SÍNDIC
EL DEFENSOR DE LES PERSONES

PLEC DE PRESCRIPCIONS TÈCNIQUES PARTICULARS PER A LA CONTRACTACIÓ DEL SUBMINISTRAMENT D'UN TALLAFOCS I SERVEI DE MANTENIMENT CORRECTIU (EXPEDIENT SGC-2025/01)

SÍNDIC
EL DEFENSOR DE LES PERSONES

ÍNDEX

SÍNDIC
EL DEFENSOR DE LES PERSONES

1. Objecte del contracte

Subministrament d'un tallafocs i servei manteniment correctiu amb un màxim de 200 hores per la durada del contracte.

2. Context actual

El tallafocs actual utilitza totes les funcionalitats del mateix i esta connectat a:

- Xarxes i subxarxes de la LAN
- Diverses conexions WAN
- Vlan's
- Punts d'accés wifi

3. Requeriments tècnics del nou tallafocs

Es relacionen a continuació les característiques que com a mínim haurà de complir el nou tallafocs:

- **El Tallafocs ha d'estar qualificat per l' última versió de la guia del CCN CERT per obtenir el certificat de l'Esquema nacional de seguretat**.
- Tallafocs a "Statefull Packet Inspection" (Firewall tradicional basat en port – protocol: 5.5 Gbps (mínim).
- Tallafocs amb control del 100% sobre les aplicacions: 3,5 Gbps (mínim).
- Tallafocs amb inspecció 100% del trànsit SSL: 850 Mbps
- Tallafocs de nivell 7 en una cadena d'anàlisi composta per URL Filtering,
- Un mínim de 100 llicències d'usuaris connectats per vpn ssl de forma concurrent.
- Antivirus, IPS, AntiSpyware, FileBlocking i DLP amb el 100% de les firmes disponibles aplicades sobre cadascun dels filtres: 3,5 Gbs
- Connexions mínimes (SPI/DPI/DPI SSL): 2.000.000 / 750.000 / 150.000
- Wan amb balanceig de càrrega de forma individualitzada i personalitzada a nivell 4 i 7. Capacitat per suportar balanceig de línia automàtic tipus Round Robin, o Split Over. Amb negociació PPPOE. Compatible amb mòdems 4G/5G.
- Configuració que utilitzi dos firewalls de manera simultània (HA) per protegir una xarxa o sistema informàtic obtenint la capacitat del sistema per mantenir la seva funcionalitat sense interrupcions, fins i tot en cas de fallada d'un dels tallafocs.
- Sistema d'alimentació elèctric redundant, amb doble font d'alimentació.
- 24x1GbE, 6x10G SFP+, 4x5G SFP+, 2 USB 3.0, 1 Console, 1 Mgmt. Port

4. Funcionalitats de la prestació:

1. Mode de configuració entre dispositius NGFW de: parella d'equips d'alta disponibilitat amb sincronització d'estats.

2. Tallafoc de nivell 4. Els equips oferiran totes les funcionalitats bàsiques d'un tallafoc típic: filtratge de trànsit per IP i port amb control de sessió, nat, pat, log del trànsit, etc.

3. Tallafocs de nivell 7: Els equips hauran de poder filtrar el trànsit a nivell d'aplicació podent distingir les aplicacions independentment del port que usin. El fabricant

haurà d'anar actualitzant i ampliant regularment la llista d'aplicacions reconegudes.

4. Gestió d'usuaris: Els equips hauran de poder reconèixer l'usuari que està generant un trànsit determinat. Per això els equips s'hauran de comunicar amb l'Active Directory (MICROSOFT) de la xarxa interna amb protocols LDAP, Radius, TACACS+. Els equips hauran de desar el detall de l'usuari als logs del trànsit.

5. IPS: Els equips hauran d'incorporar un motor IPS (Intrusion Prevention System) per poder detectar i aturar el nombre més gran possible d'atacs. El fabricant haurà d'anar actualitzant i ampliant regularment la llista d'atacs reconeguts.

