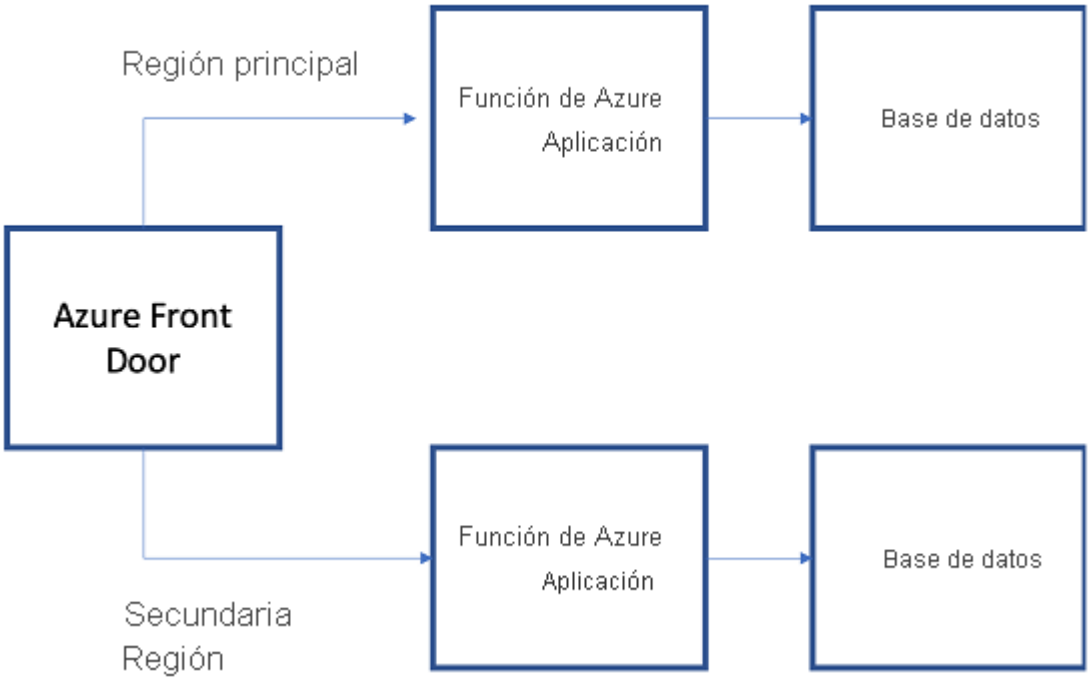
**Configuración y administración de Azure Front Door**

Azure Front Door permite definir, administrar y supervisar el enrutamiento global para el tráfico web mediante la optimización para obtener el mejor rendimiento y la conmutación por error global instantánea para alta disponibilidad. Con Front Door, las aplicaciones empresariales y de consumidor globales (de varias regiones) se pueden transformar en aplicaciones modernas personalizadas, sólidas y de alto rendimiento, API y contenido que lleguen a un público global mediante Azure.

Front Door opera en la capa 7 o en la capa HTTP/HTTPS y usa el **protocolo de difusión por proximidad basado en TCP dividido**. Front Door garantiza que los usuarios finales se conecten rápidamente al POP (punto de presencia) de Front Door más cercano. Por tanto, según la selección del método de enrutamiento en la configuración, puede asegurarse de que Front Door enruta las solicitudes de cliente al back-end de aplicación más rápido y disponible. Un back-end de aplicación es cualquier servicio accesible desde Internet hospedado dentro o fuera de Azure. Front Door proporciona una serie de métodos de enrutamiento del tráfico y opciones de seguimiento de estado del back-end para satisfacer las distintas necesidades de las aplicaciones y los modelos de conmutación automática por error. Al igual que Traffic Manager, Front Door es resistente a errores, incluidos los que afectan a una región completa de Azure.




