Expedient número: IDES-2024-04

Plec de prescripcions tècniques que regulen la contractació de la renovació anual del manteniment de la infraestructura de seguretat de xarxa (tallafocs), accés a la xarxa sense fils (wifi) i manteniment dels equips d'electrònica de xarxa de l'Institut d'Estadística de Catalunya per a l'any 2024.

1. Objecte

Renovació del manteniment de la infraestructura de seguretat de xarxa (tallafocs), accés sense fils (Wifi) de la marca Fortinet i manteniment dels equips d'electrònica de xarxa (switch) de la marca Huawei de l'Institut d'Estadística de Catalunya (en endavant Idescat).

2. Seguretat de xarxa (tallafocs)

2.1 Situació actual dels equips tallafocs

Actualment els Access Points de l'Idescat son del fabricant Fortinet, concretament el model FAP221E que requereix un servei de seguretat gestionada amb tallafocs NGFW en HA.

Totes les funcionalitats requerides a continuació han de ser llicenciades per a tota la durada del contracte directament per l'adjudicatari, qui gestionarà absolutament qualsevol aspecte d'aquesta plataforma i/o solució. Aquest clúster serà a les dependències de l'Idescat. Els tallafocs proposats hauran de tenir les següents funcionalitats com a mínim:

a) A nivell de funcionalitats NGFW

- 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 proposta 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.

b) A nivell de 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 20/18/10 Gbps de rendiment de tallafocs per paquets de 1518, 512 i 64 bytes en IPv4 respectivament, i de 20/18/10 Gbps

de rendiment de tallafocs per paquets de 1518, 512 i 86 bytes en IPv6 respectivament.

- 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 inferior a 5 µs (per paquets 64 byte UDP) que caldrà acreditar amb el datasheet oficial del fabricant.
- Ha de tenir capacitat per com a mínim de 10.000 polítiques de tallafocs.
- 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: 1,6 Gbps per tràfic Enterprise MIX.
    - Rendiment amb Threat Protection: 1 Gbps per tràfic Enterprise MIX.
    - Rendiment Inspecció SSL amb IPS: 1 Gbps mesurat amb diferents Ciphers.
    - Rendiment per control d'aplicacions: 2,2 Gbps mesurat per http 64K.

c) A nivell de connectivitat

- 1 port de consola.
- 1 port USB 3.0 per a la connexió de mòdem 3G/4G i/o pendrive. El port USB ha de permetre la instal·lació desatesa del firmware i aplicació de configuració en el booting de l'equip per realitzar tasques automàtiques d'instal·lació i canvis d'equipament.
- 2 ports 10GE SFP+ Slots
- 4 ports 1GE SFP Slots
- 12 ports 1GE RJ45 i 2 ports 1GE RJ45 WAN Ports.
- Instal·lació en rack de 19'' i no més de 1 RU.
- Consum màxim inferior a 125 W.

d) A nivell de 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 del 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, es consideren incloses en l'oferta econòmica durant tota l'execució 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 Tràfic Shaping tant de trànsit sortint com a entrant sent capaç de reservar ample de banda i marcar el trànsit amb DSCP. Aquest tràfic shaping ha de basar-se en aplicacions i URLs a nivell global de perfil o per ip.

e) A nivell de HA:

- La funcionalitat d'alta disponibilitat ha d'estar disponible sense necessitat de cap llicència addicional.
- Suport HA tipus Actiu – Passiu, Actiu - Actiu i mode mixte. El mode mixte implica poder tenir tallafocs virtuals actius i passius de forma barrejada, es a dir, que el màster de certs Tallafocs virtuals sigui la primera unitat de tallafocs, mentre que la segona unitat de tallafocs ~~es~~ sigui màster de la resta de tallafocs 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.

f) A nivell de 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 d'un extrem a l'altre 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.

g) A nivell de seguretat

- Capacitat de definir polítiques de seguretat IPv4/v6 utilitzant els següents paràmetres de coincidència:
    - 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 característiques 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.
    - 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 Tallafocs, 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 que es pugui fer captura de paquets 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.

h) A nivell de Control d'aplicacions

- Capacitat per identificar un mínim de 2000 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 aquestes aplicacions customitzades, també siguin analitzades per motors de protecció (IPS i antimalware).

