PLEC DE PRESCRIPCIONS TÈCNIQUES PER A L'ADQUISICIÓ DE FIREWALLS PERIMETRALS PER A L'HOSPITAL CLÍNIC DE BARCELONA

Exp. 2023-170

ÍNDEX

1. Objecte i necessitat

L'objecte d'aquest contracte és l'adquisició de dos nous firewalls perimetrals.

L'abast del contracte inclourà elements de hardware, programari, així com serveis de manteniment associats.

La present contractació esdevé necessària per a poder cobrir les necessitats de creixement, rendiment, alta disponibilitat i resposta a contingències i així poder donar un millor servei amb garantia i rapidesa a tots els usuaris de l'Hospital Clinic de Barcelona (en endavant HCB).

2. Descripció del subministrament

La solució a subministrar per l'empresa licitadora inclou el subministrament de hardware i programari. Les empreses licitadores hauran de disposar de la gama de productes, que sigui necessària per a atendre les necessitats de l'HCB.

Les empreses licitadores han d'oferir un conjunt de productes, que aportin les darreres millores tecnològiques del mercat, que siguin escalables i totalment integrables amb l'equipament de transmissió de dades de l'HCB.

2.1 Elements a subministrar

La solució a subministrar per les empreses licitadores inclourà:

- 2 tallafocs per a securitzar el tràfic d'una de les seus de l'HCB.

Aquest equipament ha d'incloure els transceptors de l'electrònica a la que aniran connectats.

En el Formulari que figura a l'Annex 3 del PPT, les licitadores detallaran la relació de productes Hardware i Programari que s'inclouran en el subministrament.

2.2 Característiques tècniques

Els elements a subministrar i els serveis objecte d'aquest contracte hauran de complir amb les característiques tècniques establertes a l'annex 1 d'aquest PPT, el no compliment d'algun dels requisits imprescindibles serà motiu d'exclusió.

L'HCB ha de desplegar nova infraestructura de xarxa per tal d'incorporar un tallafocs que doni servei a l'edifici CEK. Cal dotar de la mateixa infraestructura homologada existent a les altres seus per a poder complir amb els requeriments actuals de connectivitat definits per l'HCB. Per tant, a nivell de l'equipament a subministrar s'ha de complir amb que:

- Els tallafocs han de permetre integrar-se sense problemes amb la infraestructura actual de l'HCB i s'han de poder integrar tant amb la consola central d'administració com amb el recolector de logs central actual.

3. Garantia

Atesa la naturalesa del contracte, el període de garantia, certificat pel fabricant, haurà de ser obligatòriament de 5 anys, incloent hardware i software, i començarà a comptar a partir de la data de la certificació de la posada en marxa de tots els sistemes inclosos en la licitació. Contemplarà:

- Per a incidències que requereixin d'un canvi de maquinari (reemplaçament avançat de maquinari) s'aplica el SLA (service level agreement):
    - Es requereix d'una GARANTIA OBLIGATÒRIA DEL FABRICANT. 24x7x4 (24 hores, 7 dies a la setmana i un temps de resposta en 4 hores), ONSITE (el fabricant o l'empresa licitadora és qui ha de fer el canvi de l'equip espatllat) i ha de cobrir els dispositius oferts. L'assistència inclourà el cost de les peces, de la mà d'obra i dels desplaçaments i transports.
- Per a la resta d'incidències o incidències de programari, s'aplica el següent SLA (service level agreement):
    - Es requereix d'una garantia 24x7x4 (24 hores, 7 dies i temps de resposta de 4 hores), EN REMOT (i en el cas que la incidència ho requereixi, la presència INSITU) i ha de cobrir a tots els equips oferts (o tota la solució proposada).

La garantia ha d'incloure obligatòriament:

- L'actualització de programari tant de versions menors com majors de tot el programari.
- Revisions periòdiques trimestrals de la salut del sistema que permeti detectar aspectes a corregir o millorar, incloent informació rellevant a la detecció de vulnerabilitats per part de fabricant. Es lliurarà un informe amb els problemes identificats. L'empresa adjudicatària es farà càrrec de les tasques i accions associades a la resolució d'aquests problemes, com podrien ser canvis de configuració o aplicar actualitzacions.

