Universitat de Lleida
Sistemes d'Informació
i Comunicacions

Plaça de Víctor Siurana, 1
E 25003 LLEIDA (Catalunya)
Tel. +34 973 70 22 29
sic@udl.cat
www.udl.cat/ca/serveis/asic/

Plec de Prescripcions Tècniques pel

SUBMINISTRAMENT, INSTAL·LACIÓ I MANTENIMENT DELS TALLAFOCS DE LA UDL

Exp. 2024/SUB-XX

Full de control de la documentació

Títol		
SUBMINISTRAMENT, INSTAL·LACIÓ I MANTENIMENT DELS TALLAFOCS DE LA UDL Plec de Prescripcions Tècniques		
Revisió		**Data**
V7		06/06/2024
Classificació	**Tipus de document**	**Estat**
Públic **X**	Document tècnic **X**	Esborrany
Restringit intern	Presentació	Informe Final **X**
Restringit client	Proposta/ Informe	
Nom d'arxiu	PPT_Firewall_v6.odt	
Resum del contingut		
Plec de Prescripcions Tècniques		

	Nom	Firma
Edició (SIC) **(Responsable actualització doc.)**	Fernando Villa Estebaranz	
Aprovat (SIC)	Judith Pintó Subirada	
Vistiplau (Direcció SIC)	Alexandre Ballesté Crevillén	

Full de control de la distribució

Còpia	Nom	Càrrec	Organització
1	Alexandre Ballesté Crevillén	Cap de Sistemes d'Informació i Comunicacions	UdL
2	Ariadna Tudela Pi	Unitat d'economia	UdL
3	Judith Pintó Subirada	Cap d'Operació de serveis TIC	UdL
4	Fernando Villa Estebaranz	Cap de Comunicacions i Sistemes	UdL

Full de registre de canvis

Versió	Data	Pàgines afectades	Notes i raons del canvi
1	08-02-2024	Totes	Elaboració del document
2	27-02-2024	Modificació	Correcció errors i modificació condicions.
3	27-02-2024	Modificació	Correcció errors i modificació condicions proposades per Judith i Alexandre.
4	05-04-2024	Modificació	Correcció redacció.
5	19-04-2024	Modificació	Correccions unitat de contractació
6	24-04-2024	Modificació	Correcció característiques equips seu remota.
7	06-06-2024	Modificació	Característiques generals concretes.

Índex

1 INTRODUCCIÓ

La Universitat de Lleida (UdL) és una institució pública dedicada a l'ensenyament i la recerca, que vetlla per la qualitat de les activitats que s'hi duen a terme. Amb aquest objectiu, en els darrers anys s'han realitzat nombroses inversions per optimitzar el servei que, des de la unitat de Sistemes d'Informació i Comunicacions (SIC), es proporciona a tota la comunitat universitària.

2 OBJECTE

L'objecte del present document consisteix a proporcionar una solució integral per garantir la seguretat informàtica i la protecció dels recursos digitals de la Universitat mitjançant la implementació, migració i manteniment dels sistemes de tallafocs.

Subministrament: La Universitat de Lleida necessita instal·lar un tallafoc a la seu principal del Rectorat i un altre a la seu remota d'Igualada. Subministrar els equips de firewall necessaris, per proveir una solució a les ubicacions de Rectorat i Igualada, així com qualsevol component addicional requerit per a la implementació eficaç del sistema. El subministrament inclou tots els elements, maquinari, programari, servei de suport integral dels dispositius (mínim 5 anys) i llicenciament específic (mínim 5 anys) per assegurar una defensa robusta contra amenaces cibernètiques. La solució ha d'incloure funcionalitats de control d'aplicacions, IPS, Antimalware amb Cloud Sandbox inclós, Webfilter, DNS Filter, Antispam, protecció antiDoS i Web Application Firewall. Totes aquestes funcionalitats han d'estar llicenciades com a mínim per 5 anys.

Les propostes han d'incloure els equips i les quantitats necessàries per complir amb totes les especificacions tècniques i els acords de nivell corresponents. La solució de tallafoc proposada ha de satisfer els requisits descrits en el PPT, incloent-hi que a la seu principal els equips que conformen el tallafoc han de ser idèntics, redundants i d'alta disponibilitat. Per exemple, una possible solució seria instal·lar un conjunt d'equips (clúster) a la seu principal i un únic equip a la seu remota.

Instal·lació, posada en marxa amb migració: Es requereix la posada en marxa dels firewalls, incloent-hi la migració de les configuracions i integracions existents. Aquest procés s'ha de realitzar de manera coordinada i eficient per minimitzar les interrupcions en els serveis informàtics de la Universitat.

Manteniment: Es preveu un servei de manteniment continuat dels firewalls durant la vigència del contracte (1 any) a comptar a partir de la validació de la instal·lació, que abasteix tasques com revisions periòdiques, actualitzacions de seguretat, resolució d'incidències i altres tasques de suport tècnic. El contractista s'obliga a proporcionar un nivell de servei que asseguri el rendiment òptim dels firewalls i la seva adaptació als canvis en l'entorn cibernètic.

3 DESCRIPCIÓ DEL SISTEMA DE TALLAFOCS ACTUAL

El sistema de tallafocs actual implementat per a la Universitat es basa en la reconeguda solució del fabricant Fortinet, que proporciona una defensa robusta i integral contra amenaces cibernètiques. La infraestructura de tallafocs està dissenyada per assegurar la protecció perimetral i la supervisió efectiva del trànsit de xarxa en múltiples ubicacions clau.

