**Introducción**

Los grupos de seguridad de red son una manera de limitar el tráfico de red a los recursos de la red virtual. Los grupos de seguridad de red contienen reglas de seguridad que permiten o deniegan el tráfico de red entrante o saliente.

Supongamos que su empresa tiene varias ubicaciones y quiere migrar a una solución basada en la nube. La empresa soloconsidera la posibilidad de migrar los sistemas clave a la plataforma en la nube si se pueden cumplir estrictos requisitos de seguridad. Entre estos, se incluye un estrecho control sobre qué equipos tienen acceso de red a los servidores de aplicaciones. Necesita proteger tanto las redes de máquinas virtuales como las de los servicios de Azure. El objetivo es impedir que el tráfico de red no seguro o no deseado pueda llegar a los sistemas clave.

En este módulo, aprenderá a crear un grupo de seguridad de red, configurar reglas de puerto de entrada y salida, y comprobar la conectividad segura.

El objetivo de este módulo es enseñar a controlar el tráfico de red con grupos de seguridad de red.

**Objetivos de aprendizaje**

En este módulo aprenderá a:

* Determinar cuándo usar grupos de seguridad de red
* Crear grupos de seguridad de red.
* Implementar y evaluar las reglas del grupo de seguridad de red.
* Describir la función de los grupos de seguridad de la aplicación.

**Requisitos previos**

* Estar familiarizado con las redes virtuales y recursos de Azure, como las máquinas virtuales.
* Conocimientos prácticos de Azure Portal, para que puede configurar los grupos de seguridad de red.
* Conocimientos básicos sobre el enrutamiento del tráfico y las estrategias de control de tráfico.

**Implementación de grupos de seguridad de red**

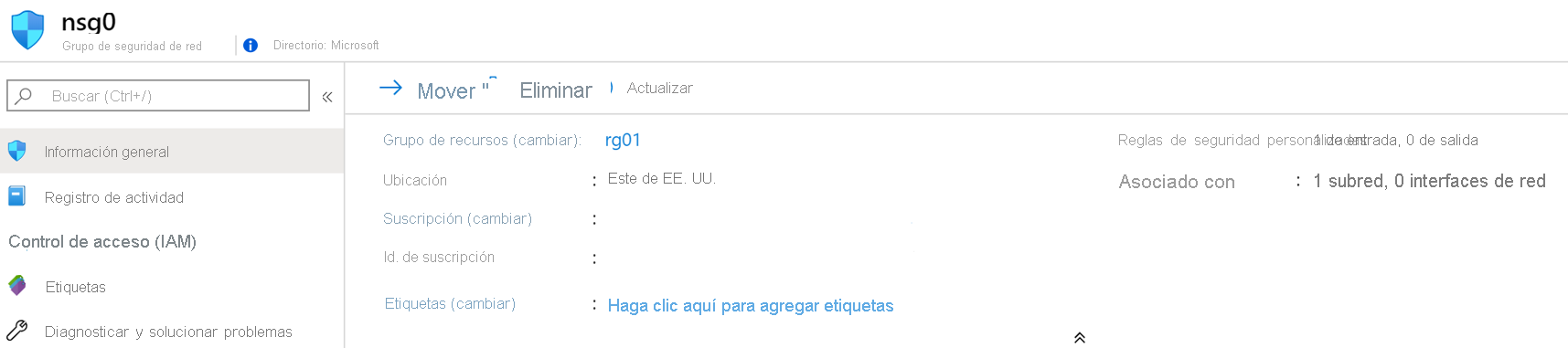
Puede limitar el tráfico de red a los recursos de una red virtual mediante un grupo de seguridad de red. Un grupo de seguridad de red se puede asignar a una subred o a una interfaz de red, y se pueden definir reglas de seguridad en el grupo para controlar el tráfico de red.

**Aspectos que saber sobre los grupos de seguridad de red**

Echemos un vistazo a las características de los grupos de seguridad de red.

* Un grupo de seguridad de red contiene reglas de seguridad que permiten o deniegan el tráfico de red entrante o saliente.
* Un grupo de seguridad de red se puede asociar a una subred o a una interfaz de red.
* Además, se puede asociar varias veces.
* El grupo de seguridad de red se crea y luego se definen reglas de seguridad en Azure Portal.

Los grupos de seguridad de red se definen para las máquinas virtuales en Azure Portal. La página **Información general** de una máquina virtual proporciona información sobre los grupos de seguridad de red asociados. Puede ver detalles como las subredes asignadas, las interfaces de red asignadas y las reglas de seguridad definidas.



