Universitat Autònoma de Barcelona

PLEC DE PRESCRIPCIONS TÈCNIQUES

PROCEDIMENT OBERT

Contracte núm. 13/2021

Subministrament d'equipament i llicències pel control d'accés a la xarxa i la gestió de l'adreçament IP de la Universitat Autònoma de Barcelona.

PLEC DE PRESCRIPCIONS TÈCNIQUES

PROCEDIMENT OBERT

Contracte núm. 13/2021

Subministrament d'equipament i llicències pel control d'accés a la xarxa i la gestió de l'adreçament IP de la Universitat Autònoma de Barcelona

Contingut

1. OBJECTE DE LA PROPOSTA

L'objectiu de la present licitació és la contractació del disseny, subministrament i posada en producció d'un nou sistema de gestió dels dispositius que es connecten a la xarxa.

El nou sistema ha de:

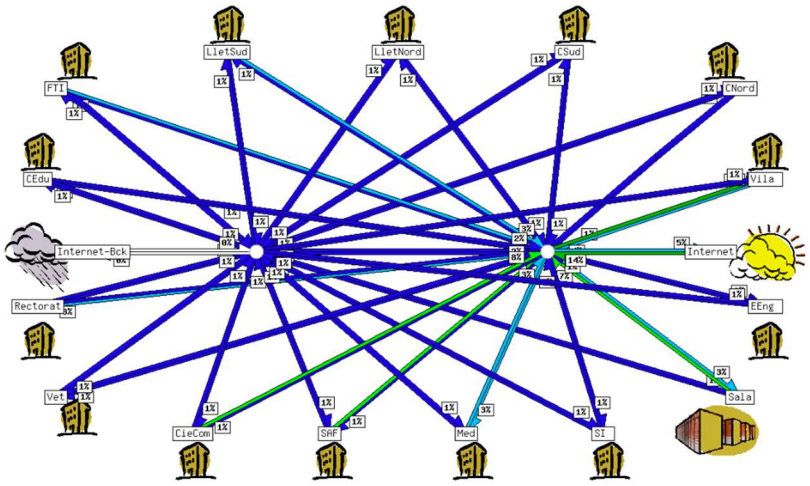
- Aportar informació detallada dels dispositius que es connecten a la xarxa
- Permetre l'aplicació de polítiques d'accés segons dispositiu i tipus d'usuari, avaluable dinàmicament
- Permetre l'aplicació de polítiques de seguretat al tràfic de l'usuari o entre xarxes (VLAN)
- Substituir íntegrament l'actual sistema de gestió de l'adreçament IP

El projecte de *subministrament de l'equipament i llicències pel control d'accés a la xarxa i la gestió de l'adreçament IP* haurà de tenir en consideració els següents punts:

- El licitador o licitadors hauran d'incorporar a la proposta tècnica la planificació detallada de la posada en funcionament del nou sistema de gestió d'accés a la xarxa (NAC) i el procediment de migració des de la configuració de xarxa de partida. La proposta haurà de detallar els perfils professionals que duran a terme les diferents tasques, la seva experiència i la seva implicació en el projecte.
- El licitador o licitadors hauran d'incorporar a la proposta tècnica la planificació detallada per a la migració de l'actual sistema de gestió d'adreçament a l'ofert al plec detallant al màxim les implicacions que suposa el canvi. La proposta haurà de detallar els perfils professionals que duran a terme les diferents tasques, la seva experiència i la seva implicació en el projecte.
- Caldrà detallar tots els elements – tan de maquinari com de programari – que en formaran part detallant tots els seus requeriments tècnics.
- Tots els elements necessaris s'hauran de proveir físicament o s'hauran de desplegar a l'entorn VMware de la Universitat (vSphere v7).
- La posada en producció del sistema o sistemes resultant/s d'aquesta licitació haurà de dur-se a terme de manera transparent a l'estructura actual. Per tant, el nou sistema objecte de la licitació haurà de conviure amb l'existent durant tot o part del cicle de vida del projecte d'implantació. Les interrupcions de serveis per necessitats de migració hauran de ser les mínimes possibles.
- L'equipament nou a instal·lar s'haurà d'integrar amb les eines de gestió del servei i, si cal, incorporarà eines pròpies de gestió en consonància a l'evolució tecnològica que es pretén assolir a través d'aquesta licitació.
- La proposta adjudicatària haurà de contemplar la posada en producció d'aquesta plataforma així com la documentació i la formació necessàries per a l'equip tècnic encarregat de dur a terme l'operació de la mateixa.
- La proposta adjudicatària haurà de contemplar el manteniment i suport de tot el sistema per un període de 5 anys a comptar des de la posada en marxa del servei en producció.
- La proposta econòmica haurà de contemplar tant el subministrament del maquinari (si s'escau) i complements com el cost associat de tot el programari i les llicències necessàries per donar cobertura a les especificacions tècniques que es detallen en aquest document. També haurà de contemplar els serveis professionals d'instal·lació, configuració, documentació, formació i posada en producció, així com el cost de manteniment per a tota la plataforma en els termes que s'indiquen en aquest document. La proposta econòmica haurà de contemplar totes les despeses derivades del projecte i per tant no s'acceptarà cap cost addicional associat a la posada en funcionament del maquinari (si s'escau) subministrat.

