FGC
Ferrocarrils
de la Generalitat
de Catalunya

Subministrament per la renovació dels tallafocs d'aplicació de FGC i posada en servei

Especificació tècnica

Àrea de Ciberseguretat
Tecnologies de la Informació i les Comunicacions

Agost 2024

Índex

Introducció

Ferrocarrils de la Generalitat de Catalunya (FGC), disposa d'una ampli número d'aplicacions que es publiquen a internet, indispensables per oferir serveis necessaris tan operatius com corporatius i que cal protegir adequadament.

FGC, per tal de mantenir una adequada seguretat, control i publicació dels serveis, disposa d'equipament físic de tallafocs d'aplicació del fabricant F5 Big IP (2 equips). Aquest equipament permet la detecció i neutralització d'intrusions i la protecció de totes les aplicacions publicades així com el control d'aquestes.

Objecte

El que es pretén amb aquesta licitació és la renovació tecnològica dels 2 equips, així com la millora de prestacions i tenir tot el llicenciament de seguretat nou durant el període d'execució del contracte. Per aquest motiu, és fa necessària la compra de nou equipament físic de tallafocs per a mantenir la seguretat detallada anteriorment.

Requeriments dels equips sol·licitats

Generals

La solució completa està formada per 2 tallafocs que formen 1 clúster, administrats seran administrats per una consola centralitzada.

El fabricant dels equips tallafocs oferts haurà de ser F5 Big IP, donat que els equips actuals ho son i això ens permet simplificar el procés de migració i posada en servei, així com aprofitar els coneixements i formacions ja adquirits pels equips d'administració d'aquests.

La proposta haurà d'incloure durant la totalitat de la duració del contracte, així com les possibles pròrrogues, totes les llicències i subscripcions necessàries per activar, en el cas que sigui necessari, totes les funcionalitats associades als requeriments obligatoris que es llisten a continuació. També s'haurà d'incloure el manteniment dels equips durant tota la durada del contracte.

Els equips tallafocs han de ser en format appliance virtual. Appliance virtual compatible amb Vmware ESX, així com entorns de cloud pública como AWS, Azure y Google Cloud Platform

La solució ha d'incloure funcionalitats actuals de manera perpetua com a mínim de:

- Anti-Virus Checks
- Base Endpoint Security Checks
- Firewall Checks
- Network Access
- Secure Virtual Keyboard
- APM, Web Application
- Machine Certificate Checks
- Protected Workspace
- Remote Desktop
- App Tunnel
- Rate Shaping
- SDN Services, VE
- Routing Bundle, VE
- ASM, VE
- Acceleration Manager, VE
- Max Compression, VE
- AFM, VE
- DNS-GTM, Base, 200M
- IPV6 Gateway
- Ram Cache
- SSL, VE
- DNS Rate Limit, 1000 QPS

- GTM Rate, 1000
- VE, Carrier Grade NAT (AFM ONLY)
- PSM, VE
- DNSSEC
- Advanced Protocols, VE
- Anti-Bot Mobile, VE 200 Mbps
- App Mode (TMSH Only, No Root/Bash)
- ASM to AWF Upgrade, VE-200M
- Best, 200 Mbps -1 Gbps Upgrade
- BIG-IP VE, Multicast Routing
- Concurrent Users and Access Sessions, VE
- Crytpo Offload, VE, Tier 1 (25M - 200M)
- DNS and GTM (250 QPS), VE
- External Interface and Network HSM, VE
- FIPS 140-2 Level 1, BIG-IP VE-200M
- Intrusion Prevention System, VE-200M
- IP Intelligence, 1Yr, VE
- IP Intelligence, 1Yr, VE-200M/VE-25M
- IP Intelligence, 3Yr, VE
- IP Intelligence, 3Yr, VE-200M/VE-25M
- PEM URL Filtering, 1Yr, 200Mbps
- PEM URL Filtering, 1Yr, VE-10M LAB, 200M
- PEM URL Filtering, 3Yr, 200Mbps
- PEM URL Filtering, 3Yr, VE-10M LAB, 200M
- PEM, ADD-VE, 200M
- PEM, Quota Management, VE
- Secure Web Gateway, 1Yr, VE
- Secure Web Gateway, 3Yr, VE
- Secure Web Gateway, VE-25M-1G, 500 Sessions, 1Yr
- Secure Web Gateway, VE-25M-1G, 500 Sessions, 3Yr
- SSL Orchestrator, VE (25MB/200MB/1G)
- SSL, Forward Proxy, VE
- URL Filtering, 1Yr, VE
- URL Filtering, 3Yr, VE
- URL Filtering, VE-25M-1G, 500 Sessions, 1Yr
- URL Filtering, VE-25M-1G, 500 Sessions, 3Yr
- VPN Users

Totes aquestes funcionalitats han d'estar llicenciades de manera perpetua.

