JUNTA MUNICIPAL DE ASUNCION
DIRECCION OPERATIVA DE CONTRATACIONES

ADENDA Nº 1

LICITACIÓN POR CONCURSO DE OFERTA PAC Nº 263.217/13 *"PROVISIÓN E INSTALACIÓN DE CABLEADO ESTRUCTURAL - AD REFEREMDUM- PLURIANUAL"*

Estimados:
Por la presente, la Dirección Operativa de Contrataciones de la Junta Municipal de Asunción cumple en informarles las modificaciones sufridas en el Pliego de Bases y Condiciones de la Licitación Por Concurso de Oferta N° 06/13, PAC N° **263.217/13** "***PROVISIÓN E INSTALACIÓN DE CABLEADO ESTRUCTURAL - AD REFEREMDUM- PLURIANUAL***, se procede a la Addenda del citado llamado:

Se deja sin efecto los siguientes puntos:

EQUIPO DE BORDE
EQUIPO DE BORDE

ITEM	CARACTERISTICAS		MINIMO EXIGIDO	PROPUESTA DEL OFERENTE	
				CUMPLE SI/NO	EXPLICAR COMO CUMPLE
	Especificar	Marca y Modelo			
	CANTIDAD	1 Unidad			
1.	RENDIMIENTO Y CAPACIDAD	Performance Firewall Troughput en paquetes de 64 bytes	3 Gbps		
		VPN IPSEC Troughput en paquetes de 64 bytes	1 Gbps		
		Sesiones Concurrentes soportadas	2.000.000		
		Nuevas sesiones por segundo	4.000		
		Cantidad de Políticas de Seguridad	4.000		
		Cantidad de Tuneles VPN Soportados	180		
		Cantidad de Usuarios Concurrentes.	Ilimitado		
2.	CONECTIVIDAD DE RED	Cantidad de puertos 10/100/1000Base-T – Configurables como WAN, LAN o DMZ	12		
		Puertos USB 2.0	1		
3.	ROUTING	BGP	EXIGIDO		
		OSPF	EXIGIDO		
		RIP v1/v2	EXIGIDO		
		Soporte a ruteo de multicast	EXIGIDO		
		Soporte a ruteo estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas	EXIGIDO		
		Soporte a políticas de ruteo (policy routing)	EXIGIDO		
		Soporte a ruteo dinámico RIPng, OSPFv3	EXIGIDO		
		Soporte de ECMP (Equal Cost Multi-Path)	EXIGIDO		
4.	AUTENTICACION DE USUARIOS Y CONTROL DE ACCESO	Capacidad de integrarse con Servidores de Autenticación RADIUS	EXIGIDO		
		Capacidad nativa de integrarse con directorios LDAP	EXIGIDO		
		Soporte a inclusión en autoridades certificadoras (enrollment) mediante SCEP	EXIGIDO		

JUNTA MUNICIPAL
LIC. ISIDRA MACHADO TROCHE
DIRECTORA - DUOC
JUNTA MUNICIPAL DE ASUNCION

		(Simple Certificate Enrollment Protocol) y mediante archivos.			
5.	TRADUCCION DE DIRECCIONES	NAT	EXIGIDO		
		PAT	EXIGIDO		
		NAT estatico	EXIGIDO		
		NAT con PAT	EXIGIDO		
6.	ASIGNACION DE DIRECCIONES IP	Cliente DHCP	EXIGIDO		
		Servidor DHCP	EXIGIDO		
		DHCP Relay	EXIGIDO		
7.	CONMUTACION EN LAYER 2	Soporte de VLAN 802.1Q	256		
		Soporte de Link Aggregation Group (802.3ad) con un mínimo de 4 interfaces por grupo	EXIGIDO		
		Soporte a etiquetas de VLAN (802.1q) y creación de zonas de seguridad en base a VLANs	EXIGIDO		
8.	ADMINISTRACION DE TRAFICO Y CALIDAD DE SERVICIO (QoS)	Capacidad de poder asignar parámetros de traffic shapping sobre reglas de firewall	EXIGIDO		
		Capacidad de poder definir ancho de banda garantizado en KiloBytes por segundo	EXIGIDO		
		Capacidad de poder definir límite de ancho de banda (ancho de banda máximo) en KiloBytes por segundo	EXIGIDO		
		Capacidad para definir prioridad de tráfico, en al menos tres niveles de importancia	EXIGIDO		
		Capacidad de poder asignar parámetros de traffic shaping diferenciadas para el tráfico en distintos sentidos de una misma sesión	EXIGIDO		
		Capacidad de definir parámetros de traffic shaping que apliquen para cada dirección IP en forma independiente, en contraste con la aplicación de las mismas para la regla en general.	EXIGIDO		
9.	ALTA DISPONIBILIDAD	Soporte de Alta Disponibilidad en modo transparente, es decir, sin pérdida de conexiones en caso de que un nodo falle.	EXIGIDO		
		Soporte de Alta Disponibilidad en modo Activo-Activo	EXIGIDO		
		Soporte de Alta Disponibilidad en modo Activo-Pasivo	EXIGIDO		
		Posibilidad de definir al menos dos interfaces para sincronia para Alta Disponibilidad de forma a evitar el uso de Multicast en la red	EXIGIDO		
10.	CONTROL DE APLICACIONES	El equipo deberá poseer prestaciones de Control de Aplicaciones.	EXIGIDO		
		Lo solución debe soportar la capacidad de identificar la aplicación que origina cierto tráfico a partir de la inspección del mismo	EXIGIDO		
		La identificación de la aplicación debe ser independiente del puerto y protocolo hacia el cual esté direccionado dicho tráfico	EXIGIDO		
		Las solución debe tener un listado de al menos 1000 aplicaciones ya definidas por el fabricante	EXIGIDO		
		El listado de aplicaciones debe actualizarse periódicamente	EXIGIDO		
		Para aplicaciones identificadas deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log	EXIGIDO		