6. El tallafocs haurà de tenir una solució de Gateway antivirus integrada amb capacitat d'inspeccionar protocols HTTP/HTTPS – SMTP-FTP – POP3 – IMAP –CIFS/NETBIOS TCP Stream, sense limitació de mida dels fitxers propietària i no de tercers.

7. URL filtering: Els equips hauran de categoritzar les url's i per categories per gestionar les que els usuaris puguin navegar. El fabricant haurà d'anar actualitzant i ampliant regularment el llistat d'urls i categories categoritzades.

8. Des encriptació SSL: Els equips hauran de poder desencriptar i inspeccionar el trànsit xifrat. Es valorarà que aquesta tasca no es faci via programari sinó amb maquinari dedicat. La solució ha de permetre definir quines categories d'url's o url's concretes es desencriptin i quines no.

9. Aplicació de polítiques de qualitat de servei (QoS). Els equips hauran de poder gestionar l'amplada de banda i la prioritat dedicats a cada política de seguretat.

10. Reputació d'ip's i/o url's: Els equips hauran de poder reconèixer ip's públiques i/o url's que siguin reconegudes com a origen de codi maliciós, i per tant aturar les connexions a/des d'aquestes ip's.

11. Sandboxing: Els equips hauran de poder enviar-los fitxers que considerin sospitosos enviar els fitxers sospitosos a un entorn al cloud que realitzi aquesta tasca i inspeccioni els fitxers en un entorn virtual amb multimotor amb inspecció profunda de memòria amb possibilitat de bloquejar fitxers a fins que hi hagi un veredicte.

12. Es valorarà entre altres millores, l'ús de tècniques antievassive threats, la informació que s'obté de les anàlisis, o la quantitat de plataformes suportades i la capacitat d'aturar els arxius al Gateway.

13. Es valorarà un enfocament de Sandboing multimotor amb motors propietaris i tercers tipus motor RTDMI o similar tecnologia més precisa, minimitzant els falsos positius i identifica i mitiga atacs sofisticats.

14. VPN: Els equips permetran la creació de vpn's, tant del tipus ipsec com del tipus vpn-ssl. Per a la solució vpn-ssl (certificat wildcard) calen clients que es puguin instal·lar localment en màquines Windows com Mac, Linux i Android.

15. Funcions automatitzades per la protecció d'atacs DDoS, així com totes aquelles que permetin la millor protecció possible contra atacs i vulnerabilitats avançades, com ara APT's, atacs dia 0 o botnets.

16. Els equips han de poder funcionar com un proxy de navegació transparent per als usuaris interns, gràcies a les funcionalitats de control d'aplicacions, control d'usuaris, url filtering i reporting entre d'altres.

17. Creació de zones de seguretat independents (xarxa perimetral, xarxa interna...), garantint que el trànsit d'una zona no podrà passar mai a les altres independentment de les regles de seguretat que hi hagi.

18. Els equips han d'implementar IPv6 i facilitar la transició d'IPv4 a IPv6 de la xarxa corporativa i la connexió a Internet.

19. Monitorització de la salut del sistema. El sistema de monitorització s'haurà de fer mitjançant.

20. Visibilitat i reporting:
    a. El sistema ha de permetre visualitzar tots els logs recollits pels equips (trànsit, events de seguretat, etc...) i fer-hi cerques de forma intuïtiva, mostrant tot el detall d'informació possible en temps real
    b. El sistema també ha d'agrupar els logs per aplicació, usuari, ip, url, etc... o per qualsevol combinació d'aquests paràmetres, com, per exemple, quines aplicacions ha fet servir determinat usuari, quants bytes ha consumit amb cadascuna , etc...
    c. El sistema permet extreure diversos tipus d'informes automatitzats i descarregables.
    Entre ells hi haurà d'haver informes de l'activitat d'un determinat usuari de l'Active Directory corporatiu: a quin web ha navegat, durant quant de temps, quines aplicacions ha fet servir (aplicacions amb trànsit cap a Internet que travessin els tallafocs), quines categories d'url ha visitat, quins accessos se li han denegat, etc...
    d. Visió global, mitjançant gràfics i altres recursos, de l'estat de la xarxa a cada moment: quantitat de trànsit, quantitat de codi maliciós aturat, aplicacions detectades, url's més visitades, usuaris més actius, etc.

21. Possibilitat de compartir llicències entre tots dos dispositius en HA, reduint el TCO en les futures renovacions.

L'equip tindrà la capacitat per a incorporar les següents funcionalitats futures per integrar-se amb els clients d'antivirus dels equips.

- Endpoint Security Enforcement o similar: els punts finals darrere del tallafoc que no tinguin client en execució no podran accedir als serveis basats en Internet mitjançant el tallafoc.
- Visibilitat d'usuari i Single Sign-On (SSO) IP. Les adreces IP dels punts finals darrere del tallafoc s'assignen automàticament a l'usuari connectat als punts finals en el moment que s'utilitza per als informes d'activitat de l'usuari, així com l'inici de sessió únic (SSO) al tallafoc per a polítiques d'accés basades en l'usuari.

- Els punts finals que executen el client que desencadenen deteccions d'amenaces al tallafoc per part dels motors GAV, IPS, App Control o Botnet veuran una notificació al seu punt final.
- DPI-SSL amb les polítiques de certificats de confiança de client, els administradors poden imposar la instal·lació de certificats SSL que s'utilitzaran per inspeccionar el trànsit xifrat cap a/des dels punts finals mitjançant la funció DPI-SSL.
- Capacitat d'integració amb antivirus amb tecnologia EDR i XDR

5. Pla de treball: lliurament, instal·lació i posada en funcionament del maquinari

El contractista resta obligat a assumir les operacions següents:

a) Transportar el maquinari a la seu del Síndic de Greuges de Catalunya i dipositar-lo en l'àrea d'informàtica.

b) Lliurar al Síndic de Greuges un certificat de lliurament o un albarà que ha d'incloure, com a mínim, les dades identificatives de cada producte, els números de sèrie, l'adreça MAC, la llicència de programari i altres dades que s'acordin durant la posada en funcionament del projecte, d'acord amb el que s'hagi acordat amb el Síndic.

c) Instal·lació de tots els equips, programari necessaris, llicències i configuracions com estaven la infraestructura original.

d) Configuració de les noves funcionalitats del tallafocs a nivell de seguretat, etc.

e) Connectar totes les xarxes i proves de funcionament, aquesta part s'ha de realitzar fora d'horari perquè tinguem el mínim impacte en el canvi.

6. Manteniment Correctiu

El manteniment correctiu es sol·licitarà cada vegada que es consideri necessari per a realitzar les accions detallades a continuació i tindrà un preu per hora màxim de 68€. Les hores màximes anuals de servei de manteniment correctiu seran de 40 hores cada any, amb un total de 200 hores per la durada del contracte.

Aquest manteniment estarà destinat a tota la infraestructura de xarxa tant del tallafocs com de tots els dispositius de xarxa que pengen del mateix.

- Actualitzacions del Sistema:
  Assegurar-se que el firmware o software del firewall estigui actualitzat regularment amb les últimes correccions de seguretat.
  Programar actualitzacions fora de les hores de major activitat per minimitzar interrupcions.

- Configuracions noves del sistema:
  Noves configuracions per raons tècniques o de ciberseguretat com la segmentació i comunicació de xarxes internes.
  Noves WAN's, Subxarxes, DMZ's, VLAN's, etc

- Regles del Firewall:
  Crear noves, revisar i actualitzar les regles del firewall periòdicament per assegurar-se que només les connexions necessàries estiguin permeses.
  Eliminar regles innecessàries o obsoletes.

- Control d'Accés:
  Revisar i actualitzar les llistes de control d'accés (ACL) per garantir que només els usuaris autoritzats tinguin accés a determinats recursos.
  Monitoritzar els registres d'accés per a possibles activitats sospitoses.

- Protecció contra Malware:
  Actualitzar les signatures d'antivirus i assegurar-se que els mecanismes anti-malware estiguin habilitats i actualitzats.
  Realitzar escaneigs periòdics per identificar possibles amenaces.

- Còpies de Seguretat:
  Realitzar còpies de seguretat regulars de la configuració del firewall per poder restaurar ràpidament la configuració en cas de fallades o errors de configuració.
  Provar la restauració de còpies de seguretat periòdicament.

- Monitorització del Rendiment:
  Utilitzar eines de monitorització per supervisar el rendiment del firewall i la càrrega del sistema.
  Identificar i respondre a pics inesperats d'activitat.

- Auditories de Seguretat:
  Realitzar auditories de seguretat periòdiques per avaluar l'eficàcia dels controls de seguretat implementats.
  Identificar i corregir les possibles vulnerabilitats.

- Gestió de Registres:
  Configurar la recopilació i l'emmagatzematge de registres d'activitat del firewall.
  Revisar els registres regularment per identificar possibles amenaces o anomalies.

- Plans d'Emergència:
  Desenvolupar i revisar plans d'emergència per afrontar atacs o fallades de seguretat.
  Assegurar-se que l'equip de seguretat estigui format i sigui conscient dels procediments d'emergència.

- Comunicació amb el Personal:
  Mantenir una comunicació constant amb l'equip de seguretat i altres interessats sobre les actualitzacions, canvis de configuració i amenaces recents.

- Proves de Penetració:
  Realitzar proves de penetració regulars per identificar possibles punts febles i avaluar la resistència del firewall contra atacs externs.

- Revisió de Polítiques de Seguretat:
  Revisar i actualitzar les polítiques de seguretat de la xarxa i del firewall segons les necessitats i canvis en l'entorn.

- Registre i Informació d'Incidents:
  Establir un sistema de registre d'incidents per documentar i gestionar respostes a amenaces i incidents de seguretat.

- Col·laboració amb Proveïdors de Seguretat i l'agència de ciberseguretat de Catalunya:
  Mantenir una relació activa amb els proveïdors de seguretat i l'agència de ciberseguretat de Catalunya per rebre informació sobre amenaces actuals i solucions.

7. Garantia del subministrament del tallafocs.

En el cas de substitució d'elements coberts per la garantia hauran de substituir-se per productes nous

L'empresa adjudicatària ha de prestar una garantia de fabricant amb cobertura de reparació per qualsevol avaria o anomalia que pateixin els equips com a mínim durant el període de 5 anys a partir de la posada en marxa. Si s'acredita l'existència de vicis o defectes en els béns subministrats, s'actuarà d'acord amb l'article 305 de la Llei de contractes del sector públic (LCSP).

El licitador, en cas de no ésser el fabricant del producte, haurà de presentar un certificat d'aquest conforme la garantia dels equips està contractada directament al fabricant.

Amb caràcter general, les reparacions s'han de fer *in situ* i oferint un temps de resposta que minimitzi el temps en què l'usuari haurà d'estar sense dispositiu.

En cas d'avaria o parada dels equips per una incidència tècnica, el temps màxim de resposta del servei tècnic serà de 24 hores des de la notificació del mateix, descomptats dissabtes i festius.

Un cop iniciada la reparació coberta per la garantia, el temps de finalització de la mateixa amb operativitat total de la màquina, no podrà ser superior a 72 hores, descomptats dissabtes i festius.
Les reparacions i manteniment de les màquines es realitzaran in situ en horari d'oficina, de dilluns a divendres no festius, de 9h a 19h.

Jordi Clemente Pascual
Coordinador TIC
Barcelona, en la data de la signatura electrònica