Descripción de la protección contra DDoS de Azure

Cualquier empresa, grande o pequeña, puede ser objeto de un grave ataque de red. La naturaleza de estos ataques podría ser para mostrar una postura o simplemente porque el atacante se había puesto un desafío.

Ataques de denegación de servicio distribuido

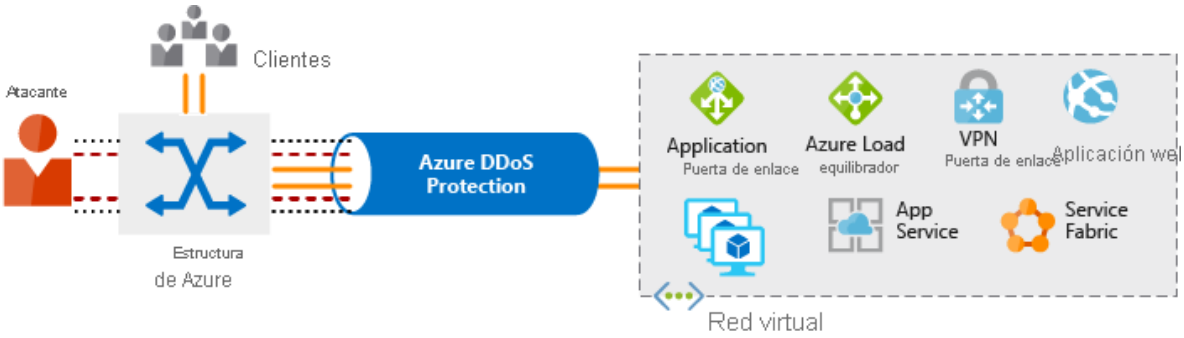
El objetivo de un ataque de denegación de servicio distribuido (DDoS) es sobrecargar los recursos en las aplicaciones y servidores, lo que les deja sin responder o ralentiza a los usuarios auténticos. Un ataque DDoS normalmente se dirige a cualquier dispositivo de acceso público al que se pueda acceder a través de Internet.

Los tres tipos más frecuentes de ataque DDoS son:

- **Ataques volumétricos**: Se tratan de ataques basados en volúmenes que inundan la red con tráfico aparentemente legítimo, sobrepasando el ancho de banda disponible. El tráfico legítimo no logra comunicarse. Estos tipos de ataques se miden en bits por segundo.
- **Ataques de protocolo**: Los ataques de protocolo representan un destino inaccesible al agotar los recursos del servidor con solicitudes de protocolo falsas que aprovechan los puntos débiles de los protocolos de nivel 3 (red) y nivel 4 (transporte). Estos tipos de ataques se miden normalmente en paquetes por segundo.
- **Ataques de nivel de recurso (aplicación)** : estos ataques van dirigidos a paquetes de aplicaciones web y su objetivo es interrumpir la transmisión de datos entre hosts.

¿Qué es Azure DDoS Protection?

El servicio Azure DDoS Protection está diseñado para ayudar a proteger sus aplicaciones y servidores mediante el análisis del tráfico de red y el descarte de todo lo que parezca un ataque DDoS.



En el diagrama anterior, Azure DDoS Protection identifica el intento de un atacante de sobrecargar la red. Bloquea el tráfico del atacante, asegurándose de que no llegue a los recursos de Azure. El tráfico legítimo de los clientes sigue llegando a Azure sin ninguna interrupción del servicio.

Azure 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. Durante un ataque DDoS, Azure puede

escalar las necesidades informáticas para satisfacer la demanda. Para administra el consumo de la nube, DDoS Protection se asegura de que la carga de red solo refleje el uso real de los clientes.

Azure DDoS Protection se incluye en dos niveles:

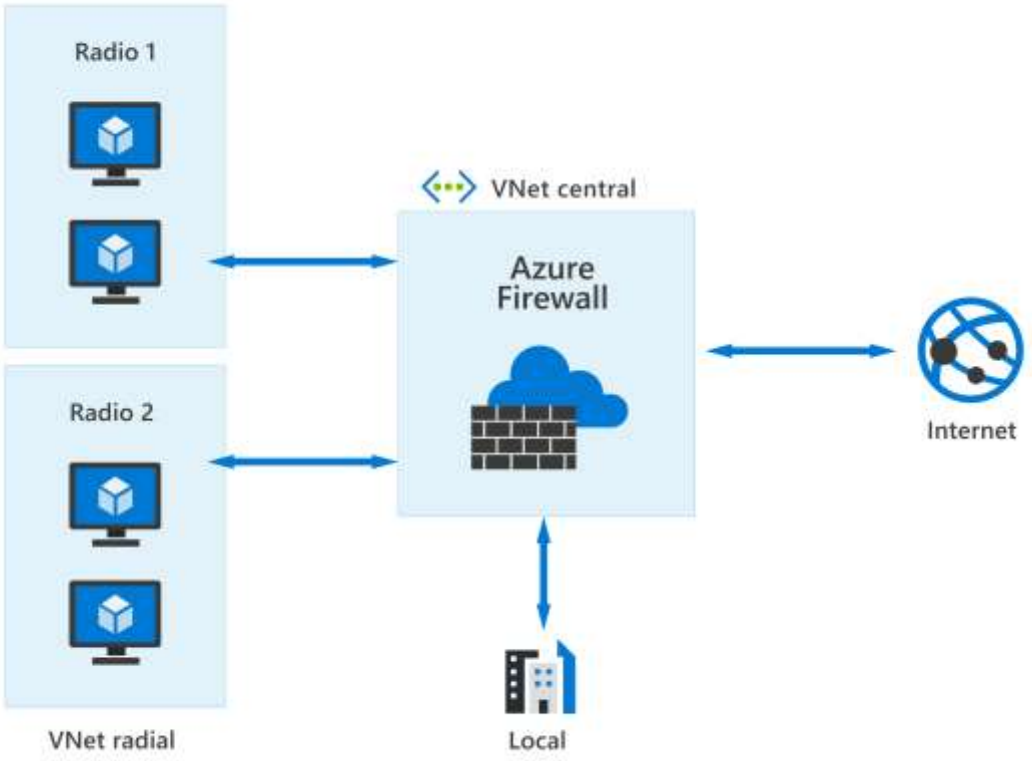
- **Básico**: El nivel de servicio Básico está habilitado automáticamente para cada propiedad de Azure, sin costo adicional, como parte de la plataforma Azure. La supervisión continua de tráfico y la mitigación en tiempo real de ataques de nivel de red comunes ofrecen la misma defensa que usan los servicios en línea de Microsoft. La red global de Azure se usa para distribuir y mitigar el tráfico de ataques en las distintas regiones.
- **Estándar**: Este nivel de servicio Estándar ofrece funcionalidades adicionales de mitigación adaptadas específicamente a los recursos de Microsoft Azure Virtual Network. DDoS Protection Estándar es fácil de habilitar y no requiere ningún cambio en la aplicación. Las directivas de protección se ajustan mediante algoritmos dedicados de supervisión del tráfico y aprendizaje automático. Las directivas se aplican a direcciones IP públicas asociadas a recursos implementados en redes virtuales, como Azure Load Balancer y Application Gateway.

El servicio Estándar de DDoS Protection tiene un cargo mensual fijo que incluye protección para 100 recursos. La protección de recursos adicionales se cobra mensualmente por cada recurso.

Use Azure DDoS para proteger los dispositivos y las aplicaciones mediante el análisis del tráfico a través de la red, y la adopción de acciones adecuadas relativas al tráfico sospechoso.

Descripción de Azure Firewall

Azure Firewall es un servicio de seguridad de red administrado y basado en la nube que protege los recursos de redes virtuales (VNet) de Azure frente a los atacantes. Puede implementar Azure Firewall en cualquier red virtual, pero el mejor enfoque es usarlo en una red virtual centralizada. Todas las demás redes virtuales y locales se enrutarán a través de ella. La ventaja de este modelo es la capacidad de ejercer de forma centralizada el control del tráfico de red para todas las redes virtuales en diferentes suscripciones.



