UPCnet

PLEC DE PRESCRIPCIONS TÈCNIQUES

Subministrament de dispositius i components pel servei de tallafocs interns de la Universitat Politècnica de Catalunya

Codi d'expedient LIC-2024-48

UPCnet

Índex de continguts

1 NECESSITAT DE LA CONTRACTACIÓ 3
2 OBJECTE DEL CONTRACTE 3
3 REQUERIMENTS OBLIGATORIS 5
3.1. Característiques generals dels equips 5
3.2. Rendiment 7
3.3. Característiques dels Tallafocs 8
3.4. Connectivitat i característiques físiques. 8
3.5. Gestió. 9
3.6. Networking. 9
3.7. Alta disponibilitat. 10
3.8. Visibilitat. 11
3.9. Seguretat. 11
3.10. Control d'aplicacions. 12
3.11. IPS. 13
3.12. Antimalware. 13
3.13. Webfilter. 14
3.14. DNS Filter. 14
3.15. Altres funcionalitats de nivell 7. 14
3.16. VPN. 15
3.17. Controladora d'accés segur integrada. 15
5. ESQUEMA NACIONAL DE SEGURETAT (ENS) 15
6. TERMINI I LLOC DE LLIURAMENT 16

UPCnet

1 NECESSITAT DE LA CONTRACTACIÓ

La Universitat Politècnica de Catalunya (UPC d'ara en endavant) 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 es proporciona a tota la comunitat universitària.

Amb aquesta línia de treball, la UPC està immersa en un procés de securització integral de les seves Unitats Tècniques de Gestió (UTG), fet que implica la implementació de diverses mesures de seguretat per garantir la integritat, disponibilitat i confidencialitat de les dades i sistemes. Fins al moment s'han dut a terme actuacions a complementar els sistemes de seguretat de diferents UTGs sobre la base de la instal·lació i posada en funcionament de diferents tallafocs del fabricant Fortinet, les prestacions i les funcionalitats del qual responen de manera precisa a les necessitats puntuals en termes de seguretat i rendiment.

Actualment, i per completar aquesta fase, és necessària l'adquisició d'un parell de tallafocs que permetin reforçar la seguretat perimetral de les xarxes internes al Campus Nord de la UPC, protegint contra amenaces externes i garantint una major resiliència davant possibles atacs.

La xarxa a protegir es troba segmentada en diferents Unitats i Escoles, cadascuna amb necessitats i requisits específics de seguretat. Per tant, és imprescindible que els dispositius a adquirir disposin de funcionalitats i gestió multi-tenant, que permetin gestionar de manera independent les polítiques de seguretat de cada segment o unitat de la xarxa, oferint així una protecció adaptada a les característiques particulars de cada àrea.

2 OBJECTE DEL CONTRACTE

El present document té com a objectiu definir els requeriments tècnics mínims i específics per a l'adquisició de dos firewalls destinats a protegir les xarxes internes de la UPC. Aquests dispositius han de ser capaços de gestionar el trànsit de dades de manera eficient, filtrar contingut maliciós, i garantir la continuïtat del servei davant possibles incidents de seguretat. També s'ha de tenir en compte el manteniment de l'equipament subministrat per un període mínim de 3 anys.

Per tant, l'objecte d'aquesta licitació és:

- L'adquisició de dos equips tallafocs, per proveir una solució de seguretat a la ubicació del Campus Nord (UTG CNTIC), 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 3 anys) i llicenciament específic (mínim 3 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 3 anys.

  A més, per a la interconnexió eficient dels diferents centres beneficiaris de la solució de seguretat, serà requisit el subministrament dels adaptadors de fibra òptica necessaris. S'han considerat necessaris aquests elements:
  - 8 Transceivers 10GE SFP+ LR
  - 8 Transceivers 10GE SFP+ SR
  - 4 Transceivers 25GE SFP28 LR
  - 4 Transceivers 25GE SFP28 SR

- L'adquisició del servei de suport per part del fabricant durant la vigència del contracte (3 anys) a comptar a partir de la validació de la instal·lació. Aquest suport ha de tenir en consideració aquestes mètriques:

	Per dispositiu
Temps de resposta davant problemes crítics	1 hora
Temps de resposta davant problemes no crítics	Next Business Day
Suport Web	Inclòs
Suport telefònic	Inclòs
RMA	Advanced replacement (NBD)
Actualitzacions programari	Inclòs
Eines de suport online	Inclòs
Portal de gestió del actius	Inclòs

UPCnet

3 REQUERIMENTS OBLIGATORIS

3.1. Característiques generals dels equips

- La proposta haurà d'incloure durant la totalitat de la duració del contracte, així com les possibles pròrrogues, 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 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 de 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 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 per tota la duració del contracte.