LIC. ISIDRA MACHADO TROCHE
DIRECTORA - DUOC
JUNTA MUNICIPAL DE ASUNCION

		Para aplicaciones no identificadas (desconocidas) deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log	EXIGIDO		
		Para aplicaciones de tipo P2P debe poder definirse adicionalmente políticas de traffic shaping	EXIGIDO		
		Preferentemente deben soportar mayor granularidad en las acciones	EXIGIDO		
11.	INSPECCION DE CONTENIDO – IDS/IPS	El equipo deberá poseer prestaciones de IDS/IPS	EXIGIDO		
		Performance Inspeccion IPS	250 Mbps		
		El Detector y preventor de intrusos deberá de estar orientado para la protección de redes	EXIGIDO		
		El Detector y preventor de intrusos deben poder implementarse tanto en línea como fuera de línea. En línea, el tráfico a ser inspeccionado pasará a través del equipo. Fuera de línea, el equipo recibirá el tráfico a inspeccionar desde un switch con un puerto configurado en span o mirror.	EXIGIDO		
		El detector y preventor de intrusos podrá implementarse en línea y fuera de línea en forma simultánea para distintos segmentos.			
		El detector y preventor de intrusos deberá estar integrado a la plataforma de seguridad sin necesidad de instalar un servidor o equipo externo, licenciamiento de un producto externo o software adicional para realizar la prevención de intrusos.	EXIGIDO		
		Deberá soportar captar ataques por Anomalía (Anomaly detection).	EXIGIDO		
		Deberá soportar captar ataques basado en análisis de firmas en el flujo de datos en la red (signature based / misuse detection).	EXIGIDO		
		Deberá permitir configurar firmas nuevas para cualquier protocolo.	EXIGIDO		
		Deberá poseer una tecnología de detección tipo Stateful basada en Firmas (signatures).	EXIGIDO		
		Deberá soportar la actualización automática de firmas para el detector de intrusos (por 3 años)	EXIGIDO		
		El Detector de Intrusos deberá mitigar los efectos de los ataques de negación de servicios	EXIGIDO		
		Deberá contar con mecanismos de deteccion de ataques basados en Reconocimiento de patrones y Análisis de protocolos.	EXIGIDO		
		Deberá contar con mecanismos de deteccion de ataques basados en Detección de anomalías.			
		Deberá contar con mecanismos de deteccion de ataques basados en Detección de ataques de RPC (Remote procedure call)	EXIGIDO		
		Deberá contar con mecanismos de Protección contra ataques de Windows o NetBios	EXIGIDO		
		Deberá contar con mecanismos de Protección contra ataques de SMTP, IMAP o POP.	EXIGIDO		
		Deberá contar con mecanismos de Protección contra ataques DNS.	EXIGIDO		
		Deberá contar con mecanismos de Protección contra ataques a FTP, SSH y Telnet.	EXIGIDO		

LIC. ISABEL MACHADO TROCHE
DIRECTORA - DUOC
JUNTA MUNICIPAL DE ASUNCION

		Deberá contar con mecanismos de Protección contra ataques de ICMP.	EXIGIDO		
		Deberá contar con Alarmas mostradas en la consola de administración del equipo.	EXIGIDO		
		Deberá contar con la capacidad de cuarentena. La misma debe ofrecer la posibilidad de definir el tiempo en que se bloqueará el tráfico. También podrá definirse el bloqueo de forma "indefinida", hasta que un administrador tome una acción al respecto	EXIGIDO		
12.	INSPECCION DE CONTENIDO – FILTRADO DE URL	El equipo poseer prestaciones de Filtrado de Páginas Web (URL Filtering).	EXIGIDO		
		El equipo deberá poseer la capacidad de trabajar como un Proxy Cache	EXIGIDO		
		Capacidad mínima de almacenamiento interno.	30 GB		
		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 75 categorías y por lo menos 39 millones de sitios web en la base de datos.	EXIGIDO		
		Filtrado de contenido basado en categorías en tiempo real, integrado a la plataforma de seguridad sin necesidad de instalar un servidor o equipo externo, licenciamiento de un producto externo o software adicional para realizar la categorización del contenido.	EXIGIDO		
		Configurable directamente desde la interfaz de administración del dispositivo. Con capacidad para permitir esta protección por política de control de acceso.	EXIGIDO		
		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	EXIGIDO		
		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.	EXIGIDO		
		Capacidad de filtrado de scripts en páginas web (JAVA/Active X).	EXIGIDO		
13.	INSPECCION DE CONTENIDO – ANTISPAM	El equipo poseer prestaciones de Antispam.	EXIGIDO		
		La capacidad antispam incluída deberá ser capaz de detectar palabras dentro del cuerpo del mensaje de correo, y en base a la presencia/ausencia de combinaciones de palabras, decidir rechazar el mensaje.	EXIGIDO		
		La capacidad AntiSpam incluída deberá permitir especificar listas blancas (confiables, a los cuales siempre se les deberá pasar) y listas negras (no confiables, a los cuales siempre les deberá bloquear). Las listas blancas y listas negras podrán ser por dirección IP o por dirección de correo electrónico (e-mail address)	EXIGIDO		
		La capacidad AntiSpam deberá poder consultar una base de datos donde se revise por lo menos dirección IP del emisor del mensaje, URLs contenidos dentro del mensaje y checksum del mensaje, como mecanismos para detección de SPAM	EXIGIDO		
		En el caso de análisis de SMTP, los mensajes encontrados como SPAM podrán ser etiquetados o rechazados (descartados). En el caso de etiquetamiento del mensaje, debe tenerse la flexibilidad para etiquetarse	EXIGIDO		

LIC. ISIDRA MACHADO TROCHE
DIRECTORA - DUOC
JUNTA MUNICIPAL ASUNCION

		en el motivo (subject) del mensaje o a través un encabezado MIME en el mensaje.			
14.	ADMINISTRACION	Soporte de Interfaz CLI	EXIGIDO		
		Soporte de Interfaz WEB (HTTP y HTTPS)	EXIGIDO		
		Puerto serial dedicado para administración.	EXIGIDO		
		Comunicación cifrada y autenticada con username y password, tanto como para la interfase gráfica de usuario como la consola de administración de línea de comandos (SSH o telnet)	EXIGIDO		
		Los administradores podrán tener asignado un perfil de administración que permita delimitar las funciones del equipo que pueden gerenciar y afectar.	EXIGIDO		
		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.	EXIGIDO		
		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, Mozilla, Firefox) instalado sin necesidad de instalación de ningun software adicional.	EXIGIDO		
		Soporte de SNMP versión 2	EXIGIDO		
		Soporte de servidores syslog para poder enviar bitácoras a servidores de SYSLOG remotos	EXIGIDO		
15.	ALIMENTACION ELECTRICA Y DIMENSIONES	Tensión de operación	Alterna, 220VCA		
		Montaje en rack de 19"	EXIGIDO		

ITEM 2.2 – SWITCH TIPO 1 :

ITEM	CARACTERISTICAS		MINIMO EXIGIDO	PROPUESTA DEL OFERENTE	
				CUMPLE SI/NO	EXPLICAR COMO CUMPLE
	Especificar	Marca y Modelo			
	Cantidad:	2 Unidades			
	RENDIMIENTO Y CAPACIDAD	Capacidad mínima de forwarding en Capa 2 en paquetes de 64 bytes	95 Mpps		
		Capacidad mínima de conmutación de paquetes	128 Gbps		
		Memoria Flash	512 MB		
		Memoria DRAM	512 MB		
		MTBF Mínimo Requerido	100.000 Hs.		
	CONECTIVIDAD DE RED	Cantidad mínima de interfaces 10/100/1000 Base-T RJ-45, con soporte y detección automática de la velocidad y duplex (IEEE 802.3, 802.3u y 802.3ab)	24		
		Cantidad de slots SFP/SFP+ soportados	4		

