TRIBUNAL SUPREMO DE ELECCIONES

PROVEEDURÍA INSTITUCIONAL

Teléfono 2287-562 Fax: 2256-6351 Email: provtse@tse.go.cr.

LICITACIÓN ABREVIADA

2012LA-000080-85001

"COMPRA E INSTALACION DE UN SISTEMA DE PREVENCIÓN DE INTRUSOS (IPS) APPLIANCE"

La Proveeduría Institucional del Tribunal Supremo de Elecciones, recibirá ofertas digitales hasta las **10:00 horas del día 11 de junio de 2012**, para la Licitación Abreviada número 2012LA-00080-85001, denominado "COMPRA E INSTALACION DE UN SISTEMA **DE PREVENCIÓN DE INTRUSOS"**

La oferta deberá presentarse vía digital mediante el sistema Comprared y utilizando la "firma digital", según el procedimiento para la presentación de Oferta Digital de la Dirección General de Administración de Bienes y Contratación Administrativa.
https://www.hacienda.go.cr/rp/manuales/Manual%20oferta%20digital%20-%20proveedor%20comercial.pdf

Para consultas y aclaraciones llamar a los teléfonos: Proveeduría Institucional: 2287-5626. Fax: 2256-6351, para consultas técnicas al teléfono: 2287-5802 con el Sr. Mario Pereira Granados.

1) **Bien a adquirir:**

Línea	Cantidad	Servicio a adquirir
1	1	Compra e Instalación de un sistema de prevención de intrusos y administración de eventos.

SE ADVIERTE A LOS OFERENTES QUE LAS ESPECIFICACIONES TÉCNICAS DEL SERVICIO A ADQUIRIR SE ENCUENTRAN EN EL ANEXO UNICO ADJUNTO AL FINAL DE ESTE CARTEL.

2) **Admisibilidad.**

- Se considerará inadmisible aquel oferente que no se encuentre **inscrito** y **al día** con el pago de las obligaciones de la Caja Costarricense de Seguro Social (CCSS) **el día de la apertura**, de conformidad con el artículo 31 reformado de la Ley Orgánica de la CCSS y artículo 65 R.L.C.A.

- La Administración verificará, mediante los medios electrónicos dispuestos para este fin, que el oferente se encuentre al día con el pago de FODESAF y del impuesto a las Sociedades, en este último caso cuando se trate de Personas Jurídicas. Cuando exista algún inconveniente con las páginas electrónicas para estas consultas se procederá a solicitarle al oferente que en el plazo de 3 días hábiles, presente la certificación que pruebe el pago de dichos impuestos. En caso de mantenerse la morosidad en dichos impuestos se declarará inadmisible la oferta.

- No se admiten a concurso las ofertas que incumplan con las condiciones legales y las especificaciones técnicas solicitadas.

- Toda oferta deberá suministrar la información completa y suficiente (entre ellos marcas, modelo, medidas y demás especificaciones técnicas) que permita su análisis y estudio comparativo para efectos de adjudicación. El no suministro de la información sustancial que permita verificar su ajuste a las condiciones significativas del cartel, descalificará la oferta.

- El oferente deberá presentar con su oferta una carta emitida por el fabricante de la marca del producto que ofrece, la carta no deberá ser mayor a 3 meses, y que se refiera a los siguientes aspectos:

    1) Que cuenta con un grupo de investigación sobre vulnerabilidades y amenazas informáticas.
    2) Que el oferente es canal autorizado para la venta, distribución y soporte del dispositivo ofertado.
    3) Que proveerá el código de sus firmas para demostrar la detección en base a vulnerabilidades y no en comparación de patrones y que podrá ser visible en cualquier momento desde la consola de administración para todas las firmas existentes en el IPS.
    4) Que la solución cuenta con el reconocimiento del último reporte de NSS Labs, líder en pruebas de productos de seguridad, que demuestre que la solución completa las pruebas satisfactoriamente con al menos 95% de efectividad.
    5) Que la solución de prevención a nivel de hardware cuenta con al menos la certificación ICSA Labs.

3) **Condiciones generales de la oferta.**

a. Se debe adjuntar comprobante de pago del **timbre** de **¢200,00** (Doscientos colones exactos) del Colegio de Profesionales en Ciencias Económicas (Ley 7105) extendido a la cuenta electrónica del CPCE en el Banco de Costa Rica 001-0281016-6 en colones bajo la denominación “Pago de timbres CPCECR” y el **timbre** de ¢**20,00** (Veinte colones exactos) de La

Ciudad de Las Niñas (Ley 6496)el cual deberá adjuntarlo a la oferta digital debidamente cancelado con el sello de la empresa oferente y debidamente identificado el número de la Licitación, documento que de esta forma deberá escanear e incluir en la oferta digital.

b. Los oferentes podrán concurrir a través de cualquiera de las formas de representación contenidas en el artículo 18 del R.L.C.A.

c. La **vigencia de la oferta** deberá ser igual ó mayor a **60 días hábiles** a partir de la apertura de las ofertas.

d. Garantía comercial: La garantía del producto deberá ser como mínimo de **doce meses** contra defectos de fabricación para el equipo IPS y para el software el cual tendrá derecho a todas sus actualizaciones.

e. El plazo de entrega: El plazo de entrega no podrá ser mayor a 30 días hábiles, los cuales serán efectivos a partir del día siguiente a la notificación de la orden de inicio dada por el órgano fiscalizador y previo a la notificación por medio de Comprared de la Orden de Compra emitida. Para las compras de importaciones el oferente debe manifestar en su oferta el plazo efectivo de la entrega, en DÍAS HÁBILES, indicando por separado lo siguiente:

a) El plazo en el que se hará entrega de los documentos necesarios para el trámite de exoneración ante la Proveeduría Institucional del TSE.

