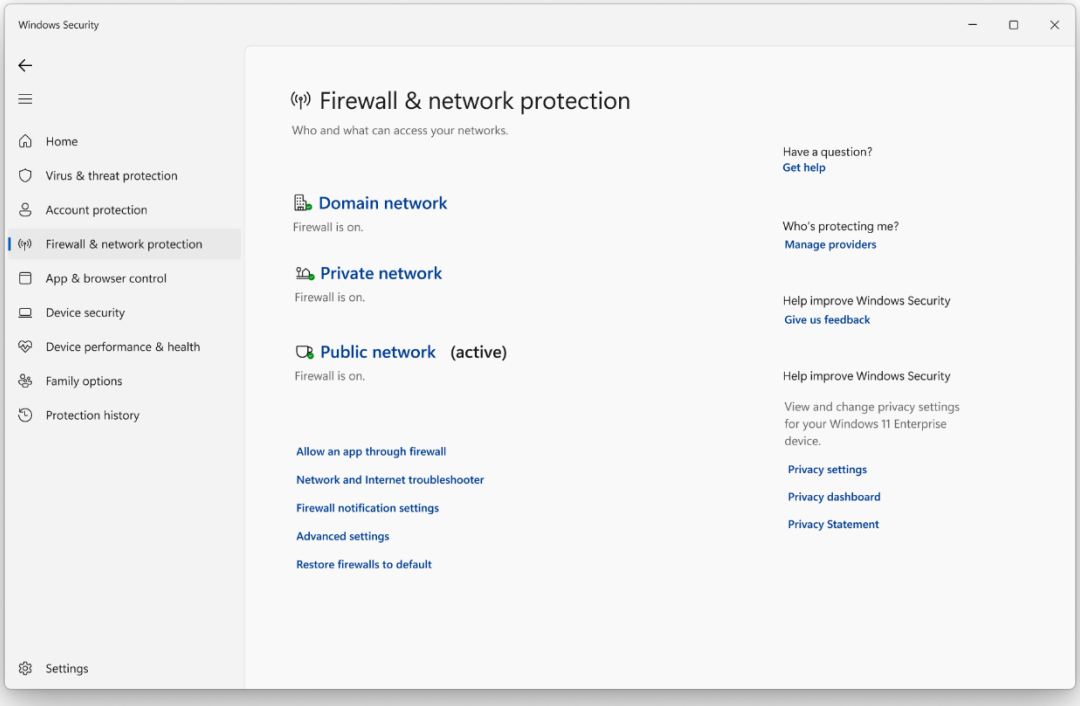
Introducción a Firewall de Windows

Firewall de Windows es una característica de seguridad que ayuda a proteger el dispositivo filtrando el tráfico de red que entra y sale del dispositivo. Este tráfico se puede filtrar según varios criterios, incluida la dirección IP de origen y destino, el protocolo IP o el número de puerto de origen y destino. Firewall de Windows se puede configurar para bloquear o permitir el tráfico de red en función de los servicios y las aplicaciones que se instalan en el dispositivo. Esto le permite restringir el tráfico de red solo a aquellas aplicaciones y servicios a los que se les permite comunicarse explícitamente en la red.

Firewall de Windows es un firewall basado en host que se incluye con el sistema operativo y está habilitado de forma predeterminada en todas las ediciones de Windows.

Firewall de Windows admite la seguridad del protocolo de Internet (IPsec), que puede usar para requerir la autenticación de cualquier dispositivo que intente comunicarse con el dispositivo. Cuando se requiere autenticación, los dispositivos que no se pueden autenticar como *un dispositivo de confianza* no se pueden comunicar con el dispositivo. Puede usar IPsec para requerir que determinado tráfico de red esté cifrado para evitar que lo lean los analizadores de paquetes de red que un usuario malintencionado podría asociar a la red.

Firewall de Windows también funciona con reconocimiento de ubicación de red para que pueda aplicar la configuración de seguridad adecuada a los tipos de redes a las que está conectado el dispositivo. Por ejemplo, Firewall de Windows puede aplicar el perfil de *red pública* cuando el dispositivo está conectado a una cafetería wi-fi y el perfil de *red privada* cuando el dispositivo está conectado a la red doméstica. Esto le permite aplicar configuraciones más restrictivas a las redes públicas para ayudar a mantener el dispositivo seguro.



