PLEC DE PRESCRIPCIONS TÈCNIQUES DE LA LICITACIÓ:

"NOVA PLATAFORMA D'ACCÉS A INTERNET"

ÍNDEX

Introducció

L'Autoritat Portuària de Barcelona (APB a partir d'ara) disposa d'una plataforma de connexió a Internet per a la prestació de serveis online. Aquesta plataforma adquirida i posada en marxa fa diversos anys, no està actualitzada i alguns elements estan en discontinuïtat de millores per part del fabricant en la versió actual.

El rendiment de la plataforma ja no és suficient per proporcionar els serveis que presta amb prou qualitat. A més els costos de gestió associats a la plataforma i en concret dels de gestió delegada dels balancejadors són alts a causa de la complexitat de gestió tècnica alguns elements. La plataforma ha provocat de forma reiterada problemes de rendiment en l'accés a les web corporativa del Port i al Portal de l'Empleat de l'APB, detectant puntualment temps de resposta anormalment alts en l'accés de l'exterior, arribant en alguns casos a fer inoperatius els serveis que proporcionen.

Amb la posada en marxa de la seu digital i els serveis associats de la llei 11/2007 és necessari garantir l'accessibilitat i el rendiment donat que aquests serveis son molt crítics. És per tant necessari actualitzar aquesta plataforma per poder assumir aquests nous reptes i millorar la usabilitat dels serveis que actualment s'estan donant.

Objectius del projecte

Els objectius d'aquest projecte són, partint de la plataforma actual de connexió a Internet, dotar l'APB d'una plataforma millorada:

- ✓ Amb més rendiment.
- ✓ Amb més funcionalitats.
- ✓ Amb una administració millorada, més senzilla, que permeti reduir els costos d'administració i operació, reduint els recursos que actualment s'estan dedicant a l'administració de la plataforma. Haurà de quedar clarament reflectida en la proposta com s'aconsegueix aquest objectiu.
- ✓ Garantir el manteniment i l'actualització de versions i llicències durant tot el període temporal definit als plecs.

Situació actual

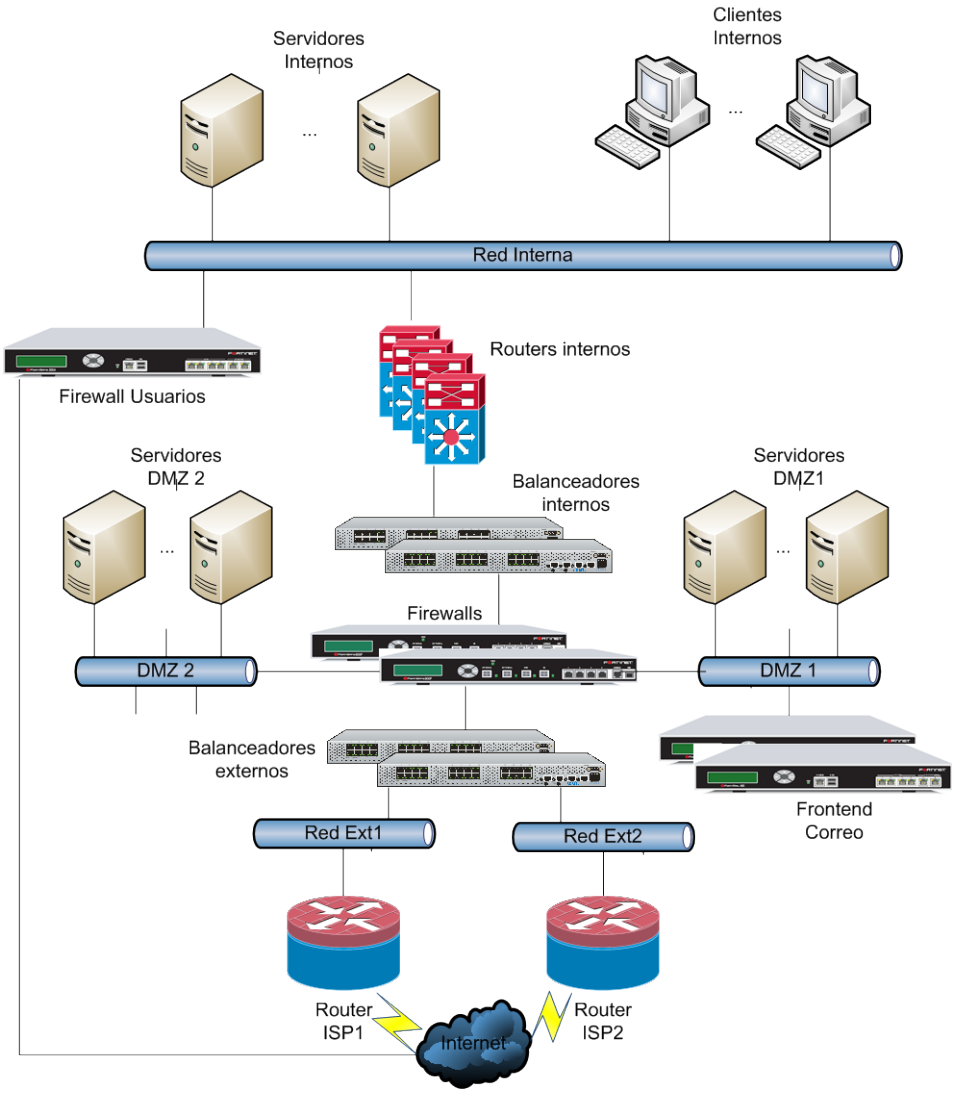
Arquitectura i components d'accés a internet

La Plataforma de connexió a Internet actual de l'APB disposa dels següents elements:

- ✓ Firewalls,
- ✓ Balancejadors de servidors i de connexions a Internet,
- ✓ Routers de connexió a ISP,
- ✓ Frontend de correu,
- ✓ Servidors DNS/DHCP.

