Uso de grupos de seguridad de red para controlar el acceso a la red

Como parte del proyecto para migrar el sistema de ERP a Azure debe asegurarse de que los servidores tengan el aislamiento adecuado, de manera que solo los sistemas permitidos puedan realizar conexiones de red. Por ejemplo, tiene servidores de bases de datos que almacenan datos de la aplicación de ERP. Quiere evitar que sistemas prohibidos se comuniquen con los servidores a través de la red, al tiempo que permite a los servidores de aplicaciones comunicarse con los servidores de bases de datos.

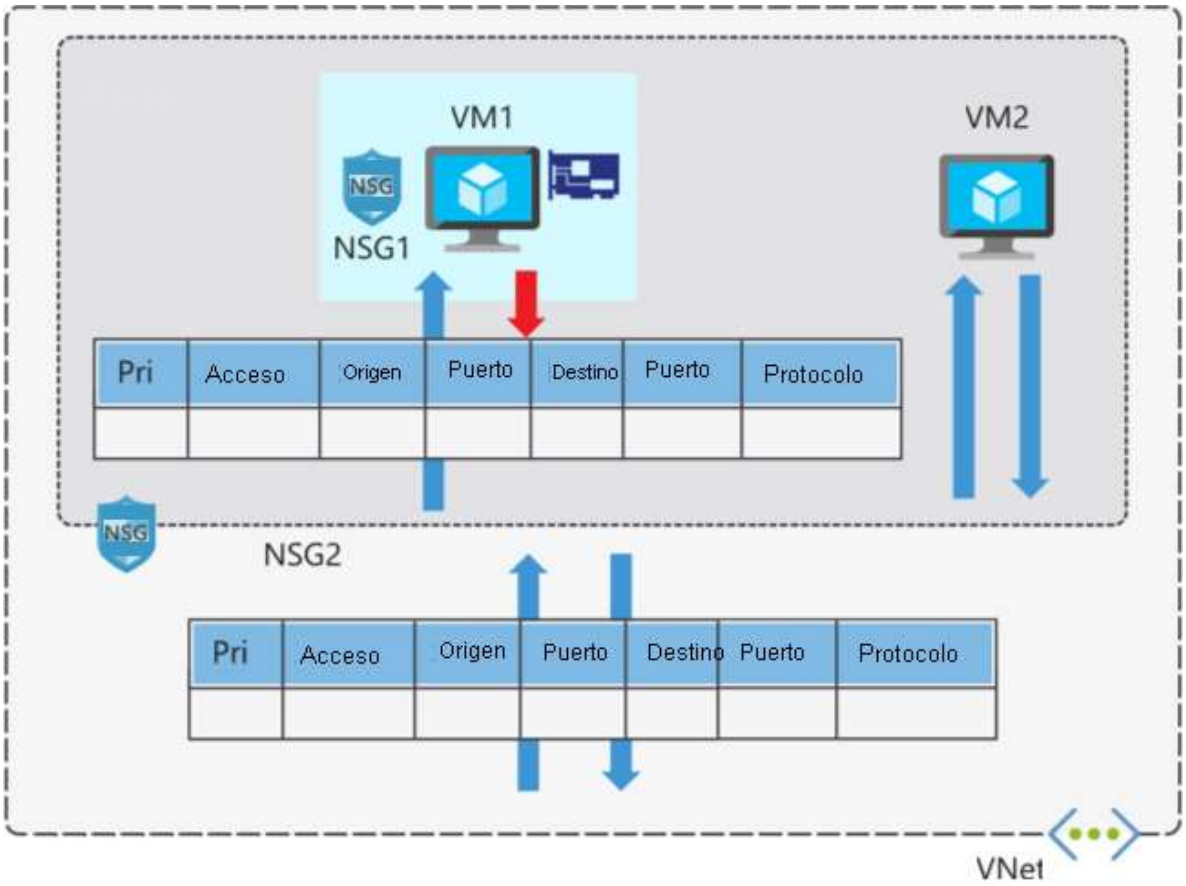
Grupos de seguridad de red

Los grupos de seguridad de red filtran el tráfico de red hacia y desde recursos de Azure. También contienen reglas de seguridad que se configuran para permitir o denegar el tráfico entrante y saliente. Puede usar grupos de seguridad de red para filtrar el tráfico entre máquinas virtuales o subredes, tanto dentro de una red virtual como desde Internet.

Asignación y evaluación de grupos de seguridad de red

Los grupos de seguridad de red se asignan a una interfaz de red o una subred. Al asignar un grupo de seguridad de red a una subred, las reglas se aplican a todas las interfaces de red de esa subred. Puede restringir aún más el tráfico si asocia un grupo de seguridad de red a la interfaz de red de una máquina virtual.

Al aplicar grupos de seguridad de red a una subred y a una interfaz de subred, cada grupo de seguridad de red se evalúa por separado. El tráfico entrante primero lo evalúa el grupo de seguridad de red aplicado a la subred y, después, el grupo de seguridad de red aplicado a la interfaz de red. A la inversa, el grupo de seguridad de red aplicado a la interfaz de red es el primero en evaluar el tráfico que sale de una máquina virtual, y luego lo hace el grupo de seguridad de red aplicado a la subred.



Aplicar un grupo de seguridad de red a una subred, en lugar de interfaces de red individuales, puede reducir los esfuerzos de administración. Este enfoque también garantiza que todas las máquinas virtuales dentro de la subred especificada estén protegidas con el mismo conjunto de reglas.

Cada interfaz de red y subred puede tener un grupo de seguridad de red aplicado. Los grupos de seguridad de red admiten TCP, UDP e ICMP, y operan en la capa 4 del modelo OSI.

En este escenario de la empresa manufacturera, los grupos de seguridad de red pueden ayudarle a proteger la red. Puede controlar qué equipos se pueden conectar a los servidores de aplicaciones. El grupo de seguridad de red se configura para que solo un intervalo de direcciones IP concretas se puedan conectar a los servidores. Esto se puede bloquear incluso más si solo se permite el acceso a o desde puertos específicos o direcciones IP individuales. Estas reglas se pueden aplicar a dispositivos que se conectan de forma remota desde redes locales o entre recursos de Azure.

Reglas de seguridad

Un grupo de seguridad de red contiene una o varias reglas de seguridad. Configure las reglas de seguridad para permitir o denegar el tráfico.

Las reglas tienen varias propiedades:

Propiedad	Explicación
Nombre	Un nombre único dentro del grupo de seguridad de red.
Priority	Un número entre 100 y 4096.
Origen y destino	Cualquiera, una dirección IP individual, un bloque de enrutamiento entre dominios sin clases (CIDR) (10.0.0.0/24, por ejemplo), una etiqueta de servicio o un grupo de seguridad de aplicaciones.
Protocolo	TCP, UDP o cualquiera.
Dirección	Si la regla se aplica al tráfico entrante o al saliente.
Intervalo de puertos	Un puerto individual o un intervalo de puertos.
Acción	Permitir o denegar el tráfico.

Las reglas de seguridad de los grupos de seguridad de red se evalúan por prioridad mediante información en tuplas de cinco elementos (origen, puerto de origen, destino, puerto de destino y protocolo) para permitir o denegar el tráfico. Cuando las condiciones de una regla coinciden con la configuración del dispositivo, se detiene el procesamiento de la regla.

Por ejemplo, imagine que la empresa ha creado una regla de seguridad para permitir el tráfico entrante en el puerto 3389 (RDP) a los servidores web con una prioridad de 200. Después imagine que otro administrador ha creado una regla para denegar el tráfico entrante en el puerto 3389, con una prioridad de 150. La regla de denegación tiene prioridad porque se procesa primero. La regla con prioridad 150 se procesa antes que la regla con prioridad 200.

Con los grupos de seguridad de red, las conexiones tienen estado. El tráfico de retorno se permite de forma automática para la misma sesión TCP/UDP. Por ejemplo, una regla de entrada que permite el tráfico en el puerto 80 también permite que la máquina virtual responda a la solicitud (normalmente en un puerto efímero). No se necesita una regla de salida correspondiente.

Respecto al sistema de ERP, los servidores web de la aplicación de ERP se conectan a los servidores de bases de datos que se encuentran en sus propias subredes. Puede aplicar reglas de seguridad para indicar que la única comunicación permitida desde los servidores web a los de bases de datos sea el puerto 1433 para las comunicaciones de bases de datos de SQL Server. Se denegará el resto del tráfico a los servidores de bases de datos.

Reglas de seguridad predeterminadas

Cuando sea crea un grupo de seguridad de red, Azure crea varias reglas predeterminadas. Estas reglas predeterminadas no se pueden modificar, pero se pueden reemplazar por reglas propias. Estas reglas predeterminadas permiten la conectividad dentro de una red virtual y de los equilibradores de carga de Azure. También permiten la comunicación saliente a Internet y denegar el tráfico entrante desde Internet.

Las reglas predeterminadas para el tráfico de entrada son las siguientes:

Prioridad	Nombre de la regla	Descripción
65000	AllowVnetInbound	Permitir el tráfico entrante procedente de todas las máquinas virtuales a cualquier máquina virtual dentro de la subred.
65001	AllowAzureLoadBalancerInbound	Permitir el tráfico desde el equilibrador de carga predeterminado a cualquier máquina virtual dentro de la subred.
65500	DenyAllInBound	Denegar el tráfico desde cualquier origen externo a cualquiera de las máquinas virtuales.