Aplicaciones prácticas

Firewall de Windows ofrece varias ventajas para abordar los desafíos de seguridad de red de la organización:

- Menor riesgo de amenazas de seguridad de red: al reducir la superficie expuesta a ataques de un dispositivo, Firewall de Windows proporciona una capa adicional de defensa al modelo de defensa en profundidad. Esto aumenta la capacidad de administración y reduce la probabilidad de un ataque exitoso.
- Protección de datos confidenciales y propiedad intelectual: Firewall de Windows se integra con IPsec para proporcionar una manera sencilla de aplicar comunicaciones de red autenticadas de un extremo a otro. Esto permite el acceso escalable y en niveles a los recursos de red de confianza, lo que ayuda a aplicar la integridad de los datos y, si es necesario, a proteger la confidencialidad de los datos.
- Valor extendido de las inversiones existentes: Firewall de Windows es un firewall basado en host incluido con el sistema operativo, por lo que no se requiere hardware ni software adicionales. También está diseñado para complementar las soluciones de seguridad de red existentes que no son de Microsoft a través de una API documentada.

El comportamiento predeterminado de Firewall de Windows es:

- bloquear todo el tráfico entrante, a menos que se solicite o coincida con una *regla*
- permitir todo el tráfico saliente, a menos que coincida con una *regla*

Reglas de firewall

Las reglas de firewall identifican el tráfico de red permitido o bloqueado y las condiciones para que esto suceda. Las reglas ofrecen una amplia selección de condiciones para identificar el tráfico, entre las que se incluyen:

- Nombre de aplicación, servicio o programa
- Direcciones IP de origen y destino
- Puede usar valores dinámicos, como la puerta de enlace predeterminada, los servidores DHCP, los servidores DNS y las subredes locales.
- Nombre o tipo de protocolo. Para los protocolos de capa de transporte, TCP y UDP, puede especificar puertos o intervalos de puertos. Para los protocolos personalizados, puede usar un número entre 0 y 255 que represente el protocolo IP.
- Tipo de interfaz
- Tipo de tráfico ICMP/ICMPv6 y código

Perfiles de firewall

Firewall de Windows ofrece tres perfiles de red: dominio, privado y público. Los perfiles de red se usan para asignar reglas. Por ejemplo, puede permitir que una aplicación específica se comunique en una red privada, pero no en una red pública.

Red de dominio

El perfil de *red de dominio* se aplica automáticamente a un dispositivo que está unido a un dominio de Active Directory, cuando detecta la disponibilidad de un controlador de dominio. Este perfil de red no se puede establecer manualmente.

Sugerencia

Otra opción para detectar la *red de dominio* es configurar las opciones de directiva en el CSP de directiva **NetworkListManager**, que también se aplica a Microsoft entre dispositivos unidos.

Red privada

El perfil *de red privada* está diseñado para redes privadas como una red doméstica. Un administrador puede establecerlo manualmente en una interfaz de red.

Red pública

El perfil de *red pública* está diseñado teniendo en cuenta una mayor seguridad para las redes públicas, como puntos de acceso Wi-Fi, cafeterías, aeropuertos, hoteles, etc. Es el perfil predeterminado para las redes no identificadas.

Sugerencia

Use el cmdlet Get-NetConnectionProfile de PowerShell para recuperar la categoría de red activa (NetworkCategory). Use el cmdlet Set-NetConnectionProfile de PowerShell para cambiar la categoría entre *privada* y *pública*.

Reglas de Firewall de Windows

En muchos casos, un primer paso para los administradores es personalizar los perfiles de firewall mediante *reglas de firewall* para que puedan trabajar con aplicaciones u otros tipos de software. Por ejemplo, un administrador o usuario puede optar por agregar una regla para dar cabida a un programa, abrir un puerto o protocolo o permitir un tipo predefinido de tráfico.

Precedencia de reglas para las reglas de entrada

En muchos casos, se requiere permitir tipos específicos de tráfico entrante para que las aplicaciones funcionen en la red. Los administradores deben tener en cuenta los siguientes comportamientos de precedencia de reglas al configurar las excepciones entrantes:

1. Las reglas de permiso definidas explícitamente tienen prioridad sobre la configuración de bloque predeterminada
2. Las reglas de bloque explícitas tienen prioridad sobre las reglas de permiso en conflicto
3. Las reglas más específicas tienen prioridad sobre las reglas menos específicas, excepto si hay reglas de bloque explícitas como se menciona en 2. Por ejemplo, si los parámetros de la regla 1 incluyen un intervalo de direcciones IP, mientras que los parámetros de la regla 2 incluyen una única dirección HOST IP, la regla 2 tiene prioridad.