La pròpia plataforma ha de tenir connectors automàtics amb l'objectiu d'integrar-se amb identitats terceres i poder recollir informació, adreçament ip, inventari d'objectes i etiquetes. També ha de poder enviar els logs en els diferents formats mes coneguts per a integrar-se amb sistemes de recollida i correlació de logs més comuns al mercat.

La solució ha de mantenir la alta disponibilitat i sempre ha de poder estar en funcionament un dels dos equips.

La mateixa solució de seguretat ha de permetre la creació d'automatismes per tal de:

- Poder treballar en mode automàtic per a poder aprendre les característiques de les aplicacions a protegir i establir un perfil de seguretat a aplicar.

- Bloquejar de manera automàtica qualsevol atac a les aplicacions tenint en compte firmes i comportaments.

Plataforma i Rendiment

Els equips tallafocs tindran un sistema operatiu de propòsit específic i no d'ús genèric. Es requereix un sistema operatiu de 64 bits desenvolupat i mantingut pel fabricant per a propòsit de gestió avançada de tràfic amb capacitats de Full-Proxy i manipulació del tràfic en tots els nivells de la capa OSI.

Els equips han de ser en format appliance virtual compatible amb VmWare ESX, així como entorns de cloud publica como AWS, Azure i Google Cloud Platform.

A nivell 4, l'equip ha de disposar d'un rendiment com a mínim de:

- 200Mbps de Throughput L4

- Capacitat de fins 40k de HTTP Request L4 por segons

- 20k connexions L4 por segons

- Fins 1M connexions concurrents L4

A nivell 7, l'equip ha de disposar d'un rendiment com a mínim de:

- 200Mbps Throughput L7

- 16k Connexions L7 por segons (cps) (1-1)

- 25k Requests per segon (rps) (1-inf)

- 40k Requests per segon (rps) (inf-inf)

Respecte a capacitats i rendiment del tràfic xifrat, la solució ha de permetre:

- Capacitat per a configurar l'equip per tasques de xifrat/desxifrat, de forma independent entre client i servidor, permetent offload del tràfic SSL o modificar el tipus de xifrat i certificats presentats entre la part client i servidor, permetent totes las configuracions independents entre el costat client (xifrat/en clar) y el costat servidor (xifrat/en clar).
- Suport de claus de 4096 bits, implementació de xifrat Diffie-Hellman, suport de xifrat el·líptic (ECC), capacitat de xifrat selectiu de contingut en L7, suport de la RFC 5077
- Suport a protecció en front a atacs SSL y control de renegociació de la clau de sessió d'usuari.

- Suport per la presentació de diferents certificats per servei (IP/port) mitjançant la inspecció del campo SNI
- Suport a la presentació de diferents certificats per servei (IP/port) mitjançant programació avançada per scripting en TCL
- 3000 SSL/TLS TPS (RSA 2K Keys) incloses
- Capacitat per fins 900 SSL/TLS TPS (RSA 2K Keys)
- Fins 200k sessions concurrents SSL
- 175Mbps de xifrat SSL bulk
- Capacitat per offloading de l'establiment de sessió xifrada a un equipo físic per redir la carga de CPU en la gestió de tràfic SSL
- La solució ha de suportar AES, AES-GCM, SHA1/MD5 i algoritmes de clau pública: RSA, Diffie-Hellman, Digital Signature Algorithm (DSA) y Elliptic curve cryptography (ECC), ECDHE, DHE, Ciphers Camellia, TLS1.2, tant del costar client com servidor.
- Capacitat d'integració amb dispositius HSM externs (mínim Thales nShield i Gemalto (SafeNet) Luna Safe).

Respecte a l'optimització de tràfic la solució ha de complir mínimament:

- Capacitat d'acceleració d'aplicació a nivell:
  Memòria cache
  Compressió de tràfic http
  Optimització de tràfic TCP

- Capacitat d'emmagatzemament d'objectes comprimits, cache http.

