RENOVACIÓN TECNOLÓGICA DE FW NGFW PARA PUESTOS DE MANDO Y RED CORPORATIVA

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARTICULARES

ÍNDICE

1.- OBJETO DEL PLIEGO DE PRESCRIPCIONES TÉCNICAS PARTICULARES

2.- RELACIONES ENTRE ETS Y EL CONTRATISTA. DEFINICIONES

3.- ANTECEDENTES

4.- DESCRIPCIÓN DE LOS EQUIPOS INFORMÁTICOS Y TRABAJOS

5.- PLAZO DE EJECUCIÓN DE LOS TRABAJOS

6.- PRECIOS UNITARIOS

7.- JUSTIFICACIÓN DEL PRESUPUESTO

8.- FORMA DE ADJUDICACIÓN

ANEXOS

Nº 1 DESCRIPCIÓN DE ESPECIFICACIONES TÉCNICAS Y TRABAJOS A REALIZAR

1. OBJETO DEL PLIEGO DE PRESCRIPCIONES TÉCNICAS PARTICULARES

El objeto del presente Pliego de Prescripciones Técnicas Particulares es el de establecer las Condiciones Técnicas que han de regir la adjudicación y, en su momento, la realización de los trabajos de **RENOVACIÓN TECNOLÓGICA DE FW NGFW PARA PUESTOS DE MANDO Y RED CORPORATIVA.**

2. RELACIONES ENTRE ETS Y LA CONTRATISTA. DEFINICIONES

A los efectos de fijar las relaciones contractuales se definen las siguientes figuras jurídicas:

- PROPIEDAD.- Euskal Trenbide Sarea, Ente Público del Gobierno Vasco.
- RESPONSABLE DEL CONTRATO.- Euskal Trenbide Sarea designará una persona Responsable del Contrato, bajo la supervisión del Secretario General de ETS. La persona responsable del Contrato podrá rodearse del equipo técnico necesario que le asesorará y en su caso podrá actuar por delegación del mismo.
- CONTRATISTA.- Licitadora Adjudicataria, persona natural o jurídica que adquirirá esa condición a la firma del Contrato.
- DELEGADO DEL CONTRATISTA.- Técnico/a designado/a por la Contratista para hacerse cargo de la coordinación técnica de los trabajos y representar a éste frente a ETS. Todo el equipo de la Contratista dependerá del Delegado quien informará directamente y cuantas veces sea requerido a la persona Responsable del Contrato.

3. ANTECEDENTES

La red IP de ETS se divide en dos zonas principales. Por un lado, se encuentra la red de Explotación o red OT, y por otra la red Corporativa o red IT. A su vez, estas dos redes se gestionan de forma lógica por el área geográfica a la que pertenecen, Gipuzkoa o Bizkaia.

Las dos redes independientes se extienden a todas las sedes y estaciones principales de ETS, soportando de forma segura todas las comunicaciones que son necesarias para el desarrollo de sus funciones. Ambas redes están protegidas de forma controlada y existen dispositivos de Firewall para gestionar, monitorizar e implementar el control de acceso del tráfico IP.

Además del control de acceso de ambas redes, existen accesos desde el exterior, accesos con operadores ferroviarios (Metro Bilbao y EuskoTren), segmentos o Vlanes dedicadas para diferentes servicios (Telefonía IP, DMZ, servidores, oficina Sindicatos, Accesos a la red OT, Sistemas de control de barreras ferroviarias, redes wifi, redes VPN, Batera, …).

Arquitectura de los firewalls en ETS

En ETS se potencia la seguridad de la red incluyendo como cortafuegos locales un clúster lógico en HA Activo/Pasivo de firewalls NGFW (Next Generation Firewall)

- ***BIZKAIA***

  Con el fin de mantener una barrera para proteger las conexiones citadas, ETS dispone para la parte de red IT Vizcaína, dos líneas de cortafuegos: una local y otra perimetral.

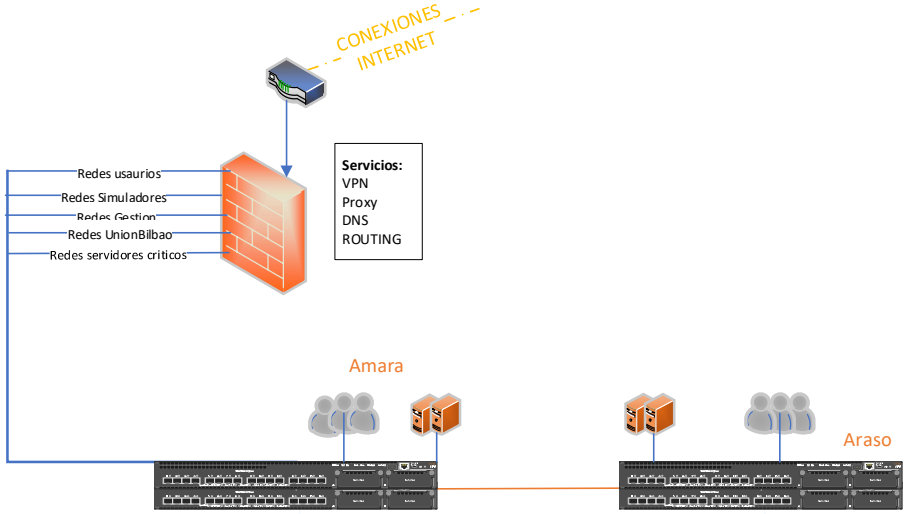
  Desde 2016, junto la adquisición e instalación de los firewalls PALO ALTO NGFW locales, se contrató un soporte asociado del fabricante. Dicho soporte incluye la resolución de incidencias hardware y software del firewall, además de las actualizaciones de sistema operativo y del propio servicio de protección asociado:

  - PAN Threat Prevention
  - PAN-DB URL Filtering
  - PAN WildFire License
  - PAN DNS Security

