PLEC DE PRESCRIPCIONS TÈCNIQUES (PPT) PER A L'ADJUDICACIÓ DEL SUBMINISTRAMENT DE PROGRAMARI I MAQUINARI I DELS SERVEIS DE SUBSTITUCIÓ I MILLORA DE LA XARXA TELEMÀTICA DE BARCELONA ACTIVA

1 INTRODUCCIÓ

L'objecte d'aquest plec de condicions tècniques és definir els criteris de contractació del programari, el maquinari i els serveis necessaris per a la substitució i millora de la xarxa telemàtica de Barcelona Activa.

La licitació inclou eines i serveis amb l'objectiu d'aconseguir una important millora en la capacitat, la fiabilitat, la seguretat i la gestió de les xarxes telemàtiques de Barcelona Activa.

Barcelona Activa vol contractar un projecte claus en mà el qual inclogui el maquinari, programari i serveis necessaris per disposar d'aquesta nova plataforma.

Els objectius a assolir són:
- Millorar la seguretat cibernètica
- Millorar els nivells de fiabilitat i qualitat
- Millorar les eines de gestió
- Obtenir els millors preus que pugui proporcionar el mercat

2 SITUACIÓ ACTUAL

El Centre de Processament de Dades (CPD) de Barcelona Activa disposa d'equips tallafocs per protegir els accessos a Internet i el tràfic entre equips del mateix CPD.

Barcelona Activa no disposa en l'actualitat de plataformes tallafocs que permetin la securització ni la microsegmentació de la xarxa telemàtica a les diferents seus. A més, força equips de commutació de la xarxa estan fora de suport o propers a la data de final de suport per part del fabricant, el que significa que aquest no oferirà actualitzacions de programari davant possibles problemes de seguretat.

Els armaris a on s'allotgen els equips de xarxa actual disposen de l'espai, les connexions amb altres racks, les línies d'alimentació elèctrica i els equips d'alimentació ininterrompuda necessaris per donar servei als equips a subministrar.

3 ABAST

L'objecte de la licitació és un projecte claus en ma que inclogui el subministrament dels equips així com els serveis necessaris per a disposar d'una nova xarxa telemàtica d'accés completament operativa.

La licitació es divideix en dos fases. La primera a realitzar durant l'any 2025 (previsiblement de setembre a desembre) i la segona a realitzar durant tot l'any 2026.

4 PERIODIFICACIÓ DELS SUBMINISTRAMENTS I ELS SERVEIS

El projecte es dividirà de dos fases atenent a l'any al qual correspondrà el subministrament o servei.

ANY 2025

Durant l'any 2025 s'haurà de lliurar i configurar:

- El maquinari, programari i serveis associats a la posada en producció, configuració de la plataforma Fortimanager (en alta disponibilitat) incloent-hi tots els serveis descrits.

- El programari, maquinari i servei associats per la renovació complerta de la xarxa de les dotze seus incloses com a seus petites;
  - Escola Bàrkeno
  - Espai Jove Boca Nord
  - Espai Jove La Fontana
  - Casal de Barri del Maresme
  - Associació de veïns de Roquetes
  - Centre Cívic Bon Pastor
  - Centre Cívic Trinitat Vella
  - D.S. Pers. i Territori S. Martí
  - Disseny Hub Barcelona
  - Oficina Pla de Barris Torre Baró
  - Serveis d'Ocupació i Promoció Econòmica Sants-Montjuïc
  - Subseu Districte - Ciutat Vella

- El detall d'equips a subministrar durant l'any 2025 serà:
  - 2 equips del model FMG-410G Centralized management appliance (FortiManager)
  - 1 equip del model FG-120G-BDL-950-36 Hardware plus FortiCare Premium and FortiGuard Unified Threat Protection (UTP) (Tallafocs seus mitjana)
  - 11 equips del model FG-80F-POE-BDL-950-36 Hardware plus FortiCare Premium and FortiGuard Unified Threat Protection (UTP) (Tallafoc seu petita)
  - 2 equips del model FS-424E-FPOE Layer 2/3 FortiGate switch controller compatible PoE+ switch with 24 x GE RJ45 ports, 4 x 10 GE (Commutador 234 ports PoE)
  - 2 equips del model FS-424E Layer 2/3 FortiGate switch controller compatible switch with 24 x GE RJ45 ports, 4 x 10 GE SFP+ (Commutador 24 Ports)

- Durant l'any 2025 no s'haurà de lliurar òptiques ni cablejat

- La documentació de la instal·lació i configuracions de la plataforma de gestió (FortiManager)

- La documentació de les instal·lacions i configuracions a les seus petites

ANY 2026

Durant l'any 2026 s'haurà de lliurar i configurar:

- Tot el programari, maquinari i serveis per la renovació completa de la xarxa de les cinc seus incloses com a mitjanes:
  - Convent de Sant Agustí
  - Innoba Ca n'Andalet
  - Nou Barris Activa
  - Sant Andreu Activa
  - Sants-Montjuïc Activa

- Tot el programari, maquinari i serveis per la renovació completa de la xarxa de les tres seus incloses com a grans:
  - Campus Central el qual inclou els equipaments de la Seu Central, Porta 22, Incubadora de Glòries i Centre per la Iniciativa Emprenedora de Glòries

