**Introducción**

Completado100 XP

* 1 minuto

Todas las aplicaciones y todos los servicios, tanto si están en la nube como en un entorno local, deben diseñarse teniendo en cuenta la seguridad, Hay demasiado que perder. Por ejemplo, un ataque por denegación de servicio podría evitar que los clientes llegaran al sitio o los servicios web, y podría impedirle hacer negocios. O bien, el sitio web podría ser objeto de ataques, lo que provocaría daños en la reputación. Una vulneración de datos sería incluso peor, ya que puede arruinar la confianza que tanto ha costado conseguir y provoca daños personales y financieros considerables.

**Conozca Tailwind Traders**

[Tailwind Traders](https://www.tailwindtraders.com/) es una empresa ficticia que distribuye productos para la remodelación del hogar. Esta empresa cuenta con ferreterías minoristas en todo el mundo y en línea.



Tailwind Traders está especializada en precios competitivos, envío rápido y una amplia gama de artículos. Va a examinar las tecnologías en la nube para mejorar las operaciones comerciales y apoyar el crecimiento en nuevos mercados. Al migrar a la nube, la empresa tiene previsto mejorar su experiencia de compra para diferenciarse de sus competidores.

**¿Cómo protegerá Tailwind Traders sus redes?**

A medida que Tailwind Traders se cambia a la nube, debe evaluar sus necesidades de seguridad antes de poder implementar una sola línea de código en producción.

Aunque la seguridad se debe tener en cuenta en todas las capas de las aplicaciones de la empresa (desde los servidores físicos hasta los datos de la aplicación), hay algunos factores que se relacionan específicamente con la configuración de red y el tráfico de red de cargas de trabajo basadas en la nube.

En este módulo, se centrará en las funcionalidades de seguridad de red de Azure y revisará cómo estas le ayudan a proteger sus soluciones en la nube, en función de sus necesidades empresariales.

**Objetivos de aprendizaje**

Después de completar este módulo, podrá:

* Identificar las capas que componen una estrategia de *defensa en profundidad*.
* Explicar cómo Azure Firewall permite controlar qué tráfico se permite en la red.
* Configurar grupos de seguridad de red para filtrar el tráfico de red desde y hacia los recursos de Azure en una red virtual de Microsoft Azure.
* Explicar cómo Azure DDoS Protection ayuda a proteger sus recursos de Azure frente a ataques DDoS.

**Requisitos previos**

* Debe estar familiarizado con la terminología y los conceptos básicos relacionados con la informática.
* Es útil estar familiarizado con la informática en la nube, pero no es necesario.

**¿Qué es la defensa en profundidad?**

Completado100 XP

* 6 minutos

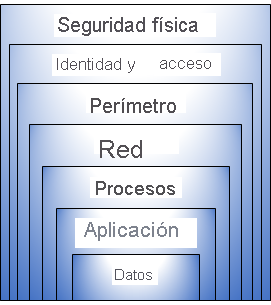
En la actualidad, Tailwind Traders ejecuta sus cargas de trabajo de forma local, en su centro de datos. La ejecución en el entorno local implica que es responsable de todos los aspectos de la seguridad, desde el acceso físico a los edificios hasta el modo en que los datos entran y salen de la red. La empresa quiere saber cómo se compara su estrategia de defensa actual en profundidad con la ejecución en la nube.

El objetivo de la *defensa en profundidad* es proteger la información y evitar que personas no autorizadas a acceder a ella puedan sustraerla.

Una estrategia de defensa en profundidad usa una serie de mecanismos para ralentizar el avance de un ataque dirigido a adquirir acceso no autorizado a los datos.

**Capas de la defensa en profundidad**

La defensa en profundidad se puede visualizar como un conjunto de capas, con los datos que se deben proteger en el centro.



Cada capa proporciona protección de modo que, si se produce una brecha en una capa, ya existe otra en funcionamiento para evitar una mayor exposición. Este enfoque elimina la dependencia de cualquier capa de protección única. Ralentiza un ataque y proporciona telemetría de alertas sobre la que pueden actuar los equipos de seguridad, ya sea de forma automática o manual.

Aquí tiene una breve descripción del rol de cada capa:

* La capa de *seguridad física* es la primera línea de defensa para proteger el hardware informático del centro de datos.
* La capa de *identidad y acceso* controla el acceso a la infraestructura y al control de cambios.
* La capa *perimetral* usa protección frente a ataques de denegación de servicio distribuido (DDoS) para filtrar los ataques a gran escala antes de que puedan causar una denegación de servicio para los usuarios.
* La capa de *red* limita la comunicación entre los recursos a través de controles de acceso y segmentación.
* La capa de *proceso* protege el acceso a las máquinas virtuales.
* La capa de *aplicación* ayuda a garantizar que las aplicaciones sean seguras y estén libres de vulnerabilidades de seguridad.
* La capa de *datos* controla el acceso a los datos empresariales y de clientes que es necesario proteger.