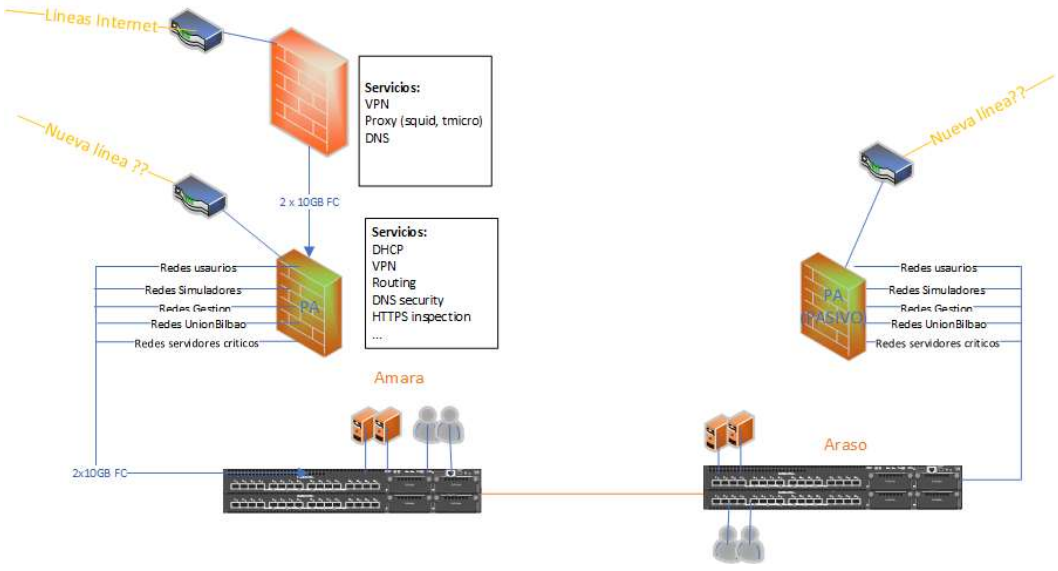
  Los contratos de soporte y mantenimiento del hardware y de los servicios expiran el 18/2/2026.

- ***GIPUZKOA***

Actualmente, la parte IT guipuzcoana dispone de un firewall perimetral que gestiona y filtra el tráfico de las distintas redes conectadas, con el objetivo de proteger las conexiones previamente citadas.



ETS tiene la intención de evolucionar hacia el modelo implementado en Bizkaia, incorporando cortafuegos locales adicionales que funcionen conjuntamente con el perimetral existente, permitiendo así fortalecer la seguridad y aumentar su eficacia.



ETS, consciente de la evolución de las tecnologías, así como de las propias necesidades cambiantes de los usuarios de la red y en previsión del aumento de las necesidades de filtrado e inspección de tráfico debido al incremento de la delincuencia cibernética, ha decidido abordar la renovación tecnológica de los cortafuegos citados con los siguientes objetivos:

- Incrementar el número de conexiones posibles.
- Incrementar la capacidad de inspección de tráfico.
- Incrementar la capacidad de respuesta frente a intrusiones.

Para la renovación de tecnológica de los cortafuegos, se requiere:

- BIZKAIA (Albia-Atxuri):
  Sustituir el hardware actual Palo Alto PA-3220, por el modelo Palo Alto PA-1420 y adquirir el paquete de suscripción a 5 años que incluye licenciamiento para:
  - Advanced Threat Protection (ATP)
  - Advanced Wildfire (AWF)
  - Advanced URL Filtering (AURL)
  - Advanced DNS Security (ADNS)
  - SD-WAN

  El cambio de hardware se realizará en horario de oficina y sin parada de servicio.

- GIPUZKOA (Amara-Araso):
  Suministro, instalación y puesta en marcha de un clúster en HA de dos nodos modelo 1410 y adquirir el paquete de suscripción a 5 años que incluye licenciamiento para:
  - Advanced Threat Protection (ATP)
  - Advanced Wildfire (AWF)
  - Advanced URL Filtering (AURL)
  - Advanced DNS Security (ADNS)
  - SD-WAN

  La instalación y puesta en marcha del nuevo clúster local se realizará con la mínima parada de servicio posible.

4. DESCRIPCIÓN DE LOS EQUIPOS INFORMATICOS Y TRABAJOS

Los equipos se deberán sujetar a los requisitos mínimos exigidos en las especificaciones técnicas señaladas en el Anexo nº1. Cada licitadora deberá detallar las características de los equipos ofertados.

Los materiales ofertados serán entregados perfectamente embalados, de acuerdo con el precio y los plazos de entrega establecidos en la oferta. Los gastos de transporte, seguros, descarga y ubicación correrán a cargo del adjudicatario.

Todo el equipamiento suministrado deberá ser nuevo, original y de marca única del fabricante, en ningún caso restaurado ("refurbished").

La oferta de la renovación del NGFW incluirá las siguientes tareas para los dos clústeres:

Suministro, instalación, configuración, puesta en marcha, soporte y mantenimiento de cortafuegos y sus licencias/suscripciones asociadas.

El paquete de licencias/suscripciones asociadas a los dos clústeres NGFW a suministrar será el denominado "Subscription Bundle (ATP+AURL+AWF+ADNS+SD-WAN) - 5 years", que incluye:

- Advanced Threat Protection (ATP)
- Advanced URL Filtering (AURL)
- Advanced Wildfire (AWF)
- Advanced DNS Security (ADNS)
- SD-WAN

5. PLAZO DE EJECUCIÓN DE LOS TRABAJOS

El plazo máximo para suministro e instalación de los equipos es el indicado en la carátula.

6. PRECIOS UNITARIOS

Los precios unitarios a ofertar serán como mínimo los indicados en el punto 7 del presente Pliego.

7. JUSTIFICACIÓN DEL PRESUPUESTO

El presupuesto máximo de licitación es el indicado en la carátula.

Cada licitadora calculará el Presupuesto, aplicando los precios unitarios ofertados a las mediciones correspondientes y de acuerdo con la siguiente estructura:

Mediciones	**Código**	**Descripción**	**Coste unitario, sin IVA**	**Coste Total, sin IVA**
2		Palo Alto PA-1420 in HA		
2		PA-1420 Subscription Bundle (ATP+AURL+AWF+ADNS+ SD-WAN) - 5 years		
2		PA-1420 450W spare power supply		
2		PA-1420 4-Post rack mount kit for 1U		
2		PA-1420, Partner enabled premium support, 5 years		
2		Palo Alto PA-1410 in HA		
2		PA-1410 Subscription Bundle (ATP+AURL+AWF+ADNS+ SD-WAN) - 5 years		
2		PA-1410 450W spare power supply		
2		PA-1410 4-Post rack mount kit for 1U		
2		PA-1410, Partner enabled premium support, 5 years		
12	PAN-SFP-PLUS-SR	SFP+ form factor, SR 10Gb optical transceiver, short reach 300m, OM3 MMF, duplex LC, IEEE 802.3ae 10GBASE-SR compliant: - 4 x PA-1420 Albia - 4 x PA-1420 Atxuri - 2 x PA-1410 Amara		