LIC. ISIDRA MACHADO TROCHE
DIRECTORA - DUOC
JUNTA MUNICIPAL DE ASUNCION
U.O.C. Nº 2

		Capacidad de conectar Transceptores SFP 10/100/1000Base-T	EXIGIDO		
		Capacidad de conectar Transceptores SFP 1000 Base-X Multimodo	EXIGIDO		
		Capacidad de conectar Transceptores SFP 1000 Base-X Monomodo	EXIGIDO		
		Capacidad de conectar Transceptores SFP+ 10 GbE	EXIGIDO		
		Cantidad mínima de puertos 10/100/1000 BaseT Ethernet adicional e independiente para administración del equipo.	1		
		Los puertos SFP/SFP+ no deben ser del tipo COMBO, es decir, deben ser 100% independientes y no deben anular de ninguna manera los puertos eléctricos 10/100/1000 BASE-T RJ45.	EXIGIDO		
3.	CONMUTACION EN LAYER 2	Mínimo VLANS soportadas	4.096		
		Mínimo de direcciones MAC	16.000		
		Soporte de 802.1D Spanning Tree Protocol	SI		
		Soporte de 802.1w Rapid Spanning Tree	EXIGIDO		
		Soporte de 802.1s Multiple Instance Spanning Tree	EXIGIDO		
		Jumbo Frames (9000 Byte)	EXIGIDO		
		Deberá contar con la capacidad de agregar, mediante licencias, la funcionalidad de Q-in-Q	EXIGIDO		
4.	STACKING	Los equipos deberán soportar STACKING	EXIGIDO		
		Vinculación de equipos por puertos de uso exclusivo para Stack excluyendo las interfaces de RED	EXIGIDO		
		Configuración desde una única dirección IP y para su administración actuarán como un único equipo.	EXIGIDO		
		Capacidad mínima de backplane del Stack utilizando los puertos específicas de stacking expresado en bandwidth full-duplex	64Gbps		
		Redundancia de Supervisora de Enrutamiento y Administración	EXIGIDO		
		El reemplazo de un miembro del stack deberá ser no disruptivo. En caso que la versión de Sistema Operativo del equipo a incorporar sea distinta de la vigente el stack, la misma deberá actualizarse automáticamente.	EXIGIDO		
		Capacidad de conectarse entre si por Uplink de 1Gbps conformando un único equipo desde el punto de vista de la administración	EXIGIDO		
		Capacidad de conectarse entre si por Uplink de 10Gbps conformando un único equipo desde el punto de vista de la administración	EXIGIDO		
		Mínimo de equipos agrupados para administrar con un único acceso administrativo	10		
		En el caso de Stack los puertos de LAG deben poder pertenecer a diferentes miembros del Stack	EXIGIDO		
5.	ROUTING	Mínimo de rutas IPv4 unicast	8000		
		RIP (v1 y v2)	EXIGIDO		

JUNTA MUNICIPAL
LIC. ISIDRA MACHADO TROCHE
DIRECTORA - DUOC

		Ruteo estático.	EXIGIDO		
		Deberá contar con la capacidad de agregar, mediante licencias, los siguientes protocolos de ruteo dinámico: OSPF y BGP	EXIGIDO		
6.	MULTICAST	Deberá contar con la capacidad de agregar, mediante licencias, los siguientes protocolos de Multicast: IGMP (v1, v2 y v3) y PIM	EXIGIDO		
7.	AUTENTICACION DE USUARIOS Y CONTROL DE ACCESO	ACL que permitan la clasificación de direcciones origen/destino L2	EXIGIDO		
		ACL que permitan la clasificación de direcciones origen/destino L3	EXIGIDO		
		ACL que permitan ser aplicadas en el puerto al ingreso o egreso de los paquetes.	EXIGIDO		
		ACL que permitan ser aplicadas en la VLAN al ingreso y egreso de los paquetes.	EXIGIDO		
		ACL basadas en el encabezado de TCP/IP aplicadas al ingreso y egreso de los paquetes.	EXIGIDO		
		Funcionalidad de 802.1x en cada por puerto.	EXIGIDO		
		Integración con sistemas de control de acceso por medio del protocolo RADIUS y 802.1x para autenticación de usuario.	EXIGIDO		
		Autenticación del usuario debe realizarse antes que los dispositivos conectados reciban una dirección IP de un Servidor DHCP.	EXIGIDO		
		El estándar 802.1X está basado en EAP (Extensible Authentication Protocol).	EXIGIDO		
		Deberá soportar EAP-MD5	EXIGIDO		
		Deberá soportar EAP-TLS	EXIGIDO		
		Deberá soportar EAP-TTLS	EXIGIDO		
		Deberá soportar EAP-PEAP	EXIGIDO		
		Bloquear todo el tráfico generado por cualquier dispositivo conectado a la red y no autenticado.	EXIGIDO		
		Una vez que los dispositivos son autenticados podrán recibir parámetros, via atributo de RADIUS, de la VLANs correspondiente.	EXIGIDO		
		Una vez que los dispositivos son autenticados podrán recibir parámetros, via atributo de RADIUS, de las Listas de Acceso correspondientes.	EXIGIDO		
		Para los equipos que no posean el suplicante 802.1X o dispositivos que fallan en la autenticación el Switch permitirá la conexión a una VLAN especial.	EXIGIDO		
		Autenticación por dirección MAC sobre un servidor Radius.	EXIGIDO		
		Asignar VLAN cuando la autenticación fue realizada por Dirección MAC	EXIGIDO		
8.	ASIGNACION DE DIRECCIONES IP	Funcionalidad de Servidor DHCP en todas sus interfaces.	EXIGIDO		
		DHCP Relay	EXIGIDO		

LIC. ISIDRA MACHADO TROCHE
DIRECTORA- DUOC

		Cliente DHCP	EXIGIDO		
9.	ADMINISTRACION DE TRAFICO Y CALIDAD DE SERVICIO (QoS)	Mínimo de cantidad de listas de acceso por hardware para control de tráfico o políticas de calidad de servicio	1.500		
		Mínimo de colas por hardware de calidad de servicio por interfase	8		
		Deberá soportar los siguientes criterios de clasificación: por interfaz, por dirección MAC, por campo 802.1p, por VLAN, por dirección IP origen y/o destino, por campo DSCP/IP Precedence, por puertos TCP/UDP.	EXIGIDO		
		Configurar Ancho de banda garantizado (mínimo) para la clase de servicio	EXIGIDO		
		Configurar un límite de tráfico entrante en cada puerto	EXIGIDO		
		Configurar la priorización del tráfico saliente para cada clase de Servicio	EXIGIDO		
10.	ALTA DISPONIBILIDAD	Deberá soportar la agregación de interfaces para formar un único link, esta técnica es conocida como LAG (Link Aggregation Group) bajo la norma 802.3ad	EXIGIDO		
		Cantidad mínima de grupos LAG por sistema	32		
		Cantidad mínima de puertos pertenecientes a grupos LAG	EXIGIDO		
		Mecanismo de protección contra loops de L2: 802.1D (Spanning Tree), 802.1w (Rapid Spanning Tree) y 802.1s (Multiple Spanning Tree)	EXIGIDO		
		Deberá contar con la capacidad de agregar, mediante licencias, soporte para el protocolo VRRP.	EXIGIDO		
11.	SEGURIDAD	Deberá poder limitar la cantidad de Direcciones MAC por puerto.EXIGIDO	EXIGIDO		
		Deberá permitir o negar direcciones MAC configurables por puerto.	EXIGIDO		
		Deberá soportar Dynamic ARP inspection (DAI)	EXIGIDO		
		Deberá soportar Local Proxy ARP	EXIGIDO		
		Deberá soportar DHCP Snooping	EXIGIDO		
		Deberá soportar Static ARP	EXIGIDO		
12.	ADMINISTRACION	Soporte de Interfaz CLI (Telnet, SSHv2 y Puerto Serial)	EXIGIDO		
		Soporte de Interfaz WEB (HTTP y HTTPS)	EXIGIDO		
		Monitoreo remoto mediante SNMP y permitiendo los queries de SNMP a través de la definición de direcciones IP autorizadas para realizar las consultas.	v2c, v3		
		Configuración como cliente de NTP	EXIGIDO		
		Logging remoto utilizando syslog	EXIGIDO		
		Autenticación de usuarios	Local, RADIUS y TACACS+		
		Configuración de administradores locales	EXIGIDO		

