A: Comité Evaluador

De: Víctor Villalba, Jefe
Casildo S. Miranda M., Técnico
Dirección TIC's

VICTOR D. VILLALBA
Jefe Sección Redes

CASILDO S. MIRANDA M.
Técnico
Redes y Comunicaciones

Fecha: 31-03-14

OBJETO: Remitir Evaluación Técnica correspondiente al P.AC. 44/2013 Id Nº: 256.694 "Adquisición de Equipos de Informática para el Datacenter".

Oferente: Tecnología en Electrónica e Informática S.A.

ITEM 1 – ROUTER/FIREWALL DE BORDE

Marca: Fortinet

Modelo: Fortigate 200B

ITEM	CARACTERISTICAS		MINIMO EXIGIDO	Evaluación	
				Ofertado	**CUMPLE SI/NO**
1.	GENERALIDADES	El equipo cumplirá funciones tanto de ruteo como de seguridad perimetral. Por dicho motivo, el mismo deberá poseer prestaciones tanto de Router como de Firewall. Este requerimiento obedece a la necesidad de tomar todas las precauciones posibles en cuanto a seguridad se requiere, sobre todo debido al importante incremento de ataques informáticos ocurridos en estos últimos tiempos. A fin de permitir una mayor participación de oferentes, serán aceptadas soluciones que distribuyan las funciones de ruteo y seguridad en equipos separados, siempre y cuando la solución como conjunto cumpla con los requerimientos mínimos exigidos para este ítem.	EXIGIDO	Marca: Fortinet Modelo: Fortigate 200B	Si Cumple
2.	RENDIMIENTO Y CAPACIDAD	Performance Firewall Troughput en paquetes de 64 bytes	4 Gbps	5 Gbps	Si Cumple
3.		VPN IPSEC Troughput en paquetes de 64 bytes	2 Gbps	2.5 Gbps	Si Cumple
4.		Sesiones Concurrentes soportadas	400.000	500.000	Si Cumple
5.		Nuevas sesiones por segundo	12.000	15.000	Si Cumple
6.		Cantidad de Access Lists o políticas de seguridad	10.000	12.000	Si Cumple
7.		Cantidad de puertos 10/100/1000Base-T – Configurables como WAN, LAN o DMZ	8	8	Si Cumple
8.		Puertos USB 2.0	1	3	Si Cumple
9.	ROUTING	BGP	EXIGIDO	Soportado	Si Cumple
10.		OSPF	EXIGIDO	Soportado	Si Cumple
11.		RIP v1/v2	EXIGIDO	Soportado	Si Cumple
12.		Soporte a ruteo de multicast	EXIGIDO	Soportado	Si Cumple
13.		Soporte a ruteo estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas	EXIGIDO	Soportado	Si Cumple
14.		Soporte a políticas de ruteo (policy routing)	EXIGIDO	Soportado	Si Cumple
15.		Soporte a ruteo dinámico RIPng, OSPFv3	EXIGIDO	Soportado	Si Cumple
16.		Soporte de ECMP (Equal Cost Multi-Path)	EXIGIDO	Soportado	Si Cumple
17.	AUTENTICACION DE USUARIOS Y CONTROL DE ACCESO	Capacidad de integrarse con Servidores de Autenticación RADIUS	EXIGIDO	Soportado	Si Cumple
18.		Capacidad nativa de integrarse con directorios LDAP	EXIGIDO	Soportado	Si Cumple
19.		Soporte a inclusión en autoridades certificadoras (enrollment) mediante SCEP (Simple Certificate Enrollment Protocol) y mediante archivos.	EXIGIDO	Soportado	Si Cumple
20.	TRADUCCION DE DIRECCIONES	NAT	EXIGIDO	Soportado	Si Cumple
21.		PAT	EXIGIDO	Soportado	Si Cumple
22.		NAT estático	EXIGIDO	Soportado	Si Cumple
23.		NAT con PAT	EXIGIDO	Soportado	Si Cumple
24.	ASIGNACION DE DIRECCIONES IP	Cliente DHCP	EXIGIDO	Soportado	Si Cumple
25.		Servidor DHCP	EXIGIDO	Soportado	Si Cumple
26.		DHCP Relay	EXIGIDO	Soportado	Si Cumple
27.	CONMUTACION EN	Soporte de VLAN 802.1Q	8192	8192	Si Cumple

28.	LAYER 2	Soporte de Link Aggregation Group (802.3ad) con un mínimo de 4 interfaces por grupo	EXIGIDO	Soportado	Si Cumple
29.		Soporte a etiquetas de VLAN (802.1q) y creación de zonas de seguridad en base a VLANs	EXIGIDO	Soportado	Si Cumple
30.	ADMINISTRACION DE TRAFICO Y CALIDAD DE SERVICIO (QoS)	Capacidad de poder asignar parámetros de traffic shapping.	EXIGIDO	Soportado	Si Cumple
31.		Capacidad de poder definir ancho de banda garantizado en KiloBytes por segundo	EXIGIDO	Soportado	Si Cumple
32.		Capacidad de poder definir límite de ancho de banda (ancho de banda máximo) en KiloBytes por segundo	EXIGIDO	Soportado	Si Cumple
33.		Capacidad para definir prioridad de tráfico, en al menos tres niveles de importancia	EXIGIDO	Soportado	Si Cumple
34.		Capacidad de poder asignar parámetros de traffic shaping diferenciadas para el tráfico en distintos sentidos de una misma sesión	EXIGIDO	Soportado	Si Cumple
35.		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	Soportado	Si Cumple
36.	ALTA DISPONIBILIDAD	Soporte de Alta Disponibilidad en modo transparente, es decir, sin pérdida de conexiones en caso de que un nodo falle.	EXIGIDO	Soportado	Si Cumple
37.		Soporte de Alta Disponibilidad en modo Activo-Activo	EXIGIDO	Soportado	Si Cumple
38.		Soporte de Alta Disponibilidad en modo Activo-Pasivo	EXIGIDO	Soportado	Si Cumple
39.	ADMINISTRACION	Soporte de Interfaz CLI	EXIGIDO	Soportado	Si Cumple
40.		Soporte de Interfaz WEB (HTTP y HTTPS)	EXIGIDO	Soportado	Si Cumple
41.		Puerto serial dedicado para administración.	EXIGIDO	Soportado	Si Cumple
42.		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	Soportado	Si Cumple
43.		Los administradores podrán tener asignado un perfil de administración que permita delimitar las funciones del equipo que pueden gerenciar y afectar.	EXIGIDO	Soportado	Si Cumple
44.		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	Soportado	Si Cumple
45.		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	Soportado	Si Cumple
46.		Soporte de SNMP versión 2	EXIGIDO	Soportado	Si Cumple
47.		Soporte de servidores syslog para poder enviar bitácoras a servidores de SYSLOG remotos	EXIGIDO	Soportado	Si Cumple
48.	ALIMENTACION ELECTRICA Y DIMENSIONES	Tensión de operación	Alterna, 220VCA	100-240 VAC	Si Cumple
49.		Deberá contar con la posibilidad de agregar una fuente de poder secundaria para redundancia, ya sea esta interna o externa.	EXIGIDO	Soportado	Si Cumple
50.		MTBF Mínimo Requerido	90.000Hs.	92.334 Hs.	Si Cumple
51.		Montaje en rack de 19"	EXIGIDO	Soportado	Si Cumple

ITEM 2 – SWITCH DE CORE

Marca: Juniper

Modelo: EX4550

CASILDO S. MIRANDA M.
Técnico
Redes y Comunicaciones

ITEM	CARACTERISTICAS		MINIMO EXIGIDO	Evaluación	
				Ofertado	**CUMPLE SI/NO**
1.	GENERALES	A fin de permitir una mayor participación de oferentes, serán aceptadas soluciones tanto del formato "Chassis" (modular) como del formato "Stacking" (sistema único conformado por múltiples equipos apilados).	EXIGIDO	*Marca: Juniper* *Modelo: EX4550*	Si Cumple
2.		En cualquiera de los dos casos se deberán respetar los requisitos mínimos solicitados en las presentes especificaciones. Se hace una salvedad para los requisitos inherentes a solo una de las tecnologías.	EXIGIDO	*Stacking*	Si Cumple

