



Gipuzkoako Garraioaren Lurralde Agintaritza
Autoridad Territorial del Transporte de Gipuzkoa

PLIEGO DE PRESCRIPCIONES TÉCNICAS QUE HAN DE REGIR EN EL CONTRATO DE SUMINISTRO HARDWARE Y SOFTWARE PARA LA MEJORA DE LA DISPONIBILIDAD Y SEGURIDAD

Exp. E4/2023/01



ANTECEDENTES	3
1. DESCRIPCIÓN INFRAESTRUCTURA ACTUAL	3
2. OBJETO	4
3. ALCANCE Y DISEÑO DE LOS SERVICIOS.....	4
4. LICENCIAMIENTO.....	6
5. SERVICIOS PROFESIONALES	6

ANTECEDENTES

La Autoridad Territorial del Transporte de Gipuzkoa (ATTG) lidera el proyecto de Integración Tarifaria de Gipuzkoa (ITG), Sistema MUGI, el cual fue implantado con éxito el 4 de marzo de 2013.

El Sistema MUGI define una política tarifaria única en los servicios de autobuses urbanos de Gipuzkoa (Donostia, Irun, Errenteria, Eibar, Zarautz, Arrasate, Hernani, Lasarte-Oria, Oiartzun, Oñati y Tolosa), autobuses interurbanos de Lurraldebus, servicios ferroviarios de EuskoTren y RENFE y próximamente el servicio de transporte marítimo de Pasaia, ITSASZERBI. Todo ello mediante el uso de un único soporte de pago: la Tarjeta MUGI.

El Sistema MUGI además permite el uso de una misma tarjeta para pagar en urbano de Vitoria (TUVISA), interurbanos de Araba (Álavabus), tranvía de Vitoria, Metro Bilbao y tranvía de Bilbao, así como el funicular de Larreineta y Alavabus.

Además, el sistema implica llevar todo el proceso desde el aprovisionamiento de tarjetas, gestión de solicitudes y personalización, emisión de tarjetas, permitir la posibilidad de recargar las tarjetas por distintas vías, atender a las personas usuarias y liquidar a las empresas operadoras en función de los viajes realizados entre otros.

1. DESCRIPCIÓN INFRAESTRUCTURA ACTUAL

Actualmente el entorno de virtualización de ATTG esta basado en VMware vSphere en su versión 7.0, con dos clústers formados por:

2 VMware vCenter Server Standard (vcsa01.lurraldebus.local y vcsa02.lurraldebus.local) en versión 7.0.3 build-21784236.

2 servidores HPE Proliant DL360 Gen10 SFF, con doble procesador Intel Xeon Silver 4210R (10 cores, 2,4 GHz), 384 GB (12x32) de RAM DDR4-2933 y 2 puertos FC 16Gb para conexión con la red SAN de almacenamiento

Los dos hosts tienen la misma versión instalada VMware ESXi 7.0.3 build-19193900:

3 servidores HPE DL380 Gen9 con doble procesador Intel Xeon E5-2609 v3 (1.90GHz, 6 cores) y 96 GB de RAM, 8 puertos Base-T 1Gbps y 2 puertos FC 16 Gb para la conexión a la red SAN de almacenamiento.

Los tres hosts tienen la misma versión instalada VMware ESXi 7.0.3 build-21686933:

El almacenamiento es servido mediante protocolo Fiber Channel a través de la red SAN existente formada por 2 switches FC Switch HPE SN3000B

(Brocade) a los que están conectadas 3 cabinas de almacenamiento: HPE MSA 2050, HPE MSA 2040 y HPE P2000 G3 (Está última actualmente en desuso).

En total los switches FC tiene licenciados únicamente 12 puertos, los cuales están actualmente todos ocupados.

El cluster gestionado por el vcsa01 esta formado por los 3 servidores Gen9 aloja 23 máquinas virtuales, las cuales 18 pertenecen a DFG, 2 son de uso común, y las 3 restantes son del sistema.

El cluster gestionado por el vcsa02 esta formado por los 2 servidores Gen10 aloja 42 máquinas virtuales, las cuales 25 pertenecen a ATTG, 14 son de uso común, y las 3 restantes son del sistema.

2. OBJETO

El objeto del presente contrato es la mejora de la disponibilidad y seguridad de la red de la ATTG. Como consecuencia del control mensual de seguridad de los sistemas de la ATTG, se ha llegado a la conclusión de que son necesarias varias actualizaciones y actuaciones en el sistema para su mantenimiento actualizado y mejora de la seguridad.

Entre otros, se busca la renovación de la Red LAN, obsoleta, la implantación de la doble autenticación "2FA", contratar y activar servicios de suscripción del tipo UTP, implantar una arquitectura HA para los firewalls y el diseño y despliegue de una adecuada segmentación.

3. ALCANCE Y DISEÑO DE LOS SERVICIOS

En base a lo analizado por la asistencia técnica para la seguridad y el equipo propio de la ATTG, se han identificado los siguientes suministros a realizar:

1. Renovación de Red LAN (switches), la red actual la conforman equipos básicos descatalogados e incluso algunos modelos con puertos de 100Mbps de velocidad, y con una configuración muy básica con múltiples riesgos al no disponer de mecanismos de redundancia ni de seguridad como segmentación.

Implantar una arquitectura HA real para los firewalls, actualmente no disponen de la conectividad necesaria para dar servicio de Alta Disponibilidad. Para ello sería necesario instalar dos unidades de switch en stack/switch virtual de core HA para conectar de forma redundante los firewalls, la DMZ y las conexiones de red hacia fuera con los equipos WAN y hacia dentro con los equipos LAN y resto de equipamientos de red central como servidores, cabinas, etc.

