Parc Científic de Barcelona
UNIVERSITAT DE BARCELONA

PLEC DE PRESCRIPCIONS TÈCNIQUES PEL SUBMINISTRAMENT, INSTAL·LACIÓ, MANTENIMENT, LLICENCIAMENT i GARANTIES PER LA SUBSTITUCIÓ PER OBSOLESCÈNCIA DELS TALLAFOCS PERIMENTRALS ACTUALS I L'ADQUISICIÓ DE NOUS TALLAFOCS PER A LA FUNDACIÓ PARC CIENTÍFIC DE BARCELONA. EXP. NÚM. 2024-04

1. INTRODUCCIÓ

La xarxa informàtica de la Fundació Parc Científic de Barcelona, en endavant FCPB, que està integrada a la xarxa informàtica de la Universitat de Barcelona (UB), disposa de diversos elements de seguretat informàtica per garantir la seguretat envers a possibles intents de ciberatacs.

La solució tecnològica de seguretat actual tant de la FPCB com de la UB pel que fa a equips tallafocs de nova generació (NGFW) està composada per diversos elements, tant físics com virtuals, del fabricant Palo Alto i gestionats centralitzadament amb la plataforma Panorama del mateix fabricant. Aquests equips formen parelles configurades com a clúster, en actiu-actiu o actiu-passiu depenent de les seves funcionalitats i àmbit de protecció.

La FPCB disposa d'un d'aquests clúster per a la securització perimetral, que cal renovar ja que properament quedarà sense suport per part del fabricant en arribar al seu EOL. Els nous tallafocs hauran de reemplaçar els actuals i hauran d'assegurar la seva total compatibilitat amb la totalitat dels altres elements de la infraestructura per que fa a la seva funcionalitat, gestió i monitorització.

A la FPCB s'hi allotgen diverses institucions tant de l'àmbit públic com privat, a les que la FPCB els hi ofereix una sèrie de serveis generals però que com a entitat són autònomes. Cal garantir la seva segregació a nivell de xarxa i la possibilitat d'aplicar regles de seguretat independents per entitat. Així doncs, addicionalment, es pretén reforçar la seguretat amb un parell de clústers addionals: un per al CPD i un altre per impedir la propagació lateral en cas que alguna entitat hagi vist compromesa la seva seguretat informàtica, que hauran d'assegurar la seva total compatibilitat amb la totalitat dels altres elements de la infraestructura per que fa a la seva funcionalitat, gestió i monitorització.

El present Plec de Prescripcions Tècniques conté les especificacions i requeriments tècnics per a la renovació dels tallafocs actuals i la posada en marxa de nous clústers indicats anteriorment.

Els capítols a continuació inclouen una descripció dels sistemes actuals així com els requeriments tècnics generals aplicables i els requeriments tècnics de la present contractació.

2. OBJECTIUS

En aquest plec es demana:

- Dos equips tallafocs idèntics que funcionaran com a una parella en alta disponibilitat per a la renovació dels dos tallafocs actuals.
- Dos equips tallafocs idèntics que funcionaran com a una parella en alta disponibilitat per a la securització del CPD.
- Dos equips tallafocs idèntics que funcionaran com a una parella en alta disponibilitat per a la securització entre entitats (propagació lateral).
- Transceptors òptics necessaris (en funció de les primeres reunions d'inici i anàlisi del projecte amb l'adjudicatari es ratificarà el número exacte de transceptors a demanar. Al plec s'especifica el màxim que podrien ser necessaris).
- Garanties del fabricant pels períodes definits.
- Llicenciament per les funcionalitats demanades pels equips durant els períodes definits.
- Serveis per a la substitució, claus en ma, segons s'especifica en aquest plec tècnic.
- Serveis per a la instal·lació i configuració, claus en ma, segons s'especifica en aquest plec tècnic.

3. ABAST DEL CONTRACTE

3.1 Requisits generals

Els equips han de poder reconèixer i controlar totes les aplicacions (nivell 7 pila TCP) sobre qualsevol port TCP/UDP, tant per a IPv4 com a IPv6, de manera nativa, sense llicències ni mòduls addicionals que puguin impactar en el seu rendiment.

Els perfils de seguretat i filtratge han d'incloure totes les firmes o mecanismes actius sense degradació del rendiment pel nombre de firmes actives.