VICTOR D. VILLALBA
Jefe Sección Redes

		Por ejemplo: Los requisitos de "Stacking" no serán exigidos en equipos cuya solución este basada en el formato "Chassis" (modular)			
3.	RENDIMIENTO Y CAPACIDAD	Capacidad mínima de forwarding, de la supervisora, en Capa 2 en paquetes de 64 bytes	650 Mpps	714 Mpps	Si Cumple
4.		Capacidad mínima de conmutación de paquetes de la supervisora.	900 Gbps	960 Gbps	Si Cumple
5.		Capacidad mínima de forwarding entre módulos (backplane),	40 Gbps	40 Gbps	Si Cumple
6.		Memoria Flash	1 GB	2 GB	Si Cumple
7.		Memoria DRAM	1 GB	2 GB	Si Cumple
8.		MTBF Mínimo Requerido	80.000 Hs.	146.000 Hs.	Si Cumple
9.	CONECTIVIDAD DE RED	Capacidad de conectar Transceptores SFP 1000Base-T	EXIGIDO	Soportado	Si Cumple
10.		Capacidad de conectar Transceptores SFP 1000Base-X Multimodo	EXIGIDO	Soportado	Si Cumple
11.		Capacidad de conectar Transceptores SFP 1000Base-X Monomodo	EXIGIDO	Soportado	Si Cumple
12.		Capacidad de soportar Módulos SFP+ 10 GigabitEthernet SR Multimodo	EXIGIDO	Soportado	Si Cumple
13.		Capacidad de soportar Módulos SFP+ 10 GigabitEthernet LR Monomodo	EXIGIDO	Soportado	Si Cumple
14.		Cantidad de slots SFP+	30	32	Si Cumple
15.		Cantidad Mínima de interfaces 1000Base-T soportadas	54	56	Si Cumple
16.		Cantidad Mínima de interfaces 1000Base-X soportadas	30	32	Si Cumple
17.		Cantidad Mínima de interfaces 10 GbE soportadas	30	32	Si Cumple
18.		Cantidad de Módulos SFP+ 10 Gigabit Ethernet SR Multimodo instalados.	2	2	Si Cumple
19.		Cantidad de Módulos SFP+ 10 Gigabit Ethernet LR Monomodo instalados.	10	10	Si Cumple
20.		Cantidad de Módulos SFP 1000 BASE-LX Monomodo instalados.	8	8	Si Cumple
21.		Cantidad de Módulos SFP 1000 BASE-SX Multimodo instalados.	8	8	Si Cumple
22.		Cantidad de puertos 10/100/1000 BASE-T (RJ-45) requeridos.	24	24	Si Cumple
23.		A fin de proteger la inversión los equipos deberán contar con la posibilidad de crecimiento en puertos de red mediante la agregación de módulos (formato chassis) o nuevos integrantes (formato stacking).	EXIGIDO	Soportado	Si Cumple
24.		Las capacidades finales en cuanto a cantidad de puertos de red del sistema deberán ser las siguientes: - 430 Puertos 10/100/1000 BaseT - 45 Puertos Ten Gigabit Ethernet.	EXIGIDO	430 Puertos 10/100/1000 BaseT 45 Puertos Ten Gigabit Ethernet.	Si Cumple
25.		Todas las interfaces se podrán utilizar independientemente en modo L3 o L2 , es decir se podrán agrupar para formar un dominio de Broadcast (L2) representadas por una interfase L3 virtual (Interfase VLAN) o cada interfase física o lógica podrá configurarse con una dirección IP independiente (L3)	EXIGIDO	Soportado	Si Cumple
26.		Cantidad mínima de puertos 10/100/1000 BaseT Ethernet adicional e independiente para administración del equipo.	1	1	Si Cumple
27.		Cantidad mínima de puertos SERIAL RS-232 para ser usado como consola de administración.	1	1	Si Cumple
28.	CONMUTACION EN LAYER 2	Mínimo VLANS soportadas	4.000	4.096	Si Cumple
29.		Mínimo de direcciones MAC	30.000	32.000	Si Cumple
30.		Soporte de 802.1D Spanning Tree Protocol	EXIGIDO	Soportado	Si Cumple
31.		Soporte de 802.1w Rapid Spanning Tree	EXIGIDO	Soportado	Si Cumple
32.		Soporte de 802.1s Multiple Instance Spanning Tree	EXIGIDO	Soportado	Si Cumple
33.		Jumbo Frames (9000 Byte)	EXIGIDO	Soportado	Si Cumple
34.	ROUTING	Mínimo de rutas IPv4 unicast	10.000	Soportado	Si Cumple
35.		BGP	EXIGIDO	Soportado	Si Cumple
36.		OSPF	EXIGIDO	Soportado	Si Cumple
37.		RIP (v1 y v2)	EXIGIDO	Soportado	Si Cumple
38.		ISIS	EXIGIDO	Soportado	Si Cumple
39.		Ruteo estático.	EXIGIDO	Soportado	Si Cumple
40.	MULTICAST	Soporte de IGMP (v1, v2, v3)	EXIGIDO	Soportado	Si Cumple
41.		Soporte de PIM-SM	EXIGIDO	Soportado	Si Cumple
42.		Soporte de IGMP Snooping	EXIGIDO	Soportado	Si Cumple
43.		Capacidad mínima de entradas multicast IPV4 en Hardware	4.000	4.000	Si Cumple

CASILDO S. MIRANDA M.
Técnico
Redes y Comunicaciones

VICTOR D. VILLALBA
Jefe Sección Redes

44.	AUTENTICACION DE USUARIOS Y CONTROL DE ACCESO	ACL que permitan la clasificación de direcciones origen/destino L2	EXIGIDO	Soportado	Si Cumple
45.		ACL que permitan la clasificación de direcciones origen/destino L3	EXIGIDO	Soportado	Si Cumple
46.		ACL que permitan ser aplicadas en el puerto al ingreso o egreso de los paquetes.	EXIGIDO	Soportado	Si Cumple
47.		ACL que permitan ser aplicadas en la VLAN al ingreso y egreso de los paquetes.	EXIGIDO	Soportado	Si Cumple
48.		ACL basadas en el encabezado de TCP/IP aplicadas al ingreso y egreso de los paquetes.	EXIGIDO	Soportado	Si Cumple
49.		Funcionalidad de 802.1x en cada por puerto.	EXIGIDO	Soportado	Si Cumple
50.		Múltiples suplicantes en un mismo puerto físico validándolos en forma independiente.	EXIGIDO	Soportado	Si Cumple
51.		Integración con sistemas de control de acceso por medio del protocolo RADIUS y 802.1x para autenticación de usuario.	EXIGIDO	Soportado	Si Cumple
52.		Autenticación del usuario debe realizarse antes que los dispositivos conectados reciban una dirección IP de un Servidor DHCP.	EXIGIDO	Soportado	Si Cumple
53.		El estándar 802.1X está basado en EAP (Extensible Authentication Protocol).	EXIGIDO	Soportado	Si Cumple
54.		Deberá soportar EAP-MD5	EXIGIDO	Soportado	Si Cumple
55.		Deberá soportar EAP-TLS	EXIGIDO	Soportado	Si Cumple
56.		Deberá soportar EAP-TTLS	EXIGIDO	Soportado	Si Cumple
57.		Deberá soportar EAP-PEAP	EXIGIDO	Soportado	Si Cumple
58.		Bloquear todo el tráfico generado por cualquier dispositivo conectado a la red y no autenticado.	EXIGIDO	Soportado	Si Cumple
59.		Una vez que los dispositivos son autenticados podrán recibir parámetros, via atributo de RADIUS, de la VLANs correspondiente.	EXIGIDO	Soportado	Si Cumple
60.		Una vez que los dispositivos son autenticados podrán recibir parámetros, via atributo de RADIUS, de las Listas de Acceso correspondientes.	EXIGIDO	Soportado	Si Cumple
61.		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	Soportado	Si Cumple
62.		Autenticación por dirección MAC sobre un servidor Radius.	EXIGIDO	Soportado	Si Cumple
63.		Asignar VLAN cuando la autenticación fue realizada por Dirección MAC	EXIGIDO	Soportado	Si Cumple
64.	ASIGNACION DE DIRECCIONES IP	Funcionalidad de Servidor DHCP en todas sus interfaces.	EXIGIDO	Soportado	Si Cumple
65.		DHCP Relay	EXIGIDO	Soportado	Si Cumple
66.		DHCP Helper	EXIGIDO	Soportado	Si Cumple
67.		Cliente DHCP	EXIGIDO	Soportado	Si Cumple
68.	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	1.000	1500	Si Cumple
69.		Mínimo de colas por hardware de calidad de servicio por interfase	8	8	Si Cumple
70.		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	Soportado	Si Cumple
71.		Configurar Ancho de banda garantizado (mínimo) para la clase de servicio	EXIGIDO	Soportado	Si Cumple
72.		Configurar un límite de tráfico entrante en cada puerto	EXIGIDO	Soportado	Si Cumple
73.		Configurar la priorización del tráfico saliente para cada clase de Servicio	EXIGIDO	Soportado	Si Cumple
74.	ALTA DISPONIBILIDAD	Redundancia de Supervisora de Enrutamiento y Administración	EXIGIDO	Soportado	Si Cumple
75.		Proveerá un mecanismo que minimice el impacto de la falla de uno o más equipos de la red a través de VRRP, de acuerdo con la RFC 3768.	EXIGIDO	Soportado	Si Cumple
76.		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	Soportado	Si Cumple
77.		Cantidad mínima de grupos LAG por sistema	64	64	Si Cumple
78.		Cantidad mínima de puertos pertenecientes a grupos LAG	8	8	Si Cumple
79.		Mecanismo de protección contra loops de L2: 802.1D (Spanning Tree), 802.1w (Rapid Spanning Tree) y 802.1s (Multiple Spanning Tree)	EXIGIDO	Soportado	Si Cumple
80.	SEGURIDAD	Deberá poder limitar la cantidad de Direcciones MAC por puerto.	EXIGIDO	Soportado	Si Cumple
81.		Deberá permitir o negar direcciones MAC configurables	EXIGIDO	Soportado	Si Cumple