**Grupos de seguridad de red y subredes**

Puede asignar grupos de seguridad de red a una subred y crear una subred filtrada protegida (también denominada zona desmilitarizada o *DMZ*). Una DMZ actúa como un búfer entre los recursos de la red virtual e Internet.

* Use el grupo de seguridad de red para restringir el flujo de tráfico a todas las máquinas que residen dentro de la subred.
* Cada subred puede tener como máximo un grupo de seguridad de red asociado.

**Grupos de seguridad de red e interfaces de red**

Puede asignar grupos de seguridad de red a una tarjeta de interfaz de red (NIC).

* Defina reglas de grupo de seguridad de red para controlar todo el tráfico que fluye a través de una NIC.
* Cada interfaz de red que existe en una subred puede tener un grupo de seguridad de red asociado o ninguno.

**Determinación de las reglas de grupo de seguridad de red**

Las reglas de seguridad de los grupos de seguridad de red permiten filtrar el tráfico de red. Puede definir reglas para controlar el flujo de tráfico dentro y fuera de las subredes de red virtual y de las interfaces de red.

**Aspectos que saber sobre las reglas de seguridad**

Vamos a revisar las características de las reglas de seguridad de los grupos de seguridad de red.

* Azure crea varias reglas de seguridad predeterminadas dentro de cada grupo de seguridad de red, incluido el tráfico entrante y el tráfico saliente. Un par de ejemplos de reglas predeterminadas son el tráfico DenyAllInbound y el tráfico AllowInternetOutbound.
* Azure crea reglas de seguridad predeterminadas en cada grupo de seguridad de red que cree.
* Para agregar más reglas de seguridad a un grupo de seguridad de red, hay que especificar las condiciones de cualquiera de las siguientes opciones:
  + **Nombre**
  + **Prioridad**
  + **Puerto**
  + **Protocolo** (Cualquiera, TCP o UDP)
  + **Origen** (Cualquiera, Direcciones IP o Etiqueta de servicio)
  + **Destino** (Cualquiera, Direcciones IP o Red virtual)
  + **Acción** (Permitir o Denegar)
* A cada regla de seguridad se le asigna un valor de prioridad. Todas las reglas de seguridad de un grupo de seguridad de red se procesan por orden de prioridad. Cuando una regla tiene un valor de prioridad bajo, la regla tiene una prioridad o prioridad más alta en términos de orden de procesamiento.
* Las reglas de seguridad predeterminadas no se pueden quitar.
* Una regla de seguridad predeterminada se puede invalidar creando otra regla de seguridad que tenga una configuración de prioridad más alta en el grupo de seguridad de red.

**Reglas de tráfico entrante**

Azure define tres reglas de seguridad de entrada predeterminadas para el grupo de seguridad de red. Estas reglas **deniegan todo el tráfico entrante**, excepto el tráfico desde la red virtual y los equilibradores de carga de Azure. En la siguiente imagen se muestran las reglas de seguridad de entrada predeterminadas de un grupo de seguridad de red en Azure Portal.



**Reglas de tráfico de salida**

Azure define tres reglas de seguridad de salida predeterminadas para el grupo de seguridad de red. Las reglas **solo permiten el tráfico de salida** a Internet y a la red virtual. En la siguiente imagen se muestran las reglas de seguridad de salida predeterminadas de un grupo de seguridad de red en Azure Portal.



**Determinación de las reglas vigentes del grupo de seguridad de red**

Cada grupo de seguridad de red y sus reglas de seguridad definidas se evalúan de forma independiente. Azure procesa las condiciones de cada regla definida para cada máquina virtual de la configuración.

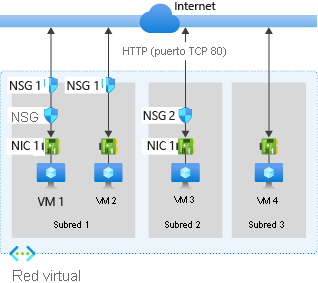
* Para el tráfico entrante, Azure procesa primero las reglas de seguridad del grupo de seguridad de red para las subredes asociadas y, a continuación, las interfaces de red asociadas.
* Para el tráfico saliente, se invierte el proceso. Azure evalúa primero las reglas de seguridad del grupo de seguridad de red para las interfaces de red asociadas seguidas de las subredes asociadas.
* En el caso del proceso de evaluación de entrada y salida, Azure también comprueba cómo aplicar las reglas para el tráfico dentro de la subred.

