Agència de l'Habitatge de Catalunya

PLEC DE PRESCRIPCIONS TÈCNIQUES PER A LA CONTRACTACIÓ DEL SUBMINISTRAMENT DE MAQUINARI PER L'EVOLUCIÓ DE LA SEGURETAT PERIMETRAL DE L'AGÈNCIA DE L'HABITATGE DE CATALUNYA AMB TECNOLOGIA TIPUS FORTINET

1. OBJECTE DEL SERVEI

L'objectiu del servei és ampliar l'entorn de seguretat perimetral que actualment té l'Agència a les seves instal·lacions del carrer Diputació, 92 a les oficines de les seus territorials de Lleida i Tarragona, amb el subministrament de nou maquinari i contractar el servei de manteniment de tots els components que formen la seguretat perimetral de l'Agència.

La seguretat perimetral és un terme que s'utilitza en les instal·lacions informàtiques per indicar els components que formen part de la protecció entre una organització i la resta del mon. Actualment i donat el creixement desmesurat d'atacs contra diferents webs, fuites d'informació, espionatge industrial, etc. fa que sigui del tot necessari seguir incorporant noves mesures de seguretat que ens protegeixin dels atacs més habituals des d'internet i fora d'ella.

1.1. Situació actual.

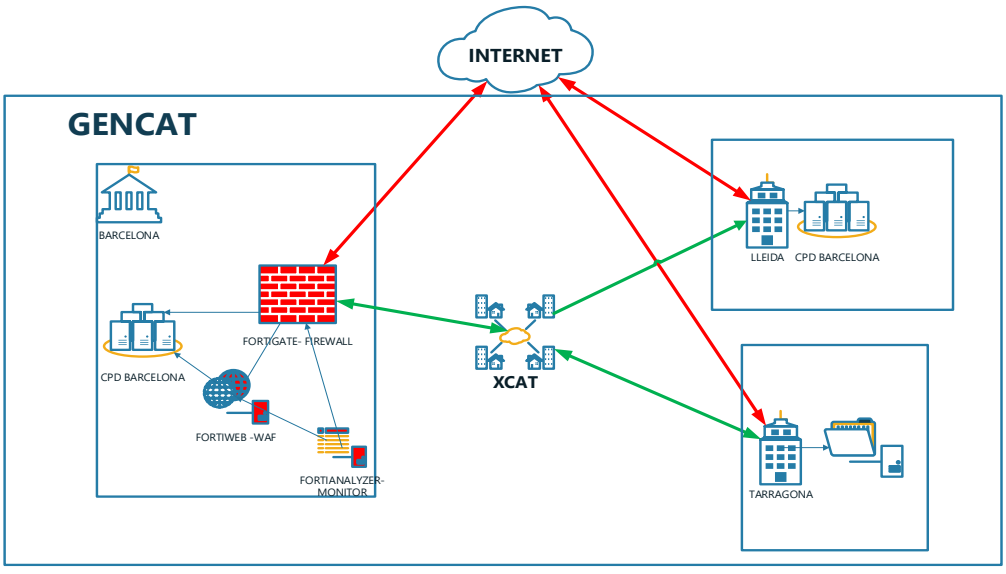
Actualment l'Agència disposa d'un sistema de seguretat perimetral en tecnologia Fortinet que li permet defensar-se dels atacs informàtics que li arriben des d'internet, podent afectar a les aplicacions com Habicat, Xarxa, correu, Ajuts, etc., a la navegació per internet o a l'hora de compartir fitxers.

Aquest sistema de seguretat està composat de tres parts:

- Firewall: tallafocs d'aplicatius que protegeix del tràfic d'internet

- Waf: un Firewall d'aplicacions web (WAF) és un tipus de tallafocs que supervisa, filtra o bloqueja el tràfic HTTP cap a i des d'una aplicació web. Es diferencia d'un tallafocs normal en què pot filtrar el contingut d'aplicacions web especifiques, mentre que un tallafocs de xarxa protegeix el trànsit entre els servidors. A l'inspeccionar el tràfic HTTP 1, WAF protegeix les aplicacions web contra atacs com els d'injecció SQL, XSS i falsificació de petició de llocs creuats (CSRF).

