

Exploración de grupos de seguridad de red (NSG)

El tráfico de red puede filtrarse hacia y desde los recursos de Azure en una red virtual de Azure con un **grupo de seguridad de red**. Un grupo de seguridad de red contiene reglas de seguridad que permiten o deniegan el tráfico de red entrante o el tráfico de red saliente de varios tipos de recursos de Azure. Para cada regla, puede especificar un origen y destino, un puerto y un protocolo.

Las máquinas virtuales que se crean a través del modelo de implementación de Resource Manager pueden tener conectividad directa a Internet mediante una dirección IP pública que se asigna directamente a las máquinas virtuales. Solo el firewall de host configurado dentro de las máquinas virtuales ayuda a proteger estas máquinas virtuales de Internet.

Las máquinas virtuales que se crean mediante el modelo de implementación clásico se comunican con los recursos de Internet a través del servicio en la nube al que se asigna la dirección IP pública, que también se conoce como VIP. Las máquinas virtuales que residen dentro del servicio en la nube comparten esa VIP y establecen la comunicación con los recursos de Internet mediante puntos de conexión. Si quita los puntos de conexión de máquina virtual que asignan el puerto público y la dirección IP pública del servicio en la nube al puerto privado y la dirección IP privada de la máquina virtual, la máquina virtual deja de ser accesible desde Internet a través de la dirección IP pública.

Los grupos de seguridad de red (NSG) ayudan a proporcionar seguridad avanzada para las máquinas virtuales que se crean a través del modelo de implementación (Resource Manager o clásico). Los NSG controlan el tráfico entrante y saliente que pasa a través de un adaptador de red (en el modelo de implementación de Resource Manager), una máquina virtual (en el modelo de implementación clásico) o una subred (en ambos modelos de implementación).

Reglas del grupo de seguridad de red

Los NSG contienen reglas que especifican si se aprobará o denegará el tráfico. Cada regla se basa en una dirección IP de origen, un puerto de origen, una dirección IP de destino y un puerto de destino. En función de si el tráfico coincide con esta combinación, la regla permite o deniega el tráfico. Cada regla consta de las siguientes propiedades:

- **Nombre.** Se trata de un identificador único para la regla.
- **Dirección.** Esto especifica si el tráfico es entrante o saliente.
- **Prioridad.** Si varias reglas coinciden con el tráfico, se aplican las reglas con mayor prioridad.
- **Acceso.** Esto especifica si el tráfico se permite o se deniega.
- **Prefijo de dirección IP de origen.** Este prefijo identifica dónde se originó el tráfico. Se puede basar en una única dirección IP; un intervalo de direcciones IP en notación

Enrutamiento de interdominios sin clases (CIDR) o el asterisco (*), que es un carácter comodín que coincide con todas las direcciones IP posibles.

- **Intervalo de puertos de origen.** Esto especifica los puertos de origen mediante un número de puerto único de 1 a 65 535; un intervalo de puertos (por ejemplo, 200-400); o el asterisco (*) para indicar todos los puertos posibles.
- **Prefijo de dirección IP de destino.** Esto identifica el destino del tráfico en función de una única dirección IP, un intervalo de direcciones IP en notación CIDR o el asterisco (*) para que coincida con todas las direcciones IP posibles.
- **Intervalo de puertos de destino.** Esto especifica los puertos de destino mediante un número de puerto único de 1 a 65 535; un intervalo de puertos (por ejemplo, 200-400); o el asterisco (*) para indicar todos los puertos posibles.
- **Protocolo.** Especifica un protocolo que coincide con la regla. Puede ser UDP, TCP o el asterisco (*).

Reglas personalizadas del grupo de seguridad de red

Existen reglas predeterminadas y predefinidas para el tráfico entrante y saliente. No puede eliminar estas reglas, pero se pueden invalidar porque tienen la prioridad más baja. Las reglas predeterminadas permiten todo el tráfico entrante y saliente dentro de una red virtual, permiten el tráfico saliente hacia Internet y permiten el tráfico entrante hacia un equilibrador de carga de Azure. También existe una regla predeterminada con la prioridad más baja en los conjuntos de reglas entrantes y salientes que deniega toda la comunicación de red.

Al crear una regla personalizada, puede usar etiquetas predeterminadas en los prefijos de la dirección IP de origen y destino para especificar categorías predefinidas de direcciones IP. Estas etiquetas predeterminadas son:

- **Internet.** Esta etiqueta representa las direcciones IP de Internet.
- **Virtual_network.** Esta etiqueta identifica todas las direcciones IP que define el intervalo IP de la red virtual. También incluye intervalos de direcciones IP desde redes locales cuando se definen como red local a red virtual.
- **Azure_loadbalancer.** Esta etiqueta especifica el destino predeterminado del equilibrador de carga de Azure.

