Contrato de adquisición de sistema de protección perimetral (Firewall), que celebran por una parte el Poder Ejecutivo del Estado de Campeche, representado en este acto por Jezrael Isaac Larracilla Pérez, en su carácter de Secretario de Administración y Finanzas, a quien en lo sucesivo se le denominará "El Estado" y por la otra parte la persona moral Comercializadora Sistemas Stone, S.A. de C.V., representada en este acto por el ciudadano Carlos Amilcar Novelo Basto, a quien en lo sucesivo se denominará "El Proveedor", al tenor de las siguientes declaraciones y cláusulas:

OPERADO CON RECURSOS -2022-

FAFEF

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, 15 y 22 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 Jezrael Isaac Larracilla Pérez, comparece en su carácter de Secretario de Administración y Finanzas, personalidad que acredita con el nombramiento expedido a su favor por la Titular del Poder Ejecutivo del Estado de Campeche, el día 01 de enero de 2022, y está facultado para celebrar el presente instrumento según lo previsto por los artículos 4, 22 apartado A fracción II, y 28 fracciones XLVIII, XLIX y LII de la Ley Orgánica de la Administración Pública del Estado de Campeche; y numerales 1, 3, 4 apartado A fracción I, 13 y 14 fracciones I, II, XVIII, XLIX y LVI del Reglamento Interior de la Secretaría de Administración y Finanzas de la Administración Pública del Estado de Campeche.

1.3.- Que mediante oficio SEGOB/DRPPyC/CAMP/3433/2022, recibido el 14 de septiembre de 2022 firmado por el Mtro. Luis Fernando Mex Ávila, Director General del Registro Público de la Propiedad y de Comercio del Estado de Campeche, solicita la adquisición de mobiliario y diverso equipo informático, para destinarse a la unidad administrativa a su cargo.

1.4.- Que de conformidad con lo establecido por los artículos 1, 3, 4, 6, 21, 22, 23 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, 2 fracción VII y demás relativos aplicables de la Ley de Presupuesto de Egresos del Estado de Campeche, para el ejercicio fiscal 2022, la presente contratación se efectúa mediante la modalidad de Licitación Pública Estatal No. **SAFIN-EST-037-2022.**

1.5.- Que la erogación de la presente contratación se encuentra prevista y será cubierta con cargo al Fondo de Aportaciones para el Fortalecimiento de las Entidades Federativas (FAFEF), Ejercicio Fiscal 2022.

1.6.- Que tiene establecido su domicilio en la calle 8 número 149, entre calle 61 y 63, colonia Centro, código postal 24000, San Francisco de Campeche, Campeche, mismo que señala para los fines y efectos legales de este contrato.

1.7.- Que su Registro Federal de Contribuyentes es: GEC950401659.

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

2.1.- Ser una sociedad mercantil constituida bajo escritura pública número 157, de fecha 15 de agosto de 2003, otorgada ante la fe del licenciado Emilio Ortega Salinas, notario público número 38, del Primer Distrito Judicial del Estado de Campeche, por impedimento temporal de su titular el licenciado José Enrique Adam Richaud, documento que quedo inscrito bajo el folio mercantil electrónico número 18288 * 1, de fecha 24 de septiembre de 2003, ante el Registro

Público de la Propiedad y de Comercio del Estado de Campeche, con capacidad de comercializar el bien que en este caso requiere "El Estado".

2.2.- Que su representante legal es el ciudadano Carlos Amílcar Novelo Basto, quien acredita su personalidad con la escritura pública número 208 de fecha 28 de octubre de 2003, pasada ante la fe del licenciado Emilio Ortega Salinas, notario público en ejercicio, encargado de la notaría pública número 38, del Primer Distrito Judicial del Estado de Campeche, por impedimento temporal de su titular el licenciado José Enrique Adam Richaud, documento que quedo inscrito bajo el folio mercantil electrónico numero 18288 * 1, de fecha 29 de julio de 2004, ante el Registro Público de la Propiedad y de Comercio del Estado de Campeche, y se identifica con credencial para votar con fotografía y con clave de elector [redacted] expedida a su favor por el Instituto Nacional Electoral.

2.3.- Que tiene capacidad jurídica para contratar y reúne las condiciones técnicas y económicas para obligarse a proveer el bien 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 calle 12 número 248, entre calle Allende y Bravo, barrio de San Román, código postal 24040, San Francisco de Campeche, Campeche; mismo que señala para todos los fines y efectos legales de este contrato.

2.6.- Que su número del padrón de proveedores es: 2030, con vigencia al 24 de mayo de 2023.

2.7.- Que su Registro Federal de Contribuyentes es: CSS030815RX2.

3.- De ambas partes:

3.1.- Que en razón de lo declarado anteriormente y con fundamento en lo previsto por los artículos 39, 40, 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 1698, 1699, 1700, 1701, 1703, 1705, 1708, 1709, 1712, 1730, 1731, 1740, 1744, 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 contratación al tenor de las siguientes:

Cláusulas

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

Cant.	Unidad de medida	Descripción	Precio unitario	Importe
1	Pieza	Sistema de protección perimetral (Firewall). **Marca:** Fortinet **Modelo:** 200F Vigencia de la licencia de actualización y soporte: la vigencia de las actualizaciones para los servicios de	$385,716.00	$385,716.00

		Antivirus Sandbox en la nube, IPS y Filtrado de URL es por 36 meses.		
			Subtotal	**$385,716.00**
			I.V.A.	**$61,714.56**
			Total	**$447,430.56**

Mismo que "El Proveedor" se obliga a entregar en su totalidad, acatando para ello lo establecido en el presente contrato, anexo único, bases de licitación, así como por los diversos ordenamientos y normas legales aplicables.

Segunda.- Monto del contrato: El monto total del contrato es de **$447,430.56 (Son: Cuatrocientos cuarenta y siete mil cuatrocientos treinta pesos 56/100 M.N.) I.V.A. incluido**, precio fijo con el cual se considera satisfecho "El Proveedor".

Tercera.- Plazo y condiciones de entrega: "El Proveedor" se obliga a cumplir con la entrega del bien en un plazo máximo de **86 (ochenta y seis) días naturales** contados a partir de la firma del presente instrumento contractual.

En caso de que el último día de entrega sea inhábil, la entrega del bien se llevará a cabo el día siguiente hábil, entendiéndose como días hábiles de lunes a viernes en un horario de 09:00 a 15:00 horas.

Cuarta.- Modificaciones al contrato: En el caso de que se requiera modificación en cuanto conceptos o volúmenes, esta se realizará en **una sola ocasión** 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 máximo de 10 (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 General de Recursos Materiales de la Secretaría de Administración y Finanzas, para su autorización.

Sin embargo, no se otorgarán prórrogas en cuanto al plazo de cumplimiento de obligaciones al licitante que resulte adjudicado de la presente licitación. Lo anterior, con fundamento a lo establecido en el artículo 40 de la Ley de Disciplina Financiera y Responsabilidad Hacendaria del Estado de Campeche y Sus Municipios, el cual señala que *"una vez concluida la vigencia de los presupuestos de Egresos del Estado, sólo se procederá hacer pagos con base en ellos por los conceptos efectivamente devengados en el año que corresponda..."*

Quinta.- Forma de pago: El bien será pagado contra entrega recepción de la totalidad del mismo, 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".

