CONTRATO 086/2017

Contrato de adquisición de una licencia firewall, que celebran por una parte el Estado de Campeche, representado en este acto por el ingeniero Gustavo Manuel Ortiz González en su carácter de Secretario de Administración e Innovación Gubernamental, a quien en lo sucesivo se le denominará "El Estado" y por la otra parte la persona moral Estrategias en Tecnología Corporativa, S.A. de C.V., representada en este acto por el ingeniero Juan Gualberto Cabrera Pérez, a quien en lo sucesivo se denominará "El Proveedor" al tenor de las siguientes declaraciones y cláusulas:

Declaraciones

1.- Declara "El Estado" a través de su representante:

1.1.- Que de acuerdo con los artículos 40, 41, 42 y 43 de la Constitución Política de los Estados Unidos Mexicanos, 1, 2, 4, 23, 24, 26, 59, 71 fracciones XV inciso a) y XXXI y 72 de la Constitución Política del Estado de Campeche, 1, 2, 12 y 16 de la Ley Orgánica de la Administración Pública del Estado de Campeche; Campeche es un estado libre y soberano que forma parte integrante de la Federación, cuya administración pública centralizada se encuentra conformada por las dependencias que lo integran, estando facultados sus titulares para que en representación del Estado de Campeche suscriban convenios, contratos y demás actos jurídicos con la Federación, con los otros estados de la república, con los ayuntamientos de los municipios de la entidad y con personas físicas y morales.

1.2.- Que el ingeniero Gustavo Manuel Ortiz González, comparece en su carácter de Secretario de Administración e Innovación Gubernamental, personalidad que acredita con el nombramiento expedido a su favor por el ejecutivo estatal el día 03 de noviembre de 2015 y está facultado para celebrar el presente instrumento según lo previsto por los artículos 4, 16 fracción III y 23 fracciones X, XI y XXIII de la Ley Orgánica de la Administración Pública del Estado de Campeche.

1.3.- Que mediante oficio número SSPCAM/RF/0604/2017 de fecha 19 de junio de 2017, el Dr. Jorge de Jesús Argáez Uribe, Secretario de Seguridad Pública, solicitó la adquisición de una licencia firewall, para destinarse a la dependencia a su cargo.

1.4.- Que según a lo establecido por los artículos 1, 3, 6, 21, 22, 33, 35 y demás aplicables de la Ley de Adquisiciones, Arrendamientos y Prestación de Servicios Relacionados con Bienes Muebles del Estado de Campeche, en relación con los artículos 1°, 25 fracción VII, 49 segundo párrafo y demás aplicables de la Ley de Coordinación Fiscal, 1 y 2 fracción IV, 8 y demás concordantes de la Ley de Presupuesto de Egresos del Estado de Campeche para el Ejercicio Fiscal 2017; la presente operación de adquisición se efectúa mediante la modalidad de adjudicación directa.

1.5.- Que la erogación de la presente compra se encuentra prevista y será cubierta con recursos del Fondo de Aportaciones para la Seguridad Pública de los Estados y del Distrito Federal (FASP), mediante el siguiente esquema programático: **Ejercicio Fiscal** 2015, **Programa con Prioridad Nacional de Seguridad Pública:** Fortalecimiento de Programas Prioritarios de las Instituciones Estatales de Seguridad Pública e Impartición de Justicia; **Capítulo.- 5000:** Bienes Muebles, Inmuebles e Intangibles.

1.6.- Que tiene establecido su domicilio en la calle 8, sin número, colonia Centro, de la ciudad de San Francisco de Campeche, Campeche, mismo que señala para los fines y efectos legales de este contrato.

2.- Declara "El Proveedor" a través de su representante:

2.1.- Ser una sociedad anónima de capital variable con capacidad de comercializar los bienes que en este acto requiere "El Estado", constituida bajo escritura pública número 1,391 de fecha 14 de julio 2006, otorgada ante la fe del Licenciado Mario Humberto Torres Verdín, notario público número 128 de Guadalajara, Jalisco, inscrita en el Registro Público de la Propiedad y de Comercio del Estado de Jalisco, mediante el folio mercantil electrónico número 32134 * 1, de fecha 11 de septiembre de 2006.

OPERADO CON RECURSOS FASP 2015

2.2.- Que su representante legal es el ingeniero Juan Gualberto Cabrera Pérez, quien se identifica con su credencial para votar con folio 0106067747716, expedida por el Instituto Nacional Electoral, y acredita su personalidad con el testimonio de la escritura pública número 3,616 de fecha 14 de junio de 2013, pasada ante la fe del Licenciado Mario Humberto Torres Verdin, notario público número 128 de la ciudad de Guadalajara, Jalisco, inscrita en el Registro Público de la Propiedad y de Comercio del Estado de Jalisco, mediante el folio mercantil electrónico número 32134 * 1, de fecha 20 de junio de 2013.

2.3.- Que tiene capacidad jurídica para contratar y reúne las condiciones técnicas y económicas para obligarse a proveer los bienes objeto de este contrato.

