**Introducción**

Este módulo prepara a los administradores para proteger el acceso público, garantizando la confidencialidad, integridad y disponibilidad de aplicaciones y servicios

**Escenario**

Imagine que es un especialista en seguridad de Azure responsable de administrar la seguridad de los recursos de Azure a los que se puede acceder públicamente. Su organización confía en los servicios de Azure para ofrecer aplicaciones web y API a clientes y asociados, y debe asegurarse de que estos recursos estén protegidos contra amenazas al tiempo que se mantiene un alto rendimiento.

**Objetivos de aprendizaje**

Al final de este módulo, los participantes podrán:

* Planee e implemente estrategias de seguridad para el acceso público a los recursos de Azure, protegiendo contra accesos no autorizados y vulneraciones de datos.
* Configure y administre la Seguridad de la capa de transporte (TLS) para proteger las aplicaciones, incluyendo Azure App Service y API Management, para cifrar los datos en tránsito.
* Diseñe, implemente y administre instancias de Azure Firewall, incluyendo las directivas de firewall y Azure Firewall Manager, para proteger el tráfico de red y las aplicaciones.
* Planee e implemente instancias de Azure Application Gateway para optimizar la entrega, escalabilidad y seguridad de las aplicaciones web.
* Implemente y configure instancias de Azure Front Door, incluyendo Content Delivery Network (CDN), para mejorar el rendimiento y la disponibilidad de las aplicaciones web.
* Configure y administre instancias de Web Application Firewall (WAF) para proteger las aplicaciones web frente a ataques comunes basados en la web.
* Realice recomendaciones informadas sobre cuándo usar Azure DDoS Protection Estándar para defenderse contra ataques distribuidos de denegación de servicio (DDoS).

**Objetivos**

El módulo tiene como objetivo dotar a los participantes de los conocimientos y habilidades necesarios para diseñar, implementar y administrar estrategias de seguridad completas de acceso público a los recursos de Azure. Los participantes podrán proteger eficazmente aplicaciones web, API y el tráfico de red, garantizando la disponibilidad y el rendimiento de los servicios críticos mientas protegen contra amenazas de seguridad.

**Planeamiento e implementación de Seguridad de la capa de transporte (TLS) en aplicaciones, incluidas Azure App Service y API Management**

La planeación e implementación del cifrado de TLS en aplicaciones de Azure es esencial para garantizar la seguridad de los datos durante el tránsito. Este es un resumen de seis puntos para mejorar la TLS en Azure App Service y API Management:

**1. Segmentación de red con red virtual:**

* Implemente aplicaciones de Azure, como App Service y API Management, dentro de una red virtual (VNet) privada. Asigne direcciones IP privadas a los servicios, absteniéndose de IP públicas a menos que sea explícitamente necesario.

**2. Configuración de grupos de seguridad de red (NSG):**

* Use grupos de seguridad de red para controlar el tráfico entrante y saliente. Aproveche las etiquetas de servicio de Azure Virtual Network para definir controles de acceso en grupos de seguridad de red, lo que garantiza caminos de comunicación específicos y protegidos.

**3. Aproveche Azure Private Link:**

* Implemente los puntos de conexión privados de Azure Private Link para los servicios de Azure, estableciendo un mecanismo de conectividad privado, lo que garantiza el acceso seguro y la confidencialidad de los datos.

**4. Deshabilitación del acceso a la red pública:**

* Asegúrese de que el acceso a la red pública está deshabilitado para los recursos de Azure, incluido Azure SQL Managed Instance, para reforzar la seguridad. Limite el acceso a los servicios a través de puntos de conexión privados o dentro de redes virtuales.

**5. Administración centralizada de identidades con Microsoft Entra ID:**

* Implemente la autenticación de Microsoft Entra ID para el acceso al plano de datos, lo que garantiza la administración centralizada de identidades. Limite o evite el uso de métodos de autenticación local, pasando principalmente a Microsoft Entra ID.

**6. Supervisión con Microsoft Defender for Cloud:**

* Supervise las configuraciones mediante Microsoft Defender for Cloud, usando definiciones integradas de Azure Policy para garantizar el cumplimiento de los procedimientos recomendados, como el aprovisionamiento de Microsoft Entra ID.

**Planificación, implementación y administrará una instancia de Azure Firewall, las directivas de firewall y de Azure Firewall Manager**

Azure Firewall es un servicio de seguridad de firewall de red inteligente y nativo de la nube que le proporciona la mejor protección contra amenazas para las cargas de trabajo en la nube que se ejecutan en Azure. Se trata de un firewall como servicio con estado completo que incorpora alta disponibilidad y escalabilidad a la nube sin restricciones. Asimismo, proporciona la opción de realizar la inspección del tráfico de este a oeste y de norte a sur.

Azure Firewall se ofrece en tres SKU: Estándar, Prémium y Básico.