2. SITUACIÓ ACTUAL

La xarxa de campus és una doble estrella, cada nucli està en un centre de dades i té una sortida a Internet independent. Cada edifici principal està separat a nivell 3 de la resta. La gràfica següent mostra l'esquema amb els edificis principals:



Als equipaments centrals d'edifici els arriba una xarxa d'accés per usuaris, una d'administració de dispositius de xarxa i una de telefonia IP. Aquests equipaments també encaminen la xarxa de l'aula informàtica de la facultat.

En aquests moments s'està migrant l'estructura de doble nucli a un *fabric* de Pluribus al què es connectaran els diferents edificis possibilitant l'existència de xarxes transversals.

A cada edifici hi ha armaris de planta que donen connectivitat als punts d'accés WiFi i als dispositius dels usuaris. Una part important de l'equipament d'aquests armaris s'està actualitzant a commutadors Huawei model S5720 i la família Aruba 2530.

Hi ha edificis que estan fora del campus però connectats al nucli de xarxa de la mateixa manera que els edificis del campus. Els dispositius d'aquests edificis també han d'estar coberts pel sistema.

La xarxa WiFi l'ofereixen APs Aruba amb una controladora a cada nucli de l'estrella (actualment en la versió ArubaOS 8.5.0.11).

A la xarxa WiFi hi ha dos SSIDs corporatius, un que serveix l'accés a eduroam i un altre que ofereix un portal captiu en el què hi ha l'opció d'accés amb validació contra ldap i l'opció d'accés anònim. Les polítiques del portal validat són equivalents a les d'eduroam mentre que l'accés anònim és bàsicament per accés exclusivament cap a Internet.

L'accés a Internet i l'accés al Centre de Dades estan protegits per tallafocs Fortigate (actualment en versió FortiOS 6.2.7).

Existeixen diversos servidors de DNS (BIND 9.10 / 9.11) i de DHCP (ISC) redundants que donen servei a tota la xarxa. La informació dels dispositius, la seva IP, la seva MAC i el/s responsable/s del dispositiu està emmagatzemada en una base de dades. Hi ha una aplicació web per a la gestió d'aquests serveis que periòdicament regenera les zones de DNS i la informació de DHCP. L'assignació de l'adreçament dels dispositius dels usuaris és estàtica per DHCP. Cada dispositiu té una adreça IP assignada permanentment.

Hi ha un servei de DHCP paral·lel per l'assignació dels telèfons IP.

Per a l'assignació de les adreces IP als equips dels usuaris existeix una aplicació web en mode autoservei que els permet donar d'alta una MAC en una xarxa concreta, afegir-la a altres xarxes per temes de mobilitat, modificar-la si actualitzen l'equip o donar-la de baixa. A les MACs que es donen d'alta se'ls assigna una IP estàtica que mantindran fins que el seu responsable no doni de baixa la màquina o la canviï de xarxa o fins que els administradors de la xarxa comprovin que la màquina ja no es fa servir. Es poden definir fins a dues persones responsables per cada màquina,

aquestes persones poden accedir a l'aplicació d'autoservei i gestionar les seves màquines amb les opcions que hem comentat.

