GOBIERNO DE EL SALVADOR

CAJA MUTUAL DE LOS EMPLEADOS DEL MINISTERIO DE EDUCACIÓN

ORDEN DE COMPRA No 89/2019
LIBRE GESTIÓN No 67/2019
FECHA: 09 de Agosto de 2019

NOMBRE DE LA CONTRATISTA: JMTELCOM, JESÚS MARTÍNEZ Y ASOCIADOS, S.A. DE C.V.
(NIT 0614-091288-102-2)

UNIDAD SOLICITANTE: TECNOLOGÍAS DE INFORMACIÓN

Solicito a usted(es) entregar a La Caja Mutual de los Empleados del Ministerio de Educación, lo requerido en esta orden.

ITEM	CANTIDAD	DESCRIPCIÓN	PRECIO UNITARIO	TOTAL
		"Suministro de equipos informáticos, proyección y de seguridad", según el siguiente detalle:		
6	1	FIREWALL PERIMETRAL, Marca FORTINET, modelo FORTIGATE 30E Características Generales 1. Plataforma con sistema operativo endurecido (no disco duro), para un mejor desempeño y menor posibilidad de fallas. 2. Se solicita que el hardware a ofrecer, soporte alta disponibilidad, en activo-activo y activo-pasivo (Para implementación futura). 3. Posibilidad de definir al menos dos interfaces para sincronía de H-A. 4. El H-A debe permitir redundar todas las funcionalidades tales como: VPN, Filtrado de Contenido Web, IPS, Antivirus, Antispam, por lo que se requiere redundancia en todos sus módulos. 5. Soporte a alta disponibilidad transparente, es decir, sin pérdida de conexiones en caso de que un nodo falle. 6. Debe soportar administración a través de GUI (HTTPS y HTTP), TELNET, SSH, CLI, etc. 7. Soporte de SNMP. 8. Debe de soportar diferentes niveles de acceso y permisos a la administración, de modo que se pueda dar acceso a usuarios de administrador, reportes, firewall, filtrado Web, etc., O solo lectura, etc. (administración basada en roles). 9. Debe permitir la descarga de backups de configuración, desde el GUI, TFTP y SCP. 10. Debe soportar dominios virtuales, a modo de poder crear varios sistemas virtuales con diferente administración y configuración. (incluir 5). 11. Que se pueda hacer distribución de recurso para cada dominio, para VPNS, sesiones, políticas, etc. 12. Los dominios deben operar de forma independiente, permitiendo funcionar unos en modo ruteo y otros en modo transparente. 13. Debe soportar actualización de firmware por TFTP y GUI. 14. La interface gráfica de usuario (GUI) vía web deberá poder estar en inglés con opción español, configurable por el usuario. 15. El administrador del sistema podrá tener las opciones incluías de autenticarse vía password y vía certificados digitales. 16. El equipo ofrecerá la flexibilidad para especificar que los administradores puedan estar restringidos a conectarse desde ciertas direcciones IP cuando se utilice SSH, TELNET, HTTP o HTTPS. 17. El equipo deberá poder administrarse en su totalidad (incluyendo funciones de seguridad, ruteo y bitácoras) desde cualquier equipo conectado a internet que tenga un browser (Internet Explorer, Chrome, Firefox) instalado sin necesidad de instalación de ningún software adicional. 18. Que permita política para fortalecimiento de password de administradores. 19. Inclúyase funcionalidad de intercepción de tráfico SSL, para poder hacer inspección y protección de ataques o tráfico malicioso a través de la comunicación encriptada. Soportada para los siguientes protocolos: HTTPS, POP3S, SMTPS, y IMAPS. 20. La solución debe permitir escanear virus y ataques a través del tráfico encriptado. 21. Que permita hacer reglas de excepción de inspección de tráfico (por	$ 1,250.00	$ 1,250.00

