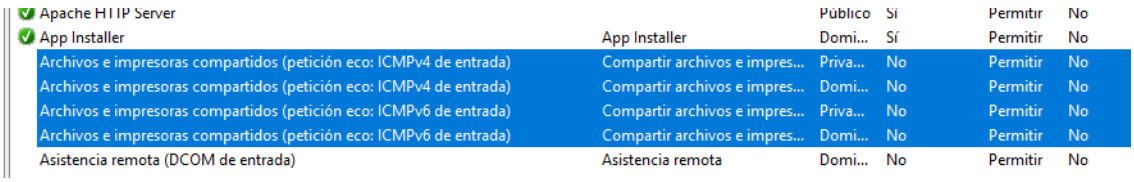
Ejercicios Prácticos: Firewall de Windows

Ejercicio 1: Bloqueo de respuesta ICMP (Ping)

Objetivo: Impedir que el equipo responda a solicitudes de ping desde la red local.

Pasos:

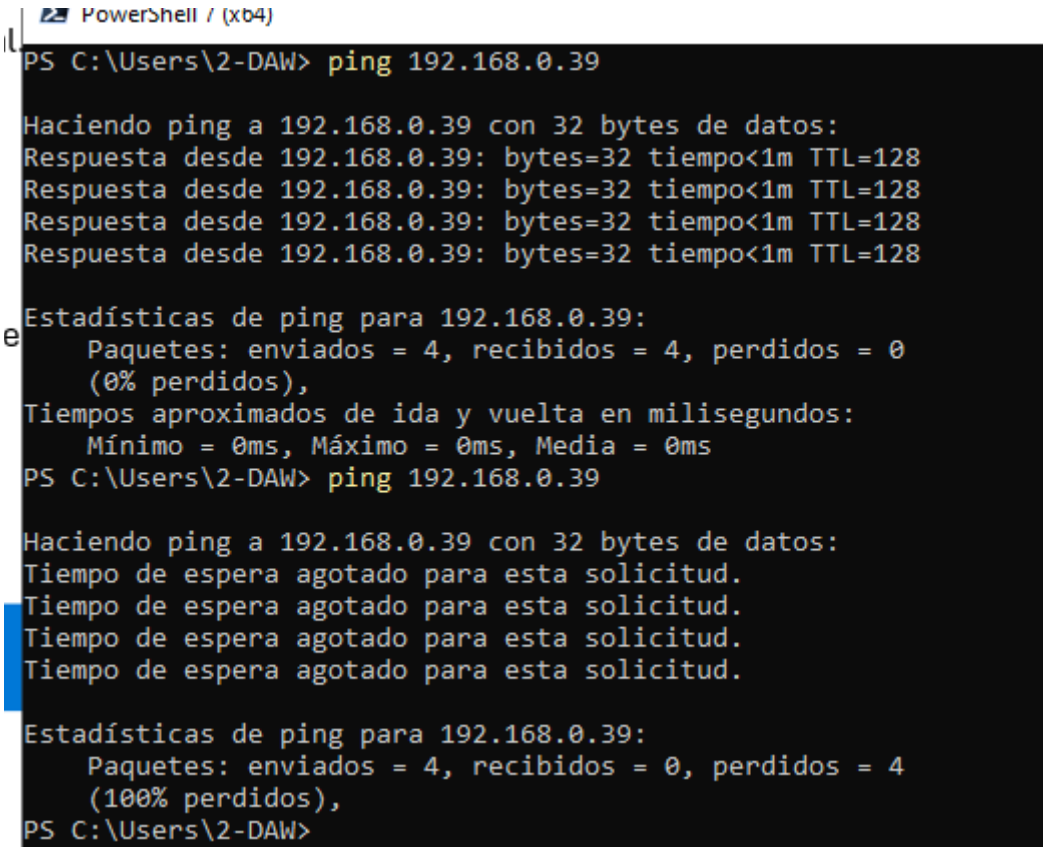
1. Abrir "Firewall de Windows Defender con seguridad avanzada"
2. Ir a "Reglas de entrada"
3. Buscar la regla "Compartir archivos e impresoras (Solicitud eco ICMPv4 de entrada)"
4. Deshabilitar o modificar la regla para el perfil de red correspondiente (Dominio/Privado/Público)