A les dependències de Rectorat ubicades en:

Plaça Víctor Siurana, 1

Lleida – 25003

S'ha implementat un clúster actiu/passiu amb dos equips Fortigate 1500D, que actuen com a nus de protecció perimetral. Aquesta configuració proporciona una alta disponibilitat i tolerància a fallades, assegurant una protecció continua sense interrupcions significatives en cas de fallada d'un dels equips.

A la seu ubicada a Igualada ubicades en:

Av. Pla de la Massa, 8

Igualada – 08700

Es fa ús d'un equip Fortigate 500E com a tallafocs dedicat, oferint una protecció localitzada i personalitzada adaptada a les necessitats específiques d'aquesta ubicació.

Per a la supervisió i anàlisi avançada de registres, s'ha implementat una solució virtualitzada del Fortianalyzer. Aquesta implementació permet centralitzar i analitzar de manera eficient els registres de trànsit de xarxa, proporcionant informació detallada sobre possibles amenaces, activitats sospitoses i tendències de seguretat.

En conjunt, aquest sistema de tallafocs basat en la tecnologia Fortinet ofereix una defensa integral amb un abast de les diverses ubicacions de la Universitat, assegurant la seguretat dels sistemes informàtics i la confidencialitat de la informació. La combinació d'equips físics i virtuals contribueix a la flexibilitat i eficàcia del sistema global de tallafocs. És rellevant destacar que els tècnics de la universitat s'han especialitzat en aquesta tecnologia específica. La seva experiència i coneixement profund d'aquesta plataforma tecnològica han estat fonamentals per assegurar el manteniment i l'optimització del sistema actual. En tot cas, i sigui quina sigui la tecnologia que s'incorpori, cal mantenir la coherència, consistència i continuïtat del servei en els mateixos termes que fins ara.

4 NO DIVISIÓ EN LOTS

D'acord amb l'article 99 de la Llei de Contractació del Sector Públic (LCSP), s'estableix l'obligatorietat de dividir en lots l'objecte del contracte sempre que la naturalesa del mateix ho permeti. No obstant això, la mateixa llei contempla l'excepció de no realitzar aquesta divisió quan hi hagi motius vàlids que així ho justifiquin, havent-se d'exposar degudament en l'expedient.

En el cas concret del subministrament i manteniment objecte del present contracte, es considera que no és convenient ni oportuna la seva divisió en lots, per les següents raons:

- **Millor solució tècnica:** La provisió d'un servei integrat de subministrament i manteniment garanteix una millor solució tècnica al contractant. En tractar-se d'un proveïdor únic, s'optimitza la coordinació i comunicació entre les diferents fases del projecte, des del subministrament inicial fins al manteniment posterior. Això es tradueix en una major eficiència en la gestió del servei, una reducció dels temps de resposta davant d'incidències i, en definitiva, una major satisfacció del client.

- **Interdependència de les prestacions:** El subministrament i el manteniment de l'objecte del contracte estan intrínsecament lligats. Un coneixement profund de les característiques tècniques de l'equip subministrat és essencial per realitzar un manteniment adequat i preventiu. **La divisió en lots podria implicar que el proveïdor del manteniment no disposi de la informació i experiència necessàries per atendre correctament l'equip**, el que podria derivar en un servei de menor qualitat i un major risc d'avaries.
- **Impossibilitat de licitar el manteniment sense conèixer l'adjudicació del subministrament:** La licitació del manteniment per separat resultaria inviable sense conèixer prèviament el proveïdor adjudicatari del subministrament. La raó és que el licitador del manteniment necessita conèixer les característiques específiques de l'equip subministrat per poder elaborar una oferta ajustada i tècnicament viable. Dividir el contracte en lots suposaria licitar el manteniment sense aquesta informació crucial, el que podria derivar en ofertes imprecises o fins i tot inviables.
- **Eficiència econòmica:** La gestió unificada del subministrament i manteniment per part d'un únic proveïdor pot optimitzar els costos del contracte. En tractar-se d'un únic interlocutor, se simplifiquen els processos administratius i de gestió, el que es pot traduir en un estalvi de costos per a l'Administració.
- **Major control i seguiment:** La gestió unificada del contracte facilita un major control i seguiment de l'execució d'aquest. L'administració té una visió global del servei prestat, el que li permet avaluar millor el compliment dels objectius establerts i prendre les mesures correctores necessàries en cas que sigui necessari.

En virtut dels arguments exposats, es considera que la no divisió en lots del subministrament i manteniment de l'objecte del contracte es troba plenament justificada, en respondre a criteris de millor solució tècnica, eficiència econòmica, control i seguiment, i impossibilitat de licitar el manteniment sense l'adjudicació prèvia del subministrament.

5 CARACTERÍSTIQUES TÈCNIQUES DEL MAQUINARI A SUBMINISTRAR

5.1 REQUERIMENTS GENERALS DELS EQUIPS

La proposta ha d'incloure durant la totalitat de la duració del contracte, totes les llicències i subscripcions necessàries per activar, en el cas que sigui necessari, totes les funcionalitats associades als requeriments obligatoris que es llisten a continuació.

