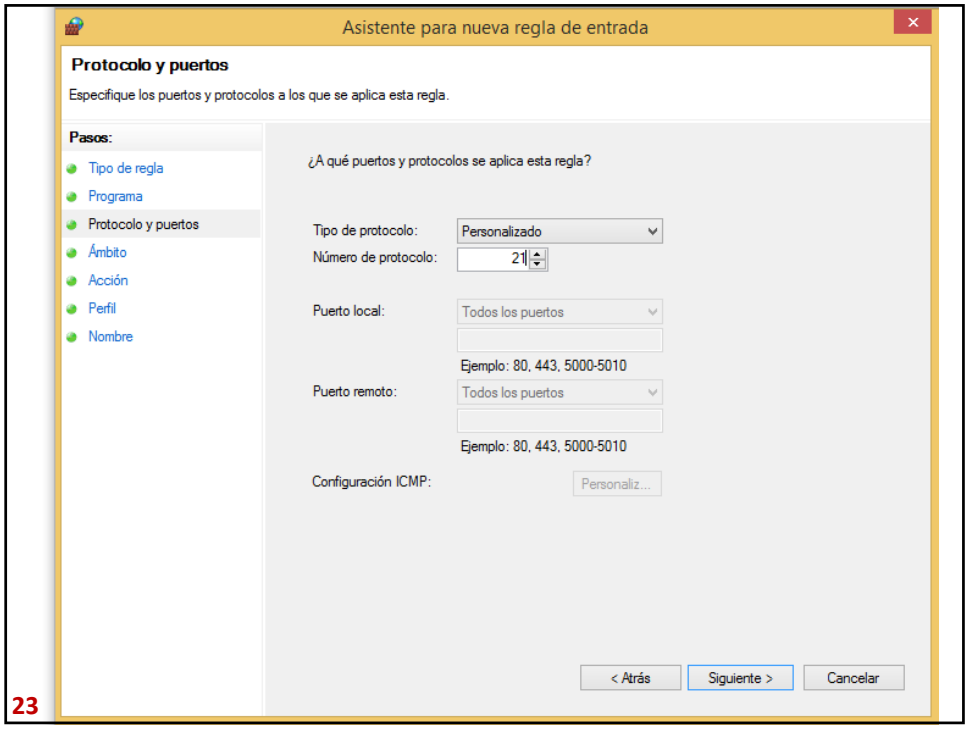


21

Podremos gestionar los protocolos que se verán afectados por la regla. Podemos seleccionar los protocolos que vienen predefinidos, o bien podremos configurar uno desde cero