Planeamiento de grupos de seguridad de red

Puede diseñar grupos de seguridad de red para aislar redes virtuales en zonas de seguridad, como hace el modelo usado por la infraestructura local. Puede aplicar grupos de seguridad de red a subredes, lo que le permite crear subredes filtradas protegidas, o redes perimetrales, que pueden restringir el flujo de tráfico a todas las máquinas que residen dentro de esa subred. Con el modelo de implementación clásico, también puede asignar grupos de seguridad de red a equipos individuales para controlar el tráfico que tiene como destino la VM y que sale de ella. Con el modelo de implementación de Resource Manager, puede asignar grupos de seguridad de red a un adaptador de red para que las reglas de tal grupo controlen solo el tráfico que fluye a través de ese adaptador de red. Si la máquina virtual tiene varios adaptadores de red, las reglas del grupo de seguridad de red no se aplicarán automáticamente al tráfico designado para otros adaptadores de red.

Los grupos de seguridad de red se crean como recursos de un grupo de recursos, pero se pueden compartir con otros grupos de recursos de la suscripción.

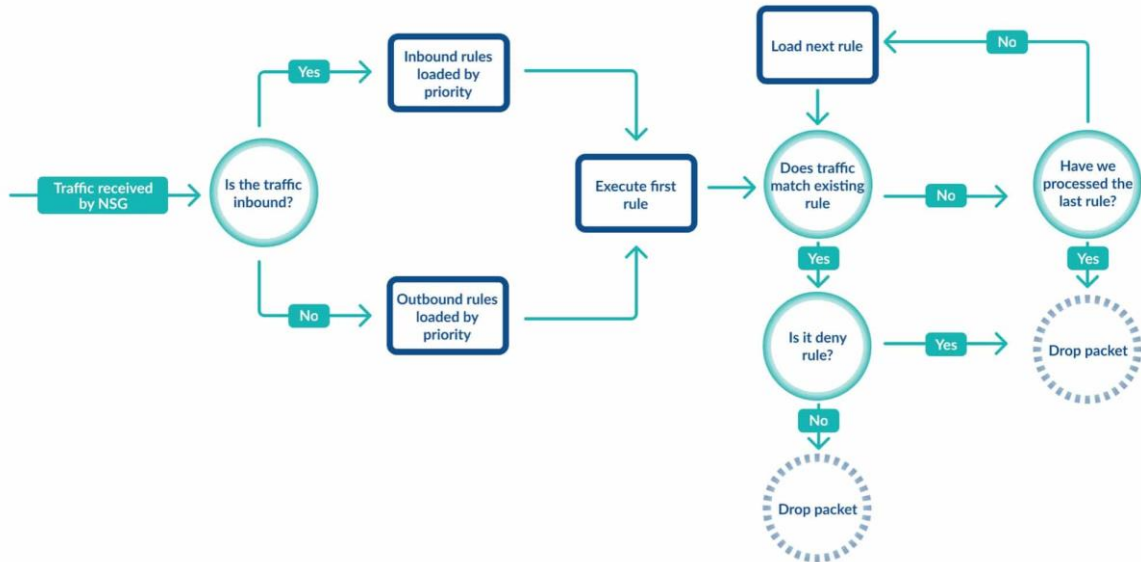
Capacidades de Azure NSG

Los NSG de Azure controlan el acceso y administran la comunicación entre:

- Cargas de trabajo individuales hospedadas en una o más redes virtuales de Azure.
- Conectividad entre entornos locales y Azure a través de Application Gateway, VPN Gateway, Azure Firewall, Azure Bastion service y Virtual Network Appliances.
- Conexiones desde y hacia Internet.

El siguiente diagrama detalla el flujo de tráfico de red y el protocolo de cumplimiento de reglas que sigue un NSG de Azure.

Una suscripción estándar de Azure puede tener hasta 5000 NSG y cada NSG puede tener un máximo de 1000 reglas. La siguiente tabla especifica la configuración de la regla y sus propiedades asociadas.



Una suscripción estándar de Azure puede tener hasta 5000 NSG y cada NSG puede tener un máximo de 1000 reglas. La siguiente tabla especifica la configuración de la regla y sus propiedades asociadas.