Estas capas proporcionan una guía para ayudarle a tomar decisiones de configuración de seguridad en todas las capas de las aplicaciones.

Azure proporciona herramientas y características de seguridad en todas las capas del concepto de defensa en profundidad. Veamos cada capa con más detalle:



**Seguridad física**

La protección física del acceso a los edificios y el control del acceso al hardware de proceso del centro de datos son la primera línea de defensa.

La intención de la seguridad física es proporcionar medidas de seguridad físicas contra el acceso a los recursos. Estas medidas garantizan que no se puedan omitir otras capas y se controle apropiadamente la pérdida o el robo. Microsoft usa varios mecanismos de seguridad físicos en sus centros de datos de la nube.



**Identidad y acceso**

En esta capa, es importante que realice lo siguiente:

* Controle el acceso a la infraestructura y al control de cambios.
* Use el inicio de sesión único (SSO)y la autenticación multifactor.
* Audite los eventos y los cambios.

La capa de identidad y acceso consiste en garantizar que las identidades están protegidas, que solo se otorga el acceso necesario y que se registran los cambios y los eventos de inicio de sesión.

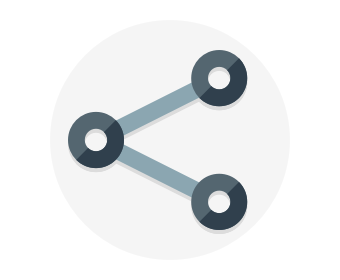


**Perímetro**

En esta capa, es importante que realice lo siguiente:

* Use protección contra DDoS para filtrar los ataques a gran escala antes de que puedan afectar a la disponibilidad de un sistema para los usuarios.
* Use firewalls perimetrales para identificar los ataques malintencionados contra la red y alertar sobre ellos.

En el perímetro de la red, se trata de la protección frente a ataques basados en red contra los recursos. Identificar estos ataques, eliminar sus repercusiones y recibir alertas sobre ellos cuando suceden son formas importantes de proteger la red.



**Network**

En esta capa, es importante que realice lo siguiente:

* Limite la comunicación entre los recursos.
* Deniegue de forma predeterminada.
* Restrinja el acceso entrante de Internet y limite el saliente cuando sea apropiado.
* Implemente conectividad segura a las redes locales.

En esta capa, el enfoque está en limitar la conectividad de la red en todos los recursos para permitir solo la necesaria. Al limitar esta comunicación, se reduce el riesgo de que se propaguen los ataques a otros sistemas de la red.



**Proceso**

En esta capa, es importante que realice lo siguiente:

* Proteja el acceso a las máquinas virtuales.
* Implemente la protección del punto de conexión de los dispositivos y mantenga los sistemas revisados y actualizados.

El software malintencionado, los sistemas sin revisiones aplicadas y los sistemas protegidos inadecuadamente abren el entorno a los ataques. El enfoque en esta capa es asegurarse de que sus recursos de proceso estén seguros y de que cuenta con los controles adecuados para minimizar los problemas de seguridad.



**Aplicación**

En esta capa, es importante que realice lo siguiente:

* Garantice que las aplicaciones son seguras y están libres de vulnerabilidades.
* Almacene los secretos de aplicación confidenciales en un medio de almacenamiento seguro.
* Convierta la seguridad en un requisito de diseño en todo el desarrollo de aplicaciones.

La integración de la seguridad en el ciclo de vida de desarrollo de aplicaciones ayuda a reducir el número de vulnerabilidades en el código. Todos los equipos de desarrollo deberían asegurarse de que sus aplicaciones son seguras de forma predeterminada.



**Datos**

En casi todos los casos, los atacantes intentan conseguir datos:

* Almacenados en una base de datos.
* Almacenados en discos en máquinas virtuales.
* Almacenados en aplicaciones de software como servicio (SaaS), como Office 365.
* Administrados mediante el almacenamiento en la nube.

Los que almacenan y controlan el acceso a los datos son responsables de asegurarse de que están protegidos correctamente. A menudo, los requisitos legales dictan los controles y procesos que deben cumplirse para garantizar la confidencialidad, la integridad y la disponibilidad de los datos.

**Posición de seguridad**

El *nivel de seguridad* es la capacidad de su organización de protegerse frente a amenazas de seguridad y responder a ellas. Los principios comunes usados para definir un nivel de seguridad son la *confidencialidad*, la *integridad* y la *disponibilidad*, lo que se conoce colectivamente como CIA por sus siglas en inglés.

* **Confidencialidad**

El *principio de privilegios mínimos* implica restringir el acceso a la información únicamente a los usuarios a las que se concede acceso de forma explícita, solo al nivel necesario para realizar su trabajo. Esta información incluye la protección de contraseñas de usuario, contenido de correo electrónico y niveles de acceso a las aplicaciones y a la infraestructura subyacente.