En quant a les funcionalitats requerides:

1. **Funcionalitats 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 llindar d'ús en un temps determinat.
   - Capacitat de creació de firmes d'IPS per a un reconeixement personalitzat.

2. **Funcionalitats Antimalware**
   - Capacitat de detecció de malware (virus, grayware, worms, 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 d'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. Capacitat de bloquejar mitjançant comparació amb malware de repositoris externs amb threat inteligence.

3. Funcionalitats 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.

4. Funcionalitats 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 actualitzada possible.
- Suport per a la creació de llistes blanques/negres externes sense necessitat de llicència.

5. Altres funcionalitats de nivell 7

- Altres funcionalitats de nivell 7 que la proposta ha d'incloure i han d'estar llicenciades son:
    a. DLP (Data Leak Prevention)
    b. Web Application Tallafocs
    c. ICAP (Internet Content Adaptation Protocol)

6. VPN

- El dispositiu ha d'admetre fins a un màxim de 500 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:
    a. 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.
    b. Mode túnel: per a equips remots que executen una varietat d'aplicacions de client i servidor.

*El sistemes operatius i navegadors compatibles en aquest mode hauran de ser com a mínim els que es descriuen a la següent taula:

Sistema Operatiu	**Navegadors**
Microsoft Windows 7 SP1 (32-bit & 64-bit)	Mozilla Firefox version 85 Google Chrome version 88
Microsoft Windows 10 (64-bit)	Microsoft Edge Mozilla Firefox version 85 Google Chrome version 88
macOS Big Sur 11.0	Apple Safari version 14 Mozilla Firefox version 85 Google Chrome version 88
iOS	Apple Safari Mozilla Firefox Google Chrome
Android	Mozilla Firefox Google Chrome

2.2 Servei de recol·lecció de logs dels tallafocs.

La eina proposada haurà de ser compatible amb els tallafocs proposats de manera nativa, sense integració mitjançant APIs i que sigui alhora compatible amb els tallafocs proposats, de manera que els tallafocs enviïn en temps real els logs generats, amb els següents objectius:

- Que sigui una eina de monitorització en temps real del trànsit filtrat pels diferents mòduls dels equips.
- Qui sigui una eina de monitorització històrica externa als dispositius, emmagatzematge de logs, reports, del tràfic analitzat pels equips amb capacitat de fer informes de fins a 12 mesos aproximadament (cal incloure llicenciament i suport necessari durant tota la durada del contracte).
- Poder crear reports i alarmes en funció d'adreces, ports, protocols.
- Poder crear reports i alarmes en funció d'usuaris i/o grups d'usuaris (AD/LDAP).
- Poder analitzar, correlacionar i fer informes de la informació de seguretat de manera centralitzada.
- Que tingui un panell de control amb vista general d'usuaris destacables, aplicacions, destinacions, llocs web, vulnerabilitats, etc.
- Poder crear models d'informes preconfigurats, editables, modificables i exportables.
- Que tingui una gestió de esdeveniments amb generació d'alertes automàtiques a administradors.
- Que tingui un visor de logs en temps real o històric, que permeti distingir-los entre trànsit, esdeveniments i seguretat.
- Que tingui una visió de logs per dispositiu, dominis d'administració o agregats.
- Que tingui capacitat de filtratge i granularitat d'anàlisi de logs.
- Que tingui un dissenyador d'alertes.
- Que tinguin la possibilitat de generació d'alertes per nivells de seguretat, esdeveniments específics, accions o destinacions i nombre d'esdeveniments en un determinat temps.
- Que tingui capacitat de cercar alertes històriques.
- Que tingui capacitat de notificació d'alertes per correu electrònic, SNMP o syslog.
- Que executi rotació de logs recopilats i pugui enviar reports resum d'històric.

- Que tingui una visibilitat dels logs en format TXT descarregables.
- Que tingui una vista comparada de patrons de trànsit i amenaces.
- Que realitzi un anàlisi exhaustiva de totes les activitats relacionades amb el trànsit i els dispositius.
- Que es pugui elaborar informes sobre totes les activitats de trànsit i de dispositius.