- Capacitats per integrar funcionalitats antifrau, amb detecció de malware sobre los dispositius que es connecten al servei, detecció de phising i xifrat de la capa d'aplicació de forma transparent a l'aplicació i al client.

- Ha de permetre comprimir tràfic http a través del estàndard GZIP i compatible amb els navegadors mes comuns (MS Internet Explorer, Google Chrome, Mozilla Firefox, Safari, etc).

- Ha de suportar el protocol HTTP 2.0 i funcionar com Gateway HTTP 2.0 tot i que els servidors web no ho suportin, actuant como HTTP2 Gateway a HTTP1.1

- La solució ha de poder oferir "Content Spooling" per optimitzar la comunicació amb qualsevol terminal, permetent que el servidor enviï les dades a una tassa òptima, mentre que l'usuari pugui rebre les dades a la tassa de transferència que necessiti.

- S'ha de suportar i incloure la Geolocalització d'adreces IP per prendre decisions de gestió del tràfic en base a aquest paràmetre.

La solució ha de suportar scripts de programació basats en llenguatge scripting estructurat (TCL) que permeti crear funcionalitats que per defecte no estan al

menú de configuració/opcions i ha de poder suportar creació de procediments o funciones que poden ser utilitzades per a qualsevol altre script.

El sistema ha de suportar programació i ampliació de funcionalitat mitjançant node.js, ampliant capacitats de scripting amb la inclusió de llibreries de node.js que permetin connectivitat amb altres sistemes (p.e. connectivitat amb base de dades).

S'ha de poder gestionar l'ample de banda. S'ha de poder definir polítiques de "Rate Shaping" per servei, por VLAN i per contexts, podent establir amples de banda mínims assegurats i possibilitat de creixement en cas de ser necessari.

La solució ha de ser compatible amb tràfico IPSEC i ser certificat com dispositiu IPSEC 1.3

La solució ha d'optimitzar el tràfic a nivell TCP, mitjançant tècniques que permetin modificar l'stack TCP optimitzat que es faci servir cap al costat client i servidor.

Optimització automàtica del perfil TCP a aplicar a la comunicació y auto-configuració de buffers

Administració de la solució

La solució ha de permetre com a mínim les següents capacitats d'administració:

Capacitat de creació de configuracions que no se apliquin sobre el tràfic fins que es confirmin els canvis.

Capacitat de modificació de la configuració d'un equipo del clúster amb rèplica automàtica als nodes secundaris.

Capacitat de modificació de la configuració en un equip del clúster sense que es propaguin canvis a l'equip passiu (o viceversa) fins la confirmació manual d'aquest canvis, permetent roll back de les configuracions.

La solució ha de poder desplegar aplicacions de manera automàtica desplegament d'aplicacions mitjançant plantilles personalitzables, i que es puguin invocar via REST-API (mínim serveis de Microsoft: Exchange, Sharepoint, Lync, federació amb o365, etc.)

La solució de ha d'integrar-se amb Directori Actiu Windows 2008R2 o superior, LDAP, RADIUS.

La solució he de permetre la comunicació xifrada i autenticació d'accés al equipo d'usuaris admins amb certificats digitals.

El reportin de la solució ha de permetre com a mínim enviament d'alertes i events a un sistema centralitzat o SIEM, mitjançant:

- Protocol SysLog
- Notificació via SMTP

- SNMP versión.2.0 o superior

La solució ha de permetre mantenir dos o mes versions del sistema operatiu instal·lat per poder fer rollback ràpid si no ha anat be un Update o migració de versió.

La solució ha de permetre una consola centralitzada per a poder administrar i gestionar múltiples dispositius i serveis.

La solució ha d'incorporar eina o eines de diagnòstic de problemes, anàlisi de configuracions que permeti diagnosi de l'estat dels equips en servei, indicant recomanació

La configuració del dispositiu ha d'estar protegida i xifrada per a poder protegir l'accés a informació sensible o critica.

La solució ha de permetre desplegar diversos entorns de Routing independents (>4000) amb capacitat de solapament ip i taules de Routing independents. De la mateixa manera ha de permetre desplegar un numero similar al citat, d'entorns d'administració independents (amb diferents administradors i rols).