2.4.- Que conoce el contenido y los requisitos que establece la Ley de Adquisiciones, Arrendamientos y Prestación de Servicios Relacionados con Bienes Muebles del Estado de Campeche.

2.5.- Que tiene establecido su domicilio en Avenida Mariano Otero N1249-12 GWTC Torre Atlántico Colonia Rinconada del Bosque, Guadalajara, Jalisco, mismo que señala para todos los fines y efectos legales de este contrato.

2.6.- Que su número del padrón de proveedores es: 02895 expedido el 04 de mayo de 2017.

2.7.- Que su Registro Federal de Contribuyentes es: ETC060715147.

3.- De ambas partes:

3.1.- Que en virtud de lo declarado anteriormente y con fundamento en lo previsto por los artículos 39, 40, 41, 46, 47, 50, 51, 52, 53, 58, 60 y demás relativos aplicables de la Ley de Adquisiciones, Arrendamientos y Prestación de Servicios Relacionados con Bienes Muebles del Estado de Campeche, así como por los artículos 1755, 1756, 1757, 1758, 1759, 1760, 2135, 2136, 2147, 2148, 2150, 2154, 2168, 2182, 2183, 2184, 2190 y 2192 del Código Civil del Estado de Campeche, han decidido formalizar la compraventa al tenor de las siguientes:

Cláusulas

Primera.- Objeto: "El Estado" encomienda a "El Proveedor" a entregar el bien y servicio, que a continuación se describe, acatando para ello lo establecido en el presente contrato y anexo único, el cual se detalla a continuación

Cant.	Concepto	Unidad de medida	Precio unitario	Importe
1	**Renovación de licencias Fortinet** tipo: UTM Bundle (24x7 FortiCare plus NGFW, AV, Web Filtering and Antispam Services). Fecha de término: 30/Junio/2018 Para equipos con número de serie: *FGT60D4613054250 *FGT60D4613057081 *FGT90D3Z14017471 *FGT90D3Z14017487 Alcances: 1. Mesa de ayuda 5x8 por 12 meses. 2. Soporte telefónico y en sitio tipo Plata 5x8 por 12 meses.	Licencia	$154,653.00	$154,653.00

OPERADO CON RECURSOS FASP 2015

	3. Tiempo de respuesta telefónico de 2 horas para prioridad uno y 4 horas para prioridad dos, dentro del tiempo 5x8. 4. Tiempo de respuesta ingeniero en sitio al día siguiente hábil, con atención dentro del tiempo 5x8. 5. El tiempo de respuesta para ingeniero en sitio inicia a conteo a partir de que se determine la necesidad. 6. Apertura de casos con el fabricante con contrato vigente. 7. Seguimiento puntual de caso abierto al fabricante y ejecución de acciones a través del acceso remoto dispuesto por el cliente. 8. Análisis remoto de error y propuesta inicial de solución. 9. Notificación de existencia de actualizaciones y parches vía email. 10. Soporte para instalación de parches vía remota mediante acceso dispuesto por el cliente. 11. Soporte sobre resolución de dudas sobre la administración de la herramienta vía email.			
			Subtotal:	**$154,653.00**
			16% I.V.A.	**$ 24,744.48**
			Total:	**$179,397.48**

Mismos que "El Proveedor" se obliga a entregar en su totalidad el bien y servicio, acatando para ello lo establecido en el presente contrato, así como por los diversos ordenamientos y normas legales aplicables.

Segunda.- Monto del contrato: El monto total del contrato con I.V.A. incluido es de **$179,397.48 (Son: Ciento setenta y nueve mil trescientos noventa y siete pesos 48/100 M.N.),** precio con el cual se considera satisfecho "El Proveedor", "El Proveedor" previo a la entrega del bien y servicio, deberá notificar en un término de 5 días hábiles, la entrega de los mismos al área requirente.

Tercera.- Plazo y condiciones de entrega: "El Proveedor" se obliga a cumplir con la entrega de los bien y servicio objeto de este contrato, en un tiempo máximo de 21 días naturales contados a partir de la firma del presente instrumento contractual.

Cuarta.- Modificaciones al contrato: En el caso de que se requiera modificación en cuanto conceptos, volúmenes o plazos de cumplimiento, esta se realizará por causas debidamente justificadas y de común acuerdo entre las partes, de conformidad con lo establecido en el artículo 44 de la Ley de Adquisiciones, Arrendamientos y Prestación de Servicios Relacionados con Bienes Muebles del Estado de Campeche, debiendo "El Proveedor" presentar en su caso en un plazo de diez días hábiles antes de que finalice el plazo del contrato, escrito de solicitud y documentación que compruebe las razones de la solicitud, ante la Dirección de Recursos Materiales de la Secretaría de Administración e Innovación Gubernamental, para su autorización.