b) El plazo en el que se hará entrega efectiva del objeto contractural una vez recibida la exoneración. El oferente deberá considerar aquí la instalación y puesta en marcha del equipo.

c) En caso de que el contratista requiera para el desalmacenaje la suscripción de un contrato de cesión de disposición de mercancías deberá entregar la documentación necesaria dentro de ese mismo plazo.

d) Una vez que se cuente con el desalmacenaje y el contrato de cesión de derechos, los mismos se entregarán a la contratista para que proceda a hacer entrega del bien, dentro del plazo ofrecido.

e) Para efecto de adjudicación se sumará el plazo de exoneración y el plazo efectivo de entrega del bien, el cual no podrá superar los 30 días hábiles.

f. **Cláusula Penal:** De presentarse algún atraso en la entrega del objeto contractual por causas imputables al adjudicatario, se le cobrará un 1% del monto por lo entregado tardíamente, por cada día hábil de atraso en la

entrega, hasta un máximo del 25% del monto total de lo adjudicado; salvo en los casos en que el atraso obedeciere a causas no imputables al contratista o razones de fuerza mayor o caso fortuito debidamente demostrado. El monto correspondiente a la cláusula penal será descontado de la factura que se encuentre pendiente de pago, según lo dispuesto en los artículos 47 siguientes y concordantes del R.L.C.A. La ejecución de la caución o la aplicación de la cláusula penal no exime al adjudicatario de la aplicación de las demás sanciones administrativas que prevé el ordenamiento jurídico como lo son las sanciones previstas en los artículos 99 y 100 de la Ley de Contratación Administrativa y 215 del R.L.C.A, cuando corresponda.

g. El oferente en la cotización deberá indicar el desglose de los componentes en los costos de la línea que oferta, debiendo presentar los precios unitarios y totales, con las disposiciones estipuladas en los artículos 25, 26, 27 y 52 del R.L.C.A.

h. Los precios deberán ser ciertos y definitivos, sin perjuicio de eventuales revisiones. **Se cotizará la oferta libre de tributos**, debiéndose indicar a la vez el monto total de la oferta, en números y letras coincidentes.

i. El oferente deberá presentar Declaración Jurada, en la que manifieste Bajo la Fe de Juramento que no le alcanzan ninguna de las prohibiciones de los artículos 22 y 22bis de la Ley de Contratación Administrativa y que se encuentra al día con el pago de los impuestos nacionales y municipales.

j. Lugar de entrega: Será en la Sección de Infraestructura Tecnológica, del TSE, en la Sede Central.

k. **Órgano Fiscalizador:** Jefe Sección de Infraestructura de TI o quien ocupe su puesto.

l. Toda notificación de esta contratación se realizará por medio del Sistema Informático Comprared, de conformidad con el plazo para cada uno de los actos que se realicen.

m) **Modalidad y Forma de Pago:** USUAL **DE GOBIERNO.** El tiempo máximo para el pago de facturas, mediante transferencia bancaria, será de **TREINTA DÍAS NATURALES**, de conformidad con la Directriz No 033-H del 4 de marzo de 2009, publicada en el Diario Oficial La Gaceta No. 64 del 1º de abril de 2009) a partir de la presentación de la factura y una vez recibido el bien o servicio de manera definitiva.

4) **Condiciones Específicas**

a) El oferente, deberá de poseer 5 años de experiencia en la venta y soporte de equipos de seguridad de los cuales 3 años deberán de ser en el producto ofrecido. Para lo cual deberá aportar una declaración jurada.

b) El oferente deberá de poseer dos instalaciones exitosas de equipos similares a los de esta contratación, para lo cual citará las empresas, nombre y teléfono de la persona con suficiente criterio técnico para determinar el grado de satisfacción.

c) El oferente, deberá tener un técnico certificado en el producto ofrecido como mínimo con dos años de experiencia.

d) El oferente, estará **obligado** a describir de forma completa y precisa, las condiciones propias del servicio que se compromete a entregar, sin necesidad de reiterar la aceptación de las cláusulas invariables o condiciones obligatorias, cuyo cumplimiento se presume.

e) Una vez adjudicado el servicio no se aceptarán cambios en la solución propuesta, tampoco ampliaciones de los plazos de entrega, salvo que se trate de mejoras.

f) La institución se reserva el derecho de rechazar al momento de la recepción, aquel servicio que no cumpla con los requisitos de calidad, presentación y condiciones técnicas; siendo obligación del proveedor reponer el producto defectuoso en un plazo no mayor a 24 horas posteriores a la comunicación de dicha condición.

5) Adjudicación.

- El Tribunal Supremo de Elecciones, resolverá este concurso en un plazo que no podrá ser superior al doble del plazo fijado para recibir ofertas; incluyendo las prórrogas que se den. (Artículo 87 y 95 R.L.C.A.).

- Y podrá adjudicar parcialmente esta contratación, según lo establece el artículo 27 del R.L.C.A, así como aumentar las cantidades o bien declarar desierta la contratación.

6) Del Adjudicado o Contratista.