* **Integridad**

Evitar cambios no autorizados en la información:

* + En reposo: cuando se almacenan.
  + En tránsito: cuando se transfieren de un lugar a otro, incluido desde un equipo local a la nube.

Un enfoque común que se usa en la transmisión de datos es la creación de una huella digital única de los datos por parte del remitente mediante un algoritmo hash unidireccional. El hash se envía al receptor junto con los datos. El receptor vuelve a calcular el hash de los datos y lo compara con el original para asegurarse de que los datos no se han perdido ni modificado en tránsito.

* **Disponibilidad**

Asegúrese de que los servicios funcionan y que solo pueden acceder a ellos los usuarios autorizados. Los *ataques por denegación de servicio* están diseñados para degradar la disponibilidad de un sistema, lo que afecta a sus usuarios.

**Protección de redes virtuales mediante el uso de Azure Firewall**

Completado100 XP

* 5 minutos

Un *firewall* es un dispositivo de seguridad de red que supervisa el tráfico de red entrante y saliente y decide si se permite o bloquea un tráfico específico en función de un conjunto definido de reglas de seguridad. Puede crear reglas de firewall que especifiquen intervalos de direcciones IP. Solo los clientes a los que se les hayan concedido direcciones IP de dentro de dichos intervalos pueden acceder al servidor de destino. Las reglas de firewall también pueden incluir información específica de puertos y protocolos de red.

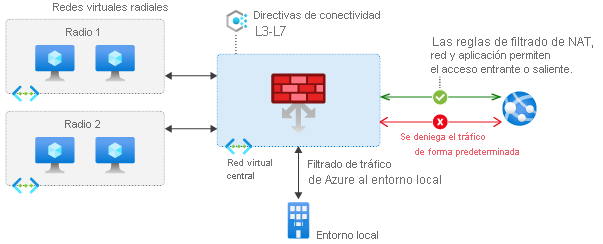
En la actualidad, Tailwind Traders ejecuta dispositivos de firewall, que combinan hardware y software, para proteger su red local. Para funcionar, estos dispositivos de firewall necesitan una cuota de licencia mensual, y que el personal de TI realice un mantenimiento rutinario. A medida que Tailwind Traders se cambia a la nube, el administrador de TI quiere saber qué servicios de Azure pueden proteger las redes en la nube y las redes locales de la empresa.

En esta parte, explorará Azure Firewall.

**¿Qué es Azure Firewall?**

[Azure Firewall](https://azure.microsoft.com/services/azure-firewall) es un servicio de seguridad de red administrado y basado en la nube que ayuda a proteger los recursos en las redes virtuales de Azure. Una red virtual es similar a una red tradicional con la que trabajaría en su propio centro de datos. Es un bloque de creación fundamental para la red privada que permite que las máquinas virtuales y otros recursos de proceso se comuniquen de forma segura entre sí, con Internet y con redes locales.

Este es un diagrama en el que se muestra una implementación básica de Azure Firewall:

[](https://docs.microsoft.com/es-mx/learn/azure-fundamentals/secure-network-connectivity-azure/media/3-firewall-overview-large.png#lightbox)

Azure Firewall es un firewall *con estado*. Un firewall con estado analiza el contexto completo de una conexión de red, no solo un paquete individual de tráfico de red. Azure Firewall incluye alta disponibilidad y escalabilidad en la nube sin restricciones.

Azure Firewall proporciona una ubicación central para crear, aplicar y registrar directivas de conectividad de red y de aplicaciones entre suscripciones y redes virtuales. Azure Firewall usa una dirección IP pública estática (invariable) para los recursos de redes virtuales, lo que permite que los firewall externos identifiquen el tráfico entrante de redes virtuales. El servicio se integra con Azure Monitor para habilitar el registro y el análisis.

Azure Firewall proporciona muchas características, entre las que se incluyen:

* Alta disponibilidad integrada
* Escalabilidad en la nube sin restricciones.
* Reglas de filtrado entrante y saliente.
* Compatibilidad con la traducción de direcciones de red de destino (DNAT).
* El registro de Azure Monitor.

Normalmente implementa Azure Firewall en una red virtual central para controlar el acceso general a la red.

En este vídeo breve se explica cómo Azure Firewall supervisa el tráfico de red de entrante y saliente en función de un conjunto definido de reglas de seguridad. El vídeo también explica las diferencias entre Azure Firewall y las aplicaciones de firewall tradicionales.

**¿Qué se puede configurar con Azure Firewall?**

Con Azure Firewall, puede configurar:

* Reglas de aplicación que definen los nombres de dominio completos (FQDN) a los que se puede acceder desde una subred.
* Reglas de red que definen la dirección de origen, el protocolo, el puerto de destino y la dirección de destino.
* Reglas de traducción de direcciones de red (NAT) que definen los puertos y las direcciones IP de destino para traducir las solicitudes entrantes.

