Seguridad y protección en Windows Server 2019

1. Configuración de protección en Windows Defender ATP y verificar Microsoft Defender ATP en Windows Server 2019.

Para ello:

- Configurar escaneos programados y análisis en tiempo real.

```
PS C:\Users\Administrador> Set-MpPreference -ScanScheduleDay 1 -ScanScheduleTime 05:00:00

PS C:\Users\Administrador>
```

Se definió un escaneo diario todos los lunes a las 05:00 AM.

```
PS C:\Users\Administrador> Set-MpPreference -DisableRealtimeMonitoring $false

PS C:\Users\Administrador> Get-MpPreference | Select-Object DisableRealtimeMonitoring

DisableRealtimeMonitoring
-------------------------
                   False
```

Habilitamos el monitoreo en tiempo real

- Implementar alertas automáticas y respuestas a incidentes.

```
PS C:\Users\Administrador> Set-MpPreference -LowThreatDefaultAction Quarantine

PS C:\Users\Administrador> Set-MpPreference -ModerateThreatDefaultAction Quarantine

PS C:\Users\Administrador> Set-MpPreference -HighThreatDefaultAction Quarantine

PS C:\Users\Administrador> Set-MpPreference -SevereThreatDefaultAction Quarantine

PS C:\Users\Administrador> Get-MpPreference | Select-Object LowThreatDefaultAction, ModerateThreatD

LowThreatDefaultAction ModerateThreatDefaultAction HighThreatDefaultAction SevereThreatDefaultActi
                                                                                                 on
---------------------- --------------------------- ----------------------- -----------------------
                     2                           2                       2                       2
```

Dejamos definido acciones para cada tipo de amenaza

```
PS C:\Users\Administrador> Set-MpPreference -MAPSReporting Advanced

PS C:\Users\Administrador> Set-MpPreference -SubmitSamplesConsent AlwaysPrompt

PS C:\Users\Administrador> Get-MpPreference | Select-Object MAPSReporting, SubmitSamplesConsent

MAPSReporting SubmitSamplesConsent
------------- --------------------
            2                    0
```

Habilitamos la seguridad avanzada y envío automático detallado de amenazas hacia Microsoft

- Generar una captura de pantalla del estado de ATP y un informe detallado de las configuraciones realizadas.

```
PS C:\Users\Administrador> Set-MpPreference -EnableNetworkProtection Enabled

PS C:\Users\Administrador> Set-MpPreference -EnableControlledFolderAccess Enabled

PS C:\Users\Administrador> Set-MpPreference -MAPSReporting Advanced
```

Preparamos las configuraciones para activar el ATP.

```
PS C:\Users\Administrador> Set-MpPreference -DisableBehaviorMonitoring $false

PS C:\Users\Administrador> Set-MpPreference -DisableIOAVProtection $false

PS C:\Users\Administrador> Set-MpPreference -DisableRealtimeMonitoring $false
```

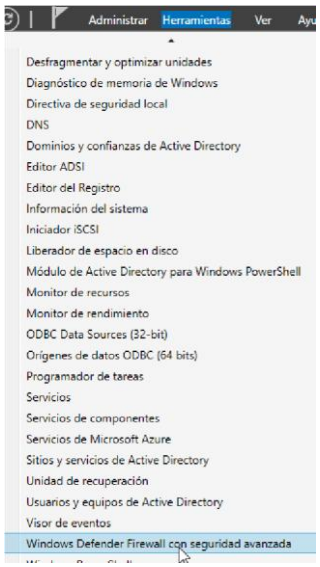
Habilitamos la protección avanzada.

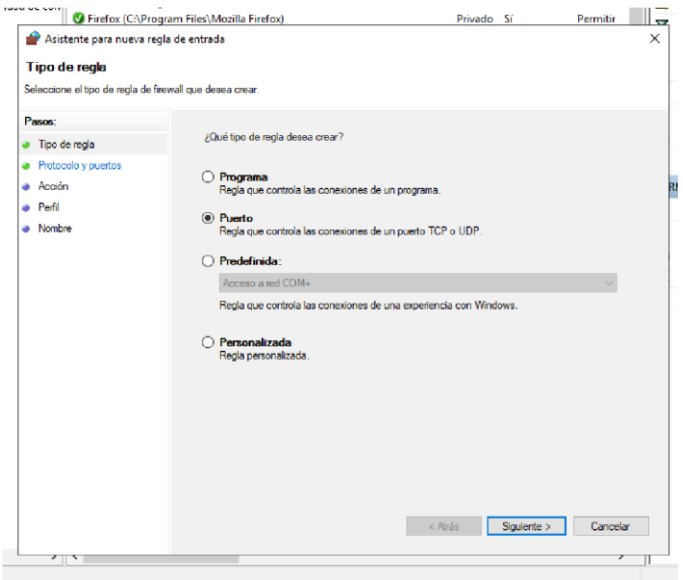
```
PS C:\Users\Administrador> New-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows Advanced Threat Protection\Status" -Name "Onboarding

Onboardingtate : 1
PSPath         : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Wind
                 ows Advanced Threat Protection\Status
PSParentPath   : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Wind
                 ows Advanced Threat Protection
PSChildName    : Status
PSDrive        : HKLM
PSProvider     : Microsoft.PowerShell.Core\Registry
```

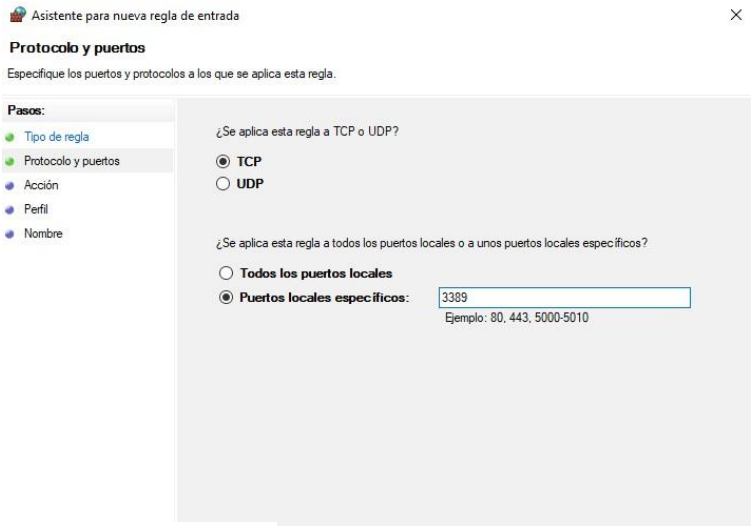
Implementamos ATP dentro del servidor.

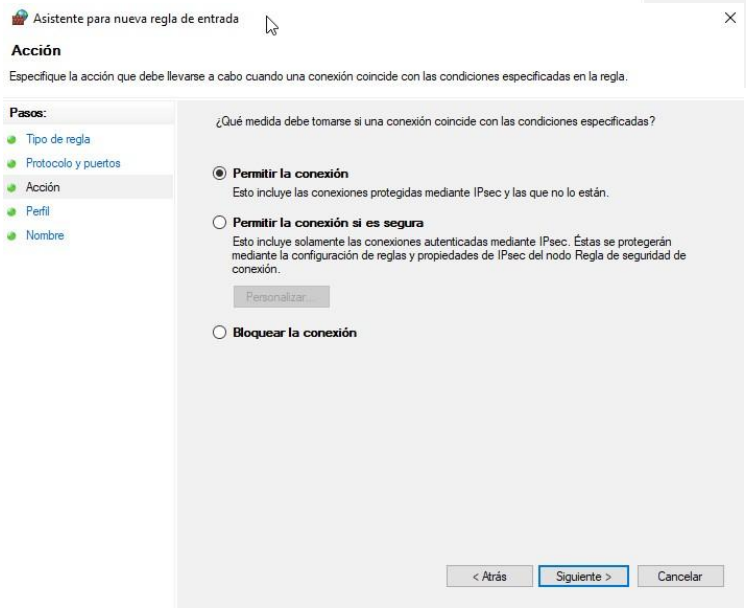
Con estas configuraciones y protecciones habilitadas, el sistema posee una mayor robustez y preparación frente a amenazas existentes o que aún no se hayan creado, ya que se encuentra en constante monitorización y análisis para detectar y actuar al instante, garantizando así un servidor más seguro y alerta en caso de cualquier eventualidad.

