AJUNTAMENT DE CASTELLBISBAL

DEPARTAMENT DE SISTEMES D'INFORMACIÓ
Ref. expedient: 2023/11/TAB
Ref. informe: PPT_1_XS_Licitació Nou Firewall Corporatiu V1
/xsu

PLEC DE PRESCRIPCIONS TÈCNIQUES PEL SUBMINISTRAMENT D'UN NOU SUBSISTEMA DE SEGURETAT INFORMÀTICA (FIREWALL) PER L'AJUNTAMENT DE CASTELLBISBAL

Av. Pau Casals, 9 | 08755 Castellbisbal | tel. 93 772 02 25 | fax 93 772 13 07 | bustia@castellbisbal.cat | www.castellbisbal.cat

PLEC DE PRESCRIPCIONS TÈCNIQUES PEL SUBMINISTRAMENT D'UN NOU SUBSISTEMA DE SEGURETAT INFORMÀTICA (FIREWALL) PER L'AJUNTAMENT DE CASTELLBISBAL

ÍNDEX

PLEC DE PRESCRIPCIONS TÈCNIQUES PEL SUBMINISTRAMENT D'UN NOU SUBSISTEMA DE SEGURETAT INFORMÀTICA (FIREWALL) PER L'AJUNTAMENT DE CASTELLBISBAL

1. Objecte del plec de prescripcions tècniques

L'objecte d'aquest plec és la definició de les especificacions tècniques i de serveis requerides pel subministrament, serveis d'instal·lació, posada en règim d'explotació, manteniment i suport, d'un nou subsistema de seguretat informàtica (en endavant Firewall) per la protecció de l'entorn informàtic de l'Ajuntament en front a possibles ciberatacs.

2. Abast

El contracte pel subministrament, serveis d'instal·lació, posada en règim d'explotació, manteniment i suport del Firewall, te com abast:

- El subministrament del maquinari, programari i llicències d'ús que permeti, en resum, gestionar els següents nivells de protecció informàtica a l'Ajuntament:
    - Control i gestió d'intrusions
    - Prevenció, control i gestió d'amenaces
    - Control i gestió Antivirus
    - Control d'accés i filtrat d'URL-Web

- Els serveis d'instal·lació i activació del maquinari i del programari així com la seva posada en regim d'explotació.
  Aquest regim d'explotació es considerarà assolit, un cop traslladades i verificades al nou subsistema totes les configuracions, polítiques i regles de seguretat actualment operatives a l'actual Firewall de l'Ajuntament.

- El servei de manteniment i suport del maquinari, programari i llicències d'ús del Firewall subministrat.
  Aquest servei inclourà tot el que pugui fer referència a les necessitats de manteniment i suport relacionades amb les incidències, avaries, recanvi de peces, actualitzacions de firmware i altres intervencions, actualitzacions i ajustos que siguin necessàries aplicar al Firewall instal·lat per a mantenir tant la seva òptima operativitat com els nivells de protecció desitjats en front de ciberatacs.

3. Situació actual

L'Ajuntament de Castellbisbal actualment disposa d'un Firewall de la empresa PaloAlto Networks que es composa d'una plataforma tallafocs amb control d'intrusions IPS (WildFire), d'una plataforma antivirus de primer nivell (Threat Prevention) i d'una plataforma de control d'accés a URL-Web (URL Filtering), suportada a nivell de maquinari, per dos equips PaloAlto Networks model PA-3020 treballant en Alta Disponibilitat (HA) activa-passiva.

Maquinari instal·lat i operatiu a l'Ajuntament de Castellbisbal:

- 2x Equip PaloAlto Networks Model PA-3020
    - Equip-1: Número de sèrie: 001801015382

- Equip-2: Número de sèrie: 001801015211
- Versió de Programari: 9.1.12-h3
- Agent de GlobalProtect: 4.1.13

Sobre aquest maquinari treballen els següents programaris/plataformes de seguretat:

- 2x Plataforma tallafocs amb control d'intrusions IPS (WildFire)
- 2x Plataforma d'Antivirus (Threat Prevention)
- 2x Plataforma de control d'accés a URL-Web (URL Filtering)

4. Especificacions tècniques del subministrament a contractar

Tots les especificacions i requeriments relacionats en aquest punt, es consideren essencials.

