Nro. GS-2023- 047826 **/SUINP-SIPOL– 20.1**

Bogotá D.C., 04 OCT 2023

Señor Coronel
WILLIAM CASTAÑO RAMOS
Director
Dirección de Carabineros y Protección Ambiental
Avenida Boyacá 142 A 55
Bogotá D.C

Asunto: respuesta observaciones dentro del proceso PN DICAR MIC 059 2023

De manera atenta me permito enviar a mi coronel, la respuesta a la observación allegada por la empresa Boyra S.A, en el marco del proceso PN DICAR MIC 059 2023 cuya descripción es "ADQUISICIÓN, INSTALACIÓN Y PUESTA EN FUNCIONAMIENTO DE UN DISPOSITIVO TIPO FIREWALL PARA LA SECCIONAL DE INTELIGENCIA POLICIAL DE LA DIRECCIÓN DE CARABINEROS Y PROTECCIÓN AMBIENTAL", así:

Observación N° 1:

En el ítem "1.5.2. Throughput de Threat Prevention de 690 Mbps mediciones con mínimo las siguientes funcionalidades habilitadas simultáneamente: Firewall con control de aplicaciones, Sistema de Prevención de Intrusos (IPS) y Anti-malware."

Se solicita a la entidad que además de soportar las funcionalidades de Firewall con control de aplicaciones, Sistema de Prevención de Intrusos (IPS) y Anti-malware, puedan soportar activas de manera simultánea, sin disminuir su desempeño (Performance del hardware propuesto), las funcionalidades de:

Antivirus: La entidad podrá crear reglas a través de perfiles que permiten proteger contra virus, gusanos y troyanos, así como contra descargas de software espía. Utilizando un motor de prevención de malware basado en flujo, que inspecciona el tráfico en el momento en que se recibe el primer paquete. Este perfil busca una amplia variedad de malware en ejecutables, archivos PDF, virus HTML y JavaScript, incluida la compatibilidad con el escaneo dentro de archivos comprimidos y esquemas de codificación de datos.

Antispyware: Otorgar a la entidad la capacidad de impedir que el software espía en los hosts comprometidos intente enviar señales a servidores externos de comando y control (C2), lo que le permite detectar tráfico malicioso que sale de la red desde clientes infectados. Deber ser posible aplicar varios niveles de protección entre zonas.

DNS Security: De esta manera la entidad podrá agregar una capa extra de seguridad para garantizar que las solicitudes DNS que se generan al interior de la red, son auténticas y benignas, es decir, que no estén asociadas a ningún tipo de amenaza a través de este vector (DNS). Algunas amenazas modernas que se pueden detectar serian: amenazas de C2, incluidos túneles DNS, ataques de re-vinculación de DNS, dominios creados mediante generación automática, hosts de malware y muchos más.

Bloque de archivos: Utilizar esta característica para que la entidad tenga la capacidad para bloquear tipos de archivos específicos en aplicaciones específicas y en la dirección de flujo de sesión especificada (entrante/saliente/ambas). Puede configurar el perfil para alertar o bloquear al cargar y/o descargar y puede especificar qué aplicaciones estarán sujetas al perfil de bloqueo de archivos. También puede configurar páginas de bloqueo personalizadas que aparecerán cuando un usuario intente descargar el tipo de archivo especificado. Esto permite al usuario tomarse un momento para considerar si desea o no descargar un archivo.

Toda vez que en las actuales circunstancias de ataques permanentes es indispensable tener la posibilidad de reforzar la seguridad de la red y que el hardware esté preparado para recibir estas funcionalidades sin afectar su desempeño.

De acuerdo a lo anterior se solicita a la entidad modificar el punto 1.5.2 de la siguiente manera:

1.5.2. Throughput de Threat Prevention de 690 Mbps mediciones con mínimo las siguientes funcionalidades habilitadas simultáneamente: Firewall con control de aplicaciones, Sistema de Prevención de Intrusos (IPS) y Anti-malware, y con capacidad de soportar si se requiere con solo licenciamiento habilitar funcionalidades de antivirus, antispyware, seguridad de DNS, y bloqueo de archivos.

Respuesta Observación N° 1:

No se acepta la observación, teniendo presente que dentro de las características buscadas para los equipos relacionados en las especificaciones técnicas no se tuvo en cuenta lo manifestado en la presente observación, llevando a cabo el estudio de mercado correspondiente sin considerar estas características sugeridas, motivo por el cual no se pueden solicitar porque podrían limitar la participación de posibles oferentes.

Observación N° 2:

En el ítem "1.5.9. 1 (Una) interfaz de tipo consola"

Se solicita a la entidad que además de la interfaz de consola, el hardware propuesto tenga la capacidad de un puerto tipo OOB (Out Of the box por sus siglas en inglés) con fines de administración del NGFW. Cuyo puerto se considera necesario para poder gestionar la UI (User Interface) y línea de comandos (CLI) del equipo sin tener que usar las interfaces de tráfico; esto genera independencia entre el tráfico que procesa el NGFW y los procesos de control o gestión del mismo, por ejemplo si la entidad llegase a estar bajo un ataque de inundación de tráfico (DoS), bajo el esquema de que la administración del NGFW se efectué a través del OOB port, el equipo de TI, podrá seguir gestionando el NGFW sin inconvenientes, entre muchas otras ventajas que esto trae.

