**Introducción**

Azure Application Gateway es un equilibrador de carga para el tráfico web. Los administradores implementan una puerta de enlace de aplicaciones para administrar el tráfico a sus aplicaciones web.

Suponga que trabaja para el departamento de vehículos motorizados de una organización gubernamental. El departamento cuenta con varios sitios web públicos que permiten a los conductores registrar sus vehículos y renovar sus permisos en línea. El sitio web de registro de vehículos se ha estado ejecutando en un único servidor y ha sufrido varias interrupciones debido a errores del servidor. Las interrupciones han provocado la frustración de los conductores que intentan registrar sus vehículos antes de que expiren sus registros.

Usted es la persona responsable de mejorar la resistencia del sitio agregando varios servidores web para distribuir la carga. Querrá centralizar el sitio en un servicio de equilibrio de carga único y simplificar las direcciones URL para los visitantes del sitio. Está investigando cómo implementar Azure Application Gateway.

**Objetivos de aprendizaje**

En este módulo aprenderá a:

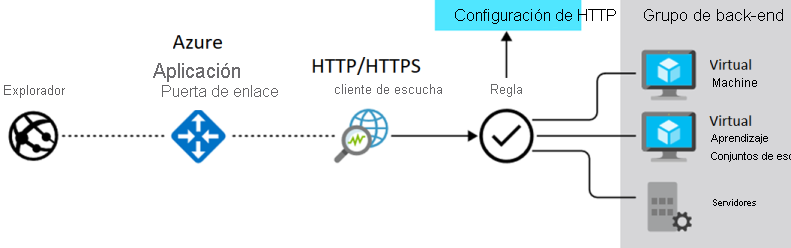
* Identificar las características y los casos de uso de Azure Application Gateway.
* Implementar una puerta de enlace de aplicación de Azure, incluida la selección de un método de enrutamiento.
* Configurar componentes de puerta de enlace, como clientes de escucha, sondeos de estado y reglas de enrutamiento.

**Implementación de Azure Application Gateway**

Los administradores usan Azure Application Gateway para administrar solicitudes de aplicaciones cliente a sus aplicaciones web. Una puerta de enlace de aplicaciones escucha el tráfico entrante a las aplicaciones web y comprueba si hay mensajes enviados a través de protocolos como HTTP. Las reglas de puerta de enlace dirigen el tráfico a los recursos de un grupo de back-end.

**Escenario empresarial**

Considere un escenario en el que las aplicaciones cliente de Internet solicitan acceso a los recursos de un grupo de back-end con equilibrio de carga. Las solicitudes se pueden administrar mediante la implementación de Azure Application Gateway para escuchar mensajes HTTP(S). Las reglas de equilibrio de carga pueden controlar los mensajes para dirigir el tráfico de solicitudes de cliente a los recursos adecuados del grupo. En el siguiente diagrama, se ilustra este escenario:



**Aspectos que debe saber sobre Azure Application Gateway**

Vamos a examinar algunas de las ventajas de usar Azure Application Gateway para administrar el tráfico de Internet a las aplicaciones web.

| **Prestación** | **Descripción** |
| --- | --- |
| **Enrutamiento de la capa de aplicación** | Use el enrutamiento de la capa de aplicación para dirigir el tráfico a un grupo back-end de servidores web a partir de la dirección URL de una solicitud. El grupo back-end puede estar compuesto de máquinas virtuales de Azure, Azure Virtual Machine Scale Sets, Azure App Service e incluso servidores locales. |
| **Flujo de equilibrio de carga round robin** | Utilice el equilibrio de carga round robin para distribuir el tráfico entrante entre varios servidores. Envíe solicitudes de equilibrio de carga a los servidores de cada grupo back-end. Las solicitudes de cliente se reenvían en un ciclo a través de un grupo de servidores para crear un equilibrio eficaz para la carga del servidor. |
| **Permanencia de sesión** | Aplique la permanencia de sesión a la puerta de enlace de aplicación para garantizar que las solicitudes de cliente de una misma sesión se enrutan al mismo servidor back-end. |
| **Protocolos admitidos** | Cree una puerta de enlace de aplicación para admitir los protocolos HTTP, HTTPS, HTTP/2 o WebSocket. |
| **Protección por firewall** | Implemente un firewall de aplicaciones web para protegerse frente a vulnerabilidades de aplicaciones web. |
| **Cifrado** | Admita el cifrado de solicitudes de un extremo a otro para las aplicaciones web. |
| **Escalado automático de carga** | Ajuste dinámicamente la capacidad a medida que cambia la carga del tráfico web. |

**Determinación del enrutamiento de Azure Application Gateway**

Los clientes envían solicitudes a las aplicaciones web especificando la dirección IP o el nombre DNS de la puerta de enlace de aplicación. La puerta de enlace dirige las solicitudes a un servidor web seleccionado en el grupo de back-end según un conjunto de reglas. Se definen las reglas de la puerta de enlace para identificar las rutas permitidas para el tráfico de solicitud.