Una vez en firme el acto de adjudicación el contratista deberá tomar en cuenta lo siguiente:

a) El contratista se sujetará a las disposiciones contempladas en la normativa que rige la materia de Contratación Administrativa.

b) El contratista tiene el deber ineludible de cumplir las obligaciones laborales y de seguridad social, incluido el pago de los salarios mínimos para sus trabajadores establecido por el Ministerio de Trabajo y Seguridad Social, durante todo el periodo de ejecución contractual. La omisión de esta estipulación se tomará como causal de incumplimiento de acuerdo a la Directriz No. 34 del Poder Ejecutivo publicada en La Gaceta No. 39 del 25 de febrero del 2002, haciéndose acreedor el contratista a las sanciones

establecidas en la Ley de Contratación Administrativa y su Reglamento en éstos casos.

c) El contratista deberá aportar dentro de los 3 días hábiles posteriores a la firmeza del Acto de Adjudicación, y en el caso de resultar ser una empresa lo siguiente:

d) Certificación Original de Personería Jurídica y del Capital Social, así como de la distribución de las acciones con vigencia no menor de TRES MESES de emitida.

e) Certificación de la propiedad de las Cuotas o Acciones, con vista en los Libros de la Sociedad emitida por un Notario Público.

f) El adjudicatario se comprometerá a impartir un curso certificado del equipo instalado en el TSE, para dos funcionarios de este organismo, este curso se deberá de impartir una vez que este debidamente instalado y en funcionamiento el equipo a satisfacción del Órgano fiscalizador.

g) De los anteriores documentos el adjudicatario podrá presentar copia certificada siempre y cuando indique expresamente el número de expediente de la contratación en la que se encuentran los originales dentro de esta Proveeduría, y que los mismos no tienen más de 1 año de haber sido emitidos y deberá declarar bajo de Fe de Juramento que los datos consignados en las copias de dichas certificaciones se mantienen invariables, salvo que esta información conste en el expediente electrónico del adjudicatario en el Registro de Proveedores de la Dirección General de Administración de Bienes y Contratación Administrativa.

7) Sistema de valoración y comparación

Con las ofertas admisibles para una eventual adjudicación, se procederá a realizar la calificación de cada oferta, aplicando la Metodología de Evaluación siguiente:

7.1 Metodología de Evaluación

Precio 100%

Las ofertas que cumplan con todos los requisitos solicitados serán evaluadas de la siguiente manera:

El puntaje se calculará de acuerdo a la razón del precio menor dividido entre cada uno de los precios de las ofertas en estudio, multiplicado por 100.

$$\text{Puntaje} = \frac{\text{Menor Precio}}{\text{Precio de la oferta en estudio}} \times 100$$

Notas:

- Las ofertas deberán cotizarse preferiblemente en colones, moneda de Costa Rica. Sin embargo, si la oferta se cotiza en dólares de los Estados Unidos, para efectos de comparación de las ofertas, la conversión a colones se realizará utilizando el tipo de cambio de venta oficial establecido por el Banco Central de Costa Rica al día de la apertura de las ofertas. Para efectos de cancelación de facturas de ofertas cotizadas en dólares se utilizará el tipo de cambio venta del colón con respecto al dólar calculado por el Banco Central de Costa Rica vigente a la fecha del pago efectivo.

- El precio se deberá cotizar y se entenderá para todos los efectos, libre de los impuestos. El oferente deberá indicar el desglose porcentual del factor precio en mano de obra, insumos, gastos administrativos y utilidad (P= MO+I+GA+U) que componen el precio cotizado, de manera que permita revisar y resolver en forma rápida y correcta las solicitudes de reajuste que eventualmente formule el contratista.

8) Criterio de desempate de las ofertas

De conformidad con el artículo 20 de la Ley 8262, se establece como mecanismo de desempate para la adjudicación de la oferta el siguiente:

- Se preferirán a la **PYME** de Producción Nacional.

- Cuando existan dos o más PYME nacionales participando en un mismo procedimiento de contratación administrativa, la Administración preferirá a aquella que tenga mayor valor agregado nacional calculado con la fórmula establecida en el Decreto Ejecutivo número 33305-MEIC-H, denominado Reglamento Especial para la Promoción de las PYMES en la Compras de Bienes y Servicios de la Administración."

- De persistir el empate, la Proveeduría establecerá un sistema de rifa entre las ofertas que se encuentren en esa condición en presencia de un asesor legal, el analista encargado y los representantes legales de cada una de las empresas, previa convocatoria. Ante la inasistencia de alguno de los representantes, un funcionario de la Proveeduría Institucional tomará su lugar en el sorteo, en el cual se utilizarán papelitos de igual tamaño, color y uno de ellos tendrá la palabra ganador.

La no asistencia de las partes no impedirá la realización de la rifa. De lo actuado se levantará un acta que se incorporará al expediente.

9) Garantía de cumplimiento.

Quien resulte adjudicatario está en el deber de asegurar la correcta ejecución del contrato y por tal razón rendirá una garantía de cumplimiento en la Proveeduría, dentro de los cinco (5) días hábiles posteriores a la fecha en que hubiese recibido requerimiento por escrito de la Proveeduría del Tribunal Supremo de Elecciones. Esta garantía equivaldrá al 5% del monto total adjudicado y tendrá un término de validez de sesenta (60) días naturales que se contarán a partir de la entrega conforme del producto.

En caso rendir garantía de cumplimiento en efectivo, deberá aportar el número de licitación para que la Contaduría emita dos comprobantes, un original para el adjudicatario para que posteriormente solicite la devolución correspondiente, y una copia que adjudicatario debe entregar en la Proveeduría. En el caso que sea en colones, puede hacer el depósito en la cuenta N° 001-0132062-9 del Banco de Costa Rica y cuando se trate de dólares, puede hacer el depósito en la cuenta No. 100-02-000-621441, del Banco Nacional, en cualquier caso, debe presentar el recibo emitido por el banco en la Contaduría (Área de Tesorería) para que esta a su vez emita los comprobantes indicados en este punto.

