



Términos de Referencia

Licenciamiento Load Balancer, WAF y DDoS.

Gestión 2025

CONFIDENCIALIDAD

La información contenida en este documento es confidencial y propiedad de la Empresa YPFB TRANSPORTE S.A. Queda prohibida su copia y/o distribución parcial o total sin el expreso consentimiento del propietario.

INDICE DE CONTENIDO

1. ANTECEDENTES Y OBJETO DEL REQUERIMIENTO	3
ANTECEDENTES	3
OBJETO DEL REQUERIMIENTO	3
2. ALCANCE	3
3. VALIDEZ DE LA PROPUESTA	11
4. REQUISITOS	12
5. PLAZOS DE ENTREGA	12
6. PAGOS	12

1. ANTECEDENTES Y OBJETO DEL REQUERIMIENTO

ANTECEDENTES

YPFB TRANSPORTE S.A. cuenta con equipamiento RADWARE, se requiere renovar licenciamiento y soporte de 2 (DOS) Balanceadores Radware Alteon D-5208 por 3 (tres) años.

YPFB TRANSPORTE S.A. requiere la adquisición de licenciamiento de una solución que contemple licenciamiento WAF y protección contra DDoS por 3 (tres) años.

OBJETO DEL REQUERIMIENTO

Renovar el licenciamiento, para 2 (DOS) Balanceadores Radware Alteon D-5208 de propiedad de YPFB TRANSPORTE S.A. Poder contar con actualizaciones de las versiones del sistema de los equipos, contar con soporte y servicios del fabricante.

Adquirir licenciamiento de solución de protección WAF y DDoS para aplicaciones y publicaciones con servicios propios del fabricante.

2. ALCANCE

El Alcance deberá contemplar la renovación de licenciamiento conforme a lo detallado en la siguiente tabla:

Ítem	P/N Descripción Del Producto	S/N	Periodo de Vigencia
1	1920128001RS Renewal of Standard Support for Alteon D-5208S HPP Perform - 6G/ODS- VL2/32GB/SSL/Dual/SSD – 3 Year	41807008	10-JAN-25 - 09-JAN-28
	9006000007Y1 Perform Package Subscription for 4K/5K – 3 Year	41807008	10-JAN-25 - 09-JAN-28
	1920128001RS Renewal of Standard Support for Alteon D-5208S HPP Perform - 6G/ODS- VL2/32GB/SSL/Dual/SSD - 3 Year	41807049	10-JAN-25 - 09-JAN-28
	9006000007Y1 Perform Package Subscription for 4K/5K – 3 Year	41807049	10-JAN-25 - 09-JAN-28
	9000000013Y1 APSolute Vision - VA - 3 Year	4016576516	10-JAN-25 - 09-JAN-28
	9000000038Y1 APSolute Vision Analytics – ADC - 3 Year	4016576516	10-JAN-25 - 09-JAN-28
	9000000140Y1 APSolute Vision Analytics – AW - 3 Year	4016576516	10-JAN-25 - 09-JAN-28
	9070107 APSolute Vision Reporter (AVR) - 3 Year Subscription	4016576516	10-JAN-25 - 09-JAN-28
	9070110 APSolute Vision additional RTU - 6/30 - 3 Year	4016576516	10-JAN-25 - 09-JAN-28