Debido a 1 y 2, al diseñar un conjunto de directivas, debe asegurarse de que no haya otras reglas de bloque explícitas que puedan superponerse involuntariamente, lo que impide el flujo de tráfico que desea permitir.

Nota

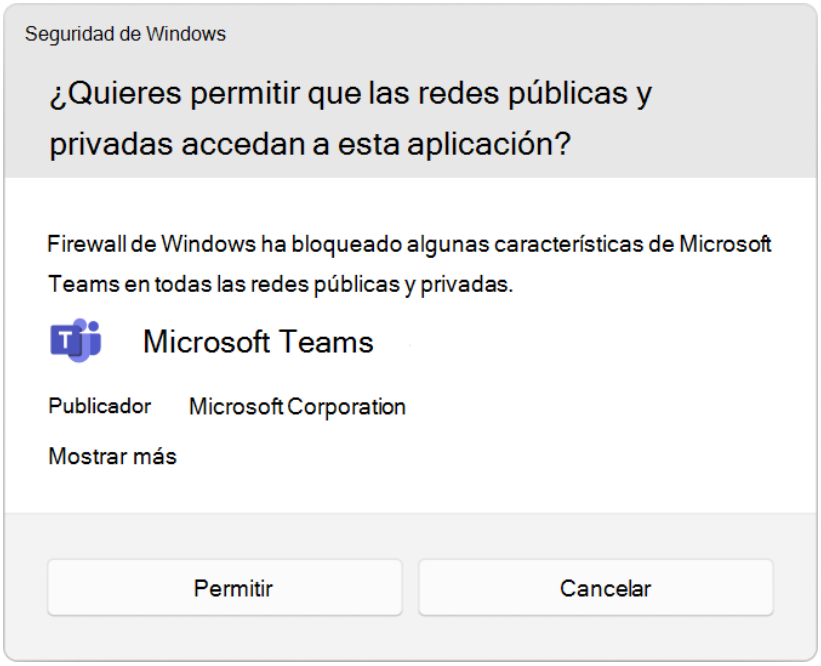
Firewall de Windows no admite el orden de reglas ponderado y asignado por el administrador. Se puede crear un conjunto de directivas efectivo con comportamientos esperados teniendo en cuenta los pocos comportamientos de reglas lógicas, coherentes y como se describe.

Reglas de aplicaciones

Cuando se instalan por primera vez, las aplicaciones de red y los servicios emiten una *llamada de escucha* que especifica la información de protocolo o puerto necesaria para que funcionen correctamente. Dado que hay una acción de *bloque* predeterminada en Firewall de Windows, debe crear reglas de excepción de entrada para permitir el tráfico. Es habitual que la aplicación o el propio instalador de la aplicación agreguen esta regla de firewall. De lo contrario, el usuario (o el administrador de firewall en nombre del usuario) debe crear manualmente una regla.

Si no hay ninguna aplicación activa o reglas de permiso definidas por el administrador, un cuadro de diálogo solicita al usuario que permita o bloquee los paquetes de una aplicación la primera vez que se inicie la aplicación o intente comunicarse en la red:

- Si el usuario tiene permisos de administrador, se le pedirá. Si responden *No* o cancelan el aviso, se crean reglas de bloque. Normalmente se crean dos reglas, una para el tráfico TCP y UDP.
- Si el usuario no es un administrador local, no se le pedirá. En la mayoría de los casos, se crean reglas de bloque



En cualquiera de estos escenarios, una vez agregadas las reglas, se deben eliminar para volver a generar el mensaje. Si no es así, el tráfico continúa bloqueado.

Nota

La configuración predeterminada del firewall está diseñada para la seguridad. Permitir todas las conexiones entrantes de forma predeterminada presenta la red a varias amenazas. Por lo tanto, la creación de excepciones para las conexiones entrantes desde software que no es de Microsoft debe estar determinada por desarrolladores de aplicaciones de confianza, el usuario o el administrador en nombre del usuario.