[Azure Application Gateway](https://azure.microsoft.com/services/application-gateway) también proporciona un firewall, denominado *firewall de aplicaciones web* (WAF). El firewall de aplicaciones web proporciona protección entrante centralizada para las aplicaciones web contra vulnerabilidades de seguridad comunes. [Azure Front Door](https://azure.microsoft.com/services/frontdoor/) y [Azure Content Delivery Network](https://azure.microsoft.com/services/cdn/) también proporcionan servicios de firewall de aplicaciones web.

**Protección contra ataques de DDoS mediante el uso de Azure DDoS Protection**

Completado100 XP

* 3 minutos

Cualquier compañía de gran tamaño puede ser objeto de un ataque de red a gran escala. Tailwind Traders no es una excepción. Los atacantes podrían inundar la red para crear una instrucción o simplemente por el desafío. A medida que se traslada a la nube, Tailwind Traders quiere comprender cómo Azure puede ayudarle a evitar los ataques de denegación de servicio distribuido (DDoS), entre otros.

En esta sección, obtendrá información sobre cómo Azure DDoS Protection (nivel de servicio Estándar) ayuda a proteger sus recursos de Azure frente a ataques DDoS. En primer lugar, vamos a definir qué es un ataque DDoS.

**¿Qué son los ataques DDoS?**

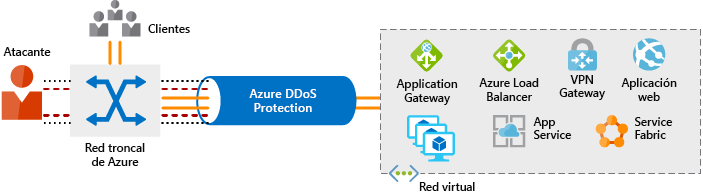
Un [ataque de denegación de servicio distribuido](https://azure.microsoft.com/services/ddos-protection) intenta sobrecargar y agotar los recursos de una aplicación, lo que provoca que sea lenta o no responda a los usuarios legítimos. Los ataques DDoS pueden estar dirigidos a cualquier recurso que sea accesible públicamente a través de Internet, incluidos los sitios web.

**¿Qué es Azure DDoS Protection?**

[Azure DDoS Protection](https://azure.microsoft.com/services/ddos-protection/) (Estándar) ayuda a proteger sus recursos de Azure frente a ataques DDoS.

Al combinar DDoS Protection con los procedimientos recomendados de diseño de aplicaciones, contribuye a la defensa frente a los ataques DDoS. DDoS Protection usa la escala y la elasticidad de la red global de Microsoft para incorporar capacidad de mitigación de DDoS a cada región de Azure. El servicio DDoS Protection ayuda a proteger las aplicaciones de Azure al analizar y descartar el tráfico de DDoS en la red perimetral de Azure antes de que afecte a la disponibilidad del servicio.

Este diagrama muestra el tráfico de red que llega a Azure de los clientes y un atacante:



La protección contra DDoS de Azure identifica el intento del atacante de sobrecargar la red y evita que llegue más tráfico de él, y asegura que el tráfico nunca llega a los servicios de Azure. El tráfico legítimo de los clientes sigue llegando a Azure sin ninguna interrupción del servicio.

DDoS Protection también puede ayudarle a administrar el consumo de la nube. Al ejecutar de forma local, tiene un número fijo de recursos de proceso. Pero, en la nube, la informática elástica significa que puede escalar horizontalmente la implementación de forma automática en función de la demanda. Un ataque de DDoS diseñado inteligentemente puede hacer que aumente la asignación de recursos, lo que provoca gastos innecesarios. DDoS Protection Estándar ayuda a garantizar que la carga de red que se procesa refleja el uso del cliente. También puede recibir crédito por los costos acumulados para los recursos escalados horizontalmente durante un ataque DDoS.

**¿Qué niveles de servicio están disponibles para DDoS Protection?**

DDoS Protection proporciona estos niveles de servicio:

* **Basic**

El nivel de servicio básico está habilitado de forma automática sin coste como parte de la suscripción de Azure.

La supervisión continua del tráfico y la mitigación en tiempo real de ataques de nivel de red comunes ofrecen la misma defensa que usan los servicios en línea de Microsoft. El nivel Básico garantiza que la infraestructura de Azure no se vea afectada durante un ataque DDoS a gran escala.

La red global de Azure se usa para distribuir y mitigar el tráfico de ataques entre regiones de Azure.

* **Estándar**

El nivel Estándar ofrece funcionalidades adicionales de mitigación adaptadas específicamente a los recursos de Azure Virtual Network. DDoS Protection Estándar es relativamente fácil de habilitar y no requiere ningún cambio en la aplicación.

