PLEC DE PRESCRIPCIONS TÈCNIQUES PER LA RENOVACIÓ TECNOLÒGICA DE LA SEGURETAT PERIMETRAL DE L'AJUNTAMENT DE TARRAGONA

INDEX

Plaça de la Font, 1 • 43003 TARRAGONA • Tel. 977 29 61 00 • NIF P-4315000-B • www.tarragona.cat

1. INTRODUCCIÓ

Actualment l'Ajuntament de Tarragona disposa de dos dispositius de seguretat perimetral (tallafocs) del fabricant Palo Alto, concretament el model PA-3020 (amb PANOS 9.1.X), treballant en alta disponibilitat (HA) i, a més té contractades una sèrie de subscripcions de seguretat (Advanced *URL Filtering*, *WildFire*, *Global Protect* Gateway i *Threat Prevention*) i suport/actualització del maquinari i programari de l'equipament fins el 23 d'octubre de 2023.

Aquests dispositius es van adquirir a l'any 2014, per tant properament arribaran al final de la seva vida útil i es fa necessària una renovació tecnològica dels mateixos.

2. OBJECTE DEL CONTRACTE

L'objecte d'aquest contracte és:

- Adquisició d'equipament. Concretament 2 tallafocs de nova generació (NGFW) físics (*appliances*) per a treballar en HA.
- Subscripcions necessàries, durant 3 anys, per a complir amb unes funcionalitats i especificacions de seguretat que es descriuran a les següents clàusules del PPT.
- Suport i manteniment, per part del fabricant, i durant 3 anys de l'equipament subministrat.
- Serveis associats a la instal·lació, configuració i migració del que hi ha als tallafocs que actualment estan en producció als nous equips subministrats.

3. SITUACIÓ ACTUAL

Tal com ja s'ha comentat, actualment l'Ajuntament disposa de dos tallafocs de nova generació Palo Alto PA-3020 treballant en HA (actiu/passiu). Aquests dispositius són físics tipus *appliance*. Hi ha habilitades les següents característiques/funcionalitats:

- Polítiques a nivell 7 (aplicacions).
- Integració dels usuaris corporatius que tenim a Microsoft Active Directory.
- Desxifrat tràfic TLS/SSL per analitzar possible tràfic maliciós a la navegació web. Aquest desxifratge és fa tant pel tràfic entrant com sortint.
- VPN (IPSec i SSL) per tal que els usuaris corporatius puguin fer teletreball i connectar de forma segura altres empreses/organismes.

Plaça de la Font, 1 • 43003 TARRAGONA • Tel. 977 29 61 00 • NIF P-4315000-B • www.tarragona.cat

- Integració amb eina de 2FA (Cisco DUO) per a usuaris en teletreball. Servidor autenticació RADIUS.
- Llistes de bloqueig dinàmiques.
- Definició de Perfils de seguretat: antivirus, antispyware, protecció de vulnerabilitats, filtrat d'URL, bloqueig d'arxius, anàlisi de prevenció de malware de dia zero, protecció d'atacs contra denegació de servei (DoS).
- Reenviament de tràfic basat en polítiques.
- Enviament de logs a servidor Syslog remot.
- Bloqueig per regions.
- Anàlisi de registres sobre tràfic, amenaces, filtratge de URL, vpn ssl, usuaris, aplicacions, configuracions, alarmes, etc.
- DNS sinkhole: Capacitat de fer filtratge basat a les peticions DNS, així com la realització de sinkhole per a la identificació d'equips interns infectats.
- Interfície d'usuari única per a tota la gestió.
- Actualitzacions de versió senzilles amb possibilitat de tornada enrere.
- Informes sota demanda i programats. Exemples:
    - A nivell d'internet: categories i webs més visitades, aplicacions, usuaris, etc.
    - A nivell de seguretat: atacants, *spyware*, virus, vulnerabilitats, etc.
    - A nivell d'aplicacions SaaS: ús, riscs, categories, transferència de dades, etc.
- Subscripcions avançades de seguretat a tots dos dispositius, actualment en producció, fins el 23 d'octubre de 2023:
    - Threat Prevention: Protecció avançada (IPS) contra els *exploits* coneguts, el *malware*, les adreces URL malicioses, el *spyware*, les activitats de comandament y control, etc.
    - Advanced URL Filtering: Garanteix un accés segur a Internet amb un sistema de prevenció en temps real aplicable a llocs web coneguts i desconeguts, que a més bloqueja les adreçes URL malicioses.
    - WildFire: Servei al núvol que garanteix la seguretat dels arxius detectant i bloquejant automàticament el *malware* desconegut.
    - Porta d'enllaç de Global Protect: Serveix per a dotar de característiques avançades a la solució segura d'accés remot (VPN) que porten els tallafocs. Per exemple: poder realitzar comprovacions HIP (*Host Information Profile*), permet fer connexions des de dispositius mòbils, des de Linux, etc

Plaça de la Font, 1 • 43003 TARRAGONA • Tel. 977 29 61 00 • NIF P-4315000-B • www.tarragona.cat

- Actualment tenim contractat el suport *Partner Premium* amb el fabricant, amb data de finalització 23 d'octubre de 2023.