4. Termini i lloc de lliurament

4.1 Termini

El termini aplicable per fer els lliuraments de tots els materials inclosos en aquest expedient és d'un màxim de 2 mesos comptant a partir del dia en què s'ha emès la comanda per part de l'HCB. L'empresa licitadora indicarà el termini de lliurament de tot el material i llicències.

4.2 Lloc de lliurament

El subministrament de l'equipament i altres elements es realitzarà en les ubicacions que es detallen a l'annex 2 del PPT.

En tots els casos, els lliuraments es realitzaran dins dels horaris que indiqui la Direcció de Sistemes d'Informació de l'HCB.

4.3 Documentació dels lliuraments

Els articles s'acompanyaran del corresponent albarà el qual inclourà la següent informació:

- Número de Comanda
- Descripció del Material
- Nombre d'unitats que es lliuren
- Models, Números de sèrie i adreces MAC dels materials
- Import unitari i import total

5. Defectes ocults

Entenem per defectes ocults aquells defectes d'algun o alguns dels elements del Sistema objecte de l'expedient, que no es van detectar en el moment del lliurament i posada en servei dels equips i que no es poden resoldre en el marc del Contracte de Manteniment, com per exemple defectes de fabricació o disseny.

En cas que es determini l'existència de defectes ocults, l'Hospital podrà optar per demanar el canvi del l'equipament subministrat per altres de gamma no inferior al subministrat que no tingui aquest defecte, sense cost, tant pel que fa als equips com als serveis necessaris per dur a terme l'esmentat canvi.

El canvi es durà a terme en les mateixes condicions que el primer lliurament de l'equipament.

Aquesta opció comportarà una penalització del 10% de l'import adjudicat de l'equip subministrat, per a compensar les disfuncions derivades dels mateixos.

6. Condicions d'Execució del Contracte

Al llarg del primer mes de vigència del contracte (a comptar a partir de la data de la formalització del mateix), l'adjudicatari haurà d'aportar documentació que acrediti que ha contractat amb el fabricant els elements de garantia necessaris per tal de que la garantia resultant s'ajusti a les condicions que s'especifiquen en el punt 3 d'aquest PPT, i en el seu cas, amb les millores que hagi presentat a l'Annex 3.2 del PCAP (altres criteris quantificables automàticament).

Barcelona, 26 de setembre de 2023

David Vidal Fernández
Director Sistemes d'Informació

Annex 1 PPT- Declaració responsable del compliment dels requisits imprescindibles

El/la Sr./Sra..... , en nom i representació de l'empresa ..... DECLARA que els equips que ofereix compleixen amb els requeriments tècnics obligatoris que es relacionen en aquesta declaració i amb tota la normativa aplicable a la tipologia d'equip subministrat .

Característica	Valors requisits Concurs	Requisit Imprescindible / opcional
Característiques generals Tallafocs		
Els equips tallafocs han de tenir les certificacions d'Internet Computer Security Association (ICSA): tallafocs, IPSec, IPS, Antivirus, SSL VPN; NSS Labs, Common Criteria i participar en el Cyber Threat Alliance.	Si	Imprescindible
Els equips tallafocs han de ser en format appliance del mateix fabricant de seguretat, queden exclosos màquines virtuals ni servidors de propòsit general. Han de poder ser instal•lats en un rack estàndard de 19".	Si	Imprescindible
Els dos equips físics de ser de idèntiques característiques, redundats i en alta disponibilitat (HA, High availability). Han de permetre treballar en mode HA actiu-actiu i actiu-passiu.	Si	Imprescindible
La solució ha d'incloure funcionalitats de control d'aplicacions, IPS, Antimalware, Webfilter, Antispam i web application firewall. Totes aquestes funcionalitats han d'estar llicenciades per a la duració del contracte.	Si	Imprescindible
La solució ha de tenir funcionalitat d'auditoria propia del Sistema, que com a resultat tingui un indicador o valor número de risc, així com puntuació negative per cada parametre auditat no complert. Aquests parametres que s'han de comprobar son com a minim: políticas de seguretat sense ús en els últims 90 dies, política de contrasenyas debils i comprobació del llicenciament/suport.	Si	Imprescindible
La solució de seguretat ha de permetre diferents modes de funcionament, podent-se combinar entre els diferents Firewalls virtuals: o Mode transparent. o Mode routed i/o mode sniffer.	Si	Imprescindible
La mateixa solució de seguretat ha de permetre la creació d'automatismes per tal de: o Davant la detecció d'un host compromés, els tallafocs	Si	Imprescindible