Les característiques funcionals que han de complir els equips objecte de la licitació són:

- Suport d'alta disponibilitat, tant actiu/passiu com actiu/actiu.
- Amb l'objectiu de poder garantir que una sobrecàrrega del maquinari destinat a donar el servei (tràfic de xarxa), no afecti la gestió d'aquest, els equips han de disposar de maquinari independent de gestió integrat a l'equip, fins i tot sistema operatiu diferent amb l'objectiu d'independitzar totalment els plànols de gestió i xarxa. S'ha de documentar quins recursos hardware es destinen específicament a la gestió i quins a producció (xarxa).
- Port de gestió dedicat fora de banda.
- Es necessiten ports específics de gestió d'alta disponibilitat dedicats a fi de garantir que no consumeixin interfícies de servei per a aquesta tasca.
- Els equips han de poder ser completament gestionats tant des d'entorn web com des d'entorn CLI.
- Suport per a sistemes virtuals per tal de crear entorns completament diferenciats.
- Desplegaments de xarxa en mode *sniffing* (fora de línia, rebent un *mirror* del tràfic), cable (transparent), capa 2 i capa3 (*routing*). S'han de poder barrejar diferents tipus de topologies d'interfícies de xarxa simultàniament sobre el mateix equip.
- Suport de l'estàndard IEEE 802.1Q (encapsulat de diverses vlans sobre el mateix enllaç físic) i IEEE 802.3ad (agregació de diversos enllaços físics).
- Suport a Jumbo Frames (MTU 9192 bytes).
- Suport d'IPv6 tant en mode nivell 3 com en mode transparent.
- L'equip ha de suportar les següents característiques de VPN (Virtual Private Network) :
    - Suport a VPNs sobre IPSec (Internet Protocol Security).
    - Suport a VPNs sobre SSL (Secure Socket Layer).
    - Suport a x-auth en SSL-VPNs per a integració amb clients de tercers.
- Gestió d'esdeveniments dels equips mitjançant:
    - Enviament de logs a tercers sistemes, via syslog.
    - Gestió via SNMP.
- Suport de protocols d'encaminament (*routing*):
    - Protocols dinàmics de routing: RIP, OSPF i BGP
    - Suport de *routing* per a tràfic *multicast* (PIM *Sparse Mode*)
    - Suport de *Policy Routing*.
- Suport de RBAC (*Role Based Access Control* - Perfils per a gestió diferenciada i gestió delegada).
- Capacitat de realitzar tasques de NAT i PAT, inclòs NAT transparent.
- Suport de HTTP2, sense cap configuració addicional. (Aquesta millora permet protegir els servidors web que presten serveis sobre HTTP/2 i permet beneficiar els usuaris de la velocitat i l'eficiència de consum de recursos d'aquest protocol).
- Inspecció de les amenaces en l'*stream* HTTP/2.
- Capacitat de generació de certificats digitals, així com de importació de certificats emesos per tercers.
- Suport a OCSP (*Online Certificate Status Protocol*) i llistes de revocació de certificats (CRL).
- Suport a la integració amb mòduls HSM de tercers per emmagatzemar les claus criptogràfiques.
- Permetre aplicar QoS per aplicació, usuari o URL. Establiment d'amplada de banda màxima i garantida. L'activació d'aquesta funcionalitat no ha de minvar la resta de capacitats exigides a la solució, ni en funcionalitat ni en rendiment.

3.2 Requisits hardware dels tallafocs

Es requereix la instal·lació de dues anelles de securització, cadascuna de les quals estarà formada per dos equips de les mateixes característiques, que treballaran en alta disponibilitat (HA).

Les característiques de capacitat mínimes que ha de complir cadascun dels equips objecte de la licitació són:

3.2.1 Anella 1 (2 equips)

- Arquitectura hardware separada per a gestió i servei, amb recursos hardware dedicats independents, que en cap cas es comparteixin amb el pla de dades, amb l'objectiu de poder garantir que una sobrecàrrega del hardware destinat a prestar el servei no afecti a la gestió i viceversa.
- 12 ports Ethernet 1G/2.5G/5G/10G.
- 10 ports 1G/10G (SFP/SFP+).
- 4 ports 25G (SFP28)
- Disc dur redundat SSD per a Sistema Operatiu (Mínim 400GB)
- Port dedicat per a gestió "out-of-band".
- Ports dedicats per a Alta Disponibilitat.
- Port de consola RJ45.
- Fonts d'alimentació redundants.