La forma en que Azure termina aplicando las reglas de seguridad definidas para una máquina virtual determina la *vigencia* general de las reglas.

**Aspectos que se deben conocer sobre reglas de seguridad vigentes**

Vamos a explorar cómo se definen y procesan las reglas del grupo de seguridad de red dentro de una red virtual para producir las reglas vigentes.

Tenga en cuenta la siguiente configuración de red virtual que muestra los grupos de seguridad de red (NSG) que controlan el tráfico a las máquinas virtuales (VM). La configuración requiere reglas de seguridad para administrar el tráfico de red hacia y desde Internet a través del puerto TCP 80 por la interfaz de red.



En esta configuración de red virtual, hay tres subredes. La subred 1 contiene dos máquinas virtuales: VM 1 y VM 2. La subred 2 y la subred 3 contienen una máquina virtual: VM 3 y VM 4, respectivamente. Cada máquina virtual tiene una tarjeta de interfaz de red (NIC).

Azure evalúa cada configuración de NSG para determinar las reglas de seguridad vigentes:

| **Evaluación** | ***NSG* de subred** | ***NSG* de NIC** | **Reglas de entrada** | **Reglas de salida** |
| --- | --- | --- | --- | --- |
| **VM 1** | Subred 1 *NSG 1* | NIC *NSG 2* | Las reglas de subred *NSG 1* tienen prioridad sobre las reglas de NIC de *NSG 2* | Las reglas de NIC *NSG 2* tienen prioridad sobre las reglas de subred de *NSG 1* |
| **VM 2** | Subred 1 *NSG 1* | NIC *none* | Las reglas de subred *NSG 1* se aplican a la subred y a la NIC | Las reglas predeterminadas de Azure se aplican a la NIC y las reglas de subred *NSG 1* solo se aplican a la subred |
| **VM 3** | Subred 2 *none* | NIC *NSG 2* | Las reglas predeterminadas de Azure se aplican a la subred y las reglas de *NSG 2* se aplican a la NIC | Las reglas de NIC *NSG 2* se aplican a la NIC y a la subred |
| **VM 4** | Subred 3 *none* | NIC *none* | Las reglas predeterminadas de Azure se aplican a la subred y a la NIC y se permite todo el tráfico entrante | Las reglas predeterminadas de Azure se aplican a la subred y a la NIC y se permite todo el tráfico saliente |

**Reglas vigentes del tráfico entrante**

Azure procesa reglas para el tráfico entrante para todas las máquinas virtuales de la configuración. Azure identifica si las máquinas virtuales son miembros de un NSG y si tienen una subred o una NIC asociadas.

* Cuando se crea un NSG, Azure crea la regla de seguridad predeterminada DenyAllInbound para el grupo. El comportamiento predeterminado es denegar todo el tráfico entrante desde Internet. Si un grupo de seguridad de red tiene una subred o NIC, las reglas de la subred o la NIC pueden invalidar las reglas de seguridad predeterminadas de Azure.
* Las reglas de entrada de NSG para una subred de una máquina virtual tienen prioridad sobre las reglas de entrada de NSG para una NIC en la misma máquina virtual.

**Reglas vigentes del tráfico saliente**

Azure procesa reglas para el tráfico saliente examinando primero las asociaciones de NSG para las NIC en todas las máquinas virtuales.

* Cuando se crea un NSG, Azure crea la regla de seguridad predeterminada AllowInternetOutbound para el grupo. El comportamiento predeterminado es permitir todo el tráfico saliente a Internet. Si un grupo de seguridad de red tiene una subred o NIC, las reglas de la subred o la NIC pueden invalidar las reglas de seguridad predeterminadas de Azure.
* Las reglas de salida de NSG para una NIC en una máquina virtual tienen prioridad sobre las reglas de salida de NSG para una subred de la misma máquina virtual.

**Aspectos que hay que tener en cuenta al crear reglas vigentes**

Revise las consideraciones siguientes sobre la creación de reglas de seguridad vigentes para las máquinas de la red virtual.

