Plec de prescripcions tècniques per a l'adquisició d'un sistema tallafoc redundat pel centre dades del CSUC

Barcelona, 19 de novembre de 2020

Validat per,	Aprovat per,

Sumari

1. Antecedents

El Consorci de Serveis Universitaris de Catalunya (CSUC) va néixer per impulsar l'eficiència en la gestió de les universitats catalanes a través de la cooperació i la coordinació, a iniciativa de la Generalitat de Catalunya. Està integrat per la Generalitat de Catalunya i les següents universitats: la de Barcelona, l'Autònoma de Barcelona, la Politècnica de Catalunya, la Pompeu Fabra, la de Lleida, la de Girona, la Rovira i Virgili. Es consideren entitats agregades la Universitat Oberta de Catalunya i la Universitat Ramon Llull.

El CSUC ofereix un ampli ventall de serveis per a la universitat i la recerca, basant-se en diverses línies d'activitat: els sistemes per a càlcul científic; les xarxes de comunicacions; els portals i repositoris; l'administració electrònica; el suport per millorar els serveis bibliotecaris; la consorciació de serveis; la promoció d'aquests serveis, i l'operació i el manteniment de la infraestructura del Consorci.

Dins l'àmbit de serveis TIC, el CSUC gestiona infraestructura tecnològica en un centre de dades propis d'es d'on es serveixen molts dels serveis prestats. Aquests serveis prestats, es fonamenten entre d'altres, en la persistència de les dades que aporta el servei de còpies de seguretat en diferents formats i protocols.

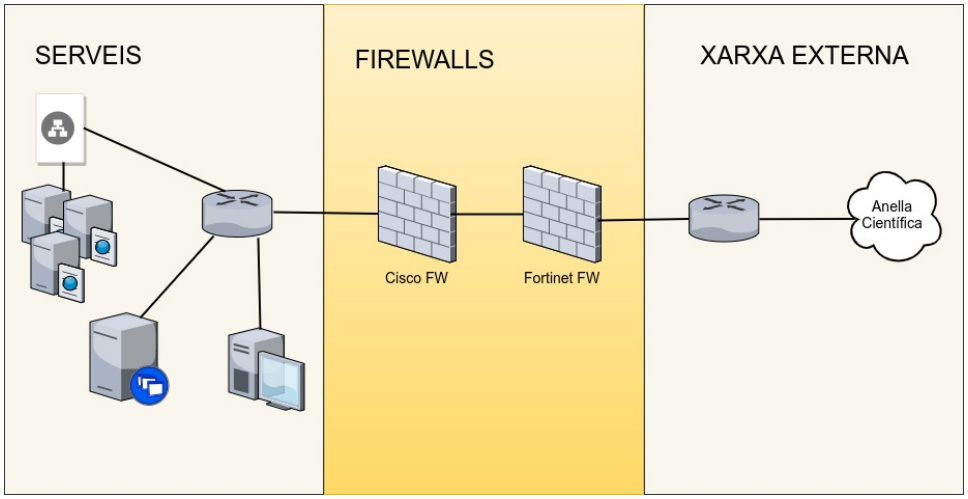
2. Abast del projecte

L'objectiu d'aquesta licitació és l'adquisició d'un sistema tallafoc redundat, la seva instal·lació i posada en funcionament, i el seu manteniment per a cinc anys; de manera que compleixi amb els requisits funcionals, tècnics i normatius que més endavant es detallaran, i que s'integri en l'entorn tecnològic actual del CSUC.

Actualment es disposa de dues línies de seguretat diferenciades mitjançant Next Generation Firewalls (NGFW), la primera d'elles del fabricant Fortinet i la segona del fabricant Cisco.

Els equips a substituir serien uns firewalls Fortinet 800C en configuració master-slave.

Per tal de complir amb l'Esquema Nacional de Seguretat (ENS) i disposar d'una arquitectura de protecció de perímetre tipus 5 (APP-5), l'accés a Internet s'ha de realitzar a través d'una doble capa de firewalls o tallafocs de diferent fabricant.