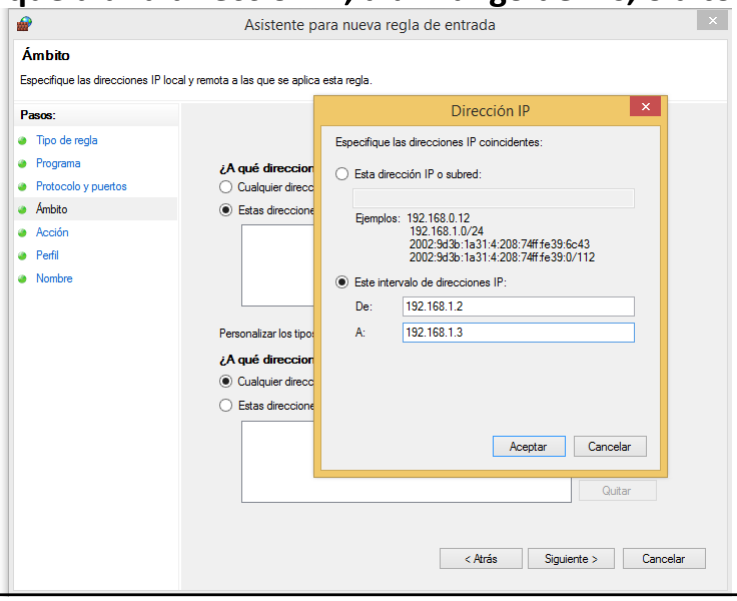


22



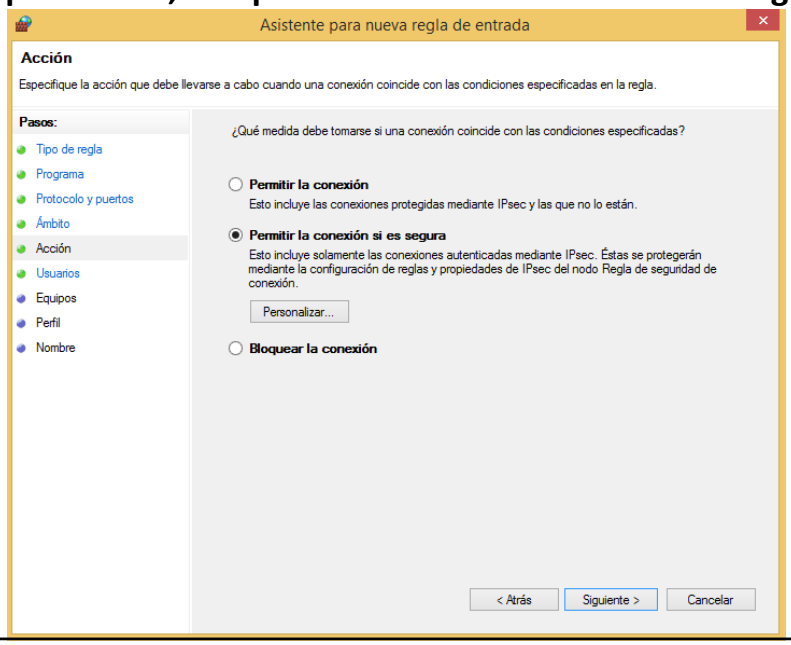
23

El siguiente paso será indicar las direcciones IP que se verán afectadas por la regla. Podremos filtrar para que solo se aplique a una dirección IP, a un rango de IPs, o a todas

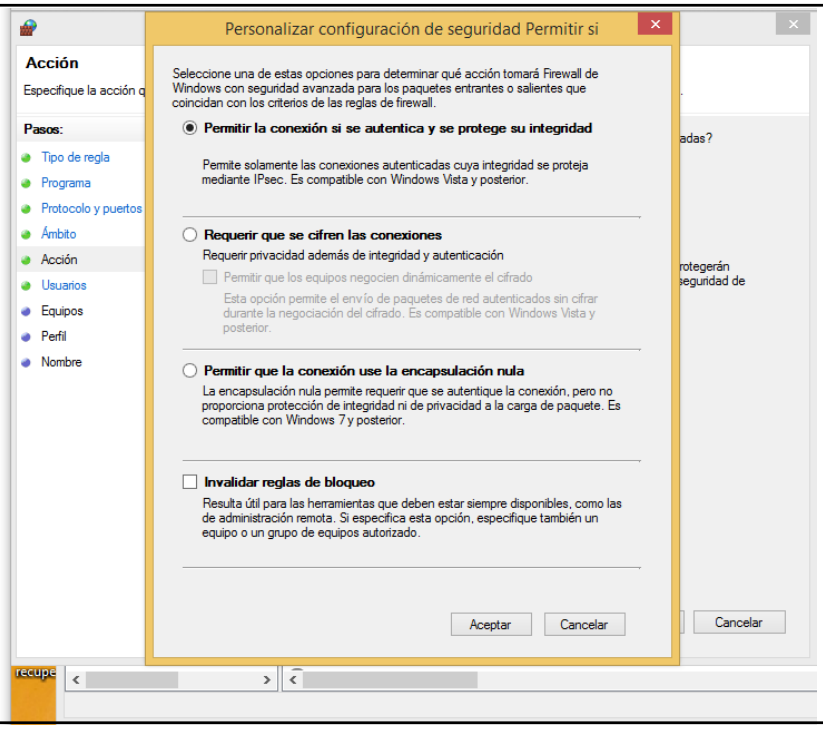


24

A continuación indicaremos si permitiremos la conexión, la bloquearemos, o la permitiremos únicamente si es segura