Pel que fa a capacitats de reporting, cal que la solució disposi com a mínim:

- Ha de disposar d'un mòdul de reporting amb Drill Down que permeti visualització gràfica de l'estat de seguretat i el comportament d'aplicacions HTTP, latències cap als servers, latències d'URLs, Direccions IPs que accedeixen a aplicacions, URLs mes visitats en las aplicacions, Throughput cap als servidores i estadístiques de serveis i servidors físics.

- S'ha de poder permetre definir umbrals de alerta segons paràmetres de trafico així com activació automàtica de mesures correctives automàtiques i enviament d'alertes via SNMP/email/syslog.

  Creació d'estadístiques personalitzades ad-hoc.

Suport de fabricant

Els equips han de contar amb suport tècnic avançat de fabricant en caso d' incidències en formato 8x5, ha d'incloure accés cmdb de coneixements , accés a serveis de suport, actualitzacions de software y firmware, suport proactiu per actualitzacions o modificacions planificades, i suport per a configuració i programació de srcipts als equips.

Integració amb la xarxa

Suport VLAN 802.1q, Vlan tagging
Suport de 802.3ad

Suport de NAT, SNAT
Suport de IPv6: L'equip ha de funcionar com a Gateway entre xarxes IPv6 e IPv4 permetent tenir ambos tipus de xarxes en paral·lel.
Suport de Rate Shapping.
Suport de dominis d'enrutament, amb Default Gateway propi i connectats a xarxes IP amb igual adreçament.
Suport VXLAN, VXLAN Gateway, NVGRE y Transparent Ethernet Bridging per entorn de xarxa virtualitzats.
Suport de protocols de routing dinàmic RIP, BGP, OSPF
Ha de permetre anunciar serveis i aplicacions aprovisionades per routing dinàmic en funció de disponibilitat.
Suport a IPSEC certificat.
Suport per a marcat de Type of Service (TOS), DSCP y 802.1p VLAN 802.1q, Vlan tagging.

Elements de seguretat
Les característiques mínimes del elements de seguretat principals per a la protecció i securització d'aplicacions ha de ser:

Balanceig i gestió del tràfic:

- Capacitat de caching en RAM per accelerar entrega de continguts.
- La solució ha de permetre funcions de balanceig de tràfic d'aplicacions basades en TCP/UDP, inclosos serveis web.
- La solució ha de permetre definicions d'IP/Port virtual per la prestació de servei, ha de permetre que es gestioni mitjançant una granja de servidores identificats amb adreça IP/Port del servei igual o diferent del publicat.
- La solució ha de tenir arquitectura Full-Proxy, control de entrada i sortida de connexions fent distinció de les connexions del costat client i servidor.
- La solució ha de permetre fer el control del balanceig de tràfic segons es defineixi segons algoritmes de balanceig com:
    - · Round Robin
    - · Rati
    - · Rati dinàmic
    - · Resposta ràpida
    - · Connexions mínimes
    - · Anàlisis de carrega
    - · Menor número de sessions
    - · Balanceig personalitzat mitjançant llenguatge de programació
- La solució ha de poder identificar fallades de servei per a redundància d'aplicacions. Ha d'incloure monitoreig avançat de serveis analitzant respostes de servidor a peticions concretes i capacitat per integrar múltiples monitors per identificar fallades dels components aplicatiu/servidor.

- Ha de suportar a modificació de la capçalera o contingut en el payload (funció de Proxyinverso). També s'ha de suportar reescriptures de Url y Uri incloses en el GUI de configuració.

- La solució ha de permetre la gestió del tràfic MQTT (3.1/3.1.1) per poder aplicar polítiques específiques i gestió de tràfic de entorns IoT, permetent tenir visibilitat dels diferents paràmetres de la conversació MQTT, como tòpics, identificació de client, gestió del tràfic xifrat, logging i/o autenticació de los clients per certificat.

- Ha de ser possible modificar el contingut HTML utilitzant objectes de configuració (sense scripts).