- Els tallafocs han de ser en format appliance d'un únic fabricant, quedant exclosos màquines virtuals ni servidors de propòsit general. Han de poder ser instal·lats en un rack estàndard de 19''.
- La solució ha d'incloure funcionalitats de control d'aplicacions, IPS, Antimalware amb Cloud Sandbox inclós, Webfilter, DNS Filter, Antispam, protecció antiDoS i Web Application Firewall. Totes aquestes funcionalitats han d'estar llicenciades com a mínim per 5 anys.
- S'ha de subministrar fonts d'alimentació redundants per a cada equip.
- 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.
- La solució de seguretat ha de permetre diferents modes de funcionament, podent-se combinar entre els diferents Firewalls virtuals:
  - Mode transparent
  - Mode routed
  - Mode sniffer
- La mateixa plataforma ha de tenir connectors automàtics amb l'objectiu d'integrar-se amb identitats terceres i poder recollir informació, adreçament IP, inventari d'objectes i etiquetes. Aquesta funcionalitat ha d'estar suportada en els appliances de seguretat (sense necessitat de consola addicional). En concret es requereixen les següents:

- Cloud pública: Azure.
- Cloud privada: Vmware ESXi i Kubernetes.
- Fonts d'identitat: adAS SSO, LDAP, Active directory i Radius.
- Fonts d'amaneces: Llistat d'IP, dominis, URLs i hash's de malware customitzats.

- La mateixa solució de seguretat ha de permetre la creació d'automatismes per tal de:
  - Davant la detecció d'un host compromès, els tallafocs enviïn (tots alhora): un email, poder bloquejar l'adreça IP, Azure Functions i Webhook.
  - Davant el canvi de configuració del tallafocs, un failover, reboot, actualització de firmes, de forma programada i qualsevol event del tallafocs, aquest remeti (tots alhora): un email, Azure Functions, comanda per CLI i Webhook.
- Capacitat de configuració de Proxy explícit per Interface, amb la funcionalitat de Proxy chaining en cas necessari, a més de capacitat de caching.

5.2 CARACTERÍSTIQUES AVANÇADES TALLAFOCS SEU RECTORAT

Els datacenters de nova generació, amb adopció de tecnologies de connectivitat 25G/40G requereixen tallafocs de nova generació amb hardware específic. Cal que els equips oferts suportin les següents funcionalitats:

- Processadors Hardware (SPU) preparats per datacenters hyperescalars amb acceleració hardware.
- Suport de processament hardware amb alt rendiment i molt baixa latència amb acceleració de tràfic IPv4, IPv6, CAPWAP, VXLAN, GRE i IPSEC.
- Capacitat de protecció antiDoS (Denegació de Servei) implementada per hardware contra atacs volumètrics.
- Suport de QoS per hardware incloent traffic shaping i queuing.
- Suport d'Elephant Flows de fins a 100 Gbps.

- La solució oferta ha d'incloure coprocessadors hardware per accelerar el tràfic criptogràfic així com la inspecció de seguretat per hardware, incloent-hi la recerca de signatures d'atacs.
- Els equips físics 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 funcionalitat d'alta disponibilitat ha d'estar disponible sense necessitat de llicència o que estigui inclosa. La transferència de servei d'un equip a l'altre s'ha de poder fer sense talls, ni pèrdua de les connexions TCP, sense pèrdua dels nivells de servei, o de seguretat. Les configuracions s'han de traspassar de manera automàtica entre els dos equips.
- Els tallafocs han d'incloure en l'oferta presentada el següent nombre d'interfícies com a mínim (per equip):
  - 1 port de consola.
  - En el cas que l'equipament permeti ampliacions modulars d'interfícies, cal que tots els mòduls d'ampliació estiguin equipats amb interfícies com a mínim de les mateixes velocitats que es sol·liciten pels ports mínims obligatoris.
    - 2 ports 40GE QSFP.
    - 4 ports 10GE/25GE SFP28/SFP+ amb els corresponents transceptors òptics de 10GBase-SR.
    - 8 ports 1GE.
- Instal·lació en rack de 19" i no més de 2 RU.
- Fonts d'alimentació redundants i amb Hot Swap.
- 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 i garantir baixa latència.

- Rendiment:
  - El tallafocs ha de disposar de fins 198 / 197 / 140 Gbps de rendiment de firewall per paquets de 1518, 512 i 64 bytes en IPv4 ; i de 198 / 197 / 140 Gbps de rendiment de firewall per paquets de 1518, 512 i 86 bytes en IPv6 .
  - El tallafocs ha de ser capaç de gestionar fins 12 Milions sessions concurrents. Així com a mínim 750.000 noves sessions per segon.
  - El tallafocs ha de tenir una latència inferior a 4 µs (per paquets 64 byte UDP).
  - Ha de tenir capacitat per com a mínim de 20000 polítiques de firewall.
  - El rendiment per tràfic SSL VPN ha de ser de com a mínim 10 Gbps i per tràfic IPSEC VPN (512 bytes) de 20 Gbps.
  - A nivell 7, l'equip ha de disposar de com a mínim el següent rendiment:
    - Rendiment NGFW (IPS i control d'aplicacions): 10 Gbps.
    - Rendiment amb Threat Protection (Firewall més IPS, control d'aplicacions i motor antimalware actius): 9 Gbps
    - Rendiment Inspecció SSL amb IPS: 10 Gbps mesurats amb diferents Ciphers.
    - Rendiment per control d'aplicacions: 30 Gbps mesurat per HTTP 64K.

5.3 CARACTERÍSTIQUES AVANÇADES TALLAFOCS SEU REMOTA

Els datacenters de nova generació, amb adopció de tecnologies de connectivitat 25G/40G requereixen tallafocs de nova generació amb hardware específic. Cal que els equips oferts suportin les següents funcionalitats:

- Processadors Hardware (SPU) preparats per datacenters hyperescalars amb acceleració hardware.
- Suport de processament hardware amb alt rendiment i molt baixa latència amb acceleració de tràfic IPv4, IPv6, CAPWAP, VXLAN, GRE i IPSEC.

