Argo Tunnel

Protege los servidores web de ataques directos en el origen

Los agentes maliciosos avanzados pueden eludir la protección de seguridad basada en la nube descubriendo y atacando direcciones IP de origen y puertos abiertos.

Los enfoques comunes para proteger los servidores web del ataque directo incluyen la creación de listas de control de acceso (ACL) y listas blancas de direcciones IP entrantes o el establecimiento de un túnel GRE. Estos enfoques son engorrosos de configurar y mantener, carecen de cifrado integrado y pueden introducir una latencia adicional y tarifas costosas.

Utilizando un daemon ligero instalado en la infraestructura de origen, Cloudflare crea un túnel cifrado entre el centro de datos y origen de Cloudflare más cercano sin mantener abiertos los puertos entrantes públicos.

Como resultado, los ataques DDoS volumétricos en los puertos HTTP/S no pueden sobrecargar directamente los servidores web. Los intentos de violaciones de datos, como los ataques mediante fuerza bruta, pueden detectarse y bloquearse, ya que se fuerza al tráfico a pasar por las proxies de Cloudflare.

PROTEGE LOS SERVIDORES WEB DE LOS ATAQUES DIRECTOS

Después de implementar Argo Tunnel y cerrar los puertos, solo el tráfico web que fluye a través de los servicios de seguridad de Cloudflare y un túnel cifrado seguro puede llegar al origen.

Los intentos de DDoS y violación de datos ya no pueden llegar directamente a los servidores web de origen a través de sus direcciones IP públicas.

ACCESO EXTERNO SEGURO A APLICACIONES INTERNAS

Argo Tunnel protege las aplicaciones internas orientadas a Internet (incluidas las puestas en escena) obligado a todo el tráfico a enrutarse a través de la red de Cloudflare.

Cuando Argo Tunnel se combina con Cloudflare Access, los usuarios se autentican con un proveedor de identidad importante sin un VPN.

Las aplicaciones antes accesibles para cualquiera a través de la IP de origen, ahora requieren una autenticación de usuario.

ACELERA EL TRÁFICO DE ORIGEN CON SMART ROUTING

Argo Tunnel requiere habilitar Argo Smart Routing.

Argo Smart Routing mejora el rendimiento al enrutar los visitantes a través de las rutas menos congestionadas y más confiables a lo largo de la red privada de Cloudflare, reduciendo la latencia un 35 % en promedio y los errores de conexión en un 27 %.