LIC. ISIDRA MACHADO TROCHE
DIRECTORA - DUOC

		Definición de longitud mínima para el password de administrador almacenado en la base de datos local.	EXIGIDO		
		Creación de perfiles de administrador con facultadas especificas de modificar la configuración o solo acceder a vistas de la misma y listado de comandos disponibles para ejecutar por cada perfil.	EXIGIDO		
		Roll-back a varias configuraciones anteriores almacenadas en el equipo (mínimo 3 configuraciones) o una configuración de rescate almacenada especialmente por el administrador	EXIGIDO		
		Configuradón de puerto de monitoreo para el tráfico proveniente de una VLAN o de una selección de puertos	EXIGIDO		
		Sensor de temperatura que permitirá constatar si el mismo trabaja en las condiciones adecuadas y en caso de superar un umbral establecido por el operador enviara una alarma (TRAP-SNMP) a la consola de administración	EXIGIDO		
		Permitirá la configuración de funciones de RMON y SFLOW	EXIGIDO		
		El equipo deberá contar con un display LCD donde pueda ser visualizada información de estado del mismo.	EXIGIDO		
13.	ALIMENTACION ELECTRICA Y DIMENSIONES	Tensión de operación	Alterna, 220VCA		
		Montaje en rack de 19"	EXIGIDO		
14.	NORMAS Y ESTANDARES	RFC 2925 MIB for remore ping, trace	EXIGIDO		
		RFC 1122 Host Requirements	EXIGIDO		
		RFC 768 UDP	EXIGIDO		
		RFC 791 IP	EXIGIDO		
		RFC 783 TFTP	EXIGIDO		
		RFC 792 ICMP	EXIGIDO		
		RFC 793 TCP	EXIGIDO		
		RFC 826 ARP	EXIGIDO		
		RFC 894 IP over Ethernet	EXIGIDO		
		RFC 903 RARP	EXIGIDO		
		RFC 906 TFTP Bootstrap	EXIGIDO		
		RFC 1027 Proxy ARP	EXIGIDO		
		RFC 2068 HTTP server	EXIGIDO		
		RFC 1812 Requirements for IP Version 4 Routers	EXIGIDO		
		RFC 1519 CIDR	EXIGIDO		
		RFC 1256 IPv4 ICMP Router Discovery (IRDP)	EXIGIDO		
		RFC 1058 RIP v1	EXIGIDO		

JUNTA MUNICIPAL U.O.C. Nº 2
LIC. ISIDRA MACHADO TROCHE
DIRECTORA - DUOC

		RFC 2453 RIP v2	EXIGIDO		
		RFC 1492 TACACS+	EXIGIDO		
		RFC 2138 RADIUS Authentication	EXIGIDO		
		RFC 2139 RADIUS Accounting	EXIGIDO		
		RFC 3579 RADIUS EAP support for 802.1x	EXIGIDO		
		RFC 5176 Dynamic Authorization Extensions to RADIUS	EXIGIDO		
		RFC 2267 Network Ingress Filtering	EXIGIDO		
		RFC 2030 SNTP, Simple Network Time Protocol	EXIGIDO		
		RFC 854 Telnet client and server	EXIGIDO		
		RFC 951, 1542 BootP	EXIGIDO		
		RFC 2131 BOOTP/DHCP relay agent and DHCP server	EXIGIDO		
		RFC 1591 DNS	EXIGIDO		
		RFC 2474 DiffServ Precedence	EXIGIDO		
		RFC 2598 DiffServ Expedited Forwarding (EF)	EXIGIDO		
		RFC 2597 DiffServ Assured Forwarding (AF)	EXIGIDO		
		LLDP Media Endpoint Discovery (LLDP-MED), ANSI/TIA-1057, draft 08	EXIGIDO		

SWITCH TIPO 2:

ITEM	CARACTERISTICAS		MINIMO EXIGIDO	PROPUESTA DEL OFERENTE	
				CUMPLE SI/NO	EXPLICAR COMO CUMPLE
	Especificar	Marca y Modelo			
	Cantidad:	8 Unidades			

JUNTA MUNICIPAL U.O.C. N° 2
LIC. ISIDRA MACHADO TROCHI
DIRECTORA - DUOC

1. 1	RENDIMIENTO Y CAPACIDAD	El equipo deberá contar con al menos 104 Gbps de capacidad mínima de conmutación de paquetes.	EXIGIDO		
		El equipo deberá contar con, al menos, 77 Mpps de capacidad mínima de forwarding en Capa 2, en paquetes de 64 bytes	EXIGIDO		
		Debera estar equipado con una memoria flash de al menos 1 GB	EXIGIDO		
		Debera estar equipado con una memoria DRAM de al menos 512 MB	EXIGIDO		
		MTBF Mínimo Requerido de 125.000 hs.	EXIGIDO		
2.	CONECTIVIDAD DE RED	Deberá contar con al menos 48 puertos 10/100/1000 Base-T	EXIGIDO		
		Deberá contar con al menos 4 slots SFP independientes	EXIGIDO		
		La utilización de cualquiera de los mencionados slots SFP no deberá afectar la cantidad final de 24 puertos 10/100/1000 Base-T utilizables. Es decir no serán aceptados dispositivos que utilicen la modalidad "COMBO" para dichos slots.	EXIGIDO		
		Cada uno de los 4 slots SFP deberá soportar los siguientes tipos de transceptores SFP: 1000Base-T, SFP 1000Base-X Multimodo (500 mts de alcance), 1000Base-X Monomodo (10 kms de alcance).	EXIGIDO		
		Deberá estar equipado con al menos 2 Módulos SFP Gigabit Ethernet LX Monomodo instalados.	EXIGIDO		
		Deberá contar con al menos 1 puerto 10/100/1000 BaseT Ethernet adicional e independiente para administración del equipo.	EXIGIDO		
		Deberá contar con al menos 1 puerto SERIAL RS-232 para ser usado como consola de administración.	EXIGIDO		
		Deberá contar con al menos 1 puerto USB para el almacenado y descarga de configuraciones y sistema operativo.	EXIGIDO		
	CONMUTACION EN LAYER 2	Deberá soportar como mínimo 1024 VLANS	EXIGIDO		
		Deberá soportar como mínimo 4096 VLAN-IDs	EXIGIDO		
		Deberá soportar al menos 16.000 direcciones MAC	EXIGIDO		
		Soporte de 802.1D Spanning Tree Protocol	EXIGIDO		
		Soporte de 802.1w Rapid Spanning Tree	EXIGIDO		
		Soporte de 802.1s Multiple Instance Spanning Tree	EXIGIDO		