Per la gestió avançada hi ha una altra aplicació web que permet definir els rangs de xarxa, visualitzar la informació de la base de dades i fer modificacions a usuaris administradors.

Per a obtenir més informació del que hi ha connectat a la xarxa, hi ha una aplicació que periòdicament consulta tot l'equipament de xarxa obtenint les MACs de les màquines i la IP que estan utilitzant (recuperada de la taula ARP dels *routers*). També ens ofereix la informació de la utilització de cada port en el darrer any.

Els usuaris connecten tot tipus de dispositius a la xarxa (tant cablejada com WiFi).

Els ordinadors de la Universitat poden ser homologats (compra centralitzada), amb una imatge corporativa o poden ser específics per necessitats especials dels usuaris. A l'equipament específic s'inclouen els MAC, els Linux i els Windows amb característiques no cobertes pels equips homologats.

També es connecten dispositius BYOD, impressores, equipament de laboratori, IoT...

Els alumnes es connecten a la xarxa WiFi i a les xarxes de les aules informatitzades (tant amb els ordinadors de les aules com amb els seus propis dispositius).

A la xarxa WiFi també es connecten els dispositius mòbils (Android o iOS) tant del personal com dels alumnes o visitants.

3. REQUERIMENTS DE LA PROPOSTA

La solució haurà de proveir un sistema d'accés a la xarxa (NAC) i haurà de substituir íntegrament la gestió d'adreçament que s'ha explicat en el punt anterior podent mantenir-se únicament, si es considera convenient no substituir-los per sistemes nous, els servidors de DNS i DHCP.

3.1 Solució de control d'accés a la xarxa (NAC)

Es vol tenir un coneixement exhaustiu de tot el que es connecta a la xarxa per aplicar polítiques de seguretat diferents segons el perfil del dispositiu i/o usuari que es connecta i fins i tot poder canviar aquesta política si el dispositiu deixa de complir els requeriments que li han donat dret a la política aplicada en el moment d'accés (CoA).

El sistema a implantar recollirà la informació necessària per poder classificar un dispositiu com ordinador corporatiu, ordinador no corporatiu Windows, Linux o Mac, impressora, telèfon IP, mòbil Android o iOS, IoT (per fabricant o per tipus) i altres dispositius, deixant la possibilitat oberta de definir nous tipus de classificació.

Tota la solució haurà de ser compatible amb els sistemes operatius utilitzats a la Universitat (Windows 10 o 7, MacOS, Linux tipus Debian, RedHat o Ubuntu, Android des de la versió 7 o iOS) amb funcionalitats similars per aquests sistemes operatius. També haurà de poder gestionar la resta de dispositius que es connecten a la xarxa, tant cablejada com WiFi.

Tota la solució haurà de ser compatible amb la majoria de commutadors que hi ha a la Universitat (Huawei model S5720, la família Aruba 25309 i nucli Pluribus)

En un futur es vol autenticar els dispositius corporatius amb certificats (802.1x), per tant, la solució haurà de contemplar-ho.

Amb la informació proveïda per la solució, es podrà decidir quins dispositius admetre a la xarxa i quina política se'ls haurà d'assignar en funció tant del dispositiu com de l'usuari. La implementació inicial haurà d'incloure la possibilitat de classificar els dispositius amb perfils diferents per staff, per alumnes, per convidats i per altres dispositius i una xarxa de quarantena pels dispositius que no compleixin la política de seguretat establerta.

Els dispositius en quarantena tindran un accés limitat a les eines que els permetin corregir el problema que els ha portat a ser classificats d'aquesta manera.

Apart de la informació disponible sobre els dispositius i usuaris connectats, es voldrà poder autenticar l'accés a la xarxa en els dispositius que es decideixi tant amb protocol 802.1x com amb portal captiu o adreça MAC.

La solució haurà de proveir un sistema que permeti la **gestió de convidats** permetent la identificació del convidat via correu electrònic (autenticant que sigui vàlid), xarxes socials, sponsor o qualsevol altre mètode que permeti lligar una sessió a la identitat de la persona. Qualsevol dels mètodes ha de ser en modalitat d'autoservei, sense necessitat de gestió centralitzada. Caldrà poder establir un temps màxim de validesa del servei per convidat.

