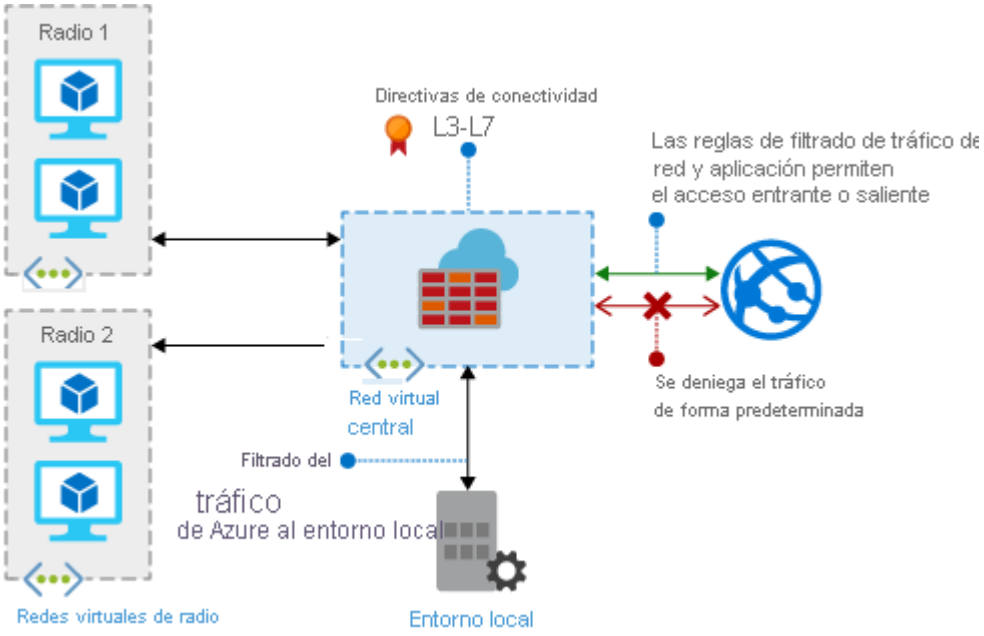
Implementación de Azure Firewall

El control del acceso de red saliente es una parte importante de un plan de seguridad de red de ámbito general. Por ejemplo, es posible que desee limitar el acceso a sitios web. O bien, que desee limitar las direcciones IP de salida y los puertos a los que se puede acceder.

Una manera de controlar el acceso de red saliente desde una subred de Azure es con Azure Firewall. Con Azure Firewall, puede configurar:

- Reglas de aplicación que definen los nombres de dominio completos (FQDN) a los que se puede acceder desde una subred.
- Reglas de red que definen la dirección de origen, el protocolo, el puerto de destino y la dirección de destino.

El tráfico está sujeto a las reglas de firewall configuradas cuando enruta el tráfico al firewall como puerta de enlace predeterminada de la subred.



Etiqueta de nombre de dominio completo (FQDN)

Una etiqueta FQDN representa un grupo de nombres de dominio completo (FQDN) asociados con los servicios de Microsoft conocidos. Puede usar una etiqueta FQDN en las reglas de una aplicación para permitir que pase el tráfico de red saliente necesario a través del firewall.

Por ejemplo, para permitir manualmente el tráfico de red de **Windows Update** a través del firewall, debe crear varias reglas de aplicación según la documentación de Microsoft. Si usa etiquetas FQDN, puede crear una regla de aplicación e incluir la etiqueta Windows Update

para que el tráfico de red que apunta a los puntos de conexión de Windows Update pueda fluir a través del firewall.

Nombres de dominio completos de infraestructura

Azure Firewall incluye una colección de reglas integradas para FQDN de infraestructura que están permitidos de forma predeterminada. Estos FQDN son específicos para la plataforma y no se pueden usar para otros fines.

En la colección integrada de reglas se incluyen los siguientes servicios:

- Acceso de proceso al repositorio de imágenes de la plataforma (PIR) de almacenamiento
- Acceso al almacenamiento de estado de los discos administrados
- Azure Diagnostics y registro (MDS)

Registros y métricas

Puede supervisar Azure Firewall mediante los registros del firewall. También puede usar los registros de actividad para auditar las operaciones de los recursos de Azure Firewall.