LIC. ISIDRA MACHADO TROCH
DIRECTORA - DUOC
JUNTA MUNICIPAL DE ASUNCION

		Jumbo Frames (9000 Bytes o superior)	EXIGIDO		
3.	STACKING	Los equipos deberán soportar STACKING	EXIGIDO		
		Debera soportar la configuración desde una única dirección IP y para su administración actuarán como un único equipo.	EXIGIDO		
		El reemplazo de un miembro del stack deberá ser no disruptivo. En caso que la versión de Sistema Operativo del equipo a incorporar sea distinta de la vigente el stack, la misma deberá actualizarse automáticamente.	EXIGIDO		
		Deberá contar con la capacidad de conectarse entre si por Uplink de 1 Gbps conformando un único equipo desde el punto de vista de la administración	EXIGIDO		
		Deberá soportar un mínimo de 4 equipos agrupados para administrar con un único acceso administrativo	EXIGIDO		
		Los puertos que forman parte de un puerto LAG podrán pertenecer a cualquiera de los miembros del Stack	EXIGIDO		
4.	ROUTING	Deberá soportar como mínimo 6.000 rutas IPv4 unicast	EXIGIDO		
		RIP (v1 y v2)	EXIGIDO		
		Soporte de Bidirectional Forwarding Detection (BFD)	EXIGIDO		
		Ruteo estático.	EXIGIDO		
		IP Directed Broadcast	EXIGIDO		
		ACL que permitan la clasificación de direcciones origen/destino L2 y L3	EXIGIDO		
		ACL que permitan ser aplicadas en el puerto al ingreso o egreso de los paquetes.	EXIGIDO		
		ACL que permitan ser aplicadas en la VLAN al ingreso y egreso de los paquetes.	EXIGIDO		
		ACL basadas en el encabezado de TCP/IP aplicadas al ingreso y egreso de los paquetes.	EXIGIDO		
	AUTENTICACION DE USUARIOS Y CONTROL DE ACCESO	Funcionalidad de 802.1x en cada por puerto.	EXIGIDO		
		Múltiples suplicantes en un mismo puerto físico validándolos en forma independiente.	EXIGIDO		
		Integración con sistemas de control de acceso por medio del protocolo RADIUS y 802.1x para autenticación de usuario.	EXIGIDO		
		Autenticación del usuario debe realizarse antes que los dispositivos conectados reciban una dirección IP de un Servidor DHCP.	EXIGIDO		

		El estándar 802.1X está basado en EAP (Extensible Authentication Protocol).	EXIGIDO		
		Deberá soportar EAP-MD5	EXIGIDO		
		Deberá soportar EAP-TLS.	EXIGIDO		
		Deberá soportar EAP-TTLS	EXIGIDO		
		Deberá soportar EAP-PEAP	EXIGIDO		
		Bloquear todo el tráfico generado por cualquier dispositivo conectado a la red y no autenticado.	EXIGIDO		
		Una vez que los dispositivos son autenticados podrán recibir parámetros, via atributo de RADIUS, de la VLANs correspondiente.	EXIGIDO		
		Una vez que los dispositivos son autenticados podrán recibir parámetros, via atributo de RADIUS, de las Listas de Acceso correspondientes.	EXIGIDO		
		Para los equipos que no posean el suplicante 802.1X o dispositivos que fallan en la autenticación el Switch permitirá la conexión a una VLAN especial.	EXIGIDO		
		Autenticación por dirección MAC sobre un servidor Radius.	EXIGIDO		
		Asignar VLAN cuando la autenticación fue realizada por Dirección MAC	EXIGIDO		
		Funcionalidad de Servidor DHCP en todas sus interfaces.	EXIGIDO		
		DHCP Relay	EXIGIDO		
5.	ASIGNACION DE DIRECCIONES IP	DHCP Helper	EXIGIDO		
		Cliente DHCP	EXIGIDO		
		Deberá soportar un mínimo de 1.500 listas de acceso por hardware para control de tráfico o políticas de calidad de servicio	EXIGIDO		
		Deberá soportar un mínimo de 8 colaspor interfaz, por hardware, de calidad de servicio.	EXIGIDO		

JUNTA MUNICIPAL U.O.C. Nº 2
LIC. ISIDRA MACHADO TROCHE
DIRECTORA - DUOC
JUNTA MUNICIPAL DE ASUNCION

6.	ADMINISTRACION DE TRAFICO Y CALIDAD DE SERVICIO (QoS)	Deberá soportar los siguientes criterios de clasificación: por interfaz, por dirección MAC, por campo 802.1p, por VLAN, por dirección IP origen y/o destino, por campo DSCP/IP Precedence, por puertos TCP/UDP.	EXIGIDO		
		Configurar un límite de tráfico entrante en cada puerto	EXIGIDO		
		Deberá soportar la agregación de interfaces para formar un único link, esta técnica es conocida como LAG (Link Aggregation Group) bajo la norma 802.3ad	EXIGIDO		
		Deberá soportar al menos 32 grupos LAG por sistema	EXIGIDO		
7.	ALTA DISPONIBILIDAD	Deberá soportar como mínimo 8 puertos pertenecientes a un grupo LAG	EXIGIDO		
		Mecanismo de protección contra loops de L2: 802.1D (Spanning Tree), 802.1w (Rapid Spanning Tree) y 802.1s (Multiple Spanning Tree)	EXIGIDO		
		Deberá poder limitar la cantidad de Direcciones MAC por puerto.	EXIGIDO		
		Deberá permitir o negar direcciones MAC configurables por puerto.	EXIGIDO		
	SEGURIDAD	Deberá soportar Dynamic ARP inspection (DAI)	EXIGIDO		
		Deberá soportar Proxy ARP	EXIGIDO		
		Deberá soportar DHCP Snooping	EXIGIDO		
		Deberá soportar IP Source Guard	EXIGIDO		
		Deberá soportar Static ARP	EXIGIDO		
		Soporte de Interfaz CLI (Telnet, SSHv2 y Puerto Serial)	EXIGIDO		
		Soporte de Interfaz WEB (HTTP y HTTPS)	EXIGIDO		
8.	ADMINISTRACION	Soporte de creación de Certificados locales para conexión HTTPs	EXIGIDO		
		Monitoreo remoto mediante SNMP (v1, v2c y v3) y permitiendo los queries de SNMP a través de la definición de direcciones IP autorizadas para realizar las consultas	EXIGIDO		
		Configuración como cliente de NTP	EXIGIDO		
		Logging remoto utilizando syslog	EXIGIDO		
		Autenticación de usuarios mediante TACACS+ y/o RADIUS	EXIGIDO		
		Soporte de Time Domain Reflectometry para detectar las fallas en cables UTP	EXIGIDO		
		Deberá soportar los protocolos Syslog, Telnet y SSH sobre IPv6 para administración del equipo	EXIGIDO		

