Índice:

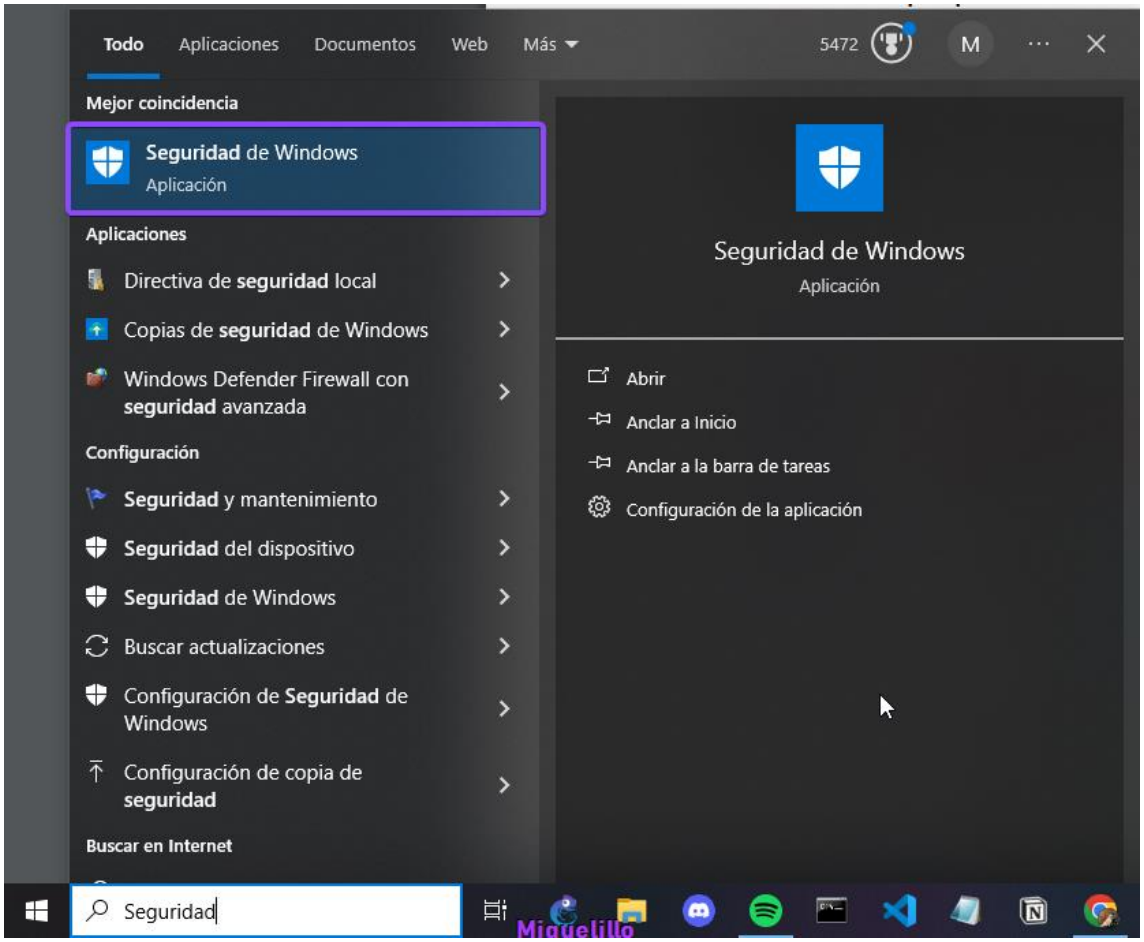
Informe sobre el uso de Firewall en Windows

a) Microsoft Defender

Solución:

El Firewall de Windows es una herramienta crucial para la seguridad de los sistemas operativos, Windows trae integrado uno propio por defecto. Su función principal es proteger la red y el sistema contra amenazas externas, controlando el tráfico de red entrante y saliente. Su configuración adecuada y el seguimiento regular son esenciales para garantizar una protección efectiva contra amenazas externas.

Para acceder a él vamos a **Seguridad de Windows**



Una vez aquí podemos ver el estado de los distintos perfiles para firewalls predeterminados que existen

- **Perfil de Red Pública:**

  Cuando se Utiliza: Cuando el dispositivo se conecta a una red pública, como en cafeterías, aeropuertos o redes Wi-Fi abiertas.

  Configuración Predeterminada: Este perfil generalmente establece configuraciones ***más restrictivas*** para proteger el dispositivo de posibles amenazas en entornos públicos.