Las reglas predeterminadas para el tráfico de salida son las siguientes:

Prioridad	Nombre de la regla	Descripción
65000	AllowVnetOutbound	Permitir el tráfico de salida desde cualquier máquina virtual a cualquier máquina virtual dentro de la subred.
65001	AllowInternetOutbound	Permitir el tráfico saliente a Internet desde cualquier máquina virtual.
65500	DenyAllOutBound	Denegar el tráfico desde cualquier máquina virtual interna al sistema situado fuera de la red virtual.

Reglas de seguridad aumentada

Las reglas de seguridad aumentada se pueden usar para los grupos de seguridad de red con el fin de simplificar la administración de un gran número de reglas. Las reglas de seguridad aumentada también son útiles cuando es necesario implementar conjuntos de reglas de red más complejos. Las reglas aumentadas permiten agregar las opciones siguientes en una sola regla de seguridad:

- Varias direcciones IP
- Varios puertos
- Etiquetas de servicio
- Grupos de seguridad de aplicaciones

Imagine que su empresa quiere restringir el acceso a los recursos del centro de datos, repartidos en varios intervalos de direcciones de red. Con las reglas aumentadas, puede agregar todos estos intervalos en una única regla, lo que reduce la sobrecarga administrativa y la complejidad en los grupos de seguridad de red.

Etiquetas de servicio

Las etiquetas de servicio se pueden usar para simplificar todavía más la seguridad de los grupos de seguridad de red. Puede permitir o denegar el tráfico a un servicio de Azure específico, ya sea de forma global o por regiones.

Las etiquetas de servicio simplifican la seguridad de las máquinas virtuales y las redes virtuales de Azure, ya que permiten restringir el acceso por recursos o servicios. Las etiquetas de servicio representan un grupo de direcciones IP y ayudan a simplificar la configuración de las reglas de

seguridad. Para los recursos que se pueden especificar mediante una etiqueta, no es necesario conocer los detalles del puerto o la dirección IP.

Puede restringir el acceso a muchos servicios. Microsoft administra las etiquetas de servicio, lo cual significa que no puede crear las suyas propias. Algunos ejemplos de etiquetas:

- **VirtualNetwork**: representa todas las direcciones de red virtual en cualquier lugar de Azure, y en la red local si usa conectividad híbrida.
- **AzureLoadBalancer**: indica el equilibrador de carga de infraestructura de Azure. La etiqueta se traduce en la dirección IP virtual del host (168.63.129.16) donde se originan los sondeos de mantenimiento de Azure.
- **Internet**: representa todo lo que está fuera de la dirección de red virtual y a lo que se accede de forma pública, incluidos recursos que tienen direcciones IP públicas. Un recurso de este tipo es la característica Web Apps de Azure App Service.
- **AzureTrafficManager**: representa la dirección IP de Azure Traffic Manager.
- **Storage**: representa el espacio de direcciones IP de Azure Storage. Puede especificar si se permite o se deniega el tráfico. También puede especificar si solo se permite el acceso a una región específica, pero no puede seleccionar cuentas de almacenamiento individuales.
- **SQL**: representa la dirección de los servicios Azure SQL Database, Azure Database for MySQL, Azure Database for PostgreSQL y Azure Synapse Analytics. Puede especificar si se permite o se deniega el tráfico, así como limitarlo a una región específica.
- **AppService**: representa prefijos de dirección de Azure App Service.

Grupos de seguridad de aplicaciones

Los grupos de seguridad de aplicaciones permiten configurar la seguridad de red de los recursos que se usan en aplicaciones específicas. Puede agrupar las máquinas virtuales de forma lógica, con independencia de su dirección IP o asignación de subred.

Use los grupos de seguridad de aplicaciones dentro de un grupo de seguridad de red para aplicar una regla de seguridad a un grupo de recursos. Es más fácil implementar y escalar verticalmente cargas de trabajo de aplicaciones específicas. Solo tiene que agregar una nueva implementación de máquina virtual a uno o más grupos de seguridad de aplicaciones, y esa máquina virtual toma de forma automática las reglas de seguridad de esa carga de trabajo.

Un grupo de seguridad de aplicaciones permite agrupar interfaces de red. Luego se puede usar ese grupo de seguridad de aplicaciones como regla de origen o destino dentro de un grupo de seguridad de red.

Por ejemplo, su empresa tiene una serie de servidores front-end en una red virtual. Los servidores web deben ser accesibles a través de los puertos 80 y 8080. Los servidores de bases de datos deben ser accesibles a través del puerto 1433. Las interfaces de red de los servidores web se asignan a un grupo de seguridad de aplicaciones y las interfaces de red de los servidores de bases de datos a otro grupo de seguridad de aplicaciones. Después, crea dos reglas de entrada en el

grupo de seguridad de red. Una regla permite el tráfico HTTP a todos los servidores del grupo de seguridad de aplicaciones del servidor web. La otra regla permite el tráfico SQL a todos los servidores del grupo de seguridad de aplicaciones del servidor de bases de datos.

Sin los grupos de seguridad de aplicaciones, deberá crear una regla independiente para cada máquina virtual o agregar un grupo de seguridad de red a una subred y, posteriormente, agregar todas las máquinas virtuales a esa subred.

La principal ventaja de los grupos de seguridad de aplicaciones es que facilitan la administración. Puede agregar y quitar interfaces de red en un grupo de seguridad de aplicaciones con facilidad mientras implementa o vuelve a implementar servidores de aplicaciones. También puede aplicar de forma dinámica reglas nuevas a un grupo de seguridad de aplicaciones, que después se aplican automáticamente a todas las máquinas virtuales de ese grupo de seguridad de aplicaciones.

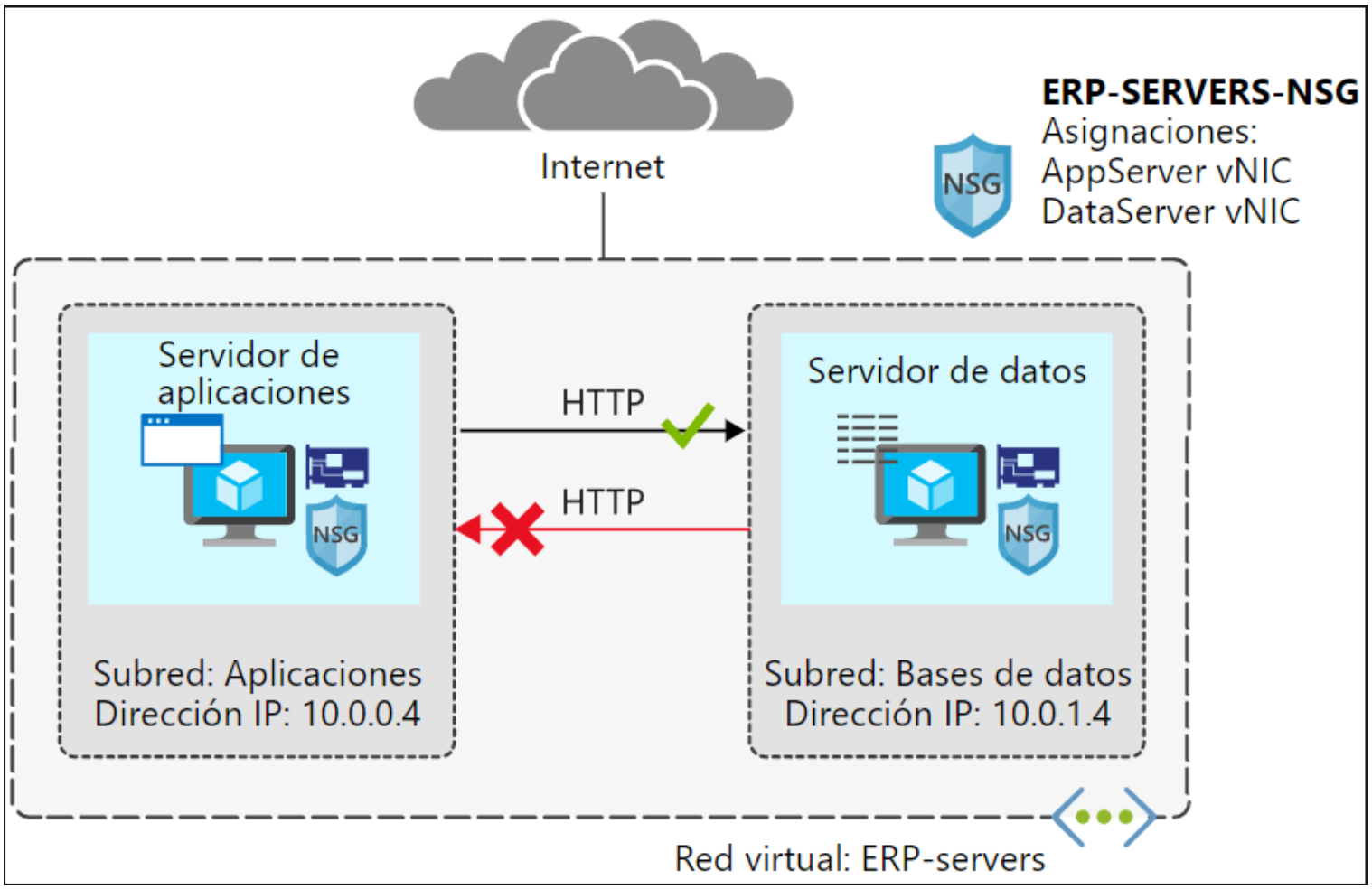
Cuándo usar grupos de seguridad de red

Como procedimiento recomendado, siempre debe usar grupos de seguridad de red para ayudar a proteger los recursos de red contra el tráfico no deseado. Los grupos de seguridad de red ofrecen control de acceso pormenorizado sobre el nivel de red, sin la complejidad potencial de establecer reglas de seguridad para cada máquina virtual o red virtual.

