Consorci
Administració Oberta
de Catalunya

Plec de prescripcions tècniques per l'adquisició de tallafocs de capa 7

Expedient AOC-2024-23

Generalitat
de Catalunya

Consorci de governs locals
per a la societat de la informació

Contenido

1. Introducció

El Consorci AOC té diversos Centres de Processament de Dades des d'on dóna els serveis als seus clients.

Per poder donar els serveis amb unes condicions de seguretat adequades, cal que cada Centre de Processament de Dades disposi de dispositius tallafocs de capa 7, que tenen unes funcionalitats de seguretat avançades.

En un dels Centres de Processament de Dades del Consorci AOC, disposa d'uns tallafocs de capa 7 que properament entraran en fase *End Of Life*, per la qual cosa s'han de renovar.

En un altre dels Centres de Processament de Dades no es disposa de tallafocs de capa 7.

L'objecte del contracte es:

- Subministrament de 2 parelles de tallafocs de capa 7 amb les característiques indicades a continuació.
- Instal·lació dels tallafocs en 2 clusters, cada un en el Centre de Processament de Dades corresponent.

2. Requeriments generals.

Per donar compliment a la mesura de seguretat de l'Esquema Nacional de Seguridad "Componentes certificados [op.pl.5]", el dispositius subministrats hauran de ser un "**Producte qualificat de nivell Alt**".

Per acreditar la qualificació, el dispositiu haurà d'estar present al Catàleg de Productes i Serveis de Seguretat de les Tecnologies de la Informació i Comunicació (CPSTIC) del CCN, en com a mínim 1 de les següents categories::

- Tallafocs
- Dispositius de prevenció i detecció d'intrusions (IDS, IPS y AntiDDoS)
- Xarxes privades virtuals: IPSec

Enllaç al catàleg CPSTIC: CCN-STIC 105 Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación - Actualizado Mar 2023 (cni.es)

L'adjudicatari haurà de subministrar els següents components:

- 4 dispositius tallafocs de capa 7 i els components necessaris per crear 2 clústers, amb les característiques tècniques especificades al punt 4.
- Els components necessaris per poder ser enrackats en un armari rack estandard de 19".
- Les llicències necessàries per habilitar totes les funcionalitats requerides, amb una vigència de 3 anys.
- Un paquet de manteniment de maquinari contractat al fabricant, amb una vigència de 3 anys.
- El licitador haurà de ser partner del fabricant del dispositiu tallafocs que estigui oferint.

3. Instal·lació dels dispositius

L'adjudicatari haurà d'enrackar i instal·lar els 4 dispositius, creant 2 clusters de firewalls, cada un en un Centre de Processament de Dades ubicats a la província de Barcelona.

En el cas de que l'adjudicatari subcontracti el servei d'instal·lació dels dispositius, el subcontractiste haurà de ser partner del fabricant dels mateixos.

En el cas d'existir una "Guia de empleo seguro" del dispositiu ofert per l'adjudicatari, publicada pel CCN, aquest haurà de seguir les recomanacions de la guia. La relació de guies és la següent: 1000 Procedimientos de empleo seguro (cni.es)

L'adjudicatari haurà de fer proves de failover.

L'adjudicatari haurà d'entregar un document al final del projecte, amb la informació rellevant a nivell de configuració, mapa de xarxa i resultat de les proves de validació.

L'adjudicatari haurà de reservar 4h per fer traspàs d'informació al Consorci AOC. El contingut del traspàs haurà d'incloure una explicació general d'administració dels dispositius, incloent les possibilitats que poden donar de cara a futur i la configuració aplicada.

2.2 *Cluster 1.*

El clúster 1 substituirà un clúster de tallafocs del fabricant Palo Alto que actualment estan en producció.

L'adjudicatari haurà de transferir totes les regles existents als nous dispositius. Aproximadament, els tallafocs actuals tenen unes 30 regles de seguretat.

L'adjudicatari haurà d'afegir unes regles bàsiques de Control d'aplicacions, Webfilter, DNS Filter, protecció antiDoS i Web Application Firewall. L'objectiu d'aquestes regles és que quedin configurada la configuració inicial per a que el Consorci les completi.

2.3 *Cluster 2.*

El clúster 2 de tallafocs s'instal·larà en un Centre de Processament de dades on actualment no hi ha cap dispositiu equivalent.

L'adjudicatari haurà d'instal·lar els dispositius i crear unes regles bàsiques de Control d'aplicacions, Webfilter, DNS Filter, protecció antiDoS i Web Application Firewall. L'objectiu d'aquestes regles és que quedi la configuració inicial per a que el Consorci les completi.

4. Subministrament del manteniment de maquinari

L'adjudicatari haurà de subministrament un paquet de manteniment de maquinari amb una vigència de 3 anys.

El manteniment s'haurà de contractar al fabricant dels dispositius i estarà a nom del Consorci AOC.

El manteniment serà per resoldre incidències de maquinari en modalitat 24x7.

5. Especificacions tècniques dels dispositius

La proposta haurà d'incloure les llicències necessàries per tenir totes les funcionalitats requerides a continuació durant 3 anys de vigència.

L'adjudicatari haurà de subministrar uns dispositius tallafocs en format *appliance* d'un únic fabricant i model, quedant exclosos màquines virtuals i servidors de propòsit general. Han de poder ser instal·lats en un rack estàndard de 19".