NOMBRE DE LA CONTRATISTA: JMTELCOM, JESÚS MARTÍNEZ Y ASOCIADOS, S.A. DE C.V. (NIT 0614-091288-102-2)

UNIDAD SOLICITANTE: TECNOLOGÍAS DE INFORMACIÓN

ITEM	CANTIDAD	DESCRIPCIÓN	PRECIO UNITARIO	TOTAL
		ejemplo no interceptar transacciones a sitios financieros). 22. Administración de ancho de banda (traffic shaping) con opciones tales como: traffic shaping basado en políticas, etc. 23. Soporte de VPN con estándar IPSEC, SSL, PPTP, L2TP. 24. Además debe permitir autenticación de usuarios a través de una base local. 25. Debe permitir integrarse con sistemas de autenticación tales como: RADIUS, LDAP, ACTIVE DIRECTORY, TACACS+. 26. Debe soportar autenticación de usuarios de tipo Single Sign On, para Active Directory; de modo que el usuario solo tenga que autenticarse en el dominio de AD, y que ya no requiera autenticación para los servicios de navegación y otros que pasen por el firewall. 27. Debe de permitir creación de políticas basadas en FQDN, para poder controlar Hosts de forma independiente, tanto del lado de la LAN como del Internet. 28. Debe de soportar aplicaciones y protocolos de multimedia tales como: H.323, SIP, SCCP. 29. La solución debe tener capacidad de generación de VLANS TAG (802.1q). 30. Debe de soportar modo de operación transparente y NAT (ruteo). 31. Debe soportar IP secundarias en cada una de sus interfaces. 32. Soporte de DHCP server, regular o relay. 33. Soporte de NAT y PAT. 34. Las políticas de restricción o acceso deben de permitir la asociación por IP fuente, IP destino, grupos de usuarios o FQDN. 35. Debe soportar la creación de políticas para permiso o denegación en base a schedule. 36. Soporte de creación de nuevos servicios con propósito de permitir o denegarlos. 37. La solución debe de soportar IPV4 e IPV6. 38. Soporte a reglas de firewall para tráfico de multicast, pudiendo especificar puerto físico fuente, puerto físico destino, direcciones IP fuente, dirección IP destino. 39. Deberá soportar reglas de firewall en IPV6 configurables tanto por cli (Command Line Interface -interface de línea de comando-) como por GUI (graphical user interface). 40. Que permita hacer políticas de firewall basadas en filtros geográficos. 41. Debe soportar Internet Content Adaptation Protocol (ICAP). 42. Soporte de protocolo WCCP. Filtrado de Contenido WEB 1. El dispositivo solicitado, debe incluir un sistema de filtrado de contenido WEB, para HTTP y HTTPS. 2. Facilidad para incorporar control de sitios a los cuales naveguen los usuarios, mediante categorías. Por flexibilidad, el filtro de URLS debe tener por lo menos 80 categorías divididas en grupos principales y por lo menos 2 billones de páginas WEB en la base de datos. 3. 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. 4. Que permita la implementación de políticas de búsqueda segura (Safe Search), para los buscadores de INTERNET, tales como Google, Yahoo y		