Ejercicio: Creación y administración de grupos de seguridad de red

Como arquitecto de soluciones de la empresa manufacturera, ahora quiere empezar a migrar a Azure los servidores de bases de datos y la aplicación de ERP. Como primer paso, va a probar el plan de seguridad de red con dos de los servidores.

En esta unidad, configurará un grupo de seguridad de red y reglas de seguridad para restringir el tráfico de red a servidores específicos. Quiere que el servidor de aplicaciones se pueda conectar al servidor de bases de datos a través de HTTP. No quiere que el servidor de bases de datos pueda usar HTTP para conectarse al servidor de aplicaciones.



Creación de una red virtual y un grupo de seguridad de red

En primer lugar, creará la red virtual y las subredes para los recursos de servidor. Después, creará un grupo de seguridad de red.

1. En Azure Cloud Shell, ejecute el siguiente comando para asignar el grupo de recursos del espacio aislado a la variable rg:

CLI de Azure

rg=learn-71cd0808-341a-4b88-bef8-c552e245ce4d

2. Para crear la red virtual **ERP-servers** y la subred **Applications** (Aplicaciones), ejecute el comando siguiente en Cloud Shell:

CLI de Azure

```
az network vnet create \
  --resource-group $rg \
  --name ERP-servers \
  --address-prefixes 10.0.0.0/16 \
  --subnet-name Applications \
  --subnet-prefixes 10.0.0.0/24
```

3. Ejecute el comando siguiente en Cloud Shell para crear la subred **Databases** (Bases de datos):

CLI de Azure

```
az network vnet subnet create \
  --resource-group $rg \
  --vnet-name ERP-servers \
  --address-prefixes 10.0.1.0/24 \
  --name Databases
```

4. Ejecute el comando siguiente en Cloud Shell para crear el grupo de seguridad de red **ERP-SERVERS-NSG**:

CLI de Azure

```
az network nsg create \
  --resource-group $rg \
  --name ERP-SERVERS-NSG
```

Creación de máquinas virtuales que ejecutan Ubuntu

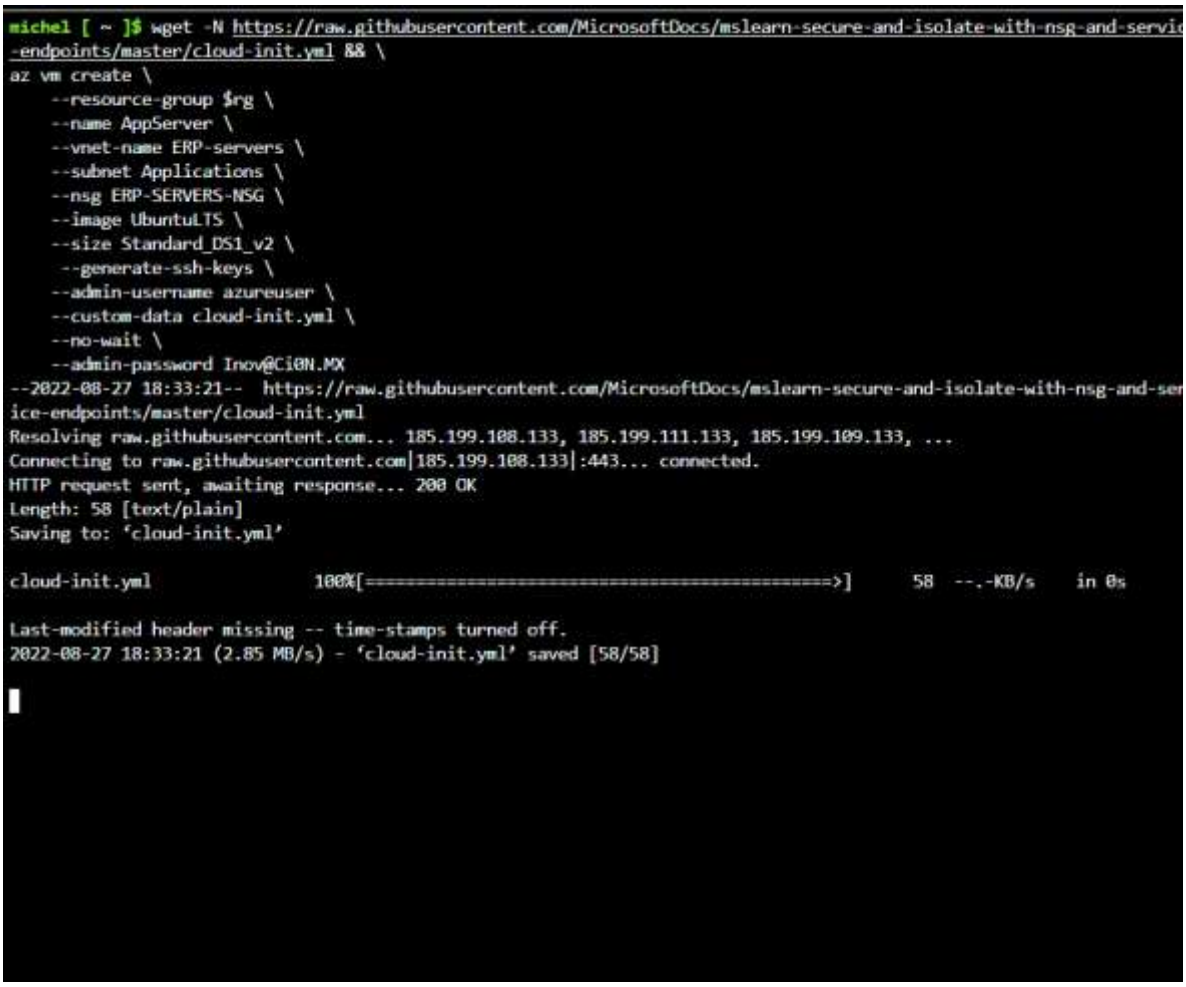
Ahora va a crear dos máquinas virtuales denominadas **AppServer** y **DataServer**.
Implemente **AppServer** en la subred **Applications** y **DataServer** en la subred **Databases**. Agregue las interfaces de red de máquina virtual al grupo de seguridad de red **ERP-SERVERS-NSG**. Luego, para probar el grupo de seguridad de red, use estas máquinas virtuales.

1. Para compilar la máquina virtual **AppServer**, ejecute el comando siguiente en Cloud Shell. Para la cuenta de administrador, reemplace <password> por una contraseña compleja.

CLI de Azure

```
wget -N https://raw.githubusercontent.com/MicrosoftDocs/mslearn-secure-and-isolate-with-nsg-and-service-endpoints/master/cloud-init.yml && \
```

```
az vm create \
    --resource-group $rg \
    --name AppServer \
    --vnet-name ERP-servers \
    --subnet Applications \
    --nsg ERP-SERVERS-NSG \
    --image UbuntuLTS \
    --size Standard_DS1_v2 \
     --generate-ssh-keys \
    --admin-username azureuser \
    --custom-data cloud-init.yml \
    --no-wait \
    --admin-password <password>
```



2. Para compilar la máquina virtual **DataServer**, ejecute el comando siguiente en Cloud Shell. Para la cuenta de administrador, reemplace <password> por una contraseña compleja.

CLI de Azure

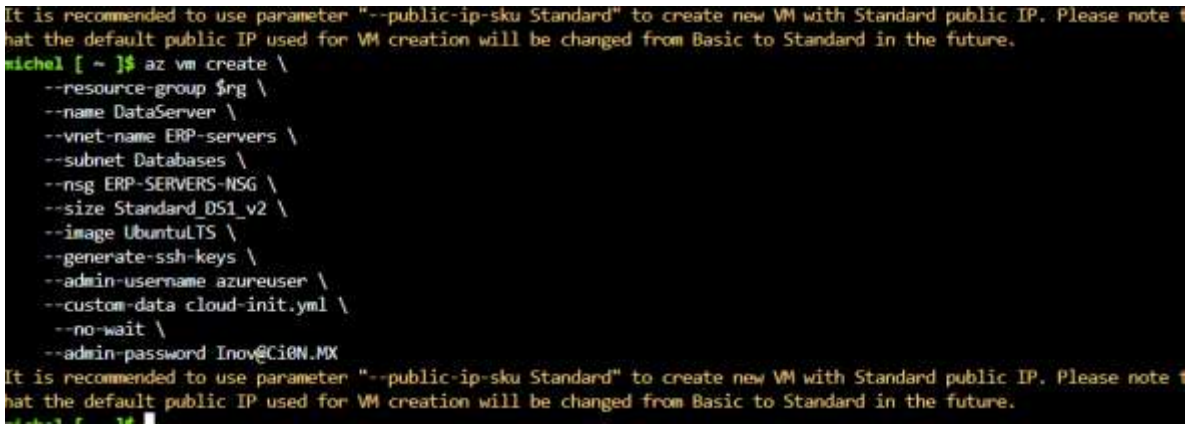
```
az vm create \
   --resource-group $rg \
   --name DataServer \
   --vnet-name ERP-servers \
   --subnet Databases \
   --nsg ERP-SERVERS-NSG \
   --size Standard_DS1_v2 \
   --image UbuntuLTS \
   --generate-ssh-keys \
```

--admin-username azureuser \

--custom-data cloud-init.yml \

--no-wait \

--admin-password <password>



3. Las máquinas virtuales pueden tardar varios minutos en estar en estado de ejecución. Ejecute el comando siguiente en Cloud Shell para confirmar que las máquinas virtuales están en ejecución:

CLI de Azure

az vm list \

--resource-group $rg \

--show-details \

--query "[*].{Name:name, Provisioned:provisioningState, Power:powerState}" \

--output table

Una vez completada la creación de la máquina virtual, debería ver la salida siguiente.