En el caso de aportar la garantía en una modalidad distinta al efectivo, deberá presentar el documento original y una fotocopia, la Contaduría emitirá dos comprobantes, el original es para el adjudicatario y una copia es para adjuntarle la fotocopia del documento de garantía para que el adjudicatario los entregue en la Proveeduría.

10) Sanciones: Conforme lo establece el capítulo X de la Ley de Contratación Administrativa. Los contratistas que durante el curso de los procedimientos de contratación, incurran en las causales previstas en dicho capítulo, serán sancionados con apercibimiento e inhabilitación, según corresponda, de conformidad con lo establecido en el Art. 215 del Reglamento a la Ley de Contratación Administrativa.

11) Cesión de la Contratación: Los derechos y obligaciones derivados de un contrato en ejecución o listo para iniciarse, podrán ser cedidos a un tercero, siempre y cuando no se trate de una obligación personalísima. En todo caso, la cesión debe ser autorizada por la Administración mediante acto debidamente razonado. Cuando la sesión corresponda a más de un 50% del objeto del contrato, independientemente del avance en su ejecución, deberá ser autorizada por la Contraloría General de la República. (Art. 209 del R.L.C.A.)

12) Formalización: Se advierte a los participantes que cuando la estimación de la adjudicación se encuentre sujeta de aprobación interna por parte del Departamento Legal del Tribunal Supremo de Elecciones o requiera refrendo por parte de la Contraloría General de la República, se deberá elaborar el contrato respectivo, de acuerdo con el Reglamento de Refrendos de las Contrataciones Administrativas, emitido por el Ente Rector, publicado en La Gaceta No. 202 del 22 de octubre de 2007.

Antes de la suscripción del contrato el adjudicatario deberá rendir la garantía de cumplimiento en los términos establecidos en el presente cartel.

13) Timbres y Pedido: El adjudicatario deberá cancelar el pago de especies fiscales equivalente al 0,25% del monto adjudicado. La Orden de Compra, se notificará mediante Comprared 2.0

_____

Lic. Ronny Jiménez Padilla
Subproveedor

ANEXO

ESPECIFICACIONES TECNICAS

1. El proceso de actualización de vulnerabilidades y otros aspectos del mantenimiento (como parches y upgrades) deberá ser mediante el sitio Web del fabricante del producto y de varias formas: por medio del propio producto, bajando del sitio Web un archivo de actualización o bien automáticamente.

2. La solución de prevención a nivel de hardware debe contar con al menos la certificación ICSA Labs, organización que se encarga de la certificación y testeo de productos de seguridad informática, para lo cual deberá presentar la documentación respectiva.

3. La solución de prevención debe poseer licenciamiento ilimitado de usuarios y Host, para lo cual se deberá presentar la documentación respectiva.

4. La solución de administración debe permitir mecanismos de integración en forma de APIs abiertas, para lo cual deberá de presentar la documentación respectiva con cuales tecnologías se cumple con este modo de integración.

A)Especificaciones para la prevención de intrusiones (dispositivo);

Monitorear el tráfico de red para prevenir ataques, port scanning, ataques de denegación de servicio y tráfico malicioso.

Funcionalidades Básicas

1. El dispositivo debe ser una solución de software y hardware basado en appliances, el cual tenga la capacidad de realizar su monitoreo y prevención de manera en línea además de ser de un sólo fabricante.

2. El monitoreo del dispositivo debe ser transparente para los usuarios y operar en la capa 2 del modelo de OSI, por lo que las interfaces no requieren de una dirección IP ni una direccion MAC.

3. El dispositivo podrá configurarse en modo transparente; es decir, de detección en línea, pero sin bloquear tráfico. El sistema sólo alerta que eventos serían bloqueados.

4. El dispositivo debe permitir la configuración de modo transparente para todo el tráfico o apenas para paquetes especificados por dirección IP, protocolo, VLAN ID incluyendo frames 802.1q.

5. El dispositivo debe permitir la creación de reglas y filtros de acceso.

6. El dispositivo debe ser capaz de indicar a un dispositivo de tipo FW, en respuesta a un ataque, la adición de reglas para mitigar el ataque apropiadamente de manera escalonada en las dos capas de seguridad, IPS y FW.

7. El dispositivo debe soportar un motor de detección que inspeccione no solo los detalles de la capa de red, además información en las cabeceras de los paquetes, a través de una gama amplia de protocolos.

8. El dispositivo debe tener la capacidad de detectar tráfico anómalo o vulnerabilidades en las siguientes aplicaciones Instant Messenger y P2P: AOL Instant Messenger; MSN Messenger; Yahoo! Messenger; ICQ; Gnutella; Kazaa; eDonkey; BitTorrent; SoulSeek.

9. El dispositivo debe ser capaz de inspeccionar el tráfico asociado a distintos segmentos de redes diferentes (en lugar de tener una sola politica por interfaz).

10. El dispositivo debe ser resistente a diversas tecnicas de URL obfuscation en ataques basados en HTML.

11. El dispositivo deberá soportar funcionamiento pasivo como un IDS (sistema de detección de intrusos), con alertas de ataque, tráfico malicioso o no deseado, sin interferir con el tráfico.

12. El dispositivo debe soportar reglas de detección basada en un leguaje abierto permitiendo a los usuarios crear sus propias reglas.