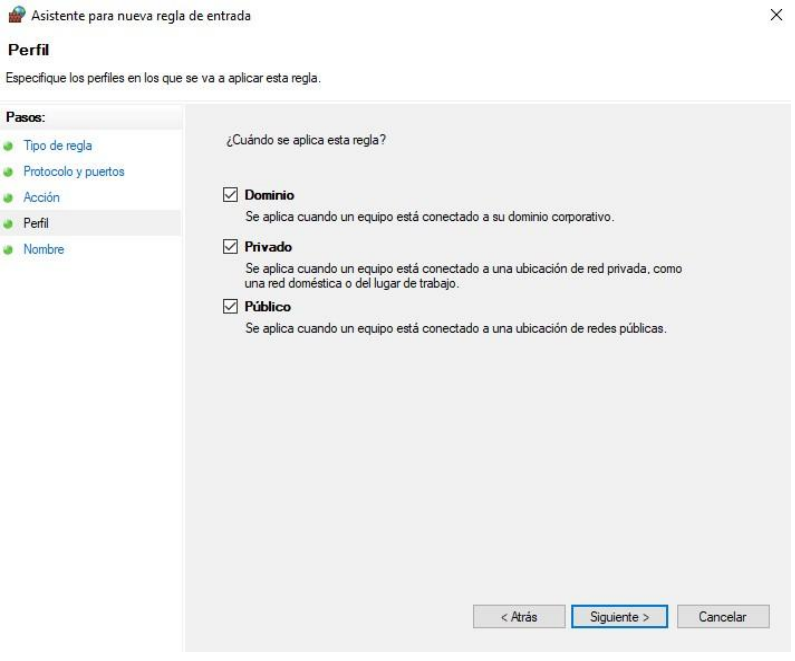
2. Configuración y evaluación del Firewall de Windows Defender
   - Configurar reglas de entrada y salida en el Firewall de Windows Defender según buenas prácticas de seguridad. Regla de entrada: permitir el puerto 3389 (RDP)

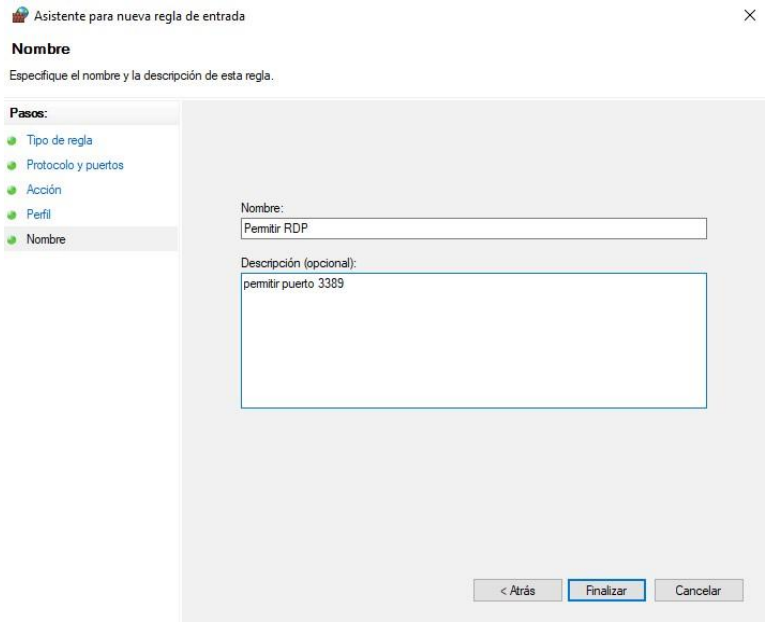




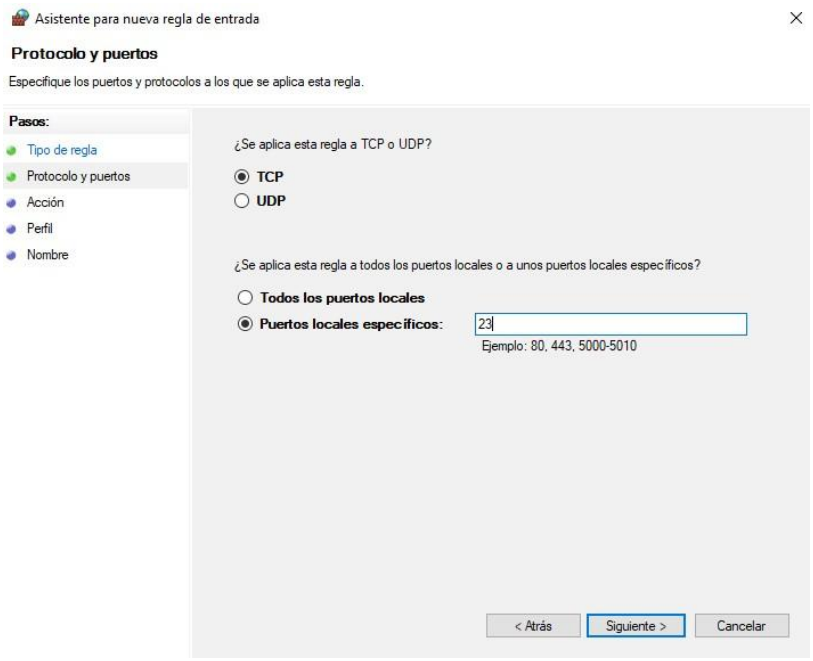

Asistente para nueva regla de entrada
Protocolo y puertos
Especifique los puertos y protocolos a los que se aplica esta regla.
Pasos:
Tipo de regla
Protocolo y puertos
Acción
Perfil
Nombre
¿Se aplica esta regla a TCP o UDP?
TCP
UDP
¿Se aplica esta regla a todos los puertos locales o a unos puertos locales específicos?
Todos los puertos locales
Puertos locales específicos:
3389
Ejemplo: 80, 443, 5000-5010
< Atrás
Siguiente >
Cancelar

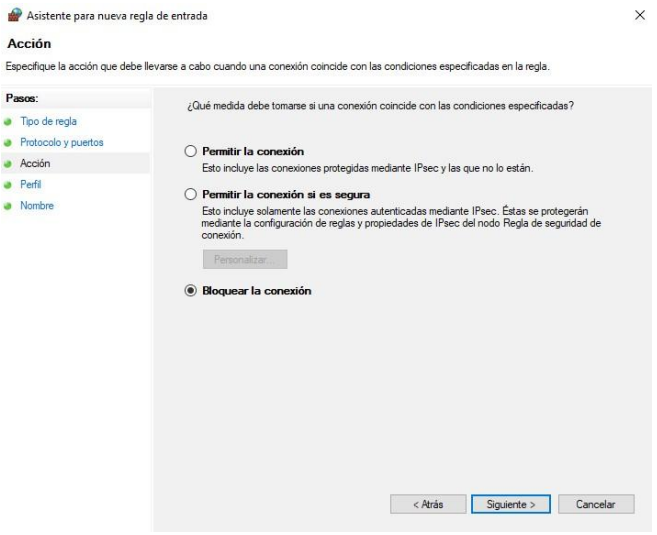

Asistente para nueva regla de entrada
Acción
Especifique la acción que debe llevarse a cabo cuando una conexión coincide con las condiciones especificadas en la regla.
Pasos:
Tipo de regla
Protocolo y puertos
Acción
Perfil
Nombre
¿Qué medida debe tomarse si una conexión coincide con las condiciones especificadas?
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