La nostra arquitectura de servidors està orientada al núvol i es basa en un disseny d'abstracció en tres capes: **virtualització, emmagatzematge i maquinari**.

Aquest model proporciona una arquitectura sòlida que permet entorns complexos, de gran volum, flexibles i redundants; així com una base tecnològica homogènia i, per tant, eficient i sostenible. A més, permet una evolució contínua que garanteix la qualitat i disponibilitat dels serveis.

Entorn de xarxa

El nostre model d'infraestructura tecnològica es basa en l'abstracció del maquinari, que implica una segmentació de la infraestructura en tres capes segons la seva naturalesa, i on la xarxa té un paper estratègic:

- Infraestructura virtual (servidors).
- Maquinari.
- Emmagatzematge.

La xarxa es troba físicament distribuïda (Edifici Nexus, Edifici Annexus, Equinix i Nexica). Les seves característiques són:

- Diversos tipus de serveis per un perfil d'usuari diferenciat.
- Més de 80 subxarxes i més de 350 nodes connectats.
- Segmentació en diversos entorns: proves, preproducció i producció.

Entre els serveis de xarxa, disposem de balancejadors de càrrega, que distribueixen les peticions entre els servidors disponibles per a cada servei de manera intel·ligent, d'aquesta manera aportem un altre punt de seguretat envers la continuïtat en el servei.

3. Característiques de la solució sol·licitada

En aquesta secció es descriuen, en primer lloc, els requisits mínims que ha de complir la solució. En segon lloc, es detallen les condicions d'instal·lació, migració, formació, documentació i manteniment.

3.1. Requisits mínims de la solució

Es demana que la solució a subministrar (CSUC Campus Nord) compleixi els requisits d'una solució d'alta disponibilitat descrits a l'apartat 3.1.1. El licitador haurà de justificar quina serà la solució proposada, considerant que la solució global haurà de poder evolucionar al llarg dels propers anys de manera conjunta.

3.1.1. Requisits mínims per a la solució del sistema de tallafoc

Les funcionalitats i els requisits mínims sol·licitats per a la solució són els següents:

- Els equips tallafocs han de ser en format *appliance* d'un únic fabricant, quedant exclosos màquines virtuals i servidors de propòsit general. Han de poder ser instal·lats en un rack estàndard de 19".
- Els dos equips físics han de ser d'idèntiques característiques, redundats i en alta disponibilitat (HA, High availability). Han de permetre treballar en mode HA actiu-actiu i actiu-passiu. En el cas d'activar sistemes virtuals, aquests poden funcionar en qualsevol dels dos nodes, de forma que s'aconsegueixi un actiu-actiu.
    - La transferència de servei d'un equip a l'altre s'ha de poder fer sense talls, ni pèrdua de les connexions TCP, ni aturada de servei.
    - Les configuracions s'han de traspassar de manera automàtica entre els dos equips.
    - En el cas de necessitat de llicenciament o subscripcions per activar l'alta disponibilitat, caldrà que aquestes estiguin incloses en la proposta durant la duració completa del contracte.