Tots els serveis en alta disponibilitat i amb cada parella d'equips situats en sales CPD separades i interconnectats per una xarxa Gigabit Ethernet.

L'estructura de la plataforma és la següent:



Il·lustració 1 Esquema d'accés a internet

L'APB disposa actualment de quatre balancejadors Nortel Alteon 2224 agrupats en dos parells configurats en alta disponibilitat mitjançant VRRP. Cada parell proveeix les següents funcionalitats.

Balancejadors interns:

- ✓ Balanceig de càrrega i alta disponibilitat de servidors Interns per a connexions entrants de clients interns i Internet.
- ✓ Balanceig de càrrega i alta disponibilitat de servidors de les dues DMZs per a connexions entrants de clients interns.

Balancejadors externs:

- ✓ Balanceig de càrrega i alta disponibilitat de servidors de les dues DMZs per a connexions entrants des de clients externs.
- ✓ Balanceig de connexions sortints a través dels dos proveïdors de connexió a Internet.
- ✓ Balanceig de connexions entrants a través dels dos proveïdors de connexió a Internet, per a serveis específics (Web, Correu, etc.).

El control d'accés es fa a dues bandes. Primer en els routers-firewall de connexió amb l'ISP (propietat de l'APB) i després en el firewall central situat entre els dos parells de balancejadors. Internament s'utilitza direccionament IP privat i són els routers de connexió a Internet els qui s'encarreguen de fer la traducció de direccions (NAT).

Els Firewalls centrals són dos FortiGate 800 en alta disponibilitat i proporcionen les següents funcionalitats:

- ✓ Separació de seguretat entre zona externa, interna i les tres DMZs.
- ✓ Antivirus perimetral
- ✓ IDS i IPS.
- ✓ Control de continguts en l'accés a Internet.
- ✓ Gestió de VPNs de xarxa a xarxa.
- ✓ Concentrador VPNs IPsec i SSL per a accés remot.
- ✓ Integració del control de continguts i accés amb el Directori Actiu de Microsoft.

El firewall d'usuaris s'utilitza principalment per desviar tot el tràfic de navegació web dels usuaris a una connexió a Internet dedicada per evitar que aquest afecti el tràfic de servidors. Tot el tràfic d'usuaris cap a internet va autenticat contra el Directori Actiu 2008 corporatiu utilitzant l'usuari autenticat al PC client. Addicionalment per a usuaris externs, les màquines dels quals no són dins de domini o no poden utilitzar aquest tipus d'autenticació, existeix un Servidor Intermediari HTTP instal·lat en una màquina en el segment de servidors que realitza l'autenticació amb els mecanismes estàndard de HTTP, i valida contra el nostre directori actiu. El trànsit d'aquest servidor intermediari també és desviat pel firewall d'usuaris.

Els routers externs són dos CISCO 2821 i el Routing intern es fa des d'un core de quatre CISCO 6500 en alta disponibilitat per VRRP.

De la DMZ 1 pengen dos Fortimail 400 en alta disponibilitat que realitzen la funcionalitat de Frontend de correu SMTP i AntiSpam.

De la DMZ 1 pengen també tres equips Infoblox 550 en una configuració d'un clúster entre dos i un tercer equip amb funcionalitats de redundància. Proporcionen les funcionalitats de DNS primari i secundari tant intern com a extern, DHCP Intern tant per a PC's com per a telèfons IP CISCO, i servidor NTP central per a tota la infraestructura, sincronitzat contra servidors externs.

Serveis proporcionats actualment per la plataforma

Els Serveis que actualment es presten amb la plataforma són:

- ✓ Accés al web corporatiu. Actualment és un web d'informació corporativa principalment. Té un total d'aproximadament 20.000 visites mensuals. No es tenen dades d'accessos màxims concurrents. Es considera vital la seva disponibilitat per l'impacte en la imatge corporativa. Està muntat sobre el portal Liferay.
- ✓ Accés a la Seu corporativa. És un portal amb registre telemàtic muntat sobre el Portal i BPM de Polymita.

- ✓ Accés al portal de l'empleat. És un portal de serveis interns per a empleats de l'APB amb accés interior i exterior muntat sobre Websphere Portal.
- ✓ Accés a correu corporatiu via Web. Suposa un accés via web a la plataforma de correu Domino. L'accés normal és a través de del Portal de l'empleat, però també existeix un accés directe.
- ✓ Connexió VPN SSL per a accés tant d'usuaris interns, com de proveïdors externs.
- ✓ Servei balancejat de LDAP. Aquest servei d'autenticació és crític per al funcionament de moltes aplicacions internes.
- ✓ Accés a internet d'usuaris amb control antivirus i d'aplicacions/continguts.
- ✓ Intercanvis documentals entre l'APB i tercers, com la Duana, Consignataris, Empreses Estibadores, etc.

Especificacions del sistema a implantar

Abast del projecte

El projecte es considera "claus en mà", per la qual cosa s'hauran de tenir en compte totes les unitats d'obra necessàries, per complir amb tots els requeriments que es sol·liciten en aquest plec tècnic.

L'abast del projecte contemplarà com a mínim els següents apartats:

- ✓ Proposta global d'arquitectura, que contempli la interconnexió de tots els elements, i la integració amb els sistemes de l'APB descrits en aquest plec tècnic. El projecte està obert al plantejament de qualsevol arquitectura que compleixi amb els requisits tècnics i funcionals establerts al plec.