- Edifici Mediatic el qual inclou els equipaments de Oficina d'Atenció a l'Empresa (planta baixa, altell i 3a planta), Cibernàrium 22@ i Lidera
- Parc Tecnològic Barcelona Nord el qual inclou el propi Parc Tecnològic i el Cibernàrium Nou Barris

- El detall d'equips a subministrar durant l'any 2026 serà:
  - 4 equips del model FG-200G-BDL-950-36 Hardware plus FortiCare Premium and FortiGuard Unified Threat Protection (UTP) (Tallafocs seus gran)
  - 10 equips del model FG-120G-BDL-950-36 Hardware plus FortiCare Premium and FortiGuard Unified Threat Protection (UTP) (Tallafocs seus mitjana)
  - 2 equip del model FS-2048F Layer 2/3 FortiGate switch controller compatible switch with 48x25G(SFP28) +8x100G (distribució Seu Central)
  - 78 equip del model FS-424E-FPOE Layer 2/3 FortiGate switch controller compatible PoE+ switch with 24 x GE RJ45 ports, 4 x 10 GE(Commutador 24 ports PoE)
  - 36 equips del model FS-424E Layer 2/3 FortiGate switch controller compatible switch with 24 x GE RJ45 ports, 4 x 10 GE SFP+ (Commutador 24 Ports)
  - 23 equips del model FS-108F-FPOE L2+ management switch with 8xGE + 2xSFP + 1xRJ45 console and automatic limited 130W POE (Commutador 8 ports PoE)

- El detall de les òptiques i cables a subministrar durant l'any 2026 serà:
  - 64 òptiques del model FN-TRAN-SFP+GC-T80 10 GE SFP+ transceiver module, range 80m, RJ45 connector, CAT6A, -5°C to 85°C
  - 32 òptiques del model FN-TRAN-SFP+SRI 10 GE SFP+ transceiver module, short range 400m, LC connector, MMF, 850nm, -40°C to 85°C
  - 4 òptiques del model N-TRAN-SX 1 GE SFP transceiver module, short range 500m, LC connector, MMF, 850nm, -20°C to 85°C
  - 8 òptiques del model FN-TRAN-SFP28-SR 25GE SFP28 transceiver module, short range
  - 108 cables del model FN-CABLE-SFP+3 10 GE SFP+ passive direct attach cable, 3m, 0°C to 70°
  - 4 cables del model N-CABLE-QSFP+3 40 GE QSFP+ passive direct attach cable, 3m, -40°C to 85°C,

- La documentació final del projecte.

5 REQUERIMENTS TÈCNICS SOLUCIÓ

Per tal de garantir una total integració i homogeneïtat amb la plataforma de seguretat actual de Barcelona Activa (gestionar i aplicar polítiques directament des d'aquesta), cal que els commutadors es gestionin i configurin des d'aquesta constituïda per dos equips FortiGate 1801F en alta disponibilitat. Quedaran excloses totes les solucions que no facin servir la pròpia gestió webGUI dels tallafocs FortiGate 1801F per configurar els commutadors, com integracions via API i similars.

Per facilitar la gestió d'aquests i assegurar les prestacions de latència i rendiment, tot el maquinari, connectors i adaptadors oferts han de ser del mateix fabricant.

Es distingeixen tres tipologies de seu que es detallen a continuació.

5.1 SEU GRAN

En aquestes seus i per la quantitat de dispositiu necessaris, a més de la plataforma tallafocs pròpia de la seu, s'hi hauran d'afegir commutadors en alta disponibilitat per connectar altres commutadors a la xarxa.

Els equipaments que entren en aquest categoria són:

- Campus Central el qual inclou els equipaments de la Seu Central, Porta 22, Incubadora de Glòries i Centre per la Iniciativa Emprenedora de Glòries
- Edifici Mediatic el qual inclou els equipaments de Oficina d'Atenció a l'Empresa (planta baixa, altell i 3a planta), Cibernàrium 22@ i Lidera
- Parc Tecnològic Barcelona Nord el qual inclou el propi Parc Tecnològic i el Cibernàrium Nou Barris

Es requerirà el nombre i tipologia següent de commutadors amb les característiques que es detallaran en els següents apartats i tots els elements necessaris per tal de realitzar la interconnexió (transceptors, fuetons de fibra o coure, etc.).

- Campus Central:
  - No caldrà afegir plataforma tallafocs. Utilitzarem la preexistent
  - 2 Fortiswicth-2048F com a equips de distribució a la Seu Central
  - 32 Fortiswitch-424F-FPOE
  - 14 Fortiswitch-424F (dos d'ells connectats en alta disponibilitat)
  - 12 Fortiswitch-108F- FPOE

- Mediatic:
  - 2xFortiGate 200G
  - 16 Fortiswitch-424F-FPOE
  - 12 Fortiswitch-424F (dos d'ells connectats en alta disponibilitat)
  - 1 Fortiswitch-108F- FPOE

- Parc Tecnològic:
  - 2xFortiGate 200G
  - 15 Fortiswitch-424F-FPOE
  - 4 Fortiswitch-424F (dos d'ells connectats en alta disponibilitat)
  - 7 Fortiswitch-108F- FPOE

5.2 SEU MITJANA

Es requerirà d'una plataforma tallafocs amb alta disponibilitat del model Fortigate 120G per a cada un dels equipaments inclosos en aquesta categoria.

