Universitat Autònoma de Barcelona

PLEC DE PRESCRIPCIONS TÈCNIQUES

PROCEDIMENT OBERT

Contracte núm. CONTR-66/2024

Subministrament, instal·lació i manteniment de l'equipament de tallafocs per al nou nucli de xarxa

PLEC DE PRESCRIPCIONS TÈCNIQUES

Contracte núm. CONTR-66/2024

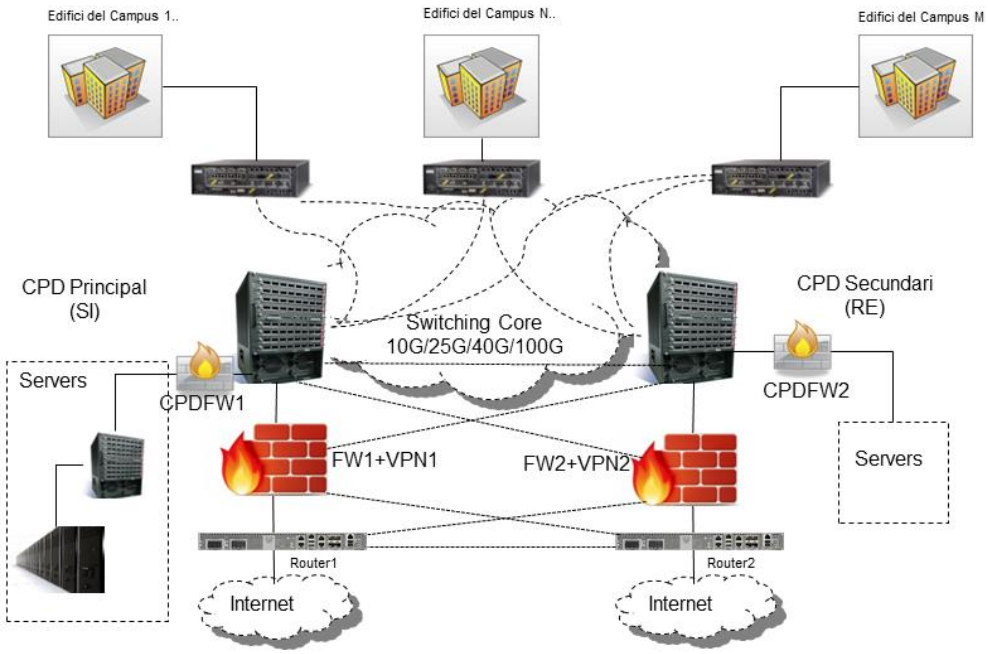
Subministrament, instal·lació i manteniment de l'equipament de tallafocs per al nou nucli de xarxa

1. Antecedents i plantejament de la necessitat

La UAB ha fet la renovació del nucli de la seva xarxa informàtica en base al procediment obert contracte número 49/2019. Per aquest contracte, s'ha augmentat la capacitat del nucli de la xarxa per 25. Paral·lelament la UAB ha millorat la seva connexió a Internet amb una nova infraestructura que li ha permès d'entrada doblar el cabdal de connexió i li dona la capacitat per multiplicar fàcilment per 10 aquest mateix cabdal.

En aquest escenari l'equipament de tallafocs disponible per la gestió d'aquesta nova xarxa ha quedat obsolet. Es per això que la UAB sol·licita una proposta i oferta econòmica per la renovació de l'equipament de tallafocs per al nucli de la seva xarxa informàtica. Aquests equips s'integraran a l'estructura de doble nucli que es mostra a l'esquema.

Esquema per la renovació dels Tallafocs 2024



Es demana oferta per la substitució dels equips FW1+VPN1 i FW2+VPN2 per equips de més capacitat. També es demana els serveis necessaris per la instal·lació, migració, substitució i posta en producció d'aquest equipament. Actualment aquesta funció la desenvolupen dos equips Fortigate 2201E. Els equips substituïts Fortigate 2201E es posaran en les posicions i funcions CPDFW1 i CPDFW2 i el concurs inclou també aquesta reconversió.

Es preveu que en la vida útil del nou equipament hi haurà increments regulars en el tràfic suportat que podran arribar al 500% del tràfic inicial. Es demana equipament que tingui un marge de creixement en el tràfic que permeti aquests increments sense necessitat de fer cap ampliació.

2. Requeriments de l'equipament i de l'oferta

Es demanen dos equips físics enrackables en armaris estàndard de 19 polsades.

Cada equip disposarà de les següents característiques:

- Un mínim de 14 interfícies de 25 GE SFP28 / 10 GE SFP+ i 6 interfícies de 100 GE QSFP28 / 40 GE QSFP+
- Les interfícies han d'admetre la connexió de mòduls SFP genèrics.
- Capacitat de virtualització d'un mínim de 10 sistemes virtuals per equip.
- Capacitat de tallafocs fins a nivell d'aplicació (NGFW Throughput) per un cabdal mínim de 34 Gbps.
- Capacitat de prevenció i detecció d'intrusions, antivirus i antimalware, IPS/IDS per un cabdal de 30 Gbps.
- 70 Milions de sessions concurrents.
- 870.000 noves sessions per segon.
- Suport per IPv4 i IPv6.
- Capacitat de contenció d'atacs web, filtrat d'URLs específiques.
- Capacitat de filtratge DLP.
- Capacitat de gestió SSL per Hardware.
- Capacitat de gestió i restricció de l'ample de banda, QoS, per tipus d'aplicació.
- Capacitats SDWan.
- Capacitat de gestió d'atacs DoS i DDoS.
- Capacitat per més de dos encaminaments virtuals amb OSPF i BGP.
- Funcionalitats WAF bàsiques.
- Possibilitat de creació de regles vinculades a llistes dinàmiques de DNS o de fitxers externs.
- Possibilitat de filtrar tràfic dins de la mateixa interface vlan.
- Doble font d'alimentació

Els equips han de tenir totes les llicències i estar dimensionats per suportar totes les capacitats de tractament indicades activades simultàniament per tot el tràfic i per totes les regles. Han d'estar certificats pel CCN i han d'aparèixer al seu catàleg CPSTIC (el model o algun model anterior de la seva família). Per a possibles futurs desenvolupaments, aquests equips han de disposar d'una versió en màquina virtual que no s'ha de subministrar en aquest concurs. A més la instal·lació haurà de complir els següents requeriments:

- Operació actiu/actiu sense connexió dedicada entre els dos aparells.
- Els dos equips s'integraran a la xarxa de la universitat en les posicions FW-VPN que marca l'esquema i els equips sortints substituiran els que estan en les posicions CPDFW.
- Han de poder gestionar regles per VLAN's.
- Han d'encaminar el tràfic en funció de l'estat de la xarxa de forma automàtica (sense la intervenció de l'operador). Actualment la gestió de l'alta disponibilitat es fa per OSPF però han de poder encaminar per BGP.
- Gestió de regles integrada: sense necessitat d'una plataforma de gestió separada es gestionaran les regles i aquestes es distribuiran als dos equips simultàniament. Quedaran excloses aquelles solucions que requereixin una plataforma de gestió externa per gestionar i administrar la solució.
- Gestió de regles basades en dispositius i en usuaris validats a Microsoft Entra ID o a les aplicacions corporatives (CAS). Suport de portal captiu d'accés per poder validar els usuaris que no son reconeguts pels sistema.
- Gestió basada en web simple i amigable.

- 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.
- S'oferirà gestió i reporting complets.
- Anàlisi i correlació d'events incloent tecnologia UEBA o equivalent per tot el tràfic dels firewalls en un equipament addicional, pot ser sobre una màquina virtual que s'hostatjarà en una plataforma que no forma part d'aquesta licitació.
- La plataforma d'anàlisi ha de tenir una capacitat de gestió d'un màxim de 120GB diaris.
- Interfícies de gestió i anàlisi amigables.
- 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, Netflow
- Sistema amb el pla de gestió dedicat i separat del pla de dades, per evitar que la saturació d'un dels dos plans afecti l'altre.
- Servei de VPN per els usuaris de la universitat amb validació SAML amb Microsoft Entra ID i dos nivells d'ús: usuaris amb accés Proxy web proporcionat pels propis equips i usuaris amb accés addicional de túnel SSL.
    - Servei de VPN bàsica per un número il·limitat d'usuaris sense llicència addicional, amb qualsevol dels dos nivells d'ús (proxy web i client de VPN).
    - Servei de VPN avançada que permeti polítiques en funció de la posició de seguretat de la màquina des d'on es connecta l'usuari amb 1000 llicències .
    - Polítiques associades a la identitat de l'usuari a Microsoft Entra ID, en funció del grup al que pertanyin.
    - Possibilitat de definir usuaris locals amb doble factor de protecció.
    - Client de VPN per sistemes Windows/Linux/MacOS/Android/iOS/iPadOS.
- Servei de prevenció d'atacs "zero day" amb connexió al núvol del fabricant en temps real.
- L'oferta ha d'incloure la instal·lació dels nous equips, la migració de les funcionalitats, la incorporació de la inspecció del nucli de la xarxa de campus, la reubicació dels equips que actualment estan en producció en la posició final desitjada com a tallafocs de CPD i la creació d' una estructura DMZ addicional associada a aquest nucli. Els firewalls tenen un total aproximat de 1500 regles, la VPN té uns 50.000 usuaris potencials amb una simultaneïtat màxima de 5000 usuaris. Aquesta instal·lació s'ha de fer amb un impacte mínim en els serveis en producció (això vol dir que les actuacions amb més impacte s'hauran de programar fora dels dies o els horaris de treball oficials).
- L'oferta també ha d'incloure els mòduls SFP (genèrics o de fabricant) i els fuetons necessaris per la connexió a la infraestructura de xarxa que es demana.
- Es farà una formació de la instal·lació a mida, a les dependències de la Universitat, tant per al personal de la UAB que ha de fer el suport de segon nivell com per l'empresa que porta l'explotació del servei.

Es demana una oferta econòmica amb els preus desglossats i que inclogui com a mínim aquests conceptes valorats:

- Preu de l'equipament (maquinari) i manteniment de l'equipament per a 5 anys NBD.
- Preu de les subscripcions (programari) i manteniment de fabricant per 5 anys NBD, incloent-hi totes les actualitzacions de software i subscripcions que hi hagi en aquest període.
- Serveis d'instal·lació, configuració, migració, reubicació i formació.
- Serveis de suport de l'integrador per 5 anys.
- Desglossament de les llicències d'operació per 5 anys.

El preu sumat dels conceptes anteriors ha de coincidir amb el preu de l'oferta econòmica.

També s'adjuntarà una memòria tècnica en què es detallin, com a mínim, les següents funcionalitats:

- Descripció del funcionament del tallafocs i el portal VPN i l'operativa de la redundància per la instal·lació que es proposa.
- Descripció de les eines d'administració i gestió, monitorització, elaboració i gestió d'informes.

- Descripció del sistema de prevenció d'amenaces (IPS) i antivíric.
- Descripció del servei de prevenció d'atacs "zero day".
- Descripció de les tècniques de detecció d'aplicacions de la plataforma.
- Descripció dels mecanismes d'identificació d'usuaris.
- Descripció dels mecanismes de qualitat de servei (QoS).

Juntament amb la memòria tècnica, s'inclourà un document diferent on s'exposarà el projecte d'implantació. En aquest projecte es descriuran els perfils dels professionals assignats, el compromís de dedicació i les hores dedicades de cada perfil i s'inclourà una proposta de desenvolupament amb les tasques i fites més rellevants explicades. El projecte inclourà també un cronograma versemblant i realista amb el desenvolupament de la implantació que inclogui les tasques i fites explicades anteriorment. També es presentarà el pla de formació amb el seu temari i durada.

Per aquest concurs es demana que l'empresa adjudicatària del contracte estigui certificada ENS o ISO 27001 o, si no és el cas, ha de poder presentar la documentació conforme està en procés de certificació d'algun d'aquests dos estàndards.

3. Prova de concepte

La UAB es reserva el dret de demanar a l'empresa que hagi presentat l'oferta més avantatjosa i sense cost addicional, la verificació del funcionament correcte de la seva solució.

La prova consistirà en una valoració del rendiment amb tràfic real tenint en compte la previsió que els equips hauran de suportar durant la seva vida útil un increment del tràfic del 500%.

Per la prova s'instal·larà un dels equips proposats amb un port mirroring de tot el tràfic que estan rebent els tallafocs actuals en producció. L'equip haurà de tenir una única regla que obligui a processar el 100% del tràfic amb totes les funcionalitats de seguretat activades, sense proxificar cap comunicació, sense descartar cap paquet i detectant totes les aplicacions que corren en tots els ports, no només els per defecte. La base de dades de signatures de seguretat (antivirus, vulnerabilitats, etc.) s'haurà d'utilitzar de manera integral, sense possibilitat de fer servir subconjunts de signatures. La política haurà de proporcionar visibilitat del tipus de fitxers que es mouen. Durant la prova s'haurà d'analitzar el software maliciós en el servei de prevenció d'atacs "zero day" amb connexió al núvol del fabricant.

Es monitoritzarà l'ús de la CPU de tots els processadors d'aquest equip des del sistema de gestió Cacti corporatiu (l'empresa haurà de proporcionar les MIBs adients que permetin aquesta monitorització).

La prova es considerarà superada si es compleix que l'ocupació de les CPUs determinada pel mostreig amb refresc cada 5 minuts en hora punta no supera el 15% d'ocupació en el pic màxim.

En tot cas, la prova de concepte només es durà a terme si de la proposta tècnica presentada per l'empresa no es pot deduir el compliment dels requisits tècnics d'una forma segura i definitiva. La mesa de contractació decidirà si la prova és necessària o no.