Sexta.- Requisitos de la factura: Además de los datos fiscales, la(s) factura(s) deberá(n) expedirse en términos de lo establecido por los artículos 29 y 29-A del Código Fiscal de la Federación y Anexo 20 *"Guía de llenado de los comprobantes fiscales digitales por Internet"*, debiendo ser emitida por el monto total establecido en la cláusula primera del presente contrato, la(s) cual(es) deberá(n) incluir el número de serie del bien en caso que corresponda.

Séptima.- Para garantizar el cumplimiento y vicios ocultos del contrato: 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 Poder Ejecutivo del Estado de Campeche, el cual tendrá una vigencia forzosa de hasta doce meses posteriores a la entrega total del bien, a satisfacción de "El Estado".

OPERADO CON RECURSOS FAFEF -2022-

"El Proveedor" deberá presentar la garantía de cumplimiento y vicios ocultos, en un plazo máximo de 05 días hábiles siguientes a la firma del presente contrato.

Octava.- Lugar de entrega del bien: La recepción del bien motivo del presente contrato será total, conforme al plazo establecido en la cláusula tercera de este instrumento, y se realizará en las oficinas que ocupa la Dirección General del Registro Público de la Propiedad y de Comercio, con dirección en calle Castellot, Manzana K, lote 20, área Ah-Kim-Pech, sección Fundadores, código postal 24014, San Francisco de Campeche, Campeche; o en los domicilios que para tales efectos determine "El Estado"; reservándose 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 lineamientos, requisitos y plazos que para tal efecto se establece en el mismo.

Novena.- Vigilancia, seguimiento, recepción del bien por parte de "El Estado": "El Estado" designa como responsable para la vigilancia, seguimiento y recepción del bien contratado, al servidor público Mtro. Luis Fernando Mex Ávila, Director General, en coordinación con el Lic. José Román Guerrero Tejero, Subdirector de Informática, ambos de la Dirección General del Registro Público de la Propiedad y de Comercio; o por personal que éstos mismos designen, quien deberá en todo momento exigir a "El Proveedor" la entrega total del mismo.

"El Proveedor", entregará junto con el bien al servidor público indicado en el párrafo que antecede, la garantía que corresponde al bien objeto del presente instrumento contractual, así como la metodología a aplicar para hacerla efectiva.

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

Décima primera.- Integridad: El anexo único del presente contrato es parte integral de este instrumento contractual y se incorpora al mismo por referencia. Este contrato únicamente podrá ser modificado o adicionado mediante un instrumento por escrito firmado por cada una de las partes y entregado a la otra parte.

Décima segunda.- "El Proveedor" se obliga a no ceder a terceras personas físicas o morales, sus derechos y obligaciones sobre el bien que ampara este contrato, en los términos de la Ley de Adquisiciones, Arrendamientos y Prestación de Servicios Relacionados con Bienes Muebles del Estado de Campeche.

Décima tercera.- Suspensión temporal del contrato: "El Estado" podrá suspender temporalmente en todo o en parte la presente contratación 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.

Décima cuarta.- Penas convencionales: En función del bien no entregado oportunamente motivo de este contrato, "El Estado" procederá a un descuento en la facturación por una cantidad igual a 5 al millar diario por cada día de incumplimiento de "El proveedor", 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 efectiva la garantía de cumplimiento y vicios ocultos del contrato.

Décima quinta.- Deducciones de pago y rescisión administrativa del contrato: "El Estado" podrá realizar deducciones al pago del bien que "El Proveedor" entregue de manera parcial o deficiente, una vez que haya sido notificado al respecto de manera oficial y en el caso de que "El Proveedor" no hubiese subsanado dichas fallas en el plazo que para esos efectos hubiese establecido "El Estado", en estos casos y cuando se trate de fallas o deficiencias presentadas únicamente de manera parcial (por cantidades no entregadas) el límite de incumplimiento a partir del cual "El Estado"

OPERADO CON RECURSOS -2022- FAFEF

procederá a la cancelación del contrato correspondiente será del 30% de las cantidades contratadas, "El Estado" podrá rescindir este en los términos previstos en el artículo 47 de 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.

"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 sexta.- Las partes se obligan a sujetarse estrictamente para la adquisición del bien objeto de este contrato, a todas y cada una de las cláusulas que lo integran, así como a los términos, lineamientos, procedimientos y requisitos que establece 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 séptima.- 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 octava.- 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 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 28 de octubre de 2022.

Por "El Estado"

Jezrael Isaac Larracilla Pérez
Secretario de Administración
y Finanzas

Por "El Proveedor"

C. Carlos Amílcar Novelo Basto
Representante legal de Comercializadora
Sistemas Stone, S.A. de C.V.

Testigos

Concepción Chávez Ramos
Directora General de Recursos Materiales

Lic. Víctor Manuel Saravia Pacheco
Director de Recursos Materiales

Licda. Gloria Selina Portillo Sandoval
Subdirectora de Adquisiciones Federales

OPERADO CON RECURSOS -2022- FAFEF

Anexo único

Cantidad	Descripción	Unidad de medida
1	**Sistema de protección perimetral (Firewall).** **Marca:** Fortinet **Modelo:** 200F **Especificaciones técnicas:** Sistema de seguridad informática perimetral que es del tipo Administración Unificada de Amenazas (UTM por sus siglas en inglés), donde se ofrece ya incluidas y listas para ser utilizadas, las funcionalidades que se detallan a continuación: **Características del Equipo:** Rendimiento de por lo menos 11 Gbps con la funcionalidad de firewall habilitada para tráfico IPv4 y IPv6 Soporte a por lo menos 3M conexiones simultáneas. Soporte a por lo menos 280K nuevas conexiones por segundo. Rendimiento de al menos 13 Gbps de VPN IPSec. Esta licenciado para, o soportar sin necesidad de licencia, 2K túneles de VPN IPSec site-to-site simultáneos. Esta licenciado para, o soportar sin necesidad de licencia, 16K túneles de clientes VPN IPSec simultáneos. Throughput de al menos 2 Gbps de VPN SSL. Soporta al menos 500 clientes de VPN SSL simultáneos. Soportar al menos 5 Gbps de throughput de IPS. Soporta al menos 4 Gbps de throughput de Inspección SSL. Soporta al menos 13 Gbps de throughput de Application Control. Soporta al menos 3.5 Gbps de throughput de NGFW. Soporta al menos 3 Gbps de throughput de Threat Protection. Permite gestionar al menos 256 Access Points. Tener al menos 16 interfaces 1 Gbps. Esta tiene incluido sin costo adicional, al menos 10 sistemas virtuales lógicos (Contextos) por appliance. **Requisitos mínimos de funcionalidad:** Características del dispositivo. La solución consiste en una plataforma de protección de Red, basada en un dispositivo con funcionalidades de Firewall de Próxima Generación (NGFW), así como consola de gestión y monitoreo. Por funcionalidades de NGFW se entiende: Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos. Las funcionalidades de protección de red que conforman la plataforma de seguridad, puede ejecutarse en múltiples dispositivos siempre que cumplan todos los requisitos de esta especificación. La plataforma está optimizada para análisis de contenido de aplicaciones en capa 7. El equipo proporcionado es adecuado para montaje en rack de 19", incluyendo un rail kit (si es necesario) y los cables de alimentación.	Pieza