Les polítiques de control de tràfic es podran aplicar a nivell d'equipament d'accés. Es valorarà també la integració amb el nou nucli Pluribus.

La solució ha de ser redundada i el node o nodes redundants s'instal·laran tenint en compte l'estructura de doble nucli i doble CPD de la xarxa.. Ha de ser possible la configuració en mode actiu/passiu i es valorarà suport per alta disponibilitat actiu/actiu La solució no ha d'implicar posar un dispositiu a cada xarxa gestionada o a cada edifici.

Tot i els mecanismes redundants, el sistema ha de permetre que, en cas de no disponibilitat del servei de NAC, els dispositius connectats a la xarxa segueixin funcionant amb les polítiques que tenien assignades.

Requeriments de la solució

- La solució ha d'estar configurada en mode d'alta disponibilitat, sense punts únics de fallada.
- La solució implementada estarà basada en appliances físiques o bé en appliances virtuals sobre la plataforma VMware de la UAB.

- La solució permetrà també la seva implementació sobre plataformes de virtualització Hyper-V i KVM, així com el desplegament sobre núvols públiques AWS i Azure. Caldrà també poder fer desplegaments híbrids amb alguns components al CPD de la UAB i altres a diferents núvols públics. Totes les funcionalitats hauran d'estar suportades en totes les plataformes. La solució permetrà generar clústers que combinin diferents formats de desplegament (per exemple, appliance físiques, virtuals i al núvol).
- S'ha de tractar d'una solució fora de banda, sense requerir la replicació de tràfic.
- La solució ha d'integrar-se amb dispositius multi-fabricant. El desplegament inicial haurà d'integrar-se amb els switchos existents (predominantment Huasei S5720 i Aruba 2530), la xarxa WiFi (Aruba), la xarxa core (Pluribus) i els tallafocs i VPN (Fortinet), però ha de ser compatible amb dispositius d'altres fabricants, sense que això impliqui cap cost addicional.
- La solució haurà d'utilitzar protocols Standard que garanteixin la seva compatibilitat amb equipaments d'accés (switchos, routers, tallafocs, controladores WiFi, terminadors VPN...) de diferents fabricants.
- La solució ha d'incloure mecanismes de descobriment automàtic de nous equips de xarxa i detectar de manera ràpida dispositius no autoritzats com switchos, punts d'accés WiFi no gestionats, etc.
- La solució ha de ser capaç de detectar i gestionar múltiples VLANs i dispositius connectats al mateix port. En el cas de múltiples dispositius connectats a un únic port (per exemple, un ordinador i un telèfon IP), ha de poder gestionar-los de manera independent.
- La solució ha de ser capaç de detectar l'ús de NAT en ports d'accés i gestionar-los adequadament.
- La classificació i control dels dispositius ha de ser possible tant si aquests tenen instal·lat un agent com si no el tenen.
- La solució inclourà la possibilitat d'instal·lar agents, bé siguin de manera permanent o temporal (agents "solubles" o "volàtils") per analitzar aplicacions instal·lades i possibles vulnerabilitats. Els agents estaran disponibles per les plataformes Windows, Mac i Linux. Els agents hauran de comunicar-se amb els dispositius de control d'accés mitjançant protocols xifrats i segurs.
- Els agents "solubles" o "volàtils" no han de requerir drets d'administrador per part de l'usuari per al seu funcionament.
- La solució ha de tenir capacitat per perfilar i inventariar tots els dispositius connectats a la xarxa, detectant automàticament dispositius com impressores, smartphones, telèfons IP, càmeres i tota mena de dispositius IoT. Per tal d'aconseguir-ho farà servir un ampli ventall de metodologies com DHCP fingerprinting, nmap, MAC OUI, ports oberts, interaccions via http/https, ssh/Telnet o WMI/WINRM, scripts a mida, etc. Els resultats de tots els mètodes de perfilat disponibles s'hauran de poder combinat per crear regles de perfilat a mida.
- La solució ha de permetre actuar en cas de detectar una activitat sospitosa aïllant el dispositiu (xarxa de quarantena), restringint el tràfic afectat o fins i tot, depenent de l'activitat, posant el remei automàticament. El mateix s'hauria d'aplicar en cas de detectar un equip que no compleixi els requeriments de seguretat definits.
- La solució ha d'oferir la possibilitat d'avisar a l'usuari en cas d'incompliment de les polítiques definides.
- La solució ha de permetre comprovar periòdicament si els resultats del perfilat han canviat i generar accions en cas de que així sigui.
- La solució ha de permetre controlar els dispositius connectats a la xarxa cablejada, a la xarxa WiFi i a través de VPN, fent servir un ampli ventall de mètodes (SNMP, CLI, RADIUS...) per garantir-ne l'efectivitat.
- La solució s'haurà d'integrar amb els sistemes d'identitat basats en Microsoft Active Directory, RADIUS, LDAP, bases de dades, Kerberos i Microsoft Azure Active Directory, i suportar també identitats locals.