4.1. Requeriments generals

S'indiquen a continuació els requeriments mínims del maquinari, programari, equips, funcions i capacitats a ser suportades pel nou Firewall a desplegar.

El Firewall haurà de poder reconèixer i controlar les aplicacions (nivell 7 pila TCP) sobre qualsevol port TCP/UDP, tant per IPv4 como IPv6, de manera nativa, sense llicencies ni mòduls addicionals que puguin impactar en el seu rendiment.

Els perfils de seguretat i filtrat han d'incloure totes les regles i/o mecanismes de protecció actius sense degradació del rendiment pel nombre de regles actives.

4.2. Característiques i requeriments funcionals

Les característiques i requeriments funcionals que ha de complir el Firewall objecte de la licitació son:

- Suport d'alta disponibilitat, tant actiu/passiu com actiu/actiu.
- Arquitectura de processament en paral·lel. Un sol cicle per a fer tots els processos de seguretat.
- Arquitectura "Single Pass Single Policy" de tal manera que, amb tots els motors i signatures d'inspecció d'amenaces activats, el rendiment del sistema no es vegi afectat ni tampoc hi hagi impacte al rendiment i l'estabilitat de la xarxa.
- L'arquitectura haurà de tenir separada els recursos de l'entorn de gestió i de l'entorn de dades amb recursos hardware dedicats e independents amb l'objectiu de garantir que una sobrecàrrega del hardware dedicat a la gestió no afecti al servei de seguretat (tràfic de dades a la xarxa). Els equips han de disposar, de manera independent, de hardware de gestió integrat amb l'objectiu d'independitzar els dos entorns (gestió i dades). S'haurà de documentar quins recursos hardware es destinen específicament a la gestió i quins a producció (tràfic / xarxa). No és permet l'ús de CPU's multi-propòsit per aquesta gestió.
- Port de gestió dedicat fora de banda.
- No haurà d'haver major impacte al rendiment del sistema pel fet d'habilitar més o menys regles als serveis d'inspecció d'amenaces conegudes (IPS, Antivirus, AntiSpyware, URL Filtering).

- Ports dedicats i d'alta disponibilitat específics per a la gestió, per a garantir que no hi ha consum d'interfícies de servei per aquesta tasca.
- El sistema ha de poder ser completament gestionat tant des d'un entorn Web com des d'un entorn CLI.
- Desplegament híbrid de xarxa dins del mateix equip i de forma simultània en un mateix equip permetent utilitzar varis interfícies de xarxa treballant en diferents modes simultàniament (Nivell 3, Nivell 2, Mode TAP, Mode Transparent).
- Suport dels estàndards IEEE 802.1Q (encapsulat de vàries VLAN sobre el mateix enllaç físic) i IEEE 802.3ad (agregació de varis enllaços físics).
- Suport de Jumbo Frames (MTU 9192 bytes).
- Suport de IPv6 tant en mode nivell 3 com en mode transparent.
- Ha de suportar les següents característiques de VPN (Virtual Private Network):
    - Suport de VPN's sobre IPSec (Internet Protocol Security).
    - Suport de VPN's sobre SSL (Secure Socket Layer).
    - Suport de a x-auth en SSL-VPNs per integració amb clients de tercers.
- Gestió d'esdeveniments dels equips mitjançant:
    - Enviament de 'logs' a altres sistemes via 'syslog'.
    - Gestió via SNMP.
- Ha de suportar protocols d'enrutament (routing protocols):
    - Protocols dinàmics de routing: RIP, OSPF i BGP
    - Suport de routing per 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 per realitzar tasques de NAT i PAT, inclòs NAT transparent.
- Suport de HTTP/2, sense cap configuració addicional que permeti securitzar servidors Web que prestin serveis sobre HTTP/2.
- Inspecció d'amenaces al 'stream' HTTP/2.
- Capacitat de generació de certificats digitals, així com la importació de certificats digitals emesos per tercers.
- Suport de OCSP (Online Certificate Status Protocol) i a llistes de revocació de certificats (CRL).
- Suport a la integració amb mòduls HSM (Hardware Security Module) de tercers per l'emmagatzematge de les claus criptogràfiques.
- Capacitat de funció de SSL Packet Broker. Desxifrat de tràfic i enviament en clar a altres solucions per funcions d'inspecció per a retornar-lo després pel seu enviament a destí xifrat un cop aplicades les polítiques de seguretat que correspongui.
- Ha de permetre aplicar QoS per aplicació, usuari o URL. Establiment d'amplada de banda màxim i garantit. L'activació d'aquesta funcionalitat no ha de minvar la resta de capacitats exigides a la solució ni en les seves funcionalitats ni en el seu rendiment.
- Capacitat de funcionament en mode Proxy Web explícit i transparent.

