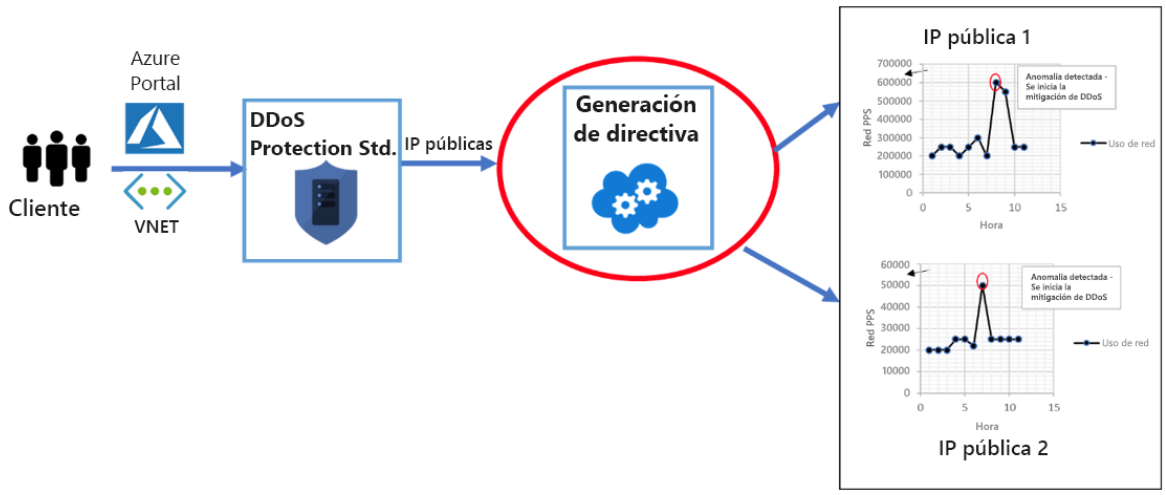
Configuración de una implementación de protección de denegación de servicio distribuido

La protección contra la denegación de servicio distribuido (DDoS) de Azure en conjunto con los procedimientos recomendados para el diseño de aplicaciones proporcionan defensa frente a ataques DDoS. La protección contra DDoS de Azure proporciona los siguientes niveles de servicio:

- **Básico**: habilitado de forma automática como parte de la plataforma de Azure. La supervisión continua del tráfico y la reducción en tiempo real de los ataques a nivel de red más comunes ofrecen la misma defensa que usan los servicios en línea de Microsoft. Puede usarse la escala completa de una red global de Azure para distribuir y reducir el tráfico de ataques en las distintas regiones. Se proporciona protección para direcciones IP públicas de Azure IPv4 e IPv6.
- **Estándar**: ofrece funciones adicionales de reducción de ataques en comparación con el nivel de servicio básico, adaptadas específicamente a los recursos de Azure Virtual Network. El servicio Protección contra DDoS estándar es fácil de habilitar y no requiere ningún cambio en la aplicación. Las directivas de protección se ajustan a través de la supervisión del tráfico dedicado y los algoritmos de Machine Learning. Las directivas se aplican a direcciones IP públicas asociadas a recursos implementados en redes virtuales, como instancias de Azure Load Balancer, Azure Application Gateway y Azure Service Fabric, pero esta protección no se aplica a las instancias de App Service Environment. La telemetría en tiempo real está disponible a través de las vistas de Azure Monitor durante un ataque y para el historial. En la configuración de diagnóstico, hay disponibles análisis avanzados de mitigación de ataques. La protección del nivel de aplicación se puede agregar mediante el firewall de aplicaciones web de Azure Application Gateway Web o instalando un firewall de terceros desde Azure Marketplace. Se proporciona protección para direcciones IP públicas de Azure IPv4 e IPv6.

Funcionamiento de la protección contra denegación de servicio de Azure

DDoS Protection Estándar supervisa el uso real del tráfico 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 un nivel por debajo del umbral, se quita la mitigación.



Durante la mitigación, DDoS Protection redirige el tráfico enviado al recurso protegido y realiza varias comprobaciones, entre las que se incluyen:

- Ayudar a garantizar que los paquetes cumplen con las especificaciones de Internet y no tienen un formato incorrecto.
- Interactuar con el cliente a fin de determinar si el tráfico puede ser un paquete suplantado electrónicamente (por ejemplo, mediante el uso de SYN Auth o SYN Cookie, bien quitando un paquete para que el origen vuelva a transmitirlo).
- Si no puede aplicar ningún otro método de cumplimiento, usar paquetes con límite de frecuencia.

DDoS Protection bloquea el tráfico de ataque y reenvía el tráfico restante al destino previsto. En un intervalo de pocos minutos tras la detección del ataque, recibirá una notificación mediante las métricas de Azure Monitor. Si configura el registro de datos de telemetría de Protección contra DDoS estándar, puede escribir los registros en opciones disponibles para su posterior análisis. Azure Monitor conserva los datos de métricas para DDoS Protection Estándar durante 30 días.

Tipos de ataques por denegación de servicio que mitiga la protección de Azure

El servicio Protección contra DDoS estándar puede mitigar los tipos de ataque siguientes:

- **Ataques volumétricos**: el objetivo del ataque es desbordar la capa de la red con una gran cantidad de tráfico aparentemente legítimo. Esto incluye ataques de tipo "flood" de UDP, de amplificación y otros ataques de tipo "flood" de paquetes falsificados. DDoS Protection Standard mitiga estos posibles ataques de varios gigabytes, ya que los absorbe y los limpia automáticamente aprovechando la escala de red global de Azure.
- **Ataques a protocolos**: estos ataques representan un destino inaccesible al aprovechar una vulnerabilidad en la pila de protocolo en los niveles 3 y 4. Esto incluye ataques de tipo “flood” de SYN, ataques de reflejo y otros ataques de protocolo. El servicio Protección contra DDoS estándar mitiga estos ataques al diferenciar entre el tráfico malintencionado y el legítimo. Para ello, interactúa con el cliente y bloquea el tráfico malintencionado.

- **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. Los ataques incluyen infracciones de protocolo HTTP, inyección de código SQL, scripts de sitios y otros ataques de nivel 7. Use un firewall de aplicaciones web, por ejemplo el firewall de aplicaciones web de Azure Application Gateway, así como DDoS Protection Standard, para la defensa frente a estos ataques. También existen ofertas de firewall de aplicaciones web de terceros disponibles en Azure Marketplace.