3.2.1.1 Requisits de capacitat i rendiment

REQUERIMENT	VALOR MÍNIM
Firewall *throughput* amb inspección a nivell 7, identificació d'aplicacions i *logging* activat utilitzant paquets de 64 KB amb tràfic mixte.	11 Gbps
Threat Prevention throughput amb tots els següents serveis activats (Control d'aplicacions, IPS, Antivirus conegut, Antispyware, AntiMalware desconegut (*SandBoxing*) i *Logging* activat utilitzant paquets de 64 KB amb tràfic mixte). Control d'URL, Seguretat DNS i *File blocking*.	5.1 Gbps
IPSEC VPN *Throughput*.	6.8 Gbps
Capacitat total de sessions.	1.4 M
Sistemes virtuals.	1, ampliable a 11 amb llicència

3.2.2 Anella 2 (2 equips)

- Arquitectura hardware separada per a gestió i servei, amb recursos hardware dedicats independents, que en cap cas es comparteixin amb el pla de dades, amb l'objectiu de poder garantir que una sobrecàrrega del hardware destinat a prestar el servei no afecti a la gestió i viceversa.
- 4 ports Ethernet 10/100/1000.
- 4 ports Ethernet 1G/2.5G/5G.
- 4 ports Ethernet 1G/2.5G/5G PoE.
- 2 ports 1G SFP.
- 8 ports 1G/10G (SFP/SFP+).
- Disc dur redundat SSD per a Sistema Operatiu (Mínim 200GB)
- Port dedicat per a gestió "out-of-band".
- Ports dedicats per a Alta Disponibilitat.
- Port de consola RJ45.
- Fonts d'alimentació redundants.

3.2.2.1 Requisits de capacitat i rendiment

REQUERIMENT	VALOR MÍNIM
Firewall *throughput* amb inspecció a nivell 7, identificació d'aplicacions i *logging* activat utilitzant paquets de 64 KB amb tràfic mixte.	9.5 Gbps
Threat Prevention throughput amb tots els següents serveis activats (Control d'aplicacions, IPS, Antivirus conegut, Antispyware, AntiMalware desconegut (*SandBoxing*) i *Logging* activat utilitzant paquets de 64 KB amb tràfic mixte). Control d'URL, Seguretat DNS i *File blocking*.	4.8 Gbps
IPSEC VPN *Throughput*.	6.5 Gbps
Capacitat total de sessions.	1.4 M
Sistemes virtuals.	1, ampliable a 6 amb llicència

3.3 Requisits de seguretat

Quant a les funcionalitats de seguretat, totes s'han de poder activar de manera concurrent en tots els sistemes de seguretat tant virtuals com físics. Per tant, els equips han d'incorporar les llicències actives adequades.

3.3.1 Visibilitat i control d'aplicacions

- El motor de classificació que s'utilitzarà per identificar el tràfic de dades serà en base a l'aplicació (nivell 7 de la pila TCP), i no només el port. Així doncs, l'aplicació no ha de formar part d'un filtre que s'apliqui posteriorment, sinó que ha de ser l'element d'identificació inicial i basar la resta de l'anàlisi en el seu context.
- Capacitat per identificar i controlar, de manera nativa, sense llicències ni mòduls addicionals que puguin impactar en el rendiment, un mínim de 3.600 aplicacions actives actuals (com ara Sharepoint, Webex, Whatsapp, Facebook, Spotify, SAP, Oracle, Skype, Bit Torrent, etc.).
- Reconeixement i filtratge de qualsevol aplicació sobre qualsevol port TCP/UDP, i no només sobre els ports estàndard.
- Haurà de permetre crear signatures personalitzades per a la identificació d'aplicacions propietàries.
- Utilització d'una política de seguretat unificada, que contempli les aplicacions com a part integral de la mateixa.
- Reconeixement i control de les sub-funcions dins d'una aplicació, com ara transferències de fitxers, correu electrònic, xat, etc.
- Identificar, classificar i gestionar sistemàticament el tràfic desconegut. La solució ha de ser capaç d'identificar el tràfic desconegut, categoritzar-lo pel seu anàlisi i gestionar-lo en base a polítiques. A més, ha de ser possible prendre captures (PCAPs) automàticament del tràfic desconegut, així com generar firmes personalitzades per identificar-lo en cas que sigui tràfic desitjat.

3.3.2 Integració i identificació d'usuaris

- Identificació d'usuaris de forma transparent mitjançant la integració amb directoris LDAP inclòs l'Active Directory de Microsoft.
- Capacitat d'identificar i confirmar usuaris en entorns Microsoft mitjançant l'ús del Windows Management Instrumentation (WMI).
- API XML per a la identificació d'usuaris, que permetrà injectar usuaris apresos des d'altres sistemes, facilitant així la integració amb altres mecanismes d'autenticació via scripting (com ara sistemes 802.1x, Radius, …).