Firewall de xarxa:

El funcionament de Firewall de xarxa ha de permetre com a mínim:

- Protecció contra atacs de DDoS en capes 2-4 fent servir vectors d'atac personalitzables.
- Bloqueig d'atacs a nivell de xarxa com flood, sweep, teardrop, smurf attacks, entre altres.
- Mitigar atacs basats en protocols, inclosos SYN, ICMP, ACK, UDP, TCP, IP, DNS, ICMP, ARP.
- Suportar de manera opcional un sistema de suscripció de reputació IP per prevenir connexions bidireccionals (entrants i sortints) a direccions IP no confiables i categoritzades.
- Creació de regles basades en aplicació, independents per cada una d'elles.
- Creació de regles globals.
- Creació de regles diferents aplicables en cada domini de routing independentment.
- Permetre la creació de polítiques en staging per avaluar en paral·lel a la política activa per observar resultats en logs sense modificació del tràfic.
- Facilitar la gestió automàtica e informe sobre consistència de la política de firewall identificant regles redundants o solapades.
- Funcionar com un firewall statefull full-proxy i que este certificat com Network Firewall
- Permetre la definició d'horaris (schedules) que apliquin a les regles configurades, permetent activar regles:

    - Entre intervals de temps.
    - Fins una data.
    - Després d'una data.

- Gestionar i aplicar regles en base a Geolocalització d'adreces IP.

- Creació de llistes blanques d'adreces IP.
- Configuració de túnels IPSEC Site-to-Site i accés VPN d'usuaris.
- Protecció contra Ataques de Denegació de Servicio pel protocol DNS, poder controlar tràfic DNS segons el tipus de registre sol·licitat i detectar anomalies a nivell del protocol.
- Protecció contra Ataques de Denegació de Servei pel protocol SIP i poder controlar el tràfic SIP segons el mètode SIP rebut i detectar anomalies a nivell de protocol.
- Exportar els logs a un repositori Syslog extern.
- Integrar amb una consola centralitzada per la gestió de polítiques entre múltiples dispositius.
- L'equip ha d'estar certificat com firewall de xarxa.
- Bloquejar IPs malicioses per evitar l'entrada en la xarxa quan es detectin activitats il·licites d'una IP concreta.
- Generar línies base per la detecció automàtica de situacions de DDoS.
- Funcionament en mode TAP/mirroring, amb una copia unica del tràfic.
- Detectar atacs per comportament, generar firmes dinàmiques de l'atac i mitigar.
- Inspecció profunda de protocols amb capacitat d'us com a IPS.
- Realitzar dashboards de detecció i mitigació d'atacs amb drill down, classificació d'aquest en funció d'origen, geolocalització, protocol, destí, servei, etc.

Autenticació, control d'accés i SSO

El funcionament a nivell d'autenticació i control d'accés ha de permetre com a mínim:

- Implementació de VPN SSL y autenticació avançada.
- Mode "Portal" on la maquina es comporti com proxy revers, presentant el contingut de portals interns i presentant-los com a vincles segurs a l'usuari.
- Proporcionar acces remoto seguro a toda la xarxa per a qualsevol aplicació basada en IP (TCP o UDP).
- Split Tunnel, el tràfic especificat ha d'anar únicament per VPN.
- Túnels d aplicació, només una aplicació en particular te accés a recursos interns.
- Compressió HTTP
- Establiment de connexió segura per l'accés remot sense la necessitat d'instal·lar software de client en l'equip de l'usuari.
- Transport segur amb encapsulament DTLS (Datagrames TLS).
- Presentar en una única IP, múltiples serveis d'accés, amb capacitat de personalització total.
- Single-Sign-On (SSO), adaptant la autenticació de forma diferent del costat client i del cosatat servidor.

