UPCnet

PLEC DE PRESCRIPCIONS TÈCNIQUES

Subministrament de solució de seguretat per a la protecció perimetral de la Xarxa IP de la Universitat Politècnica de Catalunya

Expedient CES-LIC-2025-52

UPCnet

Tabla de contenido

Contingut

1. Objectiu de la proposta 3
2. Justificació i Antecedents de la Renovació 3
3. Abast 3
4. Funcionalitats i requeriments 6
   - 4.1. Requeriments de Rendiment i Capacitat (Mínims Obligatoris) 6
   - 4.2. Requeriments de Hardware i Connectivitat 7
   - 4.3. Funcionalitats de Seguretat Avançada (NGFW) 7
   - 4.4. Integració amb l'Ecosistema Actual 8
   - 4.5. Requeriment de Serveis i Suport (Subscripcions) 8
5. Oferta tècnica del licitador 9

1. Objectiu de la proposta

L'objectiu principal d'aquest document és establir les condicions tècniques i funcionals que han de regir la contractació per al subministrament d'un nou Sistema de Protecció Perimetral de nova generació per a la Universitat Politècnica de Catalunya (UPC en endavant), així com els serveis de manteniment, suport i actualització de subscripcions corresponents.

2. Justificació i Antecedents de la Renovació

Actualment, l'UPC disposa d'una infraestructura de seguretat perimetral que ha estat operativa durant els últims cinc anys i ha garantit la connectivitat i la protecció dels nostres actius digitals.

No obstant això, a causa del creixement sostingut de l'organització, l'augment del trànsit de dades, la implementació de nous serveis en línia i l'adopció de models de treball híbrids, la infraestructura actual ha quedat mal dimensionada. Aquesta situació representa un repte operatiu i de seguretat que cal abordar de manera immediata, manifestant-se sobre tot en la necessitat de renovar les subscripcions actuals.

Addicionalment, els serveis de subscripció de seguretat (Antivirus, IPS, Filtre Web, etc.) dels equips actuals estan a punt de finalitzar o han finalitzat. Aquesta renovació és l'oportunitat idònia per consolidar la inversió en una plataforma que compleixi amb els requeriments actuals de dimensionament i integri les últimes funcionalitats de seguretat de nova generació (NGFW).

Per tant, aquesta renovació és imprescindible per adequar la capacitat del sistema als requisits operacionals i de seguretat actuals i futurs de l'UPC, garantint un nivell òptim de protecció.

3. Abast

El nou sistema ha de substituir completament la infraestructura actual i ha d'incorporar les darreres tecnologies Next-Generation Firewall (NGFW) i Seguretat Unificada d'Amenaces (UTM), amb capacitat per afrontar el creixement de trànsit previst per als pròxims anys.

És un requisit fonamental que la nova solució garanteixi la compatibilitat total amb els serveis d'accés remot ja implementats (especialment les VPN-SSL i VPN-IPsec existents, basats en el software de Forticlient) i amb el hardware de comunicació Wi-Fi del fabricant Fortinet de l'organització, per assegurar la integració fluida i sense disrupcions amb l'ecosistema de seguretat actual. També haurà de mantenir compatibilitat total amb els serveis actuals de gestió de la seguretat (FortiManager) y tractament de logs (FortiAnalyzer).

Així doncs, l'objecte del contracte consisteix en el subministrament d'un clúster de tallafocs en alta disponibilitat (**mínim dues unitats**), de "capa 7" a nivell d'aplicació, per l'entrada i sortida principal a les xarxes de l'UPC, incloent-hi la xarxa pròpia del CPD corporatiu. Addicionalment, **s'inclouran tots els adaptadors òptics necessaris** per a la correcta integració d'aquest clúster de tallafocs amb la infraestructura de xarxa existent. Concretament, els adaptadors requerits són els següents:

- SFP+ 10G SR Fortinet: 4 unitats
- SFP+ 10G SR Cisco: 4 unitats
- QSFP28 SR4 100 Fortinet: 2 unitats
- QSFP28 SR4 100 HPE: 2 unitats
- SFP28 25G LR Fortinet: 3 unitats
- SFP28 25G LR Cisco: 3 unitats
- SFP+ 10G LR Cisco: 1 unitat
- SFP+ 10G LR Fortinet: 1 unitat

Tots els adaptadors òptics indicats hauran de ser lliurats juntament amb el clúster de tallafocs, assegurant la seva compatibilitat amb els dispositius de xarxa existents.