13. El dispositivo debe soportar los siguientes tipos de respuestas: bloquear, ignorar, guardar en un log, envíar correo eléctronico, SNMP, respuestas definidas por el usuario, cambios de configuración a equipos de seguridad o de red de terceros, sugerencia de cambios a la política en base al análisis de impacto de un evento.

14. El dispositivo debe soportar monitoreo stateful inspection.

15. Las interfaces del dispositivo deben poder censar tráfico en modo stealth, sin stack de TCP/IP en la interfaz.

16. El dispositivo deberá soportar la combinación de las modalidades IDS (pasivo) e IPS (en línea) dentro de un mismo equipo.

17. El dispositivo debe de soportar la identificación y protección de ataques en protocolos de Voice over IP (VoIP), tales como: SIP, H.323, H.225, H.245.

18. El dispositivo debe contar con mínimo 8 interfaces de 10/100/1000 mbps para soportar fibra o cobre y proporcionar como mínimo un throughput de 512 Mbps para el análisis del tráfico que cruza en el segmento de red.

19. El dispositivo debe contar con 1 interfaces 10/100/1000 mbps para para la comunicación con el sistema de administración de correlación de eventos.

20. El dispositivo debe proveer protección contra spywares.

21. El dispositivo debe estar basado sobre firmas en vulnerabilidades permitiendo la detección de ataques desconocidos o variaciones de ataques conocidos.

22. El dispositivo debe de permitir el paso del tráfico en el segmento de red sin afectar el funcionamiento de la red (Bypass), en caso de una falla eléctrica, este debe ser interno.

23. El dispositivo debe de soportar alta disponibilidad en varios modos; activo-failover, activo-activo, para lo cual deberá permitir un ruteo asimétrico.

24. El dispositivo debe de proveer monitoreo de segmentos de red en modo promiscuo analizando encabezamiento (header) y el área de datos (payload) de los paquetes que transitan en la red (deep packet inspection), detectando ataques y tráfico no autorizado o sospechoso.

25. El dispositivo debe de prevenir la transmisión de los informes de inteligencia del spyware desde aquellos puestos de trabajo que ya están infectados, bloqueando automáticamente la comunicación activa de programas spyware.

26. El dispositivo debe contener una tecnología de identificación de spyware el cual permita el bloqueo de programas spyware tanto conocidos como desconocidos, desde las aplicaciones a nivel de red antes de que éstos sean descargados por el usuario final.

27. El dispositivo debe permitir tener la flexibilidad de controlar políticas a nivel de dispositivo, puerto, VLAN y direcciones IP.

28. El dispositivo debe proveer múltiples opciones para responder eventos, tales como: monitoreo de paquetes; bloqueo de tráfico; reemplazo del payload del paquete; captura de paquete.

29. El dispositivo debe permitir la funcionalidad de gestión SNMP e integrarse a productos de red de terceros para proporcionar indicadores clave de estado operacional a grupos de operaciones de red y de operaciones de seguridad.

30. El dispositivo debe permitir soportar monitoreo en redes MPLS.

31. El dispositivo debe tener la habilidad de decodificar e inspeccionar todos los protocolos apoyados IPv4, y cualquier ataque asociado o mal uso incluso si está encapsulado en IPv6.

32. El dispositivo debe tener la capacidad de utilizar al menos estas técnicas de detección de ataques:

    a. Port Assignment, Port Following, Port Variability, Protocol Tunneling Recognition, Heuristics, Protocol Análisis, Aplication-layer Pre-processing, Reconnaissance, RFC Compliance Checking, Protocol Anomaly Detection, TCP Reassembly, Flow Reassembly, Protocol Modeling.

33. El dispositivo debe de poder capturar de tráfico para el análisis de evidencia en formato soportado por TCPDump y .ENC (estándar para el software de análisis de protocolos).

34. El dispositivo debe de neutralizar los paquetes en tiempo real eliminando o neutralizando los paquetes con el código malicioso mientras deja pasar los paquetes legítimos.

35. El dispositivo debe soportar revisiones automatizadas de contenido seguridad y actualizaciones de productos a través de Internet.

36. El dispositivo debe ofrecer una latencia máxima de 1 milisegundo.

37. El dispositivo debe soportar la capacidad de analizar contenido en archivos atachados y conversaciones a nivel de chat.

38. El dispositivo debe proteger contra ataques sobre aplicaciones Web como: shell command injections, Server-site injection, cross-site scripting, directory traversal.

39. El dispositivo debe de contar con protección para sistemas SCADA y tener la capacidad de proteger al menos los siguientes protocolos como DNP3, MODBUS, ICCP, MMS, con al menos 50 firmas/filtros en total.

40. El dispositivo debe ser capaz de recopilar información pasiva de los hosts de la red y sus actividades, tales como: sistema operativo; servicios, puertos abiertos; aplicaciones y vulnerabilidades, permitiendo la correlación de datos, eliminación de falsos positivos y políticas de cumplimiento.

41. El dispositivo debe ser capaz de detectar pasivamente los servicios pre-definidos como FTP, http, POP3, Telnet, etc., así como servicios personalizados.

42. El dispositivo debe ser capaz de esperar pasivamente la recopilación de información de identidad de usuarios y asignación de direcciones IP. (sin necesidad de hardware o software separado).

43. El dispositivo debe ser capaz de identificar todos los hosts que presenten un atributo o condición especifica de incumplimiento de la política.

44. El dispositivo debe ser capaz de proporcionar mayor visibilidad sobre como se consume el ancho de banda, permitiendo ayudar en la solución de problemas de interrupciones o degradaciones de rendimiento de la red.