Altres dades a tenir en compte per la migració.

Element	Valor
Interfícies utilitzades	7 ports 1Gbps connectats
Subinterfícies creades	11
Zones definides	21
Enrutadors virtuals	2
Túnels VPN IPSEC	14
Túnels VPN GRE	2
Servidors DHCP	8
Proxy DNS	2
Polítiques de seguretat	247
Polítiques de NAT	40

Plaça de la Font, 1 • 43003 TARRAGONA • Tel. 977 29 61 00 • NIF P-4315000-B • www.tarragona.cat

4. SOLUCIÓ DEMANADA

Tal com ja s'ha comentat, la solució que es demana són 2 tallafocs de nova generació físics (appliances) per a treballar en HA (actiu/passiu). Aquests han de cobrir en quant a característiques i funcionalitats, com a mínim, tot el que ja fan els actuals i que s'ha detallat a la clàusula 3 del present plec de prescripcions tècniques, incloent les funcionalitats avançades de seguretat que tenen un format de subscripció mencionades o similars.

4.1. Especificacions tècniques dels equips demanats

En quant a les especificacions tècniques, han de complir, com a mínim, les següents:

- Els tallafocs han de ser enracables en armaris de 19".

- Flux d'aire forçat de davant a darrere.
- Han de tenir doble font d'alimentació per equip.
- Que tinguin disc dur integrat, mínim, de 480GB SSD.
- En quant a Interfícies, com a mínim, han de tenir:
    - 8 ports RJ45 de 1Gb/2,5Gb/5Gb/10Gb
    - 10 ports SFP/SFP+ de 1Gb/10Gb
    - 4 ports SFP28 de 25Gbps
    - 1 port de gestió RJ45 100Mb/1000Mb
    - 1 ports RJ45 100Mb/1000Mb per alta disponibilitat (HA)
    - 1 port de consola
    - 1 port USB
- En quant a rendiment han de complir, com a mínim:
    - Del tallafocs (HTTP/combinació d'aplicacions): 13,1/11,3 Gb/s
    - De Threat Prevention (HTTP/combinació d'aplicacions): 5,1/5,9 Gb/s
    - De VPN IPSec: 6,8Gb/s
    - Numero de sessions: 1,4 milions
    - Noves sessions per segon: 130.000
    - Número de sessions concurrents de desxifratge SSL: 140.000
- Capacitats mínimes:
    - Número de polítiques de seguretat: 10.000
    - Número de polítiques de NAT: 3.000
    - Número de zones de seguretat: 40
- En quant a VPN, com ha mínim ha de complir:
    - Usuaris concurrents VPN-SSL: 1.800
    - Número de túnels IPSEC: 5.000
- El fabricant ha d'estar certificat en la ISO 27001

5. SERVEIS IMPLANTACIÓ

L'empresa adjudicatària haurà d'incloure en l'oferta la totalitat dels serveis necessaris per a que els tallafocs quedin instal·lats i totalment operatius i en producció (projecte claus en ma). Aquesta instal·lació es farà de forma coordinada i sota la supervisió amb els enginyers de sistemes del Servei TIC.

Plaça de la Font, 1 • 43003 TARRAGONA • Tel. 977 29 61 00 • NIF P-4315000-B • www.tarragona.cat

Així mateix en el procés de migració, s'optimitzaran en la mesura que es pugui, les polítiques i configuracions que hi ha definides als tallafocs per a evitar redundàncies o configuracions que es podrien millorar per assegurar al màxim el perímetre.

En l'oferta s'haurà de descriure una planificació dels treballs a realitzar, amb terminis i descripció el més acurada possible de les diferents fases, tal com es detalla a la clàusula 7.

