FGC
Ferrocarrils
de la Generalitat
de Catalunya

Subministrament per la renovació dels tallafocs interns de FGC i posada en servei

Especificació tècnica

Àrea de Ciberseguretat
Tecnologies de la Informació i les Comunicacions

Setembre 2023

Índex

Introducció

Ferrocarrils de la Generalitat de Catalunya (FGC), disposa d'una ampla xarxa de dades que resulta indispensable pel correcte funcionament de la comunicació i el desplegament de serveis entre diferents emplaçaments físics de que en disposa (oficines, estacions, centre de processament de dades, etc.).

FGC, per tal de mantenir una adequada seguretat, control i segmentació de la seva xarxa interna de dades, disposa d'equipament físic de tallafocs del fabricant FORTINET (4 equips). Aquest equipament permet la detecció i neutralització d'intrusions a la xarxa interna així com el control d'aplicacions, la segmentació i aïllament de la comunicació entre serveis i usuaris.

Objecte

El que es pretén amb aquesta licitació és la renovació tecnològica dels 4 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 4 tallafocs que formen 2 clústers, administrats seran administrats per una consola centralitzada externa.

El fabricant dels equips tallafocs oferts haurà de ser FORTINET, 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 físic, quedant exclosos màquines virtuals i servidors de propòsit general. Han de poder ser instal·lats en un rack estàndard de 19''.

S'hauran de subministrar fonts d'alimentació redundants per a cada equip.

La solució ha d'incloure funcionalitats de tallafocs, control d'aplicacions, IPS, antimalware, webfilter i antispam. Totes aquestes funcionalitats han d'estar llicenciades per a la duració del contracte.

Els equips han de tenir la funcionalitat d'auditoria pròpia del Sistema, que com a resultat tingui un indicador o valor numèric de risc/compliment, així com indicar si algun paràmetre auditat no compleix normativa. Aquests paràmetres que s'han de comprovar son com a mínim: política de seguretat sense us, política de contrasenyes dèbils, compliment de "best practices" del fabricant i comprovació del llicenciament/suport.

S'haurà d'incloure a la proposta, dintre dels mateixos appliance, la funcionalitat d'auditoria pròpia del Sistema, que com a resultat tingui un indicador o valor numèric de risc, així com puntuació negativa per cada paràmetre auditat no complert. Aquests paràmetres que s'han de comprovar son com a mínim: política de seguretat sense ús en els últims 90 dies, política de contrasenyes dèbils i comprovació del llicenciament/suport.

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.

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

- Davant la detecció d'un host compromès, la solució de seguretat ha de poder enviar alertes (de qualsevol tallafocs) i bloquejar IP.

- Davant el canvi de configuració del tallafocs, un failover, reboot, actualització de firmes, de forma programada i qualsevol event del tallafocs, la solució de seguretat ha de poder enviar alertes (de qualsevol tallafocs).

Rendiment

Els equips tallafocs tindran hardware específic per tal d'assegurar el rendiment requerit; en detall, ha de tenir un hardware específic per analitzar el tràfic a nivell 4 i un altre totalment diferent, a nivell 7 i garantir baixa latència.

A nivell 7, l'equip ha de disposar d'un rendiment igual o superior a:

- Rendiment IPS: 26 Gbps.
- Rendiment NGFW (Tallafocs, IPS i control d'aplicacions): 22 Gbps.
- Rendiment amb Threat Protection (Tallafoc, IPS, control d'aplicacions i motor antimalware actius): 20 Gbps.

A nivell 4, l'equip ha de disposar de com a mínim 100 Gbps tràfic de L4.

El tallafocs ha de ser capaç de gestionar un número de sessions concurrents igual o superior a 16 milions. Així com un número igual o superior de 700.000 noves sessions per segon.

Connectivitat, interfícies i hardware de l'equip

Cada equip haurà de tenir com a mínim el següent número d'interfícies i connexions (òptiques incloses):

- 8 interfícies de 1GE
- 4 interfícies de 10GE SFP+ / GE SFP
- 4 interfícies de 25G SFP+ / 10 GE SFP+ de baixa latència

- 1 port dedicat HA
- 1 port de consola
- 1 port d'USB 3.0 per a la connexió de mòdem 3G/4G i/o pendrive.