Quinta.- Requisitos de la factura: Además de los datos fiscales, la factura deberá contener la descripción

completa del bien, señalando marcas, modelos y números de series. Las series podrán ser desglosadas en un anexo diferente a la factura, tratándose de la adquisición de bienes que para su funcionamiento requieran de otros bienes para su correcto desempeño, se deberán de adjuntar en el anexo de la factura, el desglose de cada uno de ellos con sus series correspondientes. En los casos en que se requiera un anexo de factura, este deberá ser emitido en hoja membretada, haciendo referencia a la fecha y número de factura, nombre y firma de "El Proveedor" o representante legal incluyendo Registro Federal de Contribuyente (R.F.C.), para la identificación plena en caso de futuros reclamos por garantías, para el caso de la adquisición de software o licencias, deberá indicar la vigencia del software y el número de licencia u OEM.

Sexta.- Forma de pago: Las partes convienen que el bien y servicio objeto del presente contrato se paguen contra entrega de los mismos, a satisfacción de "El Estado" y mediante la formulación de la factura correspondiente, misma que será presentada por "El Proveedor" para su revisión, autorización y pago, en las oficinas que le indique "El Estado".

Séptima.- Garantía: Para garantizar el cumplimiento del contrato y vicios ocultos, "El Proveedor" otorgará garantía por el 20% del monto total del presente instrumento contractual, a través de cheque cruzado expedido a favor del Gobierno del Estado de Campeche, el cual tendrá una vigencia forzosa de hasta doce meses posteriores a la entrega total del bien y servicio, a satisfacción de "El Estado".

Octava.- Recepción del bien: La recepción del bien y servicio será total, conforme al plazo establecido en la cláusula tercera de este instrumento contractual y se realizará en las oficinas que ocupa la Secretaría de Seguridad Pública, ubicadas en avenida López Portillo, sin número, por avenida Lázaro Cárdenas, colonia Laureles, código postal 24096, de esta ciudad de San Francisco de Campeche, Campeche, México; reservándose "El Estado" el derecho de reclamar en caso de no estar satisfecho con la calidad del bien objeto del presente contrato conforme a lo señalado en los requisitos y plazos que para tal efecto se establecen en este mismo documento. En caso de que "El Estado" no esté satisfecho con el bien entregado por "El Proveedor", "El Estado" se lo dará a conocer a "El Proveedor" a efecto de que subsane dichas observaciones en un término no mayor de diez días naturales.

Novena.- Vigilancia, seguimiento, recepción del bien por parte de "El Estado": "El Estado" designa como responsable para la vigilancia, seguimiento y recepción del bien y servicio contratados a la Licda. Emma Vanessa Valle Abreu, Subdirectora de Recursos Federales de la Secretaría de Seguridad Pública, o por personal que esta misma designe, quien deberá en todo momento exigir a "El Proveedor" la entrega total del bien y servicio contratados.

Décima.- Responsabilidades de "El Proveedor": "El Proveedor" se obliga a que el bien y servicio objeto del presente contrato, cumplan con las normas de calidad requeridas y que la adquisición se efectúe a satisfacción de "El Estado" así como a responder por su cuenta y riesgo de los defectos de dichos bienes y servicios, atendiendo para tal efecto las condiciones de garantía requeridas por "El Estado".

Décima primera.- "El Proveedor" se obliga a no ceder a terceras personas físicas o morales, sus derechos y obligaciones sobre los bienes y servicios que amparan este contrato, sin previa aprobación expresa y por escrito de "El Estado", en los términos de la Ley de Adquisiciones, Arrendamientos y Prestación de Servicios Relacionados con Bienes Muebles del Estado de Campeche.

Décima segunda.- Suspensión temporal del contrato: "El Estado" podrá suspender temporalmente en todo o en parte la adquisición contratada en cualquier momento, por causas justificadas o razones de interés general, sin que ello implique su terminación definitiva. El presente contrato podrá continuar produciendo todos sus efectos legales, una vez que hayan desaparecido las causas que motivaron dicha suspensión.

OPERADO CON RECURSOS FASP 2015

Décima tercera.- Penas convencionales: Por la demora en la entrega del bien y servicio objeto de este contrato "El Estado" procederá a un descuento en la facturación por una cantidad igual a 5 al millar diario por cada día que "El Proveedor" incumpla con la entrega de los bienes, hasta por 20 días naturales, concluido este plazo y si "El Proveedor" continua con el incumplimiento, "El Estado" procederá a la rescisión del contrato, haciéndose efectivas las garantía de cumplimiento y vicios ocultos del contrato.

Décima cuarta.- Rescisión administrativa del contrato: "El Estado" podrá en cualquier momento rescindir administrativamente este contrato cuando "El Proveedor" incurra en incumplimiento de cualquiera de las obligaciones estipuladas en el presente contrato, aplicando en su caso a "El Proveedor" la garantía señalada en el presente instrumento contractual.

Décima quinta.- Las partes se obligan a sujetarse estrictamente para la adquisición objetos de este contrato, a todas y cada una de las cláusulas que lo integran, así como a los términos y requisitos que establece este contrato, la Ley de Adquisiciones, Arrendamientos y Prestación de Servicios Relacionados con Bienes Muebles del Estado de Campeche y demás disposiciones legales que le sean aplicables.