Con Azure Firewall puede escalar el uso verticalmente para acoger los flujos de tráfico de red cambiantes, por lo que no es necesario elaborar un presupuesto para los picos de tráfico. El tráfico de red está sujeto a las reglas de firewall configuradas cuando se enruta al firewall, como la puerta de enlace predeterminada de la subred.

Características clave de Azure Firewall

Azure Firewall incluye muchas características, incluidas, entre otras:

- **Alta disponibilidad y zonas de disponibilidad integradas**: La alta disponibilidad está integrada, por lo que no hay nada que configurar. Además, Azure Firewall se puede configurar para abarcar varias zonas de disponibilidad y aumentar la disponibilidad.
- **Filtrado a nivel de aplicación y de red**: Use la dirección IP, el puerto y el protocolo para admitir el filtrado de nombres de dominio completo para el tráfico HTTP(s) saliente y los controles de filtrado de red.
- **SNAT de salida y DNAT de entrada para comunicación con recursos de Internet**: traduce la dirección IP privada de los recursos de red a una dirección IP pública de Azure (traducción de direcciones de red de origen, SNAT) para identificar y permitir el tráfico procedente de la red virtual a destinos de Internet. Del mismo modo, el tráfico entrante de Internet a la dirección IP pública del firewall se traduce (traducción de direcciones de

red de destino o DNAT) y se filtra a las direcciones IP privadas de los recursos de la red virtual.

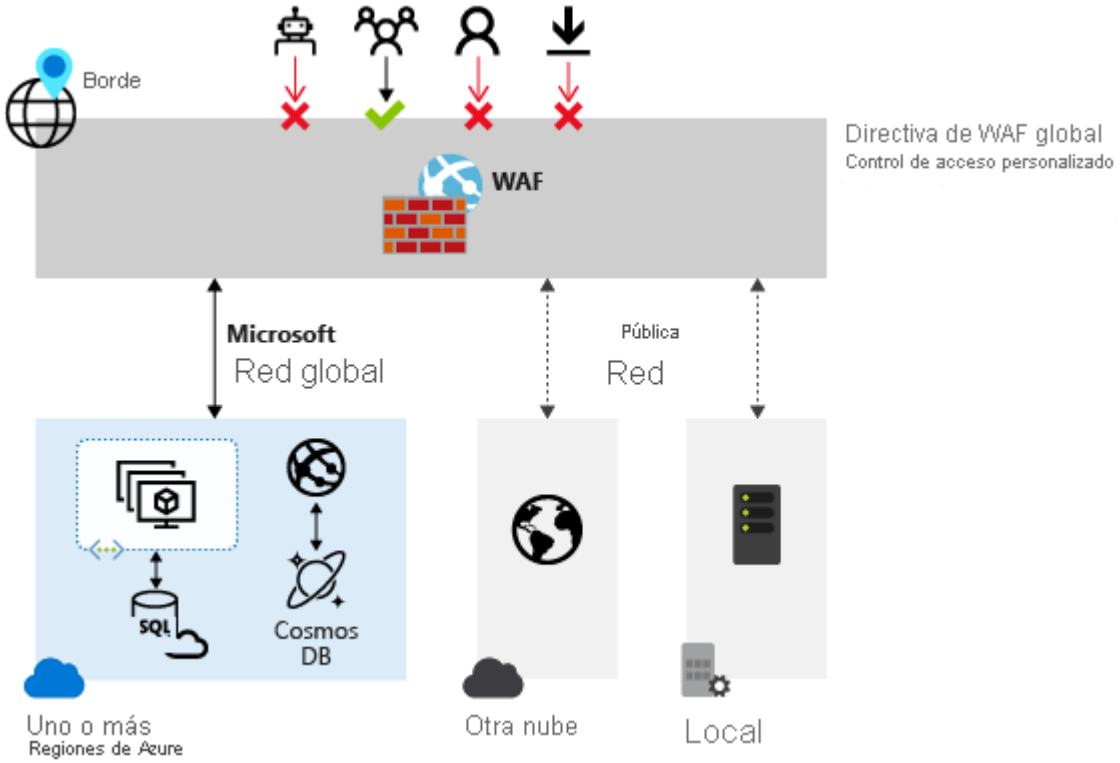
- **Varias direcciones IP públicas**: Estas direcciones se pueden asociar a Azure Firewall.
- **Inteligencia sobre amenazas**: El filtrado basado en inteligencia sobre amenazas puede habilitarse para que el firewall alerte y deniegue el tráfico desde y hacia los dominios y las direcciones IP malintencionados conocidos.
- **Integración en Azure Monitor**: Se integra en Azure Monitor para habilitar la recopilación, el análisis y la acción en función de la telemetría de los registros de Azure Firewall.

Use Azure Firewall para ayudar a proteger los recursos de Azure que ha conectado a las redes virtuales de Azure.

Descripción de Web Application Firewall

Las aplicaciones web son cada vez más el objetivo de ataques malintencionados que aprovechan vulnerabilidades habitualmente conocidas. Evitar dichos ataques en el código de la aplicación es todo un desafío. Puede requerir un mantenimiento riguroso, revisión y supervisión.

El firewall de aplicaciones web (WAF) ofrece una protección centralizada de las aplicaciones web contra las vulnerabilidades de seguridad más habituales. Un WAF centralizado ayuda a simplificar la administración de la seguridad, mejora el tiempo de respuesta ante una amenaza de seguridad y permite aplicar revisiones a una vulnerabilidad conocida en un lugar, en lugar de proteger cada aplicación web individual. Un WAF también proporciona a los administradores de la aplicación a un mejor control de la protección contra amenazas e intrusiones.



Descripción de la segmentación de red en Azure

La segmentación consiste en dividir algo en partes más pequeñas. Una organización, por ejemplo, suele estar formada por grupos empresariales más pequeños, como recursos humanos, ventas, atención al cliente, etc. En una oficina, es habitual que cada grupo empresarial tenga su propio espacio de oficina, mientras que los miembros del mismo grupo comparten una oficina. Esto permite que los miembros de un mismo grupo empresarial colaboren, al tiempo que se mantiene la separación de otros grupos para atender los requisitos de confidencialidad de cada empresa.

El mismo concepto se aplica a las redes informáticas de las empresas. Estas son las principales razones de la segmentación:

- La capacidad de agrupar recursos relacionados que forman parte de las operaciones de la carga de trabajo (o que la hacen posible).
- Aislamiento de recursos.
- Directivas de gobernanza establecidas por la organización.

La segmentación de la red también es compatible con el modelo de Confianza cero y con un enfoque de seguridad por capas que forma parte de una estrategia de defensa en profundidad.

Asumir la vulneración es un principio del modelo de Confianza Cero, por lo que la capacidad de contener a un atacante es vital para proteger los sistemas de información. Cuando las cargas de trabajo (o partes de una carga de trabajo determinada) se colocan en segmentos separados, se puede controlar el tráfico desde y hacia esos segmentos para asegurar las vías de comunicación. Si un segmento se ve comprometido, podrá contener mejor el impacto y evitar que se extienda lateralmente por el resto de su red.