ITEM	CANTIDAD	DESCRIPCIÓN	PRECIO UNITARIO	TOTAL
		Bing. 5. Que soporte filtrado WEB para determinados usuarios, aplicando cuotas de tiempo de navegación. 6. Configurable directamente desde la interfaz de administración del dispositivo appliance. Con capacidad para permitir esta protección por política de control de acceso. 7. Deberá permitir diferentes perfiles de utilización de la Web (permisos diferentes para categorías) dependiendo de fuente de la conexión o grupo de usuario al que pertenezca la conexión siendo establecida. 8. 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), deberán ser personalizables. 9. Capacidad de filtrado de scripts en páginas Web (Java/Active X). 10. Debe permitir restricción o acceso a diferentes categorías, tales como: bussiness, hacking, no productivas, spyware y malware, controversiales, finanzas, etc. 11. Que permita bloqueo por: URL, keyword o frase. 12. Lista de excepción de URL. 13. Que permita la creación de al menos 50 categorías locales. Red Privada Virtual (VPN en IPSec y SSL) 1. Posibilidad de crear VPN's entre gateways y clientes con IPSEC. Esto es, VPNs IPSec site-to-site y VPNs IPSec client-to-site. 2. Soporte a certificados PKI x.509 para construcción de VPNS cliente a sitio (client-to-site). 3. Soporte de VPNS con algoritmos de cifrado: DES, 3DES, AES. 4. Se debe soportar longitudes de llave para aes de 128, 192 y 256 Bits. 5. Debe soportar IKE v2. 6. La VPN ipsec deberá poder ser configurada en modo interface (interface-mode VPN). 7. En modo interface, la VPN IPSEC deberá poder tener asignada una dirección IP, tener rutas asignadas para ser encaminadas por esta interface y deberá ser capaz de estar presente como interface fuente o destino en políticas de firewall. 8. Debe además poder asignarse ancho de banda especificado para los diferentes túneles con diferentes niveles de prioridad (QOS). 9. Debe soportar load sharing sobre las VPN con protocolos tales como ECMP, de tal forma que pueda haber más de 2 VPN activas y que se pueda repartir el tráfico entre ambas de forma simultánea. 10. El sistema debe permitir, escaneo de virus sobre los túneles encriptados. 11. Soporte de túneles VPN en SSL vía portal Web (acceso a través de un navegador) y a través de cliente (software instalado en host). 12. Soporte a certificados PKI X.509 para construcción de VPNS SSL. 13. Soporte a asignación de aplicaciones permitidas por grupo de usuarios. 14. Soporte nativo para al menos HTTP, FTP, SMB/CIFS, VNC, SSH, RDP Y TELNET. 15. Deberá poder verificar la presencia de antivirus (propio y/o de terceros y de un firewall personal (propio y/o de terceros) en la máquina que establece la comunicación VPN SSL. 16. Capacidad integrada para eliminar y/o cifrar el contenido descargado al caché de la máquina cliente (caché cleaning).		

NOMBRE DE LA CONTRATISTA: JMTELCOM, JESÚS MARTÍNEZ Y ASOCIADOS, S.A. DE C.V. (NIT 0614-091288-102-2)

UNIDAD SOLICITANTE: TECNOLOGÍAS DE INFORMACIÓN

ITEM	CANTIDAD	DESCRIPCIÓN	PRECIO UNITARIO	TOTAL
		17. La VPN SSL integrada deberá soportar a través de algún Plug-In Activex y/o Java, la capacidad de meter dentro del túnel SSL tráfico que no sea HTTP/HTTPS. 18. Deberá soportar la redirección de página HTTP a los usuarios que se registren en la VPN SSL, una vez que se hayan autenticado exitosamente. 19. Para el caso del cliente instalado en host, éste debe ser compatible para sistemas operativos tales como: WINDOWS, MAC y LINUX. 20. Que permita autenticación de 2 factores. 21. Soporte de tuneles PPTP. Ruteo 1. La solución debe tener capacidad de ruteo con protocolos tales como RIP (v. 1 y 2), OSPF, BGP y MULTICAST (para ser usados también en túneles VPN). 2. Soporte a ruteo estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas. 3. Debe soportar la creación de políticas de ruteo, de modo que se pueda enrutar tráfico por las diferentes interfaces, basándose en IP fuente, IP destino, puerto fuente, puerto destino, TOS o por protocolos. 4. Ruteo para IPV4 e IPV6. 5. Ruteo entre diferentes dominios virtuales. 6. Soporte de ECMP para distribución de cargas entre los diferentes enlaces. 7. Funcionalidad de DHCP: como cliente DHCP, servidor DHCP y reenvío (relay) de solicitudes DHCP. 8. Que soporte redundancia automática de enlaces, con el fin de que si un enlace falla, pueda enrutar el trafico saliente a través de otro enlace disponible, sin necesidad de hacer cambios en las conexiones de los sistemas. 9. Soporte a etiquetas de VLAN (802.1Q) y creación de zonas de seguridad en base a VLANS. 10. Soporte a políticas de ruteo (policy routing). 11. El soporte a políticas de ruteo deberá permitir que ante la presencia de dos enlaces a internet, se pueda decidir cuál tráfico sale por un enlace y qué tráfico sale por otro enlace. 12. Soporte a ruteo de MULTICAST. 13. Soporte de VRRP. 14. Soporte de SFLOW. 15. Soporte de agregación de enlaces (802.3AD). Otros Requerimientos 1. Incluye la capacidad de poder hacer actualizaciones necesarias para la correcta operación del equipo con las características arriba descritas, por espacio **mínimo de 5 años.** 2. El contratista cuenta con un sistema de Helpdesk para la captura, seguimiento y conclusión de los requerimientos recibidos por parte de la Institución, con la finalidad de que CCR pueda solicitar reportes si lo considera pertinente para la resolución o toma de acciones en situaciones específicas o reclamos por garantía, por lo que la oferta deberá indicar que cumple con dicho requisito. 3. Se impartirá una capacitación para los administradores de los equipos (al menos dos personas), con una **duración mínima de 16 horas** y deberá		

