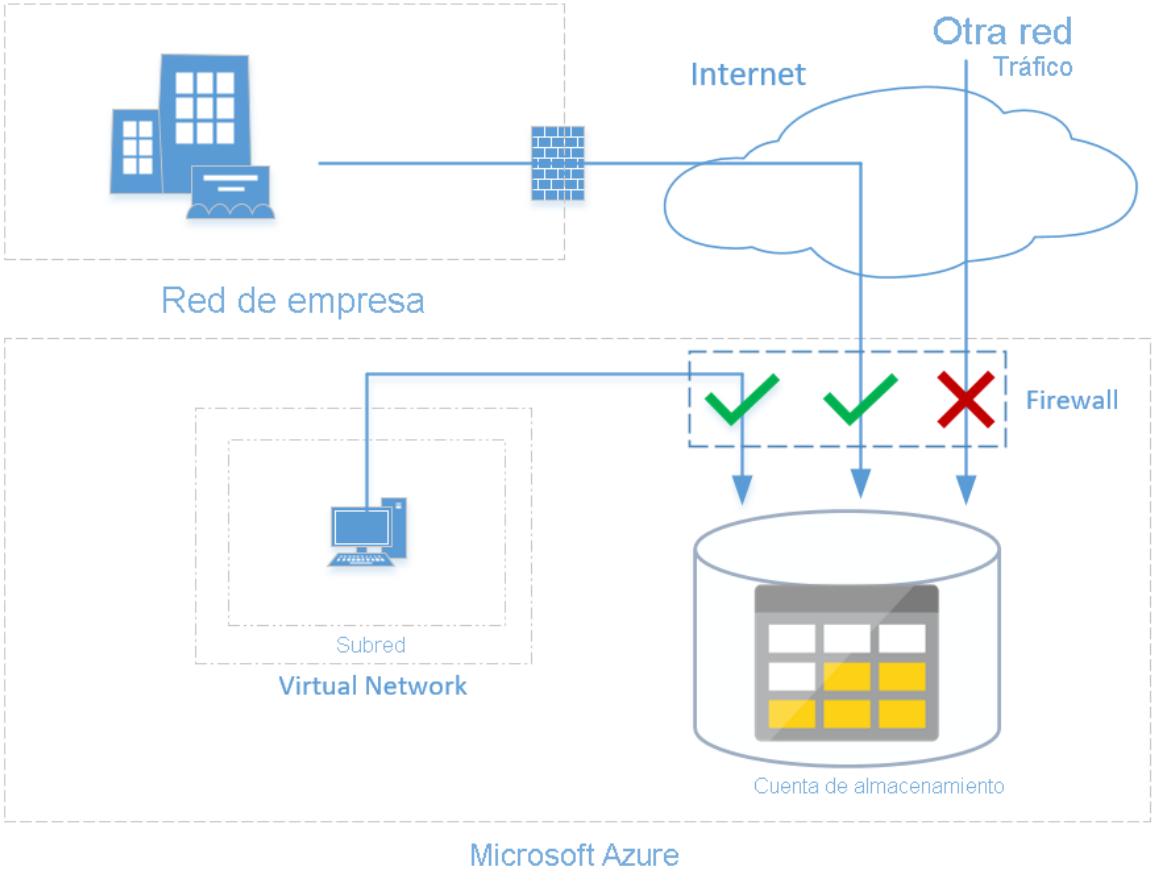
Exploración de las características de Azure Firewall

Azure Firewall es un servicio de seguridad de red administrado y basado en la nube que protege los recursos de red virtual de Azure. Se trata de un firewall como servicio con estado completo que incorpora alta disponibilidad y escalabilidad a la nube sin restricciones. Azure Firewall bloquea el tráfico de manera predeterminada.



Qué incluyen las características de Azure Firewall

- **Alta disponibilidad integrada**: como la alta disponibilidad está integrada, no se requieren equilibradores de carga adicionales ni tampoco es necesario configurar nada.
- **Escalabilidad sin restricciones en la nube**: Azure Firewall puede escalarse verticalmente todo lo que sea necesario para acoger los flujos de tráfico cambiantes, por lo que no necesita elaborar un presupuesto para el tráfico en su momento máximo.
- **Reglas de filtrado de nombre de dominio completo (FQDN) de aplicación**: puede limitar el tráfico HTTP/S saliente a una lista especificada de FQDN, incluidos caracteres comodín. Esta característica no requiere terminación de SSL.
- **Reglas de filtrado de tráfico**: puede crear reglas de filtrado de red para permitir o denegar por dirección IP de origen y destino, puerto y protocolo. Azure Firewall tiene estado

completo, de modo que puede distinguir los paquetes legítimos de diferentes tipos de conexiones. Las reglas se aplican y se registran en varias suscripciones y redes virtuales.