Configuración de reglas	Propiedades
Nombre	El nombre de la regla. Esta configuración es un campo de texto libre, pero debe ser único dentro del NSG.
Prioridad	Esta configuración debe ser un número entre 100 y 4096. Azure NSG procesa sus reglas en orden de prioridad, procesando los números más bajos antes que los más altos. Es importante tener en cuenta que Azure NSG dejará de procesar un paquete de red cuando encuentre una regla coincidente. Por lo tanto, si tiene otra regla con los mismos atributos más abajo en la lista de prioridades, el NSG no la procesará.
Origen o Destino	Esta configuración define el origen o el destino del tráfico de red. Puede establecerse en "Cualquiera" para el tráfico desde cualquier lugar, o puede bloquearlo en una sola dirección IP o un rango de IP que necesita especificar en notación CIDR, por ejemplo, 10.0.0.0/16.

Protocolo

Esta configuración de NSG describe el protocolo de red de su regla. Puede configurarlo para buscar el protocolo "Cualquiera" o especificar uno de TCP, UDP, ICMP, ESP o AH.

Dirección

Esta configuración define la dirección del tráfico de la red y puede configurarla como Entrante o Saliente.

rango de puertos

La configuración del rango de puertos describe el puerto o los puertos de la regla. Puede especificar un solo puerto, por ejemplo, 80, o un rango de puertos, por ejemplo, 1000-2000.

Acción

Esta configuración define la acción que ejecutará la regla. Puede configurarlo en "Permitir" o "Denegar".

Aplicación de reglas de Azure NSG

Cuando crea un NSG de Azure, Azure lo completa con seis reglas de seguridad predeterminadas, como se ilustra en la imagen a continuación.

<div>Filter by name</div> <div>Port == allProtocol == allSource == allDestination == allAction == all</div>						
Priority	Name	Port	Protocol	Source	Destination	Action
Inbound Security Rules						
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny
Outbound Security Rules						
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

La siguiente tabla proporciona detalles sobre cada regla y su propósito.

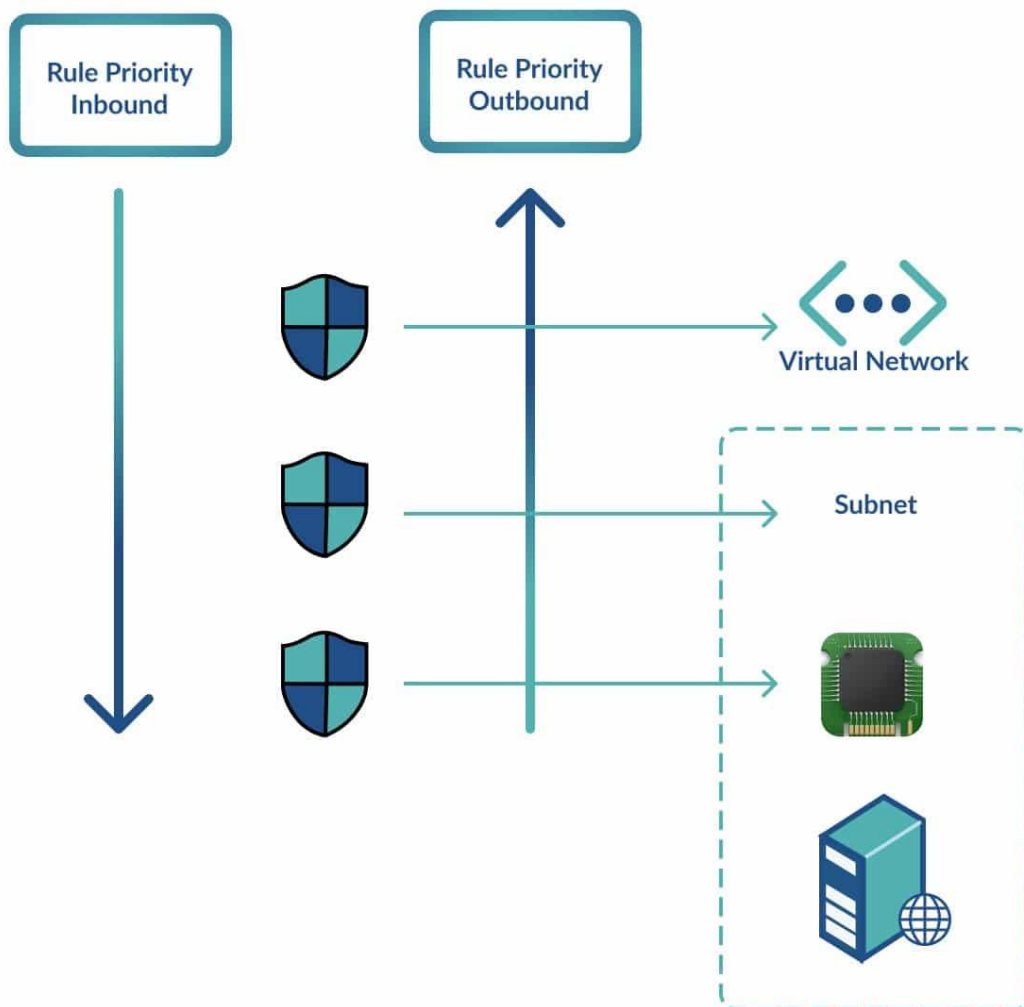
Nombre de la regla	Descripción
AllowVnetInbound	Esta regla predeterminada permite todo el tráfico entrante dentro de la red virtual. Permite que todos los hosts dentro de la misma red virtual y las subredes conectadas se comuniquen entre sí. Tenga en cuenta que esta regla permite todo el tráfico entrante entre todos los hosts. Si su estrategia de seguridad requiere bloquear algunos servicios, deberá configurar reglas de denegación adicionales para aplicarlo.
AllowAzureLoadBalancerInBound	Esta regla permite la comunicación entre Azure Load Balancer y sus recursos de Azure, es decir, VNet o Virtual Machine (VM). Por lo general, Azure usa esta regla para enviar y recibir latidos entre su VM y Load Balancer.
DenyAllInbound	Esta regla predeterminada, como su nombre lo indica, bloquea todo el tráfico entrante. Azure solo lo aplica después de procesar todas las demás reglas de la lista, ya que tiene la prioridad más baja.
AllowVnetOutbound	Esta regla predeterminada permite todo el tráfico saliente dentro de la red virtual. Permite que todos los hosts dentro de la misma red virtual y las subredes conectadas se comuniquen entre sí. Tenga en cuenta que esta regla permite todo el tráfico saliente entre todos los hosts. Si su estrategia de seguridad requiere bloquear algunos servicios, deberá configurar reglas de denegación adicionales para aplicarlo.
AllowInternetOutBound	Esta regla predeterminada permite todo el tráfico saliente a Internet. Si su configuración de seguridad establece que solo se debe permitir el acceso a Internet a puertos y servicios específicos, deberá configurar reglas adicionales.