- Monitor: enregistra totes les peticions per poder tenir un control de les peticions que passen pel sistema i fer un seguiment del tràfic d'informació/dades.



1.2. Situació desitjada.

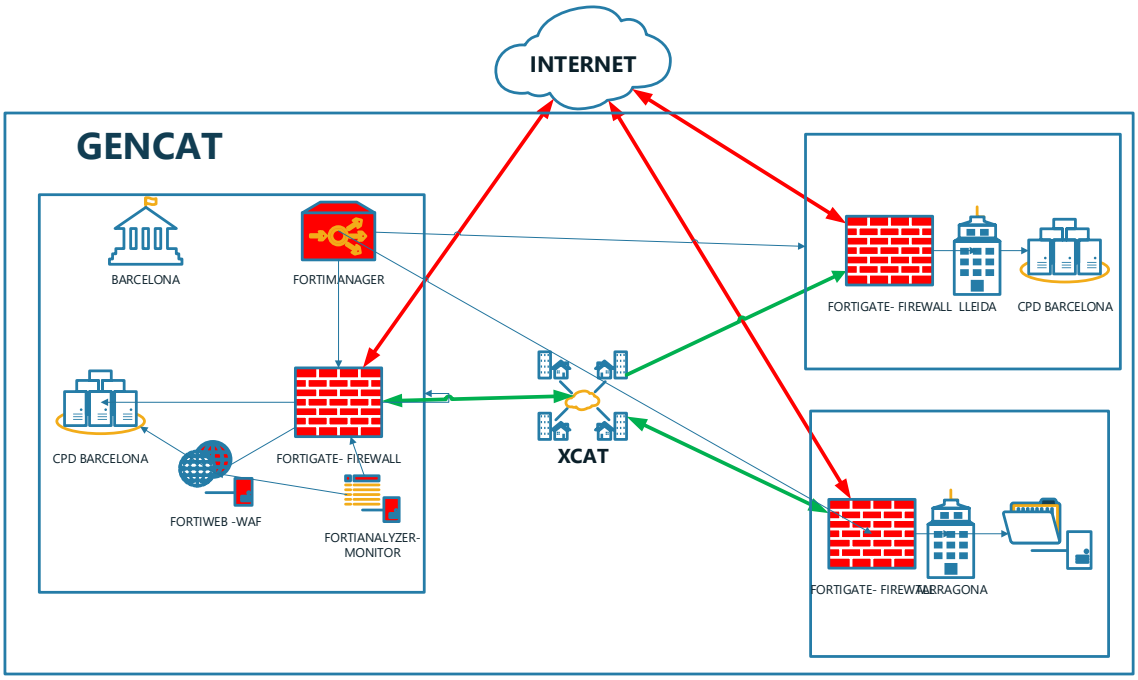
Amb l'ampliació de la seguretat perimetral dotarem a les seus de Lleida i Tarragona de la mateixa seguretat que l'Agència té a la seu central de Barcelona.

A les seus de Lleida i Tarragona només caldrà tenir el Firewall que protegeix el tràfic quan es connecten a internet.

A Barcelona hem de canviar el Firewall actual ja que s'ha quedat sense suport per part del fabricant perquè és obsolet. Renovar la llicència és més car que adquirir un de nou i igualment no es podria actualitzar (canviar de versió) per la qual cosa considerem més adient substituir-lo perquè podem tenir problemes i no es pot reaprofitar per cap altre lloc.

Actualment tenim un Firewall i la gestió/control és única, però quan tinguem la infraestructura desitjada amb 3 Firewall necessitem controlar la resta de Firewall de forma controlada, es per aquest motiu que necessitem la figura d'un gestor com Fortimanager o similar.