- Capacitat de protecció antiDoS (Denegació de Servei) implementada per hardware contra atacs volumètrics.
- Suport de QoS per hardware incloent traffic shaping i queuing.
- La solució oferta ha d'incloure coprocessadors hardware per accelerar el tràfic criptogràfic així com la inspecció de seguretat per hardware, incloent-hi la recerca de signatures d'atacs.
- Els tallafocs han d'incloure en l'oferta presentada el següent nombre d'interfícies com a mínim (per equip):
  - 1 port de consola.
  - En el cas que l'equipament permeti ampliacions modulars d'interfícies, cal que tots els mòduls d'ampliació estiguin equipats amb interfícies com a mínim de les mateixes velocitats que se sol·liciten pels ports mínims obligatoris.
    - 2 ports 10GE/25GE SFP28/SFP+ amb els corresponents transceptors òptics de 10GBase-SR.
    - 8 ports 1GE .
- Instal·lació en rack de 19" i no més de 2 RU.
- Fonts d'alimentació redundants i amb Hot Swap.
- Els equips tallafocs tenen 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 i garantir baixa latència.
- Rendiment:
  - El tallafocs ha de disposar de fins 139 / 137 / 70 Gbps de rendiment de firewall per paquets de 1518, 512 i 64 bytes en IPv4 ; i de 139 / 137 / 70 Gbps de rendiment de firewall per paquets de 1518, 512 i 86 bytes en IPv6.

- El tallafocs ha de ser capaç de gestionar fins a 8 Milions sessions concurrents. Així com a mínim 550.000 noves sessions per segon.
- El tallafocs ha de tenir una latència inferior a 4.12 µs (per paquets 64 byte UDP).
- Ha de tenir capacitat per com a mínim de 5000 polítiques de firewall.
- El rendiment per tràfic SSL VPN ha de ser de com a mínim 4 Gbps i per tràfic IPSEC VPN (512 bytes) de 20 Gbps.
- A nivell 7, l'equip ha de disposar de com a mínim el següent rendiment:
  - Rendiment NGFW (IPS i control d'aplicacions): 10 Gbps.
  - Rendiment amb Threat Protection (Firewall més IPS, control d'aplicacions i motor antimalware actius): 10 Gbps
  - Rendiment Inspecció SSL amb IPS: 5 Gbps mesurats amb diferents Ciphers.
  - Rendiment per control d'aplicacions: 30 Gbps mesurats per HTTP 64K.

5.4 GESTIÓ

- La gestió ha de ser de fàcil ús i intuïtiva.
- Capacitat de gestió dels equips mitjançant accés via web (HTTPS) i terminal (SSH) per la total configuració de les polítiques de seguretat de la plataforma.
- Queden excloses aquelles solucions que requereixin una plataforma de gestió externa per gestionar i administrar la solució.
- Tots els canvis efectuats en els tallafocs han de ser aplicats de forma immediata, sense necessitat de compilar o similar.
- Creació de diferents tipus d'usuari per l'administració podent aplicar diferents rols o perfils, així com definir xarxes d'origen confiables. És necessari també la possibilitat de crear usuaris de tipus REST-API.
- Suport de SNMP i sFlow.

- Exportació de logs vía SYSLOG, FTP, SCP i TFTP.

5.5 CAPACITAT D'INTEROPERABILITAT DE XARXA

Com a mínim la solució proposada ha de permetre les següents característiques:

- Suport de protocols RIP v1/v2, OSPF, ISIS, BGP, WCCP i Multicast per IPv4 e IPv6, Routing basat en política o PBR i funcionalitats avançades SD-WAN.
- Suport de VRFs (múltiples taules de Routing) i multiVRF Routing (per BGP i OSPF).
- 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 nombre 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, dns i TWANP. El número de Health-checks ha de ser de com a mínim 100.
    - Verificació 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 adreça IP), en el destí (adreça IP, aplicacions i/o serveis d'Internet/apli-

cacions) i en la línia amb millor qualitat d'aquell moment basat en valors de jitter, packet loss, latència, tràfic de pujada/baixada o amplada de banda, així com una combinació per pesos.

- En el cas de necessitat de llicenciament o subscripcions per activar aquestes funcionalitats, cal que aquestes estiguin incloses en la proposta durant la duració completa del contracte.

- Suport d'VXLAN i VXLAN VTEP per extensió de nivell 2 sobre xarxes de nivell 3.
- El sistema proposat ha de tenir una funcionalitat integrada de Traffic Shaping tant de trànsit sortint com a entrant sent capaç de reservar ample de banda i marcar el trànsit amb DSCP. Aquest traffic shaping ha de basar-se en aplicacions i URLs a nivell global de perfil o per IP.

5.6 VISIBILITAT

Els equips tallafocs han de poder generar topologies gràfiques físiques i lògiques, amb la integració d'altres tallafocs del fabricant, per tal de poder ser capaç de veure en un extrem a extrem que està passant en tota la xarxa.

Funcionalitat de consolidació de logs amb diferents nivells d'agrupació, en concret: per origen, destí, aplicació, amenaça, websites i polítiques per a la seva visualització.

L'eina centralitzada de gestió de registres ha de ser capaç de gestionar els logs diaris, preveient un increment anual del 5%. Durant la darrera setmana, els logs gestionats han estat:

Dia 1: 17,11 GB
Dia 2: 16,38 GB
Dia 3: 16,32 GB
Dia 4: 17,10 GB
Dia 5: 17,56 GB
Dia 6: 7,08 GB
Dia 7: 8,00 GB

L'eina proposada ha de tenir característiques similars a les eines líders del mercat per garantir la seva eficàcia i capacitat de gestió.