4.3. Requeriments Hardware

Tot seguit es descriu a alt nivell, l'equipament HW/SW a subministrar i la tipologia HW/SW de cadascun dels ítems:

S'oferiran dos (2) equips en total que treballaran en Alta Disponibilitat (HA). Les característiques de tipologia i capacitat que han de complir cadascun dels equips objecte de la licitació son:

- Arquitectura hardware separada per a gestió i servei, amb recursos hardware dedicats independents i que en cap cas es comparteixin a l'entorn de dades, amb l'objectiu de poder garantir que una sobrecàrrega del hardware destinat al servei no afecti a la gestió i viceversa.
- 4 Ports Ethernet 1G
- 8 Ports Ethernet 1G/2.5G/5G, dels quals, al menys 4 d'ells han d'oferir la capacitat PoE amb una potència de 90W per cada port.
- 2 Ports 1G (SFP).
- 8 Ports 1G/10G (SFP/SFP+).
- Disc dur de tecnologia SSD pel Sistema Operatiu (Mínim 256 GB de capacitat)
- Port dedicat per gestió "out-of-band".
- Ports dedicats per HA (Alta Disponibilitat).
- Port de consola RJ45.
- Capacitat de disposar de fonts d'alimentació redundants.

4.4. Requeriments 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 HTTP/tràfic mixt	8,9 / 6,8 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 HTTP/tràfico mixt). Control d' URL, Seguretat DNS i File blocking	3,3 / 3,2 Gbps
IPSEC VPN Throughput	4,6 Gbps
Capacitat Total de Sessions	945.000
Sistemes Virtuals	1, ampliable a més

4.5. Requeriments de seguretat

Totes les funcionalitats s'hauran de poder activar de forma concurrent en tots els Sistemes de Seguretat tant virtuals com físics.

<u>Visibilitat i control d'aplicacions</u>

- El motor de classificació per identificar el tràfic ha de ser a nivell aplicació (nivell 7 de la pila TCP) i no solament a nivell port. La aplicació ha de ser l'element d'identificació inicial per basar la resta de l'anàlisi en el seu context.

- Capacitat per identificar i controlar, de manera nativa i sense llicències ni mòduls addicionals, un mínim de 3.700 aplicacions actives actualment (per exemple, Webex, Sharepoint, WhatsApp, Facebook, Spotify, Tuenti, Bit Torrent, SAP, Oracle, GMail, Skype, etc.).
- Reconeixement i filtrat de qualsevol aplicació sobre qualsevol port TCP/UDP i no solament sobre els ports estàndard.
- Haurà de permetre crear regles personalitzades per a la identificació d'aplicacions propietàries.
- Reconeixement i control de les sub-funcions dintre d'una aplicació, com transferències de fitxers, correu electrònic, xat, etc.
- Identificar, classificar i gestionar sistemàticament el tràfic desconegut. La solució ha de poder identificar el tràfic desconegut, categoritzar-lo pel seu anàlisi i gestionar-lo en base a polítiques, així com generar regles personalitzades per a identificar-lo en el cas de que sigui tràfic desitjat.