- La solució ha d'incloure funcionalitats, que han d'estar llicenciades durant la duració del contracte, de:
    - Control d'aplicacions
        - Capacitat per identificar un mínim de 1.900 aplicacions actives actuals (incloent aplicacions web 2.0).
        - La solució ha de classificar les aplicacions en diferents categories i subcategories, per poder aplicar regles d'acord amb aquestes categories / subcategories (control granular dins de l'aplicació).
        - Aplicar tècniques d'identificació d'aplicacions a tots els ports TCP / UDP i no només en els més comuns.
        - Capacitat per identificar les aplicacions sota túnels HTTPS.
        - Capacitat de creació de firmes d'aplicacions per un reconeixement personalitzat. Es obligatori que en aquelles aplicacions customitzades, també siguin analitzades per motors de protecció (IPS i *antimalware*).
    - IPS
        - Capacitat per protegir tant servidors com clients amb un mínim de 10.000 firmes d'IPS, agrupades per categoria, severitat, objectiu i protocol. Davant la identificació d'un atac per IPS, cal que el tallafocs capturi el tràfic en un arxiu PCAP per tal d'evidenciar-ho i fer un estudi posterior.
        - Capacitat per identificar patrons d'atacs basats en comportament o *rated-base*, per tal de bloquejar intents d'atacs un cop superat un llindar d'ús en un temps determinat.
    - *Antimalware*
        - Capacitat de detecció de *malware* (virus, *grayware*, *worns*, etc.) basat en firmes conegudes o mètodes avançats de detecció.
        - Suport de *sandboxing* en el núvol, amb una mida mínima de fitxer de 100 MB indistintament del tipus de fitxer.
        - Capacitat per l'eliminació del contingut dinàmic (macros, *javascript*, URL) explotable dintre de documents ofimàtics i pdf, que es distribueixen per protocols SMTP, IMAP i HTTP.
        - Capacitat de comprovació de si es tracta d'un fitxer bo o dolent, en funció del hashing i comparat amb la BBDD del fabricant. Així com bloquejant mitjançant *malware* de repositoris externs de *threat inteligence*.
    - *Webfilter*
        - Capacitat de categoritzar més de 250 milions de pàgines web en més de 60 categories web per tal d'aplicar: *block, monitor* i aplicació de quotes de temps o tràfic per categoria.

  - Suport de protocols HTTP v1.0, 1.1 i 1.2.
  - La base de dades de categories web caldrà consumir-se com un servei al núvol en temps real i no podrà basar-se únicament en llistats locals per tal de tenir la categorització de les url's el més actualitzat possible.
  - Suport per a la creació de llistes blanques/negres externes sense necessitat de llicencia.
  - *Antispam*, DLP, DNS *Filter*, ICAP.

- Els equips han de disposar de la funcionalitat de *Firewalls* virtuals per tal de crear entorns completament diferencials. Ha d'incloure com a mínim 10 Firewalls virtuals per equip.
- Ha de tenir capacitat per com a mínim de 10.000 polítiques de *firewall*.
- La solució de seguretat ha de permetre diferents modes de funcionament, podent-se combinar entre els diferents *Firewalls* virtuals:
  - Mode transparent.
  - Mode *routed* i/o mode *sniffer*.
- Disposar de connectors automàtics amb l'objectiu d'integrar-se amb identitats terceres i poder recollir informació, adreçament IP, inventari d'objectes i etiquetes. Aquesta funcionalitat haurà d'estar suportada en els *appliances* de seguretat (sense necessitat de consola addicional). En concret es requereixen les següents:
  - Cloud pública: Google Cloud, Azure i AWS.
  - Cloud privada: VMware NSX i ESXi, Openstack i Kubernetes.
  - Fonts d'identitat: Active directory i Radius.
  - Fonts d'amenaces: Llistat d'IP, dominis i *hash's* de *malware*.
- Els equips tallafocs tindran *hardware* específic (de tipus ASIC) per tal d'assegurar el rendiment requerit; en detall, ha de tenir un hardware específic per analitzar el tràfic a nivell 4 i un altre totalment diferent, a nivell 7.
- El tallafocs ha de ser capaç de gestionar fins 4 milions de sessions concurrents. Així com a mínim 150.000 noves sessions per segon.
- Disposar de com a mínim el següent rendiment:
  - Rendiment Firewall: mínim 17 Gbps
  - Rendiment IPS: mínim 7 Gbps.
  - Rendiment NGFW (IPS i control d'aplicacions): mínim 6,5 Gbps.
  - Rendiment amb *Threat Protection* (IPS, control d'aplicacions i motor antimalware actius): mínim 4 Gbps.