5.7 SEGURETAT

Quant al punt de gestió de la seguretat la solució proposada ha de contemplar les següents característiques:

- Capacitat de definir polítiques de seguretat IPv4/v6 utilitzant els següents paràmetres de coincidència:
  - Com a origen (totes les opcions):
    - Capacitat de definir una i/o més d'una interfície d'origen, incloent-hi "any". Així com "zones".
    - Capacitat d'utilitzar adreces IP, rangs i/o xarxes, FQDN, països, serveis d'internet i adreces IP's reconegudes com origen de xarxes TOR, proxy anònims (aquestes direccions han d'actualitzar-se automàticament), així com els objectes exportats dels connectors esmentats a l'apartat de característiques generals de l'equip.
    - Capacitat de fer ús usuaris/grups locals o remots mitjançant connectors AD, NAC o altres repositoris d'identitat.
    - Capacitat per declarar horaris, tant per dia/hora com a data màxima de venciment.
    - Capacitat de selecció del servei a emprar.
  - Com a destí:
    - Capacitat de definir una i/o més d'una interfície de destí, incloent-hi "any". Així com "zones".
    - Capacitat fer servir adreces IP, rangs i/o xarxes, així com objectes FQDN, països i serveis d'internet.
- Capacitat de definir polítiques de seguretat IPv4/v6 utilitzant la següent parametrització:
  - S'ha de poder seleccionar quin tràfic s'analitza a nivell 4 i quin a nivell 7, per política, sense excepció.

- La configuració del NAT sortint s'ha de poder configurar dintre de cadascuna de les polítiques de seguretat, de forma granular.
- Les diferents funcionalitats de seguretat avançades de nivell 7 s'han d'activar de forma individual a nivell de política, mai globalment. A més aquestes s'han de gestionar amb perfils per tal de ser granulars en els permisos. Aquestes funcionalitats són: antivirus, webfilter, DNS filter, Web Application Firewall, Control d'aplicacions, IPS, i DLP.
- Decidir a nivell de política quin tràfic SSL serà desxifrat per la seva anàlisi i quin només a nivell de certificat.
- En l'àmbit de logging, cal que la solució permeti activar el logging de només nivell 7, o tant de nivell 4 més nivell 7. Cal també fer captura de packets en la mateixa política.

- Capacitat de creació de regles de DoS a nivell 3 i 4, podent aplicar umbrals per serveis publicats on poder filtrar per adreces IP o països per: ip_src_session, ip_dst_session, tcp_syn_flood, tcp_port_scan, tcp_src_session, tcp_dst_session, udp_flood, udp_scan, udp_src_session, udp_dst_session, icmp_flood, icmp_sweep, icmp_src_session, icmp_dst_session, sctp_flood, sctp_scan, sctp_src_session i sctp_dst_session.
- Capacitat de definir polítiques en l'àmbit d'interfície per tal de denegar tràfic i no ser processat per la política de seguretat global. S'han de poder utilitzar adreces IP's, països, així com rangs i xarxes IP com a origen.
- Per tal d'evitar l'accés de xarxes botnet, els tallafocs han de tenir una base de dades de reputació dinàmica que bloquegi els accessos en l'àmbit d'interfície.
- Visualització del nombre d'usos i quantitat de tràfic de cada regla de seguretat, de forma àgil tant en la mateixa secció de polítiques de seguretat, això com també dintre de la configuració de cada política. També cal veure l'última vegada que s'ha emprat.

5.8 CONTROL D'APLICACIONS

La solució proposada ha de ser capaç per complir amb les següents característiques:

- Capacitat per identificar un mínim de 4000 aplicacions actives actuals (incloent-hi aplicacions web 2.0), com per exemple distingir Facebook, d'una sub-aplicació Facebook-chat o post.
- 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. És obligatori que en aquelles aplicacions personalitzades, també siguin analitzades per motors de protecció (IPS i antimalware).

5.9 IPS

Els firewalls han d'integrar una solució d'IPS, amb:

- Capacitat per protegir tant servidors com clients amb un mínim de 10000 firmes d'IPS, agrupades per categoria, severitat, objectiu i protocol. Davant la identificació d'un atac per IPS, cal que els tallafocs capturin 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.
- Capacitat de creació de firmes d'IPS per un reconeixement personalitzat.

5.10 ANTIMALWARE

Els tallafocs també han de permetre combatre qualsevol programari maliciós i per això es demana que tinguin:

- Capacitat de detecció de malware (virus, grayware, worns, etc...) basat en firmes conegudes o mètodes avançats de detecció.
- Suport de sandboxing en el cloud, 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.

5.11 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 cuotes 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 cloud 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 restringir l'accés a Youtube i Google en mode "safe search".
- Suport de rating per imatges per URL.
- Suport per a la creació de llistes blanques/negres externes sense necessitat de llicència.

5.12 DNS FILTER

- Capacitat de categoritzar dominis DNS en categories per i poder realitzar intercepció del tràfic DNS amb les següents accions: block, monitor i redirect (redirigir les consultes cap a un portal web cloud o personalitzat de bloqueig).

- La base de dades de categories dns caldrà consumir-se com un servei cloud 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 restringir l'accés a Youtube i Google en mode "safe search".
- Suport per a la creació de llistes blanques/negres externes sense necessitat de llicència.

5.13 ALTRES FUNCIONALITATS DE NIVELL 7

Altres funcionalitats de nivell 7 que la proposta ha d'incloure i han d'estar llicenciades són:

- DLP
- ICAP
- Web application firewall

5.14 APLICACIÓ DE VPN MULTIPLATAFORMA I GRATUÏTA

Cal proporcionar un client multiplataforma de forma completament gratuïta i garantir el seu funcionament durant almenys cinc anys, suportant com a mínim els sistemes operatius Microsoft Windows, Apple OS X, Linux, Android i Apple iOS. La solució ha de ser capaç de suportar com a mínim 5000 clients simultanis.