Els equipaments que entren en aquesta categoria són:
- Convent de Sant Agustí
- Innoba Ca n'Andalet
- Nou Barris Activa
- Sant Andreu Activa
- Sants-Montjuïc Activa

Es requerirà el nombre i tipologia següent de commutadors amb les característiques que es detallaran en els següents apartats i tots els elements necessaris per tal de realitzar la interconnexió (transceptors, fuetons de fibra o coure, etc.)

El detall de commutadors necessaris en aquests equipaments són:

- Convent de Sant Agustí
  - 2 Fortigate 120G
  - 5 Fortiswitch-424F-FPOE
  - 2 Fortiswitch-424F

- Innoba Ca n'Andalet

- 2 Fortigate 120G
- 5 Fortiswitch-424F-FPOE
- 1 Fortiswitch-424F
- 1 Fortiswitch-108F-FPOE

- Nou Barris Activa
  - 2 Fortigate 120G
  - 2Fortiswitch-424F-FPOE
  - 1 Fortiswitch-424F

- Sant Andreu Activa
  - 2 Fortigate 120G
  - 1 Fortiswitch-424F-FPOE
  - 1 Fortiswitch-424F
  - 1 Fortiswitch-108F-FPOE

- Sants-Montjuïc Activa
  - 2 Fortigate 120G
  - 3 Fortiswitch-424F-FPOE
  - 1 Fortiswitch-424F

5.3 SEU PETITA

Es tots ells -excepte l'Escola Bàrkeno que requerirà un tallafocs del model FortiGate120G- s'instal·larà un tallafocs del model Fortigate 80G que, en molts casos, col·lapsarà les funcions de commutador de centre.

Els centres que entren en aquesta categoria són:
- Escola Bàrkeno (FortiGate 120G)
- Espai Jove Boca Nord
- Espai Jove La Fontana
- Casal de Barri del Maresme
- Associació de veïns de Roquetes
- Centre Cívic Bon Pastor
- Centre Cívic Trinitat Vella
- D.S. Pers. i Territori S. Martí
- Disseny Hub Barcelona
- Oficina Pla de Barris Torre Baró
- Serveis d'Ocupació i Promoció Econòmica Sants-Montjuïc
- Subseu Districte - Ciutat Vella

Es requerirà el nombre i tipologia següent de commutadors amb les característiques que es detallaran en els següents apartats i tots els elements necessaris per tal de realitzar la interconnexió (transceptors, fuetons de fibra o coure, etc.)

El detall d'aquests centres que necessitaran commutadors addicionals són:
- Escola Bàrkeno: 1 Fortiswitch-424F-FPOE i 1 Fortiswitch-424F
- Espai Jove Boca Nord: 1 Fortiswitch-424F-FPOE i 1 Fortiswitch-424F

5.4 TIPOLOGIA TALLAFOCS

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

- Els equips tallafocs han de ser en format appliance d'un únic fabricant, quedant exclosos màquines virtuals ni servidors de propòsit general. Han de poder ser instal·lats en un rack estàndard de 19 amb una safata o un adaptador.

- En les seus amb dos equips físics, els dos han de ser d'idèntiques característiques, redundats i en alta disponibilitat. 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.

- 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, per a tots els equips de seguretat 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 equips 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 personalitzats.

- 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 prohibir 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 incident 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, en entorns Actiu-Passiu, de connectar operadors diferents en els dos equips i poder utilitzar-los simultàniament.

- Els equips tallafocs tindran maquinari específic (de tipus ASIC) per tal d'assegurar el rendiment requerit; en detall, ha de tenir un maquinari específic per analitzar el tràfic a nivell 4 i un altre totalment diferent, a nivell 7 i garantir baixa latència.

- En el cas que l'equipament permeti ampliacions modulars d'interfícies, 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 aquest estigui equipat amb el màxim de capacitats RAM i de disc suportats pel fabricant.

- Respecte la 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.

- Pel logging i reporting caldrà que la solució s'integri amb la solució de la que es disposa actualment, FortiAnalyzer

- Suport de protocols RIP v1/v2, OSPF, ISIS, BGP, WCCP i Multicast per IPv4 i 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 com a mínim 256.
  - Verificació de la disponibilitat d'Internet per cadascuna de les línies, per protocols http, ping, dns, MOS 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.

- Respecte l'alta disponibilitat:
  - Suport HA tipus Actiu – Passiu, Actiu - Actiu i mode mixt. El mode mixt implica poder tenir tallafocs virtuals actius i passius de forma barrejada, es a dir, el màster de certs tallafocs virtuals sigui la primera unitat de tallafocs, mentre que la segona unitat de tallafocs es 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.

- 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 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 Interfície Gràfica dels tallafocs, en temps real i sense necessitat d'una consola central de gestió.

- 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 "qualsevol". 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 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 "qualsevol". 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 registre d'activitat, cal que la solució permeti activar el registre de només nivell 7, o tant de nivell 4 més nivell 7. Cal també fer captura de paquets en la pròpia política.
  - Capacitat de creació de regles de DoS a nivell 3 i 4, podent aplicar llindars 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'interfície 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'interfície.
  - 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.

- Capacitat de poder connectar un dispositiu del mateix fabricant del tallafoc que proporcioni connectivitat 5G/LTE i que pugui ser gestionat pel propi tallafoc. D'aquesta forma, aquest dispositiu ha d'aparèixer com una interfície de xarxa més i s'ha de permetre gestionar la connexió i implementar protecció avançada igual que qualsevol altra interfície del tallafoc.