Décima sexta.- Ausencia de vicios del consentimiento: Ambas partes manifiestan que en la celebración del presente contrato no existe ningún error, dolo, violencia, mala fe, ni enriquecimiento ilícito que pudiese invalidarlo.

Décima séptima.- Para la interpretación y cumplimiento del contenido del presente contrato, así como para todo aquello que no esté expresamente establecido en el mismo, las partes se someten a jurisdicción de los tribunales establecidos en la ciudad de San Francisco de Campeche, Estado de Campeche, renunciando a cualquier otro que por su domicilio presente o futuro pudiere corresponderles.

Leído lo que fue el presente contrato, ambas partes se manifiestan conformes con su contenido, procediendo a suscribirlo por triplicado, en la ciudad de San Francisco de Campeche, Campeche, el día 17 de julio de 2017.

Por "El Estado"

Ing. Gustavo Manuel Ortiz González
Secretario de Administración e
Innovación Gubernamental

Por "El Proveedor"

Ing. Juan Gualberto Cabrera Pérez
Representante legal de Estrategias en
Tecnología Corporativa, S.A. de C.V.

Testigos

Licda. Eloy Daniela Chuc Solis
Directora de Recursos Materiales

Licda. Denice Elizabeth Castro Córdova
Subdirectora de Licitaciones y Contratos

OPERADO CON RECURSOS FASP 2015

Anexo único

Cant.	Descripción	Unidad de medida
1	**Licencia para equipo de Seguridad UTM** 1. Objeto: Adquisición de licencias para un sistema de seguridad informática perimetral del tipo Administración Unificada de Amenazas (UTM por sus siglas en inglés), donde se ofrecen las funcionalidades que se detallan en el presente documento. 2. Equipos Se considera la licencia y los servicios para los siguientes números de serie: • FGT60D4613054250 • FGT60D4613057081 • FGT90D3Z14017471 • FGT90D3Z14017487 Firewall • Las reglas de firewall analizan las conexiones que atraviesan en el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs. • Por granularidad y seguridad, el firewall puede especificar políticas tomando en cuenta puerto físico fuente y destino. Esto es, el puerto físico fuente y el puerto físico destino deberán formar parte de la especificación de la regla de firewall. • Es posible definir políticas de firewall que son independientes del puerto de origen y puerto de destino. • Las reglas del firewall se toman en cuenta dirección IP origen (que puede ser un grupo de direcciones IP), dirección IP destino (que puede ser un grupo de direcciones IP) y servicio (o grupo de servicios) de la comunicación que se está analizando • Soporte a reglas de firewall para tráfico de multicast, especificando puerto físico fuente, puerto físico destino, direcciones IP fuente, dirección IP destino. • Las reglas de firewall pueden tener limitantes y/o vigencia en base a tiempo. • Las reglas de firewall tienen limitantes y/o vigencia en base a fechas (incluyendo día, mes y año) • Soporta la capacidad de definir nuevos servicios TCP y UDP que no estan contemplados en los predefinidos. • Puede definirse el tiempo de vida de una sesión inactiva de forma independiente por puerto y protocolo (TCP y UDP) • Tiene capacidad de hacer traslación de direcciones estático, uno a uno, NAT. • Tiene capacidad de hacer tráslación de direcciones dinámico, muchos a uno, PAT. • Soporta reglas de firewall en IPv6 configurables tanto por CLI (Command Line Interface, Interface de línea de comando) como por GUI (Graphical	**Licencia**