- **Perfil de Red Privada:**

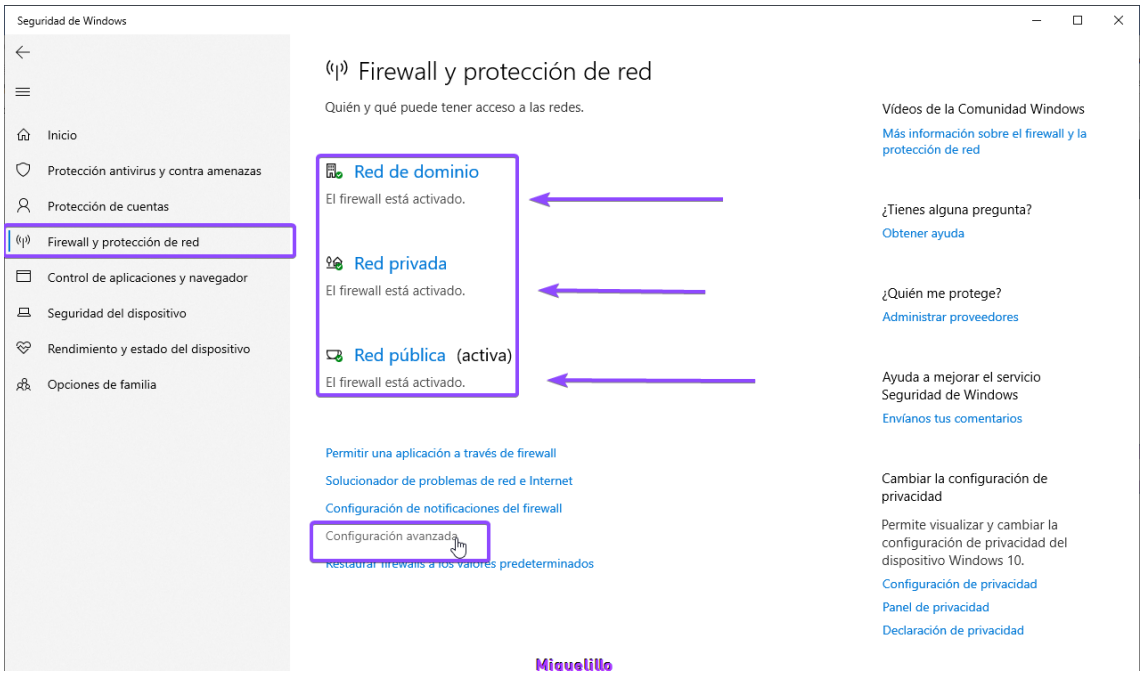
  Cuando se Utiliza: Cuando el dispositivo se conecta a una red doméstica o de oficina.

  Configuración Predeterminada: Este perfil es ***más permisivo*** en comparación con el perfil público, ya que se asume que las redes privadas son más seguras. Permite una mayor visibilidad y accesibilidad entre dispositivos en la misma red.