- Sol·licitud de credencials d'usuari una vegada, i autenticar a l'usuari en tots els portals que requereixin autenticació.
- Validació de l'equip d'usuari. Ha de poder validar com a minim:
    - Presencia d'anti-virus i que estigui actualitzat.
    - Presencia de Firewall personal.
    - Presencia de processos executant-se en el equipo.
    - Presencia de certificats digitals instal·lats en l'equip.
    - Presencia d'arxius en l'equip.
    - Entrades de registre en clientes Windows.
    - Verificació de Sistema Operatiu.
    - Identificació de hardware de l'equip.
- Accés remot SSL-VPN clientless dels clientes mitjançant Edge, Chrome, Firefox, Safari tant per SSOO windows como IOS/Linux.
- Inspecció de los clients quan es connecten amb Edge, Chrome, Firefox, Safari tant per SSOO windows como IOS/Linux..
- Permetre autenticació d'usuaris contra sistemes LDAP, LDAPS, RADIUS, TACACS+, Directori Activo, etc.
- Integració amb múltiples factors d'autenticació que fa servir tokens de hardware o software.
- Us de client stand-alone inclòs amb la solució, per equips Windows, Android, Linux, iOS..
- Us de Single-Sign-On utilizant Security Assertion Markup Language (SAML) 2.0 funcionant com identity provider (IdP) i/o service provider (SP).
- Integració amb VMware Horizon funcionant com proxy PCOIP.
- Suport per Oauth 2.0 per la integració amb serveis externs de autenticació o proveir federació d'accessos amb tercers.
- Autenticació mitjançant JSON Web Token (JWT) amb Oauth, en rols d'OAuth Authorization o Client o Resource Server, (RFC 7519), JWK (RFC 7517), signat de JWS (RFC 7515), amb integració amb Azure AD, ADFS, Amazon o Google.
- Capacitat per sol·licitar mesures addicionals de seguretat per a URLs concretes, de manera que tinguin requeriments de seguretat diferenciats per URL tot i que l'usuari ja estigui autenticat.
- Integrar el seu propi mecanisme de doble factor de autenticació (tokens).
- Integració amb sistemes MDM, incluyendo Airwatch i MS Intune, entre altres.
- Permetre publicació nativa del protocol RDP per la publicació de serveis RemoteApp de Microsoft.
- Soportar Google reCAPTCHA v2.
- Poder fer SSO multi-domini.

- Permetre presentar múltiples portals i política d'autenticació en una única IP/port de servei, aplicant una política o altre segons URL/hostname/SNI i altres.
- Integració amb eina de gestió de gestió centralitzada pe la visibilitat, reporting i gestió de polítiques des d'un element central de múltiples dispositius.
- Proxificar l'Active Directory Federation Services 3.0 & 4.0 (certificació MS per Proxy Integration Protocol (PIP)), ha de tenir capacitat per alterar les funcionalitats de Proxy de Microsoft WAP, securització del accés a Office 365, MFA i escalat de MS ADFS.
- Integració amb vmware workspace ONE amb suport per ViDM i SSO.

WAF

Pel que fa al funcionament de Firewall d'aplicacions, protegint i securitzant la publicació d'aplicacions, la solució ha de permetre com a mínim:

- Treballar com a Proxy TCP invers i/o transparent. Ha de poder treballar en mode TAP o sniffer, rebent copia única del tràfic de les aplicacions.
- Creació automàtica de polítiques. Aquesta creació automàtica, haurà d'unificar múltiples URLs explícites utilitzant wildcards amb l'objectiu de reduir la quantitat d'objectes en la configuració.
- Treballar en mode bloqueig o en modo anàlisi (transparent/informatiu).
- Diferents polítiques per diferents aplicacions amb mecanismes d'autoaprenentatge, amb diferents mètriques d'aprenentatge basat en la confiabilitat d'Ips de origen de las peticiones.
- Crear signatures de seguretat personalitzades.
- Treballar amb models de seguretat positiva y negativa.
- Aprendre del comportament de les aplicacions sense intervenció humana. Aquest aprenentatge s'ha de poder passar a regla de seguretat.
- Permetre la personalització de les pàgines de bloqueig incloent la capacitat de respondre a webservices amb codi HTTP 500. S'han de poder crear respostes diferents personalitzades per a pàgines de login, XML, Ajax, cookies, Captcha, interacció amb aplicacions mòbils i HoneyPots.
- Prevenir exposar el "OS fingerprinting"
- Integració amb eines de verificació de vulnerabilitats.
- Aniuat de polítiques de nivell 7 mitjançant mecanismes multicapa.
- Protecció a Web Services XML y restringir el accés a mètodes definits via Web Services Description Language (WSDL)
- Suportar formato swagger (OpenAPI) para la definició de protecció d'API´s.
- Restringir el número de crides per endpoint i client.
- Protección contra el Top 10 d'ataques definits en OWASP

- Protegir contra Web Scraping
- Session-aware, es ha dir cal que s'identifqui i es forci a que l'usuari sempre tingui sessió.
- Verificar les signatures d'atacs en les respostes del servidor cap a l'usuari.
- Emmascarar informació sensible filtrada por el servidor.
- Bloqueigs de tràfic basat en la ubicació geogràfica.
- Integració amb servidors d'antivirus mitjançant el protocol ICAP
- Protecció contra atacs DoS /DDoS de Capa 7. Mitjançant establiment de mesures de seguretat i challenges al client per identificar-lo. Les mesures a establir com a mínim son:

    - Revisió d'activitat del client

    - Challenges javascript

    - Challenges CAPTCHA

- Protecció contra atacs DoS /DDoS de Capa 7. Mitjançant la detecció de comportament d'atacants i establint signatures dinàmiques de comportament per a mitigació automàtica.
- Protecció contra atacs DoS /DDoS de Capa 7. Mitjançant anàlisis de uso/abuso del servei fent servir establiment automàtic d'umbrals de transaccions per segons des d'una IP origen, geolocalització, latència en les aplicacions, etc.
- Protecció contra atacs DoS /DDoS de Capa 7. Mitjançant del temps de resposta dels servidores.
- Identificar usuaris i atacants mitjançat la identificació del client (browser) de forma única, distingint diferents usuaris tot i accedir per la mateixa IP (NAT o proxy).
- Poder descartar tots els paques que provinguin d'una IP sospitosa un cop detectat l'atac.
- Poder realitzar captures tcpdump un cop s'ha detectat un atac i esta en curs.
- Suportar tecnologías AJAX y JSON.
- La protecció mínima que ha de garantir la solució:

    - Atacs de Força Bruta

    - Cross-site scripting (XSS)

    - Cross Site Request Forgery

    - SQL injection

    - Parameter and HPP tampering

    - Sensitive information leakage

    - Session highjacking

    - Buffer overflows

    - Cookie manipulation
    - Various encoding attacks
    - Broken access control
    - Forceful browsing
    - Hidden fields manipulation
    - Request smuggling
    - XML bombs/DoS
    - Open Redirect

- Protecció de serveis Websocket, amb inspecció de signatures sobre el contingut i detecció a la capa de websocket.
- Verificar la seguretat i validació a protocols FTP y SMTP
- Comparació de polítiques definides i mostrar diferencies entre ambdues.
- Suportar integració de bases de dades d'intel·ligència i reputació d'IPs que permetin blocar el tràfic segons categories com:
    - Scanners
    - Exploits Windows
    - Denial of Service
    - Proxies de Phishing
    - Botnets
    - Proxies anónims
- Xifrat criptogràfic de les cookies para verificar integritat.
- Enviament de logs en formato personalitzat per TCP o UDP.
- Actualitzacions automàtiques de signatures.
- Evitar fuites d'informació amb l'anàlisi de les respostes del servidor.
- Detecció de BOTS basats en signatures. Detecció de BOTS tot i que puguin executar javascript.
- Protecció anti bots en serveis basats en l'intercanvi de fitxers JSON, tot i que no permetin injecció de javascript.
- Soporte de protección anti-bot para la aplicaciones móviles que no soporten javascript
- La solució ha ser capaç d'identificar dispositius mitjançant ID.
- Protegir davant de les OWASP Automated Threats mediante la configuración de microservicios.
- Suportar aplicacions "single-page".
- La protecció de Bots ha de ser capaç de visualitzar el detall del tràfic de Bots rebut globalment i per servei.
- Proporcionar protecció des del navegador fins a l'aplicació amb xifrat d'informacio a capa 7.

- El seguiment dels diferents monitors com, FTP, Gateway ICMP, HTTP, HTTPS, ICMP, SOAP, TCP, TCP Half Open, UDP.
- Suportar les aplicacions següents: HTTP, HTTP Compression, Web Acceleration, FTP, TFTP, DNS, ICAP, Request Adapt, Response Adapt, Diameter, DHCPv4, DHCPv6, Radius, SMTP, SMTPS, Client LDAP, Server LDAP, iSession, Rewrite, XML,SOCKS, FIX, GTP, Websocket, PPTP, IPsecALG, Netflow
- Suportar HTTP2 de manera nativa

Requeriments de la instal·lació i posada en marxa dels equips

La solució proposada haurà de constar de 2 equips instal·lats a l'entorn virtual, que hauran de treballar en clúster actiu passiu per donar alta disponibilitat a tota la solució.

Els equips cal que tinguin manteniment del fabricant durant la durada del contracte.

El projecte (instal·lació i posada en marxa dels nous equips) ha de ser "claus en mà":

- Subministrament i instal·lació de tot el maquinari requerit, realitzar la instal·lació i configuració adient de tot el programari necessari.

- S'hauran d'incloure totes les llicencies per complir els requeriment definits al llarg d'aquest document així com el suport del fabricant pel període de durada del contracte.