El nivel Estándar proporciona supervisión del tráfico siempre activa y mitigación en tiempo real de los ataques a nivel de red más comunes. Proporciona las mismas defensas que los servicios en línea de Microsoft.

Las directivas de protección se ajustan a través de la supervisión del tráfico dedicado y los algoritmos de Machine Learning. Las directivas se aplican a direcciones IP públicas asociadas a recursos implementados en redes virtuales, como Azure Load Balancer y Application Gateway.

La red global de Azure se usa para distribuir y mitigar el tráfico de ataques entre regiones de Azure.

**¿Qué tipos de ataques ayuda a evitar DDoS Protection?**

El nivel Estándar puede ayudar a evitar:

* **Ataques volumétricos**

El objetivo de este ataque es desbordar la capa de red con una gran cantidad de tráfico aparentemente legítimo.

* **Ataques de protocolo**

Estos ataques vuelven un destino inaccesible al aprovechar una vulnerabilidad en la pila de protocolo de capa 3 y 4.

* **Ataques de nivel de recurso (nivel de aplicación) (solo con el firewall de aplicaciones web)**

Estos ataques van dirigidos a paquetes de aplicaciones web para interrumpir la transmisión de datos entre hosts. Necesita un firewall de aplicaciones web (WAF) para protegerse contra ataques de L7. DDoS Protection Estándar protege el firewall de aplicaciones web de los ataques de protocolo y volumétricos.

**Filtrado del tráfico de red mediante grupos de seguridad de red**

Completado100 XP

* 2 minutos

Aunque Azure Firewall y Azure DDoS Protection pueden ayudar a controlar el tráfico que puede provenir de orígenes externos, a Tailwind Traders también quiere saber cómo proteger sus redes internas en Azure. Esto le proporcionará una capa adicional de defensa contra los ataques.

En esta parte, se examinan los grupos de seguridad de red (NSG).

**¿Que son los grupos de seguridad de red?**

Un [grupo de seguridad de red](https://docs.microsoft.com/es-ES/azure/virtual-network/security-overview#network-security-groups?azure-portal=true) permite filtrar el tráfico de red desde y hacia los recursos de Azure en una red virtual de Azure. Puede considerar los grupos de seguridad de red como un firewall interno. Un NSG puede contener varias reglas de seguridad entrantes y salientes que permiten filtrar el tráfico con los recursos por dirección IP de origen y destino, puerto y protocolo.

**¿Cómo se especifican las reglas de NSG?**

Un grupo de seguridad de red puede contener tantas reglas como sea necesario, dentro de los límites de suscripción de Azure. Cada regla especifica las siguientes propiedades:

| **Propiedad** | **Descripción** |
| --- | --- |
| Nombre | Nombre único para el grupo de seguridad de red. |
| Priority | Un número entre 100 y 4096. Las reglas se procesan en orden de prioridad, donde los números más bajos se procesan antes que los números más altos. |
| Origen o destino | Una dirección IP o intervalo de direcciones IP, una etiqueta de servicio o un grupo de seguridad de aplicaciones únicos. |
| Protocolo | **TCP**, **UDP** o **cualquiera**. |
| Dirección | Si la regla se aplica al tráfico entrante o al saliente. |
| Intervalo de puertos | Un único puerto o un intervalo de puertos. |
| Acción | **Permitir** o **Denegar**. |

Cuando se crea un grupo de seguridad de red, Azure crea una serie de reglas predeterminadas para proporcionar un nivel de línea de base de seguridad. No puede quitar las reglas predeterminadas, pero puede invalidarlas si crea otras con prioridades más altas.

**Ejercicio: configuración del acceso de red a una máquina virtual mediante un grupo de seguridad de red**

Completado100 XP

* 10 minutos

Este módulo requiere un espacio aislado para completarse.

Un [**espacio aislado**](https://docs.microsoft.com/en-us/learn/support/faq?pivots=sandbox) le da acceso a recursos gratuitos. No se le cobrará en su suscripción personal. El espacio aislado solo podrá usarse para completar el aprendizaje en Microsoft Learn. El uso para cualquier otro motivo está prohibido y podría generar la pérdida permanente del acceso al espacio aislado.

Microsoft ofrece esta experiencia de laboratorio y el contenido relacionado con fines educativos. Toda la información presentada es propiedad de Microsoft y está destinada únicamente a brindar información sobre los productos y servicios abordados en este módulo de Microsoft Learn.

Activar espacio aislado

En este ejercicio, configurará el acceso de red a una máquina virtual (VM) que se ejecuta en Azure.

Para empezar, creará una máquina virtual Linux e instalará Nginx, un conocido servidor web, en esa máquina virtual. Para que el servidor web sea accesible, cree una regla de grupo de seguridad de red (NSG) que permita el acceso entrante en el puerto 80 (HTTP).