* **Considere la posibilidad de permitir todo el tráfico**. Si coloca la máquina virtual dentro de una subred o utiliza una interfaz de red, no tiene que asociar la subred o la NIC a un grupo de seguridad de red. Este enfoque permite todo el tráfico de red a través de la subred o la NIC según las reglas de seguridad predeterminadas de Azure. Si no le preocupa controlar el tráfico al recurso en un nivel específico, no asocie el recurso en ese nivel a un grupo de seguridad de red.
* **Considere la importancia de las reglas de permiso**. Al crear un grupo de seguridad de red, debe definir una regla de **permiso** para la subred y la interfaz de red del grupo para asegurarse de que el tráfico puede pasar. Si tiene una subred o una NIC en el grupo de seguridad de red, debe definir una regla de permiso en cada nivel. De lo contrario, se deniega el tráfico para cualquier nivel que no proporcione una definición de regla de permiso.
* **Considere el tráfico dentro de la subred**. Las reglas de seguridad de un grupo de seguridad de red asociado a una subred pueden afectar al tráfico entre todas las máquinas virtuales de la subred. De forma predeterminada, Azure permite que las máquinas virtuales de la misma subred envíen tráfico entre sí (lo que se conoce como *tráfico dentro de la subred*). Puede prohibir el tráfico dentro de la subred definiendo una regla en el grupo de seguridad de red para denegar todo el tráfico entrante y saliente. Esta regla impide que todas las máquinas virtuales de la subred se comuniquen entre sí.
* **Considere la prioridad de las reglas**. Las reglas de seguridad de un grupo de seguridad de red se procesan en orden de prioridad. Para asegurarse de que siempre se procesa una regla de seguridad determinada, asigne el valor de prioridad más bajo posible a la regla. Se recomienda dejar espacios en la numeración de prioridad, como 100, 200, 300, etc. Los espacios en la numeración permiten agregar nuevas reglas sin tener que editar las reglas existentes.

**Visualización de las reglas de seguridad vigentes**

Si tiene varios NSG y no está seguro de qué reglas de seguridad se aplican, puede usar el vínculo **Reglas de seguridad vigentes** en Azure Portal. Puede usar el vínculo para comprobar qué reglas de seguridad se aplican a las máquinas, subredes e interfaces de red.

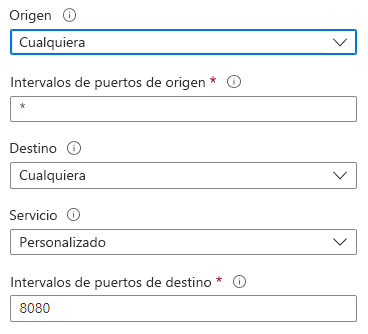


**Creación de reglas de grupo de seguridad de red**

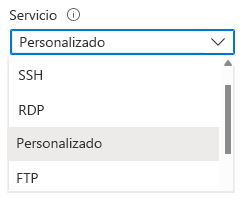
Agregar reglas de seguridad para controlar el tráfico entrante y saliente en Azure Portal es fácil. Se pueden configurar reglas de grupo de seguridad de red virtual y seleccionar de entre una gran variedad de servicios de comunicación, como HTTPS, RDP, FTP y DNS.

**Aspectos que saber sobre la configuración de reglas de seguridad**

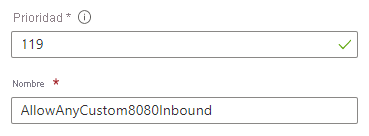
Echemos un vistazo a algunas de las propiedades que es necesario especificar para crear las reglas de seguridad. A medida que revise esta configuración, piense en las reglas de tráfico que necesita crear y qué servicios pueden cubrir sus requisitos de red.



* **Origen**: identifica cómo la regla de seguridad controla el tráfico **entrante**. Este valor especifica un intervalo de direcciones IP de origen específico que está permitido o denegado. El filtro de origen puede ser cualquier recurso, un intervalo de direcciones IP, un grupo de seguridad de aplicaciones o una etiqueta predeterminada.
* **Destino**: identifica cómo la regla de seguridad controla el tráfico **saliente**. Este valor especifica un intervalo de direcciones IP de destino específico que está permitido o denegado. El valor del filtro de destino es similar al del filtro de origen. Este valor puede ser cualquier recurso, un intervalo de direcciones IP, un grupo de seguridad de aplicaciones o una etiqueta predeterminada.
* **Servicio**: esta configuración especifica el protocolo de destino y el intervalo de puertos de la regla de seguridad. Puede elegir un servicio predefinido (como RDP o SSH) o proporcionar un intervalo de puertos personalizado. Hay un gran número de servicios entre los que seleccionar.