- ✓ Solució tècnica de balanceig. Subministrament i instal·lació dels equips necessaris per substituir les dues parelles de balancejadors:
  - Sense perdre cap de les funcionalitats actuals del sistema, i sense que el desplegament de la nova plataforma afecti la disponibilitat del sistema actual. (la nova plataforma requereix també d'alta disponibilitat)
  - Millorar el rendiment i la gestió segons especificacions tècniques.

- ✓ Solució tècnica de seguretat. Subministrament i instal·lació d'un sistema de Firewall:
  - En alta disponibilitat que garanteixi totes les funcionalitats actuals, i sense que el desplegament de la nova plataforma afecti la disponibilitat del sistema actual.
  - Millorar el rendiment i la gestió segons especificacions tècniques.

- ✓ Solució tècnica d'antispam. Es mantindran els equips actuals que s'hauran d'integrar amb la nova plataforma, que s'hauran d'actualitzar a l'última versió de firmware disponible suportada pels equips existents.

- ✓ Solució Tècnica de servidor DNS/DHCP. Subministrament i instal·lació d'un sistema de gestió DNS i DHCP:
  - En alta disponibilitat que garanteixi totes les funcionalitats actuals i sense que el desplegament de la nova plataforma afecti la disponibilitat del sistema actual.
  - Millorar el rendiment i la gestió segons especificacions tècniques.

- ✓ Renovació dels routers d'accés a internet (actuals CISCO 2821), en alta disponibilitat. Subjectes a les condicions de manteniment que especifica el plec.

- ✓ Proposta d'un sistema WAF (Web aplication server), que analitzi el tràfic web (entre el servidor web i la WAN), i les dades rebudes per part de l'usuari. Haurà de protegir de diferents atacs web com: SQL Injection, Cros Site Scripting, Remote and Local File Inclusion, Buffer Overflows, Cookie Poisoning, etc. Aquest dispositiu, prova de protegir dels atacs dirigits al servidor web que els IDS/IPS no poden defensar.

- ✓ Proposta d'una eina de recol·lecció i anàlisi de logs, que haurà de contemplar l'elaboració d'informes i reports a partir de la informació recollida.

- ✓ Interfície d'integració amb el sistema de monitoratge Tango/04
  - L'objectiu és integrar la plataforma d'accés a Internet amb l'actual sistema de gestió de l'APB basat en l'eina Visual Message Center de l'empresa Tango/04 Computing Group.

- ✓ Proposta de migració de serveis i funcionalitats. Traspàs de totes les configuracions i regles dels equips actuals als nous equips que s'instal·lin, incloent, regles de balanceig, firewall, integracions amb LDAP i directori actiu, i configuracions específiques del correu. S'haurà d'incloure la reconfiguració de les polítiques i configuracions per aprofitar el màxim potencial de la nova plataforma.

- ✓ Subministrament i instal·lació de programari de gestió i aplicacions necessàries associades a la plataforma. El sistema haurà de ser capaç de guardar i generar informes d'ús i connexions establertes pels diferents sistemes i usuaris de cara a poder fer un seguiment i auditoria de l'ús de la connexió a Internet.

- ✓ Subministrament i instal·lació d'elements accessoris necessaris (ancoratges, cablat de dades i alimentació, cargols, etc.) per a la seva instal·lació en racks estàndards de 19".

- ✓ Reconfiguració de l'equipament de routing, firewall, i antispam existent en cas de ser necessari.

- ✓ Realització de proves de rendiment de la plataforma per a connexions de l'interior i de l'exterior.

- ✓ Documentació de la instal·lació.
- ✓ Curs de Formació per a administradors i operadors.
- ✓ Garantia especial de 5 anys, que inclourà el servei d'assistència tècnica. A l'adjudicatari del concurs s'haurà de fer càrrec del manteniment de tots aquells components de la plataforma actual que no siguin substituïts (CISCO2821, CISCO 1812, etc.). Veure Annex 2.

Requisits de prestacions

Tots les característiques requerides dels diferents sistemes seran d'obligat compliment. Les característiques desitjables no seran d'obligat compliment però es valoraran especialment. Les característiques tècniques de disseny, de rendiment, i de funcionalitat de la nova plataforma hauran de ser les següents:

Arquitectura de la solució proposada:

Característiques requerides

- ✓ Alta disponibilitat. Tots els elements hauran de garantir la màxima disponibilitat del sistema. S'haurà d'explicar l'operativa del balanceig en cas de fallada o incidència. S'haurà de proporcionar temps de balanceig entre elements, i d'indisponibilitat del servei.
- ✓ Cada parella d'equips en alta disponibilitat han de poder sincronitzar-se per LAN, i estaran ubicats en sales i edificis diferents. S'haurà d'explicar el model de configuració i funcionament, així com les prestacions.
- ✓ La plataforma ha d'estar dimensionada per suportar com a mínim 600 usuaris interns en l'accés al Portal i 3000 externs en l'accés a web corporatiu i Seu Digital. S'haurà de proporcionar les prestacions màximes a arribar per la plataforma proposada sota uns requisits de maquinari i configuració concrets.
- ✓ La de gestió de tota la solució ha de ser intuïtiva i fàcil. Per a la seva valoració s'hauran de lliurar els manuals d'ús de cada una de les plataformes de gestió a implementar. La no justificació detallada d'aquest apartat deixarà sense valor aquesta prestació.
- ✓ Tota l'arquitectura haurà de suportar IPV6.