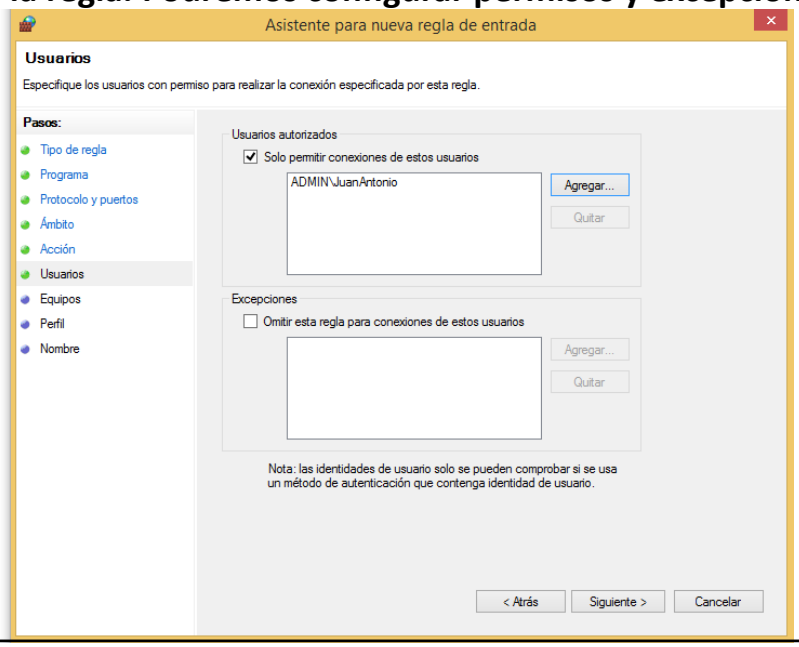


25



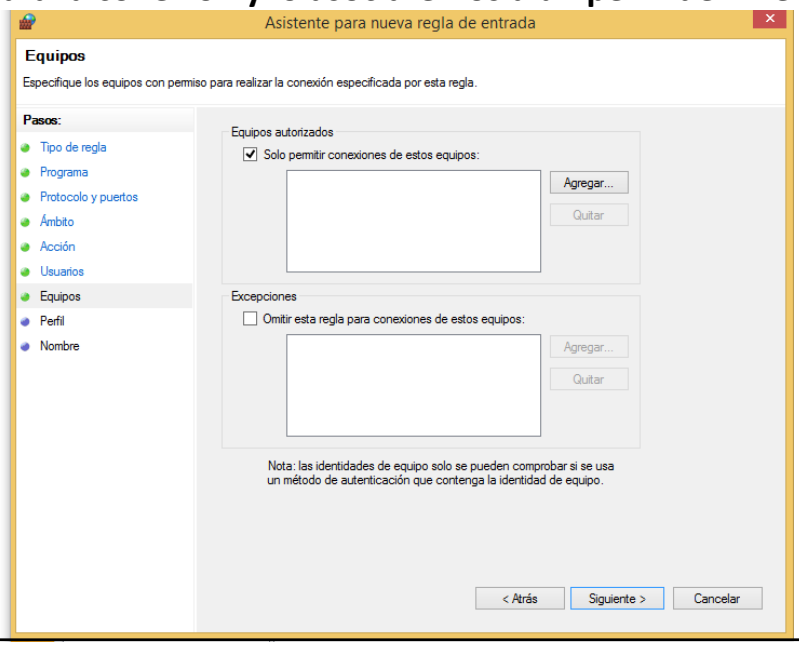
26

Después indicaremos los usuarios que se verán afectados por la regla. Podremos configurar permisos y excepciones



27

Y finalmente seleccionaremos los equipos a los que se aplicará la conexión y lo asociaremos a un perfil del Firewall



28

https://www.sysadmit.com/2018/03/windows-habilitar-ping-icmp.html

EJEMPLO:
HABILITAR PING (ICMP) EN WINDOWS

29

Por línea de comandos

Habilitar respuesta ICMP IPv4

```
netsh advfirewall firewall add rule name="Habilitar respuesta ICMP IPv4" protocol=icmpv4:8,any dir=in action=allow
```

Habilitar respuesta ICMP IPv6

```
netsh advfirewall firewall add rule name="Habilitar respuesta ICMP IPv6" protocol=icmpv6:8,any dir=in action=allow
```

Deshabilitar respuesta ICMP IPv4

```
netsh advfirewall firewall add rule name="Deshabilitar respuesta ICMP IPv4" protocol=icmpv4:8,any dir=in action=block
```

Deshabilitar respuesta ICMP IPv6

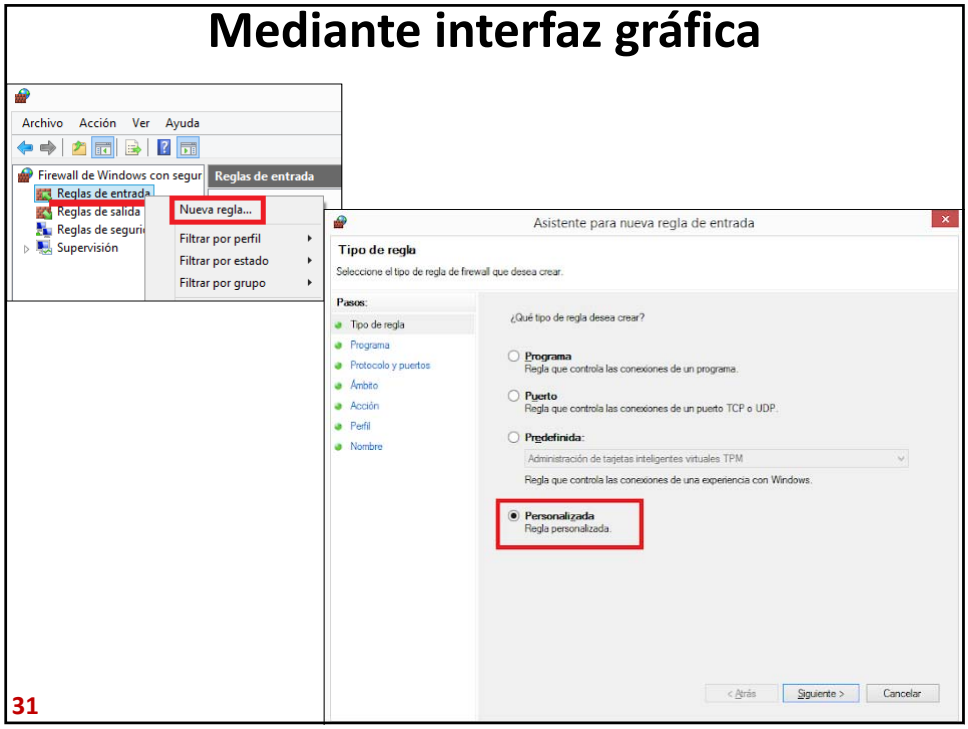
```
netsh advfirewall firewall add rule name="Deshabilitar respuesta ICMP IPv6" protocol=icmpv6:8,any dir=in action=block
```