Integració i identificació d'usuaris

- Identificació d'usuaris transparent a través de la integració amb directoris LDAP inclòs el Active Directory de Microsoft , en concret el Active Directory de Microsoft Windows 2008 R2 actualment operatiu a l'Ajuntament de Castellbisbal.
- Capacitat d'identificar i confirmar usuaris en entorns Microsoft a través de l'ús de WMI (Windows Management Instrumentation).
- API XML per a la identificació d'usuaris, que permeti registrar usuaris provinents d'altres sistemes, facilitant així la integració amb altres mecanismes d'autenticació via 'scripting' (como son els sistemes 802.1x, Radius, etc…).
- Serveis d'autenticació basats en LDAP (incloent NTLM), Kerberos (inclòs Single Sign On), Radius i base de dades local al Sistema de Seguretat pels accessos VPN i per l'accés a aplicacions. Aquest serveis d'autenticació hauran de suportar l'autenticació d'usuaris d'entorns Windows 7, Windows 10, usuaris Citrix XenApp 6.5 sobre Windows Server 2008 R2, entorns actualment operatius a l'Ajuntament de Castellbisbal.
    - Capacitat d'integració nativa amb serveis d'autenticació MFA – Multi-Factor Authentication (Okta, PingID, RSA, Duo,...).
    - Possibilitat de connexió del Firewall amb un servei central d'autenticació al núvol que integri tots els sistemes d'autenticació de l'organització per a poder evitar la configuració de tots els sistemes de seguretat a tots els Firewall.
    - Capacitat de mostrar un portal captiu amb tots els sistemes de autenticació quan s'accedeix a determinades URL's que estiguin darrera del Firewall. Aquesta funcionalitat es podrà programar per a una, varies o totes les aplicacions.
    - Capacitat de fer servir MFA per accés VPN d'un, varis o tots els usuaris.
- Capacitat per a crear grups dinàmics els membres dels quals s'actualitzin a través d'una API XML.

Protecció davant d'atacs de denegació de servei (DoS)

- Reconeixement i prevenció d'escanejos de xarxa.
- Detecció i mitigació d'atacs de DoS. S'haurà de disposar al menys dels següents tipus de protecció: SYN Flood, UDP Flood, ICMP Flood, protecció davant desbordaments per noves sessions o protecció per atacs de desbordament de límits de sessions establertes, podent en cada cas establir 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 pel seu ús en el Firewall de manera nativa.

Protecció davant vulnerabilitats

El Firewall ofert haurà de tenir la possibilitat d'aplicar polítiques de protecció davant de vulnerabilitats i 'exploits' tant pel tràfic entrant com pel sortint, havent de complir amb totes les següents funcionalitats:

- S'han de poder aplicar polítiques tant de detecció com de prevenció (modes IDS i IPS) davant possibles 'exploits' de vulnerabilitats que es detectin al tràfic entrant i sortint, efectuant l'anàlisi en temps real en una única passada per a qualsevol tipus d'amenaça (threat) sense incórrer en cap degradació del rendiment.
- A la protecció davant vulnerabilitats, el criteri a utilitzar serà la identificació de l'aplicació per a poder aplicar perfils de seguretat ajustats a aquesta aplicació.
- Els perfils de detecció i protecció davant vulnerabilitats han de permetre ser aplicats tant pel tràfic originat des de la xarxa interna com pel tràfic originat des de Internet. Ha de ser possible aplicar detecció i protecció davant vulnerabilitats especificant si son vulnerabilitats que apliquen als clients, els servidors o ambdós indistintament.
- Les diferents vulnerabilitats gestionades han d'estar categoritzades per tipus i per nivells de risc, de forma que l'aplicació dels perfils de protecció es pugui realitzar en base a aquestes categories.
- S'ha de permetre utilitzar la identificació CVE (Common Vulnerabilities and Exposures) de vulnerabilitats per a poder fer servir aquesta identificació a l'aplicació de perfils de protecció específics.
- Utilització de la identificació d'aplicacions com criteri per a seleccionar els perfils de protecció de vulnerabilitats, de manera que només s'apliquin aquelles regles especifiques a l'aplicació utilitzada.
- Capacitat de creació de regles IPS a partir de la informació de una regla de Snort. S'ha de permetre importar de manera automàtica un llistat de regles de Snort.
- Suport en línia de Deep Learning i anàlisi al núvol.
- Prevenció de 'Command and Control' desconegut basat en Machine Learning des del núvol.