NOMBRE DE LA CONTRATISTA: JMTELCOM, JESÚS MARTÍNEZ Y ASOCIADOS, S.A. DE C.V.
(NIT 0614-091288-102-2)

UNIDAD SOLICITANTE: TECNOLOGÍAS DE INFORMACIÓN

ITEM	CANTIDAD	DESCRIPCIÓN	PRECIO UNITARIO	TOTAL
		orientarse a la administración de los equipos, generación e interpretación de reportes e indicadores, diagnósticos básicos, cobertura de la garantía, por lo que la oferta deberá indicar que cumple con dicho requisito. 4. El equipo de seguridad deberá interactuar entre el equipo de comunicaciones del ISP y La red de servidores de Correo Local en CCR. 5. Se **incluiye carta de autorización del fabricante del producto**, que indique que el Proveedor es Certificado para la Distribución y mantenimiento de los productos ofrecidos. 6. Se contará al menos con **5 técnicos certificados de fábrica**, residentes en el país, para dar soporte en la solución que ofrece. 7. El tiempo máximo de respuesta por soporte, de parte del Oferente, no podrá ser mayor a 4 horas, desde que se le reporte una falla durante el tiempo de garantía. 8. Garantía: Los equipos ofertados (FortiGate 30E y FortiAp 221E), cuentan con garantía de un año por desperfectos de fabricación, que pueden ser extendidos anualmente a través de un contrato de FortiCare, así mismo, las actualizaciones para el correcto funcionamiento y soporte podrán ser renovados anualmente en los próximos 5 años		
7	2	Acces Point, Marca: FORTINET, modelo FORTI AP 221E 1. Factor de forma: External. 2. Alimentación por Ethernet (PoE): IEEE 802.3af (12.9W). 3. Diseño resistente para interiores. 4. Banda de frecuencias 2.4 GHz/5 GHz. 5. Número de antenas: 4 internas. 6. Tecnología de conectividad inalámbrica. 7. Compatible con los protocolos de interconexión IEE: 802.11a, 802.11b, 802.11e, 802.11g, 802.11h, 802.11i, 802.11j, 802.11n, 802.1x, 802.3af, 802.11ac. 8. Incorporar características: Tecnología 2T2R MIMO (Múltiple entrada múltiple salida) para aumento de tasa de transferencia y cobertura, comprobación de paridad de baja densidad (LDPC), montaje en pared o en techo, Máxima probabilidad de demodulación (MLD), Maximum Ratio Combining (MRC), calidad de servicio (QoS), Transmit Beam-forming (TxBF) ready, soporte de Wi-Fi Multimedia (WMM), detección de puntos de acceso fraudulento, ranura para bloqueo de seguridad. 9. Velocidad de transferencia de datos 867 Mbps. 10. Puerto de conexión Ethernet: 1xGE RJ45. 11. Algoritmo de cifrado: RC4, TLS, TTLS, TKIP, WPA, WPA2, WPA-PSK, AES-CCMP, WPA2-PSK, WEP Método de autentificación MS-CHAP v.2, Extensible Authentication Protocol (EAP), EAP-FAST. 12. Adaptador de alimentación externo. 13. Frecuencia requerida: 50/60 Hz. 14. Compatible con Firewall FortiGate modelo 240D. 15. Garantía de 1 Año. 16. Esto incluye: a. Servicios profesionales de instalación y configuración, sin costo adicional para La Caja. b. Servicio de soporte en sitio con técnicos certificados en NSE 7, contrato 8 horas x 5 días x 12 meses, sin costo adicional para La Caja. Otros Requerimientos 1. Tendrá la capacidad de poder hacer actualizaciones necesarias para la	$ 715.69	$ 1,431.38