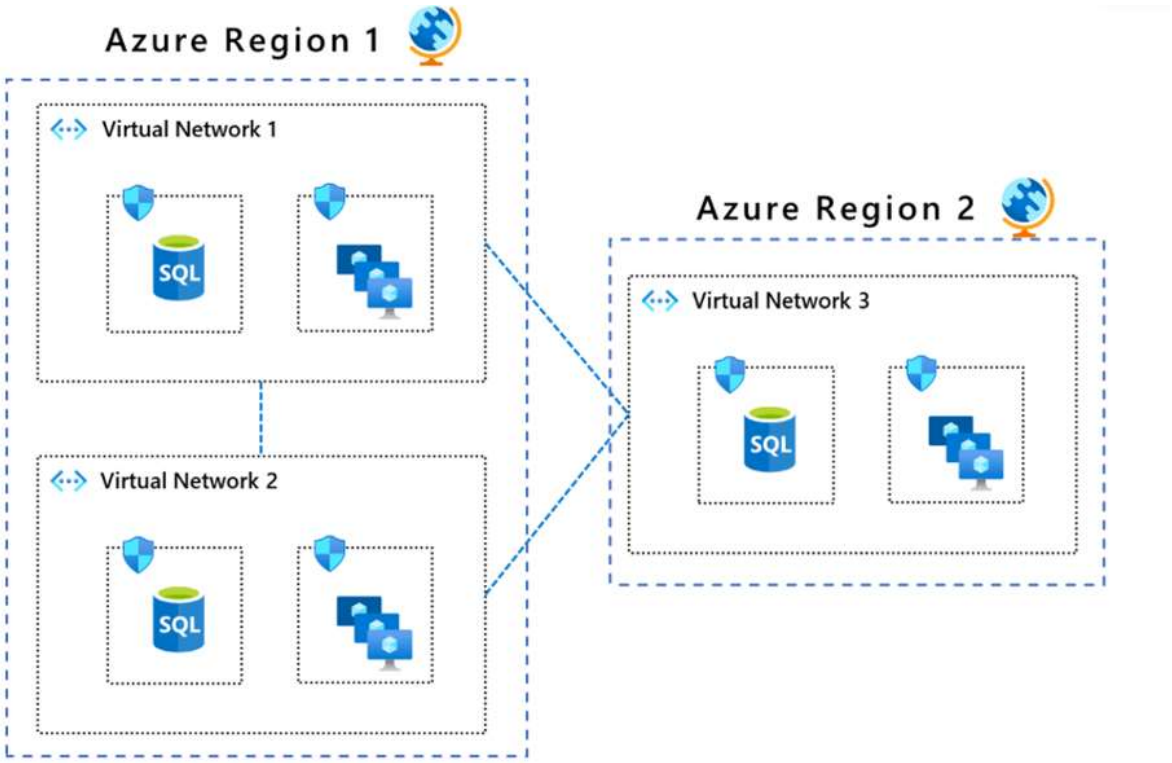
La segmentación de la red puede asegurar las interacciones entre los perímetros. Este enfoque puede reforzar la postura de seguridad de una organización, contener los riesgos en caso de infracción y evitar que los atacantes accedan a toda la carga de trabajo.

Azure Virtual Network

Azure Virtual Network (VNet) es la pieza clave para la red privada de su organización en Azure. VNet es similar a una red tradicional que funcionaría en su propio centro de datos, pero aporta las ventajas adicionales de la infraestructura de Azure, como la escala, la disponibilidad y el aislamiento.

Azure VNet permite a las organizaciones segmentar su red. Las organizaciones pueden crear varias VNets por región y por suscripción, y se pueden crear varias redes más pequeñas (subredes) dentro de cada VNet.

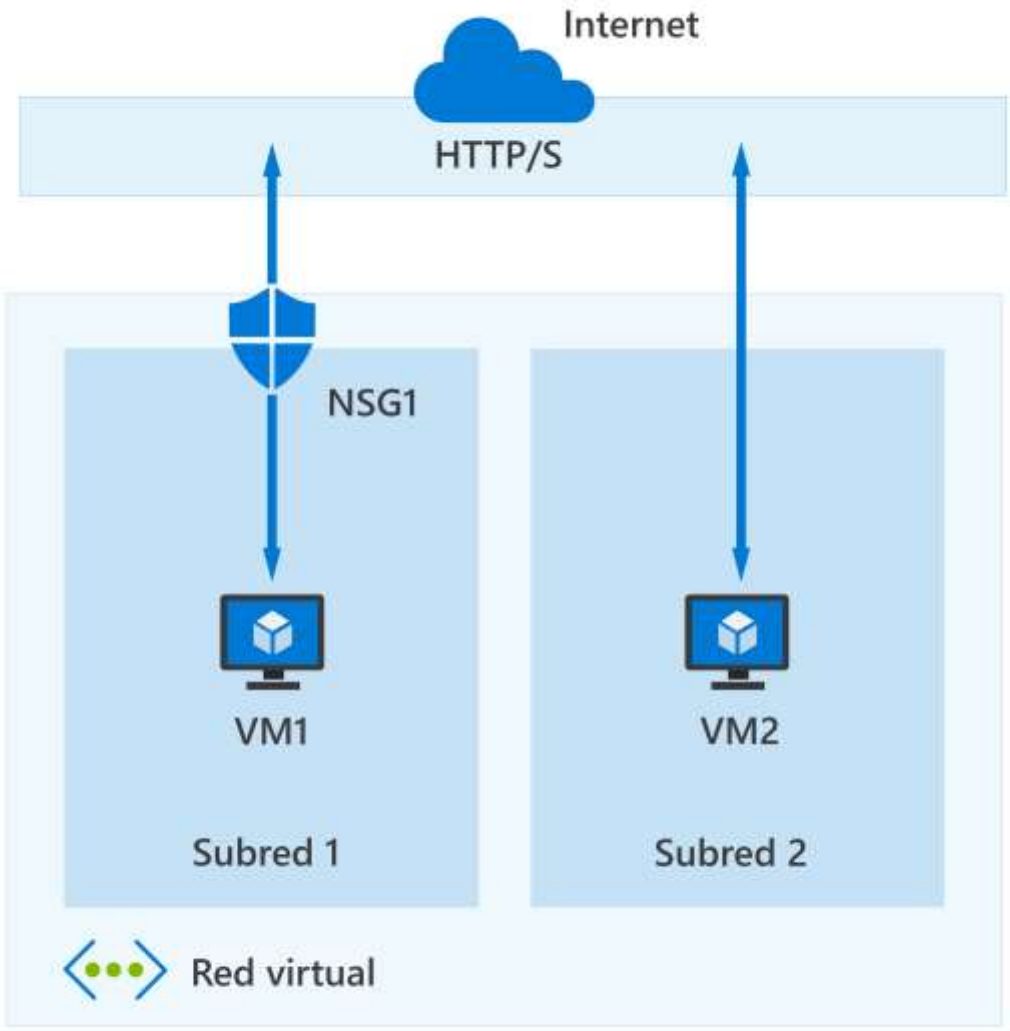
Las VNets proporcionan una contención a nivel de red de los recursos sin que se permita el tráfico a través de las VNets o de entrada a la VNet, de forma predeterminada. La comunicación tiene que ser aprovisionada de forma explícita. Esto permite un mayor control sobre la forma en que los recursos de Azure en una VNet se comunican con otros recursos de Azure, Internet y las redes locales.



Descripción de los grupos de seguridad de red de Azure

Los grupos de seguridad de red (NSG) permiten filtrar el tráfico de red hacia y desde los recursos de Azure en una red virtual de Azure; por ejemplo, una máquina virtual. Un NSG consta de reglas que definen cómo se filtra el tráfico. Solo puede asociar un grupo de seguridad de red a cada subred e interfaz de red de la red virtual en una máquina virtual. Sin embargo, el mismo grupo de seguridad de red se puede asociar a tantas subredes e interfaces de red distintas como elija.

En el diagrama muy simplificado que se muestra a continuación, puede ver una red virtual de Azure con dos subredes que están conectadas a Internet, y cada subred tiene una máquina virtual. La subred 1 tiene un NSG asignado que filtra el acceso entrante y saliente a VM1, que necesita un mayor nivel de acceso. En cambio, VM2 podría representar una máquina de acceso público que no requiere un NSG.



Reglas de seguridad de entrada y salida

Un NSG se compone de reglas de seguridad de entrada y salida. Las reglas de seguridad del NSG se evalúan por prioridad con cinco elementos de información: origen, puerto de origen, destino, puerto de destino y protocolo, para permitir o denegar el tráfico. De manera predeterminada, Azure crea una serie de reglas, tres reglas de entrada y tres de salida, 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.

Cada regla especifica una o varias de las siguientes propiedades:

- **Nombre**: Cada regla de NSG debe tener un nombre único que describa su propósito. Por ejemplo, FiltroSoloAccesoAdmin.
- **Prioridad**: las reglas se procesan en orden de prioridad, donde los números más bajos se procesan antes que los números más altos. Cuando el tráfico coincide con una regla, el

procesamiento se detiene. Esto significa que no se procesarán otras reglas con una prioridad más baja (números mayores).