Antivirus

- El Firewall proposat ha de tenir la capacitat de definir polítiques d'antivirus, per tal que les descàrregues de fitxers en els dos sentits (Internet – Xarxa Interna o Xarxa Interna – Internet) siguin inspeccionades i bloquejades si el seu contingut es detecta maliciós.
- S'han de poder establir polítiques que permetin aplicar el motor antivirus sobre diferents protocols com ftp, http, imap, pop3, smb o smtp, definint per a cadascun

d'aquests protocols l'acció a realitzar davant la detecció del fitxer maliciós per part del motor antivirus (permetre els fitxers, descartar els fitxers, desconnectar la sessió o registrar mitjançant 'logs')

- El Firewall ha de permetre l'aplicació de polítiques d'antivirus de forma granular (aplicació de polítiques per determinats usuaris o determinats grups d'usuaris, per determinats segments o vlan de la xarxa o per determinades aplicacions)
- El mòdul antimalware haurà de disposar d'un motor d'anàlisi estàtic basat en algoritmes de Machine Learning que permetin identificar mostres malicioses desconegudes en temps real sense necessitat d'esperar al veredicte del mòdul de Sandboxing

Filtrat d'URL's

- Ha de suportar la creació de categories d'URL i la inspecció o no del tràfic xifrat SSL en base a dites categories. Desxifrat de tràfic SSL i SSH sobre qualsevol port. Capacitat per a identificar les aplicacions reals dintre dels túnels SSL. Ha de tenir la possibilitat de bloquejar les sessions SSL que no puguin ser desxifrades o aquelles amb certificats de servidors no confiables.

    - Suport de desxifrat de tràfic TLS1.3 y HTTP/2, incloent un 'log' dedicat per aquest tràfic, fent més eficient el seu anàlisi.
    - El desxifrat SSL haurà de fer-se en hardware dedicat específicament per aquesta funció.
    - Suport de categorització en línia basat en Deep Learning i lliurat des del núvol.
    - Expansió de la inserció de la capçalera HTTP
    - Anàlisi de dominis basats en Machine Learning
    - Motor para de-ofuscar Java-script
    - Motors d'anàlisi estàtic i dinàmic
    - Anàlisis recursiu de Deep Learning

- Possibilitat de detectar l'enviament de credencials corporatives (usuaris i contrasenyes de la xarxa corporativa) cap a les web que es visiten, de manera que es pugui advertir, bloquejar o permetre l'enviament de dites credencials en funció de la categoria de les web visitades.

- Capacitat de realitzar filtrat per URL o per categoria d'URL. S'oferirà un sistema de filtrat que inclogui la categorització d'URL's per part del fabricant, així com la seva actualització automàtica. S'ha de incloure també un mecanisme per a poder sol·licitar canvis a la categorització de les URL's. Es valorarà positivament que les categories de 'malware' s'actualitzin automàticament amb la intel·ligència recopilada per altres elements de la solució quan detectin activitat maliciosa.

    - Possibilitat de configurar filtrat d'URL multi-categoria, es a dir, poder categoritzar una URL en fins a quatre (4) categories en funció del seu contingut, del domini al qual pertany o d'altres.

- Disposar d'un motor d'anàlisi estàtic basat en algoritmes de Machine Learning que sigui capaç de prevenir l'accés a URL's de 'Phishing' i descàrrega de fitxers JavaScript desconeguts, en temps real, a l'hora de passar pel Firewall i sense la necessitat d'haver d'esperar al veredicte del mòdul de Sandboxing

Bloqueig de fitxers i dades sensibles

- El Firewall ha de tenir, de manera nativa, capacitat per a controlar quins tipus de fitxers circulen per la xarxa, inclosos el fitxers comprimits, diferenciant entre fitxers 'upload' i 'download' i permeten o no la seva circulació en base al context de l'aplicació.
- El Firewall ha de disposar de la possibilitat d'incloure en un futur, un servei DLP (Data Loss Prevention) al núvol que controli el moviment de fitxers i permeti establir les polítiques de circulació dels mateixos.
- El servei de DLP s'ha de poder integrar nativament al Firewall sense necessitat de cap desplegament ni cap configuració d'equips addicionals.
- El suport de DLP es basarà a nivell de fitxer.

