

RESPUESTA A PREGUNTAS Y OBSERVACIONES EXTEMPORÁNEAS

INVITACIÓN SIMPLIFICADA No. 960 - SEGURIDAD PERIMETRAL COTERM FORTINET

Se procede a dar respuesta a las preguntas y observaciones extemporáneas presentadas:

1. INTERESADO UNO – GAMMA INGENIEROS.

1.1. OBSERVACIÓN # 1: Respuesta observaciones TDR

1.5. OBSERVACIÓN # 5: 2.3. CONDICIONES TECNICAS OBLIGATORIAS

2.3.1.10. Actualización Full UTM (gestión unificada de amenazas) que incluye el software para todos los equipos alcance del contrato (Intrusion Prevention System, Antivirus, Antispam, Web Filtering, Application Control, Data Loss Prevention, Wireless Controller, IoT Security).

Agradecemos a la entidad aclarar si su intención es proceder con la renovación del licenciamiento actual (UTP) de las soluciones Fortigate, o si, por el contrario, desea renovar el licenciamiento a nivel ENTERPRISE, lo cual incluiría las características descritas en dicho ítem.

RESPUESTA OBSERVACIÓN # 5:

Renovación del licenciamiento a nivel ENTERPRISE.

Revisando la respuesta informada por la entidad y luego de revisar los requerimientos actuales de esta, y teniendo en cuenta que actualmente ha estado operando con licenciamiento UTP, queremos resaltar que no es necesario realizar el cambio a una licencia Enterprise en este momento toda vez que:

1. Actualmente Fortinet para las soluciones de firewall cuenta con varios tipos de licenciamiento como estrategia de seguridad, estas con el tiempo se han ido actualizando, ajustando e incorporando nuevas funcionalidades para abordar la creciente complejidad de las amenazas cibernéticas, pero siempre manteniendo un enfoque de simplicidad y seguridad para las organizaciones. dentro de estas actualizaciones se encuentran:

- **Licencia UTP:** está diseñada para ofrecer una solución integral de seguridad que cubre aspectos como firewall, VPN, protección contra amenazas, filtrado web, antivirus, prevención de intrusiones, control de aplicaciones, Fortisandbox Cloud.
- **Licencia Enterprise:** Además de las funcionalidades de la UTP, incluye funcionalidades de Data loss prevention y Attack Surface Security.

Lo anterior con el fin de que se de claridad a las diferencias que se tienen en el licenciamiento.

2. Adecuación de la licencia UTP a las necesidades actuales: La entidad ha estado operando satisfactoriamente bajo el modelo de licenciamiento UTP, que ha cubierto de manera eficiente las necesidades de seguridad y red. No se ha identificado una carencia o limitación significativa que justifique el incremento en los costos asociados con la transición a una licencia Enterprise, dado que la funcionalidad de la licencia UTP sigue alineada con los requerimientos actuales.

3. Costo-beneficio del cambio: El licenciamiento Enterprise generalmente está orientado a entornos con necesidades de mayor escalabilidad o características avanzadas que no son imprescindibles para la operación actual de la entidad. Considerando que la estructura y el volumen de tráfico no han experimentado cambios significativos, el costo adicional de este cambio podría no justificar el impacto en los presupuestos asignados para la operación.

Por último, dado que la entidad ha venido trabajando satisfactoriamente con una licencia UTP, y teniendo en cuenta que el licenciamiento UTP ha evolucionado significativamente para cubrir muchas de las necesidades actuales, el cambio implicaría un costo adicional que impactaría al presupuesto sobre costearlo el mismo y no entraría dentro del mismo.

RESPUESTA OBSERVACIÓN # 1:

Se acepta la observación, toda vez que el presente proceso busca renovar el licenciamiento actual en las mismas condiciones con las cuales se ha renovado en años anteriores, se mantiene el licenciamiento UTP.

1.2. OBSERVACIÓN # 2: Respuesta observaciones TDR

RESPUESTA OBSERVACIÓN # 12:

El proveedor deberá incluir en su oferta, el valor agregado que considere, sin costo adicional para la entidad.

Los appliance con que cuenta la entidad actualmente son físicos por tanto los valores agregados deberán ser también físicos.

Las características técnicas mínimas para el FortiAnalyzer ofrecido como valor agregado son las siguientes:

- Logs Diarios: Mínimo 100 GB
- Interfaces: Mínimo 4X RJ45 GE – 2X GE SFP
- Tiempo de licenciamiento: 1 año
- Capacidad de almacenamiento: Mínimo 4 TB

Las características técnicas mínimas para el Fortigate 60 ofrecido como valor agregado son las siguientes:

- Interfaces: 1 x USB Port 2 - 1 x Console Port - 2 x GE RJ45 WAN Ports - 1 x GE RJ45 DMZ Port 6 - 2 x GE RJ45 FortiLink Ports - 5 x GE RJ45 Internal Ports
- Tiempo de licenciamiento: 1 año
- Capacidad de almacenamiento: 128 GB SSD

Ver Adenda No. 1

Teniendo en cuenta que los valores agregados solicitados dentro del proceso hacen referencia a la solución **Fortigate del modelo 60F** el cual se aclara en las respuestas dadas por la entidad (**Respuesta observación 13**), solicitamos amablemente retirar la solicitud de disco duro dentro de las características del mismo toda vez que este haría que el modelo cambiara a un fortigate 61F.