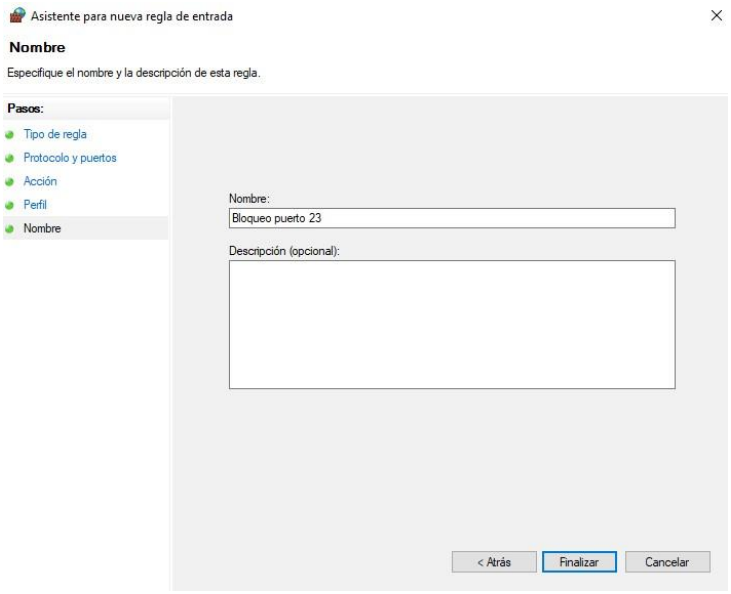

Asistente para nueva regla de entrada
Perfil
Especifique los perfiles en los que se va a aplicar esta regla.
Pasos:
Tipo de regla
Protocolo y puertos
Acción
Perfil
Nombre
¿Cuándo se aplica esta regla?
Dominio
Se aplica cuando un equipo está conectado a su dominio corporativo.
Privado
Se aplica cuando 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



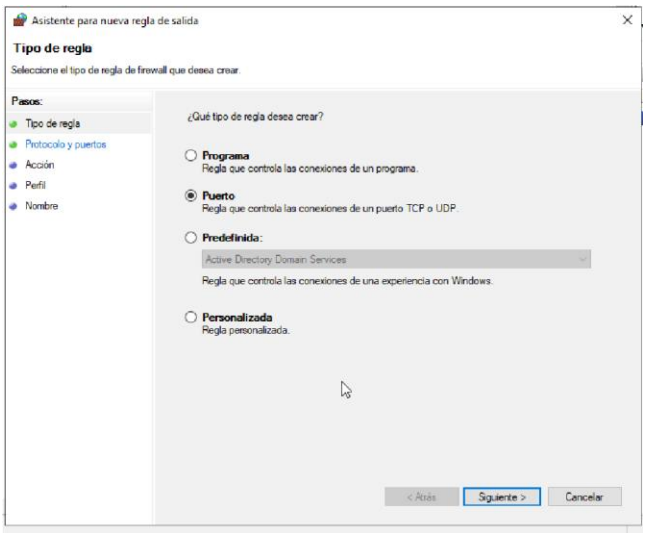
Regla de entrada: Bloquear el puerto 23 por ser inseguro y objetivo general de ataques.

