CONCURSO DE PRECIOS Nº

DECRETO N° /21

PLIEGO DE CONDICIONES PARTICULARES Y ESPECIFICACIONES TÉCNICAS

ARTÍCULO 1º: OBJETO

El presente Concurso tiene por objeto la adquisición de equipos para la actualización, implementación y mantenimiento de la infraestructura de la red informática municipal, con las características y cantidades que se detallan a continuación:

OBJETO 1: Sistema de Firewall (hardware+software)

Se deberá cotizar la provisión de un equipo junto con su licencia correspondiente (de al menos un año) que permita la defensa y manejo unificado de amenazas desde una consola de administración que brinde acceso a todas las configuraciones, manejo y monitoreo de las funciones disponibles. La propuesta deberá contemplar un equipo de seguridad perimetral ("Firewall") de tipo NGFW + su licencia por al menos un año.

El sistema de seguridad perimetral ("Firewall") de tipo NGFW deberá contar con las siguientes funcionalidades detalladas a continuación:

Generales

- Aceleración por Hardware para las funciones de ruteo, firewall y tunelización de tráfico WiFi.
- HA activo-pasivo y activo-activo (se requiere un cluster de al menos 2 equipos)
- IPv6 en forma nativa (manteniendo la mismas características y rendimiento que IPv4)
- Soporte a ruteo estático y dinámico (RIP, OSPF v2 y v3, ISIS y BGP)
- Soporte a ruteo por política.
- Soporte a protocolos de monitoreo como SNMP y sFlow
- Soporte a Syslog, con capacidad de envío mediante TCP y SSL.
- Debe permitir la creación de hasta 10 sistemas virtuales en el mismo equipo.
- Soporte a VXLAN
- Debe soportar Traffic Shaping con la posibilidad de aplicarlo, por usuario, IP, interface o aplicación detectada.

- La solución debe identificar potenciales vulnerabilidades y destacar las mejores prácticas que podrían ser usadas para mejorar la seguridad general y el rendimiento de la solución.

Firewall:

- Debe soportar la creación de zonas.
- Aplicación de políticas por zona o interfaces, por usuarios, direcciones IP o tipos de dispositivo.
- NAT
- VPN IPSec de sitio a sitio y para acceso remoto (sin límite de licencias)
- VPN SSL para acceso remoto
- Protecciones contra DoS (denegación de servicio)
- Inspección de trafico SSL (con la capacidad de descifrar el trafico cifrado) entrante y saliente.
- Posibilidad de armar políticas en base a objetos Geográficos
- Base de datos de Servicios de Internet (actualizada dinámicamente) para el uso en políticas de seguridad.
- Capacidad de funcionar como proxy web explícito y como proxy transparente.
- Debe permitir la autenticación transparente (SSO) con sistemas de Active Directory.

SDWAN:

- Balanceo de vínculos a Internet, VPNs y enlaces WAN (ej: MPLS)
- Balanceo Round Robin, Balanceo por peso, cantidad de sesiones, ancho de banda y derrame.
- Definición de políticas de SDWAN por Aplicación, Servicio de internet, usuarios, IPs o Interfaces/zonas.
- Soporte a más de 5 vínculos a Internet.
- La función debe tener un mecanismo por el cual se puedan enviar datos adicionales de manera tal que ante la pérdida de paquetes en alguno de los vínculos permita la reconstrucción del stream en sitio receptor.

Control de Aplicaciones:

- Control de Aplicaciones en capa 7, para la detección de trafico sin importar el puerto que utilicen.

- Reconocer al menos 3000 aplicaciones diferentes
- Debe inspeccionar el contenido del paquete de datos con el fin de detectar las firmas de las aplicaciones conocidas independiente de puerto y protocolo que usen;
- Debe permitir la creación de firmas de aplicación manuales.
- 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.
- Debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo.
- Debe permitir la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo.
- Limitar el ancho de banda (carga / descarga) utilizado por las aplicaciones (traffic shaping), basado en IP de origen, usuarios y grupos.