enviin (tots alhora): un email, una notificació tipus push a dispositius Iphone, poder banejar l'adreça ip, invocar funcions AWS Lambda i Webhook. o Davant el canvi de configuració del tallafocs, un failover, reboot, actualització de firmes i qualsevol event del tallafocs, aquest envii (tots alhora): un email, una notificació tipus push a dispositius Iphone e invocar funcions AWS Lambda i Webhook.		
Capacitat de configuración de proxy explícit per interface, amb la funcionalitat de proxy chaining en cas necessari.	Si	Imprescindible
Característiques físiques Firewalls		
Ports GE RJ45	16	Imprescindible
Ports GE RJ45 Management	2	Imprescindible
Ports GE SFP	8	Imprescindible
Ports GE RJ45/ SFP compartits	4	Imprescindible
Ports 10G SFP	2	Imprescindible
Ports USB	1	Imprescindible
Ports RJ45 Consola	1	Imprescindible
Característiques rendiment Firewalls		
Througput del FW amb paquets de 1518 bytes UDP	20 Gbps	Imprescindible
Througput del FW amb paquets de 512 bytes UDP	18 Gbps	Imprescindible
Througput del FW amb paquets de 64 bytes UDP	10 Gbps	Imprescindible
Latència del FW amb paquets de 64 bytes UDP	4.97 µs	Imprescindible
Sessions concurrents (TCP)	1500000	Imprescindible
Noves sessions per segon (TCP)	56000	Imprescindible
Polítiques de firewall	10000	Imprescindible
Througput amb Control d'Aplicacions (HTTP 64K)	2.2 Gbps	Imprescindible
Firewalls Virtuals suportats (Per defecte/Màxim)	10/10	Imprescindible
Througput IPS amb tràfic mixte d'empresa	2.6 Gbps	Imprescindible
Througput NGFW amb tràfic mixte d'empresa	1.6 Gbps	Imprescindible
Througput Threat Protection amb tràfic mixte d'empresa	1 Gbps	Imprescindible
Característiques gestió Firewalls		
Capacitat de gestió dels equips mitjançant accés via web (https) i terminal (ssh) per la total configuració de la plataforma.	Si	Imprescindible

Tots els canvis efectuats en els tallafocs han de ser aplicats de forma inmediata, sense necessitat de compilar o similar.	Si	Imprescindible
Creació de diferents tipus d'usuari per l'administració podent aplicar diferents rols o perfils, així com definir xarxes d'origen confiables. Es necessari també la possibilitat de crear usuaris de tipus REST-API.	Si	Imprescindible
El port USB ha de permetre la instal•lació desassistida del firmware i aplicació de configuració en el booting de l'equip per realitzar tasques automatiques d'instal•lació i canvis d'equipament.	Si	Imprescindible
Suport de SNMP i sFlow.	Si	Imprescindible
Exportació de logs vía SYSLOG, FTP, SCP i TFTP.	Si	Imprescindible
Característiques networking Firewalls		
Cal que la solució de seguretat tingui capacitats de SD-WAN, en concret: o Balanceig intel•ligent de sortides a internet indiferentment del tipus de connexió WAN (MPLS, 3G/4G, FTTH, etc..). o Chequeig de la disponibilitat d'Internet per cadascuna de les linees. o Chequeig de parametres avançats: jitter, packet loss i latencia per linea. o Configuració de politiques de routing intel•ligent basat en origen (usuaris AD i dirección IP), en el destí (dirección IP, aplicacions i/o serveis d'Internet) i en la línea amb millor qualitat d'aquell moment basat en valors de jitter, packet loss, latencia, tràfic de pujada/baixada o ampla de banda.	Si	Imprescindible
Cal que al port USB és pogui connectar un modem 3G/4G per fer-ho servir com connexió a internet o backup.	Si	Imprescindible
Capacitats d'VXLAN i VXLAN VTEP per l'extensió de xarxes de nivell 2 entre xarxes de nivell 3.	Si	Imprescindible
El sistema proposat ha de tenir una funcionalitat integrada de Traffic Shaping tant de trànsit sortint com a entrant sent capaç de reservar ample de banda i marcar el trànsit amb DSCP. Aquest traffic shaping ha de basar-se en aplicacions i URLs.	Si	Imprescindible
Suport de protocols RIP v1/v2, OSPF, ISIS, BGP i Multicast per IPv4 e IPv6.	Si	Imprescindible
Routing basat en política o PBR.	Si	Imprescindible