- El rendiment per tràfic SSL VPN i per tràfic IPSEC VPN ha de ser de com a mínim 7 Gbps.
    - El dispositiu ha d'admetre fins a un màxim de 10.000 usuaris simultanis VPN SSL, ja sigui amb agent o sense, però en qualsevol cas sense llicència addicional.
    - Ha de complir els estàndards de la indústria, sense el suport extern addicional de maquinari o mòduls: IPSEC VPN (IPv4 i IPv6), PPTP VPN, L2TP VPN, SSL VPN i GRE sobre IPSEC.
    - Ha de suportar 2 modes de funcionament SSL VPN:
        - Sense client - Accés web: per a clients remots que només necessiten un navegador i no requereix la instal·lació de cap agent, per tal d'accedir via web a: HTTP / HTTPS Servidor intermediari, FTP, Telnet, SMB / CIFS, SSH, VNC i RDP.
        - Mode túnel: per a equips remots que executen una varietat d'aplicacions de client i servidor.
- Disposar del següent número mínim de ports:
    - 1 port de consola.
    - 1 port d'USB per permetre la instal·lació desassistida del firmware i aplicació de configuració en el *booting* de l'equip per realitzar tasques automàtiques d'instal·lació i manteniment.
- Cadascun dels equips ha de disposar de:
    - 2 x 10GE SFP+
    - 8 x GE SFP
    - 10 x GE RJ45
    - Disc dur de fins a 240 GB en format SSD.
    - Transceptors
    - Consum elèctric inferior a 250 W amb tots els ports ocupats.
    - Doble font d'alimentació.
- Capacitat de gestió dels equips mitjançant accés via web (https), prescindint d'interfícies basades en Java, i terminal (ssh) per la total configuració de les polítiques de seguretat de la plataforma.
    - Quedaran excloses aquelles solucions que requereixin una plataforma de gestió externa per gestionar i administrar la solució.
    - Creació de diferents tipus d'usuari per l'administració podent aplicar diferents rols o perfils, així com definir xarxes d'origen confiables. Es necessari també la possibilitat de crear usuaris de tipus REST-API.

- Tots els canvis efectuats en els tallafocs han de ser aplicats de forma immediata, sense necessitat de compilar o similar.
- Suport de SNMP i sFlow.
- Exportació de logs via SYSLOG, FTP, SCP i TFTP.

- *Networking*
  - Suport de protocols RIP v1/v2, OSPF, ISIS, BGP, WCCP i Multicast per IPv4 e IPv6, Routing basat en política o PBR.
  - Suport Dual Stack IPv4 e IPv6 simultàniament.
  - Network address translation NAT IPv4, NAT64 i NAT66.
  - DHCP server / DHCP Relay /DNS Server / DNS Proxy / NTP Server.
  - 802.1Q VLANs i Point-to-Point Protocol over Ethernet (PPPoE).
  - 802.3ad Capacitat de crear enllaços LACP per l'agregació de ports.
  - Capacitat de balanceig de servidors a nivell 4 per tots els serveis, com també possibilitat de fer SSL *off-loading* pel tràfic HTTPS.
  - Cal que la solució de seguretat tingui capacitats integrades de SD-WAN, en concret:
    - Balanceig intel·ligent de connexions físiques i lògiques, indiferentment del tipus de connexió WAN (MPLS, 3G/4G, FTTH, VPN, etc..).
    - El número mínim de connexions físiques i lògiques que es poden afegir a l'SD-WAN ha de ser de 256.
    - Verificació de la disponibilitat d'Internet per cadascuna de les línies, per protocols HTTP, ping i TWANP. El número de validacions ha de ser de com a mínim 100.
    - Verificació de paràmetres de qualitat en temps real: jitter, packet loss i latència per línia.
    - Configuració de polítiques de SD-WAN intel·ligent basat en origen (usuaris AD i direcció IP), en el destí (direcció IP, aplicacions i/o serveis d'Internet/aplicacions) i en la línia amb millor qualitat d'aquell moment basat en valors de *jitter*, *packet loss*, latència, tràfic de pujada/baixada o ampla de banda, així com una combinació per pesos.
    - En el cas de necessitat de llicenciament o subscripcions per activar aquestes funcionalitats, caldrà que aquestes estiguin incloses en la proposta durant la duració completa del contracte.
  - Suport d'VXLAN i VXLAN VTEP per l'extensió de xarxes de nivell 2 entre xarxes de nivell 3.

- Permetre la creació d'automatismes per tal de:
    - Davant la detecció d'un host compromès, els tallafocs enviïn (tots alhora): un correu electrònic, una notificació tipus *push* a dispositius Iphone, poder banejar l'adreça IP, invocar funcions AWS Lambda, Google functions, Azure Functions i Webhook.
    - Davant el canvi de configuració del tallafocs, un *failover*, *reboot*, actualització de firmes, de forma programada i qualsevol esdeveniment del tallafocs, aquest enviï (tots alhora): un correu electrònic, una notificació tipus *push* a dispositius Iphone e invocar funcions AWS Lambda, Google functions, Azure Functions, AliCloud Function, comanda per CLI i Webhook.

Addicionalment, la solució haurà de proveir un *Web Application Firewall* (WAF) de forma integrada o be amb equipament addicional del mateix fabricant. Haurà de complir:

- Processament SSL/TLS per hardware.
- Throughput d'1,3 Gbps.

3.2. Instal·lació, migració, traspàs de coneixement, documentació i suport

L'adjudicatari haurà de proveir l'assistència tècnica necessària per a la instal·lació de l'equipament i migració dels serveis ja en funcionament en els equips a canviar, coordinant-se amb el CSUC per garantir la instal·lació, migració i posada en marxa amb la mínima interrupció en el servei.

També haurà d'impartir la formació necessària adreçada a un mínim de deu (10) persones per a la gestió per part del CSUC de l'equipament, així com de l'arquitectura de la solució proposada amb personal certificat pel fabricant. El temari haurà d'incloure, com a mínim, la informació necessària per la configuració i l'operació del programari, permetent als tècnics del CSUC ser autònoms en la seva gestió. Caldrà lliurar, en format digital, un manual d'operació i administració de la solució proposada, i una descripció de la configuració resultant.

L'adjudicatari farà arribar al CSUC la documentació que descrigui l'arquitectura de la solució i la configuració dels equips proposada.

Quant a la descripció del projecte, es demana incloure en la proposta la següent informa:

- Cronograma d'implantació i posta en marxa de tots els elements a subministrar.
- Pla de migració dels serveis.
- Plantejament tècnic del procés de translació de regles dels sistemes actuals als nous *firewalls*.
- Metodologia de traspàs.
- Pla de proves de maquinari i continuïtat del servei en cadascun dels sistemes instal·lats.

- Pla de proves de restauració de configuració (a partir d'un backup de la configuració).
- Pla d'acceptació i posada en producció.

La posada en producció des de la signatura del contracte no pot ser superior a (1) un mes.

El manteniment de la solució proposada serà per cinc anys, a partir de la posada en operació. Aquest servei haurà de contemplar, com a mínim, els següents requisits:

- L'adjudicatari haurà de proveir accés a la plataforma del fabricant per a la consulta d'incidències, així com per a descàrregues d'actualitzacions de programari.
- Complir els temps de resposta i resolució que s'indiquen a l'apartat 3.2.1.. En cas d'incompliment d'aquests temps de resposta i resolució s'aplicaran les penalitzacions indicades a l'apartat O. del PCAP.