5.15 INTEGRACIONS

La plataforma ha d'incorporar les següents integracions essencials:

1. Integració amb SIEM Allienvault: la implementació d'una integració completa amb SIEM Allienvault per a l'enviament eficaç de registres (Logs). A més, és crucial incorporar una automatització que permeti el bloqueig immediat d'adreces IP malicioses detectades pel mateix SIEM.
2. Integració del servei de VPN amb SAML i SSO AdAs: és necessari la integració harmoniosa del servei VPN via SAML al producte Single Sign-On (SSO) d'AdAs.

Aquesta configuració optimitza els processos d'autenticació, garantint una experiència d'usuari més eficient i segura.

6 SUBMINISTRAMENT, INSTAL·LACIÓ I MANTENIMENT

En aquest apartat es descriu la instal·lació de la nova plataforma, la seva posada en marxa amb migració de l'actual i la posterior explotació i manteniment.

6.1 INSTAL·LACIÓ I POSADA EN MARXA:

El proveïdor de serveis gestionats ha de realitzar una instal·lació eficient dels tallafocs i la consola de registre centralitzat a les infraestructures de la Universitat de Lleida.

Garantir una posada en marxa adequada que minimitzi el temps d'inactivitat, en finestres de tall pactes i que asseguri la transició suau i transparent als nous sistemes.

Proporcionar una formació integral al personal de la universitat per assegurar-ne el correcte ús i manteniment.

6.2 MIGRACIÓ DE CONFIGURACIONS/INTEGRACIONS/DADES:

Realitzar una migració de les configuracions, integracions i dades segura i fiable des dels sistemes existents cap als nous, assegurant la integritat i la disponibilitat de la solució.

Mitigar qualsevol impacte negatiu en el rendiment dels serveis durant el procés de migració. S'ha de garantir en tot moment el servei amb la plataforma actual o amb la nova.

Assegurar la integració amb altres sistemes existents a la universitat i que ja estan en ús en la plataforma actual.

6.3 MANTENIMENT (PREVENTIU, CORRECTIU I EVOLUTIU):

Pla de Manteniment Preventiu:

El proveïdor de serveis gestionats ha de desenvolupar un pla de manteniment preventiu exhaustiu per assegurar que els tallafocs i la consola de registre centralitzat

estiguin sempre a l'avantguarda de la seguretat informàtica. Les tasques executades sobre l'equipament tenen com a objectiu prevenir possibles problemes o incidències que puguin sorgir.

Aquest pla ha d'incloure revisions periòdiques de les configuracions de seguretat, actualitzacions de firmware, comprovacions d'integritat del sistema i altres accions preventives que es considerin necessàries per prevenir incidents de seguretat. S'ha de dur a terme com a mínim dues vegades a l'any.

Dins de l'oferta, el licitador ha d'incloure obligatòriament una proposta del protocol de manteniment preventiu ofert, amb una descripció de les tasques que el licitador proposa realitzar i els elements sobre els quals es duen a terme. De la inspecció feta, s'ha d'emetre un informe final de resultats i recomanacions. Quan les operacions de manteniment preventiu requereixin la interrupció dels serveis, o en aquells casos en què no es pugui garantir la seva continuïtat, s'han de programar en l'horari que causi menys molèsties als serveis afectats.

Serveis de Suport Tècnic:

S'ha de proporcionar serveis de suport tècnic dedicats amb temps de resposta ràpids per afrontar qualsevol incident o problema emergent que pugui afectar el rendiment dels tallafocs i la consola de registre centralitzat. Aquests serveis com a mínim han de respondre als acords de nivell de servei d'aquest plec.

S'ha d'implementar un sistema de tiquets o una plataforma similar per gestionar les sol·licituds de suport, garantint una traçabilitat i resolució eficients dels incidents reportats.

Manteniment Correctiu:

El seu objectiu principal és **retornar l'equip al seu estat original**, permetent que torni a funcionar correctament i a oferir el servei pel qual va ser dissenyat. Aquest consisteix en un conjunt d'accions destinades a detectar i solucionar problemes que puguin impedir o dificultar el correcte funcionament dels equips, amb la intenció de garantir la completa operativitat del servei. Les tasques de manteniment correctiu es realitzaran com a resposta a un avís d'incidència, a conseqüència d'una alarma detec-

tada a través del sistema de monitoratge o com a resultat de la detecció d'anomalies durant les tasques pròpies del manteniment preventiu.

L'objectiu perseguit amb el servei de manteniment correctiu és la reposició en el menor temps possible, mai superior als acords de nivell del servei d'aquest document, mitjançant la reparació i/o utilització de les peces de recanvi disponibles. Aquest servei ha d'incloure tots els aspectes relacionats, especialment la mà d'obra, les peces de recanvi i els desplaçaments dels tècnics necessaris per a la reparació "in situ" dels equips. S'ha d'emprar en la mesura del possible peces de recanvi originals del fabricant, noves, no reparades i actualitzades tecnològicament.

En cas d'incidents o anomalies, el proveïdor ha d'implementar mesures correctives de manera immediata per minimitzar el temps d'inactivitat i restaurar la funcionalitat normal dels sistemes afectats.

S'ha de proporcionar un informe detallat de cada incident, incloent-hi la causa, la solució implementada i les recomanacions per evitar incidents similars en el futur.

Manteniment Evolutiu:

Per adaptar-se als canvis en l'entorn de seguretat cibernètica, el proveïdor ha d'incorporar millores evolutives als tallafocs i la consola de registre centralitzat.

