



Plec de Prescripcions Tècniques

Nova Arquitectura Identity Awareness dels Firewalls Check Point

Expedient: 15012814

Febrer 2024

Signatura

Nom: Jose Molina López
Tècnic de xarxes

Xarxes i infraestructures de Telecomunicacions
Solucions de Negoci
Àrea de Tecnologia

Índex de continguts

1. Presentació	3
2. Àmbit de la contractació.....	4
2.1. Serveis de disseny i implantació de la nova infraestructura de Identity Awareness de Checkpoint	4
2.2. Serveis professionals d'Enginyers de Checkpoint.	5
2.3. Garantia i manteniment.....	5
3. Documentació a entregar	6
3.1. Informes de seguiment	6

1. Presentació

Actualment la xarxa de TMB disposa de diferents tallafocs del fabricant Checkpoint. Tradicionalment les polítiques dels tallafocs es fonamentaven en la utilització de les adreces IPs d'origen i destí per establir les regles, però cada vegada més la tendència és fer la regles per la identitat de l'usuari que es connecta i no per l'adreça IP.

Els tallafocs de Checkpoint disposen de funcionalitats anomenades "Identity Awareness" per obtenir la identitat dels usuaris que hi ha darrere una IP per diferents mecanismes (consulta directa al directori actiu, col·lectors de identitat, integració amb altres eines,...).

Actualment a TMB ja tenim implementada aquestes funcionalitats de "Identity Awareness" i tenim regles basades en la identitat de l'usuari, però cal fer una revisió i una redifinició per optimitzar-la i perquè té mancances.

2. Àmbit de la contractació

L'objectiu d'aquest plec és la contractació d'un projecte per redissenyar la infraestructura de Identity Awareness dels Firewalls Checkpoint de TMB per poder aplicar de forma correcta les polítiques de seguretat en funció de l'usuari i no de l'adreça IP del equip.

El projecte haurà d'incloure la contractació dels serveis professionals d'enginyers de Checkpoint per tal de fer el disseny d'aquesta infraestructura. En el disseny es determinarà l'adquisició del hardware i llicències que siguin necessàries. En el cas de requerir el desplegament de nous gateways de Checkpoint es podrà fer servir la infraestructura de Checkpoint VSX que actualment hi ha a TMB.

2.1. Serveis de disseny i implantació de la nova infraestructura de Identity Awareness de Checkpoint

Es demana els serveis necessaris per dissenyar, desplegar, configurar i posar en producció la nova infraestructura de Identity Awareness de TMB. Aquests serveis hauran d'incloure com a mínim el següent:

- El disseny i enginyeria global (projecte detall, instal·lació i configuració) del desplegament de la nova infraestructura segons requeriments funcionals de TMB. Haurà de contemplar la correcta integració amb els següents elements:
 - Directori Actiu de Microsoft
 - Plataforma Cisco ISE.
 - Escriptoris i PCs virtuals de Cítrix.
- En la situació actual cada Firewall intenta obtenir la identitat de l'usuari de forma independent i el que es vol amb la nova infraestructura és fer un repartiment dels rols i especialitzar equips en obtenir la identitat del usuari i que després la comparteixin amb tots els Firewalls que la necessitin en les seves polítiques per evitar duplictat de processos.
- És molt important tenir en compte que els tallafocs actuals de TMB estan en producció i que es treballarà amb l'objectiu de minimitzar el possible tall de servei que es pugui produir. Això implicarà que una part dels treballs d'aquest projecte s'hauran de realitzar en horari nocturn segons indicacions de TMB.
- Documentació d'acord amb els requeriments de TMB de la instal·lació realitzada i dels procediments bàsics d'operació.

- Formació als tècnics del departament de Xarxes de TMB.
- Formació als tècnics TLC del departament d'Operacions de TMB.

Per qüestions de seguretat no es proporcionen els detalls de la configuració actual a aquest plec i només es proporcionaran a les empreses que es presentin a la licitació per a que puguin dimensionar la seva oferta.

2.2. Serveis professionals d'Enginyers de Checkpoint.

S'hauran de contractar 6 jornades de serveis professionals d'enginyers del fabricant Checkpoint. L'objectiu d'aquestes jornades és que l'enginyer de Checkpoint participi a les següents funcions

- Revisió de requisits de TMB:
 - Casos d'ús.
 - Integració amb Directori Actiu.
 - Integració amb Cisco ISE.
 - Escriptoris i PCs virtuals de Citrix.
 - Requisits de disponibilitat.
- Definició d'una proposta d'arquitectura.
- Validació en entorn de proves de l'arquitectura proposada.
- Documentació de l'arquitectura.
- Suport avançat, si cal, durant el desplegament del projecte per part del licitador.

2.3. Garantia i manteniment

Garantia de 1 any de la instal·lació realitzada amb un temps de resposta de 24x7x4, a partir de la data de posada en servei.

3. Documentació a entregar

A la finalització de la instal·lació de l'equipament de xarxa s'haurà de lliurar la següent documentació:

- Documentació "AS BUILT". Ha d'incloure descripció de la ubicació i configuració de tots els equips així com un mapa global de tota la xarxa. També inclourà la definició dels serveis de la xarxa i l'adreçament IP definit.
- Diagrames de xarxa. Per tal de tenir la xarxa ben documentada serà necessari entregar, a més del mapa global de la xarxa, els següents diagrames:
 - Diagrama Físic: mostra tots els switchs, routers, connexió MPLS, etc. (ha d'incloure enllaços, grups, velocitats, ports, slots, tipus de xassís, software, MACAddress, ports bloquejats, enllaços principals, enllaços de backup...).
 - Diagrama Lògic: mostra les funcionalitats a nivell 3 (routers, VLANs i segments Ethernet). Adreces IP, subxarxes, capes d'accés, distribució i nucli i tota la informació de routing.
- La documentació es complementarà amb catàlegs de tot l'equipament instal·lat amb les seves característiques tècniques incloent codis i referències.
- Inventari detallat per introduir a la CMDB de TMB tot el material instal·lat amb la següent informació: equipament (nom, model, versió HW), número de sèrie, adreça IP, versió software.
- Procediments bàsics d'operació.

Seràn propietat de TMB tots els documents elaborats para la instal·lació del present contracte.

Tota la documentació estarà escrita en català o en castellà.

3.1. Informes de seguiment

Per tal de tenir un control exhaustiu de tota la instal·lació que s'està realitzant serà necessari la següent informació:

- Abans de començar la instal·lació serà necessari una planificació detallada de tota la instal·lació.
- Actes de seguiment periòdiques amb tot el que s'ha instal·lat durant aquest període. En aquestes actes s'ha de contemplar evolució de la instal·lació, incidències possibles que hi hagi pogut haver, fotos dels punts crítics d'instal·lació, així com tota aquella informació que el Contractista consideri oportuna. La periodicitat pot variar si TMB ho creu necessari i segons l'avanç del projecte.

A part d'aquesta documentació seran necessàries reunions periòdiques per fer el seguiment de l'avanç del projecte i analitzar problemes o futures actuacions. Aquestes reunions podran ser quinzenals o mensuals segons cregui TMB. En aquestes reunions s'haurà de lliurar tota documentació de les setmanes anteriors i la planificació al dia de la instal·lació indicant punts crítics per possibles de retards si s'escau.

Annex A: Taula Amidaments Revisió Arquitectura Identity Awareness dels Firewalls Check Point.