Característiques desitjables

- ✓ Es permeten variacions en l'arquitectura de xarxa. Tenint en aquestes variacions que els sistemes han de ser els menys intrusius possibles i han d'afectar el mínim possible al tràfic de xarxa. Es valorarà la possibilitat que els balancejadors no s'hagin de posar en "línia" amb la resta de tràfic que no és balancejat tal com són ara
- ✓ Es valorarà en tots els casos l'escalabilitat en nombre d'usuaris i accessos simultanis de la solució per sobre del dimensionament mínim requerit.
- ✓ Es podran proposar arquitectures que eliminin la necessitat del firewall d'usuari, però com a opció alternativa, si bé seran valorades. Detallar avantatges i inconvenients d'aquesta proposta.

- ✓ Es valorarà la gestió unificada des d'una única consola de tota la solució. En els casos de parelles d'equips en alta disponibilitat es valorarà que es puguin configurar com un només equips sense necessitat de replicar a mà la configuració entre els diversos nodes.

Solució de balancejadors.

Característiques requerides

- ✓ Alta disponibilitat.
- ✓ Capacitat per suportar un mínim de 2 Gbps de throuput global i 500 CPS.
- ✓ Suport d'acceleració SSL
- ✓ Hauran de poder funcionar fora de línia (Mode Proxy) i donar servei a més d'una subxarxa amb el mateix equip.
- ✓ La gestió ha de ser intuïtiva i de poder realitzar-se remotament.
- ✓ Capacitat de balanceig per protocol (Nivell 7).
- ✓ Capacitat de gestió de la disponibilitat dels servidors amb sondes complexes (disponibilitat del servei, nombre de connexions, càrrega del servidor, etc.).
- ✓ Capacitat per mantenir la sessió en diferents protocols. És especialment important en els protocols HTTP i HTTPS, on haurà de suportar els diversos mecanismes de sessió més típics utilitzats per aquests protocols (cookies, sessió aneu, etc.). S'haurà de detallar que mecanismes de manteniment de la sessió suporten els equips.

Característiques desitjables

- ✓ Es valorarà que sigui unificada per a cada parella d'equips. S'haurà d'explicar en detall com es realitza aquesta gestió.
- ✓ Es valorarà que sigui virtualitzable podent repartir els ports i capacitats del mateix entre diversos balancejadors virtuals.
- ✓ Es valorarà que l'equip suporti la captura de tràfic no només per port (port-mirroring) sinó també per sessió.

Solució tècnica de seguretat. Firewalls.

Característiques requerides

- ✓ Alta disponibilitat per a la parella de firewalls central.
- ✓ Capacitat de gestió de tràfic mínima de 2Gbps en tràfic de firewall.
- ✓ Gestió intuïtiva i unificada per al clúster. S'haurà de poder gestionar tot el clúster com un únic equip des del punt de vista de la gestió. S'haurà d'explicar en detall com es realitza aquesta gestió.
- ✓ Control antivirus.
- ✓ IDS i IPS
- ✓ Gestió de continguts integrada amb el directori actiu. Els usuaris hauran de poder autenticar-se al firewall utilitzant les credencials obtingudes en accedir al Directori Actiu mitjançant SSO entre el Directori Actiu i el Firewall.
- ✓ Control avançat de protocols. El firewall haurà de poder detectar no només el protocol si no també quina aplicació corre sobre la sessió i realitzar un control sobre ella.
- ✓ VPNs IPsec LAN to LAN.
- ✓ VPNs SSL per a l'accés d'usuaris remots.

Característiques desitjables

- ✓ Es valorarà la interoperabilitat de l'accés VPN amb dispositius mòbils de diferents plataformes. S'hauran d'especificar que plataformes són suportades i quins requisits tenen (si són suportades de forma nativa o requereixen algun programari addicional, etc.).

Solució Tècnica de servidor DNS/DHCP

Característiques requerides

- ✓ Alta disponibilitat.
- ✓ Compatibilitat del DNS amb Microsoft Directori Actiu.
- ✓ Possibilitat de crear vistes diferenciades del DNS segons la IP origen de la consulta.
- ✓ Haurà de disposar d'un sistema per a gestió de direccionament IP.
- ✓ Gestió intuïtiva i unificada per al clúster. S'haurà d'explicar en detall com es realitza aquesta gestió.

Routers d'accés a Internet

Característiques requerides

- ✓ Funcionalitats de Firewall bàsiques.
- ✓ Funcionalitats de NAT per separar el direccionalment intern de l'extern proporcionat per l'ISP. S'haurà de dimensionar per suportar NAT dinàmic per als 700 usuaris interns mitjançant NAT/PAT i NAT estàtic per a uns 200 servidors amb IPv4.
- ✓ Capacitat de procés per suportar línies de connexió a Internet de 100Mbps amb totes les funcionalitats actives.

Integració amb el sistema de monitoratge i gestió de serveis de negoci de l'APB

El sistema permetrà el monitoratge de forma remota dels equips de comunicacions i equips centrals a través de l'eina Visual Message Center de Tango04 existent al Port de Barcelona. S'hauran de monitoritzar com a mínim els següents elements

- ✓ Appliances
- ✓ Equips de comunicacions
- ✓ BBDD
- ✓ Aplicacions i serveis

S'ha de contemplar com a mínim la realització de les següents tasques en relació amb l'aplicació Visual Message Center:

- ✓ Creació i personalització de monitors i dashboard del sistema de monitoratge.
- ✓ Modelització del servei a monitoritzar.
- ✓ Definició i creació alarmes del sistema a monitoritzar.
- ✓ Subministrament de llicències del producte de monitoratge en cas que sigui necessari.
- ✓ Les necessitats funcionals concretes a disposar en l'aplicació Visual Message Center es definiran amb l'APB una vegada adjudicat el projecte.