DenyAllOutbound

Esta regla predeterminada, como su nombre lo indica, bloquea todo el tráfico saliente. Azure solo lo aplica después de procesar todas las demás reglas de la lista, ya que tiene la prioridad más baja.

Prioridades de reglas

Como se mencionó, los NSG de Azure ejecutan las reglas en orden de prioridad, y las prioridades con números más bajos se procesan antes que los números más altos. Sin embargo, también puede anidar NSG para un recurso en particular, como se muestra en la imagen a continuación. En el diagrama, hay una máquina virtual que ejecuta un servidor web conectado a una subred. Esa subred forma parte de una red virtual más extensa. El administrador de Azure configuró tres NSG y adjuntó uno a la red virtual, la subred y la tarjeta de red de la máquina virtual.



Como hay tres NSG de Azure activos, la configuración de reglas para la máquina virtual requiere establecer la configuración correcta en los tres NSG. Por ejemplo, si desea permitir el acceso desde Internet al puerto 80 (el puerto HTTP predeterminado) en la máquina virtual, deberá crear una regla de entrada en los tres NSG. Dado que el tráfico entrante primero atraviesa la red virtual, luego se enruta a la subred y finalmente a la tarjeta de red de la máquina virtual, cada NSG necesita una regla de permiso. Estas reglas de permiso explícitas son necesarias porque cada NSG tiene la regla predeterminada DenyAllInbound.

Para el tráfico saliente, las reglas de NSG se aplican a la inversa. Por ejemplo, supongamos que el servidor web también proporciona un servicio SMTP a otras máquinas virtuales alojadas en la misma red virtual y sus políticas de seguridad dictan que no puede enviar ningún tráfico SMTP a Internet. En ese caso, deberá configurar una regla de permiso SMTP en el NSG de la tarjeta de red de la VM y en el NSG de la subred para permitir que el tráfico SMTP fluya entre las VM *dentro* de la red virtual. La regla DenyAllOutbound en el NSG de la red virtual evitará que el tráfico SMTP vinculado a Internet salga de la red virtual.