ResultadoCopiar

Name Provisioned Power

---------- ------------ ----------

AppServer Succeeded VM running

DataServer Succeeded VM running

```
michel [ ~ ]$ az vm list \
    --resource-group $rg \
    --show-details \
    --query "[*].{Name:name, Provisioned:provisioningState, Power:powerState}" \
    --output table
Name        Provisioned    Power
----------  -------------  ----------
AppServer   Succeeded      VM running
DataServer  Succeeded      VM running
michel [ ~ ]$
```

Comprobación de la conectividad predeterminada

Ahora va a intentar abrir una sesión de Secure Shell (SSH) para cada una de las máquinas virtuales. Recuerde que hasta ahora ha implementado un grupo de seguridad de red con reglas predeterminadas.

1. Para conectarse a las máquinas virtuales, use SSH directamente desde Cloud Shell. Para ello, necesita las direcciones IP públicas que se han asignado a las máquinas virtuales. Ejecute el comando siguiente en Cloud Shell para mostrar las direcciones IP que se van a usar para conectarse a las máquinas virtuales:

CLI de Azure

az vm list \

--resource-group $rg \

--show-details \

--query "[*].{Name:name, PrivateIP:privateIps, PublicIP:publicIps}" \

--output table

```
----------  -------------  ----------
AppServer   Succeeded      VM running
DataServer  Succeeded      VM running
michel [ ~ ]$ az vm list \
    --resource-group $rg \
    --show-details \
    --query "[*].{Name:name, PrivateIP:privateIps, PublicIP:publicIps}" \
    --output table
Name        PrivateIP    PublicIP
----------  -----------  --------------
AppServer   10.0.0.4     20.237.251.10
DataServer  10.0.1.4     20.237.251.118
michel [ ~ ]$
```

2. Para facilitar la conexión a las máquinas virtuales durante el resto de este ejercicio, asigne las direcciones IP públicas a variables. Ejecute el comando siguiente en Cloud Shell para guardar la dirección IP pública de **AppServer** y **DataServer** en una variable:

Bash

```
APPSERVERIP="$(az vm list-ip-addresses \
        --resource-group $rg \
        --name AppServer \
        --query "[].virtualMachine.network.publicIpAddresses[*].ipAddress" \
        --output tsv)"

DATASERVERIP="$(az vm list-ip-addresses \
        --resource-group $rg \
        --name DataServer \
        --query "[].virtualMachine.network.publicIpAddresses[*].ipAddress" \
        --output tsv)"
```

3. Ejecute el comando siguiente en Cloud Shell para comprobar si se puede conectar a la máquina virtual **AppServer**:

Bash

```
ssh azureuser@$APPSERVERIP -o ConnectTimeout=5
```

Aparecerá un mensaje Connection timed out.

4. Ejecute el comando siguiente en Cloud Shell para comprobar si se puede conectar a la máquina virtual **DataServer**:

Bash

```
ssh azureuser@$DATASERVERIP -o ConnectTimeout=5
```

Aparecerá el mismo mensaje de error de conexión.

Recuerde que las reglas predeterminadas deniegan todo el tráfico entrante en una red virtual, a menos que proceda de la misma red virtual. La regla **Denegar todo el tráfico entrante** ha bloqueado las conexiones SSH entrantes que acaba de intentar.

Entrada

Nombre	Prioridad	IP de origen	IP de destino	Acceso
Permitir el tráfico entrante de red virtual	65000	VIRTUAL_NETWORK	VIRTUAL_NETWORK	Permitir
Denegar todo el tráfico entrante	65500	*	*	Denegar

Creación de una regla de seguridad para SSH

Como acaba de comprobar, las reglas predeterminadas del grupo de seguridad de red **ERP-SERVERS-NSG** incluyen una regla **Denegar todo el tráfico entrante**. Ahora agregará una regla para poder usar SSH para conectarse a **AppServer** y **DataServer**.

1. Ejecute el comando siguiente en Cloud Shell para crear una regla de seguridad de entrada para habilitar el acceso SSH:

```
michel [ ~ ]$ az network nsg rule create \
    --resource-group $rg \
    --nsg-name ERP-SERVERS-NSG \
    --name AllowSSHRule \
    --direction Inbound \
    --priority 100 \
    --source-address-prefixes '*' \
    --source-port-ranges '*' \
    --destination-address-prefixes '*' \
    --destination-port-ranges 22 \
    --access Allow \
    --protocol Tcp \
    --description "Allow inbound SSH"
/ Running ..
```

```
michel [ ~ ]$ az network nsg rule create \
    --resource-group $rg \
    --nsg-name ERP-SERVERS-NSG \
    --name AllowSSHRule \
    --direction Inbound \
    --priority 100 \
    --source-address-prefixes '*' \
    --source-port-ranges '*' \
    --destination-address-prefixes '*' \
    --destination-port-ranges 22 \
    --access Allow \
    --protocol Tcp \
    --description "Allow inbound SSH"
{
  "access": "Allow",
  "description": "Allow inbound SSH",
  "destinationAddressPrefix": "*",
  "destinationAddressPrefixes": [],
  "destinationApplicationSecurityGroups": null,
  "destinationPortRange": "22",
  "destinationPortRanges": [],
  "direction": "Inbound",
  "etag": "W/\"46ef939a-e8f2-463b-b2b9-af2f15c5bb70\"",
  "id": "/subscriptions/c2f06750-c94e-42e9-9895-629c9db91bce/resourceGroups/learn-71cd0808-341a-4b88-bef8-c552e245ce4
d/providers/Microsoft.Network/networkSecurityGroups/ERP-SERVERS-NSG/securityRules/AllowSSHRule",
  "name": "AllowSSHRule",
  "priority": 100,
  "protocol": "Tcp",
  "provisioningState": "Succeeded",
  "resourceGroup": "learn-71cd0808-341a-4b88-bef8-c552e245ce4d",
  "sourceAddressPrefix": "*",
  "sourceAddressPrefixes": [],
  "sourceApplicationSecurityGroups": null,
  "sourcePortRange": "*",
  "sourcePortRanges": [],
  "type": "Microsoft.Network/networkSecurityGroups/securityRules"
}
```

CLI de Azure

```
az network nsg rule create \
    --resource-group $rg \
    --nsg-name ERP-SERVERS-NSG \
    --name AllowSSHRule \
    --direction Inbound \
    --priority 100 \
    --source-address-prefixes '*' \
```

```
--source-port-ranges '*' \
--destination-address-prefixes '*' \
--destination-port-ranges 22 \
--access Allow \
--protocol Tcp \
--description "Allow inbound SSH"
```

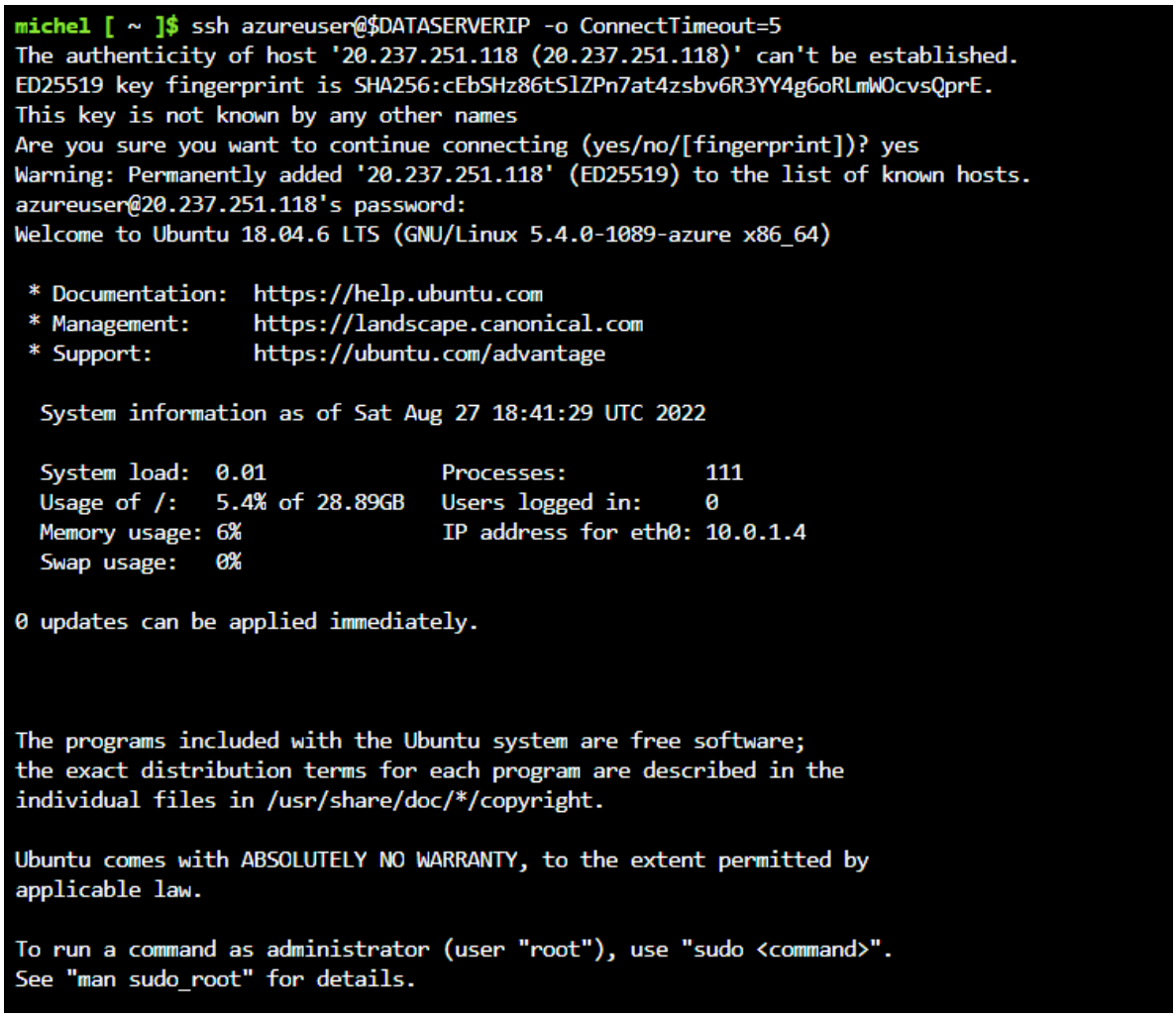
2. Ejecute el comando siguiente en Cloud Shell para comprobar si se puede conectar ahora a la máquina virtual **AppServer**:

Bash

```
ssh azureuser@$APPSERVERIP -o ConnectTimeout=5
```

La regla del grupo de seguridad de red puede tardar uno o dos minutos en surtir efecto. Si recibe un mensaje de error de conexión, vuelva a intentarlo.