- **Origen o destino**: especifique una dirección IP individual o un intervalo de direcciones IP, una etiqueta de servicio (un grupo de prefijos de dirección IP de un servicio de Azure determinado) o un grupo de seguridad de aplicaciones. La especificación de un intervalo, una etiqueta de servicio o grupo de seguridad de aplicaciones le permite crear menos reglas de seguridad.
- **Protocolo**: Qué protocolo de red comprobará la regla. El protocolo puede ser cualquiera de los siguientes: TCP, UDP, ICMP o Any.
- **Dirección**: Indica si la regla debe aplicarse al tráfico entrante o saliente.
- **Intervalo de puertos**: Puede especificar un puerto individual o un intervalo de puertos. La especificación de intervalos permite ser más eficaz al crear reglas de seguridad.
- **Acción**: Por último, debe decidir qué ocurrirá cuando se desencadene esta regla.

Por ejemplo, en la tabla siguiente se muestran las reglas de entrada predeterminadas, que se incluyen en todos los grupos de seguridad de red. En este ejemplo, suponga que no se ha definido ninguna otra regla de entrada para este grupo de seguridad de red.

Nombre	**Prioridad**	**Source**	**Puertos de origen**	**Destination**	**Puertos de destino**	**Protocolo**	**Acceso**
AllowVNetInBound	65000	VirtualNetwork	0-65535	VirtualNetwork	0-65535	Any	Allow
AllowAzureLoadBalancerInBound	65001	AzureLoadBalancer	0-65535	0.0.0.0/0	0-65535	Any	Allow
DenyAllInBound	65500	0.0.0.0/0	0-65535	0.0.0.0/0	0-65535	Any	Denegar

- La regla AllowVNetInBound se procesa primero, ya que tiene el valor de prioridad más bajo. Recuerde que las reglas con el valor de prioridad más bajo se procesan primero. Esta regla permite el tráfico desde cualquier Virtual Network (según lo definido por la etiqueta de servicio VirtualNework) de cualquier puerto a cualquier Virtual Network de cualquier puerto, mediante cualquier protocolo. Si se encuentra una coincidencia para esta regla, no se procesarán otras reglas. Si no se encuentra ninguna coincidencia, se procesa la siguiente regla.
- La regla AllowAzureLoadBalancerInBound se procesa en segundo lugar, ya que su valor de prioridad es mayor que la regla AllowVNetInBound. Esta regla permite el tráfico desde cualquier Azure Load Balancer (según lo definido por la etiqueta de servicio AzureLoadBalancer) de cualquier puerto a cualquier dirección IP de cualquier puerto, mediante cualquier protocolo. Si se encuentra una coincidencia para esta regla, no se

procesarán otras reglas. Si no se encuentra ninguna coincidencia, se procesa la siguiente regla.

- La última regla de este grupo de seguridad de red es la regla DenyAllInBound. Esta regla deniega todo el tráfico desde cualquier dirección IP de origen en cualquier puerto a cualquier otra dirección IP en cualquier puerto, mediante cualquier protocolo.

En resumen, cualquier subred de red virtual o tarjeta de interfaz de red a la que se asigne este grupo de seguridad de red solo permitirá el tráfico entrante desde una instancia de Azure Virtual Network o de Azure Load Balancer. Se deniega todo el tráfico de red de entrada restante. Aunque no se muestra en este ejemplo, también hay tres reglas de salida predeterminadas que se incluyen en todos los grupos de seguridad de red. No puede quitar las reglas predeterminadas, pero puede reemplazarlas si crea otras con prioridades más altas (valores de prioridad más bajos).

¿Cuál es la diferencia entre los grupos de seguridad de red (NSG) y Azure Firewall?

Ahora que ha obtenido información sobre los grupos de seguridad de red y Azure Firewall, es posible que se pregunte en qué difieren, ya que ambos protegen los recursos de red virtual. El servicio Azure Firewall complementa la funcionalidad de grupo de seguridad de red. Juntos proporcionan una mejor seguridad de red de "defensa en profundidad". Los grupos de seguridad de red proporcionan filtrado de tráfico distribuido de 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 con estado y centralizado, que proporciona protección de nivel de red y de aplicación ***entre*** las diferentes suscripciones y redes virtuales.

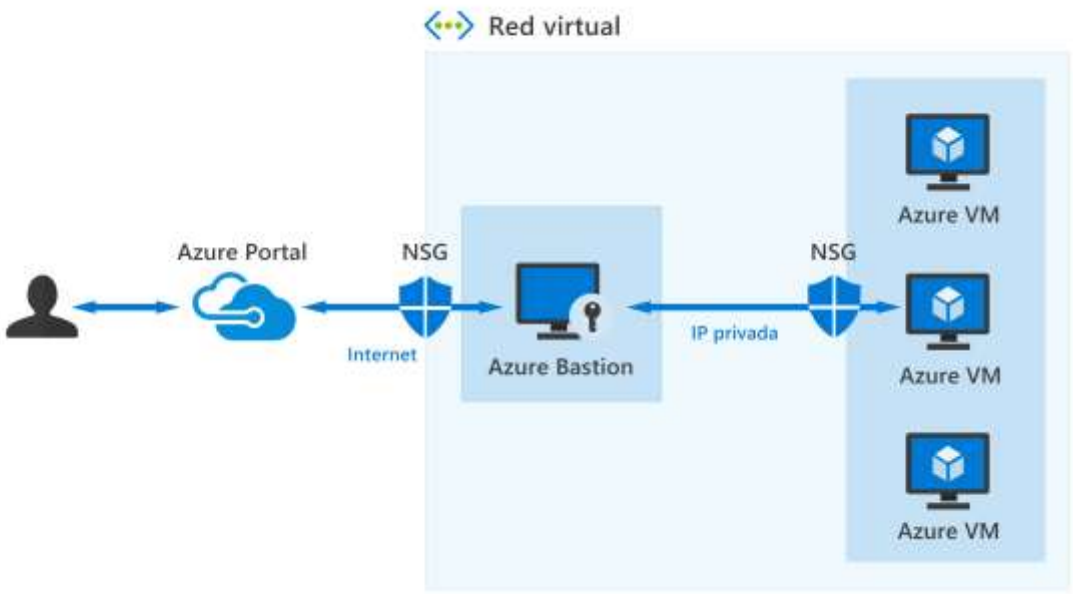
Descripción del acceso JIT y Azure Bastion

Supongamos que ha configurado varias redes virtuales que usan una combinación de NSG e instancias de Azure Firewall para proteger y filtrar el acceso a los recursos, incluidas las máquinas virtuales (VM). Ahora está protegido contra amenazas externas, pero debe permitir a los desarrolladores y científicos de datos, que trabajan de forma remota, acceso directo a esas VM.

En un modelo tradicional, debe exponer los puertos del Protocolo de escritorio remoto (RDP) o Secure Shell (SSH) a Internet. Estos protocolos se pueden usar para obtener acceso remoto a las VM. Este proceso crea una amenaza de superficie significativa que los atacantes que buscan activamente máquinas accesibles con puertos de administración abiertos, como RDP o SSH, pueden explotar. Cuando se consigue poner en peligro a una máquina virtual, se usa como punto de entrada para atacar más recursos dentro de su entorno.

Azure Bastion

Azure Bastion es un servicio que se implementa que le permite conectarse a una máquina virtual mediante el explorador y Azure Portal. Azure Bastion es un nuevo servicio PaaS totalmente administrado por la plataforma que se aprovisiona en las redes virtuales. Azure Bastion proporciona conectividad RDP y SSH segura e ininterrumpida a las máquinas virtuales, directamente desde Azure Portal mediante la Seguridad de la capa de transporte (TLS). Cuando se conecta a través de Azure Bastion, las máquinas virtuales no necesitan una dirección IP pública, un agente ni software cliente especial.



Bastion proporciona conectividad segura de RDP y SSH a todas las VM en la red virtual y las redes virtuales emparejadas en la que se está aprovisionando. El uso de Azure Bastion protege las máquinas virtuales frente a la exposición de los puertos de RDP/SSH al mundo exterior, al tiempo que ofrece acceso seguro mediante RDP/SSH.

Por cada red virtual con soporte para emparejamiento de red virtual se lleva a cabo una implementación de Azure Bastion, y no por suscripción, cuenta o máquina virtual. Una vez que haya aprovisionado el servicio Azure Bastion en su red virtual, la experiencia RDP/SSH estará disponible para todas las máquinas virtuales de la misma red virtual, así como las redes virtuales emparejadas.