Respuesta observación N° 2:

No se acepta la observación, teniendo presente que dentro de las características buscadas para los equipos relacionados en las especificaciones técnicas no se tuvo en cuenta lo manifestado en la presente observación, llevando a cabo el estudio de mercado correspondiente sin considerar estas características sugeridas, motivo por el cual no se pueden solicitar porque podrían limitar la participación de posibles oferentes.

Observación N° 3:

En el ítem "1.5.10. Puerto USB"

Se solicita a la entidad incluir la necesidad de que el hardware propuesto posea un puerto de micro USB que se pueda emplear como alternativa de puerto de consola en caso de que el administrador requiera ingresar directamente al equipo y no cuente con un cable de consola (RJ45-RS232), este puerto micro USB realiza una conversión de serial a micro USB para este propósito. Lo anterior se recomienda netamente con fines de brindar facilidad al momento de administrar de manera local el/los dispositivos.

Respuesta observación N° 3:

Se acepta la observación, por motivos expuestos anteriormente y teniendo en cuenta que es una alternativa para conectarse al dispositivo, motivo por el cual se modifica el ítem 1.5.10, que estaba de la siguiente manera, así:

1.5.10	1 Puerto USB

Se modifica el ítem de la siguiente forma:

1.5.10	1 Puerto USB y/o puerto de micro USB

Observación N° 4:

En el ítem 1.14.17 y el 1.15.1:

"1.14.17. El agente de VPN client-to-site debe ser compatible al menos con: Windows 7, Windows 8, Windows 10, MacOS X, Linux, Android y iPhone." Y, en el Ítem 1.15.1. El agente de VPN client- to-site debe ser compatible al menos con: Windows 7, Windows 8, Windows 10, MacOS X, Linux, Android y ios.

Se solicita a la entidad actualizar los requerimientos en cuanto a la compatibilidad del agente de VPN, sugiriendo el siguiente párrafo:

"El agente de VPN client-to-site debe ser compatible al menos con*: Apple macOS, Apple iOS, iPadOS, Windows 10, Windows 11, Linux, Google Android y Google Chrome"*

La anterior modificación sugerida, es en vista de que WINDOWS 7 y WINDOWS 8 en todas sus versiones ya NO ES SOPORTADO por el fabricante MICROSOFT.

Además de incluir el soporte de otros sistemas operativos que posiblemente la entidad en un futuro pueda adquirir.

https://support.microsoft.com/en-au/office/what-windows-end-of-support-means-for-office-and-microsoft-365-34e28be4-1e4f-4928-b210-3f45d8215595

Respuesta observación N° 4:

Se acepta parcialmente la observación, por cuanto se evidencia que se debe aclarar de una forma directa el ítem sin dar lugar a interpretaciones que estén por fuera de la especificación técnica buscada por esta Dirección, no obstante, por parte del estructurador se tiene a bien modificar el presente ítem dando claridad al mismo, manteniendo el principio de la pluralidad de oferentes, motivo por el cual se modifican los ítem 1.14.17 y 1.15.1, que estaban de la siguiente manera, así:

1.14.17	El agente de VPN client-to-site debe ser compatible al menos con: Windows 7, Windows 8, Windows 10, MacOS X, Linux, Android y Iphone.

1.15.1	El agente de VPN client-to-site debe ser compatible al menos con: Windows 7, Windows 8, Windows 10, MacOS X, Linux, Android y IOS

Se modifica el ítem de la siguiente forma:

1.14.17	El agente de VPN client-to-site debe ser compatible al menos con: sistemas operativos Windows, MacOS, Linux, Android y IOS para Iphone.

1.15.1	El agente de VPN client-to-site debe ser compatible al menos con: sistemas operativos Windows, MacOS, Linux, Android y IOS para Iphone.

Observación N° 5:

Respecto al ítem 2.16, 2.17 se solicita que la transferencia de conocimiento, se permita la transferencia de manera remota, con eso se evita desplazamiento de los funcionarios, además de tener una flexibilidad en el horario.

Respuesta observación N° 5:

No se acepta la observación, y se aclara que la transferencia de conocimiento solicitada se debe dictar de forma presencial según las condiciones establecidas en el ítem, previa coordinación con el supervisor del contrato.