- S'ha de tenir en compte que tot l'entorn comentat en aquesta licitació, esta en producció i l'adjudicatari haurà de garantir que durant la durada de la migració d'equipaments, no es perd el servei, ni es rebaixa en cap moment el nivell de seguretat aplicada.

- S'haurà de realitzar una auditoria de la situació actual per dimensionar i avaluar la planificació del projecte que serà presentada a FGC. Aquesta haurà d'incloure:

    - Estat actual (arquitectura, seguretat, polítiques, etc.)
    - Pla d'actuació (tenint en compte que actualment esta en producció tot l'entorn objecte de millora definit en aquest plec).
    - Pla de possibles millores
    - Pla d'activitats a realitzar

- El licitador haurà de garantir el correcte funcionament de la xarxa amb la solució hardware proposada.

- S'hauran d'efectuar proves/demostracions de funcionament, rendiment i operativitat per tal de poder validar l'acceptació de la instal·lació.

- El projecte s'entregarà a punt per operar-lo. S'entregarà un guia operativa amb tot el que s'ha realitzat i l'estat actual de configuració i seguretat.

- S’haurà de realitzar una fase de formació i traspàs de coneixements si han hagut canvis significatius en la nova implantació.

- S’entregarà documentació complerta de tot el projecte (arquitectura dissenyada, implementació feta, configuració detallada realitzada als equips, regles de seguretat aplicades, etc.).

- El projecte d’instal·lació i posada en marxa s’executarà en un període estimat màxim d’uns 3 mesos seguint aquest Planning:
  - Fase 1: Anàlisis de l’arquitectura actual
    Disseny i planificació
  - Fase 2: Instal·lació i preparació d’equips
    Configuració de la nova plataforma
  - Fase 3: Migració de la configuració a la nova plataforma
    Adaptació i fine tunning de la configuració
    Proves i validacions de la nova plataforma
  - Fase 4: Posada en producció. L’adjudicatari farà les actuacions i intervencions necessàries per fer la instal·lació i posada en servei del nou equipament, tenint en compte que l’entorn esta en producció i ha d’haver el menor impacte possible. S’haurà de presentar un pla d’actuació i s’haurà de validar per FGC.
    La Fase 4 no quedarà tancada fins que FGC no doni el vist i plau de que es compleixen els requeriments necessaris.
  - Fase 5: Suport a la implantació
    Implantació de les millores
  - Fase 6: Entrega de documentació i tancament del projecte. FGC haurà d’acceptar la documentació entregada.

Requeriments de suport

L'adjudicatari, donarà un suport especialitzat que contemplarà coma mínim les següents tasques durant tota la durada del contracte:

Resoldre consultes o incidents relacionats amb l'operació i administració dels dispositius de seguretat subministrats que puguin sorgir. S'haurà d'ajudar a resoldre dubtes d'administració sobre les funcionalitat dels equips objecte d'aquest contracte, així com donar suport necessari en cas d'incidència que requereixi coneixement expert sobre la tecnologia i/o el fabricant.

Donar suport, resoldre dubtes i aconsellar en les tasques de manteniment i actualitzacions a realitzar als equips.

En el cas de problemes relacionats amb els equips subministrats, l'adjudicatari es farà càrrec de les gestions pertinents amb el fabricant per efectuar qualsevol dret de FGC relacionat amb la garantia de fàbrica (reposició, reparacions, etc.).

Per tal de poder requerir suport especialitzat a l'adjudicatari, aquest haurà de proporcionar una eina de tiquets, portal web o procediment per tal de garantir la correcta gestió i resposta sobre els incidents o consultes realitzades. Periòdicament l'empresa adjudicatària enviarà un informe del número d'incidents, peticions i consultes gestionades, en quin estat es troben i agrupades per severitat/criticitat durant el període d'enviament definit. S'ha de complir un SLA de servei:

Atenció incident:

Nivell de Severitat	**Resposta**
CRÍTIC	30 min
ALT	60 min
MIG-BAIX	90 min

Resolució de l'incident:

Nivell de Severitat	**Resposta**
CRÍTIC	4 hores (+SLA HW)
ALT	8 hores (+SLA HW)
MIG-BAIX	72 hores (+SLA HW)

Catalogació:

Nivell de Severitat	Definició
CRÍTIC	Incidències que impliquen tal de Servei.
ALT	Incidències que impliquen degradació de Servei.
MIG-BAIX	Incidències amb impacte al Servei.