OPERADO CON RECURSOS FAFEF -2022-

	La gestión del equipo(s) es compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red. Los dispositivos de protección de red soportan 4094 VLANs Tags 802.1q. Los dispositivos de protección de red soportan agregación de enlaces 802.3ad y LACP. Los dispositivos de protección de red soportan Policy based routing y policy based forwarding. Los dispositivos de protección de red soportan encaminamiento de multicast (PIM-SM y PIM-DM). Los dispositivos de protección de red soportan DHCP Relay. Los dispositivos de protección de red soportan DHCP Server. Los dispositivos de protección de red soportan sFlow. Los dispositivos de protección de red soportan Jumbo Frames. Los dispositivos de protección de red soportan sub-interfaces Ethernet lógicas. Es compatible con NAT dinámica (varios-a-1) Es compatible con NAT dinámica (muchos-a-muchos). Soporta NAT estática (1-a-1) Admite NAT estática (muchos-a-muchos). Es compatible con NAT estático bidireccional 1-a-1 Es compatible con la traducción de puertos (PAT). Es compatible con NAT Origen. Es compatible con NAT de destino. Soporta NAT de origen y NAT de destino de forma simultánea. Soporta NAT de origen y NAT de destino en la misma política. Soporta Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico. Es compatible con NAT64 y NAT46 Permite implementar el protocolo ECMP. Soporta el balanceo de enlace hash por IP de origen. Soporta el balanceo de enlace por hash de IP de origen y destino. Soporta balanceo de enlace por peso. En esta opción es posible definir el porcentaje de tráfico que fluirá a través de cada uno de los enlaces. Es compatible con el balanceo en al menos tres enlaces. Permite implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales. Permite el monitoreo por SNMP de fallas de hardware, uso de recursos por gran número de sesiones, conexiones por segundo, cantidad de túneles establecidos en la VPN, CPU, memoria, estado del clúster, ataques y estadísticas de uso de las interfaces de red. Envía logs a sistemas de gestión externos simultáneamente. Tiene la opción de enviar logs a los sistemas de control externo a través de TCP y SSL. Soporta protección contra la suplantación de identidad (anti-spoofing). Permite Implementar la optimización del tráfico entre dos dispositivos. Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP). Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3) Soportar OSPF graceful restart. Los dispositivos de protección tienen la capacidad de operar simultáneamente en una única instancia de servidor de seguridad, mediante el uso de sus interfaces físicas en los siguientes modos: modo sniffer (monitoreo y análisis de tráfico de red), capa 2 (L2) y capa 3 (L3)	

FAFEF OPERADO CON RECURSOS -2022-

	Es compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red. Soporta modo capa-2 (L2) para la inspección de datos y visibilidad en línea del tráfico. Soporta modo capa-3 (L3) para la inspección de datos y visibilidad en línea del tráfico. Soporta el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas. Soporta la configuración de alta disponibilidad activo/pasivo y activo/activo: En modo transparente. Soporta la configuración de alta disponibilidad activo/pasivo y activo/activo: En capa 3 Soporta la configuración de alta disponibilidad activo/pasivo y activo/activo: En la capa 3 y con al menos 3 dispositivos en el cluster. La configuración de alta disponibilidad permite sincronizar: Sesiones. La configuración de alta disponibilidad permite sincronizar: Configuraciones, incluyendo, pero no limitando, políticas de Firewalls, NAT, QoS y objetos de la red. La configuración de alta disponibilidad mermite sincronizar: Las asociaciones de seguridad VPN. La configuración de alta disponibilidad permite sincronizar: Tablas FIB. En modo HA (Modo de alta disponibilidad) permite la supervisión de fallos de enlace. Soporta la creación de sistemas virtuales en el mismo equipo. Para una alta disponibilidad, el uso de clusters virtuales es posible, ya sea activo-activo o activo-pasivo, que permita la distribución de la carga entre los diferentes contextos. Permite la creación de administradores independientes para cada uno de los sistemas virtuales existentes, con el fin de permitir la creación de contextos virtuales que se pueden administrar por diferentes áreas funcionales. La solución de gestión es compatible con el acceso a través de SSH y la interfaz web (HTTPS), incluyendo, pero no limitado a, la exportación de configuración de sistemas virtuales (contextos) por ambos tipos de acceso. Control, inspección y descifrado de SSL para tráfico entrante (Inbound) y saliente (Outbound), soporta el control de los certificados individualmente dentro de cada sistema virtual, o sea, aislamiento de las operaciones de adición, remoción y utilización de los certificados directamente en los sistemas virtuales (contextos). Soporta un tejido de seguridad para proporcionar una solución de seguridad integral que abarque toda la red. El tejido de seguridad identifica potenciales vulnerabilidades y destaca las mejores prácticas que podrían ser usadas para mejorar la seguridad general y el rendimiento de una red. Tiene la opción de un Servicio de Soporte que ofrezca a los clientes un chequeo de salud periódico con un informe de auditoría mensual personalizado de sus appliances NGFW y WiFi. **Control de políticas de Firewall:** Soporta controles de zona de seguridad. Cuenta con políticas de control por puerto y protocolo. Cuenta con políticas por aplicación, grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (en base a las características y comportamiento de las aplicaciones) y categorías de aplicaciones. Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad. Firewall puede aplicar la inspección UTM (control de aplicaciones y filtrado web como	

OPERADO CON RECURSOS FAFEF -2022-

	mínimo) directamente a las políticas de seguridad en vez de usar perfil obligatoriamente. Además de las direcciones y servicios de destino, los objetos de servicio de Internet pueden agregarse directamente a las políticas de firewall. Soporta el almacenamiento de bitácoras (logs) en tiempo real tanto para entorno de la nube como entorno local (on-premise). Soporta el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF). Tiene una manera de evitar que el almacenamiento de logs en tiempo real no supere la velocidad de subida de los mismos (upload). Soporta el protocolo estándar de la industria VXLAN. **SDWAN:** La solución es capaz de implementar la distribución de tráfico independiente mente del transporte o proveedor de servicio. El equipo es capaz de implementar la distribución de tráfico a través de subinterfaces VLAN, de igual forma independientemente del transporte o proveedor de servicio. La solución puede realizar la distribución de tráfico a través de diferentes túneles VPN por medio de la funcionalidad de SDWAN. La solución hace uso de todos los enlaces de manera simultánea y tomar decisiones basadas en políticas, Calidad de enlace (IP SLAS) y tipo de tráfico o aplicaciones. El equipo es capaz de implementar la distribución de tráfico a través de conexiones VPN sitio a sitio con enrutamiento dinámico. En el caso de conexión VPN el equipo tiene la capacidad de hacer división de tráfico de VPN y tráfico de Internet, esto con el fin de evitar enviar el tráfico de Internet a través del túnel. Tiene la capacidad de realizar distribución de tráfico basado en políticas independientes a las políticas de Firewall con base en: IP origen, IP destino, Puerto origen y Puerto destino; usuario autenticado Origen; dispositivo origen; aplicación destino. Es capaz de tomar decisión automática del uso del enlace y del enrutamiento del tráfico con base en la verificación del estado del enlace (Link quality health checks). Los criterios de calidad de enlace deben contar con mecanismos de verificación del enlace como son latencia, jitter, perdida de paquetes, velocidad de descarga, velocidad de carga y Ancho de banda. Tiene la capacidad de crear criterios de calidad de servicio del enlace (SLA) definidos por los usuarios. Tiene la capacidad de crear de múltiples SLAs por regla de SD-WAN. Tiene la posibilidad de especificar el enlace de preferencia en la regla de SD-WAN. Tiene la capacidad de seleccionar la mejor ruta o enlace WAN basado en la calidad del enlace WAN. Soporta implementación de SDWAN a través de VPNs con IPs dinámicas, esto con el fin de evitar tener IPs fijas en sitios remotos y usar un nodo central para realizar la comunicación a través de un nodo central (Overlay a través del nodo central). Distribución de tráfico de servicio de Internet de acuerdo al tipo de aplicación. La administración u orquestación es centralizada, sin embargo, el appliance depende de esta para tener continuidad del servicio, por lo cual parte del plano de control y el plano de datos deben estar embebidos en el equipo. Soporta el enrutamiento dinámico BGP dentro de los túneles asociados a la	