User Interface, Interface Gráfica de Usuario),

- La solución tiene la capacidad de balancear carga entre servidores. Esto es realizar una traslación de una única dirección a múltiples direcciones de forma tal que se distribuya el tráfico entre ellas.
- En la solución de balanceo de carga entre servidores, se soporta persistencia de sesión al menos mediante HTTP Cookie o SSL Session ID
- En la solución de balanceo de carga de entre servidores se soportan mecanismos para detectar la disponibilidad de los servidores, de forma tal de poder evitar enviar tráfico a un servidor no disponible.
- El equipo permite la creación de políticas de tipo Firewall con capacidad de seleccionar campos como dirección, identificador de usuarios o identificador de dispositivos para el caso de dispositivos móviles como smartphones y tabletas.
- El equipo permite la creación de políticas de tipo VPN con capacidad de seleccionar campos como IPSEC o SSL según sea el tipo de VPN
- La solución tiene la capacidad de hacer captura de paquetes por política de seguridad implementada para luego ser exportado en formato PCAP.
- La solución de seguridad permite la creación de servicios de Firewall para implementar dentro de las políticas de seguridad y categorizarlos de manera personalizada
- La solución es capaz de integrar los servicios dentro de las categorías de Firewall predefinidas o personalizadas y ordenarlos alfabéticamente
- El dispositivo de seguridad puede determinar accesos y denegación a diferentes tipos de tráfico predefinidos dentro de una lista local de políticas
- La solución es capaz de habilitar o deshabilitar el paso de tráfico a través de procesadores de propósito específico, si el dispositivo cuenta con estos procesadores integrados dentro del mismo
- La solución puede crear e implementar políticas de tipo Multicast y determinar el sentido de la política, así como también la habilitación del NAT dentro de cada interface del dispositivo
- El dispositivo de seguridad es capaz de crear e integrar políticas contra ataques DoS las cuales se pueden aplicar por interfaces.
- El dispositivo de generar logs de cada una de las políticas aplicadas para evitar los ataques de DoS
- La solución de seguridad permite configurar el mapeo de protocolos a puertos de manera global o especifica
- La solución es capaz de configurar el bloqueo de archivos o correos electrónicos por tamaño, o por certificados SSL inválidos.
- El dispositivo integra la inspección de tráfico tipo SSL y SSH bajo perfiles predefinidos o personalizados
- El dispositivo es capaz de ejecutar inspección de tráfico SSL en todos los puertos y seleccionar bajo que certificado será válido este tráfico
- Tiene la capacidad de hacer escaneo a profundidad de tráfico tipo SSH dentro de todos o cierto rango de puertos configurados para este análisis
- La solución permitie bloquear o monitorear toda la actividad de tipo Exec, Port-Forward, SSH-Shell, y X-11 SSH

Antivirus

- Tiene la capacidad de analizar, establecer control de acceso y detener ataques y hacer Antivirus en tiempo real en al menos los siguientes

protocolos aplicativos: HTTP, SMTP, IMAP, POP3, FTP.

- El Antivirus se puede configurar en modo Proxy como en modo de Flujo. En el primer caso, los archivos son totalmente reconstruidos por el motor antes de hacer la inspección. En el segundo caso, la inspección de antivirus se hace por cada paquete de forma independiente.
- Antivirus en tiempo real, integrado a la plataforma de seguridad "appliance". Sin necesidad de instalar un servidor o appliance externo, licenciamiento de un producto externo o software adicional para realizar la categorización del contenido.
- El Antivirus integrado soporta la capacidad de inspeccionar y detectar virus en tráfico IPv6.
- La configuración de Antivirus en tiempo real sobre los protocolos HTTP, SMTP, IMAP, POP3 y FTP está completamente integrada a la administración del dispositivo appliance, que permite la aplicación de esta protección por política de control de acceso.
- El antivirus soporta múltiples bases de datos de virus de forma tal de que el administrador define cuál es conveniente utilizar para su implementación evaluando desempeño y seguridad.
- El appliance puede de manera opcional inspeccionar por todos los virus conocidos.
- El Antivirus integrado tiene la capacidad de poner en cuarentena archivos encontrados infectados que estan circulando a través de los protocolos http, FTP, IMAP, POP3, SMTP.
- El Antivirus integrado tiene la capacidad de poner en cuarentena a los clientes cuando se haya detectado que los mismos envían archivos infectados con virus.
- El Antivirus incluye capacidades de detección y detención de tráfico spyware, adware y otros tipos de malware/grayware que pudieran circular por la red.
- El antivirus puede hacer inspección y cuarentena de archivos transferidos por mensajería instantánea (Instant Messaging) para al menos MSN Messenger.
- El antivirus es capaz de filtrar archivos por extensión
- El antivirus es capaz de filtrar archivos por tipo de archivo (ejecutables, por ejemplo) sin importar la extensión que tiene el archivo
- Tiene capacidad de actualizar automáticamente la firma de Antivirus mediante tecnología de tipo "Push" (permite recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin programación previa), adicional a tecnologías tipo "pull" (Consulta los centros de actualización por versiones nuevas)

AntiSpam

- La capacidad antiSpam incluida es capaz de detectar palabras dentro del cuerpo del mensaje de correo, y en base a la presencia/ausencia de combinaciones de palabras, decidir rechaza el mensaje.
- La capacidad AntiSpam incluida permite especificar listas blancas (confiables, a los cuales siempre se les pasa) y listas negras (no confiables, a los cuales siempre se les bloquea). Las listas blancas y listas negras pueden ser por dirección IP o por dirección de correo electrónico (e-mail address).
- La capacidad AntiSpam puede consultar una base de datos donde se

revisa por lo menos dirección IP del emisor del mensaje, URLs contenidos dentro del mensaje y checksum del mensaje, como mecanismos para detección de SPAM

- En el caso de análisis de SMTP, los mensajes encontrados como SPAM pueden ser etiquetados o rechazados (descartados). En el caso de etiquetamiento del mensaje, se tiene la flexibilidad para etiquetarse en el motivo (subject) del mensaje o a través un encabezado MIME en el mensaje.