Els quatre equips físics han de ser de idèntiques característiques, redundats i per crear 2 cluster 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.

Els dispositius han de tenir les següents funcionabilitats de seguretat: Control d'aplicacions, IPS, Antimalware amb Cloud Sandbox inclós, Webfilter, DNS Filter, Antispam, protecció antiDoS i Web Application Firewall.

Els dispositius hauran de disposar de fonts d'alimentació redundants per a cada un.

Els dispositius hauran 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

Els dispositius hauran d'incloure alguna funcionalitat d'auditoria de la configuració aplicada amb indicadors de risc.

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.

A nivell d'estructura hardware, els dispositius hauran tenir les següents especificacions::

- Processadors Hardware (SPU) 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.

Els dispositius hauran de tenir la capacitat de programar accions quan es produeixin events. Com a mínim haurà de poder enviar notificacions via mail.

Els dispositius hauran de tenir la capacitat de configuració de Proxy explícit per Interface, amb la funcionalitat de Proxy chaining en cas necessari, a més de capacitat de caching.

5.1. Requeriments de rendiment

Els dispositius tallafocs tindran hardware específic (de tipus ASIC) per tal d'assegurar el rendiment requerit. A més, hauran de tenir un hardware específic per analitzar el tràfic a nivell 4 i un altre totalment diferent, a nivell 7 i garantir baixa latència.

Els dispositius hauran de complir amb els següents requeriments mínims:

- Fins a 27 / 27 / 11 Gbps de rendiment de firewall per paquets de 1518, 512 i 64 bytes en IPv4.
- Hauran de ser capaços de gestionar fins 3 Milions sessions concurrents i com a mínim 280.000 noves sessions per segon.
- Hauran de tenir una latència inferior a 4.78 µs (per paquets 64 byte UDP) que caldrà acreditar amb el datasheet oficial del fabricant.
- Hauran de tenir capacitat per com a mínim de 10000 polítiques de firewall.
- Hauran de tenir un rendiment per tràfic SSL VPN ha de ser de com a mínim 2 Gbps i per tràfic IPSEC VPN (512 bytes) de 13 Gbps.

A nivell 7, els dispositius hauran de tenir com a mínim el següent rendiment:

- Rendiment IPS: 5 Gbps per tràfic Enterprise MIX.
- Rendiment NGFW (IPS i control d'aplicacions): 3.5 Gbps per tràfic Enterprise MIX.
- Rendiment amb Threat Protection (Firewall mes IPS, control d'aplicacions i motor antimalware actius): 3 Gbps per tràfic Enterprise MIX.

L'adjudicatari haurà d'acreditar que aquestes tres últimes dades siguin amb logging actiu.

- Rendiment Inspecció SSL amb IPS: 4 Gbps mesurat amb diferents Ciphers.
- Rendiment per control d'aplicacions: 13 Gbps mesurat per http 64K.

5.2. Conectivitat i caracteristiques fisiques

Els tallafocs han d'incloure en l'oferta presentada el següent número d'interfícies com a mínim (per equip):

- 1 port de consola.
- 1 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+
- 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 122 W.
- Ha de disposar de com a mínim 2 disc durs de 480 SSD cadascun.
- 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.
- En el cas que l'equip suporti ampliacions de memòria RAM i Disc Dur, caldrà que l'appliance estigui equipat amb el màxim de capacitats RAM i de Disc suportats pel fabricant.
- Fonts d'alimentació redundants i amb Hot Swap.

5.3. Requeriments de gestió

El dispositius hauran de complir amb els següents requeriments referits a la gestió dels mateixos:

- 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.

5.4. Requeriments de networking

El dispositius hauran de complir amb els següents requeriments referits al 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 com a mínim.
    - 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.

5.5. Requeriments per l'alta disponibilitat

El dispositius hauran de complir amb els següents requeriments referits a l'alta disponibilitat:

- 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.

5.6. Requeriments en quant a la visibilitat

El dispositius hauran de complir amb els següents requeriments referits a la 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.

5.7. Requeriments en quant a la seguretat

El dispositius hauran de complir amb els següents requeriments referits a la 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.

5.8. Requeriments pel control d'aplicacions

El dispositius hauran de complir amb els següents requeriments referits al 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. Es obligatori que en aquelles aplicacions customitzades, també siguin analitzades per motors de protecció (IPS i antimalware).

5.9. IPS

El dispositius hauran de complir amb els següents requeriments referits a la funcionalitat de Intrusion Prevention System:

- 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.

5.10. Antimalware

El dispositius hauran de complir amb els següents requeriments referits a la funcionalitat d'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.

5.11. Webfilter

El dispositius hauran de complir amb els següents requeriments referits a la funcionalitat de 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.

5.12. DNS Filter

El dispositius hauran de complir amb els següents requeriments referits al 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.

5.13. VPN

El dispositius hauran de complir amb els següents requeriments referits a la funcionalitat de VPN:

- 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.

5.14. 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 256 punts d'accés wifi gestionats del mateix fabricant, i de switchs de 64 gestionats i 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.

Barcelona,

Ivan Caballero Domínguez

Responsable de Sistemes de Seguretat del Consorci AOC.