Registros de flujo de Azure NSG

El objetivo principal de un NSG de Azure es proteger los recursos encargados en una red virtual de Azure. Sin embargo, las mejores prácticas de seguridad establecen que el monitoreo continuo de su entorno es vital. Dado que las alertas entrantes pueden ayudarlo a identificar cualquier incidente de seguridad, es crucial implementar medidas que monitoreen su entorno.

[Azure NSG Flow Logs](#) es una característica proporcionada por [Azure Network Watcher](#). Este servicio le permite registrar información de tráfico de IP para los datos que fluyen a través de sus NSG configurados. Azure envía estos datos de registro de flujo a una cuenta de almacenamiento de Azure donde puede acceder a ellos o exportarlos para que los analice un SIEM o un IDS.

Casos de uso del registro de flujo de Azure NSG

Los registros de flujo de NSG de Azure le brindan la información que necesita para monitorear la seguridad, el cumplimiento y el rendimiento de su entorno. Al analizar los datos sobre el estado actual de su red virtual de Azure, brindan información vital, como qué servicios tienen conexiones, de dónde provienen esas conexiones y qué puertos están abiertos a Internet. Puede aprovechar Azure Flow Logs en varios casos de uso diferentes, como se ilustra en la siguiente tabla.

Caso de uso	Ejemplos
Monitoreo de red	<ul style="list-style-type: none"> ● Identificar tráfico de red desconocido o sospechoso. ● Supervisar el consumo de ancho de banda y los niveles de tráfico. ● Aproveche el filtrado por IP y puerto para determinar el comportamiento de la aplicación de referencia. ● Exportar datos de registro para informes o fuentes de panel de monitoreo en vivo.
Supervisión y optimización de uso	<ul style="list-style-type: none"> ● Identifique a los principales hablantes de su red. ● Aproveche Geo-IP e identifique el tráfico entre regiones. ● Utilizar datos de registro de flujo para la previsión de capacidad. ● Identificar y resolver reglas de tráfico no optimizadas.
Cumplimiento	<ul style="list-style-type: none"> ● Verifique que sus reglas de tráfico cumplan con las obligaciones de aislamiento y cumplimiento de la red.
Análisis forense y de seguridad de redes	<ul style="list-style-type: none"> ● Exportar datos de registro de flujo a cualquier IDS o SIEM. ● Analice el flujo de la red desde direcciones IP sospechosas o interfaces de red.

Cómo funcionan los registros de flujo de Azure NSG

Los registros de flujo de NSG de Azure registran todos los flujos de IP que entran y salen de un NSG, y Azure recopila estos datos en intervalos de un minuto. El servicio almacena la información registrada en formato JSON con un período de retención predeterminado de un año para todos los registros. Es fundamental tener en cuenta que Azure configura los registros de flujo de NSG para que estén deshabilitados de forma predeterminada. Sin embargo, puede activar y administrar este servicio mediante varias funcionalidades de administración de Azure, incluido Azure Portal, la CLI de Azure y Azure PowerShell.

Un enfoque integral para la gestión de la nube híbrida

Habilitación de registros de flujo de Azure NSG mediante Azure Portal

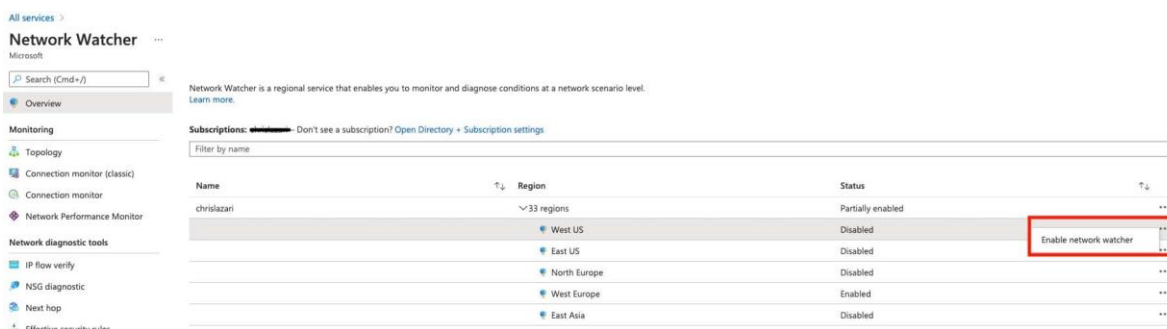
Antes de activar los registros de flujo de NSG de Azure mediante Azure Portal, debe habilitar Network Watcher y registrar el proveedor de Insights.