Hay muchas formas de crear y administrar máquinas virtuales, incluida su configuración de red. Por ejemplo, puede usar la Azure Portal, la CLI de Azure, Azure PowerShell o una plantilla de Azure Resource Manager (ARM).

Aquí, usará la CLI de Azure. La CLI de Azure le permite conectarse a Azure y ejecutar comandos administrativos en recursos de Azure. Al igual que con otras interfaces de la línea de comandos, puede ejecutar los comandos directamente desde un terminal o puede agregar comandos a un script de Bash o a un script de PowerShell. El CLI de Azure se ejecuta en Windows, macOS o Linux.

Aquí, accede a la CLI de Azure desde Azure Cloud Shell. Cloud Shell es una experiencia de shell basado en el explorador que usa para administrar y desarrollar recursos de Azure. Piense en Cloud Shell como una consola interactiva que se ejecuta en la nube.

Si no está familiarizado con la CLI de Azure o con Cloud Shell, siga adelante.

**Creación de una máquina virtual Linux e instalación de Nginx**

Use los comandos siguientes de la CLI de Azure para crear una máquina virtual Linux e instalar Nginx. Una vez creada la máquina virtual, usará la extensión de script personalizado para instalar Nginx. La extensión de script personalizado es una manera fácil de descargar y ejecutar scripts en máquinas virtuales de Azure. Es solo una de las numerosas formas de configurar el sistema después de que la máquina virtual esté en funcionamiento.

1. Desde Cloud Shell, ejecute el siguiente comando az vm create para crear una máquina virtual Linux:

CLI de AzureCopiar

az vm create \

--resource-group [sandbox resource group name] \

--name my-vm \

--image UbuntuLTS \

--admin-username azureuser \

--generate-ssh-keys

La máquina virtual tardará unos minutos en aparecer.

Asigne el nombre **my-vm** a la máquina virtual. Use este nombre para hacer referencia a la máquina virtual en los pasos posteriores.

1. Ejecute el siguiente comando az vm extension set para configurar Nginx en la máquina virtual:

CLI de AzureCopiar

az vm extension set \

--resource-group [sandbox resource group name] \

--vm-name my-vm \

--name customScript \

--publisher Microsoft.Azure.Extensions \

--version 2.1 \

--settings '{"fileUris":["https://raw.githubusercontent.com/MicrosoftDocs/mslearn-welcome-to-azure/master/configure-nginx.sh"]}' \

--protected-settings '{"commandToExecute": "./configure-nginx.sh"}'

Este comando usa la extensión de script personalizado para ejecutar un script de Bash en la máquina virtual. El script se almacena en GitHub.

Mientras se ejecuta el comando, puede optar por [examinar el script de Bash](https://raw.githubusercontent.com/MicrosoftDocs/mslearn-welcome-to-azure/master/configure-nginx.sh) en una pestaña independiente del explorador.

En resumen, el script hace lo siguiente:

* 1. Ejecuta apt-get update para descargar la información más reciente del paquete desde Internet. Este paso ayuda a garantizar que el siguiente comando pueda encontrar la versión más reciente del paquete Nginx.
  2. Instala Nginx.
  3. Establece la página principal, */var/www/html/index.html*, para que imprima un mensaje de bienvenida en el que se incluye el nombre de host de la máquina virtual.

**Acceso al servidor web**

En este procedimiento se obtiene la dirección IP de la máquina virtual y se intenta acceder a la página principal del servidor web.

1. Ejecute el siguiente comando az vm list-ip-addresses para obtener la dirección IP de la máquina virtual y almacenar el resultado como una variable de Bash:

CLI de AzureCopiar

IPADDRESS="$(az vm list-ip-addresses \

--resource-group [sandbox resource group name] \

--name my-vm \

--query "[].virtualMachine.network.publicIpAddresses[\*].ipAddress" \

--output tsv)"

1. Ejecute el siguiente comando curl para descargar la página principal:

BashCopiar

curl --connect-timeout 5 http://$IPADDRESS

El argumento --connect-timeout especifica que se conceden hasta cinco segundos para que se produzca la conexión.

Después de cinco segundos, verá un mensaje de error que indica que se ha agotado el tiempo de espera de la conexión:

ResultadoCopiar

curl: (28) Connection timed out after 5001 milliseconds

Este mensaje significa que no se pudo acceder a la máquina virtual dentro del tiempo de espera.

1. Como paso opcional, intente acceder al servidor web desde un explorador:
   1. Ejecute lo siguiente para imprimir la dirección IP de la máquina virtual en la consola:

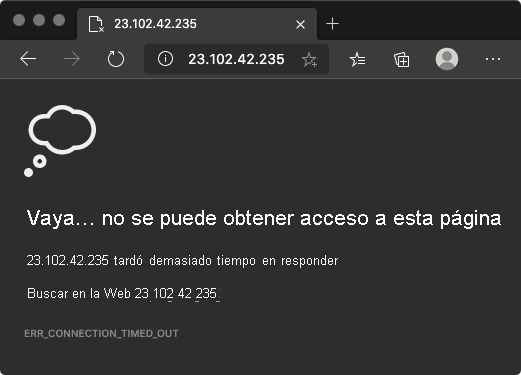
BashCopiar

echo $IPADDRESS

Verá una dirección IP, por ejemplo, *23.102.42.235*.