CASILDO S. MIRANDA M.
Técnico
Redes y Comunicaciones

VICTOR D. VILLALBA
Jefe Sección Redes

		por puerto.			
82.		Deberá soportar Dynamic ARP inspection (DAI)	EXIGIDO	Soportado	Si Cumple
83.		Deberá soportar Local Proxy ARP	EXIGIDO	Soportado	Si Cumple
84.		Deberá soportar DHCP Snooping	EXIGIDO	Soportado	Si Cumple
85.		Deberá soportar Static ARP	EXIGIDO	Soportado	Si Cumple
86.	ADMINISTRACION	Soporte de Interfaz CLI (Telnet, SSHv2 y Puerto Serial)	EXIGIDO	Soportado	Si Cumple
87.		Soporte de Interfaz WEB (HTTP y HTTPS)	EXIGIDO	Soportado	Si Cumple
88.		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	Soportado	Si Cumple
89.		Configuración como cliente de NTP	EXIGIDO	Soportado	Si Cumple
90.		Logging remoto utilizando syslog	EXIGIDO	Soportado	Si Cumple
91.		Autenticación de usuarios	Local, RADIUS y TACACS+	Soportado	Si Cumple
92.		Configuración de administradores locales	EXIGIDO	Soportado	Si Cumple
93.		Definición de complejidad y longitud mínima para el password de administrador almacenado en la base de datos local.	EXIGIDO	Soportado	Si Cumple
94.		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	Soportado	Si Cumple
95.		Roll-back a varias configuraciones anteriores almacenadas en el equipo (mínimo 3 configuraciones) o una configuración de rescate almacenada especialmente por el administrador	EXIGIDO	Soportado	Si Cumple
96.		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	Soportado	Si Cumple
97.		Almacenar en forma automática la configuración en servidor FTP ante cada uno de los cambios realizados, con propósito de backup	EXIGIDO	Soportado	Si Cumple
98.		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	Soportado	Si Cumple
99.		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	Soportado	Si Cumple
100.		Permitirá la configuración de funciones de RMON y SFLOW	EXIGIDO	Soportado	Si Cumple
101.	ALIMENTACION ELECTRICA Y DIMENSIONES	Tensión de operación	Alterna, 220VCA	100-240 VAC	Si Cumple
102.		El equipo deberá estar equipado con fuentes de alimentación redundantes en configuración n+1, donde n es la cantidad de fuentes necesarias para la operación del equipo en la configuración solicitada.	EXIGIDO	Soportado	Si Cumple
103.		El equipo deberá soportar la cantidad de fuentes para operar en redundancia n+1 para la configuración del equipo totalmente equipado con placas de línea.	EXIGIDO	Soportado	Si Cumple
104.		La fuente de alimentación debe tener la posibilidad de extracción y reemplazo en campo.	EXIGIDO	Soportado	Si Cumple
105.		El equipo debe soportar la falla o pérdida de alimentación eléctrica en una fuente de alimentación sin afectar su funcionamiento. Las fuentes deben poder ser reemplazadas durante la operación normal del equipo, sin necesidad de apagarlo.	EXIGIDO	Soportado	Si Cumple
106.		La bandeja de ventiladores debe tener la posibilidad de extracción y reemplazo en campo.	EXIGIDO	Soportado	Si Cumple
107.		El equipo debe soportar la falla o pérdida de al menos un ventilador sin afectar su funcionamiento.	EXIGIDO	Soportado	Si Cumple
108.		Montaje en rack de 19"	EXIGIDO	Soportado	Si Cumple
109.	NORMAS Y ESTANDARES	RFC 1122 Host Requirements	EXIGIDO	Soportado	Si Cumple
110.		RFC 768 UDP	EXIGIDO	Soportado	Si Cumple
111.		RFC 791 IP	EXIGIDO	Soportado	Si Cumple
112.		RFC 783 TFTP	EXIGIDO	Soportado	Si Cumple
113.		RFC 792 ICMP	EXIGIDO	Soportado	Si Cumple
114.		RFC 793 TCP	EXIGIDO	Soportado	Si Cumple
115.		RFC 826 ARP	EXIGIDO	Soportado	Si Cumple