Prevención de Amenazas:

- Debe incluir firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (antivirus, anti-spyware y sandboxing);
- La aplicación de controles de IPS y Antimalware deben ser aplicadas a través de las reglas de seguridad.
- Debe contar con motores heurísticos, sandboxing en la nube, detección de anomalías de protocolo y antibotnet.
- Debe contar con firmas específicas para la mitigación de ataques DoS y DDoS;
- Debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación;
- Debe tener 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;
- Debe incluir el servicio de Sandbox en la nube, con la capacidad de enviar hasta 10 muestras por segundo.
- Debe poder crear firmas personalizadas en la interfaz gráfica del producto.
- Debe permitir 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.

Filtrado de URL

- Tener por lo menos 60 categorías de URL, actualizadas dinámicamente por el fabricante de la solución.
- Permitir página de bloqueo personalizadas;
- Los filtros URL deben poder aplicarse por política de seguridad.
- Debe permitir la definición de listas negras y blancas de URL.
- Permitir 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 Web Proxy explícito, debe soportar proxy web transparente;
- Debe tener 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.

Identificación de Usuarios

- Las políticas de seguridad deben permitir la integración con servicios de Active Directory, LDAP, y base de datos local.
- Debe permitir crear reglas por grupos de usuario o usuarios individuales.
- Debe tener integración con RADIUS.
- Debe incluir portal captivo para autenticación explicita de los usuarios.
- Debe soportar métodos de autenticación como NTLM y Kerberos.
- Debe ser integrable con entornos de Citrix XenApp/XenDesktop y Terminal Services.

DLP

- Permite la creación de filtros para archivos (por tipo y tamaño) y datos predefinidos.
- Permitir identificar y opcionalmente prevenir la transferencia de varios tipos de archivo (MS Office, PDF, etc.) identificados en las aplicaciones (HTTP, FTP, SMTP, etc.);
- Soportar la identificación de archivos comprimidos y cifrados.
- Permitir identificar y opcionalmente prevenir la transferencia de información sensible

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;
- Soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen y destino, usuario y grupo.
- Soportar la creación de políticas de QoS y Traffic Shaping para aplicaciones incluyendo, pero no limitado a Skype, BitTorrent, Azureus y YouTube;
- Soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto;
- En QoS debe permitir la definición de tráfico con ancho de banda garantizado;
- En QoS debe permitir la definición de tráfico con máximo ancho de banda;
- En QoS debe permitir la definición de colas de prioridad;
- Soportar la priorización de protocolo en tiempo real de voz (VoIP) como H.323, SIP, SCCP, MGCP y aplicaciones como Skype;
- Soportar marcación de paquetes DiffServ, incluso por aplicación;
- Soportar la modificación de los valores de DSCP para Diffserv;
- Soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service);
- Proporcionar estadísticas en tiempo real para clases de QoS y Traffic Shaping;
- Debe soportar QoS (traffic-shapping) en las interfaces agregadas o redundantes;

Geolocalización

- Soportar la creación de políticas por geo-localización, permitiendo bloquear el tráfico de cierto País/Países;
- Debe permitir la visualización de los países de origen y destino en los registros de acceso;
- Debe permitir la creación de zonas geográficas por medio de la interfaz gráfica de usuario y la creación de políticas usando las mismas

VPN

- Soporte VPN de sitio-a-sitio y cliente-a-sitio;

- Soportar VPN IPSec, VPN SSL
- La VPN IPSec debe ser compatible con 3DES y AES de 128, 192 y 256 (Advanced Encryption Standard)
- La VPN IPSec debe ser compatible con la autenticación MD5 y SHA-1;
- La VPN IPSec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14;
- La VPN IPSec debe ser compatible con Internet Key Exchange (IKEv1 y v2);
- La VPN SSL debe soportar 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;
- Soportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local.

Wireless Controller

- Deberá gestionar de manera centralizada los puntos de acceso del mismo fabricante de la solución ofertada.
- Debe generar túneles cifrados hacia los AP para la gestión de los mismos.
- Soporte al cifrado de túneles entre la controladora y el punto de acceso inalámbrico para el tráfico de las redes WiFi
- Debe permitir elegir si el tráfico de cada SSID se enviará hacia la controladora por un túnel o directamente por la interfaz de punto de acceso en una determinada VLAN.
- Proporcionar autenticación a la red inalámbrica a través de bases de datos externas, tales como LDAP o RADIUS (via 802.1x), con la posibilidad de usar un portal captivo interno.
- Permitir autenticar a los usuarios de la red inalámbrica de manera transparente en dominios Windows
- Permitir la visualización de los dispositivos inalámbricos conectados por usuario; IP, tipo de autenticación, canal, ancho de banda utilizado, potencia de la señal, tiempo de asociación.
- Para la autenticación de los usuarios y dispositivos deberá soportar WPA y WPA2 con 802.1x o Preshared key, WEP y un portal cautivo Web, así como con listas negras y blancas basadas en MAC
- La controladora inalámbrica deberá permitir configurar los parámetros de radio como banda y canal.
- La configuración de los puntos de acceso debe ser Zero Touch.
- Debe contar con un módulo de WIDS.