* **Prioridad**: asigna el valor de orden de prioridad de la regla de seguridad. Las reglas se procesan según el orden de prioridad de todas las reglas de un grupo de seguridad de red, incluida una subred y una interfaz de red. Cuanto menor sea el valor de prioridad, mayor será la prioridad de la regla.



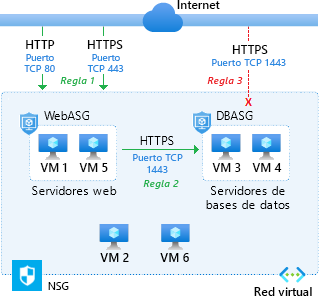
**Implementación de grupos de seguridad de aplicaciones**

Puede implementar [grupos de seguridad de aplicaciones](https://learn.microsoft.com/es-es/azure/virtual-network/application-security-groups) en la red virtual de Azure para agrupar lógicamente las máquinas virtuales por carga de trabajo. Después, puede definir las reglas del grupo de seguridad de red en función de los grupos de seguridad de aplicaciones.

**Aspectos que se deben saber sobre el uso de grupos de seguridad de aplicaciones**

Los grupos de seguridad de aplicaciones funcionan de la misma manera que los grupos de seguridad de red, pero proporcionan una manera centrada en la aplicación de examinar la infraestructura. Las máquinas virtuales se unen a un grupo de seguridad de aplicaciones. A continuación, use el grupo de seguridad de aplicaciones como origen o destino en las reglas del grupo de seguridad de red.

Vamos a examinar cómo implementar grupos de seguridad de aplicaciones mediante la creación de una configuración para un minorista en línea. En nuestro escenario de ejemplo, es necesario controlar el tráfico de red a las máquinas virtuales en los grupos de seguridad de aplicaciones.



**Requisitos del escenario**

Estos son los requisitos del escenario para nuestra configuración de ejemplo:

* Tenemos seis máquinas virtuales en nuestra configuración con dos servidores web y dos servidores de bases de datos.
* Los clientes acceden al catálogo en línea hospedado en nuestros servidores web.
* Los servidores web deben ser accesibles desde Internet mediante el puerto HTTP 80 y el puerto HTTPS 443.
* La información de inventario se almacena en nuestros servidores de bases de datos.
* Los servidores de bases de datos deben ser accesibles desde el puerto HTTPS 1433.
* Solo nuestros servidores web deben tener acceso a nuestros servidores de bases de datos.

**Solución**

Para nuestro escenario, es necesario crear la siguiente configuración:

1. Cree grupos de seguridad de aplicaciones para las máquinas virtuales.
   1. Cree un grupo de seguridad de aplicaciones denominado WebASG para agrupar las máquinas del servidor web.
   2. Cree un grupo de seguridad de aplicaciones denominado DBASG para agrupar las máquinas del servidor de bases de datos.
2. Asigne las interfaces de red para las máquinas virtuales.
   1. En cada servidor de máquinas virtuales, asigne su NIC al grupo de seguridad de aplicaciones adecuado.
3. Cree un grupo de seguridad de red y reglas de seguridad.
   1. **Regla 1**: establezca **Prioridad** en 100. Permita el acceso desde Internet a las máquinas del grupo WebASG desde el puerto HTTP 80 y el puerto HTTPS 443.

La regla 1 tiene el valor de prioridad más bajo, por lo que tiene prioridad sobre las demás reglas del grupo. El acceso de los clientes a nuestro catálogo en línea es primordial en nuestro diseño.

* 1. **Regla 2**: establezca **Prioridad** en 110. Permita el acceso desde máquinas del grupo WebASG a máquinas del grupo DBASG desde el puerto HTTPS 1433.
  2. **Regla 3**: establezca **Prioridad** en 120. **Deniegue** el acceso (X) desde cualquier lugar a las máquinas del grupo DBASG desde el puerto HTTPS 1433.

La combinación de la Regla 2 y la Regla 3 garantiza que solo nuestros servidores web puedan acceder a nuestros servidores de bases de datos. Esta configuración de seguridad protege nuestras bases de datos de inventario frente a ataques externos.

**Cosas que hay que tener en cuenta al usar grupos de seguridad de aplicaciones**

Hay varias ventajas al implementar grupos de seguridad de aplicaciones en las redes virtuales.