CASILDO S. MIRANDA IV
Técnico
Redes y Comunicaciones

VICTOR D. VILLALBA
Jefe Sección Redes

116.		RFC 894 IP over Ethernet	EXIGIDO	Soportado	Si Cumple
117.		RFC 903 RARP	EXIGIDO	Soportado	Si Cumple
118.		RFC 906 TFTP Bootstrap	EXIGIDO	Soportado	Si Cumple
119.		RFC 1027 Proxy ARP	EXIGIDO	Soportado	Si Cumple
120.		RFC 2068 HTTP server	EXIGIDO	Soportado	Si Cumple
121.		RFC 1812 Requirements for IP Version 4 Routers	EXIGIDO	Soportado	Si Cumple
122.		RFC 1519 CIDR	EXIGIDO	Soportado	Si Cumple
123.		RFC 1256 IPv4 ICMP Router Discovery (IRDP)	EXIGIDO	Soportado	Si Cumple
124.		RFC 1058 RIP v1	EXIGIDO	Soportado	Si Cumple
125.		RFC 2453 RIP v2	EXIGIDO	Soportado	Si Cumple
126.		RFC 1112 IGMP v1	EXIGIDO	Soportado	Si Cumple
127.		RFC 2236 IGMP v2	EXIGIDO	Soportado	Si Cumple
128.		RFC 3376 IGMP v3	EXIGIDO	Soportado	Si Cumple
129.		RFC 1075 DVMRP	EXIGIDO	Soportado	Si Cumple
130.		RFC 1492 TACACS+	EXIGIDO	Soportado	Si Cumple
131.		RFC 2138 RADIUS Authentication	EXIGIDO	Soportado	Si Cumple
132.		RFC 2139 RADIUS Accounting	EXIGIDO	Soportado	Si Cumple
133.		RFC 3579 RADIUS EAP support for 802.1x	EXIGIDO	Soportado	Si Cumple
134.		RFC 5176 Dynamic Authorization Extensions to RADIUS	EXIGIDO	Soportado	Si Cumple
135.		RFC 2267 Network Ingress Filtering	EXIGIDO	Soportado	Si Cumple
136.		RFC 2030 SNTP, Simple Network Time Protocol	EXIGIDO	Soportado	Si Cumple
137.		RFC 854 Telnet client and server	EXIGIDO	Soportado	Si Cumple
138.		RFC 951, 1542 BootP	EXIGIDO	Soportado	Si Cumple
139.		RFC 2131 BOOTP/DHCP relay agent and DHCP server	EXIGIDO	Soportado	Si Cumple
140.		RFC 1591 DNS	EXIGIDO	Soportado	Si Cumple
141.		RFC 2338 VRRP	EXIGIDO	Soportado	Si Cumple
142.		RFC 2328 OSPF v2 (Edge-mode)	EXIGIDO	Soportado	Si Cumple
143.		RFC 1587 OSPF NSSA Option	EXIGIDO	Soportado	Si Cumple
144.		RFC 1765 OSPF Database Overflow	EXIGIDO	Soportado	Si Cumple
145.		RFC 2154 OSPF w/Digital Signatures (Password, MD-5)	EXIGIDO	Soportado	Si Cumple
146.		RFC 2370 OSPF Opaque LSA Option	EXIGIDO	Soportado	Si Cumple
147.		RFC 3623 OSPF Graceful Restart	EXIGIDO	Soportado	Si Cumple
148.		RFC 2362 PIM-SM (Edge-mode)	EXIGIDO	Soportado	Si Cumple
149.		RFC 3569 draft-ietf-ssm-arch-06.txt PIM-SSM PIM Source Specific Multicast	EXIGIDO	Soportado	Si Cumple
150.		RFC 1771 Border Gateway Protocol 4	EXIGIDO	Soportado	Si Cumple
151.		RFC 1965 Autonomous System Confederations for BGP	EXIGIDO	Soportado	Si Cumple
152.		RFC 2796 BGP Route Reflection (supersedes RFC 1966)	EXIGIDO	Soportado	Si Cumple
153.		RFC 1997 BGP Communities Attribute	EXIGIDO	Soportado	Si Cumple
154.		RFC 1745 BGP4/IDRP for IP-OSPF Interaction	EXIGIDO	Soportado	Si Cumple
155.		RFC 2385 TCP MD5 Authentication for BGPv4	EXIGIDO	Soportado	Si Cumple
156.		RFC 2439 BGP Route Flap Damping	EXIGIDO	Soportado	Si Cumple
157.		RFC 2918 Route Refresh Capability for BGP-4	EXIGIDO	Soportado	Si Cumple
158.		RFC 3392 Capabilities Advertisement with BGP-4	EXIGIDO	Soportado	Si Cumple
159.		RFC 2796 Route Reflection	EXIGIDO	Soportado	Si Cumple
160.		RFC 4360 BGP Extended Communities Attribute	EXIGIDO	Soportado	Si Cumple
161.		RFC 4486 Subcodes for BGP Cease Notification message	EXIGIDO	Soportado	Si Cumple
162.		RFC 1195 Use of OSI IS-IS for Routing in TCP/IP and Dual Environments (TCP/IP transport only)	EXIGIDO	Soportado	Si Cumple
163.		RFC 2474 DiffServ Precedence	EXIGIDO	Soportado	Si Cumple
164.		RFC 2598 DiffServ Expedited Forwarding (EF)	EXIGIDO	Soportado	Si Cumple
165.		RFC 2597 DiffServ Assured Forwarding (AF)	EXIGIDO	Soportado	Si Cumple
166.		RFC 2475 DiffServ Core and Edge Router Functions	EXIGIDO	Soportado	Si Cumple
167.		RFC 3619 Ethernet Automatic Protection Switching (EAPS) and EAPSv2	EXIGIDO	Soportado	Si Cumple
168.		LLDP Media Endpoint Discovery (LLDP-MED), ANSI/TIA-1057, draft 08	EXIGIDO	Soportado	Si Cumple
169.	STACKING	Las soluciones basadas en el formato "Stacking" deberán cumplir con los siguientes requerimientos:	EXIGIDO	Soportado	Si Cumple
170.		Vinculación de equipos por puertos de uso exclusivo para Stack excluyendo las interfaces de RED	EXIGIDO	Soportado	Si Cumple
171.		Configuración desde una única dirección IP y para su administración actuarán como un único equipo.	EXIGIDO	Soportado	Si Cumple
172.		Capacidad mínima de backplane del Stack utilizando los puertos específicas de stacking expresado en bandwidth full-duplex	40Gbps	64 Gbps	Si Cumple
173.		El reemplazo de un miembro del stack deberá ser no	EXIGIDO	Soportado	Si Cumple

CASILDO S. MIRANDA M.
Técnico
Redes y Comunicaciones

VICTOR D. VILLALBA
Jefe Sección Redes

		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.			
174.		Mínimo de equipos agrupados para administrar con un único acceso administrativo	10	10	Si Cumple
175.		Los puertos de LAG deben poder pertenecer a diferentes miembros del Stack	EXIGIDO	Soportado	Si Cumple

ITEM 3 –FIREWALL DE CORE

Marca:Fortinet

Modelo: Fortigate 800C

ITEM	CARACTERISTICAS		MINIMO EXIGIDO	Evaluación	
				Ofertado	**CUMPLE SI/NO**
1.	GENERALIDADES	La función de este equipo será la de proteger el Data Center. Para ello se requiere que cuente con funcionalidades de seguridad, análisis e inspección de contenido a nivel inclusive de las capas superiores. A fin de permitir una mayor participación de oferentes, serán aceptadas soluciones que distribuyan las diferentes funciones seguridad, en equipos separados, siempre y cuando la solución como conjunto cumpla con los requerimientos mínimos exigidos para este ítem.	EXIGIDO	*Marca:Fortinet* *Modelo: Fortigate 800C*	Si Cumple
2.	RENDIMIENTO Y CAPACIDAD	Performance Firewall Troughput en paquetes de 64 bytes	18 Gbps	20 Gbps	Si Cumple
3.		Sesiones Concurrentes soportadas	6.500.000	7.000.000	Si Cumple
4.		Nuevas sesiones por segundo	185.000	190.000	Si Cumple
5.		Cantidad de Políticas de Seguridad	10.000	10.000	Si Cumple
6.	CONECTIVIDAD DE RED	Cantidad de puertos 10/100/1000Base-T – Configurables como WAN, LAN o DMZ	10	12	Si Cumple
7.		Cantidad de slots SFP para interfaces 1000BaseX.	8	8	Si Cumple
8.		Cantidad de slots SFP+ para interfaces 10GBaseX (10 GbE).	2	2	Si Cumple
9.		Cantidad de módulos 10 GbE SR (corta distancia sobre fibra multimodo) a ser provistos	2	2	Si Cumple
10.		Puertos USB 2.0	1	1	Si Cumple
11.	ROUTING	BGP	EXIGIDO	Soportado	Si Cumple
12.		OSPF	EXIGIDO	Soportado	Si Cumple
13.		RIP v1/v2	EXIGIDO	Soportado	Si Cumple
14.		Soporte a ruteo de multicast	EXIGIDO	Soportado	Si Cumple
15.		Soporte a ruteo estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas	EXIGIDO	Soportado	Si Cumple
16.		Soporte a políticas de ruteo (policy routing)	EXIGIDO	Soportado	Si Cumple
17.		Soporte a ruteo dinámico RIPng, OSPFv3	EXIGIDO	Soportado	Si Cumple
18.		Soporte de ECMP (Equal Cost Multi-Path)	EXIGIDO	Soportado	Si Cumple
19.	AUTENTICACION DE USUARIOS Y CONTROL DE ACCESO	Capacidad de integrarse con Servidores de Autenticación RADIUS	EXIGIDO	Soportado	Si Cumple
20.		Capacidad nativa de integrarse con directorios LDAP	EXIGIDO	Soportado	Si Cumple
21.		Soporte a inclusión en autoridades certificadoras (enrollment) mediante SCEP (Simple Certificate Enrollment Protocol) y mediante archivos.	EXIGIDO	Soportado	Si Cumple
22.	TRADUCCION DE DIRECCIONES	NAT	EXIGIDO	Soportado	Si Cumple
23.		PAT	EXIGIDO	Soportado	Si Cumple
24.		NAT estático	EXIGIDO	Soportado	Si Cumple
25.		NAT con PAT	EXIGIDO	Soportado	Si Cumple
26.	ASIGNACION DE DIRECCIONES IP	Cliente DHCP	EXIGIDO	Soportado	Si Cumple
27.		Servidor DHCP	EXIGIDO	Soportado	Si Cumple
28.		DHCP Relay	EXIGIDO	Soportado	Si Cumple
29.	CONMUTACION EN LAYER 2	Soporte de VLAN 802.1Q	4000	4096	Si Cumple
30.		Soporte de Link Aggregation Group (802.3ad) con un mínimo de 4 interfaces por grupo	EXIGIDO	Soportado	Si Cumple
31.		Soporte a etiquetas de VLAN (802.1q) y creación de zonas de seguridad en base a VLANs	EXIGIDO	Soportado	Si Cumple
32.	ADMINISTRACION DE TRAFICO Y CALIDAD DE SERVICIO (QoS)	Capacidad de poder asignar parámetros de traffic shapping sobre reglas de firewall	EXIGIDO	Soportado	Si Cumple
33.		Capacidad de poder definir ancho de banda	EXIGIDO	Soportado	Si Cumple