45. El dispositivo debe proporcionar la capacidad inteligente para correlacionar los eventos de intrusión priorizándolo por tipo de bandera de impacto, en donde se categorice por: 0 Unknown; 1 Vulnerable; 2 Potentially Vulnerable; 3 Currently Not Vulnerable; 4 Unknown Target.

46. El dispositivo debe soportar integración a través del directorio activo y/o LDAP para determinar el comportamiento de la red a través de direcciones IP asociadas a los eventos sospechosos.

47. El dispositivo debe proporcionar una completa visión del comportamiento de la red para detectar nuevas amenazas, incluyendo la capacidad de establecer líneas de base de tráfico a través de técnicas de flujos.

48. El dispositivo debe ser capaz de reducir significativamente el esfuerzo del operador y la aceleración de respuesta a las amenazas por dar prioridad a las alertas de forma automática.

49. El dispositivo debe ser capaz de proporcionar de forma automática los adecuados controles permitiendo la protección el tráfico enviado a través de puertos de comunicación no estándares.

50. El dispositivo debe ser capaz de esperar pasivamente la recopilación de información sobre los flujos de sesión para todos los hosts, incluyendo el tiempo inicio/fin, puertos, servicios y cantidad de datos.

51. El dispositivo debe soportar un sistema de correlación de eventos y detección de anomalías con las siguientes características:

    a. Permitir un análisis dinámico y en tiempo real para crear un mapa de la red monitoreada, incluyendo al menos lo siguiente parámetros: Redes existentes; Host activos; Nuevos host o servers en la red; Nuevas MAC address en la red; Maquinas virtuales nuevas o existentes; Sistema operativo de cada uno de los host identificados; Servicios activos de cada uno de los host identificados; Applicaciones activas de cada uno de los host identificados; Vulnerabilidades de cada uno de los host identificados.

52. Deberá ser capaz de agregar a su base de datos de conocimiento los resultados de un análisis de vulnerabilidades realizado por un analizador de vulnerabilidades (escaner) del mismo fabricante e incluido como parte del mismo módulo de correlación.

53. Deberá ser capaz de hacer recomendación de afinación (tuning) de políticas en base a la información aprendida de la red, mostrando un registro de las reglas recomendadas.

54. Deberá ser capaz de crear un perfil de tráfico de la red para crear baselines del tráfico existente en la red.

55. Deberá poder crear perfiles de tráfico con reglas específicas para monitorear el tráfico entre dos host de la red y crear una alarma cuando cierto umbral sea rebasado.

56. Deberá ser capaz de detectar anomalías de tráfico en la red, en base a los patrones de tráfico identificados.

57. Deberá de crear una bandera de impacto por cada uno de los host a través de la información aprendida de la red, así como las vulnerabilidades por cada uno de los eventos de seguridad.

58. Deberá contar al menos con las siguientes banderas de impacto para cada uno de los eventos del IPS, independientemente de la criticidad de la

vulnerabilidad en el exterior: Vulnerable; No Vulnerable; Posible Vulnerabilidad Existente.

59. Deberá ser capaz de crear perfiles de cumplimiento con alguna normativa de seguridad, para emitir una alarma cuando algunos de los servicios no permitidos por una normativa de seguridad sea utilizado en el segmento de red acotado por la normativa de seguridad.

60. Deberá ser capaz de realizar un escaneo de vulnerabilidades a los host de la red para validar la existencia de las vulnerabilidades o como una respuesta a un incidene, por ejemplo al detectar un nuevo host en la red, deberá escanearlo inmediatamente.

61. Deberá permitir una integración automática para realizar un cambio de configuración o enviar información a módulos de terceros como: Scanners de vulnerabilidades; SEM/SIEM systems; Firewall; Routers; Switches; Sistemas de patch management; Wireless Access Point; NAC servers; Ticket management Systems.

62. Deberá permitir reportes detallados sobre lo siguiente: Nuevos host en la red; Vulnerabiidades existentes en la red; Servicios existentes en la red; Anomalias de tráfico; Perfiles de tráfico; Sistemas operativos existentes en la red; Vulnerabilidades por cada host; Uso de tráfico por aplicación; Uso de tráfico por usuario; Uso de tráfico por host; Uso de tráfico por servicio; Eventos de seguridad por impacto en la red; Eventos de seguridad por criticidad de la vulnerabilidad.

63. Deberá ser capaz a través de una versión virtual, monitorear y asegurar una granja de servidores virtuales, sin necesidad de instalar un agente a cada servidor virtual utilizado.

64. Deberá ser capaz de integrarse con herramientas de terceros, para crear un mapa geo-gráfico de la red.

65. Deberá ser capaz de crear un mapa de flujo de tráfico entre host de la red, para guardar registro de la cantidad de tráfico entre los dispositivos de la red.

66. Deberá identificar vulnerabilidades de los host de la red en tiempo real y sin necesidad de correr un análisis de vulnerabilidades

67. El dispositivo deberá incluir un sistema de integración con directorio activo, del mismo fabricante, que provea las siguientes características:

68. Deberá permitir la integración con el directorio activo de la red para tener un mapeo de usuario e IP utilizada actualmente.

69. Deberá permitir tener la información de contacto de los usuarios que están siendo atacados.

70. Los eventos de seguridad reportados deberán mostrar el usuario que esta generando o recibiendo el ataque y generar una alerta o tomar acciones en base al perfil del usuario en cuestión.