Habilitar Network Watcher a través de Azure Portal es un proceso rápido de tres pasos.

Busque Network Watcher después de seleccionar Todos los servicios en Azure Portal.



Luego, seleccione la región asociada con su red virtual y NSG, y habilite Network Watcher como se ilustra en la imagen a continuación.



El proveedor de Microsoft Insights es un requisito previo para el registro de flujo de Azure NSG. Puede seguir los pasos a continuación para habilitarlo mediante Azure Portal.

Busque Suscripciones después de seleccionar Todos los servicios en Azure Portal.



Abra la suscripción correspondiente y, en el menú de la hoja, seleccione Proveedores de recursos en la sección Configuración.

Settings

- Programmatic deployment
- Resource groups
- Resources
- Preview features
- Usage + quotas
- Policies
- Management certificates
- My permissions
- Resource providers**
- Deployments
- Properties
- Resource locks

Confirme que microsoft.insights se muestra como registrado, como se muestra en la imagen a continuación.

Filter by name...	
Microsoft.OperationsManagement	Registered
microsoft.insights	Registered
Microsoft.Advisor	Registered

Como se mencionó, los registros de NSG Flow requieren una cuenta de almacenamiento para almacenar datos. Si no tiene una cuenta de almacenamiento, deberá crear una antes de habilitar el registro de flujo de NSG.

Una vez que haya confirmado que Network Watcher está habilitado, Microsoft Insights Provider está registrado y tiene una cuenta de almacenamiento disponible, puede habilitar el registro de flujo de Azure NSG siguiendo estos pasos.

Busque Network Watcher después de seleccionar Todos los servicios en Azure Portal.



En la barra de navegación vertical de la izquierda, seleccione Registros de flujo de NSG.

[All services](#) >





Network Watcher

Microsoft

<<

 Overview

Monitoring

-  Topology
-  Connection monitor (classic)
-  Connection monitor
-  Network Performance Monitor



Network diagnostic tools

-  IP flow verify
-  NSG diagnostic
-  Next hop
-  Effective security rules
-  VPN troubleshoot
-  Packet capture
-  Connection troubleshoot

Metrics

-  Usage + quotas

Logs

-  NSG flow logs
-  Diagnostic logs
-  Traffic Analytics

Haga clic en el NSG que desea monitorear con Azure NSG Flow Logs.

Name	Resource type	Resource group	Status
 NSG1	Network security group	Temp	⊖ Disabled

Establezca el estado del registro de flujo en Activado, seleccione su cuenta de almacenamiento y haga clic en Guardar. También puede establecer otras opciones para los registros de flujo de NSG en este formulario. Por ejemplo, la versión 1 solo registra el flujo de tráfico IP de entrada y salida para el tráfico permitido y denegado, mientras que la versión 2 proporciona información de rendimiento adicional (bytes y paquetes) por flujo. También puede habilitar el análisis de tráfico si tiene configurado un área de trabajo de Log Analytics. Esta función ofrece otros análisis y visualizaciones enriquecidos, como la capacidad de profundizar en el mapa geográfico, descubrir rápidamente los puntos críticos de tráfico y obtener información sobre las posibilidades de optimización.

Flow logs settings ...

 Save  Discard

Flow logs

Status

Off

On

Flow Logs version ⓘ

Version 1

Version 2

Version 1 logs ingress and egress IP traffic flows for both allowed and denied traffic. Version 2 provides additional throughput information (bytes and packets) per flow.

[Learn more.](#)

nsgflowclaz

[Select storage account](#)

Retention (days) ⓘ



0

Traffic Analytics



Traffic Analytics provides rich analytics and visualization derived from NSG flow logs and other Azure resources' data. Drill through geo-map, easily figure out traffic hotspots and get insights into optimization possibilities.

[Learn about all features](#)

To use this feature, choose an Log Analytics workspace. To minimize data egress costs, we recommend that you choose a workspace in the same region your flow logs storage account is located. Network Performance Monitor solution will be installed on the workspace. We also advise that you use the same workspace for all NSGs as much as possible. Additional meta-data is added to your flow logs data, to provide enhanced analytics.

Traffic Analytics status

Off

On

Traffic Analytics processing interval ⓘ

Every 1 hour



nsgflow

[Select Log Analytics workspace](#)

[Microsoft privacy statement](#)

This privacy statement explains what personal data Microsoft collects from you, through our interactions with you and through our products, and how we use that data.