Per a més informació sobre el sistema de monitoratge consultar l'Annex 1 de les especificacions tècniques.

Gestió i execució del projecte

El pla d'implantació per a aquest projecte contemplarà com a mínim les següents fases:

Elaboració projecte executiu

Una vegada comunicada l'adjudicació del contracte, l'adjudicatari disposarà de 15 dies naturals per lliurar a l'APB un document de Projecte Executiu. Durant l'elaboració d'aquest, l'adjudicatari donarà visibilitat als responsables de l'APB de l'avanç de la redacció del mateix.

Una vegada rebut el Projecte Executiu, aquest es sotmetrà a l'anàlisi i validació per part de l'APB, que indicarà les propostes de modificacions que consideri convenients. Una vegada comunicades les esmenes, l'adjudicatari disposarà de 7 dies naturals a fi d'incorporar les modificacions corresponents.

El projecte executiu inclourà entre d'altres:

- ✓ Definició dels equips de treball i el model de relació amb l'APB:
  - Definir els interlocutors vàlids per a cada tasca i cada fase del projecte
  - Establir una planificació de reunions de seguiment
- ✓ Disseny final de la solució tècnica, haurà de proposar una arquitectura tècnica detallada que contempli la integració amb els sistemes de l'APB. Es tractarà d'adaptar la proposta d'arquitectura realitzada en l'oferta a l'estat de l'art vigent en l'APB.
- ✓ Proposta migració, revisió i millora de la configuració de la plataforma.
- ✓ Proposta de detall de la documentació de la plataforma a realitzar.
- ✓ Planificació de la instal·lació, desplegament, i configuració dels sistemes.

Una vegada validat el projecte executiu s'iniciaran els treballs d'implementació dels sistemes dissenyats, segons la planificació establerta.

Migració de la plataforma. Revisió i millora.

S'haurà de realitzar un treball previ d'anàlisi de la configuració de la plataforma actual, en la qual s'hauran d'incloure detalls i especificacions des del punt de vista de topologia i funcional de la plataforma en el seu conjunt, incloent detalls sobre possibles millores a implantar durant la migració en el que a canvis de topologies o manera de funcionament dels equips es refereix.

Aspectes generals de la plataforma

- ✓ Definició d'una topologia de la plataforma partint de la situació actual, incloent la descripció funcional de la plataforma.
- ✓ Detallar les possibles millores a introduir en l'esmentada topologia en funció de l'equipament a instal·lar, amb l'objectiu de simplificar i fer més eficient la topologia en la mesura possible.
- ✓ Descripció tècnica de les millores a introduir quant a funcionalitat i implementació de les mateixes es refereix.

Aspectes específics dels diferents elements de la plataforma

Referent als diferents elements de la plataforma, es demanarà el següent:

- ✓ Revisió i avaluació dels perfils/polítiques de seguretat configurats als firewalls de la plataforma. Optimització, neteja i reorganització de les regles en funció dels perfils de seguretat proposats.
- ✓ Revisió dels serveis de balanceig (SLB i Link Load Balancing) configurats en els balancejadors de càrrega, incloent, si fos necessari, una optimització de les funcionalitats suportades pels balancejadors, com per exemple health check avançat per a determinats serveis o la utilització de balanceig Layer7.
- ✓ Adequació de la configuració dels serveis balancejats, eliminant de l'esmentada configuració qualsevol element (servei, filtre, servidor, etc) que sigui prescindible.
- ✓ Revisió i optimització de les regles d'accés i polítiques d'inspecció configurades en els routers d'accés a Internet de la plataforma.
- ✓ Implementació, si fos necessari, de les millores en la topologia comentades en l'apartat anterior (4.2.1. Aspectes generals de la plataforma)
- ✓ Sempre que sigui possible, els treballs comentats en aquest apartat s'haurien de realitzar prèviament a la posada en producció dels diferents elements de la nova plataforma.

Instal·lació i configuració de la plataforma d'accés a Internet

Inclou com a mínim, les següents tasques:

- ✓ Implementar la infraestructura necessària per a la plataforma d'accés a internet:
  - Instal·lació i configuració del maquinari proporcionat.
  - Instal·lació i configuració del programari proporcionat.
- ✓ Recopilar i revisar la política de seguretat del sistema actual
- ✓ Configurar les polítiques de seguretat aprovades per l'APB
- ✓ Configuració de sistemes addicionals. En cas de ser necessària la reconfiguració d'algun dels sistemes existents en l'APB, el proveïdor serà el responsable de realitzar les esmentades tasques prèvia autorització del personal tècnics de l'APB.

Monitoratge del sistema de backup. L'APB disposa del programa Tango04 per al monitoratge dels seus sistemes. S'haurà de proporcionar la informació i configuració necessàries per al monitoratge del nou sistema de backup amb Tango04. Aquest monitoratge haurà de permetre veure si l'operativa de backup ha finalitzat correctament cada dia.

Entorn de proves i validació

Definir un entorn i un pla de proves dels elements, com a pas previ a la posada en producció. Aquest entorn de proves permetria provar els diferents elements en el seu conjunt o separadament.

S'hauran de realitzar proves de forma unitària i/o conjunta dels elements de la plataforma.

- ✓ Proves de rendiment segons especificacions plec
- ✓ Proves funcionals
- ✓ Validació final del sistema

Pas a producció de la plataforma

El licitador haurà de definir una proposta de pas a producció de la plataforma, explicant per a cada fase les accions a realitzar i l'afectació prevista del servei.