En el cas que l'equip suporti ampliacions de memòria RAM i Disc Dur, caldrà que l'appliance estigui equipat amb el màxim de capacitats RAM i de Disc suportats.

En el cas que l'equipament permeti ampliacions modulars d'interfaces, caldrà que tots els mòduls d'ampliació estiguin equipats amb interfícies com a mínim de les mateixes velocitats que es sol·liciten pels ports mínims obligatoris.

Arquitectura de xarxa

Cal mantenir la solució ja implantada, formada per dos clúster físics iguals, cadascun dels clústers format per dos membres i estan ubicats a cada CPD. Aquest clúster ha de treballar en el mateix mode que actualment.

En el cas de necessitat de llicenciament o subscripcions per activar l'alta disponibilitat, caldrà que aquestes estiguin incloses en la proposta durant la duració completa del contracte.

Gestió

La gestió ha de ser de fàcil ús i intuïtiva.

Ha de permetre gestionar de manera unificada els 4 tallafocs.

Cal que puguem aplicar la mateixa política de seguretat (una o més d'una) sobre tots els equips (o clústers de dos equips) alhora i de forma centralitzada.

La solució sol·licitada ha d'incloure tot el llicenciament necessari per a poder gestionar de manera unificada tots els elements inclosos durant tota la durada del contracte.

El llicenciament mínim requerit per a tota la durada del contracte es Fortimanager: "FortiManager - VM FortiCare Premium Support / FortiCare Premium Support (1 - 10 devices/Virtual Domains)". Aquest producte poden variar segons les necessitats reals d'FGC o els possibles canvis efectuats en el propi fabricant.

Elements de seguretat

Les característiques del elements de seguretat principals per a la protecció de la capa interna ha de ser:

Tallafocs L4:

- Els equips han d'oferir possibilitat de definir que es treballi a L4 pels fluxos desitjats.

Control d'aplicacions:

- Proporcionar la visibilitat i control d'un mínim de 3.500 aplicacions i sub-aplicacions, widgets i aplicacions web 2.0.

- Capacitat per identificar les aplicacions sota túnels HTTPS.

- La solució ha de classificar les aplicacions en diferents categories i subcategories, per poder aplicar regles d'acord amb aquestes categories / subcategories (control granular dins de l'aplicació).

- Capacitat de creació de firmes d'aplicacions per un reconeixement personalitzat.

- Es obligatori que en aquelles aplicacions customitzades, també siguin analitzades per motors de protecció (IPS i antimalware).

IPS:

- Capacitat per protegir tant servidors com clients amb un mínim de 10000 firmes d'IPS, agrupades per categoria, severitat, objectiu i protocol, etc.

- Davant la identificació d'un atac per IPS, cal que el tallafocs capturi el tràfic en un arxiu pcap per tal d'evidenciar-ho i fer un estudi posterior.

- Capacitat per identificar patrons d'atacs basats en rated-base, per tal de bloquejar intents d'atacs un cop superat un umbral d'ús en un temps determinat.

- Capacitat de creació o importació de firmes d'IPS per un reconeixement personalitzat.

Antimalware:

- Capacitat de detecció de malware (virus, grayware, worns, etc…) basat en firmes conegudes o mètodes avançats de detecció.

- Capacitat de comprovació de si es tracta d'un fitxer bo o dolent, en funció del hashing i comparat amb la BBDD del fabricant. Així com bloquejant mitjançant malware de repositoris externs.

- Capacitat de crear firmes antimalware personalitzades. El format d'aquestes firmes seran, IPs, dominis o hashses.

S'ha d'incorporar funcionalitat de control i prevenció de fuga d'informació (DLP).

S'ha d'incorporar funcionalitats de filtrat de DNS (Capacitat de

bloqueig de DNS compromesos).

S'ha d'incorporar la capacitat per a integrar-se amb elements de seguretat de tercers via API (Infoblox, Opennac i TrendMicro).

S'ha d'incorporar la possibilitat d'obtenir fonts pròpies del fabricant, d'indicadors de compromís (IOCs).

El llicenciament mínim requerit per a tots els equips, durant la durada del contracte es: "Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium)". Aquest producte poden variar segons les necessitats reals d'FGC o els possibles canvis efectuats en el propi fabricant.