Aquest **clúster** es convertirà en l'element principal de la seguretat de la xarxa de la UPC, darrere del qual se situaran no tan sols els sistemes d'informació i comunicacions, sinó tots els equips finals de la Universitat. Per això ha d'estar dotat d'altes prestacions quant a capacitat, fiabilitat, disponibilitat i funcionalitat. Els objectius funcionals que es persegueixen amb aquesta adquisició són els integrals en els firewall de Nova Generació (NGFW):

- Implementar seguretat activa a nivell de IPS (Intrusion Prevention System) i firewall de nova generació.

- Gestionar la seguretat d'accessos en les xarxes segures de la UPC, millorant tant el rendiment com el nivell de protecció amb tecnologies d'inspecció avançada de tràfic, identificació d'aplicacions i usuaris, antivirus, aplicació de polítiques d'autorització i filtrat i prevenció d'intrusions.

Els licitadors presentaran una única oferta sense alternatives ni variants. En el següents apartats s'especifiquen els requisits obligatoris que han de complir els equips proposats.

Qualsevol consulta sobre el contingut d'aquestes prescripcions s'haurà d'adreçar, per correu electrònic, a:

licitacions@upcnet.es

4. Funcionalitats i requeriments

El sistema de protecció perimetral (Firewall) proposat ha de complir obligatòriament amb els següents requeriments funcionals i tècnics per tal de satisfer les necessitats presents i futures de l'organització.

4.1. Requeriments de Rendiment i Capacitat (Mínims Obligatoris)

La solució ha d'estar dimensionada per gestionar el trànsit actual amb marge de creixement i ha d'oferir els següents nivells de rendiment mínims mesurats amb totes les funcionalitats de seguretat activades (Next-Generation Firewall), en cadascun dels equips subministrats:

	Valor Mínim Requerit
Throughput Firewall	**198 Gbps**
Throughput NGFW (Inspecció completa)	**17 Gbps**
Throughput IPS (Sistema de Prevenció d'Intrusions)	**22 Gbps**
Throughput de VPN IPsec	**55 Gbps**
Connexions Concurrents	**12 Milions**
Noves Connexions/segon	**750.000**
Throughput de protecció contra Amenaces (Threat Protection)	**15 Gbps**

4.2. Requeriments de Hardware i Connectivitat

Els equips hauran de ser de tipus “Appliance” dissenyats per a entorns de centre de dades, amb redundància de hardware (Font d'alimentació i disc dur) i capaç d'operar en mode Alta Disponibilitat (HA) actiu-passiu o actiu-actiu. En quant a interfaces físiques, haurà de disposar com a mínim dels següents ports:

Requeriment de Port/Mòdul	**Especificació Mínima**
Ports 100GE	Mínim **4**
Ports 25GE/10GE SFP+	Mínim **25/2**
Ports 1GE RJ45/SFP	Mínim **18/8**

En quant als adaptadors òptics, es necessitaran aquestes quantitats:

Tipus de mòdul	**Velocitat**	**Fabricant**	**Quantitat**
SFP+ 10G SR	10 Gbps	Fortinet	4
SFP+ 10G SR	10 Gbps	Cisco	4
QSFP28 SR4 100	100 Gbps	Fortinet	2
QSFP28 SR4 100	100 Gbps	HPE	2
SFP28 25G LR	25 Gbps	Fortinet	3
SFP28 25G LR	25 Gbps	Cisco	3
SFP+ 10G LR	10 Gbps	Cisco	1
SFP+ 10G LR	10 Gbps	Fortinet	1

4.3. Funcionalitats de Seguretat Avançada (NGFW)

El nou sistema ha d'integrar obligatòriament els següents mòduls de seguretat avançada:

- **Sistema de Prevenció d'Intrusions (IPS):** Capacitat de detecció i bloqueig d'explotacions, amb actualitzacions en temps real.
- **Inspecció SSL/TLS:** Capacitat d'inspeccionar tràfic xifrat (incloent SSL 4.0 fins a TLS 1.3) a nivell de rendiment especificat, sense degradació significativa.
- **Control d'Aplicacions**: Identificació i control granular de milers d'aplicacions i serveis, independentment del port o protocol que utilitzin.