- La solució s'integrarà amb el sistema d'identitats corporatiu per identificar l'usuari actiu en el dispositiu i poder així aplicar polítiques específiques per diferents tipus d'usuaris (per exemple, PAS, PDI, alumnes o personal extern).
- La solució no ha de requerir desplegar 802.1x o RADIUS, tot i que ha de ser-ne compatible.
- La solució permetrà l'autenticació de dispositius per IP o MAC, però inclourà la possibilitat d'incloure paràmetres addicionals de validació per tal d'evitar la clonació d'IPs o MACs.
- La solució inclourà un sistema de registre de dispositius en el moment en què es connecten a la xarxa. El sistema de registre inclourà diferents mètodes: registre automàtic per perfilat, registre assistit per perfilat, auto-registre amb portal, API o 802.1x, o amb importació de dades des d'un fitxer.
- La solució ha de ser escalable, permetent ampliacions posteriors de la capacitat afegint-hi més llicències i/o dispositius (físics o virtuals), però sense haver de canviar l'arquitectura del sistema.
- El sistema ha de tenir la capacitat per gestionar d'un mínim de 30.000 dispositius simultanis.
- El sistema ha d'estar llicenciat per gestionar un mínim de 10.000 dispositius simultanis.
- La gestió de la solució es farà des d'una consola única i fàcil d'utilitzar. La consola de gestió ha de permetre crear diferents usuaris d'administració amb rols i privilegis diferenciats. Aquests usuaris podran ser locals o d'un sistema centralitzat com Active Directory o LDAP.
- La traça de les operacions haurà de ser exportable a un sistema SIEM basat en Elasticsearch.
- La solució haurà de ser compatible amb IPv6.
- Totes les comunicacions han de ser xifrades i segures.

Millores valorables amb criteris objectius

- Llicenciament per gestionar entre 10.000 i 30.000 dispositius simultanis.
- Llicenciament perpetu del nombre de dispositius gestionats.
- Consum d'una llicència per dispositiu, independentment del nombre d'interfícies de xarxa que tingui o del nombre d'usuaris que hi tinguin accés.
- Consum de llicència per dispositius connectats concurrentment *en temps real*.
- Possibilitat d'instal·lar agents persistents o solubles en tots els dispositius llicenciats sense cost addicional.
- Integració bidireccional i aplicació de polítiques dinàmiques de tallafoc amb els sistemes de tallafocs existents (Fortinet).
- Integració nativa amb VMware (Vsphere i ESXi) i VMware NSX per la classificació automàtica i creació de perfils de màquines virtuals.
- Disponibilitat d'un servei dinàmic de perfilat de dispositius actualitzat regularment (com a mínim amb periodicitat diària) al núvol que ajudi a la identificació dels dispositius connectats, i sense cost addicional.
- Control de canvis que permeti comprovar els canvis realitzats i retrocedir els últims canvis en cas necessari.

Millores valorables amb criteris subjectius

- Capacitat d'orquestració amb els sistemes existents a la Universitat: WiFi Aruba, tallafocs i VPN Fortigate i xarxa core Pluribus.
- Capacitat d'integració i orquestració amb els sistemes de seguretat d'endpoint existents a la Universitat: tallafocs i antimalware de TrendMicro i els serveis de seguretat de Microsoft (Defender for Endpoint, SCCM i InTune).