OPERADO CON RECURSOS FAFEF -2022-

	distribución mediante SD-WAN. Puede realizar la recuperación automática del enlace seleccionado como primario. Soporta traffic shaping tráfico basado en porcentaje de la interfaz física para garantizar calidad en el SDWAN. **Control de Aplicación:** Los dispositivos de protección de red tienen tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo. Es posible liberar y bloquear aplicaciones sin necesidad de abrir o cerrar puertos y protocolos. Reconocer al menos 1.700 aplicaciones diferentes, incluyendo, pero no limitado a: El tráfico relacionado peer-to-peer, redes sociales, acceso remoto, actualización de software, protocolos de red, VoIP, audio, vídeo, Proxy, mensajería instantánea, compartición de archivos, correo electrónico. Reconocer al menos las siguientes aplicaciones: BitTorrent, Gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs. Inspecciona el payload del paquete de datos con el fin de detectar las firmas de las aplicaciones conocidas por el fabricante independiente de puerto y protocolo. Detecta aplicaciones a través del análisis del comportamiento del tráfico observado, incluyendo, pero no limitado a las aplicaciones de VoIP que utilizan cifrado propietario y BitTorrent. Identifica el uso de tácticas evasivas, es decir, tiene la capacidad de ver y controlar las aplicaciones y los ataques con tácticas evasivas a través de las comunicaciones cifradas, tales como Skype y la utilización de la red Tor. Para tráfico cifrado SSL, debe poder descifrarlo a fin de posibilitar la lectura de payload para permitir la identificación de firmas de la aplicación conocidas por el fabricante. Hace la decodificación de protocolos con el fin de detectar aplicaciones encapsuladas dentro del protocolo y validar que el tráfico corresponde a la especificación del protocolo, incluyendo, pero no limitado a Yahoo Instant Messenger utilizando HTTP. La decodificación de protocolo también debe identificar las características específicas dentro de una aplicación, incluyendo, pero no limitado al intercambio de ficheros dentro de Webex. Identifica el uso de tácticas evasivas a través de las comunicaciones cifradas. Actualización de la base de firmas de la aplicación de forma automática. Limitar el ancho de banda (carga/descarga) utilizado por las aplicaciones (traffic shaping), basado en IP de origen, usuarios y grupos. Los dispositivos de protección de red tienen la capacidad de identificar al usuario de la red con la integración de Microsoft Active Directory sin necesidad de instalación del agente en el controlador de dominio, o en estaciones de trabajo de usuario. Es posible añadir múltiples reglas de control de aplicaciones, es decir, no debe limitar habilitar el control de aplicaciones de control solamente en algunas reglas. Es compatible con múltiples métodos de identificación y clasificación de las aplicaciones, al menos verificar firmas y protocolos de decodificación. Para mantener la seguridad de red eficiente debe soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas.	

	Permitir la creación de forma nativa de firmas personalizadas para el reconocimiento de aplicaciones propietarias en su propia interfaz gráfica, sin la necesidad de la acción del fabricante. La creación de firmas personalizadas debe permitir el uso de expresiones regulares, el contexto (sesiones o transacciones), utilizando la posición en el payload de paquetes TCP y UDP, y el uso de decodificadores de al menos los siguientes protocolos: HTTP, FTP, NBSS, DCE RPC, SMTP, Telnet, SSH, MS-SQL, IMAP, DNS, LDAP, SSL y RTSP. El fabricante permite solicitar la inclusión de aplicaciones en su base de datos. Alerta al usuario cuando sea bloqueada una aplicación. Permite la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo. Permite la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo. Permite la diferenciación y manejo de las aplicaciones de chat; por ejemplo, permitir a Hangouts el chat, pero impedir la llamada de video. Permite la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo. Es posible la creación de grupos dinámicos de aplicaciones, basado en las características de las mismas, tales como: Tecnología utilizada en las aplicaciones (Client-Server, Browse Based, Network Protocol, etc). Es posible crear grupos dinámicos de aplicaciones basados en características de las mismas, tales como: Nivel de riesgo de la aplicación. Es posible crear grupos estáticos de aplicaciones basadas en características de las mismas, tales como: Categoría de Aplicación. Es posible configurar Application Override seleccionando las aplicaciones individualmente. **Prevención de amenazas:** Para proteger el entorno contra los ataques, tiene un módulo IPS, protección de malware integrado en el propio equipo. Incluye firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (protección de malware). Las características de IPS, protección de malware funcionan de forma permanente, pudiendo utilizarlas de forma indefinida, aunque no exista el derecho a recibir actualizaciones o no exista un contrato de garantía del software con el fabricante. Sincroniza las firmas de IPS, antivirus, anti-spyware cuando se implementa en alta disponibilidad. Implementa los siguientes tipos de acciones a las amenazas detectadas por IPS: Permitir, permitir y generar registro, bloquear, bloquear IP del atacante durante un tiempo y enviar tcp-reset. Las firmas deben son capaces de ser activadas o desactivadas, o activadas sólo en el modo de monitoreo. Es posible crear políticas para usuarios, grupos de usuarios, IP, redes o zonas de seguridad. Excepciones por IP de origen o destino son posibles en las reglas o en cada una de las firmas. Soporta granularidad en las políticas de IPS, protección de malware, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio y la combinación de todos estos elementos.	

OPERADO CON RECURSOS -2022-

FAFEF

	Permite el bloqueo de vulnerabilidades. Permite el bloqueo de exploits conocidos. Incluye la protección contra ataques de denegación de servicio. **Tiene los siguientes mecanismos de inspección IPS:** - Análisis de patrones de estado de las conexiones. - Análisis de decodificación de protocolo. - Análisis para detectar anomalías de protocolo. - Análisis heurístico. - Desfragmentación IP. - Reensamblado de paquetes TCP. - Bloqueo de paquetes con formato incorrecto (malformed packets). Es inmune y capaz de prevenir los ataques básicos, tales como inundaciones (flood) de SYN, ICMP, UDP, etc. Detectar y bloquear los escaneos de puertos de origen. Bloquear ataques realizados por gusanos (worms) conocidos. Cuenta con firmas específicas para la mitigación de ataques DoS y DDoS. Cuenta con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow). Puede crear firmas personalizadas en la interfaz gráfica del product. Permite utilizar operadores de negación en la creación de firmas personalizadas de IPS o anti-spyware, permitiendo la creación de excepciones con granularidad en la configuración. Permite el bloqueo de virus y software espía en por lo menos los siguientes protocolos: HTTP, FTP, SMB, SMTP y POP3 Soportar el bloqueo de archivos por tipo. Identificar y bloquear la comunicación con redes de bots. Registra en la consola de supervisión la siguiente información sobre amenazas concretas: El nombre de la firma o el ataque, la aplicación, el usuario, el origen y destino de las comunicaciones, además de las medidas adoptadas por el dispositivo. Es compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación. Permite la captura de paquetes por tipo de firma IPS y definir el número de paquetes capturados o permitir la captura del paquete que dio lugar a la alerta, así como su contexto, facilitando el análisis forense y la identificación de falsos positivos. Tiene la función de protección a través de la resolución de direcciones DNS, la identificación de nombres de resolución de las solicitudes a los dominios maliciosos de botnets conocidos. Los eventos identifican el país que origino la amenaza. Incluye protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms). Tiene protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP. Permite la configuración de diferentes políticas de control de amenazas y ataques basados en políticas de firewall considerando usuarios, grupos de usuarios, origen, destino, zonas de seguridad, etc., es decir, cada política de firewall puede tener una configuración diferente de IPS basada en usuario, grupos de usuarios, origen, destino, zonas de seguridad.	