3. Ahora debería poder conectarse. Después del mensaje Are you sure you want to continue connecting (yes/no)?, especifique yes.
4. Escriba la contraseña que ha definido al crear la máquina virtual.

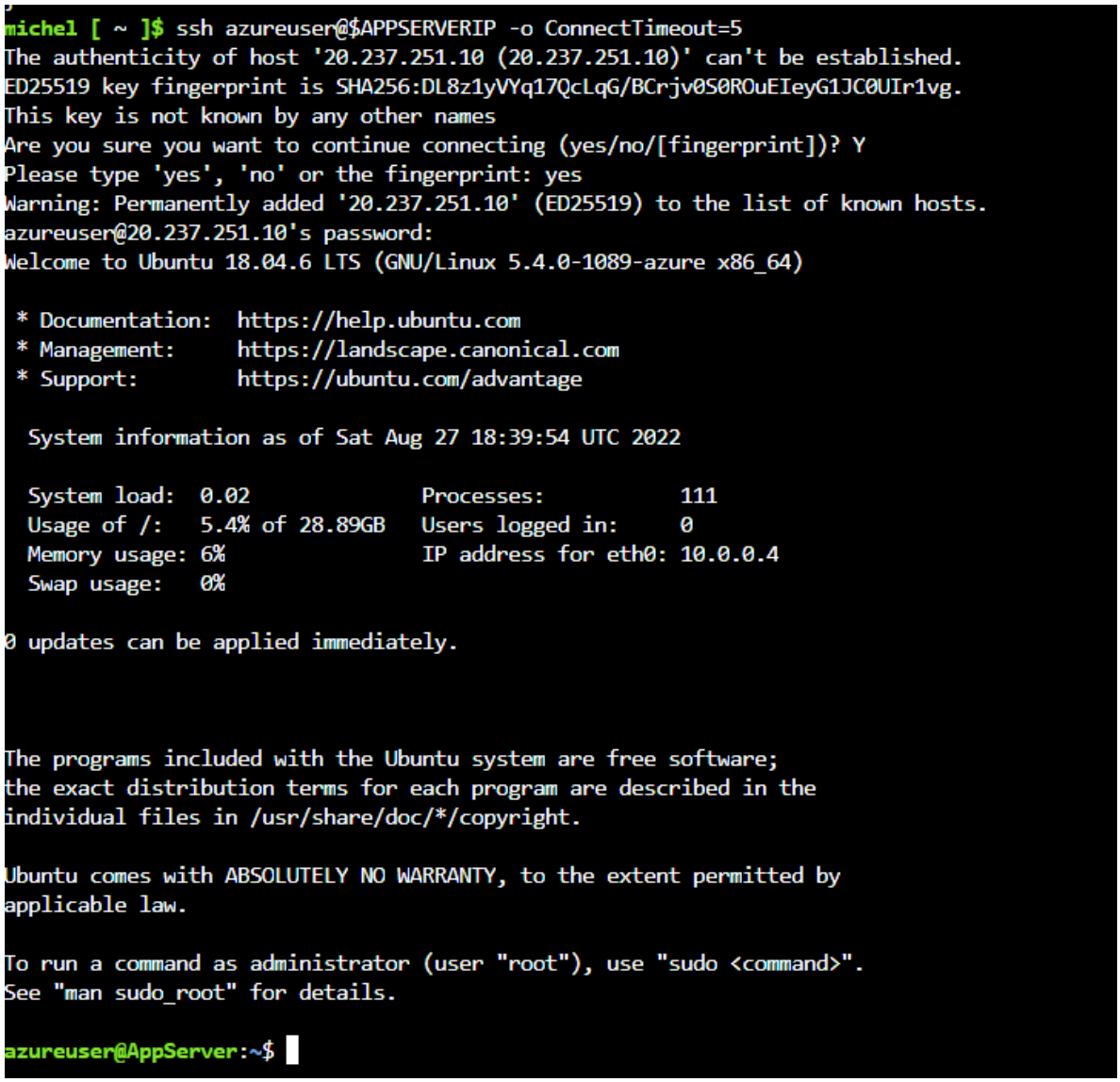


5. Para cerrar la sesión de **AppServer**, escriba exit.
6. Ejecute el comando siguiente en Cloud Shell para comprobar si se puede conectar ahora a la máquina virtual **DataServer**:

Bash

```
ssh azureuser@$DATASERVERIP -o ConnectTimeout=5
```

7. Ahora debería poder conectarse. Después del mensaje Are you sure you want to continue connecting (yes/no)?, especifique yes.
8. Escriba la contraseña que ha definido al crear la máquina virtual.



9. Para cerrar la sesión de **DataServer**, especifique exit.

Creación de una regla de seguridad para impedir el acceso web

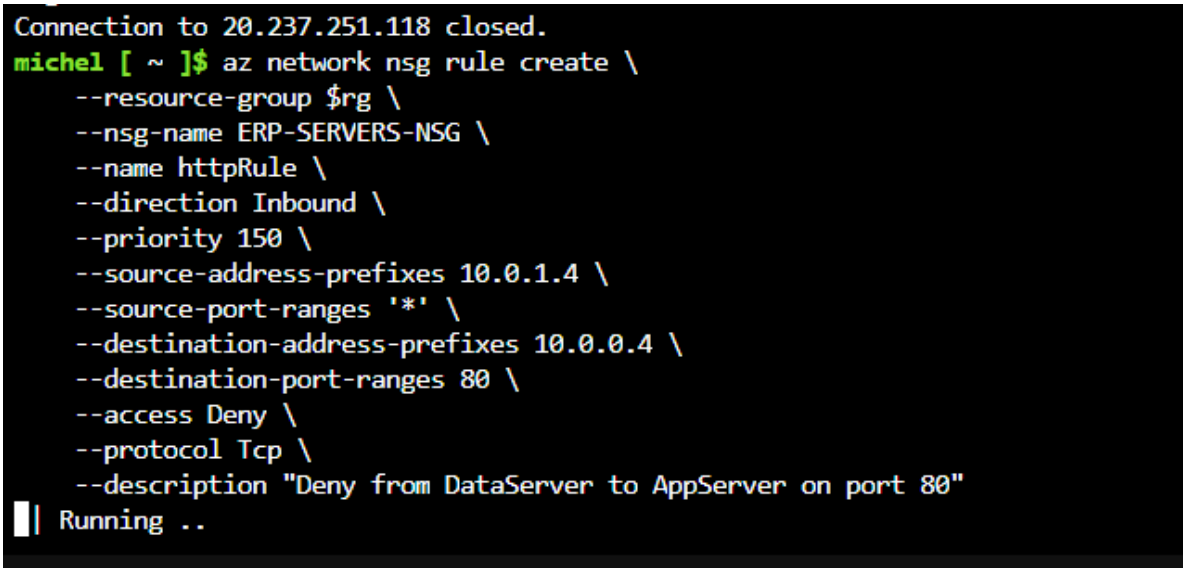
Ahora agregue una regla para que **AppServer** se pueda comunicar con **DataServer** a través de HTTP, pero **DataServer** no se pueda comunicar con **AppServer** a través de HTTP. Estas son las direcciones IP internas para estos servidores:

Nombre del servidor	**Dirección IP**
AppServer	10.0.0.4
DataServer	10.0.1.4

1. Ejecute el comando siguiente en Cloud Shell para crear una regla de seguridad de entrada para denegar el acceso HTTP a través del puerto 80:

CLI de Azure

```
az network nsg rule create \
   --resource-group $rg \
   --nsg-name ERP-SERVERS-NSG \
   --name httpRule \
   --direction Inbound \
   --priority 150 \
   --source-address-prefixes 10.0.1.4 \
   --source-port-ranges '*' \
   --destination-address-prefixes 10.0.0.4 \
   --destination-port-ranges 80 \
   --access Deny \
   --protocol Tcp \
   --description "Deny from DataServer to AppServer on port 80"
```



```
    --resource-group $rg \
    --nsg-name ERP-SERVERS-NSG \
    --name httpRule \
    --direction Inbound \
    --priority 150 \
    --source-address-prefixes 10.0.1.4 \
    --source-port-ranges '*' \
    --destination-address-prefixes 10.0.0.4 \
    --destination-port-ranges 80 \
    --access Deny \
    --protocol Tcp \
    --description "Deny from DataServer to AppServer on port 80"
{
  "access": "Deny",
  "description": "Deny from DataServer to AppServer on port 80",
  "destinationAddressPrefix": "10.0.0.4",
  "destinationAddressPrefixes": [],
  "destinationApplicationSecurityGroups": null,
  "destinationPortRange": "80",
  "destinationPortRanges": [],
  "direction": "Inbound",
  "etag": "W/\"6cf8ec49-992a-43a8-af24-a6e44d23402d\"",
  "id": "/subscriptions/c2f06750-c94e-42e9-9895-629c9db91bce/resourceGroups/learn-71cd0808-341
d/providers/Microsoft.Network/networkSecurityGroups/ERP-SERVERS-NSG/securityRules/httpRule",
  "name": "httpRule",
  "priority": 150,
  "protocol": "Tcp",
  "provisioningState": "Succeeded",
  "resourceGroup": "learn-71cd0808-341a-4b88-bef8-c552e245ce4d",
  "sourceAddressPrefix": "10.0.1.4",
  "sourceAddressPrefixes": [],
  "sourceApplicationSecurityGroups": null,
  "sourcePortRange": "*",
  "sourcePortRanges": [],
  "type": "Microsoft.Network/networkSecurityGroups/securityRules"
}
```

Prueba de la conectividad HTTP entre máquinas virtuales

Ahora, comprobará si la nueva regla funciona. **AppServer** debería poder comunicarse con **DataServer** a través de HTTP. **DataServer** no debería poder comunicarse con **AppServer** a través de HTTP.