GOBIERNO DE EL SALVADOR

CAJA MUTUAL DE LOS EMPLEADOS DEL MINISTERIO DE EDUCACIÓN

ORDEN DE COMPRA No 89/2019
LIBRE GESTIÓN No 67/2019
FECHA: 09 de Agosto de 2019

NOMBRE DE LA CONTRATISTA: JMTELCOM, JESÚS MARTÍNEZ Y ASOCIADOS, S.A. DE C.V.
(NIT 0614-091288-102-2)

UNIDAD SOLICITANTE: TECNOLOGÍAS DE INFORMACIÓN

ITEM	CANTIDAD	DESCRIPCIÓN	PRECIO UNITARIO	TOTAL
		correcta operación del equipo con las características arriba descritas, por espacio **mínimo de 5 años.** 2. Se contará con un sistema de Helpdesk para la captura, seguimiento y conclusión de los requerimientos recibidos por parte de la Institución, con la finalidad de que CCR pueda solicitar reportes si lo considera pertinente para la resolución o toma de acciones en situaciones específicas o reclamos por garantía. 3. Los oferentes deberán **incluir carta de autorización del fabricante del producto**, que indique que el Proveedor es Certificado para la Distribución y mantenimiento de los productos ofrecidos. 4. Se contará al menos con **5 técnicos certificados de fábrica,** residentes en el país, para dar soporte en la solución que ofrece. 5. El tiempo máximo de respuesta por soporte, de parte del contratista, no podrá ser mayor a 4 horas, desde que se le reporte una falla durante el tiempo de garantía.		
		Garantía: Mínima de 1 año por desperfectos de fábrica.		
		Tiempo de entrega: 30 días calendario, después de recibida la Orden de Compra		
		Lugar de entrega: Oficina central de La Caja Mutual, ubicada en Calle Guadalupe y Blvd. Dr. Héctor Silva # 156, Colonia Médica, San Salvador.		
		Administradora de la orden de compra, Karla Ramírez, Técnica de TI.		
		SON DOS MIL SEISCIENTOS OCHENTA Y UNO 38/100 DÓLARES		$ 2,681.38

FORMA DE PAGO: CON QUEDAN A 8 DÍAS CALENDARIO

NOTA: Se retendrá en concepto de anticipo del Impuesto a la Transferencia de Bienes Muebles y a la prestación de Servicios, el 1% por ciento, de conformidad al artículo 162 del Código Tributario, por lo que deberá emitir la factura indicando el valor de la retención.

Realizado
UACI

UNIDAD DE ADQUISICIONES Y CONTRATACIONES INSTITUCIONAL

PRESIDENCIA

ADJUDICADO
Presidente en funciones

Vo.Bo.
Jefe Unidad de Administración

UNIDAD DE ADMINISTRACION

Vo. Bo.

GERENCIA

rgv