Mostrar reglas firewall:

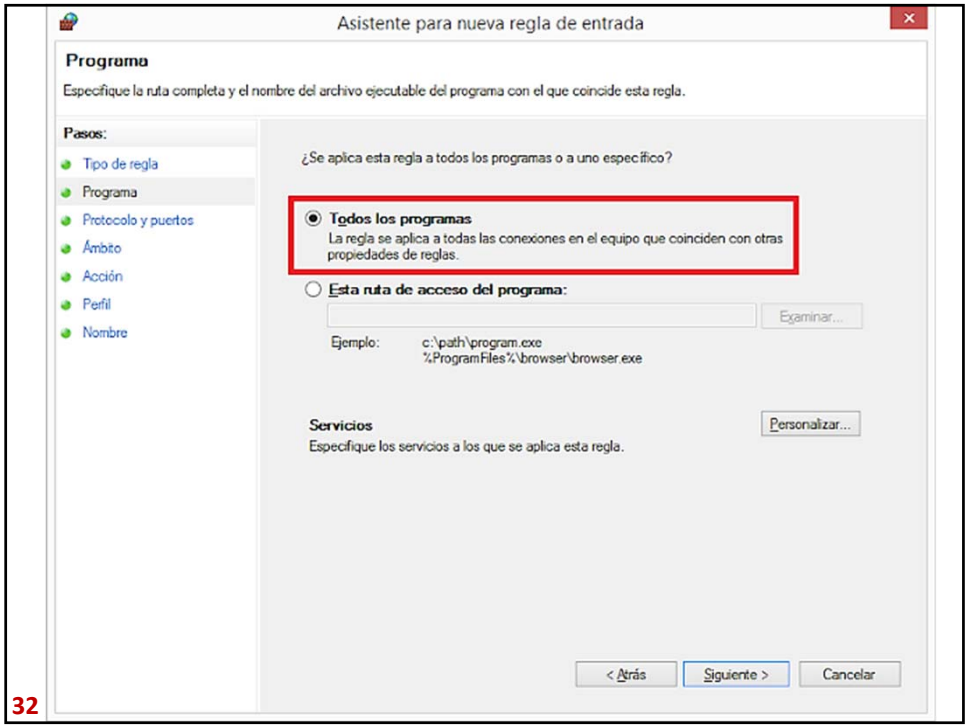
```
netsh advfirewall firewall show rule name=all
```