- **Perfil de Red de Dominio:**

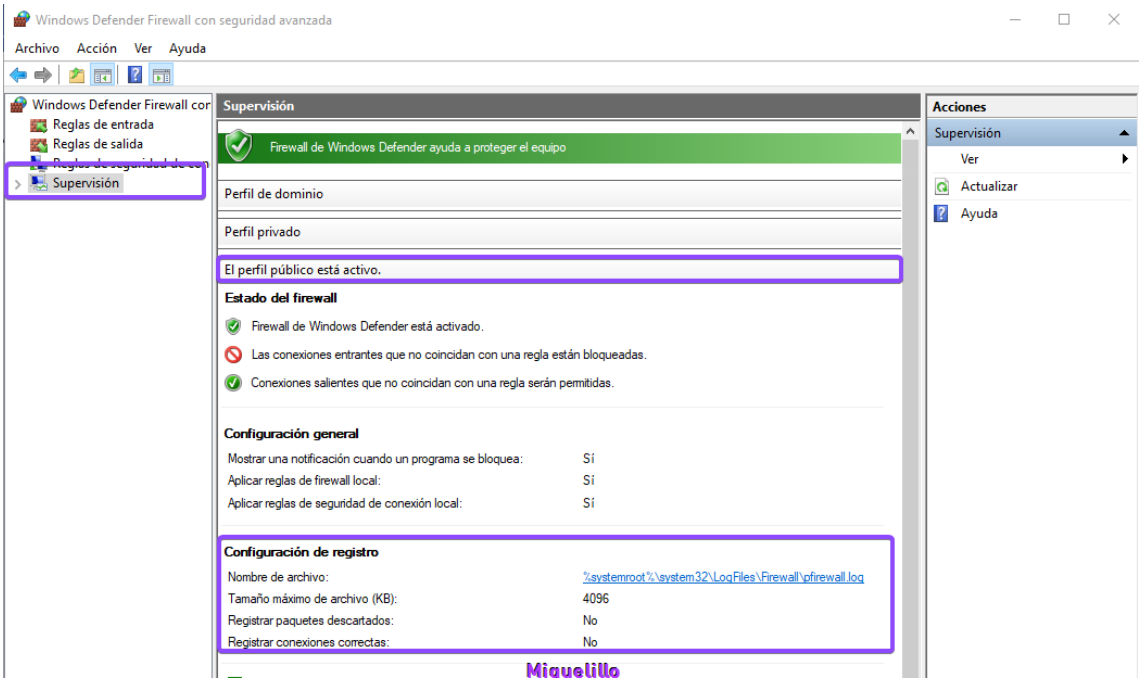
  Cuando se Utiliza: En entornos de red de dominio, donde el dispositivo forma parte de un dominio de Active Directory.

  Configuración Predeterminada: Este perfil se aplica cuando el dispositivo está conectado a un dominio de red controlado por un servidor de dominio. ***Permite configuraciones específicas definidas por el administrador de red***.