Filtraje de URLs (URL Filtering)

- Tiene facilidad para incorporar control de sitios a los cuales navegan los usuarios, mediante categorías. Por flexibilidad, el filtro de URLs tiene por lo menos 75 categorías y por lo menos 54 millones de sitios web en la base de datos.
- Puede categorizar contenido Web requerido mediante IPv6.
- Tiene filtrado de contenido basado en categorías en tiempo real, integrado a la plataforma de seguridad "appliance". Sin necesidad de instalar un servidor o appliance externo, licenciamiento de un producto externo o software adicional para realizar la categorización del contenido.
- Es configurable directamente desde la interfaz de administración del dispositivo appliance. Con capacidad para permitir esta protección por política de control de acceso.
- Permite diferentes perfiles de utilización de la web (permisos diferentes para categorías) dependiendo de fuente de la conexión o grupo de usuario al que pertenece la conexión siendo establecida
- La solución permite realizar el filtrado de contenido, tanto realizando reconstrucción de toda la sesión (modo proxy) como realizando inspección paquete a paquete sin realizar reconstrucción de la comunicación (modo flujo).
- Los mensajes entregados al usuario por parte del URL Filter (por ejemplo, en caso de que un usuario intente navegar a un sitio correspondiente a una categoría no permitida) son personalizables. Estos mensajes de remplazo pueden aplicarse para conexiones http y https, tanto en modo proxy como en modo flujo.
- Los mensajes de remplazo pueden ser personalizados por categoría de filtrado de contenido.
- Tiene capacidad de filtrado de scripts en páginas web (JAVA/Active X).
- La solución de Filtraje de Contenido soporta el forzamiento de "Safe Search" o "Búsqueda Segura" independientemente de la configuración en el browser del usuario. Esta funcionalidad no permite que los buscadores retornen resultados considerados como controversiales. Esta funcionalidad se soporta al menos para Google, Yahoo! y Bing.
- Es posible definir cuotas de tiempo para la navegación. Dichas cuotas pueden asignarse por cada categoría y por grupos.
- Es posible exceptuar la inspección de HTTPS por categoría.
- Cuenta con la capacidad de implementar el filtro de Educación de Youtube por Perfil de Filtro de Contenido para trafico HTTP, garantizando de manera centralizada, que todas las sesiones aceptadas por una política de seguridad con este perfil, pueden acceder solamente a contenido de tipo Educativo en Youtube, bloqueando cualquier tipo de contenido no Educativo.

- El sistema de filtrado de URLs tiene al menos 3 métodos de inspección:
  1. Modo de Flujo: La página es inspeccionada paquete a paquete sin reconstruir la página completa.
  2. Modo Proxy: La página es reconstruida completamente para ser analizada a profundidad.
  3. Modo DNS: La inspección se basa únicamente en la categorización del dominio accesado.
- Se incluye la funcionalidad de reputación basada en filtrado de URLs.
- La funcionalidad de reputación busca que, al acceder a páginas de contenido no deseado (tales como Malware, pornografía, consumo de ancho de banda excesivo, etc) se asigne un puntaje a cada usuario o IP cada vez visita una página de esta índole. De acuerdo a esto se extrae los usuarios que infringen las políticas de filtrado con más frecuencia con el fin de detectar zombies dentro de la red.
- El sistema de filtrado de URLs incluye la capacidad de definir cuotas de navegación basadas en volumen de tráfico consumido.
- Se incorpora la funcionalidad de filtrado educativo de Youtube (Youtube Education Filter)
- En dicho sistema cada organismo obtiene un ID de Youtube para habilitar el contenido educativo del mismo. Se inserta dicho código en la configuración de filtrado de URLs del equipo para habilitar únicamente el contenido educativo de Youtube.

Protección contra intrusos (IPS)

- El Detector y preventor de intrusos puede implementarse tanto en línea como fuera de línea. En línea, el tráfico a ser inspeccionado pasa a través del equipo. Fuera de línea, el equipo recibe el tráfico a inspeccionar desde un switch con un puerto configurado en span o mirror.
- Es posible definir políticas de detección y prevención de intrusiones para tráfico IPv6. A través de sensores.
- Tiene capacidad de detección de más de 4000 ataques.
- Tiene capacidad de actualización automática de firmas IPS mediante tecnología de tipo "Push" (permitie recibir las actualizaciones cuando los centros de actualización envían notificaciones sin programación previa), adicional a tecnologías tipo "pull" (Consulta los centros de actualización por versiones nuevas)
- El detector y preventor de intrusos está integrado a la plataforma de seguridad "appliance". Sin necesidad de instalar un servidor o appliance externo, licenciamiento de un producto externo o software adicional para realizar la prevención de intrusos. La interfaz de administración del detector y preventor de intrusos está perfectamente integrada a la interfaz de administración del dispositivo de seguridad appliance, sin necesidad de integrar otro tipo de consola para administrar este servicio. Esta permite la protección de este servicio por política de control de acceso.
- El detector y preventor de intrusos soporta captar ataques por variaciones de protocolo y además por firmas de ataques conocidos (signature based / misuse detection).
- Basado en análisis de firmas en el flujo de datos en la red, permite configurar firmas nuevas para cualquier protocolo.
- Actualización automática de firmas para el detector de intrusos