Así, el perímetro deberá estar protegido frente a las últimas amenazas de virus y demás malware, contra amenazas de día cero y ataques avanzados, se deberá poder controlar el uso web como filtrar contenido web inadecuado o prohibido dentro de la compañía, filtrado de URL que incluye cuotas, anulaciones de usuarios, búsqueda segura transparente y registro de palabras clave del motor de búsqueda, etc.

Diseño y despliegue de una adecuada segmentación de la red de acuerdo a los servicios actuales y futuros.

Suministro, instalación y puesta en marcha de:

- Nuevo modelo FortiSwitch-448E-POE (Layer 2/3 FortiGate switch controller compatible PoE+ switch con 48xGE RJ45 puertos, 4x10 GE SFP+, con automatic Max 421W POE límite de output) del fabricante Fortinet, con 1 año de soporte FortiCare premium incluido (Forticare premium ticket handling, Advanced hardware replacement (NBD), firmware y upgrades generales).
 - Nuevo modelo FortiSwitch-448E (Layer 2/3 FortiGate switch controller compatible PoE+ switch con 48xGE RJ45 puertos, 4x10 GE SFP+), del fabricante Fortinet, con 1 año de soporte FortiCare premium incluido (Forticare premium ticket handling, Advanced hardware replacement (NBD), firmware y upgrades generales).
 - 10 GE SFP+ passive direct attach cable, 1m por sistemas con slots SFP+ and SFP/SFP+
 - 10 GE SFP+ passive direct attach cable, 3m por sistemas con slots SFP+ and SFP/SFP+
2. Implementar al menos doble factor de autenticación "2FA" para los usuarios remotos que se conectan a través de VPN para reforzar la seguridad. Estará basado en FortiAuthenticator-VM, en formato de máquina virtual licenciado para hasta 100 usuarios (Unlimited vCPU, Supporting VMware ESXi/ESX, Microsoft Hyper-V, Linux Kernel-based virtual Machine (KVM) en Virtual Machine Manager y QEMU 2.5.0. y Xen Virtual Machine platforms) con 1 año de servicio de soporte del fabricante FortiCare Premium. Licencias electrónicas perpetuas FortiTokenMobile (Software one-time password tokens for iOS, Android y Windows Phone mobile devices) para 50 usuarios como token para el 2FA.
3. Contratar y activar los servicios de suscripción de tipo "Unified Threat Protection (UTP)", de equipos FortiGate.100F (SN: FG100FTK23002083/FG100FTK23005418) hasta un año que incluye: IPS, AV, Botnet IP/Domain, Mobile Malware, FortiGate Cloud Sandbox including Virus Outbreak and Content Disarm & Reconstruct, Application Control, URL, DNS & Video Filtering, Antispam Service.

El soporte solicitado será ilimitado en horario de servicio de la administración de sistemas de la ATTG, de 8:00 a 18:00

4. LICENCIAMIENTO

La solución diseñada deberá estar optimizada para minimizar al máximo el coste de licenciamiento, tanto del entorno de virtualización basado en VMware, como del licenciamiento de los servidores virtuales con sistema operativo Microsoft, como del entorno de las copias de seguridad. El licenciamiento de lo suministrado será como mínimo para un año. En el caso de doble autenticación, se valorará la ampliación de dicho licenciamiento.

5. SERVICIOS PROFESIONALES

Los servicios profesionales necesarios son los asociados al correcto despliegue e instalación de los recursos mencionados:

1. Instalación y despliegue de la nueva Red LAN: Servicios de análisis, diseño, configuración y puesta en marcha de nueva solución de red FortiSwitch de Fortinet en el CPD de ATTG, con gestión centralizada y unificada desde FortiGate, en el CPD, incluidos la migración de los servicios de red sobre los nuevos equipos y la documentación final de la red instalada. Incluye la revisión, el estudio de nuevo plan de direccionamiento IP y la reconfiguración de toda la red LAN para su optimización y segmentación en VLANs diferenciadas por servicio, con una arquitectura HA para redundar las conexiones críticas, y la retirada de la electrónica existente obsoleta.
2. Para implementar el doble factor de autenticación "2FA" para los usuarios remotos que se conectan a través de VPN para reforzar la seguridad:
 - Instalación y configuración inicial
 - Homologación de firmware para nueva unidad
 - Configuración y carga de licencias
 - Integración con 1 servidor LDAP
 - Configuración de sync rule para grupos de AD y entrega de token
 - Agregar cliente de radius y configuración de política de radius
 - Integración con firewall FortiGate para el uso de 2FA en VPN de acceso remoto (validando usuario y token)
 - Inducción al cliente sobre funcionamiento de la solución
3. Desplegar y activar los servicios de suscripción de tipo "Unified Threat Protection (UTP)", que incluye: IPS, AV, Botnet IP/Domain, Mobile Malware, FortiGate Cloud Sandbox including Virus Outbreak and



Content Disarm & Reconstruct, Application Control, URL, DNS & Video Filtering, Antispam Service.

Se programará por parte del licitador el traspaso de conocimiento, formación sobre la infraestructura instalada y entrega de documentación completa de la instalación realizada.

El licitador explicará en su oferta de forma detallada como realizar estas tareas sin interrumpir, o en caso estrictamente necesario, interrumpir lo mínimo el servicio actual. Detallará el plan de actuación para todos los casos.