Apache HTTP Server		Público	Sí	Permitir	No
App Installer	App Installer	Domi...	Sí	Permitir	No
Archivos e impresoras compartidos (petición eco: ICMPv4 de entrada)	Compartir archivos e impres...	Priva...	No	Permitir	No
Archivos e impresoras compartidos (petición eco: ICMPv4 de entrada)	Compartir archivos e impres...	Domi...	No	Permitir	No
Archivos e impresoras compartidos (petición eco: ICMPv6 de entrada)	Compartir archivos e impres...	Priva...	No	Permitir	No
Archivos e impresoras compartidos (petición eco: ICMPv6 de entrada)	Compartir archivos e impres...	Domi...	No	Permitir	No
Asistencia remota (DCOM de entrada)	Asistencia remota	Domi...	No	Permitir	No

5. Probar desde otro equipo de la red con ping [IP_del_equipo]
6. Verificar que no hay respuesta

Verificación: El ping debe mostrar "Tiempo de espera agotado" o similar.



```
PowerShell 7 (x64)
PS C:\Users\2-DAW> ping 192.168.0.39

Haciendo ping a 192.168.0.39 con 32 bytes de datos:
Respuesta desde 192.168.0.39: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.39: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.39: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.39: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.0.39:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
PS C:\Users\2-DAW> ping 192.168.0.39

Haciendo ping a 192.168.0.39 con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 192.168.0.39:
    Paquetes: enviados = 4, recibidos = 0, perdidos = 4
    (100% perdidos),
PS C:\Users\2-DAW>
```

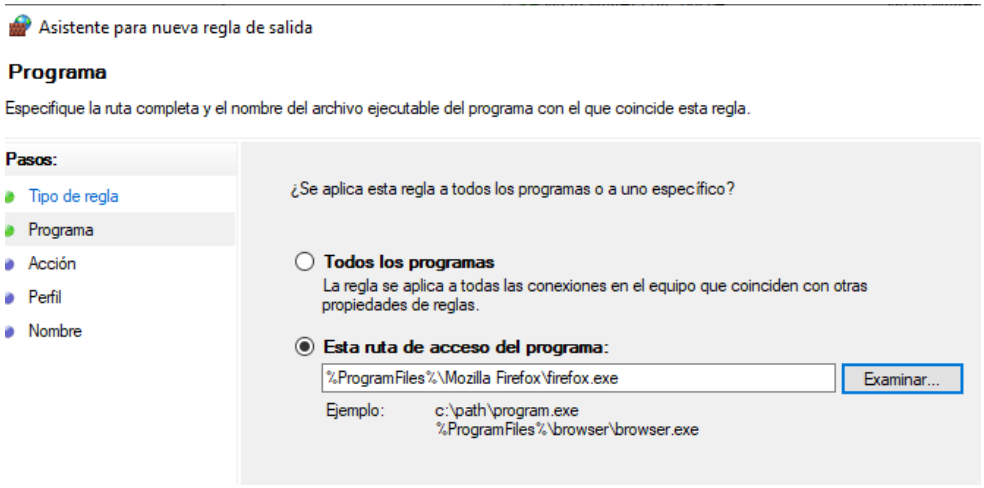
Ejercicio 2: Bloquear el acceso a un programa específico

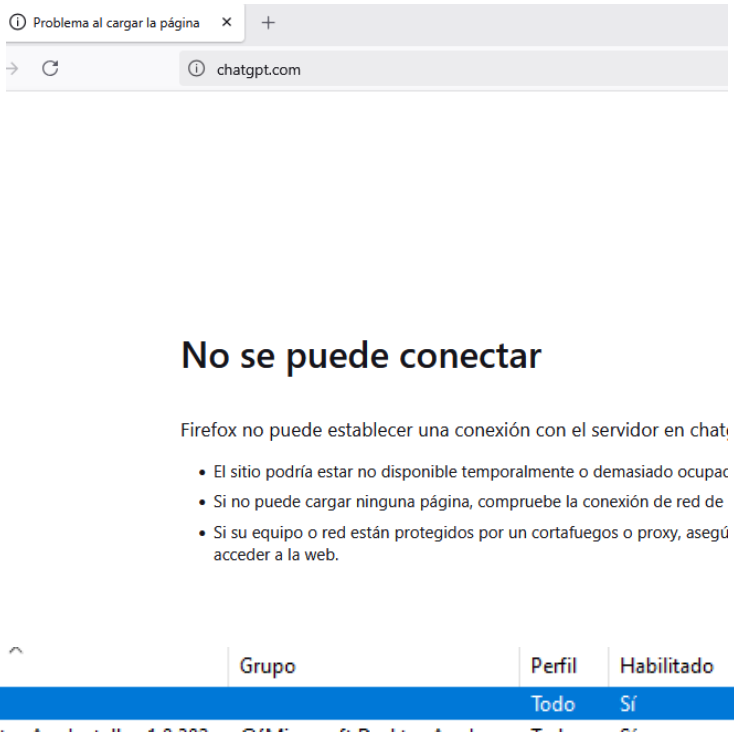
Objetivo: Impedir que una aplicación concreta (por ejemplo, navegador alternativo o juego) acceda a Internet.