Características clave de Azure Bastion

Las siguientes características están disponibles:

- **RDP y SSH directamente en Azure Portal:** Puede ir a la sesión RDP y SSH en Azure Portal con una experiencia de un solo clic.
- **Sesión remota a través de TLS y cruce de firewall para RDP/SSH**: desde Azure Portal, una conexión a la máquina virtual, abrirá un cliente web basado en HTML5 que se transmite automáticamente al dispositivo local. Obtendrá el Protocolo de escritorio remoto (RDP) y Secure Shell (SSH) para atravesar los firewalls corporativos de forma segura. La conexión se realiza de forma segura mediante el protocolo Seguridad de la capa de transporte (TLS) para establecer el cifrado.
- **No se requiere ninguna dirección IP pública en la VM de Azure:** Azure Bastion abre la conexión RDP/SSH a la máquina virtual de Azure con la dirección IP privada en la VM. No necesita una IP pública.

- **No hay problemas de administración de los NSG:** Un servicio PaaS de Azure de plataforma totalmente administrada que se refuerza internamente para proporcionar una conexión RDP/SSH segura. No es necesario que aplique ningún NSG en una subred de Azure Bastion.
- **Protección frente al examen de puertos:** Ya no es necesario exponer las máquinas virtuales a Internet, las VM están protegidas contra la exploración de puertos por parte de usuarios malintencionados o no autorizados que se encuentran fuera de la red virtual.
- **Protección en un solo lugar frente a explotaciones de vulnerabilidades de día cero**: Azure Bastion es un servicio PaaS totalmente administrado de plataforma. Dado que se encuentra en el perímetro de la red virtual, no es necesario preocuparse por proteger cada máquina virtual de la red virtual. La plataforma de Azure protege contra ataques de día cero manteniendo automáticamente el servicio Azure Bastion protegido y siempre actualizado.

Use Azure Bastion para establecer la conectividad RDP y SSH segura con las máquinas virtuales de Azure.

Acceso Just-In-Time

El acceso Just-In-Time (JIT) permite bloquear el tráfico entrante a las máquinas virtuales; ya que reduce la exposición a ataques al mismo tiempo que se proporciona un acceso sencillo para conectarse a las máquinas virtuales cuando sea necesario.

Cuando se habilita el acceso a la máquina virtual Just-in-Time, se pueden seleccionar los puertos en la máquina virtual en los que se bloqueará el tráfico entrante. Microsoft Defender for Cloud, una herramienta para la administración de posiciones y protección frente a amenazas, garantiza que existen reglas para "denegar todo el tráfico entrante" de los puertos seleccionados en el grupo de seguridad de red (NSG) y las reglas de Azure Firewall. Estas reglas restringen el acceso a los puertos de administración de las máquinas virtuales de Azure y los defienden frente a ataques.

En caso de que ya existan otras reglas relativas a los puertos seleccionados, las reglas existentes tendrán prioridad sobre las nuevas reglas para "denegar todo el tráfico entrante". Si no hay ninguna regla existente en los puertos seleccionados, las nuevas reglas tendrán prioridad principal en los grupos de seguridad de red y Azure Firewall.

Cuando un usuario solicita acceso a una máquina virtual, Defender for Cloud comprueba que este tenga permisos de control de acceso basado en rol (RBAC de Azure) para ella. Si la solicitud se aprueba, Defender for Cloud configura los grupos de seguridad de red y Azure Firewall para permitir el tráfico entrante a los puertos seleccionados desde las direcciones (o rangos) IP relevantes durante el periodo especificado. Una vez transcurrido ese tiempo, Defender for Cloud restaura los NSG a su estado anterior. Las conexiones que ya están establecidas no se interrumpen.

JIT necesita que Microsoft Defender para servidores esté habilitado en la suscripción.

Descripción de las maneras en que Azure cifra los datos

El espionaje, el robo de datos y la filtración de datos constituyen una amenaza real para cualquier empresa. La pérdida de datos confidenciales puede ser paralizante y tener consecuencias jurídicas. Para la mayoría de las organizaciones, los datos son el recurso más valioso. En una estrategia de seguridad por capas, el uso del cifrado sirve como la última y más fuerte línea de defensa.

Cifrado en Azure

Microsoft Azure proporciona muchas maneras diferentes de proteger los datos, cada una de ellas depende del servicio o el uso que se requiera.

- **Azure Storage Service Encryption** ayuda a proteger los datos en reposo al cifrarlos automáticamente antes de almacenarlos en discos administrados de Azure, Azure Blob Storage, Azure Files o Azure Queue Storage, y descifrarlos antes de recuperarlos.
- **Azure Disk Encryption** le ayuda a cifrar discos de las máquinas virtuales de IaaS con Windows y Linux. Azure Disk Encryption usa la característica estándar del sector BitLocker de Windows y la característica dm-crypt de Linux para ofrecer cifrado de volumen para los discos de datos y del sistema operativo.
- El **cifrado de datos transparente (TDE)** ayuda a proteger Azure SQL Database y Azure Data Warehouse frente a la amenaza de actividad malintencionada. También realiza cifrado y descifrado de la base de datos en tiempo real, copias de seguridad asociadas y archivos de registro de transacciones en reposo sin necesidad de efectuar cambios en la aplicación.

¿Qué es Azure Key Vault?

Azure Key Vault es un servicio centralizado en la nube para almacenar secretos de aplicación. Key Vault ayuda a controlar los secretos de la aplicación al mantenerlos en una sola ubicación centralizada y al proporcionar funcionalidades de acceso seguro, control de permisos y registro de acceso. Es útil para diferentes tipos de escenarios:

- **Administración de secretos**. Puede usar Key Vault para almacenar de forma segura y controlar de manera estricta el acceso a tokens, contraseñas, certificados, claves de interfaz de programación de aplicaciones (API) y otros secretos.
- **Administración de claves**. Puede usar Key Vault como solución de administración de claves. Key Vault facilita la creación y el control de las claves de cifrado usadas para cifrar los datos.
- **Administración de certificados**. Key Vault permite aprovisionar, administrar e implementar certificados públicos y privados de Capa de sockets seguros y de Seguridad de la capa de transporte (SSL/TLS) para los recursos de Azure y los recursos conectados internamente, con más facilidad.
- **Almacenamiento de secretos respaldados por módulos de seguridad de hardware (HSM)**. Las claves y los secretos se pueden proteger mediante software, o bien con dispositivos HSM validados por FIPS 140-2 nivel 2.

Use las distintas formas en que Azure puede cifrar los datos para protegerlos con independencia de su ubicación o estado.

Descripción de las funcionalidades de administración de seguridad de Azure

Descripción de la administración de la posición de seguridad en la nube

Los sistemas basados en la nube evolucionan y cambian continuamente a medida que las empresas se mueven de un entorno local a la nube. Este cambio hace difícil para cualquier Departamento de TI saber si sus datos o recursos gozan de la protección total de la que solían gozar. Incluso un pequeño error de configuración de una nueva característica puede aumentar la superficie de ataque disponible para que los delincuentes la aprovechen.

La administración de la posición de seguridad en la nube (CSPM) es una clase relativamente nueva de herramientas diseñadas para mejorar la administración de la seguridad en la nube. Evalúa los sistemas y alerta automáticamente al personal de seguridad de su Departamento de TI cuando se detecta una vulnerabilidad. CSPM usa herramientas y servicios en el entorno de nube para supervisar y priorizar las mejoras y características de seguridad.

CSPM usa una combinación de herramientas y servicios:

- Control de acceso basado en la confianza cero: Considera el nivel de amenaza activo durante las decisiones de control de acceso.
- Puntuación del riesgo en tiempo real: Proporciona visibilidad sobre los principales riesgos.
- Administración de amenazas y vulnerabilidades (TVM): Establece una vista holística de la superficie y el riesgo de ataque de la organización, y la integra en las operaciones y la toma de decisiones de ingeniería.
- Detección de riesgos: para comprender la exposición de los datos de la propiedad intelectual de la empresa en servicios en la nube autorizados y no autorizados.
- Directiva técnica: Permite aplicar barreras para auditar y exigir los estándares y directivas de la organización a los sistemas técnicos.
- Arquitecturas y sistemas de modelado de amenazas: Se usan junto con otras aplicaciones específicas.