- El Sistema de Seguretat integrarà un recol·lector de syslog (tant TCP com UDP) per poder aprendre usuaris que han estat validats en altres sistemes d'autenticació.
- Serveis d'autenticació basat en LDAP (incloent-hi NTLM), Kerberos (inclòs Single Sign On), Radius i base de dades local al Sistema de Seguretat per als accessos VPN i per a l'accés a aplicacions.
    - Valoració extra: capacitat d'integració nativa amb serveis d'autenticació MFA (Okta, PingID, RSA, DUO...).
    - Possibilitat de connectar els tallafocs amb un servei central d'autenticació en el núvol que integri tots els sistemes d'autenticació de la organització evitant tenir que configurar tots aquests sistemes en tots els tallafocs.
    - Capacitat de mostrar un portal captiu amb tots els sistemes d'autenticació quan s'accedeixi a determinades URL's que es trobin darrera del tallafocs. Aquesta funcionalitat es podrà programar per una, diverses o totes les aplicacions.
    - Capacitat d'utilitzar MFA per accés VPN d'un, diversos o tots els usuaris.
- Capacitat per crear grups dinàmics els membres dels quals s'actualitzin mitjançant una API XML.

3.3.3 Protecció davant d'atacs de denegació de servei

- Reconeixement i prevenció d'escaneigs de xarxa.
- Detecció i mitigació d'atacs de DoS. S'haurà de comptar almenys amb els següents tipus de protecció: SYN Flood, UDP Flood, ICMP Flood, protecció davant inundacions per noves sessions, o protecció per atacs de desbordament per límits de sessions establertes, sent capaç d'establir, en cada cas, els llindars necessaris per activar aquestes proteccions.
- Capacitat de que el fabricant ofereixi llistes d'IP's malicioses, que s'actualitzin i mantinguin automàticament i es disposin per a ús en el tallafocs de manera nativa.

3.3.4 Protecció davant de vulnerabilitats

Quant a protecció davant de vulnerabilitats, el tallafocs oferts hauran de comptar amb la possibilitat d'aplicar polítiques de protecció davant de vulnerabilitats i exploits tant al tràfic entrant com al sortint, havent de complir amb les següents funcionalitats:

- S'han de poder aplicar polítiques tant de detecció com de prevenció (mode IDS o IPS) davant de possibles *exploits* de vulnerabilitats que es detectin en el tràfic, ja sigui entrant o sortint, d'Internet efectuant l'anàlisi en una única passada per a tot tipus d'amenaces.
- En la protecció davant de vulnerabilitats el criteri a utilitzar és la identificació de l'aplicació per poder aplicar perfils de vulnerabilitats ajustats a aquesta aplicació, de manera que no es vegi afectat el rendiment de l'equip.
- Els perfils de detecció i protecció davant de vulnerabilitats han de permetre ser aplicats tant per al tràfic originat des de la xarxa interna com per al tràfic originat des d'Internet, havent de ser possible l'aplicació de detecció i protecció davant de vulnerabilitats especificant si són vulnerabilitats que apliquen als clients, als servidors o tots dos indistintament.
- Les vulnerabilitats han d'estar categoritzades per tipus i per nivells de risc, de manera que l'aplicació de perfils de protecció al tràfic es pugui fer sobre la base d'aquestes categories.
- S'ha de poder utilitzar la identificació CVE de vulnerabilitats per poder utilitzar aquesta identificació a l'aplicació de perfils de protecció específics.
- Utilització de la identificació d'aplicacions com a criteri per seleccionar els perfils de protecció de vulnerabilitats, de manera que només s'apliquin aquelles firmes específiques segons l'aplicació que s'està utilitzant.
- Capacitat de creació de signatures d'IPS a partir de la informació d'una signatura d'Snort, i que permeti importar de manera automàtica un llistat de regles d'Snort.
- Suport en línia de *deep Learning* i anàlisi en el núvol.
- Prevenció de *Command and Control* desconegut basat en *Machine Learning* des del núvol.

3.3.5 Antivirus

El tallafoc proposat ha de tenir la capacitat de definir polítiques d'antivirus, de manera que les descàrregues de fitxers realitzades en sentit Internet xarxa Interna o viceversa siguin inspeccionades i bloquejades si el contingut és maliciós.