		- 2 x PA-1410 Araso		
12	SFP+ Aruba J9150D	SFP+ J9150D para Switch: -4 x Switch Aruba 6300M (JL658A) en CPD Albia -4 x Switch Aruba 3810M (JL075A) en CPD Atxuri -2 x Switch Aruba 3810M (JL075A) en CPD Amara -2 x Switch Aruba 3810M (JL075A) en CPD Araso		
1		Importe de servicios de instalación, configuración, migración y puesta en marcha Bizkaia		
1		Importe de servicios de instalación, configuración, migración y puesta en marcha Gipuzkoa		
1		Soporte Adjudicatario Bizkaia		
1		Soporte Adjudicatario Gipuzkoa		
		TOTAL, IVA excluido		

El Presupuesto resultante será reflejado por la licitadora en la Proposición Económica y tendrá el carácter de Presupuesto Máximo del Contrato. A efectos de homogeneización de ofertas será el que se valore de acuerdo con los criterios descritos en la carátula.

Todos los trabajos descritos en el Pliego están incluidos en estos precios.

8. FORMA DE ADJUDICACION

La adjudicación del Contrato se efectuará bajo la modalidad de Licitación, y recaerá en la propuesta más ventajosa en conjunto, económica y técnicamente, de acuerdo con los criterios fijados en la carátula del presente pliego.

ANEXO Nº 1

DESCRIPCIÓN DE ESPECIFICACIONES TÉCNICAS Y TRABAJOS A REALIZAR

1. Arquitectura actual

BIZKAIA:

En la actualidad la arquitectura de firewall local se basa en un clúster lógico de dos appliances físicos de Palo Alto modelo PA-3220, configurado en Alta Disponibilidad (HA).

Ambos nodos están situados en Bilbao: uno en el CPD de Albia y otro en el CPD de Atxuri conectados ambos mediante fibra propia y a una distancia menor de 2 km.

Licencias incluidas:

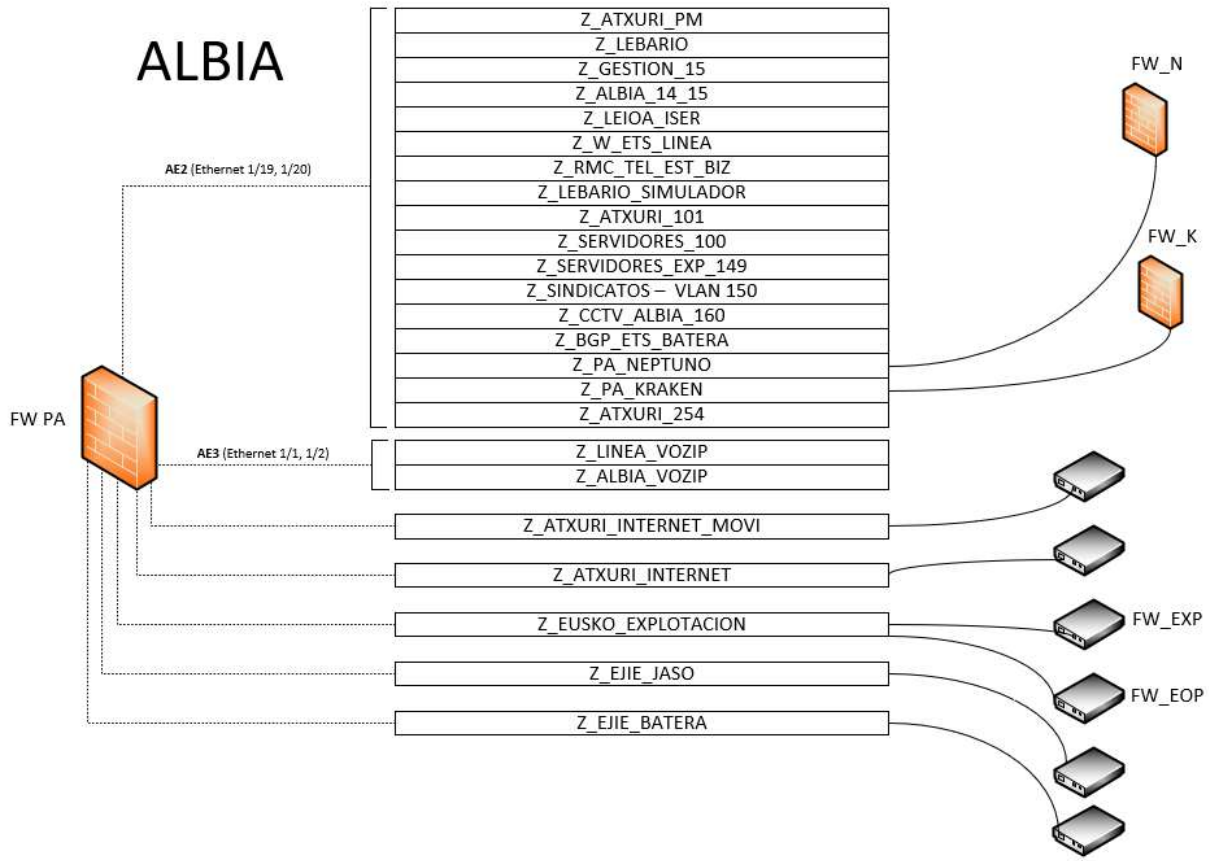
- Threat prevention
- URL Filtering
- WildFire License
- DNS Security

Interfaces:

Actualmente, además de los dos puertos de HA y el de gestión, están conectados 2 puertos SFP+ de 10 Gb formando un agregado, 2 puertos Ethernet formando un segundo agregado y 5 puertos Ethernet individuales.

Es necesario que el nuevo equipamiento al menos mantenga la capacidad de throughput de cada uno de los agregados existentes.

A modo informativo, los firewalls actuales tienen la siguiente configuración de conexionado.