30

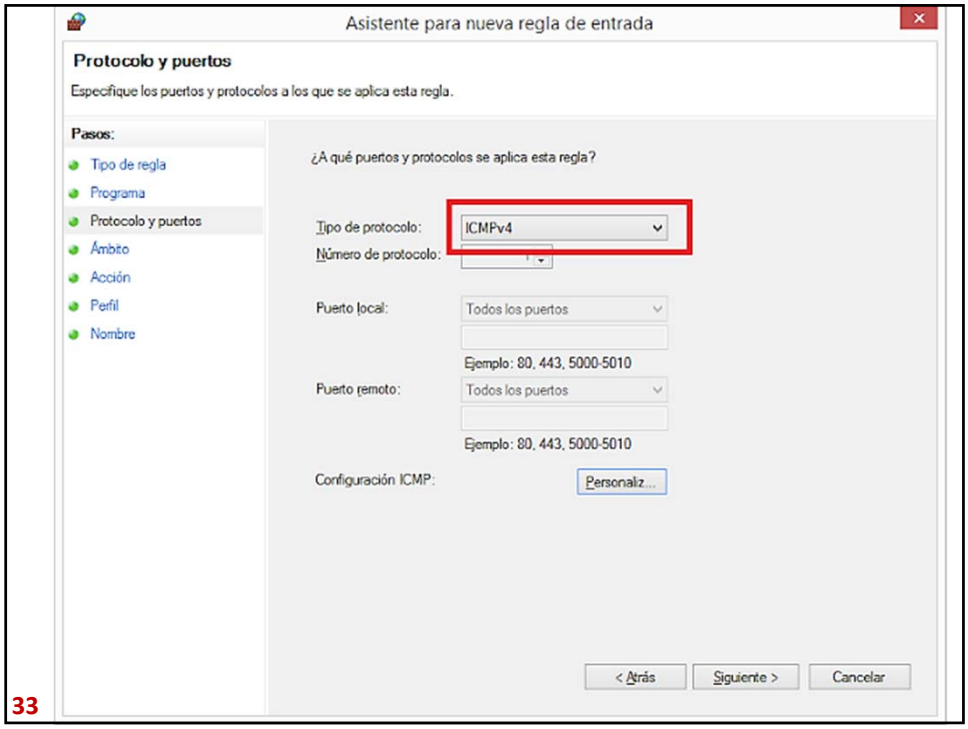
Mediante interfaz gráfica



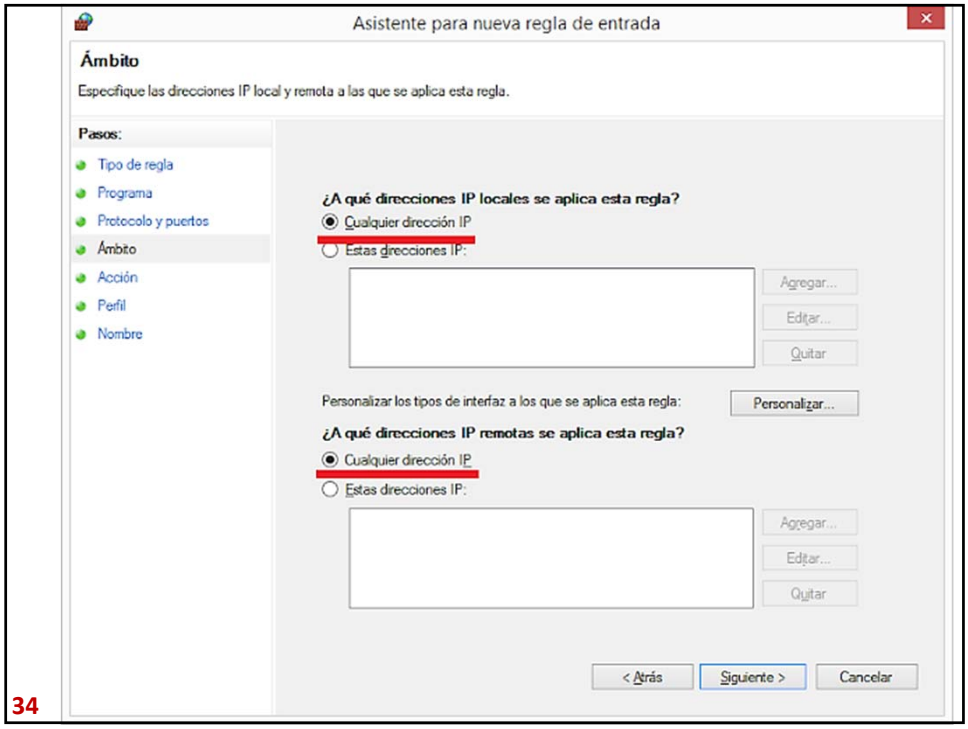
31



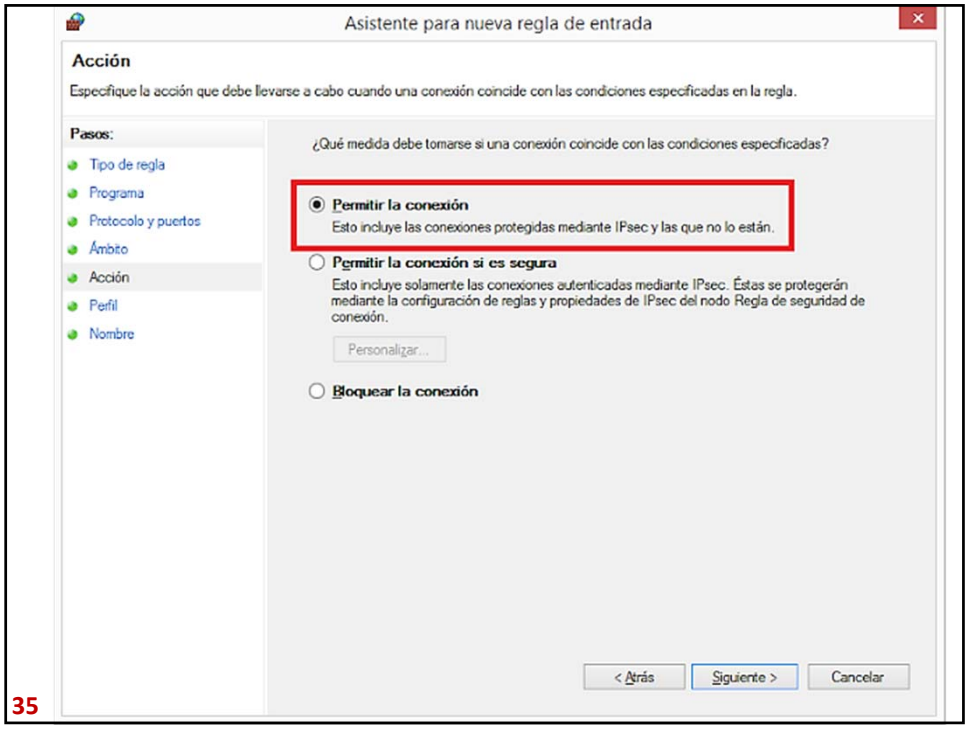
32

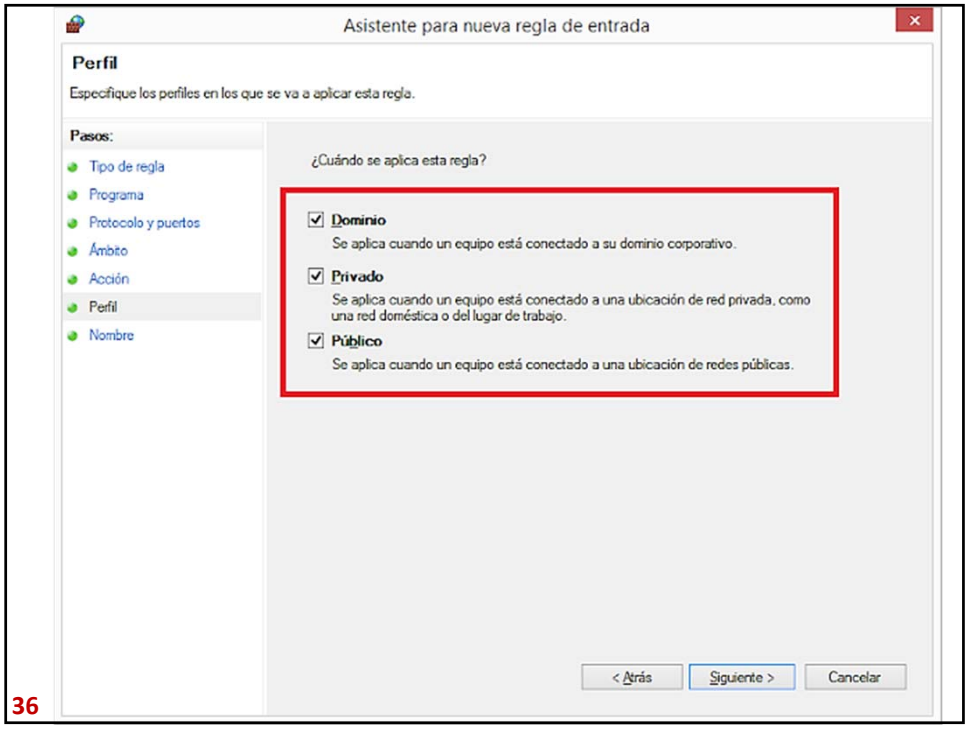

Asistente para nueva regla de entrada
Protocolo y puertos
Especifique los puertos y protocolos a los que se aplica esta regla.
Pasos:
Tipo de regla
Programa
Protocolo y puertos
Ámbito
Acción
Perfil
Nombre
¿A qué puertos y protocolos se aplica esta regla?
Tipo de protocolo:
ICMPv4
Número de protocolo:
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

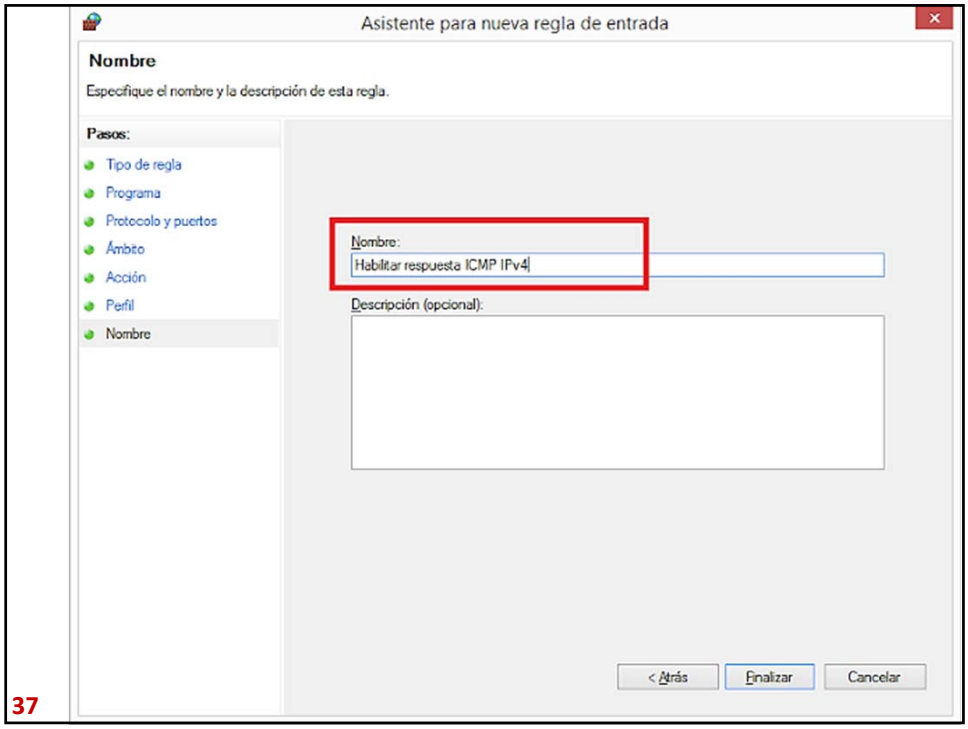
33


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

34


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.
Personalizar...
Bloquear la conexión
< Atrás
Siguiente >
Cancelar
35


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
36



37

2019_Cómo abrir o cerrar un puerto en Firewall Windows 10 - Solvetic.pdf

DOCUMENTO:
¿CÓMO ABRIR O CERRAR UN PUERTO DE FIREWALL EN WINDOWS 10?