LIC. ISIDRA MACHADO TROCHE
DIRECTORA - DUOC
JUNTA MUNICIPAL DE ASUNCION

		Deberá soportat IPv6 Network Discovery Protocol (NDP)	EXIGIDO		
		Configuración de administradores locales	EXIGIDO		
		Definición de complejidad y longitud mínima para el password de administrador almacenado en la base de datos local.	EXIGIDO		
		Las passwords (claves) de administrador almacenadas localmente deben estar encriptadas usando hash MD5 o SHA1	EXIGIDO		
		Deberá soportar la creación de al menos 20 perfiles de administrador con facultadas especificas de modificar la configuración o solo acceder a vistas de la misma y listado de comandos disponibles para ejecutar por cada perfil.	EXIGIDO		
		Roll-back a varias configuraciones anteriores almacenadas en el equipo (mínimo 3 configuraciones) o una configuración de rescate almacenada especialmente por el administrador	EXIGIDO		
		Mecanismos de automatización mediante scripts o similares que permitan chequear el cumplimiento y administrar los cambios de configuraciones, aplicar configuraciones predefinidas, visualizar conjuntos de comandos para el diagnóstico, análisis y administración de eventos, y generar respuestas predefinidas a eventos.	EXIGIDO		
		Configuración de puerto de monitoreo para el tráfico proveniente de una VLAN o de una selección de puertos, el tráfico que se envía al puerto de monitoreo deberá controlarse con el uso de filtros para evitar enviar tráfico no deseado.	EXIGIDO		
		Deberá tener la capacidad de enviar una alarma de temperatura interna cuando la misma exceda los limites configurados. Debe acreditarse la existencia de un sensor de temperatura para el cumplimiento de esta función.	EXIGIDO		
		Deberá proveer un mecanismos que permita configurar sensores de trafico para detectar retardos entre equipos utilizando las MIBs RPM según RFC 2925.	EXIGIDO		
		Permitirá la configuración de funciones de RMON (al menos 4 grupos: statistics, history, alarm y events) y SFLOW	EXIGIDO		
		Tensión de operación alterna de 220VCA	EXIGIDO		
		El equipo deberá contar con un puerto para conexión de fuente redundante externa	EXIGIDO		
9.	ALIMENTACION ELECTRICA Y DIMENSIONES	No se aceptarán transformadores de 220VCA a 110VCA agregados a la fuente integrada en el equipo. Dicha fuente debe aceptar directamente 220VCA 50 hz.	EXIGIDO		
		Deberá incluir los accesorios necesarios para montar en racks estándar de 19".	EXIGIDO		
		RFC 1122 Host Requirements	EXIGIDO		

JO. ISIDRA MACHADO TROCHE
DIRECTORA - DOOC
JUNTA MUNICIPAL DE ASUNCION

		RFC 768 UDP	EXIGIDO		
	NORMAS Y ESTANDARES	RFC 791 IP	EXIGIDO		
		RFC 783 TFTP	EXIGIDO		
		RFC 792 ICMP	EXIGIDO		
		RFC 793 TCP	EXIGIDO		
		RFC 826 ARP	EXIGIDO		
		RFC 894 IP over Ethernet	EXIGIDO		
		RFC 903 RARP	EXIGIDO		
		RFC 906 TFTP Bootstrap	EXIGIDO		
		RFC 1027 Proxy ARP	EXIGIDO		
		RFC 2068 HTTP server	EXIGIDO		
		RFC 1812 Requirements for IP Version 4 Routers	EXIGIDO		
		RFC 1519 CIDR	EXIGIDO		
		RFC 1256 IPv4 ICMP Router Discovery (IRDP)	EXIGIDO		
		RFC 1058 RIP v1	EXIGIDO		
		RFC 2453 RIP v2	EXIGIDO		
		RFC 1492 TACACS+	EXIGIDO		
		RFC 2138 RADIUS Authentication	EXIGIDO		
		RFC 2139 RADIUS Accounting	EXIGIDO		
		RFC 3579 RADIUS EAP support for 802.1x	EXIGIDO		
		RFC 5176 Dynamic Authorization Extensions to RADIUS	EXIGIDO		
		RFC 2267 Network Ingress Filtering	EXIGIDO		
		RFC 2030 SNTP, Simple Network Time Protocol	EXIGIDO		
		RFC 854 Telnet client and server	EXIGIDO		
		RFC 951, 1542 BootP	EXIGIDO		
		RFC 2131 BOOTP/DHCP relay agent and DHCP server	EXIGIDO		
		RFC 1591 DNS	EXIGIDO		

LIC. ISIDRA MACHADO TROCHE
DIRECTORA - DDOC
JUNTA MUNICIPAL DE ASUNCION

		RFC 2474 DiffServ Precedence	EXIGIDO		
		RFC 2598 DiffServ Expedited Forwarding (EF)	EXIGIDO		
		RFC 2597 DiffServ Assured Forwarding (AF)	EXIGIDO		
		LLDP Media Endpoint Discovery (LLDP-MED), ANSI/TIA-1057, draft 08	EXIGIDO		

CONTROLADOR INALAMBRICO

ITEM	CARACTERISTICAS	MINIMO EXIGIDO	PROPUESTA DEL OFERENTE	
			CUMPLE SI/NO	EXPLICAR COMO CUMPLE
	Cantidad: 1 Unidad			
1.	Marca y Modelo del controlador	Especificar		
2.	El controlador debe ser un dispositivo independiente - no se aceptan soluciones de módulos en el chasis de otros equipos (como un switch).	EXIGIDO		
3.	El controlador debe configurar y controlar los Access Points de forma centralizada.	EXIGIDO		
4.	La arquitectura de la solución debe permitir que los datos de usuarios se conmuten en un controlador centralizado.	EXIGIDO		
5.	La arquitectura de la solución también debe permitir que los datos se conmuten de forma distribuida (sin pasar por el controlador) y cada Access Point realiza la conmutación local de paquetes. La funcionalidad de conmutación de paquetes locales no debe depender del tipo de AP o ubicación.	EXIGIDO		
6.	La arquitectura de la solución debe permitir al usuario moverse entre los Access Points (que pueden estar asociados con diferentes controladores) sin afectar al usuario (incluyendo el tráfico de VoIP), mientras se mantiene la sesión, VLAN y dirección IP.	EXIGIDO		
7.	El controlador debe ejecutar las políticas de autorización integrada con un servidor AAA (RADIUS) central en la red.	EXIGIDO		
8.	Los puertos Ethernet del controlador deben soportar load-sharing.	EXIGIDO		
9.	Los puertos Ethernet del controlador deben ser soportar trunking 802.1Q	EXIGIDO		
10.	El controlador debe soportar Spanning Tree (802.1D) y ser compatible con per-VLAN spanning tree (PVST+).	EXIGIDO		
11.	El controlador debe proporcionar la calidad de servicio y ACL a los Access Points.	EXIGIDO		
12.	Debe ser capaz de clasificar y marcar el tráfico basado en capa 2 y 3	EXIGIDO		
13.	El controlador debe ser compatible con 802.1X con asignación de VLAN	EXIGIDO		
14.	Debe soportar EAP (EAP-TLS, PEAP / MSCHAP, TTLS)	EXIGIDO		
15.	Soporte para Autenticación Web-based y la autenticación por MAC	EXIGIDO		
16.	El tráfico de control entre el controlador y Access Point debe estar encriptado.	EXIGIDO		
17.	El tráfico de control entre los controladores debe estar encriptado.	EXIGIDO		