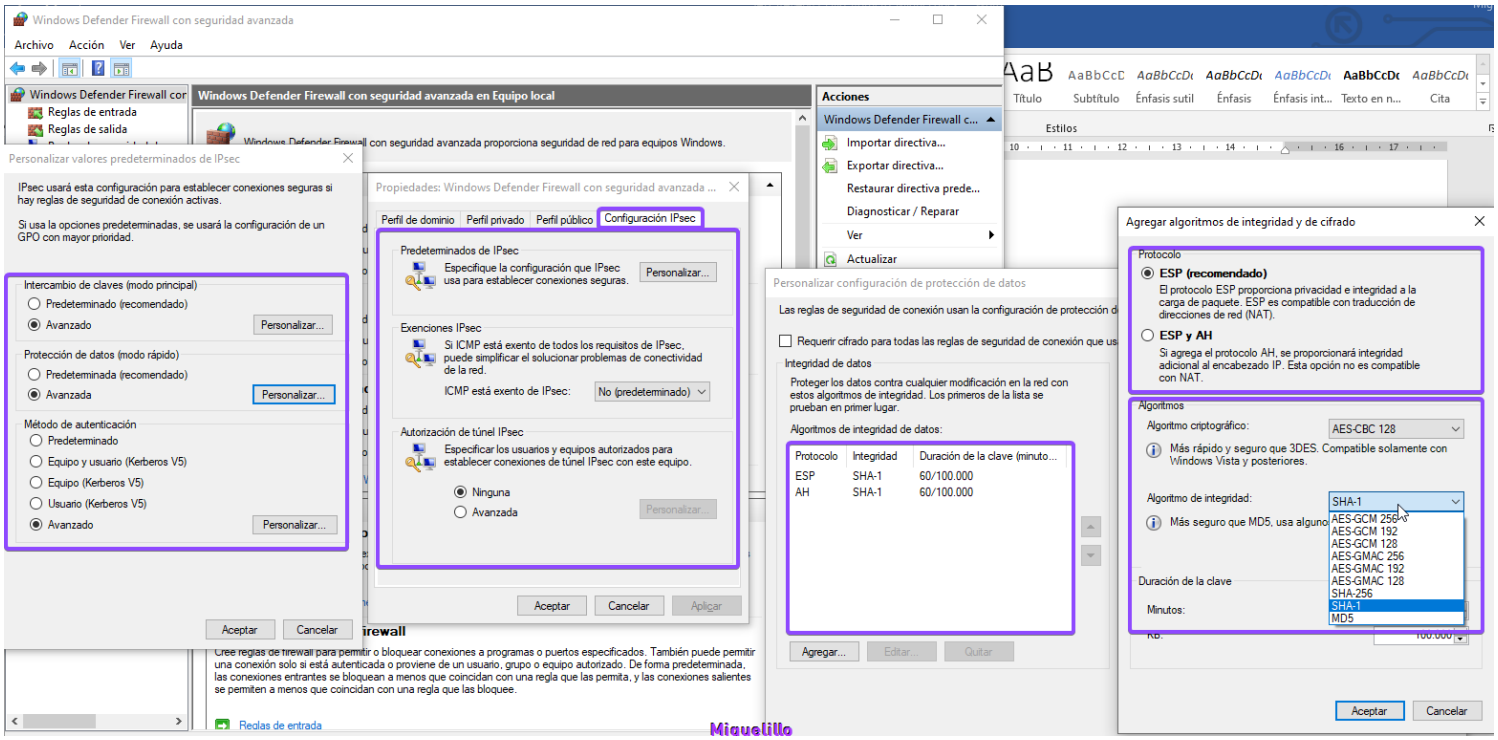


Para configurarlos vamos a **Configuración avanzada**. Aquí podemos ver y crear reglas tanto de entrada cómo de salida

También podemos ver que perfil de firewall estamos utilizando actualmente y el registro.



Hay una opción para poder personalizar el firewalll cuando usamos Ipsec donde le indicamos los protocolos que vamos a utilizar



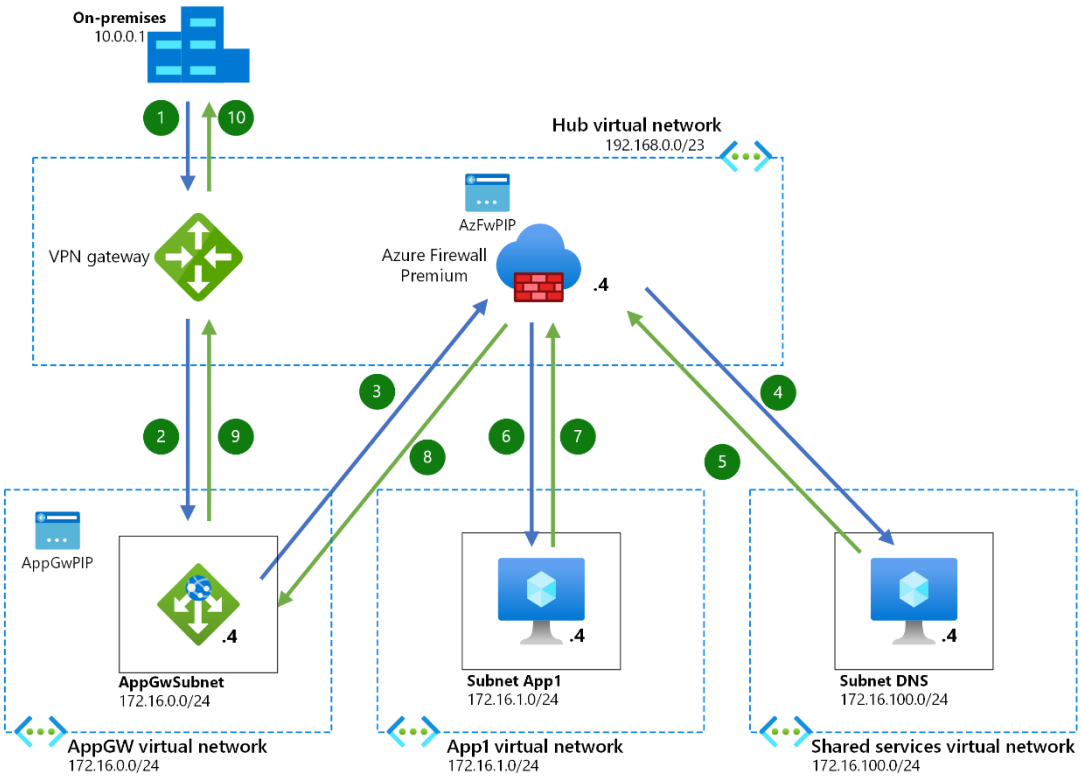
b) Azure Firewall

Solución:

Azure Firewall es un servicio de seguridad en la nube de Microsoft diseñado para proteger las redes virtuales en Azure.Puede examinar el tráfico a nivel de aplicación, permitiendo o bloqueando según nombres de dominio o categorías de aplicaciones. Incorpora inteligencia de amenazas de Microsoft para detectar y bloquear actividades maliciosas.