S'han de poder aplicar polítiques que permetin aplicar el motor d'antivirus sobre protocols com ftp, http, imap, pop3, smb o smtp, definint per a cadascun d'aquests protocols l'acció a realitzar (permetre els fitxers, descartar els fitxers, desconnectar la sessió o registrar mitjançant logs) davant la detecció del fitxer maliciós pel motor d'antivirus.

El tallafoc ha de permetre l'aplicació de polítiques d'antivirus de forma granular, permetent, per exemple, l'aplicació d'aquestes polítiques a certs usuaris de determinats grups, a certs segments de xarxa amb encaminament determinat o a certes aplicacions.

El mòdul d'antimalware haurà de disposar d'un motor d'anàlisi estàtic basat en algorismes de *Machine Learning* que permetin identificar mostres malicioses desconegudes en temps real sense haver d'esperar el veredicte del mòdul de *Sandboxing*.

3.3.6 Filtratge d'URLs

- Els equips han de suportar la creació de categories d'URL i la inspecció o no del trànsit xifrat SSL segons aquestes categories. Desxifrat de trànsit SSL i SSH sobre qualsevol port. Capacitat per identificar les aplicacions reals dins dels túnels SSL. Ha de tenir la possibilitat de bloquejar les sessions SSL que no poden ser desxifrades o aquelles amb certificats de servidor no confiables.
    - Suport de desxifrat de tràfic TLS1.3 i HTTP/2, incloent un log dedicat per a aquest tràfic.
    - El desxifrat SSL haurà de fer-se en hardware dedicat específicament per a això.
    - Suport de categorització en línia basat en *Deep Learning* i entregat des del núvol.
    - Expansió de la inserció de la capçalera HTTP.
    - Anàlisi de dominis basats en *Machine Learning*
    - Motor per de-ofuscar java-script.
    - Motors d'anàlisi estàtic i dinàmic
    - Anàlisi recursiu de *Deep Learning*

- Possibilitat de detectar l'enviament de credencials corporatives (usuaris i contrasenyes de la xarxa corporativa) cap a les webs que es visiten, de manera que es pugui advertir, bloquejar o permetre aquest enviament de credencials en funció de les categories de web visitades.
- Capacitat de fer filtratge per URL o per categoria d'URL. S'ofertarà un sistema de filtratge que inclogui la categorització d'URLs per part del fabricant, així com la seva actualització automàtica. Així mateix, s'inclourà un mecanisme per poder sol·licitar canvis en la categorització de les URLs.
- Possibilitat de configurar filtratge d'URL multicategoria, és a dir, categoritzar una URL fins a un total de 4 categories, en funció del seu contingut, del domini al que pertanyen, etc., i així poder definit polítiques que permetin l'accés pereò limitin les possibilitats de navegació.
- Ha de disposar d'un monitor d'anàlisi estàtic basat en algoritmes de *Machine learning* que sigui capaç de prevenir l'accés a URL's de *phising* i descàrrega de fitxers *javascript* desconeguts en tems real en el moment que passen pel tallafocs, i sense necessitat de tenir que esperar el veredicte del mòdul de *sandboxing*.

3.3.7 Bloqueig de fitxers i dades sensibles

- Cal que els tallafocs tinguin, de manera nativa, capacitat de controlar quin tipus de fitxers circulen per la xarxa, inclosos els fitxers comprimits. La solució ha de diferenciar entre *upload/download*.

- Capacitat de poder controlar els fitxers en funció del seu tipus i *upload/download* en base al context de l'aplicació.
- Es requereix que els tallafocs disposin de la possibilitat de contractar a futur un servei de DLP en un format del núvol i que cobreixi el moviment de fitxers a través del tallafocs.
    - El servei DLP ha de disposar d'un punt central d'intel·ligència en el núvol des del qual:
        - S'haurà de gestionar l'inventari de documents classificant-los automàticament en funció de la seva tipologia mitjançant algoritmes de *Machine learning* que analitzin patrons basant-se en expressions regulars i en clusterització dels continguts del fitxer
        - S'haurà de poder realitzar les accions de resposta necessàries per assegurar que no redueixin al màxim els riscos de exfiltració i exposició de les dades:
            - Posar en quarantena el document.
            - Borrar el document
            - Eliminar enllaç de compartició utilitzat comunament en serveis SaaS.
            - Notificar al propietari del document quan un dels seus documents violi una de les polítiques de DLP.
    - El servei de DLP s'ha d'integrar nativament en el tallafocs sense necessitat de desplegar ni configurar equips addicionals.
    - Suport de DLP basat en fitxers.