Directivas de etiquetado de App Control

Firewall de Windows admite el uso de etiquetas de app control para aplicaciones empresariales (AppID) en las reglas de firewall. Con esta funcionalidad, las reglas de Firewall de Windows se pueden limitar a una aplicación o a un grupo de aplicaciones haciendo referencia a etiquetas de proceso, sin usar la ruta de acceso absoluta ni sacrificar la seguridad. Hay dos pasos para esta configuración:

1. Implementar *directivas de etiquetado de AppId de App Control*: se debe implementar una directiva de App Control para empresas, que especifica aplicaciones individuales o grupos de aplicaciones para aplicar una *etiqueta PolicyAppId* a los tokens de proceso. A continuación, el administrador puede definir reglas de firewall que tienen como ámbito todos los procesos etiquetados con el *PolicyAppId* coincidente. Para obtener más información, consulte la guía de etiquetado appId de App Control para crear, implementar y probar una directiva de AppID para etiquetar aplicaciones.
2. Configure reglas de firewall mediante *etiquetas PolicyAppId* mediante uno de los dos métodos:
    - Usar el nodo PolicyAppId del CSP de firewall con una solución MDM como Microsoft Intune. Si usa Microsoft Intune, puede implementar las reglas desde Microsoft Intune Administración centro, en la ruta de acceso**Firewall**> de **seguridad**> de punto de conexión**Crear directiva**>**Windows 10, Windows 11 y Windows windows de Windows Server**> **Reglas de firewall**. Al crear las reglas, proporcione la *etiqueta AppId* en la configuración **De id. de aplicación de** directiva.
    - Crear reglas de firewall locales con PowerShell: use el New-NetFirewallRule cmdlet y especifique el -PolicyAppId parámetro. Puede especificar una etiqueta a la vez al crear reglas de firewall. Se admiten varios identificadores de usuario

Combinación de directivas locales y reglas de aplicación

La configuración de la directiva de combinación de reglas controla cómo se pueden combinar las reglas de diferentes orígenes de directiva. Los administradores pueden configurar diferentes comportamientos de combinación para perfiles *de dominio*, *privado* y *público*.

La configuración de la directiva de combinación de reglas permite o impide que los administradores locales creen sus propias reglas de firewall, además de las que se obtienen de CSP (Cloud Solution Provider) o GPO (Group Policy Object)

Expandir tabla

	Ruta de acceso
CSP	Perfil de dominio: ./Vendor/MSFT/Firewall/MdmStore/DomainProfile/AllowLocalPolicyMerge AllowLocalPolicyMerge de perfil./Vendor/MSFT/Firewall/MdmStore/PrivateProfile/ privado AllowLocalPolicyMerge del perfil ./Vendor/MSFT/Firewall/MdmStore/PublicProfile/ público
GPO	**Configuración del**> equipo**Configuración de**> Windows**Configuración de**> seguridad**Firewall de Windows Defender con seguridad avanzada**

Los administradores pueden deshabilitar *LocalPolicyMerge* en entornos de alta seguridad para mantener un control más estricto sobre los puntos de conexión. Esta configuración puede afectar a algunas aplicaciones y servicios que generan automáticamente una directiva de firewall local tras la instalación.

Importante

Si la combinación de directivas locales está deshabilitada, se requiere la implementación centralizada de reglas para cualquier aplicación que necesite conectividad de entrada.

Es importante crear y mantener una lista de estas aplicaciones, incluidos los puertos de red que se usan para las comunicaciones. Normalmente, puede encontrar qué puertos deben estar abiertos para un servicio determinado en el sitio web de la aplicación. Para implementaciones más complejas, podría ser necesario realizar un análisis exhaustivo mediante herramientas de captura de paquetes de red.

En general, para mantener la máxima seguridad, los administradores solo deben implementar excepciones de firewall para aplicaciones y servicios determinados para servir con fines legítimos.

Nota

El uso de patrones comodín, como C:*\teams.exe no se admite en las reglas de aplicación. Solo puede crear reglas mediante la ruta de acceso completa a las aplicaciones.