- 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 les aplicacions personalitzades també siguin analitzades per motors de protecció (IPS i antimalware).

- 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 llindars d'ús, per tal de bloquejar intents d'atacs un cop superat un llindar d'ús en un temps determinat.
  - Capacitat de creació de firmes d'IPS per un reconeixement personalitzat.

- 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 una mida mínima de fitxer de 100 MB indistintament del tipus de fitxer.
  - Capacitat per l'eliminació del contingut dinàmic (macros, javascript, URL) explotable dintre de documents ofimàtics i PDF, que es distribueixen per protocols SMTP, IMAP i HTTP.
  - Capacitat de comprovació de si es tracta d'un fitxer bo o dolent, en funció del hashing i comparat amb la BBDD del fabricant. Així com bloquejant mitjançant malware de repositoris externs de threat inteligence.

- 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.

- 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 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 llicències addicionals.

- 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.
  - Suport d'agregació de túnels VPN i balanceig per paquet 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.

5.5 TALLAFOCS SEUS PETITES

A continuació s'indiquen les característiques que, a part de les anteriorment indicades a nivell general del tallafoc, caldrà que compleixin els tallafocs especificats per les catalogades com a Seu Petita:

5.5.1 Rendiment

- El tallafocs disposarà de fins 10/10/7 Gbps de rendiment de tallafocs per paquets de 1518, 512 i 64 bytes en IPv4.

- El tallafocs ha de ser capaç de gestionar fins 1.5 Milions de sessions concurrents. Així com a mínim 45.000 noves sessions per segon.

- El tallafocs ha de tenir una latència inferior a 3.24 µs (per paquets 64 byte UDP) que caldrà acreditar amb el datasheet oficial del fabricant.

- Ha de tenir capacitat per com a mínim de 5000 polítiques de tallafocs.

- El rendiment per tràfic SSL VPN ha de ser de com a mínim 950 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 (Firewall més IPS, control d'aplicacions i motor antimalware actius): 900 Mbps per tràfic Enterprise MIX.
    Caldrà acreditar que aquestes tres últimes dades siguin amb logging actiu.
  - Rendiment Inspecció SSL amb IPS: 715 Mbps mesurat amb diferents Ciphers.
  - Rendiment per control d'aplicacions: 1.8 Gbps mesurat per http 64K.

5.5.2 Connectivitat i característiques físiques

Els tallafocs han de disposar de Trusted Platform Module (TPM) i s'ha d'incloure en la oferta presentada el següent número de 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.

- 2 ports GE RJ45/SFP Shared Media Pairs

- 8 ports GE RJ45 PoE/+ Ports

- Consum màxim inferior a 118 W.

5.5.3 VPN

- El 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.

5.5.4 Controladora d'accés segur integrada

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

- Capacitat de gestionar fins a 96 punts d'accés wifi del mateix fabricant i de 24 switchos 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.

5.5.5 Connectivitat i característiques físiques

Els tallafocs han de disposar de Trusted Platform Module (TPM) i s'ha d'incloure en la oferta presentada el següent número de 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.

- 2 ports GE RJ45/SFP Shared Media Pairs

- 8 ports GE RJ45 Ports

- Wireless Interface:
  - Dual WiFi Radio (5 GHz, 2.4 GHz) 802.11a/b/g/n/ac/ax
  - 1 Scanning Radio

- 3 Antena Ports (SMA)

- Consum màxim inferior a 28 W

5.5.6 VPN

- El 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.

5.5.7 Controladora d'accés segur integrada

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

- Capacitat de gestionar fins a 96 punts d'accés wifi del mateix fabricant i de 24 switchos 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.

5.6 TALLAFOCS SEUS MITJANES

A continuació s'indiquen les característiques que, a part de les anteriorment indicades a nivell general del tallafoc, caldrà que compleixin els tallafocs especificats per les catalogades com a Seus Mitjanes:

5.6.1 Rendiment

- El tallafocs disposarà de fins 39/39/28 Gbps de rendiment de firewall per paquets de 1518, 512 i 64 bytes en IPv4.

- El tallafocs ha de ser capaç de gestionar fins 3 Milions de sessions concurrents. Així com a mínim 140.000 noves sessions per segon.

- El tallafocs ha de tenir una latència inferior a 3.18 µs (per paquets 64 byte UDP) que caldrà acreditar amb el datasheet oficial del fabricant.

- Ha de tenir capacitat per com a mínim de 10000 polítiques de firewall.

- El rendiment per tràfic SSL VPN ha de ser de com a mínim 1.5 Gbps i per tràfic IPSEC VPN (512 bytes) de 35 Gbps.

- Capacitat de configuració de Proxy explícit per Interface, amb la funcionalitat de Proxy chaining en cas necessari.

- A nivell 7, l'equip ha de disposar de com a mínim el següent rendiment:
  - Rendiment IPS: 5.3 Gbps per tràfic Enterprise MIX.
  - Rendiment NGFW (IPS i control d'aplicacions): 3.1 Gbps per tràfic Enterprise MIX.
  - Rendiment amb Threat Protection (Firewall més IPS, control d'aplicacions i motor antimalware actius): 2.8 Gbps per tràfic Enterprise MIX.
    Caldrà acreditar que aquestes tres últimes dades siguin amb logging actiu.
  - Rendiment Inspecció SSL amb IPS: 3 Gbps mesurat amb diferents Ciphers.
  - Rendiment per control d'aplicacions: 6.7 Gbps mesurat per http 64K.