- Soportar monitoreo y supresión de puntos de acceso indebidos y de intrusos on wire.
- La controladora inalámbrica debe permitir agendar horarios en que momento la red inalámbrica (SSID) se encuentra disponible.
- Ofrecer 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.
- Debe tener un mecanismo de ajuste automático de potencia de la señal y de balanceo de usuarios entre puntos de acceso.
- Permitir ignorar a los clientes inalámbricos que tienen señal débil, estableciendo un umbral de señal a partir de la cual los clientes son ignorados.
- Debe permitir asociación dinámica de VLANs a los usuarios autenticados en un SSID especifico mediante protocolo RADIUS o VLAN pooling
- El controlador inalámbrico debe soportar la funcionalidad de Fast-roaming.
- La controladora inalámbrica debe soportar protocolo LLDP.
- Debe permitir la visualización de los usuarios conectados en forma de topología lógica de red representando la cantidad de datos transmitidos y recibidos;
- La controladora inalámbrica debe permitir combinar redes WiFi y redes cableadas con un software switch integrado.
- Debe proporcionar la capacidad de crear varias claves pre-compartidas de acceso protegido WiFi (WPA-PSK) para un mismo SSID para que no sea necesario compartir PSK entre dispositivos.
- Gestión de firmware desde el controlador centralizado.

Licenciamiento y actualizaciones

El licenciamiento de todas las funcionalidades debe ser ILIMITADO en cuanto a usuarios, conexiones, equipos que pasan a través de la solución, limitándola solamente por el desempeño del equipo.

Funcionalidades:

- Antispam
- Antivirus
- Sandbox Cloud
- Application control NGFW e IPS
- Web filtering
- Content disarm & reconstruction
- Virus outbreak protection

- Security Rating Service
- Industrial Service
- CASB SaaS-Only service

La vigencia del soporte para actualizaciones de software, soporte del fabricante y soporte de hardware debe proveerse por al menos 1 año

Desempeño / Conectividad

El equipo debe por lo menos ofrecer las siguientes características de desempeño y conectividad

Número de Interfaces Requeridas	10x GE RJ45 ports (including 7x Internal ports, 2x WAN ports, 1x DMZ port).
Throughput de Firewall (con paquetes de 1518/512/64 Bytes)	10/10/6 Gbps
Latencia de firewall (con paquetes de 64 byte)	4 µs
Throughput de VPN IPSec (con paquetes de 512 byte)	6.5 Gbps
Throughput de NGFW	1 Gbps
Throughput de Inspección SSL	750 Mbps
Politicas de Firewall admitidas	5000
Túneles IPsec gateway to gateway	200
Túneles IPsec client to gateway	500
Throughput VPN SSL	900 Mbps
Sesiones Concurrentes	700000
Nuevas sesiones / segundo	35000
Sistemas Virtuales incluidos / Máximo soportado	10/10

OBJETO 2: Memorias RAM para servidor DELL

Se requiere la provisión de **memorias RAM para llevar la capacidad actual del servidor** de 8GB a **32GB**.

El servidor es un **Power Edge r520 DELL (**con **código de** ServiceTag: **HJY33W1).**

Verificar las características técnicas de las mismas con el número se Service Tag: **HJY33W1.** Las memorias deben ser compatibles con la que se encuentra instalada hoy en día de 8GB (corroborar con código de service tag).

Las mismas deben contar con garantía de al menos 1 año y los oferentes deben garantizar la compatibilidad con el modelo del servidor y de la memoria ya instalada.

Como se mencionó anteriormente, el servidor cuenta actualmente con 8GB de RAM y se solicita proveer las memorias necesarias para llevarlo a 32GB.