* **Considere el mantenimiento de direcciones IP**. Al controlar el tráfico de red mediante grupos de seguridad de aplicaciones, no es necesario configurar el tráfico entrante y saliente para direcciones IP específicas. Si tiene muchas máquinas virtuales en la configuración, puede ser difícil especificar todas las direcciones IP afectadas. A medida que mantiene la configuración, el número de servidores puede cambiar. Estos cambios pueden requerir que modifique cómo se admiten diferentes direcciones IP en las reglas de seguridad.
* **Considere la posibilidad de no usar subredes**. Al organizar las máquinas virtuales en grupos de seguridad de aplicaciones, no es necesario distribuir también los servidores entre subredes específicas. Puede organizar los servidores por aplicación y propósito para lograr agrupaciones lógicas.
* **Considere la posibilidad de usar reglas simplificadas**. Los grupos de seguridad de aplicaciones ayudan a eliminar la necesidad de varios conjuntos de reglas. No tiene que crear una regla independiente para cada máquina virtual. Puede aplicar dinámicamente nuevas reglas a los grupos de seguridad de aplicaciones designados. Las nuevas reglas de seguridad se aplican automáticamente a todas las máquinas virtuales del grupo de seguridad de aplicaciones especificado.
* **Considere la compatibilidad con cargas de trabajo**. Una configuración que implementa grupos de seguridad de aplicaciones es fácil de mantener y comprender porque la organización se basa en el uso de la carga de trabajo. Los grupos de seguridad de aplicaciones proporcionan organizaciones lógicas para las aplicaciones, los servicios, el almacenamiento de datos y las cargas de trabajo.

**Prueba de conocimientos**

Su empresa va a migrar varios sitios a Azure. Usted es responsable de implementar grupos de seguridad de red y de diseñar reglas de seguridad eficaces para controlar el tráfico de red. Necesita proteger tanto las redes de máquinas virtuales como las de los servicios de Azure.

* El equipo de infraestructura tiene dos reglas de seguridad de NSG para el tráfico de entrada a los servidores web back-end. Hay una regla de permiso con una prioridad de 200 y una regla de denegación con una prioridad de 150.
* El equipo de TI quiere aplicar etiquetas de servicio de Azure nuevas y preexistentes para las direcciones IP de la máquina virtual.
* Está viendo cómo usar reglas predeterminadas para aplicar seguridad al tráfico entrante desde máquinas virtuales dentro de la red virtual.

**Responda a las siguientes preguntas**

Elija la respuesta más adecuada para cada una de las siguientes preguntas. Después, seleccione **Comprobar las respuestas**.

Principio del formulario

**1. ¿Cuál de las reglas de seguridad definidas por el equipo de infraestructura tiene prioridad?**

1. La regla de permiso tiene precedencia.
2. La regla de denegación tiene precedencia.
3. La regla que se creó primero tiene precedencia.

**2. ¿Cómo definiría una regla de seguridad de entrada predeterminada?**

1. Permitir el tráfico entrante de una máquina virtual de otra red virtual.
2. Permitir el tráfico de cualquier origen externo a cualquier máquina virtual.
3. Permitir el tráfico entrante de cualquier máquina virtual a cualquier otra máquina virtual de la red virtual.

**3. ¿Cuál es una etiqueta de servicio válida para las reglas del grupo de seguridad de red?**

1. Virtual Network
2. VPN Gateway
3. Database
4. B
5. C
6. A

Final del formulario

**Resumen y recursos**

En este módulo, ha obtenido información sobre los grupos de seguridad de red (NSG) en Azure. Los grupos de seguridad de red se usan para limitar el tráfico de red a los recursos de la red virtual mediante una lista de reglas de seguridad. Puede asociar grupos de seguridad de red a subredes o interfaces de red, y definir reglas para controlar el tráfico entrante y saliente.

También ha aprendido cómo se evalúan y procesan las reglas de los grupos de seguridad de red. Por último, ha aprendido cómo permiten los grupos de seguridad de aplicaciones agrupar máquinas virtuales en función de la carga de trabajo.

Las principales conclusiones de este módulo son:

* Los grupos de seguridad de red son esenciales para controlar el tráfico de red en las redes virtuales de Azure.
* Las reglas del grupo de seguridad de red se evalúan y procesan en función de la prioridad y se pueden crear para subredes e interfaces de red.
* Se pueden conseguir reglas de NSG eficaces teniendo en cuenta la prioridad de las reglas, el tráfico dentro de la subred y la administración de la prioridad de las reglas.
* Los grupos de seguridad de aplicaciones proporcionan una vista centrada en la aplicación de la infraestructura y simplifican la administración de reglas.