Por otro lado, además de los objetos, servicios, perfiles de red y reglas (la mayoría en Capa 7), los firewalls realizan otras funciones:

- Portal cautivo de acceso a la red wifi.
- Servidor DHCP de diferentes redes.
- Global Protect VPN (incluido portal, Gateway, doble autenticación SAML2 a través de OKTA)
- Tunel ipsec site to site
- Virtual Routers. Protocolos de enrutamiento estático y dinámicos.
- Configuraciones NAT y PAT.
- Integración con Microsoft Active Directory para identificación de usuarios

- Certificados (CA Gandi, wildcard, Global Protect, OKTA, …)
- Descifrado
- Url Filtering
- Sinkhole
- Alertas de disponibilidad de la plataforma (caída parcial o completa, fallo de comunicación con AD y terceros, caducidad licencias
- Alertas de seguridad (infección masiva virus, Alertas botnets, malware…)
- Otros…

GIPUZKOA:

Actualmente no existe un clúster NGFW local en HA en Gipuzkoa. Se dispone servidor Linux ubicado en las oficinas de Amara con función de firewall perimetral de capa 4 que filtra tráfico en base a los siguientes objetos:

- Zonas (Interfaces)
- Redes
- Equipos y grupos de equipos
- Servicios (TCP/UDP)
- Reglas de tráfico.
- NAT enmascaramiento y redirección

Además de la función de firewall el servidor tiene otras funciones:

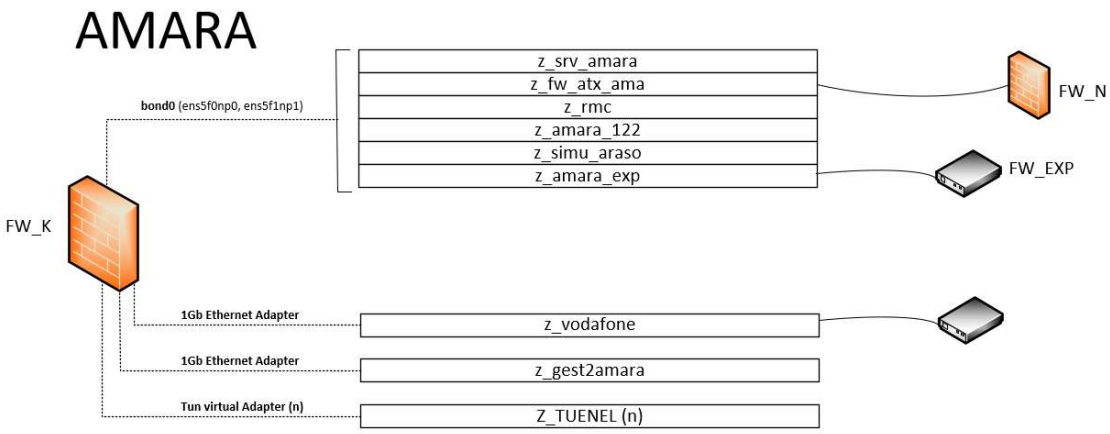
- Servidor VPN
- Proxy
- Servidor DNS
- Router

<u>Interfaces:</u>

Físicamente, en el servidor/firewall hay dos interfaces a 10Gbs formando un agregado (bond0), una interface a 1Gbs para la salida a internet y una interface a 1Gbs para la red de gestión.

Por cada instancia de VPN configurada en el servidor, se crea de forma automática una interfaz virtual gestionada por el propio servicio VPN.

De forma resumida, el firewall perimetral tiene la siguiente configuración de conexionado:



2. Suministro de hardware. Características mínimas

Se requiere el suministro del siguiente modelo con sus licencias asociadas:

Mediciones	Código	Descripción
2		Palo Alto Networks PA-1420 in HA (Bizkaia)
2		PA-1420 Subscription Bundle (ATP+AURL+AWF+ADNS+SD-WAN) - 5 years (Bizkaia)
2		PA-1420 450W spare power supply (Bizkaia)
2		PA-1420 4-Post rack mount kit for 1U (Bizkaia)
2		PA-1420, Partner enabled premium support, 5 years (Gipuzkoa)
2		Palo Alto Networks PA-1410 in HA (Gipuzkoa)
2		PA-1410 Subscription Bundle (ATP+AURL+AWF+ADNS+SD-WAN) - 5 years (Gipuzkoa)

2		PA-1410 450W spare power supply (Gipuzkoa)
2		PA-1410 4-Post rack mount kit for 1U (Gipuzkoa)
2		PA-1410, Partner enabled premium support, 5 years (Gipuzkoa)
12	PAN-SFP-PLUS-SR	SFP+ form factor, SR 10Gb optical transceiver, short reach 300m, OM3 MMF, duplex LC, IEEE 802.3ae 10GBASE-SR compliant 4 x PA-1420 en CPD Albia 4 x PA-1420 en CPD Atxuri 2 x PA-1420 CT Amara 2 x PA-1420 CT Araso
12	SFP+ Aruba J9150D	SFP+ J9150D para connexion a Switch: -4 x Switch Aruba 6300M (JL658A) en CPD Albia -4 x Switch Aruba 3810M (JL075A) en CPD Atxuri -2 x Switch Aruba 3810M (JL075A) en CPD Amara -2 x Switch Aruba 3810M (JL075A) en CPD Araso

3. Trabajos a realizar

Los servicios de instalación, configuración y puesta en marcha deberán realizarse de forma que los usuarios se vean mínimamente afectados, siendo necesario presentar un plan de implantación, que asegure este punto, y que deberá contar con la validación de ETS.

Todos los gastos de desplazamiento necesarios para la ejecución de los trabajos asociados al proyecto estarán incluidos.

Los sistemas enrutados y securizados a través de los firewalls Palo Alto en ETS dan soporte a la infraestructura ferroviaria sensible.

Es importante recalcar que la planificación y tiempos de parada expuestos en el pliego de condiciones deben ser cumplidos al detalle en el proyecto ya que son fundamentales para el correcto funcionamiento del servicio ferroviario. Servicios de localización de los trenes en Vía, apoyo al personal de visibilidad reducida, acceso a los mantenedores, gestión de incidencias de circulación o acceso a telemandos dependen directamente de los firewalls.

3.1. Bizkaia:

Los trabajos se iniciarán en Albia y Atxuri (Bizkaia) y tendrán que estar finalizados antes de que acabe el soporte de los PA 3220 actuales.

Fase 1. Instalación y conexionado físico del sistema

La empresa adjudicataria instalará el hardware en un rack existente del CPD de Albia en Bilbao (APC) y otro en el de Atxuri en Bilbao. Tanto en Albia como en Atxuri la conexión entre diferentes racks (rack del firewall y racks de electrónica de comunicación) se realiza a través de paneles preconectorizados.