OBJETO 3: Discos Rígidos para servidor DELL

Se requiere la provisión de **3 DISCOS RIGIDOS de 1TB SAS Hot Plug** compatible con servidor **DELL Power Edge r520** con número de ServiceTag: **HJY33W1.**

Por cuestiones de compatibilidad, los discos deben ser de la misma marca que el servidor.

Las mismas deben contar con garantía de al menos 1 año y los oferentes deben garantizar la compatibilidad con el modelo del servidor. Chequear a través del código de service tag que los modelos de los discos sean iguales a los que tiene hoy en día el servidor. La finalidad es llevar la matriz de discos de RAID 1 a RAID 5, por lo que los discos deben ser compatibles entre si.

PRESENTAR, EN MESA DE ENTRADAS, EN SOBRE CERRADO, CONSIGNANDOSE EN LA CUBIERTA DEL MISMO NÚMERO DE CONCURSO DE PRECIOS, DIA Y HORA DE APERTURA, LA PROPUESTA ECÓNOMICA ESCRITA JUNTO CON EL PLIEGO DE CONDICIONES PARTICULARES FIRMADO EN TODAS SUS HOJAS, Y TAMBIÉN DEBERÁ ENVIAR LA PROPUESTA ECONÓMICA JUNTO CON EL PLIEGO DE CONDICIONES PARTICULARES FIRMADO EN TODAS SUS HOJAS (ORIENTACIÓN DE LA HOJA VERTICAL) A LA DIRECCIÓN DE CORREO ELECTRÓNICO hacienda.lapazer@gmail.com

LAS PROPUESTAS DEBERÁN SER PRESENTADAS EN MESA DE ENTRADA HASTA UNA HORA ANTES DE LA FECHA FIJADA PARA LA APERTURA, EN TANTO QUE LAS PROPUESTAS PODRÁN SER ENVIADAS A LA DIRECCION DE CORREO ELECTRÓNICO ESTABLECIDA, HASTA LA HORA FIJADA PARA LA APERTURA DEL CONCURSO.

ARTÍCULO 2º: PRESUPUESTO OFICIAL

El Presupuesto Oficial se fija en la suma de PESOS QUINIENTOS SESENTA MIL.----------

ARTÍCULO 3º: LUGAR Y FECHA DE APERTURA

El lugar y fecha de apertura del presente Concurso, queda determinado en la Municipalidad de La Paz, Sección Suministros – sito en calle Echagüe y Moreno – el día 22 de Abril de 2021 a las 10:00 horas.

ARTÍCULO 4º: FORMA DE COTIZACIÓN

Los proponentes deberán cotizar en pesos, consignando el precio unitario y el total de la oferta, la que deberá incluir el Impuesto al Valor Agregado.

ARTÍCULO 5º: MANTENIMIENTO DE LA OFERTA

Los proponentes se comprometen a mantener las ofertas por el término de VEINTE (10) días hábiles – como mínimo – posteriores al acto de apertura, todo plazo menor fijado por los oferentes se entenderá por no escrito.

ARTÍCULO 6º: ADJUDICACIÓN

La Municipalidad de La Paz adjudicará por renglón o por el total, según convenga como consecuencia de la comparación de las ofertas presentadas al acto respectivo, conforme los criterios establecidos en la Ordenanza Nº 633/02 que regula el sistema de Compras y Contrataciones en el ámbito municipal.

ARTÍCULO 7º: PLAZO DE ENTREGA

La mercadería objeto del presente Concurso de precios deberá ser entregada dentro de los CINCO (5) días hábiles contados a partir de la fecha de notificación de la adjudicación, puesta en la Ciudad de La Paz, en el lugar que la Municipalidad determine, libre de gastos de flete y de descarga.

ARTÍCULO 8º: FORMA DE PAGO

La Municipalidad de La Paz abonará el importe correspondiente al presente concurso, dentro de los CINCO (5) días hábiles posteriores a la fecha de presentación de la factura, en la que deberá consignar la recepción total de los materiales adjudicados.

ARTÍCULO 9º: RECONOCIMIENTO DE VARIACIONES DE COSTOS

Para la provisión a que se refiere el presente concurso, no se reconocerán variaciones de costos de ninguna naturaleza y por ningún concepto.

ARTÍCULO 10º: DOCUMENTACIÓN OBLIGATORIA A PRESENTAR

Se deberá presentar nota constituyendo dirección de correo electrónico, en la que se tendrán por válidas todas las notificaciones que se realicen en el proceso.