Junta General
del Principado de Asturias

Servicio de Informática y Organización Digital

Pliego de Prescripciones Técnicas

CDN con control de ataques distribuidos y filtro de seguridad para la web corporativa

ÍNDICE

1 Introducción

El presente documento es el Pliego de Prescripciones Técnicas que rigen el contrato del «Servicio de CDN con control de ataques distribuidos y filtro de seguridad para la web corporativa». La oferta que presente la empresa licitadora debe abarcar la totalidad de las actividades y funciones especificadas en este pliego y en el pliego de cláusulas administrativas particulares (PCAP).

2 Definición del servicio

- El servicio se prestará en modo SaaS, no siendo necesaria la instalación de software o equipamiento físico en la infraestructura local de la Junta General.
- Todo el tráfico objeto de este servicio se dirigirá a la infraestructura del adjudicatario, que analizará y filtrará el mismo de tal forma que únicamente se entregará a la Junta General el que se considere legítimo.
- El servicio deberá contar con capacidades de CDN (*content delivery network*)
- El servicio debe contar con protección contra ataques de denegación de servicio distribuidos (DDoS) de tal forma que el tráfico del ataque no llegue a la red interna de la institución.
- El servicio debe contar con protección contra *bots*, de tal forma que el tráfico de las webs corporativas protegidas tenga mecanismos de detección de patrones de acceso para asegurar que las peticiones recibidas son lícitas.
- El servicio debe contar con protección contra amenazas específicas de tráfico web (WAF), incorporando una capa adicional de seguridad a los cortafuegos e IPS corporativos con un sistema de cortafuegos de aplicación específico para web.
- Todas las capacidades de seguridad se integrarán en la propia CDN, comportándose como un único servicio a efectos de configuración, gestión y administración.

2.1 Características generales

- La administración del servicio podrá realizarse mediante un portal de autoprovisión o *dashboard*, que permitirá la configuración y consulta.
- Se podrá realizar geolocalización de peticiones/usuarios para bloquear/permitir contenido.
- Sistema de precalentamiento de caches.
- Reescritura de cabeceras.
- Entrega de logs en tiempo real.
- Anti DDoS en capas 3, 4 y 7 del modelo OSI.
- Gestión de certificados SSL, bien sea los proporcionados por la Junta General o mediante la integración con certificados gratuitos tipo Let's Encrypt.
- Soporte para HTTP/2.
- Capacidades de invalidación de objetos.
- Configuración modificable por el usuario de forma granular.
- Detección automática de anomalías.
- Al menos 10 URL contempladas en el servicio.
- Al menos 10TB de tráfico mensual.
- Al menos 200 millones de peticiones mensuales.
- La CDN deberá contar con al menos 3 puntos de presencia en Europa, uno de ellos en España.
- El soporte se prestará en castellano en horario 8/5 con tiempo de respuesta menor a 4 horas.

2.2 Características DDoS

- Visibilidad en tiempo real de ataques distribuidos.
- Respuesta proactiva mediante la gestión de anomalías, detectando comportamientos sospechosos.
- Protección de ataques en capa 3 y 4.

- Protección contra inundación de peticiones HTTP, amplificación DNS y ataques de fuerza bruta.

2.3 Características anti *bots*

- Detección en el servicio, antes de entregar el tráfico a la Junta General.
- Sistema de bloqueo sobre *scoring* de direcciones IP.
- Detección de tráfico en base a listas de reputación. Deberá contar con sus propias bases de datos de IP maliciosas en todo el mundo.
- Capacidad para gestionar listas blancas o negras.
- Cumplimiento RGPD; no realizará tracking ni identificación de usuarios.
- Capacidad de incorporar mecanismos *captcha*.

2.4 Características detección anomalías

- Granularidad completa por sitio web.
- Personalización de umbral y sensibilidad.
- Definición de reacciones automáticas ante eventos.
- Capacidad para contar con listas de excepciones.
- Sensores:
    - Incremento en el tráfico.
    - Hit ratio.
    - Peticiones por dirección IP.
    - Tiempo de respuesta.
    - Código de estado.
    - Escáner de vulnerabilidades.
    - Detección de *crawlers*.

2.5 Características WAF

- Capacidad de funcionamiento en modo detección/modo detección y bloqueo.
- Sistema de reglas gestionado por el proveedor, de tal forma que el servicio cuente con un core rule set (CRS) actualizado.
- Protección contra ataques de aplicación:
    - SQL Injection.
    - XSS.
    - CSRF.
- Analítica en tiempo real para toma de decisiones.
- Reportes diarios con actividad de ataques.
- Rate limit.
- Gestión de ACL.
- Modo bajo ataque, que permite poner a la plataforma activa con todas las capacidades y en modo agresivo cuando se detecta un ataque masivo en curso.