**Azure Firewall Estándar**

Azure Firewall Estándar proporciona fuentes de inteligencia sobre amenazas y filtrado L3-L7 directamente desde Microsoft Cyber Security. El filtrado basado en la inteligencia sobre amenazas puede enviar alertas y denegar el tráfico desde o hacia dominios y direcciones IP malintencionados, que sean conocidos y que se actualicen en tiempo real para protegerle frente a ataques nuevos y emergentes.

**Azure Firewall Prémium**

Azure Firewall Premium proporciona funcionalidades avanzadas que incluyen IDPS basados en firmas para permitir la detección rápida de ataques mediante la búsqueda de patrones específicos. Estos patrones pueden incluir secuencias de bytes en el tráfico de red o secuencias de instrucciones malintencionadas conocidas usadas por malware. Existen más de 67 000 firmas en más de 50 categorías que se actualizan en tiempo real para protegerle contra vulnerabilidades nuevas y emergentes. Las categorías de vulnerabilidades de seguridad incluyen malware, suplantación de identidad, minería de monedas y ataques de troyanos.

**Azure Firewall Básico**

La versión básica de Azure Firewall está pensada para que los clientes de pymes protejan sus entornos en la nube de Azure. de red. Proporciona la protección esencial que los clientes pymes necesitan a un precio asequible.

La versión básica de Azure Firewall es similar a Firewall Estándar, pero tiene las siguientes limitaciones principales:

* Solo admite el modo de alerta de Intel para amenazas
* Se ha corregido la unidad de escalado para que el servicio se ejecute en dos instancias de back-end de máquina virtual
* Se recomienda para entornos con un rendimiento estimado de 250 Mbps

**Azure Firewall Manager**

**Azure Firewall Manager** es un servicio de administración de seguridad que proporciona una directiva de seguridad central y administración de rutas para perímetros de seguridad en la nube.

Firewall Manager puede proporcionar administración de seguridad para dos tipos de arquitectura de red:

* **Centro virtual protegido**

Un centro de Azure Virtual WAN es un recurso administrado por Microsoft que permite crear fácilmente arquitecturas de tipo hub-and-spoke (centro y radio). Cuando las directivas de seguridad y enrutamiento están asociadas a ese concentrador, se denomina centro virtual protegido .

* **Red virtual de centro**

Se trata de una red virtual estándar de Azure que crea y administra uno mismo. Cuando las directivas de seguridad están asociadas con este tipo de centro, se conoce como red virtual de centro. En este momento, solo se admite la directiva de Azure Firewall. Puede emparejar las redes virtuales de radio que contienen los servidores y servicios de carga de trabajo. También puede administrar los firewalls de redes virtuales independientes que no estén emparejadas con ningún radio.

**Características de Azure Firewall Manager**

Azure Firewall Manager ofrece las siguientes características:

**Implementación y configuración centralizadas de Azure Firewall**

Puede implementar y configurar de forma centralizada varias instancias de Azure Firewall que abarquen diferentes regiones y suscripciones de Azure.

**Directivas jerárquicas (globales y locales)**

Puede usar Azure Firewall Manager para administrar de forma centralizada las directivas de Azure Firewall en varios centros de conectividad virtuales protegidos. Los equipos de TI centrales pueden crear directivas de firewall globales para aplicar la directiva de firewall a los equipos de toda la organización. Las directivas de firewall creadas localmente permiten un modelo de autoservicio de DevOps, lo que aumenta la agilidad.

**Integración con seguridad como servicio de terceros para la seguridad avanzada**

Además de Azure Firewall, puede integrar los proveedores de seguridad como servicio (SECaaS) de terceros para proporcionar mayor protección de red para las conexiones de Internet de la red virtual y las ramas.

Esta característica solo está disponible en implementaciones de centros virtuales protegidos.

* Filtrado de tráfico de la red virtual a Internet (V2I)
  + Filtre el tráfico saliente de la red virtual con el proveedor de seguridad de terceros que prefiera.
  + Aproveche la protección de Internet avanzada con reconocimiento del usuario para sus cargas de trabajo en la nube que se ejecutan en Azure.
* Filtrado de tráfico de la rama a Internet (B2I)

Aproveche la conectividad de Azure y la distribución global para agregar fácilmente el filtrado de terceros para escenarios de rama a Internet.

**Administración centralizada de rutas**

Enrute fácilmente el tráfico al centro de conectividad seguro para filtrar y registrar sin necesidad de configurar manualmente rutas definidas por el usuario (UDR) en redes virtuales de radios.

Esta característica solo está disponible en implementaciones de centros virtuales protegidos.

Puede usar proveedores de terceros para el filtrado de tráfico de rama a Internet (B2I), en paralelo con Azure Firewall para rama a red virtual (B2V), red virtual a red virtual (V2V) y red virtual a Internet (V2I).

**Plan de protección contra DDoS**

Puede asociar las redes virtuales a un plan de protección contra DDoS en Azure Firewall Manager. Para más información, consulte Configuración de un plan de Azure DDoS Protection mediante Azure Firewall Manager.