- **Etiquetas de dominio calificados**: las etiquetas de nombres de dominio completos (FQDN) facilitan la tarea de permitir el tráfico del servicio de Azure conocido a través del firewall. Por ejemplo, supongamos que quiere permitir el tráfico de red de Windows Update a través del firewall. Puede crear una regla de aplicación e incluir la etiqueta de Windows Update. Ahora, el tráfico de red de Windows Update puede fluir a través del firewall.
- **Compatibilidad con la traducción de direcciones de red de origen saliente (OSNAT)**: todas las direcciones IP del tráfico de red virtual saliente se traducen a la IP pública de Azure Firewall. Puede identificar y permitir el tráfico procedente de la red virtual a destinos de Internet remotos.
- **Compatibilidad con la traducción de direcciones de red de destino (DNAT) entrante**: el tráfico entrante a la IP pública del firewall se traduce y se filtra a las direcciones IP privadas en las redes virtuales.
- **Registro de Azure Monitor**: todos los eventos se integran en Azure Monitor, lo que permite archivar registros en una cuenta de almacenamiento, transmitir eventos al centro de eventos o enviarlos a los registros de Azure Monitor.

Agrupar las características anteriores en grupos lógicos revela que Azure Firewall tiene tres tipos de reglas: **reglas NAT**, **reglas de red** y **reglas de aplicación**. La prioridad del orden de las aplicaciones para las reglas es que se aplican primero las reglas de red y, a continuación, las de aplicación. Las reglas son de finalización, es decir, si se encuentra una coincidencia en las reglas de red, no se procesan las reglas de aplicación. Si no hay ninguna coincidencia de reglas de red y el protocolo de paquetes es HTTP/HTTPS, las reglas de aplicación evalúan el paquete. Si no se encuentra ninguna coincidencia, el paquete se evalúa en función de la colección de reglas de infraestructura. Si todavía no hay ninguna coincidencia, el paquete se deniega de manera predeterminada.

Reglas NAT

Puede configurar la conectividad de entrada mediante la configuración de la traducción de direcciones de red de destino (DNAT), tal como se describe en Filtrado del tráfico entrante con DNAT de Azure Firewall mediante Azure Portal. Las reglas de DNAT son las primeras que se aplican. Si se encuentra alguna coincidencia, se agrega una regla de red correspondiente implícita para permitir el tráfico traducido. Para invalidar este comportamiento, agregue explícitamente una colección de reglas de red con reglas de denegación que coinciden con el tráfico traducido. No se aplican reglas de aplicación a estas conexiones.

Reglas de firewall para proteger Azure Storage

Azure Storage proporciona un modelo de seguridad en capas, el que le permite proteger las cuentas de almacenamiento en un conjunto específico de redes admitidas. Cuando se configuran las reglas de red, solo las aplicaciones que solicitan datos del conjunto especificado de redes pueden acceder a una cuenta de almacenamiento.

Una aplicación que accede a una cuenta de almacenamiento cuando las reglas de red están en vigor requiere la autorización adecuada en la solicitud. La autorización es compatible con las credenciales de Azure AD para blobs y colas, una clave de acceso de cuenta válida o un token de SAS.

De forma predeterminada, las cuentas de almacenamiento aceptan conexiones de clientes en cualquier red. Para limitar el acceso a redes seleccionadas, primero debe cambiar la acción predeterminada. La realización de cambios en reglas de red puede afectar a la capacidad de las aplicaciones de conexión a Azure Storage. Si se establece la regla de red predeterminada en Denegar, se bloquea el acceso a los datos, a menos que se apliquen también las reglas de red específicas para conceder acceso. Asegúrese de conceder acceso a las redes permitidas con reglas de red antes de cambiar la regla predeterminada para denegar el acceso.

Concesión de acceso desde una red virtual

Puede configurar las cuentas de almacenamiento para permitir el acceso solo desde redes virtuales específicas.

Se habilita un punto de conexión de servicio para Azure Storage dentro de la red virtual. Este punto de conexión proporciona al tráfico una ruta óptima hasta el servicio de Azure Storage. Las identidades de la red virtual y la subred también se transmiten con cada solicitud. Luego, los administradores pueden configurar reglas de red para la cuenta de almacenamiento que permitan que se reciban solicitudes desde subredes específicas en la red virtual. Los clientes a los que se concedió acceso a través de estas reglas de red deben seguir cumpliendo los requisitos de autorización de la cuenta de almacenamiento para acceder a los datos.

Cada cuenta de almacenamiento admite hasta 100 reglas de red virtual, que se pueden combinar con reglas de red IP.

Controlar el acceso de red saliente y entrante es una parte importante de un plan de seguridad de red general. El tráfico está sujeto a las reglas de firewall configuradas cuando se enruta al firewall, como la puerta de enlace predeterminada