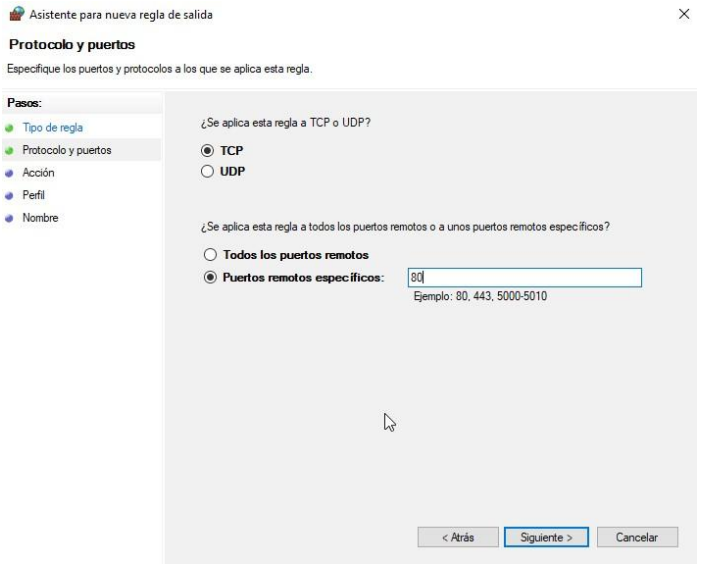


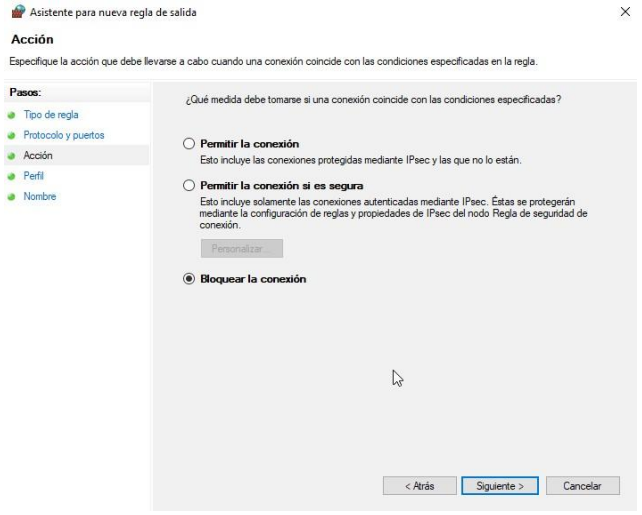


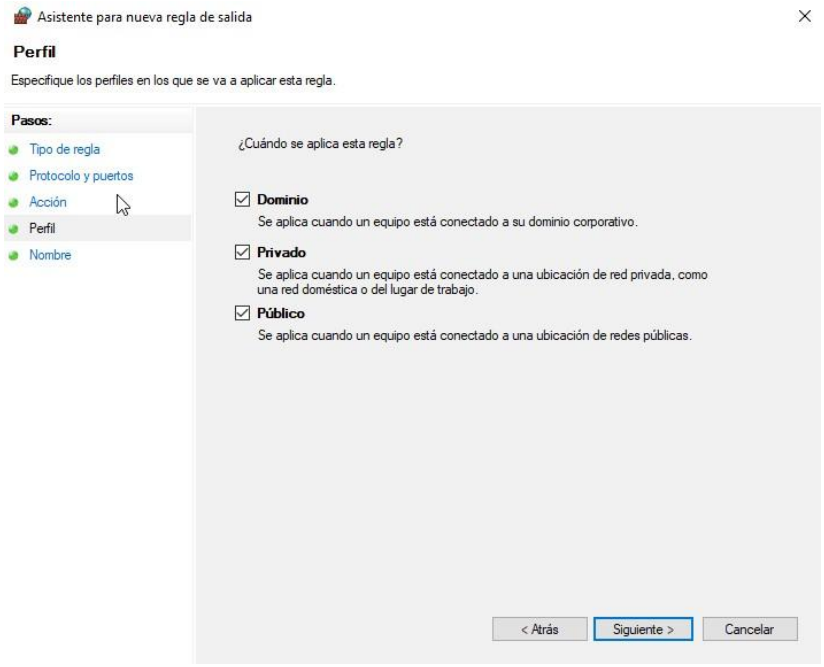


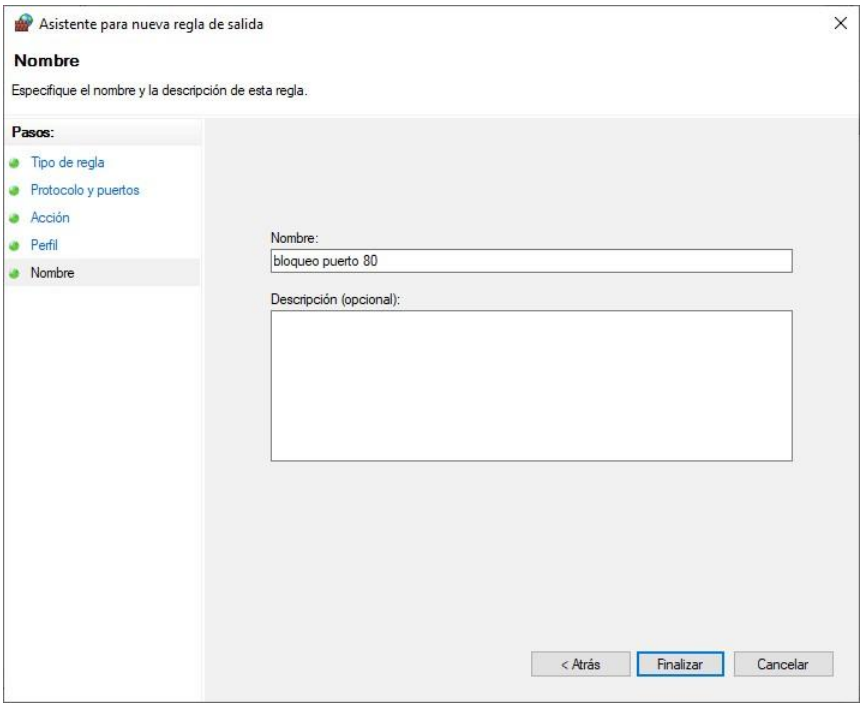
Regla de salida:
Restringir puerto 80 para mantener controlado la información y tráfico que va hacia Internet.

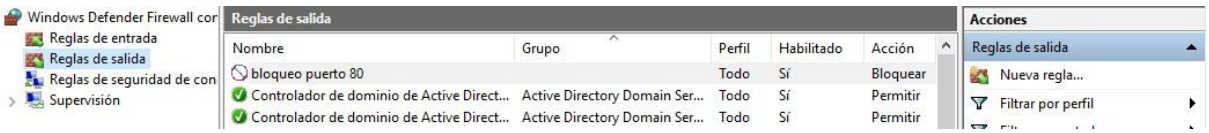



Asistente para nueva regla de salida
Protocolo y puertos
Especifique los puertos y protocolos a los que se aplica esta regla.
Pasos:
Tipo de regla
Protocolo y puertos
Acción
Perfil
Nombre
¿Se aplica esta regla a TCP o UDP?
TCP
UDP
¿Se aplica esta regla a todos los puertos remotos o a unos puertos remotos específicos?
Todos los puertos remotos
Puertos remotos específicos:
80
Ejemplo: 80, 443, 5000-5010
< Atrás
Siguiente >
Cancelar


Asistente para nueva regla de salida
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

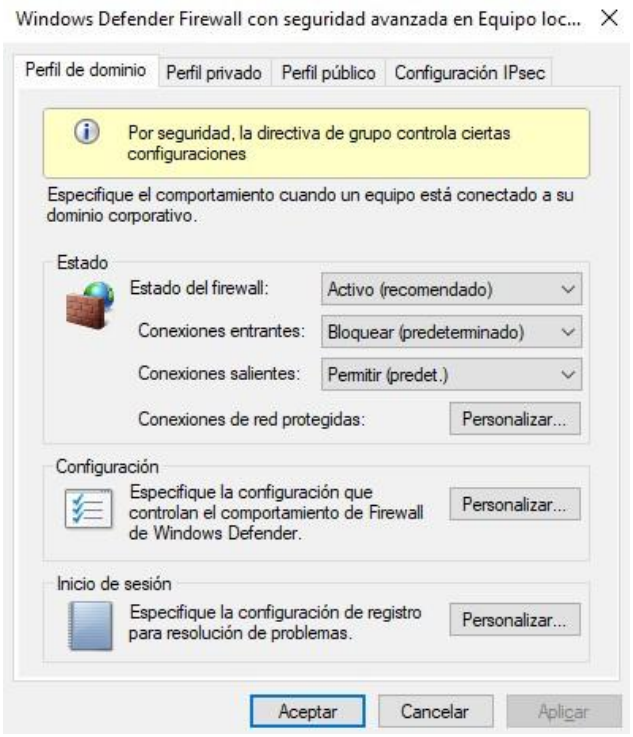

Asistente para nueva regla de salida
Perfil
Especifique los perfiles en los que se va a aplicar esta regla.
Pasos:
Tipo de regla
Protocolo y puertos
Acción
Perfil
Nombre
¿Cuándo se aplica esta regla?
Dominio
Se aplica cuando un equipo está conectado a su dominio corporativo.
Privado
Se aplica cuando 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

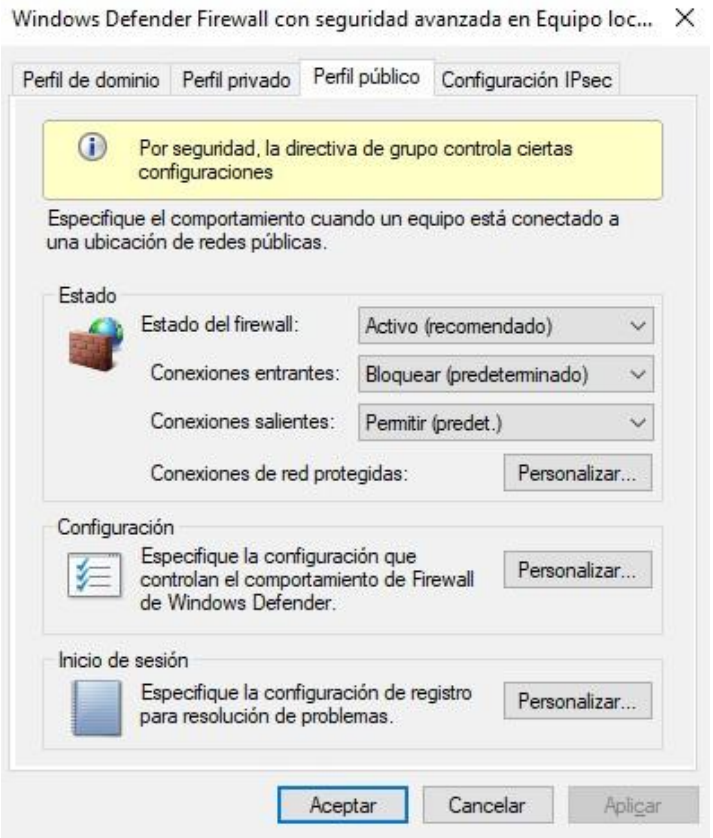

Asistente para nueva regla de salida
Nombre
Especifique el nombre y la descripción de esta regla.
Pasos:
Tipo de regla
Protocolo y puertos
Acción
Perfil
Nombre
Nombre:
bloqueo puerto 80
Descripción (opcional):
< Atrás
Finalizar
Cancelar


Windows Defender Firewall cor
Reglas de entrada
Reglas de salida
Reglas de seguridad de con
Supervisión
Reglas de salida
Nombre
Grupo
Perfil
Habilitado
Acción
bloqueo puerto 80
Todo
Sí
Bloquear
Controlador de dominio de Active Direct...
Active Directory Domain Ser...
Todo
Sí
Permitir
Controlador de dominio de Active Direct...
Active Directory Domain Ser...
Todo
Sí
Permitir
Acciones
Reglas de salida
Nueva regla...
Filtrar por perfil

-

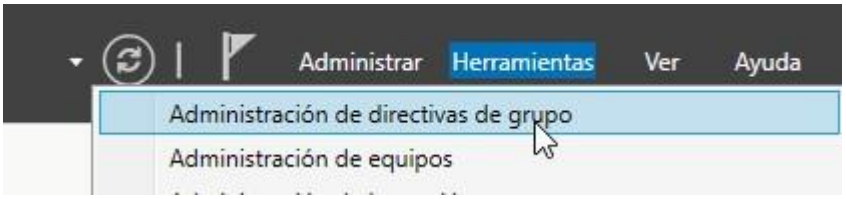
Aplicar restricciones en los perfiles de red (Dominio, Privado y Público).

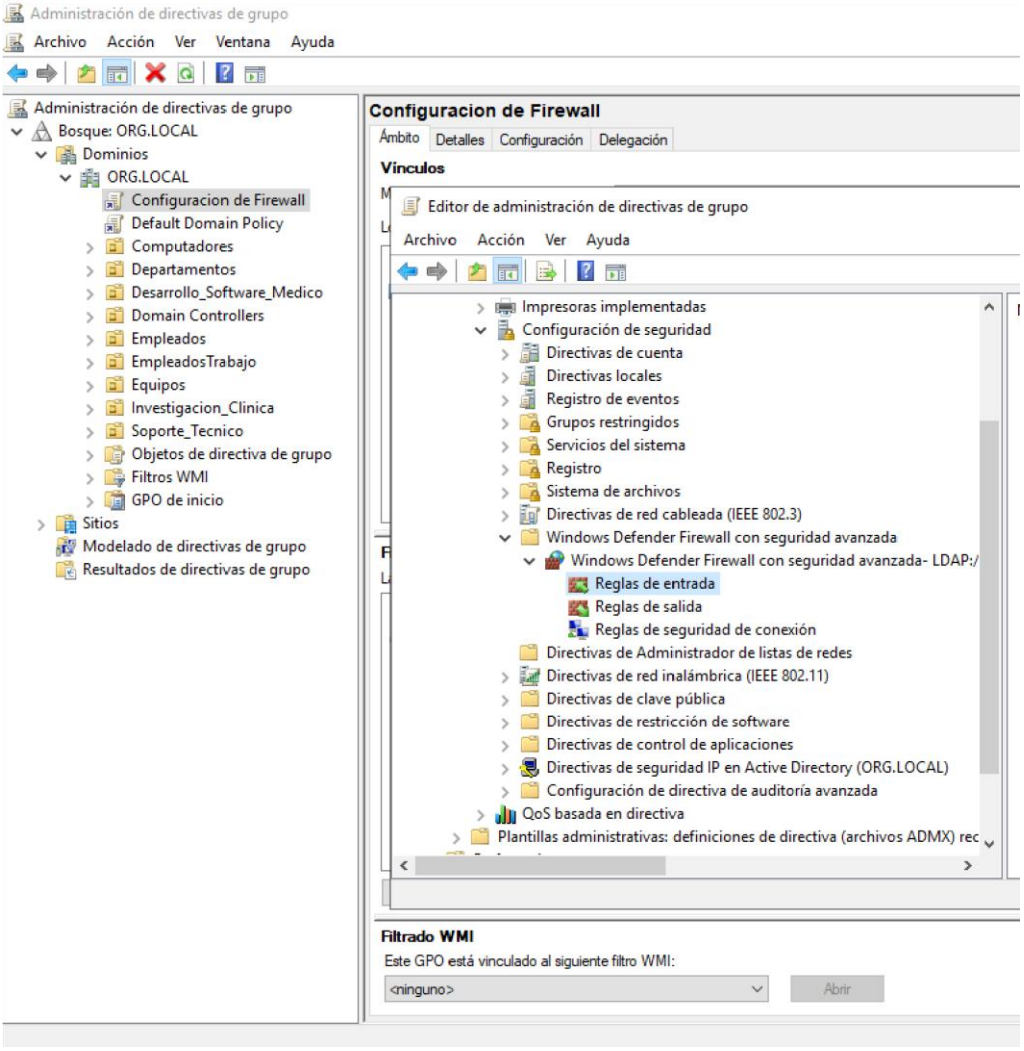


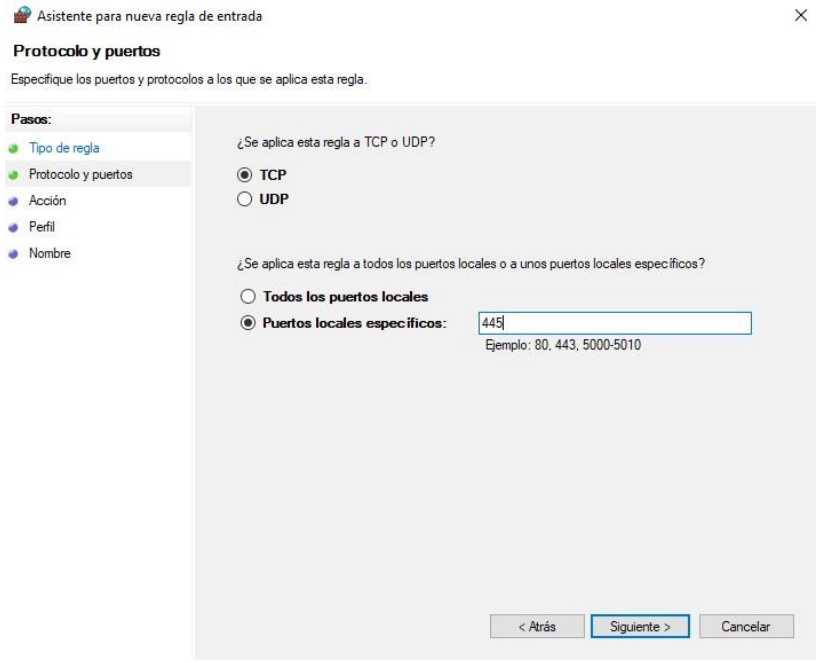


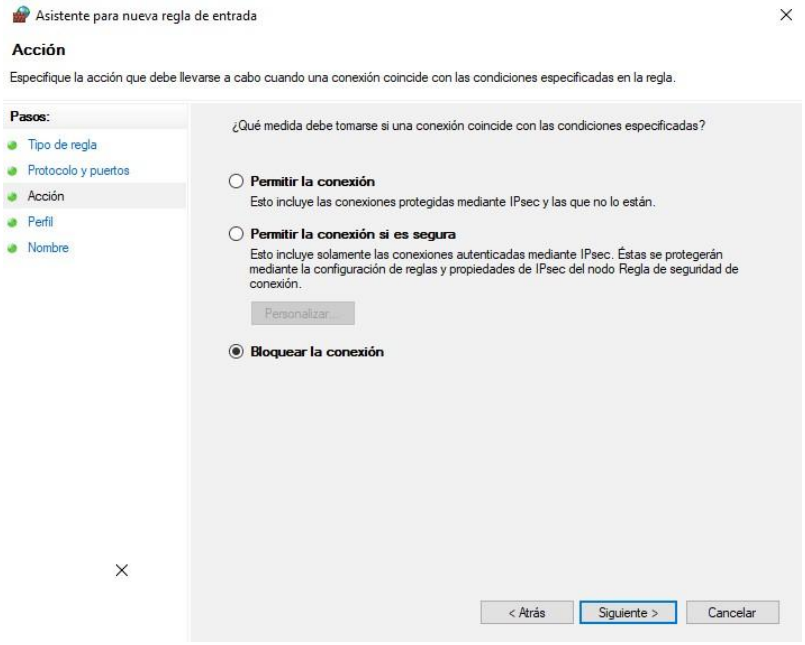
- Implementar y evaluar directivas de grupo para reforzar la seguridad del Firewall.