38

2019_Telnet_ qué es y cómo activarlo en Windows 10.pdf

DOCUMENTO: ¿QUÉ ES TELNET Y CÓMO ACTIVARLO EN WINDOWS 10?

39

https://www.sysadmit.com/2016/03/linux-respuesta-ping-habilitar-o-deshabilitar.html

EJEMPLO: RESPUESTA PING (HABILITAR O DESHABILITAR EN LINUX)

40

En sistemas Linux, por defecto la respuesta a `ping` (protocolo ICMP - Internet Control Message Protocol) está habilitada a nivel de kernel.

Para modificar este comportamiento, tenemos varias formas:

1) Modificar los parámetros de carga del kernel:

Al cargar el kernel, se leen los parámetros indicados en el fichero `/etc/sysctl.conf`.

Especial cuidado en modificar de forma incorrecta el contenido de este fichero.

También se pueden modificar los parámetros en caliente modificando los ficheros situados en: `/proc/sys/`

Dentro de `/proc/sys/` encontraremos varios directorios, entre ellos el directorio `net/`, para configuraciones de red.

Modificar directamente `/proc/sys/` hará que los cambios sean temporales, es decir, se perderán los cambios al reiniciar el equipo.

Una buena práctica es primero modificar `/proc/sys/`, verificar si el comportamiento es el esperado y luego modificar `/etc/sysctl.conf` para configurar los cambios de forma permanente.

41

2) Configurar el firewall del equipo:

La otra forma que tenemos para bloquear la respuesta a ping, es configurar el firewall del equipo.

Con el firewall del equipo, podemos configurar reglas que descarten los paquetes ICMP entrantes, tanto para IPv4 como para IPv6.

Veamos como habilitar o deshabilitar la respuesta ICMP a nivel de kernel:

Configuración temporal:

Para habilitar que el ICMP sea ignorado:

```
echo 1> /proc/sys/net/ipv4/icmp_echo_ignore_all
```

Para deshabilitar que el ICMP sea ignorado:

```
echo 0> /proc/sys/net/ipv4/icmp_echo_ignore_all
```

Configuración permanente:

Editamos el fichero: `/etc/sysctl.conf`

Para habilitar que el ICMP sea ignorado:

42

Configuración temporal:

Para habilitar que el ICMP sea ignorado:

```
echo 1> /proc/sys/net/ipv4/icmp_echo_ignore_all
```

Para deshabilitar que el ICMP sea ignorado:

```
echo 0> /proc/sys/net/ipv4/icmp_echo_ignore_all
```

Configuración permanente:

Editamos el fichero: `/etc/sysctl.conf`

Para habilitar que el ICMP sea ignorado:

```
net.ipv4.icmp_echo_ignore_all=1
```

Para deshabilitar que el ICMP sea ignorado:

```
net.ipv4.icmp_echo_ignore_all=0
```

Otra forma de bloquear las respuestas ICMP es utilizando `iptables`:

Pata bloquear tráfico ICMP entrante sobre IPv4:

```
iptables -A INPUT -p icmp --icmp-type echo-request -j DROP
```

Pata bloquear tráfico ICMP entrante sobre IPv6:

```
iptables -A INPUT -p icmpv6 --icmp-type echo-request -j DROP
```

43

https://www.sysadmit.com/2018/05/windows-saber-si-el-ping-lo-bloquea-el-firewall.html

WINDOWS: SABER SI PING ES BLOQUEADO POR EL FIREWALL O NO HAY RESPUESTA PORQUE EL SISTEMA ESTÁ APAGADO O DESCONECTADO

44

Si no podemos acceder al firewall del equipo remoto y este está bloqueando el protocolo ICMP, con ping, no podemos saber si el equipo destino está encendido o apagado.