**Cosas que debe saber sobre el enrutamiento del tráfico**

Echemos un vistazo más de cerca a las opciones de enrutamiento para Azure Application Gateway.

* Azure Application Gateway ofrece dos métodos principales para enrutar el tráfico:
  + El **enrutamiento basado en rutas de acceso** envía solicitudes con distintas rutas de acceso de URL a distintos grupos de servidores back-end.
  + El **enrutamiento multisitio** configura más de una aplicación web en la misma instancia de Application Gateway.
* Puede configurar la puerta de enlace de aplicación para **redirigir** el tráfico.

Application Gateway puede redirigir el tráfico recibido en un cliente de escucha a otro cliente de escucha o a un sitio externo. Las aplicaciones web suelen usar este enfoque para redirigir automáticamente las solicitudes HTTP para comunicarse a través de HTTPS. El redireccionamiento garantiza que toda la comunicación entre la aplicación web y los clientes se produzca a través de una ruta de acceso cifrada.

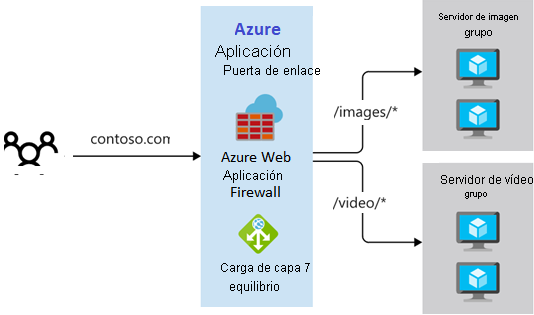
* Puede implementar Application Gateway para **reescribir encabezados HTTP**.

Los encabezados HTTP permiten que el cliente y el servidor pasen información de parámetros con la solicitud o la respuesta. En este escenario, puede traducir las direcciones URL o los parámetros de cadenas de consulta y de modificar los encabezados de solicitud y respuesta. Agregue condiciones para asegurarse de que las direcciones URL o los encabezados solo se reescribirán para determinadas condiciones.

* Application Gateway permite crear páginas de error personalizadas, en lugar de mostrar las páginas de error predeterminadas. Puede usar su propia marca y diseño utilizando una página de error personalizada.

**Enrutamiento basado en ruta de acceso**

Puede implementar el enrutamiento basado en rutas de acceso para dirigir las solicitudes para rutas de acceso de dirección URL específicas al grupo de back-end adecuado. Considere un escenario en el que la aplicación web recibe solicitudes para vídeos o imágenes. Puede usar el enrutamiento basado en rutas de acceso para dirigir las solicitudes para la ruta de acceso /video/\\* a un grupo de servidores back-end optimizados para controlar el streaming de vídeo. Las solicitudes de imagen de la ruta de acceso /images/\\* se pueden dirigir a un grupo de servidores que controlan la recuperación de imágenes. En la ilustración siguiente se muestra este método de enrutamiento:

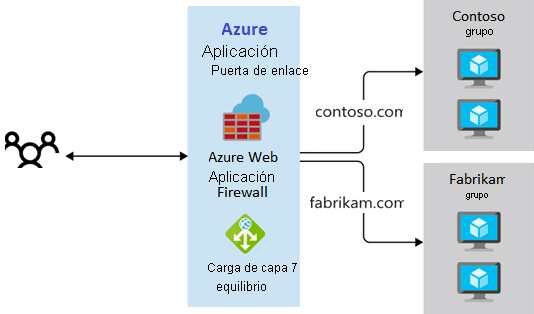


**Enrutamiento multisitio**

Si necesita admitir varias aplicaciones web en la misma instancia de puerta de enlace de aplicación, el enrutamiento multisitio es la mejor opción. Las configuraciones de varios sitios son útiles para admitir aplicaciones de varios inquilinos, donde cada inquilino tiene su propio conjunto de máquinas virtuales u otros recursos que hospedan una aplicación web.

En esta configuración, hay que registrar varios nombres de DNS (CNAME) para la dirección IP de la puerta de enlace de aplicación y especificar el nombre de cada sitio. Application Gateway usa agentes de escucha independientes para esperar por las solicitudes de cada sitio. Cada agente de escucha pasa la solicitud a otra regla, que puede enrutar las solicitudes a servidores en otro grupo de servidores back-end.