Lo cual no se hace necesario ya que la capacidad de procesamiento y memoria del 60F es suficiente para manejar el tráfico de la red y proteger contra amenazas sin la necesidad de aumentar recursos adicionales, especialmente porque ya se cuenta con un **FORTIANALYZER** que gestiona y almacena los logs y datos analíticos. Esto permite optimizar el rendimiento del firewall, sin sobrecargarlo con tareas de almacenamiento.

Lo anterior, se impactaría directamente al presupuesto toda vez que el cambio de modelo generaría un incremento innecesario para el proyecto ya que cuenta con las herramientas adecuadas.

RESPUESTA OBSERVACIÓN # 2:

De acuerdo con la observación, por error se incluyo un almacenamiento que no corresponde, por lo cual, se mantienen las características del equipo Fortigate 60F, el cual no tiene almacenamiento interno. Por lo anterior, se procede a adendar este punto, Ver Adenda No. 3

1.3. OBSERVACIÓN # 3: Respuesta observaciones TDR

1.7. OBSERVACIÓN # 7: 2.3. CONDICIONES TECNICAS OBLIGATORIAS

2.3.1.5. Contar con una línea de soporte telefónico y un sistema de registro para la creación de casos para la atención de incidentes y requerimientos.

Agradecemos a la entidad atentamente aclarar si el anterior ítem hace referencia solo a la atención de incidentes operativos; los cuales se definen como los eventos no planeados que generan interrupción total o parcial del servicio en la red o en algunas de sus funcionalidades,

y no hace referencia a prestar un servicio gestión que es la Atención a requerimientos de cambios de configuración solicitados por parte de la cliente.

RESPUESTA OBSERVACIÓN # 7:

Se solicita una línea de soporte telefónico y un sistema de registro para la creación de casos para la atención de **incidentes y requerimientos** (incluyen cambios de configuración).

Se sugiere respetuosamente a la entidad delimite la gestión de requerimiento a una bolsa de 30 horas por año como apoyo a los cambios de configuración solicitados por el cliente, dado que la entidad ya cuenta con personal idóneo y capacitado para llevar a cabo estas tareas de forma eficiente. Esta medida permitirá establecer un marco claro de requerimientos y optimizar los recursos disponibles, asegurando que las modificaciones solicitadas se gestionen de manera controlada y dentro de un tiempo razonable.

Adicionalmente, la entidad realiza la administración directa de las soluciones implementadas, lo que evidencia su capacidad para manejar los cambios y ajustes de manera autónoma. Por lo tanto, limitar la intervención externa a un número específico de horas proporcionará un balance adecuado entre la gestión de requerimientos y la autonomía operativa de la entidad, optimizando el tiempo y los costos involucrados.

Lo anterior también teniendo presente la respuesta dada por la entidad a nivel de administración y tickets las cuales se relacionan a continuación.

3. INTERESADO TRES – TELEFONICA.

3.1. OBSERVACIÓN # 1: "2.2.2. Soporte del proveedor remoto o en sitio desde Bogotá, cuando así se requiera, con un esquema de atención 365 días al año, 24 horas al día y 7 días a la semana."

Se solicita amablemente a la entidad confirmar el alcance esperado por parte del proveedor. Es nuestro entender que el alcance incluye el soporte de la solución pero la administración será realizada por parte de Procolombia. ¿Es correcto nuestro entendimiento?

RESPUESTA OBSERVACIÓN # 1:

Correcto, el soporte según el literal señalado debe ser entregado por el proveedor, la administración es realizada por ProColombia.

3.2. OBSERVACIÓN # 2: "2.2.2. Soporte del proveedor remoto o en sitio desde Bogotá, cuando así se requiera, con un esquema de atención 365 días al año, 24 horas al día y 7 días a la semana."

Se solicita amablemente a la entidad confirmar el número de tickets mensuales aproximados que se presentan con el contrato vigente con el fin de hacer una estimación precisa del requerimiento.

RESPUESTA OBSERVACIÓN # 2:

En promedio se generan 2 casos mensuales. No obstante lo anterior y al margen del promedio anotado que es información de mera referencia, el eventual contratista deberá atender la totalidad de solicitudes de soporte que se hagan durante el término de vigencia del contrato, bajo el esquema de atención señalado.

RESPUESTA OBSERVACIÓN # 3:

No se acepta la observación, toda vez que ProColombia ha mantenido este nivel de atención durante los contratos anteriores, sin limitarlo a un número de horas establecidos en una bolsa, por tal razón, este requerimiento se mantiene como está establecido en los Términos de Referencia.

La presente se publica el veintiocho (28) de enero de 2025 en la página web www.fiducoldex.com.co y SECOP I en cumplimiento de las condiciones indicadas en los términos de referencia y el manual de contratación de PROCOLOMBIA.

PROCOLOMBIA – FIDUCOLDEX