Habilitación de registros de flujo de NSG de Azure mediante la CLI de Azure

También puede habilitar los registros de flujo de NSG de Azure mediante la CLI de Azure. Al igual que con Azure Portal, primero debe registrar Insights Provider. El comando de la CLI de Azure para realizar este paso es:

```
az provider register --namespace Microsoft.Insights
```

Una vez que haya confirmado el registro del proveedor de Insights, puede ejecutar este comando para habilitar el registro de NSG Flow:

```
az network watcher flow-log create --resource-group resourceGroupName --enabled true --nsg nsgName --storage-account storageAccountName --location location
```

Azure también le permite configurar ajustes adicionales para el registro de flujo de Azure NSG a través de la CLI de Azure. Por ejemplo, si desea habilitar el registro con la versión 2, puede ejecutar este comando:

```
az network watcher flow-log create --resource-group resourceGroupName --enabled true --nsg nsgName --storage-account storageAccountName --location location --format JSON --log-version 2
```

Habilitación de registros de flujo de Azure NSG mediante Azure PowerShell

También puede administrar los registros de flujo de Azure NSG con Azure PowerShell.

Primero, debe configurar sus variables, como se muestra en el ejemplo de secuencia de comandos a continuación.

```
$NW = Get-AzNetworkWatcher -ResourceGroupName NetworkWatcherRg -Name NetworkWatcher_  
$nsg = Get-AzNetworkSecurityGroup -ResourceGroupName nsgRG -Name nsgName  
$storageAccount = Get-AzStorageAccount -ResourceGroupName StorageRG -Name contosostorage123  
Get-AzNetworkWatcherFlowLogStatus -NetworkWatcher $NW -TargetResourceId $nsg.Id
```

Si desea habilitar el análisis de tráfico, también deberá configurar estos parámetros.

```
$workspaceResourceId = "/subscriptions/bbbbbbbb-bbbb-bbbb-bbbb-bbbbbbbbbbbb/resourcegroups/trafficanalyticsrg/providers/microsoft.operationalinsights/workspaces/taworkspace"  
$workspaceGUID = "cccccccc-cccc-cccc-cccc-cccccccccccc" $workspaceLocation = " e.g. westcentralus"
```

Los siguientes comandos de Azure PowerShell proporcionan ejemplos de cómo habilitar el registro de flujo de NSG con varias opciones.

Configurar registros de flujo de la versión 1

```
Set-AzNetworkWatcherConfigFlowLog -NetworkWatcher $NW -TargetResourceId $nsg.Id -StorageAccountId $storageAccount.Id -EnableFlowLog $true -FormatType Json -FormatVersion 1
```


Configurar registros de flujo de la versión 2 y configurar análisis de tráfico

Set-AzNetworkWatcherConfigFlowLog -NetworkWatcher \$NW -TargetResourceId \$nsg.Id -StorageAccountId \$storageAccount.Id -EnableFlowLog \$true -FormatType Json -FormatVersion 2

Configure los registros de flujo de la versión 2 con el análisis de tráfico configurado

Set-AzNetworkWatcherConfigFlowLog -NetworkWatcher \$NW -TargetResourceId \$nsg.Id -StorageAccountId \$storageAccount.Id -EnableFlowLog \$true -FormatType Json -FormatVersion 2 -EnableTrafficAnalytics -WorkspaceResourceId \$workspaceResourceId -WorkspaceGUID \$workspaceGUID -WorkspaceLocation \$workspaceLocation

Estado de registro de flujo de consulta

Get-AzNetworkWatcherFlowLogStatus -NetworkWatcher \$NW -TargetResourceId \$nsg.Id

Prácticas recomendadas de Azure NSG

Trabajar con varios NSG puede ser un desafío, especialmente si necesita comprender las reglas efectivas cuando dos o más NSG controlan el tráfico de su red. Sin embargo, seguir algunas prácticas recomendadas puede ayudarlo a administrar Azure NSG de manera más eficaz.

Alinear los NSG con los grupos de recursos y servicios

No necesita configurar un NSG para cada recurso de Azure hospedado en una red virtual. Según su caso de uso, puede administrar fácilmente todas sus reglas a nivel de red virtual o subred. Sin embargo, es importante tener en cuenta la mantenibilidad.

Por ejemplo, administrar todas sus reglas de acceso en un solo NSG puede parecer más sencillo porque no necesita tener en cuenta ninguna otra regla de NSG. Sin embargo, un NSG puede tener hasta 1000 reglas, y mantener cientos de configuraciones de permitir y denegar puede volverse complejo a medida que escala. A su vez, esta complejidad puede conducir a descuidos y malas configuraciones. Al igual que con cualquier otra implementación de tecnología, la estructura debe alinearse con la estrategia. A medida que desarrolle su estrategia de seguridad de Azure, asegúrese de tener en cuenta la mantenibilidad de sus reglas de NSG.