**Administración de directivas de Web Application Firewall**

Puede crear y asociar de forma centralizada directivas de Web Application Firewall (WAF) para las plataformas de entrega de aplicaciones, como Azure Front Door y Azure Application Gateway. Para más información, consulte el artículo Administración de directivas de Web Application Firewall.

**Disponibilidad en regiones**

Las directivas de Azure Firewall se pueden usar en diferentes regiones. Por ejemplo, puede crear una directiva en Oeste de EE. UU. y usarla en Este de EE. UU.

**Planeamiento e implementación de una instancia de Azure Application Gateway**

**Cómo una puerta de enlace de aplicaciones acepta una solicitud**

1. Antes de que un cliente envíe una solicitud a una puerta de enlace de aplicaciones, resuelve el nombre de dominio de la puerta de enlace de aplicaciones mediante un servidor del sistema de nombres de dominio (DNS). Azure controla la entrada de DNS, ya que todas las puertas de enlace de aplicaciones están en el dominio de azure.com.
2. Azure DNS devuelve la dirección IP al cliente, que es la dirección IP de front-end de la puerta de enlace de aplicaciones.
3. La puerta de enlace de aplicaciones acepta el tráfico entrante en uno o varios clientes de escucha. Un cliente de escucha es una entidad lógica que comprueba si hay solicitudes de conexión. Se configura con una dirección IP de front-end, un protocolo y un número de puerto para las conexiones de los clientes a la puerta de enlace de aplicaciones.
4. Si el firewall de aplicaciones web (WAF) está en uso, la puerta de enlace de aplicaciones comprueba los encabezados y el cuerpo de la solicitud, si están presentes, según las reglas de WAF. Esta acción determina si la solicitud es una solicitud válida o una amenaza de seguridad. Si la solicitud es válida, se enruta al back-end. Si la solicitud no es válida y WAF se encuentra en modo de prevención, se bloquea como una amenaza de seguridad. Si está en modo de detección, la solicitud se evalúa y se registra, pero se reenvía al servidor back-end.

Azure Application Gateway puede usarse como un equilibrador de carga interno de la aplicación o como un equilibrador de carga de aplicación orientado a Internet. Una puerta de enlace de aplicaciones orientada a Internet usa direcciones IP públicas. El nombre DNS de una puerta de enlace de aplicaciones orientada Internet puede resolverse públicamente en su dirección IP pública. Como consecuencia, las puertas de enlace de aplicaciones orientadas a Internet pueden enrutar las solicitudes de cliente desde Internet.

Las puertas de enlace de aplicaciones internas usan solo las direcciones IP privadas. Si usa una zona DNS privada o personalizada, el nombre de dominio debe poder resolverse internamente en la dirección IP privada de la instancia de Application Gateway. Por lo tanto, los equilibradores de carga internos solo pueden enrutar las solicitudes de clientes con acceso a una red virtual para la puerta de enlace de aplicaciones.

**Cómo una puerta de enlace de aplicaciones enruta una solicitud**

Si una solicitud es válida o no está bloqueada por WAF, la puerta de enlace de aplicaciones evalúa la regla de enrutamiento de solicitud que está asociada con el cliente de escucha. Esta acción determina a qué grupo de back-end se va a enrutar la solicitud.

Según la regla de enrutamiento de solicitud, la puerta de enlace de aplicaciones determina si debe enrutar todas las solicitudes en el cliente de escucha a un grupo de back-end específico, enrutar las solicitudes a grupos de back-end diferentes en función de la ruta de acceso URL, o redirigir las solicitudes al otro puerto o sitio externos.

Cuando la puerta de enlace de aplicaciones selecciona el grupo de back-end, envía la solicitud a uno de los servidores back-end correctos en el grupo (y.y.y.y). Un sondeo de estado determina el estado del servidor. Si el grupo de back-end contiene varios servidores, la puerta de enlace de aplicaciones utiliza un algoritmo round robin para enrutar las solicitudes entre los servidores en buen estado. Esta carga equilibra las solicitudes en los servidores.

Después de que la puerta de enlace de aplicaciones determina el servidor back-end, abre una nueva sesión TCP con el servidor back-end según la configuración HTTP. La configuración HTTP especifica el protocolo, el puerto y otras configuraciones relacionadas con el enrutamiento que son necesarias para establecer una nueva sesión con el servidor back-end.

El puerto y el protocolo usados en la configuración HTTP determinan si el tráfico entre los servidores back-end y la puerta de enlace de aplicaciones está cifrado (para lograr TLS de un extremo a otro) o sin cifrar.

**Nota**

Las reglas se procesan en el orden en que aparecen en el portal para SKU v1.

Cuando una puerta de enlace de la aplicación envía la solicitud original al servidor back-end, respeta las opciones personalizadas en la configuración HTTP relacionadas con reemplazar el nombre de host, la ruta de acceso y el protocolo. Esta acción mantiene la afinidad de sesión basada en cookies, la purga de la conexión y la selección de nombre de host desde el back-end, entre otros.

