

Especificaciones Técnicas - SOLICITUD DE COTIZACION No: ASU/09/026

FECHA LIMITE DE PRESENTACION DE OFERTA: Viernes 04/09/09 a las 17:00 hs.

Item 2. EQUIPOS INFORMATICOS DE SEGURIDAD		
2.1 Router de Acceso		
Cantidad:		1 (UNO)
Características	REQUERIMIENTO MINIMO	Ofrecido
Marca	Especificar	
Modelo	Especificar	
Bahías libres	Al menos 2 bahias para tarjetas adicionales	
Puertos disponibles en chasis. Se requieren PUERTOS independientes. No se aceptaran puertos con funcionalidad Switch para ampliar la capacidad. Se deben cotizar puertos separados. Si se deben cotizar placas de Interfaces se deben cotizar las mismas en capacidad Gigabit en forma operativa unitaria.	2 interfaces Ethernet 10/100/1000	
Memoria RAM minima provista	512 MB	
Memoria RAM para operación . Se debe declarar la capacidad máxima de RAM del equipo ofertado.	Se debe proveer la memoria suficiente para soportar en forma operativa los requerimientos establecidos en el presente pliego. Presentar documentacion para avalar este dimensionamiento	
Expansion Memoria FLASH	1 GB.	
Fuente de alimentacion	220V AC 50Hz	
Puerto USB externo	2	
Instalacion en RACK 19"	Equipo apto para instalacion en Rack 19" sin necesidad de bandeja exterior	
Performance en VPN IPSec	200 Mbps o Superior	
Eficiencia de Routing minimo requerido para el equipo base. Medido en paquetes de 64K	200.000 pps o Superior	
Eficiencia de Routing minimo requerido para el equipo base con la funcionalidad de 3DES-SHA habilitado. Medido en paquetes de 64K	50.000 pps o Superior	
Cantidad máxima de VPN's IPSec a manejar	500 o Superior	
Soporte de protocolos de red	RFC 791/ 1812- IPv4 / Full stack IPv6	
Soporte de protocolos de ruteo	OSPFv2 / OSPFv3 / BGP Multiprotocolo /	
Soporte	VPNs RFC 4798, Soporte 6PE RFC 2702, Requirements for	
Soporte de Subneting	CIDR	
Alta disponibilidad	VRRP	
Función de translación red privada	NAT y PAT	
Soporte de NAT	Si	
Soporte de rutas con OSPF con la memoria ofrecida	Minimo 8.000	
Soporte de rutas estaticas con la memoria ofrecida	Minimo 8.000	
Soporte de Tuneles VPN concurrentes con la memoria ofrecida	Minimo 400	
Numero de Peers BGP	Minimo 40	
Standards en Interfaces Ethernet - LAN	Ethernet IEEE 802.3i - FastEthernet IEEE 802.3u - IEEE 802.1p - IEEE 802.1Q	
Licencia de acceso tipo VPN Cliente permitido	100 Usuarios	
Acceso de administració	Interface WEB, Telnet, SSHv2	
Soporte de QoS	Clasificacion-Clases- Colas de transmision- Políticas para cada clase – Soporte modelo DiffServ	
Garantía Total Extendida sobre hardware del fabricante, incluye renovación de versión de sistema operativ	2 Años	

Item 2. EQUIPOS INFORMATICOS DE SEGURIDAD		
2.1 Router de Acceso		
Cantidad:		1 (UNO)
Características	REQUERIMIENTO MINIMO	Ofrecido
Período de reemplazo ante falla 2 años	El equipo deberá ser reparado o reemplazado por otro que cumpla con estas especificaciones técnicas al siguiente día hábil a la notificación de la falla.	
MTBF minimo	50.000 horas	
Varios	CD con manuales, cable de consola y alimentación	
	El equipo ofertado debe tener certificación ISO 9001	
	Presentar documentación del fabricante donde autorice a la empresa oferente como representante para la región y avale la garantía exigida.	
	Presentar respaldado por escrito del fabricante a la empresa oferente autorizándola a prestar el servicio técnico y el cambio de partes por garantía, el cual deberá contar con stock de repuestos.	
	Los técnicos de la empresa oferente deberán estar certificados por el fabricante. Se exigirá la presentación de los certificados de los técnicos pertenecientes a la empresa autorizada por el fabricante. La documentación emitida por el fabricante; no deberá exceder a 4 (cuatro) años de su emisión.	
	En caso de que el equipo deba ser retirado por reparación dentro de la Garantía, el plazo máximo para la reposición en funcionamiento del mismo es de 15 días calendario. Durante este periodo el oferente deberá proporcionar un equipo en reemplazo temporal, que será devuelto contra entrega del equipo.	
	En la oferta debe incluirse el servicio de instalación y configuración, una vez instalado el equipo las configuraciones deben cubrir las necesidades detalladas por el Área de Informática.	
	El oferente será responsable por la puesta en marcha de plataforma teniendo que incluir los costos para los siguientes trabajos: .Creación de DMZ para alojar servidores y segmentación de LAN interna.	
	Creación de 5 perfiles de acceso a servicios.	
	Configuración de 3 Vlans segmentando Servicios en el nuevo Swtich Principal.	
	Capacitación sobre plataforma provista al personal IT (4 horas como mín.)	
Garantía.	2 años con actualización y soporte incluido.	
Tipo de Garantía	Tipo de Garantía y Servicio: en sitio bajo la modalidad 24x7, incluye reemplazo de hardware temporal mientras se gestiona el RMA del equipo con el fabricante.	