El modelo de los switches de unión existentes es el indicado en el punto "2. Suministro de hardware. Características mínimas".

Los dos firewalls nuevos coincidirán en el mismo rack que los Firewalls Actuales.

La empresa adjudicataria conectará los equipos a la red eléctrica y de Ethernet/fibra.

Todo el cableado de cobre y fibras necesarias para la conexión, se incluirá en el proyecto sin coste adicional alguno.

Debido al cambio de configuración de puertos de conexión y agregados, se debe incluir cualquier elemento necesario para que los equipos queden plenamente operativos, como latiguillos de red (mínimo Cat 6a), latiguillos de fibra, SFPs (de firewall y Switch), etiquetas, fijaciones…

***Fase 2*.** Configuración de la gestión del clúster, licenciamiento.

El adjudicatario configurará en las dependencias de ETS la interfaz de gestión asignándole una IP establecida por ETS. Se actualizarán el sistema operativo PANOS de los cortafuegos suministrados a la versión actual de los 3220.

La implantación se realizará en una configuración de Alta Disponibilidad (HA) activo-pasivo, similar a la actual.

Todas aquellas licencias/suscripciones incluidas en la oferta deberán ser activadas y agregadas.

Se configurarán y activarán las actualizaciones dinámicas (Antivirus, Threaths, Diccionario del dispositivo, Wildfire, …) y la descarga de nuevas versiones de software (PANOS, Global Protect, …").

Fase 3. Carga de configuración y adaptación de configuración según nuevos conexionados 10Gb

El adjudicatario cargará la configuración de los firewalls antiguos.

Cambiará la configuración de conexionado físico, quedando un único agregado compuestos por cuatro interfaces de 10Gb. Solamente quedarán conectados a interfaces de 1Gb Ethernet (Cat 6 mínimo) los puertos de HA y de gestión del FW.

Todas las subinterfaces y redes pertenecientes a cada zona pasarán a ser parte de este nuevo agregado. Para llegar a la configuración final del conexionado el adjudicatario deberá:

- Mantener la configuración del agregado AE2 y añadir 2 interfaces de 10 Gb, quedando compuesto por un total de 4 interfaces de 10Gb.
- Eliminar el agregado AE3 y configuración residual relacionada.
- Eliminar la configuración residual de los 5 interfaces.

Se comprobarán que toda la configuración cargada funciona correctamente:

- Objetos
- Servicios
- Perfiles
- Etiquetas
- Reglas
- DHCP server
- Portal cautivo
- Túneles VPN
- Global Protect VPN
- Configuraciones NAT y PAT.
- Integración con Microsoft Active Directory para identificación de usuarios
- Importación de certificados (CA Gandi, wildcard, Global Protect…)
- Descifrado
- Url Filtering
- SinkHole
- Reenvío de logs
- integración con Kaspersky (programa a medida KSCvsPAN).
- Otros…

Fase 4*.* Puesta en producción, revisión de la arquitectura y adaptación de las nuevas interfaces.

El paso a producción de los FW nuevos, debe suponer un corte máximo de 30 minutos. Estas operaciones se realizarán en horario de oficina, y los técnicos del adjudicatario y los técnicos de ETS lo harán de forma presencial (8:00 – 19:00).

Una vez se pasen a producción los nuevos FW, inmediatamente después del pase a producción se realizará una batería de pruebas propuesta por el adjudicatario revisada, actualizada y aprobada por ETS. Se comprobará la conexión a todas las redes conectadas, el correcto funcionamiento de las reglas y los servicios asociados, comprobando que toda la configuración cargada funciona correctamente.

En el caso de considerar ETS que el servicio no se ofrece de forma adecuada a las personas usuarias (debido a un fallo en la configuración del nuevo appliance), el adjudicatario volverá atrás, conectando las interfaces a los firewalls antiguos hasta encontrar el fallo. Se deberá prever una vuelta atrás que no supere los 30 minutos de parada.

Fase 5*.* Tareas posteriores (3-4 meses después de la puesta en producción)

- Revisión de la configuración del firewall a realzar por el adjudicatario.
    - Revisión de las reglas: revisará las reglas que no se han usado, los objetos de las reglas obsoletos y pasará las reglas que no estén en capa 7 o en capa de usuario.
    - Analizará y mejorará las políticas/reglas de los servicios de ETS publicados en Internet.
    - Aplicará configuración de grupos en las reglas.

Fase 6. Retirada de los equipos antiguos (6-12 meses después de la puesta en producción)

El adjudicatario desconectará los PA-3220 y su cableado. Se encargará de su retirada y entregará el certificado del "Documento de identificación de residuos" de cumplimiento en el Real Decreto 110/2015 de 20 de febrero "Sobre los residuos de aparatos eléctricos y electrónicos".

3.2. Gipuzkoa

Una vez finalizada y verificada la estabilidad de la instalación de Bizkaia, ETS y el adjudicatario acordarán el inicio de los trabajos para la instalación, configuración y puesta en marcha de los nuevos firewalls en Amara y Araso (Gipuzkoa).

Es importante recalcar que la planificación y tiempos de parada expuestos en el pliego de condiciones deben ser cumplidos al detalle en el proyecto ya que son fundamentales para el correcto funcionamiento del servicio ferroviario. Servicios de localización de los trenes en Vía, acceso a los mantenedores, gestión de incidencias de circulación o acceso a telemandos dependen directamente de los firewalls.

Fase 1. Instalación y conexionado físico del sistema (Jornada 1 y 2)

La empresa adjudicataria deberá realizar la instalación y conexionado de los nuevos PA 1410 a lo largo de dos jornadas diferentes, en horario de oficina, dedicando un primer día a la instalación en las oficinas de Amara y un segundo día a la instalación en las oficinas de Araso.

La instalación del Hardware se realizará en los racks existentes en las oficinas de Amara (HP 600mmx1075mm, 48U) y en las oficinas de Araso (Rittal 800mm x 1200mm, 42U).

Tanto en Amara como en Araso, la electrónica de red a la que se conecta cada uno de los nodos se ubican en el mismo rack. El modelo de los switches a conectar es el indicado en el punto "2. Suministro de hardware. Características mínimas".

La empresa adjudicataria conectará los equipos a la red eléctrica y de Ethernet/fibra.