L'eina de reporting i logs haurà de tenir capacitat suficient per conservar fins a 5GB diaris de logs entre tots els tallafocs proposats. El llicenciament quant a capacitat de logging, haurà d'estar inclòs a l'oferta econòmica.

Aquesta eina si s'ofereix en format de virtual appliance, haura de ser des de un cloud privat del licitador. no es permetrà el hosting per part de l'idescat. El cost de hosting del licitador haurà d'estar inclòs a l'oferta econòmica.

3. Accés sense fils

Actualment la xarxa sense fils (wifi) de l'Idescat esta composta per 6 APs Fortinet FortiAP 221E del fabricat Fortinet integrat i gestionat des de l'estructura del tallafoc de l'Idescat.

Es requereix la renovació del suport de fabricant grau **FortiCare Premium Support** per a la durada del contracte això com la gestió i manteniment de les configuracions actuals.

4. Manteniment i suport dels equips d'electrònica de xarxa de l'Idescat

Actualment l'Idescat té el següent equipament d'infraestructura de Xarxa basada en el fabricant Huawei amb contractes de manteniment. Aquests contractes corresponen a un nivell de servei per part de Huawei anomenat **24x7 Premium Support & 8x5xNBD**, i corresponen als 14 switches que conformen la infraestructura de Xarxa de IDESCAT, els contractes tenen els números següents

- 0Y072422000032
- 0Y07242101490R

Equipament inclòs en el contractes actuals:

- 6 uds Huawei Cloud Engine S5720-52X, amb bels SN:
  - 21980106192SJ8601813
  - 21980106192SJ8601927
  - 21980106192SJ8601928
  - 21980106192SJ8601929
  - 21980106192SJB602912
  - 21980106192SJB602913
- 5 uds Huawei Cloud Engine S5720-28X, amb bels SN:
  - 21980105932SL7500197
  - 21980105932SL7500199
  - 21980105932SL7500210
  - 21980105932SJ7600246
  - 21980105932SJB600743
- 3 uds. Huawei CloudEngine S5732-H48UM2CC, amb bels SN:
  - 1021C5548368
  - 1021C5548370
  - 1021C5548376

Es requereix la renovació del suport del fabricant per a tota la durada de contracte amb el mateix nivell de suport actual.

5. Suport del adjudicatari als elements objecte del contracte

Es requereix per part del licitador un servei de suport en horari laboral (10x5) per a tota aquesta infraestructura de xarxa, i que inclogui les següents tasques:

- Tramitació de incidències de HW amb el fabricant
- Manteniment correctiu, preventiu y proactiu
- Administració de l'equipament
- Servei Hotline il·limitat.
- Còpia de seguretat de la configuració dels dispositius amb retenció de 30 dies
- Monitorització de l'equipament (disponibilitat, caiguda de línia, rendiment...).

En aquest suport, s'inclouen els següents actius:

- Els equips de seguretat de xarxa (tallafocs),la recol·lecció de logs (propietat i gestió per part de l'adjudicatari)
- Equipament sense fils (Wifi) APs Fortinet FortiAP 221E (propietat de l'Idescat)
- Equips de electrònica de xarxa (switches) (propietat de l'Idescat)

6. Obligacions de l'empresa adjudicatària

Resolució de qualsevol incidència de programari per restablir el funcionament correcte dels equips descrits en .

En el marc del manteniment de caràcter preventiu de l'equipament informàtic, es duran a terme les actuacions següents:

- Revisió periòdica dels equips, mitjançant eines de diagnosi del fabricant tant remota com in situ.
- Subministrament d'actualitzacions del maquinari realitzades pel fabricant dels equips.
- Suport tècnic per a la resolució de dubtes o consultes relacionats amb la seva instal·lació i ús.

  Aquest servei es podrà prestar, en primera instància, de manera remota, mitjançant un servei d'atenció telefònica o similar; quan no s'aconsegueixi resoldre el problema remotament, l'assistència tècnica es prestarà in situ a la seu de l'Idescat.

El subdirector general d'Informació i Comunicació