Si el grupo de back-end:

* Es un punto de conexión público, la puerta de enlace de aplicaciones usa su dirección IP pública de front-end para tener acceso al servidor. Si no hay una dirección IP pública de front-end, se asigna una a la conectividad saliente externa.
* Contiene un FQDN que se puede resolver internamente o una dirección IP privada, la puerta de enlace de aplicaciones enruta la solicitud al servidor back-end mediante las direcciones IP privadas de su instancia.
* Contiene un punto de conexión externo o un FQDN que puede resolverse externamente, la puerta de enlace de aplicaciones enruta la solicitud al servidor back-end mediante la dirección IP pública de su front-end. Si la subred contiene puntos de conexión de servicio, la puerta de enlace de aplicación enrutará la solicitud al servicio a través de su dirección IP privada. La resolución de DNS se basa en una zona DNS privada o un servidor DNS personalizado (si está configurado), o bien utiliza el DNS predeterminado proporcionado por Azure. Si no hay una dirección IP pública de front-end, se asigna una a la conectividad saliente externa.

**Resolución DNS del servidor back-end**

Cuando el servidor de un grupo de back-end está configurado con un nombre de dominio completo (FQDN), Application Gateway realiza una búsqueda DNS para obtener las direcciones IP del nombre de dominio. El valor de IP se almacena en la memoria caché de la puerta de enlace de aplicación para permitir que llegue a los destinos más rápido al atender las solicitudes entrantes.

Application Gateway conserva esta información almacenada en caché durante el período equivalente al TTL (período de vida) del registro DNS y realiza una búsqueda DNS nueva una vez que expira el TTL. Si una puerta de enlace detecta un cambio en la dirección IP de su consulta de DNS posterior, comenzará a enrutar el tráfico a este destino actualizado. En caso de problemas como que la búsqueda DNS no reciba una respuesta o que el registro ya no exista, la puerta de enlace sigue usando las direcciones IP válidas conocidas. Esto garantiza un impacto mínimo en la ruta de acceso de datos.

* Al usar servidores DNS personalizados con Virtual Network de Application Gateway, es fundamental que todos los servidores sean idénticos y respondan de forma coherente con los mismos valores DNS.
* Los usuarios de servidores DNS personalizados locales deben garantizar la conectividad con Azure DNS a través de Azure DNS Private Resolver (recomendado) o la máquina virtual del reenviador DNS al usar una zona DNS privada para el punto de conexión privado.

**Modificaciones a una solicitud**

Application Gateway inserta seis encabezados adicionales en todas las solicitudes antes de reenviarlas al back-end. Estos encabezados son x-forwarded-for, x-forwarded-port, x-forwarded-proto, x-original-host, x-original-url y x-appgw-trace-id. El formato del encabezado x-forwarded-for es una lista separada por comas de valores IP:**puerto**.

Los valores válidos para x-forwarded-proto son HTTP o HTTPS. X-forwarded-port especifica el puerto al que llegó la solicitud en la puerta de enlace de aplicaciones. El encabezado x-original-host contiene el encabezado de host original con el que llegó la solicitud. Este encabezado es útil en la integración de Azure Website, donde el encabezado de host entrante se modifica antes de que el tráfico se enrute al back-end. Si la opción de afinidad de sesión está habilitada, se agrega una cookie de afinidad administrada por la puerta de enlace.

X-appgw-trace-id es un GUID único que genera Application Gateway para cada solicitud de cliente y que presenta en la solicitud reenviada al miembro del grupo de back-end. El GUID consta de 32 caracteres alfanuméricos presentados sin guiones (por ejemplo: ac882cd65a2712a0fe1289ec2bb6aee7). Este GUID se puede usar para correlacionar una solicitud recibida e iniciada por Application Gateway con un miembro del grupo de back-end a través de la propiedad transactionId de los registros de diagnóstico.

Puede configurar la puerta de enlace de aplicaciones para que modifique los encabezados y URL de solicitud y respuesta mediante la rescritura de encabezados HTTP y URL o para que modifique la ruta de acceso URI mediante una configuración de invalidación de la ruta de acceso. Sin embargo, a menos que realice la configuración, todas las solicitudes entrantes se procesan con proxy hacia el back-end.

**Planeamiento e implementación de una instancia de Azure Front Door, incluido Content Delivery Network (CDN)**

Tanto si va a entregar contenido y archivos como si va a compilar aplicaciones y API globales, Azure Front Door puede ayudarle a ofrecer una mayor disponibilidad, menor latencia, mayor escala y experiencias más seguras a los usuarios dondequiera que estén.

Azure Front Door es la nube moderna de Microsoft Content Delivery Network (CDN) que proporciona acceso rápido, confiable y seguro entre los usuarios y el contenido web estático y dinámico de las aplicaciones en todo el mundo. Azure Front Door entrega el contenido mediante la red perimetral global de Microsoft con cientos de puntos de presencia globales y locales (POP) distribuidos por todo el mundo cerca de los usuarios finales de empresa y consumidor.