5.6.2 Connectivitat i característiques físiques

Els tallafocs han de disposar de Trusted Platform Module (TPM) i s'ha d'incloure en la oferta presentada el següent número de 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.

- 16 ports GE RJ45 Ports

- 2 ports GE RJ45 HA

- 8 ports GE SFP Slots

- 4 ports 10 GE SFP+

- Consum màxim de 40 W

5.6.3 VPN

- El 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.

5.6.4 Controladora d'accés segur integrada

- El sistema ha de ser capaç d'actuar com controladora de punts d'accés wireless així com de switchos del mateix fabricant.
- Capacitat de gestionar fins a 128 punts d'accés wifi del mateix fabricant i de 32 switchos 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.

5.7 TALLAFOCS TIPUS SEU GRAN

A continuació s'indiquen les característiques que, a part de les anteriorment indicades a nivell general del tallafoc, caldrà que compleixin els tallafocs especificats com Seu Gran

5.7.1 Rendiment

- El tallafocs disposarà de fins 79.5/78.5/70 Gbps de rendiment de firewall per paquets de 1518, 512 i 64 bytes en IPv4.
- El tallafocs ha de ser capaç de gestionar fins 7.8 Milions de sessions concurrents. Així com a mínim 500.000 noves sessions per segon.
- El tallafocs ha de tenir una latència inferior a 4.2 µs (per paquets 64 byte UDP) que caldrà acreditar amb el datasheet oficial del fabricant.
- Ha de tenir capacitat per com a mínim de 10000 polítiques de firewall.
- El rendiment per tràfic SSL VPN ha de ser de com a mínim 3.6 Gbps i per tràfic IPSEC VPN (512 bytes) de 55 Gbps.
- Capacitat de configuració de Proxy explícit per Interface, amb la funcionalitat de Proxy chaining en cas necessari.
- A nivell 7, l'equip ha de disposar de com a mínim el següent rendiment:
  - Rendiment IPS: 12 Gbps per tràfic Enterprise MIX.
  - Rendiment NGFW (IPS i control d'aplicacions): 10 Gbps per tràfic Enterprise MIX.
  - Rendiment amb Threat Protection (Firewall més IPS, control d'aplicacions i motor antimalware actius): 9 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: 28 Gbps mesurat per http 64K.

5.7.2 Connectivitat i característiques físiques

Els tallafocs han de disposar de Trusted Platform Module (TPM) i s'ha d'incloure en la oferta presentada el següent número de 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.

- 16 ports GE RJ45 Ports
- 2 ports GE RJ45 de gestió
- 8 ports GE SFP Slots
- 4 ports 10 GE SFP+
- 4 ports 10 GE SFP+ d'ultra baixa latència amb valors de latència màxims de 2.5 µs (per paquets 64 byte UDP)
- Consum màxim inferiors a 190 W

5.7.3 VPN

- El dispositiu admet fins a un màxim de 5000 usuaris simultanis VPN SSL, ja sigui amb agent o sense, però en qualsevol cas sense llicència addicional.

5.7.4 Controladora d'accés segur integrada

- El sistema ha de ser capaç d'actuar com controladora de punts d'accés wireless així com de switchos del mateix fabricant.
- Capacitat de gestionar fins a 512 punts d'accés wifi del mateix fabricant i de 72 switchos 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.

5.8 TIPOLOGIA COMMUTADORS

A continuació es detallen els requeriments dels commutadors sol·licitats.
Tots ells, cal que disposin d'aquestes funcionalitats mínimes aplicables:

- IPv4 i IPv6
  - Unicast/Multicast
  - 802.1Q Vlan

  - LACP per la agregació de ports.
- Gestió i administració
  - Possibilitat de tornar a una configuració anterior (Rollback)
  - Suport de SNMP.
  - Exportació de *logs* mitjançant FTP, SCP i/o TFTP
- Log d'events
- 802.1Q Vlan
- LACP per la agregació de ports.
- DHCP Snooping
- IP Source Guard
- DAI Dynamic ARP Inspection
- Qualitat de Servei (QoS): Per Queue Traffic Shaping i Per Port Traffic Shaping
- Possibilitat de gestionar a través d'una consola centralitzada, amb accés mitjançant RADIUS
- Monitorització de tràfic via SPAN i RemoteSPAN (Nivell 2)
- Mínim de 1023 VLAN configurables
- Capacitat de detecció automàtica dels dispositius connectats en cada port. Cada switch alimentarà de forma automàtica la base de dades de dispositius dels tallafocs mitjançant integració nativa del propi fabricant.
- Automatismes per a que els tallafocs puguin posar en quarantena a dispositius infectats o maliciosos bloquejant de forma automàtica a nivell de port d'accés en el commutador.
- Cal que es pugui realitzar una assignació dinàmica de vlan del dispositiu que es connecti a un port en funció de l'adreça MAC, el fabricant del dispositiu, la família del dispositiu, tipus de dispositiu, sistema operatiu o usuari.
- Cal que la solució permeti realitzar una microsegmentació dins de la vlan per poder estar protegits contra el moviment lateral de programari maliciós i poder disposar de visibilitat de les comunicacions dins d'una vlan. Cal que es pugui aplicar una política de tallafoc com quan es realitza entre dues interfícies diferents, dins de la mateixa vlan i filtrant en el tallafocs el tràfic que es consideri.