Las características siguientes se incluyen con Front Door:

- **Aceleración del rendimiento de la aplicación**: al usar el protocolo de difusión por proximidad basado en TCP, Front Door garantiza que sus usuarios finales se conecten rápidamente al POP (punto de presencia) de Front Door más cercano.
- **Aumento de la disponibilidad de las aplicaciones con sondeos de estado inteligentes**: Front Door ofrece una alta disponibilidad para sus aplicaciones críticas mediante los

sondeos de estado inteligentes, la supervisión de sus back-end tanto en latencia como en disponibilidad y la oferta de una conmutación automática por error cuando un back-end se queda sin servicio.

- **Enrutamiento basado en URL**: el enrutamiento basado en la ruta de la URL le permite enrutar el tráfico a los grupos de back-end en función de las rutas de la URL de la solicitud. Uno de los escenarios es el enrutamiento de solicitudes de diferentes tipos de contenido a diferentes grupos de back-end.
- **Hospedaje de varios sitios**: el hospedaje de varios sitios le permite configurar más de un sitio web en la misma configuración de Front Door.
- **Afinidad de sesión**: la característica de afinidad de sesión basada en cookies es útil cuando se desea mantener una sesión de usuario en el mismo back-end de aplicación.
- **Terminación de Seguridad de la capa de transporte (TLS)**: Front Door admite la terminación TLS en el perímetro; es decir, los usuarios individuales pueden configurar una conexión TLS con entornos de Front Door en lugar de establecerla a través de conexiones de largo recorrido con el back-end de la aplicación.
- **Dominios personalizados y administración de certificados**: cuando se utiliza Front Door para distribuir contenido, es necesario un dominio personalizado si desea que el nombre de su propio dominio sea visible en la URL de Front Door.
- **Seguridad de la capa de aplicación**: Azure Front Door le permite crear reglas personalizadas de Web Application Firewall (WAF) para el control de acceso con el fin de proteger su carga de trabajo HTTP/HTTPS frente a la explotación basada en las direcciones IP de los clientes, el código de país y los parámetros HTTP.
- **Redireccionamiento de URL**: con el fuerte empuje de la industria para admitir solo la comunicación segura, se espera que las aplicaciones web redirijan automáticamente cualquier tráfico HTTP a HTTPS.
- **Reescritura de URL**: Front Door admite la reescritura de URL permitiendo configurar una ruta de acceso de reenvío personalizada opcional que se usará cuando al construir la solicitud para reenviar al back-end.
- **Compatibilidad con protocolos: tráfico IPv6 y HTTP/2**: Azure Front Door admite de forma nativa la conectividad IPv6 de un extremo a otro y el protocolo HTTP/2.

Como se mencionó anteriormente, el enrutamiento a los entornos de Azure Front Door aprovecha la difusión por proximidad para el tráfico DNS (sistema de nombres de dominio) y HTTP (protocolo de transferencia de hipertexto), por lo que el tráfico del usuario irá al entorno más cercano en términos de topología de red (pocos saltos). Normalmente, esta arquitectura ofrece mejores tiempos de ida y vuelta para los usuarios finales (maximiza las ventajas de la División TCP). Front Door organiza sus entornos en "anillos" principales y de reserva. El anillo exterior tiene entornos que están más próximos a los usuarios, ofreciendo latencias más bajas. El anillo interior tiene entornos que pueden controlar la conmutación por error para el entorno del anillo exterior en caso de que se produzca un problema. El anillo exterior es el destino preferido para todo el tráfico,

pero el anillo interior es necesario para controlar el desbordamiento de tráfico desde el anillo exterior. En términos de direcciones VIP (direcciones del protocolo de Internet virtual), se asigna una dirección VIP principal a cada host de front-end o dominio servido por Front Door, que los entornos anuncian en el anillo interior y exterior, así como una dirección VIP de reserva, que los entornos solo anuncian en el anillo interior.

Esta estrategia garantiza que las solicitudes de los usuarios finales siempre alcanzan el entorno de Front Door más cercano y que incluso si el entorno de Front Door preferido es incorrecto, el tráfico pasa automáticamente al siguiente entorno más cercano.

---