Sandboxing

- Capacitat de detecció de 'malware' desconegut en base a tecnologia de Sandboxing al núvol. Els fitxers desconeguts s'identifiquen al Firewall i s'envien al sistema de detecció de 'malware' al núvol en base a l'aplicació, el tipus de fitxer, la direcció del flux o l'usuari.
- El sistema d'anàlisi d'amenaces al núvol ha d'estar ubicat a la Unió Europea, i ha de poder acreditar el compliment de les normatives Europees en matèria de protecció de dades.
- El sistema de detecció al núvol ha d'executar el fitxer que ha estat enviat utilitzant un sandbox virtual per a determinar qualsevol comportament maliciós. El sistema ha de ser capaç també de generar regles de manera automàtica en base a l'activitat observada i distribuir-les al Firewall.
- L'administrador del Sistema de Seguretat ha de poder ser capaç d'accedir a aquesta Sandbox per a veure l'estat dels fitxers inspeccionats. També ha de poder pujar fitxers a la mateixa Sandbox de manera manual per a la seva inspecció.
- S'han d'inspeccionar al menys els fitxers de tipus EXE, DLL, PDF, APK, Java, Office de Microsoft, Mach-O i DMG de OS-X.
- Inspecció de fitxers de script JScript, VBScript, and PowerShell Script
- Possibilitat de gestionar la confidencialitat, de manera que sense pujar fitxers al Sandbox, es puguin rebre de forma continua les noves defenses.
- El Sandbox ha de disposar de certificacions oficials d'organismes de defensa o països dintre de l'OTAN (SOC2, FedRAMP, ENS, ...)
- El temps de resposta del servei Sandbox ha de ser com a màxim de 5 minuts.
- El servei Sandbox ha de disposar de la capacitat d'executar les mostres en màquines 'Bare Metal' per assegurar que la mostra no faci servir sistemes d'evasió de Sandbox.

Seguretat DNS

El Firewall ha de tenir capacitat per a detectar i prevenir de manera automàtica i dinàmica les peticions de DNS malicioses associades amb dominis de 'malware', a les que el Firewall ha de respondre automàticament amb una IP falsa per comptes del servidor autoritatiu (DNS Sinkholing). La base de dades de dominis maliciosos podrà ser nodrida per les següents fonts:

- Sistema de Sandbox per a trobar nous dominis C2 (Command and Control)
- DNS passius i telemetries

4.6. Requeriments de gestió i administració

Els requeriments de gestió i administració del Firewall son:

- Funcionalitats bàsiques integrades al Firewall: Les capacitats de gestió, administració, gestió de 'logs' i informes, han de ser components nadius en el Firewall, sense necessitat d'adquirir altres elements hardware o software per a disposar d'aquestes funcionalitats.
- Ha de disposar de mecanismes per a fer auditoria de configuracions , incloent la cerca de diferències entre diferents fitxers de configuració.
- La solució ha de permetre reporting totalment personalitzable per a tots els 'logs' sobre el propi equip (sense necessitat de fer servir equips secundaris per aquestes tasques).
- Utilitzant les funcionalitats incloses, els administradors han de poder generar informes personalitzats. A més, ha de ser possible extreure tant els informes predefinits com els personalitzats a través d'una API XML que permeti la integració amb sistemes externs.
- La solució serà capaç de realitzar de manera automàtica un anàlisi de comportament diari, en base a tots els logs, en la cerca d'equips que puguin formar part de 'Botnet's' desconegudes. El resultat serà un informe que inclourà tots els equips susceptibles d'haver sigut reclutats per noves 'Botnet's' així com els comportaments que han tingut i pels quals se'ls ha considerat infectats.
- Disponibilitat del mapa geogràfic per a identificar l'origen i destí dels fluxos i amenaces que entren i surten de la xarxa.
- Capacitat per a incorporar al Firewall indicadors de compromisos maliciosos de tercers de manera automàtica (llistes de IPs, URLs i DNS).
- Actualitzacions automàtiques i programables per les regles d'Aplicació, IPS, Antivirus, AntiSpyware i Threat Prevention.

4.7. Altres requeriments

La solució proposta, haurà de disposar de mecanismes que permetin la inclusió al Firewall, de manera automàtica, de llistes dinàmiques provinents de bases de dades de tercers (serveis anti phishing, llistes de dominis maliciosos, serveis anti spamming, serveis d'identificació de nodes TOR, avisos de CERT's, etc.). Aquestes diferents fonts

d'informació hauran de ser rebudes de manera automàtica, processades i injectades al Firewall sense intervenció humana.