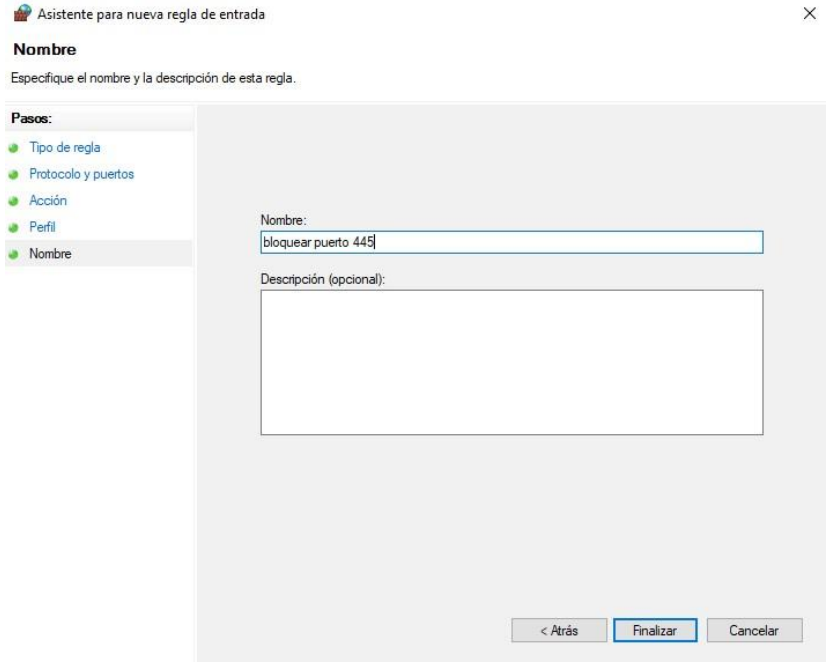
GPO: Bloquear puerto 445 en el firewall para evitar compartir archivos de manera accidentada.


Administrar
Herramientas
Ver
Ayuda
Administración de directivas de grupo
Administración de equipos


Administración de directivas de grupo
Archivo Acción Ver Ventana Ayuda
Administración de directivas de grupo
Bosque: ORG.LOCAL
Dominios
ORG.LOCAL
Configuracion de Firewall
Default Domain Policy
Computadores
Departamentos
Desarrollo_Software_Medico
Domain Controllers
Empleados
EmpleadosTrabajo
Equipos
Investigacion_Clinica
Soporte_Tecnico
Objetos de directiva de grupo
Filtros WMI
GPO de inicio
Sitios
Modelado de directivas de grupo
Resultados de directivas de grupo
Configuracion de Firewall
Ámbito Detalles Configuración Delegación
Vínculos
Editor de administración de directivas de grupo
Archivo Acción Ver Ayuda
Impresoras implementadas
Configuración de seguridad
Directivas de cuenta
Directivas locales
Registro de eventos
Grupos restringidos
Servicios del sistema
Registro
Sistema de archivos
Directivas de red cableada (IEEE 802.3)
Windows Defender Firewall con seguridad avanzada
Windows Defender Firewall con seguridad avanzada- LDAP:/
Reglas de entrada
Reglas de salida
Reglas de seguridad de conexión
Directivas de Administrador de listas de redes
Directivas de red inalámbrica (IEEE 802.11)
Directivas de clave pública
Directivas de restricción de software
Directivas de control de aplicaciones
Directivas de seguridad IP en Active Directory (ORG.LOCAL)
Configuración de directiva de auditoría avanzada
QoS basada en directiva
Plantillas administrativas: definiciones de directiva (archivos ADMX) rec
Filtrado WMI
Este GPO está vinculado al siguiente filtro WMI:
<ninguno>
Abrir

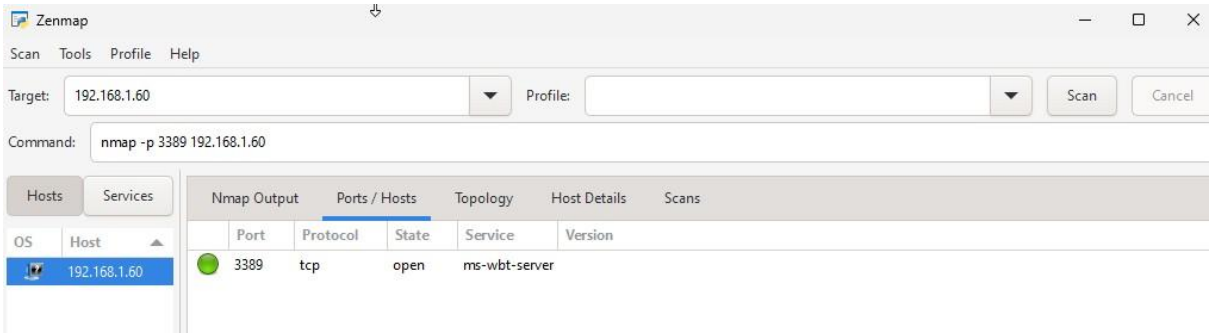

Asistente para nueva regla de entrada
Protocolo y puertos
Especifique los puertos y protocolos a los que se aplica esta regla.
Pasos:
Tipo de regla
Protocolo y puertos
Acción
Perfil
Nombre
¿Se aplica esta regla a TCP o UDP?
TCP
UDP
¿Se aplica esta regla a todos los puertos locales o a unos puertos locales específicos?
Todos los puertos locales
Puertos locales específicos:
445
Ejemplo: 80, 443, 5000-5010
< Atrás
Siguiente >
Cancelar


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

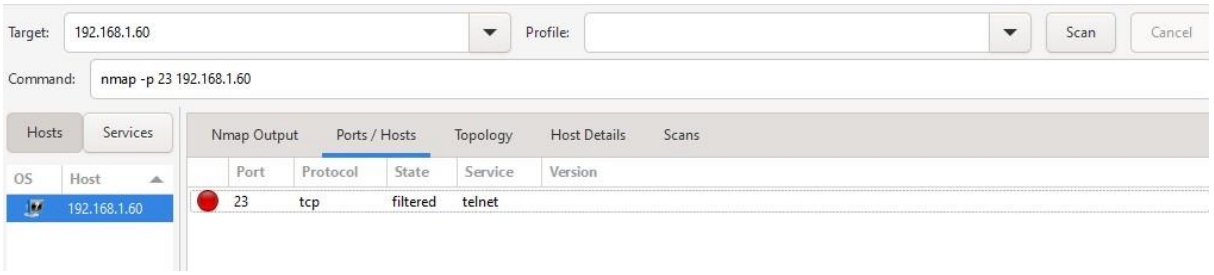

Asistente para nueva regla de entrada
Nombre
Especifique el nombre y la descripción de esta regla.
Pasos:
Tipo de regla
Protocolo y puertos
Acción
Perfil
Nombre
Nombre:
bloquear puerto 445
Descripción (opcional):
< Atrás
Finalizar
Cancelar

- Probar la configuración mediante la simulación de tráfico de red permitido y bloqueado.