- **Antimalware/Antivirus**: Protecció en temps real contra programari maliciós, ransomware i amenaces zero-day.
- **Filtratge Web i DNS:** Control d'accés a categories de pàgines web i filtratge de peticions DNS malicioses.
- **Sandboxing:** Integració nativa o funcionalitat de Sandboxing per a l'anàlisi automàtica d'arxius sospitosos en un entorn aïllat.
- **Seguretat Unificada (UTM**): Capacitat d'executar simultàniament tots els serveis de seguretat anteriors sense impacte de rendiment més enllà dels requisits mínims.

4.4. Integració amb l'Ecosistema Actual

La solució proposada ha de garantir la màxima integració i compatibilitat amb la nostra infraestructura de seguretat existent:

- **Compatibilitat VPN**: Manteniment total de la connectivitat per a accessos remots mitjançant protocols VPN-SSL i VPN-IPsec actuals, basats en el programari de Forticlient, permetent la migració de les polítiques de tunelització amb mínima disrupció.
- **Integració Wi-Fi:** Ha de suportar la gestió centralitzada de la nostra infraestructura Wi-Fi actual del fabricant Fortinet, actuant com a controlador sense fils i permetent la gestió de tots els punts d'accés existents.
- **Gestió Centralitzada:** La solució ha de ser gestionable des d'una única interfície i ha de permetre la gestió unificada de diversos dispositius Firewall i la integració amb sistemes de registre (SIEM/Syslog).

4.5. Requeriment de Serveis i Suport (Subscripcions)

És un requisit imprescindible que el subministrament inclogui totes les llicències de software i subscripcions de seguretat necessàries (Threat Protection, NGFW Bundle, etc.) i el servei de manteniment i suport del fabricant 24x7 amb temps de reposició RMA NBD per un període mínim de **cinc (5) anys**. La vigència d'aquest període de manteniment i subscripció ha de ser unificada i ha d'iniciar-se a partir de la data de la posada en producció de l'equip.

La solució ha de **donar compliment a l'establert en el Esquema Nacional de Seguridad,** en quant a la definició d'un perímetre segur (control mp.com.1), segregar

xarxes (control mp.com.4), la detecció d'intrusions (control mp.mon.1), i la protecció de serveis i aplicacions web [control mp.s.2], per sistemes d'informació i serveis categoritzats com a baix o mitjà.

La proposta ha de basar-se en equipament que sigui present a les guies de recomanació com a fabricant homologat per el CCN-CERT (https://www.ccn-cert.cni.es/pdf/guias/series-ccTn-stic/guias-de-acceso-publico-ccn-stic/2536-ccn-stic-105-catalogo-de-productos-de-seguridad-de-las-tecnologias-de-la-informacion-y-la-comunicacion/file.html , i ser reconegut com a líder en el darrer quadrant de Gartner per a Enterprise Firewalls.

5. Oferta tècnica del licitador

L'oferta del licitador haurà d'incloure la següent documentació tècnica:

1. Document de disseny general i resum executiu. Aquest document haurà de tenir en compte el projecte global descrivint amb detalls l'arquitectura. S'han de preveure en aquest moment tots els elements necessaris, tant físics com virtuals o llicències, que componen l'arquitectura final. Es valorarà en aquest sentit el grau de detall i claredat de les diferents ofertes avaluades.

2. Document detallat de la proposta que ha d'incloure amb el màxim de detall possible el conjunt de materials objecte de la licitació – maquinari, programari, llicències, adaptadors òptics, cablatge, conversors, etc.

Tota la documentació s'haurà d'entregar en format electrònic no escanejat i ha de permetre cerques de text. Es podran entregar tants documents annexos com es consideri convenient.