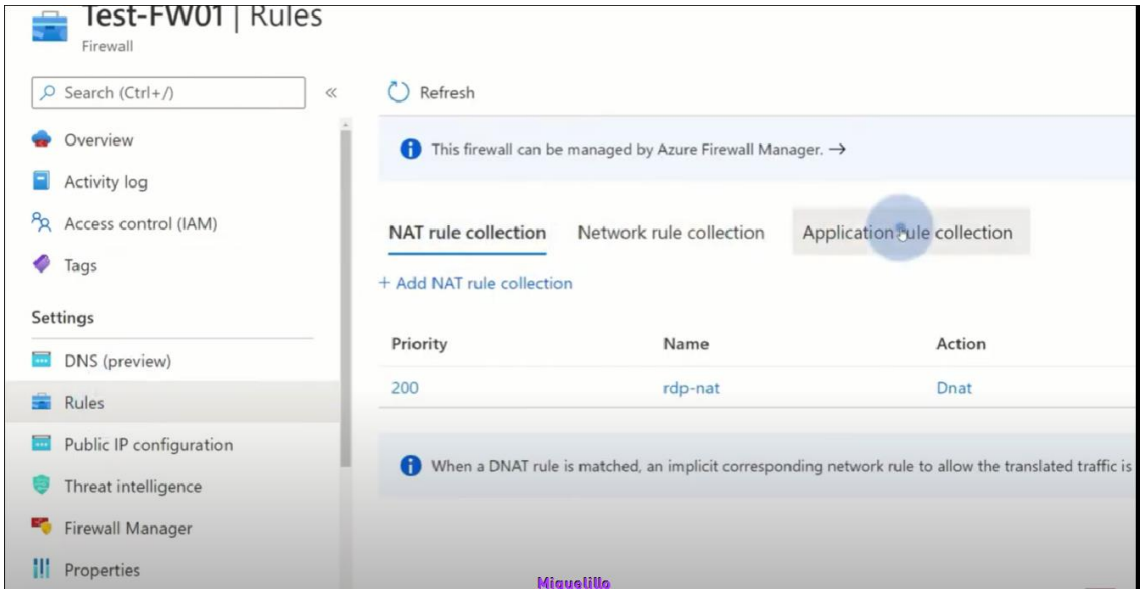
Funcionamiento:

- Un recurso en la VNet intenta enviar o recibir datos.
- El tráfico pasa a través de Azure Firewall.
- Azure Firewall aplica reglas de seguridad para determinar si se permite o se bloquea el tráfico.
- El tráfico permitido continúa su ruta normal, mientras que el tráfico bloqueado se detiene.

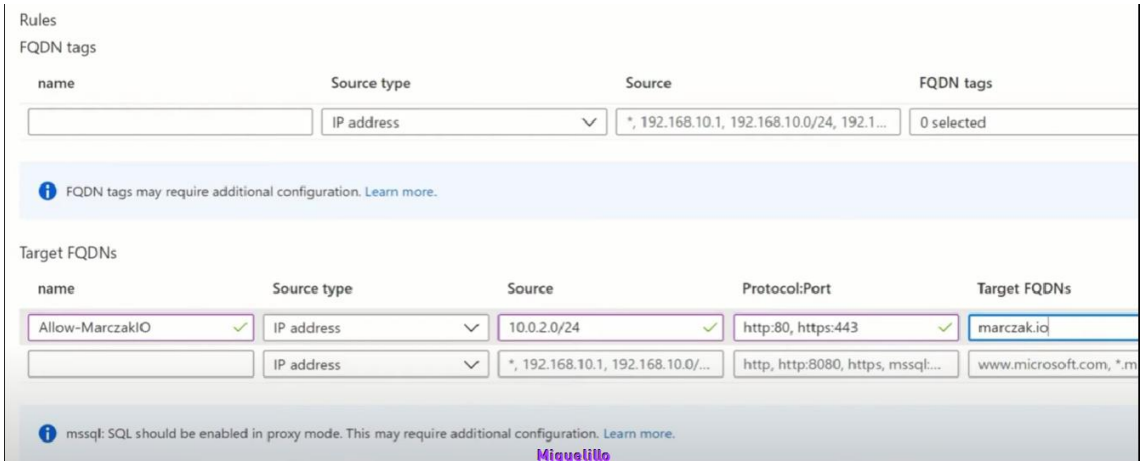


Microsoft Azure

En **Rules** podemos añadir diferentes reglas



Formato de las reglas



Los precios de este servicio son los siguientes: