PLEC DE PRESCRIPCIONS TÈCNIQUES PER A LA CONTRACTACIÓ DE LA INSTAL·LACIÓ I MANTENIMENT DE FIREWALLS PERIMETRALS

EXPEDIENT 24SM0872

SUBMINISTRAMENT I SUBSTITUCIÓ DE FIREWALLS PERIMETRALS

1 OBJECTE DEL CONTRACTE

L'objecte del present contracte és el Subministrament, instal·lació i manteniment 24*7 del tres primers anys de dos nous Firewalls perimetrals corporatius, per substituir els actuals ja obsolets. El present plec té per objecte establir les prescripcions tècniques particulars que regiran la prestació i definir les qualitats tècniques mínimes generals dels equips a adquirir.

El CCSPT disposa d'una plataforma de seguretat perimetral formada per un sistema distribuït en alta disponibilitat compost per dos equips Palo Alto Networks 3020 en alta disponibilitat i la seva corresponent subscripció als serveis Threat Prevention (Intrussion Prevention System), filtrat de continguts de navegació web (Advanced URL filtering), el servei Wildfire de Paloalto per analitzar de forma proactiva atacs de malware conegut i desconegut així com atacs APT (Advanced Persistent Threat) i el servei Global Protect.

Aquests Firewalls perimetrals PALOALTO, a més de no disposar de la suficient potència per analitzar tot el tràfic SSL i assegurar la xarxa interna, no suporten les darreres versions de firmware PAMOS del fabricant PaloAlto i en breu arribaran a la fi de la seva vida útil i el fabricant deixarà de publicar actualitzacions de seguretat. Per tant el present plec té per objecte establir les prescripcions tècniques particulars per la substitució per obsolescència dels actuals Firewalls perimetrals corporatius i substitució per models actuals, amb suport de les actuals versions de firmware PAMOS del fabricant PaloAlto i amb potència suficient per poder configurar noves funcionalitats com la inspecció HTTPS.

La prestació contemplada en aquesta licitació deurà contemplar el subministrament de nous firewalls amb les característiques tècniques que es detallen al següents punts i que facin ús de les llicències que el CCSPT ja disposa:

- Threat Prevention (Intrussion Prevention System)
- Filtrat de continguts de navegació web (Advanced URL filtering)
- El servei Wildfire de Paloalto per analitzar de forma proactiva atacs de malware conegut i desconegut així com atacs APT (Advanced Persistent Threat)
- El servei Global Protect.

Amb el subministrament d'aquests firewalls, caldrà incloure l'ampliació del període de validesa de les actuals llicències per que finalitzin juntament amb el període de suport dels firewalls (3 anys) i caldrà incloure la llicència necessària per implementar una nova funcionalitat de "DNS Security" especificada en aquest plec.

El servei també haurà de contemplar la substitució dels antics firewalls pels nous i aquesta substitució haurà de ser transparent pel CCSPT, sense pèrdua de les regles de seguretat actualment implementades i amb el menor tall de servei possible.

L'adjudicatari, mitjançant una borsa d'hores de no menys de 100 hores anuals, s'encarregarà de donar suport a l'àrea de sistemes de la direcció de sistemes d'Informació a l'hora de resoldre les incidències diàries de la plataforma. Així mateix s'encarregarà de fer el manteniment preventiu de la plataforma, instal·lant els pegats de seguretat i upgrade tant del sistema operatiu (firmware). S'encarregarà d'obrir els casos de suport amb el fabricant en cas de requerir un

tercer nivell de suport. També proposarà al CCSPT l'evolució d'aquesta plataforma en el futur, amb nous productes o noves funcionalitats que redundin en un major servei als usuaris de la Corporació. Altres accions a desenvolupar seran:

- Gestió d'incidències on site.
- Gestió d'incidències i consultes tècniques en remot.
- Suport telefònic i documental via e-mail.
- Intervenció presencial de resolució d'incidències on site en els casos d'emergència requerits.
- Manteniment evolutiu de la solució.