Ítem	Requerimiento	Detalle
2	Protección de aplicaciones y APIs.	Licenciamiento de Marca a Definir
	Cantidad de aplicaciones y Throughput	Debe proteger un total de 6 aplicaciones con ancho de banda igual o mayor de 10 Mbps.
	Vigencia	Licenciamiento vigente periodo de 3 años.
	Protección de aplicaciones y APIs (WAAP)	<p>La protección de aplicaciones y APIs (WAAP) debe soportar despliegues siempre activos, a través de modificación de DNS y que no requieran modificación alguna de Hardware o Software del lado de los servidores a proteger y tener las siguientes características:</p> <ul style="list-style-type: none"> • Plataforma Cloud, administrado por el fabricante como SaaS. • Debe poder proteger aplicaciones publicadas tanto On-Prem como aplicaciones en nube. • Debe soportar un modelo de integración basado en API que no requiera cambios de DNS o BGP para proteger las aplicaciones y que cuente con las siguientes características: <ul style="list-style-type: none"> - En la arquitectura basada en API no se requiere compartir el certificado digital. - En la arquitectura basada en API los requerimientos van directamente a la aplicación. • Debe proveer una cobertura completa de ataques en capa de aplicación WEB incluyendo todos los ataques descritos en el OWASP TOP 10. • Debe permitir integración con el SIEM de la entidad para el envío de logs de seguridad (QRadar) en caso de ser requerido. • Deberá soportar modificaciones programáticas sobre el servicio vía RESTful API. • Los usuarios (clientes de la aplicación) deben poder conectarse vía TLS 1.3 a las aplicaciones protegidas por el WAAP.
	Requerimientos Seguridad WEB y APIs.	<p>La política de seguridad no debe ser genérica, ni basada en políticas por defecto o mejores prácticas. Debe ser una política a la medida, ajustada a cada aplicación aprovisionada.</p> <p>Las aplicaciones aprovisionadas se podrán configurar en</p>

		<p>modo activo, bloqueando los paquetes de ataques de forma proactiva o en modo monitoreo, simplemente reportando eventos, pero no bloqueándolos.</p> <p>Las políticas de seguridad deben implementar filtros de seguridad que soporten modelos de seguridad positivos y negativos.</p> <p>El servicio debe:</p> <ul style="list-style-type: none"> • Proteger contra ataques de tipo SSRF (Server side request forgery) y RFI (Remote File Inclusion). • Bloquear conexiones que no sean HTTP RFC Compliance. • A través del portal de administración, debe permitir la configuración del bloqueo de tráfico proveniente de anonymous proxies hacia las aplicaciones. • Proveer una protección basada en firmas que proteja la aplicación contra vulnerabilidades conocidas. • Proveer una protección contra comandos de SQL, comandos de shell y ataques de cross-site scripting, usando un algoritmo de reducción para detectar posibles segmentos de código en los parámetros. • Debe cubrir al menos las siguientes amenazas: Cross Site Scripting (XSS), SQL Injections, Injection Flaws, Command Execution, Database Sabotage, Stealth Commanding, Backdoor. • Proveer una protección basada en modelo de seguridad positivo que evalúe los requerimientos hacia la aplicación, contra una lista que contenga la URI y métodos permitidos, bloqueando todos aquellos requerimientos que no se encuentren explícitamente definidos. • Incluir una protección basada en inteligencia de amenazas que podrá activarse o desactivarse desde el portal y permitirá crear excepciones de IP que deban ser excluidas de dichas listas. • Brindar al menos las siguientes opciones de página de bloqueo: <ul style="list-style-type: none"> - Proveer una página de bloqueo por defecto la cual es mostrada a usuarios identificados como atacantes que intentan acceder la aplicación. - Personalizar la página de bloqueo a través de la redirección a un sitio web específico. • Permitir crear reglas de rate limiting definiendo al menos los siguientes parámetros por regla: <ul style="list-style-type: none"> - Acción de la regla: Mínimo requerido, bloqueo y solo reporte.
--	--	--