CASILDO S. MIRANDA
Técnico
Redes y Comunicaciones

VICTOR D. VILLALBA
Jefe Sección Redes

		garantizado en KiloBytes por segundo			
34.		Capacidad de poder definir límite de ancho de banda (ancho de banda máximo) en KiloBytes por segundo	EXIGIDO	Soportado	Si Cumple
35.		Capacidad para definir prioridad de tráfico, en al menos tres niveles de importancia	EXIGIDO	Soportado	Si Cumple
36.		Capacidad de poder asignar parámetros de traffic shaping diferenciadas para el tráfico en distintos sentidos de una misma sesión	EXIGIDO	Soportado	Si Cumple
37.		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	Soportado	Si Cumple
38.	ALTA DISPONIBILIDAD	Soporte de Alta Disponibilidad en modo transparente, es decir, sin pérdida de conexiones en caso de que un nodo falle.	EXIGIDO	Soportado	Si Cumple
39.		Soporte de Alta Disponibilidad en modo Activo-Activo	EXIGIDO	Soportado	Si Cumple
40.		Soporte de Alta Disponibilidad en modo Activo-Pasivo	EXIGIDO	Soportado	Si Cumple
41.		Posibilidad de definir al menos dos interfaces para sincronía para Alta Disponibilidad de forma a evitar el uso de Multicast en la red	EXIGIDO	Soportado	Si Cumple
42.	CONTROL DE APLICACIONES	El equipo deberá poseer prestaciones de Control de Aplicaciones.	EXIGIDO	Soportado	Si Cumple
43.		Lo solución debe soportar la capacidad de identificar la aplicación que origina cierto tráfico a partir de la inspección del mismo	EXIGIDO	Soportado	Si Cumple
44.		La identificación de la aplicación debe ser independiente del puerto y protocolo hacia el cual esté direccionado dicho tráfico	EXIGIDO	Soportado	Si Cumple
45.		Las solución debe tener un listado de al menos 1000 aplicaciones ya definidas por el fabricante	EXIGIDO	Soportado	Si Cumple
46.		El listado de aplicaciones debe actualizarse periódicamente	EXIGIDO	Soportado	Si Cumple
47.		Para aplicaciones identificadas deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log	EXIGIDO	Soportado	Si Cumple
48.		Para aplicaciones no identificadas (desconocidas) deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log	EXIGIDO	Soportado	Si Cumple
49.		Para aplicaciones de tipo P2P debe poder definirse adicionalmente políticas de traffic shaping	EXIGIDO	Soportado	Si Cumple
50.		Preferentemente deben soportar mayor granularidad en las acciones	EXIGIDO	Soportado	Si Cumple
51.	INSPECCION DE CONTENIDO – IDS/IPS	El equipo deberá poseer prestaciones de IDS/IPS	EXIGIDO	Soportado	Si Cumple
52.		Performance Inspeccion IPS	5.5 Gbps	6 Gbps	Si Cumple
53.		El Detector y preventor de intrusos deberá de estar orientado para la protección de redes	EXIGIDO	Soportado	Si Cumple
54.		El Detector y preventor de intrusos deben poder implementarse tanto en línea como fuera de linea. 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	Soportado	Si Cumple
55.		El detector y preventor de intrusos podrá implementarse en linea y fuera de linea en forma simultánea para distintos segmentos.	EXIGIDO	Soportado	Si Cumple
56.		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	Soportado	Si Cumple
57.		Deberá soportar captar ataques por Anomalía (Anomaly detection).	EXIGIDO	Soportado	Si Cumple
58.		Deberá soportar captar ataques basado en análisis de firmas en el flujo de datos en la red (signature based / misuse detection).	EXIGIDO	Soportado	Si Cumple
59.		Deberá permitir configurar firmas nuevas para cualquier protocolo.	EXIGIDO	Soportado	Si Cumple
60.		Deberá poseer una tecnología de detección tipo Stateful basada en Firmas (signatures).	EXIGIDO	Soportado	Si Cumple
61.		Deberá soportar la actualización automática de firmas para el detector de intrusos (por 3 años)	EXIGIDO	Soportado	Si Cumple
62.		El Detector de Intrusos deberá mitigar los efectos de los ataques de negación de servicios	EXIGIDO	Soportado	Si Cumple
63.		Deberá contar con mecanismos de deteccion de ataques basados en Reconocimiento de patrones y Análisis de protocolos.	EXIGIDO	Soportado	Si Cumple
64.		Deberá contar con mecanismos de deteccion de	EXIGIDO	Soportado	Si Cumple

CASILDO S. MIRANDA M.
Técnico
Redes y Comunicaciones

HECTOR D. VILLALBA
Jefe Sección Redes

		ataques basados en Detección de anomalías.			
65.		Deberá contar con mecanismos de deteccion de ataques basados en Detección de ataques de RPC (Remote procedure call)	EXIGIDO	Soportado	Si Cumple
66.		Deberá contar con mecanismos de Protección contra ataques de Windows o NetBios	EXIGIDO	Soportado	Si Cumple
67.		Deberá contar con mecanismos de Protección contra ataques de SMTP, IMAP o POP.	EXIGIDO	Soportado	Si Cumple
68.		Deberá contar con mecanismos de Protección contra ataques DNS.	EXIGIDO	Soportado	Si Cumple
69.		Deberá contar con mecanismos de Protección contra ataques a FTP, SSH y Telnet.	EXIGIDO	Soportado	Si Cumple
70.		Deberá contar con mecanismos de Protección contra ataques de ICMP.	EXIGIDO	Soportado	Si Cumple
71.		Deberá contar con Alarmas mostradas en la consola de administración del equipo.	EXIGIDO	Soportado	Si Cumple
72.		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	Soportado	Si Cumple
73.	INSPECCION DE CONTENIDO – FILTRADO DE URL	El equipo poseer prestaciones de Filtrado de Páginas Web (URL Filtering).	EXIGIDO	Soportado	Si Cumple
74.		El equipo deberá poseer la capacidad de trabajar como un Proxy Cache	EXIGIDO	Soportado	Si Cumple
75.		Capacidad mínima de almacenamiento interno.	64 GB	64 GB	Si Cumple
76.		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	Soportado	Si Cumple
77.		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	Soportado	Si Cumple
78.		Configurable directamente desde la interfaz de administración del dispositivo. Con capacidad para permitir esta protección por política de control de acceso.	EXIGIDO	Soportado	Si Cumple
79.		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	Soportado	Si Cumple
80.		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	Soportado	Si Cumple
81.		Capacidad de filtrado de scripts en páginas web (JAVA/Active X).	EXIGIDO	Soportado	Si Cumple
82.	INSPECCION DE CONTENIDO – ANTISPAM	El equipo poseer prestaciones de Antispam.	EXIGIDO	Soportado	Si Cumple
83.		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	Soportado	Si Cumple
84.		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	Soportado	Si Cumple
85.		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	Soportado	Si Cumple
86.		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 en el motivo (subject) del mensaje o a través un encabezado MIME en el mensaje.	EXIGIDO	Soportado	Si Cumple
87.	ADMINISTRACION	Soporte de Interfaz CLI	EXIGIDO	Soportado	Si Cumple
88.		Soporte de Interfaz WEB (HTTP y HTTPS)	EXIGIDO	Soportado	Si Cumple
89.		Puerto serial dedicado para administración.	EXIGIDO	Soportado	Si Cumple