També s'ha d'adquirir l'antivirus del fabricant perquè dona una visibilitat que actualment no tenim dels ordinadors amb aquesta solució i com és configurable en remot, permet un control del que passa a cada ordinador. Amb la situació actual és cada vegada més important tenir control dels ordinadors remotament.



2. DESCRIPCIÓ DEL SERVEI

Per a poder realitzar aquesta ampliació s'ha d'adquirir el següent material en tecnologia tipus Fortinet o similar amb el corresponent manteniment:

	PRODUCTES FORTINET	
PART NUMBER	**DESCRIPCIÓ**	**QUANTITAT**
FG-600E-BDL-950-36	FORTIGATE-600E hardware plus 3 anys 24x7 FortiCare i FortiGuard Unified Threat Protection (UTP)	2
FG-60F-BDL-950-36	FortiGate-60F hardware plus 3 anys 24x7 FortiCare i FortiGuard Unified Threat Protection (UTP)	2
FG-100F-BDL-950-36	FortiGate-100F hardware plus 3 anys 24x7 FortiCare i FortiGuard Unified Threat Protection (UTP)	2
FC1-15-EMS01-297-02-12	FortiClient Security Fabric Agent per a 25 clients 1 any Security Fabric Agent subscripció llicència per a 25 endpoints. Inclòs Fabric Agent, Anti-malware, Remote Access, Web Filter, Vulnerability Scan, Software Inventory, Application Firewall, SSOMA, Theat Outbreak Detection, Sandbox Agent (On-Prem), Central Management (On-Prem) i suport 24x7	32
FMG-VM-BASE	Llicència base per a FortiManager-VM	1
FC1-10-M3004-248-02-36	Manteniment 24x7 FortiCare Contract (1-10 devices/Virtual Domains)	1

	SERVEIS PROFESSIONALS	
	DESCRIPCIÓ	**QUANTITAT**
Desplegament de la solució Forti	Serveis professionals d'instal·lació i configuració dels equips segons abast indicat. No s'inclouen els treballs fora d'horari laboral	1
Servei de suport i manteniment correctiu i preventiu de la plataforma ofertada segons l'abast indicat (1 any en modalitat 8x5)	Serveis professionals de suport i manteniment correctiu i preventiu 8x5	1
Servei de suport i manteniment evolutiu de la plataforma ofertada segons l'abast indicat (bossa anual de 40 hores).	Serveis professionals de suport i manteniment evolutiu (bossa anual de 40 hores)	1

Els requeriments obligatoris i generals dels equips de seguretat són els següents:

- 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 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 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 durant tota la duració del contracte.

- 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 són 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'amenaces: 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 correu electrònic, una notificació tipus push a dispositius mòbils, 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 mòbils 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.

2.1. Característiques del maquinari

Seu de Barcelona:

Renovació clúster firewalls Fortigate FG-200D-BDL actuals per equips de nova generació, un clúster de 2 firewalls Fortigate FG-600E que disposa de ports de 10 GB, configurats en alta disponibilitat.

Característiques FG-600E:

- 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 36 / 36 / 27 Gbps de rendiment de firewall per paquets de 1518, 512 i 64 bytes en IPv4 ; i de 36 / 36 / 27 Gbps de rendiment de firewall per paquets de 1518, 512 i 64 bytes en IPv6 .

- El tallafocs ha de ser capaç de gestionar fins 8 Milions sessions concurrents. Així com a mínim 450.000 noves sessions per segon.

- El tallafocs ha de tenir una latència de 1,54 µs (per paquets 64 byte UDP).

- Ha de tenir capacitat per com a mínim de 10.000 polítiques de firewall.

- El rendiment per tràfic SSL VPN ha de ser de com a mínim 7 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 IPS: 10 Gbps per tràfic Enterprise MIX.
    - Rendiment NGFW (IPS i control d'aplicacions): 9,5 Gbps per tràfic Enterprise MIX.
    - Rendiment amb Threat Protection (IPS, control d'aplicacions i motor antimalware actius): 7 Gbps per tràfic Enterprise MIX.

