Soluciones Windows Microsoft para Firewall (200fwdz)

Introducción

Tanto en Windows 11 como en Windows Server 2025 integran herramientas y componentes que permiten configurar un firewall y, hasta cierto punto, funcionar como un "firewall router" para gestionar tráfico LAN y WAN. Este documento enumera las opciones más relevantes de este tipo de soluciones actuales (23/03/2025) de tecnología Microsoft.

1. Windows Defender Firewall con seguridad avanzada

Este componente está presente tanto en Windows 11 como en Windows Server 2025. Esta solución, ofrece filtrado avanzado de paquetes y reglas de seguridad tanto para redes entrantes como salientes. Sin embargo, está diseñado más para proteger al propio sistema operativo que para actuar como firewall de borde o enrutador para toda una red.

Pros: Fácil de configurar desde la consola gráfica (`wf.msc`) o mediante *PowerShell*.

Contras: No tiene capacidad de enrutamiento NAT avanzado como se esperaría en un firewall dedicado.

2. RRAS (Routing and Remote Access Service)

Exclusivo para las ediciones Server (Windows Server 2025). RRAS permite configurar un servidor como un router y firewall básico. Soporta NAT (Network Address Translation), VPN y enrutamiento dinámico estático y RIP.

Pros:

- Soporte para VPN y NAT.
- Se puede gestionar a través de la GUI o PowerShell (`Add-WindowsFeature -Name RemoteAccess, Routing`).

Contras:

- Es menos potente y flexible comparado con soluciones dedicadas a firewall (como pf, iptables, firewalld, etc).
- Configuración más compleja para integrarse con entornos no Windows.

3. IPSec

Aunque IPSec está diseñado para asegurar el tráfico de red mediante túneles seguros, se puede combinar con *Windows Defender Firewall* para crear reglas avanzadas de filtrado de tráfico.

Pros:

- Alta seguridad y encriptación para conexiones específicas.

Contras:

- No es una solución de firewall router propiamente dicha, sino más bien para asegurar el tráfico de red.

4. PowerShell y scripts avanzados

Para escenarios complejos, puedes automatizar y ampliar las capacidades de firewall y enrutamiento con ***PowerShell*** y scripts personalizados. El módulo ***NetSecurity*** y ***cmdlets*** como `New-NetFirewallRule` permiten gestionar reglas de firewall avanzadas.

Pros:

- Alto control y capacidad de automatización.

Contras:

- Se requiere conocimiento avanzado y pruebas rigurosas para evitar problemas de conectividad.

¿Es viable usar Windows como firewall router en entornos de producción?

> En entornos pequeños o de laboratorio sí puede funcionar bien, especialmente si ya se tiene un servidor Windows desplegado y se pretende aprovechar.
>
> Para entornos medianos o grandes con demandas complejas de seguridad y enrutamiento, es preferible usar soluciones dedicadas sean basadas en software o mejor aún en hardware especializado.