Item 2. EQUIPOS INFORMATICOS DE SEGURIDAD		
2.2 FIREWALL		
CANTIDAD:	1 (UNO)	
Características	REQUERIMIENTO MINIMO	Ofrecido
Marca	Especificar	
Modelo	Especificar	
Capacidad de Procesamiento de datos a filtrar en Firewall IMIX (declarar este valor)	500Mbps o Superior	
Capacidad de tráfico en paquetes por segundo en tamaño de 64 Kbps	200.000 pps o Superior	
Cantidad de usuarios habilitados en el firewall	Se debe cotizar la funcionalidad de acceso de usuarios ilimitados	
Performance sostenido con todos los servicios activos en simultaneo , AV+DI+UF en el equipo	Superior a 75 Mbps.	
Cantidad de Sesiones concurrentes	120.000 o Superior	
Vlans Sportadas	20	
Volumen de datos en VPN's	220 Mbps o Superior	
Cantidad máxima de VPN's IPSec a manejar	50	
Zonas Seguras sportadas	35 o Superior	
Funcionalidades Adicionales	<p>Debe soportar SNAT , DNAT y PAT</p> <p>Aplicación de SNAT y DNAT y PAT en forma simultanea sobre una misma conexión.</p> <p>Deberá soportar NAT estático y dinámico.</p> <p>Aplicación de PAT sobre cualquier tipo de conexión</p> <p>Deberá soportar la configuración de NAT estático sobre todas las interfaces físicas y lógicas utilizando direcciones IP virtuales que no sean las propias IP declaradas en las interfaces del firewall.</p> <p>Soporte de IPSec NAT Traversal</p> <p>Soporte de protocolo H323 soportando Nat Traversal</p> <p>El equipo deberá poder configurarse en modo L3 o en modo L2 (también conocido como Modo Transparente) que permita integrarse a una topología existente sin cambiar el direccionamiento IP de los equipos instalados previamente.</p> <p>Deberá proveer funcionalidad de Servidor y relay de</p> <p>DHCP en todas las interfaces físicas y lógicas.</p> <p>Deberá permitir monitoreo remoto mediante SNMP v2 permitiendo los queries de SNMP a través de la definición de direcciones IP autorizadas para realizar las consultas.</p> <p>Proveer de logeo remoto utilizando syslog</p> <p>Soporte de Alta disponibilidad en modo Activo-Pasivo.</p> <p>Soporte de WINS</p> <p>Autenticación de usuarios en forma local, por RADIUS, LDAP, Firmas digitales.</p> <p>Soporte de protocolo de enrutamiento RIP</p> <p>Soporte de Policy Based Routing basados en IP-Source/Puerto(TCP o UDP) IP-Destino/Puerto (TCP o UDP) y TOS</p>	