Documentació

En aquest apartat s'inclourà una documentació de la plataforma, que hauria d'incloure el següent:

- ✓ Documentació d'administració i "polítiques" implantades.
  - Esquemes de la topologia física/lògica de la plataforma
  - Documentació de gestió/administració dels diferents equips. Manuals d'usuari de cadascun dels equips subministrats.
  - Documentació de les polítiques/perfils de seguretat implementats als firewalls de la plataforma, partint de l'avaluació i revisió de les polítiques/perfils de seguretat comentats en el punt 1.2. S'haurien de referenciar, en la mesura dels possible, les regles de firewall associades als diferents perfils/polítiques.
  - Documentació dels serveis balancejats en els balancejadors de càrrega, incloent SLB, Link Load Balancing, Bandwidth Management i comentaris de les particularitats de cada servei configurat.
  - Documentació de la integració dels equips de la plataforma amb els diferents serveis amb els quals interactua, com per exemple l'accés al web públic del Port de Barcelona o a la Intranet de l'APB. Aquesta documentació, o alguna part d'ella, hauria d'incloure's o enllaçar-se amb la documentació sobre els diferents serveis afectats existent en l'APB.

- ✓ Manual d'explotació contenint el següent:
  - Diagrama de blocs
    - Equips/servidors instal·lats i configurats amb el seu nom i adreça IP. S'hauran d'incloure també els elements virtuals que s'hagin configurat amb el projecte tals com serveis balancejats, etc.
    - Programari instal·lat a cada màquina
    - Flux de dades/dependències entre els elements del sistema
  - Llistat de programari amb les seves versions.
  - Requisits de programari del sistema Base (Plataforma del sistema operatiu, versió sistema operatiu, programari necessari- Apatxe, Oracle, 32/64bits- etc.)
  - Requisits de maquinari del sistema (Memòria, # CPUs, # Discos, espai de cada unitat de disc).
  - Document de configuració (amb l'explicació de la instal·lació i configuració de tots els elements)
  - Troubleshooting. Procediment de detecció d'avaries per resoldre incidències i com resoldre'ls per a cadascun dels equips subministrats
  - Procediments d'arrencada i parada
  - Procediment de Backup (en calent)
  - Procediments d'administració. (gestió d'usuaris/permisos, Gestió de recursos, revisions, neteja de fitxers, etc.)
  - Monitoratge.

- ✓ Protocol d'avís d'avaries dins de la garantia o manteniment amb telèfons horaris, etc.
- ✓ Proposta del protocol de proves d'acceptació de la instal·lació.

Tota la documentació que lliuri l'adjudicatari una vegada finalitzada la instal·lació tindrà una còpia electrònica en CD i en format WORD, a excepció de plans i esquemes que serà en format VISIO.

La documentació es lliurarà a l'APB en format electrònic sense protegir. Els formats admesos són:

- ✓ Word: Documents de text + gràfics
- ✓ Visio: Diagrames de bloc

A excepció dels manuals originals dels fabricants (que podran ser en idioma castellà, anglès o francès), la resta de la documentació vindrà necessàriament en català o castellà.

Pla de formació

S'hauran de crear dues tipologies de formació una de destinada al suport de HelpDesk del que s'hauran de proposar dos torns amb l'objectiu que la gent de Helpdesk pugui assumir el concepte de l'arquitectura del sistema i les operacions que hagin de realitzar com a primer nivell de suport.

El segon tipus de curs estarà destinat als administradors del sistema. Aquesta de formació haurà de ser de tipus pràctic i prenent el manual d'explotació que es lliurarà en la documentació del projecte i plataforma instal·lada, com guia i manual del curs.

Els cursos s'impartiran, en català (o castellà), a les dependències de l'APB que es determinessin, per personal amb experiència, coneixements i titulacions requerides per a una activitat d'aquest tipus.

Per a cada un dels cursos s'indicarà:

- Durada.
- Torns: mati i tarda.
- Mitjans didàctics i documentals.
- Planificació.

En tots els casos la formació serà presencial i serà donada a les oficines de l'APB, que es farà càrrec de proporcionar la infraestructura necessària (aula, equips, etc.).

Projecte tancat "claus en mà"

El projecte de la nova plataforma d'accés a Internet és considerat per l'APB com un projecte "claus en mà" per part de l'adjudicatari, que es responsabilitzarà de proporcionar tots els productes i serveis sol·licitats sense cap cost addicional al de l'adjudicació.
L'adjudicatari a més, haurà de gestionar el manteniment dels productes i les seves renovacions dins del termini establert pel contracte, en cas de ser necessari.
L'adjudicatari no carregarà a l'APB els costos d'utilització de cap eina utilitzada en el transcurs del projecte, tant per a la migració dels equips, com per a la implantació de la resta de sistemes i la seva gestió.

Pla de seguretat i salut

L'adjudicatari haurà d'assumir els costos derivats de les tasques relatives a l'elaboració i validació del Pla de Seguretat i Salut per a l'execució del projecte. L'adjudicatari s'haurà d'adaptar a les normatives de Seguretat i Salut indicades per l'APB per a la implantació dels diferents sistemes.

L'Adjudicatari designarà un Coordinador de Seguretat i Salut del Projecte que serà l'encarregat de gestionar, controlar i exigir a tot el personal que treballi en el projecte tot el que sigui d'aplicació en el disposat en la llei 31/95 de Prevenció de Riscos Laborals i en el R.D. 1627/97 de disposicions mínimes de Seguretat i Salut a les obres.