Se puede acceder a algunos de estos registros mediante el portal. Se pueden enviar registros a los registros de Azure Monitor, a Storage y a Event Hubs, y se pueden analizar en los registros de Azure Monitor o mediante otras herramientas como Excel y Power BI.

Las métricas son ligeras y pueden admitir escenarios casi en tiempo real, lo que las hace útiles para alertas y detección rápida de problemas.

Filtrado basado en inteligencia sobre amenazas

El filtrado basado en inteligencia sobre amenazas puede habilitarse para que el firewall alerte y deniegue el tráfico desde y hacia los dominios y las direcciones IP malintencionados. La direcciones IP y los dominios proceden de la fuente Inteligencia sobre amenazas de Microsoft. Intelligent Security Graph impulsa la Inteligencia sobre amenazas de Microsoft y lo utilizan numerosos servicios, incluido Microsoft Defender for Cloud. Si ha habilitado el filtrado basado en inteligencia sobre amenazas, las reglas asociadas se procesan antes que cualquiera de las reglas NAT, reglas de red o reglas de aplicación.

Puede optar por registrar solo una alerta cuando se desencadena una regla o puede elegir el modo de alerta y denegación. De forma predeterminada, el filtrado basado en inteligencia sobre amenazas está habilitado en el modo de alerta.

Lógica de procesamiento de reglas

Puede configurar reglas NAT, reglas de red y reglas de aplicaciones en Azure Firewall. Las colecciones de reglas se procesan según el tipo de regla en orden de prioridad, de números inferiores a números mayores desde 100 hasta 65 000. El nombre de una colección de reglas solo puede contener letras, números, guiones bajos, puntos o guiones. Debe comenzar con una letra o un número y terminar con una letra, un número o un guión bajo. La longitud máxima del nombre es de 80 caracteres.

Es mejor espaciar inicialmente los números de prioridad de la colección de reglas en incrementos de 100 (100, 200, 300, etc.) para disponer de espacio para agregar más colecciones de reglas si es necesario.

Etiquetas de servicio

Una etiqueta de servicio representa un grupo de prefijos de direcciones IP que ayudan a reducir la complejidad de la creación de reglas de seguridad. No puede crear su propia etiqueta de servicio, ni especificar qué direcciones IP se incluyen dentro de una etiqueta. Microsoft administra los prefijos de direcciones que incluye la etiqueta de servicio y actualiza automáticamente esta a medida que las direcciones cambian.

Las etiquetas de servicio de Azure Firewall se pueden usar en el campo de destino de las reglas de red. Puede usarlas en lugar de direcciones IP específicas.

Soporte para el trabajo remoto

VDI

Las directivas de trabajo desde casa requieren que muchas organizaciones de TI aborden cambios fundamentales en relación con la capacidad, la red, la seguridad y la gobernanza. Los empleados no están protegidos por directivas de seguridad por niveles asociadas a servicios locales cuando trabajan desde casa. Las implementaciones de Infraestructura de escritorio virtual (VDI) en Azure pueden ayudar a las organizaciones a responder rápidamente a este entorno cambiante. Sin embargo, necesita una forma de proteger el acceso a Internet entrante o saliente a y desde estas implementaciones de VDI. Puede usar las reglas de DNAT de Azure Firewall junto con sus funcionalidades de filtrado basado en inteligencia sobre amenazas para proteger las implementaciones de VDI.

Compatibilidad con Virtual Desktop

Windows Virtual Desktop es un servicio completo de virtualización de escritorio y de aplicaciones que se ejecuta en Azure. Es la única infraestructura de escritorio virtual (VDI) que ofrece administración simplificada, Windows 10 de varias sesiones, optimizaciones para Microsoft 365 ProPlus y compatibilidad con entornos de Servicios de Escritorio remoto (RDS). Puede implementar y escalar sus aplicaciones y escritorios de Windows en

Azure en cuestión de minutos y obtener características integradas de seguridad y cumplimiento. Windows Virtual Desktop no requiere que abra ningún acceso de entrada a la red virtual. Sin embargo, debe permitir un conjunto de conexiones de red de salida para las máquinas virtuales con Windows Virtual Desktop que se ejecutan en la red virtual.