LIC. ISIDRA MACHADO TROCHE
DIRECTORA - DDOC
JUNTA MUNICIPAL DE ASUNCION

18.	Soportar la funcionalidad de restringir, permitir o priorizar el tráfico por usuario, SSID, aplicación, dirección IP, protocolo o CoS.	EXIGIDO		
19.	Debe permitir aplicar ACL a los usuarios o grupos de usuarios	EXIGIDO		
20.	Debe ser compatible con "IETF CAPWAP WG Taxonomy and Architecture (RFC 4118)	EXIGIDO		
21.	El controlador debe permitir una topología redundante N: 1	EXIGIDO		
22.	El controlador debe permitir una topología redundante N:N, formando un "cluster".	EXIGIDO		
23.	fuente de alimentación 220VCA	EXIGIDO		
24.	Soportar 802.11d, 802.11e, 802.11h, 802.11i	EXIGIDO		
25.	Detectar los siguientes tipos de ataques y vulnerabilidades: address masquerading, RF jamming, weak WEP IV detection, rogue detection, denial of service (DoS) attacks, flood attacks, unauthorized SSIDs, deauthentication attacks, null probes, decryption errors y spoofed APs.	EXIGIDO		
26.	Soporte para el acceso de guest (Guest VLAN)	EXIGIDO		
27.	La solución ofrecida debe soportar In Service Software Upgrade con la mínima interrupción de los servicios.	EXIGIDO		
28.	Soportar acceso a CLI y interfaz web (HTTPS), SSL, XML	EXIGIDO		
29.	Soportar SNMP v1, 2,3	EXIGIDO		
30.	Soportar Syslog	EXIGIDO		
31.	Especificar las dimensiones del controlador	EXIGIDO		
32.	**Especificación de la gestión de red inalámbrica**			
33.	El software de gestión debe mostrar la ubicación de los Access Points.	EXIGIDO		
34.	El software de gestión debe realizar el diseño, simulación, configuración, monitoreo y optimización de la red inalámbrica.	EXIGIDO		
35.	Se debe analizar el mapa de la cobertura de la señal teniendo en cuenta tres dimensiones (3D).	EXIGIDO		
36.	Debe colectar eventos y fallas y exponer la correlación de estos en un Tablero de Control- Dashboard.	EXIGIDO		
37.	Debe gestionar y controlar la red de RF para la protección contra intrusiones y ataques DoS.	EXIGIDO		
38.	Se debe identificar y mostrar la ubicación de Rogue Access Points y redes ad-hoc	EXIGIDO		
39.	Debe ser capaz de guardar los datos y mostrar un análisis de tendencias para ser utilizado en análisis de incidentes y Forense	EXIGIDO		
40.	Debe ser capaz de generar informes, incluyendo informes de cumplimiento con HIPAA, GLBA, SOX, PCI.	EXIGIDO		
41.	Soportar las importaciones de dibujos de Autocad.	EXIGIDO		
42.	Plazo de garantía, de al menos:	12 meses.		
43.	Instalación; El equipo deberá ser configurado, instalado y probado de acuerdo a las indicaciones del personal técnico del oferente.	EXIGIDO		

PUNTOS DE ACCESO INALAMBRICO

ITEM	CARACTERISTICAS	MINIMO EXIGIDO	PROPUESTA DEL OFERENTE	
			CUMPLE	EXPLICAR

Lic. ISIDRA MACHADO TROCHEZ
DIRECTORA - DUOC

JUNTA MUNICIPAL DE ASUNCION
DIRECCION OPERATIVA DE CONTRATACIONES

			SI/NO	COMO CUMPLE
	Cantidad: 8 Unidades			
1.	Marca y Modelo del AP	Especificar		
2.	El AP debe recibir la configuración del controlador.	EXIGIDO		
3.	El AP debe ser compatible con PoE (IEEE 802.3af) para la conexión con un switch PoE o con un Power Injector.	EXIGIDO		
4.	El AP debe tener single radio single para operar en 802.11a/n (5 GHz) o 802.11b/g/n (2,4 GHz)	EXIGIDO		
5.	El AP debe ser controlado para realizar ajustes automáticos de los canales de RF y intensidad de la señal.	EXIGIDO		
6.	Las antenas deben ser internas. No se aceptaran equipo con antenas externas	EXIGIDO		
7.	Debe soportar Mesh y Bridging.	EXIGIDO		
8.	Debe soportar 2x2 MIMO	EXIGIDO		
9.	Soportar los canales de 20 y 40 MHz	EXIGIDO		
10.	Soportar una interfaz de uplink Ethernet 10/100/1000Base-T, RJ-45, POE	EXIGIDO		
11.	Claves de encriptación y las credenciales del usuario no se almacenan en el AP	EXIGIDO		
12.	No debe poseer puerto de consola para garantizar la seguridad	EXIGIDO		
13.	Soportar Kensington Security slot para utilizar elementos de anclaje estándar de la industria y prevenir hurtos	EXIGIDO		
14.	Es posible realizar el scanning y la mitigación de la red inalámbrica en Access Points dedicados a esta función o en Access Points compartidos con servicios inalámbricos para clientes.	EXIGIDO		
15.	Soportar WIDS/WIPS.	EXIGIDO		
16.	Soportar encriptación (AES / CCMP y TKIP)	EXIGIDO		
17.	Soportar Fast Roaming (PMK caching)	EXIGIDO		
18.	Soportar control de admisión de llamadas (TSPEC)	EXIGIDO		
19.	Soportar WEP, WPA, WPA2.	EXIGIDO		
20.	Cuando el controlador primario asociado con el AP no está disponible, el AP de inmediato debe unirse a otro controlador, sin tener que reiniciar el AP.	EXIGIDO		
21.	Cuando hay un fail-over de un AP de un controlador a otro controlador, la sesión del usuario no debe ser interrumpido.	EXIGIDO		
22.	Soportar WiFi Alliance Certification para 802.11 a / b / g / n	EXIGIDO		
23.	Temperatura de funcionamiento operacional:	de 0 a 50 grados C		
24.	Humedad:	10 a 95% (sin condensación)		
25.	Para los outdoor Access Points: temperatura de funcionamiento operacional	40 a 70 grados C		
26.	Para los outdoor Access Points: humedad	10 a 95% (sin condensación).		
27.	Número máximo de SSID por radio	32		