5. Serveis d'instal·lació, posada en marxa, migració, formació, manteniment i suport

A més dels serveis d'instal·lació, activació i posada en règim d'explotació associats al subministrament del maquinari, programari, mòduls i llicències que corresponguin per a proveir els nivells de seguretat informàtica i protecció contra ciberatacs que es requereixen pel nou Firewall de l'Ajuntament de Castellbisbal i que es relacionen al punt 4 d'aquest plec, els licitadors hauran de oferir, indicant el seu abast i valoració econòmica apart si correspon (per exemple en el cas de la migració de configuracions, regles de seguretat i de la formació), els següents serveis de migració, formació, manteniment i suport:

- Migració de configuracions i regles de seguretat:

  El règim d'explotació indicat al paràgraf anterior es considerarà assolit i certificat, un cop traslladades i verificades en el seu correcte funcionament al nou Firewall, totes les configuracions, polítiques i regles de seguretat actualment operatives a l'actual Firewall de l'Ajuntament.

  Per aquesta migració es demana la redacció d'un Pla de Migració de Polítiques i Regles de Seguretat que, en resum, contempli el següent:

  - Identificació inicial, per part del licitador, de les polítiques, regles i serveis configurats a l'entorn actual.
  - Validació per part del personal tècnic de l'Ajuntament de les dades obtingudes al punt anterior.
  - Programar un calendari de migració, consensuat entre el licitador i el personal tècnic de l'Ajuntament, que contempli els diferents ítems de les polítiques, regles i serveis a migrar, efectuant sobre els mateixos les corresponents proves de validació per part de l'Ajuntament.

- Formació al personal tècnic de l'Ajuntament relacionada amb la gestió i administració del nou Firewall. Aquesta formació haurà de ser com a mínim de 5 hores.

- Servei de manteniment i suport de la solució Firewall subministrat:

  Aquest servei inclourà tot el que pugui fer referència a les necessitats de manteniment i suport relacionades amb les incidències, avaries, recanvi de peces, actualitzacions de firmware i altres intervencions, actualitzacions, ajustos, llicències d'ús dels diferents mòduls, etc. que siguin necessàries aplicar al Firewall instal·lat per a mantenir tant la seva òptima operativitat com els nivells de protecció desitjats en front de ciberatacs.

  Aquest servei de manteniment i suport, sobre tot pel que fa a la part del suport, haurà de contemplar la possibilitat de disposar també d'un nombre d'hores de servei per a la depuració de problemes de configuració que poguessin estar provocant incidències en els serveis de seguretat que gestiona el Firewall i que no s'haguessin detectat i/o considerat en el moment en que es va fer la migració inicial.

Tots els serveis indicats en aquest punt hauran de ser completats en un termini màxim de 2 mesos des de la confirmació oficial del contracte, amb l'excepció del servei de manteniment i suport que haurà d'estar actiu durant tota la vigència del contracte.

6. Determinació del pressupost de licitació

Es valora el pressupost del contracte en la quantitat de **62.617,50 € IVA inclòs**, corresponent a **51.750,00 € de pressupost sense IVA i 10.867,50 € al 21% d'IVA**.

Aquest pressupost inclou tant les despeses directes, com les indirectes, el benefici industrial i els impostos afegits, sense que es puguin desglossar tots ells.

7. Valor estimat del contracte

La proposta de contractació és per a una durada inicial de tres (3) anys amb la possibilitat d'aplicar dues pròrrogues addicionals d'un (1) any (per tant estaríem parlant d'una contractació total de 5 anys). Per tant el valor estimat del contracte és de **82.916,67 € sense IVA (100.329,17 € IVA inclòs).**

8. Termini de lliurament

La data inicial d'aplicació del contracte que es proposa en aquest plec s'estableix pel dia **12 de desembre de 2023**.

Datat a Castellbisbal el dia de la signatura del document.

Document signat electrònicament per:
Cap de Sistemes d'Informació (Xavier Sordé De Uralde)

Av. Pau Casals, 9 | 08755 Castellbisbal | tel. 93 772 02 25 | fax 93 772 13 07 | bustia@castellbisbal.cat | www.castellbisbal.cat