3.3.8 Sandboxing

Capacitat de detecció de codi maliciós desconegut en base a tecnologia de *sandboxing* al núvol.

- El sistema d'anàlisi d'amenaces al núvol ha d'estar ubicat a la Unió Europea, i que pugui acreditar el compliment de les normatives Europees en matèria de protecció de dades.
- El sistema de detecció del núvol ha d'executar el fitxer que ha estat enviat utilitzant una *sandbox* virtual per determinar qualsevol comportament maliciós. El sistema ha de ser capaç de generar signatures automàticament en base a l'activitat observada i distribuir-les als tallafocs.
- L'administrador del Sistema de Seguretat ha de ser capaç d'accedir a aquesta *sandbox* per veure l'estat dels fitxers inspeccionats, així com també pujar-hi fitxers de manera manual.
- • Cal inspeccionar almenys fitxers EXE, DLL, PDF, APK, Java, Office de Microsoft, Mach-O i DMG d'OS-X.

3.3.9 Seguretat DNS

Capacitat per detectar i prevenir de manera automàtica i dinàmica les peticions de DNS malicioses associades amb dominis de codi maliciós (malware), a les quals el tallafocs ha de respondre automàticament amb una IP falsa en lloc del servidor autoritatiu (DNS sinkholing). La base de dades de dominis maliciosos ha de ser nodrida per les fonts següents:

- Sistema de sandbox per trobar nous dominis C2
- DNS passius i telemetries
- Fast-flux domains
    - Prevenció d'amenaces de DNS en l'ús de servidors intermediaris de Botnets basats en DNS
- Dictionary DGA
    - Detecció i prevenció d'atacs basats en dominis maliciosos que usen paraules conegudes
- Ultra-slow DNS tunneling
    - Detecció i prevenció de túnels C2 basats en DNS amb moviment lent
- Dangling DNS attacks
    - Detecció i prevenció d'amenaces en atacs basats en dominis DNS oblidats
- NRD Maliciós
    - Detecció d'atacs basats en l'ús de dominis DNS de nova creació

3.4 Requisits de gestió i administració

Els requeriments de gestió de l'equip són:

- Tant les capacitats de gestió, administració, gestió de logs i informes, han de ser components nadius al tallafocs, sense necessitat d'adquirir altres elements hardware o software per disposar d'aquestes funcionalitats.
- Auditoria de configuracions, incloent la cerca de diferències entre diferents fitxers de configuració.
- La solució de gestió ha de ser capaç de correlar automàticament esdeveniments disjunts que, quan s'uneixen al llarg d'un període de temps per a un mateix equip o usuari, indiquen que aquest equip ha estat probablement compromès. Per exemple, una vulnerabilitat des d'un exploit kit, juntament amb un accés posterior a un domini maliciós que acaba finalment amb una descàrrega de codi maliciós (malware) ha de generar un esdeveniment correlat indicant compromís, a més dels tres esdeveniments individuals.
- La solució ha de suportar informes totalment personalitzables per a tots els logs sobre el propi equip (sense necessitat per tant utilitzar un equip secundari per a aquestes tasques). A més, ha de ser possible extreure tant els informes predefinits com els personalitzats mitjançant una API XML, que permetrà la integració amb sistemes externs.
- La solució serà capaç de realitzar de manera automàtica una anàlisi de comportament diari, en base a tots els logs, a la recerca d'equips que puguin formar part de botnets desconegudes. El resultat serà un informe que inclourà totes les màquines susceptibles d'haver estat reclutades per botnets noves, així com els comportaments que han tingut pels quals se les considera infectades.
- Disponibilitat de mapa geogràfic per identificar l'origen i la destinació dels fluxos i amenaces que entren i surten de la xarxa.
- Capacitat per consumir indicadors de compromís de tercers i incorporar-los automàticament als tallafocs. Cal consumir almenys llistes d'IPs, URLs i DNS.
- Actualitzacions automàtiques, programables, per a les firmes d'Aplicació, IPS, Antivirus i AntiSpyware. Cal llicència corresponent a la prevenció d'amenaces.