5.9 GESTIÓ

Cal proporcionar a la solució una plataforma de gestió centralitzada que permeti gestionar tant els tallafocs com commutadors i APs mitjançant plantilles de configuració en una única eina.

La plataforma de gestió ha de proporcionar les següents funcionalitats:
- Configuració centralitzada i senzilla, orquestració basada en plantilles i monitorització dels tallafocs, commutadors i punts d'accés.
- Capacitat de gestió independent per grans entorns mitjançant dominis d'administració
- Capacitat de ZTP (zero touch provisioning), ha de permetre aprovisionar la configuració dels equips per aplicar-la un cop tinguin connectivitat a la plataforma de gestió.
- Capacitat de provisió ràpida de configuracions, seguiment detallat de revisions i capacitat d'auditoria.
- Permetre l'homogeneïtzació de configuracions i objectes per tot l'equipament administrat.
- Gestió de forma centralitzada les versions de firmware i programar l'actualització de dispositius gestionats.
- Funcionalitats de reversió de configuracions de forma automàtica en cas de pèrdua de connexió
- Ha de poder gestionar de forma nativa la plataforma de correlació de logs de que disposa BCNActiva, FortiAnalyzer.
- Ha de permetre configuració d'equipament en mode redundant mitjançant una còpia de seguretat dinàmica podent estar els dos equips en la mateixa xarxa o en xarxes separades geogràficament sempre que existeixi comunicació entre elles.

- La solució ha de disposar de la funcionalitat d'agrupació en una plantilla de diferents tipus de plantilla per a poder realitzar desplegaments massius amb equips diferents.
- Les plantilles han de poder ser creades mitjançant diferents menús contextuals per crear nous perfils de dispositiu. S'han de poder configurar les opcions mitjançant un widget o importar les característiques d'un dispositiu específic.
- Ha de permetre la creació de plantilles específiques per túnels IPSEC que pugui aplicar-se a diferents dispositius, poden reaprofitar-la utilitzant variables i poden fer un mapeig a interfícies normalitzades o utilitzades en polítiques de seguretat o en configuracions de SDWAN.
- Cal que es puguin realitzar plantilles SDWAN per configurar un o diversos equips SDWAN mitjançant una gestió centralitzada de la xarxa SDWAN. Això ha de permetre realitzar un desplegament uniforme a tota la xarxa SDWAN, sense configuració local en els dispositius i d'aquesta forma eliminar els errors de configuració.
- Ha de permetre monitoritzar el SLA de rendiment de la xarxa des de cada una de les seus, d'una forma centralitzada.
- Cal disposar de plantilles d'enrutament estàtic i BGP
- La solució ha de disposar de la possibilitat de definir aprovacions o notificacions de fluxos de treball quan es requereix crear i instal·lar polítiques o modificar objectes.
- Per tal de reduir latències de la xara i la utilització d'internet, s'han de poder proporcionar des de la plataforma de gestió les actualitzacions de les firmes d'antivirus, atacs, web filtering i email filtering.
- Ha de permetre disposar d'un magatzem de configuracions per gestionar les revisions de les configuracions dels equips. D'aquesta forma, després de modificar una configuració, es pot emmagatzemar i cal que es pugui fer ala plataforma una comparativa entre les diferents versions de les configuracions.

5.10 GESTIÓ DE PUNTS D'ACCÉS

Ha de permetre gestionar els punts d'accés que son gestionats pel tallafocs sense que sigui necessària cap llicència addicional per punt d'accés.

S'han de poder crear, editar i importar perfils WIFI que han de poder ser aplicats sobre qualsevol dispositiu, independentment del tallafoc que el gestioni.

5.11 GESTIÓ DE SWITCHING

Ha de permetre gestionar els switchos que son gestionats pel tallafocs sense que sigui necessària cap llicència addicional per switch.

S'han de poder configurar els ports de tots els switchos administrats.

A les plantilles cal que sigui possible mostrar, crear i editar tant VLANs, polítiques de NAC, polítiques de seguretat, perfils LLDP, polítiques de QoS i comandes personalitzades.

5.12 GESTIÓ D'EQUIPAMENT 5G

Ha de permetre gestionar l'equipament 5G que son gestionats pel tallafocs sense que sigui necessària cap llicència addicional per equipament 5G.

S'han de poder realitzar plantilles personalitzades on es configurin perfils SIM i plans de dades.

DESCRIPCIÓ DELS SERVEIS:

Les tasques descrites en aquests apartats s'hauran de fer coordinadament amb el personal tècnic de Barcelona Activa per a que aquest pugui obtenir els coneixements necessaris per la futura gestió de la plataforma

Instal·lació dels dos equips FortiManager seguint recomanacions del fabricant, incloent-hi:

- Configuració de paràmetres de xarxa per pas a producció (IP,DNS ,NTP ,encaminament, etc.)
- Configuració de paràmetres bàsics (còpia de seguretat de les configuracions, usuaris d'accés, clients confiables, certificats, etc.)
- Configuració de servidor de correu per a enviament d'alertes
- Configuració d'accés a Fortimanager autenticat via RADIUS o LDAP
- Si fos necessari, integració amb Fortiauthenticator (autenticació multi-factor)
- Activació de llicències
- Actualització de les firmes d'antivirus, atacs, filtrat de web, etc.
- Creació de fins a tres dominis administratius si fos necessari
- Afegir dispositius Fortinet de la xarxa actual a Fortimanager (és possible que calgui fer canvis de configuració en Fortigate i FortiAPs actuals):
    - Fortigate 1801 en HA + FortisAPs en producció (170 unitats aproximadament)
    - Confirmar correcte funcionament de l'entorno de seguretat Fortigate
    - Confirmar correcte funcionament de l'entorno wireless gestionat per Fortigate

- Afegir Fortianalyzer actualment en producció a Fortimanager
- Des de Fortimanager configurar Fortigate per enviar logs a Fortianalyzer
- Creació de connectors externs AWS, VMWare, Google Cloud, etc. (si fos necessari)
- Creació de fins a cinc plantilles (sistema , encaminament , IPSec, amenaces, firmware, etc.)
- Creació de plantilles SD-WAN per a posterior desplegament (maqueta i producció)
- Creació de fins a tres paquets de polítiques per a agrupació de polítiques posteriors
- Creació de fins a deu polítiques de seguretat per a dispositius Fortigate (comprovar la integració amb les polítiques actuals del FG1801)
- Creació de perfils de seguretat (filtrat web, IPS, contra programari maliciós, des-encriptació SSL, etc.) per aplicar a les polítiques de seguretat creades (si fos necessari)
- Visualització gràfica de l'entorn Fortinet creat

Serveis de seguretat a configurar per a tot el nou entorn de xarxa Fortinet. Tot ha de ser configurat des de Fortimanager amb l'excepció d'allò que per característiques del fabricant no sigui suportat

- Autenticació als ports de xarxa cablejada mitjançant Fortiautenticator (necessària la configuració de polítiques a Fortiautenticator)
    - 802.1x amb credencials d'usuari/màquina del domini AD i assignació d'una VLAN depenent del grup de AD al que pertany l'usuari
    - (Possibilitat) 802.1x amb certificat de client desplegat per Barcelona Activa i assignació d'una VLAN depenent del grup de AD al que pertany l'usuari
    - En cas d'autenticació errònia, assignació d'una VLAN de quarantena (definició dels permisos d'aquesta VLAN)
    - Proves d'autenticació/autorització i tràfic dels dispositius clients
- Detecció de dispositius
    - Identificació de dispositius en base a diferents paràmetres (detecció de dispositius de FortiOS)
        - Adreça MAC de fabricant de dispositiu
        - Sistema operatiu del dispositiu connectat
        - Família de dispositiu

        - Adreça IP (en el cas de dispositius amb IP estàtica)
    - Assignació d'una VLAN diferenciada depenent de la detecció de dispositiu realitzada
    - En caso de identificació errònia, assignació d'una VLAN de quarantena (definició dels permisos d'aquesta VLAN)
    - Proves de detecció i funcionament
- Microsegmentació per a segments de xarxa crítics
    - Configuració de bloqueig de tràfic en dispositius de la mateixa VLAN (a definir la quantitat de VLANs crítiques)
    - Configuració de polítiques de seguretat de Tallafocs per a permetre tràfic dels clients de VLANs crítiques (fins a cinc polítiques)
    - Proves de fluxos de tràfic i bloqueig/permís
- Creació d'entorn SD-WAN entre totes les seus(definit en Fortimanager)
    - Definició de la topologia SD-WAN, enllaços per seu i política de flux de tràfic/serveis a monitoritzar (SLAs/polítiques de recuperació en cas de fallada)
    - Configuració dels enllaços WAN
    - Creació de l'encaminament entre seus/central/Internet (possibilitat de encaminament dinàmic i diferents connexions WAN per cada seu)
    - Creació de túnels VPN IPSec
    - Creació de regles SD-WAN i monitors d'enllaç (SLAs, latència, jitter, aplicació, etc.)
    - Configuració de polítiques SD-WAN origen (usuari AD, Dir IP) destí (dir IP, aplicació…)
    - Proves de connectivitat i redundància
- Fortianalyzer
    - Des de Fortimanager configurar Tallafocs per enviar registres a Fortianalyzer
    - Comprovar que des de tots els dispositius Tallafocs es reben registres durant la seva instal·lació.
    - Crear connector amb FortiAutenticator
    - Activar els gestors d'esdeveniments predefinits necessaris per a l'entorn de xarxa
    - Revisió de possibles incidents i esdeveniments quant s'hi afegeixin nous equips a la xarxa
    - Crear perfils de notificació en cas de produir-se un esdeveniment definit (correu, SNMP, etc.)
    - (depenent de llicència Security Automation) Definició i configuració de playbooks (dos com a màxim) para desencadenar accions a la xarxa (Quarantine Endpoint, Compromised Host)
    - configuració d'informes (dos com a màxim)

Creació de maqueta de xarxa per assegurar configuracions i desplegaments posteriors