		<ul style="list-style-type: none"> - Identificador de cliente: Mínimo requerido, tracking por IP y tracking a través de una cookie insertada por el servicio. - Método, Path. - Límite permitido (Threshold) - Tiempo de bloqueo. <ul style="list-style-type: none"> • Permitir al administrador, crear firmas personalizables. Mediante este mecanismo el administrador podrá incorporar a las protecciones incluidas en la solución patrones específicos que desee tratar como eventos de seguridad. • Contar con un mecanismo que permita el bloqueo automático y temporal de direcciones IP de origen (source-blocking), basado en el seguimiento de los ataques que dicho origen a realizado. • Estar basada en una tecnología de WAAP que utilice un modelo de seguridad positivo que aprenda automáticamente los patrones de actividades legítimas de los usuarios, construya automáticamente políticas de seguridad diseñadas para permitir esas actividades y bloquee cualquier acción que se desvíe de estos patrones de comportamiento legítimo. • Incluir una protección que enmascare o bloquee información confidencial proveniente de la aplicación incluyendo mensajes de errores del servidor. • Incluir un mecanismo de Fingerprinting que permita identificar de forma única el dispositivo que está ingresando a la aplicación web sin necesidad de conocer su dirección IP. • Realizar Schema Enforcement en XML y JSON validando el método, endpoint, query parameters, header parameters, cookie parameters y body parameters. • A través del portal, debe permitir añadir o modificar los parámetros de tipo query, header cookies o body de los endpoints. • Contar con un mecanismo que permita visualizar los subdominios y/o URLs que invocan los scripts de java (JS) desde el navegador de los usuarios que consumen las aplicaciones, así como el nivel de amenaza de los mismos y si es que estos cuentan o no con certificados de seguridad. • La protección del lado del Cliente, debe soportar inventario de Scripts y de dominios accedidos. • La protección del lado del cliente, debe ser capaz de
--	--	--

		<p>informar cuando:</p> <ul style="list-style-type: none"> - Se detecta comunicación con un nuevo dominio. - Se detecta una nueva solicitud saliente - Se detecta un nuevo origen • Proveer un mecanismo avanzado de categorización del riesgo de cada script incluyendo entre otros: <ul style="list-style-type: none"> - Detección de manipulación de datos sensibles. - Scoring de los dominios destino - Análisis de comportamiento de los scripts
	Requerimientos de protección contra ataques de DDoS	La protección de ataques DDoS debe proteger contra ataques de capa de red de día cero a través de análisis de comportamiento e identificando la huella (footprint) del tráfico anómalo. Debe cubrir a las aplicaciones en nube que se encuentren dentro de las 6 aplicaciones solicitadas en el servicio de WAF.
	Requerimientos de la consola de administración y funcionales.	<p>El licenciamiento debe incluir un portal desde donde se aprovisionen los certificados digitales, aplicaciones y que incluya dashboards, eventos, analítica, alertas y reportes.</p> <p>El portal debe:</p> <ul style="list-style-type: none"> • Soportar doble factor de autenticación. • Permitir visualizar los cambios realizados tanto por los usuarios administradores como por el fabricante y debe conservar la información por al menos 60 días. • Permitir bajar los eventos asociados a los cambios en el servicio en formato CSV mínimamente. • Mostrar como mínimo la siguiente información relacionada con el plan adquirido: <ul style="list-style-type: none"> - Número de aplicaciones adquiridas / número de aplicaciones aprovisionadas - Ancho de banda adquirido / ancho de banda promedio / ancho de banda pico - Periodo de Suscripción. - Servicios adicionales contratados. • Permitir subir los certificados digitales asociados a las aplicaciones a proteger • Mostrar las aplicaciones aprovisionadas especificando: <ul style="list-style-type: none"> - El estado de protección de las aplicaciones, indicando si la aplicación está brindando protección activa o aún está en modo aprendizaje. - La fecha de creación. - El dominio.