- El Detector de Intrusos mitiga los efectos de los ataques de negación de servicios.
- Métodos de notificación:
  - Alarmas mostradas en la consola de administración del appliance.
  - Alertas vía correo electrónico.
  - Tiene la capacidad de cuarentena, es decir prohibir el tráfico subsiguiente a la detección de un posible ataque. Esta cuarentena puede definirse al menos para el tráfico proveniente del atacante o para el tráfico del atacante al atacado.
  - La capacidad de cuarentena ofrece la posibilidad de definir el tiempo en que se bloquea el tráfico. También se puede definir el bloqueo de forma "indefinida", hasta que un administrador tome una acción al respecto.
  - Se ofrece la posibilidad de guardar información sobre el paquete de red que detonó la detección del ataque, así como al menos los 5 paquetes sucesivos. Estos paquetes pueden ser visualizados por una herramienta que soporte el formato PCAP.
- Se incluye protección contra amenazas avanzadas y persistentes (Advanced Persistent Threats). Dentro de estos controles se incluye:
- 1. Protección contra botnets: Se bloquean intentos de conexión a servidores de Botnets, para ello se cuenta con una lista de los servidores de Botnet más utilizado. Dicha lista se actualiza de forma periódica por el fabricante.
- 2. Sandboxing: La funcionalidad de Sandbox hace que el archivo sea ejecutado en un ambiente seguro para analizar su comportamiento y, a base del mismo, tomar una acción sobre el mismo.

Prevención de Fuga de Información (DLP)

- La solución ofrece la posibilidad de definir reglas que permiten analizar los distintos archivos que circulan a través de la red en búsqueda de información confidencial.
- La funcionalidad soporta el análisis de archivos del tipo: MS-Word, PDF, Texto, Archivos comprimidos.
- Puede soportar el escaneo de archivos en al menos los siguientes protocolos: HTTP, POP3, SMTP, IMAP, NNTP y FTP.
- Ante la detección de una posible fuga de información puede aplicarse las siguientes acciones: Bloquear el tráfico del usuario, Bloquear el tráfico de la dirección IP de origen, registrar el evento.
- En caso del bloqueo de usuarios, la solución permite definir por cuánto tiempo se hará el bloqueo o en su defecto bloquear por tiempo indefinido hasta que el administrador tome una acción.
- La solución soporta la capacidad de guardar una copia del archivo identificado como posible fuga de información. Esta copia puede ser archivada localmente o en otro dispositivo.
- La solución permite la búsqueda de patrones en archivos mediante la definición de expresiones regulares.
- Se provee la funcionalidad de filtrado de fuga de información. Dentro de las técnicas de detección se consideran como mínimo las siguientes:
  1. Filtrado por tipo de archivo
  2. Filtrado por nombre de archivo
  3. Filtrado por expresiones regulares: Se detectan los archivos según las

expresiones regulares que se encuentran dentro de los mismos.
4. Fingerprinting: Se toma una muestra del archivo que se considere como confidencial. Según esto se bloquean archivos que sean iguales a esta muestra.
5. Watermarking: Se inserta un "sello de agua" dentro del archivo considerado como confidencial. De acuerdo a esto se analizan los archivos en busca de este sello de agua, este se detecta incluso si el archivo sufrió cambios.

Control de Aplicaciones

- Lo solución soporta la capacidad de identificar la aplicación que origina cierto tráfico a partir de la inspección del mismo.
- La identificación de la aplicación es independiente del puerto y protocolo hacia el cual esta direccionado dicho tráfico.
- La solución tiene un listado de al menos 1000 aplicaciones ya definidas por el fabricante.
- El listado de aplicaciones puede actualizarse periódicamente.
- Para aplicaciones identificadas se pueden definir al menos las siguientes opciones: permitir, bloquear, registrar en log.
- Para aplicaciones no identificadas (desconocidas) se pueden definir al menos las siguientes opciones: permitir, bloquear, registrar en log.
- Para aplicaciones de tipo P2P se pueden definir adicionalmente políticas de traffic shaping.
- Puede soportar mayor granularidad en las acciones.

Inspección de Contenido SSL

- La solución puede soportar la capacidad de inspeccionar tráfico que esta siendo encriptado mediante TLS al menos para los siguientes protocolos: HTTPS, IMAPS, SMTPS, POP3S.
- La inspección se realizar mediante la técnica conocida como Hombre en el Medio (MITM - Man In The Middle).
- La inspección de contenido encriptado no requiere ningún cambio de configuración en las aplicaciones o sistema operativo del usuario.
- Para el caso de URL Filtering, es posible configurar excepciones de inspección de HTTPS. Dichas excepciones evitan que el tráfico sea inspeccionado para los sitios configurados. Las excepciones pueden determinarse al menos por Categoría de Filtrado.
- El equipo es capaz de analizar contenido cifrado (SSL o SSH) para las funcionalidades de Filtrado de URLs, Control de Aplicaciones, Prevención de Fuga de Información, Antivirus e IPS.