1. Para conectarse a la máquina virtual **AppServer**, ejecute el comando siguiente en Cloud Shell. Compruebe si **AppServer** puede comunicarse con **DataServer** a través de HTTP.

Bash

```
ssh -t azureuser@$APPSERVERIP 'wget http://10.0.1.4; exit; bash'
```

```
michel [ ~ ]$ ssh -t azureuser@$APPSERVERIP 'wget http://10.0.1.4; exit; bash'
azureuser@20.237.251.10's password:
--2022-08-27 18:45:27--  http://10.0.1.4/
Connecting to 10.0.1.4:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 10918 (11K) [text/html]
Saving to: 'index.html'

index.html                  100%[=========================================>]  10.66K  --.-KB/s    in 0s

2022-08-27 18:45:27 (292 MB/s) - 'index.html' saved [10918/10918]

Connection to 20.237.251.10 closed.
```

2. Escriba la contraseña que ha definido al crear la máquina virtual.
3. La respuesta debe incluir un mensaje 200 OK.
4. Para conectarse a la máquina virtual **DataServer**, ejecute el comando siguiente en Cloud Shell. Compruebe si **DataServer** puede comunicarse con **AppServer** a través de HTTP.

Bash

ssh -t azureuser@$DATASERVERIP 'wget http://10.0.0.4; exit; bash'

```
michel [ ~ ]$ ssh -t azureuser@$DATASERVERIP 'wget http://10.0.0.4; exit; bash'
azureuser@20.237.251.118's password:
--2022-08-27 18:46:29--  http://10.0.0.4/
Connecting to 10.0.0.4:80... failed: Connection timed out.
Retrying.

--2022-08-27 18:48:40--  (try: 2)  http://10.0.0.4/
Connecting to 10.0.0.4:80... ^CConnection to 20.237.251.118 closed.
michel [ ~ ]$
```

5. Escriba la contraseña que ha definido al crear la máquina virtual.
6. Esto no se debería ejecutar de forma correcta porque ha bloqueado el acceso a través del puerto 80. Después de varios minutos, debe obtener un mensaje Connection timed out. Para detener el comando antes del tiempo de espera, presione

Protección del acceso de red a servicios PaaS mediante puntos de conexión de servicio de red virtual

Ha migrado la aplicación existente y los servidores de bases de datos del sistema de ERP a Azure como máquinas virtuales. Ahora, para reducir los costos y los requisitos administrativos, está planteándose la posibilidad de usar algunos servicios de plataforma como servicio (PaaS) de Azure. Los servicios de almacenamiento contendrán algunos recursos de archivos grandes, como diagramas de ingeniería. Estos diagramas de ingeniería tienen información de su propiedad y deben permanecer protegidos frente a accesos no autorizados. Estos archivos solo deben ser accesibles desde sistemas específicos.

En esta unidad, verá cómo se pueden usar los puntos de conexión de servicio de red virtual para proteger servicios de Azure admitidos.

Puntos de conexión de servicio de red virtual

Use los puntos de conexión de servicio de red virtual para ampliar el espacio de direcciones privadas en Azure proporcionando una conexión directa a los servicios de Azure. Los puntos de conexión de servicio solo permiten proteger los recursos de Azure en la rede virtual. El tráfico del servicio permanecerá en la red troncal de Azure y no pasa a Internet.

De forma predeterminada, todos los servicios de Azure están diseñados para el acceso directo a Internet. Todos los recursos de Azure tienen direcciones IP públicas, incluidos los servicios PaaS como Azure SQL Database y Azure Storage. Como estos servicios se exponen a Internet, cualquiera puede acceder a los servicios de Azure.

Los puntos de conexión de servicio pueden conectar determinados servicios PaaS directamente al espacio de direcciones privado de Azure, por lo que actúan como si estuvieran en la misma red virtual. Use el espacio de direcciones privado para acceder directamente a los servicios PaaS. La incorporación de puntos de conexión de servicio no quita el punto de conexión público. Simplemente proporciona un redireccionamiento del tráfico.

Los puntos de conexión de servicio de Azure están disponibles para muchos servicios, como los siguientes:

- Azure Storage
- Azure SQL Database
- Azure Cosmos DB
- Azure Key Vault
- Azure Service Bus
- Azure Data Lake

Para un servicio como SQL Database, al que no se puede acceder hasta que se agreguen direcciones IP al firewall, los puntos de conexión de servicio siguen siendo una posibilidad. El uso de un punto de conexión de servicio para SQL Database restringe el acceso a redes virtuales específicas, lo que proporciona mayor aislamiento y reduce la superficie expuesta a ataques.

Funcionamiento de los puntos de conexión de servicio

Para habilitar un punto de conexión de servicio, debe:

1. Desactivar el acceso público al servicio.
2. Agregar el punto de conexión de servicio a una red virtual.

Cuando se habilita un punto de conexión de servicio, se restringe el flujo de tráfico y se permite que las máquinas virtuales de Azure accedan directamente al servicio desde el espacio de direcciones privado. Los dispositivos no pueden acceder al servicio desde una red pública.

En una vNIC de máquina virtual implementada, si examina **Rutas eficaces**, verá el punto de conexión de servicio como **Tipo del próximo salto**.

Esta es una tabla de rutas de ejemplo, antes de habilitar un punto de conexión de servicio:

ORIGEN	ESTADO	PREFIJOS DE DIRECCIÓN	TIPO DE PRÓXIMO SALTO
Predeterminado	Activo	10.1.1.0/24	VNet
Predeterminado	Activo	0.0.0.0./0	Internet
Valor predeterminado	Activo	10.0.0.0/8	None
Valor predeterminado	Activo	100.64.0.0./10	Ninguno
Valor predeterminado	Activo	192.168.0.0/16	Ninguno

Y esta es una tabla de rutas de ejemplo después de agregar dos puntos de conexión de servicio a la red virtual:

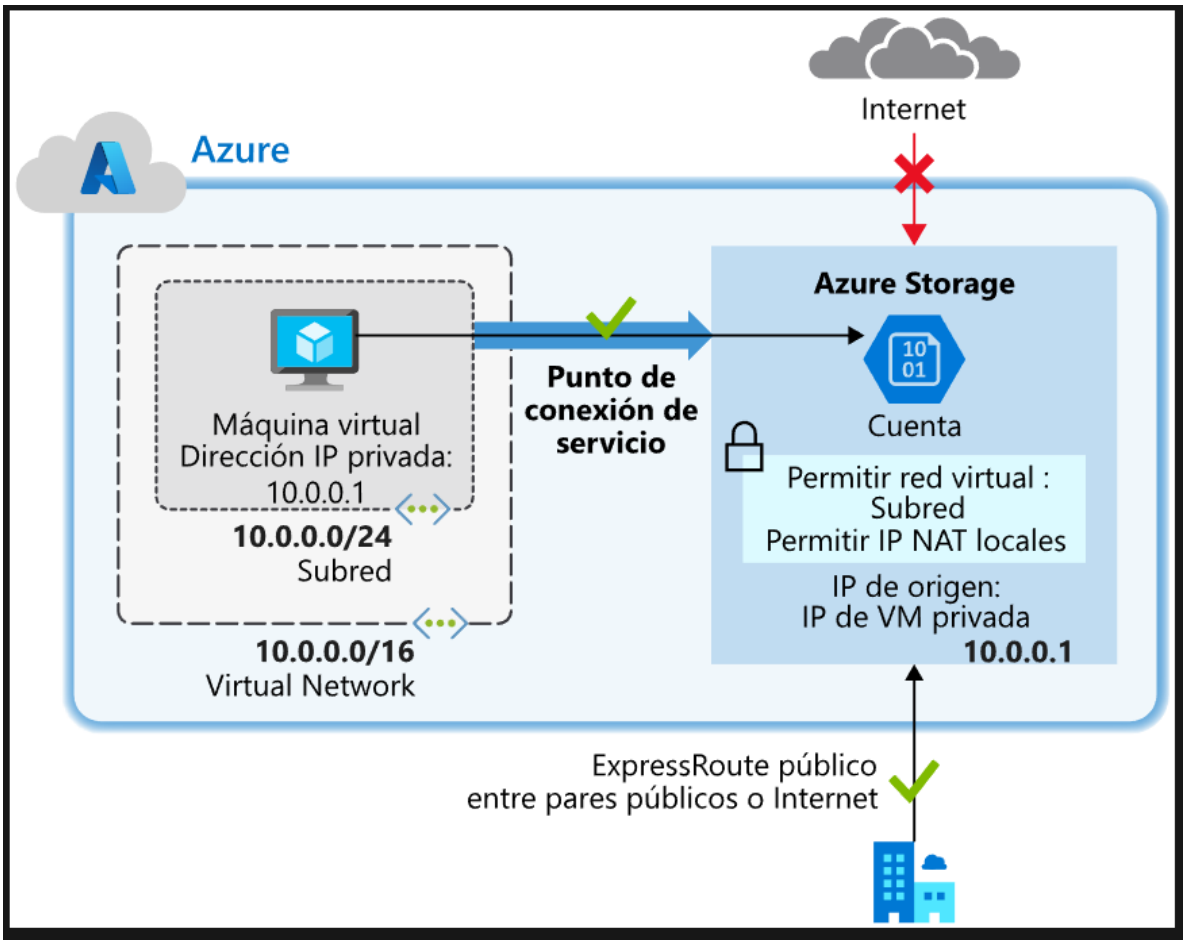
ORIGEN	ESTADO	PREFIJOS DE DIRECCIÓN	TIPO DE PRÓXIMO SALTO
Predeterminado	Activo	10.1.1.0/24	VNet
Predeterminado	Activo	0.0.0.0./0	Internet
Valor predeterminado	Activo	10.0.0.0/8	None
Valor predeterminado	Activo	100.64.0.0./10	Ninguno
Valor predeterminado	Activo	192.168.0.0/16	None
Valor predeterminado	Activo	20.38.106.0/23, 10 más	VirtualNetworkServiceEndpoint
Predeterminado	Activo	20.150.2.0/23, 9 más	VirtualNetworkServiceEndpoint