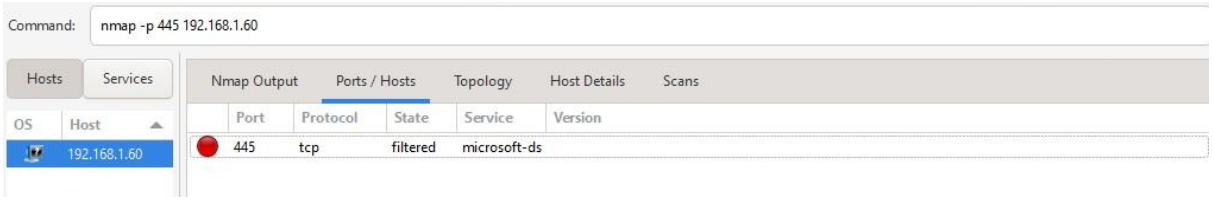
Nmap en windows 11 (cliente)



Nmap en windows 11 (cliente) bloqueo de puerto 23



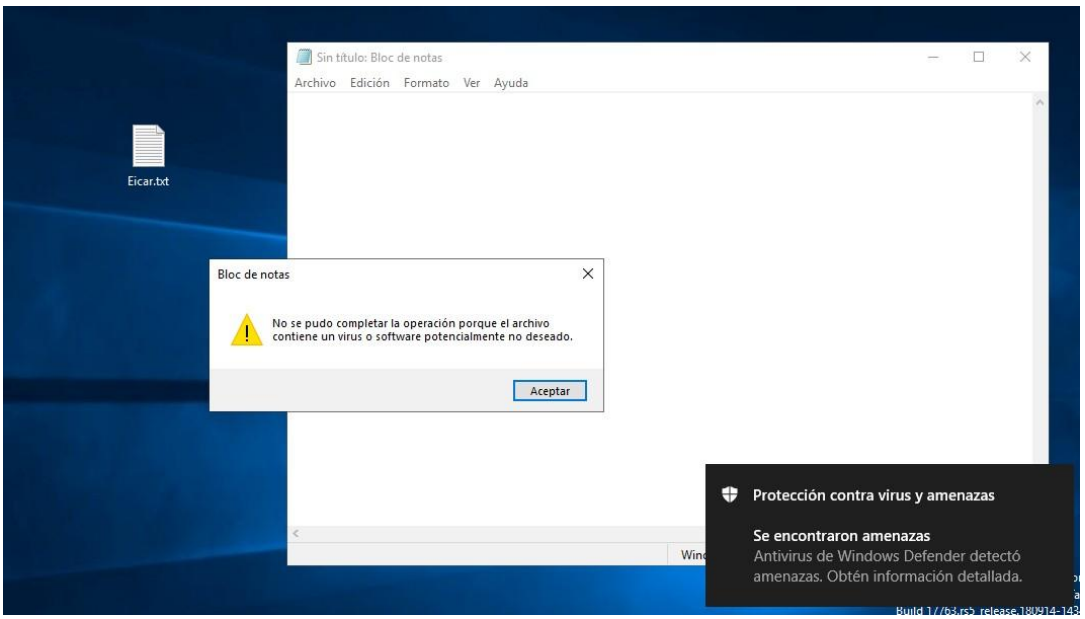
Nmap en window 11 (cliente) bloqueo por 445

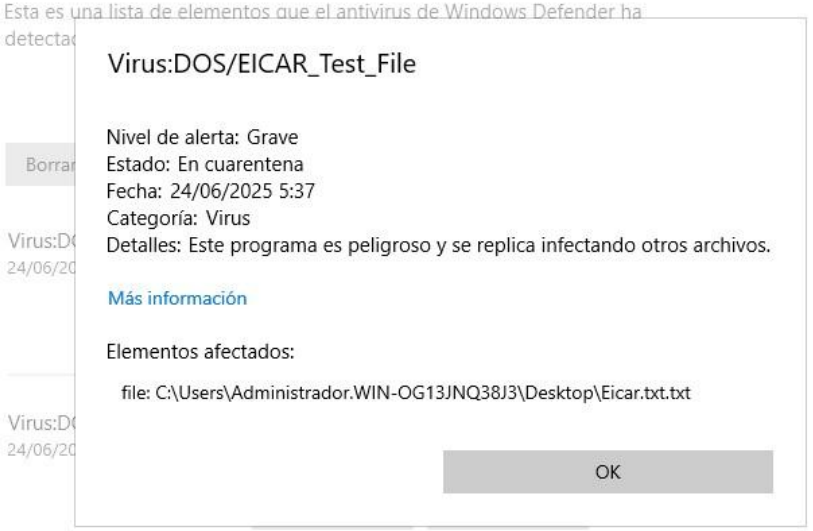


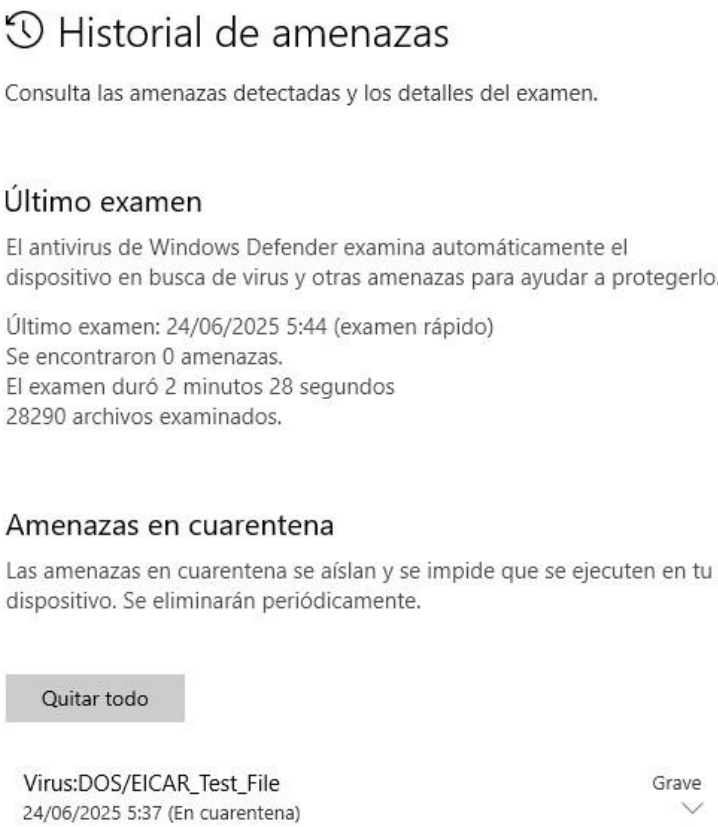
Se bloquearon los puertos 23 y 445 para maximizar la seguridad, evitando tráfico por ellos para así evitar accidentes, ataques y problemas en la conectividad.