Pasos:

1. En "Reglas de salida", crear nueva regla
2. Seleccionar "Programa"
3. Buscar el ejecutable (ej: C:\Program Files\Mozilla Firefox\firefox.exe)
4. Seleccionar "Bloquear la conexión"
5. Aplicar a todos los perfiles
6. Nombrar la regla descriptivamente
7. Intentar usar el programa y verificar que no accede a Internet

Verificación: El navegador o aplicación no debe conectarse a Internet.



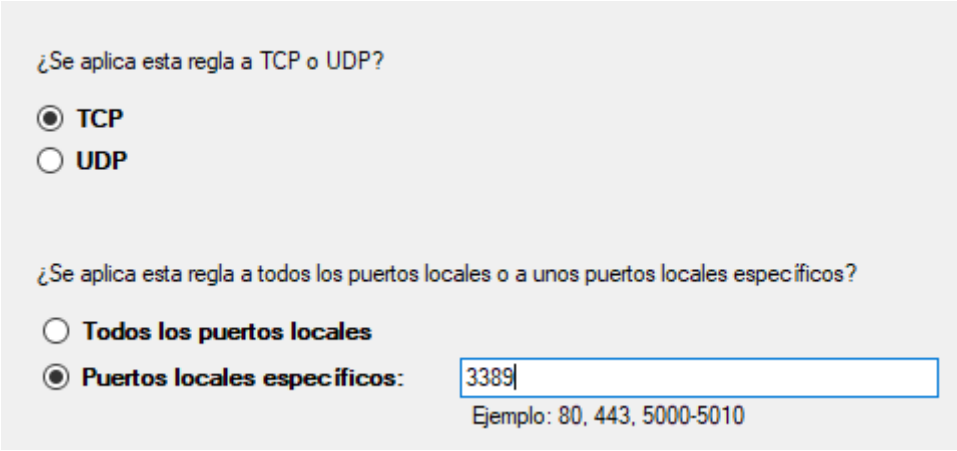


Ejercicio 3: Permitir solo un rango de IPs específico

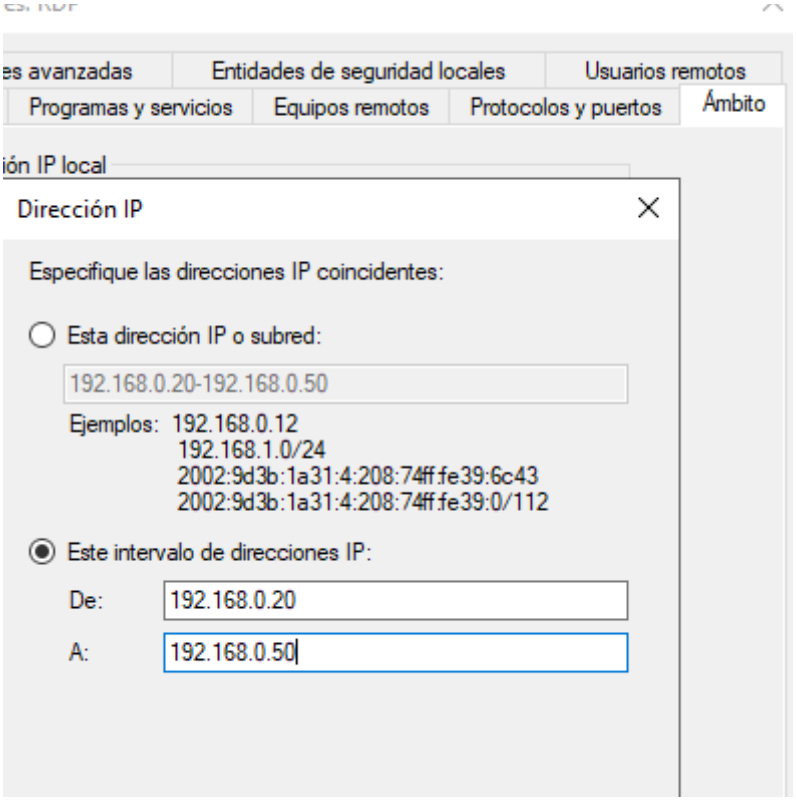
Objetivo: Configurar el firewall para que solo acepte conexiones RDP (puerto 3389) desde IPs de la red administrativa (ej: 192.168.1.100-192.168.1.110).