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

    - Rendiment Inspecció SSL amb IPS: 8 Gbps mesurat amb diferents Ciphers.
    - Rendiment per control d'aplicacions: 15 Gbps mesurat per http 64K.

Seu de Lleida:

Adquisició/Implantació d'un nou clúster de 2 firewalls Fortigate FG-100-F configurats en alta disponibilitat.

Característiques FG-100F:

- 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 20 / 18 / 10 Gbps de rendiment de firewall per paquets de 1518, 512 i 64 bytes en IPv4.

- El tallafocs ha de ser capaç de gestionar fins 1,5 Milions sessions concurrents. Així com a mínim 56.000 noves sessions per segon.

- El tallafocs ha de tenir una latència de 4,97 µs (per paquets 64 byte UDP).

- Ha de tenir capacitat per com a mínim de 10.000 polítiques de firewall.

- El rendiment per tràfic SSL VPN ha de ser de com a mínim 1 Gbps i per tràfic IPSEC VPN (512 bytes) de 11,5 Gbps.

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

    - Rendiment IPS: 2,6 Gbps per tràfic Enterprise MIX.
    - Rendiment NGFW (IPS i control d'aplicacions): 1,6 Gbps per tràfic Enterprise MIX.
    - Rendiment amb Threat Protection (IPS, control d'aplicacions i motor antimalware actius): 1 Gbps per tràfic Enterprise MIX.

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

    - Rendiment Inspecció SSL amb IPS: 1 Gbps mesurat amb diferents Ciphers.

- Rendiment per control d'aplicacions: 2,2 Gbps mesurat per http 64K.

Seu de Tarragona:

Adquisició/Implantació d'un nou clúster de 2 firewalls Fortigate FG-60F configurats en alta disponibilitat.

Característiques FG-60F:

- 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 10/10/6 Gbps de rendiment de firewall per paquets de 1518, 512 i 64 bytes en IPv4.

- El tallafocs ha de ser capaç de gestionar fins 700.000 sessions concurrents. Així com a mínim 35.000 noves sessions per segon.

- El tallafocs ha de tenir una latència de 3,3 µs (per paquets 64 byte UDP).

- Ha de tenir capacitat per com a mínim de 5.000 polítiques de firewall.

- El rendiment per tràfic SSL VPN ha de ser de com a mínim 900 Mbps i per tràfic IPSEC VPN (512 bytes) de 6,5 Gbps.

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

    - Rendiment IPS: 1,4 Gbps per tràfic Enterprise MIX.
    - Rendiment NGFW (IPS i control d'aplicacions): 1 Gbps per tràfic Enterprise MIX.
    - Rendiment amb Threat Protection (IPS, control d'aplicacions i motor antimalware actius): 700 Mbps per tràfic Enterprise MIX.

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

    - Rendiment Inspecció SSL amb IPS: 630 Mbps mesurat amb diferents Ciphers.
    - Rendiment per control d'aplicacions: 1,8 Gbps mesurat per http 64K.

El maquinari de les 3 seus haurà de tenir 3 anys de suport en modalitat 24x7 que inclogui el bundle Unified Threat Protection.

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.

Característiques de la configuració de la xarxa

- Suport de protocols RIP v1/v2, OSPF, ISIS, BGP, WCCP i Multicast per IPv4 e IPv6, Routing basat en política o PBR.
-
- 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.

Alta disponibilitat

- La funcionalitat d'alta disponibilitat ha d'estar disponible sense necessitat de llicencia.

- Suport HA tipus Actiu – Passiu, Actiu - Actiu i mode mixta. 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 es 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.

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 esta 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.

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.

o 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:

o S'ha de poder seleccionar quin tràfic s'analitzarà a nivell 4 i quin a nivell 7, per política, sense excepció.

o La configuració del NAT sortint s'ha de poder configurar dintre de cadascuna de les polítiques de seguretat, de forma granular.

o 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.

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

o 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.

Control d'aplicacions

- Capacitat per identificar un mínim de 1900 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. 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 10000 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.