Todo el cableado de cobre y fibras necesarias para la conexión, se incluirá en el proyecto sin coste adicional alguno.

Se debe incluir cualquier elemento necesario para que los equipos queden plenamente operativos, como latiguillos de red (mínimo Cat 6a), latiguillos de fibra, SFPs (de firewall y Switch), etiquetas, fijaciones…

Fase 2. Configuración de la gestión del clúster y licenciamiento (Jornada 1-2)

Durante los dos días de la fase de "Instalación física y conexionado", en horario de oficina, el adjudicatario también configurará la interfaz de gestión asignándole una IP establecida por ETS. Se actualizará el sistema operativo PANOS de los cortafuegos suministrados a la misma versión instalada en los firewalls del clúster previamente instalado en Bizkaia.

La implantación se realizará en una configuración de Alta Disponibilidad (HA) activo-pasivo.

Todas aquellas licencias incluidas en la oferta deberán ser activadas y agregadas.

Se configurarán y activarán las actualizaciones dinámicas (Antivirus, Threaths, Diccionario del dispositivo, Wildfire, …) y la descarga de nuevas versiones de software (PANOS, Global Protect,…").

Antes de pasar a la siguiente fase, se comprobará durante un mínimo de 7 días la estabilidad de las actualizaciones, el correcto sincronismo entre nodos del clúster y la adecuada integración del sistema en la red gestión de ETS.

Fase 3: Conexionado con FW Perimetral existente (Jornada 3)

El adjudicatario, fuera de horario de oficina, deberá configurar en el nuevo firewall PA-1410 un enlace agregado compuesto por dos interfaces de 10 Gb, el cual deberá integrarse con la electrónica de red existente, previamente configurada con un LACP

dinámico. Sobre dicho agregado se deberá desplegar la red de interconexión entre el PA y el firewall perimetral, que constituirá el canal de enrutamiento del tráfico correspondiente.

La configuración requerida en el firewall perimetral será ejecutada por el actual mantenedor del servicio. Por lo tanto, será condición indispensable que el adjudicatario coordine previamente todas las actuaciones con dicho mantenedor, a fin de garantizar la correcta integración y operatividad de la solución.

Fase 4: Puesta en producción (Jornadas 3, 4, 5, 6 y 7)

Debido a la criticidad ya expuesta, la puesta en servicio del nuevo firewall Palo Alto se llevará a cabo en distintas fases, distribuidas en jornadas y horarios diferenciados. Dichas actuaciones se realizarán de forma presencial en las dependencias de ETS y contemplarán un tiempo máximo de interrupción del servicio de 30 minutos.

Respecto al conexionado en el nuevo PA-1410, todas las redes a migrar se configurarán como subinterfaces del agregado de dos puertos de 10 Gb. Solamente quedarán conectados a interfaces de 1Gb Ethernet (Cat 6 mínimo) los puertos de HA y de gestión.

El adjudicatario migrará y adaptará de forma progresiva, en función de las necesidades de cada fase, la configuración del firewall perimetral existente al nuevo FW PA-1410. Dicha migración incluirá Zonas, Redes, Equipos, Grupos, Servicios (TCP/UDP), Reglas de tráfico, NAT, enmascaramiento, redirecciones, Routing, entre otros. Asimismo, procederá a la configuración de las nuevas funcionalidades que ofrece el clúster NGFW PA 1410 respecto al firewall perimetral existente. Finalmente, se verificará el correcto funcionamiento de dichas funcionalidades, que corresponden con:

- Objetos
- Servicios
- Perfiles
- Etiquetas
- Reglas
- DHCP server

- Portal cautivo
- Túneles VPN
- Configuraciones NAT y PAT.
- Integración con Microsoft Active Directory para identificación de usuarios
- Importación de certificados (CA Gandi, wildcard)
- Descifrado
- Url Filtering
- SinkHole
- Reenvío de logs
- Router virtual (Rutas estáticas, …)
- Otros…

Una vez los nuevos FW den servicio a producción, con una batería de pruebas definida por ETS, se comprobará la conexión a todas las redes conectadas. Así como el correcto funcionamiento de las reglas.

En el caso de considerar ETS que el servicio no se ofrece de forma adecuada a los usuarios por algún fallo en la configuración del nuevo appliance, podrá volverse atrás, hasta encontrar el fallo. Se deberá prever una vuelta atrás que no supere los 30 minutos de parada.

a) Migración de Gateway de la Red de Usuarios (Jornada 3)

El mismo día en que se ejecute la fase 3 "Conexionado con el FW Perimetral Existente", fuera de horario de oficina, se llevará a cabo la migración del Gateway de la red de usuarios (*z_amara_122*) desde el firewall perimetral. El nuevo firewall asumirá la dirección IP correspondiente a la puerta de enlace predeterminada de la red de usuarios, adoptando así la función de Gateway para los clientes.

La red de usuarios se implementará en el nuevo PA como una subinterfaz del agregado de dos puertos de 10 Gb, manteniendo el mismo VLAN ID y asociándola a una nueva zona.

En esta fase, el nuevo PA no realizará tareas de filtrado. El tráfico será enrutado a través de la red de interconexión hacia el firewall perimetral, el cual mantendrá la responsabilidad de aplicar las políticas de filtrado vigentes.

De manera coordinada con el mantenedor del servicio del firewall perimetral, el adjudicatario efectuará todas las configuraciones asociadas al nuevo firewall para completar la migración de la red de usuarios, el enrutamiento correspondiente y el filtrado de tráfico.

Esta fase implicará una interrupción máxima de 60 minutos en el servicio para la red de usuarios. El resto del tráfico entrante o saliente, no vinculado a dicha red, no se verá afectado.

Antes de iniciar la siguiente fase del proyecto, se establecerá un periodo mínimo de observación de 7 días, durante el cual se comprobará la estabilidad de la red y el correcto funcionamiento de todos los servicios.

b) Migración de filtrado de la Red de Usuarios (Jornada 4 y 5)

En esta fase, el nuevo firewall PA asumirá el rol de filtrado del tráfico correspondiente a la red de usuarios. Para su correcta implantación, se dedicarán dos jornadas de trabajo en las dependencias de ETS.

