Implementación de grupos de seguridad de red

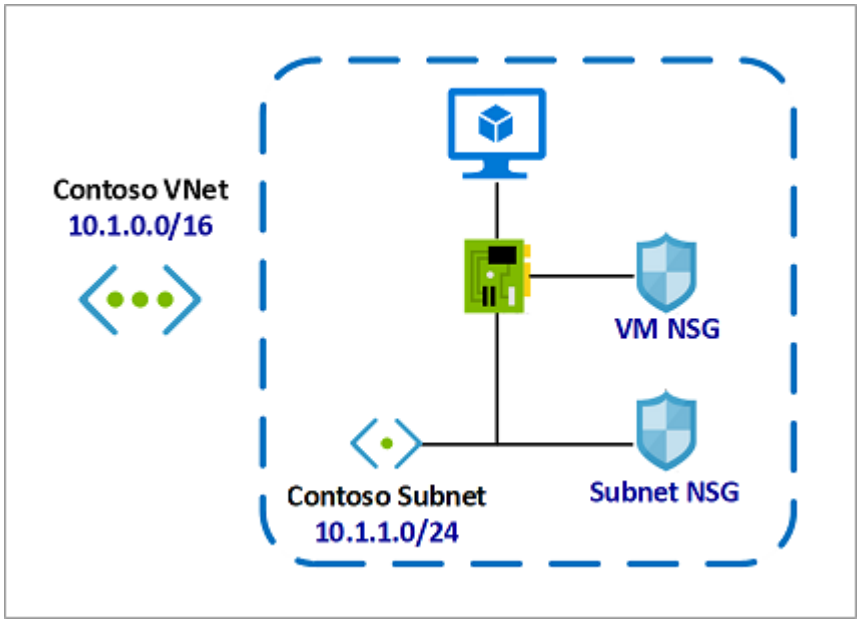
Al implementar los NSG, estos son los límites a tener en cuenta:

- De forma predeterminada, puede crear 100 NSG por región y suscripción. Para aumentar este límite a 400, póngase en contacto con el Soporte técnico de Azure.
- Solo puede aplicar un NSG a una máquina virtual, subred o adaptador de red.
- De forma predeterminada, puede tener hasta 200 reglas en un único NSG. Para aumentar este límite a 500, póngase en contacto con el Soporte técnico de Azure.
- Puede aplicar un NSG a varios recursos.

Una subred individual puede o no tener un grupo de seguridad de red asociado. Una interfaz de red individual también puede o no tener un grupo de seguridad de red asociado. Por lo tanto, puede restringir eficazmente el tráfico dual para una máquina virtual mediante la asociación de un NSG, primero a una subred y, a continuación, otro NSG a la interfaz de red de la VM. En este caso, la aplicación de reglas de grupo de seguridad de red depende de la dirección del tráfico y la prioridad de las reglas de seguridad aplicadas.

Consideremos un ejemplo sencillo con una máquina virtual como se indica a continuación:

- La máquina virtual se encuentra en la subred Contoso.
- La subred Contoso está asociada al grupo de seguridad de red de la subred.
- La interfaz de red de la máquina virtual también está asociada a un grupo de seguridad de red de máquina virtual.



En este ejemplo, para el tráfico entrante, primero se evalúa el grupo de seguridad de red de la subred. A continuación, el grupo de seguridad de red de la máquina virtual evalúa el tráfico permitido mediante el grupo de seguridad de red de la subred. Lo contrario es aplicable para el

tráfico saliente, el grupo de seguridad de red de la máquina virtual se evalúa primero. A continuación, el grupo de seguridad de red de la subred evalúa el tráfico permitido mediante el grupo de seguridad de red de la máquina virtual.

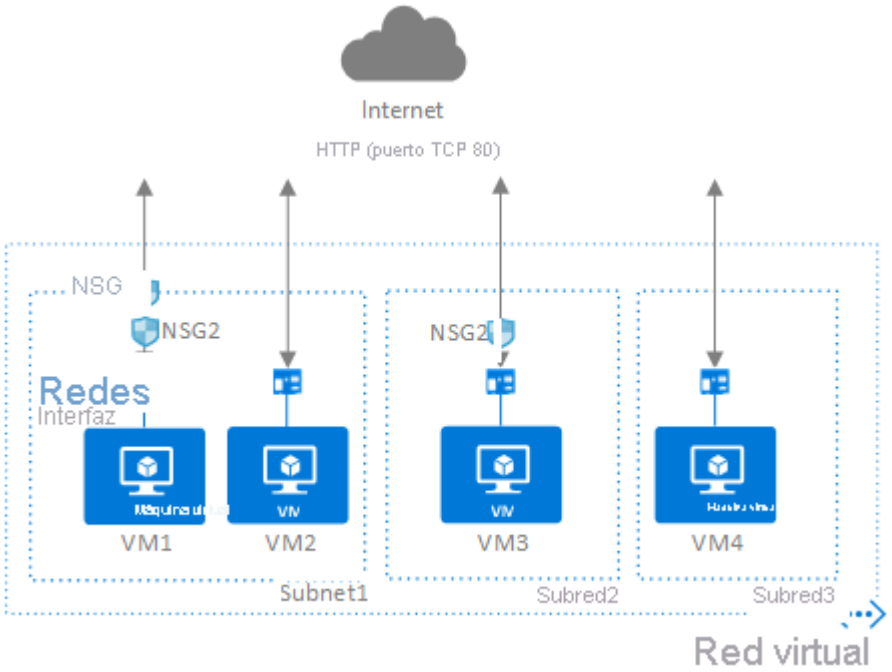
Esto permite la aplicación de la regla de seguridad específica. Por ejemplo, puede que desee permitir el acceso entrante a Internet para algunas máquinas virtuales de aplicación (por ejemplo, las de front-end) en una subred, pero restringir el acceso a Internet para otras máquinas virtuales (por ejemplo, las de base de datos o de back-end). En este caso puede tener una regla más flexible en el grupo de seguridad de red de la subred que permita el tráfico de Internet y restringir el acceso para máquinas virtuales específicas al denegar el acceso en el grupo de seguridad de red de la máquina virtual. Lo mismo se aplica al tráfico saliente.