Azure Front Door permite a las aplicaciones orientadas a Internet:

* **Crear y operar arquitecturas modernas de Internet** que tengan experiencias digitales dinámicas y de alta calidad con plataformas altamente automatizadas, seguras y confiables.
* **Acelerar y entregar la aplicación y el contenido globalmente** a escala a los usuarios dondequiera que estén creando oportunidades para que pueda competir, cambiar el tiempo y adaptarse rápidamente a la nueva demanda y los mercados.
* **Proteger de forma inteligente el patrimonio digital** frente a amenazas conocidas y nuevas con seguridad inteligente que adoptan un marco de confianza cero.

**Ventajas principales**

Escala de entrega global mediante la red de Microsoft

Escale horizontalmente y mejore el rendimiento de las aplicaciones y el contenido mediante la nube global CDN y WAN de Microsoft.

* Aproveche más de 118 ubicaciones perimetrales en 100 ciudades metropolitanas conectadas a Azure mediante una WAN privada de nivel empresarial y mejore la latencia de las aplicaciones hasta tres veces.
* Acelere el rendimiento de las aplicaciones mediante la difusión por proximidad de Front Door y las conexiones mediante Split TCP.
* Finalice la descarga SSL en el perímetro y use la administración de certificados integrada.
* Compatibilidad nativa con la conectividad IPv6 de un extremo a otro y el protocolo HTTP/2.

**Entrega de aplicaciones y arquitecturas modernas**

Modernización de las primeras aplicaciones de Internet en Azure con experiencias nativas en la nube

* Integración con las herramientas de línea de comandos compatibles con DevOps en los SDK de diferentes lenguajes, Bicep, plantillas de Azure Resource Manager, CLI y PowerShell.
* Definición del propio dominio personalizado con validación de dominios flexible.
* Equilibre la carga y enrute el tráfico entre orígenes y use la supervisión inteligente de sondeos de estado entre aplicaciones o contenido hospedado en Azure o en cualquier lugar.
* Integre con otros servicios de Azure, como DNS, Web Apps, Storage y muchos más para la administración de dominios y orígenes.
* Mueva la lógica de negocios de enrutamiento al borde con funcionalidades mejoradas del motor de reglas, incluidas las expresiones regulares y las variables de servidor.
* Análisis de informes integrados con un panel que integre los patrones de Front Door y de seguridad.
* Supervisión del tráfico de Front Door en tiempo real y configuración de alertas que se integran con Azure Monitor.
* Registro de cada solicitud de Front Door y de los sondeos de estado con error.

**Simple y rentable**

* Entrega estática y dinámica unificada que se ofrece en un solo nivel para acelerar y escalar la aplicación a través del almacenamiento en caché, la descarga SSL y la protección contra DDoS de nivel 3 a 4.
* Certificados SSL gratuitos administrados y con rotación automática que ahorran tiempo y protegen rápidamente las aplicaciones y el contenido.
* Precio de entrada bajo y un modelo de costos simplificado que reduce la complejidad de la facturación al tener menos medidores necesarios para planear.
* Precios de salida integrados de Azure a Front Door que quitan el cargo de salida independiente de las regiones de Azure a Azure Front Door.

**Comparación entre Azure Front Door y los servicios de Azure CDN**

Azure Front Door y Azure CDN son servicios de Azure que ofrecen entrega de contenido global con funcionalidades de enrutamiento inteligente y almacenamiento en caché en el nivel de la aplicación. Ambos servicios se pueden usar para optimizar y acelerar las aplicaciones proporcionando una red distribuida globalmente de puntos de presencia (POP) cerca de los usuarios. Ambos servicios también ofrecen una variedad de características para ayudarle a proteger las aplicaciones frente a ataques malintencionados, y a supervisar el estado y el rendimiento de la aplicación.

**Planeamiento e implementación una instancia de Web Application Firewall (WAF)**

El firewall de aplicaciones web (WAF) ofrece una protección centralizada de las aplicaciones web contra las vulnerabilidades de seguridad más habituales. Las aplicaciones web son cada vez más el objetivo de ataques malintencionados que aprovechan vulnerabilidades habitualmente conocidas. Los scripts entre sitios y las inyecciones de código SQL están dentro de los ataques más comunes.

Evitar dichos ataques en el código de la aplicación es todo un desafío. Puede requerir un mantenimiento riguroso, revisión y supervisión en varias capas de la topología de la aplicación. Un firewall de aplicaciones web centralizado ayuda a simplificar muchísimo la administración de la seguridad. Un WAF también proporciona a los administradores de la aplicación a un mejor control de la protección contra amenazas e intrusiones.

Una solución de WAF puede reaccionar más rápido ante una amenaza de la seguridad mediante la aplicación centralizada de revisiones que aborden una vulnerabilidad conocida, en lugar de proteger de manera individual cada aplicación web.