Soporte de Fabricante
La solución cuenta con soporte directo del fabricante por 12 meses con los siguientes alcances:

- Acceso a la base de datos de conocimiento del fabricante en un esquema 5x8
- Soporte telefónico 8x5 para atención de reporte de fallas o incidentes
- Soporte Web 8x5 para atención de reporte de fallas o incidentes
- Soporte vía Chat 8x5 para atención de reporte de fallas o incidentes
- Soporte de software con releases de mantenimiento y upgrades a nuevas versiones

OPERADO CON RECURSOS FASP 2015

- Soporte de hardware tipo reemplazo avanzado

Soporte por parte de "El Proveedor"
"El Proveedor" incluye un servicio de soporte para el soporte de los equipos con los siguientes alcances:

- Duración de 12 meses
- Atención de fallas con un tiempo máximo de 2 horas con esquema 5x8.
- Considera un (1) mantenimiento preventivo al año para los equipos, previo acuerdo con la Convocante. Los insumos necesarios para el mantenimiento corren por cuenta de "El Proveedor".
- Incluye soporte telefónico sin costo adicional en horario de lunes a viernes en horario de oficina.
- Para los equipos o software de la solución de seguridad para los cuales el fabricante libera nuevas versiones dentro de la vigencia de la póliza de soporte, "El Proveedor" instala sin costo dichas actualizaciones.

Reporte de fallas

- "El Proveedor" cuenta con una Mesa de Ayuda para recibir cualquier evento relacionado con la operación de la infraestructura requerida por parte de la Secretaría de Seguridad Pública. Este centro de atención es propio de "El Proveedor". y está ubicado en sus instalaciones, mediante el uso de sus propias herramientas y de manera dedicada para el soporte de la infraestructura de comunicaciones.
- Las tareas que "El Proveedor" realiza con la Mesa de Ayuda son: recibir, registrar, analizar, resolver y canalizar los reportes de incidentes o faltas, dar seguimiento y solución a los reportes informando a los usuarios oportunamente; así mismo, genera un registro histórico que permite consultas, generación de reportes y seguimiento sobre el tipo de fallas presentadas y la forma como se solucionaron.
- La atención y soporte es posible a través de un número telefónico único con servicio 01-800 sin costo adicional para la Secretaria de seguridad pública de Campeche y a través de correo o una página Web.
- Los datos que contiene un reporte de falla, mismo que se integran en el control de eventos e incidentes son:
  - Identificador del reporte o número de incidente o evento
  - Identificador del usuario que reporta. Estos son los datos que identifican al usuario que levantó el reporte. Nombre, teléfono, correo electrónico y ubicación. La definición final de estos datos se acuerda con "El Proveedor".
  - Hora en que reporta el problema por parte del usuario autorizado
  - Tipo de fallo
  - Descripción del fallo
  - Tiempo de solución del incidente y restablecimiento del servicio.
- Atención de fallas: De lunes a domingo 24 horas, el tiempo máximo es de 2 horas a partir del reporte de la falla para iniciar con el diagnóstico.

Administración de servicios

- "El Proveedor" alinea todos sus procesos relacionados con la

administración del servicio, a la biblioteca de Mejores Prácticas de ITIL (IT Infrastructure Library). Esto engloba a todos los procesos de entrega y soporte de servicio:

- Administración de configuraciones
- Administración de cambios
- Administración de incidencias
- Administración de problemas
- Administración de liberaciones
- Administración de la capacidad
- Administración de los niveles de servicio
- Administración de la disponibilidad
- Administración de Costo
- Mesa de Servicio (Función)

- Se adjunta en los documentos copias que certifican al personal propio de "El Proveedor" para la implementación en las mejores prácticas de ITIL (IT Infrastructure Library), por cuando menos 3 personas.

"El Proveedor" tiene las siguientes responsabilidades:

- Identificar la causa de la raíz de tales problemas.
- Asegurar que los recursos apropiados se asignen conforme sea necesario para identificar, solventar la falla, y dar seguimiento al informe sobre cualquier consecuencia de la falla.
- Proporcionar al cliente un reporte escrito detallado que informe la causa y el procedimiento para corregirla o mitigarla cuando sea posible. Proporcionar actualizaciones de manera mensual.
- Verificar que todas las acciones necesarias se han tomado para prevenir la repetición de tal falla.
- Mantener los procesos de administración de cambios, incluyendo los procedimientos y métodos vigentes para los cambios.
- Mantener las herramientas y procesos de administración de problemas para la gestión de todos los problemas y acciones preventivas desde la identificación de la causa raíz hasta el cierre del problema.
- Preparar y comunicar los impactos mediante la documentación de la causa raíz del problema, los esfuerzos para corregir temporal o permanentemente el problema y los siguientes pasos para su seguimiento.
- Escalación de los problemas que hayan rebasado los umbrales de respuesta basados en la severidad del problema.