71. Deberá de poder generar un mapa de eventos de seguridad generados/recibidos por usuario.

72. Deberá de poder generar un mapa de tráfico generado/recibido por usuario.

73. Deberá ser capaz de mantener un mapa de los usuarios, ip actual, tipo de aplicación usada, y un historial de las IPS que ese usuario ha usado en el tiempo.

74. El dispositivo debe contar con al menos las siguientes categorías de reglas: Backdoors; DDoS; DoS; Exploit; P2P; Phising-Spam; Scada; Shellcode; Spyware; Web-PHP; SQL; VoIP; WEB-CGI; Sensitive-Data; RPC; Botnet.

75. El dispositivo debe poder soportar reglas por plataforma tal como: Apple; Cisco; Compaq; HP; IBM; Juniper; Microsoft; Nokia; RedHat; Suse; Sun.

76. El dispositivo debe de soportar reset de la sesión TCP cuando se utiliza en modo pasivo.

77. El dispositivo debe soportar reglas de contenido con al menos los siguientes parámetros: Message; Reference; Action; Protocol; SID; GID; Direction, Source IP, Destination IP, Source port; Destination port; Rule overhead, Metadata.

78. El dispositivo debe incluir al menos la capacidad de detectar a través de firmas de análisis de contenido: correo electrónico, números de tarjeta de crédito.

79. El dispositivo debe poder actualizar su sistema operativo y actualizarlo en caliente sin detener el flujo de tráfico (Hitless OS upgrades) que pasa por él, esto con el objetivo de no perder comunicación durante los procesos de actualización del sistema.

80. El dispositivo debe de neutralizar los paquetes en tiempo real eliminando o neutralizando los paquetes con el código malicioso mientras deja pasar los paquetes legítimos.

81. El dispositivo deberá de soportar syslog para eventos de filtrado y errores del sistema.

82. El dispositivo debe tener la capacidad de ser administrado a través de conexiones SSH, CLI y HTTPS.

83. El dispositivo deberá de soportar SNMP v2 y v3.

84. El dispositivo debe contar con la capacidad de medir el tráfico que pasa por las diferentes interfaces del sistema y poder generar graficas de tráfico de las interfaces mediante consola de reportes.

85. El dispositivo deberá tener una funcionalidad de “packet level” para realizar actividades de análisis forense.

86. El dispositivo deberá de proveer protección contra DoS y DDoS (inundación de ataques tipo “SYN DOS”).

87. El dispositivo deberá incluir protección contra virus y gusanos de manera integrada, además deberá ser habilitado o deshabilitada desde la consola de administración.

88. El dispositivo debe de soportar inspección de tráfico en GRE.

89. El dispositivo debe contar con un puerto de consola serial, que permita la configuración mediante línea de comandos.

90. El dispositivo deber contar con cobertura de filtros que protejan las vulnerabilidades de internet Explorer.

91. El dispositivo debe contener redundancia en fuentes para prevenir fallas graves en este hardware. Trabajar con voltaje de 100-127V y/o 220/240V, una temperatura de operación de 10°C – 35°C y una humedad relativa 95% a 23°C a 40°C (73°F a 104°F)

Especificaciones para administración de seguridad (DC):
Administrar, correlacionar y priorizar eventos permitiendo; seguimiento en tiempo real de ataques o usos indebidos, tratamiento de eventos, creación automática de incidentes y excepciones, identificación de falsos positivos y la integración de eventos generados por dispositivos de terceros.

B) Funcionalidades Básicas

1. El sistema de administración centralizada debe tener la capacidad de desempeñar el análisis automatizado de impactos al correlacionar eventos IDS & IPS con el estado de la vulnerabilidad, la información del sistema operativo para determinar la posibilidad de éxito contra el objetivo.

2. El sistema de administración centralizada debe soportar administración de productos de análisis de vulnerabilidades.

3. El sistema de administración centralizada debe soportar ajustes dinámicos de severidad en los ataques como resultado de la correlación de eventos.

4. El sistema de administración centralizada debe soportar la correlación de datos de vulnerabilidades, soporte a la correlación de patrones de ataques (múltiples eventos identificados como un único ataque).

5. El sistema de administración centralizada debe soportar reportes en formato texto y gráfico, con exportación en los formatos HTML, PDF e CSV.

6. El sistema de administración debe soportar la correlación de patrones de ataques (múltiples eventos identificados como un único ataque). Esto se refiere a que el equipo ofertado sea lo suficientemente inteligente para que pueda identificar eventos similares y los pueda relacionar como una sola anomalía, con aplicaciones del mismo fabricante.

7. El sistema de administración centralizada debe soportar consola remota con interfaz gráfica, consola remota web en formato gráfico para el uso en modo de consulta, perfiles diferentes de usuarios.

8. El sistema de administración centralizada debe soportar auditoria de las actividades de los usuarios.

9. El sistema de administración centralizada debe ser un appliance.

10. El sistema de administración centralizada debe contar con al menos 2 GB de memoria RAM, con un almacenamiento de al menos 100 GB.

11. El sistema de administración debe soportar la administración de por lo menos 10 sistemas IPS sin necesidad de actualizar el software o licenciamiento.

12. El sistema de administración debe soportar un máximo de 20 millones de eventos.

13. El sistema de administración debe soportar un máximo de 2000 eventos por segundo.

14. El sistema de administración centralizada debe soportar actualización remota de los dispositivos tanto a nivel de hardware como de software.

15. El sistema de administración debe generar reportes en forma automática y enviarlos a una cuenta de correo electrónico para agilizar el proceso de análisis.