El objetivo principal de un equipo de seguridad en la nube que trabaja en la administración de la posición es informar continuamente sobre la posición de seguridad de la organización y mejorar dicha posición, centrándose en interrumpir la rentabilidad de la inversión (ROI) de un posible atacante.

La función de CSPM en su organización se puede diseminar por varios equipos o puede tener un equipo dedicado. CSPM puede ser útil para muchos equipos de su organización:

- Equipo información sobre amenazas
- Tecnología de la información
- Equipos de administración de riesgos y cumplimiento

- Líderes empresariales y expertos en la materia
- Arquitectura y operaciones de seguridad
- Equipo de auditoría

Use CSPM para mejorar la administración de la seguridad en la nube mediante la evaluación del entorno y el envío automático de alertas al personal de seguridad en caso de presentarse vulnerabilidades.

Descripción de Microsoft Defender for Cloud

Microsoft Defender for Cloud es una herramienta para la administración de la posición de seguridad y la protección contra amenazas. Esta refuerza la posición de seguridad de los recursos en la nube y, gracias a los planes integrados de Microsoft Defender, Defender for Cloud protege las cargas de trabajo híbridas que se ejecutan en Azure y otras plataformas en la nube.

Microsoft Defender for Cloud rellena tres necesidades vitales a medida que administra la seguridad de los recursos y las cargas de trabajo en la nube y en el entorno local:

- **Evaluación continua**: conozca su posición de seguridad, identifique y realice un seguimiento de las vulnerabilidades.
- **Seguridad**: proteja todos los recursos y servicios conectados.
- **Defender**: detecte y resuelva las amenazas a recursos, cargas de trabajo y servicios.

Las características de Microsoft Defender for Cloud, que cumplen estos requisitos, cubren dos grandes pilares de la seguridad en la nube: administración de la posición de seguridad en la nube y protección de cargas de trabajo en la nube.

Administración de la posición de seguridad en la nube (CSPM)

En Microsoft Defender for Cloud, las características de administración de posición proporcionan:

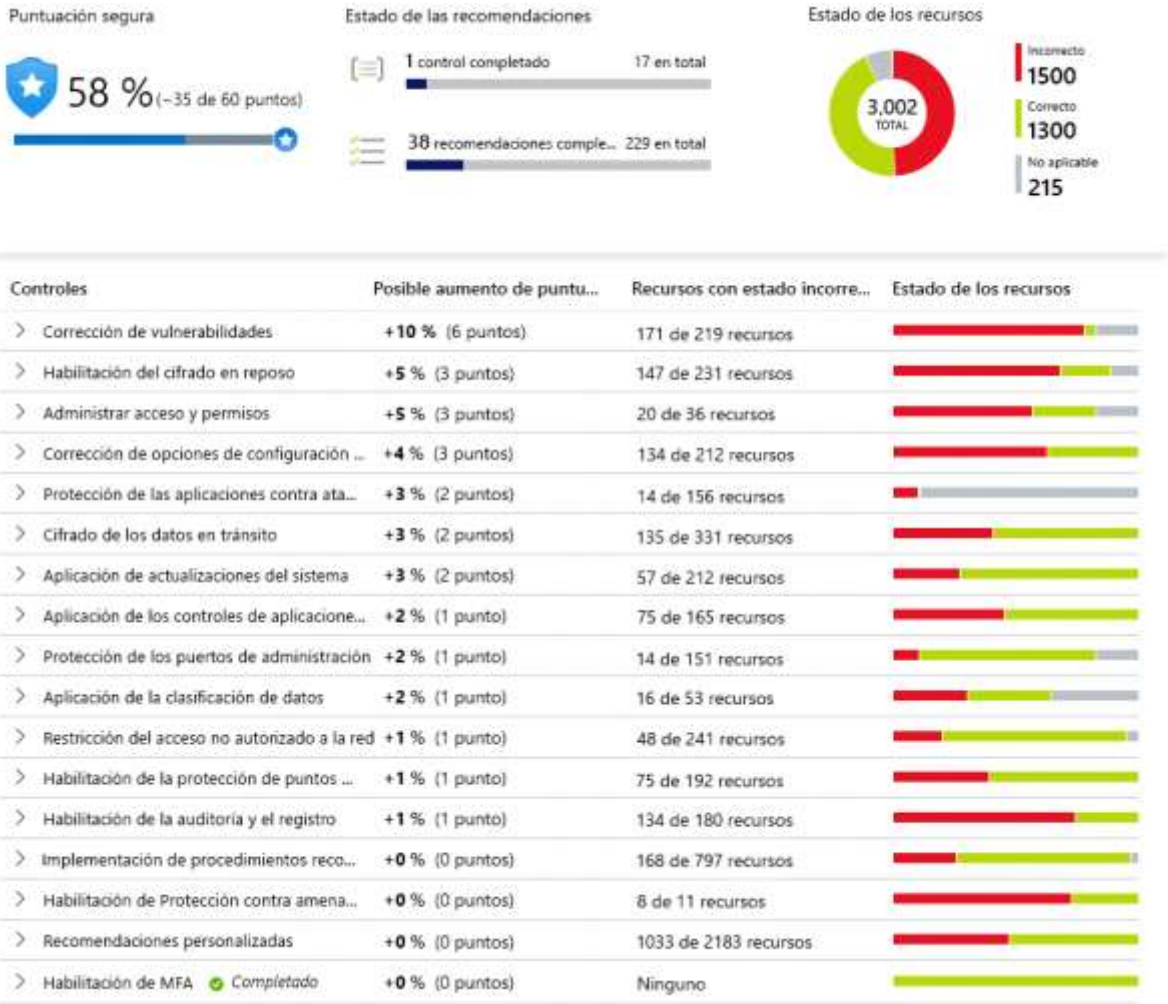
- Visibilidad: para ayudarle a entender su situación de seguridad actual.
- Guía de protección: para ayudarle a mejorar la seguridad de forma eficaz.

Recomendaciones de protección y visibilidad

La característica central de Microsoft Defender for Cloud que le permite lograr esos objetivos es la puntuación segura. Microsoft Defender for Cloud evalúa continuamente los recursos, las suscripciones y la organización en busca de problemas de seguridad. A continuación, agrega todos los resultados a una sola puntuación para que pueda conocer de un vistazo la situación de la seguridad actual: cuanto mayor sea la puntuación, menor será el nivel de riesgo identificado.

Microsoft Defender for Cloud también proporciona recomendaciones de protección basadas en los errores de configuración y los puntos débiles de seguridad identificados. Las recomendaciones se agrupan en controles de seguridad. Cada control es un grupo lógico de recomendaciones de seguridad relacionadas y refleja las superficies de ataque vulnerables. La puntuación solo mejora cuando corrige todas las recomendaciones para un solo recurso de un control. Use estas

recomendaciones de seguridad para reforzar la posición de seguridad de los recursos híbridos y de varias nubes de Azure de su organización.



En el procedimiento interactivo siguiente se muestra cómo puede usar las recomendaciones de puntuación segura y protección en Microsoft Defender for Cloud. Seleccione la imagen siguiente para empezar y siga las indicaciones que aparecen en pantalla.

Protección de cargas de trabajo en la nube (CWP)

El segundo pilar de la seguridad en la nube es la protección de cargas de trabajo en la nube. A través de las funcionalidades de protección de cargas de trabajo en la nube, Microsoft Defender for Cloud puede detectar y resolver amenazas a recursos, cargas de trabajo y servicios. Las protecciones de las cargas de trabajo en la nube se entregan mediante planes integrados de Microsoft Defender, específicos de los tipos de recursos de las suscripciones y proporcionan características de seguridad mejorada para las cargas de trabajo. Se describen en la unidad siguiente.