2 REQUISITS GENERALS

Els equips han de ser capaços de reconèixer i controlar totes les aplicacions (nivell 7 pila TCP) sobre qualsevol port TCP/UDP, tant per a IPv4 com IPv6, de manera nativa, sense llicències ni mòduls addicionals que puguin afectar al seu rendiment.
Els perfils de seguretat i filtratge han d'incloure totes les signatures o mecanismes actius sense degradació del rendiment pel nombre de signatures actives.
Les característiques funcionals que ha de complir el NGFW objecte de la licitació són:

- Suport d'alta disponibilitat, tant actiu/passiu com actiu/actiu.
- Amb l'objectiu de garantir que una sobrecàrrega del maquinari destinat a donar el servei (trànsit de xarxa) no afecti la gestió d'aquest, els equips han de disposar de maquinari independent de gestió integrat en l'equip, fins i tot amb sistema operatiu diferent amb l'objectiu d'independitzar totalment els plans de gestió i de xarxa. S'ha de documentar quins recursos de maquinari es destinen específicament a la gestió i quins a producció (xarxa).
- Port de gestió dedicat fora de banda.
- Es necessiten ports específics de gestió d'alta disponibilitat dedicats amb l'objectiu de garantir que no consumeixin interfícies de servei per a aquesta tasca.
- L'equip ha de poder ser gestionat completament tant des de l'entorn Web com des de l'entorn CLI.
- Desplegaments de xarxa en mode sniffing (fora de línia, rebent un mirall del trànsit), cable (transparent), capa 2 i capa 3 (routing). S'han de poder mesclar diferents tipus de topologies d'interfícies de xarxa de manera simultània sobre el mateix equip.
- Suport a l'estàndard IEEE 802.1Q (encapsulament de diverses VLAN sobre el mateix enllaç físic) i IEEE 802.3ad (agregació de diversos enllaços físics).
- Suport a Jumbo Frames (MTU 9192 bytes).
- Suport d'IPv6 tant en mode nivell 3 com en mode transparent.
- Ha de suportar les següents característiques de VPN (Xarxa Privada Virtual):
    - Suport a VPNs sobre IPSec (Internet Protocol Security).
    - Suport a VPNs sobre SSL (Secure Socket Layer).
    - Suport a x-auth en SSL-VPNs per a la integració amb clients de tercers.
- Gestió d'esdeveniments dels equips mitjançant:
    - Enviament de registres a sistemes tercers, via syslog.
    - Gestió mitjançant SNMP.

- Suportar protocols d'Encaminament (routing):
  - Protocols dinàmics d'encaminament: RIP, OSPF i BGP.
  - Suport d'encaminament per al trànsit multicast (PIM Sparse Mode).
  - Suport de Policy Routing.
- Suport a RBAC (Role Based Access Control - Perfils per a gestió diferenciada i gestió delegada).
- Capacitat de realitzar tasques de NAT i PAT, incloent-hi NAT transparent.
- Suport de HTTP2, sense cap configuració addicional. Aquesta millora permet securitzar servidors web que presten serveis sobre HTTP/2 i beneficia als usuaris amb la velocitat i eficiència de consum de recursos d'aquest protocol.
- Inspecció de les amenaces en el flux HTTP/2.
- Capacitat de generació de certificats digitals, així com la importació de certificats emesos per tercers.
- Suport a OCSP (Online Certificate Status Protocol) i llistes de revocació de certificats (CRL).
- Suport a la integració amb mòduls HSM de tercers per a l'emmagatzematge de les claus criptogràfiques.
- Permetre aplicar QoS per aplicació, usuari o URL. Establiment d'ample de banda màxim i garantit. L'activació d'aquesta funcionalitat no ha de minvar la resta de capacitats exigides en la solució, ni en funcionalitat ni en rendiment.

REQUISITS DEL HARDWARE

Es oferiran dos equips que treballaran en alta disponibilitat (HA). Les característiques de capacitat que han de complir cadascun dels dos equips objecte de la licitació són:

• Arquitectura hardware separada per a gestió i servei, amb recursos hardware dedicats independents, que en cap cas es compartiran amb el pla de dades, amb l'objectiu de poder garantir que una sobrecàrrega del hardware destinat a prestar el servei no afecti a la gestió i viceversa.
• 12 ports Ethernet 1G/2.5G/5G/10G.
• 10 ports 1G/10G (SFP/SFP+).
• 4 ports 25G (SFP28)
• Disc dur redundat SSD per a Sistema Operatiu (Mínim 400GB)
• Port dedicat per a gestió "out-of-band".
• Ports dedicats per a Alta Disponibilitat.
• Port de consola RJ45.
• Fonts d'alimentació redundants.

Requisits de capacitat i rendiment

Firewall throughput amb inspecció a nivell 7, identificació d'aplicacions i logging activat utilitzant paquets de 64 KB amb trànsit mixt	11 Gbps
Threat Prevention throughput amb tots els següents serveis activats (Control d'Aplicacions, IPS, Antivirus conegut, Antispyware, AntiMalware desconegut (SandBoxing) i logging activat utilitzant paquets de 64 KB amb trànsit mixt). Control d'URL, Seguretat DNS i Bloqueig de fitxers	5.1 Gbps
IPSEC VPN Throughput.	6.8 Gbps
Capacitat total de sessions.	1.4 M
Sistemes virtuals	1, ampliable a 11 amb llicència

REQUISITS DE SEGURETAT

Totes les funcionalitats es poden activar de forma concurrent en tots els Sistemes de Seguretat tant virtuals com físics.

2.1 Visibilitat i control d'aplicacions

• El motor de classificació que s'utilitzarà per identificar el trànsit serà en base a l'aplicació (nivell 7 de la pila TCP), i no només el port. Així, l'aplicació no ha de formar part d'un filtre que s'apliqui posteriorment, sinó que ha de ser l'element d'identificació inicial i basar la resta de l'anàlisi en el seu context.
• Capacitat per identificar i controlar, de manera nativa, sense llicències ni mòduls addicionals que puguin afectar al rendiment, un mínim de 3.600 aplicacions actives actuals (com ara, Webex, Sharepoint, Whatsapp, Facebook, Spotify, Tuenti, Webex, Bit Torrent, SAP, Oracle, GMail, Last.Fm, Skype, Meebo, etc.).
• Reconeixement i filtrat de qualsevol aplicació sobre qualsevol port TCP/UDP, i no només sobre els ports estàndard.
• Ha de permetre crear signatures personalitzades per a la identificació d'aplicacions pròpies.
• Ús d'una política de seguretat unificada, que contempli les aplicacions com a part integral de la mateixa.
• Reconeixement i control de les subfuncions dins d'una aplicació, com ara transferències de fitxers, correu electrònic, xat, etc.
• Identificar, classificar i gestionar sistemàticament el trànsit desconegut. La solució ha de ser capaç d'identificar el trànsit desconegut, categoritzar-lo per a la seva anàlisi i gestionar-lo en base a polítiques. A més, ha de ser possible prendre PCAPs automàticament del trànsit desconegut, així com generar signatures personalitzades per identificar-lo en cas que sigui trànsit desitjat.

2.2 Integració i identificació d'usuaris

- Identificació d'usuaris transparent a través de la integració amb directoris LDAP, incloent-hi l'Active Directory de Microsoft i el Novell eDirectory.
- Capacitat d'identificar i confirmar usuaris en entorns Microsoft mitjançant l'ús de WMI (Windows Management Instrumentation).
- API XML per a la identificació d'usuaris, que permetrà injectar usuaris après des d'altres sistemes, facilitant així la integració amb altres mecanismes d'autenticació via scripting (com ara, sistemes 802.1x, Radius, …).
- El Sistema de Seguretat integrarà un recopilador de syslog (tant TCP com UDP) per poder aprendre usuaris que han estat validats en altres sistemes d'autenticació. Aquesta funcionalitat permetrà als administradors redirigir els esdeveniments de syslog d'autenticació contra el servei de syslog del Sistema de Seguretat, que comptarà amb un sistema de parsing automàtic dels logs per extreure i aprendre d'aquests la tupla usuari-IP. Aquest mecanisme permet integrar les funcions d'identificació d'usuaris pràcticament de manera transparent amb qualsevol sistema d'autenticació que generi esdeveniments de syslog.
- Serveis d'autenticació basada en LDAP (incloent NTLM), Kerberos (inclosa la funció de Single Sign On), Radius i base de dades local al Sistema de Seguretat per als accessos VPN i per a l'accés a aplicacions.

- Valoració extra: capacitat d'integració nativa amb serveis d'autenticació MFA (Okta, PingID, RSA, Duo...).
- Possibilitat de connectar els firewalls amb un servei central d'autenticació a la núvol que integri tots els sistemes d'autenticació de l'organització, evitant haver de configurar tots aquests sistemes en tots els firewalls.
- Capacitat d'usar MFA per a l'accés VPN d'un, diversos o tots els usuaris.
- Capacitat per crear grups dinàmics amb membres actualitzats a través d'una API XML.

2.3 Protecció davant d'atacs de denegació de servei

- Reconeixement i prevenció d'escaneigs de xarxa.
- Detecció i mitigació d'atacs de DoS. S'ha de comptar almenys amb els següents tipus de protecció: SYN Flood, UDP Flood, ICMP Flood, protecció davant d'inundacions per noves sessions o protecció per atacs de desbordament per límits de sessions establertes, podent en cada cas establir els llindars necessaris per activar aquestes proteccions.
- Capacitat que el fabricant ofereixi llistes d'IPs malicioses, que s'actualitzin i mantinguin automàticament i es posin a disposició per a l'ús al firewall de manera nativa.

2.4 Protecció davant de vulnerabilitats

Pel que fa a la protecció davant de vulnerabilitats, el tallafoc ofert ha de comptar amb la possibilitat d'aplicar polítiques de protecció davant de vulnerabilitats i exploits tant al trànsit entrant com al sortint, complint amb les següents funcionalitats:

- S'ha de poder aplicar polítiques tant de detecció com de prevenció (mode IDS o IPS) davant possibles exploits de vulnerabilitats que es detectin en el trànsit ja sigui entrant o sortint d'Internet, realitzant l'anàlisi en una única passada per a tot tipus d'amenaces.
- En la protecció davant de vulnerabilitats, el criteri a utilitzar és la identificació de l'aplicació per poder aplicar perfils de vulnerabilitats ajustats a aquesta aplicació, de manera que no es vegi afectada la rendiment de l'equip.
- Els perfils de detecció i protecció davant de vulnerabilitats han de permetre's aplicar tant al trànsit originat des de la xarxa interna com al trànsit originat des d'Internet, i ha de ser possible l'aplicació de detecció i protecció davant de vulnerabilitats especificant si són vulnerabilitats que s'apliquen als clients, els servidors o a ambdós indistintament.
- Les vulnerabilitats han d'estar categoritzades per tipus i per nivells de risc, de manera que l'aplicació de perfils de protecció en el trànsit es pugui realitzar en base a aquestes categories.
- S'ha de poder usar la identificació CVE de vulnerabilitats per a l'aplicació de perfils de protecció específics.
- Ús de la identificació d'aplicacions com a criteri per seleccionar els perfils de protecció de vulnerabilitats, de manera que s'apliquin només aquelles signatures específiques segons l'aplicació que s'està utilitzant.
- Capacitat de creació de signatures de IPS a partir de la informació d'una signatura de Snort i que es permeti importar de manera automàtica un llistat de regles de Snort.
- Suport en línia de Deep Learning i anàlisi a la núvol.

- Prevenció de Command and Control desconegut basat en Machine Learning des de la núvol.

2.5 Antivirus

El tallafoc proposat ha de tenir la capacitat de definir polítiques d'antivirus, de manera que les descàrregues de fitxers realitzades en sentit Internet xarxa Interna o viceversa siguin inspeccionades i bloquejades si el seu contingut és maliciós.
S'ha de poder aplicar polítiques que permetin aplicar el motor d'antivirus sobre protocols com ftp, http, imap, pop3, smb o smtp, definint per a cadascun d'aquests protocols l'acció a realitzar (permetre els fitxers, descartar els fitxers, desconnectar la sessió o registrar mitjançant logs) davant la detecció del fitxer maliciós pel motor d'antivirus.
El tallafoc ha de permetre l'aplicació de polítiques d'antivirus de manera granular, permetent, per exemple, l'aplicació d'aquestes polítiques a certs usuaris de determinats grups o a certs segments de xarxa amb determinat direccionament o a certes aplicacions.
El mòdul d'antimalware ha de disposar d'un motor d'anàlisi estàtic basat en algorismes de Machine Learning que permetin identificar mostres malicioses desconegudes en temps real sense necessitat de haver d'esperar al veredicte del mòdul de Sandboxing.

2.6 Filtratge d'URLs

- Ha de suportar la creació de categories d'URL i la inspecció o no del trànsit xifrat SSL basant-se en aquestes categories. Desxifrat de trànsit SSL i SSH sobre qualsevol port. Capacitat per identificar les aplicacions reals dins dels túnels SSL. Ha de tenir la possibilitat de bloquejar les sessions SSL que no es poden desxifrar o aquelles amb certificats de servidor no fiables.
    - Suport de desxifrat de trànsit TLS1.3 i HTTP/2, incloent un registre dedicat per a aquest trànsit, facilitant així el seu anàlisi.
    - El desxifrat SSL s'ha de fer en maquinari dedicat específicament per a això.
    - Suport de categorització en línia basat en Deep Learning i lliurat des de la núvol
    - Expansió de la inserció de la capçalera HTTP
    - Anàlisi de dominis basat en Machine Learning
    - Motor per a desofuscar java-script
    - Motors d'anàlisi estàtic i dinàmic
    - Anàlisi recursiva de Deep Learning
- Possibilitat de detectar l'enviament de credencials corporatives (usuaris i contrasenyes de la xarxa corporativa) cap als llocs web que es visiten, de manera que es pugui advertir, bloquejar o permetre aquest enviament de credencials en funció de les categories de llocs web visitades.
- Capacitat de realitzar el filtratge per URL o per categoria d'URL. S'oferirà un sistema de filtratge que inclogui la categorització d'URLs per part del fabricant, així com la seva actualització automàtica. S'inclourà també un mecanisme per poder sol·licitar canvis en la categorització de les URLs.
- Possibilitat de configurar el filtre de URL multicategoria, és a dir, categoritzar una URL amb fins a 4 categories basades en el seu contingut, el domini al qual pertany, etc., i així poder establir polítiques que permetin l'accés però limitin les possibilitats de navegació...
- Ha de disposar d'un motor d'anàlisi estàtic basat en algoritmes d'aprenentatge automàtic que sigui capaç de prevenir l'accés a URLs de phishing i la descàrrega de fitxers JavaScript

desconeguts en temps real en el moment que passen pel tallafoc i sense haver d'esperar pel veredicte del mòdul de sandboxing.

2.7 Bloqueig de fitxers i dades sensibles

- Es requereix que els tallafocs tinguin, de manera nativa, capacitat de controlar quin tipus de fitxers circulen per la xarxa, inclosos els fitxers comprimits. La solució ha de diferenciar entre pujades i baixades.
- Capacitat de controlar els fitxers en funció del seu tipus i de pujades i baixades basant-se en el context de l'aplicació (per exemple, no poder pujar fitxers a aplicacions de correu, però sí a aplicacions de compartició de fitxers).
- Es requereix que els tallafocs disposin de la possibilitat de contractar en el futur un servei de DLP en un format de la núvol i que cobreixi el moviment de fitxers a través del tallafocs.
    - El servei DLP ha de disposar d'un punt central d'intel·ligència a la núvol des del qual:
        - S'ha de gestionar l'inventari de documents classificant-los automàticament en funció de la seva tipologia mitjançant algoritmes de machine learning que analitzin patrons basant-se en expressions regulars i en clusterització dels continguts del fitxer.
        - S'han de poder realitzar les accions de resposta necessàries per assegurar que es redueixin al màxim els riscos d'extracció i exposició de les dades:
            - Posar en quarantena el document.
            - Esborrar el document.
            - Eliminar l'enllaç de compartició utilitzat habitualment en serveis SaaS.
            - Notificar al propietari del document quan un dels seus documents incompleixi alguna de les polítiques de DLP.
    - El servei de DLP ha d'estar integrat nativament al firewall sense necessitat de desplegar ni configurar equips addicionals.
    - Suport de DLP basat en fitxers.

2.8 Sandboxing

- Capacitat de detecció de malware desconegut basada en tecnologia de sandboxing a la núvol. Els fitxers desconeguts es identifiquen al tallafocs i s'envien al sistema de detecció de malware a la núvol segons l'aplicació, el tipus de fitxer, la direcció del flux o l'usuari.
    - El sistema d'anàlisi de amenaces a la núvol ha d'estar ubicat a la Unió Europea, i ha d'acreditar el compliment de les normatives europees en matèria de protecció de dades.
    - El sistema de detecció a la núvol ha d'executar el fitxer enviat utilitzant una sandbox virtual per determinar qualsevol comportament maliciós. El sistema també ha de ser capaç de generar signatures automàticament basades en l'activitat observada i distribuir-les als tallafocs.
    - L'administrador del Sistema de Seguretat ha de ser capaç d'accedir a aquesta sandbox per veure l'estat dels fitxers inspeccionats, així com també pujar fitxers manualment a la mateixa.

- S'han d'inspeccionar com a mínim fitxers EXE, DLL, PDF, APK, Java, Office de Microsoft, Mach-O i DMG de OS-X.
- Inspecció de fitxers de script JScript, VBScript i PowerShell Script.
- Gestionar la confidencialitat de manera que sense pujar fitxers a la sandbox, puguem rebre, de manera contínua, les noves defenses.
- La Sandbox ha de disposar de certificacions oficials d'organismes de defensa o països OTAN (SOC2, FedRAMP, ENS nivell alt...).
- Temps de resposta del servei Sandbox màxim de 5 minuts.
- El servei de sandbox ha de proporcionar algoritmes d'anàlisi estàtics dels fitxers executables i scripts de PowerShell utilitzant Machine Learning que permetin donar veredictes en temps real per a la majoria de les mostres desconegudes. Aquest algoritme d'anàlisi estàtic ha d'analitzar patrons en els fitxers com el compressor utilitzat, l'assemblador, entropia, i altres característiques estàtiques del fitxer.

2.9 Seguretat DNS

Capacitat per detectar i prevenir de manera automàtica i dinàmica les sol·licituds DNS malicioses associades amb dominis de malware, a les quals el tallafocs ha de respondre automàticament amb una IP falsa en lloc del servidor autoritatiu (DNS sinkholing). La base de dades de dominis maliciosos ha de ser alimentada per les següents fonts:

- Sistema de sandbox per trobar nous dominis C2.
- DNS passius i telemetries.

El servei que gestioni els veredictes dels dominis DNS ha d'estar a la núvol per assegurar que el nombre de dominis gestionats sigui il·limitat i pugui escalar-se. Aquest servei eliminarà la necessitat de gestionar actualitzacions dinàmiques al tallafocs.
Ha de tenir la capacitat de detectar atacs basats en DNS:

- Atacs que usen Algorismes de Generació de Dominis (DGA)
  - Els DGA són programes integrats en el malware per generar ràpidament quantitats massives de noms de domini que el malware utilitza per rebre instruccions o robar dades (generalment anomenats "comandament i control" o C2).
  - Els atacants utilitzen DGA per poder canviar ràpidament els dominis que estan utilitzant per als atacs de malware. Els atacants fan això perquè el programari de seguretat i els proveïdors actuen ràpidament per bloquejar i eliminar dominis maliciosos que utilitza el malware. Els atacants van desenvolupar DGA específicament per contrarestar aquestes accions.
  - En el passat, els atacants mantenien una llista estàtica de dominis maliciosos; els defensors podien fàcilment prendre aquesta llista i començar a bloquejar i eliminar aquests llocs. En utilitzar un algorisme per construir la llista de dominis, els atacants també fan que sigui més difícil per als defensors saber o predir quins dominis s'utilitzaran que si tinguessin una llista simple de dominis. Per obtenir aquesta llista de dominis que utilitzarà el malware, els defensors han de descodificar l'algorisme, la qual cosa pot ser difícil.
  - Molts DGA estan dissenyats per utilitzar centenars o fins i tot milers de dominis. I aquests dominis solen estar actius només per períodes de temps limitats.
- Atacs que encapsulen tunels de comandament i control en trànsit DNS

    - El trànsit DNS cap a Internet es permet en totes les organitzacions per poder tenir accés a recursos a Internet. Els atacants poden "camuflar-se" junts amb consultes DNS vàlides i amagar les seves accions en petits "fragments" que semblen ser part del flux normal de DNS.
    - Els atacants aconsegueixen dividir les seves instruccions en fragments de mida molt petita que es poden integrar en un trànsit aparentment vàlid. Aquests fragments després es llegeixen al destí i es torna a muntar aquests fragments en una llista completa d'instruccions per a la següent etapa de l'atac.
    - El túnel de DNS també es pot utilitzar per "fragmentar" dades confidencials i extreure-les lentament de l'organització en sol·licituds DNS vàlides, que seran muntades posteriorment al costat de l'atacant.
    - La identificació del túnel DNS requereix inspeccionar el trànsit DNS en temps real amb anàlisi profund.
- Dominis de Retorn (Callback Domains)
    - Malware i dominis C2.
    - Prevenció d'amenaces de DNS en l'ús de servidors intermediaris de xarxes de bots basades en DNS.
    - Dominis de flux ràpid.
    - DGA aleatòris.
    - DGA de diccionari.
        - Detecció i prevenció d'atacs basats en dominis maliciosos que utilitzen paraules conegudes.
- Dominis de Alt Risc (High Risk Domains)
    - Grayware.
    - Dominis registrats recentment.
    - Dominis estacionats.
    - Evitació de servidors intermediaris.
    - DNS dinàmic.
    - Detecció predictiva.
    - Dominis caducats de manera estratègica.
- Atacs als Registres DNS
    - Domain Squatting.
    - Dangling DNS.
    - Zones DNS compromeses.
    - Wildcard DNS.
    - Camuflatge CNAME.
- Atacs basats en el protocol DNS
    - Reversió DNS.
    - Atac NXNS.
- Canals encoberts
    - Tunelització DNS.
    - Tunelització DNS molt lenta.
    - Infiltració de DNS.
    - Detecció i prevenció de tunels C2 basats en DNS amb moviment lent.

Consola d'administració a la núvol navegable on poder visualitzar quadres de comandament amb informació sobre el trànsit DNS, tipus d'atac, freqüència d'accés, context (whois, threat

intelligence...).

2.10 Detecció i Prevenció d'amenaces en dispositius IoT

- S'ha de permetre als tallafocs contractar, en un futur, mitjançant una llicència addicional, una eina que mantingui un inventari, avaluï el risc i controli les amenaces als dispositius IoT a partir del trànsit que es veu als mateixos tallafocs, sense necessitat d'implantar cap altre tipus de sonda o dispositiu.
    - Descobrir un inventari de dispositius IoT instal·lats, identificant el tipus de dispositiu, fabricant i model.
    - Avaluació de riscos de cadascun dels dispositius a partir del comportament que tenen, comparant-lo amb el comportament normal dels mateixos.
    - Detecció de possibles anomalies en el comportament de xarxa dels dispositius a partir d'una línia base de xarxa.
    - Detecció i visibilitat d'amenaces desconegudes als dispositius IoT a partir del seu comportament en xarxa.
    - Prevenció d'amenaces conegudes als dispositius IoT.
    - Possibilitat de crear polítiques als tallafocs utilitzant la informació d'inventari descoberta (tipus de dispositiu, fabricant i model).

3 EXIGÈNCIES DE GESTIÓ I ADMINISTRACIÓ.

Les exigències de gestió de l'equip són:

- Funcionalitats integrades al tallafoc: tant les capacitats de gestió, administració, gestió de registres i informes han de ser components natius al tallafoc, sense necessitat d'adquirir altres elements de maquinari o programari per disposar d'aquestes funcionalitats.
- Auditoria de configuracions, incloent la cerca de diferències entre diferents fitxers de configuració.
- La solució de gestió ha de ser capaç de correlacionar automàticament esdeveniments desconnectats que, quan es reuneixen al llarg d'un període de temps per a un mateix equip o usuari, indiquen que aquest equip ha estat probablement compromès. Per exemple, una vulnerabilitat des d'un kit d'explotació, juntament amb un accés posterior a un domini maliciós que acaba finalment amb una descàrrega de programari maliciós, ha de generar un esdeveniment correlacionat que indiqui el compromís, a més dels tres esdeveniments individuals.
- La solució ha de suportar informes totalment personalitzables per a tots els registres sobre l'equip mateix (sense necessitat, per tant, d'utilitzar un equip secundari per a aquestes tasques).
- Utilitzant les funcionalitats incloses al dispositiu, els administradors han de ser capaços de generar informes personalitzats. A més, ha de ser possible extreure tant els informes predefinits com els personalitzats mitjançant una API XML, que permetrà la integració amb sistemes externs.
- La solució ha de ser capaç de realitzar de manera automàtica una anàlisi del comportament diària, basada en tots els registres, a la recerca d'equips que puguin formar part de botnets desconegudes. El resultat serà un informe que inclourà totes les màquines susceptibles d'haver estat reclutades per a noves botnets, així com els comportaments que han tingut i que les fan considerar infectades.
- Disponibilitat de mapa geogràfic per identificar l'origen i destí dels fluxos i amenaces que entren i surten de la xarxa.
- Capacitat per consumir indicadors de compromís de tercers i incorporar-los automàticament als tallafocs. S'han de poder consumir com a mínim llistes d'IP, URLs i DNS.
- Tant la interfície gràfica com la documentació oficial del producte (guia d'usuari) han d'estar disponibles com a mínim en castellà.
- Eina del fabricant que faciliti la posada en marxa dels següents escenaris:
    - Migració: possibilitat de "traduir" fitxers de configuració de tallafocs Paloalto, Cisco, Checkpoint, Fortinet, Forcepoint, a polítiques de capa 7. Un cop traduïts, podem seleccionar quines polítiques ens interessa exportar al tallafoc.
    - Greenfield: per desplegaments des de zero, deixant inicialment una política de any-any allow i mitjançant mecanismes d'aprenentatge automàtic, identificar totes les aplicacions i proposar polítiques basades en el comportament i ús d'aquestes aplicacions.
- Eina d'optimització de polítiques integrada al tallafoc, de manera que ens guiï i faciliti la millora de les configuracions basades en regles no utilitzades, polítiques a modificar segons l'ús de les aplicacions, etc.

- Poder programar en el temps des de la consola l'enviament de configuracions als tallafocs.
- Actualitzacions automàtiques, programables, per a les signatures d'aplicació, IPS, Antivirus i AntiSpyware.
- Millora de les operacions mitjançant coneixement basat en l'aprenentatge automàtic per a una millor postura de seguretat i per evitar errors humans en la configuració.
    - Prediccions basades en l'aprenentatge automàtic i detecció d'anomalies.
    - Recomanacions de configuració basades en les millors pràctiques.
    - Creació de tiquets de manera automàtica i senzilla.
    - Alertes de manera proactiva sobre l'estat de salut i la seguretat del NGFW.
    - Avís sobre vulnerabilitats conegudes de programari, fi de vida i caducitat de llicències.
    - Visualització i informes sobre l'eficàcia de la seguretat.

4 ALTRES REQUERIMENTS

- Per complir amb els requeriments del “Esquema Nacional de Seguridad (ENS)” el fabricant ha de tenir publicades les guies de configuració recomanades pel Centro Criptológico de Seguridad, CCN-STIC.

- Per complir amb els requeriments del “Esquema Nacional de Seguridad (ENS)”, el producte ofertat ha de figurar en el Catàleg de Productes de Seguretat TIC, CPSTIC, recomanats pel Centro Criptológico Nacional.

- La solució proposada ha de disposar de mecanismes que injectin automàticament, en els firewalls, llistes dinàmiques provinents de bases de dades de tercers (per exemple, serveis anti-phishing, llistes de dominis maliciosos, serveis antispam, serveis d'identificació de nodes TOR, avisos de CERTs, etc.). Aquestes fonts han de ser rebudes de manera automàtica, processades i injectades en els firewalls a través de STIX, TAXI, JSON, llistes dinàmiques, etc., sense intervenció humana.

5 SERVEIS PROFESSIONALS DE MIGRACIÓ

A continuació, es detallen els serveis professionals que s'han d'incloure a la proposta:

5.1 Gestió de projecte

Fase del projecte que s'encarregarà de gestionar el propi projecte a nivell alt, incloent totes aquelles tasques necessàries perquè el projecte sigui un èxit.

- Reunió de Kickoff: presentació de l'equip de treball, revisió de l'abast del projecte, requeriments per ambdues parts.
- Gestió logística d'equips.
- Comunicacions periòdiques amb CCSPT: comunicacions puntuals entre el proveïdor i CCSPT per al correcte desenvolupament de les diferents tasques i perquè el projecte sigui exitós.
- Reunió de tancament: revisió del projecte una vegada tancat, traspàs a operacions i comentar punts importants vistos durant el projecte (si n'hi hagués).

5.2 Fase de Definició

Fase del projecte que s'encarregarà de definir tots aquells documents i/o configuracions necessàries, de manera teòrica.

- Recopilació i anàlisi d'informació sobre els equips (exportació de la informació dels equips a migrar, recopilació d'informació d'equips de l'entorn, etc.)
- Configuració IP bàsica i importació de configuració existent.
- Elaboració de pla de marxa enrere.
- Elaboració de pla de proves juntament amb el client.

5.3 Fase de Staging

Fase del projecte que es centrarà en l'acondicionament dels diferents equips de xarxa a desplegar, incloent la càrrega de la configuració dels nous equips. Aquesta fase es realitzarà a les dependències del proveïdor.

- Recepció d'equips i comprovacions de maquinari.
- Actualització de software a l'última versió estable dels nous equips.
- Adaptació i càrrega de la configuració dels actuals equips als nous.
- Verificació de la configuració de l'equip.
- Enviament dels diferents equips a les dependències de CSPT, on aniran instal·lats els nous equips.

5.4 Fase de Migració

Fase del projecte que es centrarà en la posada en producció dels nous equips i en totes aquelles tasques necessàries per la correcta migració dels firewalls actuals PaloAlto.

- Execució de pla de test abans de la migració dels equips, per determinar el bon funcionament de la xarxa i poder descartar possibles errors durant la migració.
- Instal·lació dels equips en paral·lel amb els equips actuals.
- Migració del servei des del Firewalls actuals PaloAlto cap als nous equips.

- Execució de pla de test un cop migrats els equips.
- Babysitting: suport durant el següent matí laborable per a la resolució de possibles problemes no contemplats.

5.5 Fase de Pilot - Desencriptació tràfic SSL

Es realitzarà un pilot per a la desencriptació d'una part del tràfic del CCSPT a mode de prova, i amb la finalitat de mostrar al CCSPT com es realitza aquesta configuració. L'objectiu és que el CCSPT sigui autosuficient perquè pugui implementar SSL Decrypt sobre diferents fluxos de tràfic.

- Definició de perfils i polítiques per a la realització de SSL Decrypt.
- Proves de desencriptació de tràfic SSL. Estudi del rendiment dels equips.

5.6 Fase de Tancament

Fase del projecte que donarà tancament al projecte, una vegada la migració dels firewalls sigui un èxit.

- Documentació del projecte: redacció de documentació bàsica de final de projecte.
- Traspàs a Operacions: activació dels contractes de suport dels nous equips.

5.7 Assumpcions i Consideracions

A continuació, es detallen totes aquelles assumpcions, condicions i consideracions que afecten les diferents tasques del projecte:

Totes les tasques de subministrament i migració (substitució dels firewalls actuals) es realitzaran en horari laboral, llevat de la referent a la posada en producció dels nous Firewalls i substitució dels Firewalls actuals, que es planificarà de manera conjunta entre el proveïdor i el CCSPT en un horari de mínima afectació al servei.
No cal incloure el subministrament de cap tipus de petit material passiu.
No es realitzaran configuracions noves sobre cap equip, llevat de les indicades en els apartats anteriors.