3.2 Solució de gestió d'assignació d'adreces (IPAM)

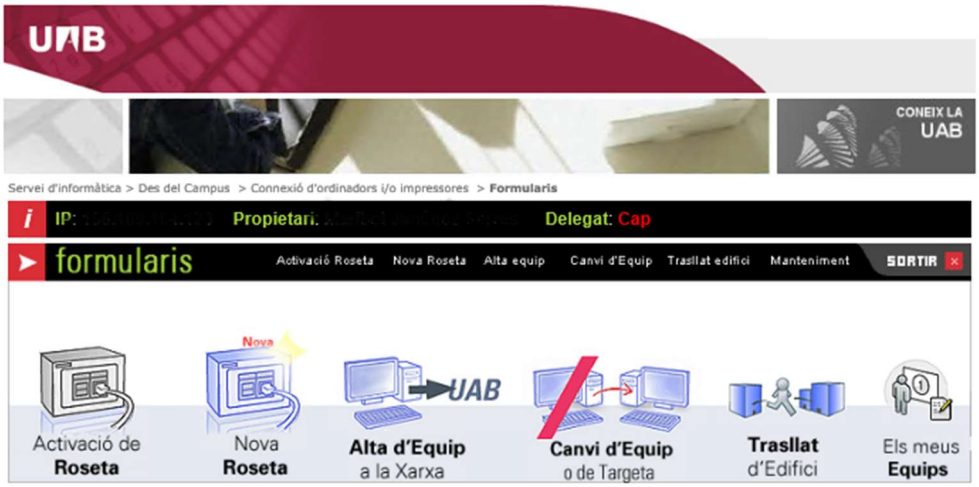
La solució proposada en aquest contracte ha de substituir íntegrament la gestió de l'adreçament IP de la xarxa cablejada, amb l'opció de mantenir únicament els serveis de DNS (*bind*) i DHCP (*ISC*). No caldrà fer modificacions a la gestió de la xarxa WiFi, que treballa amb adreçament dinàmic i privat.

Es proposa que les noves xarxes que s'hagin de crear per necessitats del NAC tinguin, fins a on sigui possible, assignacions DHCP dinàmiques amb adreçament privat.

El servei actual de DNS gestiona diverses zones, algunes primàries i altres secundàries. La Universitat té tots els dispositius donats d'alta tant en el domini uab.cat com en el domini uab.es. L'autoservei gestiona l'adreçament de la zona uab.es i el sistema replica aquesta informació a la zona uab.cat. La solució haurà de permetre la gestió automatitzada de la dualitat de noms del dispositius.

El sistema actual consta de:

- Un gestor web de DNS/DHCP que replica la informació de la base de dades al servidors DNS/DHCP
- 7 servidors de DNS i 4 servidors de DHCP redundants en diferents ubicacions.
- Una aplicació d'autoservei que permet que els propis usuaris donin d'alta els seus dispositius. L'aplicació assigna una IP fixa a cada màquina. La gestió permet
    - Alta de màquina (amb la MAC i ubicació per determinar la xarxa)
    - Canvi d'ubicació de la màquina (se li canvia la IP per una del rang desitjat)
    - Afegir ubicació (en cas que calgui que la màquina funcioni a més d'una ubicació)
    - Canvi de MAC de la màquina per renovació de l'equip. Es manté la IP en el nou equip i per tant es mantenen els permisos que s'han assignat a aquesta
    - Baixa d'equip
    - Consulta i gestió dels dispositius de l'usuari
- Una aplicació de gestió de l'aplicació d'autoservei amb funcionalitats avançades



Requeriments del nou servei de gestió d'adreçament:

- Gestionar l'assignació de totes les adreces IP/MAC des d'un entorn web (IPAM)
- Sincronitzat amb els servidors de DNS/DHCP