Ahora, todo el tráfico del servicio se enruta a **VirtualNetworkServiceEndpoint** y sigue siendo interno en Azure.

Puntos de conexión de servicio y redes híbridas

De forma predeterminada, los recursos de servicio que se han protegido mediante puntos de conexión de servicio de red virtual no son accesibles desde redes locales. Para acceder a los recursos desde una red local, use direcciones IP de NAT. Si usa ExpressRoute para la conectividad desde el entorno local a Azure, tiene que identificar las direcciones IP de NAT que ExpressRoute usa. De forma predeterminada, en cada circuito se usan dos direcciones IP de NAT para conectarse a la red troncal de Azure. Después, tendrá que agregar estas direcciones IP a la configuración del firewall IP del recurso de servicio de Azure (por ejemplo, Azure Storage).

En el siguiente diagrama se muestra cómo usar una configuración de punto de conexión de servicio y firewall para permitir que los dispositivos locales accedan a los recursos de Azure Storage.



Ejercicio: Restricción del acceso a Azure Storage mediante puntos de conexión de servicio

Como arquitecto de soluciones, planea mover archivos de diagrama de ingeniería confidenciales a Azure Storage. Los archivos solo deben ser accesibles desde equipos internos de la red corporativa. Quiere crear un punto de conexión de servicio de red virtual para Azure Storage con el fin de proteger la conectividad a las cuentas de almacenamiento.

En esta unidad, creará un punto de conexión de servicio y usará reglas de red para restringir el acceso a Azure Storage. Creará un punto de conexión de servicio de red virtual para Azure Storage en la subred **Databases**. Después, comprobará que la máquina virtual **DataServer** puede acceder a Azure Storage. Por último, va a comprobar que la máquina virtual **AppServer**, que se encuentra en otra subred, no puede acceder al almacenamiento.

Incorporación de reglas al grupo de seguridad de red

Asegúrese de que las comunicaciones con Azure Storage pasan a través del punto de conexión de servicio. Agregue reglas de salida para permitir el acceso al servicio de Storage, pero denegando el resto del tráfico de Internet.

1. Ejecute el siguiente comando en Cloud Shell para crear una regla de salida que permita el acceso a Storage:

CLI de AzureCopiar

```
az network nsg rule create \
  --resource-group $rg \
  --nsg-name ERP-SERVERS-NSG \
  --name Allow_Storage \
  --priority 190 \
  --direction Outbound \
  --source-address-prefixes "VirtualNetwork" \
  --source-port-ranges '*' \
  --destination-address-prefixes "Storage" \
  --destination-port-ranges '*' \
  --access Allow \
  --protocol '*' \
  --description "Allow access to Azure Storage"
```

2. Ejecute el siguiente comando en Cloud Shell para crear una regla de salida para denegar todo el acceso a Internet:

CLI de AzureCopiar

```
az network nsg rule create \
  --resource-group $rg \
  --nsg-name ERP-SERVERS-NSG \
  --name Deny_Internet \
  --priority 200 \
  --direction Outbound \
  --source-address-prefixes "VirtualNetwork" \
```

```
    --source-port-ranges '*' \
    --destination-address-prefixes "Internet" \
    --destination-port-ranges '*' \
    --access Deny \
    --protocol '*' \
    --description "Deny access to Internet."
```

Ahora debería tener las reglas siguientes en ERP-SERVERS-NSG:

Nombre de la regla	**Dirección**	**Prioridad**	**Propósito**
AllowSSHRule	Entrada	100	Permitir SSH de entrada
httpRule	Entrada	150	Denegar desde DataServer a AppServer en 80
Allow_Storage	Salida	190	Permitir el acceso a Azure Storage
Deny_Internet	Salida	200	Denegar el acceso a Internet desde la red virtual

En este punto, tanto **AppServer** como **DataServer** tienen acceso al servicio Azure Storage.

Configuración de la cuenta de almacenamiento y el recurso compartido

En este paso, creará una cuenta de almacenamiento y, después, le agregará un recurso compartido de archivos de Azure. Este recurso compartido es donde almacenará los diagramas de ingeniería.

1. Ejecute el siguiente comando en Cloud Shell para crear una cuenta de almacenamiento para los documentos de ingeniería:

BashCopiar

```
STORAGEACCT=$(az storage account create \
        --resource-group $rg \
        --name engineeringdocs$RANDOM \
        --sku Standard_LRS \
        --query "name" | tr -d '"')
```

2. Ejecute el siguiente comando en Cloud Shell para almacenar la clave principal del almacenamiento en una variable:

BashCopiar

```
STORAGEKEY=$(az storage account keys list \
        --resource-group $rg \
```

--account-name $STORAGEACCT \

--query "[0].value" | tr -d '"')

3. Ejecute el siguiente comando en Cloud Shell para crear un recurso compartido de archivos de Azure con el nombre **erp-data-share**:

CLI de AzureCopiar

az storage share create \

--account-name $STORAGEACCT \

--account-key $STORAGEKEY \

--name "erp-data-share"

Habilitación del punto de conexión de servicio

Ahora tendrá que configurar la cuenta de almacenamiento para que sea accesible solamente desde los servidores de bases de datos, mediante la asignación del punto de conexión de almacenamiento a la subred **Databases**. Después, necesitará agregar una regla de seguridad a la cuenta de almacenamiento.

1. Ejecute el siguiente comando en Cloud Shell para asignar el punto de conexión **Microsoft.Storage** a la subred:

CLI de AzureCopiar

az network vnet subnet update \

--vnet-name ERP-servers \

--resource-group $rg \

--name Databases \

--service-endpoints Microsoft.Storage

2. Ejecute el siguiente comando en Cloud Shell para denegar todo acceso para cambiar la acción predeterminada a Deny. Después de que se deniega el acceso a la red, no se puede acceder a la cuenta de almacenamiento desde ninguna red.

CLI de AzureCopiar

az storage account update \

--resource-group $rg \

--name $STORAGEACCT \

--default-action Deny

3. Ejecute el siguiente comando en Cloud Shell para restringir el acceso a la cuenta de almacenamiento. De forma predeterminada, las cuentas de almacenamiento están

abiertas para aceptar todo el tráfico. Quiere que solo el tráfico procedente de la subred **Databases** pueda acceder al almacenamiento.

CLI de AzureCopiar

```
az storage account network-rule add \
  --resource-group $rg \
  --account-name $STORAGEACCT \
  --vnet-name ERP-servers \
  --subnet Databases
```

Prueba del acceso a los recursos de almacenamiento

En este paso, se conectará a los dos servidores y comprobará que solo **DataServer** tiene acceso al recurso compartido de archivos de Azure en la cuenta de almacenamiento.

1. Ejecute el siguiente comando en Cloud Shell para guardar las direcciones IP públicas de **AppServer** y **DataServer** en variables:

BashCopiar

```
APPSERVERIP="$(az vm list-ip-addresses \
        --resource-group $rg \
        --name AppServer \
        --query "[].virtualMachine.network.publicIpAddresses[*].ipAddress" \
        --output tsv)"

DATASERVERIP="$(az vm list-ip-addresses \
        --resource-group $rg \
        --name DataServer \
        --query "[].virtualMachine.network.publicIpAddresses[*].ipAddress" \
        --output tsv)"
```

2. Ejecute el siguiente comando en Cloud Shell para conectarse a la máquina virtual **AppServer** e intentar montar el recurso compartido de archivos de Azure:

BashCopiar

```
ssh -t azureuser@$APPSERVERIP \
  "mkdir azureshare; \
```

```
sudo mount -t cifs //$STORAGEACCT.file.core.windows.net/erp-data-share azureshare \
-o
vers=3.0,username=$STORAGEACCT,password=$STORAGEKEY,dir_mode=0777,file_mode=0777,sec=ntlmssp; findmnt \
-t cifs; exit; bash"
```

3. Escriba la contraseña que ha usado al crear la máquina virtual.
4. La respuesta debe incluir un mensaje mount error. Esta conexión no se permite porque no hay ningún punto de conexión de servicio para la cuenta de almacenamiento en la subred **Applications**.
5. Ejecute el siguiente comando en Cloud Shell para conectarse a la máquina virtual **DataServer** e intentar montar el recurso compartido de archivos de Azure.