FAFEF OPERADO CON RECURSOS -2022-

	El Firewall permite analizar la implementación del tejido de seguridad para identificar posibles vulnerabilidades y resaltar las mejores prácticas que podrían utilizarse para mejorar la seguridad y el rendimiento general de su red. En caso de que el firewall pueda coordinarse con software de seguridad en equipo de usuario final (LapTop, DeskTop, etc) cuenta con un perfil donde pueda realizar análisis de vulnerabilidad en estos equipos de usuario y asegurarse de que estos ejecuten versiones compatibles. Existen los recursos de postura de seguridad para permitir que el software de seguridad de endpoint aplique protección en tiempo real, antivirus, filtrado de Web y control de aplicaciones en el punto final. Proporcionan protección contra ataques de día cero a través de una estrecha integración con componentes del tejido de seguridad, incluyendo NGFW y Sandbox (en las instalaciones y en la nube). **Filtrado de URL:** Permite especificar la política por tiempo, es decir, la definición de reglas para un tiempo o período determinado (día, mes, año, día de la semana y hora). Permite crear políticas para usuarios, IPs, redes, o zonas de seguridad. Tiene la capacidad de crear políticas basadas en la visibilidad y el control de quién está utilizando las URL esto mediante la integración con los servicios de directorio Active Directory y la base de datos local. Tiene la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando las URL que mediante la integración con los servicios de directorio Active Directory y la base de datos local, en modo de proxy transparente y explícito. Soporta la capacidad de crear políticas basadas en control por URL y categoría de URL. Tiene la base de datos de URLs en caché en el equipo o en la nube del fabricante, evitando retrasos de comunicación/validación de direcciones URL. Tiene por lo menos 60 categorías de URL. Tiene la funcionalidad de exclusión de URLs por categoría. Permite página de bloqueo personalizada. Permite bloqueo y continuación (que permita al usuario acceder a un sitio potencialmente bloqueado, informándole en pantalla del bloqueo y permitiendo el uso de un botón Continuar para que el usuario pueda seguir teniendo acceso al sitio). Además del Explicit Web Proxy, soportar proxy web transparente. **Identificación de Usuarios:** Se incluye la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando dichas aplicaciones a través de la integración con los servicios de directorio, a través de la autenticación LDAP, Active Directory, E-directorio y base de datos local. Tiene integración con Microsoft Active Directory para identificar a los usuarios y grupos, permitiendo granularidad a las políticas/control basados en usuarios y grupos de usuarios. Tiene integración y soporte para Microsoft Active Directory para los siguientes sistemas operativos: Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 y Windows Server 2012 R2 Tiene integración con Microsoft Active Directory para identificar a los usuarios y grupos que permita tener granularidad en las políticas/control basados en usuarios y grupos de usuarios, soporte a single-sign-on. Esta funcionalidad no debe tener límites	

OPERADO CON RECURSOS FAFEF -2022-

	licenciados de usuarios o cualquier restricción de uso como, pero no limitado a, utilización de sistemas virtuales, segmentos de red, etc. Tiene integración con RADIUS para identificar a los usuarios y grupos que permiten las políticas de granularidad/control basados en usuarios y grupos de usuarios. Tiene la integración LDAP para la identificación de los usuarios y grupos que permiten granularidad en la política/control basados en usuarios y grupos de usuarios. Permite el control sin necesidad de instalación de software de cliente, el equipo que solicita salida a Internet, antes de iniciar la navegación, entre a un portal de autentificación residente en el equipo de seguridad (portal cautivo). Soporta la identificación de varios usuarios conectados a la misma dirección IP en entornos Citrix y Microsoft Terminal Server, lo que permite una visibilidad y un control granular por usuario en el uso de las aplicaciones que se encuentran en estos servicios. Permite implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP/AD. Permite la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma. Proporciona al menos un token de forma nativa, lo que permite la autenticación de dos factores. **QoS Traffic Shaping:** Con el fin de controlar el tráfico y aplicaciones cuyo consumo puede ser excesivo (como YouTube, Ustream, etc.) y que tienen un alto consumo de ancho de banda, se requiere de la solución que, además de permitir o denegar dichas solicitudes, debe tener la capacidad de controlar el ancho de banda máximo cuando son solicitados por los diferentes usuarios o aplicaciones, tanto de audio como de video streaming. Soporta la creación de políticas de QoS y Traffic Shaping por dirección de origen. Soporta la creación de políticas de QoS y Traffic Shaping por dirección de destino. Soporta la creación de políticas de QoS y Traffic Shaping por usuario y grupo. Soporta la creación de políticas de QoS y Traffic Shaping para aplicaciones incluyendo, pero no limitado a Skype, BitTorrent, Azureus y YouTube. Soporta la creación de políticas de calidad de servicio y Traffic Shaping por Puerto. En QoS permite la definición de tráfico con ancho de banda garantizado. En QoS permite la definición de tráfico con máximo ancho de banda. En QoS permite la definición de colas de prioridad. Soporta la priorización de protocolo en tiempo real de voz (VoIP) como H.323, SIP, SCCP, MGCP y aplicaciones como Skype. Soporta marcación de paquetes DiffServ, incluso por aplicación. Soporta la modificación de los valores de DSCP para Diffserv. Soporta priorización de tráfico utilizando información de Tipo de Servicio (Type of Service). Proporciona estadísticas en tiempo real para clases de QoS y Traffic Shaping. Soporta QoS (traffic-shapping) en las interfaces agregadas o redundantes. **Filtro de Datos:** Permite la creación de filtros para archivos y datos predefinidos. Los archivos son identificados por tamaño y tipo. Permite identificar y opcionalmente prevenir la transferencia de varios tipos de archivo (MS Office, PDF, etc.) identificados en las aplicaciones (HTTP, FTP, SMTP, etc.). Soporta la identificación de archivos comprimidos o la aplicación de políticas sobre el	