Considere un escenario en el que necesita admitir el tráfico a dos sitios en la misma puerta de enlace. Puede dirigir todas las solicitudes del sitio http://contoso.com a los servidores de un grupo back-end y las solicitudes del sitio http://fabrikam.com a otro grupo de back-end. En la ilustración siguiente se muestra este método de enrutamiento.



**Configuración de componentes de Azure Application Gateway**

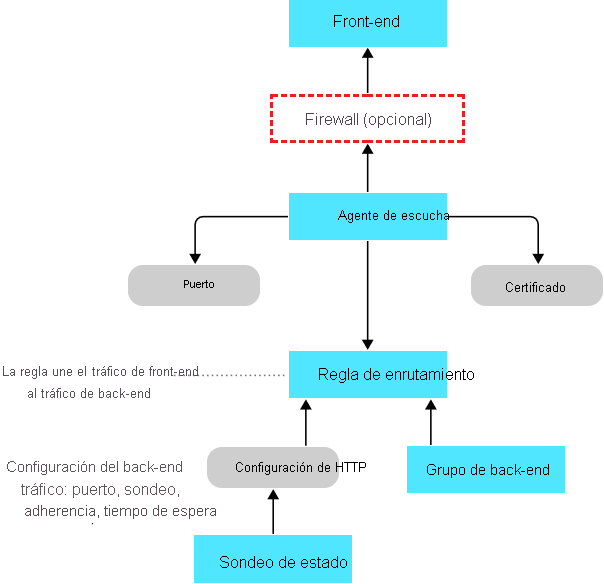
Azure Application Gateway tiene una serie de componentes que se combinan para enrutar las solicitudes a un grupo de servidores web y para comprobar el estado de dichos servidores web. Estos componentes incluyen la dirección IP de front-end, los grupos de back-end, las reglas de enrutamiento, los sondeos de estado y los clientes de escucha. Como opción, la puerta de enlace también puede implementar un firewall.

**Aspectos que se deben saber sobre los componentes de Application Gateway**

Vamos a explorar cómo funcionan conjuntamente los componentes de una puerta de enlace de aplicaciones.

* La **dirección IP de front-end** recibe las solicitudes del cliente.
* Un **firewall** opcional comprueba el tráfico entrante en busca de amenazas comunes antes de que las solicitudes lleguen a los clientes de escucha.
* Uno o varios **clientes de escucha** reciben el tráfico y enrutan las solicitudes al grupo de back-end.
* Las **reglas de enrutamiento** definen cómo analizar la solicitud para dirigirla al grupo de back-end adecuado.
* Un **grupo de back-end** contiene servidores web para recursos como máquinas virtuales o Virtual Machine Scale Sets. Cada grupo tiene un equilibrador de carga para distribuir la carga de trabajo entre los recursos.
* Los **sondeos de estado** determinan qué servidores del grupo de back-end están disponibles para el equilibrio de carga.

En el diagrama de flujo siguiente se muestra cómo funcionan conjuntamente los componentes de Application Gateway para dirigir las solicitudes de tráfico entre los grupos de servidores front-end y back-end de la configuración.



**Dirección IP de front-end**

Las solicitudes de cliente se reciben a través de una dirección IP de front-end. La puerta de enlace de aplicaciones puede tener una dirección IP pública o privada, o ambas. Solo puede tener una dirección IP pública y una dirección IP privada.

**Agentes de escucha**

Los clientes de escucha aceptan el tráfico que llega a una combinación especificada de protocolo, puerto, host y dirección IP. Cada cliente de escucha enruta las solicitudes a un grupo de back-end según las reglas de enrutamiento. Un agente de escucha puede ser *básico* o *multisitio*. Un agente de escucha básico solo enruta una solicitud según la ruta de acceso de la dirección URL. Un cliente de escucha multisitio también puede enrutar las solicitudes mediante el elemento de nombre de host de la dirección URL. Los agentes de escucha también controlan los certificados TLS/SSL para proteger la aplicación entre el usuario y Application Gateway.

**Reglas de enrutamiento**

Una regla de enrutamiento enlaza los clientes de escucha a los grupos de back-end. Una regla especifica cómo interpretar los elementos de nombre de host y ruta de la dirección URL de una solicitud y, después, dirigir la solicitud al grupo de servidores back-end adecuado. Una regla de enrutamiento también tiene un conjunto de configuración de HTTP asociado. Estas configuraciones de HTTP indican si se cifra el tráfico entre Application Gateway y los servidores back-end y cómo hacerlo. Entre las otras informaciones de configuración se incluye el protocolo, la permanencia de sesión, el drenaje de conexiones, el período de tiempo de espera de una solicitud y los sondeos de estado.