* 1. Copie en el portapapeles la dirección IP que vea.
  2. Abra una pestaña nueva del explorador y vaya al servidor web.

Transcurridos unos instantes, verá que la conexión no se está produciendo. Si espera a que se agote el tiempo de espera del explorador, verá algo parecido a esto:



Mantenga esta pestaña del explorador abierta para usarla más tarde.

**Enumeración de las reglas del grupo de seguridad de red actuales**

No se pudo acceder al servidor web. Para averiguar el motivo, vamos a examinar las reglas actuales del grupo de seguridad de red.

1. Ejecute el siguiente comando az network nsg list para que muestre los grupos de seguridad de red asociados a la máquina virtual:

CLI de AzureCopiar

az network nsg list \

--resource-group [sandbox resource group name] \

--query '[].name' \

--output tsv

Verá lo siguiente:

ResultadoCopiar

my-vmNSG

Cada máquina virtual de Azure está asociada a, al menos, un grupo de seguridad de red. En este caso, Azure le creó un grupo de seguridad de red denominado*my-vmNSG*.

1. Ejecute el siguiente comando az network nsg rule list para mostrar las reglas asociadas al grupo de seguridad de red denominado *my-vmNSG*:

CLI de AzureCopiar

az network nsg rule list \

--resource-group [sandbox resource group name] \

--nsg-name my-vmNSG

Verá un bloque grande de texto en formato JSON en la salida. En el paso siguiente, ejecutará un comando similar que facilita la lectura de este resultado.

1. Ejecute por segunda vez el comando az network nsg rule list.

Esta vez, use el argumento --query para recuperar solo el nombre, la prioridad, los puertos afectados y el acceso (**Permitir** o **Denegar**) para cada regla.

El argumento --output da formato a la salida como una tabla para que sea fácil de leer.

CLI de AzureCopiar

az network nsg rule list \

--resource-group [sandbox resource group name] \

--nsg-name my-vmNSG \

--query '[].{Name:name, Priority:priority, Port:destinationPortRange, Access:access}' \

--output table

Verá lo siguiente:

ResultadoCopiar

Name Priority Port Access

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

default-allow-ssh 1000 22 Allow

Verá la regla predeterminada *default-allow-ssh*. Esta regla permite conexiones entrantes a través del puerto 22 (SSH). SSH (Secure Shell) es un protocolo que se usa en Linux para permitir que los administradores accedan al sistema de forma remota.

La prioridad de esta entrada es 1000. Las reglas se procesan en orden de prioridad, donde los números más bajos se procesan antes que los números más altos.

De forma predeterminada, un grupo de seguridad de red de una máquina virtual de una máquina virtual Linux solo permite el acceso a la red en el puerto 22. Esto permite que los administradores accedan al sistema. También debe permitir las conexiones entrantes en el puerto 80, que permite el acceso a través de HTTP.

**Creación de la regla de seguridad de red**

En este caso, creará una regla de seguridad de red que permita el acceso de entrada en el puerto 80 (HTTP).

1. Ejecute el siguiente comando az network nsg rule create para crear una regla denominada *allow-http* que permita el acceso entrante en el puerto 80:

CLI de AzureCopiar

az network nsg rule create \

--resource-group [sandbox resource group name] \

--nsg-name my-vmNSG \

--name allow-http \

--protocol tcp \

--priority 100 \

--destination-port-ranges 80 \

--access Allow

Con fines de aprendizaje, aquí establecerá la prioridad en 100. En este caso, la prioridad no importa. Tendrá que tener en cuenta la prioridad si tuviera intervalos de puertos superpuestos.

1. Para comprobar la configuración, ejecute az network nsg rule list para ver la lista actualizada de reglas:

CLI de AzureCopiar

az network nsg rule list \

--resource-group [sandbox resource group name] \

--nsg-name my-vmNSG \

--query '[].{Name:name, Priority:priority, Port:destinationPortRange, Access:access}' \

--output table

Verá las dos reglas, *default-allow-ssh* y la nueva regla *allow-http*:

ResultadoCopiar

Name Priority Port Access

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

default-allow-ssh 1000 22 Allow

allow-http 100 80 Allow

**Volver a acceder al servidor web**

Ahora que ha configurado el acceso de red al puerto 80, vamos a intentar acceder al servidor web una segunda vez.