**Servicio admitido**

WAF se puede implementar con el servicio Azure Application Gateway, Azure Front Door y Azure Content Delivery Network (CDN) de Microsoft. WAF en Azure CDN se encuentra actualmente en versión preliminar pública. WAF tiene características personalizadas para cada servicio específico. Para más información sobre las características de WAF para cada servicio, consulte la introducción a cada servicio.

**Recomendar cuándo usar Azure DDoS Protection Standard**

Los ataques por denegación de servicio distribuido (DDoS) son uno de los problemas de seguridad y disponibilidad más extendidos a los que se enfrentan los clientes que mueven sus aplicaciones a la nube. Un ataque DDoS intenta agotar los recursos de una aplicación haciendo que esta no esté disponible para los usuarios legítimos. Los ataques DDoS pueden ir dirigidos a cualquier punto de conexión que sea públicamente accesible a través de Internet.

Azure DDoS Protection, junto con los procedimientos recomendados de diseño de aplicaciones, proporciona características mejoradas de mitigación DDoS para protegerse de los ataques DDoS. Se ajusta automáticamente para proteger los recursos específicos de Azure de una red virtual. La protección se puede habilitar fácilmente en cualquier red virtual nueva o existente y no requiere cambios en las aplicaciones ni los recursos.

**Azure DDoS Protection: Niveles**

**Protección de red contra DDoS**

Protección de red contra DDoS de Azure, junto con los procedimientos recomendados de diseño de aplicaciones, proporciona características mejoradas de mitigación DDoS para protegerse de los ataques DDoS. Se ajusta automáticamente para proteger los recursos específicos de Azure de una red virtual.

**Protección de IP contra DDoS**

Protección de IP contra DDoS es un modelo de IP de pago por protección. Protección de IP contra DDoS contiene las mismas características de ingeniería principales que Protección de red contra DDoS, pero variará en los siguientes servicios de valor añadido: compatibilidad con respuesta rápida de DDoS, protección de costos y descuentos en WAF.

**Azure DDoS Protection: Características clave**

* Supervisión continua del tráfico: los patrones de tráfico de la aplicación se supervisan de forma ininterrumpida en busca de indicadores de ataques DDoS. Azure DDoS Protection mitiga instantánea y automáticamente el ataque, una vez detectado.
* Optimización en tiempo real adaptable: la generación de perfiles de tráfico inteligente va conociendo con el tiempo el tráfico de la aplicación y selecciona y actualiza el perfil que resulta más adecuado para el servicio. El perfil se ajusta a medida que el tráfico cambia con el tiempo.
* Análisis, métricas y alertas de DDoS Protection: Azure DDoS Protection aplica tres políticas de mitigación autoajustadas (TCP SYN, TCP y UDP) para cada IP pública del recurso protegido en la red virtual que tiene habilitado el DDoS. Los umbrales de las directivas se configuran automáticamente con el sistema de generación de perfiles de tráfico de red basado en aprendizaje automático. La mitigación de DDoS se produce para una dirección IP que está siendo atacada solo cuando se supera el umbral de la directiva.  
  + Análisis de ataques: ofrece informes detallados en incrementos de cinco minutos durante un ataque y un resumen completo después de que el ataque termine. Transmita los registros del flujo de mitigación a Microsoft Sentinel o a un sistema de administración de eventos e información de seguridad (SIEM) sin conexión para supervisar el sistema casi en tiempo real durante un ataque. Consulte Visualización y configuración del registro de diagnóstico de DDoS para obtener más información.
  + Métricas de ataques: con Azure Monitor se puede acceder a un resumen de métricas de cada ataque. Consulte Visualización y configuración de la telemetría de protección contra DDoS para más información.
  + Alertas de ataques: las alertas se pueden configurar en el inicio y la detención de un ataque y a lo largo de la duración del ataque mediante métricas de ataque integradas. Las alertas se integran en el software operativo, como los registros de Microsoft Azure Monitor, Splunk, Azure Storage, el correo electrónico y Azure Portal. Consulte Visualización y configuración de alertas de protección contra DDoS para obtener más información.
* Respuesta rápida de Azure DDoS Protection: Durante un ataque activo, los clientes de Azure DDoS Protection tienen acceso al equipo de Respuesta rápida de DDoS (DRR), que puede ayudar con la investigación de ataques durante un ataque y con el análisis posterior al ataque. Para más información, consulte Respuesta rápida de Azure DDoS.
* Integración de plataforma nativa: integrado de forma nativa en Azure. Incluye la configuración a través de Azure Portal. Azure DDoS Protection entiende sus recursos y la configuración de los mismos.
* Protección inmediata: La configuración simplificada protege de inmediato todos los recursos de una red virtual desde el momento en que se habilita la Protección de red de DDoS. No se requiere intervención ni definición del usuario. De forma similar, la configuración simplificada protege inmediatamente un recurso de DIRECCIÓN IP pública cuando DDoS IP Protection está habilitado para él.
* Protección de varias capas: Cuando se implementa con un firewall de aplicaciones web (WAF), Azure DDoS Protection protege tanto en la capa de red (Capas 3 y 4, que ofrece Azure DDoS Protection) como en la capa de la aplicación (Capa 7, que ofrece un WAF). Entre las ofertas de WAF se incluyen la SKU de WAF de Application Gateway de Azure, y ofertas de firewall de aplicaciones web de terceros disponibles en Azure Marketplace.
* Escala de mitigación amplia: Se pueden mitigar todos los vectores de ataque L3/L4 con capacidad global para protegerse contra los ataques DDoS más conocidos.
* Garantía de costo: reciba crédito de servicio de escalabilidad horizontal de aplicaciones y transferencia de datos para los costos de recursos en los que se incurre como resultado de ataques DDoS documentados.