Suport Dual Stack IPv4 e IPv6 simultáneament.	Si	Imprescindible
Network address translation NAT IPv4, NAT64 i NAT66.	Si	Imprescindible
DHCP server / DHCP Relay /DNS Server / DNS Proxy / NTP Server.	Si	Imprescindible
802.1Q VLANs	Si	Imprescindible
Routing basat en continguts: ICAP i WCCP.	Si	Imprescindible
Característiques connexió amb tercers Firewalls		
Connector per tal d'identificar usuaris, integrant-se amb Microsoft Active Directory i Novell eDirectory, control d'usuaris Citrix, control d'usuaris de Microsoft Terminal Server, suport de missatges Radius Accounting per SSO i autenticació en servidors remots mitjançant LDAP, RADIUS i TACACS+.	Si	Imprescindible
Connector SDN per tal d'identificar direccions ip's i servidors en entorns AWS, Azure, Nuage, Oracle, Cisco ACI i VmWare NSX.	Si	Imprescindible
Connector de feeds d'amenaces per tal de descarregar els propis feeds de tercers basats en categories URL, direccions ip I noms de domini.	Si	Imprescindible
Característiques seguretat Firewalls		
Arquitectura basada en interfaces i zones, per a l'aplicació de politiques de seguretat	Si	Imprescindible
Capacitat de definir politiques de seguretat IPv4/v6 utilitzant els següents parametres de coincidencia: o Com a origen (totes les opcions): - Capacitat d'utilizar direccions ip, rangs i/o xarxes, aixi com objectes FQDN, paisos, serveis d'internet i direccions ip's reconegudes com origen de xarxes TOR i proxies anonims (aquestes direccions han d'actualitzar-se automaticament). - Capacitat de definir una i/o més d'una interface d'origen/destí, incloent "any". Així com també "zones". - Capacitat d'utilitzar usuaris/grups locals o AD. - Capacitat d'utilitzar dispositius (Windows, MAC, Iphone i Android) sense fer servir cap agent instal•lat en el dispositiu origen. - Capacitat per declarer horaris o "schedule" tant per dia/hora com a data màxima de venciment. - Capacitat de selecció del servei a utilitzar. o Com a destÍ:	Si	Imprescindible

- Capacitat d'utilizar direccions ip, rangs i/o xarxes, aixi com objectes FQDN, paisos i serveis d'internet.		
Capacitat de definir politiques de seguretat IPv4/v6 utilitzant la següent parametrització: o Cal que la configuració del NAT sortint estigui en cadascuna de les politiques, aixo com també a nivell global. o Les diferents funcionalitats de seguretat avançades de nivell 7 s'activaràn de forma individual a nivell de política, mai a nivell global. A més aquestes es gestionaran amb perfils per tal de ser granulars en els permisos. Aquestes funcionalitats son: antivirus, webfilter, DNS filter, Web Application Firewall, Control d'aplicacions, IPS, DLP i Antispam. o Decidir a nivell de politica quin tràfic SSL serà desxifrat pel seu análisis i quin només a nivell de certificat. o A nivell de logging, cal que la solució permeti activa full logging a nivell de politica.	Si	Imprescindible
Cal que la plataforma permeti decidir quin tràfic será analitzat a nivell de control d'aplicacions i quin no.	Si	Imprescindible
Capacitat de creació de regles de DoS a nivell 3 i 4, podent aplicar umbrals per serveis publicats on poder filtrar per direccions ip I països per: ip_src_session, ip_dst_session, tcp_syn_flood, tcp_port_scan, tcp_src_session, tcp_dst_session, udp_flood, udp_scan, udp_src_session, udp_dst_session, icmp_flood, icmp_sweep, icmp_src_session, icmp_dst_session, sctp_flood, sctp_scan, sctp_src_session i sctp_dst_session.	Si	Imprescindible
Capacitat de definir politiques a nivell d'interface per tal de denegar tràfic i no ser processat per la política de seguretat global. S'han de poder utilitzar direccions IP's, paisos, aixi com rangs i xarxes ip com a origen.	Si	Imprescindible
Per tal d'evitar l'accés de xarces botnet, els tallafocs han de tenir una base de dades de reputació dinámica que bloquegi els accesos a nivell d'interface.	Si	Imprescindible
Visualització del número d'usos i quantitat de tráfic de cada regla de seguretat, així com de l'ultima vegada que se ha utilizat.	Si	Imprescindible