1. Ejecute el mismo comando curl que ha ejecutado antes:

BashCopiar

curl --connect-timeout 5 http://$IPADDRESS

Verá lo siguiente:

HTMLCopiar

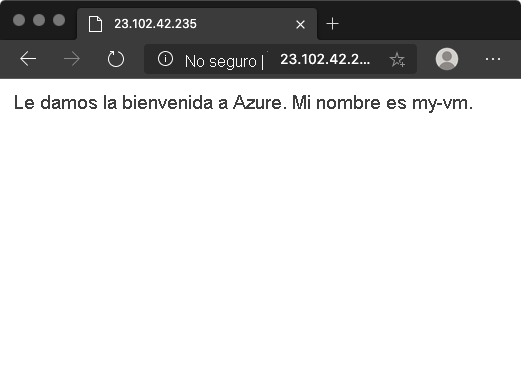
<html><body><h2>Welcome to Azure! My name is my-vm.</h2></body></html>

**Nota**

Puede haber un ligero retraso entre la adición de las reglas y la apertura de los puertos.

1. Como paso opcional, actualice la pestaña del explorador que apunta al servidor web.

Verá lo siguiente:



**Limpieza**

El espacio aislado limpia los recursos automáticamente cuando haya terminado con este módulo.

Al trabajar en una suscripción propia, se recomienda identificar al final de un proyecto si aún necesita los recursos creados. Los recursos que deja en ejecución pueden costar dinero. Puede eliminar los recursos de forma individual o eliminar el grupo de recursos para eliminar todo el conjunto de recursos.

Buen trabajo. En la práctica, puede crear un grupo de seguridad de red independiente que incluya las reglas de acceso de red entrantes y salientes que necesite. Si tiene varias máquinas virtuales que tienen el mismo propósito, puede asignar ese grupo de seguridad de red a cada máquina virtual en el momento de crearla. Esta técnica permite controlar el acceso de red a varias máquinas virtuales en un único conjunto central de reglas.

**Combinación de servicios de Azure para crear una solución de seguridad de red completa**

Completado100 XP

* 3 minutos

Al considerar una solución de seguridad de Azure, tenga en cuenta todos los elementos de la defensa en profundidad.

Estas son algunas recomendaciones sobre cómo combinar los servicios de Azure para crear una solución de seguridad de red completa.

**Protección de la capa perimetral**

La capa perimetral trata sobre la protección de los recursos de su organización frente a ataques basados en red. Identificar estos ataques, alertar a los equipos de seguridad adecuados y eliminar su impacto es importante para proteger la red. Para ello, siga estos pasos:

* Use Azure DDoS Protection para filtrar los ataques a gran escala antes de que puedan causar una denegación de servicio para los usuarios.
* Use firewalls perimetrales con Azure Firewall para identificar los ataques malintencionados contra la red y alertar sobre ellos.

**Protección de la capa de red**

En esta capa, el enfoque está en limitar la conectividad de la red en todos los recursos para permitir solo la necesaria. Segmente los recursos y use controles de nivel de red para restringir la comunicación a lo imprescindible.

Al restringir esta conectividad, se reduce el riesgo de desplazamiento lateral en la red ante un ataque. Use los grupos de seguridad de red para crear reglas que definan qué comunicación entrante y saliente se permite en esta capa. Estos son algunos procedimientos recomendados:

* Limite la comunicación entre los recursos mediante la segmentación de la red y la configuración de controles de acceso.
* Deniegue de forma predeterminada.
* Restrinja el acceso entrante de Internet y limite el saliente cuando sea apropiado.
* Implemente conectividad segura a las redes locales.

**Combinación de servicios**

También puede combinar los servicios de redes y seguridad de Azure para administrar la seguridad de red y proporcionar mayor protección por capas. Estas son dos formas de combinar los servicios:

* **Grupos de seguridad de red y Azure Firewall**

Azure Firewall complementa la funcionalidad de los grupos de seguridad de red. Juntos, proporcionan una mejor seguridad de la red de defensa en profundidad.

Los grupos de seguridad de red proporcionan filtrado de tráfico distribuido a nivel de red para limitar el tráfico a los recursos dentro de las redes virtuales de cada suscripción.

Azure Firewall es un firewall de red como servicio centralizado y con estado completo. Proporciona protección de nivel de red y de aplicación en diferentes suscripciones y redes virtuales.

* **Firewall de aplicaciones web de Azure Application Gateway y Azure Firewall**

El firewall de aplicaciones web (WAF) es una característica de Azure Application Gateway que proporciona a las aplicaciones web una protección entrante centralizada contra vulnerabilidades de seguridad comunes.

Azure Firewall proporciona lo siguiente:

* + Protección entrante para protocolos que no son HTTP/S (por ejemplo, RDP, SSH y FTP).
  + Protección de nivel de red de salida para todos los puertos y protocolos.
  + Protección de nivel de aplicación para HTTP/S saliente.

La combinación de todos ellos proporciona más niveles de protección.