Això ha d'incloure la implementació de noves funcionalitats, adaptacions a noves amenaces de seguretat i actualitzacions continuades del software i els protocols de seguretat.

Auditories Periòdiques:

Realització d'auditories periòdiques per avaluar l'eficàcia dels mecanismes de seguretat implementats.

Les auditories han de tenir l'abast d'aspectes tècnics, com ara la configuració dels tallafocs, i processos operatius, garantint una supervisió completa de la seguretat.

Mitjançant aquest enfocament integral del manteniment, es pretén assegurar que els tallafocs i la consola de registre centralitzat de la Universitat de Lleida estiguin sempre actualitzats, eficaços i resistents davant de les amenaces cibernètiques en constant evolució.

Monitoratge

La Universitat de Lleida té un sistema de monitoratge basat en el programari Zabbix que actualitza de manera regular. L'adjudicatari pot utilitzar aquest sistema per incloure els actius objecte d'aquest contracte, o bé si ho considera adient, habilitar sistemes de supervisió i monitoratge externs a les dependències de la UdL, de cara a garantir la supervisió continuada dels sistemes. En qualsevol cas s'ha d'estudiar la compatibilitat i en cas que no sigui possible s'ha d'emprar el que la UdL ja té en producció.

7 ACORDS DE NIVELL DE SERVEI (ANS)

Els acords de nivell de servei fan referència, principalment, a les condicions que s'estableixen en la prestació del manteniment.

7.1 CONDICIONS GENERALS

A continuació s'indiquen les principals condicions del servei:

Horari tramesa d'incidències	24 x 7
Suport remot	24 x 7
Suport in situ	24 x 7
Suport telefònic	24 x 7
Diagnòstic remot	24 x 7
Resolució d'incidències	(segons s'indica més endavant)

7.2 CLASSIFICACIÓ D'INCIDÈNCIES

L'atenció a la resolució d'incidències es procura segons la prioritat assignada a aquestes. La UdL classifica les incidències tenint en compte dos factors:

- **IMPACTE**: mesura quant d'important és la incidència en l'afectació al volum d'activitat que se'n deriva. Es valora a partir del nombre d'usuaris que es veuen afectats per aquesta.
- **URGÈNCIA**: amb caràcter general s'associa a la rellevància del servei IT que es veu afectat (per exemple: correu electrònic, web, altres...)

Tenint en compte l'anterior, s'estableix la següent classificació de prioritats en la resolució d'incidències segons es mostra en la taula adjunta:

		IMPACTE		
		ALT	MIG	BAIX
URGÈNCIA	ALTA	Prioritat 1	Prioritat 2	Prioritat 3
	MITJA	Prioritat 2	Prioritat 3	Prioritat 4
	BAIXA	Prioritat 3	Prioritat 4	Prioritat 4

Com a criteri general es consideren dos grans grups d'incidències:

- **CRÍTIQUES** les que tenen associades prioritats 1 i 2. Temps de resposta inferior a 1 h.
- **NO CRÍTIQUES** les que tenen associades prioritats 3 i 4. Temps de resposta inferior a 8 h.

El licitador indica quins són els temps de resposta i resolució per als diferents tipus d'incidències que s'han considerat en la classificació anterior. Els temps de resolució no pot superar els màxims indicats.

7.3 DIAGNÒSTIC RESULTA EN AVARIA DE MAQUINARI

En el cas que la incidència sigui provocada per una avaria de maquinari, s'efectua la reposició del component defectuós (i la seva configuració) en un termini no superior a les VUIT (8) hores (in situ).

En el supòsit que la previsió de disponibilitat del recanvi superi les 24 hores, l'adjudicatari ha de proposar una mesura alternativa per tal de garantir la continuïtat del servei.

7.4 DIAGNÒSTIC RESULTA EN FALLIDA DE PROGRAMARI

En aquest cas la resolució de les incidències s'ha d'ajustar als temps màxims establerts que s'indiquen a continuació:

GRUP	PRIORITAT	Temps resolució (h)
CRÍTIQUES	1	4 h

	2	8 h
NO CRÍTIQUES	3	24 h
	4	72 h

7.5 RESUM ANS

ANS						
Franja Horària	**Categorització**		**Horari de recepció**	**Temps màxim de resposta**	**Temps màxim d'inici d'actuació**	**Temps màxim de resolució**
24x7	**CRITICA**	**1**	**PERMANENT**	**IMMEDIAT**	**< 2 h**	**< 4 hores**
		2				**< 8 hores**
	NO CRITICA	**3**				**24 h**
		4				**72 h**

8 DURACIÓ DEL CONTRACTE I TERMINI D'EXECUCIÓ

El present punt estipula un termini de 16 setmanes, començant des de la data de signatura del contracte, per a la recepció, instal·lació del material, així com tota la migració i configuració dels sistemes acordats. Des del moment de validació de la posada en marxa per part de la Universitat començarà a comptar termini de validesa del llicenciament i garantia.

La duració del contracte de manteniment s'estableix en un període d'un any a partir de la posada en marxa de l'equipament.

A més a més, és imperatiu que el suport proporcionat pel fabricant, tant pel que fa al programari, com el maquinari, s'estengui durant un termini mínim de cinc anys. Aquesta prolongació del suport ha d'assegurar la continuïtat operativa i l'estabilitat dels sistemes al llarg del temps especificat.