- S'hauran 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

- S'haurà d'incloure a la proposta, dintre dels mateixos appliance, la funcionalitat d'auditoria pròpia del Sistema, que com a resultat tingui un indicador o valor numèric de risc, així com puntuació negativa per cada paràmetre auditat no complert. Aquests paràmetres que s'han de comprovar son com a mínim: política de seguretat sense ús en

els últims 90 dies, política de contrasenyes dèbils i comprovació del llicenciament/suport.

- La pròpia 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 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, AWS, Oracle i AliCloud.
    - Cloud privada: VMware NSX i ESXi, Openstack, Kubernetes, Cisco ACI i Nuage.
    - Fonts d'identitat: 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, 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 event del tallafocs, aquest enviï (tots alhora): un email, una notificació tipus push a dispositius Iphone e invocar funcions AWS Lambda, Google functions, Azure Functions, AliCloud Function, 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.

- S'exigeix el màxim nivell de certificació del fabricant per a assegurar el correcte desplegament i integració dels equips.

3.2. Rendiment

- 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.

- El tallafocs disposarà 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 **8 Milions sessions concurrents**. Així com a mínim **550.000** noves sessions per segon.

- El tallafocs ha de tenir una **latencia** inferior a 4.12 µs (per paquets 64 byte UDP) que caldrà acreditar amb el datasheet oficial del fabricant.

- Ha de tenir capacitat per com a mínim de **30.000 polítiques de firewall.**

- El rendiment per tràfic SSL VPN ha de ser de com a mínim 4.3 Gbps i per tràfic IPSEC VPN (512 bytes) de 55 Gbps.

- A nivell 7, l'equip ha de disposar de com a mínim el següent rendiment:

    - Rendiment IPS: 14 Gbps per tràfic Enterprise MIX.
    - Rendiment NGFW (IPS i control d'aplicacions): 11.5 Gbps per tràfic Enterprise MIX.
    - Rendiment amb Threat Protection (Firewall mes IPS, control d'aplicacions i motor antimalware actius): 10.5 Gbps per tràfic Enterprise MIX.

  Caldrà acreditar que aquestes tres últimes dades siguin amb logging actiu.

    - Rendiment Inspecció SSL amb IPS: 9 Gbps mesurat amb diferents Ciphers.
    - Rendiment per control d'aplicacions: 32 Gbps mesurat per http 64K.

3.3. Característiques dels Tallafocs.

Es requereix que els nous tallafocs siguin de nova generació amb hardware específic. Caldrà 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 haurà d'incloure coprocessadors hardware per accelerar el tràfic criptogràfic així com la inspecció de seguretat per hardware, incloent la recerca de signatures d'atacs.

3.4. Connectivitat i característiques físiques.

Els tallafocs han de incloure en la oferta presentada el següent número de interfícies com a mínim (per equip):

- 1 port de consola.
- 2 port d'USB 3.0 per a la connexió de modem 3G/4G i/o pendrive.
- El port USB ha de 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 canvis d'equipament.
- 4 ports 10GE SFP+
- 4 ports 25GE/10GE SFP28/SFP+
- 24 ports 1GE (16 ports 1GE RJ45 + 8 ports 1GE SFP)
- 2 ports HA/Gestió dedicats
- Instal·lació en rack de 19'' i no més de 1 RU.
- Consum màxim inferior a 255 W.
- En el cas que l'equipament permeti ampliacions modulars d'interfaces, caldrà 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.
- Fonts d'alimentació redundants i amb Hot Swap.

3.5. 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.
- Quedaran 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. Es 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.

3.6. Networking.

- 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 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, dns i TWANP. El numero 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 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 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.

3.7. Alta disponibilitat.

- La funcionalitat d'alta disponibilitat ha d'estar disponible sense necessitat de llicencia.
- Suport HA tipus Actiu – Passiu, Actiu - Actiu i mode mixte. El mode mixte implica poder tenir Firewalls virtuals actius i passius de forma barrejada, es a dir, el màster de certs Firewalls virtuals sigui la primera unitat de tallafocs, mentre que la segona unitat de tallafocs és màster de la resta de firewalls virtuals alhora.
- 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.
- Capacitat de funcionament en mode actiu/actiu sincronitzant sessions entre els dos nodes però mantenint adreçament IP diferenciat en les interfícies de cada node del clúster.
- 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.

3.8. 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.