Monitoreig i reporting

S'ha de permetre el monitoreig a temps real del trànsit filtrat pels diferents mòduls dels equips.

S'ha de tenir històric de logs del tràfic analitzat pels equips, amb capacitat de 5 GB/Day of Logs and 3 TB (incloure llicenciament i suport necessari durant tota la durada del contracte).

La solució ha de permetre reports i alarmes en funció de adreces, ports i protocols.

La solució ha de permetre reports i alarmes en funció de usuaris i/o grups d'usuaris (AD/LDAP).

La solució ha de permetre poder analitzar, correlacionar i fer informes de la informació de seguretat de manera centralitzada.

La solució ha de permetre mostrar un panell de control amb vista general d'usuaris destacables, aplicacions, destinacions, llocs web, vulnerabilitats, etc.

La solució ha de permetre models d'informes preconfigurats, editables, modificables i exportables.

La solució ha de permetre la gestió d'events amb generació d'alertes automàtiques a administradors.

La solució ha de permetre que el visor de logs en temps real o històric, que permeti distingir-los entre trànsit, events i seguretat.

La solució ha de tenir capacitat de filtratge i granuralitat d'anàlisi de logs.

La solució ha de permetre dissenyar alertes i ha de ser intuitu i comprensible.

La solució ha de permetre la possibilitat de generació d'alertes per nivells de seguretat, events específics, accions o destinacions i nombre d'events en un determinat temps.

La solució ha de tenir capacitat de cercar alertes històriques i logs de manera eficaç.

La solució ha de permetre la notificació d'alertes per correu electrònic, SNMP o syslog.

La solució ha de permetre la rotació de logs recopilats automàtica amb enviament d'històrics a d'altres sistemes per email, FTP, HTTP, etc.

La solució ha de permetre la exportació de logs i reports fàcilment a diversos formats estàndards.

La solució ha de permetre la vista comparada de patrons de trànsit i amenaces.

La solució ha de permetre l'anàlisi exhaustiva de totes les activitats relacionades amb el trànsit i els dispositius.

En el cas de que el fabricant de la solució disposi de fonts pròpies d'indicadors de compromís (IOCs), s'ha d'incloure el subministrament de llicencies per tot el període del contracte.

El llicenciament mínim requerit per a tota la durada del contracte es Fortianalyser i aquest ha d'ingestar 35G/día de logs: "FortiAnalyzer-VM FortiCare Premium Support / FortiCare Premium Support". Aquest producte poden variar segons les necessitats reals d'FGC o els possibles canvis efectuats en el propi fabricant.

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

Lo solució proposada haurà de constar de 4 equips instal·lats als CPD de Sarrià i Rubí.

Els equips estan configurats en actiu passiu per donar alta disponibilitat a tota la solució.

Els tallafocs son el Gateway de l'enrutament i reenviament virtual (VRF) per tal de que siguin aquests els que controlin la visibilitat i permetin establir regles de seguretat a la xarxa MPLS.

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 aplicat a la xarxa.

- 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'haurà de realitzar una revisió de seguretat on s'avaluï l'estat actual de les polítiques de seguretat i visibilitat aplicades i es proposin polítiques més restrictives i millores de la seguretat. S'hauran d'implementar i validar.

- S’haurà de realitzar una revisió de la integració actual dels tallafocs amb el Active Directory de FGC (FSSO) per tal d’aplicar millores i donar redundància a la configuració feta.

- 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. Es revisarà i actualitzarà la guia d’operació existent a FGC, amb les millores i canvis significatius o rellevants.

- S’haurà de realitzar una fase de formació i traspàs de coneixements si han hagut canvis significatius en la nova implantació. Aquesta formació s’haurà de fer en dos vegades per tal de cobrir tot el personal assistent.

- 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 d’uns 5 mesos seguint aquest Planning:
  - Fase 1: Subministrament d’equips (3 setmanes)
  - Fase 2: Revisió i auditoria (3 setmanes)
  - Fase 3: Posada en producció dels tallafocs. (4 setmanes)
    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 3 no quedarà tancada fins que FGC no doni el vist i plau de que es compleixen els requeriments necessaris.
  - Fase 4: Implantació de les millores (6 setmanes)
  - Fase 5: Entrega de documentació i tancament del projecte (2 setmanes). 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 el hardware subministrat, 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.