Antivirus

- 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.

Webfilter (tallafocs web)

- 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.

DNS Filter

- Capacitat de categoritzar domins DNS en més de 60 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 llicencia.

Altres funcionalitats

- Altres funcionalitats de nivell 7 que la proposta ha d'incloure son:
    - DLP.
    - DNS Filter.

- ICAP.
- Web application firewall.

VPN

- FG-600E, ell dispositiu admet fins a un màxim de 10.000 usuaris simultanis VPN SSL, ja sigui amb agent o sense, però en qualsevol cas sense llicència addicional.

- FG-100F, ell dispositiu admet fins a un màxim de 500 usuaris simultanis VPN SSL, ja sigui amb agent o sense, però en qualsevol cas sense llicència addicional.

- FG-60F, ell dispositiu admet fins a un màxim de 200 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 IPsec 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.

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.

- FG-600E, la capacitat mínima de punts d'accés ha de ser de 1.024, i de switchs de 512.

- FG-100F, la capacitat mínima de punts d'accés ha de ser de 128, i de switchs de 24.

- FG-60F , la capacitat mínima de punts d'accés ha de ser de 64, i de switchs de 16.

- 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.

2.2. Subministrament de software

FortiClient avançat per 800 endpoints: és un antivirus que és gestionat per la pròpia consola de gestió central EMS (Endpoint Management Server) i que permet:

- Protecció automatitzada contra amenaces
- Visibilitat i control d'extrem a extrem
- Protecció automatitzada basada en el comportament contra amenaces desconegudes
- Protecció contra vulnerabilitats conegudes
- Gestió de pegats (parches) i protecció de vulnerabilitats
- Gestió simplificada i aplicació de polítiques amb EMS
- Accés remot segur VPN SSL e IPSec

2.3. Serveis professionals

2.3.1. Desplegament del maquinari

Les tasques que s'hauran de realitzar quan es subministri el material són les següents:

- Anàlisi i disseny (revisió regles, polítiques, etc.)
- Upgrade de la plataforma actual Fortigate de l'Agència (versió 6.0) i configuració de l'arquitectura "Security Fabric".
- Definició de la migració de les regles a nous appliances físics.
- Definició de la solució endpoint (maqueta). S'ha de desplegar l'agent per a 10 dispositius de diferents tipus, la resta dels 800 es realitzarà mitjançant GPO o eina de distribució de software (responsabilitat de l'Agència).
- Instal·lació i migració del clúster de firewalls.
- Configuració
- Proves i posada en producció d'ambdues solucions
- Documentació

2.3.2. Suport i manteniment correctiu i preventiu anual

L'empresa adjudicatària haurà d'oferir aquest suport en modalitat 8x5 i les funcions que han d'estar contemplades són:

- Únic punt de contacte per al suport per a les incidències
- Suport de primer i segon nivell
- Escalat al tercer nivell del fabricant
- Gestió de RMAs
- Resolució remota i in-situ (si fos necessari)
- Revisió física dels equips (semestral)
- Revisió de configuracions i anomalies (semestral)

2.3.3. Suport evolutiu

L'empresa adjudicatària haurà d'oferir una bossa anual de 40 hores per a la realització sota demanda d'activitats relacionades amb l'evolució de la plataforma Fortinet indicada, entre d'altres:

- Optimització de regles i polítiques
- Upgrade de noves releases de firmware
- Training personalitzat
- Assessorament sobre noves versions, pegats (parches), etc. Publicades pel fabricant

- Avaluació de l'impacte funcional i assistència a la planificació, configuració i parametrització dels sistemes davant canvis de l'estructura del client.
- Consulta de qüestions tècniques plantejades per al client en relació amb la plataforma.

L'empresa adjudicatària mensualment haurà d'informar de les hores realitzades i l'estat de la bossa (consums realitzats i hores pendents).

S'haurà de detallar com es computaran les hores depenen de si el servei és fora d'oficina, si la intervenció és in-situ o en remot.