FAEF OPERADO CON RECURSOS -2022-

	contenido de este tipo de archivos. Soporta la identificación de archivos cifrados y la aplicación de políticas sobre el contenido de este tipo de archivos. Permite identificar y opcionalmente prevenir la transferencia de información sensible, incluyendo, pero no limitado a, número de tarjeta de crédito, permitiendo la creación de nuevos tipos de datos a través de expresiones regulares. **Geo Localización:** Soporta la creación de políticas por geo-localización, permitiendo bloquear el tráfico de cierto País/Países. Permite la visualización de los países de origen y destino en los registros de acceso. Permite la creación de zonas geográficas por medio de la interfaz gráfica de usuario y la creación de políticas usando las mismas. **VPN:** Soporta VPN de sitio-a-sitio y cliente-a-sitio. Soporta VPN IPSec. Soporta VPN SSL. La VPN IPSec es compatible con 3DES. La VPN IPSec es compatible con la autenticación MD5 y SHA-1 La VPN IPSec es compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14 La VPN IPSec es compatible con Internet Key Exchange (IKEv1 y v2). La VPN IPSec es compatible con AES de 128, 192 y 256 (Advanced Encryption Standard). La VPN IPSec es compatible con la autenticación a través de certificados IKE PKI. Tiene interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall. Soporta VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec. Pemrite activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso throubleshooting. La VPN SSL Soporta que el usuario pueda realizar la conexión a través de cliente instalado en el sistema operativo de su máquina o a través de la interfaz web. Las características de VPN SSL se cumplen con o sin el uso de agentes. Permite que todo el tráfico de los usuarios VPN remotos fluya hacia el túnel VPN, previniendo la comunicación directa con dispositivos locales como un proxy. Asignación de DNS en la VPN de cliente remote. Permite la creación de políticas de control de aplicaciones, IPS, antivirus, filtrado de URL y AntiSpyware para el tráfico de clientes remotos conectados a la VPN SSL. Soporta autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local. Soporta lectura y revisión de CRL (lista de revocación de certificados). Permite la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL. Permite que la conexión a la VPN se establezca de la siguiente manera: Antes de que el usuario se autentique en su estación. Permite que la conexión a la VPN se establezca de la siguiente manera: Después de la autenticación de usuario en la estación. Permite que la conexión a la VPN se establezca de la siguiente manera: Bajo demanda de los usuarios. Manteniene una conexión segura con el portal durante la sesión.	

OPERADO CON RECURSOS FAFEF -2022-

	El agente de VPN SSL o IPSEC cliente-a-sitio es compatible con al menos Windows 7 (32 y 64 bits), Windows 8 (32 y 64 bits), Windows 10 (32 y 64 bits) y Mac OS X (v10.10 o superior). **Wireless Controller:** Gestiona de manera centralizada puntos de acceso del mismo fabricante de la solución. Soporta servicio de servidor DHCP por SSID para proporcionar direcciones IP a los clientes inalámbricos. Soporte IPv4 e IPv6 por SSID. Permite elegir si el tráfico de cada SSID se enviará a la controladora o directamente por la interfaz de punto de acceso en una determinada VLAN. Permite definir qué redes se acceden a través de la controladora y que redes serán accedidas directamente por la interfaz del Access Point. Soporta monitoreo y supresión de puntos de acceso indebidos. Proporciona autenticación a la red inalámbrica a través de bases de datos externas, tales como LDAP o RADIUS. Permite autenticar a los usuarios de la red inalámbrica de manera transparente en dominios Windows. Permite la visualización de los dispositivos inalámbricos conectados por usuario. Permite la visualización de los dispositivos inalámbricos conectados por IP. Permite la visualización de los dispositivos inalámbricos conectados por tipo de autenticación. Permite la visualización de los dispositivos inalámbricos conectados por canal. Permite la visualización de los dispositivos inalámbricos conectados por ancho de banda usado. Permite la visualización de los dispositivos inalámbricos conectados por potencia de la señal. Permite la visualización de los dispositivos inalámbricos conectados por tiempo de asociación. Soporta Fast Roaming en autenticación con portal cautivo. Soporta configuración de portal cautivo por SSID. Permite el bloqueo de tráfico entre los clientes conectados a un SSID y AP específico. Es compatible con Wi-Fi Protected Access (WPA) y WPA2 por SSID, usando un algoritmo AES y / o TKIP. Es compatible con el protocolo 802.1x RADIUS. La controladora inalámbrica deberá permitir configurar los parámetros de radio como banda y canal. La controladora permite métodos de descubrimiento de puntos de acceso de manera automática. La controladora permite métodos de descubrimiento de puntos de acceso por IP estática. La controladora permite métodos de descubrimiento de puntos de acceso por DHCP. La controladora permite métodos de descubrimiento de puntos de acceso por DNS. La controladora permite métodos de descubrimiento de puntos de acceso por Broadcast. La controladora permite métodos de descubrimiento de puntos de acceso por Multicast. La controladora inalámbrica suministra una lista de Puntos de Acceso autorizados y	

OPERADO CON RECURSOS FAFEF -2022-

	puntos de acceso indebidos (Rogue). La controladora cuenta con protección contra ataques ARP Poisoning en el controlador inalámbrico. La controladora cuenta con mecanismos de protección de tramas de administración de acuerdo a las especificaciones de la alianza Wi-Fi y estándar 802.11ac. La controladora inalámbrica tiene de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo ASLEAP. La controladora inalámbrica tiene de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Association Frame Flooding. La controladora inalámbrica tiene de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Authentication Frame Flooding. La controladora inalámbrica tiene de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Broadcasting De-authentication. La controladora inalámbrica tiene de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo EAPOL Packet flooding. La controladora inalámbrica tiene de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Invalid MAC OUI. La controladora inalámbrica tiene de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Long Duration Attack. La controladora inalámbrica tiene de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Null SSID probe response. La controladora inalámbrica tiene de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Spoofed De-authentication. La controladora inalámbrica tiene de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Weak WEP IV Detection. La controladora inalámbrica tiene de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Wireless Bridge. Implementar canales de auto-aprovisionamiento de los puntos de acceso con el fin de minimizar la interferencia entre ellas. Permite seleccionar el día y hora en que se producirá la optimización de aprovisionamiento automática de canales en los puntos de acceso. La controladora inalámbrica permite agendar horarios para determinar en qué momento la red inalámbrica (SSID) se encuentra disponible. La controladora inalámbrica ofrece funcionalidad de Firewall integrado UTM basado en la identidad del usuario. Permite configurar el número máximo de clientes que pueden ser permitidos por SSID. Permite configurar el número máximo de clientes que pueden ser permitidos por punto de acceso. Permite configurar el número máximo de clientes que pueden ser permitidos por Radio. La controladora permite crear, administrar y autorizar las redes inalámbricas mesh. Ofrece un mecanismo de creación automática y/o manual de usuarios visitantes y contraseñas, que puedan ser enviados por correo electrónico o SMS a los usuarios, con ajuste de tiempo de expiración de la contraseña. La comunicación entre la controladora y el punto de acceso inalámbrico puede ser realizada de forma cifrada utilizando protocolo DTLS. Tiene un mecanismo de ajuste automático de potencia de la señal con el fin de reducir la interferencia entre canales entre dos puntos de acceso administrados. Ofrece un mecanismo de balanceo de trafico/usuarios entre Puntos de acceso.	