		<ul style="list-style-type: none"> - La región (POP en el cual fue creada). - Representación gráfica de los eventos durante mínimamente los últimos 7 días. • Desde el portal se deben poder configurar múltiples puertos de servicio para una aplicación / dominio específico, teniendo la posibilidad de configurar los siguientes tipos: <ul style="list-style-type: none"> - TCP: Tráfico NO http. - HTTP: Tráfico HTTP sin encriptación. - HTTPS: Tráfico HTTP encriptado. • Debe permitir configurar desde el portal y por cada aplicación chequeos de salud de tipo TCP, HTTP y HTTPS. <ul style="list-style-type: none"> - El chequeo de salud HTTP/HTTPS debe permitir configurar el hostname, la URL y el código de respuestas esperado. • Permitir configurar el nivel de seguridad de TLS, permitiendo seleccionar el protocolo a utilizar y el nivel de seguridad de los ciphers, por cada aplicación aprovisionada. • Permitir configurar desde el portal la forma en la cual se copia la dirección IP real de los clientes, al encabezado HTTP por cada aplicación aprovisionada. • Permitir personalizar el campo del header en el cual se copiará la IP real de los clientes, por cada aplicación aprovisionada. • Deberá soportar, para cada aplicación protegida, la configuración de un servidor de origen primario y uno secundario que entra a trabajar si el chequeo de salud del primario falla. • Soportar, para cada aplicación protegida, el balanceo de carga entre mínimamente hasta 4 servidores origen y métricas de round-robin, incluyendo persistencia por IP. • Permitir la configuración de listas blancas de IP desde el portal de servicios, por cada aplicación aprovisionada. • Permitir la configuración de bloqueo por geografía desde el portal de servicios, por cada aplicación aprovisionada. • Permitir crear excepciones de IP que se encuentren incluidas dentro del bloqueo por geografía. • A través del portal, debe permitir crear reglas de control de acceso por IP a las aplicaciones protegidas. • A través del portal, y por cada aplicación, debe permitir la redirección de tráfico en base al
--	--	--

		<p>contenido del mismo, como mínimo considerando:</p> <ul style="list-style-type: none"> - Encabezados - Métodos - IP/CIDR - País de Origen - URI <ul style="list-style-type: none"> • A través del portal, y por cada aplicación, debe permitir la creación de reglas manuales de seguridad en base al contenido, como mínimo considerando: <ul style="list-style-type: none"> - Encabezados - Métodos - IP/CIDR - País de Origen - URI • A través del portal, y por cada aplicación, debe permitir la creación de reglas para, remover y reescribir los encabezados en el request, como mínimo considerando: <ul style="list-style-type: none"> - Encabezados - Métodos - IP/CIDR - País de Origen - URI • A través del portal, y por cada aplicación, debe permitir la creación de reglas para, remover, reescribir e insertar encabezados en el response. • Debe permitir la distribución de una política de seguridad de una aplicación a otra permitiendo configurar la distribución de forma periódica. • El portal de servicios debe permitir visualizar los eventos de seguridad por aplicación. La información mínima que deben tener estos logs: <ul style="list-style-type: none"> - Acción tomada por el servicio - Dirección IP origen - País de Origen - Aplicación - Fecha y hora del evento - Severidad - Tipo de ataque - Clasificación del ataque de acuerdo al OWASP Top 10 - Entregar el detalle del encabezado del request de HTTP del ataque • Permitir refinar el evento (crear una excepción) desde la vista de eventos de seguridad. • Para los eventos relacionados a bloqueo por origen (source blocking), el evento de seguridad debe
--	--	--

		<p>proporcionar la historia del ataque, permitiendo identificar el tipo y número de ataques registrados que llevaron a tomar la decisión de bloquear el origen, así como el tiempo de bloqueo de dicho origen.</p> <ul style="list-style-type: none"> • Permitir visualizar sugerencias de refinamiento para la protección de API, permitiendo visualizar las modificaciones en formato JSON, antes de aplicarlas. • Permitir la descarga de los eventos de seguridad en formato CSV. • Incluir analítica de seguridad que agrupe múltiples eventos de seguridad en actividades, permitiendo a los administradores enfocarse en alertas de alta prioridad. • La analítica de seguridad debe mostrar un histograma con información acerca de los eventos detectados, las actividades analizadas, nuevas actividades descubiertas, y tráfico limpio en función del tiempo. • La analítica de seguridad debe mostrar la siguiente información para cada una de las actividades (agrupación de eventos de seguridad): <ul style="list-style-type: none"> - Indicar cuando fue la primera vez que se registró la actividad. - Las IP origen asociadas a la actividad. - Gráfico de tendencia de los eventos de seguridad asociados a dicha actividad. - Nombre del parámetro afectado. - Descripción del evento. • Permitir configurar el envío de alertas que se activen bajo un patrón configurable. • Permitir la configuración de reportes para envío vía correo electrónico. • Contar con un dashboard con al menos las siguientes vistas: <ul style="list-style-type: none"> - Tabla resumen de la actividad del WAAP - Gráfico con el tráfico limpio hacia las aplicaciones en bps - Gráfico con las transacciones por segundo por aplicación - Gráfico con los eventos de seguridad registrados en las aplicaciones - Gráfico de ataques clasificados por el OWASP top 10 - TOP de orígenes de ataques en capa de aplicación - TOP de las aplicaciones atacadas
--	--	--