**Azure DDoS Protection: Arquitectura**

Azure DDoS Protection se ha diseñado para los servicios que se implementan en una red virtual. Para otros servicios, se aplica la protección contra DDoS de nivel de infraestructura predeterminada, que se defenderá frente a ataques comunes de nivel de red. Para obtener más información sobre las arquitecturas admitidas, consulte Arquitecturas de referencia de DDoS Protection.

**Precios**

En el caso de la protección de redes DDoS, bajo un inquilino, un único plan de protección DDoS puede utilizarse en varias suscripciones, por lo que no es necesario crear más de un plan de protección DDoS. Para DDoS IP Protection, no es necesario crear un plan de protección contra DDoS. Los clientes pueden habilitar Protección de IP contra DDoS en cualquier recurso de IP pública.

**Procedimientos recomendados para DDoS Protection**

Maximice la eficacia de la estrategia de protección contra DDoS siguiendo estos procedimientos recomendados:

* Diseñe las aplicaciones y la infraestructura teniendo en cuenta la redundancia y la resistencia.
* Implemente un enfoque de seguridad multicapa, incluida la red, la aplicación y la protección de datos.
* Prepare un plan de respuesta a incidentes para garantizar una respuesta coordinada a los ataques DDoS.

**Características de Azure DDoS Protection**

**Supervisión del tráfico Always On**

Azure DDoS Protection supervisa el uso de tráfico real y lo compara constantemente con los umbrales definidos en la directiva de DDoS. Cuando se supera el umbral de tráfico, se inicia automáticamente la mitigación de DDoS. Cuando el tráfico vuelve a estar por debajo del umbral, se detiene la mitigación.

Durante la mitigación, el servicio Protección contra DDoS redirige el tráfico enviado al recurso protegido y realiza varias comprobaciones, por ejemplo:

* Asegurarse de que los paquetes se ajustan a las especificaciones de Internet y no tienen un formato incorrecto.
* Interactúe con el cliente para determinar si el tráfico es un posible paquete falsificado (por ejemplo, Autorización de SYN o Cookie de SYN o colocando un paquete para que el origen lo retransmita).
* Limitar la velocidad de los paquetes si no se puede realizar ningún otro método de cumplimiento.

Azure DDoS Protection anula el tráfico del ataque y reenvía el tráfico restante al destino previsto. En un intervalo de pocos minutos tras la detección del ataque, recibe una notificación mediante las métricas de Azure Monitor. Si configura el registro de datos de telemetría de DDoS Protection, puede escribir los registros en opciones disponibles para su análisis posterior. Los datos métricos de Azure Monitor para DDoS Protection se conservan actualmente durante 30 días.

**Ajuste adaptable en tiempo real**

La complejidad de los ataques (por ejemplo, ataques DDoS multivector), así como los comportamientos de los inquilinos, específicos de cada aplicación, hacen necesarias directivas de protección personalizadas para cada cliente.

El servicio lo lleva a cabo mediante el uso de dos tipos de información:

* Aprendizaje automático de los patrones de tráfico de las capas 3 y 4 de cada cliente (por dirección IP pública).
* Reducción de los falsos positivos ya que el escalado de Azure le permite absorber una cantidad importante de tráfico.

**Directivas de mitigación de Azure DDoS Protection**

En Azure Portal, seleccione Supervisar > Métricas. En el panel Métricas, seleccione el grupo de recursos, un tipo de recurso de Dirección IP pública y la dirección IP pública de Azure. Las métricas de DDoS estarán visibles en el panel Métricas disponibles.

DDoS Protection aplica tres directivas de mitigación autoajustadas (TCP SYN, TCP y UDP) para cada IP pública del recurso protegido, en la red virtual que tiene habilitado DDoS. Para ver los umbrales de la directiva, seleccione la métrica "Inbound packets to trigger DDoS mitigation" (Paquetes de entrada para desencadenar la mitigación de DDoS).

Los umbrales de las directivas se configuran automáticamente con el sistema de generación de perfiles de tráfico de red basado en aprendizaje automático. La mitigación de DDoS se produce para una dirección IP que está siendo atacada solo cuando se supera el umbral de la directiva.