CASILDO S. MIRANDA M.
Técnico
Redes y Comunicaciones

VICTOR D. VILLALBA
Jefe Sección Redes

90.		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	Soportado	Si Cumple
91.		Los administradores podrán tener asignado un perfil de administración que permita delimitar las funciones del equipo que pueden gerenciar y afectar.	EXIGIDO	Soportado	Si Cumple
92.		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	Soportado	Si Cumple
93.		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	Soportado	Si Cumple
94.		Soporte de SNMP versión 2	EXIGIDO	Soportado	Si Cumple
95.		Soporte de servidores syslog para poder enviar bitácoras a servidores de SYSLOG remotos	EXIGIDO	Soportado	Si Cumple
96.	ALIMENTACION ELECTRICA Y DIMENSIONES	Tensión de operación	Alterna, 220VCA	Soportado	Si Cumple
97.		Deberá contar con la posibilidad de agregar una fuente de poder secundaria para redundancia.	EXIGIDO	Soportado	Si Cumple
98.		MTBF Mínimo Requerido	50.000 Hs.	51.840 Hs.	Si Cumple
99.		Montaje en rack de 19"	EXIGIDO	Soportado	Si Cumple

ITEM 4 – BALANCEADOR

Marca: Brocade

Modelo:ADX SI-1216

Nº	CARACTERISTICAS		MINIMO EXIGIDO	**Ofertado** *Marca: Brocade* *Modelo:ADX SI-1216*	**CUMPLE SI/NO**
1.	RENDIMIENTOYCAPACIDAD	Performance mínima en Layer 7	9 Gbps	9 Gbps	Si Cumple
		Cantidad mínima de Transacciones por Segundo.	2.500.000	2.500.000	Si Cumple
		Cantidad mínima de Conexiones por segundo	375.000	375.000	Si Cumple
		Cantidad mínima de Conexiones Concurrentes	16.000.000	16.000.000	Si Cumple
		Cantidad mínima de Transacciones SSL por Segundo.	25.000	29.000	Si Cumple
		Cantidad mínima de Conexiones SSL por segundo	6.000	6.500	Si Cumple
		Cantidad mínima de Sesiones Concurrentes	32.000.000	32.000.000	Si Cumple
		Latencia mínima de PaquetSwitching, en microsegundos	20 µs	20 µs	Si Cumple
		Cantidad mínima de Request DNS por segundo en modo stateless	2.250.000	2.250.000	Si Cumple
		Cantidad mínima de Request DNS por segundo en modo stateful	550.000	550.000	Si Cumple
		Capacidad mínima de protección de ataques SYN (en ataques por segundo)	15.000.000	15.000.000	Si Cumple
		Capacidad mínima de protección de ataques DDoS (en paquetes por segundo)	15.000.000	15.000.000	Si Cumple
		Cantidad mínima de VIP (Virtual IP) soportadas	1.024	1.024	Si Cumple
		Cantidad mínima de Servidores Reales soportados	4.096	4.096	Si Cumple
		Cantidad Mínima de interfaces 1000Base-T soportadas	16	16	Si Cumple
2.	CONECTIVIDADDERED	Cantidad Mínima de interfaces 10 GbE instaladas	2	2	Si Cumple

CASILDO S. MIRAN
Técnico
Redes y Comunicaciones

VICTOR D. VILLALBA
Jefe Sección Redes

		Cantidad mínima de puertos USB para almacenamiento externo	1	1	Si Cumple
		Cantidad mínima de puertos SERIAL RS-232 para ser usado como consola de administración.	1	1	Si Cumple
		Soporte de 802.1q VlanTagging	SI	Soportado	Si Cumple
3.	CONMUTACIONENLAYER 2	Mínimo de direcciones MAC	16.000	Soportado	Si Cumple
		Soporte de 802.1D SpanningTreeProtocol	EXIGIDO	Soportado	Si Cumple
		Soporte de 802.1w Rapid Spanning Tree	EXIGIDO	Soportado	Si Cumple
		BGP	EXIGIDO	Soportado	Si Cumple
4.	ROUTING	OSPF	EXIGIDO	Soportado	Si Cumple
		RIPv2	EXIGIDO	Soportado	Si Cumple
		ISIS	EXIGIDO	Soportado	Si Cumple
		Ruteo estático.	EXIGIDO	Soportado	Si Cumple
		Ruteo entre Vlans	EXIGIDO	Soportado	Si Cumple
		Soporte de IPv6	EXIGIDO	Soportado	Si Cumple
		Soporte de IPv6 NAT64	EXIGIDO	Soportado	Si Cumple
		El equipo propuesto deberá de contar con funcionalidades para la distribución de cargas basado en servicios de IP entre múltiples servidores, al mismo tiempo deberá de contar con mecanismos para inspeccionar el estado de las aplicaciones, esto con el fin de proporcionar alta disponibilidad a las mismas.	EXIGIDO	Soportado	Si Cumple
5.	FUNCIONES DE BALANCEO DE CARGA	Deberá de contar con funcionalidades de Balanceo de cargas basado en el encabezado de HTTP	EXIGIDO	Soportado	Si Cumple
		Deberá de contar con funcionalidades de Balanceo de cargas basado en contenido de XML	EXIGIDO	Soportado	Si Cumple
		Deberá de contar con Soporte para redirecciones peticiones a URL o dominios alternos.	EXIGIDO	Soportado	Si Cumple
		Deberá de contar con Soporte de funciones de re-escrituración, borrado e inserción de encabezados de HTTP y Cookies, así como persistencia de sesiones tanto de capa 4 como en capa 7.	EXIGIDO	Soportado	Si Cumple
		Balanceo Global – deberá de soportar funcionalidades de balanceo global geográfico, mediante licenciamiento, para esquemas de recuperación de desastres mediante la redirección transparente de las peticiones de los usuarios a diferentes sitios geográficamente dispersos.	EXIGIDO	Soportado	Si Cumple
		Inspección de L7 – deberá de contar con inspección de aplicativos a nivel de capa 7, con el fin de optimizar y escalar las aplicaciones.	EXIGIDO	Soportado	Si Cumple
		SIP – deberá de soportar el balanceo de servidores de	EXIGIDO	Soportado	Si Cumple