16. El sistema de administración centralizada debe contar con información detallada de ayuda para firmas. Cuando aparece una amenaza en la pantalla de la consola, el usuario debe tener la capacidad de visualizar información detallada acerca de la vulnerabilidad hacia la cual está dirigida la amenaza. Ello debe incluir una explicación de la vulnerabilidad, de los sistemas que pueden verse afectados, de información sobre falsos positivos, de información CVE, de explicaciones para parcheo o restauración y de URLs.

17. Es importante que el sistema de administración cuente con herramientas integradas para tener visibilidad en forma de graficas en tiempo real e historial sobre el estado de salud, como mínimo de: CPU, interfaces, memoria, performance, disco, temperatura.

18. El sistema de administración centralizada debe tener la posibilidad de realizar análisis de inteligencia con facilidad. Ello incluye análisis basados en el contexto lógico del evento siendo evaluado. Entre los ejemplos se encuentran el retorno de todos los eventos desde el IP fuente elegido, el retorno de todas las vulnerabilidades asociadas con el puerto objetivo elegido, etc. Deben incluirse mecanismos capaces de desempeñar los ejemplos anteriores, y más. El usuario debe poder navegar y analizar, con facilidad, más de un millón de eventos al día.

19. El sistema de administración centralizada debe poder correlacionar eventos desde el producto de valoración de vulnerabilidades.

20. El sistema de administración centralizada debe contar con soporte para la personalización de la pantalla de la consola. El usuario debe poder personalizar el contenido de la pantalla y los filtros con base en la dirección IP, rango de red, protocolo, tipo de evento, nombre de evento y servicio, para después guardar dicha configuración bajo nombres personalizados para su uso futuro.

21. El sistema de administración centralizada deberá ser capaz de integrarse con tecnologías de seguridad de terceros (Firewall, IPS Wireless, Switches, Routers, Patch Management System, AV Consoles, etc) para generar acciones yo configuraciones necesarias para remediación de incidentes de seguridad.

22. El sistema de administración centralizada debe incluir reportes previamente definidos. La consola debe tener la capacidad de producir métricas gráficas y reportes de comparación con base en segmentos de tiempo. La información en los reportes debe estar disponible para un grupo de activos, para todo un sitio o para toda una empresa. Asimismo, el usuario debe poder llegar hasta estos reportes para visualizar los detalles pertinentes.

23. El sistema de administración debe proporcionar la capacidad de activar, desactiva y modificar las reglas individuales, por grupos o categoría de normas.

24. El sistema de administración debe proporcionar la capacidad de seleccionar informes pre-definidos y la posibilidad completa de personalización y generación de nuevos reportes.

25. El sistema de administración debe incluir las capacidades de flujo de trabajo para la gestión del ciclo de vida completo de un evento, des la notificación inicial a través de cualquier respuesta y resolución de las actividades que sean necesarias.

26. El sistema de administración debe ser compatible con multiples opciones para responder automáticamente a las amenazas detectas ya sea por alertas automatizados y/o remediación del firewall.

27. El sistema de administración debe de tener una interface de red 10/100/1000 para la administración.

28. El sistema de administración debe contar un una fuente de poder, además debe trabajar con voltaje de 110V y 220V, 50/60Hz una temperatura de operación de 10°C – 35°C y una humedad relativa de 90% @ 82°F (28°C)

29. El sistema de administración debe proveer análisis de tráfico sobre las reglas de control de velocidad aplicadas en los dispositivos de prevención con reportes mostrando tráfico por horas, días, o fechas específicas indicadas por el operador.

30. El sistema de administración debe contar con soporte para la personalización de la pantalla de la consola. El usuario debe poder personalizar el contenido de la pantalla en base en la dirección IP, rango de red, protocolo, tipo de evento, nombre de evento y servicio, para después guardar dicha configuración bajo nombres personalizados para su uso futuro.

31. El sistema de administración debe soporta roles múltiples para el usuario dentro de los cuales deben estar: Administrator; Maintenance User; Policy & Response Administrator; Intrusio Event Analyst; Real-Time Network Awareness. Estos roles deben dar lugar o prevenir el uso de ciertos privilegios de parte del usuario. Los privilegios deben incluir una gama de funciones administrativas de reporte o visualización.

32. El sistema de administración debe incluir un mecanismo de integración, en forma de APIs abiertas y / o interfaces estándar, para permitir una respuesta automática a las amenazas de los componentes externos y las aplicaciones de recuperación, tales como routers, firewalls, sistemas de gestión de parches, etc.

33. El sistema de administración debe incluir un mecanismo de integración, en forma de APIs abiertas y / o interfaces estándar, para permitir a los eventos y registro de datos sean compartidos con la red externa y las aplicaciones de gestión de seguridad, tales como sistemas de ticketing, SIEM, plataformas de sistemas de gestión y registro de las herramientas de gestión.

34. El sistema de administración debe incluir un mecanismo de integración, en forma de APIs abiertas y / o interfaces estándar, para recibir información de fuentes externas, como bases de datos de gestión de configuración, herramientas de administración de vulnerabilidades y sistemas de gestión de parches, de correlación de amenazas y política de TI propósitos de cumplimiento.

35. El sistema de administración debe incluir un mecanismo de integración, en forma de APIs abiertas y / o interfaces estándar, para exportar información SNMP para sistemas de gestión de la red.

36. El sistema de administración debe incluir un mecanismo de integración, en forma de APIs abiertas y / o interfaces estándar, para obtener inteligencia de la red (es decir, NetFlow) de routers y switches Cisco.