  Aquesta visualització ha de ser tipus "Drill-down", és a dir, poder seleccionar uns dels objectes agrupats i anar filtrant el resultat en base a aquesta selecció, fins a saber el detall complet.

Aquests requeriments hauran de poder acomplir-se des de la mateixa GUI dels appliances, en temps real, i sense necessitat d'una consola central de gestió.

3.9. Seguretat.

- 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 Interface d'origen, incloent "any". Així com també "zones".
    - Capacitat d'utilitzar direccions ip, rangs i/o xarxes, FQDN, països, serveis d'internet i direccions ip's reconegudes com origen de xarxes TOR, proxies anònims (aquestes direccions han d'actualitzar-se automàticament), així com els objectes exportats dels connectors esmentats a l'apartat de caracterisques generals de l'equip.
    - Capacitat d'utilitzar usuaris/grups locals o remots mitjançant connectors AD, NAC o altres repositoris d'identitat.
    - Capacitat per declarar horaris o "schedule" tant per dia/hora com a data màxima de venciment.
    - Capacitat de selecció del servei a utilitzar.
  - Com a destí:
    - Capacitat de definir una i/o més d'una Interface de destí, incloent "any". Així com també "zones".
    - Capacitat d'utilitzar direccions 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'analitzarà 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'activaran de forma individual a nivell de política, mai a nivell global. A més aquestes es gestionaran amb perfils per tal de ser granulars en els permisos. Aquestes funcionalitats son: antivirus, webfilter, DNS filter, Web Application Firewall, Control d'aplicacions, IPS, i DLP.

- Decidir a nivell de política quin tràfic SSL serà desxifrat pel seu anàlisis i quin només a nivell de certificat.

- A nivell 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 pròpia política.

- Capacitat de creació de regles de DoS a nivell 3 i 4, podent aplicar umbrals per serveis publicats on poder filtrar per direccions 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 a nivell d'Interface per tal de denegar tràfic i no ser processat per la política de seguretat global. S'han de poder utilitzar direccions 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 a nivell d'Interface.

- Visualització del número d'usos i quantitat de tràfic de cada regla de seguretat, de forma àgil tant en la pròpia secció de polítiques de seguretat, això com també dintre de la configuració de cada política. També cal veure l'ultima vegada que se ha utilitzat.

3.10. Control d'aplicacions.

- Capacitat per identificar un mínim de 4400 aplicacions actives actuals (incloent 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 per identificar aplicacions Industrials com Modbus.

- Capacitat de creació de firmes d'aplicacions per un reconeixement personalitzat. És obligatori que en aquelles aplicacions customitzades, també siguin analitzades per motors de protecció (IPS i antimalware).

3.11. IPS.

- Capacitat per protegir tant servidors com clients amb un mínim de 11000 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 umbral d'ús en un temps determinat.

- Capacitat de creació de firmes d'IPS per un reconeixement personalitzat.

3.12. Antimalware.

- 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 un tamany mínim 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.

3.13. 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 llicencia.

3.14. DNS Filter.

- Capacitat de categoritzar dominis DNS en més de 60 categories per 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 llicencia.

3.15. Altres funcionalitats de nivell 7.

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

    - DLP

    - ICAP

    - Web application firewall

3.16. VPN.

- El dispositiu admetrà fins a un màxim de 10.000 usuaris simultanis VPN SSL, ja sigui amb agent o sense, però en qualsevol cas sense llicència addicional.

- El sistema proposat haurà 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.

- El sistema proposat haurà 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.

- Suport d'agregació de túnels VPN i balanceig per packet podent així afegir l'ampla de banda dels accessos VPN_IP entre seus.

- Capacitat d'integració del mateix fabricant de doble factor d'autenticació via token mòbil, així com per SMS i correu electrònic, integrat en la mateixa plataforma de seguretat. Aquest token també s'ha de poder fer servir per l'accés a la GUI dels equips tallafocs.

3.17. Controladora d'accés segur integrada.

- El sistema ha de ser capaç d'actuar com controladora de punts d'accés wireless així com de switches del mateix fabricant.

- La capacitat mínima de 1024 punts d'accés wifi gestionats del mateix fabricant, i de 96 switchs gestionats del mateix fabricant.

- 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 gestió dels APs i Switches es farà des de la mateixa interfície gràfica i CLI des de la qual es gestiona el Firewall o des de la consola central de gestió.

5. 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.

6. TERMINI I LLOC DE LLIURAMENT

Els terminis màxims a partir de la data de formalització del contracte són de 60 dies per completar el subministrament.

El lloc de lliurament serà el següent:

UPCnet
Edifici C' - Carrer Pascual i Vila 15
08028 BARCELONA