Pasos:

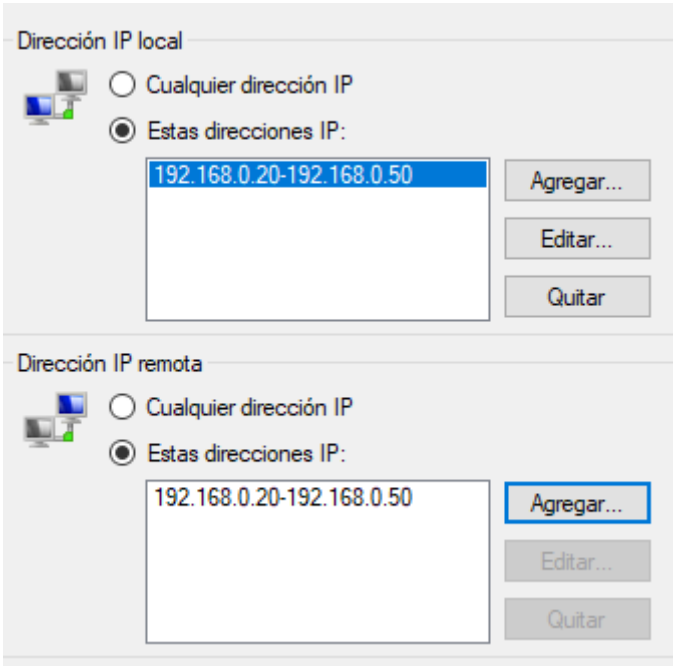
1. En "Reglas de entrada", buscar o crear regla para RDP (Puerto TCP 3389)



2. Hacer clic derecho → Propiedades
3. Ir a la pestaña "Ámbito"
4. En "Dirección IP remota", seleccionar "Estas direcciones IP"
5. Agregar el rango: 192.168.1.100-192.168.1.110



6. Aplicar cambios



7. Probar conexión RDP desde una IP dentro y fuera del rango

Verificación: Solo equipos en el rango permitido podrán conectarse por RDP.

Ejercicio 4: Bloquear puerto específico de salida

Objetivo: Impedir que cualquier aplicación use el puerto 25 (SMTP) para evitar el envío no autorizado de correos.

Pasos:

1. Ir a "Reglas de salida"
2. Crear nueva regla → "Puerto"
3. Seleccionar TCP y especificar puerto 25
4. Elegir "Bloquear la conexión"
5. Aplicar a todos los perfiles de red
6. Nombrar como "Bloqueo SMTP puerto 25"
7. Intentar enviar correo con cliente de email o telnet al puerto 25

Verificación: Las conexiones al puerto 25 deben fallar.

Ejercicio 5: Crear excepción temporal para servidor web local

Objetivo: Permitir acceso HTTP (puerto 80) solo durante horario laboral para un servidor web de pruebas.

Pasos:

1. Instalar un servidor web simple (ej: Apache, IIS o Python SimpleHTTPServer)
2. En "Reglas de entrada", crear nueva regla
3. Tipo: Puerto → TCP 80
4. Permitir la conexión
5. Aplicar solo al perfil "Privado"
6. En "Propiedades" → pestaña "Avanzadas", configurar restricciones adicionales
7. Probar acceso desde otro equipo: http://[IP_del_servidor]
8. Documentar cómo deshabilitar/habilitar rápidamente la regla según horario

Verificación: El navegador debe mostrar la página web servida localmente.

Consejos para la práctica:

- Trabajar en parejas para poder probar conexiones entre equipos
- Usar Test-NetConnection -ComputerName [IP] -Port [puerto] en PowerShell para verificar puertos
- Documentar cada cambio realizado
- Hacer capturas de pantalla del antes/después
- Practicar deshacer cambios restaurando reglas a su estado original