Por ejemplo, en lugar de tener un solo NSG para una red virtual completa, considere alinear sus NSG con un grupo de recursos o servicio en particular. El uso de este enfoque le permite administrar y mantener un conjunto más pequeño de reglas que es más fácil y eficiente. También ofrece seguridad adicional cuando retira los servicios. Puede eliminar el NSG con su grupo de recursos, mitigando el riesgo de reglas abiertas que ya no necesita.

Usar convenciones de nombres lógicos

Azure le brinda mucha flexibilidad cuando se trata de nombrar recursos. Si etiqueta sus NSG de Azure con una convención de nomenclatura que proporcione al lector suficiente información, reducirá la cantidad de esfuerzo necesario para admitir su entorno de Azure. Por ejemplo, si necesita encargar un NSG para una máquina virtual denominada SRV-WEB-01, llamarlo NSG-SRV-WEB-01 es mucho más fácil de identificar para el soporte técnico que un nombre genérico como NSG01.

Aproveche los rangos de IP para agilizar la creación de reglas

Los NSG de Azure le permiten especificar una sola dirección IP y puerto o ingresar un rango. Cuando sea posible, use rangos en lugar de direcciones individuales, ya que limitará la cantidad de reglas que necesita crear y administrar. Sin embargo, si necesita restringir el acceso a un solo recurso, se recomienda una sola dirección IP y puerto.

Deje espacios entre los números de prioridad de las reglas

Como se mencionó, los NSG de Azure procesan las reglas en orden de prioridad, y los números más bajos se procesan primero. Por lo tanto, al crear reglas, deje suficiente espacio entre sus prioridades en caso de que necesite crear una regla que requiera procesamiento antes que una regla anterior. Por ejemplo, comience su primera regla con una prioridad de 110 en lugar de 100. El uso de este enfoque le brindará la flexibilidad en caso de que necesite crear otra regla que deba precederla.

Use etiquetas para mejorar la legibilidad

Cuando necesite administrar varios objetos, puede aprovechar [las etiquetas de servicio de red virtual](#) . Estos recursos de Azure representan un grupo de prefijos de direcciones IP que se relacionan con un servicio de Azure en particular. Por ejemplo, "Red virtual" representa todo el intervalo de direcciones de red virtual e "Internet" indica todas las direcciones IP externas que se pueden enrutar públicamente. Por lo tanto, el uso de etiquetas en los campos de origen y destino mejora la legibilidad de las reglas de NSG.

Deficiencias y limitaciones de Azure NSG

Aunque los NSG de Azure ofrecen una seguridad adecuada, tienen algunas limitaciones. Microsoft ofrece [Azure Firewall](#) , un servicio administrado de alta disponibilidad que proporciona características de seguridad adicionales relevantes para algunos casos de uso. La siguiente tabla detalla la funcionalidad disponible para ambos productos de seguridad.

Rasgo	Grupo de seguridad de Azure	Firewall Azure
Capas OSI	Filtra el tráfico en la Capa 3 (red) y la Capa 4 (sesión).	Filtra el tráfico en la capa 3 (red), la capa 4 (sesión) y la capa 7 (aplicación).
Filtrado de tráfico basado en protocolos	Sí	Sí
Soporte de etiquetas de servicio	Sí	Sí
Compatibilidad con etiquetas de nombre de dominio completo (FQDN)	No	Sí: con Azure Firewall, puede etiquetar un grupo de nombres de dominio completos, como actualizaciones de Windows o servicios de Microsoft 365.
Traducción de dirección de red de origen (SNAT)	No	Sí, Azure Firewall le permite configurar una IP pública para enmascarar una IP interna.
Traducción de direcciones de red de destino (DNAT)	No	Sí, Azure Firewall es compatible con DNAT, que puede usar para traducir el tráfico entrante a la dirección IP privada de su red virtual.
Integrado con Azure Monitor	Sí, sin embargo, los registros de flujo con análisis de tráfico no están habilitados de manera predeterminada.	Sí: sin embargo, el registro de diagnóstico no está habilitado de forma predeterminada.
Inteligencia de amenazas	No	Sí, Azure Firewall le brinda la capacidad de bloquear el tráfico en función de los datos de análisis de amenazas de Microsoft.