3.5 Altres requeriments

- Es requereix que el fabricant proposat, figuri a l'apartat de líders del quadrant màgic de gartner d'Enterprise Firewalls, durant els darrers 10 anys.
- El fabricant ha de tenir publicades les guies de configuració recomanades del Centre Criptològic de Seguretat, CCN-STIC.
- El producte ofert ha d'aparèixer al Catàleg de Productes de Seguretat TIC, CPSTIC, recomanats pel Centre Criptològic Nacional.
- La solució proposada haurà de disposar de mecanismes que injectin als tallafocs, de manera automàtica, llistes dinàmiques provinents de bases de dades de tercers (per exemple serveis anti phishing, llistes de dominis maliciosos, serveis antispam, serveis d'identificació de nodes TOR, avisos de CERTs etc). Aquestes fonts hauran de ser rebudes de manera automàtica, processades i injectades als tallafocs a través de STIX, TAXI, JSON, llistes dinàmiques, etc. sense intervenció humana.

4. SERVEIS DE DIRECCIÓ I EXECUCIÓ DEL PROJECTE

El projecte és claus en mà, per tant, l'adjudicatari haurà de proporcionar tots els recursos de personal i petits materials necessaris per a la seva execució.

- El dimensionament de l'equip de treball ha de ser el necessari per complir amb les tasques demanades en aquest plec.
- L'equip de treball ha d'estar configurat per persones amb coneixements i experiència suficient per garantir l'execució i la qualitat de les tasques contractades.

- Es requereix que o bé el cap de projecte o algun membre de l'equip de treball acrediti titulació Cisco CCIE Enterprise Infraestructure activa.
- Es requereix que, com a mínim, l'empresa acrediti dues persones amb titulacions del fabricant del maquinari (encaminadors i tallafocs) equivalents a Cisco CCIE i altres dos equivalents a Cisco CCNP
- Tots els perfils tindran la formació i el bagatge necessari per executar la seva funció.
- Per cada un dels membres de l'equip de treball ha de poder acreditar-se el nivell de coneixements y experiència adequats a les funcions que realitza.

Cal entregar un pla de projecte que contindrà, com a mínim, la següent informació: calendari, tasques, fases del projecte i metodologia de projecte.

4.1 Tasques a realitzar

La instal·lació / substitució / migració dels tallafocs es realitzarà en dues fases:

- Fase 1: substitució dels actuals tallafocs perimetrals PaloAlto que estan propers a la fi del seu període de vida, pels nous tallafocs objecte d'aquest projecte. Aquest entorn es mantindrà en el model actual Actiu-Actiu, i es mantindrà la ubicació dels tallafocs.
- Fase 2: instal·lació, configuració i posada en marxa de la segona corona, per a la gestió dels tallafocs E-W en la ubicació que decideixi la FPCB.

Per a ambdues fases, cal que el canvi es realitzi amb les màximes garanties d'èxit i el mínim impacte als serveis a usuaris. Els canvis amb afectació es realitzaran en horari nocturn o en l'horari més convenient per a la FPCB. Es vol preinstal·lar tots els equipaments que després substituiran els actuals en paral·lel, i garantir prèviament al canvi que l'element nou ja ha estat correctament integrat per l'adjudicatari en les plataformes de gestió de UB (Centreon, Panorama).

Caldrà documentar els canvis i facilitar tota la documentació pròpia del projecte.

5. GARANTIES DE FABRICANT

Per tots els equips és obligatori que l'adjudicatari subcontracti al fabricant dels mateixos les corresponents "garanties hardware i software de fabricant" en règim 24x7x4 per un període mínim de 4 anys. Aquestes garanties, així com les llicències necessàries, s'activaran a partir de la posada en producció del projecte.

Els licitadors hauran d'incloure, dins de les seves propostes tècniques, una/es carta/es del fabricant/s garantint que poden contractar aquestes garanties. La no presentació d'aquest documents, o la seva presentació amb posterioritat a l'obertura del sobre amb la documentació tècnica, serà motiu d'exclusió de la licitació.

Els contractes de garantia amb el fabricant seran gestionats per l'adjudicatari però aniran a nom de la Fundació Parc Científic de Barcelona que, entre d'altres, podrà obrir, directament o a través de tercers, casos il·limitats al fabricant i fer seguiment dels mateixos.

Important

L'adjudicatari haurà d'acreditar i demostrar davant la FPCB, abans de 30 dies naturals des de la data de signatura del contracte, que ha realitzat les corresponents contractacions amb els fabricants.

Cas que aquesta certificació no s'hagi fet durant aquest període, la FPCB es reserva el dret a adquirir les garanties de fabricant pel seu compte. La FPCB, si és el cas, comunicarà a l'adjudicatari que procedeix a tramitar aquesta contractació l'import total de la qual, més un 20% de penalització, serà descomptat de l'import total d'adjudicació de la present licitació.