En la primera jornada, fuera del horario de oficina, con el objetivo de garantizar una transición adecuada, el adjudicatario deberá:

- Migrar íntegramente los objetos y reglas de filtrado asociados a la red de usuarios desde el firewall perimetral al nuevo PA.
- Realizar todas las configuraciones necesarias en el nuevo firewall para aplicar el correcto filtrado de la red de usuarios.
- Verificar la correcta aplicación de las políticas migradas (Seguridad, Descifrado, NAT, PBF, Autenticación, …).

En la segunda jornada, una vez realizada la migración, el técnico implantador se desplazará nuevamente a las dependencias de ETS en horario de oficina, con el fin de:

- Monitorizar y comprobar que todo el tráfico de la red de usuarios filtra correctamente por el nuevo PA-1410.
- Atender y resolver posibles incidencias derivadas del cambio realizado.

Esta fase no implicará una interrupción en el servicio.

Antes de iniciar la siguiente fase del proyecto, se establecerá un periodo mínimo de observación de 7 días, durante el cual se comprobará la estabilidad de la red y el correcto funcionamiento de todos los servicios.

c) Migración de Gateway y filtrado de Redes IT (Jornada 6)

A esta fase se dedicará una jornada, durante la cual los trabajos requeridos se realizarán in situ fuera de horario de oficina.

El nuevo firewall asumirá el Gateway y el filtrado de trafico de las redes de IT, que son las correspondientes a las siguientes zonas del firewall perimetral:

- z_srv_amara
- z_rmc
- z_simu_araso
- z_gest2amara

Cada una de las redes IT a migrar, se implementarán en el nuevo PA como subinterfaces del agregado de dos puertos de 10 Gb, manteniendo el mismo VLAN ID y asociándolas a una nueva zona correspondiente a cada red.

Con el objetivo de garantizar una transición adecuada, el adjudicatario deberá:

- Migrar Gateway de cada una de las Redes IT.
- Migrar íntegramente los objetos y reglas de filtrado asociados a las Redes IT desde el firewall perimetral al nuevo PA.
- Realizar todas las configuraciones necesarias en el nuevo firewall para aplicar el correcto enrutamiento y filtrado de las Redes IT.
- Verificar la correcta aplicación de las políticas migradas. (Seguridad, Descifrado, NAT, PBF, Autenticación, …)
- Monitorizar y comprobar que todo el tráfico de las Redes IT es filtrado correctamente por el nuevo PA-1410.
- Atender y resolver posibles incidencias derivadas del cambio realizado.

Para llevar a cabo esta fase, será necesario que el adjudicatario se coordine previamente con el responsable del mantenimiento del firewall perimetral, con el fin de garantizar una migración correcta y evitar duplicidades.

Antes de iniciar la siguiente fase del proyecto, se establecerá un periodo mínimo de observación de 7 días, durante el cual se comprobará la estabilidad de la red y el correcto funcionamiento de todos los servicios.

d) Migración de Gateway y filtrado de Redes OT (Jornada 7)

A esta fase se dedicará una jornada, durante la cual los trabajos requeridos se realizarán in situ fuera de horario de oficina.

El nuevo firewall asumirá el Gateway y el filtrado de tráfico de la red de interconexión OT (z_amara_exp).

Esta red, se implementará en el nuevo PA como una subinterfaz del agregado de dos puertos de 10 Gb, manteniendo el mismo VLAN ID y asociándola a una nueva zona.

Con el objetivo de garantizar una transición adecuada, el adjudicatario deberá:

- Migrar Gateway de cada una de las zonas.
- Migrar íntegramente los objetos y reglas de filtrado asociados a la red de usuarios desde el firewall perimetral al nuevo PA.
- De manera coordinada con el mantenedor del servicio del firewall perimetral, efectuará todas las configuraciones asociadas al nuevo firewall para completar la migración de las redes de IT, el enrutamiento correspondiente y el filtrado de tráfico.
- Verificar la correcta aplicación de las políticas migradas. (Seguridad, Descifrado, NAT, PBF, Autenticación, …).
- Monitorizar y comprobar que todo el tráfico de la red de usuarios se encuentra filtrado correctamente por el nuevo PA-1410.
- Atender y resolver posibles incidencias derivadas del cambio realizado.

Fase 5. Tareas posteriores (2 meses después de la puesta en producción)

- Aplicar capa 7 a las reglas con la detección de aplicaciones en la propia regla.
- Revisión de la configuración del firewall perimetral. Se deshabilitarán y etiquetarán todas las reglas que no aplican tras la puesta en producción del nuevo firewall.
- Revisión de la configuración del firewall.
    - Revisión de las reglas: tras haber pasado un mínimo de 3 semanas para obtener logs de tráfico, apps… revisar las reglas que no se han usado, los objetos de las reglas obsoletos, pasar las reglas que no estén en capa 7 o en capa de usuario.
    - Análisis y mejora de las políticas/reglas de los servicios de ETS publicados en Internet.
    - Aplicar configuración de grupos en las reglas.
- Configuración de una conexión VPN punto a punto por caminos redundantes entre los clústeres PA NGFW de Bilbao/Atxuri y Amara/Araso. El medio principal serán fibras propias de ETS y el secundario será la WAN.
- Configurar Global Protect VPN (Portal, Gateway, integración con OKTA para doble autenticación).
- Configuración wifi y portal cautivo.

4. Documentación de la instalación

Se entregará la documentación técnica de proyecto con las topologías, configuraciones y los diagramas de red que sean necesarios:

- Diagrama de topología física de la red de ETS
  - Incluyen toda la electrónica de los dos CPDs
  - Incluyen los nuevos firewalls y aquellos que se mantienen
  - Se identifican los puertos e interfaces de conexión
- Diagrama de topología lógica de red IPv4 de ETS
  - Se incluyen los elementos lógicos de la red
  - Se incluyen los direccionamientos
- Se incluirá asimismo, toda aquella información adicional no contenida en data sheets o manuales del equipamiento que sea necesaria para el correcto funcionamiento de la instalación.