- Poder definir rangs dinàmics en el servidor DHCP i consultar la informació de les adreces assignades
- Compatible con la solució NAC del licitador o licitadors
- Poder definir adreces IP estàtiques, siguin públiques o privades, en el servidor DHCP per equips que requereixen mantenir sempre la mateixa IP. Usualment perquè son servidors d'algun tipus o perquè tenen accés a serveis específics per la IP que tenen assignada.
- Accés per rols que permeti tenir usuaris amb perfil de consulta, operació bàsica o administrador total.
- L'accés web ha de permetre delegar la gestió de grups d'IPs a diferents usuaris per fer tasques concretes com canviar el nom o la MAC de l'equip
- Es valorà que el sistema permeti definir patrons per l'assignació automàtica de dispositius a grups, segons el seu nom
- Si la solució no s'integra a l'entorn VMWare de la Universitat, haurà de proveir l'equipament necessari per dotar-la de mecanismes de redundància.
- Suport total IPv6
- Suport DNSSec
- Suport per mecanismes de *Response Policy Zone*
- Suport per autenticació contra l'AD i LDAP i es valorarà si també suporta CAS
- Cal que informi de l'ocupació de les diferents subxarxes

4. DISSENY DE LA PROPOSTA I POSADA EN PRODUCCIÓ

4.1 Solució de control d'accés a la xarxa (NAC)

El licitador haurà de proveir el material i llicències necessaris per la implantació de la solució en el total de dispositius d'usuari connectats a la xarxa cablejada. Resta fora de la solució els dispositius del centre de processament de dades.

La solució implementada gestionarà un mínim de 10.000 dispositius simultanis tot i que caldrà que la solució pugui ampliar-se per arribar a gestionar fins a 30.000 dispositius o més. Els controladors s'hauran d'instal·lar en mode redundant a ubicacions diferents (un a cada centre de procés de dades) amb interfícies redundants. La gestió del sistema s'ha de poder fer des d'una consola d'accés web amb alta disponibilitat.

Amb la instal·lació feta, es configuraran les fonts de dades que calgui (logs de DHCP, AD...) per tal de poder començar a recollir el màxim d'informació dels dispositius connectats per tal d'avaluar, juntament amb el licitador, quins són els paràmetres o propietats en que s'han de basar les polítiques NAC. Aquest descobriment s'haurà de fer amb la informació obtinguda pel descobriment de dispositius, sense la inclusió d'agents.

S'obtindrà informació dels tipus de dispositiu que hi ha a la xarxa, sistema operatiu, usuari... Caldrà detectar automàticament les impressores, telèfons IP i altres dispositius IoT

Amb el coneixement del nivell d'informació que puguem obtenir es decidirà el nivell d'accés que podem aplicar i s'implementarà en, al menys, dos edificis.

S'implementaran polítiques d'accés per perfil d'usuaris i tipus de màquines així com polítiques de tallafoc a nivell de Pluribus i, si és possible, de firewall local de les màquines (TrendMicro o tallafocs de Windows), o d'electrònica d'accés.

Es generaran els informes necessaris per conèixer ràpidament l'estat de tot el sistema gestionat (usuaris i màquines registrades, equips que no compleixen els requeriments de seguretat, errors

4.2 Solució de gestió d'assignació d'adreces (IPAM)

El licitador haurà de proveir el material i llicències necessaris per la implantació de la solució en el centre de procés de dades principal. Si la solució inclou els servidor de DNS i DHCP, aquests s'hauran d'instal·lar a les ubicacions a on estan els servidors actuals alguns dels quals estan fora del campus.

El sistema de virtualització de la Universitat està basat en VMware 7.0.

Els servidors de DNS/DHCP estan virtualitzats. Si cal substituir-los, es pot comptar amb el hardware que s'està fent servir actualment.

Caldrà configurar la nova solució amb els permisos adequats per permetre una gestió distribuïda. L'usuari administrador haurà de ser local a la màquina però la resta d'usuaris s'hauran d'autenticar a AD/LDAP o CAS.