Fins que el subministrament, instal·lació i configuració del nou equipament es faci efectiva, l'adjudicatari assumeix la responsabilitat de mantenir tant en programari,

com en maquinari, la plataforma actual. A continuació, es detallen les fases clau d'aquest termini:

Fase de Preparació:

- Definició del programa de treball, pla detallat d'execució i assignació de recursos.
- Recepció del material necessari i verificació de la seva integritat.
- Establiment de reunions inicials amb el personal tècnic de la Universitat de Lleida per coordinar les activitats.

Fase d'instal·lació:

- Execució de les instal·lacions físiques dels tallafocs i la consola de registre centralitzat.
- Verificació de la correcta connexió dels equips amb la infraestructura existent.
- Validació de la disponibilitat dels serveis bàsics i les connexions de xarxa necessàries. És possible que no es disposi de les connexions suficients per duplicar totes les connexions mentre la plataforma actual està en servei.

Fase de Configuració:

- Adequació del firmware dels equips per tal que la migració sigui tan senzilla com sigui possible.
- Configuració dels paràmetres de seguretat dels tallafocs segons les especificacions de la Universitat de Lleida.
- Desenvolupament i implementació de polítiques de registre centralitzat.
- Proves exhaustives per assegurar la interoperabilitat dels sistemes configurats.

Fase de Migració:

- Desenvolupament d'un pla detallat de migració de configuració i dades, incloent-hi la identificació i classificació de les configuracions/dades a migrar. Revi-

sió de qualsevol configuració a la plataforma existent que pugui ser obsoleta i no sigui necessari traslladar.

- Execució de la migració amb una atenció especial a la integritat i la disponibilitat de la informació.
- Actualització de la versió del firmware dels equips per tal que la solució quedi en la versió més adequada per tal de garantir el bon funcionament amb el màxim de funcionalitats.
- Reconnexió física per posada en producció del nou equipament.
- Realització de proves post-migració per validar la integritat de les dades migrades.

Durant l'any de durada del contracte, a comptar des de la posada en marxa del nou equipament, el proveïdor es compromet a proporcionar serveis gestionats. El proveïdor ha d'assegurar el funcionament òptim dels tallafocs actuals mentre no siguin reemplaçats per la nova solució, així com de la nova plataforma desplegada i de la consola de registre centralitzat.

Ubicació de l'equipament

[Ubicació 1] Sistema tallafocs en alta disponibilitat
Edifici Rectorat (Sala CPD 1.12-13)
Plaça Víctor Siurana s/n
25001 Lleida

[Ubicació 2] Firewall de seu remota
Campus Universitari d'Igualada UdL (Sala CPD)
Av. Pla de la Massa, 8
08700 Igualada

9 LLIURABLES DOCUMENTALS DEL CONTRACTE

Es demana com a mínim la següent documentació a entregar durant l'execució del contracte:

- Informes amb les proves de validació realitzades, els seus resultats i acceptació per part de la Universitat.
- Procediment per fer efectiu el compromís de suport. Aquest procediment ha d'incloure com a mínim una adreça de correu i un telèfon, juntament amb els temps de resposta i resolució acordats.
- Credencials per accedir al suport del fabricant.
- Model de relació detallant instruccions sobre la gestió de peticions i incidències al llarg de la vigència del contracte.
- Certificat de garantia i de llicenciament vàlid per mínim 5 anys.
- Repositori de tot el programari utilitzat: eines de gestió, monitoratge, programari instal·lat.
- En els casos d'incidències l'adjudicatari emet amb posterioritat a la seva resolució, un informe detallat sobre el diagnòstic efectuat i accions dutes a terme, així com la seva cronologia.
- Com a criteri general, en la resolució d'incidències que no donin compliment als ANS establerts en aquest plec de prescripcions, l'adjudicatari ha d'emetre un informe amb el pla d'acció dut a terme. La finalitat de justificar les accions extraordinàries que comporten l'incompliment dels acords de nivell de servei establerts, o si és per causes imputables a terceres parts.
- Documentació en format electrònic (PDF).

10 INFORMACIÓ BASE

La unitat de Sistemes d'informació i comunicacions (SIC) facilita a l'empresa adjudicatària la informació de què disposi relacionada amb les tasques encomanades objecte del present contracte. Tota la informació que es proporcioni és propietat de la Universitat de Lleida i no podrà ser utilitzada per altres finalitats. En els termes que descriu el Reglament General de Protecció de Dades (RGPD).

11 ESQUEMA NACIONAL DE SEGURETAT (ENS)

L'adjudicatari ha de complir la normativa legal aplicable en matèria de seguretat en el marc dels serveis prestats, específicament, Llei 9/2017, de 8 de novembre, de Contractes del Sector Públic, per la qual es transposen a l'ordenament jurídic espanyol les Directives del Parlament Europeu i de Consell 2014/23/UE i 2014/24/UE, de 26 de febrer de 2014 i amb el Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'Administració Electrònica.

Aquest plec està sotmès al Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'Administració Electrònica (ENS), i, per tant, es imperatiu complir els més alts estàndards de seguretat.

En particular l'article 18 de Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'Administració Electrònica, el licitador inclou referència precisa, documentada i acreditativa que els productes de seguretat, serveis, equips, sistemes, aplicacions o els seus components, compleixen amb el que indica la mesura op.pl.5 sobre components certificats, recollida en l'apartat 4.1.5 de l'annex II de l'esmentat Reial decret 3/2010, de 8 de gener. En el cas que no hi hagi la certificació indicada en el paràgraf anterior, o estigui en procés, s'inclou, igualment, referència precisa, documentada i acreditativa que són els més idonis.

És imprescindible seguir detalladament les guies de suport proporcionades pel CCN, amb especial atenció a la guia del procediment d'ús segur dels tallafocs FortiGate o qualsevol solució que resulti guanyadora de la present licitació.