El adjudicatario entregará la correspondiente documentación con el diseño y configuración del sistema instalado en cada una de las ubicaciones (Bizkaia y Gipuzkoa). Se entregarán los procedimientos necesarios de las tareas habituales a realizar por el administrador de sistemas en ETS, por ejemplo:

- Creación de rutas
- Creación de reglas
- Identificación del tráfico de una aplicación no estándar
- "Best Practices" de configuración firewall
- Restore de una configuración mal aplicada.
- Renovación y sustitución de los certificados caducados que aplican en diferentes configuraciones (portal cautivo, Global Project, Desencriptación SSL…)

El diseño y configuración de la instalación deberá estar aprobada por parte del Fabricante. Las empresas licitadoras deberán contar con las siguientes certificaciones aportarse la documentación que lo acredite:

- Certificaciones generales de empresa:
  - CERT
  - CSIRT.es
  - ENS categoría media (ALTO)

    - ISO-9001
    - ISO27001
    - ISO20000-1
- Certificaciones mínimas de empresa específicas del fabricante Palo Alto:
    - Platinum Innovator Solution Provider with the following Specializations: Hardware Firewall; Software Firewall

- Certificaciones del equipo implantador (el instalador insitu) de al menos dos técnicos asignados al proyecto, técnico implantador y técnico implantador de contingencia, a menos de 1h de las instalaciones de ETS:
    - PCNSE – Palo Alto Networks Certified Network Security Engineer

(En cartula)

Deberá aportarse la documentación que acredite dicha certificación.

5. Formación

Durante todo el proceso de instalación, configuración, migración y pruebas, el adjudicatario transferirá el conocimiento necesario a los técnicos de ETS para que estos sean autónomos en la gestión del nuevo sistema.

La formación comenzará con una sesión inicial, previa a la configuración del sistema. La instalación y configuración del SW de gestión se realizará conjuntamente con los miembros del departamento de Sistemas de Información de ETS, formando en la realización de las tareas tipo. Finalmente se instruirá al personal del departamento de Sistemas para la realización de tareas de mantenimiento.

Todo el proceso se realizará en las instalaciones de ETS.

6. Soporte

Soporte del fabricante

Las licencias que sean suministradas en el presente contrato incluirán un soporte de fabricante para 5 años.

- Bizkaia: PA-1420 Subscription Bundle (ATP+AURL+AWF+ADNS+SD-WAN) - 5 years

- Gipuzkoa: PA-1410 Subscription Bundle (ATP+AURL+AWF+ADNS+SD-WAN) 5 years

Soporte del Adjudicatario

Se requiere además del soporte del fabricante un soporte por parte del licitador que incluya los siguientes servicios durante 5 años:

- Monitorización del sistema

  Se monitorizará de forma continua el estado de cada dispositivo:

  - Estado de las máquinas
  - Fallos en el clúster de HA (Si lo hay)
  - Estado de la CPU
  - Estado de la Memoria
  - Error de Paquetes
  - Sesiones
  - Estado de las Interfaces

- Operación remota de la plataforma en horario 10x5

Se realizarán todas las tareas de gestión necesarias para el mantenimiento de la plataforma ya definida:

  - Modificación de reglas

- Modificación de perfiles de acceso
- Aplicación de la solución ante incidencias
- Actualización y parches

La operación será realizada de forma peticionada por ETS o consensuado entre ambas partes cuando el adjudicatario lo proponga de forma proactiva. La operación puede darse de la siguiente forma:

- Cuando los recursos de ETS soliciten un cambio de configuración (forma reactiva)
- Cuando se asesore y se consensue una mejora en la gestión de firewalls entre ambas partes.

- Actualizaciones de la plataforma

Estas intervenciones se realizarán en horario laboral (8x5), minimizando al máximo los cortes del servicio y aprovechando la arquitectura de alta disponibilidad de los dos nodos. Se procederá de la siguiente forma:

- Se acordará con ETS la fecha para la actualización y se le explicará las implicaciones que tiene.
- Ejecución de la actualización sobre la solución y verificación del correcto funcionamiento del servicio.
- Notificación a ETS de la finalización del proceso de actualización

- Aplicación de medidas extraordinarias contra amenazas.

Se contempla la aplicación de medidas extraordinarias contra amenazas que el adjudicatario estime como importantes, críticas y generalizadas; como por ejemplo, la definición de reglas genéricas para el bloque de ficheros infectados con el Malware Emotet.

- Informes de servicio
  - Semestralmente, un técnico senior, elaborará un informe donde reflejará el estado de la plataforma y las recomendaciones de mejora;

tras su elaboración, el técnico cerrará una reunión en remoto para presentación del mismo y a su finalización, mandará un acta de la misma con las conclusiones y las acciones acordadas.

- De este informe pueden salir acciones que estén contempladas en el soporte y otras que no, en cuyo caso, el técnico se lo comunicará al comercial responsable de la cuenta para su presupuestación.

Para el soporte, el adjudicatario dispondrá de una conexión VPN permanente con ETS de tipo "Ipsec Tunnels" a los nuevos Palo Alto instalados.

La gestión remota de la Consola de Palo Alto se realizará a través de canal cifrado mediante VPN.

Acuerdos de nivel del servicio del soporte

Este servicio se prestará bajo un modelo de provisión de servicios en el que la gestión y la realización de actividades será responsabilidad del adjudicatario y la prestación del servicio está basado en **SLOs (Service Level Objective)**, de forma que, en el transcurso de su horario de atención, el objetivo de equipo de soporte del adjudicatario será responder ante una incidencia o consulta, en un tiempo máximo establecido:

Alerta	Riesgo de impacto	Descripción	Tiempo máximo respuesta
Alta o grave	Caída del servicio	El producto está en peligro de caída o ha cesado.	<= 1 hora
Media o moderada	Servicio en riesgo	La incidencia produce problemas operacionales de forma intermitente.	<= 4 horas
Baja o leve	Bajo rendimiento	La incidencia no produce ningún tipo de problema a los usuarios en el ámbito operacional.	<= 16 horas
Consulta	Asistencia General / Consulta	Consultas relativas a configuración "Cómo hacer", resolución de incidencias no críticas o asistencia general.	<= 24 horas

Ante incidencias de categoría Alta/Grave que requieran de acceso presencial a las instalaciones de ETS donde se ubican los equipos suministrados, el técnico deberá presentarse en menos de 1 hora. Las direcciones de las instalaciones donde se ubican cada uno de los nodos:

Bizkaia:

- Albia:
  San Vicente 8 Planta 14,
  Edificio Albia 1,
  48001 Bilbao,
  Bizkaia

- Atxuri:
  Calle Atxuri 10,
  48006 Bilbao,
  Bizkaia

Gipuzkoa:

- Amara:
  Easo Plaza, 9,
  20006 Donostia,
  Gipuzkoa

- Araso:
  Mazula Berri, Mazuola Kalea, 2,
  20305 Irun,
  Gipuzkoa