Item 2. EQUIPOS INFORMATICOS DE SEGURIDAD

2.2 FIREWALL

CANTIDAD:	1 (UNO)	
Características	REQUERIMIENTO MINIMO	Ofrecido
	<p>La solución deberá permitir el uso de objetos dinámicos aplicables a todo tipo de regla, definiendo las propiedades de los mismos sobre cada firewall en particular. Los objetos deben poder referenciar servidores y redes como mínimo. Por ejemplo, permitir</p> <p>Las reglas deben permanecer en medio físico, no volátil.</p> <p>Los administradores que accedan a los firewalls deberán autenticarse mediante Radius, LDAP o SECURID</p> <p>Las redes de los administradores serán controladas y se configurara el equipo para que solo equipos pertenecientes a dichas redes puedan acceder para configurarlo . Cantidad mínima de redes de administradores : 6</p> <p>El equipo permitirá la vuelta atrás (roll-back) a la ultima configuración estable aplicada, luego de realizada una modificación en la misma.</p> <p>El mecanismo de control de filtrado utilizado por el engine del equipo deberá estar basado en técnicas "statefull inspection" que crean conexiones virtuales, incluso para los protocolos connection-less como UDP y RPC.</p> <p>La solución deberá soportar la funcionalidad de Proxy de protocolo ARP sobre todas sus interfaces. Entendiéndose dicha funcionalidad como la capacidad de responder a pedidos de ARP que no son dirigidos directamente hacia direcciones IP declaradas en sus p</p> <p>Deberá poseer capacidad de manejo de apertura de puertos dinámicos en base a protocolos de uso común (FTP, H323, SIP, SCCP, MGCP) y posibilidad de crear sesiones personalizadas que manejen dicho comportamiento.</p> <p>La solución deberá soportar la configuración de parámetros referidos a timeout en la tabla de estados de conexiones sobre cualquier servicio TCP en forma individual y global.</p> <p>La solución deberá soportar la activación y desactivación de técnicas de detección y evasión de ataques de DOS (Denegación de servicio).</p> <p>La solución deberá soportar la activación y desactivación de técnicas de protección de ataques de generación masiva de conexiones (SYN attack) permitiendo su configuración para una dirección IP en particular.</p> <p>La solución deberá soportar la activación y desactivación de técnicas de anti-spoofing sobre cada zona de seguridad.</p> <p>La solución deberá soportar técnicas de mitigación de spoofing en todas las interfaces.</p> <p>Las reglas deberán poder definirse, diferenciando protocolo, IP destino / IP origen, puerto destino / puerto origen, zona de seguridad y horario.</p>	
Cantidad de interfases 10/100/1000	2	
Cantidad de Slots ampliables disponibles mínimos	Mínimo 2	

Item 2. EQUIPOS INFORMATICOS DE SEGURIDAD		
2.2 FIREWALL		
CANTIDAD:	1 (UNO)	
Características	REQUERIMIENTO MINIMO	Ofrecido
MTBF	6 Años	
Garantía Total Extendida sobre hardware del fabricante, incluye renovación de versión de sistema operativo	2 Años	
Período de reemplazo ante falla 2 años	El equipo deberá ser reparado o reemplazado por otro que cumpla con estas especificaciones técnicas al siguiente día hábil a la notificación de la falla.	
Vigencia de protección y actualización de firmas sobre recursos de filtrado de contenido Antivirus, IPS y Web Filter	2 Años	
Varios	CD con manuales, cable de consola y alimentación	
	El equipo ofertado debe tener certificación ISO 9001	
	Presentar documentación del fabricante donde autorice a la empresa oferente como representante para la región y avale la garantía exigida.	
	Presentar respaldado por escrito del fabricante a la empresa oferente autorizándola a prestar el servicio técnico y el cambio de partes por garantía, el cual deberá contar con stock de repuestos.	
	Los técnicos de la empresa oferente deberán estar certificados por el fabricante. Se exigirá la presentación de los certificados de los técnicos pertenecientes a la empresa autorizada por el fabricante. La documentación emitida por el fabricante; no deber	
	En caso de que el equipo deba ser retirado por reparación dentro de la Garantía, el plazo máximo para la reposición en funcionamiento del mismo es de 15 días calendario. Durante este periodo el oferente deberá proporcionar un equipo en reemplazo temporal,	
	En la oferta debe incluirse el servicio de instalación y configuración, una vez instalado el equipo las configuraciones deben cubrir las necesidades detalladas por la Dirección de Informática.	
	El oferente será responsable por la puesta en marcha de plataforma teniendo que incluir los costo para los siguientes trabajos: .Creación de DMZ para alojar servidores y segmentación de LAN interna.	
	Creación de 5 perfiles de acceso a servicios.	
	- Configuración de 3 Vlans segmentando Servicios en el nuevo Swtich Principal.	
	. Capacitación sobre plataforma provista al personal IT (4 horas como mín.)	
Garantía.	2 años con actualización y soporte incluido.	
Tipo de Garantía	Tipo de Garantía y Servicio: en sitio bajo la modalidad 24x7, incluye reemplazo de hardware temporal mientras se gestiona el RMA del equipo con el fabricante.	