Observación N° 6:

Respecto al ítem 3.1 ***"El proponente deberá presentar una Certificación del fabricante donde conste que el proponente es un Canal Certificado, lo cual lo hace idóneo para diseñar, instalar y colocar en funcionamiento la solución presentada. El nivel mínimo deber ser su homologación de partner en nivel intermedio, lo que corresponde en las diferentes marcas, así: FORTINET - GOLD PARTNER o PALO ALTO – PLATINUM INNOVATOR o CISCO – PREMIER o CHECK POINT – TRES ESTRELLAS o su equivalente en las diferentes marcas."***

Solicitamos a la entidad qua para el numeral 3.1 para la marca PALO ALTO – sea tenido en cuenta la membresía **INNOVATOR.**

Respuesta observación N° 6:

Se acepta la observación, por los motivos expuestos anteriormente y teniendo en cuenta que la certificación mencionada cumple con lo solicitado. En el ITEM 3.1 no se está exigiendo PLATINUM INNOVATOR

3.1	El proponente deberá presentar una Certificación del fabricante donde conste que el proponente es un Canal Certificado, lo cual lo hace idóneo para diseñar, instalar y colocar en funcionamiento la solución presentada. El nivel mínimo deber ser su homologación de partner en nivel intermedio, lo que corresponde en las diferentes marcas, así: FORTINET - GOLD PARTNER o PALO ALTO – INNOVATOR o CISCO – PREMIER o CHECK POINT – TRES ESTRELLAS o su equivalente en las diferentes marcas.

Observación N° 7:

En cuanto al ítem 3.3. "NIVEL ACADEMICO: El oferente deberá presentar un profesional en Ingeniería de Sistemas y/o Ingeniería en Telecomunicaciones y/o ingeniería Electrónica, deberá anexar fotocopia del diploma y/o acta de grado; de igual forma, se debe anexar al menos una (01) certificación en los niveles de experto, otorgados por fabricante de los equipos ofertados, dicha certificación se deberá adjuntar.

Se solicita respetuosamente permitir, ya que no en todos los fabricantes se manejan los mismos términos en las certificaciones de fabricante, para el caso específico de PALO ALTO sean aceptadas las certificaciones de fabricante denominadas **PCNSE** o **PCNSA** sustentado en que:

La certificación **PCNSE** valida el conocimiento y las habilidades requeridas para los ingenieros de seguridad de redes que diseñan, implementan, operan, administran y solucionan los problemas de los NGFW Palo Alto Networks.
La certificación **PCNSA** valida el conocimiento y las habilidades requeridas para los administradores de seguridad de red responsables de operar y administrar el firewall de próxima generación de Palo Alto Networks. Las personas certificadas por PCNSA han demostrado conocimiento del conjunto de características de los NGFW de Palo Alto Networks.

Es decir que el personal presentado pueda tener alguna de estas certificaciones. Dicha información puede ser encontrada directamente en la página del fabricante. https://www.paloaltonetworks.com

Respuesta observación N° 7:

Se acepta la observación, por los motivos expuestos anteriormente y teniendo en cuenta que las certificaciones mencionadas cumplen con lo solicitado.

3.3	NIVEL ACADEMICO: El oferente deberá presentar un profesional en Ingeniería de Sistemas y/o Ingeniería en Telecomunicaciones y/o ingeniería Electrónica, deberá anexar fotocopia del diploma y/o acta de grado; de igual forma, se debe anexar al menos una (01) certificación en los niveles de experto, otorgados por fabricante de los equipos ofertados, dicha certificación se deberá adjuntar. NOTA: En caso de ser profesional extranjero deberá presentar certificado de homologación de su título profesional ante el Ministerio de Educación Nacional de Colombia

Se modifica el ítem de la siguiente forma:

3.3	NIVEL ACADEMICO: El oferente deberá presentar un profesional en Ingeniería de Sistemas y/o Ingeniería en Telecomunicaciones y/o ingeniería Electrónica, y/o Ingeniería Informática y/o carrera afines, se deberá anexar fotocopia del diploma y/o acta de grado; de igual forma, se debe anexar al menos una (01) certificación en los niveles de experto y/o intermedio y/o avanzado, otorgados por fabricante de los equipos ofertados, (para PALOALTO –PCNSA y/o PCNSE, para FORTINET – NSE6 y/o NSE7, para CISCO – CCNP DE SEGURIDAD y/o CCIE de SEGURIDAD, para CHECK POINT – CCSE y/o CCSM) dicha certificación se deberá adjuntar. NOTA 1: En caso de ser profesional extranjero deberá presentar certificado de homologación de su título profesional ante el Ministerio de Educación Nacional de Colombia. NOTA 2: Si en los diferentes fabricantes se actualizo o cambio el nombre de la certificación debe anexar a la propuesta la dirección web del fabricante donde se evidencie el cambio pero que tiene la misma validez o afinidad o familia o nivel.

Finalmente, me permito indicar que las observaciones aceptadas serán modificadas en el pliego de condiciones definitivas y apertura del proceso de selección.

Atentamente,

Capitán FABIAN ESTEBAN MONTAÑA SARMIENTO
Jefe Grupo Operaciones de Inteligencia

Anexo: no

Elaboró: PT. Cristian Fernando Solano Cifuentes
Estructurador Estudio Previo - SIPOL SUINP

Revisó: CT. Fablán Esteban Montaña Sarmiento
SIPOL-GROPI

Fecha de elaboración: 04-10-2023
Ubicación: Z:\JEFATURA\TELEMATICA\2023\FIREWALL

Avenida Boyacá 142 A - 55
5189796 ext. 21873
dicar.sipol@dipol.gov.co
www.policia.gov.co

Humana

INFORMACIÓN PÚBLICA