LIC. [illegible]RA MACHADO TROCHE
DIRECTORA - DUOC

28.	Soportar distribución de carga de asociación de Access Points al controlador de forma automática.	EXIGIDO		
29.	Especificar las dimensiones del Access Point	EXIGIDO		
30.	Especificar la potencia máxima del AP (Maximum transmit power)	EXIGIDO		

Se incluyen las siguientes modificaciones de las secciones dejadas sin efecto:

EQUIPO DE BORDE

Especificar Marca y modelo ofertado:

- Cantidad de enrutadores: 1 unidad
- Administración vía interfaz web segura (HTTPS)
- Calidad de servicio basada en aplicaciones
- Capacidad de configurar ancho de banda de uplink y downlink
- Certificaciones CE, FCC, Anatel
- Debe tener un puerto configurable a DMZ
- Fuente de alimentación automática de 100 a 240 V, 50-60 Hz
- NAT throughput mínimo de 200 Mbps
- NAT uno-a-uno, NAT trasversal, PAT, NAPT
- Por lo menos 8 interfaces LAN RJ-45 Fast Ethernet
- Por lo menos dos interfaces ethernet Fast Ethernet configurables para la WAN
- Protocolos en la interfaz WAN: DHCP, Static Ip, PPTP, Modo Bridge, PPoE
- Registro de eventos (syslog)
- Routing estático y Routing Dinámico (RIP)
- Soporte de protocolo SNMP
- Tamaño: rackeable, 1U
- VPN throughput de por lo menos 90 Mbps

Características de seguridad

- Stateful Packet Inspection
- Bloqueo de URL estática
- Definición de complejidad mínima de contraseña de administración
- Por lo menos poder levantar 100 túneles Ipsec site to site
- Por lo menos 30 entradas de port forwarding y port triggering
- Por lo menos 40 reglas de acceso
- Reporte por email en caso de ataques: Denegación de servicio, IP spoofing, SYN flood, Land Attack, ping de la muerte

SWITCH TIPO 1:

1.1 Especificaciones técnicas - Switch tipo 1 (Switch layer 3)

Especificar marca y modelo ofertado:

- Cantidad de switches tipo 1: 1 unidad
- Administrable vía interfaz web, sobre conexión segura (HTTPS)
- Cantidad mímina de puertos: 50
- Capacidad mínima de switching en Gbps: 100
- Capacidad mínima en millones de paquetes por segundo (con paquetes de 64 bytes): 70
- Características de ahorro de energía: corte de energía por puerto, cuando el enlace no está

JUNTA MUNICIPAL
LIC. ROSA MARGARITA
DIRECTORA - DUOC

activo

- Certificación: UL, CSA, FCC, CE
- Fuente de alimentación automática de 100 a 240 V, 50-60 Hz
- Inspección ARP dinámica
- La totalidad de los puertos debe ser Gigabit Ethernet
- Por lo menos 2 puertos deben ser SFP, el resto debe ser RJ-45
- Por lo menos 500 rutas estáticas
- Posibilidad de definir clase de servicio por VLAN
- Posibilidad de definir por lo menos 100 interfaces IP
- Posibilidad de realizar Port Mirroring
- Posibilidad de realizar ruteo de paquetes IPV4
- Posibilidad de realizar VLAN Mirroring
- Posibilidad de ser un server DHCP
- Seguridad de puertos: Bloquear direcciones MAC de origen a los puerto
- Seguridad de puertos: Bloquear por software puertos no utilizados
- Soporte de 802.3ad, por lo menos 8 grupos.
- Soporte de por lo menos 4000 VLANs simultáneas
- Soporte de SNMP V3
- Tamaño: rackeable, 1U

1.2 Especificaciones técnicas - Switch tipo 2

Especificar marca y modelo ofertado:

- Cantidad de switches tipo 2: 8 unidades
- Administrable vía interfaz web (HTTP)
- Cantidad mímina de puertos: 48
- Capacidad mínima de switching en Gbps: 12
- Capacidad mínima en millones de paquetes por segundo (con paquetes de 64 bytes): 10
- Características de ahorro de energía: Ajuste de la intensidad de señal, según longitud del cable.
- Certificación: UL, CSA, FCC, CE
- Fuente de alimentación automática de 100 a 240 V, 50-60 Hz
- Por lo menos 2 puertos deben ser Gigabit Ethernet (para el uplink), el resto debe ser Fast Ethernet
- Por lo menos 2 puertos deben ser SFP, el resto debe ser RJ-45
- Posibilidad de definir clase de servicio por VLAN
- Posibilidad de realizar Port Mirroring
- Posibilidad de realizar VLAN Mirroring
- Seguridad de puertos: Bloquear direcciones MAC de origen a los puerto
- Seguridad de puertos: Bloquear por software puertos no utilizados
- Soporte de 802.3ad, por lo menos 4 grupos.
- Soporte de por lo menos 256 VLANs simultáneas
- Soporte de Jumbo Frames de 10KB
- Tamaño: rackeable, 1U

1.3 Especificaciones Técnicas - Red Inalámbrica

Especificar marca y modelo ofertado:

- Cantidad de punto de acceso inalámbricos (access point): 8 unidades

<u>Características del access point:</u>

- Aislamiento de tráfico de visitantes
- Alimentación vía Power over Ethernet
- Antenas integradas, con soporte de MIMO y Diversidad Espacial
- Cantidad mínima de clientes concurrentes por access point: 75

JUNTA MUNICIPAL
LIC. ISIDRA MACHADO TROCHE
DIRECTORA - DUOC

- Certificaciones del producto: CE, FCC, IC
- Mínimo una interfaz Fast Ethernet
- Posibilidad de roaming de usuarios entre los access points, sin perder conexión
- Seguridad: 802.11i, WPA-TKIP, WPA-PSK, WPA2-AES, WEP
- Soporte de los estándares Wifi 802.11 B/G/N 2.4GHz
- Soporte de por lo menos 4 BSSID
- Soporte de VLAN 802.1Q
- Tasa de calidad de servicio limitable por usuario
- Tasa de datos de por lo menos 300 Mbps en 802.11n
- Wifi Multimedia (WMM)

Características de administración de access points:

- Administración **centralizada** de todos los access points a través de navegador web
- Definición de Portal de visitantes / portal cautivo.
- Gráficos y estadísticas detalladas de tráfico de la red inalámbrica, usuarios conectados, datos de cada access point.
- Posibilidad de configurar diferentes niveles de acceso a la administración de la red inalámbrica
- Registro de eventos (errores, fecha de conexión de usuarios, informaciones, etc.) para el troubleshooting

LIC. ISIDRA MACHADO TROCH
DIRECTOR - DUOC
JUNTA MUNICIPAL
U.O.C. Nº