3.2.1. Qualitat del servei, manteniment i suport tècnic

El període de suport tècnic i manteniment, haurà de ser obligatòriament assumit per l'adjudicatari per tota la durada del contracte (5 anys) i inclourà actualitzacions de programari, canvis de components del maquinari i resolució de problemes i incidències que puguin afectar al sistema de tallafoc redundat. El període de suport i manteniment començarà a comptar a partir de la data de la signatura de l'acta de conformitat amb la posada en marxa de tots els equips inclosos en la licitació per part del CSUC i ha de cobrir els 365 dies de l'any, els 7 dies de la setmana, les 24 hores del dia. El manteniment ha d'incloure els components, la mà d'obra, les dietes i els desplaçaments.

Pel que fa a les incidències, es considera que una incidència és:

- De **prioritat alta** quan per causa de la mateixa es produeixi una afectació total o parcial en els serveis oferts pel CSUC mitjançant el sistema de tallafoc redundat.
- De **prioritat mitja** quan els *logs* o missatges d'error dels equips indiquin que s'ha produït una alteració no esperada del seu comportament o bé quan s'hagi produït algun error que calgui esmenar, però que no afecti ni total ni parcialment els serveis oferts pel CSUC mitjançant el sistema de tallafoc redundat.
- De **prioritat baixa** quan sigui informativa.

El temps màxim de resposta i resolució en cas d'incidència s'indiquen a les figures següents:

Tipus de prioritat de la incidència	Temps de resposta màxim
Alta	30 min
Mitja	1 hora
Baixa	1 dia laborable

Figura 1. Temps de resposta màxim

Tipus de prioritat de la incidència	Temps de resolució màxim
Alta	4 hores
Mitja	24 hores
Baixa	5 dies laborables

Figura 2. Temps de resolució màxim

En cas d'incompliment d'aquests temps s'aplicaran les penalitats indicades a l'apartat O del PCAP.

Es considera que un problema és la causa d'una o més incidències.

En cas de produir-se una incidència de prioritat alta, el CSUC podrà demanar a l'adjudicatari informes puntuals sobre la mateixa, que hauran d'estar disponibles en el termini màxim de 3 dies laborables.

Se sol·licita que els licitadors especifiquin els perfils dels tècnics que portaran a terme el servei de suport tècnic i manteniment.

3.3. Política de creixement

El licitador ha de descriure a l'oferta la seva política per a possibles ampliacions de la solució, incloent la possibilitat de proporcionar altres equips o funcionalitats que es puguin adaptar al servei en cas que els inicials quedin limitats pel creixement del servei.

3.4. Característiques tècniques i funcionals complementàries

1. Augment de la capacitat de gestionar les sessions concurrents fins 8 milions.
2. Augment de la capacitat de gestionar les noves sessions per segon fins a 450.000.
3. Augment del rendiment Firewall fins a 27 Gbps.
4. Augment del rendiment a nivell 7 IPS fins a 10 Gbps.
5. Augment del rendiment a nivell 7 NGFW (IPS i control d'aplicacions) fins a 9,5 Gbps.
6. Augment del rendiment a nivell 7 Threat Protection (IPS, control d'aplicacions i motor *antimalware* actius) fins a 7 Gbps.
7. Augment del rendiment per tràfic IPSEC VPN (512 bytes) fins a de 20 Gbps.
8. Disposar d'una controladora d'accés segur integrada.
    a. El sistema ha de poder actuar com a controladora de punts d'accés *wireless* (AP)de Fortinet (FAP-221E).

b. La gestió dels AP i commutadors es farà des de la mateixa interfície gràfica i CLI des de la qual es gestiona el Firewall.

9. En cas que s'ofereixi un equipament addicional per la funcionalitat WAF aquest ha de disposar de:
    a. 2 x 10GE SFP+
    b. 4 x GE SFP
    c. 2 x GE RJ45
    d. 2 x GE ports de gestió
    e. Disc dur de fins a 2 TB
    f. Consum elèctric inferior a 150 W amb tots els ports ocupats.
    g. Doble font d'alimentació.
    h. Transceptors.
    i. Llicència, si s'escau.