6. CARACTERÍSTIQUES DEL MANTENIMENT

Caldrà proporcionar els serveis de manteniment de l'equipament que forma part de la present licitació a partir de l'endemà del dia que s'hagi formalitzat el contracte. Aquest contracte podrà ser prorrogat anualment segons les condicions definides al plec administratiu.

Les característiques del manteniment són les següents:

a) Modalitat de resolució d'avaries -

- Franja horària d'atenció d'avaries : 7x24 (24 hores de dilluns a diumenge)
- Temps presència tècnic : És el temps màxim, comptat a partir del moment en què l'avaria es reportada a l'empresa adjudicatària, fins que es desplaça un tècnic per realitzar un diagnòstic a les instal·lacions del PCB. S'estableix en 2 hores.
- Temps de resolució : És el temps màxim en hores, comptat a partir del moment en què l'avaria es reportada a l'empresa adjudicatària fins que el mal funcionament queda completament solucionat. S'estableix en 4 hores, excepte en el cas d'avaria hardware, que haurà de ser menor o igual a NBD.

b) Acords de suport tècnic -

L'empresa haurà d'acreditar que disposa dels acords suficients amb els fabricants del maquinari objecte del servei que li permetin prestar amb garanties el contracte de manteniment. En concret, hauran de presentar la condició de màxim certificat com a distribuïdor de:

- Palo Alto 'ASC' (*Authorized Support Center*) i '*Diamond Innovator Partner'*

c) Material i mà d'obra -

És responsabilitat de l'empresa adjudicatària aportar tots els recursos humans i materials necessaris per restaurar el correcte funcionament de l'equipament i programari objecte del concurs: mitjans tècnics, equips de diagnosi, peces de reposició, la mà d'obra, els transports, etc.

Cal remarcar que, cas que no sigui possible reparar un equip o peça, caldrà que aquest/a sigui substituït/ïda per un/a altre/a de prestacions i funcionalitats idèntiques o superiors fins que la reparació es pugui fer efectiva.

d) Ampliacions -

Els equips objectes d'aquest contracte podran sofrir ampliacions i/o modificacions sense que això signifiqui la pèrdua del contracte de manteniment per als components ja contractats.

e) Serveis -

El manteniment ha d'incloure l'actualització del software dels equips sota demanda del PCB-UB. Serà responsabilitat de l'adjudicatari, i de forma prèvia a la instal·lació, la tasca de valoració i assessoria del programari que es proposa instal·lar. Aquesta valoració haurà d'incloure :

- Informe d'errors i problemes coneguts de la nova versió.
- Requeriments hardware de la plataforma on es vol instal·lar
- Valoració de la idoneïtat d'implantar o no aquesta versió i/o possibles alternatives.
- Pla de treball per realitzar la instal·lació. Aquest pla preveurà les accions que caldrà realitzar per restaurar el software original en cas de mal funcionament del nou.

El PCB-UB podrà a més a més realitzar consultes tècniques a l'empresa adjudicatària.

f) Accés al Web de suport tècnic -

S'entregaran tants comptes com requereixi el PCB-UB per als seus tècnics per accedir al Web de suport tècnic del fabricant de l'equipament.

7. LLIURAMENT DELS EQUIPS

El subministrament de l'equipament es farà a la següent adreça:

Servei d'Informàtica i Comunicacions
Av. Dr. Marañón 6, rampa 2
08028 Barcelona

Aquesta és l'adreça del Magatzem. L'adjudicatari, o el transportista que subcontracti, el portarà a la sala o sales que el personal del departament d'informàtica l'indiqui. Tot el recorregut es pot fer per passadissos, rampes i ascensors.

L'horari en què es realitzarà el lliurament dels equips serà el següent:

- De dilluns a dijous, de 10h a 17h
- Divendres de 8h a 15h

Els costos de transport, lliurament dels equips a les sales definitives indicades pel personal del servei d'informàtica això com el del transport pels canvis que s'hagin d'efectuar per la manca de correspondència amb els models sol·licitats per la FPCB formen part de la proposta econòmica del licitant, no podent aquest repercutir cap cost addicional pels motius indicats.

El termini de lliurament serà d'un màxim de 30 dies.

27/03/2024

X Miguel Ángel Moruno Apari...

Sr. Miguel Ángel Moruno Aparicio
Cap del SIT- Fundació PCB
Firmado por: MORUNO APARICIO MIGUEL ANGEL -