Caldrà configurar la solució per mantenir les funcionalitats actuals

S'haurà de migrar el sistema actual al nou minimitzant el temps de desconnexió

5. OFERTA TÈCNICA

L'oferta del licitador haurà d'incloure un document amb, com a mínim les següents parts:

- Resum executiu
- Disseny general on es presentarà el disseny de la proposta tècnica. Ha d'incloure amb el màxim de detall el conjunt de materials objecte de la licitació – maquinari, programari, llicències, requeriments d'energia i de connectivitat, etc. així com la descripció de la solució proposada: arquitectura de connexió spine-leaf, detalls tècnics de funcionament com el temps de convergència en la fallida dels components significatius, esquema de la disposició de tots els elements amb el màxim de detall, etc.
- Proposta d'implantació on es definirà el procés de migració des del model actual al proposat i la forma en què es produirà la substitució de l'equipament de xarxa actual pel del nou escenari de funcionament.
- Perfils professionals de les persones dedicades al projecte per part del licitador, indicant, si s'escau, si inclou serveis professionals del fabricant de la solució (amb declaració responsable que ho certifiqui).

Aquest document inclourà també una proposta inicial de planificació que inclourà el desglossat del projecte en termes de tasques, fites i terminis, i presentarà l'equip de projecte proposat. La proposta tindrà especialment en compte que la migració no ha de comportar canvis disruptius que requereixin de talls de servei de llarga durada. Aquesta proposta haurà de servir de base a la que es definirà dins del projecte d'implantació.

Tota la documentació s'haurà d'entregar en format electrònic no escanejat (ha de permetre cerques de text). Es podran entregar tants documents annexes com es consideri convenient.

6. GESTIÓ DEL PROJECTE D'IMPLANTACIÓ

El projecte d'implantació estarà liderat per el Servei d'Informàtica de la UAB, que definirà el calendari i les fites. Durant la fase d'anàlisi es definirà el comitè de seguiment de projecte en què s'avaluarà el projecte i es detectaran les mancances.

En el comitè de seguiment hi participaran tant els responsables de servei que la UAB designi com la direcció de projecte de l'adjudicatari, així com aquelles persones, tant de la UAB com del licitador rellevants per les reunions específiques. El comitè serà l'òrgan màxim de direcció del projecte i s'hauran de complir les seves directrius.

L'adjudicatari s'haurà d'adaptar al calendari de projectes i disponibilitat de recursos interns de la UAB, pel que el calendari final reflectirà, no només la disponibilitat de recursos del licitador, sinó també de la UAB i les dependències amb altres projectes en curs.

El projecte d'implantació haurà de tenir en compte que el procés de migració ha de ser obligatòriament transparent i sense interrupcions, o, en el seu defecte, amb interrupcions parcials i acotades. Si es veiés la necessitat de realitzar actuacions amb impacte significatiu en els serveis, aquestes s'haurien de programar fora dels dies i/o els horaris de treball oficials. Tant l'esquema de funcionament actual, com el nou, hauran de poder conviure durant tota la migració.

Durant el projecte, la UAB podrà re-planificar les tasques i el calendari en funció de les necessitats de negoci. Aquesta re-planificació es presentaria en el següent comitè de projecte o en un comitè de projecte d'urgència. L'adjudicatari podrà ajustar la planificació en base als seus propis recursos per tal de tancar una nova planificació que s'ajusti tant als nous requisits de calendari com a la disponibilitat de recursos del licitador.

El licitador es compromet a proveir els recursos humans i tècnics adients a la seva proposta. En cas que el licitador hagi de reemplaçar un dels recursos, haurà d'informar a la UAB amb una setmana d'antelació d'aquest fet. La UAB es reserva el dret de demanar un canvi de recurs si aquest no compleix amb els requisits de qualitat, coneixements tècnics o de lliurament de tasques que s'hagin acordat.

7. FORMACIÓ I DOCUMENTACIÓ

L'oferta ha d'incloure les jornades de formació que es considerin necessàries per a l'administració correcta de la instal·lació.

Aquesta formació serà per 7 o 8 persones i es durà a terme quan ho determini el comitè de seguiment del projecte.

El projecte inclourà la redacció del document de descripció de la instal·lació lliurada en el format establert per la UAB.

8. CONDICIONS DEL SERVEI DE MANTENIMENT

Tot l'equipament subministrat haurà de tenir manteniment i suport tant del licitador com del fabricant (tant HW com SW) durant cinc anys amb reposició de material avariat (RMA) amb un SLA mínim de 8x5xNBD a comptar des de la posada en producció del servei.