Descripción de la seguridad mejorada de Microsoft Defender for Cloud

Microsoft Defender for Cloud se ofrece en dos modos:

- Microsoft Defender for Cloud (gratis): Microsoft Defender for Cloud está habilitado de forma gratuita en todas las suscripciones de Azure. Mediante modo gratuito tendrá la puntuación segura y sus características relacionadas: la directiva de seguridad, la evaluación de seguridad continua y las recomendaciones de seguridad prácticas para que pueda proteger los recursos de Azure.
- Microsoft Defender for Cloud con características de seguridad mejorada: la habilitación de la seguridad mejorada amplía las funcionalidades del modo gratuito a las cargas de trabajo que se ejecutan en nubes de Azure, híbridas y otras plataformas de nube, lo que proporciona una administración de seguridad unificada y protección contra amenazas en todas las cargas de trabajo. Las protecciones de las cargas de trabajo en la nube se entregan mediante planes integrados de Microsoft Defender, específicos de los tipos de recursos de las suscripciones y proporcionan características de seguridad mejorada para las cargas de trabajo.

Planes de Defender

Microsoft Defender for Cloud incluye una gama de protecciones avanzadas e inteligentes para las cargas de trabajo. Las protecciones de cargas de trabajo se proporcionan a través de planes de Microsoft Defender específicos de los tipos de recursos de las suscripciones. Estos son los planes de Microsoft Defender for Cloud que puede seleccionar:

- **Microsoft Defender para servidores** agrega la detección de amenazas y defensas avanzadas para las máquinas Windows y Linux.
- **Microsoft Defender para App Service** identifica ataques dirigidos a aplicaciones que se ejecutan mediante App Service.
- **Microsoft Defender para Storage** detecta actividad potencialmente dañina en las cuentas de Azure Storage.
- **Microsoft Defender para SQL** protege las bases de datos y sus datos dondequiera que se encuentran.
- **Microsoft Defender para Kubernetes** proporciona protección del entorno de seguridad de Kubernetes nativa de nube, protección de cargas de trabajo y protección en tiempo de ejecución.
- **Microsoft Defender para registros de contenedor** protege todos los registros basados en Azure Resource Manager de su suscripción.
- **Microsoft Defender para Key Vault** es una protección contra amenazas avanzada para Azure Key Vault.
- **Microsoft Defender para Resource Manager** supervisa automáticamente las operaciones de administración de recursos en la organización.
- **Microsoft Defender para DNS** proporciona una capa adicional de protección para los recursos que usan la funcionalidad de resolución de nombres proporcionada por Azure de Azure DNS.
- **Microsoft Defender para las protecciones relacionales de código abierto** ofrece protección contra amenazas para bases de datos relacionales de código abierto.

Estos planes diferentes se pueden habilitar por separado y se ejecutarán simultáneamente para proporcionar una defensa completa para procesos, datos y capas de servicio de su entorno.

Características de seguridad mejoradas

Los planes de Microsoft Defender específicos de los tipos de recursos de las suscripciones proporcionan características de seguridad mejorada para las cargas de trabajo. A continuación se enumeran algunas de las características de seguridad mejorada.

- Detección y respuesta de puntos de conexión completa: Microsoft Defender para servidores incluye Microsoft Defender para punto de conexión para una detección y respuesta de puntos de conexión (EDR) completa.

- Examen de vulnerabilidades para máquinas virtuales, registros de contenedor y recursos SQL: implemente fácilmente un analizador en todas las máquinas virtuales. Vea, investigue y corrija los resultados directamente en Microsoft Defender for Cloud.
- Seguridad en varias nubes: conecte las cuentas de Amazon Web Services (AWS) y Google Cloud Platform (GCP) para proteger los recursos y cargas de trabajo de esas plataformas con una variedad de características de seguridad de Microsoft Defender for Cloud.
- Seguridad híbrida: Obtenga una vista unificada de la seguridad de todas sus cargas de trabajo locales y en la nube. Aplique directivas de seguridad y evalúe constantemente la seguridad de las cargas de trabajo de nube híbrida para garantizar el cumplimiento normativo con los estándares de seguridad. Recopile, busque y analice datos de seguridad de varios orígenes, incluidos firewalls y otras soluciones de partners.
- Alertas de protección contra amenazas: supervise las redes, las máquinas y los servicios en la nube para detectar ataques entrantes y actividad posterior a una infracción de seguridad. Optimice la investigación con herramientas interactivas e inteligencia de amenazas contextual.
- Seguimiento del cumplimiento de una serie de estándares: Microsoft Defender for Cloud evalúa continuamente el entorno de nube híbrida para analizar los factores de riesgo de acuerdo con los controles y procedimientos recomendados de Azure Security Benchmark. Al habilitar las características de seguridad mejoradas, puede aplicar una variedad de otros estándares del sector, estándares normativos y puntos de referencia según las necesidades de la organización. Agregue estándares y realice un seguimiento del cumplimiento con ellos desde el panel de cumplimiento normativo.
- Controles de acceso y aplicación: bloquee el malware y otras aplicaciones no deseadas aplicando recomendaciones basadas en el aprendizaje automático adaptadas a sus cargas de trabajo específicas para crear listas de bloqueos y permisos. Reduzca la superficie de la red que está expuesta a ataques mediante un acceso Just-In-Time controlado a los puertos de administración de las VM de Azure. Los controles de acceso y aplicación reducen drásticamente la exposición a ataques por fuerza bruta y a otros ataques de la red.

Entre las ventajas adicionales se incluye la protección contra amenazas para los recursos conectados al entorno de Azure y a las características de seguridad de contenedores, entre otras. Algunas características pueden estar asociadas a planes de Defender específicos para cargas de trabajo concretas.

Descripción de Azure Security Benchmark y las líneas de base de seguridad para Azure

Diariamente se publican nuevos servicios y características en Azure; los desarrolladores publican rápidamente nuevas aplicaciones en la nube basadas en estos servicios y los atacantes buscan siempre nuevas formas de aprovechar los recursos configurados incorrectamente.

Azure Security Benchmark (ASB) y las líneas de base de seguridad de Azure, que están estrechamente relacionadas, ayudan a las organizaciones a proteger sus soluciones en la nube en Azure.

Azure Security Benchmark

Microsoft ha descubierto que el uso de puntos de referencia de seguridad puede ayudar a las organizaciones a proteger rápidamente sus implementaciones en la nube y reducir el riesgo.

La prueba comparativa de seguridad de Azure (ASB) proporciona recomendaciones y procedimientos recomendados para ayudar a mejorar la seguridad de las cargas de trabajo, los datos y los servicios de Azure. La mejor manera de entender Azure Security Benchmark consiste en verlo en GitHub Azure Security Benchmark V3. Alerta de spoiler, es una hoja de cálculo de Excel. Algunos de los elementos clave de información de ASB V3 son los siguientes:

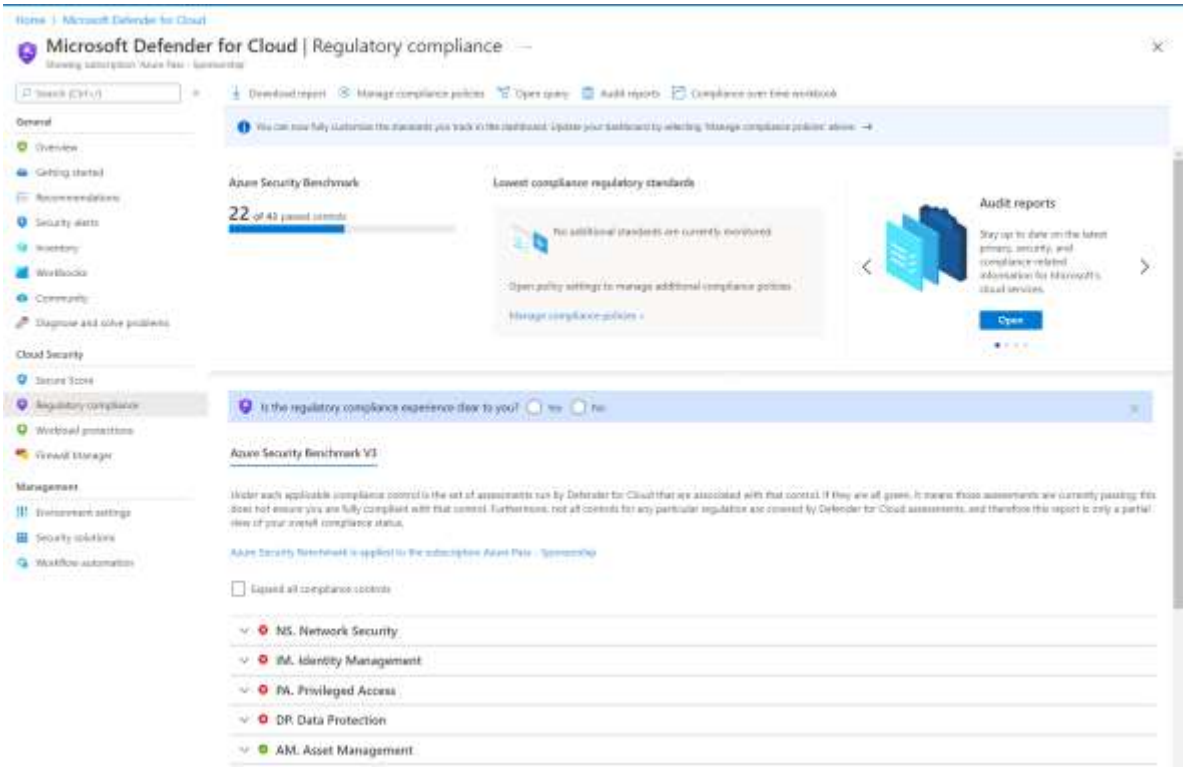
- Identificador de ASB: cada elemento de línea de ASB tiene un identificador que se asigna a una recomendación específica.
- Dominio de control: los dominios de control de ASB incluyen seguridad de red, protección de datos, administración de identidades, acceso con privilegios, respuesta a incidentes, seguridad de punto de conexión, por nombrar solo algunos. El dominio de control se describe mejor como una característica o actividad general que no es específica de una tecnología o implementación.
- Asignación a marcos del sector: las recomendaciones incluidas en ASB se asignan a marcos del sector existentes, como el Centro de Seguridad de Internet (CIS), el Instituto Nacional de Estándares y Tecnología (NIST), y los marcos de estándares de seguridad de datos del sector de tarjetas de pago (PCI DSS). Esto facilita la seguridad y el cumplimiento para las aplicaciones cliente que se ejecutan en servicios de Azure.
- Recomendación: para cada área de dominio de control puede haber muchas recomendaciones distintas. Cada recomendación captura una funcionalidad específica asociada al área de dominio de control y es un control por si misma. Por ejemplo, el dominio de control "Seguridad de red" de ASB v3 tiene 10 recomendaciones distintas identificadas como NS-1 a NS-10. Cada una de estas recomendaciones describe un control específico bajo la seguridad de red.
- Principio de seguridad: cada recomendación enumera un "principio de seguridad" que explica el "por qué" del control en el nivel independiente de la tecnología
- Guía de Azure: la guía de Azure se centra en el "cómo", y detalla las características técnicas pertinentes y las formas de implementar los controles en Azure.

Otros fragmentos de información de ASB incluyen vínculos a información sobre la implementación y sobre las partes interesadas de la seguridad e instrucciones sobre la asignación a Azure Policy. No se muestran en la imagen siguiente. La imagen siguiente es un extracto de Azure Security Benchmark (ASB v3) y se muestra como un ejemplo del tipo de contenido que se incluye en ASB v3. La imagen no está pensada para mostrar el texto completo de ninguno de los elementos de línea.

Mapping to industry frameworks

ASB ID	Control Domain	CIS Controls v7.1 ID(s)	CIS Controls v8 ID(s)	NIST SP800-53 v4 ID(s)	PCI-DSS v3.2.1 ID(s)	Recommendation	Security Principle	Azure Guidance
NS-1	Network Security	9.2 - Ensure Only Approved Ports, Protocols and Services Are Running 9.4 - Apply Host-Based Firewalls or Port Filtering 12.3 - Deny Communications with Known Malicious IP	3.12 - Segment Data Processing and Storage Based on Sensitivity 13.4 - Perform Traffic Filtering Between Network Segments 4.4 - Implement and Manage a Firewall on Servers	AC-4: INFORMATION FLOW ENFORCEMENT SC-2: APPLICATION PARTITIONING SC-7: BOUNDARY PROTECTION	1.1 1.2 1.3	Establish network segmentation boundaries	Ensure that your virtual network deployment aligns to your enterprise segmentation strategy defined in the GS-2 security control. Any workload that could incur higher risk for the organization should be in isolated virtual networks.	Create a virtual network (VNet) as a fundamental segmentation approach in your Azure network, so resources such as VMs can be deployed into the VNet within a network boundary. To further segment the network, you can create subnets inside VNet for smaller sub-networks.
NS-2	Network Security	14.1 - Segment the Network Based on Sensitivity	3.12 - Segment Data Processing and Storage Based on Sensitivity 4.4 - Implement and Manage a Firewall on Servers	AC-4: INFORMATION FLOW ENFORCEMENT SC-2: APPLICATION PARTITIONING SC-7: BOUNDARY PROTECTION	1.1 1.2 1.3	Secure cloud services with network controls	Secure cloud services by establishing a private access point for the resources. You should also disable or restrict access from public network when possible.	Deploy private endpoints for all Azure resources that support the Private Link feature, to establish a private access point for the resources. You should also disable or restrict public network access to services where feasible.

Microsoft Defender for Cloud evalúa continuamente el entorno de nube híbrida de una organización para analizar los factores de riesgo de acuerdo con los controles y procedimientos recomendados de Azure Security Benchmark. Algunos de los controles usados en ASB incluyen seguridad de red, control de identidad y acceso, protección de datos, recuperación de datos, respuesta a incidentes, etc.



Bases de referencia de seguridad para Azure

Las líneas de base de seguridad para Azure aplican instrucciones de Azure Security Benchmark al servicio específico para el que se define. Por ejemplo, la línea de base de seguridad para Azure Active Directory aplica instrucciones de la versión 2.0 de Azure Security Benchmark a Azure Active Directory.

Las líneas de base de seguridad de Azure ayudan a las organizaciones a reforzar la seguridad gracias mediante herramientas, seguimiento y características de seguridad mejorados. También les proporcionan una experiencia coherente a la hora de proteger su entorno. El contenido de la

línea de base de seguridad se agrupa por los dominios de control definidos por Azure Security Benchmark y que son aplicables al servicio.

Cada línea base de seguridad de Azure incluye la siguiente información:

- **Identificador de Azure**: El identificador de la prueba comparativa de seguridad de Azure que corresponde a la recomendación.
- **Control de Azure**: el contenido se agrupa por área de dominio de control, como se muestra en Azure Security Benchmark, y se aplica al servicio para el que se define la línea de base de seguridad.
- **Recomendación de puntos de referencia**: esto se asigna a la recomendación para el identificador de ASB asociado (o el identificador de Azure). Cada recomendación describe un control individual en un dominio de control.
- **Guía del cliente**: la lógica de la recomendación y vínculos a instrucciones sobre cómo implementarla.
- **Responsabilidad**: ¿Quién es el responsable de implementar el control? Las posibles respuestas son: responsabilidad del cliente, responsabilidad de Microsoft o responsabilidad compartida.
- **Supervisión de Microsoft Defender for Cloud**: ¿Microsoft Defender for Cloud supervisa el control?

La imagen siguiente es un extracto de la línea de base de Azure AD y se muestra como un ejemplo del tipo de contenido que se incluye en la línea de base. La imagen no está pensada para mostrar el texto completo de ninguno de los elementos de línea.

Service	Azure Control	Azure ID	Benchmark Recommendation	Customer Guidance	Responsibility	Microsoft Defender for Cloud Monitoring
Azure Active Directory	Network Security	NS-6	Simplify network security rules	Use Azure Virtual Network Service Tags to define network access controls on network security groups or Azure Firewall configured for your Azure Active Directory resources.	Customer	Not applicable
Azure Active Directory	Network Security	NS-7	Secure Domain Name Service (DNS)	Azure Active Directory does not expose its underlying DNS configurations; these settings are maintained by Microsoft.	Microsoft	Not applicable

Consulte la documentación de Azure Security Benchmark para obtener una lista completa de las líneas base disponibles.