Recomendaciones de reglas de firewall

Esta es una lista de recomendaciones al diseñar las reglas de firewall:

- Mantenga la configuración predeterminada del Firewall de Windows siempre que sea posible. La configuración está diseñada para proteger el dispositivo para su uso en la mayoría de los escenarios de red. Un ejemplo clave es el *comportamiento de bloque* predeterminado para las conexiones entrantes.
- Cree las reglas en los tres perfiles, pero habilite solo el grupo de reglas de firewall en los perfiles que se adapten a sus escenarios. Por ejemplo, si va a instalar una aplicación de uso compartido que solo se usa en una red privada, sería mejor crear reglas de firewall en los tres perfiles, pero habilitar solo el grupo de reglas de firewall que contiene las reglas en el perfil privado.
- Configure las restricciones en las reglas de firewall en función del perfil al que se apliquen las reglas. En el caso de aplicaciones y servicios diseñados para que solo puedan acceder los dispositivos de una red doméstica o de pequeña empresa, es mejor modificar la restricción de direcciones remotas para especificar solo *la subred local* . La misma aplicación o servicio no tendría esta restricción cuando se usa en un entorno empresarial. Para ello, agregue la restricción de direcciones remotas a las reglas que se agregan a los perfiles privados y públicos, al tiempo que las deja sin restricciones en el perfil de dominio. Esta restricción de direcciones remotas no debe aplicarse a aplicaciones o servicios que requieran conectividad global a Internet.
- Una práctica recomendada de seguridad general al crear reglas de entrada es ser lo más específica posible. Sin embargo, cuando se deben realizar nuevas reglas que usen puertos o direcciones IP, considere la posibilidad de usar intervalos o subredes consecutivos en lugar de direcciones individuales o puertos siempre que sea posible. Este enfoque evita la creación de varios filtros bajo el capó, reduce la complejidad y ayuda a evitar la degradación del rendimiento.
- Al crear una regla de entrada o salida, debe especificar detalles sobre la propia aplicación, el intervalo de puertos utilizado y notas importantes como la fecha de creación. Las reglas deben estar bien documentadas para facilitar su revisión tanto por usted como por otros administradores.

- Para mantener la máxima seguridad, los administradores solo deben implementar excepciones de firewall para aplicaciones y servicios determinados para servir con fines legítimos.

Problemas conocidos con la creación automática de reglas

Al diseñar un conjunto de directivas de firewall para la red, se recomienda configurar *reglas de permiso* para las aplicaciones en red implementadas en el host. Tener las reglas en su lugar antes de que el usuario inicie por primera vez la aplicación ayuda a garantizar una experiencia sin problemas.

La ausencia de estas reglas almacenadas provisionalmente no significa necesariamente que, al final, una aplicación no pueda comunicarse en la red. Sin embargo, los comportamientos implicados en la creación automática de reglas de aplicación en tiempo de ejecución requieren la interacción del usuario y privilegios administrativos. Si se espera que los usuarios no administrativos usen el dispositivo, debe seguir los procedimientos recomendados y proporcionar estas reglas antes del primer inicio de la aplicación para evitar problemas de red inesperados.

Para determinar por qué algunas aplicaciones no se comunican en la red, compruebe las siguientes instancias:

1. Un usuario con privilegios suficientes recibe una notificación de consulta que le informa de que la aplicación necesita realizar un cambio en la directiva de firewall. Al no comprender completamente el aviso, el usuario cancela o descarta el aviso.
2. Un usuario carece de privilegios suficientes y, por tanto, no se le pide que permita a la aplicación realizar los cambios de directiva adecuados.
3. La combinación de directivas locales está deshabilitada, lo que impide que la aplicación o el servicio de red creen reglas locales.

Los administradores también pueden prohibir la creación de reglas de aplicación en tiempo de ejecución mediante la configuración de directivas o la aplicación configuración.

Consideraciones sobre reglas de salida

A continuación, se indican algunas directrices generales para configurar las reglas de salida.

- El cambio de las reglas de salida a *bloqueadas* se puede tener en cuenta para determinados entornos de alta seguridad. Sin embargo, la configuración de la regla de entrada nunca debe cambiarse de forma que permita todo el tráfico de forma predeterminada.
- Se recomienda *permitir la salida* de forma predeterminada para la mayoría de las implementaciones con el fin de simplificar las implementaciones de

aplicaciones, a menos que la organización prefiera controles de seguridad estrictos sobre la facilidad de uso.

- En entornos de alta seguridad, se debe registrar y mantener un inventario de todas las aplicaciones. Los registros deben incluir si una aplicación usada requiere conectividad de red. Los administradores deben crear nuevas reglas específicas para cada aplicación que necesite conectividad de red e insertar esas reglas de forma centralizada, a través de GPO o CSP.