CASILDO S. MIRANDA M.
Técnico
Redes y Comunicaciones

VICTOR D. VILLALBA
Jefe Sección Redes

		SIP.			
		Balanceo de Caches – se requiere de una solución capaz de redireccionar paquetes de manera transparente hacia servidores de Cache (Proxy).	EXIGIDO	Soportado	Si Cumple
		El equipo deberá de soportar un mínimo de 1024 servicios virtuales, de un mínimo de 4096 servidores a ser balanceados y de 8192 servicios (puertos) a ser balanceados.	EXIGIDO	1024 Virtual Server 4096 Servidores Reales 8192 Máximo de Puertos	Si Cumple
		Deberá soportar la agregación de interfaces para formar un único link, esta técnica es conocida como LAG (Link AggregationGroup).	EXIGIDO	Soportado	Si Cumple
6.	ALTADISPONIBILIDAD	El equipo deberá de poder ser colocado en la infraestructura de la red mediante esquemas de alta disponibilidad tanto activo/activo, como activo/pasivo soportando "statefulfailover".	EXIGIDO	Soportado	Si Cumple
		Soporte de VRRP/VRRP-E	EXIGIDO	Soportado	Si Cumple
		El equipo deberá de contar con soporte de procesamiento de listas de control de acceso a velocidad de cable.	EXIGIDO	Soportado	Si Cumple
7.	SEGURIDAD	Deberá de proveer de seguridad contra ataques de negación de servicios y ataques de negación de servicios distribuidos.	EXIGIDO	Soportado	Si Cumple
		Deberá de contar con administración vía una línea de comandos mediante un puerto serial. Asimismo deberá de soportar administración vía SSH, Telnet y Web GUI.	EXIGIDO	Soportado	Si Cumple
8.	ADMINISTRACION	La interface de administración grafica deberá de ser basada en páginas de Web y deberá de residir en el dispositivo ofertado.	EXIGIDO	Soportado	Si Cumple
		Las funcionalidades mínimas con las que deberá de contar la interface de administración se muestran a continuación: • Administración Vlans y enrutamiento (Capas 2 y 3) • Balanceo de servidores en capa 4 • Políticas de balanceo de carca a nivel de l7 • Funciones de monitoreo y estadísticas de trafico Administración de certificados digitales para el balanceo de aplicaciones de SSL (Vía licenciamiento).	EXIGIDO	Soportado	Si Cumple
		Deberá soportar los siguientes Mecanismos de balanceo de carga: • Tiempo de respuesta • Round Robin • Ancho de banda • Mínimo número de conexiones • Distribución por pesos	EXIGIDO	Soportado	Si Cumple
		• Tensión de operación	Alterna, 220VCA		Si Cumple
9.	ALIMENTACIONELECTRICA. DIMENSIONES Y CONDICIONES	El equipo deberá de contar con fuentes de poder redundantes internas. Estas fuentes de poder deberán de poder ser intercambiables sin interrumpir la	EXIGIDO	Soportado	Si Cumple

CASILDO S. MIRANDA M.
Técnico
Redes y Comunicaciones

VICTOR D. VILLALBA
Jefe Sección Redes

	AMBIENTALES	operación del equipo.			
		Las fuentes de poder no deberán de exceder un consumo de 400 Watts por fuente de poder.	EXIGIDO	390 Watts.	Si Cumple
		Montaje en rack de 19"	EXIGIDO	Soportado	Si Cumple
		Temperatura en Operación	De 0 °C a 40 °C	0º a 40º C	Si Cumple
		Humedad Relativa en Operación a 40 °C	De 5 a 90%	5 a 90 %	Si Cumple
		Temperatura en Almacenamiento	De -25 °C a 70 °C	-25º a 70º C	Si Cumple
		Humedad Relativa en Almacenamiento	Max: 95%	95%	Si Cumple
		802.3 10BaseT	EXIGIDO	Soportado	Si Cumple
10.	NORMASYESTANDARES	802.3u 100BaseTX,100BaseFX	EXIGIDO	Soportado	Si Cumple
		802.3ae 10GbE	EXIGIDO	Soportado	Si Cumple
		802.1q VLAN Tagging	EXIGIDO	Soportado	Si Cumple
		802.1d Bridging	EXIGIDO	Soportado	Si Cumple
		802.1w RSTP	EXIGIDO	Soportado	Si Cumple
		802.1ad Link Aggregation	EXIGIDO	Soportado	Si Cumple
		SNMPV2	EXIGIDO	Soportado	Si Cumple
		EN 60950-1:2001	EXIGIDO	Soportado	Si Cumple
		IEC 60950-1:2001	EXIGIDO	Soportado	Si Cumple
		EN 60825-1:1994	EXIGIDO	Soportado	Si Cumple
		UL 60950-1	EXIGIDO	Soportado	Si Cumple
		FCC Part 15, Subpart B (Class A)	EXIGIDO	Soportado	Si Cumple
		EN 55022	EXIGIDO	Soportado	Si Cumple
		EN 61000-3-2	EXIGIDO	Soportado	Si Cumple
		EN 61000-3-3	EXIGIDO	Soportado	Si Cumple
		EN 61000-6-1	EXIGIDO	Soportado	Si Cumple
		EN55024	EXIGIDO	Soportado	Si Cumple
		ICES-003	EXIGIDO	Soportado	Si Cumple
		AS/NZ 55022	EXIGIDO	Soportado	Si Cumple
		VCCI	EXIGIDO	Soportado	Si Cumple

CASILDO S. MIRANDA M.
Técnico
Redes y Comunicaciones

ITEM 5– WEB FIREWALL

Marca: Fortinet

Modelo: FortiWeb 400C

Nº	CARACTERISTICAS		MINIMO EXIGIDO	Ofertado Marca: Fortinet Modelo: FortiWeb 400C	CUMPLE SI/NO
1.	CARACTERISTICAS GENERALES	Interfaces Ethernet 10/100/1000 Mbps	4	4	Si Cumple
		Capacidad mínima de procesamiento de paquetes HTTP	100 Mbps	100 Mbps	Si Cumple
		Capacidad mínima de transacciones HTTP por	10.000	10.000	Si Cumple

VICTOR D. VILLALBA
Sección Redes

		segundo			
		Capacidad mínima de disco duro (almacenamiento) incluido	1 TB	1 TB	Si Cumple
		Capacidad mínima de Servidores Web controlados.	10	10	Si Cumple
		Capacidad mínima de Portales Web controlados.	10	10	Si Cumple
		La plataforma deberá tener la capacidad de trabajar en un esquema de Alta Disponibilidad en formato Activo-Pasivo	EXIGIDO	Soportado	Si Cumple
		La plataforma deberá ser tipo "appliance" de propósito específico. No se aceptan dispositivos de propósito genérico y/o con sistemas operativos genéricos.	EXIGIDO	Applicance	Si Cumple
2.	FUNCIONALIDADES	El sistema debe funcionar como Proxy reverso	EXIGIDO	Soportado	Si Cumple
		El sistema deberá permitir su implementación en modo Transparente	EXIGIDO	Soportado	Si Cumple
		El sistema deberá permitir su implementación en modo Offline (conectado a un puerto en modo sniffer/span)	EXIGIDO	Soportado	Si Cumple
		El sistema deberá soportar el Auto-Aprendizaje de perfiles de seguridad. Es decir que permita hacer el descubrimiento de la estructura y patrones de uso de las aplicaciones Web para ser protegidas.	EXIGIDO	Soportado	Si Cumple
		El sistema deberá permitir habilitar la detección, alertas y bloqueo de ataques reconocidos en las aplicaciones Web, tales como: SQL Injection, Cross Site Scripting, CSRF, etc.	EXIGIDO	Soportado	Si Cumple
		El sistema deberá tener la capacidad de proteger contra Ataques de Denegación de Servicio sobre HTTP	EXIGIDO	Soportado	Si Cumple
		El sistema debe permitir hacer Validación de esquemas WSDL para XML	EXIGIDO	Soportado	Si Cumple
		El sistema deberá soportar la Funcionalidad de Inspección para XML	EXIGIDO	Soportado	Si Cumple
		El sistema deberá poseer la Capacidad de aplicar firmas de ataques conocidos para HTTP	EXIGIDO	Soportado	Si Cumple
		El sistema deberá poseer la Capacidad de hacer encaminamiento para Protocolo HTTP	EXIGIDO	Soportado	Si Cumple
		El sistema deberá proteger con las siguientes amenazas Web: - Cross site scripting - SQL injection - Session hijacking - Cookie tampering/poisoning - Cross site request forgery - Command injection - Remote file inclusion - Forms tampering - Hidden field manipulation - Outbound data leakage - HTTP request smuggling - Encoding attacks - Broken access control - Forceful browsing - Directory traversal - Site reconnaissance - Search engine hacking - Brute force login - Access rate control - Schema poisoning - XML parameter tampering - XML intrusion prevention - WSDL scanning - Recursive payload - External entity attack - Buffer overflows - Denial of service	EXIGIDO	Soportado	Si Cumple
		El sistema deberá ser el encargado del manejo de los certificados digitales para todas las aplicaciones de tipo https de la institución	EXIGIDO	Soportado	Si Cumple
		El sistema deberá poseer la capacidad de hacer load balancing para los servidores de aplicaciones y servidores Web	EXIGIDO	Soportado	Si Cumple
		El sistema deberá poseer la capacidad de acelerar las aplicaciones Web.	EXIGIDO	Soportado	Si Cumple
		El sistema deberá poseer la funcionalidad de URL	EXIGIDO	Soportado	Si Cumple