		<ul style="list-style-type: none"> - Debe proporcionar un mapa que indique el origen geográfico de los ataques en capa de aplicación Web. - Debe proporcionar un mapa con las geografías que han sido bloqueadas. <p>El portal permitirá personalizar el dashboard a través de:</p> <ul style="list-style-type: none"> - Configurar el tiempo de visualización para todas las vistas o por cada una de ellas. - Seleccionar las aplicaciones sobre las cuales se mostrará la información de cada una de las vistas.
	Soporte administrado de seguridad del fabricante	<ul style="list-style-type: none"> a) La disponibilidad mínima de la infraestructura de red debe ser de: 99.99% b) El debe ser un servicio de seguridad administrado por el fabricante con disponibilidad 7x24x365. c) Debe contar con los siguientes mecanismos de contacto mínimamente: <ul style="list-style-type: none"> - Portal Web de Soporte - Soporte Telefónico • Debe monitorear constantemente el estado de salud de las aplicaciones configuradas. • La retención de logs en la plataforma debe ser mínimamente de 60 días. • Debe brindar durante la fase de implementación y configuración de las aplicaciones los servicios propios del fabricante. • Debe contar, como mínimo, con los siguientes estándares de seguridad y calidad: <ul style="list-style-type: none"> - ISO/IEC 27001 (Information Security Management Systems). - ISO/IEC 27032 (Security Techniques -- Guidelines for Cybersecurity) - ISO 27017 (Information Security for Cloud Services) - ISO 27018 (Information Security Protection of Personally identifiable information (PII) in public clouds) - US SSAE16 SOC-1 Type II, SOC-2 Type II

3. VALIDEZ DE LA PROPUESTA

La Propuesta deberá tener una validez no menor a noventa (90) días calendario, desde la fecha límite fijada para la entrega de las Propuestas.

4. REQUISITOS

Es un requisito indispensable para el Proveedor presentar:

Para Ítem 1 y 2

- a) Certificado o carta emitida por el fabricante donde demuestre y avale su condición de canal autorizado para distribución y comercialización de licenciamiento ofertados.

Para Ítem 1

- a) El proveedor local debe contar con al menos una (1) persona con certificación vigente mínima de Radware Alteon Professional Certification.

Para Ítem 2:

- a) Certificado o carta emitida por el fabricante donde demuestre que la provisión de licenciamiento será de una plataforma de seguridad administrada por el fabricante con disponibilidad 7x24x365. Incluyendo la configuración y despliegue inicial de la solución y protección de las aplicaciones con servicios propios del fabricante.
- b) El proveedor local debe contar con al menos una (1) persona con certificación vigente mínima del fabricante de la solución propuesta.

5. PLAZOS DE ENTREGA

Al ser ítems separados, el o los proveedores que se adjudique(n) el o los ítems, deben cumplir los siguientes requisitos de entrega del licenciamiento ofertado a YPFB TRANSPORTE S.A.:

La entrega de licenciamiento deberá ser de hasta 10 días calendario para el Ítem 1

La entrega de licenciamiento deberá ser de hasta 30 días calendario para el Ítem 2 que debe incluir la configuración y puesta en marcha del licenciamiento y solución por parte del fabricante, los plazos inician después de la emisión de la orden de proceder. La entrega del licenciamiento se realizará DDP- en Almacén YPFB TRANSPORTE Santa Cruz

6. PAGOS

El pago se realizará:

- 100% al término satisfactorio de la entrega de licenciamiento e instalación de cada ítem, previa validación y conformidad de las licencias y las pruebas de aceptación.