Protección de redes virtuales mediante el uso de Azure Firewall

100 XP

5 minutos

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

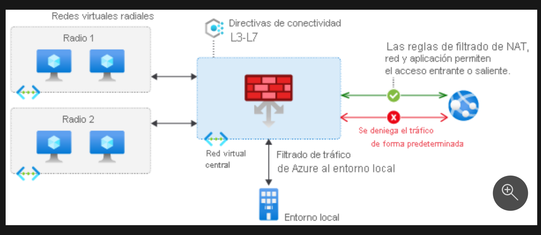
En la actualidad, Tailwind Traders ejecuta dispositivos de firewall, que combinan hardware y software, para proteger su red local. Para funcionar, estos dispositivos de firewall necesitan una cuota de licencia mensual, y que el personal de TI realice un mantenimiento rutinario. A medida que Tailwind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

En esta parte, explorará Azure Firewall.

¿Qué es Azure Firewall?

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

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



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

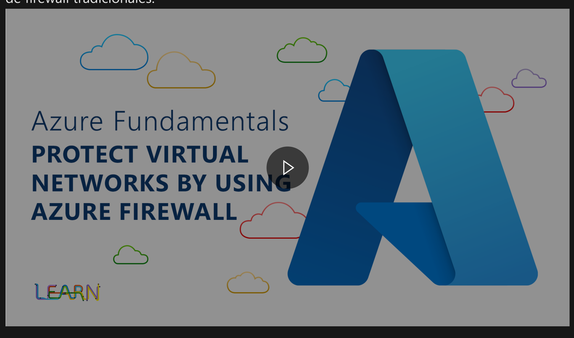
Azure Firewall proporciona una ubicación central para crear, aplicar y registrar directivas de conectividad de red y de aplicaciones entre suscripciones y redes virtuales. Azure Firewall usa una dirección IP pública estática (invariable) para los recursos de redes virtuales, lo que permite que los firewall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

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

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

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

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



¿Qué se puede configurar con Azure Firewall?

Con Azure Firewall, puede configurar:

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

Azure Application Gateway también proporciona un firewall, denominado *firewall de aplicaciones web* (WAF). El firewall de aplicaciones web proporciona protección entrante centralizada para las aplicaciones web contra vulnerabilidades de seguridad comunes. Azure Front Door y Azure Content Delivery Network también proporcionan servicios de firewall de aplicaciones web.

Siguiente unidad: Protección contra ataques de DDoS mediante el uso de Azure DDoS Protection

Continuar