- Instal·lació i cablejat físic Tallafocs en alta disponibilitat
- Descobriment i autorització Tallafocs en Fortimanager
- Instal·lació i cablejat físic d'un parell de commutadors en MCLAG
- Afegir dispositius en Fortimanager i comprovació de les configuracions aplicades.
- Creació d'entorn SD-WAN entre seu Maqueta y seu Central (Fortigate 1800)
- Proves d'entorn (a consensuar amb Barcelona Activa)
    - Autenticació 802.1x d'un PC corporatiu (usuari, màquina o certificat) i assignació a una VLAN
    - Proves de connectivitat a la xarxa corporativa
    - Error d'autenticació 802.1x d'un PC corporatiu (usuari, màquina o certificat) i assignació a una VLAN de quarantena
    - Detecció d'un dispositiu no 802.1x (detecció per MAC, SO o IP) i assignació a una VLAN
    - Proves de connectivitat a la xarxa corporativa
    - Error de detecció d'un dispositiu no 802.1x (detecció por MAC, SO o IP) i assignació a VLAN de quarantena
    - Comprovar en Fortiautenticator/Fortimanager/Fortianalyzer els registres de accés exitós/error
- Proves de redundància (a consensuar amb BCN Activa)

  - Desconnexió de Tallafocs actiu / entrada en producció Tallafocs passiu
  - Proves de connectivitat a la xarxa corporativa
  - Recuperació Tallafocs i retorn a la normalitat
  - Comprovar a Fortimanager i Fortianalyzer els registres de caiguda/recuperació
  - Comprovar l'enviament d'alertes per correu (en cas d'haver estat configurades)
  - Desconnexió d'un enllaç de pujada d'un commutador connectat al Tallafocs
  - Proves de connectivitat a la xarxa corporativa
  - Recuperació enllaç de pujada i retorn a la normalitat
  - Comprovar a Fortimanager i Fortianalyzer els registres de caiguda/recuperació
  - Comprovar l'enviament d'alertes per correu (en cas d'haver estat configurades)
- Proves SD-WAN (a consensuar amb Barcelona Activa)
  - Canvi de les condicions de connexió en els enllaços WAN (modificació SLAs, modificació latència, modificació serveis monitoritzats, etc.) que provoquin la caiguda d'un enllaç (en cas de haver-hi dos)
  - Canvi de les condicions de connexió en els enllaços WAN (modificación SLAs, modificació latència, modificació serveis monitoritzats…) que provoquin pèrdua de servei
  - comprovar gràfiques d'estat
  - comprovar a Fortimanager i Fortianalyzer els registres de funcionament
- Preves de seguretat (a consensuar amb Barcelona Activa)
  - Intent d'accés des d'un usuari/dispositiu corporatiu a un recurs no autoritzat a les polítiques de seguretat
  - Intent d'accés des d'un dispositiu identificat a un recurs no autoritzat a les polítiques de seguretat
  - (En cas de llicència Web Filter) Intent d'accés des d'un usuari/dispositiu corporatiu a una URL prohibida
  - (En cas de llicència DNS Filter) Intent de resolució DNS des d'un usuari/dispositiu corporatiu a una URL prohibida
  - Bloqueig de descàrrega de programari maliciós(per exemple EICAR) i remediació mitjançant enviament a quarantena del dispositiu client. Implica registre en Fortianalyzer per a remediació.
  - comprovar en Fortimanager i Fortianalyzer els registres de seguretat
- Validació de l'entorn de maqueta per part de Barcelona Activa
- Documentació d'alt nivell per als desplegaments posteriors de xarxa

Substitució entorn de xarxa per a cada seu petita

Totes aquestes tasques es podran realitzar en horari laboral consensuat amb els responsables del projecte de Barcelona Activa a fi efecte d'afectar el mínim possible el servei

- Instal·lació i cablejat físic Firewall segons nova topologia de xarxa
- Descobriment i autorització Firewall en Fortimanager
- Instal·lació i cablejat físic commutadors
- Afegir commutadors a Fortimanager i comprovació de les configuracions aplicades
- Proves bàsiques de connectivitat consensuades amb BCN Activa

Substitució entorn de xarxa per a cada seu mitjana

Totes aquestes tasques es podran realitzar en horari laboral consensuat amb els responsables del projecte de Barcelona Activa a fi efecte d'afectar el mínim possible el servei

- Instal·lació i cablejat físic Tallafocs en alta disponibilitat segons nova topologia de xarxa
- Descobriment i autorització Firewall en Fortimanager
- Proves de comprovació alta disponibilitat dels Tallafocs
- Instal·lació i cablejat físic commutadors

- Afegir commutadors a Fortimanager i comprovació de les configuracions aplicades
- Proves bàsiques de connectivitat consensuades amb BCN Activa

Substitució entorn de xarxa per a cada seu gran

Una gran part d'aquestes tasques s'hauran de fer fora de l'horari laboral per no afectar els serveis de xarxa.

- Instal·lació i cablejat físic Tallafocs en alta disponibilitat segons nova topologia de xarxa
- Descobriment i autorització Firewall en Fortimanager
- Proves de comprovació alta disponibilitat dels Tallafocs
- Instal·lació i cablejat físic commutadors
- Afegir commutadors a Fortimanager i comprovació de les configuracions aplicades
- Proves bàsiques de connectivitat consensuades amb BCN Activa
- Migració progressiva de seu
    - Substitució controlada de commutadors per planta/armari de la xarxa a la nova topologia
    - Validació y proves de connectivitat en producció consensuades amb BCN Activa
    - Suport al següent dia laborable per possibles problemes post migració

VIDsigner code: 97517A3A27CB4F5A93...

- 27/03/2025 10:42:26

Marc Puente Vila-masana - DNI 43685322...

Marc Puente Vila-Masana
Director de Tecnologia