6. MANTENIMENT I SUPORT TÈCNIC

Es demana que hi hagi un manteniment i suport contractat amb el fabricant, durant 3 anys, tenint en compte que és un element crític de la ciberseguretat de l'Ajuntament. Aquest ha de contemplar:

- Actualitzacions de funcionalitats i programari.
- Accés directe a experts/enginyers en els tallafocs.
- Assistència telefònica, per part d'enginyers experts dels tallafocs, les 24 hores al dia, els 365 dies de l'any.
- El temps de resposta per part del fabricant ha de ser inferior a una hora per a incidències crítiques, considerades totes aquelles on el tallafocs està caigut i l'entorn de producció de l'Ajuntament es veu molt afectat.
- El servei de reemplaçament (RMA), que implica que hi ha un problema al maquinari i s'ha de substituir l'equipament per un altre sense defectes, ha de fer-se al dia següent laborable (NBD).
- Portal web d'atenció: ha de proporcionar accés a documentació dels productes, base de dades de resolució de problemes, gestió de casos, etc.

A més, es demana un suport de primer nivell per part de l'adjudicatari, en forma de borsa d'hores anuals per a poder resoldre incidents, consultes, peticions, etc. que puguin sorgir al llarg de la durada del termini del suport de 3 anys demanat. Concretament es demanen **25 hores per cada any**.

Els tècnics del Servei TIC idealment haurien de poder obrir incidències directament al fabricant, o en cas que el tipus de suport no ho permeti, l'adjudicatari haurà de fer d'intermediari per a obrir la/es incidència/es al fabricant sense cap cost addicional per a l'Ajuntament, independentment de si s'han exhaurit les hores de la borsa d'hores. És a dir, aquesta intermediació va a banda de la borsa d'hores.

Plaça de la Font, 1 • 43003 TARRAGONA • Tel. 977 29 61 00 • NIF P-4315000-B • www.tarragona.cat

7. PLA DE PROJECTE

L'empresa adjudicatària haurà d'aportar el pla de projecte, per a poder avaluar-lo, amb, com a mínim els següents punts:

- Calendari d'execució del projecte. Ha de contemplar l'estimació de subministrament com els serveis associat a la posada en marxa.
- Planificació/Descripció de les tasques d'anàlisi, disseny, instal·lació, configuració, migració, optimització, proves i posada en producció.
- Informació generada referent a la instal·lació/configuració del sistema.
- Calendari i pla de formació als tècnics de sistemes del Servei de TIC, per tal que aquests tinguin els coneixements suficients per a portar amb èxit la gestió diària del sistema.
- Suport post-implantació.
- Persones involucrades al projecte, amb la seva titulació/certificació i experiència en instal·lacions similars.

El no presentar el pla de projecte serà motiu d'exclusió.

8. TERMINI D'EXECUCIÓ I LLIURAMENT

El lloc de lliurament dels béns serà al Servei TIC de l'Ajuntament de Tarragona, ubicat a l'edifici de Plaça de la Font, 1.

El termini màxim per a tenir els nous tallafocs en producció (subministrament i serveis realitzats) serà tres mesos a comptar des del dia següent de la signatura del contracte, excepte que l'adjudicatari hagués ofert un altre termini menor.

9. CONDICIONS I HORARIS

L'adjudicatari realitzarà els serveis en el seu conjunt durant els dies laborables; dilluns a divendres no festius de 08:00h a 15:00h, a excepció dels casos previstos, com per exemple actuacions que tinguin impacte en l'activitat de l'Ajuntament, etc. Aquests seran planificades i consensuats entre l'adjudicatari i el Servei TIC per evitar que afectin a l'Ajuntament en horari laboral.

Plaça de la Font, 1 • 43003 TARRAGONA • Tel. 977 29 61 00 • NIF P-4315000-B • www.tarragona.cat

10. CONFIDENCIALITAT

L'empresa adjudicatària queda expressament obligada a mantenir absoluta confidencialitat i reserva sobre qualsevol dada que pogués conèixer amb ocasió del compliment del contracte, especialment les de caràcter personal, que no podrà copiar o utilitzar amb una finalitat diferent a la que figura en aquest plec, ni tampoc cedir a altres ni tant sols a efectes de conservació.

L'empresa adjudicatària quedarà obligada a la no difusió de cap tipus de codi d'accés o qualsevol altre tipus d'informació que pugui facilitar l'entrada als sistemes de l'Ajuntament, així com a no fer un ús incorrecte dels permisos i privilegis que es concedeixin al seu personal per a l'execució d'aquest contracte.

Tarragona, en data de la signatura

Plaça de la Font, 1 • 43003 TARRAGONA • Tel. 977 29 61 00 • NIF P-4315000-B • www.tarragona.cat