**Grupos de servidores back-end**

Un grupo de servidores back-end hace referencia a una colección de servidores web. Al configurar el grupo, proporciona la dirección IP de cada servidor web y el puerto en el que escucha las solicitudes. Cada grupo puede especificar un conjunto fijo de máquinas virtuales, Virtual Machine Scale Sets, una aplicación hospedada por Azure App Services o una colección de servidores locales. Cada grupo de servidores back-end tiene un equilibrador de carga asociado que distribuye el trabajo en el grupo.

**Sondeos de estado**

Los sondeos de estado determinan qué servidores del grupo de back-end están disponibles para el equilibrio de carga. Application Gateway usa un sondeo de estado para enviar una solicitud a un servidor. Cuando el servidor devuelve una respuesta HTTP con un código de estado entre 200 y 399, se considera que el servidor está en buen estado. Si no configura un sondeo de estado, Application Gateway crea un sondeo predeterminado que espera 30 segundos antes de identificar un servidor como no disponible (incorrecto).

**Firewall (opcional)**

Puede habilitar Azure Web Application Firewall para que Azure Application Gateway controle las solicitudes entrantes antes de que lleguen al cliente de escucha. El firewall comprueba cada solicitud en busca de riesgos según Open Web Application Security Project (OWASP). Entre las amenazas comunes se incluyen la inyección de código SQL, scripting entre sitios, la inserción de comandos, el contrabando de solicitudes HTTP y la división de respuestas y la inclusión remota de archivos. Otras amenazas pueden provenir de bots, rastreadores, escáneres e infracciones y anomalías del protocolo HTTP.

OWASP define un conjunto de reglas genéricas para detectar ataques. Estas reglas se conocen como Core Rule Set (CRS). Los conjuntos de reglas están en continua revisión, puesto que los ataques son cada vez más sofisticados. Azure Web Application Firewall admite dos conjuntos de reglas: CRS 2.2.9 y CRS 3.0. CRS 3.0 es el valor predeterminado y más reciente de estos conjuntos de reglas. Si es necesario, puede optar por seleccionar únicamente determinadas reglas en un conjunto de reglas para atacar determinadas amenazas. Además, puede personalizar el firewall para que especifique qué elementos de una solicitud debe examinar y limitar el tamaño de los mensajes para evitar que cargas masivas sobrecarguen los servidores.

**Comprobación de conocimiento**

El departamento de TI agrega varios servidores web para distribuir la carga en el sitio web de registro del departamento de vehículos motorizados. Está trabajando en el plan de configuración para centralizar el sitio mediante Azure Application Gateway. Algunos equipos han enviado sus requisitos de configuración y sus preguntas para que los evalúe:

* El equipo web está instalando la puerta de enlace de aplicación. Quieren asegurarse de que las solicitudes entrantes se comprueban para ver si contienen amenazas habituales relacionadas con la seguridad, como los scripts entre sitios y los rastreadores.
* El equipo del servidor ha solicitado información sobre cómo Application Gateway enruta las solicitudes a los servidores web.
* Debe presentar una comparación de alto nivel de las estrategias de equilibrio de carga al comité ejecutivo.

**Responda a las siguientes preguntas**

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

Principio del formulario

**1. ¿Qué criterios utiliza Azure Application Gateway para enrutar las solicitudes a un servidor web?**

1. La región donde se encuentran los servidores que hospedan la aplicación web.
2. Nombre de host, puerto y ruta en la dirección URL de la solicitud.
3. Información de autenticación de los usuarios.

**2. ¿Qué estrategia de equilibrio de carga implementa Azure Application Gateway?**

1. Las solicitudes se distribuyen al servidor del grupo back-end que tiene la carga más ligera.
2. Cada servidor del grupo de back-end se sondea a su vez y la solicitud se envía al primer servidor que responde.
3. A su vez, las solicitudes se distribuyen a cada servidor disponible en un grupo de back-end a través de una técnica round robin.

**3. ¿Cómo se pueden abordar las preocupaciones sobre las amenazas de seguridad?**

1. Instale Azure Web Application Firewall.
2. Instalación de un equilibrador de carga interno
3. Instale Azure Firewall.

Final del formulario

* 1. B
  2. C
  3. A

**Resumen y recursos**

Azure Application Gateway proporciona funcionalidades de equilibrio de carga y enrutamiento de aplicaciones en varios sitios web. Hay varios métodos de enrutamiento disponibles, incluido el de multisitio y basado en rutas de acceso. Application Gateway también proporciona Azure Web Application Firewall para proporcionar características de seguridad integradas.

En este módulo, ha identificado las características y los casos de uso de Azure Application Gateway. Ha explorado los componentes de Application Gateway, incluidos los clientes de escucha, firewalls, sondeos de estado y reglas de enrutamiento. Ha aprendido a implementar una puerta de enlace de aplicaciones, incluida la selección del método de enrutamiento adecuado.