Para ayudar a proteger los recursos de Azure, asegúrese de que el planeamiento de NSG es un procedimiento operativo estándar (SOP) para las implementaciones.

Cómo se evalúa el tráfico

Varios recursos de los servicios de Azure se pueden implementar en una red virtual de Azure. Puede asociar cero o un grupo de seguridad de red a cada subred e interfaz de red de la red virtual en una máquina virtual. El mismo grupo de seguridad de red se puede asociar a tantas interfaces de red y subredes como se desee.

La siguiente imagen ilustra los diferentes escenarios de cómo se podrían implementar grupos de seguridad de red para permitir el tráfico de red hacia y desde Internet a través del puerto TCP 80:



Consulte el diagrama anterior, junto con el texto siguiente, para comprender cómo Azure procesa las reglas de entrada y salida para los grupos de seguridad de red:

Tráfico entrante

Para el tráfico entrante, Azure procesa las reglas de un grupo de seguridad de red asociadas a una subred en primer lugar, si hay alguna y, a continuación, las reglas de un grupo de seguridad de red asociadas a la interfaz de red, si hay alguna.

- **VM1:** las reglas de seguridad de NSG1 se procesan, ya que está asociado a Subnet1 y VM1 está en Subnet1. A menos que haya creado una regla que permita el puerto 80 de entrada, la **regla de seguridad predeterminada DenyAllInbound** deniega el tráfico y NSG2 nunca lo evalúa, ya que NSG2 está asociado a la interfaz de red. Si NSG1 tiene una regla de seguridad que permite el puerto 80, NSG2 procesa el tráfico. Para permitir el puerto 80 para la máquina virtual, tanto NSG1 como NSG2 deben tener una regla que permita el puerto 80 desde Internet.
- **VM2:** las reglas de NSG1 se procesan porque VM2 también está en Subnet1. Puesto que VM2 no tiene un grupo de seguridad de red asociado a su interfaz de red, recibe todo el tráfico permitido por NSG1 o se deniega todo el tráfico denegado por NSG1. El tráfico se permite o deniega a todos los recursos de la misma subred cuando un grupo de seguridad de red está asociado a una subred.
- **VM3:** dado que no hay ningún grupo de seguridad de red asociado a Subnet2, se permite el tráfico en la subred y NSG2 lo procesa, porque NSG2 está asociado a la interfaz de red conectada a VM3.
- **VM4:** se permite el tráfico a VM4, porque un grupo de seguridad de red no está asociado a Subnet3 ni a la interfaz de red de la máquina virtual. Si no tienen un grupo de seguridad de red asociado, se permite todo el tráfico de red a través de una subred y una interfaz de red.

Tráfico saliente

Para el tráfico saliente, Azure procesa las reglas de un grupo de seguridad de red asociadas a una interfaz de red en primer lugar, si hay alguna y, a continuación, las reglas de un grupo de seguridad de red asociadas a la subred, si hay alguna.

- **VM1:** se procesan las reglas de seguridad de NSG2. A menos que cree una regla de seguridad que deniegue el puerto 80 de salida a Internet, la regla de seguridad predeterminada AllowInternetOutbound permite el tráfico de NSG1 y NSG2. Si NSG2 tiene una regla de seguridad que deniega el puerto 80, el tráfico se deniega y NSG1 nunca lo evalúa. Para denegar el puerto 80 desde la máquina virtual, uno o ambos de los grupos de seguridad de red deben tener una regla que deniegue el puerto 80 a Internet.
- **VM2:** se envía todo el tráfico a través de la interfaz de red a la subred, ya que la interfaz de red conectada a VM2 no tiene un grupo de seguridad de red asociado. Se procesan las reglas de NSG1.
- **VM3:** si NSG2 tiene una regla de seguridad que deniega el puerto 80, también se deniega el tráfico. Si NSG2 tiene una regla de seguridad que permite el puerto 80, dicho puerto tiene permitida la salida a Internet, ya que no hay un grupo de seguridad de red asociado a Subnet2.

- **VM4:** se permite todo el tráfico desde VM4, porque un grupo de seguridad de red no está asociado a la interfaz de red conectada a la máquina virtual, ni a Subnet3.

Tráfico dentro de la subred

Es importante tener en cuenta que las reglas de seguridad de un NSG asociado a una subred pueden afectar la conectividad entre las máquinas virtuales dentro de ella. Por ejemplo, si se agrega una regla a NSG1 que deniega todo el tráfico entrante y saliente, VM1 y VM2 ya no podrán comunicarse entre sí. Otra regla tendría que agregarse específicamente para permitirlo.

Directrices generales

A menos que tenga una razón concreta, se recomienda que asocie un grupo de seguridad de red a una subred o a una interfaz de red, pero no a ambas. Puesto que las reglas de un grupo de seguridad de red asociado a una subred pueden entrar en conflicto con las reglas de un grupo de seguridad de red asociado a una interfaz de red, puede tener problemas de comunicación inesperados que necesiten solución.