El coordinador en matèria de seguretat i salut, durant l'execució de les obres, haurà de desenvolupar, com a mínim, les següents funcions:

- ✓ Coordinar l'aplicació dels principis Generals de Prevenció i de Seguretat:
- ✓ Prendre les decisions tècniques i d'organització amb la finalitat de planificar els diferents treballs o fases de treballs que es vagin a desenvolupar simultàniament o successivament.
- ✓ Preveure la durada requerida per a l'execució dels diferents treballs o fases de treballs.
- ✓ Coordinar les activitats de l'obra per garantir que els contractistes i en el seu cas els subcontractistes i els treballadors autònoms, apliquin de manera lògica i responsable els principis de l'acció preventiva que s'indiquen a l'article 15 de la Llei de Prevenció de Riscos Laborals durant l'execució de l'obra i, en particular en les tasques o activitats a què es refereix l'article 10 del reial decret 1627/1997, del 24 d'octubre BOE núm. 256 del 25 d'octubre.

- ✓ Aprovar el Pla de Seguretat i Salut redactat pel contractista i en el seu cas les modificacions introduïdes pel mateix.
- ✓ Organitzar la coordinació d'activitats empresarials previstes a l'article 24 de la Llei de Prevenció de Riscos Laborals.
- ✓ Coordinar les accions i funcions de control de l'aplicació correcta dels mètodes de treball.
- ✓ Adoptar les mesures necessàries perquè només les persones autoritzades puguin accedir a l'obra.
- ✓ Responsabilitzar-se del llibre d'incidències i tramitar una còpia de qualsevol incidència reflectida, en un termini inferior a les 24 hores, a la Inspecció de Treball i Seguretat Social de la província on es realitza la instal·lació, segons indica el reial decret citat.
- ✓ Realització d'informes de seguiment setmanals en matèria de Seguretat i Salut, on es faran constar les visites d'obra realitzades, l'estat de les mateixes i les mesures correctores aplicades si n'hi hagués.

Annexo 1 Monitoratge amb l'eina Tango/04

Requisits de la integració amb l'eina Tango/04

A continuació es detallen les característiques i protocols d'integració de l'aplicació Visual Message Center.

Visual Message Center disposa de diversos agents pre empaquetats per monitoritzar sistemes, dispositius o aplicacions, per als quals en molts casos l'única informació que es necessita introduir són els paràmetres de connexió (IP, usuari, contrasenya, etc.):

- ✓ Maquinari
- ✓ HP Insight Manager.
- ✓ IBM Director.
- ✓ Dispositius de xarxa Cisco.
- ✓ Sistemes operatius
- ✓ OS/400.
- ✓ Microsoft Windows.
- ✓ Linux en les seves diverses distribucions (RedHat, Mandrake, Suse, etc.).
- ✓ Oracle Solaris.
- ✓ AIX.
- ✓ HP-UX.
- ✓ VMWare ESX.
- ✓ Aplicacions i bases de dades
- ✓ Microsoft SQL Server.
- ✓ Oracle.
- ✓ IBM Websphere Application Server.
- ✓ VMWare.

Visual Message Center permet rebre esdeveniments d'aplicacions de tercers així com monitoritzar productes de tercers. Per a això, Visual Message Center proporciona una interfície de programació d'aplicació (API) que permet a qualsevol aplicació inserir un esdeveniment en la base d'esdeveniments de la SmartConsole. Per cridar a aquesta API basta amb què l'aplicació de tercers sigui capaç d'executar un comando DOS en un servidor Windows on sigui configurat l'accés a la base de dades de Tango/04 (habitualment un DSN).

El sistema Visual Message Center permet integrar o monitoritzar aplicacions de tercers directament a través dels monitors de ThinkServer, que utilitzen els següents mètodes per capturar la informació:

- ✓ Recepció de traps SNMP (Agent SNMP Traps).
- ✓ Recepció de missatges via TCP o UDP Syslog (Agent Syslog).
- ✓ Lectura de valors mitjançant SNMP (Agent SNMP).
- ✓ Lectura de valors guardats en bases de dades utilitzant ODBC (Agent Data Adapter).
- ✓ Lectura de fitxers de text pla en format ANSI (Agent Log Reader).
- ✓ Lectura de fitxers o de URLs en format XML (Agent XML).
- ✓ Recepció i interpretació de correus electrònics dirigits a un compte de lectura exclusiva per part de Tango/04 (Agent POP3 Correu).
- ✓ Lectura de valors mitjançant el protocol WMI per a aplicacions Microsoft (Agent WMI genèric).

- ✓ Lectura de missatges d'aplicació registrats en el "log" estàndard del sistema operatiu:
- ✓ Eventlog (Windows).
- ✓ Syslog (Unix).
- ✓ QSYSOPR, Log HST (iSeries).

VISUAL Message Center incorpora dos agents capaços de gravar i executar transaccions complexes per obtenir temps de resposta globals, de cada pas, èxit o fracàs de la transacció etc.

- ✓ Transaccions web (HTML no dinàmic): L'agent WTA (Web Transaction Agent) és capaç de registrar i reproduir transaccions web navegant per pàgines HTML sense elements dinàmics. Aquest agent processa directament els comandos HTML.
- ✓ Transaccions genèriques: Per a les pàgines web que incloguin elements dinàmics, o per a qualsevol altra aplicació Windows (que pot executar-se remotament en altres sistemes com iSeries o Unix) existeix l'agent UTA (Universal Transaction Agent). Aquest agent és un agent gràfic, que memoritza els moviments del ratolí per la pantalla, les entrades des del teclat i és capaç de comprovar àrees rectangulars de la pantalla per comprovar-les amb el resultat esperat de la transacció.