**Métricas de una dirección IP sometida a un ataque de DDoS**

Si la dirección IP pública está siendo atacada, el valor de la métrica Under DDoS attack or not (Bajo ataque de DDoS o no) cambia a 1 cuando aplicamos la mitigación al tráfico de ataque.

Se recomienda configurar una alerta en esta métrica. Si lo hace, recibirá una notificación cuando se esté aplicando una mitigación de DDoS en su dirección IP pública.

**Firewall de aplicaciones web para ataques a recursos**

En el caso de los ataques a recursos en el nivel de aplicación, los clientes deben configurar un firewall de aplicaciones web (WAF) para ayudar a proteger las aplicaciones web. Un WAF inspecciona el tráfico web entrante para bloquear las inyecciones de SQL, los scripts entre sitios, DDoS y otros ataques al nivel 7. Azure ofrece WAF como una característica de Application Gateway para ofrecer una protección centralizada de las aplicaciones web contra las vulnerabilidades de seguridad comunes. En Azure Marketplace encontrará ofertas de WAF de asociados de Azure que podrían ser más adecuadas para sus necesidades.

Incluso los firewalls de aplicaciones web son susceptibles de sufrir ataques de agotamiento del estado y volumétricos. Es muy recomendable activar DDoS Protection en la red virtual del WAF para impedir los ataques a protocolos y volumétricos.

**Planeamiento de la protección**

El planeamiento y la preparación son cruciales para entender cómo se comportará un sistema durante un ataque de DDoS. Diseñar un plan de respuesta de administración de incidentes forma parte de este esfuerzo.

Si dispone de DDoS Protection, asegúrese de que esté habilitado en la red virtual de los puntos de conexión accesibles desde Internet. La configuración de alertas de DDoS le ayuda a vigilar constantemente los posibles ataques contra su infraestructura.

Supervise las aplicaciones de forma independiente. Debe conocer el comportamiento normal de una aplicación. Debe estar preparado para actuar si la aplicación no se comporta como está previsto durante un ataque de DDoS.

**Prueba de conocimientos**

Elija la mejor respuesta para cada una de las preguntas. Después, seleccione **Comprobar las respuestas**.

**Comprobación de conocimientos**

Principio del formulario

**1. ¿Cuál es el propósito principal de Azure Front Door?**

1. Permite la automatización y la validación de la creación y el desmontaje de entornos para contribuir a ofrecer plataformas de hospedaje de aplicaciones seguras y estables
2. Un servicio de base de datos basado en la nube que permite la creación, administración y escalado de bases de datos NoSQL
3. Proporciona acceso rápido, confiable y seguro entre los usuarios y el contenido web estático y dinámico de las aplicaciones en todo el mundo

**2. ¿Qué hace Azure DDoS Protection para proporcionar directivas de protección adaptadas para cada cliente?**

1. Aplica las mismas directivas de mitigación para todos los clientes.
2. Se basa en los clientes para configurar sus propias directivas de protección.
3. Aprende automáticamente los patrones de tráfico de IP pública por cliente para las capas 3 y 4.

**3. Un especialista en seguridad debe asegurarse de que los recursos de Azure estén protegidos contra amenazas al tiempo que mantienen un alto rendimiento. ¿Cuál de las siguientes opciones permite la automatización y validación de la creación y desmontaje de entornos para contribuir a ofrecer plataformas de hospedaje de aplicaciones seguras y estables?**

1. Azure Front Door
2. Azure Firewall Manager
3. Azure DevOps

**4. Una empresa quiere garantizar la seguridad de sus aplicaciones web frente a vulnerabilidades de seguridad comunes. ¿Cuál de las siguientes soluciones podría ayudarles a lograr esto?**

1. Protección de cada aplicación web individual por separado
2. Implementación de varias capas de seguridad en el código de la aplicación
3. Implementación de un firewall de aplicaciones web (WAF) centralizado

**5. Una empresa desea asegurar la automatización y validación de la creación y desmontaje de entornos para contribuir a ofrecer plataformas de hospedaje de aplicaciones seguras y estables. ¿Cuál de las siguientes opciones habilitaría esto?**

1. Usar una herramienta diferente que no admita la automatización
2. Usar un proceso manual para crear y desmontar entornos
3. Usar una infraestructura como herramienta de código para automatizar la creación y desmontaje de entornos
4. C
5. C
6. C
7. C
8. C

Final del formulario

**Resumen**

En este módulo, ha aprendido a planear e implementar medidas de seguridad sólidas para el acceso público a los recursos de Azure, incluido el uso de seguridad de la capa de transporte (TLS) para aplicaciones, la implementación y administración de Azure Firewall con Azure Firewall Manager y las directivas de firewall, la configuración de Azure Application Gateway y Azure Front Door con Content Delivery Network (CDN) para mejorar el rendimiento y la seguridad de las aplicaciones, configurar un firewall de aplicaciones web (WAF) para la protección contra ataques basados en web y realizar recomendaciones informadas sobre cuándo usar Azure DDoS Protection Estándar para defenderse contra ataques de denegación de servicio distribuidos (DDoS).