FAFEF OPERADO CON RECURSOS -2022-

	Proporciona un mecanismo de balanceo de trafico/usuarios entre frecuencias y/o radios de los Puntos de Acceso. Permite la identificación del firmware utilizado por cada punto de acceso gestionado y permitir la actualización a través de la interfaz gráfica. Permite que sean deshabilitados clientes inalámbricos que tengan baja tasa de transmission. Permite ignorar a los clientes inalámbricos que tienen señal débil, estableciendo un umbral de señal a partir de la cual los clientes son ignorados. La controladora permite configurar el valor de Short Guard Interval para 802.11n y 802.11ac en 5 GHz. Permite seleccionar individualmente para cada punto de acceso los SSID que van a ser propagados. Permite asociación dinámica de VLANs a los usuarios autenticados en un SSID específico mediante protocolo RADIUS. Permite asociación dinámica de VLANs a los usuarios autenticados en un SSID específico mediante vlan pooling. Permite visualizar las aplicaciones y amenazas por cada dispositivo inalámbrico. La controladora inalámbrica permite identificar los clientes WiFi que presenten algún riesgo basado en aplicaciones. La controladora inalámbrica permite identificar los clientes WiFi que presenten algún riesgo basado en dirección de destino. La controladora inalámbrica permite identificar los clientes WiFi que presenten algún riesgo basado en amenaza. La controladora inalámbrica permite identificar los clientes WiFi que presenten algún riesgo basado en sesiones. La controladora inalámbrica Soporta una licencia que permita al menos 10000 firmas de aplicaciones para reconocimiento de tráfico. El controlador inalámbrico tiene un interface de administración integrado en el mismo equipo. El controlador inalámbrico Soporta la funcionalidad de Fast-roaming para enlaces mesh entre el nodo secundario y nodos principals. La controladora inalámbrica Soporta aceleración de tráfico del protocolo CAPWAP a través de un procesador de red de propósito específico. La controladora inalámbrica Soporta aceleración de túnel de tráfico de puente inalámbrico a través de un procesador de red de propósito específico. La controladora inalámbrica Soporta protocolo LLDP. Permite la técnica de detección de APs intrusos On-wire a través de dirección MAC exacta. Permite la técnica de detección de APs intrusos On-wire a través de dirección MAC adyacente. Permite la visualización de los usuarios conectados en forma de topología lógica de red representando la cantidad de datos transmitidos y recibidos. La controladora inalámbrica permite combinar redes WiFi y redes cableadas con un software switch integrado. La controladora inalámbrica permite crear un portal cautivo en el software switch integrado para redes WiFi y redes cableadas. La controladora inalámbrica permite gestionar switches de acceso del mismo fabricante de la solución. Soporta la conversión de Multicast a Unicast para mejorar el rendimiento del tiempo	

OPERADO CON RECURSOS FAFEF -2022-

	de aire. En el entorno de alta disponibilidad, existe el concepto de controladores primarios y secundarios en la unidad AP, permitiendo que la unidad decida el orden en el que el AP selecciona una unidad controladora y cómo la unidad AP se conecta a un controlador de backup en el caso de que el controlador primario falle. Proporciona la capacidad de crear varias claves pre-compartidas de acceso protegido WiFi (WPA-PSK) para que no sea necesario compartir PSK entre dispositivos. Licenciamiento y actualizaciones. **Tamaño de licencias:** El licenciamiento de todas las funcionalidades es ILIMITADO en cuanto a usuarios, conexiones, equipos que pasan a través de la solución, limitándose solamente por el desempeño del equipo. **Vigencia de licencia de actualización y soporte:** La vigencia de las actualizaciones para los servicios de Antivirus, Sandbox en la nube, IPS y Filtrado de URL es por **36 meses.** El fabricante cuenta con un centro de atención al cliente (TAC) basado en la ciudad de México con atención y soporte en lenguaje Español. Además de un soporte mundial tipo "follow-the-sun". **Respaldo del proveedor:** Se incluyen los siguientes documentos para respaldar a "El Proveedor": Certificados de nueve ingenieros certificados en la solución Fortinet, para realizar las actividades de instalación, configuración, puesta a punto y en marcha, con los niveles de certificación NSE4, NSE5, NSE6 y NSE7 Y un ingeniero Certificado en Check Point Certified Security Expert R80, para la interconexión y convivencia con de la nueva solución. **Servicio de instalación:** Montaje de equipo en rack e interconexión de red. Registro del appliance en el portal Web del fabricante. Actualización de firmware a la última versión estable. Configuración de parámetros de red (IP, Hostname, rutas estáticas,DNS, NTP). Configuración de interfaces (PI, DHCP, VLAN). Configuración de SD-WAN con 2 enlaces de internet. Configuración de perfiles de seguridad: FW, VPN, IPS, APLC, WEBF, AV con 3 perfiles básicos. Configuración de políticas de firewall y objetos de direcciones, hasta 2 políticas por interfaz. Configuración de hasta 3 políticas de traffic shaping Configuración de rutas por un ingeniero nivel NSE7 de equipo con Firewall, filtrado WEB, aplicación Control, IPS, 5 políticas. La configuración del equipo considera la interconexión, identificación y convivencia con los otros tres firewall ya instalados y en operación en las oficinas registrales de Cd. del Carmen, Escárcega y Site en Palacio de Gobierno. Pruebas de funcionalidad sobre servicios habilitados. Transferencia de conocimientos básica. Entrega de Memoria Técnica.	

OPERADO CON RECURSOS FAFEF -2022-

Soporte del proveedor:
Se considera un soporte por parte de "El Proveedor" el cual tiene los siguientes alcances:
Duración de 36 meses.
Atención de fallas con un tiempo máximo de 2 horas.
Considera un (1) mantenimiento preventivo al año, previo acuerdo con el área requirente. Los insumos necesarios para el mantenimiento deberán correr por cuenta de "El Proveedor".
Incluir 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 libere nuevas versiones dentro de la vigencia de la póliza de soporte, "El Proveedor" instalará sin costo para la convocante dichas actualizaciones.

Asistencia técnica:
"El Proveedor" cuenta con un centro de consulta o asesoría telefónica que permite al personal técnico del área requirente realizar aclaraciones y consultas sobre el uso y configuración del equipo antes mencionado. Para esta clase de servicio no se totalizan horas mensuales en uno o varios eventos, los eventos son ilimitados y no habrá restricción en la duración de cada evento.

Tiempos de respuesta de atención/solución:
El tiempo del inicio de atención o respuesta a un reporte efectuado:
Tiempo máximo de solución de fallas después del inicio de la atención:
Dos horas como máximo para inicio de diagnóstico, en el caso de fallas mayores su atención se continúa aún fuera de horario de cobertura hasta su solución, sin ningún costo, siempre que haya iniciado su atención dentro del horario de servicio.
En el caso de que en alguna reparación de los equipos se requiera cambio o sustitución de alguna parte o componente, "El Proveedor" tendrá la obligación de remplazarlo en sitio, dentro del tiempo máximo de atención del reporte. Si el equipo no pudiera repararse dentro de los tiempos establecidos, "El Proveedor" deberá sustituir el equipo o parte dañada con equipo de respaldo que cuenta con las mismas características o superiores que el equipo original, esta sustitución se efectuará dentro de los tiempos máximos de atención definidos y permanecerá durante el tiempo que tarde la compostura del equipo dañado.
En el caso de que existan equipos de respaldo instalados al término del contrato, estos deberán seguir dando el servicio hasta que se reparen los equipos dañados, aun cuando haya terminado la vigencia del contrato, extendiéndose los derechos que se otorgan para estos reportes de falla, en los términos originales.
Sí después de realizado el mantenimiento correctivo a un equipo, este vuelve a presentar la misma falla, se considera como no realizado y su reparación es sin cargo alguno.
"El Proveedor" estará obligado a continuar con la atención, sin costo, de fallas o problemas detectados dentro de la vigencia del contrato hasta su solución, aun cuando ésta, se extienda más allá de aquélla; prorrogándose los derechos que otorga dicho contrato para estos reportes de falla, en los términos originales.