En el mòdul SmartConsole es poden configurar alarmes que es disparen davant de la recepció d'un esdeveniment, la no recepció d'un esdeveniment en un calendari determinat o la correlació de diversos esdeveniments. Les accions que poden executar aquestes alarmes són:

- ✓ Enviar un correu.
- ✓ Reproduir un so.
- ✓ Executar un comando DOS.
- ✓ Escriure en el Windows Event Log.
- ✓ Enviar una Trap SNMP.
- ✓ Executar un comando en un servidor iSeries.
- ✓ Respondre a un missatge de pregunta d'un servidor iSeries.
- ✓ Enviar un missatge SMS.
- ✓ Enviar correus i/o missatges SMS mitjançant llistes d'escalat.

Mitjançant el mòdul d'alarmes de la SmartConsole, Tango/04 pot enviar esdeveniments a aplicacions de tercers, utilitzant les APIs d'integració que proporcioni el fabricant de les esmentades aplicacions. Com a alternativa, també es poden utilitzar els següents mètodes:

- ✓ Tramesa d'e-mails que rebrà una bústia de l'aplicació externa.
- ✓ Tramesa de SMS.
- ✓ Tramesa de Traps SNMP.
- ✓ Escriptura de fitxers de text pla.

Respecte a la interfície d'integració amb el sistema de monitoratge i gestió de serveis de negoci de l'APB se sol·licita el següent:

- ✓ El sistema permetrà el monitoratge de forma remota dels equips de comunicacions i equips centrals a través de l'eina Visual Message Center existent al Port de Barcelona.
- ✓ Monitoratge dels equips centrals:
  - o Sistemes basats en W2008R2: monitoratge mitjançant WMI.

- Sistemes basats en Suse Linux 11: monitoratge mitjançant SSH.
- Sistemes basats en caixes negres: monitoratge mitjançant protocols i connectors estàndard suportats segons especificacions d'aquest mateix document.

Monitoratge dels equips de comunicacions:

- ✓ Basat en protocol SNMP (càrrega de CPU, temperatura, ús de memòria i estat i ús de les interfícies).

El conjunt d'alarmes detallades incloses en el sistema de gestió Visual Message Center serà definit conjuntament amb l'Autoritat Portuària una vegada adjudicat el projecte. Encara així, s'ha de facilitar una proposta general d'alarmes en l'oferta.

La integració realitzada ha de permetre accedir a eines de suport als usuaris del sistema:

- ✓ El sistema ha de permetre la generació d'informes per hora/dia/setmana/mes:
- ✓ Per tipus d'esdeveniment / alarma: crític, no crític, d'altres.
- ✓ Gestió de recursos assignats.
- ✓ Llistat d'inventari i dispositius del sistema amb característiques bàsiques: versió de programari, tipus de dispositiu, etc.
- ✓ D'altres.

El sistema ha de permetre l'extracció de dades estadístiques d'incidències:

- ✓ Filtres per tipus d'incidència.
- ✓ Recerca per nom, tipus d'incidència, recursos assignats, ...
- ✓ Resum d'incidències.
- ✓ Etc.

Els licitadors del present concurs hauran d'incloure en les seves propostes la realització de les modificacions necessàries en l'aplicació Visual Message Center amb la finalitat de personalitzar / parametritzar per als usuaris del sistema (tècnics de sistemes i administrador de xarxa).

S'ha de contemplar com a mínim la realització de les següents tasques en relació amb l'aplicació Visual Message Center:

- ✓ Creació i personalització del dashboard de gestió d'alarmes per als usuaris del sistema.
- ✓ Gestió i alta de nous perfils i usuaris.
- ✓ Modificació de llicències en cas que sigui necessari.
- ✓ Gestió de permisos d'accés.
- ✓ Creació d'informes estadístics preconfigurats per als usuaris del sistema.
- ✓ Possibilitat de creació d'informes personalitzats per part dels usuaris del sistema.
- ✓ Parametrització a base de menús gràfics.
- ✓ Accés a procediments operatius i protocols de contingència.
- ✓ Creació d'alertes i indicadors.
- ✓ Les necessitats funcionals concretes a disposar en l'aplicació Visual Message Center es definiran amb l'APB una vegada adjudicat el projecte.

El sistema ha de ser fàcilment escalable quant a senyals a integrar a la gestió, elements a controlar, usuaris i perfils.

Els licitadors hauran d'aportar totes les ampliacions de llicències, maquinari i programari necessaris per permetre la integració en el sistema Visual Message Center

Annex 2. Inventario sistemes de seguretat i accés a internet

FABRICANT	MODEL	DESCRIPCIÓ	DIMENSIONAMENT	TIPOLOGIA
Nortel	EB1412011	Alteon 2224	4	Balancejador
Nortel	AA1419014	1 port 1000BaseX MiniGbic MT-RJ	4	N.A.
CISCO	CISCO 2821 (ADVSECURITY-K9)	CISCO 2821 (amb IOS ADVSECURITY-K9)	2	Router
Fortinet	FE-400-B	Fortimail 400 10/100/1000	2	Analitzador correu / Antispam
Fortinet	FG-800-BDL-X	FortiGate-800 Bundle 4 10/100/1000 ports, 4 user-definable 10/100 ports	2	Firewall
Fortinet	FG-300A-BDL-X	FortiGate-300 A Bundle 2 GE and 4 10/100 ports	1	Firewall
Infoblox	IB-550-DNS-04	Infoblox-550 with DNSone Package, EUR Power cord	3	Servidor DNS/DHCP/NTP