Point-to-Point Protocol over Ethernet (PPPoE).	Si	Imprescindible
802.3ad Capacitat de crear enllaços LACP per l'agregació de ports.	Si	Imprescindible
Capacitat de balanceig de servidors, com també posibilitat de fer SSL off-loading pel tráfic HTTPS.	Si	Imprescindible
Funcionalitat integrada del mateix fabricant de doble factor d'autenticació via token mobil, així com per SMS i correu electrónic, integrat en la mateixa plataforma de seguretat.	Si	Imprescindible
Característiques control d'aplicacions Firewalls		
Capacitat per identificar un mínim de 3000 aplicacions actives actuals (incloent aplicacions web 2.0).	Si	Imprescindible
La solució ha de classificar les aplicacions en diferents categories i subcategories, per poder aplicar regles d'acord amb aquestes categories / subcategories (control granular dins de l'aplicació).	Si	Imprescindible
Aplicar tècniques d'identificació d'aplicacions a tots els ports TCP / UDP i no només en els més comuns.	Si	Imprescindible
Capacitat per identificar les aplicacions sota túnels HTTPS.	Si	Imprescindible
Capacitat per identificar aplicacions Industrials com Modbus.	Si	Imprescindible
Capacitat de creació de firmes d'aplicacions per un reconeixament personalizat.	Si	Imprescindible
Característiques IPS Firewalls		
Capacitat per protegir tant servidors com clients amb un minim de 10000 firmes d'IPS, agrupades per categoría, severitat, objectiu i protocol. Davant l'identificació d'un atac per IPS, cal que el tallafocs capturi el tràfic en un arxiu pcap per tal d'evidenciar-ho i fer un estudi posterior.	Si	Imprescindible
Capacitat per identificar patrons d'atacs basats en comportament o rated-base, per tal de bloquejar intents d'atacs un cop superat un umbral d'ús en un temps determinat.	Si	Imprescindible
Capacitat de creació de firmes d'IPS per un reconeixament personalizat.	Si	Imprescindible
Característiques AntiMalware Firewalls		
Capacitat de detecció de malware (virus, grayware, worns, etc…) basat en firmes conegudes o metodes avançats de detecció.	Si	Imprescindible
Capacitat de sandboxing en el cloud/onpremises amb un tamany minim de fitxer de 100 megas indistintament del tipus de fitxer.	Si	Imprescindible

Capacitat per l'eliminació del contingut (CDR) explotable dintre de documents ofimatics i pdf, que es distribueixen per protocols SMTP, IMAP i http.	Si	Imprescindible
Característiques Webfilter Firewalls		
Capacitat de categoritzar més de 250 milions de pàgines web en més de 60 categories web per tal d'aplicar: block, monitor i aplicación de cuotes de temps o tràfic per categoría.	Si	Imprescindible
Suport de protocols http v1.0, 1.1 i 1.2.	Si	Imprescindible
La base de dades de categories web no pot estar en local per tal de tenir la categorització de les url's el més actualitzat possible.	Si	Imprescindible
Capacitat per restringir l'accés a Youtube i Google en mode "safe search".	Si	Imprescindible
Capacitat per a la creació de llistes blanques/negres sense necessitat de llicencia.	Si	Imprescindible
Garantia dels Tallafocs		
Garantia mínima dels equips, expressada en anys	5	Imprescindible
Nivell de cobertura dels serveis de suport	24x7	Imprescindible obert a millora
Temps de resposta, en hores	4	Imprescindible obert a millora
Serveis de Suport i Manteniment proveïts per el fabricant dels equips	Si	Imprescindible

Signatura
lloc i data

Annex 2 PPT- Adreça de lliurament dels elements del expedient

L'equipament es lliuraran a les ubicacions que s'indiquen al a següent taula:

Adreça de lliurament
Centre de procés de dades de Consultes Externes (CEX, situat al Carrer Rosselló 161 de Barcelona)

Annex 3 PPT – Formulari de Productes Hardware i Software que s'inclouran en el subministrament

En aquest formulari, es recull la relació detallada d'articles inclosos en la configuració oferta:

Fabricant	Part Number	Descripció	Quantitat