BashCopiar

```
ssh -t azureuser@$DATASERVERIP \
"mkdir azureshare; \
sudo mount -t cifs //$STORAGEACCT.file.core.windows.net/erp-data-share azureshare \
-o
vers=3.0,username=$STORAGEACCT,password=$STORAGEKEY,dir_mode=0777,file_mode=0777,sec=ntlmssp;findmnt \
-t cifs; exit; bash"
```

6. Escriba la contraseña que ha usado al crear la máquina virtual.
7. El montaje debe ser correcto y la respuesta debe incluir los detalles del punto de montaje. Esto se permite porque ha creado el punto de conexión de servicio para la cuenta de almacenamiento en la subred **Databases**.

Mediante el punto de conexión de servicio de almacenamiento de la subred **Databases** ya ha comprobado que **DataServer** puede acceder al almacenamiento. También ha comprobado que **AppServer** no puede acceder al almacenamiento. El motivo es que este servidor está en otra subred y no tiene acceso al punto de conexión de servicio de red virtual.

Como arquitecto de soluciones, planea mover archivos de diagrama de ingeniería confidenciales a Azure Storage. Los archivos solo deben ser accesibles desde equipos internos de la red corporativa. Quiere crear un punto de conexión de servicio de red virtual para Azure Storage con el fin de proteger la conectividad a las cuentas de almacenamiento.

En esta unidad, creará un punto de conexión de servicio y usará reglas de red para restringir el acceso a Azure Storage. Creará un punto de conexión de servicio de red virtual para Azure Storage en la subred Databases. Después, comprobará que la máquina virtual DataServer puede acceder a Azure Storage. Por último, va a comprobar que la máquina virtual AppServer, que se encuentra en otra subred, no puede acceder al almacenamiento.

Incorporación de reglas al grupo de seguridad de red

Asegúrese de que las comunicaciones con Azure Storage pasan a través del punto de conexión de servicio. Agregue reglas de salida para permitir el acceso al servicio de Storage, pero denegando el resto del tráfico de Internet.

- Ejecute el siguiente comando en Cloud Shell para crear una regla de salida que permita el acceso a Storage:

  CLI de AzureCopiar

```
az network nsg rule create \
    --resource-group $rg \
    --nsg-name ERP-SERVERS-NSG \
    --name Allow_Storage \
    --priority 190 \
    --direction Outbound \
    --source-address-prefixes "VirtualNetwork" \
    --source-port-ranges '*' \
    --destination-address-prefixes "Storage" \
    --destination-port-ranges '*' \
    --access Allow \
    --protocol '*' \
    --description "Allow access to Azure Storage"
```

- Ejecute el siguiente comando en Cloud Shell para crear una regla de salida para denegar todo el acceso a Internet:

  CLI de AzureCopiar

```
az network nsg rule create \
    --resource-group $rg \
    --nsg-name ERP-SERVERS-NSG \
    --name Deny_Internet \
    --priority 200 \
```

```
    --direction Outbound \
    --source-address-prefixes "VirtualNetwork" \
    --source-port-ranges '*' \
    --destination-address-prefixes "Internet" \
    --destination-port-ranges '*' \
    --access Deny \
    --protocol '*' \
    --description "Deny access to Internet."
```

Ahora debería tener las reglas siguientes en ERP-SERVERS-NSG:

Nombre de la regla	Dirección	Prioridad	Propósito
AllowSSHRule	Entrada	100	Permitir SSH de entrada
httpRule	Entrada	150	Denegar desde DataServer a AppServer en 80
Allow_Storage	Salida	190	Permitir el acceso a Azure Storage
Deny_Internet	Salida	200	Denegar el acceso a Internet desde la red virtual

En este punto, tanto AppServer como DataServer tienen acceso al servicio Azure Storage.

Configuración de la cuenta de almacenamiento y el recurso compartido

En este paso, creará una cuenta de almacenamiento y, después, le agregará un recurso compartido de archivos de Azure. Este recurso compartido es donde almacenará los diagramas de ingeniería.

- Ejecute el siguiente comando en Cloud Shell para crear una cuenta de almacenamiento para los documentos de ingeniería:

  Bash Copiar

  ```
  STORAGEACCT=$(az storage account create \
                --resource-group $rg \
                --name engineeringdocs$RANDOM \
                --sku Standard_LRS \
                --query "name" | tr -d '"')
  ```

- Ejecute el siguiente comando en Cloud Shell para almacenar la clave principal del almacenamiento en una variable:

BashCopiar

```
STORAGEKEY=$(az storage account keys list \
                --resource-group $rg \
                --account-name $STORAGEACCT \
                --query "[0].value" | tr -d '"')
```

- Ejecute el siguiente comando en Cloud Shell para crear un recurso compartido de archivos de Azure con el nombre erp-data-share:

CLI de AzureCopiar

```
az storage share create \
    --account-name $STORAGEACCT \
    --account-key $STORAGEKEY \
    --name "erp-data-share"
```

Habilitación del punto de conexión de servicio

Ahora tendrá que configurar la cuenta de almacenamiento para que sea accesible solamente desde los servidores de bases de datos, mediante la asignación del punto de conexión de almacenamiento a la subred Databases. Después, necesitará agregar una regla de seguridad a la cuenta de almacenamiento.

- Ejecute el siguiente comando en Cloud Shell para asignar el punto de conexión Microsoft.Storage a la subred:

CLI de AzureCopiar

```
az network vnet subnet update \
    --vnet-name ERP-servers \
    --resource-group $rg \
    --name Databases \
    --service-endpoints Microsoft.Storage
```

- Ejecute el siguiente comando en Cloud Shell para denegar todo acceso para cambiar la acción predeterminada a Deny. Después de que se deniega el acceso a la red, no se puede acceder a la cuenta de almacenamiento desde ninguna red.

CLI de AzureCopiar

```
az storage account update \
```

```
    --resource-group $rg \
    --name $STORAGEACCT \
    --default-action Deny
```

- Ejecute el siguiente comando en Cloud Shell para restringir el acceso a la cuenta de almacenamiento. De forma predeterminada, las cuentas de almacenamiento están abiertas para aceptar todo el tráfico. Quiere que solo el tráfico procedente de la subred Databases pueda acceder al almacenamiento.

  CLI de AzureCopiar

```
az storage account network-rule add \
    --resource-group $rg \
    --account-name $STORAGEACCT \
    --vnet-name ERP-servers \
    --subnet Databases
```

Prueba del acceso a los recursos de almacenamiento

En este paso, se conectará a los dos servidores y comprobará que solo DataServer tiene acceso al recurso compartido de archivos de Azure en la cuenta de almacenamiento.

- Ejecute el siguiente comando en Cloud Shell para guardar las direcciones IP públicas de AppServer y DataServer en variables:

  BashCopiar

```
APPSERVERIP="$(az vm list-ip-addresses \
                    --resource-group $rg \
                    --name AppServer \
                    --query
"[].virtualMachine.network.publicIpAddresses[*].ipAddress" \
                    --output tsv)"

DATASERVERIP="$(az vm list-ip-addresses \
                    --resource-group $rg \
                    --name DataServer \
                    --query
"[].virtualMachine.network.publicIpAddresses[*].ipAddress" \
```

```
--output tsv)"
```

- Ejecute el siguiente comando en Cloud Shell para conectarse a la máquina virtual AppServer e intentar montar el recurso compartido de archivos de Azure:

  BashCopiar

```
ssh -t azureuser@$APPSERVERIP \
    "mkdir azureshare; \
    sudo mount -t cifs
//$STORAGEACCT.file.core.windows.net/erp-data-share azureshare
\
    -o
vers=3.0,username=$STORAGEACCT,password=$STORAGEKEY,dir_mode=0
777,file_mode=0777,sec=ntlmssp; findmnt \
    -t cifs; exit; bash"
```

- Escriba la contraseña que ha usado al crear la máquina virtual.
- La respuesta debe incluir un mensaje `mount error`. Esta conexión no se permite porque no hay ningún punto de conexión de servicio para la cuenta de almacenamiento en la subred Applications.
- Ejecute el siguiente comando en Cloud Shell para conectarse a la máquina virtual DataServer e intentar montar el recurso compartido de archivos de Azure.

  BashCopiar

```
ssh -t azureuser@$DATASERVERIP \
    "mkdir azureshare; \
    sudo mount -t cifs
//$STORAGEACCT.file.core.windows.net/erp-data-share azureshare
\
    -o
vers=3.0,username=$STORAGEACCT,password=$STORAGEKEY,dir_mode=0
777,file_mode=0777,sec=ntlmssp;findmnt \
    -t cifs; exit; bash"
```

- Escriba la contraseña que ha usado al crear la máquina virtual.
- El montaje debe ser correcto y la respuesta debe incluir los detalles del punto de montaje. Esto se permite porque ha creado el punto de conexión de servicio para la cuenta de almacenamiento en la subred Databases.

Mediante el punto de conexión de servicio de almacenamiento de la subred Databases ya ha comprobado que DataServer puede acceder al almacenamiento. También ha comprobado que AppServer no puede acceder al almacenamiento. El motivo es que este servidor está en otra subred y no tiene acceso al punto de conexión de servicio de red virtual.