Si el equipo destino está en el mismo segmento de red y no hay ningún router entre medio, podemos utilizar la siguiente técnica:

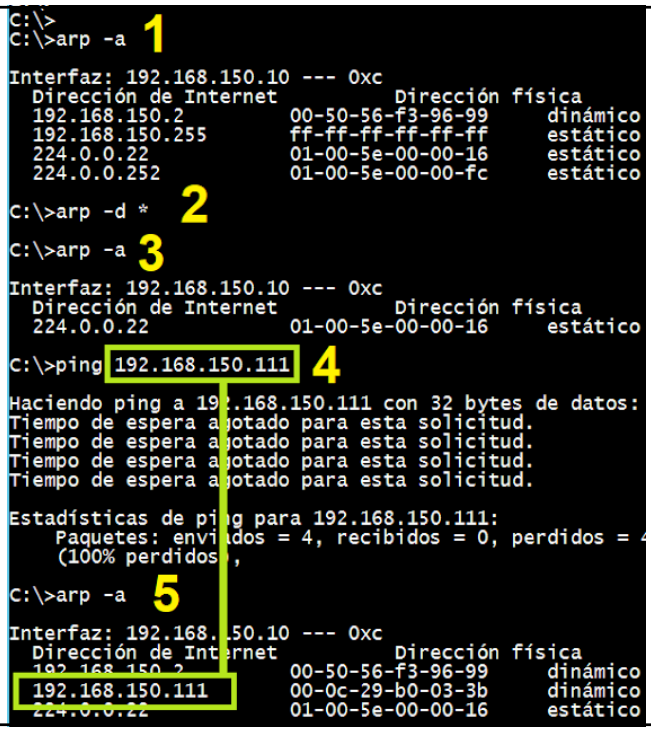
- Realizamos un ping al equipo destino.

- El destino no contesta.

- Verificamos la tabla ARP (Address Resolution Protocol) del equipo origen: Si la dirección MAC del equipo destino figura en la tabla, significa que el firewall del equipo destino está bloqueando el protocolo ICMP utilizado por el ping.

Laboratorio 1: El ping lo bloquea el firewall

45



46

1) Visualizamos el contenido de la tabla ARP con el comando: arp -a.

2) Eliminamos el contenido de la tabla ARP con el comando: arp -d *

3) Visualizamos el contenido de la tabla ARP con el comando: arp -a. No aparece ninguna dirección IP del segmento propio de red.

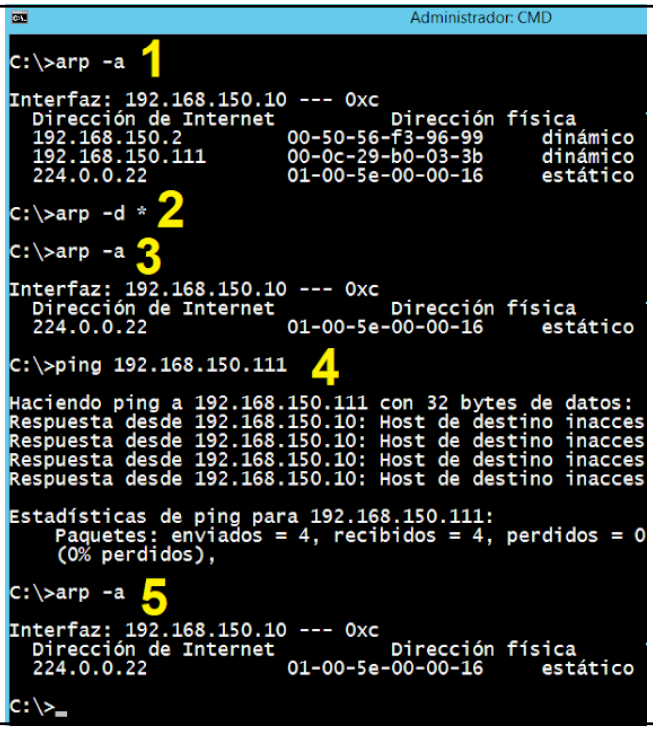
4) Realizamos un ping a la dirección IP del equipo destino. Vemos que el equipo destino, no contesta. La respuesta es: "Tiempo de espera agotado para esta solicitud".

5) Visualizamos el contenido de la tabla ARP con el comando: arp -a. Vemos como aparece la dirección IP destino.

Conclusión: El equipo destino está online, pero el firewall de Windows del equipo destino está bloqueando los paquetes ICMP.

Laboratorio 2: El ping no lo bloquea el firewall, el equipo destino está apagado.

47



48

1) Visualizamos el contenido de la tabla ARP con el comando: arp -a.

2) Eliminamos el contenido de la tabla ARP con el comando: arp -d *

3) Visualizamos el contenido de la tabla ARP con el comando: arp -a. No aparece ninguna dirección IP del segmento propio de red.

4) Realizamos un ping a la dirección IP del equipo destino. Vemos que el equipo destino, no contesta.

5) Visualizamos el contenido de la tabla ARP con el comando: arp -a. Vemos como no aparece la dirección IP destino.

Conclusión: El equipo destino no está online o no se dispone de conectividad con el mismo. No es el firewall de Windows del equipo destino que está bloqueando los paquetes ICMP, ya que no aparece la dirección IP destino en la tabla ARP.

49

WINDOWS DEFENDER

50

Estudiar los siguientes documentos:

- **2019_Cómo activar la Protección contra alteraciones de Windows Defender.pdf**

ACTIVACIÓN DE PROTECCIÓN CONTRA ALTERACIONES DE WINDOWS DEFENDER (SOLO W10 1903 O SUPERIOR)

51