CASILDO S. MIRANDA M.
Técnico
Redes y Comunicaciones

VICTOR D. VILLALBA
Jefe Sección Redes

		Black/White List, para inspeccionar o bloquear peticiones a URLs específicos			
		El sistema deberá poseer la funcionalidad de URL Black/White List, para inspeccionar o bloquear tráfico desde direcciones IP específicas	EXIGIDO	Soportado	Si Cumple
		El sistema deberá incluir un Sensor para Control de Robots	EXIGIDO	Soportado	Si Cumple
		El sistema deberá permitir los siguientes algoritmos de Balanceo para Servidores: a) Weighted Round Robing b) LeastConnection c) LeastTraffic d) Response Time	EXIGIDO	Soportado	Si Cumple
		El sistema deberá soportar los siguientes métodos de HealthCheck: a) Ping b) TCP c) HTTP	EXIGIDO	Soportado	Si Cumple
3.	ADMINISTRACION	El sistema deberá soportar administración a través de GUI (HTTPS y HTTP), CLI (Telnet, SSH), etc.	EXIGIDO	Soportado	Si Cumple
		El sistema deberá contar con un puerto de consola serial para su administración por CLI	EXIGIDO		Si Cumple
		El sistema deberá poseer Soporte de SNMP	EXIGIDO	Soportado	Si Cumple
		Deberá de soportar diferentes niveles de acceso y permisos a la administración, de modo que se pueda dar acceso a usuarios de administrador, reportes,o sólo lectura, etc.	EXIGIDO	Soportado	Si Cumple
		Deberá permitir la descarga de Backups de configuración, desde el GUI, TFTP	EXIGIDO	Soportado	Si Cumple
		Deberá soportar Actualización de Firmware por TFTP y GUI	EXIGIDO	Soportado	Si Cumple
		El administrador del sistema podrá tener las opciones incluías de autenticarse vía password y vía certificados digitales	EXIGIDO	Soportado	Si Cumple
		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	Soportado	Si Cumple
		El equipo deberá poder administrarse en su totalidad (incluyendo funciones de seguridad, Balanceo y bitácoras) desde cualquier equipo conectado a Internet que tenga un browser (Internet Explorer, Mozilla, Firefox) instalado sin necesidad de instalación de ningún software adicional	EXIGIDO	Soportado	Si Cumple
		El sistema deberá poseer la capacidad de alertar/notificar en tiempo real al administrador ante la ocurrencia de un ataque por medio de la consola de gestión.	EXIGIDO	Soportado	Si Cumple
		El sistema deberá soportar la generación de alarmas de Eventos	EXIGIDO	Soportado	Si Cumple
		El sistema deberá permitir enviar notificaciones vía correo electrónico	EXIGIDO	Soportado	Si Cumple
4.	ALIMENTACIONELECTRICA YDIMENSIONES	Tensión de operación	Alterna, 220VCA		Si Cumple
		La fuente de poder deberá ser integrada al equipo. No serán aceptados equipos que posean fuente externa o transformadores..	EXIGIDO	Soportado	Si Cumple
		Montaje en rackde 19"	EXIGIDO	Soportado	Si Cumple

CASILDO S. MIRANDA M.
Técnico
Redes y Comunicaciones

ITEM 6 – ANALIZADOR DE SEGURIDAD

Marca: Fortinet

Modelo: FortiAnalyzer 200D

Nº	CARACTERISTICAS		MINIMOEXIGIDO	Ofertado *Marca: Fortinet* *Modelo: FortiAnalyzer 200D*	CUMPLE SI/NO
	RENDIMIENTO, CAPACIDAD Y CONECTIVIDAD	Capacidad mínima de recepción de reportes por día, en GigaBytes.	5 GB	5	Si Cumple
		Cantidad mínima de sesiones por día soportadas.	18,000.000	18.000.000	Si Cumple
		Cantidad mínima de interfaces Gigabit Ethernet 10/100/1000Base-T	4	4	Si Cumple
		Cantidad mínima de dispositivos de seguridad que	150	150	Si Cumple

VICTOR D. VILLALBA
Jefe Sección Redes

		pueden enviar registros			
		Capacidad mínima de almacenamiento	1 TB	1 TB	Si Cumple
2.	ADMINISTRACION	Soporte de Interfaz CLI (Telnet, SSHv2 y Puerto Serial)	EXIGIDO	Soportado	Si Cumple
		Soporte de Interfaz WEB (HTTP y HTTPS)	EXIGIDO	Soportado	Si Cumple
		Debe tener la posibilidad de definir administradores para la solución, de modo que pueda segmentarse la responsabilidad de los administradores por tareas operativas	EXIGIDO	Soportado	Si Cumple
		Debe tener la capacidad de poder integrar dispositivos de seguridad para que le reporten, y establecer comunicaciones seguras con dichos dispositivos	EXIGIDO	Soportado	Si Cumple
		Debe tener la capacidad de asignar cuotas de espacio en disco por dispositivo, de modo que un solo dispositivo no consuma la totalidad del disco de la solución	EXIGIDO	Soportado	Si Cumple
3.	ANALISIS FORENSE, CORRELACION Y ANALISIS DE VULNERABILIDADES	Debe ser capaz de hacer correlación de la información almacenada. Esto es, identificar patrones y/ o tendencias en la información almacenada	EXIGIDO	Soportado	Si Cumple
		Debe ser capaz de hacer búsquedas por username o dirección IP, paraquetodalainformaciónalmacenadadedichousernameodirecciónIPseamostradaenunreportedondepuedadarseseguimientoasuactividad	EXIGIDO	Soportado	Si Cumple
		Debe poseer (integrado o por separado) la capacidad de hacer análisis de vulnerabilidades en la red, mediante plug-ins de ataques actualizables, ygenerarunreportedecuálesvulnerabilidadesfueronencontradasenlared	EXIGIDO	Soportado	Si Cumple
4.	CUARENTENA	Debepoderrecibirarchivosdedispositivosomecanismosantiviruscompatiblesconlafinalidaddeusarelespacioendiscocomoespacioparacuarentena	EXIGIDO	Soportado	Si Cumple
		Debepoderrecibirarchivosdedispositivosomecanismosantispamcompatiblesconlafinalidaddeusarelespacioendiscocomoespacioparacuarentena	EXIGIDO	Soportado	Si Cumple
5.	ALMACENAMIENTO DE CONTENIDO	Debe ser capaz de recibir bitácoras de los protocolos http, SMTP y messengers (Yahoo, MSN) parapoderalmacenarlosmensajesquehayanfluidoenlaredatravésdedichosprotocolos, para su posterior visualización	EXIGIDO	Soportado	Si Cumple
		Los mensajes deberán poder ser almacenados completamente, o solo un "resumen" de la conexión. El mensaje completo exhibirá el contenido completo, mientras que el resumen solo mostrará fuente y destino de la comunicación, así como su duración	EXIGIDO	Soportado	Si Cumple
		Debe de ser capaz de hacer búsquedas sobre los mensajes almacenados	EXIGIDO	Soportado	Si Cumple
6.	ALIMENTACIONELECTRICAY DIMENSIONES	Tensión de operación	Alterna, 220VCA	100 240 220 VCA	Si Cumple
		La fuente de poder deberá ser integrada al equipo. No serán aceptados equipos que posean fuente externa o transformadores..	EXIGIDO	220VCA	Si Cumple
		Montaje en rack de 19"	EXIGIDO	220VCA	Si Cumple

Información Adicional

Documentos Requeridos	Cumple Si/NO	Observación
Autorización del Fabricante	**Si Cumple**	-
Técnicos Certificados en todas las marcas ofertadas.	**Si Cumple**	-

VICTOR D. VILLALBA
Jefe Sección Redes

CASILDO S. MIRANDA
Técnico
Redes y Comunicaciones

RECIBIDO
31 MAYO 2014
Exp. No. 3646
08:31

Lic. María Olga Peralta Ch.
Departamento de Programación
y Evaluación de Ofertas