3. Evaluación y ajuste de seguridad del sistema

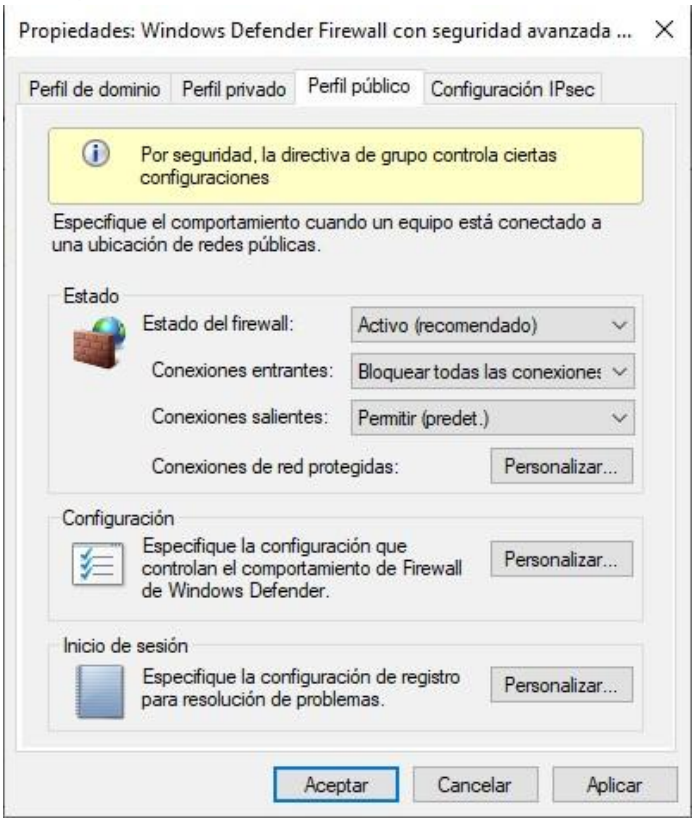
- Realizar una prueba de detección de amenazas con un archivo de prueba EICAR y verificar la respuesta de Windows Defender.

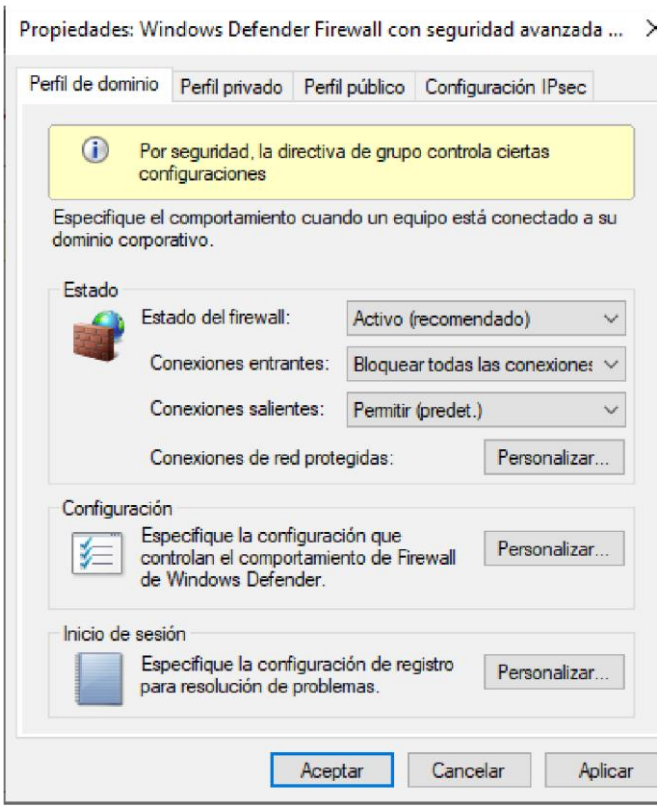

Eicar.txt
Sin título: Bloc de notas
Archivo Edición Formato Ver Ayuda
Bloc de notas
No se pudo completar la operación porque el archivo contiene un virus o software potencialmente no deseado.
Aceptar
Protección contra virus y amenazas
Se encontraron amenazas
Antivirus de Windows Defender detectó amenazas. Obtén información detallada.

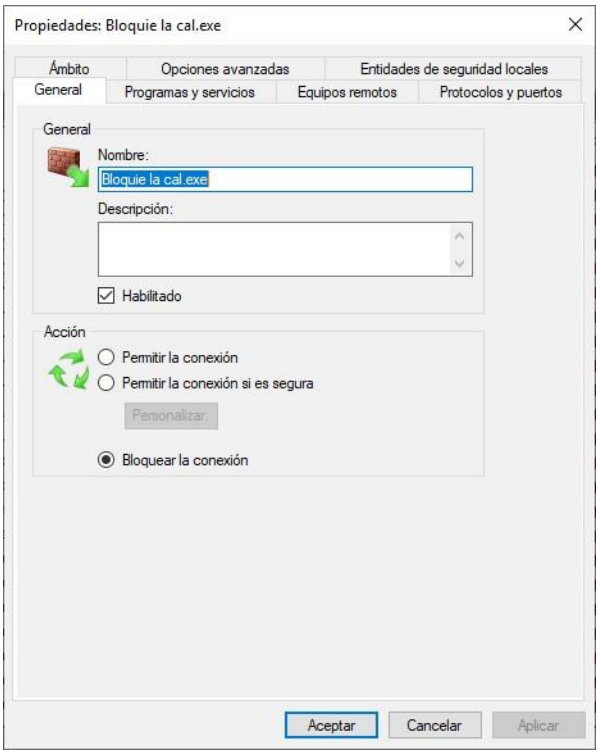

Historial completo
Esta es una lista de elementos que el antivirus de Windows Defender ha
Virus:DOS/EICAR_Test_File
Nivel de alerta: Grave
Estado: En cuarentena
Fecha: 24/06/2025 5:37
Categoría: Virus
Detalles: Este programa es peligroso y se replica infectando otros archivos.
Más información
Elementos afectados:
file: C:\Users\Administrador.WIN-OG13JNQ38J3\Desktop\Eicar.txt.txt
OK



- Ajustar la configuración del Firewall según los resultados de la prueba.







Frente a la amenaza del archivo detectado se ajustaron las configuraciones de los perfiles en firewall para mayor seguridad, añadiendo además un bloqueo en ejecutables que pueden traer amenazas peligrosas.

- Generar un informe de evaluación con mejoras recomendadas para optimizar la seguridad del servidor.

☐ Actualización del Server.

☐ Bloquear todas las conexiones entrantes no solicitadas en el firewall.

- Minimiza la superficie de ataque al rechazar todo tráfico no explícitamente permitido.

- Protege contra escaneo de puertos y exploits remotos que aprovechan servicios expuestos.

☐ Eliminar o deshabilitar reglas de firewall innecesarias.

- Cierra posibles “backdoors” inadvertidos.
- Facilita auditorías y gestión futura
- Reduce la complejidad y confusión en la administración del firewall.

☐ Restringir accesos críticos (como RDP) a IPs autorizadas solamente.

- Añade un control de acceso por red complementario a la autenticación de usuario.
- Protege contra ataques de fuerza bruta y herramientas de escaneo automatizado.

☐ Habilitar el registro de eventos de firewall y seguridad para monitoreo continuo.

- Proporciona trazabilidad para investigaciones forenses.
- Permite la detección proactiva de patrones sospechosos (p.ej., múltiples intentos fallidos).
- Apoya el cumplimiento de normativas y buenas prácticas.

☐ Aplicar políticas de actualización automática y contraseñas seguras.

- Forzar actualizaciones de seguridad críticas vía GPO.
- Establecer políticas de complejidad de contraseñas (longitud ≥ 12, alfanumérica, caducidad, historial).
    1. Previene explotación de vulnerabilidades conocidas.

2. Mitiga el riesgo de acceso no autorizado por contraseñas débiles

Frente a la amenaza simulada se entregan diversas recomendaciones y peticiones para mejorar y refinar la seguridad dentro del servidor, llevando así un control más exhaustivo frente a peligros que aun no se hacen presente en el servidor.