Mantenimiento Preventivo:

OPERADO CON RECURSOS FAFEF -2022-

	El mantenimiento preventivo se deberá dar a todos y cada uno de los equipos inventariados señalados en el programa de mantenimiento preventivo, 1 (una) vez durante la vigencia del contrato. El mantenimiento deberá ser proporcionado al "hardware" y al "software" que componen los equipos, con la finalidad de mantener la vigencia tecnológica del equipo, este mantenimiento incluirá las actualizaciones del "software" a la última versión gratuita emitida por el fabricante y que no requieran modificaciones en el hardware del equipo. Se considera proporcionar, por escrito, un análisis experto del estado que guarda el hardware y software, con la finalidad de garantizar un óptimo nivel del funcionamiento de los equipos. Se elaborará y revisará conjuntamente el personal técnico, el programa de trabajo, las actividades y fechas del mantenimiento preventivo a detalle; con cantidades, nombres de los responsables a ejecutar y supervisar la aplicación de dichos servicios, a más tardar en la segunda semana contada a partir de la formalización del contrato. Se entregará copia de los programas, procedimientos o calendarios formalizados conjuntamente en la fase de revisión. En caso de que existan modificaciones al programa validado, estas se registrarán por escrito y de común acuerdo entre ambas partes. Para el cumplimiento del programa de mantenimiento preventivo "El Proveedor" presentará por escrito los recursos humanos y técnicos, así como protocolos de prueba, con los que cubrirá el servicio. **Actividades consideradas:** Limpieza física de los equipos. Revisión de conexiones eléctricas, de tierra física y de datos. Pruebas de diagnóstico al hardware de los equipos. Actualizaciones de software a la última versión emitida por el fabricante y que no requieren modificaciones en el hardware del equipo. Instalación de parches de seguridad en caso de ser requerido. Respaldos de configuraciones. Entregará por escrito, un análisis experto del estado que guarda el hardware y software de los equipos. Reporte de actividades. "El Proveedor" considera todos los gastos asociados al mantenimiento incluyendo servicio, materiales y accesorios requeridos. **Mantenimiento Correctivo:** Se proporcionarán los mantenimientos correctivos surgidos durante la vigencia del contrato, al hardware y software del equipo, el cual incluirá las refacciones y/o partes originales y actualizaciones del "software" que se requieran para reparaciones del equipo, así mismo se deberá suministrar la mano de obra para su instalación. Los equipos que se utilicen en todos los casos tendrán la calidad y características técnicas iguales o superiores a las del equipo original, de tal manera que se garantice el funcionamiento adecuado del hardware y software. Se aplicarán las pruebas de diagnóstico y operación de respaldo antes de proceder a la reparación de este, según resulte el diagnóstico aplicado. Al finalizar se entregará copia del reporte de servicio de mantenimiento correctivo. En el caso de una contingencia mayor o de severidad crítica, "El Proveedor" asignará un ingeniero en sitio hasta la resolución total del problema.	

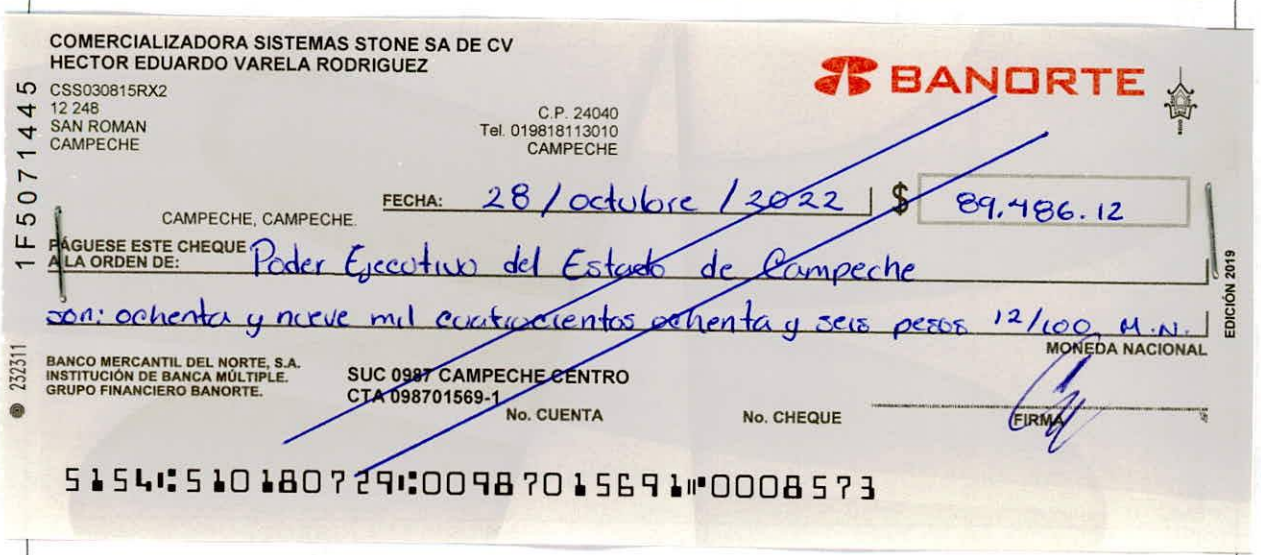
OPERADO CON RECURSOS FAFEF -2022-

San Francisco de Campeche a 28 de Octubre del 2022

PODER EJECUTIVO DEL ESTADO DE CAMPECHE
SECRETARIA DE ADMINISTRACIÓN Y FINANZAS
DIRECCIÓN GENERAL DE RECURSOS MATERIALES
DIRECCIÓN DE RECURSOS MATERIALES

GARANTÍA DE CUMPLIMIENTO Y VICIOS OCULTOS, CORRESPONDIENTE AL 20% DEL MONTO TOTAL DEL CONTRATO NÚMERO 123/2022.

RAZON SOCIAL: COMERCIALIZADORA SISTEMAS STONE SA DE CV.


COMERCIALIZADORA SISTEMAS STONE SA DE CV
HECTOR EDUARDO VARELA RODRIGUEZ
CSS030815RX2
12 248
SAN ROMAN
CAMPECHE
C.P. 24040
Tel. 019818113010
CAMPECHE
BANORTE
1F5071445
CAMPECHE, CAMPECHE.
FECHA: 28/octubre/2022
$ 89,486.12
PÁGUESE ESTE CHEQUE A LA ORDEN DE: Poder Ejecutivo del Estado de Campeche
son: ochenta y nueve mil cuatrocientos ochenta y seis pesos 12/100, M.N.
MONEDA NACIONAL
EDICIÓN 2019
232311
BANCO MERCANTIL DEL NORTE, S.A.
INSTITUCIÓN DE BANCA MÚLTIPLE.
GRUPO FINANCIERO BANORTE.
SUC 0987 CAMPECHE CENTRO
CTA 098701569-1
No. CUENTA
No. CHEQUE
FIRMA
5154:510180729:00987015691:0008573

TIPO DE DOCUMENTO: CHEQUE CRUZADO

NUMERO: 0008573
IMPORTE: $ 89,486.12
NUMERO DE CUENTA:098701569-1

DE FECHA: 28/10/2022
CON CARGO A: BANCO MERCANTIL DEL NORTE S.A.

Carlos A. Novelo Basto
Representante Legal

OPERADO CON RECURSOS FAFEF -2022-

Comercializadora Sistemas Stone S.A. de C.V.
+52(981) 811 3010
contacto@sistemasstone.com.mx
C 12 #248, Col. San Roman, Campeche, Camp. C.P. 24040 RFC CSS-030815-RX2
www.sistemasstone.com.mx