

**NOMBRE DE LA EMPRESA: 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
2	15	<p><b>SUMINISTRO DE DISPOSITIVOS DE SEGURIDAD FIREWALL</b>, según el siguiente detalle:</p> <p>Marca: FORTIGATE, FORTIWIFI 30 E</p> <p>CARACTERÍSTICAS GENERALES:</p> <ul style="list-style-type: none"> <li>- Plataforma con sistema operativo endurecido (no disco duro), para un mejor desempeño y menor posibilidad de fallas.</li> <li>- Se solicita que el hardware a ofrecer, soporte alta disponibilidad, en activo-activo y activo-pasivo (Para implementación futura).</li> <li>- Posibilidad de definir al menos dos interfaces para sincronía de H-A</li> <li>- El H-A debe permitir redundar todas la funcionalidades tales como: VPN, Filtrado de Contenido Web, IPS, Antivirus, Antispam, por lo que se requiere redundancia en todos sus módulos.</li> <li>- Soporte a alta disponibilidad transparente, es decir, sin pérdida de conexiones en caso de que un nodo falle.</li> <li>- Debe soportar administración a través de GUI (HTTPS y HTTP), TELNET, SSH, CLI, etc.</li> <li>- Soporte de SNMP.</li> <li>- 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).</li> <li>- Debe permitir la descarga de backups de configuración, desde el GUI, TFTP y SCP.</li> <li>- Debe soportar dominios virtuales, a modo de poder crear varios sistemas virtuales con diferente administración y configuración. (Incluir 5).</li> <li>- Que se pueda hacer distribución de recurso para cada dominio, para VPNS, sesiones, políticas etc.</li> <li>- Los dominios deben operar de forma independiente, permitiendo funcionar unos en modo ruteo y otros en modo transparente.</li> <li>- Debe soportar actualización de firmware por TFTP y GUI.</li> <li>- La interface gráfica de usuario (GUI) vía web deberá poder estar en inglés con opción español, configurable por el usuario.</li> <li>- El administrador del sistema podrá tener las opciones incluías de autenticarse vía password y vía certificados digitales.</li> <li>- 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.</li> <li>- 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.</li> <li>- Que permita política para fortalecimiento de password de administradores.</li> <li>- Inclúyase funcionalidad de interceptación 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.</li> <li>- La solución debe permitir escanear virus y ataques a través del tráfico encriptado.</li> <li>- Que permita hacer reglas de excepción de inspección de tráfico (por ejemplo no interceptar transacciones a sitios financieros).</li> <li>- Administración de ancho de banda (traffic shaping) con opciones tales como: traffic shaping basado en políticas, etc.</li> <li>- Soporte de VPN con estándar IPSEC, SSL, PPTP, L2TP.</li> <li>- Además debe permitir autenticación de usuarios a través de una base local.</li> <li>- Debe permitir integrarse con sistemas de autenticación tales como: RADIUS, LDAP, ACTIVE DIRECTORY, TACACS+.</li> <li>- 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.</li> <li>- 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.</li> <li>- Debe de soportar aplicaciones y protocolos de multimedia tales como: H.323, SIP, SCCP.</li> <li>- La solución debe tener capacidad de generación de VLANS TAG (802.1q).</li> <li>- Debe de soportar modo de operación transparente y NAT (ruteo).</li> <li>- Debe soportar IP secundarias en cada una de sus interfaces.</li> <li>- Soporte de DHCP server, regular o relay.</li> <li>- Soporte de NAT y PAT.</li> <li>- Las políticas de restricción o acceso deben de permitir la asociación por IP fuente, IP destino, grupos de usuarios o FQDN.</li> <li>- Debe soportar la creación de políticas para permiso o denegación en base a schedule.</li> <li>- Soporte de creación de nuevos servicios con propósito de permitir o denegarlos.</li> </ul>		\$ 12,889.00



**NOMBRE DE LA EMPRESA: 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
		<ul style="list-style-type: none"> <li>- La solución debe de soportar IPV4 e IPV6.</li> <li>- Soporte a reglas de firewall para tráfico de multicast, pudiendo especificar puerto físico fuente, puerto físico destino, direcciones IP fuente, dirección IP destino.</li> <li>- 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).</li> <li>- Que permita hacer políticas de firewall basadas en filtros geográficos.</li> <li>- Debe soportar Internet Content Adaptation Protocol (ICAP).</li> <li>- Soporte de protocolo WCCP.</li> </ul>		
		FILTRADO DE CONTENIDO WEB, con detalle de especificaciones		
		RED PRIVADA VIRTUAL (VPN en IPSec y SSL), con detalle de especificaciones		
		RUTEO, con detalle de especificaciones		
		Además:		
		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.		
		Cuenta con un sistema de Helpdesk para la captura, seguimiento y conclusión de los requerimientos recibidos.		
		Deberá impartir una capacitación para los administradores de los equipos (al menos dos personas), con una duración mínima de 16 horas y deberá orientarse a la administración de los equipos, generación e interpretación de reportes e indicadores, diagnósticos básicos, cobertura de la garantía.		
		El equipo de seguridad deberá interactuar entre el equipo de comunicaciones del ISP y La red de servidores de Correo Local en CCR.		
		El tiempo máximo de respuesta por soporte, no podrá ser mayor a 4 horas, desde que se le reporte una falla durante el tiempo de garantía.		
		1 años de garantía por desperfectos de fabricación.		
		Tiempo de entrega: 45 días calendario máximo, después de recibida la orden de compra. Las especificaciones técnicas de la Libre Gestión, así como la oferta adjudicada, son parte integrante de esta orden de compra. Administrador de la orden de compra: Karla Ramírez, Técnica de Tecnologías de Información.		
		<b>**SON DOCE MIL OCHOCIENTOS OCHENTA Y NUEVE 00/100 DOLARES ****</b>		<b>\$ 12,889.00</b>

**FORMA DE PAGO: CON QUEDAN HASTA UN MÁXIMO DE 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



ADJUDICADO  
Presidente

Calle Guadalupe y Blvd. Dr. Héctor Silva # 156, Col. Médica, Edificio de Caja Mutual, San Salvador, Tel. 2132-4130/31